BEST PRACTICES GUIDE

VMware vSphere 5 on Nimble Storage

Table of Contents

1 INTRODUCTION **3**

2 DESIGN CONSIDERATIONS AND BEST PRACTICES **4**

a. BASE CONNECTIVITY FOR HIGH AVAILABILITY **4**

b. MANAGEABILITY **6**

c. VIRTUAL STORAGE ACCESS CONSIDERATIONS **9**

d. BACKUP AND RESTORE **16**

3 VSPHERE STORAGE FEATURES INTEROPERABILITY **22**

1 INTRODUCTION

VMware vSphere enables customers to transform current IT infrastructure into a private cloud. It provides a solid foundation with built-in availability, scalability, manageability and business continuity for the virtualization of business critical applications. If you want to take advantage of the built-in features such as vSphere HA, DRS, vMotion, Storage vMotion, shared storage is a requirement. Therefore storage planning and architectural design become imperative for the successful deployment of a solid foundational architecture that provides Infrastructure as a Service.

The Nimble Storage solution is built to provide a complete application-aware data storage solution that includes primary storage, intelligent caching, instant application-aware backup, and replication. You can consolidate management of primary, secondary, and off-site disaster recovery storage within a single storage solution. A Nimble Storage array provides iSCSI target volumes (LUNs) to VMware hosts as well as guest virtual machines. Any Volumes that you create on Nimble arrays are highly optimized for virtual machines by providing the following benefits:

- In-line Compression: Reduces storage footprint on physical disks by 50%-70%.
- Thin Provisioning: Efficiently stores actual data written rather than reserved space.
- Snapshot Backups: Instant point-in-time backup that eliminates the backup window.
- Zero-Copy Cloning: Preemptive de-duplication to eliminate storage footprint of repetitive data.
- WAN-Optimized Replication: Dramatically reduces bandwidth required for disaster recovery.

This document reviews the design considerations and best practices for implementing VMware vSphere with Nimble storage arrays. It is written for audiences that have a basic understanding of VMware vSphere and Nimble Storage.

2 DESIGN CONSIDERATIONS AND BEST PRACTICES

Base Connectivity for High Availability

Host

Make sure that the VMware vSphere ESX host has a minimum of two physical NICs. It is recommended that you have a minimum of two physical NICs dedicated for iSCSI storage access. On the ESX host, you can use the following NIC allocation model could as a reference:

vmnic0 and vmnic1 (Management, vMotion traffic and VM traffic)
vmnic2 and vmnic3 (VMkernel port for IP storage)

Software iSCSI connectivity is the preferred method for accessing Nimble Storage. You can use the following methods to achieve high availability and load distribution for storage access.

Method 1:

One vmnic per vSwitch, and one vmkernel port per vSwitch
All vmkernel ports must be bound to software iSCSI adapter.

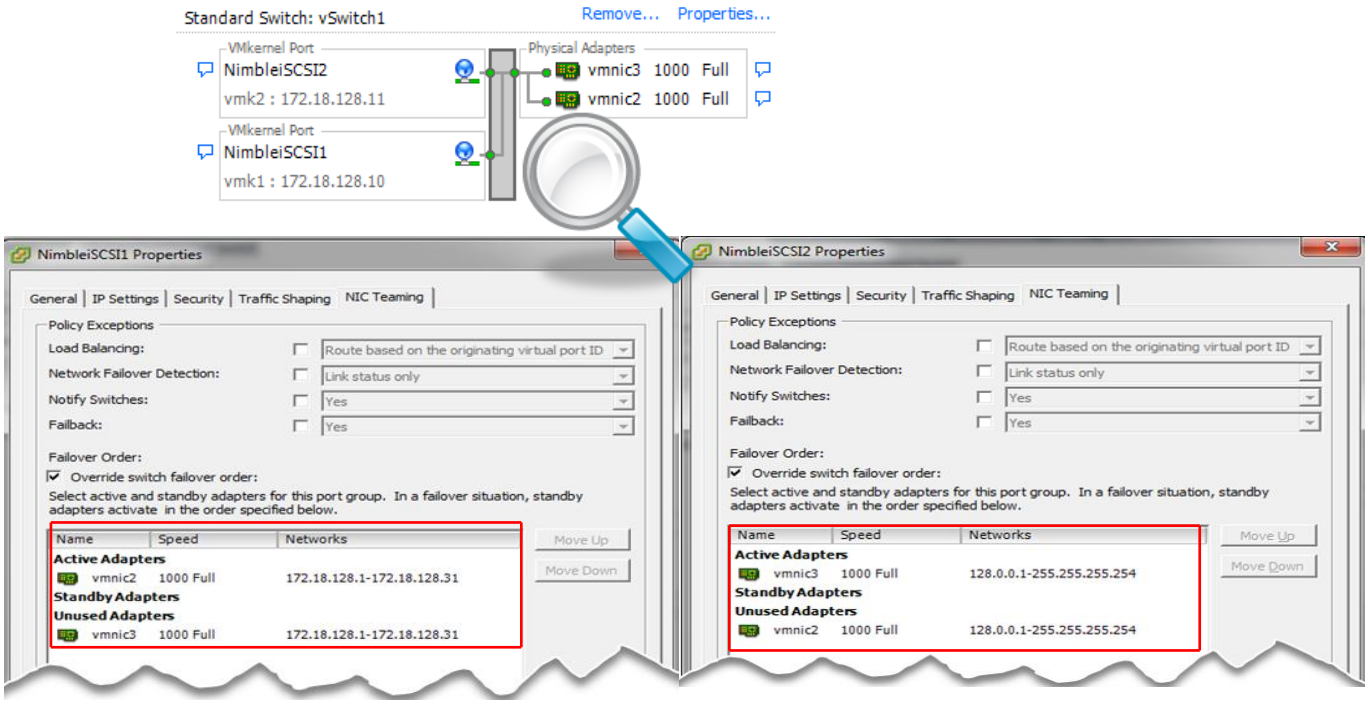
Method 2:

Two or more vmnics per vSwitch, dedicate one vmkernel port to one vmnic
All vmkernel ports must be bound to the software iSCSI adapter

NOTE:
Make sure that the NIC teaming active/standby policy is overridden so that one vmkernel port is active on only a single vmnic. Refer to *VMware Integration Guide* for detailed instructions

Both methods enable the ESX iSCSI multipathing to provide high availability and load distribution for storage access. The second method is recommended because it is easier to deploy and manage because only one vSwitch is required. If multi-port NICs are used, you need to ensure that iSCSI traffic spans different physical NICs instead of multiple ports on the same physical NIC. This avoids a single physical NIC failure to disrupt access to iSCSI storage.

Figure 1: One-to-one relationship between the VMkernel ports and the vmnics in the vSwitch



It is recommended to have dual physical switches for the connectivity between the ESX host and the Nimble Storage array to prevent single switch failure that can cause an outage to the virtual infrastructure.

The Nimble array supports the following types of network interface functions:

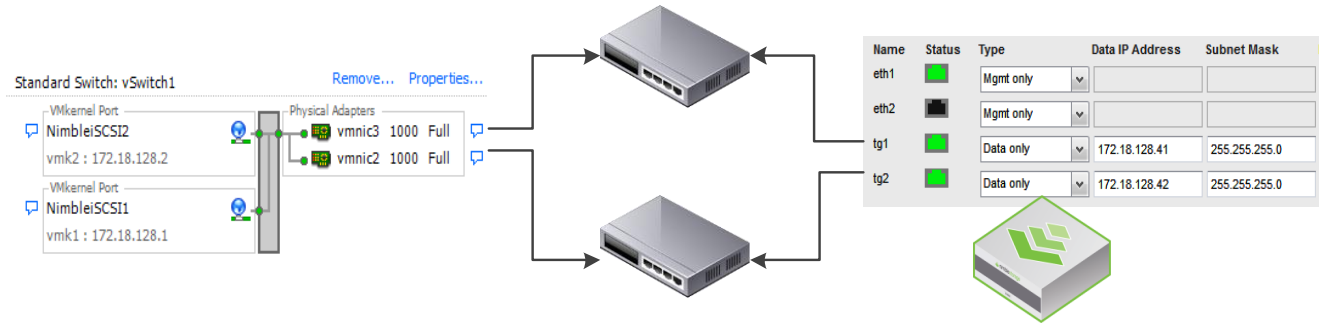
- The first network interface function serves as the management network interface and the other serves as the data access interface. Although the interfaces can serve both types of traffic, it is recommended to have a dedicated pair of interfaces for management traffic while the remaining interfaces serving data only traffic. You need to make sure that all data access interfaces are connected to the physical switch dedicated for storage traffic. If the physical switch is shared with other traffic such as management, vMotion, and virtual machine networks, you need to make sure that a private address (non-routable) set is used for connectivity between the ESX VMkernel ports and the Nimble data access interfaces.

