Technical Report

SnapDrive 7.0 for Windows for Data ONTAP 8.2 Operating in 7-Mode: Best Practices Guide

Santhosh Harihara Rao, NetApp
September 2013 | TR-4230

Simplifying and Automating Storage and Data Management for Windows Environments

NetApp® SnapDrive® for Windows® simplifies the management of business-critical information with its advanced server-based storage virtualization. It also helps businesses respond quickly to growth by providing the ability to expand storage on the fly with no downtime. In addition, it 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 6.5 for Windows.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This document is a best practices guide for NetApp storage systems using SnapDrive for Windows on NetApp storage systems running the Data ONTAP® 8.2 or earlier operating in 7-Mode. This document also provides recommendations on various configuration options that are available with the solution and the guidelines for when and where to use these 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.

For best practices on SnapDrive 7.0 for Windows for clustered Data ONTAP, refer to the TR-4228: SnapDrive 7.0 for Windows for Clustered Data ONTAP 8.2 – Best Practices Guide for SAN Environments

Unless otherwise specified, you should assume that all references to Data ONTAP in this document are applicable for Data ONTAP operating in 7-Mode.

1.2 Target Audience

This guide is for storage and server administrators managing storage provisioning and Snapshot copies in NetApp storage systems using SnapDrive for Windows. NetApp recommends that you refer to the following guides before using this guide:

- SnapDrive 7.0 for Windows Installation and Administration Guide
- SnapDrive 7.0 for Windows Release Notes
- NetApp Interoperability Matrix Tool
- Data ONTAP 8.2 System Administration Guide
- SAN Administration Guide
- Host Utilities Installation and Setup Guide

A good understanding of Windows file system administration is necessary, as well as an understanding of FCP and iSCSI concepts.

2 Installation and Basic Configuration

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 file system–consistent storage provisioning, application-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 integrates seamlessly with the clustering technology supported by the host operating system.

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 with NetApp Snapshot to create point-in-time images of data stored in LUNs
- Works 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® Windows failover cluster configurations

- Simplifies iSCSI session management
- Enhances management of pass-through disks with Microsoft Hyper-V™ virtual machines and raw devices and VMDKs when used in a VMware® environment
- Supports LUN migration with VMware VMotion®, SRM, and DRS functionalities
- Supports ESXi™ 5.1 five-node, out-of-the-box FC cluster
- Supports group managed service accounts in Windows Server 2012
- Supports Virtual Fibre Channel in Windows Server 2012

2.1 Best Practices for SnapDrive Preinstallation

SnapDrive for Windows can be used either as a standalone product or as part of other NetApp solutions. For example, it can be deployed along with SnapManager® for Exchange, Microsoft SQL Server®, and SharePoint®. In both these deployments, SnapDrive for Windows serves as a tool to create and manage storage. It also creates backups and restores the storage from those backups using Snapshot. SnapDrive for Windows integrates with Windows Logical Disk Manager and Microsoft's VSS framework and works in clustering and multipathing deployments using FCP and iSCSI transport protocols.

For supported platforms, refer to the NetApp Interoperability Matrix Tool.

2.2 Best Practices for Storage System Setup

For proper functionality with SnapDrive for Windows, make sure 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 SnapDrive 7.0 for Windows documentation.

Table 1) Storage system checklist.

Step	Action
1	Verify the license on the storage system. Use the `license` command on the command-line interface (CLI), the FilerView® tool, or System Manager to verify installed licenses: • FCP, iSCSI, CIFS, 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 using the following commands on the storage system CLI: For FCP, run `fcp show adapter` For iSCSI, run `iscsi portal show`
4	Make sure the Fibre Channel port on the NetApp storage system is configured as target, using the `fcadmin config` command.

5	Enable, configure, and test RSH or SSH access on the storage systems for administrative access. NetApp recommends SSH because it is more secure.

2.3 Best Practices for SnapDrive Host Setup

Before using or installing SnapDrive for Windows, make sure 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.

Verify the following

- Confirm that SnapDrive for Windows supports your environment. For specific information on requirements, see:
  - SnapDrive 7.0 for Windows Installation and Administration Guide
  - Fibre Channel and iSCSI Configuration Guide for Data ONTAP

  Note: NetApp recommends installing the latest Data ONTAP DSM before installing SnapDrive.
- Make sure that .NET 3.5 SP1 and .NET 4.0 is installed on the host system
- If using multipathing, make sure that Data ONTAP DSM 4.0.1 is installed on the system. Another option is to install the latest supported Microsoft DSM.
- Make sure that Windows PowerShell® 2.0 or later is installed on the host.
- Perform all procedures from the system console and not from a terminal service client.

Once the preceding checklist has been verified, follow the steps in the SnapDrive 7.0 for Windows Installation and Administration Guide to install SnapDrive for Windows.

- Refer to the SnapDrive 7.0 for Windows Release Notes for the latest fixes, known issues, and documentation correction.

2.4 Best Practices for SnapDrive Services

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

The SnapDrive services should be running for any SnapDrive for Windows command or API to work. This section lists the services available in the SnapDrive for Windows installation.

Table 2) SnapDrive 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 using CLI or GUI	C:\Program Files\NetApp\SnapDrive\SDMgmtSvc.exe
SnapDrive Storage Management Service	Manages the SMB 3.0 workflows	C:\Program Files\NetApp\SnapDrive\SnapDriveservice.exe

The path to the SnapDrive executables is determined by the drive letter used when installing SnapDrive for Windows.

- Virtualized environments with large numbers of virtual machines might experience slow SnapDrive service startup times.
- Check the SnapDrive dependencies and system event logs to see if other services are causing SnapDrive to start more slowly.
- Verify that no dynamic disk or offline disk exists in disk management.

2.5 Best Practices for SnapDrive FCP Environment

- Check the SnapDrive for Windows supported HBA and Host Utility version from the NetApp Interoperability Matrix Tool.
- Download and install the appropriate version from the NetApp Support site and see the Host Utilities Installation and Setup Guide to install (or upgrade) and configure Host Utilities.
- Physical nodes require the Host Utility kit, and virtualized nodes within ESX®, Hyper-V™, and so on do not require the Host Utility Kit.
- Identify the HBA adapters on the host and verify that the ports are enabled:
  C:\Program Files\NetApp\Windows Host Utilities
- If the user is using Data ONTAP DSM 4.0.1, the Windows Host Utilities do not need to be installed separately.

2.6 Best Practices for SnapDrive iSCSI Environment

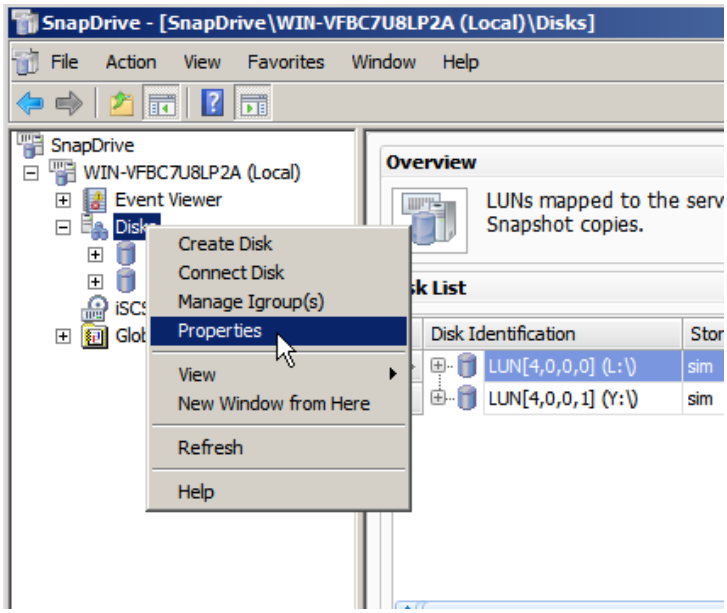
- Check the SnapDrive for Windows supported HBA and Host Utility version from the NetApp Interoperability Matrix Tool.
- Download and install the appropriate version from the NetApp Support site and see the Host Utilities Installation and Setup Guide to install (or upgrade) and configure Host Utilities.
- Identify the iSCSI initiator running on the Windows host:
  C:\Program Files\NetApp\Windows Host Utilities
- If the user is using Data ONTAP DSM 4.0.1, installing Windows Host Utilities separately is not required.

2.7 Best Practices for SnapDrive Preferred Storage System IP Address

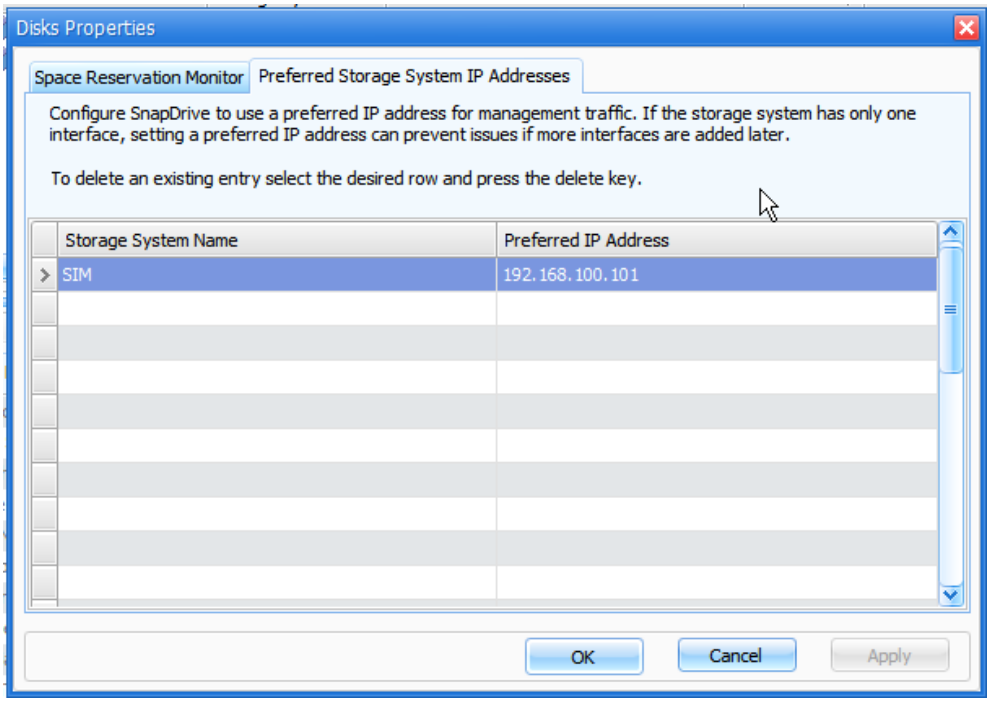
The preferred storage system IP address setting allows users to select the specific IP address used for management traffic to and from the storage array and is required with the addition of proper DNS resolution. Always set the preferred IP address to the management port of the NetApp storage array. This is important regardless of whether you use the FCP or iSCSI protocol, since this communication is vital to the proper functioning and performance of SnapDrive for Windows.

