Abstract

This document provides an overview of the different options for data protection in SAP HANA. It also provides a detailed setup and use case description of a disaster recovery solution based on asynchronous storage replication. The solution uses the NetApp® Snap Creator® storage management framework with the SAP HANA plug-in to manage database consistency. It also uses NetApp Snapshot® copies and NetApp SnapMirror® data replication.
TABLE OF CONTENTS

1 Data Protection Overview ........................................................................................................... 4

2 Disaster Recovery Solution Comparison ...................................................................................... 6
  2.1 Backup and Recovery .................................................................................................................. 7
  2.2 Synchronous Storage Replication ............................................................................................. 8
  2.3 Asynchronous Storage Replication ............................................................................................ 9
  2.4 SAP HANA System Replication ................................................................................................ 10
  2.5 Summary .................................................................................................................................... 12

3 Asynchronous Storage Replication ............................................................................................. 13
  3.1 Combine Backup and Disaster Recovery Replication ............................................................... 13
  3.2 Replication of Data Volume Only ............................................................................................. 14
  3.3 Data Volume Replication Combined with Log Backup Volume Replication ............................. 15
  3.4 Comparison of Asynchronous Storage Replication Approaches ............................................. 16

4 Installation and Configuration Steps ......................................................................................... 17
  4.1 Lab Setup ................................................................................................................................... 17
  4.2 Disaster Recovery Configuration Overview .............................................................................. 19
  4.3 Preparation of Disaster Recovery Storage .................................................................................. 19
  4.4 Snap Creator Configuration ....................................................................................................... 22

5 Disaster Recovery Failover Testing ............................................................................................ 26
  5.1 Preparation of Target Server ...................................................................................................... 27
  5.2 Creation of FlexClone Copies of Database, Log Backup, and Binary Volumes ......................... 29
  5.3 Requirement to Split FlexClone Copies .................................................................................... 32
  5.4 Mount Volumes Test at Target Server and Start SAP Services .............................................. 32
  5.5 Recovery Test with SAP HANA Studio Excluding Log Files .................................................. 33
  5.6 Recovery Test with SAP HANA Studio Including Log Files ................................................... 37
  5.7 Test Start SAP System .............................................................................................................. 42

6 Disaster Failover ........................................................................................................................ 42
  6.1 Preparation of Disaster Recovery Server .................................................................................. 43
  6.2 Breaking SnapMirror Replication Relationship ....................................................................... 45
  6.3 Restoring SAP HANA Database Data Volume ......................................................................... 47
  6.4 Mount Volumes at Target Server and Start SAP Services ...................................................... 49
  6.5 Recovery with SAP HANA Studio Excluding Log Files ........................................................... 49
  6.6 Recovery with SAP HANA Studio Including Log Files ............................................................ 49
  6.7 Start the SAP System ............................................................................................................... 50
LIST OF TABLES
Table 1) Disaster recovery solution comparison..............................................................................12
Table 2) Comparison of asynchronous storage replication approaches...............................................17
Table 3) List of volumes and storage replication. ................................................................................18
Table 4) Protection relationships for SVM disaster recovery.................................................................21
Table 5) Schedules for an RPO of multiple hours. .............................................................................25
Table 6) Schedules for an RPO of less than one hour. .........................................................................26
Table 7) Volume names of FlexClone copies. ....................................................................................28
Table 8) Volume names at disaster recovery storage. ........................................................................44

LIST OF FIGURES
Figure 1) Data protection overview..................................................................................................4
Figure 2) NetApp storage–based backups. .........................................................................................8
Figure 3) Synchronous storage replication.........................................................................................9
Figure 4) Asynchronous storage replication......................................................................................10
Figure 5) SAP system replication with dedicated DR servers.............................................................11
Figure 6) SAP system replication with shared servers—cold standby. ...........................................12
Figure 7) Combine backup and disaster recovery replication............................................................14
Figure 8) Replication of data volume only. .........................................................................................15
Figure 9) Data replication combined with log backup replication.......................................................16
Figure 10) Lab setup. ........................................................................................................................18
Figure 11) Disaster recovery testing..................................................................................................27
1 Data Protection Overview

Studies have shown that business application downtime has a significant negative impact on the business of enterprises. Such downtime has not only a financial impact, but it can also affect the company’s reputation, staff morale, and customer loyalty. Downtime can therefore be very damaging. Surprisingly, not all companies have a comprehensive disaster recovery policy.

Running SAP HANA on NetApp storage 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 so that customers can select metrics that support their business needs.

To develop a comprehensive disaster recovery policy, customers must understand the business application requirements and technical capabilities needed for data protection and disaster recovery. An overview of this subject is shown in Figure 1. A typical two-site architecture is shown. This model addresses a disaster such as a complete failure of the primary data center.

Figure 1) Data protection overview.

Business application requirements

- 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 could differ if you are protecting against hardware failures within a single site. They might also differ if you are preparing for catastrophic disasters such as the loss of a complete data center. 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 available.
High Availability

The infrastructure hardware for SAP HANA, such as server, network, and storage, must have redundant components to ensure that there is no single point of failure.

Failures on the network side are typically addressed with redundant network paths to different network components. Storage systems usually offer failover capabilities to another storage controller. As a result, failures in these redundant systems should not cause any application downtime.

To provide high availability on the server and application side, standby SAP HANA nodes can be configured for built-in high availability with SAP HANA. If a server or an application fails, the SAP HANA service fails over to the standby node. The failover to the standby node 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 system replication is discussed in more detail in the chapter “Disaster Recovery Solution Comparison.”

Addressing 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 within an SAP application. SAP applications very 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, NetApp recommends fixing the logical error within the system. For this scenario, you should 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 would be lost.

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, backup must be combined with synchronous data replication.

The RTO for restore and recovery is defined by the needed 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.

On the other hand, a backup solution must address logical corruption, because data replication solutions cannot cover all kinds of logical corruption. For more details, see the section “Backup and Recovery.”

Synchronous or Asynchronous Data Replication

The RPO primarily determines which data replication method you should use. If the RPO must be zero, the data must be replicated synchronously. However, there are technical limitations for synchronous...
replication such as the distance between the two data centers. In most cases, synchronous replication is not appropriate for distances larger than 100km. Indeed, synchronous replication over a large distance places significant demands on the network infrastructure between the two data centers and therefore can be very expensive.

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.

**Hot or Cold Standby Server**

The startup time for an SAP HANA database is much longer relative to 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, the SAP HANA database must be started in case of failover to the disaster recovery site (the cold standby server).

SAP HANA system replication offers an operation mode in which the data is preloaded and continuously updated at the disaster recovery server. This mode enables very low RTO values, and yet it also requires a dedicated server that is only used to receive the replication data from the source system.

