Protect datastores and virtual machines

ONTAP tools for VMware vSphere 9.8

NetApp
February 17, 2022

Table of Contents

Protect datastores and virtual machines

Enable SRA to protect datastores

The ONTAP tools for VMware vSphere provides the option to enable the SRA capability to be used with VSC to configure disaster recovery.

What you will need

- You must have set up your vCenter Server instance and configured ESXi.
- You must have deployed ONTAP tools.
- You must have downloaded the `.msi` file for the SRA plug-in, or the `.tar.gz` file for SRM appliance only if you want to configure the Site Recovery Manager (SRM) disaster recovery solution.

  Site Recovery Manager Installation and Configuration Site Recovery Manager 8.2 has more information.

About this task

The flexibility to enable VASA Provider and SRA capabilities enables you to execute only the workflows that you require for your enterprise.

Steps

1. Log in to the web user interface of VMware vSphere.
2. From the vSphere Client, click **Menu** > **ONTAP tools Console**.
3. Click **Settings**.
4. Click **Manage Capabilities** in the **Administrative Settings** tab.
5. In the **Manage Capabilities** dialog box, select the SRA extension want to enable.
6. Enter the IP address of ONTAP tools and the administrator password, and then click **Apply**.
7. You can use one of the following methods to deploy SRA:

For Windows SRM	For SRM appliance
a. Double-click the downloaded `.msi` installer for the SRA plug-in. b. Follow the on-screen instructions. c. Enter the IP address and password of your deployed ONTAP tools.	a. Access the SRM appliance page, and then go to Storage Replication Adapters page of SRM appliance. b. Click **New Adapter**. c. Upload the *.tar.gz* installer for the SRA plug-in to SRM. d. Rescan the adapters to verify that the details are updated in the SRM Storage Replication Adapters page.

You must log out of the vSphere Client, and then log in again to verify that your selected extension is available for configuration.

Related information

Configure Storage Replication Adapter for disaster recovery

Configure storage system for disaster recovery

Configure Storage Replication Adapter for SAN environment

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

What you will need

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

  The adapter is installed either on SRM.

Steps

1. Verify that the primary ESXi hosts are connected to the LUNs in the primary storage system on the protected site.
2. Verify that the LUNS are in igroups that have the `ostype` option 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.

Configure Storage Replication Adapter for NAS environment

What you will need

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

- SRM

  Documentation about installing SRM can be found on the VMware site.

  VMware Site Recovery Manager Documentation

- SRA

  The adapter is installed on SRM and the 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 are present are specified in the **NFS Addresses** field when using the Array Manager wizard to add arrays to SRM.
4. Use the `ping` command on each ESXi host at the recovery site 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.

NetApp Support

Configure Storage Replication Adapter for highly scaled environment

You must configure the storage timeout intervals per the recommended settings for Storage Replication Adapter (SRA) to perform optimally in highly scaled environments.

Storage Provider settings

You should set the following timeout values on SRM for scaled environment:

Advanced settings	Timeout values
`StorageProvider.resignatureTimeout`	Increase the value of the setting from 900 seconds to 12000 seconds.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Set a high value(For example: 99999)

You should also enable the `StorageProvider.autoResignatureMode` option.

See VMware documentation for more information on modifying Storage Provider settings.

VMware vSphere Documentation: Change Storage Provider Settings

Storage settings

You must set the value of the `storage.commandTimeout` and `storage.maxConcurrentCommandCnt` timeout interval for highly scaled environments to 99,999 seconds.

The timeout interval specified is the maximum value. You do not need to wait for the maximum timeout to be reached. Most commands finish within the set maximum timeout interval.

You should also set the maximum time for SRA to perform a single operation in the vvol.properties file:

offtap.operation.timeout.period.seconds=86400.

NetApp Knowledgebase Answer 1001111: NetApp Storage Replication Adapter 4.0/7.X for ONTAP Sizing Guide

VMware documentation on modifying SAN Provider settings has more information.

VMware Site Recovery Manager Documentation: Change Storage Settings

Configure SRA on the SRM Appliance

After you have deployed the SRM Appliance, you should configure SRA on the SRM Appliance. The successful configuration of SRA enables SRM Appliance to communicate with SRA for disaster recovery management. You should store the ONTAP tools credentials (IP address and administrator password) in the SRM Appliance to enable communication between SRM Appliance and SRA.

What you will need

You should have uploaded the *tar.gz* file to SRM Appliance.

About this task

The configuration of SRA on SRM Appliance stores the SRA credentials in the SRM Appliance.

