Abstract

NetApp® ONTAP® is a powerful and flexible data management solution for VMware vSphere environments and continues to add innovative capabilities to simplify management while reducing costs. This document introduces the ONTAP solution for vSphere, including the latest product information, along with best practices to streamline deployment, reduce risk, and simplify ongoing management.
# TABLE OF CONTENTS

## 1 ONTAP for vSphere

1.1 Why ONTAP for vSphere? ................................................. 4
1.2 ONTAP Capabilities for vSphere .......................................... 5
1.3 ONTAP Licensing .......................................................... 6
1.4 Virtualization Tools for ONTAP ............................................ 7

## 2 Best Practices

2.1 vSphere Datastore and Protocol Features ................................. 9
2.2 Selecting a Storage Protocol ............................................... 11
2.3 Datastore Layout ............................................................ 11
2.4 Datastore and VM Migration ............................................... 13
2.5 Virtual Storage Console .................................................. 13
2.6 General Networking ......................................................... 15
2.7 SAN (FC, FCoE, iSCSI), RDM ............................................ 16
2.8 NFS .............................................................................. 18

## 3 Other Capabilities for vSphere

3.1 Data Protection ............................................................... 20
3.2 Space Reclamation .......................................................... 21
3.3 VM and Datastore Cloning ................................................ 21
3.4 Storage Efficiency and Thin Provisioning ................................ 23
3.5 Quality of Service (QoS) .................................................... 25
3.6 VMware Storage Distributed Resource Scheduler (SDRS) ........... 26
3.7 Storage Policy-Based Management and Virtual Volumes (VVols) 27
3.8 Cloud Migration and Backup ............................................. 29
3.9 Encryption for vSphere Data ................................................. 30

## Appendix A: ONTAP and vSphere Release-Specific Information

ONTAP Releases ............................................................... 32
vSphere and ESXi Support .................................................. 32
NFS Plug-In for VMware VAAI ............................................. 33
VASA Provider ................................................................. 33
Virtual Storage Console ..................................................... 33
Appendix B: Recommended ESXi Host and Other ONTAP Settings ................................................. 34
Version History .......................................................................................................................... 36
Contact Us ............................................................................................................................... 36

LIST OF TABLES
Table 1) vSphere supported traditional datastore features with ONTAP (does not apply to VVol datastores). ........9
Table 2) Supported VMware storage-related functionalities. ......................................................................9
Table 3) Supported ONTAP storage management features. ..................................................................10
Table 4) Supported backup features. .................................................................................................11
Table 5) Best tools for provisioning datastores..................................................................................14
Table 6) Applicability of network configuration. ................................................................................16
Table 7) NFS versions and supported features. ..................................................................................19
Table 8) ONTAP QoS and VMware SIOC comparison. ......................................................................26

LIST OF FIGURES
Figure 1) ONTAP tools for vSphere................................................................. 8
Figure 2) Virtual storage console datastore provisioning.................................................................14
Figure 3) OnCommand System Manager provisioning.................................................................15
Figure 4) Multipath connectivity from vSphere host to ONTAP LUN. .............................................18
Figure 5) Example SnapCenter deployment....................................................................................20
Figure 6) ONTAP cloning. ..............................................................................................................22
Figure 7) Combined effect of ONTAP storage efficiency features. .................................................23
Figure 8) VASA Provider 7.1 dashboard. .........................................................................................27
Figure 9) VVol components.............................................................................................................29
Figure 10) NetApp hybrid cloud solutions. ....................................................................................30
1 ONTAP for vSphere

NetApp ONTAP software has been a leading storage solution for VMware vSphere environments for over a decade and continues to add innovative capabilities to simplify management while reducing costs. This document introduces the ONTAP solution for vSphere, including the latest product information, along with best practices to streamline deployment, reduce risk, and simplify ongoing management.

Best practices supplement other documents such as guides and compatibility lists. They are developed based on lab testing and extensive field experience by NetApp engineers and customers. They might not be the only practices that work or are supported, but are generally the simplest solutions that meet the needs of the most customers.

This document is focused on capabilities in recent releases of ONTAP (9.x) running on vSphere 5.5 or later. See Appendix A for details related to specific releases.

1.1 Why ONTAP for vSphere?

There are many reasons why more than 50,000 customers have selected ONTAP as their storage solution for vSphere, such as a unified storage system supporting both SAN and NAS protocols, robust data protection capabilities using space-efficient Snapshot™ copies, and a wealth of tools to help you manage application data. Using a storage system separate from the hypervisor allows you to offload many functions and maximize your investment in vSphere host systems. This approach not only makes sure your host resources are focused on application workloads, but also avoids random performance impacts to applications from storage operations.

Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses, make sure data is protected at lower cost, and provide consistent high performance. And because virtualized workloads are mobile, you can explore different approaches using Storage vMotion to move VMs across VMFS, NFS, or VVol datastores, all on the same storage system.

Here are key factors customers value today:

**Unified storage**

Systems running ONTAP software are unified in several significant ways. Originally this approach referred to both NAS and SAN protocols, and ONTAP continues to be a leading platform for SAN along with its original strength in NAS. In the vSphere world, this approach could also mean a unified system for virtual desktop infrastructure (VDI) together with virtual server infrastructure (VSI). Systems running ONTAP software are typically less expensive for VSI than traditional enterprise arrays, yet have advanced storage efficiency capabilities to handle VDI in the same system. ONTAP also unifies a variety of storage media, from SSDs to SATA, and can extend that easily into the cloud. There's no need to buy one flash array for performance, a SATA array for archives, and separate systems for the cloud. ONTAP ties them all together.

**Virtual volumes and storage policy-based management**

NetApp was an early design partner with VMware in the development of vSphere Virtual Volumes (VVols), providing architectural input and early support for VVols and VMware vSphere APIs for Storage Awareness (VASA). Not only did this approach bring VM granular storage management to VMFS, it also supported automation of storage provisioning through Storage Policy-Based Management. This approach allows storage architects to design storage pools with different capabilities that can be easily consumed by VM administrators. ONTAP leads the storage industry in VVol scale, supporting hundreds of thousands of VVols in a single cluster, whereas enterprise array and smaller flash array vendors support as few as several thousand VVols per
array. NetApp is also driving the evolution of VM granular management with upcoming capabilities in support of VASA 3.0.

**Storage efficiency** Although NetApp was the first to deliver deduplication for production workloads, this innovation wasn’t the first or last one in this area. It started with ONTAP Snapshot copies, a space-efficient data protection mechanism with no performance impact, along with FlexClone® technology to instantly make read/write copies of VMs for production and backup use. NetApp went on to deliver inline capabilities, including deduplication, compression, and zero-block deduplication, to squeeze out the most storage from expensive SSDs. Most recently, ONTAP added the ability to pack smaller I/O operations and files into a disk block using compaction. The combination of these capabilities has resulted in customers seeing up to 5:1 savings for VSI and up to 30:1 for VDI.

**Hybrid cloud** Whether used for on-premises private cloud, public cloud infrastructure, or a hybrid cloud that combines the best of both, the NetApp Data Fabric helps streamline and optimize data management. Start with high-performance all-flash systems, then couple them with either disk or cloud storage systems for data protection and cloud compute. Choose from Azure, AWS, IBM, or Google clouds to optimize costs and avoid lock-in. Leverage advanced support for OpenStack and container technologies as needed. NetApp also offers cloud-based backup (AltaVault™) and storage tiering and archiving tools (FabricPool) for ONTAP to help reduce operating expenses and leverage the broad reach of the cloud.

**And more** Take advantage of the extreme performance of NetApp All Flash FAS (AFF) systems to accelerate your virtualized infrastructure while managing costs. Enjoy completely nondisruptive operations, from maintenance to upgrades to complete replacement of your storage system, using scale-out ONTAP clusters. Protect data at rest with NetApp Volume Encryption capabilities at no additional cost. Make sure performance meets business service levels through fine-grained quality of service capabilities. They are all part of the broad range of capabilities that come with ONTAP, the world’s #1 open networked branded storage OS (source: IDC Worldwide Quarterly Enterprise Storage Systems Tracker, Q3 2017, November 30, 2017 [Open Networked Enterprise Storage Systems revenue and terabytes]).

### 1.2 ONTAP Capabilities for vSphere

**Protocols**

ONTAP supports all major storage protocols used for virtualization, such as iSCSI, Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) for SAN environments, as well as NFS (v3 and v4.1) and SMB (for guest connections). Customers are free to pick what works best for their environment and may combine protocols as needed on a single system (for example, augmenting general use of NFS datastores with a few iSCSI RDMs or guest shares).

**Features**

There are many ONTAP features that are useful for managing virtualized workloads. Some require additional product licenses and are described in the next section. Others are packaged as standalone tools, some for ONTAP and others for the entire NetApp portfolio, and those are described after that.

Here are further details about base ONTAP features:
ONTAP offers instant Snapshot copies of a VM or datastore with zero performance impact to create or use the Snapshot copy. They are valuable by themselves to make a restoration point of a VM prior to patching or for simple data protection. Note that these are different from VMware (consistency) snapshots, which are generally not recommended due to performance and other impacts. The easiest way to make an ONTAP Snapshot copy is to use the SnapCenter® Plug-In for VMware vSphere to back up VMs and datastores.

### Storage efficiency
Covered later in this document, ONTAP supports inline and background deduplication and compression, zero-block deduplication, and data compaction.

### DataMotion™
Allows nondisruptive movement of volumes and LUNs supporting vSphere datastores and VVols within the ONTAP cluster to balance performance and capacity or support nondisruptive maintenance and upgrades.

