SnapMirror active sync

ONTAP 9

NetApp
February 12, 2026

Table of Contents

SnapMirror active sync

Introduction

Learn about ONTAP SnapMirror active sync

SnapMirror active sync, also known as SnapMirror Business Continuity (SM-BC), allows business services to continue functioning in the event of a complete site failure. This technology enables applications to failover seamlessly to a secondary copy without manual intervention or custom scripting.

NetApp SnapMirror active sync (SM-as) is designed to be a more granular, lower-cost, easier-to-use application-level protection with automatic failover. SnapMirror active sync enables mission-critical business services to keep operating, even during a complete site failure. With SnapMirror active sync, you can now synchronously replicate multiple volumes of an application (by adding them to a consistency group) between sites at geographically dispersed locations. You can automatically failover to the secondary copy in case of disruption of the primary, thus enabling business continuity for tier one applications.

Regulations for financial institutions in some countries require businesses to periodically be serviceable from their secondary data centers. SnapMirror active sync, with its high availability clusters, enables these data center switchovers for business continuity.

Available beginning with ONTAP 9.9.1, SnapMirror active sync is supported on AFF and All-Flash SAN Array (ASA) clusters. The primary and secondary clusters must be of the same type: either ASA, ASA r2, or AFF. SnapMirror active sync protects applications with iSCSI or FCP LUNs or NVMe namespaces.

SnapMirror active sync supports both symmetric and asymmetric configurations. Support for symmetric active/active was introduced in ONTAP 9.15.1. Symmetric active/active configuration allows both copies of a protected LUN to perform read and write I/O operations with bidirectional synchronous replication, enabling each LUN copy to serve local I/O requests.

> Beginning July 2024, content from technical reports previously published as PDFs has been integrated with ONTAP product documentation. The ONTAP SnapMirror active sync documentation now includes content from *TR-4878: SnapMirror active sync*.

Benefits

SnapMirror active sync provides the following benefits:

- Continuous availability for business-critical applications.
- Ability to host critical applications alternately from primary and secondary sites.
- Simplified application management using consistency groups for dependent write-order consistency.
- The ability to test failover for each application.
- Instantaneous creation of mirror clones without impacting application availability.
- The ability to deploy protected and non-protected workloads in the same ONTAP cluster.
- LUN, NVMe namespace, NVMe subsystem, or storage unit identity remains the same, so the application sees them as a shared virtual device.
- The ability to reuse secondary clusters with flexibility to create instantaneous clones for application usage

for dev-test, UAT or reporting purposes without impacting application performance or availability.

SnapMirror active sync allows you to protect your data LUNs or NVMe namespaces, which enables applications to fail over transparently for the purpose of business continuity in the event of a disaster. For more information, see Use cases.

Key concepts

SnapMirror active sync uses consistency groups to ensure your data is replicated. SnapMirror active sync uses the ONTAP Mediator or, beginning with ONTAP 9.17.1, the Cloud Mediator for automated failover, ensuring the data is served in the event of a disaster scenario. When planning your SnapMirror active sync deployment, it is important to understand the essential concepts in SnapMirror active sync and its architecture.

Asymmetry and symmetry

In symmetric active/active configurations, both sites can access local storage for active I/O. Symmetric active/active is optimized for clustered applications including VMware vMSC, Windows Failover Cluster with SQL, and Oracle RAC.

In asymmetric active/active configurations data on the secondary site is proxied to a LUN, namespace or storage unit.

For more information, see SnapMirror active sync architecture.

Consistency group

For AFF and ASA systems a consistency group is a collection of FlexVol volumes that provide a consistency guarantee for the application workload that must be protected for business continuity. In ASA r2 systems, a consistency group is a collection of storage units.

The purpose of a consistency group is to take simultaneous snapshot images of a collection of volumes or storage units, thus ensuring crash-consistent copies of the collection at a point in time. A consistency group ensures all volumes of a dataset are quiesced and then snapped at precisely the same point in time. This provides a data-consistent restore point across volumes or storage units supporting the dataset. A consistency group thereby maintains dependent write-order consistency. If you decide to protect applications for business continuity, the group of volumes or storage units corresponding to this application must be added to a consistency group so a data protection relationship is established between a source and a destination consistency group. The source and destination consistency must contain the same number and type of volumes.

Constituent

An individual volume, LUN, or NVMe namespace (beginning with ONTAP 9.17.1) that is part of the consistency group protected in the SnapMirror active sync relationship.

ONTAP Mediator

The ONTAP Mediator receives health information about peered ONTAP clusters and nodes, orchestrating between the two and determining if each node/cluster is healthy and running. ONTAP Mediator provides health information about:

- Peer ONTAP clusters
- Peer ONTAP cluster nodes
- Consistency groups (which define the failover units in a SnapMirror active sync relationship); for each consistency group, the following information is provided:
  - Replication state: Uninitialized, In Sync, or Out of Sync

- Which cluster hosts the primary copy
- Operation context (used for planned failover)

With this ONTAP Mediator health information, clusters can differentiate between distinct types of failures and determine whether to perform an automated failover. ONTAP Mediator is one of the three parties in the SnapMirror active sync quorum along with both ONTAP clusters (primary and secondary). To reach consensus, at least two parties in the quorum must agree to a certain operation.

> Beginning with ONTAP 9.15.1, System Manager displays the status of your SnapMirror active sync relationship from either cluster. You can also monitor the ONTAP Mediator's status from either cluster in System Manager. In earlier releases of ONTAP, System Manager displays the status of SnapMirror active sync relationships from the source cluster.

ONTAP Cloud Mediator

ONTAP Cloud Mediator is available beginning with ONTAP 9.17.1. ONTAP Cloud Mediator provides the same services as ONTAP Mediator, except that it is hosted in the cloud using the NetApp Console.

Planned failover

A manual operation to change the roles of copies in a SnapMirror active sync relationship. The primary sites becomes the secondary, and the secondary becomes the primary.

Automatic unplanned failover (AUFO)

An automatic operation to perform a failover to the mirror copy. The operation requires assistance from the ONTAP Mediator to detect that the primary copy is unavailable.

Primary-first and primary bias

SnapMirror active sync uses a primary-first principle that gives preference to the primary copy to serve I/O in case of a network partition.

Primary-bias is a special quorum implementation that improves availability of a SnapMirror active sync protected dataset. If the primary copy is available, primary-bias comes into effect when the ONTAP Mediator is not reachable from both clusters.

Primary-first and primary bias are supported in SnapMirror active sync beginning with ONTAP 9.15.1. Primary copies are designated in System Manager and output with the REST API and CLI.

Out of Sync (OOS)

When the application I/O is not replicating to the secondary storage system, it will be reported as **out of sync**. An out of sync status means the secondary volumes are not synchronized with the primary (source) and that SnapMirror replication is not occurring.

If the mirror state is `Snapmirrored`, this indicates a SnapMirror relationship is established and the data transfer is complete, meaning the destination volume is up-to-date with the source volume.

SnapMirror active sync supports automatic resync, enabling copies to return to an InSync state.

Beginning with ONTAP 9.15.1, SnapMirror active sync supports automatic reconfiguration in fan-out configurations.

Uniform and non-uniform configuration

- **Uniform host access** means that hosts from both sites are connected to all paths to storage clusters on both sites. Cross-site paths are stretched across distances.

- **Non-uniform host access** means hosts in each site are connected only to the cluster in the same site. Cross-site paths and stretched paths aren’t connected.

ⓘ Uniform host access is supported for any SnapMirror active sync deployment; non-uniform host access is only supported for symmetric active/active deployments.

Zero RPO

RPO stands for recovery point objective, which is the amount of data loss deemed acceptable during a given time period. Zero RPO signifies that no data loss is acceptable.

Zero RTO

RTO stands for recovery time objective, which is the amount of time that is deemed acceptable for an application to return to normal operations non-disruptively following an outage, failure, or other data loss event. Zero RTO signifies that no amount of downtime is acceptable.

SnapMirror active sync configuration support by ONTAP version

Support for SnapMirror active sync varies depending on your version of ONTAP:

ONTAP version	Supported clusters	Supported protocols	Supported configurations
9.17.1 and later	• AFF • ASA • C-Series • ASA r2	• iSCSI • FC • NVMe for VMware workloads	• Asymmetric active/active ⓘ Asymmetric active/active does not support ASA r2 and NVMe For more information about NVMe support, see NVMe configuration, support, and limitations. • Symmetric active/active

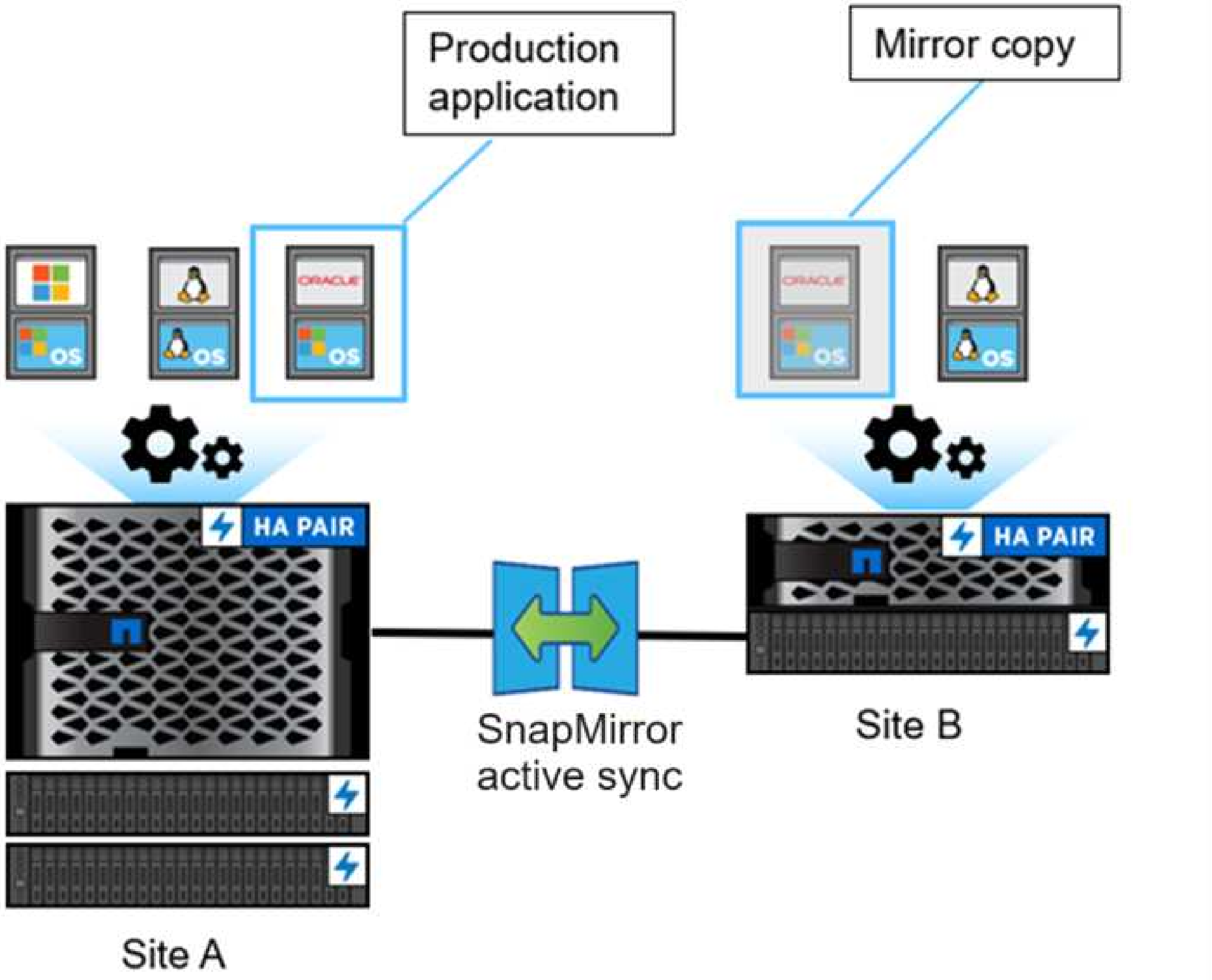
9.16.1 and later	• AFF • ASA • C-Series • ASA r2	• iSCSI • FC	• Asymmetric active/active • Symmetric active/active Symmetric active/active configurations support 4-node clusters in ONTAP 9.16.1 and later. For ASA r2, only 2-node clusters are supported.
9.15.1 and later	• AFF • ASA • C-Series	• iSCSI • FC	• Asymmetric active/active • Symmetric active/active Symmetric active/active configurations support 2-node clusters in ONTAP 9.15.1. 4-node clusters are supported in ONTAP 9.16.1 and later.
9.9.1 and later	• AFF • ASA • C-Series	• iSCSI • FC	Asymmetric active/active

Primary and secondary clusters must be of the same type: either ASA, ASA r2, or AFF.

ONTAP SnapMirror active sync architecture

The SnapMirror active sync architecture enables active workloads on both clusters, where primary workloads can be served simultaneously from both clusters. Regulations for financial institutions in some countries require businesses to be periodically serviceable from their secondary data centers as well, called "Tick-Tock" deployments, which SnapMirror active sync enables.

The data protection relationship to protect for business continuity is created between the source storage system and destination storage system, by adding the application specific LUNs or NVMe namespaces from different volumes within a storage virtual machine (SVM) to the consistency group. Under normal operations, the enterprise application writes to the primary consistency group, which synchronously replicates this I/O to the mirror consistency group.



Even though two separate copies of the data exist in the data protection relationship, because SnapMirror active sync maintains the same LUN or NVMe namespace identity, the application host sees this as a shared virtual device with multiple paths while only one LUN or NVMe namespace copy is being written to at a time. When a failure renders the primary storage system offline, ONTAP detects this failure and uses the Mediator for re-confirmation; if neither ONTAP nor the Mediator are able to ping the primary site, ONTAP performs the automatic failover operation. This process results in failing over only a specific application without the need for manual intervention or scripting which was previously required for the purpose of failover.

Other points to consider:

- Unmirrored volumes which exist outside of protection for business continuity are supported.
- Only one other SnapMirror asynchronous relationship is supported for volumes being protected for business continuity.
- Cascade topologies are not supported with protection for business continuity.

The role of mediators

SnapMirror active sync uses a mediator to act as a passive witness to SnapMirror active sync copies. In the event of a network partition or unavailability of one copy, SnapMirror active sync uses the mediator to determine which copy continues to serve I/O, while discontinuing I/O on the other copy. In addition to the on-premises ONTAP Mediator, beginning with ONTAP 9.17.1, you can install ONTAP Cloud Mediator to provide the same functionality in a cloud deployment. You can use ONTAP Mediator or ONTAP Cloud Mediator, but you cannot use both at the same time.

The Mediator plays a crucial role in SnapMirror active sync configurations as a passive quorum witness, ensuring quorum maintenance and facilitating data access during failures. It acts as a ping proxy for controllers to determine the liveliness of peer controllers. Although the Mediator does not actively trigger switchover operations, it provides a vital function by allowing the surviving node to check its partner’s status during network communication issues. In its role as a quorum witness, the ONTAP Mediator provides an alternate path (effectively serving as a proxy) to the peer cluster.

Furthermore, it allows clusters to get this information as part of the quorum process. It uses the node management LIF and cluster management LIF for communication purposes. It establishes redundant connections through multiple paths to differentiate between site failure and InterSwitch Link (ISL) failure. When a cluster loses connection with the Mediator software and all its nodes due to an event, it is considered not reachable. This triggers an alert and enables automated failover to the mirror consistency group in the secondary site, ensuring uninterrupted I/O for the client. The replication data path relies on a heartbeat mechanism, and if a network glitch or event persists beyond a certain period, it can result in heartbeat failures, causing the relationship to go out-of-sync. However, the presence of redundant paths, such as LIF failover to another port, can sustain the heartbeat and prevent such disruptions.

ONTAP Mediator

ONTAP Mediator is installed in a third failure domain, distinct from the two ONTAP clusters it monitors. There are three key components in this setup:

- Primary ONTAP cluster hosting the SnapMirror active sync primary consistency group
- Secondary ONTAP cluster hosting the mirror consistency group
- ONTAP Mediator

ONTAP Mediator is used for the following purposes:

- Establish a quorum
- Continuous availability via automatic failover (AUFO)
- Planned failovers (PFO)

> ⓘ ONTAP Mediator 1.7 can manage ten cluster pairs for business continuity.

> ⓘ When the ONTAP Mediator is not available, you cannot perform planned or automated failovers. The application data continues to synchronously replicate without any interruption for zero data loss.

