



VMware Site Recovery Manager (SRM) was designed to simplify DR by eliminating complex runbooks, orchestrating the workflow of failover, and enabling automation of parts of that workflow. VMware SRM leverages storage-based replication and/or new vSphere Replication to provide:

- Replication of application VMs to a secondary site
- Management of recovery and migration plans
- Non-disruptive testing

New in version 5 of VMware SRM is vSphere Replication, a combination of an agent built into vSphere 5 and a replication management server licensed with SRM and running as a VM. This solution with vSphere Replication allows customers to asynchronously replicate VMs from one location to another without the need for storage array-based replication. It provides DR (disaster recovery) for VMs, but also supports migration of VMs between sites for maintenance, testing, or any other reason (these other reasons are probably more frequent than the need for DR failover). Replication is managed at the VM level, which is much easier than at the LUN (storage) level for smaller organizations.

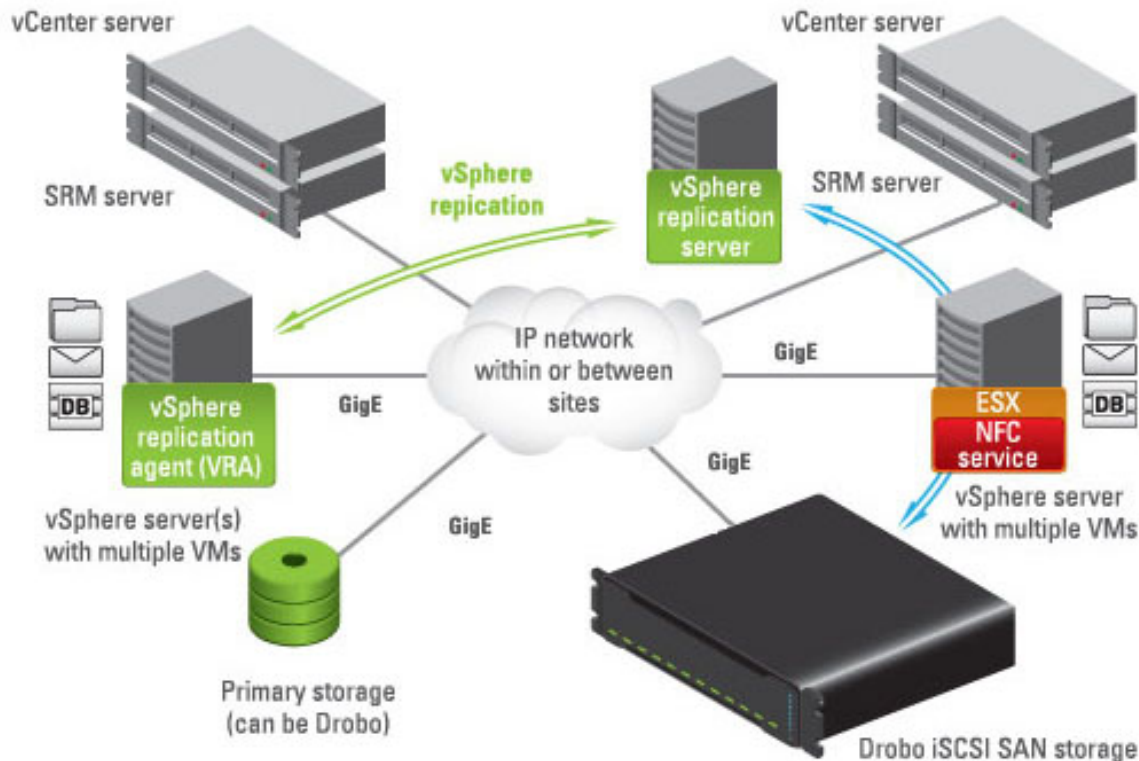
By controlling replication in software, customers can replicate between sites with dissimilar SAN hardware, something that is not possible with array (storage)-based replication. Not only can you lower the cost of the primary storage, but storage at the remote site can also be lower, particularly as most SMBs cannot afford a duplicate site, and desire DR for select applications while they recover their primary site. For larger organizations, SRM supports both array based and VR for a tiered replication solution. There are some limits when using vSphere replication with SRM compared to array-based replication, such as lower comparable performance, recovery point of 15min compared to shorter, and no automated failback in the first release.

