



NetApp® FAS/V-Series Storage Replication Adapter 2.1 for Clustered Data ONTAP®

For VMware® vCenter Site Recovery Manager

Installation and Administration Guide



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
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08477_A0
December 2013

Contents

What Storage Replication Adapter is	5
What Site Recovery Manager does	5
What Site Recovery Manager supports using Storage Replication Adapter	5
Support for IPv6 in Storage Replication Adapter	6
Components of a disaster recovery environment	6
Role of Storage Replication Adapter in a disaster recovery environment	7
Discovery of arrays and replicated devices	7
How a test recovery operation works	8
When to run a recovery operation	9
What a reprotect operation does	10
Failback (using reprotect and recovery workflows)	10
Installing Storage Replication Adapter	12
System requirements for using Storage Replication Adapter	12
Downloading Storage Replication Adapter	13
Installing 32-bit or 64-bit Storage Replication Adapter	14
Setting up Storage Replication Adapter	15
Setting up the storage system in a NAS environment	15
Setting up the storage system in a SAN environment	16
Options you can configure in the Storage Replication Adapter configuration file ...	17
Configuring Storage Replication Adapter	18
Error messages in Storage Replication Adapter	21
Address of the storage array is not reachable	21
ALUA mismatch observed	21
An error occurred during host configuration	21
An error occurred during host configuration and failed to recover datastore	22
Array ID and peer array ID are the same	22
Authentication failed	22
Creation of a temporary writable copy of the device failed	22
Device found is neither of the SAN type nor of the NAS type	23
Device is already tested for recovery	23
Device is not in the snapmirrored state	23
Device is not replicated	23

Device synchronization did not complete properly	24
Failed to promote replica devices	24
Failed to recover datastore	24
FlexClone is not licensed	24
Incorrect array ID	25
Incorrect synchronization ID received as input from SRM	25
Location for reverse replication is not source	25
No SnapMirror relationship found	25
Peer array ID provided in the SRM input is incorrect	25
Recovery of device already completed	26
SAN or NAS device not found	26
SnapMirror policy could not be imported	26
SnapMirror replication is in progress	26
SnapMirror resynchronization failed	27
SnapMirror resynchronization failed because of various reasons	27
SnapMirror version could not be traced	27
Storage IP is not defined or valid	27
Storage ports not found	28
Storage system configuration error	28
System information: host name, model, and vendor not found	28
The SRA command issued was not found	28
The temporary device is in improper state	29
The temporary writable copy created is not consistent	29
The temporary writable copy might not have enough space	29
The XML input to SRA from SRM is incorrect	29
Unable to add the initiators passed in the SRM input to an initiator group	29
Unable to create initiator group on the storage array based on the access group information	30
Unable to destroy the temporary writable copy	30
Unable to fail over the specified device	30
Unable to make the device online	30
Glossary	31
Copyright information	34
Trademark information	35
How to send your comments	36
Index	37

What Storage Replication Adapter is

Storage Replication Adapter for clustered Data ONTAP is a storage vendor specific plug-in to VMware vCenter Site Recovery Manager that enables interaction between Site Recovery Manager and the Storage Virtual Machine (SVM, formerly known as Vserver).

Storage Replication Adapter enables communication between Site Recovery Manager and the controller at the SVM level. The adapter interacts with the SVM to discover replicated datastores.

For more information about the new and enhanced features of Site Recovery Manager, see the Site Recovery Manager documentation.

What Site Recovery Manager does

Site Recovery Manager uses Storage Replication Adapter to discover arrays and replicated and exported datastores, and to fail over or test failover of datastores.

Site Recovery Manager uses virtualization to provide end-to-end disaster recovery management and automation across the entire data center. Site Recovery Manager uses VMware infrastructure to build, automate, and test disaster recovery plans for the data center. Site Recovery Manager integrates with vSphere and provides a seamless view of your environment that includes both virtual infrastructure and disaster recovery management.

Related concepts

[*Components of a disaster recovery environment*](#) on page 6

What Site Recovery Manager supports using Storage Replication Adapter

Using Storage Replication Adapter, Site Recovery Manager supports SAN storage environments, VMFS (iSCSI and FC) and RDM (iSCSI and FC); and NAS storage environments using NFS.

For more information about Site Recovery Manager, see the Site Recovery Manager documentation on the VMware site.

Support for IPv6 in Storage Replication Adapter

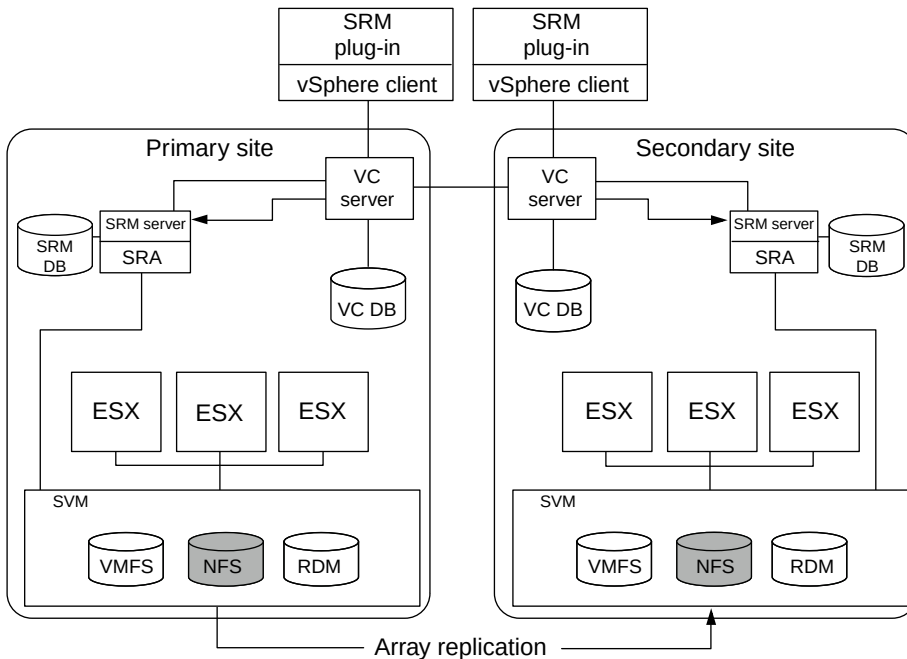
Starting with Storage Replication Adapter 2.1 for clustered Data ONTAP, IPv6 is supported for management access and data transport over NFS and iSCSI. IPv6 addressing provides expanded routing and addressing capabilities for Data ONTAP 8.2.x releases.

