BlueXP backup and recovery for VMs documentation

BlueXP backup and recovery for VMs

NetApp
April 03, 2025

Table of Contents

BlueXP backup and recovery for VMs documentation

Release notes

What’s new with BlueXP backup and recovery for VMs

Learn what’s new in BlueXP backup and recovery for VMs.

18 January 2024

Enhancements to BlueXP backup and recovery for VMs

The following are the features that are supported in BlueXP backup and recovery for VMs 1.1:

- Mount and unmount datastores
- Attach and detach VMDKs
- Restore virtual machines to alternate location
- Enable Snapshot Locking to ensure Snapshot copies are not tampered until a specified time.

13 July 2023

BlueXP backup and recovery for VMs 1.0 is now GA

You can protect data on your virtual machines by using BlueXP backup and recovery for VMs. You can back up datastores on Amazon FSx and restore virtual machines to their original location.

This solution is specifically for Virtual Machines and Datastores on VMware Cloud on AWS and Amazon FSx for NetApp ONTAP.

BlueXP backup and recovery for virtual machines on Amazon FSx

Get started

BlueXP backup and recovery for virtual machines on Amazon FSx

BlueXP backup and recovery for VMs is a standalone virtual appliance (Open Virtual Appliance format) that provides data protection services for VMs and datastores on VMware Cloud on AWS and Amazon FSx for NetApp ONTAP.

- You can backup only NFS type datastores on Amazon FSx.
- You should be running ONTAP 9.10 or later to backup NFS datastores.
- VMware Cloud comes with a pre-defined “CloudAdmin” role. The CloudAdmin role has the necessary privileges to create and manage SDDC workloads and related objects such as storage policies, content libraries, vSphere tags, and resource pools.
- You can restore VMs and VMDK to their current/alternate location.

Unsupported workflows

The following workflows are not supported in BlueXP backup and recovery for VMs 1.0 release:

- Attach and detach VMDKs
- Mount and unmount datastores
- Restore guest files and folders
- Restore to Alternate Location
- Add storage system using "Certificate" authentication method
- Add NetApp ONTAP FlexGroup volumes

Deploy BlueXP backup and recovery for VMs

Requirements and considerations

You need to be aware of several requirements and considerations before using BlueXP backup and recovery for VMs:

- BlueXP backup and recovery for VMs is deployed as a Linux VM regardless of whether you use the plug-in to protect data on Windows systems or Linux systems.
- You should deploy BlueXP backup and recovery for VMs on VMC on AWS.

  BlueXP backup and recovery for VMs and VMC should use the same timezone. Backup schedules are executed in the time zone in which BlueXP backup and recovery for VMs is deployed. VMC reports data in the time zone in which the VMC is located. Therefore, if BlueXP backup and recovery for VMs and VMC are in different time zones, data in BlueXP backup and recovery for VMs Dashboard might not be the same as the data in the reports.

- You must not deploy BlueXP backup and recovery for VMs in a folder that has a name with special characters.

  The folder name should not contain the following special characters: $!@#%^&()_+{}';.,*?"<>|

- You must deploy and register a separate, unique instance of BlueXP backup and recovery for VMs for each VMC on AWS.
  - Each VMC on AWS should be paired with a separate instance of BlueXP Backup and Recovery for VMs.
  - Each instance of BlueXP backup and recovery for VMs must be deployed as a separate Linux VM.

    For example, if you want to perform backups from six different instances of VMC on AWS, then you must deploy six BlueXP backup and recovery for VMs instances on six hosts and each VMC on AWS must be paired with a unique instance of BlueXP backup and recovery for VMs.

- On the vmc.vmware.com console, open the firewall ports to allow the compute gateway public IP to communicate over TCP 443 with the vCenter on the management network.
- On the AWS console, you must update the security group of the VPC where FSx for ONTAP is running to allow BlueXP backup and recovery for VMs access FSx for ONTAP.

Deploy BlueXP backup and recovery for VMs

To protect VMs and datastores on virtualized machines, you must deploy BlueXP backup and recovery for VMs.

Before you begin

> ⓘ The OVA deployment is supported in VMware vCenter 8.0 and above.

- You must have read the deployment requirements.
- You must be running a supported version of VMC on AWS.

- You must have configured and set up your VMC on AWS environment.
- You must have set up an ESXi host for BlueXP backup and recovery for VMs.
- You must have downloaded BlueXP backup and recovery for VMs `.tar` file.
- You must have the login authentication details for your VMC on AWS instance.
- You must have a certificate with valid Public and Private Key files. For more information, see articles under Storage Certificate Management section.
- You must have logged out of and closed all browser sessions of vSphere client and deleted the browser cache to avoid any browser cache issue during the deployment of BlueXP backup and recovery for VMs.
- You must have enabled Transport Layer Security (TLS) in vCenter. Refer to the VMware documentation.
- You must have deployed BlueXP backup and recovery for VMs in the same time zone as the vCenter.

Steps

1. For VMware vCenter 7.0.3 and later versions, follow the steps in Download the Open Virtual Appliance (OVA) section to import the certificates to vCenter.
2. In your browser, navigate to VMware vSphere vCenter.
3. Log in to the **VMware vCenter Single Sign-On page**.
4. On the Navigator pane, right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, cluster, or host, and select **Deploy OVF Template** to start the VMware deploy wizard.
5. Extract the `.tar` file, which contains the `.ova` file onto your local system. On the **Select an OVF template** page, specify the location of the `.ova` file inside the `.tar` extracted folder.
6. Click **Next**.
7. On the **Select a name and folder** page, enter a unique name for the VM or vApp, and select a deployment location, and then click **Next**.

   This step specifies where to import the `.ova` file into vCenter. The default name for the VM is the same as the name of the selected `.ova` file. If you change the default name, choose a name that is unique within each VMC on AWS VM folder.

   The default deployment location for the VM is the inventory object where you started the wizard.
8. On the **Select a resource** page, select the resource where you want to run the deployed VM template, and click **Next**.
9. On the **Review details** page, verify the `.ova` template details and click **Next**.
10. On the **License agreements** page, select the checkbox for **I accept all license agreements**.
11. On the **Select storage** page, define where and how to store the files for the deployed OVF template.
    a. Select the disk format for the VMDKs.
    b. Select a VM Storage Policy.