SRM supports several different topologies for organizations of different sizes, but this document focuses on using vSphere Replication *between a primary protected site and one recovery site* for SMB. The examples describe using Drobo as the storage at both sites, although these instructions can also be used when Drobo is the SAN storage at the recovery site protecting another vendor storage at the primary site, leveraging support for dissimilar storage hardware.



Topics

- Drobo and vCenter
- SRM Basics
- Configuring an SRM solution
- Testing and executing recovery plans



What You Will Need

- Drobo B800i or B1200i
- Drobo Dashboard management software (latest version)
- Enterprise-grade 7200RPM SAS or SATA disk drives recommended
- Network between sites, with capacity for 0.5 to 2 Mbit/sec per VM
- Physical servers with vSphere v5 standard edition installed on any server doing vSphere replication (SRM with vSphere replication not currently available for Essentials or Essentials Plus kits)
- Two instances of vCenter Server v5 installed, one at the protected and a second at the recovery site
- SRM Standard Edition licenses (up to 75 VMs), minimum quantity is 25 @ \$195 for a total of \$4,875
- VMware Site Recovery Manager components configured and running

Drobo and vCenter

This document assumes that Drobo has been set up and configured in your VMware virtualization infrastructure (ESX/ESXi and vCenter). If not, to do so, read *How To Deploy VMware and Drobo as a Complete and Cost-Effective Virtualization Solution* [www.drobo.com/downloads/how-to/HT-0045-00_vmware_drobo_virt_solution.pdf].

It covers the best practices for setting up and configuring Drobo iSCSI volumes and how to present them as VMFS datastores to VMware vCenter server.



SRM Basics

Looking at the current VMware feature set, you see features that allow IT administrators to recover in case of hardware failure, such as vMotion. However, vMotion does not protect the applications or provide 99.99% uptime in the event of a complete loss at the primary site. And using vMotion in a multi-cluster environment or using SAN shared storage across a WAN considerably increases operating budgets.

Although VMware SRM has many components, this document focuses on storage and where and how you can leverage the advantages of Drobo iSCSI SAN volumes in an SRM deployment.

Ensure that the minimum requirements have been met (detailed in the *SRM Administrator's Guide*), and that the application is running successfully. All of the following components need to be up and running at both the protected site and the recovery site:

- vCenter Server
- Microsoft SQL Server 2008
- Site Recovery Manager Application and Plug-In
- Single or multiple ESX/ESXi hosts managed by the vCenter server
- vSphere Replication Management server
- vSphere Replication server

Configuring an SRM Solution

Before going any further, verify that you have everything you need as detailed in the "What You Will Need" section and ensure that all components have been successfully installed as described.

This guide is a supplement to both the *VMware Site-Recovery-Manager Administration Guide* and the *VMware Site-Recovery-Manager Guide*. Visit the VMware corporate website for additional information on how to install and configure SRM:

- http://www.vmware.com/pdf/srm_admin_5_0.pdf
- <http://www.vmware.com/files/pdf/products/SRM/VMware-vCenter-Site-Recovery-Manager-Evaluation-Guide.pdf>



STEP 1

Configure connection pairing.

