



BlueXP SaaS for Oracle - Azure

NetApp Solutions

NetApp
October 20, 2023

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/databases/snapctr_svcs_oracle_azure.html on October 20, 2023. Always check docs.netapp.com for the latest.

Table of Contents

- TR-4977: Oracle Database backup, restore and clone with SnapCenter Services - Azure 1
 - Purpose 1
 - Audience 1
 - Solution test and validation environment 1
 - Solution deployment. 3
 - Additional information. 34

TR-4977: Oracle Database backup, restore and clone with SnapCenter Services - Azure

Allen Cao, Niyaz Mohamed, NetApp

Purpose

SnapCenter Services is the SaaS version of the classic SnapCenter database management UI tool that is available through the NetApp BlueXP cloud management console. It is an integral part of the NetApp cloud-backup, data-protection offering for databases such as Oracle and HANA running on Azure NetApp Files. This SaaS-based service simplifies traditional SnapCenter standalone server deployment that generally requires a Windows server operating in a Windows domain environment.

In this documentation, we demonstrate how you can set up SnapCenter Services to backup, restore, and clone Oracle databases deployed on Azure NetApp Files volumes and Azure compute instances. It is very easy to setup data protection for Oracle database deployed on Azure NetApp Files with web based BlueXP user interface.

This solution addresses the following use cases:

- Database backup with snapshots for Oracle databases hosted in Azure NetApp Files and Azure VMs
- Oracle database recovery in the case of a failure
- Fast cloning of primary databases for dev, test environments or other use cases

Audience

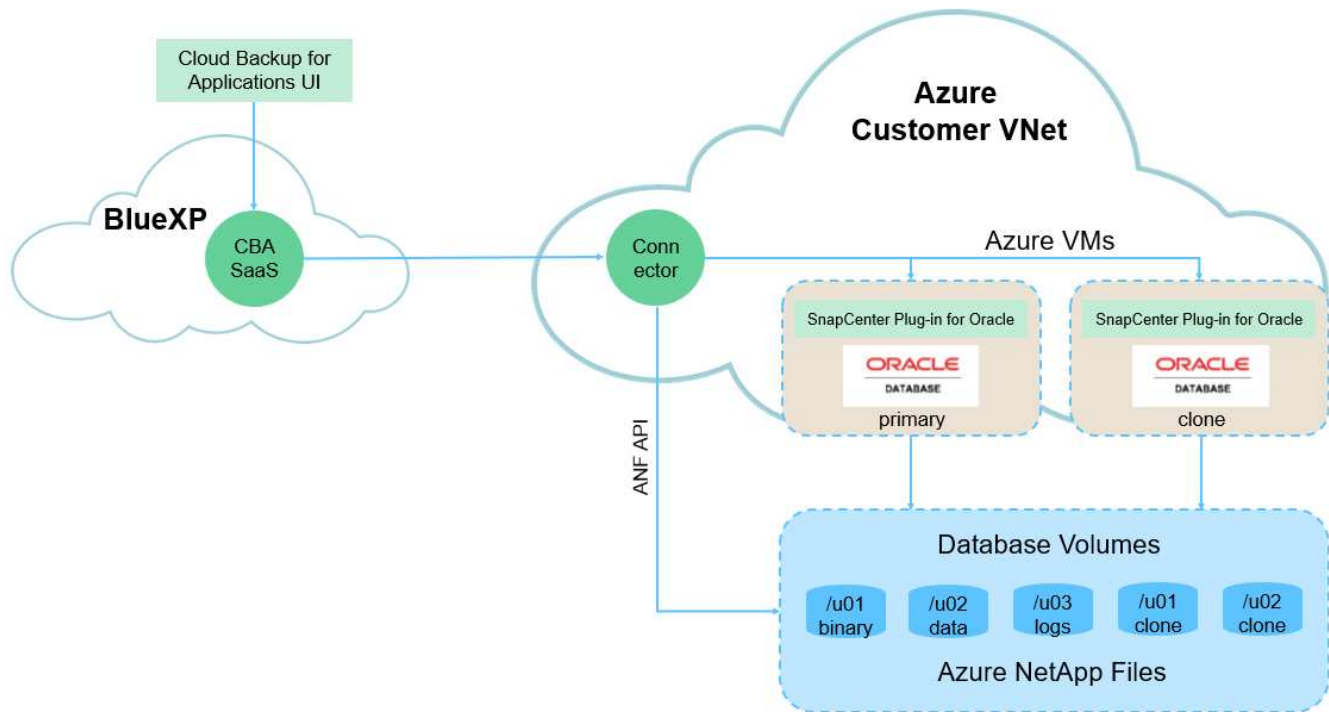
This solution is intended for the following audiences:

- The DBA who manages Oracle databases running on Azure NetApp Files storage
- The solution architect who is interested in testing Oracle database backup, restore, and clone in Azure
- The storage administrator who supports and manages the Azure NetApp Files storage
- The application owner who owns applications that are deployed to Azure NetApp Files storage and Azure VMs

Solution test and validation environment

The testing and validation of this solution was performed in a lab environment that might not match the final deployment environment. For more information, see the section [\[Key Factors for Deployment Consideration\]](#).

Architecture



This image provides a detailed picture of BlueXP backup and recovery for applications within the BlueXP console, including the UI, the connector, and the resources it manages.

Hardware and software components

Hardware

Azure NetApp Files storage	Premium Service level	Auto QoS type, and 4TB in storage capacity in testing
Azure instance for compute	Standard B4ms (4 vcpus, 16 GiB memory)	Two instances deployed, one as primary DB server and the other as clone DB server

Software

RedHat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Deployed RedHat subscription for testing
Oracle Database	Version 19.18	Applied RU patch p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Version 12.2.0.1.36	Latest patch p6880880_190000_Linux-x86-64.zip
SnapCenter Service	Version v2.5.0-2822	Agent Version v2.5.0-2822

Key factors for deployment consideration

- **Connector to be deployed in the same virtual network / subnet as databases and Azure NetApp Files.** When possible, the connector should be deployed in the same Azure virtual networks and resource groups, which enables connectivity to the Azure NetApp Files storage and the Azure compute instances.

- **An Azure user account or Active Directory service principle created at Azure portal for SnapCenter connector.** Deploying a BlueXP Connector requires specific permissions to create and configure a virtual machine and other compute resources, to configure networking, and to get access to the Azure subscription. It also requires permissions to later create roles and permissions for the Connector to operate. Create a custom role in Azure with permissions and assign to the user account or service principle. Review the following link for details: [Set up Azure permissions](#).
- **A ssh key pair created in the Azure resource group.** The ssh key pair is assigned to the Azure VM user for logging into the connector host and also the database VM host for deploying and executing a plug-in. BlueXP console UI uses the ssh key to deploy SnapCenter service plugin to database host for one-step plugin installation and application host database discovery.
- **A credential added to the BlueXP console setting.** To add Azure NetApp Files storage to the BlueXP working environment, a credential that grants permissions to access Azure NetApp Files from the BlueXP console needs to be set up in the BlueXP console setting.
- **java-11-openjdk installed on the Azure VM database instance host.** SnapCenter service installation requires java version 11. It needs to be installed on application host before plugin deployment attempt.

Solution deployment

There is extensive NetApp documentation with a broader scope to help you protect your cloud-native application data. The goal of this documentation is to provide step-by-step procedures that cover SnapCenter Service deployment with the BlueXP console to protect your Oracle database deployed on an Azure NetApp Files storage and an Azure compute instance.

To get started, complete the following steps:

- Read the general instructions [Protect your cloud native applications data](#) and the sections related to Oracle and Azure NetApp Files.
- Watch the following video walkthrough

[Video of deployment of Oracle and ANF](#)

Prerequisites for SnapCenter service deployment

Deployment requires the following prerequisites.

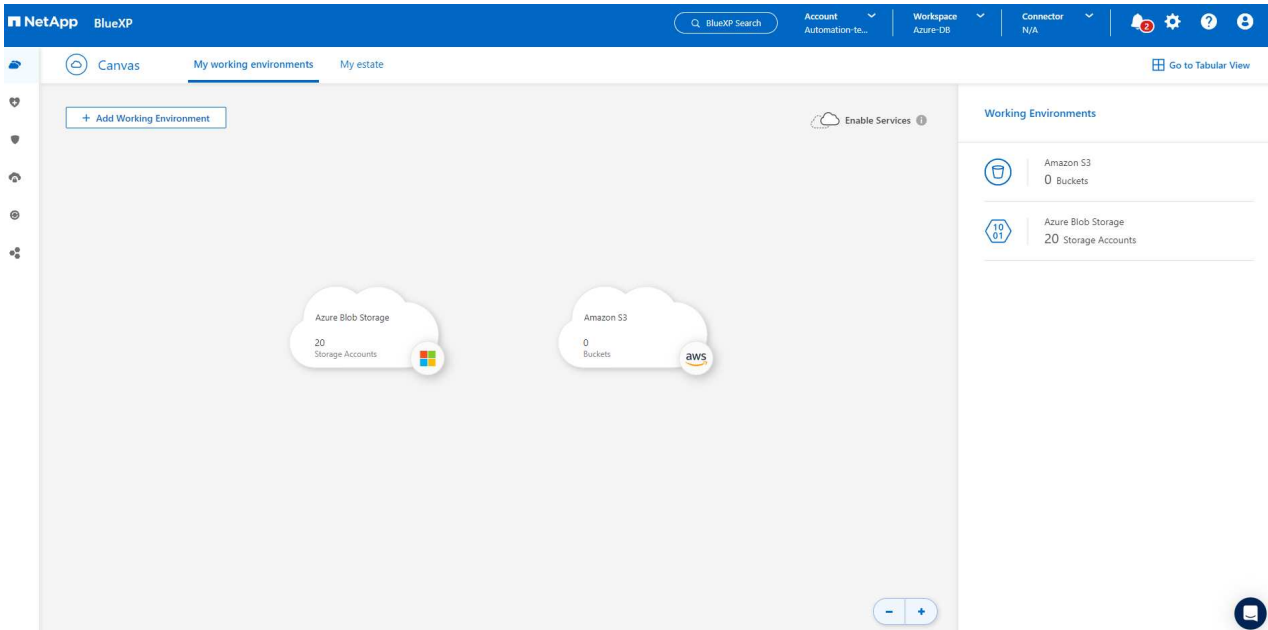
1. A primary Oracle database server on an Azure VM instance with an Oracle database fully deployed and running.
2. An Azure NetApp Files storage service capacity pool deployed in Azure that has capacity to meet the database storage needs listed in hardware component section.
3. A secondary database server on an Azure VM instance that can be used for testing the cloning of an Oracle database to an alternate host for the purpose of supporting a dev/test workload or any use cases that requires a full data set of production Oracle database.
4. For additional information for Oracle database deployment on Azure NetApp Files and Azure compute instance, see [Oracle Database Deployment and Protection on Azure NetApp Files](#).

