



Data Protection

ONTAP What's New

NetApp

November 23, 2020

This PDF was generated from https://docs.netapp.com/us-en/ontap-whatsnew/ontap98fo_data_protection.html on November 23, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Data Protection 1
 - Security..... 1
 - SnapMirror Cloud..... 2
 - SnapMirror Business Continuity (SM-BC)..... 3
 - MetroCluster 3

Data Protection

Data protection in the context of this document refers to both the notion of off-site replication of data, as well as securing that data in-flight and at-rest. This section covers the latest data protection enhancements for ONTAP 9.8.

Security

Each ONTAP release builds in new security features and enhancements, and ONTAP 9.8 is no different in that regard. For more information on ONTAP security features, see [TR-4569: Security Hardening Guide for ONTAP 9](#).

Secure Purge

In environments with classified or sensitive data, having a file mistakenly written to a volume that is accessible to people who should not have access to that file creates what is known as a data spill. This creates a scenario in which entire volumes must be deleted and disks scrubbed to clean up the spill.

NetApp Volume Encryption and Secure Purge provided a way to mitigate those potential disasters by offering a way to cryptographically shred individual files by deleting the security encryption key associated with the file. After that key is gone, that data is no longer recoverable from disk. This process has been externally validated by a data recovery company using NIST SP 800-88 guidelines for media sanitation.

But even secure purge had its limits; for example, if you must purge a file, you would need to perform a volume move, which requires available space in the system. If you have SnapMirror in place, you would need to re-baseline after a secure purge operation.

Secure Purge in ONTAP 9.8 removes those limitations by:

- Providing a simple, in-place procedure for cryptoshredding files.
- Allowing you to keep your existing SnapMirror mirrors in place with no need to re-baseline.

IPSec

IPSec is a standard mechanism for performing application-agnostic encryption over the wire. With IPSec, you can encrypt network traffic regardless of the protocol in use. That provides opportunities for simplification, particularly with NFS, where Kerberos encryption is difficult to set up and use, as well as providing the only way to encrypt iSCSI traffic over the wire.

ONTAP 9.8 now adds support for IPSec. The ONTAP implementation of IPSec leverages a pre-shared secret or key (PSK) with the connecting client. Those clients include any recent OS that leverages IKEv2 with PSK. Note that the Windows OS does not support IKEv2 with PSK.

Trusted Platform Module

With the new Trusted Platform Module (TPM) in ONTAP 9.8, the encryption keys for the onboard key manager (OKM) are no longer stored in the boot device but instead are stored in the physical TPM for systems so equipped, offering greater security and protection. Moving to the TPM is a nondisruptive process.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) is a software solution that enables encryption of any data volume on any drive type where it is enabled, with a unique key for each volume. This feature has been available since ONTAP 9.1.

ONTAP 9.8 brings NVE support to the node root volumes, which contain log files, cluster configuration backups, core files and other system-related information that you may want to secure with FIPS-140-2 compliant encryption.

SnapMirror Cloud

SnapMirror is industry-leading replication technology in ONTAP that provides a way for storage administrators to create exact copies of datasets across a WAN connection and only replicating the changed blocks for reduced network utilization.

Over the past few ONTAP releases, SnapMirror support has been expanded to include non-ONTAP systems, such as the [SolidFire Element OS](#). ONTAP 9.8 now provides a way to leverage SnapMirror to replicate to cloud or on-premises S3 object buckets.



By leveraging the new [SnapDiff 3.0 engine](#), SnapMirror can securely and efficiently replicate data from ONTAP NAS volumes to object storage buckets. This provides hybrid-cloud mobility across the ONTAP data fabric.

- Space-efficient backups of snapshots to cloud object storage preserve storage efficiency.
- Supports full-volume and single-file restore

In ONTAP 9.8, SnapMirror Cloud requires orchestration by one of the following two methods. It is not supported in System Manager or directly through APIs or the CLI.

- Through a licensed ISV partner application which creates and manage the backup and restore

workflows. A SnapMirror Cloud license is required.

- Through the Cloud Backup Service. A SnapMirror Cloud license is not required.