From the host with SnapDrive installation:

1. Open Microsoft Management Console (MMC).
2. Select SnapDrive host.
3. Right-click Disks and select Properties.



4. Enter the storage array host name and IP address used for management traffic.



Note: Certain security policies set on the Windows host or domain might cause SnapDrive service startup issues and errors.

For more information on authentication requirements, refer to the section “Configuring Access for SnapDrive” in the SnapDrive 7.0 for Windows Installation and Administration Guide.

2.8 Best Practices for Disabling iSCSI Interfaces

By default, an IP interface on the storage system accepts iSCSI commands. So 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
```

Caution

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

2.9 Best Practices for Troubleshooting SnapDrive Issues

Issues with SnapDrive for Windows installations and connectivity can cause problems with basic functions of SnapDrive and with the performance of functions within SnapDrive. Use the following steps for the proper configuration of SnapDrive for Windows.

Table 3) Basic troubleshooting.

Step	Action
1	Verify that your configuration is supported by referring to the NetApp Interoperability Matrix Tool.
2	Using the “transport protocol settings” use http or https protocol to connect to the storage system.
3	Make sure 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 might interfere with connectivity or installation. From the host, click: Local Security Policies > Security Settings > Local Policies > User Rights Assignments.
5	Check Windows Firewall on the local node and all other nodes if in a cluster configuration. • Enable SnapDrive to communicate through the firewall. For specific details, see SnapDrive 7.0 for Windows Installation and Administration Guide or Disable firewall (not recommended for security reasons).
6	User credentials during installation should be in the domainname\username format.
7	Check the network connectivity and DNS resolution from the host to the storage system: `ping <storage_system_IPaddress >; ping <storage_system_name>`

2.10 Best Practices for SnapDrive Diagnostics and Log Collection

In certain cases, troubleshooting will require advanced diagnostics and log collection to help administrators and might also be requested by NetApp Global Support. The following tools located in the Utility ToolChest are used to collect diagnostics and logs to assist in troubleshooting.

- nSANity Tool for diagnostics and log collection

  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 Utility ToolChest site.

- ONTAPWinDC tool for log collection

  The Data Collection Tool (ONTAPWinDC.exe) creates a report of the SnapDrive and SnapManager host-side information and hosting storage system values that is used by NetApp Global Support for troubleshooting and problem analysis. It runs on all Windows platforms running SnapDrive and SnapManager products. You can download this program from Data Collection Tool for SnapDrive for Windows (ONTAPWinDC.exe).

3 SnapDrive Security and Access Control

SnapDrive for Windows allows administrators to utilize a number of tools to harden their security for their environment. SnapDrive allows you to use HTTP or HTTPS in addition to the default RPC protocol for storage system communication. This feature, along with CIFS share dependency removal, means you are no longer required to have root access on the storage system for operations related to SnapDrive. There are various tools available to restrict or grant access to your storage systems.

3.1 Best Practices for SnapDrive Security and Access Control

The following documents discuss how to improve your security for SnapDrive:

- TR-3864: SnapDrive for Windows in a Least Privilege Environment
- TR-3558: Role-Based Access Control for Data ONTAP 7G
- Storage Access Control Tool for SnapDrive

3.2 Best Practices for SnapDrive Communication Protocol

Use HTTPS instead of HTTP for host-to-storage-system communication to provide added security. HTTPS allows all interactions with the storage system and host through the Data ONTAP interface, including securely sending the passwords. The `httpd.admin.enable` option must be set on the storage system in order for SnapDrive to use the HTTP or HTTPS protocol.

To use HTTPS:

1. Configure and enable HTTPS on the storage-system side.