ONTAP Cloud Mediator

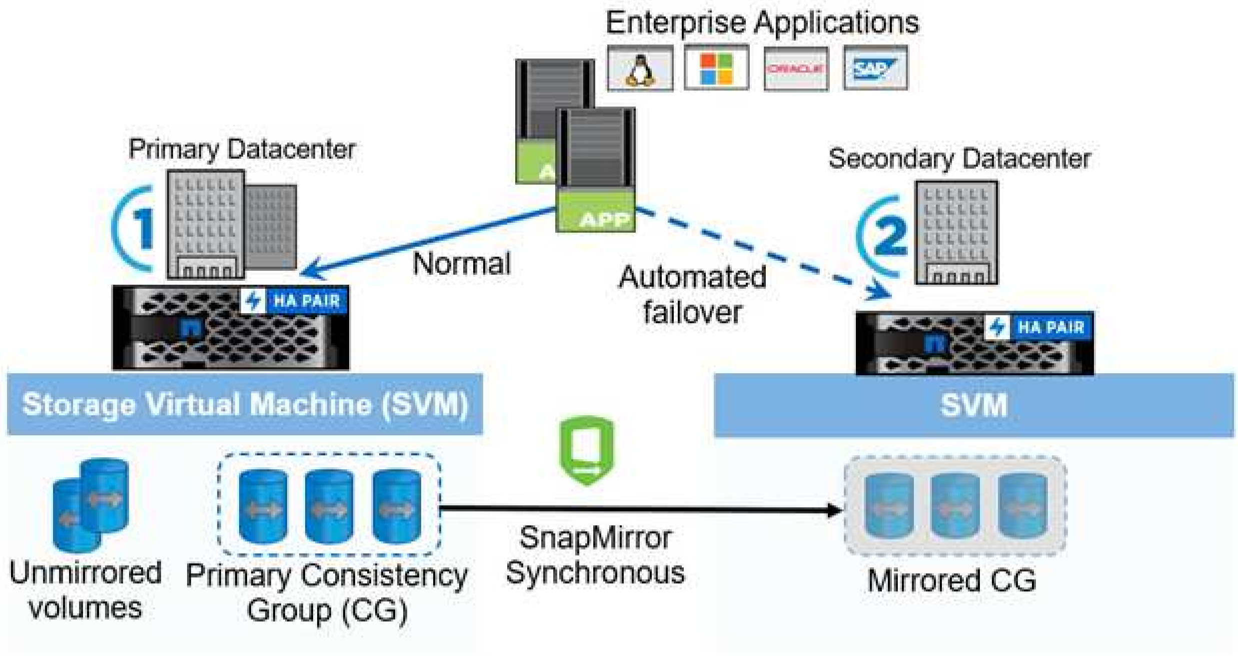
Beginning with ONTAP 9.17.1, ONTAP Cloud Mediator is available as a cloud-based service in the NetApp Console for use with SnapMirror active sync. Similar to ONTAP Mediator, ONTAP Cloud Mediator provides the following functionality in a SnapMirror active sync relationship:

- Provides a persistent and fenced store for HA or SnapMirror active sync metadata.
- Serves as a ping proxy for controller liveliness.
- Provides synchronous node health query functionality to aid in quorum determination.

The ONTAP Cloud Mediator helps simplify SnapMirror active sync deployment by using the NetApp Console cloud service as a third site that you do not need to manage. The ONTAP Cloud Mediator service provides the same functionality as the on-premises ONTAP Mediator; however, ONTAP Cloud Mediator reduces the operational complexity of maintaining a third site. In contrast, ONTAP Mediator is available as a package and must be installed on a Linux host running at a third site with independent power and network infrastructure for its operations.

SnapMirror active sync operation workflow

The following figure illustrates the design of SnapMirror active sync at a high level.



The diagram shows an enterprise application that is hosted on an storage VM (SVM) at the primary data center. The SVM contains five volumes, three of which are part of a consistency group. The three volumes in the consistency group are mirrored to a secondary data center. In normal circumstances, all write operations are performed to the primary data center; in effect, this data center serves as the source for I/O operations, while the secondary data center serves as a destination.

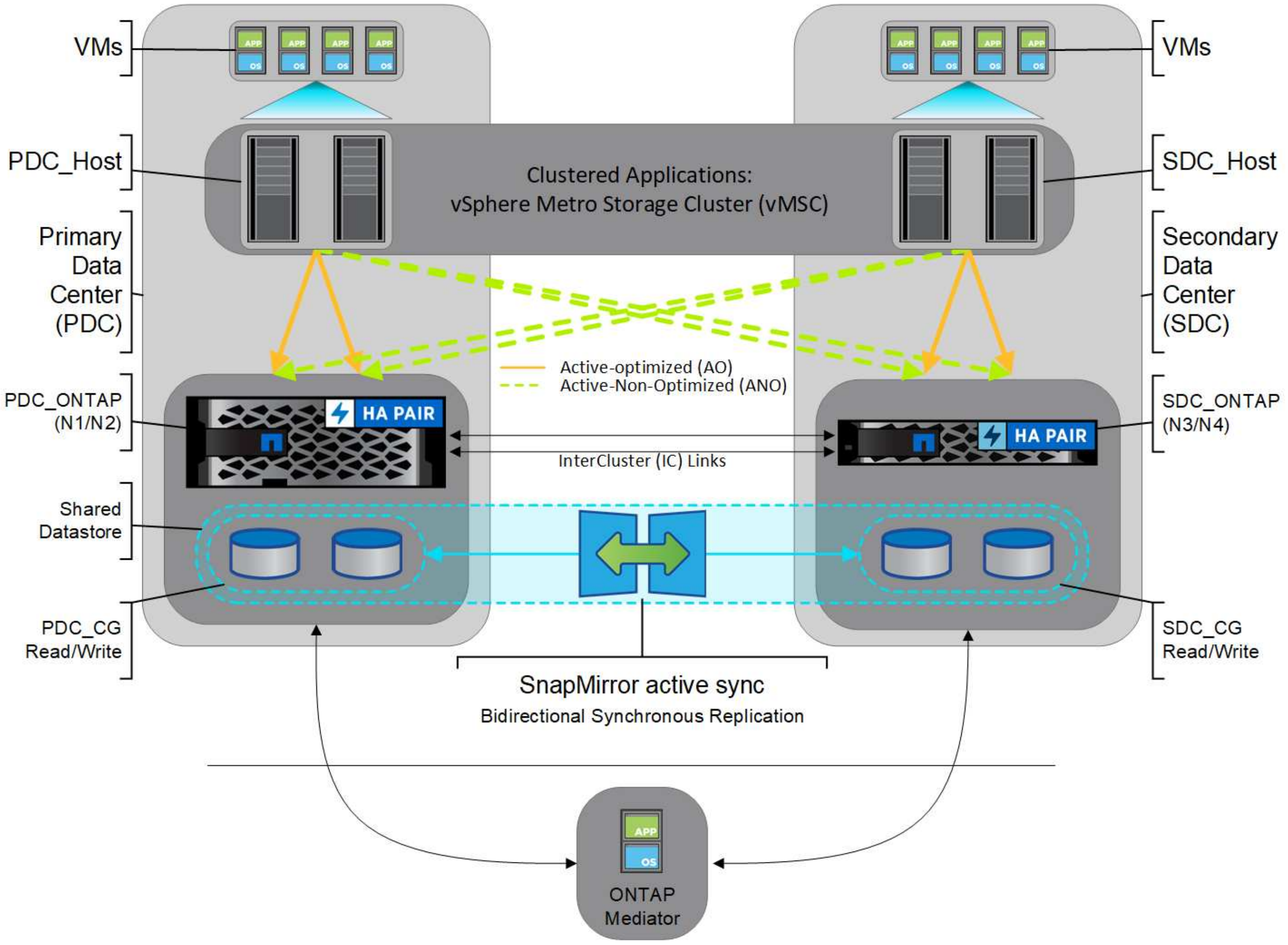
In the event of a disaster scenario at the primary data center, ONTAP directs the secondary data center to act as the primary, serving all I/O operations. Only the volumes that are mirrored in the consistency group are served. Any operations pertaining to the other two volumes on the SVM is affected by the disaster event.

Symmetric active/active

SnapMirror active sync offers asymmetric and symmetric solutions.

In *asymmetric configurations*, the primary storage copy exposes an active-optimized path and actively serves client I/O. The secondary site uses a remote path for I/O. The storage paths for the secondary site are considered active-non-optimized. Access to the write LUN is proxied from the secondary site. NVMe protocol is not supported in asymmetric configurations.

In *symmetric active/active configurations*, active-optimized paths are exposed on both sites, are host specific, and are configurable, meaning hosts on either side are able to access local storage for active I/O. Beginning with ONTAP 9.16.1, symmetric active/active is supported on clusters with up to four nodes. Beginning with ONTAP 9.17.1, symmetric active/active configurations support NVMe protocol on two node clusters.



Symmetric active/active is targeted for clustered applications including VMware Metro Storage Cluster, Oracle RAC, and Windows Failover Clustering with SQL.

Use cases for ONTAP SnapMirror active sync

The demands of a globally connected business environment demand rapid recovery of business-critical application data with zero data loss in the event of a disruption such as a cyber-attack, power outage, or natural disaster. These demands are heightened in arenas such as finance and those adhering to regulatory mandates such as the General Data Protection Regulation (GDPR).

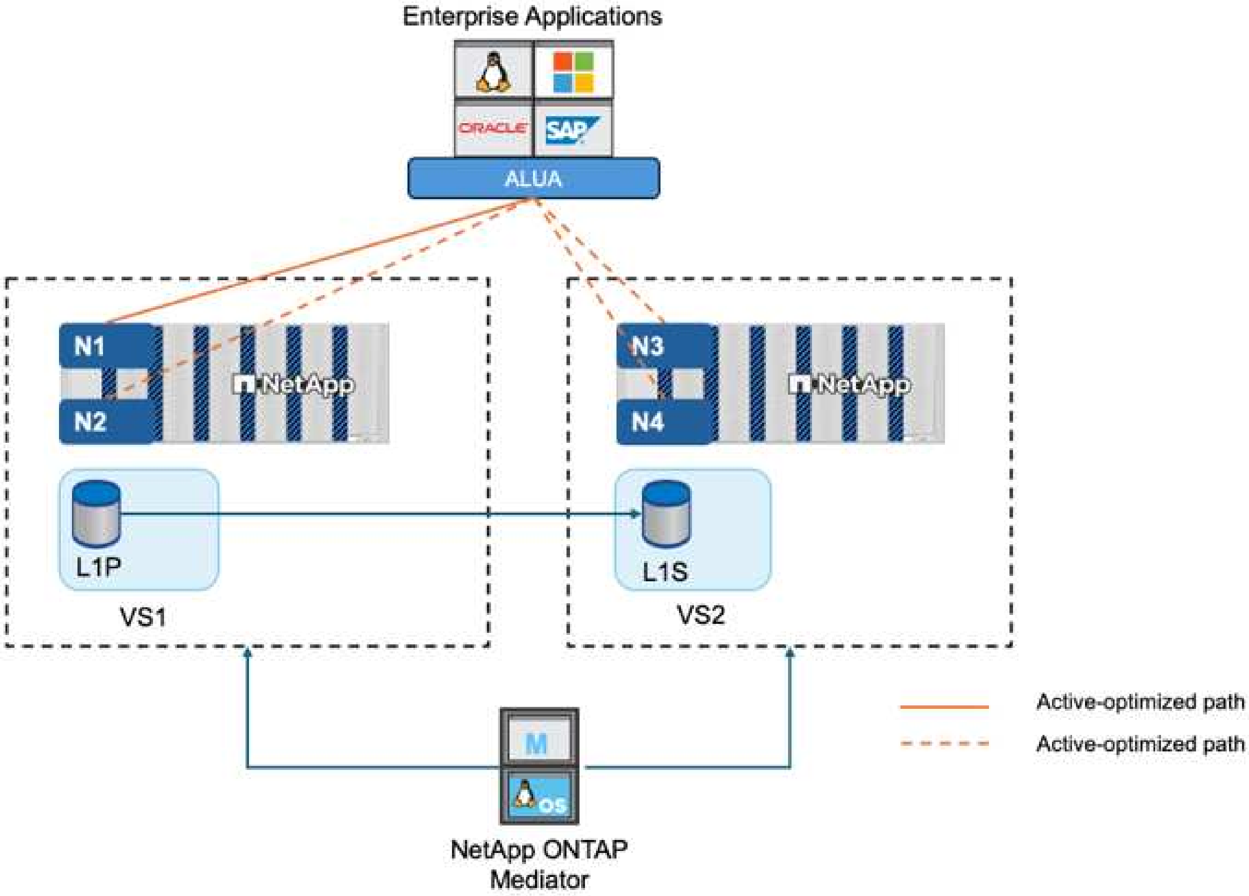
SnapMirror active sync provides the following use cases:

Application deployment for zero recovery time objective (RTO)

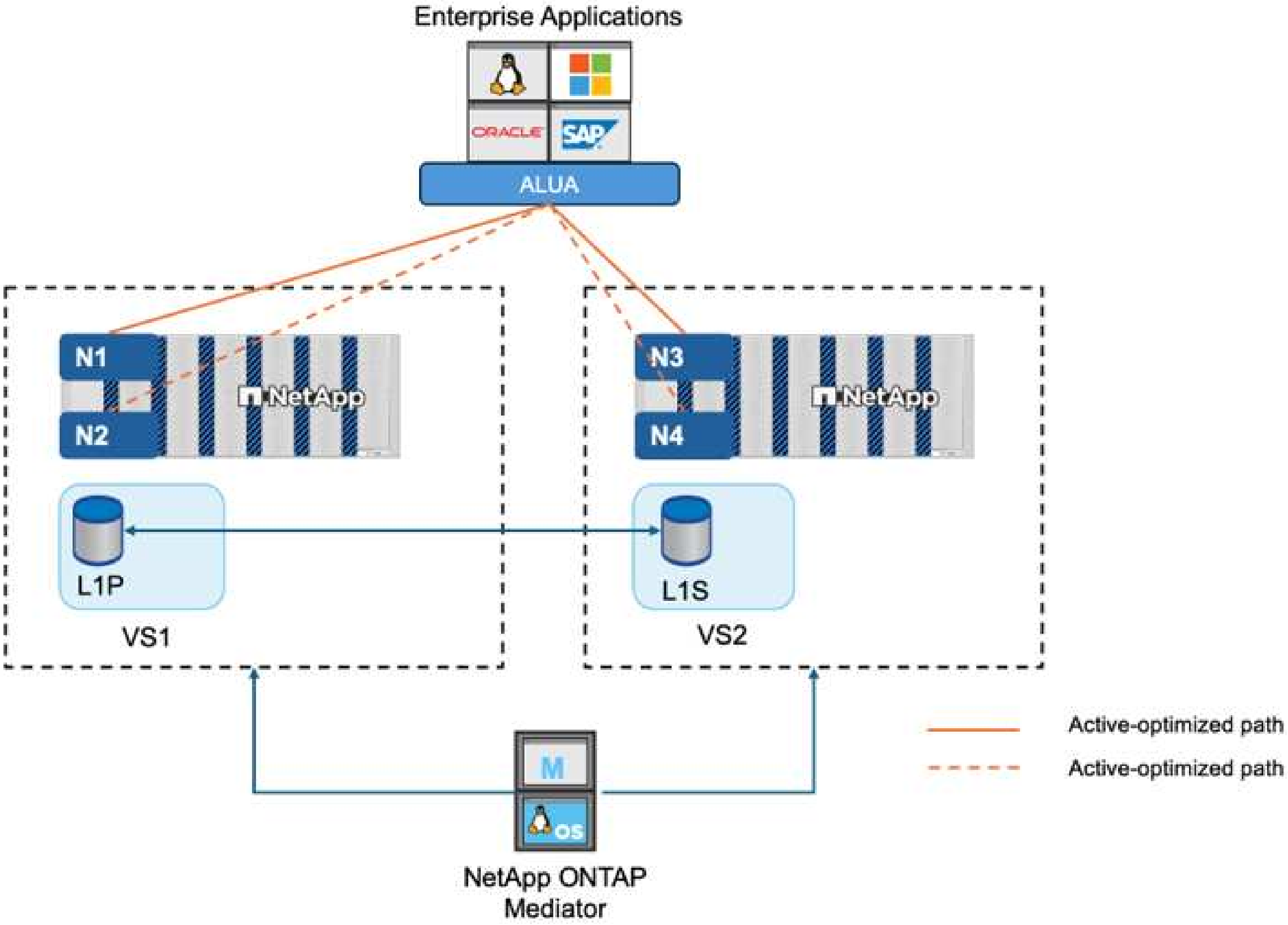
In a SnapMirror active sync deployment, you have a primary and secondary cluster. A LUN in the primary cluster (`L1P`) has a mirror (`L1S`) on the secondary; both LUNs share the same serial ID and are reported as read-write LUNs to the host. In asymmetric configurations read and write operations, however, are only serviced to the primary LUN, `L1P`. Any writes to the mirror `L1S` are served by proxy.

Application deployment for zero RTO or transparent application failover (TAF)

TAF is based on host MPIO software-based path failover to achieve non-disruptive access to the storage. Both LUN copies—for example, primary (L1P) and mirror copy (L1S)--have the same identity (serial number) and are reported as read-writable to the host. In asymmetric configurations however, reads and writes are serviced only by the primary volume. I/Os issued to the mirror copy are proxied to the primary copy. The host's preferred path to L1 is VS1:N1 based on asymmetric logical unit access (ALUA) access state Active Optimized (A/O). ONTAP Mediator is required as part of the deployment, primarily to perform failover (planned or unplanned) in the event of a storage outage on the primary.



