

Technical Report

# SAP HANA Disaster Recovery with Storage Replication

Nils Bauer, NetApp July 2020 | TR-4646

#### Abstract

This document is an overview of the options for disaster recovery protection for SAP HANA. It includes detailed setup information and a use case description of a three-site disaster recovery solution based on synchronous and asynchronous NetApp<sup>®</sup> SnapMirror<sup>®</sup> storage replication. The described solution uses NetApp SnapCenter<sup>®</sup> with the SAP HANA plug-in to manage database consistency.



### TABLE OF CONTENTS

SA	P H/	ANA Disaster Recovery with Storage Replication	1	
	Nils	Bauer, NetApp July 2020   TR-4646	1	
1	Dat	a Protection Overview	6	
	1.1	Business Application Requirements	6	
	1.2	High Availability	6	
	1.3	Logical Corruption	7	
	1.4	Backups	7	
	1.5	Synchronous or Asynchronous Data Replication	8	
	1.6	HANA System Replication with or Without Data Preload	8	
2	Dis	aster Recovery Solution Comparison	8	
	2.1	Backup and Recovery	9	
	2.2	SAP HANA Disaster Recovery Using Storage Replication	11	
	2.3	SAP HANA System Replication	13	
	2.4	Summary of Disaster Recovery Solutions	15	
3	SAI	P HANA Disaster Recovery with SnapMirror Replication	. 16	
	3.1	Lab Setup	17	
	3.2	SnapCenter Support for Synchronous SnapMirror	18	
	3.3	Configuration Steps for Synchronous SnapMirror Replication	19	
	3.4	Configuration Steps for Asynchronous SnapMirror Replication	21	
4	Ove	erview of Disaster Recovery Testing	. 27	
5	Syr	nchronous SnapMirror Disaster Recovery Testing	. 28	
	5.1	Prepare the Target Host	29	
	5.2	Create Snapshot Backups at the Source Storage System	31	
	5.3	Create FlexClone Volumes at the Disaster Recovery Storage	31	
	5.4	Mount FlexClone Volumes at the Target Host	33	
	5.5	Start the HANA Database	33	
	5.6	Cleanup Operations	34	
6	Asy	Asynchronous SnapMirror Disaster Recovery Testing		
	6.1	Prepare the Target Host	35	
	6.2	Create FlexClone Volumes at the Disaster Recovery Storage	37	
	6.3	Mount the FlexClone Volumes at the Target Host	39	
	6.4	Check Consistency of Latest Log Backups	40	
	6.5	Recover the HANA Database	41	

7	Ove	erview of Disaster Recovery Failover	. 52
8	Syn	chronous SnapMirror Disaster Recovery Failover	. 52
	8.1	Prepare Target Host	53
	8.2	Break SnapMirror Relationships	54
	8.3	Mount Volumes at Target Host	58
	8.4	Start the HANA Database	58
9	Asy	nchronous SnapMirror Disaster Recovery Failover	. 58
	9.1	Prepare Target Host	59
	9.2	Break SnapMirror Relationships	61
	9.3	Restore Data Volume to Latest SnapCenter Backup	65
	9.4	Mount FlexClone Volumes at Target Host	66
	9.5	Check Consistency of Latest Log Backups	67
	9.6	Recovery of the HANA Database	67
10	Diff	erent Steps Required in a Fibre Channel Environment	. 67
	10.1	Mapping LUNs to Disaster Recovery Server	67
	10.2	Mount File Systems	68
	10.3	Cleanup Operation	69
Wh	ere	to Find Additional Information	. 70
Ve	rsior	h History	. 70

#### LIST OF TABLES

Table 1) Disaster recovery solution comparison	15
Table 2) Comparison of asynchronous storage replication approaches.	17
Table 3) Replication relationships.	18
Table 4) Disaster recovery testing – required steps.	28
Table 5) Volume names of FlexClone volumes.	30
Table 6) Volume names of FlexClone copies	36
Table 7) Disaster recovery testing – required steps.	52
Table 8) Volume names of FlexClone volumes	54
Table 9) Volume names of FlexClone volumes.	60

#### LIST OF FIGURES

Figure 1) Data protection overview	6
Figure 2) Disaster recovery overview.	9

Figure 3) NetApp storage-based backups.	11
Figure 4) Disaster recovery with synchronous and asynchronous SnapMirror	12
Figure 5) NetApp MetroCluster combined with asynchronous SnapMirror.	13
Figure 6) SAP HANA System Replication.	14
Figure 7) SAP HANA disaster recovery with SnapMirror replication.	16
Figure 8) Lab setup	17
Figure 9) SnapMirror update warning message.	19
Figure 10) Synchronous SnapMirror - Create Protection Relationship	20
Figure 11) Synchronous SnapMirror volume relationships.	20
Figure 12) SnapCenterSync Protection Policies	21
Figure 13) Combined backup and disaster recovery replication	22
Figure 14) Replication of data volume only.	23
Figure 15) Asynchronous SnapMirror - Create Protection Relationship – Configuration Details	23
Figure 16) Asynchronous SnapMirror - Create Protection Relationship – Schedule.	24
Figure 17) Asynchronous SnapMirror Volume Relationships.	24
Figure 18) SnapCenter topology view for HANA database	26
Figure 19) SnapCenter topology view for HANA shared volume	26
Figure 20) SnapCenter policies.	27
Figure 21) Asynchronous SnapMirror policy	27
Figure 22) Synchronous SnapMirror disaster recovery testing	29
Figure 23) Create FlexClone volume using crash-consistent Snapshot backup	32
Figure 24) List of FlexClone volumes.	32
Figure 25) Junction paths configuration.	32
Figure 26) Asynchronous SnapMirror disaster recovery testing.	35
Figure 27) Create a FlexClone volume based on an application-consistent SnapCenter backup.	37
Figure 28) Create a FlexClone copy of the log backup volume	38
Figure 29) List of FlexClone volumes.	38
Figure 30) Junction path configuration.	39
Figure 31) Recovery to a specific data backup: Recovery Type	42
Figure 32) Recovery with log backups: Recovery Type.	42
Figure 33) Recovery to a specific data backup: Specify backup catalog location	43
Figure 34) Recovery with log backups: Backup catalog location	43
Figure 35) Recovery to a specific data backup: Select Destination Type.	43
Figure 36) Recovery with log backups: Backup selection	44
Figure 37) Recovery with log backups: Log backup location	44
Figure 38) Recovery to a specific data backup: Other Settings	45
Figure 39) Recovery with log backups: Other Settings	45
Figure 40) Recovery to a specific data backup: Review Recovery Settings.	46
Figure 41) Recovery with log backups: Review Recovery Settings.	
Figure 42) Recovery to a specific data backup: Recovery Execution Summary	47

Figure 43) Recovery of Tenant Database in DRS.	47
Figure 44) Recovery to a specific data backup: Recovery Type	47
Figure 45) Recovery with log backups: Specify Recovery Type	48
Figure 46) Recovery to a specific data backup:Specify backup catalog location	48
Figure 47) Recovery with log backups: Specify backup catalog location	48
Figure 48) Recovery to a specific data backup: Select Destination Type	49
Figure 49) Recovery with log backups: Select a Backup	49
Figure 50) Recovery to a specific data backup: Other Settings	50
Figure 51) Recovery to a specific data backup: Review Recovery Settings	50
Figure 52) Recovery Execution Summary.	51
Figure 53) HANA Studio: System recovered.	51
Figure 54) Synchronous SnapMirror disaster recovery failover	53
Figure 55) SnapMirror quiesce operation—step 1	55
Figure 56) SnapMirror quiesce operation—step 2	55
Figure 57) All SnapMirror target volumes are quiesced.	56
Figure 58) SnapMirror break operation—step 1	56
Figure 59) SnapMirror break operation—step 2	57
Figure 60) All SnapMirror target volumes are broken off	57
Figure 61) Junction path configuration.	58
Figure 62) Synchronous SnapMirror disaster recovery failover	59
Figure 63) SnapMirror quiesce operation—step 1	61
Figure 64) SnapMirror quiesce operation—step 2	62
Figure 65) All SnapMirror target volumes are quiesced.	62
Figure 66) SnapMirror break operation—step 1	63
Figure 67) SnapMirror break operation—step 2.	63
Figure 68) All SnapMirror target volumes are broken off	64
Figure 69) Junction path configuration.	64

# **1 Data Protection Overview**

Studies have shown that business application downtime has a significant negative impact on the business of enterprises. In addition to the financial impact, downtime can also damage the company's reputation, staff morale, and customer loyalty. Surprisingly, not all companies have a comprehensive disaster recovery policy.

Running SAP HANA on NetApp<sup>®</sup> 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 to help customers select options that support their business needs.

To develop a comprehensive disaster recovery policy, customers must understand the business application requirements and technical capabilities they need for data protection and disaster recovery (Figure 1).

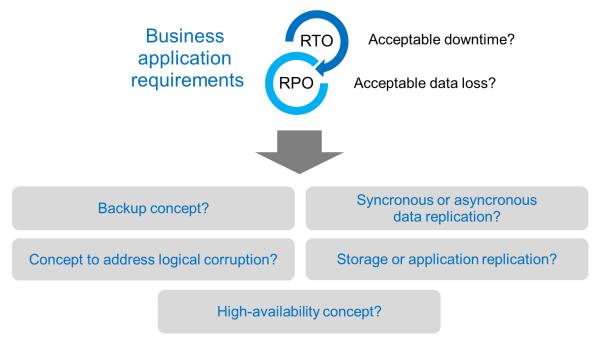


Figure 1) Data protection overview.

## **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 might differ if you are protecting against hardware failures at a single site. They might also differ if you are preparing for catastrophic disasters such as the loss of a complete data center. It's important to evaluate the business requirements that define the RPO and RTO, because these requirements have a significant impact on the technical options that are available.

## 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. Therefore, failures in these redundant systems should not cause any application downtime.

To provide high availability on the server and application side, standby SAP HANA hosts can be configured for built-in high availability with an SAP HANA multiple-host system. If a server or an SAP HANA service fails, the SAP HANA service fails over to the standby host, which causes application downtime.

If application downtime is not acceptable in the case of server or application failure, you can also use SAP HANA system replication as a high-availability solution that enables failover in a very short time frame. SAP system replication is discussed in detail in section 2.3, SAP HANA System Replication. SAP HANA customers use HANA system replication not only to address high availability for unplanned failures, but also to minimize downtime for planned operations, such as HANA software upgrades.

## **1.3 Logical Corruption**

Logical corruption can be caused by software errors, human errors, or sabotage. Unfortunately, logical corruption often cannot be addressed with standard high-availability and disaster recovery solutions. As a result, depending on the layer, application, file system, or storage where the logical corruption occurred, RTO and RPO requirements can sometimes not be fulfilled.

The worst case is a logical corruption in an SAP application. SAP applications often operate in a landscape in which different applications communicate with each other and exchange data. Therefore, restoring and recovering an SAP system in which a logical corruption has occurred is not the recommended approach. Restoring the system to a point in time before the corruption occurred results in data loss, so the RPO becomes larger than zero. Also, the SAP landscape would no longer be in sync and would require additional postprocessing.

Instead of restoring the SAP system, the better approach is to try to fix the logical error within the system, by analyzing the problem in a separate repair system. Root cause analysis requires the involvement of the business process and application owner. For this scenario, you create a repair system (a clone of the production system) based on data stored before the logical corruption occurred. Within the repair system, the required data can be exported and imported to the production system. With this approach, the productive system does not need to be stopped, and, in the best-case scenario, no data or only a small fraction of data is lost.

## 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 required restore time, the recovery time (including database start), and the loading of data into memory. For large databases and traditional backup approaches, the RTO can easily be several hours, which might not be acceptable. To achieve very low RTO values, a backup must be combined with a hot-standby solution, which includes preloading data into memory.

In contrast, a backup solution must address logical corruption, because data replication solutions cannot cover all kinds of logical corruption. For details, see section 2.1, 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 greater 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 than that of traditional databases because a large amount of data must be loaded into memory before the database can provide the expected performance. Therefore, a significant part of the RTO is the time needed to start the database. With any storage-based replication, the SAP HANA database must be started in case of failover to the disaster recovery site.

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

# 2 Disaster Recovery Solution Comparison

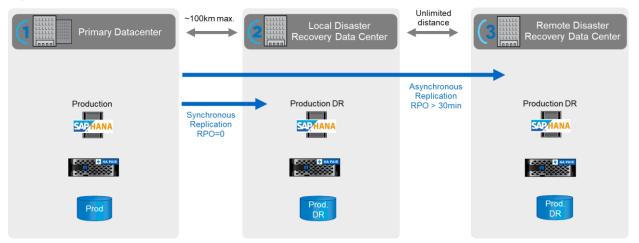
A comprehensive disaster recovery solution must enable customers to recover from a complete failure of the primary site. Therefore, data must be transferred to a secondary site, and a complete infrastructure is necessary to run the required production SAP HANA systems in case of site failure. Depending on the availability requirements of the application and the kind of disaster you want to be protected from, a two-site or three-site disaster recovery solution must be considered.

Figure 2 shows a typical three-site configuration, where the secondary data center is close to the primary. This allows you to replicate the data synchronously and to achieve an RPO of zero.

In addition, the data is also replicated asynchronously to a third, remote data center to be protected from disasters, which would influence operations in the primary as well as in the local disaster recovery data center. The minimum achievable RPO depends on the data replication frequency, which is limited by the available bandwidth between the primary and the remote disaster recovery data center. A typical minimal RPO is in the range of 30 minutes to multiple hours. Instead of running a third remote disaster recovery data center, a cloud provider IaaS (AWS, Azure, Google Cloud) could be used to provide the required resources.

This document discusses the different implementation options of a three-site disaster recovery solution. All of the use cases and scenarios described are also valid for two-site disaster recovery solutions, either with just a local or just a remote disaster recovery data center.

#### Figure 2) Disaster recovery overview.



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:

- Resource usage at the local and remote disaster recovery 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 requirements 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 detail in the following sections.

#### 2.1 Backup and Recovery

SAP HANA supports these 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 NetApp<sup>®</sup> Snapshot<sup>™</sup> backups

To choose the method that's best for them, 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 made 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 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 complete run time of the backup operation depends mainly on the required HANA savepoint operation, which needs to be done before the storage Snapshot operation. Customer data shows that the average backup run time is around 1 minute. The Snapshot 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<sup>®</sup> with the SAP HANA plug-in can facilitate an automated and fully integrated HANA backup based on Snapshot technology, 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 <u>TR-4614</u>: <u>SAP HANA Backup and Recovery with SnapCenter</u> best practices guide.

## **Addressing Logical Corruption**

As discussed in section 1, Data Protection Overview, a logical corruption in 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 crucial. With NetApp storage-based Snapshot backups, multiple consistent database images are available to create a clone of the production system by using NetApp FlexClone<sup>®</sup> technology. FlexClone volumes 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. Section 4, Overview of Disaster Recovery 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 3) NetApp storage-based backups.

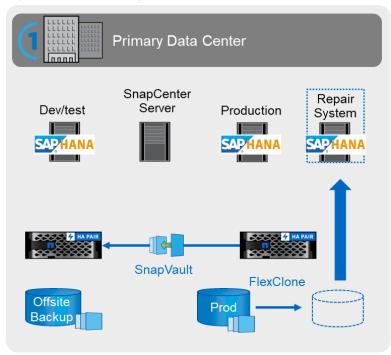


Figure 3 is an example of a backup solution using NetApp storage-based Snapshot backups to secure the system on the primary site. Backups can be automatically transferred by using NetApp SnapVault<sup>®</sup> backup software to a dedicated off-site backup storage system. This process is controlled by SnapCenter. All the backups available at the primary or off-site backup storage site can be used to create FlexClone volumes 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 SAP HANA Disaster Recovery Using Storage Replication

NetApp supports three different disaster recovery data replication methods for SAP HANA.

- Asynchronous replication with SnapMirror. NetApp SnapMirror<sup>®</sup> replication technology is built into ONTAP<sup>®</sup> for disaster recovery solutions. SnapMirror is configured through a data protection relationship between two storage volumes on a primary and a secondary storage system. SnapMirror updates the secondary volume by using efficient block delta replications. Update schedules can be either defined on the storage system itself or triggered externally. For full information, see <u>TR-4015</u>: SnapMirror Configuration and Best Practices Guide for ONTAP 9.
- Synchronous replication with SnapMirror. Synchronous SnapMirror (SM-S) was introduced with ONTAP 9.5. SM-S is configured through a data protection relationship between two storage volumes on a primary and a secondary storage system. SM-S is targeted at relatively short distances to provide exact replicas with an RPO of zero. For full information, see<u>TR-4733: SnapMirror</u> <u>Synchronous for ONTAP 9.7</u>.
- Synchronous replication with NetApp MetroCluster. NetApp MetroCluster™ configurations are used to provide high availability, zero data loss, and nondisruptive operations both within and beyond the data center. MetroCluster is a free feature of ONTAP software that synchronously mirrors data and configuration between two ONTAP clusters in separate locations or failure domains. MetroCluster provides continuously available storage for applications by automatically handling two objectives:
  - Zero RPO by synchronously mirroring data written to the cluster

 Near-zero RTO by mirroring configuration and automating access to data at the second site MetroCluster provides simplicity with automatic mirroring of data and configuration between the two independent clusters located in the two sites. As storage is provisioned in one cluster, it is automatically mirrored to the second cluster at the second site. For full information, see <u>TR-4689</u>: <u>NetApp MetroCluster IP</u> and <u>TR-4375</u>: <u>NetApp MetroCluster FC</u>

## Synchronous SnapMirror Combined with Asynchronous SnapMirror

Figure 4 shows a three-site disaster recovery solution, using synchronous SnapMirror replication to the local disaster recovery data center and asynchronous SnapMirror to replicate the data to the remote disaster recovery data center.

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

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

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

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

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

Leveraging cloud provider laaS offerings from AWS, Azure, or Google is another option for data replication to a third location. Instead of running your own remote data center resources, the data could be replicated to Cloud Volumes ONTAP by using asynchronous SnapMirror. Cloud Volumes ONTAP is available at all three main cloud providers, AWS, Azure, and Google.

The following sections cover the DR configuration, the DR workflow testing, and the DR failover workflow steps in detail.

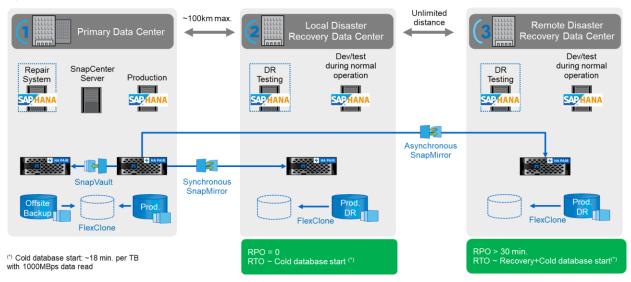


Figure 4) Disaster recovery with synchronous and asynchronous SnapMirror.

## NetApp MetroCluster Combined with Asynchronous SnapMirror

Figure 5 shows a three-site disaster recovery solution, using NetApp MetroCluster for synchronous replication to the local disaster recovery data center and asynchronous SnapMirror to replicate the data to the remote disaster recovery data center.

Synchronous storage replication based on NetApp MetroCluster provides RPO=0. This disaster recovery solution does not require any additional configuration at the SAP HANA level.

NetApp MetroCluster is supported up to 700km for MetroCluster IP. However, the maximum distance is determined by the maximum acceptable latency for the application; in most cases it is in the range of 100km.

The SAP HANA data and log volumes and the nondatabase data are synchronously replicated to the disaster recovery site, as shown in Figure 5. 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. A third-party software solution, such as <u>ProLion ClusterLion automatic</u> <u>switchover for NetApp MetroCluster</u>, can automate the MetroCluster failover process.

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 1000MB/s, loading 1TB of data takes approximately 18 minutes.

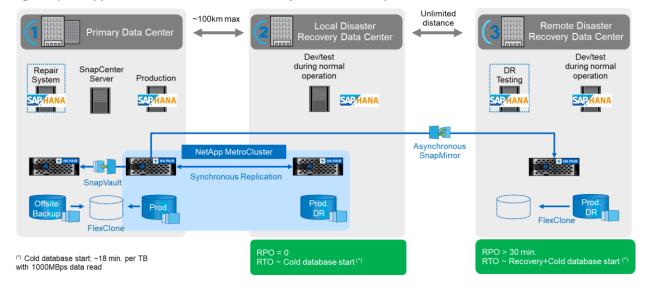


Figure 5) NetApp MetroCluster combined with asynchronous SnapMirror.

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 SAP HANA System Replication

SAP HANA System Replication works 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 one of two modes:

- With data preload into memory, with a dedicated server at the disaster recovery site:
  - The server is used exclusively as an SAP HANA System Replication secondary host.

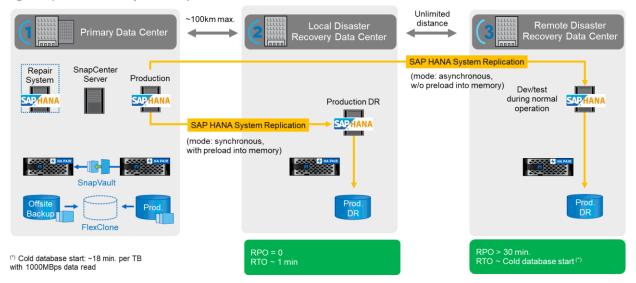
- Very low RTO values can be achieved, because the data is already loaded into memory and no database start is required in case of a failover.
- Without data preload into memory, with a shared server at the disaster recovery site:
  - The server is shared as an SAP HANA System Replication secondary and as a dev/test system.
  - RTO depends mainly on the time required to start the database and load the data into memory.

For a full description of all configuration options and replication scenarios, see the <u>SAP HANA</u> <u>Administration Guide</u>.

Figure 6 shows the setup of a three-site disaster recovery solution with SAP HANA System Replication. Synchronous replication with data preload into memory is used for the local disaster recovery data center. Asynchronous replication without data preload is configured for the remote disaster recovery data center.

**Note:** SAP HANA System Replication can also be combined with storage replication. In this case, HANA System Replication would be used for data replication to the local DR data center and asynchronous SnapMirror would be used for replication to the remote DR data center.