NOTE:
Make sure that the management interface is connected to the same network segment as the vCenter Server. The vCenter Plugin requires network connectivity between the vCenter Server and the Nimble array management interface(s).

The physical switch ports in which the ESX and Nimble array interfaces are connected must have flow control enabled. Failure to do so can cause TCP level packet retransmits or iSCSI-level abort tasks.

If Jumbo Frame are used, you must set the correct MTS size from end-to-end, including the ESX server VMKernel ports for iSCSI traffic, any physical switch ports to which the VMKernel NICs are connected, and the Nimble network interfaces.

Figure 2: Reference end-to-end network connectivity between ESX host, switch network, and the Nimble array



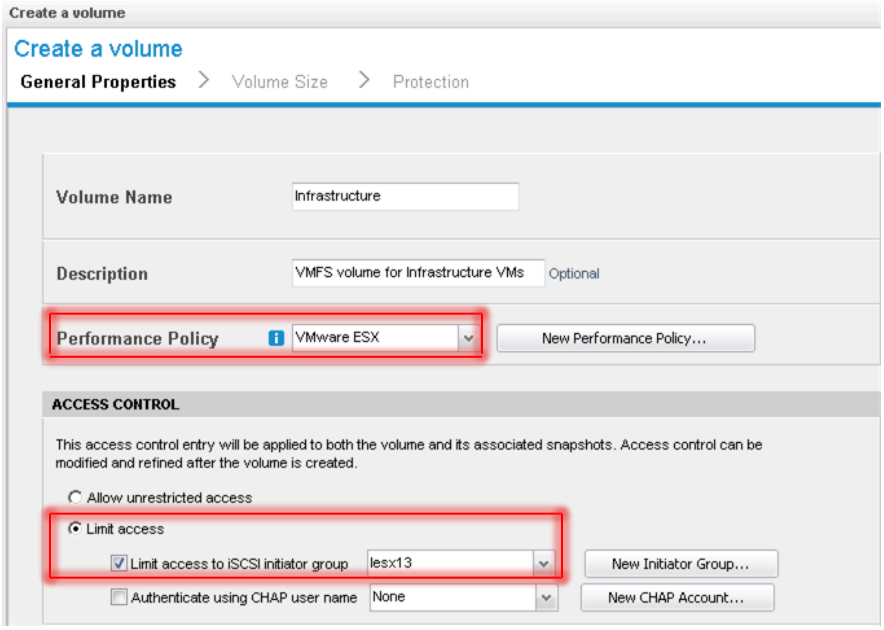
Manageability

Nimble Storage is integrated with vCenter Server to provide ease of management from a single-user interface for the virtual infrastructure. The Nimble storage plugin for vCenter Server provides the following operational management functions:

- Datastore Provisioning
  - It is recommended to provision datastores from the Nimble vCenter plugin, for simplicity and consistency. The plugin allows for creation of volume from array side, follow by creation of VMFS datastore to a selected group or all ESX hosts in a given datacenter, all in one automated workflow. Leveraging the plugin for this task greatly reduces the number of steps needed to provision storage to multiple ESX hosts, and also eliminates possibility of user error

NOTE: For environments in which the Nimble array is shared with both physical machines and ESX virtual machines, it is important to isolate all volumes to only the ESX hosts or virtual machines that need to have access to them. In such an environment, you need to provision volumes through the Nimble web interface so you can use access control. Access Control can limit access to a specific iSCSI initiator group—a list of one or more iSCSI initiator IQN identifiers.

Figure 3: Volume settings for provisioning volumes to ESX Server



- Datastore Removal
  - Datastore removal is a **TWO STEP** process:
    1. Removal of datastore from ESX host: proper steps need to be taken from ESX host side to ensure proper datastore removal. All virtual machines and/or templates need to be unregistered, removed, or migrated to other datastores before the the datastore can be removed
       - For vSphere 4.x, refer to VMware KB 1029786 for more details
       - For vSphere 5.x, refer to VMware KB 2004605 for more details
    2. Removal of volume from Nimble array: this step is required after the datastore has been properly removed from ESX host side. First set the volume offline, follow by a volume delete.

    NOTE: If you fail to follow the two-step process in the correct order could, it may result in an All Path Down (APD) condition that jeopardizes the performance and stability of the ESX host(s). Refer to VMware KB 1016626 for more details

- Datastore Performance Overview
  - There are two primary views of storage, the Data Center view shows all storage associated with the site while the datastore view permits granular control of individual Nimble volumes attached as datastores

Figure 4: Datacenter View with all datastores provisioned, along with performance and space usage stats

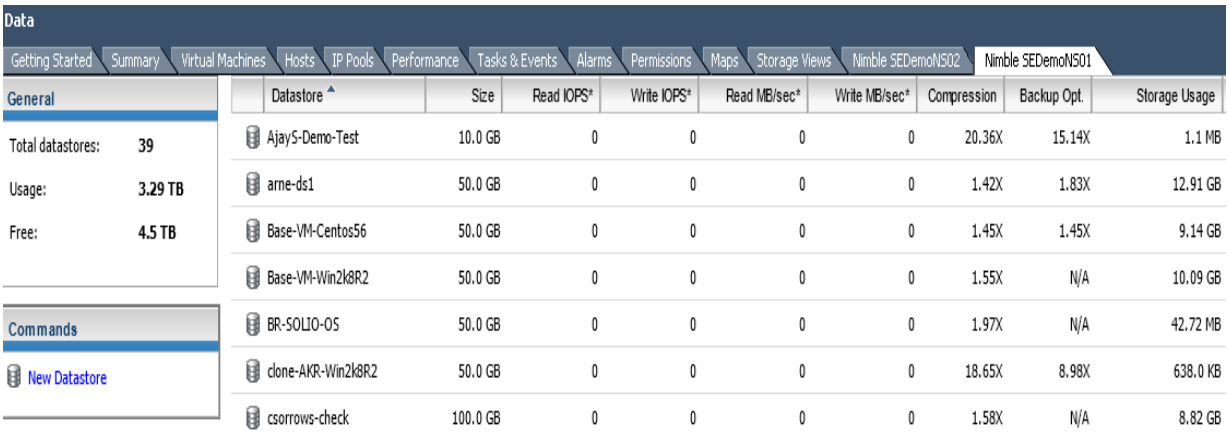
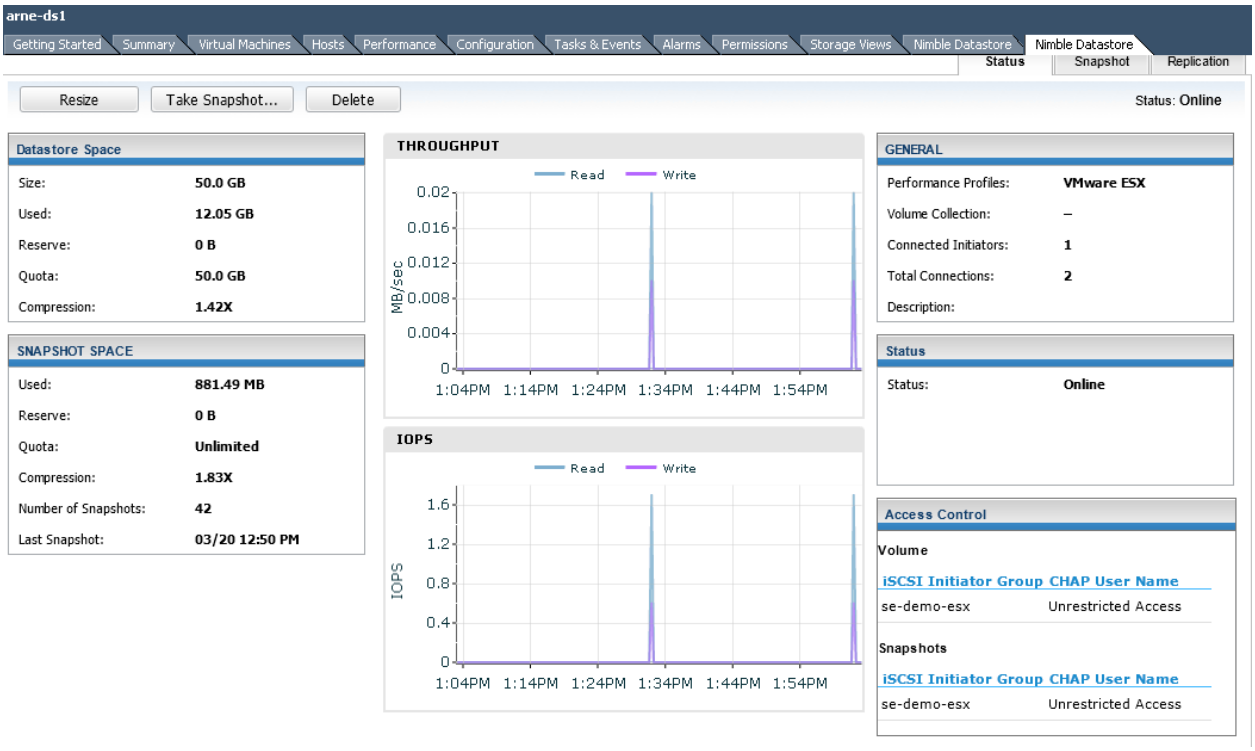


