Backup NFS datastore to Amazon FSx

BlueXP backup and recovery for VMs

NetApp
April 03, 2025

Table of Contents

Backup NFS datastore to Amazon FSx

Add storage

Before you can backup or restore VMs, you must add “Amazon FSx for NetApp ONTAP” or “Amazon FSx for NetApp ONTAP SVM” as the storage system. Adding storage enables BlueXP backup and recovery for VMs to recognize and manage backup and restore operations in vCenter.

Before you begin

The ESXi server, BlueXP backup and recovery for VMs, and each vCenter must be synchronized to the same time. If you try to add storage but the time settings for your vCenters are not synchronized, the operation might fail with a Java certificate error.

About this task

BlueXP backup and recovery for VMs perform backup and restore operations on directly connected storage VMs and on storage VMs in a storage cluster.

- Names for storage VMs must resolve to management LIFs.

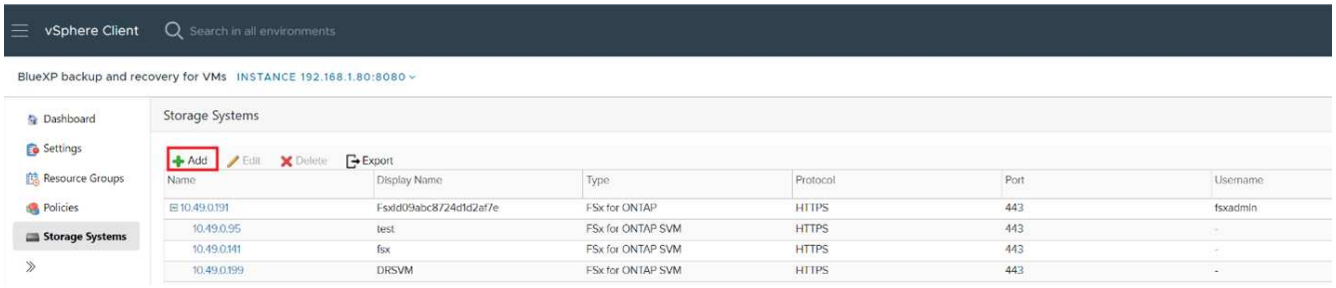
  If you added etc host entries for storage VM names in BlueXP backup and recovery for VMs, you must verify that they are also resolvable from the virtual appliance.

  If you add a storage VM with a name that cannot resolve to the management LIF, then scheduled backup jobs fail because the plug-in is unable to discover any datastores or volumes on that storage VM. If this occurs, either add the storage VM to BlueXP backup and recovery for VMs and specify the management LIF or add a cluster that contains the storage VM and specify the cluster management LIF.

- Storage authentication details are not shared between multiple instances of BlueXP backup and recovery for VMs or between Windows SnapCenter Server and BlueXP backup and recovery for VMs on vCenter.

Steps

1. In the left Navigator pane of the vSphere client, click **Storage Systems**.
2. On the Storage Systems page, click **Add**.



3. In the **Add Storage System** wizard, enter the basic storage VM or cluster information.
4. Select the **Credentials** authentication method and log in as Amazon FSx administrator.
5. Click **Add**.

If you added a storage cluster, all storage VMs in that cluster are automatically added. Automatically added storage VMs (sometimes called “implicit” storage VMs) are displayed on the cluster summary page with a

hyphen (-) instead of a username. Usernames are displayed only for explicit storage entities.

Create backup policies for VMs and datastores

You must create backup policies before you use BlueXP backup and recovery for VMs to back up VMs and datastores.

