Back up and restore virtual machines data

BlueXP backup and recovery

NetApp
July 31, 2024

Table of Contents

Back up and restore virtual machines data

Protect your virtual machines data

BlueXP backup and recovery for virtual machines provides data protection capabilities by backing up datastores and restoring virtual machines.

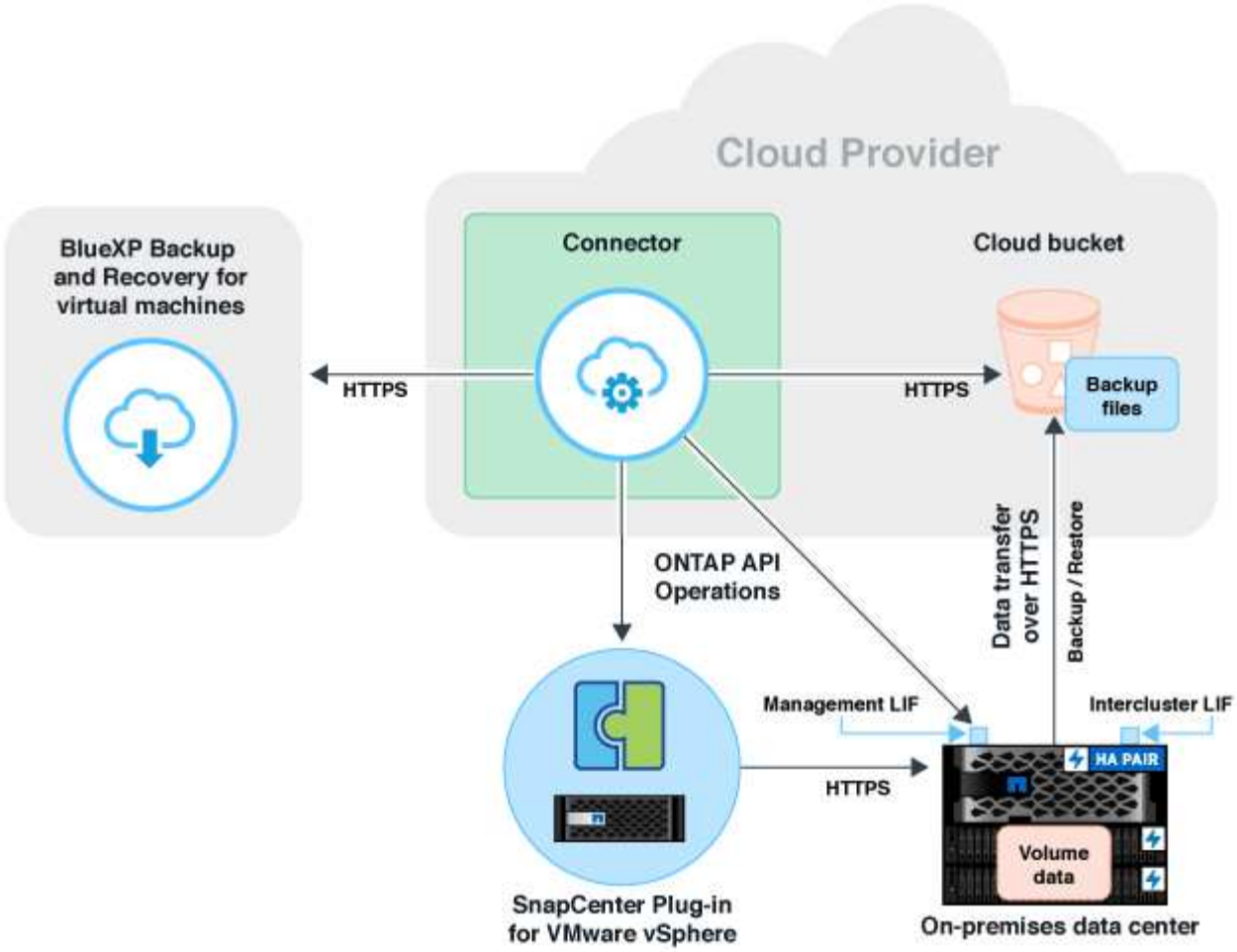
You can back up datastores to Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform, and StorageGRID and restore virtual machines back to the on-premises SnapCenter Plug-in for VMware vSphere host. BlueXP backup and recovery for virtual machines also supports connector proxy deployment model.

