Storage Replication Adapter 4.0 for ONTAP ®

Installation and Setup Guide

June 2017 | 215-11950_C0
doccomments@netapp.com

NetApp®

Contents

What Storage Replication Adapter is

Storage Replication Adapter (SRA) for ONTAP for VMware vCenter Site Recovery Manager is a storage vendor-specific plug-in for VMware vCenter Server. The adapter enables communication between Site Recovery Manager and a storage controller at the Storage Virtual Machine (SVM) level as well as at the cluster level configuration.

The adapter interacts with the SVM to discover replicated datastores. Site Recovery Manager (SRM) uses the adapter to support SAN storage environments for VMFS (iSCSI and FC) and NAS storage environments for NFS.

You must download and install the SRA server and adapter from the NetApp Support Site. The adapter is integrated with the SRA appliance, and you must register the SRA appliance with the adapter.

What Site Recovery Manager does

Site Recovery Manager uses virtualization to provide end-to-end disaster recovery management and automation across the entire data center. It uses the VMware infrastructure to build, automate, and test disaster recovery plans for the data center.

It works with Storage Replication Adapter to discover arrays and replicated and exported datastores and to fail over or test failover datastores.

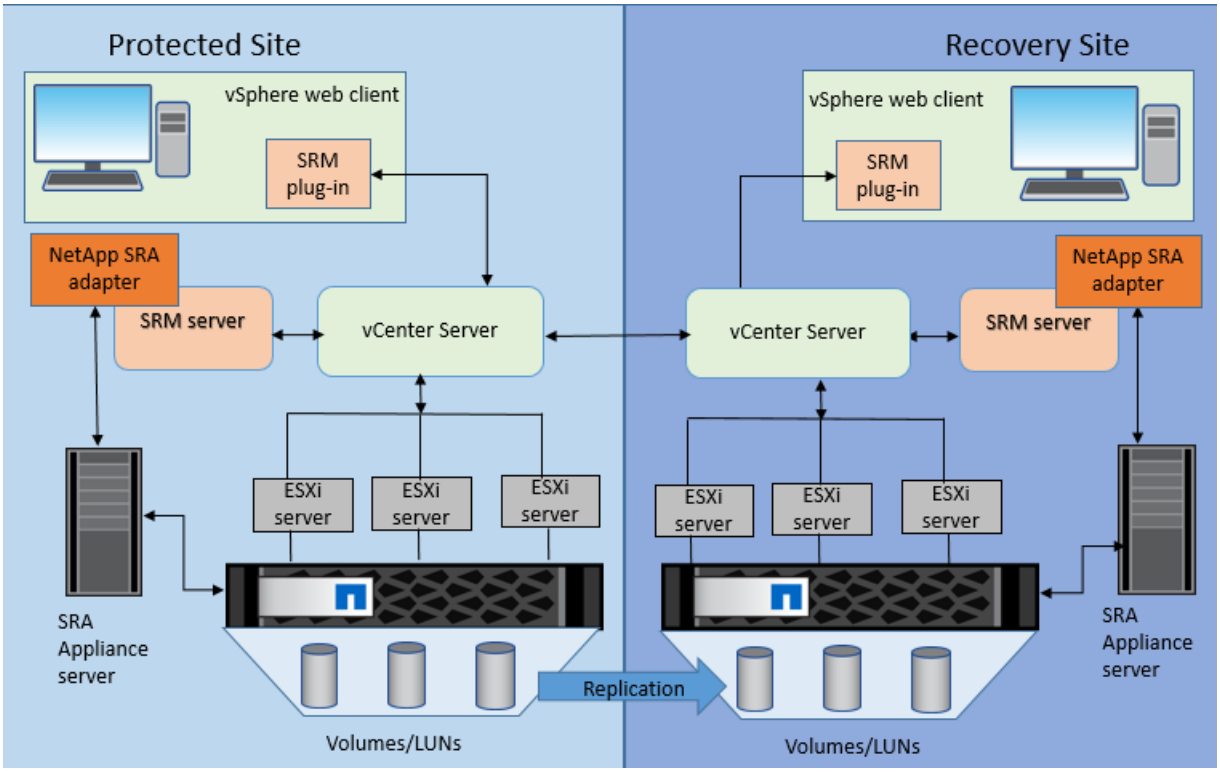
For information about Site Recovery Manager features, see the Site Recovery Manager documentation.

VMware Site Recovery Manager Documentation

Architecture of disaster recovery environment

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

The following illustration shows how Storage Replication Adapter (SRA) fits into a disaster recovery environment.



Role of Storage Replication Adapter in a disaster recovery environment

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

The adapter enables SRM to execute the following workflows:

- Discovery of arrays and replicated devices
- Test recovery
- Recovery
- Reprotect
- Failback procedure using reprotect and recovery workflows

How a test recovery operation works

A test recovery operation creates a cloned volume on the secondary storage system. You can perform a test recovery operation to verify that if a disaster or a planned migration occurs, the recovery operation will work correctly. Running a test recovery operation does not affect the SnapMirror replication.

During a test recovery operation, Storage Replication Adapter creates a FlexClone volume on the secondary storage system using the latest Snapshot copy of the SnapMirror recovery or destination volume. It displays the cloned export path or LUN path to Site Recovery Manager.

The name of the new cloned volume uses the prefix `/vol/testfailover_<volume_name>`. For example, if the primary volume is called “lab1_volume”, then the cloned volume is named “/vol/testfailover_lab1_volume”. To avoid accidentally deleting working volumes when the test recovery

operation ends, you must avoid using the term “testfailover” in the names of your working volumes. You can verify the names of the volumes on the secondary storage system by running the `vol show` command.

The test recovery operation volume does not have a space guarantee because it is not used for an actual recovery.

When the test recovery operation ends, the cleanup operation begins. During this operation, Storage Replication Adapter destroys the FlexClone volume that was used in the test recovery operation. This includes all the directories, LUNs, igroups, volumes, and NFS rules.

NAS environment

In a NAS environment, Storage Replication Adapter mounts a FlexClone volume to a junction path using the prefix `/vol/testfailover_<volume_name>`.

By default, Storage Replication Adapter creates a new export policy called “testfailover_<volume_name>_<exportpolicy>”. This new policy includes rules for all the clients that require access to the volume. The rules must allow access using the NFS protocol. However if the volume already has an export policy that was created by a test failover operation, Storage Replication Adapter uses that export policy and adds rules for any missing clients.

If you want to maintain your nested junction paths at the recovery site, you must manually mount them on the required paths after replication, but before a failover occurs.

SAN environment

In a SAN environment, the test recovery operation maps the LUNs of the FlexClone volume to an igroup with OS type set to “vmware” that contains the required initiators.

