Abstract

This reference architecture evaluates the best-in-class performance and scalability delivered by Dell EMC XtremIO X2 for automated disaster recovery of virtualized workloads using Dell EMC™ XtremIO X2 Native Replication, Dell EMC™ XtremIO X2 SRA, and VMware® Site Recovery Manager™ with varying levels of consistency.

June, 2018
## Abstract

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Executive Summary

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Introduction

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## XtremIO X2 Native Replication Overview

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Understanding XtremIO Asynchronous Replication

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Conventional Replication Products

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Topologies

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## How it Works in an Emergency

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Terminology

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Features and Benefits of VMware Site Recovery Manager:

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Deployment and Configuration

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Configuring XtremIO Data Protection Sessions for vSphere SRM

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Storage Replication Adapter

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Downloading and Installing EMC® XtremIO Storage Replication Adapter

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Upgrading Existing Installation of XtremIO X2 Adapter for VMware SRM

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Initial SRM Configuration

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |

## Configuring the XtremIO Array Based Native Replication

| Dell EMC XtremIO X2 Native Replication Adapter for VMware Site Recovery Manager |
Executive Summary

Critical business processes require data replication for various purposes such as data protection or production environment duplication for development, testing, analytics or operations.

Data replication over the wire requires many customers to compromise either on RPO (Recovery Point Objective) or bandwidth cost for transferring the high throughput generated by the applications. This is even more acute with All Flash Array high throughput.

While there are several approaches for replication, they all fundamentally struggle with RPO, limited performance and complex operational processes, forcing customers to make tradeoffs between RPO and cost.

XtremIO leverages its unique content addressable storage, in-memory metadata and copy data management implementation to offer the most efficient solution by replicating unique data only. This unique implementation significantly reduces bandwidth and storage array utilization. Furthermore, XtremIO simplifies the replication management for all use cases.

Data center consolidation by way of x86 virtualization is a trend that has gained tremendous momentum and offers many benefits. Although the physical nature of a server is transformed once it is virtualized, the necessity for data protection remains. Virtualization opens the door to new and flexible opportunities in data protection, data recovery, replication, and business continuity. This document offers best practices for automated disaster recovery of virtualized workloads using Dell EMC™ XtremIO X2 all flash arrays, native replication, and VMware® Site Recovery Manager™ (SRM) with varying levels of consistency.

Dell EMC® XtremIO Storage Replication Adapter for VMware Site Recovery Manager (SRA) allows VMware SRM to implement disaster recovery for XtremIO clusters. Dell EMC® XtremIO SRA supports SRM functions such as failing over, failing back, and failover testing using XtremIO XMS as the replication engine.
Introduction

VMware SRM is an extension to VMware vCenter that provides disaster recovery, site migration and non-disruptive testing capabilities. It is fully integrated with VMware vCenter Server and VMware vSphere™ Web Client.

SRM works in conjunction with XtremIO X2 Native to automate the process of migrating, recovering, testing, re-protecting and failing-back virtual machine workloads.

SRM coordinates the operations of the VMware vCenter Server™ at two sites. This allows virtual machine copies at a recovery site to start up as the primary virtual machines at the protected site are shut down. By using the data replicated from the protected site, these virtual machines assume responsibility for providing the same services.

This paper provides configuration examples, tips, recommended settings, and other storage guidelines to be used while integrating VMware® Site Recovery Manager™ with Dell EMC XtremIO X2. In addition to basic configuration, this document also answers frequently asked questions about VMware interactions with SRM.

Dell EMC advises reading the Site Recovery Manager Documentation provided on vmware.com before beginning an SRM implementation.
XtremIO X2 Native Replication Overview

Conventional Replication Products

Conventional replication products use different mechanisms that are streaming or snapshot based. When sending the data over the wire, the bandwidth requirements for such solutions require the customer to either compromise on RPO or increase the bandwidth cost to allow copying all the changes.

The reason for this is that with conventional solutions, all changes need to be replicated. For example, in Figure 1 data is replicated from Array 1 in primary site to Array 2 in DR (Disaster Recovery) site. When a new, non-unique block "A" is written to address "4" in Array 1, it will be fully replicated to the remote array even though the same data already exists in address location "1" as shown in Figure 2.

This means that all data changes are fully replicated on the wire, causing the following:

- The bandwidth needs to be sized according to all changed data.
- The performance of the arrays on both sides are impacted by replicating all data changes. The source array reads the data and transfers it to the remote array, and the remote array receives all the changed data and writes it to the drives.
Understanding XtremIO Asynchronous Replication

XtremIO replication leverages a unique content-based storage architecture to reduce bandwidth utilization. XtremIO stores only unique data at the array physical layer, and manages volume information at the logical layer, also called in-memory metadata. For more information, see the Introduction to Dell EMC XtremIO X2 Storage Array white paper.

Every data block that is written in XtremIO is identified by a fingerprint that is kept in the data block's metadata information. When the fingerprint is unique, the data block is physically written and the metadata points to the physical block. When the fingerprint is not unique, it is kept in the metadata and points to an existing physical block.

A non-unique (deduplicated) data block that already exists on the target array is not sent again. Instead, only the block metadata is replicated and updated at the target array.

For example, in Figure 3 a new block "D" is added to address 6. Block "D" already exists at address "5" and was already replicated to the array at the DR site.

![Figure 3. Non-Unique Block "D" Written to Address "6"](image)

When a non-unique block is written to the source array, XtremIO replication will not replicate the data, but rather will update the metadata at the target array to point to the physical block that already exists on the target array.

In Figure 4, the metadata at the DR array is modified to point to the unique block "D" that is already stored at the physical layer of the DR array. Instead of replicating the full data block, XtremIO efficiently replicates only the metadata.

![Figure 4. Address "6" Modified to Point to Block "D"](image)
XtremIO Replication Efficiency and Benefits

The following sections describe unique XtremIO capabilities which provide replication benefits and improved efficiency.

**Deduplication and Compression**

For every changed data block, XtremIO replication checks if its fingerprint exists at the target array. If the fingerprint already exists, only the metadata is updated at the target and no data is sent.

In case of a new unique block with no previous fingerprint, the source replicates the full compressed data block.

This efficient replication is not limited per volume, per replication session or per single source array, but is a global deduplication technology across all volumes and all source arrays.

XtremIO deduplication is inline, always-on, and is not sensitive to the cluster's utilization, thus making it the most efficient replication technology in the market.

**Changes Only**

XtremIO replication is based on a snapshot shipping method. Snapshots at the source are created at a frequency derived from the RPO setting of the protection session (called Cycle). Snapshots are efficiently transferred (shipped) to the target site. In each cycle, a new snapshot is created and XtremIO calculates the changes between the last 2 snapshot-sets at the source, and transfers the changes to the target array where it is merged with previous data. This mechanism essentially means that only changes between cycles are transferred to the target, thus providing additional operational efficiency.

**Write Folding**

In many cases, applications repeat writes to specific addresses of the volumes. These addresses are called "hot spots". In streaming based replication technology, when the replication granularity is per a single IO, all write I/Os need to be replicated individually and in the same order even if they are written to the same address. However, in XtremIO snapshot-based replication, for every snapshot, only the last write I/O to every address determines the data that needs to be replicated. In this way, write I/Os that were overwritten are not replicated. This is called "Write Folding", and it reduces the amount of data that needs to be replicated.

The greater the time between replication snapshots, the larger the savings which can be obtained from Write Folding.

**Replication Benefit Summary**

Based on all the above capabilities, XtremIO replication provides the following benefits:

- The bandwidth required on the wire is based only on the unique changed data.
- Data is sent compressed over the wire.
- Only unique data blocks, at either the source or target array, need to be replicated.
- Only data block changes between subsequent cycles, and not the complete block, need to be replicated.

For a typical DRR of 4:1, only one quarter of the bandwidth needs to be sent over the wire, thus the bandwidth savings is 75%.
Replication Flow

XtremIO Asynchronous Replication uses snapshot-shipping method to replicate crash-consistent copies to the remote array.

On the source cluster, XtremIO capabilities are used to create crash-consistent virtual copies, and to calculate the difference between two consecutive virtual copies. The copy creation and diff commands are performed fully in-memory and therefore are done at memory speed.