TAF operates in two modes: Automated Failover and Automated Failover Duplex. With Automated Failover, reads and writes are serviced only by the primary volume, therefore, IOs issued to the mirror copy (which cannot service writes on its own) are proxied to the primary copy. With Automated Failover Duplex, both the primary and secondary copies can service IOs so no proxy is necessary.



If you are using NVMe for host access with ONTAP 9.17.1, only the AutomatedFailoverDuplex policy is supported.

SnapMirror active sync uses ALUA, a mechanism that allows an application host multipathing software with paths advertised with priorities and access availability for the application host communication with the storage array. ALUA marks active optimized paths to the controllers owning the LUN and others as active non-optimized paths, used only if the primary path fails.

SnapMirror active sync with NVMe protocol uses Asymmetric Namespace Access (ANA), which enables application hosts to discover optimized and non-optimized paths to NVMe namespaces that are being protected. The ONTAP NVMe target publishes the appropriate path states to enable application hosts to use the optimal path for a protected NVMe namespace.

Clustered applications

Clustered applications, including VMware Metro Storage Cluster, Oracle RAC, and Windows Failover Clustering with SQL, require simultaneous access so the VMs can be failed over to other site without any performance overhead. SnapMirror active sync symmetric active/active serves IO locally with bidirectional replication to meet the requirements of clustered applications. Beginning with ONTAP 9.16.1, symmetric active/active is supported in a configuration in four-node clusters, expanding from the two-node cluster limit in ONTAP 9.15.1.

Disaster scenario

Synchronously replicate multiple volumes for an application between sites at geographically dispersed locations. You can automatically failover to the secondary copy in case of disruption of the primary, thus enabling business continuity for tier one applications. When the site hosting the primary cluster experiences a disaster, the host multipathing software marks all paths through the cluster as down and uses paths from the secondary cluster. The result is a non-disruptive failover enabled by ONTAP Mediator to the mirror copy.

Extended application support

SnapMirror active sync provides flexibility with easy-to-use application-level granularity and automatic failover. SnapMirror active sync uses proven SnapMirror synchronous replication over an IP network to replicate data at high speeds over LAN or WAN, to achieve high data availability and fast data replication for your business-critical applications such as Oracle, Microsoft SQL Server, and so on, in both virtual and physical environments.

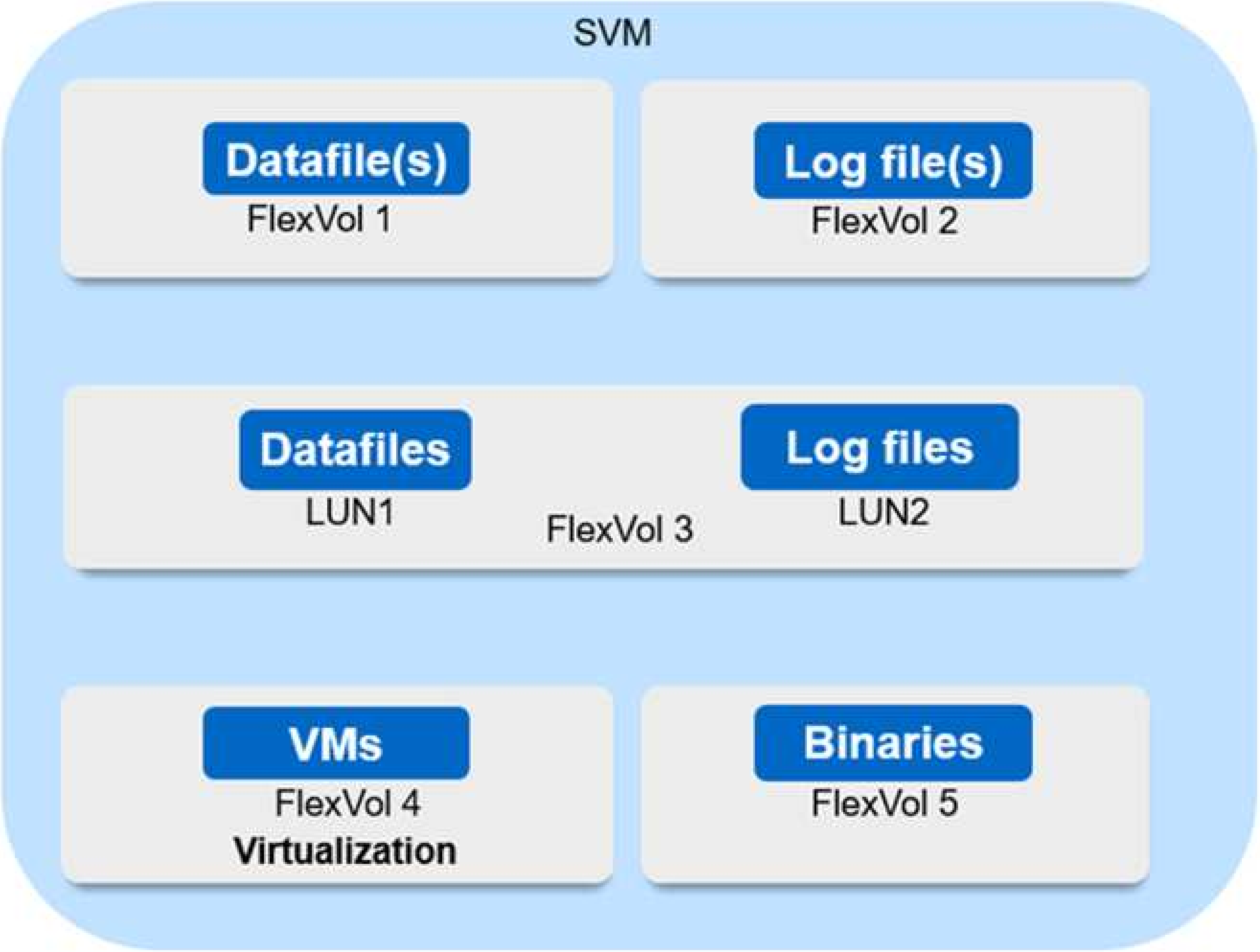
SnapMirror active sync enables mission-critical business services to continue operating even through a complete site failure, with TAF to the secondary copy. No manual intervention or additional scripting is required to trigger this failover.

Deployment strategy and best practices for ONTAP SnapMirror active sync

It is important that your data protection strategy clearly identifies the workloads that need to be protected for business continuity. The most critical step in your data protection strategy is to have clarity in your enterprise application data layout so that you can decide how you are distributing the volumes and protecting business continuity. Because failover occurs at the consistency group level on a per-application basis, make sure to add the necessary data volumes to the consistency group.

SVM configuration

The diagram captures a recommended storage VM (SVM) configuration for SnapMirror active sync.



- For data volumes:
  - Random read workloads are isolated from sequential writes; therefore, depending on the database size, the data and log files are typically placed on separate volumes.
    - For large critical databases, the single data file is on FlexVol 1 and its corresponding log file is on FlexVol 2.
    - For better consolidation, small-to-medium-size noncritical databases are grouped such that all the data files are on FlexVol 1 and their corresponding log files are on FlexVol 2. However, you will lose application-level granularity through this grouping.
  - Another variant is to have all the files within the same FlexVol 3, with data files in LUN1 and its log files in LUN 2.
- If your environment is virtualized, you would have all the VMs for various enterprise applications shared in a datastore. Typically, the VMs and application binaries are asynchronously replicated using SnapMirror.

Plan

Prerequisites for ONTAP SnapMirror active sync

When planning your SnapMirror active sync deployment, ensure you have met the various hardware, software, and system configuration requirements.

Hardware

The following table outlines the supported NetApp cluster configurations.

Cluster type	Supported models	Supported features	Maximum supported cluster nodes
AFF	A-Series, C-Series	Automated Failover Duplex (Symmetric Active/Active), Automated Failover (Asymmetric Active/Active)	• 2 (ONTAP 9.9.1 or later) • 4 (ONTAP 9.16.1 with Symmetric Active/Active configurations)
ASA	A-Series, C-Series	Automated Failover Duplex (Symmetric Active/Active), Automated Failover (Asymmetric Active/Active)	• 2 (ONTAP 9.9.1 or later • 4 (ONTAP 9.16.1 with Symmetric Active/Active configurations)
ASA r2	All	Automated Failover Duplex (Symmetric Active/Active)	• 2 (ONTAP 9.17.1 or earlier) • 4 (ONTAP 9.18.1 or later)

The table below outlines the capability for replication between cluster types.

Cluster type 1	Cluster type 2	Replication supported?
AFF A-Series	AFF C-Series	Yes
ASA r2 A-Series	ASA r2 C-Series	Yes
AFF	ASA	No
ASA	ASA r2	No
ASA r2	ASA r2	Yes

Software

- ONTAP 9.9.1 or later
- ONTAP Mediator 1.2 or later
- A Linux server or virtual machine for ONTAP Mediator running one of the following:

ONTAP Mediator version	Supported Linux versions

1.11	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recommended: 10.1, 10.0, 9.7, 9.6, 9.4, and 8.10 • Rocky Linux 10.1, 9.7, and 8.10 • Oracle Linux 10.0 and 9.6
1.10	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recommended: 10.0, 9.6, 9.4, and 8.10 • Rocky Linux 10.0, 9.6, and 8.10
1.9.1	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8 • Rocky Linux 9.5 and 8.10
1.9	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8 • Rocky Linux 9.5 and 8.10
1.8	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, and 8.8 • Rocky Linux 9.4 and 8.10
1.7	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.3, 9.2, 9.1, 9.0, 8.9, and 8.8 • Rocky Linux 9.3 and 8.9
1.6	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.2, 9.1, 9.0, and 8.8 • Rocky Linux 9.2 and 8.8
1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6

1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6

1. Compatible means that Red Hat no longer supports these RHEL versions, but ONTAP Mediator can still be installed on them.

Licensing

The following SnapMirror licenses are available as part of the ONTAP One license suite and must be applied on both clusters:

- SnapMirror synchronous
- SnapMirror

> If your ONTAP storage systems were purchased before June 2019, see ONTAP Master License Keys to get the required SnapMirror synchronous license.

- For vSphere Metro Storage Cluster (vMSC), a VMware vSphere license is required.

Networking environment

- Inter-cluster latency round trip time (RTT) must be less than 10 milliseconds.
- Beginning with ONTAP 9.14.1, SCSI-3 persistent reservations are supported with SnapMirror active sync.

Supported protocols

SnapMirror active sync supports SAN protocols.

- The FC and iSCSI protocols are supported beginning with ONTAP 9.9.1.
- The NVMe protocol is supported with VMware workloads beginning with ONTAP 9.17.1.

  SnapMirror active sync does not support the following with the NVMe protocol:

  - 4-node symmetric active/active configurations
  - Asymmetric active/active configurations
  - Changes in consistency group size

    You cannot expand or shrink a consistency group non-disruptively when using the NVMe protocol with SnapMirror active sync. Consistency group expansion and shrink operations are disruptive when using the NVMe protocol with SnapMirror active sync.

  - Coexistence of LUNs and namespaces in the same consistency group.

IPspace

The default IPspace is required by SnapMirror active sync for cluster peer relationships. Custom IPspaces are not supported.

NTFS Security Style

NTFS security style is **not** supported on SnapMirror active sync volumes.

ONTAP Mediator

- ONTAP Mediator must be provisioned externally and attached to ONTAP for transparent application failover.
- To be fully functional and to enable automatic unplanned failover, the external ONTAP Mediator should be provisioned and configured with ONTAP clusters.
- ONTAP Mediator must be installed in a third failure domain, separate from the two ONTAP clusters.
- When installing ONTAP Mediator, you should replace the self-signed certificate with a valid certificate signed by a mainstream reliable CA.
- For more information about ONTAP Mediator, see Prepare to install ONTAP Mediator.

Other prerequisites

- In releases earlier than ONTAP 9.15.1, SnapMirror active sync relationships are not supported on read-write destination volumes volumes (volumes converted to read-write from DP in an asymmetric active-active). Before you can use a read-write volume, you must convert it to a DP volume by creating a volume-level SnapMirror relationship (either async or sync) and then deleting the relationship. For details, see Convert an existing SnapMirror relationships to SnapMirror active sync.
- Storage VMs using SnapMirror active sync cannot be joined to Active Directory as a client computer.

Further information

- Hardware Universe
- ONTAP Mediator overview

ONTAP SnapMirror active sync interoperability

SnapMirror active sync is compatible with numerous operating systems, application hosts, and other features in ONTAP.

> ⓘ For specific supportability and interoperability details not covered here, consult the Interoperability Matrix Tool (IMT).

Application hosts

SnapMirror active sync supports hypervisors including Hyper-V, ESXi, operating systems like Red Hat Enterprise Linux (RHEL), Windows Server, and clustering solutions such as vSphere Metro Storage Cluster (vMSC), and, beginning with ONTAP 9.14.1, Windows Server Failover Cluster.

Operating systems

SnapMirror active sync is supported with numerous operating systems, including:

- AIX via PVR (beginning ONTAP 9.11.1)
- HP-UX (beginning ONTAP 9.10.1)
- Solaris 11.4 (beginning ONTAP 9.10.1)

AIX

Beginning with ONTAP 9.11.1, AIX is supported with SnapMirror active sync via standard engineering Feature Policy Variance Request (FPVR) with the agreement that the following stipulations are understood:

- SnapMirror active sync can provide zero RPO data protection, but the failover process with AIX requires additional steps to recognize the path change. LUNs that are not part of a root volume group will experience an I/O pause until a `cfgmgr` command is run. This can be automated, and most applications will resume operations without further disruption.
- LUNs that are part of a root volume group should generally not be protected with SnapMirror active sync. It's not possible to run the `cfgmgr` command after a failover, meaning that a reboot is required to recognize the changes in SAN paths. You can still achieve zero RPO data protection of the root volume group, but failover will be disruptive.

Consult your NetApp account team for further information about SnapMirror active sync with AIX.

HP-UX

Beginning with ONTAP 9.10.1, SnapMirror active sync for HP-UX is supported.

Automatic unplanned failover with HP-UX

An automatic unplanned failover (AUFO) event on the isolated master cluster may be caused by dual event failure when the connection between the primary and the secondary cluster is lost, and the connection between the primary cluster and the mediator is also lost. This is considered a rare event, unlike other AUFO events.

- In this scenario, it might take more than 120 seconds for I/O to resume on the HP-UX host. Depending on the applications that are running, this might not lead to any I/O disruption or error messages.
- To remediate, you must restart applications on the HP-UX host that have a disruption tolerance of less than 120 seconds.

Solaris

Beginning with ONTAP 9.10.1, SnapMirror active sync supports Solaris 11.4.

To ensure the Solaris client applications are non-disruptive when an unplanned site failover switchover occurs in an SnapMirror active sync environment, modify the default Solaris OS settings. To configure Solaris with the recommended settings, see the NetApp Knowledge Base: Solaris Host support recommended settings in SnapMirror active sync.

ONTAP interoperability

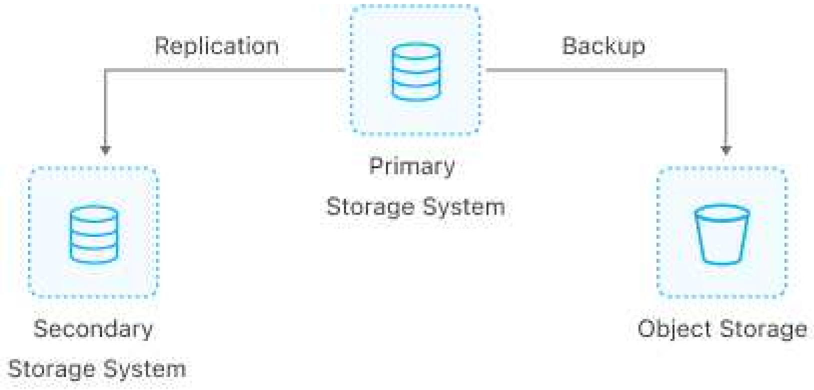
SnapMirror active sync integrates with components of ONTAP to extends its data protection capabilities.

FabricPool

SnapMirror active sync supports source and destination volumes on FabricPool aggregates with tiering policies of None, Snapshot or Auto. SnapMirror active sync does not support FabricPool aggregates using a tiering policy of All.

Fan-out configurations

In fan-out configurations, your source volume can be mirrored to a SnapMirror active sync destination endpoint and to one SnapMirror asynchronous relationship.



SnapMirror active sync supports fan-out configurations with the `MirrorAllSnapshots` policy and, beginning with ONTAP 9.11.1, the `MirrorAndVault` policy. Fan-out configurations are not supported in SnapMirror active sync with the `XDPDefault` policy.

Beginning with ONTAP 9.15.1, SnapMirror active sync supports automatic reconfiguration in the fan-out leg after a failover event. If the failover from the primary to the secondary site has succeeded, the tertiary site is automatically reconfigured to treat the secondary site as the source. The async fan-out leg can be a consistency group relationship or an independent volume relationship. The reconfiguration will work for either of the cases. Reconfiguration is triggered by either a planned or unplanned failover. Reconfiguration also occurs upon failback to the primary site.

For information about managing your fan-out configuration in earlier releases of ONTAP, see resume protection in the fan-out configuration.

