NetApp
Go further, faster

Technical Report

SnapManager 2.0 for Virtual Infrastructure Best Practices

Amrita Das, NetApp
January 2010 | TR-3737

LEVERAGING NETAPP DATA ONTAP FOR VMWARE BACKUP, RESTORE, AND DISASTER RECOVERY

Backups, restores, and disaster recovery can place a huge overhead on the VMware® virtual infrastructure. NetApp® SnapManager® for Virtual Infrastructure (SMVI) simplifies and automates the backup process by leveraging the underlying NetApp Snapshot™, SnapRestore®, and FlexClone® technologies to provide fast, space-efficient, disk-based backups and rapid, granular restore and recovery of virtual machines and the associated datastores. This document details the best practices for deploying and using SnapManager 2.0 for Virtual Infrastructure.

TABLE OF CONTENTS

1 INTRODUCTION

With the adoption of virtualization technologies, datacenters have been transformed and the number of physical servers drastically reduced. Virtualization has had many positive effects, not only in reducing the number of physical systems, but also in reducing network, power and administrative overhead.

In contrast to physical environments, where server resources are underutilized, fewer resources are available in virtualized environments. Where each physical server had dedicated network and CPU resources, virtual machines (VMs) must now share those same resources. This can result in performance issues, especially while backing up the virtual environment because many virtual machines impact host network and CPU resources concurrently. As a result, backups that once completed during non-business hours have seen their backup window grow.

NetApp SnapManager for Virtual Infrastructure addresses the resource utilization issue typically found within virtual environments by leveraging the underlying NetApp Snapshot technology , which enables you to create point-in-time copies of your virtual machines or entire data stores and then restore from these backup copies at any level of granularity— datastore, VM, disk (VMDK), or guest file —simply and quickly when required .This is all done on our storage systems, freeing your servers to run applications, not backups. SMVI can be quickly installed and configured for use in a new or existing VMware environment saving valuable time during backups and allowing quick and efficient restorations, thus reducing administrative overhead.

1.1 PURPOSE AND SCOPE

The purpose of this report is to provide best practices for deploying SMVI to back up and recover VMware virtual machines and their associated datastores. In addition, this report provides NetApp best practices for protecting the SMVI server and recovering in the event of a disaster. For detailed instructions on installation and configuration, please refer to the “SnapManager for Virtual Infrastructure Installation and Administration Guide.”

1.2 INTENDED AUDIENCE

This document is intended for VMware administrators, storage administrators, backup administrators, and architects implementing a backup, restore and disaster recovery solution for VMware environments running on NetApp storage. Readers should ideally have a solid understanding of the architecture, administration, and backup and recovery concepts within a VMware environment and should consider reviewing the following:

- Data ONTAP® 7.2 or 7.3 System Administration Guide
- SnapManager 2.0 for Virtual Infrastructure Installation and Administration Guide
- NetApp and VMware Virtual Infrastructure 3 Storage Best Practices
- NetApp and VMware vSphere Storage Best Practices
- Reference Architecture for Virtualizing Microsoft Exchange, SQL Server, and SharePoint on VMware vSphere, NetApp Unified Storage, and Cisco Unified Fabric

2 WHAT'S NEW IN SMVI 2.0

The new features supported in SMVI 2.0 are:

- More granular restore options:
  - Single File Restore (SFR)
  - VMDK restore
- Single wizard for creating manual and scheduled backup jobs
- Per-backup job options:
- Exclude datastores from backup
  - Include independent disks in backups
  - Trigger pre/post /failure scripts during backup process
- Consistent backup naming
- Serialization of VMware snapshots
- ASUP logging
- vFiler™ unit support for multiple IP addresses
- Advanced Find option to find specific backups

3 SMVI SIMPLIFIES BACKUP AND RECOVERY

3.1 CONCEPTS

Backup and Recovery

SnapManager for Virtual Infrastructure provides local backup and recovery capability with the option to replicate backups to a remote storage system via SnapMirror® relationships.

Backups can be performed on individual virtual machines or on datastores with the option of updating the SnapMirror relationship as part of the backup on a per-job basis. Similarly, restores can be performed at a datastore, individual virtual machine, VMDK level or individual file within the guest OS.

With the exception of identifying the relevant vCenter™ server and NetApp storage, very little configuration must be completed before backups can be scheduled within SMVI. No profiles or databases are required because SMVI uses an .XML catalog file to record information such as when a backup was created, which virtual machines or datastores were backed up, and how long each backup should be retained.

Backup Retention Policy

Policies can be created specifying the retention period on a per-scheduled-backup job basis, allowing the administrator flexibility to meet varying service-level agreement levels within their environment. Retention can be specified by number of days or number of backups, or maintained indefinitely until manually deleted.

Alert Notification

Alert notifications are created on a per-scheduled-backup job basis and are sent via e-mail to administrator-defined accounts. Alert notification can be configured so that the specified account is e-mailed after every backup, although NetApp does not recommend this because the number of e-mails can become unmanageable. Configuring alerts to notify administrators after an error or warning within a backup offers a more useful and practical alert level.

3.2 PORT USAGE

For SMVI, make sure the following ports are kept open:

8043: SMVI client uses this port to communicate with the SMVI server

By default, the SMVI server tries to communicate with the NetApp controller on port 443 using HTTPS. If HTTPS is not enabled, it will fall back to HTTP using port 80.

3.3 ARCHITECTURE

Figure 1 illustrates the SnapManager for Virtual Infrastructure architecture and the components that work together to provide a comprehensive and powerful backup and recovery solution for VMware environments.

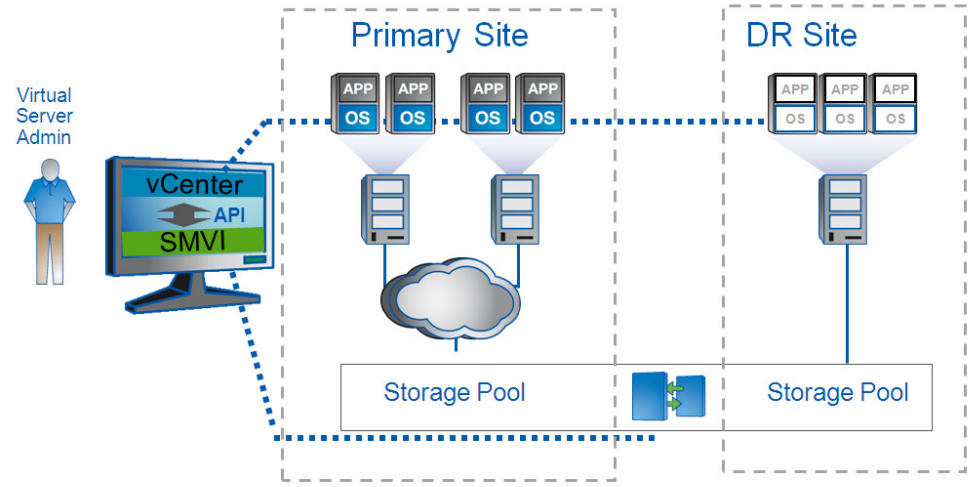


Figure 1) SnapManager for Virtual Infrastructure architecture overview

3.3.1 COMPONENTS

NETAPP DATA ONTAP

SnapManager for Virtual Infrastructure will only function within a NetApp storage environment. SMVI requires that the primary storage, where the virtual machines actually reside, and the secondary storage used as the SnapMirror destination run Data ONTAP® storage software. These storage systems can be either Data ONTAP-specific physical storage systems or vFiler units. SMVI supports Data ONTAP 7.2.x and 7.3.x on physical storage systems and 7.2.4 and above or 7.3.x on vFiler units. In addition, the following licenses are required:

- SnapRestore
- The required protocol license (NFS, FCP, iSCSI)
- SnapMirror (if required)
- FlexClone
  - FlexClone is required for mount operations of NFS datastores. FlexClone is not required for NFS VM in-place VMDK restores (SMVI uses ZAPIs). FlexClone is required for out-of-place NFS VMDK restores. Also FlexClone is optional for mounting VMFS datastores. SMVI uses LUNClone when FlexClone is not available.
  - For SMVI versions 1.2x, FlexClone is needed only if you want to perform NFS datastore mounts. For 2.0, FlexClone is required for NFS datastore mounts and NFS Single File Restore operations, since the SFR workflow internally mounts NFS datastores.

VMWARE VIRTUAL INFRASTRUCTURE

SMVI supports specific VMware versions.

VMware Virtual Infrastructure 3

- VMware ESX 3.5 Update 4 and later
- VMware ESXi 3.5 Update 4 and later
- VMware VirtualCenter 2.5 Update 4 and later

VMware vSphere™ 4

- VMware ESX 4 and later
- VMware ESXi 4 and later
- vCenter Server 4 and later

For the most current information, see the NetApp Interoperability Matrix Tool (IMT) at

http://now.netapp.com/NOW/products/interoperability.

Since SMVI communicates with vCenter rather than individual systems during backups, the clustering of ESX hosts with the high-availability (HA) and Distributed Resource Scheduling (DRS) features enabled is supported. SMVI supports both VMFS datastores over iSCSI and FCP protocols and NFS datastores. Any combination of these datastores and protocol types can be supported by a single SMVI server.

SNAPMANAGER FOR VIRTUAL INFRASTRUCTURE

SnapManager for Virtual Infrastructure has two components:

- SnapManager Server
- SnapManager Client (GUI/CLI)

SMVI can be installed on any Windows® platform (XP, 2003, Vista®, 2008) that has connectivity with the vCenter server. NetApp recommends installing SMVI on the vCenter server when possible to reduce the impact of network outages between the two components. There is no impact on the vCenter service when SMVI is installed on the same server.

SNAPMANAGER FOR VIRTUAL INFRASTRUCTURE REPOSITORY

The SMVI repository consists of several .XML files that are placed on local storage if the default locations are accepted during installation. These files are critical to recovering SMVI should a failure occur at any number of levels. NetApp recommends that the repository files be placed on shared storage, ideally within a Microsoft® Cluster Server (MSCS) if possible, and should be backed up regularly if not. Further details on configuring SMVI for shared storage and cluster configurations can be found within the “Installation and Configuration” section of this report.

4 PLANNING

4.1 STORAGE CONFIGURATION

SnapManager for Virtual Infrastructure seamlessly integrates into the VMware virtualized environment (see section 3.3.1 for supported versions of ESX and vCenter). NFS datastores are supported as well as VMFS datastores accessed via FCP and iSCSI protocols. When deploying the VMware virtual infrastructure on NetApp storage systems that will be supported by SMVI, please review and adhere to the best-practice guidelines outlined in the following documents:

- NetApp and VMware Virtual Infrastructure 3 Storage Best Practices
- NetApp and VMware vSphere Storage Best Practices

Configuring the virtual infrastructure as specified within these guides will not only result in better overall performance when running VMware on NetApp storage systems, but will also enable SMVI backups to run efficiently.

Adding Storage Systems

During the configuration of SnapManager for Virtual Infrastructure all primary and secondary storage must be identified within the Setup window of the GUI or from the command line interface. By default, the root account must be used.

NetApp recommends creating a custom storage account other than root as a security precaution. The steps required for account creation can be found in the SnapManager for Virtual Infrastructure Installation and Administration Guide.

A further step should be taken as a security precaution when configuring SnapManager for Virtual Infrastructure and the associated storage systems. NetApp recommends enabling Secure Sockets Layer (SSL) on all storage systems identified to SMVI. Enabling SSL ensures account passwords are encrypted when transmitted to the storage system.

Step-by-step information on how to enable SSL on a NetApp storage system can be found in the Data ONTAP® 7.2, 7.3, or 7.4 System Administration Guide.

SnapManager for Virtual Infrastructure Data Layout

As NetApp best practices for VMware recommends, transient and temporary data such as the guest operating system swap file, temp files and pagefiles, should be moved to a separate virtual disk on a different datastore as snapshots of this type of data can consume a large amount of storage in a very short period of time due to the high rate of change.

