Restore VMware workloads

NetApp Backup and Recovery

NetApp
February 11, 2026

Table of Contents

Restore VMware workloads

Restore VMware workloads with NetApp Backup and Recovery

Restore VMware 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**: The VM is restored in the original location, to the same vCenter deployment, ESXi host, and datastore. The VM and all of its data is overwritten.
- **Restore to an alternate location**: You can choose a different vCenter, ESXi host, or datastore as a restore target for the VM. This is useful for managing different copies of the same VM in different locations and states.

Restore from object storage considerations

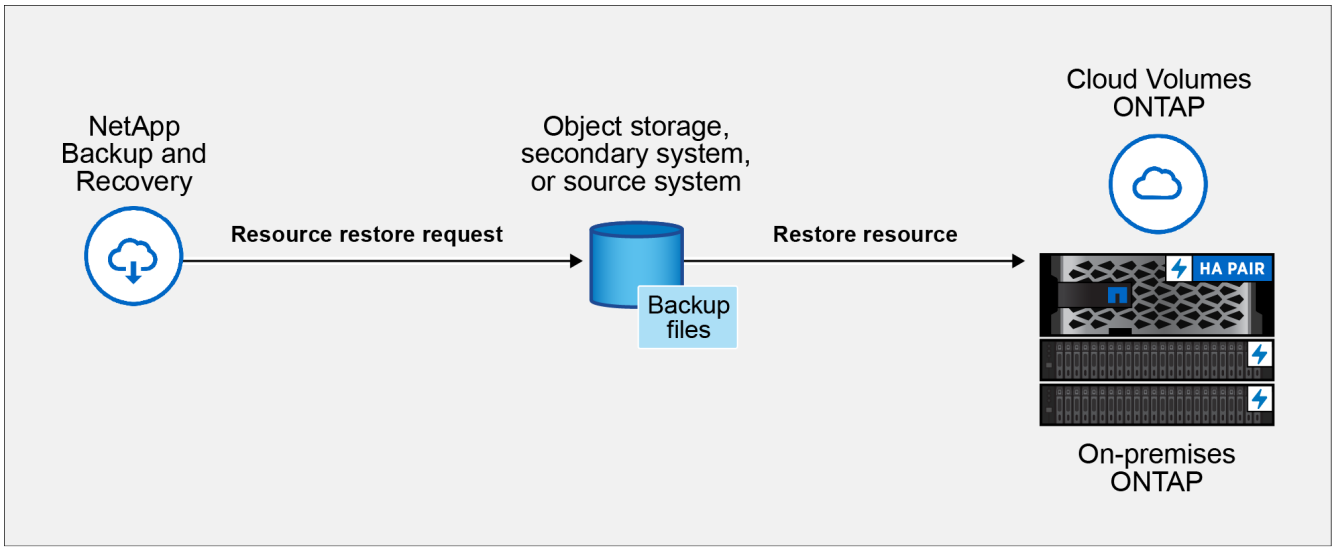
If Ransomware Resilience is enabled for a backup file in object storage, you are asked to run an extra check before restoring. We recommend performing the scan.

You might pay extra fees to your cloud provider to access the backup file.

How restoring workloads works

When you restore workloads, the following occurs:

- When you restore a workload from a local snapshot or remote backup, NetApp Backup and Recovery overwrites the original VM if you restore to the original location, and creates a *new* resource if you restore to an alternate location.
- When you restore from a replicated workload, you can restore the workload to the original on-premises ONTAP system or to a different on-premises ONTAP system.



- When you restore a backup from object storage, you can restore the data to the original system or to an on-premises ONTAP system.

From the Restore page (Search & Restore), you can restore a resource by searching for the snapshot with filters, even if you do not remember its exact name, location, or last known date.

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

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

Required NetApp Console role
Storage viewer, Backup and Recovery super admin, 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 **VMware**.
3. Enter the name of the resource you want to restore or filter for the vCenter, datacenter, or datastore where the resource that you want to restore is located.

   A list of virtual machines appears that match your search criteria.

4. Find the VM that you want to restore from in the list, and select the options menu button for that VM.
5. In the resulting menu, select **Restore virtual machine**.

   A list of snapshots (restore points) created on that virtual machine appears. By default, the latest snapshots are shown for the time frame that you select in the **Time frame** dropdown.

   For each snapshot, any illuminated icons in the **Location** column indicate the storage locations where the snapshot is available (primary, secondary, or object storage).