       This option is available only if storage policies are enabled on the destination resource.
    c. Select a datastore to store the deployed OVA template.

       The configuration file and virtual disk files are stored on the datastore.

       Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.

12. On the **Select networks** page, do the following:
    a. Select a source network and map it to a destination network.

       The Source Network column lists all networks that are defined in the OVA template.

    b. In the **IP Allocation Settings** section, select the required IP protocol and then click **Next**.

       BlueXP backup and recovery for VMs supports one network interface. If you need multiple network adapters, you must set that up manually.

13. On the **Customize template** page, do the following:
    a. In the **Register to existing vCenter** section, enter the vCenter name and the vCenter credentials of the virtual appliance.

       In the **vCenter username** field, enter the username in the format domain\username.

    b. In the **Create BlueXP backup and recovery for VMs credentials** section, enter the local credentials.

       In the **Username** field, enter the local username; do not include the domain details.

       > Make a note of the username and password that you specify. You need to use these credentials if you want to modify BlueXP backup and recovery for VMs configuration later.

    c. Enter credentials for the maint user.
    d. In **Setup Network Properties**, enter the host name.
       i. In **Setup IPv4 Network Properties** section, enter the network information such as IPv4 address, IPv4 Netmask, IPv4 Gateway, IPv4 Primary DNS, IPv4 Secondary DNS, and IPv4 Search Domains.

          > You can skip these steps and leave the entries blank in the Setup Network Properties section, if you want to proceed with DHCP as your network configuration.

    e. In **Setup Date and Time**, select the time zone where the vCenter is located.
14. On the **Ready to complete** page, review the page and click **Finish**.

    All hosts must be configured with IP addresses (FQDN hostnames are not supported). The deploy operation does not validate your input before deploying.

    You can view the progress of the deployment from the Recent Tasks window while you wait for the OVF import and deployment tasks to finish.

    When BlueXP backup and recovery for VMs is successfully deployed, it is deployed as a Linux VM, registered with vCenter, and a VMware vSphere client is installed.

15. Navigate to the VM where BlueXP backup and recovery for VMs was deployed, then click the **Summary** tab, and then click the **Power On** box to start the virtual appliance.
16. While BlueXP backup and recovery for VMs is powering on, right-click the deployed BlueXP backup and recovery for VMs, select **Guest OS**, and then click **Install VMware tools**.

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.

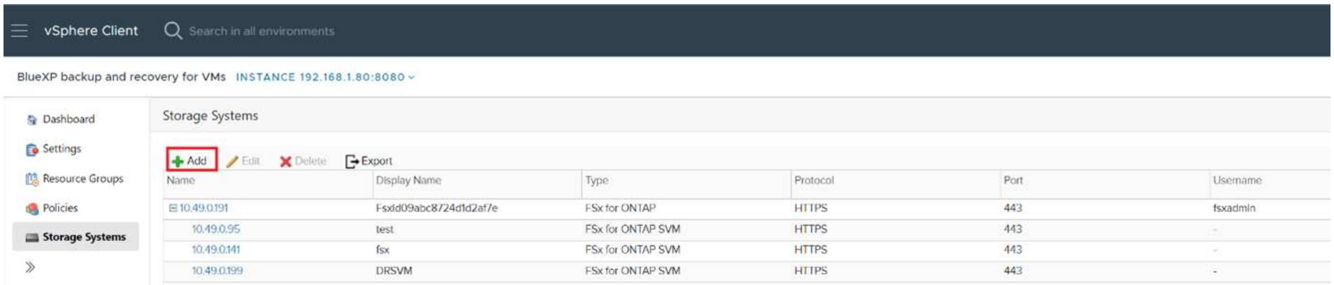
  If you added etc host entries for storage VM names in BlueXP backup and recovery for VMs, you must verify that they are also resolvable from the virtual appliance.

  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**.



Name	Display Name	Type	Protocol	Port	Username
⊟ 10.49.0.191	Fsxid09abc8724d1d2af7e	FSx for ONTAP	HTTPS	443	fsxadmin
10.49.0.95	test	FSx for ONTAP SVM	HTTPS	443	-
10.49.0.141	fsx	FSx for ONTAP SVM	HTTPS	443	-
10.49.0.199	DRSVM	FSx for ONTAP SVM	HTTPS	443	-

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.

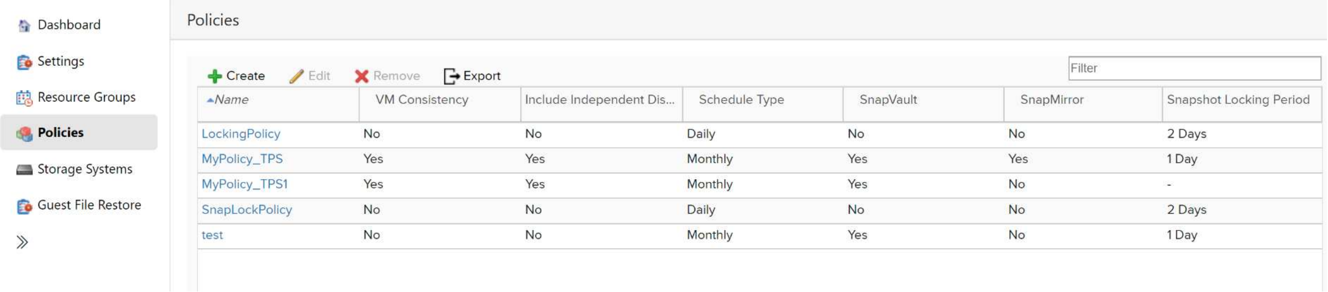
Before you begin

- 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.

