



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

NetApp Solutions SAP

NetApp
March 11, 2024

Table of Contents

- BlueXP Backup and Recovery for SAP HANA - Cloud Object storage as backup destination 1
 - BlueXP Backup and Recovery for SAP HANA - Cloud Object storage as backup destination 1
 - Configuring BlueXP Backup and Recovery for SAP HANA 3
 - Restoring SAP HANA BlueXP Backup 19
 - Additional Information and Version History 22

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-premise 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.

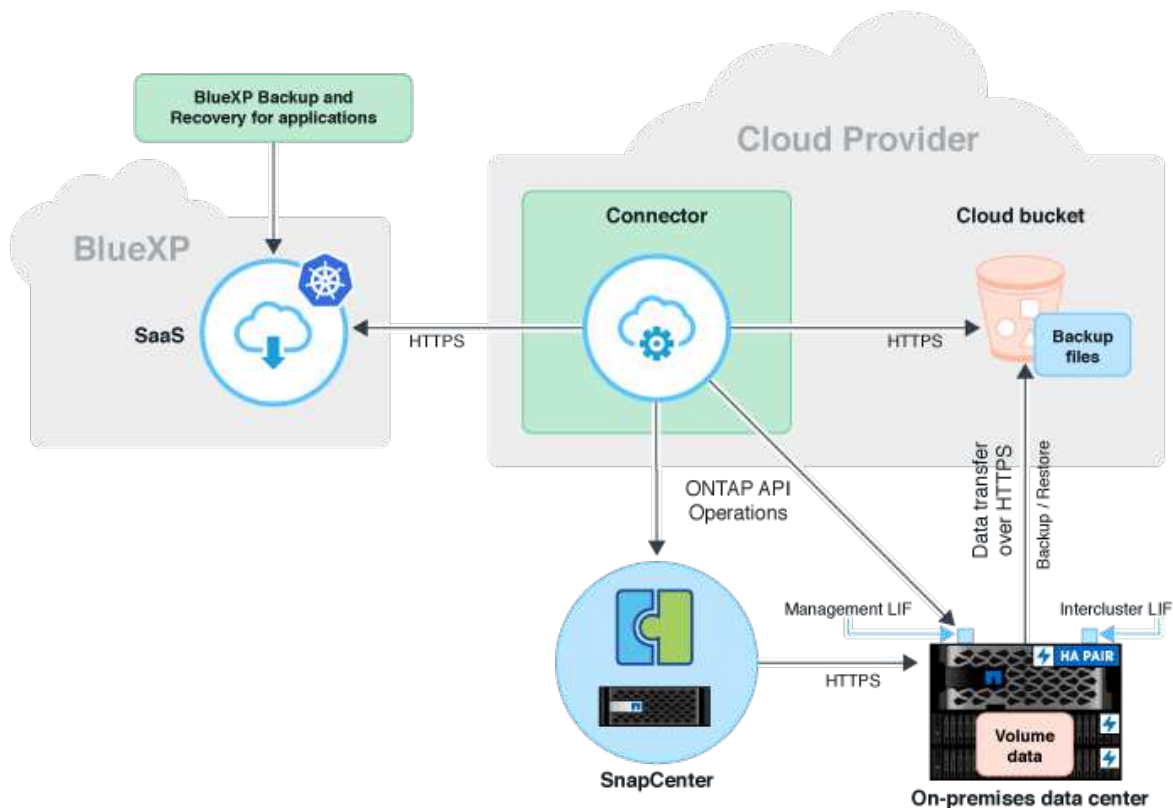
BlueXP Backup and Recovery architecture

BlueXP backup and recovery is a SaaS solution that provides data protection capabilities for applications running on NetApp on-prem 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-premise storage and the NetApp SnapCenter Server.

A BlueXP connector needs to be deployed within the customer virtual network. A connection between the on-premise environment and the cloud environment is required such as a 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-prem 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 is 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 \(netapp.com\)](https://www.netapp.com/datasheet/NetApp-SnapCenter-Configuration-NetApp-Cloud-Backup-and-Recovery-for-Applications.pdf).

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 on-premises applications data | NetApp Documentation](https://www.netapp.com/datasheet/NetApp-BlueXP-Hybrid-Application-Backup-and-Recovery-for-Applications.pdf).

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](https://www.netapp.com/datasheet/NetApp-BlueXP-Connector-Installation-and-Configuration.pdf).

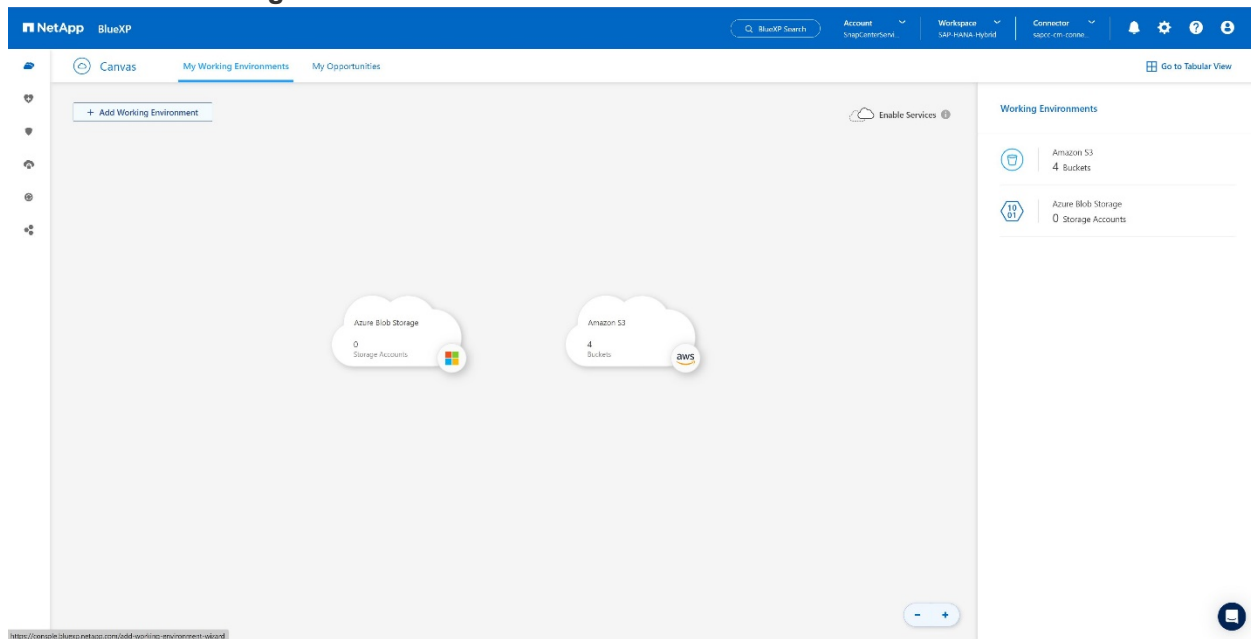
3. Add/buy a Cloud Backup license at BlueXP: <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-licensing-cloud-backup.html>.
4. Create working environment for NetApp on-prem environment and your cloud destination in BlueXP by adding your on-prem storage.
5. Create a new object store relationship for the on-prem 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

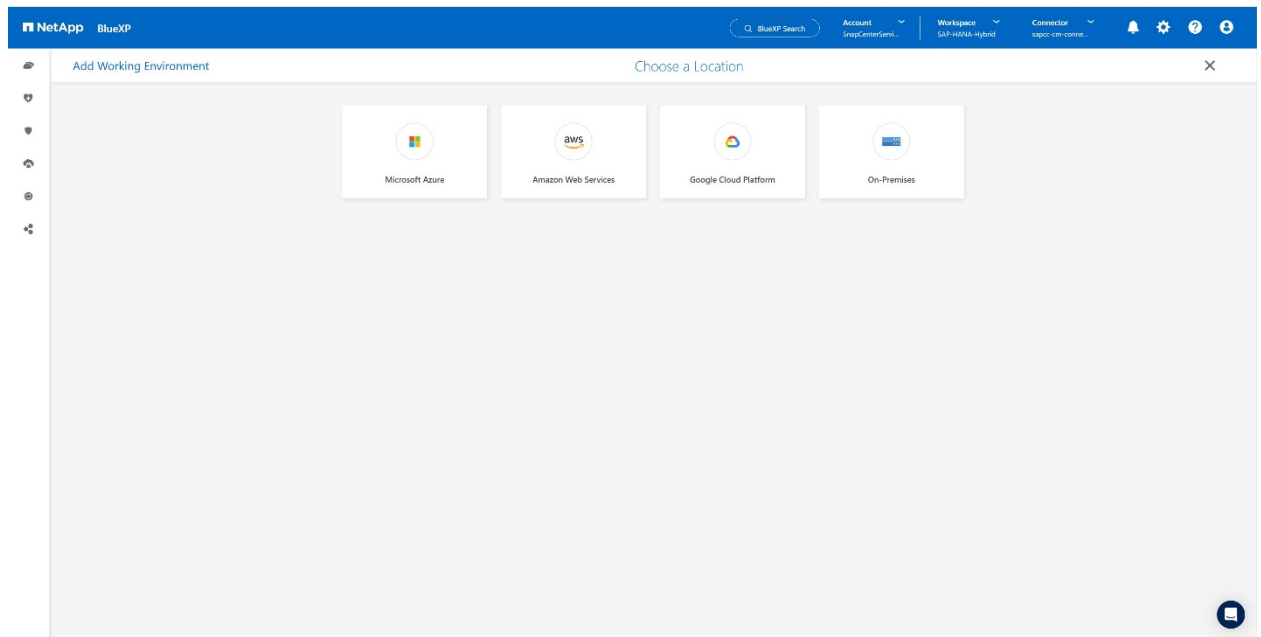
Create working environment for BlueXP

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

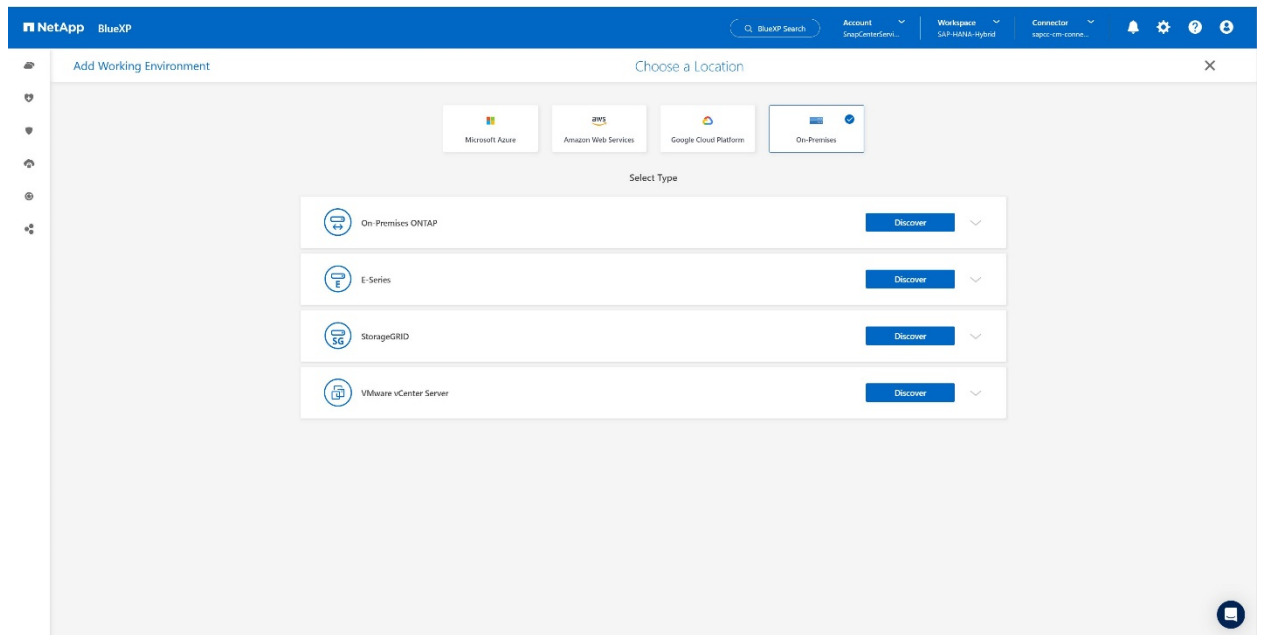
1. At the left menu choose **Storage** → **Canvas** → **My Working Environment**.
2. Press **+ Add Working Environment**.