## SAP HANA System Replication with Data Preload into Memory

Very low RTO values with SAP HANA can be achieved only with SAP HANA System Replication with data preload into memory. Operating SAP HANA System Replication with a dedicated secondary server at the disaster recovery site allows an RTO value of approximately 1 minute or less. The replicated data is received and preloaded into memory at the secondary system. Because of this low failover time, SAP HANA System Replication is also often used for near-zero-downtime maintenance operations, like HANA software upgrades.

Typically, SAP HANA System Replication is configured to replicate synchronously when data preload is chosen. The maximum supported distance for synchronous replication is in the range of 100km.

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

## SAP System Replication Without Data Preload into Memory

For less stringent RTO requirements, 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 DR 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 1000MB/s, loading 1TB of data should take approximately 18 minutes.

## 2.4 Summary of Disaster Recovery Solutions

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 with preload into memory 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 disaster recovery testing and dev/test refresh.
- All disaster recovery solutions must be combined with a backup solution that addresses logical corruption.

	Storage Replication		SAP HANA System Replication		
	NetApp SnapMirror	NetApp MetroCluster	With Data Preload	Without Data Preload	
RTO	Low to medium, depending on database startup time	Low to medium, depending on database startup time	Very low	Low to medium, depending on database startup time	
RPO	RPO=0 for synchronous RPO> 30min for asynchronous	RPO=0	RPO=0 for synchronous RPO> 30min for asynchronous	RPO=0 for synchronous RPO> 30min for asynchronous	
Servers at DR site can be used for dev/test	Yes	Yes	No	Yes	
Replication of nondatabase data	Yes	Yes	No	No	
DR data can be used for refresh of dev/test systems	Yes, for asynchronous No, for synchronous	No	No	No	
DR testing without affecting RTO and RPO	Yes	Yes	No	No	
DR configuration effort	For each storage volume used by the databases	All storage volumes are automatically replicated	For each database	For each database	

#### Table 1) Disaster recovery solution comparison.

# 3 SAP HANA Disaster Recovery with SnapMirror Replication

Figure 7 shows the volume replication relationships for a three-site disaster recovery configuration with synchronous and asynchronous SnapMirror replication. In addition to the SnapMirror replication, the HANA data and shared volume are also replicated with SnapVault to offsite backup storage.

**Note:** The following description and the lab setup focus on the HANA database. SAP application servers would have additional storage volumes, which would be protected and replicated in the same way as the HANA shared volume.

With synchronous SnapMirror replication, all three HANA volumes, the data, the log, and the shared volume must be replicated to the local disaster recovery data center. Replication of application-consistent Snapshot copies is not required. In case of a disaster failover, the replication relationship must be broken, the volumes must be mounted to the DR production server, and the HANA database must be started and will execute a crash recovery. Section 8, Synchronous SnapMirror Disaster Recovery Failover, describes the required steps.

With asynchronous SnapMirror replication, the HANA data and the HANA shared volume need to be replicated. With HANA data volume replication, typical RPO values are in the range of multiple hours. If lower RPO values are required, the HANA log backups must be replicated in addition for forward recovery. To enable HANA savepoint or forward recovery, application-consistent Snapshot data backups must be included in the HANA data volume at the disaster recovery site. This is accomplished with SnapCenter backups created at the primary site, which are then replicated to the DR site. In case of a disaster failover, the replication relationship must be broken, the volumes must be mounted to the DR production server, and the HANA database must be recovered, either to the last HANA savepoint or with forward recovery using the replicated log backups. Section 9, Asynchronous SnapMirror Disaster Recovery Failover, describes the required steps.

**Note:** The HANA shared volume includes the /hana/shared as well as the /usr/sap file system of the HANA system. The installation was done as described in <u>TR-4435: SAP HANA on NetApp AFF</u> <u>Systems with NFS</u>.

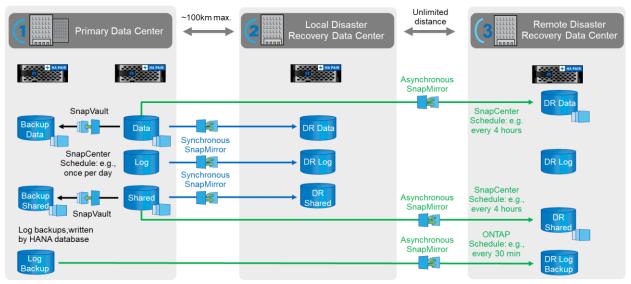


Figure 7) SAP HANA disaster recovery with SnapMirror replication.

Table 2 compares the different storage replication approaches.

Table 2) Comparison of asynchronous storage replication approaches.

Replication	RPO	RTO
Synchronous SnapMirror	• RPO = 0	<ul> <li>Break mirror and mount volumes</li> <li>HANA crash recovery</li> <li>Database start (~ 18 min per TB)</li> </ul>
Asynchronous SnapMirror with data and log backup volume replication	<ul> <li>Depends on the log backup replication frequency and the log backup interval.</li> <li>Typical RPO &gt; 30 min</li> </ul>	<ul> <li>Break mirror and mount volumes</li> <li>HANA recovery with forward recovery</li> <li>Database start (~ 18 min per TB)</li> </ul>
Asynchronous SnapMirror with data volume replication only	<ul> <li>Depends on the data volume replication frequency</li> <li>Typical RPO=multiple hours</li> </ul>	<ul> <li>Break mirror and mount volumes</li> <li>HANA recovery to last savepoint</li> <li>Database start (~ 18 min per TB)</li> </ul>

**Note:** Database start and data load into memory takes around 18 minutes per TB, with a data read throughput of 1000MB/s.

## 3.1 Lab Setup

Figure 8 shows the schematic lab setup with storage virtual machines (SVM) used for primary, backup, and disaster recovery data. SnapCenter is used to create Snapshot data backups of the HANA system with the System Identifier (SID) DRS. These backups are replicated to the offsite backup as well as to the remote disaster recovery site. For full information about configuring SnapCenter and the HANA plug-in for data protection, see <u>TR-4614</u>: <u>SAP HANA Backup and Recovery with SnapCenter</u>.

**Note:** For the lab setup, NFS is used to connect the storage volumes to the HANA hosts. The differences for a HANA host using Fibre Channel (FC) are highlighted in the subsections of section 5, 6, 8, and 9.

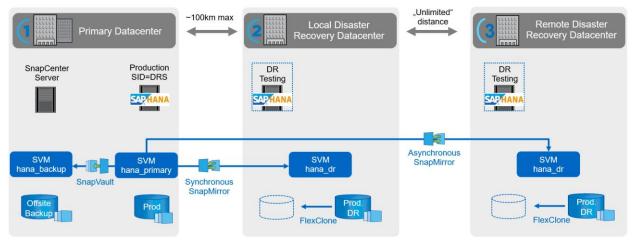


Figure 8) Lab setup.

The following software versions were used in the lab setup:

- SAP HANA 2.0 SPS4 (MDC single tenant)
- SUSE Linux SLES for SAP 15 SP1
- NetApp ONTAP 9.7

#### • SnapCenter 4.3.1P1

Table 3 shows the replication relationships, which have been configured in the lab setup. The table lists the same replication relationships that are shown in Figure 7.

Source Volume	Source SVM	Target Volume	Target SVM	Replication	Schedule	Schedule Managed By
DRS_data_ mnt00001	hana_primary	DRS_data_ mnt00001_dest	hana_backup	SnapVault	Once per day	SnapCenter
DRS_shared	hana_primary	DRS_shared_dest	hana_backup	SnapVault	Once per day	SnapCenter
DRS_data_ mnt00001	hana_primary	DRS_data_ mnt00001_dest_sm_s	hana_dr	Synchronous SnapMirror	NA	NA
DRS_log_ mnt00001	hana_primary	DRS_log_ mnt00001_dest_sm_s	hana_dr	Synchronous SnapMirror	NA	NA
DRS_shared	hana_primary	DRS_shared_ dest_sm_s	hana_dr	Synchronous SnapMirror	NA	NA
DRS_data_ mnt00001	hana_primary	DRS_data_ mnt00001_dest	hana_dr	Asynchronous SnapMirror	Every 4 hours	SnapCenter
DRS_shared	hana_primary	DRS_shared_dest	hana_dr	Asynchronous SnapMirror	Every 4 hours	SnapCenter
DRS_log_ backup	hana_backup	DRS_log_backup_dest	hana_dr	Asynchronous SnapMirror	Every 30 minutes	ONTAP

Table 3) Replication relationships.

## 3.2 SnapCenter Support for Synchronous SnapMirror

The current SnapCenter release does not have an integration of synchronous SnapMirror. Synchronous SnapMirror can be used together with SnapCenter, but you need to be aware of a few shortcomings. Synchronous SnapMirror will be supported in future SnapCenter releases.

- In the SnapCenter topology view of a HANA resource, a synchronous SnapMirror relationship is not visible.
- Snapshot backups that are created with SnapCenter are not replicated to the synchronous SnapMirror target.
  - A new protection policy (SnapCenterSync) for synchronous SnapMirror that enables Snapshot replication was introduced in ONTAP 9.7. SnapCenter does not yet support the required APIs, so SnapCenter Snapshot backups are not replicated.
- When synchronous SnapMirror is combined with asynchronous SnapMirror, SnapCenter checks the availability of the Snapshot backups at the synchronous SnapMirror target with each SnapMirror update job.
  - Because the backups are not replicated to the synchronous SnapMirror target, SnapCenter waits and tries the operation again until the timeout of 120 minutes. Therefore, the SnapMirror update job runs for about 2 hours and delays the visibility of the backup at the asynchronous SnapMirror target.
  - After the timeout, SnapCenter displays a warning message that the backup at the synchronous SnapMirror target was not found.

#### Figure 9) SnapMirror update warning message.

Job Details	×		
Backup of Resource Group 'hana-10_sapcc_stl_netapphared-Volume' with policy 'LocalSnapAndSnapMirror'			
Backup of Resource Group 'hana-10_sapcc_stl_netapp_com_hana_NonDataVolume_DRS_DRS-Shared- Volume' with policy 'LocalSnapAndSnapMirror'			
<ul> <li>hana-10.sapcc.stl.netapp.com</li> </ul>			
🛕 🔍 ( Job 13264 ) SnapMirror update			
SnapMirror update failed for 2 relationships: Relationship [hana-primary : DRS_shared ==> hana-dr : DRS_shared_dest_sm_s] failed with error: Snapshot copy 'SnapCenter_LocalSnapAndSnapMirror_04-20-2020_05.49.54.8699' not found on the SnapMirror destination hana-dr : DRS_shared_dest_sm_s Relationship [hana-primary : DRS_shared ==> hana-dr : DRS_shared_dest_sm_s] failed with error: Snapshot copy 'SnapCenter_LocalSnapAndSnapMirror_04-20-2020_05.49.54.8699' not found on the SnapMirror destination hana-dr : DRS_shared_dest_sm_s			
View Logs Cancel Job Close			

## 3.3 Configuration Steps for Synchronous SnapMirror Replication

Synchronous SnapMirror replication is configured on the storage system. Figure 10 shows the protection relationship dialog box from ONTAP System Manager, which is used to configure the replication. The dialog box includes four main configuration options.

- Replication type:
  - Synchronous
- Synchronization mode:
  - Sync or StrictSync
  - With StrictSync, the application using the source volume gets an I/O error if the replication to the target is not possible. With StrictSync, an RPO of zero can be guaranteed. However, if the secondary site is not available, the result will be application downtime.
- Source volume and target volume suffix
- Protection policy:
  - Can be Sync or SnapCenterSync for synchronous replication.
  - To enable Snapshot replication to the synchronous SnapMirror target, SnapCenterSync must be selected. Using this policy, Snapshot copies that are created with the ONTAP CLI with the label app\_consistent are replicated to the target. As discussed in section 3.2, SnapCenter Support for Synchronous SnapMirror, SnapCenter backups cannot currently be replicated. Snapshot replication based on ONTAP CLI Snapshot copies, is used for disaster recovery testing, as described in section 5, Synchronous SnapMirror Disaster Recovery Testing.

Create Protection Relationship		×				
Data protection refers to backing up data and being able to recover it. Depending on your data protection and backup needs, you can select an appropriate method to protect your data against accidental, malicious, or disaster-induced data loss. Tell me more about different types of data protection relationships.						
Relationship Type						
Replication:	Synchronous V Help me Choose	L				
Synchronization Mode:	Sync 💌	L				
Source Volume						
i Cluster:	a700-marco					
SVM:	hana-primary	L				
Volume:	DRS_data_mnt00001 0	L				
Destination Volume						
SVM:	hana-dr					
Volume Name Suffix:	_dest_sm_s					
Configuration Details						
(i) Sync Policy:	SnapCenterSync Browse					
🚺 🗷 Initialize Relationship						
SnapLock for SnapVault	SnapLock for SnapVault is applicable only for Vault protection relationships.	•				
	Create Cancel					

#### Figure 10) Synchronous SnapMirror - Create Protection Relationship.

Figure 11 shows the required volume relationships. The SAP HANA data, log, and shared volume must be replicated with synchronous SnapMirror.

	ONTAP Syste	m١	lanager											•	?	-	
é Sw	itch to the new experie	ence						Ţ	ype: All		✓ Q ≤	Search all O	bjects			+	~
	:		Volume Relation	ships													
	Dashboard		🕂 Create 🛛 🧪 Edit	🔋 Delete 🔌 Operations 🔹	C Refresh												
	Applications & Tiers	•	Source Storage 👳	Source Volume	Destination Volume	Destinatio 😇	Is Healthy 🗄	🗉 Object 😇	Relationshi	Tran 🔫	Relations	Lag Time	Policy !	Name 😇	Policy Ty	pe 1	
	Ch		hana-primary	DRS_data_mnt00001	DRS_data_mnt00001_dest_sm_s	hana-dr	Yes	Volume	Snapmirrored	InSync	Sync	None	SnapCe	enterSync	Sync		
2	Storage	*	hana-primary	DRS_log_mnt00001	DRS_log_mnt00001_dest_sm_s	hana-dr	Yes	Volume	Snapmirrored	InSync	Sync	None	SnapCe	enterSync	Sync		
	Network	•	hana-primary	DRS_shared	DRS_shared_dest_sm_s	hana-dr	🥑 Yes	Volume	Snapmirrored	InSync	Sync	None	SnapCe	enterSync	Sync		
2	Protection	*															1
	Volume																
	Relationships																
	SVM DR																
	Relationships																
	Protection Policies																
	Schedules																
	Snapshot Policies																
2	Events & Jobs	÷															
			Source Location:	hana-primary:DRS_data	Is Healthy:	✓ Yes		ransfer Status:		Sync							
Σ	Configuration	•		n: hana-dr:DRS_data_mnt00	Relationship State:	Snapmirrored		urrent Transfer T		one							
			Source Cluster:	a700-marco	Network Compression Ratio:	Not Applicable		urrent Transfer E		one							
			Destination Cluster:					urrent Transfer F		one							
			Transfer Schedule:	None Unlimited				ast Transfer Erro		one							
			Data Transfer Rate:	None				ast Transfer Type		sync /20/2020 04:0	0.00						
			Lag Time:	NOTE				atest Snapshot Ti				0.0021					
							L	atest Snapshot O			26c54-77cc-11 2157901726.2		40500				

Figure 12 shows the policy rules of the SnapCenterSync protection policy. The SnapMirror label app\_consistent enables the replication of Snapshot copies to the target volume. Snapshot replication is required for disaster recovery testing, as described in section 5, Synchronous SnapMirror Disaster Recovery Testing.

	ONTAP Syste	m N	Manager										۰	?	-	
: Sw	itch to the new experie	ence					Тур	e: All	~	् Sear	rch all Ob	jects			+	
	:	=	Protection Policies													
	Dashboard		🕂 Create 🅜 Edit 🥤 Delete 🛛 C Refresh													
	Applications & Tiers	•	Name	Туре		<b>T</b>	Comment				Ŧ	Transfer	Priority			
,	Storage		SnapCenterSync	Sync			Policy for Snap	Mirror Synchronous	for Snap Cer	iter with App	olicatio	Normal				
		,	StrictSync	StrictSync			Policy for Snap	Mirror Synchronous	where client	access will b	be disr	Normal				
	Network	۲	Sync	Sync			Policy for Snap	Mirror Synchronous	where client	access will n	not be	Normal				
)	Protection	*														
	Volume															
	Relationships															
	SVM DR															
	Relationships															
	Relationships															
	Relationships Protection Policies															
	Relationships Protection Policies Schedules	ŀ	Snapmirror-Label	Ŧ	Retention Count		Ŧ	Preserve older Snap	shot copies	f retention c	count is ex	ceeded				1
<b>≥</b>	Relationships Protection Policies Schedules Snapshot Policies	•	Snapmirror-Label sm_created	Ţ	Retention Count		Ŧ	Preserve older Snap No	shot copies	f retention c	count is exi	ceeded				

Figure 12) SnapCenterSync Protection Policies.

## 3.4 Configuration Steps for Asynchronous SnapMirror Replication

SAP HANA disaster recovery with asynchronous SnapMirror replication requires database-consistent Snapshot backups at the production site, which are then replicated to the disaster recover site. The database-consistent Snapshot backups are created with SnapCenter and the SAP HANA plug-in.

First, the asynchronous SnapMirror protection relationship must be configured on the storage layer. The initial complete data transfer is also part of this configuration.

SnapCenter is then used to initiate a SnapMirror update replication during the normal Snapshot backup workflow. The following tasks are performed during the backup workflow with SnapCenter:

- 1. Trigger an SAP HANA database snapshot, which includes a 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 in the SAP HANA backup catalog.
- 4. Initiate the replication update to the disaster recovery site by using SnapMirror.
- 5. 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.

## Data Volume Replication Combined with Log Backup Volume Replication

Figure 13 shows a disaster recovery solution based on the replication of the SAP HANA database data volume plus the replication of the log backup volume.

As discussed, data volume replication is tied to the backup workflow in SnapCenter. A typical backup frequency is "every 4 hours." In our example the data volume and the shared volume are backed up and replicated by SnapCenter every 4 hours.

The RPO is defined by the replication frequency of the log backup volume. With the standard SAP HANA log backup interval of 15 minutes and a log backup replication interval of, for example, 30 minutes, the minimal possible RPO is >30 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. Section 9, Asynchronous SnapMirror Disaster Recovery Failover, describes the required steps.

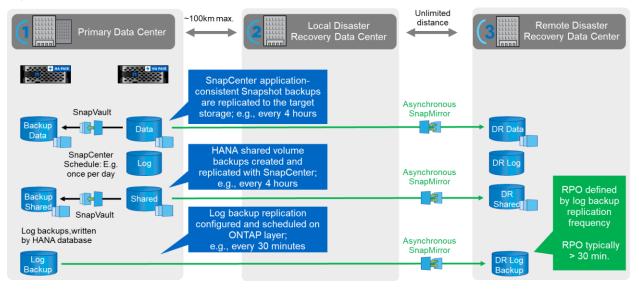


Figure 13) Combined backup and disaster recovery replication.

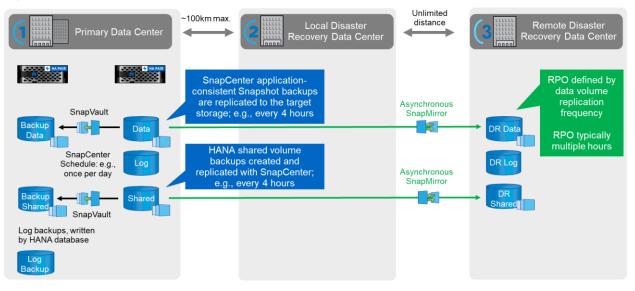
## **Replication of Data Volume Only**

Figure 14 shows a disaster recovery solution that is based on the replication of the SAP HANA database data volume. The log backup volume is not replicated.

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 1 hour. Based on this recommendation, the lowest achievable RPO is 1 to 2 hours.

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. Section 9, Asynchronous SnapMirror Disaster Recovery Failover, describes the required steps.

#### Figure 14) Replication of data volume only.



## **Configuration of ONTAP Replication Relationships**

Figure 15 shows the ONTAP System Manager dialog box for the configuration of the HANA data and log volumes. For both volumes, the selected Protection Policy is MirrorAllSnapshots, so that every backup that is created by SnapCenter is replicated to the DR site.

Because SnapCenter triggers the SnapMirror update operation as part of each backup workflow, schedule None needs to be configured in ONTAP.

Figure 15) Asynchronous SnapMirror - Create Protection Relationship – Configuration Details.

Create Protection Relationship		×
Relationship Type		*
Replication:	Asynchronous	÷
(i) Relationship Type:	Mirror 💌	
Source Volume		
(i) Cluster:	a700-marco	
SVM:	hana-primary	
Volume:	DRS_data_mnt00001 Browse 1	
Destination Volume		
SVM:	hana-dr	
Volume Name Suffix:	_dest	
Configuration Details		
(i) Mirror Policy:	MirrorAllSnapshots Browse	4
i Schedule:	hourly Browse	
	Every how r at 05 minute(s)	
	None	
🚺 🗹 Initialize Relationship		
-		*
	Create Cance	el

For the log backup volume, a schedule is configured on the storage layer. because SnapCenter is not executing any backup operation for this volume. In our example, a new schedule, Every-30-Minutes, has been created.