Onboarding to BlueXP preparation

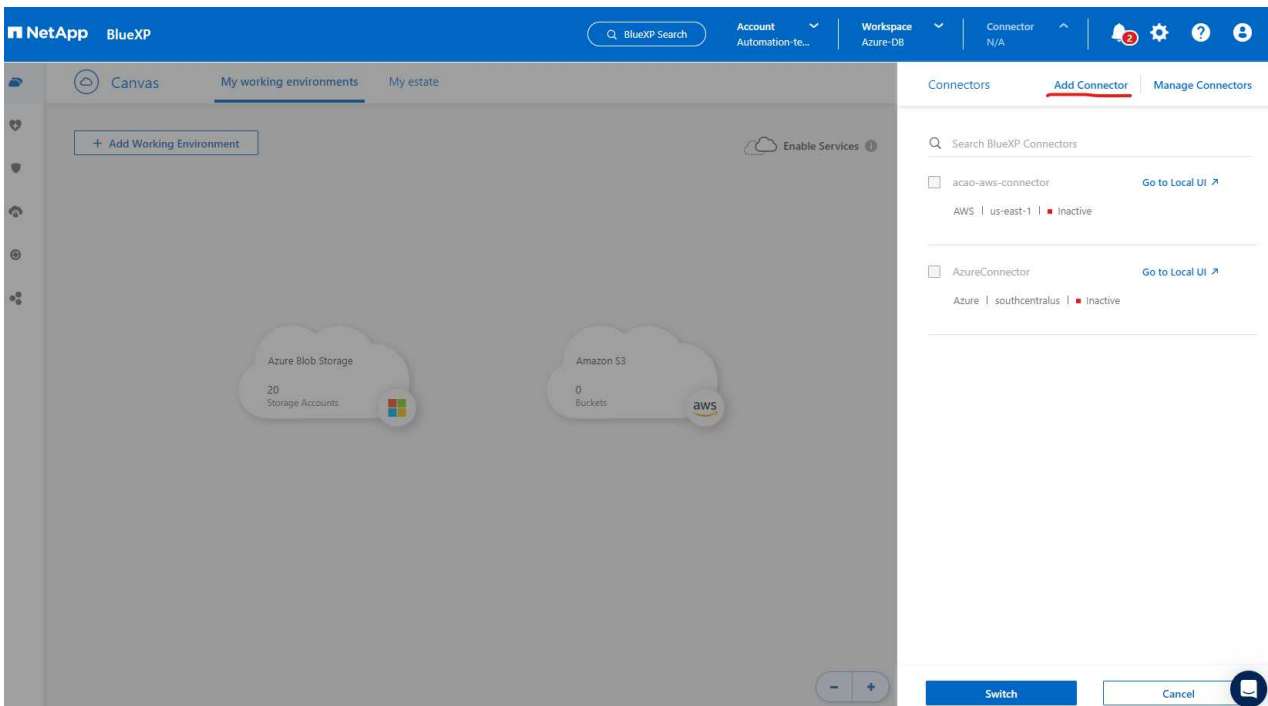
1. Use the link [NetApp BlueXP](#) to sign up for BlueXP console access.
2. Create an Azure user account or an Active Directory service principle and grant permissions with role in Azure portal for Azure connector deployment.
3. To set up BlueXP to manage Azure resources, add a BlueXP credential with details of an Active Directory service principal that BlueXP can use to authenticate with Azure Active Directory (App client ID), a client secret for the service principal application (Client Secret), and the Active Directory ID for your organization (Tenant ID).
4. You also need the Azure virtual network, resources group, security group, an SSH key for VM access, etc. ready for connector provisioning and database plugin installation.

Deploy a connector for SnapCenter services

1. Login to the BlueXP console.



2. Click on **Connector** drop down arrow and **Add Connector** to launch the connector provisioning workflow.



3. Choose your cloud provider (in this case, **Microsoft Azure**).

Provider

Choose the cloud provider where you want to run the BlueXP Connector:



[Deploy the Connector on your premises](#)

Continue

4. Skip the **Permission**, **Authentication**, and **Networking** steps if you already have them set up in your Azure account. If not, you must configure these before proceeding. From here, you could also retrieve the permissions for the Azure policy that is referenced in the previous section "[Onboarding to BlueXP preparation](#)."

Deploying a BlueXP Connector

The BlueXP Connector is a crucial component for the day-to-day use of BlueXP.

It's used to connect BlueXP's services to your hybrid-cloud environments.

The BlueXP Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for BlueXP Connector installation.

Permissions

Ensure that the Azure user or service principal you've provided has sufficient permissions

Authentication

Choose between two methods: an

[Azure user account](#) or an

[Active Directory service principal](#)

Networking

Ensure that you have details on the VNet and subnet in which the BlueXP Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



- Click on **Skip to Deployment** to configure your connector **Virtual Machine Authentication**. Add the SSH key pair you have created in Azure resource group during onboarding to BlueXP preparation for connector OS authentication.

1

VM Authentication

2

Details

3

Network

4

Security Group

5

Review

Virtual Machine Authentication

You are logged in with Azure user: [acao@netapp.com](#)

Tenant: Hybrid Cloud TME

Subscription

Hybrid Cloud TME Onprem

Location

South Central US

Resource Group

☐ Create New ☒ Use Existing

Resource Group

ANFAVSRG

Authentication Method

☐ Password ☒ Public Key

User Name

azureuser

Enter SSH Public Key

-----BEGIN RSA PRIVATE KEY----- MIIGSAIBAAKCA...

[Previous](#)[Next](#)

6. Provide a name for the connector instance, select **Create** and accept default **Role Name** under **Details**, and choose the subscription for the Azure account.

Add BlueXP Connector - Azure
More Information

VM Authentication
2 Details
3 Network
4 Security Group
5 Review

Details

Connector Instance Name
AzureConnector

Connector Role

Create
Attach existing
Manual

Role Name
BlueXP Operator-5519248

Subscriptions to apply with the role
Hybrid Cloud TME Onprem

Add Tags to Connector Instance

Previous
Next

- Configure networking with the proper **VNet**, **Subnet**, and disable **Public IP** but ensure that the connector has the internet access in your Azure environment.

Add BlueXP Connector - Azure
More Information

VM Authentication
Details
3 Network
4 Security Group
5 Review

Network

Connectivity

VNet
ANFAVSVal

Subnet
VM_Sub

Public IP
Disable

Proxy Configuration (Optional)

HTTP Proxy
Example: http://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with Azure services.

Previous
Next

8. Configure the **Security Group** for the connector that allows HTTP, HTTPS, and SSH access.

Add BlueXP Connector - Azure More Information ×

✓ VM Authentication ✓ Details ✓ Network **4** Security Group 5 Review

Security Group

The security group must allow inbound HTTP, HTTPS and SSH access.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type <input type="text" value="Anywhere"/>	Source Type <input type="text" value="Anywhere"/>	Source Type <input type="text" value="Anywhere"/>
Source (CIDR) <input type="text" value="0.0.0.0/0"/>	Source (CIDR) <input type="text" value="0.0.0.0/0"/>	Source (CIDR) <input type="text" value="0.0.0.0/0"/>

Previous Next 📄

9. Review the summary page and click **Add** to start connector creation. It generally takes about 10 mins to complete deployment. Once completed, the connector instance VM appears in the Azure portal.

Add BlueXP Connector - Azure

More Information

VM Authentication

Details

Network

Security Group

5 Review

Review

Code for Terraform Automation

BlueXP Connector Name	AzureConnector
Subscription	Hybrid Cloud TME Onprem
Location	South Central US
Resource Group	Existing - ANFAVSRG
Role	New - BlueXP Operator-5519248
Authentication Method	Password (user: azureuser)
VNet	ANFAVSVAl
Subnet	VM_Sub
Public IP	Enable
Proxy	None
Security Group	HTTP: 0.0.0.0/0, HTTPS: 0.0.0.0/0, SSH: 0.0.0.0/0

Previous

Add

10. After the connector is deployed, the newly created connector appears under **Connector** drop-down.

NetApp BlueXP

Q BlueXP Search

Account Automation-to...

Workspace Azure-DB

Connector AzureConnector

2

?

