



# **Architecture**

## **NetApp Solutions**

Ivana Devine, Dorian Henderson  
July 22, 2021

This PDF was generated from [https://docs.netapp.com/us-en/netapp-solutions/ent-apps-db/saphana\\_fas\\_fc\\_architecture.html](https://docs.netapp.com/us-en/netapp-solutions/ent-apps-db/saphana_fas_fc_architecture.html) on August 03, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Architecture ..... 1
  - SAP HANA backup..... 2
  - SAP HANA disaster recovery ..... 4

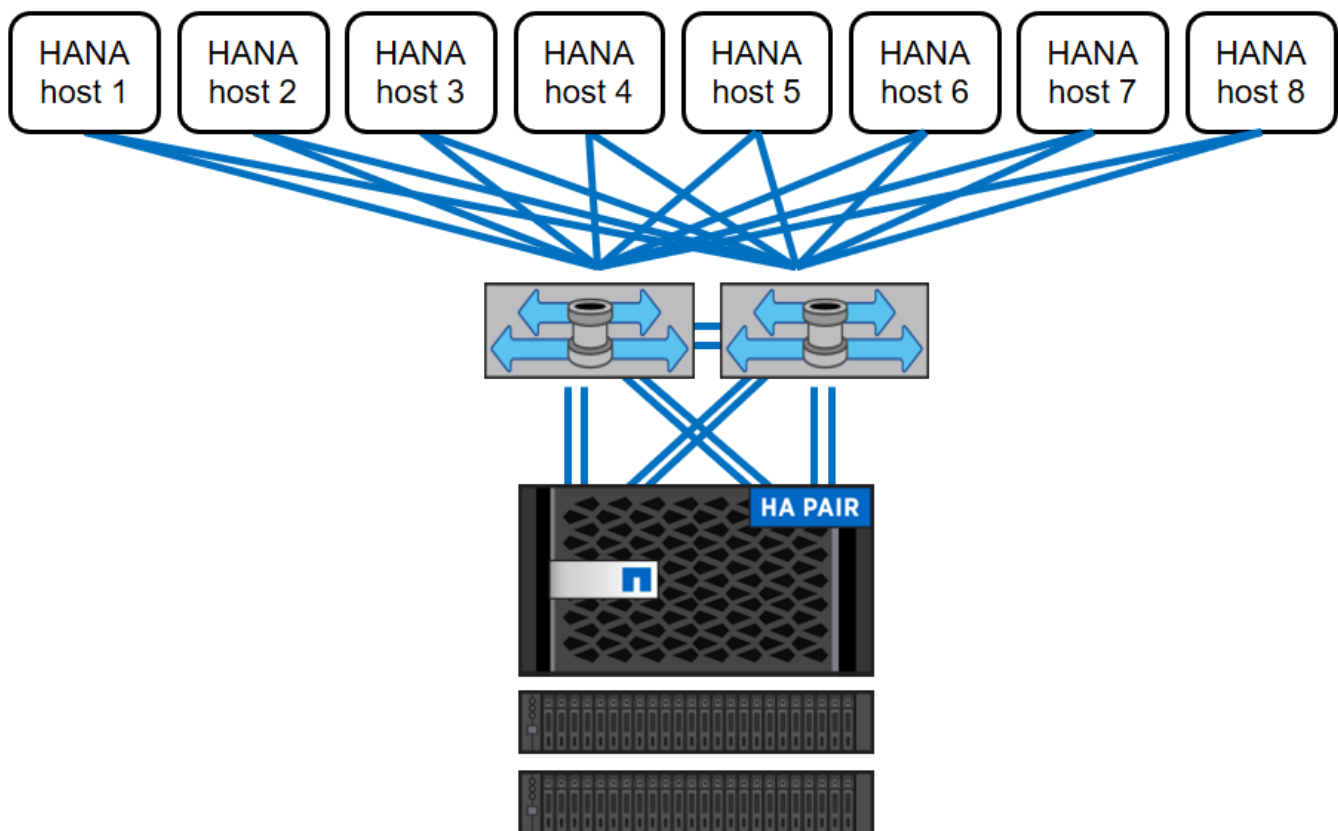
# Architecture

[Previous: SAP HANA on FAS Systems with FCP Configuration Guide.](#)

SAP HANA hosts are connected to the storage controllers using a redundant FCP infrastructure and multipath software. A redundant FCP switch infrastructure is required to provide fault-tolerant SAP HANA host-to-storage connectivity in case of switch or host bus adapter (HBA) failure. Appropriate zoning must be configured at the switch to allow all HANA hosts to reach the required LUNs on the storage controllers.

