



BlueXP SaaS for Oracle - AWS

NetApp Solutions

NetApp
October 20, 2023

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

Table of Contents

- TR-4964: Oracle Database backup, restore and clone with SnapCenter Services - AWS 1
 - Purpose 1
 - Audience 1
 - Solution test and validation environment 1
 - Solution deployment..... 3
 - Additional information..... 35

TR-4964: Oracle Database backup, restore and clone with SnapCenter Services - AWS

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 NetApp cloud storage. 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 to Amazon FSx for ONTAP storage and EC2 compute instances. Although it is much easier to set up and use, SnapCenter Services deliver key functionalities that are available in the legacy SnapCenter UI tool.

This solution addresses the following use cases:

- Database backup with snapshots for Oracle databases hosted in Amazon FSx for ONTAP
- Oracle database recovery in the case of a failure
- Fast and storage-efficient cloning of primary databases for a dev/test environment or other use cases

Audience

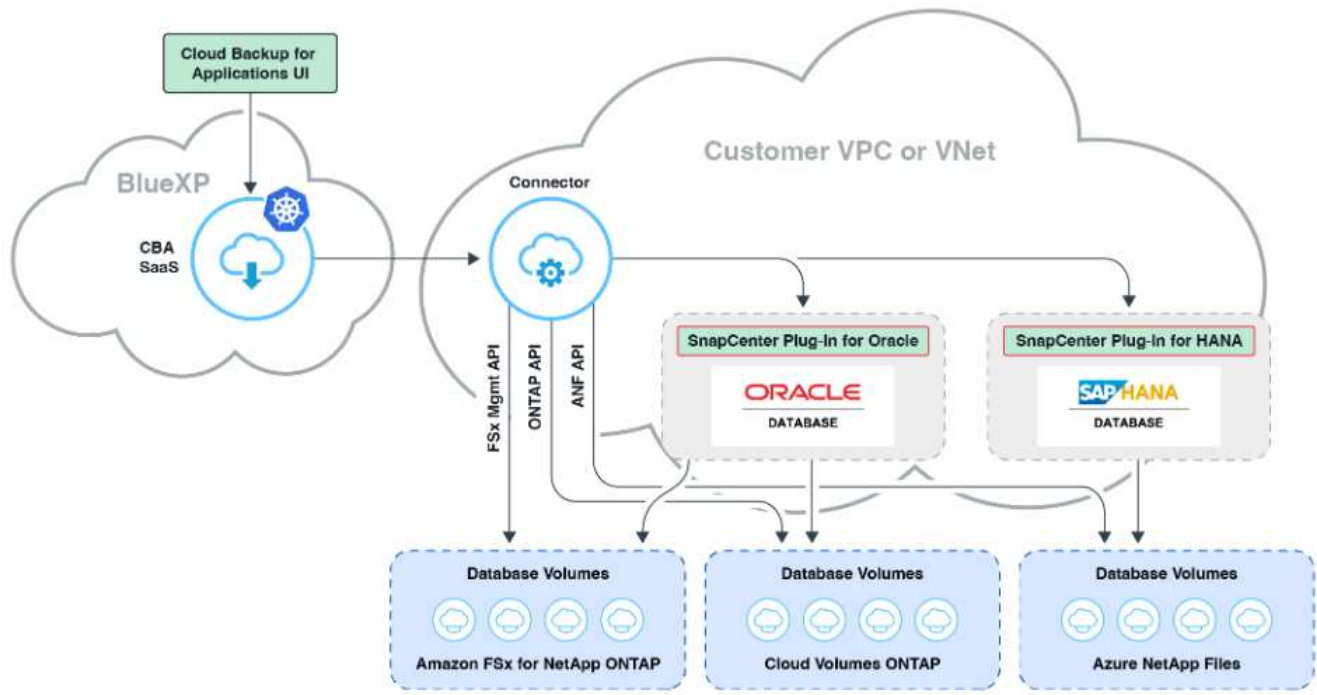
This solution is intended for the following audiences:

- The DBA who manages Oracle databases running on Amazon FSx for ONTAP storage
- The solution architect who is interested in testing Oracle database backup, restore, and clone in the public AWS cloud
- The storage administrator who supports and manages the Amazon FSx for ONTAP storage
- The application owner who owns applications that are deployed to Amazon FSx for ONTAP storage

Solution test and validation environment

The testing and validation of this solution was performed in an AWS FSx and EC2 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

FSx ONTAP storage	Current version offered by AWS	One FSx HA cluster in the same VPC and availability zone
EC2 instance for compute	t2.xlarge/4vCPU/16G	Two EC2 T2 xlarge EC2 instances, one as primary DB server and the other as clone DB server

Software

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Deployed RedHat subscription for testing
Oracle Grid Infrastructure	Version 19.18	Applied RU patch p34762026_190000_Linux-x86-64.zip
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	v2.3.1.2324

Key factors for deployment consideration

- **Connector to be deployed in the same VPC as database and FSx.** When possible, the connector should be deployed in the same AWS VPC, which enables connectivity to the FSx storage and the EC2 compute instance.
- **An AWS IAM policy created for SnapCenter connector.** The policy in JSON format is available in the detailed SnapCenter service documentation. When you launch connector deployment with the BlueXP console, you are also prompted to set up the prerequisites with details of required permission in JSON format. The policy should be assigned to the AWS user account that owns the connector.
- **The AWS account access key and the SSH key pair created in the AWS account.** The SSH key pair is assigned to the ec2-user for logging into the connector host and then deploying a database plug-in to the EC2 DB server host. The access key grants permission for provisioning the required connector with IAM policy above.
- **A credential added to the BlueXP console setting.** To add Amazon FSx for ONTAP to the BlueXP working environment, a credential that grants BlueXP permissions to access Amazon FSx for ONTAP is set up in the BlueXP console setting.
- **java-11-openjdk installed on the EC2 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 to Amazon FSx for ONTAP and an EC2 compute instance. This document fills in certain details that might be missing from more general instructions.

To get started, complete the following steps:

- Read the general instructions [Protect your cloud native applications data](#) and the sections related to Oracle and Amazon FSx for ONTAP.
- Watch the following video walkthrough.

[Solution Deployment](#)