Storage Replication Adapater creates an igroup using the naming convention *testfailover_* followed by the access group name and the initiator type received from Site Recovery Manager. For example, an igroup that is created for an FC initiator for the access group “host-group-A” has the name “testfailover_host-group-A_FC_random_string”.

What happens during a recovery operation

You can perform either a recovery operation for a planned migration of services or a disaster recovery operation. When a recovery operation occurs, the recovery (destination) site takes over for the original protected site.

How the protected site and recovery site are set up

When you use Storage Replication Adapter (SRA), you set up your environment on the protected site and use SnapMirror software to replicate data from the protected site to the recovery site. The SnapMirror software relationship between the two sites mirrors the volumes on the recovery site to the volumes on the protected site.

You can perform read and write operations on the protected site. On the failover site, the volumes are data-protected and do not have read and write permissions. During a recovery operation, the SnapMirror software relationship between the protected site and the recovery site is broken. At that point, the volumes on the recovery site become read-enabled and write-enabled. In addition, the protected virtual machines become available on the recovery site.

NAS environment

In a NAS environment, you should ensure that you have the correct configuration on the recovery site before a recovery occurs. SnapMirror does not replicate the Storage Virtual Machine (SVM).

If you want to maintain your nested junction paths at the recovery site, you must manually mount them on the required paths after replication, but before a failover occurs.

SAN environment

In a SAN environment, you must create a volume without any LUNs on the recovery site. The SnapMirror software operation then creates the LUNs on the recovery site to match the LUNs on the protected site. However, the LUNs on the recovery site remain unmapped until a recovery operation takes place.

Planned migration recovery operation

Scheduling a planned migration allows SRA to synchronize the protected site and the recovery site before the migration starts. SRA performs the following actions during a planned migration recovery operation:

- Shuts down the virtual machines at the protected site
  If SRA cannot do this, the planned migration fails.
- Performs a SnapMirror software update
- Synchronizes the storage systems
- Quiesces the devices on the recovery site
- Breaks the SnapMirror software relationship between the sites

NAS environment

In a NAS environment, SRA checks the export policy. If the existing export policy contains rules for all of the required client mappings, SRA uses that policy. Otherwise, SRA modifies the export policy by adding a new rule that has the highest priority index number.

SAN environment

In a SAN environment, SRA maps the input LUN paths to igroups with the `ostype` parameter set to "vmware". If an igroup exists that contains all of the LUNs, SRA uses that igroup. Otherwise, SRA creates a new igroup with the name failover_igroup_domain-<*`domain_id`*>.

Disaster recovery operation

Unlike a planned migration, a disaster recovery operation does not check the protected site to synchronize the data. In most cases, when a disaster recovery operation occurs, the protected site is not available.

In addition, a disaster recovery operation continues to completion even though some of the intermediate steps during the operation might fail.

During a disaster recovery operation, SRA performs the following actions on the recovery site:

- Cancels any ongoing SnapMirror software transfers from the protected site to the recovery site
- Quiesces the devices on the recovery site
- Breaks the SnapMirror software relationship between the sites

NAS environment

In a NAS environment, SRA performs the following actions during a disaster recovery operation:

- Mounts the volume at the defined file path
- Verifies that the export policy contains rules for all of the required clients
  If the export policy does not contain rules for all of the clients, SRA creates a rule with the highest priority index number for the clients.

SAN environment

In a SAN environment, SRA maps the input LUN paths to igroups with the `ostype` parameter set to "vmware". If an igroup exists that contains all of the initiators for the hosts that need to access the

LUNs, SRA uses that igroup. Otherwise, SRA creates a new igroup with the name failover_igroup_domain-<*domain_id*> and adds the required initiators.

Site Recovery Manager actions during a recovery operation

The recovery operation brings the datastores online and displays the failed-over datastores that are now active on the recovery site to Site Recovery Manager.

Site Recovery Manager runs `QueryReplicationSettings` during a planned migration to obtain information such as the replication schedule and the throttle that the SnapMirror relationship used before the failover occurred.

Note: SRA does not have a separate configuration file. SRA uses the configuration that you set for the SRA server for ONTAP.

Site Recovery Manager provides the replication settings during the reverse replication so that SRA can re-create the original settings.

Note: If you encounter problems such as database corruption, you must manually restore the protected site.

What a reprotect operation does

A reprotect operation is a reverse replication operation. You can use this operation after a recovery operation to restore the SnapMirror relationship from the recovery site to the original protected site (the site that went down). After this operation, the site roles are reversed. The recovery site serves data and acts as the protected site. The original protected site now acts as the recovery site.

Following a failover, the recovery site takes over all the jobs that you had been performing on the protected site and enables you to continue working with data. You can make changes to the job settings and the data the same way you could when you were working on the protected site.

When Storage Replication Adapter fails back to the protected site and runs a reprotect operation, the SnapMirror replication operation reverses. All the changes that you made on the recovery site are replicated to the protected site, and the protected site begins serving data. SnapMirror syncs the two sites.

Note: When the SnapMirror relationship is reversed during a reprotect operation, Storage Replication Adapter (SRA) does not check the protected site to determine whether you made any changes to the SnapMirror policy while you were working on that site. Any changes you made to a policy on the protected site are not restored when the protected site is brought back up. However, SRA issues a warning if this happens.

Site Recovery Manager provides the replication settings during the reverse replication so that SRA can recreate the original settings.

You can perform a reprotect operation by selecting the Reprotect option in the VMware vSphere Web Client.

Failback procedure using reprotect and recovery workflows

The failback procedure enables you to restore the original direction of replication between the protected site and the recovery site after a recovery operation completes.

After you perform a recovery and reprotect operation, the direction of replication is reversed. To restore the direction of replication and fail back to the original protected site, you must perform the following workflows:

1. Recovery operation for planned migration
   Migrates virtual machines from the recovery site back to the protected site.
2. Reprotect

Reverses the replication direction so that the original replication direction of going from the protected site to the recovery site is restored.

New features of Storage Replication Adapter 4.0

Storage Replication Adapter (SRA) 4.0 introduces support for new features along with enhancements to existing features.

- Support for multitenancy
  You can add SVM credentials to Site Recovery Manager's array manager to enable customers to provide multitenancy. Adding cluster credentials to array manager is also supported.
- Support for version flexible SnapMirror
  You can create SnapMirror relationships between protected and recovery sites, even if there are different versions of ONTAP at the source and destination storage systems. This version of SRA supports data protection (DP) and extended data protection (XDP) relationship types with the async-mirror and mirror-vault policies.
- Support for Linked Mode of VMware vSphere

Limitations of Storage Replication Adapter

You must be aware of certain limitations before installing Storage Replication Adapter (SRA).