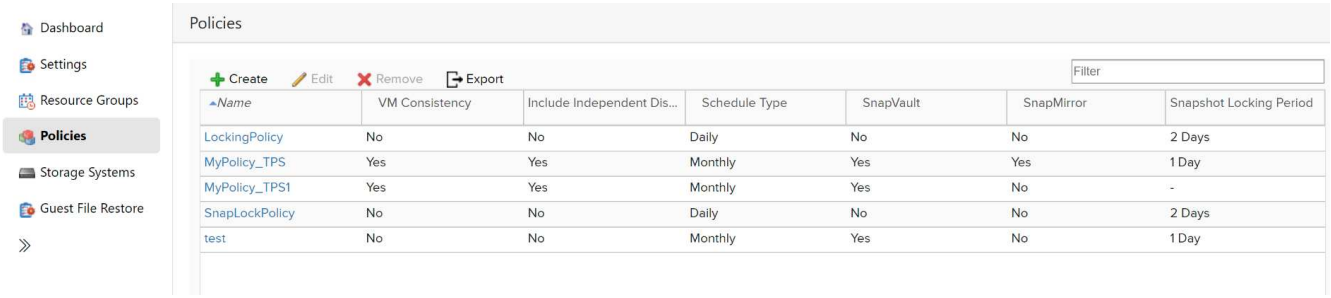
Before you begin

- You must have read the prerequisites.
- You must have secondary storage relationships configured.
  - If you are replicating Snapshot copies to a mirror or vault secondary storage, the relationships must be configured, and the storage systems of the source and destination volumes must be registered.
  - To successfully transfer Snapshot copies to secondary storage for Version-FlexibleMirror relationships on a NFS datastore, make sure that the SnapMirror policy type is Asynchronous Mirror and that the "all_source_snapshots" option is checked.
  - When the number of Snapshot copies on the secondary storage (mirror-vault) reaches the maximum limit, the activity to register backup and apply retention in the backup operation fails with the following error: This Snapshot copy is currently used as a reference Snapshot copy by one or more SnapMirror relationships. Deleting the Snapshot copy can cause future SnapMirror operations to fail.

    To correct this issue, configure the SnapMirror retention policy for the secondary storage to avoid reaching the maximum limit of Snapshot copies.
- If you want VM-consistent backups, you must have VMware tools installed and running. VMware tools are needed to quiesce VMs.

Steps

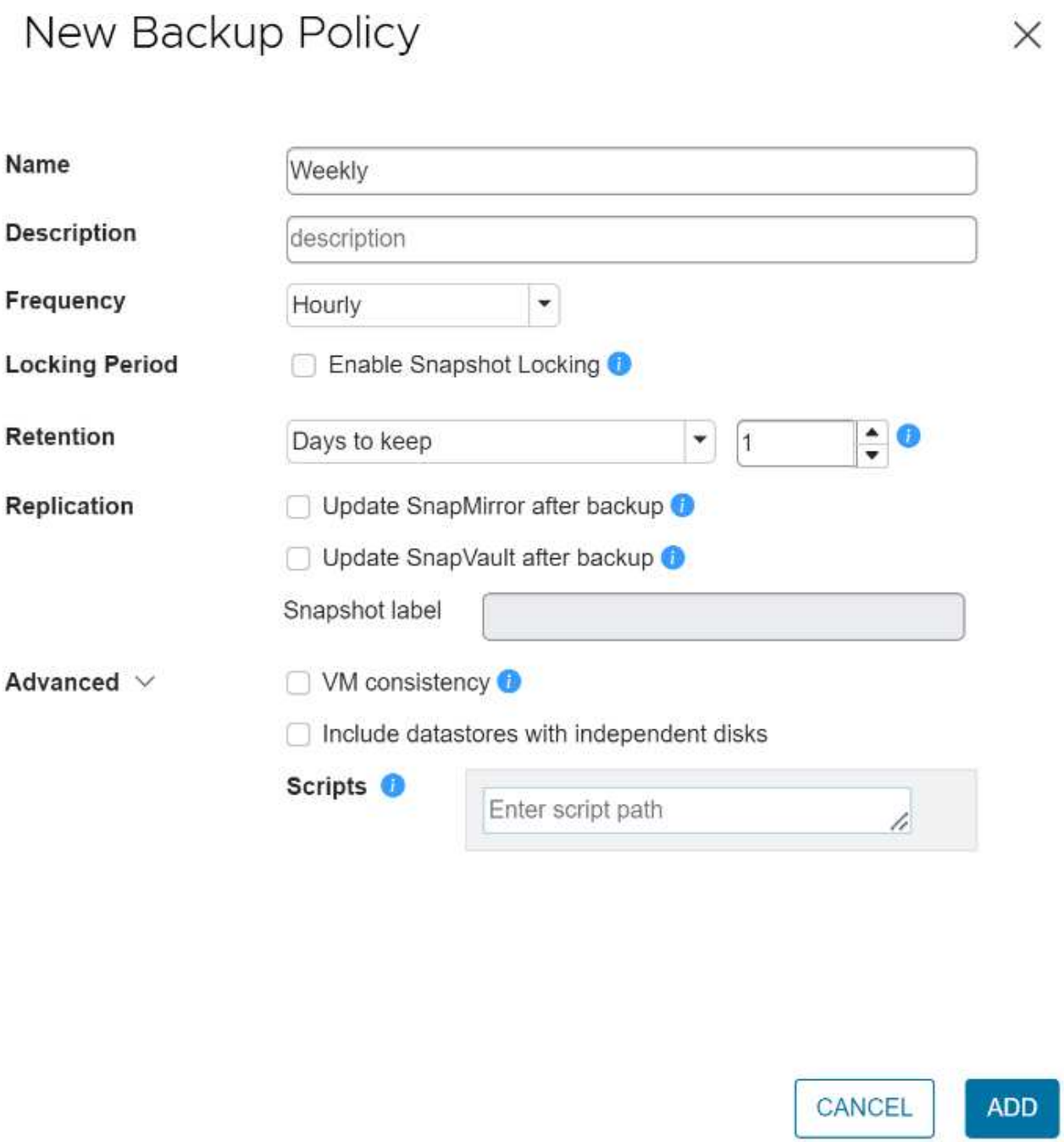
1. In the left Navigator pane of BlueXP backup and recovery for VMs, click **Policies**.
2. On the **Policies** page, click **Create** to start the wizard.