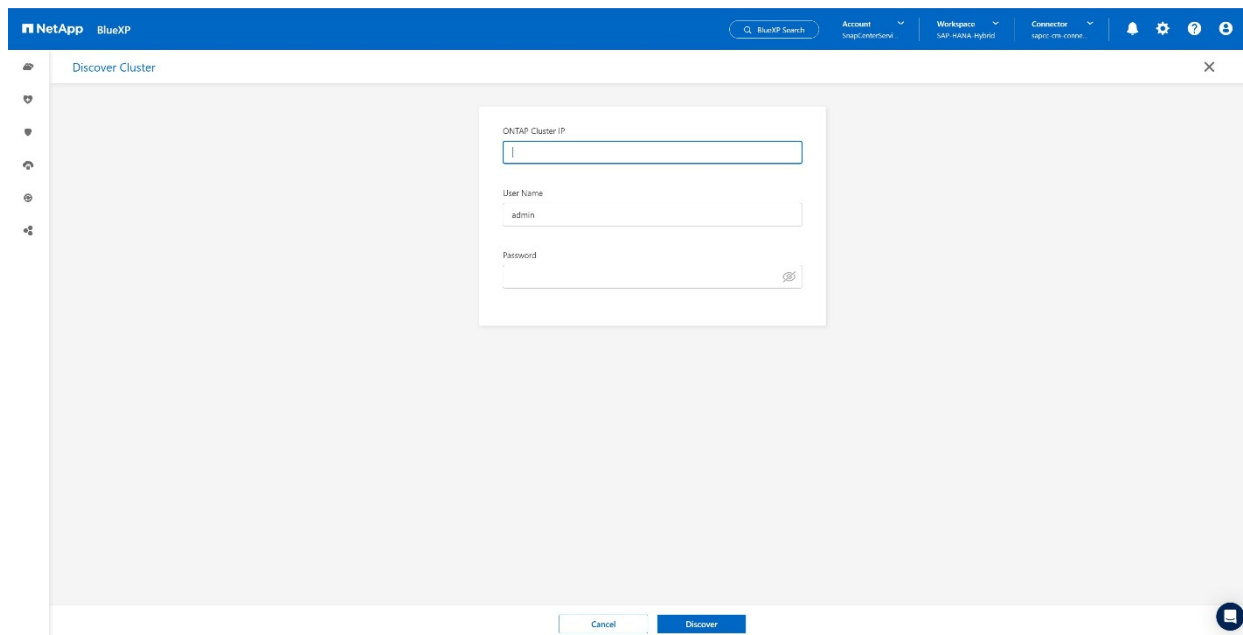
3. Choose **On-Premises**.



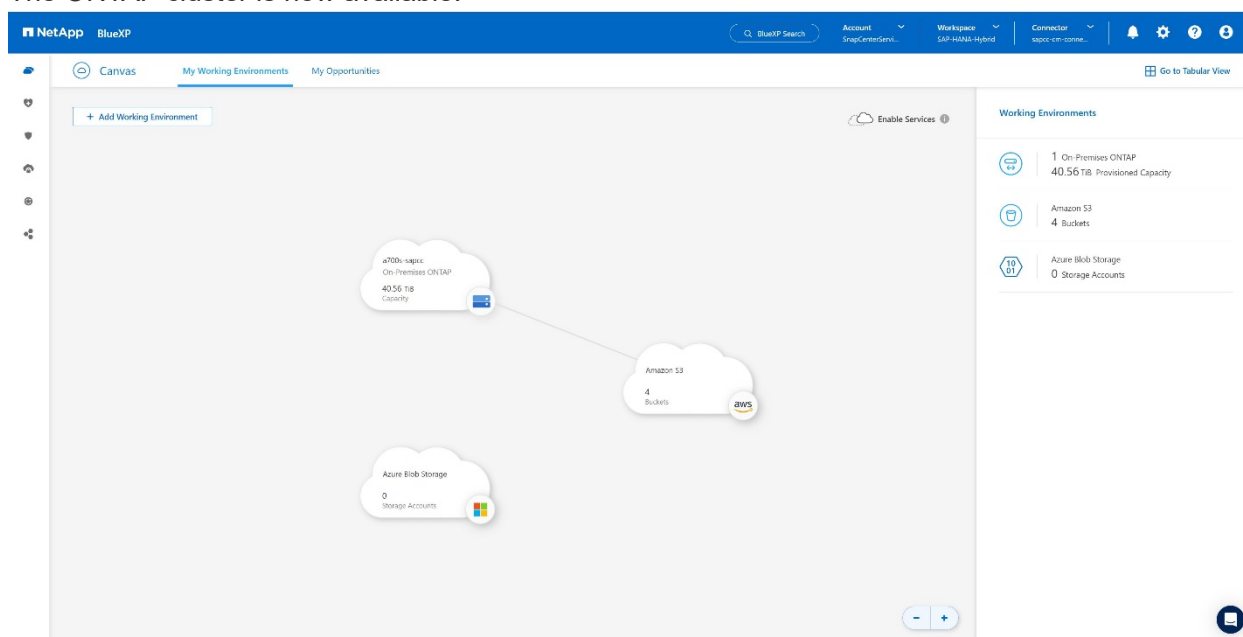
4. Choose **Discover On-Premises ONTAP**.



5. Add the IP address of the ONTAP cluster and the password and press **Discover**.



6. The ONTAP cluster is now available.



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

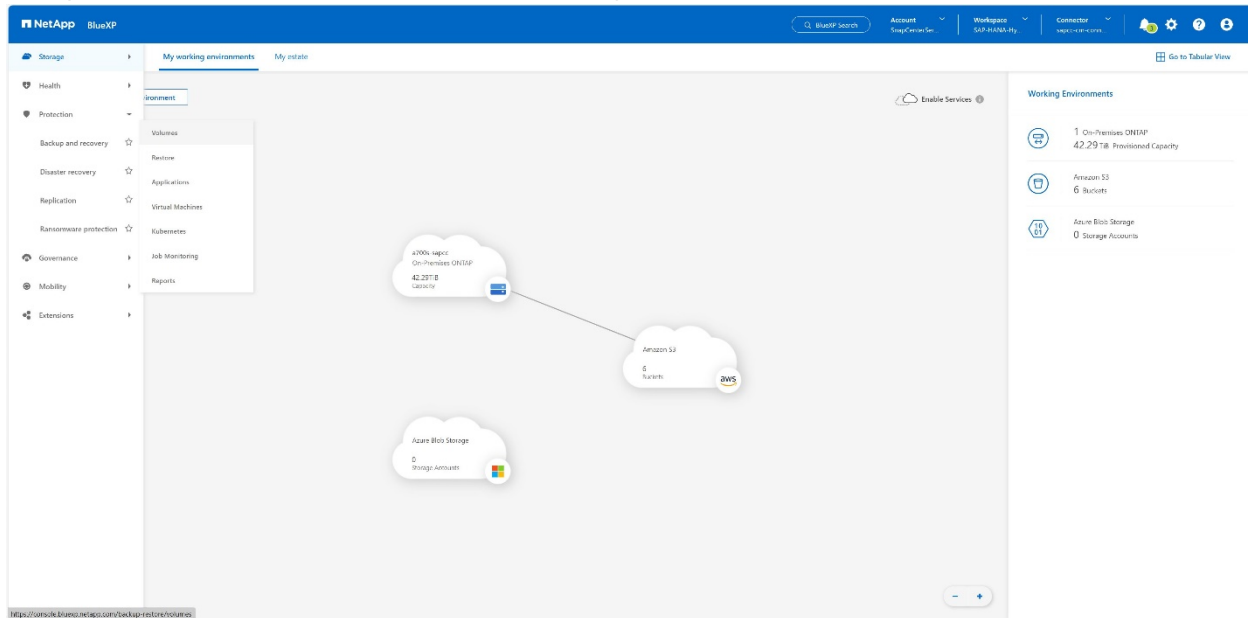
The relationship between the on-premises storage and the S3 bucket is done by creating a backup for an volume or by activating a backup of an application. If an existing site-to-site VPN shall be used for transferring the data from on-premises to S3, a volume backup needs to be used for creating the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

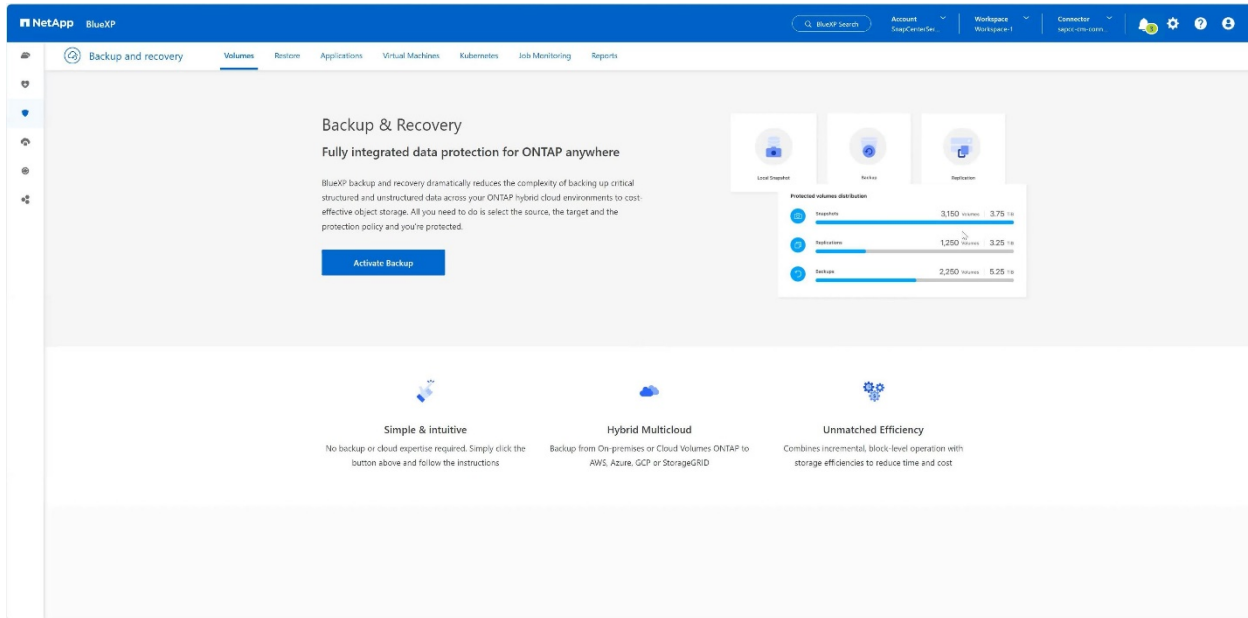
Refer to [Gateway endpoints for Amazon S3 - Amazon Virtual Private Cloud](#) how to setup VPC endpoints for S3 within your VPC.

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

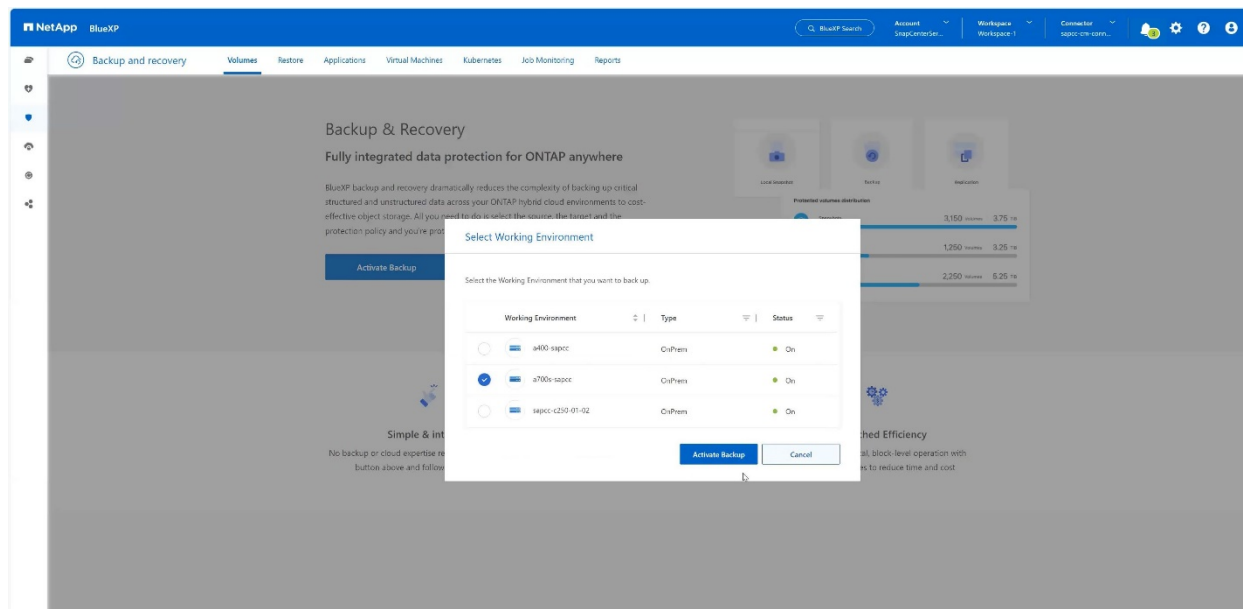
1. Navigate via **Protection** to **Backup and recovery** and choose **Volumes**.