Canvas

My working environments

My estate

+ Add Working Environment

Enable Services

Azure Blob Storage
20 Storage Accounts

Amazon S3
0 Buckets

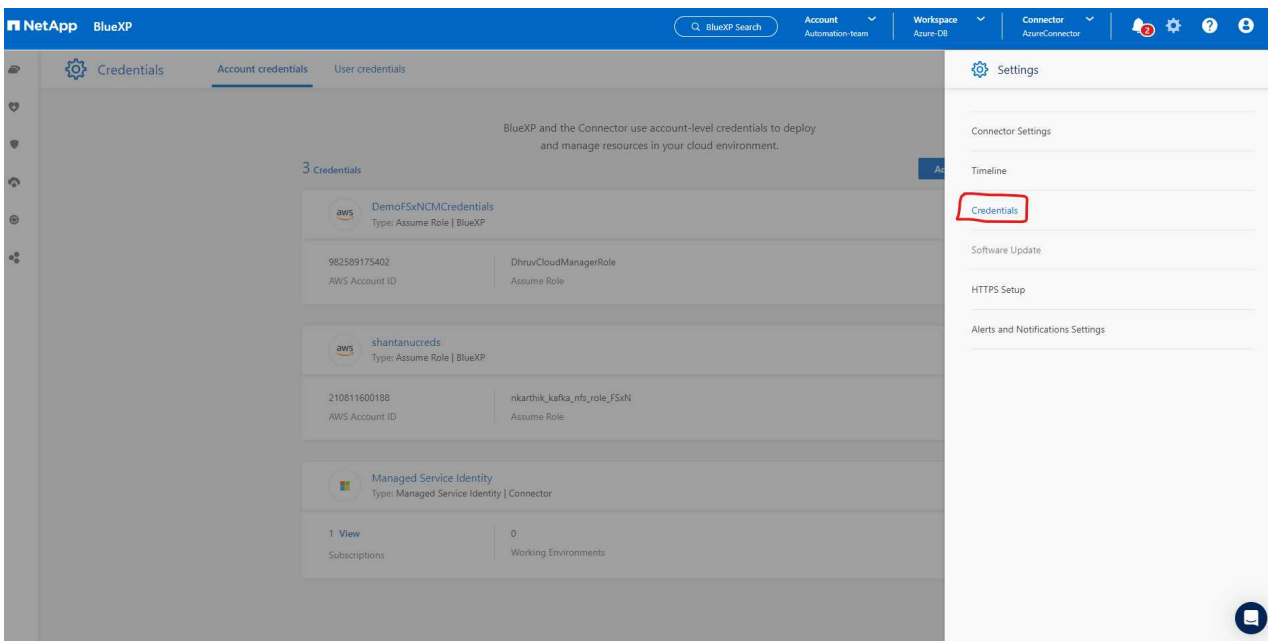
Working Environments

Amazon S3
0 Buckets

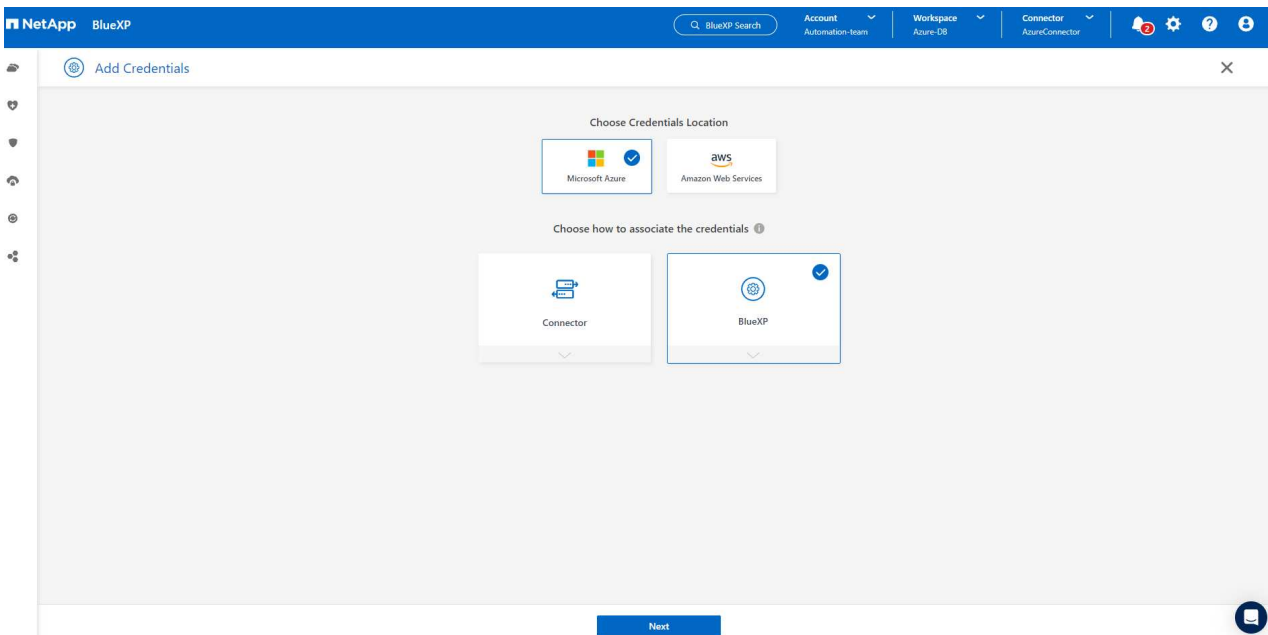
Azure Blob Storage
20 Storage Accounts

Define a credential in BlueXP for Azure resources access

1. Click on setting icon on top right corner of BlueXP console to open **Account credentials** page, click **Add credentials** to start credential configuration workflow.



2. Choose credential location as - **Microsoft Azure - BlueXP**.



3. Define Azure credentials with proper **Client Secret**, **Client ID**, and **Tenant ID**, which should have been gathered during previous BlueXP onboarding process.

NetApp BlueXP

Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

Add Credentials Credentials Type Define Credentials Marketplace Subscription Review

Define Microsoft Azure Credentials

Learn more about Azure application credentials

Credentials Name Client Secret

Azure_Hybrid_TME

Application (client) ID Directory (tenant) ID

2fbc9be5-a259-4539-bb57-036b176f5cc7 9bb0aab6-5c98-419b-9cfd-7a38bd496...

☒ I have verified that the Azure role assigned to the Active Directory service principal matches BlueXP policy requirements.

Previous Next

4. Review and Add.

NetApp BlueXP

Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

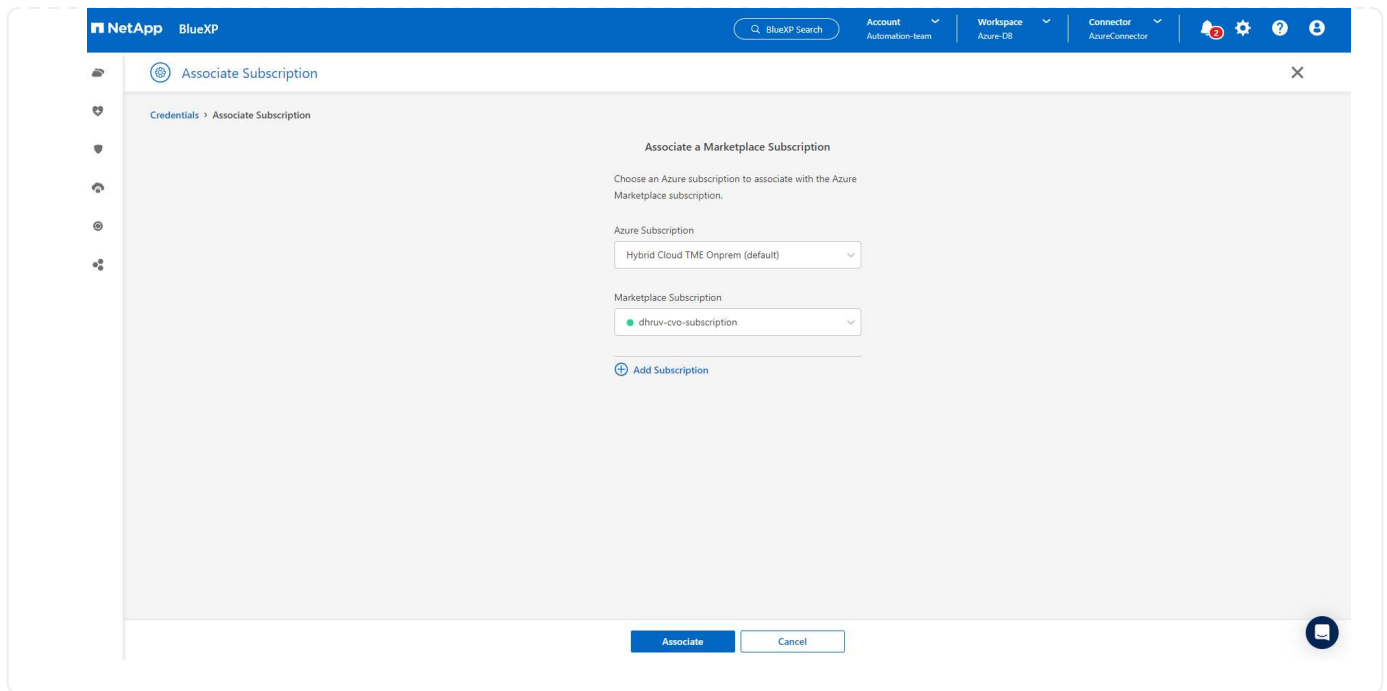
Add Credentials Credentials Type Define Credentials Review

Review

Credentials Type	Azure
Credentials Name	Azure_Hybrid_TME
Credential Storage	Cloud Manager
Application (client) ID	2fbc9be5-a259-4539-bb57-036b176f5cc7
Directory (tenant) ID	9bb0aab6-5c98-419b-9cfd-7a38bd496e1f

Previous Add

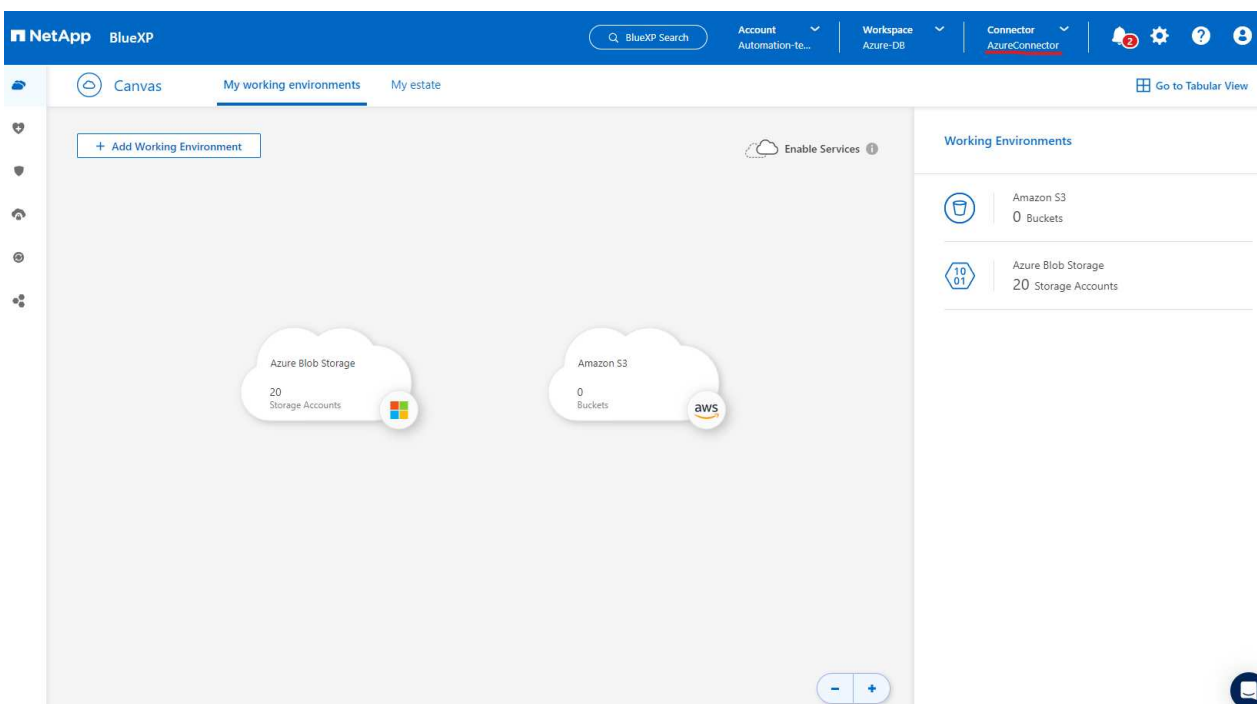
5. You may also need to associate a **Marketplace Subscription** with the credential.