When a backup is created for a virtual machine with SnapManager for Virtual Infrastructure, SMVI is aware of all VMDKs associated with the virtual machine and will initiate a NetApp Snapshot copy on all datastores upon which the VMDKs reside. For example, if a virtual machine running Windows as the guest operating system has its C drive on datastore ds1, data on datastore ds2 and transient data on datastore td1, SnapManager for Virtual Infrastructure will create a NetApp Snapshot copy against all three datastores at the underlying volume level. This defeats the purpose of separating temporary and transient data.

In order to exclude the datastore containing the transient and temporary data from the SnapManager for Virtual Infrastructure backup, NetApp recommends configuring the VMDKs residing in the datastore as “Independent Persistent” disks within vCenter. Once configured, the transient and temporary data VMDKs will be excluded from both the VMware vCenter snapshot and the NetApp Snapshot copy initiated by SnapManager for Virtual Infrastructure.

NetApp also recommends creating a datastore dedicated to transient and temporary data for all virtual machines with no other data types or VMDKs residing upon it. This will avoid a Snapshot copy being taken against the underlying volume as part of the backup of another virtual machine. NetApp recommends not deduping the data on this datastore. SnapManager 2.0 for Virtual Infrastructure has the option to include independent disks and exclude datastores from backup. This is covered in more detail in section 6.5.

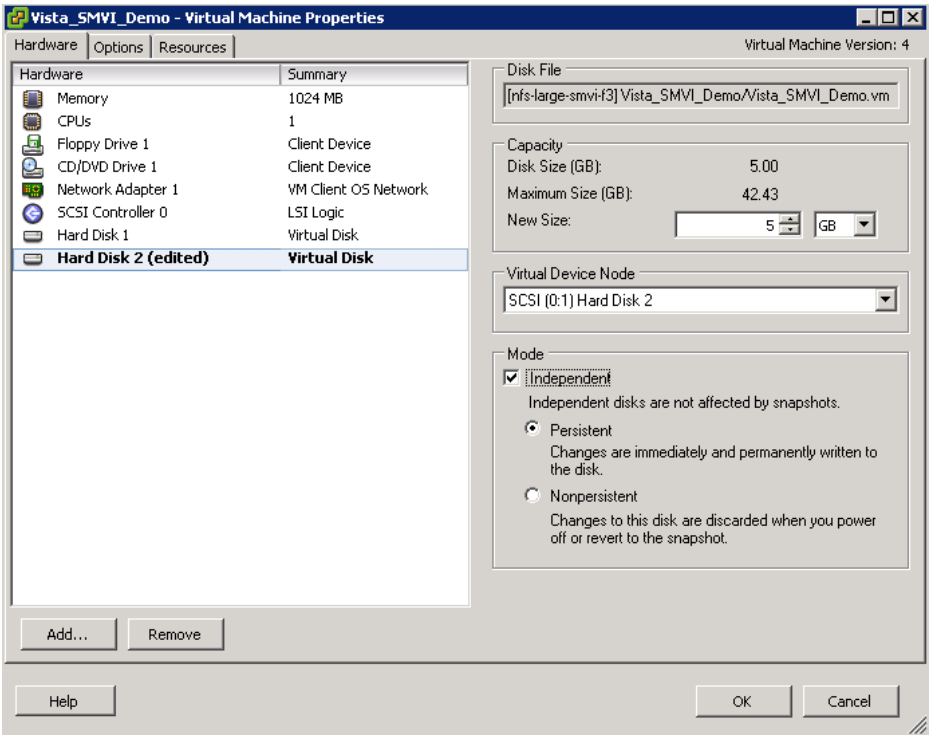


Figure 2) vCenter configuration of an independent disk

4.2 VCENTER CONFIGURATION

After installing SnapManager for Virtual Infrastructure you must configure it for the specific environment. As part of this configuration, a vCenter server must be identified. SMVI can only communicate with one vCenter server at a time.

In many environments, more than one vCenter server is in use. Since SMVI can communicate only with one vCenter server at a time, NetApp recommends installing one SMVI server per vCenter server. This will enable all scheduled backups to run successfully while ease of administration is maintained. It should be noted that this configuration will not increase the cost of the solution, because SMVI is licensed on a per-ESX host or storage-tier basis, rather than on a per-SMVI server basis.

Although the specified vCenter server within SMVI can be changed from both the GUI and the CLI, NetApp does not recommend it in an environment with multiple vCenter servers. This is because all jobs scheduled to run against a vCenter server that's not currently specified within the SMVI setup will fail.

4.3 VCENTER USER PERMISSIONS

The SMVI vCenter connection account requires the following vCenter permissions for ESX 4.0

- DATASTORE
  - Remove Datastore
  - Browse Datastore
  - Remove File
  - Rename Datastore

- HOST
  - Configuration
    - Storage Partition Configuration
    - Advanced Settings
    - Change Settings

- VIRTUAL MACHINE
  - Interaction
    - Power off
    - Power on
  - Configuration
    - Add Existing Disk
    - Add New Disk
    - Remove Disk
    - Add or Remove Device
    - Advanced
  - State
    - Create Snapshot
    - Remove Snapshot
    - Revert to snapshot

4.4 DISTRIBUTED RESOURCE SCHEDULER IMPLICATIONS

VMware's Distributed Resource Scheduler, or DRS, pools the resources of ESX hosts within a cluster, dynamically migrating virtual machines via VMotion™ to ensure optimal resource availability and virtual machine performance.

Within a DRS configuration there are three possible levels of automation, as detailed below:

- **Manual**—vCenter makes recommendations about which virtual machines should be migrated; however, migrations are manually implemented by an administrator.
- **Partially Automated**—Virtual machines are automatically placed onto an ESX host within the cluster by vCenter during power on. However, migrations are recommendations only and must be manually implemented by an administrator.
- **Fully Automated**—Virtual machines are automatically placed onto ESX hosts at power on and are automatically migrated to attain the best use of resources.

Within a Fully Automated configuration there are five possible levels of aggression that can be selected to determine the threshold for moving virtual machines. The sliding scale ranges in aggression from most conservative, where vCenter only migrates virtual machines to satisfy cluster constraints, to most aggressive, where vCenter automatically applies recommendations that promise even a slight improvement to the cluster's load balance.

Depending on the environment, the level of aggression selected has a direct effect on the number of migrations that will occur. In some cases, when the highest level of aggression has been selected, virtual machines are constantly undergoing migration. This constant migration can cause performance problems within the VMware environment due to the level of overhead involved in migrating a virtual machine. It can also cause errors to occur during an SMVI backup job.

SnapManager for Virtual Infrastructure is VMotion aware; as long as the storage system a datastore resides upon is known to SMVI it does not matter which host a virtual machine resides upon. However, SMVI cannot back up a virtual machine that is actively undergoing migration. Should a backup run against a datastore that has virtual machines actively being migrated, an error will be generated and those particular virtual machines will not be backed up. As a result, the level of aggression and the number of migrations occurring should be carefully monitored. Should backups begin to experience errors when DRS is configured in Fully Automated mode, NetApp recommends scaling back the level of aggression so that virtual machines are migrated only when a significant gain in performance can be achieved. This will improve not only the success rate of the backups, but the overall virtual machine performance as well.

5 SMVI INSTALLATION

There are a number of different options when installing SnapManager for Virtual Infrastructure, ranging from the default installation on local disk to a clustered configuration with a Microsoft Cluster Server

Although all installations depicted within this section are fully supported, NetApp recommends installing SMVI with the catalog files residing upon shared storage. This provides quick and easy recovery of the SMVI server and its associated backup files in the event of a failure.

5.1 INSTALLING VIRTUALCENTER AND SMVI ON A VIRTUAL MACHINE

VCENTER IN A VIRTUAL MACHINE

Running VMware vCenter within a virtual machine is fully supported by VMware to the same degree as if it were installed on a physical server. However, there can be ramifications in a SnapManager for Virtual Infrastructure environment if VMware's best practices for installing vCenter on a virtual machine are not strictly adhered to.

Specifically, the database associated with vCenter must not be installed on a virtual machine protected by SMVI, but rather should be installed on a physical system. Should the database be installed in a virtual machine backed up by SMVI, vCenter will fail due to vCenter timeouts caused by the VMware snapshot process

Further information on running VirtualCenter within a virtual machine can be found in a VMware Technical Note titled Running VirtualCenter in a Virtual Machine.

SMVI IN A VIRTUAL MACHINE

Installing SnapManager for Virtual Infrastructure within a virtual machine is fully supported, and the installation process is identical to that of a physical machine. Just as NetApp recommends installing both SMVI and vCenter on the same physical server, NetApp also recommends installing both SMVI and vCenter on the same virtual machine.

Although SnapManager for Virtual Infrastructure is supported when running within a virtual machine, additional steps must be taken if SMVI will be "backing up itself" to avoid potential issues after a restore of the SMVI virtual machine. Note: SMVI "backing up itself" works for crash consistent snapshots. NetApp recommends using the Windows native backup utility within the guest or some other backup application.

When the virtual machine running SnapManager for Virtual Infrastructure is backed up by SMVI, the current state of the SMVI backup workflow is captured within the Snapshot copies. Should the virtual machine be restored at a later date, SMVI within the virtual machine assumes that the host has failed in mid-workflow and attempts to resume backups at the point at which the Snapshot copy was taken. This can cause backups to run multiple times even if they were originally successful.

To prevent this issue, NetApp recommends taking the following steps when SnapManager for Virtual Infrastructure is installed on a virtual machine:

1. Set the Startup Type of the SnapManager VI Windows Service to Manual. This will prevent SnapManager for Virtual Infrastructure from restarting automatically when the virtual machine it's installed on is powered up after it has been restored.
2. After restoring the SMVI virtual machine, power the VM on and remove the contents of the %PROGRAMFILES%\NetApp\SMVI\server\crash directory. SMVI uses this directory after a crash to resume failed backups.
3. Start the SnapManager VI Windows Service.

NetApp also recommends monitoring the backup of the virtual machine containing SnapManager for Virtual Infrastructure. Should timeouts occur during the VMware snapshot process, configure the backups to run with the VMware snapshots disabled on the individual virtual machine.

5.2 DEFAULT INSTALLATION

SnapManager 2.0 for Virtual Infrastructure is easy to install and configure. A brief overview of the steps involved in the installation of SMVI is provided below. For more detailed instructions please follow the steps listed in the SnapManager for Virtual Infrastructure Installation and Administration Guide.

1. Verify that all the prerequisites mentioned in the installation and administration guide have been met. Make sure that:
    a. The vCenter and ESX versions are supported by SMVI

b. Data ONTAP is installed on the NetApp storage system(s) and the following licenses are enabled:

   i. The correct protocol (FCP, iSCSI or NFS)

   ii. SnapRestore

   iii. SnapMirror (as required)

   iv. FlexClone

2. Download the appropriate SnapManager 2.0 for Virtual Infrastructure software from the NetApp NOW™ (NetApp on the Web) site. Follow the instructions within the Installation and Administration Guide to install SMVI.

5.3 CONFIGURING SMVI FOR SHARED STORAGE

If shared storage is available, NetApp recommends that the SMVI server be installed and configured with the configuration files residing on the shared storage. These steps are for disks that have been formatted by the OS and will not be supported for mapped drives or mount points.

In the steps provided below, the shared storage device is depicted as the H drive.