NDMP restore

Beginning with ONTAP 9.13.1, you can use NDMP to copy and restore data with SnapMirror active sync. Using NDMP allows you to move data onto the SnapMirror active sync source to complete a restore without pausing protection. This is particularly useful in fan-out configurations.

SnapCenter

SnapMirror active sync is supported with SnapCenter beginning with SnapCenter 5.0. SnapCenter enables the creation of snapshots that can be used to protect and recover applications and virtual machines, enabling always available storage solutions with application-level granularity.

SnapRestore

SnapMirror active sync supports partial and single file SnapRestore.

Single file SnapRestore

Beginning with ONTAP 9.11.1, single-file SnapRestore is supported for SnapMirror active sync volumes. You can restore a single file from a snapshot replicated from the SnapMirror active sync source to the destination. Because volumes can contain one or more LUNs, this feature helps you implement a less disruptive restore operation, granularly restoring a single LUN without disrupting the other LUNs. Single File SnapRestore has two options: in-place and out-of-place.

Partial file SnapRestore

Beginning in ONTAP 9.12.1, partial LUN restore is supported for SnapMirror active sync volumes. You can restore a data from application-created snapshots that have been replicated between the SnapMirror active sync source (volume) and the destination (snapshot) volumes. Partial LUN or file restore may be necessary if you need to restore a database on a host that stores multiple databases on the same LUN. Using this functionality requires you to know the starting byte offset of the data and byte count.

Large LUNs and large volumes

Support for large LUNs and large volumes (greater than 100 TB) depends on the version of ONTAP you are using and your platform.

ONTAP 9.12.1P2 and later

- For ONTAP 9.12.1 P2 and later, SnapMirror active sync supports Large LUNs and large volumes greater than 100 TB on ASA and AFF (A-Series and C-Series). Primary and secondary clusters must be of the same type: either ASA or AFF. Replication from AFF A-Series to AFF C-Series and vice versa is supported.

> ⓘ For ONTAP Releases 9.12.1P2 and later, you must ensure that both the primary and secondary clusters are either All-Flash SAN Arrays (ASA) or All Flash Array (AFF), and that they both have ONTAP 9.12.1 P2 or later installed. If the secondary cluster is running a version earlier than ONTAP 9.12.1P2 or if the array type is not the same as primary cluster, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

ONTAP 9.9.1 - 9.12.1P1

- For ONTAP releases between ONTAP 9.9.1 and 9.12.1 P1 (inclusive), Large LUNs and large volumes greater than 100TB are supported only on All-Flash SAN Arrays. Replication from AFF A-Series to AFF C-Series and vice versa is supported.

> ⓘ For ONTAP releases between ONTAP 9.9.1 and 9.12.1 P2, you must ensure that both the primary and secondary clusters are All-Flash SAN Arrays, and that they both have ONTAP 9.9.1 or later installed. If the secondary cluster is running a version earlier than ONTAP 9.9.1 or if it is not an All-Flash SAN Array, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

More information

- How to configure an AIX host for SnapMirror active sync

Object limits for ONTAP SnapMirror active sync

When preparing to use SnapMirror active sync, be aware of the following object limits.

Consistency groups in a cluster

Consistency group limits for a cluster with SnapMirror active sync are calculated based on relationships and depend on the version of ONTAP used. Limits are platform-independent.

ONTAP version	Maximum number of relationships
ONTAP 9.11.1 and later	50*
ONTAP 9.10.1	20
ONTAP 9.9.1	5

* Beginning with ONTAP 9.16.1, SnapMirror active sync supports four-node clusters in symmetric active/active configurations. In a four-node cluster, 100 consistency groups are supported.

Volumes per consistency group

The maximum number of volumes per consistency group with SnapMirror active sync is platform independent.

ONTAP version	Maximum number of volumes supported in a consistency group relationship
ONTAP 9.15.1 and later	80
ONTAP 9.10.1-9.14.1	16
ONTAP 9.9.1	12

Volumes

Volume limits in SnapMirror active sync are calculated based on the number of endpoints, not the number of relationships. A consistency group with 12 volumes contributes 12 endpoints on both the primary and secondary cluster. Both SnapMirror active sync and SnapMirror synchronous relationships contribute to the total number of endpoints.

These limits apply to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, or ASA A20), see ASA r2 documentation.

The maximum endpoints per platform are included in the following table.

Platform	Endpoints per HA for SnapMirror active sync			Overall sync and SnapMirror active sync endpoints per HA		
	ONTAP 9.11.1 and later	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 and later	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400*	200	60	400	200	80
ASA	400*	200	60	400	200	80

* Beginning with ONTAP 9.16.1, SnapMirror active sync supports four-node clusters in symmetric active/active configurations. The total limit for a four-node cluster is 800 endpoints.

SAN object limits

SAN object limits are included in the following table. The limits apply regardless of the platform.

Object in a SnapMirror active sync relationship	Count
LUNs per volume	• 256 (ONTAP 9.9.1 - ONTAP 9.15.0) • 512 (ONTAP 9.15.1 and later)
Number of unique LUNs, namespaces, or storage units per 2 x 2 SnapMirror active sync solution	4,096
Number of unique LUNs, namespaces, or storage units per 4 x 4 SnapMirror active-sync solution (available beginning with ONTAP 9.16.1)	6,144
LIFs per SVM (with at least one volume in a SnapMirror active sync relationship)	256
Inter-cluster LIFs per node	4
Inter-cluster LIFs per cluster	8

NVMe object limits

Beginning with ONTAP 9.17.1, SnapMirror active sync supports the NVMe protocol. NVMe object limits are included in the following table.

Maximum objects in a SnapMirror active sync relationship	Count
Number of namespace maps per node	4K
Cluster size	2 nodes
Number of consistency groups per HA pair	50
Number of volumes in a single NVMe SnapMirror active sync consistency group	80
Number of volumes in an HA pair	400
NVMe subsystems per consistency group	16
Namespace maps per consistency group	256

Related information

- Hardware Universe
- Consistency group limits

Configure

Configure ONTAP clusters for SnapMirror active sync

SnapMirror active sync uses peered clusters to protect your data in the event of a failover scenario. Before you configure ONTAP Mediator or ONTAP Cloud Mediator for

SnapMirror active sync, you must first ensure the cluster is configured correctly.

Before you begin

Before you configure ONTAP Mediator or ONTAP Cloud Mediator, you should confirm the following:

1. A cluster peering relationship exists between the clusters.

   > The default IPspace is required by SnapMirror active sync for cluster peer relationships. A custom IPspace isn't supported.

   Creating a cluster peer relationship

2. The SVMs are created on each cluster.

   Creating an SVM

3. A peer relationship exists between the SVMs on each cluster.

   Creating an SVM peering relationship

4. The volumes exist for your LUNs.

   Creating a volume

5. At least one SAN LIF (either FC or iSCSI as applicable) is created on each node in both clusters.

   Considerations for LIFs in a cluster SAN environment

   Creating a LIF

6. The necessary LUNs are created and mapped to an igroup, which is used to map LUNs to the initiator on the application host.

   Create LUNs and map igroups

7. The application host is re-scanned to discover any new LUNs.

Configure the ONTAP Mediator for SnapMirror active sync

SnapMirror active sync uses peered clusters to protect your data in the event of a failover scenario. ONTAP Mediator is a key resource that enables business continuity by monitoring the health of each cluster. To configure SnapMirror active sync, you must first install ONTAP Mediator and verify that your primary and secondary clusters are configured properly.

Once you have installed ONTAP Mediator and configured your clusters, initialize ONTAP Mediator for SnapMirror active sync using self-signed certificates. You must then create, initialize, and map the consistency group for SnapMirror active sync.

ONTAP Mediator

ONTAP Mediator provides a persistent and fenced store for high availability (HA) metadata used by the ONTAP clusters in a SnapMirror active sync relationship. Additionally, ONTAP Mediator provides a synchronous node health query functionality to aid in quorum determination and serves as a ping proxy for controller liveliness detection.

Each cluster peer relationship can only be associated with a single ONTAP Mediator instance. HA Mediator instances aren’t supported. When a cluster is in several peer relationships with other clusters, the following ONTAP Mediator options are available:

- If SnapMirror active sync is configured on each relationship, each cluster peer relationship can have its own unique ONTAP Mediator instance.
- The cluster can use the same ONTAP Mediator instance for all peer relationships.

For example, if cluster B has a peer relationship with cluster A, cluster C, and cluster D, all three cluster peer relationships can have a unique associated ONTAP Mediator instance when SnapMirror active sync is configured on each relationship. Alternatively, cluster B can use the same ONTAP Mediator instance for all three peer relationships. In this scenario, the same instance of ONTAP Mediator is listed three times for the cluster.

Beginning with ONTAP 9.17.1, you can configure ONTAP Cloud Mediator to monitor the health of your cluster in a SnapMirror active sync configuration, however, you cannot use both Mediators at the same time.

> ⓘ If you are using SnapMirror active sync and ONTAP Mediator or ONTAP Cloud Mediator with ONTAP 9.17.1, you should review the **Known problems and limitations** in the ONTAP Release Notes for important information about these configurations.

Prerequisites for ONTAP Mediator

- ONTAP Mediator includes its own set of prerequisites. You must meet these prerequisites before installing ONTAP Mediator.

  For more information, see Prepare to install the ONTAP Mediator service.

- By default, the ONTAP Mediator provides service through TCP port 31784. You should make sure that port 31784 is open and available between the ONTAP clusters and the ONTAP Mediator.

Install ONTAP Mediator and confirm cluster configuration

Perform each of the following steps to install ONTAP Mediator and verify the cluster configuration. For each step, you should confirm that the specific configuration has been performed. Each step includes a link to the specific procedure that you need to follow.

Steps

1. Install ONTAP Mediator before verifying that your source and destination clusters are configured correctly.

   Prepare to install or upgrade ONTAP Mediator

2. Confirm that a cluster peering relationship exists between the clusters.

   > ⓘ The default IPspace is required by SnapMirror active sync for cluster peer relationships. A custom IPspace isn’t supported.

   Configure ONTAP clusters for SnapMirror active sync

Initialize ONTAP Mediator for SnapMirror active sync using self-signed certificates

Once you have installed ONTAP Mediator and confirmed you cluster configuration, you must initialize ONTAP Mediator for cluster monitoring. You can initialize ONTAP Mediator using System Manager or the ONTAP CLI.

System Manager

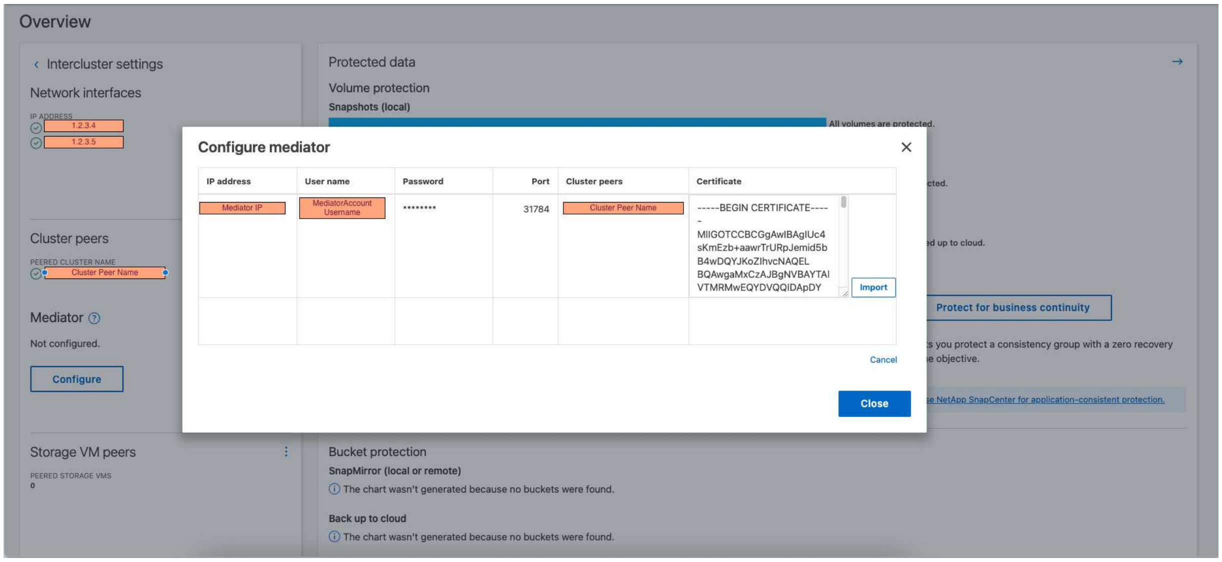
With System Manager, you can configure ONTAP Mediator for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

> ⓘ From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

ONTAP Mediator 1.9 and later

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Select **Add**, and enter the following ONTAP Mediator information:
   - IPv4 address
   - Username
   - Password
   - Certificate
3. You can provide the Certificate input in two ways:
   - **Option (a)**: Select **Import** to navigate to the `intermediate.crt` file and import it.
   - **Option (b)**: Copy the content of the `intermediate.crt` file and paste it in the **Certificate** field.

   When all details are entered correctly, the provided certificate is installed on all the peer clusters.

   Overview
   Intercluster settings
   Network interfaces
   IP ADDRESS
   1.2.3.4
   1.2.3.5
   Cluster peers
   PEERED CLUSTER NAME
   Cluster Peer Name
   Mediator
   Not configured.
   Configure
   Storage VM peers
   PEERED STORAGE VMS
   0
   Protected data
   Volume protection
   Snapshots (local)
   All volumes are protected.
   cted.
   ed up to cloud.
   Protect for business continuity
   s you protect a consistency group with a zero recovery
   e objective.
   e NetApp SnapCenter for application-consistent protection.
   Bucket protection
   SnapMirror (local or remote)
   The chart wasn't generated because no buckets were found.
   Back up to cloud
   The chart wasn't generated because no buckets were found.

   Configure mediator

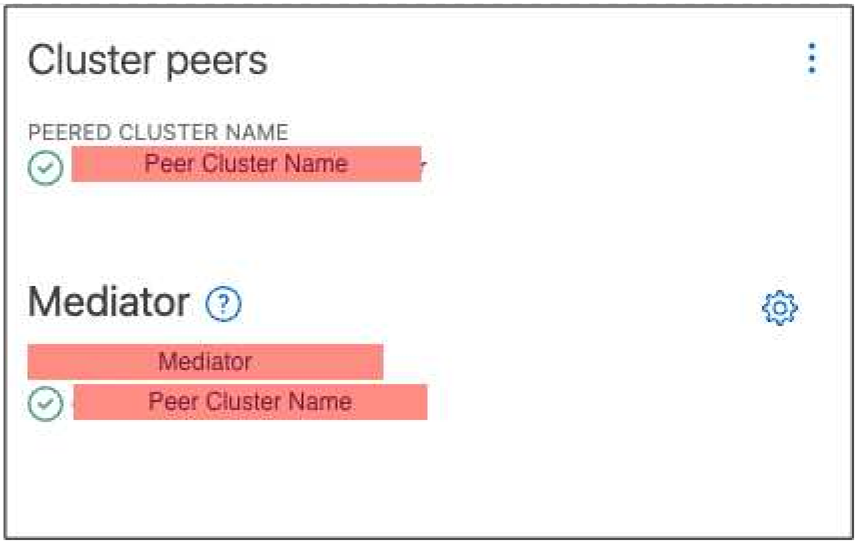
IP address	User name	Password	Port	Cluster peers	Certificate
Mediator IP	MediatorAccount Username	********	31784	Cluster Peer Name	-----BEGIN CERTIFICATE----- MIIGOTCCBCGgAwIBAgIUc4 sKmEzb+aawrTrURpJemid5b B4wDQYJKoZIhvcNAQEL BQAwgaMxCzAJBgNVBAYTAI VTMRMwEQYDVQQIDApDY Import

   Cancel

   Close

   When the certificate addition is complete, ONTAP Mediator is added to the ONTAP cluster.

   The following image demonstrates a successful ONTAP Mediator configuration:



Cluster peers

PEERED CLUSTER NAME

Peer Cluster Name

Mediator

Mediator

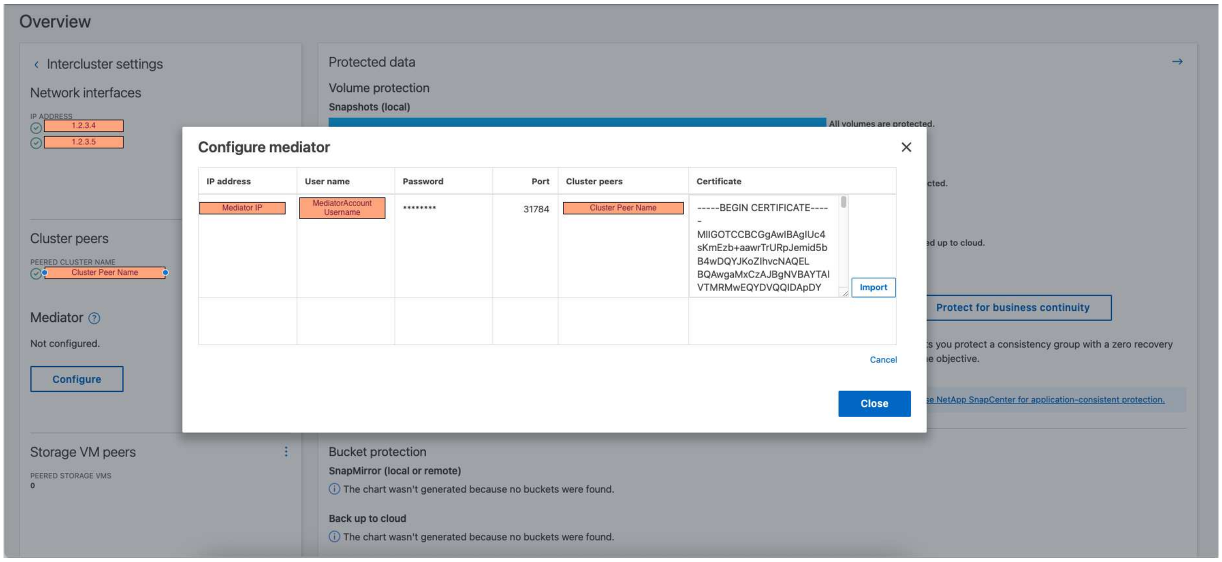
Peer Cluster Name

.