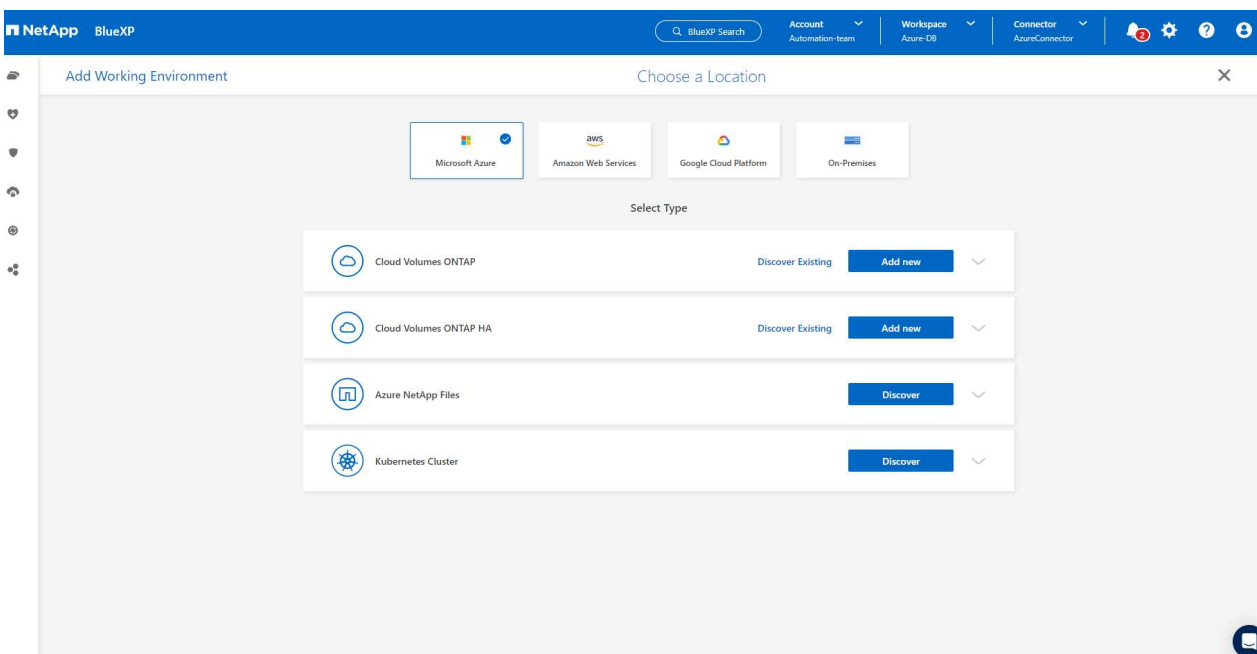
SnapCenter services setup

With the Azure credential configured, SnapCenter services can now be set up with the following procedures:

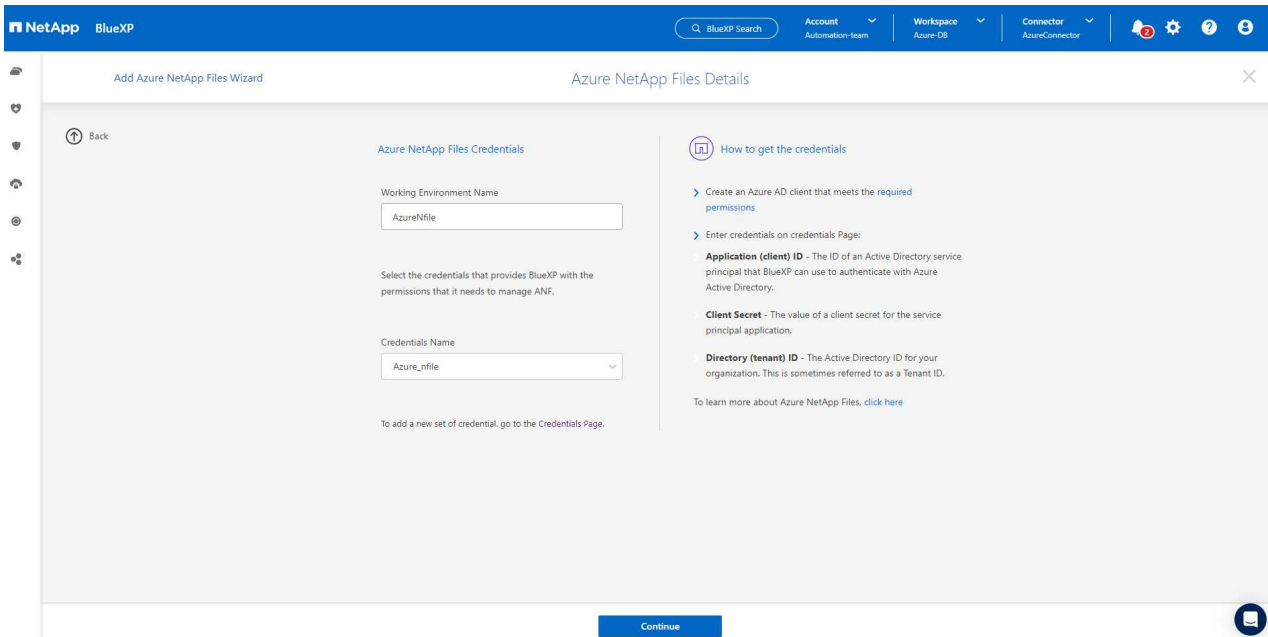
1. Back to Canvas page, from **My Working Environment** click **Add working Environment** to discover Azure NetApp Files deployed in Azure.



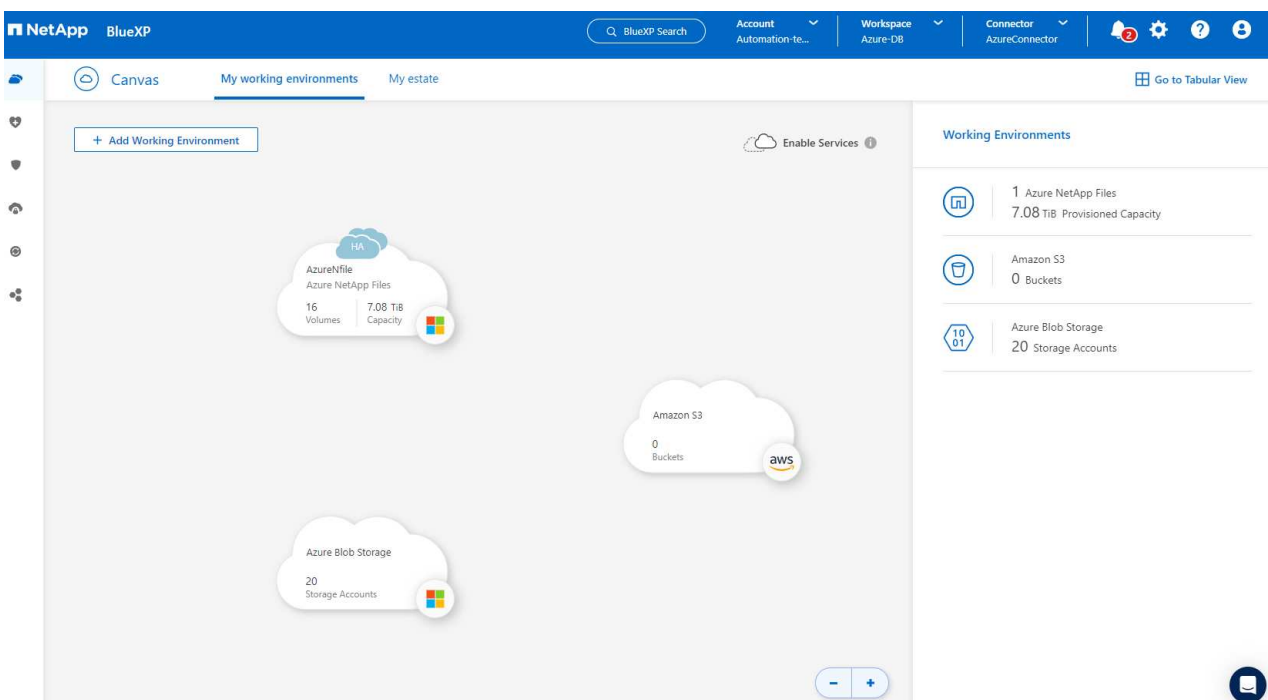
2. Choose **Microsoft Azure** as the location and click on **Discover**.



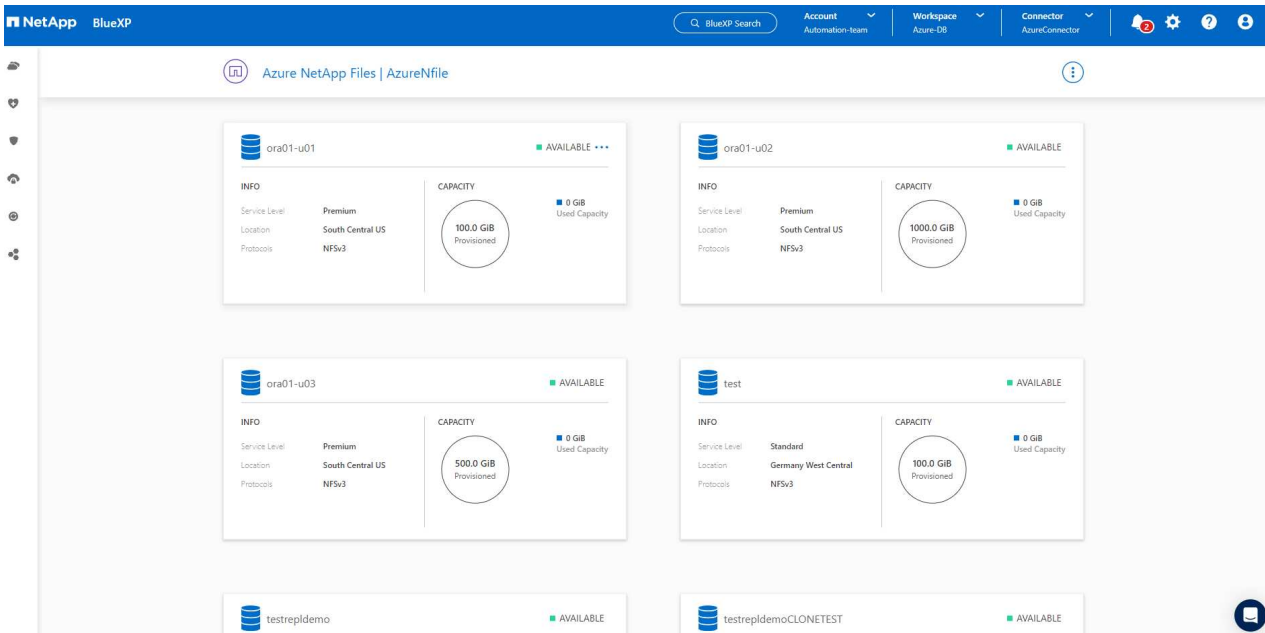
3. Name **Working Environment** and choose **Credential Name** created in previous section, and click **Continue**.