---

**2 Disaster Recovery Solution Comparison**

A comprehensive disaster recovery solution must enable customers to recover from a complete failure of the primary site. Therefore, data must be transferred to the secondary site, and a complete infrastructure is necessary to run the required production SAP HANA systems in case of site failure.

In addition to the RPO and RTO, there are additional infrastructure and business metrics that can help you identify the best implementation for your needs. Additional metrics include the following:

- Resource usage at the second site during standard operations. Are the servers available for different workloads or are they allocated explicitly for the disaster recovery setup?
  - Cold standby. Servers at the disaster recovery site are available for dev/test during standard operations.
  - Hot standby. Servers at the disaster recovery site are exclusively allocated for disaster recovery and the database data is preloaded into memory.
  - Costs for hot or cold standby.
- Distance between the sites.
  - Physical limitations for synchronous replication because of increasing latency
  - Availability and costs for the network connectivity between the sites
- Impact on the required bandwidth to synchronize the data between the sites.
  - Bandwidth requirement increase for lower RPO values.
- Could the data at the second site be used as the basis for dev or test systems?

The following options are compared and discussed in more detail in the following sections.

- Backup and recovery
- Synchronous storage replication
- Asynchronous storage replication
- SAP system replication
  - Dedicated DR servers—hot standby
  - Shared DR servers—cold standby
2.1 Backup and Recovery

SAP HANA supports different methods for database backups:

- File-based backup to a file system, typically an NFS share
- Backups using the SAP HANA BACKINT API and certified third-party backup tools
- Storage-based snapshot backups

To choose the best method, customers must understand the infrastructure and performance impact as well as the additional required features of the selected HANA backup method. The following sections provide a few examples.

File-Based Backups

With file-based backups or backups using the BACKINT API, the SAP HANA database server reads the data from the primary storage. The database server then writes the data to either an NFS share or streams the data to a backup server using the third-party backup tool. Both approaches have a significant impact on the performance of the SAP HANA database in the following ways:

- Additional CPU load at the SAP HANA database server
- Additional I/O load at the primary storage
- The load on the backup network

In addition, the backup run time, specifically for larger databases, can also be significant, resulting in lower operation speed during backup. The restore and recovery process can also be a challenge because of the long run time.

Storage-Based Snapshot Backups

NetApp storage-based Snapshot backups address the challenges discussed above. Independent of the size of the SAP HANA database, a Snapshot backup is executed within a few seconds instead of hours. The backup is executed at the storage layer, and there is no impact on the performance of the SAP HANA database. Also, the restore process occurs in a matter of seconds, which has a significant impact on the RTO if a restore operation is required.

The NetApp Snap Creator framework with the SAP HANA plug-in can facilitate an automated and fully integrated Snapshot based HANA backup, including the automation of SAP HANA block integrity checks.

Snap Creator also handles the scheduling and housekeeping of backups on the storage and within the SAP HANA backup catalog based on flexible, configurable retention policies. In addition, non-database files can be included in the backup schedule and strategy. For more details, see the technical report SAP HANA Backup and Recovery by Using Snap Creator.

Addressing Logical Corruption

As discussed in the chapter “Data Protection Overview,” a logical corruption within a production SAP system can typically not be addressed by a point-in-time recovery of the SAP HANA database. A point-in-time recovery would result in data loss and in an inconsistent SAP landscape if multiple SAP systems are exchanging data with each other. Rather, NetApp recommends fixing the logical corruption by setting up a repair system, exporting the required data, and importing that data back to the production system.

When setting up the repair system, flexibility and speed are critical. With NetApp storage-based Snapshot backups, multiple consistent database images are available to create a clone of the production system using NetApp FlexClone® technology. FlexClone copies can be created in a matter of seconds rather than multiple hours if a redirected restore from a file-based backup is used to set up the repair system. The chapter “Disaster Recovery Failover Testing” describes the process of setting up a
production clone for disaster recovery testing purposes. The same workflow can be used to set up a repair system.

Figure 2) NetApp storage–based backups.

- No site failure protection
- RPO = 30 min (worst case with 15 min standard log backup frequency)
- RTO = recovery + database start
- Multiple backups and offsite backups to address logical corruption

Figure 2 shows an example of a backup solution using NetApp storage–based Snapshot backups to secure the system on the primary site. Backups can be automatically transferred by using NetApp SnapVault® backup software to a dedicated off-site backup storage system. This process is controlled by Snap Creator. All of the backups available at the primary or off-site backup storage site can be used to create FlexClone copies and to set up a repair system to address logical corruption.

The following sections combine this backup approach with different options for disaster recovery replication.

2.2 Synchronous Storage Replication

If the RPO requirement is 0 and the required RTO is in the range of 30 minutes or longer, synchronous storage replication based on NetApp MetroCluster™ high-availability and disaster recovery storage software can be used. This disaster recovery solution does not require any additional configuration at the SAP HANA level.

NetApp MetroCluster is supported up to a distance of 300km. In reality, the maximum distance is determined by the maximum acceptable latency.

The SAP HANA data and log volumes and the nondatabase data are synchronously replicated to the disaster recovery site, as shown in Figure 3. During normal operation, the disaster recovery servers can run development or test systems. In the event of a disaster, the dev/test systems must be shut down and MetroCluster failover must be initiated at the storage layer to make the mirrored plexes available to the disaster recovery server.

After mounting the data at the disaster recovery server, you must run a normal SAP HANA database start, including crash recovery. The RTO for 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 400MBps (the key performance indicator [KPI] for data read defined by SAP), loading 1TB of data takes approximately 45 minutes.
All storage Snapshot copies stored at the primary site are also available at the secondary site. So even after a disaster failover, multiple replication images are available to address logical corruption.

### 2.3 Asynchronous Storage Replication

If the RPO and RTO requirements are in the range of 30 minutes or longer, you can use asynchronous storage replication. This disaster recovery solution does not require any additional configuration at the SAP HANA level.

**Note:** RPO values of less than 30 minutes are possible. However, to reduce the RPO to this level, you must reduce the default log backup interval to 15 minutes. In addition, you must determine the overall impact of a shorter log backup interval.

This approach combines a Snap Creator backup solution with additional data replication to the disaster recovery site with NetApp SnapMirror data replication software. Each backup of database and nondatabase data created at the primary site is replicated to the disaster recovery site, as shown in Figure 4.

The RPO depends on the frequency of backups and how fast backups can be transferred. In theory the maximum distance is unlimited, but in reality the limit depends on the amount of data that must be transferred and the connection that is available between the data centers.

During normal operation, the disaster recovery servers can be used to run development or test systems. A refresh of data for dev/test (an SAP system copy) can be accomplished by creating FlexClone copies at the disaster recovery site. Disaster recovery testing can be accomplished without interrupting or influencing replication by creating FlexClone copies at the disaster recovery site.

