Protect your data using the SnapCenter Service 1.0

Manage SAP HANA Systems

NetApp
January 2021

Learn about the SnapCenter Service

The SnapCenter Service allows you to create application consistent backups and restore data using those backups. The SnapCenter Service is enabled on the Cloud Manager and you can use the SnapCenter Service UI from the Cloud Manager to protect your SAP HANA systems residing on Cloud Volumes Service (CVS) for Google Cloud Platform (GCP).

Get Started

Requirements

- Create a Cloud Manager user account and the workspace

  For information on how to create a Cloud Manager user account and workspace, see: https://docs.netapp.com/us-en/occm/task_setting_up_cloud_central_accounts.html

- Create a connector in GCP project that can communicate with the SAP HANA system.

  For information on how to create a connector, see: https://docs.netapp.com/us-en/occm/task_creating_connectors_gcp.html#setting-up-gcp-permissions-to-create-a-connector

- Set the required permissions to create Google Kubernetes Engine (GKE) cluster for hosting the SnapCenter Service.

Required permissions to create GKE cluster

Before you enable the SnapCenter Service from Cloud Manager, you should ensure that your GCP service account that is set up for the SnapCenter Service has the required permissions.

The required permissions are as follows:

- container.clusterRoleBindings.create
- container.clusterRoles.bind
- container.clusters.create
- container.clusters.delete
- container.clusters.update
- container.clusters.get
- container.clusters.getCredentials
- container.clusters.list
- container.operations.get
-container.namespaces.create
-container.namespaces.update
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.firewalls.update
- compute.globalOperations.get
- compute.instances.get
- compute.networks.updatePolicy
- compute.instances.list
- compute.instances.setMetadata
- compute.projects.get
- compute.projects.setCommonInstanceMetadata
- compute.zoneOperations.get
- compute.zones.list

- iam.serviceAccounts.actAs
- iam.serviceAccounts.get
- iam.roles.get
- resourcemanager.projects.getIamPolicy
- compute.subnetworks.use
- container.namespaces.get

For shared VPC

1. Create a custom role in the host project using the following permissions:

   - compute.firewalls.create
   - compute.firewalls.get
   - compute.firewalls.list
   - compute.firewalls.update
   - compute.globalOperations.get
   - compute.networks.updatePolicy
   - compute.subnetworks.get

2. Get the service account created in service project to deploy SnapCenter services.
3. Add the service account in the host project from Access->IAM
4. Add custom role to the service account created in step1.

For more information on creating and managing roles and service accounts, see:

- Create a role in GCP
- Create a GCP Service account and apply the custom role

Limitations

The following features are not available in this preview release of the SnapCenter Service.

- Upgrading from Beta1 to Beta2
- High Availability of SAP HANA plug-in
- NTP Proxy
- Google Kubernetes Engine (GKE) private cluster
- Backing up the SnapCenter Service metadata
- Large number of concurrent backups

Enable the SnapCenter Service

You can enable the SnapCenter Service using the Cloud Manager UI. When the SnapCenter Service is enabled, a Google Kubernetes Engine (GKE) cluster is created in your cloud environment to host the SnapCenter Service.

Before you begin:

If the connector has shared VPC configured, you should create at least two secondary CIDR ranges in the subnet for the Pod and service addresses.

Steps:

1. Log into Cloud Manager.
2. Select the connector that has the network connectivity to the SAP HANA systems to be protected.

The SnapCenter Service will be hosted in the same project as that of the Connector

3. Add the working environment hosting the SAP HANA system Cloud Volumes Service.

   See Set up Cloud Volumes Service for Google Cloud.

4. Click **All Services > SnapCenter > Enable**.
5. On the Cluster Configuration page, perform the following:
   i. (Optional) If you are using a private cluster, specify the cluster IP address range.
   ii. If the connector you selected has a shared VPC configured, select the Pod secondary and services secondary CIDR range from the drop-down.

