Hewlett Packard Enterprise

Technical white paper

Check if the document is available in the language of your choice.

DEPLOYMENT CONSIDERATIONS FOR IMPLEMENTING HPE NIMBLE STORAGE WITH VMWARE VSPHERE 7

CONTENTS

EXECUTIVE SUMMARY

The VMware vSphere® platform enables customers to transform their existing IT infrastructure into a private cloud. With its built-in availability, scalability, manageability, and business continuity, vSphere provides a solid foundation for the virtualization of business-critical applications. Also, the added features for Kubernetes integration allows additional container-based application deployment and increased "edge" features for an increasingly remote workforce. HPE InfoSight, a leading-edge online AI tool that collects and analyzes array and VMware® based information, provides a proactive analysis of all data including space usage, VMware "noisy neighbors," and misconfiguration determination and correction.

NOTE
For more information on HPE InfoSight, watch this HPE InfoSight—VM Recommendations video.

To take advantage of vSphere features such as VMware vSphere High Availability, Storage Distributed Resource Scheduler™ (DRS), vMotion®, and Storage vMotion®, shared storage is a requirement. Therefore, you must carefully plan your storage design for the successful deployment of a foundational architecture that provides infrastructure as a service.

The HPE Nimble Storage solution provides a complete data storage architecture that includes primary storage, intelligent caching, instant application-aware backups, and replication. It enables you to consolidate the management of primary, secondary, and offsite disaster recovery storage in a single storage environment.

Intended audience

This white paper is intended for administrators of VMware vSphere 7 using NimbleOS 5.2 and later. This paper was written to provide deployment considerations and best practices from Hewlett Packard Enterprise (HPE) to VMware administrators in HPE Nimble Storage environments.

Installation and integration resources

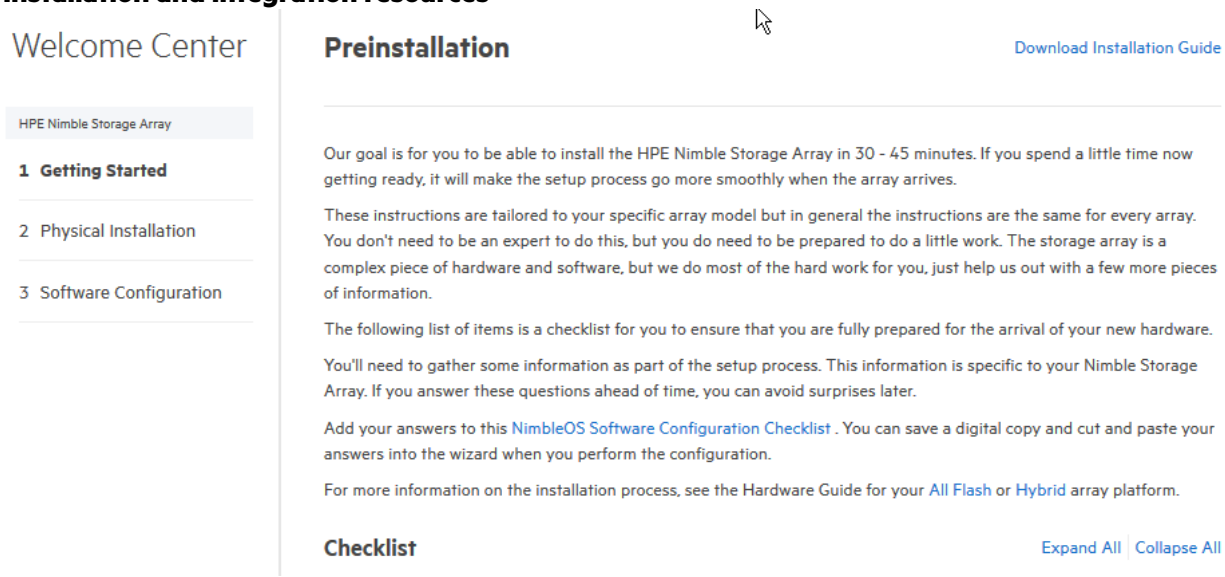


FIGURE 1. HPE InfoSight Welcome Center for HPE Nimble Storage home page

Before you get started:

- Download the Nimble Installation Guide for detailed installation instructions.
- Download and install the Nimble Connection Manager for VMware.
- Download the full VMware Integration Guide at HPE InfoSight.
- Deploy the Nimble integration plug-ins by clicking the **VMware Integration** option from the HPE InfoSight Administration main menu.

NOTE
Visit the HPE InfoSight Welcome Center for an interactive installation experience.

ADVANTAGES OF HPE NIMBLE STORAGE FOR VMWARE ADMINISTRATORS

HPE Nimble Storage arrays present iSCSI or Fibre Channel target volumes to VMware hosts and iSCSI target volumes to guest virtual machines (VMs). The volumes that you create on HPE Nimble Storage arrays are highly optimized for VMs. They offer the following benefits:

- A platform that is simple to deploy, configure, manage, and troubleshoot for VMware administrators. HPE Nimble Storage arrays deliver high-performance block storage managed through VMware vCenter®.
- HPE InfoSight cloud-driven AI-Ops delivers full-stack analytics and recommendations for resolving and optimizing VM, host, network, and storage problems and misconfigurations.
- Comprehensive integration and support for VMware Virtual Volumes (vVols) for application-defined storage through VMware Storage Policy-Based Management (SPBM).
- Multi-site synchronous and asynchronous replication with seamless integration with VMware MetroCluster (vMSC)—synchronous or VMware Site Recovery Manager (SRM)—asynchronous, as well as HPE Cloud Volumes for cloud-based mobility.
- Full implementation of the VMware vSphere Storage APIs for Storage Awareness (VASA) 3.0 standard, including storage provisioning directly from the vSphere interface.
- Support for HPE Memory-Driven Flash, which combines software intelligence, storage-class memory (SCM), and Nonvolatile Memory Express (NVMe) for vastly improved latency performance.
- Support for the VMware container storage interface (CSI) driver for VMware Tanzu as well as the HPE CSI driver delivering persistent storage for Kubernetes.

HPE INFOSIGHT ADVANCED AI-DRIVEN CROSS-STACK ANALYTICS

HPE InfoSight Cross-Stack Analytics is an advanced AI-driven engine that collects, analyzes, correlates, identifies, and predicts events from VMs to storage. It also guides VM admins on how to resolve issues by using actionable recommendation engines.

HPE InfoSight Cross-Stack Analytics for VMware

HPE InfoSight includes powerful features that enable VM administrators to analyze and resolve issues within vSphere environments. Administrators can choose to include vSphere cluster performance details as part of the HPE Nimble Storage DNA packages that are constantly being sent from HPE Nimble Storage arrays.

The DNA packages are collected directly from vCenter using HPE Nimble Storage vCenter plug-in integration. These data points are correlated and displayed in an easy-to-understand visualization that enables VM admins to quickly analyze potential issues. HPE InfoSight Cross-Stack Analytics also provides customized recommendations to help resolve issues across VMs, hosts, network, or storage issues.

Dashboards

Cross-Stack Analytics for VMware provides several dashboard views. These views are a good place to start when reviewing the overall performance picture of a virtualized environment. Dashboard views cover several categories that provide array and VMware specific information in various places. The whole-array dashboard views are Operational, Recommendations, Executive, Wellness, Capacity, and Labs.

Information collected includes telemetry data such as Cross-Stack Recommendations, Resource Planner, Capacity Consumers Forecast, AI Performance Recommendations, Pool Performance Telemetry, Replication Planning, Replication Timeline, Capacity Consumers Timeline, Volume Performance, Recurring performance Patterns, and Inter Volume Performance and Contention.

Cross-Stack Analytics for VMware dashboards include:

- **Top VMs**—The Top VMs dashboard provides two lists of VMs that have:
  - Received the highest number of I/Os over the last 24 hours
  - The highest average latency over the same time period

- **Host Activity**—The Host Activity dashboard shows CPU and memory statistics for all of the virtualization hosts that are managed by the selected vCenter instance.
- **Datastore Treemap**—The Datastore Treemap dashboard provides a quick and easy way to visualize the performance of all datastores in the vCenter environment. Datastores are represented by rectangles of varying sizes and colors. The larger the rectangle, the more I/Os the datastore has performed over the past 24 hours. The color of the rectangle indicates latency, with darkness increasing as average latency increases, as shown in Figure 2.

  To display absolute values for both size and latency, hover your cursor over the datastore name. To zoom in to the VM view, click a particular datastore. All VMs in that datastore are displayed with the same size and color scheme used for the datastores.

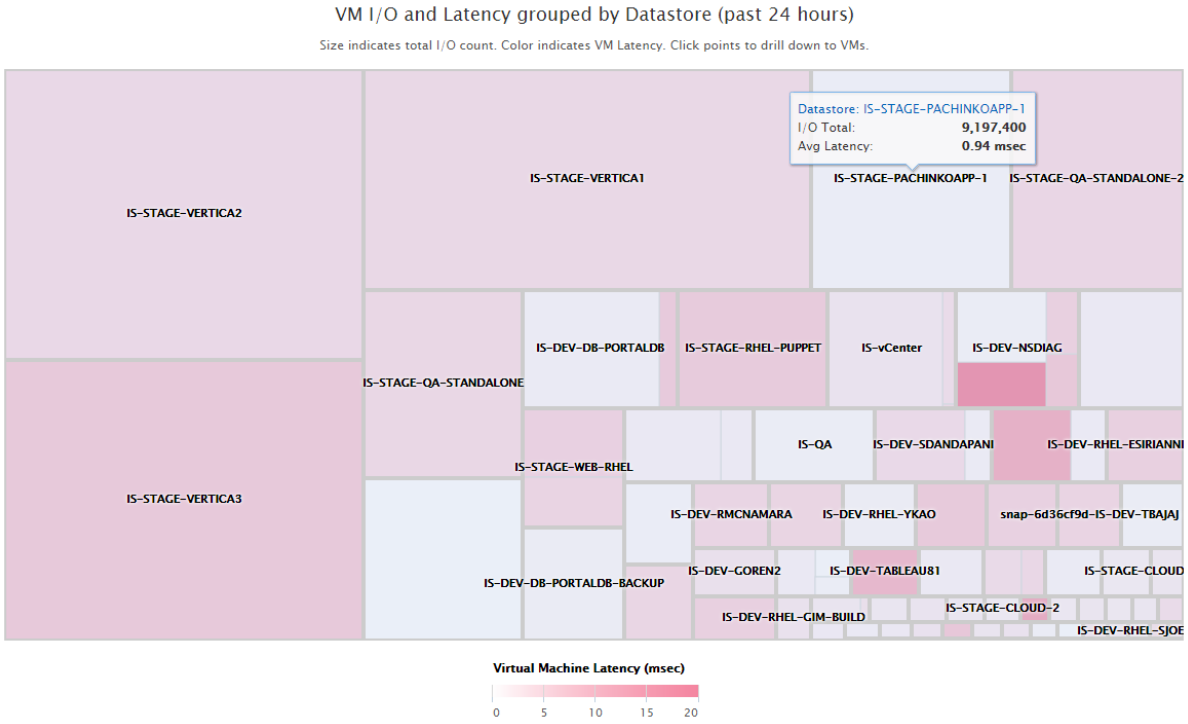


FIGURE 2. The Datastore Treemap dashboard

- **Inactive VMs**—If a VM has had no I/O operations over the past seven days, it appears in the Inactive VMs dashboard. This dashboard helps you identify VMs that are no longer in use and that have resources that can potentially be reclaimed for use elsewhere.
- **HPE Nimble Storage Arrays—**The HPE Nimble Storage Arrays dashboard view lists all of the HPE Nimble Storage arrays that are providing storage to the selected vCenter instance. It also provides links to them on HPE InfoSight to enable further detailed analysis.
- **VM Latency Analysis**—Cross-Stack Analytics for VMware enables you to examine individual VMs and analyze their respective latencies, breaking them down by hosts, network, and storage. The example in Figure 3 shows how the HPE InfoSight AI engine, using cross-stack analysis from peers around the world, provides recommendations for performance remediation. In this case, there is a problem commonly referred to as “noisy neighbor,” which is a VM that is consuming a disproportionate amount of resources. The HPE InfoSight AI engine is crossing the storage analytics engine with the VM analytics engine.