You can enable IPv4 and IPv6 on both the primary and secondary disaster recovery sites. You can enable IPv4 or IPv6 on the data LIF and cluster-management LIF of storage controllers, provided IPv4 and IPv6 are both enabled on the associated ESX host.

Components of a disaster recovery environment

A disaster recovery environment consists of the storage array, ESX or ESXi servers, Storage Virtual Machines (SVMs), Site Recovery Manager, vSphere Client, and Storage Replication Adapter.

The following illustration shows the components of a disaster recovery environment:



Role of Storage Replication Adapter in a disaster recovery environment

Storage Replication Adapter provides array-specific support for Site Recovery Manager by following the input specifications from Site Recovery Manager.

The adapter enables Site Recovery Manager to execute the following workflows:

- Discovery of arrays and replicated devices
- Test recovery
- Recovery
- Reprotect

Discovery of arrays and replicated devices

Storage Replication Adapter discovers pairs of Storage Virtual Machines (SVMs, formerly known as Vservers) that replicate data between the protected and recovery sites. It also discovers the storage devices that are replicated. You can select these devices (*datastores*) as part of the Site Recovery Manager protection group.

Multiple VMware datastores sharing the same SnapMirror replication relationship are collected by Site Recovery Manager into the same storage group. Therefore, VMware datastores that are replicated in the same SnapMirror relationship are configured in the same protection group or recovery plan to fail over together.

The discovery operation identifies the source and destination array ID, name and version of the replication software, and model and vendor of the storage array. The operation also discovers all the replicated devices in a pair of SVMs along with their destination export path or LUN path and device ID. If you want Storage Replication Adapter to discover specific volumes, you can specify the volumes in the **Volume include list/Volume exclude list** of Array Manager in Site Recovery Manager.

- For the SVM in a NAS environment, the array ID is the host name of the storage system and the device ID is `//vserver_name/volume_name`.
The volume junction path is provided for identity.
- For the SVM in a SAN environment, the array ID is the host name of the storage system and the device ID is `//vserver_name/volume_name /LUN_name`.
FC WWN or the iSCSI IQN is provided for identity.

To discover an exported volume in a NAS environment, you must ensure the following:

- Volumes are mounted on junction paths
- Volumes are associated to a valid export policy
- A rule for the valid export policy that is attached to the volume is created
- NFS server is running for the destination SVM

- Group ID and user ID are set to zero

To discover a LUN in a SAN environment, you should map the LUN to an igroup of OS type *vmware* and replicate the LUN by using SnapMirror technology. This operation discovers the devices that are mapped and then verifies whether these devices are replicated.

How a test recovery operation works

You should understand how a test recovery operation works so that you can run a test recovery operation to ensure that it works during a disaster or a planned migration. A test recovery operation does not affect an ongoing SnapMirror replication.

During a test recovery operation, Storage Replication Adapter creates a FlexClone volume from the latest Snapshot copy of the SnapMirror destination volume and displays the cloned export path or LUN path to Site Recovery Manager.

The test recovery operation creates a cloned volume on the secondary storage system with the prefix *testfailoverClone_nss_v10745371_Vservername*, followed by the parent volume name. For example, the cloned volume that is created for the *secondary_volume* is named *testfailoverClone_nss_v10745371_Vservername_secondary_volume*.

At the end of a test recovery operation, the FlexClone volume is destroyed. You must ensure that you do not have user-created volumes with names prefixed with *testfailoverClone_nss_v10745371_*. You can verify the names of the volumes in the secondary storage system by running the `vol show` command.

By default, Storage Replication Adapter creates a cloned volume with no space guarantee because the cloned volume is not used during the actual recovery and is destroyed.

In a NAS environment, the destination namespace is created automatically by Storage Replication Adapter by joining the NFS datastore to a junction path that matches the volume name in the root of the namespace. This is the default and recommended configuration for joining NFS datastores to a junction path in a namespace. If at the source you have nested the NFS datastore junction paths under other folders, or junction path names differ from volume names and if you want the configuration to be the same at the destination, then you must join the volumes to the required junction paths manually prior to failover because SnapMirror does not replicate namespace information.

In a SAN environment, the test recovery operation maps the LUNs of the FlexClone volume to an igroup of OS type *vmware*. The operation verifies whether an igroup is present for the specific initiator type and ID.

Automatically created igroups have names prefixed with *srmtest_v10745371*, followed by the access group name and initiator type received from the Site Recovery Manager input. For example, an igroup created for an FC initiator of access group *host-group-A* has the name *srmtest_v10745371_host-group-A_FC_random_string*.

When to run a recovery operation

You can perform a recovery operation for planned migration of services or for unplanned disaster recovery.

Disaster recovery

During disaster recovery, Storage Replication Adapter cancels any ongoing transfers to the SnapMirror destination, quiesces the destination, and breaks the SnapMirror relationship. When the SnapMirror relationship is broken, the destination volume is ready for read/write operations.

In a NAS environment, the destination namespace is created automatically by Storage Replication Adapter by joining the NFS datastore to a junction path that matches the volume name in the root of the namespace. This is the default and recommended configuration for joining NFS datastores to a junction path in a namespace. At the source, if you have nested the NFS datastore junction paths under other folders, or junction path names differ from volume names and if you want the configuration to be the same at the destination, then you must join the volumes to the required junction paths manually prior to failover because SnapMirror does not replicate namespace information.

Planned migration

During a planned migration, the recovery operation shuts down the virtual machines at the protected site. Storage Replication Adapter performs a SnapMirror update and synchronizes the storage systems, quiesces the destination, and breaks the SnapMirror relationship. When the SnapMirror relationship is broken, the destination volume is ready for read/write operations.

In a NAS environment, a rule for the valid export policy that is attached to the volume is either created or an existing rule is modified. In a SAN environment, the operation maps the input LUN paths to the igroups of OS type *vmware*. The operation then brings the datastores online and displays the failed-over datastores to Site Recovery Manager.

