BEST PRACTICES GUIDE:

VMware on Nimble Storage
Summary

Nimble Storage iSCSI arrays provide a complete application-aware data storage solution that includes primary storage, intelligent caching, instant application-aware backup, and replication. This allows you to 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. Volumes created 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.

While there are different methods of using VMware with Nimble Storage arrays, the best practice is to combine these methods. You should store operating system images that are logically grouped on VMFS datastores, while keeping the data on different guest attached volumes. This architecture allows you to maximize the benefits and flexibility of Nimble Storage arrays. The remainder of this guide provides supporting information for this architecture and additional best practices that you should implement to best support your investment in VMware and Nimble Storage.
Storage and Backup Considerations

There are three primary methods of connecting networked storage to VMware-based virtual systems. You can attach virtual machines directly to Nimble Storage LUNs using an iSCSI initiator within the guest operating system. You can also create a VMFS datastore on a Nimble volume or create an Raw Device Map to the Nimble volume. By planning your Nimble volume creation carefully, you can maximize the benefits of the Nimble Storage array.

It is important to note that VMware volumes mounted to the host as VMFS volumes are limited to 2 TB – 512 bytes (2 TB minus 512 bytes) or they are not usable. For example, for a 2 TB volume create the volume size as 2047 GB or as 2097151 MB. See the VMware knowledge base article for further information: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=3371739 . Using the guest-connected method provides you with the best method for taking full advantage of the Nimble Storage performance and storage optimization features as well as ensuring application data integrity during snapshot backup operations. Supporting details are provided throughout the remainder of this guide.

Use 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. The two primary methods of integration are using Microsoft VSS, which performs an application consistent quiesce; and using VMware vCenter integration, which performs a file system crash consistent quiesce.

**Limit Access to All Volumes in VMware Environments**

When using volumes in environments that run VMware, it is important to isolate all volumes to only the hosts or virtual machines that should have access to them. Failing to limit access to iSCSI volumes will cause VMware to perform excessive scanning of all volumes—including those that it should not have access to—and can possibly place your data at risk that another virtual machine could attach to them and delete data. Limiting access by Initiator Group greatly reduces this risk and improves the ESX scanning performance, which can affect the performance of storage operations such as taking snapshots. Nimble Storage provides the ability to limit access to a specific iSCSI initiator group (a list of one or more iSCSI initiator IQN identifiers). You can also control access by using CHAP authentication to further secure your iSCSI volumes.
Separate Volumes for OS/Applications and Data

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. Thus 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 triggers a VMware ESX quiesce, 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 be able to accommodate 6-10 virtual machine operating system images per volume collection; beyond that you should consider different groupings or contact Nimble support. 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, so plan accordingly to 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.
Use Performance Policies

The Nimble Storage array includes performance profiles that pre-configure new volumes using optimized configuration settings specific for different usage scenarios. For example, the default VMware performance policy is tuned to use 4 KB volume blocks to provide the best performance for VMware ESX VMFS storage LUNs. As you can see in the screen shot below, the default VMware performance policy also includes in-line compression and high-performance caching. Thus, use the VMware performance policy for VMFS volumes. Additional performance policies are included for major applications such as Microsoft SQL Server and Exchange, or create your own. You should use a performance policy specific for your application when using the guest-connected or RDM methods of working with Nimble Storage arrays. For example, you might have large files that are already highly compressed, such as a video or image server, that perform better with larger block sizes and no compression. Use the Nimble Storage array’s monitoring tools to view your volume performance under simulated production loads to better understand your unique application best practices.

Use 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.
Use Volume Collections

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.

