



NetApp SANtricity® Storage Replication Adapter 5.6

Best Practices Guide

September 2016 | 215-10052_C0
doccomments@netapp.com

TABLE OF CONTENTS

SRA DOWNLOAD	2
INSTALLATION PROCEDURE	2
PASSWORD PROTECTED STORAGE ARRAYS	3
SNAPSHOT REPOSITORY SIZING	3
NVSRAM SETTINGS	6
NETAPP SANTRICITY SRA DEVICE MANAGEMENT SERVICE	6
SERVER SETTINGS IN SRA CONFIGURATION DATA	6
SRA WINDOWS SERVICE INITIALIZATION FILE	7
ASYNCHRONOUS MIRRORING	7
ISCSI REMOTE MIRRORING	7
EFFECTS OF 4 ASYNCHRONOUS MIRROR GROUPS	7
EFFECTS OF 10 MINUTE SYNC INTERVAL	7
GENERAL VOLUME RECOMMENDATIONS	8
SRA COMMAND LINE OPTIONS	8
SRA JAVA UPDATE SCRIPT	8
SRM ADVANCED SETTINGS	8
TROUBLESHOOTING TIPS	9
DATASTORE EXPECTED TO BE AUTO-MOUNTED	9
UNABLE TO COMMUNICATE WITH REMOTE HOST	10
FAILED TO CREATE SNAPSHOT RETCODE 660	11
STEPS TO RECOVER FROM A SITE/ARRAY DOWN	11
ADDITIONAL INFORMATION	11
PHONE SUPPORT	11
COMMUNITY SUPPORT	11

LIST OF FIGURES

Figure 1 - Example MD5 Evaluation	2
Figure 2 - Site Recovery Manager (Rescan SRAs)	3
Figure 3 - SANtricity Snapshot Group View	4
Figure 4 - SANtricity Snapshot Volume View	4
Figure 5 - SANtricity Repository View	5
Figure 6 - SRM Advanced Settings.	9

SRA DOWNLOAD

The NetApp® SANtricity™ Storage Replication Adapter (SRA) is used in conjunction with VMware vCenter Site Recovery Manager (SRM) to facilitate Datacenter failover between separate VMware vCenter Server environments. To utilize the SRA, download the latest version of the SRA from VMware vCenter Site Recovery Manager download page at <http://www.vmware.com/download>.

- Current version is 05.60
- Installer: SRAInstaller-05.60.3000.xxxx.exe
- md5sum: (Refer to the SRAInstaller-05.60.3000.xxxx.md5 file for checksum)

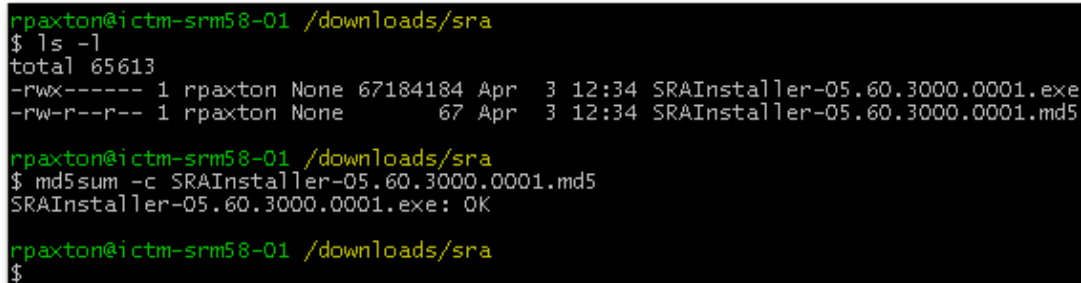
Checksums may be calculated on any UNIX host with md5sum installed or by obtaining a Windows utility like md5sum.exe from <http://etree.org/md5com.html> and issuing the following from a command prompt.