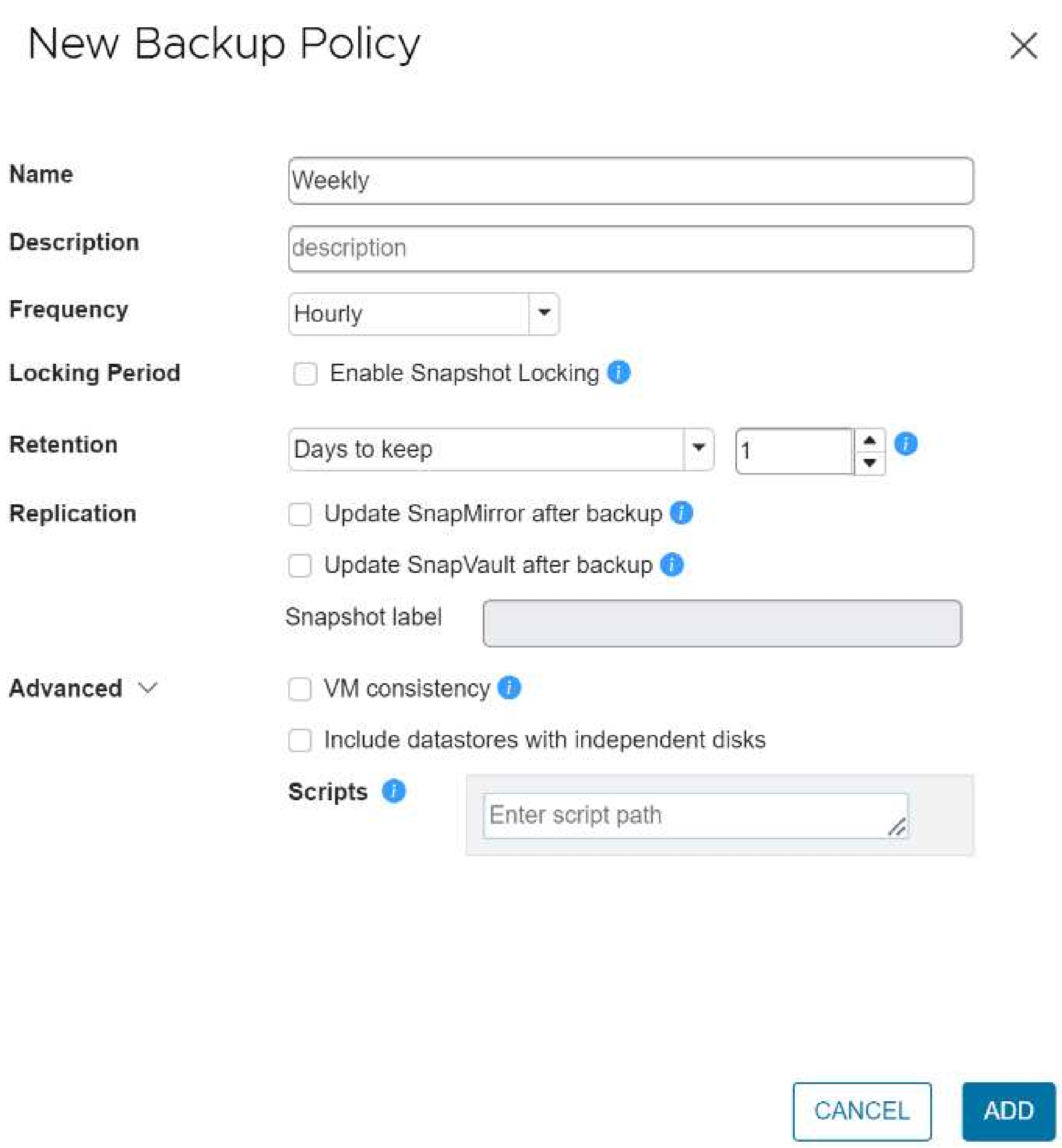


Name	VM Consistency	Include Independent Dis...	Schedule Type	SnapVault	SnapMirror	Snapshot Locking Period
LockingPolicy	No	No	Daily	No	No	2 Days
MyPolicy_TPS	Yes	Yes	Monthly	Yes	Yes	1 Day
MyPolicy_TPS1	Yes	Yes	Monthly	Yes	No	-
SnapLockPolicy	No	No	Daily	No	No	2 Days
test	No	No	Monthly	Yes	No	1 Day

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.



New Backup Policy

Name: Weekly

Description: description

Frequency: Hourly

Locking Period: □ Enable Snapshot Locking

Retention: Days to keep 1

Replication: □ Update SnapMirror after backup

□ Update SnapVault after backup

Snapshot label

Advanced: □ VM consistency

□ Include datastores with independent disks

Scripts: Enter script path

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.

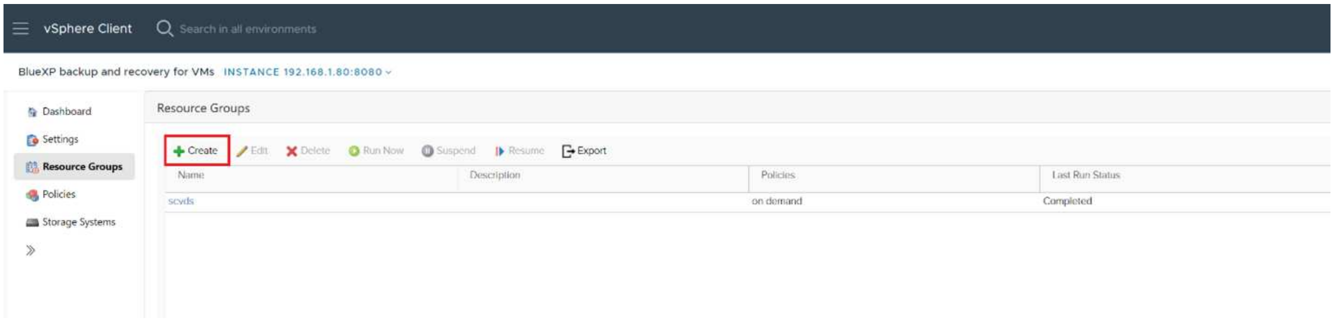
- Compatibility checks

  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.



Name	Description	Policies	Last Run Status
scvds		on demand	Completed

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.