Relationship Type   Replication:   Asynchronous   I Relationship Type:   Mirror   Source Volume   I Cluster:   a700-marco   SVM:   hana-backup   Volume:   DRS_log_backup   Browse   I Mirror AllSnapshots   I Mirror Policy:   Mirror AllSnapshots   Browse   I Mirror AllSnapshots   Browse   I Mirror AllSnapshots   Browse   I hone	×
Image: Second and a secon	^
Source Volume	- 1
Cluster: SVM: hana-backup    Volume: DRS_log_backup Browse    SVM:   hana-dr   Volume Name Suffix:	
SVM:     hana-backup       Volume:     DRS_log_backup       Browse     Image: Configuration Details       Oroffiguration Details     Image: Configuration Details       Image: MirrorAllSnapshots     Browse       Image: Schedule:     Image: Every-30-Minutes       Image: The schedule runs at @:00:30     Browse	- 1
Volume:     DRS_log_backup     Browse       Destination Volume       SVM:     hana-dr       Volume Name Suffix:     _dest       Configuration Details       Image: Mirror AllSnapshots       Browse       Schedule:       Image: Every-30-Minutes       The schedule runs at @:00;30       None	
Destination Volume SVM: hana-dr Volume Name Suffix:dest Configuration Details  Mirror Policy: MirrorAllSnapshots Browse  Schedule: Every-30-Minutes Browse The schedule runs at @:00;30 None	
SVM:     hana-dr       Volume Name Suffix:     _dest       Configuration Details     ImmorralISnapshots       Immorrality     MirrorAlISnapshots       Schedule:     ImmorralISnapshots       Immorrality     Browse       Immorrality     ImmorralISnapshots       Volume None     Browse	
Volume Name Suffix: _dest  Configuration Details  Mirror Policy: MirrorAllSnapshots Browse  Schedule:  Every-30-Minutes The schedule runs at @:00:30  None	- 1
Configuration Details	
Mirror Policy: MirrorAllSnapshots Browse     Schedule:     Every-30-Minutes     The schedule runs at @-00.:30     None	
Schedule:     Every-30-Minutes     The schedule runs at @-00.:30     None	
The schedule runs at @:00.:30	1
None	
<ol> <li>✓ Initialize Relationship</li> </ol>	
•	-
Create Ca	ncel

#### Figure 16) Asynchronous SnapMirror - Create Protection Relationship – Schedule.

Figure 17 shows all configured asynchronous SnapMirror relationships. As discussed, log backup volume replication is not required if a data-volume-only replication concept has been chosen.

Figure 17)	Asynchronous	<b>SnapMirror</b>	Volume	Relationships.

L	<b>ONTAP System</b>	m N	lanager												Ø 🕨	• •	: (	2	2
0: Swi	ritch to the new experie	ence								Type:	All		~	्, Sea	rch all Object	s		•	+ `
	Ξ	≡	Volume Relatio	onships															
	Dashboard		🕂 Create 🍞 Edit	👕 Delete 🛛 🔧 Operation	s• C	Refresh													
	Applications & Tiers	F.	Source Storag 👳	Source Volume	Destinatio	in Volume 👳	Destination 🔫	ls 👻	Object \Xi	Relationship	📼	T= Relations	nip Type		Policy Name	. <del>.</del>	Policy Ty	/pe	Ŧ
	Storage	•	hana-backup hana-primary	DRS_log_backup DRS_data_mnt00001	- 0-	ackup_dest _mnt00001_dest	hana-dr hana-dr		Volume Volume	Snapmirrore		idle Asynchron							
•	Network	۶.	hana-primary	DRS_shared	DRS_shar	ed_dest	hana-dr	🔮 Yes	Volume	Snapmirrore	d	Idle Asynchron	ious Ver	ion-Flex	MirrorAllSna	pshots	Asynchro	onous Min	ror
,	Protection	-																	
	Volume Relationships																		
	SVM DR Relationships																		
	Protection Policies																		
	Schedules																		
	Snapshot Policies																		
	Events & Jobs	F	Source Location:	hana-backup:DRS_log_ba.		Is Healthy:	♥Yes		Transfer	Status:		Idle							
	Configuration	•	Destination Locati	ion: hana-dr:DRS_log_backup.		Relationship State:	Snapmirrored		Current 1	Fransfer Type:		None							
			Source Cluster:	a700-marco		Network Compression	Not Applicable	e	Current 1	Transfer Error:		None							
			Destination Cluste	er: a700-marco		Ratio:			Current 1	Fransfer Progre	SS:	None							
			Transfer Schedule	Every-30-Minutes					Last Tran	sfer Error:		None							
			Data Transfer Rat	e: Unlimited					Last Tran	isfer Type:		Update							
			Lag Time:	None					Latest Sn	apshot Timesta	imp:	04/23/2020 06:	30:00						
									Latest Sn	apshot Copy:		snapmirror.870 00a098d994db <u></u>							
			Details	Policy Details		Snapshot Copies													

## **SnapCenter Configuration**

This section describes the SnapCenter configuration for disaster recovery. Basic operations like adding storage systems and configuring policies are described in <u>TR-4614: SAP HANA Backup and Recovery</u> with SnapCenter.

Two resources need to be configured in SnapCenter:

- HANA database resource for the backup operations of the HANA database
- Non-data-volume resource for the backup operations of the /hana/shared volume

To configure the SnapCenter resources, follow these steps:

- Add storage systems (if they are not already configured).
   For our lab setup, the storage SVMs hana-primary, hana-backup, and hana-dr need to be added.
- Add policies (if they are not already configured).
   LocalSnapAndSnapMirror, LocalSnapAndSnapVault, BlockIntegrityCheck.
- 3. Add SAP HANA system DRS.

Execute auto discovery by deploying the SnapCenter HANA plug-in on the database host.

- 4. Configure resource protection for HANA system DRS.
  - a. Select policies.
  - b. Define schedules.
- 5. Add non-data-volume resource for the DRS-shared volume.
- 6. Configure resource protection for the DRS-shared volume.
  - a. Select policies.
  - b. Define schedules.

Figure 18 shows the SnapCenter topology view for the HANA database resource and Figure 19 shows the SnapCenter topology view for the HANA shared volume.

**Note:** As discussed in section 3.2, in the current SnapCenter release, synchronous SnapMirror relationships are not displayed in the topology view.

SAP	HANA 🔽	DRS Topology								
S	earch databases		Remove I	notection Bac	L k up Now	Modily	Maintenance	j Details	Configure Database	
R.	System	Manage Copies								
-20	MH1 - Multiple hosts system	34 Backups					<i>c</i>			
20	MS1 - Multiple Hosts MDC Single Tenant	0 Clones						nary Card		
8	\$\$3	Mirror copies					64 Back	ups spshot based ba	allo and	
	DRS	Local copies						-Based backup		
	Q01	0 Clones					0 Clone	es		
	QS1	Vault copies								
		Primary Backup(s)								
_	SH1	(search 🛛							10	4
	SM1									
	551	Backup Name	Count	17						End
	SS2	SnapCenter_LocalSnapAndSnapMirror_Hourly_04-24-2020_02.22.00.6807	1						04/24/2020 2	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-23-2020_22.22.00.6527	1						04/23/2020 10	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-23-2020_18.22.00.6200	1						04/23/2020 6	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-23-2020_14.22.00.6388	1						04/23/2020 2	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-23-2020_10.22.00.6043	1						04/23/2020 10	
		SnapCenter_LocalSnapAndSnapVault_Daily_04-23-2020_06.38.00.5981	1						04/23/2020 6	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-23-2020_06.22.00.5785	1						04/23/2020 6	):23:04 A
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_22.22.01.4760	1						04/21/2020 10	):23:05 F
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_18.22.01.4532	1						04/21/2020 6	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_14.22.01.4409	1						04/21/2020 2	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_10.22.02.8722	1						04/21/2020 10	
		SnapCenter_LocalSnapAndSnapVault_Daily_04-21-2020_06.38.02.6195	1						04/21/2020 6	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_06.22.00.7847	1						04/21/2020 6	
		SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_02.22.01.8487	1						04/21/2020 2	
		SnapCenter_LocalSnapAndSnapVault_Daily_04-06-2020_06.38.00.8378	1						04/06/2020 6	:38:54 A
Tota	il 10	Total 15								

#### Figure 18) SnapCenter topology view for HANA database.



2/10	apCenter@	٥			•	■ 0-	1 sapcc\scadmi	in SnapCenter/	Admin 🖡	l Sign Ou
	SAP HANA	•	DRS-Shared-Volume Topology							
	Search dat	abases			<b></b>	6	1		1 Details	<b>₽</b>
	E 14	Name			Remove Protect	ion Back up Now	Modify	Maintenance	Details	Hefre
l	12 P	DRS-Shared-Volume SS1-Shared-Volume	Manage Copies				Summa 30 Backup	·		
			Local copies				30 Snaps O Clones	hot based backups		
			Primary Backup(s)							
			search T							<b>4</b> istore
			Backup Name	Count	1F					End D
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-21-2020_02.30.00.8067	1				04/21	/2020 2:30:	10 AM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-20-2020_22.30.00.8580	1				04/20/	2020 10:30:	10 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-20-2020_18.30.00.7280	1				04/20	)/2020 6:30:	10 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-20-2020_14.30.00.7490	1				04/20	/2020 2:30:	10 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-20-2020_10.30.00.7544	1				04/20/	2020 10:30:	10 AM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-20-2020_06.30.00.7166	1				04/20	/2020 6:30:	10 AM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-07-2020_23.20.01.6159	1				04/07/	2020 11:20:	11 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-07-2020_22.20.01.4704	1				04/07/	2020 10:20:	11 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-07-2020_21.20.01.5367	1				04/07	7/2020 9:20:	11 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-07-2020_20.20.01.5725	1				04/07	7/2020 8:20:	11 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-07-2020_19.20.01.4830	1				04/07	7/2020 7:20:	11 PM
			SnapCenter_LocalSnapAndSnapMirror_Hourly_04-07-2020_18.20.01.4250	1				04/07	7/2020 6:20:	11 PM

The details screen of the HANA resource shows the configured SnapCenter policies (Figure 20).

#### Figure 20) SnapCenter policies.

SAP		Resource - Details		
Se	arch databases			
12	System	Details for selected resource		
***	MH1 - Multiple hosts system	Туре	Multitenant I	Database Container
***	MS1 - Multiple Hosts MDC Single Tenant	HANA System Name	DRS	
8	553	SID	DRS	
	DRS	Tenant Databases	DRS	
	Q01	Plug-in Host	hana-10.sap	cc.stl.netapp.com
	QS1	HDB Secure User Store Key	DRSKEY	
	SH1	HDBSQL OS User	drsadm	
	SM1	Log backup location	/mnt/log-bac	
	SS1	Backup catalog location		5/HDB00/backup/log
		plug-in name	SAP HANA	
	552	Last backup	4/27/2020 2:	22:54 AM (Completed)
		Resource Groups		cc_stl_netapp_com_hana_MDC_DRS
	L L	Policy	BlockIntegrit	yCheck, LocalSnapAndSnapMirror, LocalSnapAndSnapVa
		Discovery Type	Auto	
		Storage Footprint		
		SVM	Volume	Junction Path
		hana-primary.sapcc.stl.netapp.com	DRS_data_mnt00001	/DRS_data_mnt00001

Figure 21 shows the SnapCenter policy for asynchronous SnapMirror. The selected secondary label is not relevant, because MirrorAllSnapshots is configured with the ONTAP protection relationship.

Figure 21) Asynchronous SnapMirror policy.

Modify SAP HA	NA Backup Policy	
1 Name	Select secondary replication options 0	
2 Settings	Update SnapMirror after creating a local Snapshot copy.	
3 Retention	Update SnapVault after creating a local Snapshot copy.	
4 Replication	Secondary policy label Hourly	
5 Summary	Error retry count 3	

## 4 Overview of Disaster Recovery Testing

An effective disaster recovery strategy requires testing the required workflow. Testing demonstrates whether the strategy works, and whether the internal documentation is sufficient, and it also allows administrators to train on the required procedures.

Storage replication with SnapMirror makes it possible to execute disaster recovery testing without putting RTO and RPO at risk. Disaster recovery testing can be done without interrupting data replication.

Disaster recovery testing for both asynchronous and synchronous SnapMirror uses Snapshot backups and FlexClone volumes at the disaster recovery target.

Table 4 is a high-level overview of the required steps. The following sections describe the disaster recovery failover test workflow in detail.

#### Table 4) Disaster recovery testing – required steps.

	Synchronous SnapMirror	Asynchronous SnapMirror
Prepare target host for testing	<ol> <li>Install SAP host agent.</li> <li>Configure user, ports, SAP services.</li> <li>Create mount points.</li> <li>Prepare /etc/fstab.</li> </ol>	<ol> <li>Install SAP host agent.</li> <li>Configure user, ports, SAP services.</li> <li>Create mount points.</li> <li>Mount new, empty log volume, and create subdirectories identical to source system.</li> <li>Prepare /etc/fstab.</li> </ol>
Provide Snapshot backup at the source storage system	<ul> <li>ONTAP CLI:</li> <li>Manual, on-demand Snapshot creation for data (crash consistent), log, and shared volume. ONTAP CLI must be used to set the required SnapMirror label.</li> </ul>	<ul> <li>SnapCenter:</li> <li>Application-consistent Snapshot backups of the data volume are available.</li> <li>Snapshot backups of the shared volume are available.</li> </ul>
Create FlexClone volumes at the disaster recovery storage	ONTAP System Manager or CLI: 1. Create FlexClone volumes for data, log, and shared volume, based on Snapshot created before.	<ul> <li>ONTAP System Manager or CLI:</li> <li>1. Create FlexClone volumes for data and shared volume, based on SnapCenter Snapshot backups.</li> <li>2. Create FlexClone volume of the log backup volume (if log backup replication is part of the DR concept).</li> </ul>
Mount FlexClone volumes at target host <b>Note:</b> This step requires additional LUN discovery operations in an FC SAN environment.	1. Mount data, log, and shared volume.	<ol> <li>Mount data and shared volume.</li> <li>Mount log backup volume (if log backup replication is part of the DR concept).</li> </ol>
Start or recover the HANA database	<ol> <li>Start SAP services.</li> <li>Start HANA database.</li> <li>Crash recovery is executed.</li> </ol>	1. Start SAP services. HANA database is recovered to the last backup (or recovered with forward recovery using log backups if log backup replication is part of the DR concept).

# 5 Synchronous SnapMirror Disaster Recovery Testing

To configure synchronous SnapMirror disaster recovery testing, follow these steps, as shown in Figure 22:

- 1. Prepare the target host.
- 2. Create Snapshot backups at the source storage system.
- 3. Snapshot backups are replicated to the target storage.
- 4. Create FlexClone volumes at the disaster recovery storage.
- 5. Mount FlexClone volumes at the target host.
- 6. Start the HANA database.

The following subsections describe these steps in detail.

Unlimited ~100km max distance Remote Disaster Local Disaster Primary Data Center Recovery Data Center Data Cente Prepare target host DR 1 Testing 5 6 2 3 SnapVault Attach volumes to DR Testing server and start HANA database DR Data Data with crash-recovery Synchronous 4 ŚnapMirror SnapCenter DR Log Schedule: e.g. once per day Synchronous SnapMirror Create FlexClone volumes Shared SnapVault Log backups.written by HANA database ONTAP CLI: Manual creation of crash-Snapshot backups with the SnapMirror label consisistent Snapshot backups at the app\_consistent are automatically replicated to primary storage system with the SnapMirror label app\_consistent the target storage Back (ONTAP protection policy: SnapCenterSync)

Figure 22) Synchronous SnapMirror disaster recovery testing.

## 5.1 Prepare the Target Host

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

During normal operation, the target host is typically used for other purposes, for example, as a HANA QA or test system. Therefore, most of the described steps must be executed when disaster failover testing is executed. On the other hand, the relevant configuration files, like /etc/fstab and /usr/sap/sapservices can be prepared and then put in production by simply copying the configuration file. The disaster recovery testing procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system.

#### **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.

**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. For full information, see the <u>SAP Host</u> Agent at the SAP help portal.

**Note:** If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

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

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the  $/{\tt etc/services}$  file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the /usr/sap/sapservices file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
hana-10:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/DRS/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/DRS/HDB00/exe/sapstartsrv pf=/usr/sap/DRS/SYS/profile/DRS_HDB00_hana-10
-D -u drsadm
limit.descriptors=1048576
```

#### Prepare Log Backup Volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host.

A volume for the log backups must be configured and mounted at the target host.

#### **Prepare File System Mounts**

Table 5 shows the naming conventions used in the lab setup. The volume names of the FlexClone copies at the disaster recovery storage are included in /etc/fstab. These volume names are used in the FlexClone copy creation step in the next section.

HANA DRS Volumes	FlexClone Volume at Disaster Recovery Storage	Mount Point at Target Host
Data volume	DRS_data_mnt00001_dest_sm_s_clone	/hana/data/DRS/mnt00001
Log volume	DRS_log_mnt00001_dest_sm_s_clone	/hana/log/DRS/mnt00001
Shared volume	DRS_hana_shared_dest_sm_s_clone/shared DRS_hana_shared_dest_sm_s_clone/usr-sap	/hana/shared /usr/sap//DRS

Table 5) Volume names of FlexClone volumes.

The mount points in Table 5 must be created at the target host.

Here are the required /etc/fstab entries.

```
hana-10:/mnt/log-backup # cat /etc/fstab
192.168.175.116:/DR_testing_log_backup /mnt/log-backup nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_data_mnt00001_dest_sm_s_clone /hana/data/DRS/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_log_mnt00001_dest_sm_s_clone /hana/log/DRS/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_shared_dest_sm_s_clone/shared /hana/shared nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_shared_dest_sm_s_clone/usr-sap /usr/sap/DRS nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
```

**Note:** In a Fibre Channel setup, the fstab entries depend on the multipath configuration. Because the SCSI IDs are different with each operation, the fstab file is not static and must be adapted after the LUN discovery process.

## 5.2 Create Snapshot Backups at the Source Storage System

The crash-consistent Snapshot backups must be created using the ONTAP CLI to include the SnapMirror label <code>app\_consistent</code>, which is required so that the Snapshot backups are also replicated to the target storage system.

```
a700-marco::> snap create -vserver hana-primary -volume DRS_data_mnt00001 -snapshot crash-
consistent -snapmirror-label app_consistent
a700-marco::> snap create -vserver hana-primary -volume DRS_log_mnt00001 -snapshot crash-
consistent -snapmirror-label app_consistent
a700-marco::> snap create -vserver hana-primary -volume DRS_shared -snapshot crash-consistent -
snapmirror-label app_consistent
```

The following command output shows the Snapshot backups at the synchronous SnapMirror targets.

#### Data volume:

#### Log volume:

#### Shared volume:

## 5.3 Create FlexClone Volumes at the Disaster Recovery Storage

The FlexClone volumes can now be created at the disaster recovery storage by using ONTAP System Manager, as shown in Figure 23.

ONTAP Syste	m Man	nager						Ø 📮	<b>\$</b>	• •	
Switch to the new experie	nce					Type: All	✓	Search all Objects		+	-
:	= vo	olumes	SVM hana-dr	'							
Dashboard	-	+ Create 🕜 E	dit 🔋 Delete 🚦 More Actions	View Missing	Protection Relationships C Refresh						
Applications & Tiers	۶.	Status \Xi	Name	Style 😇	Create FlexClone Volume	,	Туре 😇	Protection =	Storage E		plic
Storage	• +	0	DRS_data_mnt00001_dest	FlexVol	Name: DRS_data_mnt00001_dest_sm_s_c	one	dp	No	Enabled	-N4	<b>A</b> -
Nodes	+	0	DRS_data_mnt00001_dest_sm_s	FlexVol	Thin Provisioning		dp	No	Enabled	-NA	<b>A</b> -
Aggregates & Disks	+	0	DRS_log_backup_dest	FlexVol	Allocate space for the volume as it's used. Otherwi space for the entire volume.	se, the system reserves	dp	No	Enabled	-NA	<b>A</b> -
SVMs	+	0	DRS_log_mnt00001_dest_sm_s	FlexVol	FlexClone parent Snapshot copy		dp	No	Enabled	-NA	<b>A</b> -
Volumes	+	0	DRS_shared_dest	FlexVol	Name	Date	dp	No	Enabled	-NA	<b>A</b> -
LUNs	+	0	DRS_shared_dest_sm_s	FlexVol	snapmirror.87026c54-77cc-11e9-9e21-00a098.		dp	No	Enabled	-NA	<b>A</b> -
	+	0	DR_testing_log_backup	FlexVol	snapmirror.87026c54-77cc-11e9-9e21-00a098 crash-consistent	May/11/2020 00: May/11/2020 00:	rw	No	Enabled	-NA	<b>A</b> -
Qtrees	+	0	dr_root	FlexVol			rw	No	Disabled	-N4	<b>A</b> -
Quotas											
Junction Paths											
Network	•										
Protection	•										
	•										
Events & Jobs						lone Cancel					

Figure 23) Create FlexClone volume using crash-consistent Snapshot backup.

The same operation must be done for the log and the shared volume. Figure 24 shows the list of FlexClone volumes.

	ONTAP System I	Mana	ager										Ø 📮	¢ 0	-	
<b>10</b> : Sw	itch to the new experience								1	Type: All		•   ٩	Search all Objects		+	~
	Volumes SVM hand-dr															
-	Dashboard	+	Create	1	Edit 📄 Delete 🚦 More Actions 🔍 Vi	iew Missing Protec	tion Relationship	s C Refresh								•
	Applications & Tiers 🕨		Status	Ŧ	Name 😎	Style 😇	Aggre 😇	Thin Provi 😇	Availa 😇	Total 😇	% Used 😇	Туре	Protection 😇	Storage E 😇	Appli	<del></del>
1	Storage 👻	+	•		DRS_data_mnt00001_dest_sm_s_clone	FlexVol	aggr1_2	Yes	2.01 GB	10.23 GB	80	rw	No	Enabled	-NA-	
	Nodes	+			DRS_log_mnt00001_dest_sm_s_clone	FlexVol	aggr1_2	Yes	12.21 GB	64 GB	80	rw	No	Enabled	-NA-	
	Aggregates & Disks	+			DRS_shared_dest_sm_s_clone	FlexVol	aggr1_2	Yes	52.02 GB	309.13 GB	83	rw	No	Enabled	-NA-	

All three FlexClone volumes must be mounted to the namespace, as shown in Figure 25.

Figure 25) Junction paths configuration.

	ONTAP System	Manager						Ø		?	-	8
€ Sw	ritch to the new experience				Type:	All	~	Q. Search a	l Objects		+	~
	≡	Junction Paths SVM hana-dr	•									
	Dashboard	😭 Mount 🛛 🎢 Unmount 💦 🖌 Change Export Policy	C Refresh									
	Applications & Tiers	Path	Storage Object	Export Policy	Security S	yle						
	Storage 👻	4 <del></del> /	🛢 dr_root	default	unix							
	Storage 👻	TR_testing_log_backup	DR_testing_log_backup	default	unix							
	Nodes	TRS_data_mnt00001_dest_sm_s_clone	DRS_data_mnt00001_dest_sm_s_clone	default	unix							
		TRS_log_mnt00001_dest_sm_s_clone	DRS_log_mnt00001_dest_sm_s_clone	default	unix							
	Aggregates & Disks	TRS_shared_dest_sm_s_clone	DRS_shared_dest_sm_s_clone	default	unix							

**Note:** In a Fibre Channel setup, the LUNs in the FlexClone volumes must be mapped to the initiator group of the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

## 5.4 Mount FlexClone Volumes at the Target Host

The FlexClone volumes can now be mounted at the target host.

hana-10:/mnt/log-backup # mount -a

The following output shows the required file systems.