1. Install SMVI as per the SMVI Installation and Administration Guide on the desired target system.

2. Stop the SnapManager VI Windows service

3. Within a directory residing upon shared storage create the following directories:
   a. H:\NetApp\SMVI\server
   b. H:\NetApp\SMVI\server\etc (stores credentials for vCenter)
   c. H:\NetApp\SMVI\server\repository (stores backup catalogs)
   d. H:\NetApp\SMVI\server\crash (stores required files to resume operation)

4. Update the SMVI configuration files to identify the new location of the repository and crash folders on the shared storage. The following two files need to be edited:
   a. %PROGRAMFILES%\NetApp\SMVI\server\etc\smvi.config
   b. %PROGRAMFILES%\NetApp\SMVI\server\etc\smvi.override

5. Two parameters must be changed within the smvi.config file to reflect the path to the shared storage: (This parameter will have C: entered after a default installation)
   a. smvi.repository.path=H:\\NetApp\\SMVI\\\server\\repository
   b. flow.persistence.embedded.storageLocation=H:\\NetApp\\SMVI\\\server\\crash
      This should match the changes made to the smvi.config and smvi.override files

6. One parameter must be changed within the smvi.override file to reflect the path to the shared storage: (This parameter will have the C: entered after a default installation)
   a. credential.persistence.file.path=H:\\NetApp\\SMVI\\\server\\etc\\cred
7. Copy the credential file from c:\program files\netapp\smvi\server\etc to the \etc directory in the new path structure. If this is not done then use the CLI to set the vcserver IP address and credentials

8. Start the SnapManager VI Windows service

9. SMVI will now be configured to use the shared storage. Recovering from the loss of the SMVI Server when using this configuration is covered in Appendix A

5.4 CONFIGURING SMVI IN A CLUSTERED ENVIRONMENT (MSCS)

SnapManager for Virtual Infrastructure can be installed within a Microsoft Clustered Solution, if desired. The following section details the configuration of the SnapManager for Virtual Infrastructure server in a Microsoft clustered environment. In this example, the following assumptions are made:

- Windows 2003 Server SP2. In this example, a two node cluster is assumed. Regardless of the Windows operating system selected, refer to the Microsoft “Cluster Administration Guide” for cluster configuration instructions.
- You have access to shared storage, specifically a LUN created on shared storage mounted as drive letter Q to be used as the cluster’s quorum disk, and a second device on which to place SMVI’s configuration files
- The Cluster Administration Utility has been used to configure basic MSCS resources.
- A domain account has been created with access to the vCenter server

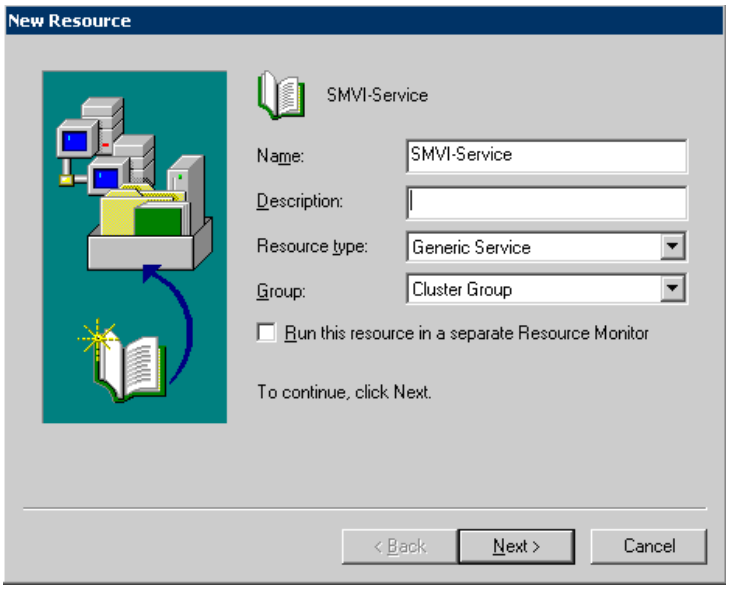
Once the cluster has been configured and tested, the following steps should be used to configure and test SnapManager for Virtual Infrastructure. As depicted in section 5.3 above, the H drive represents the shared storage device available for the SMVI configuration files.

SNAPMANAGER FOR VIRTUAL INFRASTRUCTURE CONFIGURATION

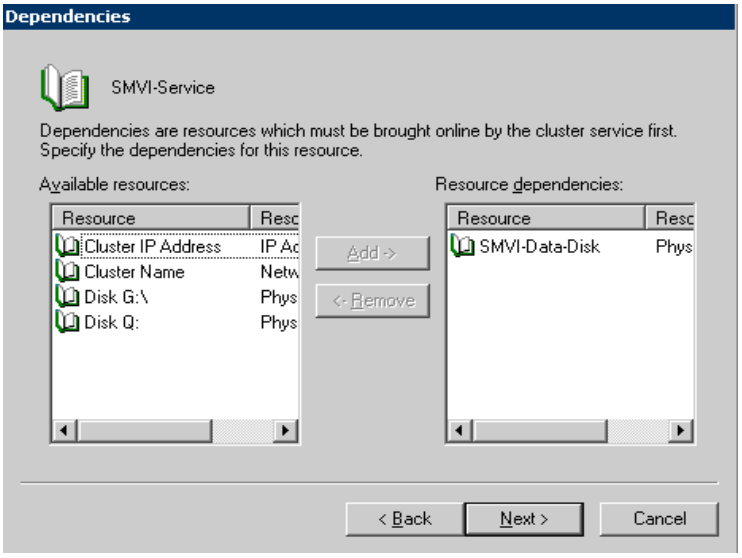
1. Perform a full install of SnapManager for Virtual Infrastructure as per the SnapManager for Virtual Infrastructure Installation and Administration Guide on both nodes within the cluster.
2. Follow steps 3–6 in section 5.3, “Configuring SMVI for Shared Storage”, on both cluster nodes.
3. Restart the SnapManager VI Windows service on node 1; this will reconfigure SMVI to use the folders created on the shared drive.
4. Stop the SnapManager VI Windows service on node 2.

CONFIGURE CLUSTER RESOURCES FOR THE SNAPMANAGER FOR VIRTUAL INFRASTRUCTURE SERVER

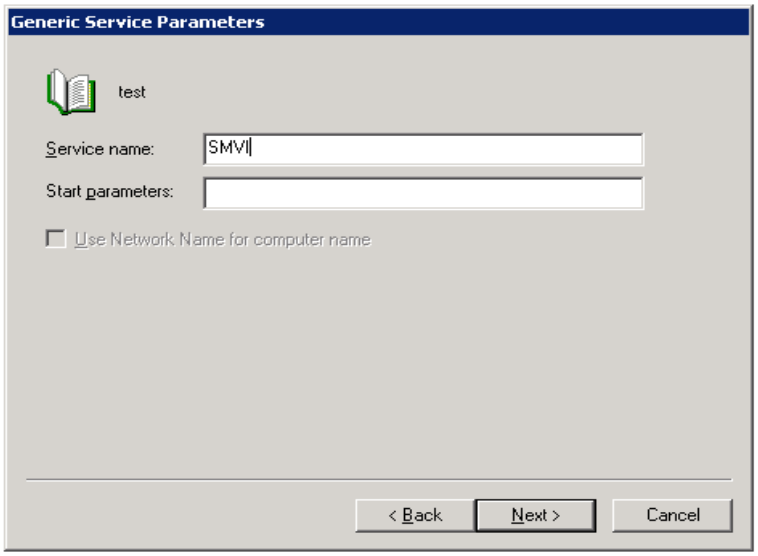
1. Start the Cluster Administrator and connect to the appropriate cluster.
2. Expand Groups in the left window pane of Cluster Administrator.
3. Right-click on the Cluster Group and select New → Resource.
4. Enter the following information in the New Resource window:



5. Ensure that all the cluster nodes appear under the “Possible Owners” list. Move cluster nodes from “Available Nodes” to “Possible Owners” as necessary.
6. Within the Dependencies window select the shared H: drive containing SnapManager for Virtual Infrastructure’s configuration files. In the example shown below, the H: drive has been named SMVI-Data-Disk within the cluster.



7. Enter the Service Name as SMVI and leave the Service Parameters field blank.



8. Leave the Registry Replication window blank and click Finish.
9. Bring the resource online by right clicking on SMVI-Service → Bring Online.

CONFIRM SNAPMANAGER FOR VIRTUAL INFRASTRUCTURE HIGH AVAILABILTIY

Once the SnapManager for Virtual Infrastructure cluster resource has been configured as described above, follow the steps listed below to test the configuration and determine that SMVI is running in a high availability mode.

1. Start the SnapManager for Virtual Infrastructure GUI on either node or on a client system with network connectivity to the cluster. Then connect to the SMVI server specifying the cluster's virtual IP address.
2. Within the Setup window of SMVI, enter the appropriate vCenter and storage information. Instructions on how to configure SMVI can be found within the SnapManager for Virtual Infrastructure Installation and Administration Guide.
3. Perform a backup using SnapManager for Virtual Infrastructure.

4. Failover the cluster group to the second node. Once the failover is complete connect to the cluster's virtual IP address and ensure that the backup taken in step 4 is available for restore

5.5 CHOOSING BETWEEN THE GUI AND THE CLI

All SnapManager for Virtual Infrastructure commands can be performed using either the GUI or the CLI with some exceptions. The creation of scheduled jobs and their associated retention policies and Single File Restore can only be performed through the GUI.

A detailed listing of all commands available via the CLI can be found in the "SMVI Installation and Administration Guide" available on the NOW site.

6 THE SMVI PROCESS FLOW

6.1 THE BACKUP PROCESS AND IMPLICATIONS

SnapManager for Virtual Infrastructure leverages NetApp Snapshot technology to create fast and space-efficient backups of VMware datastores and their associated virtual machines. These backups offer point-in-time images, or copies, of the virtual machines and are stored locally on the same storage platform on which the datastores physically reside.

In addition to the Snapshot copy stored locally, SnapManager for Virtual Infrastructure also provides an option to update an existing SnapMirror relationship upon the completion of a backup. This can be selected on a per-backup-job basis as required by the administrator.

The backup process flow is identical for both a manual and a scheduled backup job.

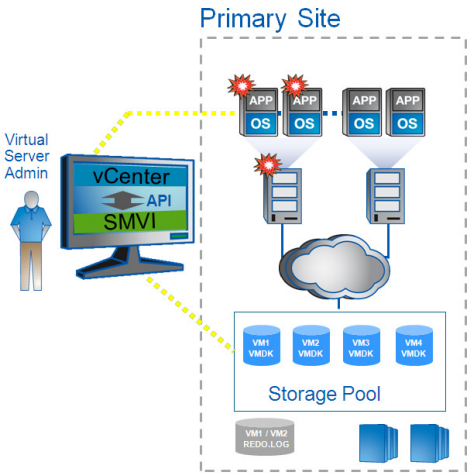


Figure 3) Virtual infrastructure and associated storage during an SMVI backup

Figure 3 represents a high-level overview of the typical SnapManager for Virtual Infrastructure architecture on the primary site storage and will be used in detailing the backup process flow.

1. A backup is initiated within SMVI.
    i. Individual VM(s) backup – A VMware snapshot will be created for each virtual machine selected for backup that is powered on at the time of backup.

ii. Datastore backup – A VMware snapshot will be created for every virtual machine that is powered on within the datastore that has been selected for backup.

iii. Regardless of backup type, virtual machines that are powered off during a backup will be backed up; however no VMware snapshot is required.

2. The VMware snapshot preserves the state of the virtual machine and is used by SMVI during restores to revert the virtual machine back to the backup point-in-time state.

   VMware snapshots initiated by SMVI capture the entire state of the individual virtual machines, including disk and settings state; however additional steps must be taken to quiesce an application within a virtual machine. Information on application consistency is provided in section 9 of this document. SMVI also gives users the option to disable VMware snapshots and just take a NetApp Snapshot copy on the volume underlying the datastore.

3. Once all the VMware snapshots have completed for a datastore, SMVI initiates a NetApp Snapshot copy on the volume underlying the datastore. The NetApp Snapshot copy is at the volume level regardless of the type of backup selected: individual virtual machine(s) or datastore.

   During the backup of a virtual machine with VMDKs residing upon multiple datastores, SnapManager for Virtual Infrastructure initiates a NetApp Snapshot on all the underlying volumes. As a result, multiple datastores are displayed within SMVI's restore window regardless of how many datastores were selected for backup.

4. Upon completion of the NetApp Snapshot copy, SMVI removes the VMware vCenter snapshot to reduce space and performance overhead. Although the vCenter snapshot is removed within vCenter, one VMware snapshot is maintained within the backup for each virtual machine that was in a powered-on state. This snapshot is maintained so it can be used by the restore process to revert the virtual machine to its point-in-time state.

