



# **Back up cloud-native SAP HANA databases**

## **BlueXP backup and recovery**

NetApp  
July 26, 2024

# Table of Contents

- Back up cloud-native SAP HANA databases ..... 1
  - Quick start ..... 1
  - Configure Azure NetApp Files ..... 1
  - Install SnapCenter Plug-in for SAP HANA and add database hosts ..... 2
  - Back up cloud-native SAP HANA databases ..... 7

# Back up cloud-native SAP HANA databases

## Quick start

Get started quickly by following these steps.

1

### Verify support for your configuration

- Operating System:
  - RHEL 7.6 or later
  - RHEL 8.1 or later for SAP-HANA SPS07
  - SLES 12 SP5 or later and 15 SPX platforms certified by SAP HANA
- NetApp Cloud Storage: Azure NetApp Files
- Storage layouts: For data and log files, Azure supports only NFSv4.1.
- Database layouts:
  - SAP HANA Multitenant Database Container (MDC) 2.0SPS5, 2.0SPS6, 2.0SPS7 with single or multiple tenants
  - SAP HANA single host system, SAP HANA multiple host system, HANA System Replication
- SAP HANA plug-in on the database host

2

### Sign up to BlueXP

BlueXP is accessible from a web-based console. When you get started with BlueXP, your first step is to sign up using your existing NetApp Support Site credentials or by creating a NetApp cloud login. For information, refer to [Sign up to BlueXP](#).

3

### Log into BlueXP

After you sign up to BlueXP, you can log in from the web-based console. For information, refer to [Log into BlueXP](#).

4

### Manage your BlueXP account

You can administer your account by managing users, service accounts, workspaces, and Connectors. For information, refer to [Manage your BlueXP account](#).

## Configure Azure NetApp Files

Using BlueXP you should create a Azure NetApp Files working environment to add and manage volumes and additional data services. You should also create a Connector in Azure that enables BlueXP to manage resources and processes within your public cloud environment.

## Create Azure NetApp Files working environment

You should create Azure NetApp Files working environments where your databases are hosted. For more information, refer to [Learn about Azure NetApp Files](#) and [Create an Azure NetApp Files working environment](#).

### Create a connector

A BlueXP account admin should deploy a Connector in Azure that enables BlueXP to manage resources and processes within your public cloud environment.

For information, refer to [Create a Connector in Azure from BlueXP](#).

- Ensure that there is connectivity from the connector to the database hosts.
- If you have the Azure NetApp Files working environment and databases in the same Virtual Network (VNet), you can deploy the connector in the same VNet.
- If you have the Azure NetApp Files working environment and databases in different VNets and have NAS (NFS) workloads configured on Azure NetApp Files, then you can create the connector on either of the VNets.

After creating the connector, add the working environment by clicking **Storage > Canvas > My Working Environments > Add Working Environment**.

## Install SnapCenter Plug-in for SAP HANA and add database hosts

You should install the SnapCenter Plug-in for SAP HANA on each of the SAP HANA database hosts. Depending on whether the SAP HANA host has an SSH key based authentication enabled, you can follow one of the methods to install the plug-in.

- If SSH is enabled for the database host, you can install the plug-in using SSH option. [Learn more](#).
- If SSH is disabled, install the plug-in manually. [Learn more](#).

### Prerequisites

Before adding the host, you should ensure that the prerequisites are met.

- Ensure that either Java 11 (64-bit) Oracle Java or OpenJDK is installed on each of the SAP HANA database hosts.
- You should have added the working environment and created the Connector.
- Ensure that the Connector has connectivity to the SAP HANA database hosts.

For information on how to resolve the connectivity issue, refer to [Failed to validate connectivity from BlueXP connector host to application database host](#).

When the connector is lost or if you have created a new connector, you should associate the connector with the existing application resources. For instructions to update the Connector, see [Update the Connector Details](#).

- Ensure that the BlueXP user has the “Account Admin” role.
- You should have created the SnapCenter user and configured sudo for the non-root (sudo) user. For

information, refer to [Configure sudo for SnapCenter user](#).

- You should have installed the SnapCenter Plug-in for SAP HANA before adding the database host.
- While adding the SAP HANA database hosts, you should add the HDB user store keys. The HDB secure user store key is used to store the connection information of SAP HANA database hosts securely on the client and HDBSQL client uses the secure user store key to connect to SAP HANA database host.
- For HANA System Replication (HSR), to protect the HANA systems, you should manually register both primary and secondary HANA systems.



The hostname must be the same as that of the host that is used in the HSR replication.

- Ensure that the Connector has the communication enabled to the SSH port (default: 22) if SSH based installation is performed.
- Ensure that the Connector has the communication enabled to plug-in port (default: 8145) for the data protection operations to work.
- Ensure that the you have the latest version of plug-in is installed. To upgrade the plug-in, refer to [Upgrade SnapCenter Plug-in for SAP HANA Database](#).

## Configure sudo for SnapCenter user

Create a non-root (sudo) user to install the plug-in.