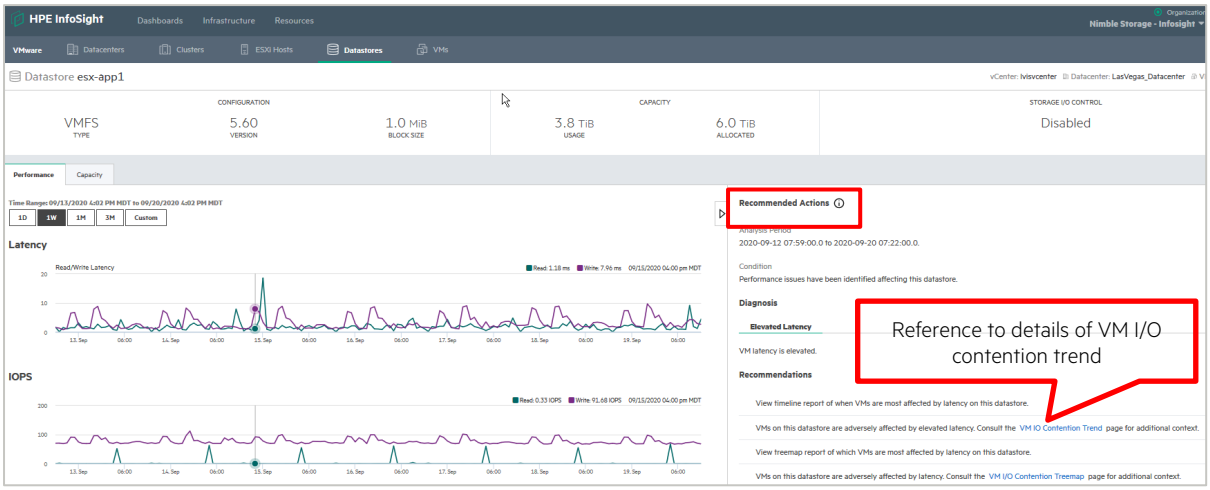


FIGURE 3. HPE InfoSight AI engine providing recommended actions for remediation of a problem with a noisy neighbor

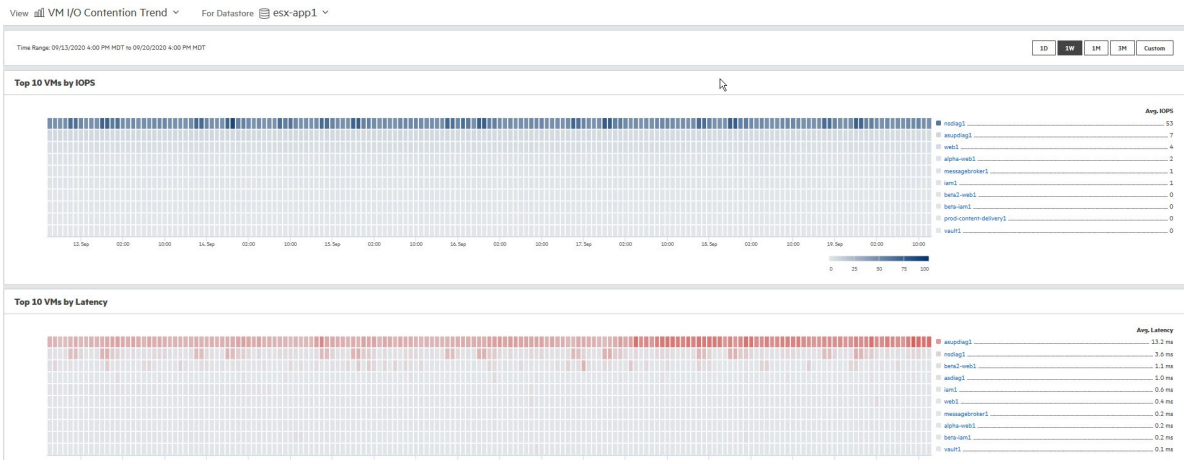


FIGURE 4. Top 10 VMs by IOPs and Top 10 VMs by Latency graphs

The two graphs in Figure 4 illustrate the I/O contention and the VMs most affected by the noisy neighbor problem. This is just one example of dozens of AI models that have been trained to recognize, diagnose, and provide remediation steps every day in easy-to-follow language.

NETWORKING CONSIDERATIONS

This section covers networking considerations and best practices when configuring networking in an HPE Nimble Storage with vSphere 7 environment.

Base connectivity for high availability

You have two options for base connectivity to the HPE Nimble Storage arrays: iSCSI or Fibre Channel.

Base iSCSI connectivity

For iSCSI connectivity between the vSphere environment and the HPE Nimble Storage arrays, the VMware ESXi™ host must have a minimum of two physical network interface cards (NICs). HPE recommends that you dedicate at least two physical NICs to iSCSI storage access. On the ESXi host, use the following NIC allocation model as a reference:

- vmnic0 and vmnic1 (for management traffic, vMotion traffic, and VM traffic)
- vmnic2 and vmnic3 (VMkernel ports for IP storage)

The VMware software iSCSI initiator is the preferred means for connecting to HPE Nimble Storage arrays by using iSCSI. Two connection methods are available to achieve high availability and load distribution:

- **Method 1:** One vmnic per vSwitch and one VMkernel port per vSwitch
- **Method 2:** Two or more vmnics per vSwitch and one dedicated VMkernel port per vmnic

Best practice: Use at least two switches and alternate cabling. For example, connect one port from each node to each of at least two switches. With both methods, the choice to bind VMkernel ports to the software iSCSI adapter depends on whether the ports are in the same Layer 2 broadcast domain and IP subnet:

- When the VMkernel ports for software iSCSI multipathing are in the same Layer 2 broadcast domain and IP subnet, you must bind the VMkernel ports to the software iSCSI adapter. Array target iSCSI ports must also reside in this broadcast domain and IP subnet.
- When the VMkernel ports for software iSCSI multipathing are in Layer 2 different broadcast domains and IP subnets, do not bind the VMkernel ports to the software iSCSI adapter.

Be sure to override the NIC teaming active/standby policy so that each VMkernel port is active on only a single vmnic.

NOTE
For detailed information about this configuration, refer to the HPE Nimble Storage documentation.

Use at least two physical NICs per controller as illustrated in Figure 5.

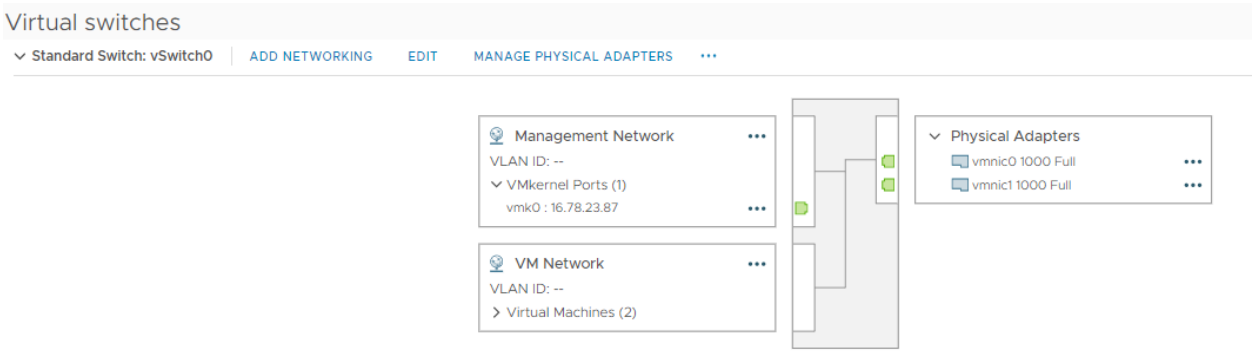


FIGURE 5. Sample network configuration using two VMkernel ports and a single vSwitch

Best practice: To prevent a single-switch failure that might cause a virtual infrastructure outage, HPE recommends that you use dual physical switches for the connection between the ESXi host and the HPE Nimble Storage array.

Network interface types

On an HPE Nimble Storage array, you can designate separate network interfaces for management traffic and data traffic, or you can share management traffic and data traffic on the same interface, although a single interface can serve both types of traffic.

Best practice: HPE recommends that you dedicate a pair of interfaces to management traffic and use the remaining interfaces to serve only data traffic. Ensure that all data access interfaces are connected to the physical switch that is dedicated to storage traffic. If the physical switch is shared with other traffic (such as management traffic, vMotion traffic, or VM networks), use a private (noncountable) address set for connectivity between the ESXi VMkernel ports and the HPE Nimble Storage data access interfaces.

You must connect the management interface to the same network segment to which the VMware vCenter Server® instance is connected. The HPE Nimble Storage vCenter plug-in requires network connectivity between the vCenter Server and the HPE Nimble Storage array management interfaces.

NOTE
As of NimbleOS 5.2, it is no longer necessary to have routable replication management addresses between sites. All replication control signaling is in line with the data path. This allows offsite replication to a cloud service provider, for example, to have secured interfaces both on-premises and off-premises.

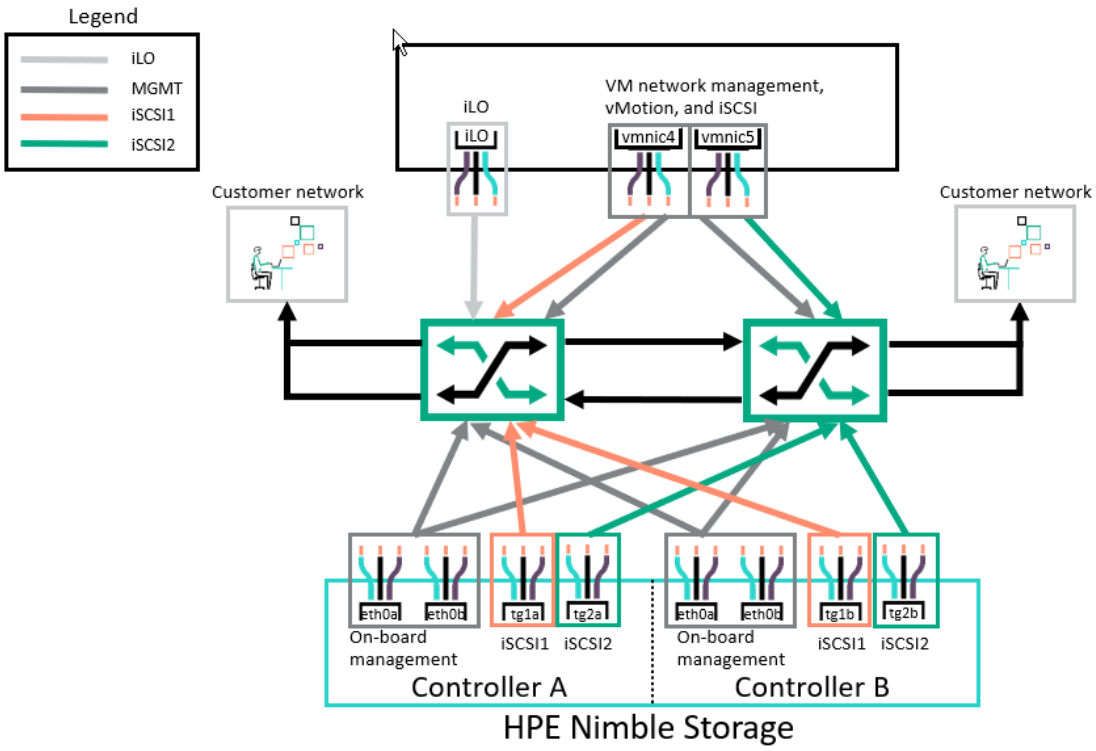


FIGURE 6. End-to-end network iSCSI connectivity

HPE recommends enabling flow control on the physical switch ports to which the ESXi interfaces and the HPE Nimble Storage array interfaces are connected. Failure to enable flow control on these ports might cause TCP-level packets to retransmit or iSCSI-level tasks to abort.