Before you begin

Read the following requirements to make sure that you have a supported configuration before you start backing up datastores and virtual machines to a cloud provider.

- SnapCenter Plug-in for VMware vSphere 4.6P1 or later
  - You should be using SnapCenter Plug-in for VMware vSphere 4.7P1 or later to back up datastores from on-premises secondary storage.
- ONTAP 9.8 or later
- BlueXP
- NFS and VMFS datastores are supported. vVols are not supported.
- For VMFS support, SnapCenter Plug-in for VMware vSphere host should be running on 4.9 or later. Ensure to take a backup of the VMFS datastore if the SnapCenter Plug-in for VMware vSphere host was upgraded from an earlier version to the 4.9 release.
- At least one backup should have been taken in SnapCenter Plug-in for VMware vSphere 4.6P1.
- At least one daily, weekly, or monthly policy in SnapCenter Plug-in for VMware vSphere with no label or same label as that of the Virtual Machines policy in BlueXP.
- For pre-canned policy, the schedule tier should be the same for the datastore in SnapCenter Plug-in for VMware vSphere and in the cloud.
- Ensure that there are no FlexGroup volumes in the datastore because backing up and restoring FlexGroup volumes are not supported.
- Disable "**_recent**" on the required resource groups. If you have "**_recent**" enabled for the resource group, then the backups of those resource groups cannot be used for data protection to cloud and subsequently cannot be used for the restore operation.
- Ensure that the destination datastore where the virtual machine will be restored has enough space to accommodate a copy of all virtual machine files such as VMDK, VMX, VMSD, and so on.
- Ensure that the destination datastore does not have stale virtual machine files in the format of restore_xxx_xxxxxx_filename from the previous restore operation failures. You should delete the stale files before triggering a restore operation.
- To deploy a connector with proxy configured, ensure that all outgoing connector calls are routed through the proxy server.

The following image shows each component and the connections that you need to prepare between them:



Register SnapCenter Plug-in for VMware vSphere host

You should register the SnapCenter Plug-in for VMware vSphere host in BlueXP for the datastores and virtual machines to be displayed. Only a user with administrative access can register the SnapCenter Plug-in for VMware vSphere host.

You can register multiple SnapCenter Plug-in for VMware vSphere hosts in BlueXP. However, once registered, you cannot remove the SnapCenter Plug-in for VMware vSphere host.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. From the **Settings** drop-down, click **SnapCenter Plug-in for VMware vSphere**.
3. Click **Register SnapCenter Plug-in for VMware vSphere**.
4. Specify the following details:
   a. In the SnapCenter Plug-in for VMware vSphere field, specify the FQDN or IP address of the SnapCenter Plug-in for VMware vSphere host.
   b. In the Port field, specify the port number on which the SnapCenter Plug-in for VMware vSphere host is running.

You should ensure that communication is open between on-premises SnapCenter Plug-in for VMware vSphere host which is running on the default 8144 port and BlueXP Connector instance which could be either running in any cloud providers (Amazon Web Services, Microsoft Azure, Google Cloud Platform) or on-premises.

c. In the Username and Password field, specify the credentials of the vCenter user with the administrator role.

5. Click **Register**.

After you finish

Click **Backup and recovery** > **Virtual Machines** to view all the datastores and virtual machines that are protected using the registered SnapCenter Plug-in for VMware vSphere host.

Create a policy to back up datastores

You can create a policy or use one of the following predefined policies that are available in BlueXP.

Before you begin

- You should create policies if you do not want to edit the predefined policies.
- To move backups from object store to archival storage, you should be running ONTAP 9.10.1 or later and Amazon Web Services or Microsoft Azure should be the cloud provider.
- You should configure the archive access tier for each cloud provider.