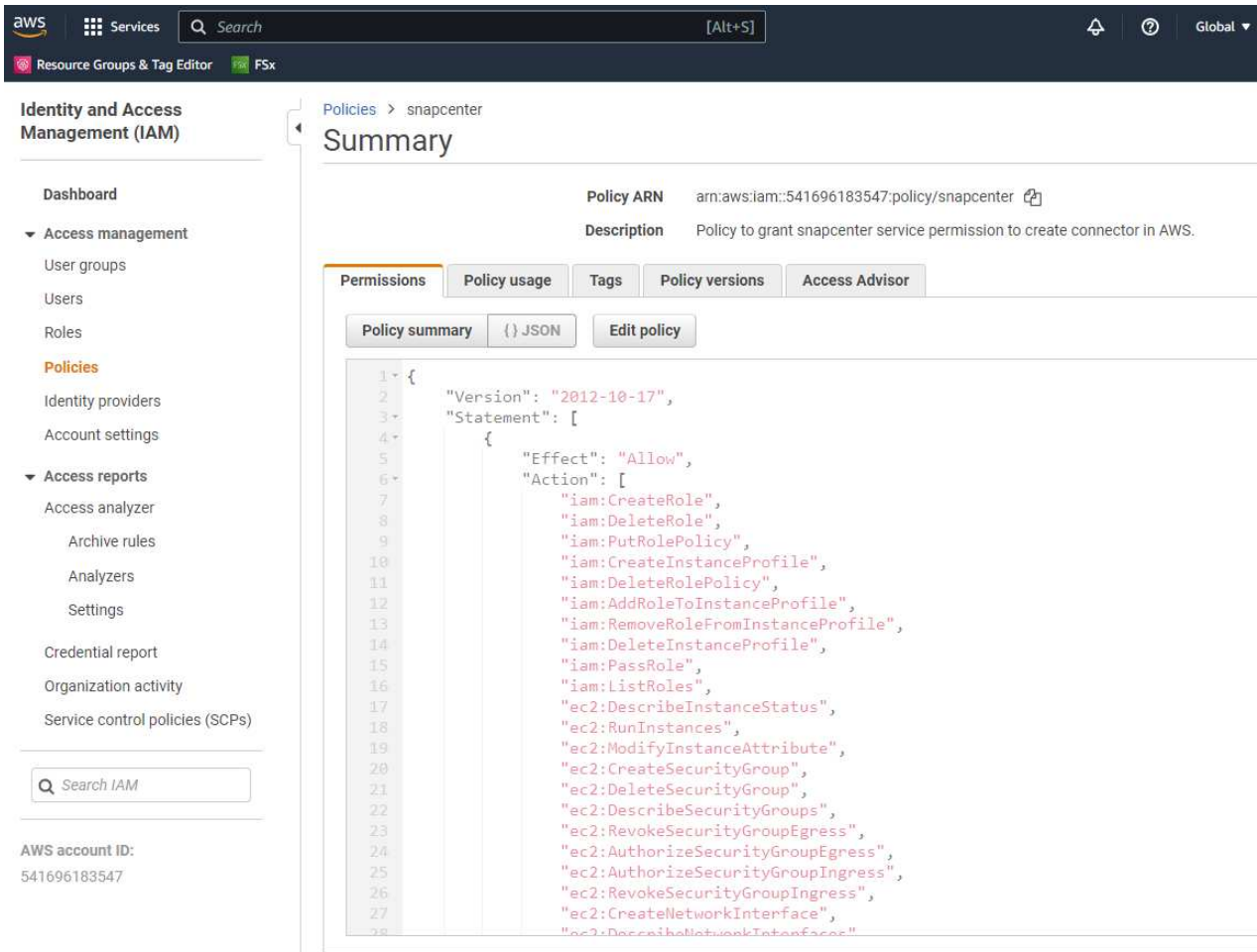
Prerequisites for SnapCenter service deployment

Deployment requires the following prerequisites.

1. A primary Oracle database server on an EC2 instance with an Oracle database fully deployed and running.
2. An Amazon FSx for ONTAP cluster deployed in AWS that is hosting the database volumes above.
3. An optional database server on an EC2 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 a production Oracle database.
4. If you need help to meet the above prerequisites for Oracle database deployment on Amazon FSx for ONTAP and EC2 compute instance, see [Oracle Database Deployment and Protection in AWS FSx/EC2 with iSCSI/ASM](#) or white paper [Oracle Database Deployment on EC2 and FSx Best Practices](#)

Onboarding to BlueXP preparation

1. Use the link [NetApp BlueXP](#) to sign up for BlueXP console access.
2. Login to your AWS account to create an IAM policy with proper permissions and assign the policy to the AWS account that will be used for BlueXP connector deployment.



The screenshot shows the AWS IAM console interface. On the left is a navigation menu with sections like 'Dashboard', 'Access management', 'Policies', 'Identity providers', 'Account settings', 'Access reports', and 'Service control policies (SCPs)'. The main content area is titled 'Policies > snapcenter' and 'Summary'. It displays the 'Policy ARN' as 'arn:aws:iam::541696183547:policy/snapcenter' and the 'Description' as 'Policy to grant snapcenter service permission to create connector in AWS.' Below this, there are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is active, showing a 'Policy summary' and a 'JSON' view. The JSON string is as follows:

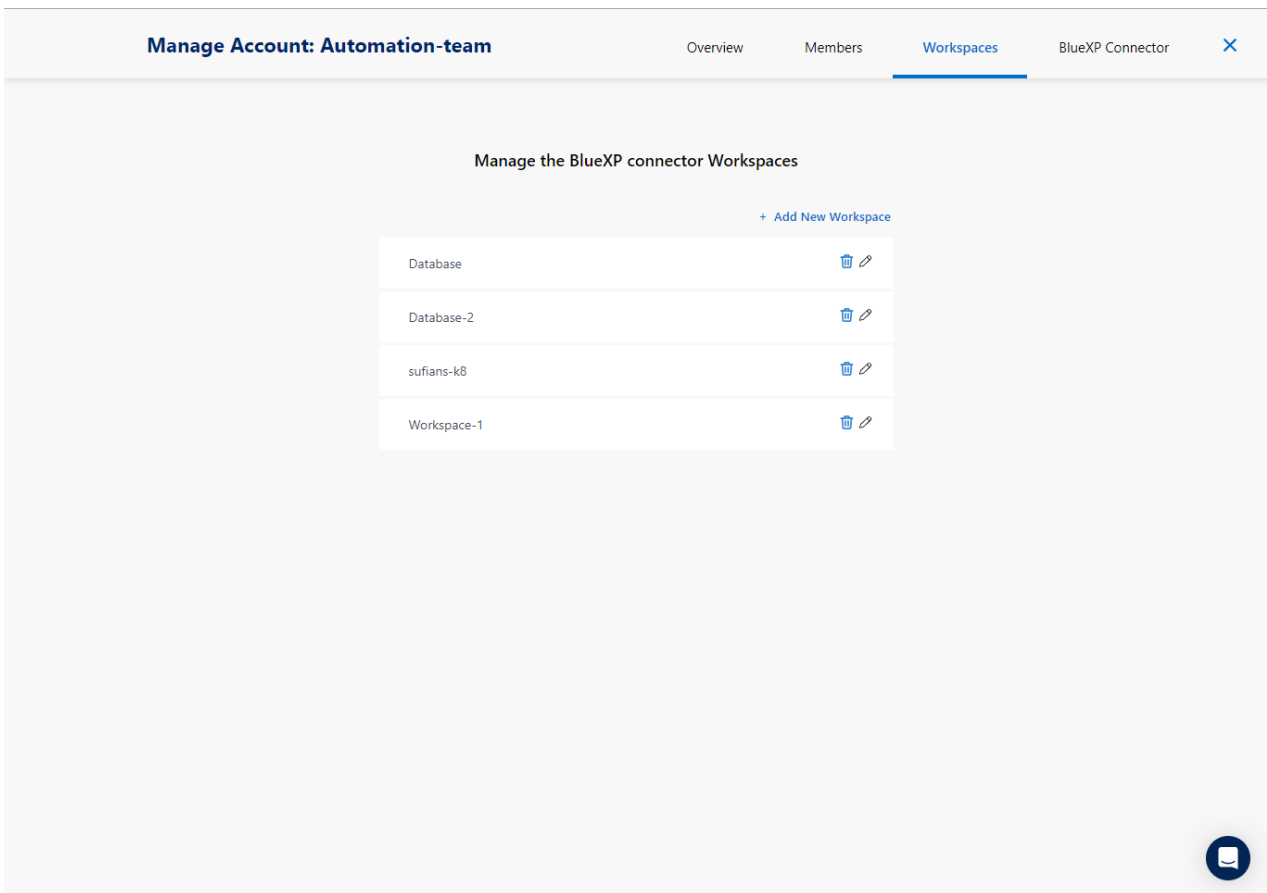
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ]
    }
  ]
}
```

The policy should be configured with a JSON string that is available in NetApp documentation. The JSON string can also be retrieved from the page when connector provisioning is launched and you are prompted for the prerequisites permissions assignment.

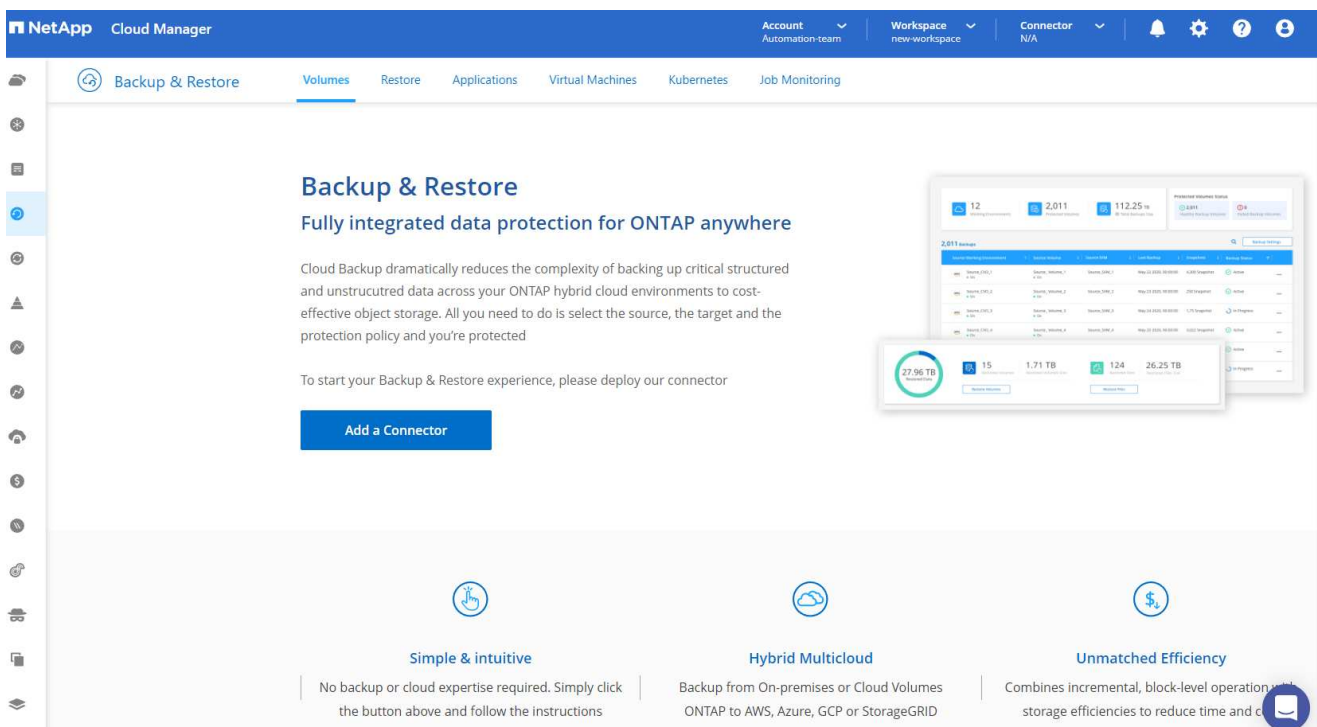
3. You also need the AWS VPC, subnet, security group, an AWS user account access key and secrets, an SSH key for ec2-user, and so on ready for connector provisioning.

Deploy a connector for SnapCenter services

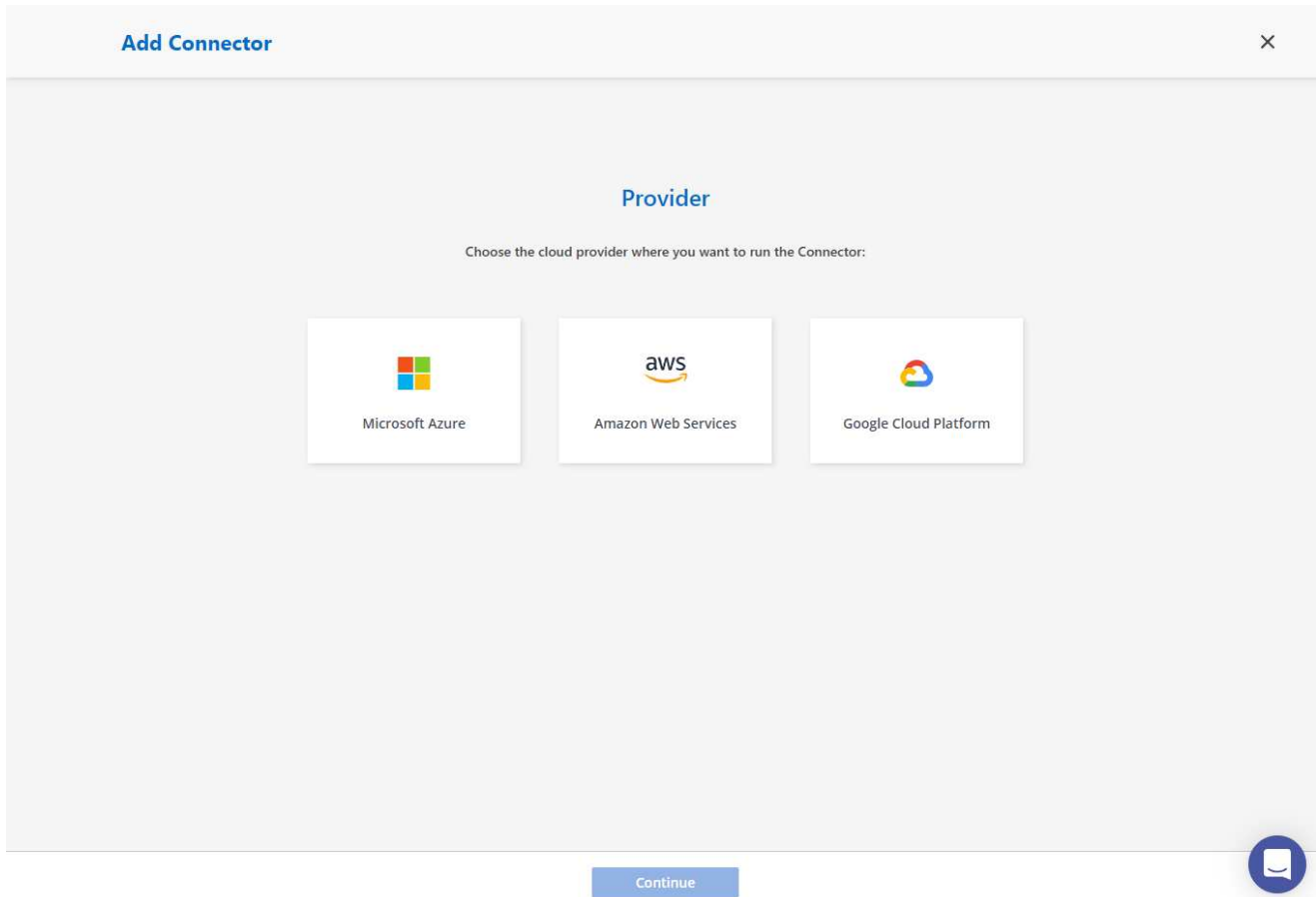
1. Login to the BlueXP console. For a shared account, it is a best practice to create an individual workspace by clicking **Account > Manage Account > Workspace** to add a new workspace.



2. Click **Add a Connector** to launch the connector provisioning workflow.



1. Choose your cloud provider (in this case, **Amazon Web Services**).



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

Deploying a Connector

The Connector is a crucial component for the day-to-day use of Cloud Manager.
It's used to connect Cloud Manager's services to your hybrid-cloud environments.
The 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 Connector installation.

Permissions

Set up an IAM role with the required permissions

Authentication

Choose between two AWS authentication methods: AWS keys or assuming an IAM role

Networking

Obtain details about the VPC and subnet in which the Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



1. Enter your AWS account authentication with **Access Key** and **Secret Key**.

- 1 AWS Credentials
- 2 Details
- 3 Network
- 4 Security Group
- 5 Review

AWS Authentication

Region

us-east-1 | US East (N. Virginia)

Select the Authentication Method: ☐ Assume Role ☒ AWS Keys

AWS Access Key

AKIA6JRXA6ZVGVFSHMO3

AWS Secret Key

.....

Want to launch an instance without AWS Credentials? [▼](#)

[Previous](#)

[Next](#)



2. Name the connector instance and select **Create Role** under **Details**.

Add Connector - AWS

More Information X

1 AWS Credentials

2 Details

3 Network

4 Security Group

5 Review

Details

Connector Instance Name ⓘ

SnapCenterSvs

Connector Role ⓘ

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-VZzSSP9-SnapCenter

☐ AWS Managed Encryption ⓘ

Master Key: aws/ebs (default) [Change Key](#)

+ Add Tags to Connector Instance

Previous

Next

1. Configure networking with the proper **VPC**, **Subnet**, and SSH **Key Pair** for connector access.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ Details

3 Network

4 Security Group

5 Review

Network

Connectivity

VPC

vpc-0b522d5e982a50ceb - 172.30.15.0/25

Subnet

172.30.15.0/25 | priv-subnet-01

Key Pair

sufi_new

Public IP

Use subnet settings (Disable)

Notice:

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

Proxy Configuration (Optional)

HTTP Proxy

Example: http://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous

Next

2. Set the **Security Group** for the connector.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ 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

1 Security Group

Security Group Name	Description
<input checked="" type="radio"/> default	default VPC security group

Previous

Next

3. 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 appears in the AWS EC2 dashboard.

Add BlueXP Connector - AWS

More Information X

✓ AWS Credentials

✓ Details

✓ Network

✓ Security Group

5 Review

Review

[Code for Terraform Automation](#)

BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIA4H43ZT56IWWR3TI
Region	us-east-1
VPC	vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet	172.30.15.0/25 priv-subnet-01
Key Pair	sufi_new
Public IP	Use subnet settings (Disable)
Proxy	None
Security Group	default

Previous

Add

Define a credential in BlueXP for AWS resources access

1. First, from AWS EC2 console, create a role in **Identity and Access Management (IAM)** menu **Roles**, **Create role** to start role creation workflow.

The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like 'Dashboard', 'Access management', 'Access reports', and 'Related consoles'. The main area displays a table of roles, including 'AmazonEC2RoleforAWSUser', 'AmazonSSMRoleforInstancesQuickSetup', and 'aws-controltower-AdministratorExecutionRole'. The 'Create role' button is in the top right.

2. In **Select trusted entity** page, choose **AWS account**, **Another AWS account**, and paste in the BlueXP account ID, which can be retrieved from BlueXP console.

The screenshot shows the 'Select trusted entity' page in the AWS IAM console. The 'Trusted entity type' section has 'AWS account' selected. Under 'An AWS account', the 'Another AWS account' radio button is selected, and the 'Account ID' field contains the value '992013314444'. The 'Options' section includes checkboxes for 'Require external ID' and 'Require MFA'.

3. Filter permission policies by fsx and add **Permissions policies** to the role.

Add permissions [Info](#)Permissions policies (Selected 1/889) [Info](#)

Choose one or more policies to attach to your new role.

Q Filter policies by property or policy name and press enter. 4 matches

'fsx' X Clear filters

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	AmazonFSxReadOnlyAccess	AWS ma...	Provides read only access to Amazon FSx.
<input checked="" type="checkbox"/>	AmazonFSxFullAccess	AWS ma...	Provides full access to Amazon FSx and access to related AWS services.
<input type="checkbox"/>	AmazonFSxConsoleReadOnlyAccess	AWS ma...	Provides read only access to Amazon FSx and access to related AWS services via the AWS Management Console.
<input type="checkbox"/>	AmazonFSxConsoleFullAccess	AWS ma...	Provides full access to Amazon FSx and access to related AWS services via the AWS Management Console.

Set permissions boundary - optional [Info](#)

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

[Cancel](#)[Previous](#)[Next](#)4. In **Role details** page, name the role, add a description, then click **Create role**.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

fsxn_bluexp

Maximum 64 characters. Use alphanumeric and +, -, @, _ characters.

Description

Add a short explanation for this role.

Grant permission for BlueXP access to FSxN in AWS.

Maximum 1000 characters. Use alphanumeric and +, -, @, _ characters.

Step 1: Select trusted entities

[Edit](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "952013314444"
9       },
10      "Condition": {}
11    }
12  ]
13 }
```

