Protect your data using SnapCenter Service 1.0

Manage SAP HANA Systems

NetApp
November 2020

Learn about SnapCenter Service

SnapCenter Service allows you to create application consistent backups and restore data using those backups. SnapCenter Service is enabled on the Cloud Manager and you can use 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 can deploy 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*
- *compute.firewalls.create*
- *compute.firewalls.delete*
- *compute.firewalls.get*
- *compute.firewalls.list*
- *compute.firewalls.update*
- *compute.globalOperations.get*
- *compute.instances.get*
- *compute.networks.updatePolicy*
- *iam.serviceAccounts.actAs*
- *iam.serviceAccounts.get*
- *iam.roles.get*
- *resourcemanager.projects.getIamPolicy*

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 SnapCenter Service.

- High availability
- NTP Proxy
- Deleting the SAP HANA system that were added for protection
- File-based backup
- Retention scenarios
    - Cleaning up of backups while performing volume-based snapshot restore
    - Cleaning up of backups while editing a policy or unassigning a policy from the backup
    - Deleting file-based backups
- Large number of concurrent backups

Enable 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.

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:
    1. (Optional) If you are using a private cluster, specify the cluster IP address range.
    2. Select **Non-High Availability** to create a GKE cluster with single node.
    3. Click **Continue**.
6. After the SnapCenter Service is successfully deployed, click **Finish**.

Install HDBSQL client and create HDB secure user store key

After enabling SnapCenter Service, install the HDBSQL client and create the HDB secure user store key to perform data protection operations on SAP HANA databases.

The HDBSQL client is used to communicate with the SAP HANA systems. 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.

1. Install the HDBSQL client
2. Create HDB secure user store key

Install the HDBSQL client

You should download the HDBSQL client from the SAP account, copy it to the GKE cluster node, and then install.

Steps:

1. Click to obtain the GKE cluster details and copy the name of the cluster.
2. In the Google Cloud Platform (GCP), click **Google Kubernetes Engine** and search using the name of the cluster.
3. Connect to that GKE cluster in GCP.
4. Obtain the GKE cluster node by running:

   kubectl get nodes -n snapcenter
5. Upload the **HDB_CLIENT_LINUX_X86_64.tar.gz** file to the GKE node using GCP.
6. In the GCP, click **Compute Engine > VM Instances** and search for the GKE node.
7. Select the node and click **SSH**.
8. In the SSH console, change the directory to "**/tmp**".
9. Click > Upload file.
10. Select the **HDB_CLIENT_LINUX_X86_64.tar.gz** file from your local machine.

    The file is uploaded to **/home/<username>**.
11. Copy the file to the **/tmp** path by running:

    sudo cp /home/<username>/HDB_CLIENT_LINUX_X86_64.tar.gz /tmp
12. Install the HDBSQL client by running:

    kubectl exec -it sc-hana-plugin-0 -n snapcenter -- /bin/sh/tmp/hdbclient/hdbclient-setup.sh

Create HDB secure user store key

Create the HDB secure user store key by running:

kubectl exec -it -n snapcenter sc-hana-plugin-0 -- hdbuserstore set USERSTOREKEY <hana-db-host>:3<NN>13 <username> <password>

where, <NN> is the SAP instance number.

- For HANA tenant databases and HANA system databases in multi-tenant system, the port number is *3<NN>13*.
- For HANA single tenant databases, the port number is *3<NN>15*.

Several commands are available to manage the connection information stored in the user store. See https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.02/en-US/ddbdd66b632d4fe7b3c2e0e6e341e222.html?q=hdbuserstore for more information.

Add SAP HANA systems

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

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems** > **Add**.
2. On the System Details page, select the type of system you want to add and specify the details.
    - Select **Multitenant Database Container** and specify the SID, user store keys, and system name.
    - Select **Single Container** and specify the SID, user store keys, and system name.
    - Select **Shared Non-Data Volume** and specify the associated SIDs and system name.
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 the SAP HANA systems that were added to SnapCenter Service.

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 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**.

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 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 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.