Steps

1. Log in using administrator account to the SRM Appliance using putty.
2. Switch to the root user using the command: `su root`
3. At the log location enter the command to get the docker ID used by SRA docker `ps -l`
4. To login to the container ID, enter command docker `exec -it -u srm <container id> sh`
5. Configure SRM with the ONTAP tools IP address and password using the command: `perl command.pl -I <va-IP> administrator <va-password>`

   A success message confirming that the storage credentials are stored is displayed. SRA can communicate with SRA server using the provided IP address, port and credentials.

Update SRA credentials

For SRM to communicate with SRA, you should update SRA credentials on the SRM server if you have modified the credentials.

What you will need

You should have executed the steps mentioned in the topic "Configuring SRA on SRM appliance".

Configuring SRA on the SRM Appliance

Steps

1. Delete the contents of the `/srm/sra/confdirectory` using:
   a. `cd /srm/sra/conf`
   b. `rm -rf *`
2. Execute the perl command to configure SRA with the new credentials:
   a. `cd /srm/sra/`
   b. `perl command.pl -I <va-IP> administrator <va-password>`

Migration of Windows SRM to SRM Appliance

If you are using Windows based Site Recovery Manager(SRM) for disaster recovery and you want to use the SRM Appliance for the same setup, then you should migrate your Windows disaster recovery setup to the appliance based SRM.

The steps involved in the migration of the disaster recovery are:

1. Upgrading your existing ONTAP tools to the 9.7.1 release.

   Upgrade to the latest release of ONTAP tools

2. Migrating Windows based Storage Replication Adapter to Appliance based SRA.
3. Migrating Windows SRM data to SRM Appliance.

See Migrate from Site Recovery Manager for Windows to Site Recovery Manager Virtual Appliance for detailed steps

Configure replication for vVols datastore to protect virtual machines

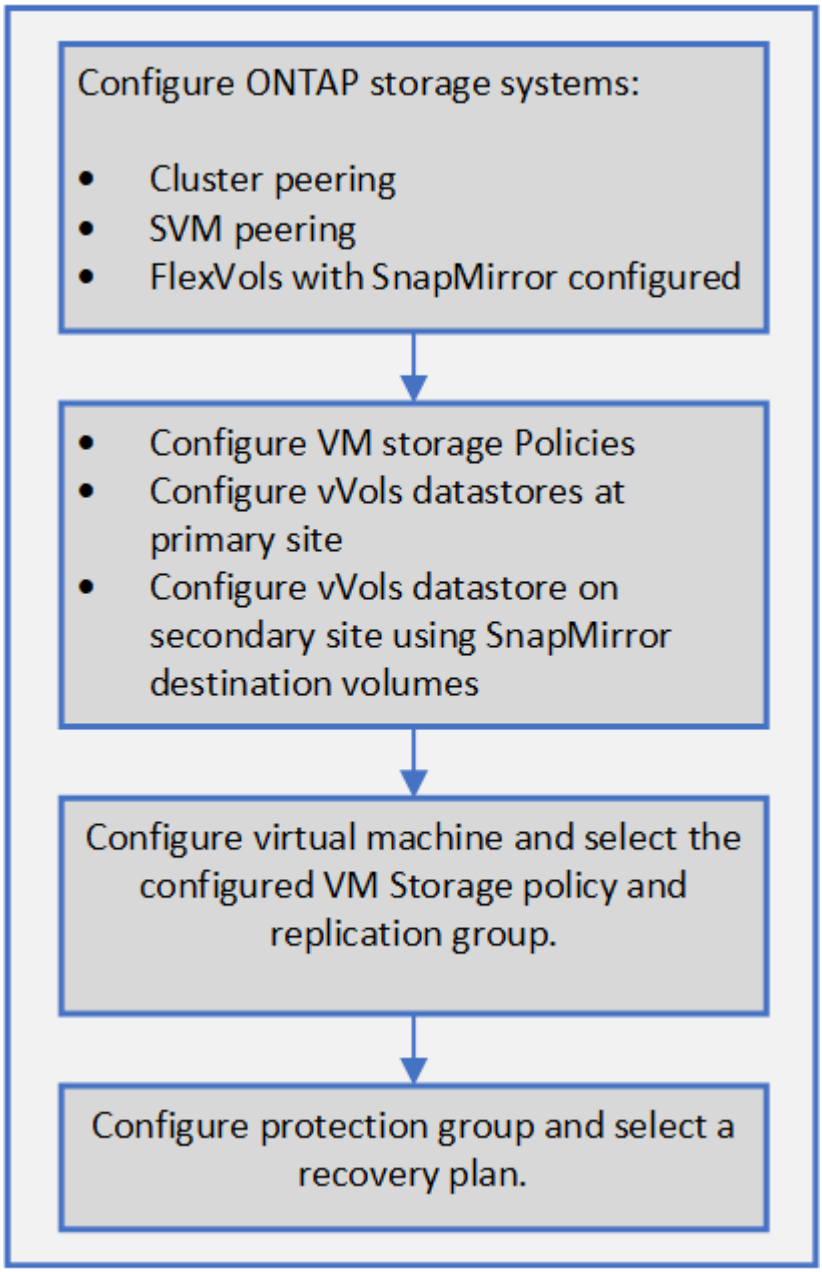
You can configure replication for your vVols datastore using ONTAP tools. The main aim of vVols replication is to protect critical virtual machines during disaster recovery using VMware Site Recovery Manager (SRM).

