NetApp

Protect your data using the SnapCenter Service 1.0
Manage SAP HANA Systems

NetApp
June 2021

doccomments@netapp.com SnapCenter Service 1.0

Learn about the SnapCenter Service

The SnapCenter Service provides data protection capabilities for applications running on NetApp® Cloud Storage. SnapCenter Service enabled within NetApp Cloud Manager offers efficient, application consistent, policy-based backup and restore for SAP HANA® Systems residing on Azure NetApp Files (ANF) or on Cloud Volumes Service (CVS) for Google Cloud Platform (GCP).

Supported functionalities

- Adding SAP HANA systems
- Creating on-demand backup of SAP HANA systems
- Protecting SAP HANA systems using system-defined policies or create a custom policy for scheduled backups
- Retaining backups based on the policy
- Restoring SAP HANA systems
- Monitoring jobs
- Displaying the protection summary, configuration details, and job status on the Dashboard
- Sending alerts through email

## Supported working environments

SnapCenter Service supports data protection of HANA systems residing on following working environments:

- Azure NetApp Files (ANF)
- Cloud Volumes Service (CVS) on Google Cloud Platform (GCP)

Getting started with SnapCenter Service

1. Create a Cloud Manager Connector in your cloud account for your region.

2. Deploy SnapCenter Service.
   SnapCenter Service is a cloud provider managing Kubernetes cluster that is deployed in the same network as that of the Connector.

3. Add SAP HANA systems.

4. Protect SAP HANA systems using system-defined or custom policies.

The following diagram shows the relationship between each component of SnapCenter Service :
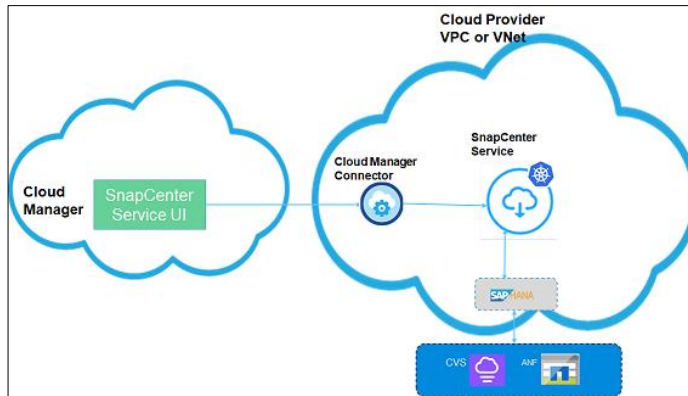
The SnapCenter Service UI communicates with the Cloud Manager Connector for user-initiated request. The Connector then communicates to SnapCenter Service and SnapCenter Service invokes ANF or CVS GCP management APIs and HANA system commands to perform data protection operations.

SnapCenter Service can be deployed in the same VPC or VNet as that of the HANA system, or a different one. If SnapCenter Service and HANA systems are on different network, network connectivity is required between them.

SnapCenter Service deployment for ANF environment

Deploying SnapCenter Service for Azure NetApp Files (ANF) environment includes the following tasks:

1. Creating an Azure Connector in Cloud Manager

2. Enabling the SnapCenter Service

Limitations

- Internationalization in not supported, ensure to use English browsers.

- Proxy Server is not supported.

- Only a Cloud Manager user with "Account Admin" role can enable the SnapCenter Service.

- High availability cluster configuration is not supported.

- SnapCenter Service does not clean up the latest Backup Catalog entries of backups when restoring from an earlier Snapshot. This leads to stale catalog entries in the HANA Backup Catalog.

Create an Azure Connector in Cloud Manager

An Account Admin should deploy a *Connector* before you can use the Cloud Manager features. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

What you will need:

- Depending on your Azure Active Directory settings, you may require the consent of the Azure tenant admin if you are creating the Connector for the first time in this subscription.

- Ensure that the subnet chosen for the Connector should not overlap with the following IP address ranges reserved for Azure Kubernetes Service (AKS): 169.254.0.0/16, 172.30.0.0/16, 172.31.0.0/16, and 192.0.2.0/24.

- Ensure that there are no AKS running in the chosen subnet.

- Ensure that the chosen subnet has outbound network connectivity to the internet.

- Ensure that the chosen subnet can access the SAP HANA systems on the respective ports.

- If the VNet of the chosen subnet is different from the VNet of the SAP HANA systems, ensure that the VNets can communicate with each other through VPN gateway, peering, or other means.