The replication flow is as follows:

1. When replication starts, a full copy is performed to ensure that the production and the target are identical. To perform the full copy, XtremIO replicates the first snapshot-set to the target cluster. The data is sent efficiently, and only unique blocks are sent (compressed) over the wire. This initialization phase is shown in Figure 5:
   - Step 1 – First snapshot created.
   - Step 2 – Only unique blocks sent compressed.
   - Step 3 – Snapshot stored at target.

2. For every subsequent cycle, a new snapshot-set is created at the source and only the differences between the previous snapshot-set and the current snapshot-set are sent to the target cluster. The difference between the snapshot-sets reflects all the blocks that were changed between the 2 cycles and that need to be replicated. The unique data is sent compressed.
   - Each new snapshot-set is consistent across all volumes in the consistency group. XtremIO compares the metadata of the current snapshot-set to the metadata of the previous snapshot-set to determine the differences. It then gets the fingerprints of the changed blocks and checks if the same fingerprint exists at the target array. If the fingerprint exists, the metadata is updated at the target. If it does not exist, the data is read and sent compressed to the target array.

3. On the XtremIO target array, a new snapshot-set is created to which the incoming data is written. When replication of the snapshot-set delta is completed, the snapshot-set that is received from source becomes the latest snapshot at the target array and is available for the DR host. When the snapshot-set becomes available to the DR host, the previous snapshot-set at the source array can be deleted. Figure 6 shows the steps in these subsequent phases:
   - Step 1 – A new snapshot is created.
   - Step 2 – Changes between the current and previous snapshot are calculated.
   - Step 3 – Only unique blocks are sent compressed.
   - Step 4 – The new snapshot is merged and stored at the target.
4. The trigger for starting a new cycle depends on the RPO settings specified by the user for the protection session. The RPO in XtremIO can be as low as 30 seconds and up to 24 hours. XtremIO will attempt to meet the required RPO and will start a new cycle halfway through the desired RPO. For instance, if the RPO is set to one minute, XtremIO will start a cycle every 30 seconds to ensure compliance with the replication RPO.

- In case there are many changes or packet losses on the wire which cause a new time interval to pass before the previous cycle has finished, the new cycle will start on completion of the previous one. A longer interval results in more efficient data transfer, because of Write-Folding, where a single, final write replaces multiple writes to the same location in the same cycle at the source volume.

5. XtremIO automates the cycle of creating a new snapshot-set at the source, sending the changes to the target array, creating a new snapshot-set at the target, and deleting the snapshot-set from the source. The process is repeated indefinitely.

Retention Policy

The protection window and the maximum number of snapshot-sets that XtremIO keeps are determined by the Retention policy. The maximum snapshot-sets per protection session is 500 (for the initial version; please check the Release Note for the latest scalability numbers).

The retention policies are defined once and can then be used by multiple protection sessions.

The retention policy specifies:
- The Required Protection Window
- The number of snapshot-sets that will be kept within the protection window

For example, for a Production Consistency Group, a user can create a "Gold" policy, with a short protection window of 30 snapshots for 60 minutes, a medium protection period of 23 snapshots for 23 hours, and a long protection period of 2 snapshots for 2 days. This essentially means your production consistency group has a PIT every 2 minutes for the first 60-minute period, a PIT every 1 hour for the next 23 hours, and a PIT per day after that.

A Silver policy, for Test/Dev, may use a single long period window of 1 snapshot per day for a week.
The Required Protection Window is specified by the user; from a short period of minutes to a long period of up to one year.

In addition, with XtremIO the protection window can be split to 1 to 3 time-periods with different number of snapshot-sets and different granularity.

XtremIO automatically manages the retention of the snapshot-sets according to the retention policy settings. In case the protection window settings or the number of snapshot-sets is changed, XtremIO will automatically adhere to the new retention policy settings.

The retention of snapshot-sets runs:

- As per Retention Policy executed every 5 seconds.
- At the end of a replication cycle.
- Whenever the retention policy settings are updated.

When the protection session is suspended, the retention policy is suspended as well, and the system will not delete any snapshot-sets. This will allow the user to test the snapshot-sets at the target when recovery is required and prevents any snapshot-set deletion until a decision is made regarding the use of the snapshot-sets for recovery.
Accessing a Snapshot-Set at the Target

Accessing the snapshot-sets at the target is required for the following use cases:

- **Permanent:**
  - When near-instantaneous disaster recovery or testing are required
  - Repurposing copies and environments
- **Temporary:**
  - Technology refreshes
  - System upgrades
  - Data center moves or expansion
  - Production data migration to a target array

When replicating to the remote array, the volumes at the remote site must be defined as read-only or no-access mode depending on user preference for the host access on that site. In the event of a failover, the volumes at the remote site are changed to read-write.

Refresh Capability

XtremIO provides the option to refresh the data of a host volume from any PIT (Point in Time) that exists in the system. The refresh can be done from any PIT snapshot-set that was created for protection. The refresh operation is instantaneous, as the refresh operation is a metadata operation that is done completely in-memory. The refresh operation doesn’t require any metadata copy or roll-forward/backward of any data or metadata. The refresh doesn’t change the SCSI personality of the volume and therefore is transparent to the host. Thus, there is no need to perform any mapping or scanning operation for the data to be accessible to the host.

The refresh operation performs the following steps:

1. Create a virtual copy from the snapshot-set used for the refresh.
2. Change the host volume to point to the newly created virtual copy, as shown in Figure 8.

![Figure 8. Host Volume Points to Data Container Including Metadata Information](image-url)
When the data of the host volume needs to be restored or refreshed from a virtual copy, the refresh operation will just update the host volume to point to the new virtual copy data, as shown in Figure 9.

![Figure 9. Refresh Operation](image)

**Testing a Snapshot-Set**

Testing a remote replica is required to validate that all data is fully and correctly replicated. Testing a snapshot-set at the target arrays is instantaneous, using a single command. All that is required is that the snapshot-set which contains the desired PIT be promoted to be the volume of the DR-host. While the host accesses the new PIT replica, snapshot-sets continues as usual, adhering to the RPO.

Testing the snapshot-set at the remote host is not limited by time and can therefore be used indefinitely. This is very useful when extensive testing of a replication snapshot-set is required.

During a test scenario, the volumes at the remote site are switched from No-Access/Read-only to Read-Write. However, when testing of a snapshot-set is completed, the access-mode of the target volumes changes back to read-only, and all the data written to the target volumes are discarded. To keep the data of a tested copy, a protection-copy of the target needs to be taken prior to the finish-test-copy command.

Any target snapshot-set can be used for testing. When the user selects a snapshot-set, XtremIO provides access to a copy of the selected snapshot-set, thus the original protection copy is not affected.

The test-copy operation is performed by using the "Refresh" capability as described above.

Before finishing the test copy, host applications accessing the copy must be shut down and the file-system must be unmounted. The test-copy-finish command removes write-access from target volumes to prevent data corruption on the next test-copy or failover operations.

**Failover**

When performing failover, the replication direction is reversed. The target Consistency Group and target volumes become the production, and the production volumes of the consistency group become the target volumes. As part of the failover command there is an option to start the replication in the reverse direction immediately after switching sides. When the replication to the new target (original production) is started, a full check is performed which will check the whole volume. But replications will only be made of the differences between the source and the target volumes. These differences are calculated by matching the fingerprints between the source and target snapshot-sets.
After failover, the previous snapshot-sets are deleted. To keep the snapshot-sets, create a protection copy where needed.

Failover to the target site can be done on demand with or without first using a "Test snapshot-set" operation. When a snapshot-set is mounted using the Test snapshot-set option, the user can run some recovery procedures on the host. Upon completion, the user can decide whether or not to use the current mounted data for the failover.

XtremIO supports all failover scenarios including "Planned Migration" (sync-and-failover) and "Disaster Recovery" to any PIT at the target. The failover operation for "Disaster Recovery" scenarios with XtremIO is instantaneous and requires no metadata copy, log roll-forward or log roll-backward.

The following diagrams represent the failover process.

1. **Figure 10** shows the initial state at the DR site.
   - Volumes are mapped and visible to the DR host.
   - Write-access is disabled to the DR host volumes.
   - Multiple Point-in-Time Copies exist on the target.

   ![Figure 10. Initial State at DR Site](image)

2. When a failover needs to be performed, select the PIT copy for failover, and execute the failover command, as shown in **Figure 11**.

