Technical Report

SnapDrive 7.0 for Windows SMB 3.0: Best Practices and Deployment Guide

Santhosh Harihara Rao, NetApp
August 2013 | TR-4218

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Overview

NetApp® SnapDrive® for Windows® (SDW) helps you to perform storage-provisioning tasks and manage data in Microsoft® Windows environments. You can run SnapDrive software on Windows® hosts in either a physical or a virtual environment. SnapDrive software integrates with Windows Volume Manager so that storage systems can serve as virtual storage devices for application data in Windows Server® 2008 R2 and Windows Server 2012. It can also be used to provision storage for Windows virtual machines hosted on ESX® hypervisors.

SnapDrive manages LUNs on a storage system, making these LUNs available as local disks on Windows hosts. This allows Windows hosts to interact with LUNs as if they belonged to a directly attached redundant array of independent disks (RAID).

In addition to provisioning in SAN environments, SnapDrive can also provision Server Message Block (SMB) 3.0 shares to support provisioning and protecting Hyper-V® over SMB and SQL over SMB workloads.

2 Purpose and Scope

SnapDrive for Windows performs storage-management tasks, enables application-consistent backup, and restores by integrating with SnapManager® products. It also enables replication of Snapshot™ copies to remote storage for both SAN and SMB environments. The purpose of this document is to enable users who use SnapDrive 7.0 for Windows for environments to deploy workloads such as Hyper-V over SMB, CIFS shares, and SQL over SMB.

SnapDrive best practices for SAN environments are covered in TR 4000 - SnapDrive 7.0 for Windows Best Practices Guide for Clustered Data ONTAP which is available at fieldportal.netapp.com.

3 Clustered Data ONTAP 8.2

The clustered Data ONTAP® 8.2 operating system provides a complete solution for NetApp customers to deploy a virtualized environment and protect virtual machines (VMs) running on file-level data storage provided by the SMB 3.0 protocol.

3.1 SMB 3.0 Protocol in Clustered Data ONTAP 8.2

One of the major components added to clustered Data ONTAP 8.2 is support for the SMB 3.0 NAS protocol, which enables NetApp customers to use the SMB 3.0 features introduced with Microsoft Windows Server 2012. With these new features, clustered Data ONTAP can be used to host VM virtual disks and configuration settings on a CIFS file share.

Some of the SMB 3.0 features implemented in clustered Data ONTAP 8.2 to support continuously available file shares and Hyper-V storage are:

- Persistent handles (continuously available file shares)
- Witness protocol
- Clustered client failover
- Scale-out awareness
- Remote VSS

Note: SMB multichannel and SMB direct (SMB over (Remote Direct Memory Access)) are not supported with Data ONTAP 8.2.

Hyper-V over SMB and SQL over SMB workloads are supported only on the following combination:

1. SMB 3.0

2. Clustered Data ONTAP 8.2
3. Windows Server 2012

Persistent Handles (Continuously Available File Shares)

To enable continuous availability on a file share, the SMB client opens a file on behalf of the application, such as a VM running on a Hyper-V host, and requests persistent handles for the VHDX file. When the SMB server receives a request to open a file with a persistent handle, the SMB server retains sufficient information about the file handle, along with a unique resume key supplied by the SMB client. Persistent-handle information is shared between nodes in a cluster.

In the case of a planned move of file share resources from one node to another, or at the failure of a node, the SMB client will reconnect to an active and available node and will reopen the file using persistent handles. The application/VM running on the SMB client computer does not experience any failures or errors during this operation. From a VM perspective, it appears that the I/O operations to virtual disk were delayed for a small amount of time, similar to a brief loss of connectivity to the disk, but no disruption is noticed.

Note: Continuously available shares are not supported for SQL over SMB environments.

Witness Protocol

When an SMB server node fails, the SMB client usually relies on the TCP timeout to detect a failure of the file share resource, such as an open file. SMB 3.0 allows variable values for TCP timeouts and, since the virtual disk is a critical resource, the VM running on a Hyper-V server needs faster detection of network resources failing over. Witness protocol significantly improves the SMB client reconnect time.

During connection to a shared resource (TREE_CONNECT), the SMB server provides information about features enabled on a share, such as if the resource is clustered, scaled out, and continuously available. Based on this information, the SMB client requests this same data from other nodes. Upon receiving the information, the SMB client registers itself with the other node.

In the case of a cluster node failure, the SMB client is already connected to another node, which can detect the failure and then notify the SMB client. This saves the SMB client from waiting until the TCP timeout is over and instead initiates a reconnect to the running node immediately; minimizing the time the client is disconnected from the resource. For VMs with virtual disks stored on such SMB shares, disk disconnection time is reduced to the point at which the VM would not detect such disconnects as hardware failure.

This feature is enabled on clustered Data ONTAP by default only if all best practices are followed and there is a LIF on each node in the cluster in every storage virtual machine (SVM) (formerly called a Vserver). In addition, the witness protocol comes into play only for continuously available shares.

Clustered Client Failover (CCF)

To increase redundancy in a VM environment, Hyper-V servers should be placed into a Microsoft failover cluster. When the Hyper-V server node running a VM fails, the VM is live-migrated/moved to another node. Before clustered client failover (CCF) with SMB 3.0, a VM moving to another cluster node was considered as a new application instance. New application instances connecting to files already opened on file shares have to wait until the TCP timeout is over and the file handle is closed. CCF gives the VM the capability to open a virtual disk file on a file share and provides a unique application identifier. When a Hyper-V server cluster node fails, the VM starts on another Hyper-V server node and supplies the same application identifier, letting the SMB server close existing file handles. The SMB client can then reconnect to the previously open file.

Scale-Out Awareness

Clustered Data ONTAP is scale-out by design and provides the capability to serve data from multiple nodes. It brings additional data redundancy on the network and spreads the load of multiple SMB clients between multiple nodes in a cluster. Scale-out awareness allows SMB clients to connect to all nodes in the cluster and get to the same data.

Remote Volume Shadow Copy Service (VSS)

Volume Shadow Copy Service (VSS) is a framework that provides coordination of application I/O and physical storage on the same server and allows creation of application-consistent Snapshot copies of the storage. Windows Server 2012 extends the functionality of VSS to multiple servers. For instance, an application running on one server has storage on another server's file share. Remote VSS coordinates I/O activities during a backup process between both servers and provides application-consistent backup Snapshot copies of the storage for applications running remotely on the storage server. Clustered Data ONTAP 8.2 extends the functionality of remote VSS by plugging into the VSS framework; a VSS service runs on a NetApp controller and a VSS provider runs on a Windows Server 2012 machine. From a VSS perspective, the NetApp array acts exactly as a Windows file server. SnapDrive 7.0 for Windows uses remote VSS to back up and restore workloads hosted on SMB shares.

