



ANF Cross-Region Replication with SAP HANA

NetApp Solutions

NetApp
August 03, 2021

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ent-apps-db/saphana-dr-anf_configuration_options_for_cross-region_replication_with_sap_hana.html on August 03, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- ANF Cross-Region Replication with SAP HANA 1
 - Configuration options for Cross-Region Replication with SAP HANA 1
 - Requirements and best practices. 2
 - Lab setup 3
 - Configuration steps for ANF Cross-Region Replication 5
 - Monitoring ANF Cross-Region Replication. 10

ANF Cross-Region Replication with SAP HANA

[Previous: Disaster recovery solution comparison.](#)

Application agnostic information on Cross-Region Replication can be found at [Azure NetApp Files documentation | Microsoft Docs](#) in the concepts and how- to guide sections.

[Next: Configuration options for Cross-Region Replication with SAP HANA.](#)

Configuration options for Cross-Region Replication with SAP HANA

[Previous: ANF Cross-Region Replication with SAP HANA.](#)

The following figure shows the volume replication relationships for an SAP HANA system using ANF Cross-Region Replication. With ANF Cross-Region Replication, the HANA data and the HANA shared volume must be replicated. If only the HANA data volume is replicated, typical RPO values are in the range of one day. If lower RPO values are required, the HANA log backups must be also replicated for forward recovery.



The term “log backup” used in this document includes the log backup and the HANA backup catalog backup. The HANA backup catalog is required to execute forward recovery operations.

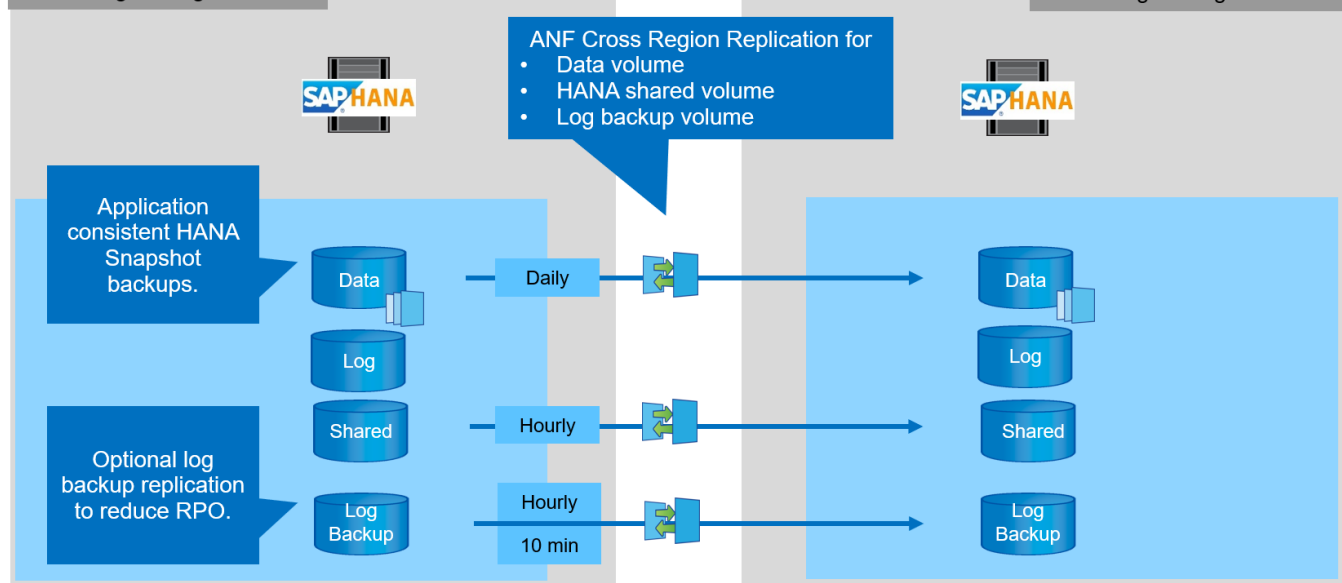


The following description and the lab setup focus on the HANA database. Other shared files, for example the SAP transport directory would be protected and replicated in the same way as the HANA shared volume.

