# Table of Contents

SAP HANA Disaster Recovery with Azure NetApp Files ................................................. 1
TR-4891: SAP HANA disaster recovery with Azure NetApp Files .................................. 1
Disaster recovery solution comparison ........................................................................... 3
ANF Cross-Region Replication with SAP HANA ............................................................ 7
Disaster recovery testing ................................................................................................. 19
Disaster recovery failover ............................................................................................... 33
Update history .................................................................................................................. 43
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 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...
• 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.

<table>
<thead>
<tr>
<th>Storage replication</th>
<th>SAP HANA system replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-region replication</td>
<td>With data preload</td>
</tr>
<tr>
<td>RTO</td>
<td>Low to medium, depending on database startup time and forward recovery</td>
</tr>
<tr>
<td>RPO</td>
<td>RPO &gt; 20min asynchronous replication</td>
</tr>
<tr>
<td>Servers at DR site can be used for dev/test</td>
<td>Yes</td>
</tr>
<tr>
<td>Replication of nondatabase data</td>
<td>Yes</td>
</tr>
<tr>
<td>DR data can be used for refresh of dev/test systems</td>
<td>Yes</td>
</tr>
<tr>
<td>DR testing without affecting RTO and RPO</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Next: ANF Cross-Region Replication with SAP HANA.

**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.
<table>
<thead>
<tr>
<th></th>
<th>Data volume replication</th>
<th>Data and log backup volume replication</th>
<th>Data and log backup volume replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRR schedule data volume</td>
<td>Daily</td>
<td>Daily</td>
<td>Daily</td>
</tr>
<tr>
<td>CRR schedule log backup</td>
<td>n/a</td>
<td>Hourly</td>
<td>10 min</td>
</tr>
<tr>
<td>volume</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max RPO</td>
<td>24 hours + Snapshot</td>
<td>1 hour</td>
<td>2 x 10 min</td>
</tr>
<tr>
<td>schedule (e.g., 6 hours)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max RTO</td>
<td>Primarily defined by</td>
<td>HANA startup time +</td>
<td>HANA startup time +</td>
</tr>
<tr>
<td></td>
<td>HANA startup time</td>
<td>recovery time</td>
<td>recovery time</td>
</tr>
<tr>
<td>Forward recovery</td>
<td>NA</td>
<td>Logs for the last 24 hours + Snapshot</td>
<td>Logs for the last 24 hours + Snapshot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>schedule (e.g., 6 hours)</td>
<td>schedule (e.g., 6 hours)</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>HANA volume</th>
<th>Source</th>
<th>Destination</th>
<th>Replication schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>HANA data volume</td>
<td>PR1-data-mnt00001</td>
<td>PR1-data-mnt00001-sm-dest</td>
<td>Daily</td>
</tr>
<tr>
<td>HANA shared volume</td>
<td>PR1-shared</td>
<td>PR1-shared-sm-dest</td>
<td>Hourly</td>
</tr>
<tr>
<td>HANA log/catalog backup</td>
<td>hanabackup</td>
<td>hanabackup-sm-dest</td>
<td>Hourly</td>
</tr>
</tbody>
</table>

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.

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.
Create a new protection 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.
Disaster recovery testing

Disaster Recovery Testing

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 that 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](https://help.sap.com) 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.

```bash
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.

```bash
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.

<table>
<thead>
<tr>
<th>HANA PR1 volumes</th>
<th>New volume and subdirectories at disaster recovery site</th>
<th>Mount point at target host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data volume</td>
<td>PR1-data-mnt00001-sm-dest-clone</td>
<td>/hana/data/PR1/mnt00001</td>
</tr>
<tr>
<td>Shared volume</td>
<td>PR1-shared-sm-dest-clone/shared PR1</td>
<td>/hana/shared/usr/sap/PR1</td>
</tr>
<tr>
<td>Log backup volume</td>
<td>hanabackup-sm-dest-clone</td>
<td>/hanabackup</td>
</tr>
</tbody>
</table>

The mount points listed in this table must be created at the target host.

Here are the required `/etc/fstab` entries.

```bash
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
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
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 /usr/sap/PR1 nfs
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,lock 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.
Create a volume

<table>
<thead>
<tr>
<th>Basics</th>
<th>Protocol</th>
<th>Tags</th>
<th>Review + create</th>
</tr>
</thead>
</table>

Configure access to your volume.

**Access**

- Protocol type: NFS, SMB, Dual-protocol (NFSv3 and SMB)

**Configuration**

- File path: PR1-data-mnt00001-sm-dest-clone
- Versions: NFSv4.1
- Kerberos: Enabled, Disabled

**Export policy**

Configure the volume's export policy. This can be edited later. Learn more

<table>
<thead>
<tr>
<th>Index</th>
<th>Allowed clients</th>
<th>Access</th>
<th>Root Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0/0</td>
<td>Read &amp; Write</td>
<td>On</td>
</tr>
</tbody>
</table>

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          0          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 107377026560 6672640   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096 107377048320 11204096   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096 107377048320 11204096   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone 107379429120 35293440 107379429120 35293440   1% /hanabackup
```

Next: HANA database recovery.

HANA database recovery

Previous: Mount the volumes at the target host.

Start the required SAP services.
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  2597  0 11:29 ?        00:00:00
/prusr/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**
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.
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**
  
  ```python
  recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"
  ```

- **Tenant database**
  
  ```plaintext
  Within hdfsll: 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**
Tenant database recovery

```
prladm@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.

```
prladm@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.

**Next: Disaster recovery failover.**

**Disaster recovery failover**

**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...
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.

```bash
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.

```bash
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`. 

---

35
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
time,lock,_netdev,sec=sys 0 0
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noatime,lock,sec=sys 0 0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
time,lock,_netdev,sec=sys 0 0
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noatime,lock,sec=sys 0 0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
time,lock,_netdev,sec=sys 0 0
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noatime,lock,sec=sys 0 0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
time,lock,_netdev,sec=sys 0 0
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noatime,lock,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,nolock 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.

```bash
vm-pr1:~ # mount -a
```

The following output shows the required file systems.
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.
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**

  ```bash
  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**
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>
```
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.

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.

Next: Update history.

Update history

Previous: HANA database recovery.

The following technical changes have been made to this solution since its original publication.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Update summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>April 2021</td>
<td>Initial version</td>
</tr>
</tbody>
</table>