About this task

The following predefined policies are available in BlueXP:

Policy Name	Label	Retention Value
1 Year Daily LTR (Long Term Retention)	Daily	366
5 Years Daily LTR	Daily	1830
7 Year Weekly LTR	Weekly	370
10 Year Monthly LTR	Monthly	120

Steps

1. In the Virtual machines page, from the Settings drop-down list, select **Policies**.
2. Click **Create policy**.
3. In the Policy Details section, specify the policy name.
4. In the Retention section, select one of the retention type and specify the number of backups to retain.
5. Select Primary or Secondary as the backup storage source.
6. (Optional) If you want to move backups from object store to archival storage after a certain number of days for cost optimization, select the **Tier Backups to Archival** checkbox and enter the number of days after

which the backup should be archived.

7. Click **Create**.

> You cannot edit or delete a policy, which is associated with a datastore.

Back up datastores to Amazon Web Services

You can back up and archive one or more datastores to Amazon Web Services to improve storage efficiency and cloud transition.

If the datastore is associated with an archival policy, you have an option to select the archival tier. The supported archival tiers are Glacier and Glacier Deep.

Before you begin

Ensure that you have met all the requirements before backing up datastores to the cloud.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. Click ••• corresponding to the datastore that you want to back up and click **Activate Backup**.
3. In the Assign Policy page, select the policy and click **Next**.
4. Add the working environment.

   Configure the cluster management LIF that you want BlueXP to discover. After adding the working environment for one of the datastores, it can be reused for all the other datastores residing on the same ONTAP cluster.

   a. Click **Add Working Environment** corresponding to the SVM.
   b. In the Add Working Environment wizard:
      i. Specify the IP address of the cluster management LIF.
      ii. Specify the credentials of the ONTAP cluster user.
   c. Click **Add Working Environment**.
5. Select **Amazon Web Services** to configure it as the cloud provider.
   a. Specify the AWS account.
   b. In the AWS Access Key field, specify the key for data encryption.
   c. In the AWS Secret Key field, specify the password for data encryption.
   d. Select the region where you want to create the backups.
   e. Specify the IP addresses of the cluster management LIF that were added as the working environments.
   f. Select the archival tier.

      It is recommended to set the archival tier because this is an one time activity and you cannot set it up later.
6. Review the details and click **Activate Backup**.

Back up datastores to Microsoft Azure

You can back up one or more datastores to Microsoft Azure by integrating the SnapCenter Plug-in for VMware vSphere host with BlueXP. This will help the VM administrators to easily and quickly back up and archive data for storage efficiency and accelerate cloud transition.

If the datastore is associated with an archival policy, you will be provided with an option to select the archival tier. The supported archival tier is Azure Archive Blob Storage.

Before you begin

Ensure that you have met all the requirements before backing up datastores to the cloud.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. Click ••• corresponding to the datastore that you want to back up and click **Activate Backup**.
3. In the Assign Policy page, select the policy and click **Next**.
4. Add the working environment.

   Configure the cluster management LIF that you want BlueXP to discover. After adding the working environment for one of the datastores, it can be reused for all the other datastores residing on the same ONTAP cluster.

   a. Click **Add Working Environment** corresponding to the SVM.
   b. In the Add Working Environment wizard:
      i. Specify the IP address of the cluster management LIF.
      ii. Specify the credentials of the ONTAP cluster user.
   c. Click **Add Working Environment**.
5. Select **Microsoft Azure** to configure it as the cloud provider.
   a. Specify the Azure subscription ID.
   b. Select the region where you want to create the backups.
   c. Create a new resource group or use an existing resource group.
   d. Specify the IP addresses of the cluster management LIF that were added as the working environments.
   e. Select the archival tier.

      It is recommended to set the archival tier because this is an one time activity and you will not be allowed to set it up later.
6. Review the details and click **Activate Backup**.

Back up datastores to Google Cloud Platform

You can back up one or more datastores to Google Cloud Platform by integrating the SnapCenter Plug-in for VMware vSphere host with BlueXP. This will help the VM administrators to easily and quickly back up and archive data for storage efficiency and

accelerate cloud transition.

Before you begin

Ensure that you have met all the requirements before backing up datastores to the cloud.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. Click ••• corresponding to the datastore that you want to back up and click **Activate Backup**.
3. In the Assign Policy page, select the policy and click **Next**.
4. Add the working environment.

