Back up and restore on-premises applications data

BlueXP backup and recovery

NetApp
June 14, 2024

Table of Contents

Back up and restore on-premises applications data

Protect your on-premises applications data

BlueXP backup and recovery for applications provides data protection capabilities for application consistent Snapshots from on-premises ONTAP primary to cloud provider.

You can back up Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL, and PostgreSQL applications data from on-premises ONTAP systems to Amazon Web Services, Microsoft Azure, Google Cloud Platform, and StorageGRID.

For more information about BlueXP backup and recovery for applications, refer to:

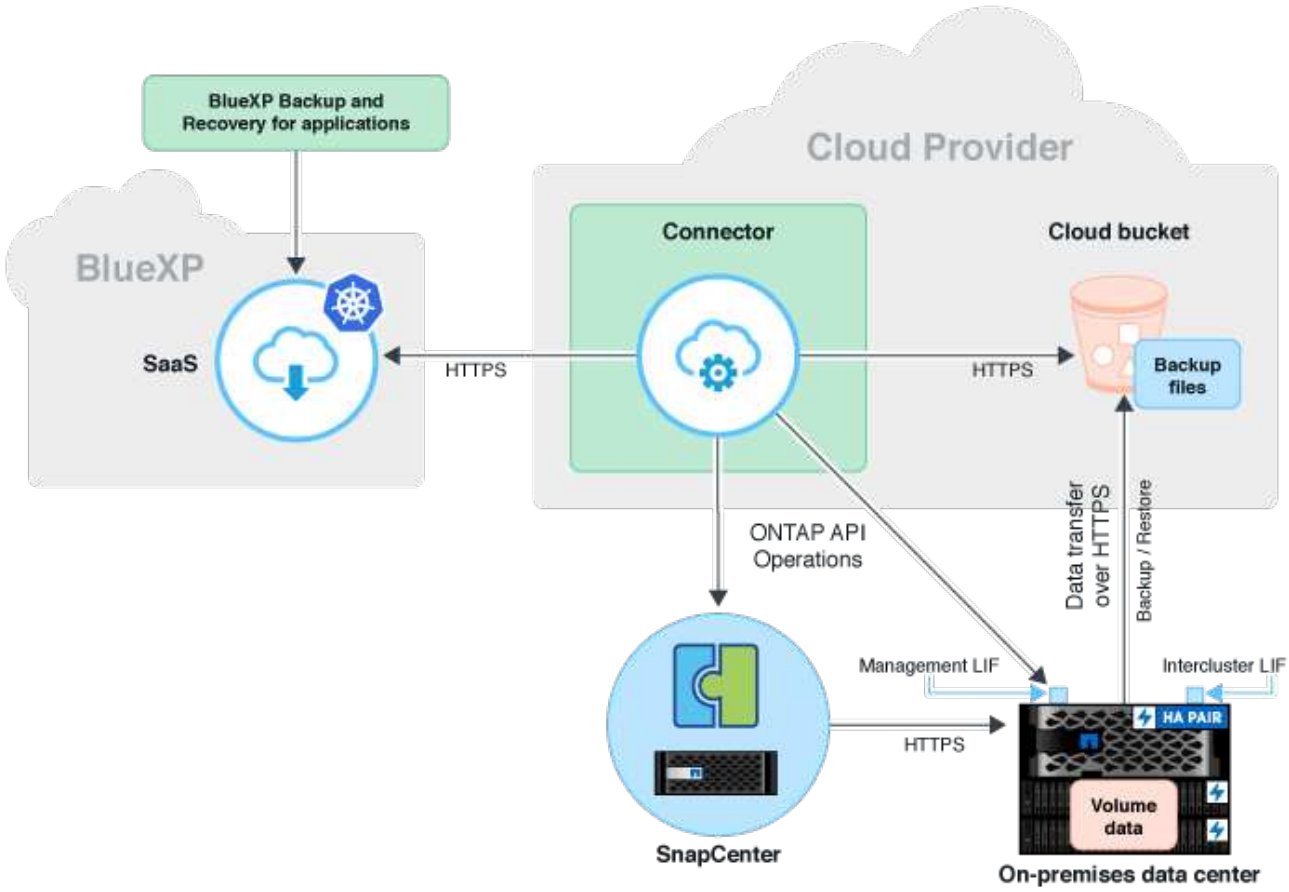
- Application aware backup with BlueXP backup and recovery and SnapCenter
- BlueXP backup and recovery for applications podcast

Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up application data to cloud provider.

- ONTAP 9.8 or later
- BlueXP
- SnapCenter Server 4.6 or later
  - You should be using SnapCenter Server 4.7 or later if you want to use the following features:
    - Protect backups from on-premises secondary storage
    - Protect SAP HANA applications
    - Protect Oracle and SQL applications that are on VMware environment
    - Storage export of a backup
    - Deactivate backups
    - Unregister SnapCenter Server
  - You should be using SnapCenter Server 4.9 or later if you want to use the following features:
    - Mount Oracle database backups
    - Restore to the alternate storage
  - You should be using SnapCenter Server 4.9P1 if you want to protect MongoDB, MySQL, and PostgreSQL applications
- At least one backup per application should be available in SnapCenter Server
- At least one daily, weekly, or monthly policy in SnapCenter with no label or same label as that of the policy in BlueXP

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



Register SnapCenter Server

Only a user with SnapCenterAdmin role can register the host on which SnapCenter Server 4.6 or later is running. You can register multiple SnapCenter Server hosts in BlueXP.

Steps

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

      You should ensure that the port is open for communication to happen between SnapCenter Server and BlueXP.

   c. In the Tags field, specify a site name, city name, or any custom name with which you want to tag the SnapCenter Server.

      The tags are comma separated.

d. In the Username and Password field, specify the credentials of the user with SnapCenterAdmin role.

5. Select the Connector from the **Connector** drop-down.
6. Click **Register**.

After you finish

Click **Backup & Restore** > **Applications** to view all the applications that are protected using the registered SnapCenter Server host. By default, the applications are automatically discovered every day midnight.

The supported applications and their configurations are:

- Oracle database:
  - Full backups (data + log) created with at least one daily, weekly, or monthly schedules
  - SAN, NFS, VMDK-SAN, VMDK-NFS, and RDM
- Microsoft SQL Server database:
  - Standalone, failover cluster instances, and availability groups
  - Full backups created with at least one daily, weekly, or monthly schedules
  - SAN, VMDK-SAN, VMDK-NFS, and RDM
- SAP HANA database:
  - Single Container 1.x
  - Multiple Database Container 2.x
  - HANA System Replication (HSR)

    You should have at least one backup on both primary and secondary sites. You can decide to do a pro-active failure or a deferred failover to the secondary.

  - Non-data Volumes (NDV) resources such as HANA binaries, HANA archive log volume, HANA shared volume, and so on
- MongoDB
- MySQL
- PostgreSQL

The following databases are not displayed:

- Databases that have no backups
- Databases that have only on-demand or hourly policy
- Oracle databases residing on NVMe

Create a policy to back up applications

You should create a policy to back up the application data to cloud.

Before you begin

- If you want to move backups from object store to archival storage, ensure that you are using the required ONTAP version.
  - If you are using Amazon Web Services, you should be using ONTAP 9.10.1 or later

- If you are using Microsoft Azure, you should be using ONTAP 9.10.1 or later
- If you are using Google Cloud, you should be using ONTAP 9.12.1 or later
- If you are using StorageGrid, you should be using ONTAP 9.12.1 or later

- You should configure the archive access tier for each cloud provider.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. From the Settings drop-down, click **Policies** > **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.
7. Click **Create**.

You cannot edit or delete a policy, which is associated with an application.