However, to configure vVols replication for ONTAP tools, VASA Provider capability and vVols replication must be enabled. VASA Provider is enabled by default in ONTAP tools. The Array Based Replication is performed at the FlexVol level. Each vVols datastore is mapped to a storage container that consists of one or more FlexVol volumes. The FlexVol volumes should be pre-configured with SnapMirror from ONTAP.

You should not configure a mix of protected and unprotected virtual machines in a single vVols datastore. A reprotect operation after failover will cause unprotected virtual machines to be deleted. Ensure that all virtual machines in a vVols datastore are protected when using replication.

Replication groups are created during vVols datastore create workflow for each FlexVol volume. To use vVols replication, you will need to create VM Storage Policies that include replication status and schedule along with storage capability profile. A Replication group includes virtual machines that are replicated as part of disaster recovery to the target site. You can configure replication groups with protection groups and recovery plans using SRM console, for DR workflows.

If you are using disaster recovery for vVols datastore, then you do not need to configure Storage Replication Adapter (SRA) separately as VASA Provider capability is enhanced to have vVols replication.



Protect unprotected virtual machines

You can configure protection for your existing unprotected virtual machines that were created using VM storage Policy with replication disabled. To provide protection, you should change the VM storage policy and assign a replication group.

About this task

If SVM is having both IPv4 and IPv6 LIFs, then you should disable IPv6 LIFs and later perform disaster recovery workflows.

Steps

1. Click the required virtual machine and verify that it is configured with default VM storage policy.
2. Right-click the selected virtual machine, and click **VM Policies** > **Edit VM Storage Policies**.
3. Select a VM Storage policy that has replication enabled from the **VM storage policy** drop-down.
4. Select a replication group from the **Replication group** drop-down, and then click **OK**.
5. Verify the Summary of the virtual machine to confirm that the virtual machine is protected.

- This release of ONTAP tools does not support hot clone of protected virtual machines. You should power off the virtual machine and then perform the clone operation.
- If a datastore does not appear in ONTAP tools after a Reprotect operation, then you should run a storage system discovery or wait for the next scheduled discovery operation.

Configure protected and recovery sites

Configure VM Storage Policies

You should configure VM storage policies to manage virtual machines that are configured on vVols datastore and to enable services like replication for the virtual disks. For the traditional datastores, it is optional to use these VM storage policies.

About this task

The vSphere web client provides default storage policies. But you can create policies and assign them to the virtual machines.

Steps

1. On the vSphere Client page, click **Menu** > **Policies and Profiles**.
2. Click **VM Storage Policies** > **Create VM Storage Policy**.
3. In the Create VM Storage Policy page, provide the following details:
   a. Enter a name and description for the VM Storage Policy.
   b. Select **Enable rules for "NetApp clustered Data ONTAP.VP.vvol" storage**.
   c. Select the required storage capability profile in the Placement tab.
   d. Select the **Custom** option to enable Replication.
   e. Click **ADD RULE** to select **Asynchronous** replication and required SnapMirror Schedule, and then click **NEXT**.
   f. Verify the compatible datastores listed, and then click **NEXT** in the Storage compatibility tab.

      For vVols datastores having data protection FlexVol volumes, compatible datastores check is not performed.
4. Review your VM Storage Policy selection in the **Review and finish** tab, and then click **Finish**.

Configure protection groups

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

What you will need

You should ensure that both the source and target sites are configured for the following:

- Same version of SRM installed
- vVols datastore configured with replication enabled and datastore mounted
- Similar storage capability profiles
- Similar VM Storage Policies with replication capability that must be mapped in SRM
- Virtual machines
- Paired protected and recovery sites
- Source and destination datastores should be mounted on respective sites

Steps

1. Log in to your vCenter Server, and then click **Site Recovery** > **Protection Groups**.
2. In the **Protection Groups** pane, click **New**.
3. Specify a name and description for the protection group, direction, and then click **NEXT**.
4. In the **Type** field, select one of the following:

For…	Type field option…
Traditional datastore	Datastore groups (array-based replication)
vVols datastore	Virtual Volumes (vVol replication)

   The fault domain is nothing but SVMs with replication enabled. The SVMs that have only peering implemented and with no issues are displayed.