Automatically created igroups have names in the format `access-group_initiator-type_random-string`. For example, an igroup created for an FC initiator of access group `host-group-A` has the name `host-group-A_FC_random_string`.

Replication settings are run during a planned migration. Replication settings is designed to allow Site Recovery Manager to collect replication settings, such as the schedule and throttle, for replicated devices before failover and pass these settings to Storage Replicator Adapter after failover to ensure that replication settings are preserved when the replication direction is reversed or restored. Site Recovery Manager passes this information as is to the `reverseReplication` and `restoreReplication` commands. Site Recovery Manager issues a `ReplicationSettings` command periodically and stores the results in its database.

Note: You must manually reverse the replication if problems are encountered in the database and if Site Recovery Manager fails to provide replication details for the reprotect operation.

What a reprotect operation does

After a recovery operation, you can run the reprotect operation to replicate the changes made at the recovery site to the original protected site.

During a reprotect operation, Storage Replication Adapter reverses the direction of the existing SnapMirror relationships and starts replicating the changes made at the recovery site to the original protected site.

Before running the reprotect operation, you must have reviewed the SnapMirror Requirements for Storage Replication Adapter section.

SnapMirror requirements for Storage Replication Adapter

You must ensure that you meet all the SnapMirror requirements before running a reprotect operation.

By default, a reprotect operation imports the replication settings at the original recovery site to the recovery site. You can create a named schedule by using the `job schedule cron create` command. Site Recovery Manager provides the schedule values as input during a reverse replication.

After the client data access is failed over to the destination volume, you can continue to operate in this configuration and set this volume as the new primary volume. However, when the original source cluster is available and if you want to resynchronize the original source volume with the changes in the current primary volume, you can perform a reverse resynchronization operation. This operation makes the original source volume a destination of the current primary volume, ensuring data protection for the primary data.

As part of reverse resynchronization, Storage Replication Adapter removes the SnapMirror relationship from the destination site and a reverse resynchronization operation is performed from the source site.

Note: The default value for `snap autodelete` is set to `try` to prevent Data ONTAP from deleting the SnapMirror Snapshot copies. You must retain the default setting of `snap autodelete` because if the setting is modified and the SnapMirror Snapshot copies are deleted, then Storage Replication Adapter cannot reverse and resynchronize the replication from the affected volume.

Failback (using reprotect and recovery workflows)

Failback procedure enables you to restore the original protected and recovery sites after a recovery operation.

To perform failback after recovery, you must execute the following workflows:

1. Reprotect

Reverses the replication direction of the existing SnapMirror relationships from the recovery site to the protected site.

If the devices and the SnapMirror relationships do not exist after a disaster, you should create new devices at the protected site and initialize the SnapMirror relationship from the recovery site to the original protected site.

2. **Planned migration**
Migrates virtual machines from the recovery site back to the protected site.
3. **Reprotect**
Reverses the replication direction from the protected site to the recovery site, thus restoring the original direction of replication between the protected and recovery sites.

Installing Storage Replication Adapter

You should ensure that you meet the system requirements to install Storage Replication Adapter.

System requirements for using Storage Replication Adapter

Before you run Storage Replication Adapter, you must meet certain requirements related to Data ONTAP and Site Recovery Manager.

- For the 32-bit Storage Replication Adapter, the Site Recovery Manager version you are using must be 5.0.
- For the 64-bit Storage Replication Adapter, the Site Recovery Manager version you are using must be 5.1 or 5.5.
- One of the following Site Recovery Manager versions must be installed on Windows: 5.0, 5.1, or 5.5.
- Your storage system must be running Data ONTAP for configuring Storage Virtual Machines (SVMs) as storage arrays.
- FlexClone license must be enabled for test failover operation.
The license is optional because a test failover operation can be performed when the option `replication_disruptive_test_failover` is set to on in the `ontap_config` file.
- SnapMirror license must be enabled on the storage system.
- In a NAS environment, NFS services must be running.
- In a SAN environment, iSCSI services must be running.
- Storage Replication Adapter must be installed on the Site Recovery Manager server at the protected and recovery sites.
- Perl 5.8.8 or Perl 5.14.2 must be installed on the system on which Site Recovery Manager is installed.

Note: If the Site Recovery Manager installation does not include the required Perl version, you can install Perl separately with the default configuration. For more information about downloading Perl, see the Perl download page.

- To use secureHTTP, SSH must be enabled using security login.
By default, SSL is enabled.
By default, Storage Replication Adapter calls the Data ONTAP API over HTTP.
- The 80 or 443 port corresponding to the HTTP or SSL protocol must be open on the firewall. The port is between the Site Recovery Manager server and the storage system running Data ONTAP.
- For Data ONTAP 8.2.x, the cluster should be enabled with IPv6 before enabling IPv6 for data LIFs and the cluster-management LIF.

For a detailed list of the supported software version and storage systems, see the Interoperability Matrix.

For information about the NetApp platforms that are supported in the VMware environment, see the NetApp-VMware platform compatibility matrix on the VMware site.

Related information

VMware Compatibility Guide: www.vmware.com/resources/compatibility/search.php?deviceCategory=srax

Perl script download page: www.perl.com/download.csp

NetApp Support Site: support.netapp.com

Interoperability Matrix: support.netapp.com/matrix

Downloading Storage Replication Adapter

Before you install Storage Replication Adapter, you have to download the installation file from the NetApp Support Site.

Steps

1. Log in to the NetApp Support Site and click the **Downloads** tab.
2. In the **Downloads** page, select **Software**.
3. From the list of products, select **Storage Replication Adapter for clustered Data ONTAP**.
4. Follow the instructions on the page until you reach the download page.
5. Download the file in one of the following ways:
 - Download it directly to your target system.
 - Download it to a PC host and copy it to the target system.

After you finish

You can unzip the file and install Storage Replication Adapter.

Related tasks

[Installing 32-bit or 64-bit Storage Replication Adapter](#) on page 14

Related information

NetApp Support Site: support.netapp.com

Installing 32-bit or 64-bit Storage Replication Adapter

You can install Storage Replication Adapter from the location where you downloaded the scripts.