To enable HANA save-point recovery or forward recovery using the log backups, application-consistent data Snapshot backups must be created at the primary site for the HANA data volume. This can be done for example with the ANF backup tool AzAcSnap (see also [What is Azure Application Consistent Snapshot tool for Azure NetApp Files | Microsoft Docs](#)). The Snapshot backups created at the primary site are then replicated to the DR site.

In the case of a disaster failover, the replication relationship must be broken, the volumes must be mounted to the DR production server, and the HANA database must be recovered, either to the last HANA save point or with forward recovery using the replicated log backups. The chapter [Disaster recovery failover](#), describes the required steps.

The following figure depicts the HANA configuration options for cross-region replication.



With the current version of Cross-Region Replication, only fixed schedules can be selected, and the actual replication update time cannot be defined by the user. Available schedules are daily, hourly and every 10 minutes. Using these schedule options, two different configurations make sense depending on the RPO requirements: data volume replication without log backup replication and log backup replication with different schedules, either hourly or every 10 minutes. The lowest achievable RPO is around 20 minutes. The following table summarizes the configuration options and the resulting RPO and RTO values.

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

[Next: Requirements and best practices.](#)

Requirements and best practices

[Previous: Configuration options for Cross-Region Replication with SAP HANA.](#)

Microsoft Azure does not guarantee the availability of a specific virtual machine (VM) type upon creation or when starting a deallocated VM. Specifically, in case of a region failure, many clients might require additional

VMs at the disaster recovery region. It is therefore recommended to actively use a VM with the required size for disaster failover as a test or QA system at the disaster recovery region to have the required VM type allocated.

For cost optimization it makes sense to use an ANF capacity pool with a lower performance tier during normal operation. The data replication does not require high performance and could therefore use a capacity pool with a standard performance tier. For disaster recovery testing, or if a disaster failover is required, the volumes must be moved to a capacity pool with a high-performance tier.

If a second capacity pool is not an option, the replication target volumes should be configured based on capacity requirements and not on performance requirements during normal operations. The quota or the throughput (for manual QoS) can then be adapted for disaster recovery testing in the case of disaster failover.

Further information can be found at [Requirements and considerations for using Azure NetApp Files volume cross-region replication | Microsoft Docs](#).

Next: [Lab setup](#).

Lab setup

Previous: [Requirements and best practices](#).

Solution validation has been performed with an SAP HANA single-host system. The Microsoft AzAcSnap Snapshot backup tool for ANF has been used to configure HANA application-consistent Snapshot backups. A daily data volume, hourly log backup, and shared volume replication were all configured. Disaster recovery testing and failover was validated with a save point as well as with forward recovery operations.

The following software versions have been used in the lab setup:

- Single host SAP HANA 2.0 SPS5 system with a single tenant
- SUSE SLES for SAP 15 SP1
- AzAcSnap 5.0

A single capacity pool with manual QoS has been configured at the DR site.

The following figure depicts the lab setup.



ANF Cross Region Replication for

- Data volume
- HANA shared volume
- Log backup volume



NetApp Account: saponanf

Capacity Pool: sap-pool1

NetApp Account: dr-saponanf

Capacity Pool: dr-sap-pool-premium

Application consistent
HANA Snapshot
backups.



Daily



Hourly



Hourly



Snapshot backup configuration with AzAcSnap

At the primary site, AzAcSnap was configured to create application-consistent Snapshot backups of the HANA system PR1. These Snapshot backups are available at the ANF data volume of the PR1 HANA system, and they are also registered in the SAP HANA backup catalog, as shown in the following two figures. Snapshot backups were scheduled for every 4 hours.

With the replication of the data volume using ANF Cross-Region Replication, these Snapshot backups are replicated to the disaster recovery site and can be used to recover the HANA database.

The following figure shows the Snapshot backups of the HANA data volume.