In the event of a disaster, the dev/test systems must be shut down and the failover must be initiated at the storage layer to make the SnapMirror target volumes available to the disaster recovery server. After mounting the data at the disaster recovery server, the SAP HANA database must be recovered using the normal recovery process, for example, with SAP HANA Studio. 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 400MBps (the KPI for data read defined by SAP), loading 1TB of data would take approximately 45 minutes.

All storage Snapshot copies stored at the primary site are also available at the secondary site. So even after a disaster failover, multiple replication images are available to address logical corruption.
This solution is described in detail in the chapter "Asynchronous Storage Replication" and in the following sections.

2.4 SAP HANA System Replication

SAP HANA system replication occurs at the application 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 two different modes:

- Hot standby, with a dedicated server at the disaster recovery site
  The server is exclusively used as an SAP HANA system replication secondary.
- Cold standby, with a shared server at the disaster recovery site
  The server is used as an SAP HANA system replication secondary and as a dev/test system.

You can find a complete description of all configuration options and replication scenarios in the HANA Administration Guide.

SAP HANA System Replication with Dedicated DR Servers—Hot Standby

Very low RTO values with SAP HANA can be achieved only with a hot standby solution. Operating SAP HANA system replication with a dedicated secondary server at the disaster recovery site allows an RTO value of approximately one 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 can also be used for near-zero-downtime maintenance operations.

If the required RPO is zero, SAP HANA system replication can be configured to replicate synchronously, as shown in Figure 5. The maximum supported distance for synchronous replication is in the range of 100km. If the RPO is higher, asynchronous replication can also be configured.

SAP HANA system replication does not include replication of nondatabase files, so any system changes outside of the database require an additional replication method. Therefore, SAP HANA system replication is typically combined with storage-based replication for nondatabase data.

Since SAP HANA system replication does not address logical corruption, it is important to combine the solution with a backup approach that addresses this type of corruption, such as a NetApp backup solution.
SAP System Replication with Shared DR Servers—Cold Standby

If your RTO requirement is 30 minutes or longer, you can use SAP HANA system replication as a cold standby solution. In this operational mode, the data at the disaster recovery site is not loaded into memory. The server at the disaster recovery site is still used to process SAP HANA system replication running all of the required SAP HANA processes. However, most of the server’s memory is available to run other workloads, 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 400MBps (the KPI for data read defined by SAP), loading 1TB of data should take approximately 45 minutes.

Figure 6 shows SAP HANA system replication with asynchronous replication. For an RPO of zero, this system can also be configured to replicate synchronously.

Since SAP HANA system replication does not address logical corruption, it is important to combine the solution with a backup approach that addresses this type of corruption, such as a NetApp backup solution.
2.5 Summary

Table 1 compares the disaster recovery solutions discussed in this chapter and highlights the most important indicators.

The key findings are:

- If a very low RTO is required, SAP HANA system replication in hot standby mode is the only option.
  - Storage replication is also needed to replicate nondatabase data.
- For medium RTO requirements, storage replication can also be used:
  - To combine database and nondatabase data replication
  - To cover additional use cases such as dev/test refresh
- All disaster recovery solutions must be combined with a backup solution that addresses logical corruption.

Table 1) Disaster recovery solution comparison.

<table>
<thead>
<tr>
<th></th>
<th>SAP HANA System Replication with Dedicated Disaster Recovery Servers</th>
<th>SAP HANA System Replication with Shared Disaster Recovery Servers</th>
<th>NetApp Snap Creator and SnapMirror</th>
<th>NetApp MetroCluster</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RTO</strong></td>
<td>Very low—hot standby</td>
<td>Medium—cold standby</td>
<td>Medium—cold standby</td>
<td>Medium—cold standby</td>
</tr>
<tr>
<td><strong>RPO = 0 min</strong></td>
<td>Synchronous replication</td>
<td>Synchronous replication</td>
<td>N/A</td>
<td>Synchronous replication</td>
</tr>
<tr>
<td><strong>RPO &gt;30 min</strong></td>
<td>Asynchronous replication</td>
<td>Asynchronous replication</td>
<td>Asynchronous replication</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Servers can be used for dev/test</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### 3 Asynchronous Storage Replication

#### 3.1 Combine Backup and Disaster Recovery Replication

The creation of database-consistent storage Snapshot backups at the production site is the core of this solution. The database-consistent Snapshot backups are created using the Snap Creator framework with the SAP HANA plug-in. These database-consistent images are replicated to an off-site backup site as well as to the disaster recovery site.

Snap Creator is used to execute replication to both sites during the normal Snapshot backup workflow. Figure 7 shows a high-level overview of the solution process. The following steps are performed during the backup workflow with Snap Creator:

- Trigger an SAP HANA backup savepoint to get a consistent image on the persistence layer.
- Create a storage Snapshot copy at the production site.
- Register a backup within the SAP HANA backup catalog.
- Execute a replication update to the off-site backup site using SnapVault.
- Execute a replication update to the disaster recovery site using SnapMirror.
- Perform retention management and housekeeping for data and log backups.

Because the replication to the disaster recovery site is part of the backup process, the replication frequency of the SAP HANA data volume depends on the backup frequency.

**Note:** An off-site backup is not required. However, we use one in the configuration example in this document.

<table>
<thead>
<tr>
<th>Replication of nondatabase data</th>
<th>SAP HANA System Replication with Dedicated Disaster Recovery Servers</th>
<th>SAP HANA System Replication with Shared Disaster Recovery Servers</th>
<th>NetApp Snap Creator and SnapMirror</th>
<th>NetApp MetroCluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Disaster recovery image usable for dev/test refresh</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Multiple images to address logical corruption</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
3.2 Replication of Data Volume Only

Figure 8 provides an overview of a disaster recovery solution that is based on the replication of the SAP HANA database data volume. The log backup volume is not replicated. This figure only shows HANA database replication. However, other data, such as HANA binaries and SAP binaries, must also be replicated. A more detailed description of how these volumes are replicated is covered in the chapter "Installation and Configuration Steps."

The RPO is defined by the replication frequency of the data volume. Replication to the DR site is part of the normal backup workflow. Therefore, a higher replication frequency can be achieved only by adopting a higher backup frequency. In general, NetApp does not recommend having a backup interval of less than 30 minutes. Based on this recommendation, the lowest achievable RPO is between 30 and 60 minutes.

In the event of a disaster failover, the RTO is defined by the time required to recover the database without forward recovery plus the time needed for infrastructure preparations.
From a high-level perspective, the following steps must be performed in the event of a disaster failover.

- **Storage operations**
  - Break the SnapMirror replication relationship.
  - Perform a SnapRestore restore to the last consistent backup.

- **Operations at the disaster recovery server on the operating system level**
  - Mount storage volumes.

- **Recovery with SAP HANA Studio**
  - Recover the database to a specific data backup or storage Snapshot copy.
  - Specify a backup without a catalog.