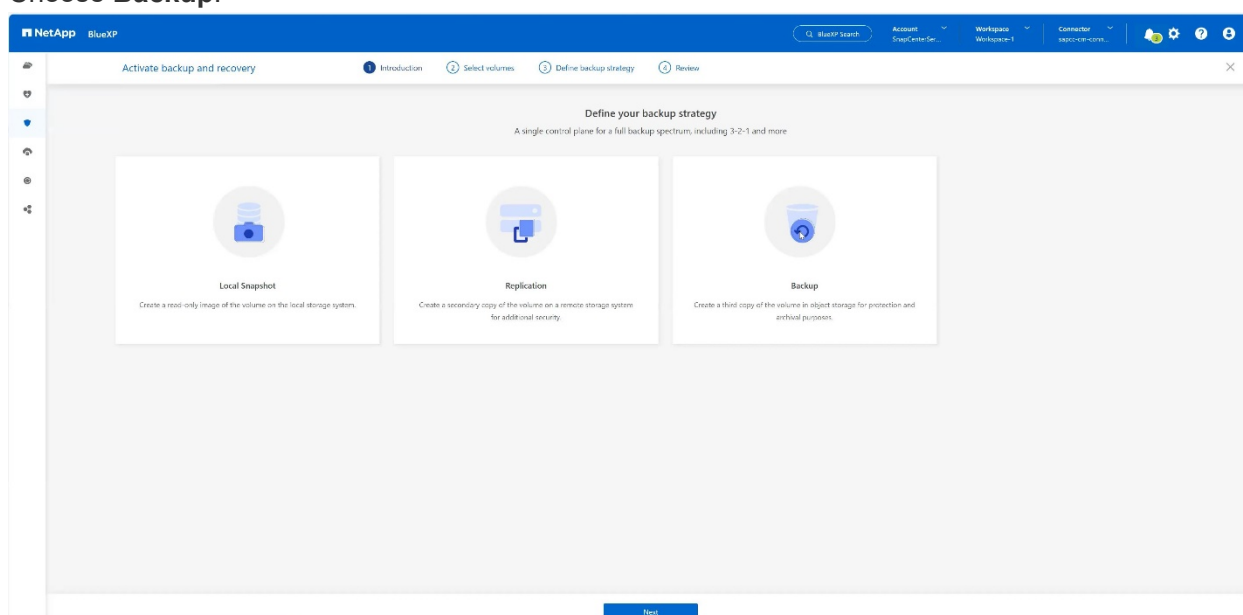
2. Press the **Activate Backup** button.



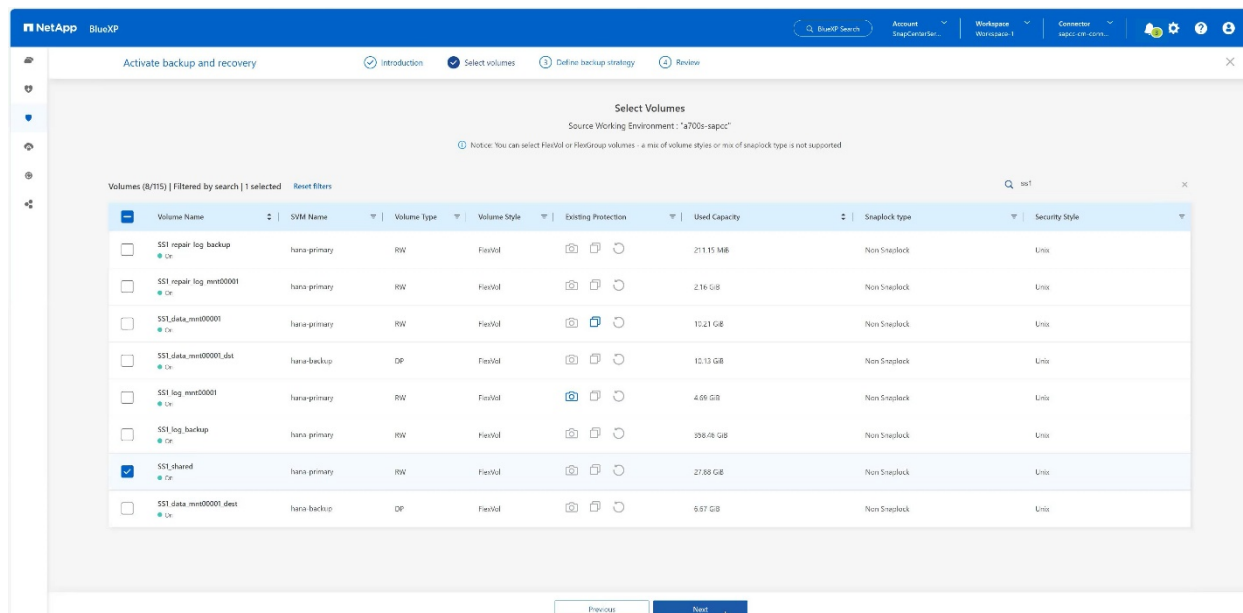
3. Choose the desired on-premises storage system and click **Activate Backup**.



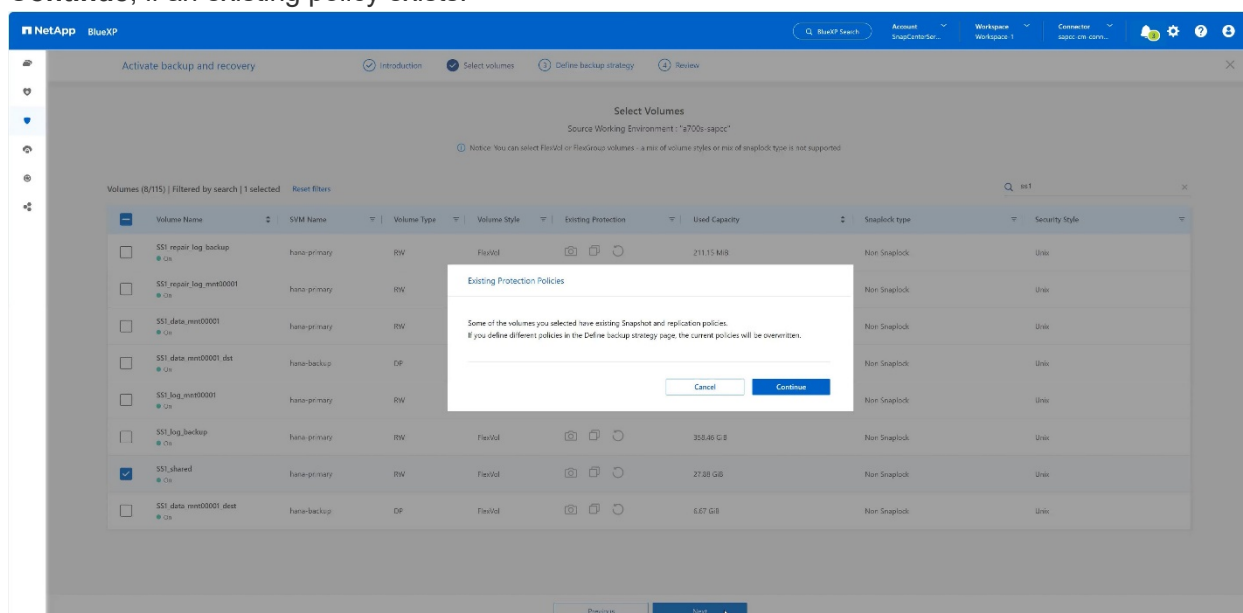
4. Choose **Backup**.



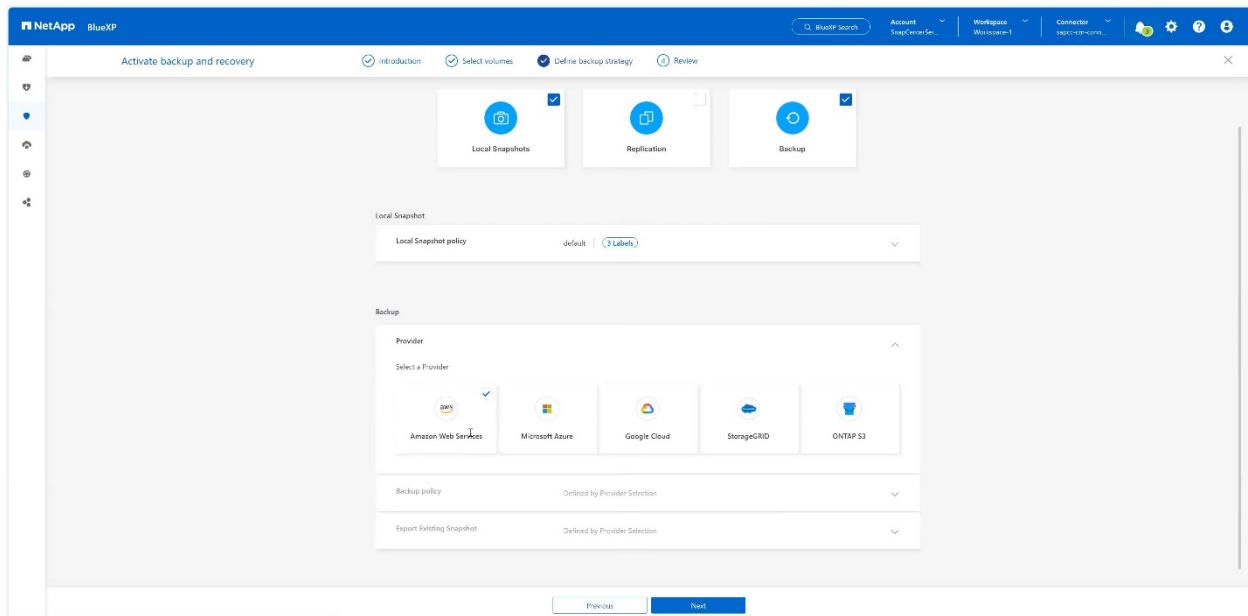
- Choose a volume which is stored at the same SVM as your SAP HANA data files and press **Next**. In this example the volume for /hana/shared has been chosen.



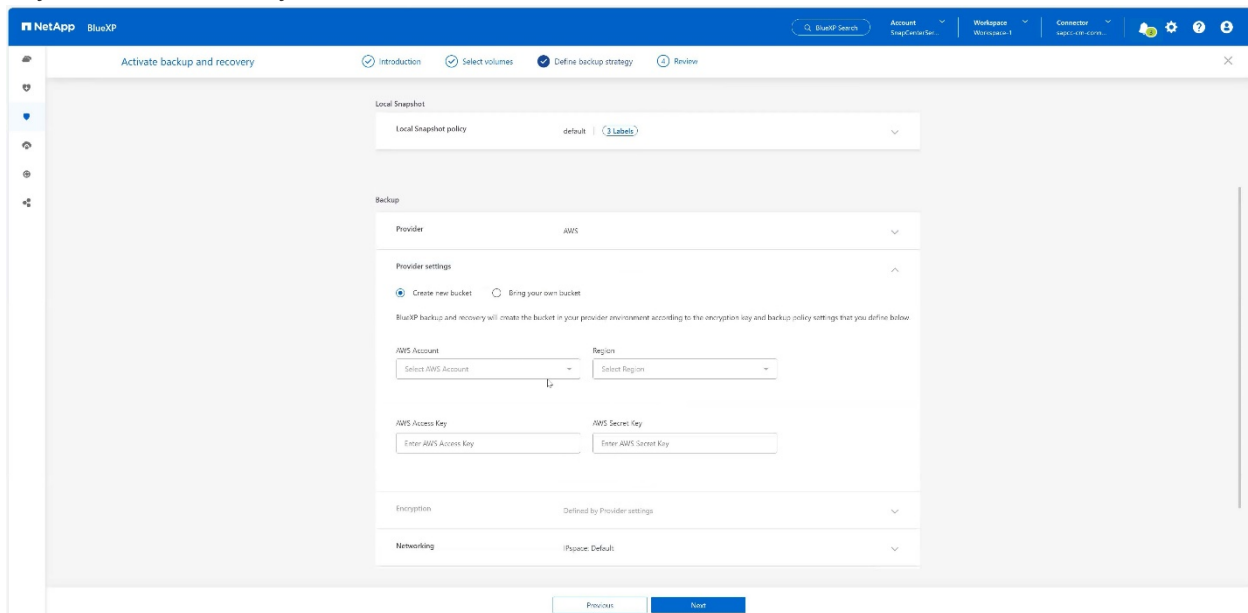
6. **Continue**, if an existing policy exists.