5. Upon completion of the local backup, SnapManager for Virtual Infrastructure updates an existing SnapMirror relationship on the volume underlying the datastore if the SnapMirror option was selected. SnapMirror is discussed in further detail in a later section of this document.

Backup Process Implications

As documented above, the process flow is similar regardless of the type of backup performed: individual virtual machine(s) or datastore. However, the number of virtual machines that will undergo a VMware vCenter snapshot will vary depending on the type of backup selected, as will the number of NetApp Snapshot copies per volume.

When an individual virtual machine is selected for backup, only that virtual machine has a VMware vCenter snapshot created. As a result, only the selected virtual machine will be available for restoration, even though the entire underlying datastore volume was protected via a NetApp Snapshot copy.

Conversely, when a datastore is selected for backup, every virtual machine in the datastore in a powered-on state has a VMware vCenter snapshot created, before a single NetApp Snapshot copy of the volume is performed.

Unlike the individual virtual machine backup, any virtual machine that resided upon the specified datastore can be selected for restoration. The entire datastore need not be restored unless required; individual virtual machines can be selected from the backup as necessary.

NetApp recommends that datastore-level backups be configured whenever possible, especially for scheduled backups. This not only reduces administrative overhead by lessening the number of backups that need to be configured and tracked, but also reduces the number of NetApp Snapshot copies per volume. Multiple NetApp Snapshot copies of the volume are required if each virtual machine is selected for backup individually, rather than the single NetApp Snapshot copy required per datastore backup.

Reducing the number of NetApp Snapshot copies per volume increases the number of backups that can be retained.

To reduce both storage and administrative overhead as well as increase the restoration options available to the administrator, NetApp recommends configuring datastore-level backups as much as practically possible.

Note: For SMVI the first 24 characters of a datastore should be unique

6.2 SCHEDULED BACKUPS AND RETENTION POLICIES

The limit of 255 NetApp Snapshots per volume must be taken into consideration when scheduling backups and configuring the associated retention policies. The number of Snapshot copies per volume can be managed with the proper scheduling and retention policies on a per-scheduled-backup basis while still meeting Service level agreements (SLAs) on the virtual machines.

BACKUP SCHEDULING

Five scheduling options are available when creating a backup within SMVI:

- Hourly
- Daily
- Weekly
- Monthly
- None

The frequency of the backup has a direct bearing on the number of NetApp Snapshot copies taken on the underlying volume, regardless of the type of backup performed: individual VM(s) or datastore.

The backup frequency, as well as the number of different backups performed against a datastore – for example one backup running against datastore ds_1 weekly and another monthly – must be taken into account when specifying the retention policy so as not to exceed the maximum number of Snapshots per volume. Should the number of Snapshot copies exceed 255 on any given volume, future backups against that volume will fail. Selecting the None option and choosing to delete the job are equivalent to the manual backup-job creation option.

RETENTION POLICIES

Three options available to the administrator when configuring retention polices for a scheduled backup:

- Maximum number of days
- Maximum number of backups
- Indefinitely

NetApp recommends using the policies not only to meet specific SLAs, but also to maintain a supported number of NetApp Snapshots on the underlying volumes. This can be achieved by using either of the first two options listed above. For example, setting a retention policy of 30 backups on an hourly backup will limit the maximum number of Snapshots associated with the backup to 30. However, if the retention policy had been configured as 30 days, the Snapshot limit per volume would be reached after 10 days and backups would begin to fail from that point on (24 backups per day would reach the 255 Snapshot limit on the 11th day).

The third option, indefinitely, should be used with caution. When selecting this option, backups and the associated NetApp Snapshot copies are maintained until manually deleted by the administrator. These Snapshot copies are included in the maximum number supported on a volume. Of further note, the NetApp Snapshot copies associated with manual backups must also be considered when determining the number of Snapshot copies maintained against a volume.

6.3 SNAPSHOT NAMING

SMVI 2.0 includes the following changes to the snapshot naming convention

- Jobs scheduled via GUI have the snapshot naming pattern "smvi_{jobName}_[novmsnap]_{date}{time}". A job has multiple backups associated with it, taken at different times depending on the schedule, only the most recent backup of the job has snapshots with the name "smvi_{jobName}_[novmsnap]_recent". When the job runs the next time, the current recent Snapshot copy of the job is renamed to smvi_{backupName}_[novmsnap]_{date}{time}, where {date}{time} is the start time of the backup. The [novmsnap] String is inserted depending on whether VMware Snapshots were taken for that particular backup.
- Manual backups done through the CLI have the snapshot naming pattern "smvi_{backupName}_{date}{time}". Manual backups never have recent in their snapshot names.

6.4 SCRIPTING

SnapManager for Virtual Infrastructure provides users the ability to run pre-, post- and failure backup phase scripts. These 'scripts' are any executable process on the operating system in which the SMVI server is running. When defining the backup to run, the pre, post and failure backup scripts can be chosen using either the SMVI GUI or CLI. The scripts must be saved in the <SMVI Installation>/server/scripts/ directory. Each chosen script runs as a pre-, post- and failure backup script.

From the GUI, the user can select multiple scripts using the backup creation wizard or when editing an existing backup job. The UI will list all files found in the server/scripts/ directory. SMVI runs the scripts before creating the VMware snapshots and after the cleanup of VMware snapshots.

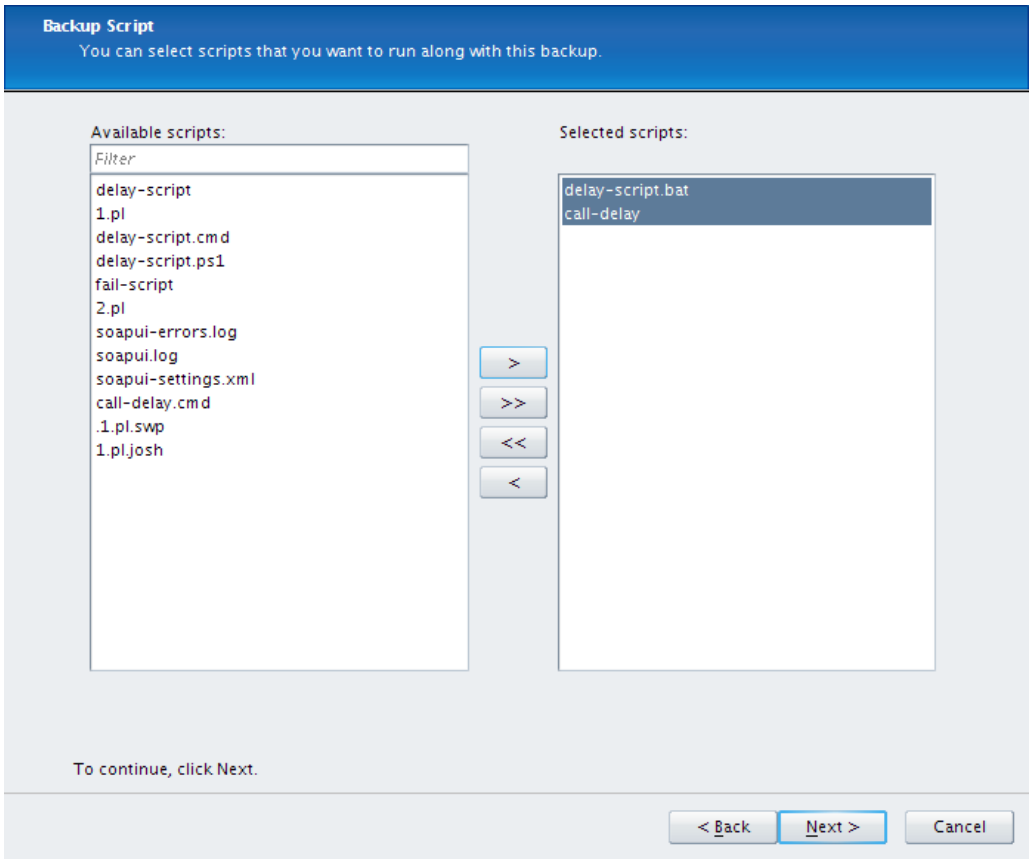


Figure 4) Select backup scripts from the GUI

When SMVI starts each script, a progress message will be logged indicating the start of the script. When the script completes, or is terminated by SMVI since it was running too long, a progress message will be logged to indicate the completion of the script and if the script was successful or failed. If a script is defined for a backup but is not found in the scripts directory, a message will be logged stating that the script cannot be found. The SMVI server will maintain a global configuration value to indicate the amount of time that a script can execute. Once a script has run for this length of time, the script will be terminated by the SMVI server in order to prevent run away processing by scripts. If the SMVI server has to terminate a script, it will implicitly be recognized as a failed script and may force termination of the SMVI backup in the pre-backup phase. With the default settings, SMVI will wait for up to 30 minutes for each script to complete in each phase. This default setting can be configured using the following entry in the server/etc/smvi.override file.

smvi.script.timeout.seconds=1800

SMVI backup scripts will receive inputs from environment variables. This will allow sending the inputs in a way that avoids CLI line length limits. The set of variables will vary based on the backup phase.

Environment Variables

The scripts can expect the following environment variables in the appropriate phases.

Table 1) List of environment variables

Variable	Content	Format	Phase
BACKUP_NAME	Name of the backup		All phases
BACKUP_DATE	Date of the backup	Yyyymmdd	All phases
BACKUP_TIME	Time of the backup	HHMMss	All phases
BACKUP_PHASE	Phase of the backup	PRE_BACKUP, POST_BACKUP or FAILED_BACKUP	All phases
VIRTUAL_MACHINES	The number of VM's in the backup		All phases
VIRTUAL_MACHINE.#	One of the defined virtual machines	Uses the fixed format <VM name>|<VM UUID>|<power state - POWERED_ON|POWERED_OFF|SUSPENDED>|<VM snapshot will be taken - true|false>|<ip addresses>.	All phases
STORAGE_SNAPSHOTS	The number of storage snapshots in the backup		POST_BACKUP
STORAGE_SNAPSHOT.#	One of the defined storage snapshots	Uses the standard convention of <filer>:/vol/<volume>:<ONTAP snapshot name>.	POST_BACKUP

Sample environment variables and sample scripts are available in Appendix D. The sample SMVI SnapVault® script is available in Appendix E.

Upon completion of the script, SMVI expects an exit value of zero (0) to indicate success. Any exit value other than zero (0) will indicate a failure by the script. If a script fails in the PRE_BACKUP phase, the SMVI backup will fail. Script failures in the POST_BACKUP phase will result in a WARN message but will not fail the backup. Scripts may write output to stdout/stderr. This output will be read by the SMVI server and will be collected for each script that is run. The entire contents of stdout/stderr will be logged in the SMVI server log file along with the exit value of the script.

The most common problem is that the script is written in a particular language, but the required binaries for that language are not on the system PATH. NetApp recommends a quick check to open a command prompt and type echo %PATH'%. If the path to the language is not on the path, it must be added. Another check is to create a .cmd script which echoes the input variables, including PATH. Then a backup can be run with this script and the output can be viewed from the SMVI server log file. If a script is developed using perl, do not use backticks (``) to run another process: instead, use the system() call.

When running a backup from the CLI, a new option is available to define which scripts are run as both pre- and postbackup scripts:

Smvi backup create

[-scripts {script name} [script name ...]

: (optional) name of the scripts to run with this backup, multiple script names can be specified. The script name must match the name of the script as found on the SMVI server. Only include the script name, not the path to the script. Scripts must reside in the scripts directory on the SMVI server and cannot be in a sub folder. The order in which scripts are run is not guaranteed.