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

NetApp BlueXP [Q BlueXP Search](#) [Account Automation-te...](#) [Workspace Database-2](#) [Connector acio-aws-conn...](#) [🔔](#) [⚙️](#) [?](#) [🔍](#)

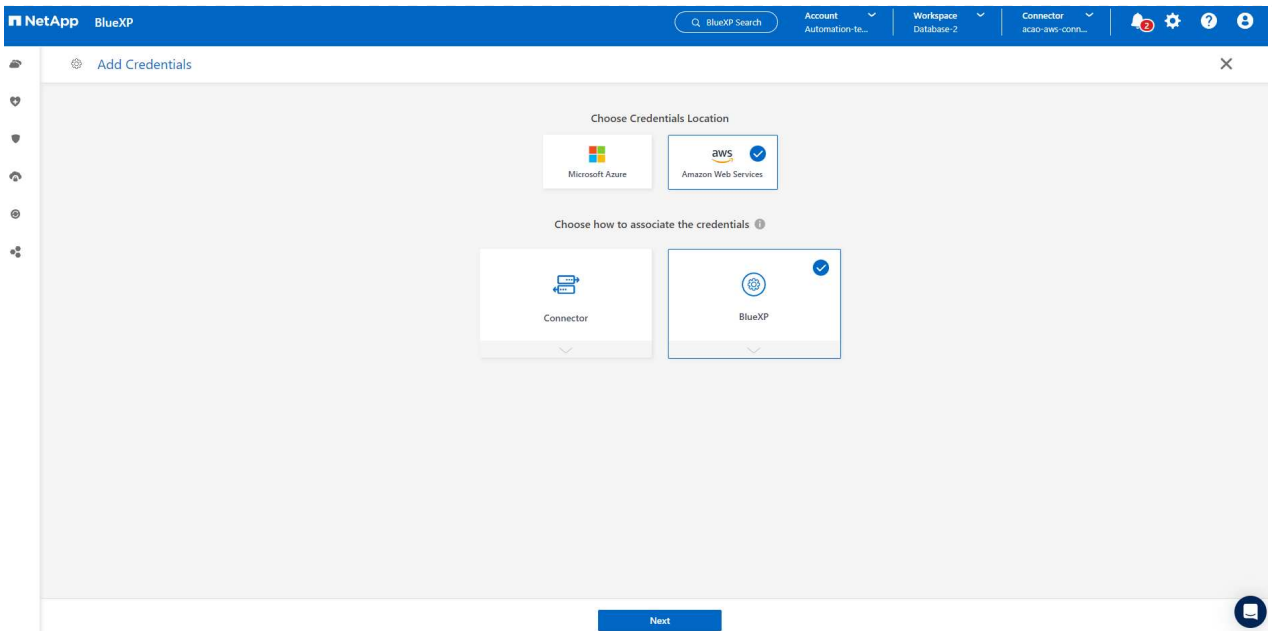
[Credentials](#) [Account credentials](#) [User credentials](#)

BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

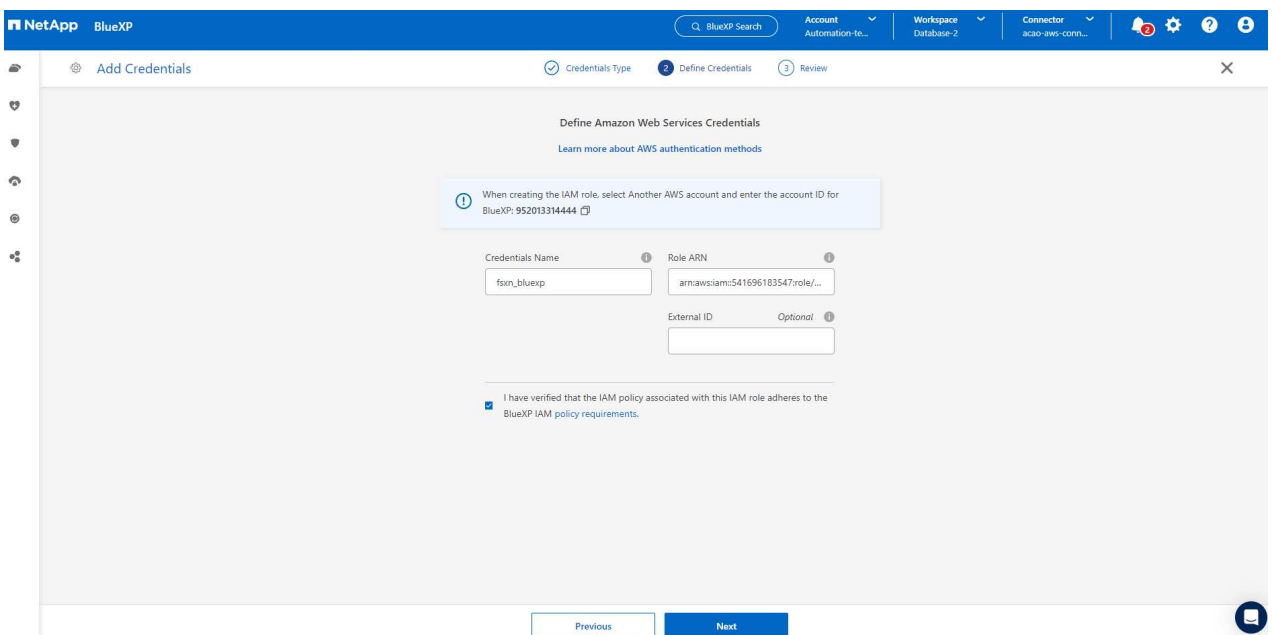
5 Credentials [Add credentials](#)

shantanucreds	
Type: Assume Role BlueXP	
210811600188 AWS Account ID	nkarthik_kafka_nfs_role_FSxN Assume Role

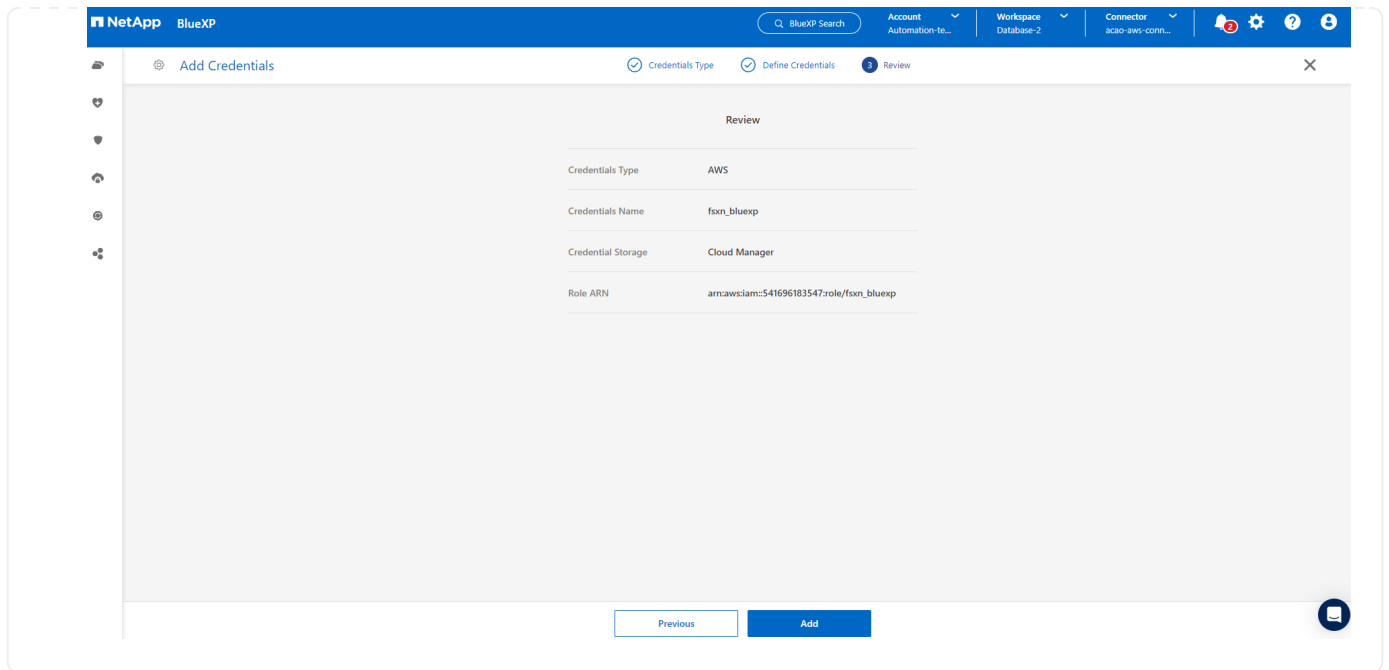
6. Choose credential location as - **Amazon Web Services - BlueXP**.



7. Define AWS credentials with proper **Role ARN**, which can be retrieved from AWS IAM role created in step one above. BlueXP **account ID**, which is used for creating AWS IAM role in step one.



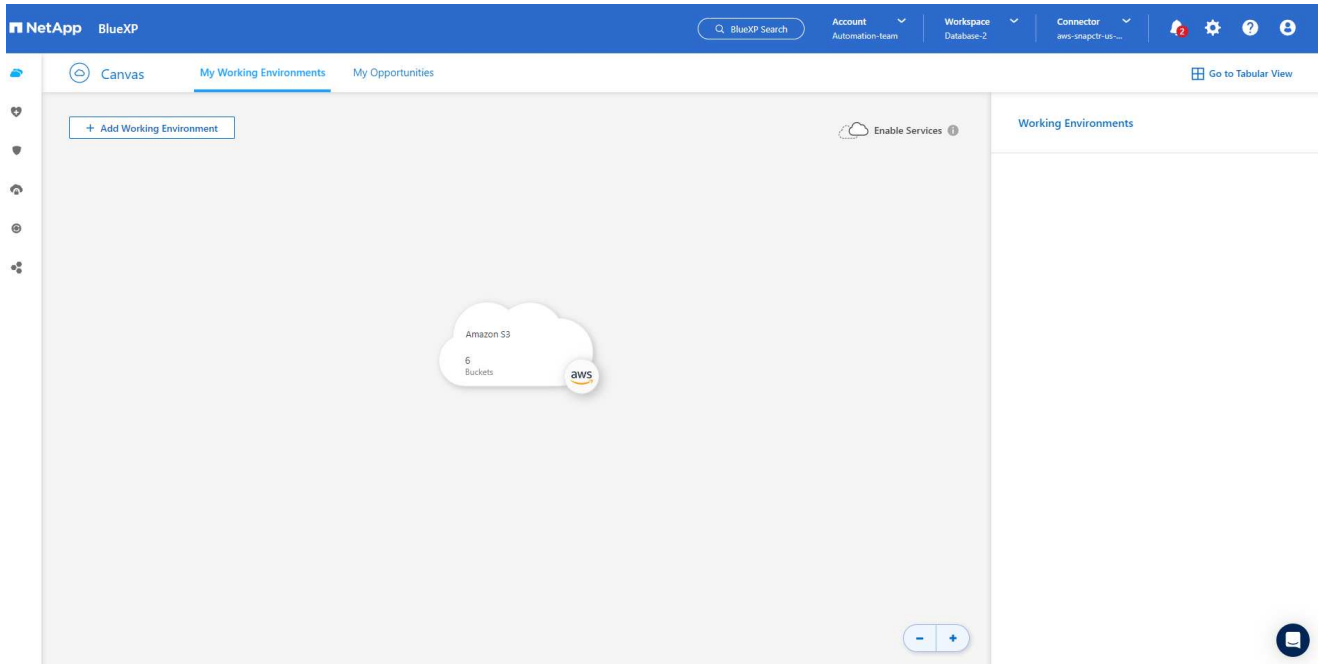
8. Review and **Add**.