   Configure the cluster management LIF that you want BlueXP to discover. After adding the working environment for one of the datastores, it can be reused for all the other datastores residing on the same ONTAP cluster.

   a. Click **Add Working Environment** corresponding to the SVM.
   b. In the Add Working Environment wizard:
      i. Specify the IP address of the cluster management LIF.
      ii. Specify the credentials of the ONTAP cluster user.
   c. Click **Add Working Environment**.
5. Select **Google Cloud Platform** to configure it as the cloud provider.
   a. Select the Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups.
   b. In the Google Cloud Access Key field, specify the key.
   c. In the Google Cloud Secret Key field, specify the password.
   d. Select the region where you want to create the backups.
   e. Specify the IP space.
6. Review the details and click **Activate Backup**.

Back up datastores to StorageGRID

You can back up one or more datastores to StorageGRID by integrating the SnapCenter Plug-in for VMware vSphere host with BlueXP. This will help the VM administrators to easily and quickly back up and archive data for storage efficiency and accelerate cloud transition.

Before you begin

Ensure that you have met all the requirements before backing up datastores to the cloud.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. Click ••• corresponding to the datastore that you want to back up and click **Activate Backup**.
3. In the Assign Policy page, select the policy and click **Next**.
4. Add the working environment.

Configure the cluster management LIF that you want BlueXP to discover. After adding the working environment for one of the datastores, it can be reused for all the other datastores residing on the same ONTAP cluster.

   a. Click **Add Working Environment** corresponding to the SVM.
   b. In the Add Working Environment wizard:
      i. Specify the IP address of the cluster management LIF.
      ii. Specify the credentials of the ONTAP cluster user.
   c. Click **Add Working Environment**.
5. Select **StorageGRID**.
   a. Specify the Storage Server IP.
   b. Select the access key and secret key.
6. Review the details and click **Activate Backup**.

Manage protection of datastores and virtual machines data

You can view policies, datastores, and virtual machines before you back up and restore data. Depending upon the change in database, policies, or resource groups, you can view the updates from the BlueXP UI.

View policies

You can view all the default pre-canned policies. For each of these policies, when you view the details, all the associated policies and virtual machines are listed.

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. From the **Settings** drop-down, click **Policies**.
3. Click **View Details** corresponding to policy whose details you want to view.

The associated policies and virtual machines are listed.

View datastores and virtual machines

The datastores and virtual machines that are protected using the registered SnapCenter Plug-in for VMware vSphere host are displayed.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines** > **Settings** > **SnapCenter Plug-in for VMware vSphere**.
2. Click the SnapCenter Plug-in for VMware vSphere host for which you want to see the datastores and virtual machines.

Unprotect datastores

You can unprotect a datastore which was already protected earlier. You can unprotect a datastore when you want to delete the cloud backups or do not want to back it up to the cloud anymore. The datastore can be protected again after the unprotection is successful.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines**.
2. Click ••• corresponding to the datastore that you want to unprotect and click **Unprotect**.

Edit the SnapCenter Plug-in for VMware vSphere Instance

You can edit the details of the SnapCenter Plug-in for VMware vSphere host in BlueXP.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines** > **Settings** > **SnapCenter Plug-in for VMware vSphere**.
2. Click ••• and select **Edit**.
3. Modify the details as required.
4. Click **Save**.

Refresh resources and backups

If you want to view the latest datastores and backups that have been added to the application, you should refresh the resources and backups. This will initiate the discovery of the resources and backups and the latest details will be displayed.

1. Click **Backup and recovery** > **Virtual Machines**.
2. From the **Settings** drop-down, click **SnapCenter Plug-in for VMware vSphere**.
3. Click ••• corresponding to the SnapCenter Plug-in for VMware vSphere host and click **Refresh Resources and Backups**.

Refresh policy or resource group

If there is a change to the policy or resource group, you should refresh the protection relationship.

1. Click **Backup and recovery** > **Virtual Machines**.
2. Click ••• corresponding to the datastore and click **Refresh Protection**.

Unregister SnapCenter Plug-in for VMware vSphere host

All datastores and virtual machines associated with the SnapCenter Plug-in for VMware vSphere host will be unprotected.