3.2 Other Features Supported in Clustered Data ONTAP 8.2

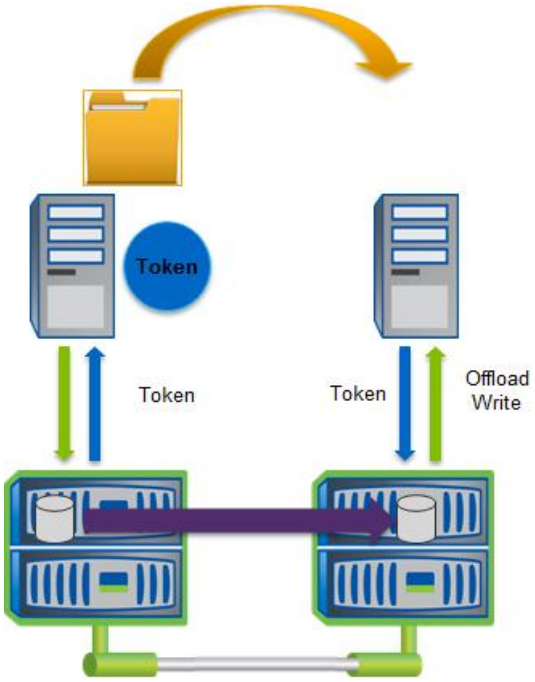
Offload Data Transfer

Copy-Offload provides a mechanism to perform full-file or sub-file copies between two directories residing on remote servers; the servers can be the same or different. Here, the copy is created by copying data between the servers (or the same server if both source and destination files are on the same server) without the client reading the data from source and writing to the destination. This reduces the client/server processor/memory utilization and minimizes network I/O bandwidth.

With Windows Server 2012, Microsoft introduced a copy-offload mechanism that can be used for making copies between two independent servers (provided there is an underlying mechanism to move data between the servers); the previous server-side copy mechanism required both the source and destination file to be on the same server.

Before proceeding with copy operation on the host, make sure that copy offload settings are configured on the storage system. SnapDrive 7.0 for Windows does not enable copy offload settings on the storage system directly. After provisioning LUN/shares using SnapDrive, activities such as storage live migration and file copy are offloaded to the storage system and SnapDrive does not participate in these operations.

Figure 1) Offloaded data transfer.



Storage Quality of Service (QOS)

Storage QoS is a new feature in NetApp Data ONTAP 8.2 that provides the ability to group storage objects and set throughput limits on the group. With this ability, a storage administrator can separate workloads by organization, application, business unit, or production versus development environments.

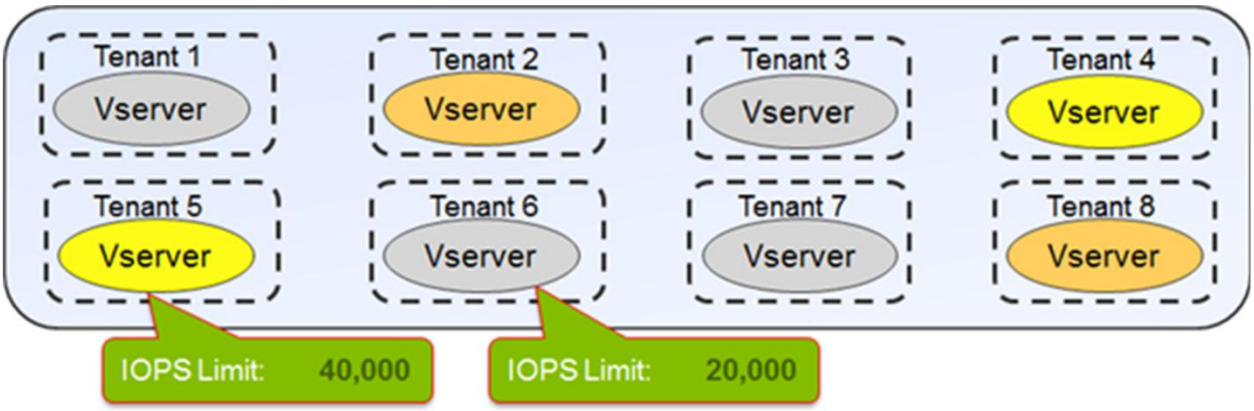
In enterprise environments, storage QoS helps achieve the following:

- Helps to prevent user workloads from affecting each other
- Helps to protect critical applications that have specific response times that must be met in IT-as-a-service (ITaaS) environments, storage QoS.
- Helps to prevent tenants from affecting each other
- Helps to avoid performance degradation with each new tenant

QoS allows you to limit the amount of I/Os sent to an SVM, a flexible volume, a LUN, or a file. The I/Os can be limited by the number of operations or the raw throughput.

After configuring Vservers or volumes for QOS, SnapDrive 7.0 for Windows can be used to provision storage from these SVMs onto the host system or the guest virtual machines after adding these SVMs' details on the host. For Microsoft application specific QOS best practices, refer to the respective SnapManager Best Practice Guides.

Figure 2) Each Vserver with its own QOS policy.



IPv6 Support

Clustered Data ONTAP 8.2 supports IPv6. SnapDrive 7.0 for Windows supports IPv6 in all its workflows that require adding an IP address/host name, such as adding a storage system in the transport protocol settings. Use the following command to enable IPv6 in a Data ONTAP 8.2 cluster.

```
network options ipv6 modify -enabled true
```

Verify that the DNS server has either the IPv6 or IPv4 address of the host system but not both.

Note: SnapDrive does not support mixed-mode IP formats. This means that both the host and storage system must use the same IP format (IPv4 or IPv6).

Note: After IPv6 has been enabled on the storage cluster, it cannot be disabled.

Note: In IPv6 environments, NetApp recommends providing FQDN in SnapDrive.

For more information, refer to the Clustered Data ONTAP Network Management Guide.