ONTAP Mediator 1.8 and earlier

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Select **Add**, and enter the following ONTAP Mediator information:
   - IPv4 address
   - Username
   - Password
   - Certificate
3. You can provide the Certificate input in two ways:
   - **Option (a)**: Select **Import** to navigate to the `ca.crt` file and import it.
   - **Option (b)**: Copy the content of the `ca.crt` file and paste it in the **Certificate** field.

     When all details are entered correctly, the provided certificate is installed on all the peer clusters.

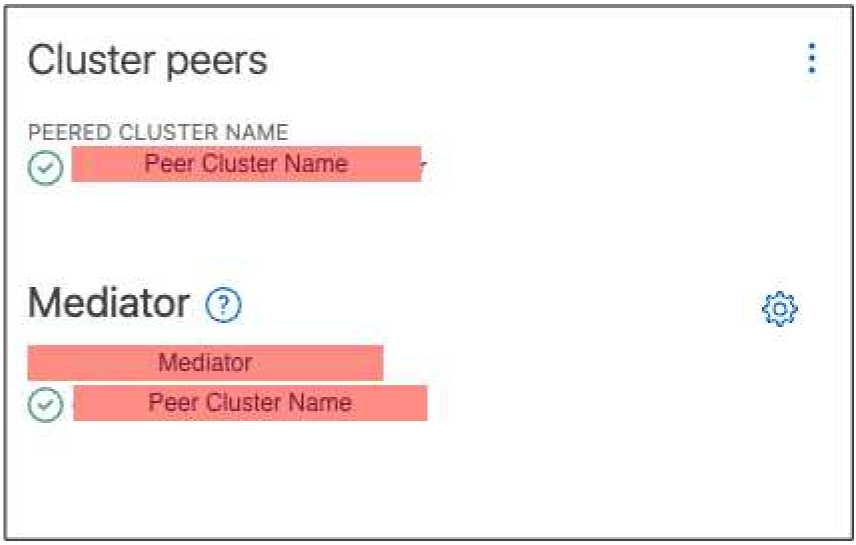


Configure mediator

IP address	User name	Password	Port	Cluster peers	Certificate
Mediator IP	MediatorAccount Username	********	31784	Cluster Peer Name	-----BEGIN CERTIFICATE----- MIIGOTCCBCGgAwIBAgIUc4 sKmEzb+aawrTrURpJemid5b B4wDQYJKoZIhvcNAQEL BQAwgaMxCzAJBgNVBAYTAI VTMRMwEQYDVQQIDApDY

When the certificate addition is complete, ONTAP Mediator is added to the ONTAP cluster.

The following image demonstrates a successful ONTAP Mediator configuration:



Cluster peers

PEERED CLUSTER NAME

Peer Cluster Name

Mediator

Mediator

Peer Cluster Name

CLI

You can initialize ONTAP Mediator from either the primary or secondary cluster using the ONTAP CLI. When you issue the `mediator add` command on one cluster, ONTAP Mediator is automatically added on the other cluster.

When using ONTAP Mediator to monitor a SnapMirror active sync relationship, ONTAP Mediator cannot be initialized in ONTAP without a valid self-signed or certificate authority (CA) certificate. You add a valid certificate to the certificate store for peered clusters. When using ONTAP Mediator to monitor MetroCluster IP systems, HTTPS isn’t used after the initial configuration; therefore, certificates aren’t required.

ONTAP Mediator 1.9 and later

1. Find the ONTAP Mediator CA certificate from the ONTAP Mediator Linux VM/host software installation location `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Add a valid certificate authority to the certificate store on the peered cluster.

   Example:

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Add the ONTAP Mediator CA certificate to an ONTAP cluster. When prompted, insert the CA certificate obtained from ONTAP Mediator. Repeat the steps on all of the peer clusters:

   `security certificate install -type server-ca -vserver <vserver_name>`

   Example:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. View the self-signed CA certificate installed using the generated name of the certificate:

   ```
   security certificate show -common-name <common_name>
   ```

   Example:

   ```
   C1_test_cluster::*> security certificate show -common-name
   ONTAPMediatorCA
   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- --------------------------------------
   ------------
   C1_test_cluster
              6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                              ONTAPMediatorCA
   server-ca
       Certificate Authority: ONTAP Mediator CA
             Expiration Date: Thu Feb 15 14:35:25 2029
   ```

5. Initialize ONTAP Mediator on one of the clusters. ONTAP Mediator is automatically added for the other cluster:

   ```
   snapmirror mediator add -mediator-address <ip_address> -peer-cluster
   <peer_cluster_name> -username user_name
   ```

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Optionally, check the job ID status `job show -id` to verify if the SnapMirror Mediator add command is successful.

   Example:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Check the status of the ONTAP Mediator configuration:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with ONTAP Mediator; a status of `true` indicates successful synchronization.

ONTAP Mediator 1.8 and earlier

1. Find the ONTAP Mediator CA certificate from the ONTAP Mediator Linux VM/host software installation location `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Add a valid certificate authority to the certificate store on the peered cluster.

   Example:

   ```
   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Add the ONTAP Mediator CA certificate to an ONTAP cluster. When prompted, insert the CA certificate obtained from the ONTAP Mediator. Repeat the steps on all of the peer clusters:

   `security certificate install -type server-ca -vserver <vserver_name>`

   Example:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. View the self-signed CA certificate installed using the generated name of the certificate:

   ```
   security certificate show -common-name <common_name>
   ```

   Example:

   ```
   C1_test_cluster::*> security certificate show -common-name
   ONTAPMediatorCA
   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- --------------------------------------
   ------------
   C1_test_cluster
              6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                              ONTAPMediatorCA
   server-ca
       Certificate Authority: ONTAP Mediator CA
             Expiration Date: Thu Feb 15 14:35:25 2029
   ```

5. Initialize ONTAP Mediator on one of the clusters. ONTAP Mediator is automatically added for the other cluster:

   ```
   snapmirror mediator add -mediator-address <ip_address> -peer-cluster
   <peer_cluster_name> -username user_name
   ```

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Optionally, check the job ID status `job show -id` to verify if the SnapMirror Mediator add command is successful.

   Example:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Check the status of the ONTAP Mediator configuration:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true
```

`Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with ONTAP Mediator; a status of `true` indicates successful synchronization.

Re-initialize ONTAP Mediator with third-party certificates

You might need to re-initialize ONTAP Mediator. There might be situations that require the re-initialization of ONTAP Mediator such as a change in the ONTAP Mediator IP address, certificate expiration, and so on.

The following procedure illustrates the re-initialization of ONTAP Mediator for a specific case when a self-signed certificate needs to be replaced by a third-party certificate.

About this task

You need to replace the SnapMirror active sync cluster’s self-signed certificates with third-party certificates, remove the ONTAP Mediator configuration from ONTAP, and then add ONTAP Mediator.

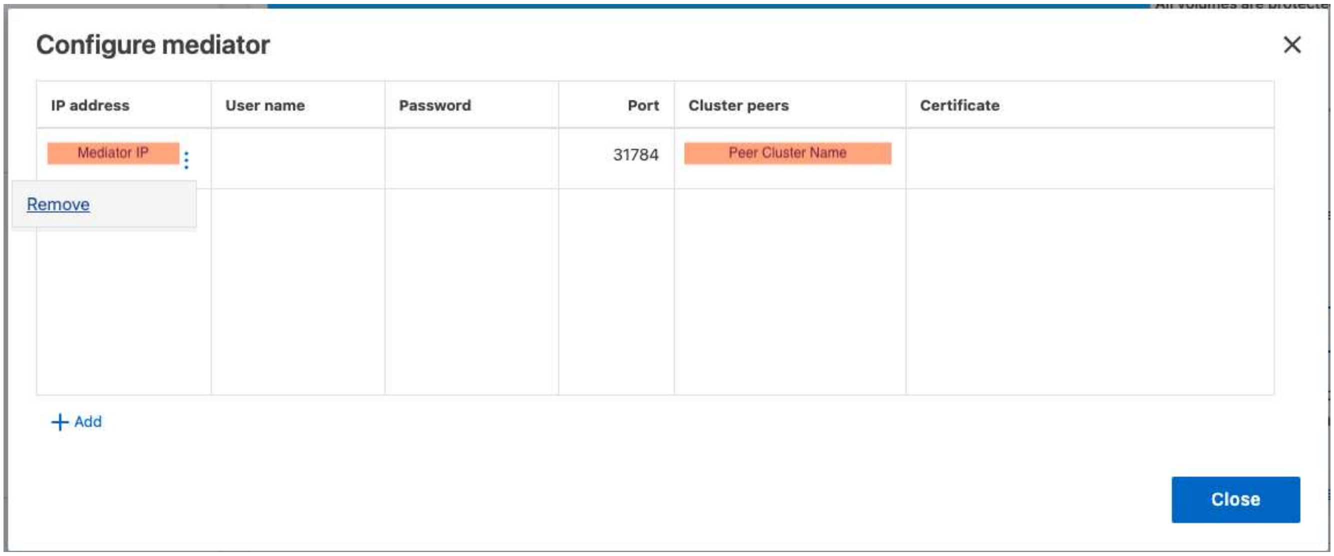
System Manager

With System Manager, you need to remove the ONTAP Mediator version configured with the old self-signed certificate from the ONTAP cluster and re-configure the ONTAP cluster with the new third-party certificate.

Steps

1. Select the menu options icon and select **Remove** to remove ONTAP Mediator.

> This step does not remove the self-signed server-ca from the ONTAP cluster. NetApp recommends navigating to the **Certificate** tab and removing it manually before performing the next step below to add a third-party certificate:

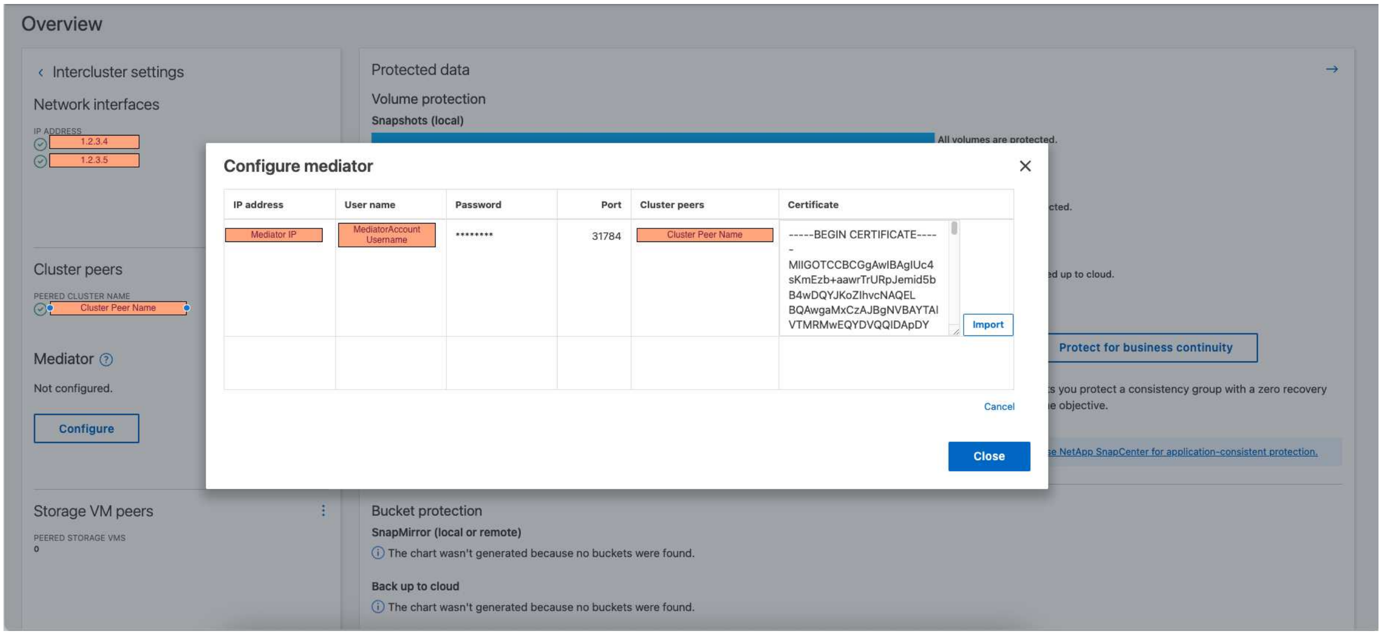


Configure mediator

IP address	User name	Password	Port	Cluster peers	Certificate
Mediator IP			31784	Peer Cluster Name	

2. Add ONTAP Mediator again with the correct certificate.

ONTAP Mediator is now configured with the new third-party self-signed certificate.



Configure mediator

IP address	User name	Password	Port	Cluster peers	Certificate
Mediator IP	MediatorAccount Username	********	31784	Cluster Peer Name	-----BEGIN CERTIFICATE----- MIIGOTCCBCGgAwIBAgIUc4 sKmEzb+aawrTrURpJemid5b B4wDQYJKoZIhvcNAQEL BQAwgaMxCzAJBgNVBAYTAI VTMRMwEQYDVQQIDApDY

CLI

You can re-initialize ONTAP Mediator from either the primary or secondary cluster by using the ONTAP CLI to replace the self-signed certificate with the third-party certificate.

ONTAP Mediator 1.9 and later

1. Remove the self-signed `intermediate.crt` installed earlier when you used self-signed certificates for all clusters. In the example below, there are two clusters:

   Example:

   ```
    C1_test_cluster::*> security certificate delete -vserver
   C1_test_cluster -common-name ONTAPMediatorCA
    2 entries were deleted.

    C2_test_cluster::*> security certificate delete -vserver
   C2_test_cluster -common-name ONTAPMediatorCA *
    2 entries were deleted.
   ```

2. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster using `-force true`:

   Example:

   ```
   C1_test_cluster::*> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   1.2.3.4          C2_test_cluster   connected         true

   C1_test_cluster::*> snapmirror mediator remove -mediator-address
   1.2.3.4 -peer-cluster C2_test_cluster -force true

   Warning: You are trying to remove the ONTAP Mediator configuration
   with force. If this configuration exists on the peer cluster, it
   could lead to failure of a SnapMirror failover operation. Check if
   this configuration
            exists on the peer cluster C2_test_cluster and remove it as
   well.
   Do you want to continue? {y|n}: y

   Info: [Job 136] 'mediator remove' job queued

   C1_test_cluster::*> snapmirror mediator show
   This table is currently empty.
   ```

3. Refer to the steps described in Replace self-signed certificates with trusted third-party certificates for instructions on how to obtain certificates from a subordinate CA, referred to as `intermediate.crt`. Replace self-signed certificates with trusted third-party certificates

The `intermediate.crt` has certain properties that it derives from the request that need to be sent to the PKI authority, defined in the file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Add the new third-party ONTAP Mediator CA certificate `intermediate.crt` from the ONTAP Mediator Linux VM/host software installation location:

   Example:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Add the `intermediate.crt` file to the peered cluster. Repeat this step for all peer clusters:

   Example:

   ```
   C1_test_cluster::*> security certificate install -type server-ca
   -vserver C1_test_cluster

   Please enter Certificate: Press when done
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----

   You should keep a copy of the CA-signed digital certificate for
   future reference.

   The installed certificate's CA and serial number for reference:
   CA: ONTAP Mediator CA
   serial: D86D8E4E87142XXX

   The certificate's generated name for reference: ONTAPMediatorCA

   C1_test_cluster::*>
   ```

6. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster:

   Example:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Add ONTAP Mediator again:

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with the mediator; a status of `true` indicates successful synchronization.

ONTAP Mediator 1.8 and earlier

1. Remove the self-signed `ca.crt` installed earlier when you used self-signed certificates for all clusters. In the example below, there are two clusters:

   Example:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster using `-force true`:

   Example:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Refer to the steps described in Replace self-signed certificates with trusted third-party certificates for instructions on how to obtain certificates from a subordinate CA, referred to as `ca.crt`.
   Replace self-signed certificates with trusted third-party certificates

   > ⓘ The `ca.crt` has certain properties that it derives from the request that need to be sent to the PKI authority, defined in the file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Add the new third-party ONTAP Mediator CA certificate `ca.crt` from the ONTAP Mediator Linux VM/host software installation location:

Example:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Add the `intermediate.crt` file to the peered cluster. Repeat this step for all peer clusters:

   Example:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster:

   Example:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Add ONTAP Mediator again:

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with the mediator; a status of `true` indicates successful synchronization.