Steps:

1. Sign up to NetApp Cloud Central so you can access NetApp's cloud services. [Learn more](#).

2. Log into Cloud Manager and create a Cloud Central account. [Learn more](#).

3. Create a Connector in Azure from Cloud Manager. [Learn more](#).

   Note: The username and password or the key that was provided while creating the Connector would be required to connect to the machine.

4. Create an Azure NetApp Files working environment in Cloud Manager for ANF to create and manage NetApp accounts, capacity pools, volumes, and snapshots. [Learn more](#).

Enable SnapCenter Service for ANF

You can enable the SnapCenter Service using the Cloud Manager UI. When the SnapCenter Service is enabled, Azure Kubernetes Service (AKS) cluster is created that will host the SnapCenter Service.

The AKS cluster will be created in the same resource group and the same subnet that was chosen while creating the Connector. If your Connector is created without public IP address, then the AKS cluster will be created in private mode.

A user assigned managed identity with necessary permissions is required to create and manage AKS cluster. The user assigned managed identity should be assigned to the Connector VM.

What you'll need:

You should register the "Microsoft.ContainerService" resource provider in your Azure subscription. Learn more.

Steps:

1. Log into Cloud Manager.

2. Select the Azure Connector that was created in the Cloud Manager.

   Ensure that the Connector has the network connectivity to the SAP HANA systems to be protected.

3. Click **All Services > SnapCenter > Enable**.

4. Perform one of the following:

If you want…	Tasks…
SnapCenter to automatically create the user assigned managed identity with necessary permissions and assign it to the Connector VM.	1. On the Get Ready page, Click **Continue**. 2. Specify the Azure credentials. If the Azure login account does not have subscription owner level permissions, you should assign the required permissions. Learn more.
To manually create the user assigned managed identity with necessary permissions and assign it to the Connector VM.	1. In the Azure portal run the script. Learn more. 2. On the Get Ready page, click **specify**. 3. Specify the name of the user-assigned managed identity that was created by the script. 4. Click **Save**. 5. Click **Continue**.

5. On the Cluster Configuration page, perform the following:

    i. Select the cluster configuration.

- If you select **High Availability**, an Azure Kubernetes Service (AKS) cluster with 3 worker nodes across 3 zoned will be created.

    Note: For BETA, high availability cluster configuration is not supported.

- If you select **Non-High Availability**, an AKS cluster with single node will be created.

    ii. Specify the Kubernetes Pod address range.

Ensure that the Kubernetes Pod address range does not overlap with IP ranges of your virtual network, peered virtual networks, and on-premises networks that are connected. Also, the range should not overlap with the Service address range and Docker bridge address.

    iii. Specify the Kubernetes Service address.

Ensure that the Kubernetes service address range does not overlap with the IP ranges of your virtual network, peered virtual networks, and on-premise networks that are connected. Also, the range should not overlap with the Pod address range and Docker bridge address.

    iv. Specify the Docker bridge network.

Ensure that the Docker Bridge address does not overlap with the IP ranges of your virtual network, peered virtual networks, and on-premise networks that are connected. Also, the range should not overlap with the Pod address range and Service address range.

    v. On the Review page, review the details and click **Continue**.

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

The AKS cluster details can be obtained by clicking ⚌ .

Note: If the deployment fails, you can fix the issue and click **Retry** to enable SnapCenter Service.

Permissions required for Azure login account

Azure login account is used to create the user assigned managed identity, required roles, and assigning the identity to the Connector VM.

Note: The credentials of the login account is not stored anywhere in the SnapCenter Service and are not used to call APIs. The credentials are used only in the UI.

Steps:

1. Create a custom role using the **SnapCenter_Deployment_Role1.json** file available at: https://docs.netapp.com/us-en/occm/media/SnapCenter_Deployment_Role1.json

You should replace the *<Subscription_ID>* in the SnapCenter_Deployment_Role1.json file with your Azure subscription ID.

2. Assign the role to the login account at the scope of Connector's resource group.

3. Create a custom role using the **SnapCenter_Deployment_Role2.json** file available at: https://docs.netapp.com/us-en/occm/media/SnapCenter_Deployment_Role2.json

You should replace the *<Subscription_ID>* in the SnapCenter_Deployment_Role2.json file with your Azure subscription ID.

4. Assign the role to the login account at the scope of Connector's VNet or higher.

Manually create user assigned managed identity and roles using a script

You can run a script to create the user-assigned managed identity and the roles.

What you will need:

Ensure that the login account has the permissions specified in [Permissions required for Azure login account](#).