HPE also recommends the use of a jumbo frame—a 9000-byte frame instead of the default of 1500 bytes. The larger frame size reduces the processing power required to process frame headers. Jumbo frames must be enabled end-to-end, meaning the switches must have jumbo frames enabled. It is essential to ensure that jumbo frames are enabled on all switch ports between the array and servers. Jumbo frames should be enabled on all of the following ports for maximum throughput with minimal processing overhead:

- The ESXi server VMkernel ports for iSCSI traffic
- Any physical switch ports to which the VMkernel NICs are connected
- The HPE Nimble Storage network interfaces

HPE Nimble Storage Connection Manager

The HPE Nimble Storage Connection Manager (NCM) for VMware manages connections from the host to volumes on HPE Nimble Storage systems. To simplify configuring multiple connections and MPIO, NimbleOS requires that only one IP address (the iSCSI discovery IP address) be advertised at the time of discovery, not the full set of iSCSI network interfaces.

This means that you do not need to configure static iSCSI connections to the appropriate interfaces or worry about how many connections there are to a volume. NCM ensures that, because connections are made to the same address (group target portal), the connections are redirected to the appropriate distribution of actual iSCSI network interfaces.

Best practice: When you deploy ESXi on HPE Nimble Storage arrays, HPE recommends installing the NCM on the ESXi host. NCM consists of the HPE Nimble Storage Connection Service (NCS) and the HPE Nimble Storage path selection policy (PSP). NCS is essential for optimizing iSCSI sessions from the ESXi host to the HPE Nimble Storage group. The PSP optimizes I/O multipathing.

Considerations regarding NCM include:

- NCM can be installed on hosts that also connect to other arrays.
- If raw device maps are used, as can be the case with Microsoft® clusters, NCM does not support SCSI-3 persistent reservations and will require blacklisting paths. For complete information and instructions, refer to the VMware Integration Guide at HPE InfoSight.
- In HPE Nimble Storage dHCI implementations, NCM updates are handled from within vCenter using the VMware vRealize® Suite Lifecycle Manager™
- If you are scaling out with multi-array pools, the use of NCM is required.

Base Fibre Channel connectivity

Target Driven Zoning (TDZ) is a feature that enables storage arrays to create Fibre Channel fabric zones automatically. Best practice is to ensure that TDZ is enabled on the array. This feature removes the need for storage administrators to configure Fibre Channel zones manually for each initiator/target port pair, making it easier to configure Fibre Channel zones in large Fibre Channel environments.

To enable TDZ on an array, go to **Administration → Network → General**, click **Configure Active Settings**, and then check the **Enabled** box under FC Target Driven Zoning. A consideration to keep in mind when enabling TDZ is that the FC Target Driven Zoning setting automatically creates peer zones for each supported initiator group. When TDZ is enabled, the host ports (WWPNs in the initiator groups) are associated with these peer zones. The host port scans and then logs in to the target ports; administrators do not need to configure Fibre Channel zones manually.

If you have a large number of target ports, HPE recommends that you check your initiator group configuration to ensure that you have an optimal number of paths per LUN before enabling TDZ. If the Enabled checkbox does not appear, make sure that **FC + iSCSI** is selected in the protocol drop-down menu.

To establish base Fibre Channel connectivity between an HPE Nimble Storage array and the VMware compute environment, ensure that all components have a supported Fibre Channel configuration, including:

- HPE Nimble Storage arrays
- Fibre Channel switches
- ESXi installation
- Host bus adapters (HBAs)
- Drivers
- Associated cabling
- HBA utilities from Emulex or QLogic, downloaded from the manufacturer's site

To access ESXi configurations verified by HPE, refer to the HPE InfoSight Validated Configuration Matrix.

Implementing three-site availability using HPE Nimble Storage Peer Persistence and vSphere Metro storage clustering

The following three sections are excerpted from the VMware KB article Implementing vSphere Metro Storage Cluster (vMSC) using HPE Nimble Storage Peer Persistence.

What is vMSC?

vMSC is a tested and supported configuration for stretched storage cluster architectures. A vMSC configuration is designed to maintain data availability beyond a single physical or logical site. All supported storage devices are listed on either the VMware Storage Compatibility Guide or the Partner Verified and Supported Products (PVSP) pages.

What is HPE Nimble Storage Peer Persistence?

Built from a resilient architecture, HPE Peer Persistence is available on HPE Nimble Storage arrays. To the hosts connected to them, paired arrays located at metropolitan distances present a continuous storage system. This capability allows you to configure a high-availability solution between two sites where storage failover and failback remains completely transparent to the hosts and applications running on those hosts. This results in elimination of recovery times because unlike traditional failover models, the applications do not have to be restarted after a failover.

HPE Nimble Storage Quorum Witness

The HPE Nimble Storage Quorum Witness is a component provisioned as a VM that HPE recommends deploying at a third site. The HPE Nimble Storage Quorum Witness, along with the two HPE Nimble Storage systems, forms a three-part quorum system. This quorum system monitors the status of both the HPE Nimble Storage systems and the storage site inter-links. Many sites and inter-link failure scenarios are recognized by this three-part quorum system, and appropriate failover actions are implemented.

If a disaster brings down one of the storage sites, a failover to the surviving HPE Nimble Storage site is automatically initiated. During this failover operation, replicated volumes on the remaining storage system are made active. The host paths to those volumes are also made active, thereby ensuring that hosts can continue to access their volumes without any disruption or outage. Communication among the three sites for a quorum is via the Quorum Witness IP address and the service management IP addresses of the two HPE Nimble Storage systems.

Quorum Witness does not actively participate in data storage. A failure or removal of Quorum Witness from an otherwise functioning environment has no impact on data storage. However, it does impact the automatic switchover from one site to another in case of a disaster. Thus, the Quorum Witness is only a factor when one site or the inter-site links has failed.

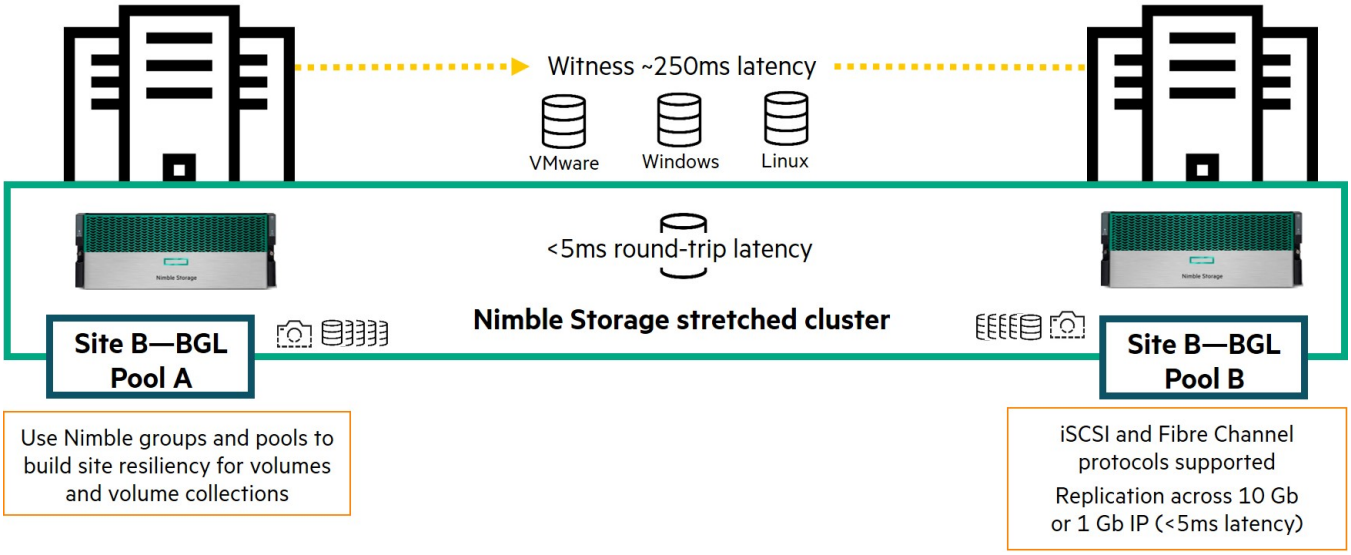


FIGURE 7. Example of a VMware stretched cluster with a Quorum Witness in a third location

NOTE

For detailed implementation and considerations, refer to the HPE Nimble Storage Peer Persistence deployment considerations technical white paper.

SRM and HPE Nimble Storage integration

SRM is a plug-in to vCenter Server that enables you to create and test disaster recovery plans in a VMware environment. SRM provides the following options for working with HPE Nimble Storage arrays:

- SRM works with the HPE Nimble Storage Replication Adapter (SRA). You can use SRM and SRA with HPE Nimble Storage arrays to perform array-based recovery operations.
- SRM 8.3 works with VASA providers to fully integrate with vVols. It provides protection granularity to the level of a VM on an HPE Nimble Storage array.

NOTE

In addition to using SRM, you can also use VASA providers running VASA 3.0 or later to provide a disaster recovery feature that restores vVols. For more information about using VASA providers with vVols, read Using VASA Provider to Provide Disaster Recovery for vVols.

Best practice: If multisite replication is available, use SRM for greater availability. For more information, refer to the SRM and HPE Nimble Storage SRA Integration guide.

Recommendations regarding best practices for HBAs

HBA manufacturers offer utilities for managing and controlling their adapters. These utilities are useful when you provision LUNs and troubleshoot connectivity because they can provide an HBA-level view of the SAN and available targets. It is usually preferable to install these tools during initial deployment.

Emulex and QLogic installations include a Common Information Model (CIM) provider and a vCenter plug-in. The CIM provider enables you to implement API integration with ESXi and to manage the HBA from the ESXi CLI.

For information about how to install and use the utilities, consult the documentation provided by the HBA manufacturer.

Installation

Install the components for Fibre Channel connectivity in a logical order, beginning with the hardware components and stepping through each piece of software. In addition to the HBA utilities, you must install the software required for storage I/O multipathing on the ESXi hosts.

HBAs and driver packages

Install the HBAs and their corresponding software in the following order:

1. Install the physical HBAs in the server according to the HBA manufacturer's specifications and instructions.
2. After the hardware installation is complete, boot the system into ESXi.
3. Locate the driver packages on the manufacturer's website; for a list of verified HBA and driver combinations, see the HPE InfoSight Validated Configuration Matrix.
4. Download and install the appropriate driver package according to the manufacturer's instructions.
5. Install the HBA utilities.

ESXi host components

ESXi provides storage I/O multipathing through the VMware multipathing solution. The solution includes built-in storage array-type plug-ins (SATPs) as well as the ability to register additional plug-ins. SATPs identify the type of storage array, control how multipathing interacts with the array, and provide configurable PSPs to set behavior for load balancing and path prioritization.

The NCM for VMware enables installation of the HPE Nimble Storage specific PSP on supported ESXi platforms. The correct SATP to use with HPE Nimble Storage arrays is VMW_SATP_ALUA; the ESXi host should detect and set the SATP automatically. After you install this SATP, the NIMBLE_PSP_DIRECTED PSP becomes available.

Visit the HPE InfoSight Software Downloads page to download the NCM for VMware and access other software integration tools.

NOTE

Multipathing using NCM now can select paths based on the lowest latency.

PROVISIONING STORAGE

For more comprehensive information on provisioning, refer to the HPE VMware Integration Guide.

