Abstract

This document describes different types of remote replication supported by NetApp® SolidFire® clusters. It also describes system features, the setup process, and configurations that you must implement in various networking scenarios.
TABLE OF CONTENTS

1 NetApp SolidFire Remote Replication Overview ................................................................. 4
   1.1 SolidFire Remote Replication Uses and Benefits .......................................................... 4

2 Prerequisites for Remote Replication .................................................................................. 5

3 Cluster Pairing and Volume Pairing .................................................................................... 5
   3.1 Prerequisites .................................................................................................................. 5
   3.2 Management Virtual IP Address and Storage Virtual IP Address .............................. 6

4 Operational Model for Replication ..................................................................................... 8
   4.1 Replicating Writes ......................................................................................................... 9
   4.2 Monitoring .................................................................................................................. 9
   4.3 Data Consistency ......................................................................................................... 10
   4.4 Data Efficiency ............................................................................................................ 10
   4.5 Replication Timeout – Application Behavior ............................................................... 10

5 Choosing the Best Replication Method ............................................................................. 10
   5.1 Considerations for Setting Up Synchronous Replication ........................................... 10
   5.2 Considerations for Setting Up Asynchronous Replication ......................................... 11
   5.3 Considerations for Setting Up Snapshot Replication ................................................. 11

6 Remote Replication Topologies and Considerations .......................................................... 11
   6.1 Scenario 1: End-to-End Maximum Transmission Unit of 9000 and Same Native VLAN End to End .......... 11
   6.2 Scenario 2: End-to-End MTU of 9000 is Supported; Site A and Site B are on Different Native VLANs ........ 12
   6.3 Scenario 3: An MTU of 9000 is Supported Locally at Each Site; WAN Connection Between Sites .......... 13

7 Cluster Pairing Walkthrough .............................................................................................. 13
   7.1 Pairing Clusters by Using MVIP .................................................................................. 13
   7.2 Pairing Clusters by Using a Pairing key ....................................................................... 14
   7.3 Validating Paired Clusters .......................................................................................... 17

8 Volume Pairing Walkthrough ............................................................................................ 17

9 Recovery Point Objective and Recovery Time Objective .................................................... 18
   9.1 Recovery Time Objective ............................................................................................. 18
   9.2 Recovery Point Objective ........................................................................................... 18

10 Summary .......................................................................................................................... 20
Appendix A: TCP Port Requirements

Appendix B: Remote Replication States and Explanation

Message: Paused Disconnected
Message: Resuming Connected
Message: Resuming RR Sync
Message: Resuming Local Sync
Message: Resuming Data Transfer
Message: Active

Volume Pairing Warnings

Where to Find Additional Information

Version History

LIST OF TABLES
Table 1) Synchronous replication latency and packet loss
Table 2) Comparison of different replication modes
Table 3) Time (in hours) required for performing an initial or full data sync
Table 4) TCP port requirements for replication

LIST OF FIGURES
Figure 1) Bond management and bond storage
Figure 2) MVIP connectivity
Figure 3) Management and storage network connectivity
Figure 4) Remote replication states
Figure 5) Remote replication on the same layer 2 network
Figure 6) Remote replication over different VLANs
Figure 7) Remote replication over different MTU networks
1 NetApp SolidFire Remote Replication Overview

Data availability is one of the most crucial issues in data management. When data is not available, it adversely affects the enterprise operation until that data is restored. There are several ways to protect data availability in the event of hardware, software, or power failure. Backups and redundant hardware help to improve data availability during hardware issues or failures. However, the process of creating and storing backups should be reliable and quick. Replication duplicates data between storage systems to facilitate data availability during disaster recovery.

1.1 SolidFire Remote Replication Uses and Benefits

The SolidFire replication architecture addresses your current business requirements such as speed of recovery and maximum permissible data loss. The SolidFire remote replication feature offers an efficient way of increasing data availability and minimizing downtime. Remote replication provides a seamless replication service over LANs and WANs and avoids synchronization errors when you restart the replication process. Remote replication can be performed after the target volume and source volume are successfully paired. SolidFire supports three types of replication:

- Synchronous replication
- Asynchronous replication
- Snapshot replication

The following challenges are typically encountered when you remotely replicate data:

- Bandwidth limitations caused by data growth
- Replication over long distances
- High latencies that affect replication performance

NetApp SolidFire offers a replication solution that addresses the problems associated with complex data recovery scenarios.