### Flash Pool™
Creates a storage pool of HDDs together with SSDs to accelerate performance cost effectively.

### Performance headroom
Provides visibility of performance capacity available for deploying new workloads on storage nodes.

### QoS
Covered later in this report, QoS allows for managing performance on an individual LUN, volume, or file. Could be used to limit an unknown or "bully" VM or to make sure an important VM gets sufficient performance resources.

### Volume Encryption
Covered later in this report, NetApp Volume Encryption offers easy software-based encryption to protect data at rest.

### FabricPool
Tiers colder data automatically at the block level to a separate object store, freeing up expensive flash storage.

## 1.3 ONTAP Licensing

Some ONTAP features that are valuable for managing virtualized workloads require an additional license, whether available at no additional cost, in a license bundle, or a la carte. For many customers, the most cost-effective approach is the Premium or Flash Bundle, which includes all the licenses listed below. Here are the key licenses relevant to vSphere and how they are used:

### FlexClone
FlexClone enables instant, space-efficient clones of ONTAP volumes and files. This cloning is used when operations are offloaded to the storage system by VMware vSphere Storage APIs – Array Integration (VAAI), for backup verification and recovery (SnapCenter software), and for VVol cloning and Snapshot copies. Here is how they are used:

- VAAI is supported with ONTAP for offloaded copy in support of vSphere clone and migration (Storage vMotion) operations. The FlexClone license allows for fast clones within a FlexVol® volume, but if not licensed it still allows clones using slower block copies.
- A FlexClone license is required for VVol functionality. It enables cloning of VVols within a single datastore or between datastores and enables vSphere-managed Snapshot copies of VVols, which are offloaded to the storage system.
- The storage replication adapter (SRA) is used with VMware Site Recovery Manager, and a FlexClone license is required to test recovery in both NAS and SAN environments. SRA may be used without FlexClone for discovery, recovery, and reprotection workflows.
- FlexClone has supported Virtual Storage Console (VSC) capabilities in the past, but these are no longer required due to product changes.

### SnapRestore
SnapRestore® technology enables instant recovery of a volume in place, without copying data. It is required by NetApp backup and recovery tools such as VSC and
SnapCenter, where it is used to mount the datastore for verification and restore operations.

**SnapMirror, SnapVault**

SnapMirror® and SnapVault® technologies allow for simple, fast replication of data between ONTAP systems, as well as other NetApp systems such as AltaVault. Currently, available releases of SnapMirror support the version flexibility of logical replication with the performance of block replication, sending only changed data to the secondary system. SnapVault extends this capability to allow retention of multiple recovery points on a secondary system, and in recent ONTAP releases, customers who license SnapMirror may use SnapVault with no additional license.

SnapMirror is required for SRA replication with Site Recovery Manager. It is also required for SnapCenter to enable replication of Snapshot copies to a secondary storage system.

**SnapCenter**

SnapCenter software provides a unified, scalable platform and plug-in suite for application-consistent data protection and clone management. A SnapCenter standard controller-based license is included with the Premium and Flash Bundles for AFF and FAS systems.

**MetroCluster**

NetApp MetroCluster™ is a synchronous replication solution combining high availability and disaster recovery in a campus or metropolitan area to protect against both site disasters and hardware outages. It provides solutions with transparent recovery from failure, with zero data loss (0 RPO) and fast recovery (RTO within minutes). It is used in vSphere environments as part of a vSphere Metro Storage Cluster configuration.

### 1.4 Virtualization Tools for ONTAP

NetApp offers several standalone software tools that may be used together with ONTAP and vSphere to manage your virtualized environment. The following tools are included with the ONTAP license at no additional cost. See Figure 1 for a depiction of how these tools work together in your vSphere environment.

**Virtual Storage Console (VSC)**

VSC is a vCenter plug-in that simplifies storage management and efficiency features, enhances availability, and reduces storage costs and operational overhead, whether using SAN or NAS. It uses best practices for provisioning datastores and optimizes ESXi host settings for NFS and block storage environments. For all these benefits, it is recommended as a best practice when using vSphere with systems running ONTAP software. It includes both a VSC server appliance and user interface extensions for vCenter.

**NFS Plug-In for VMware VAAI**

The NetApp NFS Plug-In for VMware is a plug-in for ESXi hosts that allows them to use VAAI features with NFS datastores on ONTAP. It supports copy offload for clone operations, space reservation for thick virtual disk files, and Snapshot copies for linked clones. Offloading copy operations to storage is not necessarily faster to complete, but offloads host resources such as CPU cycles, buffers, and queues. You may use VSC to install the plug-in on ESXi hosts.

**VASA Provider for ONTAP**

The VASA Provider for ONTAP supports the VMware vStorage APIs for Storage Awareness (VASA) framework. In the 7.x releases, the VASA Provider is combined with the VSC and SRA as a single virtual
appliance for ease of deployment. VASA Provider connects vCenter Server with ONTAP to aid in provisioning and monitoring VM storage. It enables VMware Virtual Volumes (VVols) support, management of storage capability profiles and individual VM VVol performance, and alarms for monitoring capacity and compliance with the profiles.

**Storage Replication Adapter**

The SRA is used together with VMware Site Recovery Manager (SRM) to manage data replication between production and disaster recovery sites and test the DR replica nondisruptively. It helps automate the tasks of discovery, recovery, and reprotection. It includes both an SRA server appliance and an SRA adapter for the SRM server.

**OnCommand System Manager**

Although OnCommand® System Manager is generally useful as a GUI to manage a system running ONTAP software, it also has functions useful in the vSphere environment. After selecting a storage virtual machine, the administrator may choose from several different application provisioning wizards, including ones for virtual desktops and virtual servers. See Virtual Storage Console later in this document for more information about provisioning.

Figure 1) ONTAP tools for vSphere.
2 Best Practices

2.1 vSphere Datastore and Protocol Features

Four protocols are used to connect VMware vSphere to datastores on a system running ONTAP software:

- FC
- FCoE
- iSCSI
- NFS

FC, FCoE, and iSCSI are block protocols that use vSphere Virtual Machine File System (VMFS) to store VMs inside ONTAP LUNs that are contained in an ONTAP volume. NFS is a file protocol that places VMs into datastores (which are simply ONTAP volumes) without the need for VMFS. SMB, iSCSI, or NFS may also be used directly from a guest OS to ONTAP.

The following tables generally apply to vSphere 5.x and 6.x releases using supported ONTAP releases. VMware Configuration Maximums documents for specific vSphere releases may also be consulted to confirm specific limits; see https://www.vmware.com/support/pubs/.

Table 1) vSphere supported traditional datastore features with ONTAP (does not apply to VVol datastores).

<table>
<thead>
<tr>
<th>Capability/Feature</th>
<th>FC/FCoE</th>
<th>iSCSI</th>
<th>NFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>VMFS or raw device mapping  (RDM)</td>
<td>VMFS or RDM</td>
<td>N/A</td>
</tr>
<tr>
<td>Maximum number of datastores or LUNs</td>
<td>256 targets/HBA</td>
<td>256 targets</td>
<td>256 mounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Default NFS. MaxVolumes is 8. Use Virtual Storage Console to increase to 256.</td>
</tr>
<tr>
<td>Maximum datastore size</td>
<td>64TB</td>
<td>64TB</td>
<td>100TB</td>
</tr>
<tr>
<td>Maximum datastore file size (for VMDKs using vSphere version 5.5 and VMFS 5 or later)</td>
<td>62TB</td>
<td>62TB</td>
<td>16TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: 62TB is the maximum size supported by vSphere.</td>
</tr>
<tr>
<td>Optimal queue depth per LUN or file system</td>
<td>64</td>
<td>64</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 2) Supported VMware storage-related functionalities.

<table>
<thead>
<tr>
<th>Capacity/Feature</th>
<th>FC/FCoE</th>
<th>iSCSI</th>
<th>NFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vMotion</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage vMotion</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VMware HA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage Distributed Resource Scheduler (SDRS)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Capacity/Feature</td>
<td>FC/FCoE</td>
<td>iSCSI</td>
<td>NFS</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>VMware vStorage APIs for Data Protection (VADP)–enabled backup software</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Cluster Service (MSCS) or failover clustering within a VM</td>
<td>Yes</td>
<td>Yes*</td>
<td>Not supported</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Yes, with eager-zeroed thick virtual machine disks (VMDKs) or virtual mode RDMs</td>
<td>Yes, with eager-zeroed thick VMDKs or virtual mode RDMs</td>
<td>Yes, with eager-zeroed thick VMDKs</td>
</tr>
<tr>
<td>Site Recovery Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Thin-provisioned VMs (virtual disks)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Note: This setting is the default for all VMs on NFS when not using VAAI.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware native multipathing</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* NetApp recommends the use of in-guest iSCSI for Microsoft clusters rather than VMDKs in a VMFS datastore. This approach is fully supported by Microsoft and VMware, offers great flexibility with ONTAP (SnapMirror to ONTAP systems on-premises or in the cloud), is easy to configure and automate, and can be protected with SnapCenter.

Table 3) Supported ONTAP storage management features.

<table>
<thead>
<tr>
<th>Capability/Feature</th>
<th>FC/FCoE</th>
<th>iSCSI</th>
<th>NFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data deduplication</td>
<td>Savings in the array</td>
<td>Savings in the array</td>
<td>Savings in the datastore</td>
</tr>
<tr>
<td>Thin provisioning</td>
<td>Datastore or RDM</td>
<td>Datastore or RDM</td>
<td>Datastore</td>
</tr>
<tr>
<td>Resize datastore</td>
<td>Grow only</td>
<td>Grow only</td>
<td>Grow, autogrow, and shrink</td>
</tr>
<tr>
<td>SnapDrive® (in guest)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SnapCenter plug-ins for Windows, Linux applications (in guest)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring and host configuration using Virtual Storage Console (VSC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Provisioning using VSC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Provisioning using OnCommand System Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 4) Supported backup features.