7. 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.



8. Create a new bucket or choose an existing one. Provide your AWS account settings, the region, your access key, and the secret key. Press **Next**.



9. Choose the correct IPspace of your on-premises storage system, select **Privat Endpoint Configuration** and choose the VPC endpoint for the S3. Press **Next**.

NetApp BlueXP | Account: SnapCenterSec | Workspace: Workspace 1 | Connector: snapcenter-conn

Activate backup and recovery | Introduction | Select volumes | Define backup strategy | Review

Backup

Provider: AWS

Provider settings: AWS Account: 123456789012 | Region: us-east-1

Encryption: AWS Managed Encryption Key | AWS SSE S3

Networking: Configure Network Settings

IPspace: Default

☒ Private Endpoint Configuration

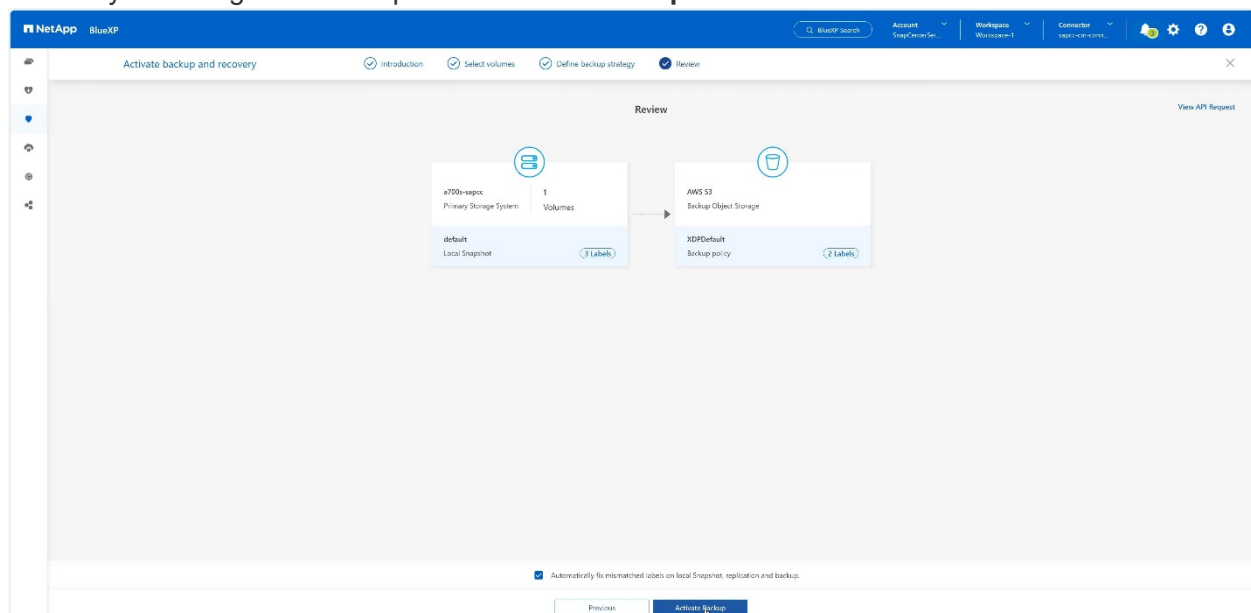
Name	VPC	Origin
...	sapcc-vpc	vpc-0a1b2c3d-e4f5g6h7-i8j9k0

Backup policy: XDRDefault | 2 Labels | Archival policy: None | Disinfect: None

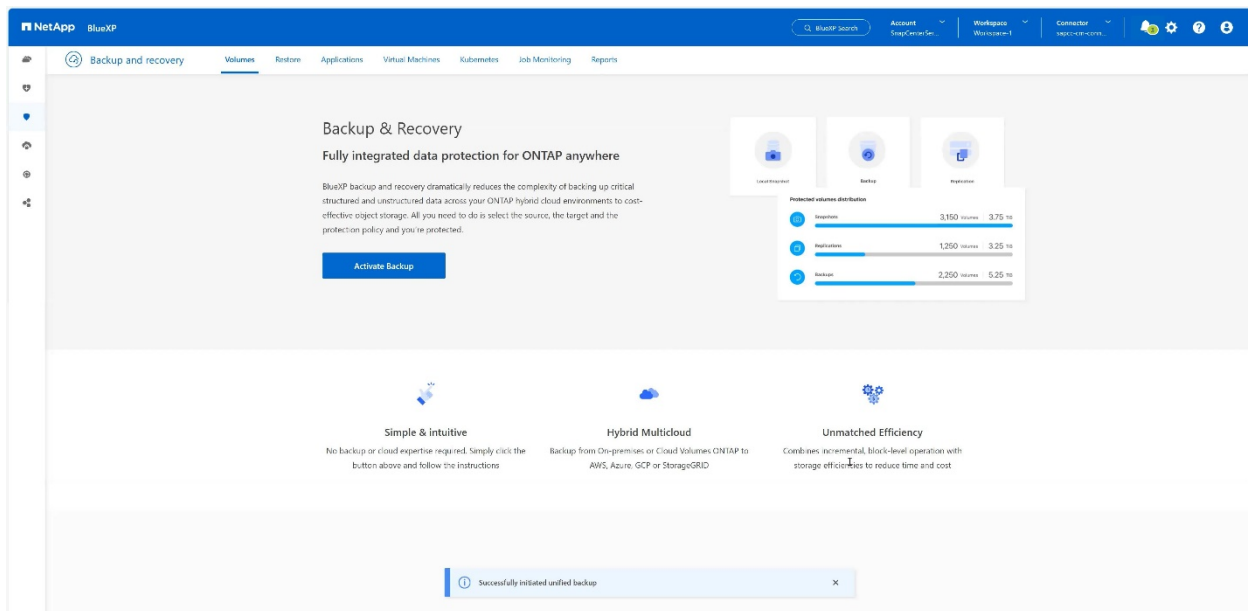
Export Existing Snapshot: Disabled

Previous | Next

10. Review your configuration and press **Activate Backup**.

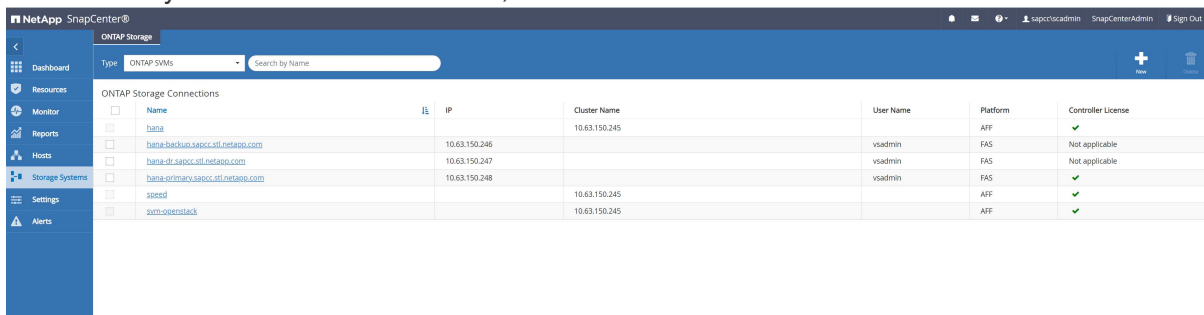


11. The backup has been successfully initiated.

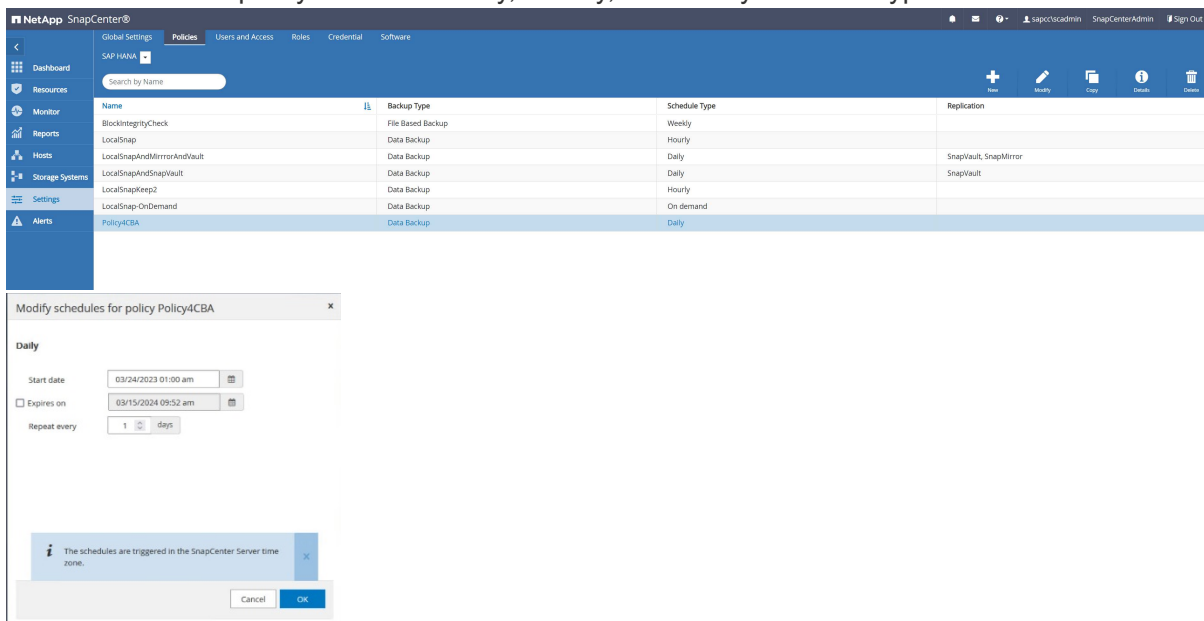


Configure the SAP HANA system resource at SnapCenter

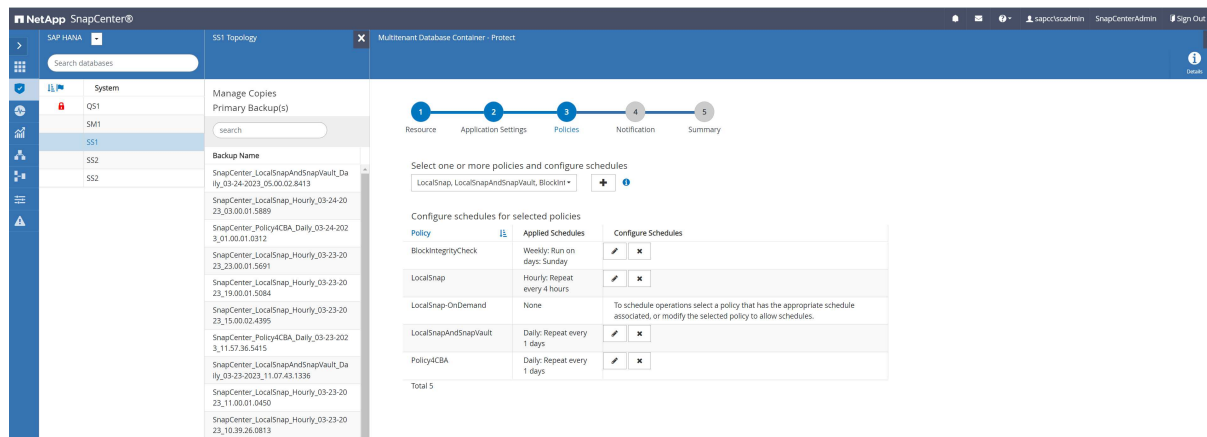
1. Check, if the SVM (hana in this example) where your SAP HANA system is stored has been added via the cluster. If only the SVM has been added, add the cluster.