Synchronous Replication

Synchronous replication (sync) continuously replicates data from the source cluster to the target cluster and is affected by latency, packet loss, jitter, and bandwidth.

During the SolidFire synchronous remote replication process, writes are acknowledged after they are committed on both the source and the target. This feedback continuously updates the target cluster. In synchronous replication, the source cluster updates data continuously so that the target cluster is always up to date. The following attributes are characteristic of synchronous replication:

- Up-to-date, crash-consistent data is available at the disaster recovery site.
- A standard IP network can be used for replication.
- Block-level replication provides consistent data across the source and target.

Synchronous replication is appropriate for the following use cases:

- The replication of a small number of systems over a short distance
- When the disaster recovery site is geographically local to the source
- For time-sensitive applications and the protection of databases
- For business continuity applications that require the secondary to act as the primary when the primary is down
Asynchronous Replication

Asynchronous replication (async) continuously replicates data from a source cluster to a target cluster without waiting for the acknowledgments from the target cluster. During asynchronous replication, writes are acknowledged to the client (application) after they are committed on the source cluster.

Asynchronous replication is useful for the following use cases:

- When the disaster recovery site is at a long distance from the source
- For applications that are not time sensitive
- When the network connecting the source and target clusters has bandwidth limitations

Snapshot Replication

This feature replicates changed data at discrete points in time to the remote cluster. Only snapshots created on the source cluster are replicated; active writes from the source volume are not. Snapshot replication does not affect asynchronous or synchronous replication. The snapshots are replicated periodically as configured by the user.

2 Prerequisites for Remote Replication

The following are the characteristics and requirements of replicated volumes:

- The ports required for remote replication should not be blocked by a firewall. See Appendix A: TCP Port Requirements.
- There should be full end-to-end connectivity between the source cluster and the target cluster.
- Cluster pairing and volume pairing should be performed before remote replication.
- The administrator must know the password for at least one and preferably both clusters.
- There should be sufficient space on the remote cluster to create a volume as large as the primary.
- A volume can be paired with only one volume at a time. Cascading replication is not supported.
- A cluster can pair with at most four other clusters.
- Any number of volumes can replicate writes in the active state. However, only 10 volumes at a time per node can be incorporated into a replication startup sequence. Therefore, if more than 10 volumes begin a replication startup sequence at the same time, only 10 of them move through the process at a time. The remaining volumes wait for a spot in the queue to open.

3 Cluster Pairing and Volume Pairing

This section introduces cluster pairing and volume pairing as a prelude to replication.

3.1 Prerequisites

Cluster Pairing

The following prerequisites are required to establish cluster pairing:

- Establish full network connectivity between the source and target clusters, including the management virtual IP addresses (MVIPs).
- Every node in the source cluster must be able to ping every other node in the target cluster.
- You must have cluster admin privileges for one or both clusters that are being paired.
- The versions of the Element® OS software present on a cluster must be compatible with the software versions of the other cluster. See NetApp SolidFire Element OS User Guide.
Volume Pairing
The following prerequisites are required to establish volume pairing:

- Cluster pairing is a prerequisite for volume pairing between the clusters.
- The access mode on the destination volume should be the replication target, and the source volume should be in read/write mode.
- The source volume should be smaller than or of equal size to the target volume. Replication transitions to an error state if the volume size of the source is larger than that of the target.
- The quality of service (QoS) settings for the target volume should be the same as for the source. This configuration allows the same volume performance for the target as for the source in the event of failover. During synchronous replication, the QoS settings should be identical on both the source and the target to avoid volume throttling.

3.2 Management Virtual IP Address and Storage Virtual IP Address

Bonded networks aggregate two physical interfaces into one logical interface. This bonding of interfaces is essential for high availability. The interfaces can be configured into two bonds on a SolidFire storage node called Bond1G and Bond10G. Bond10G is used for the storage network, and Bond1G is used for the management network. It is a best practice to assign a high-bandwidth network to storage traffic.