   ![Figure 11. PIT Selection](image)
3. The failover command creates a copy from the selected PIT copy and uses the "Refresh" capability to change the host volume to point to the new created copy as shown in Figure 12.

![Figure 12. Failover to Selected Copy](image)

Because promoting a snapshot-set to the target host is essentially instantaneous, near-zero recovery time objective (RTO) is possible when failing over, regardless of the selected point-in-time.

**Cleanup Flows**

At the end of a recovery incident, a cleanup process should be performed to delete unnecessary snapshots. Key aspects of the cleanup are as follows:

- Removing a protection session removes all protection session snapshot-sets from both the source and target clusters.
- Terminating a protection session removes the corresponding auto-created snapshot-set from the source cluster. User-created snapshot-sets (protection copies that were taken on the replication snapshot-set) will not be removed. Terminating the replication session will perform a metadata-aware full-copy when the protection session will be restarted. After the first replication, when a full sweep is needed, there is a good chance that the copy at the target is similar to the production so most of the data does not need to be transferred.
- Removing snapshot-sets from the target allows clean-up of the protection window at the target cluster.
- On Failover, when the source cluster is accessible, failing over to the target cluster triggers a swap. The source cluster volumes change to read-only/no-access mode, and the cluster switches identity from source cluster to target cluster. Similarly, the volumes at the target cluster change to Read-Write, and change identity from target cluster to source. When the source cluster is inaccessible, it is possible to failover all applications to the target cluster (thus making it the source cluster), but the original source cluster cannot be changed to target. This creates a "split brain" situation, in which there are two source clusters. In such a situation, some applications may still write to the original source cluster even after the target cluster has become the new source.
- When connection between the clusters is restored, the user needs to determine which of the clusters will function as the source (i.e. which cluster data should be used) before initiating replication. The data of the target volumes will be discarded. To preserve the data on the new target, use the create-protection-copy command on the target prior to executing the failover-cleanup command.
DR Host Volumes Accessibility

With XtremIO, the target volumes are inaccessible by default. The access mode for the target volumes can be defined in the protection session. There are 2 access modes for the target volumes: "read-only" and "no-access". The default value is "read-only".

The target-volume access mode is changed to read-write in the following scenarios:

- When testing a snapshot set at the target host
- When a failover is performed
- When the volumes are removed from the protection session

Capabilities

XtremIO Metadata-Aware Replication provides the following capabilities:

- **Best RPO** – As low as 30 seconds.
- **Performance** – Support for All Flash Array high performance workloads.
- **Efficiency** – Only unique data is sent over the wire. The data is sent compressed.
- **Changes Only** – Only changes between cycles are replicated. Resuming the replication is always incremental and is not impacted by communication failures.
- **Many PITs at the Target** – Hundreds of PITs can be kept at the target and can be used for failover or repurposing.
- **Best RTO** – Failover or test a PIT at the target is instantaneous and does not require any roll forward or metadata copy. DR Host can be easily recovered, while preserving all SCSI information (thus eliminating the need for SCSI-BUS rescan on the host side).
- **Full Support of DR Operations** – Such as test copy to any PIT, failover, and failback.
- **Bi-Directional** – XtremIO supports bi-directional replication, replicating one CG from Array "A" to Array "B" and a different CG from Array "B" to Array "A".
- **Fan-In Support** – Replicating from multiple clusters to a single target cluster benefits from global dedupe with XtremIO replication.
- **Fan-Out Support** – Replicating different CGs to different remote clusters.
- **Retention Policy Management** – The system automatically manages the PITs at the target according to the Retention Policy.
XtremIO Native Replication Integration with VMware Site Recovery Manager

When disaster occurs, administrators must switch IT operation from one location to the other. Such switching typically relies on the technical competence of the administrator to handle the many dependencies in the sequence. Further, an emergency plan needs to be generated and tested to prove that the switchover will work reliably. But such action causes many issues particularly as there is a reluctance to touch the running systems. The result in many cases is theoretical plans which have never been tested in the real operational environment. Also to be taken into account is the experience of the administrators, who, under stress from the disaster, may make mistakes, and compound the problem.

Features and Benefits of VMware Site Recovery Manager:

SRM simplifies and automates the key elements of disaster recovery: setting up disaster recovery plans, testing of those plans, executing failover when a datacenter disaster occurs, and failing back to the primary datacenter. Key benefits of SRM include:

- Application-agnostic protection eliminates the need for app-specific point solutions.
- Automated orchestration of site failover and failback with a single-click reduces recovery times.
- Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives.
- Centralized management of recovery plans from the vSphere Web Client replaces manual runbooks.
- Planned migration workflow enables disaster avoidance and data center mobility.
- Support for array-based replication offers options for asynchronous/synchronous replication with zero data loss.
- Self-service, policy-based provisioning via Storage Policy Based Protection Groups, VMware vRealize Orchestrator and VMware vRealize Automation automates protection.

From the vCenter Web Client, all actions can be monitored and managed. This gives administrators end-to-end control of the process. They can calmly prepare the emergency plan, test it and improve it where necessary without any impact on the operational systems. All actions are logged and available for audit. Furthermore, it becomes much easier to define recovery times in advance of any action. The complete set of processes needed following a disaster can be automated and tested, providing administrators with familiarity in use of all procedures.

Terminology

- Recovery time objective (RTO): Targeted amount of time in which a business process should be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity.
- Recovery point objective (RPO): Maximum age of files recovered from backup storage for normal operations to resume if a system goes offline as a result of a hardware, program, or communications failure.
- Consistency group: One or more LUNs or volumes that are replicated at the same time. When recovering items in a consistency group, all items are restored to the same point in time.
- Protected site: Site that contains protected virtual machines.
How it Works in an Emergency

Once VMware vSphere is deployed on the protected and recovery sites, disk array-based replication is established between the two sites. SRM is then used to create disaster recovery plans that designate failover instructions. In the event of a disaster, administrators are notified, enabling them to decide whether to initiate a failover. Once they initiate a failover, SRM implements the disaster recovery plan following four basic steps:

1. First, on the Protected Site, SRM shuts down the virtual machines starting with those designated as lowest priority. Failover does not require connectivity to the protected site, so if SRM cannot connect to the site, it simply notifies the administrator that it cannot power down the virtual machines and proceeds to the next step.

2. Then, at the recovery site, SRM prepares the datastore groups for failover.

3. Next, SRM suspends all virtual machines running on the recovery site designated as non-critical. This provides more resources for the virtual machines to be powered on at the recovery site.

4. Finally, SRM restarts the virtual machines at the recovery site starting with the virtual machines designated as highest priority.

Topologies

Dell EMC XtremIO X2 Native Replication and VMware Site Recovery Manager can be used in a number of different failover scenarios depending on customer requirements, constraints and objectives. All of these arrangements are supported and easily configured from the XMS and the vSphere Web Client.

Active-Passive

In the traditional active-passive scenario, there is a production site running applications and services and a secondary or recovery site that is idle until needed for recovery. This topology is common and though it provides dedicated recovery resources, it means paying for a site, servers and storage that aren't utilized much of the time.

Active-Active

Site Recovery Manager can be used in a configuration where low-priority workloads such as test and development run at the recovery site and are powered off as part of the recovery plan. This allows for the utilization of recovery site resources as well as sufficient capacity for critical systems in case of a disaster.

Bi-directional

In situations where production applications are operating at both sites, SRM supports protecting virtual machines in both directions (e.g. virtual machines at Site A protected at site B, and virtual machines at site B protected at site A).

Multi-Site

Shared Recovery:

To be used where multiple remote sites are protected by a single recovery site.

Shared Protection:

To be used where failure of a single site results in some applications/virtual machines moving to one remote site, while others move to one or more additional remote sites.

This reference architecture describes the most common configuration; the traditional active-passive scenario in which there are source and target sites, each connected to a dedicated XtremIO X2 single X-Brick.

This reference architecture is based on SRM 8.1 and vSphere 6.7. But it is important to note that the XtremIO SRA plugin provides backward compatibility starting from SRM version 5.8 and vSphere version 5.5.
Site Recovery Manager 8.1 is deployed in a paired configuration, for example, protected site and recovery site. The Site Recovery Manager 8.1 software is installed on a Microsoft Windows server at both sites. It supports multiple versions of vCenter at either site. There must be one or more vSphere hosts running version 6.0 or higher at each site. See the Compatibility Matrixes for Site Recovery Manager 8.1 for specific details.