- NetApp SRA does not support fan-out replication by using SnapMirror to mirror a datastore to multiple different destinations.
- NetApp SRA ignores SnapVault relationships; a source can be replicated with SnapMirror and with SnapVault.
  However, SnapVault relationships that are not reconfigured as SnapMirror relationships are failed over and are reversed with SRM.
- Periodic SnapMirror transfers must be managed and scheduled by using NetApp software such as the built-in scheduler in ONTAP or OnCommand System Manager.
  SRM does not perform scheduled SnapMirror updates or baseline transfers.
- SRA does not support IPv6 protocol.

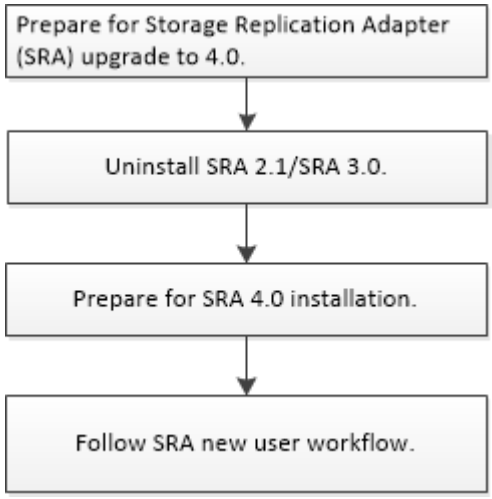
Overview of Storage Replication Adapter installation workflows

If you have an existing disaster recovery setup in your enterprise and want to upgrade to Storage Replication Adapter (SRA) 4.0, then you depending on your setup, you can either refer to the new user workflow or the existing SRA user workflow.

Installation workflow for existing Storage Replication Adapter users

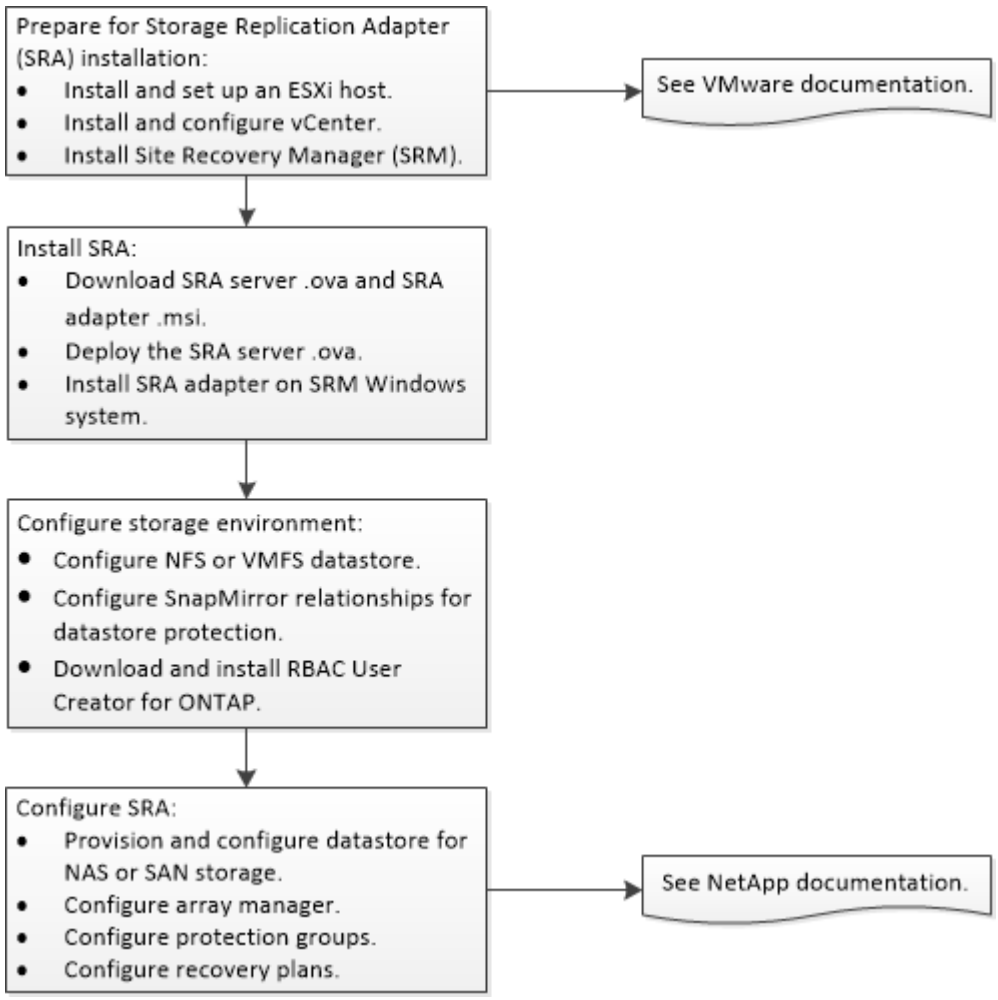
If you have an existing setup of Storage Replication Adapter (SRA) for your storage system and want to upgrade to SRA 4.0, then you can use one of the following workflow based on your current disaster recovery environment.

The following workflow shows how you can upgrade from earlier version SRA 2.1 or SRA 3.0 to SRA 4.0



Installation workflow for new users

If you are new to Storage Replication Adapter (SRA) and have never used a SRA product, you need to install and configure the server and storage, and set up NAS and SAN environment before you can set up your disaster recovery environment.



Preparing Storage Replication Adapter setup

You must be aware of several prerequisites before you begin installing Storage Replication Adapter (SRA) 4.0 and ensure that all the requirements are satisfied.

- Host requirements
- Supported storage systems and application

Host requirements for Storage Replication Adapter

Before you begin the installation of Storage Replication Adapter (SRA), you should be familiar with the installation package space requirements and some basic host system requirements.

Installation package space requirements

- 2.1 GB for thin provisioned installations
- 54.0 GB for thick provisioned installations

SRM Server host system sizing requirements

- ESX or ESXi 6.0 or higher
- Recommended memory: 8 GB RAM
- Recommended CPUs: 4

Supported storage system and applications

It is essential that you check the Interoperability Matrix on the NetApp Support Site for all the latest interoperability information. It is helpful to understand the basic storage system, application, and browser support before you begin your installation.

The following information shows the currently supported configurations. For the latest information, see the Interoperability Matrix.

Supported ONTAP versions

Storage Replication Adapter (SRA) 4.0 supports clustered Data ONTAP 8.3.2, ONTAP 9.0, and ONTAP 9.1.

vCenter server requirements

SRA 4.0 requires the following: SRM 6.0, 6.1, or 6.5

SRM requirements

SRA 4.0 requires the following: SRM 6.0,6.1 or 6.5

License

SRA 4.0 requires SnapMirror license.

Note: You must enable FlexClone and SnapMirror licenses before performing test failover and failover operations for SRA.