   Depending on the connector selected, the SnapCenter Service will list the Pod and services CIDR range. You should ensure that the same CIDR range is not selected for Pod and services.

   iii. Select the cluster configuration.
      - If you select **High Availability**, a Google Kubernetes Engine (GKE) cluster with 3 working nodes across 3 zones will be created.
      - If you select Non-High Availability, a GKE cluster with single node will be created.

   iv. Click **Continue**.
6. After the SnapCenter Service is successfully deployed, click **Finish**.

   The GKE cluster details can be obtained by clicking .

   Note: If the deployment fails, the system will be automatically rolled back to original state.

Install the HDBSQL client

After enabling the SnapCenter Service, install the HDBSQL client to perform data protection operations on SAP HANA databases. The HDBSQL client is used to communicate with the SAP HANA systems.

The HDBSQL client is automatically downloaded from the SAP account to your local machine. You should copy it to the mount path, and then install.

Steps:

1. Click **Connector** to obtain the connector name.
2. In the GCP, click **Compute Engine > VM Instances** and search for the connector VM.
3. Select the connector and click **SSH**.
4. Click > Upload file.
5. Select the **HDB_CLIENT_LINUX_X86_64.tar.gz** file from your local machine and select **Open**.

   The file is uploaded to **/home/<username>**.

6. Copy the file to the mount path by running:

   sudo cp /home/<username>/HDB_CLIENT_LINUX_X86_64.tar.gz /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/

7. Install the HDBSQL client by running:

   docker exec -it cloudmanager_snapcenter /bin/bash /opt/netapp/hdbclient/hdbclient.sh HDB_CLIENT_LINUX_X86_64.tar.gz

Add SAP HANA systems

Manually add the SAP HANA systems. Auto discovery of SAP HANA system is not supported.

While adding the SAP HANA systems, you should add the HDB user store keys. The HDB secure user store key is used to store the connection information of SAP HANA systems securely on the client and HDBSQL client uses the secure user store key to connect to SAP HANA systems.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems** > **Add**.
2. On the System Details page, perform the following actions:
   i. Select the system type.
   ii. Specify the unique ID of the SAP HANA system.
   iii. Specify the SAP HANA system name.
   iv. Click HDB Secure User Store Keys text box to add user store keys details.

   Specify the key name, system details, username, and password.

   Note: If you are adding a multi-host SAP HANA system, click + to add user store keys for each host.
3. Click **Continue**.
4. On the Storage Footprint page, select the working environment, specify the region, select all the volumes, and click **Add Storage**.
5. Review all the details specified and then click **Continue**.

You can also edit or remove the SAP HANA systems that were added to the SnapCenter Service.

When you remove a SAP HANA system, all the associated backups will be deleted and no longer be protected.

Add non-data volumes

After adding the multitenant database container or single container type SAP HANA system, you can add the non-data volumes of the HANA system.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

   All the systems added to the SnapCenter Service are displayed.
2. Click ⋯ corresponding to the multitenant database container or single container type system to which you want to add the non-data volumes.
3. Click **Add Non-Data Volumes**.
4. Click **Add New Storage**.
5. Select the working environment, specify the region, select all the volumes, and click **Add Storage**.

The **Add Non-Data Volumes** option is not available if non-data volumes are already added to the multitenant database container or single container database. If you want to add more non-data volumes, click **Edit System** > **Add Storage**.

Back up SAP HANA systems

Create backup policies

Policies specify the backup type, backup frequency, schedules, retention type, retention count, and other characteristics of data protection operations. You can create policies using the Cloud Manager UI.

By default, two system-defined policies, one each for snapshot-based and file-based backup operations are available.

Steps:

1. On the SnapCenter Service page, click **Policies** > **Add**.
2. On the Create Backup Policy page, perform the following actions:
    - Specify a policy name.
    - Select the type of backup you want to create using this policy.
    - Specify the backup name.

      The suffix timestamp is added by default. You can select the other suffixes that should be included in the backup name and define the order in which the suffixes should appear.
    - Specify the schedule frequency and the start and end time for the scheduled backups.
    - Specify the number of snapshot copies to be retained or specify the days for which the snapshot copies should be retained.
3. Click **Add**.

You can view, edit, or delete policies by clicking ⋯ corresponding to the policy.