4 Clustered Data ONTAP and CIFS Vserver Setup and Configuration

There are no special requirements for a clustered Data ONTAP 8.2 setup to use SMB 3.0 features. By default, clustered Data ONTAP 8.2 supports all versions of SMB, including 1.0, 2.0, 2.1, and 3.0. Most of the usual applications of the SMB protocol, such as user file sharing, can work on pre-3.0 SMB protocols and might not benefit from the additional features of the SMB 3.0 protocol. The Hyper-V workload requires the SMB 3.0 protocol and some of its additional features, such as continuously available shares. Considering the additional overhead of storing and replicating persistent-handle information between nodes in an HA pair to support features such as continuously available shares, NetApp strongly recommends using only continuously available shares for Hyper-V over SMB workloads.

4.1 General Considerations of Clustered Data ONTAP for SMB 3.0 Workloads

When setting up clustered Data ONTAP 8.2 for using continuously available file shares to host VHDX disk images of VMs, consider the following.

- Persistent handles work only between nodes in an HA pair.
- Witness protocol works only between nodes in an HA pair.
- Continuously available file shares are only supported for Hyper-V workloads.
- ODX is supported with clustered Data ONTAP 8.2 and works across protocols. Copying data between a file share and iSCSI or an FCP-attached LUN uses ODX.

- NetApp recommends connectivity between Hyper-V hosts and the NetApp array on a 10GB network if one is available. In the case of 1GB network connectivity, NetApp recommends creating an interface group consisting of multiple 1GB ports.
- CIFS and FlexClone® (required by remote VSS of SMHV) licenses should be installed.
- Time settings on nodes in the cluster should be set up accordingly. Network Time Protocol (NTP) should be used if the NetApp CIFS server has to participate in the Windows Active Directory® domain.

The minimum Microsoft OS versions supporting SMB 3.0 are Windows Server 2012 and Windows 8.

4.2 Root and Data Volume Settings

NetApp CIFS Vserver root and data volumes should be FlexVol® volumes and have a security style of NTFS. Symlinks, hardlinks, or widelinks are not supported with SnapManager for Hyper-V. Also, junctions inside of data volumes are not supported.

4.3 Data and Management LIF Settings

At least one data LIF should be created per node for every Vserver in the cluster. The data LIF should not be configured to "AutoRevert." Each LIF's IP address should have an entry in DNS, and no NetBIOS aliases are allowed for DNS entries. Network interface failover groups can be configured to specify network ports to which the LIF can be moved.

4.4 SMB 3.0 Settings

Though the SMB 3.0 protocol is enabled by default, it can be checked, enabled, or disabled using the `vserver cifs options` command in the advanced mode.

1. To set up the advanced mode, use the command `set advanced`.

```
Vespus::> set advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y

Vespus::*>
```

Advanced mode is required for showing and modifying all other settings.

2. To check if SMB 3.0 is enabled, use the command `vserver cifs options show`.

```
Vespus::*> vserver cifs options show

Vserver: nacifs

           Copy Offload Enabled: true
            Default Unix Group: -
             Default Unix User: pcuser
          Export Policies Enabled: false
            Is Referral Enabled: false
           Is Local Auth Enabled: true
     Is Local Users and Groups Enabled: true
            Max Multiplex Count: 255
             Read Grants Exec: disabled
          Shadowcopy Dir Depth: 5
            Shadowcopy Enabled: true
               SMB2 Enabled: true
               SMB3 Enabled: true
               WINS Servers: -
 Is Use Junction as Reparse Point Enabled: true

Vespus::*>
```

3. To enable or disable SMB 3.0, use the command `vserver cifs options modify –vserver <vserver name> -smb3-enabled {true|false}.`

```
Vespus::*> vserver cifs options modify -vserver nacifs -smb3-enabled true

Vespus::*>
```

Note: Continuously available shares are not supported for SQL over SMB environments.

4.5 ODX Settings

To utilize ODX for fast provisioning of VMs from the master image prepared with the Microsoft SysPrep utility on the same file share hosting VHDX files, the ODX feature is enabled globally or on a per-Vserver basis by default.

1. To check if ODX is enabled, use the command `vserver cifs options show`.

```
Vespus::*> vserver cifs options show

Vserver: nacifs

            Copy Offload Enabled: true
             Default Unix Group: -
              Default Unix User: pcuser
          Export Policies Enabled: false
            Is Referral Enabled: false
           Is Local Auth Enabled: true
     Is Local Users and Groups Enabled: true
            Max Multiplex Count: 255
             Read Grants Exec: disabled
           Shadowcopy Dir Depth: 5
            Shadowcopy Enabled: true
               SMB2 Enabled: true
               SMB3 Enabled: true
               WINS Servers: -
 Is Use Junction as Reparse Point Enabled: true

Vespus::*>
```

2. To enable or disable the ODX feature, use the command `vserver cifs options modify –vserver <vserver name> -copy-offload-enabled {true|false}.`

```
Vespus::*> vserver cifs options modify -vserver nacifs -copy-offload-enabled true

Vespus::*>
```

4.6 Remote VSS Settings (Shadow Copy Feature VSS)

This feature should be enabled to protect VMs if SMHV is to be deployed on Hyper-V servers.

1. To check if remote VSS is enabled, use the command `vserver cifs options show`.

```
Vespus::*> vserver cifs options show

Vserver: nacifs

           Copy Offload Enabled: true
            Default Unix Group: -
             Default Unix User: pcuser
         Export Policies Enabled: false
           Is Referral Enabled: false
          Is Local Auth Enabled: true
     Is Local Users and Groups Enabled: true
           Max Multiplex Count: 255
            Read Grants Exec: disabled
          Shadowcopy Dir Depth: 5
           Shadowcopy Enabled: true
              SMB2 Enabled: true
```

```
               SMB3 Enabled: true
               WINS Servers: -
 Is Use Junction as Reparse Point Enabled: true

Vespus::*>
```

2. To enable or disable the remote VSS feature, use the command `vserver cifs options modify –vserver <vserver name> -shadowcopy-enabled {true|false}`.

```
Vespus::*> vserver cifs options modify -vserver nacifs -shadowcopy-enabled true

Vespus::*>
```

4.7 Automatic Node Referral Settings

The Microsoft Hyper-V host relies heavily on Kerberos authentication that cannot be utilized with NetApp IP-based automatic node referral. By default, node referrals are disabled, but, when deploying Hyper-V over SMB, verify that this is the case using the command `vserver cifs options show`.

```
Vespus::*> vserver cifs options show

Vserver: nacifs

           Copy Offload Enabled: true
            Default Unix Group: -
             Default Unix User: pcuser
          Export Policies Enabled: false
            Is Referral Enabled: false
           Is Local Auth Enabled: true
     Is Local Users and Groups Enabled: true
            Max Multiplex Count: 255
             Read Grants Exec: disabled
           Shadowcopy Dir Depth: 5
            Shadowcopy Enabled: true
               SMB2 Enabled: true
               SMB3 Enabled: true
               WINS Servers: -
 Is Use Junction as Reparse Point Enabled: true

Vespus::*>
```