1-data-mnt00001)



PR1-data-mnt00001 (saponanf/sap-pool1/PR1-data-mnt00001) | Snapshots

Volume



Search (Ctrl+/)



+ Add snapshot

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- Properties
- Locks
- Storage service
- Mount instructions
- Export policy

Snapshots

Replication

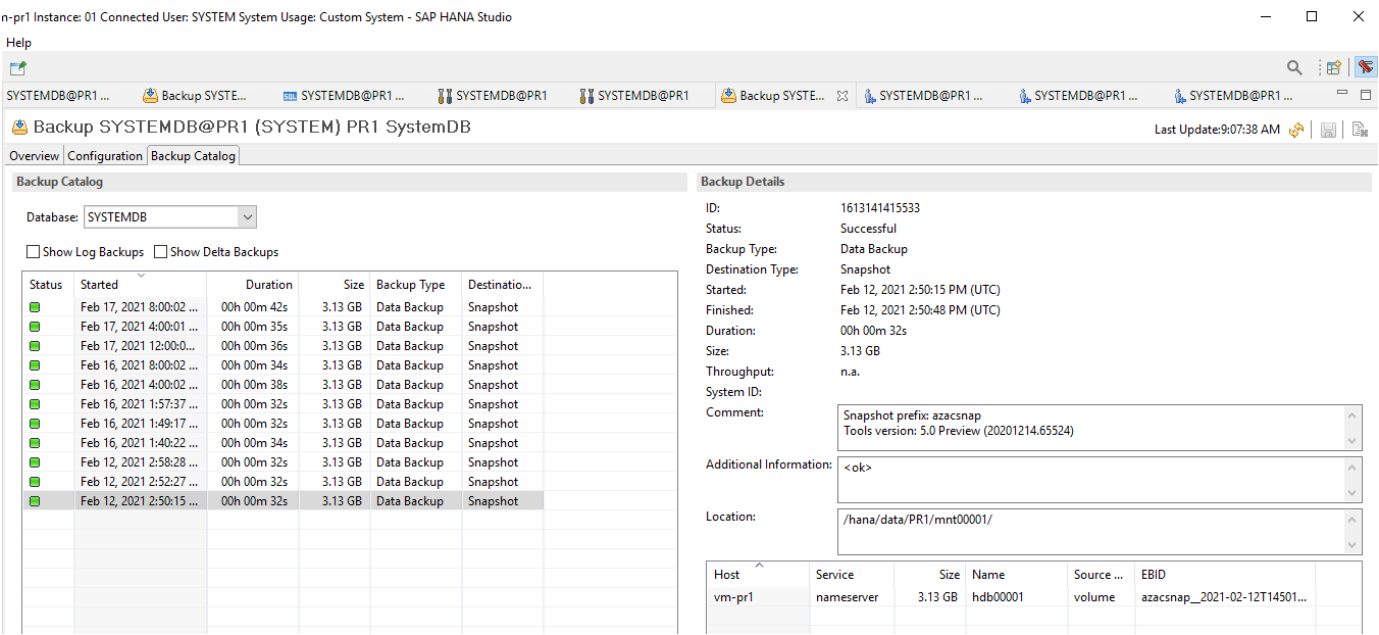
Monitoring

Metrics

Search snapshots

Name	↑↓	Location	↑↓	Created	↑↓
azacsnap__2021-02-12T145015-1799555Z		East US		02/12/2021, 03:49:48 PM	...
azacsnap__2021-02-12T145227-1245630Z		East US		02/12/2021, 03:51:24 PM	...
azacsnap__2021-02-12T145828-3863442Z		East US		02/12/2021, 03:58:01 PM	...
azacsnap__2021-02-16T134021-9431230Z		East US		02/16/2021, 02:39:18 PM	...
azacsnap__2021-02-16T134917-6284160Z		East US		02/16/2021, 02:48:55 PM	...
azacsnap__2021-02-16T135737-3778546Z		East US		02/16/2021, 02:56:32 PM	...
azacsnap__2021-02-16T160002-1354654Z		East US		02/16/2021, 04:59:40 PM	...
azacsnap__2021-02-16T200002-0790339Z		East US		02/16/2021, 08:59:42 PM	...
azacsnap__2021-02-17T000002-1753859Z		East US		02/17/2021, 12:59:32 AM	...
azacsnap__2021-02-17T040001-5454808Z		East US		02/17/2021, 04:59:31 AM	...
azacsnap__2021-02-17T080002-2933611Z		East US		02/17/2021, 08:59:40 AM	...

The following figure shows the SAP HANA backup catalog.



Next: [Configuration steps for ANF Cross-Region Replication.](#)

Configuration steps for ANF Cross-Region Replication

Previous: [Lab setup.](#)

A few preparation steps must be performed at the disaster recovery site before volume replication can be configured.