3. On the **New Backup Policy** page, select the VMC on AWS that will use the policy, and then enter the policy name and a description.
   - Unsupported characters

     Do not use the following special characters in VM, datastore, cluster, policy, backup, or resource group names: % & * $ # @ ! \ / : * ? " < > - | ; ' , .

     An underscore character (_) is allowed.



4. Specify the frequency settings.

   The policy specifies the backup frequency only. The specific protection schedule for backing up is defined in the resource group. Therefore, two or more resource groups can share the same policy and backup frequency but have different backup schedules.

5. If you do not want the Snapshot to be tampered, enable **Snapshot Locking** and specify the locking period.
6. Specify the retention settings.

> You should set the retention count to 2 backups or higher if you plan to enable SnapVault replication. If you set the retention count to 1 backup to keep, the retention operation can fail. This is because the first Snapshot copy is the reference Snapshot copy for the SnapVault relationship until the newer Snapshot copy is replicated to the target.

7. In the **Replication** fields, specify the type of replication to secondary storage, as shown in the following table:

For this field…	Do this…
Update SnapMirror after backup	Select this option to create mirror copies of backup sets on another volume that has a SnapMirror relationship to the primary backup volume. If a volume is configured with a mirror-vault relationship, you must select only the **Update SnapVault after backup** option if you want backups copied to the mirror-vault destinations.
Update SnapVault after backup	Select this option to perform disk-to-disk backup replication on another volume that has a SnapVault relationship to the primary backup volume. If a volume is configured with a mirror-vault relationship, you must select only this option if you want backups copied to the mirror-vault destinations.
Snapshot label	Enter an optional, custom label to be added to SnapVault and SnapMirror Snapshot copies created with this policy. The Snapshot label helps to distinguish Snapshots created with this policy from other Snapshots on the secondary storage system. A maximum of 31 characters is allowed for Snapshot copy labels.

8. **Optional**: In the Advanced fields, select the fields that are needed. The Advanced field details are listed in the following table.