```
hana-10:/mnt/log-backup # df
Filesystem
                                                   1K-blocks
                                                                 Used Available Use% Mounted
on
192.168.175.116:/DR testing log backup
                                                   104857600
                                                                 256 104857344 1%
/mnt/log-backup
192.168.175.116:/DRS data mnt00001 dest sm s clone
                                                   10725184 8612864 2112320 81%
/hana/data/DRS/mnt00001
192.168.175.116:/DRS log mnt00001 dest sm s clone
                                                    67106816 54305408 12801408 81%
/hana/log/DRS/mnt00001
192.168.175.116:/DRS_shared_dest_sm s clone/shared 324150976 269605952 54545024 84%
/hana/shared
192.168.175.116:/DRS_shared_dest_sm_s_clone/usr-sap 324150976 269605952 54545024 84%
/usr/sap/DRS
hana-10:/mnt/log-backup #
```

**Note:** In a Fibre Channel setup, additional steps are required before the LUNs can be mounted at the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

## 5.5 Start the HANA Database

Start the required SAP services.

hana-10:/mnt/log-backup # systemctl start sapinit

The following output shows the required processes.

```
hana-10:/mnt/log-backup # ps -ef | grep sap
drsadm 17468 1 3 02:25 ?
                                   00:00:00 /usr/sap/DRS/HDB00/exe/sapstartsrv
pf=/usr/sap/DRS/SYS/profile/DRS HDB00 hana-10 -D -u drsadm
root 17485 5714 0 02:25 pts/0 00:00:00 grep --color=auto sap
        24223 1 0 Mar25 ?
                                    00:04:14 /usr/sap/hostctrl/exe/saphostexec
root
pf=/usr/sap/hostctrl/exe/host profile
sapadm 24227 1 0 Mar25 ?
                                   00:50:25 /usr/sap/hostctrl/exe/sapstartsrv
pf=/usr/sap/hostctrl/exe/host_profile -D
                                    01:01:43 /usr/sap/hostctrl/exe/saposcol -1 -w60
root
        24443
              1 0 Mar25 ?
pf=/usr/sap/hostctrl/exe/host profile
hana-10:/mnt/log-backup #
```

The HANA database can now be started.

During the startup, the HANA database executes a crash recovery.

```
hana-10:/mnt/log-backup # su - drsadm
drsadm@hana-10:/usr/sap/DRS/HDB00> sapcontrol -nr 00 -function StartSystem HDB
11.05.2020 02:27:02
StartSystem
OK
```

Use the sapcontrol command to check the Start procedure.

drsadm@hana-10:/usr/sap/DRS/HDB00> sapcontrol -nr 00 -function GetSystemInstanceList

```
11.05.2020 02:27:11
```

```
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus
hana-10, 0, 50013, 50014, 0.3, HDB|HDB_WORKER, GRAY
11.05.2020 02:27:56
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus
hana-10, 0, 50013, 50014, 0.3, HDB|HDB_WORKER, GREEN
drsadm@hana-10:/usr/sap/DRS/HDB00>
```

The HANA database is now up and running. Additional customer-dependent failover tests can be executed as required.

## 5.6 Cleanup Operations

After finishing the testing process, follow these steps to clean up the environment.

- 1. Stop the HANA database.
- 2. Stop the SAP services.
- 3. Unmount the FlexClone volumes from the target host.
- 4. Delete the FlexClone volumes.
- 5. Delete the Snapshot backups.
  - **Note:** When the Snapshot backups are deleted at the source storage system, there can be delay until they are also deleted at the synchronous SnapMirror target. As soon as a new automated SnapMirror Snapshot is created (for resync operations), the Snapshot delete operation also happens at the target storage. If it is required to delete the Snapshot immediately, it can be deleted directly at the target storage.

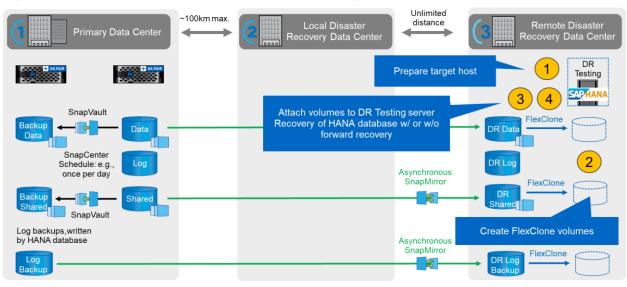
# 6 Asynchronous SnapMirror Disaster Recovery Testing

Depending on whether the log backup replication is part of the disaster recovery setup, the steps for disaster recovery are slightly different. This section describes the disaster recovery testing for data-backup-only replication. It also documents the differences if the log backups are also replicated.

To configure asynchronous SnapMirror disaster recovery testing, follow these steps.

- 1. Prepare the target host.
- 2. Create FlexClone volumes at the disaster recovery storage.
- 3. Mount the FlexClone volumes at the target host.
- 4. Recover the HANA database.
  - Data volume recovery only.
  - Forward recovery using replicated log backups.

The following subsections describe these steps in detail, as shown in Figure 26.



#### Figure 26) Asynchronous SnapMirror disaster recovery testing.

## 6.1 Prepare the Target Host

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

During normal operation, the target host is typically used for other purposes, for example, as a HANA QA or test system. Therefore, most of the described steps must be executed when disaster failover testing is executed. On the other hand, the relevant configuration files, like /etc/fstab and /usr/sap/sapservices, can be prepared and then put in production by simply copying the configuration file. The disaster recovery testing procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system.

#### **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.

**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. For full information, see the <u>SAP Host</u> Agent at the SAP help portal.

**Note:** If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

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

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the /etc/services file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the /usr/sap/sapservices file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
hana-10:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/DRS/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/DRS/HDB00/exe/sapstartsrv pf=/usr/sap/DRS/SYS/profile/DRS_HDB00_hana-10
-D -u drsadm
limit.descriptors=1048576
```

#### Prepare HANA Log Volume

Because the HANA log volume is not part of the SnapMirror replication, an empty log volume must exist at the target host. The log volume must include the same subdirectories as the source HANA system.

```
hana-10:/hana/log/DRS/mnt00001 # ls -al
total 84
drwxr-x--- 5 drsadm sapsys 4096 Apr 2 06:51 .
drwxr-x--- 1 drsadm sapsys 16 Apr 2 06:45 ..
drwxr-x--- 2 drsadm sapsys 61440 Apr 24 07:11 hdb00001
drwxr-xr-- 2 drsadm sapsys 12288 Apr 24 02:59 hdb00002.00003
drwxr-xr-- 2 drsadm sapsys 4096 Apr 24 08:31 hdb00003.00003
hana-10:/hana/log/DRS/mnt00001 #
```

#### Prepare Log Backup Volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host. A volume for the log backups must be configured and mounted at the target host.

**Note:** If log backup volume replication is part of the disaster recovery setup, a FlexClone volume is mounted at the target host and it is not necessary to prepare an additional log backup volume.

#### **Prepare File System Mounts**

Table 6 shows the naming conventions used in the lab setup. The volume names of the FlexClone volumes at the disaster recovery storage are included in /etc/fstab. These volume names are used in the FlexClone volume creation step in the next section.

HANA DRS Volumes	FlexClone Volume at Disaster Recovery Storage	Mount Point at Target Host
Data volume	DRS_data_mnt00001_dest_ clone	/hana/data/DRS/mnt00001
Shared volume	DRS_hana_shared_dest_ clone/shared DRS_hana_shared_ dest_clone/usr-sap	/hana/shared /usr/sap//DRS
Log backup volume	DRS_log_backup_dest_clone	/mnt/log-backup

Table 6) Volume names of FlexClone copies.

**Note:** A FlexClone copy of the log backup volume is required only if log backups are also replicated to the DR site.

Note: The mount points in Table 6 must be created at the target host.

Here are the required /etc/fstab entries.

```
hana-10:~ # cat /etc/fstab
192.168.175.116:/DRS_log_mnt00001 /hana/log/DRS/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_data_mnt00001_dest_clone /hana/data/DRS/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
```

192.168.175.116:/DRS_shared_dest_clone/shared /hana/shared nfs	
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0	0
192.168.175.116:/DRS_shared_dest_clone/usr-sap /usr/sap/DRS nfs	
<pre>rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0</pre>	0
192.168.175.116:/DRS_log_backup_dest_clone /mnt/log-backup nfs	
<pre>rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0</pre>	0
hana-10:~ #	

**Note:** In a Fibre Channel setup, the fstab entries depend on the multipath configuration. Because the SCSI IDs are different with each operation, the fstab file is not static and must be adapted after the LUN discovery process.

# 6.2 Create FlexClone Volumes at the Disaster Recovery Storage

Depending on the disaster recovery setup—with or without log backup replication—two or three FlexClone volumes must be created. In both cases, a FlexClone volume of the data and the shared volume must be created. A FlexClone volume of the log backup volume must be created if the log backup data is also replicated. Figure 27 through Figure 30 show the required steps using ONTAP System Manager.

	ONTAP Sys	tem	Mana	ager							(	9 🗖	٠	?	-
Swi	itch to the new exp	perience						Type:	All	~	Q Search	all Objects			+ -
		= î	Vol	umes	SVM hana-dr	•									
	Dashboard		+	Create 🥜 E	idit 📋 Delete 🚦 More Acti	ior -	na Davanta Dalata da an								
	Applications & Tie	ers 🕨		Status 😇	Name	Create FlexClor	e Volume					× tion 👻	Storage	E \Xi	Applic
	Storage		+	0	DRS_data_mnt00001_dest	Name:	DR5_data_mnt00001_dest_clone						Enabled		-NA-
	Nodes		+	٢	DRS_data_mnt00001_dest_sm_	S Thin Provi	•						Enabled	1	-NA-
	Aggregates &		+	٢	DRS_log_backup_dest		for the volume as it's used. Otherwise, the system reserves sp arent Snapshot copy	bace for t	ne entire volume.				Enabled	1	-NA-
	Disks	1	+	٢	DRS_log_mnt00001_dest_sm_s	Name			Date 👻				Enabled	I	-NA-
	SVMs		+	۲	DRS_shared_dest	snapmirro	r.87026c54-77cc-11e9-9e21-00a098d994db_2157901722.2020-	-05-12_04	25 May/12/20	20 04:25:01	A		Enabled	1	-NA-
	Volumes		+	٢	DRS_shared_dest_sm_s	snapmirro	r.87026c54-77cc-11e9-9e21-00a098d994db_2157901722.2020	-05-12_04	24 May/12/20	20 04:24:00			Enabled	1	-NA-
	LUNs						r_LocalSnapAndSnapMirror_Hourly_05-12-2020_02 22.00.9262			20 04:22:32					
	Qtrees						r.87026c54-77cc-11e9-9e21-00a098d994db_2157901726.2020								
	Quotas					shapining		00 12_0.		20 05.05.00	٣				
	Junction Paths														
l	Network														
l	Protection	-													
	Volume Relationships									Clone	Cancel				
	SVM DR Relationships														
	Protection Policie	es													
	Schodulos											D	isplaying 1	- 6 <	1.3

Figure 27) Create a FlexClone volume based on an application-consistent SnapCenter backup.

One of the SnapCenter backups is selected as a source for the FlexClone volume of the HANA data volume.

Kit with the new experience Notines </th <th>L</th> <th>ONTAP Syste</th> <th>m M</th> <th>ana</th> <th>iger</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Ø</th> <th></th> <th>*</th> <th>?</th> <th><b>:</b></th> <th>1</th>	L	ONTAP Syste	m M	ana	iger								Ø		*	?	<b>:</b>	1
Dashboard   Applications & Tiers   Storage   Storage   Nodes   Aggregates & Disks   SVMs   Volumes   Volumes <tr< th=""><th>( Sw</th><th>itch to the new experie</th><th>ence</th><th></th><th></th><th></th><th></th><th></th><th>Тур</th><th>e: All</th><th></th><th>~</th><th>Q Search al</th><th>l Objects</th><th></th><th></th><th>+</th><th>`</th></tr<>	( Sw	itch to the new experie	ence						Тур	e: All		~	Q Search al	l Objects			+	`
Applications & Tiles Applications & Tiles   Applications & Tiles i   Storage i   Nodes +   Okis_data_mmt00001_dets_ms_field   Aggregates & Ag		:		Volu	umes	SVM hana-dr	]											
Addition       Addite       Addite       Ad	•	Dashboard		+	Create 🧪	Edit 🗐 Delete 🚦 More Actions	View Missing	Protection Relationships C Refre	h									
Nodes       +       0       DRS_dsta_mn00001_dst_gam_S       Flex/ord         Aggregates & DRS_dsta_mn00001_dst_gam_S       Flex/ord       Flex/ord       Improvisioning       Auxe:       Quota       Quota       Quotas       PRS_log_mated_dest_sm_S       Flex/ord       Flex/ord       Mame:       Quota       Quotas       Improvisioning       Auxe:       Auxe:       Quotas       Quotas       Quotas       PRS_log_mated_dest_sm_S       Flex/ord       Flex/ord       Auxe:       Auxe:       Auxe:       Auxe:       Quotas       Auxe:       Auxe: <td< td=""><td></td><td>Applications &amp; Tiers</td><td>•</td><td></td><td>Status 😇</td><td>Name</td><td>Style 👳</td><td>Create FlexClone Volume</td><td></td><td></td><td>×</td><td>Туре</td><td>T Protec</td><td>tion \Xi</td><td>Storage E</td><td> <del></del></td><td>Applic</td><td>c</td></td<>		Applications & Tiers	•		Status 😇	Name	Style 👳	Create FlexClone Volume			×	Туре	T Protec	tion \Xi	Storage E	<del></del>	Applic	c
Aggrogates & Disks       +       0       Disks       Rexvol       Aggrogates & Disks       Rexvol       Aggrogates & Disks       Rexvol       Aggrogates & Disks       Aggr		Storage	•	+	۲	DR5_data_mnt00001_dest	FlexVol	Name: DRS_log_backup	dest_clone			dp	No		Enabled		-NA-	
Appendix and Disk     Image: Disk disk </td <td></td> <td>Nodes</td> <td></td> <td>+</td> <td>۲</td> <td>DRS_data_mnt00001_dest_sm_s</td> <td>FlexVol</td> <td>Thin Provisioning</td> <td></td> <td></td> <td></td> <td>dp</td> <td>No</td> <td></td> <td>Enabled</td> <td></td> <td>-NA-</td> <td></td>		Nodes		+	۲	DRS_data_mnt00001_dest_sm_s	FlexVol	Thin Provisioning				dp	No		Enabled		-NA-	
SVMS + • <			•	+	۲	DRS_log_backup_dest	FlexVol		t's used. Otherwise, the	system reserve	es	dp	No		Enabled		-NA-	
*     DR5_shared_dest_sin_s     Flexivol       Volumes     +     •     DR5_shared_dest_sin_s     Flexivol       UNs     +     •     DR5_shared_dest_sin_s     Flexivol       Volumes     Quitas     -     -       Junction Paths     -     -     -       Network     -     -     -       Protection     -     -     -       Events & Jobs     -     -     -				+	۲	DRS_log_mnt00001_dest_sm_s	FlexVol	FlexClone parent Snapshot co	у			dp	No		Enabled		-NA-	
+ • • • • • • • • • • • • • • • • • • •				+	۲	DRS_shared_dest	FlexVol	Name	Date			dp	No		Enabled		-NA-	
Vtres       Vutas       Junction Paths       Network       Protection       Events & Jobs				+	۲	DRS_shared_dest_sm_s	FlexVol									_	-NA-	
Quotas       Junction Paths       Network       Protection       Events & Jobs								shapmirror.87020C54-77CC-11	e9-9e21-00a096 May/	12/2020 07:	e9	-9e21-00a09	98d994db_21579	01723.2020	-05-12_0700	000		
Junction Paths       Network       Protection       Events & Jobs																		
Network     >       Protection     >       Events & Jobs     >																		
Protection     >       Events & Jobs     >																		
Events & Jobs																		
			*															
Configuration	<b></b>	Events & Jobs	•															
	•	Configuration	•						Clone	Cancel								
															Displaying 1			

Figure 28) Create a FlexClone copy of the log backup volume.

As a source for the log backup FlexClone volume, one of the SnapMirror Snapshot copies is selected.

I.	ONTAP Syste	m M	lana	ger									Ø 📮	٠	?	2	
0: Sw	itch to the new experie	ence								Type: All		~	○ Search all Objects			+	~
	i	=	Volur	nes	SVM hana-dr 🔻												
-8	Dashboard		+ 0	reate 🧪	Edit 📄 Delete 🚦 More Actions	View Missing Pi	rotection Relation	nships C Refresh	ı								0
	Applications & Tiers	۲		Status 👻	Name 😎	Style 📼	Aggre 👻	Thin Provis \Xi	Availa \Xi	Total S \Xi	% Used 😇	Туре	Terretection Terretection	Storage E.		Applic	
	Storage	*	+	۲	DRS_data_mnt00001_dest_clone	FlexVol	aggr1_2	Yes	1.78 GB	8.91 GB	80	rw	No	Enabled		-NA-	
	Nodes		+	0	DRS_log_backup_dest_clone	FlexVol	aggr1_2	Yes	640.58 MB	4.09 GB	84	rw	No	Enabled		-NA-	
	Aggregates & Disks	•	+	0	DRS_shared_dest_clone	FlexVol	aggr1_2	Yes	3.34 GB	21.07 GB	84	rw	No	Enabled		-NA-	
	SVMs																
	Volumes																
	LUNs																
	Qtrees																
	Quotas																
	Junction Paths																
÷	Network	۲															
9	Protection	٠															
	Events & Jobs	•															
<del>हे</del>	Configuration	•															
														Displaying 1 -			

Figure 29) List of FlexClone volumes.

#### Figure 30) Junction path configuration.

ONTAP System	n Manager							Q		٠	0	<u> </u>	
witch to the new experien	ce				Туре	: All	~	Q, Search a	Il Objects			+	3
=	Junction Paths	SVM hana-	dr 🔹										
Dashboard	🕞 Mount 📑 Unmo	ount 🧳 Change Export	Policy C Refresh										
Applications & Tiers 🕨	Path		Storage Object	Export Policy	Security Style								
Storage 👻	4 <del></del> /		🛢 dr_root	default	unix								
Storage	The sting of the s	og_backup	DR_testing_log_backup	default	unix								
Nodes	TRS_shared_	_dest_sm_s	DRS_shared_dest_sm_s	default	unix								
	TRS_log_mnt	t00001_dest_sm_s	DRS_log_mnt00001_dest_sm_s	default	unix								
Aggregates &	TRS_log_mnt	t00001	BRS_log_mnt00001	default	unix								
Disks	TRS_log_bac	kup	BRS_log_backup	default	unix								
Cloud Tiers	TRS_data_m	nt00001_dest_sm_s	BRS_data_mnt00001_dest_sm_s	default	unix								
diddd frafo	😴 DRS_data_m	nt00001_dest_clone	BRS_data_mnt00001_dest_clone	default	unix								
Aggregates	TRS_log_bac	kup_dest_clone	BRS_log_backup_dest_clone	default	unix								
	TRS_shared_	_dest_clone	BDR5_shared_dest_clone	default	unix								
Storage Pools													
Disks													
SVMs													
Volumes													
	General												
LUNs	Name:	DRS_shared_dest_cl	one										
Qtrees			unc.										
Quotas	Type:	Volume											
Quotas	Junction Path:	/DRS_shared_dest_c	lone										
Junction Paths	Export Policy:	default											
Network 🕨													
Protection +													
rioccourt P													

All volumes must be mounted to the namespace.

**Note:** In a Fibre Channel setup, the LUNs in the FlexClone volumes must be mapped to the initiator group of the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

# 6.3 Mount the FlexClone Volumes at the Target Host

The FlexClone volumes can now be mounted at the target host.

hana-10:~ # mount -a

The following output shows the required file systems.

hana-10:~ # df				
Filesystem	1K-blocks	Used	Available	Use% Mounted on
192.168.175.116:/DRS log mnt00001	104857600	512	104857088	18
/hana/log/DRS/mnt00001				
192.168.175.116:/DRS data mnt00001 dest clone	9343040	7479488	1863552	81%
/hana/data/DRS/mnt00001				
192.168.175.116:/DRS shared dest clone/shared	22094464	18594048	3500416	85% /hana/shared
192.168.175.116:/DRS shared dest clone/usr-sap	22094464	18594048	3500416	85% /usr/sap/DRS
192.168.175.116:/DR testing log backup	104857600	256	104857344	1% /mnt/log-
backup				

**Note:** If log backups are also replicated, the log backup FlexClone volume would be mounted instead of the above log backup volume.

```
192.168.175.116:/DRS_log_backup_dest_clone 4288448 3632448 656000 85% /mnt/log-
backup
hana-10:~ #
```

**Note:** In a Fibre Channel setup, additional steps are required before the LUNs can be mounted at the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

# 6.4 Check Consistency of Latest Log Backups

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.

To check the consistency of the latest log backups, follow these steps.