To provision storage to the host, perform the following tasks in order:

1. At the ESXi host, gather information about host initiator ports.
2. At the HPE Nimble Storage array, gather information about storage target ports.
3. At the Fibre Channel switch, configure Fibre Channel access to the storage if not using TDZ/SmartSAN.
4. At the HPE Nimble Storage array, create a volume.
5. At the ESXi host, discover the new device and add the storage.

Best practice: HPE recommends that you use the HPE Nimble Storage vCenter plug-in to provision storage.

Fibre Channel provisioning considerations

Record the WWPNs for both the active controllers and the standby controllers.

Best practice: Do not use the WWNN for the array.

At the Fibre Channel switch: Configure Fibre Channel access

Configuring the Fibre Channel switch is the most crucial and error-prone task in the storage provisioning process. When you configure zoning, be sure to double-check all configurations. Use the tools provided by the switch vendor to configure zoning for the fabric.

Single-initiator zoning is an industry best practice. No more than one initiator port from the ESXi host should be located in each zone. All target ports from the HPE Nimble Storage array, both active and standby, should be in the zone with the single initiator. Configure a zone for each initiator port on the ESXi host.

You can assign aliases on the Fibre Channel switch to give human-readable names to WWPNs. If you configure aliases, be sure to record all of them for use in the array configuration.

After zoning is complete, save and apply all configurations. Be sure that configurations are applied and active in the fabric.

At the HPE Nimble Storage array: Create a new volume

On the HPE Nimble Storage array, you should create an initiator group to control host access to the Fibre Channel volumes. Initiator groups must contain the WWPNs of the initiator ports on the ESXi host.

If you configured aliases on the Fibre Channel switch, you may also use aliases on the HPE Nimble Storage array. Be aware that alias names must match exactly. If an alias is used, both the alias and the WWPN must match before access to the volume is granted.

After you create the initiator group, you must complete the following tasks to provision a new volume:

1. Create a volume with the desired name, description, and performance policy.
2. Assign the initiator group that you created previously.
3. Verify that the LUN number has been set automatically or if a specific LUN number will be used, set it manually.
4. Configure the necessary volume size and capacity settings.
5. Assign a protection policy as required.
6. Complete the volume creation.

At the ESXi host: Discover and add the new storage

Formatting the new storage requires first discovering the new device on the ESXi host and then configuring the volume for use. You should also make sure that the timeout settings are correct.

To discover the new device on the ESXi host, you need to perform a rescan. In the vSphere client, complete the following steps:

1. Select the host.
2. Click the **Configuration** tab.
3. Select the **Storage Adapters** option.
4. Click the **Rescan All** link.

After the rescan is complete, you must add the new storage to configure the volume for use. In the vSphere client, complete the following steps:

1. Select the host.
2. Click the **Configuration** tab.
3. Click the **Storage** section.
4. Click **Add Storage**.
5. Follow the prompts to add the new disk or LUN.

If you are using the volume as a datastore, be sure that all VMs residing on the datastore have an up-to-date version of VMware Tools™. This sets a critical timeout within the guest operating system.

Troubleshooting

Best practice: Ensure that the array is reporting to InfoSight.hpe.com and use the advanced Recommendations Dashboard.

If no volumes are present on the ESXi host after you complete the provisioning steps, you should review your configuration as a whole. Pay close attention to WWPNs and the zoning configuration.

HPE Nimble Storage array

Check the HPE Nimble Storage array by performing these steps in order:

1. Review the volume configuration by navigating to **Manage** → **Volumes** and selecting the volume that you created.
2. Verify that the proper initiator group is assigned to the volume.
3. Check the number of connected initiators to verify that all initiators are connected.
4. Click the initiator group name to verify that the WWPN is correct and that the initiators exist.

Fibre Channel switch

Check the Fibre Channel switch by performing these steps in order:

1. Review the zoning configuration thoroughly.
2. Verify that the WWPNs are correct for initiator ports and target ports.
3. Save and apply the zoning configuration to be sure that the configured zoning is active on the fabric.

ESXi host

Check the ESXi host by performing these steps in order:

1. Use the HBA utilities to investigate whether targets are available to the HBA.
2. If no targets are available, investigate the HPE Nimble Storage array or the Fibre Channel switch.
3. If targets are available, begin troubleshooting the ESXi storage stack. If you made other changes to the configuration, rescan for devices.

Provisioning a datastore

For simplicity and consistency, provision datastores from the HPE Nimble Storage vCenter plug-in. With the plug-in, you can create volumes from the array side and then create a vSphere Virtual Machine File System (VMFS) datastore for a selected group of ESXi hosts or all ESXi hosts in a given data center, all in one automated workflow. Leveraging the plug-in for this task greatly reduces the number of steps needed to provision storage to multiple ESXi hosts. It also eliminates the possibility of user error.

FIGURE 8: Provisioning a new datastore

NOTE

The HPE Nimble Storage vCenter plug-in applies access control records when you create new datastores so that the underlying HPE Nimble Storage volume is presented only to the hosts that you specify. If appropriate iSCSI or Fibre Channel initiator groups do not already exist, the plug-in creates new ones and maps the newly created volumes to those initiator groups.

Modifying a datastore

You can use the HPE Nimble Storage vCenter plug-in to edit the properties of a datastore after it has been provisioned. You can change the datastore size and data protection settings.

Datastore size

To change the size of a datastore, use the Grow Datastore function of the vCenter plug-in. Selecting the **Grow Datastore** function automates the process to increase the size of the datastore. This process grows the underlying HPE Nimble Storage volume and expands the VMFS file system.

NOTE

You cannot decrease the size of datastores.

Best practice: Set up space consumption alerts on HPE InfoSight to monitor space consumption to eliminate the possibility of consuming all the space.

FIGURE 9: Growing a datastore by using the HPE Nimble vSphere plug-in

Data protection

You can specify datastore protection settings directly in the HPE Nimble Storage vCenter plug-in when you provision the datastore. If requirements change later, you can modify the protection settings by selecting the **Edit Datastore** option in the plug-in.

Define protection settings for a given datastore as either a stand-alone volume or part of a volume collection. If you are protecting a datastore as part of a collection, specify an existing collection name or create a new one that uses the desired settings.

The following figures illustrate the settings to implement as a best practice. The screenshots show where to edit the datastores to enable datastore protection policies, also known as “snapshots.”

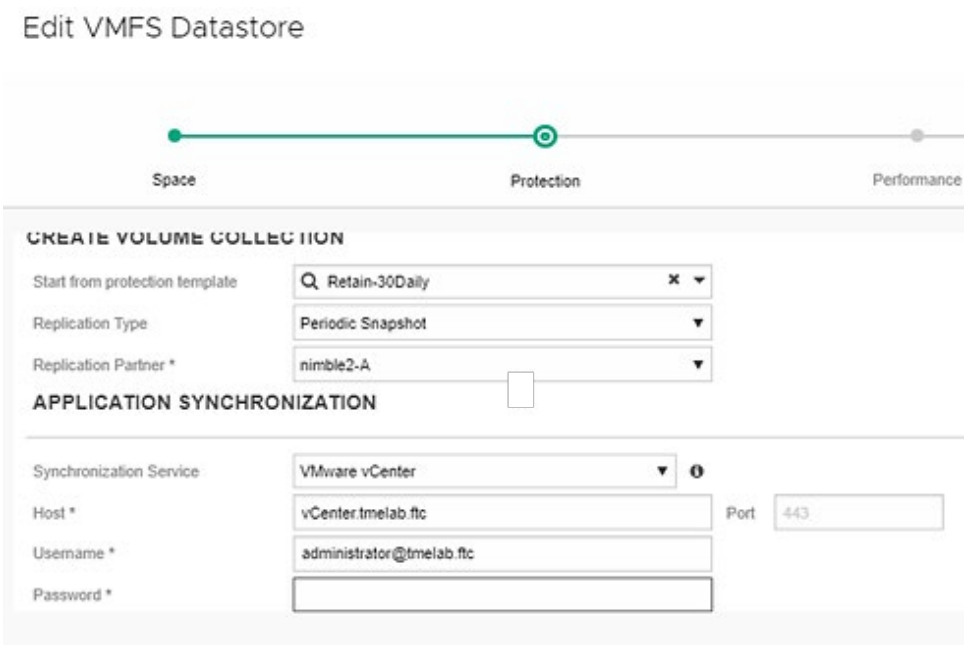


FIGURE 10: Defining datastore protection

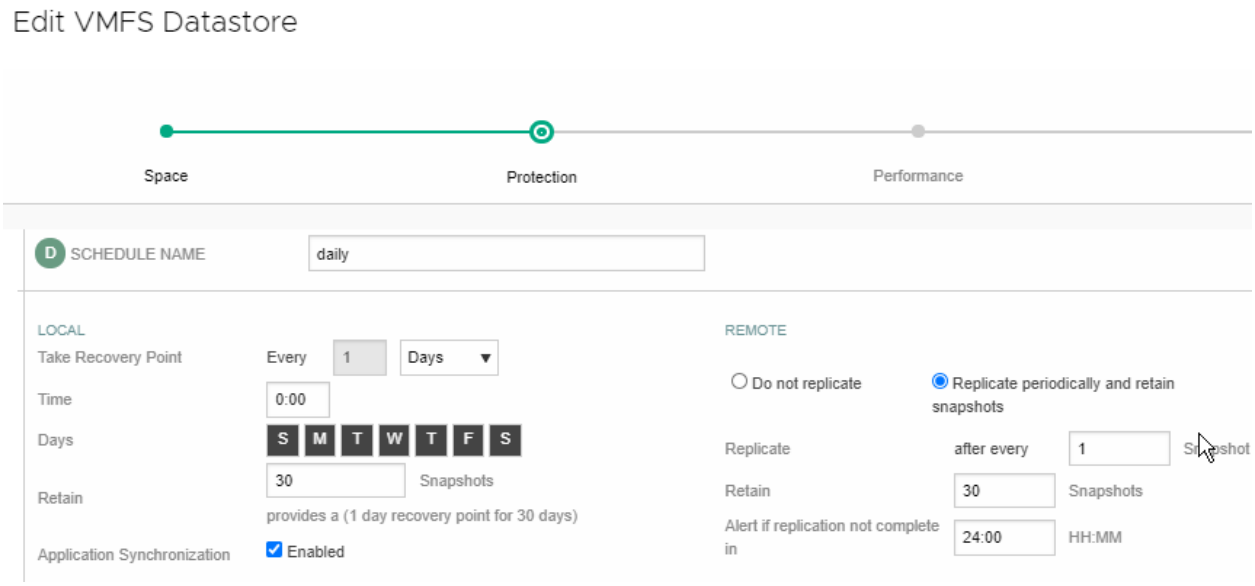


FIGURE 11: Datastore protection schedule

When you create a new volume collection or choose to protect a stand-alone volume, you have the opportunity to enable VMware synchronized snapshots. The decision to select this option depends on several factors that are covered in the "When to Use VMware Synchronized Snapshots" section of the Configuring Volume Collections page in HPE Nimble Storage Deployment Considerations for VMware vSphere 6.

To take a datastore snapshot, select **Snapshot Datastore** in the plug-in.

Deleting a datastore

The HPE Nimble Storage vCenter plug-in automates the task of datastore deletion. It first removes the datastore from vCenter and then deletes the underlying HPE Nimble Storage volume. This process is carefully orchestrated to avoid an all-paths-down condition.

Datastore deletion requires only two steps:

1. Unregister, remove, or migrate all VMs from the datastore that you will remove.

IMPORTANT
You cannot proceed with datastore deletion without completing this first step.

