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 NetApp® SnapCenter® 4.0 with the SAP HANA plug-in to manage database consistency.
# TABLE OF CONTENTS

1 Data Protection Overview .................................................................................................................. 4  
   1.1 Business Application Requirements ......................................................................................... 4  
   1.2 High Availability ...................................................................................................................... 5  
   1.3 Addressing Logical Corruption ............................................................................................... 5  
   1.4 Backups ................................................................................................................................... 5  
   1.5 Synchronous or Asynchronous Data Replication ....................................................................... 6  
   1.6 HANA System Replication with or Without Data Preload ....................................................... 6  

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 Disaster Recovery Configuration Steps ............................................................................................ 17  
   4.1 Lab Setup ............................................................................................................................... 17  
   4.2 Disaster Recovery Configuration Overview ............................................................................. 19  
   4.3 Configure Disaster Recovery for SAP HANA Data Volume .................................................. 20  
   4.4 Configure Disaster Recovery for Nondatabase Volumes ....................................................... 24  

5 Disaster Recovery Failover Testing .................................................................................................. 32  
   5.1 Prepare Target Server .............................................................................................................. 33  
   5.2 Create FlexClone Copies of Database, Log Backup, and Binary Volumes ............................. 35  
   5.3 Split or Delete FlexClone Copies ............................................................................................ 38  
   5.4 Mount Volumes at Target Server and Start SAP Services .................................................... 38  
   5.5 Execute Recovery with SAP HANA Studio ............................................................................. 39  
   5.6 Start SAP System ................................................................................................................... 48  

6 Disaster Failover Operation .............................................................................................................. 48  
   6.1 Prepare Disaster Recovery Server .......................................................................................... 49  
   6.2 Break SnapMirror Replication Relationship ......................................................................... 51
6.3 Restore SAP HANA Database Data Volume ................................................................. 53
6.4 Mount Volumes at Target Server and Start SAP Services ........................................... 54
6.5 Execute Recovery with SAP HANA Studio ..................................................................... 55
6.6 Start SAP System ........................................................................................................... 56

Where to Find Additional Information ................................................................................. 56

Version History ....................................................................................................................... 56

LIST OF TABLES
Table 1) Disaster recovery solution comparison................................................................. 12
Table 2) Comparison of asynchronous storage replication approaches ................................ 17
Table 3) Volumes and storage replication ........................................................................... 18
Table 4) Protection relationships for SVM disaster recovery ................................................ 19
Table 5) Schedules for an RPO of multiple hours. ............................................................... 20
Table 6) Schedules for an RPO of less than one hour .......................................................... 20
Table 7) Volume names of FlexClone copies .................................................................... 35
Table 8) Volume names at disaster recovery storage ......................................................... 50

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) Combined 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) Log backup configuration ................................................................................ 19
Figure 12) Protection relationships for disaster recovery ................................................. 26
Figure 13) Disaster recovery testing .................................................................................. 33
1 Data Protection Overview

Studies have shown that business application downtime has a significant negative impact on the business of enterprises. Such downtime not only has a financial impact, but also can affect the company’s reputation, staff morale, and customer loyalty. Downtime can therefore be 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.

1.1 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 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.
1.2 High Availability

The infrastructure hardware for SAP HANA, such as server, network, and storage, must have redundant components to make sure 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 SAP HANA service 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.”

1.3 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 are 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.

1.4 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 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.

In contrast, 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.”
1.5 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 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.

1.6 HANA System Replication with or Without Data Preload

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?
  - Servers at the disaster recovery site are available for dev/test during standard operations, and the database data is not preloaded into memory.
  - Servers at the disaster recovery site are exclusively allocated for disaster recovery, and the database data is preloaded into memory.
  - Costs for dedicated disaster recovery servers.
- 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?

These options are compared and discussed in more detail in the sections that follow:

- Backup and recovery
- Synchronous storage replication
- Asynchronous storage replication
- SAP system replication:
Dedicated DR servers with data preload
- Shared DR servers without data preload

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™ copy 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 subsections 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 either writes the data to 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 earlier. Independently 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.

NetApp SnapCenter 4.0 with the SAP HANA plug-in can facilitate an automated and fully integrated HANA backup based on Snapshot, including the automation of SAP HANA block integrity checks.

SnapCenter 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, nondatabase files can be secured with SnapCenter.

For more information, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.

SnapCenter 4.0 supports the following SAP HANA releases:

- SAP HANA single container:
  - SAP HANA 1.0 SPS7 and later
  - SAP HANA 2.0 up to SPS0
- SAP HANA multiple-database container (MDC) single tenant:
  - SAP HANA 2.0 SPS1 and higher
Addressing Logical Corruption

As discussed in the section “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 by 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 section “Disaster Recovery Failover Testing” describes the process for 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.