```
SecureAdmin setup ssl
Options ssl.enable on
```

2. During SnapDrive installation, you will be prompted to configure the default transport protocol as RPC, HTTP, or HTTPS. In addition, transport protocols can be set after installation using one of the following methods.
3. Enter the following command:

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

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

   Note: HTTPS is not supported with MultiStore.

   Note: The RPC protocol is not supported if Group Managed Service Accounts are configured for SnapDrive.

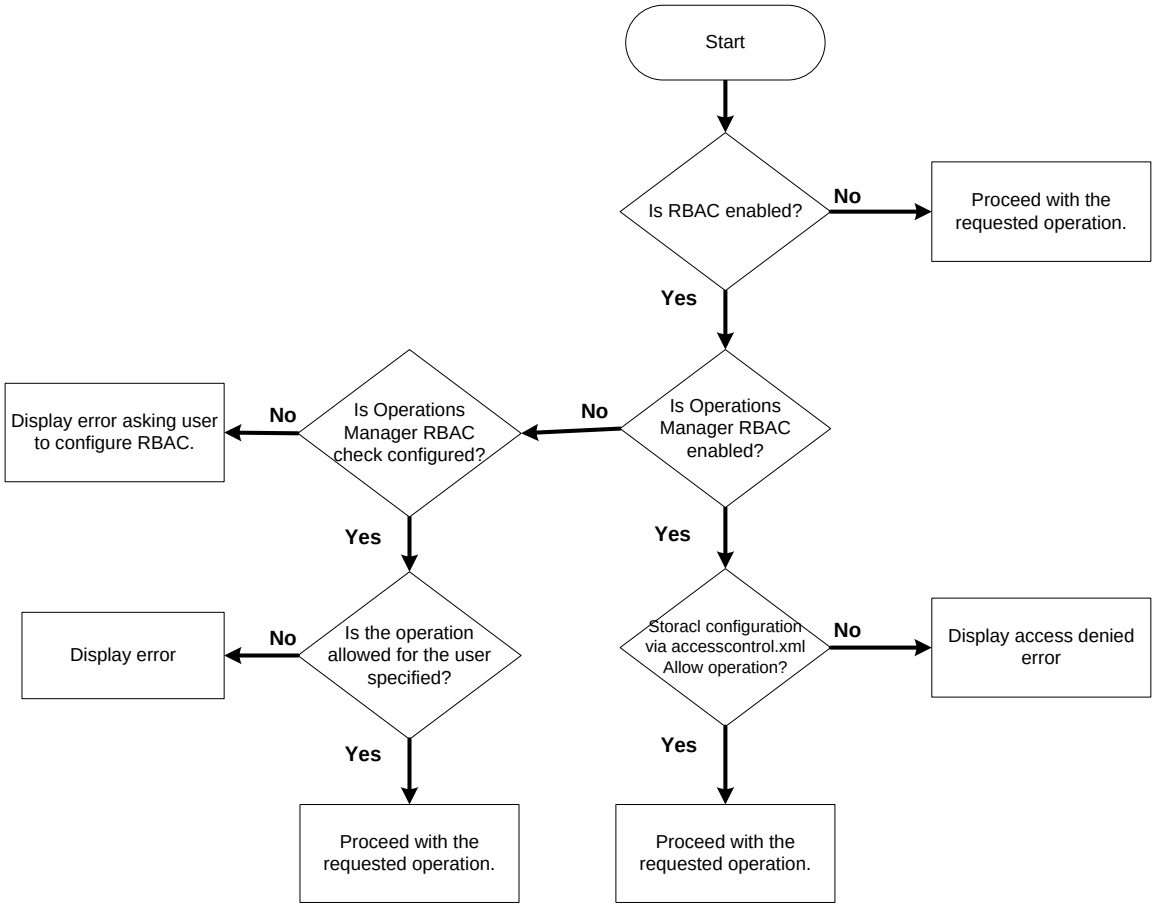
For more information on general security best practices, refer to TR-3649: Best Practices for Secure Configuration of Data ONTAP 7G.

3.3 Best Practices for Role-Based Access Control with OnCommand Unified Manager

NetApp recommends using OnCommand® Unified Manager for role-based access control (RBAC) because this provides administrators with granularity and simplicity in granting, denying, and managing access to NetApp storage arrays. RBAC is implemented using the NetApp OnCommand Unified Manager infrastructure. SnapDrive 7.0 for Windows conforms to the policies set on OnCommand Unified Manager. SnapDrive contacts OnCommand Unified 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 will produce an error message.

Figure 1 shows the flow of SnapDrive access control when RBAC has been configured with OnCommand Unified Manager and Storacl.

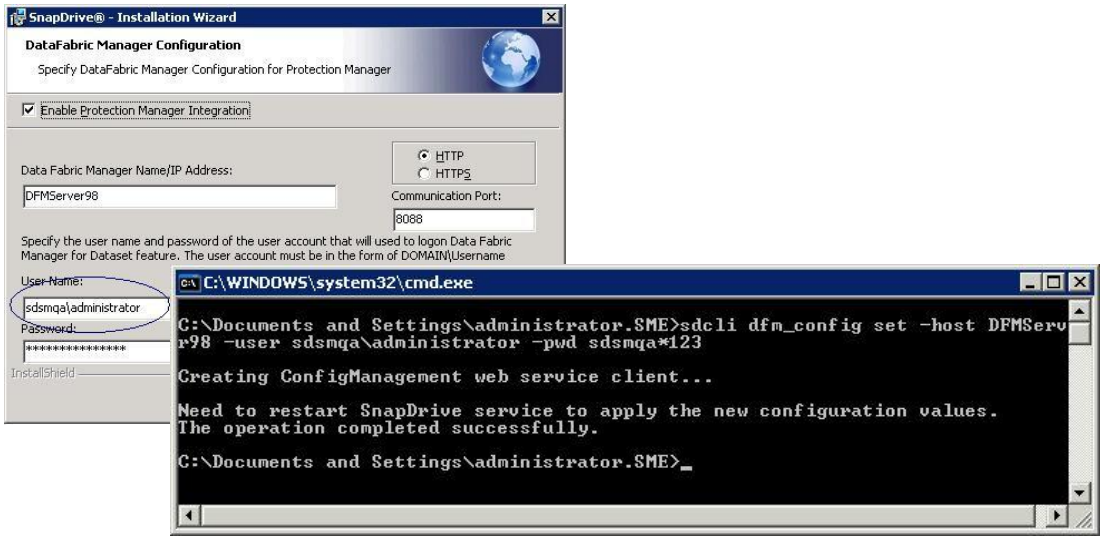
Figure 1) SnapDrive RBAC workflow.



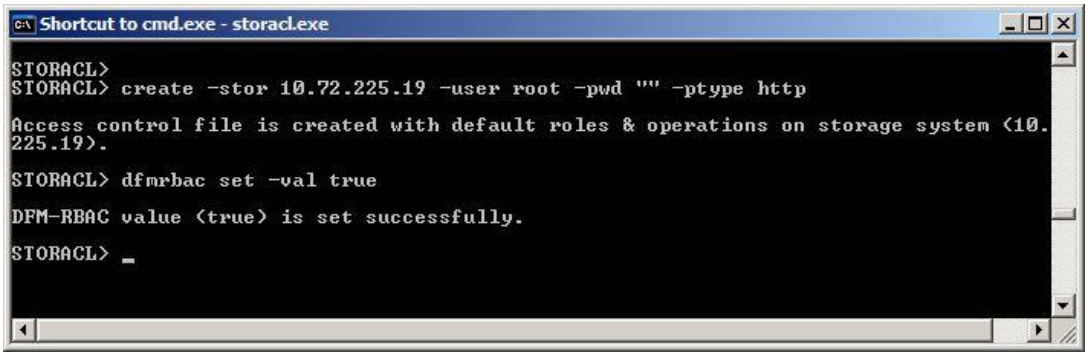
Configuring Role-Based Access Control with OnCommand Unified Manager

RBAC for SnapDrive can be enabled by using one of the following methods:

- RBAC can be enabled during the initial installation through the SnapDrive Installation Wizard.



- RBAC can be enabled using SDCLI if SnapDrive is already installed on the host.
- Enable DFM RBAC on the storage system with the Storacl tool located in the NetApp Support site Utility ToolChest.



Note: SnapDrive for Windows must be installed with the OnCommand Unified Manager server settings such as OM server name/IP address, username, and password.

The following steps need to be performed for configuring a SnapDrive for Windows RBAC user:

1. Select the SDW user who will be used for RBAC (for example, DOMAIN\username).

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

2. Perform the steps shown in Figure 2 through Figure 4.

Figure 2) Adding roles and capabilities from OnCommand Unified Manager.

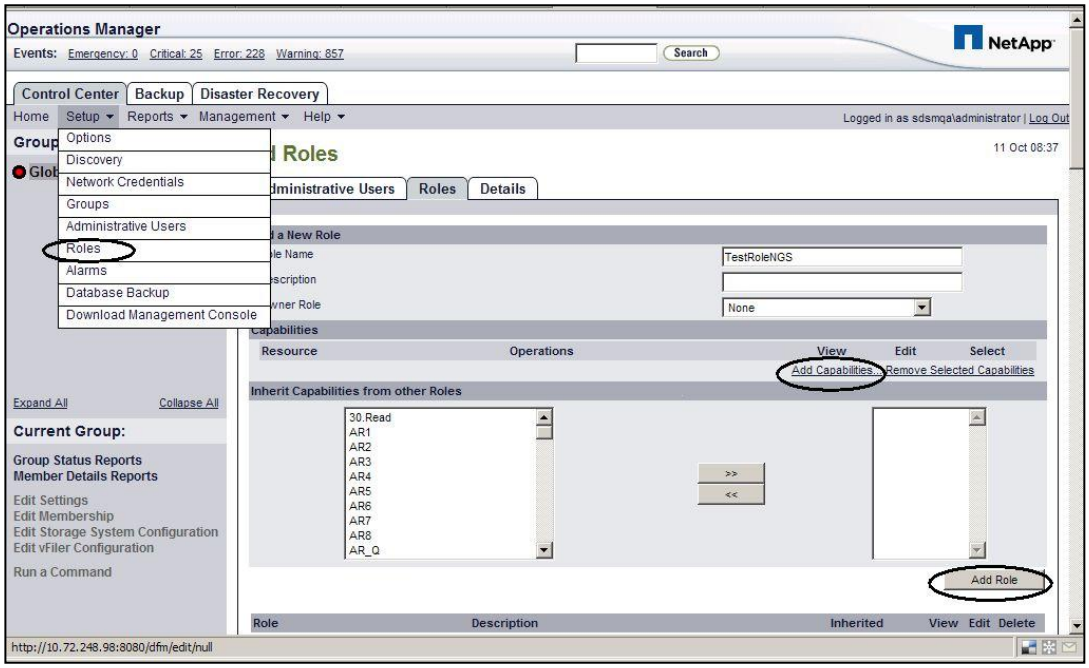


Figure 3) Available operations within OnCommand Unified Manager.

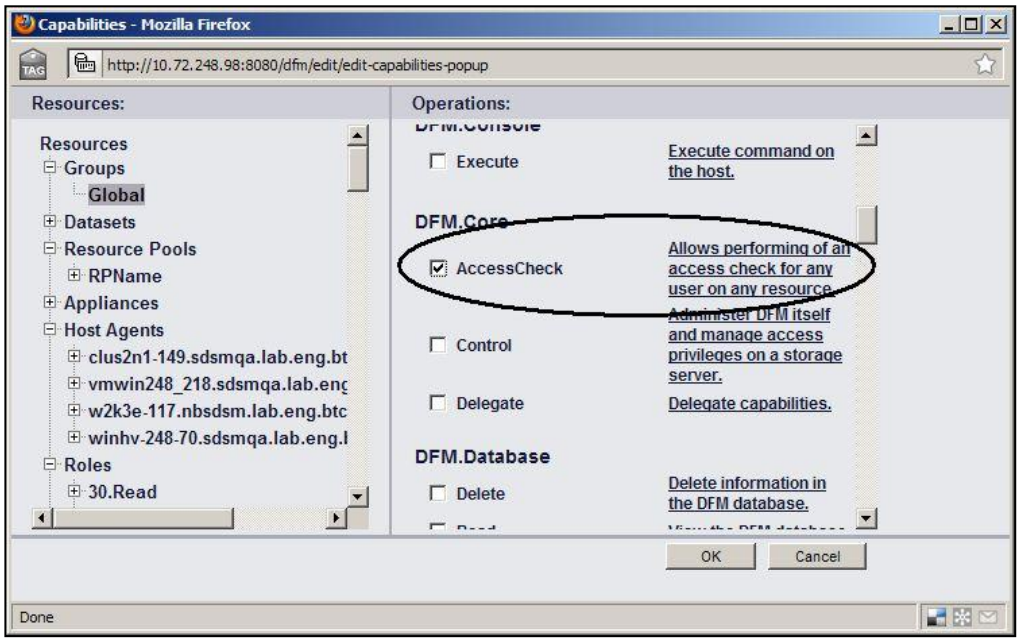
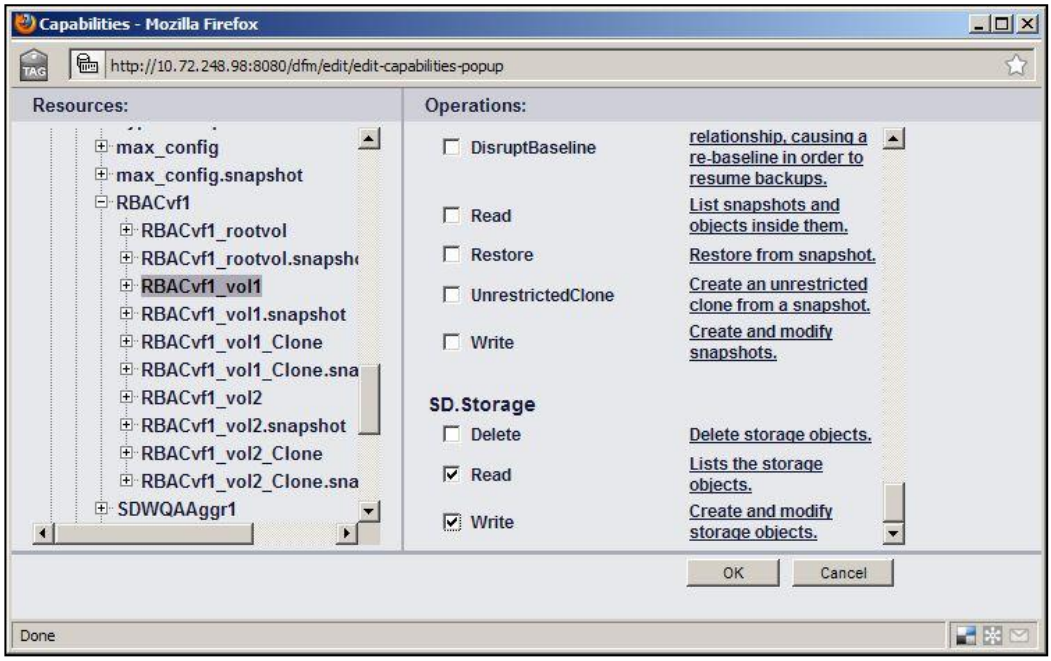


Figure 4) OnCommand Unified Manager resources and roles.



- The OnCommand Unified Manager administrator needs to grant capabilities to the invoker of SnapDrive to execute SnapDrive commands. For more information on the mapping between various capabilities compared to commands, see the SnapDrive 7.0 for Windows Installation and Administration Guide.

Preconfigured roles simplify the task of assigning roles to users. Table 4 lists the predefined roles on the OnCommand Unified Manager server.

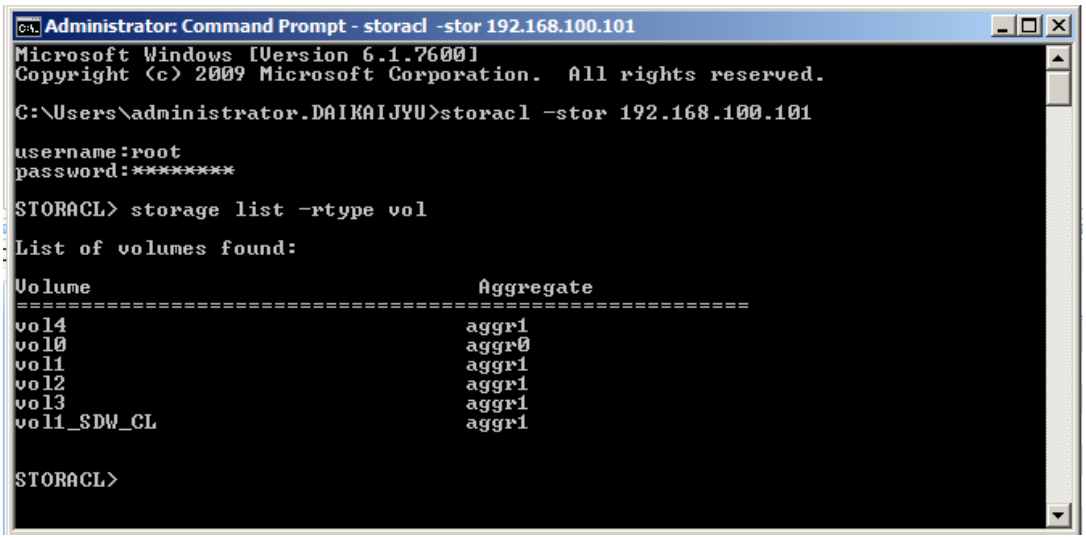
Table 4) OnCommand Unified Manager predefined roles.

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

3.4 Best Practices for Configuring Access Control Without OnCommand Unified Manager

Environments without NetApp OnCommand Unified Manager can utilize the Storacl tool to manually set and enable access control for SnapDrive. 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 of LUNs.

Figure 5) RBAC without OnCommand Unified Manager.



For more information on how to use the Storacl tool, refer to the Storage Access Control Tool for SnapDrive for Windows.

4 Storage Provisioning

SnapDrive for Windows allows administrators to create, delete, map, unmap, shrink, and grow LUNs in a storage system or connect to previously created LUNs that already exist on the storage system. If an administrator has to perform these tasks without SnapDrive for Windows, that administrator must manually log on to the storage system and perform the tasks. SnapDrive for Windows simplifies all these tasks by reducing the time for and the probable errors made during the manual process. While SnapDrive for Windows can create storage using a minimum of options, NetApp recommends that users understand the default values and use them appropriately.

4.1 Best Practices for Provisioning Storage with SnapDrive

Proper sizing is crucial to avoiding volume-full conditions that might adversely affect the environment. Properly sizing aggregates, volumes, and LUNs depends on various aspects of the environment. Use the following guidelines when planning for provisioning storage with SnapDrive:

- 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 also 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.
- Create 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 copy usage if Snapshot is enabled.

- Depending on the volume or snap reserve space available, use either the volume `auto grow` or `snap auto delete` option to avoid a volume-full condition due to poor storage sizing.
- If NetApp SnapVault is being used, NetApp recommends creating the LUNs within a qtree.

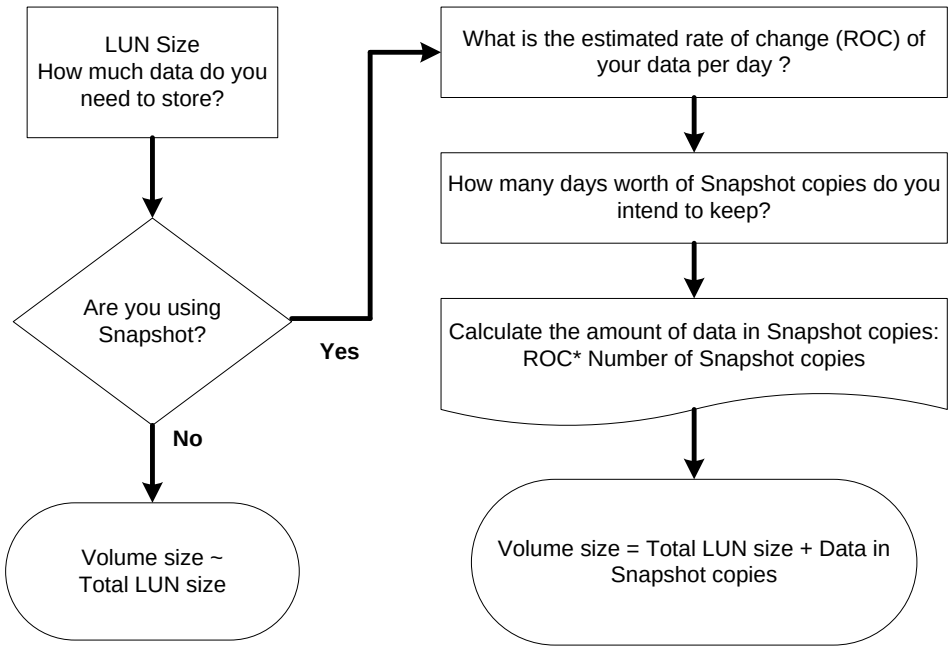
For more in-depth information about calculating the size of the storage system volume, refer to the SAN Configuration Guide or search the technical reports library for the application-specific documentation.

4.2 Best Practices for Volume and LUN Sizing

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

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

Figure 6) Volume and LUN sizing decision making.



Note: Some data protection mechanisms such as SnapMirror, rely on Snapshot copies.

General Rule of Thumb

- What is the LUN size? Do you plan to have multiple LUNs in a volume?
- Do you want to maintain Snapshot copies?
- If you want to maintain Snapshot copies, what is the number of Snapshot copies you want to maintain, and how long do you plan to retain them (retention period)?
- At what rate does data in the volume change (delta)?
- What amount of space do you need for overwrites to LUNs (fractional reserve)?

With these considerations, the general sizing best practice is to maintain (2xs LUN + delta) when sizing the volume space. For best practice guidelines for properly sizing environments with specific applications or thin provisioning, refer to the application-specific best practices guide and also the Block Access Management Guide for iSCSI and FC for your release of Data ONTAP.

4.3 Best Practices for Thin Provisioning

SnapDrive allows administrators to provision more storage than what is physically available (known as overprovisioning). Administrators can configure SAN-attached servers with LUNs large enough to meet customer needs and on the storage side can increase physical disk hardware as required, providing better storage investments.

Advantages of thin provisioning include:

- Less storage is required initially when buying a new storage system.
- More servers per storage system provide a greater level of consolidation.
- It allows overallocation of the application server's total disk capacity, thereby providing good ROI.
- Monitoring storage space is very critical in thin-provisioned environments; otherwise, available storage space might become exhausted, which would cause application downtime. One way of protecting this type of scenario is to use the snapshot autodelete and volume autogrow features. For more information on Snapshot autodelete and volume autogrow, refer to the Data ONTAP System Administration Guide.

Caution

NetApp recommends not enabling snapshot autodelete for volumes that are currently protected by other NetApp management applications such as System Manager, SnapManager for Hyper-V, and so on. Enabling snapshot autodelete on these volumes might disrupt the other protection mechanisms and cause issues with consistency.

The Storacl tool in conjunction with SnapDrive allows creating thin-provisioned LUNs on storage. The Storacl tool allows disabling LUN reservation. SnapDrive allows creating thin-provisioning LUNs with a maximum LUN size of 16TB. The Storacl tool can be downloaded from the ToolChest at the NetApp Support site, also included with SnapDrive 7.0 installation.

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:

```
"File is not found on the storage system." is returned if no policy has been set. Else, it will
return an output such as "Volume Path:volume_name Space reservation:false" or "Volume
Path:volume_name Space reservation:true" depending on whether the LUN space reservation is set to
disabled or enabled.
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 will create a file named "ThinProvision.xml" on the /etc folder of the storage system. SnapDrive will always check this file prior to creating a new LUN on a volume to determine whether LUN space reservation should be enabled for the new LUN.

For best practice guidelines in thin-provisioned environments, refer to TR-3483: Thin Provisioning in a NetApp SAN or IP SAN.

4.4 Best Practices for 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 on SnapDrive for Windows MultiStore support, refer to SnapDrive 7.0 for Windows Installation and Administration Guide.

5 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 the LUNs do not fail due to lack of disk space. Other operations, such as creating a Snapshot copy or new LUNs, can succeed only if there is enough available unreserved space.

5.1 Best Practices for Space Monitoring

Actively monitor data in the volume by using the `df -r` command from the storage console or use GUI-based tools so that overwrite reserve space is not exhausted.

For more 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.

For more information about NetApp System Manager, go to http://www.netapp.com/in/products/management-software/system-manager.html.

5.2 Best Practices for Fractional Reserve

- Use caution when changing the fractional reserve value to a value less than 100%, because, when space is fully consumed, the write operations will fail and disrupt 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 estimation 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.
- Use `snapshot autodelete` and/or `volume autosize` when setting fractional reservation to a value less than 100%.

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

5.3 Best Practices for Using Space Reclaimer

Space Reclaimer is a SnapDrive for Windows feature that optimizes LUN space by marking newly freed space that is visible to NTFS so it is also seen as available by Data ONTAP. When files are deleted or modified on a LUN, the space is tracked by NTFS. However, since this information is not communicated to the Data ONTAP file system, a disparity can grow between the available space reported by a

SnapDrive host and a storage system. Space Reclaimer verifies that newly freed blocks are marked as available on the storage system.

- Since the space reclamation process is CPU intensive, run Space Reclaimer when storage system and Windows host usage is low, for instance, at night.
- Do not run disk defragmentation when Space Reclaimer is running. This can slow the disk reclamation process.
- Space reclamation is a time-consuming operation; therefore, it is best to run Space Reclaimer on your NTFS volume when there is a large amount of unused deleted space.
- For optimum storage performance, run Space Reclaimer as often as possible and until the entire NTFS file system has been scanned.
- In MSCS configurations, Space Reclaimer can be initiated from the owner node only.
- Although Space Reclaimer reclaims nearly all space from newly freed blocks, it does not reclaim 100% of the space.
- Use Space Reclaimer on traditional LUNs and on VMDK files attached as virtual disks using NFS datastores. Space reclamation on VMDK files over NFS datastores is not supported if VMware Snapshot copies are created for that VM.
- Before running space reclamation on CSV LUNs in Windows Server 2012, make sure that CSV LUNs are in redirected mode.

6 Snapshot Copy Management

SnapDrive for Windows integrates with NetApp Snapshot to make stored data reliable to host applications. The ability to create and manage Snapshot copies from the host makes SnapDrive for Windows attractive 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 more information about the commands used to perform these tasks, refer to the SnapDrive 7.0 for Windows Installation and Administration Guide.

SnapDrive for Windows Snapshot copies are widely used because they provide the following distinct advantages:

- Create application-consistent Snapshot copies (restorable copies).
- Provide faster restore time.
- Create backups of larger amounts of data more quickly.

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 the creation of Snapshot copies.

6.1 Best Practices for Snapshot Copy Management

SnapDrive Snapshot operations and 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 providing up to 255 online point-in-time images.

- Periodically check the Snapshot copies and delete the old Snapshot copies that might unnecessarily occupy space.

- Disable automatic Snapshot copy creation on the storage system for the volume on which the LUNs are created, set the Snapshot space reserve to 0 using the following commands on the storage system, and delete any existing Snapshot copies. Automatic Snapshot does not flush I/O on the host or put the applications on the host in a backup state, which can cause inconsistent Snapshot copies.

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

- Because users can create several Snapshot copies, NetApp recommends creating Snapshot copies in a manner that indicates their usage.

For more information on Snapshot management best practices, refer to the SnapDrive 7.0 for Windows Installation and Administration Guide.