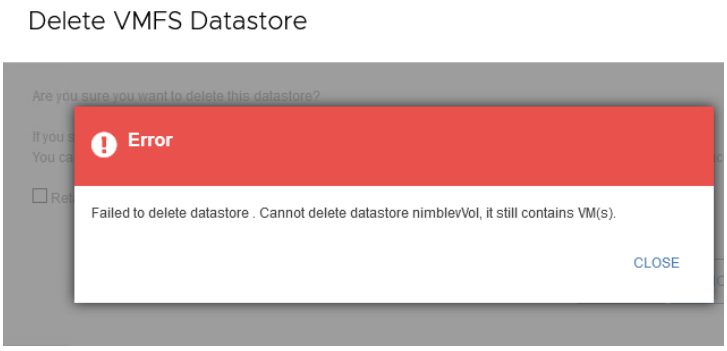


FIGURE 12. Datastore deletion warning

2. In the HPE Nimble Storage vCenter plug-in, select the datastore to be deleted and then click the waste bin icon to delete the selected datastore.

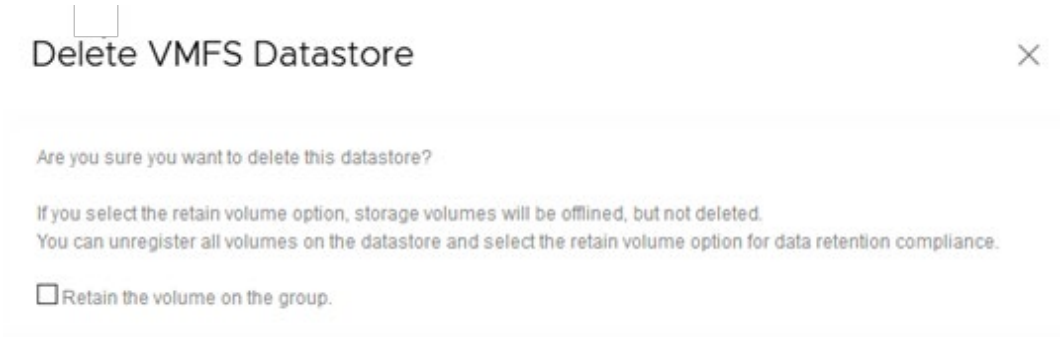


FIGURE 13. Deleting a datastore with the HPE Nimble Storage vCenter plug-in

Cloning a datastore

The HPE Nimble Storage vCenter plug-in can also automate the task of cloning a datastore. With this functionality, you can create one or more clones based on an existing snapshot, or you can create a new snapshot on which to base the clone.

The plug-in automates the workflow of creating the space-efficient and time-efficient zero-copy clone on the HPE Nimble Storage array, mapping it to the ESXi hosts, resignaturing the VMFS volume, and renaming the datastore. You can then import VMs into inventory or attach individual virtual disks to existing VMs. In addition to populating development or test environments, this functionality can be useful for data recovery.

Datastore performance overview

Data performance collection is detailed in the Nimble GUI with interwoven views. For example, specific volumes in a datastore can be visualized from individual VMs to identify problems such as noisy neighbors on vSphere servers.

Cloning a datastore provides a fast and efficient way to protect data from accidental deletions or data corruption. The following figure illustrates all datastores associated with a particular site. From here a datastore can be selected for cloning.

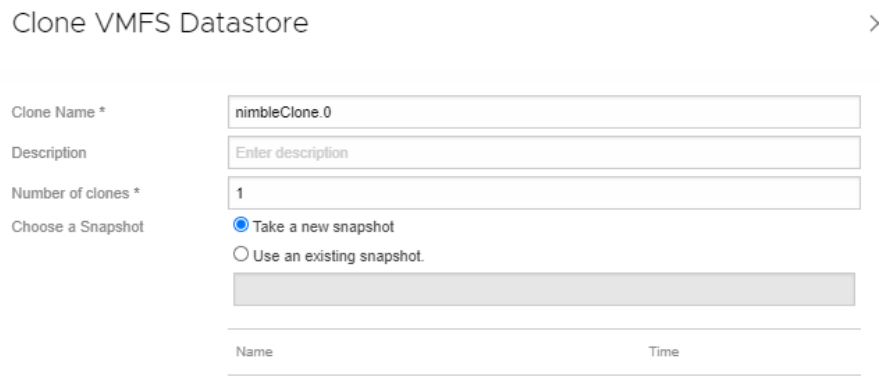
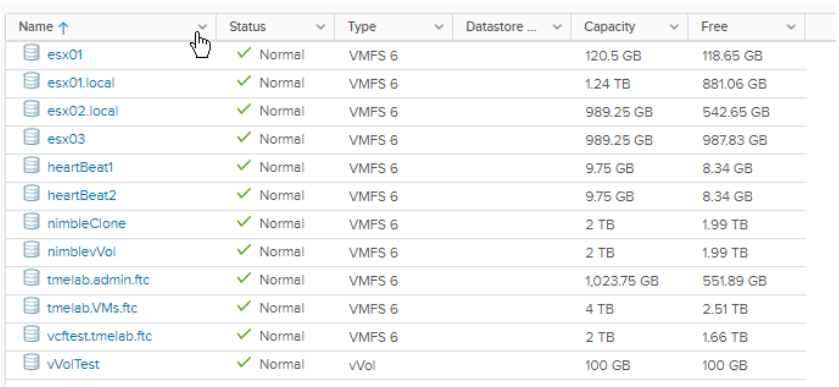


FIGURE 14. Cloning a datastore

Two views are available:

- The **datacenter** view—The datacenter view shows all storage associated with a particular site from inside vCenter.
- The **datastore** view—The datastore view provides a fine-grained view of individual HPE Nimble Storage volumes that are attached as datastores.



Name	Status	Type	Datastore ...	Capacity	Free
esx01	Normal	VMFS 6		120.5 GB	118.65 GB
esx01.local	Normal	VMFS 6		1.24 TB	881.06 GB
esx02.local	Normal	VMFS 6		989.25 GB	542.65 GB
esx03	Normal	VMFS 6		989.25 GB	987.83 GB
heartBeat1	Normal	VMFS 6		9.75 GB	8.34 GB
heartBeat2	Normal	VMFS 6		9.75 GB	8.34 GB
nimbleClone	Normal	VMFS 6		2 TB	1.99 TB
nimblevVol	Normal	VMFS 6		2 TB	1.99 TB
tmelab.admin.ftc	Normal	VMFS 6		1,023.75 GB	551.89 GB
tmelab.VMs.ftc	Normal	VMFS 6		4 TB	2.51 TB
vcftest.tmelab.ftc	Normal	VMFS 6		2 TB	1.66 TB
vVolTest	Normal	vVol		100 GB	100 GB

FIGURE 15. Datacenter view

In addition, the datacenter view provides detailed information regarding the performance of any particular datastore.

Datastore overview

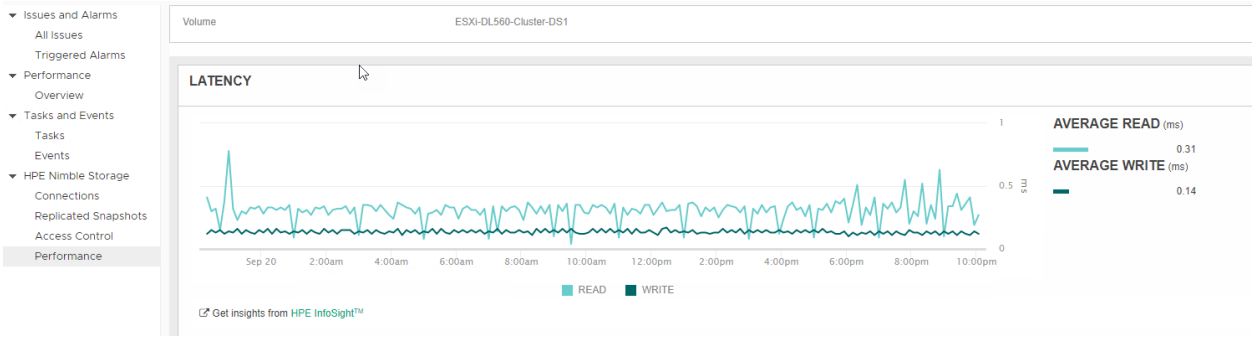


FIGURE 16. Datastore view in vCenter provides detailed views of HPE Nimble Storage specific datastore information

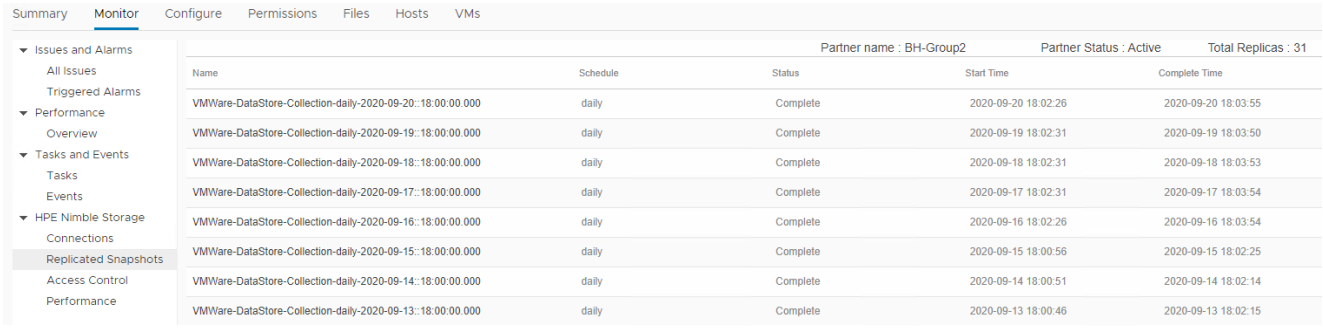


FIGURE 17. Replicated snapshots are available in this view from the Monitor tab

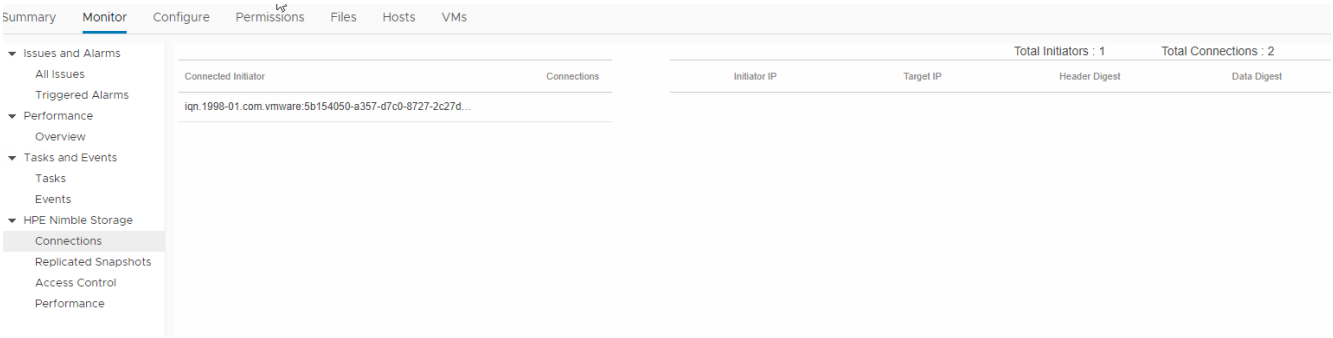


FIGURE 18. Connected hosts are also available in this view from the Monitor tab

The vSphere web client provides performance information contextually within each datastore. To see the information, select **Monitor** ⟶ **Performance** ⟶ **Nimble Volume Performance**. The datastore summary contains configuration information for each datastore, including HPE Nimble Storage volume information, space information, HPE Nimble Storage protection policy, and HPE Nimble Storage volume access control.

VIRTUAL STORAGE ACCESS CONSIDERATIONS

You can connect networked storage to vSphere in four primary ways:

- Create a VMFS datastore on an HPE Nimble Storage volume.
- Attach VMs directly to HPE Nimble Storage volumes by using an iSCSI initiator in the guest operating system.
- Create a raw device map (RDM) in either physical or virtual compatibility mode to the HPE Nimble Storage volume.
- Store VMs in VMware vVols directly on the HPE Nimble Storage array.