- A NetApp account must be available and configured with the same Azure subscription as the source.
- A capacity pool must be available and configured using the above NetApp account.
- A virtual network must be available and configured.
- Within the virtual network, a delegated subnet must be available and configured for use with ANF.

Protection volumes can now be created for the HANA data, the HANA shared and the HANA log backup volume. The following table shows the configured destination volumes in our lab setup.

To achieve the best latency, the volumes must be placed close to the VMs that run the SAP HANA in case of a disaster failover. Therefore, the same pinning process is required for the DR volumes as for any other SAP HANA production system.

HANA volume	Source	Destination	Replication schedule
HANA data volume	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Daily
HANA shared volume	PR1-shared	PR1-shared-sm-dest	Hourly
HANA log/catalog backup volume	hanabackup	hanabackup-sm-dest	Hourly

For each volume, the following steps must be performed:

1. Create a new protection volume at the DR site:
 - a. Provide the volume name, capacity pool, quota, and network information.
 - b. Provide the protocol and volume access information.
 - c. Provide the source volume ID and a replication schedule.
 - d. Create a target volume.
2. Authorize replication at the source volume.
 - Provide the target volume ID.

The following screenshots show the configuration steps in detail.

At the disaster recovery site, a new protection volume is created by selecting volumes and clicking Add Data Replication. Within the Basics tab, you must provide the volume name, capacity pool and network information.



The quota of the volume can be set based on capacity requirements, because volume performance does not have an effect on the replication process. In the case of a disaster recovery failover, the quota must be adjusted to fulfill the real performance requirements.



If the capacity pool has been configured with manual QoS, you can configure the throughput in addition to the capacity requirements. Same as above, you can configure the throughput with a low value during normal operation and increase it in case of a disaster recovery failover.

Create a new protection volume

Basics Protocol Replication Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name *	<input type="text" value="PR1-data-mnt00001-sm-dest"/>	✓
Capacity pool * ⓘ	<input type="text" value="dr-sap-pool1"/>	▼
Available quota (GiB) ⓘ	<div><div>4096</div><div>4 TiB</div></div>	
Quota (GiB) * ⓘ	<input type="text" value="500"/>	✓ 500 GiB
Virtual network * ⓘ	<div><input type="text" value="dr-vnet (10.2.0.0/16,10.0.2.0/24)"/> Create new</div>	▼
Delegated subnet * ⓘ	<div><input type="text" value="default (10.0.2.0/28)"/> Create new</div>	▼
Show advanced section	<input type="checkbox"/>	

Review + create

< Previous

Next : Protocol >

In the Protocol tab, you must provide the network protocol, the network path, and the export policy.



The protocol must be the same as the protocol used for the source volume.

Create a new protection volume

Basics Protocol Replication Tags Review + create

Configure access to your volume.

Access

Protocol type ☒ NFS ☐ SMB ☐ Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ

Versions * ▼

Kerberos ☐ Enabled ☒ Disabled

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

↑ Move up ↓ Move down ↑ Move to top ↓ Move to bottom 🗑 Delete

<input checked="" type="checkbox"/>	Index	Allowed clients	Access	Root Access	
<input checked="" type="checkbox"/>	1	<input type="text" value="0.0.0.0/0"/>	<input type="text" value="Read & Write"/> ▼	<input type="text" value="On"/> ▼	...
		<input type="text"/>	<input type="text"/> ▼	<input type="text"/> ▼	

Review + create

< Previous

Next : Replication >

Within the Replication tab, you must configure the source volume ID and the replication schedule. For data volume replication, we configured a daily replication schedule for our lab setup.



The source volume ID can be copied from the Properties screen of the source volume.