Before you begin

You must have downloaded Storage Replication Adapter from the NetApp Support Site.

Steps

1. Use Windows Explorer to navigate to the directory to which you unzipped the downloaded file, and then double-click the `setup.msi` file.

The installer finds the installed location of Site Recovery Manager from the registry and copies these scripts to that location.

2. Select the **Complete install** option.

The 32-bit Storage Replication Adapter is available at the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetApp, Inc\NetApp FAS/V-Series Storage Replication Adapter 2.1 for clustered Data ONTAP.

The 64-bit Storage Replication Adapter is available at the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\NetApp, Inc\NetApp FAS/V-Series Storage Replication Adapter 2.1 for clustered Data ONTAP.

3. Click **Finish**.

Related tasks

[Downloading Storage Replication Adapter](#) on page 13

Related information

[NetApp Support Site: support.netapp.com](http://support.netapp.com)

Setting up Storage Replication Adapter

You must set up the storage system before running Storage Replication Adapter for Site Recovery Manager. You can customize Storage Replication Adapter by changing the configuration files.

Setting up the storage system in a NAS environment

You must set up the system before running Storage Replication Adapter for Site Recovery Manager.

Steps

1. Install Site Recovery Manager.

For information about installing Site Recovery Manager, see the Site Recovery Manager documentation on the VMware site.

2. Install Storage Replication Adapter on the Site Recovery Manager server at the protected and recovery sites.
3. Ensure that the datastores at the protected site contain virtual machines that are registered with vCenter Server.
4. Ensure that the ESX or ESXi hosts at the protected site have mounted the NFS exported volumes from the Storage Virtual Machine (SVM).
5. Ensure that valid addresses, such as the IP address, host name, FQDN, are entered in the **NFS Addresses** field when adding arrays to Site Recovery Manager by using the **Array Manager** wizard.
6. Verify that the ESX or ESXi hosts at the secondary storage system have a VMkernel port that can access the IP addresses that are used to serve NFS exports from the SVM.

You can do this by using the `vmkping nfs_ip_address` command on the ESXi shell or ESX service console of each ESXi or ESX host.

nfs_ip_address is one of the NFS IP addresses on the SVM.

You can verify whether access to the ESXi shell is disabled by using the `ping vmkernel_ip_address` command on the console of the SVM.

vmkernel_ip_address is one of the IP addresses on the VMkernel port that the ESX or ESXi host uses to access the SVM.

7. Ensure that the volume that contains the exports is replicated to the secondary storage system.
8. Choose the appropriate command to confirm that the export is part of only one replication relationship:

If the Data ONTAP version is...	Enter the following command...
Data ONTAP 8.1.x	snapmirror show
Data ONTAP 8.2.x	snapmirror list-destinations

- On the secondary storage system, enter the **snapmirror show** command to confirm that the volume is replicated.

For more information about SnapMirror modes, see the *Clustered Data ONTAP Data Protection Guide*.

Related concepts

Options you can configure in the Storage Replication Adapter configuration file on page 17

Related tasks

Installing 32-bit or 64-bit Storage Replication Adapter on page 14

Related information

NetApp Support Site: support.netapp.com

Setting up the storage system in a SAN environment

You must set up the system before running Storage Replication Adapter for Site Recovery Manager.

Steps

- Install Site Recovery Manager.
For information about installing Site Recovery Manager, see the Site Recovery Manager documentation on the VMware site.
- Install Storage Replication Adapter on the Site Recovery Manager server at the protected and recovery sites.
- Ensure that the primary ESX or ESXi hosts are connected to LUNs in the primary storage system.
- Ensure that the LUNs, iSCSI, FC, or both, are in igroups of OS type *vmware* on the primary storage system.
- Ensure that the ESX or ESXi hosts at the recovery site have appropriate FC or iSCSI connectivity to the Storage Virtual Machine (SVM).

You can do this either by verifying that the ESX or ESXi hosts have local LUNs connected on the SVM, or by using the `fcv show initiators` or `iscsi show initiators` commands on the SVMs.

- Ensure that the volume that contains the LUNs is replicated to the secondary storage system.

7. Choose the appropriate command to confirm that the export is part of only one replication relationship:

If the Data ONTAP version is...	Enter the following command...
Data ONTAP 8.1.x	snapmirror show
Data ONTAP 8.2.x	snapmirror list-destinations

8. On the secondary storage system, enter the **snapmirror show** command to confirm that the volume is replicated.

For more information about SnapMirror modes, see the *Clustered Data ONTAP Data Protection Guide*.

Related concepts

[Options you can configure in the Storage Replication Adapter configuration file](#) on page 17

Related tasks

[Installing 32-bit or 64-bit Storage Replication Adapter](#) on page 14

Related information

[NetApp Support Site: support.netapp.com](#)

Options you can configure in the Storage Replication Adapter configuration file

The Storage Replication Adapter configuration file enables you to customize some of the disaster recovery behaviors, including the security settings during Site Recovery Manager recovery or test recovery. By default, the configuration file is located at `install_dir\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\ONTAP\ontap_config.txt`.

The following are some of the options that you can configure in the adapter configuration file:

- `import_replication_settings` (value can be off (default) or on)
This option imports the SnapMirror settings at the original recovery site to the required recovery site during the reprotect operation. However, compression and wsize (window size) settings are not imported and you must update these settings manually in the `/etc/snapmirror.conf` file.
- `volume_guarantee` (value can be none, file, or volume (default))
This optionally specifies the space-reservation policy for the volume.
- `replication_disruptive_test_failover` (value can be on or off (default))
The FlexClone license is optional if the value is set to on because FlexClone volumes are not created. The replication is disrupted during disaster recovery test failover operations for all executed recovery plans when `replication_disruptive_test_failover` is set to on.