About this task:

The script performs the following tasks:

- Creates a user assigned managed identity in the Connector's resource group.
- Creates custom roles required for creating and managing AKS cluster.
- Assigns the roles to the user assigned managed identity.
- Assigns the user assigned managed identity to the Connector VM.

Steps:

1. Download the **prerequisite_azure.sh** script from https://docs.netapp.com/us-en/occm/media/prerequisite_azure.sh to your local system.

2. Log into [Microsoft Azure portal](#).

3. Click ▣ to open the cloud shell.

4. Copy the script to Azure cloud shell.

5. Assign the permission to run the script.

   ```
   chmod +x ./prerequisite_azure.sh
   ```

6. Run the script.

   ```
   subscriptionID={Subscription_ID} ResourceGroup={resource_group_name}
   ConnectorName={azure_connector_name}./prerequisite_azure.sh
   ```

Result:

The script displays the name of user assigned managed identity in the following format: **SnapCenter-MSI-{*azure_connector_name*}**.

What's next:

You can now protect your SAP HANA systems. See [Protect SAP HANA systems](#).

SnapCenter Service deployment for GCP environment

Deploying SnapCenter Service for GCP environment includes the following tasks:

1. Creating a GCP Connector in Cloud Manager

2. Enabling the SnapCenter Service

Limitations

- Internationalization in not supported, ensure to use English browsers.

- Proxy Server is not supported.

- Only a Cloud Manager user with "Account Admin" role can enable the SnapCenter Service.

- High availability cluster configuration is not supported.

- SnapCenter Service does not clean up the latest Backup Catalog entries of backups when restoring from an earlier Snapshot. This leads to stale catalog entries in the HANA Backup Catalog.

Create a GCP Connector in Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager features. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

What you'll need:

You should have the consent of the GCP Auth admin if you are creating the Connector for the first time in this project.

Steps:

1. Sign up to NetApp Cloud Central so you can access NetApp's cloud services. Learn more.

2. Log into Cloud Manager and create a Cloud Central account. Learn more.

3. Create a Connector in GCP project from Cloud Manager. Learn more.

4. Create a Cloud Volumes Service for Google Cloud working environment in Cloud Manager to create and manage volumes and snapshots. Learn more.

Enable SnapCenter Service for GCP

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. The GKE cluster will be created in the same project as that of the Connector.

What you'll need:

- Enable the following Google APIs by following the steps in [Enabling an API in your Google Cloud project](#).

If you are using…	Enable…
Standalone GCP project	- Compute API - Cloud Deployment Manager V2 API - Kubernetes API - Cloud Resource Manager API
Shared VPC environment	- On the service project: - Compute API - Cloud Deployment Manager V2 API - Kubernetes API - Cloud Resource Manager API - On the host project: - Compute API - Cloud Deployment Manager V2 API - Cloud Resource Manager API

- In a shared VPC environment, log into the host project and edit the subnet that was chosen while creating the Connector to provide 2 secondary IP ranges.

  These secondary IP ranges will be used for GKE cluster's Pod secondary IP CIDR range and Service secondary IP CIDR range.

About this task:

If the public IP was disabled while creating the Connector, the GKE cluster will be created in the private network. The proxy configuration is applicable for both public and private cluster.

The VPC and the subnet chosen while creating the Connector are used for creating the GKE cluster.

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. Click **All Services > SnapCenter > Enable**.

4. Perform one of the following:

If you want…	Tasks…

SnapCenter to automatically create the required roles and bind them to the Connector's service account.	1. On the Pre-requisites page, click **Automatic** > **Next**.
	
	2. Specify the GCP user account credentials.
	
	The GCP user account should have the following permissions to automatically create the roles and assign to the Connector's service account.
	
	   • *iam.serviceAccounts.actAs*
	   • *iam.roles.create*
	   • *iam.roles.get*
	   • *iam.roles.update*
	   • *resourcemanager.projects.getIamPolicy*
	   • *resourcemanager.projects.setIamPolicy*
	
	Note: The credentials of the login account is not stored anywhere in the SnapCenter Service and are not used to call APIs. The credentials are used only in the UI.

To manually create the roles with necessary permissions and bind them to the Connector's service account.	1. On the Pre-requisites page, click **Manual**.
	
	2. Download the **prerequisite_gcp.sh** script from https://docs.netapp.com/us-en/occm/media/prerequisite_gcp.sh to your local system.
	