Create a new protection volume

Basics Protocol Replication Tags Review + create

Source volume ID ⓘ

/subscriptions/28cfc403-f3f6-4b07-9847-4eb16109e870/resourceGroups/rg... ✓

Replication schedule ⓘ

Daily ^

Every 10 minutes

Hourly

Daily

Review + create

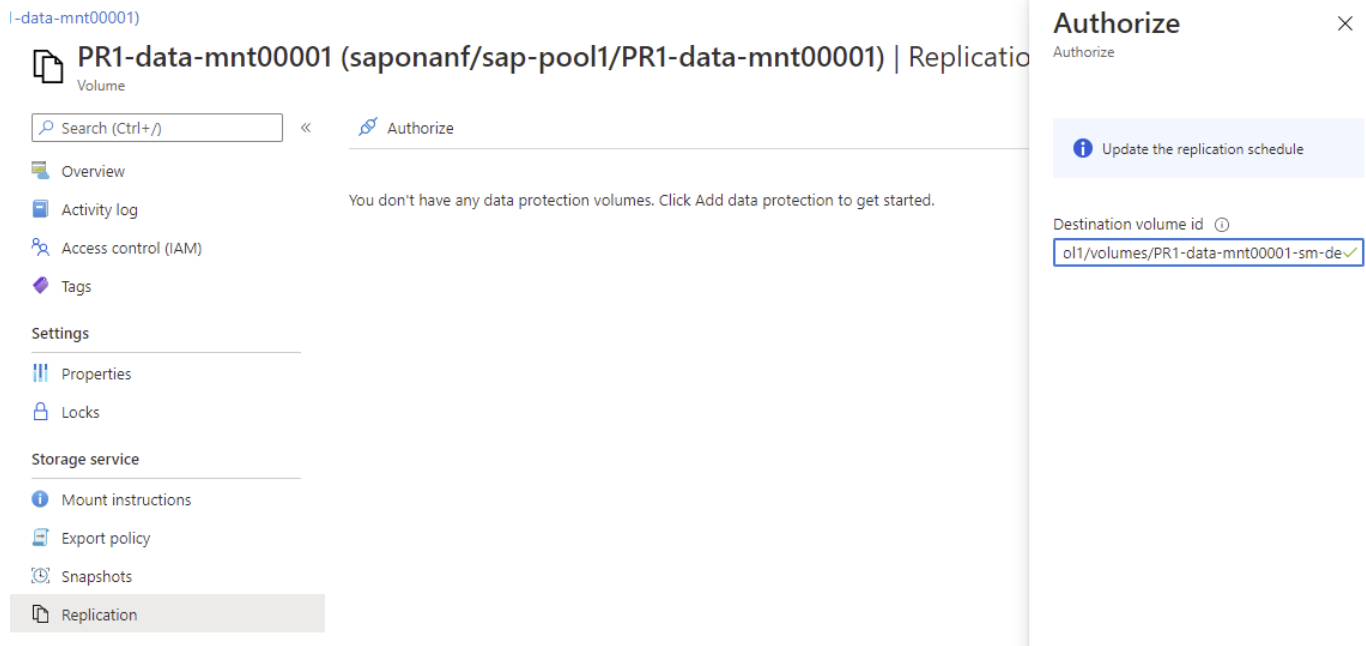
< Previous

Next : Tags >

As a final step, you must authorize replication at the source volume by providing the ID of the target volume.



You can copy the destination volume ID from the Properties screen of the destination volume.



The same steps must be performed for the HANA shared and the log backup volume.

[Next: Monitoring ANF Cross-Region Replication.](#)

Monitoring ANF Cross-Region Replication

[Previous: Configuration steps for ANF Cross-Region Replication.](#)

