Replicating data between systems

Cloud Manager

Ben Cammett
September 14, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_replicating_data.html on September 14, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Replicating data between systems 1
Data replication requirements 1
Setting up data replication between systems 2

Replicating data between systems

You can replicate data between ONTAP working environments by choosing a one-time data replication for data transfer, or a recurring schedule for disaster recovery or long-term retention. For example, you can set up data replication from an on-prem ONTAP system to Cloud Volumes ONTAP for disaster recovery.

Data replication requirements

Before you can replicate data, you should confirm that specific requirements are met for Cloud Volumes ONTAP, on-prem ONTAP clusters, or Amazon FSx for ONTAP.

Working environments

If you haven't done so already, you need to create the working environments for the source and target in the data replication relationship.

- Create an Amazon FSx for ONTAP working environment
- Launch Cloud Volumes ONTAP in AWS
- Launch Cloud Volumes ONTAP in Azure
- Launch Cloud Volumes ONTAP in GCP
- Add existing Cloud Volumes ONTAP systems
- Discover ONTAP clusters

Version requirements

You should verify that the source and destination volumes are running compatible ONTAP versions before replicating data. For details, see the Data Protection Power Guide.

Requirements specific to Cloud Volumes ONTAP

- The instance's security group must include the required inbound and outbound rules: specifically, rules for ICMP and ports 11104 and 11105.

  These rules are included in the predefined security group.

- To replicate data between two Cloud Volumes ONTAP systems in different subnets, the subnets must be routed together (this is the default setting).
- To replicate data between two Cloud Volumes ONTAP systems in different cloud providers, you must have a VPN connection between the virtual networks.

Requirements specific to ONTAP clusters

- An active SnapMirror license must be installed.
- If the cluster is on your premises, you should have a connection from your corporate network to your virtual network in AWS, Azure, or GCP. This is typically a VPN connection.
- ONTAP clusters must meet additional subnet, port, firewall, and cluster requirements.

  For details, see the Cluster and SVM Peering Express Guide.

Requirements specific to Amazon FSx for ONTAP

- An Amazon FSx for ONTAP working environment must be the target in the data replication relationship.

  The source can be Cloud Volumes ONTAP or an on-prem ONTAP cluster.

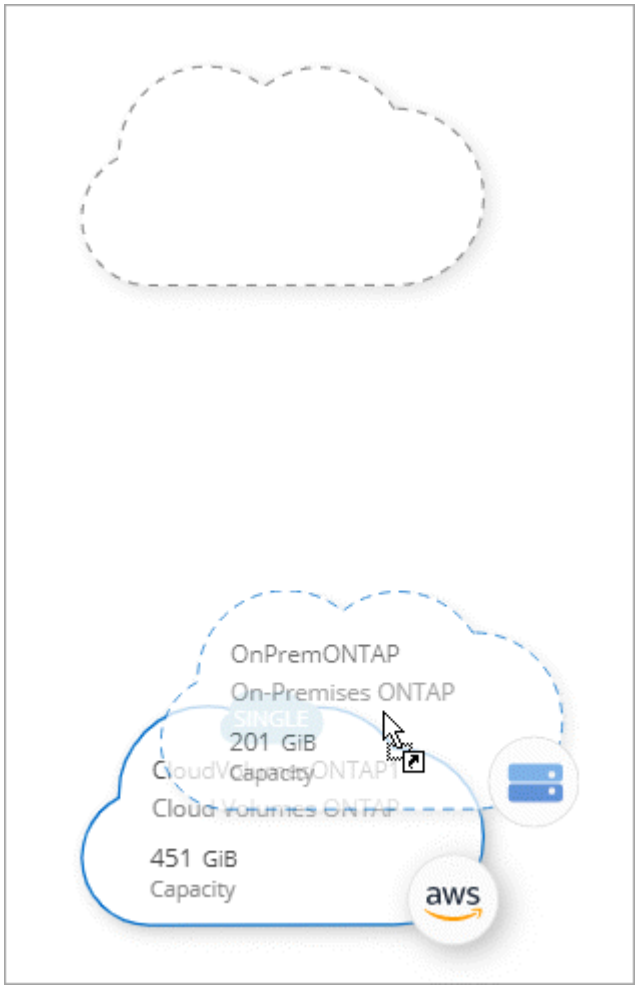
- If Cloud Volumes ONTAP is the source, ensure connectivity between VPCs by enabling VPC peering or by using a Transit Gateway.
- If an on-prem ONTAP cluster is the source, ensure connectivity between your on-premises network and the AWS VPC by using a Direct Connect or VPN connection.

Setting up data replication between systems

You can replicate data by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.



2. **Source and Destination Peering Setup**: If this page appears, select all of the intercluster LIFs for the cluster peer relationship.

   The intercluster network should be configured so that cluster peers have *pair-wise full-mesh connectivity*,

which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

These pages appear if an ONTAP cluster that has multiple LIFs is the source or destination.

3. **Source Volume Selection**: Select the volume that you want to replicate.
4. **Destination Disk Type and Tiering**: If the target is a Cloud Volumes ONTAP system, select the destination disk type and choose whether you want to enable data tiering.
5. **Destination Volume Name**: Specify the destination volume name and choose the destination aggregate.

   If the destination is an ONTAP cluster, you must also specify the destination storage VM.

6. **Max Transfer Rate**: Specify the maximum rate (in megabytes per second) at which data can be transferred.

   You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your internet performance.

7. **Replication Policy**: Choose a default policy or click **Additional Policies**, and then select one of the advanced policies.

   For help, learn about replication policies.

   If you choose a custom backup (SnapVault) policy, the labels associated with the policy must match the labels of the Snapshot copies on the source volume. For more information, learn how backup policies work.

8. **Schedule**: Choose a one-time copy or a recurring schedule.

   Several default schedules are available. If you want a different schedule, you must create a new schedule on the *destination* cluster using System Manager.

9. **Review**: Review your selections and click **Go**.

Result

Cloud Manager starts the data replication process. You can view details about the volume relationship in the Replication service.

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.