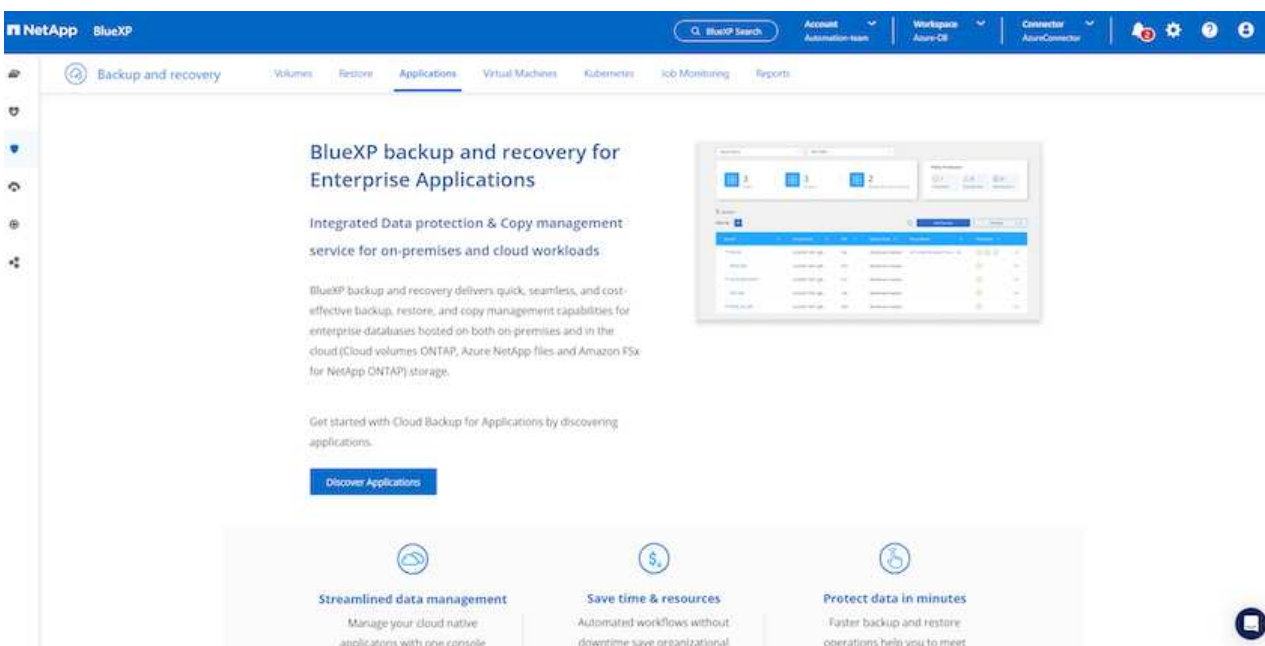
- BlueXP console returns to **My working environments** and discovered Azure NetApp Files from Azure now appears on **Canvas**.



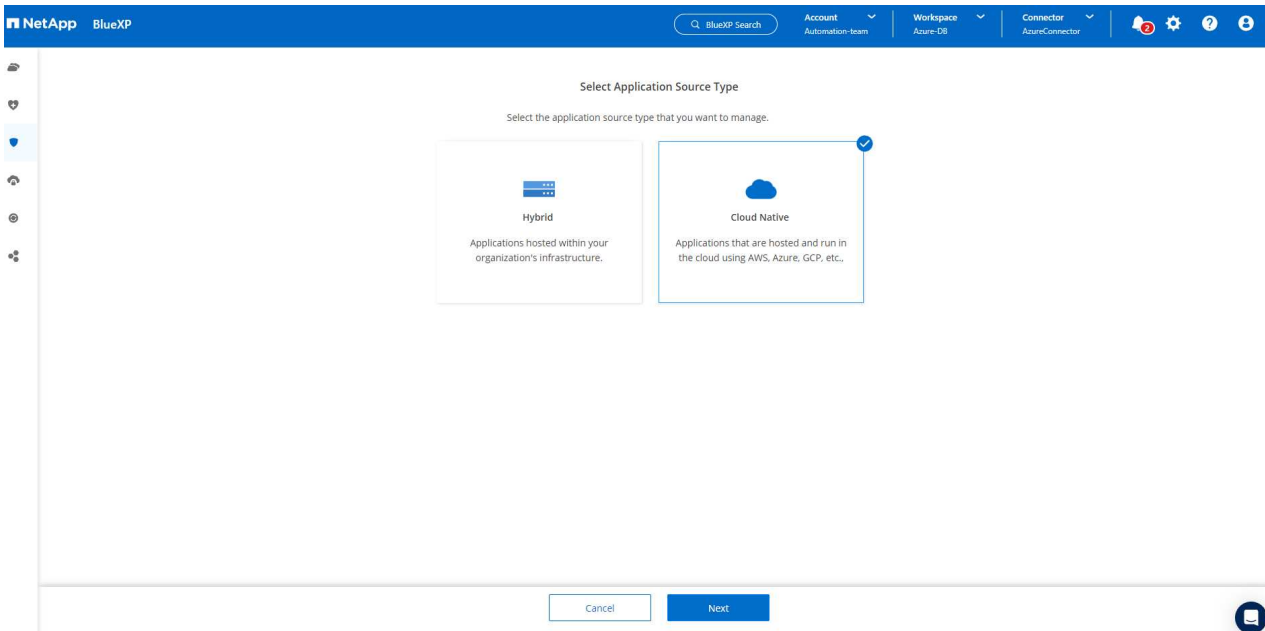
- Click on **Azure NetApp Files** icon, then **Enter Working Environment** to view Oracle database volumes deployed in Azure NetApp Files storage.



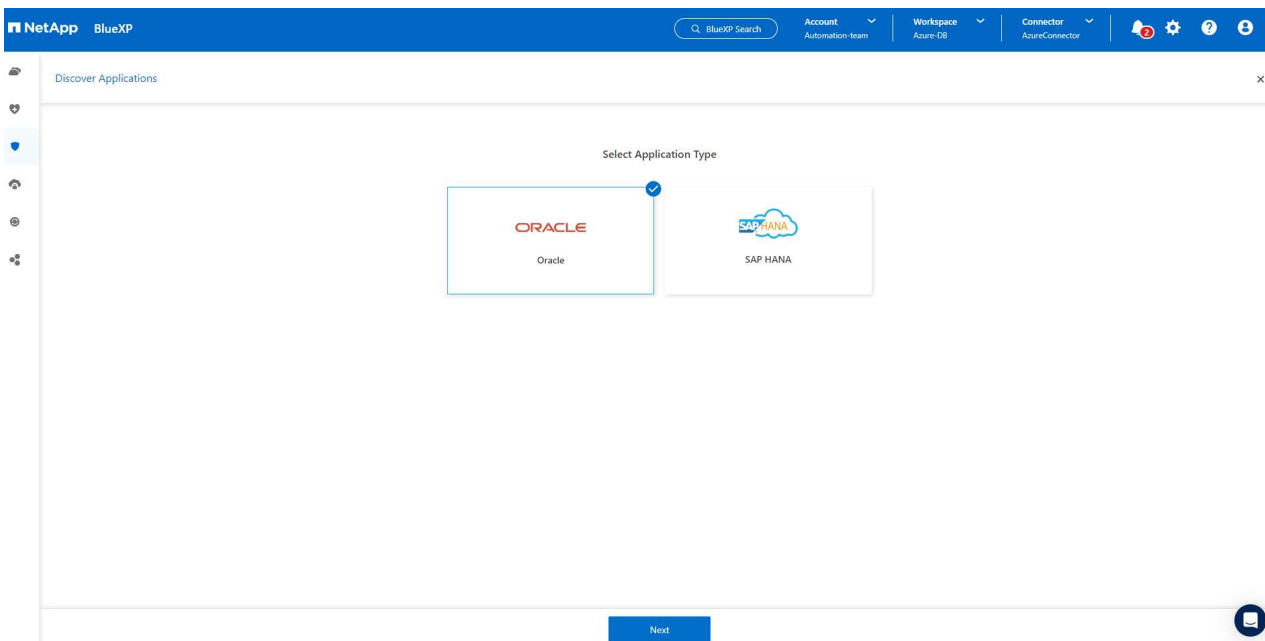
- From the left-hand sidebar of the console, hover your mouse over the protection icon, and then click **Protection > Applications** to open the Applications launch page. Click **Discover Applications**.



- Select **Cloud Native** as the application source type.



8. Choose **Oracle** for the application type, click on **Next** to open host details page.



9. Select **Using SSH** and provide the Oracle Azure VM details such as **IP address**, **Connector**, Azure VM management **Username** such as azureuser. Click on **Add SSH Private Key** to paste in the SSH key pair that you used to deploy the Oracle Azure VM. You will also be prompted to confirm the fingerprint.

