Protect Hyper-V workloads

NetApp Backup and Recovery

NetApp
February 11, 2026

Table of Contents

Protect Hyper-V workloads

Protect Hyper-V workloads overview

Protect your Hyper-V VMs with NetApp Backup and Recovery. NetApp Backup and Recovery provides fast, space-efficient, crash-consistent, and VM-consistent backup and restore operations for both standalone and FCI cluster instances. You can also protect Hyper-V virtual machines provisioned by System Center Virtual Machine Manager (SCVMM) and hosted on a CIFS share.

You can back up Hyper-V workloads to Amazon Web Services S3 or StorageGRID and restore Hyper-V workloads back to an on-premises Hyper-V host.

Use NetApp Backup and Recovery to implement a 3-2-1 protection strategy, where you have 3 copies of your source data on 2 different storage systems along with 1 copy in the cloud. The benefits of the 3-2-1 approach include:

- Multiple data copies protect against internal and external cybersecurity threats.
- Multiple media types ensure failover viability in the case of physical or logical failure of one media type.
- The onsite copy helps you quickly restore data, and you can use the offsite copies if the onsite copy is compromised.

When you add Hyper-V hosts and discover resources, NetApp Backup and Recovery installs the NetApp Hyper-V plug-in and the NetApp SnapCenter Windows FileSystem plug-in on the Hyper-V host to help with managing and protecting virtual machines.

ⓘ To switch to and from NetApp Backup and Recovery UI versions, refer to Switch to the previous NetApp Backup and Recovery UI.

You can use NetApp Backup and Recovery to perform the following tasks related to Hyper-V workloads:

- Discover Hyper-V workloads
- Create and manage protection groups for Hyper-V workloads
- Back up Hyper-V workloads
- Restore Hyper-V workloads

Discover Hyper-V workloads in NetApp Backup and Recovery

NetApp Backup and Recovery must discover Hyper-V virtual machines before you can protect them.

Required Console role
Backup and Recovery super admin. Learn about Backup and recovery roles and privileges. Learn about NetApp Console access roles for all services.

Add a Hyper-V host and discover resources

Add Hyper-V host information and let NetApp Backup and Recovery discover virtual machines. Within each Console agent, select the systems where you want to discover the resources.

> When you add Hyper-V hosts and discover resources, NetApp Backup and Recovery installs the NetApp Hyper-V plug-in and the NetApp SnapCenter Windows FileSystem plug-in on the Hyper-V host to help with managing and protecting virtual machines.

Steps

1. From the NetApp Console menu, select **Protection** > **Backup and recovery**.

   If this is your first time logging in to NetApp Backup and Recovery, you already have a system in the Console, but haven't discovered any resources, the "Welcome to the new NetApp Backup and Recovery" landing page appears and shows an option to **Discover resources**.

2. Select **Discover resources**.
3. Enter the following information:
   a. **Workload type**: Select **Hyper-V**.
   b. If you haven't yet stored credentials for this Hyper-V host, select **Add credentials**.
      i. Select the Console agent to use with this host.
      ii. Enter a name for this credential.
      iii. Enter the user name and password for the account.
      iv. Select **Done**.
   c. **Host registration**: Add a new Hyper-V host by entering the host's FQDN or IP address, credentials, Console agent, and port number. If the FQDN is not resolvable by the Console agent, use the IP address instead. For FCI clusters, enter the FCI cluster management IP address.
4. Select **Discover**.

   > This process might take a few minutes.

Result

After NetApp Backup and Recovery discovers resources, the Inventory page displays the Hyper-V workload in the list of workloads.

Continue to the NetApp Backup and Recovery Dashboard

Steps

1. From the NetApp Console menu, select **Protection** > **Backup and recovery**.
2. Select a workload tile (for example, Microsoft SQL Server).
3. From the Backup and Recovery menu, select **Dashboard**.
4. Review the health of data protection. The number of at risk or protected workloads increases based on the newly discovered, protected, and backed up workloads.

Create and manage protection groups for Hyper-V workloads with NetApp Backup and Recovery

Create protection groups to manage the backup operations for a set of virtual machines. A protection group is a logical grouping of resources such as VMs that you want to protect together.

You can perform the following tasks related to protection groups:

- Create a protection group.
- View protection details.
- Back up a protection group now. See Back up Hyper-V workloads now.
- Delete a protection group.

Create a protection group

Group workloads that you want to protect together into a protection group. Create a protection group to back up and restore workloads together.

Required Console role
Backup and Recovery super admin or Backup and Recovery backup admin role. Learn about NetApp Console access roles for all services.

Steps

1. From the NetApp Backup and Recovery menu, select **Inventory**.
2. Select a workload to view the protection details.
3. Select the Actions icon ••• > **View details**.
4. Select the **Protection groups** menu.
5. Select **Create protection group**.
6. Provide a name for the protection group.
7. Select the VMs that you want to include in the protection group.
8. Select **Next**.
9. Select the **Backup policy** that you want to apply to the protection group.
10. Select **Next**.
11. Review the configuration.
12. Select **Create** to create the protection group.

Edit a protection group

Edit a protection group to change its name or settings. You might want to edit a protection group if the resources in the group have changed.