- 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



```
rpaxton@ictm-srm58-01 /downloads/sra
$ ls -l
total 65613
-rwx----- 1 rpaxton None 67184184 Apr  3 12:34 SRAInstaller-05.60.3000.0001.exe
-rw-r--r-- 1 rpaxton None      67 Apr  3 12:34 SRAInstaller-05.60.3000.0001.md5

rpaxton@ictm-srm58-01 /downloads/sra
$ md5sum -c SRAInstaller-05.60.3000.0001.md5
SRAInstaller-05.60.3000.0001.exe: OK

rpaxton@ictm-srm58-01 /downloads/sra
$
```

INSTALLATION PROCEDURE

After verifying the download file is complete and not corrupted, copy the installer to the SRM servers that will be used. Execute the SRA installer on these SRM systems. Follow the prompts to accept the End User License Agreement and installation paths. You may view the latest information contained in the readme.txt file at the end of the installation by clicking on the Yes to view the readme. The SRA will be installed in the following location:

Install Directory:

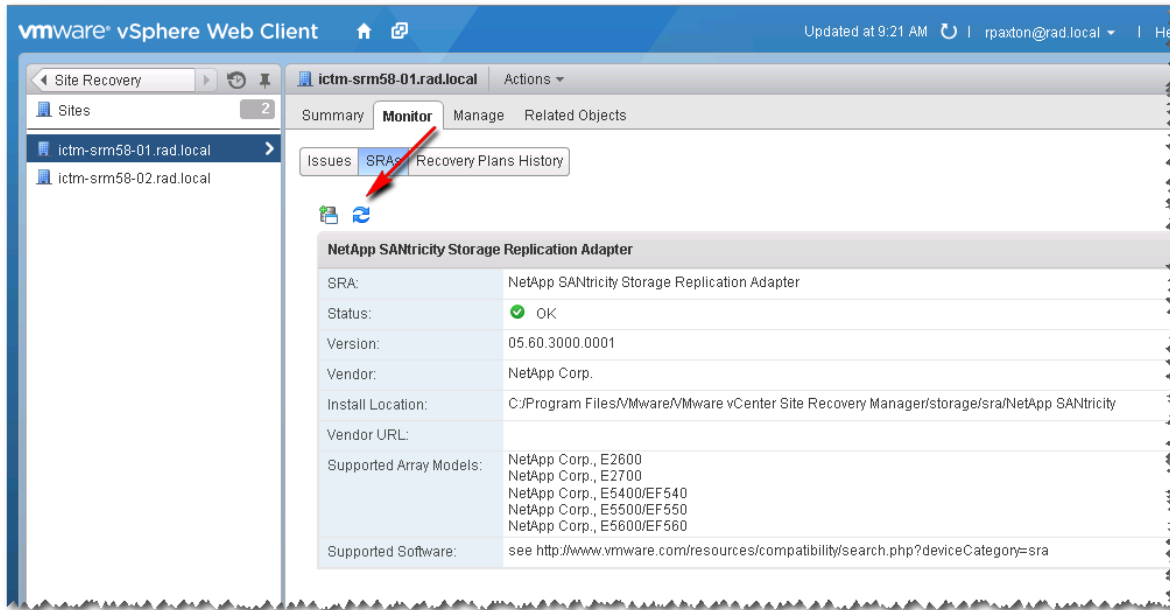
- C:\Program Files (x86)\NetApp\SANtricity Storage Replication Adapter

Scripts Directory:

- C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\NetApp SANtricity

Once installed, rescan for SRAs from the Site Recovery manager inside vSphere Client.

Figure 2 - Site Recovery Manager (Rescan SRAs)



PASSWORD PROTECTED STORAGE ARRAYS

If your environment implements password security on the storage arrays, the SraConfigurationData.xml file must be modified to prompt for storage array password. This is accomplished by the following:

- Edit C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\ sra\Netapp SANtricity\config\SraConfigurationData.xml file.
- Locate the <PasswordRequiredForArrayAccess> tag
- Change the default value of "false" to "true"
- Save the file changes and rescan SRAs within SRM Array Manager.