Figure 5: Nimble storage plugin view on individual datastore upon selection

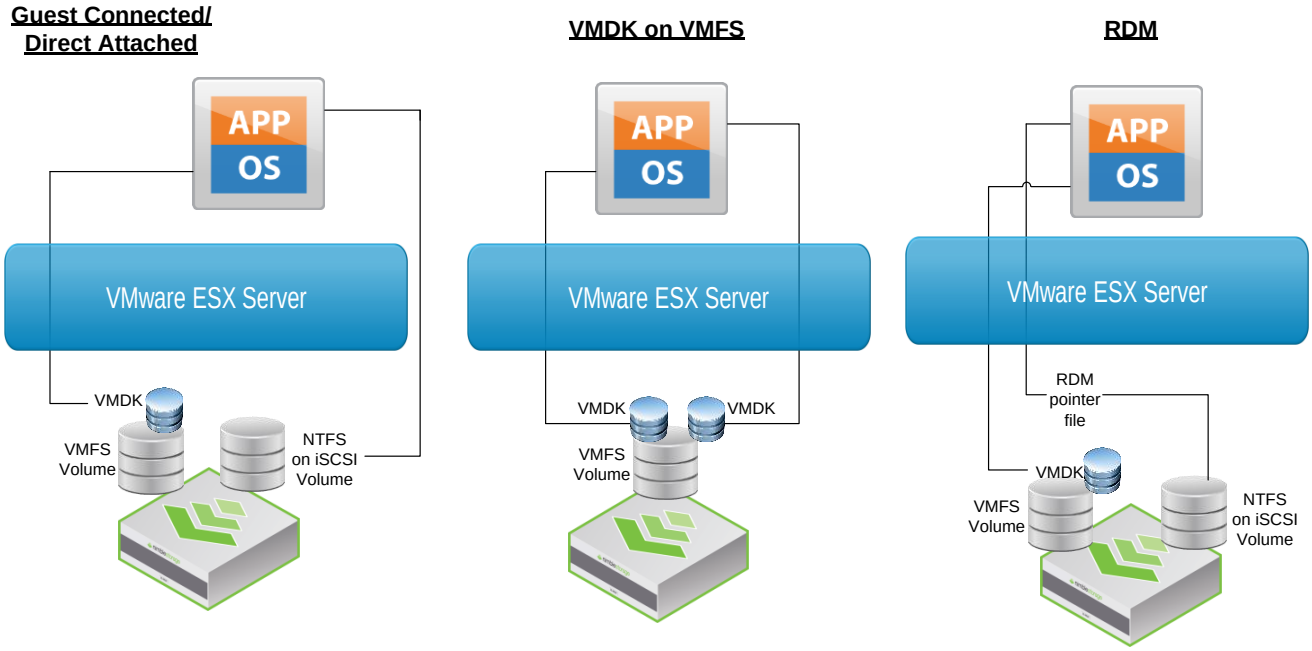


- Array Volume Management (volume resize, snapshot, replication status)
    - vSphere5 allows for expansion of VMFS volume dynamically. In the event that a specific datastore runs out of capacity, the Nimble storage plugin enables administrators to resize the array volume from vCenter Server. As soon as the Nimble volume has been resized, you can perform adapter rescan from the VI Client to discover any additional space, and then expand the VMFS partition to fully utilize the maximum capacity.
    - For infrastructure or virtual machine backup, it is recommended that you use the Nimble management user interface to create a Volume Collection, application consistency settings, and backup schedule. You can use the Nimble plugin for a one-time/manual snapshot of a given datastore.

Virtual Storage Access Considerations

There are three primary methods that you can use to connect networked storage to vSphere. You can attach virtual machines directly to Nimble Storage volumes by using an iSCSI initiator in the guest operating system. You can also create a VMFS datastore on a Nimble volume or create a Raw Device Map (in either physical or virtual compatibility mode) to the Nimble volume. By planning your Nimble volume-creation carefully, you can maximize the benefits of the Nimble Storage array.

Figure 6: Three types of disk connectivity methods for virtual machines



The following reference table highlights use cases, as well as benefits and additional considerations for usage of each connectivity method.

	Use Cases	Benefits	Planning Considerations
Guest Connected/Direct Attached	VM OS disk (VMDK on VMFS); with VM application disk(s) (NTFS/ext3) guest connected Application-consistent quiescing through Nimble Windows Toolkit VSS integration	Log truncation for Microsoft Exchange logs with Nimble Windows Toolkit VSS integration Simple to manage with one-to-one mapping between array volume and application data volume Easy to interchange between virtual and physical environments	-Site Recovery Manager requires custom script (customer defined, not created nor maintained by Nimble Storage) for mounting guest-connected storage during test failover and actual failover -Ensure that the correct performance policy is selected during volume creation (if one is not available from dropdown menu, check with application owner and/or software vendor for the application) -Ensure in-guest MPIO, firewall, disk timeout

	Item level recovery	without VMDK conversion Ability to change volume block size to match application data block size	registry settings are configured properly inside the virtual machie ***Refer to Nimble VMware Integration Guide for step-by-step instructions*** -Ensure virtual machine guest OS partition is aligned (specifically for Windows XP and Windows 2003)
VMDK in VMFS	-Both VM OS disk and application disk(s) as VMDKs on VMFS -Application consistent quiescing through VMware Tools VSS driver -Item level recovery	-Simple to configure (no in-guest iSCSI initiator to install/maintain) -Fully integrated into VMware Site Recovery Manager for virtual machine protection, test failover, failover, and failback	-Microsoft Exchange backup through VMware VSS driver does NOT truncate log files. Ensure there is third party Exchange truncation backup solution in place (i.e., Commvault Simpana Intellisnap integration with Nimble Storage) -If all VMs in a VMFS volume are hosting applications that are stateless in nature (i.e., Web Server, File Server, Print Server), VMware VSS quiesced snapshot is NOT required for such VMs; therefore, ensure that the volume synchronization setting is set to "None" -Running multiple VMDK on a VMFS volume requires additional time for VMware VSS quiesced snapshots to be taken for all VMDks on the given datastore -Ensure "VMware ESX" Performance Policy is selected during volume creation on Nimble array -Ensure virtual machine guest OS partition is aligned (specifically for Windows XP and Windows 2003) -Item level recovery involves additional steps to clone VMFS volume snapshot and attaching VMDK to staging virtual machine to export files to destination VM needing restore
RDM (Physical Compatiblity Mode)	-VMDK for OS and application binary, RDM in Physical Compatibility mode for application data	None	-There is no performance benefit in using RDM in comparison to VMDK or guest connected iSCSI storage -vSphere has 256 target maximum, consider trade-off on running more VMs per VMFS volume with one RDM target per VM

RDM (Virtual Compatibility Mode)	No use case for usage with Nimble Storage	None	-No use case for usage with Nimble Storage

Guest Connected/Direct Attached iSCSI Volumes

Using the guest-connected method ensures application data integrity during snapshot backup operations and provides quick item-level recovery. This storage architecture is a hybrid consisting of a VMFS datastore that holds the guest OS and application binary data. Actual application data, such as database and database log volumes are attached to the virtual machine using a guest-based iSCSI initiator that communicates directly with the Nimble Storage array. The tradeoff for using this connection method is the additional configuration and maintenance of iSCSI initiator inside the virtual machine guest OS. Additionally, a custom script needs to be implemented for usage with Site Recovery Manager so that the VMs can have access to their guest-connected storage during test recovery, recovery, or failover.

