Install and set up

ONTAP 9

NetApp
August 02, 2023

Table of Contents

Install and set up

Configure the ONTAP Mediator and clusters for SnapMirror Business Continuity

SnapMirror Business Continuity (SM-BC) utilizes peered clusters to ensure your data is available in the event of a failover scenario. The ONTAP Mediator is a key resource ensuring business continuity, monitoring the health of each cluster. To configure SM-BC, you must first install the ONTAP Mediator and ensure you primary and secondary clusters are configured properly.

Once you have installed the ONTAP Mediator and configured your clusters, you must Initialize the ONTAP mediator for SM-BC the ONTAP Mediator for use with SM-BC. You must then Create, initialize, and map the consistency group for SM-BC

ONTAP Mediator

The ONTAP Mediator establishes a quorum for the ONTAP clusters in an SM-BC relationship. It coordinates automated failover when a failure is detected, determining which cluster acts as the primary and ensuring data is served to and from the correct destination.

Prerequisites for the ONTAP Mediator

- The ONTAP Mediator includes its own set of prerequisites. You must meet these prerequisites before installing the mediator.

  For more information, see Prepare to install the ONTAP Mediator service.

- By default, the ONTAP Mediator provides service through TCP port 31784. You should make sure that port 31784 is open and available between the ONTAP clusters and the mediator.

Install the ONTAP Mediator and confirm cluster configuration

Proceed through each of the following steps. For each step, you should confirm that the specific configuration has been performed. Use the link included after each step to get more information as needed.

Steps

1. Install the ONTAP Mediator service before you ensure that your source and destination clusters are configured properly.

   Prepare to install or upgrade the ONTAP Mediator service

2. Confirm that a cluster peering relationship exists between the clusters.

   The default IPspace is required by SM-BC for cluster peer relationships. A custom IPspace is not supported.

   Configure peer relationships

3. Confirm that the Storage VMs are created on each cluster.

Creating an SVM

4. Confirm that a peer relationship exists between the Storage VMs on each cluster.

   Creating an SVM peering relationship

5. Confirm that the volumes exist for your LUNs.

   Creating a volume

6. Confirm that at least one SAN LIF is created on each node in the cluster.

   Considerations for LIFs in a cluster SAN environment

   Creating a LIF

7. Confirm that the necessary LUNs are created and mapped to an igroup, which is used to map LUNs to the initiator on the application host.

   Create LUNs and map igroups

8. Rescan the application host to discover any new LUNs.

Initialize the ONTAP mediator for SM-BC

Once you have installed the ONTAP Mediator and confirmed you cluster configuration, you must initialize the ONTAP Mediator for cluster monitoring. You can initialize the ONTAP Mediator using System Manager or the ONTAP CLI.

System Manager

With System Manager, you can configure the ONTAP Mediator server for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

Steps

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Select **Add**, and enter the following ONTAP Mediator server information:
   - IPv4 address
   - Username
   - Password
   - Certificate

CLI

You can initialize the ONTAP Mediator from either the primary or secondary cluster using the ONTAP CLI. When you issue the `mediator add` command on one cluster, the ONTAP Mediator is automatically added on the other cluster.

Steps

1. Initialize Mediator on one of the clusters:

   ```
   snapmirror mediator add -mediator-address IP_Address -peer-cluster
   cluster_name -username user_name
   ```

   Example

   ```
   cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
   -peer-cluster cluster2 -username mediatoradmin
   Notice: Enter the mediator password.

   Enter the password: ******
   Enter the password again: ******
   ```

2. Check the status of the Mediator configuration:

   ```
   snapmirror mediator show
   ```

   ```
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   192.168.10.1     cluster-2        connected         true
   ```

   `Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with the mediator; a status of `true` indicates successful synchronization.

Establish protection with SnapMirror Business Continuity

Configuring protection using SnapMirror Business Continuity involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group.

Before you begin

- You must have a SnapMirror Synchronous license.
- You must be a cluster or storage VM administrator.
- All constituent volumes in a consistency group must be in a single storage VM (SVM).
  - LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.
- You cannot establish SM-BC consistency group relationships across ASA clusters and non-ASA clusters.
- The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.
- The name of the consistency group must be unique.
- The volumes on the secondary (destination) cluster must be type DP.
- The primary and the secondary SVMs must be in a peered relationship.

Steps

You can configure a consistency group using the ONTAP CLI or System Manager.

Beginning in ONTAP 9.10.1, ONTAP offers a consistency group endpoint and menu in System Manager, offering additional management utilities. If you are using ONTAP 9.10.1 or later, see Configure a consistency group then configure protection to create an SM-BC relationship.

System Manager

1. On the primary cluster, navigate to **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select the LUNs you want to protect and add them to a protection group.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

CLI

1. Create a consistency group relationship from the destination cluster.
   `destination::> snapmirror create -source-path *source-path* -destination-path *destination-path* -cg-item -mappings *volume-paths* -policy *policy-name*

   You can map up to 12 constituent volumes using the `cg-item-mappings` parameter on the `snapmirror create` command.

   The following example creates two consistency groups: `cg_src_ on the source with `vol1` and `vol2` and a mirrored destination consistency group, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. From the destination cluster, initialize the consistency group.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

3. Confirm that the initialization operation completed successfully. The status should be `InSync`.

   ```
   snapmirror show
   ```

4. On each cluster, create an igroup so you can map LUNs to the initiator on the application host.
   `lun igroup create -igroup *name* -protocol *fcp|iscsi* -ostype *os* -initiator *initiator_name*`
5. On each cluster, map LUNs to the igroup:

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Verify the LUN mapping completed successfully with the `lun map` command. Then, you can discover the new LUNs on the application host.

Copyright information

Trademark information