



# **Best practices**

## **FlexPod**

NetApp  
June 08, 2021

This PDF was generated from [https://docs.netapp.com/us-en/flexpod/healthcare/medical-imaging\\_best\\_practices.html](https://docs.netapp.com/us-en/flexpod/healthcare/medical-imaging_best_practices.html) on October 13, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Best practices ..... 1
  - Storage best practices ..... 1
  - Infrastructure best practices ..... 5
  - Medical imaging system best practices ..... 5

# Best practices

## Storage best practices

### High availability

The NetApp storage cluster design provides high availability at every level:

- Cluster nodes
- Back-end storage connectivity
- RAID TEC that can sustain three disk failures
- RAID DP that can sustain two disk failures
- Physical connectivity to two physical networks from each node
- Multiple data paths to storage LUNs and volumes

### Secure multitenancy

NetApp storage virtual machines (SVMs) provide a virtual storage array construct to separate your security domain, policies, and virtual networking. NetApp recommends that you create separate SVMs for each tenant organization that hosts data on the storage cluster.

### NetApp storage best practices

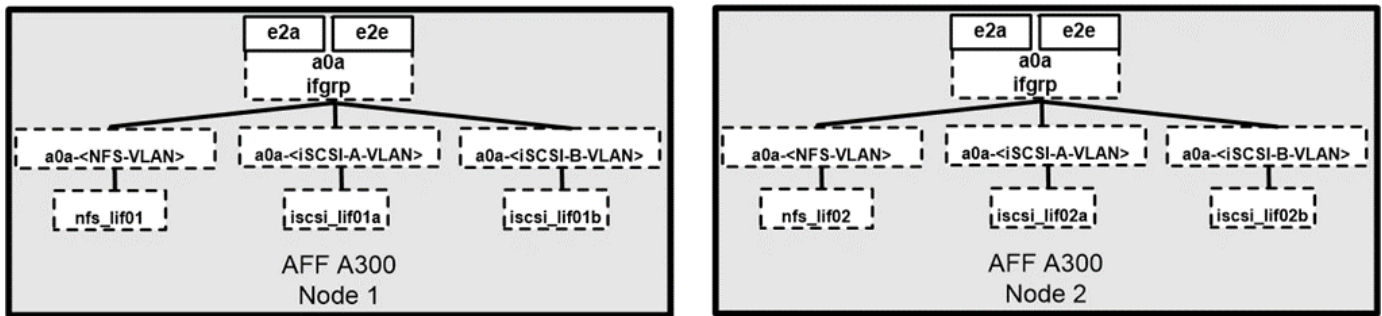
Consider the following NetApp storage best practices:

- Always enable NetApp AutoSupport technology, which sends support summary information to NetApp through HTTPS.
- For maximum availability and mobility, make sure that a LIF is created for each SVM on each node in the NetApp ONTAP cluster. Asymmetric logical unit access (ALUA) is used to parse paths and to identify active optimized (direct) paths versus active nonoptimized paths. ALUA is used for both FC or FCoE and iSCSI.
- A volume that contains only LUNs does not need to be internally mounted, nor is a junction path required.
- If you use the Challenge-Handshake Authentication Protocol (CHAP) in ESXi for target authentication, you must also configure it in ONTAP. Use the CLI (`vserver iscsi security create`) or NetApp ONTAP System Manager (edit Initiator Security under Storage > SVMs > SVM Settings > Protocols > iSCSI).

### SAN boot

NetApp recommends that you implement SAN boot for Cisco UCS Servers in the FlexPod Datacenter solution. This step enables the operating system to be safely secured by the NetApp AFF storage system, providing better performance. The design that is outlined in this solution uses iSCSI SAN boot.

In iSCSI SAN boot, each Cisco UCS Server is assigned two iSCSI vNICs (one for each SAN fabric), which provide redundant connectivity all the way to the storage. The storage ports in this example, e2a and e2e, which are connected to the Cisco Nexus switches, are grouped together to form one logical port called an interface group (ifgrp) (in this example, a0a). The iSCSI VLANs are created on the igroup, and the iSCSI LIFs are created on iSCSI port groups (in this example, a0a-`iSCSI-A-VLAN`). The iSCSI boot LUN is exposed to the servers through the iSCSI LIF by using igroups. This approach enables only the authorized server to have access to the boot LUN. For the port and LIF layout, see the figure below.



