Enterprise Applications and Databases

NetApp Solutions

NetApp
August 03, 2021

Table of Contents

Enterprise Applications and Databases

SAP Business Application and SAP HANA Database Solutions

NetApp has an extensive collection of technical reports, validated designs and solution briefs for SAP and SAP HANA. They are organized into the following 4 categories and can be expanded from the sidebar on the left for more information.

- SAP on NetApp Configuration Best Practices
- Backup & Recovery and Disaster Recovery
- SAP Lifecycle Management
- Solution Briefs

SAP on NetApp Configuration Best Practices

TR-4436: SAP HANA on NetApp AFF Systems with Fibre Channel Protocol

Nils Bauer and Marco Schoen, NetApp

Introduction

The NetApp AFF product family is certified for use with SAP HANA in TDI projects. The certified enterprise storage platform is characterized by the NetApp ONTAP software.

The certification is valid for the following models:

- AFF A220, AFF A250, AFF A300, AFF A320, AFF A400, AFF A700s, AFF A700, AFF A800
- ASA AFF A220, ASA AFF A250, ASA AFF A400, ASA AFF A700, ASA AFF A800For a complete list of NetApp certified storage solutions for SAP HANA, see the Certified and supported SAP HANA hardware directory.

This document describes AFF configurations that use the Fibre Channel Protocol (FCP).

The configuration described in this paper is necessary to achieve the required SAP HANA KPIs and the best performance for SAP HANA. Changing any settings or using features not listed herein might cause performance degradation or unexpected behavior and should only be done if advised by NetApp support.

The configuration guides for AFF systems using NFS and NetApp FAS systems can be found using the following links:

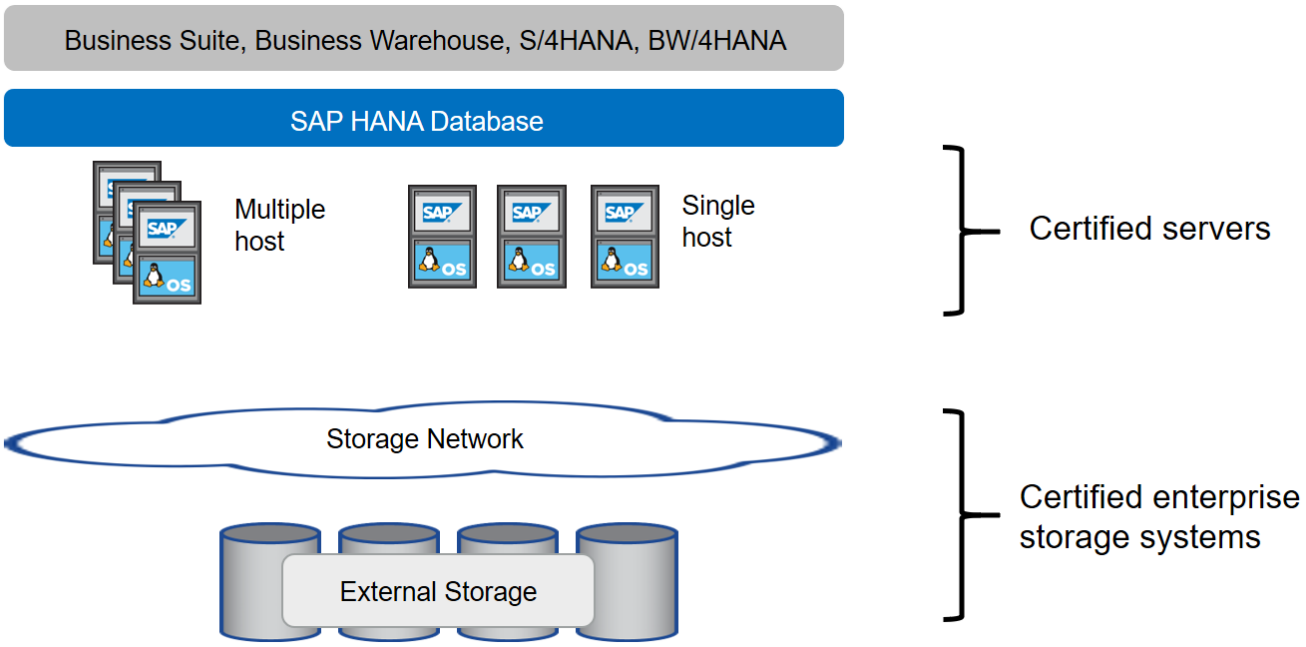
- SAP HANA on NetApp FAS Systems with FCP
- SAP HANA on NetApp FAS Systems with NFS
- SAP HANA on NetApp AFF Systems with NFS

In an SAP HANA multiple-host environment, the standard SAP HANA storage connector is used to provide fencing in the event of an SAP HANA host failover. Always refer to the relevant SAP notes for operating system configuration guidelines and HANA specific Linux kernel dependencies. For more information, see SAP Note

2235581 – SAP HANA Supported Operating Systems.

SAP HANA tailored data center integration

NetApp AFF storage systems are certified in the SAP HANA TDI program using both NFS (NAS) and FC (SAN) protocols. They can be deployed in any of the current SAP HANA scenarios, such as SAP Business Suite on HANA, S/4HANA, BW/4HANA, or SAP Business Warehouse on HANA in either single-host or multiple-host configurations. Any server that is certified for use with SAP HANA can be combined with NetApp certified storage solutions. The following figure shows an architecture overview.



For more information regarding the prerequisites and recommendations for productive SAP HANA systems, see the following resources:

- SAP HANA Tailored Data Center Integration Frequently Asked Questions
- SAP HANA Storage Requirements

SAP HANA using VMware vSphere

Raw device mappings (RDM), FCP datastores, or VVOL datastores with FCP are supported as well. For both datastore options, only one SAP HANA data or log volume must be stored within the datastore for productive use cases. In addition, Snapshot- based backup and recovery orchestrated by SnapCenter and solutions based on this, such as SAP System cloning, cannot be implemented.

For more information about using vSphere with SAP HANA, see the following links:

- SAP HANA on VMware vSphere - Virtualization - Community Wiki
- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere
- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere
- 2161991 - VMware vSphere configuration guidelines - SAP ONE Support Launchpad (Login required)

Next: Architecture.

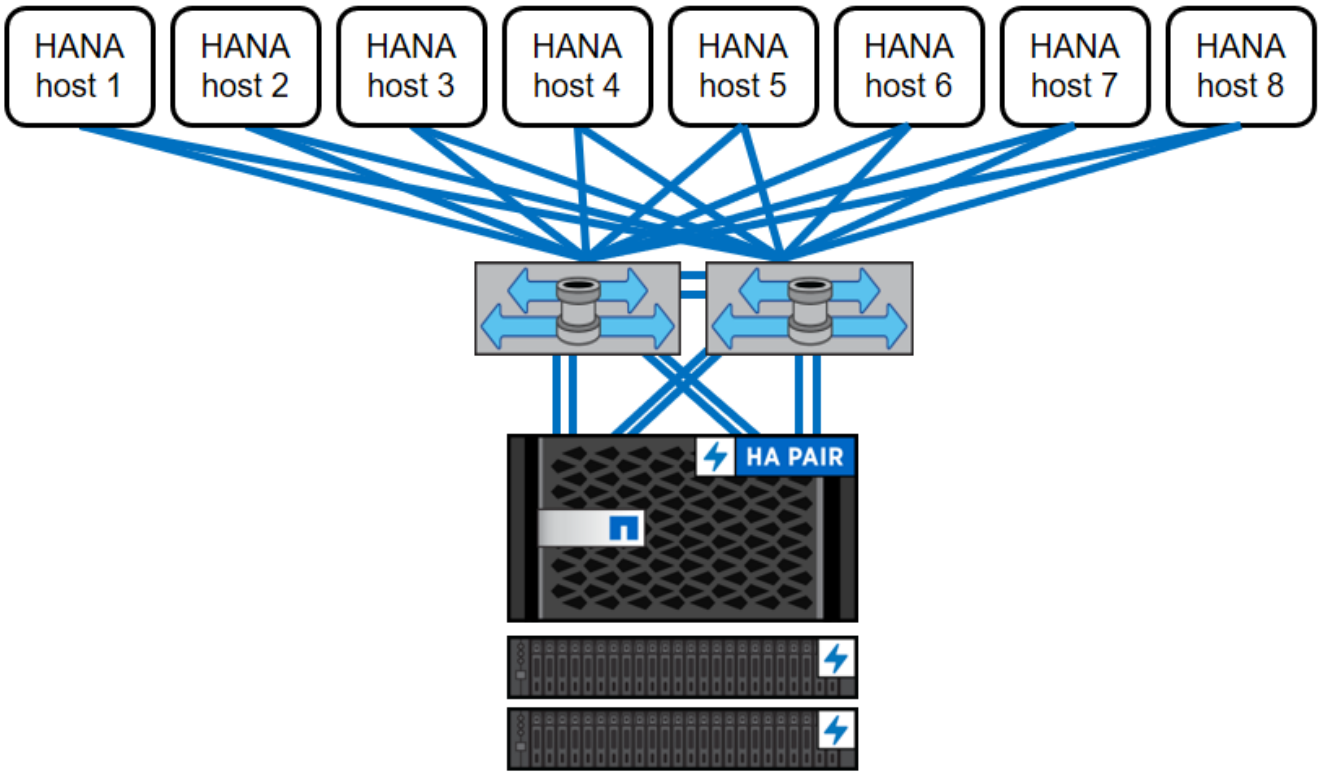
Architecture

Previous: TR-4436 - SAP HANA on NetApp AFF Systems with Fibre Channel Protocol.

SAP HANA hosts are connected to storage controllers using a redundant FCP infrastructure and multipath software. A redundant FCP switch infrastructure is required to provide fault-tolerant SAP HANA host-to-storage connectivity in case of switch or host bus adapter (HBA) failure. Appropriate zoning must be configured at the switch to allow all HANA hosts to reach the required LUNs on the storage controllers.

Different models of the AFF system product family can be mixed and matched at the storage layer to allow for growth and differing performance and capacity needs. The maximum number of SAP HANA hosts that can be attached to the storage system is defined by the SAP HANA performance requirements and the model of NetApp controller used. The number of required disk shelves is only determined by the capacity and performance requirements of the SAP HANA systems.

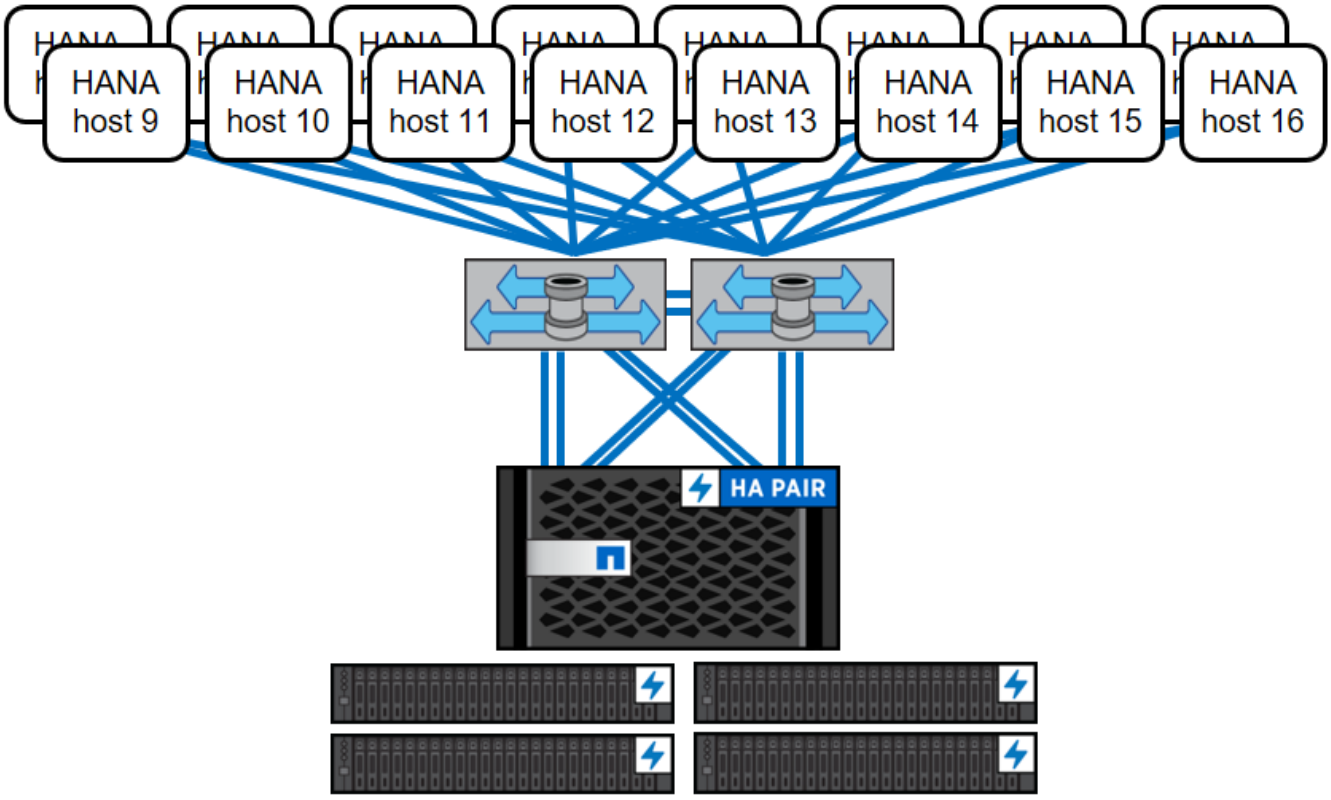
The following figure shows an example configuration with eight SAP HANA hosts attached to a storage HA pair.



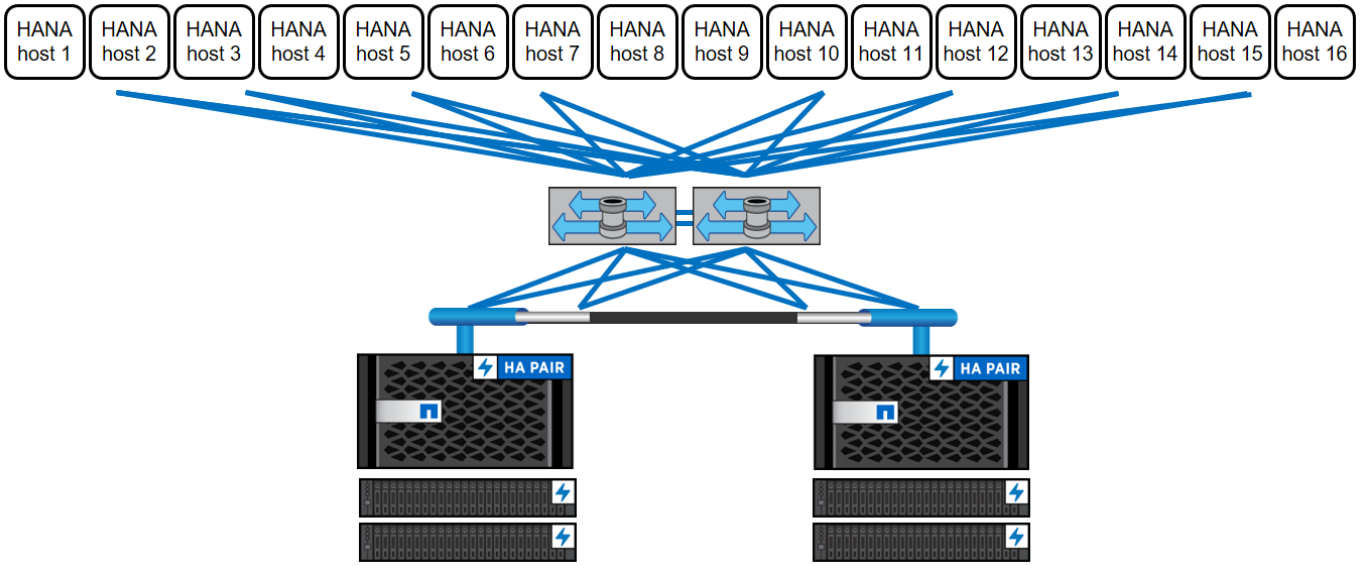
This architecture can be scaled in two dimensions:

- By attaching additional SAP HANA hosts and storage capacity to the existing storage, if the storage controllers provide enough performance to meet the current SAP HANA KPIs
- By adding more storage systems with additional storage capacity for the additional SAP HANA hosts

The following figure shows a configuration example in which more SAP HANA hosts are attached to the storage controllers. In this example, more disk shelves are necessary to meet the capacity and performance requirements of the 16 SAP HANA hosts. Depending on the total throughput requirements, you must add additional FC connections to the storage controllers.



Independent of the deployed AFF system, the SAP HANA landscape can also be scaled by adding any certified storage controllers to meet the desired node density, as shown in the following figure.



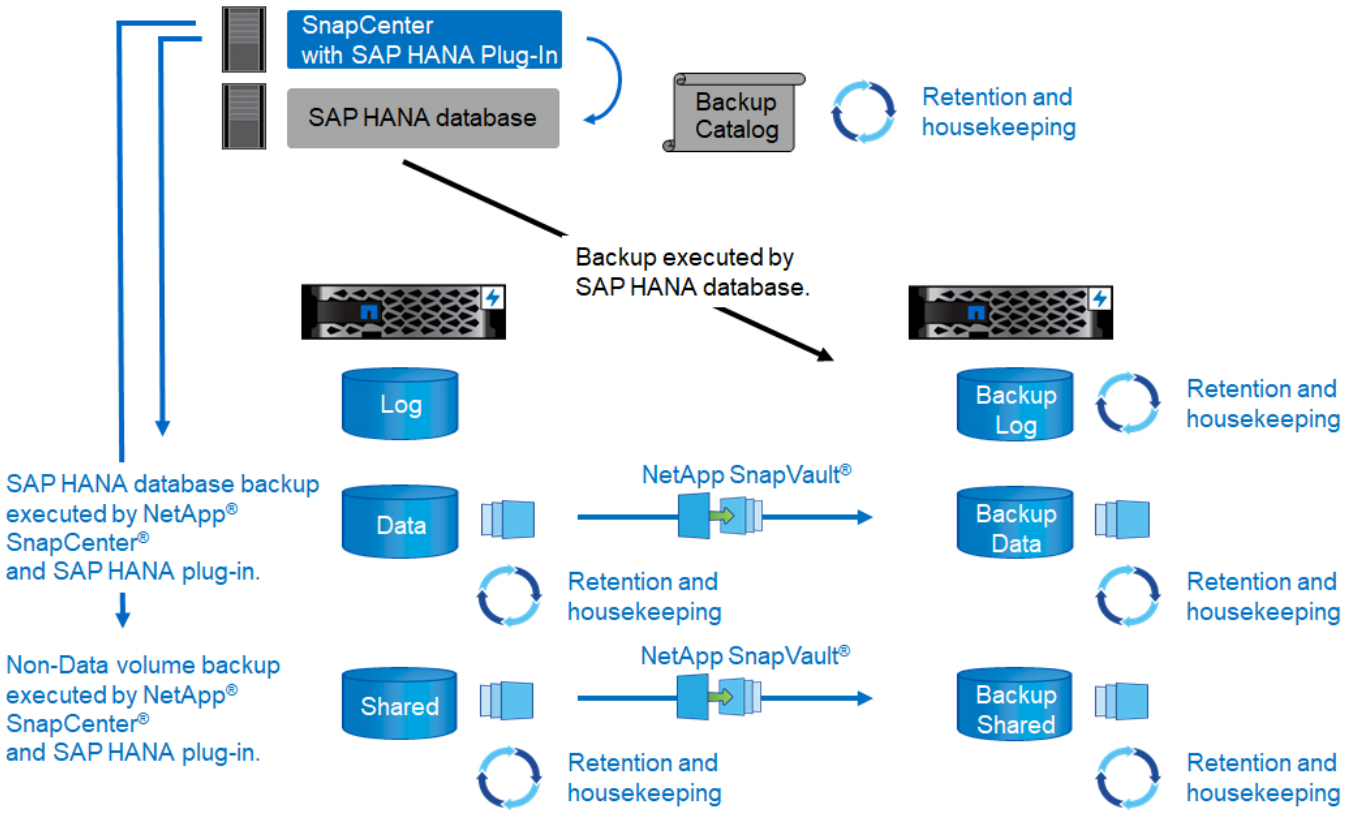
SAP HANA backup

The ONTAP software present on all NetApp storage controllers provides a built-in mechanism to back up SAP HANA databases while in operation with no effect on performance. Storage-based NetApp Snapshot backups are a fully supported and integrated backup solution available for SAP HANA single containers and for SAP HANA MDC systems with a single tenant or multiple tenants.

Storage-based Snapshot backups are implemented by using the NetApp SnapCenter plug-in for SAP HANA. This allows users to create consistent storage-based Snapshot backups by using the interfaces provided natively by SAP HANA databases. SnapCenter registers each of the Snapshot backups into the SAP HANA backup catalog. Therefore, backups taken by SnapCenter are visible within SAP HANA Studio or Cockpit where they can be selected directly for restore and recovery operations.

NetApp SnapMirror technology allows for Snapshot copies that were created on one storage system to be replicated to a secondary backup storage system that is controlled by SnapCenter. Different backup retention policies can then be defined for each of the backup sets on the primary storage and also for the backup sets on the secondary storage systems. The SnapCenter Plug-in for SAP HANA automatically manages the retention of Snapshot copy-based data backups and log backups, including the housekeeping of the backup catalog. The SnapCenter Plug-in for SAP HANA also allows for the execution of a block integrity check of the SAP HANA database by executing a file-based backup.

The database logs can be backed up directly to the secondary storage by using an NFS mount, as shown in the following figure.



Storage-based Snapshot backups provide significant advantages compared to conventional file-based backups. These advantages include, but are not limited to the following:

- Faster backup (a few minutes)
- Reduced RTO due to a much faster restore time on the storage layer (a few minutes) as well as more frequent backups
- No performance degradation of the SAP HANA database host, network, or storage during backup and recovery operations
- Space-efficient and bandwidth-efficient replication to secondary storage based on block changes

For detailed information about the SAP HANA backup and recovery solution, see TR-4614: SAP HANA Backup and Recovery with SnapCenter.

SAP HANA disaster recovery

SAP HANA disaster recovery can be done either on the database layer by using SAP HANA system replication or on the storage layer by using storage replication technologies. The following section provides an overview of disaster recovery solutions based on storage replication.

For detailed information about the SAP HANA disaster recovery solutions, see TR-4646: SAP HANA Disaster Recovery with Storage Replication.

Storage replication based on SnapMirror

The following figure shows a three-site disaster recovery solution using synchronous SnapMirror replication to the local DR datacenter and asynchronous SnapMirror to replicate the data to the remote DR datacenter.

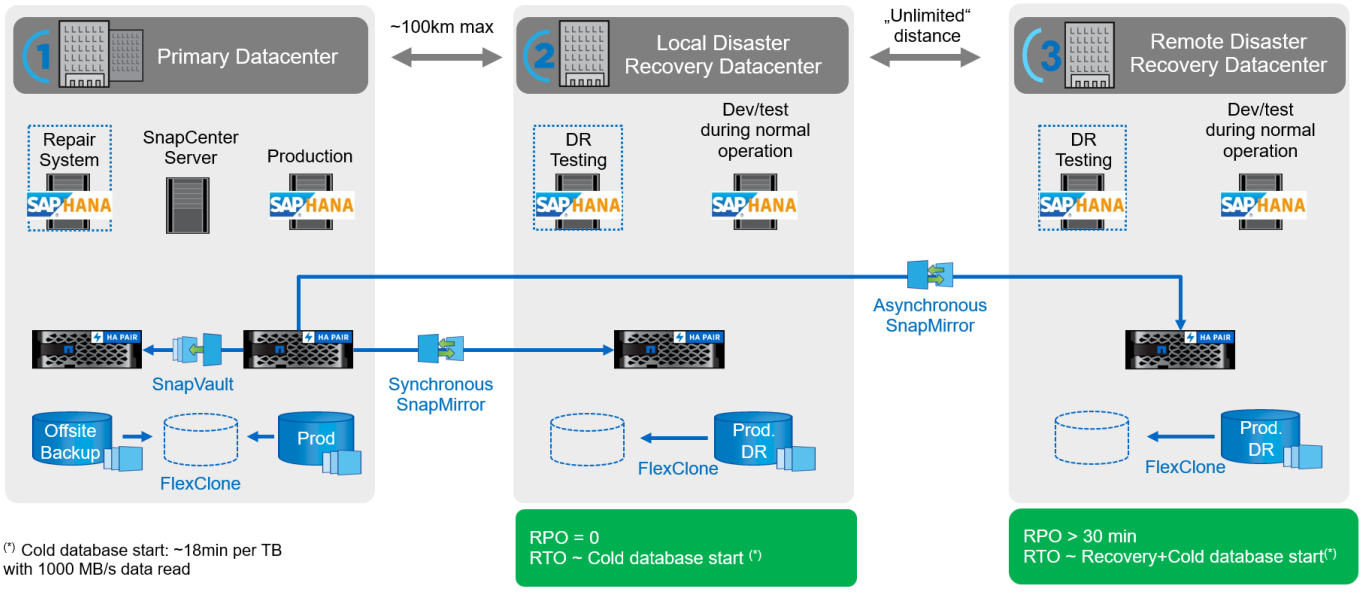
Data replication using synchronous SnapMirror provides an RPO of zero. The distance between the primary and the local DR datacenter is limited to around 100km.

Protection against failures of both the primary and the local DR site is performed by replicating the data to a third remote DR datacenter using asynchronous SnapMirror. The RPO depends on the frequency of replication updates and how fast they can be transferred. In theory, the distance is unlimited, but the limit depends on the amount of data that must be transferred and the connection that is available between the data centers. Typical RPO values are in the range of 30 minutes to multiple hours.

The RTO for both replication methods primarily depends on the time needed to start the HANA database at the DR site and load the data into memory. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data would take approximately 18 minutes.

The servers at the DR sites can be used as dev/test systems during normal operation. In the case of a disaster, the dev/test systems would need to be shut down and started as DR production servers.

Both replication methods allow to you execute DR workflow testing without influencing the RPO and RTO. FlexClone volumes are created on the storage and are attached to the DR testing servers.

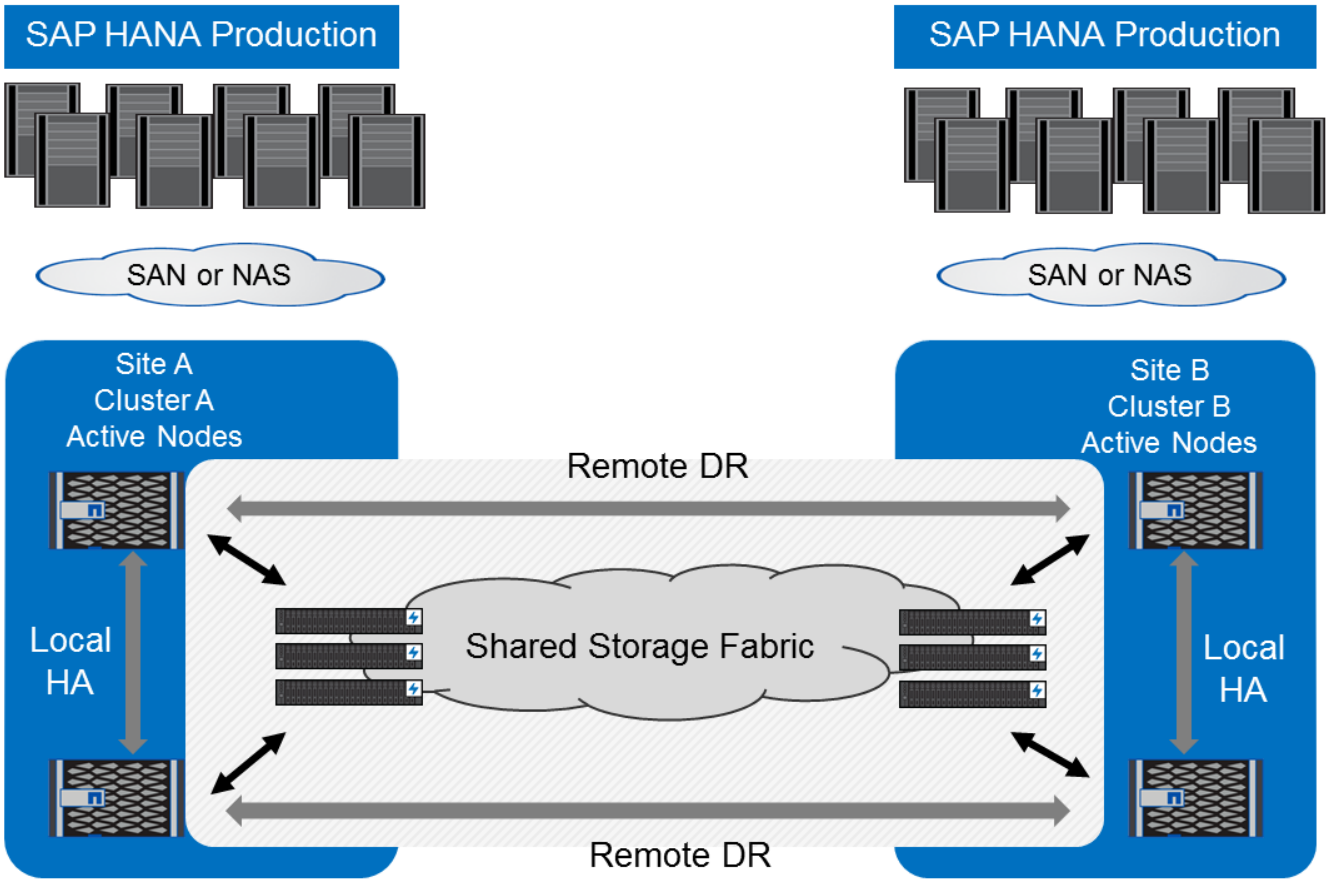


Synchronous replication offers StrictSync mode. If the write to secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage systems are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the InSync status. If the primary storage fails, application I/O can be resumed on the secondary storage after failover with

no loss of data. In StrictSync mode, the RPO is always zero.

Storage replication based on NetApp MetroCluster

The following figure shows a high-level overview of the solution. The storage cluster at each site provides local high availability and is used for the production workload. The data of each site is synchronously replicated to the other location and is available in case of disaster failover.



Next: Storage sizing.

Storage sizing

Previous: Architecture.

The following section provides an overview of performance and capacity considerations required for sizing a storage system for SAP HANA.

> Contact your NetApp or NetApp partner sales representative to support the storage sizing process and to assist you with creating a properly sized storage environment.

Performance considerations

SAP has defined a static set of storage key performance indicators (KPIs). These KPIs are valid for all production SAP HANA environments independent of the memory size of the database hosts and the applications that use the SAP HANA database. These KPIs are valid for single-host, multiple-host, Business Suite on HANA, Business Warehouse on HANA, S/4HANA, and BW/4HANA environments. Therefore, the current performance sizing approach depends on only the number of active SAP HANA hosts that are attached

to the storage system.

Storage performance KPIs are only mandated for production SAP HANA systems, but you can implement them in for all HANA system.

SAP delivers a performance test tool which must be used to validate the storage systems performance for active SAP HANA hosts attached to the storage.

NetApp tested and predefined the maximum number of SAP HANA hosts that can be attached to a specific storage model, while still fulfilling the required storage KPIs from SAP for production-based SAP HANA systems.

The maximum number of SAP HANA hosts that can be run on a disk shelf and the minimum number of SSDs required per SAP HANA host were determined by running the SAP performance test tool. This test does not consider the actual storage capacity requirements of the hosts. You must also calculate the capacity requirements to determine the actual storage configuration needed.

SAS disk shelf

With the 12Gb SAS disk shelf (DS224C), the performance sizing is performed by using fixed disk- shelf configurations:

- Half-loaded disk shelves with 12 SSDs
- Fully loaded disk shelves with 24 SSDs

Both configurations use advanced drive partitioning (ADPv2). A half-loaded disk shelf supports up to 9 SAP HANA hosts; a fully loaded shelf supports up to 14 hosts in a single disk shelf. The SAP HANA hosts must be equally distributed between both storage controllers.

The DS224C disk shelf must be connected by using 12Gb SAS to support the number of SAP HANA hosts.

The 6Gb SAS disk shelf (DS2246) supports a maximum of 4 SAP HANA hosts. The SSDs and the SAP HANA hosts must be equally distributed between both storage controllers. The following figure summarizes the supported number of SAP HANA hosts per disk shelf.

	6Gb SAS shelves (DS2246)Fully loaded with 24 SSDs	**12Gb SAS shelves (DS224C)Half-loaded with 12 SSDs and ADPv2**	**12Gb SAS shelves (DS224C)Fully loaded with 24 SSDs and ADPv2**
Maximum number of SAP HANA hosts per disk shelf	4	9	14

This calculation is independent of the storage controller used. Adding more disk shelves does not increase the maximum number of SAP HANA hosts that a storage controller can support.

NS224 NVMe shelf

The minimum number of 12 NVMe SSDs for the first shelf supports up to 16 SAP HANA hosts. A fully populated shelf supports up to 34 SAP HANA hosts.

Adding more disk shelves does not increase the maximum number of SAP HANA hosts that a storage controller can support.

Mixed workloads

SAP HANA and other application workloads running on the same storage controller or in the same storage aggregate are supported. However, it is a NetApp best practice to separate SAP HANA workloads from all other application workloads.

You might decide to deploy SAP HANA workloads and other application workloads on either the same storage controller or the same aggregate. If so, you must make sure that adequate performance is available for SAP HANA within the mixed workload environment. NetApp also recommends that you use quality of service (QoS) parameters to regulate the effect these other applications could have on SAP HANA applications and to guarantee throughput for SAP HANA applications.

The SAP HCMT test tool must be used to check if additional SAP HANA hosts can be run on an existing storage controller that is already in use for other workloads. SAP application servers can be safely placed on the same storage controller and/or aggregate as the SAP HANA databases.

Capacity considerations

A detailed description of the capacity requirements for SAP HANA is in the SAP HANA Storage Requirements white paper.

The capacity sizing of the overall SAP landscape with multiple SAP HANA systems must be determined by using SAP HANA storage sizing tools from NetApp. Contact NetApp or your NetApp partner sales representative to validate the storage sizing process for a properly sized storage environment.

Configuration of performance test tool

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage system used. These parameters must also be set for the performance test tool from SAP when the storage performance is being tested with the SAP test tool.

NetApp conducted performance tests to define the optimal values. The following table lists the parameters that must be set within the configuration file of the SAP test tool.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on
async_write_submit_blocks	all

For more information about the configuration of SAP test tool, see SAP note 1943937 for HWCCT (SAP HANA 1.0) and SAP note 2493172 for HCMT/HCOT (SAP HANA 2.0).

The following example shows how variables can be set for the HCMT/HCOT execution plan.

```
... {
```

```
         "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "LogAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
```

```
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

These variables must be used for the test configuration. This is usually the case with the predefined execution plans SAP delivers with the HCMT/HCOT tool. The following example for a 4k log write test is from an execution plan.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

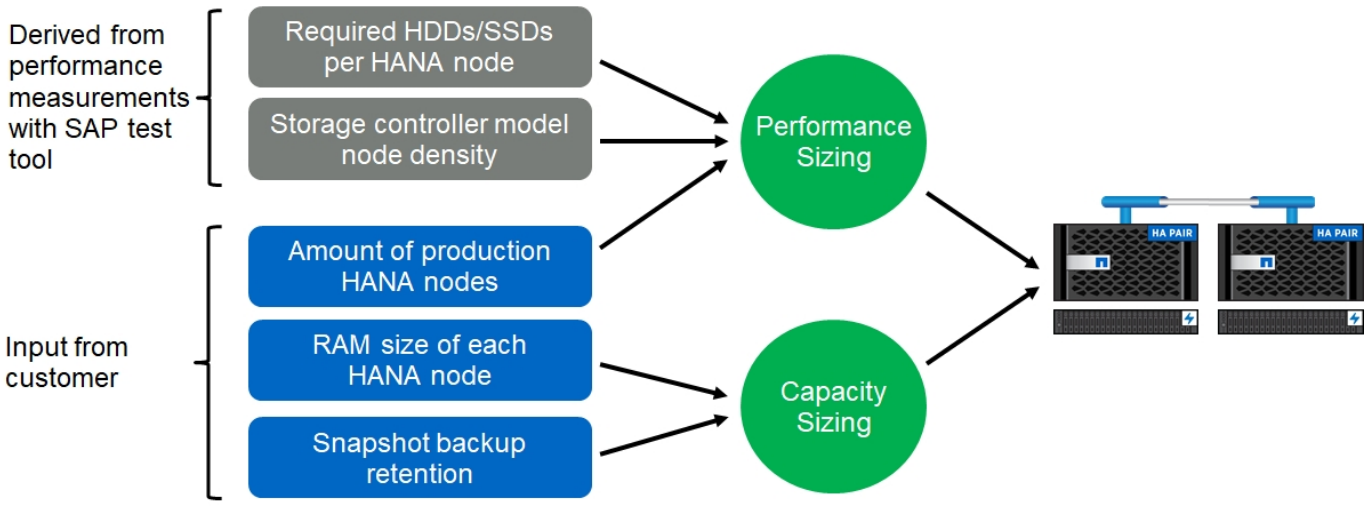
Storage sizing process overview

The number of disks per HANA host and the SAP HANA host density for each storage model were determined using the SAP HANA test tool.

The sizing process requires details such as the number of production and nonproduction SAP HANA hosts, the RAM size of each host, and the backup retention of the storage-based Snapshot copies. The number of SAP HANA hosts determines the storage controller and the number of disks required.

The size of the RAM, net data size on the disk of each SAP HANA host, and the Snapshot copy backup retention period are used as inputs during capacity sizing.

The following figure summarizes the sizing process.



Next: Infrastructure setup and configuration.

Infrastructure setup and configuration

Previous: Storage sizing.

The following sections provide SAP HANA infrastructure setup and configuration guidelines and describes all the steps needed to set up an SAP HANA system. Within these sections, the following example configurations are used:

- HANA system with SID=SS3 and ONTAP 9.7 or earlier
  - SAP HANA single and multiple host
  - SAP HANA single host using SAP HANA multiple partitions
- HANA system with SID=FC5 and ONTAP 9.8 using Linux logical volume manager (LVM)
  - SAP HANA single and multiple host

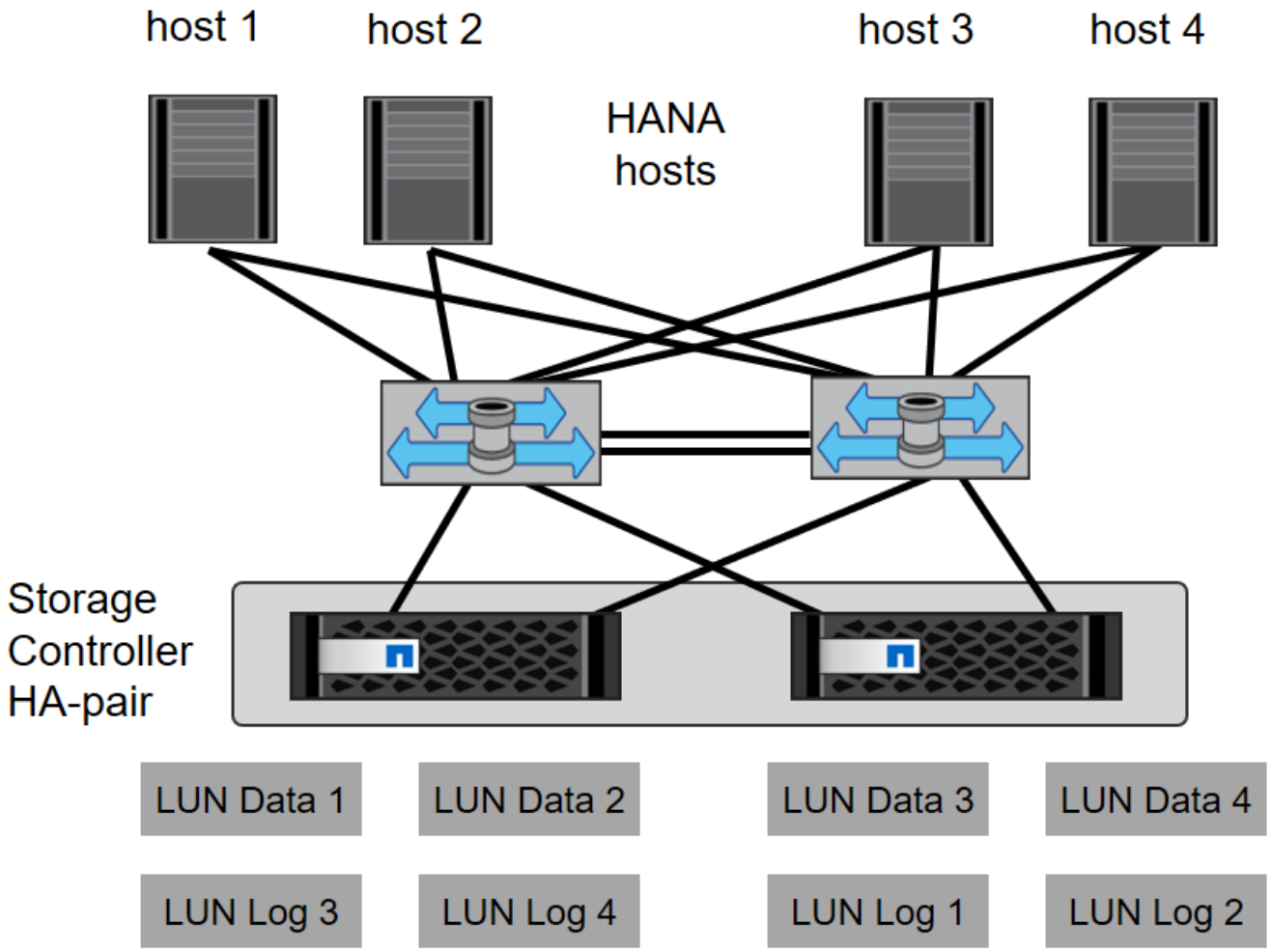
Next: SAN fabric setup.

SAN fabric setup

Previous: Infrastructure setup and configuration.

Each SAP HANA server must have a redundant FCP SAN connection with a minimum of 8Gbps bandwidth. For each SAP HANA host attached to a storage controller, at least 8Gbps bandwidth must be configured at the storage controller.

The following figure shows an example with four SAP HANA hosts attached to two storage controllers. Each SAP HANA host has two FCP ports connected to the redundant fabric. At the storage layer, four FCP ports are configured to provide the required throughput for each SAP HANA host.



In addition to the zoning on the switch layer, you must map each LUN on the storage system to the hosts that connect to this LUN. Keep the zoning on the switch simple; that is, define one zone set in which all host HBAs can see all controller HBAs.

Next: Time synchronization.

Time synchronization

Previous: SAN fabric setup.

You must synchronize the time between the storage controllers and the SAP HANA database hosts. To do so, set the same time server for all storage controllers and all SAP HANA hosts.

Next: Storage controller setup.

Storage controller setup

Previous: Time synchronization.

This section describes the configuration of the NetApp storage system. You must complete the primary installation and setup according to the corresponding Data ONTAP setup and configuration guides.

Storage efficiency

Inline deduplication, cross-volume inline deduplication, inline compression, and inline compaction are supported with SAP HANA in an SSD configuration.

NetApp Volume Encryption

The use of NetApp Volume Encryption (NVE) is supported with SAP HANA.

Quality of service

QoS can be used to limit the storage throughput for specific SAP HANA systems or no- SAP applications on a shared-use controller. One use case would be to limit the throughput of development and test systems so that they cannot influence production systems in a mixed setup.

During the sizing process, you should determine the performance requirements of a nonproduction system. Development and test systems can be sized with lower performance values, typically in the range of 20% to 50% of a production-system KPI as defined by SAP.

Starting with ONTAP 9, QoS is configured on the storage volume level and uses maximum values for throughput (MBps) and the amount of I/O (IOPS).

Large write I/O has the biggest performance effect on the storage system. Therefore, the QoS throughput limit should be set to a percentage of the corresponding write SAP HANA storage performance KPI values in the data and log volumes.

NetApp FabricPool

NetApp FabricPool technology must not be used for active primary file systems in SAP HANA systems. This includes the file systems for the data and log area as well as the `/hana/shared` file system. Doing so results in unpredictable performance, especially during the startup of an SAP HANA system.

You can use the Snapshot-Only tiering policy along with FabricPool at a backup target such as SnapVault or SnapMirror destination.

Using FabricPool for tiering Snapshot copies at primary storage or using FabricPool at a backup target changes the required time for the restore and recovery of a database or other tasks such as creating system clones or repair systems. Take this into consideration for planning your overall lifecycle-management strategy, and check to make sure that your SLAs are still being met while using this function.

FabricPool is a good option for moving log backups to another storage tier. Moving backups affects the time needed to recover an SAP HANA database. Therefore, the option `tiering-minimum-cooling-days` should be set to a value that places log backups, which are routinely needed for recovery, on the local fast storage tier.

Configure storage

The following overview summarizes the required storage configuration steps. Each step is covered in more detail in the subsequent sections. In this section, we assume that the storage hardware is set up and that the ONTAP software is already installed. Also, the connection of the storage FCP ports to the SAN fabric must already be in place.

1. Check the correct disk shelf configuration, as described in "Disk shelf connection."

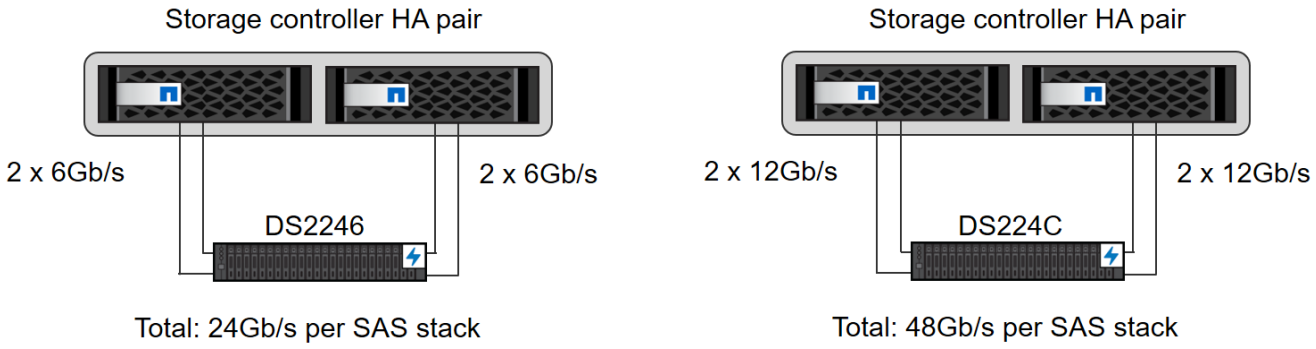
2. Create and configure the required aggregates, as described in "Aggregate configuration."
3. Create a storage virtual machine (SVM), as described in "Storage virtual machine configuration."
4. Create logical interfaces (LIFs), as described in "Logical interface configuration."
5. Create a port set, as described in "FCP port sets."
6. Create initiator groups, volumes, and LUNs within the aggregates, as described in creating "[LUNs and volumes and mapping LUNs to initiator groups]."

Disk shelf connection

SAS-based disk shelves

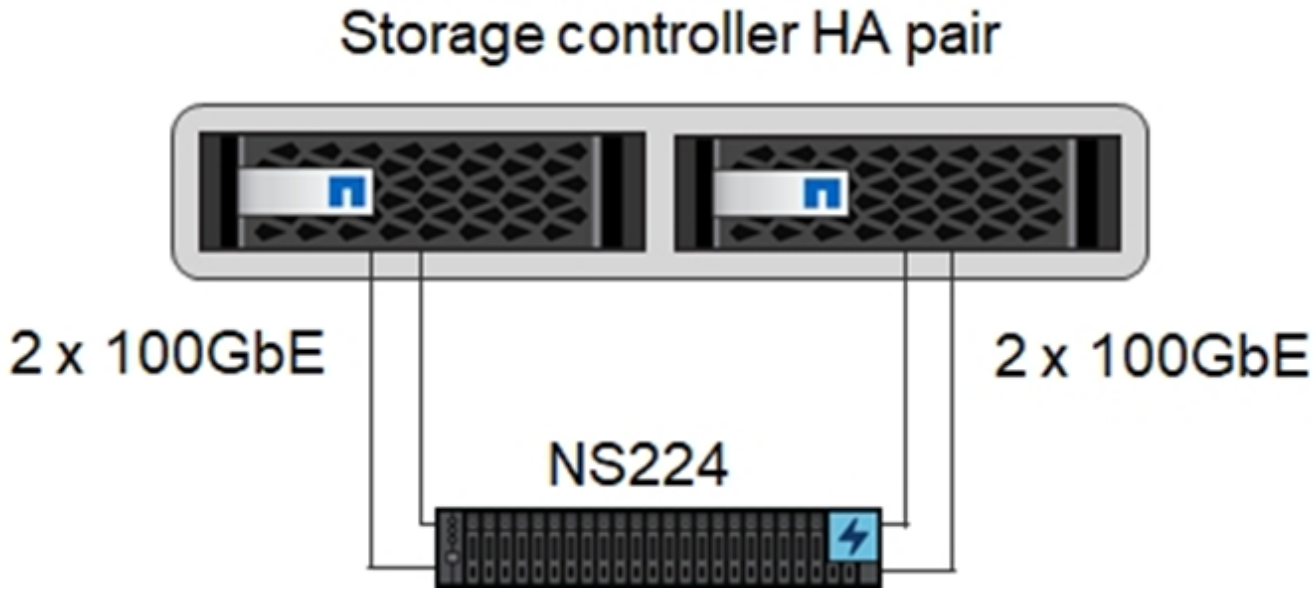
A maximum of one disk shelf can be connected to one SAS stack to provide the required performance for the SAP HANA hosts, as shown in the following figure. The disks within each shelf must be distributed equally between both controllers of the HA pair. ADPv2 is used with ONTAP 9 and the new DS224C disk shelves.

With the DS224C disk shelf, quad-path SAS cabling can also be used but is not required.



NVMe(100GbE)-based disk shelves

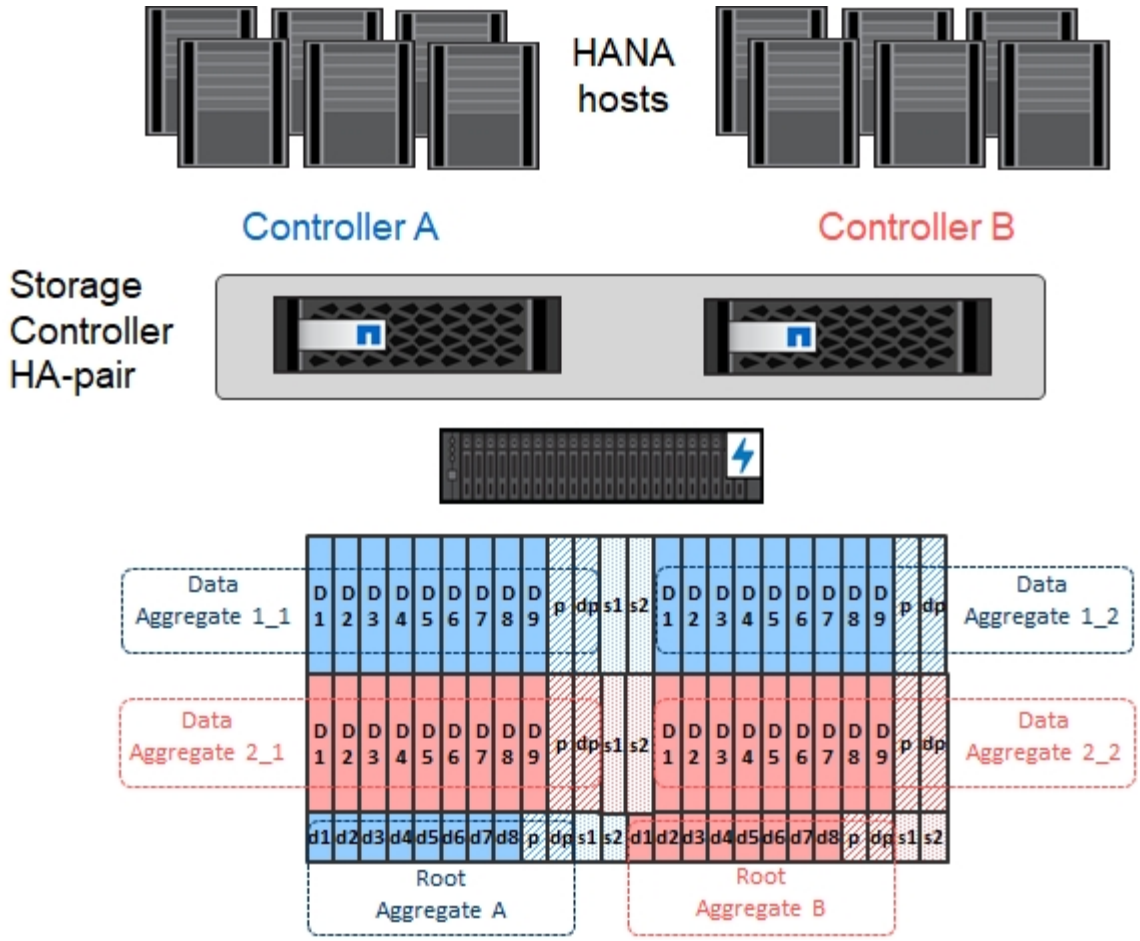
Each NS224 NVMe desk shelf is connected with two 100GbE ports per controller, as shown in the following figure. The disks within each shelf must be distributed equally to both controllers of the HA pair. ADPv2 is also used for the NS224 disk shelf.



Aggregate configuration

In general, you must configure two aggregates per controller, independent of which disk shelf or disk technology (SSD or HDD) is used. This step is necessary so that you can use all available controller resources. For AFF A200 series systems, one data aggregate is sufficient.

The following figure shows a configuration of 12 SAP HANA hosts running on a 12Gb SAS shelf configured with ADPv2. Six SAP HANA hosts are attached to each storage controller. Four separate aggregates, two at each storage controller, are configured. Each aggregate is configured with 11 disks with nine data and two parity disk partitions. For each controller, two spare partitions are available.



Storage virtual machine configuration

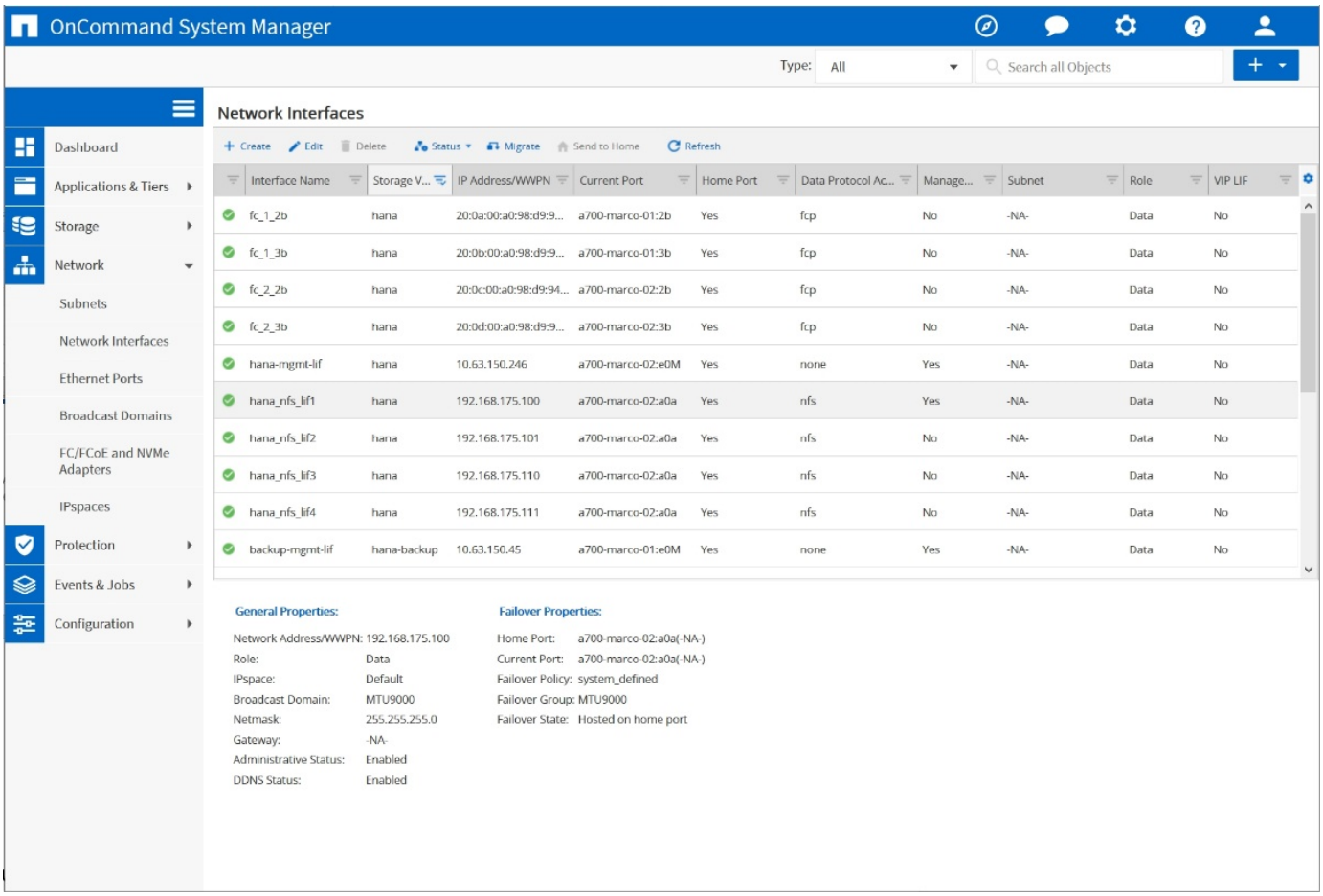
Multiple SAP landscapes with SAP HANA databases can use a single SVM. An SVM can also be assigned to each SAP landscape, if necessary, in case they are managed by different teams within a company.

If there is a QoS profile automatically created and assigned while creating a new SVM, remove this automatically created profile from the SVM to ensure the required performance for SAP HANA:

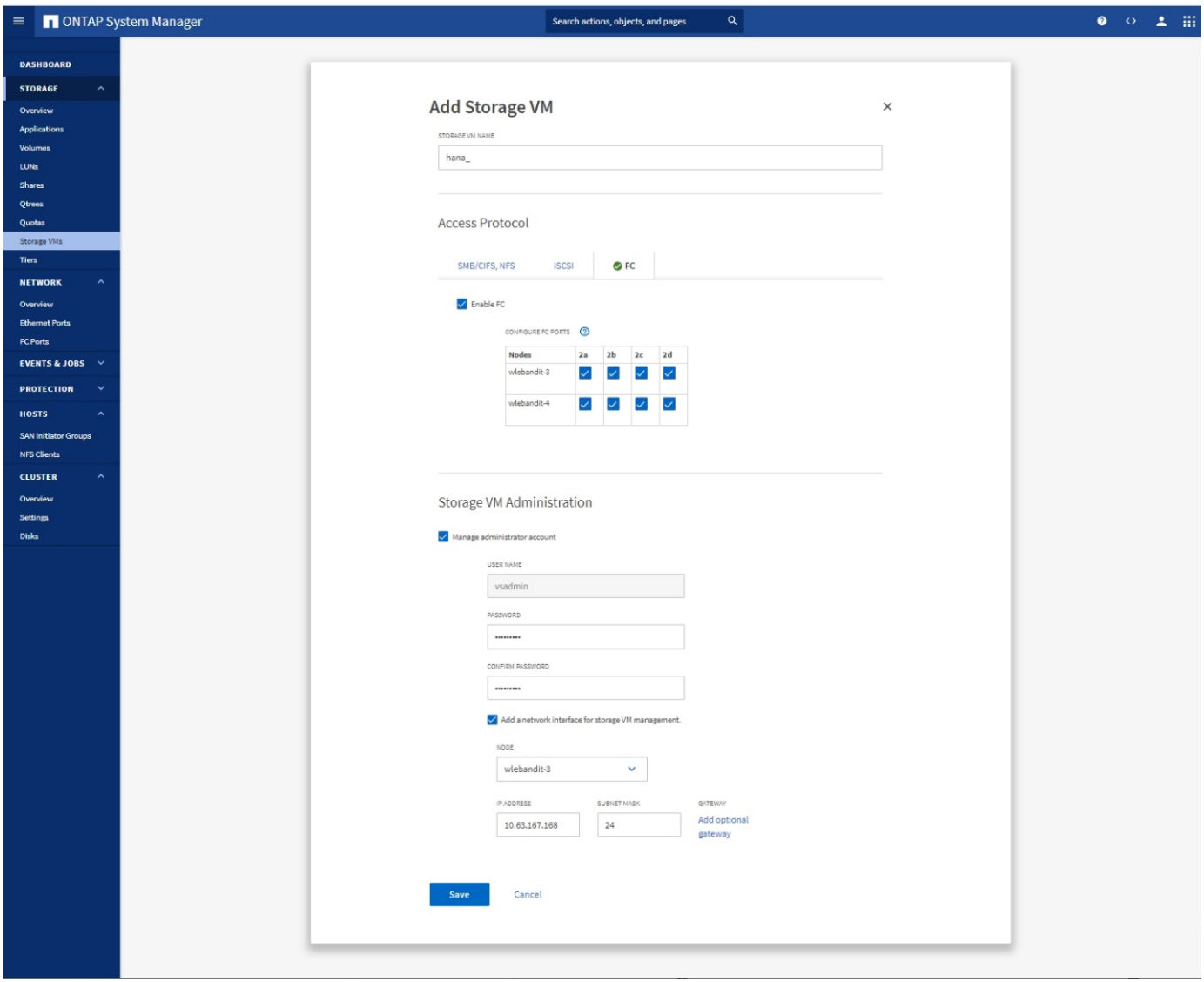
```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Logical interface configuration

Within the storage cluster configuration, one network interface (LIF) must be created and assigned to a dedicated FCP port. If, for example, four FCP ports are required for performance reasons, four LIFs must be created. The following figure shows a screenshot of the eight LIFs (named `fc_*_*`) that were configured on the `hana` SVM.

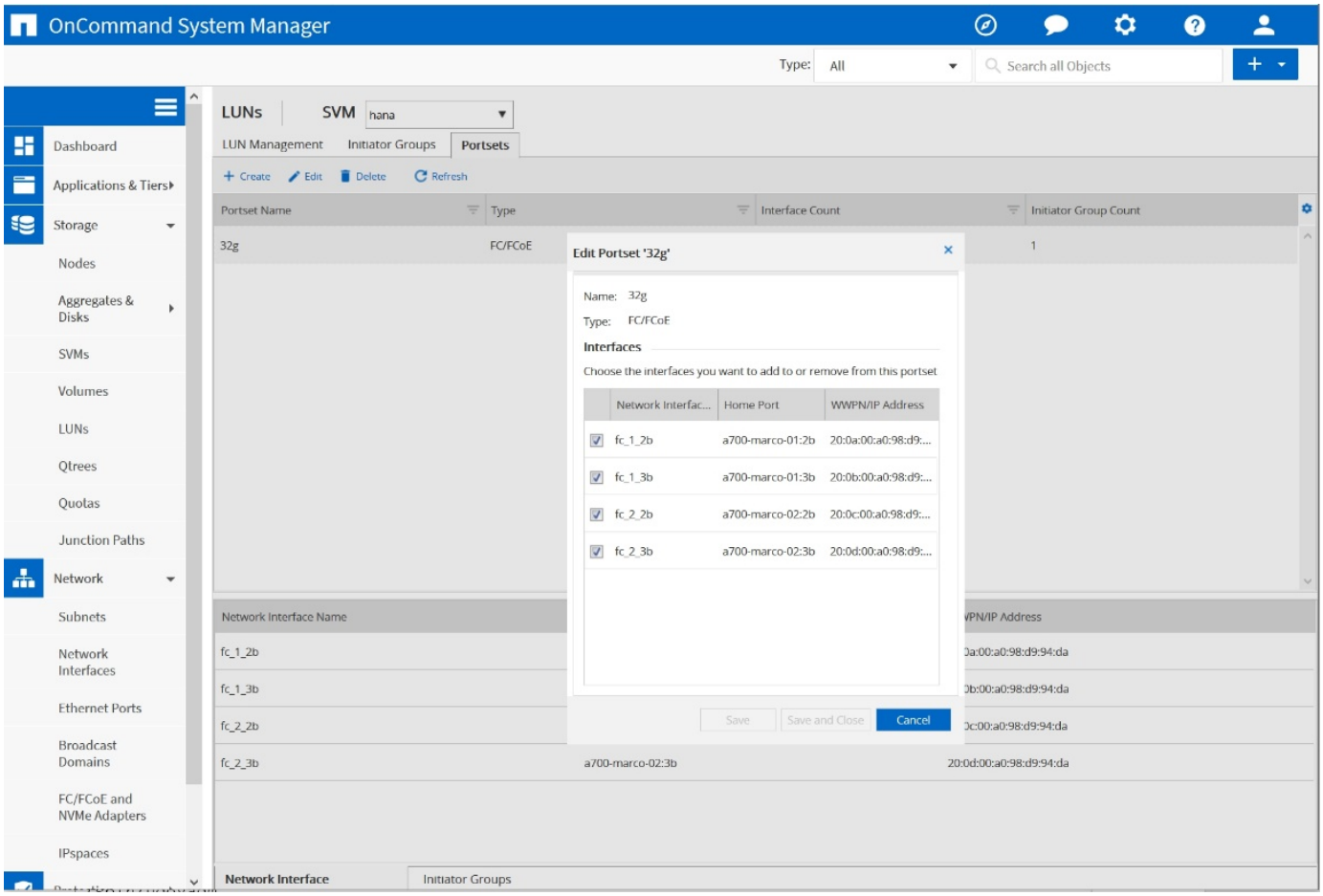


During the SVM creation with ONTAP 9.8 System Manager, you can select all of the required physical FCP ports, and one LIF per physical port is created automatically.



FCP port sets

An FCP port set is used to define which LIFs are to be used by a specific initiator group. Typically, all LIFs created for the HANA systems are placed in the same port set. The following figure shows the configuration of a port set named 32g that includes the four LIFs that were already created.

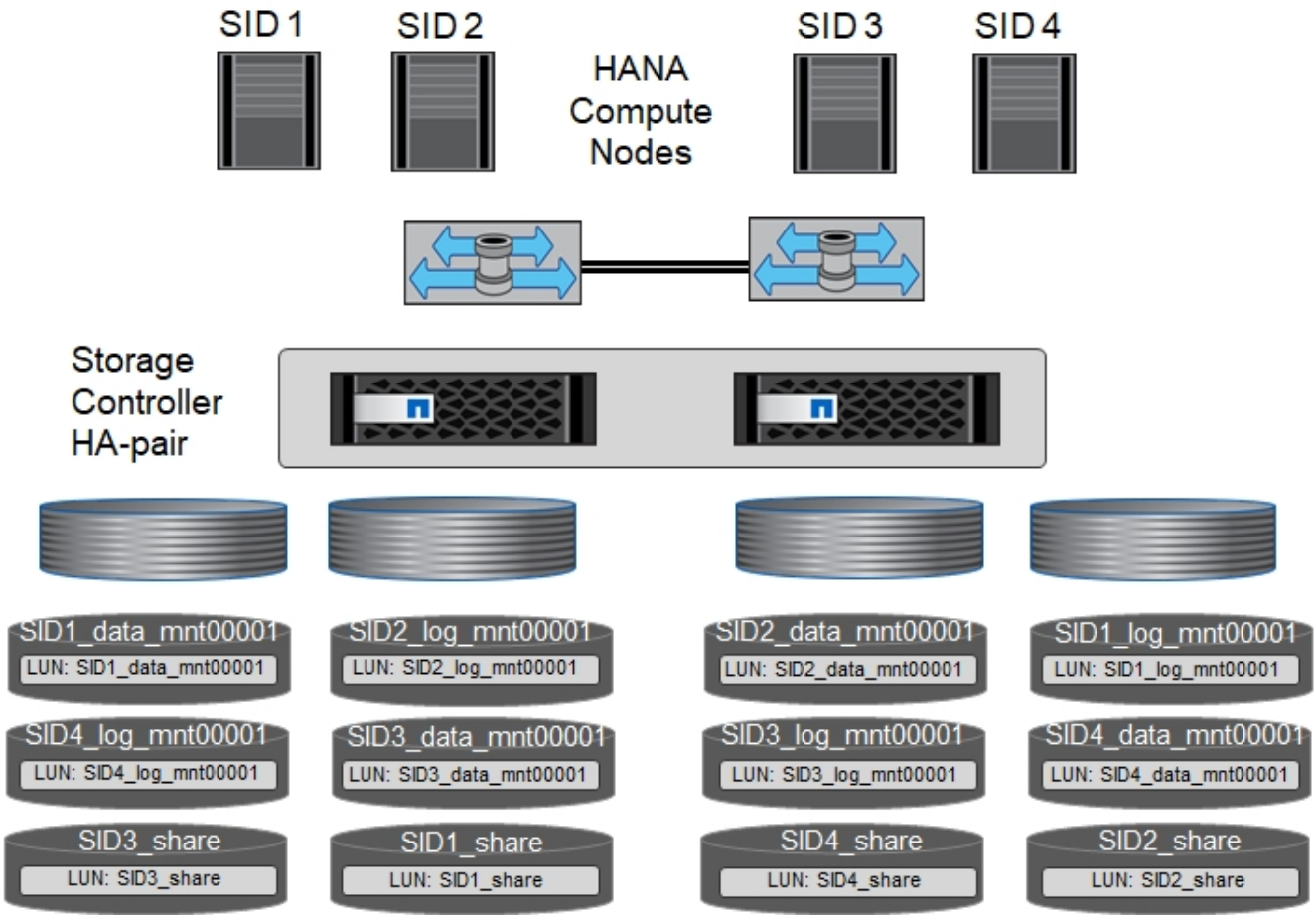


With ONTAP 9.8, a port set is not required, but it can be created and used through the command line.

Volume and LUN configuration for SAP HANA single-host systems

The following figure shows the volume configuration of four single-host SAP HANA systems. The data and log volumes of each SAP HANA system are distributed to different storage controllers. For example, volume `SID1_data_mnt00001` is configured on controller A, and volume `SID1_log_mnt00001` is configured on controller B. Within each volume, a single LUN is configured.

If only one storage controller of a HA pair is used for the SAP HANA systems, data volumes and log volumes can also be stored on the same storage controller.



For each SAP HANA host, a data volume, a log volume, and a volume for `/hana/shared` are configured. The following table shows an example configuration with four SAP HANA single-host systems.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data, log, and shared volumes for system SID1	Data volume: SID1_data_mnt00001	Shared volume: SID1_shared	–	Log volume: SID1_log_mnt00001
Data, log, and shared volumes for system SID2	–	Log volume: SID2_log_mnt00001	Data volume: SID2_data_mnt00001	Shared volume: SID2_shared
Data, log, and shared volumes for system SID3	Shared volume: SID3_shared	Data volume: SID3_data_mnt00001	Log volume: SID3_log_mnt00001	–
Data, log, and shared volumes for system SID4	Log volume: SID4_log_mnt00001	–	Shared volume: SID4_shared	Data volume: SID4_data_mnt00001

The following table shows an example of the mount point configuration for a single-host system.

LUN	Mount point at SAP HANA host	Note
SID1_data_mnt00001	/hana/data/SID1/mnt00001	Mounted using /etc/fstab entry

LUN	Mount point at SAP HANA host	Note
SID1_log_mnt00001	/hana/log/SID1/mnt00001	Mounted using /etc/fstab entry
SID1_shared	/hana/shared/SID1	Mounted using /etc/fstab entry

With the described configuration, the `/usr/sap/SID1` directory in which the default home directory of user SID1adm is stored, is on the local disk. In a disaster recovery setup with disk-based replication, NetApp recommends creating an additional LUN within the `SID1_shared` volume for the `/usr/sap/SID1` directory so that all file systems are on the central storage.

Volume and LUN configuration for SAP HANA single-host systems using Linux LVM

The Linux LVM can be used to increase performance and to address LUN size limitations. The different LUNs of an LVM volume group should be stored within a different aggregate and at a different controller. The following table shows an example for two LUNs per volume group.

It is not necessary to use LVM with multiple LUNs to fulfill the SAP HANA KPIs. A single LUN setup fulfills the required KPIs.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data, log, and shared volumes for LVM based system	Data volume: SID1_data_mnt00001	Shared volume: SID1_shared Log2 volume: SID1_log2_mnt00001	Data2 volume: SID1_data2_mnt00001	Log volume: SID1_log_mnt00001

At the SAP HANA host, volume groups and logical volumes need to be created and mounted, as indicated in the following table.

Logical volume/LUN	Mount point at SAP HANA host	Note
LV: SID1_data_mnt0000-vol	/hana/data/SID1/mnt00001	Mounted using /etc/fstab entry
LV: SID1_log_mnt00001-vol	/hana/log/SID1/mnt00001	Mounted using /etc/fstab entry
LUN: SID1_shared	/hana/shared/SID1	Mounted using /etc/fstab entry

With the described configuration, the `/usr/sap/SID1` directory in which the default home directory of user SID1adm is stored, is on the local disk. In a disaster recovery setup with disk-based replication, NetApp recommends creating an additional LUN within the `SID1_shared` volume for the `/usr/sap/SID1` directory so that all file systems are on the central storage.

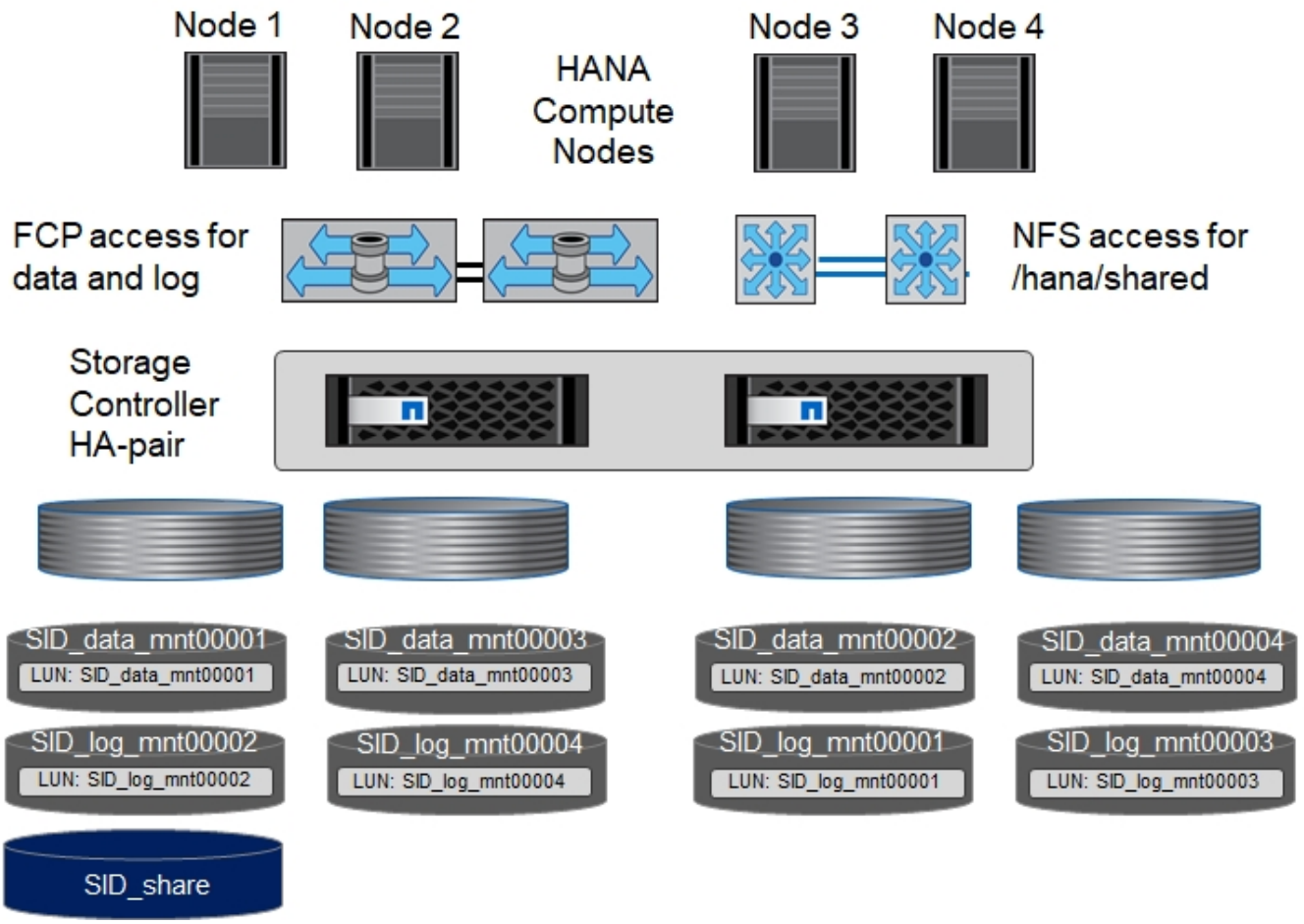
Volume and LUN configuration for SAP HANA multiple-host systems

The following figure shows the volume configuration of a 4+1 multiple-host SAP HANA system. The data volumes and log volumes of each SAP HANA host are distributed to different storage controllers. For example, the volume `SID_data_mnt00001` is configured on controller A and the volume `SID_log_mnt00001` is configured on controller B. One LUN is configured within each volume.

The `/hana/shared` volume must be accessible by all HANA hosts and is therefore exported by using NFS. Even though there are no specific performance KPIs for the `/hana/shared` file system, NetApp recommends using a 10Gb Ethernet connection.

If only one storage controller of an HA pair is used for the SAP HANA system, data and log volumes can also be stored on the same storage controller.

NetApp ASA AFF systems do not support NFS as a protocol. NetApp recommends using an additional AFF or FAS system for the `/hana/shared` file system.



For each SAP HANA host, a data volume and a log volume are created. The `/hana/shared` volume is used by all hosts of the SAP HANA system. The following table shows an example configuration for a 4+1 multiple-host SAP HANA system.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	–	Log volume: SID_log_mnt00001	–
Data and log volumes for node 2	Log volume: SID_log_mnt00002	–	Data volume: SID_data_mnt00002	–
Data and log volumes for node 3	–	Data volume: SID_data_mnt00003	–	Log volume: SID_log_mnt00003

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 4	–	Log volume: SID_log_mnt00004	–	Data volume: SID_data_mnt00004
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

The following table shows the configuration and the mount points of a multiple-host system with four active SAP HANA hosts.

LUN or volume	Mount point at SAP HANA host	Note
LUN: SID_data_mnt00001	/hana/data/SID/mnt00001	Mounted using storage connector
LUN: SID_log_mnt00001	/hana/log/SID/mnt00001	Mounted using storage connector
LUN: SID_data_mnt00002	/hana/data/SID/mnt00002	Mounted using storage connector
LUN: SID_log_mnt00002	/hana/log/SID/mnt00002	Mounted using storage connector
LUN: SID_data_mnt00003	/hana/data/SID/mnt00003	Mounted using storage connector
LUN: SID_log_mnt00003	/hana/log/SID/mnt00003	Mounted using storage connector
LUN: SID_data_mnt00004	/hana/data/SID/mnt00004	Mounted using storage connector
LUN: SID_log_mnt00004	/hana/log/SID/mnt00004	Mounted using storage connector
Volume: SID_shared	/hana/shared	Mounted at all hosts using NFS and /etc/fstab entry

With the described configuration, the `/usr/sap/SID` directory in which the default home directory of user SIDadm is stored, is on the local disk for each HANA host. In a disaster recovery setup with disk-based replication, NetApp recommends creating four additional subdirectories in the `SID_shared` volume for the `/usr/sap/SID` file system so that each database host has all its file systems on the central storage.

Volume and LUN configuration for SAP HANA multiple-host systems using Linux LVM

The Linux LVM can be used to increase performance and to address LUN size limitations. The different LUNs of an LVM volume group should be stored within a different aggregate and at a different controller.

It is not necessary to use LVM to combine several LUN to fulfill the SAP HANA KPIs. A single LUN setup fulfills the required KPIs.

The following table shows an example for two LUNs per volume group for a 2+1 SAP HANA multiple host system.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	Log2 volume: SID_log2_mnt00001	Log volume: SID_log_mnt00001	Data2 volume: SID_data2_mnt00001

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 2	Log2 volume: SID_log2_mnt00002	Data volume: SID_data_mnt00002	Data2 volume: SID_data2_mnt00002	Log volume: SID_log_mnt00002
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

At the SAP HANA host, volume groups and logical volumes need to be created and mounted, as indicated in the following table.

Logical volume (LV) or volume	Mount point at SAP HANA host	Note
LV: SID_data_mnt00001-vol	/hana/data/SID/mnt00001	Mounted using storage connector
LV: SID_log_mnt00001-vol	/hana/log/SID/mnt00001	Mounted using storage connector
LV: SID_data_mnt00002-vol	/hana/data/SID/mnt00002	Mounted using storage connector
LV: SID_log_mnt00002-vol	/hana/log/SID/mnt00002	Mounted using storage connector
Volume: SID_shared	/hana/shared	Mounted at all hosts using NFS and /etc/fstab entry

With the described configuration, the `/usr/sap/SID` directory in which the default home directory of user SIDadm is stored, is on the local disk for each HANA host. In a disaster recovery setup with disk-based replication, NetApp recommends creating four additional subdirectories in the `SID_shared` volume for the `/usr/sap/SID` file system so that each database host has all its file systems on the central storage.

Volume options

The volume options listed in the following table must be verified and set on all SVMs.

Action	
Disable automatic Snapshot copies	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disable visibility of Snapshot directory	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false

Creating LUNs, volumes, and mapping LUNs to initiator groups

You can use NetApp ONTAP System Manager to create storage volumes and LUNs and map them to the servers.