Figure 13. Active/Passive SRM Architecture with XtremIO X2 Storage Based Replication
Deployment and Configuration

The following sections detail the procedures for a typical deployment of Dell EMC XtremIO X2 arrays into an existing SRM environment.

Naming conventions used in the example deployment have been designed to highlight the relationship of components within a given SRM protection group. Folder name, datastore name, protection group name, and recovery plan names are all suffixed with a numeric value to demonstrate the relationship between each of these components. Users are encouraged to implement a naming convention that aligns with their own organizational requirements.
Configuring XtremIO Data Protection Sessions for vSphere SRM

Registering the Peer XMS

All configuration and setup actions are managed and orchestrated by XtremIO Management Servers. To allow the configuration, XMSs on both sides must communicate with each other. Communication is enabled by registering the remote XMS with the local XMS. The registration is required only in one side and the information is propagated to the remote XMS.

The following procedure should be performed for each peer XMS.

To register a peer XMS:
1. From the top menu bar, select System Settings > Remote Protection Settings to open the Remote Protection Settings window.
2. From the Remote Protection Settings menu, select the XMS Peers option.
3. In the XMS Peers table menu, click New to open the Register XMS dialog.
4. Provide the XMS name, IP address and credentials.
5. Click Register XMS.

Figure 14. XMS Registration Tab

Configuring the IP Links

Data replication requires IP links for communication between the clusters.

At least two IP links are required for HA. If necessary, you can define more IP links according to the required replicate throughput.

Only a single IP link can be configured per port. Therefore, to replicate to two remote clusters at least four ports are required.
To configure an IP link, use the following procedure:

1. From the top menu bar, select System Settings > Remote Protection Settings to open the Remote Protection Settings window.

2. From the Remote Protection Settings menu, select the IP Links option.

3. In the IP Links table menu, click New to open the IP Link Settings wizard.
4. Select a remote cluster from the list and click next.

![Remote XtremIO Cluster Selection](image1)

**Figure 18.** Remote XtremIO Cluster Selection

5. Define target pairs by selecting a local IP from the Local Targets table and a remote IP from the Remote Targets table. Click Link; the new links are displayed in the IP Links table.

![Links Pairing](image2)

**Figure 19.** Links Pairing

6. Click Next to display the Summary window.

![Summary Window](image3)
7. Confirm the defined IP linked in the IP Links table and click Apply.

![Figure 20. IP Links Settings Summary](image)

### IP LINKS Settings Summary

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Source IP</th>
<th>Target Port</th>
<th>Target IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10/24</td>
<td>X1-SC1-target1</td>
<td>192.168.1.10/24</td>
<td>X1-SC1-target1</td>
</tr>
<tr>
<td>192.168.1.11/24</td>
<td>X1-SC2-target1</td>
<td>192.168.1.11/24</td>
<td>X1-SC2-target1</td>
</tr>
</tbody>
</table>

![Figure 21. IP Link Status](image)

### IP Link Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Cluster</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Target Cluster</th>
<th>Target Address</th>
<th>Target Port</th>
<th>IP Link State</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>xbrickdmm3115-xbrickdmm3115</td>
<td>X1-SC1</td>
<td>192.168.1.50/24</td>
<td>X1-SC1-target1</td>
<td>xbrickdmm3110</td>
<td>192.168.1.60/24</td>
<td>X1-SC1-target1</td>
<td>Up</td>
<td>Enabled</td>
</tr>
<tr>
<td>xbrickdmm3115-xbrickdmm3115</td>
<td>X1-SC1</td>
<td>192.168.1.51/24</td>
<td>X1-SC1-target2</td>
<td>xbrickdmm3110</td>
<td>192.168.1.61/24</td>
<td>X1-SC1-target2</td>
<td>Up</td>
<td>Enabled</td>
</tr>
<tr>
<td>xbrickdmm3115-xbrickdmm3115</td>
<td>X1-SC2</td>
<td>192.168.1.52/24</td>
<td>X1-SC2-target1</td>
<td>xbrickdmm3110</td>
<td>192.168.1.62/24</td>
<td>X1-SC2-target1</td>
<td>Up</td>
<td>Enabled</td>
</tr>
<tr>
<td>xbrickdmm3115-xbrickdmm3115</td>
<td>X1-SC2</td>
<td>192.168.1.53/24</td>
<td>X1-SC2-target2</td>
<td>xbrickdmm3110</td>
<td>192.168.1.63/24</td>
<td>X1-SC2-target2</td>
<td>Up</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

---

**Creating a Remote Protection Session**

The next step is creating a Remote Protection Session for a Consistency Group.

Note: Creating a Remote Protection Session requires that Consistency Group and Volumes be already defined in the cluster.

Note: A Consistency Group or Volume cannot be included in more than one Remote Protection Session.
To create a Remote Protection Session, use the following procedure:

1. From the navigation menu, select Data Protection to open the Data Protection window.

2. If there are multiple clusters, select the relevant cluster by clicking View Details in the clusters summary window.

3. Launch the Create Remote Protection Session wizard by performing one of the following procedures:

To launch the wizard from the Sessions window:

1. Click Sessions in the Data Protection menu to display the Sessions window.
2. Select the Remote option and click New.

To launch the wizard from the Protected Entities window:

1. Click Protected Entities in the Data Protection menu to display the Protected Entities window.
2. Click New to open the Create Protection Session wizard.

![Remote Session Selection](image1)

**Figure 25. Remote Session Selection**

4. From the Select Source Object window, select the relevant Consistency Group from the table. You can create a new Consistency Group by clicking Create Consistency Group.

![Consistency Group Selection](image2)

**Figure 26. Consistency Group Selection**

5. Click Next to open the Select Target Cluster window.
6. Select a target cluster from the table and click next.

![Figure 27. Target Cluster Selection](image)

7. Select the pairing method as follows:
   - **Auto** – should be selected when XtremIO is used to automatically create the target Consistency Group (and included Volumes) at the target cluster.
   - **Manual** – should be selected when the Consistency Group and Volumes are already created at the target cluster and you want to manually create the Volume pairs.
8. Set the Target Volume Access by selecting Read Access. Click Next.

9. Set the required RPO by selecting the number and units from the drop-down lists (minimum RPO is 30 seconds).
10. From the Target Retention Policy table, select the relevant retention policy for the target cluster.

![Target Retention Policy Selection](image)

**Figure 30.** Target Retention Policy Selection

11. If you want alerts to be issued in case of missing Snapshot Sets (on both clusters), select the Enabled option in the Missing Snapshot Set Alert section; otherwise, select Disabled.

![Missing Snapshot Sets Alert](image)

**Figure 31.** Missing Snapshot Sets Alert Selection

12. Click Next to open the Summary window.

13. Enter a name for the new Remote Protection Session and review its details.
14. Click Finish to complete the Remote Protection Session creation without activating it. Click Finish & Start Protection to complete the Remote Protection Session creation and activate it.

Viewing a Remote Protection Session’s Details

You can view a Remote Protection Session’s details and perform session-related actions via the Session Details window using the following procedure:

1. To open the Sessions window, select Sessions from the Data Protection menu.
2. Click Remote to display the list of defined Remote Protection Sessions.

3. Double-click the relevant session or select it and click More Details.

---

**Figure 34.** Data Protection Remote Sessions View

**Figure 35.** Remote Session Details Tab
The Session Details window consists of the following panes:

- **Summary** – Includes the following information:
  - Session status – Indicates whether the session meets SLA.
  - Session state – Indicates whether the session is active, suspended or terminated and provides the date and time of the last successful Snapshot Set.
  - RPO Compliance (percentage)
  - Bandwidth
  - Replication efficiency (percentage)
  - RPO (Actual vs. Required) – Provides a graphic real-time representation of actual vs. required RPO.
  - Alerts – Displays the alerts issued for this session.
  - Replication Information – Provides the following information:
    - Last Snapshot Set (date and time).
    - Last Cycle Time (date and time).
    - Next Cycle Time (date and time).
    - Number of Target Snapshots.
    - Required RPO.
    - Actual RPO – Indicates the lag between target and source clusters.
    - Source Retention Policy.
    - Target Retention Policy.