Note: All storage arrays must utilize the same security measures. If one storage array has a password set, then 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 will be prompted for once and  
then used for all array access  
-->  
<PasswordRequiredForArrayAccess>true</PasswordRequiredForArrayAccess>
```

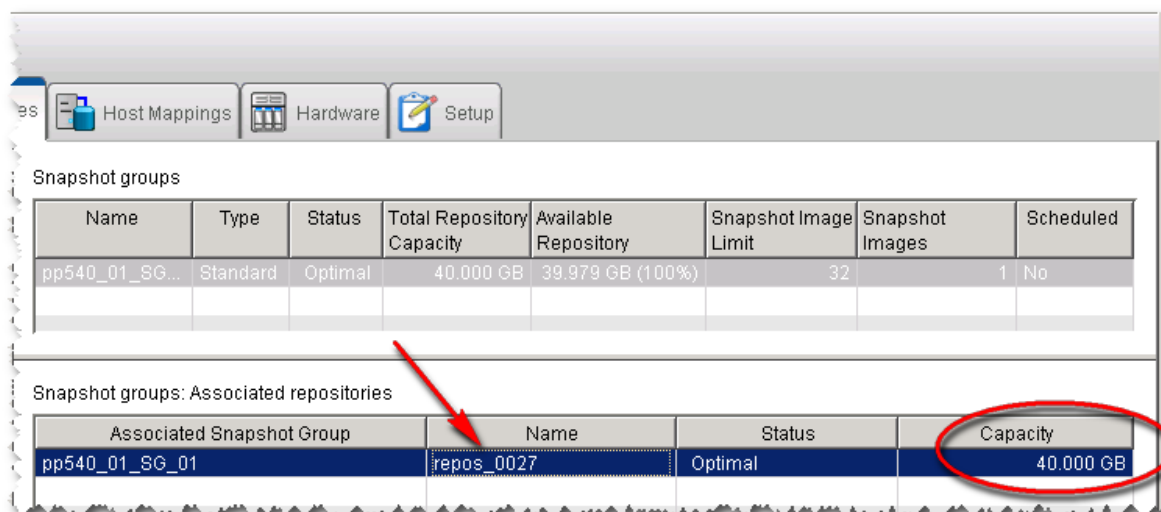
SNAPSHOT REPOSITORY SIZING

Point-in-time snapshots provide the ability to roll-back volumes to previous point-in-time saves and optimize the data changes between snapshot images. This feature utilizes two separate repositories to facilitate tracking of changes to the base volume. They are the Snapshot Group repository and Snapshot Volume repository.

SNAPSHOT GROUP REPOSITORY

The Snapshot Group repository is used to track data changes to the base volume (volume that the Snapshot Image was created from). The Snapshot Group repository may contain multiple Snapshot Images (point-in-time records of base volume). A Snapshot Volume is created from these images and can then be mapped to a host for access.

Figure 3 - SANtricity Snapshot Group View



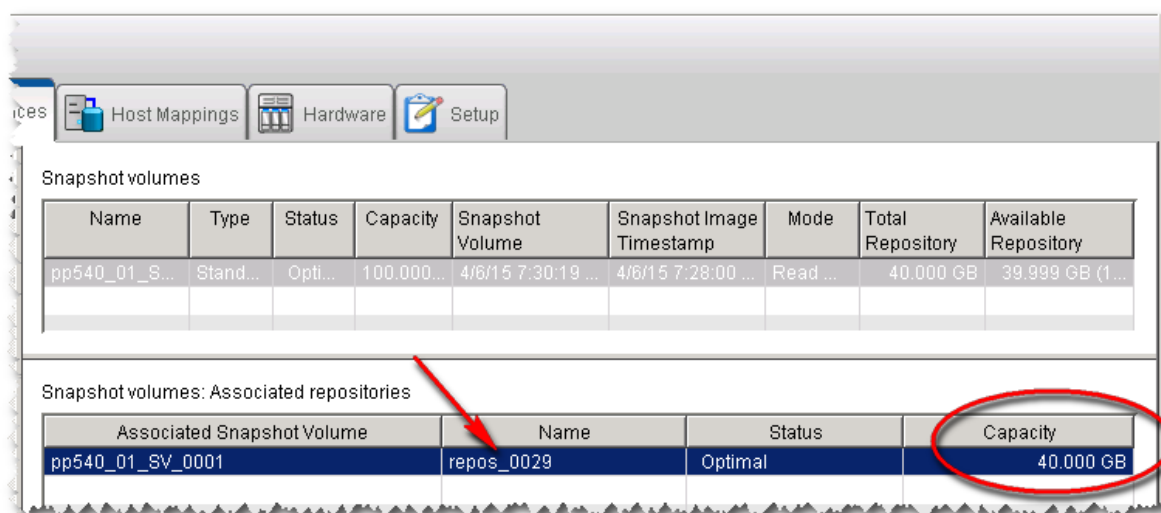
Name	Type	Status	Total Repository Capacity	Available Repository	Snapshot Image Limit	Snapshot Images	Scheduled
pp540_01_SG...	Standard	Optimal	40.000 GB	39.979 GB (100%)	32	1	No

Associated Snapshot Group	Name	Status	Capacity
pp540_01_SG_01	repos_0027	Optimal	40.000 GB

SNAPSHOT VOLUME REPOSITORY