Error Messages

All output messages from the scripts are stored in the SMVI log. If a script fails in the pre backup phase, the backup will fail with a message similar to the following.

```
smvi backup create -id Empty-Test-VM-1 -scripts fail-script
[08:15] Starting backup request
[08:15] Excluding datastore Development (Backup backup_josh-test-schedules_20090729144239) from the backup for virtual machine Empty-Test -VM-1. Empty-Test-VM-1 has only independent disks on Development (Backup backup_josh-test-schedules_20090729144239).
[08:15] Backing up datastore(s) ([Development (netfs://10.60.231.19//vol/jb_smvi_datastore2/)])
[08:15] Backing up the following virtual machine(s) ([Empty-Test-VM-1])
[08:15] Script fail-script is starting in phase PRE_BACKUP
[08:15] [ERROR] Script fail-script failed with exit code 1
[08:15] Script fail-script is starting in phase FAILED_BACKUP
[08:15] Script fail-script completed successfully in phase FAILED_BACKUP
[08:15] Storing logs for backup_5c03867780fc40811168da12e907159d in file ./repository/logs/unscheduled/backup_backup_5c03867780fc40811168da12e907159d.xml
SMVICLI-0101: Command failed
```

Failures in the post backup phase will not fail the backup. An example of a post backup phase failure output is:

```
smvi backup create -id Empty-Test-VM-1 -scripts fail-script
[08:20] Starting backup request
[08:20] Excluding datastore Development (Backup backup_josh-test-schedules_20090729144239) from the backup for virtual machine Empty-Test-VM-1. Empty-Test-VM-1 has only independent disks on Development (Backup backup_josh-test-schedules_20090729144239).
[08:20] Backing up datastore(s) ([Development (netfs://10.60.231.19//vol/jb_smvi_datastore2/)])
[08:20] Backing up the following virtual machine(s) ([Empty-Test-VM-1])
[08:20] Script fail-script is starting in phase PRE_BACKUP
[08:20] Script fail-script completed successfully in phase PRE_BACKUP
[08:20] Creating storage snapshots for all datastores/virtual machines that are being backed up.
[08:20] Script fail-script is starting in phase POST_BACKUP
[08:20] Script fail-script failed with code 1 in phase POST_BACKUP
[08:20] Storing logs for backup_449142621bee95e72b598e8e45bad68c in file ./repository/logs/unscheduled/backup_backup_449142621bee95e72b598e8e45bad68c.xml
[08:20] Backup backup_449142621bee95e72b598e8e45bad68c of datastores/virtual machines is complete.
SMVICLI-0100: Command completed successfully
```

6.5 INCLUDE INDEPENDENT DISKS AND EXCLUDE DATASTORES

NetApp recommends creating a datastore dedicated to transient and temporary data for all virtual machines with no other data types or VMDKs residing upon it. This is done in order to avoid a Snapshot copy being performed on the underlying volume as part of the backup of another virtual machine. NetApp recommends excluding datastores that contain transient and temporary data from the backup, this ensures that snapshot space is not wasted on transient data with a high rate of change. In SMVI 2.0, when selected entities in the backup span multiple datastores, one or more of the spanning datastores may be excluded from the backup. Once configured, the transient and temporary data VMDKs will be excluded from both the VMware vCenter snapshot and the NetApp Snapshot copy initiated by SnapManager for Virtual Infrastructure. In SMVI 1.0 datastores with only independent disks were excluded from the backup. In SMVI 2.0 there is an option to include them in the backup. Datastores with a mix of independent disks and normal disks or configuration files for a VM are included in the backup irrespective of this option.

In case you have a normal disk and an independent disk for backup on the same datastore, this datastore is always included for backup irrespective of the "include datastore with independent disk" option. NetApp recommends that a separate datastore be designated exclusively for swap data or system data.

Note: If you exclude non-independent disks from the backup of a VM, that VM cannot be completely restored. Only virtual disk restore and single file restore can be performed from such a backup.

6.6 MOUNTING A BACKUP AND ITS USES

SnapManager for Virtual Infrastructure provides the option of mounting a backup. The mounted backup is a clone of the protected datastore. Once mounted, the backup is displayed within vCenter and can be browsed in the same manner as a standard datastore. The mount operation can be used to verify the contents of a backup.

To mount a backup, complete the following steps:

1. In the Datastores pane of the Restore window, select a datastore to display a list of its backups in the Backups pane.
2. In the Backups pane, select the backup that should be mounted
3. Click on Mount
4. When prompted, enter the name of the ESX server on which you want to mount the datastore.
5. Browse the mounted backup through vCenter in the same manner as you would a standard datastore.

6.7 SINGLE FILE RESTORE

SMVI 2.0 supports restoring one or more files from the virtual machine without having to restore the entire virtual machine.

PRE-REQUISITES FOR SFR

- There is an existing process (for example, helpdesk/ticketing system) that will be used by end users to initiate file restore requests.
- The authentication and authorization of the end user to be able to restore files belonging to a particular VM will be done by this external tool / process, which may be different for every enterprise and is outside the scope of SMVI.
- When the request to restore files on the guest OS comes to the SMVI administrator through this tool, it is assumed that the user asking for the restore of files of the particular guest OS is authorized to do so.

TYPES OF FILE RESTORE SESSIONS

SnapManager for Virtual Infrastructure automates the process of restoring single files based on the relationship between the source virtual machine (which was backed up) and the destination virtual machine (the VM to which files will be restored). The source and destination VM can be the same or different virtual machines.

SnapManager for Virtual Infrastructure supports three types of restore sessions.

Self Service
The SnapManager for Virtual Infrastructure administrator creates a restore session using SMVI. Users can then install the Restore Agent (RA) on the destination virtual machine, browse the mounted backups on a guest virtual machine, and restore the individual disk file.

Administrator Assisted
This type of file restoration is basically the same as self-service, except that the SnapManager for Virtual Infrastructure administrator runs the Restore Agent and copies the restored files to a shared location that the user has access to.

Limited Self-Service
The SnapManager for Virtual Infrastructure administrator finds the backup copy within a user-specified range of backups and attaches the backed-up disks to the destination virtual machine. The users can then run Restore Agent on a destination virtual machine, browse the mounted backups, and restore the individual disk file.

More information on configuring Single File Restore is available in the “SMVI Installation and Administration Guide.”

For SFR NetApp recommends that the source and destination VMs have the latest VMware Tools running. You should also configure global notification settings before you can successfully use the SFR feature, since the workflow uses e-mail to send out details like the Restore Agent installer link and a configuration file. A VM that has a network assigned on a distributed vSwitch cannot be selected from the SFR wizard; then you would have to manually enter the VM name while creating the SFR session. NetApp recommends that port 8043 be open on the SMVI server if there are firewalls on vCenter or the guest(s) involved in SFR if it is a Self Service SFR

For more detailed steps on troubleshooting SFR refer to Appendix F.

SINGLE FILE RESTORE CAPABILITY FOR LINUX VMS

In order to perform a manual SFR on Linux, you must use the administrator assisted SFR mode. This mode will pre-attach the disks from the backup(s) to the VM. Restore Agent is not available for Linux VMs. The steps to perform SFR for Linux VMs are as follows:

1. SMVI administrator creates a new SFR admin-assisted restore session and pre-mounts the disk(s) from the backup(s) to the virtual machine.
2. A user on the VM must perform the following actions.
   Note that these actions require root privileges (either directly as root or through sudo)
   a. List existing disks
      # fdisk -l
   b. Rescan SCSI bus for new devices
      If your distribution ships it, there is a rescan-scsi-bus.sh script that can be run to perform the rescan. NetApp recommends using the script.
      If you do not have access to the script, you can issue the following command
      # echo "- - -" > /sys/class/scsi_host/host0/scan
      Your system may contain several directories of the form /sys/class/scsi_host/host[0-9]/. If it does, you can issue the echo command for each directory
   c. List the new disks
      # fdisk –l
      Compare this output against the first command to locate the new disks. This will also give you the partitions on the new disks along with the file system type(s).
   d. Mount the new partitions
      Use the `'mount'` command to mount your Linux partitions. You should know what file system type your partitions are. Likely partition types are ext3, ext4 and reiserfs.
      # mount –t ext3 /dev/sdb1 /mnt/disk1_partition1/
      If your disk(s) were constructed using LVM, you need to reconstruct your LVM disk group manually in order to view your disk data. That process is beyond this list of commands.
   e. Copy data from your newly mounted backup disk(s)
   f. Unmount the partitions when complete. Use the `'unmount'` command to unmount your Linux partitions when you are finished copying the data. Because we are using the admin-assisted SFR session, the virtual disks that were attached to the VM will be removed automatically by the server. Unmounting the disks first will just aid in the cleanup of the system.
      # unmount /mnt/disk1_partition1/

6.8 RESTORE PROCESS FLOW

The methodology used to restore a virtual machine or datastore is based on both the type of restore selected, as well as the environment in which the restore is being performed. The table shown below summarizes how restores are performed using SnapManager for Virtual Infrastructure.

Table 2) SMVI restore types

Datastore Type	Restore Type	Restore Method	ESX Credentials	PlatformsSupported
VMFS	Single File	Clone, mount, RA	No	3.5 +
VMFS	In place or Out-of-place disk restore	Clone, mount and copy	No	3.5 +
VMFS	VM	Clone, mount and copy	No	3.5 +
VMFS	Datastore	Single File SnapRestore	No	3.5 +
NFS	Single File	FlexClone, mount, RA	No	3.5 +
NFS	Out-of-place disk restore	FlexClone, mount and copy	No	3.5 +
NFS	VM, Datastore or in-place disk restore	Single File SnapRestore	No	3.5 +

With these differences in restore types aside, the process flow used by SnapManager for Virtual Infrastructure during a restore is as follows:

1. SMVI powers off any virtual machine that's being restored, if it is in a powered on state, unless this is for a Single File Restore
2. Files are restored as described above based on restore and datastore type
3. The virtual machine(s) is reloaded
4. The virtual machine(s) is reverted to the VMware snapshot that was taken at the time of backup, if the virtual machine was running during backup, thereby reverting the virtual machine(s) to the specified point in time.
5. SMVI removes the VMware snapshot to avoid performance overhead.

At this point, the restore is complete and virtual machines can be powered on. It should be noted that in SnapManager 2.0 for Virtual Infrastructure virtual machines must be registered with vCenter if they did not exist in inventory at the time of the restore. This can be accomplished by browsing the datastore on which the virtual machine resides, selecting the virtual machine folder; right clicking on the restored virtual machine's .vmx file and selecting "Add to Inventory" from the drop-down menu.

6.9 RESTORE ENHANCEMENTS IN SMVI 2.0

The restore enhancements in SMVI 2.0 are as follows.

VIRTUAL DISK RESTORE

SMVI 1.x allows restore at datastore and virtual machine granularity. Restore enhancements in SMVI 2.0 extend restore granularity to one more level adding the capability to restore individual virtual disks (VMDKs) of a VM.

This feature also allows disks to be restored to a different datastore. This is referred to as out-of-place restore. This allows VM administrators to test the consistency of the disks before attaching the disk to the VM. SMVI doesn't attach the restored disks automatically if the VMDK is removed from the current configuration of the VM or restored to a different datastore. Out-of-place restore copies the virtual disk files to the destination datastore after which users have to attach the disks manually.

For out-of-place virtual disk restores, if VMware snapshots already existed before the backup, NetApp recommends that you use vmkfstools to consolidate snapshots before attaching restored out of place VMDKs.

vmkfstools -i "tail-end-of-disk-00000N.vmdk" "newDiskToAttach.vmdk"

*N - Notifies the number of snapshots

If five VMware snapshots were taken, then there will be five delta disks; hence, this operation has to be performed on disk-000005.vmdk. To learn more about consolidating VMware snapshot disks, refer to the VMware KB article "Consolidating Snapshots."

Note: Consolidating snapshots may take some time to complete.

ADVANCED FIND (MORE SEARCH OPTIONS)

Using the Advanced Find feature the VM administrator can search for these types of backups:

- Recent backup
- Backups taken within a specific time range
- Backups with VMware snapshot
- Backups mounted for SFR

7 DISASTER RECOVERY

7.1 SNAPMIRROR INTEGRATION

SnapMirror is a data protection feature of Data ONTAP. It mirrors a local Snapshot copy of data from the primary storage system to a secondary storage system; typically in a remote location.