Back up on-premises applications data to Amazon Web Services

Complete a few steps to back up the applications data from ONTAP to Amazon Web Services.

BlueXP supports data lock and ransomware protection. If ONTAP cluster is running on ONTAP 9.11.1 or later and if you have not configured archival storage, you can protect the backups from overwriting, deletion, and ransomware threats.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application 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 applications, it can be reused for all the other applications residing on the same ONTAP cluster.

   a. Select the SVM and click **Add Working Environment**.
   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.

      BlueXP backup and recovery for applications only support cluster admin.

c. Click **Add Working Environment**.

5. Select **Amazon Web Services** as the cloud provider.
   a. Specify the AWS account.
   b. In the AWS Access Key field, specify the key.
   c. In the AWS Secret Key field, specify the password.
   d. Select the region where you want to create the backups.
   e. Specify the IP space.
   f. Select the archival tier if you have configured archival storage in the policy.

      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. Configure data lock and ransomware protection.
7. Review the details and click **Activate Backup**.

Back up on-premises applications data to Microsoft Azure

Complete a few steps to back up the applications data from ONTAP to Microsoft Azure.

BlueXP supports data lock and ransomware protection. If ONTAP cluster is running on ONTAP 9.12.1 or later and if you have not configured archival storage, you can protect the backups from overwriting, deletion, and ransomware threats.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application 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 applications, it can be reused for all the other applications residing on the same ONTAP cluster.

   a. Select the SVM and click **Add Working Environment**.
   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.

         BlueXP backup and recovery for applications only support cluster admin.

   c. Click **Add Working Environment**.

5. Select **Microsoft Azure** as the cloud provider.
   a. Specify the Azure subscription ID.
   b. Select the region where you want to create the backups.
   c. Either create a new resource group or use an existing resource group.

d. Specify the IP space.

e. Select the archival tier if you have configured archival storage in the policy.

   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. Configure data lock and ransomware protection.
7. Review the details and click **Activate Backup**.

Back up on-premises applications data to Google Cloud Platform

Complete a few steps to back up the applications data from ONTAP to Google Cloud Platform.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application 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 applications, it can be reused for all the other applications residing on the same ONTAP cluster.

   a. Select the SVM and click **Add Working Environment**.
   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.

      BlueXP backup and recovery for applications only support cluster admin.

   c. Click **Add Working Environment**.
5. Select **Google Cloud Platform** 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.
   f. 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 on-premises applications data to StorageGRID

Complete a few steps to back up the applications data from ONTAP to StorageGRID.

BlueXP supports data lock and ransomware protection. If ONTAP cluster is running on ONTAP 9.11.1 or later, StorageGRID systems are 11.6.0.3 or later, and if you have not configured archival storage, you can protect the backups from overwriting, deletion, and ransomware threats.

Before you begin

When backing up data to StorageGRID, a Connector must be available on your premises. You will either need to install a new Connector or make sure that the currently selected Connector resides on-prem. The Connector can be installed in a site with or without internet access.

For information, see Create Connectors for StorageGRID.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application 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 applications, it can be reused for all the other applications residing on the same ONTAP cluster.

   a. Select the SVM and click **Add Working Environment**.
   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.

      BlueXP backup and recovery for applications only support cluster admin.
   c. Click **Add Working Environment**.
5. Select **StorageGRID**.
   a. Specify the FQDN of the StorageGRID Server and the port on which the StorageGRID server is running.

      Enter the details in the format FQDN:PORT.
   b. In the Access Key field, specify the key.
   c. In the Secret Key field, specify the password.
   d. Specify the IP space.
   e. Specify the archival tier if you have configured archival storage in the policy.

If you select…	Perform the following…
AWS	1. Either select the StorageGrid from the drop-down or add the StorageGrid cluster. 2. Specify the AWS account. 3. In the AWS Access Key field, specify the key. 4. In the AWS Secret Key field, specify the password. 5. Select the region where you want to create the backups. 6. Click **Save**.
Azure	1. Either select the StorageGrid cluster from the drop-down or add the cluster. 2. Specify the Azure subscription ID. 3. Select the region where you want to create the backups. 4. Either create a new resource group or use an existing resource group. 5. Click **Save**.

