

BlueXP Backup and Recovery for SAP HANA - Cloud Object storage as backup destination

NetApp Solutions SAP

NetApp September 17, 2024

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions-sap/backup/hana-hycl-backup-overview.html on September 17, 2024. Always check docs.netapp.com for the latest.

Table of Contents

	1
	3
	6
	6
•	· · · ·

BlueXP Backup and Recovery for SAP HANA -Cloud Object storage as backup destination

BlueXP Backup and Recovery for SAP HANA - Cloud Object storage as backup destination

Overview

This document describes how to setup and configure SAP HANA for data protection from on-premises to cloud based object stores with NetApp BlueXP. It covers the BlueXP backup and recovery part of the solution. This solution is an enhancement of the on-premises SAP HANA backup solution using NetApp Snap Center and provides a cost-efficient way for long-term archiving of SAP HANA backups to cloud based object storage and offers optional tiering of object storage to archival storage like AWS Glacier/Deep Glacier, Microsoft Azure Blob Archive, and GCP Archive Storage.

The setup and configuration of the on-premises SAP HANA backup and recovery solution is described in TR-4614: SAP HANA backup and recovery with SnapCenter (netapp.com).

This TR only describes how to enhance the on-premises SnapCenter based SAP HANA backup and recovery solution with BlueXP backup and recovery for SAP HANA using AWS S3 object storage as example. The setup and configuration using Microsoft Azure and GCP object storage instead of AWS S3 is similar, but is not described within this document.

BlueXP Backup and Recovery architecture

BlueXP backup and recovery is a SaaS solution that provides data protection capabilities for applications running on NetApp on-premises Storage to the cloud. It offers efficient, application consistent, policy-based protection of SAP HANA using NetApp storage. In addition, BlueXP backup and recovery provides centralized control and oversight, while delegating the ability for users to manage application-specific backup and restore operations.

BlueXP backup and recovery runs as SaaS within NetApp BlueXP and leverages the framework and UI. The BlueXP working environment framework is used to configure and manage the credentials for NetApp ONTAP based on-premises storage and the NetApp SnapCenter Server.

A BlueXP connector needs to be deployed within the customer virtual network. A connection between the onpremises environment and the cloud environment is required such as an site to site VPN connection. The communication between the NetApp SaaS components and the customer environment is exclusively done via the connector. The connector is executing the storage operations by using the ONTAP and SnapCenter management APIs.

The data transfer between the on-premises storage and the cloud bucket is end-to-end protected with AES 256-bit encryption at rest, TLS/HTTPS encryption in flight, and customer-managed key (CMK) support. The backed-up data can be stored in an immutable and indelible WORM state. The only way to access the data from the object storage is to restore it to NetApp ONTAP based storage including NetApp CVO.



Overview of installation and configuration steps

The required installation and configuration steps can be split in three areas. Prerequisite is that the SAP HANA backup configuration has been configured at NetApp Snap Center. For setting up Snap Center for SAP HANA in the first place refer to SnapCenter configuration (netapp.com).

1. Installation and configuration of NetApp BlueXP components.

Needs to be done once during the initial setup of the data protection solution.

2. Preparation steps at NetApp SnapCenter.

Needs to be done for each SAP HANA database, which should be protected.

3. Configuration steps in BlueXP backup and recovery.

Needs to be done for each SAP HANA database, which should be protected.

Installation and configuration of NetApp BlueXP Hybrid Application Backup

The installation and configuration of the NetApp BlueXP components are described in Protect your onpremises applications data | NetApp Documentation.

- 1. Sign-up to BlueXP and setup NetApp account at https://bluexp.netapp.com/.
- 2. Deploy BlueXP connector in your environment. Description is available at Learn about Connectors | NetApp Documentation.

- 3. Add/buy a Cloud Backup license at BlueXP: https://docs.netapp.com/us-en/cloud-manager-backup-restore/ task-licensing-cloud-backup.html.
- 4. Create working environment for NetApp on-premises environment and your cloud destination in BlueXP by adding your on-premises storage.
- 5. Create a new object store relationship for the on-premises storage into an AWS S3 bucket.
- 6. Configure SAP HANA system resource at SnapCenter.
- 7. Add Snap Center to your working environment.
- 8. Create a policy for your environment.
- 9. Protect you SAP HANA System.

Configuring BlueXP Backup and Recovery for SAP HANA

Create working environment for BlueXP

Add the on-premises storage system to you work environment.