SnapMirror relationships cannot be configured through SnapManager for Virtual Infrastructure, but SMVI can update an existing SnapMirror relationship on the volume underlying the datastore or virtual machine. NetApp recommends testing the SnapMirror relationship from the storage system command line before updating through SMVI. This will aid in identifying where any potential issues might occur. Should the SnapMirror update be successful from the command line interface but fail from within SMVI, the administrator will have a better understanding of where to concentrate troubleshooting efforts.

Of further note, the destination storage must be identified within SMVI in the same manner as the relationship is configured on the storage system. For example, if a SnapMirror relationship is configured on the storage system using IP addresses rather than a DNS name, the secondary storage must be identified to SMVI by IP address also. Conversely, if identified by system name on the storage, the same name should be entered within the SMVI setup.

A step-by-step guide for implementing and updating volume SnapMirror relationships from the command line interface can be found in the Data ONTAP® 7.2 or 7.3 System Administration Guide.

Because SnapManager for Virtual Infrastructure provides support for volume SnapMirror only, NetApp recommends mapping one volume per datastore as specified in the NetApp and VMware Virtual Infrastructure 3 Storage Best Practices Guide.

During backup creation, SnapManager for Virtual Infrastructure provides the option of updating an existing SnapMirror relationship so that every time a Snapshot is created the data is transferred to a remote storage system. Whenever the backup of a virtual machine or datastore is initiated with the SnapMirror option, the update starts as soon as the backup completes, outside of the current SnapMirror schedule. Customers can schedule SnapMirror updates on a volume outside of SnapManager for Virtual Infrastructure. For example by configuring regular SnapMirror updates on a filer outside of the SMVI schedule you can cut down on the time required to update the mirror when SMVI runs(since the mirror is updated in the interim). However you should keep in mind that the updates should be scheduled in such a way that they should not conflict with the SMVI backup

SnapMirror Destinations

SnapManager for Virtual Infrastructure supports one SnapMirror destination per volume. Should a SnapMirror update be selected as part of an SMVI backup on a volume with multiple destinations; the backup will fail.

Should multiple SnapMirror destinations be required, NetApp recommends a tiered approach when configuring the SnapMirror relationships. For example, if the data must be transferred to four destinations, configure one destination from the primary storage system supported by SMVI to one destination and three additional destinations from the secondary storage through the storage system command line interface.

SnapMirror and Deduplication

NetApp recommends against using deduplication with Sync SnapMirror. Although technically it will work, the integration and scheduling of deduplication with Sync SnapMirror are complicated to implement in the type of rigorous real-world scenarios that demand synchronous replication.

When configuring volume SnapMirror and deduplication, it is important to consider the deduplication schedule and the volume SnapMirror schedule. As a best practice, start volume SnapMirror transfers of a deduplicated volume after deduplication has completed (that is, not in the middle of the deduplication process). This is to avoid sending un-deduplicated data and additional temporary metadata files over the network. If the temporary metadata files in the source volume are locked in Snapshot copies, they also consume extra space in the source and destination volumes. Volume SnapMirror performance degradation can increase with deduplicated volumes.

The scenario described above has a direct impact on backups configured within SnapManager for Virtual Infrastructure when the SnapMirror update option has been selected. NetApp recommends that scheduling an SMVI backup with the SnapMirror update option be avoided until a time when volume deduplication is known to be complete. Although a few hours should be scheduled to ensure this issue is avoided, the actual scheduling configuration will be data and customer dependant.

For further information, please refer to the Deduplication Implementation and Best Practices Guide.

7.2 CONFIGURING THE DISASTER RECOVERY STANDBY SITE

This section of the document provides an example of how to prepare and configure a true disaster recovery standby site in a SnapManager for Virtual Infrastructure environment. This example assumes the destination equipment is dedicated to a disaster recovery plan in the event of primary site loss.

Detailed steps on recovery from a disaster in this type of environment are provided in Appendix D

Primary Site SMVI Server

The SMVI server should be configured with the repository residing upon shared storage as outlined earlier in this document. NetApp recommends that Snapshot copies be taken of the repository's underlying volume, and that a SnapMirror relationship be established on that volume to the secondary storage. SnapMirror updates on the repository volume can be scheduled as required on an individual basis based on changes within the SMVI environment. This will allow quick recovery of the repository on the secondary site in the event of a failure. **Note:** In this scenario, configure the destination-side SMVI server to use shared storage before establishing the relationship as described in step 3 below.

Primary Site Storage

Configure the primary site storage per a normal SMVI installation with SnapMirror relationships established with the secondary storage. This scenario assumes that backups have been running within SMVI and SnapMirror relationships have been updated as part of those backups.

Disaster Recovery Site

Although there are a number of options when it comes to configuring the secondary site, the following is a quick and efficient way to configure the environment for rapid recovery if the secondary site is a true "standby" site.

1. Install SMVI on the vCenter server (or other Windows server as the customer's environment dictates) per the "SMVI Installation and Administration Guide."
2. Configure SMVI to use the volumes on the destination side (secondary site) storage systems.
3. Enter the vCenter server and storage system IP addresses or names within the SMVI Setup window.
4. Run the `smvi servercredential set` command from the CLI if necessary.
5. Stop the SMVI service within Windows.

6. Establish the SnapMirror relationship on the underlying volume from the primary site to secondary site. (Volumes used for SMVI on the destination side storage should be used as the SnapMirror destination volumes)

8 MISCELLANEOUS

8.1 VMWARE SNAPSHOTS

As previously discussed, the VMware snapshot preserves the state of the virtual machine and is used by SnapManager for Virtual Infrastructure during restores to revert the virtual machine back to the backup point-in-time state. VMware snapshots can capture the entire state of the individual virtual machines, including memory state, settings state and disk state. However, the memory state is not captured during a backup initiated by SnapManager for Virtual Infrastructure by design to aid in backup performance. Refer to TR 3749 and TR 3428 for recommended best practices.

By default, SnapManager for Virtual Infrastructure initiates a VMware snapshot as part of the backup process, creating a snapshot on each virtual machine undergoing backup that is in a powered-on state.

VMware snapshots can cause issues in certain environments. Should the datastore the virtual machines reside upon experience heavy disk I/O, VMware snapshots can take a long time to create and may eventually time out and fail. Although this occurs at a VMware level, SMVI depends upon the VMware snapshots for a backup to complete successfully.

Should this issue be encountered during VMware snapshot creation, whether initiated manually through vCenter or through SMVI, the administrator must reduce the number of concurrent VMware snaps, reduce the amount of disk I/O, or eliminate the VMware snapshots from the SMVI backup process.

Serialized snapshots

VMware recommends creating and deleting VMware snapshot operations in a serial manner to reduce snapshot errors. Snapshot operations consume resources from the ESX server and taking too many snapshots at a time may adversely affect the quality of service of the VMs. If different ESX servers attempt snapshots on the same datastore, lock contentions may happen, which may also affect performance. In SMVI 2.0, the number of snapshots created or deleted at a time during backup is controlled by the property vmware.max.concurrent.snapshots. The default value of this is 3 and may be changed by setting this in "smvi.override" and restarting the SMVI service. This means that by default, three snapshots will be created or deleted per datastore during backup. Setting this value higher may help with faster backups, but may increase snapshot errors as mentioned above. Setting this value too low may cause slower backups.

Installation of VMware Tools and VM alignment

NetApp recommends installing the latest VMware Tools on virtual machines to enable successful backups. We also recommend that customers align VM's according to TR-3749 and TR 3747

Reducing the number of concurrent VMware snapshots

Should virtual machine consistency be required, it is possible to limit the number of concurrent VMware snapshots by making backup configuration changes within SnapManager for Virtual Infrastructure. This can be achieved by creating multiple jobs per datastore – one per individual virtual machine or a few virtual machines - rather than at the datastore level as a whole.

There are, however, implications when using this approach to address VMware snapshot timeout issues. First, not only does this approach create additional administrative overhead, but it also may not correct the issue (snapshot failure) if the datastore the virtual machines reside upon experiences heavy disk I/O. Second, the number of NetApp Snapshot copies per volume will increase as more backup jobs are created on a given datastore, thus increasing storage overhead and reducing the amount of time a backup can be retained before reaching the maximum number of NetApp Snapshot copies per volume.

Reducing the amount of disk I/O

Although reducing the amount of disk I/O on a datastore could potentially alleviate VMware snapshot issues, this can be hard to achieve once datastores and the underlying storage platforms have been configured and are in use. Reducing the number of virtual machines per datastore, and therefore per volume, is not always practical or possible depending on the amount of available, unused storage.

Eliminate VMware vCenter snapshots from the backup process

SnapManager for Virtual Infrastructure provides an option to disable the taking of VMware snapshots, thereby eliminating this potentially problematic step from the backup process.

In an environment experiencing heavy disk I/O this will greatly increase both the speed and success rate of SnapManager for Virtual Infrastructure backups. Although disabling VMware snapshots is the NetApp recommended best practice in case of backup failures because of heavy disk I/O, it should be noted that this results in virtual machines being crash-consistent only as a NetApp Snapshot copy is taken without first quiescing the guest operating systems. While most virtual machines will not suffer any adverse effects after a restore from a crash-consistent backup, care should be taken before disabling VMware snapshots on virtual machines that contain critical applications, such as databases or e-mail servers.

9 DATA CONSISTENCY IN AN SMVI ENVIRONMENT

9.1 BACKUP

A backup can be point-in-time consistent (often called crash-consistent) or application-consistent, depending upon the type of technologies used to perform the backup.

9.1.1 Point-in-Time Consistent Backup

A point-in-time consistent backup is the simpler of the two types of backup because it requires minimal coordination among data components. There are two levels of point-in-time consistent backups possible, and SMVI supports both.

- **Point-in-time consistent backup**
  For a VMware virtual machine running on ESX or on a hosted hypervisor using unbuffered host I/O, a non-quiesced VMware snapshot provides the same level of point-in-time consistency to the software running inside a guest as a NetApp Data ONTAP Snapshot copy of the backing storage for this virtual machine. However, since the VMware snapshot delta files created during the non quiesced VMware snapshot are redundant in an SMVI scenario in which VMware's guest file system consistency isn't being used, SMVI uses the second method—a Data ONTAP Snapshot copy of the backing storage (without first triggering VMware snapshots of the virtual machines) to provide a point-in-time consistent backup with no guest file system consistency.

- **Point-in-time consistent backup with guest file system consistency**
  VMware Tools can also create quiesced snapshots of virtual machines using file system sync. The sync command comes natively with UNIX® and Linux systems, and the Windows version of VMware Tools includes an implementation of the sync driver for Windows. The sync driver provides file system consistency for the virtual machine snapshot by flushing the file system buffers and freezing I/Os while the virtual machine snapshot is being taken. By default (although an option exists to turn off taking VMware snapshots), SMVI triggers quiesced snapshots of all virtual machines selected for backup before creating the Data ONTAP Snapshot copy of the datastore to provide a point-in-time consistent backup with guest file system consistency. NetApp recommends that customers perform non-quiesced and quiesced backups with VSS participation and not use sync driver for the same. Note: Sync driver is not available in Windows Server 2008.

9.1.2 Application-Consistent Backup

With the availability of ESX 3.5 U2, Microsoft's Volume Shadow Copy Service, or VSS, was written specifically to enable third-party backup and recovery solutions to provide application-consistent backup and recovery for mission-critical Microsoft supported applications. When VSS is properly configured within the VMware virtual environment, an SMVI initiated VMware snapshot will begin the VSS process; however there are caveats when it comes to the restoration of VSS supported applications.

VSS is designed to produce fast, consistent snapshot-based online backups by coordinating backup and restore operations among business applications, file-system services, backup applications, fast-recovery solutions, and storage hardware. VSS consists of four primary components:

- Volume Shadow Copy Service—A service that coordinates various components to create consistent shadow copies of one or more volumes
- Requestor—An application that requests that a volume shadow copy be taken; a backup and restore application is an example
- Writer—A component of an application that stores persistent information on one or more volumes that participate in shadow copy synchronization; typically, this is a database application like SQL Server® or Exchange Server, or a system service like Active Directory
- Provider—A component that creates and maintains the shadow copies; examples are the system provider included with the operating system and the hardware providers included with storage arrays

The coordinated backup process includes freezing the data application I/O, flushing the file system cached I/O to disk, and creating a point-in-time snapshot of the data state. After the snapshot is created, file system and application I/O are resumed. The VSS restore process involves placing the data application into the restore state, passing backup metadata back to the application whose data is being restored, restoring the actual data, and signaling the data application to proceed with recovering the data that was restored.