VMFS Datastore Mounted Volumes

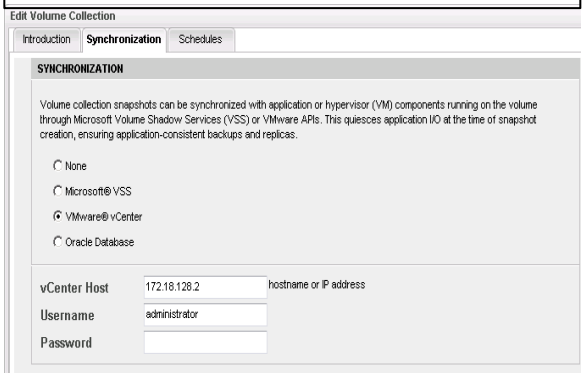
Mounting a Nimble volume as a VMFS datastore provides the simplest configuration when you use Nimble Storage with vSphere. At a minimum, VMFS datastores are used to hold the virtual machine configuration and Operating System volume. Nimble Storage is integrated with VMware VSS Provider in VMware Tools for application aware quiescing. This integration makes VMFS volumes suitable for storing transactional data (i.e., SQL, Exchange, etc.). Using VMFS Datastores reduces management burden by not requiring the installation of additional tools and the maintenance on each guest to properly quiesce applications or databases. In-addition, VMFS Datastores permit keeping the entire virtual machine together on the same protected volume. Using VMFS datastores is a convenient method of mounting storage to VMware. However, it does carry tradeoff just like guest connected storage.

Determining Volume Collection Synchronization Setting

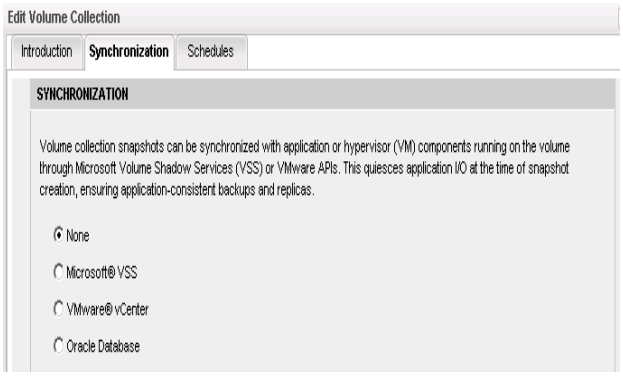
It is important to determine if VSS quiesced snapshot is required for a given virtual machine. If the VM hosting applications that are stateless in nature (i.e., web server, file server, print server), then an array based snapshot is sufficient. If the VM is hosting applications such as Microsoft Exchange, SQL Server, Sharepoint or Oracle, then proper quiescing via VSS framework is mandatory. If a given VMFS volume is only hosting VMs running stateless applications without the need for VSS quiescing, then it is best to set the Nimble volume synchronization to “None”, to speed up volume backup. If a given VMFS volume has at least one VM running application needing VSS quiescing, then the Nimble volume MUST have “VMware vCenter” checked for “Synchronization” setting.

Figure 7: Volume Collection Synchronization setting based on application type

VMFS with VMDK hosting applications that need quiescing (MS Exchange, SQL, Sharepoint, Oracle)



VMFS with VMDK hosting apps not needing quiescing (Web server, print server, file server)



When the Nimble Storage array triggers a scheduled snapshot, it passes the request to vCenter which coordinates snapshots with virtual machines running VMware tools on its' associated datastore. The VMware tools VSS driver will trigger an application quiesce on a VSS-enabled application in the virtual machine and respond back to vCenter when the data files are in a consistent state. After the VMware snapshots have been taken for all virtual machines of the datastore, Nimble then takes an array based snapshot for the VMFS volume, follow by removal of all VMware snapshots for the VMs. Nimble requests vCenter-coordinated snapshots for each Volume Collection; therefore you should limit the number of datastores in a single Volume Collection. You should also limit the number of virtual machines within a single datastore to avoid extensive interruption of service since all virtual machines on the datastore and in the same Nimble volume collection must have their I/O quiesced prior to the datastore snapshot backup.


High level recovery steps for item level recovery with VMFS

- Recover the VMDK from volume snapshot
- Attach the VMDK to the VM
- Perform restore on production VM


Microsoft Exchange Log Truncation

- Current VSS implementation in VMware Tools does not perform log truncation for Exchange. Therefore it is imperative to ensure that the environment has an Exchange-aware backup solution when this method is used. RDM Mounted Volumes (Physical and Virtual Compatibility)
- RDM in physical or virtual compatibility modes has no performance benefit compared to VMDK in VMFS, and guest connected iSCSI storage. There is no real benefit of using RDM in place of VMDK in VMFS volume.

Thin, Zero Thick, and Eager Zeroed Thick Considerations

One of the key parts of storage provisioning was originally based on estimating the amount of data space required over the lifetime of applications. This frequently resulted in either under-estimating storage requirements which resulted in downtime to find available storage resources and attach it to the production server. Over-estimating storage resources became the norm to avoid the penalty of downtime that is associated with under-estimating and resulted in unused space that still had to be paid for up-front. Thus, SAN storage provisioning has adapted over the years to include more provisioning options that make data center management an easier process.

VMware provides three primary provisioning features for VMDK files on VMFS volumes, Thin, Zeroed Thick and Eager Zeroed Thick. The provisioning model that you select for your datastores affects the density of virtual machines contained on your storage array and can also affect the runtime of virtual machines and can ensure that critical virtual machines will always have access to provisioned space and continue to run if the storage array reaches full capacity.

Figure 8: Space allocation behavior with the three VMDK formats

VMDK Format	Space Dedicated	Zeroed Out Blocks	Nimble Provisioning
Thin	As Needed	As Needed	Default (Thin)
Zeroed Thick	At Creation	As Needed	Use Volume Reservation
Eager Zeroed Thick	At Creation	At Creation	Use Volume Reservation

Nimble Storage allocates physical space using the Thin Provisioned model by default. You should typically match Nimble provisioning to your VMFS provisioning. For example, if you choose VMware Thick provisioning, then you can override Nimble's default thin provisioning by reserving space during Nimble volume creation. If you reserve less than 100% of the Nimble provisioned volume space, then the remainder of the volume continues to thin provision. The following guidelines help you decide which VMware VMDK format to use with Nimble storage.

Thick and Eager Zeroed Thick

Thick provisioned with lazy zero and thick provisioned with eager zero consumes nearly identical space usage on Nimble storage array.

 For best performance, use eager zeroed thick VMDK format as the zero blocks are compressed on the array side, and do not take up additional disk space.

Thin Provisioned

Thin provisioned VMDK on vSphere allows for space overcommit at datastore level. It means that you can provision more space to VMs than the actual capacity of the datastore. If the environment has large number of virtual machine deployments with unpredictable space growth, thin-provisioned VMDK on thin-provisioned VMFS volume could be a viable solution. However, you must exercise caution to prevent out-of-space conditions for virtual machines due to VMFS datastore level space overcommit.