The Overview screen provides the following menu options:

- **Protection Copies** – Opens the Session’s Protection Copies window which provides both graphical and list display of all Protection Copies created for this session and enables related actions. Using the graphical display, you can zoom-in to a specific timeframe.

- **Volume Pairs** – Opens the Session’s Volume Pairs window which lists all source-target Volume pairs created in this session’s context.
Storage Replication Adapter

XtremIO SRA integrates with VMware SRM and the XMS to enable SRM workflows that automate the recovery plan test, failover, reprotect, and failback operations.

XtremIO SRA is transparent in that once it is installed on the SRM Server hosts, no further action or direct administration is required.

Downloading and Installing EMC® XtremIO Storage Replication Adapter

Before installing the DELL EMC® XtremIO Storage Replication Adapter (SRA), ensure that VMware SRM is installed on each Site Recovery Manager Server host. For more information on installing Site Recovery Manager, see the VMware vCenter Site Recovery Manager documentation (https://pubs.vmware.com).

To download and install DELL EMC® XtremIO Storage Replication Adapter (SRA), use the following procedure:
1. Verify that XtremIO Clusters are configured to be fully operational, including XMS pairs, cluster pairs, consistency groups, volumes and replication sessions as mentioned earlier.
2. Download the EMC® XtremIO Storage Replication Adapter (SRA) installer file, “EMC XtremIO SRA.msi” from Dell EMC Support site.
3. Run the installer file on both the local and remote SRM servers. The installer file can be run in either interactive (InstallShield) mode with no arguments, or command line mode with an argument for no output or a progress bar.

For interactive mode:
1. Run “Dell EMC XtremIO SRA.msi”. The Install Wizard appears.

Figure 36. Dell EMC XtremIO SRA Installation Wizard

2. Click Next.
3. If you are installing without administrator privileges, then the Windows UAC prompt appears. Click Yes.

![Select Installation Folder](image1)

Figure 37. Dell EMC XtremIO SRA Installation Location

4. After successful installation, click Close.

![Installation Complete](image2)

Figure 38. Dell EMC XtremIO SRA Installation completion

5. Restart SRM service
For command line mode:

1. Open Command Prompt with administrator privileges.
2. Choose one of the following installation commands:
   - silent installation – run “EMC XtremIO SRA.msi /quiet”
   - progress bar – run “EMC XtremIO SRA.msi /passive”

Upgrading Existing Installation of XtremIO X2 Adapter for VMware SRM

The installer for XtremIO X2 SRA supports an upgrade of the SRA from earlier versions to the latest version. The process for the upgrade is similar to a fresh install of the adapter discussed in the previous section with the exception that the old files will be removed and the new SRA files will be loaded into the new directories.

Initial SRM Configuration

In addition to the prerequisites already stated, SRM should be configured to the point where array managers and arrays pairs can be configured. This includes:

- Pairing sites – Site pairing is the first step in configuring Site Recovery Manager. The most common configuration is pairing two sites, although as was outlined in the previous section on topologies, other arrangements are supported.
- Configuring inventory mappings – The following types of inventory mapping are supported in SRM: Resource mappings, folder mappings and network mappings. These mappings provide default settings for recovered virtual machines.
- Configuring placeholder datastores – For each protected virtual machine, SRM creates a placeholder virtual machine at the recovery site. Placeholder virtual machines are contained in a datastore and registered with the vCenter Server at the recovery site. This datastore is called the “placeholder datastore”. Since placeholder virtual machines do not have virtual disks they consume a minimal amount of storage.
- The protected and recovery sites will each require that a small datastore that is accessible by all hosts at that site be created or allocated for use as the placeholder datastore. Each site requires at least one placeholder datastore to allow for failover as well as failback. Please note that these datastores should not be replicated.
Configuring the XtremIO Array Based Native Replication

The configuration of the XtremIO Adapter is performed through the Array Manager wizard in the VMware vCenter Site Recovery Manager plug-in. The wizard should be invoked only after the connection between the VMware vCenter Site Recovery Manager at the protected site and recovery site has been established.

Beginning with SRM 8.1, VMware has moved the SRM plug-in to the New HTML5 Web Client. Though the GUI interface is different, the steps are the same.

To configure Site Recovery, use the following procedure:

1. From the VMware vSphere Web Client “Home” view, click the “Site Recovery” icon.

2. Open the Site Recovery HTML5 Web Client.

3. Click on ‘NEW SITE PAIR’.

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.
4. Enter the VMware PSC Details of the Target vCenter.

Figure 42. VMware PSC Details of the Target vCenter

Figure 43. Target vCenter Selection
Add Array Manager

An array manager is a logical entity that enables SRM to control a specific array by means of the appropriate SRA. For each XtremIO X2 X-Brick array at either the protected site or recovery site, an array manager should be configured with the following procedure:

From within the “Array Based Replication” pane click “Add”. This action will launch the “Add Array Manager” workflow.
The “Dell EMC XtremIO SRA” should be selected. Click the “Next” button to continue.

Add the Local Array Details. The first parameter to be input is the “Display Name” field. A descriptive “Display Name” assists in identifying the VMware SRM site and array manager with which it is associated. In the example provided, a “Display Name” has been provided that identifies the VMware SRM site name (xbrick5115) and the XMS FQDN name (vxms-xbrickdrm5115). Click the “Next” button to continue.
Add the Remote Array Details. The first parameter to be input is the “Display Name” field. A descriptive “Display Name” assists in identifying the VMware SRM site and array manager it is associated with. In the example provided, a “Display Name” has been provided that identifies the VMware SRM site name (xbrick5110) and the XMS FQDN name (vxms-xbrickdrm5110). Click the “Next” button to continue.

**Remote array manager**

- Do not create a remote array manager now.

Enter a name for the array manager on “SRM-VC-DR.tomert.xtreminio”: xbrick5110

**XtremIO XMS Server (local)**

**Local Connection Information**

- **XMS Server Address (Local)**: vxms-xbrickdrm5110.xiodm.lab.amc.com
- **Username**: admin
- **Password**: ********

Click the “Next” button to continue.

**Select the Array Pairs to be enabled and click the “Next” button to continue.**

**Array pairs**

- **SRM-VC-PRD.tomert.xtreminio**
  - **Status**: Ready to be enabled
- **xbrickdrm5110 (5110)**
  - **Status**: Ready to be enabled

Click the “Next” button to continue.
Device Discovery

VMware vCenter Site Recovery Manager automatically invokes the XtremIO Adapter to perform a discovery of the replicated LUNs between the relevant storage arrays as soon as a new array pair has been enabled. A successful completion of the process results in the detailed discovery of the replicated environment including the details of the XtremIO storage arrays objects at the protected site and the recovery site, and the number of replicated devices on the protected site XtremIO storage array. For each device pair, the target and source XtremIO device names are displayed as well as the direction and status of the replication. If the device pair hosts a VMFS volume, the volume name will appear.

Note: Arrays cannot be unpaired while downstream SRM dependencies, such as protection groups, exist.
We can navigate to the XMS and click on the sessions to obtain more detailed information about the specific replication session. This information can include bandwidth, actual vs required RPO, retention policy, replication direction, and more.

Whenever a new replicated datastore or RDM is added to the environment, the arrays should be rescanned within SRM for new devices. The array pair device discovery tool can be found in the Array Based Replication module > Manage tab. Run the device discovery on both arrays to ensure a consistent list of devices. Non-replicated volumes will not be discovered and displayed as eligible devices in SRM. Keep this in mind as a troubleshooting tip if datastores or RDMs are not listed as eligible devices in SRM. Conversely, all XtremIO X2 Series replicated volumes are discovered as devices in SRM, even if they are not used by vSphere (for example, replicated volumes belonging to other storage hosts such as physical Microsoft® Exchange®, SQL Server®, Oracle®, and file servers).
Creating Protection Groups and Recovery Plans

Protection groups are a way of grouping virtual machines that will be recovered together. In many cases, a protection group will consist of the virtual machines that support a service or application such as email or an accounting system. For example, an application might consist of a two-server database cluster, three application servers and four web servers. In most cases, it would not be beneficial to fail over part of this application (e.g. only two or three of the virtual machines in this example), so all nine virtual machines would be included in a single protection group. Creating a protection group for each application or service has the benefit of selective testing. Having a protection group for each application enables non-disruptive, low risk testing of individual applications allowing application owners to non-disruptively test disaster recovery plans as needed. A protection group contains virtual machines whose data has been replicated by either array-based replication or vSphere replication. Before a protection group can be created, replication must be configured. A virtual machine can only belong to a single protection group.