NetApp BlueXP

Discover Applications

1 Host Details 2 Configuration 3 Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type ☐ Manual ☒ Using SSH

Host FQDN or IP 172.30.137.142 Connector AzureConnector

Username azureuser Add SSH Private Key Optional

SSH Port 22 Plug-in Port 8145

Previous Next

Discover Applications

1 Host Details 2 Configuration 3 Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type ☐ Manual ☒ Using SSH

Validate fingerprint

Algorithm ssh-rsa

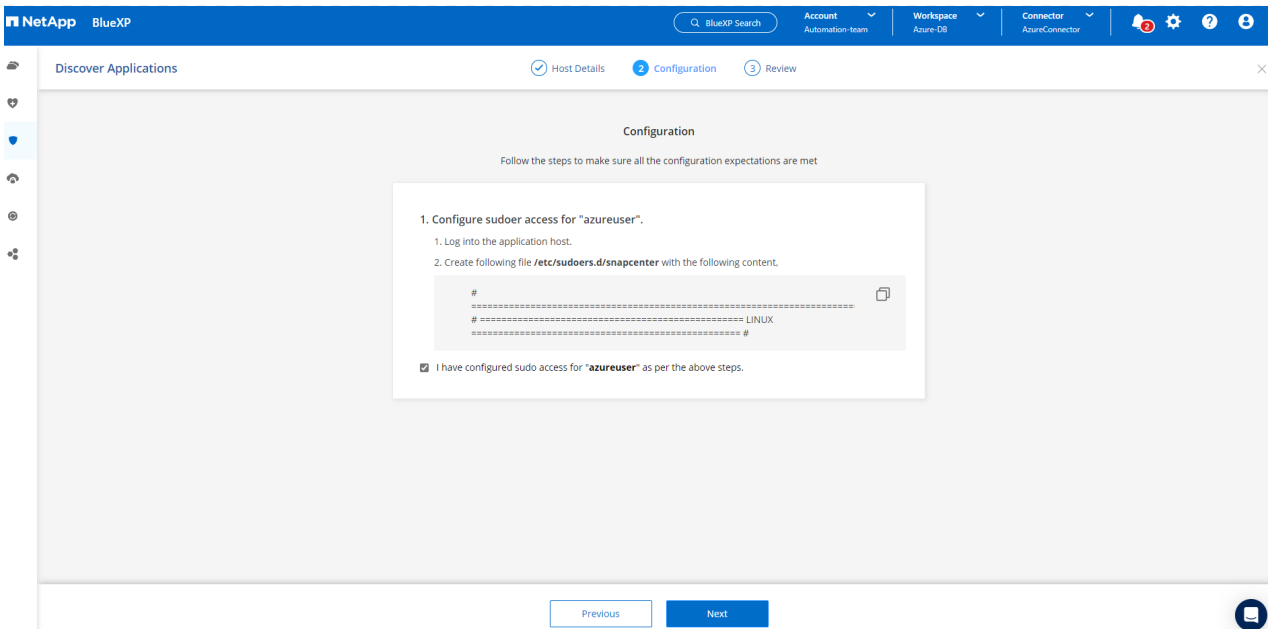
Fingerprint AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAAB... [Copy]

☒ By proceeding further, I confirm that the above fingerprint for host is valid.

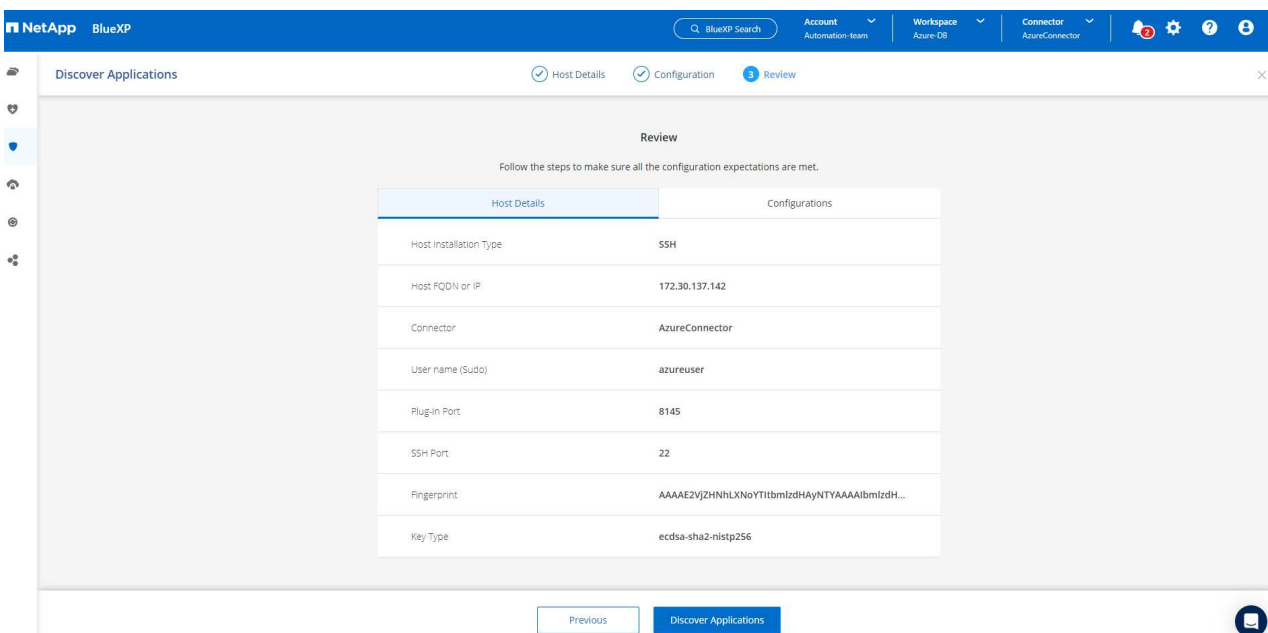
Proceed Cancel

Previous Next

10. Move on to next **Configuration** page to setup sudoer access on Oracle Azure VM.



11. Review and click on **Discover Applications** to install a plugin on the Oracle Azure VM and discover Oracle database on the VM in one step.



12. Discovered Oracle databases on Azure VM are added to **Applications**, and the **Applications** page lists the number of hosts and Oracle databases within the environment. The database **Protection Status** initially shows as **Unprotected**.

NetApp BlueXP
BlueXP Search
Account Automation-te...
Workspace Azure-DB
Connector AzureConnector
2
?

Backup and recovery
Volumes
Restore
Applications
Virtual Machines
Kubernetes
Job Monitoring
Reports

Cloud Native
Oracle

3 Hosts

3 ORACLE

0 Clone

Application Protection

0 Protected

3 Unprotected

3 Databases

Filter By
Manage Databases
Settings

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1st	172.30.15.124		Unprotected

1 - 3 of 3
1

This completes the initial setup of SnapCenter services for Oracle. The next three sections of this document describe Oracle database backup, restore, and clone operations.

Oracle database backup

1. Our test Oracle database in Azure VM is configured with three volumes with an aggregate total storage about 1.6 TiB. This gives context about the timing for the snapshot backup, restore, and clone of a database of this size.

```
[oracle@acao-ora01 ~]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.9G         0  7.9G   0% /dev
tmpfs                     7.9G         0  7.9G   0% /dev/shm
tmpfs                     7.9G      17M  7.9G   1% /run
tmpfs                     7.9G         0  7.9G   0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv 40G       23G    15G  62% /
/dev/mapper/rootvg-usrlv  9.8G      1.6G    7.7G  18% /usr
/dev/sda2                 496M     115M   381M  24% /boot
/dev/mapper/rootvg-varlv  7.9G     787M    6.7G  11% /var
/dev/mapper/rootvg-homelv 976M     323M    586M  36% /home
/dev/mapper/rootvg-optlv  2.0G      9.6M    1.8G   1% /opt
/dev/mapper/rootvg-tmplv  2.0G      22M    1.8G   2% /tmp
/dev/sda1                 500M      6.8M   493M   2% /boot/efi
172.30.136.68:/ora01-u01 100G       23G     78G  23% /u01
172.30.136.68:/ora01-u03 500G     117G    384G  24% /u03
172.30.136.68:/ora01-u02 1000G     804G    197G  81% /u02
tmpfs                     1.6G         0  1.6G   0% /run/user/1000
[oracle@acao-ora01 ~]$
```

1. To protect database, click the three dots next to the database **Protection Status**, and then click **Assign Policy** to view the default preloaded or user defined database protection policies that can be applied to your Oracle databases. Under **Settings - Policies**, you have option to create your own policy with a customized backup frequency and backup data-retention window.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. Below the navigation bar, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '4 Hosts', '3 ORACLE', and '0 Clone'. An 'Application Protection' summary shows '0 Protected' and '3 Unprotected'. A table lists databases with their protection status:

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

A dropdown menu for the 'db1' row shows options: 'View Details' and 'Assign Policy' (highlighted with a red box).

- When you are happy with the policy configuration, you can then **Assign** your policy of choice to protect the database.

The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. The title is 'Assign Policy' with a subtitle 'Assign a policy to start taking backups of the database "NTAP"'. It lists 4 policies:

Policy Name	Backup Type	Schedules
<input type="radio"/> Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input type="radio"/> Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input type="radio"/> Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input checked="" type="radio"/> my_full_bkup	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 3 Days

At the bottom, there are 'Cancel' and 'Assign' buttons.

- After the policy is applied, the database protection status changed to **Protected** with a green check mark. BlueXP executes the snapshot backup according to the schedule defined. In addition, **ON-Demand Backup** is available from the three-dot drop down menu as shown below.

The screenshot shows the NetApp BlueXP interface with the 'Applications' tab selected. At the top, there are filters for 'Cloud Native' and 'Oracle'. Below these, there are three summary cards: '3 Hosts', '3 ORACLE', and '0 Clone'. To the right, an 'Application Protection' summary shows '1 Protected' and '2 Unprotected' databases. The main section is titled '3 Databases' and includes a 'Filter By' button and a search bar. A table lists the databases:

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

A three-dot menu is open for the 'NTAP' database, showing options: 'View Details', 'On-Demand Backup' (highlighted with a red underline), 'Assign Policy', 'Un-assign Policy', and 'Restore'.

4. From **Job Monitoring** tab, backup job details can be viewed. Our test results showed that it took about 4 minutes to backup an Oracle database about 1.6 TiB.