<table>
<thead>
<tr>
<th>Capability/Feature</th>
<th>FC/FCoE</th>
<th>iSCSI</th>
<th>NFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP Snapshot copies</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SRM supported by replicated backups</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Volume SnapMirror</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VMDK image access</td>
<td>VADP-enabled backup software</td>
<td>VADP-enabled backup software</td>
<td>VADP-enabled backup software, vSphere Client, and vSphere Web Client datastore browser</td>
</tr>
<tr>
<td>VMDK file-level access</td>
<td>VADP-enabled backup software, Windows only</td>
<td>VADP-enabled backup software, Windows only</td>
<td>VADP-enabled backup software and third-party applications</td>
</tr>
<tr>
<td>NDMP granularity</td>
<td>Datastore</td>
<td>Datastore</td>
<td>Datastore or VM</td>
</tr>
</tbody>
</table>

2.2 Selecting a Storage Protocol

Systems running ONTAP software support all major storage protocols so customers can choose what is best for their environment, considering existing and planned networking infrastructure and staff skills. NetApp testing has generally shown little difference between protocols running at similar line speeds, so it's best to focus on your network infrastructure and staff capabilities over raw protocol performance.

The following factors might be useful in considering a choice of protocol:

- **Current customer environment.** Although IT teams are generally skilled at managing Ethernet IP infrastructure, not all are skilled at managing an FC SAN fabric. However, using a general-purpose IP network that's not designed for storage traffic might not work well. Consider the networking infrastructure you have in place, any planned improvements, and the skills and availability of staff to manage them.

- **Ease of setup.** Beyond initial configuration of the FC fabric (additional switches and cabling, zoning, interoperability verification of HBA and firmware), block protocols also require creation and mapping of LUNs and discovery and formatting by the guest OS. After the NFS volumes are created and exported, they are mounted by the ESXi host and ready to use. And NFS has no special hardware qualification or firmware to manage.

- **Ease of management.** With SAN protocols, if more space is needed, several steps are necessary (grow LUN, rescan to discover new size, then grow the file system). Although growing is possible, sizing a LUN smaller is not, and recovering unused space can require additional effort. NFS allows easy sizing up or down, and this resizing can be automated by the storage system.

- **Storage space transparency.** Storage utilization is easier to see in NFS environments, because thin provisioning returns savings immediately. Likewise, deduplication and cloning savings are immediately available for other VMs in the same datastore or for other storage system volumes. VM density is also typically greater in an NFS datastore, which can improve deduplication savings as well as reduce management costs by having fewer datastores to manage.

2.3 Datastore Layout

ONTAP storage systems offer great flexibility in creating datastores for VMs and virtual disks. Although many ONTAP best practices are applied when using the Virtual Storage Console to provision datastores for vSphere (and are listed in Appendix B), here are some additional guidelines to consider:
• Deploying vSphere with ONTAP NFS datastores results in a high-performing, easy-to-manage implementation that provides VM-to-datastore ratios that cannot be obtained with block-based storage protocols. This architecture can result in a tenfold increase in datastore density with a correlating reduction in the number of datastores. Although a larger datastore can benefit storage efficiency and provide operational benefits, consider using at least four datastores (or volumes) to store your VMs on a single ONTAP controller to get maximum performance from the hardware resources. This approach also allows you to establish datastores with different recovery policies (some backed up or replicated more frequently than others, based on business needs).

• NetApp recommends the use of FlexVol volumes for NFS datastores. There are several other ONTAP storage containers such as qtrees and FlexGroup volumes that are not generally recommended. NetApp tools such as VSC use FlexVol volumes for datastore provisioning, so for compatibility NetApp recommends the use of volumes. Deploying datastores as multiple qtrees in a single volume might be useful for highly automated environments that can benefit from datastore-level quotas or VM file clones. Virtualized workloads that require cloning and copy offload functionality are not currently recommended for FlexGroup volumes.

• A good size for the datastore is around 4TB to 8TB. This size is a good balance point for performance, ease of management, and data protection. Start small (say, 4TB) and grow the datastore as needed. Consider the use of ONTAP autosize to automatically grow and shrink the volume as used space changes. The VSC Datastore Provisioning Wizard allows the specification of autogrow in the details of the new datastore. Additional customization of the grow and shrink thresholds and maximum and minimum size can be done with OnCommand System Manager or the command line.

• Alternately, VMFS datastores can be configured with LUNs that are accessed by FC, iSCSI, or FCoE. VMFS allows traditional LUNs to be accessed simultaneously by every ESX server in a cluster. VMFS datastores can be up to 64TB in size and consist of up to 32 2TB LUNs (VMFS 3) or a single 64TB LUN (VMFS 5). The ONTAP maximum LUN size is 16TB; therefore, a maximum size VMFS 5 datastore is created by using four 16TB LUNs. While there can be performance benefit for high-I/O workloads with multiple LUNs (with high-end FAS or AFF systems), this benefit is offset by added management complexity to create, manage, and protect the datastore LUNs and increased availability risk. NetApp generally recommends using a single, large LUN for each datastore and only span if there is a special need to go beyond a 16TB datastore. As with NFS, consider using multiple datastores (volumes) to maximize performance on a single ONTAP controller.

• Older guest operating systems needed alignment with the storage system for best performance and storage efficiency. However, modern vendor-supported operating systems (OSs) from Microsoft and Linux distributors such as Red Hat no longer require adjustments to align the file system partition with the blocks of the underlying storage system in a virtual environment. If you are using an old OS that might require alignment, search the NetApp Support Knowledgebase for articles using “VM alignment” or request a copy of TR-3747 from a NetApp sales or partner contact.

• ONTAP has led the industry with innovative storage efficiency features, allowing you to get the most out of your usable disk space. AFF systems take this efficiency further with default inline deduplication and compression. With ONTAP 9.1 and earlier, data deduplication savings were based on the commonality of the data in a single volume or datastore. With aggregate deduplication in ONTAP 9.2 and later, data is deduplicated across all volumes in an aggregate, so you no longer need to group similar operating systems and similar applications within a single datastore to maximize savings.

• In some cases, you might not even need a datastore. For the best performance and manageability, avoid using a datastore for high-I/O applications such as databases and some applications. Instead, consider guest-owned file systems such as NFS or iSCSI file systems managed by the guest or with RDMs. For specific application guidance, see NetApp technical reports for your application. For example, TR-3633: Oracle Databases on Data ONTAP has a section about virtualization with helpful details.
2.4 Datastore and VM Migration

When migrating VMs from an existing datastore on another storage system to ONTAP, here are some practices to keep in mind:

- Use Storage vMotion to move the bulk of your virtual machines to ONTAP. Not only is this approach nondisruptive to running VMs, it also allows ONTAP storage efficiency features such as inline deduplication and compression to process the data as it migrates. Consider using vCenter capabilities to select multiple VMs from the inventory list and then schedule the migration (use Ctrl key while clicking Actions) at an appropriate time.

- While you could carefully plan a migration to appropriate destination datastores, it is often simpler to migrate in bulk and then organize later as needed. If you have specific data protection needs, such as different Snapshot schedules, you might want to use this approach to guide your migration to different datastores.

- Most VMs and their storage may be migrated while running (hot), but migrating attached (not in datastore) storage such as ISOs, LUNs, or NFS volumes from another storage system might require cold migration.

- Virtual machines that need more careful migration include databases and applications that use attached storage. In general, consider the use of the application’s tools to manage the migration. For Oracle, consider using Oracle tools such as RMAN or ASM to migrate the database files. See TR-4534 for more information. Likewise, for SQL Server, consider using either SQL Server Management Studio or NetApp tools such as SnapManager for SQL Server or SnapCenter.

2.5 Virtual Storage Console

The most important best practice when using vSphere with systems running ONTAP software is to install and use the Virtual Storage Console (VSC). The VSC is a vCenter plug-in that simplifies storage management and efficiency features, enhances availability, and reduces storage costs and operational overhead, whether using SAN or NAS. It uses best practices for provisioning datastores and optimizes ESXi host settings for multipath and HBA timeouts (these are described in Appendix B). Because it’s a vCenter plug-in, it’s available to all vSphere web clients that connect to the vCenter server.

The VSC also helps you use other NetApp tools in vSphere environments. VSC allows you to install the NFS Plug-In for VMware VAAI, which enables copy offload to ONTAP for VM cloning operations, space reservation for thick virtual disk files, and ONTAP Snapshot copies for vSphere linked clones. Although it was used together with SnapCenter in the VSC 6.x releases to manage backup and recovery, this functionality is now managed with the SnapCenter Plug-In for VMware vSphere.

The VSC is also the management interface for many functions of the VASA Provider for ONTAP, supporting storage policy-based management with VVols. After VSC is registered, use it to create storage capability profiles, map them to storage, and make sure of datastore compliance with the profiles over time. The VASA Provider also provides an interface to create and manage VVol datastores.

In general, NetApp recommends using the VSC interface within vCenter to provision traditional datastores to make sure best practices are followed. However, OnCommand System Manager also offers application provisioning templates for virtual server and virtual desktop infrastructure, for both SAN and NAS, and it might be a better choice in some cases.
Table 5) Best tools for provisioning datastores.

