Dell PowerVault MD Series Storage Replication Adapter Best Practices Guide (Web Client)

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2015 - 10

Rev. A02

Contents

1

SRA download

The Dell Modular Disk (MD) Storage Replication Adapter (SRA) is used with VMware vCenter Site Recovery Manager (SRM) to facilitate Datacenter failover between separate VMware vCenter Server environments. To use the SRA, download the latest version of the SRA from VMware vCenter SRM download page at **http://www.vmware.com/download**.

For the latest version, see the Support Matrix available at the **Dell.com/support**.

Checksums may be calculated on any UNIX host with md5sum installed or by obtaining a Windows utility like `md5sum.exe` ROM **http://etree.org/md5com.html** and issuing the following from a command prompt.

- `md5sum <file_name>`

The `SRAInstaller-05.60.3000.xxxx.md5` file is also included with the SRA downloaded package; you can run the following command to verify the installer package.

```
md5sum -c SRAInstaller-05.60.3000.xxxx.md5
```

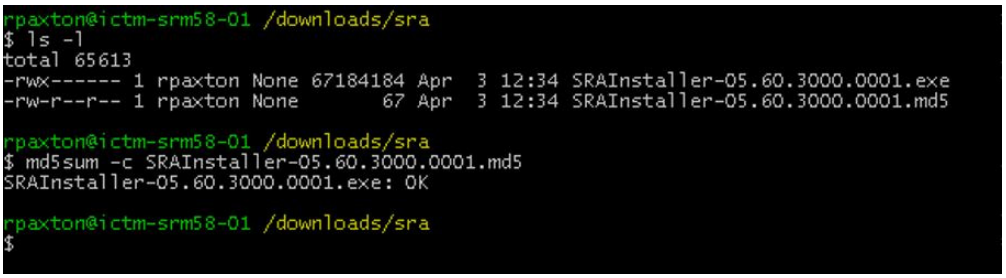

Figure 1. Example MD5 Evaluation

Installation procedure

After verifying that the download file is complete and not corrupted, perform the following steps:

1. Copy the installer to the SRM servers.
2. Run the SRA installer on these SRM systems.
3. To accept the End-User License Agreement, follow the prompts and installation paths.
   The SRA is installed in the following location:

   Install Directory:

   - C:\Program Files (x86)\Dell\MD SRA

   Scripts Directory:

   - C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\MD
4. After installing, rescan for SRAs from the SRM inside vSphere Web Client

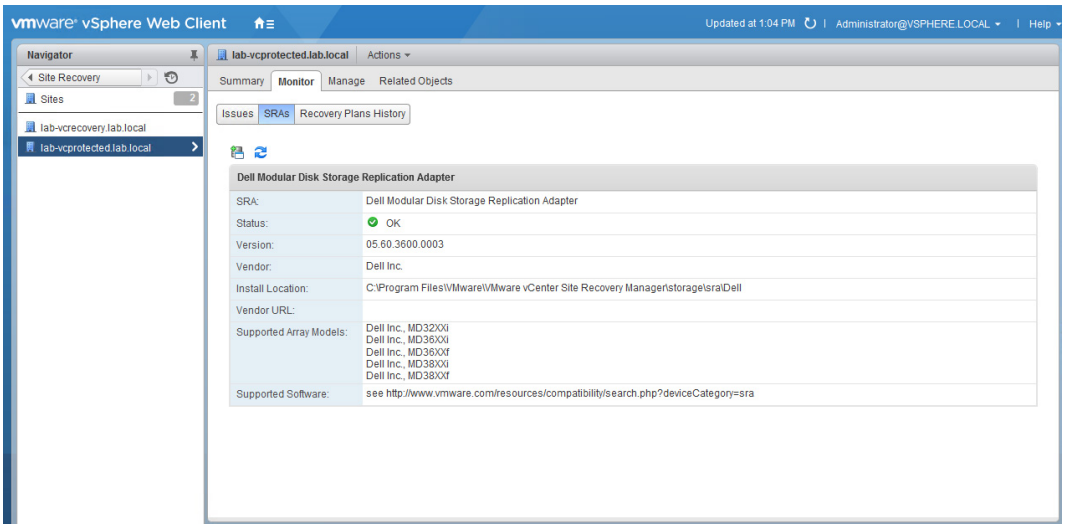

Figure 2. Site Recovery Manager (Rescan SRAs)

3

Password protected storage arrays

If your environment implements password security on the storage arrays, modify the `SraConfigurationData.xml` file to prompt for the storage array password. To modify the file, complete the following tasks:

1. Edit C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\ MD\config\SraConfigurationData.xml file.
2. Locate the`<PasswordRequiredForArrayAccess>` tag.
3. Change the default value of "false" to "true".
4. Save the file changes, and then rescan SRAs within SRM Array Manager.