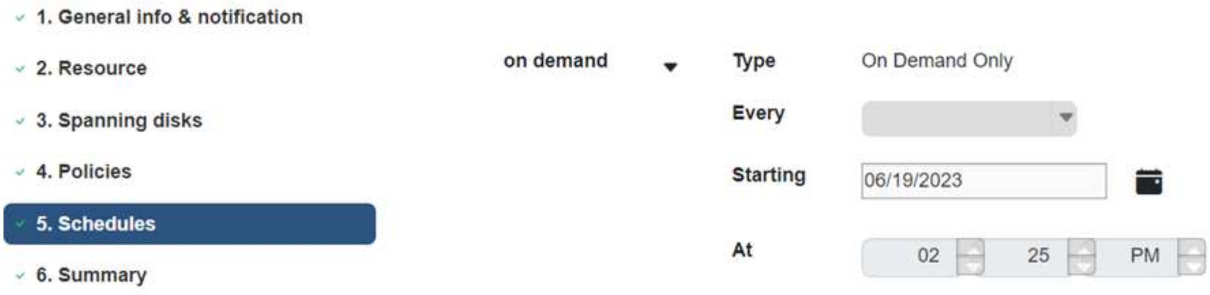
If the message selected <resource-name> is not BlueXP backup and recovery for VMs compatible is displayed, then a selected resource is not compatible with BlueXP backup and recovery for VMs.

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.



on demand

Type: On Demand Only

Every:

Starting: 06/19/2023

At: 02 25 PM

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.

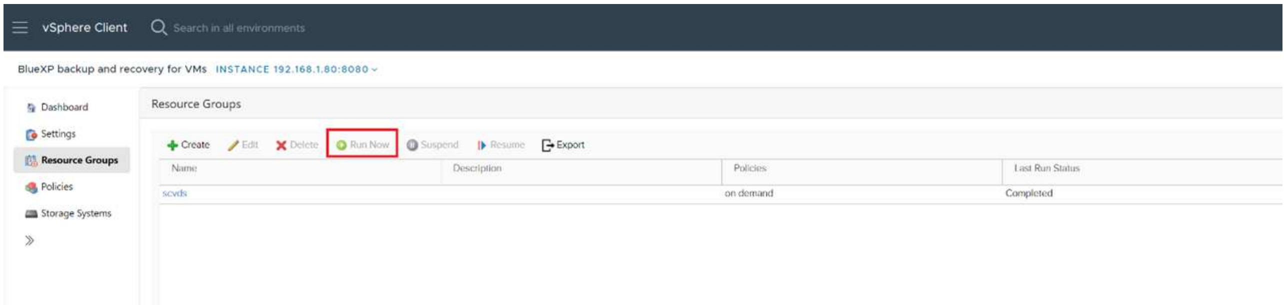
Before you begin

- 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.



Name	Description	Policies	Last Run Status
scvds		on demand	Completed

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.

Mount and unmount datastores

Mount datastores

You can mount a datastore from a backup if you want to access files in the backup.

Before you begin

- Ensure to copy the organization ID and API token from the VMC portal and add them to the VMware Cloud Services settings.
- Ensure alternate ESXi host can connect to the storage

  If you want to mount to an alternate ESXi host, you must ensure that the alternate ESXi host can connect to the storage and has the same UID and GID as that of the original host.

Steps

1. In the VMware vSphere client, navigate to ☰ > **Inventory** > **Storage**.
2. In the left navigator pane, right-click a datastore, then select **BlueXP backup and recovery for VMs** in the drop-down list, and then select **Mount Backup** in the secondary drop-down list.
3. On the **Mount Datastore** page, select a backup and a backup location (primary or secondary), and then click **Mount**.
4. Optional: To verify that the datastore is mounted, in the VMware vSphere client toolbar, click **BlueXP backup and recovery for VMs**.

   The datastore you mounted is displayed in the **Recent Job Activities** tile of the dashboard.

   To prevent new Snapshot copies from being created when you clone the volume, turn off the ONTAP schedule for the SnapVault volume. Previously existing Snapshot copies are not deleted.

Unmount datastores

You can unmount a backup when you no longer need to access the files in the datastore.

Steps

1. In the VMware vSphere client, navigate to ☰ > **Inventory** > **Storage**.
2. In the left navigator pane, right-click a datastore, then select **BlueXP backup and recovery for VMs** in the drop-down list, and then select **Unmount** in the secondary drop-down list.

   > ⓘ Make sure that you select the correct datastore to unmount. Otherwise, you might cause an impact on production work.

3. In the **Unmount Backup** dialog box, select a datastore, select the **Unmount the datastore** checkbox, and click **Unmount**.
4. Optional: To verify that the datastore is unmounted, in the VMware vSphere client toolbar, click **BlueXP backup and recovery for VMs**.

   The datastore you unmounted is displayed in the **Recent Job Activities** tile of the dashboard.

Attach and detach VMDKs

Attach VMDKs to a VM

You can attach one or more VMDKs from a backup to the parent VM, or to an alternate VM on the same ESXi host, or to an alternate VM on an alternate ESXi host managed by the same vCenter or a different vCenter in linked mode.

This makes it easier to restore one or more individual files from a drive instead of restoring the entire drive. You can detach the VMDK after you have restored or accessed the files you need.

About this task

You have the following attach options:

- You can attach virtual disks from a primary or a secondary backup.
- You can attach virtual disks to the parent VM (the same VM that the virtual disk was originally associated with) or to an alternate VM on the same ESXi host.

The following limitations apply to attaching virtual disks:

- Attach and detach operations are not supported for Virtual Machine Templates.
- When more than 15 VMDKs are attached to an iSCSI controller, the virtual machine for BlueXP backup and recovery for VMs cannot locate VMDK unit numbers higher than 15 because of VMware restrictions.

  In this case, add the SCSi controllers manually and try the attach operation again.
- Attach and restore operations connect VMDKs using the default SCSi controller. VMDKs that are attached to a VM with a NVME controller are backed up, but for attach and restore operations they are connected back using a SCSi controller.

