Protect datastores and virtual machines

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

Table of Contents

Protect datastores and virtual machines

Enable SRA to protect datastores

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

What you will need

- You should have set up your vCenter Server instance and configured ESXi host.
- You should have deployed ONTAP tools.
- You should have downloaded the SRA Adapter `.tar.gz` file from the NetApp Support Site.

Steps

1. Log in to SRM appliance management interface using the URL: `https://:<srm_ip>:5480`, and then go to Storage Replication Adapters in VMware SRM appliance management interface.
2. Select **New Adapter**.
3. Upload the *.tar.gz* installer for the SRA plug-in to SRM.
4. Rescan the adapters to verify that the details are updated on the SRM Storage Replication Adapters page.

Configure storage system for disaster recovery

Configure SRA for SAN and NAS environments

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

Configure SRA for SAN environment

What you will need

You should have the following programs installed 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 iSCSI connectivity to the storage virtual machine (SVM). The secondary site ESXi hosts should have access to the secondary site storage, similarly the primary site ESXi hosts should have access to the primary site storage.

   You can do this either by verifying that the ESXi hosts have local LUNs connected on the SVM or the `iscsi show initiators` command on the SVMs. Check the LUN access for the mapped LUNs in the ESXi host to verify iSCSI connectivity.

Configure SRA for NAS environment

What you will need

You should have the following programs installed 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.

Configure SRA for highly scaled environment

You should 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

When you hit a timeout, increase the values of `storage.commandTimeout` and `storage.maxConcurrentCommandCnt` to a higher value.

> 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.

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 ONTAP tools for VMware vSphere credentials (IP address) in the SRM appliance to enable communication between SRM Appliance and SRA.

What you will need

You should have downloaded the *tar.gz* file from NetApp Support Site.

About this task

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

Steps

1. On the SRM appliance screen, click **Storage Replication Adapter** > **New Adapter**.
2. Upload the *.tar.gz* file to SRM.
3. Log in using administrator account to the SRM appliance using putty.

4. Switch to the root user using the command: `su root`
5. Run command `cd /var/log/vmware/srm` to navigate to the log directory.
6. At the log location enter the command to get the docker ID used by SRA: `docker ps -l`
7. To log in to the container ID, enter command: `docker exec -it -u srm <container id> sh`
8. Configure SRM with ONTAP tools for VMware vSphere IP address and password using the command: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>'`

   You need to provide the password value within single quotes to ensure that the Perl script does not read the special characters in the password as a delimiter of the input.

9. Rescan the adapters to verify that the details are updated on the SRM Storage Replication Adapters page.

   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 the SRM appliance

Steps

1. Run the following commands to delete the SRM machine folder cached ONTAP tools username password:
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd /conf`
   e. `rm -rf *`
2. Run the perl command to configure SRA with the new credentials:
   a. `cd ..`
   b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` You need to have a single quote around the password value.

      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.

Configure protected and recovery sites

Configure protection groups

You should 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
- Virtual machines
- Paired protected and recovery sites
- Source and destination datastores should be mounted on respective sites

Steps

1. Log in to 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 the **Type field option…** as Datastore groups (array-based replication) for NFS and VMFS datastore. The fault domain is nothing but SVMs with replication enabled. The SVMs that have only peering implemented and have 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 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 should pair the protected and recovery sites created using your vSphere Client to enable Storage Replication Adapter (SRA) to discover the storage systems.

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

What you will need

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

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 should 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 should complete the following resource configurations:

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

What you will need

You should have connected the protected and recovery sites.

Steps

1. Log in to 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 **New** 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 used earlier to create reverse mapping, 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 should map your folders on the protected site and recovery site to enable communication between them.

What you will need

You should have connected the protected and recovery sites.

Steps

1. Log in to 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. Select **Folder** 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 used earlier to create reverse mapping, 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 should 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 should 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 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 **New** 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 used earlier to create reverse mapping, 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.

Configure placeholder datastores

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

Steps

1. Log in to 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 **New** 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 should have paired the protected sites and recovery sites in SRM.
- You should have configured your onboarded storage before configuring the array manager.
- You should have configured and replicated the SnapMirror relationships between the protected sites and recovery sites.
- You should 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 the SVMs in the cluster. If you add storage at an SVM level, then you can manage only that specific SVM.

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 should use the same connection (IP address) for the storage system that was used to onboard the storage system in ONTAP tools. For example, if the array manager configuration is SVM scoped, then the storage under ONTAP tools for VMware vSphere should 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.

      For example, if you want to discover volume src_vol1 that is in a SnapMirror relationship with volume dst_vol1, you should 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.

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

3. Click **Next**.
4. Verify that the array is discovered and displayed at the bottom of the Add Array Manager window and 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 should verify that the protected site and recovery site are successfully paired after configuring Storage Replication Adapter (SRA). The replicated storage system should be discoverable by both the protected site and the recovery site.

What you will need

- You should have configured your storage system.
- You should have paired the protected site and recovery site by using the SRM array manager.
- You should 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 ArrayPair and verify the corresponding details.

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

Copyright information

Trademark information