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 SnapCenter. All 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 zero 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. 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 1000MBps, loading 1TB of data takes approximately 18 minutes.

Figure 3) Synchronous storage replication.

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 15-minute log backup interval. In addition, you must determine the overall impact of a shorter log backup interval.

This approach combines a SnapCenter backup solution with additional data replication to the disaster recovery site with NetApp SnapMirror® data replication software. With SnapMirror 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, 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 1000MBps, loading 1TB of data would take approximately 18 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.

Figure 4) Asynchronous storage replication.

This solution is described in detail in the section titled “Asynchronous Storage Replication.”

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:

- With data preload, with a dedicated server at the disaster recovery site
  
  **Note:** The server is exclusively used as an SAP HANA system replication secondary.

- Without data preload, with a shared server at the disaster recovery site
  
  **Note:** 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 [SAP HANA Administration Guide](#).

SAP HANA System Replication with Dedicated DR Servers

Very low RTO values with SAP HANA can be achieved only with an SAP HANA system replication with data preload. 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.

Because 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.

Figure 5) SAP system replication with dedicated DR servers.

SAP System Replication with Shared DR Servers

If your RTO requirement is 30 minutes or longer, you can use SAP HANA system replication without data preload. 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 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 1000MBps, loading 1TB of data should take approximately 18 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.

Because 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 section 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
  - 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 Data Preload</th>
<th>SAP HANA System Replication Without Data Preload</th>
<th>NetApp SnapCenter and SnapMirror</th>
<th>NetApp MetroCluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTO</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>RPO = 0 minutes</td>
<td>Synchronous replication</td>
<td>Synchronous replication</td>
<td>N/A</td>
<td>Synchronous replication</td>
</tr>
<tr>
<td>RPO &gt; 18 minutes</td>
<td>Asynchronous replication</td>
<td>Asynchronous replication</td>
<td>Asynchronous replication</td>
<td>N/A</td>
</tr>
<tr>
<td>per 1TB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers can be used for dev/test</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Replication of nondatabase data</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SAP HANA System Replication with Data Preload</td>
<td>SAP HANA System Replication Without Data Preload</td>
<td>NetApp SnapCenter and SnapMirror</td>
<td>NetApp MetroCluster</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>Disaster recovery image usable for dev/test refresh</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td></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 Asynchronous Storage 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 by using SnapCenter 4.0 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.

#### 3.1 Combine Backup and Disaster Recovery Replication

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

1. Trigger an SAP HANA backup savepoint to get a consistent image on the persistence layer.
2. Create a storage Snapshot copy at the production site.
3. Register a backup within the SAP HANA backup catalog.
4. Initiate the replication update to the off-site backup site by using SnapVault.
5. Initiate the replication update to the disaster recovery site using SnapMirror.
6. Use the scheduled housekeeping task to perform retention management and housekeeping for data and log backups.

Because the replication to the disaster recovery site is part of the overall 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, an off-site backup was used in the configuration example in this document.
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 the SAP HANA database replication. However, other data, such as SAP HANA binaries and SAP binaries, must also be replicated. A more detailed description of how these volumes are replicated is covered in the section titled “Disaster Recovery 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 applying logs plus the time needed for infrastructure preparations.
In the event of a disaster failover, the following tasks must be completed:

- **Storage operations:**
  - Break the SnapMirror replication relationship.
  - Perform a SnapRestore® restore operation to restore 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 entry.

- **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 the 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.

In the event of a disaster failover, the RTO is defined by the time required to recover the database, including applying logs plus the time needed for infrastructure preparations.
In the event of a disaster failover, from a high-level perspective, the following tasks must be completed:

- Storage operations:
  a. Break the SnapMirror replication relationship.
  b. Perform a SnapRestore restore operation to the last consistent backup.
- Operations at the disaster recovery server on the operating system level:
  a. Mount storage volumes.
  b. Check the consistency of the latest log backups with the `hdbbackupcheck` tool.
- Recovery with SAP HANA Studio:
  **If the latest log backups are consistent, complete these steps:**
  a. Recover the database to its most recent state.
  b. Enter the path to the mounted log backup volume.
  c. Select Data Backup within HANA Studio.
  d. Select Check Availability of Log Backups on File System.
  e. Select Initialize Log Area.
  f. Start the SAP system.
  **If the latest log backups are inconsistent, complete these steps:**
  a. Delete or rename the log backup set that includes the inconsistent log file.
  b. Recover the database to its most recent state.
  c. Enter the path to the mounted log backup volume.
  d. Select Data Backup within HANA Studio.
  e. Select Check Availability of Log Backups on File System.
  f. Select Initialize Log Area.
  g. 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>RPO</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>Lowest achievable RPO</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>RTO</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 Disaster Recovery Configuration Steps

This section provides the configurations required for disaster recovery.