1. To disable this feature, use the command `vserver cifs options modify –vserver <vserver name> -is-referral-enabled false`.

```
Vespus::*> vserver cifs options modify -vserver nacifs -is-referral-enabled false

Vespus::*>
```

4.8 Creating Network Interface Failover Groups

1. To create a network interface failover group, use the `network interface failover-groups` command.

```
Vespus::> network interface failover-groups create -failover-group nacifs_e1a -node Vespus-01 -
port e1a

Vespus::> network interface failover-groups create -failover-group nacifs_e1a -node Vespus-02 -
port e1a

Vespus::> network interface failover-groups show
Failover
Group        Node       Port
------------------- ----------------- ----------
clusterwide
          Vespus-01     e0a
          Vespus-01     e0b
          Vespus-01     e0c
```

```
          Vespus-01     e0d
          Vespus-01     e1a
          Vespus-02     e0a
          Vespus-02     e0b
          Vespus-02     e0c
          Vespus-02     e0d
          Vespus-02     e1a
nacifs_e1a
          Vespus-01     e1a
          Vespus-02     e1a
12 entries were displayed.
```

5 SnapDrive 7.0 for Windows Architecture

SnapDrive for Windows 7.0 has undergone significant architecture changes from the earlier release to provide support for new features such as Hyper-V over SMB 3.0 and backup/restore of workloads hosted on CIFS shares by leveraging remote VSS.

SnapDrive 7.0 for Windows can now be used to provision and protect SMB workloads (Hyper-V over SMB and SQL over SMB) in addition to its already existing support for SAN. The SnapManager suite of products such as SnapManager for Hyper-V and SnapManager for SQL leverage SnapDrive 7.0 for Windows to protect their respective SMB-related workloads.

For best practices for SnapDrive 7.0 for Windows in SAN environments, refer to TR- 4000: SnapDrive 7.0 for Windows Best Practices Guide for SAN Environments available at fieldportal.netapp.com.

For best practices on setting up Windows Server 2012 Hyper-V over SMB workloads on NetApp, refer to TR-4172: Microsoft Hyper-V over SMB 3.0 with Clustered Data ONTAP: Best Practices.

For best practices protecting Hyper-V virtual machines in SMB environments using SnapManager for Hyper-V 2.0, refer to the “SnapManager for Hyper-V 2.0 Best Practices Guide for Clustered Data ONTAP.”

For best practices protecting SQL workloads in SMB environments using SnapManager for SQL, refer to the “SnapManager for SQL 7.0 Best Practices Guide for Clustered Data ONTAP.”

5.1 Prerequisites

.Net 4.0

.Net 4.0 is required for installing SnapDrive 7.0 for Windows. The earlier version of SnapDrive, that is SnapDrive 6.5 for Windows, used .Net 3.5. Therefore, in a SnapDrive upgrade scenario, verify that .Net 4.0 is first installed and then upgraded to SnapDrive 7.0 for Windows.

Note: Upgrading .Net may require a reboot depending on the state of the system.

Licenses

Verify that the following licenses are installed on the storage system while performing SMB-related operations using SnapDrive.

- CIFS license
- FlexClone (for mount operations and remote VSS)
- SnapRestore®
- SnapManager_suite license on the storage system or a SnapDrive and SnapManager host license on the server
- SnapMirror and SnapVault® (optional)

Storage-Side Settings

1. Configure all parameters as per section 4.
2. Verify that there is a separate LIF created for SMB communication.
3. Verify that there is at least one data LIF on every node that has a share for nondisruptive operations.

Best Practice
The LIF configuration process can be simplified by using System Manager.

5.2 Supported Configurations

For all SMB 3.0–related workloads, users must use the PowerShell™ cmdlets or templates that get installed after SnapDrive is installed. The templates are installed in the following location: - `C:\Program Files\NetApp\SnapDrive\templates`.

PowerShell cmdlets support SnapDrive provisioning, Snapshot copy management, and backup, restore, mounting, SnapMirror®, and SnapVault operations for both SAN and SMB.

Table 1) Supported configurations for SAN and SMB workflows with SnapDrive 7.0 for Windows.

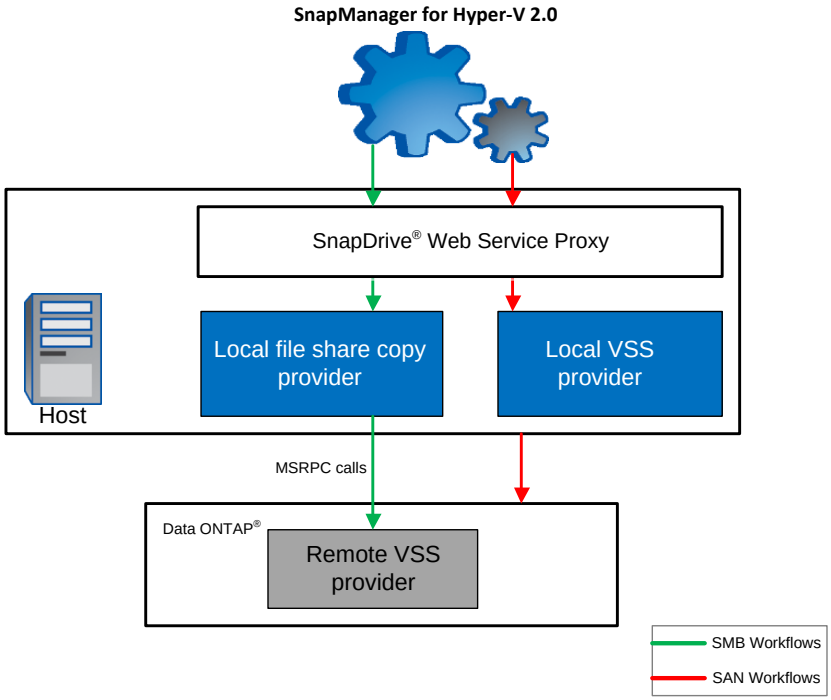
SnapDrive Interface	SAN (FC, iSCSI, and FCOE)	SMB 3.0 (Windows Server 2012 Only)
SnapDrive GUI	Supported	Not supported
SnapDrive CLI (SDCLI)	Supported	Not supported
SnapDrive PowerShell cmdlets	Basic operations are supported	Fully supports all operations and workflows

5.3 Architecture of SnapDrive 7.0 for Windows

SnapDrive 7.0 for Windows supports both SAN and SMB workflows. As discussed in the previous section, all SMB-related workflows can be accessed through the PowerShell interface. All SAN-based workflows can be performed using either the SnapDrive GUI or SDCLI commands. In the case of SMB workflows, the web service proxy passes requests such as backup, restore, and so on to the local file share copy provider that communicates to the remote VSS provider in the Data ONTAP system through MSRPC calls. If a SAN operation is initiated, these calls are passed to the VSS hardware provider that resides on the host, which communicates to Data ONTAP for SAN-related operations.