By planning your HPE Nimble Storage volume creation carefully, you can maximize the benefits of the HPE Nimble Storage array. Each storage attachment method has its own use cases and benefits, and each requires planning considerations.

VMDK in a VMFS datastore

The simplest way to configure HPE Nimble Storage arrays with vSphere is to mount an HPE Nimble Storage volume as a VMFS datastore. At a minimum, VMFS datastores are used to hold the VM configuration and the operating system volume.

For application-aware quiescing, HPE Nimble Storage arrays are integrated with VMware Tools with the VMware VSS Provider for Microsoft Volume Shadow Copy Service (VSS). This integration makes VMFS volumes suitable for storing transactional data from applications such as Microsoft SQL Server or Microsoft Exchange.

Using VMFS datastores reduces the management burden because this approach does not require you to install additional tools. It also avoids the maintenance that would otherwise be required on each guest to properly quiesce applications or databases. In addition, VMFS datastores make it possible to keep the entire VM together on the same protected volume.

VMFS datastores provide a convenient method of mounting storage to the VMware platform. However, this method does have tradeoffs that must be considered.

Benefits

VMFS datastores are appropriate if you want to take advantage of features such as:

- Increased flexibility
- Increased efficiency as VMFS datastores ae not overprovisioned
- Fine-grained performance troubleshooting and reporting
- Both VM operating system disks and application disks configured as virtual machine disks (VMDKs) on VMFS
- Application-consistent quiescing through the VMware Tools VSS driver
- Item-level recovery

VMFS datastores also offer significant advantages:

- They are simple to configure, with no in-guest iSCSI initiator to install or maintain.
- They can be fully integrated into SRM for VM protection, test failover, failover, and failback.

Planning considerations

If you plan to use VMFS datastores, it is important to consider that if all VMs in VMFS volume host applications are stateless in nature (such as a web server, a file server, or a print server), VMware VSS-quiesced snapshots are not required. In this case, ensure that the volume collection synchronization setting is set to **None**.

Guest-connected, direct-attached iSCSI volumes

The most cost-effective way to attach VMware ESXi servers to the HPE Nimble Storage array is to use iSCSI over an existing Ethernet network. A minimum of 10 Gb interfaces should be used. Using iSCSI also provides the most flexible. Be mindful of the following considerations when using iSCSI:

- Running multiple virtual disks on a VMFS volume requires additional time for VMware VSS-quiesced snapshots to be created on the given datastore.
- Create the datastore with the HPE Nimble Storage vCenter plug-in to ensure that the correct performance policy is selected.
- Ensure that the VM guest operating system partition is block-aligned (specifically for Microsoft Windows®).
- You can perform item-level recovery by cloning the VMFS datastore from the target snapshot and attaching virtual disks to a recovery VM.
- If you are using the volume as an RDM to Linux® guests, additional timeout settings are required on each guest. You can use the following CLI commands to set them:

```
for i in /sys/class/scsi_generic/*/device/timeout; do echo 180 > "$i"; done echo 'for i in
/sys/class/scsi_generic/*/device/timeout; do echo 180 > "$i"; done' >> /etc/rc.local
```

Best practice: For Red Hat Enterprise Linux (RHEL) virtual machines, HPE recommends using the HPE NCM for Linux.

The guest-connected method provides integrity for the application data during snapshot backup operations. It also provides quick item-level recovery. This hybrid storage architecture consists of a VMFS datastore that holds the guest operating system and application binary data. The application data, such as database and database log volumes, is attached to the VM through a guest-based iSCSI initiator that communicates directly with the HPE Nimble Storage array.

The tradeoff for using this connection method is the additional configuration and maintenance required for the software iSCSI initiator inside the VM guest operating system. In addition, you must implement a custom script to use with SRM so that the VMs can access their guest-connected storage during test recovery, recovery, or failover.

This method is appropriate to use if you have:

- A VM operating system disk (VMDK on VMFS)
- VM application disks (NTFS/ext3)
- Guest-connected application-consistent quiescing through HPE Nimble Storage Windows Toolkit VSS integration
- Item-level recovery

Benefits

This method offers the following benefits:

- Log truncation for Microsoft Exchange logs with HPE Nimble Storage Windows Toolkit VSS integration
- The simplicity of management with a one-to-one mapping between array volume and application data volume
- Ease of interchange between virtual and physical environments without VMDK conversion
- Ability to tune volume block size to match the application-data block size

Planning considerations

If you plan to use this method, consider the following points:

- For data volumes that contain Exchange or SQL Server data, consider protecting the data by using a volume collection that is configured to use application-specific VSS synchronization policies.
- SRM requires a custom script (customer-defined, not created, or maintained by HPE) for mounting guest-connected storage during test failover and actual failover.
- Be sure to select the correct performance policy during volume creation. If a custom policy does not already exist for the application, create one using appropriate settings.
- Ensure that in-guest MPIO, firewall, and disk timeout registry settings are configured properly inside the VM.

NOTE

For step-by-step instructions, refer to the HPE Nimble Storage VMware Integration Guide.

- Ensure that the VM guest operating system partition is aligned (specifically for Windows XP and Windows 2003).

RDM in physical compatibility mode

Raw device mapping enables you to give a VM direct access to an HPE Nimble Storage volume that has been presented to the host that contains the VM.

This method is appropriate if you are using VMDK for operating system and application binaries and RDM in physical compatibility mode for application data and in cases where SCSI-3 persistent reservations are required.

Benefits

The RDM method offers the following benefits:

- Provides a means for guest VMs to control the entire volume when connected to HPE Nimble Storage Fibre Channel arrays
- Provides full integration with VMware Site Recovery Manager without the need for additional scripts

Planning considerations

If you plan to use RDMs, consider the following points:

- There is typically no performance benefit from using RDMs as opposed to VMDKs or guest-connected iSCSI.
- When HPE Nimble Storage VSS integration is used, snapshots are verified through guest-connected iSCSI, even when RDMs are used.
- RDM development efforts will be waning as storage moves towards vVols.

Best practice: Avoid using RDMs except in cases where the use of SCSI-3 persistent reservations is required, such as Microsoft clustering.

VMware vSphere vVols

The vVols framework is a storage technology introduced in vSphere 6 and supported since NimbleOS 3. With vVols, VMDKs are treated as high priority and perform better because the guests connect directly on the storage array without being abstracted behind a VMFS datastore.

On an HPE Nimble Storage array, a VMDK that was created as a vVol exists as a native HPE Nimble Storage volume. It can be tuned through the use of performance policies for the specific application type that runs on the VM. For example, a VM running SQL Server might have three data disks: one for the operating system and application binaries, one for the database data, and one for the database logs. Each would have attributes, such as block size, caching policy, data reduction policy, and an encryption algorithm that are optimized for that specific disk rather than being grouped in a datastore with a generic VMFS performance policy.

In addition to data vVols that correspond to each VMDK, a configuration vVol is also created for the VM to store information about that VM. A vVol for swap space is created dynamically and destroyed when the VM is powered on or off. Because the number of HPE Nimble Storage volumes created with vVols might be quite large, it is important to note the number of volumes required and ensure that this number is well within the volume maximum for your HPE Nimble Storage array.

Because data vVols are native HPE Nimble Storage volumes, you can take advantage of native HPE Nimble Storage features that work at the volume level. For example, you can take a VM snapshot by using highly efficient HPE Nimble Storage volume snapshots, grouped in a snapshot collection for consistency across all of the VMDKs in the VM. Creating a VM clone from the vSphere web client invokes an HPE Nimble Storage zero-copy cloning operation to instantly provision highly space-efficient clones, regardless of the size of the VM. No data is copied, and these clones are extremely fast.

Unlike VMs in a VMFS datastore, deleting a VM on a vVol causes the deletion of the HPE Nimble Storage volume on which it is stored. To protect against accidental deletion, HPE has implemented a deferred deletion feature. With default settings, which can be adjusted to suit user preference, the volumes for a deleted VM are taken offline and hidden from the vCenter environment. Without further action, the volumes are deleted.

NOTE

By default, the deferred deletion period is 72 hours. The HPE Nimble Storage support team can assist if you require an alternate length of time for deferred deletion.

IMPORTANT

For the configuration vVol to be recovered, it must be part of a volume collection, and there must be at least one snapshot. A configuration vVol becomes part of a volume collection when a protection schedule is part of the SPBM policy.

This method is appropriate if you want separate, optimized volumes for operating system, data files, and log files. Each VMDK is represented by a unique HPE Nimble Storage volume.

Benefits

The vVols method offers the following benefits:

- Block size and performance policies are tuned for the type of data stored on the vVol.
- VM snapshots are native HPE Nimble Storage snapshots.
- VM clones use native HPE Nimble Storage zero-copy cloning.

Planning considerations

If you plan to use this method, consider the following points:

- Configure VMware storage policies to use HPE Nimble Storage array capabilities as advertised by the HPE Nimble Storage VASA provider.
- Each VM consumes one HPE Nimble Storage volume for configuration data, one for swap space, and one for each data VMDK. Plan accordingly to stay within the maximum HPE Nimble Storage volume count.
- vSphere 7 Update 1 (U1) support iSCSI and Fibre Channel provisioned vVols for Principal Workload Storage in VMware VCF (3.9.1 and later)

Best practice: Use vVols for all VMware guest deployments.

NOTE

For more information, refer to the full vVols implementation guide: VMware vSphere Virtual Volumes on HPE Nimble Storage Implementation Guide.

---

vSphere vVols—Configuring volume collections

Volume collections are accessed from **Manage** → **Data Protection** → **Create Volume Collection** and are used to configure data protection for volumes on HPE Nimble Storage arrays. They determine the frequency with which volume snapshots are taken, whether the snapshots should be replicated to a downstream replication partner, and how many snapshots should be retained on both the source and the replica. Volume collections contain one or more HPE Nimble Storage volumes, and the protection policies defined for the volume collection apply to all volumes in the collection as a group.

For HPE Nimble Storage volumes that are used as VMware datastores, you have the option of configuring VMware synchronized snapshots for the volume collection. It is important to understand what this option entails and when it is appropriate for you to select it.

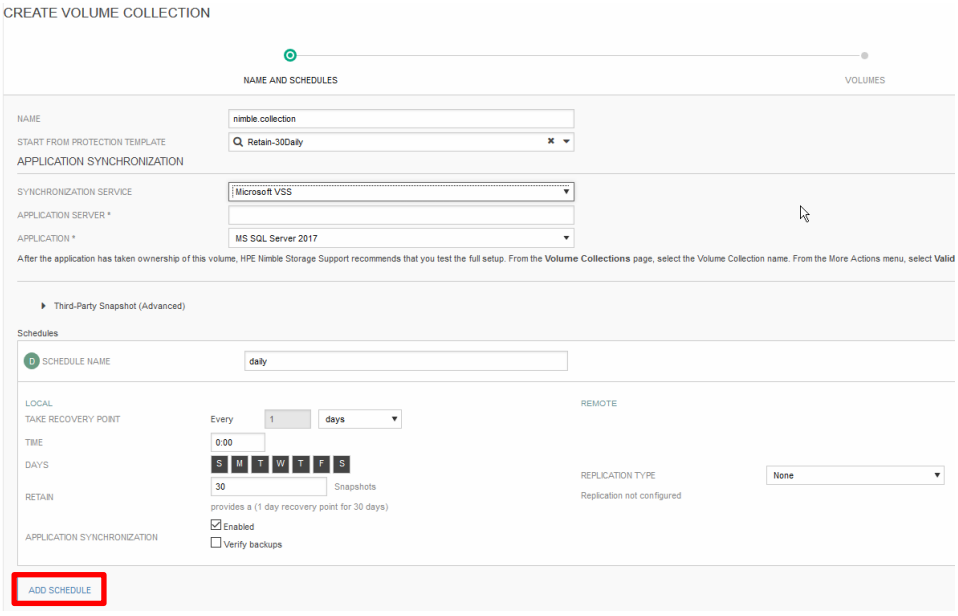


FIGURE 19: Configuring volume synchronization settings

VMware synchronized snapshots

You can use VMware synchronized snapshots to quiesce VMs by creating VMware VM-level snapshots before creating an array-level snapshot. Selecting this option for a given volume collection adds several steps to the process of creating snapshots of the member volumes.