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 more information about configuring SnapCenter and the HANA plug-in for data protection, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.

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 2.0 SPS0 (single container)
- SUSE Linux SLES 12 SP2
- NetApp ONTAP 9.1 software

The following three storage virtual machines (SVMs) were configured on the storage system, as shown in Figure 10:

- SVM hana: the primary storage system for the production SAP system
- SVM backup: the off-site backup storage system
- SVM disaster-recovery: the storage system used as a disaster recovery target

Note: For databases using SAP HANA 2.0 SPS1 or later, SAP only supports MDC. For more information about backup and recovery on an SAP HANA MDC single-tenant database, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.
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) Volumes and storage replication.**

<table>
<thead>
<tr>
<th>Description</th>
<th>Storage Volume</th>
<th>Replication</th>
<th>SnapCenter Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA P01 data volume</td>
<td>P01_data_mnt00001</td>
<td>SnapVault and SnapMirror</td>
<td>Resource</td>
</tr>
<tr>
<td>SAP HANA P01 log volume</td>
<td>P01_log_mnt00001</td>
<td>None</td>
<td>N/A</td>
</tr>
<tr>
<td>SAP HANA P01 log backup</td>
<td>log_backup</td>
<td>SnapMirror</td>
<td>Scheduled by ONTAP</td>
</tr>
<tr>
<td>SAP HANA P01 user home directory</td>
<td>P01_usr_sap</td>
<td>SnapVault and SnapMirror</td>
<td>Resource group</td>
</tr>
<tr>
<td>SAP HANA P01 binaries</td>
<td>hana_shared</td>
<td>SnapVault and SnapMirror</td>
<td>Resource group</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>PNW_usr_sap</td>
<td>SnapVault and SnapMirror</td>
<td>Resource group</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>PNW_sapmnt</td>
<td>SnapVault and SnapMirror</td>
<td>Resource group</td>
</tr>
<tr>
<td>SAP NetWeaver PNW binaries</td>
<td>trans</td>
<td>SnapVault and SnapMirror</td>
<td>Resource group</td>
</tr>
</tbody>
</table>

The HANA database is configured to write log backups to the mounted log backup volume, as shown in Figure 11.
4.2 Disaster Recovery Configuration Overview

In the example configuration, the disaster recovery strategy described in the section “Data Volume Replication Combined with Log Backup Volume Replication” is implemented. Table 4 lists all the related volumes that need to be mirrored to the SVM disaster recovery.

Table 4) Protection relationships for SVM disaster recovery.

<table>
<thead>
<tr>
<th>Source Volume</th>
<th>Target Volume</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01_data_mnt00001</td>
<td>hana_P01_data_mnt00001_mirror</td>
<td>Mirror</td>
</tr>
<tr>
<td>P01_usr_sap</td>
<td>hana_P01_usr_sap_mirror</td>
<td>Mirror</td>
</tr>
<tr>
<td>PNW_sapmnt</td>
<td>hana_PNW_sapmnt_mirror</td>
<td>Mirror</td>
</tr>
<tr>
<td>PNW_usr_sap</td>
<td>hana_PNW_usr_sap_mirror</td>
<td>Mirror</td>
</tr>
<tr>
<td>hana_shared</td>
<td>hana_hana_shared_mirror</td>
<td>Mirror</td>
</tr>
<tr>
<td>trans</td>
<td>hana_trans_mirror</td>
<td>Mirror</td>
</tr>
<tr>
<td>log_backup</td>
<td>hana_log_backup_mirror</td>
<td>Mirror</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.

Backup and Replication Schedules

Database backups and backups of nondatabase volumes can be scheduled and monitored with SnapCenter using the SAP HANA plug-in for the database volume and the nondata volumes.

Table 5 shows an example of a configuration with an RPO of eight hours. If the RPO is multiple hours, simply 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, which is a worst-case scenario. Nondatabase volumes are also replicated every four hours. These volumes contain primarily static data; therefore, the interval could be higher.
Table 5) Schedules for an RPO of multiple hours.

<table>
<thead>
<tr>
<th>RPO = 8 Hours</th>
<th>SnapCenter 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. These volumes contain mainly static data; therefore, 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>SnapCenter 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 log backup volume is mirrored from SVM backup to SVM disaster recovery by using the ONTAP scheduler and a frequency of 15 minutes.