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. Configure data lock and ransomware protection.
7. Review the details and click **Activate Backup**.

Manage protection of applications

You can manage protection of applications by viewing policies, viewing backups, viewing the changes to database layout, policies, and resource group, and monitoring all the operations from the BlueXP UI.

View policies

You can view all the policies. For each of these policies, when you view the details all the associated applications are listed.

Steps

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

   The associated applications are listed.

You cannot edit or delete a policy, which is associated with an application.

You can also view cloud extended SnapCenter policies, by running the `Get-SmResources` cmdlet in SnapCenter.
The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command name.

View backups on cloud

You can view the backups on cloud in the BlueXP UI.

Steps

1. Click **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application and click **View Details**.

The time taken for the backups to be listed depends on ONTAP's default replication schedule.

- For Oracle databases, both data and log backups, system change number (SCN) for each backup, end date for each backup are listed. You can select only the data backup and restore the database to original location. You can mount the data backup and log backup to alternate location.
- For Microsoft SQL Server databases, only the full backups and the end date for each backup are listed. You can select the backup and restore the database to original or alternate location.
- For Microsoft SQL Server instance, backups of the databases under that instance is listed.
- For SAP HANA databases, only the data backups and the end date for each backup are listed. You can select the backup and perform storage export on a given host.
- For MongoDB, MySQL, and PostgreSQL, only the data backups and the end date for each backup are listed. You can select the backup and perform storage export on a given host.

The backups created before enabling cloud protection are not listed for restore.

You can also view these backups by running the `Get-SmBackup` cmdlet in SnapCenter.
The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command name.

Deactivate backup

You can delete all the backups that are moved to object store from both SnapCenter and the object store.

Steps

1. Click **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application and click Deactivate Backup.

   By default the check box is selected and it deletes all the backups that are moved to object store from both SnapCenter and the object store.

   If you clear the checkbox, the backups are retained only in the object store but these backups cannot be used for application level restore. Later when you activate the backup for this application, the backups retained in object store are not listed for restore.

3. Click **Deactivate Backup**.

Database layout change

When volumes are added to the database, SnapCenter Server labels the snapshots on the new volumes automatically as per the policy and the schedule. These new volumes will not have the object store endpoint and you should refresh the volumes by executing the following steps:

Steps

1. Click **Backup and recovery** > **Applications**.
2. From the **Settings** drop-down, click **SnapCenter Servers**.
3. Click ••• corresponding to the SnapCenter Server hosting the application and click **Refresh**.

   The new volumes are discovered.

4. Click ••• corresponding to the application and click **Refresh Protection** to enable cloud protection for the new volume.
   - If a storage volume is added to the application after configuring the cloud provider, SnapCenter Server labels the snapshots for new backups on which the application is residing.
   - You should manually delete the object store relationship if the removed volume is not used by any other applications.
   - If you update the application inventory, it will contain the current storage layout of the application.

Policy or resource group change

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

Steps

1. Click **Backup and recovery** > **Applications**.
2. Click ••• corresponding to the application and click **Refresh Protection**.

Unregister SnapCenter Server

Steps

1. Click **Backup and recovery** > **Applications**.
2. From the **Settings** drop-down, click **SnapCenter Servers**.
3. Click ••• corresponding to the SnapCenter Server and click **Unregister**.

   By default the check box is selected and it deletes all the backups that are moved to object store from both SnapCenter and the object store.

   If you clear the checkbox, the backups are retained only in the object store but these backups cannot be used for application level restore. Later when you activate the backup for this application, the backups retained in object store are not listed for restore.

Monitor Jobs

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

Steps

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.