If thin-provisioned VMDK is used, ensure “Datastore usage on disk” alarm is enabled at the highest level of the vSphere infrastructure with acceptable value range for warning and alert trigger. By default in vSphere 5.0, the predefined value for warning is 75% of disk space usage, and alert at 85%. If/when warning or alert is received, additional space can be allocated on Nimble array side, follow by rescan on ESX host side for expansion of the VMFS partition size. Additionally, in a VMFS datastore with both thin and thick/eagerzero ed thick VMDKs, out of space condition can be corrected by either expanding the size of the VMFS volume, or converting thick or eagerzerothick VMDKs to thin format through storage vMotion migration to another datastore, followed by migration back to source datastore. Below is a reference of the necessary settings for alarm and alerts in vCenter Server.

Figure 9: Ensure “Datastore usage on disk” alarm is enabled at the highest level in vCenter

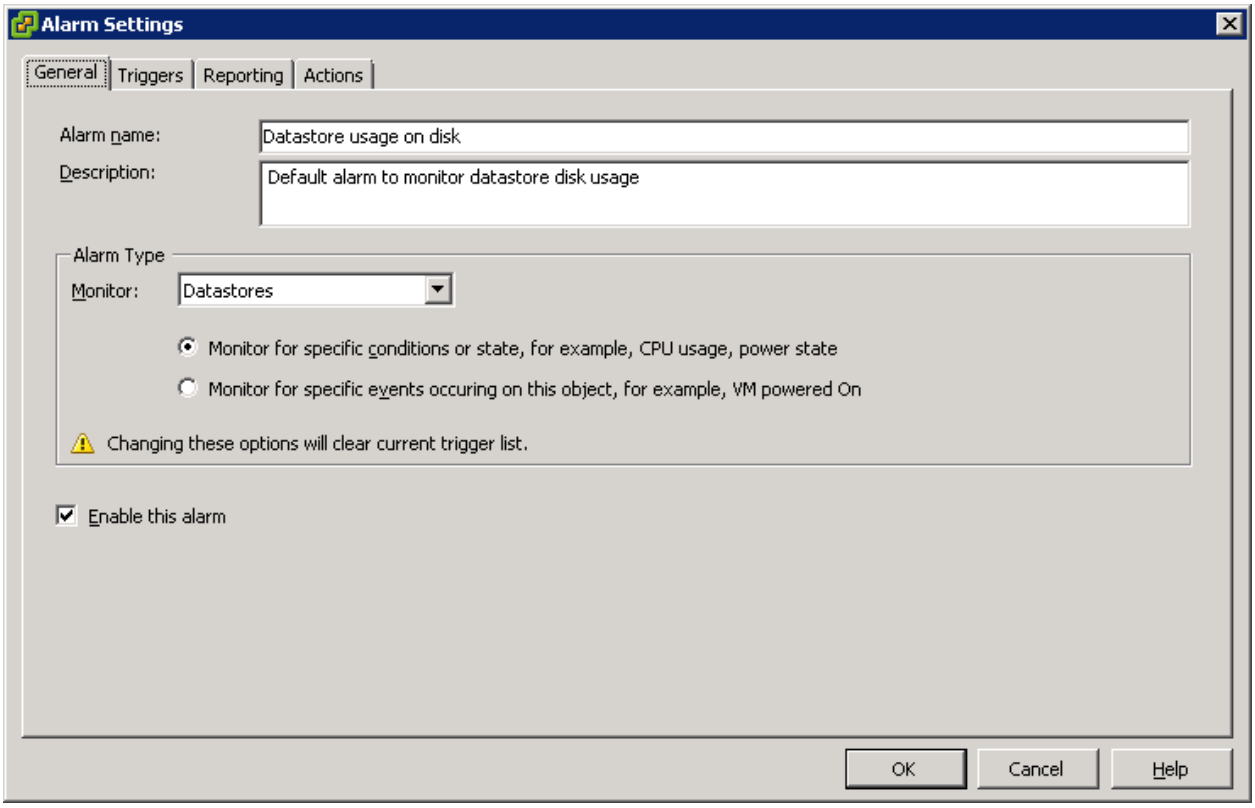


Figure 10: Check to make sure the default values for ‘warning’ and ‘alert’ are acceptable

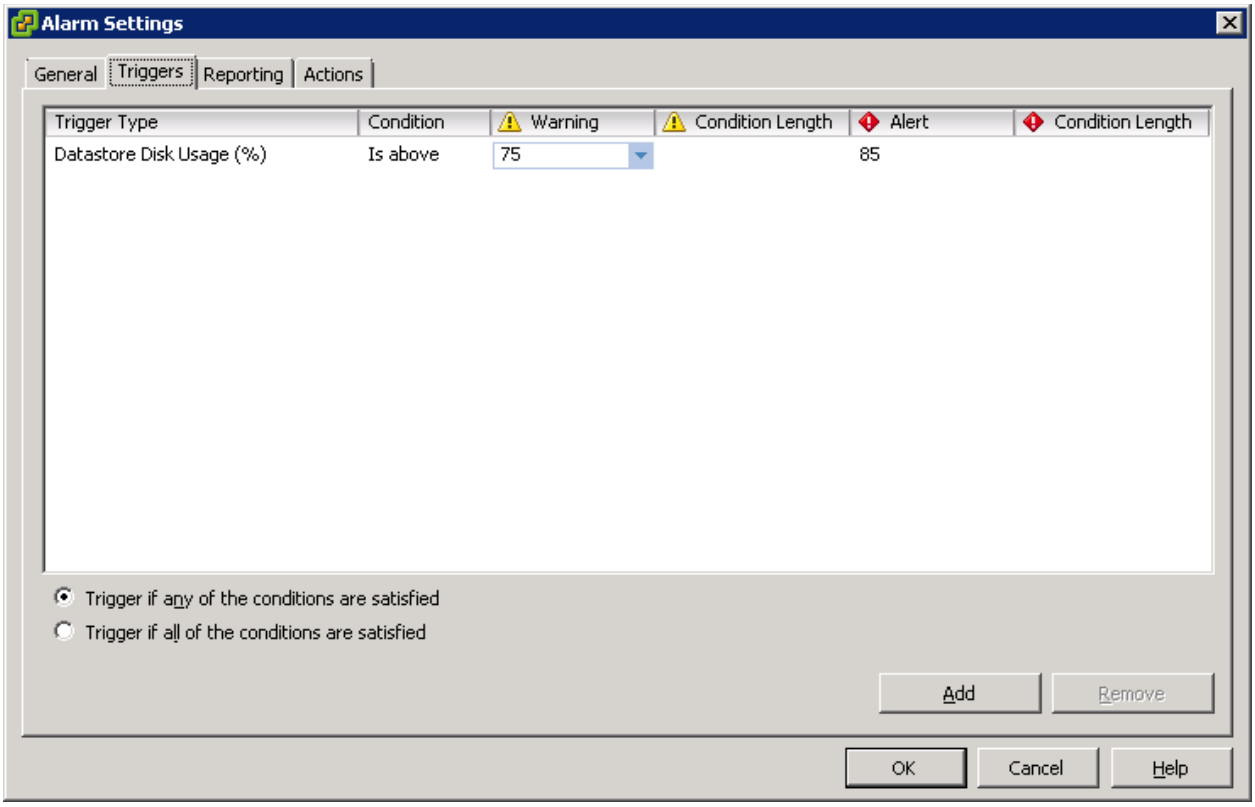
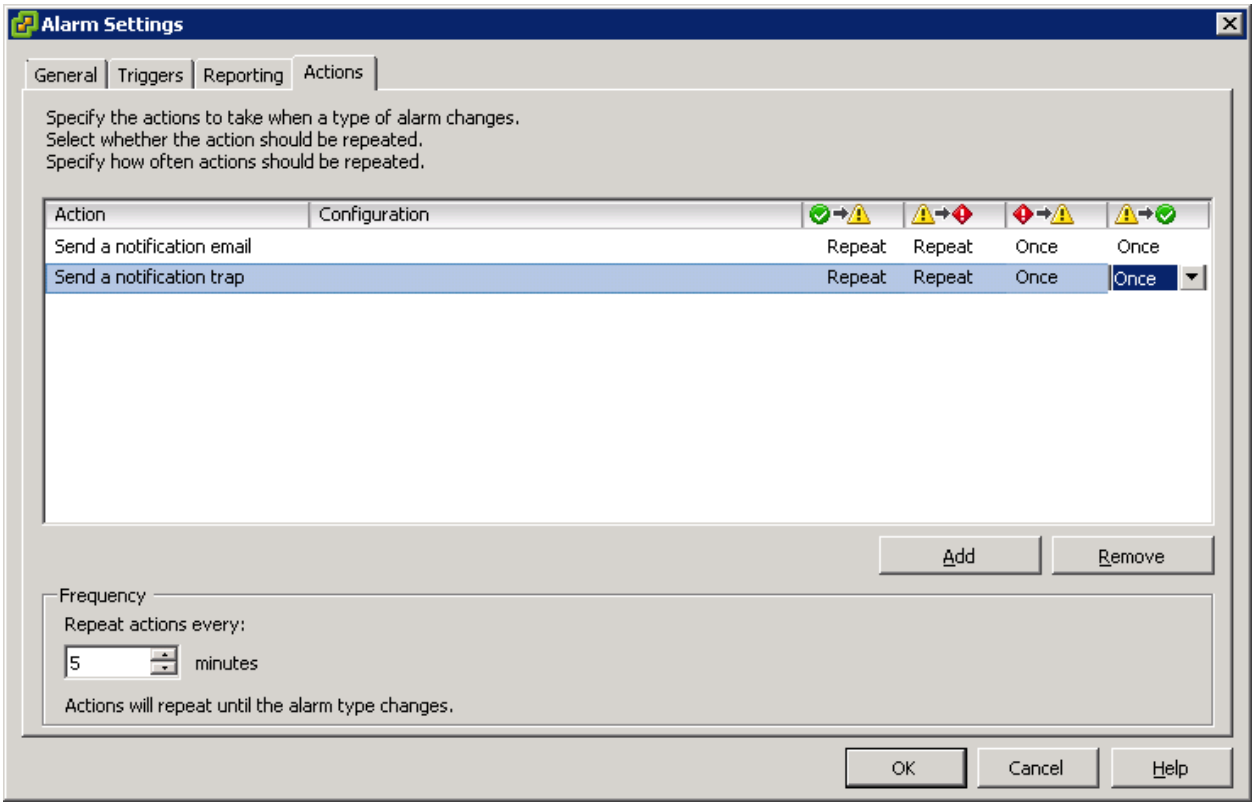