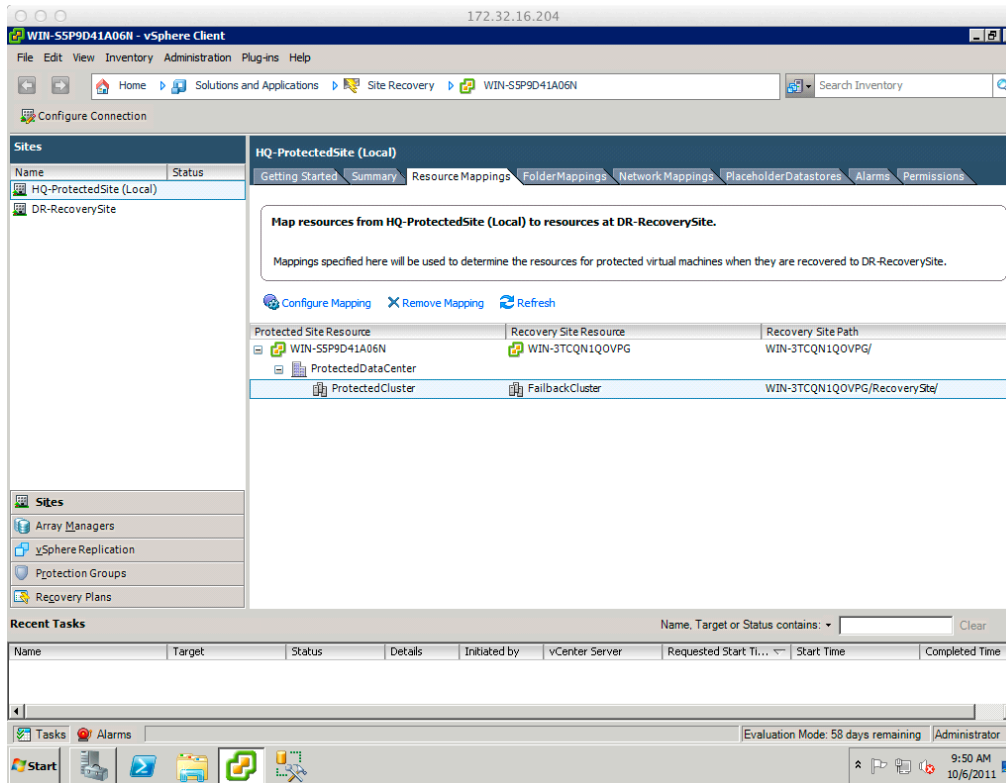
STEP 2

The next step is normally to set up the Storage Replication Adapter. However, this step is unnecessary as this document focuses on the concept of host-based replication, taking advantage of vSphere Replication, and does not use array-based replication.



STEP 3

Inventory mappings determine recovery site defaults for the VM folders, networks, and resource pools to which recovered virtual machines are assigned. Ensure at this stage that a placeholder datastore (on the Drobo) has been created at the recovery site in order to complete this step correctly. The placeholder datastore should be accessible to all hosts in the recovery cluster.



Set up inventory mapping. Ensure that you configure all inventory mapping tabs as needed: resources, folders, networks, and a placeholder datastore mapping to hold "shadow" VMs at the recovery site.



STEP 4

SRM organizes virtual machines into protection groups based on the datastore groups that are used. The protection group specifies which VMs *at the protected site* are to be included in the failover to the recovery site, including the entire datastore and all VMs that are located on it. In creating the protection group, select a replicated datastore at the DR site that will be used to house placeholder VMs. Placeholders are small files that identify VMs at the recovery site and are used until testing or failover occurs—at which time they are replaced with VMs from the replicated storage.

To set up a protection group, in the Create Protection Group screen, select the protected site and select **vSphere Replication**. Click **Next**.



STEP 5

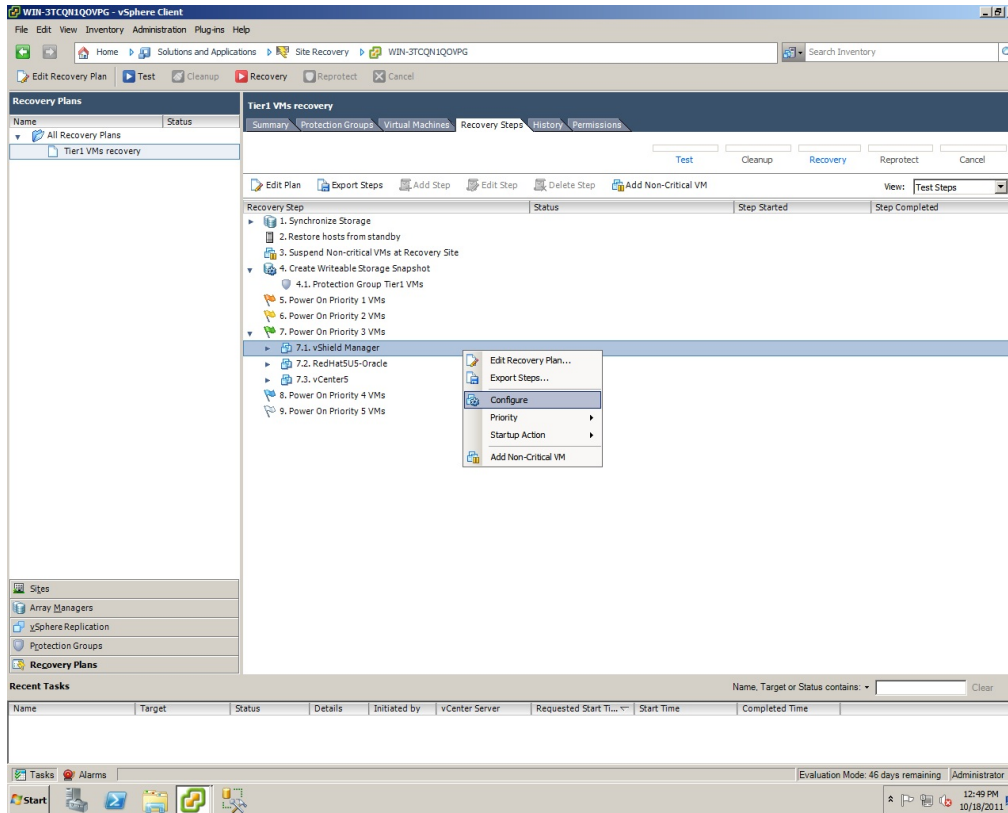
A recovery plan specifies how VMs are migrated to the recovery site. It's stored in the SRM database at the recovery site and executed by the SRM server at the recovery site.