Management Virtual IP Address

A management virtual IP (MVIP) address is assigned for the logical interface designated for management traffic of the cluster. Separating the interfaces of management traffic and storage traffic offers the following advantages:

- Management traffic does not affect the bandwidth on the storage network.
- Traffic is isolated across different switches.
- Traffic is isolated across different VLANs.

Figure 1) Bond management and bond storage.
MVIP connectivity determines the state of the cluster pairing. Traffic traveling through the MVIP includes the following:

- Web UI traffic
- Configuration traffic
- JSON API traffic
- Traffic within the cluster, including remote procedure calls; examples are StartClusterPairing() and CompleteClusterPairing()

Figure 2) MVIP connectivity.

Storage Virtual IP

The Storage Virtual IP (SVIP) address is assigned for the logical interface designated for the storage traffic of the cluster. SVIP connectivity affects the replication process.

The traffic that travels through the SVIP address includes the following:

- iSCSI traffic
- The storage traffic between the source cluster and the target cluster
4 Operational Model for Replication

After a volume pairing relationship is established, the two clusters attempt to discover each other on a polling interval. Each cluster tracks the remote replication state for the volume in its database. In the poll procedure, they exchange states. When both sides are in the Resuming Connected state, the target initiates replication.

During replication, both volumes go through the following procedure:

1. Metadata is replicated from the source primary service to the target primary service.
2. Metadata is replicated from the target primary service to the target secondary service.
3. Data is replicated from the source cluster to the target cluster.

Figure 4 describes the transition states during replication. See Appendix B for a detailed explanation of each state.
4.1 Replicating Writes

When the target has started syncing metadata, the source cluster begins replicating writes. It replicates writes as the source volume receives them; it does not break them up or coalesce them.

The following errors cause the replication sequence to restart at Paused Disconnected:

- A replicated write exceeds the timeout of eight seconds.
- The source cluster has too much data outstanding to the target.
- The source or target volume undergoes a state change such as a role change.

4.2 Monitoring

Each cluster monitors the connection status at the cluster level and for each volume. If the cluster-level poll operation fails, then the cluster generates the fault Disconnected RemoteNode. If the poll operation fails at the volume level, then the cluster changes the replication state to Paused Disconnected.

If the remote replication mode is asynchronous or synchronous, then the target cluster tracks how long it has been since the state was active. When the asynchronous delay reaches six hours, the cluster reports the RemoteRepAsyncDelayExceeded fault.

The source cluster reports the status of replication-enabled snapshots on the target cluster in the ListSnapshots API command. It collects this information in the 1-minute poll command. The state can be Present, Not Present, Deleted, or Unknown.
4.3 Data Consistency

In the Sync replication mode, as long as the replication state is Active, any write that the source has acknowledged to the client is guaranteed to have completed on the target cluster. In the synchronous and asynchronous replication modes, the target cluster processes volume writes in the same order as in the source cluster. The write order is preserved.

4.4 Data Efficiency

The source replicates compressed data to the target, and deduplication is preserved across clusters. The target cluster does not pull blocks that it already has locally.

4.5 Replication Timeout – Application Behavior

If the replication timeout exceeds 8 seconds, the volume pairs go into the Pause Disconnected state. This mechanism protects the applications that are accessing the source side, so that writes at the source side don’t go into a wait state because of network delays between the source and target. Because source volumes are still available during the timeout scenario, the writes are acknowledged to the host when the data is written to the NRAM of the source. Application tuning is not required in this scenario.

5 Choosing the Best Replication Method

Network design plays a crucial role in determining the best replication solution.

5.1 Considerations for Setting Up Synchronous Replication

Synchronous replication must be considered when the recovery point objective (RPO) requirement is zero. When the latency between the source and target clusters is a few milliseconds, the SolidFire synchronous replication solution provides an efficient way of maintaining data redundancy.

In the case of high workloads and continuous writes with a requirement of zero application downtime, NetApp recommends synchronous replication rather than asynchronous replication.

For detailed network sizing requirements, see Network Sizing Requirements for Synchronous Replication in section 9.2.

