Use SnapCenter Service to protect SAP HANA systems

SnapCenter Service

NetApp
May 18, 2022

Table of Contents

Use SnapCenter Service to protect SAP HANA systems

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.

You cannot add or modify SAP HANA systems if a node in the AKS cluster is down.

Steps

1. On the SnapCenter Service page, click **SAP HANA Systems** > **Add**.
2. On the System Details page, perform the following actions:
   a. Select the system type.
   b. Specify the SID of the SAP HANA system.
   c. Specify the SAP HANA system name.
   d. Click HDB Secure User Store Keys text box to add user store keys details.

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

   e. Click **Add**.

      You should add user store keys for each host if you are adding a multi-host SAP HANA system.

3. Click **Continue**.
4. On the Storage Footprint page, perform the following:
   a. Select the working environment and specify the NetApp account.
   b. Select the required volumes.
   c. 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 and catalog entries 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**.

Back up SAP HANA systems

You can either perform an on-demand backup or schedule backups of your SAP HANA system using system-defined or custom policies. SnapCenter Service supports both snapshot-based and file-based backups.

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:
   a. Specify a policy name.
   b. Select the type of backup you want to create using this policy.
   c. 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.

   d. Specify the schedule frequency and the start and end time for the scheduled backups.
   e. 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:
     a. In the Policy field, select **None**.
     b. Select the backup type.

        If you are backing up a non-data volume, you can only select **Snapshot Based** as the backup type.

     c. Specify the retention period.
     d. 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**.

   All the systems added to the SnapCenter Service are 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**.

Find more information
SAP HANA backup and recovery on Azure NetApp Files with SnapCenter Service

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.

> After restoring the database, if you do a point-in-time recovery of the SAP HANA system using HANA Studio then the data backup catalog entries which were deleted by SnapCenter Service as per the retention setting, might be restored.
> If the deleted data backup catalog entries are restored because of the recovery operation, SnapCenter Service will not be able to detect and delete them. This could result in SnapCenter Service not cleaning the log catalog properly.
> You can verify the backup entries in SnapCenter Service to find out which all data backup catalog entries are newly restored and manually delete those entries.

Find more information
SAP HANA backup and recovery on Azure NetApp Files with SnapCenter Service

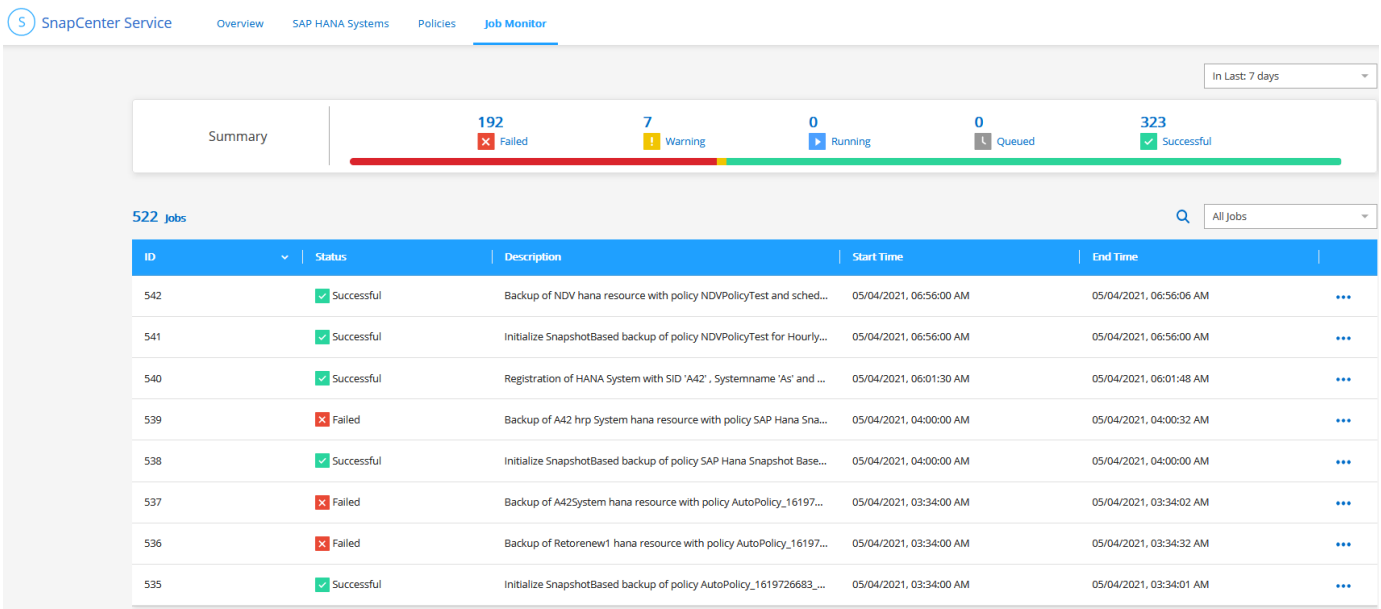
Manage operations

You can monitor the status of the jobs executed, receive email notifications, and view dashboard.

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.