- **Start the SAP system**

### 3.3 Data Volume Replication Combined with Log Backup Volume Replication

Figure 9 provides an overview of a disaster recovery solution based on the replication of the SAP HANA database data volume plus the replication of the log backup volume.

The data volume is replicated with a lower frequency and the RPO is defined by the replication frequency of the log backup volume. The RPO is between 15 and 30 minutes with the standard SAP HANA log backup interval of 15 minutes and a log backup replication interval of, for example, 10 minutes.

Because log-backup volume replication is performed independent of the log-backup process executed by the SAP HANA database, there could be open, inconsistent log backup files at the disaster recovery site. Only the latest log backup files might be inconsistent, and therefore those files should be checked before a forward recovery is performed at the disaster recovery site.

In the event of a disaster failover, the RTO is defined by the time required to recover the database, including the forward recovery time plus the time needed for infrastructure preparations.
From a high-level perspective, the following steps must be executed in the event of a disaster failover.

- **Storage operations**
  - Break the SnapMirror replication relationship.
  - Perform a SnapRestore restore to the last consistent backup.
- **Operations at the disaster recovery server on the operating system level**
  - Mount storage volumes.
  - Check the consistency of the latest log backups with the `hdbbackupcheck` tool.
- **Recovery with SAP HANA Studio**
  - If the latest log backups are consistent:
    - Recover the database to its most recent state.
    - Enter the path to the mounted log backup volume.
    - Select Data Backup within HANA Studio.
    - Select Check Availability of Log Backups on File System.
    - Select Initialize Log Area.
  - If the latest log backups are inconsistent:
    - Delete or rename the log backup set that includes the inconsistent log file.
    - Recover the database to its most recent state.
    - Enter the path to the mounted log backup volume.
    - Select Data Backup within HANA Studio.
    - Select Check Availability of Log Backups on File System.
    - Select Initialize Log Area.
- **Start the SAP system**

### 3.4 Comparison of Asynchronous Storage Replication Approaches

Table 2 provides a summary and comparison of the two asynchronous storage replication approaches.
Table 2) Comparison of asynchronous storage replication approaches.

<table>
<thead>
<tr>
<th></th>
<th>Data Replication Only</th>
<th>Data Replication Combined with Log Backup Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RPO</strong></td>
<td>Depends on the data volume replication frequency and the minimum recommended SAP HANA backup interval</td>
<td>Depends on the log backup replication frequency and the log backup interval</td>
</tr>
<tr>
<td><strong>Lowest achievable RPO</strong></td>
<td>60 minutes, with a minimum 30-minute data-volume replication interval</td>
<td>30 minutes, with the standard 15-minute log backup interval and, for example, a 10-minute log backup replication interval</td>
</tr>
<tr>
<td><strong>RTO</strong></td>
<td>Storage and server preparation and cold database start</td>
<td>Storage and server preparation, cold database start, and forward recovery</td>
</tr>
</tbody>
</table>

### 4 Installation and Configuration Steps

#### 4.1 Lab Setup

Figure 10 shows the schematic lab setup with the relevant SnapVault and SnapMirror relationships for backup and disaster recovery. Details for the disaster recovery setup are explained in the following sections. For details on configuring the Snap Creator framework with the HANA plug-in for data protection, see the technical report *SAP HANA Backup and Recovery by Using Snap Creator*.

The following software versions were used in the lab setup:

- SAP NetWeaver system PNW: SAP NetWeaver 7.4 ABAP stack
- SAP HANA database P01: SAP HANA SPS11
- SUSE Linux SLES 11 SP3
- NetApp clustered Data ONTAP® 8.3.2 software

Three storage virtual machines (SVMs) were configured on the storage system, as shown in Figure 10.

- SVM hana: Primary storage system for the production SAP system
- SVM backup: Off-site backup storage system
- SVM disaster-recovery: Storage system used as a disaster recovery target
Table 3 shows the list of volumes on SVM hana and the replication for off-site backup and disaster recovery purposes.

**Note:** The SAP HANA log volume is not replicated for backup or for disaster recovery. The backup of the log volume is handled by the SAP HANA database and the log backup target is replicated with SnapMirror to the disaster recovery site.

**Table 3) List of volumes and storage replication.**

<table>
<thead>
<tr>
<th>Description</th>
<th>Storage Volume</th>
<th>Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA P01 data volume</td>
<td>P01_data_mnt00001</td>
<td>SnapVault and SnapMirror</td>
</tr>
<tr>
<td>SAP HANA P01 log volume</td>
<td>P01_log_mnt00001</td>
<td>No</td>
</tr>
<tr>
<td>SAP HANA P01 user home directory</td>
<td>P01_usr_sap</td>
<td>SnapVault and SnapMirror</td>
</tr>
<tr>
<td>SAP HANA P01 binaries</td>
<td>hana_shared</td>
<td>SnapVault and SnapMirror</td>
</tr>
<tr>
<td>SAP HANA P01 log backup</td>
<td>log_backup</td>
<td>SnapMirror</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>PNW_usr_sap</td>
<td>SnapVault and SnapMirror</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>PNW_sapmnt</td>
<td>SnapVault and SnapMirror</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>trans</td>
<td>SnapVault and SnapMirror</td>
</tr>
</tbody>
</table>

The HANA database is configured to write log backups to the mounted log backup volume, as shown in the following screenshot.
4.2 Disaster Recovery Configuration Overview

The following steps are required to configure the disaster recovery solution:

1. Prepare SVM disaster-recovery and configure the SnapMirror relationships.
2. Configure Snap Creator to automatically replicate the SAP HANA data volume to the disaster recovery site after a database-consistent Snapshot backup is created.
3. Configure Snap Creator to automatically replicate all nondatabase volumes to the disaster recovery site after a Snapshot backup is created.
4. Configure schedules within Snap Creator for backup and replication of database and nondatabase volumes.

4.3 Preparation of Disaster Recovery Storage

For all volumes replicated to the disaster recovery site, you must create the protection relationship. The following section shows the NetApp OnCommand® System Manager Create Protection Relationship workflow:

1. Within OnCommand System Manager, select the Protection folder of the target, SVM Disaster Recovery.
2. Click Create to start the Create Protection Relationship workflow.
3. In the dialog window, the mirror relationship type and the source cluster name is Preselected.
4. If the source and target volumes are on the same cluster, then select the source SVM by clicking Browse.
5. A dialog window displaying all of the available SVMs in the clusters is shown, as seen in the following screenshot.
6. Select the source SVM (in our example, SVM hana) and click Select. The workflow returns to the previous window. If the SVM has not yet been peered, the peering is performed automatically.

7. In the Source Volume section, click Browse to select the source volume.
8. In the Destination Volume section, select New Volume and select the target aggregate.