Configure CA Certificates

You can configure CA signed certificate if you want to include additional security to your environment.

Configure SnapCenter CA signed certificate in BlueXP Connector

You should configure SnapCenter CA signed certificate in BlueXP Connector so that the Connector can verify the SnapCenter's certificate.

Before you begin

You should run the following command in the BlueXP Connector to get the <*base_mount_path*>:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Steps

1. Log in to the Connector.
   `cd <base_mount_path> mkdir -p server/certificate`
2. Copy the root CA and intermediate CA files to the *<base_mount_path>/server/certificate* directory.

   The CA files should be in .pem format.

3. If you have CRL files, perform the following steps:
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Copy the CRL files to the *<base_mount_path>/server/crl* directory.
4. Connect to the cloudmanager_snapcenter and modify the enableCACert in config.yml to true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert: false/enableCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Restart cloudmanager_snapcenter container.
   `sudo docker restart cloudmanager_snapcenter`

Configure CA signed certificate for BlueXP Connector

If 2way SSL is enabled in SnapCenter, you should perform the following steps on the Connector to use the CA certificate as the client certificate when the Connector is connecting with the SnapCenter.

Before you begin

You should run the following command to get the *<base_mount_path>*:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Steps

1. Log in to the Connector.
   `cd <base_mount_path> mkdir -p client/certificate`
2. Copy the CA signed certificate and key file to the *<base_mount_path>/client/certificate* in the Connector.

   The file name should be certificate.pem and key.pem. The certificate.pem should have the entire chain of the certificates like intermediate CA and root CA.

3. Create the PKCS12 format of the certificate with the name certificate.p12 and keep at *<base_mount_path>/client/certificate*.

   Example: openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12

4. Connect to the cloudmanager_snapcenter and modify the sendCACert in config.yml to true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert: false/sendCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Restart cloudmanager_snapcenter container.
   `sudo docker restart cloudmanager_snapcenter`
6. Perform the following steps on the SnapCenter to validate the certificate sent by the Connector.
   a. Login to the SnapCenter Sever host.
   b. Click **Start** > **Start Search**.
   c. Type mmc and press **Enter**.
   d. Click **Yes**.
   e. In File menu, click **Add/Remove Snap-in**.
   f. Click **Certificates** > **Add** > **Computer account** > **Next**.
   g. Click **Local computer** > **Finish**.
   h. If you have no more snap-ins to add to the console, click **OK**.
   i. In the console tree, double-click **Certificates**.
   j. Right-click the **Trusted Root Certification Authorities store**.
   k. Click **Import** to import the certificates and follow the steps in the **Certificate Import Wizard**.

Restore on-premises applications data

Restore Oracle database

You can restore Oracle database either to the original location or to the alternate location. For a RAC database, the data is restored to the on-premises node where the backup was created.

Only full database with control file restore is supported. If the archive logs are not present in the AFS, you should specify the location that contains the archive logs required for recovery.

Single File Restore (SFR) is not supported.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. In the **Filter By** field, select the filter **Type** and from the drop-down select **Oracle**.
3. Click **View Details** corresponding to the database that you want to restore and click **Restore**.
4. In the Restore options page, specify the location where you want to restore the database files.

If you…	Do this…
Want to restore to the original location	1. Select **Restore to original location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. Click **Next**. 4. Select **Database State** if you want to change the state of the database to the state required to perform restore and recovery operations. The various states of a database from higher to lower are open, mounted, started, and shutdown. ◦ If the database is in a higher state but the state must be changed to a lower state to perform a restore operation, you must select this check box. ◦ If the database is in a lower state but the state must be changed to a higher state to perform the restore operation, the database state is changed automatically even if you do not select the check box. ◦ If a database is in the open state, and for restore the database needs to be in the mounted state, then the database state is changed only if you select this check box. 5. Specify the recovery scope. ◦ Select **All Logs** if you want to recover to the last transaction. ◦ Select **Until SCN (System Change Number)** if you want to recover to a specific SCN. ◦ Select **Date and Time** if you want to recover to a specific data and time. You must specify the date and time of the database host's time zone. ◦ Select **No recovery** if you do not want to recover. 6. If the archive logs are not present in the active file system, you should specify the location that contains the archive logs required for recovery. 7. Select the check box if you want to open the database after recovery. In a RAC setup, only the RAC instance that is used for recovery is opened after recovery.

