Perform disaster recovery

SnapManager for Hyper-V

NetApp
June 18, 2025

Table of Contents

Perform disaster recovery

The disaster recovery feature ensures that if a disaster or other circumstance makes critical protected data at your primary storage sites unavailable, that you can provide access to the backed up copy of that data through your secondary storage sites. Disaster recovery can only be performed using the PowerShell interface.

Configure SnapManager for Hyper-V for failover

To fully enable your SnapManager for Hyper-V implementation for disaster recovery, you must ensure that the primary and secondary hosts have the same configuration and know that you can perform disaster recovery using only PowerShell.

The following types of setups support disaster recovery:

- Stand-alone primary host and stand-alone secondary Hyper-V host
- Clustered primary and secondary Hyper-V hosts
- Cluster shared volumes (CSV) on the primary and secondary Hyper-V hosts

For example, a cluster virtual machine (VM) on a primary host must be recovered as a cluster VM, a dedicated (stand-alone) VM must be recovered as a dedicated VM, and a CSV VM must be recovered as a CSV VM.

LUNs on a secondary host should be connected in the same way as their counterparts on the primary host. That is, the LUN type (dedicated, shared, or CSV) and the drive letter, mount point, or CSV reparse point should be the same on primary and secondary hosts. With SAN restore operations to an alternate path location, a different drive letter can be specified for the LUN restore operation on a secondary location.

Drive letters or CSVs and volume mount points are supported.

The following example shows a basic disaster recovery setup:

- Site A (primary) contains storage systems and a stand-alone Hyper-V host system or Hyper-V host cluster.

  VMs running on these hosts reside on Data ONTAP storage.

- Site B (secondary) contains storage systems and a Hyper-V host or cluster (same as that of primary).
- SnapDrive for Windows and SnapManager for Hyper-V are installed on both sites A and B.
- The SnapMirror relationship is initialized from site A to site B.
- On site A, a Hyper-V host or cluster added to SnapManager for Hyper-V and the VMs is backed up using SnapManager for Hyper-V.

  The policy to update SnapMirror after the backup is checked. After each backup, the secondary site is updated with new Snapshot copies of the VMs and SnapInfo copies.

Recover and restore from a disaster recovery failover

To recover from a disaster, SnapManager for Hyper-V must first fail over to a secondary storage system. Failing over involves a series of manual steps in PowerShell.

About this task

Most backups can be restored to an alternate host for both NAS and SAN; however, Windows Server 2008 R2 crash-consistent backups cannot be restored to an alternate host.

Steps

1. If you are running Data ONTAP 8.1.x, on the secondary site, enter the storage virtual machine (SVM) information to the Transport Protocol Setting (TPS) in the SnapDrive for Windows MMC.
2. From the secondary storage system, connect to all of the LUNs.

   If the secondary storage system is clustered, go to the node where the cluster group, which is the available storage group owner node in the destination cluster, is online and then connect to all of the LUNs from that node in the cluster. Refer to the SnapDrive for Windows documentation for information about mapping LUNs.

3. Depending on your configuration, take one of the following actions:

If the primary storage system is…	Then…
A stand-alone host (SAN)	Connect to all of the mount points and LUNs of the same type on the primary storage system.
A clustered host (SAN)	From the node where the cluster group is online, connect to all of the mount points and LUNs in the cluster.
Data ONTAP 8.1.x configured with a single LUN hosting VMs on a source FlexVol volume (SAN)	For SnapMirror updates to succeed, you must create a second, smaller LUN (10 MB to 100 MB) on the source FlexVol volume before initiating a backup. From the node where the cluster group is online, connect to all of the mount points and LUNs in the cluster.
A stand-alone or clustered host (NAS)	Unmount the Data Protection (DP) volume, mount the DP volume as rewriteable, verify that the volume has RWX permissions, and then create CIFS shares for the different volumes.

4. Reconfigure SnapInfo based on your environment:

If your configuration is…	Then…
SAN	Restore the SnapInfo LUN from its last Snapshot copy.
NAS	Mount the SnapInfo directory.