NOTE: All storage arrays must utilize the same security measures. If one storage array has a password set, the peer storage array must also have the password set. Mixed authentication mode is not supported by the SRA.

```
<!--
configure how array access is performed.

when true, a password is prompted for once and

then used for all array access

-->

<PasswordRequiredForArrayAccess>true</PasswordRequiredForArrayAccess>
```

4

Snapshot repository sizing

Point-in-time snapshots provide the ability to roll back virtual disks to previous point-in-time saves, and optimize the data changes between snapshot images. This feature utilizes two separate repositories, the Snapshot Group repository and Snapshot Virtual Disk repository, to facilitate tracking of changes to the base virtual disk.

Snapshot Group repository

The Snapshot Group repository is used to track data changes to the base virtual disk; the virtual disk from which the Snapshot Image was created. The Snapshot Group repository may contain multiple Snapshot Images (point-in-time records of base virtual disk). A Snapshot virtual disk is created from these images and you can map them to a host for access.

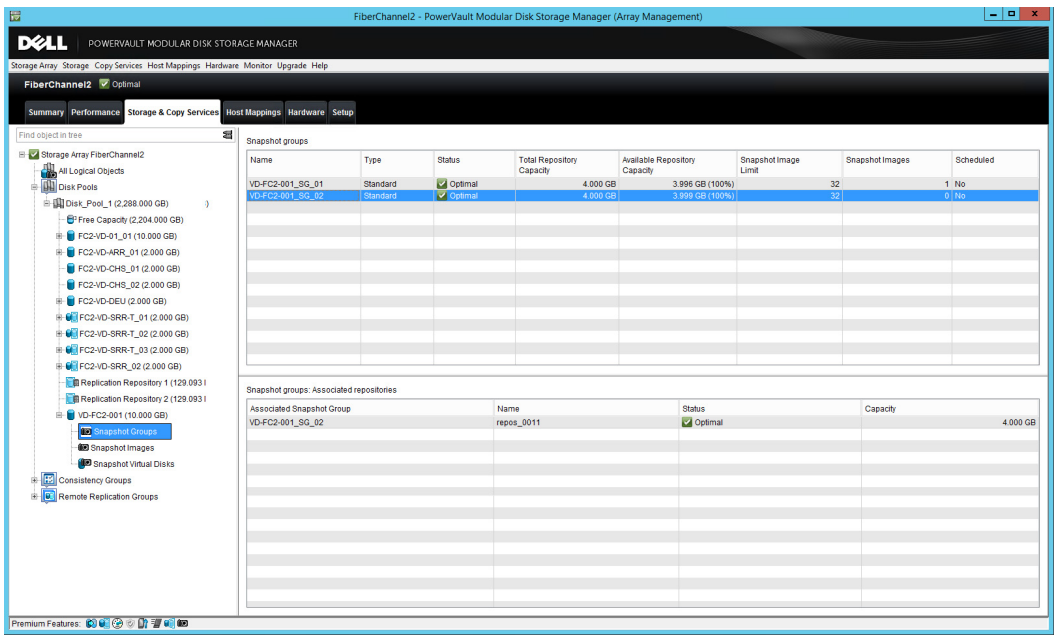

Figure 3. MD Storage Manager Snapshot Group View

Snapshot Virtual Disk repository

The Snapshot Virtual Disk repository is used to track data changes to the Snapshot Virtual Disk, if read/write access is allowed. After you map a Snapshot Virtual Disk to a host for access, any changes to the virtual disk are tracked within this repository.