Since SMVI (with VMware snapshots turned on) relies on VMware quiescing of virtual machines when creating backups, it is able to provide application-consistent backup through VMware VSS requester/provider components for the applications running inside the virtual machines. In fact, all SMVI backups with VMware snapshots turned on are "application-consistent." The limitations of this application-consistent backup methodology are explained in the "Application-Consistent Recovery" section of this document.

Note: For VMs running Windows Server 2003 as the guest operating system, the VSS snapshots are application consistent. For VMs running Windows Server 2008 and Windows Vista the snapshots are file system consistent. For more information refer to

http://www.vmware.com/pdf/vsphere4/r40/vsp_vcb_15_u1_admin_guide.pdf

The following are prerequisites for VSS-assisted application consistency:

- Virtual machines need to run on ESX 3.5 update 2 or later, and VSS components need to be installed in VMware Tools. For SMVI 2.0, ESX 3.5 update 4 or later is required
- Only applications that have VSS writers will have application consistency.
- All application data needs to be contained on virtual disks (VMDKs) in NFS or VMFS datastores, and not on RDMs or LUNs that are accessed using the Microsoft iSCSI Software Initiator in the guest OS. This will be explained in more detail in a later section.

9.2 RECOVERY

9.2.1 Point-in-Time Consistent Recovery

Since SMVI supports two levels of point-in-time consistent backup, with and without guest file system consistency, point-in-time recovery can be either guest file system consistent or not, depending upon the type of backup performed.

One of the advantages of using Snapshot technology to create backups is that these backups can also be used at a remote site for DR. Since SMVI includes an option to replicate backups to a remote system using an existing SnapMirror relationship, there is an opportunity for VMware Site Recovery Manager to use backups created by SMVI when a recovery plan is executed. The NetApp Site Recovery Adapter (SRA) recovers the latest version of the file system at the DR site. This is done since SRM does not currently support recovery of VMs that are in VMware snapshot mode, which is the state of a virtual machine that is contained in a NetApp Snapshot copy created with the VMware consistency option turned on in the SMVI backup job. The NetApp SRA does this by creating a FlexClone volume of the volume without specifying a snapshot name which means that the latest version of the volume is used, which is the latest SnapMirror snapshot. SRM DR failover is achieved by breaking the SnapMirror relationship and presenting the FlexVol volume to the VMware environment. Since this only achieves a SnapMirror relationship break the data presented is the same as that in the last SnapMirror updated snapshot, which is a non-quiesced VM, regardless of whether the SMVI job made a quiesced snapshot prior to the SnapMirror one.

9.2.2 Application-Consistent Recovery

If an application-consistent backup was taken by SMVI using the built-in VMware VSS support, the recovery will be application-consistent. Since the VMware VSS components have no application recovery capability, and no VSS writer-assisted recovery is possible using current VMware technology, the only recovery mode available to the application is recovery to the point of the last backup. It is not possible to roll forward the logs, recover to a specific point in time or specific transaction, or have other enhanced recovery functionality.

Testing validated that Microsoft SQL Server and Microsoft Exchange mailbox stores can recover from a VSS-assisted VM snapshot with no manual intervention steps required (that is, hot backup mode does not survive a reboot). For more details refer to TR-3785

9.2.3 Application Consistency in Combined Solution Environments

NetApp offers two solutions today for addressing application-consistent data protection in a VMware environment:

- SMVI, working through the VMware guest VSS stack, provides application-consistent backup and recovery for applications that have VSS writers and store their data on virtual disks (VMDKs). Recovery, in this scenario, is at the full VM level only.
- SnapDrive® and application-specific SnapManager products such as SnapManager for Exchange (SME) and SnapManager for SQL (SMSQL) running in the guest OS, provide application-consistent backup and fine-grained recovery for applications whose data is stored using Microsoft iSCSI Software Initiator LUNs or RDMs.

The critical difference in the level of protection provided by each of these solutions is in the granularity of recovery. To understand the significance of this, you need to understand the concept of roll-forward recovery. Roll-forward recovery replays information stored in transaction log files to return a database to the state it was in at an exact point in time. In order to perform a roll-forward recovery, archival logging must be enabled, a full backup image of the database must be available, and there must be access to all logged files created since the last successful backup.

Since the only recovery mode available today for applications backed up using SMVI (using the VMware built-in VSS support) is recovery to the point of the last backup, customers must use the relevant SnapManager application if more fine-grained, roll-forward recovery is required.

Today, both solutions can be used together—SMVI to back up/recover the system data and a SnapDrive and application SnapManager combination to back up/recover the mission-critical application data—to get the desired level of data protection required. Customers using the two-solution approach need to be aware of a few configuration considerations:

- SMVI supports backup and recovery of virtual disks in VMFS and NFS datastores.
- The application SnapManager products support backup and recovery of applications whose data is stored on RDM LUNs or Microsoft iSCSI Software Initiator LUNs mapped to the virtual machine.
- By default, SMVI uses quiesced VMware snapshots of virtual machines to capture the consistent state of the virtual machines prior to making a Data ONTAP Snapshot copy of the backing storage. According to VMware KB article #1009073, VMware Tools are unable to create quiesced snapshots of virtual machines that have NPIV RDM LUNs or Microsoft iSCSI Software Initiator LUNs mapped to them (this often results in timeout errors during snapshot creation). Therefore, customers using the Microsoft iSCSI Software Initiator in the guest and running SMVI with VMware snapshots turned on, which is not recommended, are at high risk of experiencing SMVI backup failures due to snapshot timeouts caused by the presence of Microsoft iSCSI Software Initiator LUNs mapped to the virtual machines.

VMware's general recommendation is to disable both VSS components and the sync driver in VMware Tools (which translates to turning off VMware snapshots for any SMVI backup jobs that include virtual machines mapped with Microsoft iSCSI Software Initiator LUNs) in environments that include both Microsoft iSCSI Software Initiator LUNs in the VM and SMVI, thereby reducing the consistency level of a virtual machine backup to point-in-time consistency. However, by using SDW/SM to back up the application data on the Microsoft iSCSI Software Initiator LUNs mapped to the virtual machine, the reduction in the data consistency level of the SMVI backup has no effect on the application data.

Another recommendation for these environments is to use physical mode RDM LUNs, instead of Microsoft iSCSI Software Initiator LUNs, when provisioning storage in order to get the maximum protection level from the combined SMVI and SDW/SM solution: guest file system consistency for OS images using VSS-assisted

SMVI backups, and application-consistent backups and fine-grained recovery for application data using the SnapManager applications.

Supported Configurations in Combined Solution Environments

The table below lists data consistency levels for operating system components and application data in configurations that differ in the way applications inside the virtual machine store their data.

- Both OS image and application data are stored on virtual disks connected to the virtual machine, and neither SnapDrive nor SnapManager products are installed.
- The OS image is stored on a virtual disk, the application data is stored on Microsoft iSCSI Software Initiator LUNs provisioned and managed using SnapDrive, and SnapManager products might or might not be installed.
- The OS image is stored on a virtual disk, the application data is stored on physical mode RDM LUNs (instead of Microsoft iSCSI Software Initiator LUNs) provisioned and managed using SnapDrive, and SnapManager products might or might not be installed.

The following scenarios assume that the environment has:

- VMware ESX Server 3.5 update 4 or later installed.
- Virtual machines running Windows 2003 SP1 or later
- The OS image installed on a VMDK
- The VMware VSS components installed as a part of VMware Tools in the virtual machines
- SMVI with VMware snapshots turned on, unless specifically noted otherwise

Table 3) Supported configurations in combined solution environments

	OS and Application Data Reside on VMDKs	OS Is on VMDK, Application Data Is on Physical Mode RDMs	OS Is on VMDK, Application Data Is on Microsoft iSCSI LUNs
Operating system	File System	File System	Point-in-time [1]
Applications without VSS writers, SnapDrive, or SnapManager	File System	No Support[2]	No Support
Applications with VSS writers, but no SnapDrive or SnapManager	Application (Windows 2003 guests) File System (Windows Vista and 2008 guests)[3]	No Support	No Support
Applications with SnapDrive installed, but no SnapManager	No Support	File System	File System
Applications with SnapDrive and SnapManager	No Support	Application	Application

[1] VSS quiescing needs to be disabled in the presence of guest-mapped iSCSI LUNs or NPIV RDM LUNs (VMware KB article #1009073).

[2] SMVI does not back up Microsoft iSCSI LUNs or RDMs attached to the virtual machine.

[3] VMware VSS components can't interact with VSS application writers in Windows 2008 (Virtual Machine Backup Guide, p. 50).

Simplifying Supported Configurations

For simplicity, the set of supported/recommended configurations that support application-consistent backup and recovery for VMware environments can be consolidated into three configurations that map to different kinds of environments: small, large, and mixed.

- The "small" environment configuration relies on SMVI and VMware VSS-assisted quiesced snapshots to back up OS images and applications in virtual machines, requires all data to be stored on virtual disks, and only provides very simple application recovery.
- The "large" environment configuration relies on SMVI and VMware VSS-assisted quiesced snapshots to back up OS images and SnapManager products to back up and recover applications requires application data to be stored on mapped LUNs and provides enhanced, fine-grained recovery as supported by SnapManager.
- The "mixed" environment configuration, which depends on future application SnapManager support for NFS and VMFS datastores (VMDKs), is essentially the same as the "large" environment configuration except that the application data is stored on VMDKs.

Table 4) Simplifying supported configurations

	Small	Large	Mixed
OS data storage	Application data and OS both stored on VMDKs connected to the VM	OS is stored on VMDKs connected to the VM	OS is stored on VMDKs connected to the VM
Application data storage		Application data is stored on mapped LUNs	Application data is stored on VMDKs
OS backup method	Application data and OS backed up together using SMVI and VMware VSS components	OS is backed up using SMVI	OS is backed up using SMVI
Application backup method		Applications are backed up using SnapManager	Applications are backed up using SnapManager
Application recovery	Only simple recovery using SMVI to the time of the last backup is possible	Enhanced application recovery is possible through application SnapManager	Enhanced application recovery is possible through application SnapManager
Recommended Usage	• Enterprise app-consistent B/R for infrastructure apps • DR	• Enterprise app-consistent B/R for infrastructure apps	• Enterprise app-consistent B/R for infrastructure apps

10 CONCLUSION

SnapManager 2.0 for Virtual Infrastructure provides a rich feature set that allows IT organizations to take advantage of NetApp Snapshot and SnapMirror technologies to provide fast, space-efficient disk based backups in a VMware environment with NetApp storage, while placing minimal overhead on the associated virtual infrastructure. The recommendations and examples in this report can help administrators get the most out of SnapManager for Virtual Infrastructure deployments. For more information about any of the solutions or products covered in this report, please contact NetApp.

11 SUMMARY OF RECOMMENDED BEST PRACTICES

This section of the report provides NetApp best-practice recommendations for SnapManager for Virtual Infrastructure 2.0 "at a glance." Details on these recommendations are provided throughout this report.

- Install SMVI on the vCenter server to reduce the impact of network disruptions.
- Install SMVI configuration files on a SAN or NAS device, thereby providing rapid recovery capability should the SMVI server fail.