Unlike NAS network interfaces, the SAN network interfaces are not configured to fail over during a failure. Instead, if a network interface becomes unavailable, the host chooses a new optimized path to an available network interface. ALUA, a standard supported by NetApp, provides information about SCSI targets, which enables a host to identify the best path to the storage.

## Storage efficiency and thin provisioning

NetApp has led the industry in storage efficiency innovation, such as with the first deduplication for primary workloads and with 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.

To realize the benefits of deduplication in a block environment, the LUNs must be thin-provisioned. Although the LUN is still seen by your VM administrator as taking the provisioned capacity, the deduplication savings are returned to the volume to be used for other needs. NetApp recommends that you deploy these LUNs in FlexVol volumes that are also thin-provisioned with a capacity that is two times the size of the LUN. When you deploy the LUN that way, the FlexVol volume acts merely as a quota. The storage that the LUN consumes is reported in the FlexVol volume and its containing aggregate.

For maximum deduplication savings, consider scheduling background deduplication. These processes use system resources when they're running, however. So, ideally, you should schedule them during less active times (such as weekends) or run them more frequently to reduce the amount of changed data to be processed. Automatic background deduplication on AFF systems has much less of an effect on foreground activities. Background compression (for hard disk-based systems) also consumes resources, so you should consider it only for secondary workloads with limited performance requirements.

## Quality of service

Systems that run ONTAP software can use the ONTAP storage QoS feature to limit throughput in megabits per second (MBps) and to limit IOPS for different storage objects such as files, LUNs, volumes, or entire SVMs. Adaptive QoS is used to set an IOPS floor (QoS minimum) and ceiling (QoS maximum), which dynamically adjust based on the datastore capacity and used space.

Throughput limits are useful for controlling unknown or test workloads before a deployment to confirm that they don't affect other workloads. You might also use these limits to constrain a bully workload after it has been identified. Minimum levels of service based on IOPS are also supported to provide consistent performance for SAN objects in ONTAP.

With an NFS datastore, a QoS policy can be applied to the entire FlexVol volume or to individual Virtual Machine Disk (VMDK) files within it. With VMFS datastores (Cluster Shared Volumes [CSV] in Hyper-V) that use ONTAP LUNs, you can apply the QoS policies to the FlexVol volume that contains the LUNs or to the individual LUNs. However, because ONTAP has no awareness of the VMFS, you cannot apply the QoS policies to individual VMDK files. When you use VMware Virtual Volumes (VVs) with VSC 7.1 or later, you can set maximum QoS on individual VMs by using the storage capability profile.

To assign a QoS policy to a LUN, including VMFS or CSV, you can obtain the ONTAP SVM (displayed as `vserver`), LUN path, and serial number from the Storage Systems menu on the VSC home page. Select the storage system (SVM), then Related Objects > SAN. Use this approach when you specify QoS by using one of the ONTAP tools.

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

## Storage layout

This section provides best practices for layout of LUNs, volumes, and aggregates on storage.

### Storage LUNs

For optimal performance, management, and backup, NetApp recommends the following LUN-design best practices:

- Create a separate LUN to store database data and log files.
- Create a separate LUN for each instance to store Oracle database log backups. The LUNs can be part of the same volume.
- Provision LUNs with thin provisioning (disable the Space Reservation option) for database files and log files.
- All imaging data is hosted in FC LUNs. Create these LUNs in FlexVol volumes that are spread across the aggregates that are owned by different storage controller nodes.

For placement of the LUNs in a storage volume, follow the guidelines in the next section.

### Storage volumes

For optimal performance, management, and backup operations, NetApp recommends the following volume design best practices:

- Isolate databases with I/O-intensive queries throughout the day in different volumes and eventually have separate jobs to back them up.
- For faster recovery, place large databases and databases that have minimal recovery time objectives (RTOs) in separate volumes.
- Consolidate into a single volume your small-to-medium-sized databases that are less critical or that have fewer I/O requirements. When you back up a large number of databases that reside in the same volume, fewer Snapshot copies need to be maintained. NetApp also recommends that you consolidate Oracle database server instances to use the same volumes to control the number of backup Snapshot copies that are created.
- For database replicas, place the data and log files for replicas in an identical folder structure on all nodes.
- Place database files in a single FlexVol; don't spread them across FlexVols.
- Configure a volume auto size policy, when appropriate, to help prevent out-of-space conditions.
- When the database I/O profile consists mostly of large sequential reads, such as with decision support system workloads, enable read reallocation on the volume. Read reallocation optimizes the blocks for better performance.