<table>
<thead>
<tr>
<th>Virtual Storage Console</th>
<th>OnCommand System Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated within vCenter so easy access for VM administrators.</td>
<td>Often used by ONTAP administrators to easily manage an ONTAP system.</td>
</tr>
<tr>
<td>Quick interface to create a single datastore by right-clicking ESXi host or cluster.</td>
<td>Use to create multiple datastores or virtual desktops in a single operation, but must specify access and mount in a subsequent operation using CLI or vCenter.</td>
</tr>
<tr>
<td>Automatically creates access controls for datastores (NFS export policies, SAN initiator groups) using defaults and mounts the datastore for use.</td>
<td>Allows specification of access controls (host IPs for exports, WWPNs for host initiators or existing initiator groups). Mount separately within vCenter.</td>
</tr>
<tr>
<td>No performance-based placement of datastores, but can move later (use policies to filter destinations). Can set maximum QoS on VVol VMs via policy.</td>
<td>Automatically places datastores in optimal location in cluster, considering available capacity and performance and applying maximum QoS to datastore (and minimum QoS for datastore on AFF).</td>
</tr>
<tr>
<td>Also used to manage VVol datastores and storage capability profiles with VASA Provider.</td>
<td>No support for VVol datastore provisioning.</td>
</tr>
</tbody>
</table>

Figure 2) Virtual storage console datastore provisioning.
2.6 General Networking

Configuring network settings when using vSphere with systems running ONTAP software is straightforward and similar to other network configuration. Here are some things to consider:

- **Separate storage network traffic** from other networks. A separate network can be achieved by using a dedicated VLAN or separate switches for storage. If the storage network shares physical paths such as uplinks, you might need QoS or additional uplink ports to make sure of sufficient bandwidth. Don’t connect hosts directly to storage; use switches to have redundant paths and allow VMware HA to work without intervention.

- **Jumbo frames** may be used if desired and supported by your network, especially when using iSCSI. If they are used, make sure they are configured identically on all network devices, VLANs, and so on in the path between storage and ESXi host. Otherwise, you might see performance or connection problems. The MTU must also be set identically on the ESXi virtual switch and VMkernel port and on the physical ports or interface groups of each ONTAP node.

- **NetApp** only recommends disabling network flow control on the cluster network ports within an ONTAP cluster. NetApp makes no other recommendations for best practices for the remaining network ports used for data traffic. You should enable or disable as necessary. See TR-4128 for more background on flow control.

- When ESXi and ONTAP storage arrays are connected to Ethernet storage networks, NetApp recommends configuring the Ethernet ports to which these systems connect as **Rapid Spanning Tree Protocol** (RSTP) edge ports or by using the Cisco PortFast feature. In an environment that uses the Cisco PortFast feature and that has 802.1Q VLAN trunking enabled to either the ESXi server or the ONTAP storage arrays, NetApp recommends enabling the Spanning-Tree PortFast trunk feature.

- **NetApp** recommends the following best practices for **link aggregation**:
  - Use switches that support link aggregation of ports on two separate switch chassis, using a multichassis link aggregation group approach such as Cisco’s Virtual PortChannel (vPC).
- Disable LACP for switch ports connected to ESXi unless using dvSwitches 5.1 or later with LACP configured.
- Use LACP to create link aggregates for ONTAP storage systems, using dynamic multimode interface groups with IP hash.
- Use IP hash teaming policy on ESXi.

Table 6 provides a summary of network configuration items and indicates where the settings are applied.

<table>
<thead>
<tr>
<th>Item</th>
<th>ESXi</th>
<th>Switch</th>
<th>Node</th>
<th>SVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>VMkernel</td>
<td>No**</td>
<td>No**</td>
<td>Yes</td>
</tr>
<tr>
<td>Link aggregation</td>
<td>Virtual switch</td>
<td>Yes</td>
<td>Yes</td>
<td>No*</td>
</tr>
<tr>
<td>VLAN</td>
<td>VMkernel and VM port groups</td>
<td>Yes</td>
<td>Yes</td>
<td>No*</td>
</tr>
<tr>
<td>Flow control</td>
<td>NIC</td>
<td>Yes</td>
<td>Yes</td>
<td>No*</td>
</tr>
<tr>
<td>Spanning tree</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MTU (for jumbo frames)</td>
<td>Virtual switch and VMkernel port (9000)</td>
<td>Yes (set to max)</td>
<td>Yes (9000)</td>
<td>No*</td>
</tr>
<tr>
<td>Failover groups</td>
<td>No</td>
<td>No</td>
<td>Yes (create)</td>
<td>Yes (select)</td>
</tr>
</tbody>
</table>

* SVM LIFs connect to ports, interface groups, or VLAN interfaces that have VLAN, MTU, and other settings, but the settings are not managed at the SVM level.
** These devices have IP addresses of their own for management, but these addresses are not used in the context of ESXi storage networking.

** 2.7 SAN (FC, FCoE, iSCSI), RDM

In vSphere, there are three ways to use block storage LUNs:
- With VMFS datastores
- With raw device mapping (RDM)
- As a LUN accessed and controlled by a software initiator from a VM guest OS

VMFS is a high-performance clustered file system that provides datastores that are shared storage pools. VMFS datastores can be configured with LUNs that are accessed using FC, iSCSI, or FCoE. VMFS allows traditional LUNs to be accessed simultaneously by every ESX server in a cluster. The ONTAP maximum LUN size is 16TB; therefore, a maximum size VMFS 5 datastore of 64TB (see Table 1 in section 2.1) is created by using four 16TB LUNs. Because the ONTAP LUN architecture does not have small individual queue depths, VMFS datastores in ONTAP can scale to a greater degree than with traditional array architectures in a relatively simple manner. Note that VSC does not currently support VMFS 6.

vSphere includes built-in support for multiple paths to storage devices, referred to as native multipathing (NMP). NMP includes the ability to detect the type of storage for supported storage systems and automatically configure the NMP stack to support the capabilities of the storage system in use. Both NMP and NetApp ONTAP support Asymmetric Logical Unit Access (ALUA) to negotiate optimized and nonoptimized paths. In ONTAP, an ALUA-optimized path follows a direct data path, using a target port on the node that hosts the LUN being accessed. ALUA is turned on by default in both vSphere and ONTAP. The NMP recognizes the ONTAP cluster as ALUA, and it uses the ALUA storage array type plug-in (VMW_SATP_ALUA) and selects the round robin path selection plug-in (VMW_PSP_RR).
ESXi 6 supports up to 256 LUNs and up to 1,024 total paths to LUNs. Any LUNs or paths beyond these limits are not seen by ESXi. Assuming the maximum number of LUNs, the path limit allows four paths per LUN. In a larger ONTAP cluster, it is possible to reach the path limit before the LUN limit. To address this limitation, ONTAP supports selective LUN map (SLM) in release 8.3 and later.

SLM limits the nodes that advertise paths to a given LUN. It is a NetApp best practice to have at least one LIF per node per SVM and to use SLM to limit the nodes advertised to the node hosting the LUN and its HA partner. Although other paths exist, they aren’t advertised by default. It is possible to modify the paths advertised with the add and remove reporting node arguments within SLM. Note that LUNs created in releases prior to 8.3 advertise all paths and need to be modified to only advertise the paths to the hosting HA pair. For more information about SLM, review section 5.9 of TR-4080. The previous method of portsets can also be used to further reduce the available paths for a LUN. Portsets help by reducing the number of visible paths through which initiators in a group can see LUNs.

- SLM is enabled by default. Unless using portsets, no additional configuration is required.
- For LUNs created prior to Data ONTAP 8.3, manually apply SLM by running the `lun mapping remove-reporting-nodes` command to remove the LUN reporting nodes and restrict LUN access to the LUN-owning node and its HA partner.

Block protocols (iSCSI, FC, and FCoE) access LUNs by using LUN IDs and serial numbers, along with unique names (FC/FCoE use worldwide names [WWNNs and WWPNs], and iSCSI uses iSCSI qualified names [IQNs]). The path to LUNs inside the storage is meaningless to the block protocols and is not presented anywhere in the protocol. Therefore, a volume that contains only LUNs does not need to be internally mounted at all, and a junction path is not needed for volumes that contain LUNs used in datastores.

Other best practices to consider:

- Make sure that a logical interface (LIF) is created for each SVM on each node in the ONTAP cluster for maximum availability and mobility. ALUA is used to parse paths and identify active optimized (direct) paths versus active nonoptimized paths. ALUA is used for both FC/FCoE and iSCSI.
- For iSCSI networks, use multiple VMkernel network interfaces on different network subnets that use NIC teaming when multiple virtual switches are used. Or use multiple physical NICs connected to multiple physical switches to provide HA and increased throughput. See Figure 4 for an example of multipath connectivity. In ONTAP, configure either a single-mode interface group for failover with two or more links that are connected to two or more switches or use LACP or other link-aggregation technology with multimode interface groups to provide HA and the benefits of link aggregation.
- If Challenge-Handshake Authentication Protocol (CHAP) is used in ESXi for target authentication, it must also be configured in ONTAP using the CLI (`vserver iscsi security create`) or with OnCommand System Manager (edit Initiator Security under Storage>SVMs>SVM Settings>Protocols>iSCSI).
- Use VSC to create and manage LUNs and igroups. VSC automatically determines WWPNs of servers and creates appropriate igroups. VSC also configures LUNs according to best practices and maps them to the correct igroups.
- Use RDMs with care, because they can be more difficult to manage, and they also use paths, which are limited, as described earlier. ONTAP LUNs support both **physical and virtual compatibility mode** RDMs.
2.8 NFS

vSphere allows customers to use enterprise-class NFS arrays to provide concurrent access to datastores to all the nodes in an ESXi cluster. As mentioned in the datastore section, there are some ease of use and storage efficiency visibility benefits when using NFS with vSphere.