The Snapshot Volume repository is used to track data changes to the Snapshot Volume, if read/write access is allowed. Once a Snapshot Volume is mapped to a host for access any changes to the volume are tracked within this repository.

Figure 4 - SANtricity Snapshot Volume View



Name	Type	Status	Capacity	Snapshot Volume	Snapshot Image Timestamp	Mode	Total Repository	Available Repository
pp540_01_S...	Stand...	Opti...	100.000...	4/6/15 7:30:19 ...	4/6/15 7:28:00 ...	Read ...	40.000 GB	39.999 GB (1...

Associated Snapshot Volume	Name	Status	Capacity
pp540_01_SV_0001	repos_0029	Optimal	40.000 GB

HOW SRA USES SNAPSHTOS

The NetApp SANtricity SRA will utilize Point-in-Time Snapshots if the feature is enabled on the storage array. During test failover, the SRA will create a Snapshot Group, Snapshot Image, and Snapshot Volume on the recovery site's storage

array for all volumes contained in the protection groups being tested. This requires the creation of the two snapshot repositories listed above and the default size for these repositories is 10% of the base volume(s) for each repository, for a total of 20% of the base volume size. This means that the amount of free capacity on the recovery site storage array must be 20% of the base volumes participating in the test failover. 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\NetApp E-Series\config\SraConfigurationData.xml`

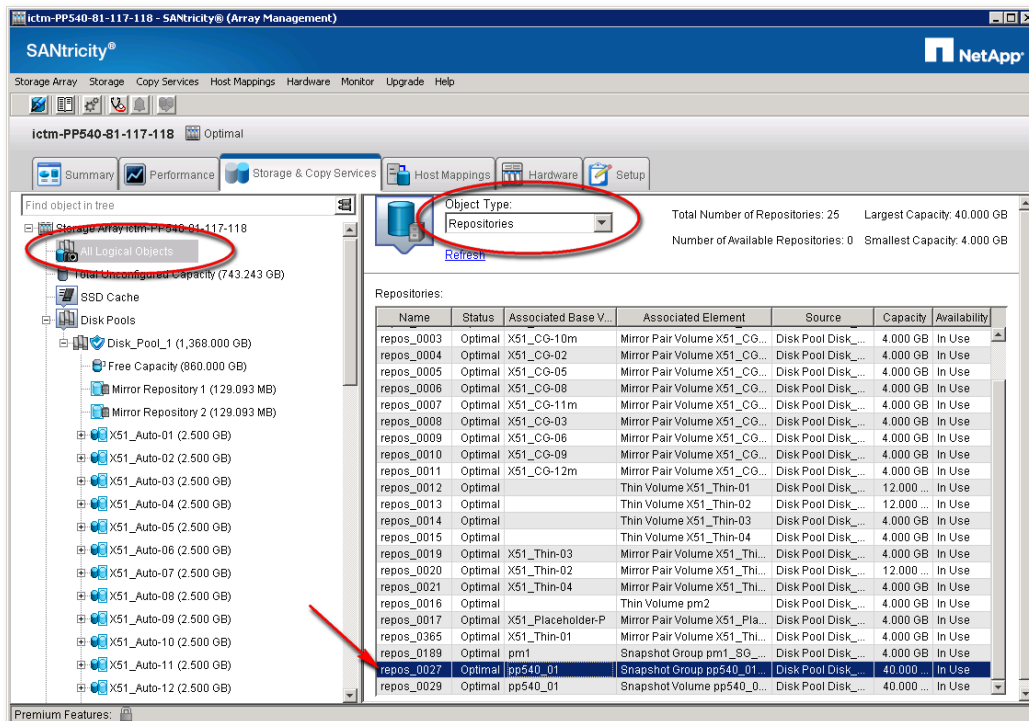
The value is set with the xml tag `<SnapshotBasePercentage>`.