NetApp offers an automated application wizard for SAP HANA within ONTAP System Manager 9.7 and earlier, which simplifies the volume and LUN provisioning process significantly. It creates and configures the volumes and LUNs automatically according to NetApp best practices for SAP HANA.

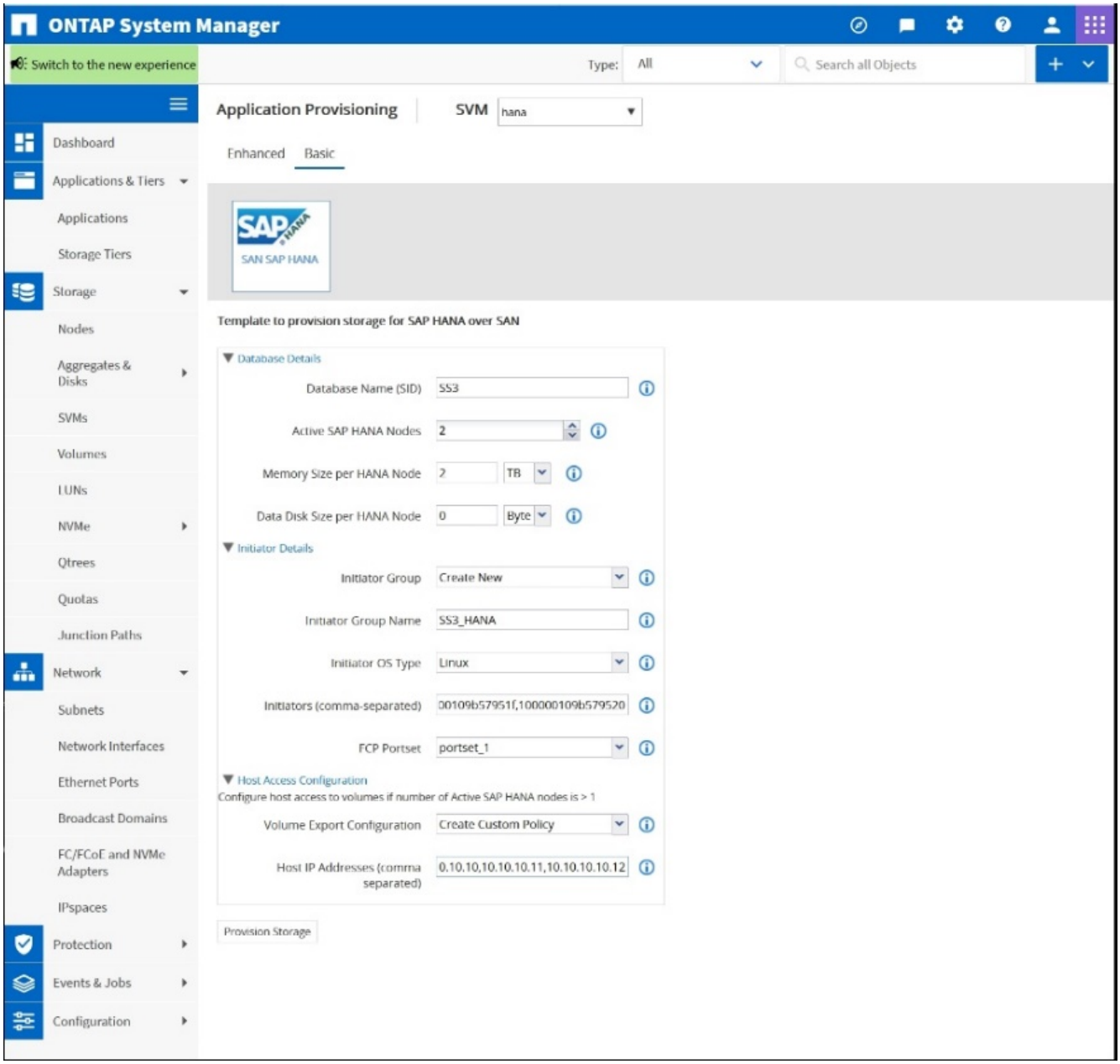
Using the `sanlun` tool, run the following command to obtain the worldwide port names (WWPNs) of each SAP HANA host:

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm
host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

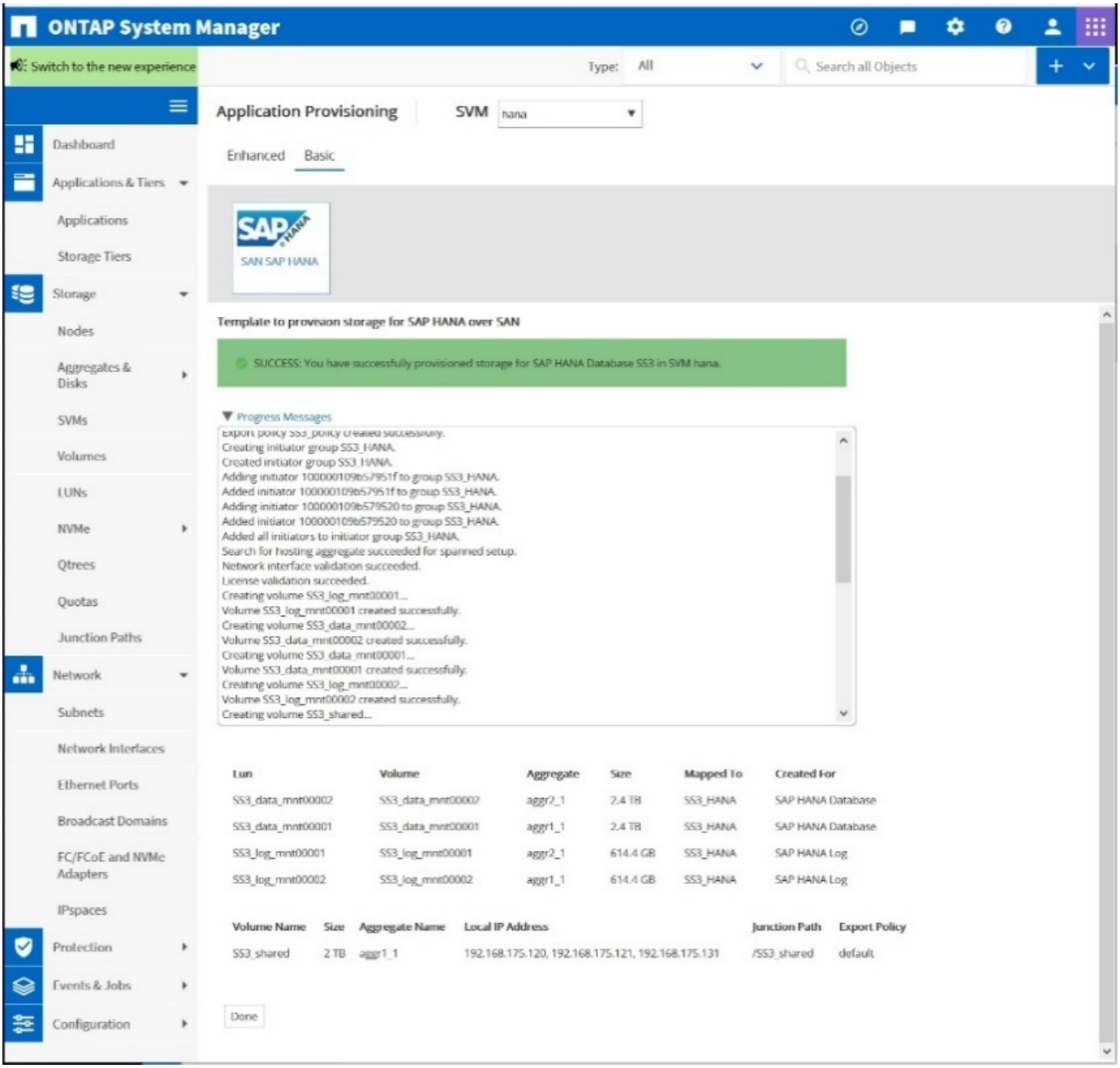
The `sanlun` tool is part of the NetApp Host Utilities and must be installed on each SAP HANA host. For more information, see the section "host_setup."

The following steps show the configuration of a 2+1 multiple-host HANA system with the SID SS3:

1. Start the Application Provisioning wizard for SAP HANA in System Manager and provide the required information. All initiators (WWPNs) from all hosts must be added.



2. Confirm that storage is successfully provisioned.



Creating LUNs, volumes, and mapping LUNs to initiator groups using the CLI

This section shows an example configuration using the command line with ONTAP 9.8 for a 2+1 SAP HANA multiple host system with SID FC5 using LVM and two LUNs per LVM volume group:

1. Create all necessary volumes.

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
nonevol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Create all LUNs.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Create the initiator group for all servers belonging to system FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb,
10000090fadcc5c1,10000090fadcc5c2,  10000090fadcc5c3,10000090fadcc5c4
-vserver hana
```

4. Map all LUNs to created initiator group.

```
lun map -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

Next: SAP HANA storage connector API.

SAP HANA storage connector API

Previous: Storage controller setup.

A storage connector is required only in multiple-host environments that have failover capabilities. In multiple-host setups, SAP HANA provides high-availability functionality so that an SAP HANA database host can fail over to a standby host. In this case, the LUNs of the failed host are accessed and used by the standby host. The storage connector is used to make sure that a storage partition can be actively accessed by only one database host at a time.

In SAP HANA multiple-host configurations with NetApp storage, the standard storage connector delivered by SAP is used. The “SAP HANA Fibre Channel Storage Connector Admin Guide” can be found as an attachment to SAP note 1900823.

Next: Host setup.

Host setup

Previous: SAP HANA storage connector API.

Before setting up the host, NetApp SAN host utilities must be downloaded from the NetApp Support site and installed on the HANA servers. The host utility documentation includes information about additional software that must be installed depending on the FCP HBA used.

The documentation also contains information on multipath configurations that are specific to the Linux version used. This document covers the required configuration steps for SLES 12 SP1 or higher and RHEL 7. 2 or later, as described in the Linux Host Utilities 7.1 Installation and Setup Guide.

Configure multipathing

Steps 1 through 6 must be executed on all worker and standby hosts in an SAP HANA multiple-host configuration.

To configure multipathing, complete the following steps:

1. Run the Linux `rescan-scsi-bus.sh -a` command on each server to discover new LUNs.

2. Run the `sanlun lun show` command and verify that all required LUNs are visible. The following example shows the `sanlun lun show` command output for a 2+1 multiple-host HANA system with two data LUNs and two log LUNs. The output shows the LUNs and the corresponding device files, such as LUN `SS3_data_mnt00001` and the device file `/dev/sdag` Each LUN has eight FC paths from the host to the storage controllers.

```
stlrx300s8-6:~ # sanlun lun show
controller(7mode/E-Series)/
device          host                  lun
vserver(cDOT/FlashRay)        lun-pathname
filename        adapter    protocol   size    product
------------------------------------------------------------------------
-------------------------------------------------
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdah       host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdag       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdaf       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdae       host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdad       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdac       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdab       host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdaa       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdz        host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdy        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdx        host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdw        host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdv        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdu        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdt        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sds        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
```

```
/dev/sdr        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdq        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdp        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdo        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdn        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdm        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdl        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdk        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdj        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdi        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdh        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdg        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdf        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sde        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdd        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdc        host10     FCP        512.0g  cDOT
```

3. Run the `multipath -r` command to get the worldwide identifiers (WWIDs) for the device file names.

In this example, there are four LUNs.

```
stlrx300s8-6:~ # multipath -r
create: 3600a098038304436375d4d442d753878 undef NETAPP,LUN C-Mode
size=512G features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:1:0 sdd  8:48   undef ready running
| |- 10:0:3:0 sdf  8:80   undef ready running
| |- 11:0:0:0 sds  65:32  undef ready running
| `- 11:0:2:0 sdu  65:64  undef ready running
```

```
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:0:0 sdc  8:32   undef ready running
  |- 10:0:2:0 sde  8:64   undef ready running
  |- 11:0:1:0 sdt  65:48  undef ready running
  `- 11:0:3:0 sdv  65:80  undef ready running
create: 3600a098038304436375d4d442d753879 undef NETAPP,LUN C-Mode
size=1.2T features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:1:1 sdj  8:144  undef ready running
| |- 10:0:3:1 sdp  8:240  undef ready running
| |- 11:0:0:1 sdw  65:96  undef ready running
| `- 11:0:2:1 sdac 65:192 undef ready running
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:0:1 sdg  8:96   undef ready running
  |- 10:0:2:1 sdm  8:192  undef ready running
  |- 11:0:1:1 sdz  65:144 undef ready running
  `- 11:0:3:1 sdaf 65:240 undef ready running
create: 3600a098038304436392b4d442d6f534f undef NETAPP,LUN C-Mode
size=1.2T features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:0:2 sdh  8:112  undef ready running
| |- 10:0:2:2 sdn  8:208  undef ready running
| |- 11:0:1:2 sdaa 65:160 undef ready running
| `- 11:0:3:2 sdag 66:0   undef ready running
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:1:2 sdk  8:160  undef ready running
  |- 10:0:3:2 sdq  65:0   undef ready running
  |- 11:0:0:2 sdx  65:112 undef ready running
  `- 11:0:2:2 sdad 65:208 undef ready running
create: 3600a098038304436392b4d442d6f5350 undef NETAPP,LUN C-Mode
size=512G features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:0:3 sdi  8:128  undef ready running
| |- 10:0:2:3 sdo  8:224  undef ready running
| |- 11:0:1:3 sdab 65:176 undef ready running
| `- 11:0:3:3 sdah 66:16  undef ready running
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:1:3 sdl  8:176  undef ready running
  |- 10:0:3:3 sdr  65:16  undef ready running
  |- 11:0:0:3 sdy  65:128 undef ready running
  `- 11:0:2:3 sdae 65:224 undef ready running
```

4. Edit the `/etc/multipath.conf` file and add the WWIDs and alias names.

The example output shows the content of the `/etc/multipath.conf` file, which includes alias names for the four LUNs of a 2+1 multiple-host system. If there is no multipath.conf file available, you can create one by running the following command: `multipath -T > /etc/multipath.conf`.

```
stlrx300s8-6:/ # cat /etc/multipath.conf
multipaths {
        multipath {
                wwid    3600a098038304436392b4d442d6f534f
                alias   hana- SS3_data_mnt00001
        }
        multipath {
                wwid    3600a098038304436375d4d442d753879
                alias   hana- SS3_data_mnt00002
        }
        multipath {
                wwid    3600a098038304436375d4d442d753878
                alias   hana- SS3_log_mnt00001
        }
        multipath {
                wwid    3600a098038304436392b4d442d6f5350
                alias   hana- SS3_log_mnt00002
        }
}
```

5. Run the `multipath -r` command to reload the device map.
6. Verify the configuration by running the `multipath -ll` command to list all the LUNs, alias names, and active and standby paths.

The following example output shows the output of a 2+1 multiple-host HANA system with two data and two log LUNs.

```
stlrx300s8-6:~ # multipath -ll
hana- SS3_data_mnt00002 (3600a098038304436375d4d442d753879) dm-1
NETAPP,LUN C-Mode
size=1.2T features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:1:1 sdj  8:144  active ready running
| |- 10:0:3:1 sdp  8:240  active ready running
| |- 11:0:0:1 sdw  65:96  active ready running
| `- 11:0:2:1 sdac 65:192 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:0:1 sdg  8:96   active ready running
```

```
  |- 10:0:2:1 sdm  8:192  active ready running
  |- 11:0:1:1 sdz  65:144 active ready running
  `- 11:0:3:1 sdaf 65:240 active ready running
hana- SS3_data_mnt00001 (3600a098038304436392b4d442d6f534f) dm-2
NETAPP,LUN C-Mode
size=1.2T features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:0:2 sdh  8:112  active ready running
| |- 10:0:2:2 sdn  8:208  active ready running
| |- 11:0:1:2 sdaa 65:160 active ready running
| `- 11:0:3:2 sdag 66:0   active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:1:2 sdk  8:160  active ready running
  |- 10:0:3:2 sdq  65:0   active ready running
  |- 11:0:0:2 sdx  65:112 active ready running
  `- 11:0:2:2 sdad 65:208 active ready running
hana- SS3_log_mnt00002 (3600a098038304436392b4d442d6f5350) dm-3
NETAPP,LUN C-Mode
size=512G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:0:3 sdi  8:128  active ready running
| |- 10:0:2:3 sdo  8:224  active ready running
| |- 11:0:1:3 sdab 65:176 active ready running
| `- 11:0:3:3 sdah 66:16  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:1:3 sdl  8:176  active ready running
  |- 10:0:3:3 sdr  65:16  active ready running
  |- 11:0:0:3 sdy  65:128 active ready running
  `- 11:0:2:3 sdae 65:224 active ready running
hana- SS3_log_mnt00001 (3600a098038304436375d4d442d753878) dm-0
NETAPP,LUN C-Mode
size=512G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:1:0 sdd  8:48   active ready running
| |- 10:0:3:0 sdf  8:80   active ready running
| |- 11:0:0:0 sds  65:32  active ready running
| `- 11:0:2:0 sdu  65:64  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:0:0 sdc  8:32   active ready running
  |- 10:0:2:0 sde  8:64   active ready running
  |- 11:0:1:0 sdt  65:48  active ready running
  `- 11:0:3:0 sdv  65:80  active ready running
```

Create LVM volume groups and logical volumes

This step is only required if LVM is used. The following example is for 2+1 host setup using SID FC5.

For an LVM-based setup, the multipath configuration described in the previous section must be completed as well. In this example, eight LUNs must be configured for multipathing.

1. Initialize all LUNs as a physical volume.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001pvcreate /dev/mapper/hana-
FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001pvcreate /dev/mapper/hana-
FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. Create the volume groups for each data and log partition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. Create a logical volume for each data and log partition. Use a stripe size that is equal to the number of LUNs used per volume group (in this example, it is two) and a stripe size of 256k for data and 64k for log. SAP only supports one logical volume per volume group.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scan the physical volumes, volume groups, and vol groups at all other hosts.

```
modprobe dm_modpvscanvgscanlvscan
```

If these commands do not find the volumes, a restart is required.

To mount the logical volumes, the logical volumes must be activated. To activate the volumes, run the following command:

```
vgchange -a y
```

Create file systems

To create the XFS file system on each LUN belonging to the HANA system, take one of the following actions:

- For a single-host system, create the XFS file system on the data, log, and `/hana/shared` LUNs.

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_data_mnt00001
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_log_mnt00001
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_shared
```

- For a multiple-host system, create the XFS file system on all data and log LUNs.

```
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_log_mnt00001
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_log_mnt00002
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_data_mnt00001
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_data_mnt00002
```

- If LVM is used, create the XFS file system on all data and log logical volumes.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

The multiple host example commands show a 2+1 multiple-host HANA system.

Create mount points

To create the required mount point directories, take one of the following actions:

- For a single-host system, set permissions and create mount points on the database host.

```
stlrx300s8- 6:/ # mkdir -p /hana/data/SS3/mnt00001
stlrx300s8- 6:/ # mkdir -p /hana/log/SS3/mnt00001
stlrx300s8- 6:/ # mkdir -p /hana/shared
stlrx300s8- 6:/ # chmod -R 777 /hana/log/SS3
stlrx300s8- 6:/ # chmod -R 777 /hana/data/SS3
stlrx300s8-6:/ # chmod 777 /hana/shared
```

- For a multiple-host system, set permissions and create mount points on all worker and standby hosts.

The example commands show a 2+1 multiple-host HANA system.

```
stlrx300s8- 6:/ # mkdir -p /hana/data/SS3/mnt00001
stlrx300s8- 6:/ # mkdir -p /hana/log/SS3/mnt00001
stlrx300s8- 6:/ # mkdir -p /hana/data/SS3/mnt00002
stlrx300s8- 6:/ # mkdir -p /hana/log/SS3/mnt00002
stlrx300s8- 6:/ # mkdir -p /hana/shared
stlrx300s8- 6:/ # chmod -R 777 /hana/log/SS3
stlrx300s8- 6:/ # chmod -R 777 /hana/data/SS3
stlrx300s8-6:/ # chmod 777 /hana/shared
```

The same steps must be executed for a system configuration with Linux LVM.

Mount file systems

To mount file systems during system boot using the `/etc/fstab` configuration file, complete the following steps:

- For a single-host system, add the required file systems to the `/etc/fstab` configuration file.

The XFS file systems for the data and log LUNs must be mounted with the `relatime` and `inode64` mount options.

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana- SS3_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana- SS3_log_mnt00001 /hana/log/SS3/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana- SS3_data_mnt00001 /hana/data/SS3/mnt00001 xfs
relatime,inode64 0 0
```

If LVM is used, use the logical volume names for data and log.

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

- For a multiple-host system, add the `/hana/shared` file system to the `/etc/fstab` configuration file of each host.

All the data and log file systems are mounted through the SAP HANA storage connector.

```
stlrx300s8-6:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

To mount the file systems, run the `mount -a` command at each host.

Next: I/O Stack configuration for SAP HANA.

I/O Stack configuration for SAP HANA

Previous: Host setup.

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage system used.

NetApp conducted performance tests to define the ideal values. The following table lists the optimal values as inferred from the performance tests.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on
async_write_submit_blocks	all

For SAP HANA 1.0 up to SPS12, these parameters can be set during the installation of the SAP HANA database, as described in SAP Note 2267798 – Configuration of the SAP HANA Database during Installation Using hdbparam.

Alternatively, the parameters can be set after the SAP HANA database installation by using the `hdbparam` framework.

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Starting with SAP HANA 2.0, `hdbparam` is deprecated, and the parameters are moved to the `global.ini` file. The parameters can be set by using SQL commands or SAP HANA Studio. For more details, refer to SAP note 2399079: Elimination of hdbparam in HANA 2. The parameters can be also set within the `global.ini`

file.

```
SS3adm@stlrx300s8-6: /usr/sap/SS3/SYS/global/hdb/custom/config>cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

For SAP HANA 2.0 SPS5 and later, use the `setParameter.py` script to set the correct parameters.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Next: SAP HANA software installation.

SAP HANA software installation

Previous: I/O stack configuration for SAP HANA.

Installation on single-host system

SAP HANA software installation does not require any additional preparation for a single-host system.

Installation on multiple-host system

Before beginning the installation, create a `global.ini` file to enable use of the SAP storage connector during the installation process. The SAP storage connector mounts the required file systems at the worker hosts during the installation process. The `global.ini` file must be available in a file system that is accessible from all hosts, such as the `/hana/shared` file system.

Before installing SAP HANA software on a multiple-host system, the following steps must be completed:

1. Add the following mount options for the data LUNs and the log LUNs to the `global.ini` file:
    - `relatime` and `inode64` for the data and log file system
2. Add the WWIDs of the data and log partitions. The WWIDs must match the alias names configured in the `/etc/multipath.conf` file.

The following output shows an example of a 2+1 multiple-host setup in which the system identifier (SID) is SS3.

```
stlrx300s8-6:~ # cat /hana/shared/global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/SS3
basepath_logvolumes = /hana/log/SS3
[storage]
ha_provider = hdb_ha.fcClient
partition_*_*__prtype = 5
partition_*_data__mountoptions = -o relatime,inode64
partition_*_log__mountoptions = -o relatime,inode64,nobarrier
partition_1_data__wwid = hana- SS3_data_mnt00001
partition_1_log__wwid = hana- SS3_log_mnt00001
partition_2_data__wwid = hana- SS3_data_mnt00002
partition_2_log__wwid = hana- SS3_log_mnt00002
[system_information]
usage = custom
[trace]
ha_fcclient = info
stlrx300s8-6:~ #
```

If the Linux LVM is used, the required configuration is different. The following example shows a 2+1 multiple-host setup with SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
Using the SAP hdblcm installation tool, start the installation by
running the following command at one of the worker hosts. Use the
`addhosts` option to add the second worker (sapcc-hana-tst-04) and the
standby host (sapcc-hana-tst-05).
```

The directory where the prepared `global.ini` file is stored is included with the `storage_cfg` CLI option (`-- storage_cfg=/hana/shared`).

Depending on the OS version being used, it might be necessary to install Python 2.7 before installing the SAP HANA database.

```
sapcc-hana-tst-03:/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_LCM_LINUX_X86_64 # ./hdblcm --action=install
--addhosts=sapcc-hana-tst-04:role=worker:storage_partion=2,sapcc-hana
-tst-05:role:=standby --storage_cfg=/hana(shared/shared
SAP HANA Lifecycle Management - SAP HANA Database 2.00.052.00.1599235305
************************************************************************
Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.052.0000.1599259237) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.052.00.1599235305) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.5.109.1598303414) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
    SAP HANA Smart Data Access (2.00.5.000.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
```

```
52/DATA_UNITS/SAP_HANA_SDA_20_LINUX_X86_64/packages
    SAP HANA Studio (2.3.54.000000) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.4.24.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.0.130.519) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.014.1) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI14_1.zip
    XSAC FILEPROCESSOR 1.0 (1.000.85) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_85.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.012.20341) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_HRTT_20/XSACHRTT12_20341.zip
    XS Messaging Service 1 (1.004.10) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACMESSSRV04_10.zip
    Develop and run portal services for customer apps on XSA (1.005.1)
in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV05_1.zip
    SAP Web IDE Web Client (4.005.1) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE05_1.zip
    XS JOB SCHEDULER 1.0 (1.007.12) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_12.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.25) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_25.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.3) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_3.zip
    XSA Cockpit 1 (1.001.17) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_17.zip
SAP HANA Database version '2.00.052.00.1599235305' will be installed.
Select additional components for installation:
  Index | Components | Description
```

```
---------------------------------------------------------------------------
--------------------
  1     | all         | All components
  2     | server      | No additional components
  3     | client      | Install SAP HANA Database Client version
2.5.109.1598303414
  4     | lss         | Install SAP HANA Local Secure Store version
2.4.24.0
  5     | studio      | Install SAP HANA Studio version 2.3.54.000000
  6     | smartda     | Install SAP HANA Smart Data Access version
2.00.5.000.0
  7     | xs          | Install SAP HANA XS Advanced Runtime version
1.0.130.519
  8     | afl         | Install SAP HANA AFL (incl.PAL,BFL,OFL) version
2.00.052.0000.1599259237
  9     | eml         | Install SAP HANA EML AFL version
2.00.052.0000.1599259237
  10    | epmmds      | Install SAP HANA EPM-MDS version
2.00.052.0000.1599259237
Enter comma-separated list of the selected indices [3]: 2,3
Enter Installation Path [/hana/shared]:
Enter Local Host Name [sapcc-hana-tst-03]:
```

3. Verify that the installation tool installed all selected components at all worker and standby hosts.

Next: Adding additional data volume partitions for SAP HANA single-host systems.

Adding additional data volume partitions for SAP HANA single-host systems

Previous: SAP HANA software installation.

Starting with SAP HANA 2.0 SPS4, additional data volume partitions can be configured. This feature allows you to configure two or more LUNs for the data volume of an SAP HANA tenant database and to scale beyond the size and performance limits of a single LUN.

It is not necessary to use multiple partitions to fulfill the SAP HANA KPIs. A single LUN with a single partition fulfills the required KPIs.

Using two or more individual LUNs for the data volume is only available for SAP HANA single-host systems. The SAP storage connector required for SAP HANA multiple-host systems does only support one device for the data volume.

Adding additional data volume partitions can be done at any time but might require a restart of the SAP HANA database.

Enabling additional data volume partitions

To enable additional data volume partitions, complete the following steps:

1. Add the following entry within the `global.ini` file.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. Restart the database to enable the feature. Adding the parameter through the SAP HANA Studio to the `global.ini` file by using the Systemdb configuration prevents the restart of the database.

Volume and LUN configuration

The layout of volumes and LUNs is like the layout of a single host with one data volume partition, but with an additional data volume and LUN stored on a different aggregate as the log volume and the other data volume. The following table shows an example configuration of an SAP HANA single-host systems with two data volume partitions.

Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data volume: SID_data_mnt00001	Shared volume: SID_shared	Data volume: SID_data2_mnt00001	Log volume: SID_log_mnt00001

The following table shows an example of the mount point configuration for a single-host system with two data volume partitions.

LUN	Mount point at HANA host	Note
SID_data_mnt00001	/hana/data/SID/mnt00001	Mounted using /etc/fstab entry
SID_data2_mnt00001	/hana/data2/SID/mnt00001	Mounted using /etc/fstab entry
SID_log_mnt00001	/hana/log/SID/mnt00001	Mounted using /etc/fstab entry
SID_shared	/hana/shared/SID	Mounted using /etc/fstab entry

Create the new data LUNs using either ONTAP System Manager or the ONTAP CLI.

Host configuration

To configure a host, complete the following steps:

1. Configure multipathing for the additional LUNs, as described in chapter 0.
2. Create the XFS file system on each additional LUN belonging to the HANA system:

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_data2_mnt00001
```

3. Add the additional file system/s to the `/etc/fstab` configuration file.

The XFS file systems for the data and log LUN must be mounted with the `relatime` and `inode64` mount options.

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-SS3_shared /hana/shared xfs default 0 0
/dev/mapper/hana-SS3_log_mnt00001 /hana/log/SS3/mnt00001 xfs
relatime,inode64,nobarrier 0 0
/dev/mapper/hana-SS3_data_mnt00001 /hana/data/SS3/mnt00001 xfs
relatime,inode64 0 0/dev/mapper/hana-SS3_data2_mnt00001
/hana/data2/SS3/mnt00001 xfs relatime,inode64 0 0
```

4. Create mount points and set permissions on the database host.

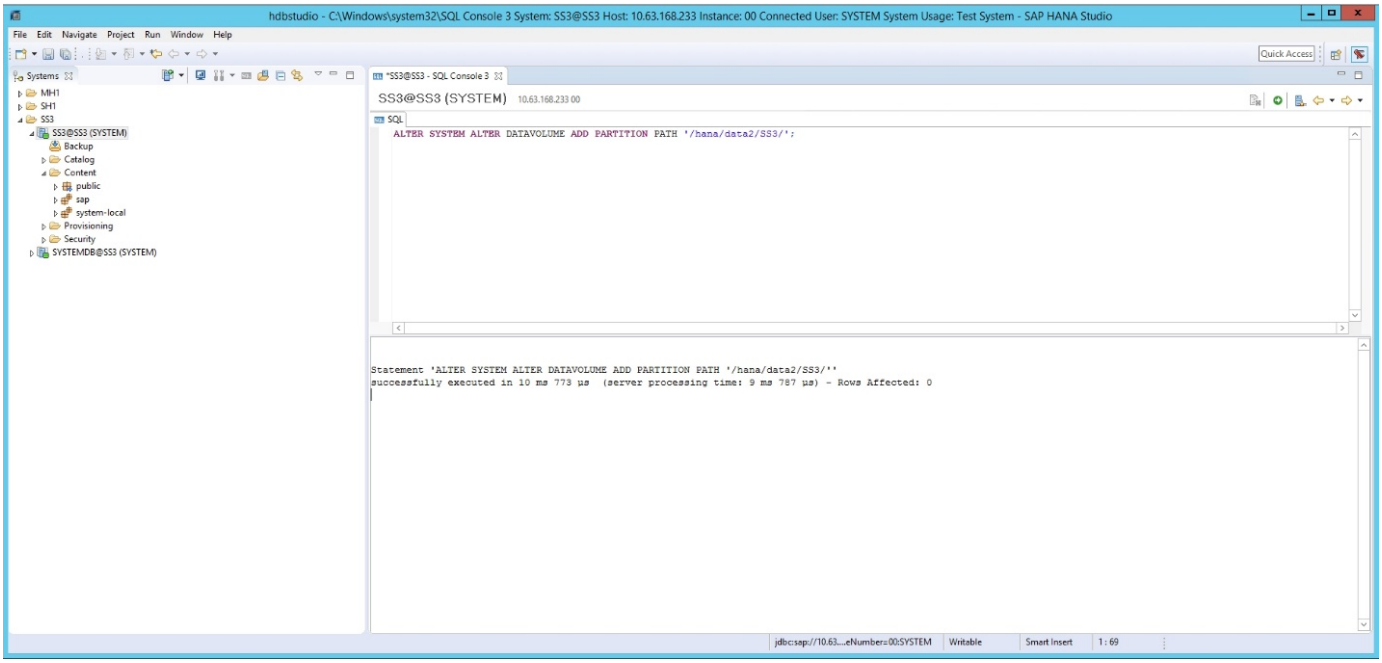
```
stlrx300s8-6:/ # mkdir -p /hana/data2/SS3/mnt00001
stlrx300s8-6:/ # chmod -R 777 /hana/data2/SS3
```

5. Mount the file systems, run the `mount -a` command.

Adding an additional datavolume partition

To add an additional datavolume partition to your tenant database, execute the following SQL statement against the tenant database. Each additional LUN can have a different path:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Next: Where to find additional information.

Where to find additional information

Previous: Adding additional data volume partitions for SAP HANA single-host systems.

To learn more about the information described in this document, refer to the following documents and/or websites:

- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere

  www.vmware.com/files/pdf/SAP_HANA_on_vmware_vSphere_best_practices_guide.pdf

- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere

  http://www.vmware.com/files/pdf/sap-hana-scale-out-deployments-on-vsphere.pdf

- SAP Certified Enterprise Storage Hardware for SAP HANA

  https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/enterprise-storage.html

- SAP HANA Storage Requirements

  http://go.sap.com/documents/2015/03/74cdb554-5a7c-0010-82c7-eda71af511fa.html

- SAP HANA Tailored Data Center Integration Frequently Asked Questions

  https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html

- TR-4646: SAP HANA Disaster Recovery with Storage Replication Using SnapCenter 4.0 SAP HANA Plug-In

  https://www.netapp.com/us/media/tr-4646.pdf

- TR-4614: SAP HANA Backup and Recovery with SnapCenter

  https://www.netapp.com/us/media/tr-4614.pdf

- TR-4338: SAP HANA on VMware vSphere with NetApp FAS and AFF Systems

  www.netapp.com/us/media/tr-4338.pdf

- TR-4667: Automating SAP System Copies Using the SnapCenter 4.0 SAP HANA Plugin

  https://www.netapp.com/us/media/tr-4667.pdf

- NetApp Documentation Centers

  https://www.netapp.com/us/documentation/index.aspx

- NetApp AFF Storage System Resources

  https://mysupport.netapp.com/info/web/ECMLP2676498.html

- SAP HANA Software Solutions

  www.netapp.com/us/solutions/applications/sap/index.aspx#sap-hana

TR-4435: SAP HANA on NetApp AFF Systems with NFS - Configuration Guide

Nils Bauer and Marco Schön, NetApp

The NetApp AFF system product family has been certified for use with SAP HANA in tailored data center integration (TDI) projects. The certified enterprise storage system is characterized by the NetApp ONTAP software.

This certification is valid for the following models:

- AFF A220, AFF A250, AFF A300, AFF A320, AFF A400, AFF A700s, AFF A700, AFF A800

A complete list of NetApp certified storage solutions for SAP HANA can be found at the Certified and supported SAP HANA hardware directory.

This document describes the ONTAP configuration requirements for the NFS protocol version 3 (NFSv3) or the NFS protocol version 4 (NFSv4.0 and NFSv4.1).

For the remainder of this document, NFSv4 refers to both NFSv4.0 and NFSv4.1.

The configuration described in this paper is necessary to achieve the required SAP HANA KPIs and the best performance for SAP HANA. Changing any settings or using features not listed herein might cause performance degradation or unexpected behavior and should only be done if advised by NetApp support.

The configuration guides for NetApp AFF systems using FCP and for FAS systems using NFS or FCP can be found at the following links:

- SAP HANA on NetApp FAS Systems with Fibre Channel Protocol
- SAP HANA on NetApp FAS Systems with NFS
- SAP HANA on NetApp AFF Systems with Fibre Channel Protocol

The following table shows the supported combinations for NFS versions, NFS locking, and the required isolation implementations, depending on the SAP HANA database configuration.

For SAP HANA single-host systems or multiple hosts that do not use Host Auto-Failover, NFSv3 and NFSv4 are supported.

For SAP HANA multiple host systems with Host Auto-Failover, NetApp only supports NFSv4, while using NFSv4 locking as an alternative to a server-specific STONITH (SAP HANA HA/DR provider) implementation.

SAP HANA	NFS version	NFS locking	SAP HANA HA/DR provider
SAP HANA single host, multiple hosts without Host Auto-Failover	NFSv3	Off	n/a
	NFSv4	On	n/a
SAP HANA multiple hosts using Host Auto-Failover	NFSv3	Off	Server-specific STONITH implementation mandatory
	NFSv4	On	Not required

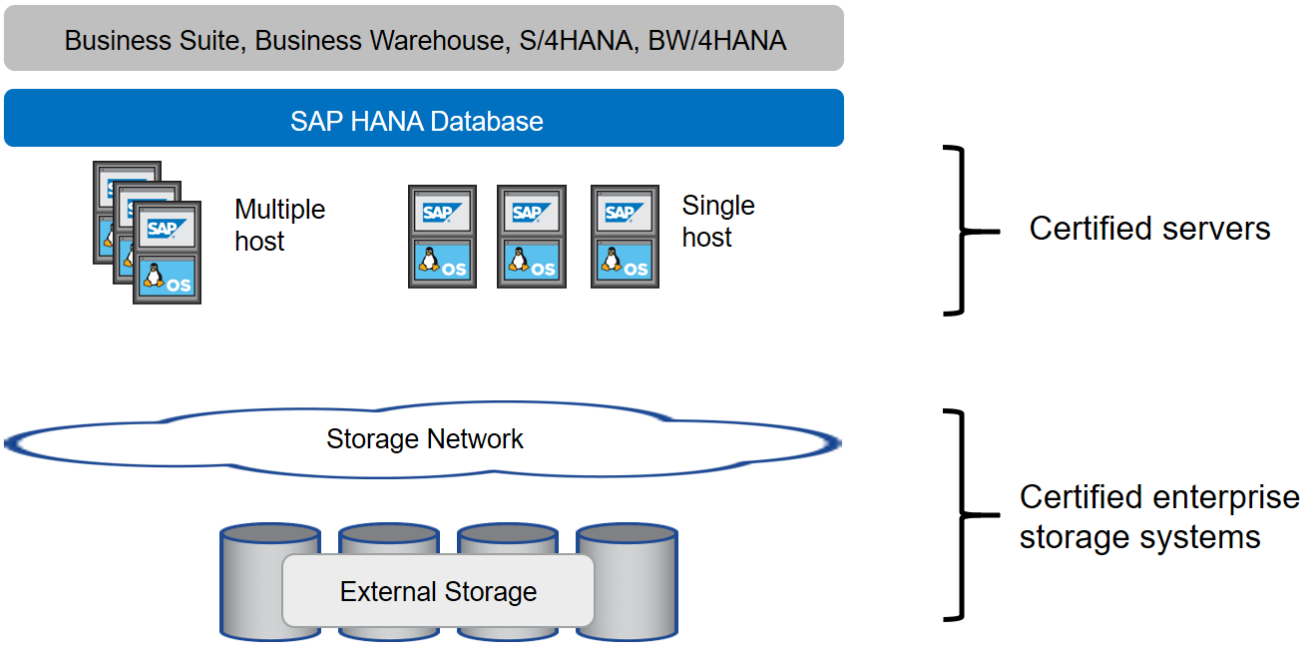
A server-specific STONITH implementation is not part of this guide. Contact your server vendor for such an implementation.

This document covers configuration recommendations for SAP HANA running on physical servers and on virtual servers that use VMware vSphere.

See the relevant SAP notes for operating system configuration guidelines and HANA-specific Linux kernel dependencies. For more information, see SAP note 2235581: SAP HANA Supported Operating Systems.

SAP HANA tailored data center integration

NetApp AFF storage controllers are certified in the SAP HANA TDI program using both NFS (NAS) and FC (SAN) protocols. They can be deployed in any of the current SAP HANA scenarios, such as SAP Business Suite on HANA, S/4HANA, BW/4HANA, or SAP Business Warehouse on HANA in either single-host or multiple-host configurations. Any server that is certified for use with SAP HANA can be combined with NetApp certified storage solutions. See the following figure for an architecture overview of SAP HANA TDI.



For more information regarding the prerequisites and recommendations for producti SAP HANA systems, see the following resources:

- SAP HANA Tailored Data Center Integration Frequently Asked Questions
- SAP HANA Storage Requirements

SAP HANA using VMware vSphere

There are several options for connecting storage to virtual machines (VMs). The preferred option is to connect the storage volumes with NFS directly out of the guest operating system. Using this option, the configuration of hosts and storage does not differ between physical hosts and VMs.

NFS datastores and VVOL datastores with NFS are supported as well. For both options, only one SAP HANA data or log volume must be stored within the datastore for production use cases. In addition, Snapshot-based

backup and recovery orchestrated by NetApp SnapCenter and solutions based on this, such as SAP System cloning, cannot be implemented.

This document describes the recommended setup with direct NFS mounts from the guest OS.

For more information about using vSphere with SAP HANA, see the following links:

- SAP HANA on VMware vSphere - Virtualization - Community Wiki
- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere
- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere
- 2161991 - VMware vSphere configuration guidelines - SAP ONE Support Launchpad (Login required)

Next: Architecture.

Architecture

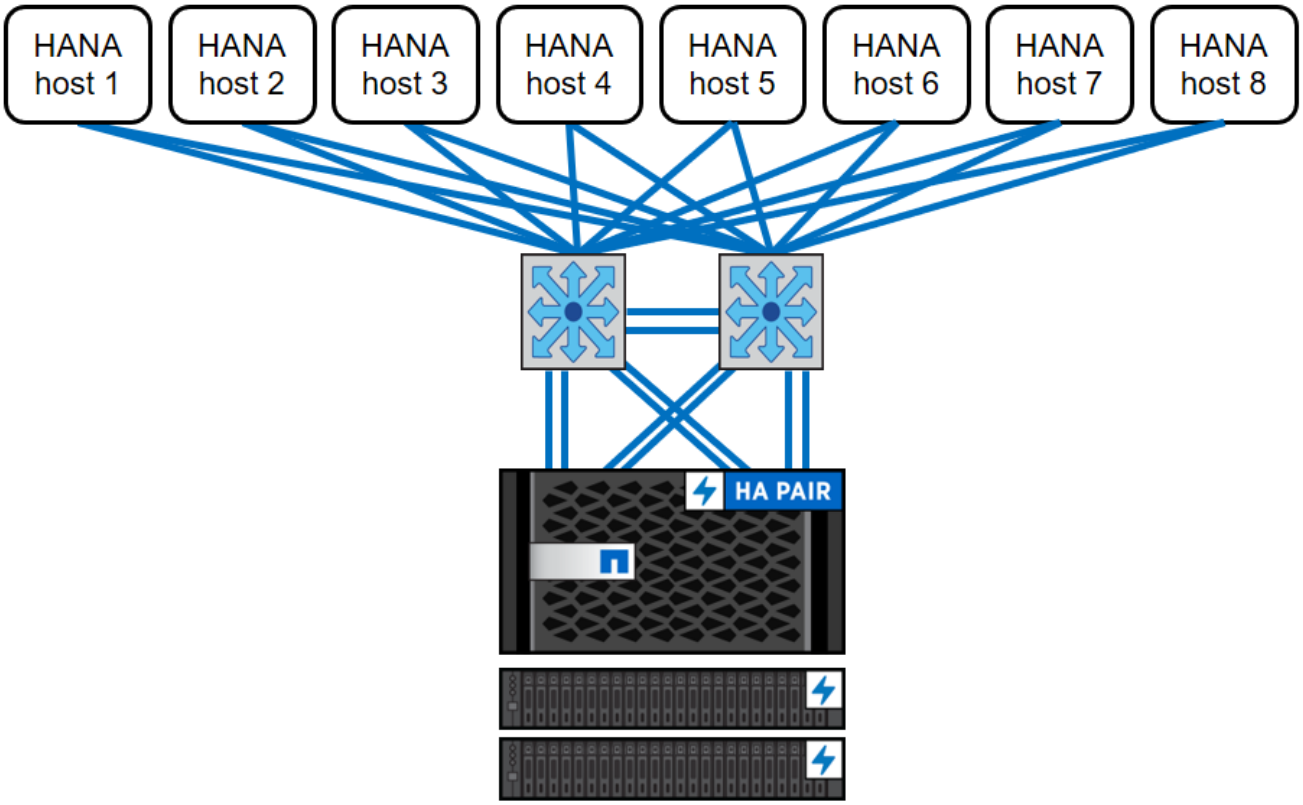
Previous: SAP HANA on NetApp All Flash FAS Systems with NFS Configuration Guide.

SAP HANA hosts are connected to storage controllers by using a redundant 10GbE or faster network infrastructure. Data communication between SAP HANA hosts and storage controllers is based on the NFS protocol. A redundant switching infrastructure is required to provide fault-tolerant SAP HANA host-to-storage connectivity in case of switch or network interface card (NIC) failure.

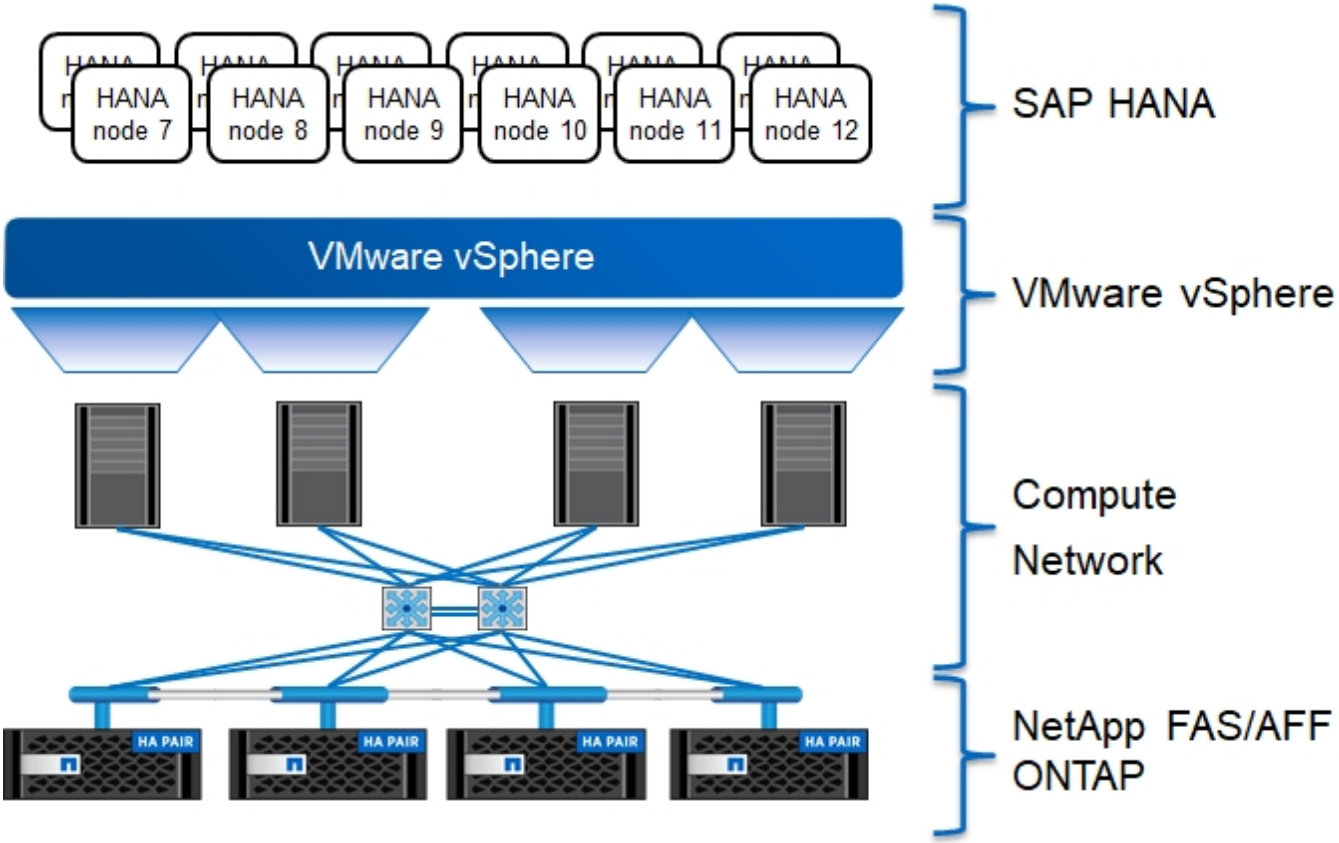
The switches might aggregate individual port performance with port channels in order to appear as a single logical entity at the host level.

Different models of the AFF system product family can be mixed and matched at the storage layer to allow for growth and differing performance and capacity needs. The maximum number of SAP HANA hosts that can be attached to the storage system is defined by the SAP HANA performance requirements and the model of NetApp controller used. The number of required disk shelves is only determined by the capacity and performance requirements of the SAP HANA systems.

The following figure shows an example configuration with eight SAP HANA hosts attached to a storage high availability (HA) pair.



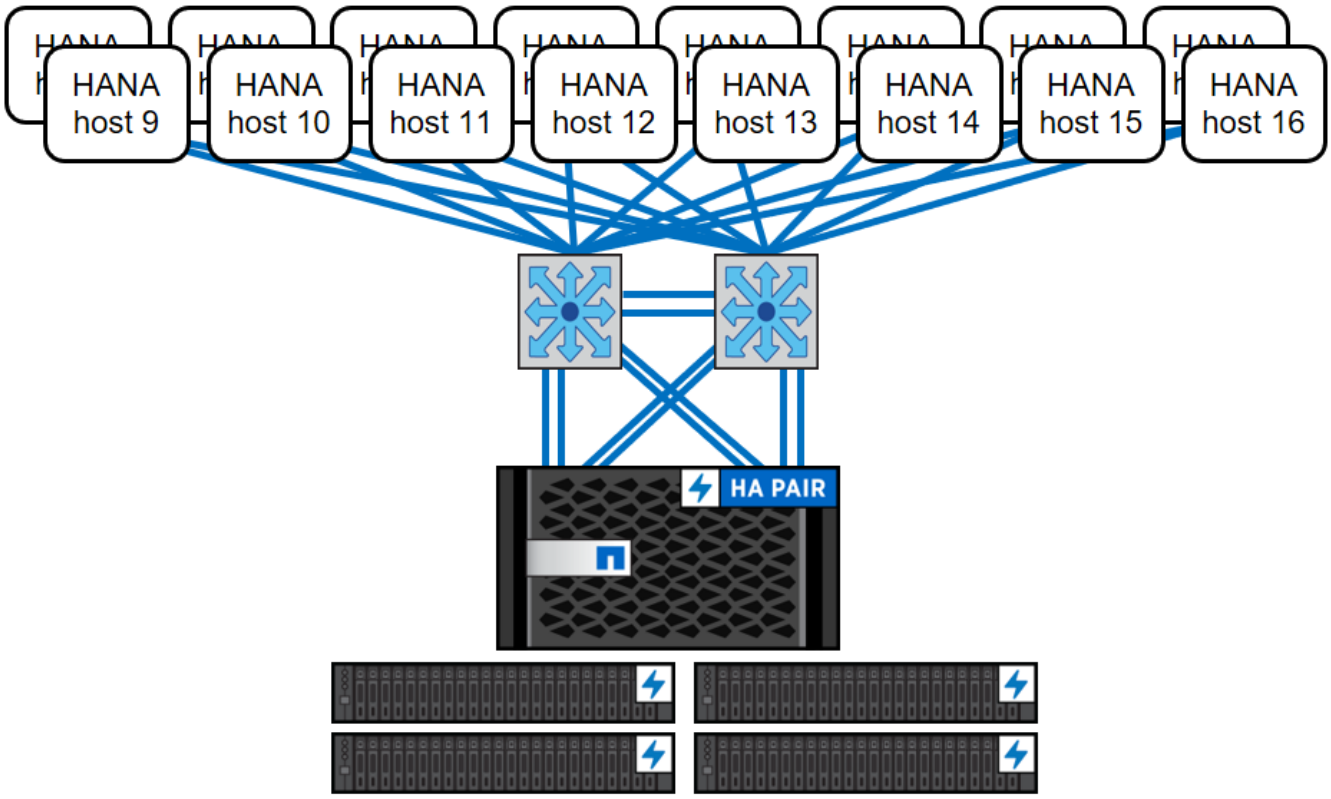
The following figure shows an example of using VMware vSphere as a virtualization layer.



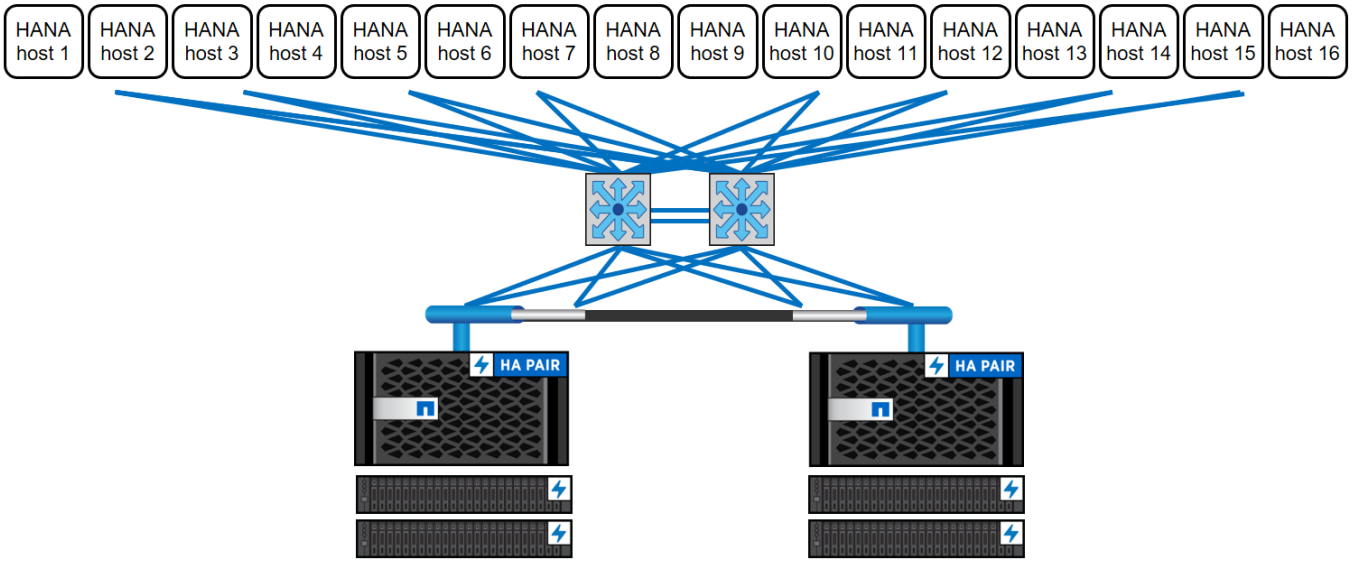
The architecture can be scaled in two dimensions:

- By attaching additional SAP HANA hosts and storage capacity to the existing storage, if the storage controllers provide enough performance to meet the current SAP HANA key performance indicators (KPIs).
- By adding more storage systems with additional storage capacity for the additional SAP HANA hosts

The following figure shows an example configuration in which more SAP HANA hosts are attached to the storage controllers. In this example, more disk shelves are necessary to fulfill the capacity and performance requirements of the 16 SAP HANA hosts. Depending on the total throughput requirements, you must add additional 10GbE or faster connections to the storage controllers.



Independent of the deployed AFF system, the SAP HANA landscape can also be scaled by adding any of the certified storage controllers to meet the desired node density, as shown in the following figure.



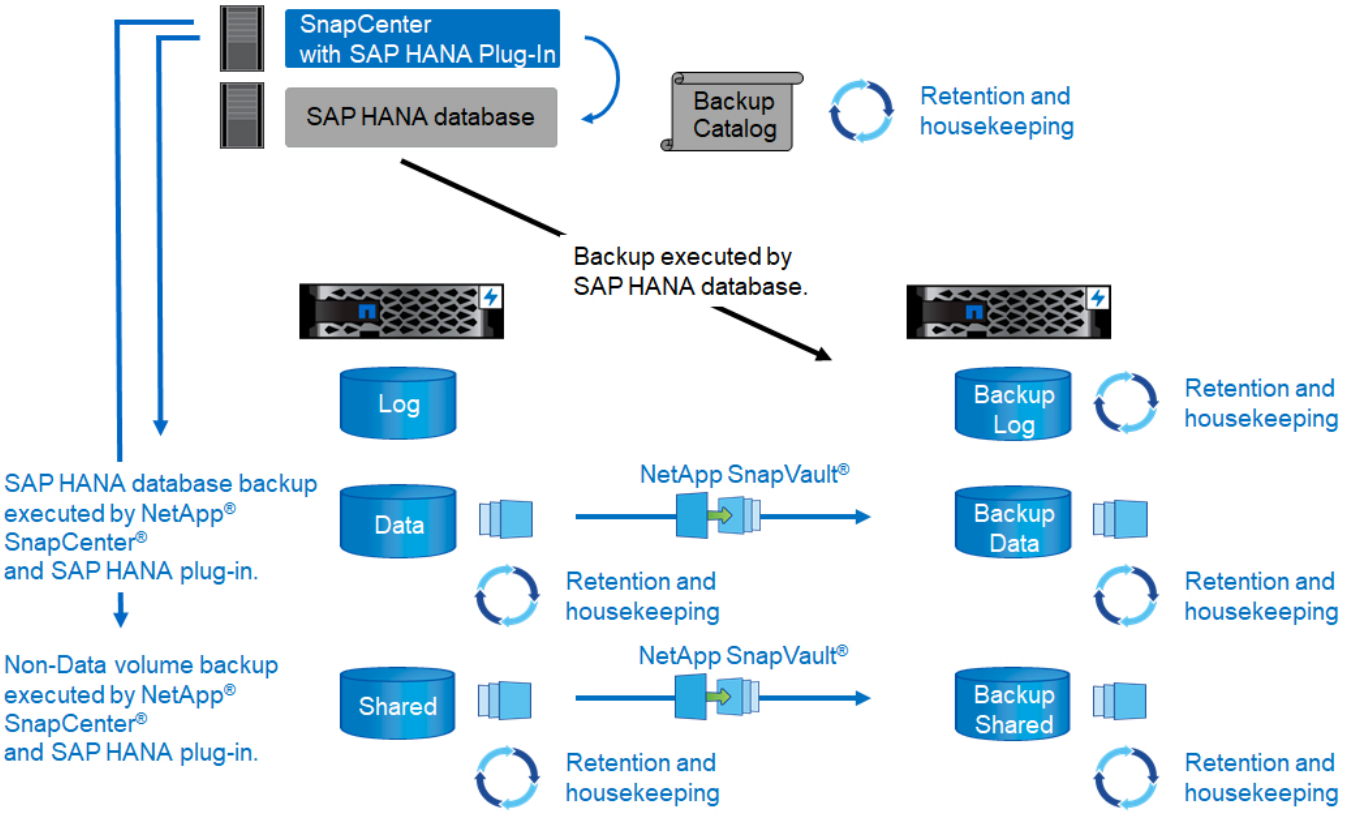
SAP HANA backup

The ONTAP software present on all NetApp storage controllers provides a built-in mechanism to back up SAP HANA databases while in operation with no effect on performance. Storage-based NetApp Snapshot backups are a fully supported and integrated backup solution available for SAP HANA single containers and for SAP HANA Multitenant Database Containers (MDC) systems with a single tenant or multiple tenants.

Storage-based Snapshot backups are implemented by using the NetApp SnapCenter plug-in for SAP HANA. This allows users to create consistent storage-based Snapshot backups by using the interfaces provided natively by SAP HANA databases. SnapCenter registers each of the Snapshot backups into the SAP HANA backup catalog. Therefore, the backups taken by SnapCenter are visible within SAP HANA Studio and Cockpit where they can be selected directly for restore and recovery operations.

NetApp SnapMirror technology enables Snapshot copies that were created on one storage system to be replicated to a secondary backup storage system that is controlled by SnapCenter. Different backup retention policies can then be defined for each of the backup sets on the primary storage and for the backup sets on the secondary storage systems. The SnapCenter Plug-in for SAP HANA automatically manages the retention of Snapshot copy-based data backups and log backups, including the housekeeping of the backup catalog. The SnapCenter Plug-in for SAP HANA also allows the execution of a block integrity check of the SAP HANA database by executing a file-based backup.

The database logs can be backed up directly to the secondary storage by using an NFS mount, as shown in the following figure.



Storage-based Snapshot backups provide significant advantages compared to conventional file-based backups. These advantages include, but are not limited to, the following:

- Faster backup (a few minutes)
- Reduced recovery time objective (RTO) due to a much faster restore time on the storage layer (a few minutes) as well as more frequent backups
- No performance degradation of the SAP HANA database host, network, or storage during backup and recovery operations
- Space-efficient and bandwidth-efficient replication to secondary storage based on block changes

For detailed information about the SAP HANA backup and recovery solution see TR-4614: SAP HANA Backup and Recovery with SnapCenter.

SAP HANA disaster recovery

SAP HANA disaster recovery (DR) can be done either on the database layer by using SAP HANA system replication or on the storage layer by using storage replication technologies. The following section provides an overview of disaster recovery solutions based on storage replication.

For detailed information about SAP HANA disaster recovery solutions, see TR-4646: SAP HANA Disaster Recovery with Storage Replication.

Storage replication based on SnapMirror

The following figure shows a three-site disaster recovery solution using synchronous SnapMirror replication to the local DR datacenter and asynchronous SnapMirror to replicate the data to the remote DR datacenter.

Data replication using synchronous SnapMirror provides an RPO of zero. The distance between the primary

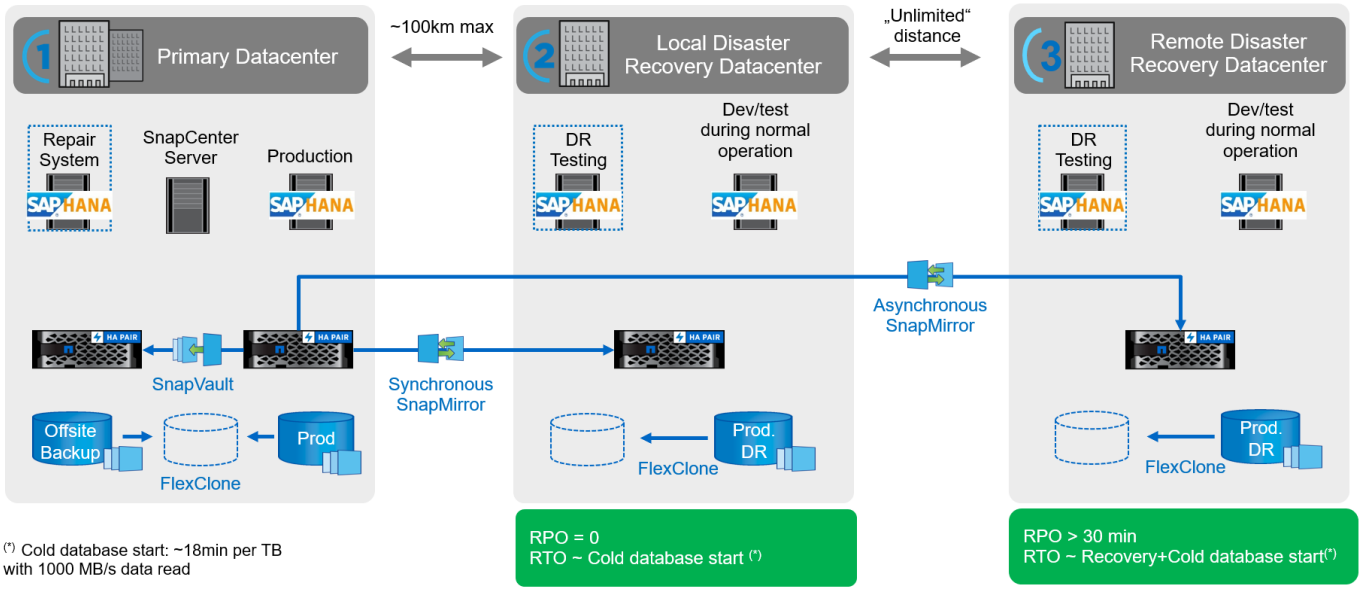
and the local DR datacenter is limited to around 100km.

Protection against failures of both the primary and the local DR site is performed by replicating the data to a third remote DR datacenter using asynchronous SnapMirror. The RPO depends on the frequency of replication updates and how fast they can be transferred. In theory, the distance is unlimited, but the limit depends on the amount of data that must be transferred and the connection that is available between the data centers. Typical RPO values are in the range of 30 minutes to multiple hours.

The RTO for both replication methods primarily depends on the time needed to start the HANA database at the DR site and load the data into memory. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data would take approximately 18 minutes.

The servers at the DR sites can be used as dev/test systems during normal operation. In the case of a disaster, the dev/test systems would need to be shut down and started as DR production servers.

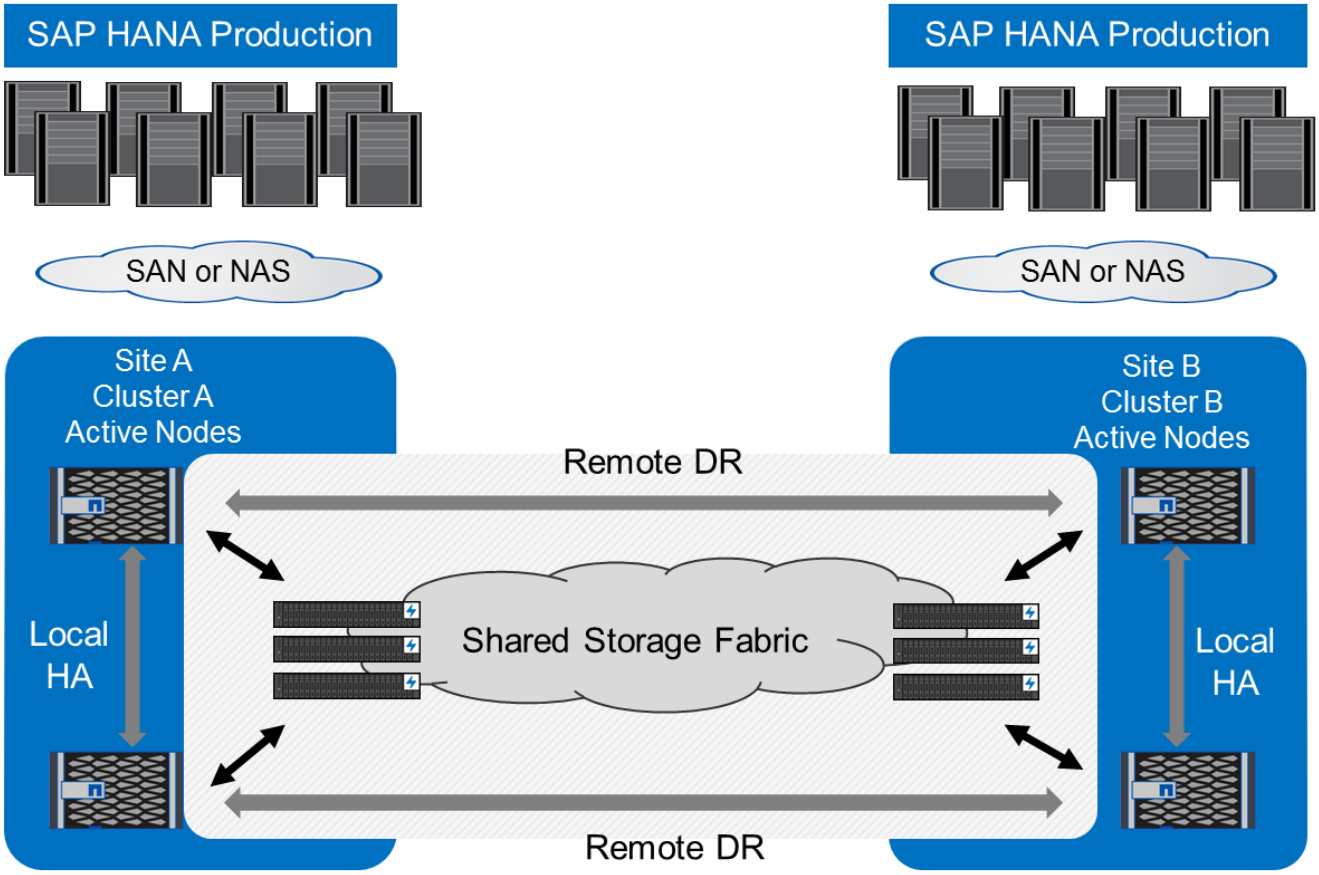
Both replication methods allow to you execute DR workflow testing without influencing the RPO and RTO. FlexClone volumes are created on the storage and are attached to the DR testing servers.



Synchronous replication offers StrictSync mode. If the write to secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage systems are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the InSync status. If the primary storage fails, application I/O can be resumed on the secondary storage after failover with no loss of data. In StrictSync mode, the RPO is always zero.

Storage replication based on MetroCluster

The following figure shows a high-level overview of the solution. The storage cluster at each site provides local high availability and is used for the production workload. The data of each site is synchronously replicated to the other location and is available in case of disaster failover.



Next: Storage sizing.

Storage sizing

Previous: Architecture.

The following section provides an overview of the required performance and capacity considerations needed for sizing a storage system for SAP HANA.

Contact NetApp or your NetApp partner sales representative to assist you in creating a properly sized storage environment.

Performance considerations

SAP has defined a static set of storage KPIs. These KPIs are valid for all production SAP HANA environments independent of the memory size of the database hosts and the applications that use the SAP HANA database. These KPIs are valid for single-host, multiple-host, Business Suite on HANA, Business Warehouse on HANA, S/4HANA, and BW/4HANA environments. Therefore, the current performance sizing approach depends on only the number of active SAP HANA hosts that are attached to the storage system.

Storage performance KPIs are only mandated for production SAP HANA systems, but you can implement them in for all HANA system.

SAP delivers a performance test tool that must be used to validate the storage system's performance for active SAP HANA hosts attached to the storage.

NetApp tested and predefined the maximum number of SAP HANA hosts that can be attached to a specific storage model while still fulfilling the required storage KPIs from SAP for production-based SAP HANA systems.

The maximum number of SAP HANA hosts that can be run on a disk shelf and the minimum number of SSDs required per SAP HANA host were determined by running the SAP performance test tool. This test does not consider the actual storage capacity requirements of the hosts. You must also calculate the capacity requirements to determine the actual storage configuration needed.

SAS disk shelf

With the 12Gb serial-attached SCSI (SAS) disk shelf (DS224C), performance sizing is performed by using the following fixed disk-shelf configurations:

- Half-loaded disk shelves with 12 SSDs
- Fully loaded disk shelves with 24 SSDs

> Both configurations use Advanced Disk Partitioning (ADPv2). A half-loaded disk shelf supports up to nine SAP HANA hosts, whereas a fully loaded shelf supports up to 14 hosts in a single disk shelf. The SAP HANA hosts must be equally distributed between both storage controllers. The same applies to the internal disks of an AFF A700s system. The DS224C disk shelf must be connected using 12Gb SAS to support the number of SAP HANA hosts.

The 6Gb SAS disk shelf (DS2246) supports a maximum of four SAP HANA hosts. The SSDs and the SAP HANA hosts must be equally distributed between both storage controllers.

The following table summarizes the supported number of SAP HANA hosts per disk shelf.

	6Gb SAS shelves (DS2246)Fully loaded with 24 SSDs	**12Gb SAS shelves (DS224C)Half loaded with 12 SSDs and ADPv2**	**12Gb SAS shelves (DS224C)Fully loaded with 24 SSDs and ADPv2**
Maximum number of SAP HANA hosts per disk shelf	4	9	14

> This calculation is independent of the storage controller used. Adding more disk shelfs do not increase the maximum amount of SAP HANA hosts a storage controller can support.

NS224 NVMe shelf

The minimum number of 12 NVMe SSDs for the first shelf supports up to 16 SAP HANA hosts. A fully populated shelf (24 SSDs) supports up to 34 SAP HANA hosts. The same applies to the internal disks of an AFF A800 system.

> Adding more disk shelfs does not increase the maximum amount of SAP HANA hosts a storage controller can support.

Mixed workloads

SAP HANA and other application workloads running on the same storage controller or in the same storage aggregate are supported. However, it is a NetApp best practice to separate SAP HANA workloads from all

other application workloads.

You might decide to deploy SAP HANA workloads and other application workloads on either the same storage controller or the same aggregate. If so, you must make sure that adequate performance is available for SAP HANA within the mixed workload environment. NetApp also recommends that you use quality of service (QoS) parameters to regulate the effect these other applications could have on SAP HANA applications and to guarantee throughput for SAP HANA applications.

The SAP performance test tool must be used to check if additional SAP HANA hosts can be run on an existing storage controller that is already in use for other workloads. SAP application servers can be safely placed on the same storage controller and/or aggregate as the SAP HANA databases.

Capacity considerations

A detailed description of the capacity requirements for SAP HANA is in the SAP HANA Storage Requirements white paper.

The capacity sizing of the overall SAP landscape with multiple SAP HANA systems must be determined by using SAP HANA storage sizing tools from NetApp. Contact NetApp or your NetApp partner sales representative to validate the storage sizing process for a properly sized storage environment.

Configuring the performance test tool

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage system used. These parameters must also be set for the performance test tool from SAP when storage performance is being tested with the SAP performance test tool.

NetApp conducted performance tests to define the optimal values. The following table lists the parameters that must be set within the configuration file of the SAP performance test tool.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on
async_write_submit_blocks	all

For more information about the configuration of the different SAP test tools, see SAP note 1943937 for HWCCT (SAP HANA 1.0) and SAP note 2493172 for HCMT/HCOT (SAP HANA 2.0).

The following example shows how variables can be set for the HCMT/HCOT execution plan.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
```

```
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
```

```
per completion queue",
          "Name": "DataExtMaxParallelIoRequests",
          "Value": "128",
          "Request": "false"
       }, …
```

These variables must be used for the test configuration. This is usually the case with the predefined execution plans SAP delivers with the HCMT/HCOT tool. The following example for a 4k log write test is from an execution plan.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

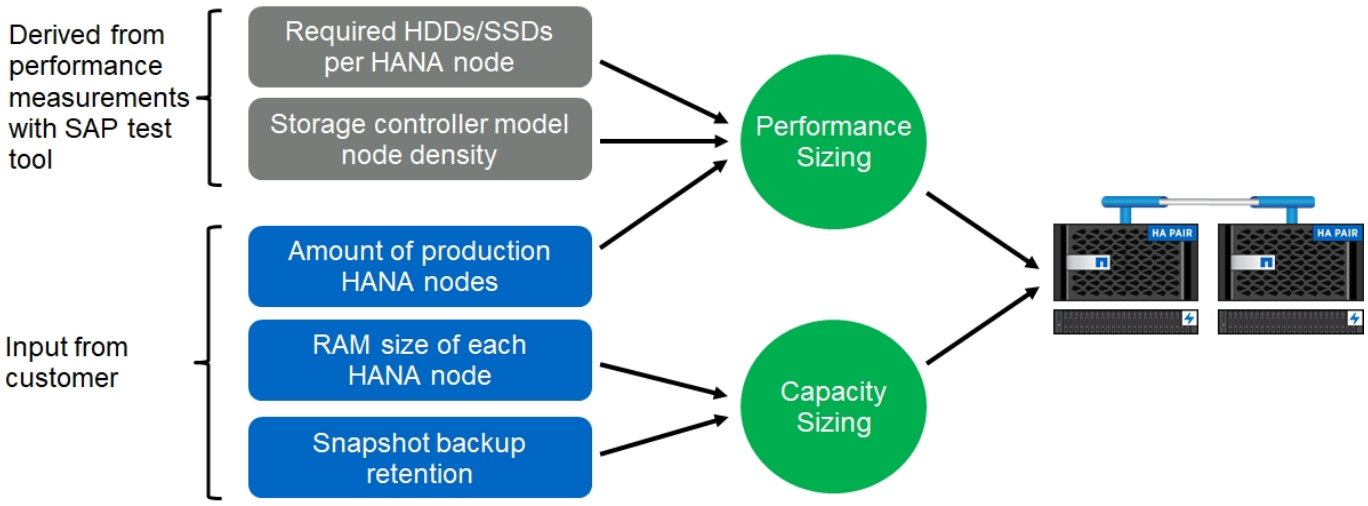
Storage sizing process overview

The number of disks per HANA host and the SAP HANA host density for each storage model were determined with performance test tool.

The sizing process requires details such as the number of production and nonproduction SAP HANA hosts, the RAM size of each host, and backup retention of the storage-based Snapshot copies. The number of SAP HANA hosts determines the storage controller and the number of disks required.

The size of the RAM, net data size on the disk of each SAP HANA host, and the Snapshot copy backup retention period are used as inputs during capacity sizing.

The following figure summarizes the sizing process.



Next: Infrastructure setup and configuration.

Overview

Previous: Storage sizing.

The following sections provide SAP HANA infrastructure setup and configuration guidelines.

Next: Network setup.

Network setup

Previous: Infrastructure setup and configuration.

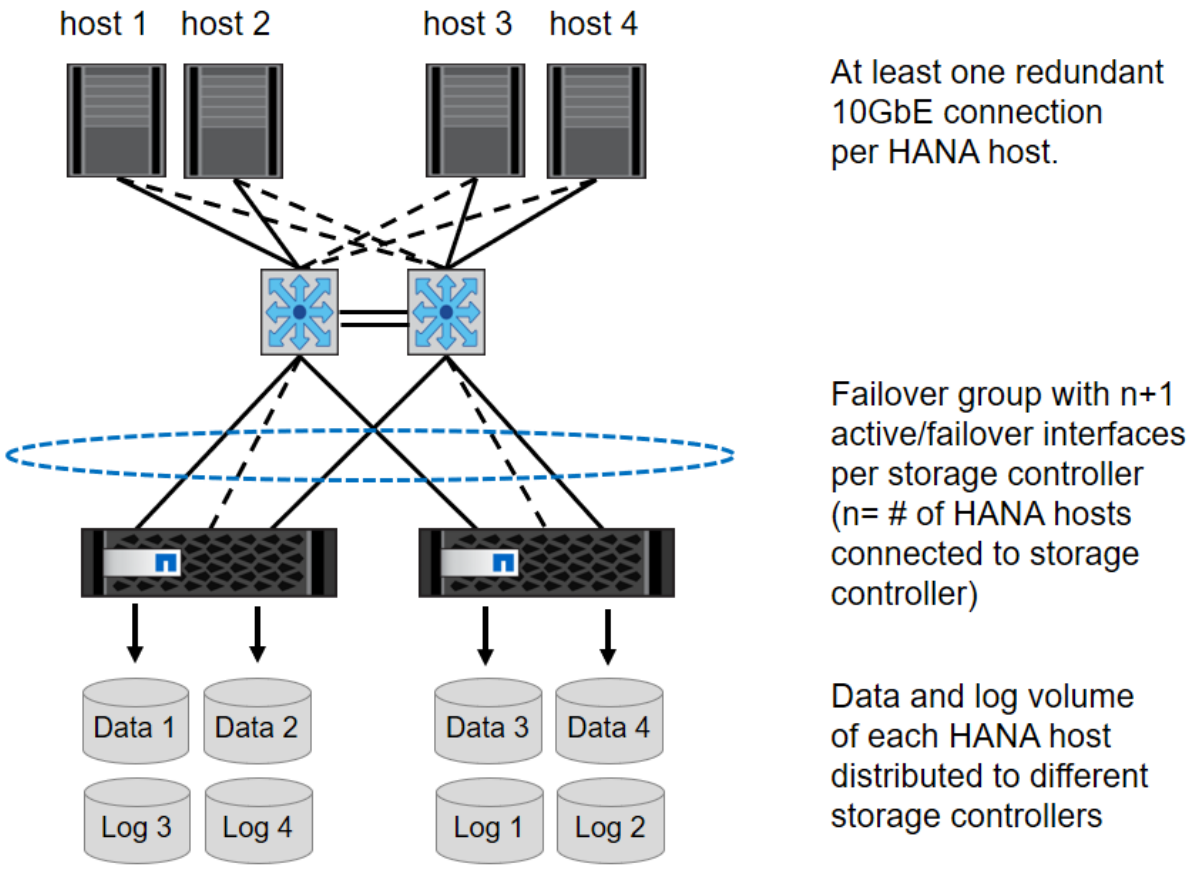
Use the following guidelines when configuring the network:

- A dedicated storage network must be used to connect the SAP HANA hosts to the storage controllers with a 10GbE or faster network.
- Use the same connection speed for storage controllers and SAP HANA hosts. If this is not possible, ensure that the network components between the storage controllers and the SAP HANA hosts are able to handle different speeds. For example, you must provide enough buffer space to allow speed negotiation at the NFS level between storage and hosts. Network components are usually switches, but other components within blade chassis, such as the back plane, must be considered as well.
- Disable flow control on all physical ports used for storage traffic on the storage network switch and host layer.
- Each SAP HANA host must have a redundant network connection with a minimum of 10Gb of bandwidth.
- Jumbo frames with a maximum transmission unit (MTU) size of 9,000 must be enabled on all network components between the SAP HANA hosts and the storage controllers.
- In a VMware setup, dedicated VMXNET3 network adapters must be assigned to each running virtual machine. Check the relevant papers mentioned in “Introduction” for further requirements.
- To avoid interference between each other, use separate network/IO paths for the log and data area.

The following figure shows an example with four SAP HANA hosts attached to a storage controller HA pair using a 10GbE network. Each SAP HANA host has an active-passive connection to the redundant fabric.

At the storage layer, four active connections are configured to provide 10Gb throughput for each SAP HANA host. In addition, one spare interface is configured on each storage controller.

At the storage layer, a broadcast domain with an MTU size of 9000 is configured, and all required physical interfaces are added to this broadcast domain. This approach automatically assigns these physical interfaces to the same failover group. All logical interfaces (LIFs) that are assigned to these physical interfaces are added to this failover group.