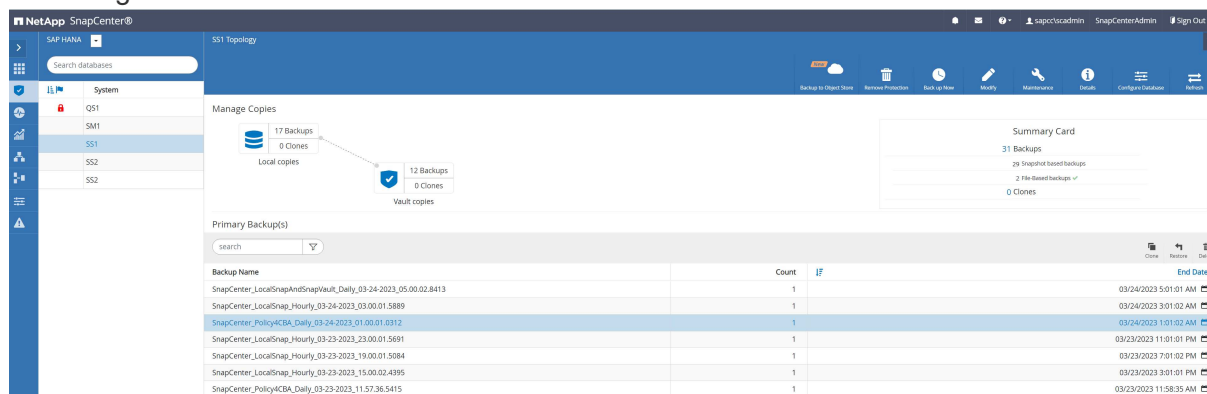
2. Define a schedule policy with either daily, weekly, or monthly schedule type.



3. Add the new policy to your SAP HANA system and assign a daily schedule.

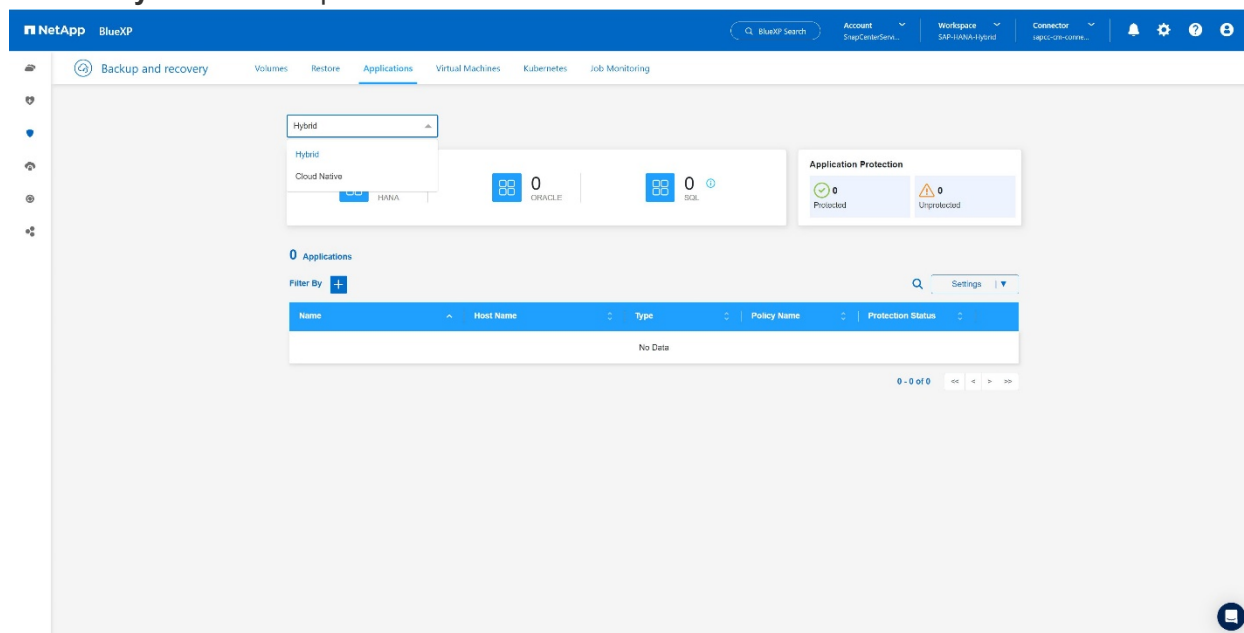


- Once configured new backups with this policy will be available after the policy has been executed according to the schedule defined.

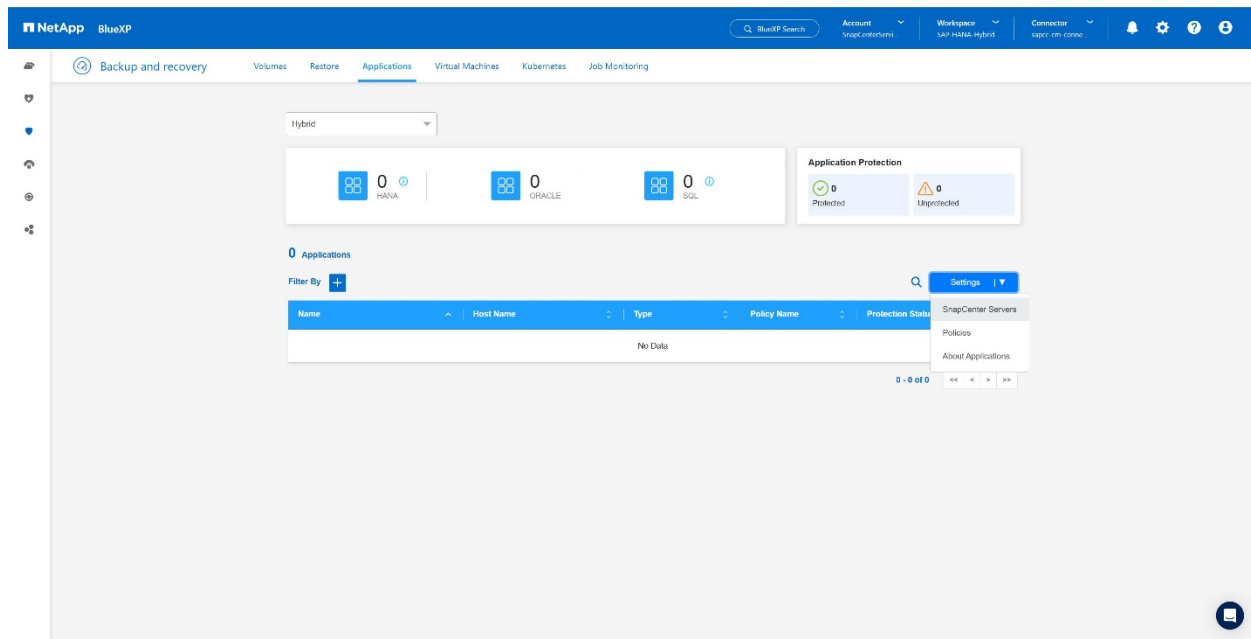


Adding SnapCenter to the BlueXP Working Environment

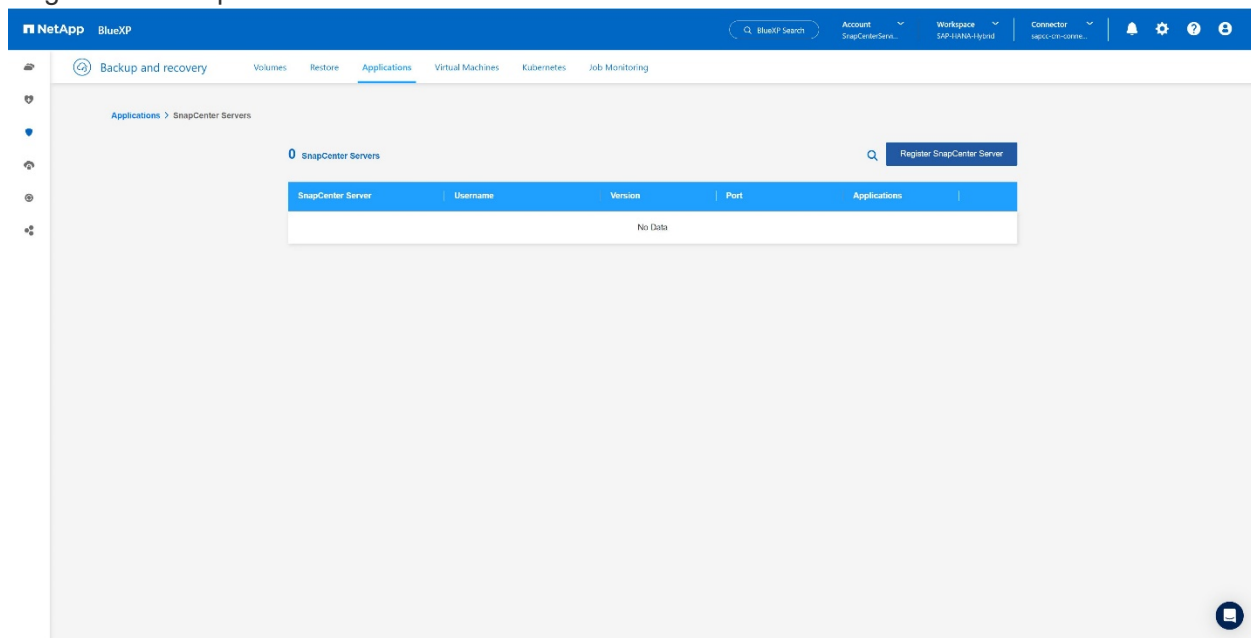
- At the left menu choose **Protection** → **Backup and recovery** → **Applications**.
- Choose **Hybrid** from the pulldown menu.



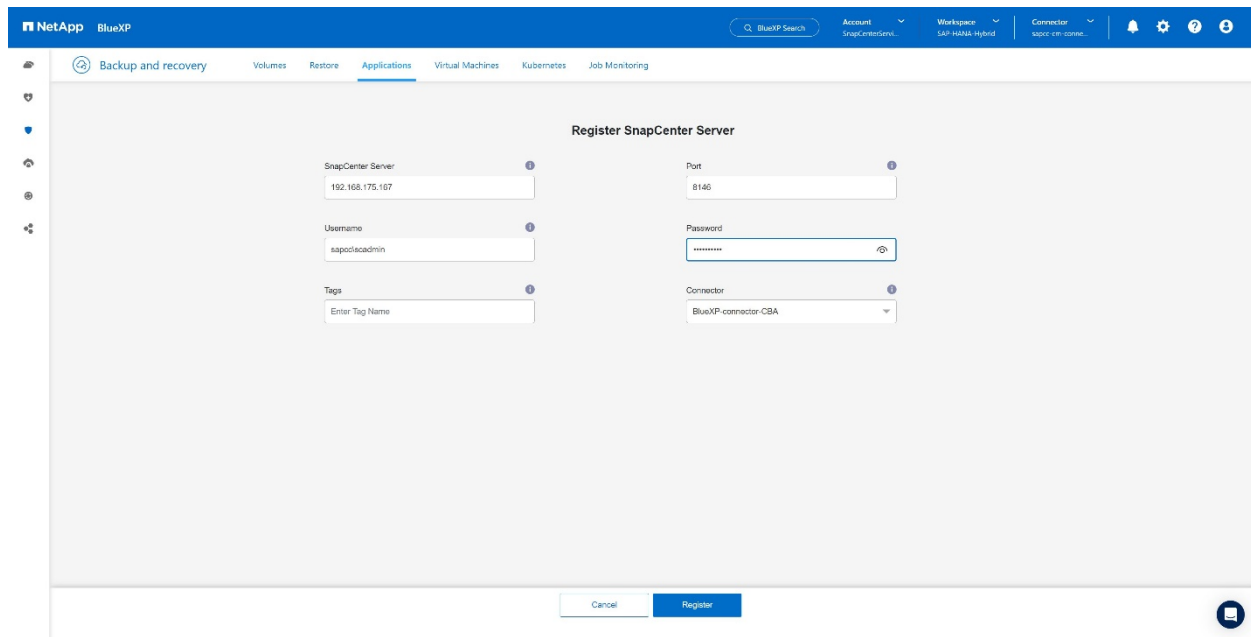
- Choose **SnapCenter Servers** at the Settings menu.