9. In the Mirror Policy section, click Browse and select the MirrorAllSnapshots policy. Keep Initialize Relationship selected.

10. Do not select a schedule within the Schedule session, because the volumes are replicated within the backup workflow of Snap Creator.

11. By clicking Create, the workflow automatically creates the new volume, establishes the SnapMirror relationship, and starts the initial transfer of the data from source to target.

12. Repeat the workflow for all relevant volumes. In our example, the following protection relationships and volumes were created.

Table 4) Protection relationships for SVM disaster recovery.

<table>
<thead>
<tr>
<th>Source Volume</th>
<th>Target Volume</th>
<th>Type</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01_data_mnt0001</td>
<td>hana_P01_data_mnt0001_mirror</td>
<td>Mirror</td>
<td>None</td>
</tr>
<tr>
<td>P01_usr_sap</td>
<td>hana_P01_usr_sap_mirror</td>
<td>Mirror</td>
<td>None</td>
</tr>
<tr>
<td>PNW_sapmnt</td>
<td>hana_PNW_sapmnt_mirror</td>
<td>Mirror</td>
<td>None</td>
</tr>
<tr>
<td>PNW_usr_sap</td>
<td>hana_PNW_usr_sap_mirror</td>
<td>Mirror</td>
<td>None</td>
</tr>
<tr>
<td>hana_shared</td>
<td>hana_hana_shared_mirror</td>
<td>Mirror</td>
<td>None</td>
</tr>
<tr>
<td>trans</td>
<td>hana_trans_mirror</td>
<td>Mirror</td>
<td>None</td>
</tr>
<tr>
<td>log_backup</td>
<td>hana_log_backup_mirror</td>
<td>Mirror</td>
<td>Every 15 minutes</td>
</tr>
</tbody>
</table>

Note: If the disaster recovery strategy is based on forward recovery at the disaster recovery site, the log backups must be replicated as well.
The protection configuration for the log backup volume is similar to the workflow described above. The only differences are that the schedule must be defined at the storage layer and then it must be selected during the workflow. The following screenshot provides an example of the workflow.

4.4 Snap Creator Configuration

This section describes the additional configuration required to set up the disaster recovery solution. NetApp assumes that the data protection configuration has already been applied. See the technical report SAP HANA Backup and Recovery by Using Snap Creator for details on configuring Snap Creator for SAP HANA.

SAP HANA Data Volume

1. Open the Snap Creator GUI and select the P01 database backup profile followed by the Connection tab. Click Add and specify the credentials of the disaster recovery SVM.
2. SnapMirror replication for the data volume is configured within the Volumes tab. Select SVM hana and click Edit. The following screenshot shows the list of protected volumes. Select Next to proceed to the final dialog window. Move the data volume into the SnapMirror area and click Save to save the configuration.
3. The following screenshot shows the final volume configuration for the SAP HANA database volume.

4. As a final step, you must activate the SnapMirror update function. Select the SnapMirror Settings tab and set the SnapMirror Update field to Yes.
With these settings for the HANA data volume, each Snap Creator backup includes a SnapMirror update.

**Nondatabase Volumes**

The same procedure as described in the previous section must be applied for all nondatabase volumes. The following screenshot shows the volume configuration for any nondatabase volumes.

![Volume Configuration Screenshot](image)

**Backup and Replication Schedules**

Database backups and backups of nondatabase volumes can be scheduled and monitored with Snap Creator.

Table 5 shows an example of a configuration with an RPO of eight hours. If the RPO is multiple hours, you can just replicate the SAP HANA database data volume. You do not need to replicate the log backup volume. The schedule for database volume backup and replication is set to four hours. Therefore, data loss would be eight hours if the disaster happened close to the start of the next replication, a worst-case situation. Nondatabase volumes are also replicated every four hours. Because these volumes contain primarily static data, the interval could be higher.

**Table 5** Schedules for an RPO of multiple hours.

<table>
<thead>
<tr>
<th>RPO = 8 Hours</th>
<th>Snap Creator Schedule</th>
<th>Storage Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA database volume</td>
<td>Every four hours</td>
<td>None</td>
</tr>
<tr>
<td>Nondatabase volumes</td>
<td>Every four hours</td>
<td>None</td>
</tr>
<tr>
<td>Log backup volume</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 6 shows an example of a configuration with an RPO of less than one hour. The schedule for database volume backup and replication is set to four hours. The log backup volume is replicated every 15 minutes using a replication schedule defined on the storage layer. Therefore, data loss would be 30 minutes in the worst case of a disaster that happens just before the next replication starts.

Nondatabase volumes are also replicated every four hours. Because those volumes contain mainly static data, the interval could also be longer. The RTO would be higher relative to the previous example because you would also need to perform a forward recovery in the event of a disaster.

Table 6) Schedules for an RPO of less than one hour.

<table>
<thead>
<tr>
<th>RPO &lt;1 Hour</th>
<th>Snap Creator Schedule</th>
<th>Storage Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA database volume</td>
<td>Every four hours</td>
<td>None</td>
</tr>
<tr>
<td>Nondatabase volumes</td>
<td>Every four hours</td>
<td>None</td>
</tr>
<tr>
<td>Log backup volume</td>
<td>None</td>
<td>Every 15 minutes</td>
</tr>
</tbody>
</table>

The following screenshot shows a schedule configuration within Snap Creator.

5 Disaster Recovery Failover Testing

The best disaster recovery strategy is worthless without testing the required workflow. Testing not only demonstrates whether the strategy works and the internal documentation is sufficient, but it also allows administrators to train on the required procedures.

The use of NetApp FlexClone technology allows you to execute a disaster recovery failover test without influencing or interrupting the ongoing replication to the disaster recovery site. Therefore, a test can be run without influencing the RTO or the RPO.

Figure 11 shows a high-level overview of the disaster recovery test.
The test of the disaster recovery failover is performed with the following steps:

1. Prepare the target server.
2. Create FlexClone copies of the SAP HANA database, log backup, and binary volumes.
3. Mount volumes at the target server and start the SAP services.
4. Execute recovery with SAP HANA Studio:
   a. Without forward recovery
   b. With forward recovery using log backups
5. Start the SAP system.

The following sections describe the required steps in detail.

### 5.1 Preparation of Target Server

**Target Server Host Name and IP Address**

The host name of the target server has to be identical to the host name of the source system. The IP address can be different. If the SAP system and the HANA database have been installed and adaptive computing enabled, then the virtual host names for the SAP and SAP HANA services must be identical to the virtual host names of the source production system.

**Note:** You must establish proper fencing of the target server 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.

**Required Software Installation**

The SAP hostcontrol software must be installed at the target server.