The screenshot shows the NetApp BlueXP interface with the 'Job Monitoring' tab selected. The breadcrumb trail is 'Job Monitoring > Job Name: Backup of NTAP oracle database on host 172.30.137.142 with policy my_full_bkup and schedule Hourly'. The job name is displayed as 'Job Name: Backup of NTAP oracle database on host 172.30.137.142 with policy my_full_bkup and schedule H...' with a job ID '61a12139-330e-4390-bca8-e7d15680869c'. Below this, a summary bar shows: 'Other Job Type', 'Jul 11 2023, 2:17:53 pm Start Time', 'Jul 11 2023, 2:21:38 pm End Time', and 'Success Job Status'. The 'Sub-Jobs(17)' section is expanded, showing a table of sub-jobs:

Job Name	Job ID	Start Time	End Time	Duration
Backup of NTAP oracle database on host 172.30...	61a12139-330e-4390-bc...	Jul 11 2023, 2:17:53 pm	Jul 11 2023, 2:21:38 pm	4 Minutes
Applying Retention	27ff9d5f-68f0-4880-a48...	Jul 11 2023, 2:21:38 pm	Jul 11 2023, 2:21:38 pm	0 Second
Performing cleanup after backup	074c0689-097e-41aa-ac...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:38 pm	2 Seconds
Finalizing Oracle database log backup	348189d3-90b5-4cce-97...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:36 pm	0 Second

5. From three-dot drop down menu **View Details**, you can view the backup sets created from snapshot backup.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. The 'Applications' section is active, showing filters for 'Cloud Native' and 'Oracle'. Summary cards indicate 4 Hosts, 3 ORACLE, and 0 Clones. An 'Application Protection' card shows 2 Protected and 1 Unprotected databases. Below, a table lists databases with their protection status. A context menu is open for the 'db1tst' database, showing options like 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore'.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

- Database backup details include the **Backup Name**, **Backup Type**, **SCN**, **RMAN Catalog**, and **Backup Time**. A backup set contains application-consistent snapshots for data volume and log volume respectively. A log volume snapshot takes place right after a database data volume snapshot. You could apply a filter if you are looking for a particular backup in the backup list.

The screenshot shows the 'Database Details' page for the 'NTAP' database. It displays various attributes in a grid: Database Name (NTAP), Protection (Protected), Policy Names (my_full_bkup), Database Type (zEHlu7vkdyabnucxllbkKELkVXTyNcllients), Host Name (172.30.137.142), Host Storage (ANF), Database Version (Unreachable), Connector Id, Clones (-), Parent Database, RMAN Catalog (Disabled), and RMAN catalog repository. Below this, a 'Backups' section shows a list of 14 backups. A table displays the first four backups with columns for Backup Name, Backup Type, SCN, RMAN Catalog, Backup Time, and a Delete link.

Backup Name	Backup Type	SCN	RMAN Catalog	Backup Time	
my_full_bkup_Hourly_NTAP_2023_07_13_12_04_28_8376...	Log	29192187	Not Cataloged	Jul 13, 2023, 8:06:22 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_4363...	Data	29192136	Not Cataloged	Jul 13, 2023, 8:03:40 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_04_28_5618...	Log	29178022	Not Cataloged	Jul 13, 2023, 2:05:50 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_03_03_6371...	Data	29177972	Not Cataloged	Jul 13, 2023, 2:03:43 am	Delete

Oracle database restore and recovery

1. For a database restore, click the three-dot drop down menu for the particular database to be restored in **Applications**, then click **Restore** to initiate database restore and recovery workflow.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and links for 'Account Automation-te...', 'Workspace Azure-DB', and 'Connector AzureConnector'. The left sidebar lists various categories: Storage, Health, Protection, Backup and recovery, Governance, Mobility, and Extensions. The main content area is titled 'Backup and recovery' and includes tabs for 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. Below the tabs, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '4 Hosts', '3 ORACLE', and '0 Clone'. An 'Application Protection' section indicates '2 Protected' and '1 Unprotected' databases. A table lists 3 databases:

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

A context menu is open for the 'db1tst' database, showing options: 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore' (highlighted).

2. Choose your **Restore Point** by time stamp. Each time stamp in the list represents an available database backup set.

The screenshot shows the 'Restore "NTAP"' dialog box in the NetApp BlueXP interface. The dialog has three steps: '1 Restore Point and Location', '2 Configuration', and '3 Review'. The 'Restore Point and Location' step is active, showing a list of restore points to choose from:

- Jul 13, 2023, 8:03:40 am
- Jul 13, 2023, 2:03:43 am
- Jul 12, 2023, 8:03:41 pm
- Jul 12, 2023, 2:03:32 pm
- Jul 12, 2023, 2:03:31 am

Below the list, there are two 'location' fields. At the bottom of the dialog, there are 'Previous' and 'Next' buttons.

3. Choose your **Restore Location** to **original location** for an Oracle database in place restore and recovery.

NetApp BlueXP

Restore "NTAP"

1 Restore Point and Location 2 Configuration 3 Review

Restore Point and Location

Specify the restore point to which the database should be restored.

Restore Point
Jul 13, 2023, 8:03:40 am

Restore to original location

Restore to alternate location

Previous Next

4. Define your **Restore Scope**, and **Recovery Scope**. All Logs mean a full recovery up to date including current logs.

NetApp BlueXP

Restore "NTAP"

Restore Point and Location 2 Configuration 3 Review

Restore Scope

☒ All Data Files
Data Files Restore

☒ Control Files
Control Files Restore

Database state will be changed if needed for restore and recovery.

Recovery Scope

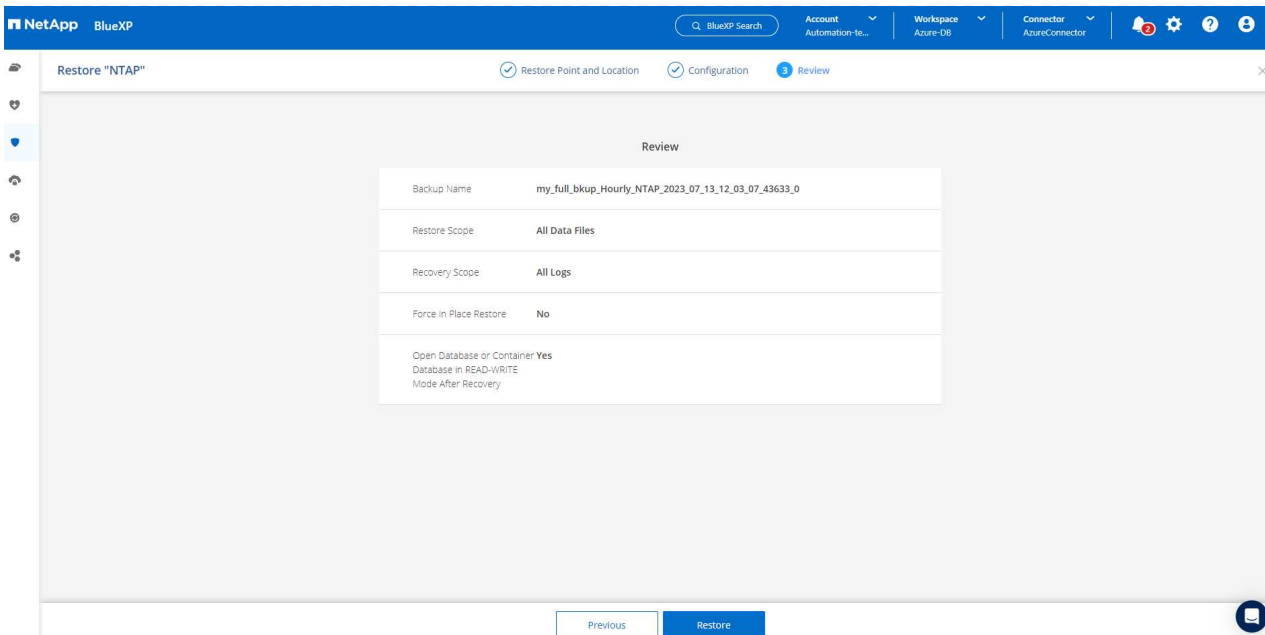
☒ All Logs ☐ Until System Change Number ☐ Date and Time ☐ No Recovery

External Archive log locations /mnt/log_location001

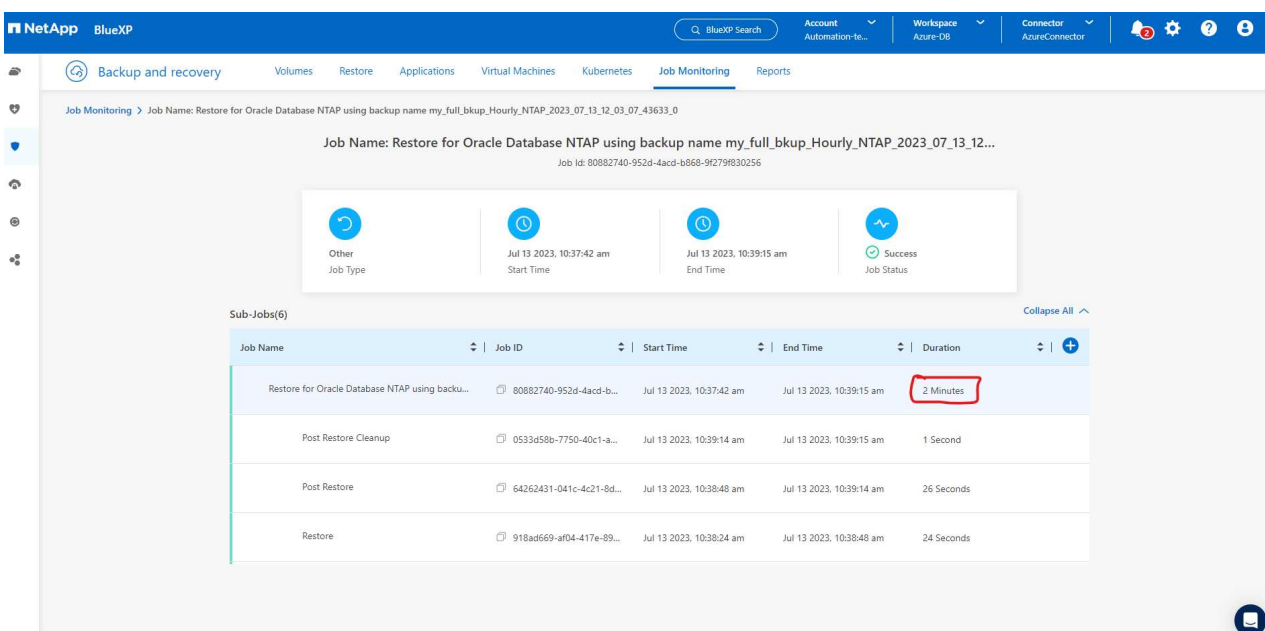
☒ Open the database or the container database in READ-WRITE mode after recovery.

Previous Next

5. Review and **Restore** to start database restore and recovery.



6. From the **Job Monitoring** tab, we observed that it took 2 minutes to run a full database restore and recovery up to date.



Oracle database clone

Database clone procedures are similar to restore but to an alternate Azure VM with identical Oracle software stack pre-installed and configured.



Ensure that your Azure NetApp File storage has sufficient capacity for a cloned database the same size as the primary database to be cloned. The alternate Azure VM has been added to **Applications**.