Steps

1. In the VMware vSphere client, navigate to ☰ > **Inventory** > **Hosts and Clusters**.
2. In the left navigator pane, right-click a **Virtual Machine**, then select **BlueXP backup and recovery for VMs** in the drop-down list, and then select **Attach Virtual Disk(s)**.
3. On the Attach Virtual Disk window, in the **Backup section**, select a backup.

   You can filter the backup list by selecting the filter icon and choosing a date and time range, selecting whether you want backups that contain VMware Snapshot copies, whether you want mounted backups, and the location. Click OK.
4. In the **Select Disks** section, select one or more disks you want to attach and the location you want to attach from (primary or secondary).

   You can change the filter to display primary and secondary locations.
5. By default, the selected virtual disks are attached to the parent VM. To attach the selected virtual disks to an alternate VM in the same ESXi host, **click Click here to attach to alternate VM** and specify the alternate VM.
6. Click **Attach**.

7. Optional: Monitor the operation progress in the **Recent Tasks** section.

   Refresh the screen to display updated information.

8. Verify that the virtual disk is attached by performing the following:

   a. Click **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.

   b. In the left Navigator pane, right-click a VM, then select **Edit settings** in the drop-down list.

   c. In the **Edit Settings** window, expand the list for each hard disk to see the list of disk files.

      The Edit Settings page lists the disks on the VM. You can expand the details for each hard disk to see the list of attached virtual disks.

Result:
You can access the attached disks from the host operating system and then retrieve the needed information from the disks.

Detach a virtual disk

After you have attached a virtual disk to restore individual files, you can detach the virtual disk from the parent VM.

Steps

1. In the VMware vSphere client, navigate to ☰ > **Inventory** > **Hosts and Clusters**.

2. In the left navigator pane, right-click a **Virtual Machine**, then select **BlueXP backup and recovery for VMs** in the drop-down list, and then select **Detach Virtual Disk(s)**.

3. In the **Detach Virtual Disk** dialog box, select one or more disks you want to detach, then select the **Detach the selected disk(s)** checkbox, and click **Detach**.

4. Optional: Monitor the operation progress in the **Recent Tasks** section.

   Refresh the screen to display updated information.

5. Verify that the virtual disk is detached by performing the following:

   a. Click **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.

   b. In the left Navigator pane, right-click a VM, then select **Edit settings** in the drop-down list.

   c. In the **Edit Settings** window, expand the list for each hard disk to see the list of disk files.

      The Edit Settings page lists the disks on the VM. You can expand the details for each hard disk to see the list of attached virtual disks.

Restore Virtual Machines from Amazon FSx

When you restore a Virtual Machine, you can overwrite the existing content with the backup copy that you select, or you can make a copy of the Virtual Machine.

You can restore VMs to the following locations:

- Restore to original location
  - To the original datastore mounted on the original ESXi host (this overwrites the original VM)
- Restore to alternate location
  - To a different datastore mounted on the original ESXi host
  - To the original datastore mounted on a different ESXi host that is managed by the same vCenter
  - To a different datastore mounted on a different ESXi host that is managed by the same vCenter
  - To a different datastore mounted on a different ESXi host that is managed by a different vCenter in linked mode

Before you begin

- A backup must exist.

  You must have created a backup of the Virtual Machine using BlueXP backup and recovery for VMs before you can restore the Virtual Machine.

  > ⓘ Restore operations cannot finish successfully if there are Snapshot copies of the Virtual Machine that were performed by software other than BlueXP backup and recovery for VMs.

- The Virtual Machine must not be in transit.

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

- HA configuration errors.

  Ensure there are no HA configuration errors displayed on the vCenter ESXi Host Summary screen before restoring backups to a different location.

About this task

- Virtual Machine is unregistered and registered again.

  The restore operation for Virtual Machines unregisters the original Virtual Machine, restores the Virtual Machine from a backup Snapshot copy, and registers the restored Virtual Machine with the same name and configuration on the same ESXi server. You must manually add the Virtual Machines to resource groups after the restore.

- Restoring datastores

  You cannot restore a datastore, but you can restore any Virtual Machine in the datastore.

- VMware consistency snapshot failures for a Virtual Machine.

  Even if a VMware consistency snapshot for a Virtual Machine fails, the Virtual Machine is nevertheless backed up. You can view the entities contained in the backup copy in the Restore wizard and use it for restore operations.

Steps

1. In the VMware vSphere client toolbar, click **Host and Clusters**, and then select the storage system.
2. In the left Navigator pane, right-click a **Virtual Machine**, then select **BlueXP backup and recovery for VMs** in the drop-down list, and then select **Restore** to start the wizard.
3. In the **Restore** wizard, on the **Select Backup** page, select the backup Snapshot copy that you want to restore.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by clicking the filter icon and selecting a date and time range, selecting whether you want backups that contain VMware Snapshots, whether you want mounted backups, and the location. Click **OK** to return to the wizard.

4. On the **Select Scope** page, select **Entire Virtual Machine** in the **Restore scope** field, then select the restore location, and then enter the destination information where the backup should be mounted.

   In the VM name field, if the same VM name exists, then the new VM name format is '<vm_name>_<timestamp>'.

   When restoring partial backups, the restore operation skips the **Select Scope** page.

5. Enable **Restart VM** checkbox if you want the Virtual Machine to be powered on after the restore operation.
6. On the **Select Location** page, select the location for the restored datastore.
7. Review the **Summary** page and then click **Finish**.
8. **Optional**: Monitor the operation progress by clicking **Recent Tasks** at the bottom of the screen.

After you finish

- Add restored Virtual Machines to resource groups.

  Ensure that the newly restored VM is protected. If it is not, protect it by manually adding the restored VM to the appropriate resource groups.

Access REST APIs using the Swagger API web page

REST APIs are exposed through the Swagger web page. You can access the Swagger web page to display the BlueXP backup and recovery for VMs REST APIs.

Before you begin

For BlueXP backup and recovery for VMs REST APIs, you must know either the IP address or the host name of the BlueXP backup and recovery for VMs appliance.

> ⓘ The plug-in only supports REST APIs for the purpose of integrating with third party applications and does not support PowerShell cmdlets or a CLI.