4. Register the SnapCenter Server.



5. Add the SnapCenter Server credentials.

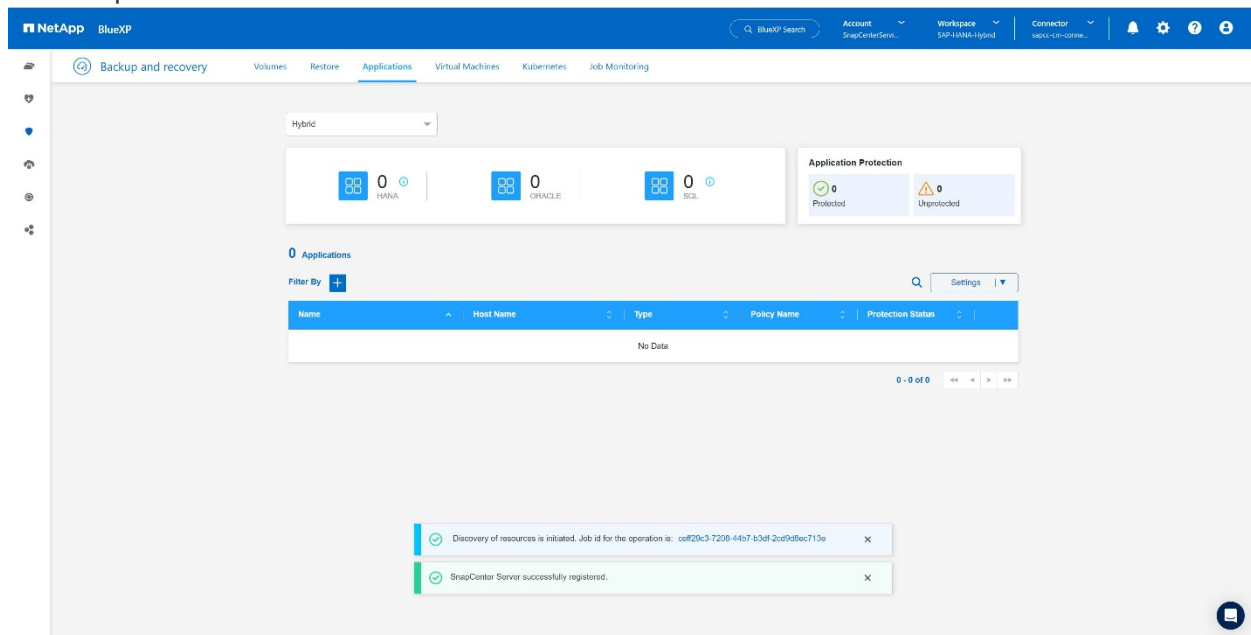


The screenshot shows the 'Register SnapCenter Server' form in the NetApp BlueXP interface. The form is titled 'Register SnapCenter Server' and contains the following fields:

- SnapCenter Server:** 192.168.175.167
- Port:** 8146
- Username:** sapccadmin
- Password:** (masked with asterisks)
- Tags:** Enter Tag Name
- Connector:** BlueXP-connector-CBA

At the bottom of the form, there are 'Cancel' and 'Register' buttons.

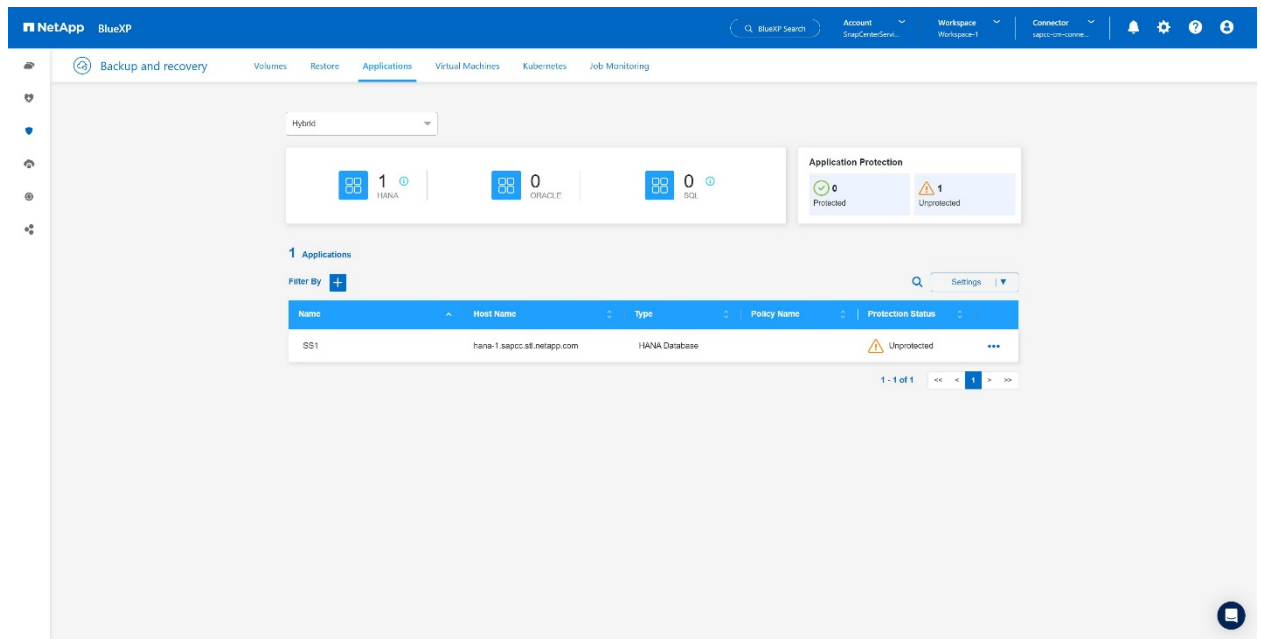
6. The SnapCenter Servers has been added and data will discovered.



The screenshot shows the 'Applications' page in the NetApp BlueXP interface. The page displays the following information:

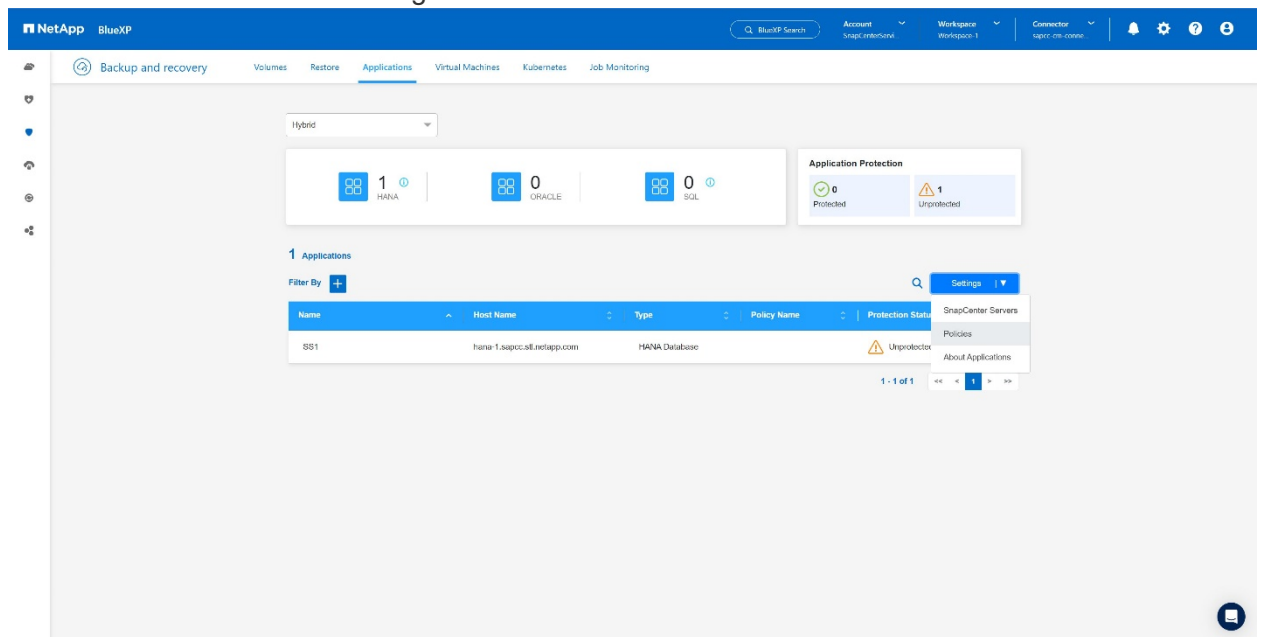
- Hybrid** dropdown menu.
- Application Protection** section showing 0 Protected and 0 Unprotected applications.
- 0 Applications** section with a 'Filter By' button and a search icon.
- Table:** A table with columns: Name, Host Name, Type, Policy Name, and Protection Status. The table is currently empty, showing 'No Data'.
- Discovery Log:** A log at the bottom showing two successful messages:
 - Discovery of resources is initiated. Job id for the operation is: cef20c3-7208-4457-b3d8-2a09d8ec713e
 - SnapCenter Server successfully registered.