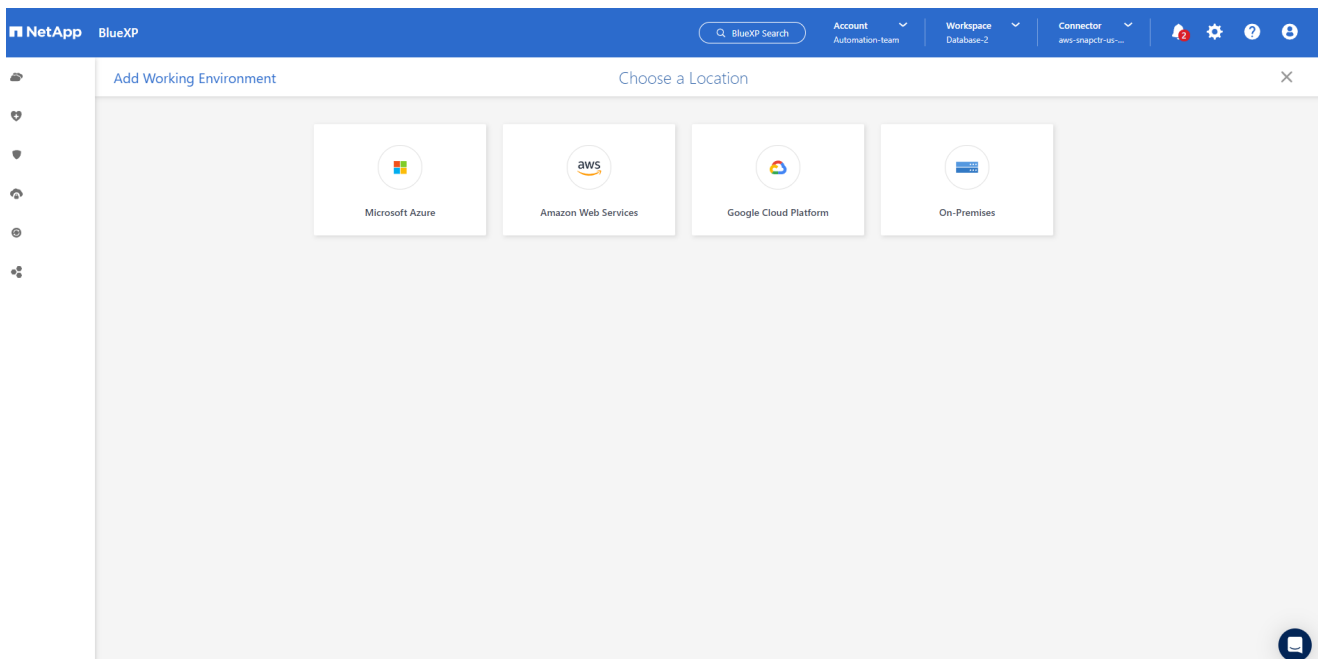
SnapCenter services setup

With the connector deployed and the credential added, SnapCenter services can now be set up with the following procedure:

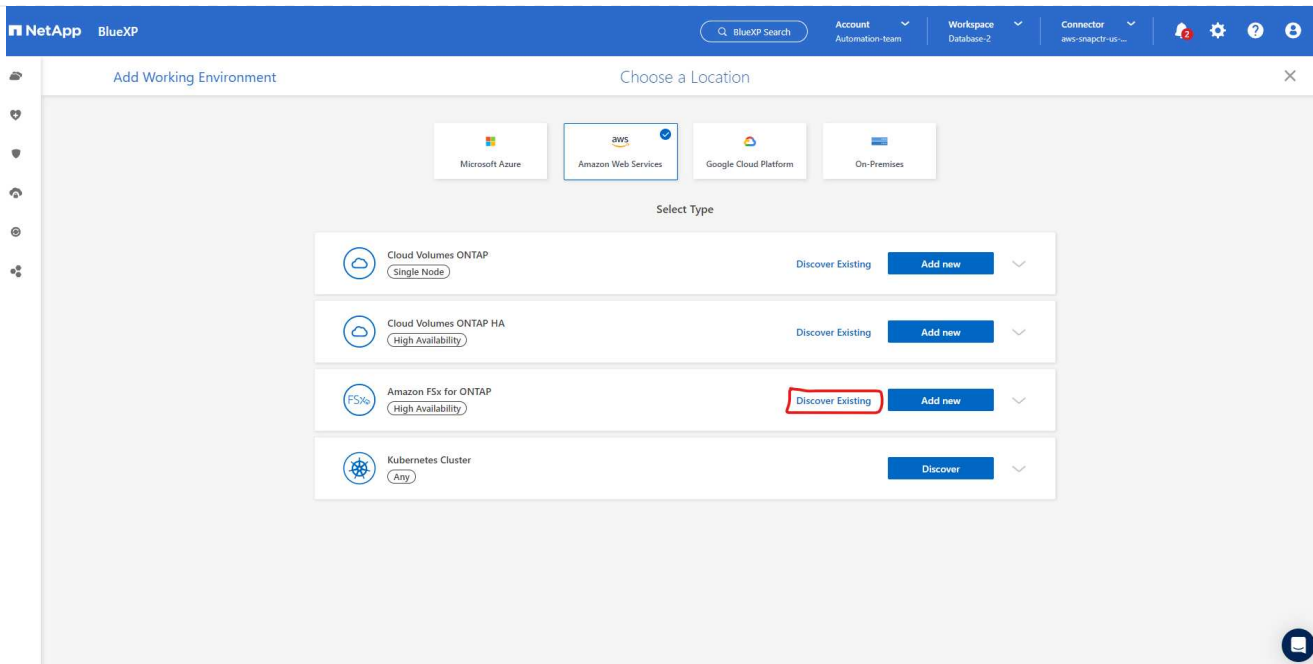
1. From **My Working Environment** click **Add working Environment** to discover FSx deployed in AWS.



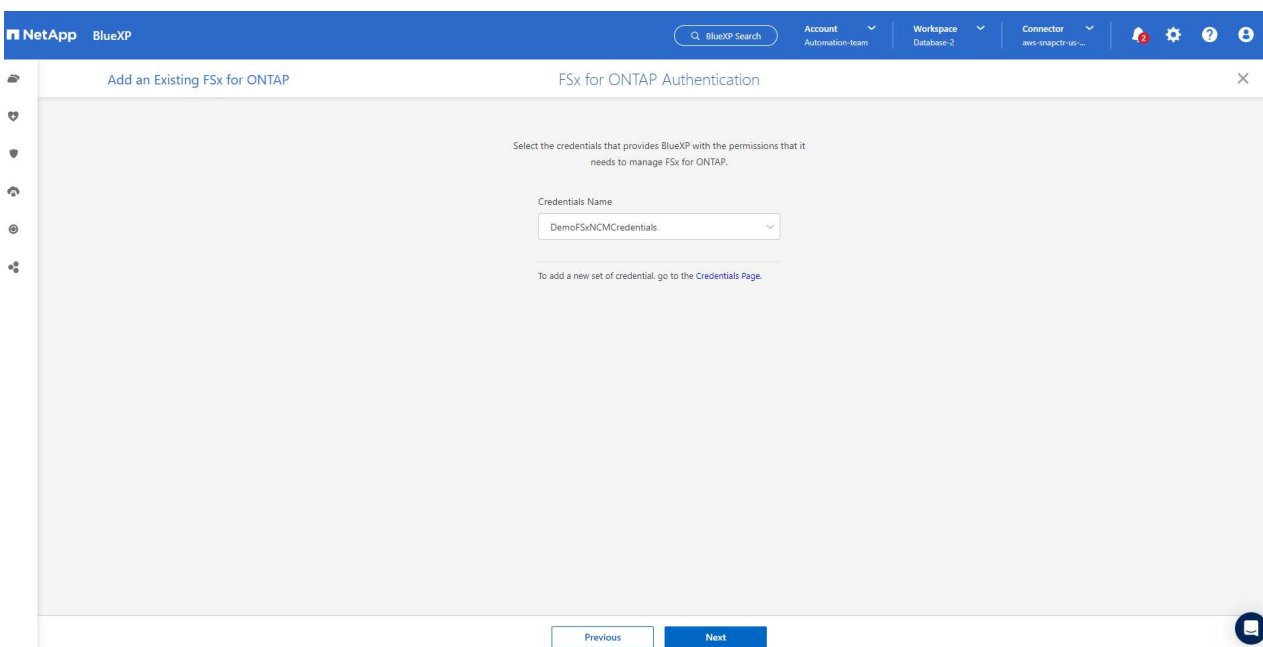
1. Choose **Amazon Web Services** as the location.