Related information

- job show
- security certificate delete
- security certificate install
- security certificate show
- snapmirror mediator add
- snapmirror mediator remove
- snapmirror mediator show

Prepare to configure ONTAP Cloud Mediator

Before you configure ONTAP Cloud Mediator, you must ensure that the prerequisites are met.

Firewall requirements

The firewall setting on the domain controller must allow HTTPS traffic to `api.bluexp.netapp.com` from both clusters.

Proxy server requirements

If you use proxy servers for SnapMirror active sync, ensure the proxy servers are created and you have the following proxy server information:

- HTTPS proxy IP
- Port
- Username
- Password

Latency

The recommended ping latency between the NetApp Console cloud server and SnapMirror active sync cluster peers is less than 200 ms.

Root CA certificates

Check the cluster for certificates

ONTAP comes with well-known root CA certificates pre-installed so in most cases you do not need to install the NetApp Console server's root CA certificate. Before you begin the ONTAP Cloud Mediator configuration, you can check the cluster to verify that the certificates exist:

Example:

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
```

```
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- --------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

Check proxy server for installed certificates

If you are using a proxy to connect to the ONTAP Cloud Mediator service in the NetApp Console, ensure that the proxy server's root CA certificates are installed in ONTAP:

Example:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

Download the CA certificate:

If necessary, you can download the root-CA certificates from the certificate authority's website and install them on the clusters.

Example:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

Configure the ONTAP Cloud Mediator for SnapMirror active sync

Beginning with ONTAP 9.17.1, you can use ONTAP Cloud Mediator to enable business continuity by monitoring the health of each cluster. ONTAP Cloud Mediator is a cloud-based service. When you use ONTAP Cloud Mediator with SnapMirror active sync, you must first confirm that NetApp Console services and client information are configured and ensure proper cluster peering.

As with ONTAP Mediator, ONTAP Cloud Mediator provides a persistent and fenced store for high availability (HA) metadata used by the ONTAP clusters in a SnapMirror active sync relationship. ONTAP Cloud Mediator provides a synchronous node health query functionality to aid in quorum determination and serves as a ping proxy for controller liveliness detection.

> ⓘ If you are using SnapMirror active sync and ONTAP Mediator or ONTAP Cloud Mediator with ONTAP 9.17.1, you should review the **Known problems and limitations** in the ONTAP Release Notes for important information about these configurations.

Before you begin

Before you configure ONTAP Cloud Mediator, you should confirm the following information:

- The cluster is configured.

  Configure ONTAP clusters for SnapMirror active sync

- You have copied your NetApp Console organization ID from the NetApp Console and created a Console member service account to use when you configure ONTAP Cloud Mediator. When you create the service account, the organization must be set to the subscription where you configured the ONTAP Cloud

Mediator. The category must be set to **Application**, and the role type must be **ONTAP Mediator Setup Role**. You must save the client ID and client secret when you create the role.

Add NetApp Console members and service accounts

Steps

You can add ONTAP Cloud Mediator using System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Protection > Overview > Mediator** and select **Add**.
2. In the **Add a mediator** window, select **Cloud** as the mediator type and enter the following information:
   - NetApp Console organization ID
   - NetApp Console client ID
   - NetApp Console client secret
3. Select the cluster peer.
4. If you are using an HTTP proxy and it's not already configured, enter the HTTP proxy information for the local and remote hosts.

   It's recommended that you use a different proxy server for each cluster peer.
5. Optional: If a root CA certificate needs to be installed in ONTAP, especially when using a proxy server, paste the certificate in the text box provided.
6. Select **Add**.
7. Navigate to **Protection > Overview** and check the status of the relationship between the SnapMirror active sync clusters and ONTAP Cloud Mediator.

CLI

1. Configure ONTAP Cloud Mediator:
   `snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp -org-id <NetApp Console Organization ID> -service-account-client-id <Service Account Client ID> -use-http-proxy-local <true|false> -use-http -proxy-remote <true|false>`
2. Check ONTAP Cloud Mediator status:
   `snapmirror mediator show`

   Example:

```
C1_cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
0.0.0.0          C2_cluster       connected         true
cloud
```

Protect with ONTAP SnapMirror active sync

SnapMirror active sync offers asymmetric protection and, beginning with ONTAP 9.15.1, symmetric active/active protection.

Configure asymmetric protection

Configuring asymmetric protection using SnapMirror active sync involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group.

Before you begin

- You must have a SnapMirror synchronous license.
- You must be a cluster or storage VM administrator.
- All constituent volumes in a consistency group must be in a single storage VM (SVM).
  - LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.
- You cannot establish SnapMirror active sync consistency group relationships across ASA clusters and non-ASA clusters.
- The default IPspace is required by SnapMirror active sync for cluster peer relationships. Custom IPspace is not supported.
- The name of the consistency group must be unique.
- The volumes on the secondary (destination) cluster must be type DP.
- The primary and the secondary SVMs must be in a peered relationship.

Steps

You can configure a consistency group using the ONTAP CLI or System Manager.

Beginning with ONTAP 9.10.1, ONTAP offers a consistency group endpoint and menu in System Manager, offering additional management utilities. If you are using ONTAP 9.10.1 or later, see Configure a consistency group then configure protection to create a SnapMirror active sync relationship.

> ⓘ From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

System Manager

1. On the primary cluster, navigate to **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select the LUNs you want to protect and add them to a protection group.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

CLI

1. Create a consistency group relationship from the destination cluster.

   ```
   destination::> snapmirror create -source-path source-path -destination-path
   destination-path -cg-item-mappings volume-paths -policy policy-name
   ```

   You can map up to 12 constituent volumes using the `cg-item-mappings` parameter on the `snapmirror create` command.

   The following example creates two consistency groups: cg_src_ on the source with `vol1 and vol2 and a mirrored destination consistency group, cg_dst.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
   ```

2. From the destination cluster, initialize the consistency group.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

3. Confirm that the initialization operation completed successfully. The status should be `InSync`.

   ```
   snapmirror show
   ```

4. On each cluster, create an igroup so you can map LUNs to the initiator on the application host.

   ```
   lun igroup create -igroup name -protocol fcp|iscsi -ostype os -initiator
   initiator_name
   ```

   Learn more about `lun igroup create` in the ONTAP command reference.

5. On each cluster, map LUNs to the igroup:

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Verify the LUN mapping completed successfully with the `lun map` command. Then, you can discover the new LUNs on the application host.

Configure symmetric active/active protection

You can establish symmetric protection using System Manager or the ONTAP CLI. In both interfaces, there are different steps for uniform and non-uniform configurations.

Before you begin

- Both clusters must be running ONTAP 9.15.1 or later.
- Symmetric active/active configurations require the `AutomatedFailoverDuplex` protection policy. Alternately, you can create a custom SnapMirror policy provided the `-type` is `automated-failover-duplex`.
- In ONTAP 9.15.1, symmetric active/active is only supported on 2-node clusters.
- Beginning with ONTAP 9.16.1 GA, SnapMirror active sync supports symmetric active/active configurations on four-node clusters.
  - To use SnapMirror active sync on a four-node cluster, you must be running ONTAP 9.16.1 GA or later.
  - Before deploying a four-node configuration, you must create a cluster peer relationship.
  - Review the limits for four-node clusters.
  - If you revert to a two-node cluster, you must remove the SnapMirror active sync relationships from the cluster before reverting.
  - You can use the four-node configuration to upgrade storage and controllers. This process is non-disruptive and expands the cluster while moving volumes into the new nodes. For more information, see refresh a cluster.
- Beginning with ONTAP 9.17.1, you can configure symmetric active/active protection on NVMe namespaces only when both clusters are running ONTAP 9.17.1 or later.

Configure symmetric active/active protection using a SCSI SnapMirror active sync configuration

Steps

You can use System Manager or the ONTAP CLI to configure symmetric active/active protection using SCSI protocol host mappings.

System Manager

Steps for a uniform configuration

1. On the primary site, create a consistency group using new LUNs.
    a. When creating the consistency group, specify host initiators to create igroups.
    b. Select the checkbox to **Enable SnapMirror** then choose the `AutomatedFailoverDuplex` policy.
    c. In the dialog box that appears, select the **Replicate initiator groups** checkbox to replicate igroups. In **Edit proximity settings**, set proximal SVMs for your hosts.
    d. Select **Save**.

Steps for a non-uniform configuration

1. On the primary site, create a consistency group using new LUNs.
    a. When creating the consistency group, specify host initiators to create igroups.
    b. Select the checkbox to **Enable SnapMirror** then choose the `AutomatedFailoverDuplex` policy.
    c. Select **Save** to create the LUNs, consistency group, igroup, SnapMirror relationship, and igroup mapping.
2. On the secondary site, create an igroup and map the LUNs.
    a. Navigate to **Hosts** > **SAN Initiator Groups**.
    b. Select **+Add** to create a new igroup.
    c. Provide a **Name**, select the **Host Operating System**, then choose **Initiator Group Members**.
    d. Select **Save** to initialize the relationship.
3. Map the new igroup to the destination LUNs.
    a. Navigate to **Storage** > **LUNs**.
    b. Select all the LUNs to map to the igroup.
    c. Select **More** then **Map to Initiator Groups**.

CLI

Steps for a uniform configuration

1. Create a new SnapMirror relationship grouping all the volumes in the application. Ensure you designate the `AutomatedFailOverDuplex` policy to establish bidirectional sync replication.

    ```
    snapmirror create -source-path <source_path> -destination-path
    <destination_path> -cg-item-mappings <source_volume:@destination_volume>
    -policy AutomatedFailOverDuplex
    ```

    Example:
    The following example creates two consistency groups: cg_src on the source with vol1 and vol2, and a mirrored consistency group on the destination, cg_dst.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. Initialize the SnapMirror relationship:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. Confirm the operation has succeeded by waiting for the `Mirrored State` to show as `SnapMirrored` and the `Relationship Status` as `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```
4. On your host, configure host connectivity with access to each cluster according to your needs.
5. Establish the igroup configuration. Set the preferred paths for initiators on the local cluster. Specify the option to replicate the configuration to the peer cluster for inverse affinity.

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   > Beginning with ONTAP 9.16.1, use the `-proximal-vserver local` parameter in this command.

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   > Beginning with ONTAP 9.16.1, use the `-proximal-vserver peer` parameter in this command.
6. From the host, discover the paths and verify the hosts have an active/optimized path to the storage LUN from the preferred cluster.
7. Deploy the application and distribute the VM workloads across clusters to achieve the required load balancing.

Steps for a non-uniform configuration

1. Create a new SnapMirror relationship grouping all the volumes in the application. Ensure you designate the `AutomatedFailOverDuplex` policy to establish bidirectional sync replication.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Example:
   The following example creates two consistency groups: cg_src on the source with vol1 and vol2, and a mirrored consistency group on the destination, cg_dst.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. Initialize the SnapMirror relationship:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. Confirm the operation has succeeded by waiting for the `Mirrored State` to show as `SnapMirrored` and the `Relationship Status` as `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. On your host, configure host connectivity with access to each cluster according to your needs.
5. Establish the igroup configurations on both the source and destination clusters.

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. From the host, discover the paths and verify the hosts have an active/optimized path to the storage LUN from the preferred cluster.
7. Deploy the application and distribute the VM workloads across clusters to achieve the required load balancing.

Configure symmetric active/active protection using an NVMe SnapMirror active sync configuration

Before you begin

In addition to the requirements for configuring symmetric active/active protection, you should be aware of the supported and unsupported configurations when using the NVMe protocol.

- Consistency groups can have one or more subsystem.
- Volumes within the consistency group can have namespace maps from multiple subsystems.
- Subsystems cannot have namespace maps that belong to more than one consistency group.
- Subsystems cannot have some namespace maps that belong to a consistency group and some namespace maps that do not belong to a consistency group.
- Subsystems must have namespace maps that are part of the same consistency group.

Steps

Beginning with ONTAP 9.17.1, you can use System Manager or the ONTAP CLI to create a consistency group and configure symmetric active/active protection using NVMe protocol host mappings.

System Manager

1. On the primary site, create a consistency group using new volumes or NVMe namespaces.
2. select **+Add** and choose **Using new NVMe namespaces**.
3. Enter the consistency group name.
4. Select **More**.
5. In the **Protection** section, select **Enable SnapMirror** then choose the `AutomatedFailoverDuplex` policy.
6. In the **Host mapping** section, choose either **Existing NVMe subsystem** or **New NVMe subsystem**.
7. Select **In proximity to** to change the proximal SVM. The source SVM is selected by default.
8. If necessary, add another NVMe subsystem.

CLI

1. Create a new SnapMirror relationship grouping all the volumes containing all NVMe namespaces used by the application. Ensure you designate the `AutomatedFailOverDuplex` policy to establish bidirectional sync replication.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Example:

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. Initialize the SnapMirror relationship:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   Example:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. Confirm the operation has succeeded by waiting for the `Mirrored State` to show as `SnapMirrored` and the `Relationship Status` as `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

   The NVMe subsystems associated with the NVMe namespaces in the primary volumes are automatically replicated to the secondary cluster.

4. On your host, configure host connectivity with access to each cluster according to your needs.
5. Specify the SVM that is proximal to each of your hosts. This enables host access to the NVMe namespace using a path from the preferred cluster. This might be the SVM in the primary cluster *or*

the SVM in DR cluster.

The following command indicates that SVM VS_A is proximal to host H1 and set VS_A as the proximal SVM:

```
SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

The following command indicates that SVM VS_B is proximal to host H2 and sets VS_B as the proximal SVM:

```
SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. From the host, discover the paths and verify the hosts have an active/optimized path to the storage from the preferred cluster.
7. Deploy the application and distribute the VM workloads across clusters to achieve the required load balancing.

Related information

- snapmirror create
- snapmirror initialize
- snapmirror show

Convert an existing ONTAP SnapMirror relationship to SnapMirror active sync relationship

If you've configured SnapMirror protection, you can convert the relationship to SnapMirror active sync. Beginning with ONTAP 9.15.1, you can convert the relationship to use symmetric active/active protection.

Convert an existing iSCSI or FC SnapMirror relationship to an asymmetric SnapMirror active sync relationship

If you have an existing iSCSI or FC SnapMirror synchronous relationship between a source and destination cluster, you can convert it to an asymmetric SnapMirror active sync relationship. This allows you to associate the mirrored volumes with a consistency group, ensuring zero RPO across a multi-volume workload. Additionally, you can retain existing SnapMirror snapshots if you need to revert to a point in time prior to establishing the SnapMirror active sync relationship.

About this task

- You must be a cluster and SVM administrator on the primary and secondary clusters.
- You cannot convert zero RPO to zero RTO sync by changing the SnapMirror policy.
- You must ensure the LUNs are unmapped before issuing the `snapmirror create` command.

  If existing LUNs on the secondary volume are mapped and the `AutomatedFailover` policy is configured, the `snapmirror create` command triggers an error.

Before you begin

- A zero RPO SnapMirror synchronous relationship must exist between the primary and secondary cluster.
- All LUNs on the destination volume must be unmapped before the zero RTO SnapMirror relationship can be created.
- SnapMirror active sync only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.
- ONTAP Mediator must be configured for SnapMirror active sync.

Steps

1. From the secondary cluster, perform a SnapMirror update on the existing relationship:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verify that the SnapMirror update completed successfully:

   ```
   SiteB::>snapmirror show
   ```

3. Pause each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
   ```

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Delete each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1
   ```

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Release the source SnapMirror relationship but retain the common snapshots:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1
   ```

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Create a zero RTO SnapMirror synchronous relationship:

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Resynchronize the consistency group:

   ```
   SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Rescan host LUN I/O paths to restore all paths to the LUNs.

Convert an existing iSCSI or FC SnapMirror relationship to symmetric active/active

Beginning with ONTAP 9.15.1, you can convert an existing iSCSI or FC SnapMirror relationship to a SnapMirror active sync symmetric active/active relationship.

Before you begin

- You must be running ONTAP 9.15.1 or later.
- A zero RPO SnapMirror synchrnous relationship must exist between the primary and secondary cluster.
- All LUNs on the destination volume must be unmapped before the zero RTO SnapMirror relationship can be created.
- SnapMirror active sync only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.
- ONTAP Mediator must be configured for SnapMirror active sync.

Steps

1. From the secondary cluster, perform a SnapMirror update on the existing relationship:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verify that the SnapMirror update completed successfully:

   ```
   SiteB::>snapmirror show
   ```

3. Pause each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
   ```

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Delete each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1
   ```

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Release the source SnapMirror relationship but retain the common snapshots:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1
   ```

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Create a zero RTO SnapMirror synchronous relationship with the AutomatedFailoverDuplex policy:

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailoverDuplex
   ```

7. If the existing hosts are local the primary cluster, add the host to the secondary cluster and establish connectivity with respective access to each cluster.
8. On the secondary site, delete the LUN maps on the igroups associated with remote hosts.

   ⓘ Ensure the igroup does not contain maps for non-replicated LUNs.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. On the primary site, modify the initiator configuration for existing hosts to set the proximal path for initiators on the local cluster.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
   <host> -proximal-vserver <server>
   ```

10. Add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Ennable igroup replication to replicate the configuration and invert the host locality on the remote cluster.