Steps

1. From a browser, enter the URL to access the plug-in Swagger web page:

   https://<OVA_IP>/api/swagger-ui/index.html

   > ⓘ Do not use the following characters in the REST API URL: +, . , %, and &.

   Example

   Access BlueXP backup and recovery for VMs REST APIs:

   https://<OVA_IP>/api/swagger-ui/index.html

   Log in use the vCenter authentication mechanism to generate the token.

2. Click an API resource type to display the APIs in that resource type.

Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes Service for Google Cloud

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account serial number (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in BlueXP).

  This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

  These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

Register BlueXP for NetApp support

To register for support and activate support entitlement, one user in your BlueXP organization (or account) must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

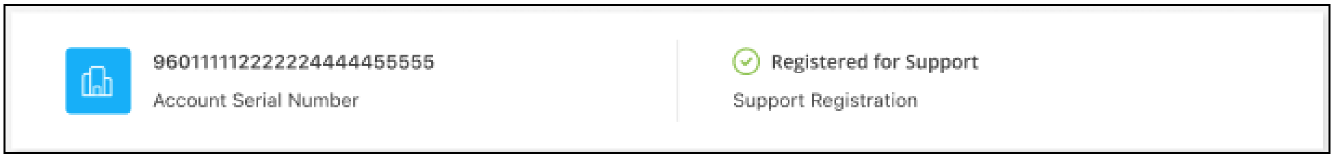
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

   The **Resources** page should show that your BlueXP organization is registered for support.

   960111112222224444455555
   Account Serial Number

   ✓ Registered for Support
   Support Registration

   Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP organization is not registered for support. As long as one user in the organization has followed these steps, then your organization has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

Steps

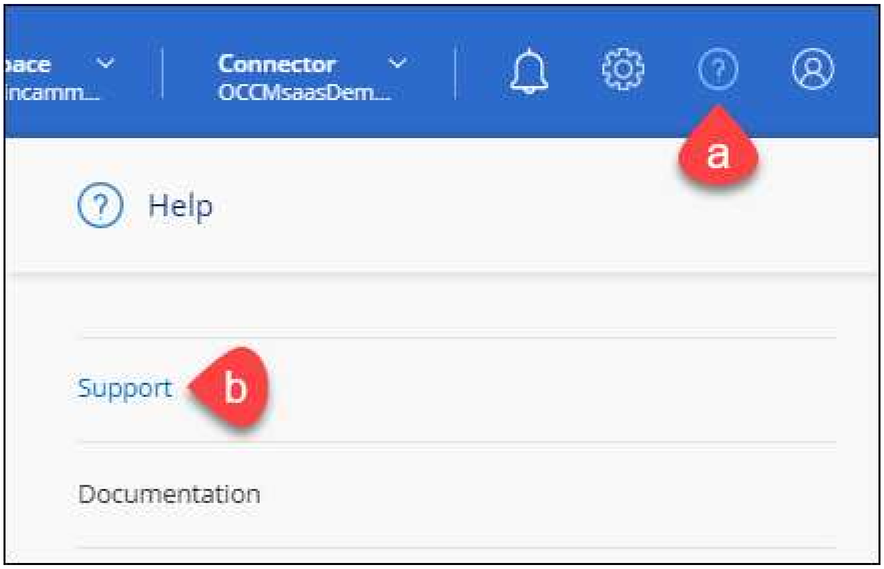
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Brand new to NetApp

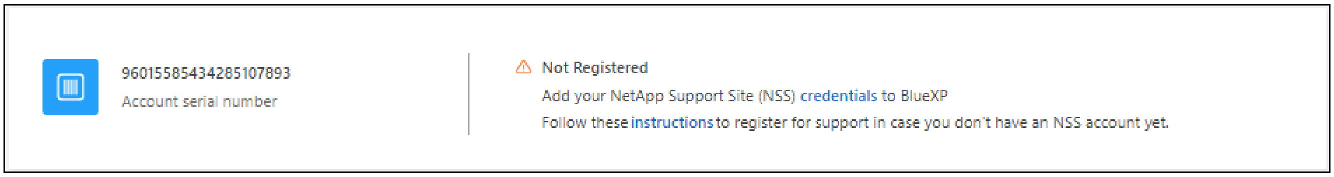
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



96015585434285107893

Account serial number

⚠ Not Registered

Add your NetApp Support Site (NSS) credentials to BlueXP

Follow these instructions to register for support in case you don't have an NSS account yet.

3. Navigate to NetApp's support registration site and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

   Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP organization is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

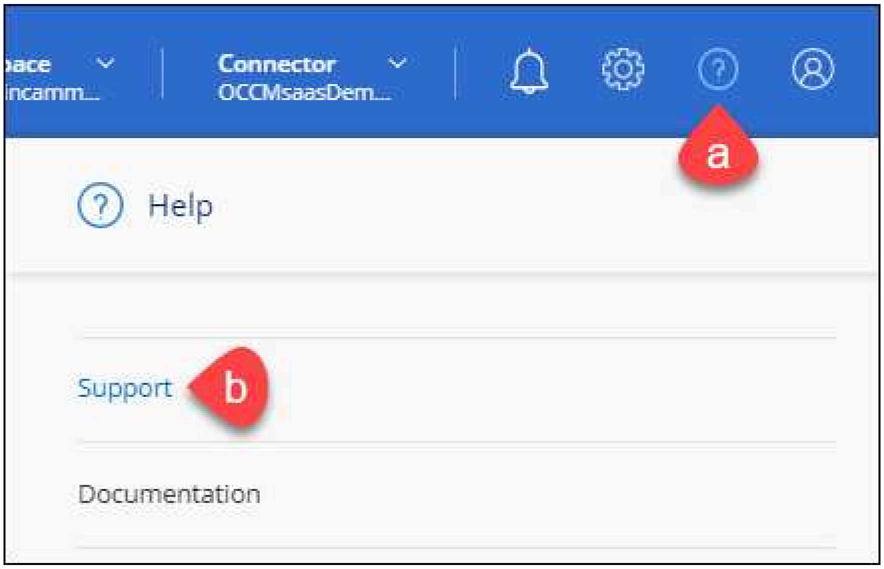
Associating NSS credentials with your BlueXP organization is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP organization ID. Users who belong to the BlueXP organization can access these credentials from **Support > NSS Management**.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   - The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
   - There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

     "The NSS customer type is not allowed for this account as there are already NSS Users of different type."