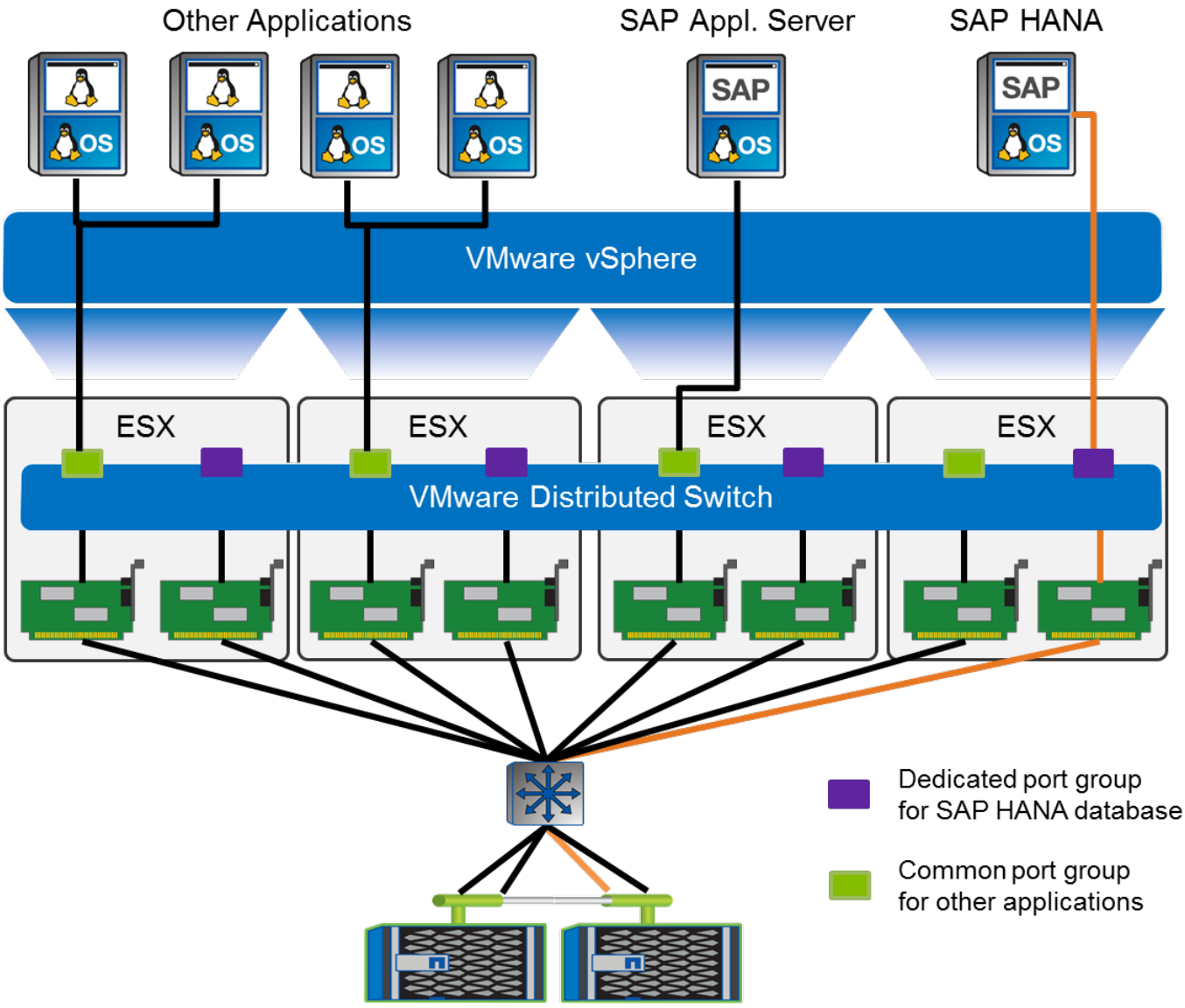
In general, it is also possible to use HA interface groups on the servers (bonds) and the storage systems (for example, Link Aggregation Control Protocol [LACP] and ifgroups). With HA interface groups, verify that the load is equally distributed between all interfaces within the group. The load distribution depends on the functionality of the network switch infrastructure.

Depending on the number of SAP HANA hosts and the connection speed used, different numbers of active physical ports are needed. For details, see the section "LIF configuration".

VMware-specific network setup

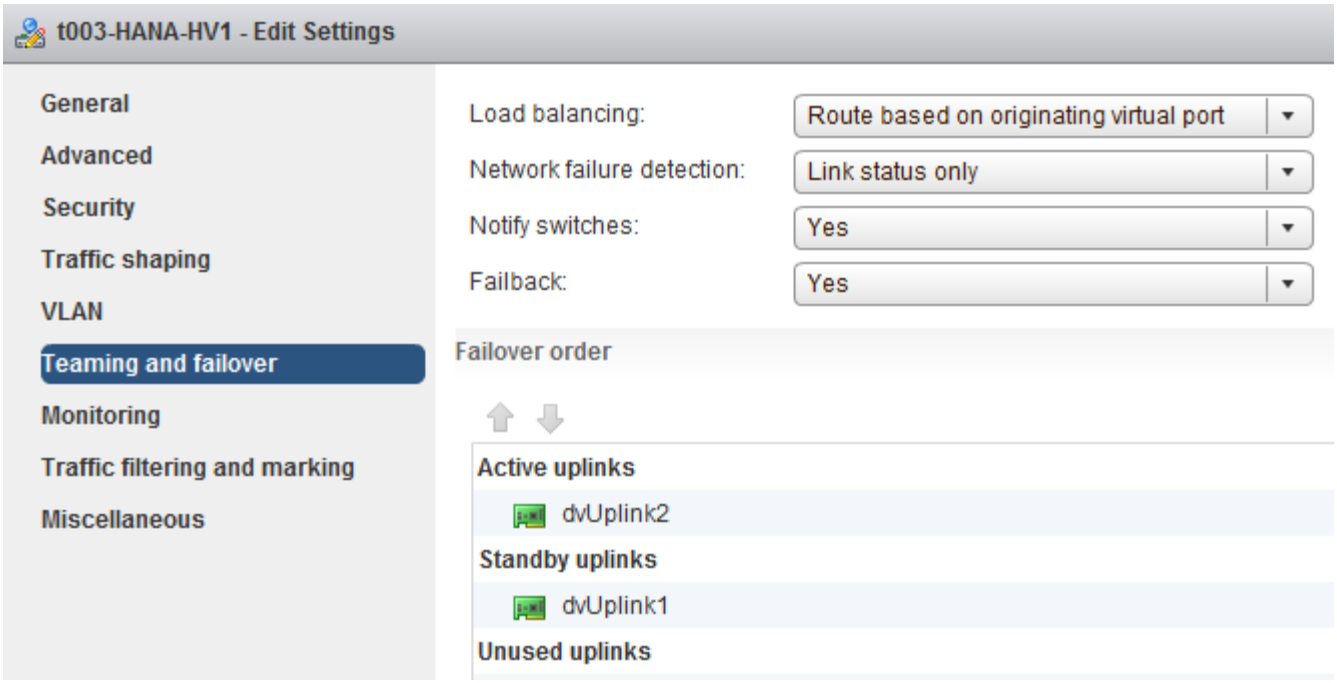
Proper network design and configuration are crucial because all data for SAP HANA instances, including performance-critical data and log volumes for the database, is provided through NFS in this solution. A dedicated storage network is used to separate the NFS traffic from communication and user access traffic between SAP HANA nodes. Each SAP HANA node requires a redundant dedicated network connection with a minimum of 10Gb of bandwidth. Higher bandwidth is also supported. This network must extend end to end

from the storage layer through network switching and computing up to the guest operating system hosted on VMware vSphere. In addition to the physical switching infrastructure, a VMware distributed switch (vDS) is used to provide adequate performance and manageability of network traffic at the hypervisor layer.



As shown in the preceding figure, each SAP HANA node uses a dedicated port group on the VMware distributed switch. This port group allows for enhanced quality of service (QoS) and dedicated assignment of physical network interface cards (NICs) on the ESX hosts. To use dedicated physical NICs while preserving HA capabilities in the event of NIC failure, the dedicated physical NIC is configured as an active uplink. Additional NICs are configured as standby uplinks in the teaming and failover settings of the SAP HANA port group. In addition, jumbo frames (MTU 9,000) must be enabled end to end on physical and virtual switches. In addition, turn off flow control on all ethernet ports used for storage traffic on servers, switches, and storage systems. The following figure shows an example of such a configuration.

LRO (large receive offload) must be turned off for interfaces used for NFS traffic. For all other network configuration guidelines, see the respective VMware best practices guides for SAP HANA.



Next: Time synchronization.

Time synchronization

Previous: Network setup.

You must synchronize the time between the storage controllers and the SAP HANA database hosts. To do so, set the same time server for all storage controllers and all SAP HANA hosts.

Next: Storage controller setup.

Storage controller setup

Previous: Time synchronization.

This section describes the configuration of the NetApp storage system. You must complete the primary installation and setup according to the corresponding ONTAP setup and configuration guides.

Storage efficiency

Inline deduplication, cross-volume inline deduplication, inline compression, and inline compaction are supported with SAP HANA in an SSD configuration.

NetApp Volume Encryption

The use of NetApp Volume Encryption (NVE) is supported with SAP HANA.

Quality of Service

QoS can be used to limit the storage throughput for specific SAP HANA systems or other applications on a shared-use controller. One use case would be to limit the throughput of development and test systems so that they cannot influence production systems in a mixed setup.

During the sizing process, you should determine the performance requirements of a nonproduction system.

Development and test systems can be sized with lower performance values, typically in the range of 20% to 50% of a production- system KPI as defined by SAP.

Starting with ONTAP 9, QoS is configured on the storage volume level and uses maximum values for throughput (MBps) and the amount of I/O (IOPS).

Large write I/O has the biggest performance effect on the storage system. Therefore, the QoS throughput limit should be set to a percentage of the corresponding write SAP HANA storage performance KPI values in the data and log volumes.

NetApp FabricPool

NetApp FabricPool technology must not be used for active primary file systems in SAP HANA systems. This includes the file systems for the data and log area as well as the `/hana/shared` file system. Doing so results in unpredictable performance, especially during the startup of an SAP HANA system.

Using the “snapshot-only” tiering policy is possible as well as using FabricPool in general at a backup target such as a NetApp SnapVault or SnapMirror destination.

Using FabricPool for tiering Snapshot copies at primary storage or using FabricPool at a backup target changes the required time for the restore and recovery of a database or other tasks such as creating system clones or repair systems. Take this into consideration for planning your overall lifecycle-management strategy and check to make sure that your SLAs are still being met while using this function.

FabricPool is a good option for moving log backups to another storage tier. Moving backups affects the time needed to recover an SAP HANA database. Therefore, the option “tiering-minimum-cooling-days” should be set to a value that places log backups, which are routinely needed for recovery, on the local fast storage tier.

Storage configuration

The following overview summarizes the required storage configuration steps. Each step is covered in detail in the subsequent sections. In this section, we assume that the storage hardware is set up and that the ONTAP software is already installed. Also, the connections between the storage ports (10GbE or faster) and the network must already be in place.

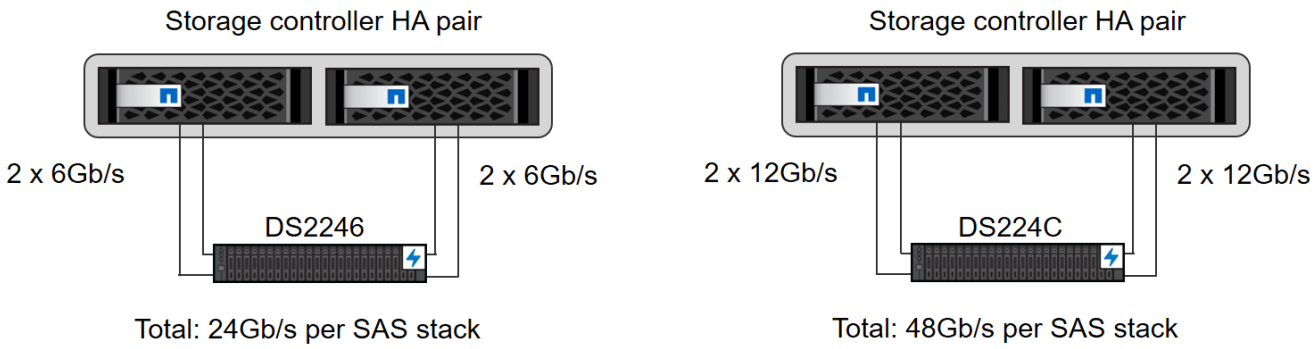
1. Check the correct disk shelf configuration as described in "Disk shelf connection."
2. Create and configure the required aggregates as described in "Aggregate configuration."
3. Create a storage virtual machine (SVM) as described in "SVM configuration."
4. Create LIFs as described in "LIF configuration."
5. Create volumes within the aggregates as described in "[Volume configuration for SAP HANA single host systems]" and "[Volume configuration for SAP HANA multiple host systems]."
6. Set the required volume options as described in "Volume options."
7. Set the required options for NFSv3 as described in "NFS configuration for NFSv3" or for NFSv4 as described in "NFS configuration for NFSv4."
8. Mount the volumes to namespace and set export policies as described in "Mount volumes to namespace and set export policies."

Disk shelf connection

SAS disk shelves

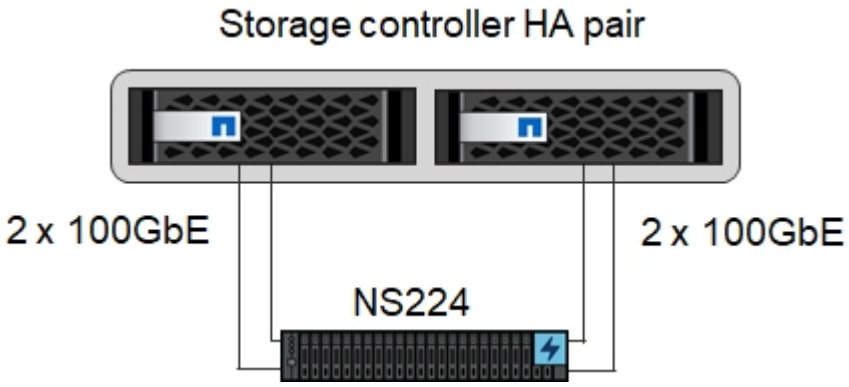
A maximum of one disk shelf can be connected to one SAS stack to provide the required performance for the SAP HANA hosts, as shown in the following figure. The disks within each shelf must be distributed equally to both controllers of the HA pair. ADPv2 is used with ONTAP 9 and the DS224C disk shelves.

With the DS224C disk shelf, quad-path SAS cabling can also be used but is not required.



NVMe (100GbE) disk shelves

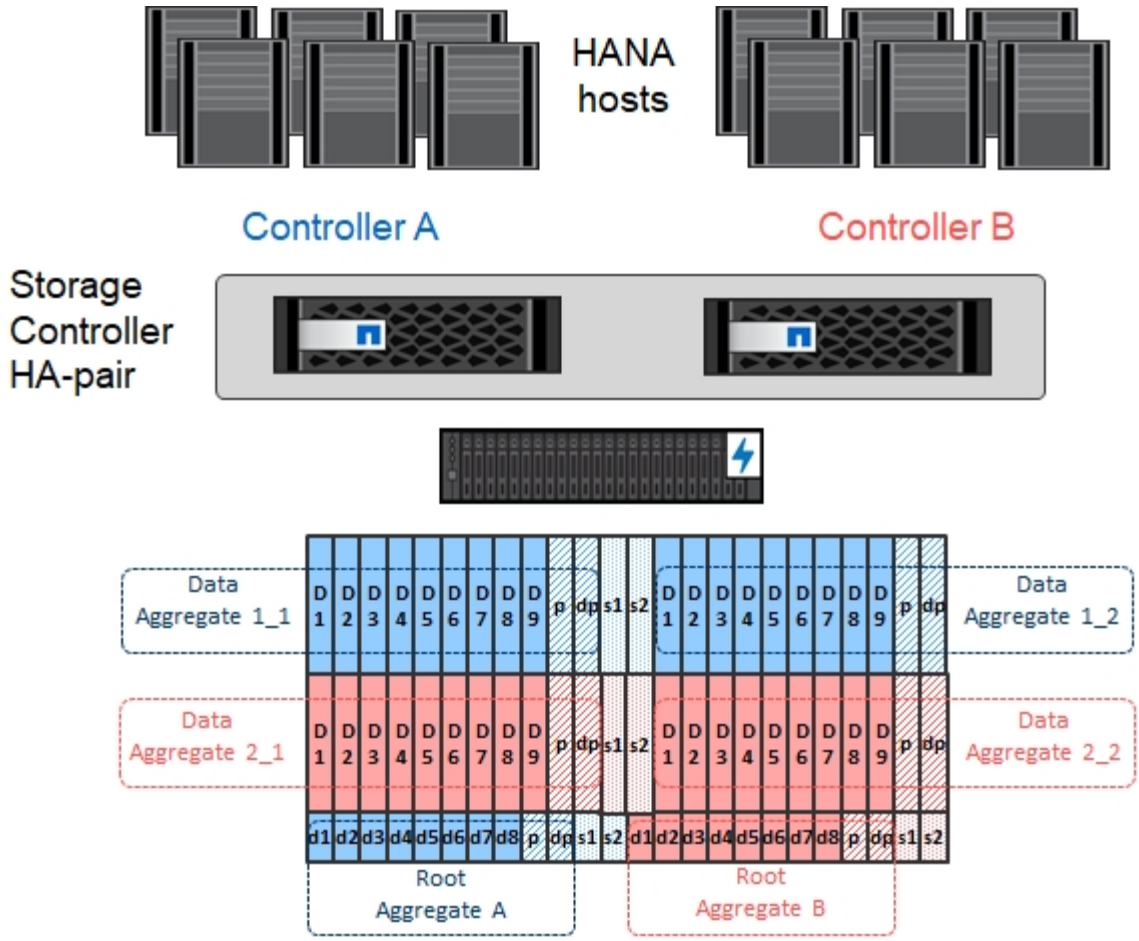
Each NS224 NVMe disk shelf is connected using two 100GbE ports per controller. The disks within each shelf must be distributed equally to both controllers of the HA pair. ADPv2, as described in the aggregate configuration chapter, is also used for the NS224 disk shelf. The following figure depicts the disk shelf connection with an NVMe drive.



Aggregate configuration

In general, you must configure two aggregates per controller, independent of the disk shelf or drive technology (SAS SSDs or NVMe SSDs) that is used. This step is necessary so that you can use all available controller resources. For AFF A200 series systems, one data aggregate is enough.

The following image shows a configuration of 12 SAP HANA hosts running on a 12Gb SAS shelf configured with ADPv2. Six SAP HANA hosts are attached to each storage controller. Four separate aggregates, two at each storage controller, are configured. Each aggregate is configured with 11 disks with nine data and two parity disk partitions. For each controller, two spare partitions are available.



SVM configuration

Multiple SAP landscapes with SAP HANA databases can use a single SVM. An SVM can also be assigned to each SAP landscape, if necessary, in case they are managed by different teams within a company.

If there is a QoS profile automatically created and assigned while creating a new SVM, remove this automatically created profile from the SVM to enable the required performance for SAP HANA:

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

LIF configuration

For SAP HANA production systems, you must use different LIFs to mount the data volume and the log volume from the SAP HANA host. Therefore at least two LIFs are required.

The data and log volume mounts of different SAP HANA hosts can share a physical storage network port by either using the same LIFs or by using individual LIFs for each mount.

The maximum amount of data and log volume mounts per physical interface are shown in the following table.

Ethernet port speed	10GbE	25GbE	40GbE	100GeE
Maximum number of log or data volume mounts per physical port	2	6	12	24

Sharing one LIF between different SAP HANA hosts might require a remount of data or log volumes to a different LIF. This change avoids performance penalties if a volume is moved to a different storage controller.

Development and test systems can use more data and volume mounts or LIFs on a physical network interface.

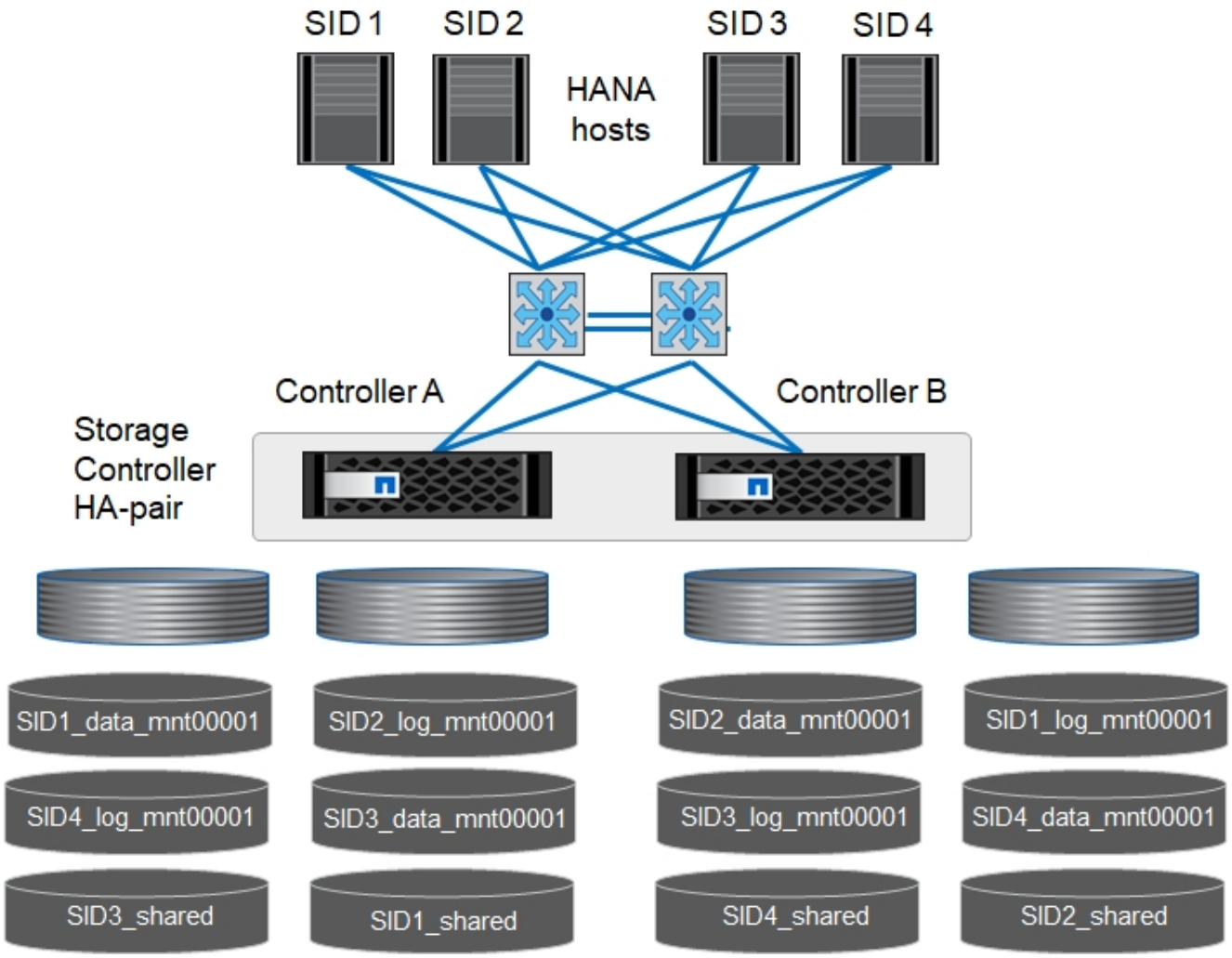
For production, development, and test systems, the `/hana/shared` file system can use the same LIF as the data or log volume.

Volume configuration for SAP HANA single-host systems

The following figure shows the volume configuration of four single-host SAP HANA systems. The data and log volumes of each SAP HANA system are distributed to different storage controllers. For example, volume `SID1_data_mnt00001` is configured on controller A, and volume `SID1_log_mnt00001` is configured on controller B.

If only one storage controller of an HA pair is used for the SAP HANA systems, data and log volumes can also be stored on the same storage controller.

If the data and log volumes are stored on the same controller, access from the server to the storage must be performed with two different LIFs: one LIF to access the data volume and the other to access the log volume.



For each SAP HANA host, a data volume, a log volume, and a volume for `/hana/shared` are configured. The following table shows an example configuration for single-host SAP HANA systems.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller b
Data, log, and shared volumes for system SID1	Data volume: SID1_data_mnt00001	Shared volume: SID1_shared	–	Log volume: SID1_log_mnt00001
Data, log, and shared volumes for system SID2	–	Log volume: SID2_log_mnt00001	Data volume: SID2_data_mnt00001	Shared volume: SID2_shared
Data, log, and shared volumes for system SID3	Shared volume: SID3_shared	Data volume: SID3_data_mnt00001	Log volume: SID3_log_mnt00001	–
Data, log, and shared volumes for system SID4	Log volume: SID4_log_mnt00001	–	Shared volume: SID4_shared	Data volume: SID4_data_mnt00001

The following table shows an example of the mount point configuration for a single-host system. To place the home directory of the `sidadm` user on the central storage, the `/usr/sap/SID` file system should be mounted

from the `SID_shared` volume.

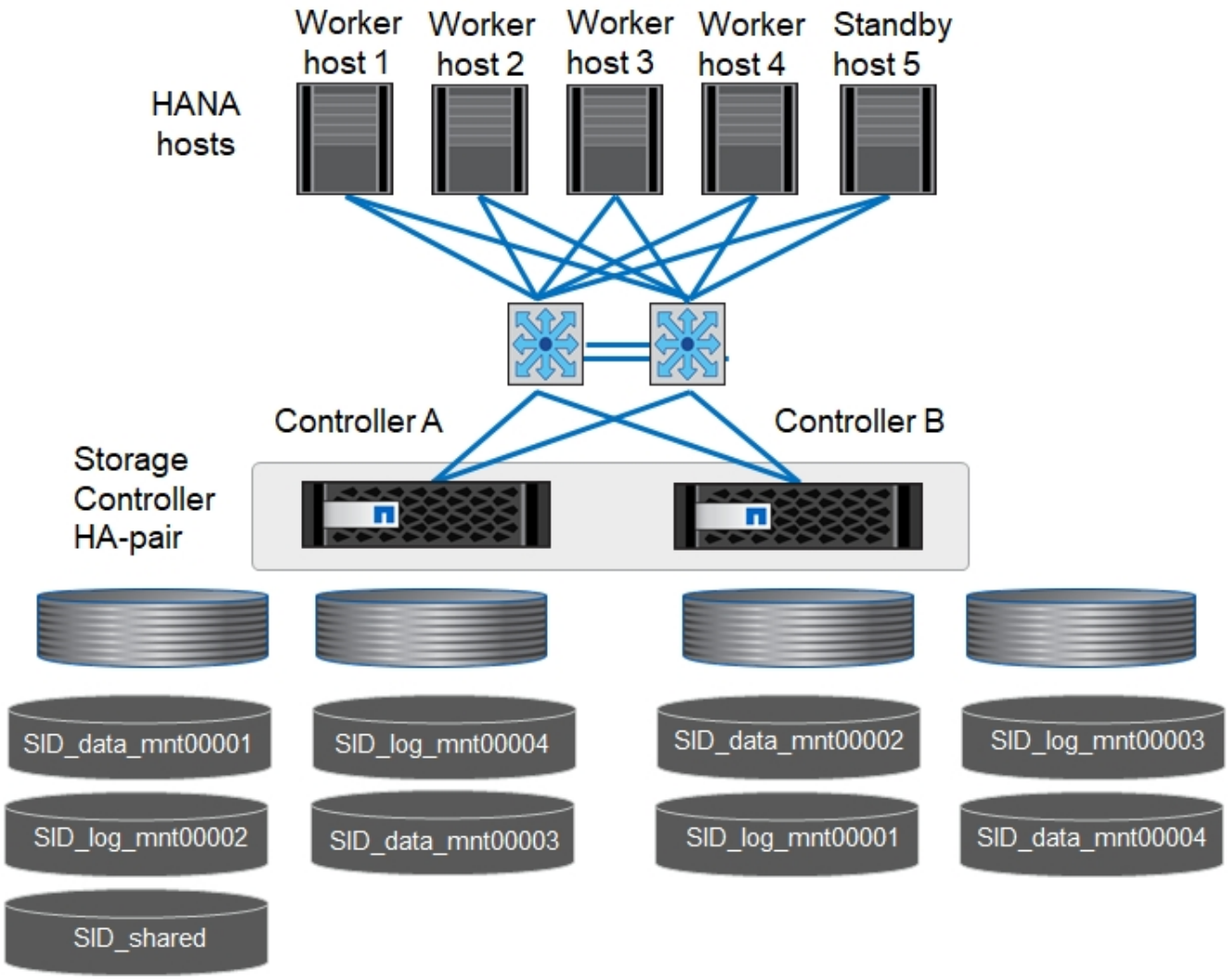
Junction path	Directory	Mount point at HANA host
SID_data_mnt00001		/hana/data/SID/mnt00001
SID_log_mnt00001		/hana/log/SID/mnt00001
SID_shared	usr-sap shared	/usr/sap/SID /hana/shared/

Volume configuration for SAP HANA multiple-host systems

The following figure shows the volume configuration of a 4+1 SAP HANA system. The data and log volumes of each SAP HANA host are distributed to different storage controllers. For example, volume `SID1_data1_mnt00001` is configured on controller A, and volume `SID1_log1_mnt00001` is configured on controller B.

If only one storage controller of an HA pair is used for the SAP HANA system, the data and log volumes can also be stored on the same storage controller.

If the data and log volumes are stored on the same controller, access from the server to the storage must be performed with two different LIFs: one LIF to access the data volume and one to access the log volume.



For each SAP HANA host, a data volume and a log volume are created. The `/hana/shared` volume is used by all hosts of the SAP HANA system. The following table shows an example configuration for a multiple-host SAP HANA system with four active hosts.

Purpose	Aggregate 1 at controller A	Aggregate 2 at controller A	Aggregate 1 at controller B	Aggregate 2 at controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	–	Log volume: SID_log_mnt00001	–
Data and log volumes for node 2	Log volume: SID_log_mnt00002	–	Data volume: SID_data_mnt00002	–
Data and log volumes for node 3	–	Data volume: SID_data_mnt00003	–	Log volume: SID_log_mnt00003
Data and log volumes for node 4	–	Log volume: SID_log_mnt00004	–	Data volume: SID_data_mnt00004
Shared volume for all hosts	Shared volume: SID_shared			

The following table shows the configuration and the mount points of a multiple-host system with four active SAP HANA hosts. To place the home directories of the `sidadm` user of each host on the central storage, the

`/usr/sap/SID` file systems are mounted from the `SID_shared` volume.

Junction path	Directory	Mount point at SAP HANA host	Note
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Mounted at all hosts
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Mounted at all hosts
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Mounted at all hosts
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Mounted at all hosts
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Mounted at all hosts
SID_log_mnt00003	–	/hana/log/SID/mnt00003	Mounted at all hosts
SID_data_mnt00004	–	/hana/data/SID/mnt00004	Mounted at all hosts
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Mounted at all hosts
SID_shared	shared	/hana/shared/SID	Mounted at all hosts
SID_shared	usr-sap-host1	/usr/sap/SID	Mounted at host 1
SID_shared	usr-sap-host2	/usr/sap/SID	Mounted at host 2
SID_shared	usr-sap-host3	/usr/sap/SID	Mounted at host 3
SID_shared	usr-sap-host4	/usr/sap/SID	Mounted at host 4
SID_shared	usr-sap-host5	/usr/sap/SID	Mounted at host 5

Volume options

You must verify and set the volume options listed in the following table on all SVMs. For some of the commands, you must switch to the advanced privilege mode within ONTAP.

Action	Command
Disable visibility of Snapshot directory	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false
Disable automatic Snapshot copies	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disable access time update, except of the SID_shared volume	set advanced vol modify -vserver <vserver-name> -volume <volname> -atime-update false set admin

NFS configuration for NFSv3

The NFS options listed in the following table must be verified and set on all storage controllers. For some of the commands shown in this table, you must switch to the advanced privilege mode.

Action	Command
Enable NFSv3	nfs modify -vserver <vserver-name> v3.0 enabled

Action	Command
ONTAP 9: Set NFS TCP maximum transfer size to 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer -size 1048576 set admin
ONTAP 8: Set NFS read and write size to 64KB	set advanced nfs modify -vserver <vserver-name> -v3-tcp-max-read -size 65536 nfs modify -vserver <vserver-name> -v3-tcp-max-write -size 65536 set admin

NFS configuration for NFSv4

The NFS options listed in the following table must be verified and set on all SVMs.

For some of the commands in this table, you must switch to the advanced privilege mode.

Action	Command
Enable NFSv4	nfs modify -vserver <vserver-name> -v4.1 enabled
ONTAP 9: Set NFS TCP maximum transfer size to 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin
ONTAP 8: Set NFS read and write size to 64KB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer-size 65536 set admin
Disable NFSv4 access control lists (ACLs)	nfs modify -vserver <vserver_name> -v4.1-acl disabled
Set NFSv4 domain ID	nfs modify -vserver <vserver_name> -v4-id-domain <domain-name>
Disable NFSv4 read delegation	nfs modify -vserver <vserver_name> -v4.1-read -delegation disabled
Disable NFSv4 write delegation	nfs modify -vserver <vserver_name> -v4.1-write -delegation disabled
Disable NFSv4 numeric ids	nfs modify -vserver <vserver_name> -v4-numeric-ids disabled

For NFS version 4. 0, replace `4.1` with `4.0` in the previous commands. While NFSv4.0 is supported, NFSv4.1 is preferred.

The NFSv4 domain ID must be set to the same value on all Linux servers (`/etc/idmapd.conf`) and SVMs, as described in the section “SAP HANA installation preparations for NFSv4.”

If you are using NFSV4.1, then pNFS is enabled and used by default (recommended).

Set the NFSv4 lease time at the SVM (as shown in the following table) if SAP HANA multiple host system are used.

Action	Command
Set the NFSv4 lease time	set advanced nfs modify -vserver <vserver_name> -v4-lease -seconds 10 set admin

Starting with HANA 2.0 SPS4, HANA provides parameters to control failover behavior. Instead of setting the lease time at the SVM level, NetApp recommends using these HANA parameters.

The parameters are within `nameserver.ini` as shown in the following table. Keep the default retry interval of 10 seconds within these sections.

Section within nameserver.ini	Parameter	Value
failover	normal_retries	9
distributed_watchdog	deactivation_retries	11
distributed_watchdog	takeover_retries	9

Mount volumes to namespace and set export policies

When a volume is created, the volume must be mounted to the namespace. In this document, we assume that the junction path name is the same as the volume name. By default, the volume is exported with the default policy. The export policy can be adapted if required.

Next: Host setup.

Host setup

Previous: Storage controller setup.

All the host-setup steps described in this section are valid for both SAP HANA environments on physical servers and for SAP HANA running on VMware vSphere.

Configuration parameter for SUSE Linux Enterprise Server

Additional kernel and configuration parameters at each SAP HANA host must be adjusted for the workload generated by SAP HANA.

SUSE Linux Enterprise Server 12 and 15

Starting with SUSE Linux Enterprise Server 12 SP1, the kernel parameter must be set in a configuration file in the `/etc/sysctl.d` directory. For example, you must create a configuration file with the name `91-NetApp-HANA.conf`.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

Saptune, included in SLES for SAP OS versions, can be used to set these values. For more information, see SAP Note 3024346 (requires SAP login).

If NFSv3 is used for connecting the storage, `sunrpc.tcp_max_slot_table_entries` must be set in `/etc/modprobe.d/sunrpc.conf`. If the file does not exist, you must first create it by adding the following line:

```
options sunrpc tcp_max_slot_table_entries=128
```

If the nconnect mount option is used, this value can be increased from 256 to 512.

Configuration parameters for Red Hat Enterprise Linux 7.2 or later

You must adjust additional kernel and configuration parameters at each SAP HANA host for the workload generated by SAP HANA.

If NFSv3 is used for connecting the storage, you must set the parameter `sunrpc.tcp_max_slot_table_entries parameter` in `/etc/modprobe.d/sunrpc.conf`. If the file does not exist, you must first create it by adding the following line:

```
options sunrpc tcp_max_slot_table_entries=128
```

If the nconnect mount option is used, this value can be increased from 256 to 512.

Starting with Red Hat Enterprise Linux 7.2, you must set the kernel parameters in a configuration file in the `/etc/sysctl.d` directory. For example, you must create a configuration file with the name `91-NetApp-HANA.conf`.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

Create subdirectories in /hana/shared volume

The following examples show an SAP HANA database with SID=NF2.

To create the required subdirectories, take one of the following actions:

- For a single- host system, mount the `/hana/shared` volume and create the `shared` and `usr-sap` subdirectories.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- For a multiple-host system, mount the `/hana/shared` volume and create the `shared` and the `usr-sap` subdirectories for each host.

  The example commands show a 2+1 multiple-host HANA system.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

Create mount points

The following examples show an SAP HANA database with SID=NF2.

To create the required mount point directories, take one of the following actions:

- For a single-host system, create mount points and set the permissions on the database host.

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- For a multiple-host system, create mount points and set the permissions on all worker and standby hosts. The following example commands are for a 2+1 multiple-host HANA system.
  - First worker host:

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- Second worker host:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- Standby host:

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

Mount file systems

Different mount options must be used depending on the NFS version and ONTAP release. The following file systems must be mounted to the hosts:

- `/hana/data/SID/mnt0000*`
- `/hana/log/SID/mnt0000*`
- `/hana/shared`
- `/usr/sap/SID`

The following table shows the NFS versions that you must use for the different files systems for single-host and multiple-host SAP HANA databases.

File systems	SAP HANA single host	SAP HANA multiple hosts
/hana/data/SID/mnt0000*	NFSv3 or NFSv4	NFSv4
/hana/log/SID/mnt0000*	NFSv3 or NFSv4	NFSv4
/hana/shared	NFSv3 or NFSv4	NFSv3 or NFSv4
/usr/sap/SID	NFSv3 or NFSv4	NFSv3 or NFSv4

The following table shows the mount options for the various NFS versions and ONTAP releases. The common parameters are independent of the NFS and ONTAP versions.

SAP LaMa requires the /usr/sap/SID directory to be local. Therefore, don’t mount an NFS volume for /usr/sap/SID if you are using SAP LaMa.

For NFSv3, you must switch off NFS locking to avoid NFS lock cleanup operations in case of a software or server failure.

With ONTAP 9, the NFS transfer size can be configured up to 1MB. Specifically, with 40GbE or faster connections to the storage system, you must set the transfer size to 1MB to achieve the expected throughput values.

Common parameter	NFSv3	NFSv4	NFSv4.1	NFS transfer size with ONTAP 9	NFS transfer size with ONTAP 8
rw, bg, hard, timeo=600, noatime	vers=3,nolock	vers=4,minorversion=0,lock	vers=4,minorversion=1,lock	rsize=1048576,wsize=1048576	rsize=65536,wsize=65536

To improve read performance with NFSv3, NetApp recommends that you use the `nconnect=n` mount option, which is available with SUSE Linux Enterprise Server 12 SP4 or later and RedHat Enterprise Linux (RHEL) 8.3 or later.

Performance tests showed that `nconnect=8` provides good read results. Log writes might benefit from a lower number of sessions, such as `nconnect=2`. Be aware that the first mount from an NFS server (IP address) defines the amount of sessions being used. Further mounts do not change this even if different values are used for nconnect.

For NFSv4, the nconnect option is supported by NetApp for NFSv4.1, starting with ONTAP 9.8. First NFS clients supporting nconnect with NFSv4.1 are available with SLES15SP2 and RHEL 8.3. For additional information check Linux vendor documentation.

The following example shows a single host SAP HANA database with SID=NF2 using NFSv3 and an NFS transfer size of 1MB. To mount the file systems during system boot with the `/etc/fstab` configuration file, complete the following steps:

1. Add the required file systems to the `/etc/fstab` configuration file.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage- vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-data01>:/NF2_shared/usr- sap /usr/sap/NF2 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
```

2. Run `mount -a` to mount the file systems on all hosts.

The next example shows a multiple-host SAP HANA database with SID=NF2 using NFSv4.1 for data and log file systems and NFSv3 for the `/hana/shared` and `/usr/sap/NF2` file systems. An NFS transfer size of 1MB is used.

1. Add the required file systems to the `/etc/fstab` configuration file on all hosts.

The /usr/sap/NF2 file system is different for each database host. The following example shows /NF2_shared/usr- sap- host1.

```
stlrx300s8-5:/ # cat /etc/fstab
<storage- vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw, vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576,
bg, noatime,lock 0 0
<storage- vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-data02>:/NF2_shared/usr- sap- host1 /usr/sap/NF2 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
```

2. Run mount -a to mount the file systems on all hosts.

Next: SAP HANA installation preparations for NFSv4.

SAP HANA installation preparations for NFSv4

Previous: Host setup.

NFS version 4 and higher requires user authentication. This authentication can be accomplished by using a central user management tool such as a Lightweight Directory Access Protocol (LDAP) server or with local user accounts. The following sections describe how to configure local user accounts.

The administration user <sidadm> and the sapsys group must be created manually on the SAP HANA hosts and the storage controllers before the installation of the SAP HANA software begins.

SAP HANA hosts

If it does not already exist, you must create the sapsys group on the SAP HANA host. Choose a unique group ID that does not conflict with the existing group IDs on the storage controllers.

The user <sidadm> is created on the SAP HANA host. A unique ID must be chosen that does not conflict with existing user IDs on the storage controllers.

For a multiple-host SAP HANA system, the user and group ID must be the same on all SAP HANA hosts. The group and user are created on the other SAP HANA hosts by copying the affected lines in /etc/group and

`/etc/passwd` from the source system to all other SAP HANA hosts.

The NFSv4 domain must be set to the same value on all Linux servers and SVMs. Set the domain parameter "`Domain = <domain_name>`" in file `/etc/idmapd.conf` for the Linux hosts.

Enable and start the NFS idmapd service:

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

The latest Linux kernels do not require this step. You can safely ignore warning messages.

Storage controllers

The user ID and group ID must be the same on the SAP HANA hosts and the storage controllers. The group and user are created by entering the following commands on the storage cluster:

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

Additionally, set the group ID of the UNIX user root of the SVM to 0.

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

Next: I/O stack configuration for SAP HANA.

I/O stack configuration for SAP HANA

Previous: SAP HANA installation preparations for NFSv4.

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage systems used.

NetApp conducted performance tests to define the ideal values. The following table lists the optimal values inferred from the performance tests.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on

Parameter	Value
async_write_submit_blocks	all

For SAP HANA 1.0 versions up to SPS12, these parameters can be set during the installation of the SAP HANA database, as described in SAP note 2267798: Configuration of the SAP HANA Database During Installation Using hdbparam.

Alternatively, the parameters can be set after SAP HANA database installation by using the `hdbparam` framework.

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Starting with SAP HANA 2.0, `hdbparam` was deprecated and the parameters were moved to `global.ini`. The parameters can be set using SQL commands or SAP HANA Studio. For more details, see SAP note 2399079: Elimination of hdbparam in HANA 2. The parameters can also be set within the global.ini as shown below:

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

As of SAP HANA 2.0 SPS5, you can use the `setParameter.py` script to set the correct parameters:

```
nf2adm@sapcc-hana-tst-03:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Next: SAP HANA data volume size.

SAP HANA data volume size

Previous: I/O stack configuration for SAP HANA.

As the default, SAP HANA uses only one data volume per SAP HANA service. Due to the maximum file size limitation of the file system, NetApp recommends limiting the maximum data volume size.

To do so automatically, set the following parameter in `global.ini` in the section `[persistence]`:

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

This creates a new data volume after the 8,000GB limit is reached. SAP note 240005 question 15 provides more information.

Next: SAP HANA software installation.

SAP HANA software installation

Previous: SAP HANA data volume size.

Install on a single-host system

SAP HANA software installation does not require any additional preparation for a single-host system.

Install on a multiple-host system

To install SAP HANA on a multiple-host system, complete the following steps:

1. Using the SAP `hdbclm` installation tool, start the installation by running the following command at one of the worker hosts. Use the `addhosts` option to add the second worker (`sapcc-hana-tst-07`) and the standby host (`sapcc-hana-tst-08`).

```
sapcc-hana-tst-06:/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_LCM_LINUX_X86_64 # ./hdblcm --action=install
--addhosts=sapcc-hana-tst-07:role=worker,sapcc-hana-tst-08:role=standby



SAP HANA Lifecycle Management - SAP HANA Database 2.00.052.00.1599235305
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.052.0000.1599259237) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
```

```
52/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.052.00.1599235305) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.5.109.1598303414) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
    SAP HANA Smart Data Access (2.00.5.000.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/SAP_HANA_SDA_20_LINUX_X86_64/packages
    SAP HANA Studio (2.3.54.000000) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.4.24.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.0.130.519) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.014.1) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI14_1.zip
    XSAC FILEPROCESSOR 1.0 (1.000.85) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_85.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.012.20341) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_HRTT_20/XSACHRTT12_20341.zip
    XS Messaging Service 1 (1.004.10) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACMESSSRV04_10.zip
    Develop and run portal services for customer apps on XSA (1.005.1)
in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV05_1.zip
    SAP Web IDE Web Client (4.005.1) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE05_1.zip
    XS JOB SCHEDULER 1.0 (1.007.12) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_12.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.25) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_25.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.3) in
```

```
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_3.zip
    XSA Cockpit 1 (1.001.17) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_17.zip


SAP HANA Database version '2.00.052.00.1599235305' will be installed.

Select additional components for installation:

  Index | Components | Description

-------------------------------------------------------------------------
---------------------
  1     | all        | All components
  2     | server     | No additional components
  3     | client     | Install SAP HANA Database Client version
2.5.109.1598303414
  4     | lss        | Install SAP HANA Local Secure Store version
2.4.24.0
  5     | studio     | Install SAP HANA Studio version 2.3.54.000000
  6     | smartda    | Install SAP HANA Smart Data Access version
2.00.5.000.0
  7     | xs         | Install SAP HANA XS Advanced Runtime version
1.0.130.519
  8     | afl        | Install SAP HANA AFL (incl.PAL,BFL,OFL) version
2.00.052.0000.1599259237
  9     | eml        | Install SAP HANA EML AFL version
2.00.052.0000.1599259237
  10    | epmmds     | Install SAP HANA EPM-MDS version
2.00.052.0000.1599259237

Enter comma-separated list of the selected indices [3]: 2,3
Enter Installation Path [/hana/shared]:
```

2. Verify that the installation tool installed all selected components at all worker and standby hosts.

Next: Adding additional data volume partitions.

Adding additional data volume partitions

Previous: SAP HANA software installation.

Starting with SAP HANA 2.0 SPS4, additional data volume partitions can be configured. This allows you to configure two or more volumes for the data volume of an SAP HANA tenant database and scale beyond the size and performance limits of a single volume.

Using two or more individual volumes for the data volume is available for SAP HANA single-host and SAP HANA multiple-host systems. You can add additional data volume partitions at any time.

Enabling additional data volume partitions

To enable additional data volume partitions, add the following entry within `global.ini` by using SAP HANA Studio or Cockpit in the SYSTEMDB configuration.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

Adding the parameter manually to the `global.ini` file requires the restart of the database.

Volume configuration for single-host SAP HANA systems

The layout of volumes for a single-host SAP HANA system with multiple partitions is like the layout for a system with one data volume partition but with an additional data volume stored on a different aggregate as the log volume and the other data volume. The following table shows an example configuration of an SAP HANA single-host system with two data volume partitions.

Aggregate 1 at controller A	Aggregate 2 at controller A	Aggregate 1 at controller B	Aggregate 2 at controller b
Data volume: SID_data_mnt00001	Shared volume: SID_shared	Data volume: SID_data2_mnt00001	Log volume: SID_log_mnt00001

The following table shows an example of the mount point configuration for a single-host system with two data volume partitions.

Junction path	Directory	Mount point at HANA host
SID_data_mnt00001	–	/hana/data/SID/mnt00001
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001
SID_log_mnt00001	–	/hana/log/SID/mnt00001
SID_shared	usr-sap shared	/usr/sap/SID /hana/shared

You can create the new data volume and mount it to the namespace using either NetApp ONTAP System Manager or the ONTAP CLI.

Volume configuration for multiple-host SAP HANA systems

The layout of volumes is like the layout for a multiple- host SAP HANA system with one data volume partition but with an additional data volume stored on a different aggregate as log volume and the other data volume. The following table shows an example configuration of an SAP HANA multiple-host system with two data volume partitions.

Purpose	Aggregate 1 at controller A	Aggregate 2 at controller A	Aggregate 1 at controller B	Aggregate 2 at controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	–	Log volume: SID_log_mnt00001	Data2 volume: SID_data2_mnt00001
Data and log volumes for node 2	Log volume: SID_log_mnt00002	Data2 volume: SID_data2_mnt00002	Data volume: SID_data_mnt00002	–
Data and log volumes for node 3	–	Data volume: SID_data_mnt00003	Data2 volume: SID_data2_mnt00003	Log volume: SID_log_mnt00003
Data and log volumes for node 4	Data2 volume: SID_data2_mnt00004	Log volume: SID_log_mnt00004	–	Data volume: SID_data_mnt00004
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

The following table shows an example of the mount point configuration for a single-host system with two data volume partitions.

Junction path	Directory	Mount point at SAP HANA host	Note
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Mounted at all hosts
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001	Mounted at all hosts
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Mounted at all hosts
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Mounted at all hosts
SID_data2_mnt00002	–	/hana/data2/SID/mnt00002	Mounted at all hosts
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Mounted at all hosts
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Mounted at all hosts
SID_data2_mnt00003		/hana/data2/SID/mnt00003	Mounted at all hosts
SID_log_mnt00003		/hana/log/SID/mnt00003	Mounted at all hosts
SID_data_mnt00004		/hana/data/SID/mnt00004	Mounted at all hosts
SID_data2_mnt00004	–	/hana/data2/SID/mnt00004	Mounted at all hosts
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Mounted at all hosts
SID_shared	shared	/hana/shared/SID	Mounted at all hosts
SID_shared	usr-sap-host1	/usr/sap/SID	Mounted at host 1
SID_shared	usr-sap-host2	/usr/sap/SID	Mounted at host 2

Junction path	Directory	Mount point at SAP HANA host	Note
SID_shared	usr-sap-host3	/usr/sap/SID	Mounted at host 3
SID_shared	usr-sap-host4	/usr/sap/SID	Mounted at host 4
SID_shared	usr-sap-host5	/usr/sap/SID	Mounted at host 5

You can create the new data volume and mount it to the namespace using either ONTAP System Manager or the ONTAP CLI.

Host configuration

In addition to the tasks described in the section "Host Setup," the additional mount points and `fstab` entries for the new additional data volume/s must be created and the new volumes must be mounted.

1. Create additional mount points.
   - For a single-host system, create mount points and set the permissions on the database host:

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - For a multiple-host system, create mount points and set the permissions on all worker and standby hosts.

     The following example commands are for a 2-plus-1 multiple-host HANA system.

     - First worker host:

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - Second worker host:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

     - Standby host:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

2. Add the additional file systems to the `/etc/fstab` configuration file on all hosts.

   See the following example for a single-host system using NFSv4.1:

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw,
vers=4minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576,bg,noati
me,lock 0 0
```

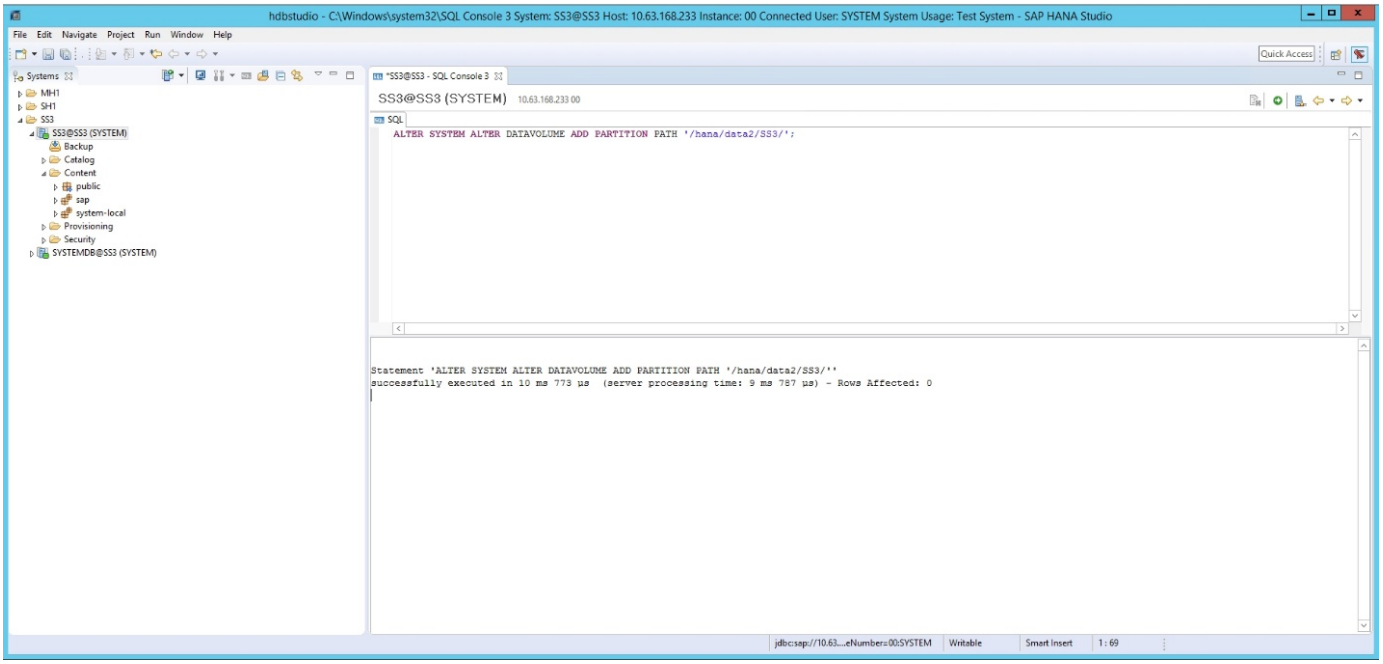
   Use a different storage virtual interface for connecting each data volume to ensure that you are using different TCP sessions for each volume

3. Mount the file systems by running the `mount -a` command.

Adding an additional data volume partition

Execute the following SQL statement against the tenant database to add an additional data volume partition to your tenant database. Use the path to additional volumes:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Next: Where to find additional information.

Where to find additional information

Previous: Adding additional data volume partitions.

To learn more about the information described in this document, refer to the following documents and/or websites:

- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere
  www.vmware.com/files/pdf/SAP_HANA_on_vmware_vSphere_best_practices_guide.pdf
- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere
  http://www.vmware.com/files/pdf/sap-hana-scale-out-deployments-on-vsphere.pdf
- SAP Certified Enterprise Storage Hardware for SAP HANA
  http://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/enterprise-storage.html
- SAP HANA Storage Requirements
  http://go.sap.com/documents/2015/03/74cdb554-5a7c-0010-82c7-eda71af511fa.html
- SAP HANA Tailored Data Center Integration Frequently Asked Questions
  https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html
- TR-4646: SAP HANA Disaster Recovery with Storage Replication
  https://www.netapp.com/us/media/tr-4646.pdf
- TR-4614: SAP HANA Backup and Recovery with SnapCenter
  https://www.netapp.com/us/media/tr-4614.pdf
- TR-4338: SAP HANA on VMware vSphere with NetApp FAS and AFF Systems
  www.netapp.com/us/media/tr-4338.pdf
- TR-4667: Automating SAP System Copies Using the SnapCenter 4.0 SAP HANA Plug- In
  https://www.netapp.com/us/media/tr-4667.pdf
- NetApp Documentation Centers
  https://www.netapp.com/us/documentation/index.aspx
- NetApp FAS Storage System Resources
  https://mysupport.netapp.com/info/web/ECMLP2676498.html
- SAP HANA Software Solutions
  www.netapp.com/us/solutions/applications/sap/index.aspx#sap-hana

TR-4290: SAP HANA on NetApp FAS systems with NFS Configuration guide

Nils Bauer and Marco Schön, NetApp

The NetApp FAS product family has been certified for use with SAP HANA in tailored data center integration (TDI) projects. The certified enterprise storage system is characterized by the NetApp ONTAP software.

This certification is currently only valid for the following models:

- FAS2720, FAS2750, FAS8300, FAS8700, and FAS9000A complete list of NetApp certified storage solutions for SAP HANA can be found at the Certified and Supported SAP HANA Hardware Directory.

This document describes the ONTAP configuration requirements for the NFS version 3 (NFSv3) protocol or the NFS version 4 (NFSv4.0 and NFSv4.1) protocol. For the remainder of this document, NFSv4 refers to both NFSv4.0 and NFSv4.1.

The configuration described in this paper is necessary to achieve the required SAP HANA KPIs and the best performance for SAP HANA. Changing any settings or using features not listed herein might cause performance degradation or unexpected behavior and should only be performed if advised by NetApp support.

The configuration guides for NetApp FAS systems using FCP and for AFF systems using NFS or FC can be found at the following links:

- SAP HANA on NetApp FAS Systems with Fibre Channel Protocol
- SAP HANA on NetApp AFF Systems with NFS
- SAP HANA on NetApp AFF Systems with Fibre Channel Protocol

The following table shows the supported combinations for NFS versions, NFS locking, and the required isolation implementations, depending on the SAP HANA database configuration.

For SAP HANA single-host systems or multiple hosts without Host Auto-Failover, NFSv3 and NFSv4 are supported.

For SAP HANA multiple host systems with Host Auto-Failover, NetApp only supports NFSv4, while using NFSv4 locking as an alternative to a server-specific STONITH (SAP HANA HA/DR provider) implementation.

SAP HANA	NFS Version	NFS Locking	SAP HANA HA/DR Provider
SAP HANA single host, multiple hosts without Host Auto-Failover	NFSv3	Off	n/a
	NFSv4	On	n/a
SAP HANA multiple hosts with Host Auto-Failover	NFSv3	Off	Server-specific STONITH implementation mandatory
	NFSv4	On	Not required

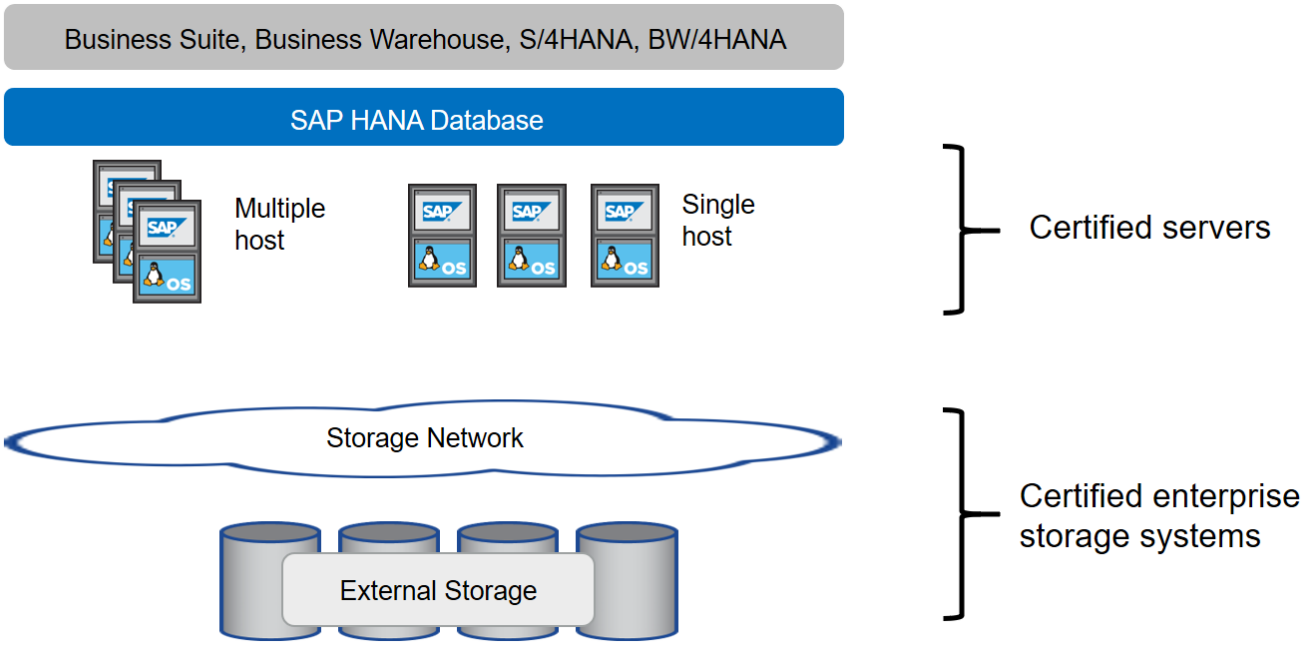
A server-specific STONITH implementation is not part of this guide. Contact your server vendor for such an implementation.

This document covers configuration recommendations for SAP HANA running on physical servers and on virtual servers that use VMware vSphere.

Always refer to the relevant SAP notes for operating system configuration guidelines and HANA- specific Linux kernel dependencies. For more information, see SAP note 2235581: SAP HANA Supported Operating Systems.

SAP HANA Tailored Data Center integration

NetApp FAS storage controllers are certified in the SAP HANA TDI program using both NFS (NAS) and FC (SAN) protocols. They can be deployed in any of the current SAP HANA scenarios such as SAP Business Suite on HANA, S/4HANA, BW/4HANA, or SAP Business Warehouse on HANA in either single- host or multiple-host configurations. Any server that is certified for use with SAP HANA can be combined with NetApp certified storage solutions. See the following figure for an architecture overview.



For more information regarding the prerequisites and recommendations for production SAP HANA systems, see the following SAP resources:

- SAP HANA Tailored Data Center Integration Frequently Asked Questions
- SAP HANA Storage Requirements

SAP HANA using VMware vSphere

There are several options to connect the storage to virtual machines (VMs). The preferred one is to connect the storage volumes with NFS directly out of the guest operating system. Using this option, the configuration of hosts and storages do not differ between physical hosts and VMs.

NFS datastores or VVOL datastores with NFS are supported as well. For both options, only one SAP HANA data or log volume must be stored within the datastore for production use cases. In addition, Snapshot copy-based backup and recovery orchestrated by SnapCenter and solutions based on this, such as SAP System cloning, cannot be implemented.

This document describes the recommended setup with direct NFS mounts from the guest OS.

For more information about using vSphere with SAP HANA, see the following links:

- SAP HANA on VMware vSphere - Virtualization - Community Wiki
- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere
- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere
- 2161991 - VMware vSphere configuration guidelines - SAP ONE Support Launchpad (Login required)

Next: Architecture.

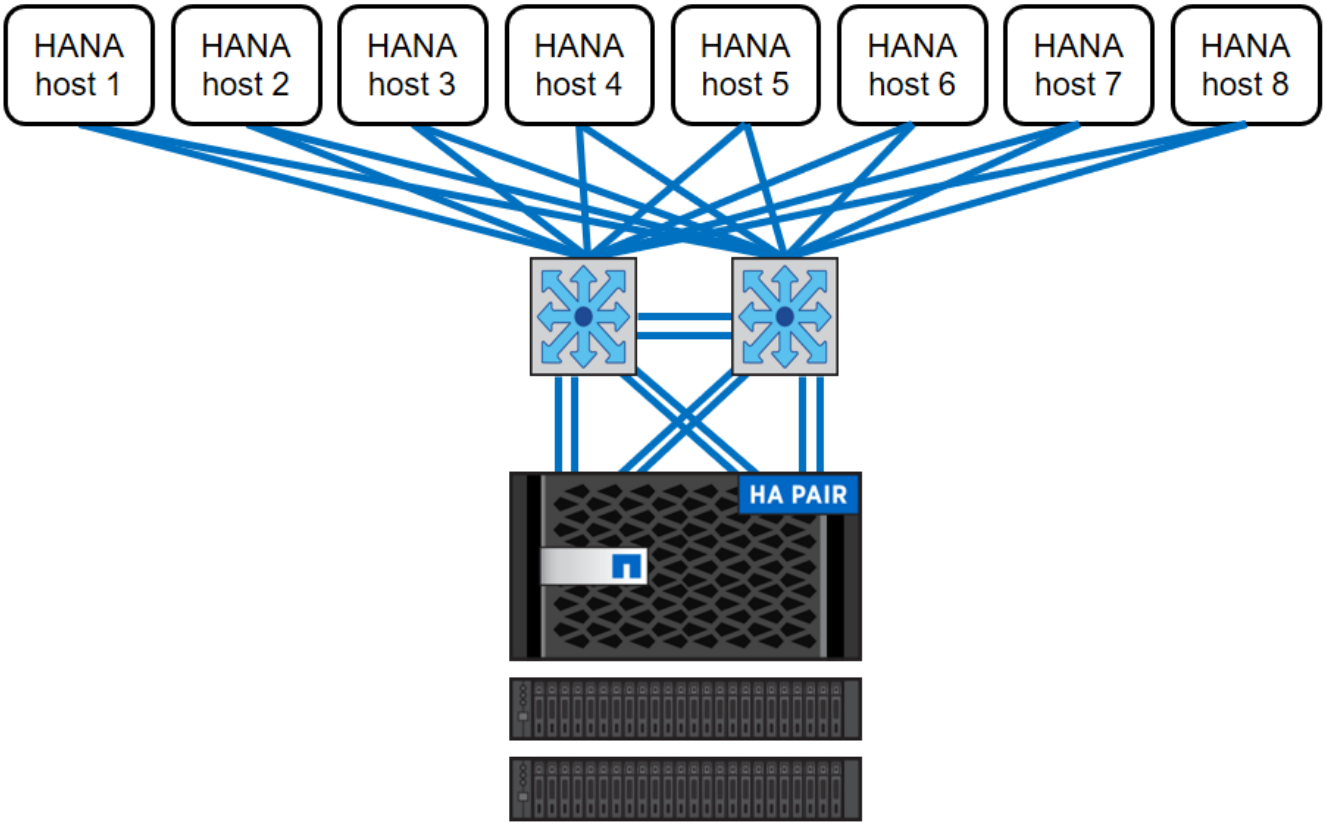
Architecture

Previous: SAP HANA on NetApp All Flash FAS Systems with NFS Configuration Guide.

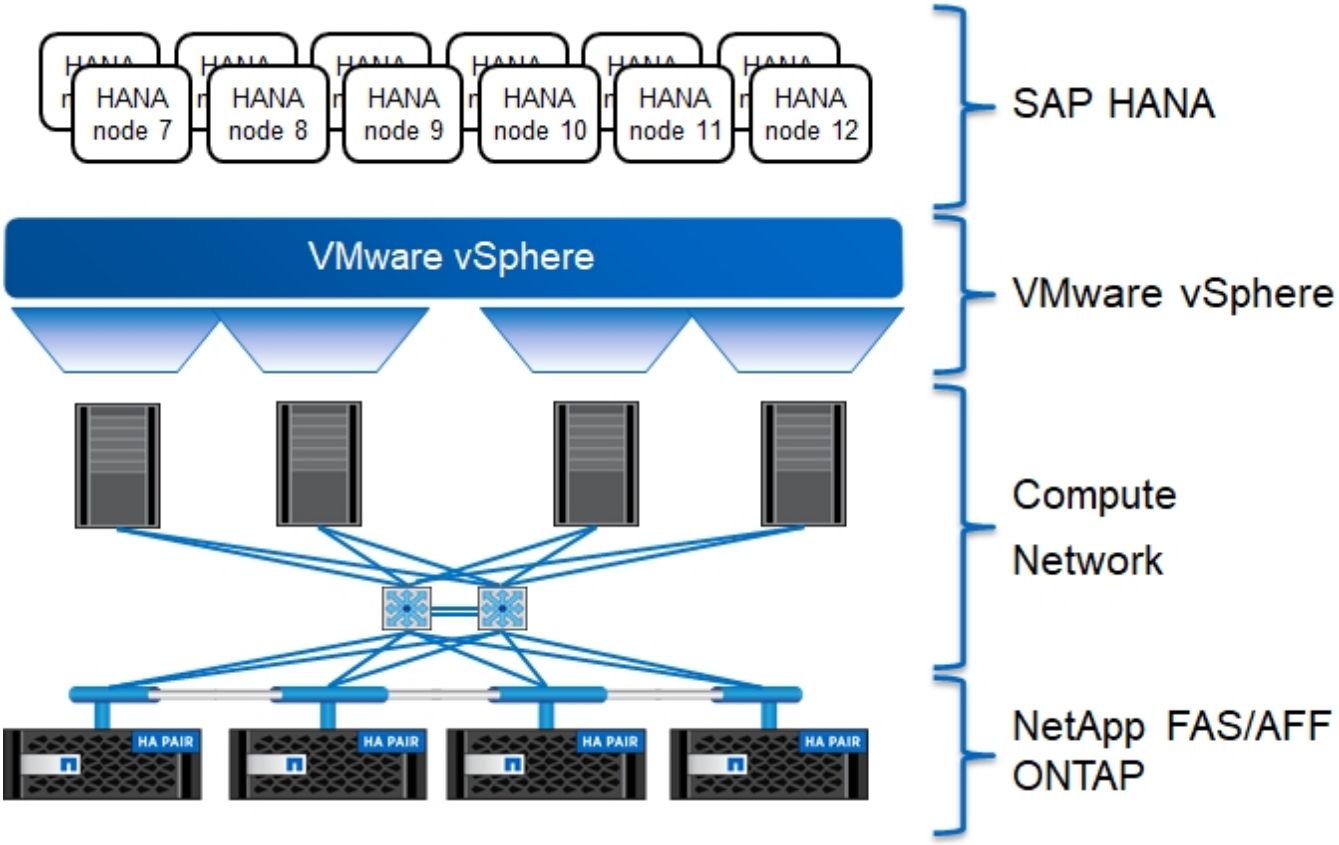
SAP HANA hosts are connected to storage controllers by using a redundant 10GbE or faster network

infrastructure. Data communication between SAP HANA hosts and storage controllers is based on the NFS protocol. A redundant switching infrastructure is recommended to provide fault-tolerant SAP HANA host- to-storage connectivity in case of switch or network interface card (NIC) failure. The switches might aggregate individual port performance with port channels in order to appear as a single logical entity at the host level.

Different models of the FAS system product family can be mixed and matched at the storage layer to allow for growth and differing performance and capacity needs. The maximum number of SAP HANA hosts that can be attached to the storage system is defined by the SAP HANA performance requirements and the model of NetApp controller used. The number of required disk shelves is only determined by the capacity and performance requirements of the SAP HANA systems. The following figure shows an example configuration with eight SAP HANA hosts attached to a storage high availability (HA) pair.



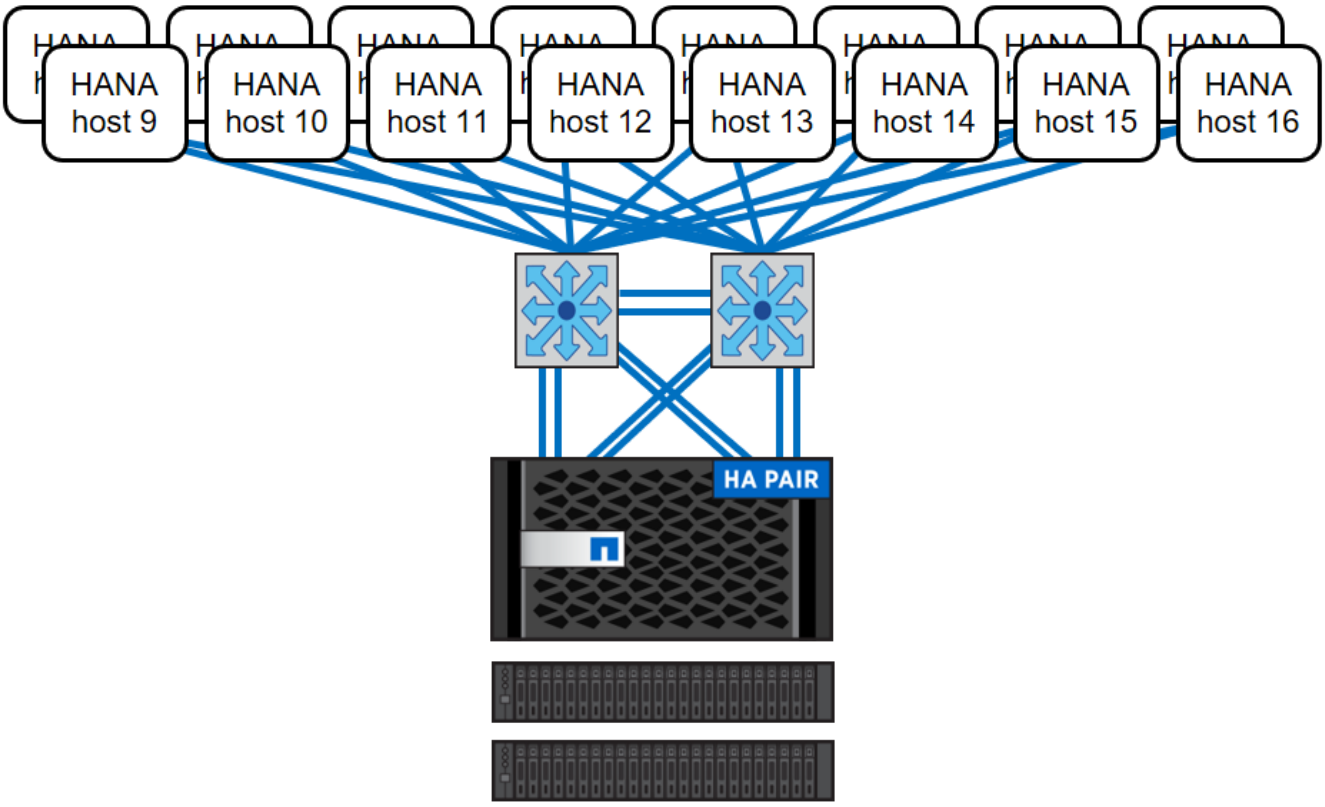
The following figure shows an example of using VMware vSphere as virtualization layer.



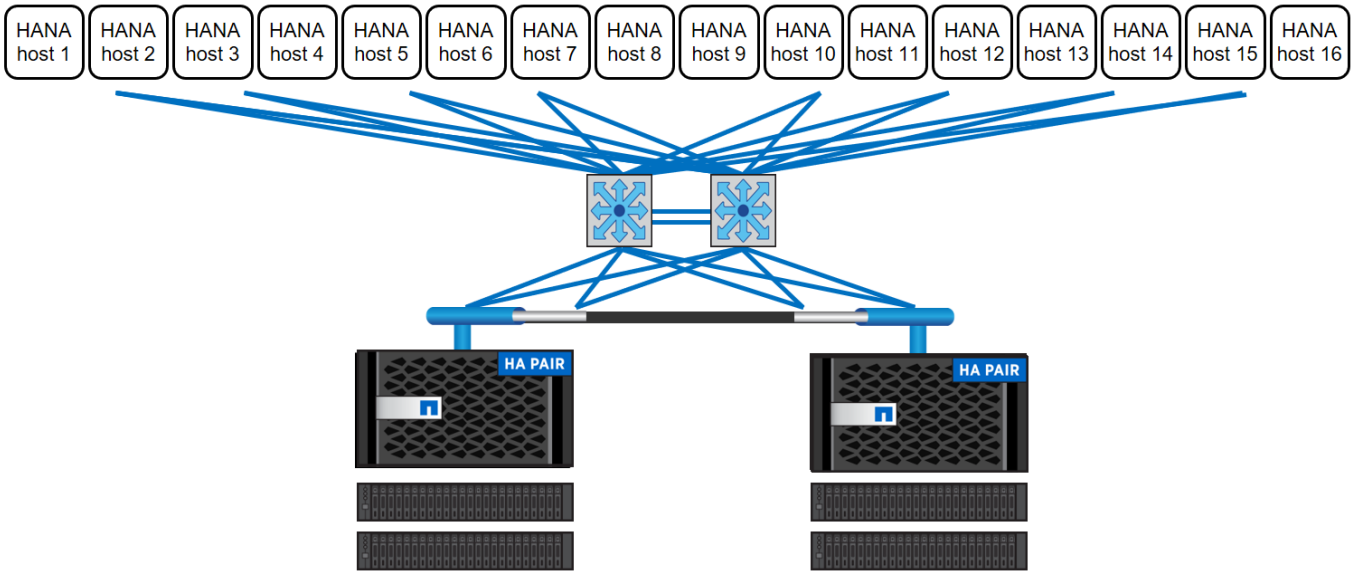
The architecture can be scaled in two dimensions:

- By attaching additional SAP HANA hosts and/or storage capacity to the existing storage, if the storage controllers provide enough performance to meet the current SAP key performance indicators (KPIs)
- By adding more storage systems with additional storage capacity for the additional SAP HANA hosts

The following figure shows an example configuration in which more SAP HANA hosts are attached to the storage controllers. In this example, more disk shelves are necessary to fulfill both the capacity and performance requirements of 16 SAP HANA hosts. Depending on the total throughput requirements, additional 10GbE (or faster) connections to the storage controllers must be added.



Independent of the deployed FAS system, the SAP HANA landscape can also be scaled by adding any of the certified storage controllers to meet the desired node density (the following figure).



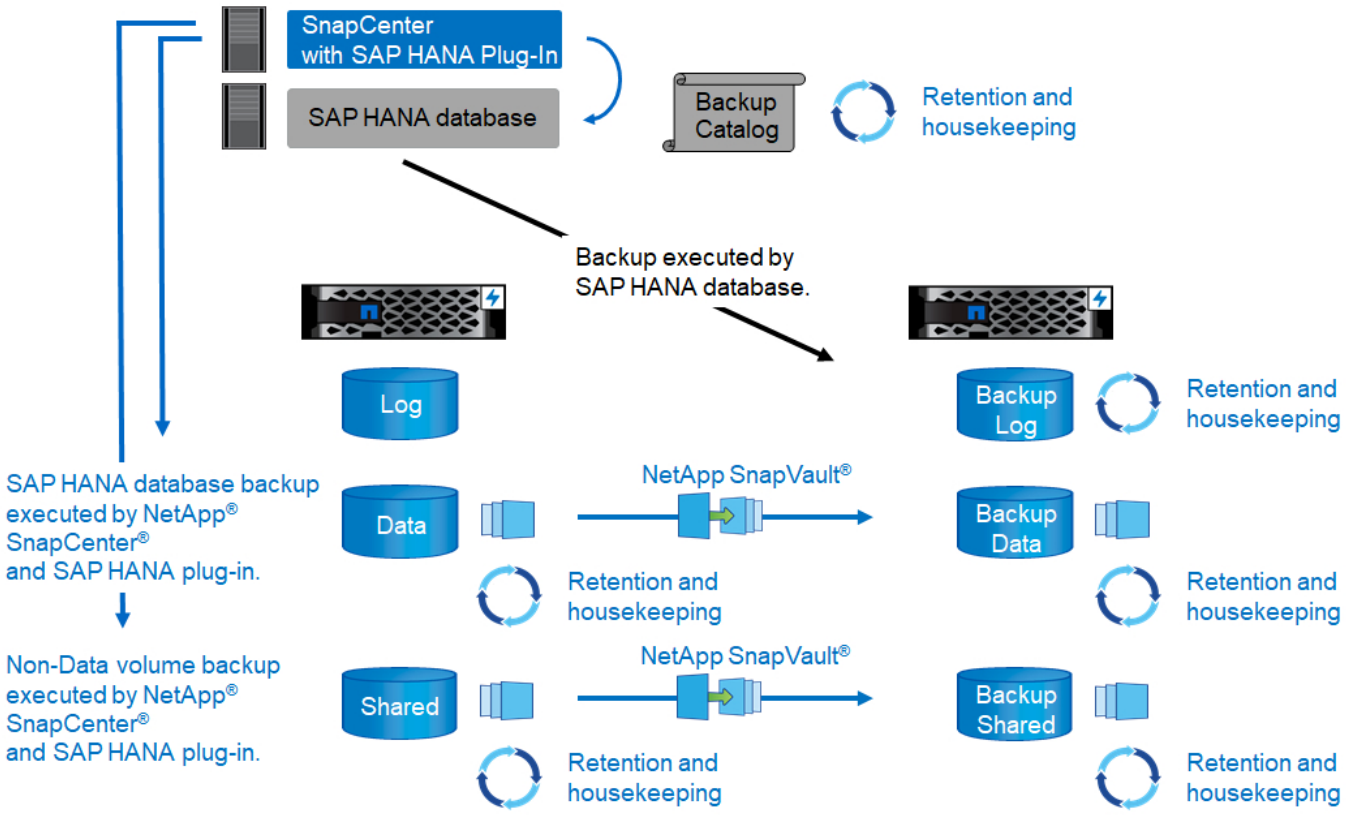
SAP HANA backup

The ONTAP software present on all NetApp storage controllers provides a built-in mechanism to back up SAP HANA databases while in operation with no effect on performance. Storage-based NetApp Snapshot backups are a fully supported and integrated backup solution available for SAP HANA single containers and for SAP HANA Multitenant Database Container (MDC) systems with a single tenant or multiple tenants.

Storage-based Snapshot backups are implemented by using the NetApp SnapCenter plug-in for SAP HANA. This allows users to create consistent storage-based Snapshot backups by using the interfaces provided natively by SAP HANA databases. SnapCenter registers each of the Snapshot backups into the SAP HANA backup catalog. Therefore, the backups taken by SnapCenter are visible within SAP HANA Studio and Cockpit where they can be selected directly for restore and recovery operations.

NetApp SnapMirror technology allows Snapshot copies that were created on one storage system to be replicated to a secondary backup storage system that is controlled by SnapCenter. Different backup retention policies can then be defined for each of the backup sets on the primary storage and for the backup sets on the secondary storage systems. The SnapCenter Plug-in for SAP HANA automatically manages the retention of Snapshot copy-based data backups and log backups, including the housekeeping of the backup catalog. The SnapCenter Plug-in for SAP HANA also allows the execution of a block integrity check of the SAP HANA database by executing a file-based backup.

The database logs can be backed up directly to the secondary storage by using an NFS mount, as shown in the following figure.



Storage-based Snapshot backups provide significant advantages when compared to conventional file-based backups. These advantages include, but are not limited to, the following:

- Faster backup (a few minutes)
- Reduced recovery time objective (RTO) due to a much faster restore time on the storage layer (a few minutes) as well as more frequent backups
- No performance degradation of the SAP HANA database host, network, or storage during backup and recovery operations
- Space-efficient and bandwidth-efficient replication to secondary storage based on block changes

For detailed information about the SAP HANA backup and recovery solution using SnapCenter, see TR-4614: SAP HANA Backup and Recovery with SnapCenter.

SAP HANA disaster recovery

SAP HANA disaster recovery can be performed either on the database layer by using SAP HANA system replication or on the storage layer by using storage replication technologies. The following section provides an overview of disaster recovery solutions based on storage replication.

For detailed information about the SAP HANA disaster recovery solutions, see TR-4646: SAP HANA Disaster Recovery with Storage Replication.

Storage replication based on SnapMirror

The following figure shows a three-site disaster recovery solution that uses synchronous SnapMirror replication to the local disaster recovery data center and asynchronous SnapMirror to replicate data to the remote disaster recovery data center.

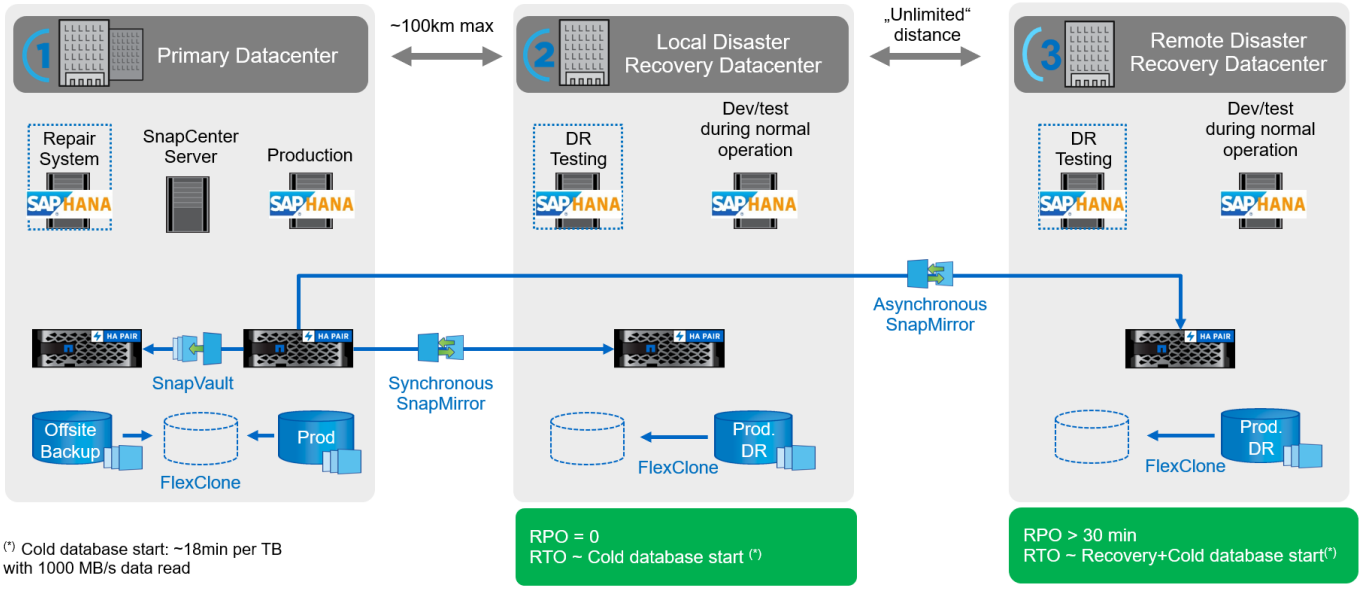
Data replication using synchronous SnapMirror provides an RPO of zero. The distance between the primary and the local disaster recovery data center is limited to around 100km.

Protection against failures of both the primary and the local disaster recovery site is performed by replicating the data to a third remote disaster recovery data center using asynchronous SnapMirror. The RPO depends on the frequency of replication updates and how fast they can be transferred. In theory, the distance is unlimited, but the limit depends on the amount of data that must be transferred and the connection that is available between the data centers. Typical RPO values are in the range of 30 minutes to multiple hours.

The RTO for both replication methods primarily depends on the time needed to start the HANA database at the disaster recovery site and load the data into memory. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data would take approximately 18 minutes.

The servers at the disaster recovery sites can be used as dev/test systems during normal operation. In the case of a disaster, the dev/test systems would need to be shut down and started as disaster recovery production servers.

Both replication methods allow to you execute disaster recovery workflow testing without influencing the RPO and RTO. FlexClone volumes are created on the storage and are attached to the disaster recovery testing servers.

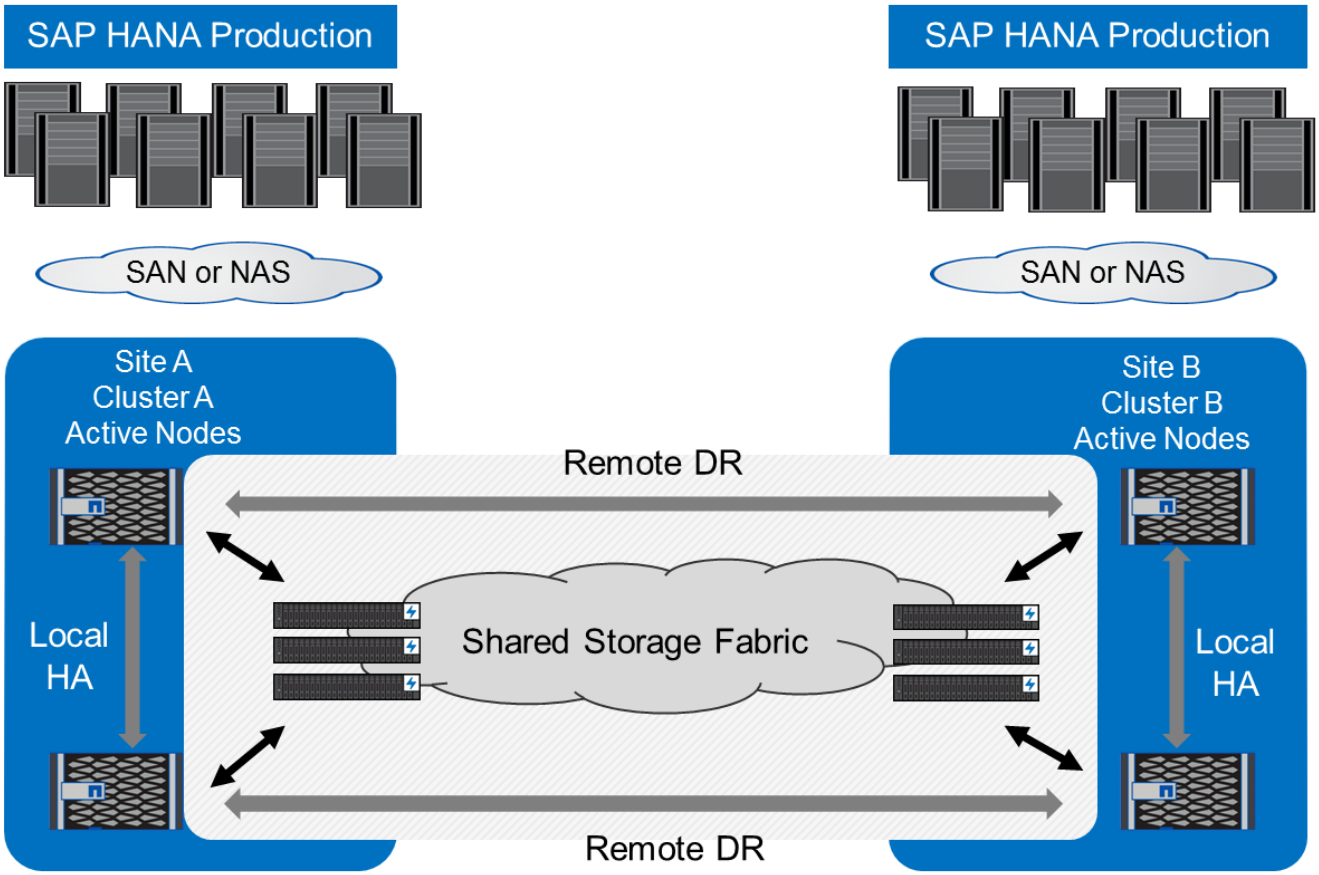


Synchronous replication offers StrictSync mode. If the write to secondary storage is not completed for any

reason, the application I/O fails, thereby ensuring that the primary and secondary storage systems are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to InSync status. If the primary storage fails, application I/O can be resumed on the secondary storage after failover, with no loss of data. In StrictSync mode, the RPO is always zero.

Storage replication based on MetroCluster

The following figure shows a high-level overview of the solution. The storage cluster at each site provides local high availability and is used for the production workload. The data of each site is synchronously replicated to the other location and is available if there is disaster failover.



Next: Storage sizing.

Storage sizing

Previous: Architecture.

The following section provides an overview of the required performance and capacity considerations needed for sizing a storage system for SAP HANA.

> Contact NetApp or your NetApp partner sales representative to assist you in creating a properly sized storage environment.

Performance considerations

SAP has defined a static set of storage KPIs that are valid for all production SAP HANA environments independent of the memory size of the database hosts and the applications that use the SAP HANA database.

These KPIs are valid for single-host, multiple-host, Business Suite on HANA, Business Warehouse on HANA, S/4HANA, and BW/4HANA environments. Therefore, the current performance sizing approach only depends on the number of active SAP HANA hosts that are attached to the storage system.

Storage performance KPIs are only mandated for production SAP HANA systems, but you can implement them in all HANA systems.

SAP delivers a performance test tool used to validate the performance of the storage system for active SAP HANA hosts attached to the storage.

NetApp tested and predefined the maximum number of SAP HANA hosts that can be attached to a specific storage model, while still fulfilling the required storage KPIs from SAP for production- based SAP HANA systems.

The storage controllers of the certified FAS product family can also be used for SAP HANA with other disk types or disk back-end solutions. However, they must be supported by NetApp and fulfill SAP HANA TDI performance KPIs. Examples include NetApp Storage Encryption (NSE) and NetApp FlexArray technology.

This document describes disk sizing for SAS HDDs and solid-state drives (SSDs).

HDDs

A minimum of 10 data disks (10k RPM SAS) per SAP HANA node is required to fulfill the storage performance KPIs from SAP.

This calculation is independent of the storage controller and disk shelf used as well as the capacity requirements of the database. Adding more disk shelfs does not increase the maximum amount of SAP HANA hosts a storage controller can support.

Solid-state drives

With SSDs, the number of data disks is determined by the SAS connection throughput from the storage controllers to the SSD shelf.

The maximum number of SAP HANA hosts that can be run on a single disk shelf and the minimum number of SSDs required per SAP HANA host were determined by running the SAP performance test tool. This test does not consider the actual storage capacity requirements of the hosts. In addition, you must also calculate the capacity requirements to determine the actual storage configuration needed.

- The 12Gb SAS disk shelf (DS224C) with 24 SSDs supports up to 14 SAP HANA hosts when the disk shelf is connected with 12Gb.
- The 6Gb SAS disk shelf (DS2246) with 24 SSDs supports up to 4 SAP HANA hosts.

The SSDs and the SAP HANA hosts must be equally distributed between both storage controllers.

The following table summarizes the supported number of SAP HANA hosts per disk shelf.

	6Gb SAS shelves (DS2246)fully loaded with 24 SSDs	**12Gb SAS shelves (DS224C)fully loaded with 24 SSDs**
Maximum number of SAP HANA hosts per disk shelf	4	14

This calculation is independent of the storage controller used. Adding more disk shelfs do not increase the maximum amount of SAP HANA hosts a storage controller can support.

Mixed workloads

SAP HANA and other application workloads running on the same storage controller or in the same storage aggregate are supported. However, it is a NetApp best practice to separate SAP HANA workloads from all other application workloads.

You might decide to deploy SAP HANA workloads and other application workloads on either the same storage controller or the same aggregate. If so, you must make sure that adequate performance is available for SAP HANA within the mixed workload environment. NetApp also recommends that you use quality of service (QoS) parameters to regulate the effect these other applications could have and to guarantee throughput for SAP HANA applications.

The SAP performance test tool must be used to check if additional SAP HANA hosts can be run on an existing storage controller that is already in use for other workloads. SAP application servers can be safely placed on the same storage controller and/or aggregate as the SAP HANA databases.

Capacity considerations

A detailed description of the capacity requirements for SAP HANA is in the SAP HANA Storage Requirements white paper.

The capacity sizing of the overall SAP landscape with multiple SAP HANA systems must be determined by using SAP HANA storage sizing tools from NetApp. Contact NetApp or your NetApp partner sales representative to validate the storage sizing process for a properly sized storage environment.

Configuration of performance test tool

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage system used. These parameters must also be set when storage performance is being tested with the SAP performance test tool.

NetApp conducted performance tests to define the optimal values. The following table lists the parameters that must be set within the configuration file of the SAP performance test tool.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on
async_write_submit_blocks	all

For more information about the configuration of the SAP test tool, see SAP note 1943937 for HWCCT (SAP HANA 1.0) and SAP note 2493172 for HCMT/HCOT (SAP HANA 2.0).

The following example shows how variables can be set for the HCMT/HCOT execution plan.