Any SMB or SAN backup, restore, or replication operation initiated via SnapManager products such as SnapManager for Hyper-V or SnapManager for SQL reaches the SnapDrive web service proxy layer directly and is redirected accordingly.

Figure 3) Architecture of SnapDrive 7.0 for Windows.



6 SnapDrive 7.0 for Windows and Windows PowerShell

SnapDrive 7.0 for Windows introduces PowerShell cmdlets that can be used to perform common operations and also build workflows. This is in addition to the existing SDCLI option. PowerShell cmdlets can be used to perform for both SAN and SMB workflows.

Table 2) PowerShell cmdlets.

PowerShell cmdlets	SAN	NAS	7-Mode System Support
Debug-SdHost	No	Yes	No
Dismount-SdSnapshot	No	Yes	No
Get-SdInfo	Yes	Yes	Yes
Get-SdSMBShadowCopyEmsMessage	No	Yes	No
Get-SdSnapMirror	No	Yes	No
Get-SdSnapshot	Yes	Yes	Yes
Invoke-SdSnapMirrorUpdate	Yes	Yes	Yes, no SnapVault (use Protection Manager)
Invoke-SdEmsAutosupportLog	Yes	Yes	Yes

PowerShell cmdlets	SAN	NAS	7-Mode System Support
Get-SdVM	Yes	Yes	Yes
Mount-SdSnapshot	No	Yes	No
Get-SdStorageConnectionSetting	Yes	Yes	Yes
Get-SdStorage	Yes	Yes	Yes
New-SdSMBShare	No	Yes	No
New-SdSnapshot	Yes	Yes	Yes
New-SdVolume	Yes	Yes	No
Remove-SdSMBShare	No	Yes	No
Remove-SdSnapshot	Yes	Yes	Yes
Remove-SdStorageConnectionSetting	Yes	Yes	Yes
Remove-SdVolume	No	Yes	No
Rename-SdSnapshot	Yes	Yes	Yes
Restore-SdSnapshot	Yes	Yes	Yes
Set-SdSnapshot	Yes	Yes	No
Set-SdStorageConnectionSetting	Yes	Yes	Yes
Get-SdSnapMirrorPolicyRule	Yes	Yes	No
Remove-SdSnapMirrorPolicyRule	Yes	Yes	No
Set-SdSnapMirrorPolicyRule	Yes	Yes	No

For more information on each PowerShell cmdlet, refer to the PowerShell reference guide that is available as part of the SnapDrive software documentation.

Note: Unlike PowerShell cmdlets, SDCLI commands do not support SMB operations or workflows.

6.1 Provisioning Templates

SnapDrive 7.0 for Windows also introduced PowerShell templates that can instantly provision SMB environments depending on the workload on which the user intends to host them. The template is configured per the best practices for the workload that will be deployed on the SMB environment. The PowerShell templates are installed at the following location:

```
C:\Program Files\NetApp\SnapDrive\templates
```

The following templates are available:

- Home directory
- SQL over SMB
- Hyper-V over SMB

Note: These templates can be customized depending on the environment.

Example:

```
PS C:\Users\administrator.HOST1> New-SdVolume -TemplateName HomeDirProvTemplate.xml -Name test -
Size 10GB -Aggregate Aggr1 -StorageSystem 10.1.1.2 -JunctionPath /home_test -VServerContext
Vserver1
```

Best Practice

NetApp recommends provisioning all SMB-related workloads such as CIFS shares for home directories, SQL workloads, and Hyper-V workloads on a host using these PowerShell provisioning templates. This will enable the environment to be configured per best practices.

Provisioning Shares for Hyper-V Using New-SdSMBShare cmdlet

This example syntax provisions a share for Hyper-V using the specified template.

```
New-SdSMBShare -Path / -Name HyperVShare -CIFSServer HyperVFileServer -TemplateName
"C:\program files\SnapDrive\HyperVVHDxProvTemplate.xml"
```

```
Acl               : {Everyone / Full Control}
AttributeCacheTtl : 1
CifsServer        : HyperVFileServer
VServer           : HyperVirtualStorageServer
Comment           : Hyper-V SMB share
DirUmask          : 1
FileUmask         : 1
Path              : /
Volume            : HyperVVolume
ShareName         : HyperVShare
ShareProperties   : {browsable, continuously_available}
SymlinkProperties : {enable}
UNCPathType       : SMBShare
IsMountedToDrive  : False
MountedDrive      :
ResourceType      : SDSMBShare
ResourceName      : \\HyperVFileServer\HyperVShare
Ranges            :
```

Provisioning a Storage System Volume Using the New-SdVolume cmdlet in The Template

This example provisions a storage system volume using the specified template.

```
New-SdVolume -Name sqldbvolume -Aggregate sqldbaggregate -JunctionPath /sqldbvolume
-TemplateName C:\Program Files\SnapDrive\Templates\HyperVVHDxProvTemplate.xml -Size
128GB -StorageSystem sqlvirtualstorageserver
```

```
Name               : sqldbvolume
Vserver            : sqlvirtualstorageserver
FullPath           : sqlvirtualstorageserver:/vol/sqldbvolume
JunctionPath       : /sqldbvolume
JunctionParentName :
SizeTotal          :
SizeUsed           :
SnapMirrorSource   :
```

```
SnapMirrorDest      :
SnapVaultPrimary    :
SnapVaultSecondary  :
FlexCloneEnabled    :
IsFlexClone         :
ResourceType        : SDStorageVolume
ResourceName        : sqlvirtualstorageserver:/vol/sqldbvolume
Ranges              :
```

7 Adding a Vserver in SnapDrive

SMB operations and workflows can be executed only after adding the CIFS Vserver system to SnapDrive. This can be achieved using the following PowerShell cmdlet.

```
Set-SdStorageConnectionSetting -Name (Vserver Mgmt LIF or Vserver name)
```

When the Vserver is added using this cmdlet, the configuration repository file that is the Nsf.config file is created at C:\Program Files\NetApp\SnapDrive\ (SnapDrive installation folder). This file is subsequently updated when new Vserver/storage system connections are established/removed.