Overview of Storage Replication Adapter installation

To install and set up Storage Replication Adapter (SRA) for ONTAP for VMware vCenter Site Recovery Manager, you must verify that your environment meets the SRA requirements and coordinate the adapter's installation with the installation of other programs.

The following is a high-level checklist of the steps you must perform to install Storage Replication Adapter:

1. If you have an earlier version of SRA for ONTAP installed, you must uninstall it.
2. Check the NetApp Interoperability Matrix tool (IMT) to determine the system requirements for Storage Replication Adapter and the correct versions of the software packages that work with SRA.
   You must also have the correct licenses.
   NetApp Interoperability Matrix Tool
3. Set up your storage systems:
   - They must be running ONTAP.
   - They must support Storage Virtual Machines (SVMs).
   - SnapMirror must be set up.
   - If you plan to use the test failover operation, you must have the FlexClone license installed.

Configuration of Storage Replication Adapter storage environment on page 19

Related information

VMware Compatibility Guide

Downloading Storage Replication Adapter

Before you install Storage Replication Adapter (SRA), you have to download the installation files for SRA, the `.OVA` file for the SRA server, and the `.msi` file for the adapter 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 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 the file directly to your target system.
   - Download the file to a PC host, and copy the file to the target system.

After you finish

You must deploy the `.OVA` file on an ESXi host, and install the `.msi` file on an SRM server.

Related information

NetApp Support Site: mysupport.netapp.com

Storage Replication Adapter and Site Recovery Manager deployment models

Storage Replication Adapter (SRA) must be installed on the Site Recovery Manager (SRM) server. You must verify the SRM configuration in your vCenter Server before installing SRA.

The SRM server is deployed in one of the following vCenter Server topologies:

- Two-site topology with one vCenter Server instance per platform services controller
- Two-site topology with multiple vCenter Server instances per platform services controller
- Single-site topology with a shared platform services controller

Whatever deployment model SRM may be installed in, the adapter must be installed on the SRM server. During the installation of the adapter, when prompted, you must provide the details of the SRA server.

Installing Storage Replication Adapter server

You must install the Storage Replication Adapter (SRA) 4.0 server for VMware's Site Recovery Manager (SRM) to enable disaster recovery and to manage your storage systems.

Before you begin

- You must have downloaded the Storage Replication Adapter installation file from the NetApp Support Site.
- You must have set up a vCenter Server to configure the disaster recovery environment.
- You must have installed Site Recovery Manager on the protected site and the recovery site.
  VMware Site Recovery Manager Documentation

Steps

1. Log in to your vCenter Server, and then click **Host & Clusters** on the homepage.
2. Right-click your ESX host, and then click **Deploy OVF Template**.
3. In the **Deploy OVF Template** wizard, browse to the folder where the SRA server `OVA` file is downloaded.
4. Select the SRA `OVA` file, and then click **Open**.
5. Review the `OVA` details, and accept the license agreements to continue.
6. Perform the following steps to provide details for your SRA installation:

In the screen...	Perform these steps...
Select a name and folder	• Enter a name for the SRA server. • Select a folder or datacenter. • Click **Next**.
Select a storage	• Select the default values for the disk format and storage policy. • Select a destination datastore. • Click **Next**.
Setup networks	• Select the default network. • Click **Next**.
Customize template	• Enter the required information in the network properties section. • Provide a password for the maintenance user and for the administrator account for the web-based command line interface (CLI). **Note:** The administrator password must have a minimum of eight characters. • Click **Finish**.

7. In the **Ready to complete** section:

   a. Review the deployment settings, and then select **Power on deployment**.

   b. Click **Finish**.

   The deployment progress is shown in the taskbar.

Result

You will receive the IP address of the SRA server after the successful completion of deployment. You can also use the SRA maintenance console for maintenance and diagnostics, or to start, stop, or enable SSH.

Installing Storage Replication Adapter

You must install the Storage Replication Adapter (SRA) on a Windows server where Storage Recovery Manager (SRM) is installed in the VMware environment.

Before you begin

- You must have installed SRM 6.0 or later for your vCenter.
- You must have completed the installation of the SRA server.

Steps

1. Download the adapter installer file from the NetApp Support site.
2. Double-click the downloaded installer and follow the on-screen instructions to complete the installation.
3. Enter the IP address of the SRA server and password when prompted to continue the installation.

Configuring storage system for disaster recovery

You must configure your storage environment and SnapMirror relationships for disaster recovery functionality to be successful.

Configuring SnapMirror relationships for Storage Replication Adapter

You must configure SnapMirror relationships between the protected site and recovery site to enable support for array-based replication of SRM.

Before you begin

- You must have installed SRM and Storage Replication Adapter (SRA) servers on the protected site and recovery site.
- You must have configured your storage system for either SAN or NAS.

About this task

NetApp SRA 4.0 leverages SnapMirror asynchronous volume replication in ONTAP for array-based replication in SRM. The following table lists the supported replication types with their corresponding policies:

Replication relationship type	Policy type	Policy name
Data protection (DP)	async-mirror	DPDefault
Extended data protection (XDP)	async-mirror	• DPDefault • MirrorLatest • MirrorAllSnapShots
Extended data protection (XDP)	mirror-vault	Mirror and vault **Note:** Extended data protection (XDP) SnapMirror relationship with "vault" only policy is not supported.

Note: SnapMirror relationships between mixed configurations of NAS and SAN storage systems are not supported.

Both the protected site and recovery site must be configured for either NAS or SAN.

You can use OnCommand System Manager to configure SnapMirror relationships.

Steps

1. Log in to OnCommand System Manager by using https://node-management-IP.

   You must enter your cluster management credentials to log into OnCommand System Manager .

2. Configure the mirror relationship between the protected and recovery sites.

ONTAP 9 Cluster Management Using OnCommand System Manager

Note: NetApp recommends that you must configure unique names for volumes on the protected and recovery sites.

Configuration of Storage Replication Adapter storage environment

Based on whether you are supporting SAN or NAS storage system, you must configure your storage requirements before installing SRA.

NAS environment storage system requirements

- You must ensure that an NFS license is installed on each storage system.
- On the protected site, you must create a volume of type RW.
- You must set up a junction path so that the volume can be mounted and accessed by the ESXi host.
- You must either create an export policy that contains rules for all the clients that require access to the volume or add the rules to an existing export policy.
  The rules must allow access using the NFS protocol.

  Note: If an export policy rule does not exist during a disaster recovery event or a planned migration, Storage Replication Adapter (SRA) creates a new export policy called *testfailover_<volume_name>_<exportpolicy>*. This new policy includes rules for all the clients that require access to the volume.
- You must map the volume with the export policy.
- You must ensure that the NFS services are running on each storage system.
- You must ensure that the volume that contains the exports is replicated to the secondary storage system on the recovery site.
  You can use the following commands on the recovery site and protected site:
  - **`snapmirror show`**
  - **`snapmirror list-destinations`**

  You can use the following command to confirm that the volume has been replicated on the recovery site:

  `snapmirror show`
  Refer to ONTAP documents for more information on SnapMirror modes.
  Clustered Data ONTAP Data Protection Guide
- You must initialize the SnapMirror relationship.