1. List the latest log backups in the log backup directory. The following output shows the latest log backups for the system and the tenant database in the lab environment.

drsadm@hana-10:/usr/sap/DRS/home> ls -altr /mnt/log-backup/SYSTEMDB
-rw-r 1 drsadm sapsys 1396736 May 12 08:38
log_backup_1_0_1619642560_1619664192.1589287111110
-rw-r 1 drsadm sapsys 1232896 May 12 08:53
log_backup_1_0_1619664192_1619683264.1589288011113
-rw-r 1 drsadm sapsys 1236992 May 12 09:08
log_backup_1_0_1619683264_1619702400.1589288911115
-rw-r 1 drsadm sapsys 561152 May 12 09:08 log_backup_0_0_0_0.1589288911144
-rw-r 1 drsadm sapsys 561152 May 12 09:22 log backup 0 0 0 0.1589289757361
-rw-r 1 drsadm sapsys 561152 May 12 09:23 log backup 0 0 0 0.1589289787462
-rw-r 1 drsadm sapsys 561152 May 12 09:23 log backup 0 0 0 0.1589289788236
-rw-r 1 drsadm sapsys 1945600 May 12 09:23
log_backup_1_0_1619702400_1619732608.1589289811118
-rw-r 1 drsadm sapsys 561152 May 12 09:23 log_backup_0_0_0_0.1589289811148

drsadm@hana-10:/usr/sap/DRS/home> ls -altr /mnt/log-backup/DB DRS/
-rw-r 1 drsadm sapsys 118784 May 12 07:48
log backup 3 0 1016494848 1016496512.1589284100889
-rw-r 1 drsadm sapsys 65536 May 12 07:48 log_backup_2_0_14169280_14170112.1589284124059
-rw-r 1 drsadm sapsys 61440 May 12 08:03
log_backup_3_0_1016496512_1016497280.1589285000892
-rw-r 1 drsadm sapsys 49152 May 12 08:18
log_backup_3_0_1016497280_1016497856.1589285900896
-rw-r 1 drsadm sapsys 45056 May 12 08:33
log_backup_3_0_1016497856_1016498368.1589286800899
-rw-r 1 drsadm sapsys 118784 May 12 08:48
log_backup_3_0_1016498368_1016500032.1589287700902
-rw-r 1 drsadm sapsys 65536 May 12 08:48 log_backup_2_0_14170112_14170944.1589287724082
-rw-r 1 drsadm sapsys 90112 May 12 09:03
log backup 3 0 1016500032 1016501248.1589288600905
-rw-r1 drsadm sapsys 602112 May 12 09:03 log_backup_0_0_0.1589288600925
-rw-r 1 drsadm sapsys 49152 May 12 09:18
log backup 3 0 1016501248 1016501824.1589289500908
-rw-r 1 drsadm sapsys 606208 May 12 09:18 log backup 0 0 0 0.1589289500928
-rw-r 1 drsadm sapsys 606208 May 12 09:22 log backup 0 0 0.1589289757363
-rw-r 1 drsadm sapsys 606208 May 12 09:23 log backup 0 0 0.1589289787926
-rw-r 1 drsadm sapsys 606208 May 12 09:23 log backup 0 0 0 0.1589289788730
drwxr-xr 2 drsadm sapsys 176128 May 12 09:23 .
drsadm@hana-10:/usr/sap/DRS/home>

#### 2. Check the latest log backups for these services by running the hdbbackupcheck command.

```
drsadm@hana-10:/usr/sap/DRS/home> hdbbackupcheck /mnt/log-
backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148' successfully checked.
drsadm@hana-10:/usr/sap/DRS/home> hdbbackupcheck /mnt/log-
backup/SYSTEMDB/log_backup_1_0_1619702400_1619732608.1589289811118
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
```

```
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_1_0_1619702400_1619732608.1589289811118' successfully
checked.
drsadm@hana-10:/usr/sap/DRS/home>
```

```
drsadm@hana-10:/usr/sap/DRS/home> hdbbackupcheck /mnt/log-
backup/DB DRS/log backup 0 0 0 0.1589289788730
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/DB DRS/log backup 0 0 0 0.1589289788730' successfully checked.
drsadm@hana-10:/usr/sap/DRS/home> hdbbackupcheck /mnt/log-
backup/DB_DRS/log_backup 3 0 1016501248 1016501824.1589289500908
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/DB DRS/log backup 3 0 1016501248 1016501824.1589289500908' successfully
checked.
drsadm@hana-10:/usr/sap/DRS/home> hdbbackupcheck /mnt/log-
backup/DB_DRS/log_backup_2 0 14170112 14170944.1589287724082
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/DB DRS/log backup 2 0 14170112 14170944.1589287724082' successfully
checked.
drsadm@hana-10:/usr/sap/DRS/home>
```

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.

# 6.5 Recover the HANA Database

Start the required SAP services.

hana-10:~ # systemctl start sapinit

The following output shows the required processes.

```
hana-10:~ # ps -ef | grep sap
root.
         15919 1 0 06:36 ?
                                          00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host profile
sapadm 15941 1 0 06:36 ? 00:00:00 /usr/lib/systemd/systemd --user

        sapadm
        15943
        15941
        0
        06:36 ?
        00:00:00 (sd-pam)

        sapadm
        15963
        1
        3
        06:36 ?
        00:00:00 /usr/sap/hostctrl/exe/sapstartsrv

pf=/usr/sap/hostctrl/exe/host profile -D
                                          00:00:00 /usr/sap/DRS/HDB00/exe/sapstartsrv
drsadm 16027 1 1 06:36 ?
pf=/usr/sap/DRS/SYS/profile/DRS HDB00 hana-10 -D -u drsadm
root 16161 1 0 06:36 ?
                                          00:00:00 /usr/sap/hostctrl/exe/saposcol -1 -w60
pf=/usr/sap/hostctrl/exe/host profile
root 16163 5714 0 06:36 pts/0 00:00:00 grep --color=auto sap
hana-10:~ #
```

The following subsections describe the recovery process using HANA Studio for the system database and the tenant database. The screenshots show recovery without and with forward recovery using replicated log backups.

#### If HANA Studio is used for recovery, the file

/hana/shared/DRS/global/hdb/metadata/net publicname/hana-10 must be adapted to

include the correct IP address of the disaster recovery testing server. Otherwise, HANA Studio will try to access the original HANA system.

```
drsadm@hana-10:/> cat /hana/shared/DRS/global/hdb/metadata/net_publicname/hana-10
10.63.167.175
```

### **Recover the System Database**

In HANA Studio, select Recover System Database and then select Recover to a Specific Data Backup.

Figure 31) Recovery to a specific data backup: Recovery Type.

hdbstudio - System: SYSTEMDB@DRS Host: hana-10 Instance:	00 - SAP HANA Stu	dio		
File Edit Navigate Project Run Window Help				
📑 🕶 🔛 🐚 🐇 🖛 🖓 🕶 🛟 🕶 🖨 💌		Recovery of SYSTEMDB@DRS	×	
		Specify Recovery Type		
₽ F® Systems X	SYSTEMDB@DI	Select a recovery type.		
🖹 👻 🔛 🖬 🕶 🚑 🖻 😫 🄝	🚯 SYSTEMDE	Recover the database to its most recent state <sup>8</sup>		
B DRS@00 (SYSTEM) DR Testing	Version: 2.00.	Recover the database to the following point in time <sup>®</sup>		
SYSTEMDB@DRS (SYSTEM) DR Testing	S Emergency inf			
	Processes Diagnos	Date: 2020-05-13 🔀 Time: 10:33:13		
	Host: <all></all>	Select Time Zone: (GMT-04:00) Eastern Daylight Time		
	Active Host	i System Time Used (GMT): 2020-05-13 14:33:13		
	😑 hana-10	Recover the database to a specific data backup <sup>®</sup>		
		Recover the database to a specific data backup-		
			Advanced >>	

**Note:** For forward recovery using the replicated log backups, select the recovery type Recover to Most Recent State.

Figure 32) Recovery with log backups: Recovery Type.

Recovery of SYSTE	■ Recovery of SYSTEMDB@DRS >								
Specify Recovery Typ	e								
Select a recovery type.									
Recover the data	base to its most recent state <sup>®</sup>								
Recover the data	base to the following point in time <sup>1</sup>								
Date:	2020-05-20 Time: 08:34:54								
Select Time Zone:	(GMT-04:00) Eastern Daylight Time 👻								
i System Time	i System Time Used (GMT)- 2020-05-20 12:34:54								
Recover the data	base to a specific data backup <sup>®</sup>								
	Advanced >	>							

Select Recover Without Backup Catalog.

Figure 33) Recovery to a specific data backup: Specify backup catalog location.

Recovery of SYSTEMDB@DR	S	×							
pecify Backup Location									
Choose whether you want to select a the next step.	a backup from a backup catalog or enter the name and the path of a backup in								
O Recover using the backup cat	alog								
O Search for the backup cat	alog in the file system only								
Backup Catalog Location:	/usr/sap/DRS/HDB00/backup/log/SYSTEMDB								
Recover without the backup catalog									
Backint System Copy									
Backint System Copy									
Source System:									

**Note:** For forward recovery using the replicated log backups, the backup catalog location must be specified.

Figure 34) Recovery with log backups: Backup catalog location.

Recovery of SYSTEMDB@DRS	×
Locate Backup Catalog	
Specify location of the backup catalog.	
Recover using the backup catalog	
Search for the backup catalog in the file system only	
Backup Catalog Location: /mnt/log-backup/SYSTEMDB	
Recover without the backup catalog	
Backint System Copy-	
Backint System Copy	
Source System:	
Source system.	

### Select Snapshot as the destination type.

Figure 35) Recovery to a specific data backup: Select Destination Type.

Recovery of S	SYSTEMDB@DRS	×
Specify the Back	sup to Recover	
Specify the backu	p to be recovered.	
Destination Type Locate the Data E Specify the dest		
Location:	/hana/data/DRS	
Backup Prefix:		

**Note:** For forward recovery using the replicated log backups, HANA Studio shows the availability of the Snapshot copy with a green icon.

Figure 36) Recovery with log backups: Backup selection.

Recovery of SYSTEMD	B@DRS				:
elect a Backup					
elect a backup to recover th	ne SAP HANA database				
elected Point in Time					
atabase will be recovered t	to its most recent state.				
ackups					
he overview shows backup ecovery time.	is that were recorded in the bac	kup catalog as successful. Th	e backup at the top is a	estimated to hav	e the shortest
Start Time	Location	Backup Prefix		Available	
2020-05-20 05 22 26	/hana/data/DRS	SNAPSHOT			
2020-05-20 01:22:23	/hana/data/DRS	SNAPSHOT	8		
2020-05-19 21:22:24	/hana/data/DRS	SNAPSHOT	0		
2020-05-19 17:22:23	/hana/data/DRS	SNAPSHOT	0		
2020-05-19 13:22:23	/hana/data/DRS	SNAPSHOT	0		
2020-05-19 09:38:24	/hana/data/DRS	SNAPSHOT	8		
2020-05-19 09:22:23	/hana/data/DRS	SNAPSHOT	0		
2020-05-19 05:22:23	/hana/data/DRS	SNAPSHOT	0		
2020-05-19 01:22:24	/hana/data/DRS	SNAPSHOT	0		
2020-05-18 21:22:24	/hana/data/DRS	SNAPSHOT	0		
etails of Selected Item tart Time: 0 2021		-		Refresh	Show More
	0-05-20 05:22:26 Destination				
ize: 9.13		1589966546 External	Backup ID: SnapCente	er_LocalSnapAn	SnapMirror,
ackup Name: /han	a/data/DRS				
Iternative Location:					
				Chec	k Availabilit

### Provide a log backup destination for recovery.

Figure 37) Recovery with log backups: Log backup location.

Recovery of SYSTEMDB@DRS	×
Locate Log Backups	
Specify location(s) of log backup files to be used to recover the database.	
Even if no log backups were created, a location is still needed to read data that will be used for recovery. If the log backups were written to the file system and subsequently moved, you need to specify their current location. If ye an alternative location for the log backups, the system uses the location where the log backups were first saved. The din will be searched recursively.	
Locations:	Add
/mnt/log-backup/SYSTEMDB	Remove All

For recovery to a specific backup, Initialize Log Area is preselected.

Figure 38) Recovery to a specific data backup: Other Settings.

Recovery of SYSTEMDB@DRS	Х
Other Settings	
Initialize Log Area	
If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.	
✓ Initialize Log Area <sup>®</sup>	
Use Delta Backups	
Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.	
Use Delta Backups (Recommended)	
Install New License Key	
If you recover the database from a different system, the old license key will no longer be valid You can:	
<ul> <li>Select a new license key to install now</li> <li>Install a new license key manually after the database has been recovered</li> </ul>	
Install New License Key	
Browse	

**Note:** For forward recovery using the replicated log backups, Initialize Log Area must be selected.

Figure 39) Recovery with log backups: Other Settings.

Recovery of SYSTEMDB@DRS				×
Other Settings				
Check Availability of Delta and Log Backups				
You can have the system check whether all required delta and log back log backups are missing, they will be listed and the recovery process wi check now, it will still be performed but later. This may result in a signif	Il stop before any da	ta is changed. I	f you choose not to	perform this
Check the availability of delta and log backups:				
✓ File System <sup>8</sup>				
Third-Party Backup Tool (Backint)				
Initialize Log Area				
If you do not want to recover log segments residing in the log area, select the log area.	ct this option. After th	ne recovery, the	log entries will be	deleted from
✓ Initialize Log Area <sup>B</sup>				
Select this option if you want to perform a recovery using delta backups. backups will be used. Use Delta Backups (Recommended) Install New License Key- If you recover the database from a different system, the old license key w You can: - Select a new license key to install now - Install a new license key manually after the database has been recover Install a new License Key	vill no longer be valio		without delta back	Browse
0	< Back	Next >	Cancel	Finish

Figures 40, 41, and 42 summarize the different recovery processes.

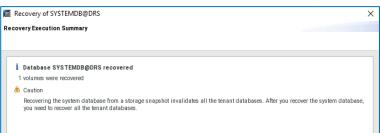
Figure 40) Recovery to a specific data backup: Review Recovery Settings.

Recovery of SYSTEMDB@DRS				×	
Review Recovery Settings					
Review the recovery settings and choose 'Finish' to start the recovery. You choosing 'Back' .	can modify the rea	covery settings by			
Database Information					
Database: SYSTEMDI Host: hana-10 Version: 2.00.044	3@DRS 00.1571081837				
	Data Backup Rec	overy)			
Caution Recovering the system database from a storage snapshot invalidate you need to recover all the tenant databases.	es all the tenant d	atabases. After yo	ou recover the syste	em database,	
Configuration File Handling Caution To recover customer-specific configuration changes, you may need to More Information: SAP HANA Administration Guide	make the change	s manually in the	target system.		
SQL Statement			×		
		Сору	Close		
Show SQL Statement					
?	< Back	Next >	Cancel	Finish	

Figure 41) Recovery with log backups: Review Recovery Settings.

Database Info	rmation		
Database: Host: Version:		SYSTEMDB@DRS hana-10 2.00.044.00.1571081837	
RecoveryDefi RecoveryType		Snapshot (Point-in-Time Recovery (Until Now))	
	the system database from a storage s recover all the tenant databases.	napshot invalidates all the tenant databases. After you recover the syst	em databas
	ion: SAP HANA Administration Guid	, you may need to make the changes manually in the target system.	
wore mortha		-	_
mare mortha	SQL Statement RECOVER DATABASE UNTIL TIM (/mnt/log-backup/SYSTEMDB') L	S ESTAMP '2021-05-20 13:15:11' CLEAR LOG USING CATALOG PATH SING LOG PATH (/mnt/log-backup/SYSTEMOB') USING DATA PATH ata/SYSTEMDB') USING SNAPSHOT CHECK ACCESS USING FILE	

Figure 42) Recovery to a specific data backup: Recovery Execution Summary.



# **Recover a Tenant Database**

In HANA Studio, select Recover Tenant Database and then select a tenant.

Figure 43) Recovery of Tenant Database in DRS.

Recovery of Tenant Database in DRS	×
Specify tenant database	
type filter text	Ø
🕑 DRS	

Select the recovery type Recover the Database to a Specific Data Backup.

Figure 44) Recovery to a specific data backup: Recovery Type.

Recovery of Tenan	t Database in DRS	×
Specify Recovery Typ	e	
Select a recovery type.		
$\bigcirc$	pase to its most recent state <sup>1</sup>	
	ase to the following point in time	
Date:	2020-05-13 Time: 11:01:44	
Select Time Zone:	(GMT-04:00) Eastern Daylight Time	
🧴 System Time	Used (GMT): 2020-05-13 15:01:44	
Recover the data	base to a specific data backup	
	Advanced >	>

**Note:** For forward recovery using the replicated log backups, select the recovery type Recover the Database to the Most Recent State.

Figure 45) Recovery with log backups: Specify Recovery Type.

Recovery of Tenar	it Database in DRS	×
Specify Recovery Typ	e	
Select a recovery type.		
Recover the data	base to its most recent state <sup>®</sup>	
O Recover the data	base to the following point in time <sup>8</sup>	
Date:	2020-05-25 Time: 05.21:03	
Select Time Zone:	(GMT-04:00) Eastern Daylight Time	
i System Time	Used (GMT): 2020-05-25 09-21:03	
<ul> <li>Recover the data</li> </ul>	base to a specific data backup <sup>®</sup>	
	Advanced >	>

### Select Recover Without the Backup Catalog.

Figure 46) Recovery to a specific data backup: Specify backup catalog location.

盾 Recovery of Tenant Database	in DRS	Х
Specify Backup Location		
Choose whether you want to select a the next step.	backup from a backup catalog or enter the name and the path of a backup in	
Recover using the backup cat	alog	
Search for the backup cat	alog in the file system only	
Backup Catalog Location:	/usr/sap/DRS/HDB00/backup/log/DB_DRS	
Recover without the backup c Backint System Copy Backint System Copy	atalog	
Source System:		

# **Note:** For forward recovery using the replicated log backups, the backup catalog location must be specified.

Figure 47) Recovery with log backups: Specify backup catalog location.

Recovery of Tenant Database in DRS	×
Locate Backup Catalog	
Specify location of the backup catalog.	
Recover using the backup catalog	
<ul> <li>Search for the backup catalog in the file system only</li> </ul>	
Backup Catalog Location: /mnt/log-backup#DB_DRS	
Recover without the backup catalog	
Backint System Copy	
Backint System Copy	
Source System:	

Figure 48) Recovery to a specific data backup: Select Destination Type.

盾 Recovery of T	enant Database in DRS	×
Specify the Back	ip to Recover	
Specify the backup	to be recovered.	
Destination Type:	Snapshot 👻	
Locate the Data B		
	nation of the data backup that you want to use to recover the database.	
Location:	/usr/sap/DRS/SYS/global/hdb/backint/DB_DRS	
Dealure Deafur		
Backup Prefix:		

**Note:** For forward recovery using the replicated log backups, HANA Studio shows the availability of the Snapshot copy with a green icon.

Figure 49) Recovery with log backups: Select a Backup.

To recover this snapshot,	it must be available in the data	area.	
Database will be recovered to	o its most recent state		
Backups			
The overview shows backup recovery time.	s that were recorded in the back	up catalog as successful. Th	ne backup at the top is estimated to have the shore
Start Time	Location	Backup Prefix	Available
2020-05-20 05:22:26	/hana/data/DRS	SNAPSHOT	🥮 ( )
2020-05-20 01:22:23	/hana/data/DRS	SNAPSHOT	0
2020-05-19 21:22:24	/hana/data/DRS	SNAPSHOT	0
2020-05-19 17:22:23	/hana/data/DRS	SNAPSHOT	0
2020-05-19 13:22:23	/hana/data/DRS	SNAPSHOT	0
2020-05-19 09:38:24	/hana/data/DRS	SNAPSHOT	0
2020-05-19 09:22:23	/hana/data/DRS	SNAPSHOT	0
2020-05-19 05:22:23	/hana/data/DRS	SNAPSHOT	8
2020-05-19 01:22:24	/hana/data/DRS	SNAPSHOT	8
2020-05-18 21:22:24	/hana/data/DRS	SNAPSHOT	8
etails of Selected Item			Refres h Show !
tart Time: 8 2020	0-05-20 05:22:26 Destination 1	ype: SNAPSHOT Source Sy	ystem: DRS@DRS
ize: 5.81	GB Backup ID:	1589966546 External	Backup ID: SnapCenter_LocalSnapAndSnapMir
ackup Name: 🛛 🚨 /hana	a/data/DRS		
Iternative Location:			
			Check Availab
			Check Availab

For recovery to a specific backup. Initialize Log Area is preselected.

Figure 50) Recovery to a specific data backup: Other Settings.

Recovery of Tenant Database in DRS	Х
Other Settings	
Initialize Log Area	
If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.	
Initialize Log Area	
Use Delta Backups	
Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.	
Use Delta Backups (Recommended)	
Install New License Key	
If you recover the database from a different system, the old license key will no longer be valid You can:	
- Select a new license key to install now	
- Install a new license key manually after the database has been recovered	
Install New License Key	
Browse	

**Note:** For forward recovery using the replicated log backups, the Initialize Log Area option must be selected.

	enant Database in DRS				
eview Recovery	Settings y settings and choose 'Finish' to start the rea	covery. You can modify the reco	overy settings by		
hoosing 'Back'.					
Database Info	rmation				
Database: Host: Version:		DRS@DRS hana-10 2.00.044.00.1571081837			
Recovery Defin Recovery Type		Snapshot (Data Backup Reco	wery)		
Configuration I	File Handling				
💩 Caution					
~	SQL Statement	OT CLEARLOG		×	
			Сору	Close	
Show SQL Statem	nent				

Figure 51) Recovery to a specific data backup: Review Recovery Settings.

Figure 52) Recovery Execution Summary.

Recovery of Tenant Database in DRS	×
Recovery Execution Summary	
i Database DRS@DRS recovered	
2 volumes were recovered	

#### Figure 53) HANA Studio: System recovered.

hdbstudio - System: DRS@00 Host: hana-10 Instance: 00 Conne	cted User: SYSTEM System Usage: Test System - SAP HANA Studio	– 🗆 X
File Edit Navigate Project Run Window Help		
T ▼ □ □ □ 20 ▼ 0 ▼ 0 ▼ 0 ▼ 0 ▼		Quick Access
₽ Bystems X	ST DRS@00 23	- 8
y-gretems 32          Image: Second	iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	Last Update: May 13, 2020 11:21:42 AM 💸 🕪 Interval: 60 🗸 Seconds 🔞 🕞
0 items selected	Meccane Plun-in	Date 🚽
o numo outorida		

### **Recover Using the Command Line**

Instead of using HANA Studio, recovery can also be done by using the command line, or it can be automated by using scripts.