For this field…	Do this…
VM consistency	Check this box to quiesce the VMs and create a VMware snapshot each time the backup job runs. You must have VMware tools running on the VM to perform VM consistent backups. If VMware Tools is not running, a crash-consistent backup is performed instead. When you check the VM consistency box, backup operations might take longer and require more storage space. In this scenario, the VMs are first quiesced, then VMware performs a VM consistent snapshot, then BlueXP backup and recovery for VMs performs its backup operation, and then VM operations are resumed. VM guest memory is not included in VM consistency Snapshots.
Include datastores with independent disks	Check this box to include in the backup any datastores with independent disks that contain temporary data.
Scripts	Enter the fully qualified path of the prescript or postscript that you want the BlueXP backup and recovery for VMs to run before or after backup operations. For example, you can run a script to update SNMP traps, automate alerts, and send logs. The script path is validated at the time the script is executed. Prescripts and postscripts must be located on the virtual appliance VM. To enter multiple scripts, press Enter after each script path to list each script on a separate line. The character ";" is not allowed.

9. Click **Add**.

   You can verify that the policy is created and review the policy configuration by selecting the policy in the Policies page.

Create resource groups

A resource group is the container for Virtual Machines and datastores that you want to protect.

For all resource groups, do not add Virtual Machines that are in an inaccessible state. Although it is possible to create a resource group that contains inaccessible Virtual Machines, backups for that resource group will fail.

About this task

You can add or remove resources from a resource group at any time.

- Backing up a single resource

  To back up a single resource (for example, a single Virtual Machine), you must create a resource group that contains that single resource.

- Backing up multiple resources

  To back up multiple resources, you must create a resource group that contains multiple resources.

- Optimizing Snapshot copies

  To optimize Snapshot copies, you should group the Virtual Machines and datastores that are associated with the same volume into one resource group.

- Backup policies

  Although it is possible to create a resource group without a backup policy, you can only perform scheduled data protection operations when at least one policy is attached to the resource group. You can use an existing policy, or you can create a new policy while creating a resource group.

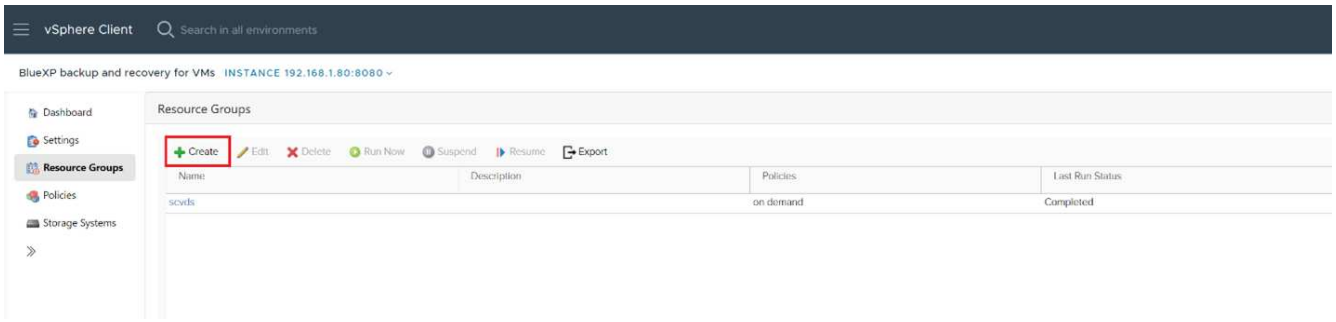
- Compatibility checks

  BlueXP backup and recovery for VMs performs compatibility checks when you create a resource group. Reasons for incompatibility might be:

  - VMDKs are on unsupported storage.
  - A shared PCI device is attached to a Virtual Machine.

Steps

1. In the left Navigator pane of BlueXP backup and recovery for VMs, click **Resource Groups**.
2. On the **Resource Groups** page, click **Create** to start the wizard.



This is the easiest way to create a resource group. However, you can also create a resource group with one resource by performing one of the following:

- To create a resource group for one Virtual Machine, click **Menu › Hosts and Clusters**, then right-click a Virtual Machine, then select BlueXP backup and recovery for VMs, and then click **Create**.
- To create a resource group for one datastore, click **Menu › Hosts and Clusters**, then right-click a datastore, then select BlueXP backup and recovery for VMs, and then click **Create**.