Different models of the FAS product family can be used at the storage layer. The maximum number of SAP HANA hosts attached to the storage is defined by the SAP HANA performance requirements. The number of disk shelves required is determined by the capacity and performance requirements of the SAP HANA systems.

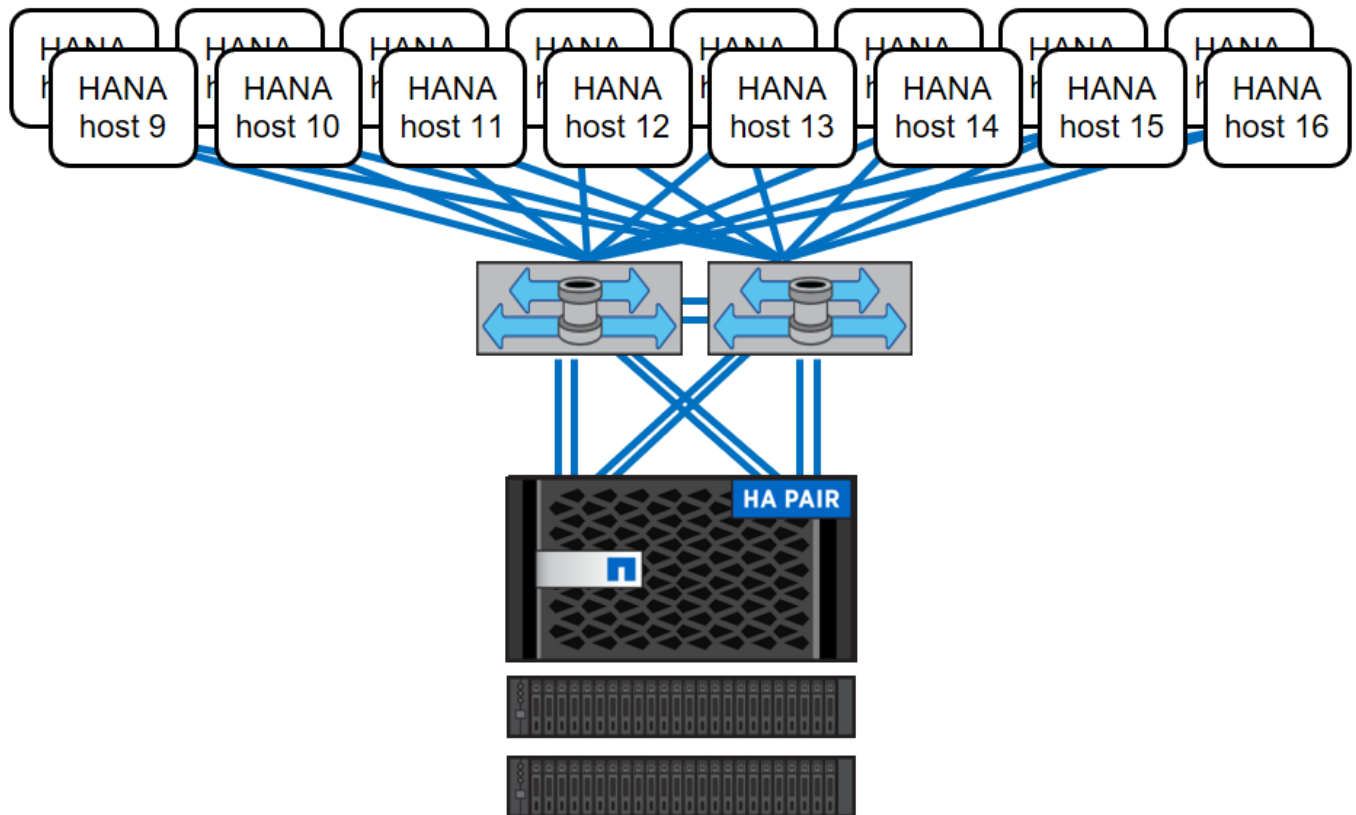
The following figure shows an example configuration with eight SAP HANA hosts attached to a storage HA pair.