### 4.3 Configure Disaster Recovery for SAP HANA Data Volume

This section describes the additional configurations required for the disaster recovery.

For more information about how to configure the SnapCenter SAP HANA plug-in to back up an SAP HANA database, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.

In this example, the following resources and settings were created as part of the backup strategy:

- In SnapCenter: the resource P01 single container – NFS – HANA database for SAP application PNW was created protecting the SAP HANA data volume P01_data_mnt00001 on SVM hana.
- In SnapCenter: two policies were created:
  - LocalSnap, with an hourly policy and a retention of 12 copies for scheduled backups.
  - LocalSnapAndSnapVault, with a daily policy and a retention of two copies on primary for scheduled backups and a SnapVault protection using the Daily label.
- In ONTAP: a SnapVault relationship to protect volume P01_data_mnt00001 by using SnapVault and a policy with the label Daily and a retention of seven copies.
- In SnapCenter: the previous resource was protected by using the LocalSnap and LocalSnapAndVault policy scheduled every four hours, once per day.

To configure protection for disaster recovery, add the following settings:

1. In ONTAP, prepare the SVM disaster recovery and configure the SnapMirror relationship for the SAP HANA data volume.
2. In SnapCenter, complete these tasks:
   a. Configure a policy that uses the SnapMirror protection.
b. Assign this policy to the SAP HANA resource and configure schedules.

Configure ONTAP

To configure ONTAP, complete the following steps:

1. In OnCommand System Manager, select Protection > Relationships.

2. Click Create to start the Create Protection Relationship workflow.

3. In the Browse SVM window, select Disaster Recovery as the target SVM.

4. The Create Protection Relationship dialog box is displayed with the mirror relationship type and source cluster name already preselected.

5. If the source and target volumes are on the same cluster, select the source SVM by clicking Browse.

6. A dialog box with all the available SVMs in the clusters is displayed.
7. 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.

8. In the Source Volume section, click Browse to select the source volume.

9. In the Destination Volume section, select New Volume and select the target aggregate.

10. In the Mirror Policy section, click Browse and select the MirrorAllSnapshots policy. Make sure that the Initialize Relationship option is selected.
11. Do not select a schedule within the Schedule section because the volumes are replicated within the backup workflow of SnapCenter.

12. When you click Create, the workflow automatically creates the new volume, establishes the SnapMirror relationship, and starts the initial transfer of the data from source to target.

Configure SnapCenter

To configure SnapCenter, complete the following steps:

1. In SnapCenter, create a new SAP HANA policy named LocalSnapAndSnapMirror, which enables SnapMirror protection. In this example, the policy replaces the LocalSnap policy and should be configured with a similar retention of 12 local Snapshot copies to keep two days of backups on the primary storage and synchronize them to the disaster recovery SVM through SnapMirror.
2. To activate the schedules for this new policy, select the resource in the resource view and modify the resource protection.

3. Clear the LocalSnap policy option and select the LocalSnapAndSnapMirror policy created in step 1.

4. Configure a backup frequency of four hours for this policy.

5. Save the configuration.

4.4 Configure Disaster Recovery for Nondatabase Volumes

To protect the nondatabase volumes, use the SnapCenter SAP HANA non-data Volume resource to complete the following tasks:

- In ONTAP: Configure a Mirror relationship for all nondatabase volumes
- In SnapCenter: Configure each volume as a resource.
In SnapCenter: Create the policies to handle SnapVault and SnapMirror protection or use the policies created for the data volume protection.

In SnapCenter: Configure the schedule based on individual policies or create a resource group for resources with identical schedule requirements and configure the schedule for the resource group.

The SnapMirror relationships need to be configured with OnCommand® System Manager.

In the example setup, the SnapMirror schedule of the log backup volume was configured at the ONTAP level only.

Configure ONTAP

For each of the nondatabase volumes (except the log backup volume), complete the following steps:

1. In OnCommand System Manager, select Protection > Relationships.
2. Click Create to start the Create Protection Relationship workflow.
3. In the dialog box, select the disaster recovery SVM as target SVM.
4. In the Create Protection Relationship dialog box, the mirror relationship type and source cluster name options are preselected.
5. If the source and target volumes are on the same cluster, select the source SVM by clicking Browse.
6. A dialog box is displayed listing all the available SVMs in the clusters. Select the source SVM (in this 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. Make sure that the Initialize Relationship option is selected.
10. Do not select a schedule within the Schedule section because the volumes are replicated within the backup workflow of SnapCenter.

11. When you click 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. For the log backup volume, repeat steps 1 through 11 with the following modifications:
   - Under Source Volume, select SVM backup.
   - Under Configuration Details, select Scheduling Every 15 Minutes instead of None.