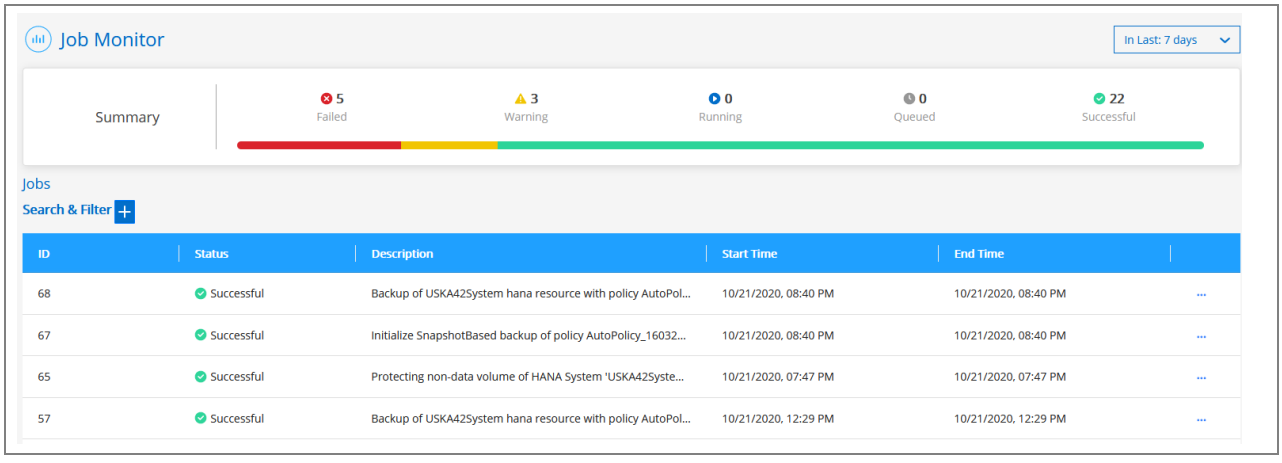
Steps:

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

   The systems added to SnapCenter Service is 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.

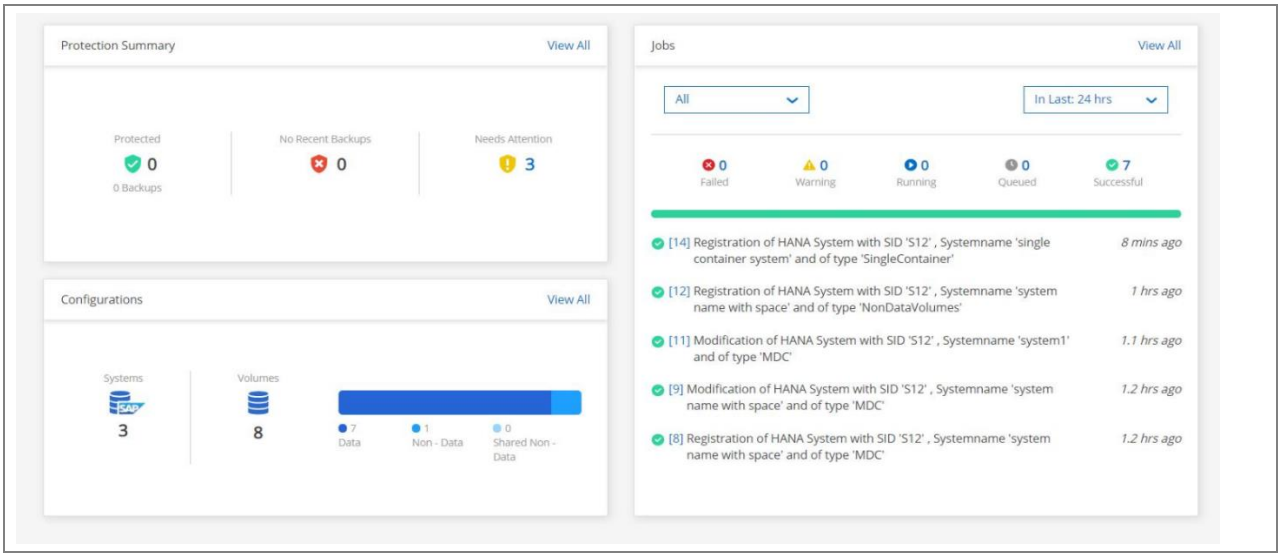
Monitor jobs

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.



Back up SnapCenter Service metadata

The SnapCenter Service metadata is stored in a MongoDB database. When you enable SnapCenter Service, the MongoDB database will be deployed as Kubernetes StatefulSet with Google Persistent Disk (PD) as the backup storage.

The metadata stored in the MongoDB database is automatically backed up every hour and the backup is stored in another Google PD.

Note: At any point of time only the last backup of the MongoDB database will be available for restore.

If you need to restore the MongoDB database from the backup, you should contact NetApp Support for the instructions.