**Users, Ports, and SAP Services Configuration**

The required users and groups for the SAP HANA database and SAP system must be available at the target server. Typically, central user management is used and therefore no configuration steps must be performed at the target server. The required ports for the SAP system must be configured at the target
hosts. The configuration could 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 could be copied from the source system by copying the /usr/sap/sapservice file to the target server. The following output shows the required entries for the SAP HANA database and the SAP NetWeaver system used in the lab setup.

```bash
stlrx300s8-5:/etc # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/P01/HDB02/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH=/usr/sap/P01/HDB02/exe/sapstartsrv
pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3 -D -u p01adm
LD_LIBRARY_PATH=/usr/sap/PNW/ASCS04/exe:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH;
pf=/usr/sap/PNW/ASCS04/exe/sapstartsrv pf=/usr/sap/PNW/SYS/profile/PNW_ASCS04_stlrx300s8-3 -D -u pnwadm
LD_LIBRARY_PATH=/usr/sap/PNW/DVEBMGS03/exe:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH;
pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u pnwadm
```

### SAP HANA Log Volume

A log volume for the SAP HANA database must be created at the disaster-recovery SVM and mounted at the target server.

```bash
stlrx300s8-3:~ # df
Filesystem 1K-blocks    Used  Available  Use% Mounted on
/dev/sda2   285762056  37695576  246905212  14% /
udev        66043064        0   66042760    0% /dev
tmpfs       100663296       816  100662480   1% /dev/shm
192.168.173.110:/DR_P01_log_mnt00001 149422080  128  149421952  1% /hana/log/P01/mnt00001
```

The required subdirectories within the mounted log volume must be created.

```bash
stlrx300s8-3:~ # cd /hana/log/P01/mnt00001/
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00001
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00002
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00003
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00004
stlrx300s8-3:/hana/log/P01/mnt00001 # chmod -R 777 mnt00001/
```

### Preparation of File System Mounts in /etc/fstab

Table 7 shows the naming convention used in the lab setup. The volume names for the FlexClone copies at the disaster recovery storage are used as /etc/fstab entries. These volume names are used in the FlexClone copy creation step in the next section.

<table>
<thead>
<tr>
<th>Description</th>
<th>Storage Volume at Disaster Recovery Storage</th>
<th>FlexClone Copy at Disaster Recovery Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA P01 data volume</td>
<td>hana_P01_data_mnt00001_mirror</td>
<td>hana_P01_data_mnt00001_mirror_clone</td>
</tr>
<tr>
<td>SAP HANA P01 user home directory</td>
<td>hana_P01_usr_sap_mirror</td>
<td>hana_P01_usr_sap_mirror_clone</td>
</tr>
<tr>
<td>SAP HANA P01 binaries</td>
<td>hana_hana_shared_mirror</td>
<td>hana_hana_shared_mirror_clone</td>
</tr>
<tr>
<td>SAP HANA P01 log backup</td>
<td>hana_log_backup_mirror</td>
<td>hana_log_backup_mirror_clone</td>
</tr>
<tr>
<td>Description</td>
<td>Storage Volume at Disaster Recovery Storage</td>
<td>FlexClone Copy at Disaster Recovery Storage</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>hana_PNW_usr_sap_mirror</td>
<td>hana_PNW_usr_sap_mirror_clone</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>hana_PNW_sapmnt_mirror</td>
<td>hana_PNW_sapmnt_mirror_clone</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>hana_trans_mirror</td>
<td>hana_trans_mirror_clone</td>
</tr>
</tbody>
</table>

The required `/etc/fstab` entries are shown below.

```bash
stlrx300s8-3:~ # cat /etc/fstab
/dev/disk/by-id/scsi-360030057013a54201aa3727d258af07f-part1 swap swap defaults 0 0
/dev/disk/by-id/scsi-360030057013a54201aa3727d258af07f-part2 / ext3 acl,user_xattr 1 1
proc /proc proc defaults 0 0
sysfs /sys sysfs noauto 0 0
devpts /dev/pts devpts mode=0620,gid=5 0 0
# SnapMirror DR
disaster-recovery:/DR_P01_log_mnt00001 /hana/log/P01/mnt00001 nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_P01_data_mnt00001_mirror_clone /hana/data/P01/mnt00001 nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_P01_usr_sap_mirror_clone /usr/sap/P01 nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_PNW_usr_sap_mirror_clone /usr/sap/PNW nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_PNW_sapmnt_mirror_clone /sapmnt/PNW nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_trans_mirror_clone /usr/sap/trans nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_hana_shared_mirror_clone/P01 /hana/shared/P01 nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,actimeo=0,noatime,nolock 0 0
disaster-recovery:/hana_log_backup_mirror_clone /mnt/log_backup nfs rw,vers=3,hard,timeo=600,rsize=65536,wsize=65536,actimeo=0,noatime,nolock 0 0
```

5.2 Creation of FlexClone Copies of Database, Log Backup, and Binary Volumes

FlexClone copies are created using NetApp OnCommand System Manager.

1. The following screenshot shows FlexClone copy creation for the SAP HANA data volume.

   **Note:** The name of the volume must be identical to the name used in the `/etc/fstab` configuration shown in Table 7.
2. The following screenshot shows FlexClone copy creation for the /usr/sap/P01 file system of the SAP HANA database.

   **Note:** Because the binary volumes are replicated with a different schedule than the database data volume, you must select a reasonable Snapshot backup. In our example, we selected a Snapshot backup that was created just before the SAP HANA data-volume Snapshot backup.
For all other binary volumes, you must perform the same procedure.

3. If the log backup volume is part of the replication approach, a FlexClone copy of the log backup volume must be created as well. The following screenshot shows FlexClone copy creation for the log backup volume.
4. When all FlexClone copies have been created, they must be mounted to the namespace using NetApp OnCommand System Manager, as shown in the following screenshot.

![NetApp OnCommand System Manager](image)

5.3 Requirement to Split FlexClone Copies

FlexClone copies at the disaster recovery storage result in busy Snapshot copies. These Snapshot copies cannot be deleted before the FlexClone copy is split or deleted.

Database and Nondatabase Volumes

If the retention time of a Snapshot backup is exceeded, Snap Creator deletes the Snapshot backup at the primary storage. The subsequent replication update to the disaster recovery site fails if this Snapshot backup has been used to create the FlexClone copy at the disaster site. Therefore, the FlexClone copies of the database and nondatabase volumes must be split when the disaster recovery test takes longer than the retention time of the Snapshot backups used to create the FlexClone copies.

Log Backup Volume

Replication of the log backup volume is not affected by the FlexClone copy. Instead, additional Snapshot copies are kept in the replicated volume at the disaster recovery storage. These Snapshot copies must be deleted manually after disaster testing. In a manner similar to that of the SAP HANA data volume, you must split the FlexClone copy if the testing takes longer, and you risk exceeding the maximum number of 255 Snapshot copies.