- 1. At the left menu choose Storage \rightarrow Canvas \rightarrow My Working Environment.
- Press + Add Working Environment. image::hana-hycl-back-image2.jpeg[hana-hycl-back-image2,width=624,height=316]
- Choose On-Premises. image::hana-hycl-back-image3.jpeg[Ein Bild, das Text enthält. Automatisch generierte Beschreibung,width=624,height=316]
- Choose Discover On-Premises ONTAP. image::hana-hycl-back-image4.jpeg[Ein Bild, das Text enthält. Automatisch generierte Beschreibung,width=624,height=316]
- 5. Add the IP address of the ONTAP cluster and the password and press **Discover**. image::hana-hycl-back-image5.jpeg[hana-hycl-back-image5,width=624,height=316]
- The ONTAP cluster is now available. image::hana-hycl-back-image6.jpeg[Ein Bild, das Diagramm enthält. Automatisch generierte Beschreibung,width=624,height=316]

Create a relationship between the on-premises storage system and an object storage bucket

The relationship between the on-premises storage and the S3 bucket is done by creating a backup for a volume or by activating a backup of an application. If an existing site-to-site VPN shall be used for transferring the data from on-premises to S3, a volume backup needs to be used for creating the relationship between the on-premises storage and S3 bucket as VPC endpoints need to be used.

At creation of this documentation the application backup workflow doesn't offer to choose VPC endpoints to access S3 buckets.

Refer to Gateway endpoints for Amazon S3 - Amazon Virtual Private Cloud how to setup VPC endpoints for S3 within your VPC.

To create a first volume backup, perform the following steps:

 Navigate via Protection to Backup and recovery and choose Volumes. image::hana-hycl-back-image7.jpeg[hana-hycl-back-image7,width=624,height=308]

- Press the Activate Backup button. image::hana-hycl-back-image8.jpeg[hana-hycl-back-image8,width=624,height=309]
- Choose the desired on-premises storage system and click Activate Backup. image::hana-hycl-back-image9.jpeg[hana-hycl-back-image9,width=624,height=304]
- Choose Backup. image::hana-hycl-back-image10.jpeg[hana-hycl-back-image10,width=624,height=307]
- Choose a volume which is stored at the same SVM as your SAP HANA data files and press Next. In this example the volume for /hana/shared has been chosen. image::hana-hycl-back-image12.jpeg[hana-hycl-back-image12,width=624,height=305]
- Continue, if an existing policy exists. image::hana-hycl-back-image11.jpeg[hana-hycl-back-image11,width=624,height=304]
- Check the Backup Option and choose your desired Backup Provider. In this example AWS. Keep the option checked for already existing policies. Uncheck options you do not want to use. image::hana-hycl-back-image13.jpeg[Ein Bild, das Text, Software, Computersymbol, Webseite enthält. Automatisch generierte Beschreibung,width=624,height=306]
- Create a new bucket or choose an existing one. Provide your AWS account settings, the regio, your access key, and the secret key. Press Next. image::hana-hycl-back-image14.jpeg[hana-hycl-back-image14,width=624,height=306]
- Choose the correct IPspace of your on-premises storage system, select Privat Endpoint Configuration and choose the VPC endpoint for the S3. Press Next. image::hana-hycl-back-image15.jpeg[hana-hycl-back-image15,width=624,height=304]
- 10. Review your configuration and press **Activate Backup**. image::hana-hycl-back-image16.jpeg[hana-hycl-back-image16,width=624,height=304]
- 11. The backup has been successfully initiated. image::hana-hycl-back-image17.jpeg[hana-hycl-back-image17,width=624,height=304]

Configure the SAP HANA system resource at SnapCenter

- Check, if the SVM (hana in this example) where your SAP HANA system is stored has been added via the cluster. If only the SVM has been added, add the cluster. image::hana-hycl-back-image18.png[Graphical user interface, application Description automatically generated,width=604,height=156]
- Define a schedule policy with either daily, weekly, or monthly schedule type. image::hana-hycl-back-image19.png[Graphical user interface, application Description automatically generated,width=604,height=140] image::hana-hycl-back-image20.jpeg[hana-hycl-back-image20,width=167,height=167]
- Add the new policy to your SAP HANA system and assign a daily schedule. image::hana-hycl-back-image21.png[Graphical user interface, application Description automatically generated,width=604,height=215]
- 4. Once configured new backups with this policy will be available after the policy has been executed according to the schedule defined. image: hana-hycl-back-image22 png[Graphica] user interface, application. Teams Description automat

image::hana-hycl-back-image22.png[Graphical user interface, application, Teams Description automatically generated,width=604,height=193]