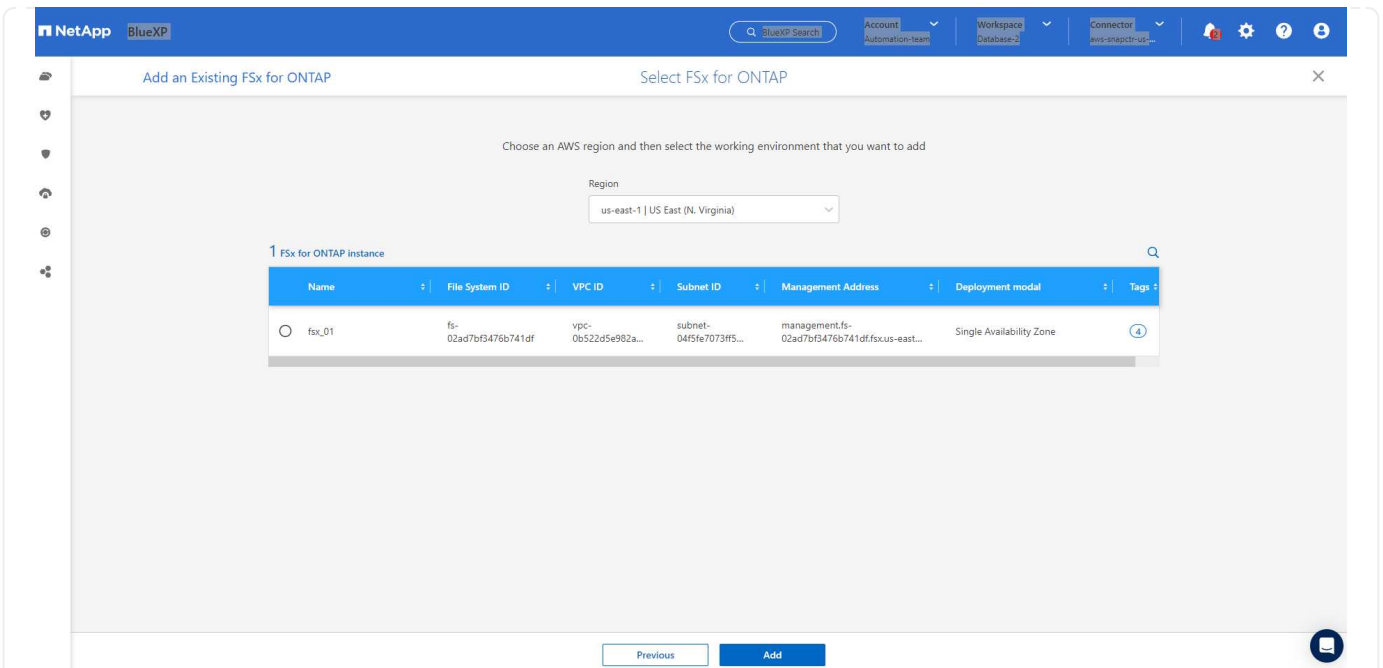
1. Click **Discover Existing** next to **Amazon FSx for ONTAP**.



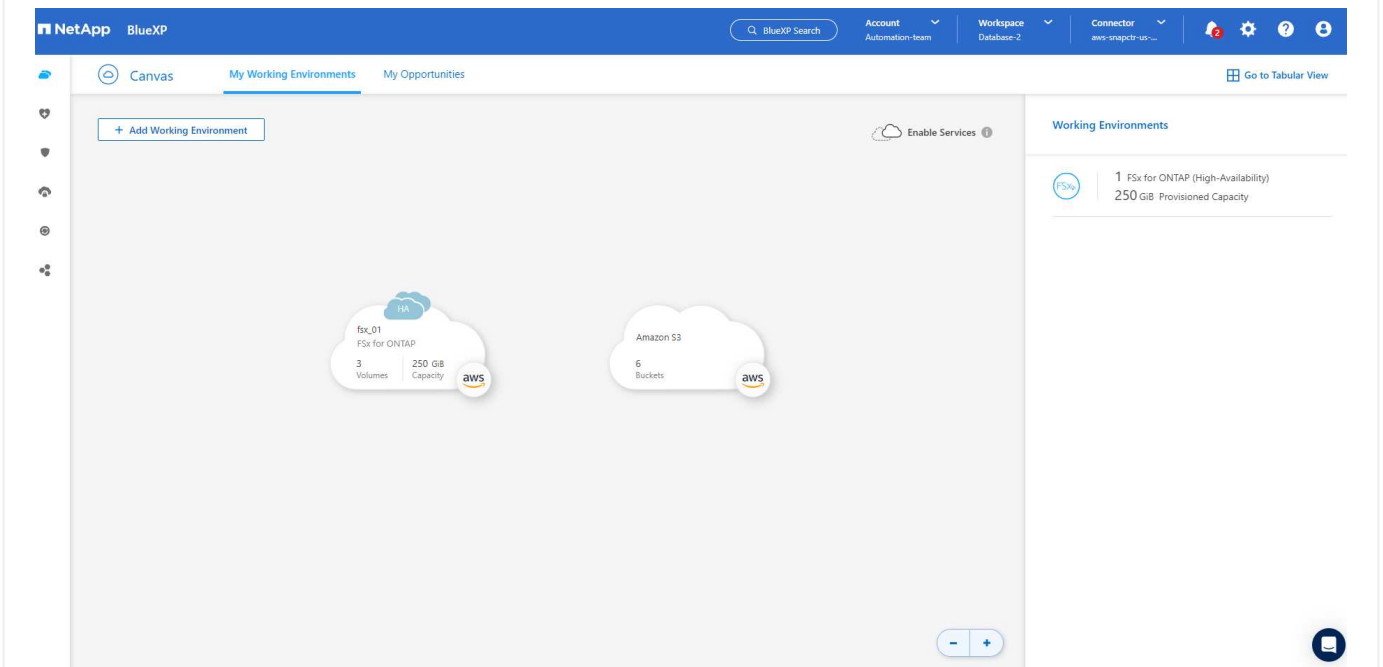
1. Select the **Credentials Name** that you have created in previous section to grant BlueXP with the permissions that it needs to manage FSx for ONTAP. If you have not added credentials, you can add it from the **Settings** menu at the top right corner of the BlueXP console.