     The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

   - Upon successful login, NetApp will store the NSS user name.

    This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

  - If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu.

    Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes Service for Google Cloud

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- Documentation

  The BlueXP documentation that you’re currently viewing.

- Knowledge base

  Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the BlueXP community to follow ongoing discussions or create new ones.

Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. Learn how to manage credentials associated with your BlueXP login.
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be associated with the serial number for that system.

Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:

    a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.

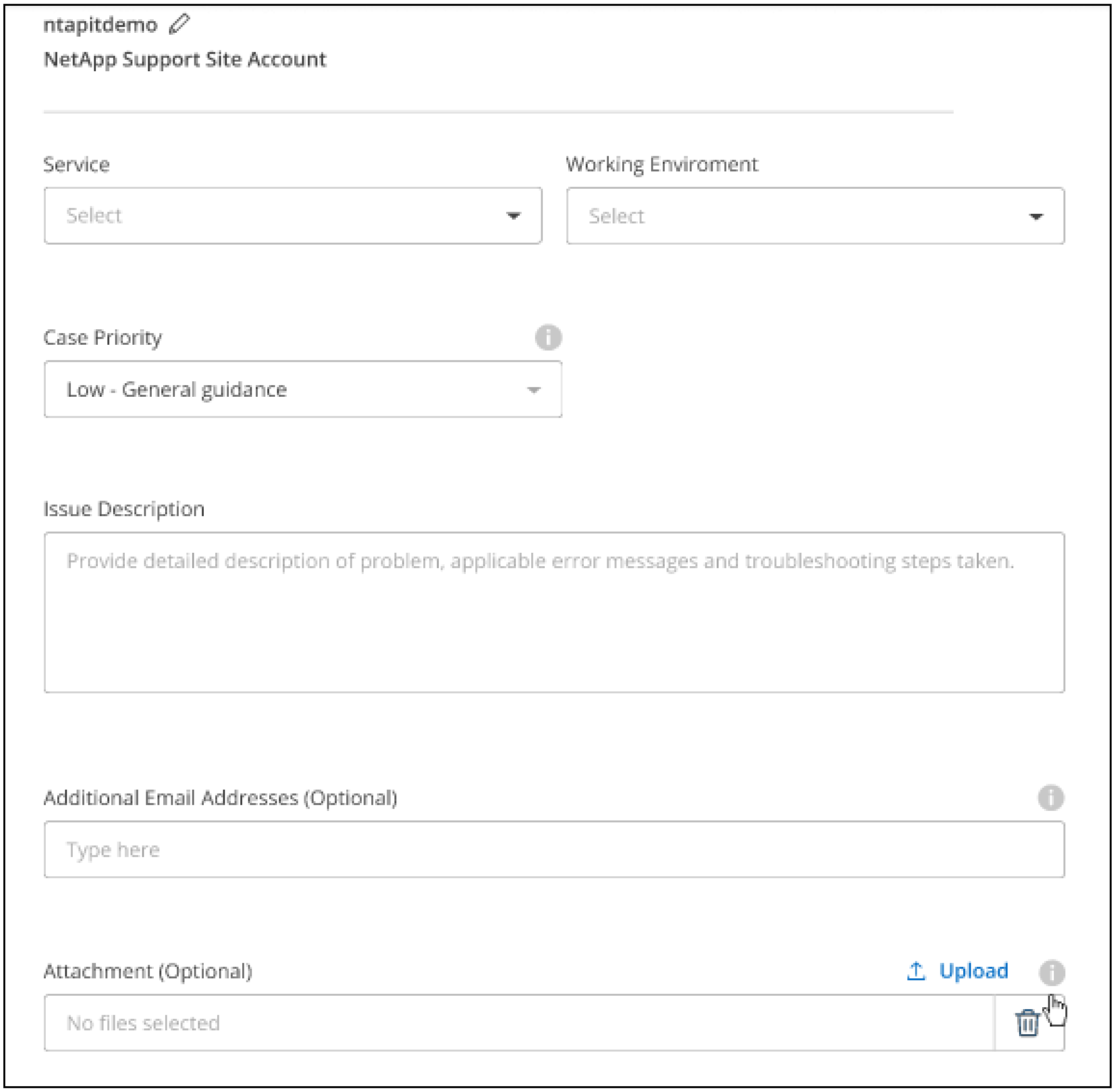
    b. Select **Create a Case** to open a ticket with a NetApp Support specialist:

    - **Service**: Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
    - **Working Environment**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

      The list of working environments are within scope of the BlueXP organization (or account), project (or workspace), and Connector you have selected in the top banner of the service.
    - **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

      To learn more details about these priorities, hover your mouse over the information icon next to the field name.
    - **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
    - **Additional Email Addresses**: Enter additional email addresses if you'd like to make someone else aware of this issue.
    - **Attachment (Optional)**: Upload up to five attachments, one at a time.

      Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.



ntapitdemo

NetApp Support Site Account

Service: Select

Working Enviroment: Select

Case Priority: Low - General guidance

Issue Description: Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional): Type here

Attachment (Optional): No files selected

After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It’s possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it’s associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

  The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

  View the steps below for more details.