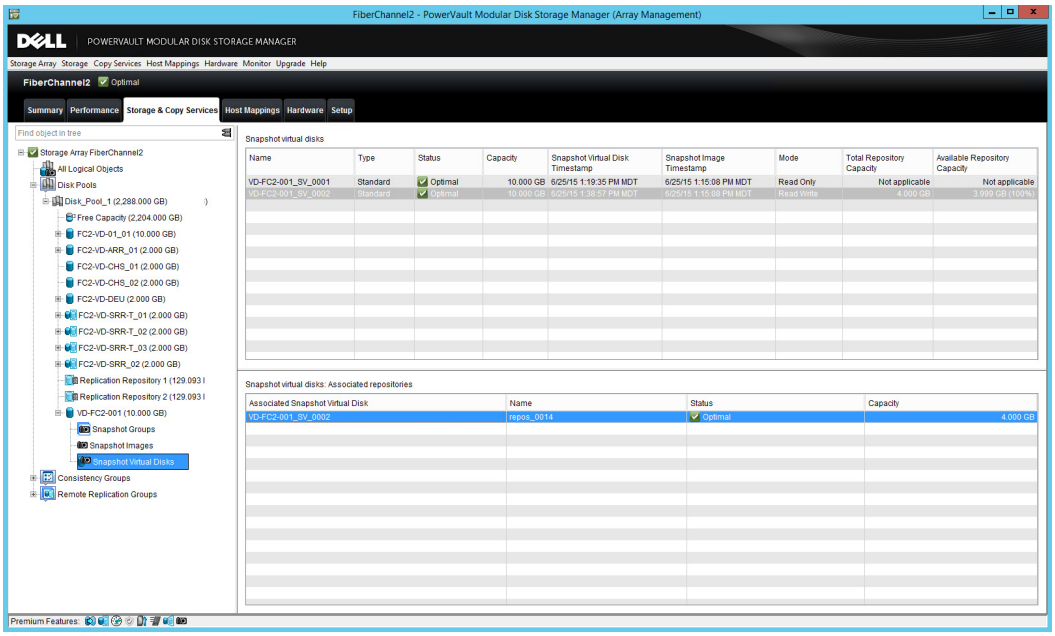

Figure 4. MD Storage Manager Snapshot Virtual Disk View

How SRA uses snapshots

The MD SRA uses Point-in-Time Snapshots if the feature is enabled on the storage array. During test failover, the SRA creates a Snapshot Group, Snapshot Image, and Snapshot Virtual Disk on the recovery site's storage array for all virtual disks contained in the protection groups being tested. This process requires the creation of the two snapshot repositories, listed earlier. The default size for these repositories is 10 percent of the base virtual disks for each repository, for a total of 20 percent of the base virtual disk size, which means that the free disk space on the recovery site storage array must be 20 percent of the base virtual disks participating in the test failover virtual disks. This value is controlled by the SraConfigurationData.xml file located in the config directory under the installation directory, typically:

C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\MD\config\SraConfigurationData.xml

The value is set with the XML tag `<SnapshotBasePercentage>`.

```
<!--

SnapshotBasePercentage represents the initial size, expressed as a percentage of virtual
disk size, of a snapshot which is formed for test failover.

-->

<SnapshotBasePercentage>10</SnapshotBasePercentage>
```

On the basis of how you use the VMs during test failover, you can fine-tune this value for your environment to reduce the free disk space required for test failover. If the test VM that is stored on the recovery site ESX host does not write extensive data to the Datastores and no synchronization (or minimal changes) occur between the protected site virtual disks and the recovery site virtual disks during test failover, you may decrease this value to 2–5 for even less free disk space during test failover. The Snapshot Virtual Disks and Snapshot Group repositories are deleted during the cleanup phase of test failover along with the Snapshot Image.

Because the Snapshot Virtual Disk is typically not used during the test failover process (minimal write activity), you may decrease the size of these repositories to small sizes in order to preserve free disk space on the recovery site's storage array. If a repository runs out of disk space during the test failover phase, the VMs on the recovery site lose access to the Datastore and underlying virtual disk is affected by the out-of-space condition of the repository, but the protected site VM functions as normal. Dell does not

recommend using these values for Snapshot repositories for other purposes. You can monitor the sizes and status of the repositories from within MD Storage Manager by selecting the **All Logical Objects** container, and then selecting **Repositories** in the **Object Type** drop-down menu.