Figure 12 shows the ONTAP protection relationships for disaster recovery.

Figure 12) Protection relationships for disaster recovery

### Configure SnapCenter

Complete the procedures in this section to configure SnapCenter.

### Create Resources

For each of the volumes, a SAP HANA resource for non-data Volume must be created. This approach provides more flexibility for scheduling and recovery compared to adding more than one volume to a single resource. To create a resource, do the following:

1. Select the Resources menu in the left pane. Make sure that the SAP HANA plug-in and the view Non-Data Volume are selected.

---

1 The screenshots show the modification of existing resources
2. Select Add SAP HANA Database to start the Resource Creation wizard.

3. On the Add/Modify SAP HANA Database Dialog select Non-data Volumes as resource type. Specify the resource name, the associated SID and the plug-in host that should be used for this resource. Click Next.
4. On the Provide Storage Footprint Details page, select hana as the source SVM and add the volume name you want to protect. Click Save to add the volume and then click Next.

5. Review and confirm the Summary page to save the data.

6. Repeat steps 1 through 5 to add all the required resources.
You can now add individual schedules for single resources, if required. In this example, we create a resource group that is used to schedule the backup of all contained resources.

Create Resource Group

To create a new resource group, complete the following steps:

1. In the Resource screen for the SAP HANA plug-in, select New Resource Group to start the Resource Group Creation wizard.

2. On the Name page, specify the name of the resource group and the tags you want to use for this group, then select the Use Custom Name Format for Snapshot Copy option. In the new field, select $CustomText, $ResourceGroup, $Policy, and $ScheduleType as variables and specify SnapCenter as custom text. Select the variable $CustomText to be able to enter the custom text for this variable. Using custom names makes it easier to identify the Snapshot copies based on their names by used schedule type or policy. Click Next.

3. On the Resources page, select the previously created resources that require an identical schedule and move them from the Available Resources column to the Selected Resources column by using the » button. Click Next.

2 The screenshots show the modification of an existing resource group.
4. On the Application Settings page, open the Snapshot Copy Tool bar and select the SnapCenter without File System Consistency option. Click Next.

5. On the Policies page, open the Policy list and select the required policies to protect the resource group volumes.
6. After you select all the required policies, close the list and configure the schedule for each selected policy. When you are finished, click Next.

7. On the Notification page, enter the e-mail notification preferences and click Next.
8. Review and confirm the Summary page. Click Finish to save the settings.
9. SnapCenter displays the Resource Group Details screen.
5 Disaster Recovery Failover Testing

A good disaster recovery strategy requires testing of the required workflow. Testing not only demonstrates whether the strategy works, and the internal documentation is sufficient, but 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 13 shows a high-level overview of the disaster recovery test.
The disaster recovery failover test was performed by completing 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 sections that follow describe the required steps in detail.

**Note:** For an SAP HANA MDC single-tenant system, the recovery of the SAP HANA database needs to be done in two steps. The first step is the recovery of the system database, followed by the recovery of the tenant database. For more information about how to back up and recover an SAP HANA MDC single-container database, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.

### 5.1 Prepare Target Server

This section describes the preparation steps required at the server, which is used for the disaster recovery failover testing.

**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. 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:** 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. The SAP host agent software must be installed at the target server. For more information, see the [SAP Host Agent](#) at the SAP help portal.

Configure Users, Ports, and SAP Services

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; therefore, no configuration steps are necessary 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:

```
stlrx300s8-3:/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;
/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;
/usr/sap/PNW/DVEBMGS03/exe/sapstartsrv pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u pnwadm
```

Create SAP HANA Log Volume

To create an SAP HANA log volume, complete the following steps:

1. Create a log volume for the SAP HANA database at the disaster recovery SVM and mount it at the target server.

```
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
192.168.173.110:/DR_P01_log_mnt00001 149422080 128 149421952 1%
```

2. Create the required subdirectories within the mounted log volume.

```
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
```

Note: For an SAP HANA MDC single-tenant system, the file system structure is different than this example of a single-container system, so the commands must be adapted accordingly. The required file system structure must be checked at the source system.
Prepare File System Mounts in `/etc/fstab`

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

**Table 7) Volume names of FlexClone copies.**

<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>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_PNW_trans_mirror</td>
<td>hana_PNW_trans_mirror_clone</td>
</tr>
</tbody>
</table>

The required `/etc/fstab` entries are the following:

```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
debugfs /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,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_P01_data_mnt00001_mirror_clone /hana/data/P01/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_P01_usr_sap_mirror_clone /usr/sap/P01 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_PNW_usr_sapmnt_mirror_clone /sapmnt/PNW nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_PNW_trans_mirror_clone /usr/sap/trans nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_PNW_sapmnt_mirror_clone /sapmnt/PNW nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_hana_shared_mirror_clone/P01 /hana/shared/P01 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
disaster-recovery:/hana_log_backup_mirror_clone /mnt/log_backup nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr, noatime, nolock 0 0
```

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

Create FlexClone copies by using OnCommand System Manager.