6. Enable the radio button for the snapshot you want to restore.
7. Select **Next**.

   Snapshot location options appear.

8. Select the restore destination for the snapshot:
    - **Local**: Restores the snapshot from the local location.
    - **Secondary**: Restores the snapshot from a remote storage location.
    - **Object store**: Restores the snapshot from object storage.

      If you choose secondary storage, select the destination location from the drop-down list.
9. Select **Next** to continue.
10. Choose the restore destination and settings:

Destination selection

Restore to original location

When restoring to the original location, you cannot change the destination vCenter, ESXi host, datastore, or name of the VM. The original VM is overwritten with the restore operation.

a. Select the **Original location** pane.

b. Choose from the following options:

- **Pre-restore options** section:
  - **Prescript**: Enable this option to automate additional tasks by running a custom script before the restore operation begins. Enter the full path for the script that should be run and any arguments that the script takes.
- **Post-restore options** section:
  - **Restart virtual machine**: Enable this option to restart the virtual machine after the restore operation completes and after the post-restore script is applied.
  - **Postscript**: Enable this option to automate additional tasks by running a custom script after the restore is complete. Enter the full path for the script that should be run and any arguments that the script takes.

c. Select **Restore**.

Restore to alternate location

When restoring to an alternate location, you can change the destination vCenter, ESXi host, datastore, and name of the VM to create a new copy of the VM in a different location or with a different name.

a. Select the **Alternate location** pane.

b. Enter the following information:

- **Destination settings** section:
  - **vCenter FQDN or IP address**: Select the vCenter server where you want to restore the snapshot.
  - **ESXi host**: Select the host where you want to restore the snapshot.
  - **Network**: Select the network where you want to restore the snapshot.
  - **Datastore**: From the drop-down list, select the name of the datastore where you want to restore the snapshot.
  - **Virtual machine name**: Enter the name of the VM where you want to restore the snapshot. If the name matches a VM that already exists in the datastore, Backup and Recovery makes the name unique by appending a current timestamp.
- **Pre-restore options** section:
  - **Prescript**: Enable this option to automate additional tasks by running a custom script before the restore operation begins. Enter the full path for the script that should be run and any arguments that the script takes.
- **Post-restore options** section:
  - **Restart virtual machine**: Enable this option to restart the virtual machine after the restore operation completes and after the post-restore script is applied.
  - **Postscript**: Enable this option to automate additional tasks by running a custom script after the restore is complete. Enter the full path for the script that should be run and any arguments that the script takes.

c. Select **Restore**.

Restore specific virtual disks from backups

You can restore existing virtual disks (VMDKs), or deleted or detached virtual disks, from either a primary or secondary backups of traditional VMs. This enables you to restore only specific VM data or applications, so that you don't need to restore the entire VM and all of its associated virtual disks in situations where only specific data is affected. After the virtual disk is restored, it is attached to its original VM and is ready to use.

You can restore one or more virtual machine disks (VMDKs) on a VM to the same datastore or to different datastores.

For improved performance of restore operations in NFS environments, enable the VMware application vStorage API for Array Integration (VAAI).

Before you begin

- A backup must exist.
- The VM must not be in transit.

  The VM that you want to restore must not be in a state of vMotion or Storage vMotion.

About this task

- If the VMDK is deleted or detached from the VM, then the restore operation attaches the VMDK to the VM.
- A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.
- Attach and restore operations connect VMDKs using the default SCSi controller.
  However, when VMDKs that are attached to a VM with a NVMe disk are backed up, the attach and restore operations use NVMe controller if available.

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 **VMware**.
3. Enter the name of the resource you want to restore or filter for the vCenter, datacenter, or datastore where the resource that you want to restore is located.

   A list of virtual machines appears that match your search criteria.
4. Find the VM that you want to restore from in the list, and select the options menu button for that VM.
5. In the resulting menu, select **Restore virtual disks**.

   A list of snapshots (restore points) created on that virtual machine appears. By default, the latest snapshots are shown for the time frame that you select in the **Time frame** dropdown.

   For each snapshot, any illuminated icons in the **Location** column indicate the storage locations where the snapshot is available (primary, secondary, or object storage).
6. Enable the radio button for the snapshot you want to restore.

7. Select **Next**.

   Snapshot location options appear.