#### System Database Recovery

• Without log backups.

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG"
```

• With log backups.

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP `timestamp' CLEAR LOG USING CATALOG PATH (`/mnt/log-backup/SYSTEM-DB') USING LOG PATH (`/mnt/log-backup/SYSTEM-DB') USING SNAPSHOT"
```

#### **Tenant Database Recovery**

• Without log backups.

Within hdbsql: RECOVER DATA FOR DRS USING SNAPSHOT CLEAR LOG

### • With log backups.

```
Within hdbsql: RECOVER DATABASE UNTIL TIMESTAMP 'timestamp' CLEAR LOG USING CATALOG PATH ('/mnt/log-backup/DRS-DB') USING LOG PATH ('/mnt/log-backup/DRS-DB') USING SNAPSHOT
```

# 7 Overview of Disaster Recovery Failover

Most of the required steps for disaster failover are identical to those described in section 4, Overview of Disaster Recovery Testing.

Table 4 is a high-level overview of the required steps. The following sections describe the disaster recovery failover workflow in detail.

	Synchronous SnapMirror	Asynchronous SnapMirror
Prepare target host	<ol> <li>Install SAP host agent.</li> <li>Configure user, ports, SAP services.</li> <li>Create mount points.</li> <li>Prepare /etc/fstab.</li> </ol>	<ol> <li>Install SAP host agent.</li> <li>Configure user, ports, and SAP services.</li> <li>Create mount points.</li> <li>Mount a new, empty log volume and create subdirectories identical to the source system.</li> <li>Prepare /etc/fstab.</li> </ol>
Break the SnapMirror relation at the target storage	ONTAP System Manager: 1. SnapMirror quiesce, SnapMirror break for data, log, and shared volume.	<ul> <li>ONTAP System Manager:</li> <li>1. SnapMirror quiesce, SnapMirror break for data, and shared volume.</li> <li>Same for log backup volume (if log backup replication is part of the DR concept).</li> </ul>
Mount volumes at target host <b>Note:</b> This step requires additional LUN discovery operations in an FC SAN environment.	1. Mount data, log, and shared volume.	<ol> <li>Mount data and shared volume.</li> <li>Mount log backup volume (if log backup replication is part of the DR concept).</li> </ol>
Start or recover the HANA database	<ol> <li>Start SAP services.</li> <li>Start HANA database. Crash recovery is executed.</li> </ol>	1. Start SAP services. The HANA database is recovered to the last backup (or recovered with forward recovery using log backups, if log backup replication is part of the DR concept).

Table 7) Disaster recovery testing – required steps.

# 8 Synchronous SnapMirror Disaster Recovery Failover

To configure synchronous SnapMirror disaster recovery failover, follow these steps.

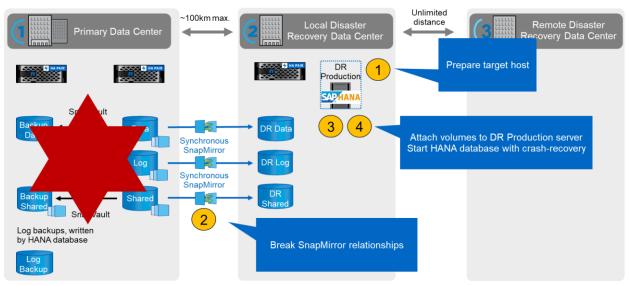
- 1. Prepare the target host.
- 2. Break SnapMirror relationships.

- 3. Mount volumes at the target host.
- 4. Start the HANA database.

The following sections describe these steps in detail.

**Note:** Manual steps are described for the different operations. All the steps could also be automated by using scripts or other automation tools.

Figure 54) Synchronous SnapMirror disaster recovery failover.



# 8.1 Prepare Target Host

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

During normal operation, the target host is typically used for other purposes—for example, as a HANA QA or test system. Therefore, most of the described steps must be executed when a disaster failover happens. On the other hand, the relevant configuration files, like /etc/fstab and /usr/sap/sapservices, can be prepared and then put in production simply by copying the configuration file. The disaster recovery testing procedure, as described in section 5, Synchronous SnapMirror Disaster Recovery Testing, ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system.

### **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. As an alternative, a virtual IP address concept can be used as well.

### Install Required Software

The SAP host agent software must be installed at the target server. For full information, see the <u>SAP Host</u> Agent at the SAP help portal.

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

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the /etc/services file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the /usr/sap/sapservices file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
hana-10:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/DRS/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/DRS/HDB00/exe/sapstartsrv pf=/usr/sap/DRS/SYS/profile/DRS_HDB00_hana-10
-D -u drsadm
limit.descriptors=1048576
```

### Prepare Log Backup Volume

Because the source system is configured with a separate volume for the HANA log backups, the log backup volume must also be available at the target host.

A volume for the log backups must be configured and mounted at the target host.

### **Prepare File System Mounts**

Table 8 shows the naming conventions that were used in the lab setup. The volume names of the FlexClone volumes at the disaster recovery storage were included in /etc/fstab. These volume names were used in the FlexClone volume creation step in the next section.

HANA DRS Volumes	Volume at Disaster Recovery Storage	Mount Point at Target Host
Data volume	DRS_data_mnt00001_dest_sm_s	/hana/data/DRS/mnt00001
Log volume	DRS_log_mnt00001_dest_sm_s	/hana/log/DRS/mnt00001
Shared volume	DRS_hana_shared_sm_s/shared DRS_hana_shared_sm_s/usr-sap	/hana/shared /usr/sap//DRS

Table 8) Volume names of FlexClone volumes.

The mount points in Table 8 must be created at the target host.

The required /etc/fstab entries are the following.

```
hana-10:~ # cat /etc/fstab
192.168.175.116:/DRS_log_backup /mnt/log-backup nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_data_mnt00001_dest_sm_s /hana/data/DRS/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_log_mnt00001_dest_sm_s /hana/log/DRS/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_shared_dest_sm_s/shared /hana/shared nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
192.168.175.116:/DRS_shared_dest_sm_s/usr-sap /usr/sap/DRS nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0
```

```
Note: In a Fibre Channel setup, the fstab entries depend on the multipath configuration. Because the SCSI IDs are different with each operation, the fstab file is not static and needs to be adapted after the LUN discovery process.
```

# 8.2 Break SnapMirror Relationships

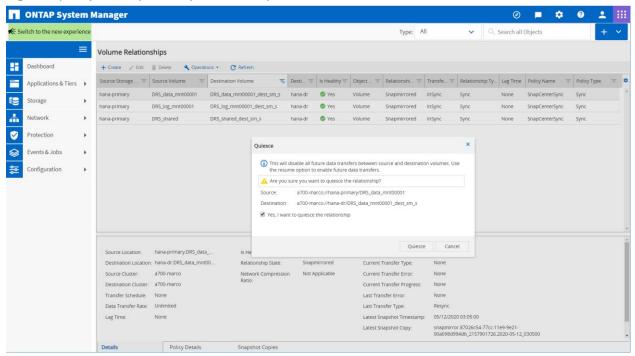
The synchronous SnapMirror relationships for the data, the log, and the shared volume must be quiesced and broken off. In addition, the volumes must be mounted to the namespace.

Figure 55 through Figure 61 show the required steps using ONTAP System Manager for the quiesce and break operations.

L.	ONTAP Syste	em I	lanager										Ø	= *	?	<u>.</u>
); Sv	itch to the new exper	ience								Type: A	1	<ul> <li>↓      </li> </ul>	Search all (	Objects		+ •
	-	=	Volume Relations	ships												
	Dashboard		+ Create 🥢 Edit	🗑 Delete 🔌	Operations • C	Refresh										
1	Applications & Tiers		Source Storage 👳	Source Volume	Testination V	/olume 🧠 😴	Desti 😇	Is Healthy $\mp$	Object 👳	Relationshi 👻	Transfe 👳	Relationship Ty	Lag Time	Policy Name	Policy Type	e =
	Channen		hana-primary	DRS_data_mnt000		nt00001_dest_sm_s	hana-dr	🔮 Yes	Volume	Snapmirrored	InSync	Sync	None	SnapCenterSync	Sync	
	Storage	*	hana-primary	DRS_log_mnt0000	/ Edit	0001_dest_sm_s	hana-dr	🔮 Yes	Volume	Snapmirrored	InSync	Sync	None	SnapCenterSync	Sync	
	Network	٠	hana-primary	DRS_shared	Delete	est_sm_s	hana-dr	🥝 Yes	Volume	Snapmirrored	InSync	Sync	None	SnapCenterSync	Sync	
,	Protection	*			C Refresh		_									
	Events & Jobs	12		l	Operations 🔸	Update										
	Events & Jobs	*					_									
ľ	Configuration	٠				Quiesce										
						Restore										
						Break										
						Resync Reverse Resyn										
			En la contra de la c	hana-primary:DR	C data	Abort	ØYe		Transfer		InSync					
			Source Location: Destination Location			Is Healthy: Relationship State:		, hirrored		Transfer Type:	None					
			Source Cluster:	a700-marco		Network Compressio		oplicable		Transfer Error:	None					
			Destination Cluster:	a700-marco		Ratio:			Current 1	Transfer Progress:	None					
				None					Last Tran	nsfer Error:	None					
			Transfer Schedule:	1 Horney												
			Data Transfer Rate:	Unlimited						nsfer Type:	Resync					
									Latest Sr	nsfer Type: hapshot Timestamp hapshot Copy:	05/12/202	0 03:05:00 r.87026c54-77cc-1				

Figure 55) SnapMirror quiesce operation—step 1.

Figure 56) SnapMirror quiesce operation—step 2.



ONTA	AP Systen	n Manage	r											Ø		•	?	-	
Switch to th	he new experien	nce								Type:	All		~	○ Search al	l Objects			+	``
	=	Volume	Relation	ships															
Dashbo	bard	+ Create	🥒 Edit	📋 Delete 🛛 🔌 Operat	ions • C F	Refresh													
Applica	tions & Tiers	Source Sto	orage 📼	Source Volume 👳	Destination V	olume =	Desti 📼	Is Healthy 😇	Object 📼	Relations!		fe 👳 Re	lai onship	Ty Lag Time	Policy N	lame 📼	Policy Ty	pe	-
		hana-prim	ary	DRS_data_mnt00001	DRS_data_mn	t00001_dest_sm_s	hana-dr	🔕 No	Volume	Snapmirre rec	d Quies	ced Sy	nc	1 min(s)	SnapCe	nterSync	Sync		
Storage	2	hana-prim	ary	DRS_log_mnt00001	DRS_log_mnt	00001_dest_sm_s	hana-dr	😣 No	Volume	Snapmirrere	d Quies	ced Sy	nc	1 min(s)	SnapCe	nterSync	Sync		
Networ	'k	hana-prim	ary	DRS_shared	DRS_shared_o	dest_sm_s	hana-dr	8 No	Volume	Snapmirre	d Quies	ced Sy	nc	1 min(s)	SnapCe	nterSync	Sync		
Protecti	ion	•																	
Events &	& lobs																		
		·																	
Configu	uration	•																	
			Location:	hana-primary:DRS_shar		Is Healthy:	8 N		Transfer			iesced							
		Destina	tion Location	n: hana-dr:DRS_shared_de	PS	Relationship State:	Snap	mirrored	Current	Transfer Type:	No	ne							
		Source		a700-marco		Network Compress Ratio:	ion Not /	pplicable		Transfer Error:									
		Destina	tion Cluster:	a700-marco			ion Not /	pplicable	Current	Transfer Progre	ess: No	ne							
		Destina Transfe	tion Cluster: r Schedule:	a700-marco None			ion Not A	pplicable	Current Last Trar	Transfer Progre nsfer Error:	ess: No No	ne							
		Destina Transfe	tion Cluster: r Schedule: ansfer Rate:	a700-marco None			ion Not A	pplicable	Current Last Trar Last Trar	Transfer Progre	ess: No No Re	ne	:38:13						

Figure 57) All SnapMirror target volumes are quiesced.

Figure 58) SnapMirror break operation—step 1.

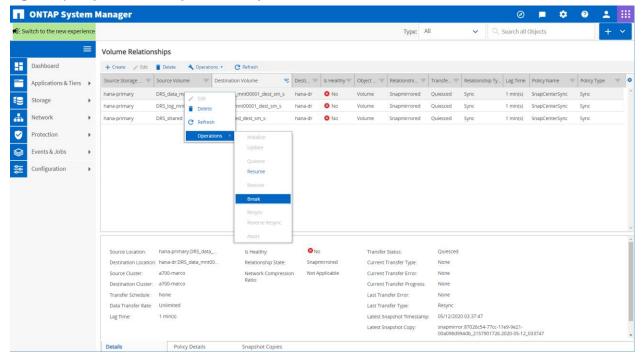


Figure 59) SnapMirror break operation—step 2.

	ONTAP Syste	em N	lanager										Ø	- *	?	-	-
E Swi	itch to the new exper	ience								Type:	All	~	Q. Search all	Objects		+	•
	2	=	Volume Relation	ships													
	Dashboard		+ Create 🥒 Edit	🛢 Delete 🔌 Operat	ions • C Refre	sh											
-	Applications & Tiers		Source Storage 👻	Source Volume 🛛 👻	Destination Volum	ne 🤜	Desti \Xi	Is Healthy =	Object 👳	Relationshi 🖲	Transfe =	Relationshi	p Ty Lag Time	Policy Name	The Policy Ty	ype =	
			hana-primary	DRS_data_mnt00001	DRS_data_mnt00	001_dest_sm_s	hana-dr	O No	Volume	Snapmirrored	Quiesced	Sync	1 min(s)	SnapCenterSync	Sync		
-	Storage	,	hana-primary	DRS_log_mnt00001	DRS_log_mnt0000	01_dest_sm_s	hana-dr	O No	Volume	Snapmirrored	Quiesced	Sync	1 min(s)	SnapCenterSync	Sync		
	Network	*	hana-primary	DRS_shared	DRS_shared_dest	_sm_s	hana-dr	O No	Volume	Snapmirrored	Quiesced	Sync	1 min(s)	SnapCenterSync	Sync		
2	Protection	+															
≥	Events & Jobs					Break						×					
	Configuration							nip permanently relationship p		the destination vo	lume type from	DP					
-	Comgulation	1						nt to break the		ync operation.							
						Source:		arco://hana-prin		mnt00001							
						Destination				0001_dest_sm_s							
						🗷 OK to br	eak the selec	ed relationship									
										Brea	k Can	-					
			Source Location:	hana-primary:DRS_data	I Is H	e				Died	K Can	lei					
			Destination Location	1: hana-dr:DRS_data_mnt	00 Rela	ationship State:	Snap	nirrored	Current	Transfer Type:	None						
			Source Cluster:	a700-marco	Net	work Compressio	in Not A	pplicable	Current	Transfer Error:	None						
			Destination Cluster	a700-marco	Nou	w.			Current	Transfer Progress	None						
			Transfer Schedule:	None					Last Tra	nsfer Error:	None						
			Data Transfer Rate:	Unlimited					Last Tra	nsfer Type:	Resync						
			Lag Time:	1 min(s)					Latest S	hapshot Timestan	p: 05/12/20	20 03:37:47					
									Latest Si	napshot Copy:			7cc-11e9-9e21- 1726.2020-05-12	_033747			
			Details	Policy Details		shot Copies											

Figure 60) All SnapMirror target volumes are broken off.

	ONTAP Syste	m I	Manager												Ø	<b>•</b> •	?	:	-
RO: SI	vitch to the new experie	ence									Type:	All		~	Q Search all	Objects		+	~
		=	Volume Relation	ship	s														
	Dashboard	-	+ Create 🥒 Edit	E De	elete 🔍 Operatio	ns • C	Refresh												
-	Applications & Tiers		Source Storage _ 👻	Souri	ce Volume 🛛 😇	Destination	/olume 🦷	Desti 🖘	Is Healthy 🗐	Object_ =	Relationshi	<b>∓</b> Tinn	sfe 👳 🛛	elationship '	Ty Lag Time	Policy Name	= Policy Ty	ype	÷ 0
			hana-primary	DRS_	data_mnt00001	DRS_data_m	nt00001_dest_sm_s	hana-dr	O No	Volum	Broken Off	ld e	s	ync	None	SnapCenterSync	Sync		^
1	Storage	*	hana-primary	DRS_	log_mnt00001	DRS_log_mn	t00001_dest_sm_s	hana-dr	O No	Volum	Broken Off	ld e	S	ync	None	SnapCenterSync	Sync		
*	Network	*	hana-primary	DRS_	shared	DRS_shared	_dest_sm_s	hana-dr	O No	Volum	Broken Off	ld e	s	ync	None	SnapCenterSync	Sync		
0	Protection	٠																	
	Events & Jobs	•																	
	Configuration																		
																			÷
			Source Location:	han	a-primary:DRS_share	ed	Is Healthy:	ON	0	Transfer	Status	Id	lle						Â
			Destination Location	n; han	a-dr:DRS_shared_de	5	Relationship State:	Brok	en Off	Current	Transfer Type:	N	lone						
			Source Cluster:	a70	0-marco		Network Compress	ion Not	oplicable	Current	Transfer Error:	N	ione						
			Destination Cluster:	a70	0-marco		Ratio:			Current	Transfer Progres	ss: N	lone						
			Transfer Schedule:	Non							nsfer Error:		lone						
			Data Transfer Rate:		mited						nsfer Type:		esync						
			Lag Time:	Non	le						napshot Timesta	2282 00	5/12/2020 0						
										Latest S	napshot Copy:				c-11e9-9e21- 27.2020-05-12_	033813			-
			Details		Policy Details		Snapshot Copies												

Figure 61 shows the required junction path configuration.

Figure 61) Junction path configuration.

	ONTAP Syste	m N	lanager						(e		?	-	1
Swit	tch to the new experi	ence				Туре	: All	~	Q. Search	all Objects		+	~
		≡	Junction Paths SVM hana	-dr 🔻									
	Dashboard		🕞 Mount 🖉 Unmount 🥒 Change Expo	rt Policy C Refresh									
,	Applications & Tiers	•	Path	Storage Object	Export Policy	Security Styl	e						
	Storage	-	4 <del></del> /	🛢 dr_root	default	unix							
	Storage		DR_testing_log_backup	DR_testing_log_backup	default	unix							
	Nodes		DRS_shared_dest_sm_s	DRS_shared_dest_sm_s	def ult	unix							
	Aggregates &		p TRS_log_mnt00001_dest_sm_s	DRS_log_mnt00001_dest_sm_s	def ult	unix							
	Disks	•	DRS_tog_backup DRS_data_mnt00001_dest_sm_s	DRS log backup	default	unix							
	SVMs			DRS_data_mnt00001_dest_sm_s	de <mark>ault</mark>	unix							
	Volumes												
	LUNs												
	Qtrees												
	Qtrees												
	Quotas												
	Junction Paths												
	Network	•											
	Protection	•											
	Events & Jobs	•		2	elect a single item from the	table to view the item	details.						
	Configuration	•											
(													

**Note:** In a Fibre Channel setup, the LUNs in the FlexClone volumes must be mapped to the initiator group of the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

# 8.3 Mount Volumes at Target Host

The volumes can now be mounted at the target host.

hana-10:~ # mount -a

The following output shows the required file systems.

```
hana-10:~ # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.116:/DRS_log_backup 104857600 256 104857344 1% /mnt/log-
backup
192.168.175.116:/DRS_data_mnt00001_dest_sm_s 10725184 8694080 2031104 82%
/hana/data/DRS/mnt00001
192.168.175.116:/DRS_log_mnt00001_dest_sm_s 67106816 54338816 12768000 81%
/hana/log/DRS/mnt00001
192.168.175.116:/DRS_shared_dest_sm_s/shared 324150976 269775616 54375360 84% /hana/shared
192.168.175.116:/DRS_shared_dest_sm_s/usr-sap 324150976 269775616 54375360 84% /usr/sap/DRS
hana-10:~ #
```

**Note:** In a Fibre Channel setup, additional steps are required before the LUNs can be mounted at the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

# 8.4 Start the HANA Database

The steps to start the HANA database are described in section 5.5, Start the HANA Database.

# 9 Asynchronous SnapMirror Disaster Recovery Failover

Follow these steps to execute the disaster recovery failover:

- 1. Prepare the target host.
- 2. Break SnapMirror relationships.
- 3. Restore to the latest SnapCenter Snapshot backup.
- 4. Mount volumes at the target host.
- 5. Recover the HANA database.

The following chapters describe these steps in detail.

**Note:** Manual steps are described for the different operations. All the steps could also be automated by using scripts or other automation tools.

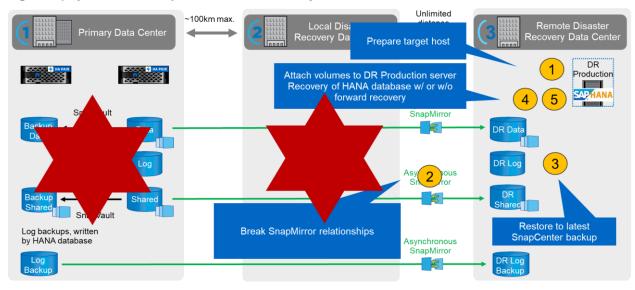


Figure 62) Synchronous SnapMirror disaster recovery failover.

# 9.1 Prepare Target Host

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

During normal operation, the target host is typically used for other purposes—for example, as a HANA QA or test system. Therefore, most of the described steps must be executed when a disaster failover testing is executed. On the other hand, the relevant configuration files, such as /etc/fstab and /usr/sap/sapservices, can be prepared and then put in production simply by copying the configuration file. The disaster recovery testing procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system.

### **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. As an alternative a virtual IP address concept can be used as well.

### Install Required Software

The SAP host agent software must be installed at the target server. For full information, see the <u>SAP Host</u> Agent at the SAP help portal.

**Note:** If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

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

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the /etc/services file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the /usr/sap/sapservices file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
hana-10:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/DRS/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/DRS/HDB00/exe/sapstartsrv pf=/usr/sap/DRS/SYS/profile/DRS_HDB00_hana-10
-D -u drsadm
limit.descriptors=1048576
```

### Prepare the HANA Log Volume

Because the HANA log volume is not part of the SnapMirror replication, an empty log volume must exist at the target host. The log volume must include the same subdirectories as the source HANA system.

```
hana-10:/hana/log/DRS/mnt00001 # ls -al
total 84
drwxr-x--- 5 drsadm sapsys 4096 Apr 2 06:51 .
drwxr-x--- 1 drsadm sapsys 16 Apr 2 06:45 ..
drwxr-x--- 2 drsadm sapsys 61440 Apr 24 07:11 hdb00001
drwxr-xr-- 2 drsadm sapsys 12288 Apr 24 02:59 hdb00002.00003
drwxr-xr-- 2 drsadm sapsys 4096 Apr 24 08:31 hdb00003.00003
hana-10:/hana/log/DRS/mnt00001 #
```

### Prepare Log Backup Volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host. A volume for the log backups must be configured and mounted at the target host.