Figure 11: Ensure “Action” is defined to notify through email or SNMP trap for corrective actions



Backup and Restore

Nimble Protection Manager (NPM)

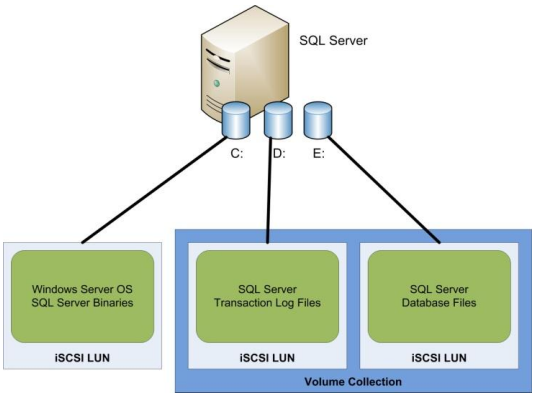
Nimble Protection Manager provides an interface between a Nimble Storage array and the native interfaces of the VMware host or guest operating system that places the operating system and application data into a consistent state that is safe for backup and recovery. This process is often referred to as a *quiesce*, and it ensures that the operating system and applications can safely start and be assured that their files and data are in a format that they can read and understand when recovering data after an outage or user data loss.

Computer servers continuously write system state and data changes to their storage devices. It's important that pending writes are flushed and the volume quiesced in a good consistent state when a snapshot is taken so that any later restore to that snapshot will allow the application to continue working properly. The two primary consistent states are called *crash consistent* and *application consistent*.

- Crash consistency is generally referred to as the ability for an operating system to boot and find its files and core functionality, especially the file system, in a good readable state.
- Application consistency takes additional steps to ensure that an application's data is functionally safe and is often referred to as *transactional consistent* when referring to database applications such as Microsoft™ SQL Server.

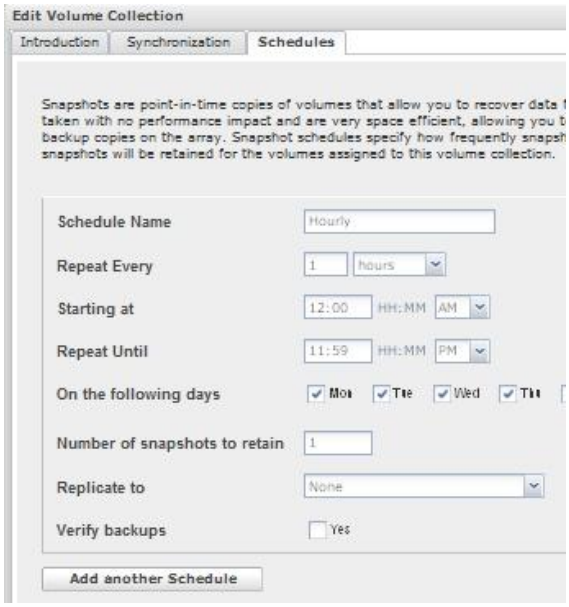
When you provision storage on a Nimble Storage array, you select one or more protection schedules that specify the intervals at which your data is preserved to that point in time. When the scheduled time arrives, it triggers the Nimble Protection Manager to coordinate a quiesce using the appropriate method, depending on how you are mounting storage from the Nimble Storage array. When mounting Nimble volumes as a VMFS datastore, no additional software is necessary for the virtual machine. If you choose to mount volumes using guest connected iSCSI storage, then each guest requires the installation of NPM which is included in the Nimble Windows Integration Toolkit to properly quiesce database applications.

OS and Application Data Disk Separation



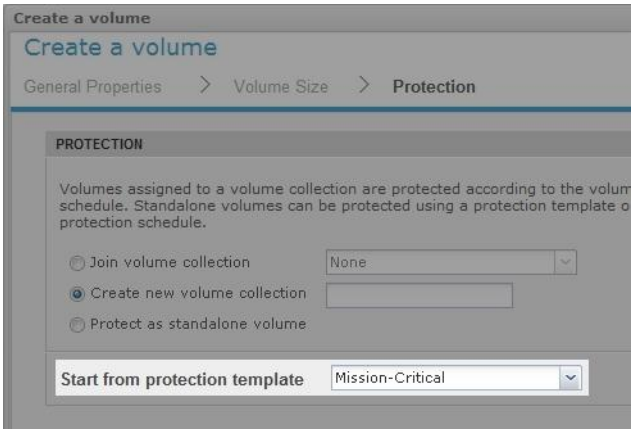
When creating a new virtual machine, you should separate the operating system and application binaries volume from the data volumes. Operating systems and application binaries change infrequently enough that simple volume crash consistency is acceptable using any of the three methods for attaching storage to a VMware virtual machine. Operating system volumes have similar low change rates and usually interoperate to support a single application, such as a multi-tiered CRM application with web front-ends, middleware servers, and database servers. Therefore you should prefer keeping OS volumes that support the same application in the same volume collection for better multi-node change management synchronization, especially during application upgrades that affect the multi-node application as a whole. When NPM quiesces the virtual machine through VMware Tools VSS framework, it performs this process

using internal timeouts. Therefore, you should take into consideration the time necessary to quiesce all of the virtual machines when grouping their associated volumes into a volume collection. You should also keep in mind that there are limits with VMware ESX hosts: maximum numbers of volumes that can attach to them and a maximum number of virtual machines that can share a volume (256 for both as of this writing). This hard limit may affect your proposed architecture. You need to plan accordingly so you can optimize the initial rollout and expected growth.