Note:

- SRA does not support Storage Virtual Machines (SVMs) with the same name on protected and recovery sites.
- You must not create a volume starting with the name "testfailover_" as the failover operation will fail due to duplicate volume names.
- When NFS datastores are created using qtrees, then protection groups cannot be created.

SAN environment storage system requirements

- You must ensure that either the FC or iSCSI license is installed on each storage system.
- You must ensure that either FC or iSCSI services are running on each storage system.
- You must create a volume of type RW, a LUN with the `ostype` set to `vmware`, and an igroup with the ESXi initiator on the protected site.
- You must create a volume of type DP on the recovery site, .
- You must ensure that the volume that contains the LUN is replicated to the secondary storage system on the recovery site.
  You can use the following commands on the recovery site and protected site to confirm that the export is part of only one replication relationship:

  `snapmirror show`
  and

  `snapmirror list-destinations`
  . You can also use the

  `snapmirror show`
  command to confirm that the volume has been replicated on the recovery site.
- You must initialize the SnapMirror relationship.

For both NAS and SAN environments, you must have the SnapMirror license.

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

Configuring role-based access control

Storage Replication Adapter (SRA) requires the use of role-based access control (RBAC). RBAC enables administrators to specify which vSphere objects and storage systems a user can access and work with. SRA supports both vCenter Server RBAC and ONTAP RBAC.

ONTAP RBAC refers to the roles that contain the ONTAP privileges that are required to enable SRA to perform storage operations such as discovering storage controllers. SRA has a discovery role for ONTAP with directly connected Storage Virtual Machines (SVMs). The discovery role has all of the required ONTAP privileges for discovering storage in an environment.

To set up an ONTAP role, you should use the RBAC User Creator tool for ONTAP. You can also manually configure the SVM administrator role and assign privileges by using OnCommand System Manager.

Creating a new user role on page 21

Before installing the RBAC tool, you must ensure that you have .NET Framework version 4.5.2 or higher and PowerShell version 3.0 or higher.

When you install the RBAC tool, an SVM administrator role is created of type SAN or NAS, depending on the storage system that you have configured. You can assign privileges to the SVM administrator for access to SRA. This tool, which enables you to quickly set up the necessary RBAC roles, is available from the NetApp ToolChest on the NetApp Support Site (*mysupport.netapp.com*).

How to use the RBAC User Creator for Data ONTAP

Creating a new user role

You can create a new user role for Storage Replication Adapter (SRA) by using OnCommand System Manager. You can also assign the required privileges for a user based on whether you are adding a cluster or a Storage Virtual Machine (SVM) to the array manager.

Steps

1. Log in to OnCommand System Manager.
2. Click **SVM > SVM Settings > Roles**.
3. Click **Add**, and then enter a name for the user role in the **Add Role** dialog box.
4. In the **Role Attributes** section, click **Add** to add a command, specify the required **Access Level** ("all" or "read-only"), and then click **OK**.

   You must add commands one at a time by using the Add button. The command for adding an NFS SVM is `vserver nfs create`.

   Configuring user roles using ONTAP commands on page 21
5. Click **Add** to create the new user role.

Creating new Storage Replication Adapter user

You can use OnCommand System Manager to create new users for Storage Replication Adapter (SRA) with the required privileges and access.

Steps

1. Login to OnCommand System Manager.
2. Click **SVM > SVM Settings > Users**.
3. In the **Add User** dialog box, enter a name and password for the new user role.
4. In the **User Login Methods** dialog box, select **ontapi** for **Applications**, for the **Role** dropdown select the new role that you have created, and then click **OK**.
5. Click **Add** to create the new user.

Configuring user roles using ONTAP commands

VMware vCenter Server and ONTAP use role-based access control (RBAC) to allow or restrict user permissions. You can manually create a user role for Storage Replication Adapter (SRA) by using OnCommand System Manager. You can provide either the cluster credentials or the Storage Virtual Machine (SVM) credentials to SRA to support multitenancy.

You can see the following knowledge base article for details on creating user roles for SRA.

https://kb.netapp.com/support/s/article/ka31A0000008h1sQAA/SRA-4-0-Configuring-ONTAP-users-and-adding-clusters-SVMs?language=en_US

Setting up initial configurations for Storage Replication Adapter

Before you can run Storage Replication Adapter (SRA) for VMware vCenter Site Recovery Manager, you must perform certain configuration tasks, such as setting up the storage systems on the sites and configuring protected and recovery sites. You can also customize SRA by using the Site Recover Manager Array Manager wizard.

Configuring Storage Replication Adapter for NAS environment

You must set up the storage systems before running Storage Replication Adapter (SRA) for VMware vCenter Site Recovery Manager.

Before you begin

You must have installed the following programs on the protected site and the recovery site:

- Site Recovery Manager
  Documentation about installing Site Recovery Manager is on the VMware site. *VMware Site Recovery Manager Documentation*
- SRA 4.0
  The adapter installed on SRM and SRA server.

Steps

1. Verify that the datastores at the protected site contain virtual machines that are registered with vCenter Server.
2. Verify that the ESXi hosts at the protected site have mounted the NFS exports volumes from the Storage Virtual Machine (SVM).
3. Verify that valid addresses, such as the IP address, host name, or FQDN, on which the NFS exports is present, are entered in the **NFS Addresses** field when using the **Array Manager** wizard to add arrays to Site Recovery Manager.
4. Use the `ping` command on each ESXi host containing secondary storage to verify that the host has a VMkernel port that can access the IP addresses that are used to serve NFS exports from the SVM.

Related information

NetApp Support Site: mysupport.netapp.com

Configuring Storage Replication Adapter for SAN environment

You must set up the storage systems before running Storage Replication Adapter (SRA) for Site Recovery Manager (SRM).

Before you begin

You must have installed the following programs on the protected site and the recovery site:

- SRM
  Documentation about installing SRM is on the VMware site. *VMware Site Recovery Manager Documentation*
- SRA 4.0
  The adapter installed on SRM and SRA server

Steps

1. Verify that the primary ESXi hosts are connected to LUNs in the primary storage system on the protected site.
2. Verify that the LUNS are in igroups that have `ostype` set to *vmware* on the primary storage system.
3. Verify that the 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 ESXi hosts have local LUNs connected on the SVM or by using the `fcp show initiators` command or the `iscsi show initiators` command on the SVMs.

Configuring Storage Replication Adapter using the web-based command-line interface

Storage Replication Adapter (SRA) 4.0 provides you with a web-based command-line interface (CLI) that you can use to add, edit, or remove clusters or Storage Virtual Machines (SVMs).