In synchronous replication, the application waits for the acknowledgment from the target cluster before performing a new write operation. Therefore, the acknowledgement from the target is crucial for updating the target. If the network between the source and target clusters experiences high packet loss, then the probability of losing the acknowledgment from the target cluster is high. This issue can affect the performance of synchronous replication.

Synchronous replication is recommended with low latencies (<5ms) and low packet loss (<2%). The distance between the source and target clusters determines the latency and packet loss of the network. Table 1 shows the level of packet loss that can be sustained by synchronous replication over different latencies (simulated using netem).

<table>
<thead>
<tr>
<th>Latency</th>
<th>Maximum packet loss (%)</th>
<th>Link bandwidth (recommended)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5ms</td>
<td>10</td>
<td>10Gbps</td>
</tr>
<tr>
<td>10ms</td>
<td>10</td>
<td>10Gbps</td>
</tr>
<tr>
<td>15ms</td>
<td>5</td>
<td>10Gbps</td>
</tr>
<tr>
<td>20ms</td>
<td>5</td>
<td>10Gbps</td>
</tr>
</tbody>
</table>
5.2 Considerations for Setting Up Asynchronous Replication

NetApp recommends asynchronous replication when the latency between the source and target clusters is very high (>5ms). Latency is affected by the distance between sites and the type of the cable used. Therefore, when the distance between the source cluster and the target cluster is high and the RPO requirement for the application is not zero, NetApp recommends asynchronous replication rather than synchronous replication.

In asynchronous replication, the application does not wait for the acknowledgment from the target cluster before performing a write from the source cluster. Therefore, NetApp recommends asynchronous replication when the application is not tolerant of added network latencies.

For detailed network sizing requirements, see Network Sizing Requirements for Asynchronous Replication in section 9.2.

5.3 Considerations for Setting Up Snapshot Replication

Snapshot replication periodically updates new writes to the target. NetApp recommends this approach when the available bandwidth is low and more rewrite operations are performed on the source cluster. The new writes are sent to the target at the specified time interval, which helps conserve bandwidth at other times. Snapshots make it possible to revert to earlier versions of the application in the event of corruption.

For snapshot settings, see Network Sizing Requirements for Snapshot-Based Replication in section 9.2.

Table 2 summarizes replication modes and their use cases:

<table>
<thead>
<tr>
<th>Replication Mode</th>
<th>Recommended when RPO requirement is zero</th>
<th>Recommended when there are high latencies (&gt; 5ms) between the source cluster and the target cluster</th>
<th>Recommended when there is low bandwidth and a shared network between the source and the target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronous</td>
<td>Recommended in networks with low packet loss</td>
<td>Recommended when an application is not tolerant of latencies</td>
<td>Recommended for reverting to a previous state of the application</td>
</tr>
</tbody>
</table>

6 Remote Replication Topologies and Considerations

6.1 Scenario 1: End-to-End Maximum Transmission Unit of 9000 and Same Native VLAN End to End

All replication traffic is carried over the storage network. All of the following considerations are for the storage traffic. Both the source and target cluster are on the same layer 2 network (in other words, the same VLAN), and an end-to-end maximum transmission unit (MTU) of 9000 is supported.
If both the source and the target are on the same VLAN, then the source and the destination are on the same layer 2 network. In this scenario, the destination cluster is pinged from the source cluster. The Internet Control Message Protocol (ICMP) packets reach the destination cluster without the need for any routing device. There is no requirement for a gateway on the bond10G interfaces. The layer 2 bridge handles the end-to-end WAN link and the local storage connectivity.

### 6.2 Scenario 2: End-to-End MTU of 9000 is Supported; Site A and Site B are on Different Native VLANs

If the source and destination are on different layer 2 networks (in other words, different VLANs), then there should be a router or layer 3 device to route the packets from the source cluster to the destination cluster and to perform volume peering. The router interface is configured as a default gateway. The router or layer 3 device routes the packet to the destination.

The Router A interface is configured as the default gateway on Cluster A. the Router B interface is configured as the default gateway on Cluster B.