    ```
    SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
    SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
    -proximal-vserver vsB
    ```

11. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN from the preferred cluster
12. Deploy the application and distribute the VM workloads across clusters.
13. Resynchronize the consistency group:

    ```
    SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
    ```

14. Rescan host LUN I/O paths to restore all paths to the LUNs.

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync
- snapmirror show

Convert ONTAP SnapMirror active sync relationship type

Beginning with ONTAP 9.15.1, you can convert between types of SnapMirror active sync protection: from asymmetric to symmetric active/active and vice versa.

Convert to a symmetric active/active relationship

You can convert a iSCSI or FC SnapMirror active sync relationship with asymmetric protection to use symmetric active/active.

Before you begin

- Both clusters must be running ONTAP 9.15.1 or later.
- Symmetric active/active configurations require the `AutomatedFailoverDuplex` protection policy. Alternately, you can create a custom SnapMirror policy provided the `-type` is `automated-failover-duplex`.

System Manager

Steps for a uniform configuration

1. Remove the destination igroup:
   a. On the destination cluster, navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup with the SnapMirror relationship, then **Delete**.
   c. In the dialog box, select the **Unmap the associated LUNs** box then **Delete**.
2. Edit the SnapMirror active sync relationship.
   a. Navigate to **Protection** > **Relationships**.
   b. Select the kabob menu next to the relationship you want to modify then **Edit**.
   c. Modify the **Protection Policy** to AutomatedFailoverDuplex.
   d. Selecting `AutoMatedFailoverDuplex` prompts a dialog box to modify host proximity settings. For the initiators, select the appropriate option for **Initiator proximal to** then **Save**.
   e. Select **Save**.
3. In the **Protection** menu, confirm the operation succeeded when the relationship displays as `InSync`.

Steps for a non-uniform configuration

1. Remove the destination igroup:
   a. On the secondary site, navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup with the SnapMirror relationship, then **Delete**.
   c. In the dialog box, select the **Unmap the associated LUNs** box then **Delete**.
2. Create a new igroup:
   a. In the **SAN Initiator Groups** menu on the destination site, select **Add**.
   b. Provide a **Name**, select the **Host Operating System**, then choose **Initiator Group Members**.
   c. Select **Save**.
3. Map the new igroup to the destination LUNs.
   a. Navigate to **Storage** > **LUNs**.
   b. Select all the LUNs to map to the igroup.
   c. Select **More** then **Map to Initiator Groups**.
4. Edit the SnapMirror active sync relationship.
   a. Navigate to **Protection** > **Relationships**.
   b. Select the kabob menu next to the relationship you want to modify then **Edit**.
   c. Modify the **Protection Policy** to AutomatedFailoverDuplex.
   d. Selecting AutoMatedFailoverDuplex initiates the option to modify host proximity settings. For the initiators, select the appropriate option for **Initiator proximal to** then **Save**.
   e. Select **Save**.
5. In the **Protection** menu, confirm the operation succeeded when the relationship displays as `InSync`.

CLI

Steps for a uniform configuration

1. Modify the SnapMirror policy from `AutomatedFailover` to `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. Modifying the policy triggers a resync. Wait for the resync to complete and confirm the relationship is `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. If the existing hosts are local the primary cluster, add the host to the second cluster and establish connectivity with respective access to each cluster.
4. On the secondary site, delete the LUN maps on the igroups associated with remote hosts.

   > Ensure the igroup does not contain maps for non-replicated LUNs.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

5. On the primary site, set the privilege level to `advanced`:

   ```
   SiteA::> set -privilege advanced
   ```

6. Modify the initiator configuration for existing hosts to set the proximal path for initiators on the local cluster.

   ```
   SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
   -initiator <host> -proximal-vserver <server>
   ```

   > You can set the privilege level back to admin after you complete this step.

7. Add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Ennable igroup replication to replicate the configuration and invert the host locality on the remote cluster.

   ```
   SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
   SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
   host2 -proximal-vserver vsB
   ```

8. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN from the preferred cluster
9. Deploy the application and distribute the VM workloads across clusters.

Steps for a non-uniform configuration

1. Modify the SnapMirror policy from `AutomatedFailover` to `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. Modifying the policy triggers a resync. Wait for the resync to complete and confirm the relationship is

```
Insync:

snapmirror show -destination-path <destination_path>
```

3. If the existing hosts are local to the primary cluster, add the host to the second cluster and establish connectivity with respective access to each cluster.
4. On the secondary site, add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Map the LUNs to the igroup.

   ```
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
   SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
   <host_name>
   SiteB::> lun mapping create -igroup <igroup> -path <path_name>
   ```

5. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN from the preferred cluster
6. Deploy the application and distribute the VM workloads across clusters.

Convert from symmetric active/active to an asymmetric iSCSI or FC relationship

If you’ve configured symmetric active/active protection using iSCSI or FC, you can convert the relationship to asymmetric protection using the ONTAP CLI.

Steps

1. Move all the VM workloads to the host local to the source cluster.
2. Remove the igroup configuration for the hosts not managing the VM instances then modify the igroup configuration to terminate igroup replication.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. On the secondary site, unmap the LUNs.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. On the secondary site, delete the symmetric active/active relationship.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. On the primary site, release the symmetric active/active relationship.

   ```
   SiteA::> snapmirror release -destination-path <destination_path> -relationship
   -info-only true
   ```

6. From the secondary site, create a relationship to the same set of volumes with the `AutomatedFailover` policy to resynchronize the relationship.

   ```
   SiteB::> snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source:@destination> -policy
   AutomatedFailover
   SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
   ```

```
<policy_type>
```

> ⓘ The consistency group on the secondary site needs to be deleted before recreating the relationship. The destination volumes must be converted to type DP. To convert the volumes to DP, perform the `snapmirror resync` command with a non-`AutomatedFailover` policy: `MirrorAndVault`, `MirrorAllSnapshots`, or `Sync`.

7. Confirm the relationship Mirror State is `Snapmirrored` the Relationship Status is `Insync`.

   ```
   snapmirror show -destination-path destination_path
   ```

8. Re-discover the paths from the host.

Related information

- snapmirror delete
- snapmirror modify
- snapmirror release
- snapmirror resync
- snapmirror show

Manage SnapMirror active sync and protect data

Create a common snapshot between ONTAP consistency groups

In addition to the regularly scheduled snapshot operations, you can manually create a common snapshot between the volumes in the primary SnapMirror consistency group and the volumes in the secondary SnapMirror consistency group.

About this task

The scheduled snapshot creation interval is 12 hours.

Before you begin

- The SnapMirror group relationship must be in sync.

Steps

1. Create a common snapshot:

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. Monitor the progress of the update:

   ```
   destination::>snapmirror show -fields newest-snapshot
   ```

Related information

- snapmirror show

Perform a planned failover of ONTAP clusters in a SnapMirror active sync relationship

In a planned failover of ONTAP clusters in a SnapMirror active sync relationship, you switch the roles of the primary and secondary clusters, so that the secondary cluster takes over from the primary cluster. During a failover, what is normally the secondary cluster processes input and output requests locally without disrupting client operations.

You may want to perform a planned failover to test the health of your disaster recovery configuration or to perform maintenance on the primary cluster.

About this task

A planned failover is initiated by the administrator of the secondary cluster. The operation requires switching the primary and secondary roles so that the secondary cluster takes over from the primary. The new primary cluster can then begin processing input and output requests locally without disrupting client operations.

Before you begin

- The SnapMirror active sync relationship must be in sync.
- You cannot initiate a planned failover when a nondisruptive operation is in process. Nondisruptive operations include volume moves, aggregate relocations, and storage failovers.
- The ONTAP Mediator must be configured, connected, and in quorum.

Steps

You can perform a planned failover using the ONTAP CLI or System Manager.

System Manager

> ⓘ From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

1. In System Manager, select **Protection > Overview > Relationships**.
2. Identify the SnapMirror active sync relationship you want to failover. Next to its name, select the … next to the relationship's name, then select **Failover**.
3. To monitor the status of the failover, use the `snapmirror failover show` in the ONTAP CLI.

CLI

1. From the destination cluster, initiate the failover operation:

```
destination::>snapmirror failover start -destination-path
vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the failover:

```
destination::>snapmirror failover show
```

3. When the failover operation is complete, you can monitor the SnapMirror synchronous protection relationship status from the destination:

```
destination::>snapmirror show
```

Related information

- snapmirror failover show
- snapmirror failover start
- snapmirror show

Recover from automatic unplanned ONTAP cluster failover operations

An automatic unplanned failover (AUFO) operation occurs when the primary cluster is down or isolated. The ONTAP Mediator detects when a failover occurs and executes an automatic unplanned failover to the the secondary cluster. The secondary cluster is converted to the primary and begins serving clients. This operation is performed only with assistance from the ONTAP Mediator.

> ⓘ After the automatic unplanned failover, it is important to rescan the host LUN I/O paths so that there is no loss of I/O paths.

Reestablish the protection relationship after an unplanned failover

You can reestablish the protection relationship using System Manager or the ONTAP CLI.

System Manager

> **Steps**
>
> From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

1. Navigate to **Protection > Relationships** and wait for the relationship state to show "InSync".
2. To resume operations on the original source cluster, click ⋮ and select **Failover**.

CLI

You can monitor the status of the automatic unplanned failover using the `snapmirror failover show` command.

For example:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Refer to the EMS reference to learn about event messages and about corrective actions.

Resume protection in a fan-out configuration after failover

Beginning with ONTAP 9.15.1, SnapMirror active sync supports automatic reconfiguration in the fan-out leg after a failover event. The async fan-out leg can be a consistency group relationship or an independent volume relationship. For more information, see fan-out configurations.

If you're using ONTAP 9.14.1 or earlier and you experience a failover on the secondary cluster in the SnapMirror active sync relationship, the SnapMirror asynchronous destination becomes unhealthy. You must manually restore protection by deleting and recreating the relationship with the SnapMirror asynchronous endpoint.

Steps

1. Verify the failover has completed successfully:
   `snapmirror failover show`
2. On the SnapMirror asynchronous endpoint, delete the fan-out endpoint:
   `snapmirror delete -destination-path` *`destination_path`*
3. On the third site, create a SnapMirror asynchronous relationships between the new SnapMirror active sync primary volume and the async fan-out destination volume:

```
snapmirror create -source-path source_path -destination-path destination_path
-policy MirrorAllSnapshots -schedule schedule
```

4. Resynchronize the relationship:
   ```
   snapmirror resync -destination-path destination_path
   ```
5. Verify the relationship status and heath:
   ```
   snapmirror show
   ```

Related information

- snapmirror create
- snapmirror delete
- snapmirror failover show
- snapmirror resync
- snapmirror show

Monitor ONTAP SnapMirror active sync operations

You can monitor the following SnapMirror active sync operations to ensure the health of your SnapMirror active sync configuration:

- ONTAP Mediator
- Planned failover operations
- Automatic unplanned failover operations
- SnapMirror active sync availability

> Beginning with ONTAP 9.15.1, System Manager displays the status of your SnapMirror active sync relationship from either cluster. You can also monitor the ONTAP Mediator’s status from either cluster in System Manager.

ONTAP Mediator

During normal operations, the ONTAP Mediator state should be connected. If it’s in any other state, this might indicate an error condition. You can review the Event Management System (EMS) messages to determine the error and appropriate corrective actions.

Planned failover operations

You can monitor status and progress of a planned failover operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Once the failover operation is complete, you can monitor the SnapMirror protection status from the new destination cluster. For example:

```
ClusterA::> snapmirror show
```

Refer to the EMS reference to learn about event messages and corrective actions.

Automatic unplanned failover operations

During an unplanned automatic failover, you can monitor the status of the operation using the `snapmirror failover show` command.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Refer to the EMS reference to learn about event messages and about corrective actions.

SnapMirror active sync availability

You can check the availability of the SnapMirror active sync relationship using a series of commands, either on the primary cluster, the secondary cluster, or both.

Commands you use include the `snapmirror mediator show` command on both the primary and secondary cluster to check the connection and quorum status, the `snapmirror show` command, and the `volume show` command. For example:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                    Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                     No-consensus
```

Related information

- snapmirror failover show
- snapmirror failover start
- snapmirror mediator show

Add or remove volumes to an ONTAP consistency group

As your application workload requirements change, you may need to add or remove volumes from a consistency group to ensure business continuity. The process of adding and removing volumes in an an active SnapMirror active sync relationship depends on the version of ONTAP you are using.

In most instances, this is a disruptive process requiring you to delete the SnapMirror relationship, modify the consistency group, then resume protection. Beginning with ONTAP 9.13.1, adding volumes to a consistency group with an active SnapMirror relationship is a non-disruptive operation.

About this task

- In ONTAP 9.9.1, you can add or remove volumes to a consistency group using the ONTAP CLI.
- Beginning with ONTAP 9.10.1, it is recommended that you manage consistency groups through System Manager or with the ONTAP REST API.

  If you want to change the composition of the consistency group by adding or removing a volume, you must first delete the original relationship and then create the consistency group again with the new composition.

- Beginning with ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SnapMirror relationship from the source or destination. This action is not supported with the NVMe protocol.

  Removing volumes is a disruptive operation. You must delete the SnapMirror relationship before removing volumes.

ONTAP 9.9.1-9.13.0

Before you begin

- You cannot begin to modify the consistency group while it is in the `InSync` state.
- The destination volume should be of type DP.
- The new volume you add to expand the consistency group must have a pair of common snapshots between the source and destination volumes.

Steps

The examples shown in two volume mappings: `vol_src1` ←→ `vol_dst1` and `vol_src2` ←→ `vol_dst2`, in a consistency group relationship between the end points `vs1_src:/cg/cg_src` and `vs1_dst:/cg/cg_dst`.

1. On the source and destination clusters, verify there is a common snapshot between the source and destination clusters with the command `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*
   ```

   ```
   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. If no common snapshot exists, create and initialize a FlexVol SnapMirror relationship:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Delete the consistency group relationship:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

4. Release the source SnapMirror relationship and retain the common snapshots:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Unmap the LUNs and delete the existing consistency group relationship:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > ⓘ The destination LUNs are unmapped, while the LUNs on the primary copy continue to serve the host I/O.

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **If you are using ONTAP 9.10.1 through 9.13.0,** delete and recreate and the consistency group on

the source with the correct composition. Follow the steps in Delete a consistency group and then Configure a single consistency group. In ONTAP 9.10.1 and later, you must perform the delete and create operations in System Manager or with the ONTAP REST API; there is no CLI procedure.

If you are using ONTAP 9.9.1, skip to the next step.

7. Create the new consistency group on the destination with the new composition:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resynchronize the zero RTO consistency group relationship to ensure it is in sync:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Remap the LUNs that you unmapped in Step 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Rescan host LUN I/O paths to restore all paths to the LUNs.

ONTAP 9.13.1 and later

Beginning with ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SnapMirror active sync relationship. SnapMirror active sync supports adding volumes from both the source or destination.

> From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

For details on adding volumes from the source consistency group, see Modify a consistency group.

Add a volume from the destination cluster

1. On the destination cluster, select **Protection** > **Relationships**.
2. Find the SnapMirror configuration you want to add volumes to. Select ⋮ then **Expand**.
3. Select the volume relationships whose volumes are to be added to consistency group
4. Select **Expand**.

Related information

- snapmirror delete
- snapmirror initialize
- snapmirror release
- snapmirror resync

Upgrade and revert with ONTAP SnapMirror active sync

SnapMirror active sync is supported beginning with ONTAP 9.9.1. Upgrading and reverting your ONTAP cluster or controllers has implications on your SnapMirror active sync relationships depending on the ONTAP version to which you are upgrading or reverting.

Refresh a cluster

Beginning with ONTAP 9.16.1, SnapMirror active sync supports four-node clusters in symmetric active/active configurations. You can use the four-node cluster to upgrade controllers and storage.

Before you begin

- Review the requirements for four-node clusters.
- You can create asymmetrical configurations during the tech refresh process; however, you should return to a symmetrical configuration after completing the refresh.
- These instructions apply to an existing four-node configuration with 50 or fewer consistency groups and 400 or fewer volume endpoints.

Steps

1. Move all the SnapMirror active sync volumes onto a *single* high-availability (HA) pair.
2. Remove the unused nodes from the cluster.
3. Add the new nodes to the cluster.
4. Move all the volumes into the new nodes.
5. Remove the unused nodes from the cluster then replace them with the new nodes.

Upgrade ONTAP with SnapMirror active sync

To use SnapMirror active sync, all nodes on the source and destination clusters must be running ONTAP 9.9.1 or later.

When upgrading ONTAP with active SnapMirror active sync relationships, you should use automated nondisruptive upgrade (ANDU). Using ANDU ensures your SnapMirror active sync relationships are in sync and healthy during the upgrade process.