7. Once the discovery job has been finished the SAP HANA system will be available.

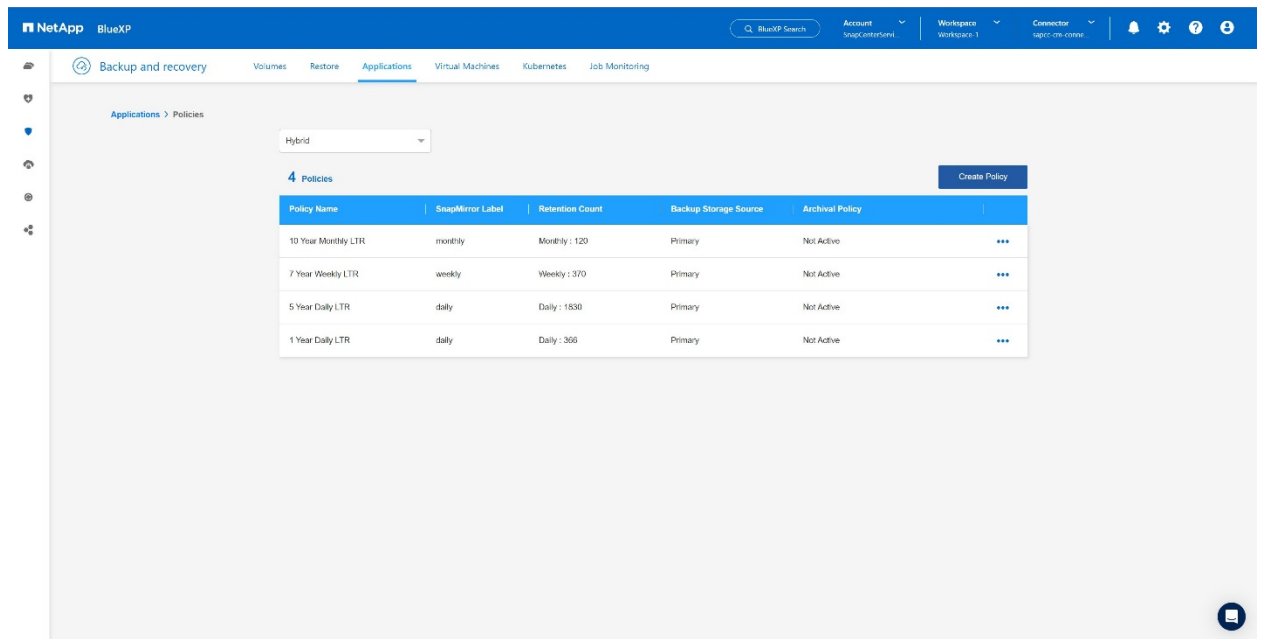


Creating a Backup Policy for Application Backup

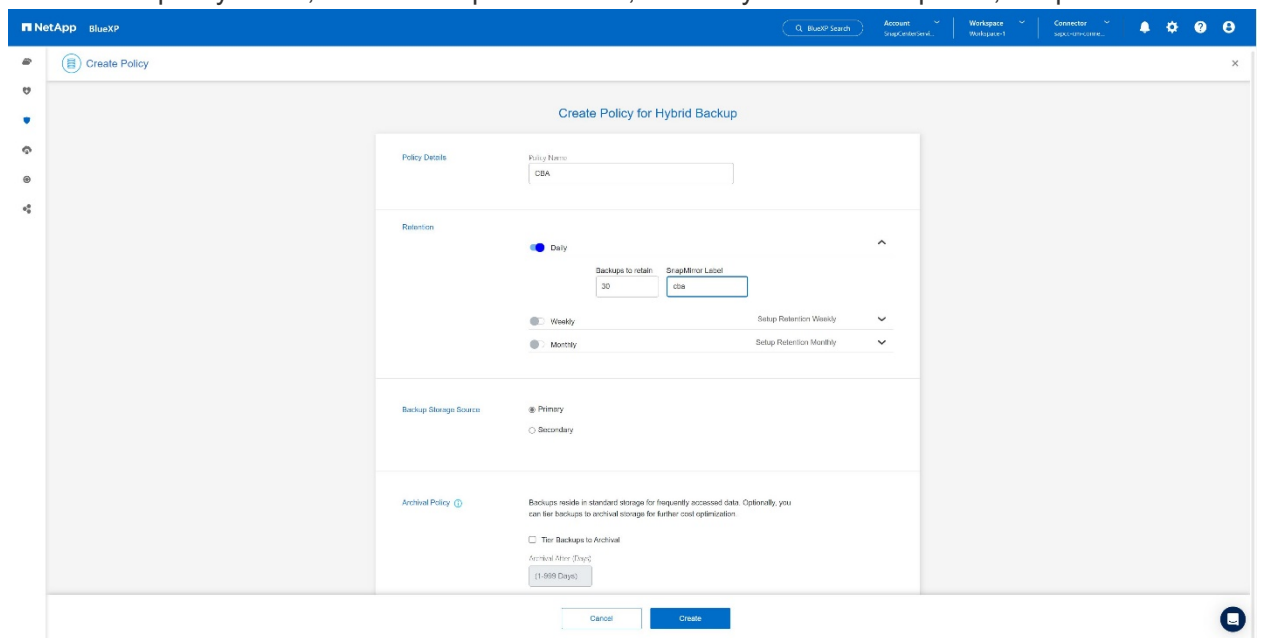
1. Choose **Policies** within the settings menu.



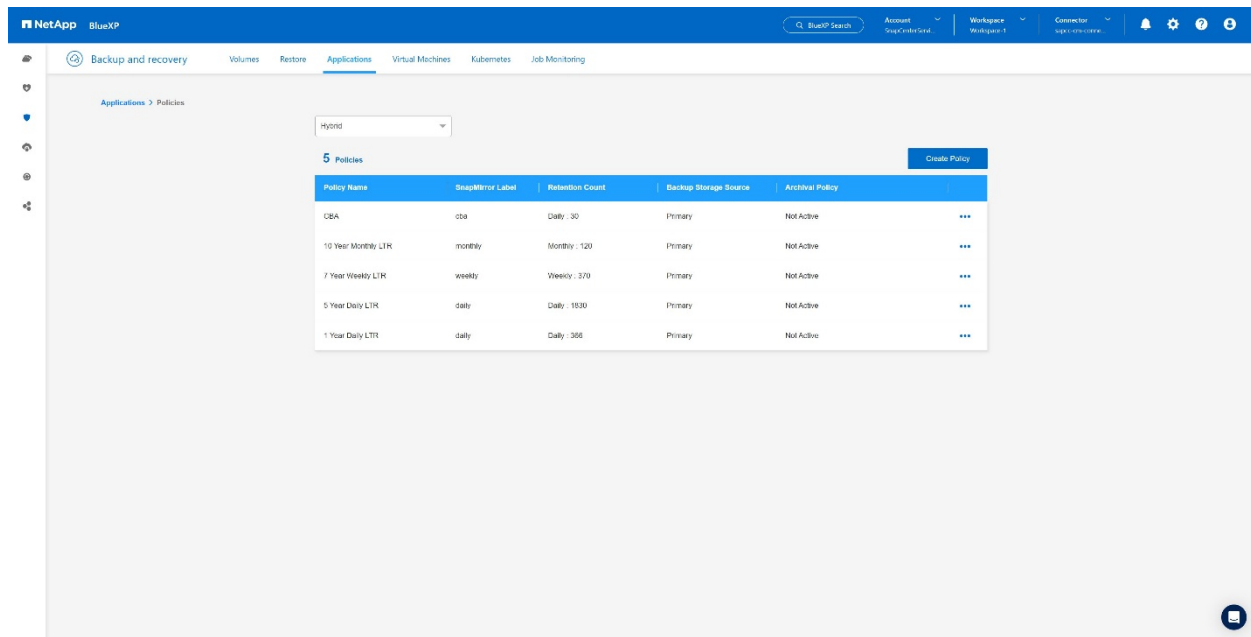
2. Create a new policy, if desired by click **Create Policy**.



3. Provide the policy name, desired SnapMirror label, choose your desired options, and press **Create**.

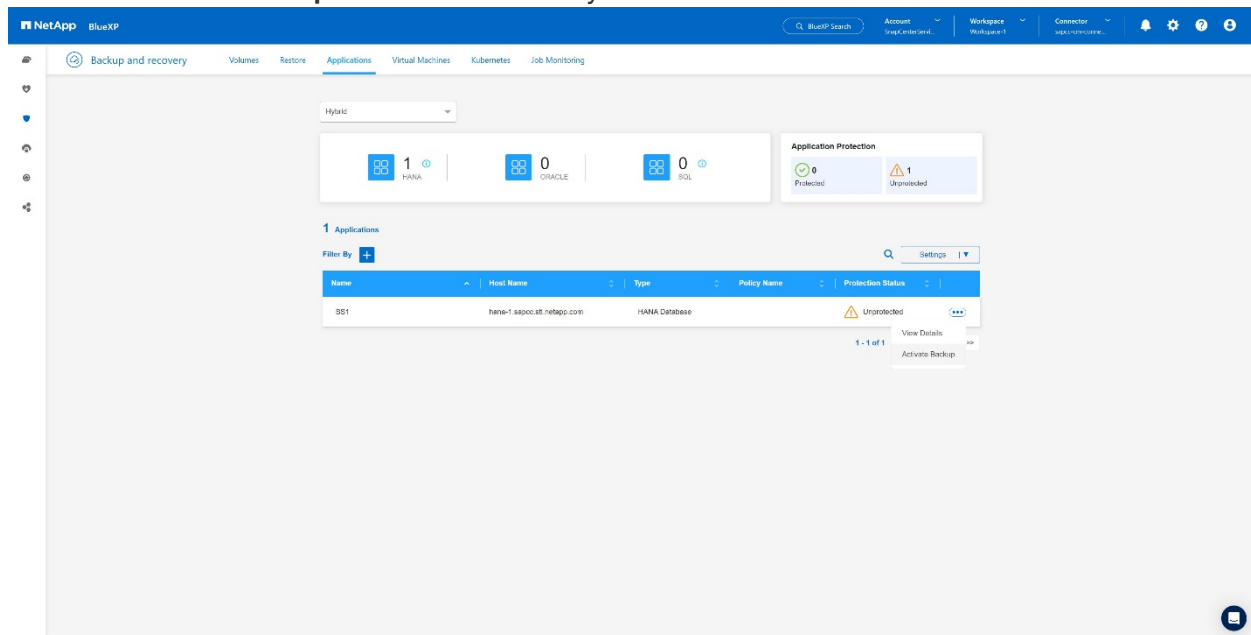


4. The new policy is available.

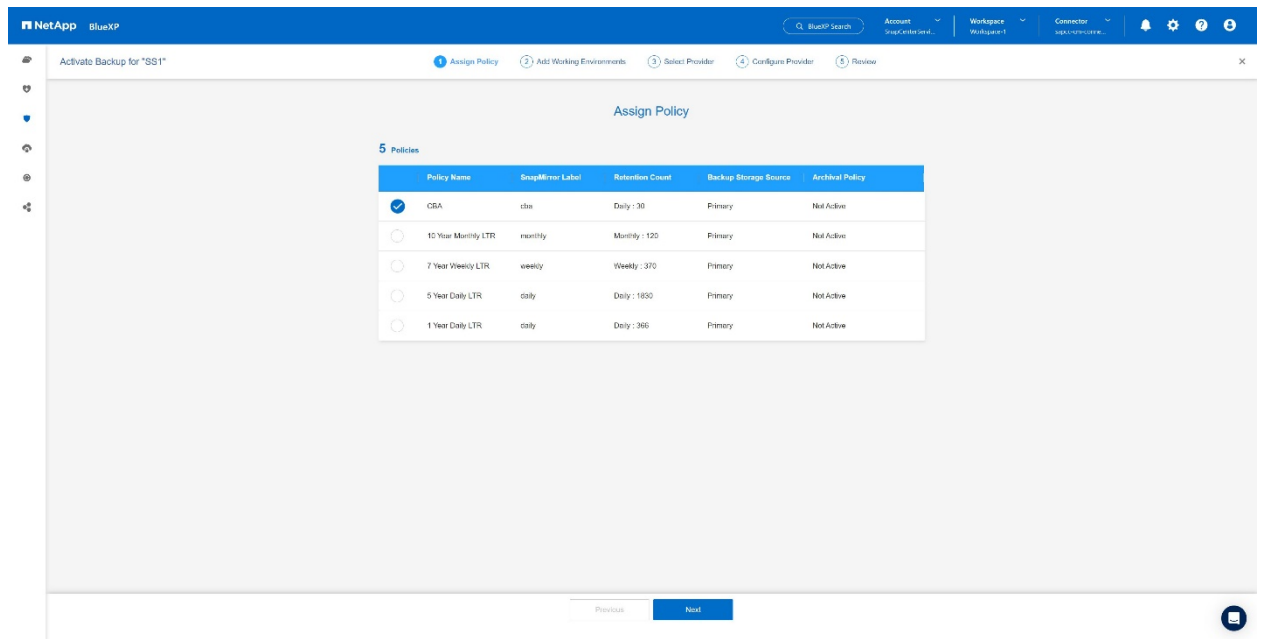


Protecting the SAP HANA database with Cloud Backup for Applications

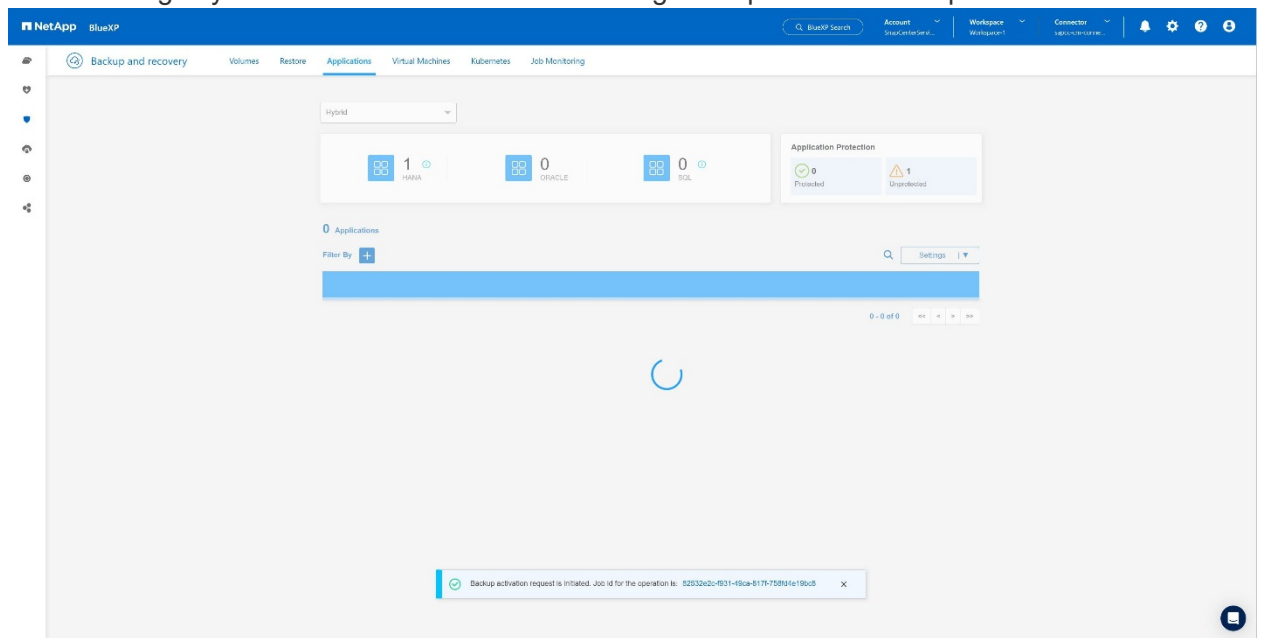
1. Choose **Activate Backup** for the SAP HANA system.