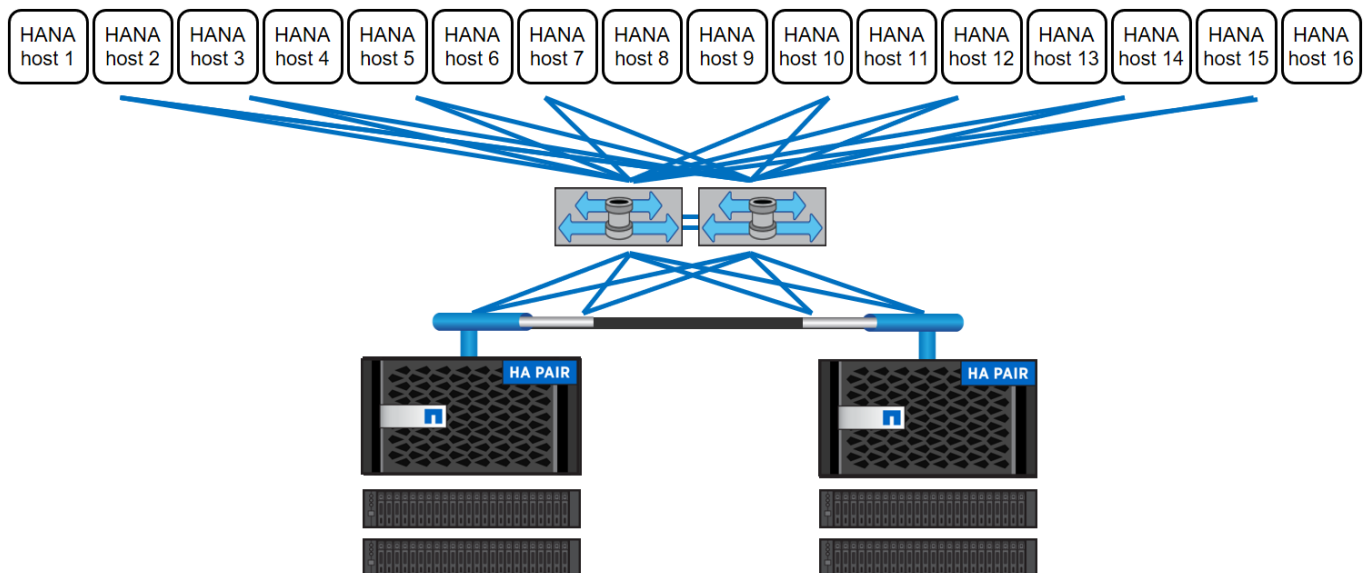
This architecture can be scaled in two dimensions:

- By attaching additional SAP HANA hosts and disk capacity to the storage, assuming that the storage controllers can provide enough performance under the new load to meet key performance indicators (KPIs)
- By adding more storage systems and disk capacity for the additional SAP HANA hosts

The following figure shows a configuration example in which more SAP HANA hosts are attached to the storage controllers. In this example, more disk shelves are necessary to meet the capacity and performance requirements of the 16 SAP HANA hosts. Depending on the total throughput requirements, you must add additional FC connections to the storage controllers.



Independent of the deployed FAS system storage model, the SAP HANA landscape can also be scaled by adding more storage controllers, as shown in the following figure.