If you…	Do this…
Want to temporarily restore to another storage and then copy the restored files to the original location	1. Select **Restore to original location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. Select **Change storage location**. If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume. 4. Click **Next**. 5. In the Storage mapping page, specify the alternate storage location details where the data restored from the object store will be stored temporarily. If you select an on-premises ONTAP system and if you haven not configured the cluster connection to the object storage, you are prompted for additional information regarding the object store. 6. Click **Next**. 7. Select **Database State** if you want to change the state of the database to the state required to perform restore and recovery operations. The various states of a database from higher to lower are open, mounted, started, and shutdown. ◦ If the database is in a higher state but the state must be changed to a lower state to perform a restore operation, you must select this check box. ◦ If the database is in a lower state but the state must be changed to a higher state to perform the restore operation, the database state is changed automatically even if you do not select the check box. ◦ If a database is in the open state, and for restore the database needs to be in the mounted state, then the database state is changed only if you select this check box. 8. Specify the recovery scope. ◦ Select **All Logs** if you want to recover to the last transaction. ◦ Select **Until SCN (System Change Number)** if you want to recover to a specific SCN. Select **Date and Time** if you want to recover

If you…	Do this…
Want to restore to an alternate location	1. Select **Restore to alternate location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. If you want to restore to alternate storage, perform the following: a. Select **Change storage location**. If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume. b. Click **Next**. c. In the Storage mapping page, specify the alternate storage location details where the data from the object store needs to be restored. 4. Click **Next**. 5. In the Destination host page, select the host on which the database will be mounted. a. (Optional) For NAS environment, specify the FQDN or IP address of the host to which the volumes restored from object store are to be exported. b. (Optional) For SAN environment, specify the initiators of the host to which LUNs of the volumes restored from object store are to be mapped. 6. Click **Next**.

5. Review the details and click **Restore**.

The **Restore to alternate location** option mounts the selected backup on the given host. You should manually bring up the database.

After mounting the backup, you cannot mount it again until it is unmounted. You can use the **Unmount** option from the UI to unmount the backup.

For information on how to bring up the Oracle database see, Knowledge base article.

Restore SQL Server database

You can restore SQL Server database either to the original location or to the alternate location.

Single File Restore (SFR), Recovery of log backups, and reseed of availability groups are not supported.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. In the **Filter By** field, select the filter **Type** and from the drop-down select **SQL**.
3. Click **View Details** to view all the available backups.
4. Select the backup and click **Restore**.
5. In the Restore options page, specify the location where you want to restore the database files.

If you…	Do this…
Want to restore to the original location	1. Select **Restore to original location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. Click **Next**.
Want to temporarily restore to another storage and then copy the restored files to the original location	1. Select **Restore to original location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. Select **Change storage location**. If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume. 4. Click **Next**. 5. In the Storage mapping page, specify the alternate storage location details where the data restored from the object store will be stored temporarily. 6. Click **Next**.

If you…	Do this…
Want to restore to an alternate location	1. Select **Restore to alternate location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. Click **Next**. 4. In the Destination host page, select a host name, provide a database name (optional), select an instance, and specify the restore paths. ⓘ The file extension provided in the alternate path must be same as the file extension of the original database file. 5. Click **Next**.
Want to temporarily restore to another storage and then copy the restored files to the alternate location	1. Select **Restore to alternate location**. 2. If the snapshot is in archival storage, select the priority to restore your data from the archival storage. 3. Select **Change storage location**. If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume. 4. Click **Next**. 5. In the Storage mapping page, specify the alternate storage location details where the data restored from the object store will be stored temporarily. 6. Click **Next**. 7. In the Destination host page, select a host name, provide a database name (optional), select an instance, and specify the restore paths. ⓘ The file extension provided in the alternate path must be same as the file extension of the original database file. 8. Click **Next**.