### Steps

1. Log into the Connector VM.
2. Download the SnapCenter Linux host plug-in binary.  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. Copy the contents of **sudoer.txt** located at: `/var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -Po "cloudmanager_scs_cloud:.*)" | sed -e 's/ *$//|cut -f2 -d":")/sc-linux-host-plugin`
4. Log into the SAP HANA system host using root user account.
5. Configure sudo access for the non-root user by copying the text copied in the step 3 to `/etc/sudoers.d/snapcenter` file.

In the lines you added to the `/etc/sudoers.d/snapcenter` file, replace the `<LINUXUSER>` with the non-root user and `<USER_HOME_DIRECTORY>` with `home/<non-root-user>`.

## Install the plug-in using script

Configure SSH key based authentication for the SAP HANA host non-root user account and perform the following steps to install the plug-in.

### Before your begin

Ensure that the SSH connection to the Connector is enabled.

### Steps

1. Log into Connector VM.
2. Install the plug-in using the script provided in the Connector.  

```
sudo bash /var/lib/docker/volumes/service-manager-
```

```
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

If you are using an older Connector, run the following command to install the plug-in.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Name	Description	Mandatory	Default
plugin_host	Specifies the SAP HANA host	Yes	-
host_user_name	Specifies the SnapCenter user with SSH privileges on the SAP HANA host	Yes	-
host_ssh_key	Specifies the SSH key of the SnapCenter user and is used to connect to the SAP HANA host	Yes	-
plugin_port	Specifies the port used by the plug-in	No	8145
host_ssh_port	Specifies the SSH port on the SAP HANA host	No	22

For example, `sudo bash /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

After installing the plug-in, you should [Add SAP HANA database hosts](#).

## Install the plug-in manually

If SSH key based authentication is not enabled on the HANA host, you should perform the below manual steps to install the plug-in.

### Steps

1. Log in to Connector VM.
2. Download the SnapCenter Linux host plug-in binary.

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

The plug-in binary is available at: `cd /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -Po "cloudmanager_scs_cloud:.*?"|sed`

```
-e 's/*$/"|cut -f2 -d":")/sc-linux-host-plugin
```

3. Copy `snapcenter_linux_host_plugin_scs.bin` from the above path to `/home/<non root user>/.sc_netapp` path for each of the SAP HANA database hosts either using scp or other alternate methods.
4. Log into the SAP HANA database host using the non-root (sudo) account.
5. Change directory to `/home/<non root user>/.sc_netapp/` and run the following command to enable execute permissions for the binary.  

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```
6. Install the SAP HANA plug-in as a sudo SnapCenter user.  

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```
7. Copy `certificate.pem` from `<base_mount_path>/client/certificate/` path of the Connector VM to `/var/opt/snapcenter/spl/etc/` on the plug-in host.
8. Navigate to `/var/opt/snapcenter/spl/etc` and execute the `keytool` command to import the certificate.  

```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks -deststorepass snapcenter -noprompt
```
9. Restart SPL: 

```
systemctl restart spl
```
10. Validate that the plug-in is reachable from the Connector by running the below command from the Connector.  

```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/PluginService/Version --cert config/client/certificate/certificate.pem --key /config/client/certificate/key.pem
```

After installing the plug-in, you should [Add SAP HANA database hosts](#).

## Upgrade SnapCenter Plug-in for SAP HANA Database

You should upgrade the SnapCenter Plug-in for SAP HANA database to gain access to the latest new features and enhancements.

### Before you begin

- Ensure that there are no operations running on the host.

### Steps

1. Configure sudo for SnapCenter user. For information, see [Configure sudo for SnapCenter user](#).
2. Run the following script.  

```
/var/lib/docker/volumes/service-manager-  
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh  
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>  
--pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
```

If you are using an older Connector, run the following command to upgrade the plug-in.