Packets that are sent to a different subnet are sent to the Router A interface by default because Router A is configured as the default gateway. Based on the routing table in Router A, packets are routed to Router B. Router B then sends the packet to the destination (Cluster B).
6.3 Scenario 3: An MTU of 9000 is Supported Locally at Each Site; WAN Connection Between Sites

An MTU of 9000 is supported locally at each site, and a WAN connection between the sites only supports an MTU of approximately 1500.

- The storage-side gateway on the cluster is configured on the bond10G interface. The gateway router supports an MTU of 9000 on the interface facing the SolidFire cluster.
- The gateway router’s WAN interface supports the WAN connection’s MTU (1500 in this case). Congestion can be caused by the difference between the supported MTUs.
- The routers at each location must support Path MTU discovery, and the ICMP replies with ICMP type 3 messages.

Figure 7) Remote replication over different MTU networks.

Path MTU Discovery Overview

Path MTU discovery is an algorithm described and implemented in TCP stacks. This algorithm attempts to discover the largest IP datagram that can be sent without fragmentation on an IP path and maximizes data transfer throughput.

Path MTU discovery is implemented when the IP sender has set the Don’t Fragment (DF) flag in the IP header. If an IP packet with this flag set reaches the router with a next-hop MTU that is too small, then the packet cannot be sent without fragmentation. In this case, the router discards the packet and sends an error, ICMP Fragmentation Needed but DF Set, to the sender of the packet. The sender is alerted to send smaller MTU packets to reach the destination.

7 Cluster Pairing Walkthrough

7.1 Pairing Clusters by Using MVIP

Two clusters can be paired by using MVIP. Cluster admin access is necessary for the pairing. Authentication must be performed before cluster pairing. Here is the method for using a pairing key:

1. On the local cluster, select Data Protection > Cluster Pairs.
2. Select Pair Cluster.
3. Select Start Pairing and then click Yes to indicate that you have access to the remote cluster.
4. Enter the remote cluster MVIP address.
5. Click Complete Pairing on the Remote Cluster.

6. In the authentication window that opens, enter the cluster user (admin) name and password.

7. Access the remote cluster and select Data Protection > Cluster Pairs.

8. Click Pair Cluster.

9. Click Complete Pairing.

10. Click the Complete Pairing button.

7.2 Pairing Clusters by Using a Pairing key

When admin access is available for only one cluster, two clusters can be paired by using a pairing key. A pairing key is created on the local cluster and is then sent to the remote cluster. Here is the method for creating a pairing key on one cluster:

1. On the local cluster, select Data Protection > Cluster Pairs.
2. Click Pair Cluster.
3. Select Start Pairing and then select No to indicate that you do not have access to the remote cluster.

4. Click Generate Key.

5. Copy the cluster pairing key.
6. Make the pairing key accessible to the remote cluster admin. Be careful not to alter the characters of the remote pair key.

7. On the remote cluster, select Data Protection > Cluster Pairs.
8. Click Pair Cluster.
9. Click Complete Pairing and enter the pairing key in the Pairing Key field.
10. Click Complete Pairing.
7.3 Validating Paired Clusters

The pairing status is validated by checking the cluster pair connection status on each of the two clusters. Select Data Protection > Cluster Pairs.

8 Volume Pairing Walkthrough

On the Data Protection > Volume Pairs page, you can access information about volumes that have been paired or are in the process of being paired.

The volume that is selected as a target should be configured as the replication target, as shown in the following steps:

1. Click the management button on the SolidFire dashboard to list all volumes.

2. Select the volumes to configure as targets. Click the Actions tab associated with the volume.

3. From the Access drop-down list, configure the target as a replication target.
Warning: If the target is not configured as a replication target, then the volume pairing displays the warning PausedMisconfigured. When the target volume is configured as a replication target, the remote replication process changes to the active state.

9 Recovery Point Objective and Recovery Time Objective

A replication architecture depends on business requirements. The parameters that define the business requirements are maximum permissible data loss, speed of recovery, and application timeout. The speed of recovery depends on the network architecture between the source and replicated nodes. Several scenarios should be considered, including different types of packet delays, application delays, and packet loss. The network architecture affects the time of recovery and the cost of the infrastructure.