   For NAS, if an access is denied error occurs, or if you cannot browse to the exposed SMB share location, you might need to reset the access control list on the share.

This is typical when using the System Center Virtual Machine Manager (SCVMM) Console and Data ONTAP SMI-S Agent.

5. Add the secondary storage system or cluster in the SnapManager for Hyper-V MMC, and then configure it with the SnapInfo path.
6. Enter the following cmdlets:
   a. Enter `Get-VMsFromBackup` to retrieve the list of VMs present in the backup metadata.
   b. Enter `Get-Backup` to get the backup copies for each VM.
7. To restore, use `Restore-Backup` with the VM GUID and the backup copy with the following parameters:

To restore from…	Enter this command…
An alternate host	`Restore-Backup -Server Secondary_host_system_or_cluster_name -DisableVerifySnapshot -RestoreToAlternateHost`
A listed backup	`Restore-Backup -Server -VirtualMachinePath -SnapShotFilePath @VHD`

   For `@VHD`, a VM might have multiple VHDs; make sure that you enter both a source and a destination path pair specified for each VHD.

8. If the secondary host system is a cluster, complete the following steps:
   a. Ensure that the LUNs on which the VMs reside are online on the cluster node that owns the cluster group.
   b. Use the failover PowerShell cmdlets to make the VMs highly available.

Failover examples

The following example shows a two-cluster setup in which smhv-cluster-01 is the primary site and hv-19-cluster is the secondary site:

```
PS C:\> Get-VMsFromBackup -Server hv-19-cluster

winxp-x64c-135                593ABA72-B323-4AF7-9AC6-9514F64C0178
csv1-xp-3                     59B85C68-BAFA-4A49-8E85-A201045843F7
vm-w2k8r2sp1                  5A248757-872B-4FE7-8282-91C8E9D45CF9
um10_11_dr                    5AC1B2A8-6603-4F90-98F5-4F2F435AB0C2
winxp-x64c-30                 5B47D3CF-5D96-495D-9BAB-FB394392CF31
winxp-x64c-126                5B57EED1-B4F1-45A3-A649-24C6947CB79C
winxp-x64c-118                5B5D417B-70DC-427C-94BB-97FF81C5B92B
winxp-x64c-122                5BEE26B8-BE57-4879-A28E-9250A6A5EEFC
csv4-w2k3-19                  5D0613E5-B193-4293-8AAD-F8B94A5D851F

PS C:\> Get-Backup -Server hv-19-cluster -ResourceName um10_11_dr

BackupName    : smhv-ccb-ds_04-10-2012_10.37.58
RetentionType : hourly
DatasetName   : smhv-ccb-ds
BackupId      : smhv-ccb-ds_04-10-2012_10.37.58
BackupTime    : 4/10/2012 10:37:58 AM
BackupType    : Application consistent
BackedupVMs   : {um10_11_dr}

PS C:\> Restore-Backup -Server hv-19-cluster -ResourceName
um10_11_dr -BackupName smhv-ccb-ds_04-10-2012_10.37.58
-DisableVerifySnapshot -RestoreToAlternateHost
```

The following example shows a SAN restore operation to an alternate path for which N:\ is the destination and I:\ is the source LUN path:

```
PS C:\> Restore-Backup -Resourcename dr-san-ded1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName san_dr_09-11-
2013_10.57.31 -Verbose
-VirtualMachinePath "N:\dr-san-ded1" -SnapshotFilePath "N:\dr-san-ded1"
-VHDs @(@{"SourceFilePath" = "I:\dr-san-ded1\Virtual Hard Disks\dr-san-
ded1.vhdx"; "DestinationFilePath" = "N:\dr-san-ded1\Virtual Hard Disks\dr-
san-ded1"})
```