There are no configuration steps to prepare SnapMirror active sync deployments for ONTAP upgrades. However, it is recommended that before and after the upgrade, you should check that:

- SnapMirror active sync relationships are in sync.
- There are no errors related to SnapMirror in the event log.
- The Mediator is online and healthy from both clusters.
- All hosts can see all paths properly to protect LUNs.

ⓘ When you upgrade clusters from ONTAP 9.9.1 or 9.9.1 to ONTAP 9.10.1 and later, ONTAP creates new consistency groups on both source and destination clusters for SnapMirror active sync relationships that can be configured using System Manager.

ⓘ The `snapmirror quiesce` and `snampirror resume` commands are not supported with SnapMirror active sync.

Revert to ONTAP 9.9.1 from ONTAP 9.10.1

To revert relationships from 9.10.1 to 9.9.1, SnapMirror active sync relationships must be deleted, followed by the 9.10.1 consistency group instance. Consistency groups with an active SnapMirror active sync relationship cannot be deleted. Any FlexVol volumes that were upgraded to 9.10.1 previously associated with another Smart Container or Enterprise App in 9.9.1 or earlier will no longer be associated on revert. Deleting consistency groups does not delete the constituent volumes or volume granular snapshots. Refer to Delete a consistency group for more information on this task in ONTAP 9.10.1 and later.

Revert from ONTAP 9.9.1

> SnapMirror active sync is not supported with mixed ONTAP clusters than include releases earlier than ONTAP 9.9.1.

When you revert from ONTAP 9.9.1 to an earlier release of ONTAP, you must be aware of the following:

- If the cluster hosts an SnapMirror active sync destination, reverting to ONTAP 9.8 or earlier is not allowed until the relationship is broken and deleted.
- If the cluster hosts an SnapMirror active sync source, reverting to ONTAP 9.8 or earlier is not allowed until the relationship is released.
- All user-created custom SnapMirror active sync policies must be deleted before reverting to ONTAP 9.8 or earlier.

To meet these requirements, see Remove a SnapMirror active sync configuration.

Steps

1. Confirm your readiness to revert, entering the following command from one of the clusters in the SnapMirror active sync relationship:

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   The following sample output shows a cluster that is not ready to revert with instructions for clean up.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   ```

```
node:
   volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
   quiesce and abort transfers on associated SnapMirror relationships
and
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. Once you’ve satisfied the requirements of the revert check, see Revert ONTAP.

Related information

- network interface
- snapmirror break
- snapmirror policy delete

- snapmirror policy show
- snapmirror quiesce
- snapmirror show

Remove an ONTAP SnapMirror active sync configuration

If you no longer require zero RTO SnapMirror synchronous protection, you can delete your SnapMirror active sync relationship.

Remove an asymmetric configuration

- Before you delete the SnapMirror active sync relationship, all LUNs in the destination cluster must be unmapped.
- After the LUNs are unmapped and the host is rescanned, the SCSI target notifies the hosts that the LUN inventory has changed. The existing LUNs on the zero RTO secondary volumes change to reflect a new identity after the zero RTO relationship is deleted. Hosts discover the secondary volume LUNs as new LUNs that have no relationship to the source volume LUNs.
- The secondary volumes remain DP volumes after the relationship is deleted. You can issue the `snapmirror break` command to convert them to read/write.
- Deleting the relationship is not allowed in the failed-over state when the relationship is not reversed.

Steps

1. From the secondary cluster, remove the SnapMirror active sync consistency group relationship between the source endpoint and destination endpoint:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. From the primary cluster, release the consistency group relationship and the snapshots created for the relationship:

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Perform a host rescan to update the LUN inventory.
4. Beginning with ONTAP 9.10.1, deleting the SnapMirror relationship does not delete the consistency group. If you want to delete the consistency group, you must use System Manager or the ONTAP REST API. See Delete a consistency group for more information.

Remove iSCSI or FC symmetric active/active configuration

You can remove a symmetric configuration using System Manager or the ONTAP CLI. In both interfaces, there are different steps for uniform and non-uniform configurations.

System Manager

Steps for a uniform configuration

1. On the primary site, remove the remote hosts from the igroup and terminate replication.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup you want to modify then **Edit**.
   c. Remove the remote initiator and terminate igroup replication. Select **Save**.
2. On the secondary site, delete the replicated relationship by unmapping the LUNs.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup with the SnapMirror relationship, then **Delete**.
   c. In the dialog box, select the **Unmap the associated LUNs** box then **Delete**.
   d. Navigate to **Protection** > **Relationships**.
   e. Select the SnapMirror active sync relationship then **Release** to delete the relationships.

Steps for a non-uniform configuration

1. On the primary site, remove the remote hosts from the igroup and terminate replication.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup you want to modify then **Edit**.
   c. Remove the remote initiator and terminate igroup replication. Select **Save**.
2. On the secondary site, remove the SnapMirror active sync relationship.
   a. Navigate to **Protection** > **Relationships**.
   b. Select the SnapMirror active sync relationship then **Release** to delete the relationships.

CLI

Steps for a uniform configuration

1. Move all the VM workloads to the host local to source cluster of SnapMirror active sync.
2. On the source cluster, remove the initiators from the igroup and modify the igroup configuration to terminate igroup replication.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. On the secondary site, delete the LUN mapping and remove the igroup configuration:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. On the secondary site, delete the SnapMirror active sync relationship.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. On the primary site, release the SnapMirror active sync relationship from primary site.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Rediscover the paths to verify that only the local path is available to the host.

Steps for a non-uniform configuration

1. Move all the VM workloads to the host local to source cluster of SnapMirror active sync.
2. On the source cluster, remove the initiators from the igroup.

   ```
   SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
   <host2>
   ```

3. On the secondary site, delete the LUN mapping and remove the igroup configuration:

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
   <>
   SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
   ```

4. On the secondary site, delete the SnapMirror active sync relationship.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. On the primary site, release the SnapMirror active sync relationship from primary site.

   ```
   SiteA::> snapmirror release -destination-path <destination_path>
   ```

6. Rediscover the paths to verify that only the local path is available to the host.

Remove an NVMe symmetric active/active configuration

System Manager

Steps

1. On the source cluster, navigate to **Protection > Replication**.
2. Locate the relationship you want to remove, select ⋮ and choose **Delete**.

CLI

1. From the destination cluster, delete the SnapMirror active sync relationship.

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   Example:

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   The subsystem and its namespaces are removed from the secondary cluster.

2. From the source cluster, release the SnapMirror active sync relationship from primary site.

   ```
   snapmirror release -destination-path <destination_path>
   ```

   Example:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. Rediscover the paths to verify that only the local path is available to the host.

Related information

- snapmirror break
- snapmirror delete
- snapmirror release

Remove ONTAP Mediator or ONTAP Cloud Mediator

If you want to remove an existing ONTAP Mediator or ONTAP Cloud Mediator configuration from your ONTAP clusters, you can do so by using the `snapmirror mediator remove` command. For example, you can use only one type of Mediator at a time, so you must remove one instance before you install the other.

Steps

You can remove ONTAP Mediator or ONTAP Cloud Mediator by completing one of the following steps.

ONTAP Mediator

1. Remove ONTAP Mediator:

   `snapmirror mediator remove -mediator-address <address> -peer-cluster <peerClusterName>`

   Example:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP Cloud Mediator

1. Remove ONTAP Cloud Mediator:

   `snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud`

   Example:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Related information

- snapmirror mediator remove

Troubleshoot

ONTAP SnapMirror delete operation fails in takover state

Use the following information if the `snapmirror delete` command fails when a SnapMirror active sync consistency group relationship is in takeover state.

Issue:

When ONTAP 9.9.1 is installed on a cluster, executing the `snapmirror delete` command fails when a SnapMirror active sync consistency group relationship is in takeover state.

Example:

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solution

When the nodes in a SnapMirror active sync relationship are in takeover state, perform the SnapMirror delete and release operation with the "-force" option set to true.

Example:

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Related information

- snapmirror delete

Failure creating an ONTAP SnapMirror relationship and initializing consistency group

Use the following information if the creation of a SnapMirror relationship and consistency group initialization fails.

Issue:

Creation of SnapMirror relationship and consistency group initialization fails.

Solution:

Ensure that you have not exceeded the limit of consistency groups per cluster. Consistency group limits in SnapMirror active sync are platform independent and differ based on the version of ONTAP. See Object limits for guidance specific to your ONTAP version.

Error:

If the consistency group is stuck initializing, check the status of your consistency group initializations with the ONTAP REST API, System Manager or the command `sn show -expand`.

ⓘ From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

Solution:

If consistency groups fail to initialize, remove the SnapMirror active sync relationship, delete the consistency group, then recreate the relationship and initialize it. This workflow differs depending on the version of ONTAP you are using.

If you are using ONTAP 9.9.1	If you are using ONTAP 9.10.1 or later

1. Remove the SnapMirror active sync configuration 2. Create a consistency group relationship then Initialize the consistency group relationship	1. Under **Protection > Relationships**, find the SnapMirror active sync relationship on the consistency group. Select ⋮, then **Delete** to remove the SnapMirror active sync relationship. 2. Delete the consistency group 3. Configure the consistency group

Planned ONTAP cluster failover unsuccessful

Use the following information if the planned failover operation is unsuccessful.

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicates that a nondisruptive operation is in progress.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                          08:35:04
08:35:04
```

Cause:

A planned failover cannot begin when a nondisruptive operation is in progress, including volume move, aggregate relocation, and storage failover.

Solution:

Wait for the nondisruptive operation to complete and try the failover operation again.

Related information

- snapmirror failover show
- snapmirror failover start

ONTAP Mediator or ONTAP Cloud Mediator not reachable or Mediator quorum status is false

Use the following information if the ONTAP Mediator or ONTAP Cloud Mediator is not reachable or the Mediator quorum status is false.

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover` `show` command displays a message indicating that either the ONTAP Mediator or ONTAP Cloud Mediator is not configured.

See Configure the ONTAP Mediator and clusters for SnapMirror active sync or Configure the ONTAP Cloud Mediator for SnapMirror active sync.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Cause:

Mediator is not configured or there are network connectivity issues.

Solution:

If the ONTAP Mediator is not configured, you must configure the ONTAP Mediator before you can establish a SnapMirror active sync relationship. Fix any network connectivity issues. Make sure Mediator is connected and quorum status is true on both the source and destination site using the snapmirror mediator show command. For more information, see Configure the ONTAP Mediator.

Example:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Related information

- snapmirror failover show
- snapmirror failover start
- snapmirror mediator show

ONTAP Cloud Mediator is reachable but responding slowly

Use the following information if the ONTAP Cloud Meditor fails with an error that says the ping latency is higher than the recommended latency.

Issue:

System Manager:
The Cloud Mediator service is reachable but it’s responding slowly.

CLI:

The `mediator add` command fails with the error:

```
Error: command failed: The ping latency of the BlueXP cloud server is <x> ms
which is higher than twice the recommended latency of 200 ms.
```

Cause:

The clusters might not be located in proximity to the NetApp Console cloud or there are network path bottlenecks.

Solution:

- Check the geographical location and proximity to the NetApp Console cloud (US East).
- Optimize network path or address bottlenecks.
- Measure round trip time (RTT) using network tools, and reduce latency to within recommended limits.
- Use an HTTP proxy to improve performance.

See Configure the ONTAP Cloud Mediator and clusters for SnapMirror active sync.

Automatic unplanned failover not triggered on Site B

Use the following information if a failure on Site A does not trigger an unplanned failover on Site B.

Issue:

A failure on Site A does not trigger an unplanned failover on Site B.

Possible cause #1:

The ONTAP Mediator or the ONTAP Cloud Mediator is not configured. To determine if this is the cause, issue the `snapmirror mediator show` command on the Site B cluster.

Example:

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

This example indicates that the Mediator is not configured on Site B.

Solution:

Ensure that Mediator is configured on both clusters, that the status is connected, and quorum is set to True.

Possible cause #2:

SnapMirror consistency group is out of sync. To determine if this is the cause, view the event log to view if the consistency group was in sync during the time at which the Site A failure occurred.

Example:

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solution:

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the `force` option.
3. Enter the `snapmirror break` command on the consistency group constituent volumes to convert volumes from DP to R/W, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with `relationship-info-only` on Site A to retain common snapshot and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from R/W to DP by setting up a volume level relationship using either the Sync policy or Async policy.
7. Issue the `snapmirror resync` to synchronize the relationships.
8. Delete the SnapMirror relationships with the Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using `relationship-info-only true` on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

Related information

- snapmirror break
- snapmirror mediator show
- snapmirror resync

Link between Site B and ONTAP Mediator down and Site A down

To check on the connection of the ONTAP Mediator or the ONTAP Cloud Mediator, use the `snapmirror mediator show` command. If the connection status is unreachable and Site B is unable to reach Site A, you will have an output similar to the one below. Follow the steps in the solution to restore connection

Example:

Using ONTAP Cloud Mediator output `snapmirror mediator show`command:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

Using ONTAP Mediator output `snapmirror mediator show`command:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solution

Force a failover to enable I/O from Site B and then establish a zero RTO relationship from Site B to Site A. Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B. This will fail, so you must first modify the igroup to remove the replication peer SVM and then delete the lun map.

Example:

```
C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_1                        igroup1       0
mixed
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
       Mediator is not configured. The configuration is locked for
replicated
       objects in this Vserver peer relationship on both clusters. The
only
       supported configuration change is to manually disable replication
on
       both sides of the relationship, after which configuration changes
are
       supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
1 entries were displayed.
```

1. Delete the SnapMirror consistency group relationship using the force option.
2. Enter the SnapMirror break command (`snapmirror break -destination_path svm:_volume_`) on the consistency group constituent volumes to convert volumes from DP to RW, to enable I/O from Site B.

   You must issue the SnapMirror break command for each relationship in the consistency group. For example, if there are three volumes in the consistency group, you will issue the command for each volume.

3. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
4. Release the consistency group with relationship-info-only on Site A to retain common snapshot and unmap the LUNs belonging to the consistency group.
5. Convert volumes on Site A from RW to DP by setting up a volume level relationship using either Sync policy or Async policy.
6. Issue the `snapmirror resync` command to synchronize the relationships.
7. Delete the SnapMirror relationships with Sync policy on Site A.
8. Release the SnapMirror relationships with Sync policy using relationship-info-only true on Site B.
9. Create a consistency group relationship between Site B to Site A.
10. From the source cluster, resynchronize the consistency group. Verify the consistency group state is in sync.
11. Rescan the host LUN I/O paths to restore all paths to the LUNs.

Related information

- snapmirror break
- snapmirror mediator show
- snapmirror resync
- snapmirror show

Link between Site A and ONTAP Mediator down and Site B down

When using SnapMirror active sync, you may lose connectivity between the ONTAP Mediator or your peered clusters. You can diagnose the issue by checking the connection, availability, and consensus status of the different parts of the SnapMirror active sync relationship then forcefully resuming connection.

Table 1. Determining the cause

What to check	CLI command	Indicator
Mediator from Site A	`snapmirror mediator show`	The connection status displays as `unreachable`
Site B connectivity	`cluster peer show`	Availability displays as `unavailable`
Consensus status of the SnapMirror active sync volume	`volume show` *`volume_name`* `-fields smbc-consensus`	The `sm-bc consensus` field displays `Awaiting-consensus`

For additional information about diagnosing and resolving this issue, refer to the NetApp Knowledge Base: Link between Site A and Mediator down and Site B down when using SnapMirror active sync.

Related information

- cluster peer show
- snapmirror mediator show

ONTAP SnapMirror delete operation fails when fence is set on destination volume

Use the following information if the SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

Issue:

SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

Solution

Performing the following operations to retry the redirection and remove the fence from the destination volume.

- SnapMirror resync
- SnapMirror update

Volume move operation stuck when ONTAP primary is down

Use the following information if a volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in a SnapMirror active sync relationship.

Issue:

A volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in a SnapMirror active sync relationship.
When the primary site is down, the secondary site performs an automatic unplanned failover (AUFO). When a volume move operation is in progress when the AUFO is triggered the volume move becomes stuck.

Solution:

Abort the volume move instance that is stuck and restart the volume move operation.

ONTAP SnapMirror release fails when unable to delete snapshot

Use the following information if the SnapMirror release operation fails when the snapshot cannot be deleted.

Issue:

The SnapMirror release operation fails when the snapshot cannot be deleted.

Solution:

The snapshot contains a transient tag. Use the `snapshot delete` command with the `-ignore-owners` option to remove the transient snapshot.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Retry the `snapmirror release` command.

Related information

- snapmirror release

Volume move reference snapshot shows as the newest for ONTAP SnapMirror relationship

Use the following information if the volume move reference snapshot shows as the newest for the SnapMirror relationship after a volume move operation.

Issue:

After performing a volume move operation on a consistency group volume, the volume move reference snapshot might incorrectly display as the newest for the SnapMirror relationship.

You can view the newest snapshot with the following command:

```
snapmirror show -fields newest-snapshot status -expand
```

Solution:

Manually perform a `snapmirror resync` or wait for the next automatic resync operation after the volume move operation completes.

Related information

- snapmirror resync
- snapmirror show

Copyright information

Trademark information