**Note:** The required steps can be automated by executed a script using the ONTAP CLI commands.
1. **In OnCommand System Manager,** select the mirrored volume at the disaster recovery SVM. Select **Clone > Create > Volume.** 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.

   ![Screen shot of OnCommand System Manager showing FlexClone copy creation]

2. **The following screenshot shows FlexClone copy creation for the `/usr/sap/P01` file system of the SAP HANA database.**

   **Note:** The binary volumes are replicated with a different schedule than the database data volume; therefore, select a reasonable Snapshot backup. In this 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. After all FlexClone copies have been created, mount them to the namespace by using OnCommand System Manager.
5.3 Split or Delete 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, SnapCenter 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 like 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 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:~ #
stlrx300s8-3:~ # df
Filesystem 1K-blocks  Used  Available  Use% Mounted
on /dev/sda2  285762056 37684260 246916528  14% /
udev 66043064 296 66042768  1% /dev
tmpfs 100663296 732 100662564  1% /dev/shm
```
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
stlrx300s8-3:~ # 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
sapadm 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
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
pnwadm 20710 1 0 Aug04 ? 00:02:31 /usr/sap/PNW/ASCS04/exe/sapstartsrv
pf=/usr/sap/PNW/SYS/profile/PNW_ASCS04_stlrx300s8-3 -D -u pnwadm
pnwadm 20970 1 0 Aug04 ? 00:02:32 /usr/sap/PNW/DVEBMGS03/exe/sapstartsrv
pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u pnwadm
stlrx300s8-3:~ #
```

5.5 Execute Recovery with SAP HANA Studio

The information in this section describes how to recover a system with SAP HANA Studio.

Recover System 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.

Note: For an SAP HANA MDC single-tenant system, the recovery of the SAP HANA database must be completed in two steps. The first step is the recovery of the system database, followed by the recovery of the tenant database. For details about how to back up and recover an SAP HANA MDC single-container database, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.

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

3. Select the Recover Without the Backup Catalog option and click Next.
4. From the Destination Type drop-down menu, select Snapshot and click Next.
5. On the Other Settings page, click Next (no input required).

6. Review the recovery settings and click Finish to start the recovery process.
7. The Recovery Execution Summary indicates a successful recovery process. Click Close.

Recover System 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.

Check Consistency of Latest Log Backups

To check the consistency of the latest log backups, complete the following steps:

1. 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 this 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.
2. Check the latest log backups for these services by running the `hdbbackupcheck` command.

```
2-r----- 1 poladm sapsys  5.4M Jul 29 14:13 log_backup_2_0_1616907136_1616995008.1469801621487
2-r----- 1 poladm sapsys  976K Jul 29 14:13 log_backup_0_0_0_0.1469801621559
2-r----- 1 poladm sapsys 1166K Jul 29 14:14 log_backup_2_0_6720445840_6720447168_1469801814155
2-r----- 1 poladm sapsys  976K Jul 29 14:24 log_backup_0_0_0_0.1469801814192
2-r----- 1 poladm sapsys  300K Jul 29 14:24 log_backup_2_0_55247360_582520232.1469802281747
2-r----- 1 poladm sapsys  976K Jul 29 14:28 log_backup_0_0_0_0.1469802281784
2-r----- 1 poladm sapsys  5.3M Jul 29 14:28 log_backup_2_0_1616995008.1617081344.1469802521488
2-r----- 1 poladm sapsys  976K Jul 29 14:28 log_backup_0_0_0_0.1469802521551
2-r----- 1 poladm sapsys  136K Jul 29 14:31 log_backup_0_6720447168_6720449216.1469802714157
2-r----- 1 poladm sapsys  976K Jul 29 14:31 log_backup_0_0_0_0.1469802714216
2-r----- 1 poladm sapsys  304K Jul 29 14:33 log_backup_2_0_58252032_582526768.1469803121715
2-r----- 1 poladm sapsys  976K Jul 29 14:38 log_backup_0_0_0_0.1469803121747
2-r----- 1 poladm sapsys  5.4M Jul 29 14:43 log_backup_2_0_1617081344_1617168192.1469803421496
2-r----- 1 poladm sapsys  900K Jul 29 14:43 log_backup_0_0_0_0.1469803421560
2-r----- 1 poladm sapsys  112K Jul 29 14:46 log_backup_0_6720449216_6720450080.1469803614159
2-r----- 1 poladm sapsys  980K Jul 29 14:46 log_backup_0_0_0_0.1469803614192
2-r----- 1 poladm sapsys  980K Jul 29 14:46 log_backup_0_0_0_0.1469803614232
```

If the output of the `hdbbackupcheck` tool shows that the latest log backups are consistent, 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 this example, the latest six log backups (3 catalog backups, 1 indexserver, 1 nameserver, and 1 XEngine backup) must 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.