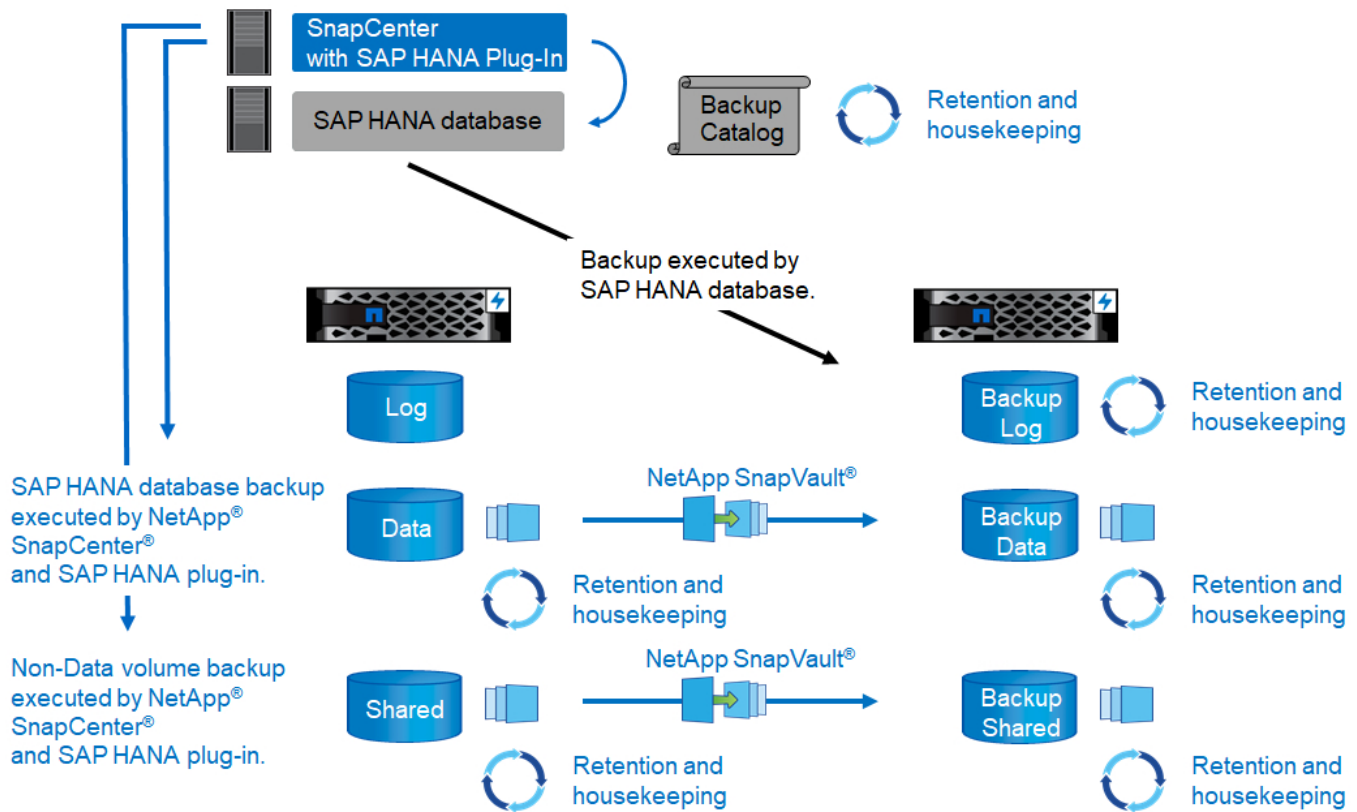
## SAP HANA backup

NetApp ONTAP software provides a built-in mechanism to back up SAP HANA databases. Storage-based Snapshot backup is a fully supported and integrated backup solution available for SAP HANA single-container systems and for SAP HANA MDC single-tenant systems.

Storage-based Snapshot backups are implemented by using the NetApp SnapCenter plug-in for SAP HANA, which enables consistent storage-based Snapshot backups by using the interfaces provided by the SAP HANA database. SnapCenter registers the Snapshot backups in the SAP HANA backup catalog so that the backups are visible within the SAP HANA studio and can be selected for restore and recovery operations.

By using NetApp SnapVault software, the Snapshot copies that were created on the primary storage can be replicated to the secondary backup storage controlled by SnapCenter. Different backup retention policies can be defined for backups on the primary storage and for backups on the secondary storage. The SnapCenter Plug-in for SAP HANA Database manages the retention of Snapshot copy-based data backups and log backups including the housekeeping of the backup catalog. The SnapCenter Plug-in for SAP HANA Database also enables the execution of a block-integrity check of the SAP HANA database by performing a file-based backup.

The database logs can be backed up directly to the secondary storage by using an NFS mount, as shown in the following figure.