The following best practices are recommended when using ONTAP NFS with vSphere:

- VMware has supported NFSv3 since VMware Infrastructure 3. vSphere 6.0 added support for NFSv4.1, which enables some advanced capabilities such as Kerberos security. Where NFSv3 uses client-side locking, NFSv4.1 uses server-side locking. Although an ONTAP volume can be exported through both protocols, ESXi can only mount through one protocol. This single protocol mount does not preclude other ESXi hosts from mounting the same datastore through a different version. Make sure to specify the protocol version to use when mounting so that all hosts use the same version and, therefore, the same locking style. Do not mix NFS versions across hosts. If possible, use host profiles to check compliancy.
  - Because there is no automatic datastore conversion between NFSv3 and NFSv4.1, create a new NFSv4.1 datastore and use Storage vMotion to migrate VMs to the new datastore.
- NFS export policies are used to control access by vSphere hosts. You may use one policy with multiple volumes (datastores). With NFSv3, ESXi uses the sys (UNIX) security style and requires the root mount option to execute VMs. In ONTAP, this option is referred to as superuser, and when the superuser option is used, it is not necessary to specify the anonymous user ID. Here’s a sample policy:
  
  ```
  Access Protocol: nfs3  
  Client Match Spec: 192.168.42.21  
  RO Access Rule: sys  
  RW Access Rule: sys  
  Anonymous UID:  
  Superuser: sys
  ```

- If the NetApp NFS Plug-In for VMware VAAI is used, the protocol should be set as nfs when the export policy rule is created or modified. The NFSv4 protocol is required for VAAI copy offload to work, and specifying the protocol as nfs automatically includes both the NFSv3 and the NFSv4 versions.
- NFS datastore volumes are junctioned from the root volume of the SVM; therefore, ESXi must also have access to the root volume in order to navigate and mount datastore volumes. The export policy for the root volume, and for any other volumes in which the datastore volume’s junction is nested, must include a rule or rules for the ESXi servers granting them read-only superuser access. Here’s a sample policy for the root volume, also using the VAAI plug-in:
  
  ```
  Access Protocol: nfs (which includes both nfs3 and nfs4)  
  Client Match Spec: 192.168.42.21
  ```
RO Access Rule: sys
RW Access Rule: never (best security for root volume)
Anonymous UID: 
Superuser: sys (also required for root volume with VAAI)

- Use the Virtual Storage Console (the most important best practice):
  - Use VSC to provision datastores because VSC simplifies management of export policies automatically.
  - When creating datastores for VMware clusters with VSC, select the cluster rather than a single ESX server. This choice triggers VSC to automatically mount the datastore to all hosts in the cluster.
  - Use the VSC mount function to apply existing datastores to new servers.
  - When not using VSC, use a single export policy for all servers, or each cluster of servers where additional access control is needed.

- Although ONTAP offers a flexible volume namespace structure to arrange volumes in a tree using junctions, this approach has no value for vSphere. It creates a directory for each VM at the root of the datastore, regardless of the namespace hierarchy of the storage. Thus the best practice is to simply mount the junction path for volumes for vSphere at the root volume of the SVM, which is how VSC provisions datastores. Not having nested junction paths also means that no volume is dependent on any volume other than the root volume and that taking a volume offline or destroying it, even intentionally, does not affect the path to other volumes.

<table>
<thead>
<tr>
<th>vSphere 6.x Features</th>
<th>NFSv3</th>
<th>NFSv4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>vMotion and Storage vMotion</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>High availability</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DRS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Host profiles</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage DRS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Storage I/O control</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SRM</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual volumes</td>
<td>Yes</td>
<td>Yes (vSphere 6.5)</td>
</tr>
<tr>
<td>Hardware acceleration (VAAI)</td>
<td>Yes</td>
<td>Yes (vSphere 6.5, NetApp VAAI Plug-in 1.1.2)</td>
</tr>
<tr>
<td>Kerberos authentication</td>
<td>No</td>
<td>Yes (enhanced with vSphere 6.5 to support AES, krb5i)</td>
</tr>
<tr>
<td>Multipathing support</td>
<td>No</td>
<td>No (ESXi 6.5 supports through session trunking; ONTAP supports through pNFS)</td>
</tr>
</tbody>
</table>
3 Other Capabilities for vSphere

3.1 Data Protection

Backing up your VMs and quickly recovering them are among the great strengths of ONTAP for vSphere, and it is easy to manage this ability inside vCenter with the Virtual Storage Console and SnapCenter. Use Snapshot copies to make quick copies of your VM or datastore without affecting performance, then send them to a secondary system using SnapMirror or SnapVault for longer-term off-site data protection. This approach minimizes storage space and network bandwidth by only storing changed information.

In the past, customers used the VSC to manage individual backup jobs using Snapshot copies and secondary replication. Today, this capability is enhanced with SnapCenter, which allows you to create backup policies that can be applied to multiple jobs. These policies can define schedule, retention, replication, and other capabilities. They continue to allow optional selection of VM-consistent snapshots, which leverages the hypervisor’s ability to quiesce I/O before taking a VMware snapshot. However, due to the performance impact of VMware snapshots, they are generally not recommended unless you need the guest file system to be quiesced. Instead, use ONTAP Snapshot copies for general protection and use application tools such as SnapCenter plug-ins to protect transactional data such as SQL Server or Oracle.

These plug-ins offer extended capabilities to protect the databases in both physical and virtual environments. With vSphere, you may use them to protect SQL Server or Oracle databases where data is stored on RDM LUNs, iSCSI LUNs directly connected to the guest OS, or VMDK files on either VMFS or NFS datastores. The plug-ins allow specification of different types of database backups, supporting online or offline backup, and protecting database files along with log files. In addition to backup and recovery, the plug-ins also support cloning of databases for development or test purposes.

Figure 5) Example SnapCenter deployment.

For enhanced disaster recovery capabilities, consider using NetApp’s Storage Replication Adapter (SRA) for ONTAP with VMware Site Recovery Manager. In addition to support for replication of datastores to a DR site, it also enables nondisruptive testing in the DR environment by cloning the replicated datastores. Recovery from a disaster and reprotecting production after the outage has been resolved are also made easy by automation built into SRA.
Finally, for the highest level of data protection, consider a VMware vSphere Metro Storage Cluster (vMSC) configuration using NetApp MetroCluster. vMSC is a VMware-certified solution that combines synchronous replication with array-based clustering, giving the same benefits of a high-availability cluster but distributed across separate sites to protect against site disaster. NetApp MetroCluster offers cost-effective configurations for synchronous replication with transparent recovery from any single storage component failure as well as single-command recovery in the event of a site disaster. It’s described in greater detail in TR-4128.

3.2 Space Reclamation

Space may be reclaimed for other use when VMs are deleted within a datastore. When using NFS datastores, space is reclaimed immediately when a VM is deleted (of course, this approach only makes sense when the volume is thin provisioned: that is, volume guarantee set to none). For LUN-based VMFS datastores, ESXi can issue VAAI UNMAP primitives to the storage (again, when using thin provisioning) to reclaim space. Depending on the release, this support is either manual or automatic.

In VMware vSphere 5.0, UNMAP was run by the `vmkfstools -y` command from the ESXi CLI, along with specifying the percentage of blocks that should be freed. In vSphere 5.5 and later, the `vmkfstools -y` command is replaced by the `esxcli storage vmfs unmap` command, which specifies the number of free blocks (see VMware KB 2057513 for more info). In vSphere 6.5 when using VMFS 6, space should be automatically reclaimed asynchronously (see Storage Space Reclamation in vSphere 6.5 documentation), but may also be run manually if needed.

3.3 VM and Datastore Cloning

Cloning a storage object allows you to quickly create copies for further use, such as provisioning additional VMs, backup/recovery operations, and so on. In vSphere, you may clone a VM, virtual disk, VVol, or datastore. After being cloned, the object may be further customized, often through an automated process. vSphere supports both full copy clones, as well as linked clones, where it tracks changes separately from the original object.

Linked clones are great in saving space, but they increase the amount of I/Os that vSphere handles for the VM, affecting performance of that VM and perhaps the host overall. That’s why NetApp customers often use storage system-based clones to get the best of both worlds: efficient use of storage and increased performance.
Cloning may be offloaded to systems running ONTAP software through several mechanisms, typically at the VM, VVol, or datastore level. These include:

- **VVols using the NetApp vSphere APIs for Storage Awareness (VASA) Provider.** ONTAP clones are used to support VVol Snapshot copies managed by vCenter that are space-efficient with minimal I/O impact to create and delete them. VMs may also be cloned using vCenter, and these are also offloaded to ONTAP, whether within a single datastore/volume or between datastores/volumes.

- **vSphere cloning and migration using vSphere APIs – Array Integration (VAAI).** VM cloning operations can be offloaded to ONTAP in both SAN and NAS environments (NetApp supplies an ESXi plug-in to enable VAAI for NFS). Storage vMotion operations are also offloaded to ONTAP for SAN, but this offload is not supported by VMware for NAS. ONTAP uses the most efficient approach based on source, destination, and installed product licenses. This capability is also used by VMware Horizon View.

- **Storage Replication Adapter (used with VMware Site Recovery Manager).** Here, clones are used to test recovery of the DR replica nondisruptively.