5.4 Mount Volumes Test at Target Server and Start SAP Services

To mount volumes at the target server and start SAP services, complete the following steps:

1. To mount the volumes, run the `mount -a` command.

```
stlrx300s8-3:~ # mount -a
stlrx300s8-3:~ #
```
To start SAP services, run the `service sapinit start` command.

```
stlrx300s8-3:~ # service sapinit start
start hostcontrol using profile /usr/sap/hostctrl/exe/host_profile
```

5.5 Recovery Test with SAP HANA Studio Excluding Log Files

If your disaster recovery strategy is based only on database data volume replication, recovery with SAP HANA Studio is performed by recovering the Snapshot copy backup without forward recovery.

1. Select Recover System within SAP HANA Studio.
2. Select Recover the Database to a Specific Data Backup or Storage Snapshot.

3. Select Specify Backup Without Catalog.
4. Select Snapshot in the Destination Type field.

5. No input is required in the Other Settings dialog box.
6. **Click Finish** to start the recovery process.

7. The following screenshot shows the successful recovery process.
5.6 Recovery Test with SAP HANA Studio Including Log Files

If your disaster recovery strategy is based on a database data volume and log backup replication, recovery with SAP HANA Studio includes a forward recovery using the replicated log backup files.

Because the backup of log segments and the replication of log backups are independent of each other, the replicated volume might include open files from the SAP HANA log backup process. Therefore, you must check the consistency of the latest log backups using the `hdbbackupcheck` tool from SAP before recovery starts.

Checking Consistency of Latest Log Backups

List the latest log backups by running the `ls -ahtlr` command in the log backup directory. The following screenshot shows the latest log backups in the lab environment.

The names of the log backup files include the volume ID of the SAP HANA services, where `log_backup_0_0_0_0*` is the SAP HANA backup catalog. In the example lab setup, `log_backup_1*` is the name of the server log backup, `log_backup_2*` is the index server log backup, and `log_backup_4*` is the XSEngine log backup.
The latest log backups for these services must be checked using the `hdbbackupcheck` command, as shown in the following screenshot.

The output of the `hdbbackupcheck` tool shows that the latest log backups are consistent and you can perform a recovery that includes them.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or renamed in the log backup directory. In our example, the latest six log backups (3 x catalog backup, 1 x indexserver, 1 x nameserver, and 1 x XSEngine backup) need to be removed or renamed. The recovery can then be started with the option Recover the Database to Its Most Recent State, as described in the next section.

**Recovery with SAP HANA Studio**

1. Select Recover System within SAP HANA Studio.
2. Select Recover the Database to Its Most Recent State.

3. Select the log backup location.
4. The green icon shows that this backup exists on the file system and can be selected for recovery.

5. Select Initialize Log Area, because the recovery should be performed using the log backup files and there are no valid log segment files in the log area.
6. Click finish to start the recovery process.

7. The following screenshot shows the successful recovery process.
5.7 Test Start SAP System

The SAP system can now be started using the `startsap` command.

```
startsa
```

6 Disaster Failover

A disaster failover is accomplished with the following steps:

1. Prepare the disaster recovery server.
2. Break the SnapMirror relationships for the SAP HANA database, log backup, and binary volumes.
3. Restore the database data volume with SnapRestore to the latest Snapshot backup.
4. Mount volumes at the disaster recovery server and start SAP services.
5. Recover with SAP HANA Studio:
   c. Without forward recovery using log backups
   d. Including forward recovery with log backups
6. Start the SAP system.

The following chapters describe the required steps in detail.

6.1 Preparation of Disaster Recovery Server

**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. However, the IP address can be different. If the SAP system and the HANA database were installed and adaptive computing was enabled, then the SAP and SAP HANA service virtual host names must be identical to the source production system virtual host names.

**Required Software Installation**

The SAP hostcontrol software must be installed at the target server.

**Users, Ports, and SAP Services Configuration**

The required users and groups for the SAP HANA database and SAP system must be available at the target server. Typically, central user management is used and therefore no configuration steps must be performed at the target server.

The required ports for the SAP system must be configured at the target hosts. The configuration could 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/sapservice` file to the target server.

The following output shows the required entries for the SAP HANA database and the SAP NetWeaver in the example lab setup.

```
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/P01/HDB02/exe:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH
/pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3 -D -u p01adm
LD_LIBRARY_PATH=/usr/sap/P01/HDB02/exe/sapstartsrv
pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3 -D -u p01adm

LD_LIBRARY_PATH=/usr/sap/PNW/ASCS04/exe:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH;
/pf=/usr/sap/PNW/SYS/profile/PNW_ASCS04_stlrx300s8-3 -D -u pnwadm

LD_LIBRARY_PATH=/usr/sap/PNW/DVEBMGS03/exe:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH;
/pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u pnwadm
```

**SAP HANA Log Volume**

A log volume for the SAP HANA database must be created at the storage system and mounted at the target server.

```
stlrx300s8-3:$ cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/P01/HDB02/exe:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH;
/pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3 -D -u p01adm
LD_LIBRARY_PATH=/usr/sap/P01/HDB02/exe/sapstartsrv
pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3 -D -u p01adm

LD_LIBRARY_PATH=/usr/sap/PNW/ASCS04/exe:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH;
/pf=/usr/sap/PNW/SYS/profile/PNW_ASCS04_stlrx300s8-3 -D -u pnwadm

LD_LIBRARY_PATH=/usr/sap/PNW/DVEBMGS03/exe:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH;
/pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u pnwadm
```

```
stlrx300s8-3:$ df
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda2 285762056 37695576 246905212 14% /
udev 66043064 284 66042780 1% /dev
tmpfs 100663296 816 100662480 1% /dev/shm
disaster-recovery:/DR_P01_log_mnt00001 149422080 128 149421952 1%
/hana/log/P01/mnt00001
```
The required subdirectories within the mounted log volume must be created.

```
stlrx300s8-3:~ # cd /hana/log/P01/mnt00001/
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00001
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00002
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00003
stlrx300s8-3:/hana/log/P01/mnt00001 # mkdir hdb00004
stlrx300s8-3:/hana/log/P01/mnt00001 #
stlrx300s8-3:/hana/log/P01 # chmod -R 777 mnt00001/
```

Preparation of File System Mounts in /etc/fstab

Table 8 shows the naming convention used in the lab setup.

Table 8) Volume names at disaster recovery storage.