For more information on SnapDiff and SnapMirror Cloud, see the following resources:

- [Tech ONTAP Podcast Episode 264: NetApp ONTAP SnapDiff](#)
- [Tech ONTAP Podcast Episode 265: NetApp SnapMirror Cloud featuring ProLion](#)
- [NetApp Blog: A new backup architecture with SnapDiff/SnapMirror Cloud-v3](#)

SnapMirror Business Continuity (SM-BC)

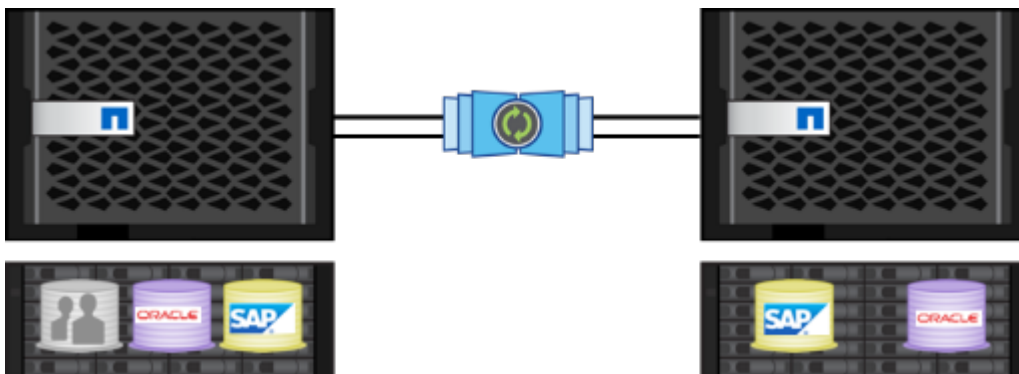
[SnapMirror Synchronous](#) (SM-S) was introduced in ONTAP 9.5 and provides volume- granular and storage-efficient synchronous data replication that enterprises depend on for backup, disaster recovery, and data mobility. SM-S replicates data on NetApp FlexVol volumes between fully redundant ONTAP storage systems located across data centers or metro regions with a round trip time (RTT) less than 10ms to achieve a zero recovery point objective and a near-zero recovery time objective.

ONTAP 9.8 takes the concept of SnapMirror Synchronous in SAN environments and brings an automated failover capability for applications at the Consistency Group, using System Manager to configure and the ONTAP Mediator to manage and maintain business continuity in the event of an outage. Because the relationship is synchronous, applications won't miss a beat when failing over. The initial release of SnapMirror Business Continuity only supports SAN (iSCSI and FCP) workloads.

For more information on SnapMirror Business Continuity, see the [Tech ONTAP Podcast Episode 267: SnapMirror Business Continuity](#).

MetroCluster

NetApp MetroCluster (MC) software is a solution that combines array-based clustering with synchronous replication to deliver continuous availability and zero data loss at the lowest cost. Administration of the array-based cluster is simpler because the dependencies and complexity normally associated with host-based clustering are eliminated.



MetroCluster immediately duplicates all your mission-critical data on a transaction-by-transaction

basis, providing uninterrupted access to your applications and data. Unlike standard data replication solutions, MetroCluster works seamlessly with your host environment to provide continuous data availability while eliminating the need to create and maintain complicated failover scripts.

With MetroCluster, you can perform the following tasks:

- Protect against hardware, network, or site failure with transparent switchover
- Eliminate planned and unplanned downtime and change management
- Upgrade hardware and software without disrupting operations
- Deploy without complex scripting, application, or operating system dependencies
- Achieve continuous availability for VMware, Microsoft, Oracle, SAP, or any critical application

ONTAP 9.8 provides the following feature enhancements for MetroCluster.

- **New entry-level and midrange platform support.** NetApp AFF A250, FAS500f, FAS8300, FAS 8700 hybrid, and A400. For new installations of A220, FAS2750, and FAS500f, a VLAN can now be specified to be greater than 100 and less than 4096.
- **Non-disruptive transition from MC-FC to MC-IP.** Four-node clusters only; two-node MCC require downtime. Simple to move to MC IP in your upcoming tech refresh.
- **Unmirrored aggregates now supported for MC IP.** Replicate only desired aggregates to the failover site for more application granularity.
- Support for the Cisco 9336C-FX2 switch and for A400, FAS 8300, and FAS 8700 on the BES-53248 switch with an additional 100G port license.

For more information about MetroCluster, see the following resources:

- [TR-4375: MetroCluster FC for ONTAP 9.7](#)
- [TR-4689: MetroCluster IP Solution Architecture and Design](#)
- [TR-4705: NetApp MetroCluster Solution Architecture and Design](#)

[Next: VMware Virtualization](#)

Copyright Information

Copyright © 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.

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.