3. On the **General Info & Notification** page in the wizard, enter the required values.
4. On the **Resources** page, do the following:

For this field…	Do this…
Scope	Select the type of resource you want to protect: • Datastores • Virtual Machines
Datacenter	Navigate to the Virtual Machines or datastores
Available entities	Select the resources you want to protect, then click > to move your selections to the Selected entities list

When you click **Next**, the system first checks that BlueXP backup and recovery for manages and is compatible with the storage on which the selected resources are located.

If the message selected <resource-name> is not BlueXP backup and recovery for VMs compatible is displayed, then a selected resource is not compatible with BlueXP backup and recovery for VMs.

5. On the **Spanning disks** page, select an option for Virtual Machines with multiple VMDKs across multiple datastores:
   - Always exclude all spanning datastores [This is the default for datastores.]
   - Always include all spanning datastores [This is the default for Virtual Machines.]
   - Manually select the spanning datastores to be included.
6. On the **Policies** page, select or create one or more backup policies, as shown in the following table:

To use…	Do this…
An existing policy	Select one or more policies from the list.
A new policy	1. Click **Create**. 2. Complete the New Backup Policy wizard to return to the Create Resource Group wizard.

7. On the **Schedules** page, configure the backup schedule for each selected policy.

In the starting hour field, enter a date and time other than zero. The date must be in the format day/month/year. You must fill in each field. BlueXP backup and recovery for VMs creates schedules in the

time zone in which BlueXP backup and recovery for VMs is deployed. You can modify the time zone by using BlueXP backup and recovery for VMs GUI.

8. Review the **summary**, and then click **Finish**.

   Before you click Finish, you can go back to any page in the wizard and change the information.

   After you click Finish, the new resource group is added to the resource groups list.

   If the quiesce operation fails for any of the Virtual Machines in the backup, then the backup is marked as not Virtual Machine consistent even if the policy selected has Virtual Machine consistency selected. In this case, it is possible that some of the Virtual Machines were successfully quiesced.

Back up resource groups on demand

Backup operations are performed on all the resources defined in a resource group. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

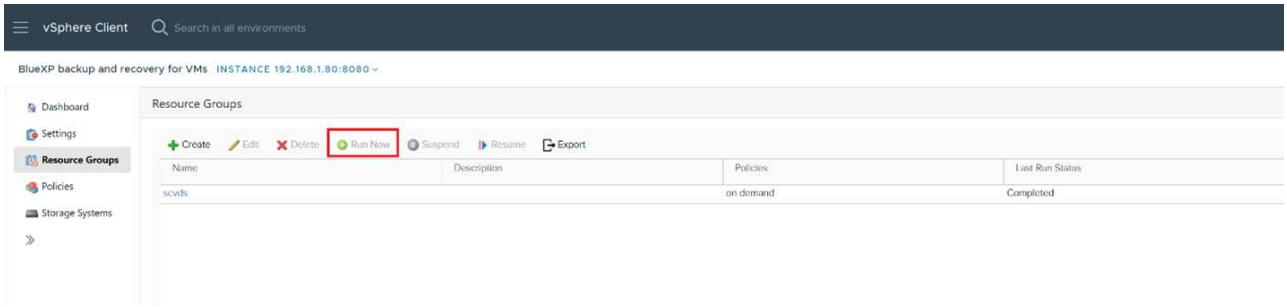
Before you begin

- You must have created a resource group with a policy attached.

  Do not start an on-demand backup job when a job to back up BlueXP backup and recovery for VMs MySQL database is already running. Use the maintenance console to see the configured backup schedule for the MySQL database.

Steps

1. In the left Navigator pane of the vCenter web client page, click **BlueXP backup and recovery for VMs** › **Resource Groups**, then select a resource group, and then click **Run Now** to start the backup.



2. If the resource group has multiple policies configured, then in the Backup Now dialog box, select the policy you want to use for this backup operation.
3. Click **OK** to start the backup.
4. If the quiesce operation fails for any of the Virtual Machines in the backup, then the backup completes with a warning and is marked as not Virtual Machine consistent even if the selected policy has Virtual Machine consistency selected. In this case, it is possible that some of the Virtual Machines were successfully quiesced. In the job monitor, the failed Virtual Machine details will show the quiesce as failed.

Copyright information

Trademark information