- `enable_asup_message` (value can be on or off (default))
The option generates AutoSupport (ASUP) messages along with events.
- `ssl` (value can be on or off (default))
This option is used to choose either secure or normal HTTP.
- `isipv4` (value can be yes or no (default))
This option is used to support the mounting of datastores by host name and FQDN instead of IPv6. You can modify the `isipv4` option in the `ontap_config.txt` file, depending on whether the IP address is IPv6 or IPv4.
You must add the IPv4 address in the NFS Address field if `isipv4` is set to yes. If the host name or FQDN is added, then Storage Replication Adapter resolves the host name with the IPv4 address.
You must add the IPv6 address in the NFS Address field if `isipv4` is set to no. If the host name or FQDN is added, then Storage Replication Adapter resolves the host name with the IPv4 address.
- `import_snapmirror_policy` (value can be on or off (default))
For Data ONTAP 8.2.x, this option imports the SnapMirror policy settings from the original recovery site to the required recovery site.

Option specific to a SAN environment

- `lun_space_reservation` (value can be yes or no (default))
This provisioning management option verifies whether the LUNs recovered for disaster recovery testing are set with space reservations enabled or disabled.

Options specific to a NAS environment

- `anon` (*anon uid*)
This option is used to force volumes to be exported with an anonymous security identifier. You should enter the required anon user ID—for example, `anon=0`. By default, the adapter does not export volumes that are using the anon option.
- `read_only` (value can be any or sys (default))
- `read_write` (value can be any or sys (default))
- `superuser` (value can be any or sys (default))

Configuring Storage Replication Adapter

You can configure Storage Replication Adapter by using the Array Manager wizard of Site Recovery Manager.

Steps

1. In Site Recovery Manager, click **Array Managers**, and then click **Add Array Manager**.
2. Enter the following information to describe the array in Site Recovery Manager:

- a) Enter a name to identify the array manager in **Display Name**.
- b) In the **SRA Type** field, select **NetApp Storage Replication Adapter for clustered Data ONTAP**.
- c) Enter the IP address in **Cluster Management LIF**.

Example

10.10.20.54

If the data protocol of a LIF is set to none, the firewall policy of the LIF is automatically set to management.

- d) Enter the name of the SVM in **SVM name**.
- e) In **NFS Addresses**, enter the IP address, host name, or FQDN of the LIFs that are used to serve NFS from the SVM to the ESX or ESXi hosts at the site where the SVM is located.

If you are using host names or FQDNs for NFS addresses, then the host names or FQDNs that are entered must be resolvable by the server where Storage Replication Adapter is installed.

Example

192.168.2.100, f3170-192-75, f3270-192.75.priv.netapp.com

If you do not enter any addresses in the **Automatic NFS LIF discovery** field, Storage Replication Adapter automatically discovers all the LIFs that have only the NFS protocol enabled on the SVM. The addresses of these LIFs are used for NFS mount during failover or test failover.

Note: The NFS LIF discovery feature is intended for use in environments where a private NFS storage network has been configured for the ESX or ESXi hosts. The ESX or ESXi hosts should have access and should intend to use the NFS LIFs configured on the SVM.

If you choose the NFS LIF discovery feature, all the LIFs that have the NFS protocol enabled are automatically discovered by Storage Replication Adapter and will be used by the ESX or ESXi hosts to mount datastores. If there are NFS LIFs on the SVM that cannot be accessed by ESX or ESXi hosts, or if there are any other protocols such as CIFS enabled on the LIFs, then the automatic NFS LIF discovery feature should not be used and you must configure all NFS addresses intended for use in the NFS addresses field.

The NFS addresses that are entered in this field are available only for NAS environments.

You must enter the addresses of the LIFs that are used by the SVM to serve NFS to the ESX or ESXi hosts. You can enter multiple addresses, separated by commas. These NFS addresses allow the use of private storage networks that are separate from the network that is used to administer the controller. If you do not enter any addresses in this field, Site Recovery Manager attempts to mount the NFS exports by using the IP addresses of any LIFs with NFS enabled on the SVM.

- f) In **Enable NFS hostname** mounting, type **Yes** or **No**.

If you type **Yes**, Storage Replication Adapter performs an address lookup operation for the host names entered and then verifies that a LIF with that address exists on the SVM. Storage

Replication Adapter returns these host names to Site Recovery Manager to allow the ESX or ESXi host to mount the NFS exports by host name instead of the IP address. If you type **No**, then NFS exports are mounted by IP address rather than by host name during test failover and failover operations.

- g) Enter the volumes to be discovered in **Volume include list**.

You must enter the source volume at the protected site and the replicated destination volume at the recovery site. You can enter either the full volume name or a string in the volume name.

Example

If you want to discover the volume *src_vol1* that is in a SnapMirror relationship with volume *dst_vol1*, you must specify *src_vol1* in the protected site and *dst_vol1* in the recovery site.

- h) Enter the volumes to be excluded from discovery in **Volume exclude list**.

You must enter the source volume at the protected site and the replicated destination volume at the recovery site. You can enter either the full volume name or a string in the volume name.

Example

If you want to exclude the volume *src_vol1* that is in a SnapMirror relationship with volume *dst_vol1*, you must specify *src_vol1* in the protected site and *dst_vol1* in the recovery site.

- i) Enter the user name of an account with privileges to the SVM in **Username**.
j) Enter the password of the user account in **Password**.

3. Click **Next**.
4. Verify that the array is discovered and displayed at the bottom of the **Add Array Manager** window.
5. Click **Finish**.

Error messages in Storage Replication Adapter

You might encounter an error message when using Storage Replication Adapter with Site Recovery Manager. The user interface of Site Recovery Manager displays the error log messages and possible solutions.

You can also use the log files of Site Recovery Manager and the log files of the controller to troubleshoot issues that you might encounter when using Storage Replication Adapter.

Address of the storage array is not reachable

Message	Address of the storage array is not reachable
Cause	Storage array might be down or IP address entered might be incorrect.
Corrective action	Ensure that the storage array is up and running and the IP address of the storage array is reachable through the command line interface.

ALUA mismatch observed

Message	ALUA mismatch observed. Ensure that the initiators are mapped to igroups with either ALUA enabled or ALUA disabled.
Cause	When both iSCSI and FCP are enabled at the same time on the ESX host at a recovery site, SRM attempts to map the LUN to both igroups (iSCSI and FCP) that have different asymmetric logical unit addressing (ALUA) settings.
Corrective action	Ensure that ALUA is either enabled or disabled on both the igroups because Storage Replication Adapter does not support a mixed ALUA configuration.

