Configure protected and recovery sites

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-tools-vmware-vsphere-10/protect/configure-protection-groups.html on June 21, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Configure protected and recovery sites . . . 1
Configure protection groups . . . 1
Pair protected and recovery sites . . . 1
Configure protected and recovery site resources . . . 2
Verify replicated storage systems . . . 6

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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.