6.2 Best Practices for File System–Consistent Snapshot Copies

Creating Snapshot copies in a SAN environment differs from doing so in a NAS environment in a 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 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 might 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
```

6.3 Best Practices for Application-Consistent Snapshot Copies

The following tools are tightly integrated with SnapDrive for Windows and the Windows application:

- SnapManager for Microsoft Exchange
- SnapManager for Microsoft SQL Server
- SnapManager for Microsoft SharePoint
- SnapManager for Microsoft Hyper-V

Utilize the various Windows application-specific tools to create application-consistent Snapshot copies.

Depending on the setup of the environment, administrators might choose to enable `snapshot autodelete`. Do not enable `snapshot autodelete` for volumes that are currently protected by any other NetApp management applications such as System Manager, SnapManager, and so on. Enabling `snapshot autodelete` on these volumes might disrupt the other protection mechanisms and cause issues with data consistency. For more information, see http://fieldportal.netapp.com.

In addition, you can refer to the NetApp Support site or the Technical Reports Library.

6.4 Best Practices for Snapshot Management with FlexClone

For Data ONTAP 8.1.3 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 using the `LUN clone split status` command before initiating SnapRestore operations from SnapDrive.

SnapDrive for Windows also allows administrators to connect to Snapshot copies. This capability permits administrators to connect to various replicated copies of existing data.

Here are a few example scenarios in which you might use the cloning feature:

- When there is an available update for the application running on the storage system LUNs to make sure that the update software satisfactorily runs 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 will use 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.

6.5 Best Practices for SnapReserve

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 SnapReserve area. By default, after the SnapReserve area is filled, the Snapshot copies start to take space from the general volume. Because of WAFL® technology, SnapReserve does not reserve specific physical blocks; rather, it is a logical space-accounting mechanism. For more information on SnapReserve, refer to the SAN Administration Guide.

NetApp recommends setting SnapReserve to 0 for SAN environments because it simplifies space management, allowing maximum usable volume space by either the LUNs or the Snapshot copies within the volume. There is no need to keep SnapReserve to the default value of 20% because user writes are already limited by the LUN size.

6.6 Best Practices for Restoring a Snapshot Copy

SnapDrive for Windows 7.0 includes the following methods for restoring a Snapshot copy:

- Rapid LUN restore (LUN clone split)
- Volume-based Snapshot copy restore
- File-level restore (FLR)

SnapDrive for Windows utilizes the LUN-clone-split method of LUN restore in the graphical user interface (GUI). Both volume-based Snapshot restores and the file-level restore methods are only available using the SnapDrive command-line utility (sdcil.exe).

- SnapDrive guarantees data consistency of files restored from consistent Snapshot copies. However, application consistency is outside the function of SnapDrive for Windows. Files restored using file-level restore operations might 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, then it is a best practice to replicate those Snapshot copies to a secondary storage system using SnapVault and then perform the file-based SnapRestore operation.

6.7 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 <Snapshot Name> -files <filepath>[...] }+ }
```

Where:

- `MachineName`: Optional. If not provided will use local machine.
- `Snapshot Name`: Name of the backup Snapshot copy from which to restore.
- `-flr`: Selects file-level restore.
- `-copy`: Optional. This is the option to force copy-restore.
- `-files`: indicates the filepath arguments are files to restore.
- `Filepath`: List of "destination" filepath, including the mount point details snapname snap_name [-force [-noprompt]] [{-reserve | -noreserve}] [-vbsr [preview|execute]].

Example:

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

For more information on Snapshot management, refer to the SnapDrive 7.0 for Windows Installation and Administration Guide

7 Data Protection

NetApp tools such as SnapRestore, SnapMirror, SnapVault, SyncMirror®, and MetroCluster™ technology, SnapManager, Protection Manager, and OnCommand Unified 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 more information on the specific data protection best practices, refer to the NetApp Support site or the technical reports library. The following references also provide in-depth knowledge of data protection using SnapDrive:

- TR-3667: SnapVault Disk-to-Disk Backup on Windows Environment
- TR-3441: iSCSI Multipathing Possibilities on Windows with Data ONTAP

7.1 Best Practices for SnapMirror Sync

NetApp SnapMirror combines disaster recovery and data distribution in a streamlined solution that supports today's global enterprises. SnapMirror is a cost-effective data replication solution that provides efficient storage and additional value by enabling you to put the DR site to active business use.

The following describes the functionality between SnapMirror and SnapDrive for Windows.

If using synchronous SnapMirror, when you connect to a LUN at the destination SnapMirror site using SnapDrive for Windows, if the sync is healthy with no reports of lag and updates are current, SnapDrive for Windows will connect to the current active file system regardless of the destination Snapshot copy.

If synchronous SnapMirror is unhealthy or the destination is not current with the source:

- SnapMirror will fail back to the asynchronous-type functionality and will connect to the last consistent Snapshot copy.
- If no Snapshot copies exist, the SnapDrive for Windows connect operation will fail.

For more information about SnapMirror, see TR-3326: SnapMirror Sync and SnapMirror Semi-Sync Overview and Design Considerations.

7.2 Best Practices for Clustering

SnapDrive for Windows is available in both physical and virtual environments and integrates with Microsoft Cluster Server, Windows failover clustering, and VMware MSCS. For more information on how to set up clustering on the different platforms, go to the NetApp Support site or refer to the SnapDrive 7.0 for Windows Installation and Administration Guide.

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 must be able to communicate with all nodes and storage controllers involved in the cluster set.

In cluster environments, check that the IP address for the cluster resource has NetBIOS enabled.

7.3 Best Practices for NetApp SnapManager

SnapDrive for Windows enables users to create file system–consistent Snapshot copies on NetApp storage. SnapManager tools enable application-specific consistency and utilize SnapDrive for Windows for its underlying technology to create Snapshot copies on NetApp storage. This tight integration of both SnapDrive and application awareness has allowed SnapManager to become 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.

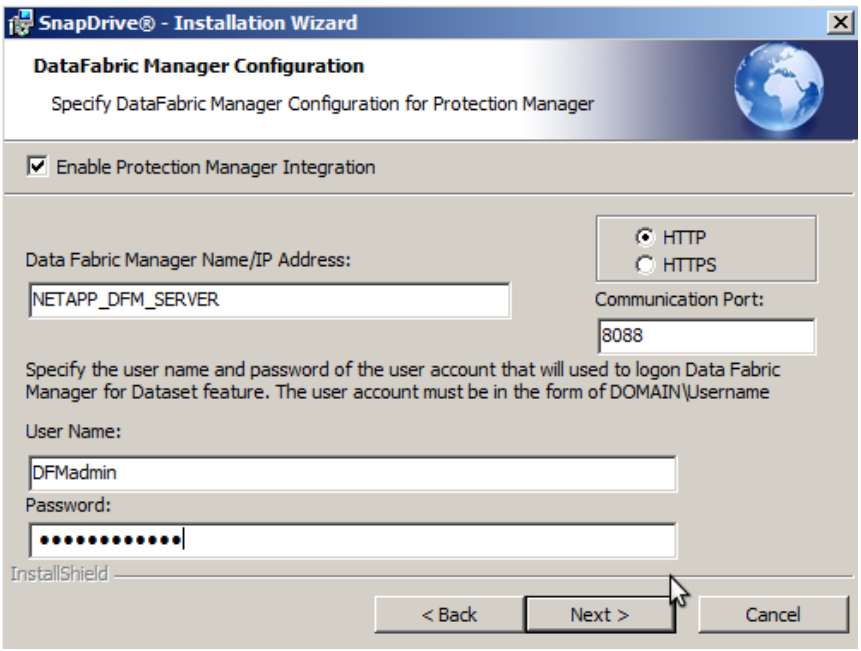
For more information on the specific application best practice and SnapManager, refer to the NetApp Support site or the technical reports library or Field Portal.

7.4 Best Practices for NetApp Protection Manager Integration

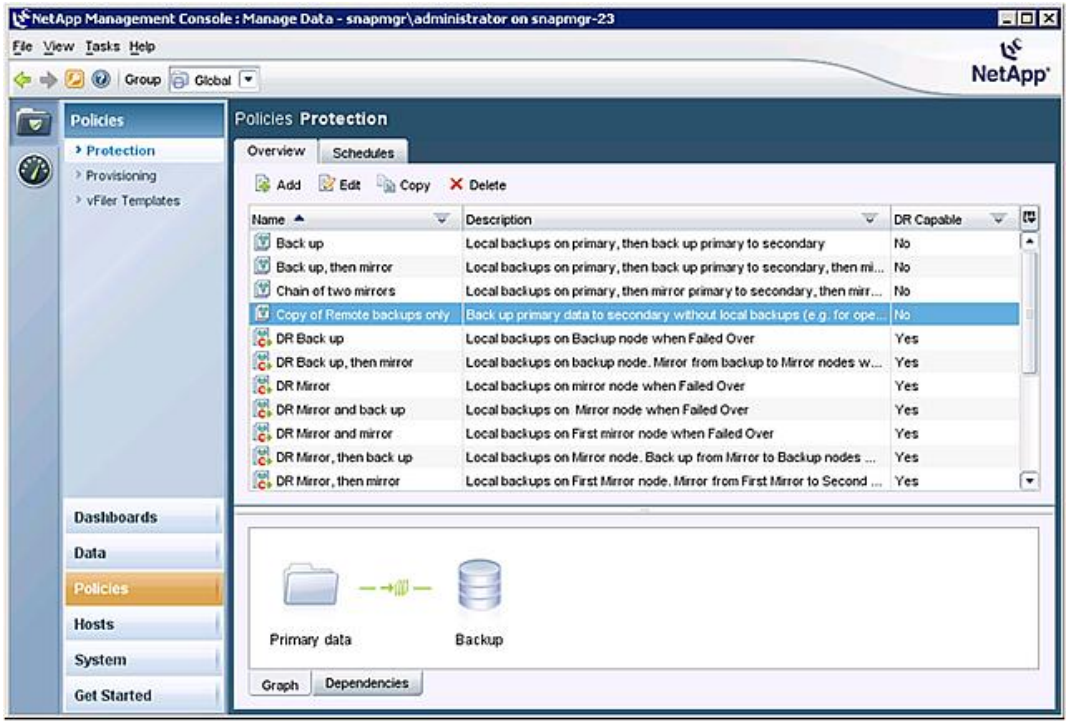
SnapDrive for Windows supports Protection Manager datasets through the SnapManager products. Protection Manager makes it easy to manage very large SnapMirror and SnapVault deployments by grouping data and storage systems into datasets and resource pools, enabling automation of many routine data protection tasks. You can configure SnapDrive with a set of DataFabric® Manager (DFM) credentials so that it can authenticate to a DFM server. This allows SnapManager to use SnapDrive as a conduit to support Protection Manager retention policies and schedules.

The following steps describe how to integrate SnapDrive, SnapManager, and Protection Manager with the assumption that Protection Manager, SnapManager, and SnapDrive are already installed in the environment.

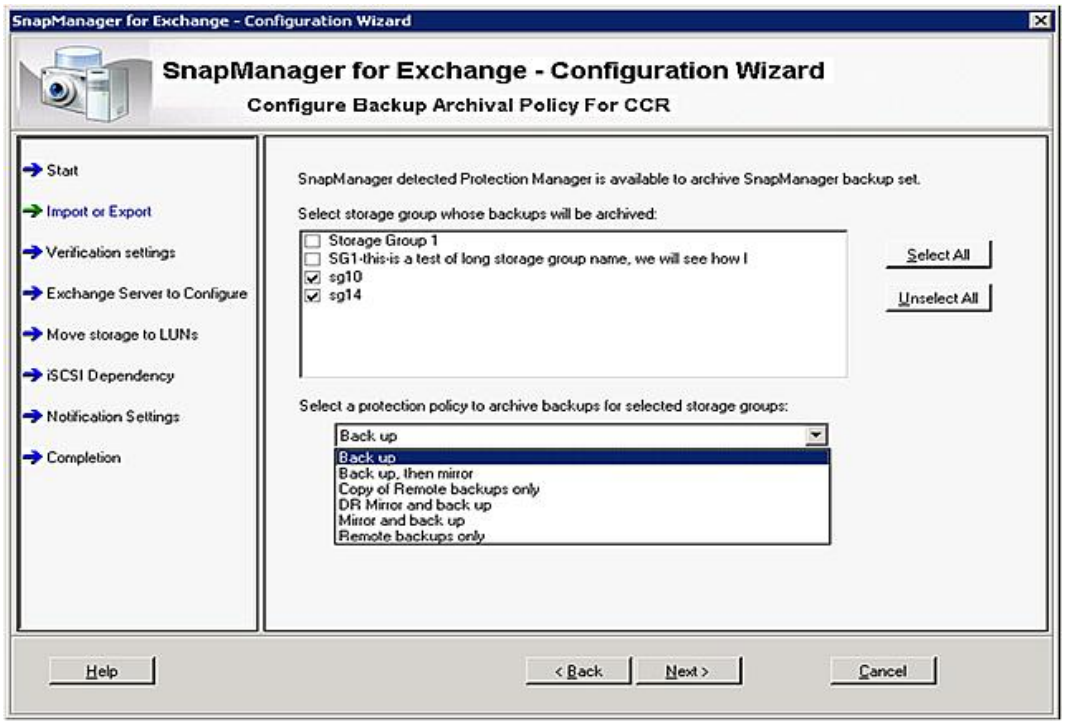
1. Enable Protection Manager integration with the SnapDrive installer.