```
<!--
SnapshotBasePercentage represents the initial size, expressed as a percentage of volume size, of a
snapshot which is formed for test failover.
-->
<SnapshotBasePercentage>10</SnapshotBasePercentage>
```

Depending on how the VMs are used during test failover, it is possible to fine tune this value for your environment to reduce the amount of free capacity needed for test failover. If the test VM residing 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 volumes and the recovery site volumes during test failover, this value may be decrease to 2-5 to require even less free capacity during test failover. The Snapshot Volume and Snapshot Group repositories are deleted during the cleanup phase of test failover along with the Snapshot Image.

Because the Snapshot Volume is typically not used during the test failover process (little write activity), the size of these repositories may be decreased to very small sizes in order to preserve free capacity on the recovery site's storage array. If a repository runs out of space during the test failover phase, the VMs on the recovery site will lose access to the Datastore and underlying volume affected by the out-of-space condition of the repository, but the protected site VM will function as normal. These values are not recommended for Snapshot repositories used for other purposes. The sizes and status of the repositories may be monitored from within SANtricity by selecting the All Logical Objects container and then selecting Repositories in the drop-down box:

Figure 5 - SANtricity Repository View



Additional details such as available repository space, mode, timestamps, etc. may be viewed by selecting the Snapshot Volumes or Snapshot Groups in the drop-down box.

NVSRAM SETTINGS

The following NVSRAM setting must be changed 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. These snapshots may be mapped to multiple hosts or host groups of the ESX/ESXi host participating in the recovery.

From the SANtricity Enterprise Management window, select **Tools → Execute Script** option from the menu pull-downs.

Enter the following commands in the script editor window:

```
show controller[A] NVSRAMByte[0x3b];
set controller[A] NVSRAMByte[0x3b]=2;
show controller[A] NVSRAMByte[0x3b];

reset controller[A];
```

Select **Tools → Verify and Execute** option from the menu pull-downs.

Repeat steps 2 and 3, substituting [B] for [A] to apply the changes to the B controller.

Exit the script editor after completing the changes for the B controller.

It will take several minutes for the controllers to reset and the execution message to complete.

This will allow for a volume to be mapped to two hosts or host groups (increasing [0x3b]=x, define the number of hosts or host groups allowed).

NETAPP SANTRICITY SRA DEVICE MANAGEMENT SERVICE

The NetAppSANtricity_SRAsvc process monitors and synchronizes communications between the SRA and the E-Series storage arrays. SRA workload is partitioned between a persistent server and multiple transient client programs which endure only for the duration of a single SRM command. Since it is typical for many SRM commands to be executed in the course of 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, no configuration is needed for the server, which will function at its default values. When it is necessary to configure the server for non-standard operation, there are two files which can be edited (for differing 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\NetApp SANtricity\config\SraConfigurationData.xml.
- The Win32 Service initialization file, **NesSvc.ini**, in the win32svc directory under the SRA's installation directory, typically C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\NetApp SANtricity\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 contents are as follows:

- **SvcHost** determines which host NesSvc is running on. **Currently the only allowed value for this 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 it will be necessary to set this value to another port number.
- **ListenBacklog** configures a performance property of the port. It should only be modified in consultation with technical support personnel.

SRA WINDOWS SERVICE INITIALIZATION FILE

In normal circumstances, there are no useful modifications that should be made to the windows service initialization file. One exception, after consultation with technical support may be to modify the following lines:

`vmarg.1=-Xms256m`

`vmarg.2=-Xmx512m`

These control the virtual memory settings with which the server uses.

Note: If this file is modified, the service must be stopped and re-started to implement the new settings.

ASYNCHRONOUS MIRRORING

Asynchronous mirroring feature allows for a new method of remote volume mirroring utilizing point-in-time copies and is referred to as aRVM. This feature supports both fibre channel and iSCSI remote array connections. The key features of aRVM to consider for SRM are:

- Support for both fibre channel and iSCSI remote array replication.
- Maximum of 4 asynchronous mirror groups (AMGs) per array.
- 10 minute sync interval between point-in-time copies.

ISCSI REMOTE MIRRORING

aRVM supports remote mirroring via iSCSI protocol. This allows for greater distances for array based replication at a cost of latency. Careful consideration should be taken during Datastore volume layout to ensure only data that is required to be replicated resides on volumes that are being replicated. Observation of the amount of data being replicated and the time required to synchronize the data should be calculated to determine the expected amount of delay between synchronization periods. If the amount of time required to synchronize data is more than the synchronization interval, the AMG will become degraded and non-functional. Proper sizing of WAN infrastructure is critical for a successful DR solution.

EFFECTS OF 4 ASYNCHRONOUS MIRROR GROUPS

With a maximum of 4 AMGs, all protected Datastore volumes must reside in one of the four groups. A group is treated as a single entity, thereby when swapping roles, all volumes contained in the AMG are changed. If cross replication of Datastores is required (i.e. mirroring from recovery site to protected site), the Datastore volumes from the recovery site must be contained in a separate AMG from the volumes for the protected site.

EFFECTS OF 10 MINUTE SYNC INTERVAL

AMGs require a 10 minute interval between both automated and manual synchronizations. This means that requesting a manual synchronization of the AMG may not occur until after the minimum interval has been reached (10 minutes). This 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 within the AMG, but if changes are detected, synchronization will be requested. The effect of this may be observed as a lack of progress or slow progress through the SRM workflows.

GENERAL VOLUME RECOMMENDATIONS

When designing a DR strategy using VMware vCenter Site Recovery Manager and NetApp E-Series and EF-Series storage arrays, several considerations should be observed.

- Protection works on a datastore level (storage array volume). All VMs located on the same datastore as the VM that requires protection will also be protected and replicated.
- Multiple small datastores and volumes should be used to limit the amount 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 additional recovery methods to return to normal operation.
- NetApp E-Series and EF-Series storage arrays with firmware of 07.84 or greater support asynchronous mirror groups, which are treated as a consistency group. Therefore, all volumes within the AMG will be treated as a single entity and failed over at the same time.
- Synchronization priority will have a dramatic effect on the speed of replication, IF sufficient bandwidth is available between the peer storage arrays recommend setting to high or highest.

SRA COMMAND LINE OPTIONS

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

- Trace Logging: This option provides for detailed logging for each command issued 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.

SRA JAVA UPDATE SCRIPT

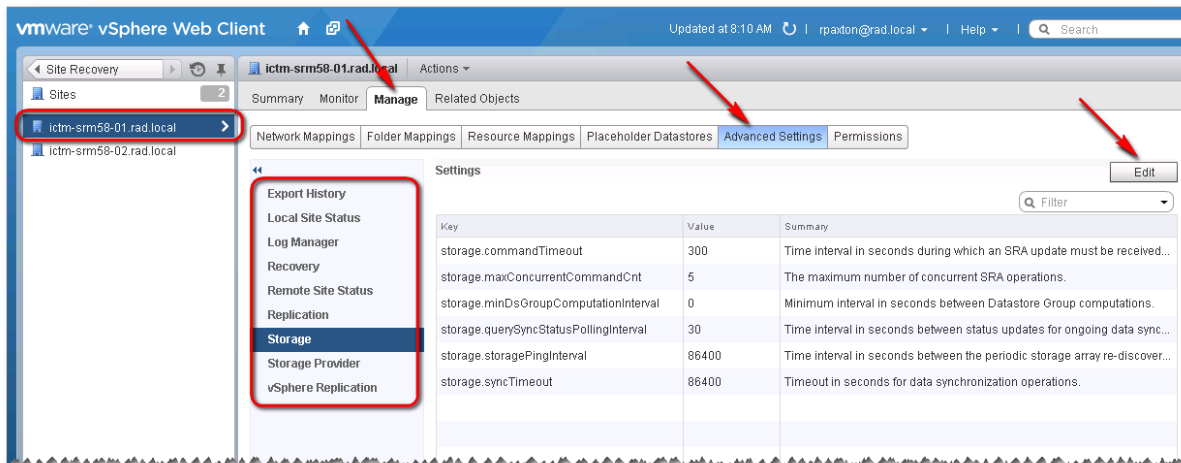
Also installed with the SRA is a command line utility to update the Java runtime environment in the event an updated JRE is required. This script is called `UpdateJREPath.bat` and is typically located in the `C:\Program Files (x86)\NetApp\SANtricity Storage Replication Adapter` directory.

- Executing the batch file without any options will display the current JRE path that is used by the SRA.
- Executing the batch file with the absolute path to a new JRE path will update the configuration files to point to the new location and restart the SRA service.

SRM ADVANCED SETTINGS

Due to the nature of the NetApp SANtricity SRA, the following SRM settings are recommended for the best operation of the SRA. SRM settings are accessed by selecting Sites, with Site Recovery Manager, selecting a site, and then the Manage tab, and then the Advanced Settings button (see Figure 6). From here, you can then select the settings group to edit.

Figure 6 - SRM Advanced Settings.



The following changes are highly recommended 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 the following changes are recommended for ESX/ESXi host settings:

- Disk.MaxLUN = Slightly larger than the number of LUNs mapped to the ESX host. (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.)

TROUBLESHOOTING TIPS

In certain environments, it may be necessary to implement one or all of the following settings to enable successful operation of the SRA. **THESE SHOULD NOT BE USED UNLESS ADVISED BY TECHNICAL SUPPORT.** These are non-standard settings and should only be used if your environment is experiencing the symptoms described for the change.

DATASTORE EXPECTED TO BE AUTO-MOUNTED

Error: Failed to recover Datastore 'XYZZY'. Datastore residing on recovered devices and expected to be auto-mounted 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>300</waitForRecoveredDatastoreTimeoutSec>
  <waitForAccessibleDatastoreTimeoutSec>900</waitForAccessibleDatastoreTimeoutSec>
</storageProvider>
```