An error occurred during host configuration

Message	An error occurred during host configuration
Cause	The device might not be exported or mapped correctly.
Corrective action	For a NAS device, ensure that it is exported with proper rules and vmkernel IP addresses. Also ensure that the NFS service is started. For a SAN device, ensure that it is mapped to an igroup of OS type vmware.

An error occurred during host configuration and failed to recover datastore

Message	Failed to recover datastore. An error occurred during host configuration. Recovery of device already completed. You must configure the SnapMirror relationship again to recover the device.
Cause	The SnapMirror relationship for the device might not exist.
Corrective action	Ensure that the SnapMirror relationship exists for the device and that the relationship status is either snapmirrored or quiesced.

Array ID and peer array ID are the same

Message	Array ID and peer array ID are the same
Cause	Storage Replication Adapter does not support this type of configuration.
Corrective action	Ensure that the protected site array and the recovery site array are different.

Authentication failed

Message	Authentication failed
Cause	Invalid user name or password.
Corrective action	Ensure that you provide a valid user name and password.

Creation of a temporary writable copy of the device failed

Message	Creation of a temporary writable copy of the device failed
Cause	The FlexClone license might not be enabled for the storage array.
Corrective action	Ensure that the FlexClone license is enabled for the storage array.

Device found is neither of the SAN type nor of the NAS type

Message	Device found is neither of the SAN type nor of the NAS type.
Cause	Device might not exist on the storage array.
Corrective action	Ensure that the device exists on the storage array and is of type NAS or SAN.

Device is already tested for recovery

Message	Device is already tested for recovery
Cause	The test recovery operation is either completed or is already running on the device.
Corrective action	If a test recovery operation is running, wait for the operation to complete and then clean up the test environment. If the test recovery is already completed, clean up the test environment.

Device is not in the snapmirrored state

Message	Device is not in the snapmirrored state
Cause	The SnapMirror relationship might be broken or uninitialized.
Corrective action	Ensure that the replication state of the device is snapmirrored for synchronization to work.

Device is not replicated

Message	Device is not replicated
Cause	This error message can occur if any one of the following conditions exists: • SnapMirror relationship is not configured on the device. • The device provided in the input is not online. • The device provided in the input does not exist.
Corrective action	Ensure that a SnapMirror relationship is configured on the device. Also ensure that the device exists on the storage system and is online.

Device synchronization did not complete properly

Message	Device synchronization did not complete properly
Cause	The device synchronization process might have been disrupted because of network failure.
Corrective action	Ensure that the storage array hosting the device is connected to the network and is accessible to its peer storage array.

Failed to promote replica devices

Message	Failed to promote replica devices. Base snapshot not found. Ensure that the SnapMirror relationship exists for the device. Verify whether base snapshot exists for SnapMirror relationship.
Cause	The volume might not be online or the base Snapshot copy might be deleted.
Corrective action	Ensure that the specified volume is online and that the base Snapshot copy exists for the SnapMirror relationship.

Failed to recover datastore

Message	Failed to recover datastore. Recovered device not found after HBA rescan.
Cause	FC and iSCSI adapters and vmkernel IP might not be configured on ESX servers.
Corrective action	Ensure that at least one initiator is configured on the ESX server.

FlexClone is not licensed

Message	FlexClone is not licensed
Cause	The FlexClone license might not be enabled on the storage system.
Corrective action	Ensure that the FlexClone license is enabled on the storage system.

Incorrect array ID

Message	Incorrect array ID
Cause	Incorrect array ID in the SRM input.
Corrective action	Verify the SRM logs.

Incorrect synchronization ID received as input from SRM

Message	Incorrect synchronization ID received as input from SRM
Cause	Synchronization ID might not be present on the storage system.
Corrective action	Check the SRM logs to verify the synchronization ID.

Location for reverse replication is not source

Message	Location for reverse replication is not source
Cause	Reverse replication might be performed at the recovery site.
Corrective action	Check the logs to ensure that reverse replication is running on the source. Reverse replication is performed at the protected site (original recovery site) to reverse the replication direction after a failover.

No SnapMirror relationship found

Message	No SnapMirror relationship found
Cause	The SAN or NAS devices might not be mirrored on separate storage arrays.
Corrective action	Ensure that at least one SAN or NAS device is mirrored and that the source and destination are on different storage arrays. Storage Replication Adapter does not support SnapMirror relationships on a single storage array.

Peer array ID provided in the SRM input is incorrect

Message	Peer array ID provided in the SRM input is incorrect
Cause	SnapMirror relationship might not exist for the peer array ID.

Corrective action Check the Site Recovery Manager logs to verify the peer array ID.

Recovery of device already completed

Message Recovery of device already completed

Cause SnapMirror relationship of the device might be in broken.

Corrective action Configure the SnapMirror relationship to recover the device.

SAN or NAS device not found

Message SAN or NAS device not found

Cause The SAN or NAS device might not be configured properly.

Corrective action Ensure that the SAN device is configured and mapped to an igroup of OS type *vmware* and the NAS device is configured and exported with *rw* rules.

SnapMirror policy could not be imported

Message 'reverseReplication' failed for device. SnapMirror policy could not be imported. Please turn the `import_snapmirror_policy` option off and run the workflow

Cause SnapMirror policy details, scheduling information, and replication details are stored in the Site Recovery Manager database using query replication settings (QRS). This information is used during a reprotect operation for SnapMirror resynchronization. If Site Recovery Manager deletes the QRS when the devices are not reported in the correct state in a scaled environment, reverse replication fails because there is no SnapMirror policy information to be replicated.

Corrective action Set the `import_snapmirror_policy` option to off and the `import_replication_settings` option to off in the `ontap_config` file.

SnapMirror replication is in progress

Message SnapMirror replication is in progress

Cause Synchronization as part of test recovery, recovery, or reprotect operations might already be running for the device.

Corrective action Wait for the replication to be completed. Check the status of the SnapMirror by using the `snapmirror status` command.

SnapMirror resynchronization failed

Message SnapMirror resynchronization failed

Cause The devices might not be configured correctly.

Corrective action Ensure that the devices are configured correctly. Check the log files for more details.