<table>
<thead>
<tr>
<th>Description</th>
<th>Storage Volume at Disaster Recovery Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA P01 data volume</td>
<td>hana_P01_data_mnt00001_mirror</td>
</tr>
<tr>
<td>SAP HANA P01 user home directory</td>
<td>hana_P01_usr_sap_mirror</td>
</tr>
<tr>
<td>SAP HANA P01 binaries</td>
<td>hana_hana_shared_mirror</td>
</tr>
<tr>
<td>SAP HANA P01 log backup</td>
<td>hana_log_backup_mirror</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>hana_PNW_usr_sap_mirror</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>hana_PNW_sapmnt_mirror</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>hana_trans_mirror</td>
</tr>
</tbody>
</table>

The required /etc/fstab entries are shown below.

```
stlrx300s8-3:-# cat /etc/fstab
/dev/disk/by-id/scsi-360030057013a54201aa3727d258af07f-part1 swap swap defaults 0 0
/dev/disk/by-id/scsi-360030057013a54201aa3727d258af07f-part2 / ext3
proc  /proc proc defaults 0 0
sysfs /sys sysfs noauto 0 0
devfs  /sys/kernel/debug debugfs noauto 0 0
usbfs  /proc/bus/usb usbfs noauto 0 0
devpts /dev/pts devpts mode=0620,gid=5 0 0

# SnapMirror DR
disaster-recovery:/DR_P01_log_mnt00001 /hana/log/P01/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_P01_data_mnt00001_mirror /hana/data/P01/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_P01_usr_sap_mirror /usr/sap/P01 nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_PNW_data_mnt00001_mirror /hana/data/PNW/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_PNW_sapmnt_mirror /sapmnt/PNW nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_PNW_usr_sap_mirror /usr/sap/PNW nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_PNW_trans_mirror /usr/sap/tranfs nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_hana_shared_mirror /P01 /hana/shared/P01 nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/hana_hana_mirror /P01 /hana/shared/P01 nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/mnt/log_backup nfs
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```

```
disaster-recovery:/mnt/log_backup mirror /mnt/log_backup mirror
rw,vers=3,hard,timeo=600,rsizew=1048576,wsizew=1048576,intr,actimeo=0,noatime,nolock 0 0
```
6.2 Breaking SnapMirror Replication Relationship

The storage volumes at the disaster recovery storage must be made read-writable so that they can be mounted and used at the disaster recovery server. Doing so is accomplished by breaking the SnapMirror relationship. The following screenshot shows NetApp OnCommand System Manager.

1. Select Protection within the disaster recovery SVM. Select the volume and then select Operations > Break.

2. Confirm that the relationship should be broken.
3. Proceed in the same way for all other required volumes. The following example depicts the breaking of all protection relationships.
4. To mount the volumes at the disaster recovery server, the volumes must be mounted to the storage system namespace. The following example depicts the mounted volumes.

6.3 Restoring SAP HANA Database Data Volume

The current active file system in the database data volume is not consistent from the SAP HANA database point of view because it is based on a SnapMirror Snapshot copy. This Snapshot copy was created after Snap Creator issued the `unquisce` command for the SAP HANA database. Therefore, the SAP HANA database data volume must be restored to the latest backup that was created with Snap Creator to get a consistent database image.

1. Select Volume within the disaster recovery SVM. Select the data volume and go to Snapshot Copies > Restore.
2. Select the latest Snap Creator Snapshot copy and click Restore.

All of the other volumes do not need to be restored because they contain only binaries and text files and no transactional data.
6.4 Mount Volumes at Target Server and Start SAP Services

To mount volumes at the target server and start SAP services, complete the following steps:

1. Mount the volumes by running the `mount -a` command.

```
mount -a
```

```
stlrx300s8-3:~ # mount -a
```

```
stlrx300s8-3:~ # df
```

Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda2 285762056 37684260 248077848 14% /
device 66043064 296 66042768 1% /dev

tmpfs 100663296 732 100662564 1% /dev/shm

```
disaster-recovery:/hana_P01_usr_sap_mirror 52428800 2624 52426176 1% /usr/sap/P01
```

```
disaster-recovery:/hana_PNW_usr_sap_mirror 52428800 2387712 50041088 5% /usr/sap/PNW
```

```
disaster-recovery:/hana_PNW_pamnt_mirror 52428800 852096 51576704 2% /sapmnt/PNW
```

```
disaster-recovery:/hana_trans_mirror 52428800 832 52427968 1% /usr/sap/trans
```

```
disaster-recovery:/hana_hana_shared_mirror/P01 1073741824 250068288 823673536 24% /hana/shared/P01
```

```
disaster-recovery:/hana_PNW_data_mnt00001_mirror 157286400 25601280 131685120 17% /hana/data/P01/mnt00001
```

2. Start the SAP services by running the `service sapinit start` command.

```
service sapinit start
```

```
start hostcontrol using profile /usr/sap/hostctrl/exe/host_profile
```

```
ps -ef | grep sap
```

```
root 5470 2689 0 07:42 pts/0 00:00:00 grep sap
p01adm 13058 1 0 Aug04 ? 00:00:00 sapstart
pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3
p01adm 13079 13058 0 Aug04 ? 00:00:22 /usr/sap/P01/HDB02/stlrx300s8-3/trace/hdb.sapP01_HDB02 -d -nw -f /usr/sap/P01/HDB02/stlrx300s8-3-daemon.ini
pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3
root 20333 1 0 Aug04 ? 00:00:10 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
sadm 20366 1 0 Aug04 ? 00:00:01 /usr/sap/hostctrl/exe/sapstartsrv
pf=/usr/sap/hostctrl/exe/host_profile -D
root 20392 1 0 Aug04 ? 00:09:42 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
p01adm 20459 1 0 Aug04 ? 00:18:05 /usr/sap/P01/HDB02/exe/sapstartsrv
pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3 -D -u p01adm
p01adm 20710 1 0 Aug04 ? 00:02:37 /usr/sap/PNW/ASCS04/exe/sapstartsrv
pf=/usr/sap/PNW/SYS/profile/PNW_ASCS04_stlrx300s8-3 -D -u p01adm
p01adm 20970 1 0 Aug04 ? 00:02:37 /usr/sap/PNW/DVEBMGS03/exe/sapstartsrv
pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u p01adm
```

6.5 Recovery with SAP HANA Studio Excluding Log Files

If your replication strategy is based on database backup replication, recovery with SAP HANA Studio is performed with Snapshot backups without forward recovery. Recovery with SAP HANA Studio is performed in the same way as described in the section “Recovery Test with SAP HANA Studio Excluding Log Files.”

6.6 Recovery with SAP HANA Studio Including Log Files

If your replication strategy is based on database backup and log backup replication, then recovery with SAP HANA Studio includes forward recovery using the replicated log backup files. The recovery with SAP HANA Studio is performed in the same way as described in the section “Recovery Test with SAP HANA Studio Including Log Files.”
6.7 Start the SAP System

The SAP system can now be started as described in the section “Test Start SAP System.”

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>March 2014</td>
<td>Initial version</td>
</tr>
<tr>
<td>Version 2.0</td>
<td>September 2016</td>
<td>Complete rewrite</td>
</tr>
</tbody>
</table>
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Fitness, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, SnapCopy, Snap Creator, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, StorageGRID, Tech OnTap, Unbound Cloud, WAFL, and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx.