HP LeftHand SAN failback procedure for VMware

White paper

Introduction

This white paper documents the procedure for failback from a VMware Site Recovery Manager (SRM) recovery site after SRM has performed a failover on an HP LeftHand SAN. This document is intended for customers who are using an HP LeftHand SAN with VMware.

The HP LeftHand Site Recovery Adapter (SRA) for VMware enables full-featured use of VMware Site Recovery Manager (SRM). Combining HP SAN/iQ® remote copy replication with VMware SRM provides an automated solution for implementing and testing disaster recovery between geographically separated sites. The steps in this white paper should be used as a guideline for failback.

Conditions after a failover

After a failover has been performed on a VMware SRM environment, production virtual machines should be running and performing I/O to the SAN at the disaster recovery (DR) site. Failback of these VMs needs to include all of the I/O that has occurred at the DR site.

Desired conditions after failback

Automatic failback is not currently facilitated by SRM, but can be performed manually. After a failback, the VMs that had been failed over to the DR site should be once again running at the production site, and they should include all updates and I/O that were performed on them while running at the DR site.

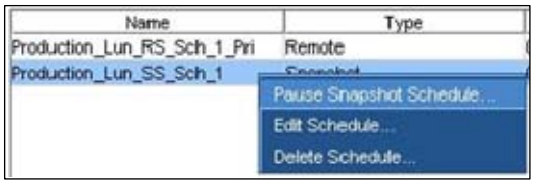
Failback steps

These steps outline the process required to use LeftHand SANs to failback volumes, including updates made to them, from a DR site back to the production site. You need to perform these steps on each set of SRM protection groups and LeftHand SAN volume(s) that are to be failed back to the production site.

Preparation

1. Remove the VMs from the production site inventory. This is required so that the failback VMs can take their place and use the same names as the original production site VMs. This action also leaves empty the protection groups that included the original VMs. (Protection groups must be empty before they can be removed in step 3 below.)
2. At the DR site, shut down the VMs that are going to be failed back. Shutting down these VMs puts them into a quiesced state before failback occurs.
3. Remove the SRM protection groups for the VMs at the production site. You will need to re-create these protection groups after failback is complete. Document their properties now so you can re-create them later.
4. As shown in Figure 1, pause all schedules on the original primary volume(s) at the production site. These schedules must be paused to allow for failback. Once failback is complete, you can simply resume schedules.

Figure 1. Pausing a schedule in VMware

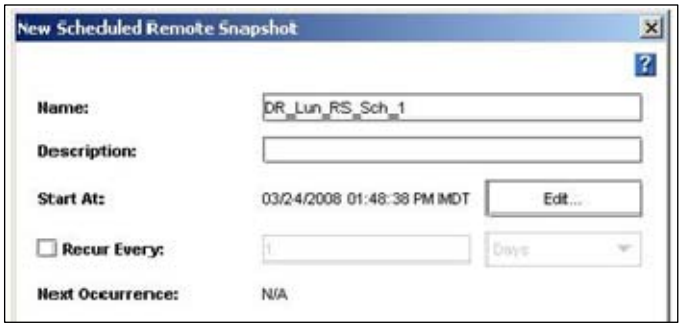


Reversing SAN replication

For each volume that was in the protection group being failed back, use the following steps to reverse replication from the DR site back to the production site:

1. Right-click the recently created primary volume at the DR site and select **New Scheduled Remote Snapshot**. You see the New Scheduled Remote Snapshot window. In order for SRM to recognize it as a replicated volume, the failback copy must be performed by a schedule.
2. In the New Scheduled Remote Snapshot window shown in Figure 2, select **Edit** and change the start time to **Now**.

Figure 2. Entering parameters for the new scheduled remote snapshot



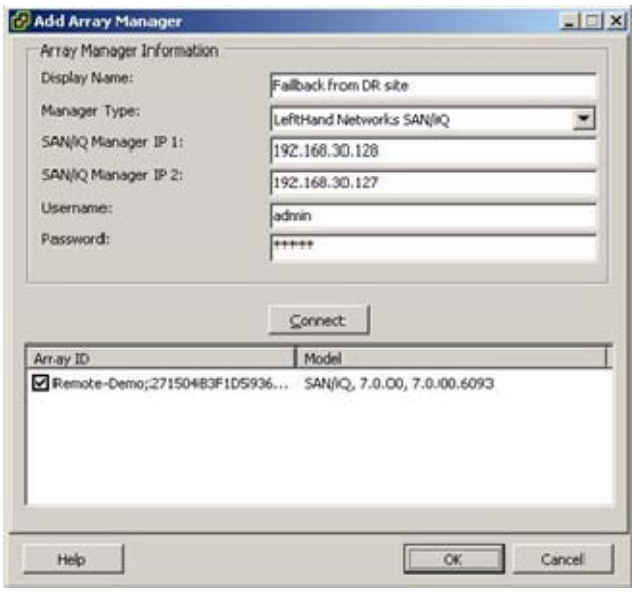
3. Clear (uncheck) the **Recur Every** check box so this replication occurs only once.
4. Select the original primary volume at the production site as the target.
5. Select **OK**. A warning advises that changing the production site volume from primary to remote will make it inaccessible and that a snapshot will be taken to preserve its current state. This is necessary for failback to complete.
6. Select **OK**. A warning advises that schedules will fail once this volume is made remote. This is necessary for failback to complete.
7. Wait for reverse replication to complete. This will copy back only the changes made to the volume since it was failed over from the production site. The time required for replication back will depend on the number of changes made to the volume and the bandwidth available for replication.

Configuring SRM for failback

Once reverse replication is complete for all volumes associated with the protection group that is being failed back, configure the SRM array managers at the DR site:

1. In SRM, at the DR site select **Configure** next to the array managers. You see the Add Array Manager window. (Array managers may already be configured if the SRM sites have been cross-replicating. If the array managers are already configured, skip to step 4 below.)
2. As shown in Figure 3, add a protection side array manager for the DR site SAN. This will require the IP addresses of the SAN/iQ managers, a username, and password.

Figure 3. Adding an array manager



3. Add a recovery side array manager for the production site SAN. This will require the IP addresses of the SAN/iQ managers, a username, and password.
4. Review the Replicated Datastores summary at the end of the wizard. The summary should include all the failback volumes that were reverse-replicated.
5. Create a new protection group at the DR site to facilitate failback to the production site. This may require setting up inventory preferences in the DR site, if they were not already configured there. The failback protection group will create shadow VMs at the production site, and these shadow VMs will eventually become the production VMs again.
6. At the production site, create a recovery plan to facilitate failback from the DR site.

Test first, then failback

Once you have performed reverse replication, created a failback protection group, and created a failback recovery plan, you should repeatedly run complete recovery tests to resolve any failback issues:

1. Select the failback recovery plan in the production site and perform a test of the recovery steps. If any issues occur during the test, resolve them and run the test again.
2. Once the failback test is completing reliably, run the recovery plan to perform the actual failback.

3. VMs should now be running at the production site, with all changes made at the DR site included.

Clean up failback, return to scheduled replication

Now that failback is complete, you should reset the environment to its original state of replicating to the DR site. You should test this replication on a regular basis.

1. Remove from inventory at the DR site any VMs that were temporarily available for production use. This is required so that you can recreate the original protection groups.
2. (Optional) Remove the recovery group from the production site that was used to failback.
3. Remove the protection group from the DR site that was used to failback.
4. Change back from primary to remote the DR site volume(s) that were failed back. You are warned that doing so will disconnect these volumes and take a snapshot to preserve their current state. Ignore the warning, since this action is necessary to continue replication from production.
5. (Optional) Delete the single remote snapshot schedule that was used to failback from the DR site on the volume(s).
6. Resume the schedules on the production site primary volume(s) so that replication and snapshots can continue as they were before failover occurred.
7. Re-create at the production site the protection group that was originally configured before failover occurred.
8. At the DR site, edit the recovery plan that had this protection group before failover occurred, and add the new protection group back to it.
9. After the next remote copy schedule is completed, test the recovery plan at the DR site to ensure the production site is again configured correctly.

This completes the failback procedure.

For more information

For more information on HP LeftHand SANs, visit www.hp.com/go/p4000

Technology for better business outcomes

4AA2-5085ENW, April 2009