Steps

1. From the NetApp Backup and Recovery menu, select **Inventory**.
2. Select a workload to view the protection details.

3. Select the Actions icon ••• > **View details**.
4. Select the **Protection groups** tab.
5. Select the protection group that you want to edit.
6. Select the Actions icon ••• > **Edit**.
7. Change any settings for the protection group such as the name or what virtual machines are in the group.
8. Select **Next**.
9. Change the protection policy if needed. When finished, select **Next**.
10. Review the configuration and select **Submit**.

Delete a protection group

Deleting a protection group removes it and all associated backup schedules. You might want to delete a protection group if it is no longer needed.

Steps

1. From the NetApp Backup and Recovery menu, select **Inventory**.
2. Select a workload to view the protection details.
3. Select the Actions icon ••• > **View details**.
4. Select the **Protection groups** tab.
5. Select the protection group that you want to delete.
6. Select the Actions icon ••• > **Delete**.
7. Review the confirmation message about deleting the associated backups and confirm the deletion.

Back up Hyper-V workloads with NetApp Backup and Recovery

Back up Hyper-V VMs from on-premises ONTAP systems to Amazon Web Services, Azure NetApp Files, or StorageGRID to ensure that your data is protected. Backups are automatically generated and stored in an object store in your public or private cloud account.

- To back up workloads on a schedule, create policies that govern the backup and restore operations. See Create policies for instructions.
- Create protection groups to manage the backup and restore operations for a set of resources. See Create and manage protection groups for Hyper-V workloads with NetApp Backup and Recovery for more information.
- Back up workloads now (create an on-demand backup now).

Back up workloads now with an on-demand backup

Use on-demand backup so that your data is protected before making system changes.

Required Console role
Backup and Recovery super admin or Backup and Recovery backup admin role. Learn about NetApp Console access roles for all services.

Steps

1. From the menu, select **Inventory**.
2. Select a workload to view the protection details.
3. Select the Actions icon ••• > **View details**.
4. Select the **Protection Groups**, **Datastores** or **Virtual machines** tab.
5. Select the protection group or virtual machines that you want to back up.
6. Select the Actions icon ••• > **Back up now**.

> The backup uses the same policy that you assigned to the protection group or virtual machine.

7. Select the schedule tier.
8. Select **Back up**.

Restore Hyper-V workloads with NetApp Backup and Recovery

Restore Hyper-V workloads from snapshots, from a workload backup replicated to secondary storage, or from backups stored in object storage using NetApp Backup and Recovery.

Restore from these locations

You can restore workloads from different starting locations:

- Restore from a primary location (local snapshot)
- Restore from a replicated resource on secondary storage
- Restore from an object storage backup

Restore to these points

You can restore data to these points:

- Restore to the original location
- Restore to an alternate location

Restore from object storage considerations

If you select a backup file in object storage, and ransomware protection is active for that backup (if you enabled DataLock and Ransomware Resilience in the backup policy), then you are prompted to run an additional integrity check on the backup file before restoring the data. We recommend that you perform the scan.

> You'll incur extra egress costs from your cloud provider to access the contents of the backup file.

How restoring workloads works

When you restore workloads, the following occurs:

- When you restore a workload from a local backup file, NetApp Backup and Recovery creates a *new* resource using the data from the backup.
- When you restore from a replicated workload, you can restore the workload to the original system or to an on-premises ONTAP system.

From the Restore page (also known as Search & Restore), you can restore a resource, even if you don’t remember the exact name, the location in which it resides, or the date when it was last in good shape. You can search for the snapshot using filters.

Restore workload data from the Restore option (Search & Restore)

Restore Hyper-V workloads using the Restore option. You can search for the snapshot by its name or by using filters.

Required Console role
Backup and Recovery super admin or Backup and Recovery restore admin role. Learn about NetApp Console access roles for all services.

Steps

1. From the NetApp Backup and Recovery menu, select **Restore**.
2. From the drop-down list to the right of the name search field, select **Hyper-V**.
3. Enter the name of the resource you want to restore or filter for the VM name, VM host, or storage pool where the resource that you want to restore is located.

   A list of snapshots appears that match your search criteria.

4. Select the **Restore** button for the snapshot that you want to restore.

   A list of possible restore points appears.

5. Select the restore point that you want to use.
6. Select a snapshot source location.
7. Select **Next** to continue.
8. Choose the restore destination and settings:

Destination selection

Restore to original location

When you restore to the original location, you can view the destination settings by expanding the **Destination settings** section, but you cannot change them.

a. In the **Post-restore options** section, consider the following option:
   - **Start the virtual machine**: Enable this option to boot the new virtual machine after it is restored.

b. Select **Restore**.

Restore to alternate location

a. In the **Destination settings**: section, enter the following information:
   - **Hyper-V FQDN or IP address**: Enter the fully qualified domain name or IP address of the destination Hyper-V host.
   - **Network**: Select the destination network where you want to restore the snapshot.
   - **Virtual machine name**: Enter the name of the VM that you want to restore.
   - **Destination location**: Enter the destination folder or CIFS share that should contain the restored data.

b. In the **Pre restore options** section, consider the following options:
   - **Quick restore**: Enable this option to make the restored VM available immediately. Only the files needed to run the VM are restored from the object store, rather than the entire volume.

c. In the **Post restore options** section, consider the following options:
   - **Start the virtual machine**: Enable this option to boot the new virtual machine after it is restored.

d. Select **Restore**.