SnapMirror resynchronization failed because of various reasons

Message SnapMirror resynchronization failed. Ensure that the device is in online state and is mapped or exported properly /
SnapMirror resynchronization failed. Ensure that the devices are configured correctly. Check the log files for more details.

Cause The source volume is offline.

Corrective action Ensure that the volume is online.

SnapMirror version could not be traced

Message SnapMirror version could not be traced

Cause Unable to get the Data ONTAP version of the storage array.

Corrective action Ensure that the version command on the storage array displays the correct Data ONTAP version.

Storage IP is not defined or valid

Message Storage IP is not defined or valid

Cause The IP address provided for the storage system is either null or invalid.

Corrective action Provide a valid IP address for the storage system.

Storage ports not found

Message	'class DR::Xml::SmlValidateException' 'StoragePorts' not found
Cause	Either the NFS IP address on the controller is incorrect or there is a mismatch between the IP address format in the NFS address field and the value set for the <code>isipv4</code> option in the <code>ontap_config</code> file.
Corrective action	Ensure that the NFS IP address on the controller is correct and that the IP address format mentioned in the NFS address field matches the value set for the <code>isipv4</code> option in the <code>ontap_config</code> file.

Storage system configuration error

Message	Storage system configuration error
Cause	FCP, iSCSI, and storage IP might not be configured properly.
Corrective action	Ensure that the storage system has proper configuration of FCP, iSCSI, and storage IP.

System information: host name, model, and vendor not found

Message	System information: host name, model, and vendor not found
Cause	Storage Replication Adapter could not collect the storage array details.
Corrective action	Ensure that the <code>hostname</code> command displays the host name for the storage array. Also ensure that the model and vendor is defined for the storage array.

The SRA command issued was not found

Message	The SRA command issued was not found
Cause	Command issued by Site Recovery Manager is not supported by Storage Replication Adapter.
Corrective action	Check the command-line options and logs.

The temporary device is in improper state

Message	The temporary device is in improper state
Cause	The temporary device might be in restricted state.
Corrective action	Manually make the device offline.

The temporary writable copy created is not consistent

Message	The temporary writable copy created is not consistent
Cause	The temporary writable copy might not be online.
Corrective action	Ensure that the temporary writable copy is in the online state.

The temporary writable copy might not have enough space

Message	The temporary writable copy might not have enough space
Cause	Enough space might not available for the creation of temporary writable copy.
Corrective action	Ensure that you reserve enough space for creating the temporary writable copy.

The XML input to SRA from SRM is incorrect

Message	The XML input to SRA from SRM is incorrect
Cause	The XML input might not be in correct format.
Corrective action	Check the Site Recovery Manager logs for more details.

Unable to add the initiators passed in the SRM input to an initiator group

Message	Unable to add the initiators passed in the SRM input to an initiator group
Cause	The initiators passed in the Site Recovery Manager input might not adhere to the required naming convention.

Corrective action	Ensure that the initiators passed in the Site Recovery Manager input adhere to the required naming convention. For example, ensure that FC has a proper WWPN or WWNN, iSCSI has a proper IQN, and NFS has a proper IPv4 address.
--------------------------	--

Unable to create initiator group on the storage array based on the access group information

Message	Unable to create initiator group on the storage array based on the access group information
Cause	The access group information to the Storage Replication Adapter might not contain a proper alphanumeric name.
Corrective action	Check the Site Recovery Manager logs to ensure that a proper alphanumeric name is specified as part of the access group information to the Storage Replication Adapter.

Unable to destroy the temporary writable copy

Message	Unable to destroy the temporary writable copy
Cause	The temporary device might be in use.
Corrective action	Ensure that temporary writable copy is not used by other operations.

Unable to fail over the specified device

Message	Unable to fail over the specified device
Cause	Either the device is not in the online state or is not mapped properly.
Corrective action	Ensure that the device is in the online state and is mapped or exported properly.

Unable to make the device online

Message	Unable to make the device online
Cause	The device might be in an inconsistent state.
Corrective action	Use the Data ONTAP commands to bring the device online.

Glossary

You should be familiar with basic storage concepts, terms, and technologies when using Storage Replication Adapter with VMware vCenter Site Recovery Manager.

Aggregate	In a NetApp FAS system, an aggregate is a collection of many physical disks that are collected into RAID groups to provide performance and disk redundancy. In a NetApp V-Series system, an aggregate is a collection of LUNs that have been provisioned on a supported third-party storage platform to provide storage for the NetApp system.
Cluster	A group of connected storage systems that share a global namespace and that you can manage as a single Storage Virtual Machine (SVM, formerly known as Vserver) or multiple SVMs, providing performance, reliability, and scalability benefits.
Cluster-management LIF	A cluster-management LIF provides a single management interface for the entire cluster. The LIFs can be configured on data ports. The cluster-management LIF can migrate or fail over to any port or node in the cluster.
Export policy	Export policies enable you to restrict access to volumes to clients that match specific IP addresses and specific authentication types. Export policies consist of individual export rules.
Export rule	An export policy can contain a large number of rules (approximately 4,000). Each rule defines a client or a set of clients, protocol, and access level (RO, RW, SU).
FlexClone volume	FlexClone volumes are writable, point-in-time copies of a parent FlexVol volume. FlexClone volumes and their parent volumes share the same disk space for any common data. Therefore, creating a FlexClone volume is instantaneous and requires no additional disk space until changes are made to the FlexClone volume or its parent. When performing a test recovery in VMware vCenter Site Recovery Manager, FlexClone volumes are created in the testing environment, and these FlexClone volumes are removed when testing is complete.
FlexVol volume	A FlexVol volume is provisioned from the available storage in an aggregate. FlexVol volumes are flexible and can be increased or decreased in size dynamically without impacting or disrupting the environment. A single aggregate can contain many FlexVol volumes. A FlexVol volume is not tied to any specific set of disks in the aggregate and is striped across all the disks in the aggregate.
Initiator	An initiator is a port that is used to connect to a LUN. It can be on an FC or an iSCSI software or hardware adapter in a host.