Note: Verify that the CIFS server name and the Vserver name are not identical.

Note: Cluster Vserver credentials are not required to be added when adding the CIFS Vserver.

Note: NetApp recommends adding the Vserver name and IP address in C:\Windows\System32\Drivers\etc.

Best Practice

NetApp recommends protecting the `Nsf.config` file by creating another copy of the file and storing it safely. Also, update the backup copy as and when new storage connections are established or existing ones are removed. After restoring the `Nsf.config` file, SnapDrive services need to be restarted.

8 Provisioning a Volume and a CIFS Share Using SnapDrive 7.0 for Windows

Volumes and shares can be provisioned using standalone PowerShell cmdlets or templates.

Volume Creation and Deletion

Volume creation for hosting SMB shares can be done using the New-SDVolume that can be used as follows.

```
New-SdVolume -Name <vol_name> -Aggregate <aggregate_name> - JunctionPath <vol_junction_path> -
TemplateName C:\Program Files \SnapDrive\Templates\HyperVVHDxProvTemplate.xml -Size <vol_size> -
StorageSystem <storage_system_name>
```

Similarly, the Remove-SDVolume cmdlet can be used to a volume from the Vserver. When you remove a volume using this cmdlet, Remove- SdVolume dismounts your volume, brings it offline, and deletes it. Note that a volume in a SnapMirror relationship cannot be deleted.

CIFS Shares

As discussed in the PowerShell templates section, SMB shares can be provisioned using templates for specific workloads such as SQL over SMB, Hyper-V over SMB, and home directories.

The following example shows how users can provision a share for a home directory.

```
New-SdSMBshare -templatename "sd_homedir_prov_template" -Path "/homedir" -CIFSServer "fileserver"
```

Example of Hyper-V over SMB

Best Practice
After provisioning a CIFS share from SnapDrive, NetApp recommends validating your environment by running the PowerShell cmdlet debug-sdhost. This enables adherence to the best practices for the workload being hosted.

Best Practice
Add a DNS entry for data LIFs mapped to each CIFS server name. If there are multiple data LIFs mapped to a CIFS server, add any of the data LIFs.

9 Backup and Restore Architecture of a CIFS Share Using SnapDrive 7.0 for Windows

9.1 Backup and Restore Architecture

SnapManager for Hyper-V and SnapManager for SQL support SMB workflows. When a backup or restore operation is initiated from one of these SnapManager products, the calls are passed to the SnapDrive web service proxy. The SnapDrive web service proxy then initiates communication between the local file share copy provider from Microsoft and the remote VSS provider using the MSRPC protocol.

9.2 Backup and Restore

SnapDrive supports the backup and restore of SMB shares. Multiple shares hosted across different CIFS servers can be backed up at once. Snapshot copies can be created using the New-SDsnapshot cmdlet. This cmdlet can be used to create Snapshot copies of a LUN or an SMB share. The following example would back up the SMB shares by creating Snapshot copies of the corresponding volumes using the Snapshot name `sql_snap`.

```
New-SdSnapshot -path "\\fileserver\sqlshare","\\fileserver\sqlshare2" -snapshot "sql_snap"
```

The restore-SDSnapshot cmdlet is used for restoring both LUNs and SMB shares locally or from the secondary storage (SnapVault). In the case of SMB shares, individual files and directories can also be restored. SnapDrive also supports restoring SMB shares from secondary storage such as SnapVault.

The following section lists the typical restore examples.

Example 1: Restore a Snapshot copy on an SMB share from a Snapshot copy.

```
Restore-SdSnapshot -Path "\\172.17.12.101\share\files.txt" -Snapshot "snapshot_1"
```

This example restores the file named file.txt on SMB share "\\172.17.12.101\share" from the specified Snapshot copy "snapshot_1."

Example 2: Restore a file under a subfolder of an SMB share from a Snapshot copy.

```
Restore-SdSnapshot -Path "\\172.17.12.101\share\dir1\file1.txt" -Snapshot snapshot_1
```

This example restores the file on "\\172.17.12.101\share\dir1\file1.txt" from the Snapshot copy snapshot_1.

Example 3: Restore a directory with its contents under an SMB share from a Snapshot copy.

```
Restore-SdSnapshot -Path "\\172.17.12.101\share\folder1\*" -Snapshot "snapshot_1"
```

This example restores the directory named "folder1" and its contents from the specified Snapshot copy "snapshot_1."

Example 4: Restore multiple files and directories under an SMB share from a Snapshot copy.

```
Restore-SdSnapshot -Path
"\\172.17.12.101\share\file0.txt","\\172.17.12.101\share\dir1\file1.txt","\\172.17.12.101\share\d
ir2\ -Snapshot snapshot_1
```

This example restores a file named "file0.txt" under the root of the SMB share, a file named "file1.txt" under directory "dir1," and a directory named "dir2" and "dir3" and their contents from the Snapshot copy named "snapshot_1."

Example 5: Restore a file on an SMB share from a Snapshot copy on the SnapVault secondary.

```
Restore-SdSnapshot -Path "\\172.17.12.101\share\dir1\file1.txt" -Snapshot "snapshot_1" -
StorageSystem 172.17.165.29 -VolumeName vaultdest_vol
```

This example restores a file named "file1.txt" under directory "dir1" from the Snapshot copy named "snapshot_1" on the SnapVault secondary storage system.

Example 6: Restore a Snapshot copy on a disk from a Snapshot copy.

```
Restore-SdSnapshot -Path E: -Snapshot "snapshot_1"
```

This example restores the Snapshot named “snapshot_1.”

Note: The restore-sdsnapshot cmdlet cannot perform file-level restores in SAN environments.

Best Practice

In case of a backup failure, use the Get-SdSMBShadowCopyEmsMessage cmdlet to retrieve EMS logs from the Vserver specific to the backup event. This will help determine the root cause of the failure.

Best Practice

If a user has to turn the volume offline for any reason, when the volume is remounted, verify that it is done using the correct junction path. Otherwise, backup operations are likely to fail.

9.3 Mounting and Dismounting a Snapshot Copy

Use the Mount-SdSnapshot cmdlet to mount a LUN or a share from the specified Snapshot copy and show them as a different set of shares by having a new GUID.

