Back up and restore on-premises applications data

Cloud Backup

NetApp
June 20, 2022

Table of Contents

Back up and restore on-premises applications data

Protect your on-premises applications data

You can integrate Cloud Backup for Applications with Cloud Manager and on-premises SnapCenter to back up the application consistent Snapshots from on-premises ONTAP to cloud. When required you can restore from cloud to on-premises SnapCenter Server.

You can back up Oracle and Microsoft SQL applications data from on-premises ONTAP systems to the following cloud providers:

- Amazon Web Services
- Microsoft Azure

You should be using SnapCenter Software 4.6.

For more information about Cloud Backup for Applications, refer to:

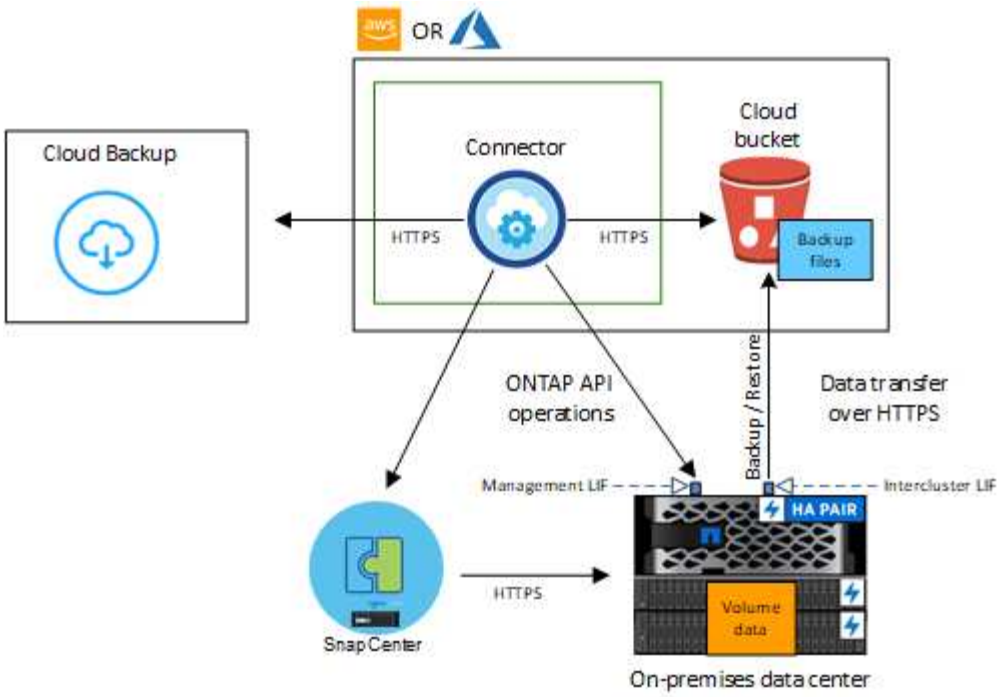
- Application aware backup with Cloud Backup and SnapCenter
- Cloud backup for applications

Requirements

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

- ONTAP 9.8 or later
- Cloud Manager 3.9
- SnapCenter Server 4.6
- 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 Cloud Backup for Applications policy in Cloud Manager.

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



Protection Policies

You should use the one of the policies defined in Cloud Backup for Applications to back up the application data to cloud.

Custom policies are not supported.

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

The labels and retention value of these policies can be modified using the REST API until the policy is associated with an application. Only one policy can be associated with an application and once associated, you cannot dissociate.

In addition to the Cloud Backup for Applications policies, you would also need at least one SnapCenter policy to back up the application data to cloud.

Back up on-premises applications data to cloud

You can back up the applications data from ONTAP to cloud by integrating Cloud Backup for Applications with Cloud Manager and on-premises SnapCenter.

Register SnapCenter Server

Only a user with SnapCenterAdmin role can register the host on which SnapCenter Server 4.6 is running. You can register multiple SnapCenter Server hosts but once registered, you cannot remove the SnapCenter Server host.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **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 is running.

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

   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. Click **Register**.

After you finish

Click **Backup & Restore** > **Applications** to view all the applications that are protected using the registered SnapCenter Server host.

For SQL Server databases, the Application Name column displays the name in *application_name (host name)* format. When you search by providing the name in *application_name (host name)* format, the SQL Server database details are not displayed.

The supported applications and their configurations are:

- Oracle database: Full backups (data + log) created with at least one daily, weekly, or monthly schedules.
- Microsoft SQL Server database:
  - Standalone, failover cluster instances, and availability groups
  - Full backups created with at least one daily, weekly, or monthly schedules

The following Oracle and SQL Server databases will not be displayed:

- Databases that have no backups
- Databases that have only on-demand or hourly policy
- Databases residing on RDM or VMDK

Back up applications data

You can protect one or more applications simultaneously to the cloud using a single policy. Only the default pre-canned policies can be assigned to protect the application.