```
... {
```

```
         "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "LogAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
```

```
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

These variables must be used for the test configuration. This is usually the case with the predefined execution plans SAP delivers with the HCMT/HCOT tool. The following example for a 4k log write test is from an execution plan.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

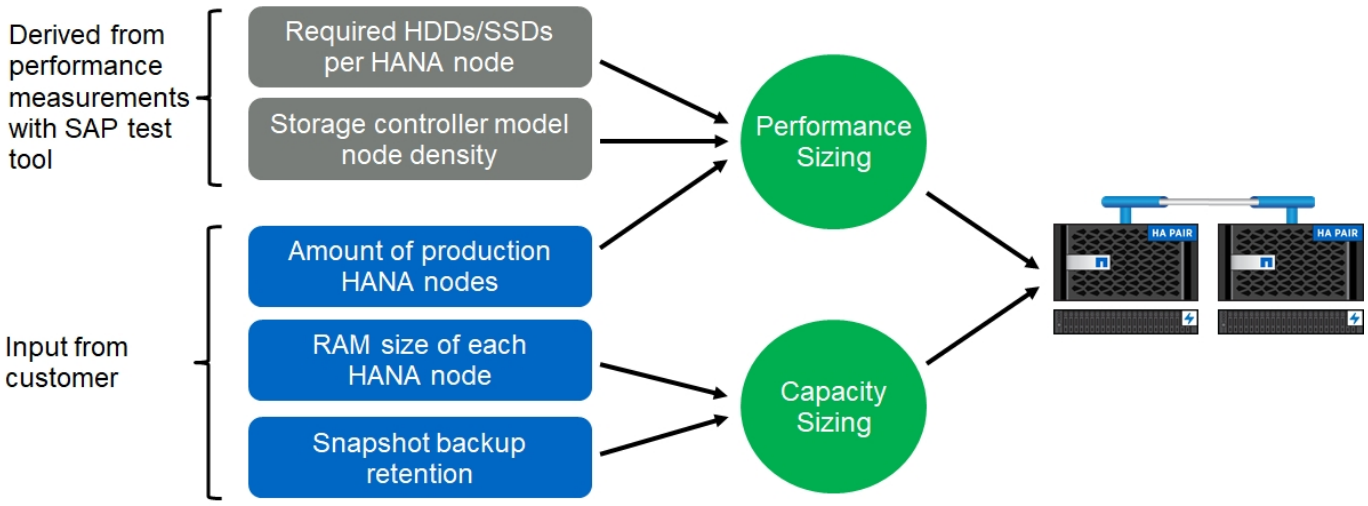
Storage sizing process overview

The number of disks per HANA host and the SAP HANA host density for each storage model were determined with the SAP performance test tool.

The sizing process requires details such as the number of production and nonproduction SAP HANA hosts, the RAM size of each host, and the backup retention of the storage-based Snapshot copies. The number of SAP HANA hosts determines the storage controller and the number of disks required.

The size of the RAM, net data size on the disk of each SAP HANA host, and the Snapshot copy backup retention period are used as inputs during capacity sizing.

The following figure summarizes the sizing process.



Next: Infrastructure setup and configuration.

Overview

Previous: Storage sizing.

The following sections provide SAP HANA infrastructure setup and configuration guidelines.

Next: Network setup.

Network setup

Previous: Infrastructure setup and configuration.

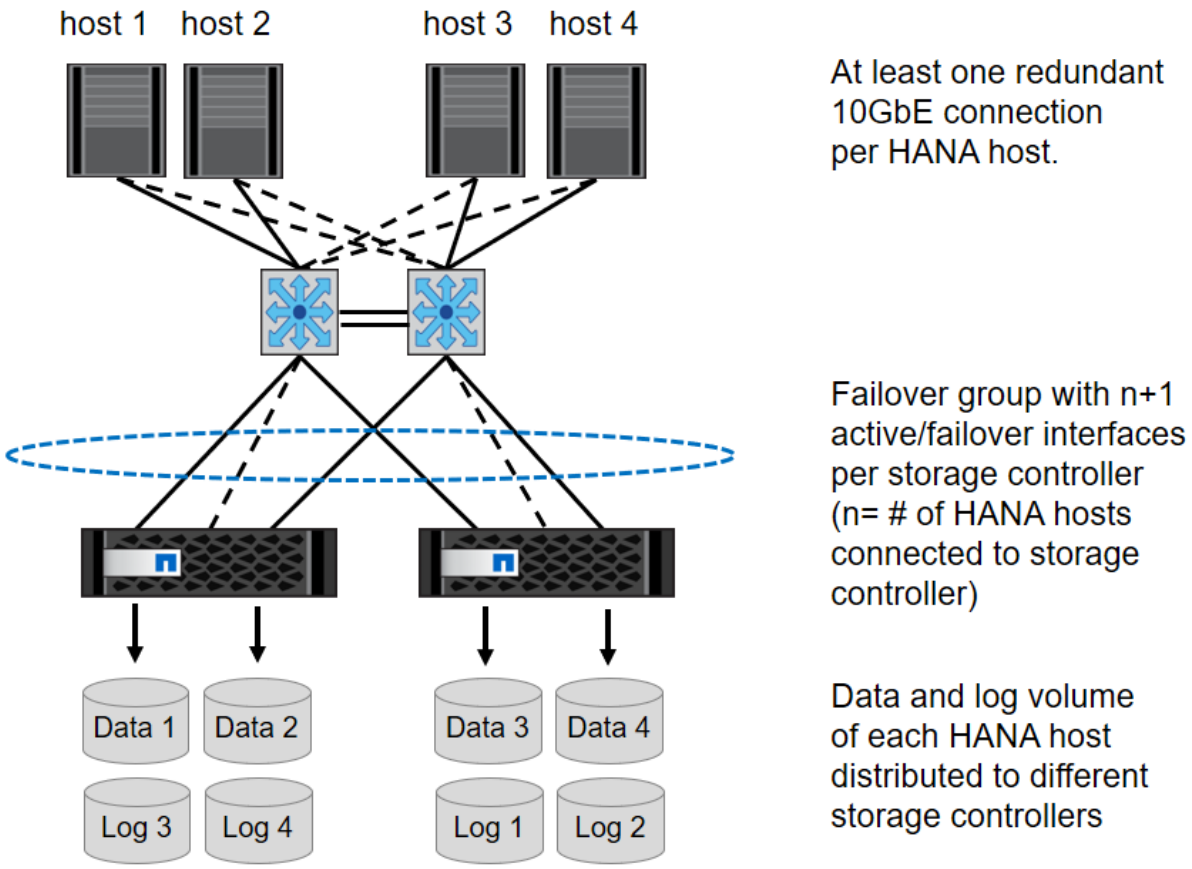
Use the following guidelines when configuring the network:

- A dedicated storage network must be used to connect the SAP HANA hosts to the storage controllers with a 10GbE or faster network.
- Use the same connection speed for storage controllers and SAP HANA hosts. If this is not possible, ensure that the network components between the storage controllers and the SAP HANA hosts are able to handle different speeds. For example, you must provide enough buffer space to allow speed negotiation at the NFS level between storage and hosts. Network components are usually switches, but other components within blade chassis, such as the back plane, must be considered as well.
- Disable flow control on all physical ports used for storage traffic on the storage network switch and host layer.
- Each SAP HANA host must have a redundant network connection with a minimum of 10Gb of bandwidth.
- Jumbo frames with a maximum transmission unit (MTU) size of 9,000 must be enabled on all network components between the SAP HANA hosts and the storage controllers.
- In a VMware setup, dedicated VMXNET3 network adapters must be assigned to each running virtual machine. Check the relevant papers mentioned in the Introduction for further requirements.
- To avoid interference between each other, use separate network/IO paths for the log and data area.

The following figure shows an example with four SAP HANA hosts attached to a storage controller HA pair using a 10GbE network. Each SAP HANA host has an active-passive connection to the redundant fabric.

At the storage layer, four active connections are configured to provide 10Gb throughput for each SAP HANA host. In addition, one spare interface is configured on each storage controller.

At the storage layer, a broadcast domain with an MTU size of 9000 is configured, and all required physical interfaces are added to this broadcast domain. This approach automatically assigns these physical interfaces to the same failover group. All logical interfaces (LIFs) that are assigned to these physical interfaces are added to this failover group.



In general, it is also possible to use HA interface groups on the servers (bonds) and the storage systems (for example, Link Aggregation Control Protocol [LACP] and ifgroups). With HA interface groups, verify that the load is equally distributed between all interfaces within the group. The load distribution depends on the functionality of the network switch infrastructure.

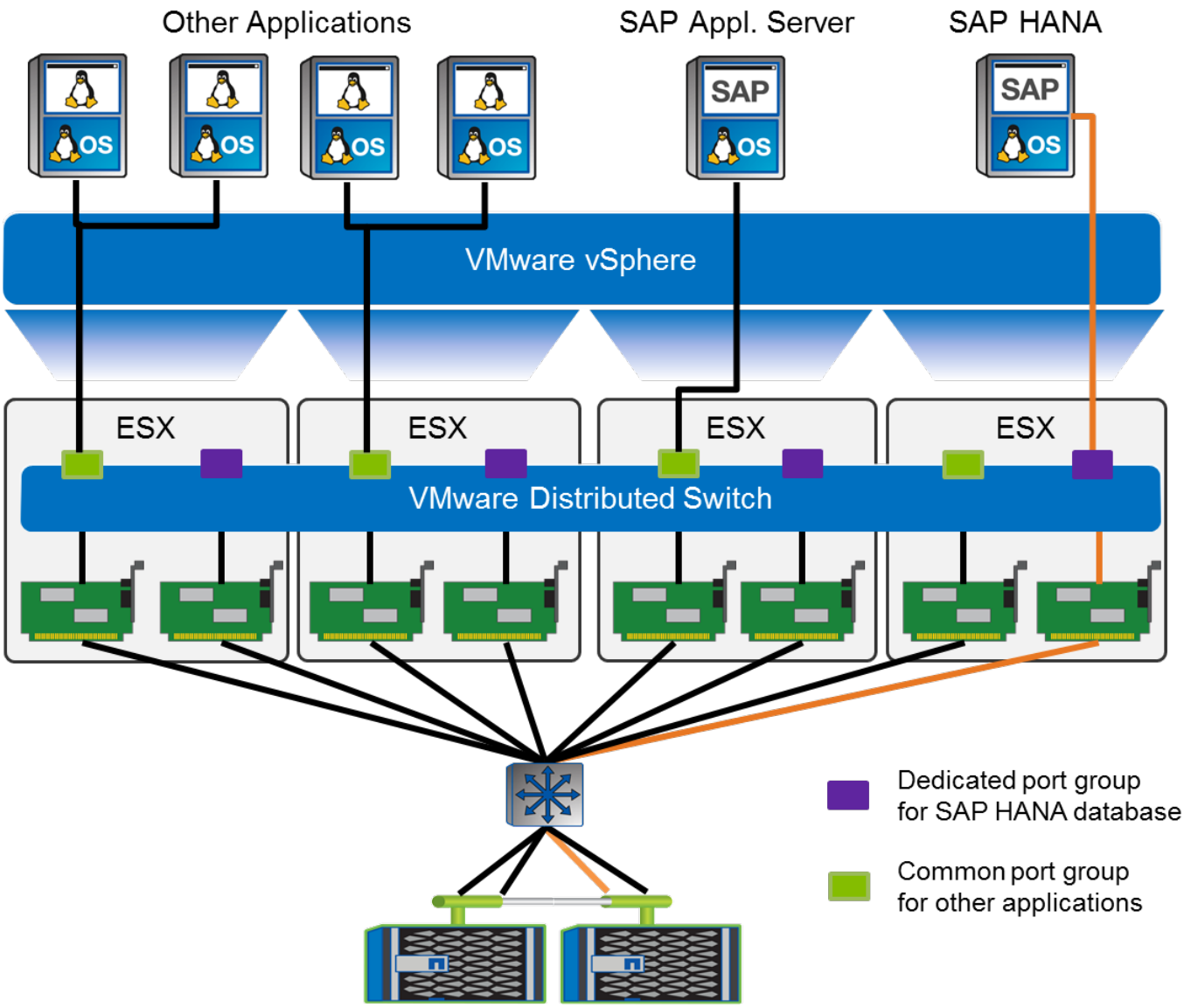
Depending on the number of SAP HANA hosts and the connection speed used, different numbers of active physical ports are needed.

VMware-specific network setup

Because all data for SAP HANA instances, including performance-critical data and log volumes for the database, is provided through NFS in this solution, proper network design and configuration are crucial. A dedicated storage network is used to separate the NFS traffic from communication and user access traffic between SAP HANA nodes. Each SAP HANA node requires a redundant dedicated network connection with a minimum of 10Gb of bandwidth. Higher bandwidth is also supported. This network must extend end to end

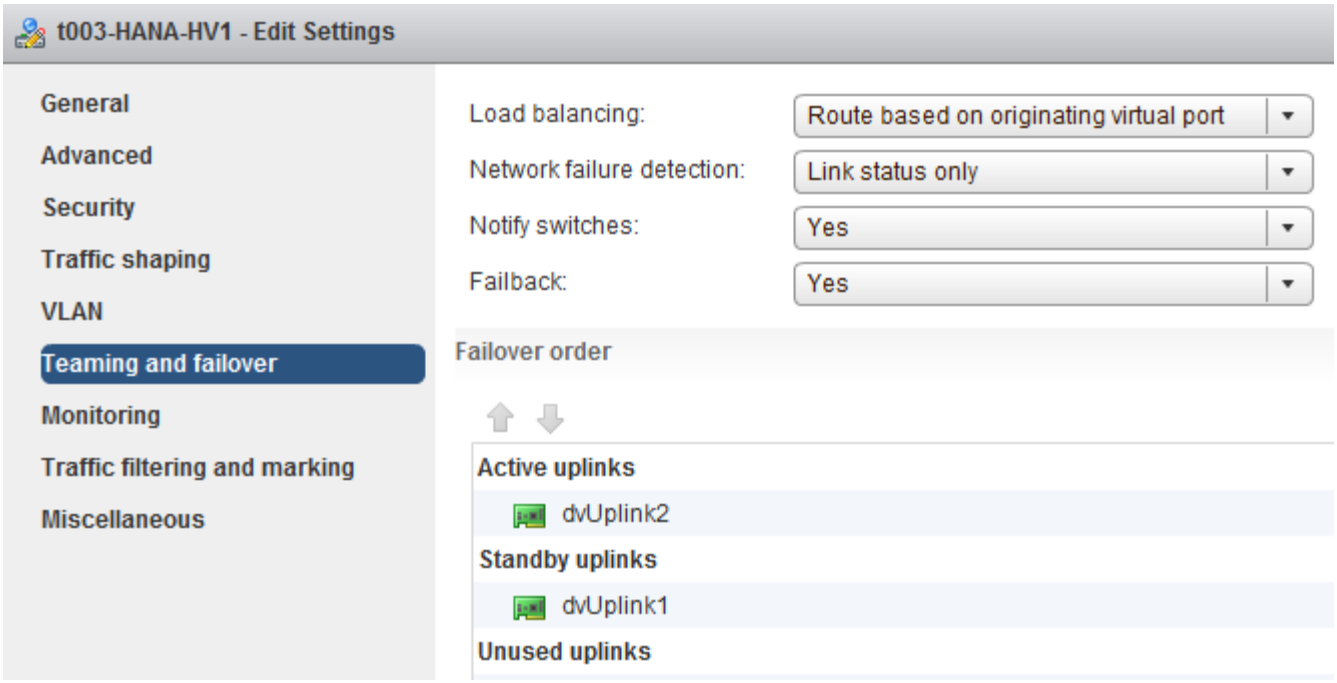
from the storage layer through network switching and computing up to the guest operating system hosted on VMware vSphere. In addition to the physical switching infrastructure, a VMware distributed switch (vDS) is used to provide adequate performance and manageability of network traffic at the hypervisor layer.

The following figure provide a network overview.



Each SAP HANA node uses a dedicated port group on the VMware distributed switch. This port group allows for enhanced quality of service (QoS) and dedicated assignment of physical network interface cards (NICs) on the ESX hosts. To use dedicated physical NICs while preserving HA capabilities if there was a NIC failure, the dedicated physical NIC is configured as an active uplink. Additional NICs are configured as standby uplinks in the teaming and failover settings of the SAP HANA port group. In addition, jumbo frames (MTU 9,000) must be enabled end to end on physical and virtual switches. In addition, turn off flow control on all ethernet ports used for storage traffic on servers, switches, and storage systems. The following figure shows an example of such a configuration.

LRO (large receive offload) must be turned off for interfaces used for NFS traffic. For all other network configuration guidelines, see the respective VMware best practices guides for SAP HANA.



Next: Time synchronization.

Time synchronization

Previous: Network setup.

You must synchronize the time between the storage controllers and the SAP HANA database hosts. To do so, set the same time server for all storage controllers and all SAP HANA hosts.

Next: Storage controller setup.

Storage controller setup

Previous: Time synchronization.

This section describes the configuration of the NetApp storage system. You must complete the primary installation and setup according to the corresponding ONTAP setup and configuration guides.

Storage efficiency

Inline deduplication, cross- volume inline deduplication, inline compression, and inline compaction are supported with SAP HANA in an SSD configuration.

Enabling storage efficiency features in an HDD-based configuration is not supported.

NetApp volume encryption

The use of NetApp Volume Encryption (NVE) is supported with SAP HANA.

Quality of service

QoS can be used to limit the storage throughput for specific SAP HANA systems or other applications on a shared-use controller. One use case would be to limit the throughput of development and test systems so that they cannot influence production systems in a mixed setup.

During the sizing process, you should determine the performance requirements of a nonproduction system. Development and test systems can be sized with lower performance values, typically in the range of 20% to 50% of a production-system KPI as defined by SAP.

Starting with ONTAP 9, QoS is configured on the storage volume level and uses maximum values for throughput (MBps) and the amount of I/O (IOPS).

Large write I/O has the biggest performance effect on the storage system. Therefore, the QoS throughput limit should be set to a percentage of the corresponding write SAP HANA storage performance KPI values in the data and log volumes.

NetApp FabricPool

NetApp FabricPool technology must not be used for active primary file systems in SAP HANA systems. This includes the file systems for the data and log area as well as the `/hana/shared` file system. Doing so results in unpredictable performance, especially during the startup of an SAP HANA system.

Using the “snapshot-only” tiering policy is possible as well as using FabricPool in general at a backup target such as a SnapVault or SnapMirror destination.

Using FabricPool for tiering Snapshot copies at primary storage or using FabricPool at a backup target changes the required time for the restore and recovery of a database or other tasks such as creating system clones or repair systems. Take this into consideration for planning your overall lifecycle- management strategy and check to make sure that your SLAs are still being met while using this function.

FabricPool is a good option for moving log backups to another storage tier. Moving backups affects the time needed to recover an SAP HANA database. Therefore, the option “tiering-minimum-cooling-days” should be set to a value that places log backups, which are routinely needed for recovery, on the local fast storage tier.

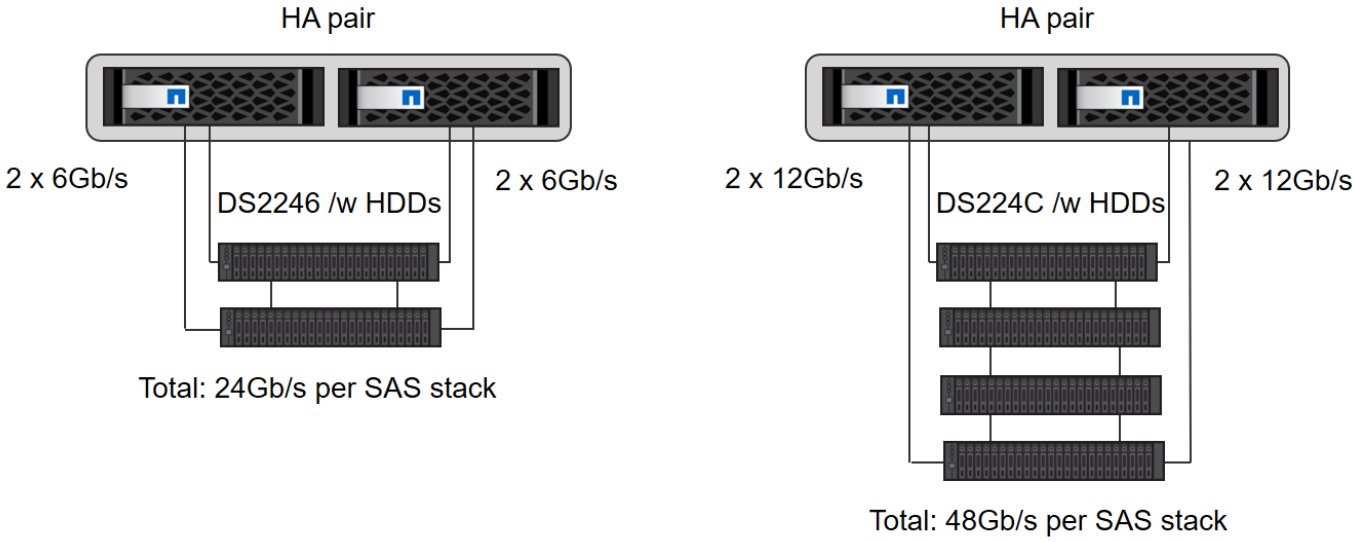
Storage configuration

The following overview summarizes the required storage configuration steps. Each step is covered in detail in the subsequent sections. In this section, we assume that the storage hardware is set up and that the ONTAP software is already installed. Also, the connections between the storage ports (10GbE or faster) and the network must already be in place.

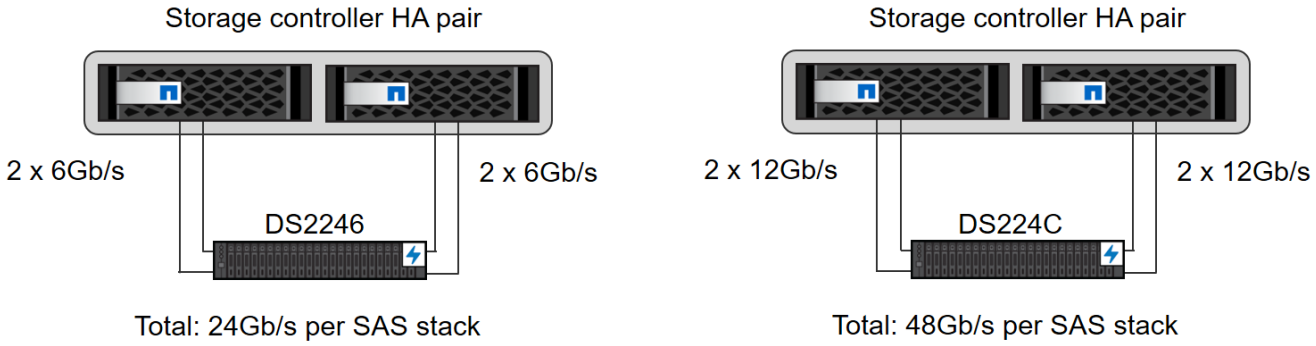
1. Check the correct SAS stack configuration as described in Disk shelf connection.
2. Create and configure the required aggregates as described in Aggregate configuration.
3. Create a storage virtual machine (SVM) as described in Storage virtual machine configuration.
4. Create LIFs as described in Logical interface configuration.
5. Create volumes within the aggregates as described in Volume configuration for SAP HANA single-host systems and Volume configuration for SAP HANA multiple-host systems.
6. Set the required volume options as described in Volume options.
7. Set the required options for NFSv3 as described in NFS configuration for NFSv3 or for NFSv4 as described in NFS configuration for NFSv4.
8. Mount the volumes to namespace and set export policies as described in Mount volumes to namespace and set export policies.

Disk shelf connection

With HDDs, a maximum of two DS2246 disk shelves or four DS224C disk shelves can be connected to one SAS stack to provide the required performance for the SAP HANA hosts, as shown in the following figure. The disks within each shelf must be distributed equally to both controllers of the HA pair.



With SSDs, a maximum of one disk shelf can be connected to one SAS stack to provide the required performance for the SAP HANA hosts, as shown in the following figure. The disks within each shelf must be distributed equally to both controllers of the HA pair. With the DS224C disk shelf, quad- path SAS cabling can also be used, but is not required.

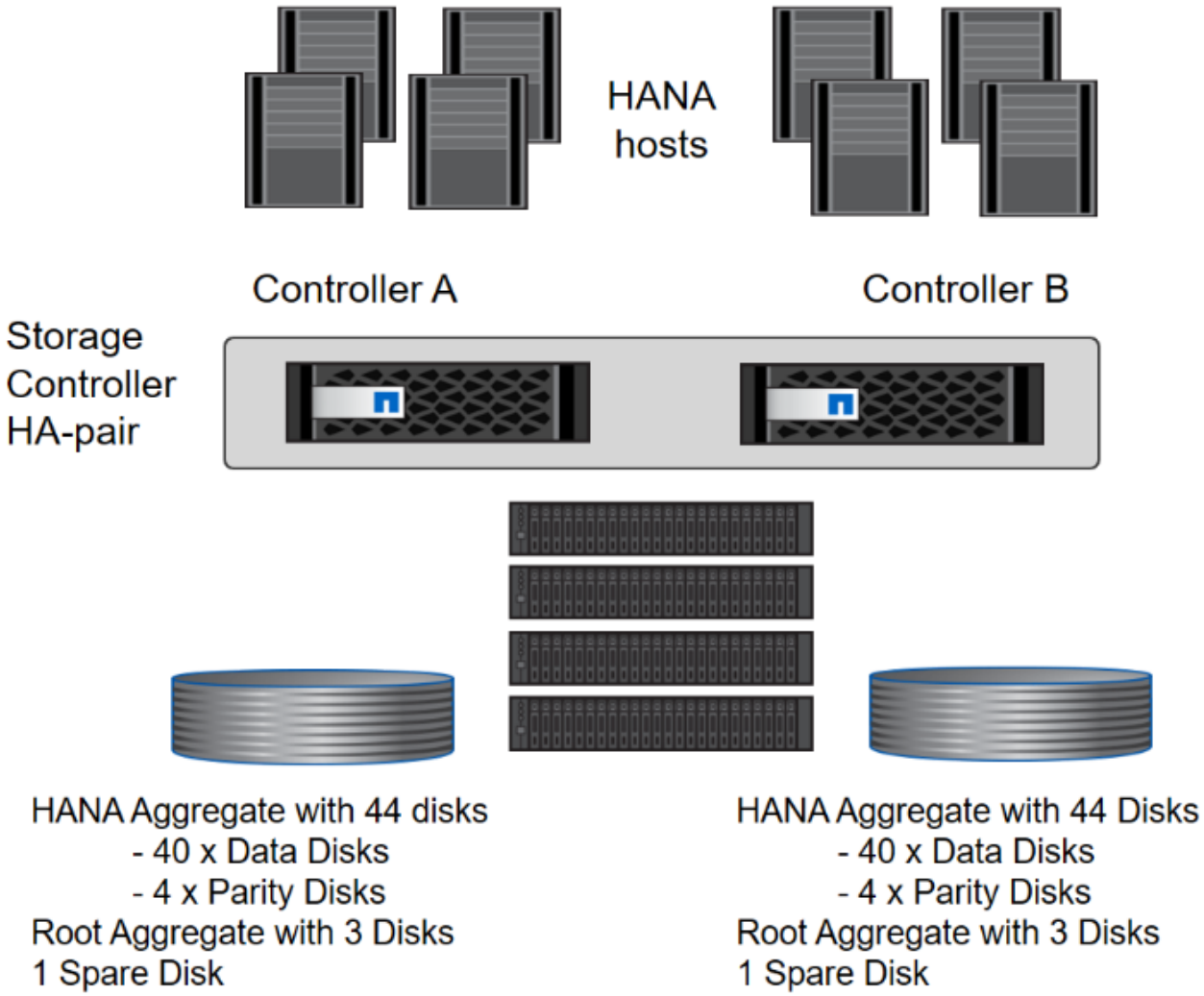


Aggregate configuration

In general, you must configure two aggregates per controller, independent of the disk shelf or drive technology (SSD or HDD) that is used. For FAS2000 series systems, one data aggregate is enough.

Aggregate configuration with HDDs

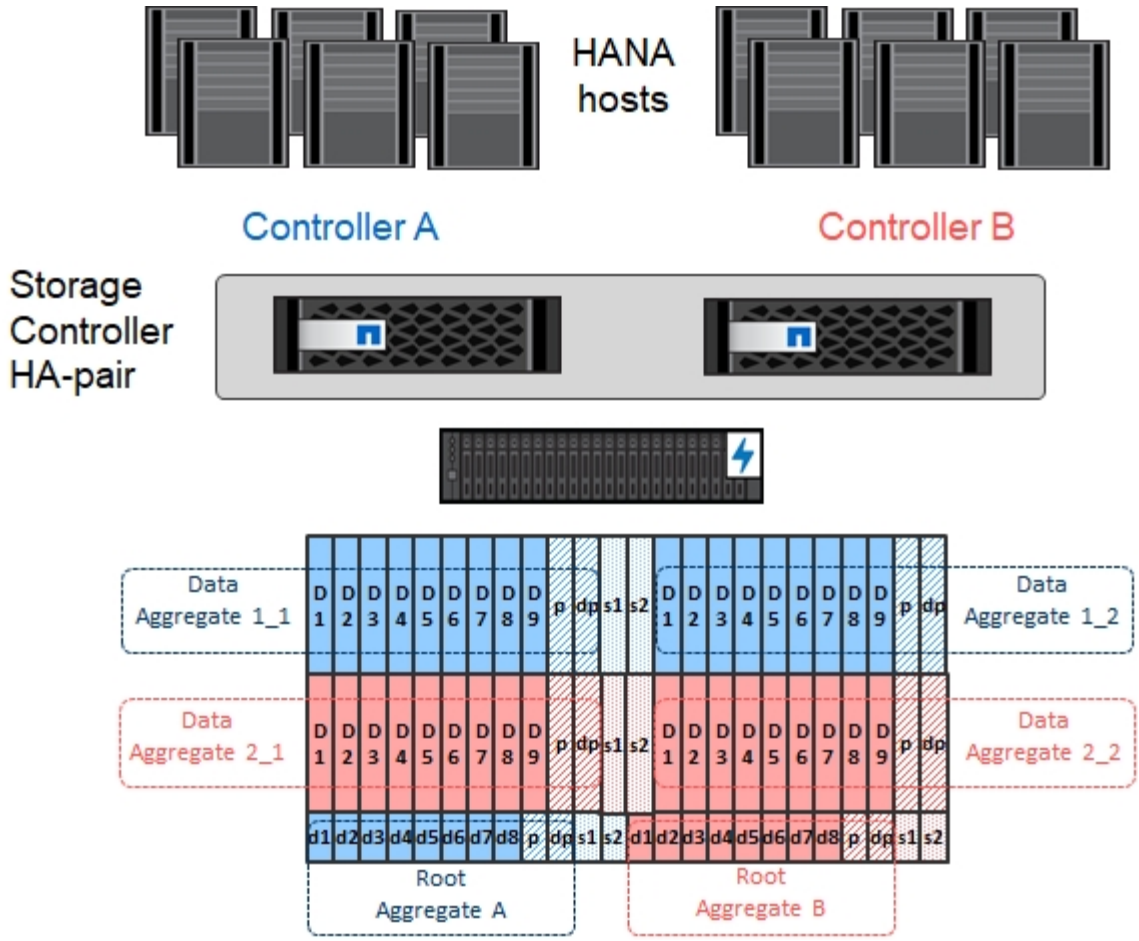
The following figure shows a configuration for eight SAP HANA hosts. Four SAP HANA hosts are attached to each storage controller. Two separate aggregates, one at each storage controller, are configured. Each aggregate is configured with 4 × 10 = 40 data disks (HDDs).



Aggregate configuration with SDD-only systems

In general, you must configure two aggregates per controller, independent of which disk shelf or disk technology (SSDs or HDDs) is used. For FAS2000 series systems, one data aggregate is enough.

The following figure shows a configuration of 12 SAP HANA hosts running on a 12Gb SAS shelf configured with ADPv2. Six SAP HANA hosts are attached to each storage controller. Four separate aggregates, two at each storage controller, are configured. Each aggregate is configured with 11 disks with nine data and two parity disk partitions. For each controller, two spare partitions are available.



Storage virtual machine configuration

Multiple SAP landscapes with SAP HANA databases can use a single SVM. An SVM can also be assigned to each SAP landscape, if necessary, in case they are managed by different teams within a company.

If a QoS profile was automatically created and assigned during new SVM creation, remove the automatically created profile from the SVM to provide the required performance for SAP HANA:

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Logical interface configuration

For SAP HANA production systems, you must use different LIFs for mounting the data volume and the log volume from the SAP HANA host. Therefore at least two LIFs are required.

The data and log volume mounts of different SAP HANA hosts can share a physical storage network port by using either the same LIFs or by using individual LIFs for each mount.

The maximum number of data and log volume mounts per physical interface are shown in the following table.

Ethernet port speed	10GbE	25GbE	40GbE	100GeE
Maximum number of log or data volume mounts per physical port	2	6	12	24

Sharing one LIF between different SAP HANA hosts might require a remount of data or log volumes to a different LIF. This change avoids performance penalties if a volume is moved to a different storage controller.

Development and test systems can use more data and volume mounts or LIFs on a physical network interface.

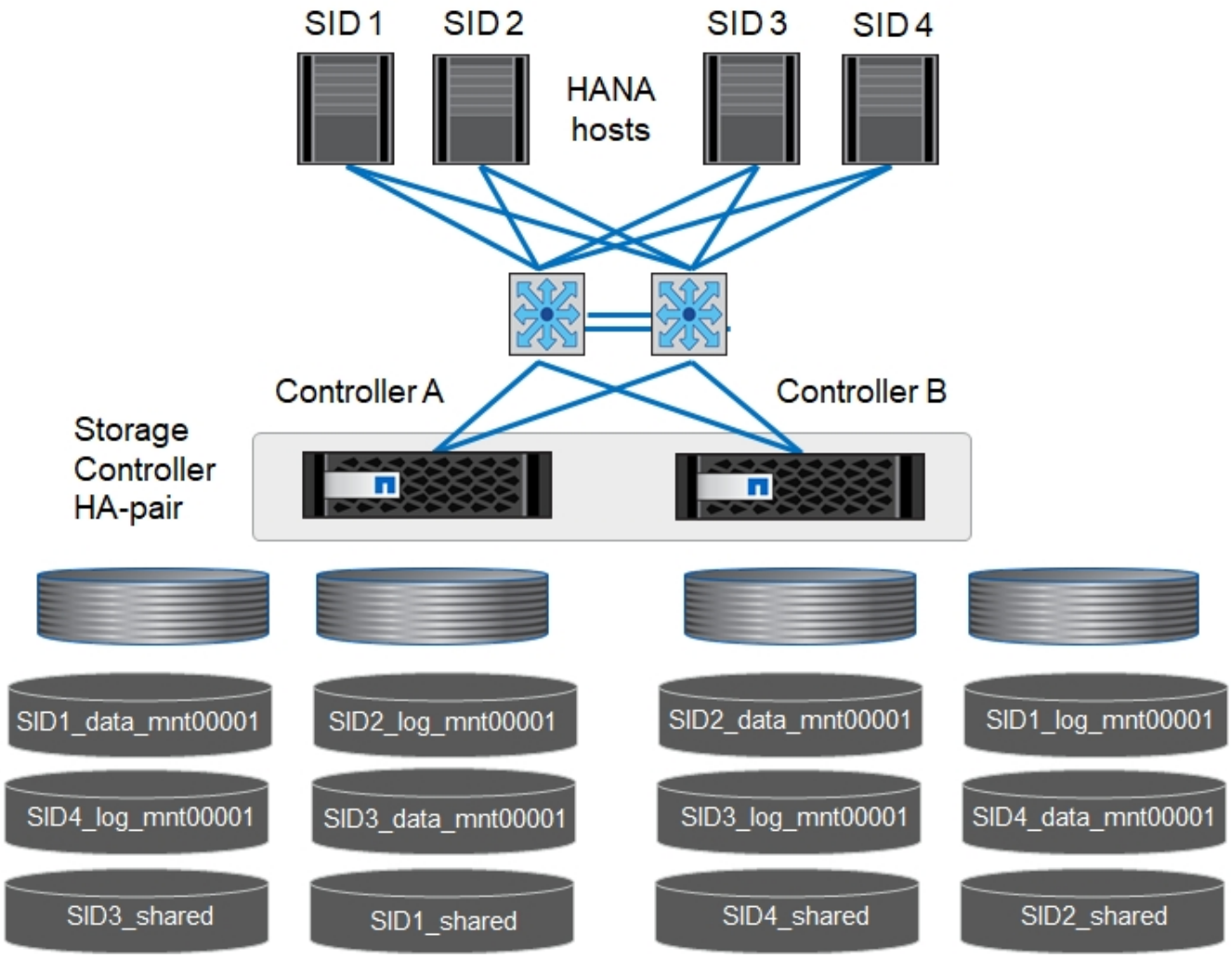
For production, development, and test systems, the `/hana/shared` file system can use the same LIF as the data or log volume.

Volume configuration for SAP HANA single-host systems

The following figure shows the volume configuration of four single-host SAP HANA systems. The data and log volumes of each SAP HANA system are distributed to different storage controllers. For example, volume `SID1_data_mnt00001` is configured on controller A, and volume `SID1_log_mnt00001` is configured on controller B.

If only one storage controller of an HA pair is used for the SAP HANA systems, data and log volumes can also be stored on the same storage controller.

If the data and log volumes are stored on the same controller, access from the server to the storage must be performed with two different LIFs: one LIF to access the data volume and one to access the log volume.



For each SAP HANA DB host, a data volume, a log volume, and a volume for `/hana/shared` are configured. The following table shows an example configuration for single-host SAP HANA systems.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller b
Data, log, and shared volumes for system SID1	Data volume: SID1_data_mnt00001	Shared volume: SID1_shared	–	Log volume: SID1_log_mnt00001
Data, log, and shared volumes for system SID2	–	Log volume: SID2_log_mnt00001	Data volume: SID2_data_mnt00001	Shared volume: SID2_shared
Data, log, and shared volumes for system SID3	Shared volume: SID3_shared	Data volume: SID3_data_mnt00001	Log volume: SID3_log_mnt00001	–
Data, log, and shared volumes for system SID4	Log volume: SID4_log_mnt00001	–	Shared volume: SID4_shared	Data volume: SID4_data_mnt00001

The following table shows an example of the mount point configuration for a single-host system. To place the home directory of the `sidadm` user on the central storage, the `/usr/sap/SID` file system should be mounted

from the `SID_shared` volume.

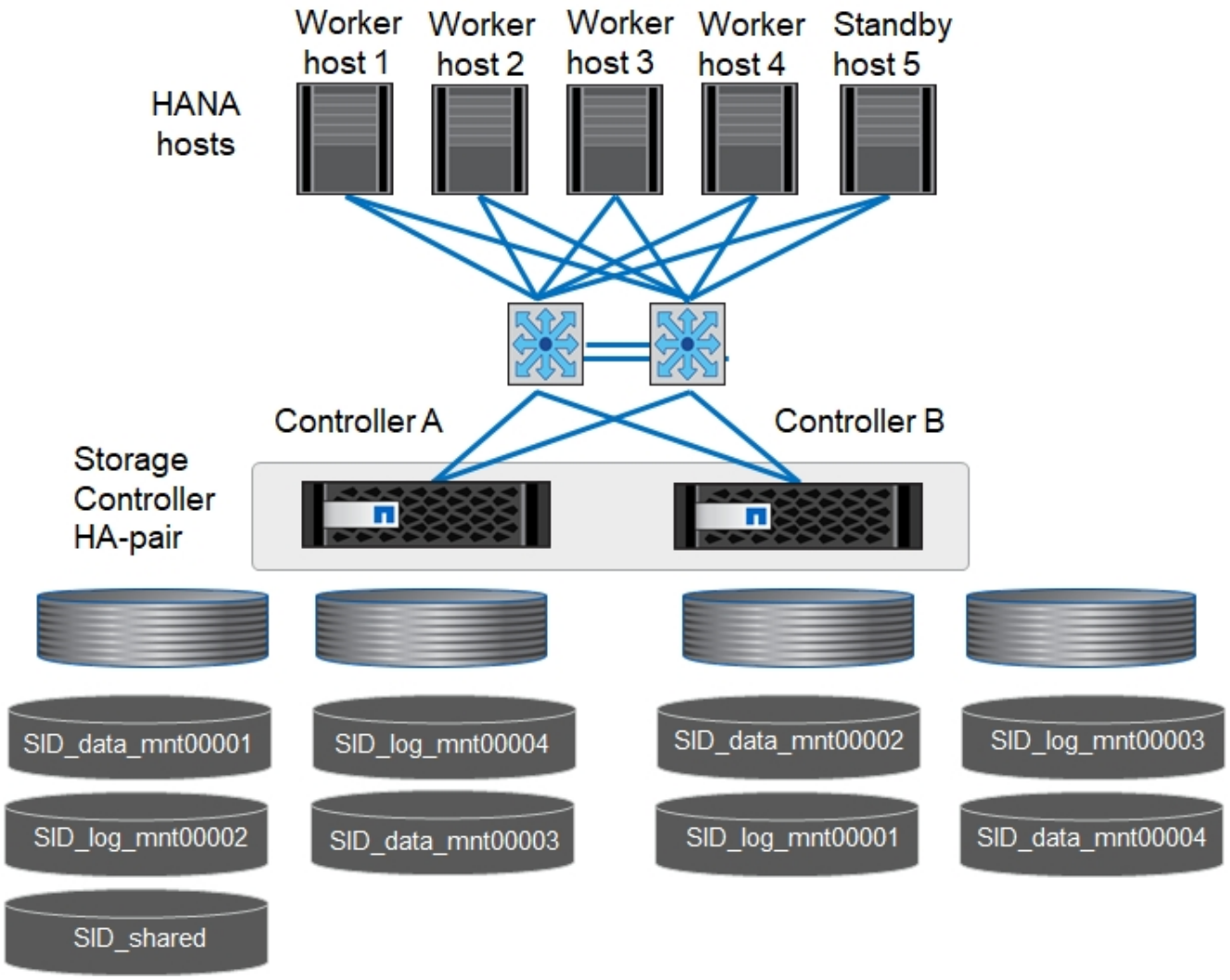
Junction Path	Directory	Mount point at HANA host
SID_data_mnt00001	–	/hana/data/SID/mnt00001
SID_log_mnt00001	–	/hana/log/SID/mnt00001
SID_shared	usr-sap shared	/usr/sap/SID /hana/shared

Volume configuration for SAP HANA multiple-host systems

The following figure shows the volume configuration of a 4+1 SAP HANA system. The data and log volumes of each SAP HANA host are distributed to different storage controllers. For example, volume `SID1_data1_mnt00001` is configured on controller A, and volume `SID1_log1_mnt00001` is configured on controller B.

If only one storage controller of an HA pair is used for the SAP HANA system, the data and log volumes can also be stored on the same storage controller.

If the data and log volumes are stored on the same controller, access from the server to the storage must be performed with two different LIFs: one to access the data volume and one to access the log volume.



For each SAP HANA host, a data volume and a log volume are created. The `/hana/shared` volume is used by all hosts of the SAP HANA system. The following table shows an example configuration for a multiple-host SAP HANA system with four active hosts.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	–	Log volume: SID_log_mnt00001	–
Data and log volumes for node 2	Log volume: SID_log_mnt00002	–	Data volume: SID_data_mnt00002	–
Data and log volumes for node 3	–	Data volume: SID_data_mnt00003	–	Log volume: SID_log_mnt00003
Data and log volumes for node 4	–	Log volume: SID_log_mnt00004	–	Data volume: SID_data_mnt00004
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

The following table shows the configuration and the mount points of a multiple-host system with four active SAP HANA hosts. To place the home directories of the `sidadm` user of each host on the central storage, the

`/usr/sap/SID` file systems are mounted from the `SID_shared` volume.

Junction path	Directory	Mount point at SAP HANA host	Note
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Mounted at all hosts
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Mounted at all hosts
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Mounted at all hosts
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Mounted at all hosts
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Mounted at all hosts
SID_log_mnt00003	–	/hana/log/SID/mnt00003	Mounted at all hosts
SID_data_mnt00004	–	/hana/data/SID/mnt00004	Mounted at all hosts
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Mounted at all hosts
SID_shared	shared	/hana/shared/	Mounted at all hosts
SID_shared	usr-sap-host1	/usr/sap/SID	Mounted at host 1
SID_shared	usr-sap-host2	/usr/sap/SID	Mounted at host 2
SID_shared	usr-sap-host3	/usr/sap/SID	Mounted at host 3
SID_shared	usr-sap-host4	/usr/sap/SID	Mounted at host 4
SID_shared	usr-sap-host5	/usr/sap/SID	Mounted at host 5

Volume options

You must verify and set the volume options listed in the following table on all SVMs. For some of the commands, you must switch to the advanced privilege mode within ONTAP.

Action	Command
Disable visibility of Snapshot directory	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false
Disable automatic Snapshot copies	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disable access time update except of the SID_shared volume	set advanced vol modify -vserver <vserver-name> -volume <volname> -atime-update false set admin

NFS configuration for NFSv3

The NFS options listed in the following table must be verified and set on all storage controllers.

For some of the commands shown, you must switch to the advanced privilege mode within ONTAP.

Action	Command
Enable NFSv3	nfs modify -vserver <vserver-name> v3.0 enabled
ONTAP 9: Set NFS TCP maximum transfer size to 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer -size 1048576 set admin
ONTAP 8: Set NFS read and write size to 64KB	set advanced nfs modify -vserver <vserver-name> -v3-tcp-max-read -size 65536 nfs modify -vserver <vserver-name> -v3-tcp-max -write-size 65536 set admin

NFS configuration for NFSv4

The NFS options listed in the following table must be verified and set on all SVMs.

For some of the commands, you must switch to the advanced privilege mode within ONTAP.

Action	Command
Enable NFSv4	nfs modify -vserver <vserver-name> -v4.1 enabled
ONTAP 9: Set NFS TCP maximum transfer size to 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer -size 1048576 set admin
ONTAP 8: Set NFS read and write size to 64KB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer -size 65536 set admin
Disable NFSv4 access control lists (ACLs)	nfs modify -vserver <vserver_name> -v4.1-acl disabled
Set NFSv4 domain ID	nfs modify -vserver <vserver_name> -v4-id-domain <domain-name>
Disable NFSv4 read delegation	nfs modify -vserver <vserver_name> -v4.1-read -delegation disabled
Disable NFSv4 write delegation	nfs modify -vserver <vserver_name> -v4.1-write -delegation disabled
Set the NFSv4 lease time	set advanced nfs modify -vserver <vserver_name> -v4-lease -seconds 10 set admin
Disable NFSv4 numeric ids	nfs modify -vserver <vserver_name> -v4-numeric-ids disabled

For NFS version 4. 0, replace `4. 1` with `4.0` in the previous commands. Although NFSv4.0 is supported, using NFSv4.1 is preferred.

The NFSv4 domain ID must be set to the same value on all Linux servers (`/etc/idmapd.conf`) and SVMs, as described in SAP HANA installation preparations for NFSv4.

If you are using NFSV4.1, then pNFS is enabled and used by default (recommended).

Set the NFSv4 lease time at the SVM as shown in the following table if SAP HANA multiple- host systems are used.

Action	Command
Set the NFSv4 lease time.	set advanced nfs modify -vserver <vserver_name> -v4-lease -seconds 10 set admin

Starting with HANA 2.0 SPS4, HANA provides parameters to control failover behavior. Instead of setting the lease time at the SVM level, NetApp recommends using these HANA parameters. The parameters are within `nameserver.ini` as shown in the following table. Keep the default retry interval of 10 seconds within these sections.

Section within nameserver.ini	Parameter	Value
failover	normal_retries	9
distributed_watchdog	deactivation_retries	11
distributed_watchdog	takeover_retries	9

Mount volumes to namespace and set export policies

When a volume is created, the volume must be mounted to the namespace. In this document, we assume that the junction path name is the same as the volume name. By default, the volume is exported with the default policy. The export policy can be adapted if required.

Next: Host setup.

Host setup

Previous: Storage controller setup.

All the steps described in this section are valid for both SAP HANA environments on physical servers and for SAP HANA running on VMware vSphere.

Configuration parameter for SUSE Linux Enterprise Server

Additional kernel and configuration parameters at each SAP HANA host must be adjusted for the workload generated by SAP HANA.

SUSE Linux Enterprise Server 12 and 15

Starting with SUSE Linux Enterprise Server (SLES) 12 SP1, the kernel parameter must be set in a configuration file in the `/etc/sysctl.d `directory. For example, a configuration file with the name `91-NetApp-HANA.conf` must be created.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384 16777216
net.core.netdev_max_backlog =
300000net.ipv4.tcp_slow_start_after_idle=0net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

Saptune, which is included in SLES for SAP OS versions, can be used to set these values. See SAP Note 3024346 (requires SAP login).

If NFSv3 is used for connecting the storage, the `sunrpc.tcp_max_slot_table_entries` parameter must be set in `/etc/modprobe.d/sunrpc.conf`. If the file does not exist, it must first be created by adding the following line:

```
options sunrpc tcp_max_slot_table_entries=128
```

If the nconnect mount option is used, the above value can be increased from 256 to 512.

Configuration parameter for Red Hat Enterprise Linux 7.2 or later

You must adjust additional kernel and configuration parameters at each SAP HANA host must for the workload generated by SAP HANA.

If NFSv3 is used for connecting the storage, you must set the parameter `sunrpc.tcp_max_slot_table_entries` in `/etc/modprobe.d/sunrpc.conf`. If the file does not exist, you must first create it by adding the following line:

```
options sunrpc tcp_max_slot_table_entries=128
```

If the nconnect mount option is used, the above value can be increased from 256 to 512.

Starting with Red Hat Enterprise Linux 7.2, you must set the kernel parameters in a configuration file in the `/etc/sysctl.d` directory. For example, a configuration file with the name `91-NetApp-HANA.conf` must be created.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog =
300000net.ipv4.tcp_slow_start_after_idle=0net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

Create subdirectories in /hana/shared volume

The examples show an SAP HANA database with SID=NF2.

To create the required subdirectories, take one of the following actions:

- For a single- host system, mount the `/hana/shared` volume and create the `shared` and `usr-sap` subdirectories.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:/mnt/tmp # umount /mnt/tmp
```

- For a multiple-host system, mount the `/hana/shared` volume and create the `shared` and the `usr-sap` subdirectories for each host.

  The example commands show a 2+1 multiple-host HANA system.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt # cd ..
sapcc-hana-tst-06:/mnt/tmp # umount /mnt/tmp
```

Create mount points

The examples show an SAP HANA database with SID=NF2.

To create the required mount point directories, take one of the following actions:

- For a single-host system, create mount points and set the permissions on the database host.

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- For a multiple-host system, create mount points and set the permissions on all worker and standby hosts.

  The following example commands are for a 2+1 multiple-host HANA system.

  - First worker host:

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- Second worker host:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- Standby host:

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

Mount file systems

Different mount options must be used depending on the NFS version and ONTAP release. The following file systems must be mounted to the hosts:

- `/hana/data/SID/mnt0000*`
- `/hana/log/SID/mnt0000*`
- `/hana/shared`
- `/usr/sap/SID`

The following table shows the NFS versions that must be used for the different file systems for single-host and multiple-host SAP HANA databases.

File systems	SAP HANA single host	SAP HANA multiple hosts
/hana/data/SID/mnt0000*	NFSv3 or NFSv4	NFSv4
/hana/log/SID/mnt0000*	NFSv3 or NFSv4	NFSv4
/hana/shared	NFSv3 or NFSv4	NFSv3 or NFSv4
/usr/sap/SID	NFSv3 or NFSv4	NFSv3 or NFSv4

The following table shows the mount options for the various NFS versions and ONTAP releases. The common parameters are independent of the NFS and ONTAP versions.

SAP LaMa requires the /usr/sap/SID directory to be local. Therefore, do not mount an NFS volume for /usr/sap/SID if you are using SAP LaMa.

For NFSv3, you must switch off NFS locking to avoid NFS lock cleanup operations if there is a software or server failure.

With ONTAP 9, the NFS transfer size can be configured up to 1MB. Specifically, with 40GbE or faster connections to the storage system, you must set the transfer size to 1MB to achieve the expected throughput values.

Common parameter	NFSv3	NFSv4	NFSv4.1	NFS transfer size with ONTAP 9	NFS transfer size with ONTAP 8
rw, bg, hard, timeo=600, noatime,	vers=3,nolock,	vers=4,minorversion=0,lock	vers=4,minorversion=1,lock	rsize=1048576,wsize=1048576,	rsize=65536,wsize=65536,

To improve read performance with NFSv3, it is recommended that you use the `nconnect=n` mount option, which is available with SUSE Linux Enterprise Server 12 SP4 or later and RedHat Enterprise Linux (RHEL) 8.3 or later.

Performance tests show that `nconnect=8` provides good read results. Log writes might benefit from a lower number of sessions, such as `nconnect=2`. Be aware that the first mount from an NFS server (IP address) defines the amount of sessions being used. Further mounts do not change this, even if different values are used for `nconnect`.

Starting with ONTAP 9.8 and SUSE SLES15SP2 or RedHat RHEL 8.3 or higher, NetApp supports the nconnect option for NFSv4.1. For additional information, check the Linux vendor documentation.

To mount the file systems during system boot with the `/etc/fstab` configuration file, complete the following steps:

The following example shows a single host SAP HANA database with SID=NF2 using NFSv3 and an NFS transfer size of 1MB.

1. Add the required file systems to the `/etc/fstab` configuration file.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage- vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-data01>:/NF2_shared/usr- sap /usr/sap/NF2 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,nolock 0 0
<storage- vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,nolock 0 0
```

2. Run `mount -a` to mount the file systems on all hosts.

The next example shows a multiple-host SAP HANA database with SID=NF2 using NFSv4.1 for data and log file systems and NFSv3 for the `/hana/shared` and `/usr/sap/NF2` file systems. An NFS transfer size of 1MB is used.

1. Add the required file systems to the `/etc/fstab` configuration file on all hosts.

The `/usr/sap/NF2` file system is different for each database host. The following example shows `/NF2_shared/usr- sap- host1`.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage- vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs rw,
vers=4, minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576, bg,
noatime,lock 0 0
<storage- vif-data02>:/NF2_shared/usr- sap- host1 /usr/sap/NF2 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
<storage- vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576, bg, noatime,nolock
0 0
```

2. Run `mount -a` to mount the file systems on all hosts.

Next: SAP HANA installation preparations for NFSv4.

SAP HANA installation preparations for NFSv4

Previous: Host setup.

NFS version 4 and higher requires user authentication. This authentication can be accomplished by using a central user management tool such as a Lightweight Directory Access Protocol (LDAP) server or with local user accounts. The following sections describe how to configure local user accounts.

The administration user `<sidadm>` and the `sapsys` group must be created manually on the SAP HANA hosts and the storage controllers before the installation of the SAP HANA software begins.

SAP HANA hosts

If it doesn't exist, the `sapsys` group must be created on the SAP HANA host. A unique group ID must be chosen that does not conflict with the existing group IDs on the storage controllers.

The user `<sidadm>` is created on the SAP HANA host. A unique ID must be chosen that does not conflict with existing user IDs on the storage controllers.

For a multiple-host SAP HANA system, the user and group ID must be the same on all SAP HANA hosts. The group and user are created on the other SAP HANA hosts by copying the affected lines in `/etc/group` and `/etc/passwd` from the source system to all other SAP HANA hosts.

The NFSv4 domain must be set to the same value on all Linux servers (`/etc/idmapd.conf`) and SVMs. Set the domain parameter "Domain = <domain-name>" in the file `/etc/idmapd.conf` for the Linux hosts.

Enable and start the NFS IDMAPD service.

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

The latest Linux kernels do not require this step. Warning messages can be safely ignored.

Storage controllers

The user ID and group ID must be the same on the SAP HANA hosts and the storage controllers. The group and user are created by entering the following commands on the storage cluster:

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

Additionally, set the group ID of the UNIX user root of the SVM to 0.

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

Next: I/O stack configuration for SAP HANA.

I/O stack configuration for SAP HANA

Previous: SAP HANA installation preparations for NFSv4.

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage systems used.

NetApp conducted performance tests to define the ideal values. The following table lists the optimal values inferred from the performance tests.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on

Parameter	Value
async_write_submit_active	on
async_write_submit_blocks	all

For SAP HANA 1.0 versions up to SPS12, these parameters can be set during the installation of the SAP HANA database, as described in SAP note 2267798: Configuration of the SAP HANA Database During Installation Using hdbparam.

Alternatively, the parameters can be set after the SAP HANA database installation by using the `hdbparam` framework.

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Starting with SAP HANA 2.0, `hdbparam` has been deprecated, and the parameters have been moved to `global.ini`. The parameters can be set using SQL commands or SAP HANA Studio. For more details, see SAP note 2399079: Elimination of hdbparam in HANA 2. You can also set the parameters within global.ini as shown in the following text:

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Since SAP HANA 2.0 SPS5, the `setParameter.py` script can be used the set the correct parameters:

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Next: SAP HANA data volume size.

SAP HANA data volume size

Previous: I/O stack configuration for SAP HANA.

As the default, SAP HANA uses only one data volume per SAP HANA service. Due to the maximum file size limitation of the file system, we recommend limiting the maximum data volume size.

To do so automatically, set the following parameter in `global.ini` in the section `[persistence]`:

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

This creates a new data volume after the 8, 000GB limit is reached. SAP note 240005 question 15 provides more information.

Next: SAP HANA software installation.

SAP HANA software installation

Previous: SAP HANA data volume size.

Install on single-host system

The SAP HANA software installation does not require any additional preparation for a single-host system.

Install on multiple-host system

To install SAP HANA on a multiple-host system, complete the following steps:

1. Using the SAP `hdbclm` installation tool, start the installation by running the following command at one of the worker hosts. Use the `addhosts` option to add the second worker (`sapcc-hana-tst-07`) and the standby host (`sapcc-hana-tst-08`).

   ```
   sapcc-hana-tst-06:/mnt/sapcc-share/software/SAP/HANA2SP5-
   52/DATA_UNITS/HDB_LCM_LINUX_X86_64 # ./hdblcm --action=install
   --addhosts=sapcc-hana-tst-07:role=worker,sapcc-hana-tst-08:role=standby
   SAP HANA Lifecycle Management - SAP HANA Database 2.00.052.00.1599235305
   ```

```
****************************************************************************
Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.052.0000.1599259237) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.052.00.1599235305) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.5.109.1598303414) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
    SAP HANA Smart Data Access (2.00.5.000.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/SAP_HANA_SDA_20_LINUX_X86_64/packages
    SAP HANA Studio (2.3.54.000000) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.4.24.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.0.130.519) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.014.1) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI14_1.zip
    XSAC FILEPROCESSOR 1.0 (1.000.85) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_85.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.012.20341) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_HRTT_20/XSACHRTT12_20341.zip
    XS Messaging Service 1 (1.004.10) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACMESSSRV04_10.zip
    Develop and run portal services for customer apps on XSA (1.005.1)
in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV05_1.zip
    SAP Web IDE Web Client (4.005.1) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE05_1.zip
    XS JOB SCHEDULER 1.0 (1.007.12) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
```

```
52/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_12.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.25) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_25.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.3) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_3.zip
    XSA Cockpit 1 (1.001.17) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_17.zip
SAP HANA Database version '2.00.052.00.1599235305' will be installed.
Select additional components for installation:
  Index | Components | Description

-------------------------------------------------------------------------
----------------------
  1     | all        | All components
  2     | server     | No additional components
  3     | client     | Install SAP HANA Database Client version
2.5.109.1598303414
  4     | lss        | Install SAP HANA Local Secure Store version
2.4.24.0
  5     | studio     | Install SAP HANA Studio version 2.3.54.000000
  6     | smartda    | Install SAP HANA Smart Data Access version
2.00.5.000.0
  7     | xs         | Install SAP HANA XS Advanced Runtime version
1.0.130.519
  8     | afl        | Install SAP HANA AFL (incl.PAL,BFL,OFL) version
2.00.052.0000.1599259237
  9     | eml        | Install SAP HANA EML AFL version
2.00.052.0000.1599259237
  10    | epmmds     | Install SAP HANA EPM-MDS version
2.00.052.0000.1599259237
Enter comma-separated list of the selected indices [3]: 2,3
Enter Installation Path [/hana/shared]:
```

2. Verify that the installation tool installed all selected components at all worker and standby hosts.

Next: Adding additional data volume partitions.

Adding additional data volume partitions

Previous: SAP HANA software installation.

Starting with SAP HANA 2.0 SPS4, you can configure additional data volume partitions, which allows you to configure two or more volumes for the data volume of an SAP HANA tenant database. You can also scale beyond the size and performance limits of a single volume.

Using two or more individual volumes for the data volume is available for SAP HANA single-host and multiple-host systems. You can add additional data volume partitions at any time, but doing so might require a restart of the SAP HANA database.

Enabling additional data volume partitions

1. To enable additional data volume partitions, add the following entry within `global.ini` using SAP HANA Studio or Cockpit in the SYSTEMDB configuration.

```
[customizable_functionalities]
 persistence_datavolume_partition_multipath = true
```

Adding the parameter manually to the `global.ini` file requires the restart of the database.

Volume configuration for a single-host SAP HANA system

The layout of volumes for a single-host SAP HANA system with multiple partitions is like the layout for a system with one data volume partition, but with an additional data volume stored on a different aggregate as the log volume and the other data volume. The following table shows an example configuration of an SAP HANA single-host system with two data volume partitions.

Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller b
Data volume: SID_data_mnt00001	Shared volume: SID_shared	Data volume: SID_data2_mnt00001	Log volume: SID_log_mnt00001

The following table shows an example of the mount point configuration for a single-host system with two data volume partitions.

Junction path	Directory	Mount point at HANA host
SID_data_mnt00001	–	/hana/data/SID/mnt00001
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001
SID_log_mnt00001	–	/hana/log/SID/mnt00001
SID_shared	usr-sap shared	/usr/sap/SID /hana/shared

Create the new data volume and mount it to the namespace using either ONTAP System Manager or the ONTAP cluster command line interface.

Volume configuration for multiple-host SAP HANA system

The layout of volumes for a multiple-host SAP HANA system with multiple partitions is like the layout for a system with one data volume partition, but with an additional data volume stored on a different aggregate as the log volume and the other data volume. The following table shows an example configuration of an SAP HANA multiple-host system with two data volume partitions.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	–	Log volume: SID_log_mnt00001	Data2 volume: SID_data2_mnt00001
Data and log volumes for node 2	Log volume: SID_log_mnt00002	Data2 volume: SID_data2_mnt00002	Data volume: SID_data_mnt00002	–
Data and log volumes for node 3	–	Data volume: SID_data_mnt00003	Data2 volume: SID_data2_mnt00003	Log volume: SID_log_mnt00003
Data and log volumes for node 4	Data2 volume: SID_data2_mnt00004	Log volume: SID_log_mnt00004	–	Data volume: SID_data_mnt00004
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

The following table shows an example of the mount point configuration for a single-host system with two data volume partitions.

Junction path	Directory	Mount point at SAP HANA host	Note
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Mounted at all hosts
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001	Mounted at all hosts
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Mounted at all hosts
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Mounted at all hosts
SID_data2_mnt00002	–	/hana/data2/SID/mnt00002	Mounted at all hosts
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Mounted at all hosts
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Mounted at all hosts
SID_data2_mnt00003	–	/hana/data2/SID/mnt00003	Mounted at all hosts
SID_log_mnt00003	–	/hana/log/SID/mnt00003	Mounted at all hosts
SID_data_mnt00004	–	/hana/data/SID/mnt00004	Mounted at all hosts
SID_data2_mnt00004	–	/hana/data2/SID/mnt00004	Mounted at all hosts
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Mounted at all hosts
SID_shared	shared	/hana/shared/SID	Mounted at all hosts
SID_shared	usr-sap-host1	/usr/sap/SID	Mounted at host 1
SID_shared	usr-sap-host2	/usr/sap/SID	Mounted at host 2

Junction path	Directory	Mount point at SAP HANA host	Note
SID_shared	usr-sap-host3	/usr/sap/SID	Mounted at host 3
SID_shared	usr-sap-host4	/usr/sap/SID	Mounted at host 4
SID_shared	usr-sap-host5	/usr/sap/SID	Mounted at host 5

Create the new data volume and mount it to the namespace using either ONTAP System Manager or the ONTAP cluster command line interface.

Host configuration

In addition to the tasks described in the section "Host setup," you must create the additional mount points and fstab entries for the new additional data volume(s), and you must mount the new volumes.

1. Create additional mount points:
   - For a single-host system, create mount points and set the permissions on the database host.

