



Protect buckets with S3 SnapMirror

ONTAP 9

NetApp
November 04, 2021

Table of Contents

Protect buckets with S3 SnapMirror	1
S3 SnapMirror overview	1

Protect buckets with S3 SnapMirror

S3 SnapMirror overview

Beginning with ONTAP 9.10.1, you can protect buckets in ONTAP S3 object stores using familiar SnapMirror mirroring and backup functionality. In addition, unlike standard SnapMirror, S3 SnapMirror can have non-NetApp destinations.

S3 SnapMirror supports active mirrors and backup tiers from ONTAP S3 buckets to the following destinations:

Target	Supports active mirrors and takeover?	Supports backup and restore?
ONTAP S3 <ul style="list-style-type: none">• buckets in the same SVM• buckets in different SVMs on the same cluster• buckets in SVMs on different clusters	✓	✓
StorageGRID Webscale		✓
AWS S3		✓

You can protect existing buckets on ONTAP S3 servers or you can create new buckets with data protection enabled immediately.

S3 SnapMirror supports fan-out and cascade relationships. For an overview, see [Fan-out and cascade data protection deployments](#).

S3 SnapMirror requirements

- ONTAP version
ONTAP 9.10.1 or later must be running source and destination clusters.
- Licensing
The following license bundles are required on ONTAP source and destination systems:
 - Core Bundle
For ONTAP S3 protocol and storage.
 - Data Protection Bundle
For S3 SnapMirror to target other NetApp object store targets (ONTAP S3, StorageGRID, and Cloud Volumes ONTAP).
 - Data Protection Bundle and Hybrid Cloud Bundle
For S3 SnapMirror to target 3rd party object stores (AWS S3).
- ONTAP S3
 - ONTAP S3 servers must be running source and destination SVMs.
 - It is recommended but not required that certificates for TLS access are installed on the S3 servers.
- Peering (for ONTAP S3 targets)

- Intercluster LIFs must be configured (for remote ONTAP targets).
- Source and destination clusters are peered (for remote ONTAP targets).
- Source and destination storage VMs are peered (for all ONTAP targets).
- SnapMirror policy
An S3-specific SnapMirror policy is required for all S3 SnapMirror relationships, but you can use the same policy for multiple relationships.
- Root user keys
The first time you create an S3 SnapMirror relationship, you must generate root user keys on the source and destination storage VMs. Root user keys are required for S3 SnapMirror and ONTAP does not assign them by default. Once assigned, it is not necessary to regenerate them for additional S3 SnapMirror relationships.

For information about S3 server configuration, see the following topics:

- [Enable an S3 server on a storage VM \(System Manager\)](#)
- [About the S3 configuration process \(CLI\)](#)

For information about cluster and storage VM peering, see the following topic:

- [Prepare for mirroring and vaulting \(System Manager, steps 1-6\)](#)
- [Cluster and SVM peering \(CLI\)](#)

S3 SnapMirror considerations and restrictions

The following standard SnapMirror functionality is not supported in the current S3 SnapMirror release:

- Fan-in deployments (data protection relationships between multiple source buckets and a single destination bucket)
S3 Snapmirror can support multiple bucket mirrors from multiple clusters to a single secondary cluster, but each source bucket must have its own destination bucket on the secondary cluster.

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.