Configuring volume collections

When the HPE Nimble Storage array triggers a scheduled snapshot, it first passes the request to vCenter, which uses VMware Tools to coordinate snapshots for every VM in the datastore. The VMware Tools VSS driver triggers an application quiesce on a VSS-enabled application in the VM. When the data files are in a consistent state, it sends a response back to vCenter.

After the VMware snapshots are created for all VMs in the datastore, NimbleOS creates an array-based snapshot for the HPE Nimble Storage volume associated with the datastore. After the array snapshot is in place, NimbleOS signals vCenter to remove each of the individual VMware snapshots. These VM snapshots are no longer needed because their quiesced state is preserved in the HPE Nimble Storage volume–level snapshot.

IMPORTANT
Before an array-level snapshot can be created, every VM on every datastore in the volume collection must first be quiesced. This process can take a long time if there are many VMs or if the VMs are generating a lot of I/O.

Best practice: HPE recommends that you limit both the number of VMs in a datastore that uses VMware synchronized snapshots and the number of datastores that belong to a single HPE Nimble Storage volume collection.

When to Use VMware synchronized snapshots

If a VM hosts applications that are stateless in nature (such as a web server, a file server, or a print server), then an array-based snapshot is generally sufficient.

Best practice: If the VM hosts applications such as Microsoft SharePoint, Exchange, SQL Server, or an Oracle® database, then HPE recommends using the VSS framework to quiesce the application properly.

If a given VMFS volume contains only VMs that run stateless applications without the need for VSS quiescing, HPE generally recommends that you set the HPE Nimble Storage volume synchronization to **None**. This setting streamlines the backup of the datastore by eliminating the step of coordinating VMware VM-level snapshots in addition to the HPE Nimble Storage snapshot that is being created. If a given VMFS volume contains at least one VM running an application that requires VSS quiescing, then the HPE Nimble Storage volume must have VMware vCenter checked for the synchronization setting.

VMware Synchronized Snapshots should not be configured on volume collections containing vSphere Virtual Volumes.

NOTE
The VSS implementation in VMware Tools does not truncate logs for applications such as Exchange. Therefore, you must ensure that the environment has an application-aware backup solution if this method is used.

Thin, zero thick, and eager-zeroed thick considerations

A key characteristic of storage provisioning originated from the need to estimate the amount of data space required over the lifetime of applications. The attempt at estimating frequently resulted in an underestimation of storage requirements, which led to downtime while administrators searched for available storage resources and attached them to the production server. Overestimating storage resources became the norm to avoid the penalty of downtime associated with underestimating. The result was an unused space that still had to be paid for upfront. Therefore, 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 (sometimes referred to as "lazy" zeroed thick)
- Eager-zeroed thick

The provisioning model that you select for your datastores affects the density of VMs contained on your storage array, and it can affect the runtime of VMs. It can also ensure that critical VMs will always have access to provisioned space and that they will continue to run if the storage array reaches full capacity. The following table lists the provisioning models.

TABLE 1. Provisioning models for datastores.

VMDK format	Space dedicated	Zeroed-out blocks	HPE Nimble Storage provisioning
Thin	As needed	As needed	Default (thin)
Zero thick	At creation	As needed	Use volume reservation
Eager-zeroed thick	At creation	At creation	Use volume reservation

By default, HPE Nimble Storage arrays use the thin-provisioned model to allocate physical space. Typically, you should match the HPE Nimble Storage provisioning to your VMFS provisioning. For example, if you choose VMware thick provisioning, then you can override the HPE Nimble Storage default thin provisioning by reserving space during HPE Nimble Storage volume creation. If you reserve less than 100% of the HPE Nimble Storage provisioned volume space, the remainder of the volume continues to be thin provisioned.

The guidelines in the following sections can help you decide which VMDK format to use with HPE Nimble Storage arrays.

Thin provisioning

Thin-provisioned virtual disks on vSphere enable you to overcommit space at the datastore level. Overcommitting space means that you can provision more space to VMs than the actual capacity of the datastore allows. If the environment has a large number of VM deployments with unpredictable space growth, using thin-provisioned virtual disks on thin-provisioned VMFS volumes might be a viable solution. However, you must exercise caution to prevent space overcommitment at the VMFS datastore level from causing out-of-space conditions for VMs.

If you do not use thin-provisioned virtual disks, ensure that the datastore usage on disk alarm setting is enabled at the highest level of the vSphere infrastructure. Also, make sure that the alarm has an acceptable value range for the warning and alert triggers. In vSphere, the predefined default value for warnings is 75% of disk space usage; the value for alerts is 85%.

When you receive a warning or alert, you can use the HPE Nimble Storage vCenter plug-in to resize datastores. Also, in a VMFS datastore that contains both thin-provisioned and thick-provisioned virtual disks, you can correct the out-of-space condition by converting thick-provisioned virtual disks to a thin format. You can convert them through a storage vMotion migration to another datastore, followed by a migration back to the source datastore.

Thick provisioning and eager-zeroed thick provisioning

For lazy-zeroed thick virtual disks, the datastore is zeroed out on demand as data is written. In contrast, eager-zeroed thick virtual disks are zeroed out fully at creation time. Because of this difference, eager-zeroed thick virtual disks are generally considered to offer superior performance.

Traditionally, the downside has been the space and time required to write all of the zeroes when provisioning. On HPE Nimble Storage arrays, however, data reduction technologies intercept the zero writes. Therefore, the provisioning jobs return very quickly and do not consume additional capacity on the array.

Best practice: HPE recommends that you use the eager-zeroed thick VMDK format.

vSphere storage feature usage considerations

The usage considerations related to vSphere storage fall into three categories:

- Storage I/O control (SIOC)
- vSphere Storage DRS
- SPBM

SIOC

SIOC works with standard quality of service (QoS) for shared storage access between VMs. SIOC is designed to address the noisy neighbor problem that is common in shared services environments and operates when the latency threshold is exceeded. SIOC enables you to define shares and IOPS limits at the level of each VMDK to ensure that critical VMs are treated as high priority better performing and configured individually. This latency triggered activation is in contrast to standard QoS, which is always operating.

NOTE

Standard QoS is a free feature whereas SIOC requires a VMware Enterprise Plus license from VMware.

HPE Nimble Storage considerations

No additional configuration is required on the HPE Nimble Storage array side to take advantage of this feature. Simply set higher share values and IOPS limits for mission-critical VMs, and the I/O QoS enforcement is adjusted accordingly.

vSphere Storage DRS

VMware vSphere 5 introduced a new object called a "datastore cluster," which is a collection of datastores that are aggregated into a single logical unit of consumption from the administrator's perspective. When a datastore cluster is enabled with Storage DRS, the VMDKs can 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. The Storage DRS feature leverages the datastore cluster construct to perform the following key functions:

- Placing the initial VM on the datastore with the lowest space utilization
- Balancing the load based on capacity usage
- Balancing the load based on I/O load

Storage DRS provides value for automating storage resource management. If you use datastore clusters on HPE Nimble Storage arrays, be sure to consider the backup-and-restore aspects in relation to the infrastructure. The following scenarios provide examples.

Scenario 1: VMs with operating system in VMDK on a VMFS volume and application data disk on a guest-connected HPE Nimble Storage volume

If multiple VMFS volumes are used to store the VMDK for the VM operating system disk, then you can create a datastore cluster for all of the VMFS volumes with the Storage DRS feature enabled. Because the guest-connected storage is treated as network traffic in ESXi, the Storage DRS operation does not affect the application data volumes.

You should place all datastores that belong to the datastore cluster in the same volume collection, along with the guest-connected volumes, for the creation of crash-consistent operating system snapshots.

Scenario 2: VMs with both operating system and application data disk in VMDK on a VMFS volume

If operating system and application VMDKs are on separate VMFS volumes, it is best to create two separate datastore clusters so that different types of VMDKs do not end up together on the same datastore.

If both operating system and application data disks are on the same VMFS volume, and multiple VMFS volumes are serving VMs in the same fashion, then you can group the VMFS volumes together on the same datastore cluster to take advantage of the VM placement and of migration between datastores to balance the load.

Best practices: Consider using VM and VMDK affinity rules to ensure that the VMDKs for the VMs stay together on the datastore. Keeping the VMDKs together is especially important when an HPE Nimble Storage array is used to back up the virtual infrastructure.

The following recommendations apply to both types of deployment scenarios:

- HPE recommends that you place Storage DRS in manual mode so that the user can review the generated recommendation and determine whether the storage vMotion migration should take place.
- It is imperative to keep track of the recommendations that have been applied. This means noting when the VMDK of a VM is migrated from one datastore to another in a given datastore cluster. Tracking the individual VMs simplifies the restore process by identifying the specific HPE Nimble Storage array snapshot that contains the snapshot image of the VM in need of a restore.

Storage Policy-Based Management

The SPBM feature enables you to predefine storage requirements for VMs. Policies are built from storage array capabilities made known to vSphere through the VASA provider for the HPE Nimble Storage array. When provisioning a new VM, select a storage policy to apply to the VM and optionally select additional storage policies to apply to individual virtual disks within the VM.

HPE Nimble Storage VASA provider

The HPE Nimble Storage VASA provider runs directly on the HPE Nimble Storage array. This arrangement makes the provider highly available and eliminates the need to maintain additional infrastructure for it. Figure 20 shows the window where you register the provider with vSphere. For a step-by-step guide to registering the provider, refer to the HPE Nimble Storage VMware Integration Guide.

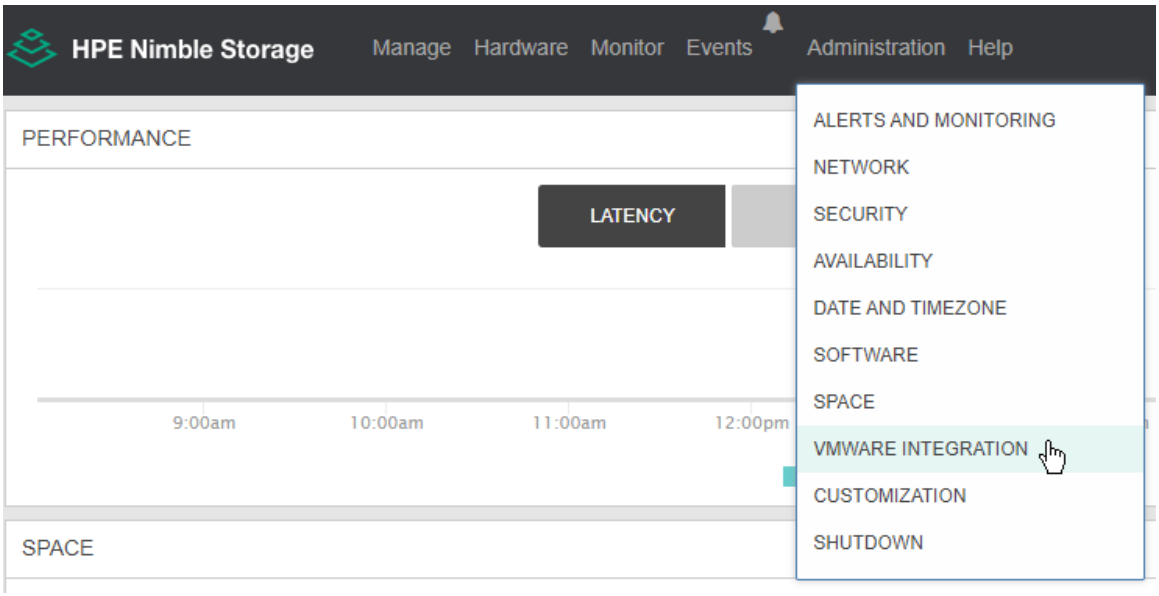


FIGURE 20: Registering the HPE Nimble Storage VASA provider in the HPE Nimble Storage GUI