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - For a multiple-host system, create mount points and set the permissions on all worker and standby hosts. The following example commands are for a 2+1 multiple-host HANA system.
     - First worker host:

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - Second worker host:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

     - Standby host:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

2. Add the additional file systems to the `/etc/fstab` configuration file on all hosts. An example for a single-host system using NFSv4.1 is as follows:

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw,
vers=4minorversion=1,hard,timeo=600,rsize=1048576,wsize=1048576,bg,noati
me,lock 0 0
```

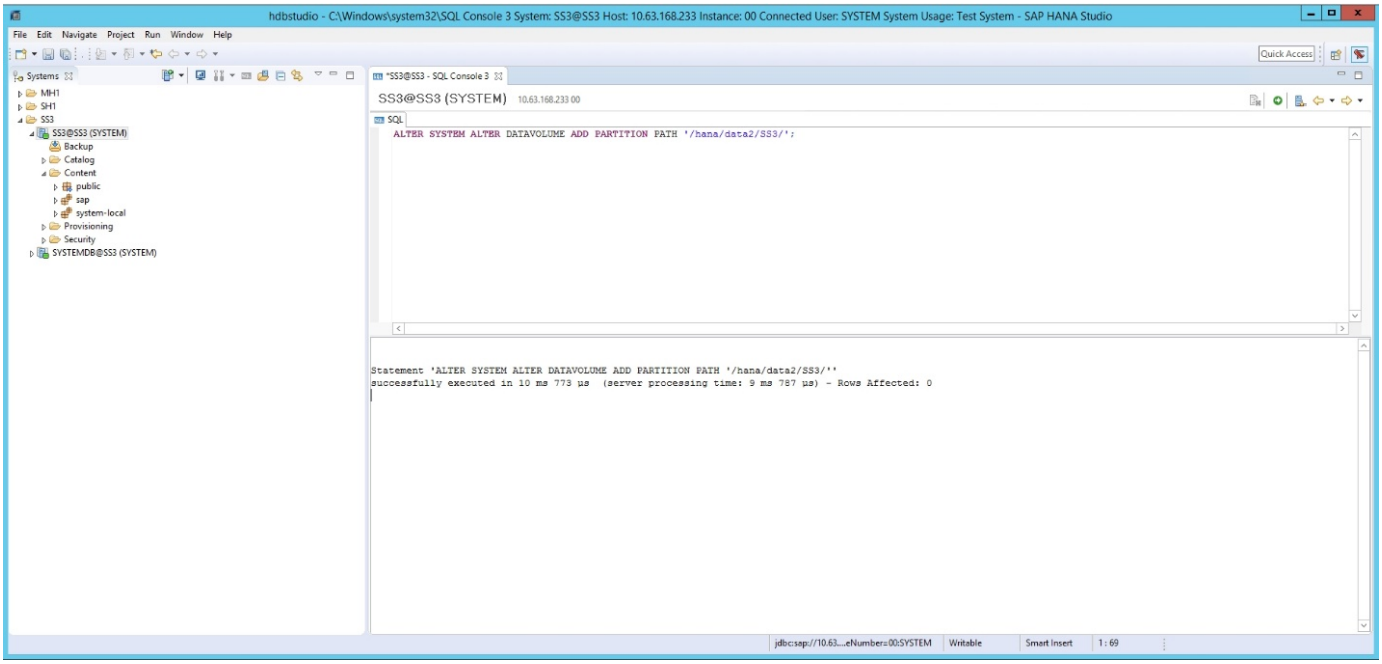
Use a different storage virtual interface for connecting to each data volume to make sure that different TCP sessions are used for each volume. You can also use the nconnect mount option if it is available for your OS.

3. To mount the file systems, run the `mount -a` command.

Adding an additional data volume partition

Execute the following SQL statement against the tenant database to add an additional data volume partition to your tenant database. Use the path to additional volume(s):

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Next: Where to find additional information.

Where to find additional information

Previous: Adding additional data volume partitions.

To learn more about the information described in this document, refer to the following documents and/or websites:

- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere www.vmware.com/files/pdf/SAP_HANA_on_vmware_vSphere_best_practices_guide.pdf

- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere www.vmware.com/files/pdf/sap-hana-scale-out-deployments-on-vsphere.pdf
- SAP Certified Enterprise Storage Hardware for SAP HANA https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/enterprise-storage.html
- SAP HANA Storage Requirements http://go.sap.com/documents/2015/03/74cdb554-5a7c-0010-82c7-eda71af511fa.html
- SAP HANA Tailored Data Center Integration Frequently Asked Questions www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html
- TR-4646: SAP HANA Disaster Recovery with Storage Replication www.netapp.com/us/media/tr-4646.pdf
- TR-4614: SAP HANA Backup and Recovery with SnapCenter www.netapp.com/us/media/tr-4614.pdf
- TR-4338: SAP HANA on VMware vSphere with NetApp FAS and AFF Systems www.netapp.com/us/media/tr-4338.pdf
- TR-4667: Automating SAP System Copies Using the SnapCenter 4.0 SAP HANA Plug- In www.netapp.com/us/media/tr-4667.pdf
- NetApp Documentation Centers https://www.netapp.com/us/documentation/index.aspx
- NetApp FAS Storage System Resources https://mysupport.netapp.com/info/web/ECMLP2676498.html
- SAP HANA Software Solutions www.netapp.com/us/solutions/applications/sap/index.aspx#sap-hana

TR-4384: SAP HANA on NetApp FAS Systems with Fibre Channel Protocol Configuration Guide

Nils Bauer and Marco Schoen, NetApp

The NetApp FAS product family has been certified for use with SAP HANA in TDI projects. The certified enterprise storage platform is characterized by the NetApp ONTAP operating system.

The certification is valid for the following models:

- FAS2720, FAS2750, FAS8200, FAS8300, FAS8700, FAS9000

For a complete list of NetApp's certified storage solutions for SAP HANA, see the certified and supported SAP HANA hardware directory.

This document describes FAS configurations that use the Fibre Channel Protocol (FCP).

The configuration described in this paper is necessary to achieve the required SAP HANA KPIs and the best performance for SAP HANA. Changing any settings or using features not listed herein might result in performance degradation or unexpected behavior and should only be done if advised by NetApp support.

The configuration guides for FAS systems using NFS and NetApp AFF systems can be found using the following links:

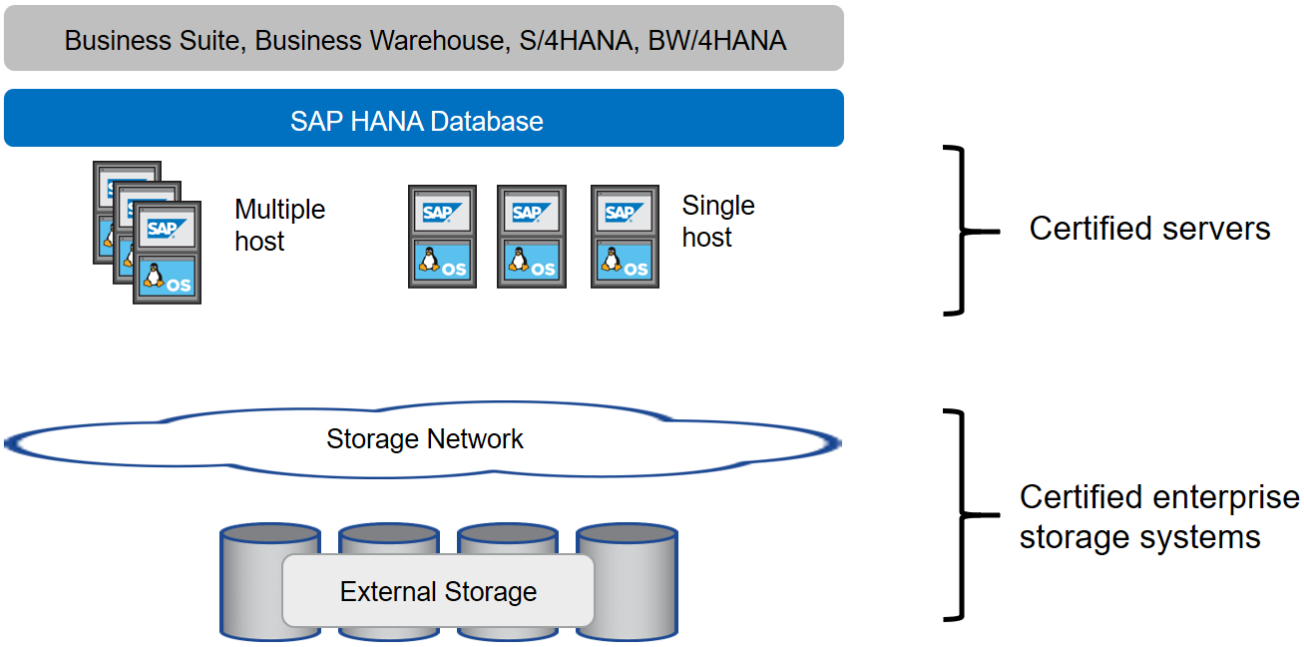
- SAP HANA on NetApp AFF Systems with Fibre Channel Protocol
- SAP HANA on NetApp FAS Systems with NFS
- SAP HANA on NetApp AFF Systems with NFS

In an SAP HANA multiple-host environment, the standard SAP HANA storage connector is used to provide fencing in the event of an SAP HANA host failover. Refer to the relevant SAP notes for operating system configuration guidelines and HANA-specific Linux kernel dependencies. For more information, see SAP Note

2235581 – SAP HANA Supported Operating Systems.

SAP HANA tailored data center integration

NetApp FAS storage controllers are certified in the SAP HANA Tailored Data Center Integration (TDI) program using NFS (NAS) and Fibre Channel (SAN) protocols. They can be deployed in any SAP HANA scenario, such as, SAP Business Suite on HANA, S/4HANA, BW/4HANA or SAP Business Warehouse on HANA in single-host or multiple-host configurations. Any server that is certified for use with SAP HANA can be combined with the certified storage solution. See the following figure for an architecture overview.



For more information regarding the prerequisites and recommendations for productive SAP HANA systems, see the following resources:

- SAP HANA Tailored Data Center Integration Frequently Asked Questions
- SAP HANA Storage Requirements

SAP HANA using VMware vSphere

There are several options for connecting storage to virtual machines (VMs). The preferred one is to connect the storage volumes with NFS directly out of the guest operating system. This option is described in SAP HANA on NetApp AFF Systems with NFS.

Raw device mappings (RDM), FCP datastores, or VVOL datastores with FCP are supported as well. For both datastore options, only one SAP HANA data or log volume must be stored within the datastore for productive use cases. In addition, Snapshot- based backup and recovery orchestrated by SnapCenter and solutions based on this, such as SAP System cloning, cannot be implemented.

For more information about using vSphere with SAP HANA, see the following links:

- SAP HANA on VMware vSphere - Virtualization - Community Wiki
- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere
- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere

- 2161991 - VMware vSphere configuration guidelines - SAP ONE Support Launchpad (Login required)

Next: Architecture.

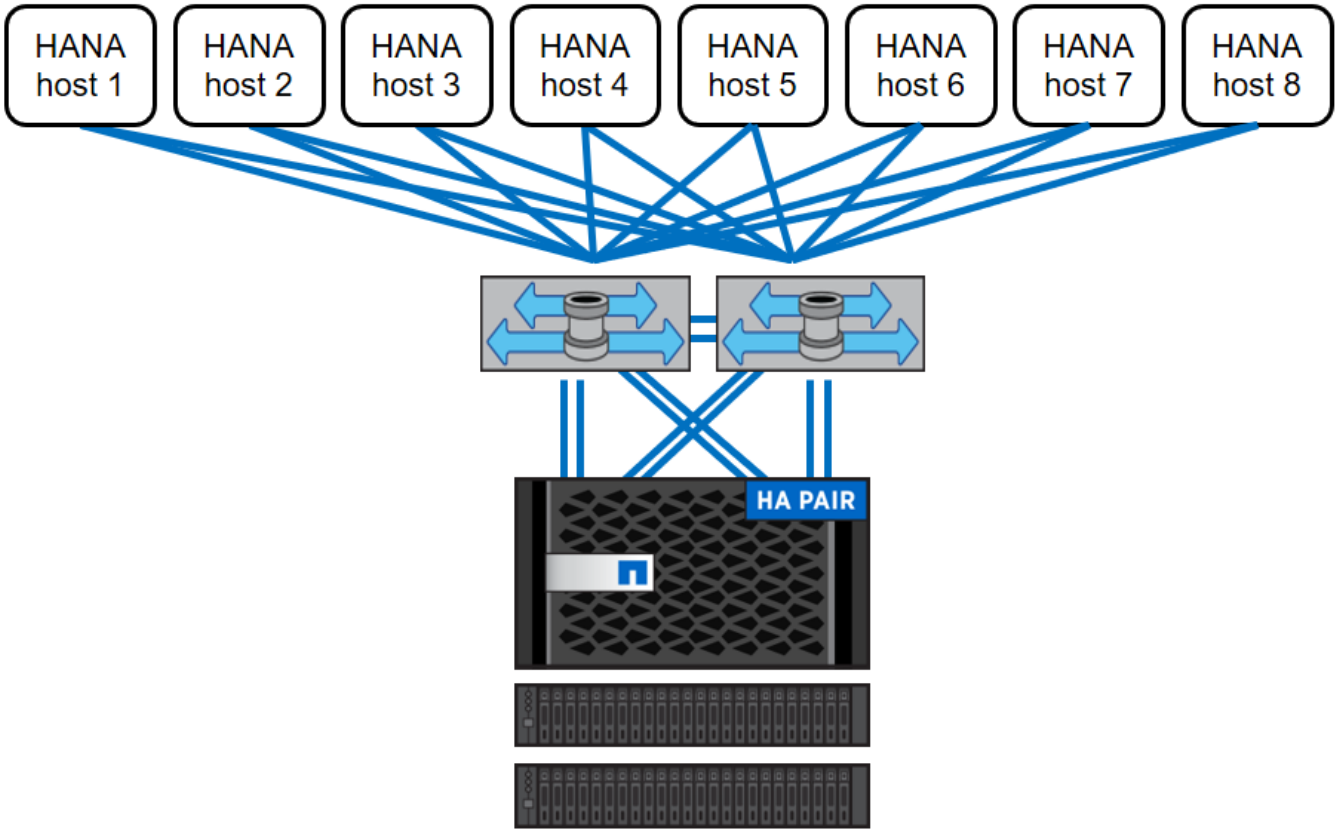
Architecture

Previous: SAP HANA on FAS Systems with FCP Configuration Guide.

SAP HANA hosts are connected to the storage controllers using a redundant FCP infrastructure and multipath software. A redundant FCP switch infrastructure is required to provide fault-tolerant SAP HANA host-to-storage connectivity in case of switch or host bus adapter (HBA) failure. Appropriate zoning must be configured at the switch to allow all HANA hosts to reach the required LUNs on the storage controllers.

Different models of the FAS product family can be used at the storage layer. The maximum number of SAP HANA hosts attached to the storage is defined by the SAP HANA performance requirements. The number of disk shelves required is determined by the capacity and performance requirements of the SAP HANA systems.

The following figure shows an example configuration with eight SAP HANA hosts attached to a storage HA pair.

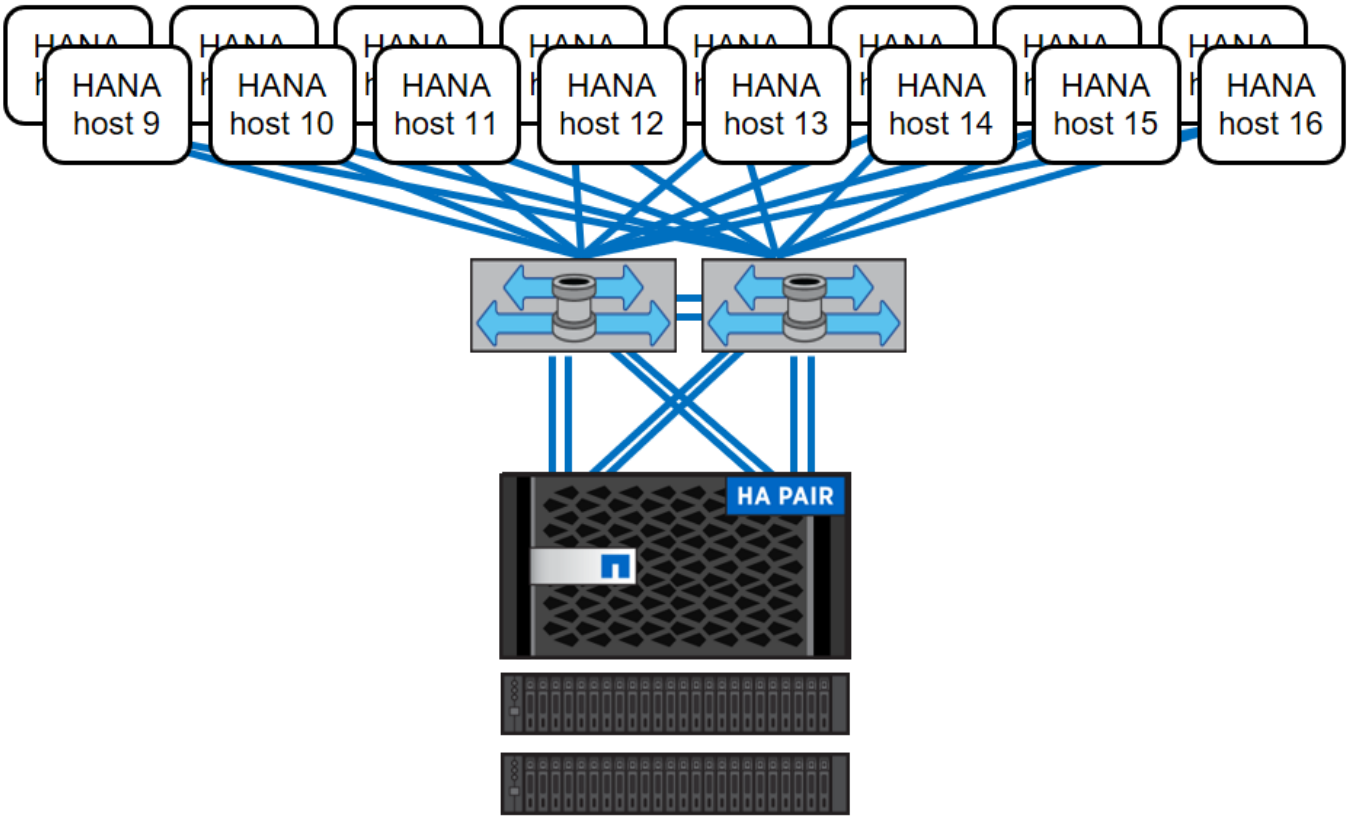


This architecture can be scaled in two dimensions:

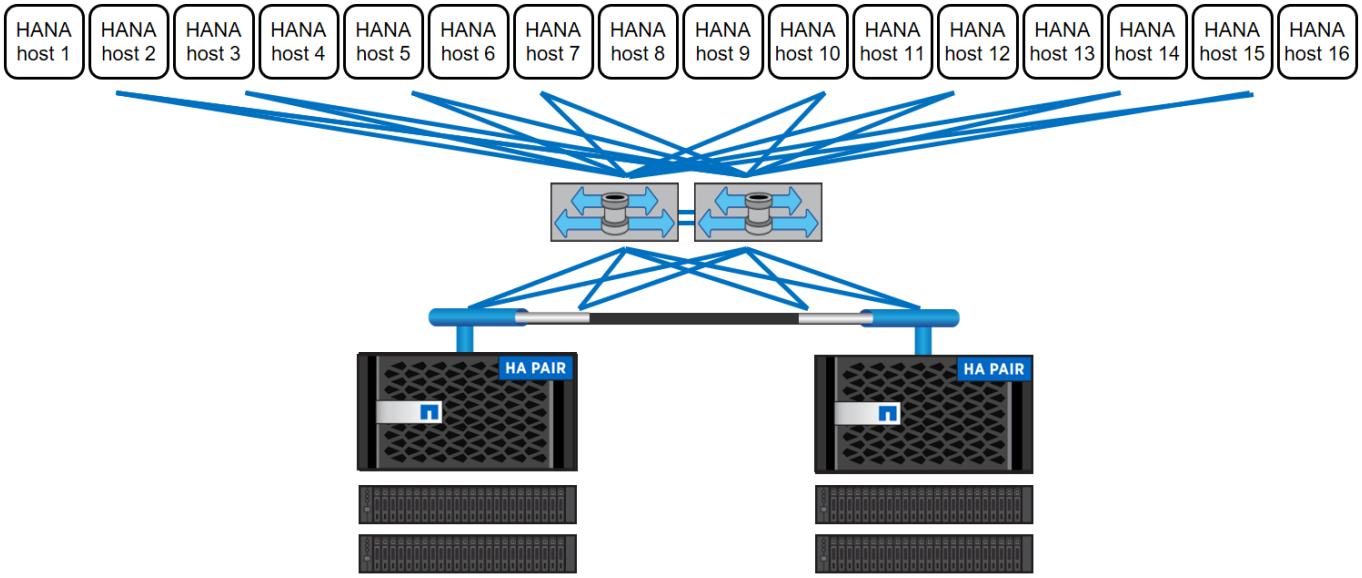
- By attaching additional SAP HANA hosts and disk capacity to the storage, assuming that the storage controllers can provide enough performance under the new load to meet key performance indicators (KPIs)
- By adding more storage systems and disk capacity for the additional SAP HANA hosts

The following figure shows a configuration example in which more SAP HANA hosts are attached to the

storage controllers. In this example, more disk shelves are necessary to meet the capacity and performance requirements of the 16 SAP HANA hosts. Depending on the total throughput requirements, you must add additional FC connections to the storage controllers.



Independent of the deployed FAS system storage model, the SAP HANA landscape can also be scaled by adding more storage controllers, as shown in the following figure.



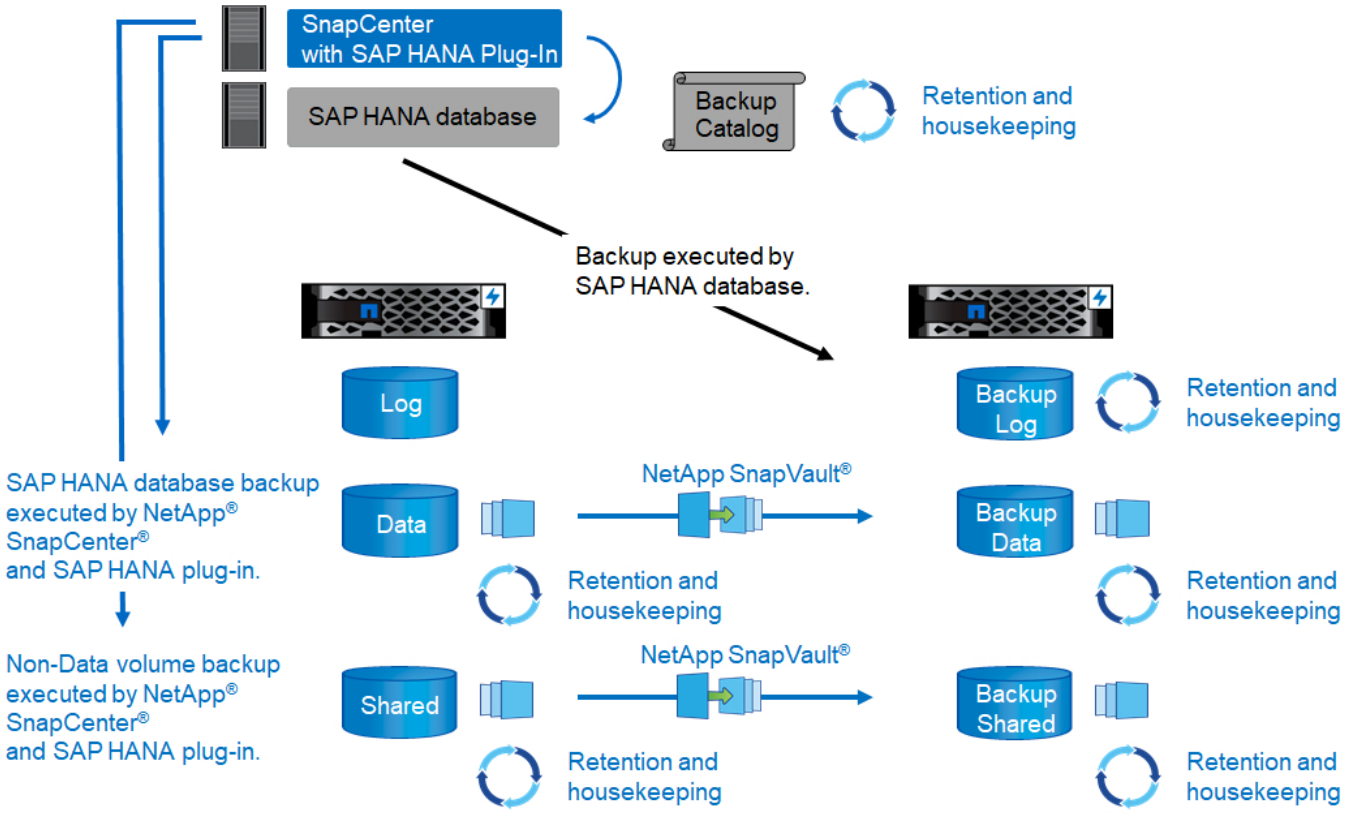
SAP HANA backup

NetApp ONTAP software provides a built-in mechanism to back up SAP HANA databases. Storage-based Snapshot backup is a fully supported and integrated backup solution available for SAP HANA single-container systems and for SAP HANA MDC single- tenant systems.

Storage-based Snapshot backups are implemented by using the NetApp SnapCenter plug-in for SAP HANA, which enables consistent storage-based Snapshot backups by using the interfaces provided by the SAP HANA database. SnapCenter registers the Snapshot backups in the SAP HANA backup catalog so that the backups are visible within the SAP HANA studio and can be selected for restore and recovery operations.

By using NetApp SnapVault software, the Snapshot copies that were created on the primary storage can be replicated to the secondary backup storage controlled by SnapCenter. Different backup retention policies can be defined for backups on the primary storage and for backups on the secondary storage. The SnapCenter Plug-in for SAP HANA Database manages the retention of Snapshot copy-based data backups and log backups including the housekeeping of the backup catalog. The SnapCenter Plug-in for SAP HANA Database also enables the execution of a block-integrity check of the SAP HANA database by performing a file-based backup.

The database logs can be backed up directly to the secondary storage by using an NFS mount, as shown in the following figure.



Storage-based Snapshot backups provide significant advantages compared to file-based backups. Those advantages include the following:

- Faster backup (few minutes)
- Faster restore on the storage layer (a few minutes)
- No effect on the performance of the SAP HANA database host, network, or storage during backup

- Space-efficient and bandwidth-efficient replication to secondary storage based on block changes

For detailed information about the SAP HANA backup and recovery solution using SnapCenter, see TR-4614: SAP HANA Backup and Recovery with SnapCenter.

SAP HANA disaster recovery

SAP HANA disaster recovery can be performed on the database layer by using SAP system replication or on the storage layer by using storage-replication technologies. The following section provides an overview of disaster recovery solutions based on storage replication.

For detailed information about the SAP HANA disaster recovery solution using SnapCenter, see TR-4646: SAP HANA Disaster Recovery with Storage Replication.

Storage replication based on SnapMirror

The following figure shows a three-site disaster recovery solution, using synchronous SnapMirror replication to the local DR datacenter and asynchronous SnapMirror to replicate data to the remote DR datacenter.

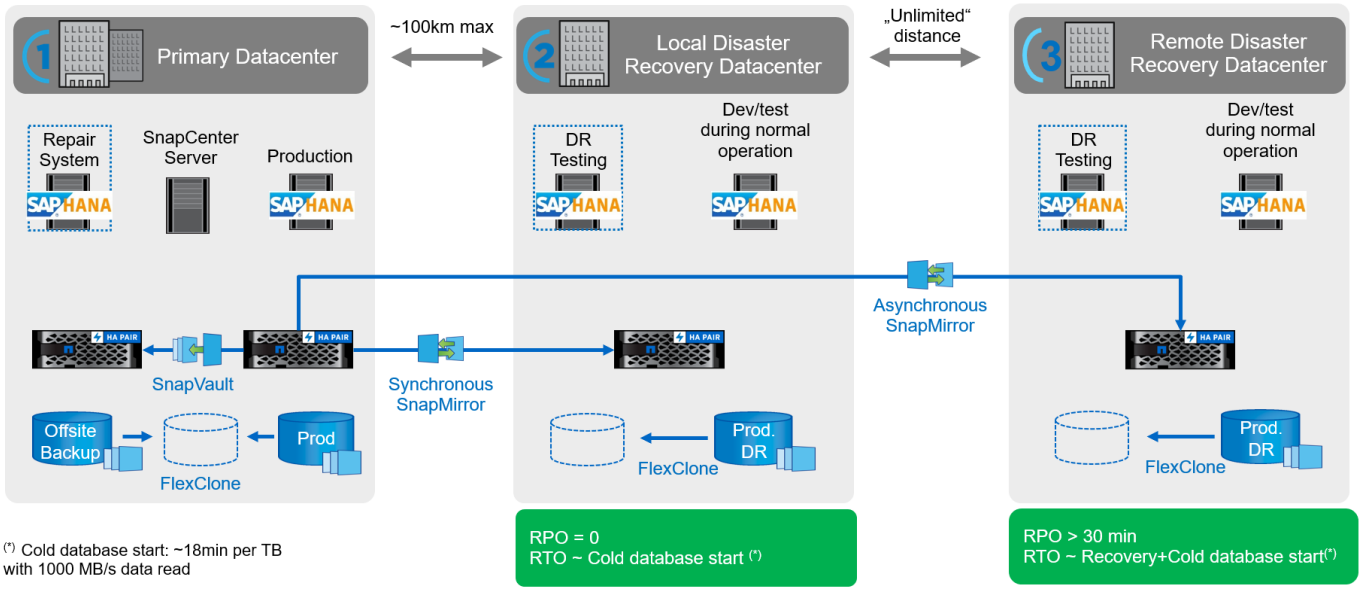
Data replication using synchronous SnapMirror provides an RPO of zero. The distance between the primary and the local DR datacenter is limited to around 100km.

Protection against failures of both the primary and the local DR site is performed by replicating the data to a third remote DR datacenter using asynchronous SnapMirror. The RPO depends on the frequency of replication updates and how fast they can be transferred. In theory, the distance is unlimited, but the limit depends on the amount of data that must be transferred and the connection that is available between the data centers. Typical RPO values are in the range of 30 minutes to multiple hours.

The RTO for both replication methods primarily depends on the time needed to start the HANA database at the DR site and load the data into memory. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data would take approximately 18 minutes.

The servers at the DR sites can be used as dev/test systems during normal operation. In the case of a disaster, the dev/test systems would need to be shut down and started as DR production servers.

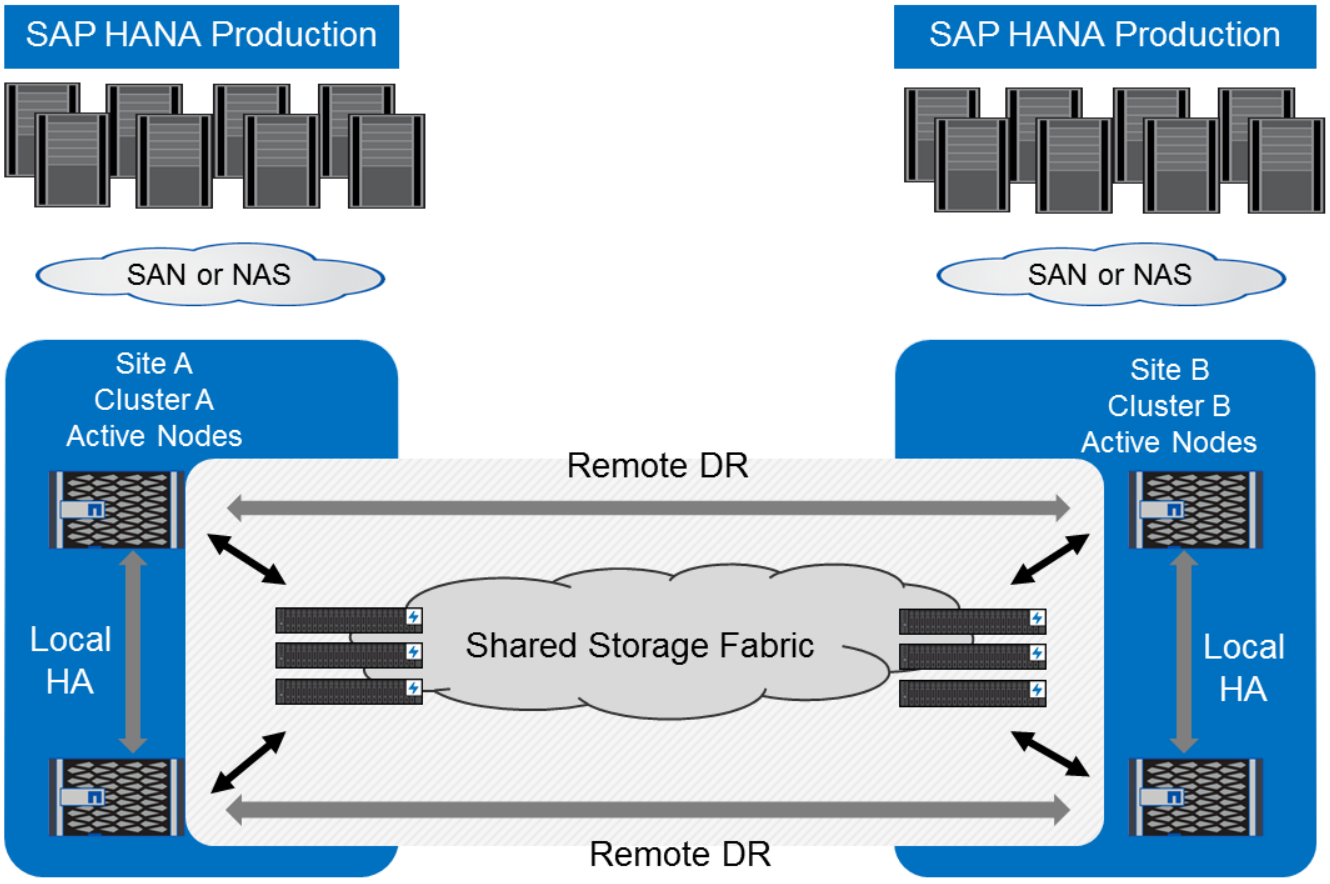
Both replication methods allow to you execute DR workflow testing without influencing the RPO and RTO. FlexClone volumes are created on the storage and are attached to the DR testing servers.



Synchronous replication offers StrictSync mode. If the write to secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage systems are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the InSync status. If the primary storage fails, application I/O can be resumed on the secondary storage after failover with no loss of data. In StrictSync mode, the RPO is always zero.

Storage replication based on NetApp MetroCluster

The following figure shows a high-level overview of the solution. The storage cluster at each site provides local high availability and is used for production workloads. The data at each site is synchronously replicated to the other location and is available in case of disaster failover.



Next: Storage sizing.

Storage sizing

Previous: Architecture.

The following section provides an overview of performance and capacity considerations for sizing a storage system for SAP HANA.

> Contact your NetApp or NetApp partner sales representative to support the storage sizing process and to create a properly sized storage environment.

Performance considerations

SAP has defined a static set of storage KPIs. These KPIs are valid for all production SAP HANA environments independent of the memory size of the database hosts and the applications that use the SAP HANA database. These KPIs are valid for single-host, multiple-host, Business Suite on HANA, Business Warehouse on HANA, S/4HANA, and BW/4HANA environments. Therefore, the current performance sizing approach depends on only the number of active SAP HANA hosts that are attached to the storage system.

> Storage performance KPIs are required only for production SAP HANA systems.

SAP delivers a performance test tool, which must be used to validate the storage performance for active SAP HANA hosts attached to the storage.

NetApp tested and predefined the maximum number of SAP HANA hosts that can be attached to a specific

storage model, while still fulfilling the required storage KPIs from SAP for production-based SAP HANA systems.

> The storage controllers of the certified FAS product family can also be used for SAP HANA with other disk types or disk back-end solutions, as long as they are supported by NetApp and fulfill SAP HANA TDI performance KPIs. Examples include NetApp Storage Encryption (NSE) and NetApp FlexArray technology.

This document describes disk sizing for SAS hard disk drives and solid-state drives.

Hard disk drives

A minimum of 10 data disks (10k RPM SAS) per SAP HANA node is required to fulfill the storage performance KPIs from SAP.

> This calculation is independent of the storage controller and disk shelf used.

Solid-state drives

With solid-state drives (SSDs), the number of data disks is determined by the SAS connection throughput from the storage controllers to the SSD shelf.

The maximum number of SAP HANA hosts that can be run on a disk shelf and the minimum number of SSDs required per SAP HANA host were determined by running the SAP performance test tool.

- The 12Gb SAS disk shelf (DS224C) with 24 SSDs supports up to 14 SAP HANA hosts, when the disk shelf is connected with 12Gb.
- The 6Gb SAS disk shelf (DS2246) with 24 SSDs supports up to 4 SAP HANA hosts.

The SSDs and the SAP HANA hosts must be equally distributed between both storage controllers.

The following table summarizes the supported number of SAP HANA hosts per disk shelf.

	6Gb SAS shelves (DS2246) fully loaded with 24 SSDs	12Gb SAS shelves (DS224C) fully loaded with 24 SSDs
Maximum number of SAP HANA hosts per disk shelf	4	14

> This calculation is independent of the storage controller used. Adding more disk shelves does not increase the maximum number of SAP HANA hosts that a storage controller can support.

Mixed workloads

SAP HANA and other application workloads running on the same storage controller or in the same storage aggregate are supported. However, it is a NetApp best practice to separate SAP HANA workloads from all other application workloads.

You might decide to deploy SAP HANA workloads and other application workloads on either the same storage controller or the same aggregate. If so, you must make sure that enough performance is always available for SAP HANA within the mixed workload environment. NetApp also recommends that you use quality of service (QoS) parameters to regulate the impact these other applications could have on SAP HANA applications.

The SAP HCMT test tool must be used to check if additional SAP HANA hosts can be run on a storage controller that is already used for other workloads. However, SAP application servers can be safely placed on the same storage controller and aggregate as the SAP HANA databases.

Capacity considerations

A detailed description of the capacity requirements for SAP HANA is in the SAP HANA Storage Requirements white paper.

The capacity sizing of the overall SAP landscape with multiple SAP HANA systems must be determined by using SAP HANA storage sizing tools from NetApp. Contact NetApp or your NetApp partner sales representative to validate the storage sizing process for a properly sized storage environment.

Configuration of performance test tool

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage system used. These parameters must also be set for the performance test tool from SAP (fsperf) when the storage performance is tested by using the SAP test tool.

Performance tests were conducted by NetApp to define the optimal values. The following table lists the parameters that must be set within the configuration file of the SAP test tool.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on
async_write_submit_blocks	all

For more information about the configuration of SAP test tool, see SAP note 1943937 for HWCCT (SAP HANA 1.0) and SAP note 2493172 for HCMT/HCOT (SAP HANA 2.0).

The following example shows how variables can be set for the HCMT/HCOT execution plan.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
      {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
```

```
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

These variables must be used for the test configuration. This is usually the case with the predefined execution

plans SAP delivers with the HCMT/HCOT tool. The following example for a 4k log write test is from an execution plan.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

Storage sizing process overview

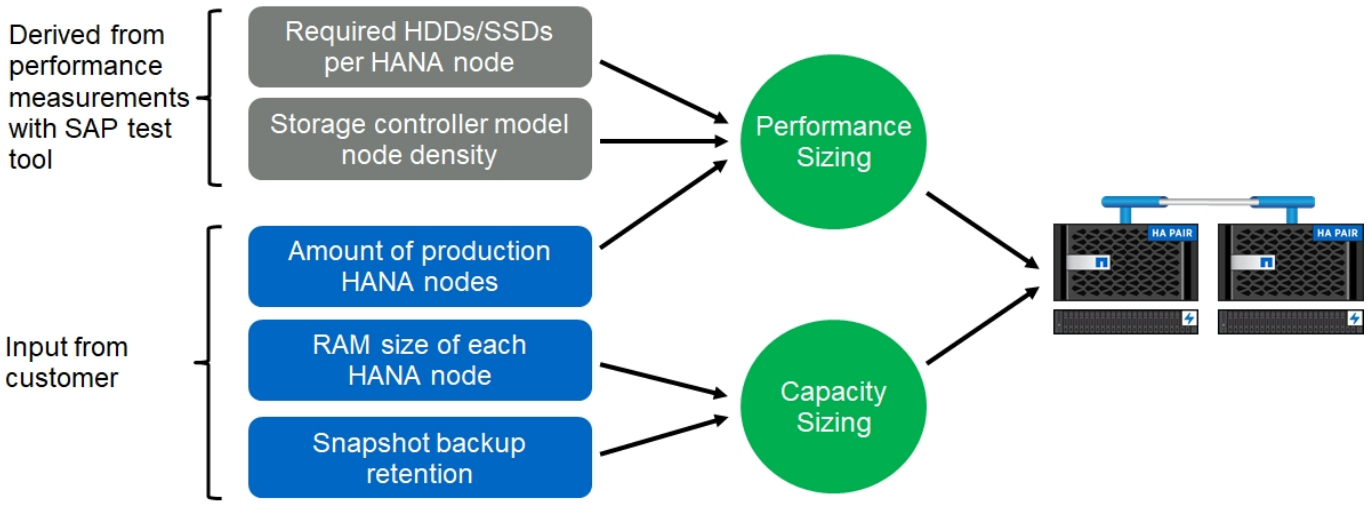
The number of disks per HANA host and the SAP HANA host density for each storage model were determined with the SAP HANA test tool.

The sizing process requires details such as the number of production and nonproduction SAP HANA hosts, the RAM size of each host, and the backup retention period of the storage-based Snapshot copies. The number of

SAP HANA hosts determines the storage controller and the number of disks required.

The size of the RAM, the net data size on the disk of each SAP HANA host, and the Snapshot copy backup retention period are used as inputs during capacity sizing.

The following figure summarizes the sizing process.



Next: Infrastructure setup and configuration.

Overview

Previous: Storage sizing.

The following sections provide SAP HANA infrastructure setup and configuration guidelines. All the steps needed to set up SAP HANA are included. An SVM is created to host the data. Within these sections, the following example configurations are used:

- HANA system with SID=SS3 and ONTAP 9.7 or earlier
  - SAP HANA single and multiple host
  - SAP HANA single host using SAP HANA multiple partitions
- HANA system with SID=FC5 and ONTAP 9.8 using Linux logical volume manager (LVM)
  - SAP HANA single and multiple host

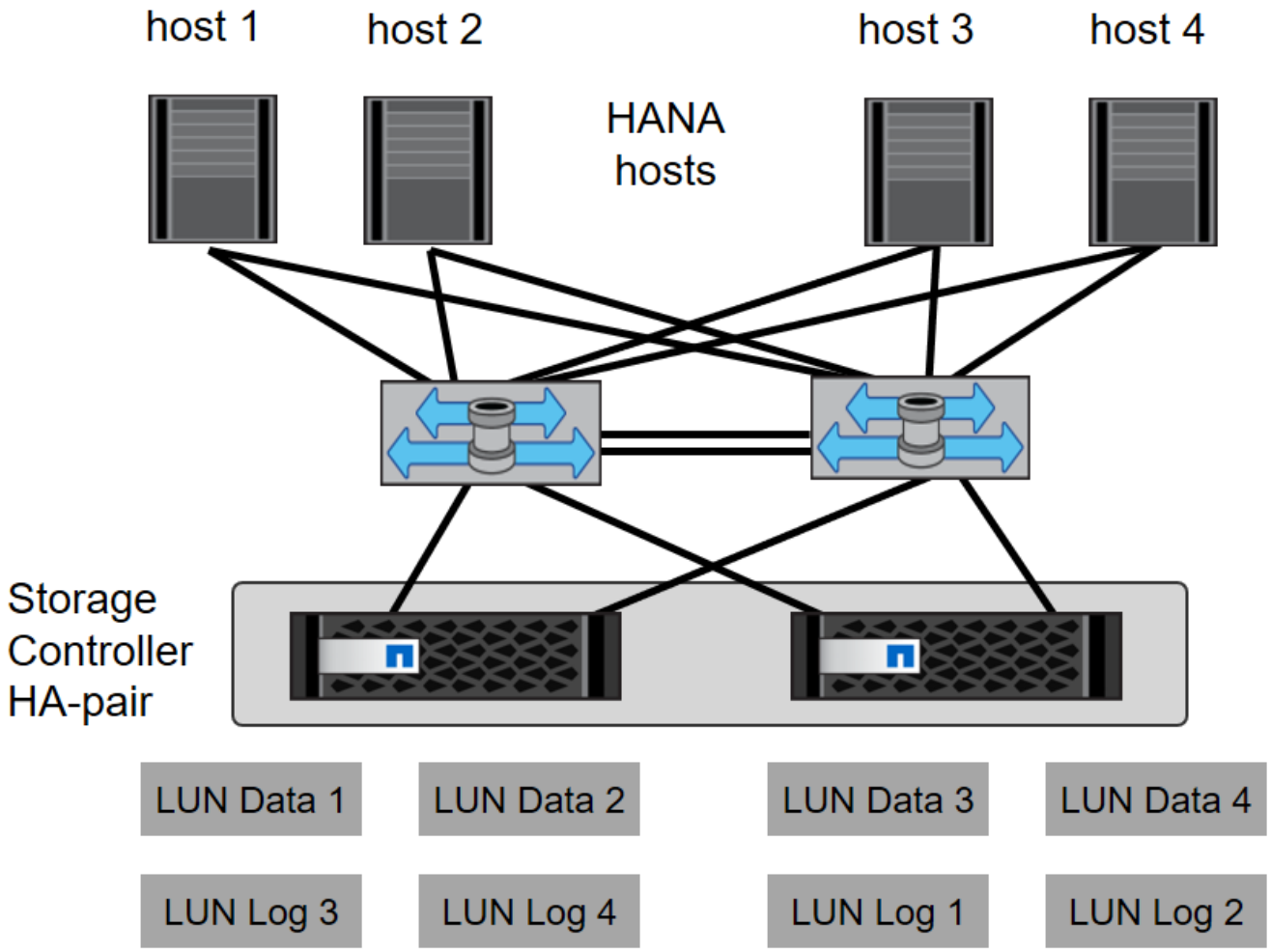
Next: SAN fabric setup.

SAN fabric setup

Previous: Infrastructure setup and configuration.

Each SAP HANA server must have a redundant FCP SAN connection with a minimum of 8Gbps bandwidth. For each SAP HANA host attached to a storage controller, at least 8Gbps of bandwidth must be configured at the storage controller.

The following figure shows an example with four SAP HANA hosts attached to two storage controllers. Each SAP HANA host has two FCP ports connected to the redundant fabric. At the storage layer, four FCP ports are configured to provide the required throughput for each SAP HANA host.



In addition to the zoning on the switch layer, you must map each LUN on the storage system to the hosts that connect to this LUN. Keep the zoning on the switch simple; that is, define one zone set in which all host HBAs can see all controller HBAs.

Next: Time synchronization.

Time synchronization

Previous: SAN fabric setup.

You must synchronize the time between the storage controllers and the SAP HANA database hosts. The same time server must be set for all storage controllers and all SAP HANA hosts.

Next: Storage controller setup.

Storage controller setup

Previous: Time synchronization.

This section describes the configuration of the NetApp storage system. You must complete the primary installation and setup according to the corresponding ONTAP setup and configuration guides.

Storage efficiency

Inline deduplication, cross- volume inline deduplication, inline compression, and inline compaction are supported with SAP HANA in an SSD configuration.

Enabling the storage efficiency features in an HDD configuration is not supported.

NetApp Volume Encryption

The use of NetApp Volume Encryption (NVE) is supported for SAP HANA.

Quality of service

QoS can be used to limit the storage throughput for specific SAP HANA systems. One use case would be to limit the throughput of development and test systems so that they cannot influence production systems in a mixed setup.

During the sizing process, the performance requirements of a nonproduction system must be determined. Development and test systems can be sized with lower performance values, typically in the range of 20% to 50% of a production system.

Starting with ONTAP 9, QoS is configured on the storage volume level and uses maximum values for throughput (MBps) and number of I/O (IOPS).

Large write I/O has the biggest performance effect on the storage system. Therefore, the QoS throughput limit should be set to a percentage of the corresponding write SAP HANA storage performance KPI values in the data and log volumes.

NetApp FabricPool

NetApp FabricPool technology must not be used for active primary file systems in SAP HANA systems. This includes the file systems for the data and log area as well as the `/hana/shared` file system. Doing so results in unpredictable performance, especially during the startup of an SAP HANA system.

Using the “snapshot-only” tiering policy is possible as well as using FabricPool in general at a backup target such as SnapVault or SnapMirror destination.

Using FabricPool for tiering Snapshot copies at primary storage or using FabricPool at a backup target changes the required time for the restore and recovery of a database or other tasks such as creating system clones or repair systems. Take this into consideration for planning your overall lifecycle- management strategy, and check to make sure that your SLAs are still being met while using this function.

FabricPool is a good option for moving log backups to another storage tier. Moving backups affects the time needed to recover an SAP HANA database. Therefore, the option “tiering-minimum-cooling-days” should be set to a value that places log backups, which are routinely needed for recovery, on the local fast storage tier.

Configure storage

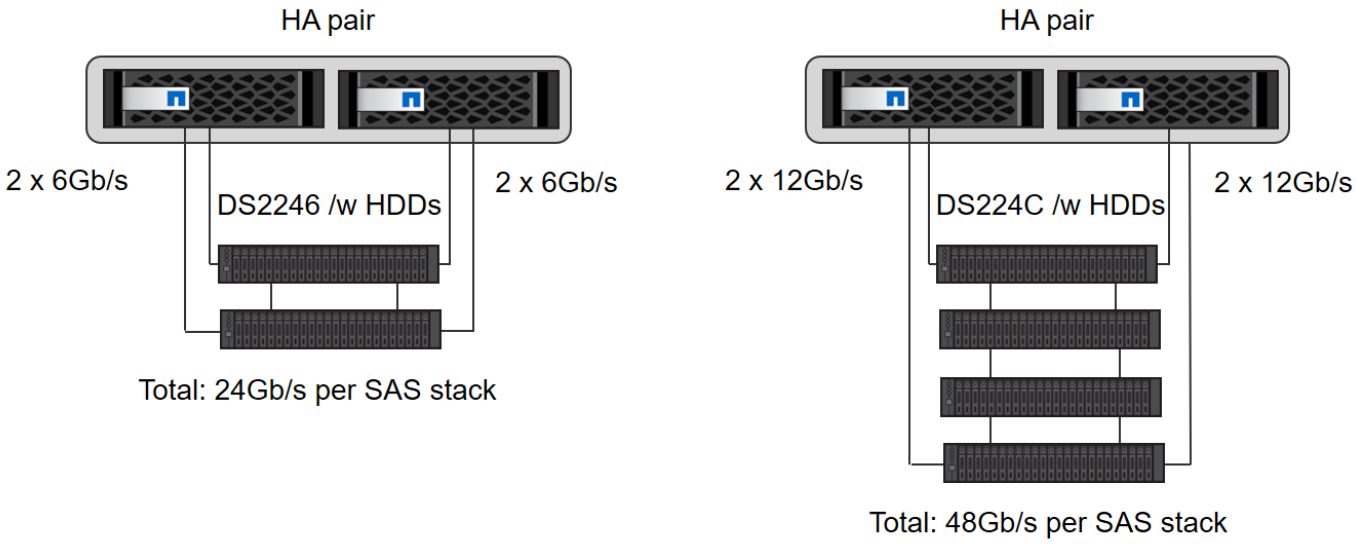
The following overview summarizes the required storage configuration steps. Each step is covered in more detail in the subsequent sections. Before initiating these steps, complete the storage hardware setup, the ONTAP software installation, and the connection of the storage FCP ports to the SAN fabric.

1. Check the correct SAS stack configuration, as described in the section Disk shelf connection.

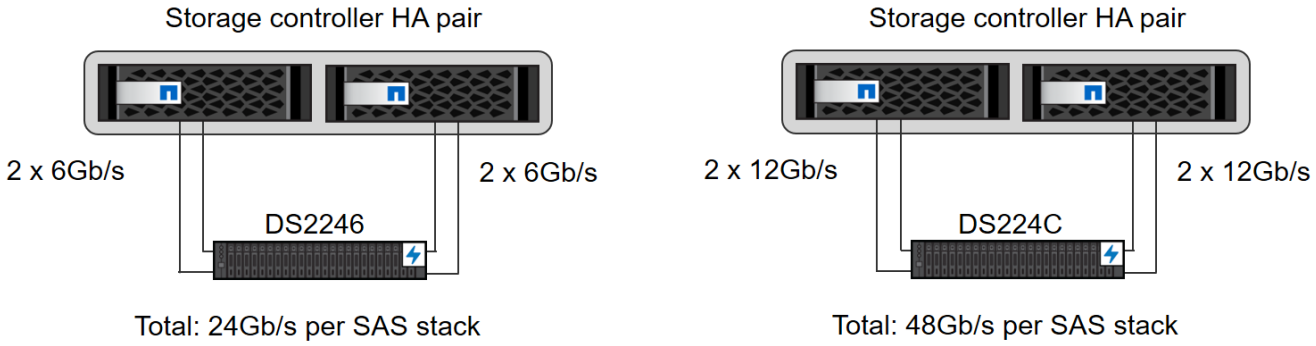
2. Create and configure the required aggregates, as described in the section Aggregate configuration.
3. Create a storage virtual machine (SVM) as described in the section Storage virtual machine configuration.
4. Create logical interfaces (LIFs) as described in the section Logical interface configuration.
5. Create FCP port sets as described in the section FCP port sets.
6. Create initiator groups (igroups) with worldwide names (WWNs) of HANA servers as described in the section Initiator groups.
7. Create volumes and LUNs within the aggregates as described in the section Volume and LUN configuration for SAP HANA single-host systems and Volume and LUN configuration for SAP HANA multiple-host systems.

Disk shelf connection

With HDDs, a maximum of two DS2246 disk shelves or four DS224C disk shelves can be connected to one SAS stack to provide the required performance for the SAP HANA hosts, as shown in the following figure. The disks within each shelf must be distributed equally to both controllers of the HA pair.



With SSDs, a maximum of one disk shelf can be connected to one SAS stack to provide the required performance for the SAP HANA hosts, as shown in the following figure. The disks within each shelf must be distributed equally to both controllers of the HA pair. With the DS224C disk shelf, quad-path SAS cabling can also be used but is not required.

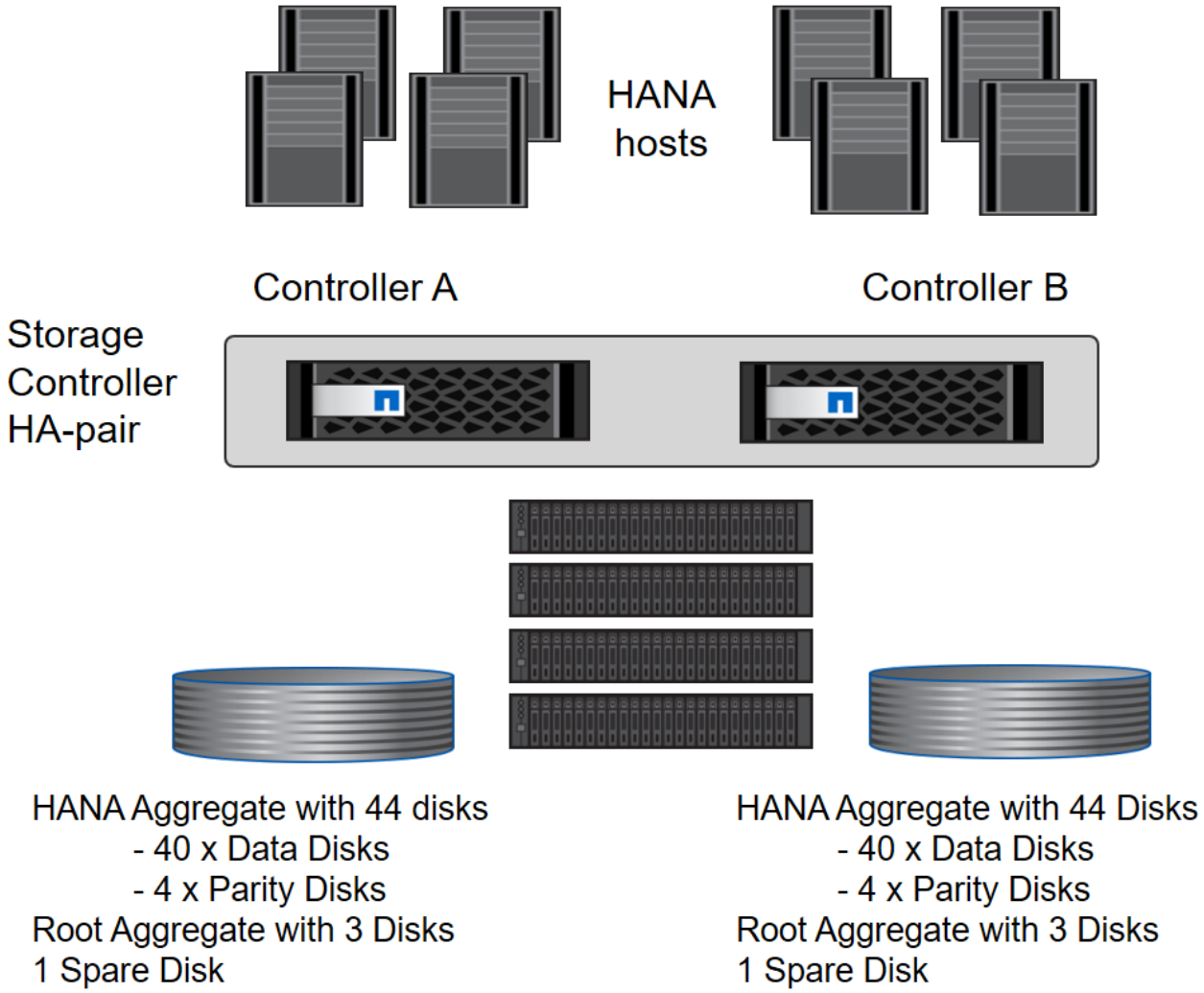


Aggregate configuration

In general, you must configure two aggregates per controller, independent of which disk shelf or disk technology (SSD or HDD) is used. This step is necessary so that you can use all available controller resources. For FAS 2000 series systems, one data aggregate is sufficient.

Aggregate configuration with HDDs

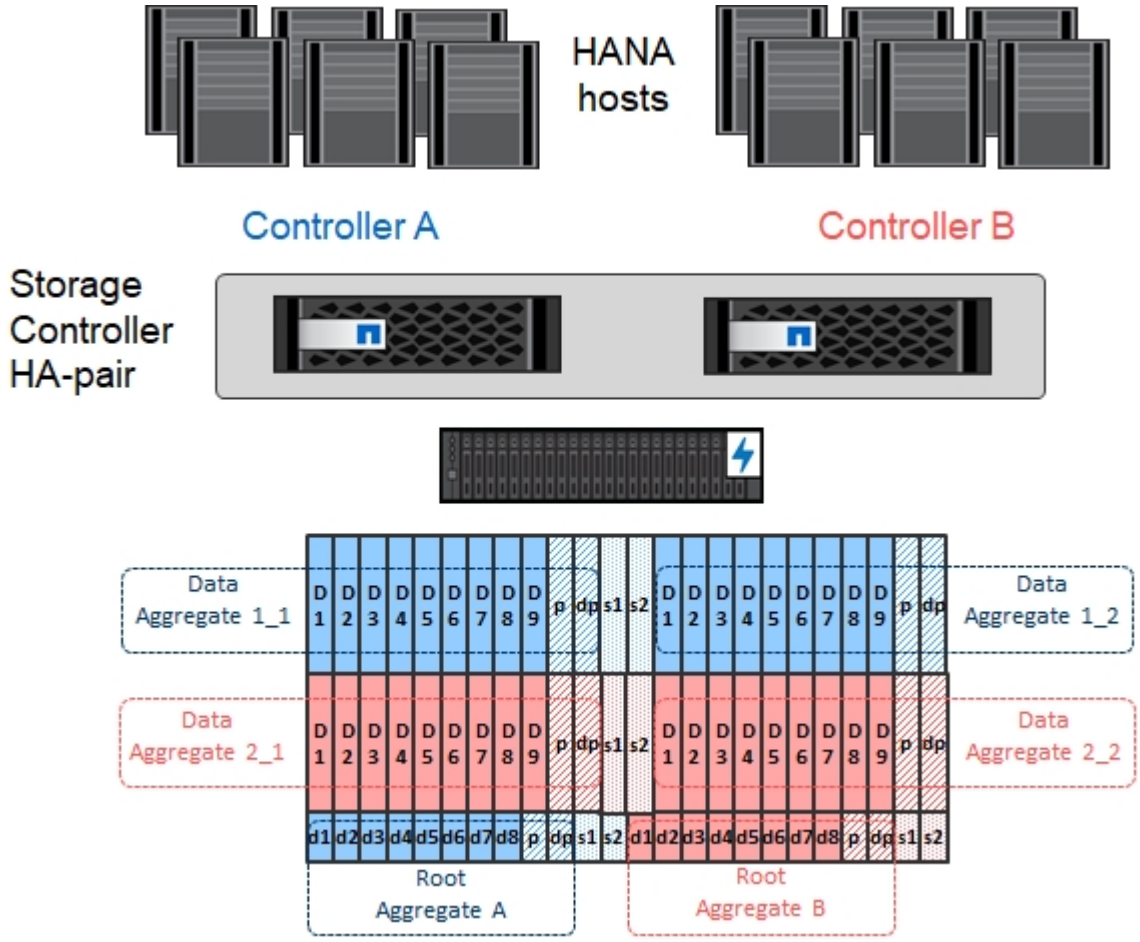
The following figure shows a configuration for eight SAP HANA hosts. Four SAP HANA hosts are attached to each storage controller. Two separate aggregates, one at each storage controller, are configured. Each aggregate is configured with 4 × 10 = 40 data disks (HDDs).



Aggregate configuration with SDD-only systems

In general, two aggregates per controller must be configured, independently of which disk shelf or disk technology (SSDs or HDDs) is used. For FAS2000 series systems, one data aggregate is sufficient.

The following figure shows a configuration of 12 SAP HANA hosts running on a 12Gb SAS shelf configured with ADPv2. Six SAP HANA hosts are attached to each storage controller. Four separate aggregates, two at each storage controller, are configured. Each aggregate is configured with 11 disks with nine data and two parity disk partitions. For each controller, two spare partitions are available.

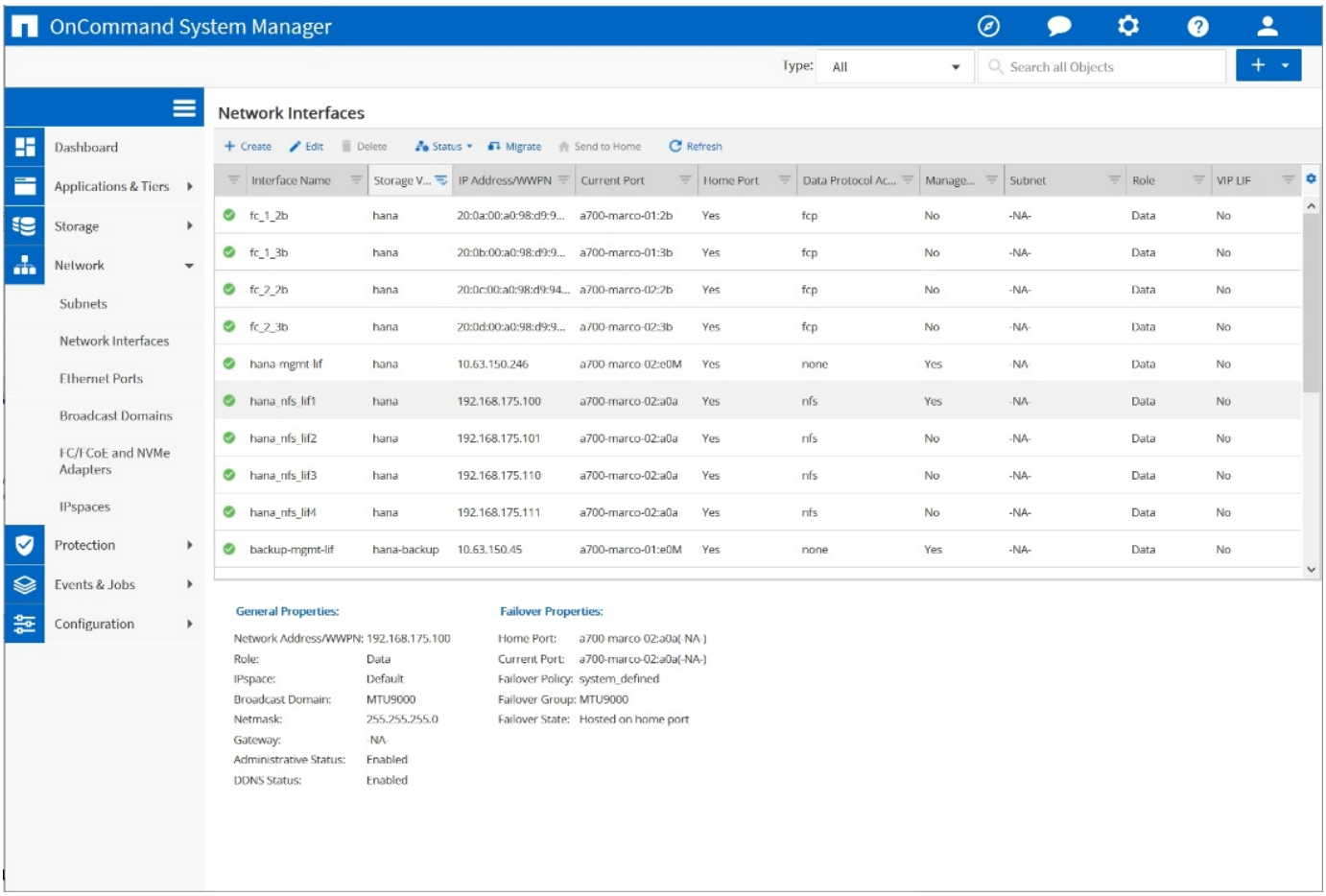


Storage virtual machine configuration

Multiple-host SAP landscapes with SAP HANA databases can use a single SVM. An SVM can also be assigned to each SAP landscape if necessary in case they are managed by different teams within a company. The screenshots and command outputs in this document use an SVM named `hana`.

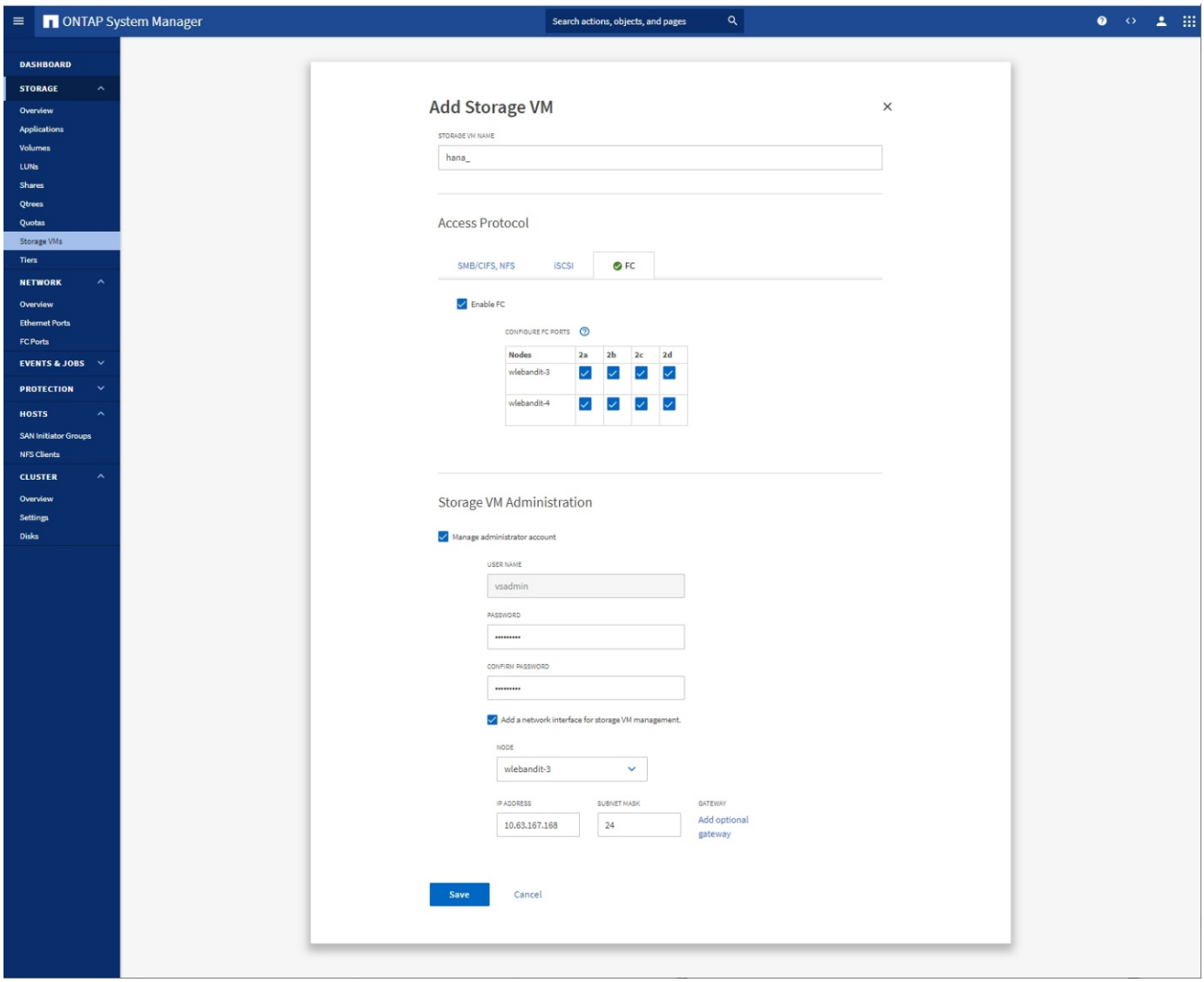
Logical interface configuration

Within the storage cluster configuration, one network interface (LIF) must be created and assigned to a dedicated FCP port. If, for example, four FCP ports are required for performance reasons, four LIFs must be created. The following figure shows a screenshot of the four LIFs (named `fc_*_*)` that were configured on the `hana` SVM.



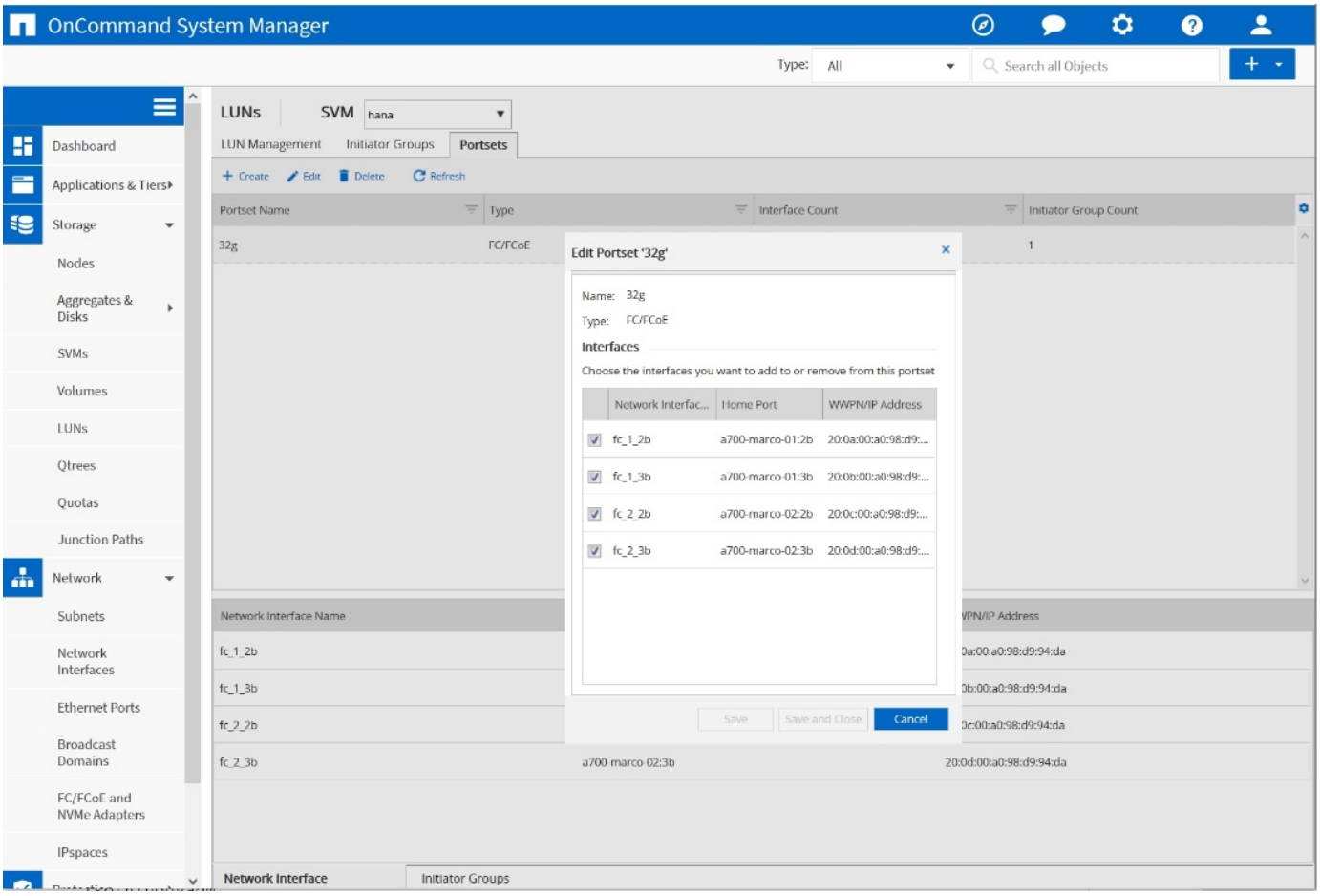
During SVM creation with ONTAP 9.8 System Manager, all the required physical FCP ports can be selected, and one LIF per physical port is created automatically.

The following figure depicts the creation of SVM and LIFs with ONTAP 9.8 System Manager.



FCP port sets

An FCP port set is used to define which LIFs are to be used by a specific igroup. Typically, all LIFs created for the HANA systems are placed in the same port set. The following figure shows the configuration of a port set named 32g, which includes the four LIFs that were already created.



With ONTAP 9.8, a port set is not required, but it can be created and used through the command line.

Initiator groups

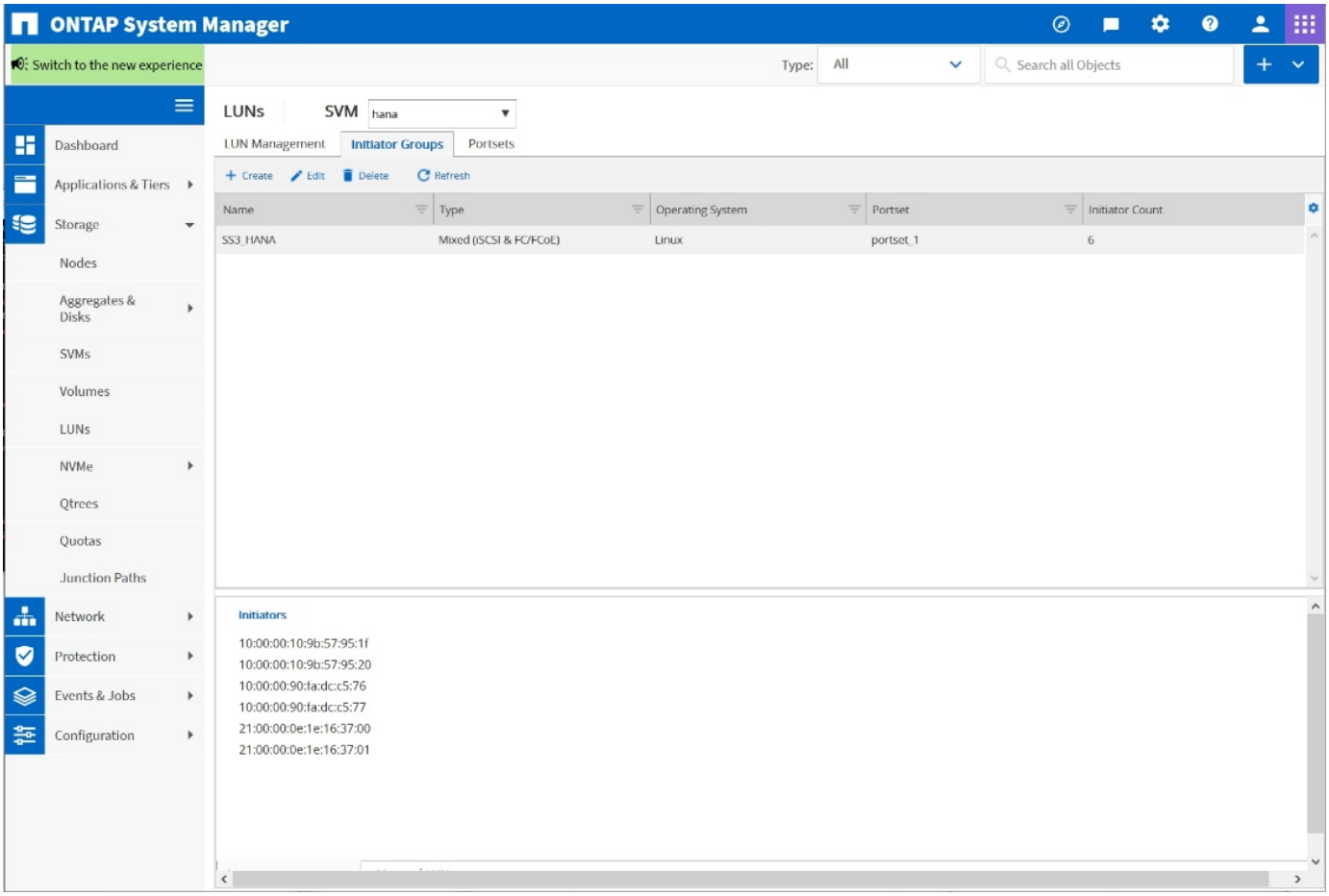
An igroup can be configured for each server or for a group of servers that require access to a LUN. The igroup configuration requires the worldwide port names (WWPNs) of the servers.

Using the `sanlun` tool, run the following command to obtain the WWPNs of each SAP HANA host:

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm
host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

The `sanlun` tool is part of the NetApp Host Utilities and must be installed on each SAP HANA host. More details can be found in section Host setup.

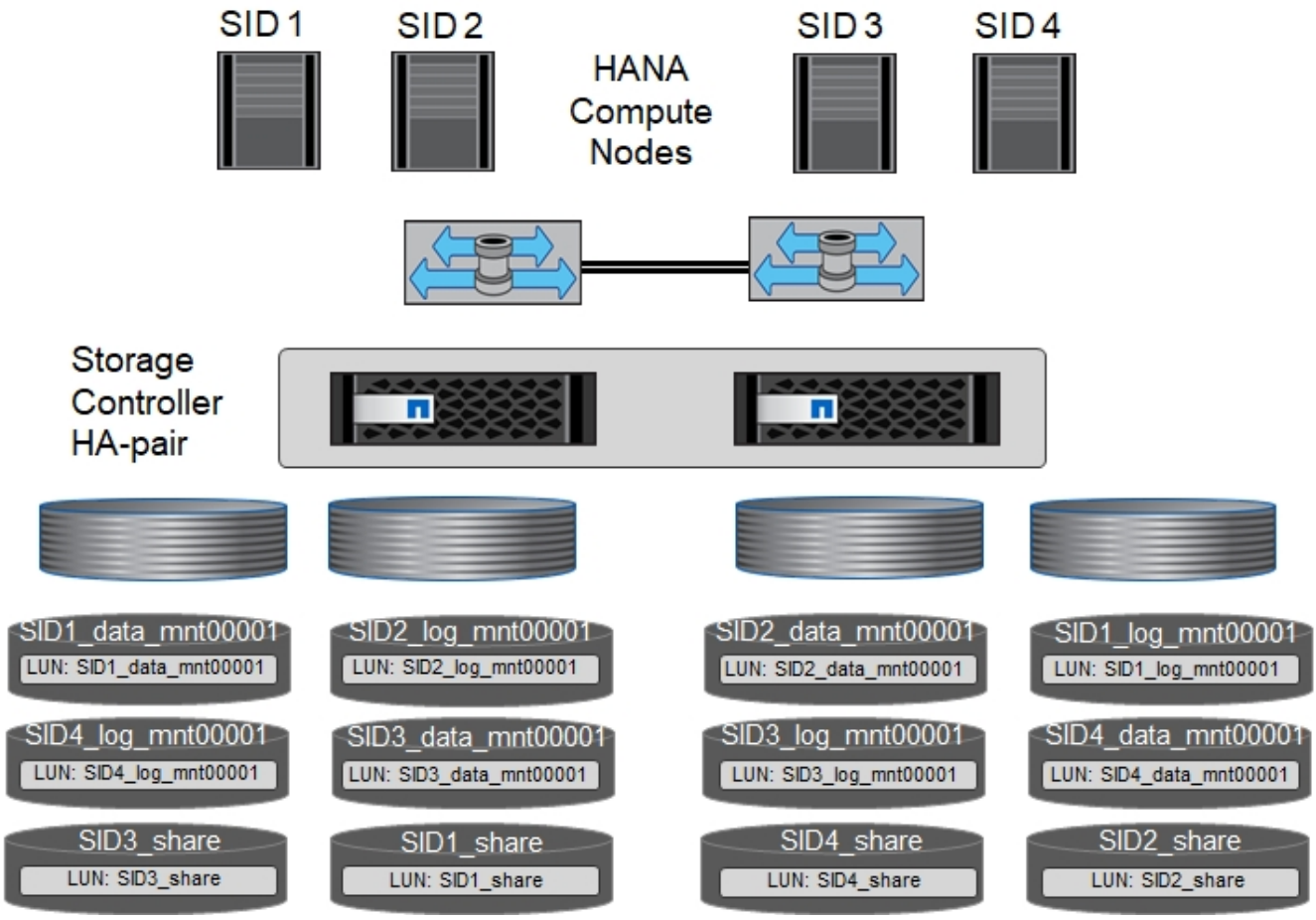
The following figure shows the list of initiators for SS3_HANA. The igroup contains all WWPNs of the servers and is assigned to the port set of the storage controller.



Volume and LUN configuration for SAP HANA single-host systems

The following figure shows the volume configuration of four single-host SAP HANA systems. The data and log volumes of each SAP HANA system are distributed to different storage controllers. For example, volume `SID1``data``mnt00001` is configured on controller A and volume `SID1``log``mnt00001` is configured on controller B. Within each volume, a single LUN is configured.

If only one storage controller of a high-availability (HA) pair is used for the SAP HANA systems, data volumes and log volumes can also be stored on the same storage controller.



For each SAP HANA host, a data volume, a log volume, and a volume for `/hana/shared` are configured. The following table shows an example configuration with four SAP HANA single-host systems.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data, log, and shared volumes for system SID1	Data volume: SID1_data_mnt00001	Shared volume: SID1_shared	–	Log volume: SID1_log_mnt00001
Data, log, and shared volumes for system SID2	–	Log volume: SID2_log_mnt00001	Data volume: SID2_data_mnt00001	Shared volume: SID2_shared
Data, log, and shared volumes for system SID3	Shared volume: SID3_shared	Data volume: SID3_data_mnt00001	Log volume: SID3_log_mnt00001	–
Data, log, and shared volumes for system SID4	Log volume: SID4_log_mnt00001	–	Shared volume: SID4_shared	Data volume: SID4_data_mnt00001

The next table shows an example of the mount point configuration for a single-host system.

LUN	Mount point at HANA host	Note
SID1_data_mnt00001	/hana/data/SID1/mnt00001	Mounted using /etc/fstab entry

LUN	Mount point at HANA host	Note
SID1_log_mnt00001	/hana/log/SID1/mnt00001	Mounted using /etc/fstab entry
SID1_shared	/hana/shared/SID1	Mounted using /etc/fstab entry

With the described configuration, the `/usr/sap/SID1` directory in which the default home directory of user SID1adm is stored, is on the local disk. In a disaster recovery setup with disk-based replication, NetApp recommends creating an additional LUN within the `SID1`_`shared `volume for the `/usr/sap/SID1` directory so that all file systems are on the central storage.

Volume and LUN configuration for SAP HANA single-host systems using Linux LVM

The Linux LVM can be used to increase performance and to address LUN size limitations. The different LUNs of an LVM volume group should be stored within a different aggregate and at a different controller. The following table shows an example for two LUNs per volume group.

It is not necessary to use LVM with multiple LUNs to fulfil the SAP HANA KPIs. A single LUN setup fulfils the required KPIs.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data, log, and shared volumes for LVM based system	Data volume: SID1_data_mnt00001	Shared volume: SID1_shared Log2 volume: SID1_log2_mnt00001	Data2 volume: SID1_data2_mnt00001	Log volume: SID1_log_mnt00001

At the SAP HANA host, volume groups and logical volumes must be created and mounted. The next table lists the mount points for single-host systems using LVM.

Logical volume/LUN	Mount point at SAP HANA host	Note
LV: SID1_data_mnt0000-vol	/hana/data/SID1/mnt00001	Mounted using /etc/fstab entry
LV: SID1_log_mnt00001-vol	/hana/log/SID1/mnt00001	Mounted using /etc/fstab entry
LUN: SID1_shared	/hana/shared/SID1	Mounted using /etc/fstab entry

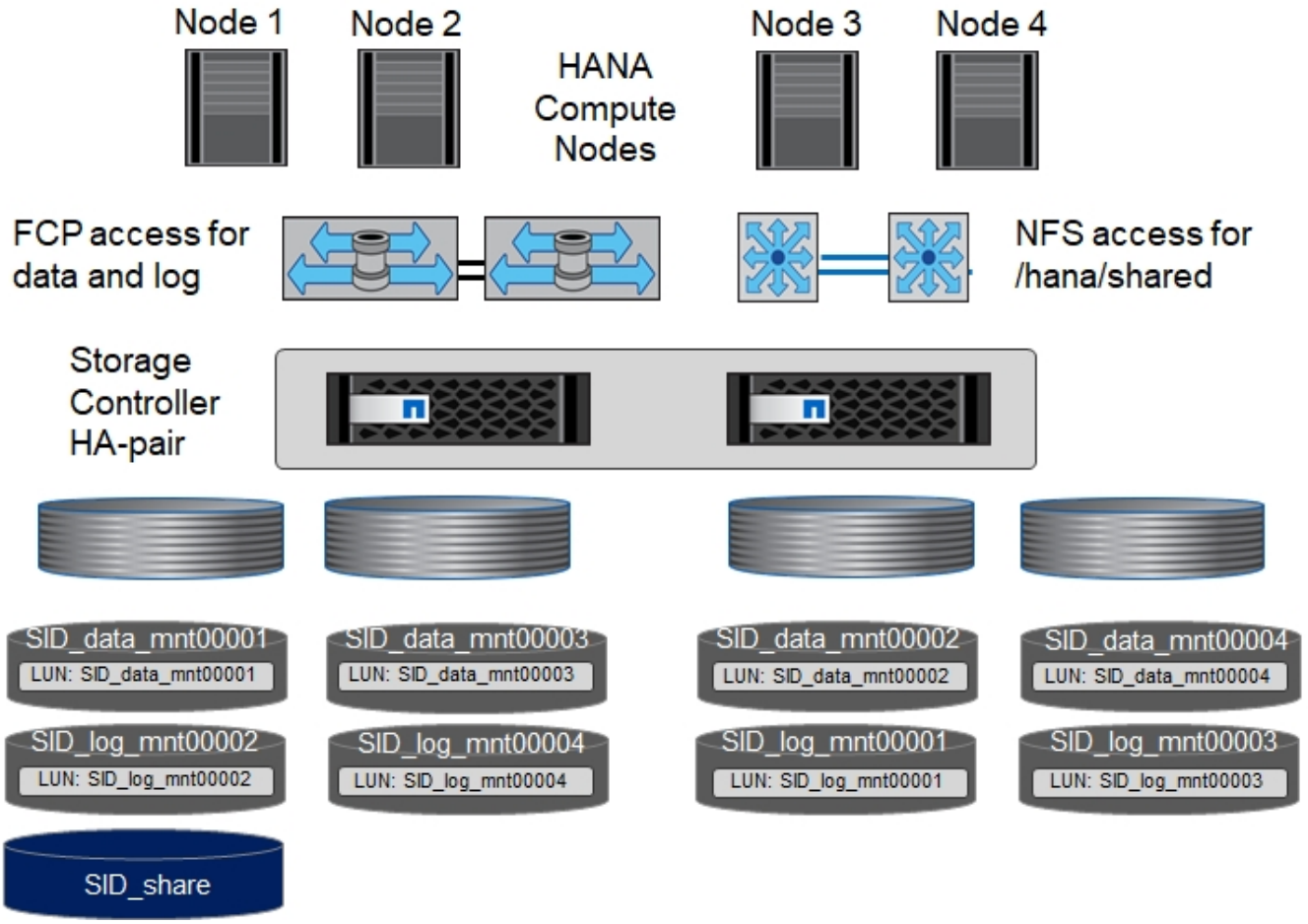
With the described configuration, the `/usr/sap/SID1` directory in which the default home directory of user SID1adm is stored, is on the local disk. In a disaster recovery setup with disk-based replication, NetApp recommends creating an additional LUN within the `SID1`_`shared `volume for the `/usr/sap/SID1` directory so that all file systems are on the central storage.

Volume and LUN configuration for SAP HANA multiple-host systems

The following figure shows the volume configuration of a 4+1 multiple-host SAP HANA system. The data volumes and log volumes of each SAP HANA host are distributed to different storage controllers. For example, the volume `SID``data``mnt00001` is configured on controller A and the volume `SID``log``mnt00001` is configured on controller B. One LUN is configured within each volume.

The `/hana/shared` volume must be accessible by all HANA hosts and is therefore exported by using NFS. Even though there are no specific performance KPIs for the `/hana/shared` file system, NetApp recommends using a 10Gb Ethernet connection.

If only one storage controller of an HA pair is used for the SAP HANA system, data and log volumes can also be stored on the same storage controller.



For each SAP HANA host, a data volume and a log volume are created. The `/hana/shared` volume is used by all hosts of the SAP HANA system. The following figure shows an example configuration for a 4+1 multiple-host SAP HANA system.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	–	Log volume: SID_log_mnt00001	–
Data and log volumes for node 2	Log volume: SID_log_mnt00002	–	Data volume: SID_data_mnt00002	–
Data and log volumes for node 3	–	Data volume: SID_data_mnt00003	–	Log volume: SID_log_mnt00003
Data and log volumes for node 4	–	Log volume: SID_log_mnt00004	–	Data volume: SID_data_mnt00004

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

The next table shows the configuration and the mount points of a multiple-host system with four active SAP HANA hosts.

LUN or Volume	Mount point at SAP HANA host	Note
LUN: SID_data_mnt00001	/hana/data/SID/mnt00001	Mounted using storage connector
LUN: SID_log_mnt00001	/hana/log/SID/mnt00001	Mounted using storage connector
LUN: SID_data_mnt00002	/hana/data/SID/mnt00002	Mounted using storage connector
LUN: SID_log_mnt00002	/hana/log/SID/mnt00002	Mounted using storage connector
LUN: SID_data_mnt00003	/hana/data/SID/mnt00003	Mounted using storage connector
LUN: SID_log_mnt00003	/hana/log/SID/mnt00003	Mounted using storage connector
LUN: SID_data_mnt00004	/hana/data/SID/mnt00004	Mounted using storage connector
LUN: SID_log_mnt00004	/hana/log/SID/mnt00004	Mounted using storage connector
Volume: SID_shared	/hana/shared/SID	Mounted at all hosts using NFS and /etc/fstab entry

With the described configuration, the `/usr/sap/SID` directory in which the default home directory of user SIDadm is stored is on the local disk for each HANA host. In a disaster recovery setup with disk-based replication, NetApp recommends creating four additional subdirectories in the `SID`_`shared` volume for the `/usr/sap/SID` file system so that each database host has all its file systems on the central storage.

Volume and LUN configuration for SAP HANA multiple-host systems using Linux LVM

The Linux LVM can be used to increase performance and to address LUN size limitations. The different LUNs of an LVM volume group should be stored within a different aggregate and at a different controller. The following table shows an example for two LUNs per volume group for a 2+1 SAP HANA multiple host system.

It is not necessary to use LVM to combine several LUN to fulfil the SAP HANA KPIs. A single LUN setup fulfils the required KPIs.

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data and log volumes for node 1	Data volume: SID_data_mnt00001	Log2 volume: SID_log2_mnt00001	Log volume: SID_log_mnt00001	Data2 volume: SID_data2_mnt00001
Data and log volumes for node 2	Log2 volume: SID_log2_mnt00002	Data volume: SID_data_mnt00002	Data2 volume: SID_data2_mnt00002	Log volume: SID_log_mnt00002

Purpose	Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Shared volume for all hosts	Shared volume: SID_shared	–	–	–

At the SAP HANA host, volume groups and logical volumes need to be created and mounted:

Logical volume (LV) or volume	Mount point at SAP HANA host	Note
LV: SID_data_mnt00001-vol	/hana/data/SID/mnt00001	Mounted using storage connector
LV: SID_log_mnt00001-vol	/hana/log/SID/mnt00001	Mounted using storage connector
LV: SID_data_mnt00002-vol	/hana/data/SID/mnt00002	Mounted using storage connector
LV: SID_log_mnt00002-vol	/hana/log/SID/mnt00002	Mounted using storage connector
Volume: SID_shared	/hana/shared	Mounted at all hosts using NFS and /etc/fstab entry

With the described configuration, the `/usr/sap/SID` directory in which the default home directory of user SIDadm is stored, is on the local disk for each HANA host. In a disaster recovery setup with disk-based replication, NetApp recommends creating four additional subdirectories in the `SID`_`shared` volume for the `/usr/sap/SID` file system so that each database host has all its file systems on the central storage.

Volume options

The volume options listed in the following table must be verified and set on all SVMs.

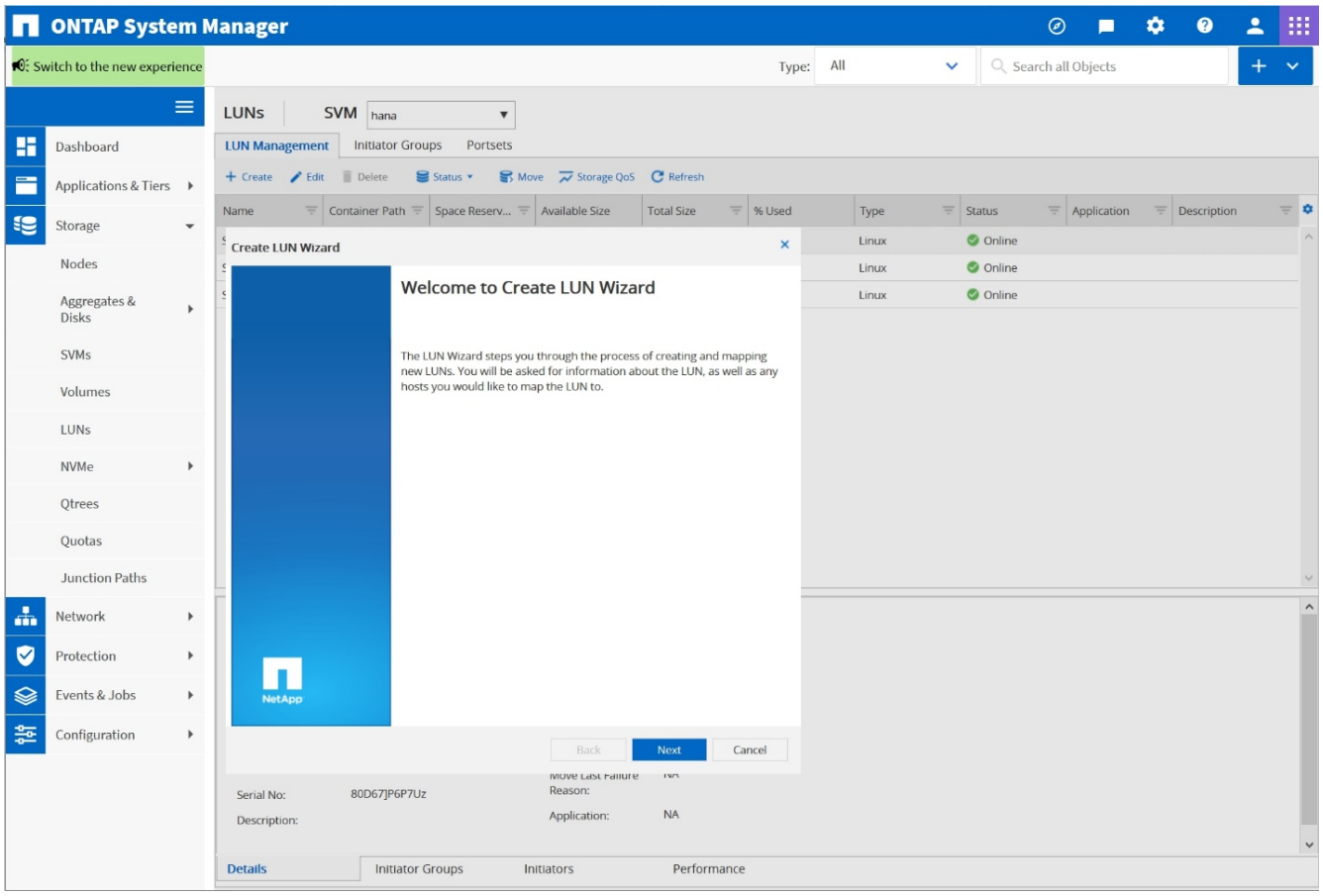
Action	ONTAP 9
Disable automatic Snapshot copies	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disable visibility of Snapshot directory	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false

Creating LUNs, volumes, and mapping LUNs to initiator groups

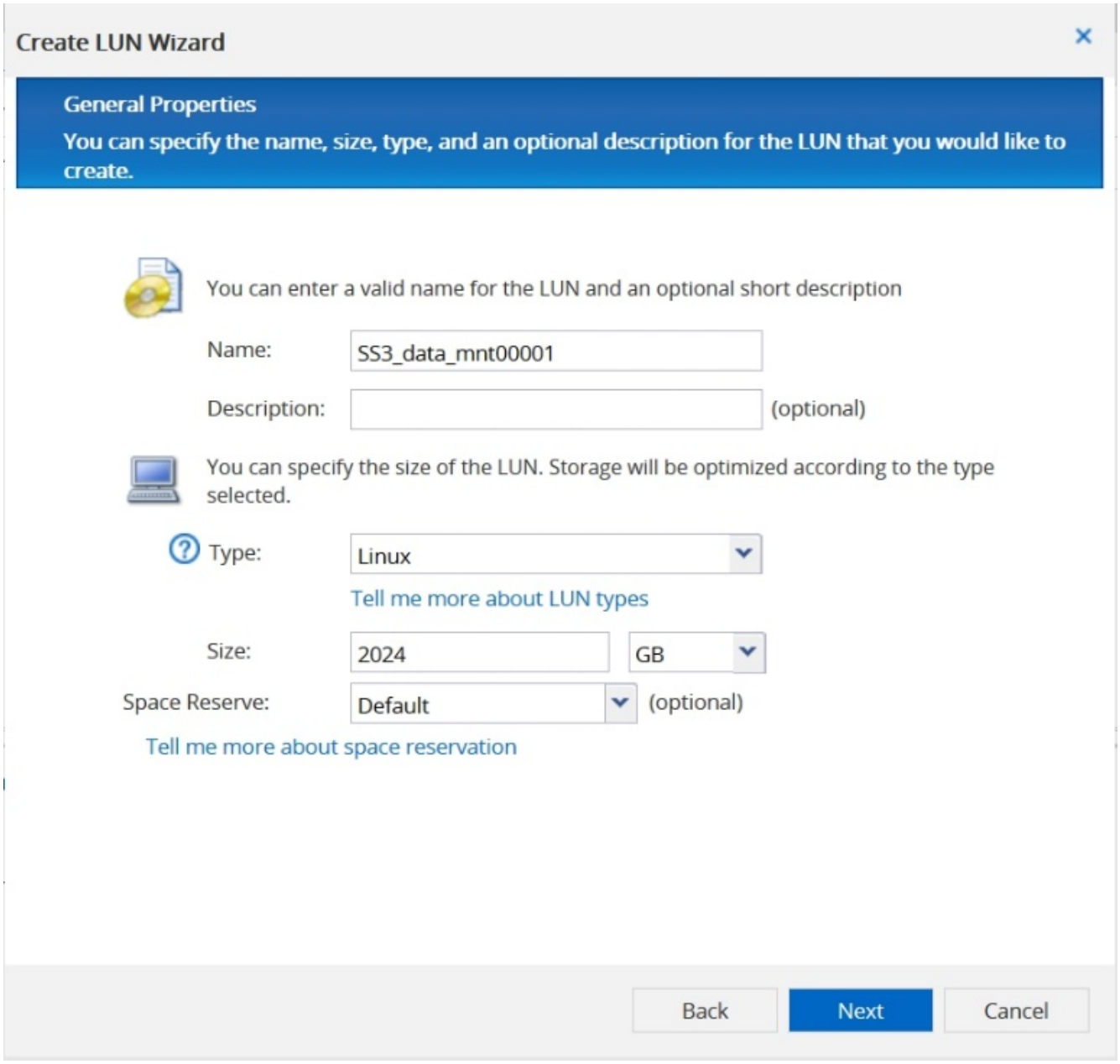
You can use NetApp OnCommand System Manager to create storage volumes and LUNs and the map them to the igroups of the servers.

The following steps show the configuration of a 2+1 multiple-host HANA system with the SID SS3.

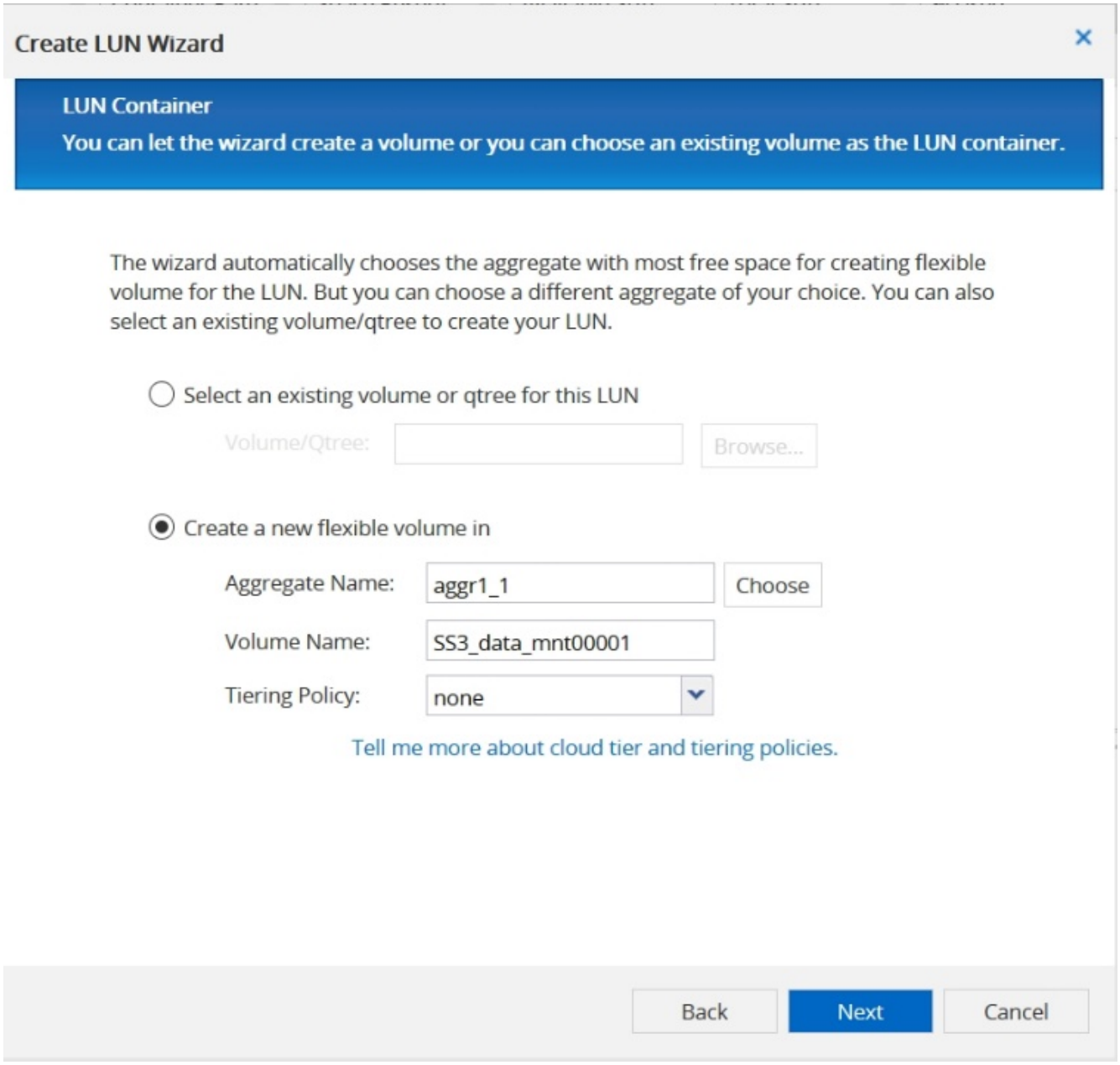
1. Start the Create LUN Wizard in NetApp ONTAP System Manager.



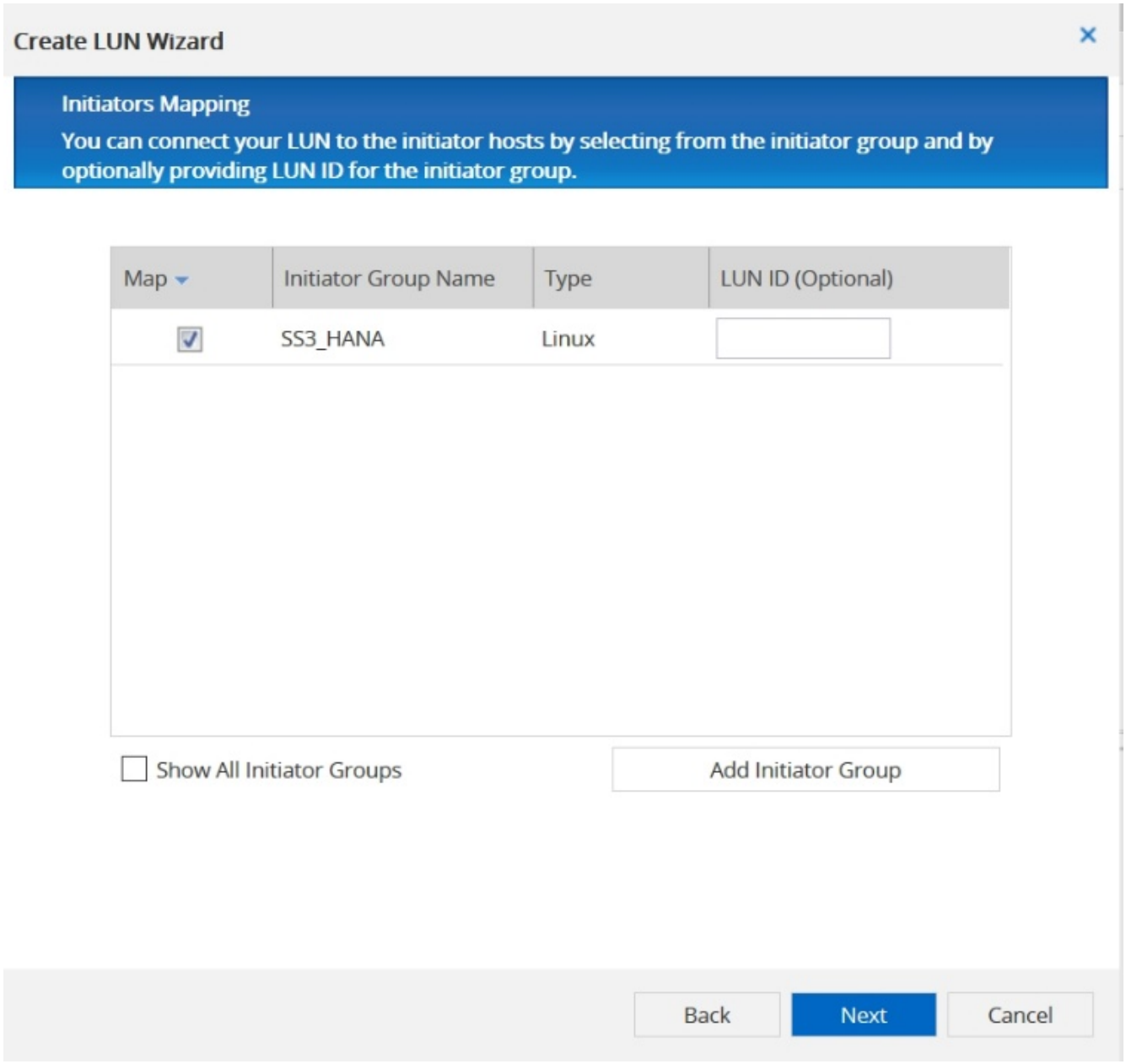
2. Enter the LUN name, select the LUN type, and enter the size of the LUN.



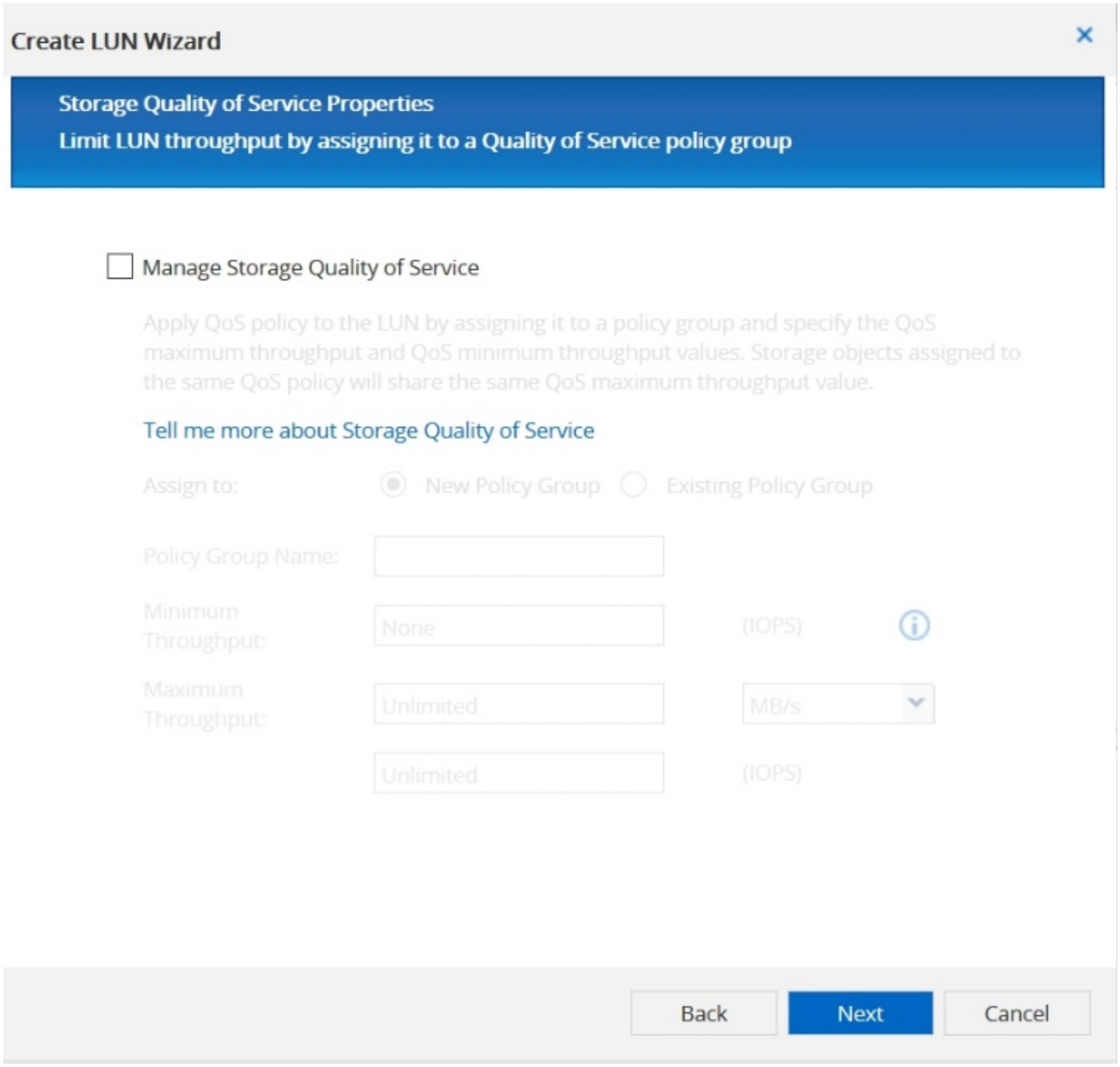
3. Enter the volume name and the hosting aggregate.



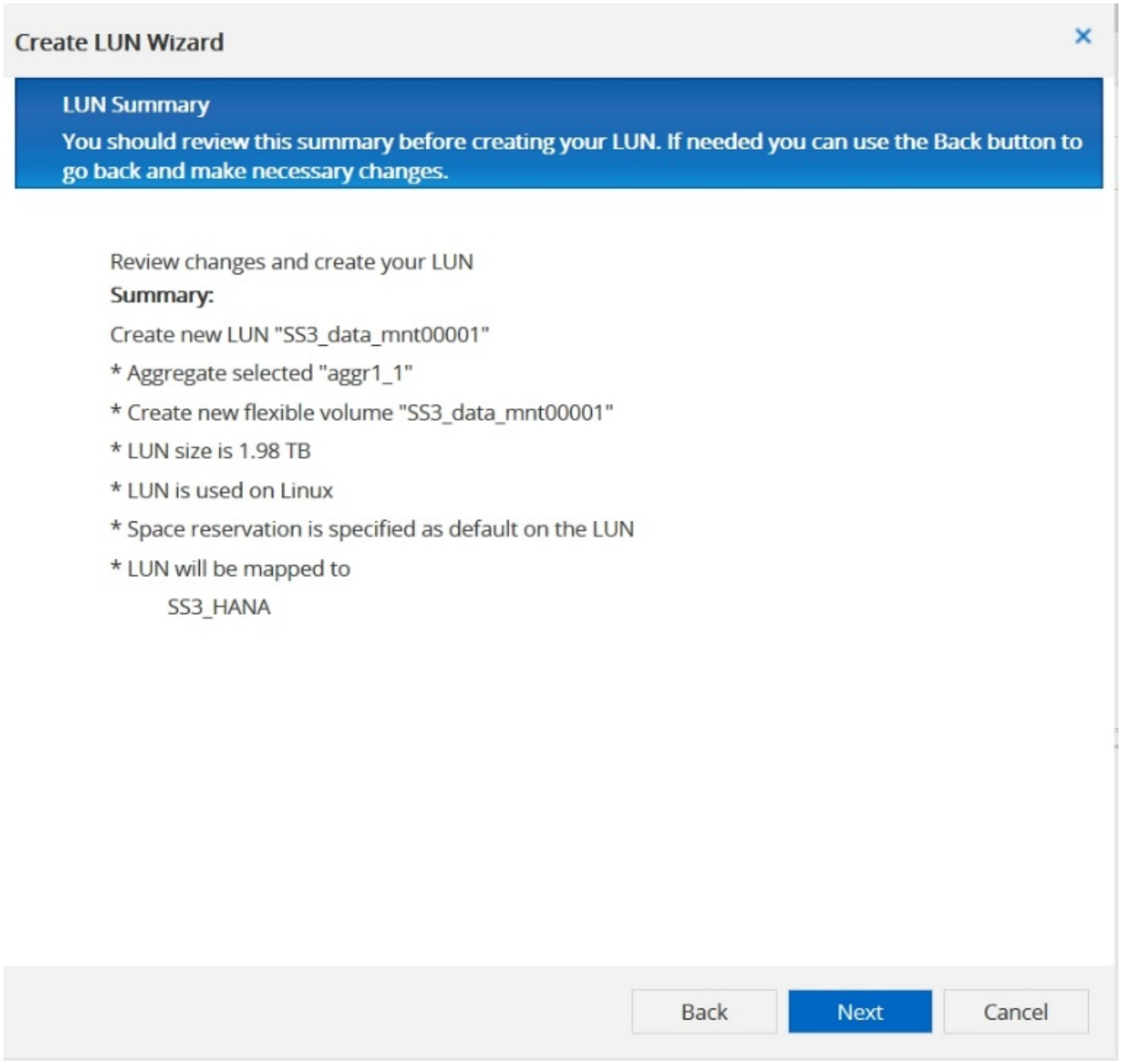
4. Select the igroups to which the LUNs should be mapped.



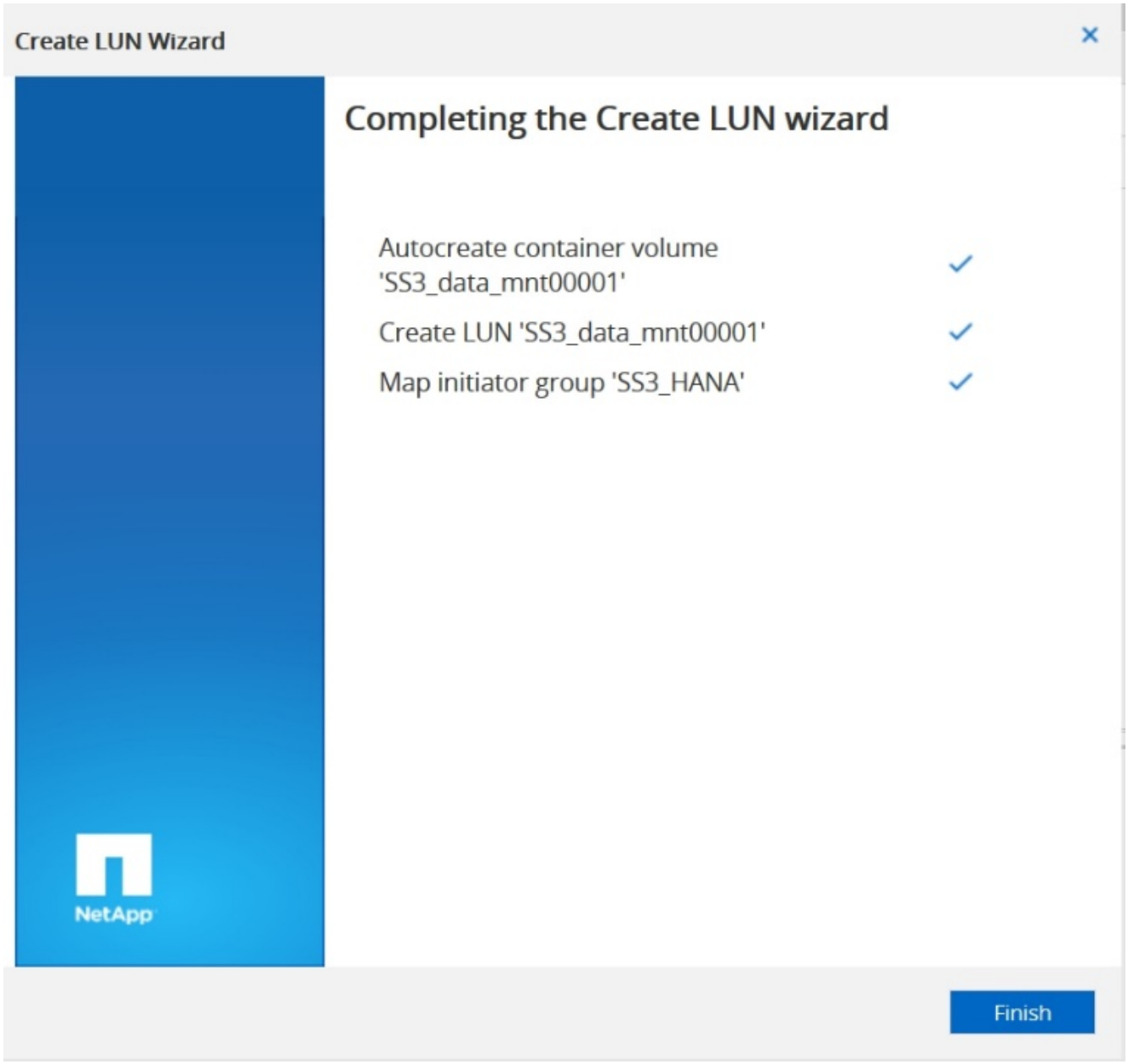
5. Provide the QoS settings.



6. Click Next on the Summary page.

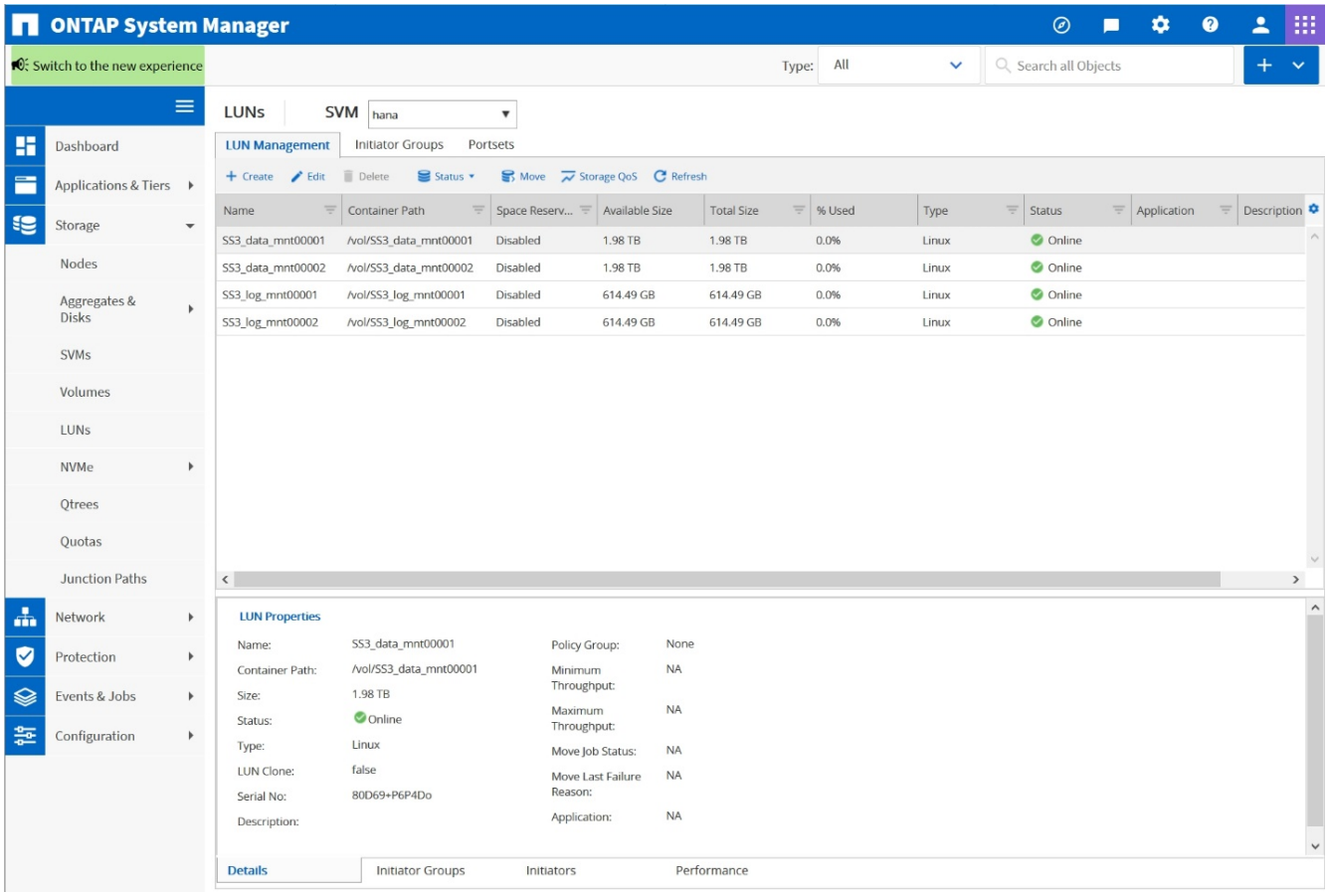


7. Click Finish on the Completion page.



8. Repeat steps 2 to 7 for each LUN.

   The following figure shows a summary of all LUNs that need to be created for 2+1 multiple-host setup.



Creating LUNs, volumes, and mapping LUNs to igroups using the CLI

This section shows an example configuration using the command line with ONTAP 9.8 for a 2+1 SAP HANA multiple host system with SID FC5 using LVM and two LUNs per LVM volume group.

1. Create all necessary volumes.

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
nonevol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Create all LUNs.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Create the igroup for all servers belonging to system FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb,
10000090fadcc5c1,10000090fadcc5c2,  10000090fadcc5c3,10000090fadcc5c4
-vserver hana
```