**Note:** For an SAP HANA MDC single-tenant system, the log backups are written into different subdirectories: `SYSTEMDB` for the system database and `DB_SID` for the tenant database. The `hdbbackupcheck` tool must be executed for the log backups of the system database as well as for the log backups of the tenant database.

### Recover System with SAP HANA Studio

To recover a system with SAP HANA Studio, complete the following steps:
Note: For an SAP HANA MDC single-tenant system, the recovery of the SAP HANA database must be done in two steps. The first step is the recovery of the system database, followed by the recovery of the tenant database.

1. Select Recover System within SAP HANA Studio.

2. Select Recover the Database to Its Most Recent State and click Next.

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

5. Select the Initialize Log Area option because the recovery should be performed by using the log backup files, and there are no valid log segment files in the log area. Click Next.
6. Review the recovery settings and click Finish to start the recovery process.

7. The Recovery Execution Summary indicates a successful recovery process. Click Close.
5.6 Start SAP System

You can now start the SAP system by running the `startsap` command.

```
stlrx300s8-3:/home # su - pnwadm
stlrx300s8-3:pnwadm 50> startsap r3
Checking HDB Database
Database is running

Starting Startup Agent sapstartsrv
OK
Instance Service on host stlrx300s8-3 started

starting SAP Instance ASCS04
Startup-Log is written to /home/pnwadm/startsap_ASCS04.log

/usr/sap/PNW/ASCS04/exe/sapcontrol -prot NI_HTTP -nr 04 -function Start
Instance on host stlrx300s8-3 started
Starting Startup Agent sapstartsrv
OK
Instance Service on host stlrx300s8-3 started

starting SAP Instance DVEBMGS03
Startup-Log is written to /home/pnwadm/startsap_DVEBMGS03.log

/usr/sap/PNW/DVEBMGS03/exe/sapcontrol -prot NI_HTTP -nr 03 -function Start
Instance on host stlrx300s8-3 started
stlrx300s8-3:pnwadm 51>
```

6 Disaster Failover Operation

To perform a disaster failover, perform the following tasks:

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. Execute recovery with SAP HANA Studio:
   a. Without forward recovery using log backups
   b. Including forward recovery with log backups
6. Start the SAP system.

The sections that follow describe these tasks in more detail.

**Note:** For an SAP HANA MDC single-tenant system, the recovery of the SAP HANA database needs to be done in two steps. The first step is the recovery of the system database, followed by the recovery of the tenant database. For more information about how to back up and recover an SAP HANA MDC single-container database, see the TR-4614: SAP HANA Backup and Recovery with SnapCenter installation and configuration guide.

### 6.1 Prepare Disaster Recovery Server

This section describes the preparation steps required at the server, which is used for the disaster recovery failover testing.

**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.

**Install Required Software**

The SAP host agent software must be installed at the target server. For more information, see the SAP Host Agent at the SAP help portal.

**Configure Users, Ports, and SAP Services**

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; therefore, no configuration steps are necessary 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:

```
stlrx300s8:/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;
/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;
/usr/sap/PNW/DVEBMGS03/exe/sapstartsrv pf=/usr/sap/PNW/SYS/profile/PNW_DVEBMGS03_stlrx300s8-3 -D -u pnwadm
```
Create SAP HANA Log Volume

To create an SAP HANA log volume, complete the following steps:

1. Create a log volume for the SAP HANA database at the storage system and mount it at the target server.

```
# 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
```

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

```
# cd /hana/log/P01/mnt00001/
# mkdir hdb00001
# mkdir hdb00002
# mkdir hdb00003
# mkdir hdb00004
```

Note: For an SAP HANA MDC single-tenant system, the file system structure is different than for this example of a single-container system. Therefore, you must adapt the commands accordingly. The required file system structure must be checked at the source system.