Replication status

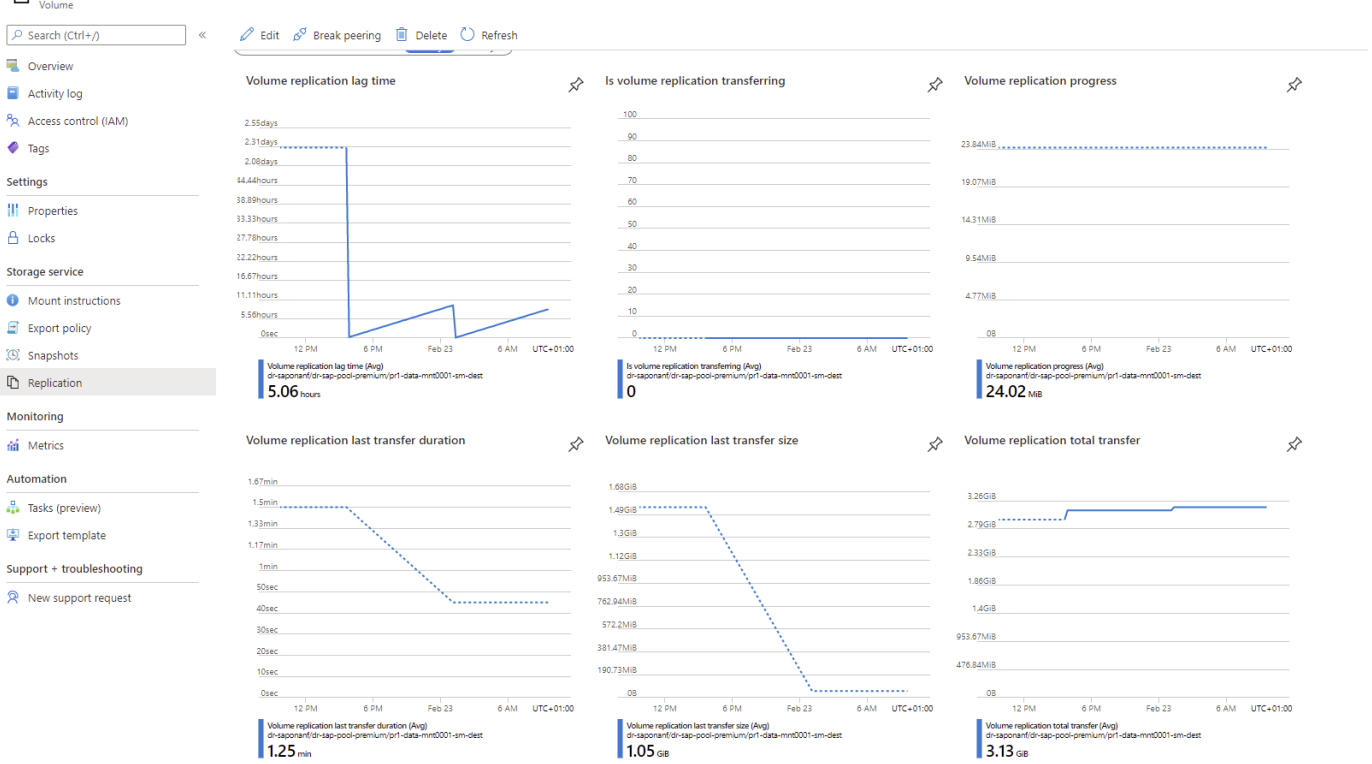
The following three screenshots show the replication status for the data, log backup, and shared volumes.

The volume replication lag time is a useful value to understand RPO expectations. For example, the log backup volume replication shows a maximum lag time of 58 minutes, which means that the maximum RPO has the same value.

The transfer duration and transfer size provide valuable information on bandwidth requirements and change the rate of the replicated volume.