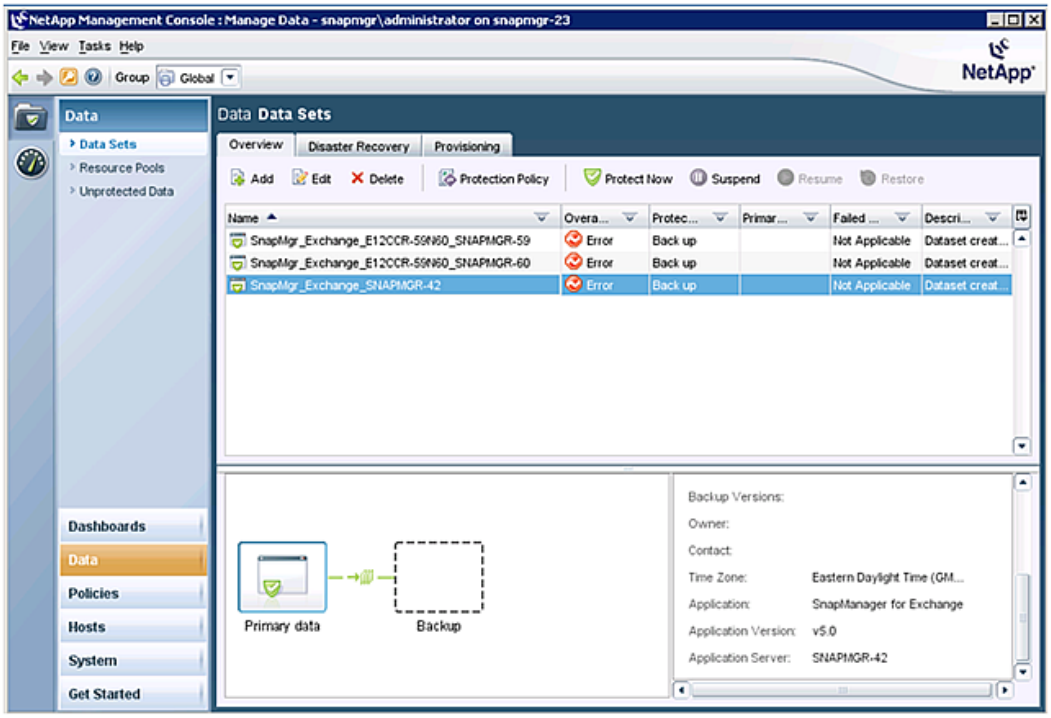
2. Create or modify a new data protection policy within Protection Manager.



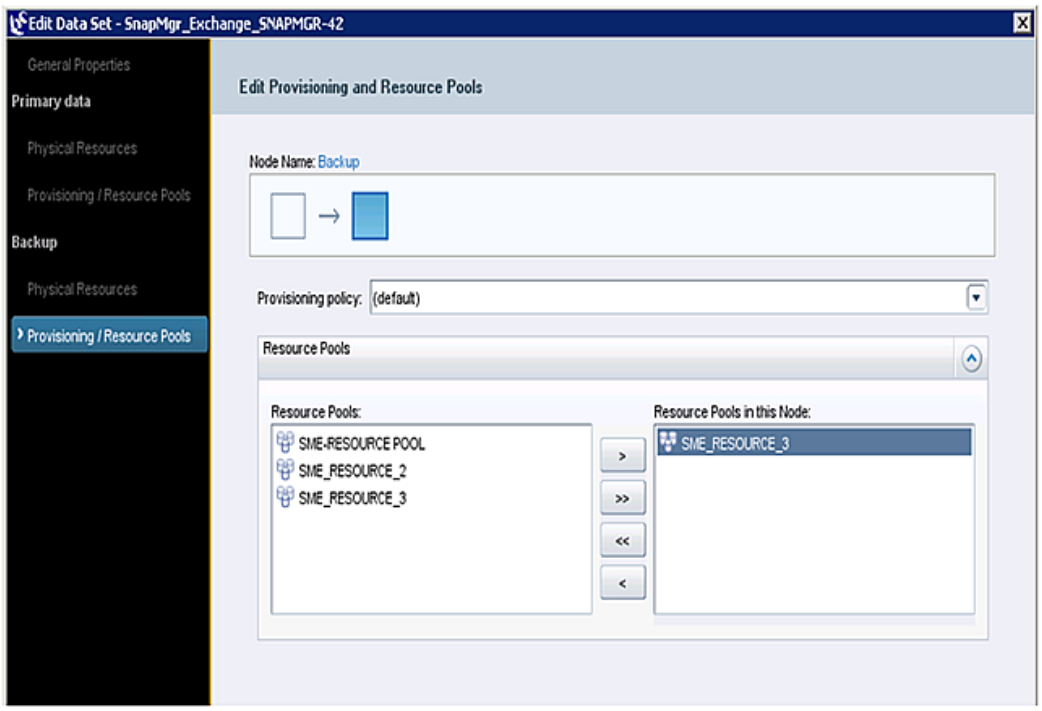
3. Select the data protection policy from within SnapManager.



4. Select the new dataset created, which will be shown as “out of conformance,” and assign the physical resources from Protection Manager.



5. Assign the resource pool for the dataset, which will then automatically create backup relationships, run schedules, and configure any additional secondary storage objects.



The SnapManager data is now protected.

For more information on Protection Manager and OnCommand Unified Manager, refer to the following documentation or review the application-specific SnapManager best practice guides (section 7.4):

- How to Configure SnapManager and SnapDrive Integration with DataFabric Manager
- DataFabric Manager Information Library, including OnCommand Unified Manager, Provisioning Manager, and Protection Manager
- TR-3710: OnCommand Unified Manager, Provisioning Manager, and Protection Manager Best Practices Guide

7.5 Best Practices for SnapVault Integration

Several SnapVault requests can be scripted as a batch file and initiated on the host. NetApp recommends that the user initiate not more than 10 SnapVault requests from SnapDrive at a time.

8 Virtualized Environments

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

8.1 Best Practices for Hyper-V Environments

SnapDrive supports the Hyper-V feature introduced in Windows Server® 2008 R2 and Windows Server 2012 and enables users to provision LUNs to VMs and pass-through disks on a Hyper-V virtual machine without shutting down the virtual machine. A pass-through disk is a disk that is physically connected to a Hyper-V parent host and is assigned to a Hyper-V virtual machine as a SCSI hard disk for use by that virtual machine.

VHDs should only be created as fixed-type VHDs. NetApp recommends not using differential VHDs or dynamic VHDs since they cannot be aligned for both performance and deduplication. The drawback of using fixed VHDs is that, when creating the fixed VHD, the OS immediately consumes the entire space, and care must be taken that such a thin-provisioned LUN does not expand past its volume free space during the format process. Once the VHD has been formatted, you can run deduplication against the volume that contains that VHD, and all that space that has zeros written to it can be immediately reclaimed as savings.

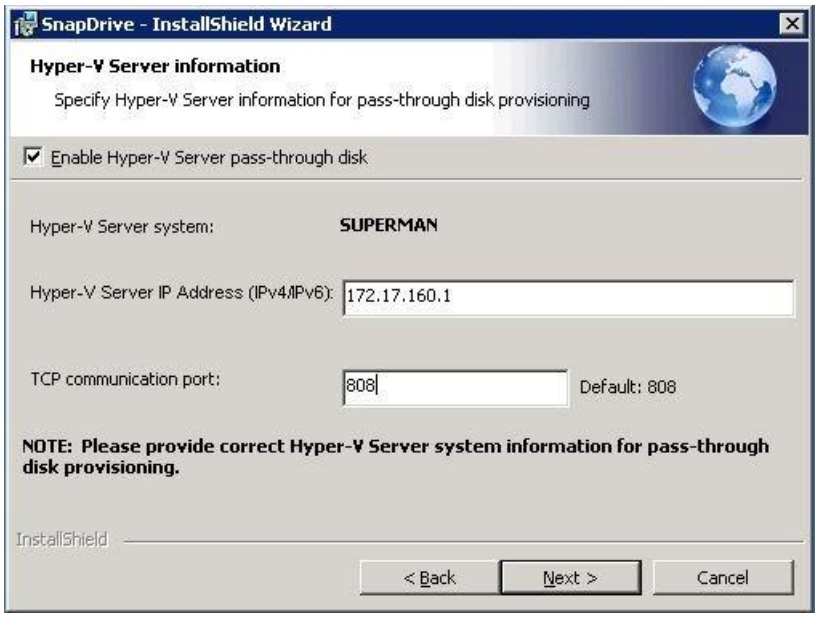
For best practices for VHDx files in a Windows Server 2012 environment, refer to section 9 “Windows Server 2012 Support.”

For best practices specific to Hyper-V, refer to TR-3702: NetApp Storage Best Practices for Microsoft Virtualization.

8.2 Best Practices for Enabling Pass-Through Disk Provisioning

The following steps enable Hyper-V pass-through disk provisioning, which is only available on Hyper-V VMs.

1. During the SnapDrive installer, the following wizard will be available only on Hyper-V VMs.
2. Select the Enable Hyper-V Server pass-through disk checkbox.
3. Fill in the Hyper-V server information. Click Next and follow the instructions on screen.



4. In the command-line prompt, enter the `sdcli hyperv_config` command to review, modify, or add Hyper-V server configurations.

   For example:

```
C:\>sdcli hyperv_config
```

   The `hyperv_config` command performs operations related to SnapDrive in the Hyper-V parent configuration. The following operations are available:

```
list  set   delete
```

   For example, to set Hyper-V parent node configuration:

```
C:\>sdcli hyperv_config help set
```

```
sdcli hyperv_config set -host <Host> -IP <IP Address> [-port <Port>]
```

Where:

`-host`: Hyper-V parent node host name.

`-IP`: Hyper-V parent node IP address.