5. In the Replication groups tab, select either the enabled array pair or the replication groups that have the virtual machine you configured, and then click **NEXT**.

   All of the virtual machines on the replication group are added to the protection group.

6. Select either the existing recovery plan or create a new plan by clicking **Add to new recovery plan**.
7. In the Ready to complete tab, review the details of the protection group that you created, and then click **Finish**.

Pair protected and recovery sites

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

What you will need

- 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.

About this task

SnapMirror fan-out configurations are those where a source volume is replicated to two different destinations. These create a problem during recovery when SRM needs to recover the virtual machine from destination.

Storage Replication Adapter (SRA) does not support fan-out SnapMirror configurations.

Steps

1. Double-click **Site Recovery** on the vSphere Client home page, 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 section, 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.

Configure protected and recovery site resources

Configure network mappings

You must configure your resource mappings like VM networks, ESXi hosts, and folders on both sites to enable the mapping of each resource from the protected site to the appropriate resource at the recovery site.

You must complete the following resource configurations:

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

What you will need

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.

Configure folder mappings

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

What you will need

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.

Configure 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.

What you will need

You must have connected the protected and recovery sites.

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.

Map storage policies

You should map the storage policies on the protected site to the storage policies on the recovery site for your recovery plan to place the recovered virtual machines on the appropriate datastores based on your mappings. After the virtual machine is recovered on recovery site, mapped VM Storage Policy will be assigned to virtual machine.

Steps

1. On the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. In the Site Pair tab, click **Configure** > **Storage Policy Mappings**.
3. Select the required site, and then click **New** to create a new mapping.
4. Select the option **Automatically prepare mappings for storage policies with matching names**, and then click **NEXT**.

   SRM will select storage policies on the protected site for which a storage policy with the same name exists on the recovery site. You can also select the manual mapping option to select multiple storage policies.

5. Click **Add mappings**, and the click **NEXT**.

6. In the **Reverse mapping** section, select the required check boxes for mapping, and then click **NEXT**.
7. In the **Ready to complete** section, review your selections and click **FINISH**.

Configure 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.

What you will need

- 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**.

   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.

Configure SRA using array manager

You can configure Storage Replication Adapter (SRA) by using the Array Manager wizard of Site Recovery Manager (SRM) to enable interactions between SRM and storage virtual machines (SVMs).

What you will need

- You must have paired the protected sites and recovery sites in SRM.
- You must have configured your storage before configuring the array manager.
- You must have configured and replicated the SnapMirror relationships between the protected sites and recovery sites.
- You must have enabled the SVM management LIFs to enable multitenancy.

SRA supports cluster-level management and SVM-level management. If you add storage at a cluster level, then you can discover and perform operations on all of the SVMs in the cluster. If you add storage at an SVM level, then you can manage only that specific SVM.

VMware does not support NFS4.1 protocol for SRM.

Steps

1. In SRM, click **Array Managers**, and then click **Add Array Manager**.
2. Enter the following information to describe the array in SRM:
   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, you should enter the cluster management LIF.
      - If you are connecting directly to an SVM, you should enter the IP address of the SVM management LIF.

      When configuring the array manager, you must use the same connection and credentials for the storage system that was used to add the storage system in Virtual Storage Console's Storage Systems menu. For example, if the array manager configuration is SVM scoped, then the storage under VSC must be added at SVM level.

   d. If you are connecting to a cluster, enter the name of the SVM in the **SVM name** field.

      You can also leave this field blank.

   e. Enter the volumes to be discovered in the **Volume include list** field.

      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.

      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 field and dst_vol1 in the recovery site field.

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

      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.

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

   g. **(Optional)** Enter the user name of the cluster-level account or SVM-level account in the **Username** field.
   h. Enter the password of the user account in the **Password** field.
3. Click **Next**.
4. Verify that the array is discovered and displayed at the bottom of the Add Array Manager window.
5. Click **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.

Verify replicated storage systems

You must verify that the protected site and recovery site are successfully paired after configuring Storage Replication Adapter (SRA). The replicated storage system must be discoverable by both the protected site and the recovery site.

What you will need

- You must have configured your storage system.
- You must have paired the protected site and recovery site by using the SRM array manager.
- You must have enabled FlexClone license and SnapMirror license before performing the test failover operation and failover operation for SRA.

Steps

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

   The storage systems must be discovered at the protected site and recovery site with the Status as “Enabled”.