- In environments with multiple vCenter servers, install one SMVI server per vCenter server to enable all backups to run as scheduled and ease administration overhead.
- When adding storage as part of the SMVI setup, configure a nonroot user on the storage.
- Enable Secure Sockets Layers (SSL) on all storage systems identified to SMVI, thereby ensuring passwords are encrypted when transmitted across the network.
- Configure VMDKs containing transient and temporary data as independent persistent disks to exclude the related datastore from the SMVI backup.
- Place all transient and temporary guest operating system data from multiple virtual machines in the same datastore configured with independent persistent disks with no other data type or VMDK residing upon it to avoid performing Snapshot copies against the underlying volume.
- Monitor the number of migrations performed in an ESX cluster configured with fully automated Distributed Resource Scheduling due to backup implications during active migrations.
- If the vCenter server is running within a virtual machine and will be backed up by SMVI, install the associated vCenter database on a physical system to avoid timeout issues during a VMware vCenter snapshot.
- Perform datastore backups rather than individual virtual machine backups to reduce the number of NetApp Snapshot copies performed against a volume.
- Use Retention Policies to meet service-level agreements (SLAs) and limit the number of NetApp Snapshot copies maintained against a volume.
- When integrating SMVI with an existing SnapMirror relationship, no more than one SnapMirror destination per volume should be configured.
- NetApp recommends installing the latest VMware Tools on virtual machines to enable successful backups. We also recommend that customers align VMs according to section 12 of TR-3749.
- For SFR, NetApp recommends that the source and destination VMs have the latest VMware Tools running.
- Configure global notification settings before using the SFR feature, since the workflow uses e-mail to send out details like the Restore Agent installer link and a configuration file.
- In case you have a normal disk and an independent disk for backup on the same datastore, this datastore is always included for backup irrespective of the "include datastore with independent disk" option. NetApp recommends that a separate datastore be designated exclusively for swap data or system data.

12 ACKNOWLEDGEMENTS

The following people have contributed to the validation of this Best Practices Guide: Lisa Haut-Mikkelsen, Leo Yaroslavsky, Josh Bonczkowski, Keith Aasen, Antony Jayaraj, Yateendra Kulkarni, Gabriel Lowe and John Ferry

APPENDIX A: LOSS OF SMVI SERVER

Recovering from Loss of SMVI Server when Installed on Local Disk

The following steps must be taken to protect SMVI when installed on local disk:

1. Backup the following two directories
    i. %PROGRAMFILES%\NetApp\SMVI\Server\repository\
    ii. %PROGRAMFILES%\NetApp\SMVI\Server\etc
2. In the event of failure of the SMVI server, install SMVI on a replacement system.
3. Stop the SMVI service
4. Copy the backed-up files listed in step 1 to their original location.
5. Restart the SMVI service within Windows.
6. Start the SMVI GUI and enter “Setup’”.
7. Enter the vCenter server name or IP address.
8. Enter the necessary storage information
9. Select “Restore” from within the SMVI GUI.

Backup jobs will be listed and scheduled jobs will run successfully.

Since the backups.xml and scheduledbackups.xml files are updated every time a backup completes, is renamed, or is deleted, these files require frequent backup in order to reflect all changes and enable all backups to be restored. Although installing SMVI on local disk is supported, NetApp recommends configuring SMVI on shared storage, as described below.

Recovering from the Loss of the SMVI Server when Installed on a Shared Device

1. In the event of the failure of the SMVI server, install SMVI on another system with access to the shared device.
2. After reinstalling SMVI, update the configuration files identifying the location of the repository and crash folders on the shared disk. The following two files will need to be edited:
    i. %PROGRAMFILES%\NetApp\SMVI\server\etc\smvi.config
    ii. %PROGRAMFILES%\NetApp\SMVI\server\etc\smvi.override
3. Change two parameters within the smvi.config file to reflect the path to the shared storage: (H drive reflects the location of the shared device)
    i. smvi.repository.path=H:\\NetApp\\SMVI\\\server\\repository
    ii. flow.persistence.embedded.storageLocation=H:\\NetApp\\SMVI\\\server\\crash
4. Change one parameter within the smvi.override file to reflect the path to the shared storage(this parameter will have the C: entered after a default installation)
    i. credential.persistence.file.path=H:\\NetApp\\SMVI\\\server\\etc\\cred
5. Restart the SMVI service within Windows.
6. Run the SMVI GUI.

All backups will be visible and restores will be possible.

APPENDIX B: LOSS OF AN ESX HOST

Within an ESX Cluster

SMVI communicates with vCenter and the NetApp storage systems rather than individual ESX hosts when running a backup. As a result, the loss of an ESX host within a cluster results in minimal interruption.

All ESX hosts within a cluster should be configured with access to the same shared storage, so that if a particular host fails the datastore will still be available and visible within vCenter, as will the VMs residing on the datastore, whether they are powered on or not. Follow standard VMware troubleshooting to resolve the issue with the ESX host. All backups will continue.

Stand-alone ESX Host

When an ESX host fails in a standalone environment the datastore(s) are no longer visible within vCenter. As a result, all scheduled SMVI backups against the datastore(s) fail. (**Note:** Users will not be able to run manual backup jobs because the datastore[s] will not be visible.)

The datastore(s) in question need to be mapped to an available ESX host managed by vCenter. If necessary, another host can be imported into vCenter. Once the datastore(s) have been mapped to the host, rescan HBAs and VMFS volumes within vCenter. The existing datastore(s) and the VMs that reside upon them will now be visible

Run "smvi discover datastores" from the SMVI CLI. You may also need to refresh the backup window within SMVI (assuming you're in it) by exiting to another window and then re-entering the backup window. Scheduled jobs can now run against the datastore(s) in question, and manual backup jobs can be configured against them.

APPENDIX C: LOSS OF PRIMARY SITE

The steps required to recover from the loss of the entire primary site, in other words, the SMVI server, ESX servers, and the primary storage systems, are detailed below.

1. Prepare the disaster recovery standby site as detailed in section 7.2 of this report.

2. After the loss of the primary site, mount the datastore(s) using the replicated datastore(s) on the secondary storage system.
   I. Break the SnapMirror relationship from the storage system CLI.
   II. Bring online the SnapMirror destination volumes on which the datastores reside.
   III. Map the LUN(s) from the replicated volume(s) to the secondary ESX server(s). Note: In ESX 3.X when the LUN from the snapshot is presented to the new ESX host at the DR site, the VMFS Datastore may not appear though the LUN does. In such a case, the LUN needs to be resignatured as described in the KB article 33990
   IV. Rescan HBAs and VMFS from within vCenter.
   V. Once the replicated datastore(s) are listed within vCenter (each datastore name is in the format "snap-00002-<original-datastore-name>"), right-click on each .vmx file and register the VMs with vCenter.

3. Manually edit the SMVI configuration files to point to the secondary storage.
   I. Use ssh to connect to the ESX server(s) to which the replicated datastore(s) are mounted.
   II. Change the directory to /vmfs/volumes and run the `ls -l` command to list the datastores and their UUIDs.
   III. Make note of the UUID for the newly mounted replicated datastore(s).
   IV. Open the %PROGRAMFILES%\NetApp\SMVI\Server\repository\backups.xml file in order to edit the text.
   V. Search and replace all occurrences of the old UUID with the new UUID as noted in a previous step.
   VI. Search and replace all occurrences of the old datastore name(s) with the new datastore name(s).
   VII. Search and replace all occurrences of the primary storage system name with the name of the secondary storage system (or IP address if used).

VIII. Save the modified file.
IX. Repeat all modifications within the %PROGRAMFILES%\NetApp\SMVI\Server\Repository\scheduledjobs.xml file being sure to save a copy of the file before making any changes

4. Start the SMVI service.

5. Once the service has restarted, start the GUI and select the 'Restore' screen.

6. The modified datastore name with the new UUID will be listed in the left window pane and backups taken on the primary site storage system will be listed and available for restore on the secondary storage system

APPENDIX D: SAMPLE SCRIPTS

Sample environment variables

BACKUP_NAME=My Backup
BACKUP_DATE=20081218
BACKUP_TIME=090332
BACKUP_PHASE=POST_BACKUP
VIRTUAL_MACHINES=3
VIRTUAL_MACHINE.1=VM 1|564d6769-f07d-6e3b-68b1-f3c29ba03a9a|POWERED_ON||true|10.0.4.2
VIRTUAL_MACHINE.2=VM 2|564d6769-f07d-6e3b-68b1-1234567890ab|POWERED_ON|true
VIRTUAL_MACHINE.3=VM 3|564d6769-f07d-6e3b-68b1-ba9876543210|POWERED_OFF|false
STORAGE_SNAPSHOTS=2
STORAGE_SNAPSHOT.1=filer2:/vol/smvi_vol_1:smvi_My_Backup_recent
STORAGE_SNAPSHOT.2=filer2:/vol/smvi_vol_2:smvi_My_Backup_recent

Script to display all environment variables during different backup phases

Create a .bat file with the following content

```
echo "============================="
set >> test.txt
echo "============================="
```

APPENDIX E: SAMPLE SMVI SNAPVAULT SCRIPT

1. From the command line on a NetApp controller, first create a new role for the SMVI script

   useradmin role add limited-sv-role –a api-snapvault-secondary-initiate-increemental-transfer,login-http-admin

2. Next create a user group that uses the above role;

   useradmin group add limited-sv-group –r limited-sv-role

3. Create the actual user;

   useradmin user add limited-smvi-user –g limited-sv-group

4. Finally set the users password

   passwd limited-sv-user password

   Now you have a user who can only call the SnapVault update API.

5. Next install the NetApp SDK onto the SMVI server. Then you build your update script and save it in the C:\Program Files\NetApp\SMVI\server\scripts directory.

```
if %BACKUP_PHASE% == PRE_BACKUP goto doSNAP

if %BACKUP_PHASE% == POST_BACKUP goto doSV

goto ende

:doSV

chdir "c:\Program Files\NetApp\ontapi"

apitest.exe torfiler3 limited-sv-user smv1rocks snapvault-secondary-initiate-incremental-transfer primary-snapshot smvi_weeklyBlock1_recent secondary-path /vol/vmblock1vault/vmblock1

goto ende

:doSNAP

chdir "c:\Program Files\NetApp\ontapi"

apitest.exe torfiler3 limited-sv-user smv1rocks snapvault-secondary-initiate-snapshot-create schedule-name smvi_weeklyvault volume-name vmblock1vault

goto ende

:ende


EXIT /b 0
```

APPENDIX F: TROUBLESHOOTING SFR

Here is information to troubleshoot SFR issues:

- SFR only works with backups performed by SMVI 2.0 or later.
- You must have flex-clone license to restore files from VMs stored on NFS datastore.
- Since the SMVI server uses a custom SSL certificate, you may see a warning in your browser while downloading the Restore Agent installer.
- ESX 3.5 supports only eight NFS datastores by default. Refer to KB Article 2239, TR 3428 or TR 3749 for details on how to increase that number to 32.
- SFR is not supported for IDE disks. If the VM has SCSI and IDE disks, you can use SFR for SCSI disks only. SFR is also not supported on dynamic disks
- This is the checklist for Restore Agent installer issues:
  - On Windows 2008 R2, .NET framework is a feature of the Operating System and must be enabled before Restore Agent can be installed.
  - You must run the RA installer as a user who is a member of the administrators group.
- This is the checklist for disk mounting issues:
  - RA only supports the first partition on a virtual disk. For other partitions, you have to manually use the Disk Management or diskpart tool.
  - RA only supports NTFS/FAT-formatted partitions on a disk.
  - SMVI can't add new SCSI controllers to power on a destination VM. Therefore the number of disks that can be attached to a VM are restricted by the available free slots on existing SCSI controllers. A VM can have a maximum of 60 disks (15 slots on 4 SCSI controllers).
  - The automount feature is by default enabled for Windows XP and Vista. Therefore on VMs running these operating systems, you may see that drive letters are preassigned to all the disks (and partitions).
- There needs to be network connectivity between the target VM and vCenter for a Self Service SFR
- This is the checklist for VM startup issues:
  - In some VMware operation failures, SMVI may not be able to detach all disks from a VM after the SFR session is expired or deleted. In such cases, the VM startup issues could be due to the stale disks that are left attached to the VM. In most cases, such stale disks can be removed by powering off the VM and then editing the VM settings. Double-check the VMDK path before you remove these disks from a VM.

- If you are unable to power on the destination VM after using it for SFR, make sure that there are no stale disks left on the destination VM. Typically this would happen for the following conditions:
  - A hosted process on an ESX server crashes while attaching a disk
  - An attach operation fails to complete due to VMware error