SRM User Guide: vVol Periodic Replication SRM Workflows

The ability to protect and recover vVol-based virtual machines that are replicated using array-based replication is supported starting with Site Recovery Manager 8. Unlike traditional VMFS or RDMs, the management of vVol-based replication does not require a Storage Replication Adapter (SRA).

It is important to review the configuration and setup documentation found here:

SRM - Requirements and Limitations
FlashArray vVols Array Based Replication and SRM - Requirements and Limitations
Configuring Site Recovery Manager vVol-Based Storage Policy Discovery

This page will overview the SRM workflows of test recovery, recovery, reprotect, and failback.

Prerequisites

In order for SRM to run any vVol operations with the FlashArray there are a few requirements:

1. Replication must be configured for the virtual machines by the way of Storage Policies.
2. The replication group(s) must be added to a SRM protection group.
3. The protection group must be in at least one recovery plan.
4. Hosts and host groups must be pre-created on the recovery FlashArray for the target recovery clusters.
5. The source and target FlashArrays must be using at least FlashArray VASA Provider 1.1.0 (initially released with Purity 5.3.6). If an earlier version of VASA is being used, you must upgrade the FlashArray(s) prior to SRM control.

Example Environment

For this environment, there is a Storage Policy assigned to 9 virtual machines:
These VMs are all assigned to the same replication group (it is important to remember that the policy itself does not matter for failover, but instead the specific replication group that is assigned to the VMs). These VMs are in a replication group called **flasharray-m50-1:srmvVolPG**: 

Which maps to a FlashArray protection group called **srmvVolPG** on the FlashArray named **flasharray-m50-1**:

This replication group has been added to a SRM protection group called **vVol-FlashArray**:
Which has been added to a recovery plan called vVol-RP:

Test Recovery

To initiate a test recovery, click on the recovery plan in SRM and click Test.

Site Recovery Manager currently offers to point-in-time options for test failover: use the latest, or create a new one. The default behavior is to create a new point-in-time and then execute the test recovery. This is enabled or disabled by selecting or deselecting the Replicate recent change to recovery site check box.
Select or de-select this and click **Next** then **Finish**.

This will create a new replication point-in-time in the target protection group on the target FlashArray. Note it will use the default naming scheme for the protection group snapshot name.

This operation (called **syncReplicationGroup**) is issued to the target FlashArray. The target FlashArray then reaches out to the source FlashArray to initiate a new synchronization. If the replication link is down this operation will fail—either enable the replication link or deselect **Replicate recent changes**.

The step "Create writable storage snapshot" will perform the following steps:

1. Create a new protection group on the target site. This will have a prefix of **r-** with the original name of the source protection group and a short identifier as a suffix. If the protection has been created for a previous test recovery, a new protection group will not be re-created and the existing one will be re-used. The only exception is if the protection group that was previously created has an unrelated volume already in it. In this case VASA will create a new protection group on the target FlashArray. The existing one will be updated to match the source protection group protection policies, though it is important to note that snapshot and replication will be put into the disabled state.

2. Create volume groups. For each recovery VM, there will be a new volume group created. It will follow standard FlashArray vVol volume group conventions. The name is NOT guaranteed to be exactly the same as the volume group on the source.

3. Create new volumes for use as vVols. These will also follow standard naming conventions and will be placed in the appropriate new volume groups.

You may rename the volumes, volume groups, and protection group as needed between the test recovery start and stop.
**Do not destroy** the protection group until after successfully completing the SRM cleanup operation. While deleting the test recovery protection group will not cause the test or cleanup to fail, it will orphan the vVol-related volumes and volume groups created during the test and manual cleanup of those objects will be required and will cause subsequent test recoveries to fail.

An example test recovery protection group:

![Protection Group Example](image1)

An example test recovery volume group:

![Volume Group Example](image2)

The next step is for VMware to prepare the vVol file mappings. During a recovery each new vVol has a new UUID. Each VM has a config vVol that stores all of the virtual machine files--like the VMX file and VMDK descriptor files. Since the replication is byte-for-byte--the files on the config vVol still point to the UUIDs of the previous vVols on the source site. Once the test recovery process completes on the FlashArray, the FlashArray VASA provider returns a mapping of the original vVol UUIDs to the new vVol UUIDs as well as the paths to their VMX files on the new config vVols.

vCenter then takes those mappings and updates the files on the each config vVol. This enables the power-on of the virtual machine to be able to identify and find the correct new volumes after recovery.

This file update process appears as a vCenter task called Datastore.updateVVolVirtualMachineFiles.label. This process currently takes the bulk of the time for the test recovery process and Pure Storage engineering is currently working with VMware engineering to improve the speed of this process. Users may note that the process is significantly faster with the actual recovery process--this is due to the fact that the ESXi improvement identified to accelerate this operation did not make release for the test recovery--only the recovery.
The test recovery process then finally registers and powers-on the virtual machines as dictated by the recovery plan.

When the test has been verified, end the test recovery by clicking **Cleanup**.
Click **Next** and then **Finish** the initiate the cleanup.

The test recovery cleanup operation will:

1. Destroy and eradicate all volumes belonging to the recovered VMs.
2. Destroy and eradicate all volume groups belonging to the recovered VMs.
3. The protection group created during test recovery will NOT be destroyed and will remain. It can be safely destroyed and eradicated manually if preferred. This protection group will be re-used for additional test recoveries if no configuration changes occur to the original source protection group.
Recovery

This section covers the recovery of a vVol-based protection group from one FlashArray to another. Choose Run on the recovery plan to start the recovery wizard.

This can be run via the planned migration or the disaster recovery process within SRM--there is no significant difference on the FlashArray operations in either mode other than the in the planned migration recovery all operations are expected to succeed. In the DR mode, any operations on the source site (operations within vCenter, SRM, or the FlashArray) can fail and the process will continue. For the FlashArray this means that if the source FlashArray is down there will be no final synchronization of changes.

It is always recommended to run recoveries in the planned migration mode--as the fewer failures, the more automatic the eventual reprotect operation will be. Only attempt a disaster recovery operation if the source site is down and a planned migration will not succeed. Complete the wizard to initiate the recovery.

The first operation to run is a synchronization of storage.

This operation reaches out to the target VASA provider to synchronize the latest point-in-time from the source FlashArray. The target VASA provider then reaches out directly to the source FlashArray to initiate a new synchronization.

This will show up on the source FlashArray audit log as a "root" operation on the protection group(s).
The VMs will then be shutdown once the synchronization completes:

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Target</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-7</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-1</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-9</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-6</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-8</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-3</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-4</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-5</td>
<td>Completed</td>
</tr>
<tr>
<td>Initiate guest OS shutdown</td>
<td>srmvm-2</td>
<td>Completed</td>
</tr>
</tbody>
</table>

The next step is for SRM to unregister the source VMs and replace them with placeholders. The placeholder datastore chosen is specified in the SRM placeholder mappings.

Note that the placeholder datastore must be a non-vVol datastore.

The vVol VMs will be unregistered but not deleted—they will remain after the recovery in the vVol datastore and on the array:

On the FlashArray:
Once completed, the synchronization will occur one more time--this will be the point-in-time used for recovery. Once the final synchronization completes, SRM will issue the recovery operation to the target FlashArray VASA provider during the **Change recovery site storage to writable** step.

This process will:

1. Create a new protection group on the target site. This will have a prefix of `r-` with the original name of the source protection group and a short identifier as a suffix. If the protection group has been created for a previous recovery, a new protection group will not be re-created and the existing one will be re-used. The only exception is if the protection group that was previously created has an unrelated volume already in it. In this case VASA will create a new protection group on the target FlashArray. The existing one will be updated to match the source protection group protection policies, though it is important to note that snapshot and replication will be put into the **disabled** state.