	3. Log into Google Cloud Platform.
	
	4. Click to activate the cloud shell.
	
	5. Click > **Upload File** to upload the script.
	
	6. Assign the permission to run the script.
	
	`chmod + ./prerequisite_gcp.sh`
	
	7. Run the script.
	
	   • In a shared VPC environment, run:
	
	`./prerequisite_gcp.sh -m -p <project_id> -a < service_account_email_id > -r <host_project_id> -n <project_number>`
	
	   • In a non-shared VPC environment, run:
	
	`./prerequisite_gcp.sh -p <project_id> -a <service_account_email_id>`
	
	8. In the Cloud Manager UI, on the Pre-requisites page, click **Next**.

5. On the Cluster Configuration page, perform the following:

   i.   Select the cluster configuration.

   - If you select **High Availability**, a Google Kubernetes Engine (GKE) cluster with 3 worker nodes across 3 zones will be created.

     Note: For BETA, high availability cluster configuration is not supported.

   - If you select **Non-High Availability**, a GKE cluster with single node will be created.

   ii.   If the public IP is disabled (private cluster), specify the master IPv4 CIDR range for the GKE cluster.

   iii.   For shared VPC environment:

   - Select the GKE Pod secondary IP CIDR range.

   - Select the GKE service secondary IP CIDR range.

   iv.   On the Review page, review the details and 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, you can fix the issue and click **Retry** to enable SnapCenter Service.

What's next:

You can now protect your SAP HANA systems. See [Protect SAP HANA systems](#).

Protect SAP HANA systems

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.

You should download the HDBSQL client software from the SAP account to your local machine.

Steps:

1. Download the latest SAPCAR utility from your SAP account.

   ```
   Example: SAPCAR_1010-70006178.EXE
   ```

2. Extract the client software with .SAR extension using the SAPCAR utility:

   ```
   <SAPCAR_utility> -xvf <path_to_client_software>

   Example: ./SAPCAR_1010-70006178.EXE -xvf
   C:\Users\netapp\Downloads\IMDB_CLIENT20_008_20-80002082.SAR
   ```

3. Create a tar.gz file:

   ```
   tar -zcvf SAP_HANA_CLIENT.tar.gz SAP_HANA_CLIENT
   ```

4. On the Cloud Manager UI, click **Connector** to obtain the connector name.

5. Perform the following depending upon your environment:

GCP Environment	ANF Environment
a. Log into [Google Cloud Platform](#). b. Click **Compute Engine > VM Instances** and search for the Connector VM. c. Select the Connector and click **SSH**. d. Click ⌨⚙ > **Upload File** to upload the **SAP_HANA_CLIENT.tar.gz** file. The file is uploaded to **/home/<username>**.	a. Log into [Microsoft Azure portal](#). b. Click **Virtual machines**. c. Search for the Cloud Manager Connector and copy the public IP address assigned to the Connector. If the Connector does not have public IP enabled, you should use a jump host. d. Copy the **SAP_HANA_CLIENT.tar.gz** file to the Connector machine. To copy the file to the Connector path, you need the credentials, or the key provided while creating the Connector. `scp SAP_HANA_CLIENT.tar.gz <username>@<IP_Address>:/home/<username>` The file is copied to **/home/<username>**. For more information, see [how to use SCP to move files](#). e. Log into the Connector VM with the ssh credentials or key.

6. Run the following commands in the Connector VM.

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

   b. ```
   sudo docker exec -it cloudmanager_snapcenter /bin/bash
   /opt/netapp/hdbclient/hdbclient.sh SAP_HANA_CLIENT.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 SID 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.

   v. Click **Add**.

   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, perform the following:

   i. Select the working environment.

   - For ANF environment, specify the NetApp account.

   - For GCP environment, specify the region.

   ii. Select the required volumes.

   iii. Click **Add Storage**.

5. Click **Continue**.

6. Review all the details and click **Add**.

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

When you remove the 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. On the Storage Footprint page, perform the following:

   i. Select the working environment.

      - For ANF environment, specify the NetApp account.

      - For GCP environment, specify the region.

   ii. Select the required volumes.

   iii. Click **Add Storage**.

6. Click **Add**.

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**, select **Non-Data Volumes**, and specify the details.

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 using SAP HANA Studio or SAP HANA Cockpit before restoring because recovery of HANA system 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.

Email notification

The email notifications are sent by default for a failed on-demand backup, scheduled backup, and restore operations. Only a Cloud Manager user with "Account Admin" role will receive the email.

View dashboard

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