Create on-demand backups

Create on-demand backups of SAP HANA systems either by associating a policy or by not associating any policy.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

   All the systems added to the SnapCenter Service are displayed.
2. Click ⋯ corresponding to the system that you want to protect.
3. Click **On-Demand Backup**.
4. On the On-Demand Backup page, perform one of the following actions:
    - If you want to associate the backup to a policy, select the policy and click **Create Backup**.
    - If you do not want to associate the backup to a policy, perform the following actions:
        i. In the **Policy** field, select **None**.
        ii. Select the backup type.

            If you are backing up a non-data volume, you can only select **Snapshot Based** as the backup type.
        iii. Specify the retention period.
        iv. Click **Create Backup**.

Create scheduled backups

Create scheduled backups by associating policies with the SAP HANA system.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

   The systems added to the SnapCenter Service is displayed.
2. Click ⋯ corresponding to the system that you want to protect.
3. Click **Protect**.
4. Select the policies that you want to use to protect the SAP HANA system.
5. Click **Protect**.

Restore SAP HANA systems

In the event of data loss, restore the SAP HANA system from one of the backups of that system.

Only storage restore is supported. You should put the HANA system in recovery mode before restoring because HANA system recovery is not supported.

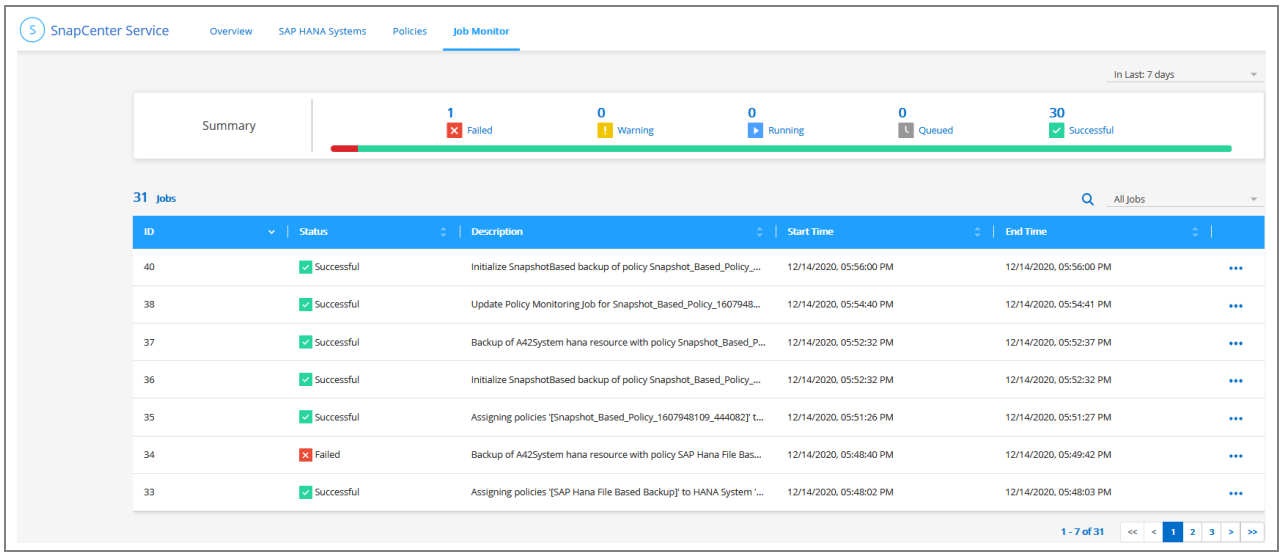
Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

   The systems added to the SnapCenter Service are displayed.
2. Click ⋯ corresponding to the system that you want to restore.
3. Click **View Backups**.
4. In the Backups section, click ⋯ corresponding to the backup that you want to use to restore the system.
5. Click **Restore**.
6. Review the message and select **Yes, Restore** to confirm.

Monitor jobs

Click **Job Monitor** on the SnapCenter Service page to view the status of the jobs. The Job Monitor page displays an overall summary and lists all the jobs. You can then click ⋯ corresponding to a particular job to view the details.



View dashboard

Click **Overview** on the SnapCenter Service page to view the protection summary, configuration details, and job status.