It is also helpful to separate data from the operating system and application to allow cloning for development and testing, which gives you quick access to production data sets without wasting storage space. Data volumes also tend to change constantly and typically have more critical protection needs. For example, database applications usually write changes first to a transaction log prior to writing to the database files. This allows them to recover any partial write activity in the event of a catastrophic system failure, such as a sudden power outage. If database applications did not perform this write process (WAL Algorithm) then the database can be left in a non-recoverable, and therefore non-trusted, state that forces a complete restoration from a backup. So, it is important to protect both the transaction logs and database in a coordinated fashion when performing any type of backup operation. Nimble Storage arrays provide functionality that allows you to group volumes that need to be mutually consistent into the same Volume Collection. A volume collection allows you to schedule the frequency and retention of snapshots as well as replication to other Nimble Storage arrays. A volume collection can coordinate protection activities between separate yet related volumes such as a database's transaction log and database file volumes to ensure that databases are snapshot with application consistency. The volume collection integrates with VMware vCenter or Microsoft VSS, which triggers them to momentarily quiesce the write activity of the file system or application respectively to ensure data integrity of the point-in-time backup. Management of a volume collection allows you to quickly change protection schedules for all related volumes. For example, suppose you have created a SQL Server database protection schedule for several databases on a SQL Server supporting an eCommerce application. It is common for databases to be partitioned into different data files with differing performance characteristics. The initial business requirements called for a configuration based on hourly snapshots for backup and replication off-site every 6 hours for disaster recovery. As business has increased, management has decided that the database has become more critical and needs more frequent backup and more frequent replication to reduce potential data loss. You can change the protection schedule for all of the associated files for the database at the same time using a volume collection, saving time and eliminating configuration errors that might inhibit recoverability.

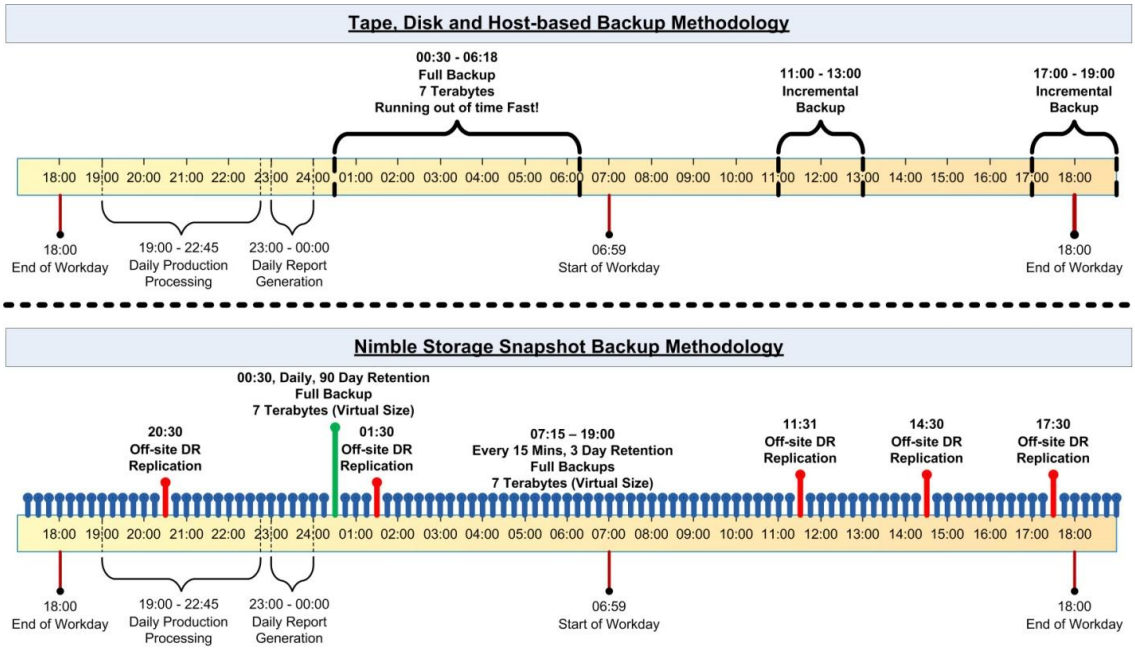
Backup Scheduling with Protection Templates



Nimble Storage arrays provide Protection Templates that consist of pre-configured schedules for snapshots, replication, and retention policies. When creating a new volume collection you can select a protection template that will insert a default schedule based on existing business rules. For example, you could create protection templates based on the criticality of the application data. Less critical applications such as middleware servers can use longer snapshot schedule intervals (4 hours) and shorter retention schedules (10 days). However, more critical applications whose data frequently changes such as databases will usually require shorter snapshot schedule intervals (15 minutes or less) and longer retention schedules (90 days), thus you will want to use a different protection template with shorter snapshot schedules and longer retention schedules. Using Protection Templates will reduce the amount of work required to create storage volumes and provide consistency for managing similar applications.

When a Nimble Volume Collection's protection schedule is triggered, the Nimble Protection Manager connects directly to the virtual machine's storage interfaces and asks it to place the application's data into a quiescent state. Applications begin to quiesce by flushing any pending I/O write activity from memory to disk and then signal NPM when they are ready for a safe snapshot backup. When NPM receives the quiesce notification, it triggers the volume collection to snapshot all its associated volumes, immediately after which data write activity is allowed to proceed. The Nimble backup method is dramatically faster and can trigger at regular short intervals unlike other solutions that have long backup windows which can take hours to complete before another backup can take place. Nimble Storage arrays perform snapshot backups instantly and can be scheduled for many more point-in-time backups per day than tape, disk, and VMware host-based backup solutions. This is a big improvement over traditional backup, which leads many administrators to find that their backup windows continue to grow until they can no longer complete a daily backup with a 12-14 hour backup window. In addition, scheduled incremental backups leave gaps in protection and don't provide replication for off-site disaster recovery.

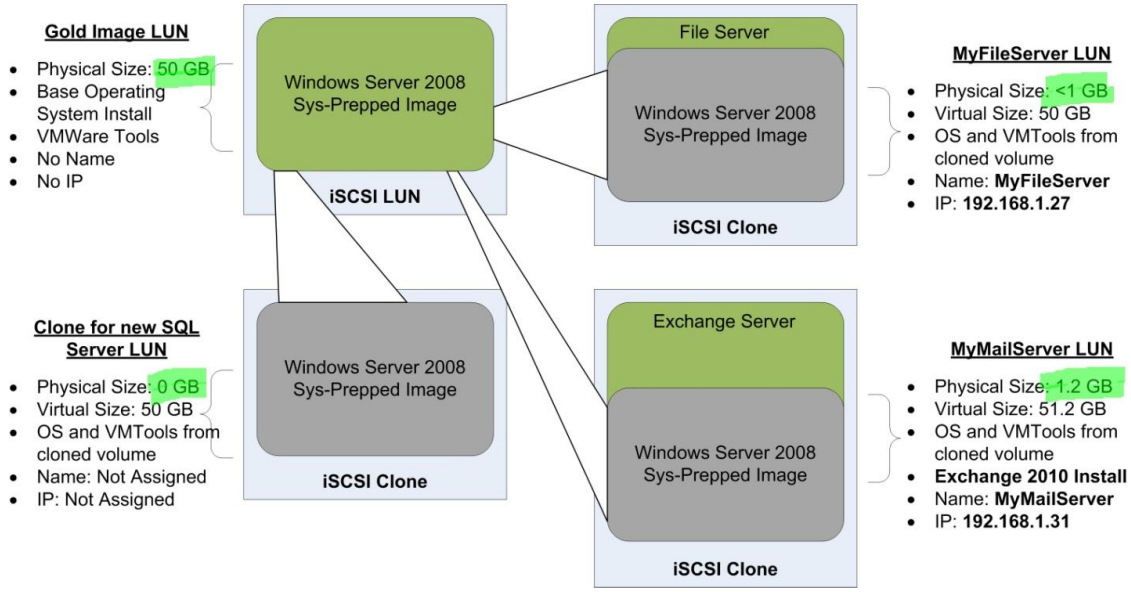
Figure 12: Nimble Storage backup methodology comparison with traditional backup methodology



CLONING

Cloning a volume (via a snapshot) creates a new volume with a new name and iSCSI target ID but uses all the other settings of the original, including data at the time the snapshot was taken. You can quickly create clones for development and Q/A testing using snapshots of production data sets without doubling the storage space requirements of those data sets. Clones also allow you to create a guest base operating system install that can be used to create additional guests based on the original clone. This dramatically reduces the amount of storage required for volumes such as operating systems that have the same files. The diagram shows these efficiencies and deduplicates the 50 GB base operating system volume, thus saving 150 GB of storage space that would be repetitive. The Windows Sys-prepped base image is cloned for each of the new virtual machines. When booted, the administrator configures the new machine with its own unique name, network address, and applications.