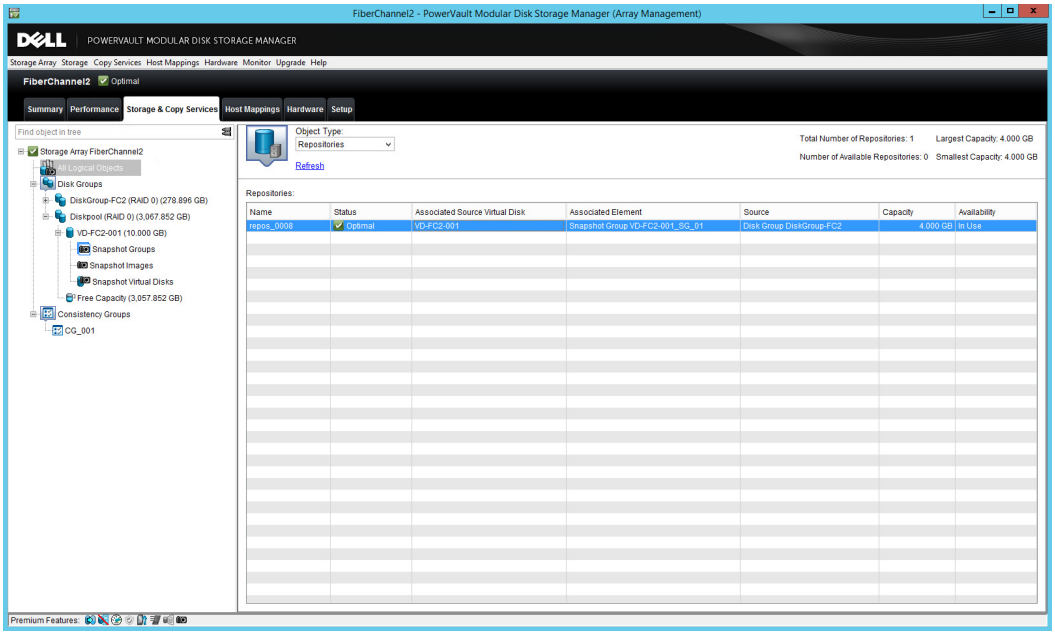

Figure 5. MD SRA Repository View

You can view more information, such as available repository space, mode, and timestamps by selecting **Snapshot Virtual Disks** or **Snapshot Groups** in the drop-down menu.

5

NVSRAM settings

You must change the following NVSRAM setting to allow for the mapping of LUNs to multiple hosts or host groups in order to support test failover within SRM. During test failover, snapshots are created on the Recovery Site Storage Array. You can map these snapshots to multiple hosts or host groups of the ESX or ESXi host participating in the recovery.

1. From the **MD Storage Manager Enterprise Management window**, select **Tools** → **Execute Script** option from the drop-down menu.
2. Enter the following commands at the script editor window:

   ```
   show allControllers NVSRAMByte[0x3b];

   set controller [0] NVSRAMByte[0x3b]=2;

   set controller [1] NVSRAMByte[0x3b]=2;

   reset controller [0];

   reset controller [1];
   ```
3. Select **Tools** → **Verify and Execute** option from the menu.
4. To apply the changes to the RAID controller module 1, repeat steps 2 and 3, substituting [1] for [0].
5. Exit the script editor after completing the changes for the RAID controller module 1.

   The controllers take several minutes to reset and the execution message to complete.

   This procedure maps a virtual disk to two hosts or host groups (increasing [0x3b]=x, define the number of hosts or host groups allowed).

6

MD SRA device management service

The MD SRAsvc process monitors and synchronizes communications between the SRA and the MD storage arrays. SRA workload is partitioned between a persistent server and multiple transient client programs, which endure only during a single SRM command. Because it is typical to run many SRM commands while performing a single SRM workflow (such as test failover), clients come and go frequently, while the server, running as a Windows Service, persists and manages all communications with storage arrays.

Typically, you do not need to configure the server, which functions at its default values. When it is necessary to configure the server for nonstandard operation, there are two files that you can edit (for different reasons):

The SRA Configuration file, SraConfigurationData.xml – in the config directory under the SRA's script directory, typically `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\MD\config\SraConfigurationData.xml`.

The Win32 Service initialization file, NesSvc.ini, in the win32svc directory under the SRAs installation directory, typically `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\MD\win32svc\NesSvc.ini`.

Server settings in SRA configuration data

The portion of `SraConfigurationData.xml` relevant to service configuration is the following:

```
<SraService>
<SvcHost>localhost</SvcHost>

<ServicePort>1701</ServicePort>

<ListenBacklog>100</ListenBacklog>

</SraService>
```

Its content is as follows:

SvcHost : determines the host on which NesSvc is running. The only allowed value is "localhost". In future releases, it may be possible to share instances of NesSvc across multiple installations of this SRA, further enhancing performance and simplifying cooperation between multiple SRA instances.