Use VMFS Formatted Datastores for OS Volumes to Ensure Block Alignment

Operating Systems installed on Nimble Storage volumes that are mounted to the ESX host and formatted with VMFS will block align automatically. If you choose to use the VMware RDM method of mounting your operating system volumes, refer to the operating system vendor’s guidelines for methods of proper block alignment. Block alignment does not affect data volumes when using the Nimble Storage best practices and mounting volumes directly to the guest OS by iSCSI. Failing to block align operating system volumes correctly results in an (avoidable) overhead in read/write operations for each data block, and can therefore result in dramatically reduced performance of the virtual machine compared with properly aligned VMs. This can cause additional system downtime when correcting block alignment after the VM has been placed in production.
Prefer Guest Connected iSCSI Volumes for Storing Data

This method of data storage connectivity provides the best solution for data protection, application consistency, and off-site replication, as well as performance enhancements, by making complete use of Nimble Storage array optimization features.

Prefer Hardware Snapshots versus Software Snapshots

Snapshots are the basis for creating point-in-time versions of storage volumes and backups that can be mounted and accessed just like any other iSCSI volume. You can create snapshots at different layers of virtualization architectures including within the Guest Software, within the Host Software, and within the Storage Hardware. Connecting data volumes directly to the guest allows NPM to trigger snapshots that use the Nimble hardware provider rather than inefficient software-based snapshots.

Nimble Storage arrays provide highly efficient hardware snapshot functionality that is optimized by Nimble’s inline compression and block incremental efficiencies. This differs from operating system native software snapshots such as Microsoft™ VSS, which are not efficiently stored within their volumes. Thus software snapshots don’t take advantage of the Nimble Storage array optimized snapshot backup functionality. The following diagram shows the differing locations in which snapshots are stored. It is preferable to use hardware-based snapshots in the Nimble Storage array that take advantage of performance, in-line compression, and cloning capabilities rather than performing software snapshots with far less flexibility.

Zero-copy Clones

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.

The basic steps for rapid cloning are cloning a volume/LUN (datastore) using Nimble's cloning on the array and then making vCenter or the ESX host aware of the new datastore and VM. These instructions assume usage of vSphere connected to either a vCenter server, or connected directly to an ESX/ESXi 4.0 host. They also assume that the ESX host's iSCSI adapter is already set to dynamically discover the array.

**Note:** Before beginning, make sure that the advanced setting in ESX/ESXi that will automatically resignature snapshots/clones (LVM/EnableResignature) is turned OFF.

**Preparing a VM/LUN as a Template**

1. Create a single volume on the Nimble array that is large enough to hold the VM. In the Nimble array GUI, select Manage > Volumes, then Create a new volume and follow the wizard.

2. Log into vSphere and create a VMFS datastore on the volume/LUN:

   a. In the vSphere **Hosts and Clusters** view, select the host.

   b. Tab to **Configuration** and select **Storage Adapters**.

   c. Select the iSCSI adapter and in the upper right click **Rescan**. Depending on the connected SANs, this may take a few minutes to complete.

   d. After the rescan is complete, click the **Storage** link and then, in the upper right, click **Add Storage**....
e. Select Disk/LUN then click Next.

f. Select the newly created volume. You might need to expand the "Path ID" column to see the full path containing the actual volume name.

g. Accept all the default options to format it as a VMFS datastore. The volume should now appear in the datastore list.

3. On the host and using the new datastore, create a new VM, or migrate/clone an existing one.

4. Power off the VM.

Perform the Necessary Steps for the Guest OS (such as sysprep for Windows)

1. Set the network interfaces to DHCP.

2. If desired, create a VMware Guest Customization Specification, accessible through the vCenter Edit > Customization Specifications... menu.

   Note: Do not set the VM to template, which would cause clones to be templates.

Creating a VM clone

Important: Create one clone at a time. Do not create multiple clones, as they cannot be re-signatured with ESX.

1. Clone the volume/LUN that holds the VM template:
   a. Log into the Nimble array. From the GUI, select the volume to clone, then click Take Snapshot.
   b. Important: By default, snapshots are offline. Set the snapshot to online.
   c. Move to the Snapshots tab on the volume, select the snapshot, and click Clone.