Adding SnapCenter to the BlueXP Working Environment

- 1. At the left menu choose Protection \rightarrow Backup and recovery \rightarrow Applications.
- 2. Choose **Hybrid** from the pulldown menu. image::hana-hycl-back-image23.jpeg[hana-hycl-back-image23,width=624,height=316]
- Choose SnapCenter Servers at the Settings menu. image::hana-hycl-back-image24.jpeg[Ein Bild, das Text enthält. Automatisch generierte Beschreibung,width=624,height=316]
- Register the SnapCenter Server. image::hana-hycl-back-image25.jpeg[Ein Bild, das Text enthält. Automatisch generierte Beschreibung,width=624,height=316]
- 5. Add the SnapCenter Server credentials. image::hana-hycl-back-image26.jpeg[hana-hycl-back-image26,width=624,height=315]
- The SnapCenter Servers has been added and data will discovered. image::hana-hycl-back-image27.jpeg[hana-hycl-back-image27,width=624,height=316]
- Once the discovery job has been finished the SAP HANA system will be available. image::hana-hycl-back-image28.jpeg[Ein Bild, das Text enthält. Automatisch generierte Beschreibung,width=624,height=316]

Creating a Backup Policy for Application Backup

- 1. Choose **Policies** within the settings menu. image::hana-hycl-back-image29.jpeg[hana-hycl-back-image29,width=624,height=316]
- Create a new policy, if desired by click Create Policy. image::hana-hycl-back-image30.jpeg[hana-hycl-back-image30,width=624,height=316]
- 3. Provide the policy name, desired SnapMirror label, choose your desired options, and press **Create**. image::hana-hycl-back-image31.jpeg[hana-hycl-back-image31,width=624,height=315]
- The new policy is available. image::hana-hycl-back-image32.jpeg[hana-hycl-back-image32,width=624,height=315]

Protecting the SAP HANA database with Cloud Backup for Applications

- Choose Activate Backup for the SAP HANA system. image::hana-hycl-back-image33.jpeg[width=624,height=316]
- Choose the previously created policy and click Next. image::hana-hycl-back-image34.jpeg[width=624,height=316]
- 3. As the storage system and the connector have configured upfront the backup will be activated. image::hana-hycl-back-image35.jpeg[width=624,height=316]
- Once the job has been completed the System will be listed. image::hana-hycl-back-image36.jpeg[width=624,height=337]
- After some time the backups will be listed at the detail view of the SAP HANA System. A daily backup will be listed the next day. image::hana-hycl-back-image37.jpeg[hana-hycl-back-image37,width=624,height=316]

In some environments it might the necessary to remove any existing schedule settings of the snapmirror source. To do so execute the following command at the source ONTAP system: *snapmirror modify -destination*

Restoring SAP HANA BlueXP Backup

A restore from of the backup can only be done to an on-premises NetApp ONTAP based storage system or NetApp CVO within the cloud. A restore can be done by doing the following steps:

- 1. In BlueXP UI, click Protection > Backup and recovery > Applications and choose Hybrid.
- 2. In the Filter By field, select the filter Type and from the drop-down select HANA.
- Click View Details corresponding to the database that you want to restore. image::hana-hycl-back-image38.jpeg[hana-hycl-back-image38,width=624,height=305]
- Select the desired backup and choose Storage Export. image::hana-hycl-back-image39.jpeg[width=624,height=308]
- Provide the desired options: image::hana-hycl-back-image40.jpeg[width=624,height=308]
 - a. For NAS environment, specify the FQDN or IP address of the host to which the volumes restored from object store are to be exported.
 - b. For SAN environment, specify the initiators of the host to which LUNs of the volumes restored from object store are to be mapped.
- 6. If the snapshot is in archival storage, select the priority to restore your data from the archival storage.
- 7. If there is not enough space on the source storage or the source storage is down, select **Change storage location**.
- 8. If you select **Change storage location**, you can append a suffix to the destination volume. If you have not selected the checkbox, then by default **_restore** is appended to the destination volume. Click **Next**.
- 9. If you selected Change Storage Location, specify the alternate storage location details where the data restored from the object store will be stored in the Storage mapping page and click **Next**.
- 10. Review the details and click **Restore**. image::hana-hycl-back-image41.jpeg[hana-hycl-back-image41,width=624,height=309]

This operation does only the storage export of the restored backup for the given host. You must manually mount the filesystem at the host and bring up the database. After utilizing the volume, the storage Administrator can delete the volume from the ONTAP cluster.

Additional Information and Version History

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp BlueXP backup and recovery Product Documentation Protect your on-premises applications data | NetApp Documentation
- SAP HANA backup and recovery with SnapCenter https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-br-scs-overview.html#the-netappsolution

Version history

Version	Date	Document version history
Version 1.0	March 2024	Initial version

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

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.