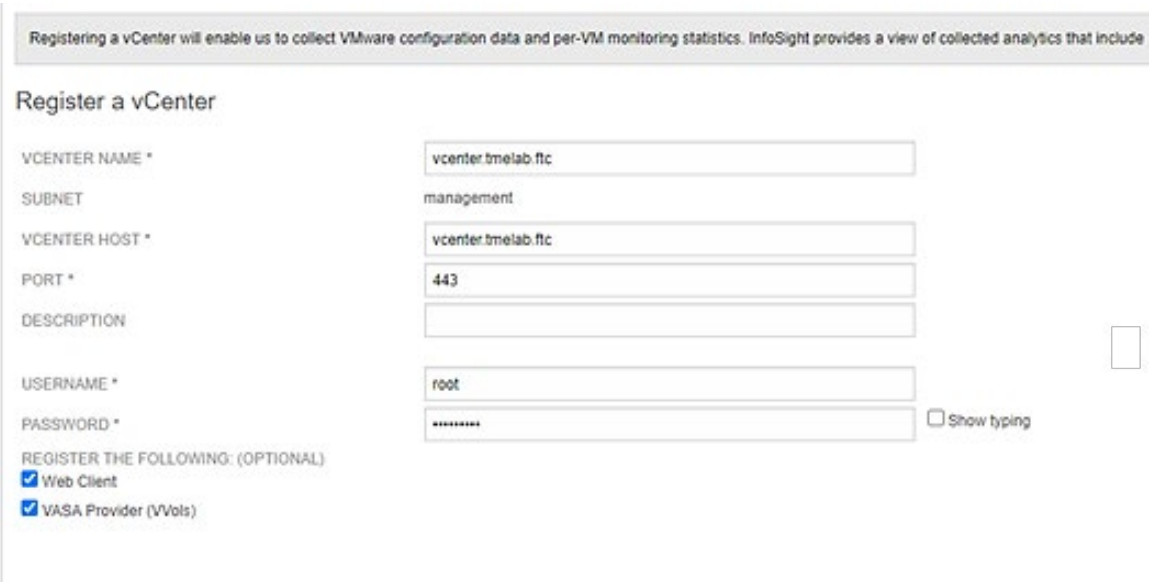


FIGURE 21. Enter connection information and credentials to register a vCenter

Storage policies

Using the capabilities advertised to vSphere through the HPE Nimble Storage VASA provider, you can create custom storage policies that define the attributes of the HPE Nimble Storage volumes to be created as vVols. These storage policies can implement one or more of the rules listed in the following table.

Table 2 lists the HPE Nimble Storage SPBM rules. Figure 22 shows the window in which these rules are entered.

TABLE 2. HPE Nimble Storage SPBM rules

Rule	Function
All-flash	This rule allows the vVol to be placed in an all-flash storage pool.
vVol functionality	NimbleOS 5.2 supports snapshots clones, volume, and replicas.
Application policy	This rule optimizes the vVol based on the expected characteristics of the application that uses the volume. Application policies are tied to HPE Nimble Storage array application-specific performance policies. They control attributes such as block size, data reduction, caching, and behavior if the quota is exceeded.
Deduplication	Although deduplication is typically configured based on the selected application policy, this rule can override the application policy so that you can enable or disable deduplication as desired.
Protection schedule	A protection schedule enables you to configure data protection as part of the storage policy. Schedule scans are by the minute or hourly, daily, or weekly. The rule defines these settings: • When snapshots should be taken • How many snapshots should be retained locally • How frequently snapshots should be replicated to an optional downstream replication partner • How many snapshots should be retained remotely • Whether the replicated volumes should be deleted • When the source volume is deleted
Data encryption cipher	Defines whether the volume should be unencrypted or encrypted with AES-256.

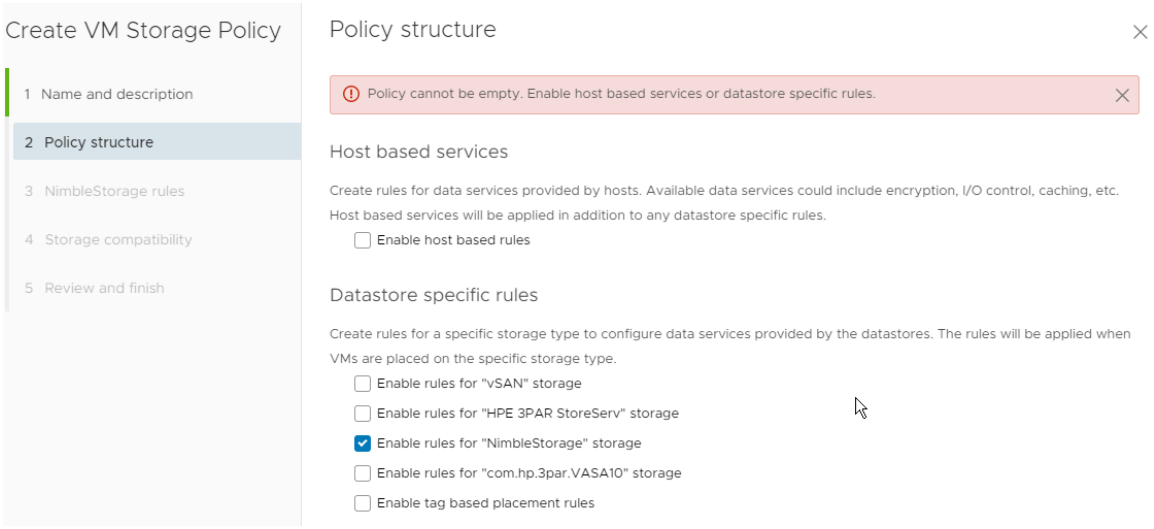


FIGURE 22. Entering HPE Nimble Storage SPBM rules from policies and profiles

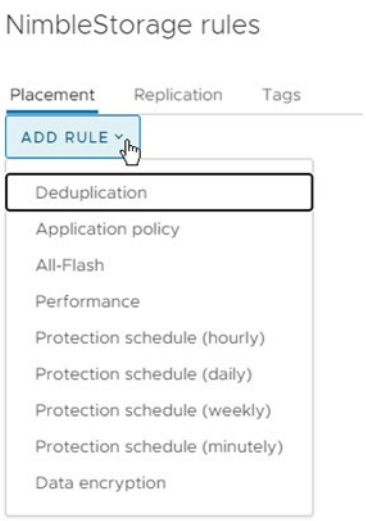


FIGURE 23. HPE Nimble Storage specific rules

As shown in Figure 23, you can access specific rules from the Policies and Profiles vCenter menu that can be enabled for HPE Nimble Storage arrays as part of SPBM:

- Deduplication can be enabled or disabled.
- The Application policy option allows for the selection of more than a dozen application profiles for application to datastores.
- All-Flash can be enabled or disabled.
- You can use a performance policy to set IOP and MB/sec limits.
- Protection schedules set snapshot schedules as well as snapshot replication partners and retention policies (in days) for both local and remote snaps.
- Data encryption can be enabled or disabled.

ADDITIONAL DEPLOYMENT CONSIDERATIONS

Additional features to be mindful of during vSphere deployment include the use of SCSI UNMAP and Storage Class Memory, if that option has been purchased.

SCSI UNMAP

VMware vVol environments support using the VAAI UNMAP primitive to reclaim space. vSphere does not automatically use UNMAP. When a guest operating system issues the UNMAP command, vSphere sends the command directly to the HPE Nimble Storage array. The array then recognizes the command.

vSphere detects support for the command for the vVol based on the protocol endpoint LUN to which the vVol is bound. vSphere does not enforce any alignment criteria when it executes a UNMAP command. vSphere handles the UNMAP command the same way it handles the VAAI Extended Copy (Xcopy) and Atomic Test and Set Locking (ATS) primitives. It detects these commands automatically and sends them to the array, thus bypassing the host.

NOTE

For more information about using UNMAP with vVols, read the VMware KB article "How Virtual Volumes and UNMAP primitive interact? (2112333)."

Storage Class Memory

With the introduction of NimbleOS, 5.2 SCM is now available across all HPE Nimble Storage products. Figure 24 describes three different array implementation types and comparisons of their I/O paths.

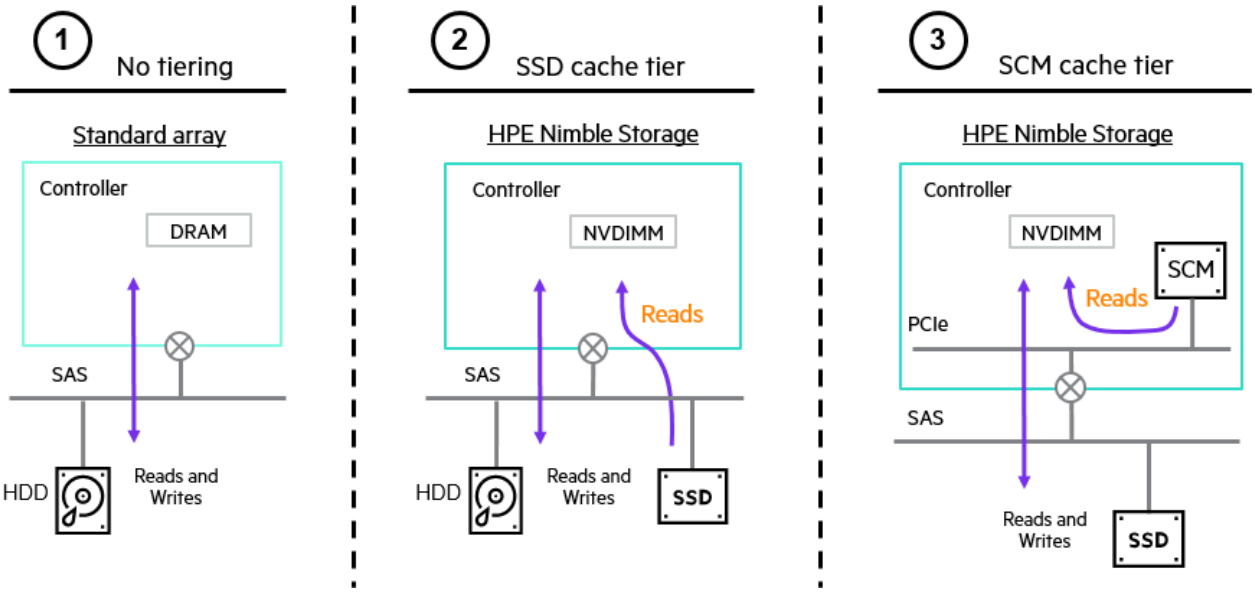


FIGURE 24. I/O path comparison of a standard array (no tiering), HPE Nimble Storage with Adaptive Flash Cache (SSD cache tier), and HPE Nimble Storage (SCM cache tier)

With the implementation of NVMe, SCM internal testing at HPE has consistently delivered performance across a variety of workloads performance under 300 microseconds. With applications that are heavily read-intensive, latency drops even further to ~ 250 microseconds.

Best practice: For use cases that require ultra-low latency such as database application as well as online trading, consider incorporating SCM.

Resources or additional links

HPE Community Around the Storage Block blogs
Setup for SRM 8.3 and HPE Nimble Storage vVols

VMware vSphere 7.0 and Nimble Storage

LEARN MORE AT

https://www.hpe.com/us/en/storage/nimble.html

a00104406ENW, November 2020

Hewlett Packard Enterprise