The following example shows a NAS restore operation to an alternate path for which \\172.17.162.174\ is the source SMB share path and \\172.17.175.82\ is the destination SMB share path:

```
PS C:\> Restore-Backup -Resourcename vm_claba87_cifs1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName ag-DR_09-09-
2013_16.59.16 -Verbose
-VirtualMachinePath "\\172.17.175.82\vol_new_dest_share\ag-vm1"
-SnapshotFilePath "\\172.17.175.82\vol_new_dest_share\ag-vm1" -VHDs
@(@{"SourceFilePath" = "\\172.17.162.174\vol_test_src_share\ag-vm1\Virtual
Hard Disks\ag-vm1.vhdx"; "DestinationFilePath" =
"\\172.17.175.82\vol_new_dest_share\ag-vm1\Virtual Hard Disks\ag-
vm1.vhdx"})
```

Related information

Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode

NetApp Documentation: SnapDrive for Windows (current releases)

SMB/CIFS Reference

Reconfigure storage systems after a disaster recovery failback

After failing over to a secondary storage system, SnapManager for Hyper-V completes disaster recovery by failing back to the original primary storage system. Failing back restores primary storage function to the original primary storage site after its storage systems are reenabled or replaced.

Steps

1. Depending on the condition of the primary storage system, take one of the following actions:

If the primary storage system is…	Then…
Recoverable	Move the data from the secondary host back to the primary storage system.
Completely destroyed	Provision a new storage system.

2. Manage the SnapMirror relationship:
   a. Initialize the SnapMirror relationship from the secondary storage system to the primary storage system to recover the data.
   b. Resynchronize the existing SnapMirror relationship from the secondary storage system to the primary storage system.
   c. Using SnapDrive on the secondary storage system, initiate a SnapMirror update for each of the LUNs or SMB shares on the secondary storage system.
3. Depending on your configuration, take one of the following actions:

If the primary storage system is…	Then…
A stand-alone host (SAN)	Connect to all the mount points and LUNs on the primary storage system of the same type.
A clustered host (SAN)	From the node where the cluster group is online, connect to all the mount points and LUNs in the cluster.
Data ONTAP 8.1.x configured with a single LUN hosting VMs on a source FlexVol volume (SAN)	For SnapMirror updates to succeed, you must create a second, smaller LUN (10 MB to 100 MB) on the source FlexVol volume before initiating a backup job. From the node where the cluster group is online, connect to all the mount points and LUNs in the cluster.
A stand-alone or clustered host (NAS)	Unmount the Data Protection (DP) volume, mount the DP volume as rewriteable, verify that the volume has RWX permissions, and then create CIFS shares for the different volumes.

4. Reconfigure SnapInfo based on your environment:

If your configuration is…	Then…
SAN	Restore the SnapInfo LUN from its last Snapshot copy.
NAS	Mount the SnapInfo directory.

   For NAS, if an access is denied error occurs, or if you cannot browse to the exposed SMB share location, you might need to reset the ACL on the share.

5. Add the primary host or cluster in SnapManager for Hyper-V MMC and configure it with the SnapInfo path.
6. Enter the following cmdlets:
   a. Retrieve the list of VMs present in the backup metadata by using the Get-VMsFromBackup cmdlet.
   b. Get the backup copies for each VM by using the Get-Backup cmdlet to get the backup copies for each VM.
7. To restore, use `Restore-Backup` with the VM GUID and the backup copy with the following parameters:

To restore from…	Enter this command…
An alternate host	`Restore-Backup -Server Secondary_host_system_or_cluster_name -DisableVerifySnapshot -RestoreToAlternateHost`

To restore from…	Enter this command…
A listed backup copy	`Restore-Backup -Server -VirtualMachinePath -SnapShotFilePath @VHD`

For `@VHD`, a VM might have multiple VHDs; you must enter both a source and a destination path pair specified for each VHD.

8. If the secondary host system is a cluster, complete the following steps:

   a. Ensure that the LUNs on which the VMs reside are online on the cluster node that owns the cluster group.

   b. Use the failover PowerShell cmdlets to make the VMs highly available.

   For NAS, after the VMs are exposed as SMB shares from one cluster node, the VMs are accessible to all hosts configured to use the storage system cluster.