Storage-based Snapshot backups provide significant advantages compared to file-based backups. Those advantages include the following:

- Faster backup (few minutes)
- Faster restore on the storage layer (a few minutes)
- No effect on the performance of the SAP HANA database host, network, or storage during backup
- Space-efficient and bandwidth-efficient replication to secondary storage based on block changes

For detailed information about the SAP HANA backup and recovery solution using SnapCenter, see [TR-4614: SAP HANA Backup and Recovery with SnapCenter](#).

# SAP HANA disaster recovery

SAP HANA disaster recovery can be performed on the database layer by using SAP system replication or on the storage layer by using storage-replication technologies. The following section provides an overview of disaster recovery solutions based on storage replication.

For detailed information about the SAP HANA disaster recovery solution using SnapCenter, see [TR-4646: SAP HANA Disaster Recovery with Storage Replication](#).

## Storage replication based on SnapMirror

The following figure shows a three-site disaster recovery solution, using synchronous SnapMirror replication to the local DR datacenter and asynchronous SnapMirror to replicate data to the remote DR datacenter.

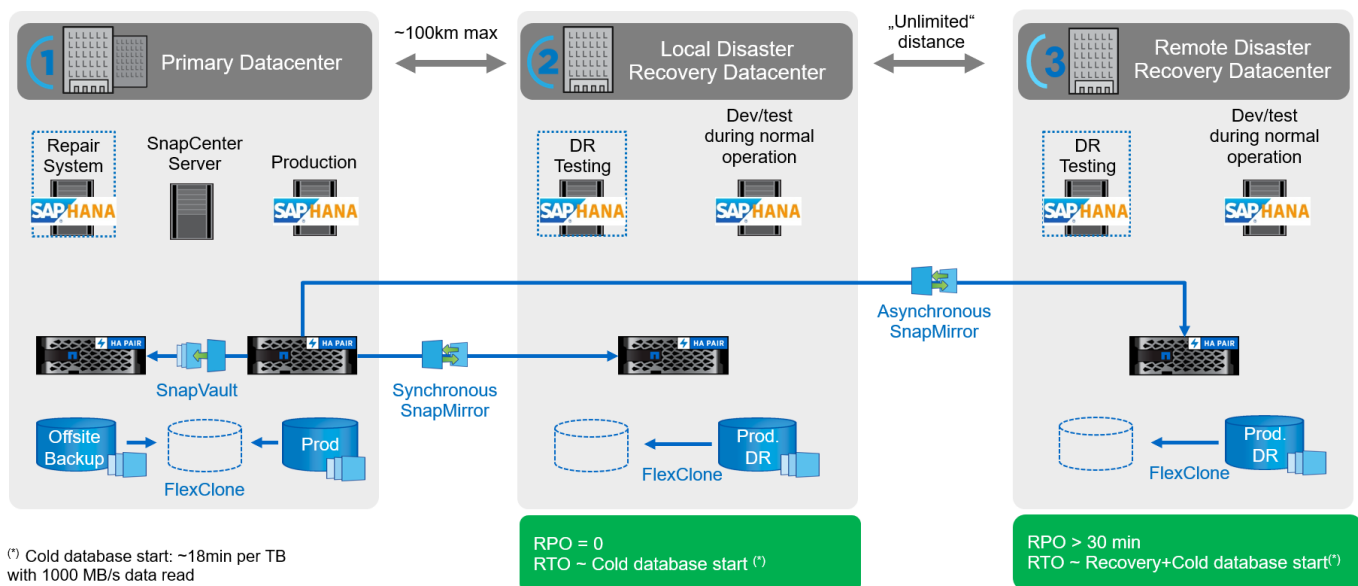
Data replication using synchronous SnapMirror provides an RPO of zero. The distance between the primary and the local DR datacenter is limited to around 100km.

Protection against failures of both the primary and the local DR site is performed by replicating the data to a third remote DR datacenter 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 primarily depends on the time needed to start the HANA database at the DR site and load the data into memory. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data would take approximately 18 minutes.