2. Identify all of the volumes that are part of the recovery operation and copy them from their respective replication snapshot in the specified protection group point-in-time

3. Create a volume group for each recovered VM (these will not have the same suffix as the source volume groups as that ID is randomly assigned to assure uniqueness)

4. Add the volumes to the volume group(s)

5. Return to VMware the paths of the VM .VMX files on the new config vVols
You may rename the volumes, volume groups, and protection group as needed between the recovery start and reprotect.

⚠️ Do not destroy the protection group created by the recovery. If you prefer to use a different protection group, re-assign the storage policy or move the VM storage using a re-assignment of the replication group in vSphere. Once the protection group is empty you may delete the protection group. In general, do not delete protection groups that have SRM-controlled vVol volumes in them—first clear them out using VMware storage policies then delete the group.

VMware will then update the reference files in the file during an operation called updatevVolVirtualMachineFiles.

SRM will proceed to then register and power-on the virtual machines as dictated in the recovery plan.

Thus completing the recovery:
Repurpose

Once a successful recovery has occurred (and the state is confirmed) it is important to run the SRM reprotect operation as soon as possible. The FlashArray recovery process for vVols will put the recovered volumes in a protection group, but replication is not enabled on them until reprotect.

Furthermore, Site Recovery Manager does re-apply the a storage policy upon recovery to the recovered virtual machines. This is achieved by looking at the storage policy mappings within SRM:

What these mappings are missing though is a replication group mapping, as what replication group to put the VM storage in may or may not be known prior to recovery. Therefore immediately after recovery the recovered VMs will be out of compliance:

To resolve this, click on Repurpose in SRM:
The VASA provider will enable the replication (and snap policy if previously configured) schedule. From

![Replication Schedule](image)

Enabled: False
Replicate a snapshot to targets every 10 minutes
Retain all snapshots on targets for 1 days
then retain 4 snapshots per day for 7 more days

to:

![Replication Schedule](image)

Enabled: True
Replicate a snapshot to targets every 10 minutes
Retain all snapshots on targets for 1 days
then retain 4 snapshots per day for 7 more days

The reprotect operation will add the correct replication group into the policy assignment for the recovered virtual machines:

![Edit VM Storage Policies](image)

Accordingly, the virtual machines will now be marked as compliant:
Lastly, the reprotect will issue a synchronization of the protection group in step 5:

Failback

The process to fail back is structurally the same as an initial recovery—the only difference is that this workload has already been recovered at least once. So fundamentally the process is the same. Since the workload is going back to a place it has already been, the recovery process will attempt to re-use those resources (protection groups/volumes/volume groups).

The assumption is that the VMs were originally on site "A" and have been recovered to site "B". When the VMs are failed back to site "A":

Volume re-use:

- For a volume to be re-used it must still be in the original replication group that it was failed over from (it can simultaneously be in other protection groups as well).
- If one or more volumes are not present in the original protection group, new volumes and volume groups will be created for the recovered VMs. Therefore the original volumes can be destroyed as they are no longer going to be re-used.
- If a VM has been added to the replication after recovery, all volumes and groups will be re-used upon failback (assuming the above requirements are met too). The new VM will have new volumes and a volume group created.
- If a VM is deleted after a reprotect, all volumes and groups will be re-used upon failback (assuming the above requirements are met too) and the corresponding volumes for the deleted VMs will be destroyed to correct what volumes reside on the recovered site.

Protection group re-use:

- If no protection group that matches is found a new protection group is created.
• If a matching protection group is found but that protection group membership has changed (volumes manually added or removed) that group will be ignored and new one will be created.

• A matching protection group is not manually created (the match is not based on configuration or name)—it is created by VASA and the pair is maintained by VASA.

• Matched protection groups will be overwritten with the protection policy of the source protection group.

• Replication and snapshot policies will be disabled upon failover, and re-enabled as originally configured upon reprotect.