8. Select the restore destination for the snapshot:
   - **Local**: Restores the snapshot from the local location.
   - **Secondary**: Restores the snapshot from a remote storage location.
   - **Object store**: Restores the snapshot from object storage.

     If you choose secondary storage, select the destination location from the drop-down list.

9. Select **Next** to continue.
10. Choose the restore destination and settings:

Destination selection

Restore to original location

When restoring to the original location, you cannot change the destination vCenter, ESXi host, datastore, or name of the virtual disk. The original virtual disk is overwritten.

a. Select the **Original location** pane.
b. In the **Destination settings** section, enable the check box for any virtual disks you want to restore.
c. Choose from the following options:
   - **Pre-restore options** section:
     - **Prescript**: Enable this option to automate additional tasks by running a custom script before the restore operation begins. Enter the full path for the script that should be run and any arguments that the script takes.
   - **Post-restore options** section:
     - **Postscript**: Enable this option to automate additional tasks by running a custom script after the restore is complete. Enter the full path for the script that should be run and any arguments that the script takes.
d. Select **Restore**.

Restore to alternate location

When restoring to an alternate location, you can change the destination datastore. The virtual disk is attached to the original VM after the restore operation regardless of the datastore you choose.

a. Select the **Alternate location** pane.
b. In the **Destination settings** section, enable the check box for any virtual disks you want to restore.
c. For any virtual disks you selected:
   i. Choose **Select datastore** to choose a different datastore restore target for the virtual disk.
   ii. Select **Select** to confirm your choice and close the selection window.
d. Choose from the following options:
   - **Pre-restore options** section:
     - **Prescript**: Enable this option to automate additional tasks by running a custom script before the restore operation begins. Enter the full path for the script that should be run and any arguments that the script takes.
   - **Post-restore options** section:
     - **Postscript**: Enable this option to automate additional tasks by running a custom script after the restore is complete. Enter the full path for the script that should be run and any arguments that the script takes.
e. Select **Restore**.

Restore guest files and folders

Requirements and limitations when restoring guest files and folders

You can restore files or folders from a virtual machine disk (VMDK) on a Windows guest OS.

Guest restore workflow

Guest OS restore operations include the following steps:

1. Attach

   Attach a virtual disk to a guest VM and start a guest file restore session.

2. Wait

   Wait for the attach operation to complete before you can browse and restore. When the attach operation finishes, a guest file restore session is automatically created.

3. Select files or folders

   Browse the VMDK files and select one or more files or folders to restore.

4. Restore

   Restore the selected files or folders to a specified location.

Prerequisites for restoring guest files and folders

Review all requirements before restoring files or folders from a VMDK on a Windows guest OS.

- VMware tools must be installed and running.

  NetApp Backup and Recovery uses information from VMware tools to establish a connection to the VMware Guest OS.

- The Windows guest OS must be running Windows Server 2008 R2 or later.

  For the latest information about supported versions, refer to NetApp Interoperability Matrix Tool (IMT).

- Credentials for the target VM use the built-in domain or local administrator account with the username "Administrator". Before starting the restore operation, configure the credentials for the VM where you want to attach the virtual disk. Credentials are required for both attach and restore operations. Workgroup users can use the built-in local administrator account.

  If you must use an account that is not the built-in administrator account, but has administrative privileges within the VM, you must disable UAC on the guest VM.

- You must know the backup snapshot and VMDK to restore from.

  NetApp Backup and Recovery does not support searching of files or folders to restore. Before you begin you must know where the files or folders are in the snapshot and the corresponding VMDK.

- Virtual disk to be attached must be in a NetApp Backup and Recovery backup.

  The virtual disk that contains the file or folder you want to restore must be in a VM backup that was performed using NetApp Backup and Recovery.

- For files with non-English-alphabet names, you must restore them in a directory, not as a single file.

You can restore files with non-alphabetic names, such as Japanese Kanji, by restoring the directory in which the files are located.

Guest file restore limitations

Before you restore a file or folder from a guest OS, you should be aware of the feature limitations.

- You cannot restore dynamic disk types inside a guest OS.
- If you restore an encrypted file or folder, the encryption attribute is not retained.
- You cannot restore files or folders to an encrypted folder.
- Hidden files and folders are displayed in the file browse page, and you cannot filter them.
- You cannot restore from a Linux guest OS.

  You cannot restore files and folders from a VM that is running Linux guest OS. However, you can attach a VMDK and then manually restore the files and folders. For the latest information on supported guest OS, refer to the NetApp Interoperability Matrix Tool (IMT).