2. Move to vSphere. Select the host on which you want the new VM.

3. On the host's Configuration tab:
   a. Select Storage Adapters and then the iSCSI adapter.
   b. In the upper right, click Rescan. Depending on the connected SANs, this may take several minutes to complete.
   c. After the rescan completes, move to the Storage link and click Add Storage...
   d. Select Disk/LUN, then click Next.
   e. Select the newly cloned volume. You might need to expand the "Path ID" column to see the full path containing the actual volume name.
   f. When you are presented with 3 VMFS mount options, select Assign a new signature.
   g. Click Next and Finish to move through the remaining creation steps.
4. The new volume now appears in the datastore listing as snap-<randomhex>-volumename, where the last part of the name is the template's volume name, not the clone volume name. To rename the volume, right-click and select Rename.

5. Right-click the new datastore and select Browse this datastore.

6. Highlight the VM folder, select the .vmx file (or .vmxt if the volume is a VM template).

7. Right-click and select Add to inventory.

8. When prompted for the source of the VM, confirm that it was copied.

9. Provide a name for the VM and any other requested information, such as in which host, cluster, and resource pool to put the VM.

10. Power on the VM.

11. Repeat for all additional clones.
**Better Backups**

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.
Host Network Considerations

These sections only apply to volumes mounted from the VMware ESX Host. Therefore, following Nimble Storage best practices this should only affect Operating System volumes mounted as VMFS file systems and not guest-attached volumes such as data-bearing volumes.

Prefer VMware iSCSI Software Initiator

When using Nimble Storage arrays with VMware hosts it is preferable to use the VMware iSCSI Software Initiator when connecting to volumes. You should also enable iSCSI multipathing, not teaming. Failing to follow this best practice can greatly impact the performance of virtual machines. You should also follow the best practice described in the Limit Access to All Volumes section of this guide to limit access to volumes to only the hosts and virtual machines that will be accessing them.

Prefer One VMkernel Port per Physical Port

VMware ESX hosts will create a network connection to a volume via all array ports. Nimble Storage arrays are typically connected to networks using 4 Ethernet ports, which will cause VMware to create a minimum of 4 network connections for each VMkernel iSCSI port for each Nimble Storage volume that is visible from an ESX host. Reducing the number of VMkernel ports per physical port reduces the number of logical network connections to the array to the minimum necessary. It is also important to limit the visibility of iSCSI volumes by creating iSCSI Initiator group filters on volumes as detailed earlier in the Limit Access to All Volumes section of this document.
Host and Guest Network Considerations

Enable Flow Control

You must enable flow control on all Physical and Virtual NICs to optimize network performance between VMware ESX hosts and Nimble Storage arrays. Indications that NIC flow control settings are not configured properly can manifest as TCP level packet retransmits or iSCSI level abort tasks.

Virtual Guest Considerations

Refer to the following guidelines for using Nimble Storage with Microsoft™ Windows.

Firewalls

Before beginning, make sure that any Windows firewall is disabled on the application server. If disabling the firewall is not possible, make sure that port 4311 is unrestricted.

For all Windows guests, make the following registry changes:

To ensure that the SQL or Exchange server is not taken offline in case of a data service restart, set the following registry entries. Note: A reboot of the Windows Server is required.

Set LinkDownTime to 45 seconds.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{class_id\}0000\Parameters\LinkDownTime
```

Set MaxRequest Hold Time to 60 seconds.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\instance-number\Parameters
```

Set TimeOutValue to 60 seconds.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue
```
Install Nimble Protection Manager (NPM) for Windows VSS

Download the Nimble Protection Manager software from the Nimble Support site.
http://www.nimblestorage.com/support/overview/

Follow the installation instructions in the Nimble Storage documentation and install NPM in each virtual machine that will run Microsoft Windows Server.

After the initial installation, manually configure NPM service recovery settings.

1. Go to Start > Administrative Tools > Services.
2. Right click on NPM and select Properties.
3. Select the Recovery tab.
4. Set the First, Second, and Subsequent failure items to Restart Service.
5. Set Reset fail count to after 7 days.
6. Click OK.