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

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

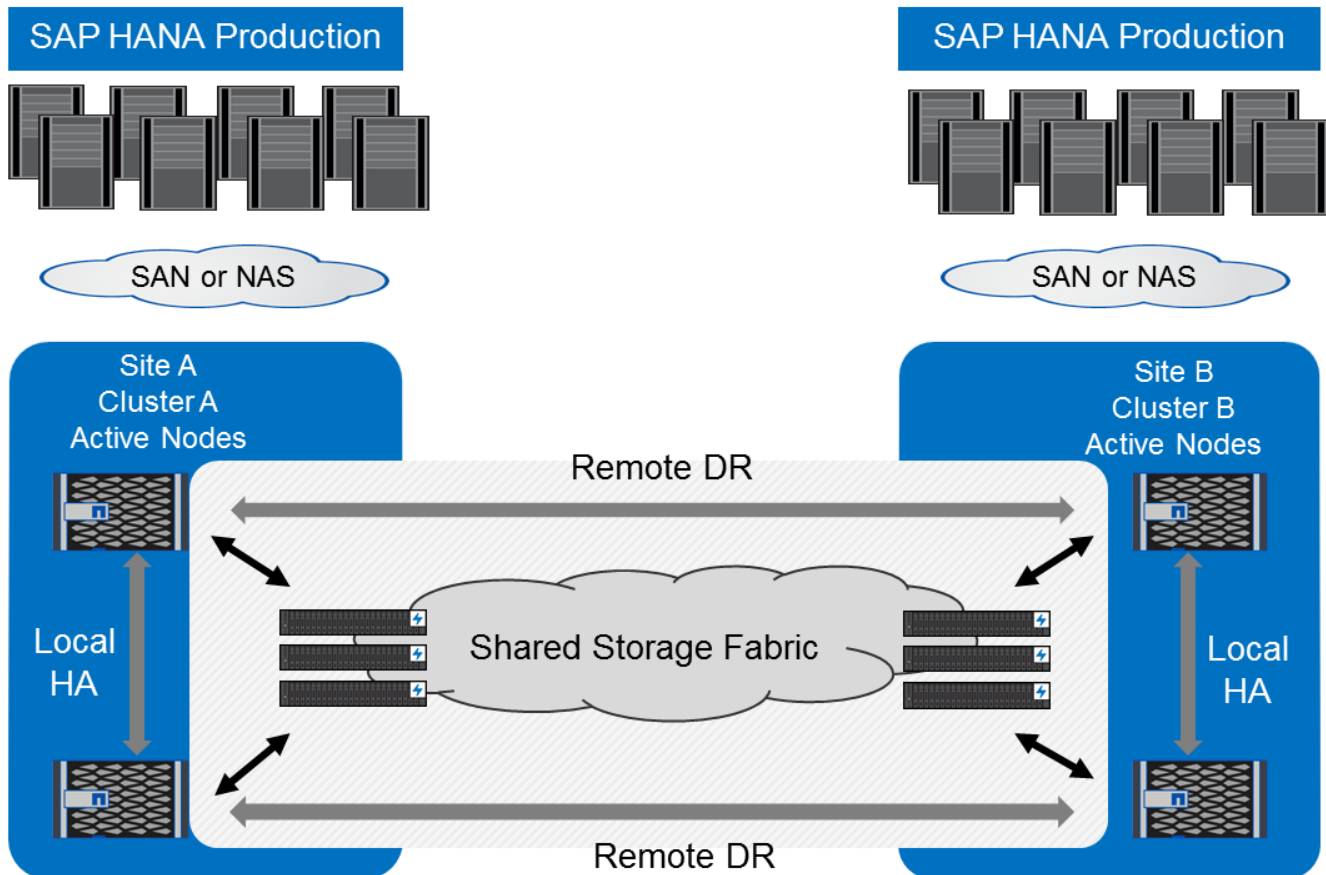


Synchronous replication offers StrictSync mode. If the write to secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage systems are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the InSync

status. If the primary storage fails, application I/O can be resumed on the secondary storage after failover with no loss of data. In StrictSync mode, the RPO is always zero.

## Storage replication based on NetApp MetroCluster

The following figure shows a high-level overview of the solution. The storage cluster at each site provides local high availability and is used for production workloads. The data at each site is synchronously replicated to the other location and is available in case of disaster failover.



Next: Storage sizing.

## 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.