ServicePort: determines which IP port the service uses for socket communications between the client and server. If another application on your system is already using port 1701 (the default), then, set this value to another port number.

ListenBacklog: configures a performance property of the port. You should modify performance property only when consulting technical support personnel.

SRA Windows service initialization file

In normal circumstances, you should not modify the windows service initialization file. The exception is when you need to modify the virtual settings that the server uses. After consultation with technical support, you can modify the following lines:

vmarg.1=-Xms256m

vmarg.2=-Xmx512m

NOTE: If you modify this file, stop and restart to implement the new settings.

7

Asynchronous remote replication

The Asynchronous Remote Replication (aRR) feature allows for a new method of remote replication utilizing point-in-time copies. This feature supports both Fibre Channel and iSCSI remote array connections. The key features of aRR to consider for SRM are:

- Support for both Fibre Channel and iSCSI remote array replication
- Maximum of four asynchronous remote replication groups (RRG) for each array
- 10-minute sync interval between point-in-time copies

iSCSI remote replication

aRR supports remote replication by using iSCSI protocol, which allows for greater distances for array-based replication at a cost of latency. Ensure that during datastore creation only data that must be replicated is included on the virtual disks you replicate. Observe and calculate the value data being replicated and the time required to synchronize the data to determine the expected delay time between synchronization periods. If the amount of time required to synchronize data is more than the synchronization interval, the RRG becomes degraded and nonfunctional. Proper sizing of WAN infrastructure is critical for a successful DR solution.

Effects of four asynchronous remote replication

With a maximum of 4 RRGs, all protected Datastore virtual disks must reside in one of the four groups. A group is treated as a single entity; thereby, when swapping roles, all virtual disks contained in the RRG are changed. If cross replication of Datastores is required (for example, replicating from recovery site to protected site), the Datastore virtual disks from the recovery site must be contained in a separate RRG from the virtual disks for the protected site.

Effects of 10-minute sync interval

RRGs require a 10-minute interval between both automated and manual synchronizations. This interval means that requesting a manual synchronization of the RRG may not occur until after the minimum interval has been reached (10 minutes). This interval may cause a delay in the SRM workflow process, which requires several sync operations to occur for both test failover and failover workflows. The SRA is optimized to avoid requesting a manual synchronization if no changes are detected in the RRG, but if changes are detected, synchronization is requested. Therefore, you may observe a lack of progress or slow progress through the SRM workflows.

8

General virtual disk recommendations

When designing a DR strategy by using VMware vCenter SRM and MD storage arrays, consider the following:

- Protection works on a datastore level (storage array virtual disk). All VMs that require protection on the same datastore as the VM will also be protected and replicated.
- Use multiple small datastores and virtual disks to limit the size of data replicated across to the recovery site.
- Locate (migrate) protected VMs to the same datastore and migrate off any VMs that do not require protection.
- SRM does not provide for application-consistent failover, but VM-consistent failover. Therefore, even with a successful failover of a VM, the applications that were running on the VM may not be in a consistent state and may require more recovery methods to return to normal operation.
- MD storage arrays with firmware of 07.84.XX.XX or greater support remote replication groups, which are treated as a consistency group. Therefore, all virtual disks within the RRG are treated as a single entity and failed over at the same time.
- Synchronization priority has a dramatic effect on the speed of replication. If sufficient bandwidth is available between the peer storage arrays, Dell recommends setting to high or highest.

9

SRA command line options

The SRA installs a command line utility that provides the following functions:

- **Trace Logging**: This option provides detailed logging for each command run and received by the SRA. The log files are placed in the `<SRA_Path>\track` directory. The command line options are `<SRA_Path>\svrCmd track on` to enable or `<SRA_Path>\svrCmd track off` to disable.

10

SRA java update script

Installed with the SRA is a command line utility to update the Java runtime environment, in the event an updated JRE is required. This script is called `UpdateJREPath.bat` and is typically located in the `C:\Program Files (x86)\Dell\ Storage Replication Adapter` directory.

- Running the batch file without any options displays the current JRE path that is used by the SRA.
- Running the batch file with the absolute path to a new JRE path updates the configuration files to point to the new location and restarts the SRA service.

SRM Advanced Settings

SRM settings are accessed by selecting **Sites** from the SRM, selecting a specific site, the **Manage** tab, and then the **Advanced Settings** button (see Figure 6). You can select the settings group to edit.