Figure 13: VM clone usage reference

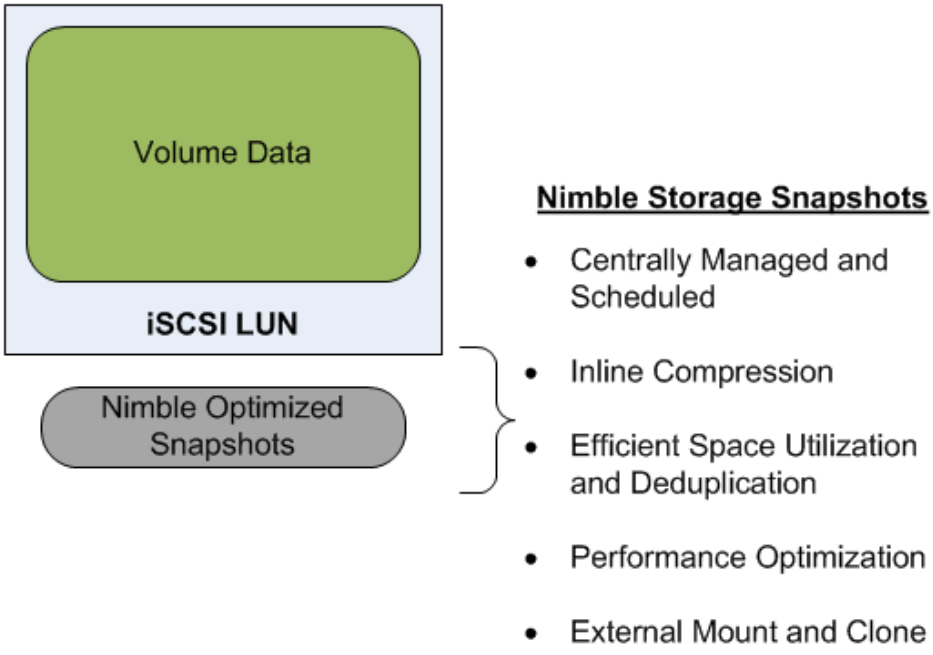


Snapshots

vSphere has built-in virtual machine snapshot capabilities, to serve two major purposes:
-enable end user to take VM snapshot in an ad-hoc fashion, to ensure point-in-time snapshot exists for rolling back operations that cause changes in the guest OS (i.e., patch update, application code change)
-enable third party backup solution integration to create crash and application consistent snapshots

Taking snapshot from vSphere on a per VM basis can be effective for one time operation of VM that may require change rollback. However, this method does not scale when the operation needs to be repeated for multiple VMs in the infrastructure. Because these snapshots are individually managed, and there is no built-in snapshot scheduling and retention capability. For backup and restore of the virtual infrastructure, consider using Nimble Protection Manager which has full integration with the VMware VSS framework. Additionally, consider the following added benefits of Nimble array based snapshots:

Figure 14: Nimble Storage snapshot benefits



3 VSPHERE 5 STORAGE FEATURES USAGE CONSIDERATIONS

Storage IO Control (SIOC)

Storage IO Control (SIOC) enables QoS (Quality of Service) for shared storage access between virtual machines. It is purpose built to address the "noisy neighbor" problem that is common in shared services environments. One can define shares and IOPS limits on a per virtual machine VMDK level, to ensure critical virtual machines are treated as first class citizen.

Nimble Storage Consideration:
No additional configuration is needed on the Nimble array side to take advantage of this feature. Simply set higher share values and IOPS limits for mission critical virtual machines, and the I/O QoS enforcement would work accordingly.

vSphere Storage DRS

With vSphere5, a new object called Datastore Cluster is introduced. It is a collection of datastores aggregated into a single logic unit of consumption from administrator's perspective. When a Datastore Cluster is enabled with Storage DRS, the virtual machine virtual disks could be balanced non-disruptively across a group of datastores in the Datastore Cluster, through storage vMotion migration. The concept is analogous to DRS for compute resources. Storage DRS feature leverages the datastore cluster construct to perform the following key functions:

- Initial virtual machine placement on datastore with lowest space utilization
- Load balance based on capacity usage
- Load balance based on IO load

Nimble Storage Considerations

Storage DRS provides value in automating storage resource management. To use Datastore Cluster on Nimble Storage, be sure to consider the backup and restore aspects for the infrastructure. Below are the scenarios along with considerations:

VMs with OS on VMDK on VMFS, application data disk on Guest Connected Nimble volume
-if multiple VMFS volumes are used to store the VMDK for the VM's OS disk, then a datastore cluster can be created for all the VMFS volumes, with Storage DRS feature enabled. Given the guest connected storage is treated as network traffic in ESX, Storage DRS operation does not affect the application data volumes. All datastores belonging to the Datastore Cluster should be placed in the same Volume Collection, along with the Guest Connected volumes, for creation of OS crash consistent snapshots

VMs with both OS and application data disk in VMDK on VMFS volume
-if OS and application VMDKs are on separate VMFS volumes, it is best to create two separate Datastore Clusters, so different types of VMDKs do not end up together on the same datastore.
-if both OS and application data disks are on the same VMFS volume, and there are multiple VMFS volumes serving virtual machines the same fashion, then the VMFS volumes could be grouped together on the same Datastore Cluster, to take advantage of the VM placement and migration between datastores to balance load. Consider using VM and VMDK affinity rules to ensure the VMDKs for the VMs stay together on the datastore. This is especially important when Nimble array is used to back up the virtual infrastructure.

The following recommendations apply for both types of deployment scenarios above:

NOTE 1: It is recommended to place Storage DRS in manual mode, so the end user could review the generated recommendation, and make a determination on whether the storage vMotion migration should take place

NOTE 1: It is imperative to keep track of the recommendations that have been applied (meaning keeping track of when a VM's VMDK has been migrated from one datastore to another in a given Datastore Cluster), doing so would simplify the restore process in identifying a specific Nimble array snapshot that would contain the snapshot image of the VM needing restore.

vSphere Profile Driven Storage

vSphere 5 introduces Profile-Driven Storage, for placement of virtual machines based on SLA, availability, backup/restore requirements and provided storage capabilities.


Nimble Storage Considerations:

Profile Driven Storage can be very useful in ensuring the virtual machines' VMDK files are residing on the appropriate datastore, with the required protection from the Nimble array side, and with consistent placement of VMDKs to keep separation between OS and application volumes. Here are some usage examples:

Defining Storage Capabilities

For User Defined Capabilities, use meaningful labels to match the attributes from the Nimble Storage. For volumes that have "Mission Critical" Protection Policy, use the same description on the User Defined Capability, and then apply the capability on all VMFS datastores tied to volumes with "Mission Critical" protection policy.

Create Profile

Once the User Defined capability has been created, then a profile could be generated to consume the user defined storage capabilities. For example, "Production" profile can be created, and tied with "Mission Critical" capability, doing so would ensure all VMs associated with this profile have all their VMDKs placed on datastores that are protected on the Nimble Storage side.

Applying Profile

Once the profile has been defined, apply it to the corresponding virtual machines running on the infrastructure. For example, apply the "Production" profile to the production VMs. Doing so will ensure the virtual machines' VMDK(s) always reside on the datastore with "Mission Critical" protection policy on the Nimble array side.

nimblestorage

Nimble Storage, Inc.

2740 Zanker Road, San Jose, CA 95134

Tel: 408-432-9600; 877-364-6253 | www.nimblestorage.com | Email: community@nimblestorage.com