Specify the recovery plan and click **Next**.



STEP 6

Administrators can customize IP settings for individual virtual machines for both the protected site and the recovery site.



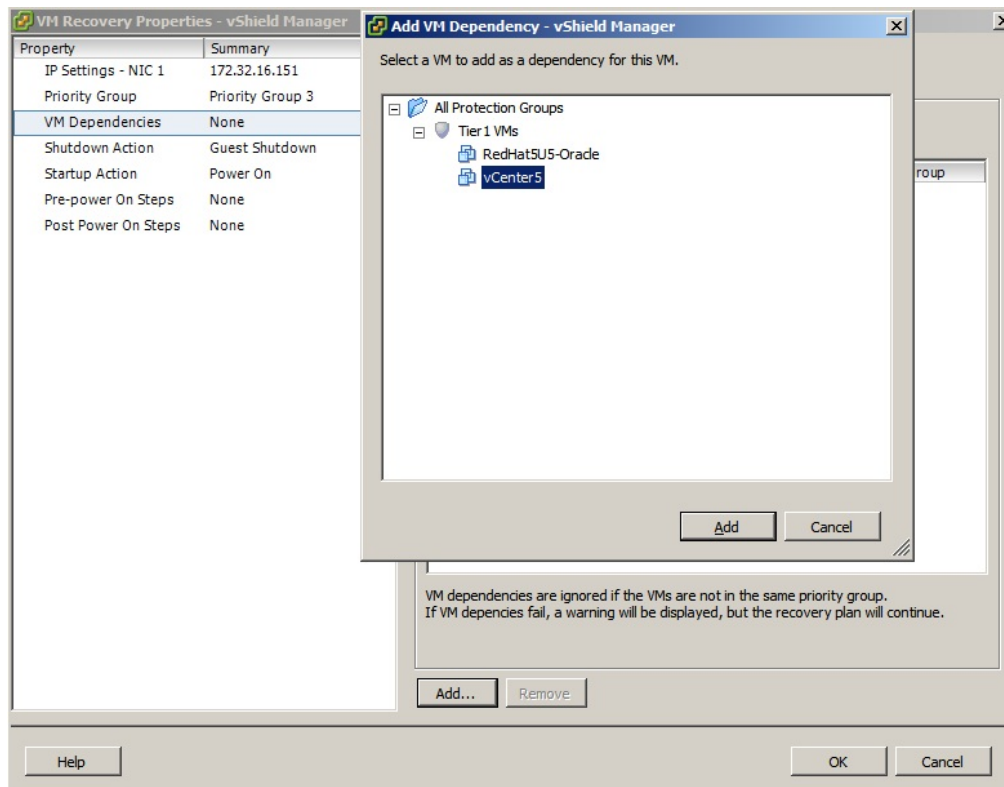
In the Recovery Steps tab of the recovery plan, right-click the VM and choose **Configure**.

Select the “Customize IP settings during recovery” to enable customization of network information. Then click **Configure Recovery** to customize which IP addresses will be injected into the VM during execution of a recovery plan.



STEP 7

Priority groups specify which VMs in a recovery plan will start at which stage of the recovery plan. This includes setting priorities for VMs in a recovery plan as well as the ability of dependencies to set policies for startup sequences for VMs.



Configure priority groups and dependencies.