This cmdlet can be used in a SQL-over -SMB environment to perform backup verification. The user can mount the database and log shares from the Snapshot copy and carry out database verification. The ACLs on the mounted share are the same as the original share.

The mount-sdsnapshot cmdlet can also be used to mount the shares from a secondary Snapshot copy (SnapVault). Here, the user must specify the storage system and volume. Verify that the aggregate of the volume that is the source of the FlexClone operation is assigned to the Vserver aggregates list. The following example mounts the share DBShare from the specified secondary Snapshot copy weekly_snap.

```
Mount-SdSnapshot -Path "\\SQLFileserver\DBShare","\\SQLFileserver\LogShare" -snapshot
"weekly_snap" -storagesystem mirror_vserver -volume dbmirrorvolume
```

While mounting a Snapshot copy, verify that the aggregate of the volume that is the source of the mount operation is added to the Vserver-assigned aggregates list option.

When a share is dismounted, it is deleted. The underlying FlexClone volume is also deleted.

Note: The FlexClone volume that is created during the mount operation is not space guaranteed.

10 Creating Virtual Machines in CIFS Shares Created by SnapDrive 7.0 for Windows

After provisioning the SMB shares using SnapDrive 7.0 for Windows, it is simple to configure Hyper-V in Windows Server 2012 to use these shares as storage for VM virtual disks. It requires setting the location of VHDX files (see Figure 4) and VM configuration files (see Figure 5).

Figure 4) VHDX location settings.

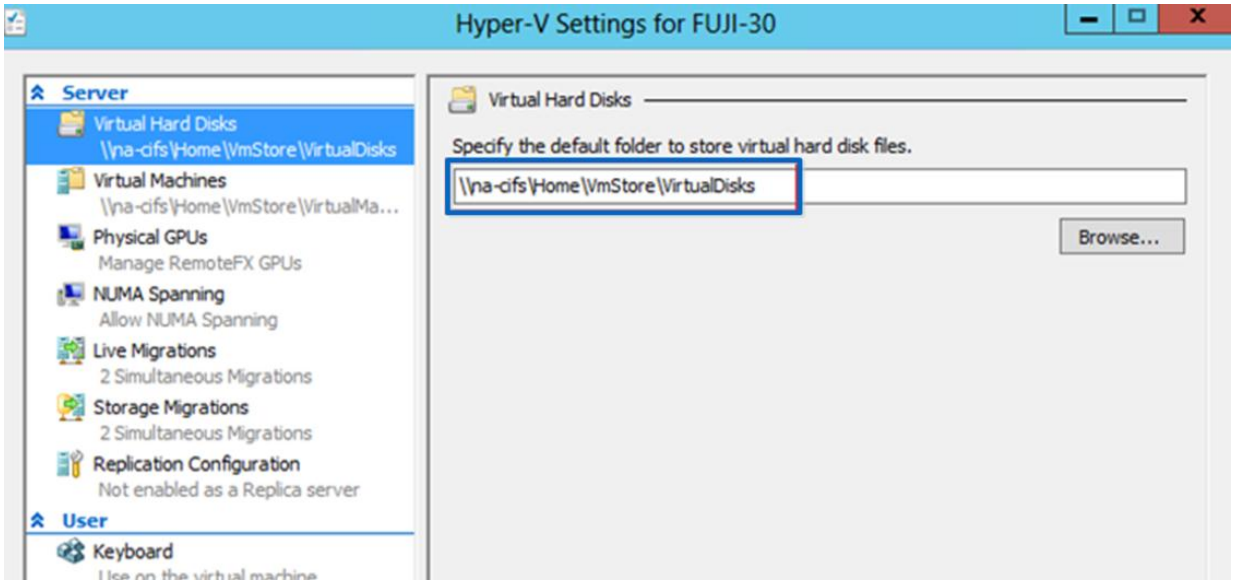
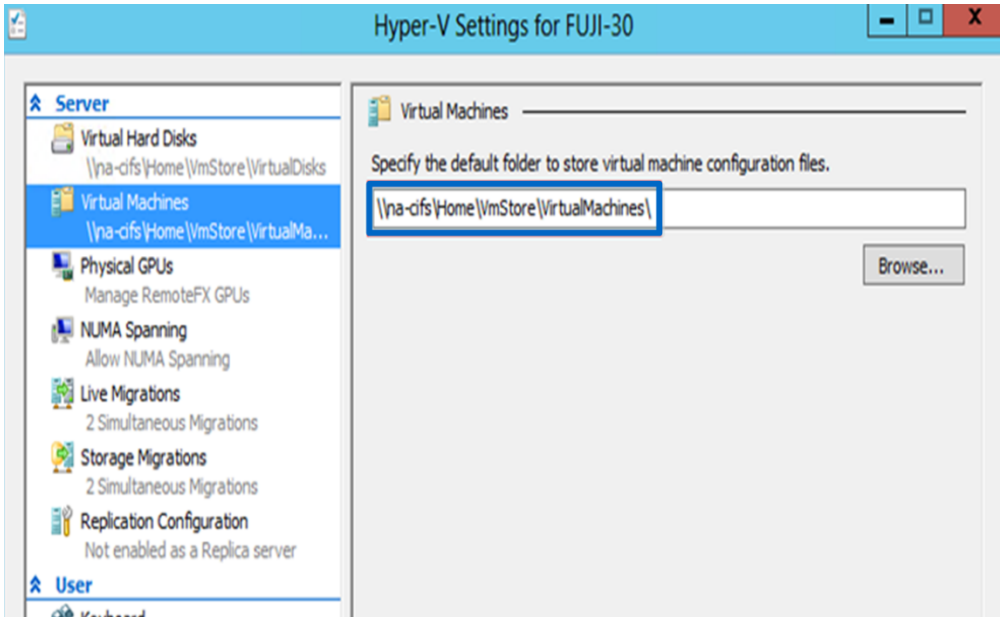


Figure 5) VM location settings.



These virtual machines then can be protected using SnapManager for Hyper-V using specific backup and replication policies. The Get-SdVM PowerShell cmdlet then can be used to retrieve VM information.