- **Backup and recovery using NetApp tools such as SnapCenter.** VM clones are used to verify backup operations, as well as to mount a VM backup so that individual files may be copied.

ONTAP offloaded cloning can be invoked by VMware, NetApp, and third-party tools. Clones that are offloaded to ONTAP have several advantages. They are space-efficient in most cases, needing storage only for changes to the object; there is no additional performance impact to read and write them, and in some cases performance is improved by sharing blocks in high-speed caches; and they offload CPU cycles and network I/O from the ESXi server.

You may also clone a volume or LUN directly within ONTAP to clone a datastore. With NFS datastores, FlexClone technology can clone an entire volume, and the clone can be exported from ONTAP and mounted by ESXi as another datastore. For VMFS datastores, ONTAP can clone a LUN within a volume or a whole volume, including one or more LUNs within it. A LUN containing a VMFS must be mapped to an ESXi initiator group (igroup) and then resignatured by ESXi to be mounted and used as a regular datastore. For some temporary use cases, a cloned VMFS can be mounted without resignaturing. After a datastore is cloned, VMs inside it can be registered, reconfigured, and customized as if they were individually cloned VMs.
In some cases, additional licensed features may be used to enhance cloning, such as SnapRestore for backup or FlexClone. These licenses are often included in license bundles with NetApp AFF systems at no additional cost. A FlexClone license is required for VVol cloning operations as well as to support managed Snapshot copies of a VVol (which are offloaded from the hypervisor to ONTAP). A FlexClone license can also improve certain VAAI-based clones when used within a datastore/volume (creates instant, space-efficient copies instead of block copies). It is also used by the Storage Replication Adapter when testing recovery of a DR replica, and SnapCenter for clone operations and to browse backup copies to restore individual files.

### 3.4 Storage Efficiency and Thin Provisioning

NetApp has led the industry with storage efficiency innovation such as the first deduplication for primary workloads, and inline data compaction, which enhances compression and stores small files and I/Os efficiently. ONTAP supports both inline and background deduplication, as well as inline and background compression.

Figure 7) Combined effect of ONTAP storage efficiency features.

Here are recommendations on using ONTAP storage efficiency in a vSphere environment:

- The amount of data deduplication savings realized is based on the commonality of the data. With ONTAP 9.1 and earlier, data deduplication operated at the volume level, but with aggregate deduplication in ONTAP 9.2 and later, data is deduplicated across all volumes in an aggregate. You no longer need to group similar operating systems and similar applications within a single datastore to maximize savings.
- To realize the benefits of deduplication in a block environment, the LUNs must be thin provisioned. Although the LUN is still seen by the VM administrator as taking the provisioned capacity, the deduplication savings are returned to the volume to be used for other needs. NetApp recommends deploying these LUNs in FlexVol volumes that are also thin provisioned with a capacity that is two times the size of the LUN. When the LUN is deployed in this manner, the FlexVol volume acts merely as a quota. The storage consumed by the LUN is reported in FlexVol and its containing aggregate.
• Thin provisioning is also recommended (and is the default) for NFS FlexVol volumes. In an NFS environment, deduplication savings are immediately visible to both storage and VM administrators with thin-provisioned volumes. This recommendation applies to the VMs as well, where NetApp generally recommends thin-provisioned VMDKs rather than thick. When using thin provisioning, make sure you monitor available space with VSC, ONTAP, or other available tools to avoid out-of-space problems.

• Note that there is no performance penalty when using thin provisioning with ONTAP systems; data is written to available space so that write performance and read performance are maximized. Despite this fact, some products such as Microsoft failover clustering or other low-latency applications might require guaranteed or fixed provisioning, and it is wise to follow these requirements to avoid support problems.

• For maximum deduplication savings, consider scheduling background deduplication. However, these processes use system resources when running, so ideally should be scheduled during less active times (such as weekends) or run more frequently to reduce the amount of changed data to be processed. Automatic background deduplication on AFF systems has much less impact on foreground activities. Background compression (for hard disk–based systems) also consumes resources, so should only be considered for secondary workloads with limited performance requirements.

• NetApp AFF systems primarily use inline storage efficiency capabilities. When data is moved to them using NetApp tools that use block replication such as the 7-Mode Transition Tool, SnapMirror, or Volume Move, it can be useful to run compression and compaction scanners to maximize efficiency savings. Review this NetApp Support KB article for additional details.

• Snapshot copies might lock blocks that could be reduced by compression or deduplication. When using scheduled background efficiency or using one-time scanners, make sure that they run and complete before the next Snapshot copy is taken. Review your Snapshot copies and retention to make sure you only retain needed Snapshot copies, especially before a background or scanner job is run.

These are the storage efficiency guidelines for virtualized workloads on different types of ONTAP storage from TR-4476:

<table>
<thead>
<tr>
<th>Workload</th>
<th>Storage Efficiency Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFF</td>
<td>Flash Pool</td>
</tr>
<tr>
<td>VDI and SVI</td>
<td>For primary and secondary workloads, use: • Adaptive inline compression • Inline deduplication • Background deduplication • Inline data compaction</td>
</tr>
<tr>
<td>AFF</td>
<td>Flash Pool</td>
</tr>
<tr>
<td>VDI and SVI</td>
<td>For primary and secondary workloads, use: • Adaptive inline compression • Inline deduplication • Background deduplication • Inline data compaction</td>
</tr>
<tr>
<td>AFF</td>
<td>Flash Pool</td>
</tr>
<tr>
<td>VDI and SVI</td>
<td>For primary and secondary workloads, use: • Adaptive inline compression • Inline deduplication • Background deduplication • Inline data compaction</td>
</tr>
</tbody>
</table>
3.5 Quality of Service (QoS)

Systems running ONTAP software may use the ONTAP storage quality of service (QoS) feature to limit throughput in MBps and/or I/Os per second (IOPS) for different storage objects such as files, LUNs, volumes, or entire SVMs.

Throughput limits are useful in controlling unknown or test workloads before deployment to make sure they don’t affect other workloads. They may also be used to constrain a bully workload after being identified. Minimum levels of service based on IOPS are also supported to provide consistent performance for SAN objects in ONTAP 9.2 and for NAS objects in ONTAP 9.3.

With an NFS datastore, a QoS policy may be applied to the entire FlexVol volume or individual VMDK files within it. With VMFS datastores using ONTAP LUNs, the QoS policies may be applied to the FlexVol volume that contains the LUNs or individual LUNs, but not individual VMDK files because ONTAP has no awareness of the VMFS file system. When using VVols with VSC 7.1, maximum QoS may be set on individual VMs using the storage capability profile.

The QoS maximum throughput limit on an object can be set in MBps and/or IOPS. If both are used, the first limit reached is enforced by ONTAP. A workload can contain multiple objects, and a QoS policy can be applied to one or more workloads. When a policy is applied to multiple workloads, the workloads share the total limit of the policy. Nested objects are not supported (for example, a file within a volume cannot each have their own policy). QoS minimums can only be set in IOPS.

The following tools are currently available for managing ONTAP QoS policies and applying them to objects:

- ONTAP CLI
- OnCommand System Manager
- OnCommand Workflow Automation
- OnCommand API Services
- OnCommand Performance Manager (now integrated with OnCommand Unified Manager)
- NetApp PowerShell Toolkit for ONTAP
- Virtual Storage Console VASA Provider

To assign a QoS policy to a VMDK on NFS, note the following guidelines:

- The policy must be applied to the `vmname-flat.vmdk` that contains the actual virtual disk image, not the `vmname.vmdk` (virtual disk descriptor file) or `vmname.vmx` (VM descriptor file).
- Do not apply policies to other VM files such as virtual swap files (`vmname.vswp`).
- When using the vSphere web client to find file paths (Datastore > Files), be aware that it combines the information of the `-flat.vmdk` and `.vmdk` and simply shows one file with the name of the `.vmdk` but the size of the `-flat.vmdk`. Add `-flat` into the file name to get the correct path.

To assign a QoS policy to a LUN, including VMFS and RDM, the ONTAP SVM (displayed as Vserver), LUN path, and serial number can be obtained from the Storage Systems menu on the VSC home page. Select the storage system (SVM), then Related Objects > SAN. Use this approach when specifying QoS using one of the ONTAP tools.

OnCommand System Manager requires a service level to be specified when provisioning virtual server datastores using application templates. System Manager uses the specified service level to select a node and aggregate with sufficient performance headroom. In 9.2, QoS is used to set an IOPS ceiling (QoS max) based on the service level and initial datastore size. In 9.3, adaptive QoS is used to set an IOPS floor (QoS min) and ceiling (QoS max), which dynamically adjust based on the datastore capacity and used space. An IOPS floor is set on AFF systems only. For more information about QoS and performance headroom, see the ONTAP Performance Management Power Guide, guaranteeing throughput with QoS section.
Maximum QoS may be easily assigned to a VVol-based VM with VSC 7.1 and later. When creating the storage capability profile for the VVol container, specify a max IOPS value under the performance capability and then reference this SCP with the VM’s Storage Policy. Use this policy when creating the VM or apply the policy to an existing VM.

**ONTAP QoS and VMware SIOC**

ONTAP QoS and VMware vSphere Storage I/O Control (SIOC) are complementary technologies that vSphere and storage administrators can use together to manage performance of vSphere VMs hosted on systems running ONTAP software. Each tool has its own strengths, as shown in Table 8. Because of the different scope of VMware vCenter and ONTAP, some objects can be seen and managed by one system and not the other.