VMware vCenter Site Recovery Manager Server service must be restarted after applying this change. This will increase the timeout for snapshot mount operations.

For iSCSI connectivity, refer to the appropriate client workflow below to add an iSCSI alias for the host.

- For the vSphere Web Client, perform the following on both the Protected and Recovery Hosts:
 - Click **configure** -> **Storage Adapter**
 - Select the iSCSI Software Adapter
 - Click the **Properties** tab
 - Click **Edit**
 - Add the iSCSI alias for the Host
 - Click **OK**
- For the traditional vSphere Client, perform the following on both the Protected and Recovery Hosts:
 - From the Storage Adapter, select iSCSI Software Adapter
 - Right-click iSCSI Software Adapter and select Properties
 - On the General Tab, click **Configure**
 - Add the iSCSI alias for the Host
 - Click **OK**

UNABLE TO COMMUNICATE WITH REMOTE HOST

Error: *Failed to recover datastore 'CG26'. VMFS volume 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 will increase the maximum amount of memory 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 will require a reboot of the ESXi host system after modification.

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 will increase the SSL handshake timeout value. This change may be necessary on busy systems. The ESXi host must be rebooted 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 will require a firmware upgrade to 07.84.44.xx or later.

Workarounds:

Adding additional volumes to the AMG group may alleviate this issue.

Ensuring both source and target volumes reside on same controller (a or b) may alleviate this issue.

Using legacy RVM will avoid this situation. Not a valid solution for iSCSI configurations.

STEPS TO RECOVER FROM A SITE/ARRAY DOWN

Event: Recovering after site/array down scenario.

Solution: Perform the following steps to recover from a site/array down:

1. Run the Recovery Plan with the array down
2. Once complete, the protected site storage array is brought back online.
3. Remove mirror relationships on the Protected array that are not failed because they lost communication with the failover volumes.

NOTE: The failover volumes had the mirroring relationship broken by the SRA running on the Failover site.

4. Remake the mirror relationships.
Ensure the volumes at the Failover are primary. It is preferable to remake the mirrors from the failover site.
5. Wait for the synchronization to complete.
 - a. Optionally, Rescan/rediscover the devices.
NOTE: SRM rescans for devices as part of its normal operation. If initiated by the SRM administrator, this should be down at Failover site. Restarting the SRA service on the Protected and Failover sites is an option if there is not enough time to wait. This is necessary to make SRM aware of the relationship of storage objects after the failure.
6. Run Reprotect from the Failover vCenter host (DR).

ADDITIONAL INFORMATION

Additional information for the NetApp SANtricity Storage Replication Adapter may be obtained from the NetApp Community site at: <https://communities.netapp.com/groups/appaware-e-series-storage-replication-adapter>. You must be a member of the NetApp Community (free) and request access to the group from one of the administrators to join.

PHONE SUPPORT

24x7 support is provided for customers on a maintenance plan at 1-888-4NetApp (463-8277).

COMMUNITY SUPPORT

VMware communities are also monitored for support issues.

Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means— graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987)

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