Initiator group (igroup)	An igroup provides LUN-masking capability to the storage system. An igroup contains one or more LUNs with their defined LUN IDs and the host initiators that are allowed to access those LUNs.
Junction path	The volumes of each SVM are related through junctions and are mounted on junction paths. These junctions present the file system in each volume. The root volume of the SVM is at the top level of the namespace hierarchy; additional volumes are mounted to the root volume of the SVM to extend the namespace.
LUN	A LUN is a block-based storage object provisioned within a FlexVol volume. LUNs are presented to an ESX or ESXi host through the iSCSI or FC protocol. A LUN can be formatted with VMFS so that it can be used as a VMware datastore to contain virtual machines, or it can be configured as an RDM device and formatted with the appropriate guest OS file system.
Namespace	Every SVM has a namespace associated with it. All the volumes associated with each SVM are accessed under the server's namespace. A namespace provides a context for the interpretation of the junctions that link together a collection of volumes.
NFS export	An NFS export is a FlexVol volume that has been shared for use as a NAS datastore by the ESX or ESXi hosts.
SnapMirror	Replication software that performs automated file system replication of a volume onto a separate disk or storage system for data protection and disaster recovery. SnapMirror runs as part of the Data ONTAP operating system on the SVM. SnapMirror replication can be configured at the FlexVol volume level. Volume SnapMirror can run in synchronous or asynchronous mode.
SnapMirror operations	• SnapMirror initialize: The initial baseline transfer of data from a source volume to a destination. • SnapMirror update: A manual update of the SnapMirror destination. • SnapMirror quiesce or break: SnapMirror quiesce or break is performed on the SnapMirror destination to convert the destination to a writable volume. • SnapMirror resync: After a SnapMirror destination is made writable, the SnapMirror resynchronization operation reestablishes the SnapMirror relationship. The operation also resynchronizes the contents of the source and destination volumes or qtrees, without repeating the initial transfer. • SnapMirror delete: Deletes a SnapMirror relationship. • SnapMirror create: Creates a SnapMirror relationship or re-creates a previous SnapMirror relationship in reverse direction.
SnapMirror relationship	Pairing of a source FlexVol volume to a destination FlexVol volume.
Snapshot copy	A point-in-time, read-only image of the storage system volume.

Storage Virtual Machine (SVM) In clustered Data ONTAP, a virtual server that provides network access through unique network addresses, that might serve data out of a distinct namespace, and that is separately administrable from the rest of the cluster. There are three types of SVMs—admin, data, and node—but unless there is a specific need to identify the type of SVM, SVM usually refers to data SVM.

Copyright information

Copyright © 1994–2013 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).

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, 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.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. 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.

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

Index

A

array ID and peer array ID are the same
cause and corrective action for the error message [22](#)

C

configuration file
options [17](#)
configuring
Storage Replication Adapter [18](#)

D

disaster recovery
components of [6](#)
options you can configure for [17](#)

E

error messages
array ID and peer array ID are the same [22](#)
no SnapMirror relationship found [25](#)
peer array ID provided in the Site Recovery Manager
input is incorrect [25](#)
SnapMirror policy could not be imported [26](#)
storage ports not found [28](#)
system information not found [28](#)
The SRA command issued was not found [28](#)
the XML input to SRA from SRM is incorrect [29](#)
unable to add the initiators passed in the SRM input
to an initiator group [29](#)
unable to create initiator group on the storage array
[30](#)

F

failback [10](#)

I

installing
Storage Replication Adapter [14](#)
IPv6
support for [6](#)

L

license requirements
for using Storage Replication Adapter [12](#)

M

migration
how test recovery operation works during planned
migration [8](#)

N

NAS
setting up storage systems in [15](#)
no SnapMirror relationship found
cause and corrective action for the error message [25](#)

P

peer array ID provided in the Site Recovery Manager
input is incorrect
cause and corrective action for the error message [25](#)

R

replicated devices
discovery of [7](#)
reprotect operation
what it does [10](#)
requirements
for reprotect operations, SnapMirror [10](#)

S

SAN
setting up storage systems in [16](#)
setting up
storage systems (NAS) [15](#)
the storage system (SAN) [16](#)
Site Recovery Manager
supported storage environments [5](#)
what it does [5](#)
SnapMirror
requirements for reprotect operations [10](#)

- SnapMirror policy could not be imported
 - cause and corrective action for the error message [26](#)
- SnapMirror relationships
 - device not replicated [23](#)
- SRA command issued was not found
 - cause and corrective action for the error message [28](#)
- storage ports not found
 - cause and corrective action for the error message [28](#)
- Storage Replication Adapter
 - configuring [18](#)
 - defined [5](#)
 - discovery of SVMs and replicated devices [7](#)
 - downloading [13](#)
 - error messages [21](#)
 - how test recovery operation works [8](#)
 - installing [12, 14](#)
 - options you can configure [17](#)
 - recovery operation
 - when to run it [9](#)
 - setting up [15](#)
 - SnapMirror requirements [10](#)
 - troubleshooting [21](#)
 - what a reprotect operation does [10](#)
 - when to run a recovery operation [9](#)
- storage systems
 - setting up (NAS) [15](#)
 - setting up (SAN) [16](#)
- SVMs
 - discovery of [7](#)
- system information not found
 - cause and corrective action for the error message [28](#)
- system requirements
 - for using Storage Replication Adapter [12](#)

T

- test recovery

- disaster
 - how test recovery operation works [8](#)
 - how it works [8](#)
- troubleshooting
 - array ID and peer array ID are the same [22](#)
 - no SnapMirror relationship found [25](#)
 - peer array ID provided in the Site Recovery Manager input is incorrect [25](#)
 - SnapMirror policy could not be imported [26](#)
 - storage ports not found [28](#)
 - system information not found [28](#)
 - The SRA command issued was not found [28](#)
 - the XML input to SRA from SRM is incorrect [29](#)
 - unable to add the initiators passed in the SRM input to an initiator group [29](#)
 - unable to create initiator group on the storage array [30](#)

U

- unable to add the initiators passed in the SRM input to an initiator group
 - cause and corrective action for the error message [29](#)
- unable to create initiator group on the storage array
 - cause and corrective action for the error message [30](#)

V

- Vservers
 - See* SVMs

X

- XML input to SRA from SRM is incorrect
 - cause and corrective action for the error message [29](#)