4. Map all LUNs to the created igroup.

```
lun map -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

Next: SAP HANA storage connector API.

SAP HANA storage connector API

Previous: Storage controller setup.

A storage connector is required only in multiple-host environments that have failover capabilities. In multiple-host setups, SAP HANA provides high-availability functionality so that an SAP HANA database host can fail over to a standby host. In this case, the LUNs of the failed host are accessed and used by the standby host. The storage connector is used to make sure that a storage partition can be actively accessed by only one database host at a time.

In SAP HANA multiple-host configurations with NetApp storage, the standard storage connector delivered by SAP is used. The “SAP HANA FC Storage Connector Admin Guide” can be found as an attachment to SAP note 1900823.

Next: Host setup.

Host setup

Previous: SAP HANA storage connector API.

Before setting up the host, NetApp SAN Host Utilities must be downloaded from the NetApp Support site and installed on the HANA servers. The Host Utility documentation includes information about additional software that must be installed depending on the FCP HBA used.

The documentation also contains information about multipath configurations that are specific to the Linux version used. This document covers the required configuration steps for SLES 15 and Red Hat Enterprise Linux 7.6 or higher, as described in the Linux Host Utilities 7.1 Installation and Setup Guide.

Configure multipathing

Steps 1 to 6 must be performed on all worker and standby hosts in the SAP HANA multiple-host configuration.

To configure multipathing, complete the following steps:

1. Run the Linux `rescan-scsi-bus.sh -a` command on each server to discover new LUNs.

2. Run the `sanlun lun show` command and verify that all required LUNs are visible. The following example shows the `sanlun lun show` command output for a 2+1 multiple-host HANA system with two data LUNs and two log LUNs. The output shows the LUNs and the corresponding device files, such as LUN `SS3_data_mnt00001` and the device file `/dev/sdag`. Each LUN has eight FC paths from the host to the storage controllers.

```
stlrx300s8-6:~ # sanlun lun show
controller(7mode/E-Series)/
device          host       lun
vserver(cDOT/FlashRay)        lun-pathname
filename        adapter    protocol   size    product
------------------------------------------------------------------------
------------------------------------------------
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdah       host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdag       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdaf       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdae       host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdad       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdac       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdab       host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdaa       host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdz        host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdy        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdx        host11     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdw        host11     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdv        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdu        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdt        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sds        host11     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
```

```
/dev/sdr        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdq        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdp        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdo        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdn        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdm        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdl        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdk        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdj        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00002/SS3_log_mnt00002
/dev/sdi        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_data_mnt00001/SS3_data_mnt00001
/dev/sdh        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_data_mnt00002/SS3_data_mnt00002
/dev/sdg        host10     FCP        1.2t    cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdf        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sde        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdd        host10     FCP        512.0g  cDOT
hana                          /vol/SS3_log_mnt00001/SS3_log_mnt00001
/dev/sdc        host10     FCP        512.0g  cDOT
```

3. Run the `multipath -r` command to get the worldwide identifiers (WWIDs) for the device file names:

In this example, there are four LUNs.

```
stlrx300s8-6:~ # multipath -r
create: 3600a098038304436375d4d442d753878 undef NETAPP,LUN C-Mode
size=512G features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:1:0 sdd  8:48   undef ready running
| |- 10:0:3:0 sdf  8:80   undef ready running
| |- 11:0:0:0 sds  65:32  undef ready running
| `- 11:0:2:0 sdu  65:64  undef ready running
```

```
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:0:0 sdc  8:32   undef ready running
  |- 10:0:2:0 sde  8:64   undef ready running
  |- 11:0:1:0 sdt  65:48  undef ready running
  `- 11:0:3:0 sdv  65:80  undef ready running
create: 3600a098038304436375d4d442d753879 undef NETAPP,LUN C-Mode
size=1.2T features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:1:1 sdj  8:144  undef ready running
| |- 10:0:3:1 sdp  8:240  undef ready running
| |- 11:0:0:1 sdw  65:96  undef ready running
| `- 11:0:2:1 sdac 65:192 undef ready running
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:0:1 sdg  8:96   undef ready running
  |- 10:0:2:1 sdm  8:192  undef ready running
  |- 11:0:1:1 sdz  65:144 undef ready running
  `- 11:0:3:1 sdaf 65:240 undef ready running
create: 3600a098038304436392b4d442d6f534f undef NETAPP,LUN C-Mode
size=1.2T features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:0:2 sdh  8:112  undef ready running
| |- 10:0:2:2 sdn  8:208  undef ready running
| |- 11:0:1:2 sdaa 65:160 undef ready running
| `- 11:0:3:2 sdag 66:0   undef ready running
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:1:2 sdk  8:160  undef ready running
  |- 10:0:3:2 sdq  65:0   undef ready running
  |- 11:0:0:2 sdx  65:112 undef ready running
  `- 11:0:2:2 sdad 65:208 undef ready running
create: 3600a098038304436392b4d442d6f5350 undef NETAPP,LUN C-Mode
size=512G features='3 pg_init_retries 50 queue_if_no_path' hwhandler='0'
wp=undef
|-+- policy='service-time 0' prio=50 status=undef
| |- 10:0:0:3 sdi  8:128  undef ready running
| |- 10:0:2:3 sdo  8:224  undef ready running
| |- 11:0:1:3 sdab 65:176 undef ready running
| `- 11:0:3:3 sdah 66:16  undef ready running
`-+- policy='service-time 0' prio=10 status=undef
  |- 10:0:1:3 sdl  8:176  undef ready running
  |- 10:0:3:3 sdr  65:16  undef ready running
  |- 11:0:0:3 sdy  65:128 undef ready running
  `- 11:0:2:3 sdae 65:224 undef ready running
```

4. Edit the `/etc/multipath.conf` file and add the WWIDs and alias names.

The example output shows the content of the `/etc/multipath.conf` file, which includes alias names for the four LUNs of a 2+1 multiple-host system. If there is no `multipath.conf` file available, you can create one by running the following command: `multipath -T > /etc/multipath.conf`.

```
stlrx300s8-6:/ # cat /etc/multipath.conf
multipaths {
        multipath {
                wwid    3600a098038304436392b4d442d6f534f
                alias   hana- SS3_data_mnt00001
        }
        multipath {
                wwid    3600a098038304436375d4d442d753879
                alias   hana- SS3_data_mnt00002
        }
        multipath {
                wwid    3600a098038304436375d4d442d753878
                alias   hana- SS3_log_mnt00001
        }
        multipath {
                wwid    3600a098038304436392b4d442d6f5350
                alias   hana- SS3_log_mnt00002
        }
}
```

5. Run the `multipath -r` command to reload the device map.
6. Verify the configuration by running the `multipath -ll` command to list all the LUNs, alias names, and active and standby paths.

The following example output shows the output of a 2+1 multiple-host HANA system with two data and two log LUNs.

```
stlrx300s8-6:~ # multipath -ll
hana- SS3_data_mnt00002 (3600a098038304436375d4d442d753879) dm-1
NETAPP,LUN C-Mode
size=1.2T features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:1:1 sdj  8:144  active ready running
| |- 10:0:3:1 sdp  8:240  active ready running
| |- 11:0:0:1 sdw  65:96  active ready running
| `- 11:0:2:1 sdac 65:192 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:0:1 sdg  8:96   active ready running
```

```
  |- 10:0:2:1 sdm  8:192  active ready running
  |- 11:0:1:1 sdz  65:144 active ready running
  `- 11:0:3:1 sdaf 65:240 active ready running
hana- SS3_data_mnt00001 (3600a098038304436392b4d442d6f534f) dm-2
NETAPP,LUN C-Mode
size=1.2T features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:0:2 sdh  8:112  active ready running
| |- 10:0:2:2 sdn  8:208  active ready running
| |- 11:0:1:2 sdaa 65:160 active ready running
| `- 11:0:3:2 sdag 66:0   active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:1:2 sdk  8:160  active ready running
  |- 10:0:3:2 sdq  65:0   active ready running
  |- 11:0:0:2 sdx  65:112 active ready running
  `- 11:0:2:2 sdad 65:208 active ready running
hana- SS3_log_mnt00002 (3600a098038304436392b4d442d6f5350) dm-3
NETAPP,LUN C-Mode
size=512G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:0:3 sdi  8:128  active ready running
| |- 10:0:2:3 sdo  8:224  active ready running
| |- 11:0:1:3 sdab 65:176 active ready running
| `- 11:0:3:3 sdah 66:16  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:1:3 sdl  8:176  active ready running
  |- 10:0:3:3 sdr  65:16  active ready running
  |- 11:0:0:3 sdy  65:128 active ready running
  `- 11:0:2:3 sdae 65:224 active ready running
hana- SS3_log_mnt00001 (3600a098038304436375d4d442d753878) dm-0
NETAPP,LUN C-Mode
size=512G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handler' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=enabled
| |- 10:0:1:0 sdd  8:48   active ready running
| |- 10:0:3:0 sdf  8:80   active ready running
| |- 11:0:0:0 sds  65:32  active ready running
| `- 11:0:2:0 sdu  65:64  active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 10:0:0:0 sdc  8:32   active ready running
  |- 10:0:2:0 sde  8:64   active ready running
  |- 11:0:1:0 sdt  65:48  active ready running
  `- 11:0:3:0 sdv  65:80  active ready running
```

Create LVM volume groups and logical volumes

This step is only needed if LVM will be used. The following example is for a 2+1 host setup using SID FC5.

For an LVM- based setup, the multipath configuration described in the previous section must be completed as well. In this example, eight LUNs must be configured for multipathing.

1. Initialize all LUNs as a physical volume.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001pvcreate /dev/mapper/hana-
FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001pvcreate /dev/mapper/hana-
FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. Create the volume groups for each data and log partition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. Create a logical volume for each data and log partition. Use a stripe size that is equal to the number of LUNs used per volume group (in example two) and a stripe size of 256k for data and 64k for log. SAP only supports one logical volume per volume group.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scan the physical volumes, volume groups, and vol groups at all other hosts.

```
modprobe dm_modpvscanvgscanlvscan
```

If the above commands do not find the volumes, a restart is required.

5. To mount the logical volumes, the logical volumes must be activated. To activate the volumes, run the following command:

```
vgchange -a y
```

Create file systems

To create the XFS file system on each LUN belonging to the HANA system, take one of the following actions:

- For a single-host system, create the XFS file system on the data, log, and `/hana/shared` LUNs.

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_data_mnt00001
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_log_mnt00001
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana- SS3_shared
```

- For a multiple-host system, create the XFS file system on all data and log LUNs.

```
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_log_mnt00001
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_log_mnt00002
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_data_mnt00001
stlrx300s8-6:~ # mkfs.xfs /dev/mapper/hana- SS3_data_mnt00002
```

- If LVM is used, create the XFS file system on all data and log logical volumes.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

The multiple host example commands show a 2+1 multiple-host HANA system.

Create mount points

To create the required mount point directories, take one of the following actions:

- For a single-host system, set permissions and create mount points on the database host.

```
stlrx300s8-6:/ # mkdir -p /hana/data/SS3/mnt00001
stlrx300s8-6:/ # mkdir -p /hana/log/SS3/mnt00001
stlrx300s8-6:/ # mkdir -p /hana/shared
stlrx300s8-6:/ # chmod -R 777 /hana/log/SS3
stlrx300s8-6:/ # chmod -R 777 /hana/data/SS3
stlrx300s8-6:/ # chmod 777 /hana/shared
```

- For a multiple-host system, set permissions and create mount points on all worker and standby hosts.

The example commands show a 2+1 multiple-host HANA system.

```
stlrx300s8-6:/ # mkdir -p /hana/data/SS3/mnt00001
stlrx300s8-6:/ # mkdir -p /hana/log/SS3/mnt00001
stlrx300s8-6:/ # mkdir -p /hana/data/SS3/mnt00002
stlrx300s8-6:/ # mkdir -p /hana/log/SS3/mnt00002
stlrx300s8-6:/ # mkdir -p /hana/shared
stlrx300s8-6:/ # chmod -R 777 /hana/log/SS3
stlrx300s8-6:/ # chmod -R 777 /hana/data/SS3
stlrx300s8-6:/ # chmod 777 /hana/shared
```

The same steps must be executed for a system configuration with Linux LVM.

Mount file systems

To mount file systems during system boot using the `/etc/fstab` configuration file, complete the following steps:

1. Take one of the following actions:
   - For a single-host system, add the required file systems to the `/etc/fstab` configuration file.

     The XFS file systems for the data and log LUN must be mounted with the `relatime` and `inode64` mount options.

     ```
     stlrx300s8-6:/ # cat /etc/fstab
     /dev/mapper/FAS8200-hana- SS3_shared /hana/shared xfs defaults 0 0
     /dev/mapper/FAS8200-hana- SS3_log_mnt00001 /hana/log/SS3/mnt00001 xfs
     relatime,inode64,nobarrier 0 0
     /dev/mapper/FAS8200-hana- SS3_data_mnt00001 /hana/data/SS3/mnt00001
     xfs relatime,inode64 0 0
     ```

     If LVM is used, use the logical volume names for data and log.

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

- For a multiple-host system, add the `/hana/shared` file system to the `/etc/fstab` configuration file of each host.

All the data and log file systems are mounted through the SAP HANA storage connector.

```
stlrx300s8-6:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs
rw,vers=3,hard,timeo=600,intr,noatime,nolock 0 0
```

2. To mount the file systems, run the `mount -a` command at each host.

Next: I/O stack configuration for SAP HANA.

I/O stack configuration for SAP HANA

Previous: Host setup.

Starting with SAP HANA 1.0 SPS10, SAP introduced parameters to adjust the I/O behavior and optimize the database for the file and storage system used.

NetApp conducted performance tests to define the ideal values. The following table lists the optimal values as inferred from the performance tests.

Parameter	Value
max_parallel_io_requests	128
async_read_submit	on
async_write_submit_active	on
async_write_submit_blocks	all

For SAP HANA 1.0 up to SPS12, these parameters can be set during the installation of the SAP HANA database as described in SAP Note 2267798 – Configuration of the SAP HANA Database during Installation Using hdbparam.

Alternatively, the parameters can be set after the SAP HANA database installation using the `hdbparam` framework.

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Starting with SAP HANA 2.0, `hdbparam` is deprecated and the parameters have been moved to the `global.ini` file. The parameters can be set by using SQL commands or SAP HANA Studio. For more information, see SAP Note 2399079 - Elimination of hdbparam in HANA 2. The parameters can be also set within the `global.ini` file.

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

With SAP HANA 2.0 SPS5 and later, you can use the `setParameter.py `script to set the parameters mentioned above.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Next: SAP HANA software installation.

SAP HANA software installation

Previous: I/O stack configuration for SAP HANA.

Install on single-host system

SAP HANA software installation does not require any additional preparation for a single-host system.

Install on multiple-host system

The following installation procedure is based on SAP HANA 1.0 SPS12 or later.

Before beginning the installation, create a `global.ini` file to enable use of the SAP storage connector during the installation process. The SAP storage connector mounts the required file systems at the worker hosts during the installation process. The `global.ini` file must be available in a file system that is accessible from all hosts, such as the `/hana/shared/SID` file system.

Before installing SAP HANA software on a multiple-host system, the following steps must be completed:

1. Add the following mount options for the data LUNs and the log LUNs to the `global.ini` file:
   - `relatime` and `inode64` for the data and log file system
2. Add the WWIDs of the data and log partitions. The WWIDs must match the alias names configured in the `/etc/multipath.conf` file.

   The following output shows an example of a 2+1 multiple-host setup in which the system identifier (SID) is SS3.

```
stlrx300s8-6:~ # cat /hana/shared/global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/SS3
basepath_logvolumes = /hana/log/SS3
[storage]
ha_provider = hdb_ha.fcClient
partition_*_*__prtype = 5
partition_*_data__mountoptions = -o relatime,inode64
partition_*_log__mountoptions = -o relatime,inode64,nobarrier
partition_1_data__wwid = hana- SS3_data_mnt00001
partition_1_log__wwid = hana- SS3_log_mnt00001
partition_2_data__wwid = hana- SS3_data_mnt00002
partition_2_log__wwid = hana- SS3_log_mnt00002
[system_information]
usage = custom
[trace]
ha_fcclient = info
stlrx300s8-6:~ #
```

   If LVM is used, the needed configuration is different. The example below shows a 2+1 multiple-host setup with SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

Using the SAP `hdblcm` installation tool, start the installation by running the following command at one of the worker hosts. Use the `addhosts` option to add the second worker (sapcc-hana-tst-04) and the standby host (sapcc-hana-tst-05).
The directory where the prepared the `global.ini` file has been stored is included with the `storage_cfg` CLI option (`--storage_cfg=/hana/shared`).
Depending on the OS version being used, it might be necessary to install phyton 2.7 before installing the SAP HANA database.

```
sapcc-hana-tst-03:/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_LCM_LINUX_X86_64 # ./hdblcm --action=install
--addhosts=sapcc-hana-tst-04:role=worker:storage_partion=2,sapcc-hana-tst
-05:role:=standby --storage_cfg=/hana(shared/shared
SAP HANA Lifecycle Management - SAP HANA Database 2.00.052.00.1599235305
************************************************************************
Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.052.0000.1599259237) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.052.00.1599235305) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.5.109.1598303414) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
    SAP HANA Smart Data Access (2.00.5.000.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/SAP_HANA_SDA_20_LINUX_X86_64/packages
    SAP HANA Studio (2.3.54.000000) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
```

```
    SAP HANA Local Secure Store (2.4.24.0) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.0.130.519) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.052.0000.1599259237) in /mnt/sapcc-
share/software/SAP/HANA2SP5-52/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.014.1)
in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI14_1.zip
    XSAC FILEPROCESSOR 1.0 (1.000.85) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_85.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.012.20341) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_HRTT_20/XSACHRTT12_20341.zip
    XS Messaging Service 1 (1.004.10) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACMESSSRV04_10.zip
    Develop and run portal services for customer apps on XSA (1.005.1) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV05_1.zip
    SAP Web IDE Web Client (4.005.1) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE05_1.zip
    XS JOB SCHEDULER 1.0 (1.007.12) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_12.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.25) in /mnt/sapcc-
share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_25.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.3) in
/mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_3.zip
    XSA Cockpit 1 (1.001.17) in /mnt/sapcc-share/software/SAP/HANA2SP5-
52/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_17.zip
SAP HANA Database version '2.00.052.00.1599235305' will be installed.
Select additional components for installation:
  Index | Components | Description

-------------------------------------------------------------------------
-------------------
  1     | all        | All components
```

```
  2     | server     | No additional components
  3     | client     | Install SAP HANA Database Client version
2.5.109.1598303414
  4     | lss        | Install SAP HANA Local Secure Store version
2.4.24.0
  5     | studio     | Install SAP HANA Studio version 2.3.54.000000
  6     | smartda    | Install SAP HANA Smart Data Access version
2.00.5.000.0
  7     | xs         | Install SAP HANA XS Advanced Runtime version
1.0.130.519
  8     | afl        | Install SAP HANA AFL (incl.PAL,BFL,OFL) version
2.00.052.0000.1599259237
  9     | eml        | Install SAP HANA EML AFL version
2.00.052.0000.1599259237
  10    | epmmds     | Install SAP HANA EPM-MDS version
2.00.052.0000.1599259237
Enter comma-separated list of the selected indices [3]: 2,3
Enter Installation Path [/hana/shared]:
Enter Local Host Name [sapcc-hana-tst-03]:
```

Verify that the installation tool installed all selected components at all worker and standby hosts.

Next: Adding additional data volume partitions for SAP HANA single-host systems.

Adding additional data volume partitions for SAP HANA single-host systems

Previous: SAP HANA software installation.

Starting with SAP HANA 2.0 SPS4, additional data volume partitions can be configured. This feature allows you to configure two or more LUNs for the data volume of an SAP HANA tenant database and to scale beyond the size and performance limits of a single LUN.

It is not necessary to use multiple partitions to fulfil the SAP HANA KPIs. A single LUN with a single partition fulfils the required KPIs.

Using two or more individual LUNs for the data volume is only available for SAP HANA single-host systems. The SAP storage connector required for SAP HANA multiple-host systems does only support one device for the data volume.

You can add more data volume partitions at any time but it might require a restart of the SAP HANA database.

Enabling additional data volume partitions

To enable additional data volume partitions, complete the following steps:

1. Add the following entry within the `global.ini` file:

```
[customizable_functionalities]persistence_datavolume_partition_multipath
= true
```

2. Restart the database to enable the feature. Adding the parameter through the SAP HANA Studio to the `global.ini` file by using the Systemdb configuration prevents the restart of the database.

Volume and LUN configuration

The layout of volumes and LUNs is similar to the layout of a single host with one data volume partition, but with an additional data volume and LUN stored on a different aggregate as log volume and the other data volume. The following table shows an example configuration of an SAP HANA single-host systems with two data volume partitions.

Aggregate 1 at Controller A	Aggregate 2 at Controller A	Aggregate 1 at Controller B	Aggregate 2 at Controller B
Data volume: SID_data_mnt00001	Shared volume: SID_shared	Data volume: SID_data2_mnt00001	Log volume: SID_log_mnt00001

The next table shows an example of the mount point configuration for a single-host system with two data volume partitions.

LUN	Mount point at HANA host	Note
SID_data_mnt00001	/hana/data/SID/mnt00001	Mounted using /etc/fstab entry
SID_data2_mnt00001	/hana/data2/SID/mnt00001	Mounted using /etc/fstab entry
SID_log_mnt00001	/hana/log/SID/mnt00001	Mounted using /etc/fstab entry
SID_shared	/hana/shared/SID	Mounted using /etc/fstab entry

Create the new data LUNs by using either ONTAP System Manager or the ONTAP CLI.

Host configuration

To configure a host, complete the following steps:

1. Configure multipathing for the additional LUNs, as described in section 0.
2. Create the XFS file system on each additional LUN belonging to the HANA system.

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-SS3_data2_mnt00001
```

3. Add the additional file system/s to the `/etc/fstab` configuration file.

The XFS file systems for the data LUN must be mounted with the `relatime` and `inode64` mount options. The XFS file systems for the log LUN must be mounted with the `relatime`, `inode64`, and `nobarrier` mount options.

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-SS3_shared /hana/shared xfs default 0 0
/dev/mapper/hana-SS3_log_mnt00001 /hana/log/SS3/mnt00001 xfs
relatime,inode64,nobarrier 0 0
/dev/mapper/hana-SS3_data_mnt00001 /hana/data/SS3/mnt00001 xfs
relatime,inode64 0 0/dev/mapper/hana-SS3_data2_mnt00001
/hana/data2/SS3/mnt00001 xfs relatime,inode64 0 0
```

4. Create the mount points and set the permissions on the database host.

```
stlrx300s8-6:/ # mkdir -p /hana/data2/SS3/mnt00001
stlrx300s8-6:/ # chmod -R 777 /hana/data2/SS3
```

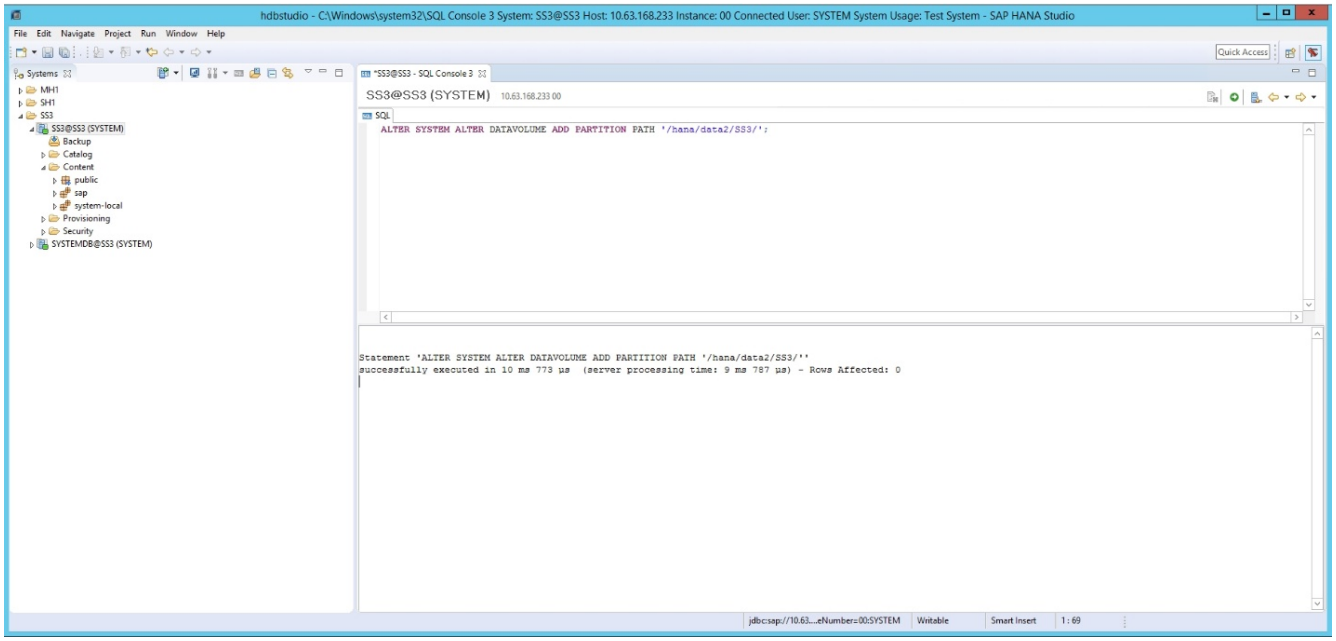
5. To mount the file systems, run the `mount -a` command.

Adding an additional datavolume partition

To add an additional datavolume partition to your tenant database, complete the following step:

1. Execute the following SQL statement against the tenant database. Each additional LUN can have a different path.

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Next: Where to find additional information.

Where to find additional information

Previous: Adding additional data volume partitions for SAP HANA single-host systems.

To learn more about the information described in this document, refer to the following documents and/or websites:

- Best Practices and Recommendations for Scale-Up Deployments of SAP HANA on VMware vSphere

  www.vmware.com/files/pdf/SAP_HANA_on_vmware_vSphere_best_practices_guide.pdf

- Best Practices and Recommendations for Scale-Out Deployments of SAP HANA on VMware vSphere

  http://www.vmware.com/files/pdf/sap-hana-scale-out-deployments-on-vsphere.pdf

- SAP Certified Enterprise Storage Hardware for SAP HANA

  https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/enterprise-storage.html

- SAP HANA Storage Requirements

  http://go.sap.com/documents/2015/03/74cdb554-5a7c-0010-82c7-eda71af511fa.html

- SAP HANA Tailored Data Center Integration Frequently Asked Questions

  https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html

- TR-4646: SAP HANA Disaster Recovery with Asynchronous Storage Replication Using SnapCenter 4.0 SAP HANA Plug-In

  https://www.netapp.com/us/media/tr-4646.pdf

- TR-4614: SAP HANA Backup and Recovery with SnapCenter

  https://www.netapp.com/us/media/tr-4614.pdf

- TR-4338: SAP HANA on VMware vSphere with NetApp FAS and AFF Systems

  www.netapp.com/us/media/tr-4338.pdf

- TR-4667: Automating SAP System Copies Using the SnapCenter 4.0 SAP HANA Plug- in

  https://www.netapp.com/us/media/tr-4667.pdf

- NetApp Documentation Centers

  https://www.netapp.com/us/documentation/index.aspx

- NetApp FAS Storage System Resources
- https://mysupport.netapp.com/info/web/ECMLP2676498.html
- SAP HANA Software Solutions

  www.netapp.com/us/solutions/applications/sap/index.aspx#sap-hana

Backup & Recovery and Disaster Recovery

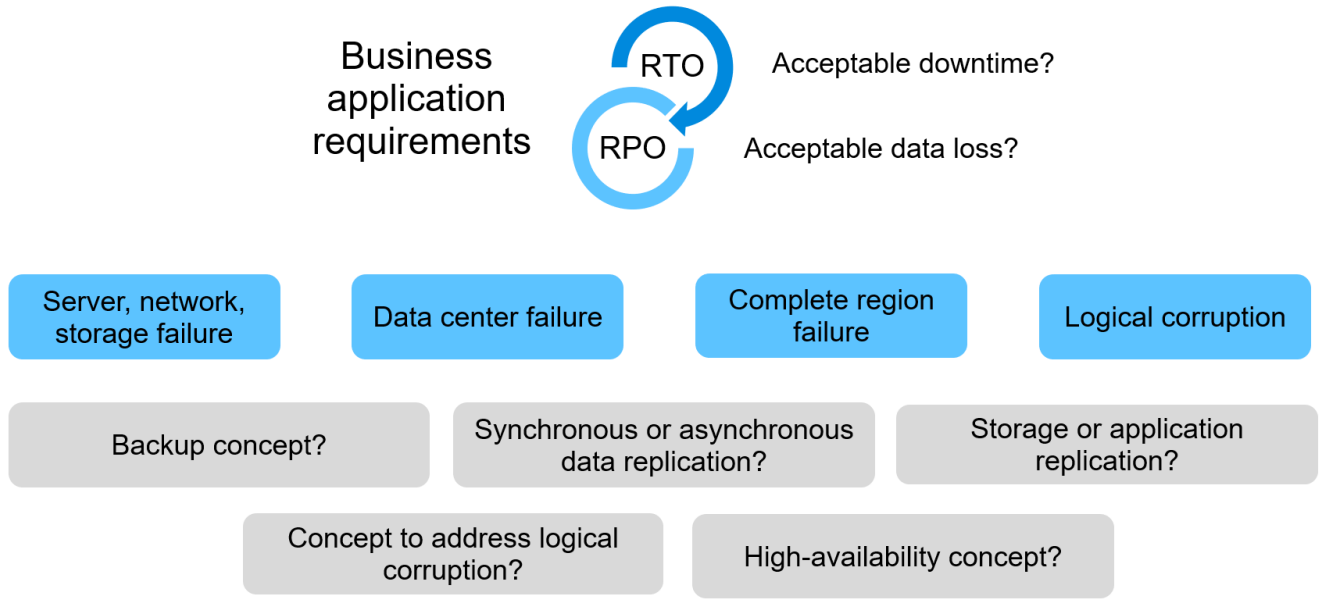
TR-4891: SAP HANA disaster recovery with Azure NetApp Files

Nils Bauer, NetApp
Ralf Klahr, Microsoft

Studies have shown that business application downtime has a significant negative impact on the business of enterprises. In addition to the financial impact, downtime can also damage the company's reputation, staff morale, and customer loyalty. Surprisingly, not all companies have a comprehensive disaster recovery policy.

Running SAP HANA on Azure NetApp Files (ANF) gives customers access to additional features that extend and improve the built-in data protection and disaster recovery capabilities of SAP HANA. This overview section explains these options to help customers select options that support their business needs.

To develop a comprehensive disaster recovery policy, customers must understand the business application requirements and technical capabilities they need for data protection and disaster recovery. The following figure provides an overview of data protection.



Business application requirements

There are two key indicators for business applications:

- The recovery point objective (RPO), or the maximum tolerable data loss
- The recovery time objective (RTO), or the maximum tolerable business application downtime

These requirements are defined by the kind of application used and the nature of your business data. The RPO and the RTO might differ if you are protecting against failures at a single Azure region. They might also differ if you are preparing for catastrophic disasters such as the loss of a complete Azure region. It is important to evaluate the business requirements that define the RPO and RTO, because these requirements have a significant impact on the technical options that are available.

High availability

The infrastructure for SAP HANA, such as virtual machines, network, and storage, must have redundant components to make sure that there is no single point of failure. MS Azure provides redundancy for the different infrastructure components.

To provide high availability on the compute and application side, standby SAP HANA hosts can be configured for built-in high availability with an SAP HANA multiple-host system. If a server or an SAP HANA service fails, the SAP HANA service fails over to the standby host, which causes application downtime.

If application downtime is not acceptable in the case of server or application failure, you can also use SAP HANA system replication as a high-availability solution that enables failover in a very short time frame. SAP customers use HANA system replication not only to address high availability for unplanned failures, but also to minimize downtime for planned operations, such as HANA software upgrades.

Logical corruption

Logical corruption can be caused by software errors, human errors, or sabotage. Unfortunately, logical corruption often cannot be addressed with standard high-availability and disaster recovery solutions. As a result, depending on the layer, application, file system, or storage where the logical corruption occurred, RTO and RPO requirements can sometimes not be fulfilled.

The worst case is a logical corruption in an SAP application. SAP applications often operate in a landscape in which different applications communicate with each other and exchange data. Therefore, restoring and recovering an SAP system in which a logical corruption has occurred is not the recommended approach. Restoring the system to a point in time before the corruption occurred results in data loss, so the RPO becomes larger than zero. Also, the SAP landscape would no longer be in sync and would require additional postprocessing.

Instead of restoring the SAP system, the better approach is to try to fix the logical error within the system, by analyzing the problem in a separate repair system. Root cause analysis requires the involvement of the business process and application owner. For this scenario, you create a repair system (a clone of the production system) based on data stored before the logical corruption occurred. Within the repair system, the required data can be exported and imported to the production system. With this approach, the productive system does not need to be stopped, and, in the best-case scenario, no data or only a small fraction of data is lost.

The required steps to setup a repair system are identical to a disaster recovery testing scenario described in this document. The described disaster recovery solution can therefore easily be extended to address logical corruption as well.

Backups

Backups are created to enable restore and recovery from different point-in-time datasets. Typically, these backups are kept for a couple of days to a few weeks.

Depending on the kind of corruption, restore and recovery can be performed with or without data loss. If the RPO must be zero, even when the primary and backup storage is lost, backup must be combined with synchronous data replication.

The RTO for restore and recovery is defined by the required restore time, the recovery time (including database start), and the loading of data into memory. For large databases and traditional backup approaches, the RTO can easily be several hours, which might not be acceptable. To achieve very low RTO values, a backup must be combined with a hot-standby solution, which includes preloading data into memory.

In contrast, a backup solution must address logical corruption, because data replication solutions cannot cover all kinds of logical corruption.

Synchronous or asynchronous data replication

The RPO primarily determines which data replication method you should use. If the RPO must be zero, even when the primary and backup storage is lost, the data must be replicated synchronously. However, there are technical limitations for synchronous replication, such as the distance between two Azure regions. In most cases, synchronous replication is not appropriate for distances greater than 100km due to latency, and therefore this is not an option for data replication between Azure regions.

If a larger RPO is acceptable, asynchronous replication can be used over large distances. The RPO in this case is defined by the replication frequency.

HANA system replication with or without data preload

The startup time for an SAP HANA database is much longer than that of traditional databases because a large amount of data must be loaded into memory before the database can provide the expected performance. Therefore, a significant part of the RTO is the time needed to start the database. With any storage-based replication as well as with HANA System Replication without data preload, the SAP HANA database must be started in case of failover to the disaster recovery site.

SAP HANA system replication offers an operation mode in which the data is preloaded and continuously updated at the secondary host. This mode enables very low RTO values, but it also requires a dedicated server that is only used to receive the replication data from the source system.

Next: Disaster recovery solution comparison.

Disaster recovery solution comparison

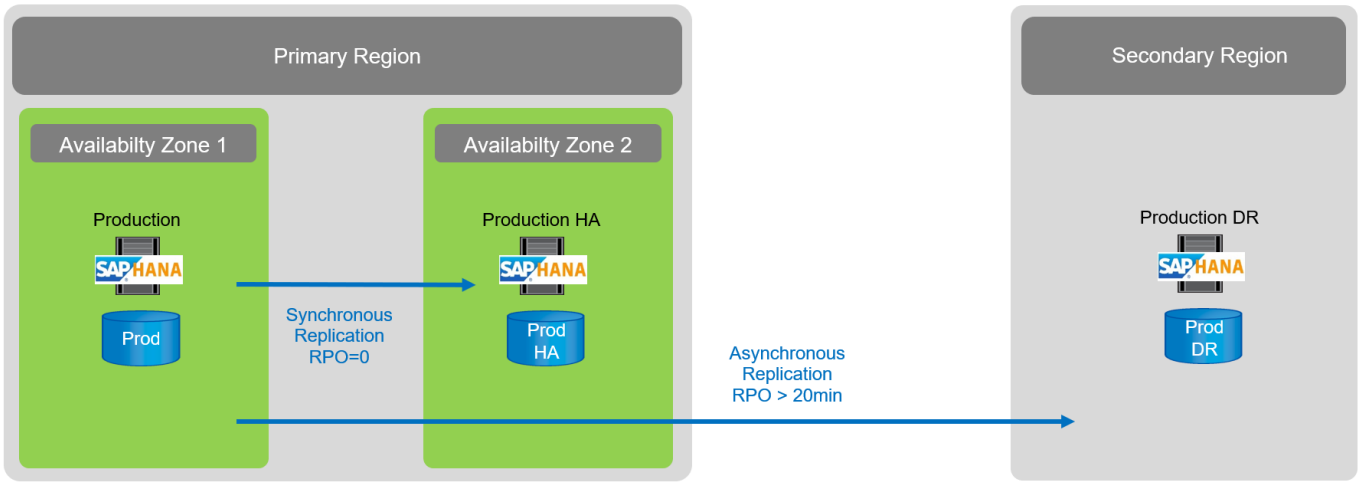
Previous: SAP HANA disaster recovery with Azure NetApp Files overview.

A comprehensive disaster recovery solution must enable customers to recover from a complete failure of the primary site. Therefore, data must be transferred to a secondary site, and a complete infrastructure is necessary to run the required production SAP HANA systems in case of a site failure. Depending on the availability requirements of the application and the kind of disaster you want to be protected from, a two-site or three-site disaster recovery solution must be considered.

The following figure shows a typical configuration in which the data is replicated synchronously within the same Azure region into a second availability zone. The short distance allows you to replicate the data synchronously to achieve an RPO of zero (typically used to provide HA).

In addition, data is also replicated asynchronously to a secondary region to be protected from disasters, when the primary region is affected. The minimum achievable RPO depends on the data replication frequency, which is limited by the available bandwidth between the primary and the secondary region. A typical minimal RPO is in the range of 20 minutes to multiple hours.

This document discusses different implementation options of a two- region disaster recovery solution.



SAP HANA System Replication

SAP HANA System Replication works at the database layer. The solution is based on an additional SAP HANA system at the disaster recovery site that receives the changes from the primary system. This secondary system must be identical to the primary system.

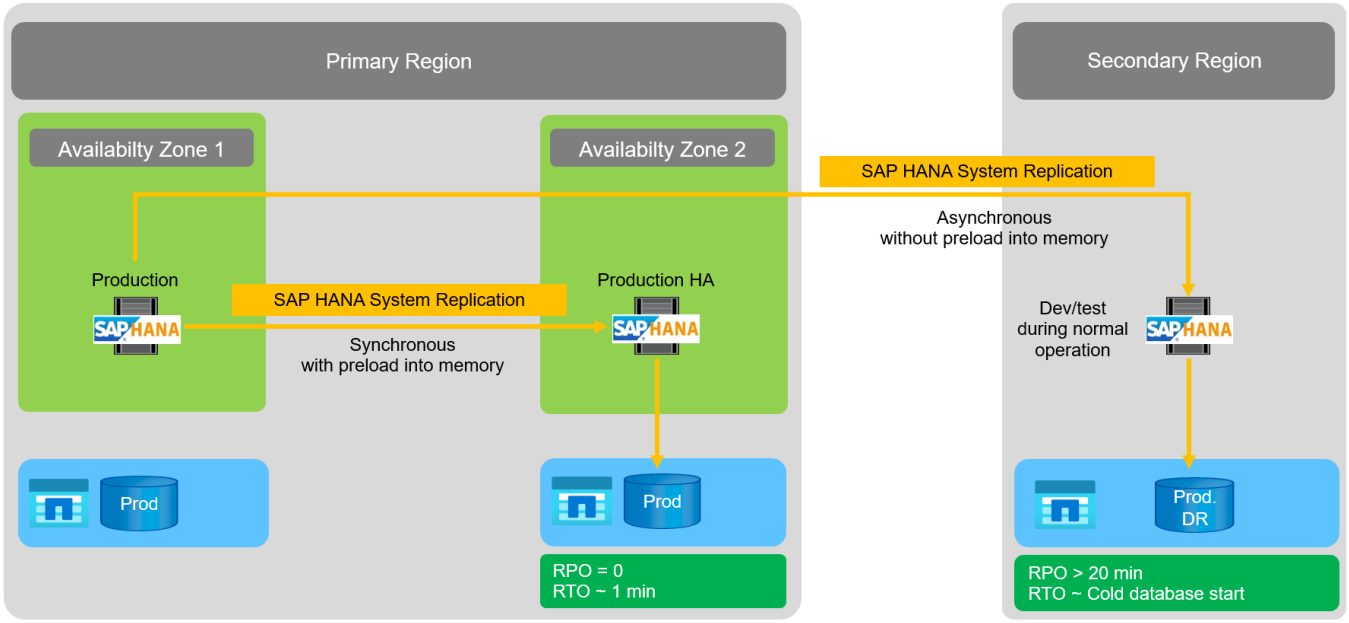
SAP HANA System Replication can be operated in one of two modes:

- With data preloaded into memory and a dedicated server at the disaster recovery site:
  - The server is used exclusively as an SAP HANA System Replication secondary host.
  - Very low RTO values can be achieved because the data is already loaded into memory and no database start is required in case of a failover.
- Without data preloaded into memory and a shared server at the disaster recovery site:
  - The server is shared as an SAP HANA System Replication secondary and as a dev/test system.
  - RTO depends mainly on the time required to start the database and load the data into memory.

For a full description of all configuration options and replication scenarios, see the SAP HANA Administration Guide.

The following figure shows the setup of a two-region disaster recovery solution with SAP HANA System Replication. Synchronous replication with data preloaded into memory is used for local HA in the same Azure region, but in different availability zones. Asynchronous replication without data preloaded is configured for the remote disaster recovery region.

The following figure depicts SAP HANA System Replication.



SAP HANA System Replication with data preloaded into memory

Very low RTO values with SAP HANA can be achieved only with SAP HANA System Replication with data preloaded into memory. Operating SAP HANA System Replication with a dedicated secondary server at the disaster recovery site allows an RTO value of approximately 1 minute or less. The replicated data is received and preloaded into memory at the secondary system. Because of this low failover time, SAP HANA System Replication is also often used for near-zero-downtime maintenance operations, such as HANA software upgrades.

Typically, SAP HANA System Replication is configured to replicate synchronously when data preload is chosen. The maximum supported distance for synchronous replication is in the range of 100km.