- For ease of monitoring from an operational perspective, set the Snapshot copy reserve value in the volume to zero.
- Disable storage Snapshot copy schedules and retention policies. Instead, use NetApp SnapCenter Plug-In for Oracle Database to coordinate Snapshot copies of the Oracle data volumes.
- Place user data files and log files on separate FlexVols so that appropriate QoS can be configured for the respective FlexVols and so that different backup schedules can be created.

## Aggregates

Aggregates are the primary storage containers for NetApp storage configurations and contain one or more RAID groups that consist of both data disks and parity disks.

NetApp performed various I/O workload characterization tests by using shared and dedicated aggregates with data files and transaction log files separated. The tests show that one large aggregate with more RAID groups and drives (HDDs or SSDs) optimizes and improves storage performance and is easier for administrators to manage for two reasons:

- One large aggregate makes the I/O abilities of all drives available to all files.
- One large aggregate enables the most efficient use of disk space.

For effective disaster recovery, NetApp recommends that you place the asynchronous replica on an aggregate that is part of a separate storage cluster in your disaster recovery site and use SnapMirror technology to replicate content.

For optimal storage performance, NetApp recommends that you have at least 10% free space available in an aggregate.

Storage aggregate layout guidance for AFF A300 systems (with two disk shelves with 24 drives) includes:

- Keep two spare drives.
- Use Advanced Disk Partitioning to create three partitions on each drive: root and data.
- Use a total of 20 data partitions and two parity partitions for each aggregate.

## Backup best practices

NetApp SnapCenter is used for VM and database backups. NetApp recommends the following backup best practices:

- When SnapCenter is deployed to create Snapshot copies for backups, turn off the Snapshot schedule for the FlexVol that host VMs and application data.
- Create a dedicated FlexVol for host boot LUNs.
- Use a similar or a single backup policy for VMs that serve the same purpose.
- Use a similar or a single backup policy per workload type; for example, use a similar policy for all database workloads. Use different policies for databases, web servers, end-user virtual desktops, and so on.
- Enable verification of the backup in SnapCenter.
- Configure archiving of the backup Snapshot copies to the NetApp SnapVault backup solution.
- Configure retention of the backups on primary storage based on the archiving schedule.

# Infrastructure best practices

## Networking best practices

NetApp recommends the following networking best practices:

- Make sure that your system includes redundant physical NICs for production and storage traffic.
- Separate VLANs for iSCSI, NFS, and SMB/CIFS traffic between compute and storage.
- Make sure that your system includes a dedicated VLAN for client access to the medical imaging system.

You can find additional networking best practices in the FlexPod infrastructure design and deployment guides.

## Compute best practices

NetApp recommends the following compute best practice:

- Make sure that each specified vCPU is supported by a physical core.

## Virtualization best practices

NetApp recommends the following virtualization best practices:

- Use VMware vSphere 6 or later.
- Set the ESXi host server BIOS and OS layer to Custom Controlled–High Performance.
- Create backups during off-peak hours.

# Medical imaging system best practices

See the following best practices and some requirements from a typical medical imaging system:

- Do not overcommit virtual memory.
- Make sure that the total number of vCPUs equals the number of physical CPUs.
- If you have a large environment, dedicated VLANs are required.
- Configure database VMs with dedicated HA clusters.
- Make sure that the VM OS VMDKs are hosted in fast tier 1 storage.
- Work with the medical imaging system vendor to identify the best approach to prepare VM templates for quick deployment and maintenance.
- Management, storage, and production networks require LAN segregation for the database, with isolated VLANs for VMware vMotion.
- Use the NetApp storage-array-based replication technology called [SnapMirror](#) instead of vSphere- based replication.
- Use backup technologies that leverage VMware APIs; backup windows should be outside the normal production hours.

## Copyright Information

Copyright © 2021 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.