```
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
```

## Add SAP HANA database hosts

You should manually add SAP HANA database hosts to assign policies and create backups. Auto discovery of SAP HANA database host is not supported.

### Steps

1. In the **BlueXP** UI, select **Protection > Backup and recovery > Applications**.
2. Select **Discover Applications**.
3. Select **Cloud Native > SAP HANA** and select **Next**.
4. In the **Applications** page, select **Add System**.
5. In the **System Details** page, perform the following actions:
  - a. Select the System Type as Multi-tenant database container or Global Non-Data Volumes.
  - b. Enter the SAP HANA system name.
  - c. Specify the SID of the SAP HANA system.
  - d. (Optional) Modify OSDB user.
  - e. If HANA system is configured with HANA System replication, enable **HANA System Replication (HSR) System**.
  - f. Select **HDB Secure User Store Keys** text box to add user store keys details.

Specify the key name, system details, username, and password and click **Add Key**.

You can delete or modify the user store keys.

6. Select **Next**.
7. In the **Host Details** page, perform the following actions:
  - a. Select **Add new host** or **Use existing host**.
  - b. Select **Using SSH** or **Manual**.

For Manual, enter the Host FQDN or IP, Connector, Username, SSH port, Plug-in port, and optionally add and validate the SSH private key.

For SSH, enter the Host FQDN or IP, Connector, Username, and Plug-in port.

- c. Select **Next**.
8. In the **Host configuration** page, verify whether the configuration requirements are met.

Select the check boxes to confirm.

9. Select **Next**.
10. In the **Storage Footprint** page, select **Add Storage** and perform the following:
  - a. Select the working environment and specify the NetApp account.

From the left navigation pane, select BlueXP **Canvas** to add a new working environment.
  - b. Select the required volumes.
  - c. Select **Add Storage**.



11. Review all the details and select **Add System**.

You can modify or remove the SAP HANA systems from the UI.


Before removing the SAP HANA system, you should delete all the associated backups and remove the protection.

### Add Non-Data Volumes

After adding the multi-tenant database container type SAP HANA system, you can add the Non-Data Volumes of the HANA system.

You can add these resources to resource groups to perform data protection operations after you discover the SAP HANA databases that are available.

#### Steps

1. In the **BlueXP** UI, click **Protection > Backup and recovery > Applications**.
2. Click **Discover Applications**.
3. Select **Cloud Native > SAP HANA** and click **Next**.
4. In the **Applications** page, click  corresponding to the system for which you want to add the Non-Data Volumes and select **Manage System > Non-Data Volume**.

### Add Global Non-Data Volumes

After adding the multi-tenant database container type SAP HANA system, you can add the Global Non-Data Volumes of the HANA system.

#### Steps

1. In the **BlueXP** UI, click **Protection > Backup and recovery > Applications**.
2. Click **Discover Applications**.
3. Select **Cloud Native > SAP HANA** and click **Next**.
4. In the **Applications** page, click **Add System**.
5. In the **System Details** page, perform the following actions:
  - a. From System Type drop-down, select **Global Non-Data Volume**.
  - b. Enter the SAP HANA system name.
6. . In the **Host Details** page, perform the following actions:
  - a. Specify the associated SIDs of the SAP HANA system.
  - b. Select the plug-in host
  - c. Click **Next**.
  - d. Review all the details and click **Add System**.

## Back up cloud-native SAP HANA databases

You can create a backup by assigning a pre-canned policy or the policy that you created.

## Create a policy to protect SAP HANA database

You can create policies if you do not want to use or edit the pre-canned policies.

1. In the **Applications** page, from the Settings drop-down list, select **Policies**.
2. Click **Create policy**.
3. Specify a policy name.
4. (Optional) Edit the format of the Snapshot copy name.
5. Select policy type.
6. Specify the schedule and retention details.
7. (Optional) Specify the scripts. [Prescripts and postscripts](#).
8. Click **Create**.

### Prescripts and postscripts

You can provide prescripts, postscripts, and exit scripts while creating a policy. These scripts are run on the HANA host during data protection operation.

The supported format for scripts are .sh, python script, perl script, and so on.

The prescript and the postscript should be registered by the host admin into `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` file.

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

### Environmental variables

For the backup workflow, the following environmental variables are available as part of prescript and postscript.

Environmental Variable	Description
SID	The System Identifier of the HANA Database chosen for restore
BackupName	Backup name chosen for restore operation
UserStoreKeyNames	Configured userstore key for the HANA database
OSDBUser	Configured OSDBUser for the HANA database
PolicyName	Only for scheduled backup
schedule_type	Only for scheduled backup

## Create a backup of the SAP HANA Database

You can either assign a pre-canned policy or create a policy and then assign it to the database. Once the policy is assigned, the backups are created as per the schedule defined in the policy.

### Before you begin

You should have added the SAP HANA database hosts.

[Add SAP HANA database hosts](#)

### About this task

For HANA System Replication (HSR), the scheduled backup job triggers only for the primary HANA system and if the system fails over to the secondary HANA system, the existing schedules triggers a backup on the current primary HANA system. If the policy is not assigned to both the primary and secondary HANA system, after failover, the schedules will fail.

If different policies are assigned to the HSR systems, the scheduled backup triggers for both the primary and secondary HANA systems and the backup will fail for the secondary HANA system.

### Steps

1. In the Applications page, if the database is not protected using any policy, click **Assign Policy**.

Though the database is protected using one or more policies, if needed, you can continue to assign more policies by clicking **...** > **Assign Policy**.

2. Select the policy and click **Assign**.

The backups are created as per the schedule defined in the policy.



The service account (*SnapCenter-account-`<account_id>`*) is used to run the scheduled backup operations.

## Create on-demand backup of the SAP HANA database

After assigning the policy, you can create an on-demand backup of the application.

### Steps

1. In the **Applications** page, click **...** corresponding to the application and click **On-Demand Backup**.
2. Select On-demand backup type.
3. For Policy Based backup, select the policy, retention tier and then click **Create Backup**.
4. For One time, select either Snapshot copy based, or File based perform the following steps:
  - a. Select the retention value and specify the backup name.
  - b. (Optional) Specify the scripts, and path for the scripts.

For more information, see [Prescripts and Postscripts](#)

- c. Click **Create Backup**.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.