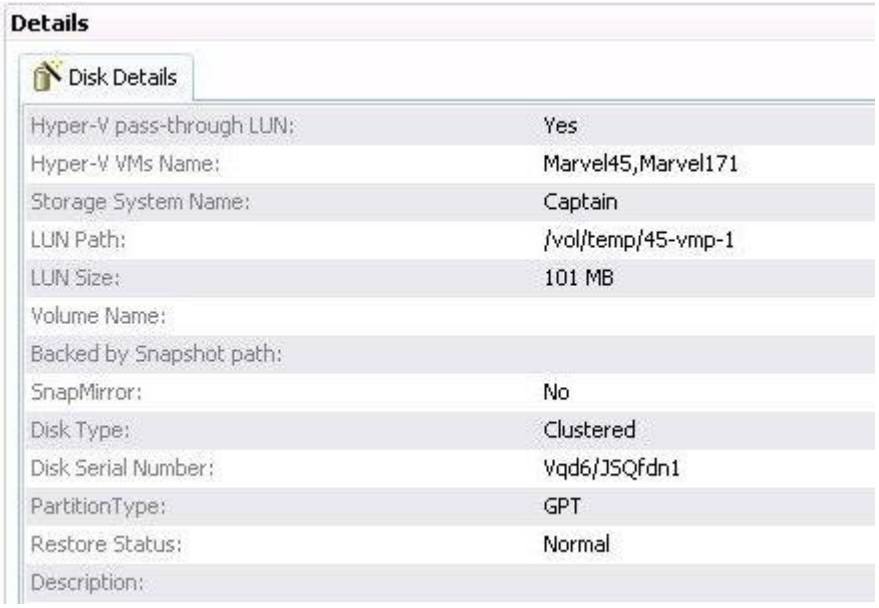
`-port`: Hyper-V parent node SnapDrive Web service TCP port number. Default 808.

8.3 Best Practices for Managing Hyper-V Pass-Through Disks

Management of large environments and multiple pass-through disks can become difficult. Monitor LUNs from the Hyper-V parent to quickly review information of VM-connected LUNs.

Figure 7 shows the details of a LUN displayed from the parent Hyper-V node.

Figure 7) Hyper-V parent pass-through disk.



For more information on the various best practices available in virtualized environments, refer to the NetApp Support site or search the Technical Reports Library for the specific application.

8.4 Best Practices for VMware Environments

SnapDrive for Windows provides LUN provisioning and file system–consistent backups and recovery leveraging NetApp storage array Snapshot copies for VMs hosted in a VMware vSphere® environment.

With VMware ESX, SnapDrive for Windows supports LUN provisioning and Snapshot copy operations in VMDKs in NFS datastores for use by SnapManager for Microsoft SQL Server when you use SnapDrive along with SnapManager for Virtual Infrastructure.

Note: Always use SnapDrive or SnapManager for specific applications to create consistent Snapshot copies of RDMs.

The following is a list of best practices for SnapDrive for Windows when installed on the guest VMs in VMware environments.

Best Practices

1. Install Virtual Storage Console 4.2 (VSC) on the VMware vCenter™ Server.
2. Install VMware tools prior to SnapDrive installation on the guest VM.
3. Disable VSS in the VMware tools of the VM where SnapDrive will be installed.
4. Disable the "sync driver" (in the VMware tools) in all VMs.
5. Set up VMware permissions for SnapDrive guest installation (see section 8.5, “Best Practices for VMware and SnapDrive Permissions”).

8.5 Best Practices for VMware and SnapDrive Permissions

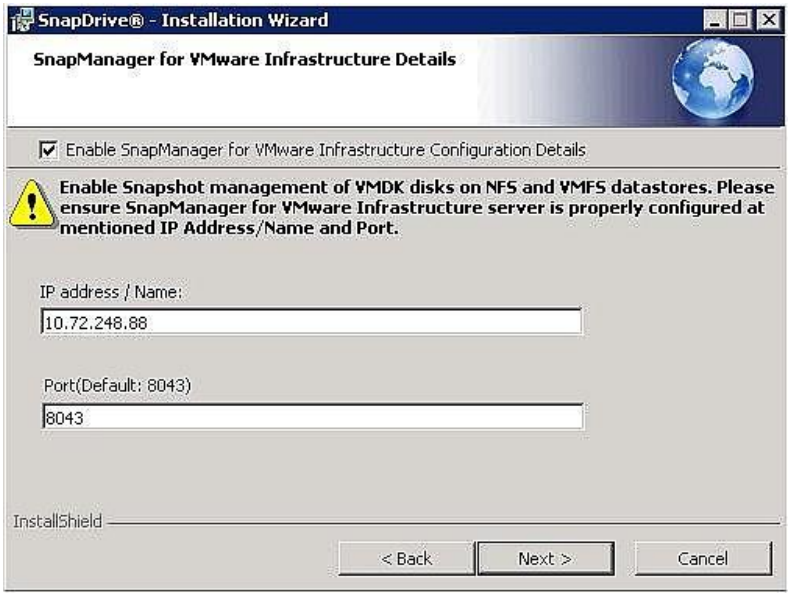
To provide additional security to the account used by SnapDrive in the guest OS, first create an account in Active Directory®. This account does not need to be in the domain administrator group or in any local administrator group. Then, create a new administrative role in the VMware vCenter server or servers at both the protected and recovery sites. Assign the following four rights to the new role and assign the role to the new user:

- Datastore > Remove File.
- Host > Configuration > Storage Partition Configuration. Required for performing operations such as `RescanAllHBA` on the ESX server.
- Virtual Machine > Configuration > Raw Device. Required for adding and deleting RDM disks.
- Virtual Machine > Configuration > Change Resource. Required intermediately when resources assigned to a VM change during disk operations.

8.6 Best Practices for VSC and SnapDrive Integration

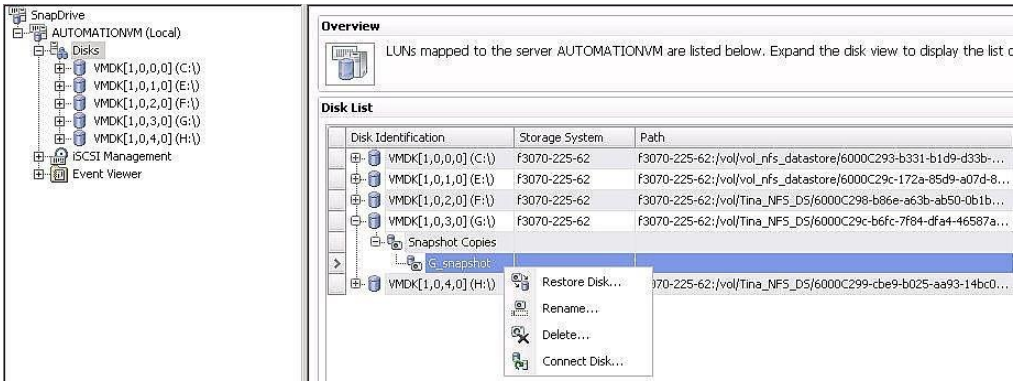
After the VMware environment is configured, you can proceed to integrate SnapDrive with the VMware environment.

1. Set up VMware infrastructure information during SnapDrive installation.



2. If SnapDrive is already installed, SDCLI can be used to set the VMware infrastructure information.

3. Once setup is complete, SnapDrive will display the VMDK information.



8.7 Best Practices for VMware SRM

The SnapDrive CLI interface, SDCLI, can be used to set or change the vCenter server setting. With the help of some environment variables provided by SRM, a command can be constructed that can be executed by SRM to make the change.

SRM command steps are executed on the SRM host. Therefore, when using SRM command steps, if the action taken must happen within the VM guest OS, then a process capable of sending commands remotely must be used. SDCLI has this capability.

Requirements for using SDCLI in SRM command steps:

- SRM command steps are executed on the SRM host; therefore, the SnapDrive management software must be installed on the SRM server.
- The service account that runs the VMware SRM service on the SRM server must be set to an authenticated account that has access to run the SDCLI command. Note that by default the SRM service runs as a local system, which has no access to the network for executing the SDCLI command.
- Not a requirement but definitely an advantage is to use domain-based accounts, which are valid at both the protected and recovery sites as the accounts used by SnapDrive for communication with the NetApp FAS arrays and the VMware vCenter server.
- If using SnapDrive for Windows version 6.4 or above, the `-user` and `-pwd` options are not required for the SDCLI command described later, assuming that the credentials used by SnapDrive do not need to be changed at the SRM recovery site.

For more information on SRM and SnapDrive automation, see KB: How to Automate SnapDrive for Windows Reconfiguration with VMware SRM.

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

- TR-3785: Running Microsoft Enterprise Applications on VMware vSphere, NetApp Unified Storage, and Cisco Unified Fabric
- TR-3822: Disaster Recovery of Microsoft Exchange, SQL Server, and SharePoint Server Using VMware vCenter Site Recovery Manager, NetApp SnapManager and SnapMirror, and Cisco Nexus Unified Fabric
- TR-3749: NetApp Storage Best Practices for VMware vSphere
- TR-3428: NetApp and VMware Virtual Infrastructure 3 Storage Best Practice
- TR-3737: SnapManager 2.0 for Virtual Infrastructure Best Practices Guide
- TR-3747: Best Practices for File System Alignment in Virtual Environments

For more information on the various best practices available in virtualized environments, refer to the Support site or Technical Reports Library for the specific application or documents listed previously.

9 Windows Server 2012 Support

9.1 Introduction

SnapDrive for Windows supports Windows Server 2012. SnapDrive 7.0 for Windows is prerequisite software that is required for installation on Windows Server 2012 to manage NetApp storage systems. SnapDrive 7.0 for Windows will support managing only SAN environments in Windows Server 2012.

Note: SnapDrive 7.0 for Windows is a prerequisite for the SnapManager suite of products to function in Windows Server 2012 environments.

9.2 Feature Overview

SnapDrive 7.0 for Windows will support all major SAN-based features in Windows Server 2012.

Here is an overview of all the features and best practices to be followed.

CSV 2.0 Support (CSVFS)

Note: In Windows Server 2012, Cluster Shared Volumes (CSVs) have undergone significant changes with respect to security, performance, and file system availability for additional cluster workloads. A new Clustered File System has been introduced and this functions as a layer of abstraction above the NTFS file system for the storage volume. As a result, simultaneous reads/writes can be performed on the CSV LUN from different nodes. For more details on CSV 2.0, refer to http://technet.microsoft.com/en-us/library/jj612868.aspx. A CSV 2.0 volume will have two volume GUIDs.

a. NTFS Volume GUID - When a disk is created and partitioned with NTFS and before it is added to the CSV

b. CSV Volume GUID - When a disk is added to the Cluster Shared Volumes

SnapDrive 7.0 for Windows supports CSVFS. SnapDrive is designed to support both application-consistent and crash-consistent backups.