Testing and Executing Recovery Plans

While SRM provides automated recovery, its strength is its ability to easily test recovery without disrupting existing production environments. You can perform a recovery test using an isolated test virtual network and a temporary copy of replicated data at the recovery site. When test plans are executed, the procedure performs each step in the recovery plan taking into account the application service dependencies for the protected VMs. While tests are running, they can be paused, resumed, and canceled at any time.

The following occurs when you execute a failover:

- Array replication between the protected site and recovery site is stopped.
- All VMs at the protected site are powered down.
- All placeholder VMs at the recovery site are replaced by powered-on VMs that will be added to the vCenter server inventory.



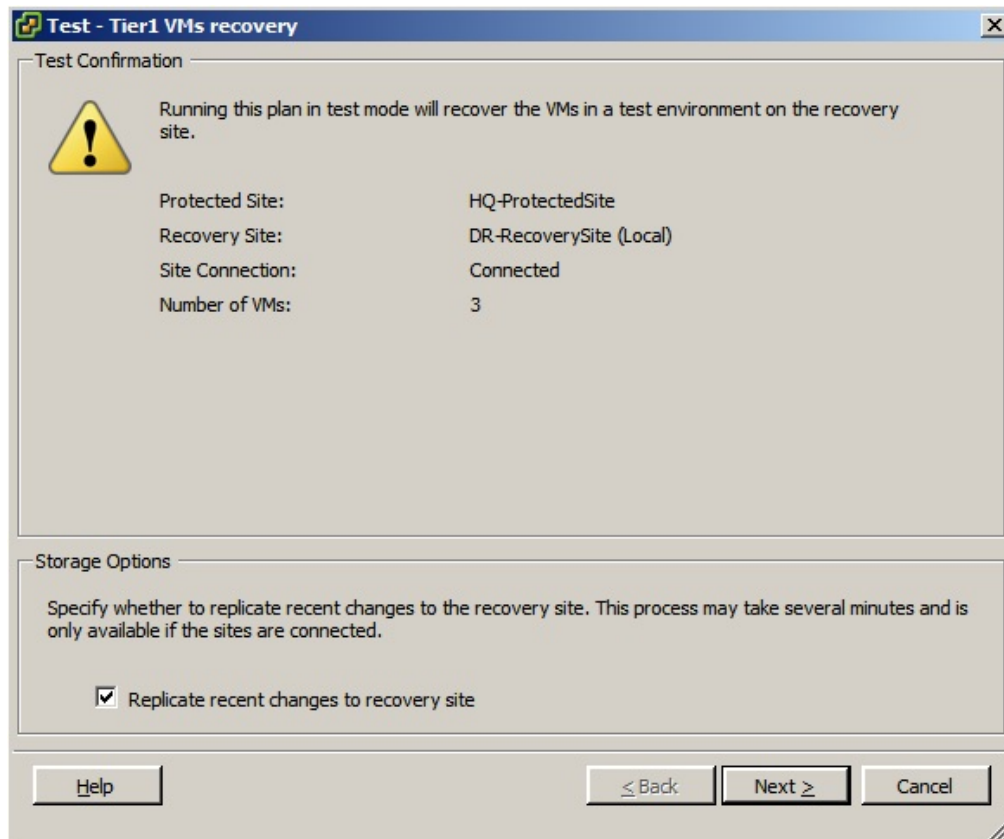
STEP 1

In the Recovery Plan section of the navigation screen on the left, select the recovery plan to test.

STEP 2

Click the **Recovery Steps** tab, and ensure that the View drop-down menu is set to show **Test Steps**.