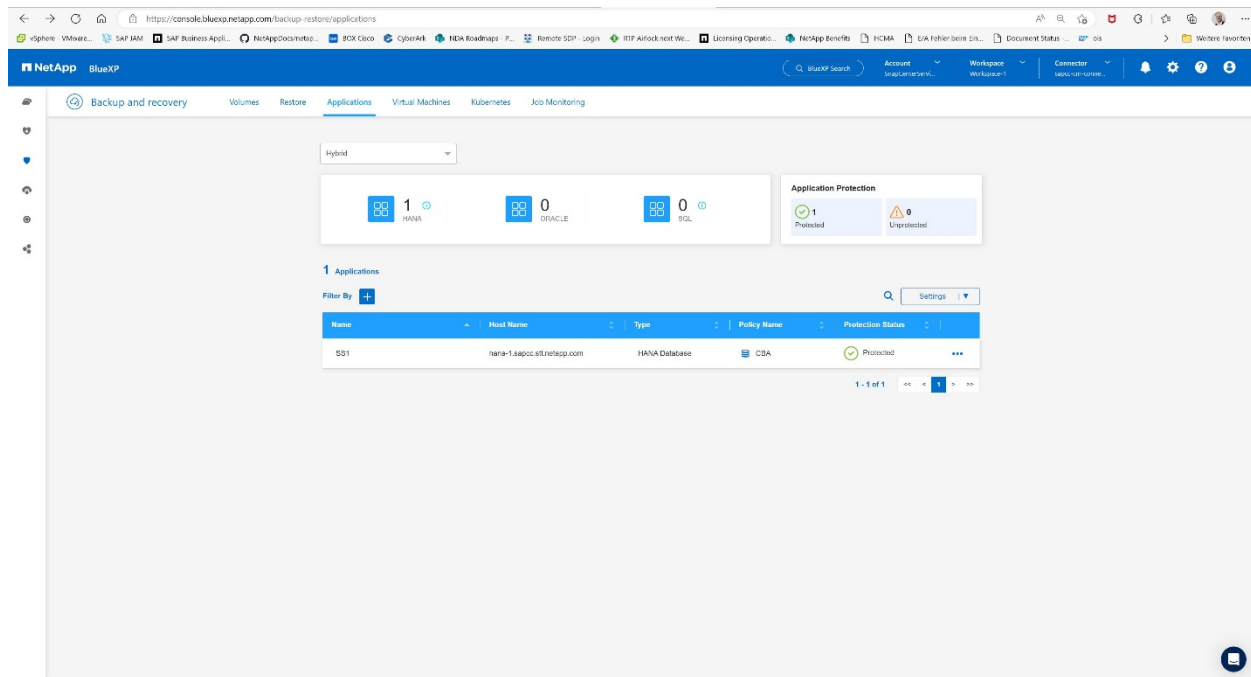
2. Choose the previously created policy and click **Next**.



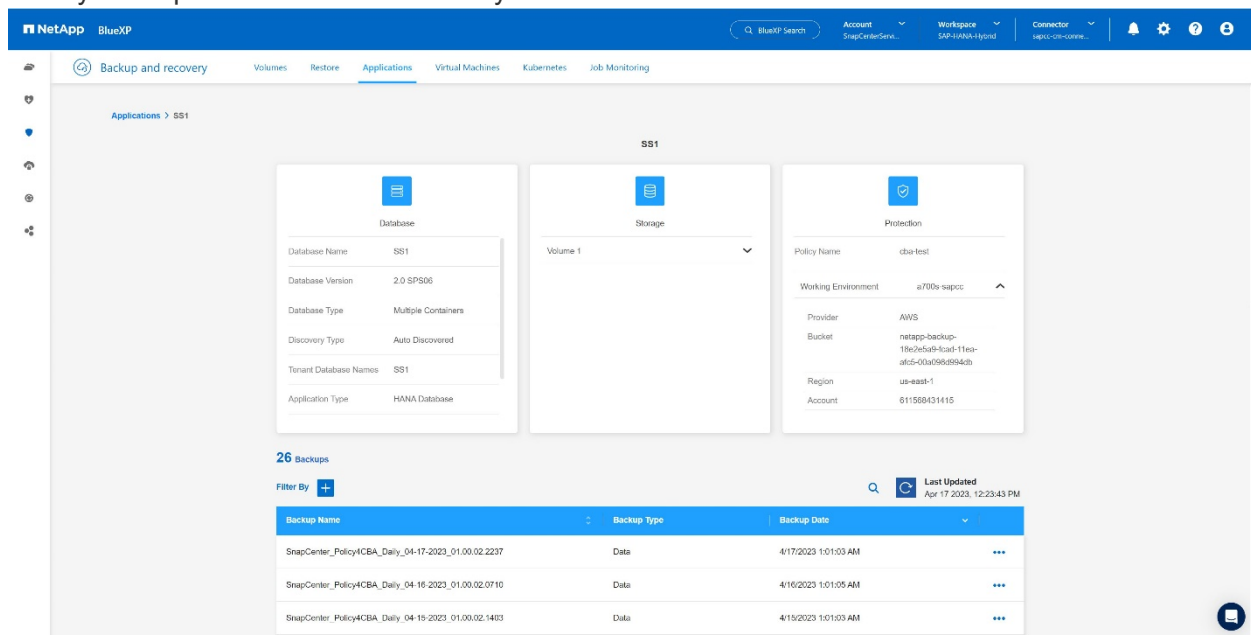
3. As the storage system and the connector have configured upfront the backup will be activated.



4. Once the job has been completed the System will be listed.



5. 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.



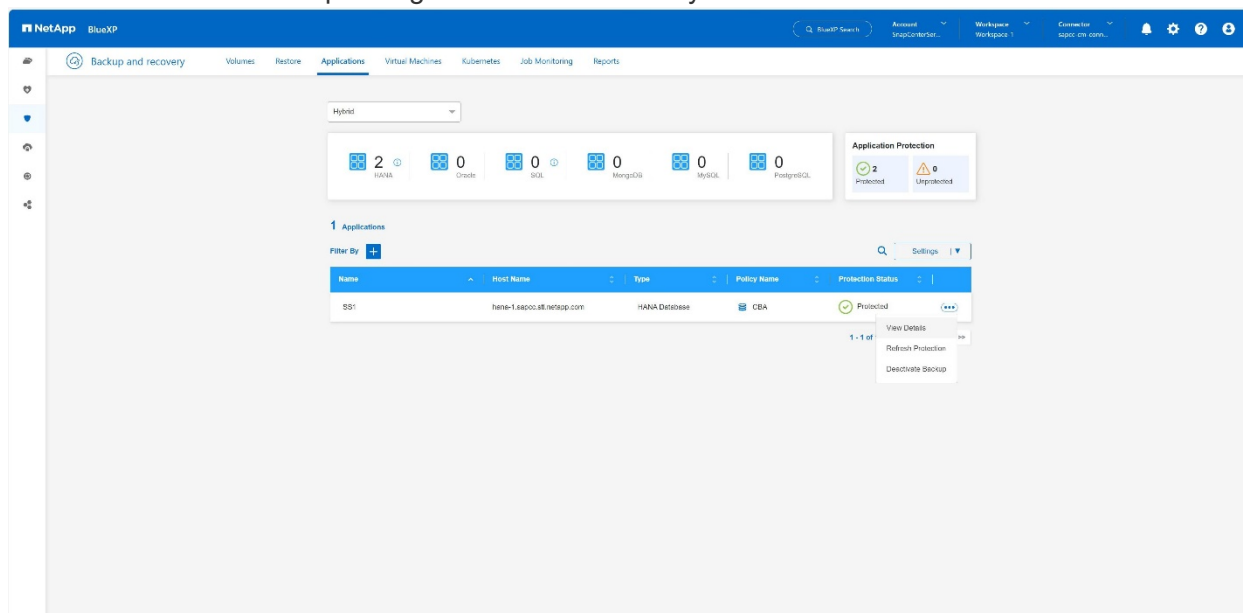
In some environments it might be necessary to remove any existing schedule settings of the snapmirror source. To do so execute the following command at the source ONTAP system: `snapmirror modify -destination -path <hana-cloud-svm>:<SID_data_mnt00001>_copy -schedule ""`.

Restoring SAP HANA BlueXP Backup

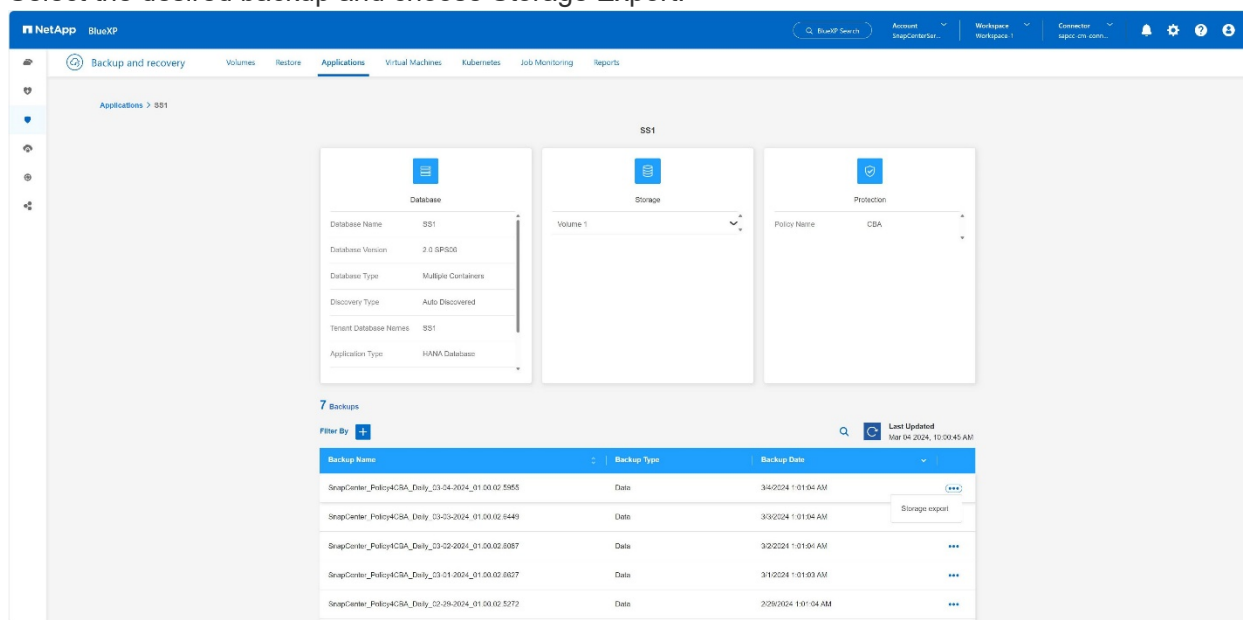
A restore from of the backup can only be done to an on-premises NetApp ONTAP based storage system or NetApp CVO within the cloud. A restore can be done by doing the following steps:

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**.
3. Click **View Details** corresponding to the database that you want to restore.



4. Select the desired backup and choose Storage Export.



5. Provide the desired options:

NetApp BlueXP

Restore "SS1"

1 Restore options 2 Storage mapping 3 Review

Restore options

Specify where you want to export the backup

FQDN or IP address

10.10.10.10

Initiators for SAN

Change storage location

By default the backup from object store will be restored in the source SVM. Use this option to choose alternate storage if the source storage does not have enough space.

Previous Next

- 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**.

NetApp BlueXP

Restore "SS1"

1 Restore options 2 Storage mapping 3 Review

Review

Backup Name	SnapCenter_PolicyICBA_Daily_03-04-2024_01:00:02.9999
FQDN or IP address	10.10.10.10
Initiators for SAN	
Destination volume name suffix	_restore

Previous Restore

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-netapp-solution>

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.