SAP System Replication without data preloaded into memory

For less stringent RTO requirements, you can use SAP HANA System Replication without data preloaded. In this operational mode, the data at the disaster recovery region is not loaded into memory. The server at the DR region is still used to process SAP HANA System Replication running all the required SAP HANA processes. However, most of the server's memory is available to run other services, such as SAP HANA dev/test systems.

In the event of a disaster, the dev/test system must be shut down, failover must be initiated, and the data must be loaded into memory. The RTO of this cold standby approach depends on the size of the database and the read throughput during the load of the row and column store. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data should take approximately 18 minutes.

SAP HANA disaster recovery with ANF Cross-Region Replication

ANF Cross-Region Replication is built into ANF as a disaster recovery solution using asynchronous data replication. ANF Cross-Region Replication is configured through a data protection relationship between two ANF volumes on a primary and a secondary Azure region. ANF Cross-Region Replication updates the secondary volume by using efficient block delta replications. Update schedules can be defined during the replication configuration.

The following figure shows a two- region disaster recovery solution example, using ANF Cross- Region Replication. In this example the HANA system is protected with HANA System Replication within the primary region as discussed in the previous chapter. The replication to a secondary region is performed using ANF

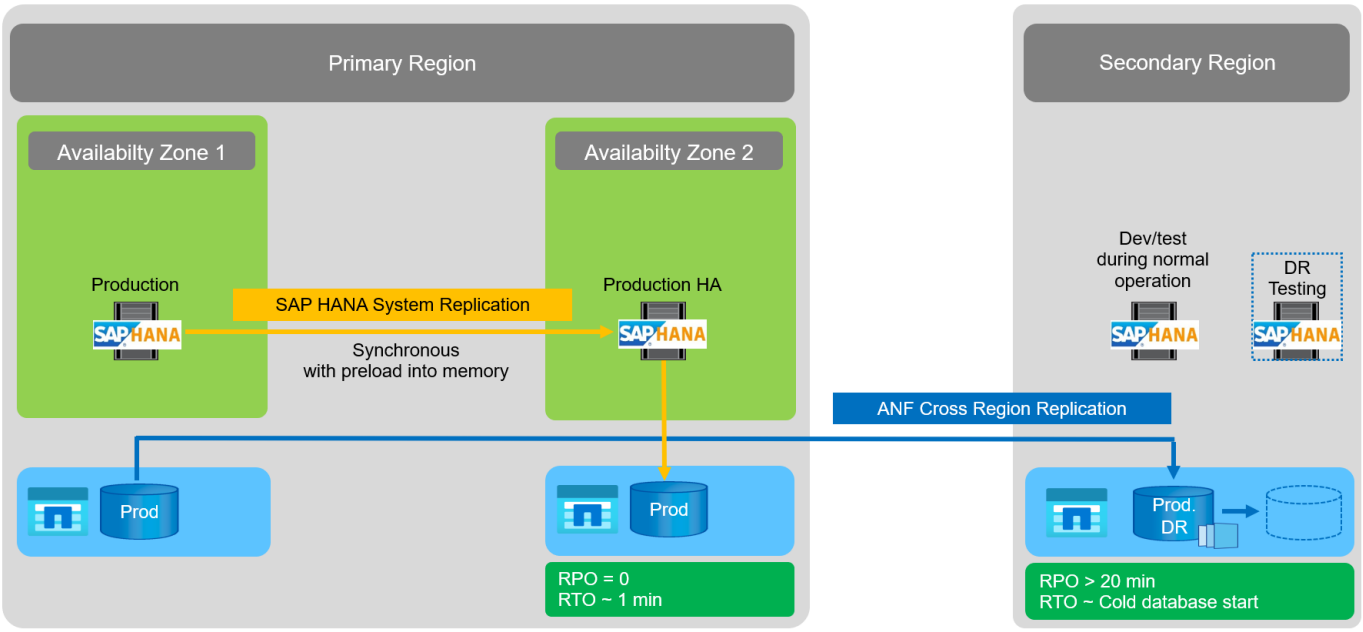
cross region replication. The RPO is defined by the replication schedule and replication options.

The RTO depends mainly on the time needed to start the HANA database at the disaster recovery site and to load the data into memory. With the assumption that the data is read with a throughput of 1000MB/s, loading 1TB of data would take approximately 18 minutes. Depending on the replication configuration, forward recovery is required as well and will add to the total RTO value.

More details on the different configuration options are provided in chapter Configuration options for cross region replication with SAP HANA.

The servers at the disaster recovery sites can be used as dev/test systems during normal operation. In case of a disaster, the dev/test systems must be shut down and started as DR production servers.

ANF Cross-Region Replication allows you to test the DR workflow without impacting the RPO and RTO. This is accomplished by creating volume clones and attaching them to the DR testing server.



Summary of disaster recovery solutions

The following table compares the disaster recovery solutions discussed in this section and highlights the most important indicators.

The key findings are as follows:

- If a very low RTO is required, SAP HANA System Replication with preload into memory is the only option.
  - A dedicated server is required at the DR site to receive the replicated data and load the data into memory.
- In addition, storage replication is needed for the data that resides outside of the database (for example shared files, interfaces, and so on).
- If RTO/RPO requirements are less strict, ANF Cross-Region Replication can also be used to:
  - Combine database and nondatabase data replication.
  - Cover additional use cases such as disaster recovery testing and dev/test refresh.
  - With storage replication the server at the DR site can be used as a QA or test system during normal operation.

- A combination of SAP HANA System Replication as an HA solution with RPO=0 with storage replication for long distance makes sense to address the different requirements.

The following table provides a comparison of disaster recovery solutions.

	Storage replication	SAP HANA system replication	
	Cross-region replication	**With data preload**	**Without data preload**
RTO	Low to medium, depending on database startup time and forward recovery	Very low	Low to medium, depending on database startup time
RPO	RPO > 20min asynchronous replication	RPO > 20min asynchronous replication RPO=0 synchronous replication	RPO > 20min asynchronous replication RPO=0 synchronous replication
Servers at DR site can be used for dev/test	Yes	No	Yes
Replication of nondatabase data	Yes	No	No
DR data can be used for refresh of dev/test systems	Yes	No	No
DR testing without affecting RTO and RPO	Yes	No	No

Next: ANF Cross-Region Replication with SAP HANA.

ANF Cross-Region Replication with SAP HANA

Previous: Disaster recovery solution comparison.

Application agnostic information on Cross-Region Replication can be found at Azure NetApp Files documentation | Microsoft Docs in the concepts and how- to guide sections.

Next: Configuration options for Cross-Region Replication with SAP HANA.

Configuration options for Cross-Region Replication with SAP HANA

Previous: ANF Cross-Region Replication with SAP HANA.

The following figure shows the volume replication relationships for an SAP HANA system using ANF Cross-Region Replication. With ANF Cross-Region Replication, the HANA data and the HANA shared volume must be replicated. If only the HANA data volume is replicated, typical RPO values are in the range of one day. If lower RPO values are required, the HANA log backups must be also replicated for forward recovery.

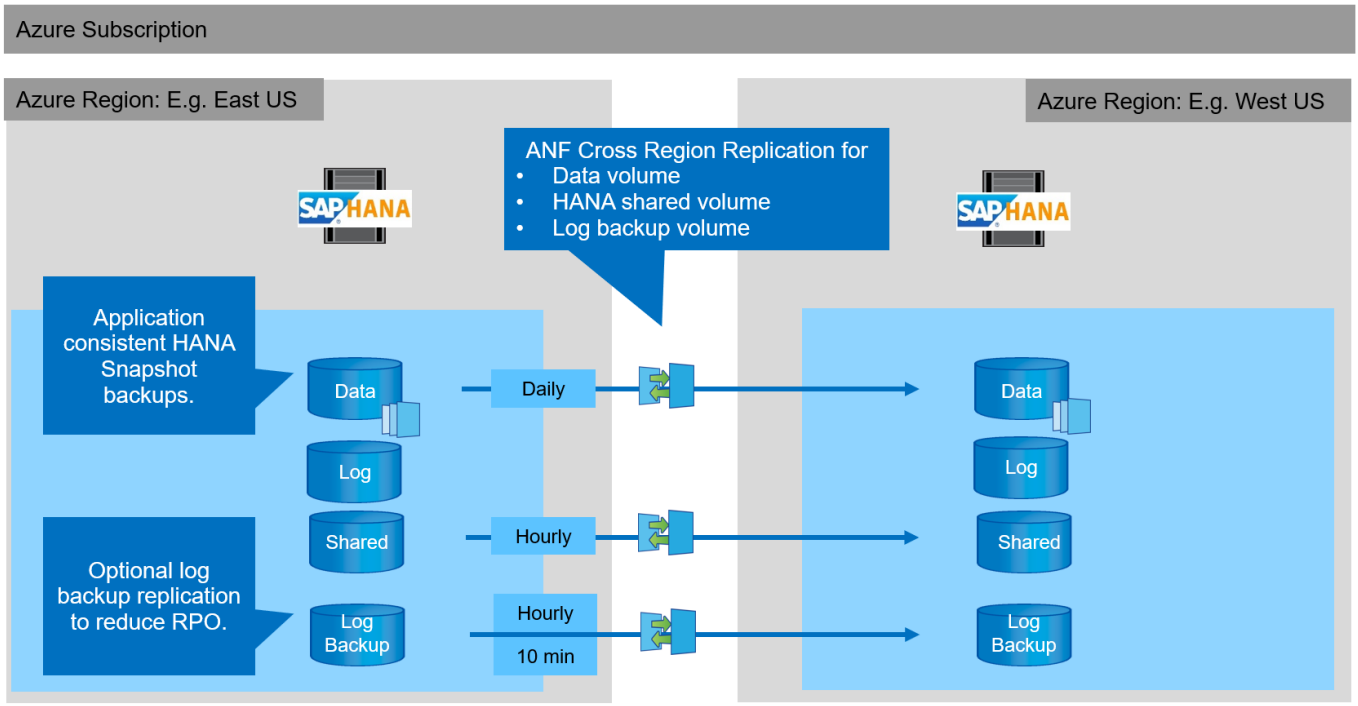
The term “log backup” used in this document includes the log backup and the HANA backup catalog backup. The HANA backup catalog is required to execute forward recovery operations.

The following description and the lab setup focus on the HANA database. Other shared files, for example the SAP transport directory would be protected and replicated in the same way as the HANA shared volume.

To enable HANA save-point recovery or forward recovery using the log backups, application-consistent data Snapshot backups must be created at the primary site for the HANA data volume. This can be done for example with the ANF backup tool AzAcSnap (see also What is Azure Application Consistent Snapshot tool for Azure NetApp Files | Microsoft Docs). The Snapshot backups created at the primary site are then replicated to the DR site.

In the case of a disaster failover, the replication relationship must be broken, the volumes must be mounted to the DR production server, and the HANA database must be recovered, either to the last HANA save point or with forward recovery using the replicated log backups. The chapter Disaster recovery failover, describes the required steps.

The following figure depicts the HANA configuration options for cross-region replication.



With the current version of Cross-Region Replication, only fixed schedules can be selected, and the actual replication update time cannot be defined by the user. Available schedules are daily, hourly and every 10 minutes. Using these schedule options, two different configurations make sense depending on the RPO requirements: data volume replication without log backup replication and log backup replication with different schedules, either hourly or every 10 minutes. The lowest achievable RPO is around 20 minutes. The following table summarizes the configuration options and the resulting RPO and RTO values.

	Data volume replication	**Data and log backup volume replication**	**Data and log backup volume replication**
CRR schedule data volume	Daily	Daily	Daily
CRR schedule log backup volume	n/a	Hourly	10 min

	Data volume replication	Data and log backup volume replication	Data and log backup volume replication
Max RPO	24 hours + Snapshot schedule (e.g., 6 hours)	1 hour	2 x 10 min
Max RTO	Primarily defined by HANA startup time	HANA startup time + recovery time	HANA startup time + recovery time
Forward recovery	NA	Logs for the last 24 hours + Snapshot schedule (e.g., 6 hours)	Logs for the last 24 hours + Snapshot schedule (e.g., 6 hours)

Next: Requirements and best practices.

Requirements and best practices

Previous: Configuration options for Cross-Region Replication with SAP HANA.

Microsoft Azure does not guarantee the availability of a specific virtual machine (VM) type upon creation or when starting a deallocated VM. Specifically, in case of a region failure, many clients might require additional VMs at the disaster recovery region. It is therefore recommended to actively use a VM with the required size for disaster failover as a test or QA system at the disaster recovery region to have the required VM type allocated.

For cost optimization it makes sense to use an ANF capacity pool with a lower performance tier during normal operation. The data replication does not require high performance and could therefore use a capacity pool with a standard performance tier. For disaster recovery testing, or if a disaster failover is required, the volumes must be moved to a capacity pool with a high-performance tier.

If a second capacity pool is not an option, the replication target volumes should be configured based on capacity requirements and not on performance requirements during normal operations. The quota or the throughput (for manual QoS) can then be adapted for disaster recovery testing in the case of disaster failover.

Further information can be found at Requirements and considerations for using Azure NetApp Files volume cross-region replication | Microsoft Docs.

Next: Lab setup.

Lab setup

Previous: Requirements and best practices.

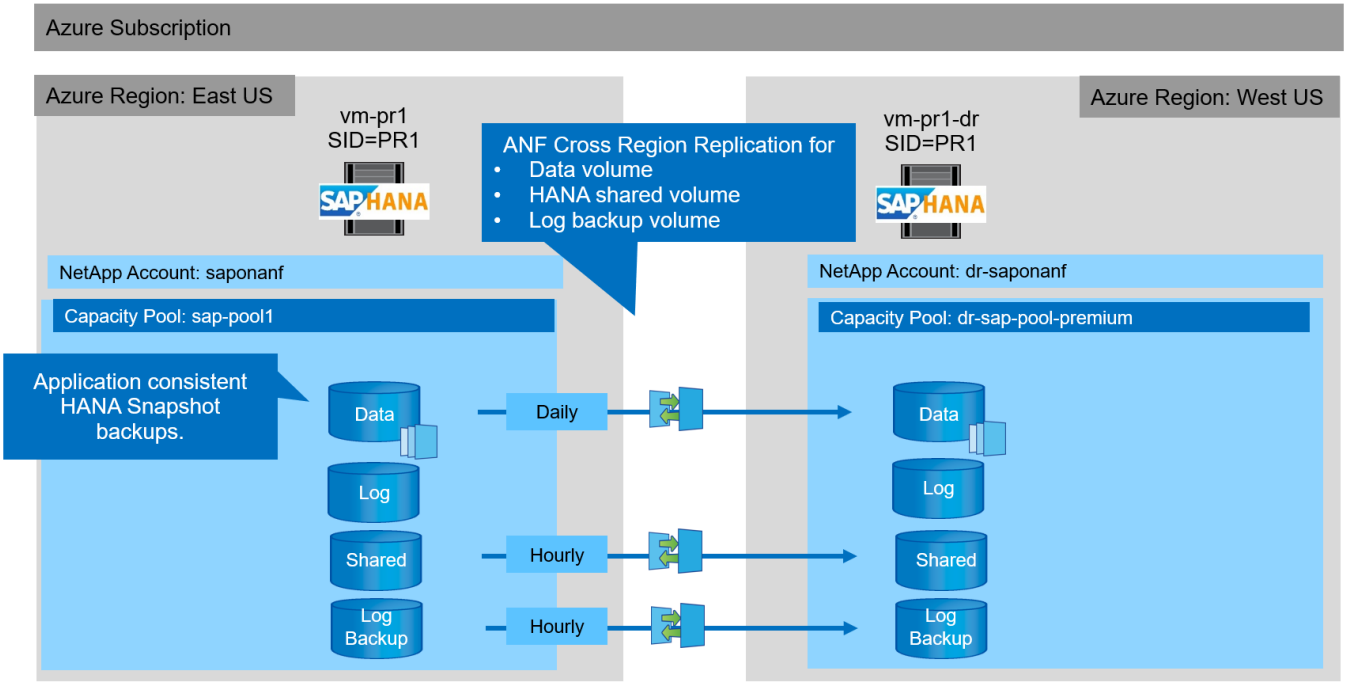
Solution validation has been performed with an SAP HANA single-host system. The Microsoft AzAcSnap Snapshot backup tool for ANF has been used to configure HANA application-consistent Snapshot backups. A daily data volume, hourly log backup, and shared volume replication were all configured. Disaster recover testing and failover was validated with a save point as well as with forward recovery operations.

The following software versions have been used in the lab setup:

- Single host SAP HANA 2.0 SPS5 system with a single tenant
- SUSE SLES for SAP 15 SP1
- AzAcSnap 5.0

A single capacity pool with manual QoS has been configured at the DR site.

The following figure depicts the lab setup.



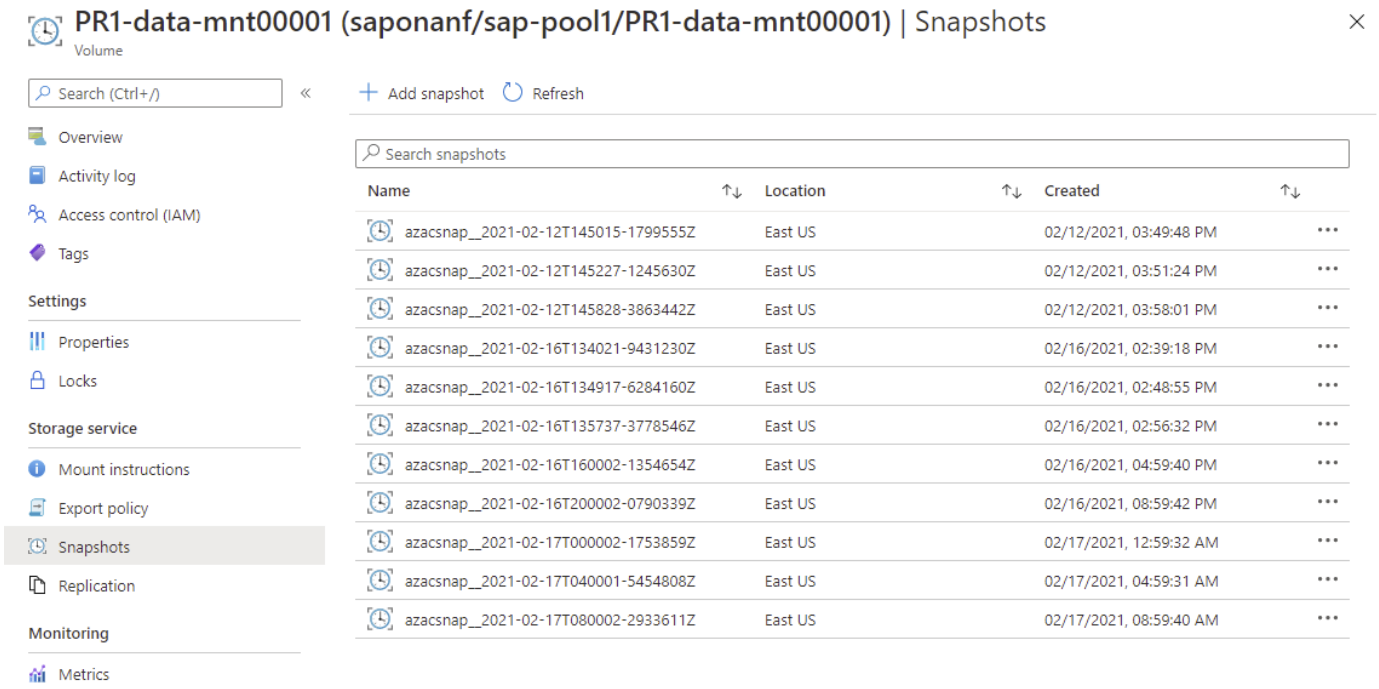
Snapshot backup configuration with AzAcSnap

At the primary site, AzAcSnap was configured to create application-consistent Snapshot backups of the HANA system PR1. These Snapshot backups are available at the ANF data volume of the PR1 HANA system, and they are also registered in the SAP HANA backup catalog, as shown in the following two figures. Snapshot backups were scheduled for every 4 hours.

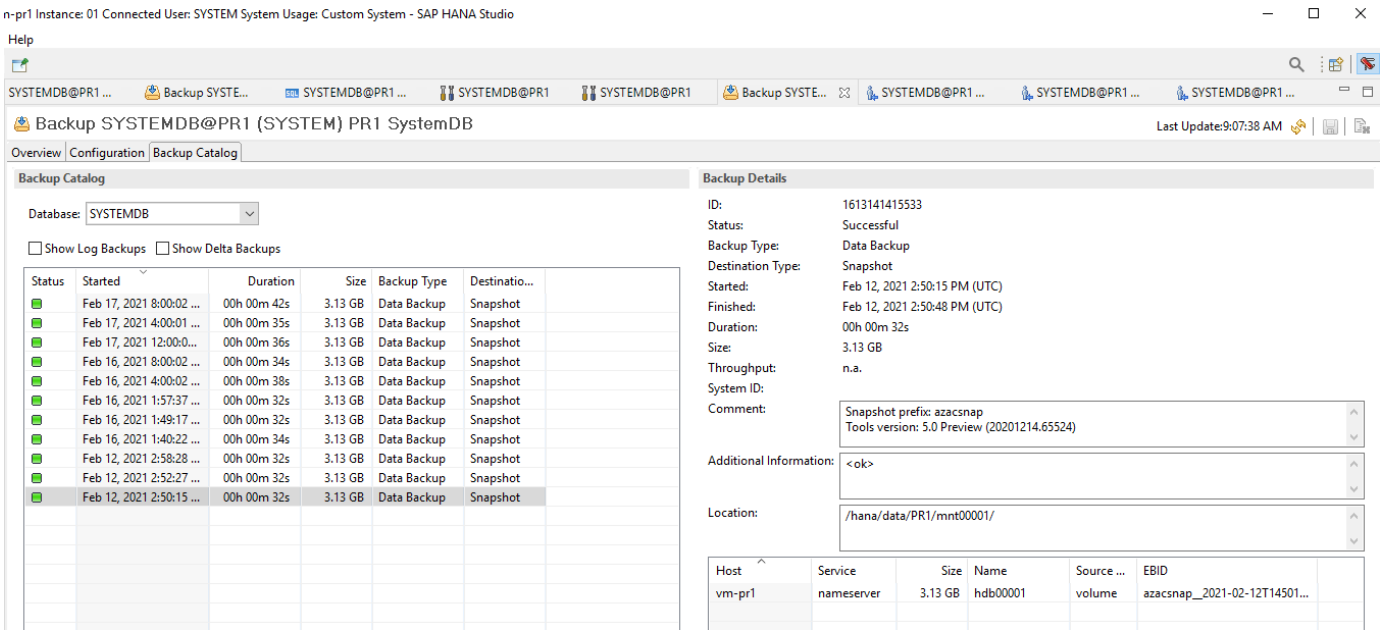
With the replication of the data volume using ANF Cross-Region Replication, these Snapshot backups are replicated to the disaster recovery site and can be used to recover the HANA database.

The following figure shows the Snapshot backups of the HANA data volume.

1-data-mnt00001)



The following figure shows the SAP HANA backup catalog.



Next: Configuration steps for ANF Cross-Region Replication.

Configuration steps for ANF Cross-Region Replication

Previous: Lab setup.

A few preparation steps must be performed at the disaster recovery site before volume replication can be configured.

- A NetApp account must be available and configured with the same Azure subscription as the source.

- A capacity pool must be available and configured using the above NetApp account.
- A virtual network must be available and configured.
- Within the virtual network, a delegated subnet must be available and configured for use with ANF.

Protection volumes can now be created for the HANA data, the HANA shared and the HANA log backup volume. The following table shows the configured destination volumes in our lab setup.

To achieve the best latency, the volumes must be placed close to the VMs that run the SAP HANA in case of a disaster failover. Therefore, the same pinning process is required for the DR volumes as for any other SAP HANA production system.

HANA volume	Source	Destination	Replication schedule
HANA data volume	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Daily
HANA shared volume	PR1-shared	PR1-shared-sm-dest	Hourly
HANA log/catalog backup volume	hanabackup	hanabackup-sm-dest	Hourly

For each volume, the following steps must be performed:

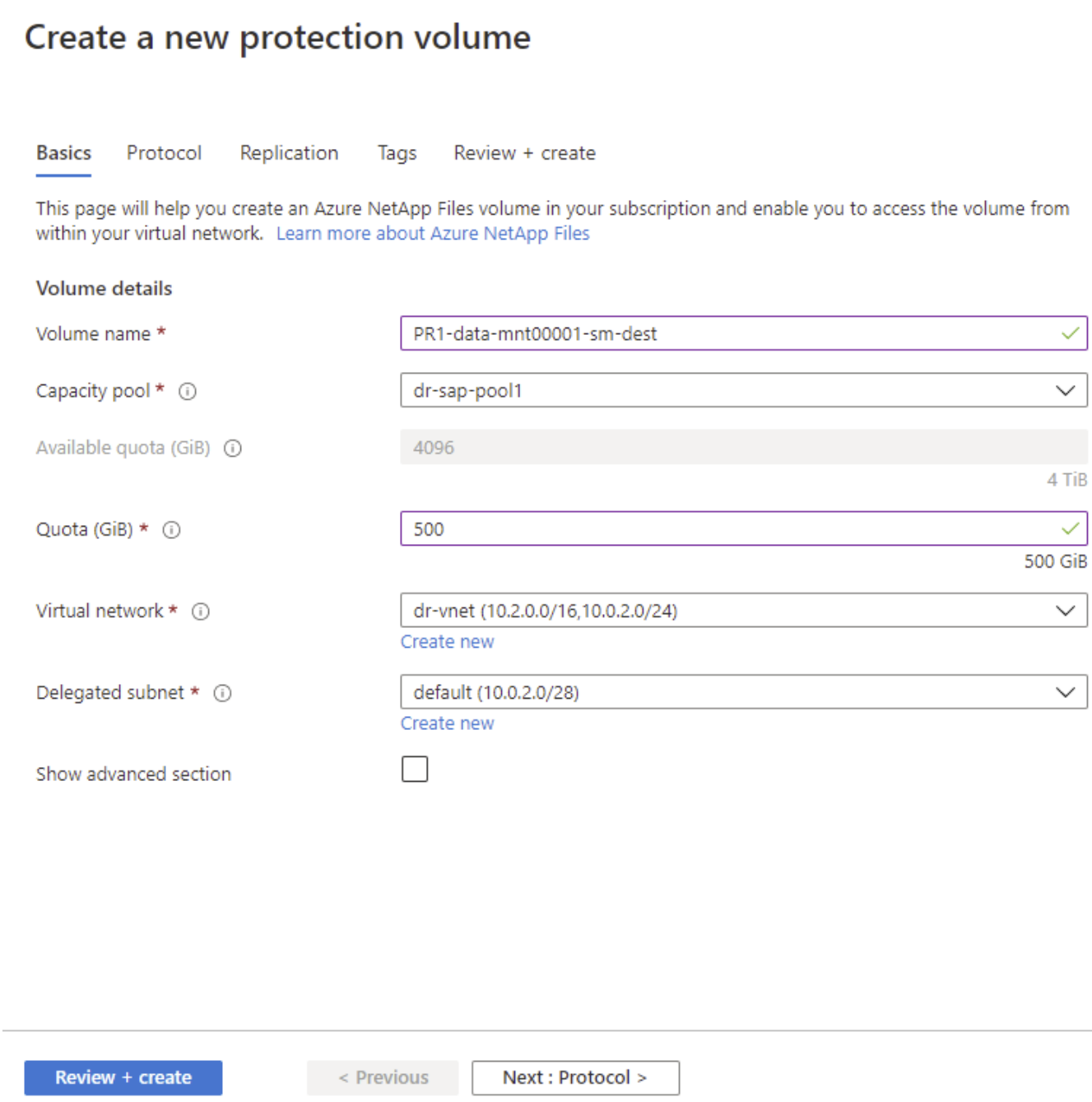
1. Create a new protection volume at the DR site:
   a. Provide the volume name, capacity pool, quota, and network information.
   b. Provide the protocol and volume access information.
   c. Provide the source volume ID and a replication schedule.
   d. Create a target volume.
2. Authorize replication at the source volume.
   - Provide the target volume ID.

The following screenshots show the configuration steps in detail.

At the disaster recovery site, a new protection volume is created by selecting volumes and clicking Add Data Replication. Within the Basics tab, you must provide the volume name, capacity pool and network information.

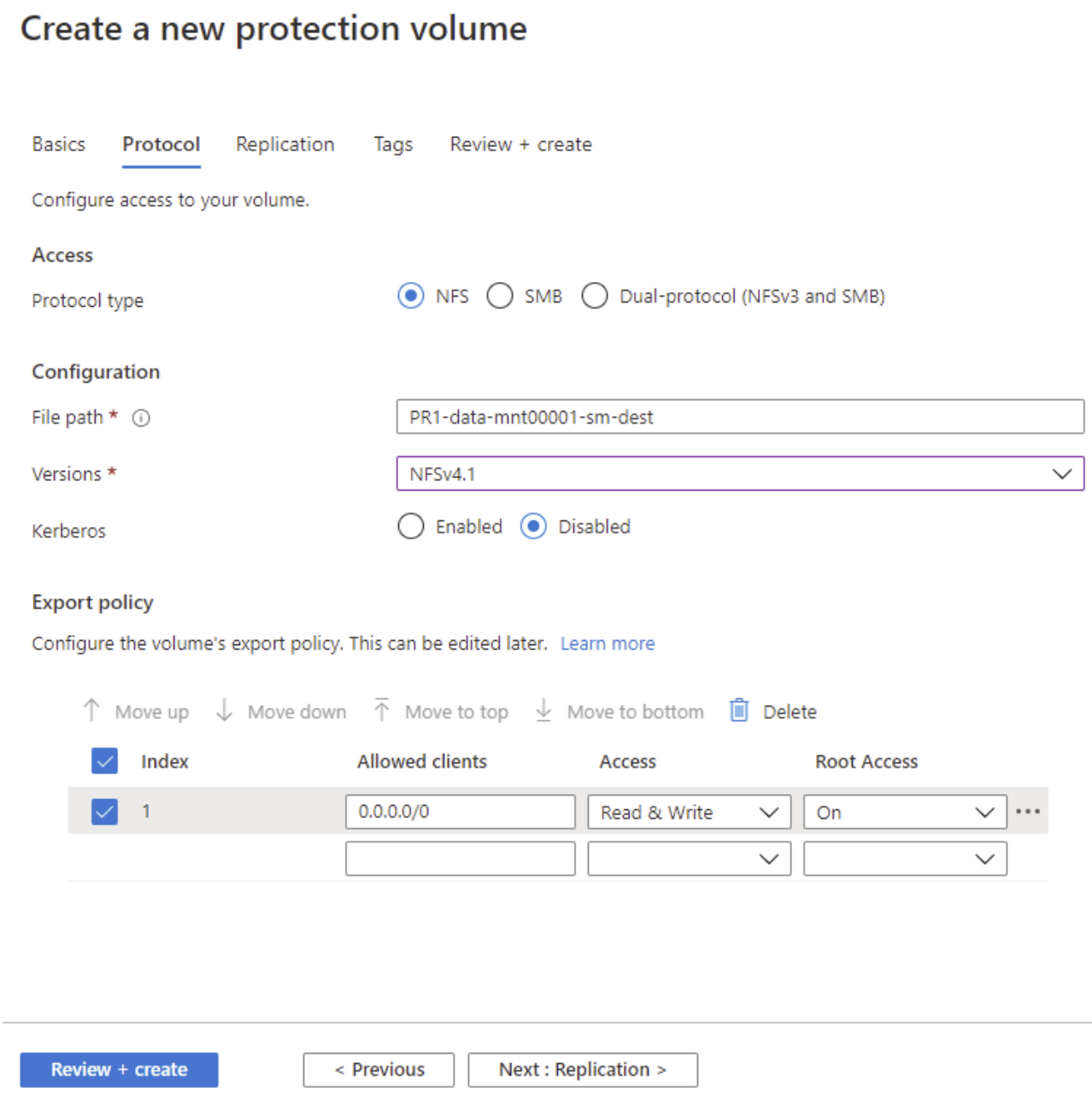
The quota of the volume can be set based on capacity requirements, because volume performance does not have an effect on the replication process. In the case of a disaster recovery failover, the quota must be adjusted to fulfill the real performance requirements.

If the capacity pool has been configured with manual QoS, you can configure the throughput in addition to the capacity requirements. Same as above, you can configure the throughput with a low value during normal operation and increase it in case of a disaster recovery failover.



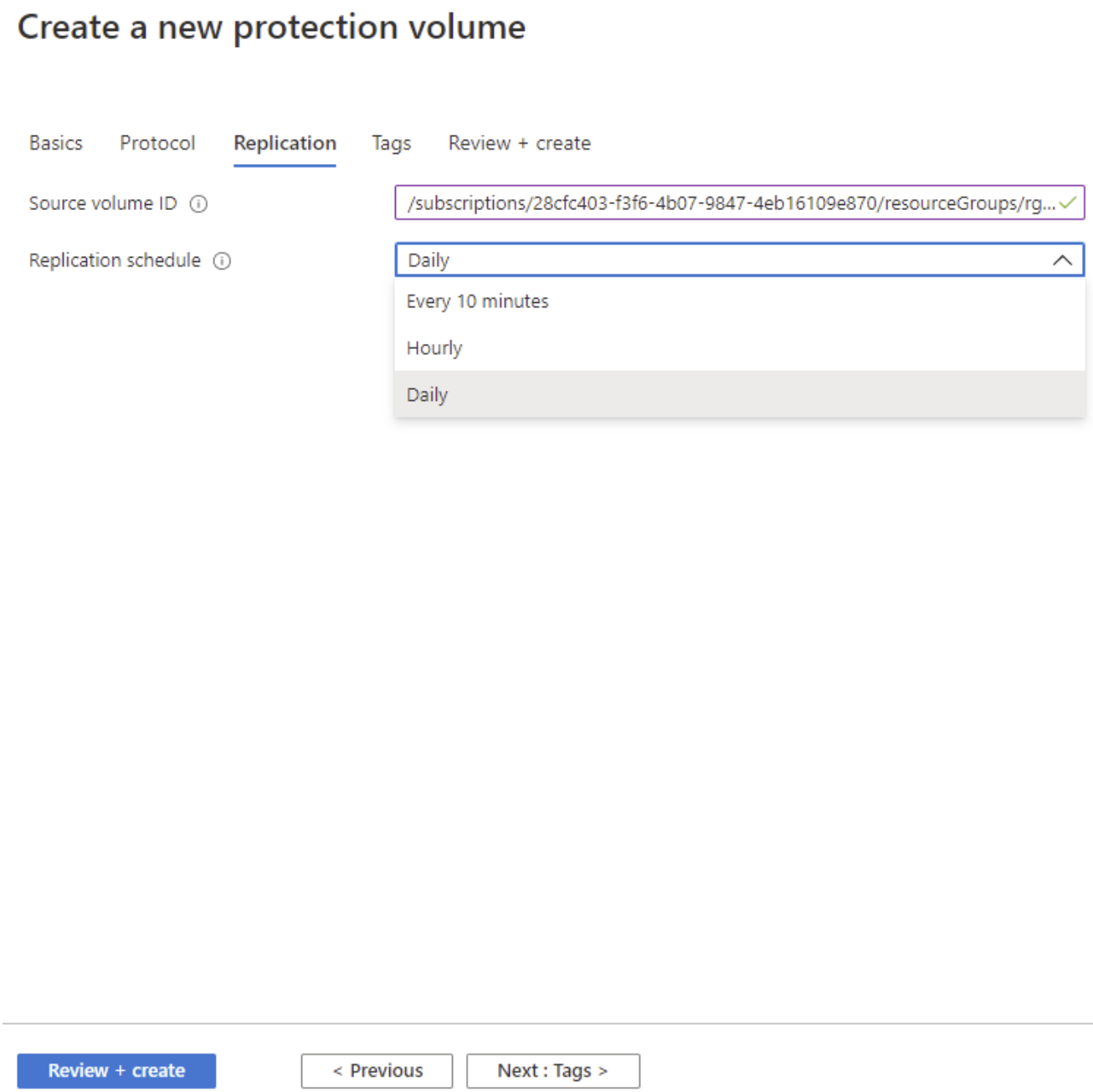
In the Protocol tab, you must provide the network protocol, the network path, and the export policy.

The protocol must be the same as the protocol used for the source volume.



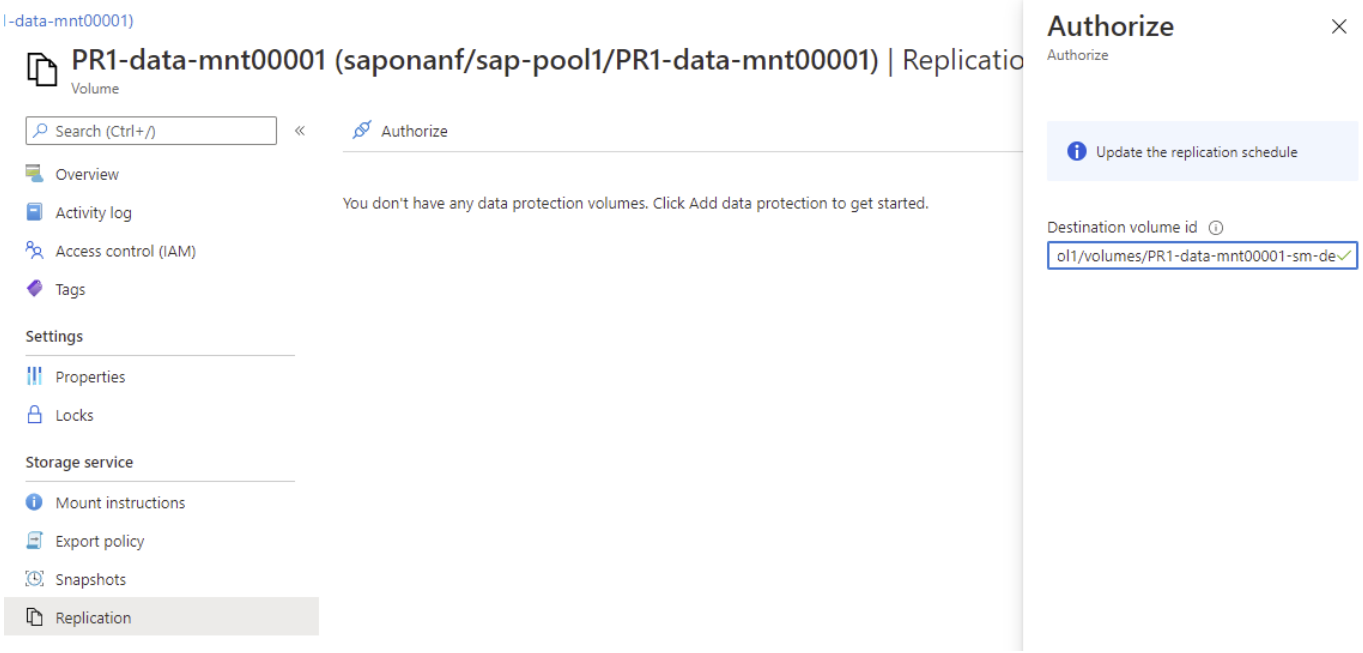
Within the Replication tab, you must configure the source volume ID and the replication schedule. For data volume replication, we configured a daily replication schedule for our lab setup.

The source volume ID can be copied from the Properties screen of the source volume.



As a final step, you must authorize replication at the source volume by providing the ID of the target volume.

You can copy the destination volume ID from the Properties screen of the destination volume.



The same steps must be performed for the HANA shared and the log backup volume.

Next: Monitoring ANF Cross-Region Replication.

Monitoring ANF Cross-Region Replication

Previous: Configuration steps for ANF Cross-Region Replication.

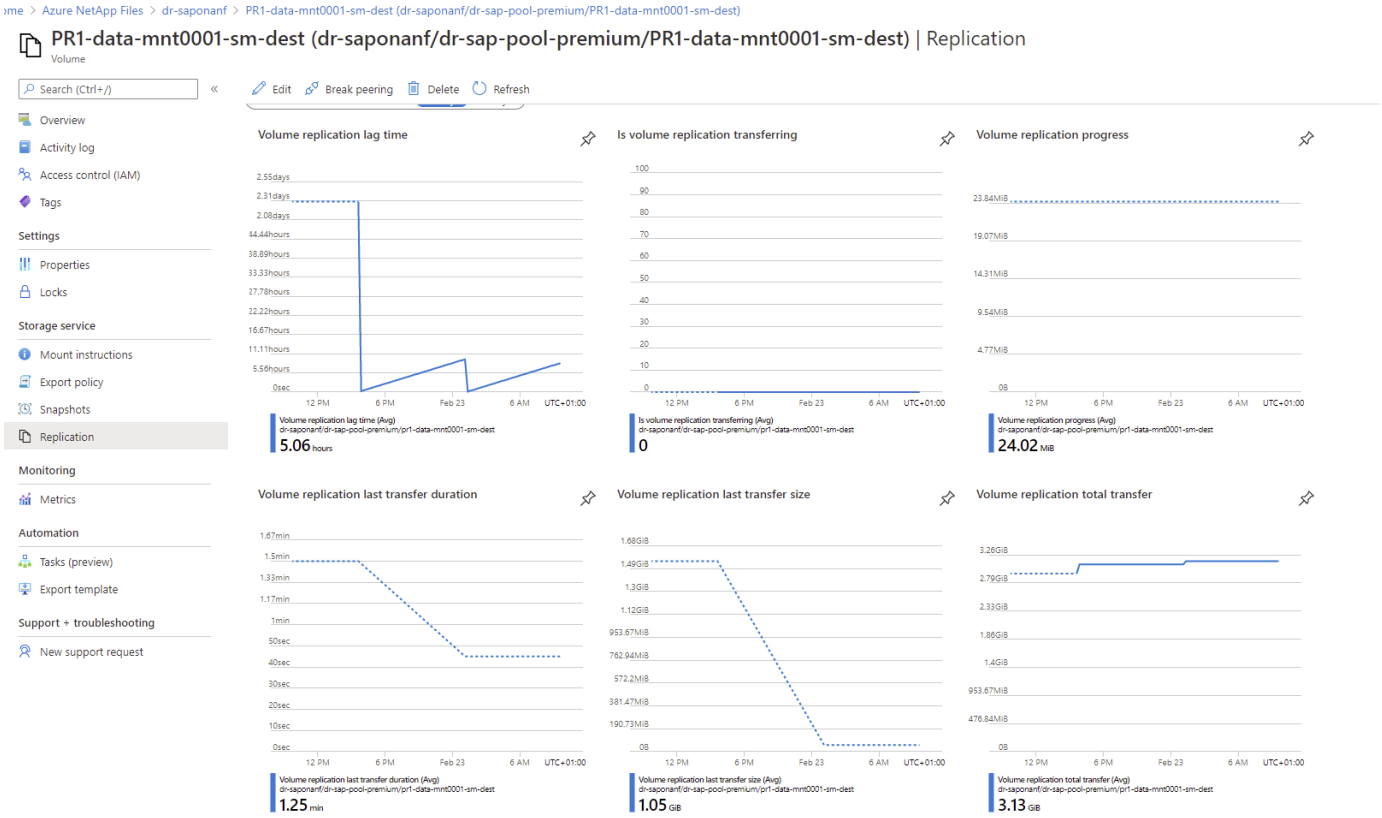
Replication status

The following three screenshots show the replication status for the data, log backup, and shared volumes.

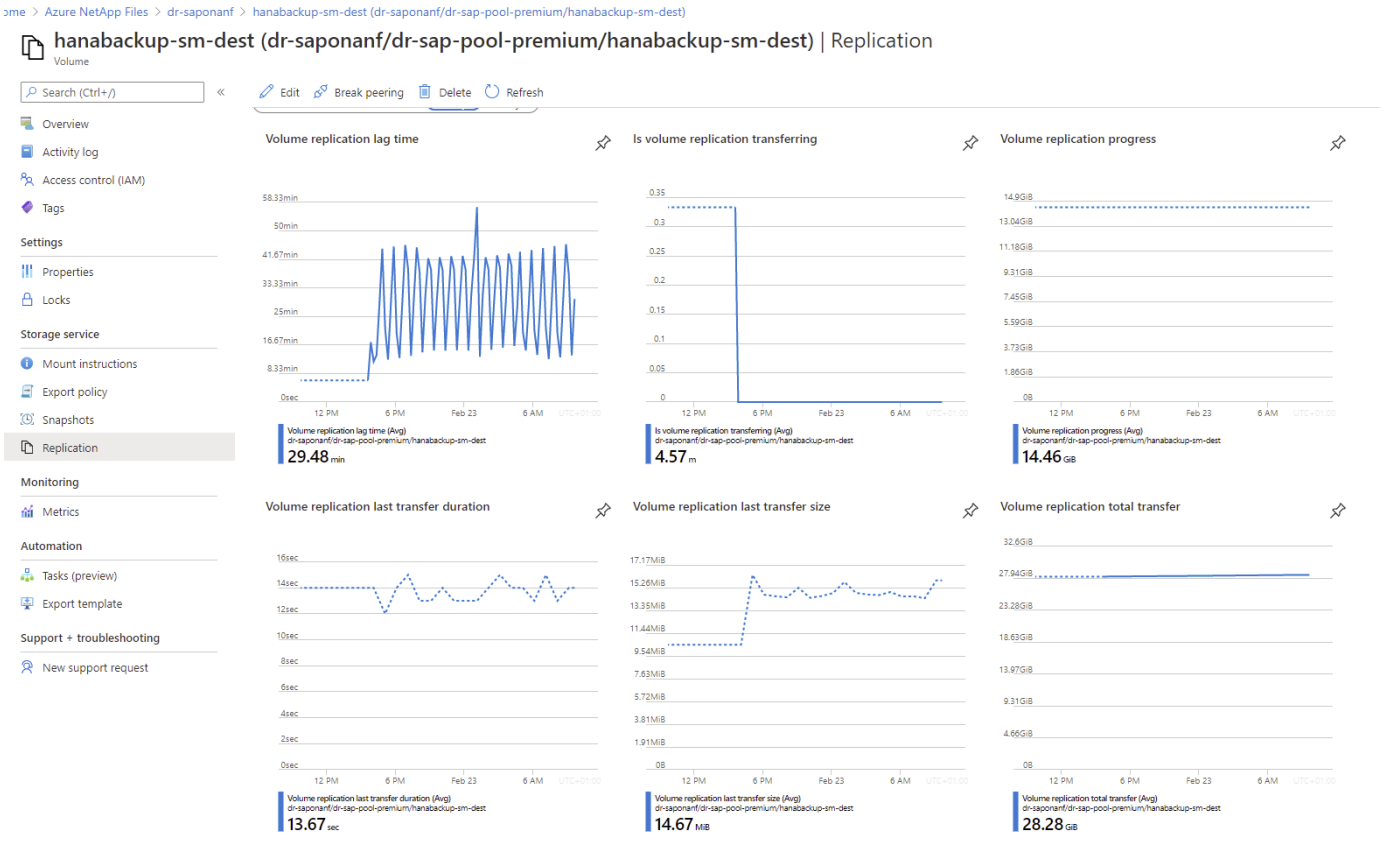
The volume replication lag time is a useful value to understand RPO expectations. For example, the log backup volume replication shows a maximum lag time of 58 minutes, which means that the maximum RPO has the same value.

The transfer duration and transfer size provide valuable information on bandwidth requirements and change the rate of the replicated volume.

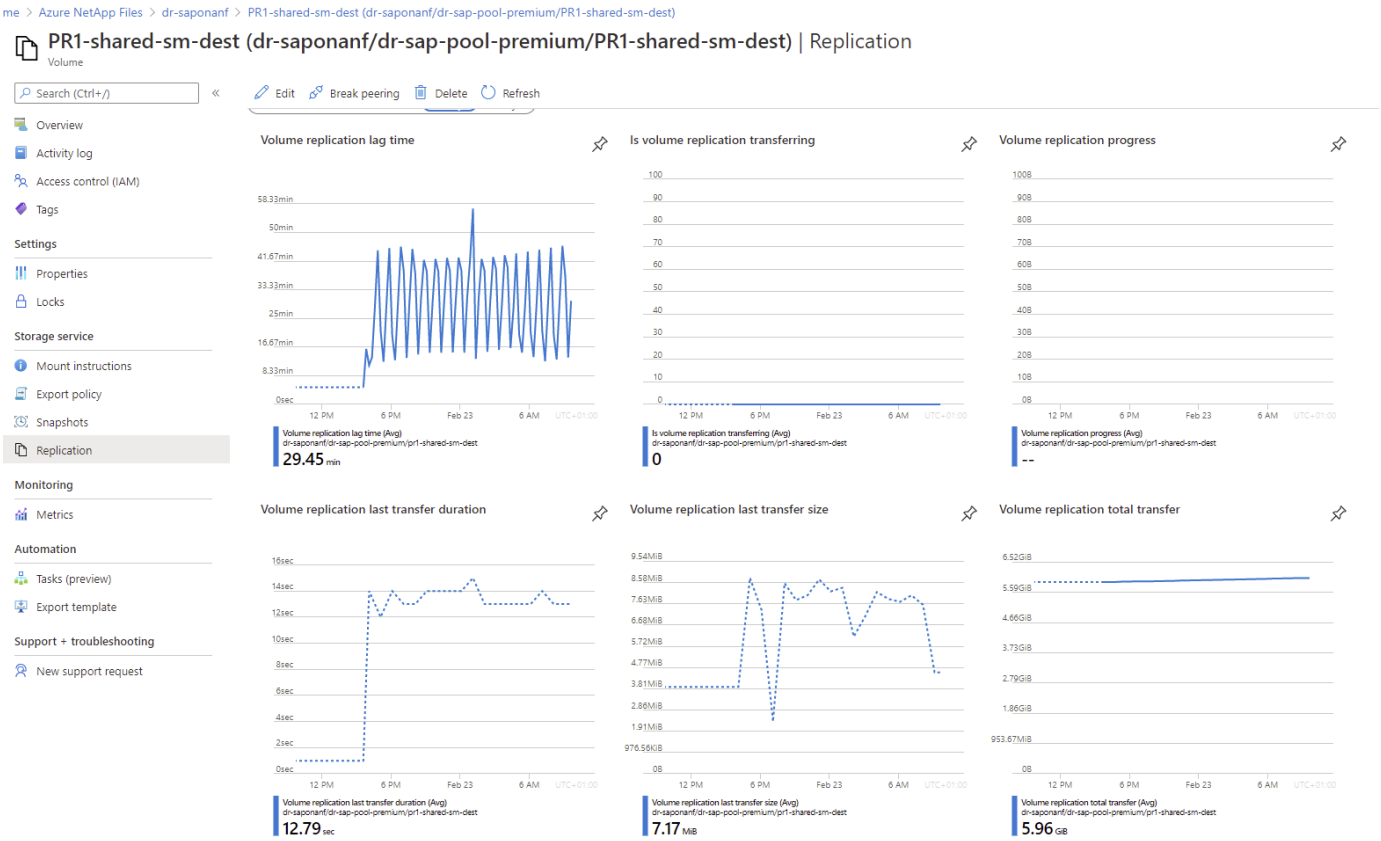
The following screenshot shows the replication status of HANA data volume.



The following screenshot shows the replication status of HANA log backup volume.



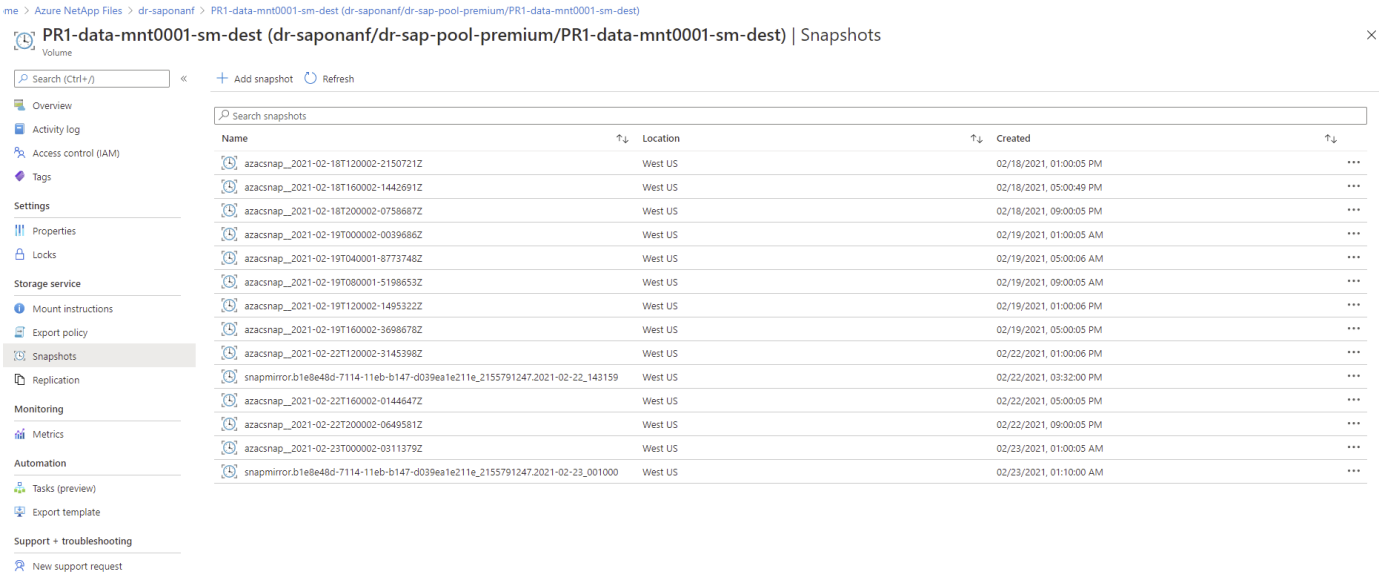
The following screenshot shows the replication status of HANA shared volume.



Replicated snapshot backups

With each replication update from the source to the target volume, all block changes that happened between the last and the current update are replicated to the target volume. This also includes the snapshots, which have been created at the source volume. The following screenshot shows the snapshots available at the target volume. As already discussed, each of the snapshots created by the AzAcSnap tool are application-consistent images of the HANA database that can be used to execute either a savepoint or a forward recovery.

Within the source and the target volume, SnapMirror Snapshot copies are created as well, which are used for resync and replication update operations. These Snapshot copies are not application consistent from the HANA database perspective; only the application-consistent snapshots created via AzaCSnap can be used for HANA recovery operations.



Next: Disaster recovery testing.

Disaster Recovery Testing

Previous: Monitoring ANF Cross-Region Replication.

To implement an effective disaster recovery strategy, you must test the required workflow. Testing demonstrates whether the strategy works and whether the internal documentation is sufficient, and it also allows administrators to train on the required procedures.

ANF Cross-Region Replication enables disaster recovery testing without putting RTO and RPO at risk. Disaster recovery testing can be done without interrupting data replication.

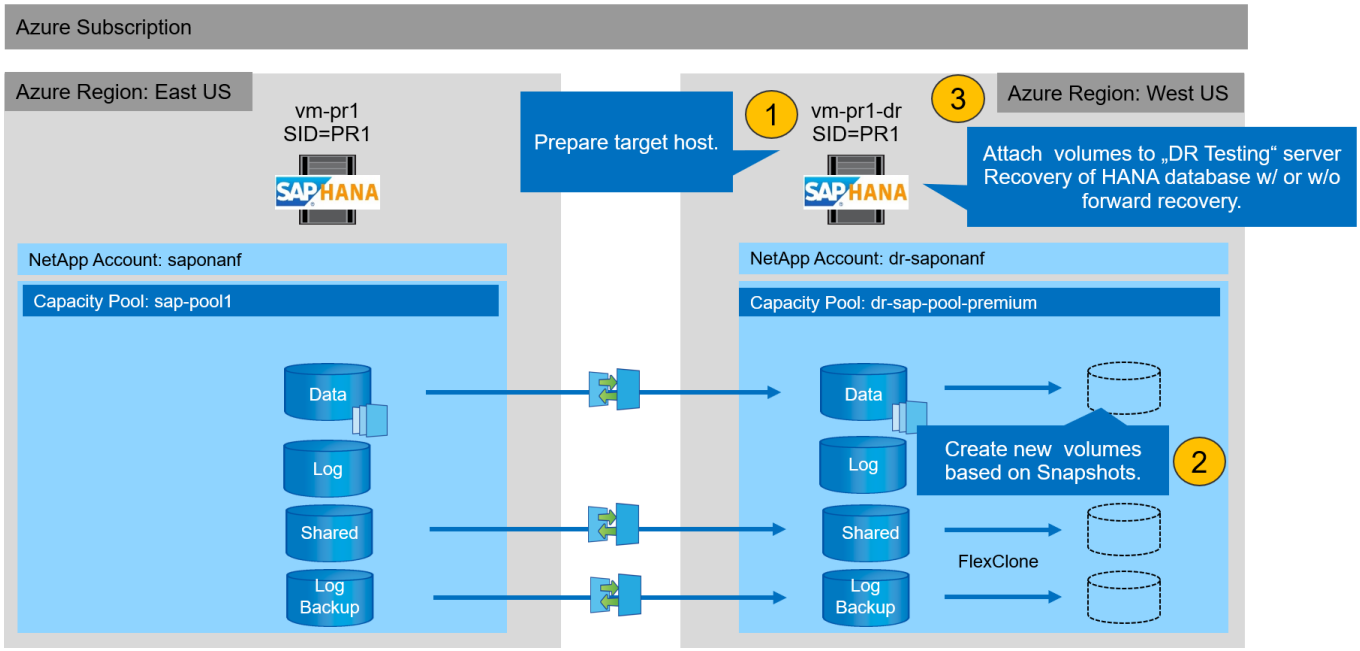
The disaster recovery testing workflow leverages the ANF feature set to create new volumes based on existing Snapshot backups at the disaster recovery target. See How Azure NetApp Files snapshots work | Microsoft Docs.

Depending on whether log backup replication is part of the disaster recovery setup or not, the steps for disaster recovery are slightly different. This section describes the disaster recovery testing for data-backup-only replication as well as for data volume replication combined with log backup volume replication.

To perform disaster recovery testing, complete the following steps:

1. Prepare the target host.
2. Create new volumes based on Snapshot backups at the disaster recovery site.
3. Mount the new volumes at the target host.
4. Recover the HANA database.
    - Data volume recovery only.
    - Forward recovery using replicated log backups.

The following subsections describe these steps in detail.



Next: Prepare the target host.

Prepare the target host

Previous: Disaster recovery testing.

This section describes the preparation steps required at the server, which is used for disaster recovery failover testing.

During normal operation, the target host is typically used for other purposes, for example as a HANA QA or test system. Therefore, most of these steps must be run when disaster failover testing is performed. On the other hand, the relevant configuration files, like `/etc/fstab` and `/usr/sap/sapservices`, can be prepared and then put into production by simply copying the configuration file. The disaster recovery testing procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system, as well as stopping all services using `systemctl stop sapinit`.

Target server host name and IP address

The host name of the target server must be identical to the host name of the source system. The IP address can be different.

Proper fencing of the target server must be established so that it cannot communicate with other systems. If proper fencing is not in place, then the cloned production system might exchange data with other production systems, resulting in logically corrupted data.

Install required software

The SAP host agent software must be installed at the target server. For more information, see the SAP Host Agent at the SAP help portal.

If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

Configure users, ports, and SAP services

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the `/etc/services` file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the `/usr/sap/sapservices` file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

Prepare HANA log volume

Because the HANA log volume is not part of the replication, an empty log volume must exist at the target host. The log volume must include the same subdirectories as the source HANA system.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Prepare log backup volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host. A volume for the log backups must be configured and mounted at the target host.

If log backup volume replication is part of the disaster recovery setup, a new volume based on a snapshot is mounted at the target host, and it is not necessary to prepare an additional log backup volume.

Prepare file system mounts

The following table shows the naming conventions used in the lab setup. The volume names of the new volumes at the disaster recovery site are included in `/etc/fstab`. These volume names are used in the

volume creation step in the next section.

HANA PR1 volumes	New volume and subdirectories at disaster recovery site	Mount point at target host
Data volume	PR1-data-mnt00001-sm-dest-clone	/hana/data/PR1/mnt00001
Shared volume	PR1-shared-sm-dest-clone/shared PR1-shared-sm-dest-clone/usr-sap-PR1	/hana/shared /usr/sap/PR1
Log backup volume	hanabackup-sm-dest-clone	/hanabackup

The mount points listed in this table must be created at the target host.

Here are the required `/etc/fstab` entries.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest-clone    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

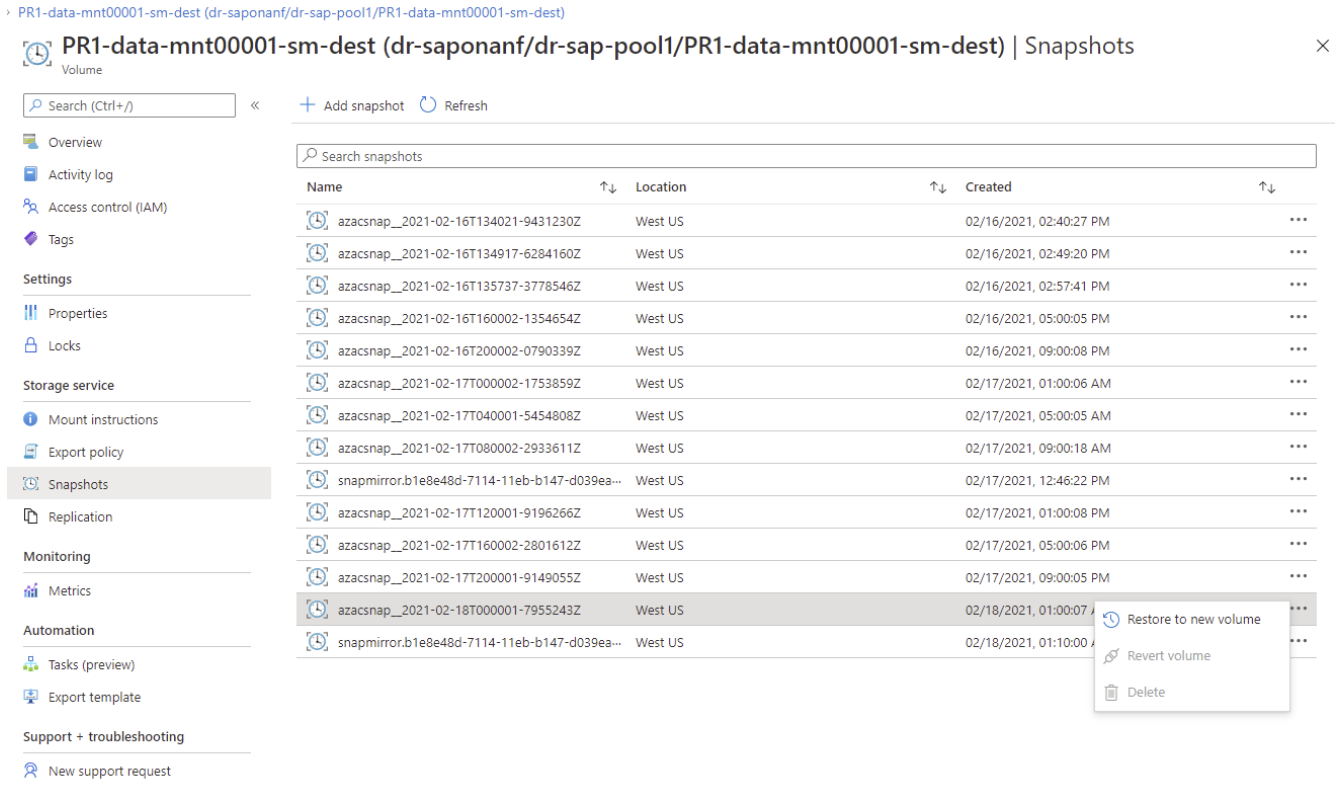
Next: Create new volumes based on snapshot backups at the disaster recovery site.

Create new volumes based on snapshot backups at the disaster recovery site

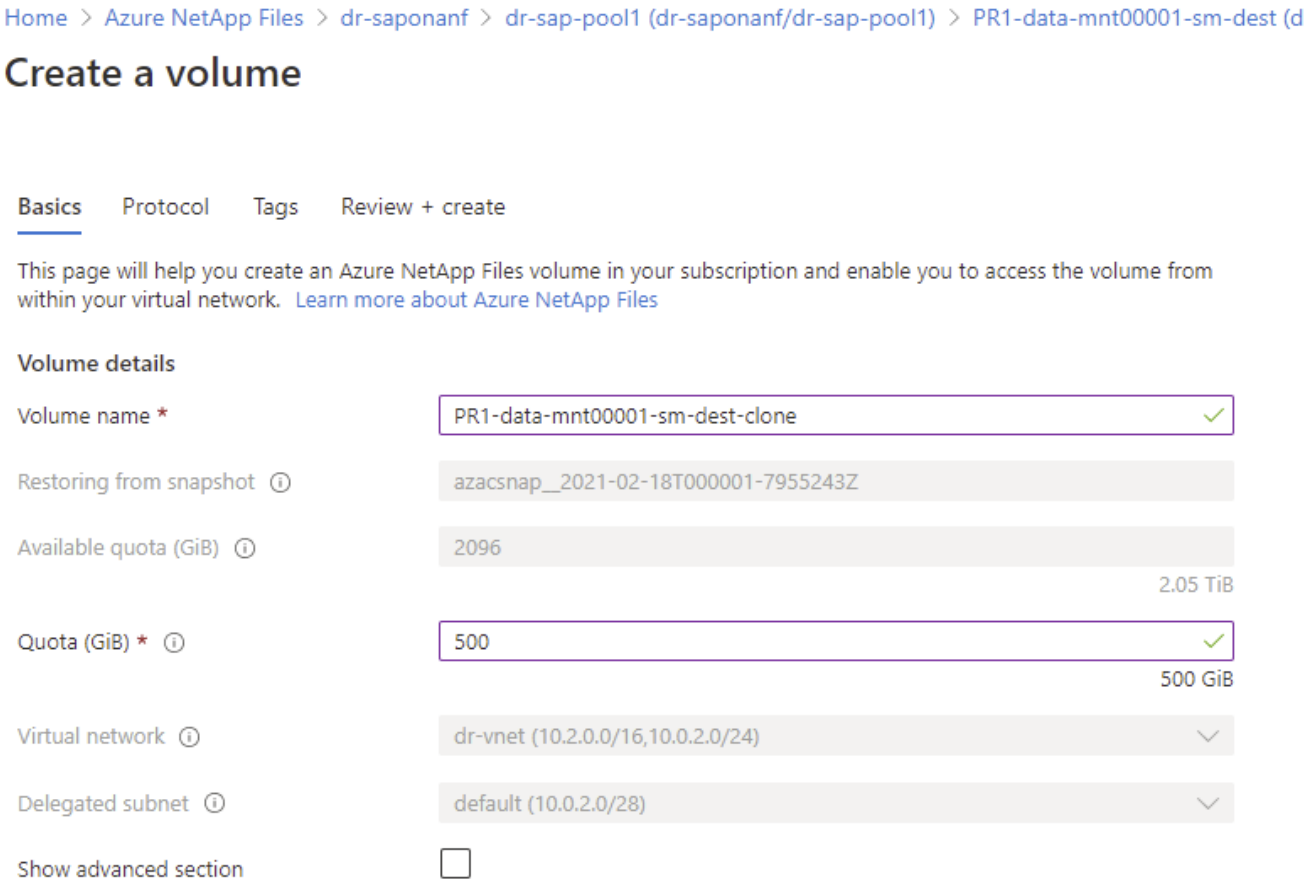
Previous: Prepare the target host.

Depending on the disaster recovery setup (with or without log backup replication), two or three new volumes based on snapshot backups must be created. In both cases, a new volume of the data and the HANA shared volume must be created. A new volume of the log backup volume must be created if the log backup data is also replicated. In our example, data and the log backup volume have been replicated to the disaster recovery site. The following steps use the Azure Portal.

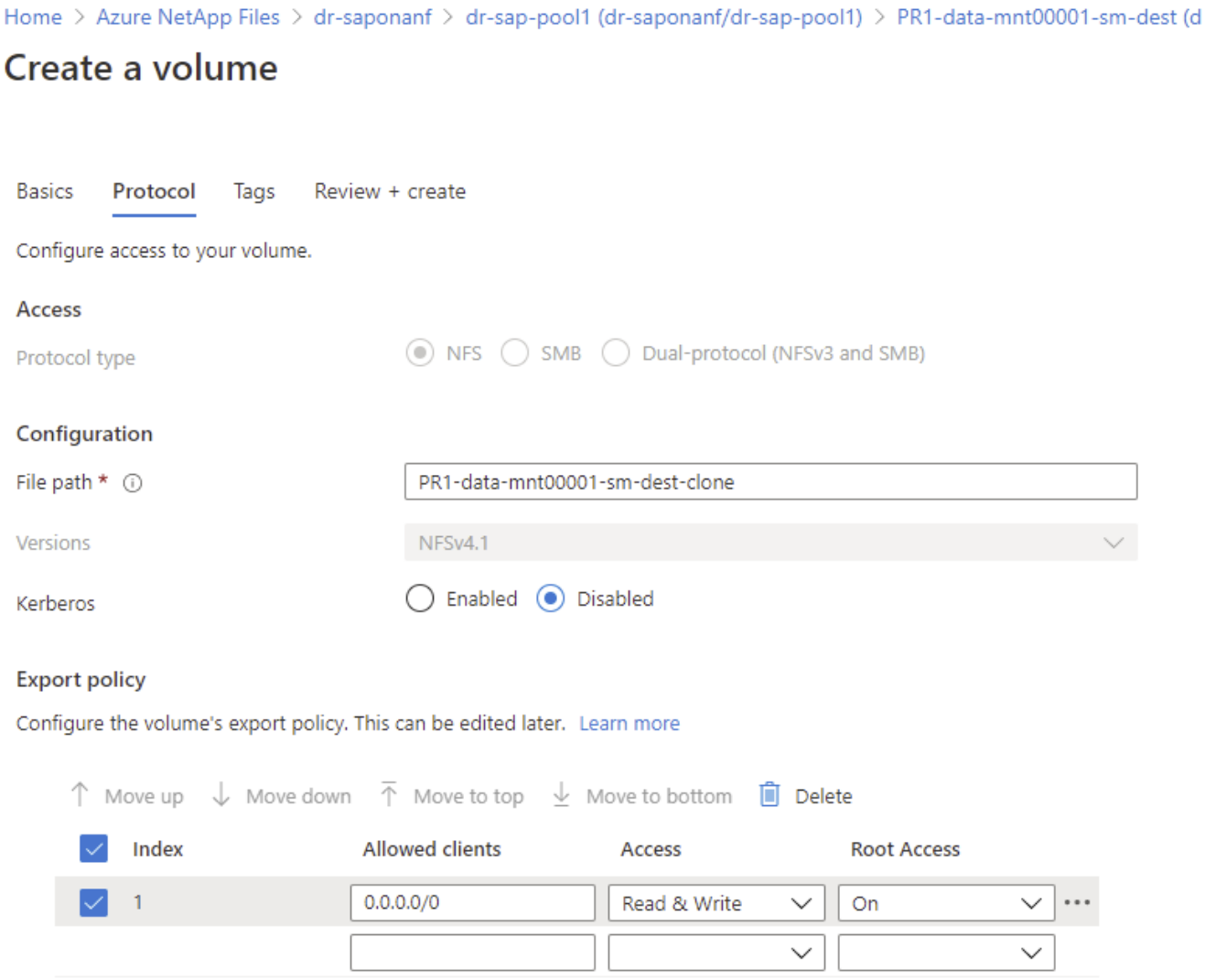
1. One of the application-consistent snapshot backups is selected as a source for the new volume of the HANA data volume. Restore to New Volume is selected to create a new volume based on the snapshot backup.



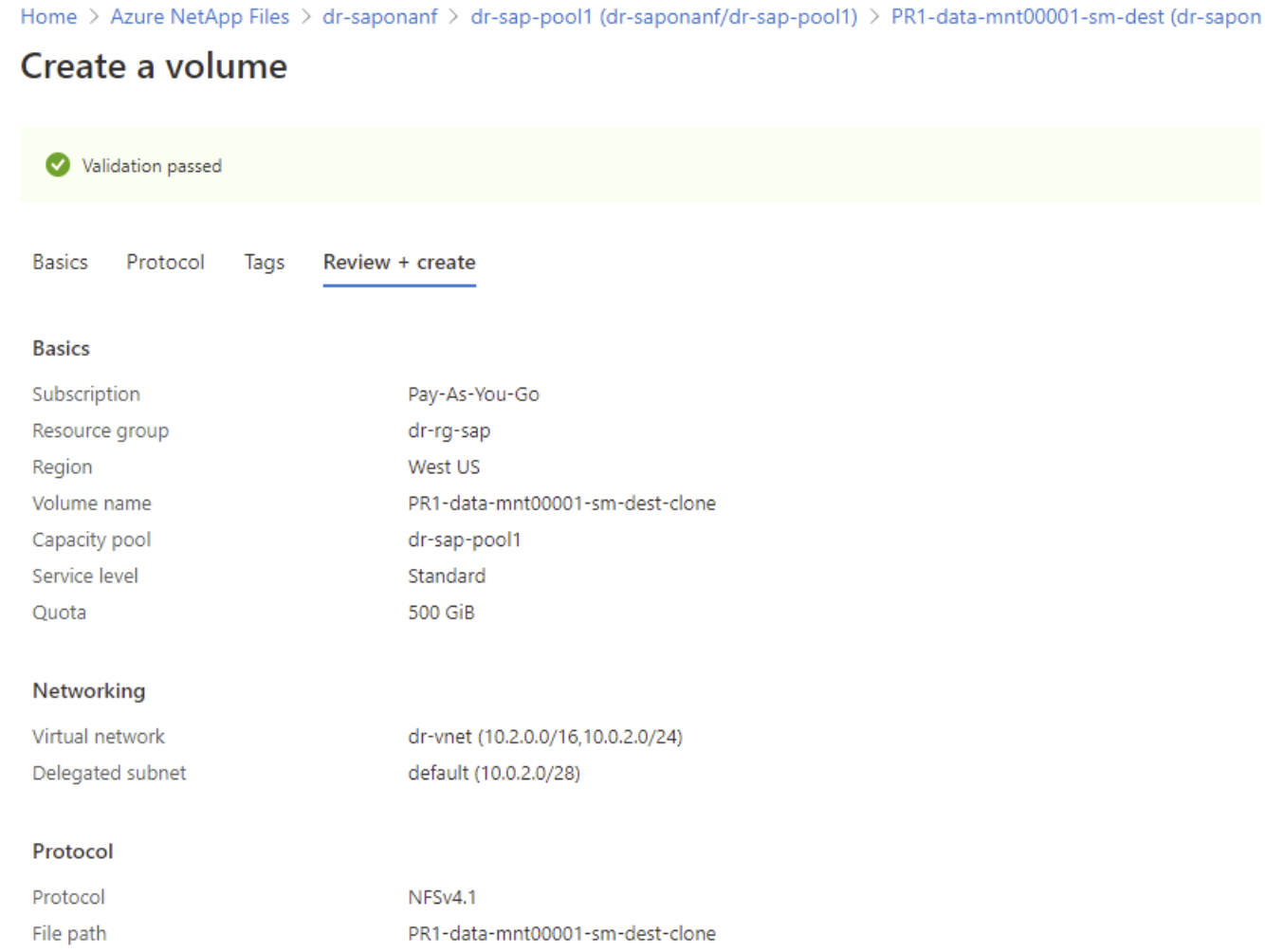
2. The new volume name and quota must be provided in the user interface.



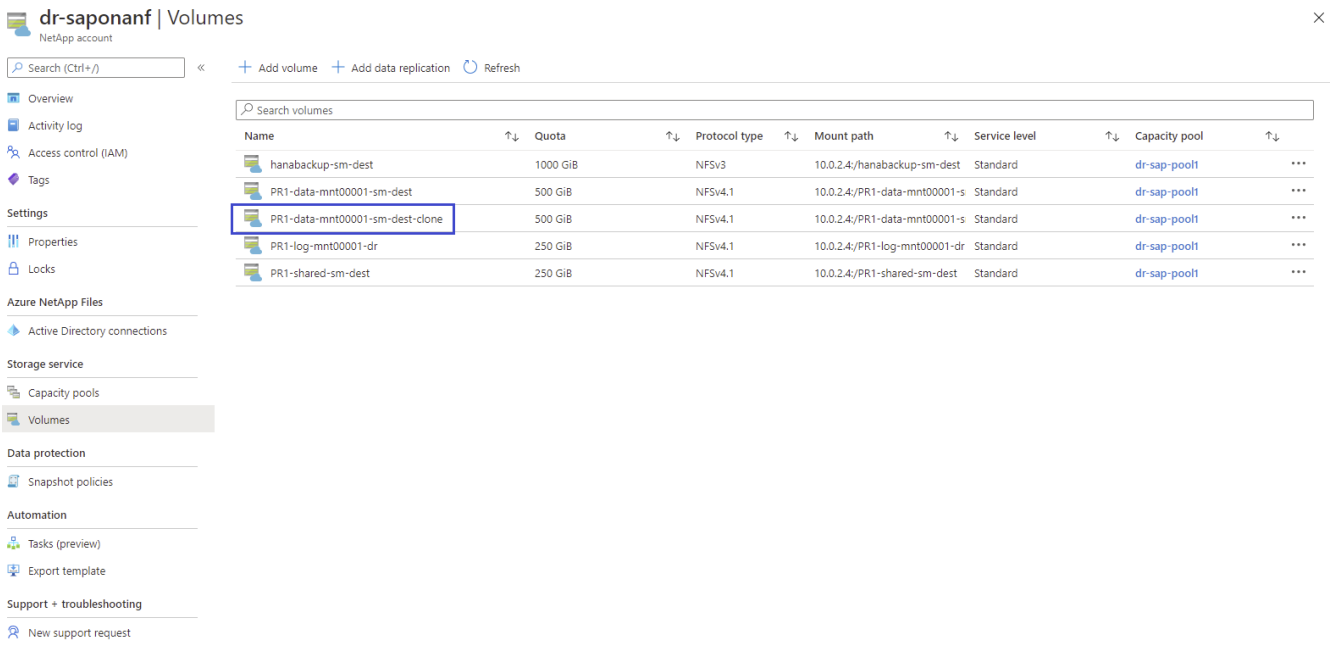
3. Within the protocol tab, the file path and export policy are configured.



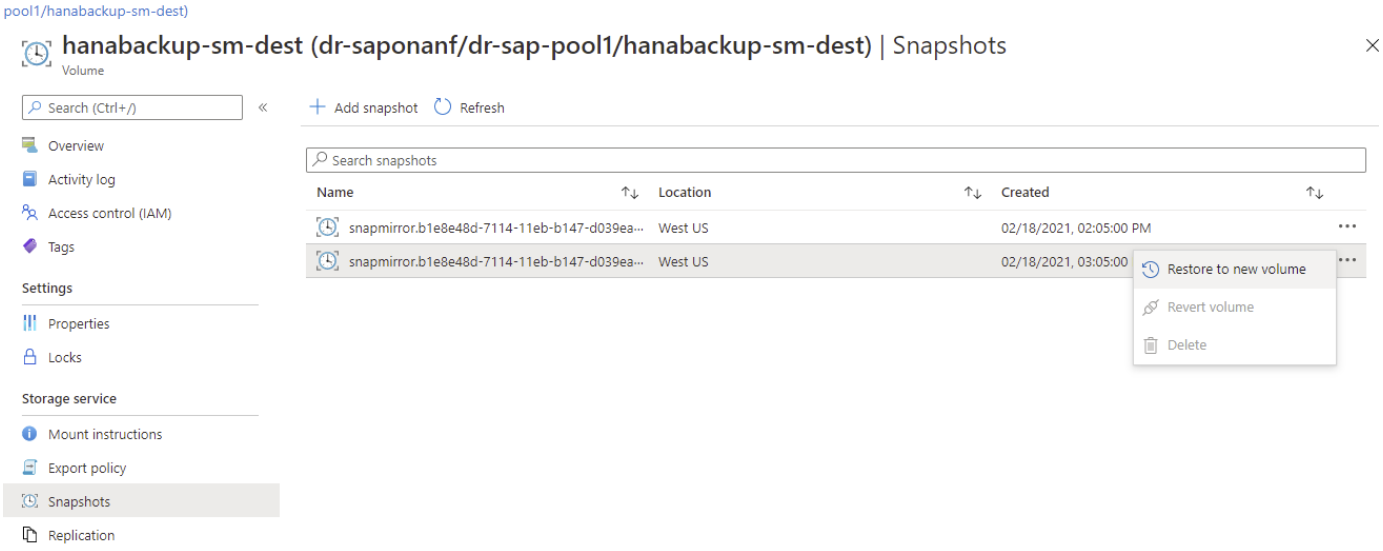
4. The Create and Review screen summarizes the configuration.