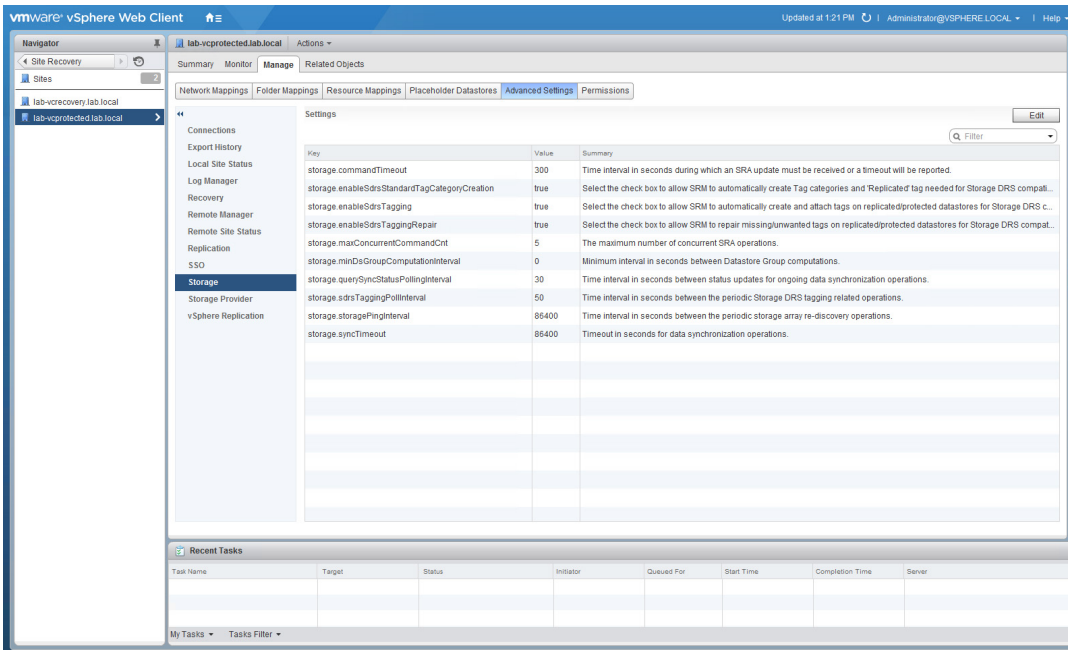

Figure 6. SRM Advanced Settings

Dell recommends the following changes for proper SRA operation:

- storage.commandTimeout = 900
- storageProvider.hostRescanRepeatCnt = 2
- storageProvider.hostRescanTimeoutSec = 900

The following are recommended based on your environment:

- storageProvider.fixRecoveredDatastoreNames = true

Additionally, Dell recommends the following changes for ESX/ESXi host settings:

- `Disk.MaxLUN` = Set this value slightly higher than the number of LUNs mapped to the ESX host. This setting provides faster rescan operations by not scanning all 256 LUN possibilities.
- `Disk.UseDeviceReset` = 0 and Disk.UseLunReset = 1 (These two settings used together indicate how device resets are issued.)

12

Troubleshooting tips

In certain environments, you may need to implement one or all the following settings to enable successful operation of the SRA. Do not change these settings unless advised by technical support. These are nonstandard settings; therefore, you should use them only if your environment is experiencing the symptoms described for the change.

Datastore expected to be automounted

Error: Failed to recover Datastore 'XYZZY'. Datastore residing on recovered devices and expected to be automounted during HBA rescan cannot be found.

Potential Fix: Modify `C:\Program Files (x86)\VMware\VMware vCenter Site Recovery Manager\config \vmware-dr.xml` file and add the following to the `<storageProvider>` section.

```
<storageProvider>

<waitForRecoveredDatastoreTimeoutSec>300waitForRecoveredDatastoreTimeoutSec>300>

<waitForAccessibleDatastoreTimeoutSec>900waitForAccessibleDatastoreTimeoutSec>900>

</storageProvider>
```

You must restart the **VMware vCenter Site Recovery Manager Server** after applying this change. This increases the timeout for snapshot mount operations.

Unable to communicate with remote host

Error: Failed to recover datastore 'CG26'. VMFS virtual disk residing on recovered devices '"67:82:BC:B0:00:28:AB:8B: 00:00:41:C8:50:C8:26:BA"' cannot be found. Recovered device '67:82:BC:B0:00:28:AB:8B:00:00:41:C8:50:C8:26:BA' not found after HBA rescan. Failed to rescan HBAs on host '10.26.25.108'. Unable to communicate with the remote host, since it is disconnected.