> ⓘ You can protect only one application at a time if you are using the Cloud Manager GUI. However, if you are using REST APIs, you can protect multiple applications simultaneously.

If you are protecting an SQL Server instance, then cloud protection will be configured for all the volumes of the eligible databases in that instance.
If you are protecting an SQL Server availability group, then cloud protection will be configured for all the volumes of the databases in that availability group. However, based on the backup preference, the Snapshot will be copied form the respective volumes.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **Applications**.
2. Click ••• corresponding to the application and click **Activate Backup**.
3. Add the working environment.

   Configure the ONTAP cluster that hosts the SVM on which the application is running. 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 ONTAP cluster.
      ii. Specify the admin credentials.

      Cloud Backup for Applications supports only cluster admin.
   c. Click **Add Working Environment**.

   > ⓘ You should not proceed until the working environment details are updated. It might take up to 30 minutes for the working environment details to be updated. After 30 minutes, you should close the wizard and retry from step 1 to view the working environment details.
   > After retrying if the working environment details are not updated, ensure that you have added the right working environment.

4. Select and configure the cloud provider.

Configure Amazon Web Services

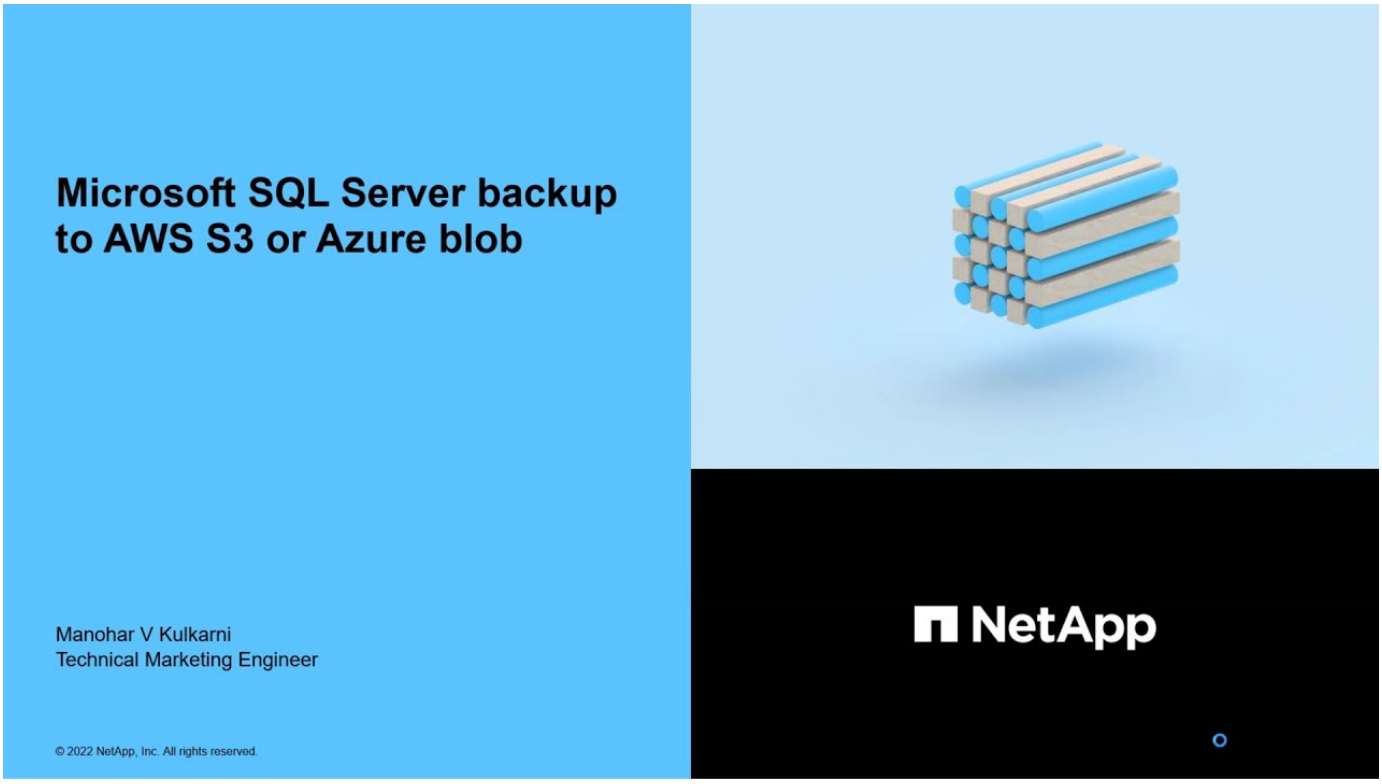
a. Specify the AWS account.
b. In the AWS Access Key field, specify the key.
c. In the AWS Secret Key field, specify the password.
d. Select the region where you want to create the backups.
e. Specify the IP addresses of the ONTAP clusters that were added as the working environments.