Before you begin

- You must have installed SRA.
- You must have configured your storage system.
- You must have the required administrator credentials that were created during installation.

Steps

1. Access the web-based CLI of SRA by using `https://sra_server_ip:9083`, and then log in with the administrator password.
2. Click **Available Commands** to view the commands that are supported for configuring storage systems.

   Note:

- If you plan to use the cluster interface for the array manager, you must add the cluster to the SRA server.
- If you plan to add SVMs in the array manager, you can add either the cluster interface or SVMs to the SRA server.
- SRA 4.0 does not support SVMs with Infinite Volume.

3. Enter the required commands on the web-based CLI, and then click **Execute** to configure your storage systems.

If you want to...	Then execute the following command...
Add a cluster to the SRA server	`cluster add -cluster_ip=cluster_mgmt_ip -username=new_user_name -password=password -ssl=true` Example: `cluster add -cluster_ip=1.2.3.4 -username=admin -password=secret -ssl=true` “1.2.3.4” is the IP address of the cluster, “admin” is the user name, and the password is “secret”. The user name must be set to “admin”.
List a cluster in the SRA server	You can use one of the following commands: • `cluster list` • `cluster list -cluster_ip=<IP address>` • `cluster list -show_usernames=false -show_uuids=false -show_svms=false -cluster_ip=<IP address>`
Delete a cluster from the SRA server	`cluster delete -cluster_ip=<IP address>`
Add an SVM to the SRA server	`vserver add -vserver_ip=vserver_admin_ip-username=new_user_name-password=password -ssl=true` Example: `vserver add -vserver_ip=1.2.3.4 -username=sraadmin -password=secret -ssl=true` “1.2.3.4” is the IP address of the SVM, “sradmin” is the user name, and the password is “secret”. The user name must be set to “sradmin”.

If you want to...	Then execute the following command...
List an SVM in the SRA server	You can use one of the following commands: • `vserver list` • `vserver list -vserver_ip=<IP address>` • `vserver list -show_usernames=false -show_uuids=false -vserver_ip=<IP address>`
Delete an SVM from the SRA server	`vserver delete -vserver_ip=<IP address>`

The parameters that are used in the commands are:

IP address

Depending on whether you want to add a cluster or an SVM, you can enter the IP address of the storage component.

User name and password

If you are using cluster credentials, you must configure an admin user. If you are using SVM credentials, you must configure an SVM admin user.

ssl

The value can be true or false based on whether you want to use SSL to connect to the cluster or the SVM.

port

The port that is used to connect to the controller.

protocol

The protocols that are used for access can have one of the following values: nfs, iscsi, or fcp.

force

If the value is set to false, this parameter skips the verification of the destination SVM for product compatibility. By default, this parameter is set to true.

flexvols

If the value is set to false, the information about flexible volumes is not shown. By default, this parameter is set to true.

uuids

If the value is set to false, UUID information is not shown. By default, this parameter is set to true.

var

This field is user-defined. You can provide your user name or password depending on the parameter that is used.

Related information

Cluster Management Using OnCommand System Manager

Pairing protected and recovery sites

You must pair the protected and recovery sites created using your vSphere web client to enable Storage Replication Adapter (SRA) to discover the storage systems.

Before you begin

- You must have installed Site Recovery Manager (SRM) on the protected and recovery sites.
- You must have installed SRA on the protected and recovery sites.

Steps

1. Double-click **Site Recovery** on the vSphere web client, and then click **Sites**.
2. Click **Objects > Actions > Pair Sites**.
3. In the **Pair Site Recovery Manager Servers** dialog box, enter the address of the protected site's Platform Services Controller, and then click **Next**.
4. In the **Select vCenter Server** option, do the following:
   a. Verify that the protected site's vCenter Server appears as a matching candidate to pair.
   b. Enter the SSO administrative credentials, and then click **Finish**.
5. If prompted, click **Yes** to accept the security certificates.

Result

Both the protected and recovery sites will appear in the Objects dialog box.

Configuring protected and recovery site resources

You must configure your resources like VM networks, ESXi hosts, and folders on both the protected site to enable identification of each resource on the protected site with a resource at the recovery site.

You must complete the following resource configurations:

- Network mappings
- Folder mappings
- Resource mappings
- Placeholder datastores

Configuring network mappings

You must map your networks on the protected site and the recovery site to enable communication between them.

Before you begin

You must have connected the protected and recovery sites.

Steps

1. Log in to your vCenter Server and click on **Site Recovery > Sites**.

2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Network Mappings**.
4. Click the  icon to create a new network mapping.

   The Create Network Mapping wizard appears.
5. In the Create Network Mapping wizard, perform the following:
   a. Select **Automatically Prepare Mappings for Networks with Matching Names**, and click **Next**.
   b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.
   c. Click **Next** after mappings are created successfully.
   d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Result

The Network Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configuring folder mappings

You must map your folders on the protected site and recovery site to enable communication between them.

Before you begin

You must have connected the protected and recovery sites.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery > Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Folder Mappings**.
4. Click the  icon to create a new folder mapping.

   The Create Folder Mapping wizard appears.
5. In the **Create Folder Mapping** wizard, perform the following:
   a. Select **Automatically Prepare Mappings for Folders with Matching Names**, and click **Next**.
   b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.
   c. Click **Next** after mappings are created successfully.
   d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Result

The Folder Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configuring resource mappings

You must map your resources on the protected site and recovery site so that virtual machines are configured to fail over into one group of hosts or the other.

Before you begin

You must have connected the protected and recovery sites.

About this task

Note: In Site Recovery Manager (SRM), resources can be resource pools, ESXi hosts, or vSphere clusters.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery > Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Resource Mappings**.
4. Click the  icon to create a new resource mapping.

   The Create Resource Mapping wizard appears.
5. In the **Create Resource Mapping** wizard, perform the following:
   a. Select **Automatically Prepare Mappings for Resource with Matching Names**, and click **Next**.
   b. Select the required data center objects for the protected and recovery sites, and click **Add Mappings**.
   c. Click **Next** after mappings are created successfully.
   d. Select the object that was used earlier to create reverse mapping, and then click **Finish**.

Result

The Resource Mappings page displays the protected site resources and the recovery site resources. You can follow the same steps for other networks in your environment.

Configuring placeholder datastores

You must configure a placeholder datastore to hold a place in the vCenter inventory at the recovery site for the protected virtual machine (VM). The placeholder datastore does not need to be large as the placeholder VMs are small and use only a few hundred or fewer kilobytes.

Before you begin

- You must have connected the protected and recovery sites.
- You must have configured your resource mappings.