With the placeholder datastore ready, protection groups can be created. Replicated datastore volumes are the foundation upon which protection groups are built. A protection group is effective immediately after being created. Once a VM is protected, it is essentially pinned to the datastore (or datastores) where the vmx and vmdk files reside. Manually moving files that belong to a virtual machine off of a datastore is not supported with SRM. If moved, the VM will not be protected or replicated from its original datastore or datastores. Automated Storage DRS (SDRS) and VMware Storage vMotion® can be sparingly used with SRM-protected VMs if certain guidelines are followed. Refer to the VMware Site Recovery Manager Administration Guide.

Note: Our recommendation is to create a dedicated Protection Group for each replication session.

To create a Protection Group, use the following procedure:

1. Within the "Site Recovery Manager" pane select the "Protection Groups" tab and click "New". This will launch the "Create Protection Group" workflow.

2. Provide a name and description for the protection group, and select the direction of the protection. Click the "Next" button to continue.

![Create Protection Group](image)

Figure 53. Create Protection Group

2. Provide a name and description for the protection group, and select the direction of the protection. Click the "Next" button to continue.
3. The appropriate “Direction of protection” radio button should be selected to reflect the correct VMware SRM protected and recovery sites. For example, if the VMs in the replicated device group reside on the site named “srm-vc-prd” and this device group is being replicated to site “srm-vc-dr”, then the radio button that reflects this replication direction should be selected.

![Create Protection Group – Name and location](image)

4. The “Protection group type” radio button “Datastore groups (array-based replication)” should be selected.

5. The array pair should be selected based on the array manager name and the desired array pair.
   - Note: It is not possible to select more than a single array pair for a given protection group.
6. Click the “Next” button to continue.

7. Click the appropriate checkbox or checkboxes to add one or more datastore groups to the protection group. The VMs contained within the selected datastore group are displayed in the “Virtual machines” section of the window.
8. Click the “Next” button to continue.

### New Protection Group

1. Name and direction
2. Type

#### 3 Datastore groups

3. Recovery plan
4. Ready to complete

#### Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together:

<table>
<thead>
<tr>
<th>Datastore Group</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRMD01, SRMD03</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRMD02, SRMD06</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRMD04, SRMD05</td>
<td>Add to this protection group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Datastore</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRM_VM11</td>
<td>SRMD05</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM12</td>
<td>SRMD01</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM13</td>
<td>SRMD01</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM14</td>
<td>SRMD05</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM15</td>
<td>SRMD03</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM16</td>
<td>SRMD02</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM17</td>
<td>SRMD03</td>
<td>Add to this protection group</td>
</tr>
<tr>
<td>SRM_VM18</td>
<td>SRMD02</td>
<td>Add to this protection group</td>
</tr>
</tbody>
</table>

Figure 56. Create Protection Group – Datastore Groups

VMware Site Recovery Manager 8.1 allows you to create recovery plans within the same Protection Group creation wizard, Recovery Plans in Site Recovery Manager are like an automated run book, controlling all the steps in the recovery process. The recovery plan is the level at which actions such as failover, planned migration, testing and re-protect are conducted. A recovery plan contains one or more protection groups and a protection group can be included in more than one recovery plan. This provides for the flexibility to test or recover an application by itself and also test or recover a group of applications or the entire site. In the example below there are two protection groups: Accounting and Email. And there are three recovery plans: The Accounting recovery plan containing the Accounting protection group, the Email recovery plan containing the Email protection group, and the Entire Site recovery plan containing both protection groups.
To create a Recovery Plan, use the following procedure:

1. Provide a name for the Recovery Plans. Click the “Next” button to continue.
2. Click the “Finish” button to continue.

3. At this point the protection group and the recovery plan have been created. You can verify this by clicking on the Protection Groups tab and check it is marked as ready.
Placeholder Virtual Machines

When you add a virtual machine or template to a protection group, Site Recovery Manager creates a placeholder virtual machine at the recovery site.

Site Recovery Manager reserves a place for protected virtual machines in the inventory of the recovery site by creating a subset of virtual machine files. Site Recovery Manager uses that subset of files as a placeholder to register a virtual machine with vCenter Server on the recovery site. The presence of a placeholder in the recovery site inventory provides a visual indication to Site Recovery Manager administrators that the virtual machines are protected. The placeholders also indicate to vCenter Server administrators that the virtual machines can power on and start consuming local resources when Site Recovery Manager tests or runs a recovery plan.

When you recover a protected virtual machine by testing or running a recovery plan, Site Recovery Manager replaces its placeholder with the recovered virtual machine and powers it on according to the settings of the recovery plan. After a recovery plan test finishes, Site Recovery Manager restores the placeholders and powers off the virtual machines as part of the cleanup process.

Figure 60  Placeholder Virtual Machines
Operational Procedures

After you install and configure your Site Recovery Manager 8.1 environment, you can perform certain operations.

For example, you can non-disruptively test your recovery plan, automate a planned or unplanned recovery, and reprotect your environment after the protected site has been activated. For an overview of SRM use cases and their associated procedures, see Table 1.

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>PROCEDURE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VMware administrator wants to validate the previously configured SRM recovery plan.</td>
<td>Perform Test Recovery Operation</td>
</tr>
<tr>
<td>The VMware administrator wants to clean up the previous test recovery operation.</td>
<td>Perform Cleanup Operation</td>
</tr>
<tr>
<td>The VMware administrator wants to perform a planned migration of selected VMs from the protected site (site A) to the recovery site (site B).</td>
<td>Perform Planned Migration</td>
</tr>
<tr>
<td>A disaster has occurred at site A, and the VMware administrator must recover the VMs on site B.</td>
<td>Perform Disaster Recovery</td>
</tr>
<tr>
<td>After failing over to the recovery site, the VMware administrator must start syncing changes from site B back to site A.</td>
<td>Perform Reprotect Operation</td>
</tr>
</tbody>
</table>

Testing a Recovery Plan

After creating a recovery plan, it is beneficial to test it to verify it works as expected. Site Recovery Manager features a non-disruptive testing mechanism to facilitate testing at any time. It is common for an organization to test a recovery plan multiple times after creation to resolve any issues encountered the first time the recovery plan was tested. When testing a recovery plan, there is an option to replicate recent changes, which is enabled by default. Replicating recent changes will provide the latest data for the testing process. However, it will also lengthen the amount of time required to recover virtual machines in the recovery plan, as replication has to finish before the virtual machines are recovered. A question often asked is whether replication continues during the test of a recovery plan. The answer is yes. VMware Site Recovery Manager utilizes snapshots – either array snapshots (or clones) with array replication or virtual machine snapshots with vSphere Replication – as part of the recovery plan test process. This approach allows powering on and modifying virtual machines recovered as part of the test while replication continues thus avoiding RPO violations. At this point, guest operating system administrators and application owners can log into their recovered virtual machines to verify functionality and perform additional testing. Site Recovery Manager easily supports recovery plan testing periods of varying lengths – from a few minutes to several days. However, longer tests tend to consume more storage capacity at the recovery site. This is due to the nature of snapshot growth as data is written to the snapshot. When testing is complete, a recovery plan must be “cleaned up”. This operation powers off virtual machines and removes snapshots associated with the test. Once the cleanup workflow is finished, the recovery plan is ready for testing or running.
To test a disaster recovery plan, use the following procedure:

1. Right-click the recovery plan, and select **Test**.

![Figure 61. Testing a Recovery Plan](image)

2. Once clicked, a few windows will pop-up to confirm the requested test failover operation. There is a check-box option offered in the first window called “Replicate Recent changes to recovery site”. This option enables/disables the “SyncOnce” operation of replicating recent changes to the recovery site.

![Figure 62. Replicate Recent Changes to Recovery Site](image)
3. Once the user has confirmed the test failover operation, the Recovery Plan will be initiated in test mode. A completed test recovery can be seen in Figure 64. The test environment will remain operational until a Cleanup operation has been executed. You can click the Recovery Steps tab to monitor the progress of the steps in the workflow.