**Note:** If log backup volume replication is part of the disaster recovery setup, a FlexClone volume will be mounted at the target host and there is no need to prepare an additional log backup volume.

### **Prepare File System Mounts**

Table 9 shows the naming conventions that were used in the lab setup. The volume names of the FlexClone volumes at the disaster recovery storage were included in /etc/fstab. These volume names were used in the FlexClone copy creation step in the next section.

HANA DRS Volumes	Volume at Disaster Recovery Storage	Mount Point at Target Host
Data volume	DRS_data_mnt00001_dest	/hana/data/DRS/mnt00001
Shared volume	DRS_hana_shared_dest/shared DRS_hana_shared_ dest/usr-sap	/hana/shared /usr/sap//DRS
Log backup volume	DRS_log_backup_dest	/mnt/log-backup

Table 9) Volume names of FlexClone volumes.

**Note:** A FlexClone of the log backup volume is required only if log backups are also replicated to the DR site.

Note: The mount points in Table 9 must be created at the target host.

The required /etc/fstab entries are the following.

hana-10:/etc # cat /etc/fstab 192.168.175.116:/DRS\_log\_mnt00001 /hana/log/DRS/mnt00001 nfs rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0 192.168.175.116:/DRS\_data\_mnt00001\_dest /hana/data/DRS/mnt00001 nfs rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0 192.168.175.116:/DRS\_shared\_dest/shared /hana/shared nfs rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0 192.168.175.116:/DRS\_shared\_dest/usr-sap /usr/sap/DRS nfs rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0 192.168.175.116:/DRS\_log\_backup\_dest /mnt/log-backup nfs rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0 0 hana-10:/etc #hana-10:~ #

**Note:** In a Fibre Channel setup, the fstab entries depend on the multipath configuration. Because the SCSI IDs are different with each operation, the fstab file will not be static and must be adapted after the LUN discovery process.

# 9.2 Break SnapMirror Relationships

The asynchronous SnapMirror relationships for the data and the shared volume must be quiesced and broken off. If log backup replication is part of the disaster recovery setup, the replication relationship of the log backup volume must be quiesced and broken off as well.

In addition, the volumes must be mounted to the namespace.

Figure 63 through Figure 69 show the steps using ONTAP System Manager for the quiesce and break operations.

ONTAP Syste	m	Manager										Ø 📮	🌣 🤨		1
🗄 Switch to the new experie	ience							Туре:	All	1	✓ Q Sea	rc <mark>h all Objects</mark>		+	~
	I î	Volume Relation	ships												
Dashboard		🕂 Create 🥒 Edit	🖥 Delete 🔍	Operations • C	Refresh										
Applications & Tiers		Source Storage 🐨	Source Volume	Testination Vo	lume 👳	Destination Stor	= Is Healthy	👳 Object Type 👳	Relationshi 🔫	T.Ŧ	Relationship Ty	Lag Time	Policy Name	Policy Ty	ype
Storage •		hana-backup	DRS_log_backup	/ Edit	p_dest	hana-dr	🔮 Yes	Volume	Snapmirrored	Idle	Asynchronous	24 min(s)	MirrorAllSnaps.	Asynchri	onou
		hana-primary	DRS_data_mnt00	Delete	0001_dest	hana-dr	Yes	Volume	Snapmirrored	Idle	Asynchronous	29 min(s)	MirrorAllSnaps	Asynchr	onou
Nodes		hana-primary	DRS_shared	C Refresh	st	hana-dr	🔮 Yes	Volume	Snapmirrored	Idle	Asynchronous	2 hr(s) 23 min.	. MirrorAllSnaps.	Asynchro	onou
Aggregates & Disks				Operations	Initialize										
SVMs					Update										
Volumes					Resume										
LUNS					Restore										
Qtrees					Break										
Quotas					Resync Reverse I	Resync									
Junction Paths		1			Abort										
Network		Source Location:	hana-backup:DR	IS_log_ba	Is Healthy:	Se Yes		Transfer Status:	Idle						
		Destination Location	n: hana-dr:DRS_log	_backup	Relationship S	tate: Snapmi	rored	Current Transfer Type:	None						
Protection -	•	Source Cluster:	a700-marco		Network Comp	pression Not App	licable	Current Transfer Error:	None						
Volume		Destination Cluster:	a700-marco		Ratio:			Current Transfer Progr	ess: None						
Relationships		Transfer Schedule:	Every-30-Minute	S				Last Transfer Error:	None						
SVM DR		Data Transfer Rate:	Unlimited					Last Transfer Type:	Update						
Relationships		Lag Time:	24 min(s)					Latest Snapshot Times	tamp: 05/27/2	020 04:3	0:00				
Protection Policies								Latest Snapshot Copy:			26c54-77cc-11e9- 2157901723.2020				
Schoduloc		Details	Policy De	tails	Snapshot Cop	les									

Figure 63) SnapMirror quiesce operation—step 1.

Figure 64) SnapMirror quiesce operation—step 2.

L	ONTAP System	n M	lanager											Ø 📮	٠	?	2	-
Sw	itch to the new experier	nce							т	ype: All		~	Q Sea	rch all Objects	{		+	•
	. =	1	Volume Relation	iships														
	Dashboard		+ Create 🖌 Edit	🔋 Delete 🔌 Oper	ations • C Refr	esh												
	Applications & Tiers	L	Source Storage 🔫	Source Volume	Destination Volum	ne 🔻	Destination Stor	F Is Healthy	👳 Object Type	= Relatio	nshi = T	= R	elationship Ty	Lag Time	Policy Nar	me 😎	Policy Typ	pe
		L	hana-backup	DRS_log_backup	DRS_log_backup_c	lest	hana-dr	🔮 Yes	Volume	Snapn	irrored Io	lle A	synchronous	24 min(s)	MirrorAllS	inaps	Asynchro	ono
3	Storage 🔹	L	hana-primary	DRS_data_mnt00001	DRS_data_mnt000	01_dest	hana-dr	🕑 Yes	Volume	Snapn	irrored Ic	lle A	synchronous	29 min(s)	MirrorAllS	inaps	Asynchro	ono
	Nodes	L	hana-primary	DRS_shared	DRS_shared_dest		hana-dr	🕑 Yes	Volume	Snapn	irrored Io	lie A	synchronous	2 hr(s) 23 min.	MirrorAllS	inaps	Asynchro	ano
	Aggregates & P Disks	L				Quiesce						×						
	SVMs	L																
	Volumes	L				th	his will disable all futur le resume option to en re you sure you want t	able future data	transfers.	destination	volumes. Use							
	LUNs	L				Sourc		://hana-backup/I										
	Qtrees	L				Destir	nation: a700-marco	//hana-dr/DRS_I										
	Quotas	L				e Ye	s, I want to quiesce the	relationship									_	
	Junction Paths	Ŀ	16.1										-				_	
	Network	L	Source Location:	hana-backup:DRS_log	_ba is i	He				Quiesce	Cance	ų.						
		L	Destination Location	n: hana-dr.DRS_log_bac	kup Re	lationship St	ate: Snapmin	rored	Current Transfer 1	lype:	None							
2	Protection -		Source Cluster:	a700-marco		twork Comp tio:	ression Not Appl	icable	Current Transfer B		None							
	Volume Relationships	L	Destination Cluster:	a700-marco Every-30-Minutes					Current Transfer F	10.00 C	None None							
	Relationships	۰.	Transfer Schedule: Data Transfer Rate:	and the second second					Last Transfer Erro		Update							
	SVM DR Relationships		Lag Time:	24 min(s)					Latest Snapshot T		05/27/2020	04:30	00					
	Protection Policies								Latest Snapshot C				c54-77cc-11e9- 157901723-2020	9e21+ )-05-27_043000				
	Schoduloc		Details	Policy Details	50.5	ipshot Copi												

As a source for the log backup FlexClone volume, one of the SnapMirror Snapshot copies is selected.

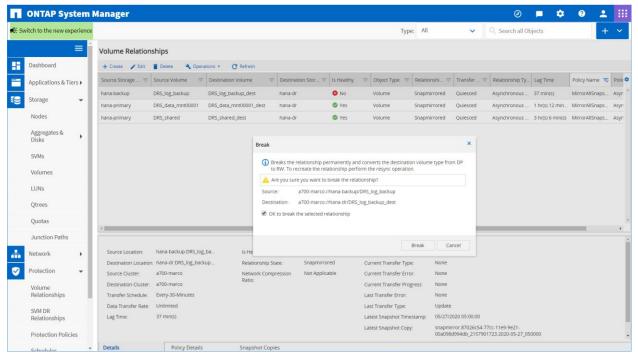
O: Cu			Manager								-				Ø	•	0 2	
, SW	vitch to the new exp	perience								Туре:	All		~	Q, Se	earch all Ob	ojects	-	+ *
		=	Volume Relation	nships														
Н	Dashboard		🕂 Create 🥜 Edit	🔋 Delete 🔌 Opera	ations • C Refresh													
-	Applications & Tie	ers 🕨	Source Storage 👳	Source Volume 👳	Destination Volume	👳 Destin	ation Stor 👳	Is Healthy	⇒ Obje	ect Type 📼	Relations		Transfer	🖅 Rélati	ionship Ty	Lag Time	Policy Name	S Poli
			hana-backup	DRS_log_backup	DRS_log_backup_dest	hana-c	Ir	O No	Volu	ime	Snapmirr	red	Quiesced	As no	chronous	35 min(s)	MirrorAllSnaps	Asy
	Storage		hana-primary	DRS_data_mnt00001	DRS_data_mnt00001_i	dest hana-c	Ir	🔮 Yes	Volu	ime	Snapmirr	red	Quiesced	As no	chronous	1 hr(s) 10 min	MirrorAllSnaps	Asyı
	Nodes	- 1	hana-primary	DRS_shared	DRS_shared_dest	hana-c	Ir	🔮 Yes	Volu	ime	Snapmirr	red	Quiesced	As no	chronous	3 hr(s) 4 min(s)	MirrorAllSnaps	Asyı
	Aggregates & Disks	•																
	SVMs	- 1																
	Volumes	- 1																
	LUNs																	
	LUNs Qtrees																	
	Qtrees		4														_	•
	Qtrees Quotas Junction Paths		< Source Location:	hana-primary-DR5_sh	ared Is Heal	thy:	© Yes		Transfer	Status		Quiesced						,
•	Qtrees Quotas	×		hana-primary:DR5_sh n: hana-dr:DR5_shared_t		thy: nship State:	♥Yes Snapmirro	red		Status: Transfer Type:		Quiesced					_	,
	Qtrees Quotas Junction Paths	) T			dest Relatio Netwo				Current								_	,
2	Qtrees Quotas Junction Paths Network Protection		Destination Location	n: hana-dr:DRS_shared_ a700-marco	dest Relatio	nship State:	Snapmirro		Current Current	Transfer Type:		None					_	•
	Qtrees Quotas Junction Paths Network		Destination Location Source Cluster:	n: hana-dr:DRS_shared_ a700-marco	dest Relatio Netwo	nship State:	Snapmirro		Current Current Current	Transfer Type. Transfer Error	ess: 1	None None					_	,
	Qtrees Quotas Junction Paths Network Protection Volume Relationships		Destination Location Source Cluster: Destination Cluster:	n: hana-dr:DRS_shared_o a700-marco a700-marco None	dest Relatio Netwo	nship State:	Snapmirro		Current Current Current Last Trar	Transfer Type: Transfer Error Transfer Progr	ess:	None None None					_	
	Qtrees Quotas Junction Paths Network Protection Volume		Destination Location Source Cluster: Destination Cluster: Transfer Schedule:	n: hana-dr:DRS_shared_o a700-marco a700-marco None	dest Relatio Netwo	nship State:	Snapmirro		Current Current Current Last Trar Last Trar	Transfer Type: Transfer Error Transfer Progr nsfer Error:	ess: I	None None None None Update	20 02:31:16					,
	Qtrees Quotas Junction Paths Network Protection Volume Relationships SVM DR	•	Destination Location Source Cluster: Destination Cluster: Transfer Schedule: Data Transfer Rate:	n: hana-dr:DRS_shared_o a700-marco a700-marco None Unlimited	dest Relatio Netwo	nship State:	Snapmirro		Current Current Current Last Trar Last Trar	Transfer Type: Transfer Error Transfer Progr nsfer Error: nsfer Type:	ess: I tamp: (	None None None Update 05/27/20: snapmirr	20 02:31:16 pr 87026c54 994db_21575			3116	_	,

Figure 65) All SnapMirror target volumes are quiesced.

#### Figure 66) SnapMirror break operation—step 1.

ONTAP System	Manager								Ø	• •	?	
• Switch to the new experience	e					Туре:	All	~	Q Search all Of	bjects		+ ~
	Volume Relations	ships									1.8	
Dashboard	+ Create 🥒 Edit	🔋 Delete 🛛 🔧 Operatio	ns • C Refresh									
Applications & Tiers	Source Storage 🐨	Source Volume =	Destination Volume 🛛 👻	Destination Stor	Is Healthy	👳 Object Type 👳	Relationshi \Xi	Transfer 🦷	Relationship Ty	Lag Time	Policy Name	😎 Polic
	hana-backup	DRS_log_backup D	DRS_log_backup_clest	hana-dr	O No	Volume	5napmirrored	Quiesced	Asynchronous	37 min(s)	MirrorAllSnap	is Asyr
Storage 🔹	hana-primary	DRS_data_mnt00001 E	DRS_da	hana-dr	🔮 Yes	Volume	5napmirrored	Quiesced	Asynchronous	1 hr(s) 12 min	MirrorAllSnap	is Asyr
Nodes	hana-primary	DRS_shared D	DRS_sf C Refresh	hana-dr	🔮 Yes	Volume	Snapmirrored	Quiesced	Asynchronous	3 hr(s) 6 min(s)	MirrorAllSnap	is Asyn
Aggregates & Disks			Operations	Initialize								
DISKS				Update								
SVMs												
Volumes				Resume								
LUNs				Restore								
Qtrees				Break								
Quotas				Resync								
Junction Paths	•			Reverse Resync							_	•
a state of the sta	Source Location:	hana-backup:DRS_log_ba	I Is Healthy:	O No		Transfer Status:	Oulesce	ed.				- 1
Network		hana-dr:DRS_log_backup			ored	Current Transfer Type:	None					
Protection 👻	Source Cluster:	a700-marco	Network Comp	oression Not Appli	cable	Current Transfer Error:	None					
Volume	Destination Cluster:	a700-marco	Ratio:			Current Transfer Progre	ess: None					
Relationships	Transfer Schedule:	Every-30-Minutes				Last Transfer Error:	None					
SVM DR	Data Transfer Rate:	Unlimited				Last Transfer Type:	Update					
Relationships	Lag Time:	37 min(s)				Latest Snapshot Timest		020 05:00:00				
Protection Policies						Latest Snapshot Copy:			77cc-11e9-9e21- 01723.2020-05-27_05	50000		
Schodulor	Details	Policy Details	Snapshot Cop	ies								

Figure 67) SnapMirror break operation—step 2.



	ONTAP Sys	stem	Manager												۰	0 💄	
Swi	itch to the new ex	perience								Type:	All	~	् Search all O	bjects		-	+ ~
		E	Volume Relation	iships													
	Dashboard	- 1	+ Create 🥜 Edit	👕 Delete 💦 🔧 Oper	ations • C Ref	fresh				_							
1	Applications & Ti	iers 🕨	Source Storage 👳	Source Volume 👘	Destination Volu	me = t	Destination Stor 👻	Is Healthy	👳 Object Ty		elationshi 👳	Tansfer 👳	Relationship Ty	Lag Tim	ie	Policy Name	T Po
		- 1	hana-backup	DRS_log_backup	DRS_log_backup_	dest h	hana-dr	8 No	Volume	в	roken Off	lc e	Asynchronous	None		MirrorAllSnaps	As
	Storage		hana-primary	DRS_data_mnt00001	DRS_data_mnt00	001_dest h	hana-dr	Yes	Volume	в	roken Off	lo e	Asynchronous	None		MirrorAllSnaps	As
	Nodes	- 1	hana-primary	DRS_shared	DRS_shared_dest	c ł	hana-dr	Yes	Volume	в	roken Off	lo e	Asynchronous	None		MirrorAllSnaps	As
	Aggregates & Disks	•															
	SVMs																
	Volumes	- 1															
	LUNs	- 1															
	LUNs Qtrees																
	Qtrees		٩														
	Qtrees Quotas	,	< Source Location:	hana-primary:DR5_sh	ared Is	Healthy:	<b>⊘</b> Yes		Transfer Statu	15:	Idle					_	
•	Qtrees Quotas Junction Paths Network	,		hana-primary.DRS_sh α: hana-dr.DRS_shared_		Healthy: elationship State		f	Transfer Statu Current Trans		Idle					_	
•	Qtrees Quotas Junction Paths	•			dest Ri	elationship State	: Broken Of			fer Type:						_	
-	Qtrees Quotas Junction Paths Network		Destination Location	n: hana-dr:DRS_shared_ a700-marco	dest Ri	elationship State	: Broken Of		Current Trans	fer Type: fer Error:	None					_	
-	Qtrees Quotas Junction Paths Network Protection		Destination Location Source Cluster:	n: hana-dr:DRS_shared_ a700-marco	dest Ri	elationship State	: Broken Of		Current Trans Current Trans	fer Type: fer Error: fer Progres	None						
•	Qtrees Quotas Junction Paths Network Protection Volume Relationships		Destination Location Source Cluster: Destination Cluster:	n: hana-dr:DRS_shared_ a700-marco a700-marco None	dest Ri	elationship State	: Broken Of		Current Trans Current Trans Current Trans	fer Type: fer Error: fer Progre: Error:	None None SS: None					-	
•	Qtrees Quotas Junction Paths Network Protection Volume		Destination Location Source Cluster: Destination Cluster: Transfer Schedule:	n: hana-dr:DRS_shared_ a700-marco a700-marco None	dest Ri	elationship State	: Broken Of		Current Trans Current Trans Current Trans Last Transfer	fer Type: fer Error: fer Progre: Error: Type:	None None SS: None None Update	20 02-31:16				-	
2	Qtrees Quotas Junction Paths Network Protection Volume Relationships SVM DR	*	Destination Location Source Cluster: Destination Cluster: Transfer Schedule: Data Transfer Rate:	n: hana-dr:DRS_shared_ a700-marco a700-marco None Unlimited	dest Ri	elationship State	: Broken Of		Current Trans Current Trans Current Trans Last Transfer Last Transfer	fer Type: fer Error: fer Progre: Error: Type: tot Timesta	None None SS: None Update Imp: 05/27/20. snapmirr	or.87026c54-77	7cc-11e3-9e21- 724.2020-05-27_0.	23116		_	

Figure 68) All SnapMirror target volumes are broken off.

All volumes must be mounted to the namespace.

Figure	69)	Junction	path	configuration.
iguio	<i>~~</i> ,	ounouon	paur	ooningaration

ONT	TAP Syst	em l	Manager								(		•	?	<u> </u>	
Switch to	o the new expe	rience						Type: Al	1	~	Q Search	all Objects			+	2
		≡ į	Junction Paths	SVM hana	-dr 🔻											
Dasht	board		🕞 Mount 📑 Unmo	ount 🕜 Change Expo	t Policy C Refresh											
Applie	ications & Tiers	•	Path		Storage Object	Export Policy	Security Style									
Stora	ITE		4 <del>*</del> 1		😂 dr_root	default	unix									
	.0-		TR_testing_li		DR_testing_log_backup	default	unix									
Node	es		TRS_shared		DRS_shared_dest_sm_s	default	unix									
		- 1	TRS_shared	_dest_clone	BRS_shared_dest_clone	default	unix									
Aggr Disks	regates &	•	TRS_log_mn	t00001_dest_sm_s	DRS_log_mnt00001_dest_sm_s	default	unix									
DISK	3		TRS_log_mn	t00001	S DR5_log_mnt00001	default	unix									
SVMs	ls		TRS_log_bac	kup_dest_clone	DRS_log_backup_dest_clone	default	unix									
		- 1	TRS_log_bac	kup	BR5_log_backup	default	unix									
Volu	imes		😴 DRS_data_m	nt00001_dest_sm_s	DRS_data_mnt00001_dest_sm_s	default	unix									
LUNS	2		DDS data m	nt00001 dest clone		outroom.	OT IN									
LUNS	s	- 1	😴 DRS_data_m	nt00001_dest	DRS_data_mnt00001_dest	default	unix									
Qtree	es		The Drs_log_bac	kup_dest	DRS_log_backup_dest	default	unix									
		- 1	TRS_shared_	dest.	DRS_shared_dest	default	unix									
Quot	tas															
Junc	ction Paths															
Netwo			General													
Netwo	югк	· .	Name:	DR5_shared_dest												
Prote	ection	-														
			Type:	Volume												
Volu			Junction Path:	/DRS_shared_dest												
Relat	itionships		Export Policy:	default												
SVM	DR		export Policy.	uerauit												
	itionships															
Prote	ection Policies															
	oduloc		Details													

**Note:** In a Fibre Channel setup, the LUNs in the FlexClone volumes must be mapped to the initiator group of the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

# 9.3 Restore Data Volume to Latest SnapCenter Backup

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.