6. In the **Pre-operations** select, select one of the following options:
   - Select **Overwrite the database with same name during restore** to restore the database with the same name.
   - Select **Retain SQL database replication settings** to restore the database and retain the existing replication settings.
7. In the **Post-operations** section, to specify the database state for restoring additional transactional logs, select one of the following options:
   - Select **Operational, but unavailable** if you are restoring all of the necessary backups now.

     This is the default behavior, which leaves the database ready for use by rolling back the uncommitted transactions. You cannot restore additional transaction logs until you create a backup.
   - Select **Non-operational, but available** to leave the database non-operational without rolling back the uncommitted transactions.

     Additional transaction logs can be restored. You cannot use the database until it is recovered.
   - Select **Read-only mode, and available** to leave the database in read-only mode.

     This option undoes uncommitted transactions, but saves the undone actions in a standby file so that recovery effects can be reverted.

     If the Undo directory option is enabled, more transaction logs are restored. If the restore operation for the transaction log is unsuccessful, the changes can be rolled back. The SQL Server documentation contains more information.
8. Click **Next**.
9. Review the details and click **Restore**.

Restore SAP HANA database

You can restore SAP HANA database to any host.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. In the **Filter By** field, select the filter **Type** and from the drop-down select **HANA**.
3. Click **View Details** corresponding to the database that you want to restore and click **Restore**.
4. In the Restore options page, specify one of the following:
   a. For NAS environment, specify the FQDN or IP address of the host to which the volumes restored from object store are to be exported.
   b. For SAN environment, specify the initiators of the host to which LUNs of the volumes restored from object store are to be mapped.
5. If the snapshot is in archival storage, select the priority to restore your data from the archival storage.
6. If there is not enough space on the source storage or the source storage is down, select **Change storage location**.

   If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume.

7. Click **Next**.
8. In the Storage mapping page, specify the alternate storage location details where the data restored from the object store will be stored.
9. Click **Next**.
10. Review the details and click **Restore**.

This operation does only the storage export of the selected backup on the given host. You should manually mount the filesystem and bring up the database. After utilizing the volume, the storage Administrator can delete the volume from the ONTAP cluster.

For information on how to bring up the SAP HANA database see, TR-4667: Overview of SAP system copy workflow with SnapCenter and TR-4667: Overview of SAP system clone workflow with SnapCenter.

Restore MongoDB, MySQL, and PostgreSQL databases

You can restore MongoDB, MySQL, and PostgreSQL databases to any host.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. In the **Filter By** field, select the filter **Type** and from the drop-down select **MongoDB**, **MySQL**, or **PostgreSQL**.
3. Click **View Details** corresponding to the database that you want to restore and click **Restore**.
4. In the Restore options page, specify one of the following:
   a. For NAS environment, specify the FQDN or IP address of the host to which the volumes restored from object store are to be exported.
   b. For SAN environment, specify the initiators of the host to which LUNs of the volumes restored from object store are to be mapped.
5. If the snapshot is in archival storage, select the priority to restore your data from the archival storage.
6. If there is not enough space on the source storage or the source storage is down, select **Change storage location**.

   If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume.
7. Click **Next**.
8. In the Storage mapping page, specify the alternate storage location details where the data restored from the object store will be stored.
9. Click **Next**.
10. Review the details and click **Restore**.

This operation does only the storage export of the selected backup on the given host. You should manually mount the filesystem and bring up the database. After utilizing the volume, the storage Administrator can delete the volume from the ONTAP cluster.

Copyright information

Trademark information