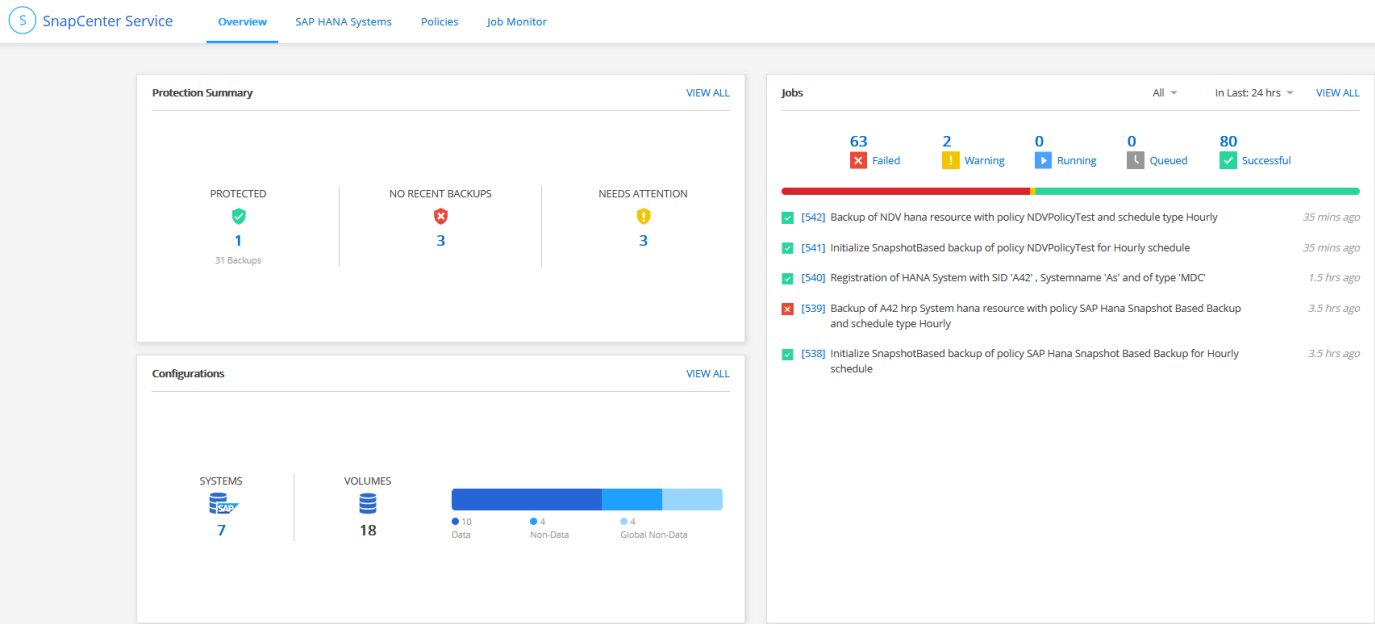


Email notification

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.



Troubleshoot issues

Issue: Redis Pods get stuck in a CrashLoopBackOff state

Description

In a high availability configuration, the AKS cluster does not come back to working state if all the nodes of the cluster are down. When you restart all the nodes, you might find all the Redis Pods to be in CrashLoopBackOff state.

Solution

You should run the following commands to restore the system.

1. Log into the Connector.
2. Delete all the Redis Pods.
    - `docker exec -it cloudmanager_snapcenter—sh`
    - `kubectl scale --replicas=0 sts sc-dependencies-redis-node -n snapcenter`
3. Verify if all the Redis Pods are deleted.
   `kubectl get pods -n snapcenter`
4. If the Redis Pods are not deleted, run the following commands:
    - `kubectl delete pod sc-dependencies-redis-node-0 -n snapcenter`

- `kubectl delete pod sc-dependencies-redis-node-1 -n snapcenter`
- `kubectl delete pod sc-dependencies-redis-node-2 -n snapcenter`

5. After all the Redis Pods are deleted, run:
   `kubectl scale --replicas=3 sts sc-dependencies-redis-node -n snapcenter`
6. Verify if all the deleted pods are up and running.
   `Kubectl get pods -n snapcenter`

Issue: Jobs are failing after restarting the cluster nodes

Description
In a high availability configuration, the AKS cluster does not come back to working state if all the nodes of the cluster are down. When you restart all the nodes, you might see jobs are failing with granular tasks either greyed out or timed out.

Solution
You should run the following commands:

1. Log into the Connector.
2. Save the RabbitMQ statefulset (sts) deployment.
   - `docker exec -it cloudmanager_snapcenter—sh`
   - `kubectl get sts rabbitmq -o yaml -n snapcenter > rabbitmq_sts.yaml`
3. Identify the persistent volumes (PVs) attached to RabbitMQ pods.
   `kubectl get pv | grep rabbitmq`
4. Delete the persistent volume claims (PVCs) attached to RabbitMQ pods.
   `kubectl get pvc -n snapcenter| grep rabbitmq | awk {'print $1'} | xargs`
   `kubectl delete pvc -n snapcenter`
5. Delete each of the PVs that you identified earlier in step 3.
   `kubectl delete pv 'pvname'`
6. Create a RabbitMQ sts.
   `kubectl create -f rabbitmq_sts.yaml -n snapcenter`

Issue: Backup operation fails during tenant database creation

Description
While creating a tenant database if an on-demand or a scheduled backup is initiated, the backup operation fails.

Solution
Creating a tenant database is a maintenance operation on the SAP HANA system.

You should put the SAP HANA system in the maintenance mode using SnapCenter Service before creating the tenant database. After putting the SAP HANA system in maintenance mode no operations can be initiated.

After creating the tenant database, you should bring back the SAP HANA system to production mode.