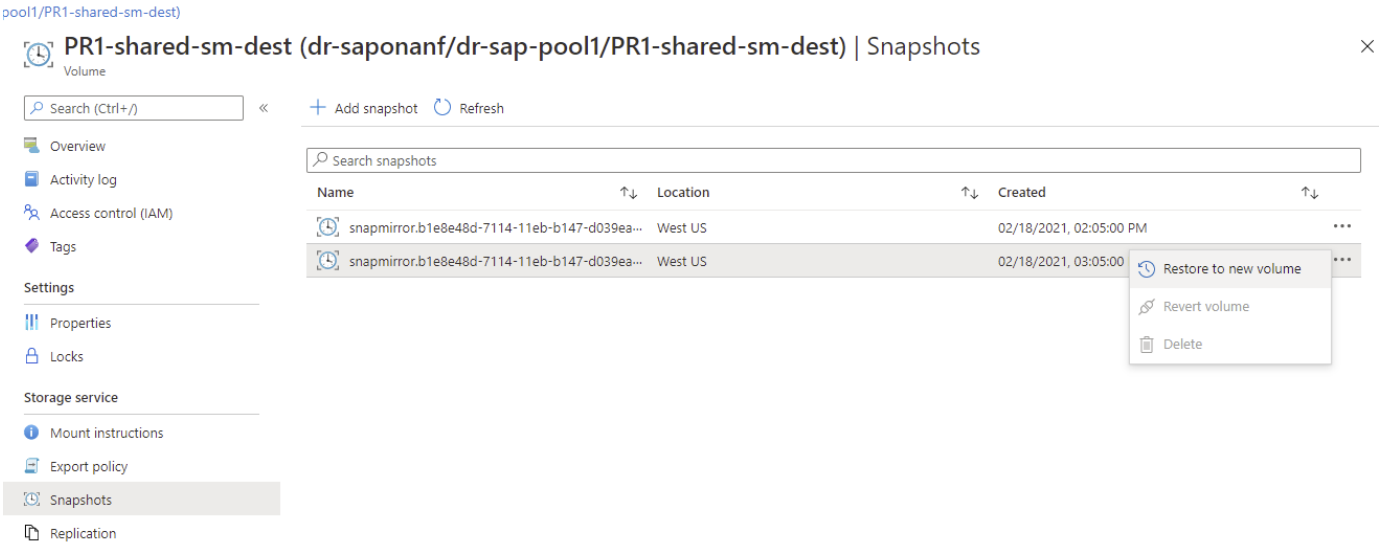
5. A new volume has now been created based on the HANA snapshot backup.



The same steps must now be performed for the HANA shared and the log backup volume as shown in the following two screenshots. Since no additional snapshots have been created for the HANA shared and log backup volume, the newest SnapMirror Snapshot copy must be selected as the source for the new volume. This is unstructured data, and the SnapMirror Snapshot copy can be used for this use case.



The following screenshot shows the HANA shared volume restored to new volume.



If a capacity pool with a low performance tier has been used, the volumes must now be moved to a capacity pool that provides the required performance.

All three new volumes are now available and can be mounted at the target host.

Next: Mount the new volumes at the target host.

Mount the new volumes at the target host

Previous: Create new volumes based on snapshot backups at the disaster recovery site.

The new volumes can now be mounted at the target host, based on the `/etc/fstab` file created before.

```
vm-pr1:~ # mount -a
```

The following output shows the required file systems.

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                          1K-blocks     Used
Available Use% Mounted on
devtmpfs                                              8190344        8
8190336   1% /dev
tmpfs                                                12313116        0
12313116   0% /dev/shm
tmpfs                                                 8208744    17292
8191452   1% /run
tmpfs                                                 8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                            29866736  2438052
27428684   9% /
/dev/sda3                                             1038336   101520
936816  10% /boot
/dev/sda2                                              524008     1072
522936   1% /boot/efi
/dev/sdb1                                            32894736    49176
31151560   1% /mnt
tmpfs                                                 1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr                    107374182400      256
107374182144   1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone         107377026560  6672640
107370353920   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone               107379429120 35293440
107344135680   1% /hanabackup
```

Next: HANA database recovery.

HANA database recovery

Previous: Mount the volumes at the target host.

Start the required SAP services.

```
vm-pr1:~ # systemctl start sapinit
```

The following output shows the required processes.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

The following subsections describe the recovery process with and without forward recovery using the replicated log backups. The recovery is executed using the HANA recovery script for the system database and hdbsql commands for the tenant database.

Recovery to latest HANA data volume backup savepoint

The recovery to the latest backup savepoint is executed with the following commands as user pr1adm:

- System database

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Tenant database

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

You can also use HANA Studio or Cockpit to execute the recovery of the system and the tenant database.

The following command output show the recovery execution.

System database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Tenant database recovery

If a user store key has not been created for the pr1adm user at the source system, a key must be created at the target system. The database user configured in the key must have privileges to execute tenant recovery operations.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

The tenant recovery is now executed with hdbsql.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

The HANA database is now up and running, and the disaster recovery workflow for the HANA database has been tested.

Recovery with forward recovery using log/catalog backups

Log backups and the HANA backup catalog are being replicated from the source system.

The recovery using all available log backups is executed with the following commands as user pr1adm:

- System database

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Tenant database

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

To recover using all available logs, you can just use any time in the future as the timestamp in the recovery statement.

You can also use HANA Studio or Cockpit to execute the recovery of the system and the tenant database.

The following command output show the recovery execution.

System database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Tenant database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)
hdbsql SYSTEMDB=>
```

The HANA database is now up and running, and the disaster recovery workflow for the HANA database has been tested.

Check consistency of latest log backups

Because log backup volume replication is performed independently of the log backup process executed by the SAP HANA database, there might be open, inconsistent log backup files at the disaster recovery site. Only the latest log backup files might be inconsistent, and those files should be checked before a forward recovery is performed at the disaster recovery site using the `hdbbackupcheck` tool.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or deleted.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

The check must be executed for the latest log backup files of the system and the tenant database.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or deleted.

Disaster recovery failover

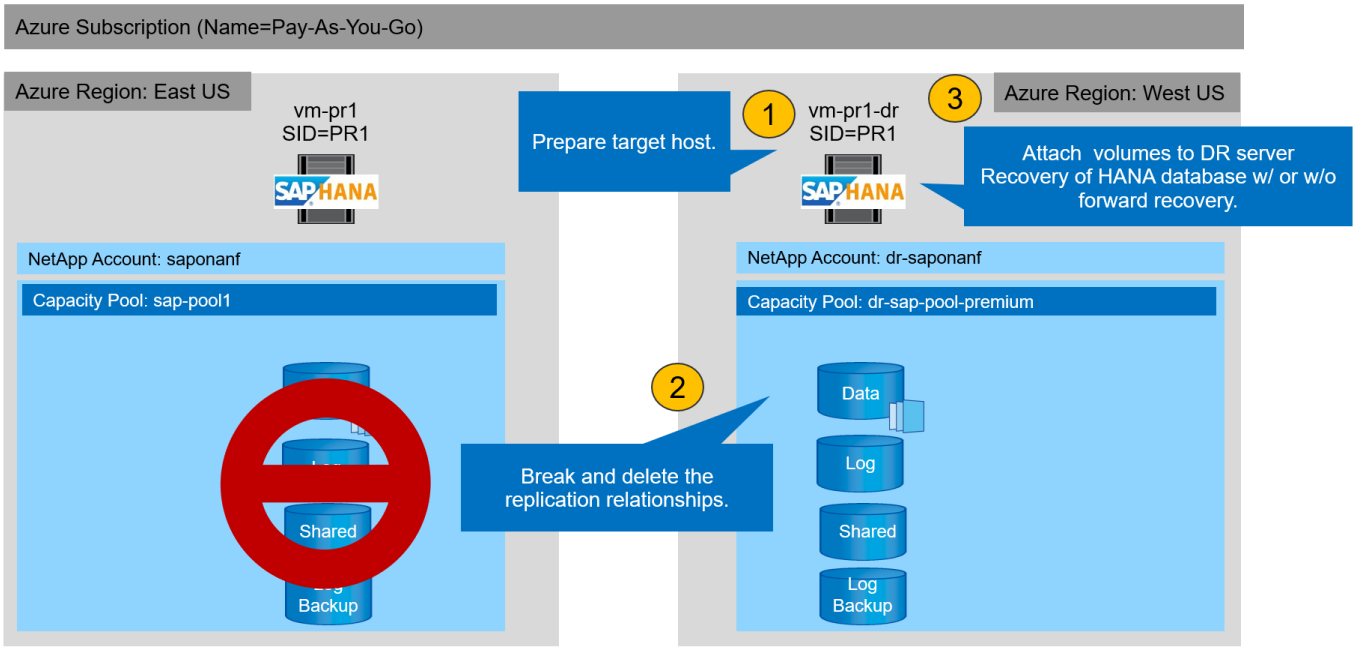
Previous: HANA database recovery.

Depending on whether the log backup replication is part of the disaster recovery setup, the steps for disaster recovery are slightly different. This section describes the disaster recovery failover for data-backup-only replication as well as for data volume replication combined with log backup volume replication.

To execute disaster recovery failover, complete these steps:

1. Prepare the target host.
2. Break and delete the replication relationships.
3. Restore the data volume to the latest application- consistent snapshot backup.
4. Mount the volumes at the target host.
5. Recover the HANA database.
    - Data volume recovery only.
    - Forward recovery using replicated log backups.

The following subsections describe these steps in detail, and the following figure depicts disaster failover testing.



Next: Prepare the target host.

Prepare the target host

Previous: Disaster recovery failover.

This section describes the preparation steps required at the server that is used for the disaster recovery failover.

During normal operation, the target host is typically used for other purposes, for example, as a HANA QA or test system. Therefore, most of the described steps must be executed when disaster failover testing is executed. On the other hand, the relevant configuration files, like `/etc/fstab` and `/usr/sap/sapservices`, can be prepared and then put in production by simply copying the configuration file. The disaster recovery failover procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system as well as stopping all services using `systemctl stop sapinit`.

Target server host name and IP address

The host name of the target server must be identical to the host name of the source system. The IP address can be different.

Proper fencing of the target server must be established so that it cannot communicate with other systems. If proper fencing is not in place, then the cloned production system might exchange data with other production systems, resulting in logically corrupted data.

Install required software

The SAP host agent software must be installed at the target server. For full information, see the SAP Host Agent at the SAP help portal.

If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

Configure users, ports, and SAP services

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the `/etc/services` file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the `/usr/sap/sapservices` file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

Prepare HANA log volume

Because the HANA log volume is not part of the replication, an empty log volume must exist at the target host. The log volume must include the same subdirectories as the source HANA system.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Prepare log backup volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host. A volume for the log backups must be configured and mounted at the target host.

If log backup volume replication is part of the disaster recovery setup, the replicated log backup volume is mounted at the target host, and it is not necessary to prepare an additional log backup volume.

Prepare file system mounts

The following table shows the naming conventions used in the lab setup. The volume names at the disaster recovery site are included in `/etc/fstab`.

HANA PR1 volumes	Volume and subdirectories at disaster recovery site	Mount point at target host
Data volume	PR1-data-mnt00001-sm-dest	/hana/data/PR1/mnt00001
Shared volume	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Log backup volume	hanabackup-sm-dest	/hanabackup

The mount points from this table must be created at the target host.

Here are the required `/etc/fstab` entries.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

Next: Break and delete replication peering.

Break and delete replication peering

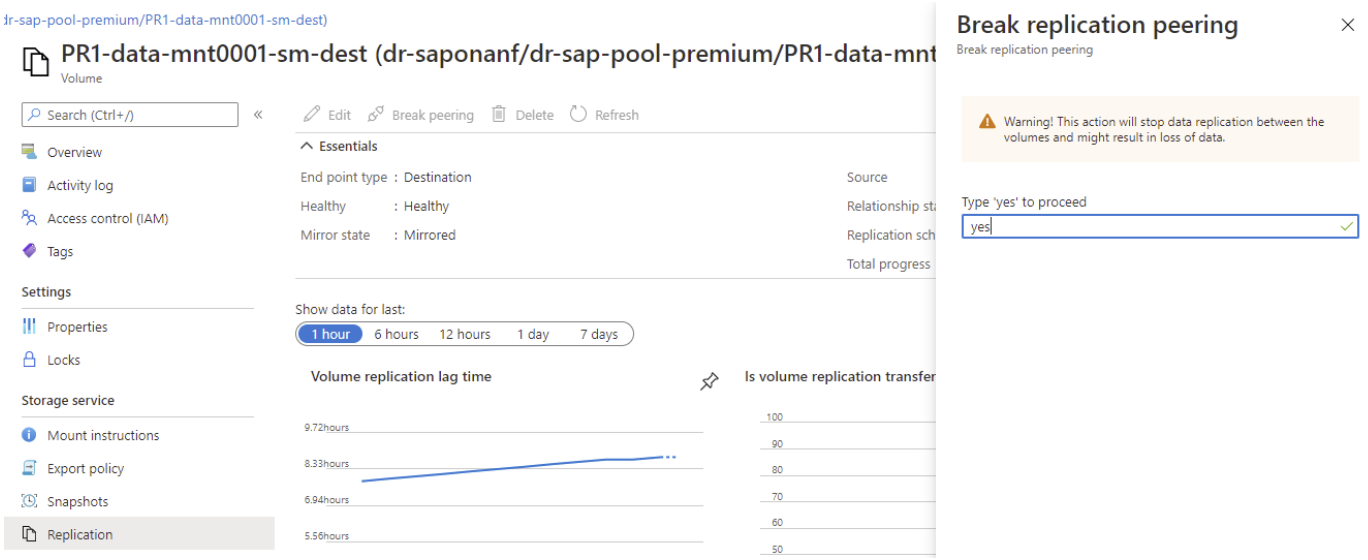
Previous: Prepare the target host.

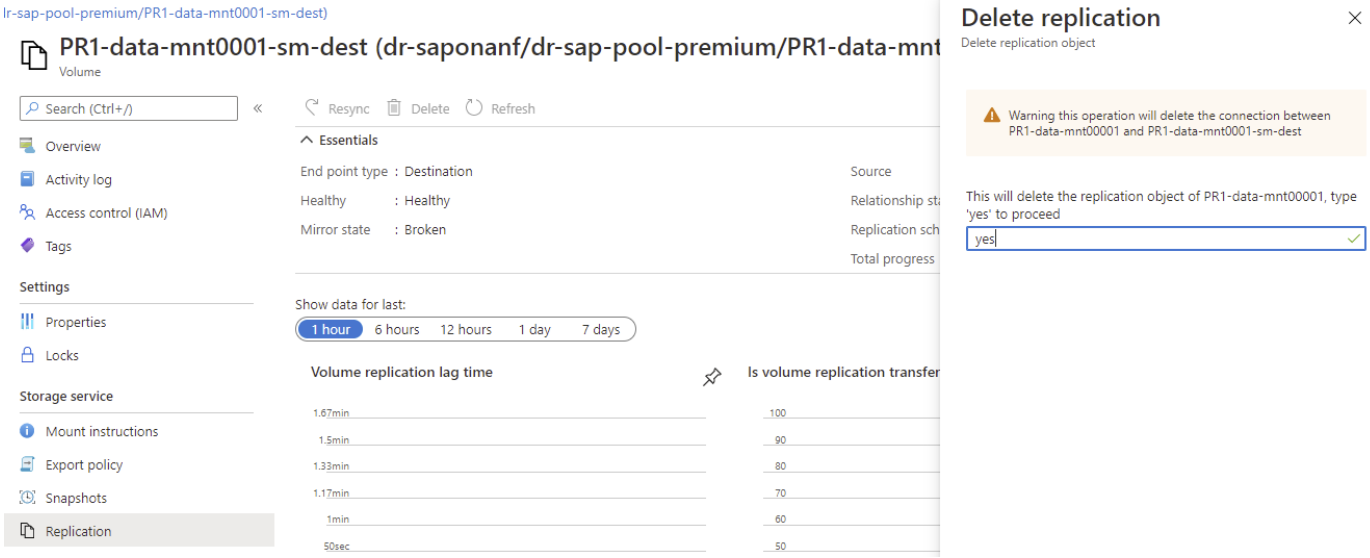
In case of a disaster failover, the target volumes must be broken off so that the target host can mount the volumes for read and write operations.

For the HANA data volume, you must restore the volume to the latest HANA snapshot backup created with AzAcSnap. This volume revert operation is not possible if the latest replication snapshot is marked as busy due to the replication peering. Therefore, you must also delete the replication peering.

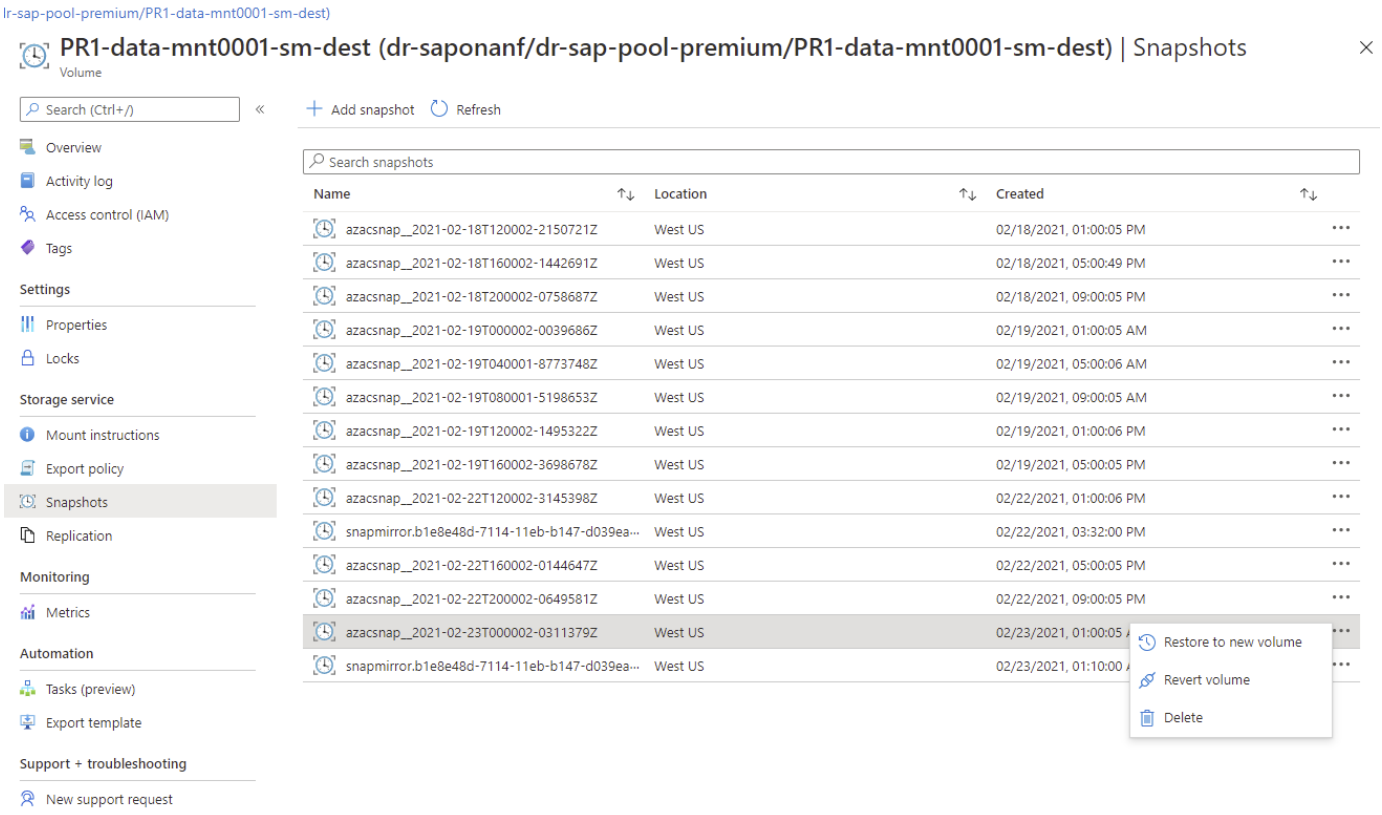
The next two screenshots show the break and delete peering operation for the HANA data volume. The same

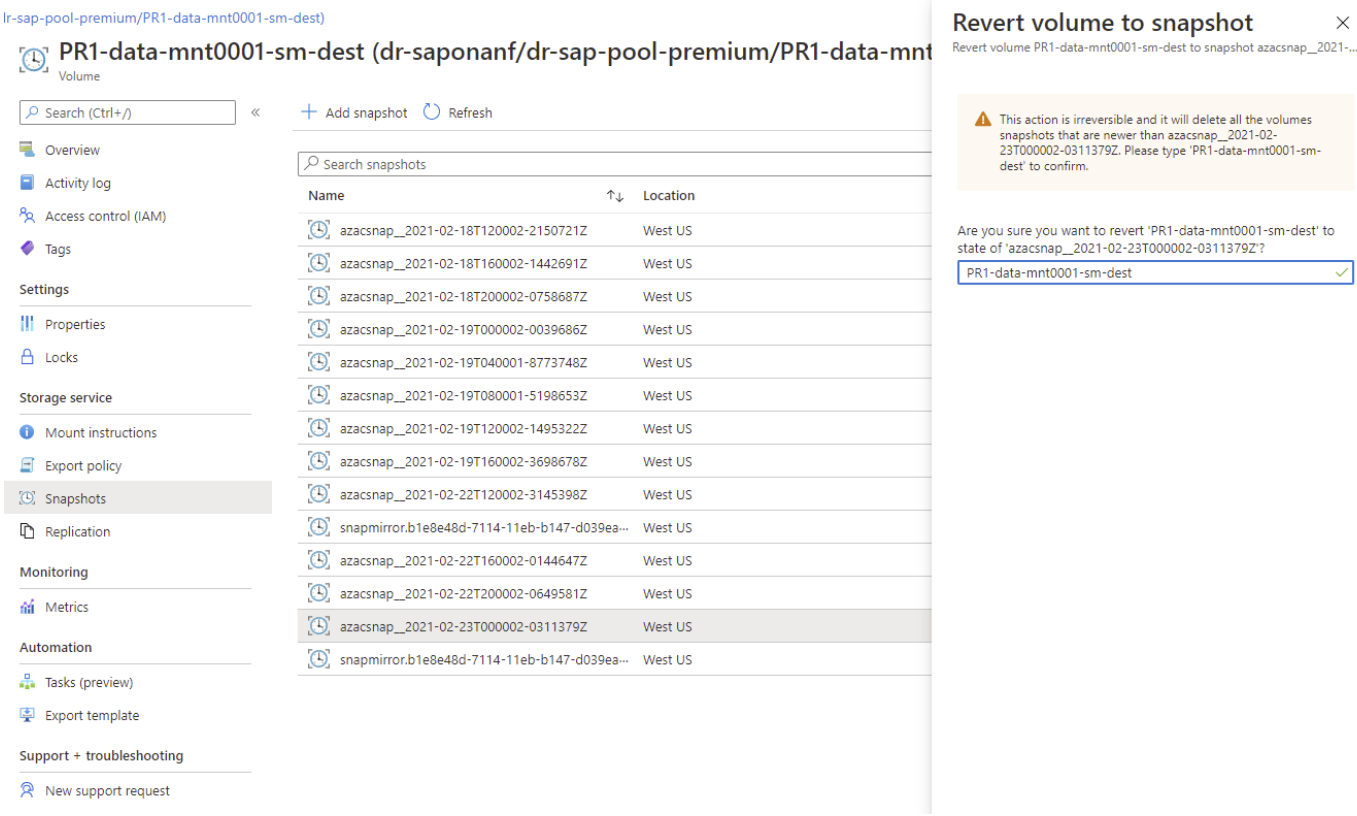
operations must be performed for the log backup and the HANA shared volume as well.





Since replication peering was deleted, it is possible to revert the volume to the latest HANA snapshot backup. If peering is not deleted, the selection of revert volume is grayed out and is not selectable. The following two screenshots show the volume revert operation.





After the volume revert operation, the data volume is based on the consistent HANA snapshot backup and can now be used to execute forward recovery operations.

If a capacity pool with a low performance tier has been used, the volumes must now be moved to a capacity pool that can provide the required performance.

Next: Mount the volumes at the target host.

Mount the volumes at the target host

Previous: Break and delete replication peering.

The volumes can now be mounted at the target host, based on the `/etc/fstab` file created before.

```
vm-pr1:~ # mount -a
```

The following output shows the required file systems.

```
vm-pr1:~ # df
Filesystem                                      1K-blocks     Used
Available Use% Mounted on
devtmpfs                                          8201112        0
8201112   0% /dev
tmpfs                                            12313116        0
12313116   0% /dev/shm
tmpfs                                             8208744     9096
8199648   1% /run
tmpfs                                             8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                        29866736  2543948
27322788   9% /
/dev/sda3                                         1038336    79984
958352   8% /boot
/dev/sda2                                          524008     1072
522936   1% /boot/efi
/dev/sdb1                                        32894736    49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr                107374182400     6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                             1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared 107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest                 107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest           107376511232  6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #
```

Next: HANA database recovery.

HANA database recovery

Previous: Mount the volumes at the target host.

Start the required SAP services.

```
vm-pr1:~ # systemctl start sapinit
```

The following output shows the required processes.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

The following subsections describe the recovery process with forward recovery using the replicated log backups. The recovery is executed using the HANA recovery script for the system database and hdbsql commands for the tenant database.

The commands to execute a recovery to the latest data savepoint is described in chapter Recovery to latest HANA Data Volume Backup Savepoint.

Recovery with forward recovery using log backups

The recovery using all available log backups is executed with the following commands as user pr1adm:

- System database

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Tenant database

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

To recover using all available logs, you can use any time in the future as the timestamp in the recovery statement.

You can also use HANA Studio or Cockpit to execute the recovery of the system and the tenant database.

The following command output show the recovery execution.

System database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING
SNAPSHOT"
[139792805873472, 0.008] >> starting recoverSys (at Tue Feb 23 12:05:16
2021)
[139792805873472, 0.008] args: ()
[139792805873472, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-23 12:05:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-23 12:05:17
stopped system: 2021-02-23 12:05:18
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-23 12:05:23
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-23T12:07:53+00:00  P0012969      177cec93d51 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
23T09:03:11+00:00, reached log position 43123520
recoverSys finished successfully: 2021-02-23 12:07:54
[139792805873472, 157.466] 0
[139792805873472, 157.466] << ending recoverSys, rc = 0 (RC_TEST_OK),
after 157.458 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Tenant database recovery

If a user store key has not been created for the pr1adm user at the source system, a key must be created at the target system. The database user configured in the key must have privileges to execute tenant recovery operations.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-24
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 98.740038 sec; server time 98.737788 sec)
hdbsql SYSTEMDB=>
```

Check consistency of latest log backups

Because log backup volume replication is performed independently of the log backup process executed by the SAP HANA database, there might be open, inconsistent log backup files at the disaster recovery site. Only the latest log backup files might be inconsistent, and those files should be checked before a forward recovery is performed at the disaster recovery site using the `hdbbackupcheck` tool.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

The check must be executed for the latest log backup files of the System and the tenant database.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or deleted.

SAP Lifecycle Management

Solution Briefs

Oracle Database

Deploying Oracle Database

Solution Overview

Automated Deployment of Oracle19c for ONTAP on NFS

Organizations are automating their environments to gain efficiencies, accelerate deployments, and reduce manual effort. Configuration management tools like Ansible are being used to streamline enterprise database operations. In this solution, we demonstrate how you can use Ansible to automate the provisioning and configuration of Oracle 19c with NetApp ONTAP. By enabling storage administrators, systems administrators, and DBAs to consistently and rapidly deploy new storage, configure database servers, and install Oracle 19c software, you achieve the following benefits:

- Eliminate design complexities and human errors, and implement a repeatable consistent deployment and best practices
- Decrease time for provisioning of storage, configuration of DB hosts, and Oracle installation
- Increase database administrators, systems and storage administrators productivity
- Enable scaling of storage and databases with ease

NetApp provides customers with validated Ansible modules and roles to accelerate deployment, configuration, and lifecycle management of your Oracle database environment. This solution provides instruction and Ansible playbook code, to help you:

- Create and configure ONTAP NFS storage for Oracle Database
- Install Oracle 19c on RedHat Enterprise Linux 7/8 or Oracle Linux 7/8
- Configure Oracle 19c on ONTAP NFS storage

For more details or to begin, please see the overview videos below.

AWX/Tower Deployments

- Part 1: Getting Started, Requirements, Automation Details and Initial AWX/Tower Configuration

▶ https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v1.mp4 *(video)*

- Part 2: Variables and Running the Playbook

▶ https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v2.mp4 *(video)*

CLI Deployment

- Part 1: Getting Started, Requirements, Automation Details and Ansible Control Host Setup

▶ https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v4.mp4 *(video)*

- Part 2: Variables and Running the Playbook

▶ https://docs.netapp.com/us-en/netapp-solutions/media/oracle3.mp4 *(video)*

Getting started

This solution has been designed to be run in an AWX/Tower environment or by CLI on an Ansible control host.

AWX/Tower

For AWX/Tower environments, you are guided through creating an inventory of your ONTAP cluster management and Oracle server (IPs and hostnames), creating credentials, configuring a project that pulls the Ansible code from NetApp Automation Github, and the Job Template that launches the automation.

1. Fill out the variables specific to your environment, and copy and paste them into the Extra Vars fields in your job template.
2. After the extra vars have been added to your job template, you can launch the automation.
3. The job template is run in three phases by specifying tags for ontap_config, linux_config, and

oracle_config.

CLI via the Ansible control host

1. To configure the Linux host so that is can be used as an Ansible control host
   click here for RHEL 7/8 or CentOS 7/8, or
   here for Ubuntu/Debian
2. After the Ansible control host is configured, you can git clone the Ansible Automation repository.
3. Edit the hosts file with the IPs and/or hostnames of your ONTAP cluster management and Oracle server's management IPs.
4. Fill out the variables specific to your environment, and copy and paste them into the `vars.yml` file.
5. Each Oracle host has a variable file identified by its hostname that contains host-specific variables.
6. After all variable files have been completed, you can run the playbook in three phases by specifying tags for `ontap_config`, `linux_config`, and `oracle_config`.

Requirements

Environment	Requirements
Ansible environment	AWX/Tower or Linux host to be the Ansible control host
	Ansible v.2.10 and higher
	Python 3
	Python libraries - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP version 9.3 - 9.7
	Two data aggregates
	NFS vlan and ifgrp created
Oracle server(s)	RHEL 7/8
	Oracle Linux 7/8
	Network interfaces for NFS, public, and optional mgmt
	Oracle installation files on Oracle servers

Automation Details

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations.
The following table describes which tasks are being automated.

Role	Tasks
ontap_config	Pre-check of the ONTAP environment
	Creation of NFS based SVM for Oracle
	Creation of export policy
	Creation of volumes for Oracle
	Creation of NFS LIFs
linux_config	Create mount points and mount NFS volumes
	Verify NFS mounts
	OS specific configuration
	Create Oracle directories
	Configure hugepages
	Disable SELinux and firewall daemon
	Enable and start chronyd service
	increase file descriptor hard limit
	Create pam.d session file
oracle_config	Oracle software installation
	Create Oracle listener
	Create Oracle databases
	Oracle environment configuration
	Save PDB state
	Enable instance archive mode
	Enable DNFS client
	Enable database auto startup and shutdown between OS reboots

Default parameters

To simplify automation, we have preset many required Oracle deployment parameters with default values. It is generally not necessary to change the default parameters for most deployments. A more advanced user can make changes to the default parameters with caution. The default parameters are located in each role folder under defaults directory.

Deployment instructions

Before starting, download the following Oracle installation and patch files and place them in the `/tmp/archive` directory with read, write, and execute access for all users on each DB server to be deployed. The automation tasks look for the named installation files in that particular directory for Oracle installation and configuration.

```
LINUX.X64_193000_db_home.zip -- 19.3 base installer
p31281355_190000_Linux-x86-64.zip -- 19.8 RU patch
p6880880_190000_Linux-x86-64.zip -- opatch version 12.2.0.1.23
```

License

You should read license information as stated in the Github repository. By accessing, downloading, installing, or using the content in this repository, you agree the terms of the license laid out here.

Note that there are certain restrictions around producing and/or sharing any derivative works with the content in this repository. Please make sure you read the terms of the License before using the content. If you do not agree to all of the terms, do not access, download, or use the content in this repository.

After you are ready, click here for detailed AWX/Tower deployment procedures or here for CLI deployment.

Step-by-step deployment procedure

AWX/Tower deployment Oracle 19c Database

1. Create the inventory, group, hosts, and credentials for your environment

This section describes the setup of inventory, groups, hosts, and access credentials in AWX/Ansible Tower that prepare the environment for consuming NetApp automated solutions.

1. Configure the inventory.
    a. Navigate to Resources → Inventories → Add, and click Add Inventory.
    b. Provide the name and organization details, and click Save.
    c. On the Inventories page, click the inventory created.
    d. If there are any inventory variables, paste them in the variables field.
    e. Navigate to the Groups sub-menu and click Add.
    f. Provide the name of the group for ONTAP, paste the group variables (if any) and click Save.
    g. Repeat the process for another group for Oracle.
    h. Select the ONTAP group created, go to the Hosts sub-menu and click Add New Host.
    i. Provide the IP address of the ONTAP cluster management IP, paste the host variables (if any), and click Save.
    j. This process must be repeated for the Oracle group and Oracle host(s) management IP/hostname.
2. Create credential types. For solutions involving ONTAP, you must configure the credential type to match username and password entries.
    a. Navigate to Administration → Credential Types, and click Add.
    b. Provide the name and description.
    c. Paste the following content in Input Configuration:

```
fields:
  - id: username
    type: string
    label: Username
  - id: password
    type: string
    label: Password
    secret: true
  - id: vsadmin_password
    type: string
    label: vsadmin_password
    secret: true
```

d. Paste the following content into Injector Configuration:

```
extra_vars:
  password: '{{ password }}'
  username: '{{ username }}'
  vsadmin_password: '{{ vsadmin_password }}'
```

3. Configure the credentials.
   a. Navigate to Resources → Credentials, and click Add.
   b. Enter the name and organization details for ONTAP.
   c. Select the custom Credential Type you created for ONTAP.
   d. Under Type Details, enter the username, password, and vsadmin_password.
   e. Click Back to Credential and click Add.
   f. Enter the name and organization details for Oracle.
   g. Select the Machine credential type.
   h. Under Type Details, enter the Username and Password for the Oracle hosts.
   i. Select the correct Privilege Escalation Method, and enter the username and password.

2. Create a project

1. Go to Resources → Projects, and click Add.
   a. Enter the name and organization details.
   b. Select Git in the Source Control Credential Type field.
   c. enter https://github.com/NetApp-Automation/na_oracle19c_deploy.git as the source control URL.
   d. Click Save.
   e. The project might need to sync occasionally when the source code changes.

3. Configure Oracle host_vars

The variables defined in this section are applied to each individual Oracle server and database.

1. Input your environment-specific parameters in the following embedded Oracle hosts variables or host_vars form.

   The items in blue must be changed to match your environment.

Unresolved directive in ent-apps-db/awx_automation.adoc - include::ent-apps-db/host_vars.adoc[]

a. Fill in all variables in the blue fields.
b. After completing variables input, click the Copy button on the form to copy all variables to be transferred to AWX or Tower.
c. Navigate back to AWX or Tower and go to Resources → Hosts, and select and open the Oracle server configuration page.
d. Under the Details tab, click edit and paste the copied variables from step 1 to the Variables field under the YAML tab.
e. Click Save.
f. Repeat this process for any additional Oracle servers in the system.

4. Configure global variables

Variables defined in this section apply to all Oracle hosts, databases, and the ONTAP cluster.

1. Input your environment-specific parameters in following embedded global variables or vars form.

   The items in blue must be changed to match your environment.

   Unresolved directive in ent-apps-db/awx_automation.adoc - include::ent-apps-db/vars.adoc[]

2. Fill in all variables in blue fields.
3. After completing variables input, click the Copy button on the form to copy all variables to be transferred to AWX or Tower into the following job template.

5. Configure and launch the job template.

1. Create the job template.
   a. Navigate to Resources → Templates → Add and click Add Job Template.
   b. Enter the name and description
   c. Select the Job type; Run configures the system based on a playbook, and Check performs a dry run of a playbook without actually configuring the system.
   d. Select the corresponding inventory, project, playbook, and credentials for the playbook.
   e. Select the all_playbook.yml as the default playbook to be executed.
   f. Paste global variables copied from step 4 into the Template Variables field under the YAML tab.
   g. Check the box Prompt on Launch in the Job Tags field.
   h. Click Save.

2. Launch the job template.
    a. Navigate to Resources → Templates.
    b. Click the desired template and then click Launch.
    c. When prompted on launch for Job Tags, type in requirements_config. You might need to click the Create Job Tag line below requirements_config to enter the job tag.

requirements_config ensures that you have the correct libraries to run the other roles.

    d. Click Next and then Launch to start the job.
    e. Click View → Jobs to monitor the job output and progress.
    f. When prompted on launch for Job Tags, type in ontap_config. You might need to click the Create "Job Tag" line right below ontap_config to enter the job tag.
    g. Click Next and then Launch to start the job.
    h. Click View → Jobs to monitor the job output and progress
    i. After the ontap_config role has completed, run the process again for linux_config.
    j. Navigate to Resources → Templates.
    k. Select the desired template and then click Launch.
    l. When prompted on launch for the Job Tags type in linux_config, you might need to select the Create "job tag" line right below linux_config to enter the job tag.
    m. Click Next and then Launch to start the job.
    n. Select View → Jobs to monitor the job output and progress.
    o. After the linux_config role has completed, run the process again for oracle_config.
    p. Go to Resources → Templates.
    q. Select the desired template and then click Launch.
    r. When prompted on launch for Job Tags, type oracle_config. You might need to select the Create "Job Tag" line right below oracle_config to enter the job tag.
    s. Click Next and then Launch to start the job.
    t. Select View → Jobs to monitor the job output and progress.

6. Deploy additional database on same Oracle host

The Oracle portion of the playbook creates a single Oracle container database on an Oracle server per execution. To create additional container databases on the same server, complete the following steps.

1. Revise host_vars variables.
    a. Go back to step 2 - Configure Oracle host_vars.
    b. Change the Oracle SID to a different naming string.
    c. Change the listener port to different number.
    d. Change the EM Express port to a different number if you are installing EM Express.
    e. Copy and paste the revised host variables to the Oracle Host Variables field in the Host Configuration Detail tab.

2. Launch the deployment job template with only the oracle_config tag.

Unresolved directive in ent-apps-db/awx_automation.adoc - include::ent-apps-db/validation.adoc[]

Step-by-step deployment procedure

CLI deployment Oracle 19c Database

This section covers the steps required to prepare and deploy Oracle19c Database with the CLI. Make sure that you have reviewed the Getting Started and Requirements section and prepared your environment accordingly.

Download Oracle19c repo

```
1. From your ansible controller, run the following command:
```

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

```
2. After downloading the repository, change directories to
na_oracle19c_deploy <cd na_oracle19c_deploy>.
```

Edit the hosts file

Complete the following before deployment:

1. Edit your hosts file na_oracle19c_deploy directory.
2. Under [ontap], change the IP address to your cluster management IP.
3. Under the [oracle] group, add the oracle hosts names. The host name must be resolved to its IP address either through DNS or the hosts file, or it must be specified in the host.
4. After you have completed these steps, save any changes.

The following example depicts a host file:

```
#ONTAP Host<div>
[ontap]
<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>10.61.184.183<i></i></span>
</div>
#Oracle hosts<div>
<div>
[oracle]<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>rtpora01<i></i></span>
<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>rtpora02<i></i></span>
</div>
```

This example executes the playbook and deploys oracle 19c on two oracle DB servers concurrently. You can also test with just one DB server. In that case, you only need to configure one host variable file.

The playbook executes the same way regardless of how many Oracle hosts and databases you deploy.

Edit the host_name.yml file under host_vars

Each Oracle host has its host variable file identified by its host name that contains host-specific variables. You can specify any name for your host. Edit and copy the `host_vars` from the Host VARS Config section and paste it into your desired `host_name.yml` file.

The items in blue must be changed to match your environment.

Unresolved directive in ent-apps-db/cli_automation.adoc - include::ent-apps-db/host_vars.adoc[]

Edit the vars.yml file

The `vars.yml` file consolidates all environment-specific variables (ONTAP, Linux, or Oracle) for Oracle deployment.

- Edit and copy the variables from the VARS section and paste these variables into your `vars.yml` file.

Unresolved directive in ent-apps-db/cli_automation.adoc - include::ent-apps-db/vars.adoc[]

Run the playbook

After completing the required environment prerequisites and copying the variables into `vars.yml` and `your_host.yml`, you are now ready to deploy the playbooks.

<username> must be changed to match your environment.

```
1. Run the ONTAP playbook by passing the correct tags and ONTAP cluster
username. Fill the password for ONTAP cluster, and vsadmin when prompted.
```

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t
ontap_config -e @vars/vars.yml
```

```
2. Run the Linux playbook to execute Linux portion of deployment. Input
for admin ssh password as well as sudo password.
```

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t
linux_config -e @vars/vars.yml
```

```
3. Run the Oracle playbook to execute Oracle portion of deployment. Input
for admin ssh password as well as sudo password.
```

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t
oracle_config -e @vars/vars.yml
```

Deploy Additional Database on Same Oracle Host

The Oracle portion of the playbook creates a single Oracle container database on an Oracle server per execution. To create additional container database on the same server, complete the following steps:

1. Revise the host_vars variables.
   a. Go back to step 3 - Edit the `host_name.yml` file under `host_vars`.
   b. Change the Oracle SID to a different naming string.
   c. Change the listener port to different number.
   d. Change the EM Express port to a different number if you have installed EM Express.
   e. Copy and paste the revised host variables to the Oracle host variable file under `host_vars`.
2. Execute the playbook with the `oracle_config` tag as shown above in Run the playbook.

Unresolved directive in ent-apps-db/cli_automation.adoc - include::ent-apps-db/validation.adoc[]

Microsoft SQL Server

TR-4897: SQL Server on Azure NetApp Files - Real Deployment View

Niyaz Mohamed, NetApp

IT organizations face constant change. Gartner reports nearly 75% of all databases will require cloud-based storage by 2022. As a leading relational database management system (RDBMS), Microsoft SQL Server is the go-to choice for Windows platform-designed applications and organizations that rely on SQL Server for everything from enterprise resource planning (ERP) to analytics to content management. SQL Server has helped to revolutionize the way enterprises manage massive data sets and power their applications to meet the schema and query performance demands.

Most IT organizations follow a cloud-first approach. Customers in a transformation phase evaluate their current IT landscape and then migrate their database workloads to the cloud based on an assessment and discovery exercise. Some factors driving customers toward cloud migration include elasticity/burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and so on. The reason for migration can vary based on each organization and their respective business priorities. When moving to the cloud, choosing the right cloud storage is very important in order to unleash the power of SQL Server database cloud deployment.

Use case

Moving the SQL Server estate to Azure and integrating SQL Server with Azure's vast array of platform-as-a-service (PaaS) features such as Azure Data Factory, Azure IoT Hub, and Azure Machine Learning creates tremendous business value to support digital transformation. Adopting the cloud also enables the respective business unit to focus on productivity and delivering new features and enhancements faster (DevTest use case) than relying on the CAPEX model or traditional private cloud models. This document covers a real-time deployment of SQL Server Always On availability group (AOAG) on Azure NetApp Files leveraging Azure Virtual Machines.

Azure NetApp Files provides enterprise-grade storage with continuously available file shares. Continuously available shares are required by SQL Server production databases on SMB file share to make sure that the node always has access to the database storage, including during disruptive scenarios such as controller upgrades or failures. Continuously available file shares eliminate the need to replicate data between storage nodes. Azure NetApp Files uses SMB 3.0 scale-out, persistent handles, and transparent failover to support nondisruptive operations (NDOs) for planned and unplanned downtime events, including many administrative tasks.

When planning cloud migrations, you should always evaluate the best approach to use. The most common and easiest approach for application migration is rehosting (also known as lift and shift). The example scenario provided in this document uses the rehosting method. SQL Server on Azure virtual machines with Azure NetApp Files allows you to use full versions of SQL Server in the cloud without having to manage on-premises hardware. SQL Server virtual machines (VMs) also simplify licensing costs when you pay as you go and provides elasticity and bursting capabilities for development, test, and estate refresh scenarios.

Factors to consider

VM performance

Selecting the right VM size is important for optimal performance of a relational database in a public cloud. Microsoft recommends that you continue using the same database performance-tuning options that are applicable to SQL Server in on-premises server environments. Use memory-optimized VM sizes for the best performance of SQL Server workloads. Collect the performance data of existing deployment to identify the RAM and CPU utilization while choosing the right instances. Most deployments choose between the D, E, or M series.

Notes:

- For the best performance of SQL Server workloads, use memory-optimized VM sizes.
- NetApp and Microsoft recommend that you identify the storage performance requirements before choosing the instance type with the appropriate memory-to-vCore ratio. This also helps select a lower-instance type with the right network bandwidth to overcome storage throughput limits of the VM.

VM redundancy

To increase redundancy and high availability, SQL Server VMs should either be in the same availability set or different availability zones. When creating Azure VMs, you must choose between configuring availability sets versus availability zones; an Azure VM cannot participate in both.

High availability

For high availability, configuring SQL Server AOAG or Always On Failover Cluster Instance (FCI) is the best option. For AOAG, this involves multiple instances of SQL Server on Azure Virtual Machines in a virtual network. If high availability is required at the database level, consider configuring SQL Server availability groups.

Storage configuration

Microsoft SQL Server can be deployed with an SMB file share as the storage option. Starting with SQL Server 2012, system databases (master, model, msdb, or tempdb), and user databases can be installed with Server Message Block (SMB) file server as a storage option. This applies to both SQL Server stand-alone and SQL Server FCI.

File share storage for SQL Server databases should support continuously available property. This provides uninterrupted access to the file-share data.

Azure NetApp Files provides high performing file storage to meet any demanding workload, and it reduces SQL Server TCO as compared to block storage solutions. With block storage, VMs have imposed limits on I/O and bandwidth for disk operations; network bandwidth limits alone are applied against Azure NetApp Files. In other words, no VM-level I/O limits are applied to Azure NetApp Files. Without these I/O limits, SQL Server running on smaller VMs connected to Azure NetApp Files can perform as well as SQL Server running on much larger VMs. Azure NetApp Files reduce SQL Server deployment costs by reducing compute and software licensing costs. For detailed cost analysis and performance benefits of using Azure NetApp Files for SQL Server deployment, see the Benefits of using Azure NetApp Files for SQL Server deployment.

Benefits

The benefits of using Azure NetApp Files for SQL Server include the following:

- Using Azure NetApp Files allows you to use smaller instances, thus reducing compute cost.
- Azure NetApp Files also reduces software licensing costs, which reduce the overall TCO.
- Volume reshaping and dynamic service level capability optimizes cost by sizing for steady-state workloads and avoiding overprovisioning.

Notes:

- To increase redundancy and high availability, SQL Server VMs should either be in the same availability set or in different availability zones. Consider file path requirements if user-defined data files are required; in which case, select SQL FCI over SQL AOAG.
- The following UNC path is supported: \\ANFSMB-b4ca.anf.test\SQLDB and \\ANFSMB-b4ca.anf.test\SQLDB\.

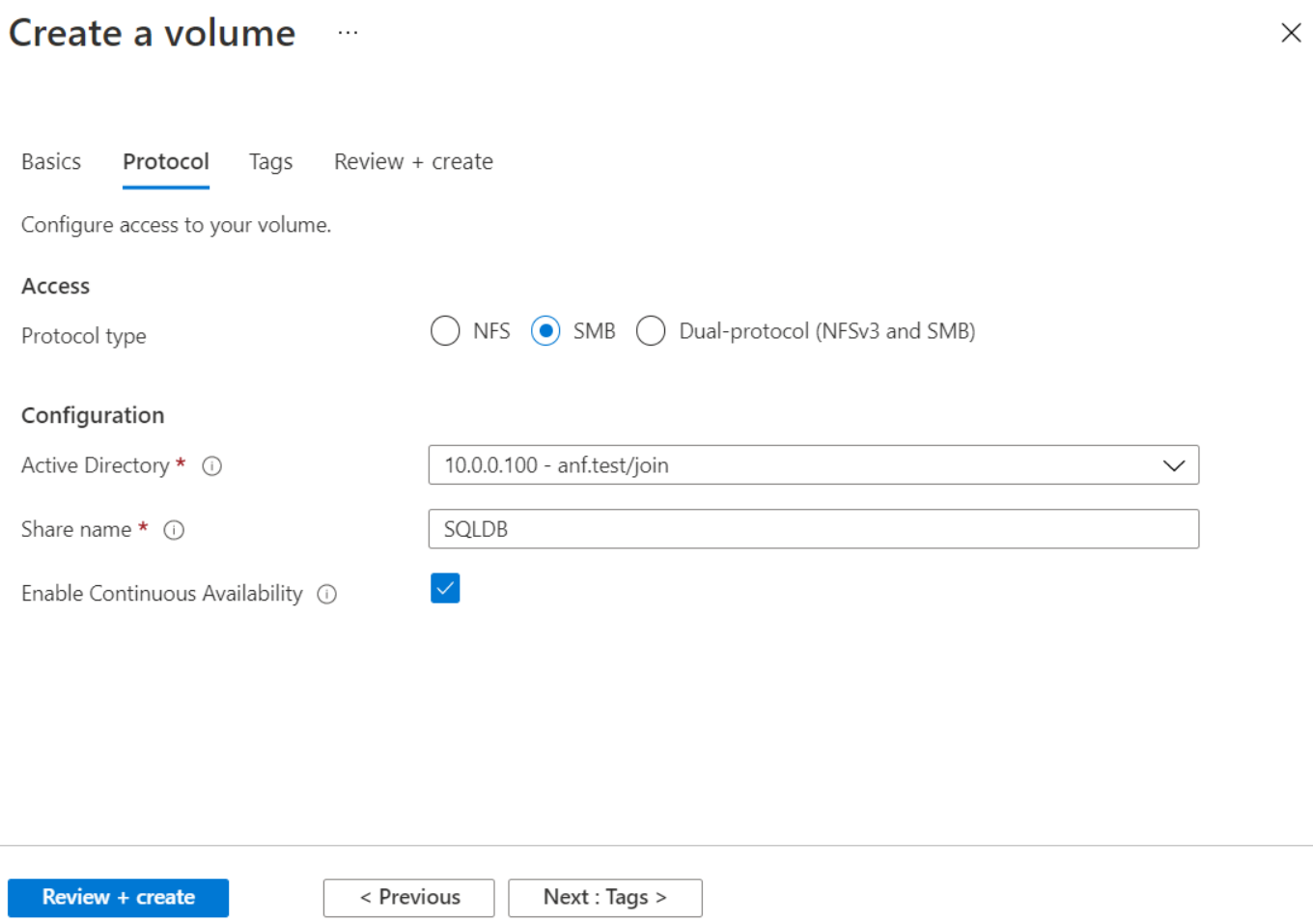
- The loopback UNC path is not supported.
- For sizing, use historic data from your on-premises environment. For OLTP workloads, match the target IOPS with performance requirements using workloads at average and peak times along with the disk reads/sec and disk writes/sec performance counters. For data warehouse and reporting workloads, match the target throughput using workloads at average and peak times and the disk read bytes/sec and disk write bytes/sec. Average values can be used in conjunction with volume reshaping capabilities.

Create continuously available shares

Create continuously available shares with the Azure portal or Azure CLI. In the portal, select the Enable Continuous Availability property option. for the Azure CLI, specify the share as a continuously available share by using the `az netappfiles volume create with the smb-continuously-avl` option set to `$True`. To learn more about creating a new, continuous availability-enabled volume, see Creating a Continuously Available Share.

Notes:

- Enable continuous availability for the SMB volume as shown in the following image.
- If a non-administrator domain account is used, make sure the account has the required security privilege assigned.
- Set the appropriate permissions at the share level and proper file-level permissions.
- A continuously available property cannot be enabled on existing SMB volumes. To convert an existing volume to use a continuously available share, use NetApp Snapshot technology. For more information, see Convert existing SMB volumes to use Continuous Availability.

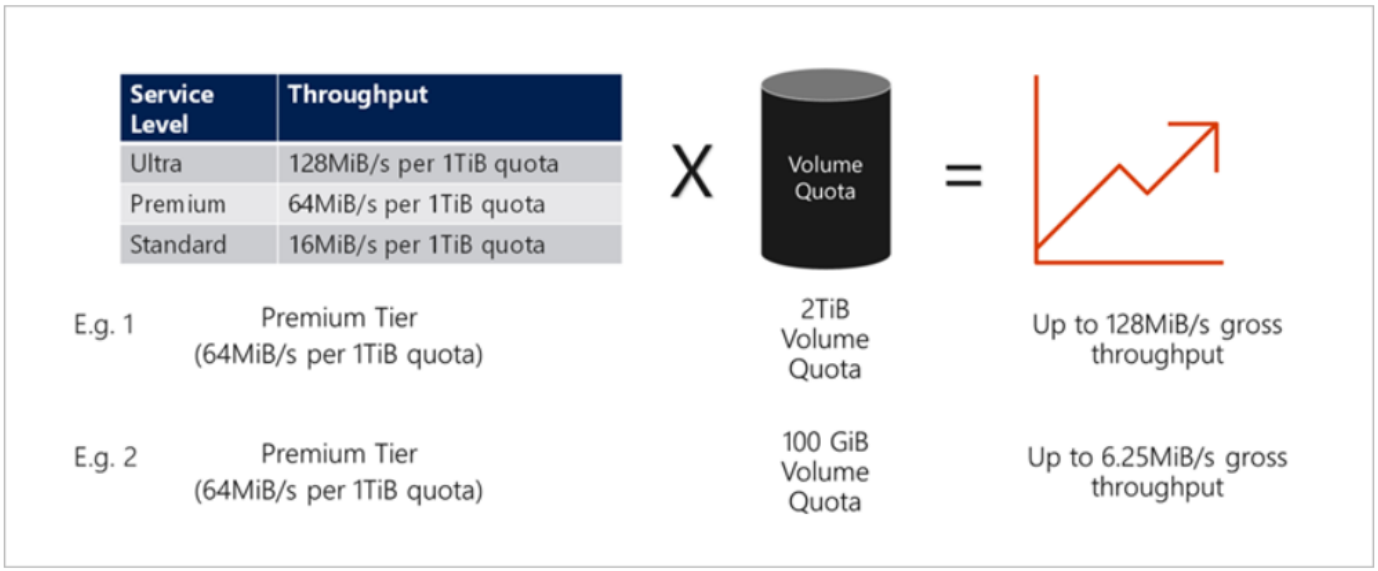


Performance

Azure NetApp Files supports three service levels: Standard (16MBps per terabyte), Premium (64MBps per terabyte), and Ultra (128MBps per terabyte). Provisioning the right volume size is important for optimal performance of the database workload. With Azure NetApp Files, volume performance and the throughput limit are based on a combination of the following factors:

- The service level of the capacity pool to which the volume belongs
- The quota assigned to the volume
- The quality of service (QoS) type (auto or manual) of the capacity pool

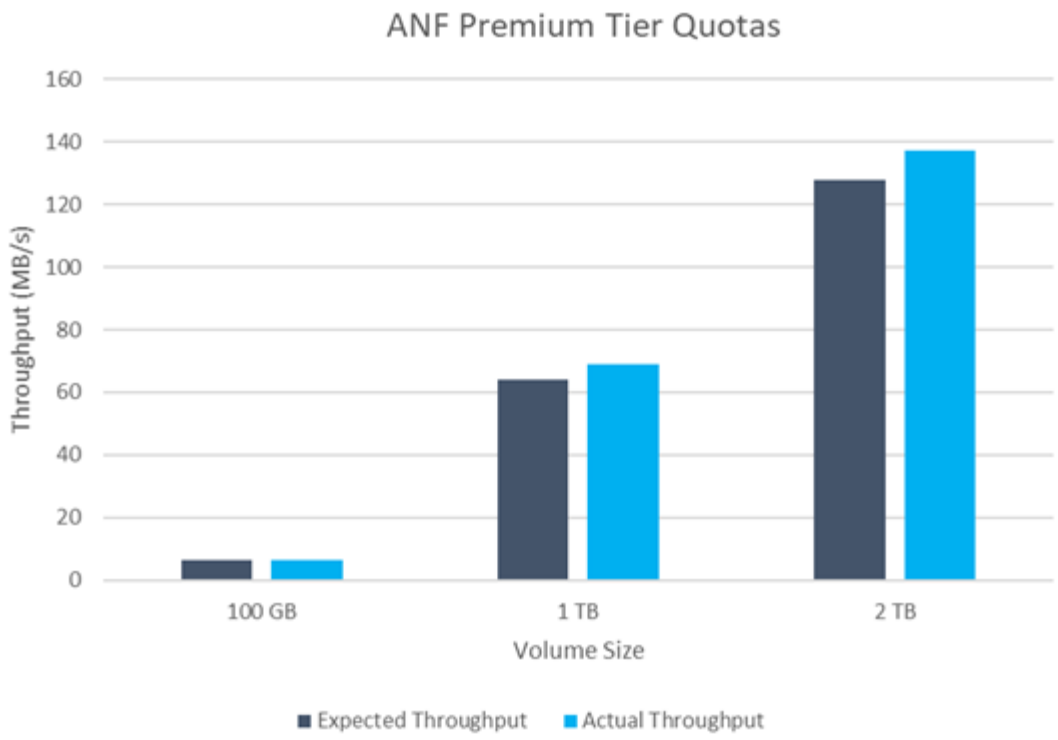
For more information, see Service levels for Azure NetApp Files.



Performance validation

As with any deployment, testing the VM and storage is critical. For storage validation, tools such as HammerDB, Apploader, the SQL Server storage benchmark (SB) tool, or any custom script or FIO with the appropriate read/write mix should be used. Keep in mind however that most SQL Server workloads, even busy OLTP workloads, are closer to 80%–90% read and 10%–20% write.

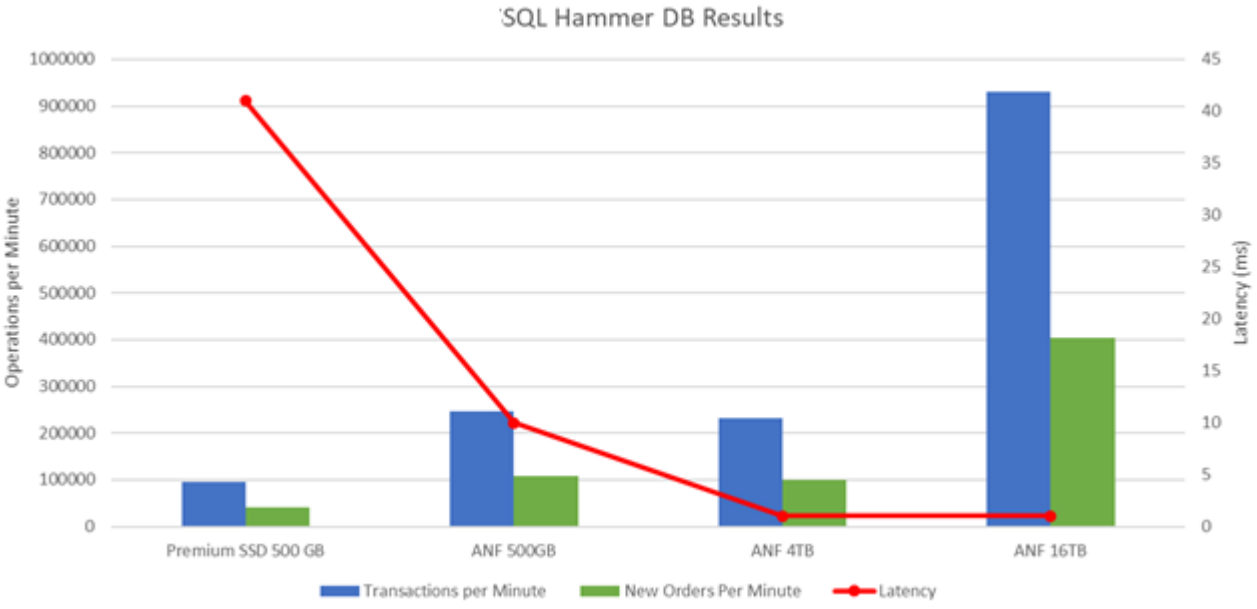
To showcase performance, a quick test was performed against a volume using premium service levels. In this test, the volume size was increased from 100GB to 2TB on the fly without any disruption to application access and zero data migration.



Here is another example of real time performance testing with HammerDB performed for the deployment covered in this paper. For this testing, we used a small instance with eight vCPUs, a 500GB Premium SSD, and a 500GB SMB Azure NetApp Files volume. HammerDB was configured with 80 warehouses and eight users.

The following chart shows that Azure NetApp Files was able to deliver 2.6x the number of transactions per minute at 4x lower latency when using a comparable sized volume (500GB).

An additional test was performed by resizing to a larger instance with 32x vCPUs and a 16TB Azure NetApp Files volume. There was a significant increase in transactions per minute with consistent 1ms latency. HammerDB was configured with 80 warehouses and 64 users for this test.



Cost optimization

Azure NetApp Files allows nondisruptive, transparent volume resizing and the ability to change the service levels with zero downtime and no effect on applications. This is a unique capability allowing dynamic cost management that avoids the need to perform database sizing with peak metrics. Rather, you can use steady state workloads, which avoids upfront costs. The volume reshaping and dynamic service-level change allows you to adjust the bandwidth and service level of Azure NetApp Files volumes on demand almost instantaneously without pausing I/O, while retaining data access.

Azure PaaS offerings such as LogicApp or Functions can be used to easily resize the volume based on a specific webhook or alert rule trigger to meet the workload demands while dynamically handling the cost.

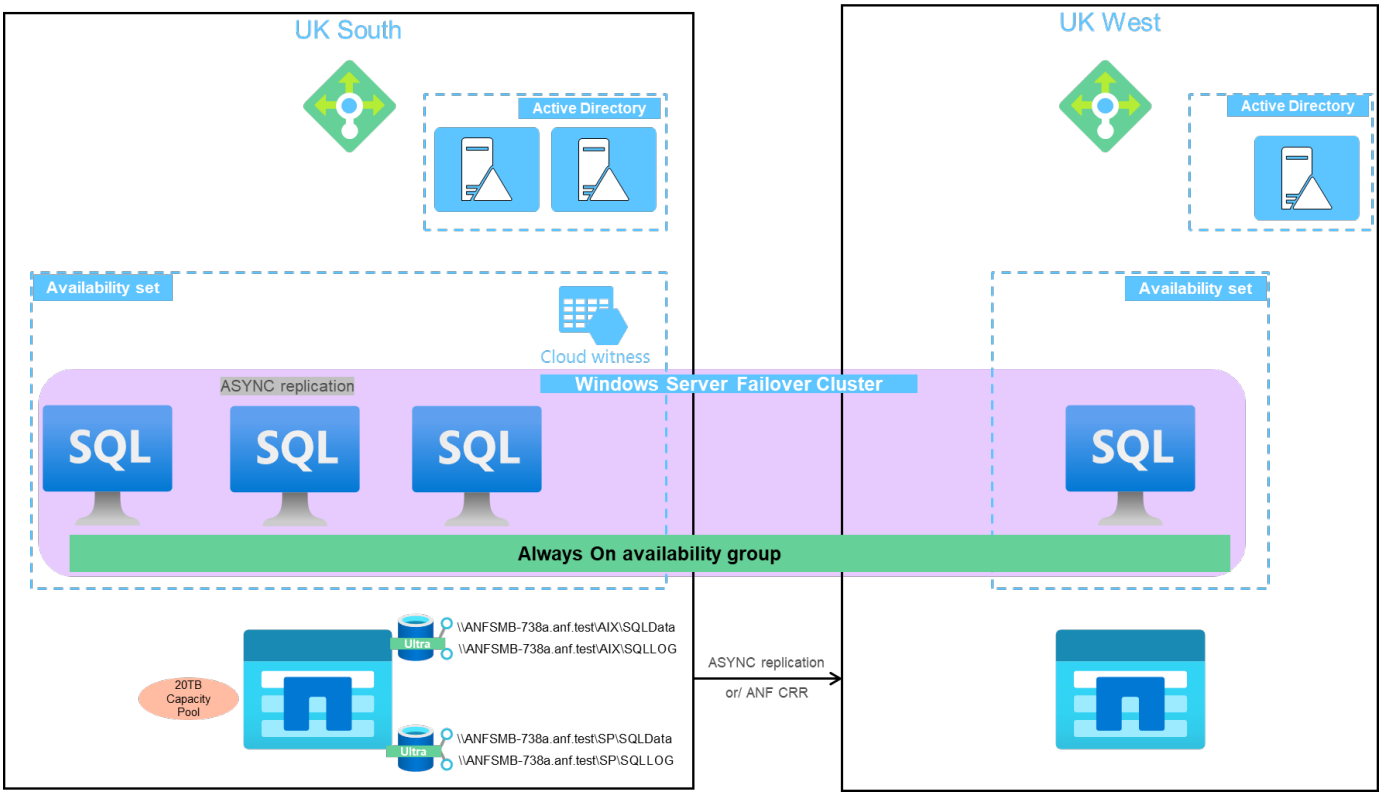
For example, consider a database that needs 250MBps for steady state operation; however, it also requires a peak throughput of 400MBps. In this case, the deployment should be performed with a 4TB volume within the Premium service level to meet the steady-state performance requirements. To handle the peak workload, increase the volume size using Azure functions to 7TB for that specific period, and then downsize the volume to make the deployment cost effective. This configuration avoids overprovisioning of the storage.

Real-time, high-level reference design

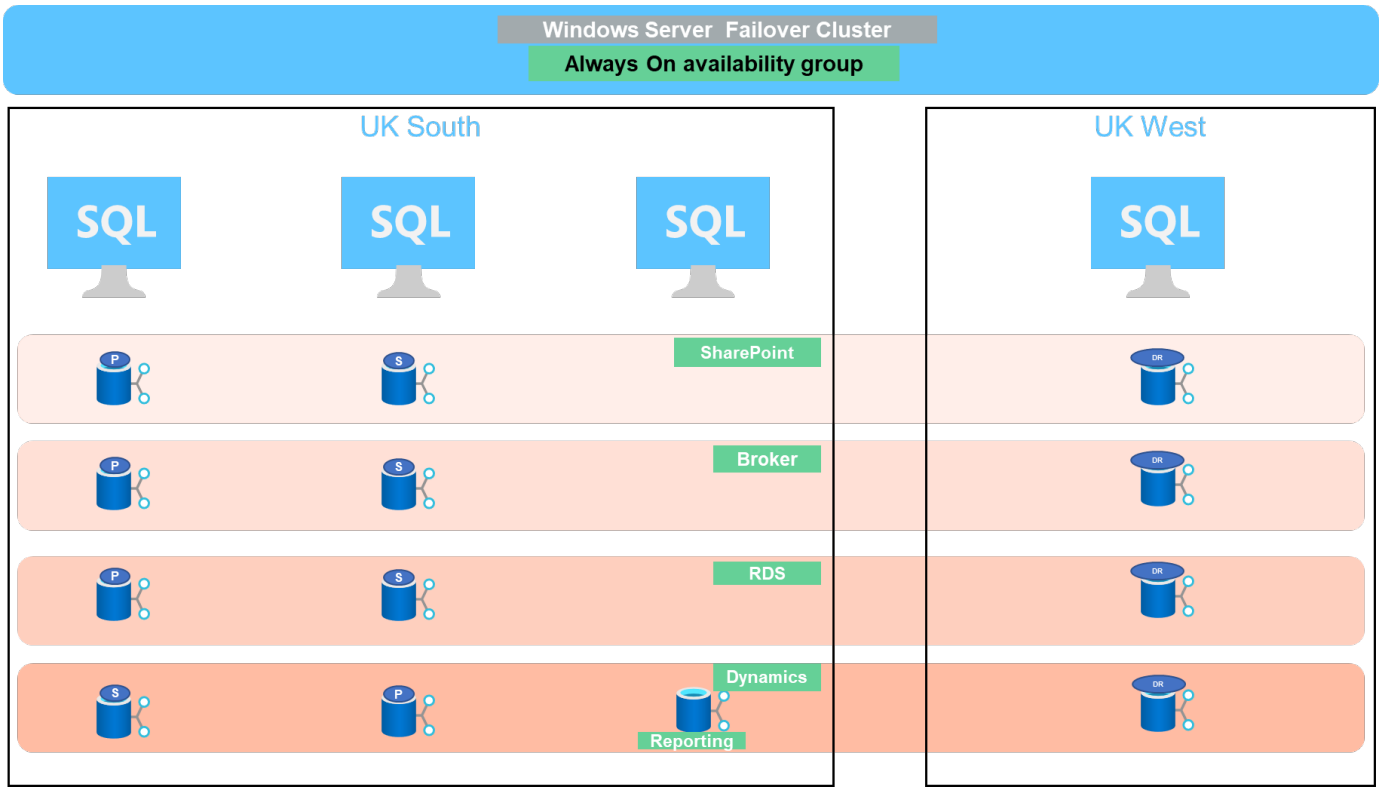
This section covers a real-time deployment of a SQL database estate in an AOAG configuration using an Azure NetApp Files SMB volume.

- Number of nodes: 4
- Number of databases: 21
- Number of availability groups: 4
- Backup retention: 7 days
- Backup archive: 365 days

Deploying FCI with SQL Server on Azure virtual machines with an Azure NetApp Files share provides a cost-efficient model with a single copy of the data. This solution can prevent add-file operation issues if the file path differs from the secondary replica.



The following image shows the databases within AOAG spread across the nodes.



Data layout

The user database files (.mdf) and user database transaction log files (.ldf) along with tempDB are stored on the same volume. The service level is Ultra.

The configuration consists of four nodes and four AGs. All 21 databases (part of Dynamic AX, SharePoint, RDS connection broker, and indexing services) are stored on the Azure NetApp Files volumes. The databases are balanced between the AOAG nodes to use the resources on the nodes effectively. Four D32 v3 instances are added in the WSFC, which participates in the AOAG configuration. These four nodes are provisioned in the Azure virtual network and are not migrated from on-premises.

Notes:

- If the logs require more performance and throughput depending on the nature of the application and the queries executed, the database files can be placed on the Premium service level, and the logs can be stored at the Ultra service level.
- If the tempdb files have been placed on Azure NetApp Files, then the Azure NetApp Files volume should be separated from the user database files. Here is an example distribution of the database files in AOAG.

Notes:

- To retain the benefits of Snapshot copy-based data protection, NetApp recommends not combining data and log data into the same volume.
- An add-file operation performed on the primary replica might fail on the secondary databases if the file path of a secondary database differs from the path of the corresponding primary database. This can happen if the share path is different on primary and secondary nodes (due to different computer accounts). This failure could cause the secondary databases to be suspended. If the growth or performance pattern cannot be predicted and the plan is to add files later, a SQL Server failover cluster with Azure NetApp Files is an acceptable solution. For most deployments, Azure NetApp Files meets the performance requirements.

Migration

There are several ways to migrate an on-premises SQL Server user database to SQL Server in an Azure virtual machine. The migration can be either online or offline. The options chosen depend on the SQL Server version, business requirements, and the SLAs defined within the organization. To minimize downtime during the database migration process, NetApp recommends using either the AlwaysOn option or the transactional replication option. If it is not possible to use these methods, you can migrate the database manually.

The simplest and most thoroughly tested approach for moving databases across machines is backup and restore. Typically, you can start with a database backup followed by a copy of the database backup into Azure. You can then restore the database. For the best data transfer performance, migrate the database files into the Azure VM using a compressed backup file. The high-level design referenced in this document uses the backup approach to Azure file storage with Azure file sync and then restore to Azure NetApp files.

Azure Migrate can be used to discover, assess, and migrate SQL Server workloads.

To perform a migration, complete the following high-level steps:

1. Based on your requirements, set up connectivity.
2. Perform a full database backup to an on-premises file-share location.
3. Copy the backup files to an Azure file share with Azure file sync.
4. Provision the VM with the desired version of SQL Server.
5. Copy the backup files to the VM by using the `copy` command from a command prompt.
6. Restore the full databases to SQL Server on Azure virtual machines.

To restore 21 databases, it took approximately nine hours. This approach is specific to this scenario. However, other migration techniques listed below can be used based on your situation and requirements.

Other migration options to move data from an on-premises SQL Server to Azure NetApp Files include the following:

- Detach the data and log files, copy them to Azure Blob storage, and then attach them to SQL Server in the Azure VM with an ANF file share mounted from the URL.
- If you are using Always On availability group deployment on-premises, use the Add Azure Replica Wizard to create a replica in Azure and then perform failover.
- Use SQL Server transactional replication to configure the Azure SQL Server instance as a subscriber, disable replication, and point users to the Azure database instance.
- Ship the hard drive using the Windows Import/Export Service.

Backup and recovery

Backup and recovery are an important aspect of any SQL Server deployment. It is mandatory to have the appropriate safety net to quickly recover from various data failure and loss scenarios in conjunction with high availability solutions such as AOAG. SQL Server Database Quiesce Tool, Azure Backup (streaming), or any third-party backup tool such as Commvault can be used to perform an application- consistent backup of the databases,

Azure NetApp Files Snapshot technology allows you to easily create a point-in-time (PiT) copy of the user databases without affecting performance or network utilization. This technology also allows you to restore a Snapshot copy to a new volume or quickly revert the affected volume to the state it was in when that Snapshot copy was created by using the revert volume function. The Azure NetApp Files snapshot process is very quick and efficient, which allows for multiple daily backups, unlike the streaming backup offered by Azure backup. With multiple Snapshot copies possible in a given day, the RPO and RTO times can be significantly reduced. To add application consistency so that data is intact and properly flushed to the disk before the Snapshot copy is taken, use the SQL Server database quiesce tool (SCSQLAPI tool; access to this link requires NetApp SSO login credentials). This tool can be executed from within PowerShell, which quiesces the SQL Server database and in turn can take the application-consistent storage Snapshot copy for backups.

*Notes: *

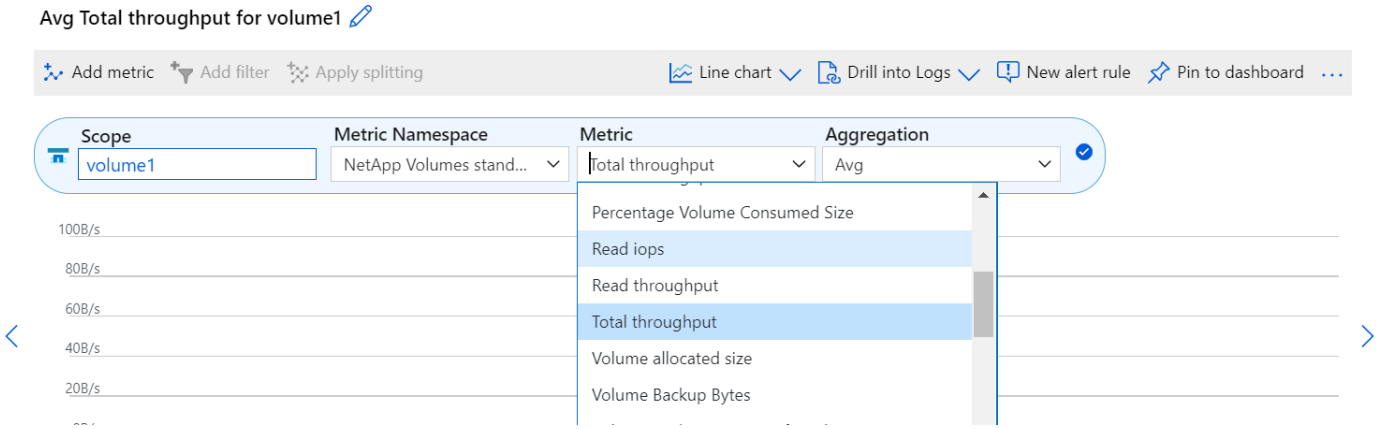
- The SCSQLAPI tool only supports the 2016 and 2017 versions of SQL Server.
- The SCSQLAPI tool only works with one database at a time.
- Isolate the files from each database by placing them onto a separate Azure NetApp Files volume.

Because of SCSQL API's vast limitations, Azure Backup was used for data protection in order to meet the SLA requirements. It offers a stream-based backup of SQL Server running in Azure Virtual Machines and Azure NetApp Files. Azure Backup allows a 15-minute RPO with frequent log backups and PiT recovery up to one second.

Monitoring

Azure NetApp Files is integrated with Azure Monitor for the time series data and provides metrics on allocated storage, actual storage usage, volume IOPS, throughput, disk read bytes/sec, disk write bytes/sec, disk reads/sec and disk writes/sec, and associated latency. This data can be used to identify bottlenecks with alerting and to perform health checks to verify that your SQL Server deployment is running in an optimal configuration.

In this HLD, ScienceLogic is used to monitor Azure NetApp Files by exposing the metrics using the appropriate service principal. The following image is an example of the Azure NetApp Files Metric option.



DevTest using thick clones

With Azure NetApp Files, you can create instantaneous copies of databases to test functionality that should be implemented by using the current database structure and content during the application development cycles, to use the data extraction and manipulation tools when populating data warehouses, or to even recover data that was mistakenly deleted or changed. This process does not involve copying data from Azure Blob containers, which makes it very efficient. After the volume is restored, it can be used for read/write operations, which significantly reduces validation and time to market. This needs to be used in conjunction with SCSQLAPI for application consistency. This approach provides yet another continuous cost optimization technique along with Azure NetApp Files leveraging the Restore to New volume option.

Notes:

- The volume created from the Snapshot copy using the Restore New Volume option consumes capacity from the capacity pool.
- You can delete the cloned volumes by using REST or Azure CLI to avoid additional costs (in case the capacity pool must be increased).

Hybrid storage options

Although NetApp recommends using the same storage for all the nodes in SQL Server availability groups, there are scenarios in which multiple storage options can be used. This scenario is possible for Azure NetApp Files in which a node in AOAG is connected with an Azure NetApp Files SMB file share and the second node is connected with an Azure Premium disk. In these instances, make sure that the Azure NetApp Files SMB share is holding the primary copy of the user databases and the Premium disk is used as the secondary copy.

Notes:

- In such deployments, to avoid any failover issues, make sure that continuous availability is enabled on the SMB volume. With no continuously available attribute, the database can fail if there is any background maintenance at the storage layer.
- Keep the primary copy of the database on the Azure NetApp Files SMB file share.

Business continuity

Disaster recovery is generally an afterthought in any deployment. However, disaster recovery must be addressed during the initial design and deployment phase to avoid any impact to your business. With Azure

NetApp Files, the cross-region replication (CRR) functionality can be used to replicate the volume data at the block level to the paired region to handle any unexpected regional outage. The CRR-enabled destination volume can be used for read operations, which makes it an ideal candidate for disaster recovery simulations. In addition, the CRR destination can be assigned with the lowest service level (for instance, Standard) to reduce the overall TCO. In the event of a failover, replication can be broken, which makes the respective volume read/write capable. Also, the service level of the volume can be changed by using the dynamic service level functionality to significantly reduce disaster recovery cost. This is another unique feature of Azure NetApp Files with block replication within Azure.

Long-term Snapshot copy archive

Many organizations must perform long-term retention of snapshot data from database files as a mandatory compliance requirement. Although this process is not used in this HLD, it can be easily accomplished by using a simple batch script using AzCopy to copy the snapshot directory to the Azure Blob container. The batch script can be triggered based on a specific schedule by using scheduled tasks. The process is straightforward—it includes the following steps:

1. Download the AzCopy V10 executable file. There is nothing to install because it is an `exe` file.
2. Authorize AzCopy by using a SAS token at the container level with the appropriate permissions.
3. After AzCopy is authorized, the data transfer begins.

Notes:

- In batch files, make sure to escape the % characters that appear in SAS tokens. This can be done by adding an additional % character next to existing % characters in the SAS token string.
- The Secure Transfer Required setting of a storage account determines whether the connection to a storage account is secured with Transport Layer Security (TLS). This setting is enabled by default. The following batch script example recursively copies data from the Snapshot copy directory to a designated Blob container:

```
SET source="Z:\~snapshot"
echo %source%
SET
dest="https://testanfacct.blob.core.windows.net/azcoptst?sp=racwdl&st=2020
-10-21T18:41:35Z&se=2021-10-22T18:41:00Z&sv=2019-12
-12&sr=c&sig=ZxRUJwFlLXgHS8As7HzXJOaDXXVJ7PxxIX3ACpx56XY%%3D"
echo %dest%
```

The following example cmd is executed in PowerShell:

```
-recursive
```

```
INFO: Scanning...
INFO: Any empty folders will not be processed, because source and/or
destination doesn't have full folder support
Job b3731dd8-da61-9441-7281-17a4db09ce30 has started
Log file is located at: C:\Users\niyaz\.azcopy\b3731dd8-da61-9441-7281-
17a4db09ce30.log
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
INFO: azcopy.exe: A newer version 10.10.0 is available to download
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
Job b3731dd8-da61-9441-7281-17a4db09ce30 summary
Elapsed Time (Minutes): 0.0333
Number of File Transfers: 2
Number of Folder Property Transfers: 0
Total Number of Transfers: 2
Number of Transfers Completed: 2
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 5
Final Job Status: Completed
```

Notes:

- A similar backup feature for long-term retention will soon be available in Azure NetApp Files.
- The batch script can be used in any scenario that requires data to copied to Blob container of any region.

Cost optimization

With volume reshaping and dynamic service level change, which is completely transparent to the database, Azure NetApp Files allows continuous cost optimizations in Azure. This capability is used in this HLD extensively to avoid overprovisioning of additional storage to handle workload spikes.

Resizing the volume can be easily accomplished by creating an Azure function in conjunction with the Azure alert logs.

Conclusion

Whether you are targeting an all-cloud or hybrid cloud with stretch databases, Azure NetApp Files provides excellent options to deploy and manage the database workloads while reducing your TCO by making data requirements seamless to the application layer.

This document covers recommendations for planning, designing, optimizing, and scaling Microsoft SQL Server deployments with Azure NetApp Files, which can vary greatly between implementations. The right solution depends on both the technical details of the implementation and the business requirements driving the project.

Takeaways

The key points of this document include:

- You can now use Azure NetApp Files to host the database and file share witness for SQL Server cluster.

- You can boost the application response times and deliver 99.9999% availability to provide access to SQL Server data when and where it is needed.
- You can simplify the overall complexity of the SQL Server deployment and ongoing management, such as raid striping, with simple and instant resizing.
- You can rely on intelligent operations features to help you deploy SQL Server databases in minutes and speed development cycles.
- If Azure Cloud is the destination, Azure NetApp Files is the right storage solution for optimized deployment.

Where to find additional information

To learn more about the information described in this document, refer to the following website links:

- Solution architectures using Azure NetApp Files

  https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures

- Benefits of using Azure NetApp Files for SQL Server deployment

  https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server

- SQL Server on Azure Deployment Guide Using Azure NetApp Files

  https://www.netapp.com/pdf.html?item=/media/27154-tr-4888.pdf

- Fault tolerance, high availability, and resilience with Azure NetApp Files

  https://cloud.netapp.com/blog/azure-anf-blg-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files