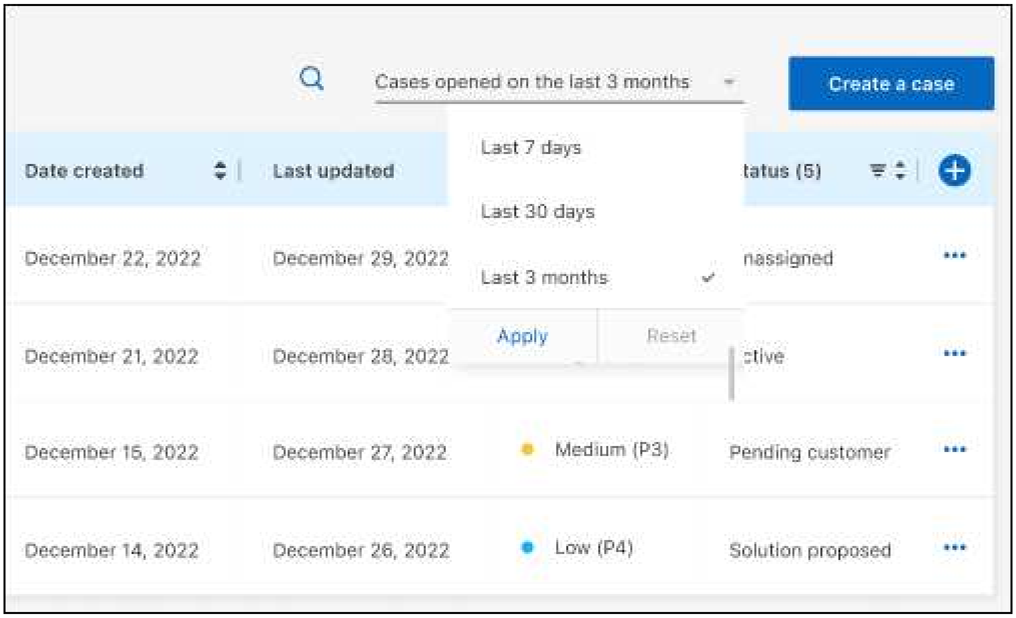
- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

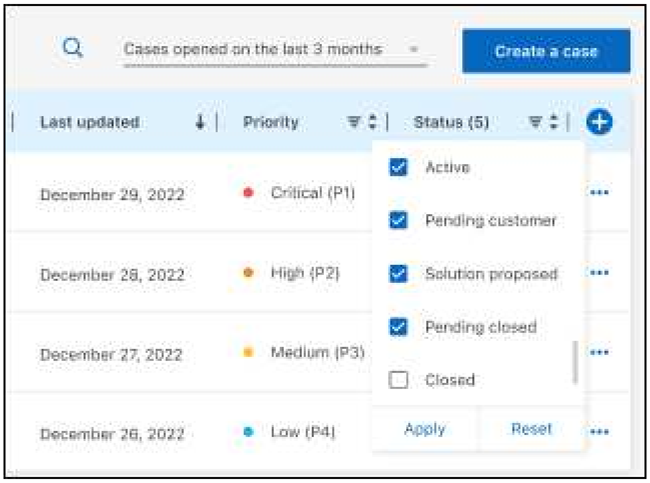
   The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
   - Under **Organization's cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.



Date created	Last updated		tatus (5)
December 22, 2022	December 29, 2022		nassigned
December 21, 2022	December 28, 2022		ctive
December 15, 2022	December 27, 2022	● Medium (P3)	Pending customer
December 14, 2022	December 26, 2022	● Low (P4)	Solution proposed

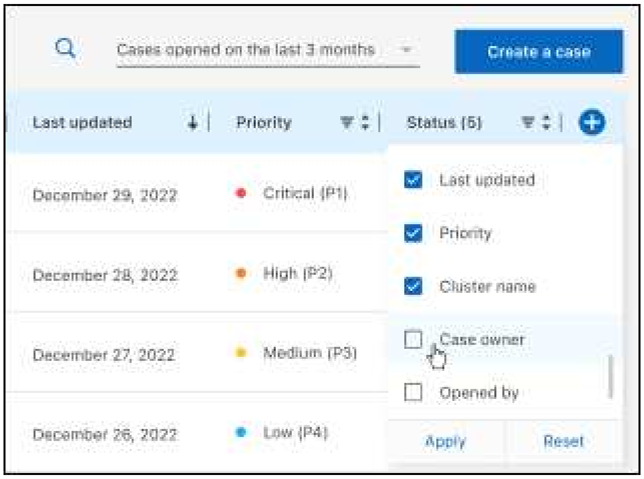
- Filter the contents of the columns.



Last updated	Priority	Status (5)
December 29, 2022	● Critical (P1)	
December 28, 2022	● High (P2)	
December 27, 2022	● Medium (P3)	
December 26, 2022	● Low (P4)	

☑ Active
☑ Pending customer
☑ Solution proposed
☑ Pending closed
□ Closed

- Change the columns that appear in the table by selecting ⊕ and then choosing the columns that you'd like to display.



Last updated	Priority	Status (5)
December 29, 2022	● Critical (P1)	
December 28, 2022	● High (P2)	
December 27, 2022	● Medium (P3)	
December 26, 2022	● Low (P4)	

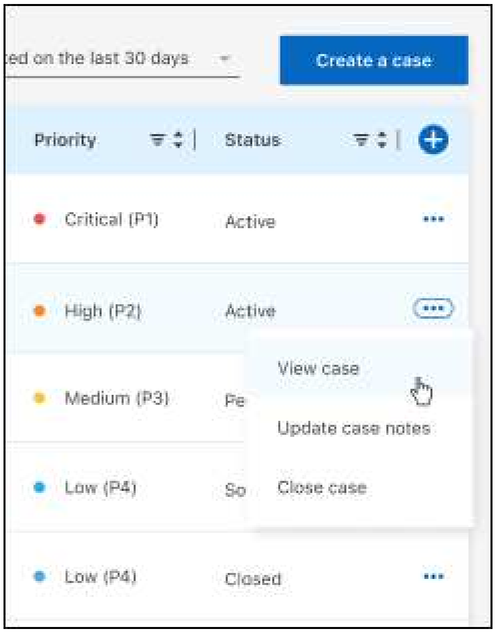
☑ Last updated
☑ Priority
☑ Cluster name
□ Case owner
□ Opened by

4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **View case**: View full details about a specific case.
   - **Update case notes**: Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

   - **Close case**: Provide details about why you're closing the case and select **Close case**.



Priority	Status
Critical (P1)	Active
High (P2)	Active
Medium (P3)	Pe
Low (P4)	So
Low (P4)	Closed

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Copyright information

Trademark information