![Figure 63. Test Failover Recovery Steps Tab](image)

4. Optional: When the test recovery operation has completed, click the **History** tab to review a detailed report.

5. On the XMS side, you can see that all replicated volumes have become Write-Access on the Target XtremIO X2 X-Brick.

![Figure 64. Replicated Volumes – XMS View](image)
6. From performance perspective, you can see that the entire load of virtual machines is now running in the DR environment, without any impact on the production environment.

![Performance Chart](image)

**Test Cleanup Operation**

Once a recovery plan has been tested, the test environment can be discarded and reset through the use of the "Cleanup" operation offered by SRM. The Cleanup operation automatically reverts all changes incurred by the recovery plan test and allows for subsequent failover operations. The Cleanup operation performs the following operations:

- Power off and unregister test virtual machines.
- Unmount and detach replica VMFS volumes or RDMs.
- Replace recovered virtual machines with original placeholders (shadow VMS), thus preserving their identity and configuration information.
- Clean up replicated storage snapshots that were used by the recovered virtual machines during the test.
Before resetting the environment after a test failover, ensure that the recovery plan worked as desired. Verify the success of any custom scripts, application functionality, networking, etc. Once all facets of the test have been verified by the involved stakeholders, a Cleanup operation can be executed with the following procedure:

1. In the Site Recovery home interface, select the **Recovery Plans** tab from the left window pane. Highlight the desired recovery plan from the left window pane and then click the Cleanup Recovery Plan icon to perform the operation.

2. Confirm that you are ready to perform the cleanup and then click **Next** and **Finish** to complete the wizard.

<table>
<thead>
<tr>
<th>Cleanup - RP01</th>
<th>Confirmation options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Confirmation options</td>
<td>Cleanup confirmation</td>
</tr>
<tr>
<td>2 Ready to complete</td>
<td>Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.</td>
</tr>
<tr>
<td></td>
<td>Protected site: srm-vc-pro.tomer.xtremio</td>
</tr>
<tr>
<td></td>
<td>Recovery site: srm-vc-dr.tomer.xtremio</td>
</tr>
<tr>
<td></td>
<td>Server connection: Connected</td>
</tr>
<tr>
<td></td>
<td>Number of VMs: 50</td>
</tr>
</tbody>
</table>

**Figure 66. Cleanup Confirmation Options**

3. After the cleanup is complete, the state of the recovery plan is now ready for recovery operation.

4. Optional: If the cleanup encounters errors, run cleanup again with the **Force Cleanup** option selected. The Force Cleanup option cleans up and ignores any errors that might occur. If necessary, run cleanup several times with the Force Cleanup option selected until the cleanup completes successfully.

5. On the XMS side, you can see that all the replicated volumes have become Read-Access again on the Target XtremIO X2 X-Brick.

**Figure 67. Read-Access Applied to Replicated Volumes on Target XtremIO X2 X-Brick**
Recovery Operation

Running a recovery plan differs from testing a recovery plan. Testing a recovery plan does not disrupt virtual machines at the protected site. When running a recovery plan, Site Recovery Manager will attempt to shut down virtual machines at the protected site before the recovery process begins at the recovery site. Recovery plans are run when a disaster has occurred, and failover is required or when a planned migration is desired. Clicking the Run Recovery Plan button opens a confirmation window requiring the selection of a recovery type – either a planned migration or a disaster recovery. In both cases, Site Recovery Manager will attempt to replicate recent changes from the protected site to the recovery site. It is assumed that for a planned migration, data loss should be avoided.

A planned migration will be canceled if errors in the workflow are encountered. For disaster recovery, the priority is recovering workloads as quickly as possible after disaster strikes. A disaster recovery workflow will continue even if errors occur. The default selection is a planned migration. After a recovery type is selected, the operator must also select a confirmation checkbox as an additional safety measure. The idea behind this checkbox is to make sure the operator knows that he or she is running (not testing) a recovery plan.

The first step in running a recovery plan is the attempt to synchronize storage. Then, protected virtual machines at the protected site are shut down. This effectively quiesces the virtual machines and commits any final changes to disk as the virtual machines complete the shutdown process. Storage is synchronized again to replicate any changes made during the shutdown of the virtual machines. Replication is performed twice to minimize downtime and data loss.

After successfully completing a test recovery, run the recovery operation to perform a planned migration or disaster recovery. During a recovery operation, all VMs in the recovery plan are migrated to the recovery site. The corresponding VMs in the protected site are shut down.

When choosing to run a planned migration or disaster recovery plan (as opposed to running a test), keep in mind this procedure is disruptive and results in virtual machines being powered off at the primary site, replication mirrors being broken, and virtual machines being recovered at the secondary site. A recovery operation makes significant changes in the configurations of the protected and recovery sites, and it stops replication. Do not run any recovery plan without testing it first.

When a planned migration occurs, SRM completes the following tasks:

1. Replication of all protected VMs.
2. Graceful shutdown of the protected VMs.
3. Replication of the powered-down VMs.
4. Stopping the XtremIO Native replication and making the recovery datastore writable.
5. Mounting the replicated datastore.
6. Powering on the VMs according to the priority that was configured in the recovery plan.
To run a Recovery Plan, use the following procedure:

1. In the Site Recovery home interface, select the **Recovery Plans** tab from the left window pane.

2. In the event of a disaster or planned migration, right-click the **Recovery Plan** and select **Run**.

3. Confirm the safety precaution message to execute a live plan.

4. Select "I understand that this process will permanently alter the Virtual Machines and Infrastructure of both the Protected and Recovery Datacenters".

![Running Recovery Operation](image)  

Figure 68. Running Recovery Operation
5. Under Recovery Type, select Planned Migration and click Next.

6. Click the Recovery Steps tab to monitor the progress of the recovery workflow.
7. Optional: After the recovery operation has completed, click the History tab to view a detailed report.

![Failover Recovery Steps Tab](image)

8. On the XMS side, you can see that the virtual workload is now running on the target XtremIO X2 brick and the replication status is inactive.

![Failover from Source to Target X-Brick](image)

**Reprotect and Failback**

After virtual machines are migrated from one site to another using either the disaster recovery or planned migration features in SRM, they are in an active running state on the network at the alternate site. However, they are vulnerable to a site failure with no SRM protection.

Site Recovery Manager features the ability to not only fail over virtual machine workloads, but also fail them back to their original site. However, this assumes that the original protected site is still intact and operational. An example of this is a disaster avoidance situation: The threat could be rising floodwaters from a major storm and Site Recovery Manager is used to migrate virtual machines from the protected site to the recovery site. Fortunately, the floodwater subsides before any damage was done leaving the protected site unharmed.
Reprotection

A recovery plan cannot be immediately failed back from the recovery site to the original protected site. The recovery plan must first undergo a re-protect workflow. This operation involves reversing replication and setting up the recovery plan to run in the opposite direction.

Once protected virtual machines are migrated, or disaster recovery failed over to the secondary site, the VMs are unprotected. Following the migration of a protected group, SRM offers the ability to automate the reprotection of the virtual machines. The reprotection is carried out in a series of automated steps.

During a reprotect, SRM commands the SRA to reverse storage replication in the opposite direction for each of the datastores/volumes in the protection group. The protection group originally set up at the primary site is migrated to the secondary site. Placeholder VMs originally set up at the secondary site are now created at the opposite site (the new recovery site) on its respective placeholder datastore.

To run the reprotect operation, use the following procedure:

1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.
2. Highlight the desired recovery plan from the left window pane and then click the Reprotect recovery plan icon to perform the operation.

3. Select "I Understand That This Operation Cannot be Undone" and click Next.
4. Click Finish to complete the wizard.

Figure 75. Recovery Summary Tab

5. Click the Recovery Steps tab to monitor the progress of the reprotect operation.

6. Optional: When the recovery has completed, click the History tab to view a detailed report of the operation.

Figure 76. SRM Recovery Steps
7. Once the operation completed successfully, you can navigate to the SRM Discovery Tab and see the replication direction has changed – from the Target XtremIO X-Brick to the Source XtremIO X-Brick.

![SRM Discovery Tab](image1)

Figure 77. SRM Discovery Tab

8. From the XMS, you can see that the replication sessions are active again, replicating the data from the target site to the source site.