Steps

1. Log in to your vCenter Server, and click on **Site Recovery** > **Sites**.
2. Select your protected site, and then click **Manage**.
3. In the Manage tab, select **Placeholder Datastores**.
4. Click the  icon to create a new placeholder datastore.
5. Select the appropriate datastore, and then click **OK**.

   Note: Placeholder datastores can be local or remote and should not be replicated.
6. Repeat the steps 3 to 5 to configure a placeholder datastore for the recovery site.

Configuring array manager

You can configure Storage Replication Adapter (SRA) by using the Array Manager wizard of Site Recovery Manager (SRM) to enable interaction between SRM and Storage Virtual Machine (SVM).

Before you begin

- The protected and recovery sites must already be paired in SRM.
- SnapMirror relationships between the protected and recovery sites must already be configured and replicated.

About this task

SRA 4.0 supports cluster-level management and SVM-level management. You must enable SVM management LIFs to enable multitenancy.

Steps

1. In SRM, 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 the **Display Name** field.
   b. In the **SRA Type** field, select **NetApp Storage Replication Adapter for ONTAP**.
   c. Enter the information to connect to the cluster or the SVM:
      - If you are connecting to a cluster, enter the cluster management LIF.
      - If you are connecting directly to an SVM, enter the IP address of the SVM.

      Note: You can add either the SVM management IP using the SRA server web CLI `vserver add` command or the cluster management IP using the `cluster add`.

      You must have configured your storage before configuring array manager. See *Configuring Storage Replication Adapter using the web-based command-line interface* on page 23.

   d. If you are connecting to a cluster, enter the name of the SVM in **SVM name**; otherwise, leave this field blank.
   e. Optional: Enter the volumes to be discovered in **Volume include list**.

You can 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 the partial volume name.

Example

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

f. Optional: Enter the volumes to be excluded from discovery in **Volume exclude list**.

You can 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

For 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 fields and *dst_vol1* in the recovery site fields.

g. Enter the user name of the cluster-level or SVM-level account in **Username**.

h. 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**.

After you finish

You can follow the same steps for the recovery site by using the appropriate SVM management IP addresses and credentials. On the Enable Array Pairs screen of the Add Array Manager wizard, you should verify that the correct array pair is selected, and that it shows as ready to be enabled.

Verifying the replicated storage environment

You must to verify that the protected site and recovery site are successfully paired after configuring Storage Replication Adapter (SRA) using Site Recovery Manager (SRM) array manager. The replicated storage must be discoverable by both the protected and recovery sites.

Before you begin

- You must have configured your storage system.
- You must have paired the protected and recovery sites by using SRM's array manager.
- You must enable FlexClone and SnapMirror licenses before performing test failover and failover operations for SRA.

Steps

1. Log in to your vCenter.
2. Access **Site Recovery > Array Based Replication**.
3. Select the required SVM and verify the corresponding details in the **Array Pairs**.

   Tthe storage systems must be discovered at the protected site and recovery site with the Status as **Enabled**.

Configuring Storage Replication Adapter for disaster recovery

After completing the initial Storage Replication Adapter (SRA) configuration, you must set up disaster recovery workflows that can be executed.

To configure disaster recovery workflows, you must create protection groups, and then create a recovery plan.

Note: During disaster recovery, SRA checks for existing export policies for the selected volumes. If an existing export policy is associated with the storage object, then that policy is used. In the absence of an export policy, SRA creates an export policy to be used for the volume.

Building protection groups

You must create protection groups to protect a group of virtual machines on the protected site.

Before you begin

- You must have installed Storage Replication Adapter (SRA) and Site Recovery Manager (SRM) in your vCenter Server.
- You must have configured SRA and performed replication operation for the protected site. Each replicated virtual machine must be assigned to an existing resource pool, folder, and network on the recovery site using inventory mappings.

Steps

1. Log in to your vCenter Server, and click **Site Recovery** > **Protection Groups**.
2. In the **Protection Groups** pane, click > **Objects** >  .
3. In the **Create Protection Group** wizard, enter the following information:
   a. Enter a name and description for the protection group, and then click **Next**.
   b. In the Protection group type field, select the protected site, array-based replication (ABR) as the protection group type, and then click **Next**.
   c. In the Datastore groups tab, select the required datastore groups, and then click **Next**.

      All the virtual machines on the selected datastore are added to the protection group.
   d. In the **Ready to complete** tab, review all the details of the protection group created, and then click **Finish**.

Result

The protection group is created. You can repeat steps 2 and 3 to create more protection groups.

Creating a recovery plan

You must create a recovery plan to define the protection groups that must be recovered simultaneously.

Before you begin

- You must have configured your storage system.

- You must have installed the Storage Replication Adapter (SRA) and Site Recovery Manager (SRM) applications.
- You must have created protection groups.

About this task

You can include multiple protection groups in a single recovery plan or include a single protection group in multiple recovery plans.

Steps

1. Log in to your vCenter Server, and click **Site Recovery** > **Sites**..
2. In the **Related Objects** tab, select **Recovery Plans**, and then click the  icon.
3. In the **Create Recovery Plan** wizard, enter the following details:
   a. In the **Name and location** tab, enter a name and description for the recovery plan, and then click Next.
   b. In the **Recovery site** tab, select the recovery site, and click **Next**.
   c. In the **Protection groups** tab, select the protection groups for the recovery plan, and then click **Next**.
   d. In the **Test networks**, select the test networks to be used for running test recovery, and then click **Next**.
   e. In the **Ready to complete** tab, review the recovery plan details, and then click **Finish**.

Verifying disaster recovery setup using test recovery workflow

You can run the test recovery workflow of Site Recovery Manager (SRM) to confirm that the Storage Replication Adapter (SRA) is configured appropriately for disaster recovery in your environment.

Before you begin

- You must have installed SRA and SRM.
- You must have configured your storage system and configured array manager by using SRM.
- You must have connected the protected and recovery sites.
- You must have configured protection groups.
- You must have configured a recovery plan.

About this task

You can the execute cleanup workflow after the test recovery operation to return the protected VMs to their initial state. To understand how storage systems are affected during different disaster recovery workflows, see *Role of Storage Replication Adapter in a disaster recovery environment* on page 6

Steps

1. Log in to your vCenter Server, and click **Site Recovery**.
2. Click **Recovery Plans**, and select the appropriate recovery plan.
3. Click the 

icon to start the process of test recovery.

4. If required select **Replicate recent changes to recovery site** in the **Confirmation** dialog box of the recovery plan, and click **Next**.
5. In the **Ready to complete** dialog box, review the recovery details, and click **Finish**.

   You can view the progress of the steps in the workflow from the Recovery Steps tab.

After you finish

You can use the History tab to review the details of the test recovery operation.

Related information

VMware Site Recovery Manager Documentation

Upgrade overview of Storage Replication Adapter

There is no direct upgrade from an earlier version of Storage Replication Adapter (SRA) 2.1 or SRA 3.0 to SRA 4.0. You must uninstall the earlier versions of SRA in your disaster environment before upgrading to SRA 4.0.