9.1 Recovery Time Objective

The recovery time objective (RTO) is defined as the maximum time that can elapse before recovering an application. This value varies depending on the business requirements. The RTO varies from a few seconds to a few minutes, based on the use case and data being stored. The RTO of remote replication depends on the following factors:

- Volume recovery
- Switching the target volume to the source volume through API calls (takes approximately 5 seconds)
- Detecting the network failure

9.2 Recovery Point Objective

The recovery point objective (RPO) is defined as the maximum permissible data loss. In the context of a database, the amount of log data that can be lost defines the RPO.
Network Sizing Requirements for Synchronous Replication

In the case of synchronous replication, the RPO is zero. The following factors affect the networking design of synchronous replication.

Latency

Latency is the amount of time required for a single write to reach the target cluster. It is also the amount of time the write acknowledgement takes to return to the source cluster. As the distance between the source and target increases, the round-trip time increases as well. Therefore, this distance is the factor that limits the number of I/Os per second.

In addition to the latencies induced by distance, other latencies are introduced by the networking equipment. The latency plays a major role in determining the IOPS performance on both sides. The speed of the write signal determines the latency in the fiber cable. The speed of an electric signal in an optical fiber is 200,000kmps. To complete a successful write operation, the signal must travel the distance between the source and target twice. The theoretical maximum possible I/O is calculated as:

\[
RTT = \frac{2 \times \text{distance}}{200,000 \text{kmps}}
\]

\[
1 \text{s} / RTT = \text{max number of IOPS}
\]

For a distance of 10 miles between the source and target, the maximum number of IOPS achieved is 6,250. As the number of network elements between the source and target increases, the RTT increases and effectively reduces the maximum number of IOPS.

Bandwidth

Bandwidth plays an important role during the initial metadata and blockdata sync between the volumes. As the size of the data increases, higher bandwidths are required to perform the metadata and blockdata sync in shorter periods of time. Bandwidth plays another important role in syncing the metadata after pausing and resuming replication. Table 3 shows the time required for performing the data sync over different bandwidth links.

<table>
<thead>
<tr>
<th>Data Size</th>
<th>DS1 (1.544Mbps)</th>
<th>DS3 (44.76Mbps)</th>
<th>OC-1 (54.8Mbps)</th>
<th>OC-3 (155.52Mbps)</th>
<th>OC-12 (622 Mbps)</th>
<th>OC-48 (2.4 Gbps)</th>
<th>OC-192 (9.6 Gbps)</th>
<th>10Gbps Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>50GB</td>
<td>72.5</td>
<td>2.48</td>
<td>2.16</td>
<td>0.76</td>
<td>.178</td>
<td>0.048</td>
<td>0.016</td>
<td>0.0111</td>
</tr>
<tr>
<td>1TB</td>
<td>1430</td>
<td>49.7</td>
<td>43.2</td>
<td>14.3</td>
<td>3.57</td>
<td>.926</td>
<td>.231</td>
<td>.222</td>
</tr>
</tbody>
</table>

Network Sizing Requirements for Asynchronous Replication

In asynchronous replication, the RPO is defined by the delay introduced. The factors that influence RPO are the size of outstanding data, the rate of change, and the bandwidth. The bandwidth should be designed to resynchronize the outstanding data within a six-hour period. After the six hours, the cluster raises a cluster fault. The following factors should be considered in defining the network:

- The maximum round-trip time latency for asynchronous mirroring is eight seconds.
- NetApp recommends using a 10Gbps link (or more) for efficient performance.
- NetApp recommends using a dedicated storage network for replicating traffic.
Network Sizing Requirements for Snapshot-Based Replication

When using snapshot-based replication along with synchronous or asynchronous replication, snapshot replication is given the primary preference. Synchronous or asynchronous replication is always performed prior to snapshot replication.

The RPO of snapshot-based replication is affected by the following factors:

- The snapshot time interval
- The size of the dataset
- The bandwidth connecting the source and target clusters

To determine the RPO, the resynchronization time required to replicate the snapshot on the target must be considered. From the point of completely synchronizing the existing snapshot until the new snapshot arrives, new writes are not delivered to the target. These new writes are not protected until the target is resynchronized with the new snapshot. Replication time (RT) is defined as the time taken to replicate the snapshot. The RPO can be defined in terms of the synchronization interval (SI) and the RT as follows:

\[(SI + \text{discovery timer (0-60)s + RT}) <= \text{RPO}\]

The synchronization interval should be greater than the RT.