<table>
<thead>
<tr>
<th>Property</th>
<th>ONTAP QoS</th>
<th>VMware SIOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>When active</td>
<td>Policy is always active</td>
<td>Active when contention exists (datastore latency over threshold)</td>
</tr>
<tr>
<td>Type of units</td>
<td>IOPS, MBps</td>
<td>IOPS, shares</td>
</tr>
<tr>
<td>vCenter or application scope</td>
<td>Multiple vCenter environments, other hypervisors and applications</td>
<td>Single vCenter server</td>
</tr>
<tr>
<td>Set QoS on VM?</td>
<td>VMDK on NFS only</td>
<td>VMDK on NFS or VMFS</td>
</tr>
<tr>
<td>Set QoS on LUN (RDM)?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Set QoS on LUN (VMFS)?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Set QoS on volume (NFS datastore)?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Set QoS on SVM (tenant)?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Policy-based approach?</td>
<td>Yes; throughput is shared by all workloads in the policy.</td>
<td>No; shares and limits are set on each VM’s virtual disk.</td>
</tr>
<tr>
<td>License required</td>
<td>Included with ONTAP</td>
<td>Enterprise Plus</td>
</tr>
</tbody>
</table>

### Table 8) ONTAP QoS and VMware SIOC comparison.

3.6 **VMware Storage Distributed Resource Scheduler (SDRS)**

VMware Storage Distributed Resource Scheduler (SDRS) is a vSphere feature that places VMs on storage based on the current I/O latency and space usage. It then moves the VM or VMDKs nondisruptively between the datastores in a datastore cluster (also referred to as a pod), selecting the best datastore in which to place the VM or VMDKs in the datastore cluster. A datastore cluster is a collection of similar datastores that are aggregated into a single unit of consumption from the vSphere administrator’s perspective.

When using SDRS with the NetApp VSC, you must first create a datastore with VSC, then use vCenter to create the datastore cluster and add the datastore to it. After the datastore cluster is created, additional datastores can be added to the datastore cluster directly from the VSC provisioning wizard on the Details page.

Other ONTAP best practices for SDRS:

- All datastores in the cluster should use the same type of storage (such as SAS, SATA, SSD), be either all VMFS or NFS datastores, and have the same replication and protection settings.
Consider using SDRS in default (manual) mode. This approach allows you to review the recommendations and decide whether to apply them or not. Be aware of these impacts of VMDK migrations:

- When SDRS moves VMDKs between datastores, any space savings from ONTAP cloning or deduplication are lost. You can rerun deduplication to regain these savings.
- After SDRS moves VMDKs, NetApp recommends recreating the Snapshot copies at the source datastore because space is otherwise locked by the VM that was moved.
- Moving VMDKs between datastores on the same aggregate has little benefit, and SDRS does not have visibility into other workloads that might share the aggregate.

3.7 Storage Policy-Based Management and Virtual Volumes (VVols)

VMware vSphere APIs for Storage Awareness (VASA) make it easy for a storage administrator to configure datastores with well-defined capabilities and let the VM administrator use those whenever needed to provision VMs without having to interact with each other. It’s worth taking a look at this approach to see how it can streamline your virtualization storage operations and avoid a lot of trivial work.

Prior to VASA, VM administrators could define VM storage policies, but had to work with the storage administrator to identify appropriate datastores, often by using documentation or naming conventions. With VASA, the storage administrator can define a range of storage capabilities, including availability, performance, capacity, space efficiency, replication, and protocol. A set of capabilities for a volume or a set of volumes is called a storage capability profile (SCP).

Starting with ONTAP 9.3 and VSC 7.1, the SCP has been extended to support maximum QoS for a VM’s data VVol. The VASA Provider 7.1 also has a new dashboard that displays VM granular performance and logical capacity for VVols on ONTAP 9.3 systems. With these new capabilities in VASA Provider 7.1 along with ONTAP 9.3, NetApp is also offering guaranteed storage efficiency of 4:1 for VVol datastores on ONTAP 9.3 systems through the All-Flash Guarantee program. Contact your NetApp or partner team for more details.

Figure 8) VASA Provider 7.1 dashboard.

After the storage capability profile is defined, it can be used to provision VMs using the storage policy that identifies its requirements. The mapping between VM storage policy and datastore storage capability
profile allows vCenter to display a list of compatible datastores for selection. This approach is known as storage policy-based management.

VASA 2.0 provides the technology to query storage and return a set of storage capabilities to vCenter. VASA vendor providers supply the translation between the storage system APIs and constructs and the VMware APIs that are understood by vCenter. NetApp’s VASA Provider for ONTAP is offered as an appliance VM, and the VSC provides the interface to provision and manage VVol datastores, as well as the ability to define storage capability profiles (SCPs).

ONTAP supports both VMFS and NFS VVol datastores. Using VVols with SAN datastores brings some of the benefits of NFS such as VM-level granularity. Here are some best practices to consider, and you can find additional information in TR-4400:

- A VVol datastore may consist of multiple FlexVol volumes on multiple cluster nodes. The simplest approach is a single datastore, even when the volumes have different capabilities. SPBM makes sure that a compatible volume is used for the VM. However, the volumes must all be part of a single ONTAP SVM and accessed using a single protocol. One LIF per node for each protocol is sufficient. Avoid using multiple ONTAP releases within a single VVol datastore because the storage capabilities might vary across releases.

- Use the VSC to create and manage VVol datastores. In addition to managing the datastore and its profile, the VSC automatically creates a protocol endpoint to access the VVols if needed. If LUNs are used, note that LUN PEs are mapped using LUN IDs 300 and higher. Verify that the ESXi host advanced system setting Disk.MaxLUN allows a LUN ID number that is higher than 300 (the default is 1,024). Do this step by selecting the ESXi host in vCenter, then the Configure tab, and find Disk.MaxLUN in the list of Advanced System Settings.

- Do not install or migrate VASA Provider, vCenter Server (appliance or Windows based), or VSC onto a VVol datastore, because they are then mutually dependent, limiting your ability to manage them in the event of a power outage or other data center disruption.

- Back up the VASA Provider VM regularly. At a minimum, create hourly Snapshot copies of the traditional datastore that contains VASA Provider. For more about protecting and recovering the VASA Provider, see this KB article.
3.8 Cloud Migration and Backup

Another ONTAP strength is broad support for hybrid cloud, merging systems in your on-premises private cloud with public cloud capabilities. Here are some NetApp cloud solutions that can be used in conjunction with vSphere:

NetApp Private Storage for Cloud

NetApp offers two cloud-based storage solutions that can easily integrate with your on-premises ONTAP system while giving you complete control over your data. NetApp Private Storage for Cloud provides storage services to Amazon Web Services, Google Cloud Platform, IBM Cloud, and Microsoft Azure public clouds using high-performance systems connected at low latency from colocated data centers. Use this approach to keep data in sync between cloud and in-house applications, safely leverage inexpensive cloud compute for your enterprise data, or explore options to use this as part of your dev/test or disaster recovery approach.

ONTAP Cloud

The second solution, the NetApp ONTAP Cloud storage software service, delivers enterprise control, protection, and efficiency to your data with the flexibility of the Amazon Web Services or Microsoft Azure cloud. A single management console helps you deploy and manage ONTAP Cloud instances together with your on-premises ONTAP systems. ONTAP Cloud on AWS works together with VMware Cloud on AWS so that your VMs can access ONTAP Cloud data, taking advantage of advanced features such as FlexClone, SnapMirror, or SnapVault for dev/test or data protection use cases.

Cloud Backup with AltaVault

Use the NetApp AltaVault cloud-integrated storage system to protect your vSphere environment while continuing to use your existing backup software. Back up your VMs to the cloud with secure encryption and use AltaVault inline deduplication and compression for up to 30:1 data reduction ratios.
FabricPool, introduced in ONTAP 9.2, offers quick and easy tiering for ONTAP data. Cold blocks in Snapshot copies may be migrated to an object store in either the public Amazon Web Services S3 cloud or a private StorageGRID® Webscale object store and are automatically recalled when the ONTAP data is accessed again. Or use the object tier as a third level of protection for data that is already managed by SnapVault. This approach can allow you to store more Snapshot copies of your VMs on primary and/or secondary ONTAP storage systems. Use NetApp’s software-defined storage to extend your private cloud across the Internet to remote facilities and offices, where you can use ONTAP Select to support block and file services as well as the same vSphere data management capabilities you have in your enterprise data center.

Figure 10) NetApp hybrid cloud solutions.

3.9 Encryption for vSphere Data

Today there are increasing demands to protect data at rest through encryption. Although the initial focus was on financial and healthcare information, there is growing interest in protecting all information, whether it’s stored in files, databases, or other data types.

Systems running ONTAP software make it easy to protect any data with at-rest encryption. More than five years ago, NetApp Storage Encryption (NSE) brought self-encrypting disk drives to ONTAP to protect SAN and NAS data. NetApp introduced NetApp Volume Encryption (NVE) as part of ONTAP 9.1, a simple, software-based approach to encrypt volumes on any disk drives. NVE doesn’t require special disk drives or external key managers and is available to ONTAP customers at no additional cost. You can upgrade and start using it without any disruption to your clients or applications. And NVE is validated to the FIPS 140-2 level 1 standard, including the onboard key manager.

There are several approaches for protecting the data of virtualized applications running on VMware vSphere. One approach is to protect the data with software inside the VM at the guest OS level. Newer hypervisors such as vSphere 6.5 now support encryption at the VM level as another alternative. However, NetApp Volume Encryption is simple and easy and has these benefits:

- **No impact to virtual server CPU.** Some virtual server environments need every available CPU cycle for their applications, yet tests have shown up to 5x CPU resources are needed with hypervisor-level encryption. Even if the encryption software supports Intel’s AES-NI instruction set to offload...
encryption workload (as NVE does), this approach might not be feasible due to the requirement for
new CPUs not compatible with older servers.