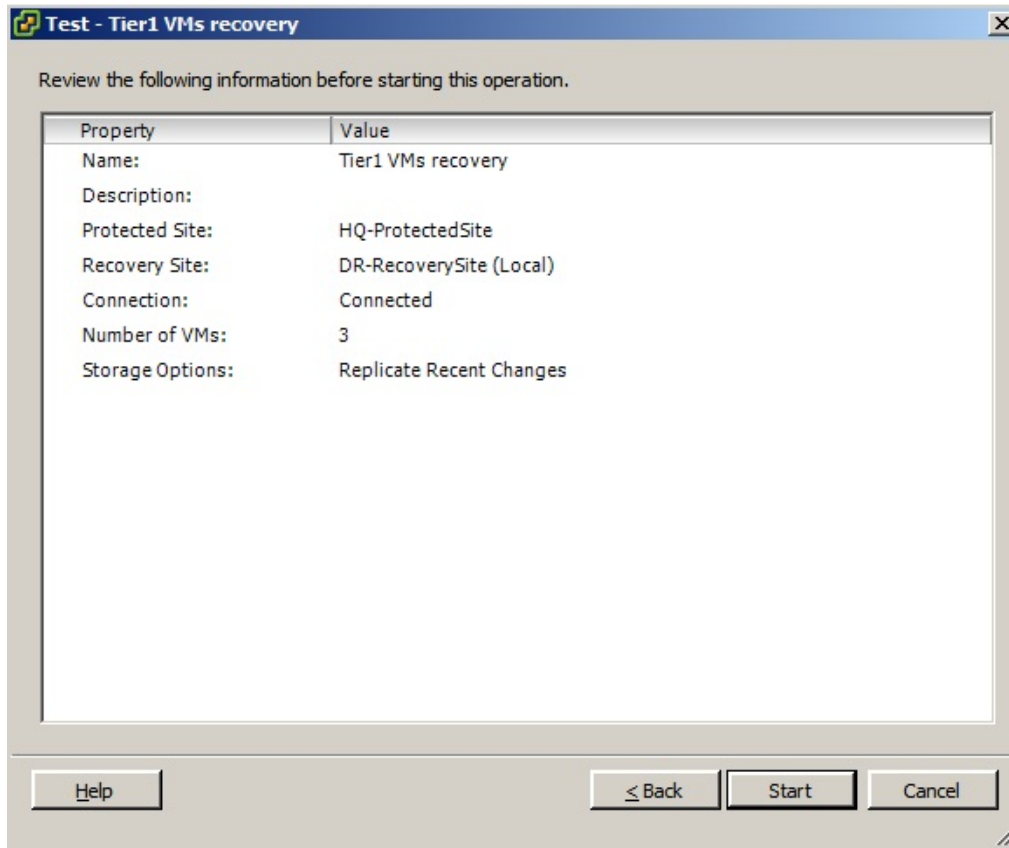
STEP 3



In the Commands area of the Summary window, click the text labeled **Test**. In the Test VMs recovery screen, click **Next**.

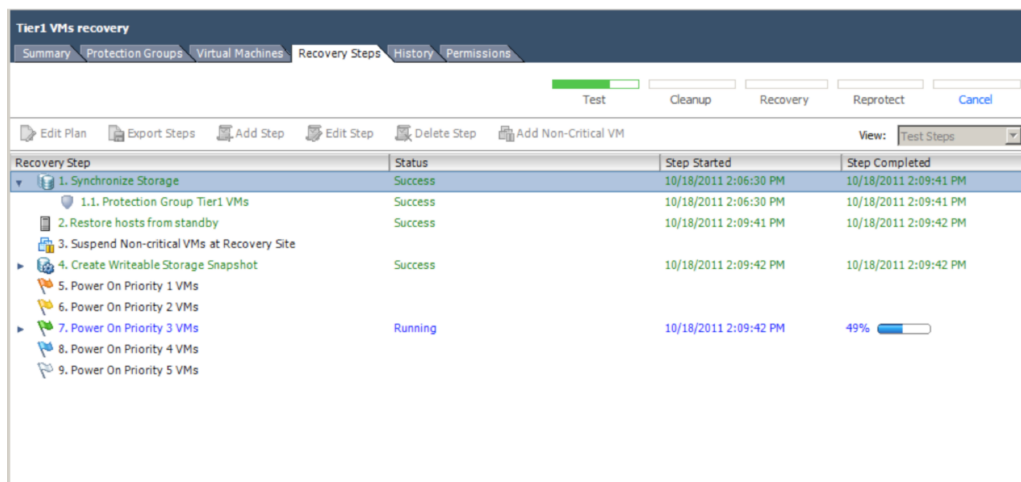


STEP 4



Verify the options selected for the recovery plan test, and click **Start** to initiate the test.

Step 5



While the simulated failover test is running, the status of each step in the recovery plan can be monitored.

Drobo • 2460 North First Street, Suite 100, San Jose, CA • www.drobo.com • 1.866.97.DROBO

Copyright 2011 Drobo, Inc. Data Robotics, Drobo, DroboElite, DroboPro, BeyondRAID, and Smart Volumes are trademarks of Drobo, Inc., which may be registered in some jurisdictions. All other trademarks used are owned by their respective owners. All rights reserved. Specifications subject to change without notice. • HT-0060-00 • October 2011