1. Click **Backup and recovery** > **Virtual Machines**.
2. From the **Settings** drop-down, click **SnapCenter Plug-in for VMware vSphere**.
3. Click ••• corresponding to the SnapCenter Plug-in for VMware vSphere host and click **Unregister**.

Monitor Jobs

Jobs are created for all the BlueXP backup and recovery operations. You can monitor all the jobs and all the sub tasks that are performed as part of each task.

1. Click **Backup and recovery** > **Job Monitoring**.

When you initiate an operation, a window appears stating that the job is initiated. You can click the link to monitor the job.

2. Click the primary task to view the sub tasks and status of each of these sub tasks.

Restore virtual machines data from the cloud

You can restore virtual machines data from the cloud back to the on-premises vCenter. You can restore the virtual machine to the exact same location from where the backup was taken or to an alternate location. If the virtual machine was backed up using archival policy, then you can set the archival restore priority.

You cannot restore virtual machines that span across datastores.

Before you begin

- Ensure that you have met all the requirements before restoring virtual machines from the cloud.
- If you are restoring to an alternate location:
  - Ensure that the source and destination vCenters are in linked mode.
  - Ensure that the source and destination cluster details are added in BlueXP Canvas and in linked mode vCenters in both SnapCenter Plug-in for VMware vSphere host.
  - Ensure that the Working Environment (WE) is added corresponding to the alternate location in BlueXP Canvas.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Virtual Machines** > **SnapCenter Plug-in for VMware vSphere** and select the SnapCenter Plug-in for VMware vSphere host.

   If the source virtual machine is moved to another location (vMotion), and if the user triggers a restore of that virtual machine from BlueXP, then the virtual machine is restored to the source location from where the backup was taken.

2. You can restore the virtual machine to the original location or to an alternate location from the datastore or from virtual machines:

If you want to restore the virtual machine…	Do this…
to the original location from datastore	1. Click ••• corresponding to the datastore that you want to restore and click **View Details**. 2. Click **Restore** corresponding to the backup you want to restore. 3. Select the virtual machine that you want to restore from the backup and click **Next**. 4. Ensure that **Original** is selected and click **Continue**. 5. If the virtual machine is protected using a policy where archival settings are configured, select the **Archival Restore Priority** and click **Next**. The supported archival restore priority for Amazon Web Services are high, standard, and low and the supported archival restore priority for Microsoft Azure are high and standard. 6. Review the details and click **Restore**.
to an alternate location from datastore	1. Click ••• corresponding to the datastore that you want to restore and click **View Details**. 2. Click **Restore** corresponding to the backup you want to restore. 3. Select the virtual machine that you want to restore from the backup and click **Next**. 4. Select **Alternate**. 5. Select the alternate vCenter Server, ESXi host, datastore, and network. 6. Provide a name for the VM after restore and click **Continue**. 7. If the virtual machine is protected using a policy where archival settings are configured, select the **Archival Restore Priority** and click **Next**. The supported archival restore priority for Amazon Web Services are high, standard, and low and the supported archival restore priority for Microsoft Azure are high and standard. 8. Review the details and click **Restore**.

If you want to restore the virtual machine…	Do this…
to the original location from virtual machines	1. Click ••• corresponding to the virtual machine that you want to restore and click **Restore**. 2. Select the backup through which you want to restore the virtual machine. 3. Ensure that **Original** is selected and click **Continue**. 4. If the virtual machine is protected using a policy where archival settings are configured, select the **Archival Restore Priority** and click **Next**. The supported archival restore priority for Amazon Web Services are high, standard, and low and the supported archival restore priority for Microsoft Azure are high and standard. 5. Review the details and click **Restore**.
to an alternate location from virtual machines	1. Click ••• corresponding to the virtual machine that you want to restore and click **Restore**. 2. Select the backup through which you want to restore the virtual machine. 3. Select **Alternate**. 4. Select the alternate vCenter Server, ESXi host, datastore, and network. 5. Provide a name for the VM after restore and click **Continue**. 6. If the virtual machine is protected using a policy where archival settings are configured, select the **Archival Restore Priority** and click **Next**. The supported archival restore priority for Amazon Web Services are high, standard, and low and the supported archival restore priority for Microsoft Azure are high and standard. 7. Review the details and click **Restore**.

Copyright information

Trademark information