If \(SI + \text{discovery timer (0-60)s} = \text{RPO}\), then the RT is zero. However, an RT of zero is not possible. If the available bandwidth is low and shared between multiple systems, then the RT might be a few seconds, depending on the bandwidth. The discovery timer is the time taken by the target cluster to detect a snapshot being created on the source. The value of the discovery timer varies from 0s to 60s. In the case just described, the RPO is calculated as follows:

Assuming that the SI is set to 5min and the replication time is \(x\) ms, then:

\[SI \text{ (5min) + discovery timer (0-60)s + RT (} x \text{ ms} = \text{RPO (5min + (0-60)s + x ms)}\]

Network Sizing for Minimizing the Replication Time

The RT duration depends on the number of changes made during the synchronization interval and the bandwidth connecting the target cluster and the source cluster. The bandwidth must be chosen such that the expected maximum number of changes can be replicated on the target within the synchronization period. The RT can be calculated if the administrator knows how much data must be synchronized over a synchronization interval.

Consider an example RT calculation. If a dataset is approximately 30TB in size and 10% changes during a peak business day, then 3TB of data must be transferred to the target cluster. Assume that 15% of this changed data occurs during the peak business hour of that day. Therefore, the total amount of data that must be transferred during that single hour is 45GB.

If the link between the source and target cluster is 10Gbps, then the 45GB of data change requires 400s (RT) to replicate the snapshot. To have a lower RT, a higher bandwidth must be used.

10 Summary

NetApp SolidFire provides an efficient method for data protection through various types of replication. Replication is an easier way to meet the business requirements of RPO and RTO in the case of shared bandwidth and long-distance replication. Replication offers a perfect solution for businesses that must protect their data in a simple, performance-efficient, and low-cost manner.
Appendix A: TCP Port Requirements

Table 4) TCP port requirements for replication.

<table>
<thead>
<tr>
<th>Port type</th>
<th>Port number</th>
<th>Usage of port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td></td>
<td>Cluster-to-cluster latency</td>
</tr>
<tr>
<td>TCP-HTTP</td>
<td>2181</td>
<td>Remote replication cluster communication takes place through these ports</td>
</tr>
<tr>
<td>TCP-RPC</td>
<td>4000-4020</td>
<td>Data communications between nodes</td>
</tr>
<tr>
<td>TCP-HTTPS</td>
<td>442</td>
<td>Node access to cluster</td>
</tr>
<tr>
<td>TCP-HTTPS</td>
<td>443</td>
<td>Remote replication for cluster communications; all node IPs and MVIPs</td>
</tr>
</tbody>
</table>

Appendix B: Remote Replication States and Explanation

This appendix describes the various volume states.

**Message: Paused Disconnected**

This message is displayed on both the source and the target, indicating that source replication or sync remote procedure calls are timed out. Connections to the remote cluster have been lost. The network connections to the remote cluster must be checked.

**Message: Resuming Connected**

This message is displayed on both the source and the target, indicating that replication sync is now active. It also notifies the user that the sync process is beginning or resuming and that the target is waiting for data.

**Message: Resuming RR Sync**

This message is displayed on both the source and the target, indicating that a single-helix copy of the volume metadata is being transferred to the paired cluster.

**Message: Resuming Local Sync**

This message is displayed on both the source and the target, indicating that a double helix copy of the volume metadata is being transferred to the paired cluster.

**Message: Resuming Data Transfer**

This message is displayed on both the source and the target, indicating that data transfer has been resumed.

**Message: Active**

This message is displayed on both the source and the target, indicating that volumes are paired, data is being sent from the source to the target, and both volumes are in sync.
Volume Pairing Warnings

See the NetApp SolidFire Element OS User Guide.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NetApp SolidFire Element OS User Guide
  https://fieldportal.netapp.com/content/531671
- SANtricity OS 11.40 Synchronous and Asynchronous Mirroring

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>April 2018</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2018 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.