Failback examples

The following example shows a two-cluster setup in which smhv-cluster-01 is the primary site and hv-19-cluster is the secondary site:

```
PS C:\> Get-VMsFromBackup -Server smhv-cluster-01

winxp-x64c-135                593ABA72-B323-4AF7-9AC6-9514F64C0178
csv1-xp-3                     59B85C68-BAFA-4A49-8E85-A201045843F7
vm-w2k8r2sp1                  5A248757-872B-4FE7-8282-91C8E9D45CF9
um10_11_dr                    5AC1B2A8-6603-4F90-98F5-4F2F435AB0C2
winxp-x64c-30                 5B47D3CF-5D96-495D-9BAB-FB394392CF31
winxp-x64c-126                5B57EED1-B4F1-45A3-A649-24C6947CB79C
winxp-x64c-118                5B5D417B-70DC-427C-94BB-97FF81C5B92B
winxp-x64c-122                5BEE26B8-BE57-4879-A28E-9250A6A5EEFC
csv4-w2k3-19                  5D0613E5-B193-4293-8AAD-F8B94A5D851F

PS C:\> Get-Backup -Server smhv-cluster-01 -ResourceName
um10_11_dr

BackupName    : smhv-ccb-ds_04-10-2012_10.37.58
RetentionType : hourly
DatasetName   : smhv-ccb-ds
BackupId      : smhv-ccb-ds_04-10-2012_10.37.58
BackupTime    : 4/10/2012 10:37:58 AM
BackupType    : Application consistent
BackedupVMs   : {um10_11_dr}

PS C:\> Restore-Backup -Server smhv-cluster-01 -ResourceName
um10_11_dr -BackupName smhv-ccb-ds_04-10-2012_10.37.58
-DisableVerifySnapshot -RestoreToAlternateHost
```

The following example shows a SAN restore operation to an alternate path for which N:\ is the destination and I:\ is the source LUN path:

```
PS C:\> Restore-Backup -Resourcename dr-san-ded1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName san_dr_09-11-
2013_10.57.31 -Verbose
-VirtualMachinePath "N:\dr-san-ded1" -SnapshotFilePath "N:\dr-san-ded1"
-VHDs @(@{"SourceFilePath" = "I:\dr-san-ded1\Virtual Hard Disks\dr-san-
ded1.vhdx"; "DestinationFilePath" = "N:\dr-san-ded1\Virtual Hard Disks\dr-
san-ded1"})
```

The following example shows a NAS restore operation to an alternate path for which \\172.17.162.174\ is the source SMB share path and \\172.17.175.82\ is the destination SMB share path:

```
PS C:\> Restore-Backup -Resourcename vm_claba87_cifs1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName ag-DR_09-09-
2013_16.59.16 -Verbose
-VirtualMachinePath "\\172.17.175.82\vol_new_dest_share\ag-vm1"
-SnapshotFilePath "\\172.17.175.82\vol_new_dest_share\ag-vm1" -VHDs
@(@{"SourceFilePath" = "\\172.17.162.174\vol_test_src_share\ag-vm1\Virtual
Hard Disks\ag-vm1.vhdx"; "DestinationFilePath" =
"\\172.17.175.82\vol_new_dest_share\ag-vm1\Virtual Hard Disks\ag-
vm1.vhdx"})
```

Related information

Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode

SMB/CIFS Reference

Restore the original configuration for standalone hosts

After the VMs are backed up on the primary storage system, you can return to the original configuration using a SnapMirror relationship that is established from the primary storage system to the secondary storage system.

Steps

1. Shut down the VMs running on the secondary storage system.
2. Delete the VMs running on the secondary storage system.
3. Disconnect the SnapInfo disk and the disks containing VMs using SnapDrive.
4. Resynchronize the SnapMirror relationship from the primary storage system to the secondary storage system.

Restore the original configuration for clustered hosts

After the VMs are backed up on the primary storage system, you can return to the original configuration using a SnapMirror relationship which is established from the primary storage system to the secondary storage system.

Steps

1. Offline the virtual machine resource and virtual machine configuration resource for all the VMs.
2. Delete these resources from the cluster.
3. Delete all the VMs from Hyper-V Manager.
4. Disconnect all the disks by using SnapDrive.
5. Resynchronize the SnapMirror relationship from the primary storage system to the secondary storage system.

Copyright information

Trademark information