11 SnapMirror and SnapVault

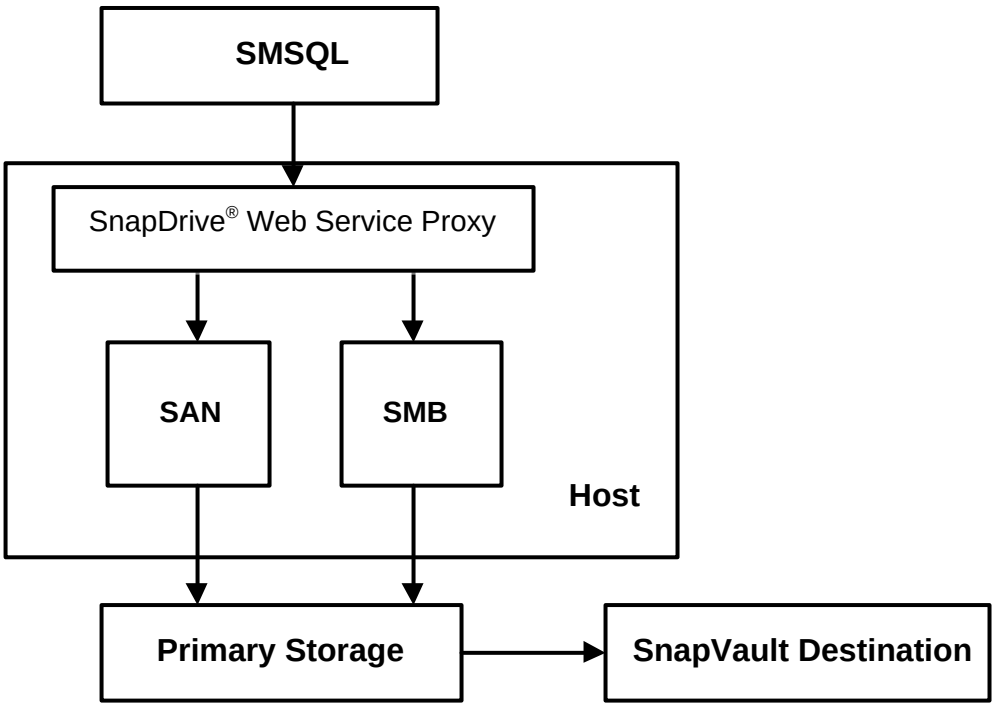
11.1 SnapMirror

SnapDrive 7.0 for Windows supports SnapMirror for volumes containing SMB shares. If the SnapMirror source volume is replicated to multiple destination volumes (fan-out scenarios), all the destinations are updated. For best practices on SnapMirror configurations, refer to the following link: https://fieldportal.netapp.com/Core/DownloadDoc.aspx?documentID=69125&contentID=73752.

11.2 SnapVault

SnapDrive 7.0 for Windows introduces native SnapVault integration. This means that in clustered Data ONTAP 8.2 environments, OnCommand® Protection Manager is no longer required to configure and update SnapVault datasets. SnapVault can be configured using PowerShell cmdlets. It can be initiated by the SnapManager for SQL or SnapManager for Hyper-V GUI.

Figure 6) SnapVault workflow.



Note: In the case of Data ONTAP systems operating in 7-Mode, SnapDrive will continue to require OnCommand Protection Manager for SnapVault configuration in SAN environments.

Note: Cascaded SnapVault is not supported.

In order to configure specific retention period policies for the Snapshot copies, use the Set-SdSnapMirrorPolicyRule PowerShell cmdlet. Each volume that has a SnapVault relationship that hosts SMB shares can have a SnapVault policy associated with it. These rules help users to configure the retention periods and the action taken after the threshold is reached. Users have the option to create custom labels depending on specific business needs.

The Set-SdSnapMirrorPolicyRule cmdlet can be used to set the SnapVault retention policies along with thresholds. For example, the following command will set the SnapMirror policy rule myWeekly on the policy of the specified relationship.

```
Set-SdSnapMirrorPolicyRule -SourceStorageSystem vs01 -SourceStorageSystemVolume src_vol01 -
DestinationStorageSystem vs02 -DestinationStorageSystemVolume dest_vol01 -SnapMirrorLabel
myWeekly -Retention 8 -Preserve -WarnThreshold 3 -verbose -Confirm:$false
```

Before setting the policy rule, verify that the policy is created at the cluster Vserver.

Users also can use the PowerShell cmdlet set-SDsnapshot to attach labels to Snapshot copies and then select the secondary retention bucket by specifying the appropriate label.

The following example added the suffix label “monthly” to the specified Snapshot copy “salesdb_backup.”

```
Set-SdSnapshot -storagesystem prodvserver -volume voldb,vollog -snapshot salesdb_backup | set-
Sdsnapshot -label monthly
```

The GetMirrorInfo cmdlet can be used to get information on the SnapVault and SnapMirror relationships that were established from a given storage system.

```
PS C:\Users\administrator.TEST>(Get-SdStorage -StorageSystem 172.17.162.61 -
GetMirrorInfo -Verbose).StorageSystemResource.volume
```

Note: When restoring from a SnapVault storage system, verify that a valid FlexClone and CIFS license was installed on the SnapVault system. Also, a valid CIFS server must be present in the SnapVault system.

Note: The secondary CIFS server should be in the same domain as the primary CIFS server; if they are in different domains there should be trust between the two domains. The secondary CIFS server should be in the same domain as the primary CIFS server; if they are in different domains there should be trust between the two domains.

Note: Add the SnapVault and SnapMirror destination Vserver credentials in transport protocol settings.

If the SnapVault destination is in the same cluster, then ODX should be used.

12 Restoring Snapshot Copies After Storage Live Migration

The storage live migration feature in Windows Server 2012 enables migration of virtual machine–related files to a different storage location without the VM having to undergo downtime. This process is faster if the storage supports Offload Data Transfer. As discussed in the previous sections, Data ONTAP 8.2 supports offload data transfer.

When you initiate a storage migration of a virtual machine from one SMB share to another SMB share or LUN within the same volume or a different volume, Windows Server 2012 queries the storage system on whether it is “Copy-offload” enabled. If it is, Windows Server then offloads the copy activity to the storage system.

Best Practice
It is best to avoid SnapDrive operations during storage live migration because they might corrupt the virtual machine.

Best Practice
After performing storage migration of a VM from one share to another share, the virtual machine can no longer be restored with the previous Snapshot copies. As a safety net, take a Snapshot/backup copy immediately after the VM storage migration is complete.

Note: After performing storage migration of a VM from one share to another share hosted on a different volume, the SnapMirror and SnapVault relationship needs to be reestablished with the new destination. Also, previously existing Snapshot copies cannot be restored from the SnapVault storage system.

Version History

Version	Date	Document Version History
Version 1.0	August 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®