1. Click the three-dot drop down menu for the particular database to be cloned in **Applications**, then click **Restore** to initiate clone workflow.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and links for 'Account', 'Workspace', and 'Connector'. The left sidebar shows various categories like 'Storage', 'Health', 'Protection', 'Governance', 'Mobility', and 'Extensions'. The main content area is titled 'Applications' and shows a summary of resources: 4 Cloud Native Hosts, 3 ORACLE, and 0 Clones. Below this, there's a section for '3 Databases' with a table listing them. A context menu is open for the 'db1tst' database, showing options like 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore' (which is highlighted).

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

2. Select the **Restore Point** and check the **Restore to alternate location**.

The screenshot shows the 'Restore "NTAP"' configuration page in NetApp BlueXP. The page has three steps: '1 Restore Point and Location', '2 Configuration', and '3 Review'. The current step is 'Restore Point and Location', which prompts the user to 'Specify the restore point to which the database should be restored.' A dropdown menu for 'Restore Point' is set to 'Jul 13, 2023, 8:03:40 am'. Below this, there are two options: 'Restore to original location' (with a database icon) and 'Restore to alternate location' (with a database icon and a checkmark). At the bottom, there are 'Previous' and 'Next' buttons.

3. In the next **Configuration** page, set alternate **Host**, new database **SID**, and **Oracle Home** as configured at alternate Azure VM.

The screenshot shows the 'Configuration' step in the 'Restore "NTAP"' workflow. The page title is 'Configuration' with a subtitle 'Specify the alternate host details on which the database will be restored and throughput.' The form contains the following fields:

- Host:** A dropdown menu showing '172.30.137.147'.
- SID:** A text input field containing 'NTAP1'.
- Oracle Home:** A text input field containing '/u01/app/oracle/product/19.0.0/clone'.
- Database Credentials:** A section labeled 'Optional' with an 'Add Credential' button.
- Maximum storage throughput (MiB/s):** A section labeled 'Optional' with a text input field containing 'Enter throughput (1-4500)'.

At the bottom of the form are 'Previous' and 'Next' buttons.

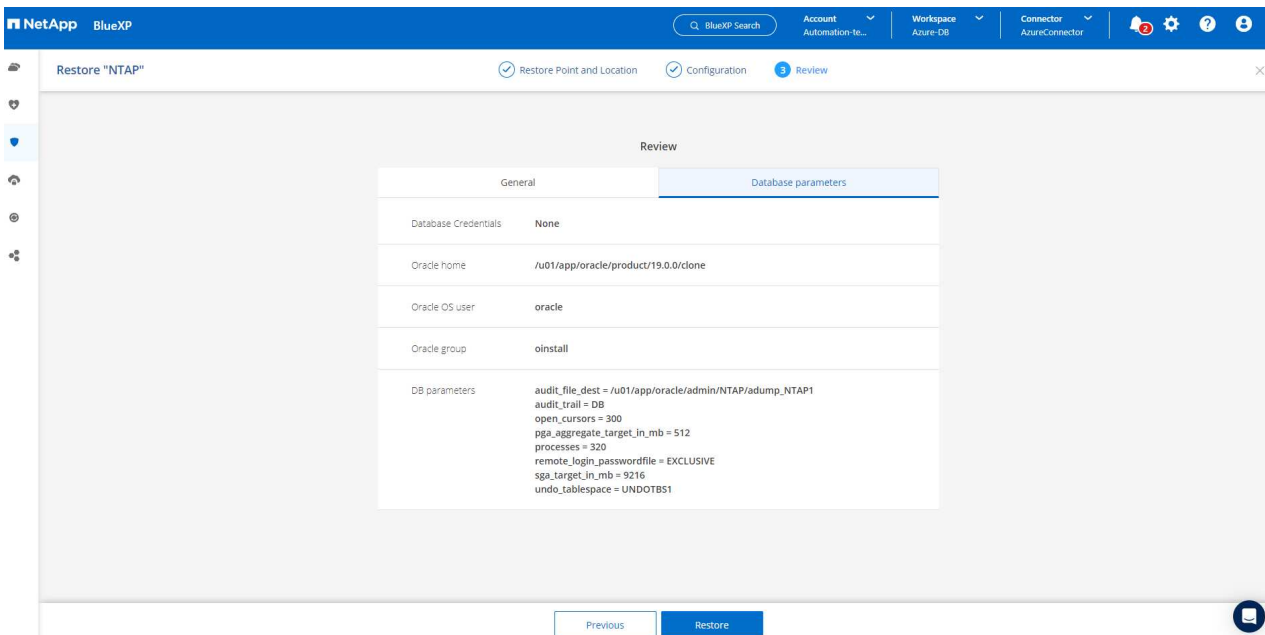
4. Review **General** page shows the details of cloned database such as SID, alternate host, data file locations, recovery scope etc.

The screenshot shows the 'Review' step in the 'Restore "NTAP"' workflow. The page title is 'Review' with a subtitle 'General'. The page is divided into two tabs: 'General' (selected) and 'Database parameters'. The 'General' tab displays the following details:

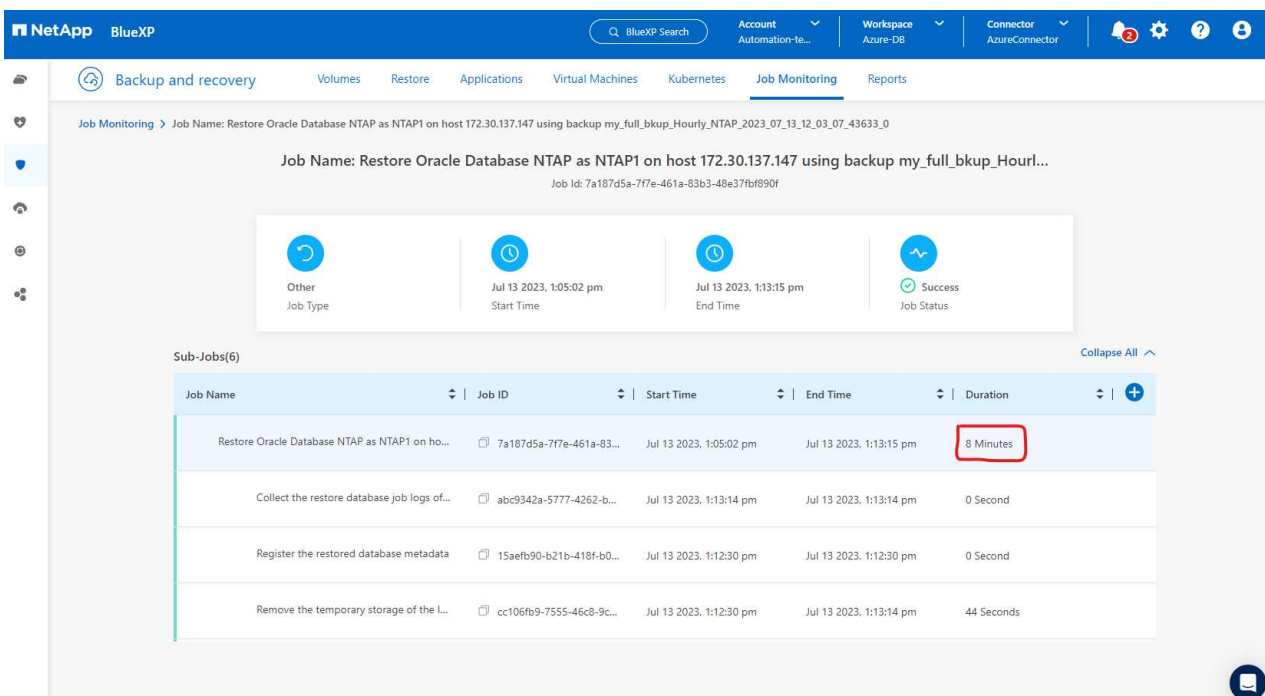
Field	Value
Backup Name	my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0
SID	NTAP1
Host	172.30.137.147
Datafile locations	/u02_NTAP1
Control files	/u02_NTAP1/NTAP1/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs
Recovery Point	Jul 13, 2023, 8:03:40 am
Location	Alternate Location

At the bottom of the page are 'Previous' and 'Restore' buttons.

5. Review **Database parameters** page shows the details of cloned database configuration as well as some database parameters setting.



6. Monitor the cloning job status from the **Job Monitoring** tab, we observed that it took 8 minutes to clone a 1.6 TiB Oracle database.



7. Validate the cloned database in BlueXP **Applications** page that showed the cloned database was immediately registered with BlueXP.

Account Automation-te...

Workspace Azure-DB

Connector AzureConnector

Backup and recovery
Volumes
Restore
Applications
Virtual Machines
Kubernetes
Job Monitoring
Reports

Cloud Native

Oracle

4 Hosts

4 ORACLE

0 Clone

Application Protection

2 Protected

2 Unprotected

4 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status	
NTAP	172.30.137.142	my_full_bkup	Protected	...
NTAP1	172.30.137.147		Unprotected	...
db1	172.30.15.99	my_full_bkup	Protected	...
db1tst	172.30.15.124		Unprotected	...

1 - 4 of 4
<<
<
1
>
>>

8. Validate the cloned database on the Oracle Azure VM that showed the cloned database was running as expected.

```

[oracle@acao-ora02 admin]$ cat /etc/oratab
#

# This file is used by ORACLE utilities.  It is created by root.sh
# and updated by either Database Configuration Assistant while creating
# a database or ASM Configuration Assistant while creating ASM instance.

# A colon, ':', is used as the field terminator.  A new line terminates
# the entry.  Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively.  The third field indicates
# to the dbstart utility that the database should , "Y", or should not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAP1:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAP1
[oracle@acao-ora02 admin]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/clone
[oracle@acao-ora02 admin]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@acao-ora02 admin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Jul 13 17:16:31 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.18.0.0.0

SQL> select name, open_mode, log_mode from v$database;

NAME          OPEN_MODE          LOG_MODE
-----
NTAP1         READ WRITE         NOARCHIVELOG

```

This completes the demonstration of an Oracle database backup, restore, and clone in Azure with NetApp BlueXP console using SnapCenter Service.

Additional information

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

- Set up and administer BlueXP

<https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html>

- BlueXP backup and recovery documentation

<https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html>

- Azure NetApp Files

<https://azure.microsoft.com/en-us/products/netapp>

- Get started with Azure

<https://azure.microsoft.com/en-us/get-started/>

Copyright information

Copyright © 2023 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.