- **Onboard key manager included.** NetApp Volume Encryption includes an onboard key manager at
  no additional cost, which makes it easy to get started without high-availability key management
  servers that are complex to purchase and use.

- **No impact to storage efficiency.** Storage efficiency techniques such as deduplication and
  compression are widely used today and are key to using flash disk media cost-effectively. However,
  encrypted data cannot typically be deduplicated or compressed. NSE and NVE operate at a lower
  level and allow full use of NetApp’s industry-leading storage efficiency features, unlike other
  approaches.

- **Easy datastore granular encryption.** With NVE, each volume gets its own AES 256-bit key. If you
  need to change it, you can do so with a single command. This approach is great if you have multiple
  tenants or need to prove independent encryption for different departments or apps. And you manage
  this encryption at the datastore level, which is a lot easier than managing individual VMs.

It’s simple to get started with NVE. After the license is installed, simply configure the onboard key
manager by specifying a passphrase and then either create a new volume or do a storage-side volume
move to enable encryption. NetApp is working to add more integrated support for encryption capabilities
in future releases of its VMware tools.
Appendix A: ONTAP and vSphere Release-Specific Information

This section provides guidance on capabilities supported by specific releases of ONTAP and vSphere. NetApp recommends confirming a specific combination of releases with the NetApp Interoperability Matrix.

ONTAP Releases

At the time of publication, NetApp provides full support for three release families:

- ONTAP 9.1
- ONTAP 9.2
- ONTAP 9.3

The following capabilities might be of value to vSphere environments.

| ONTAP 9.1 | • Support new FAS2600, FAS8200, FAS9000, AFF200, AFF300, AFF700, and AFF700s storage systems  
|           | • NetApp Volume Encryption with onboard key management  
|           | • SAN cluster scales to 12 nodes  
|           | • SnapMirror integration with AltaVault for cloud backup  

| ONTAP 9.2 | • FabricPool support (maintain more Snapshot copies by moving cold blocks to cloud)  
|           | • Inline aggregate deduplication (greater storage efficiency across datastores for AFF systems)  
|           | • QoS minimum for AFF SAN  
|           | • OnCommand System Manager for easy cluster creation and expansion and headroom-based provisioning of datastores with QoS  
|           | • SAN performance optimizations  

| ONTAP 9.3 | • Automatic background deduplication (volume and aggregate)  
|           | • Multithreading improvements to iSCSI read performance  
|           | • Adaptive QoS scales performance with storage capacity (IOPS/TB; volumes only)  
|           | • QoS minimum for AFF NAS  
|           | • OnCommand System Manager provisioning supports service-level changes, Snapshot copies, adaptive QoS, MetroCluster  
|           | • Enhanced security with multifactor authentication for administrators, external key manager for NetApp Volume Encryption  
|           | • Performance and space counters for individual VVol files/LUNs (view with VSC 7.1)  

vSphere and ESXi Support

NetApp ONTAP has broad support for vSphere ESXi hosts. The three major release families just described (9.1, 9.2, 9.3) are supported as data storage platforms for recent vSphere releases, including 5.5, 6.0, and 6.5 (including updates for these releases). NFS v3 interoperability is broadly defined, and NetApp supports any client, including hypervisors, that is compliant with the NFS v3 standard. NFSv4.1 support is limited to vSphere 6.0 and 6.5.

For SAN environments, NetApp conducts extensive testing of SAN components. In general, NetApp supports standard X86-64 rack servers and Cisco UCS servers together with standard Ethernet adapters for iSCSI connections. FC and FCoE environments have more specifically defined support due to the HBA firmware and drivers needed.
Always check the [NetApp Interoperability Matrix](https://www.netapp.com/interoperability) to confirm support for a specific hardware and software configuration.

**NFS Plug-In for VMware VAAI**

This plug-in for ESXi hosts helps by offloading operations to ONTAP using VAAI. The latest release, 1.1.2, added support for NFSv4.1 datastores, including Kerberos (krb5 and krb5i) support. It is supported with ESXi 5.5, 6.0, and 6.5, together with ONTAP 9.1, 9.2, and 9.3.

**VASA Provider**

NetApp’s VASA Provider supports VVol provisioning and management (see section 3.7). Recent VASA Provider releases support ESXi 5.5, 6.0, and 6.5, together with ONTAP 9.1, 9.2, and 9.3.

**Virtual Storage Console**

The Virtual Storage Console is a key tool for managing ONTAP storage together with vSphere (using it is a best practice). The latest release, 7.1, is supported with vSphere 6.0 and 6.5, together with ONTAP 9.1, 9.2, and 9.3.
Appendix B: Recommended ESXi Host and Other ONTAP Settings

NetApp has developed a set of ESXi host multipathing and HBA timeout settings for proper behavior with ONTAP based on NetApp testing. These are easily set using the Virtual Storage Console. (From the VSC Summary dashboard, click Edit Settings in the Host Systems portlet or right-click the host in vCenter, then VSC > Set Recommended Values.) Here are the currently recommended host settings.

<table>
<thead>
<tr>
<th>Host Setting</th>
<th>NetApp Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESXi Advanced Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>VMFS3.HardwareAcceleratedLocking</td>
<td>Set to 1.</td>
</tr>
<tr>
<td>VMFS3.EnableBlockDelete</td>
<td>Set to 0. For more information, see VMware KB article 2007427.</td>
</tr>
<tr>
<td><strong>NFS Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Net.TcpipHeapSize</td>
<td>vSphere 5.0 or later, set to 32. All other NFS configurations, set to 30.</td>
</tr>
<tr>
<td>Net.TcpipHeapMax</td>
<td>Set to 1536 for vSphere 6.0 and later, 512 for vSphere 5.5, 128 for vSphere 5.0 and 5.1, and 120 for earlier vSphere releases.</td>
</tr>
<tr>
<td>NFS.MaxVolumes</td>
<td>vSphere 5.0 or later, set to 256. All other NFS configurations, set to 64.</td>
</tr>
<tr>
<td>NFS41.MaxVolumes</td>
<td>vSphere 6.0 or later, set to 256.</td>
</tr>
<tr>
<td>NFS.MaxQueueDepth</td>
<td>vSphere 5.0 or later, set to 64. Consider increasing to 128, especially when using only AFF systems for a host cluster.</td>
</tr>
<tr>
<td>NFS.HeartbeatMaxFailures</td>
<td>Set to 10 for all NFS configurations.</td>
</tr>
<tr>
<td>NFS.HeartbeatFrequency</td>
<td>Set to 12 for all NFS configurations.</td>
</tr>
<tr>
<td>NFS.HeartbeatTimeout</td>
<td>Set to 5 for all NFS configurations.</td>
</tr>
<tr>
<td><strong>FC/FCoE Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Path selection policy</td>
<td>Set to <strong>RR</strong> (round robin) when FC paths with ALUA are used. Set to <strong>FIXED</strong> for all other configurations. Setting this value to <strong>RR</strong> helps provide load balancing across all active/optimized paths. The value <strong>FIXED</strong> is for older, non-ALUA configurations and helps prevent proxy I/O. In other words, it helps keep I/O from going to the other node of a high-availability (HA) pair in an environment that has Data ONTAP® operating in 7-Mode.</td>
</tr>
<tr>
<td>Disk.QFullSampleSize</td>
<td>Set to 32 for all configurations. Setting this value helps prevent I/O errors.</td>
</tr>
<tr>
<td>Disk.QFullThreshold</td>
<td>Set to 8 for all configurations. Setting this value helps prevent I/O errors.</td>
</tr>
<tr>
<td>Emulex FC HBA timeouts</td>
<td>Use the default value.</td>
</tr>
<tr>
<td>QLogic FC HBA timeouts</td>
<td>Use the default value.</td>
</tr>
<tr>
<td><strong>iSCSI Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Host Setting</td>
<td>NetApp Recommended Value</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Path selection policy</td>
<td>Set to <strong>RR</strong> (round robin) for all iSCSI paths. Setting this value to <strong>RR</strong> helps provide load balancing across all active/optimized paths.</td>
</tr>
<tr>
<td>Disk.QFullSampleSize</td>
<td>Set to <strong>32</strong> for all configurations. Setting this value helps prevent I/O errors.</td>
</tr>
<tr>
<td>Disk.QFullThreshold</td>
<td>Set to <strong>8</strong> for all configurations. Setting this value helps prevent I/O errors.</td>
</tr>
</tbody>
</table>

The Virtual Storage Console also specifies certain default settings when creating ONTAP FlexVol volumes:

- Snapshot reserve (-percent-snapshot-space) 0
- Fractional reserve (-fractional-reserve) 0
- Access time update (-atime-update) False
- Minimum readahead (-min-readahead) False
- Scheduled Snapshot copies None
- Storage efficiency Enabled
Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>May 2017</td>
<td>Initial release</td>
</tr>
<tr>
<td>Version 2.0</td>
<td>January 2018</td>
<td>Updated for ONTAP 9.2 and 9.3, VSC 7.x; additional best practices based on reader feedback</td>
</tr>
</tbody>
</table>

Contact Us

Do you have comments about this technical report?
Send them to us at docfeedback@netapp.com, and include TR-4597 in the subject line.
Alternately, look for a blog post regarding this report at blog.netapp.com/updated-technical-report-for-vsphere-with-ontap, and leave comments there.
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

Copyright © 2017–2018 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.