Best Practice

NetApp recommends, in SDW, creating a CSV from the node that owns the available cluster storage group. Use the "`CLUSTER GROUP`" command or "`Get-Cluster Group`" cmdlet to identify the node that owns "Available Storage" Group before creating a CSV disk.

9.3 Asymmetric Clustering

Asymmetric clustering is a feature with which users can create a shared disk or Cluster Shared Volume among only a few nodes in a cluster.

Note: SnapDrive does not support this feature.

9.4 BitLocker Encryption

BitLocker was a data protection feature and was part of Windows 7 and Windows 2008 R2. This feature is now available with Windows Server 2012 with the additional functionality. The user will now be able to encrypt Cluster Shared SAN Volumes. For more information on Bitlocker configuration, refer to http://technet.microsoft.com/en-us/library/hh831713.

SnapDrive for Windows will support BitLocker functionality for CSVs provisioned through it.

9.5 New Virtual Hard Disk Format

Windows Server 2012 has introduced a new virtual hard disk format, VHDx. Unlike the previous VHD format, this format supports up to a 64TB size. Also, the VHDx format has a 4kB logical sector size that increases performance of applications that are designed for 4kB sector sizes.

SnapDrive 7.0 for Windows supports this new format. The block allocation unit size of LUNs created by SnapDrive is 4kB. This complements the new VHDx format and there is no scope for VM misalignment.

Note: SnapDrive 7.0 for Windows currently cannot create LUNs beyond 16TB and, therefore, NetApp advises creating a VHDx for sizes less than 16TB and to use other means of provisioning additional storage (pass-through disks, guest i-SCSI initiator) on the VM.

9.6 Hyper-V Virtual Machine Live Migration

In Windows Server 2012, users can perform concurrent live migration of multiple VMs from one node to another.

Best Practice
It is best to avoid SnapDrive-related operations within the virtual machine during live migration.

9.7 Hyper-V VM Storage Live Migration

This feature in Windows Server 2012 enables migrating virtual machine–related files to a different storage location without the VM having to undergo downtime. SnapDrive 7.0 for Windows supports this feature, which simplifies change management. It is no longer necessary to take the virtual machine state offline when migrating to a different storage system. Please refer to the following link for more information on VM storage live migration.

Best Practice
It is best to avoid SnapDrive-related operations during storage live migration. Otherwise, such operations could corrupt the virtual machine.

9.8 Virtual Fibre Channel

Windows Server 2012 supports the provisioning of storage to guest virtual machine through virtual Fibre Channel. Also, features such as live migration and MPIO are supported. Virtual Fibre Channel requires an NPIV-enabled Fibre Channel HBA. At most, four Fibre Channel ports are supported. If the host system is configured with multiple FC ports and presented to the VM, then MPIO must be installed in the VM to enable multipathing. Also, pass-through disks cannot be provisioned to the host if MPIO is being used on the host. This is because pass-through disks do not support MPIO.

Best Practice

If you are using multiple FC initiators on the host, NetApp recommends installing Data ONTAP DSM in the guest virtual machines to enable multipathing in the guest.

SnapDrive supports provisioning of storage through virtual Fibre Channel using Windows Server 2008 R2 SP1 and Windows Server 2012 guest virtual machines. After SnapDrive is installed in the guest VM, SnapDrive recognizes the virtual Fibre Channel initiator and enables storage provisioning. Up to 256 LUNs can be provisioned per vFC port presented to the VM. All the SnapDrive features such as Snapshot and restore are supported on a vFC LUN.

Note: For information about FC HBAs, refer to the NetApp Interoperability Matrix.

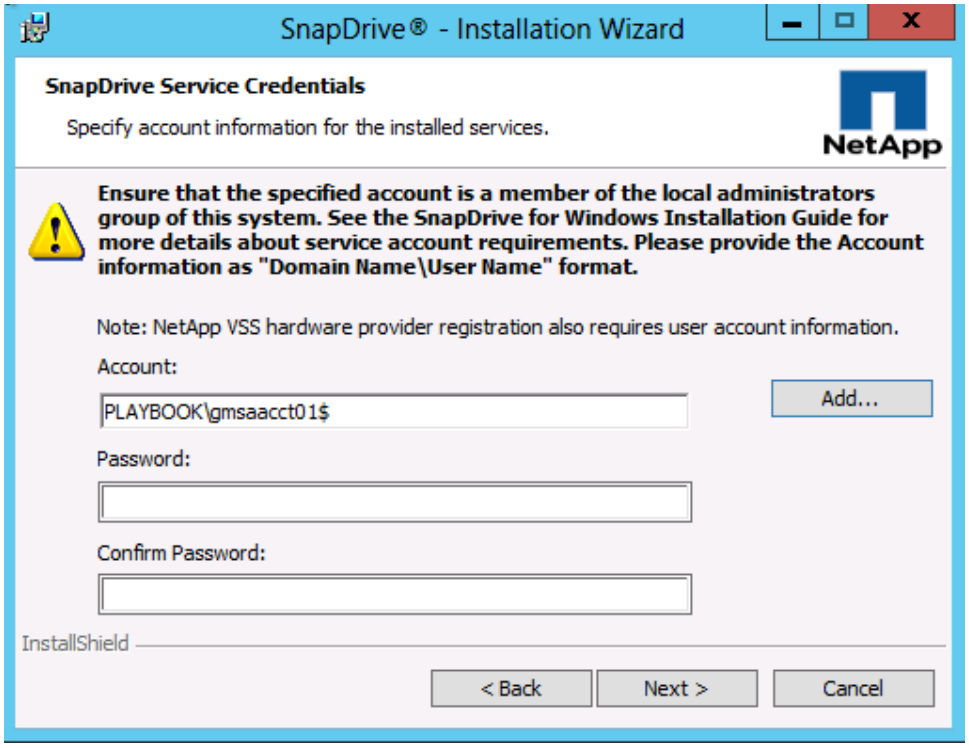
For more information on virtual Fibre Channel, refer to http://technet.microsoft.com/en-us/library/hh831413.aspx. Also, you can refer to the appendix for more information on how to use virtual Fibre Channel on NetApp storage systems.

9.9 Group Managed Service Accounts

Group managed service accounts (GMSA) is a password management solution for service accounts in Windows Server 2012 environments. It is an improvised version of managed service accounts, which was introduced in Windows Server 2008 R2. Unlike managed service accounts, in GMSA the password is generated and maintained by the key distribution service (KDS) on Windows Server 2012 domain controllers, thereby allowing multiple hosts to use GMSA. Member servers that want to use the GMSA simply query the domain controller for the current password, thus eliminating the need for an administrator to manually administer passwords for these accounts.

To configure SnapDrive for GMSA, SnapDrive service must be allowed to run from GMSA and should be able to perform all supported operations.

Figure 8) SnapDrive configured with GMSA account.



Note: If SnapDrive is configured using GMSA, it cannot connect to a storage system over RPC protocol.

9.10 Windows Server 2012 Features That Are Not Supported from SnapDrive 7.0 When Connected to NetApp Storage Systems Running Data ONTAP 7-Mode

SnapDrive 7.0 for Windows, and the NetApp SnapManager suite of products do not support the following features for Windows Server 2012 when connected to Data ONTAP 7-Mode systems

- Hyper-V over SMB 3.0
- SMB over remote file shares
- SMB VSS for remote file shares (Remote VSS)

The preceding features are available only when the host is connected to clustered Data ONTAP 8.2. systems. For more information, refer to TR: 4218: SnapDrive 7.0 for Windows SMB 3.0: Best Practices and Deployment Guide.

Note: Hyper-V replica and Windows Server 2012 native thin provisioning are not supported in SnapDrive 7.0 for Windows.

9.11 Windows Server 2012 Virtual Machine Support for ESX Environments

ESXi™ 5.0 U1 and ESXi 5.1 support Windows Server 2012 virtual machines.

Appendix

SnapDrive and Windows Server 2012 Behavior When a New Node Is Added to the Cluster

Consider three nodes named NODE1, NODE2, and NODE3 that are part of a cluster called W2012CLUS.

Also, assume that the nodes are configured as follows:

- NODE1 and NODE2 are part of cluster W2012CLUS

  NODE1 is the owner of the following:
  - Cluster - W2012CLUS
  - "Available Storage" group
  - NODE1 and NODE2 have one dedicated disk each
  - NODE1's dedicated disk has drive letter E:\
  - NODE2's dedicated disk has drive letter F:\
- Now a new node, NODE3, is added to the cluster W2012CLUS using "Add Node Wizard." The wizard presents an option “Add all eligible storage to the cluster” to the user, which is selected by default.

Behavior

- NODE3 is added to the cluster W2012CLUS

  NODE1's dedicated disk (E:\) is converted as follows:
  - Dedicated disk is converted to a clustered disk
  - A cluster resource is created for the disk that is "Cluster Disk 1"
  - Cluster resource is part of "Available Storage"
  - Disk is online and accessible
- NODE2's dedicated disk (F:\) is converted as follows:

  - Dedicated disk is converted to a clustered disk
  - A cluster resource is created for the disk that is "Cluster Disk 2"
  - Cluster resource is part of “Available Storage" owned by NODE1
  - Disk is offline and not accessible by SnapDrive
- The dedicated disk of NODE2, that is, F:\, will neither be seen by NODE1 SnapDrive nor NODE2 SnapDrive
  - In NODE2, go to Disk Management and locate the dedicated disk. The disk will be offline. A mouse hover will give a tool tip "Reserved (The disk is offline because of policy set by an administrator)."
  - If you try to make the disk Online from the Disk Management console, you will see an error message: "The specified disk or volume is managed by the Microsoft Failover Clustering component. The disk must be in cluster maintenance mode and the cluster resource status must be online to perform this operation."
  - Also, SnapDrive gives out the following error for the disk in the debug logs: "The LUN may not have a file system created on it, or it may not be formatted with the NTFS file system. If it is a cluster system this situation can be caused by the LUN being offline, or not owned by this computer."

Resolution

To bring the "Cluster Disk 2" on line, perform the following steps:

1. Add the iSCSI Initiator of NODE1 to the LUN using NetApp FilerView\Cluster Element Manager
2. Bring the associated Cluster Resource "Cluster Disk 2" on line in Failover Cluster Manager.
3. Refresh "Disks" in SnapDrive MMC Console and you will be able to see the "Cluster Disk 2" in SnapDrive.
4. Repeat the same operation for "Cluster Disk 1" to see the disk in SnapDrive.

References

- Review the SnapDrive 7.0 for Windows release notes for additional information such as limitations, upgrade information, fixed issues, known issues, and documentation corrections.
- Visit the online FAQ for SnapDrive Frequently Asked Questions.
- Review the specific links noted in this document for environment-specific best practices.
- Visit the NetApp Support site for Technical Assistance and Documentation.
- Download the latest software available from Software Downloads.
- Talk to your peers and other experts by visiting the NetApp Communities.
- Get free instructor-led training sessions: “Getting Started with Software Packs.”

Version History

Version	Date	Document Version History
Version 1.0	September 2013	Initial release

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.

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

Go further, faster®

www.netapp.com