![XMS Replication Sessions](image2)

Figure 78. XMS Replication Sessions
9. You can click on the sessions to obtain more detailed information about the specific replication session such as bandwidth, actual vs required RPO, retention policy, replication direction, and more.

Figure 79. Replication Session Detailed Information

History Reports

When workflows such as a recovery plan test and cleanup are performed in Site Recovery Manager, history reports are automatically generated. These reports document items such as the workflow name, execution times, successful operations, failures, and error messages. History reports are useful for a number of reasons including internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports can be exported to HTML, XML, CSV, or a Microsoft Excel or Word document.

Figure 80. SRM History Reports
Modify Settings to Run Large Site Recovery Manager Environments

VMware Site Recovery Manager ships with a default configuration that is tuned for a large cross-section of environments. However, each environment is unique in terms of architecture, infrastructure, size, and recovery time objective (RTO). Larger or more complex SRM environments may require tuning adjustments within SRM in order for SRM to work properly.

To customize storage settings for your environment, use the following procedure:

1. Click Sites in the Site Recovery Manager interface.
2. Right-click the site on which to change settings.
3. Select Advanced Settings.
4. Click Storage Provider.
5. Modify the Storage Provider settings. For a full list of the available settings, see section following this procedure.
6. Make sure you change the settings for both sites and restart the SRM service to take effect.

![Figure 81. SRM Advanced Parameters](image)
Storage Provider Parameters

storage.commandTimeout – Min: 0 Default: 300

This option specifies the timeout allowed (in seconds) for running SRA commands in array-based replication-related workflows. Increasing this value is typically required for larger environments, or environments with Live Volume stretched storage. Recovery plans with a large number of datastores to manage may fail if the storage-related commands take longer than five minutes to complete. For larger environments, increase this value (for example, to 3600 or higher) in the advanced SRM settings. For environments including Live Volume stretched storage within protection groups, this value should be increased by 90 seconds for each Live Volume managed by SRM.

storageProvider.hostRescanRepeatCnt – Min: 0 Default: 1

This option specifies the number of additional host rescans during test, planned migration, and recovery workflows. This feature was not available in SRM 5.0 and was re-introduced in SRM 5.0.1. Increase this value (for example, to 2 or higher) in the advanced SRM settings.

storageProvider.hostRescanTimeoutSec – Min: 0 Default: 300

This option specifies the timeout allowed (in seconds) for host rescans during test, planned migration, and recovery workflows. Recovery plans with a large number of datastores and/or hosts will fail if the host rescans take longer than five minutes to complete. Increase this value (for example, to 600 or higher) in the advanced SRM settings.

storageProvider.fixRecoveredDatastoreNames – Min: 0 Default: 0

This option is disabled by default. During the execution of SRM recovery plan, a re-signature operation is carried out on the recovered devices. This lead to the addition of a prefix like "snap-xxxxxxx" to the datastore name. Enabling this option renames the datastore to its original name.

storageProvider.resignatureFailureRetryCount – Min: 0 Default: 0

The default value of this parameter is 0. During a recovery plan or test recovery plan, it may be necessary to change this value to allow SRM to retry a re-signature operation. In most cases keeping this value equal to the value of storageProvider.hostRescanRepeatCnt works the best.

storageProvider.hostRescanDelaySec – Min: 0 Default: 0

The default value of this parameter is 0. SRAs can send responses to SRM before a promoted storage device on the recovery site has become available to the ESXi hosts. When SRM receives a response from an SRA, it performs a rescan of the storage devices. If the storage devices are not fully available yet, ESXi Server does not detect them and SRM does not find the replicated devices when it performs rescans. Datastores are not created and recovered virtual machines cannot be found. In large scale environments you might experience problems with unavailable datastores, SRM provides this setting to allow you to delay the start of rescans after an SRA promotes a storage device.

storage.minDsGroupComputationInterval Min: 0 Default: 600

The default value of this parameter is 0. By default, vCenter Site Recovery Manager checks arrays for changes to device configurations by rescanning arrays every 10 minutes. You can reconfigure the frequency with which vCenter Site Recovery Manager performs regular array scans by changing this parameter’s value.
**Point-in-Time Recovery Images**

By default, whenever you perform a failover or test-failover, SRM will recover the volumes at the target site to the last point in-time.

The combination of XtremIO X2 Native Replication and the EMC VSI plugin offers administrators an extremely powerful tool in relation to BCDR planning activities. As long as VMware SRM is tasked with management of the XtremIO X2 Consistency Group, and the VSI plugin has been fully integrated, system administrators will have the ability to specify the Point-in-Time (PiT) copy used during a SRM Test Recovery Plan or disaster recovery scenarios. This means that system administrators can actively assign what PiT instance of their protected datasets are brought online at the secondary site.

The EMC VSI plugin provides unique storage integration capabilities between VMware vSphere and XtremIO. This tool enables VMware administrators to view, manage and optimize XtremIO storage for their ESX/ESXi servers. It consists of a graphical user interface and the EMC Solutions Integration Service (SIS), which provides communication and access to XtremIO array(s). The VSI plugin allows the users to interact with their XtremIO array directly from the vCenter web client. This provides VMware administrators with the capabilities to monitor, manage and optimize their XtremIO hosted storage from a single GUI. For example, a user can provision VMFS datastores and RDM Volumes, create full clones using XtremIO Virtual Copy technology, view on-array used logical capacity of datastores and RDM Volumes, extend datastore capacity, and do bulk provisioning of datastores and RDM Volumes.

The procedure for choosing the desired PiT copy to be used during the Test Recovery Plan or failover is relatively simple, with the only caveat being that the PiT copies available will be dependent on the Snapshot Pruning and Retention settings defined in the CG Replication policies. By default, the most recent synchronized copy of the protected Volumes is brought online at the recovery site in the case of a test or actual SRM Recovery plan. To specify a particular PiT image for VSI and XtremIO X2 to use during a recovery operation, the administrator can, via the vCenter web client, select a particular VM from the desired Consistency Group and examine the EMC VSI tab that lists the VM's associated Consistency Groups. After selecting the desired Consistency Group, administrators are presented with a listing of all available PiT copies for this XtremIO X2 CG. To select the PiT image that the VMs of this Consistency Group will revert to post-completion of the recovery plan, the administrator simply chooses the desired time and image and then applies and verifies the choice.

1. To select an existing point in time or create a new bookmark manually, navigate to the XMS, mark the replicated session, and select Replicate Now.
2. Navigate to one of the virtual machines and selecting the EMC VSI tab. You will be able to see the new manual bookmark.

3. To see the session details, select the desired bookmark.
4. Click on "Set as SRM Recovery Point" and click OK. Next time you perform a failover or a test-failover, SRM will recover the volumes from the specific bookmark you selected.
As mentioned, this functionality offers an extremely powerful capability to data center administrators with responsibilities for BCDR planning and implementation. With this feature, administrators can now revert a user-defined set of VMs to any particular Point-in-Time (based on retention period, defined RPO and Snapshot maximums) and protect against compromised environments, virus infections and configuration errors that can go undetected for some time, before leading to organizational IT downtime and possible data loss or corruption.

The described functionality can also be extended to the provisioning of desired PIT datasets for use in the test and development activities of the organization. With proper collaboration between the development, database and data center administration teams, appropriate datasets for test/dev activities can be identified, bookmarked and provisioned to the secondary test and development site, all from the single pane of the vCenter server web client.
Conclusion

Dell EMC XtremIO X2 offers the market an advanced revolutionary architecture, optimized for all-SSD enterprise storage subsystems. Dell EMC XtremIO X2 offers a rich set of features that leverage and optimize SSD capabilities and have been especially designed to provide unparalleled solutions for enterprise customers’ needs and requirements.

Dell EMC XtremIO X2 arrays, VMware vSphere, Site Recovery Manager, combine to provide a highly available business platform for automated disaster recovery with the best possible RTO and RPO, as well as planned migrations for your virtualized data center.
References
How to Learn More

For a detailed presentation explaining XtremIO X2 Storage Array's capabilities and how XtremIO X2 substantially improves performance, operational efficiency, ease-of-use and total cost of ownership, please contact XtremIO X2 at XtremIO@emc.com. We will schedule a private briefing in person or via a web meeting. XtremIO X2 provides benefits in many environments and mixed workload consolidations, including virtual server, cloud, virtual desktop, database, analytics and business applications.