Preparing Storage Replication Adapter for upgrade

Before uninstalling the Storage Replication Adapter (SRA) version from your disaster recovery environment, you must note the existing site configurations for the protected and recovery sites.

You must note the following details before uninstalling SRA:

- Array manager configurations
  - Recovery plans
  - Storage controller information either from the cluster or from the SVM.
- Protection groups
- SVM management IP address along with the credentials if you want to configure multitenancy. However, you can continue to use cluster management IP address with SVM.

You must create backup of all data from VASA provider. The data should be obtained from VSC vCenter Server plug-in interface.

VASA Provider 6.0 for Clustered Data ONTAP User's Guide

Uninstalling Storage Replication Adapter

Before you uninstall Storage Replication Adapter (SRA) 2.1 or SRA 3.0 in order to upgrade to SRA 4.0, you must be aware of a few storage considerations.

Before you begin

- You must have gone over the preparation for upgrade.
  Preparing Storage Replication Adapter for upgrade on page 34
- You must have a created backup of the existing storage setup and configurations.

Steps

1. Go to the Control Panel on your system and access the list of installed software.
2. Click **Storage Replication Adapter**, and then click **Uninstall**.
3. Follow on-screen instructions to complete the uninstallation of SRA.

Upgrading to Storage Replication Adapter 4.0

You can upgrade to Storage Replication Adapter (SRA) 4.0 by downloading and installing the installer files that are available at the NetApp Support Site.

Before you begin

- You must have created a backup of your data from SRA.
  Preparing Storage Replication Adapter for upgrade on page 34
- You must have uninstalled the earlier version of SRA.
- You must have downloaded the installer files for SRA 4.0 from the NetApp Support Site.

Steps

1. Log in to your vCenter Server.
2. Install the downloaded installer files.

   Installing Storage Replication Adapter server on page 15

Troubleshooting

If you encounter unexpected behavior or failure while installing Storage Replication Adapter (SRA) 4.0, you can use the installation log files to identify the cause and resolve the issue.

Suggestions for handling problems installing or running Storage Replication Adapter

Storage Replication Adapter (SRA) for ONTAP for VMware vCenter Site Recovery Manager is a robust plug-in that normally works without any issues. If you do not meet certain SRA installation requirements then that might prevent the installation or performance as expected.

Where to find solutions

The following sections provide some suggestions for handling possible problems.

If you encounter a problem, but you do not see information for resolving it here, you should check the Release Notes. You can access the *Release Notes* from the NetApp Support Site at *mysupport.netapp.com*.

Possible installation issues

The Storage Replication Adapter installation fails if you do not have the prerequisite software installed. This includes the following:

- Site Recovery Manager
- Perl

Possible warning codes and error messages

Storage Replication Adapter stores warning codes and error messages in its log files: `sra.log` and `vvolvp.log`. These files are stored on SRA Server appliance.

You might encounter some of the following issues:

Unmapped LUNs result in warning and error messages

If you attempt to enable array pairs with unmapped LUNs, an error can occur:

- In the log files, the error might be logged as:
  ```
  Warning code 2067: Device in Discovery is not mapped to ESX
  host. Make sure that the device given is mapped to the ESX host,
  otherwise it won't appear in the list of storage objects.
  ```
- In the GUI, you might see an error message similar to the following:
  ```
  Device '//SRA_B/san_vol/lun3' cannot be matched to a remote peer
  device.
  ```

If you encounter one of these errors, you should perform the following actions:

- It is a good practice to check the log files when you get a warning or error message to see if they provide information about the problem.
- If the device is mapped or mounted for the storage array, you should refresh or reenable the array manager or do both.

- If the error occurs at the end of a testfailover, failover, or reprotect operation, you should take the appropriate action for your environment:
  - In a NAS environment, you should verify that the mount point can reach the host. You should verify the export policy to ensure that it provides access to the host.
  - In a SAN environment, you should verify that the LUNs are mapped and attached for SAN.

Message stating that device synchronization fails to complete correctly

If your system is misconfigured, you might see an error message similar to the following:

```
Device synchronization did not complete properly

Device synchronization might have been disrupted because of network
failure. Ensure that the storage array hosting the device is
connected to the network and accessible to its peer storage array.
Also check storage array for replication errors in the SnapMirror
log file.
```

If you encounter this problem, you should check the following things:

- Is the SnapMirror policy set to low priority?
  If you set the policy to normal priority, you should be able to resolve the problem.
- Is there a network latency with packet loss problem?
  If you are having a network problem, you should diagnose and resolve that.

Message stating that device synchronization fails to complete correctly

Description

If you system is misconfigured, you might see the an error message similar to the following:`Device synchronization did not complete properly`

```
Device synchronization might have been disrupted because of network
failure. Ensure that the storage array hosting the device is connected to
the network and accessible to its peer storage array. Also check storage
array for Replication errors in the snapmirror log file
```

Corrective action

If you encounter this problem, you should check the following things:

- Is the SnapMirror policy set to a low priority?
  If you set the policy to the normal priority, you should resolve the problem.
- Is there a network latency with packet loss problem?
  If you are having a network problem, you need to diagnose and resolve that.

When you change timezone for Storage Replication Adapter server, the change is not reflected in the web CLI

Description

If you change the timezone using the **Change TimeZone** option of Storage Replication Adapter (SRA) maintenance console, then you must restart application services for the changed timezone to be reflected in the SRA web command line interface.

SRA fails to perform optimally in a highly scaled environment

If SRA is not performing optimally in a highly scaled environment and you notice issues such as timeout error or zapi ontap timeout, then you must modify the timeout intervals.

Corrective action

If you encounter this problem, you must modify the following settings:

Storage Provider settings

- Timeout interval: Increase the value of the `StorageProvider.resignatureTimeout` option from 900 seconds to 12000 seconds.
- Enable the `StorageProvider.autoResignatureMode` option.

See the VMware documentation for modifying Storage Provider settings.

https://pubs.vmware.com/srm-60/index.jsp?topic=%2Fcom.vmware.srm.admin.doc%2FGUID-E4060824-E3C2-4869-BC39-76E88E2FF9A0.html

Storage settings

Update the timeout interval (`storage.commandTimeout`) to 12000 seconds.

See the VMware documentation for modifying Storage settings.

https://pubs.vmware.com/srm-60/index.jsp#com.vmware.srm.admin.doc/GUID-711FD223-50DB-414C-A2A7-3BEB8FAFDBD9.html

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 SVM 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 those 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, a protocol, and an 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 ONTAP data management software 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 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 unless there is a specific need to identify the type of SVM, SVM usually refers to data SVM.

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

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.

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

Index

O

P

R

S

T

U

V

W