Prepare File System Mounts in /etc/fstab

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

<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_PNW_trans_mirror</td>
</tr>
</tbody>
</table>

The required /etc/fstab entries are the following:

```
# cat /etc/fstab
/dev/disk/by-id/scsi-360030057013a54201aa3727d258af07f-part1 swap defaults 0 0
defaults 0 0
/acl, user_xattr 1 1
proc /proc proc defaults 0 0
sysfs /sys sysfs noauto 0 0
debugfs /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
6.2 Break SnapMirror Replication Relationship

The storage volumes at the disaster recovery storage must be made readable and writable so that they can be mounted and used at the disaster recovery server. To make these storage volumes readable and writable, you must break the SnapMirror relationship.

Note: The following screenshots show NetApp OnCommand System Manager. These steps can also be automated by executing a script using the ONTAP CLI commands.

1. In OnCommand System Manager, select Protection within the disaster recovery SVM.
2. Select the volume and then select Operations > Break.

3. To confirm that you want to break the relationship, click Break.
4. Repeat steps 1 through 3 for all other required volumes.

5. To mount the volumes at the disaster recovery server, they must be mounted to the storage system namespace. The following example depicts the mounted volumes.
6.3 Restore 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 SnapCenter issued the unquiesce command for the SAP HANA database. Therefore, the SAP HANA database data volume must be restored to the latest backup that was created with SnapCenter to get a consistent database image.

**Note:** The following screenshots show NetApp OnCommand System Manager. These steps can also be automated by executing a script using the ONTAP CLI commands.

To restore the SAP HANA database data volume, complete the following steps:

1. Select Volume within the disaster recovery SVM. Select the data volume and select Snapshot Copies > Restore.
2. Select the latest SnapCenter Snapshot copy and click Restore.

Note: The remainder of the 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 246916528  14% /
udev       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
```

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
stlrx300s8-3:~ # ps -ef | grep sap
root    5470  2689  0 07:42 pts/0  00:00:00 grep sap
p01adm  13058     1  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
p01adm  13079  13058  0 Aug04 ? 00:00:00 /usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3/pf=/usr/sap/P01/SYS/profile/P01_HDB02_stlrx300s8-3
root    20333 10 Aug04 ? 00:00:10 /usr/sap/hostctrl/exe/saphostexec
p01adm  20366     1  0 Aug04 ? 00:00:01 /usr/sap/hostctrl/exe/sapstartsrv
p01adm  20392     1  0 Aug04 ? 00:00:09 /usr/sap/hostctrl/exe/saposcol -l -w60
p01adm  20459  10 Aug04 ? 00:18:05 /usr/sap/P01/HDB02/exe/sapstartsrv
p01adm  20710  10 Aug04 ? 00:02:31 /usr/sap/PNW/ASCS04/exe/sapstartsrv
p01adm  20970  10 Aug04 ? 00:02:32 /usr/sap/PNW/DVEBMGS03/exe/sapstartsrv
pnwadm   20970  10 Aug04 ? 00:02:32 /usr/sap/PNW/DVEBMGS03/exe/sapstartsrv
stlrx300s8-3:~ #
```

6.5 Execute Recovery with SAP HANA Studio

The information in this section describes how to recover a system with SAP HANA Studio.

**Recover System 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 “Recover System with SAP HANA Studio Excluding Log Files.”

**Recover System 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 “Recover System with SAP HANA Studio Including Log Files.”
6.6 Start SAP System

You can now start the SAP system by running the `startsap` command.

```
stlrx300s8-3:/home # su - pnwadm
stlrx300s8-3:pnwadm 50> startsap r3
Checking HDB Database
Database is running
-------------------------------------------
Starting Startup Agent sapstartsrv
OK
Instance Service on host stlrx300s8-3 started
-------------------------------------------
starting SAP Instance ASCS04
Startup-Log is written to /home/pnwadm/startsap_ASCS04.log
-------------------------------------------
/usr/sap/PNW/ASCS04/exe/sapcontrol -prot NI_HTTP -nr 04 -function Start
Instance on host stlrx300s8-3 started
Starting Startup Agent sapstartsrv
OK
Instance Service on host stlrx300s8-3 started
-------------------------------------------
starting SAP Instance DVEBMGS03
Startup-Log is written to /home/pnwadm/startsap_DVEBMGS03.log
-------------------------------------------
/usr/sap/PNW/DVEBMGS03/exe/sapcontrol -prot NI_HTTP -nr 03 -function Start
Instance on host stlrx300s8-3 started
stlrx300s8-3:pnwadm 51>
```

Where to Find Additional Information

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

- NetApp SnapCenter Software Resource page: [http://mysupport.netapp.com/snapcenter/resources](http://mysupport.netapp.com/snapcenter/resources)

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>November 2017</td>
<td>Initial release.</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>April 2018</td>
<td>Update to cover SnapCenter 4.0</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 © 2017 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

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

TR-4646-1117