Configure Microsoft Azure

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 addresses of the ONTAP clusters that were added as the working environments.

5. In the Assign Policy page, select the policy and click **Next**.
6. Review the details and click **Activate Backup**.

The following video shows a quick walkthrough of protecting a database:



Manage protection of applications

You can view the policies and backups. Depending upon the change in database, policies, or resource groups, you can refresh the updates from the Cloud Manager UI.

View policies

You can view all the default pre-canned policies. For each of these policies, when you view the details all the associated Cloud Backup for Applications policies and all the associated applications are listed.

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

   The associated Cloud Backup for Applications policies and all the applications are listed.

   You should not delete the Cloud Backup for Applications policies.

You can also view cloud extended SnapCenter policies, by running the `Get-SmResources` SnapCenter cmdlet.
The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command_name. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

View backups on cloud

You can view the backups on cloud in the Cloud Manager UI.

1. Click **Backup & Restore** > **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 (maximum of 1 hour) and Cloud Manager (maximum of 6 hours).

- For Oracle databases, both data and log backups, SCN number for each backup, end date for each backup are listed. You can select only the data backup and restore the database to on-premises SnapCenter Server.
- 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 on-premises SnapCenter Server.
- For Microsoft SQL Server instance, backups are not listed instead only the databases under that instance is listed.

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

You can also view these backups by running the `Get-SmBackup` SnapCenter cmdlet.
The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command_name. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

Database layout change

When volumes are added to the database, SnapCenter Server will label 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 by executing the following steps:

1. Click **Backup & Restore** > **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 removed from the application after configuring the cloud service, for new backups SnapCenter Server will only label the snapshots on which the application is residing. If the removed volume is not used by any other applications, then you should manually delete the object store relationship.
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.

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

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.

1. Click **Backup & Restore** > **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

If you have CA certificates, you should manually copy the root CA certificates to the connector machine.

However, if you do not have CA certificates, you can proceed without configuring CA certificates.

Steps

1. Copy the certificate to the volume that can be accessed from the docker agent.
   - `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_certs`
   - `chmod 777 sc_certs`
2. Copy the RootCA certificate files to the above folder on the connector machine.

   ```
   cp <path on connector>/<filename>
   /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
   ```

3. Copy the CRL file to the volume which can be accessed from the docker agent.

- `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl`
- `chmod 777 sc_crl`

4. Copy the CRL files to the above folder on the connector machine.

```
cp <path on connector>/<filename>
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_crl
```

5. After copying the certificates and CRL files, restart the Cloud Backup for Apps service.
   - `sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation: true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-agent/config/config.yml`
   - `sudo docker restart cloudmanager_snapcenter`

Restore applications data

Restore Oracle database

You can only restore the Oracle database to the same SnapCenter Server host, same SVM, or to the same database host. For a RAC database, the data will be 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.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **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. On the Restore Type page, perform the following actions:
   a. Select **Control files** if you want to restore control file along with full database.
   b. Select **Change database state if needed for restore and recovery** 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. You must select this check box if the database is in a higher state but the state must be changed to a lower state to perform a restore operation. 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. On the Recovery Scope page, perform the following actions:
   a. Specify the recovery scope.

If you…	Do this…
Want to recover to the last transaction	Select **All Logs**.
Want to recover to a specific System Change Number (SCN)	Select **Until SCN (System Change Number)**.
Want to recover to a specific data and time	Select **Date and Time**. You must specify the date and time of the database host's time zone.
Do not want to recover	Select **No recovery**.
Want to specify any external archive log locations	If the archive logs are not present in the AFS, you should specify the location that contains the archive logs required for recovery.

b. 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.

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

Restore SQL Server database

You can restore SQL Server database either to the same host or to the alternate host. Recovery of log backups and reseed of availability groups are not supported.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **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. Select the location where you want to restore the database files.

Option	Description
Restore the database to the same host where the backup was created	Select this option if you want to restore the database to the same SQL server where the backups are taken.

Option	Description
Restore the database to an alternate host	Select this option if you want the database to be restored to a different SQL server in the same or different host where backups are taken. 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. If the **Restore the database to an alternate host** option is not displayed in the Restore Scope page, clear the browser cache.

6. On the **Pre Restore Options** page, 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. On the **Post Restore Options** page, 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. Review the details and click **Restore**.