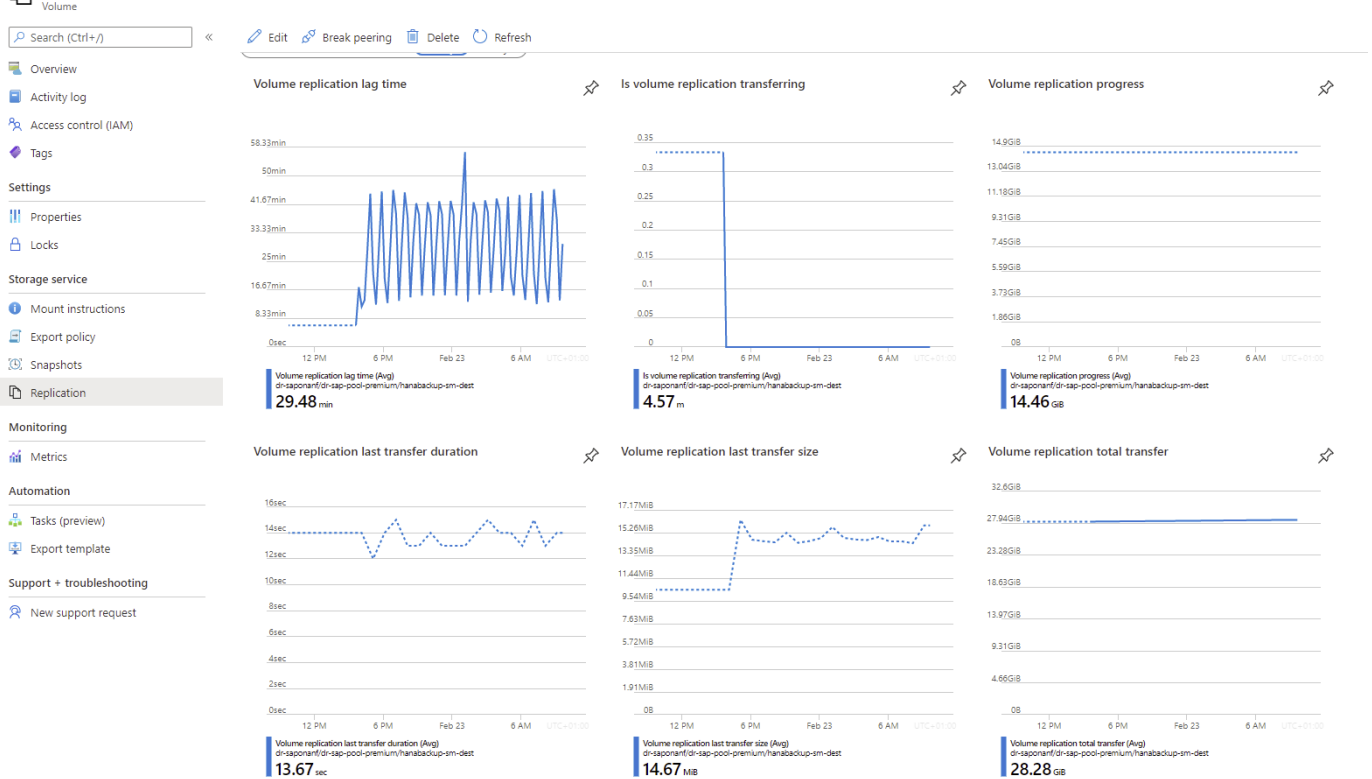
The following screenshot shows the replication status of HANA data volume.

PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Replication



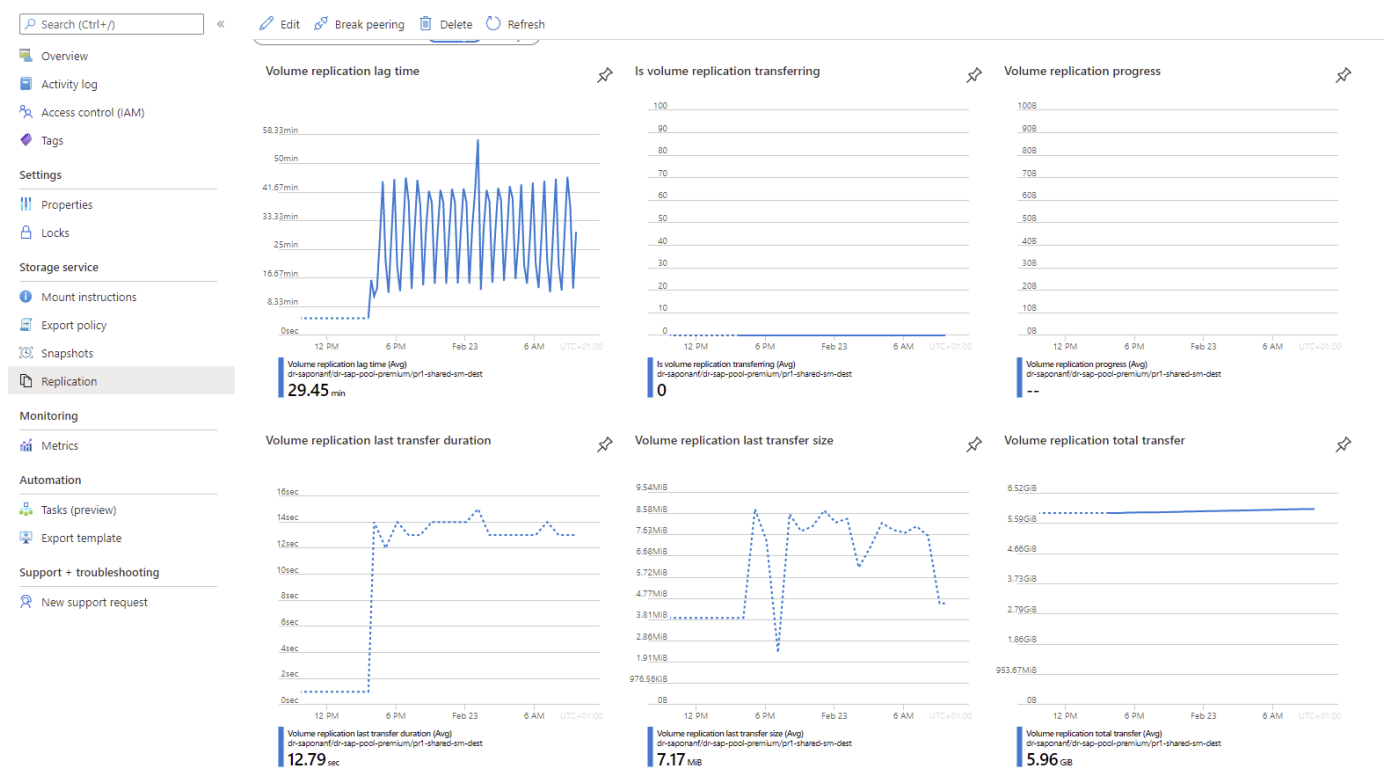
The following screenshot shows the replication status of HANA log backup volume.