To restore the SAP HANA database data volume, follow these steps.

1. In the disaster recovery SVM, select Volume. Select the data volume and then select Manage Snapshots and Restore.

	ONTAP Sy	stem	man	ager										Ø 📮	<b>\$</b> ?	-
E Sw	itch to the new ex	kperienc	e								Type: All		<ul> <li>Q Sea</li> </ul>	rch all Objects		+ `
		≡	Vo	umes	SVM hana-dr	•										
	Dashboard		+	Create 🧪	Edit 🗐 Delete 🚦 Mo	re Actions 🛛 View Mis	ising Protect	ion Relationship	s C Refresh							
	Applications & T	iers 🕨		Status \Xi	Name		/le 👳	Aggre 👳	Thin Provi $=$	Availa 😇	Total 😇	% Used 😇	Туре 😇	Protection 😇	Storage E 😇	Appli
	Storage	•	+	0	DRS_data_mnt00001_	Edit		aggr1_2	Yes	1.39 GB	9.11 GB	84	rw	No	Enabled	-NA-
	Nodes		+	۲	DRS_data_mnt00001_			aggr1_2	Yes	1.29 GB	8.6 GB	84	rw	No	Enabled	-NA-
	Aggregates & Disks	•	+	۲	DRS_data_mnt00001_	Refresh Change status to		aggr1_2	Yes	1.49 GB	9.37 GB	84	dp	No	Enabled	-NA-
	SVMs		+	۲	DRS_log_backup	Resize Protect		aggr1_1	Yes	99.98 GB	100 GB	0	rw	No	Enabled	-NA-
	Volumes		+	۲	DRS_log_backup_dest	Storage QoS		aggr1 2	Yes	1.06 GB	6.87 GB	84	rw	No	Enabled	-NA-
	LUNs		+	0	DRS_log_backup_dest	Manage Snapshots Clone		eate onfiguration Sett	tings	1.07 GB	7.02 GB	84	rw	No	Enabled	-NA-
			+	۲	DRS_log_mnt00001	Storage Efficiency Move	Re	estore		98.3 GB	100 GB	1	rw	No	Enabled	-NA-
	Qtrees		+	۲	DRS_log_mnt00001_d	Change Tiering Policy		aggr1_2	Yes	5.91 GB	37.85 GB	84	dp	No	Enabled	-NA-
	Quotas		+	۲	DRS_shared_dest	Fle	exVol	aggr1_2	Yes	3.76 GB	22.9 GB	83	rw	No	Enabled	-NA-
	Junction Paths		+	۲	DRS_shared_dest_clone	Fle	exVol	aggr1_2	Yes	3.66 GB	23.99 GB	84	rw	No	Enabled	-NA-
	Network	-	+	۲	DRS_shared_dest_sm_s	Fle	exVol	aggr1_2	Yes	5.03 GB	30.31 GB	83	dp	No	Enabled	-NA-
2	Protection	*	+	۲	DR_testing_log_backup	Fle	exVol	aggr2_1	Yes	99.99 GB	100 GB	0	rw	No	Enabled	-NA-
	Volume Relationships		+	۲	dr_root	Fle	exVol	aggr2_1	No	970.55 MB	1 GB	0	rw	No	Disabled	-NA-
	SVM DR Relationships															
	Protection Polic	cies	۰.													
	Schodulos													Dis	playing 1 - 13 <	1.3

2. Select a SnapCenter Snapshot backup.

witch to the new experience					Type:	All		v Qs	earch all Objects		+
=	Volumes	SVM hana-dr V									
Dashboard	+ Create / I		View Missing F	Protection Relationships C Refresh							
Applications & Tiers 🕨	Status 👳	Name	= Style	⊤ Aggre      ⊤ Thin Provi      ▼ Availa      ▼	Tota	l Ŧ	% Used 🗐	Туре 😇	Protection 🐨	Storage E 😇	Appli
Storage 👻	+ 0	DRS_data_mnt00001_dest	FlexVol	Restore Volume from Snapshot copy	• • •		×	rw	No	Enabled	-NA-
Nodes	+ 0	DRS_data_mnt00001_dest_clone	FlexVol	and the second		Cr Ap		rw	No	Enabled	-NA-
Aggregates & Disks	+ 0	DRS_data_mnt00001_dest_sm_s	FlexVol		l'			dp	No	Enabled	-NA-
	+ 0	DRS_log_backup	FlexVol	SnapCenter_LocalSnapAndSnapMirror_Hourly_05-26 SnapCenter_LocalSnapAndSnapMirror_Hourly_05-26		M No M No	-	rw	No	Enabled	-NA-
SVMs	+ 0	DRS_log_backup_dest	FlexVol					rw	No	Enabled	-NA
Volumes	+ 0	DRS_log_backup_dest_clone	FlexVol	SnapCenter_LocalSnapAndSnapMirror_Hourly_05-27	2020	M No		ΓW	No	Enabled	-NA
LUNS	+ 0	DRS_log_mnt00001	FlexVol					rw	No	Enabled	-NA-
Qtrees	+ 0	DRS_log_mnt00001_dest_sm_s	FlexVol	SnapCenter_LocalSnapAndSnapVault_Daily_05-25-20 SnapCenter_LocalSnapAndSnapVault_Daily_05-26-20				dp	No	Enabled	-NA
Quotas	+ 0	DRS_shared_dest	FlexVol	snapmirror.87026c54-77cc-11e9-9e21-00a098d994d	_215	M No		38:33	No	Enabled	-NA
Junction Paths	+ 0	DRS_shared_dest_clone	FlexVol		-			rw	No	Enabled	-NA
Network +	+ 0	DRS_shared_dest_sm_s	FlexVol	snapmirror.87026c54-77cc-11e9-9e21-00a098d994di snapmirror.87026c54-77cc-11e9-9e21-00a098d994di	-		-	dp	No	Enabled	-NA
Protection 👻	+ 0	DR_testing_log_backup	FlexVol					rw	No	Enabled	-NA
Volume Relationships	+ 📀	dr_root	FlexVol		tore	Cance		rw	No	Disabled	-NA
SVM DR Relationships											
Protection Policies	<		_		-	-	_	_	_	_	-

### 3. Execute the restore operation.

ONTAP Sy	stem I	Mana	iger									Ø 📮	<b>\$ 0</b>	<b>±</b>
Switch to the new ex	xperience								Type: All		Q Sei	arch all Objects		+
	= î	Volu	umes	SVM hana-dr 🔻										
Dashboard		+	Create 📝 E	Edit 📱 Delete 🚦 More Actions 🌒	View Missing Prote	ection Relationsh	ips C Refresh							
Applications & T	iers 🕨		Status 😇	Name	style =	Aggre =	Thin Provi 🔫	Avalla 👳	Total 👳	% Used 🗐	Туре 👳	Protection =	Storage E 👳	Appli.
Storage	-	+	٥	DRS_data_mnt00001_dest	FlexVol	aggr1_2	Yes	1.39 GB	9.11 GB	84	rw	No	Enabled	-NA-
Nodes	- 1	+	0	DRS_data_mnt00001_dest_clone	FlexVol	aggr1_2	Yes	1.29 GB	8.6 GB	84	rw	No	Enabled	-NA-
Aggregates & Disks		+	٥	DRS_data_mnt00001_dest_sm_s	FlexVol	aggr1_2	Yes	1.49 GB	9.37 GB	84	dp	No	Enabled	-NA-
SVMs	- 1	+	٥	DRS_log_backup	FlexVol	aggr1_1	Yes	99.98 GB	100 GB	0	rw	No	Enabled	-NA-
Volumes	- 1	+	0	DRS_log_backup_dest	Restore Vo	lume				×	rw	No	Enabled	-NA-
LUNs	- 1	+	٥	DRS_log_backup_dest_clone	A Voluz 'Snap	me 'DRS_data_mr Center_LocalSna	nt00001_dest' will be pAndSnapVault_Daily	restored using th _05-26-2020_06.	e Snapshot copy 38.01.7192' ?		rw	No	Enabled	-NA-
Otrees	- 1	+	٥	DRS_log_mnt00001			r this Snapshot copy	was created will t	be lost.		rw	No	Enabled	-NA-
	- 1	+	٥	DRS_log_mnt00001_dest_sm_s	Resto	ore volume from	this Snapshot copy.				dp	No	Enabled	-NA-
Quotas	- 1	+	0	DRS_shared_dest					Restore	Cancel	rw	No	Enabled	-NA-
Junction Paths	- 1	+	٥	DRS_shared_dest_clone	FlexVol	aggr1_2	Yes	3.66 GB	23.99 GB	84	rw	No	Enabled	·NA-
Network	•	+	0	DRS_shared_dest_sm_s	FlexVol	aggr1_2	Yes	5.03 GB	30.31 GB	83	dp	No	Enabled	-NA-
Protection	-	+	٥	DR_testing_log_backup	FlexVol	aggr2_1	Yes	99.99 GB	100 GB	0	rw	No	Enabled	-NA-
Volume Relationships		+	۰	dr_root	FlexVol	aggr2_1	No	970.55 MB	1 GB	0	rw	No	Disabled	-NA-
SVM DR Relationships														
Protection Polic	cies	•	-		_	_	_	_	_	_	-	_	_	_
Schoelulae												Dis	playing 1 - 13 🔍	

# 9.4 Mount FlexClone Volumes at Target Host

The FlexClone volumes can now be mounted at the target host.

hana-10:~ # mount -a

The output shows the required file systems.

hana-10:/etc # df						
Filesystem	1K-blocks	Used	Available	Use%	Mounted on	
192.168.175.116:/DRS log mnt00001	104857600	1778240	103079360	28		
/hana/log/DRS/mnt00001						
192.168.175.116:/DRS data mnt00001 dest	9553472	8096192	1457280	85%		
/hana/data/DRS/mnt00001						
192.168.175.116:/DRS shared dest/shared	24013312	20064512	3948800	84%		
/hana/shared						
192.168.175.116:/DRS shared dest/usr-sap	24013312	20064512	3948800	84%		
/usr/sap/DRS						
192.168.175.116:/DRS_log_backup_dest	7200512	6084992	1115520	<mark>85</mark> 응		
/mnt/log-backup						

Note: This output includes a replicated log backup volume..

**Note:** In Fibre Channel setup, additional steps are required before the LUNs can be mounted at the target host. See section 10, Different Steps Required in a Fibre Channel Environment.

# 9.5 Check Consistency of Latest Log Backups

The consistency check is done in the same way as described in the disaster recovery testing section 6.4, Check Consistency of Latest Log Backups.

# 9.6 Recovery of the HANA Database

The recovery of the SAP HANA database is done in the same way as described in the disaster recovery testing section 6.5, Recover the HANA Database.

# **10 Different Steps Required in a Fibre Channel Environment**

Most of the steps required for disaster recovery testing and disaster recovery failover are identical with those for NFS and Fibre Channel. This section describes the steps that are different.

# 10.1 Mapping LUNs to Disaster Recovery Server

After FlexClone volumes have been created or SnapMirror relationships have been broken off, the LUNs must be mapped to the initiator group of the disaster recovery server.

Figure 70) Mapping LUN to target host.

Login	×	ONTAP System Manager	×   🖉 Privacy error	× 🖪 stlaurora-9	and10 - ONTA	P Syster × +	-				- 0
→ C ▲ Not secu	re   10.63	3.173.215/sysmgr/lun&svm	=SAP_NVA_DR								@ ☆ 8
ONTAP Sys	tem N	lanager							Ø 📮	\$	0 👱
Switch to the new exp	erience						Type: All	~	Q Search all Objects		+
		LUNs SV	M SAP_NVA_DR V								
Dashboard		LUN Management	Initiator Groups Portsets			Edit LUN				×	
Applications & Tie	rs 🕨	+ Create 👩 Clone	🧨 Edit 📋 Delete 🛛 😂 Statu	us 🔹 😭 Move 😾 Ste	orage QoS						
		Name	- Container Path		-	General	Initiator Groups			_	= Status
Storage	*	SH1_shared	/vol/SH1_shared_vol_dest_sm	15		Map 👻	Initiator Group Nam	е Туре	LUN ID (Optional)		S Onl
Nodes		SH1_shared	/vol/SH1_shared_vol_dest_sm		4 29		wlerx2540m4_22	Linux	2		Son Son
Aggregates & SH1_data_mnt00001 /vol/S_19_SAP_Data_vol_dest_sm_s											S Onl
Disks	•	SH1_data_mnt00001	/vol/S_19_SAP_Data_vol_dest_		2739_31						📀 Onl
SVMs		SH1_log_mnt00001	/vol/S_19_SAP_Log_vol_dest_s								🔮 Onl
Volumes		SH1_log_mnt00001	/vol/S_19_SAP_Log_vol_dest_s	sm_s_clone_13022020_0728	341_29						🔮 Onl
volumes		MH1_data_mnt00001	/vol/S_20_SAP_Data_vol_dest_	_sm_s							🥝 Onl
LUNs		MH1_log_mnt00001	/vol/S_20_SAP_Log_vol_dest_s	sm_s							🥝 Onl
Qtrees		tort lunt	hightest vol1								🗖 ()n
Quotas										-	
		LUN Properties	SH1_data_mnt00001	Dellas Group	None						
Network	•	Name: Container Path:	/vol/S_19_SAP_Data_vol	Policy Group: Minimum	NA	Show Al	Initiator Groups		Add Initiator Group		
Protection	•	Size:	500.08 GB	Throughput:							
Events & Jobs		Status:	Online	Maximum Throughput:	NA			Save	Save and Close Canc	el	
	,	Туре:	Linux	Move Job Status:	NA						
Configuration	•	LUN Clone:	false	Move Last Failure	NA						

# **10.2 Mount File Systems**

After the LUNs have been mapped, the discover process at the target host can be started.

```
wlerx2540m4-19:/usr/sap # rescan-scsi-bus.sh -a
```

The device files of the different LUNs can be determined with the NetApp sanlun utility. Depending on the multipathing configuration, there will be multiple device files. The following output shows the output for the data volume LUN. The same command must be executed for the log and the shared volume LUNs.

```
wlerx2540m4-19:/usr/sap # sanlun lun show | grep SAP_NVA_DR | grep data
SAP NVA DR
/vol/S_19_SAP_Data_vol_dest_sm_s_clone_13022020_072739_31/SH1_data_mnt00001 /dev/sddp
host12
         FCP
                  500.1g cDOT
SAP NVA DR
/vol/S_19_SAP_Data_vol_dest_sm_s_clone_13022020_072739_31/SH1_data_mnt00001 /dev/sddm
host12
                 500.1g CDOT
         FCP
SAP NVA DR
/vol/s 19 SAP Data vol dest sm s clone 13022020 072739 31/SH1 data mnt00001 /dev/sddj
host12
                   500.1g CDOT
         FCP
SAP NVA DR
/vol/S_19_SAP_Data_vol_dest_sm_s_clone_13022020_072739_31/SH1_data_mnt00001 /dev/sddg
host12
                   500.1g cDOT
         FCP
SAP NVA DR
/vol/S 19 SAP Data vol dest sm s clone 13022020 072739 31/SH1 data mnt00001 /dev/sddd
                 500.1g CDOT
host11
         FCP
SAP NVA DR
/vol/S 19 SAP Data vol dest sm s clone 13022020 072739 31/SH1 data mnt00001 /dev/sdda
                   500.1g CDOT
host11
         FCP
SAP NVA DR
/vol/s_19_SAP_Data_vol_dest_sm_s_clone_13022020_072739_31/SH1_data_mnt00001 /dev/sdcx
host11
         FCP
                  500.1g cDOT
SAP NVA DR
/vol/S_19_SAP_Data_vol_dest_sm_s_clone_13022020_072739 31/SH1 data mnt00001 /dev/sdcu
host11
         FCP
                   500.1g CDOT
```

One of the device files can now be selected to determine the UUID of the LUN. The same step must be done for the log and shared LUNs.

```
wlerx2540m4-19:/usr/sap # /lib/udev/scsi_id -g -u -d <mark>/dev/sddp</mark>
3600a098038304132793f4f7050757369
```

This UUIDs are now used to mount the file systems.

wlerx2540m4-19:~ # cat /etc/fstab							
/dev/system/swap	swap	swap	defaults	0	0		
/dev/system/root	/	btrfs	defaults	0	0		
/dev/system/root	/.snapshots	btrfs	subvol=/0/.snapshots	0	0		
/dev/system/root	/var	btrfs	subvol=/@/var	0	0		
/dev/system/root	/usr/local	btrfs	subvol=/@/usr/local	0	0		
/dev/system/root	/tmp	btrfs	subvol=/@/tmp	0	0		
/dev/system/root	/srv	btrfs	subvol=/@/srv	0	0		
/dev/system/root	/root	btrfs	subvol=/@/root	0	0		
/dev/system/root	/opt	btrfs	subvol=/0/opt	0	0		
/dev/system/root	/home	btrfs	subvol=/@/home	0	0		
/dev/system/root	/boot/grub2/x86 64-efi	btrfs	subvol=/@/boot/grub2/x86 64-e:	fi	0	0	
/dev/system/root	/boot/grub2/i386-pc	btrfs	subvol=/@/boot/grub2/i386-pc	0	0		
UUID=AD43-17E1	/boot/efi	vfat	defaults	0	0		
<pre>/dev/mapper/3600a098038304132793f4f705075736a /hana/log/SH1/mnt00001 xfs relatime,inode64,nobarrier,noauto 0 0 /dev/mapper/3600a098038304132793f4f7050757369 /hana/data/SH1/mnt00001 xfs relatime,inode64,noauto 0 0 /dev/mapper/3600a098038304133535d4f7466746a2f /hana/shared xfs defaults,noauto 0 0</pre>							

wlerx2540m4-19:/usr/sap # df -h | grep 3600 /dev/mapper/3600a098038304132793f4f7050757369 500G 7.1G 493G 2% /hana/data/SH1/mnt00001 /dev/mapper/3600a098038304132793f4f705075736a 500G 5.7G 495G 2% /hana/log/SH1/mnt00001 /dev/mapper/3600a098038304133535d4f7466746a2f 500G 67G 434G 14% /hana/shared

# **10.3 Cleanup Operation**

Unmount data, log, and shared file systems.

wlerx2540m4-22:~ # umount /hana/data/SH1/mnt00001 /hana/log/SH1/mnt00001 /hana/shared

Check in the output of multipath -ll for the WWID and the multipath devices of the LUN to be deleted.

wler	x2540m4-22	:~ # multipa	ath -11	
<mark>3600a</mark>	a098038304	132793f4f70	50757369 dm-5 NETAPP,LUN C-Mode	
size	=500G feat	ures='3 que	ue_if_no_path pg_init_retries 50' hwhandler='1 alua' wp=rw	
`-+-	policy='s	ervice-time	0' prio=50 status=active	
-	<mark>11:0:7:3</mark>	sdbi 67:192	2 active ready running	
-	<mark>11:0:0:3</mark>	sde 8:64	active ready running	
-	<mark>11:0:2:3</mark>	sdt 65:48	active ready running	
-	<mark>11:0:6:3</mark>	sdbe 67:12	8 active ready running	
-	12:0:7:3	sddq 71:12	8 active ready running	
-	12:0:1:3	sdbx 68:17	6 active ready running	
-	12:0:2:3	sdcb 68:24	0 active ready running	
`-	<mark>12:0:6:3</mark>	sddm 71:64	active ready running	

Remove the WWID by using multipath -f <WWID>.

```
wlerx2540m4-19:~ # multipath -f /dev/mapper/3600a098038304132793f4f7050757369
wlerx2540m4-19:~ # multipath -f /dev/mapper/3600a098038304132793f4f705075736a
wlerx2540m4-19:~ # multipath -f /dev/mapper/3600a098038304133535d4f7466746a2f
wlerx2540m4-19:~ #
```

### To remove the multipath device from *all* paths to the LUN, run

echo 1 > /sys/bus/scsi/devices/\${H:B:T:L}/delete
(where H = host:B = bus:T = target:L = lun).

wlerx2540m4-19:~ # echo 1 > /sys/bus/scsi/devices/11:0:7:3/delete

Note: This command must be executed for all device files listed in the multipath -ll output.

See also HOWTO: Add, Resize and Remove LUN without restarting SLES or OES Linux.

# Where to Find Additional Information

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

- TR-4436: SAP HANA on NetApp All Flash FAS Systems with Fibre Channel Protocol <u>http://www.netapp.com/us/media/tr-4436.pdf</u>
- TR-4435: SAP HANA on NetApp All Flash FAS Systems with NFS <u>http://www.netapp.com/us/media/tr-4435.pdf</u>
- TR-4614: SAP HANA Backup and Recovery with SnapCenter <u>https://www.netapp.com/us/media/tr-4614.pdf</u>
- TR-4667: Automating SAP System Copies Using the SnapCenter <u>https://www.netapp.com/us/media/tr-4667.pdf</u>
- TR-4719: SAP HANA System Replication, Backup and Recovery with SnapCenter <u>https://www.netapp.com/us/media/tr-4719.pdf</u>
- NetApp SnapCenter Software Resource page: <u>http://mysupport.netapp.com/snapcenter/resources</u>
- SAP Software Solutions product page: <u>http://www.netapp.com/us/solutions/applications/sap/index.aspx</u>

Version	Date	Document Version History						
Version 1.0	November 2017	Initial release.						
Version 1.1	April 2018	Update to cover SnapCenter 4.0						
Version 2.0	July 2020	<ul> <li>Complete rewrite:</li> <li>Three-site disaster recovery solution with synchronous and asynchronous SnapMirror replication</li> <li>DR testing and failover workflows for synchronous and asynchronous replication</li> <li>New software versions, SnapCenter 4.3, HANA 2.0 SPS4, SLES 15SP1, ONTAP 9.7</li> </ul>						

# **Version History**

Refer to the <u>Interoperability Matrix Tool (IMT)</u> 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 © 2017–2020 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc.

United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

### **Trademark Information**

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

TR-4646-0720