- You cannot restore from a NTFS file system to a FAT file system.

  When you try to restore from NTFS-format to FAT-format, the NTFS security descriptor is not copied because the FAT file system does not support Windows security attributes.

- You cannot restore guest files from a cloned VMDK or an uninitialized VMDK.
- You cannot restore the directory structure for a file.

  When you restore a file from a nested directory, the system restores only the file, not its directory structure. To restore the entire directory tree, copy the top-level directory.

- You cannot restore guest files from a vVol VM to an alternate host.
- You cannot restore encrypted guest files.

Restore guest files and folders from VMDKs

You can restore one or more files or folders from a VMDK on a Windows guest OS.

Before you begin

You need to create credentials for the guest VM in NetApp Backup and Recovery before you can restore files and folders from it. NetApp Backup and Recovery uses these credentials to authenticate with the guest VM when attaching the virtual disk.

About this task

Guest file or folder restore performance depends upon two factors: the size of the files or folders being restored; and the number of files or folders being restored. Restoring a large number of small-sized files might take a longer time than anticipated compared to restoring a small number of large-sized files, if the data set to be restored is of same size.

Only one attach or restore operation can run at the same time on a VM. You cannot run parallel attach or restore operations on the same VM.

With the guest restore feature, you can view and restore system and hidden files and view encrypted files. Do not overwrite an existing system file or restore encrypted files to an encrypted folder. During the restore operation, the hidden, system, and encrypted attributes of guest files are not kept in the restored file. Viewing or browsing reserved partitions might cause an error.

Steps

1. From the NetApp Backup and Recovery menu, select **Inventory**.
2. Select the **Virtual machines** menu.
3. Choose a virtual machine from the list that contains files that you want to restore.
4. Select the Actions icon ••• for that VM.
5. Select **Restore files and folders**.
6. Select a snapshot from which to restore and then select **Next**.
7. Choose the snapshot location to restore from. If you choose a secondary location, select the secondary snapshot from the list.
8. Select **Next**.
9. Choose virtual disk from the list to attach to the VM and then select **Next**.
10. On the *Select virtual machine credential* page, if you haven't yet stored a credential for the guest VM, select **Add credentials** and do the following:
    a. **Credentials name**: Enter a name for the credentials.
    b. **Authentication mode**: Select **Windows**.
    c. **Agents**: Select a Console agent from the list that will handle communication between NetApp Backup and Recovery and this host.
    d. **Domain and user name**: Enter the NetBIOS or domain FQDN and user name for the credentials.
    e. **Password**: Enter a password for the credential.
    f. Select **Add**.
11. Choose a virtual machine credential to use to authenticate with the guest VM.

    NetApp Backup and Recovery attaches the virtual disk to the VM and displays all files and folders, including hidden ones. It assigns a drive letter to every partition, including system reserved partitions.

    Files and folders you have selected are listed in the right pane of the screen.
12. Select **Next**.
13. Enter the UNC share path to the guest where the selected files will be restored.
    - IPv4 address example: `\\10.60.136.65\c$`
    - IPv6 address example: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

    If there are existing files with the same name, you can choose to overwrite or skip them.
14. Select **Restore**.

    You can view the restore progress on the Job Monitoring page.

Guest file restore troubleshooting

When attempting to restore a guest file, you might encounter any of the following scenarios.

Guest file restore session is blank

This issue occurs if you create a guest file restore session and the guest operating system reboots during the session. VMDKs in the guest OS might stay offline, so the guest file restore session list is blank.

To correct the issue, manually put the VMDKs back online in the guest OS. When the VMDKs are online, the guest file restore session will display the correct contents.

Guest file restore attach disk operation fails

This issue occurs when you start a guest file restore operation, but the attach disk operation fails even though VMware tools is running and the Guest OS credentials are correct. If this occurs, the following error is returned:

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

To correct the issue, restart the VMware Tools Windows service on the Guest OS, and then retry the guest file restore operation.

Backups are not detached after guest file restore session is discontinued

This issue occurs when you perform a guest file restore operation from a VM-consistent backup. While the guest file restore session is active, another VM-consistent backup is performed for the same VM. When the guest file restore session is disconnected, either manually or automatically after 24 hours, the backups for the session are not detached.

To correct the issue, manually detach the VMDKs that were attached from the active guest file restore session.

Copyright information

Trademark information