hanabackup-sm-dest (dr-saponanf/dr-sap-pool-premium/hanabackup-sm-dest) | Replication



The following screenshot shows the replication status of HANA shared volume.

PR1-shared-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-shared-sm-dest) | Replication



Replicated snapshot backups

With each replication update from the source to the target volume, all block changes that happened between the last and the current update are replicated to the target volume. This also includes the snapshots, which have been created at the source volume. The following screenshot shows the snapshots available at the target volume. As already discussed, each of the snapshots created by the AzAcSnap tool are application-consistent images of the HANA database that can be used to execute either a savepoint or a forward recovery.



Within the source and the target volume, SnapMirror Snapshot copies are created as well, which are used for resync and replication update operations. These Snapshot copies are not application consistent from the HANA database perspective; only the application-consistent snapshots created via AzaCSnap can be used for HANA recovery operations.

Search (Ctrl+/)

«

+ Add snapshot

↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation















Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	↑↓ Location	↑↓ Created	↑↓
 azacsnap__2021-02-18T120002-2150721Z	West US	02/18/2021, 01:00:05 PM	...
 azacsnap__2021-02-18T160002-1442691Z	West US	02/18/2021, 05:00:49 PM	...
 azacsnap__2021-02-18T200002-0758687Z	West US	02/18/2021, 09:00:05 PM	...
 azacsnap__2021-02-19T000002-0039686Z	West US	02/19/2021, 01:00:05 AM	...
 azacsnap__2021-02-19T040001-8773748Z	West US	02/19/2021, 05:00:06 AM	...
 azacsnap__2021-02-19T080001-5198653Z	West US	02/19/2021, 09:00:05 AM	...
 azacsnap__2021-02-19T120002-1495322Z	West US	02/19/2021, 01:00:06 PM	...
 azacsnap__2021-02-19T160002-3698678Z	West US	02/19/2021, 05:00:05 PM	...
 azacsnap__2021-02-22T120002-3145398Z	West US	02/22/2021, 01:00:06 PM	...
 snapmirror.b1e8e48d-7114-11eb-b147-d039ea1e211e_2155791247.2021-02-22_143159	West US	02/22/2021, 03:32:00 PM	...
 azacsnap__2021-02-22T160002-0144647Z	West US	02/22/2021, 05:00:05 PM	...
 azacsnap__2021-02-22T200002-0649581Z	West US	02/22/2021, 09:00:05 PM	...
 azacsnap__2021-02-23T000002-0311379Z	West US	02/23/2021, 01:00:05 AM	...
 snapmirror.b1e8e48d-7114-11eb-b147-d039ea1e211e_2155791247.2021-02-23_001000	West US	02/23/2021, 01:10:00 AM	...

Next: Disaster recovery testing.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

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