Possible Solution 1: **(For vCenter Server 5.x only)** Modify `C:\Program Files\VMware\ Infrastructure\tomcat\conf \wrapper.conf` and change the following:

```
wrapper.java.additional.9="-Xmx2048M"
```

This modification changes the maximum disk space for the VMware vCenter Inventory Services. Restart the vCenter Server to apply this change.

Possible Solution 2: **(For ESXi 5.x Only)** Modify `/etc/vmware/vpxa/vpxa.cfg` and add the following section to increase the ping timeout for SOAP requests.

```
<vmomi>
<calls>false</calls>

<soapStubAdapter>

<pingTimeoutSeconds>300</pingTimeoutSeconds>
```

```
</soapStubAdapter>

</vmomi>
```

This modification requires a restart of the ESXi host system.

Possible Solution 3:**(For ESXi 5.x Only)** Modify `/etc/vmware/hostd/config.xml` and add the following entry under <vmacore>/<ssl>:

```
<ssl>

<doVersionCheck>false</doVersionCheck>

<useCompression>true</useCompression>

<handshakeTimeoutMs>120000</handshakeTimeoutMs>

<libraryPath>/lib/</libraryPath>

</ssl>
```

This modification increases the SSL handshake timeout value. This change may be necessary on busy systems. You must restart the ESXi host to apply this change.

Failed to create snapshot RetCode 660

Error: Failed to create snapshots of replica devices. Failed to create snapshot of replica consistency group 67:82:BC:B0:00:28:AB:8B: 00:00:42:40:50:C8:2E:F8. SRA command 'testFailoverStart' failed for consistency group '67:82: BC:B0:00:28:AB:8B: 00:00:42:40:50:C8:2E:F8'. Failed to create snapshot image in snapshot group SRMt-CG09m_G. Reason: 660 See log for more information. Use the RetCode utility to interpret code 660.

Solution: This error requires a firmware upgrade to 07.84.44.xx or later.

Workarounds:

- Adding additional virtual disks to the aRR group may alleviate this issue.
- Ensuring both source and target virtual disks reside on same controller (0 or 1) may alleviate this issue.
- Using Legacy aRR avoids this situation. It is not a valid solution for iSCSI configurations.

13

Getting help

Documentation matrix

The documentation matrix provides information about documents that you can refer to for setting up and managing your system.

Dell documentation

- For all PowerEdge and PowerVault documentation, go to **Dell.com/support** and enter the system Service Tag to get your system documentation.
- For all Virtualization documents, go to **Dell.com/virtualizationsolutions**.
- For all operating system documents, go to **Dell.com/operatingsystemmanuals**.
- For all storage controllers and PCIe SSD documents, go to **Dell.com/storagecontrollermanuals**.
- For Dell Support Forums, go to **en.community.dell.com/support-forums/default.aspx**.
- For Dell Advanced Search, go to **search.dell.com/index.aspx**.

VMware documentation

- For vCenter SRM 6.0 documentation, go to

  https://www.vmware.com/support/pubs/srm_pubs.html
- For vSphere 6.0 Documentation (ESXi, ESX, and vCenter Server), go to

  https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html
- For information about VMware Knowledge Base (Searchable Support Issues), go to

  http://kb.vmware.com/selfservice/microsites/microsite.do
- For information about VMware Communities (Help Forums), go to

  https://communities.vmware.com/welcome
- For VMware Compatibility Guide, go to

  http://www.vmware.com/resources/compatibility/search.php?deviceCategory=io

Contacting Dell

Dell provides several online and telephone-based support and service options. If you do not have an active internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical assistance, or customer-service issues:

1. Go to **Dell.com/support**.
2. Select your country from the drop-down menu on the bottom right corner of the page.
3. For customized support:
   a. Enter your system Service Tag in the **Enter your Service Tag** field.
   b. Click **Submit**.

The support page that lists the various support categories is displayed.

4. For general support:
   a. Select your product category.
   b. Select your product segment.
   c. Select your product.

      The support page that lists the various support categories is displayed.

Locating your system Service Tag

Your system is identified by a unique Express Service Code and Service Tag number. The Express Service Code and Service Tag are found on the front of the system by pulling out the information tag. This information is used by Dell to route support calls to the appropriate personnel.