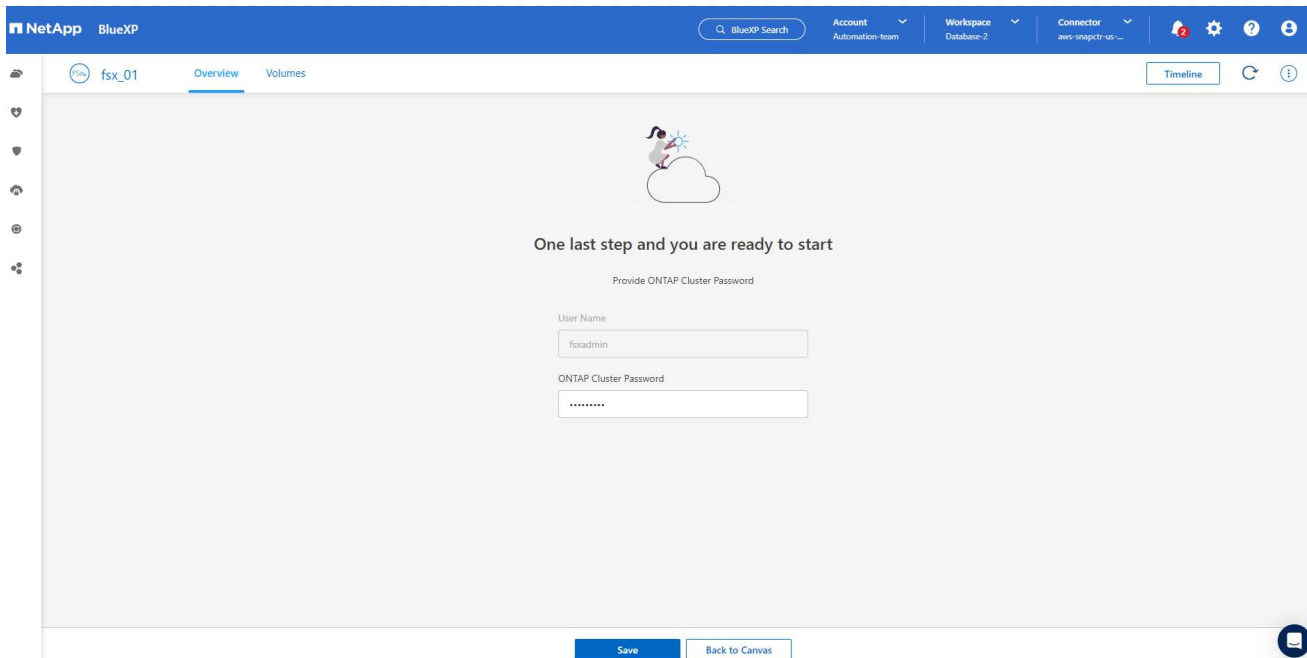
2. Choose the AWS region where Amazon FSx for ONTAP is deployed, select the FSx cluster that is hosting the Oracle database and click Add.



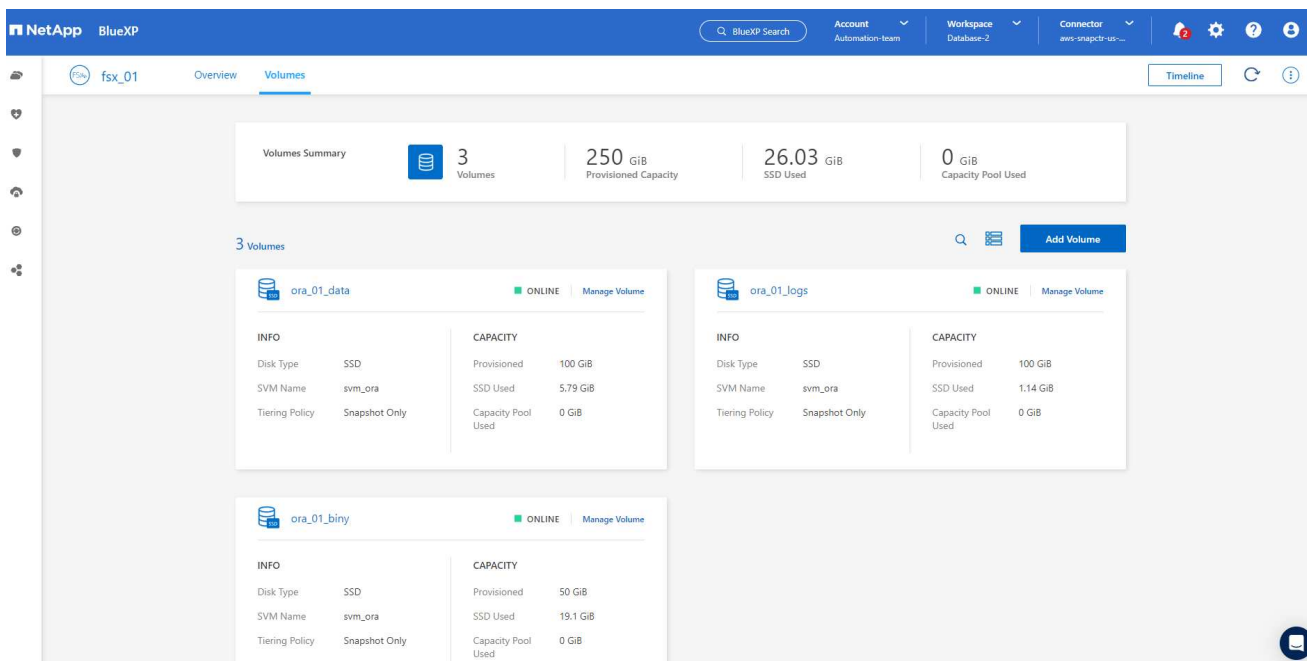
1. The discovered Amazon FSx for ONTAP instance now appears in the working environment.



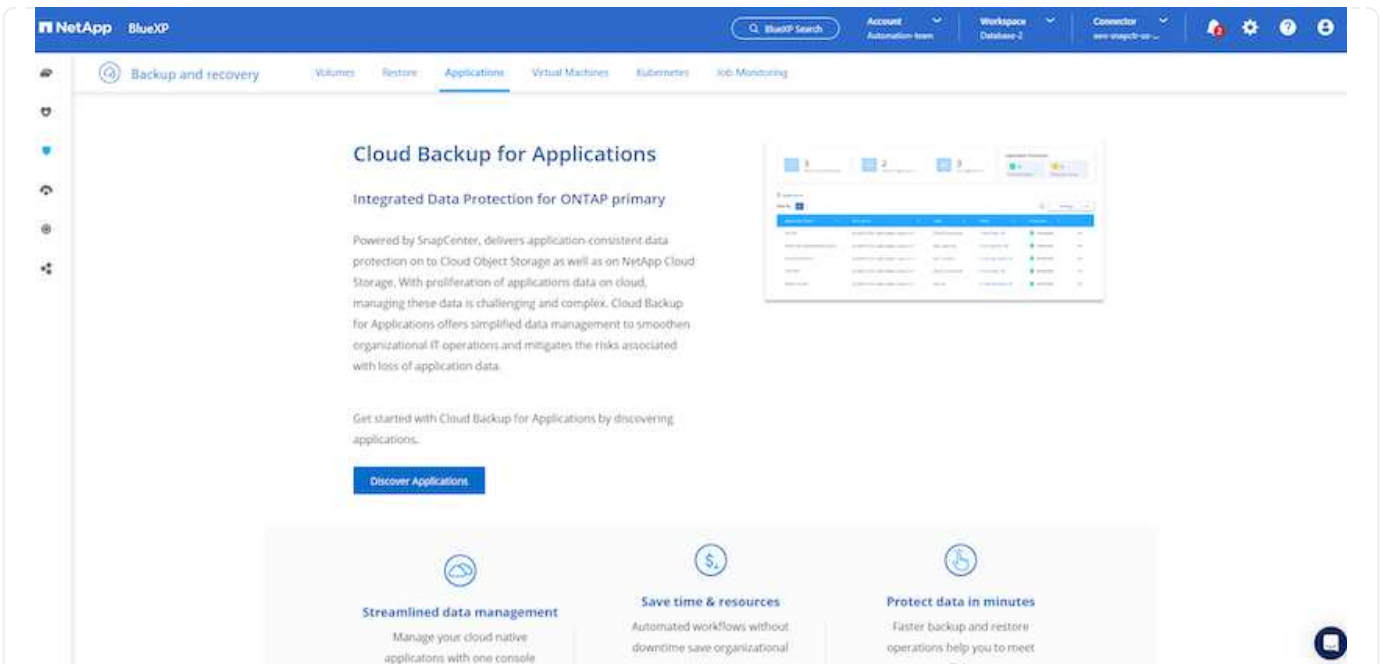
1. You can log into the FSx cluster with your fsxadmin account credentials.



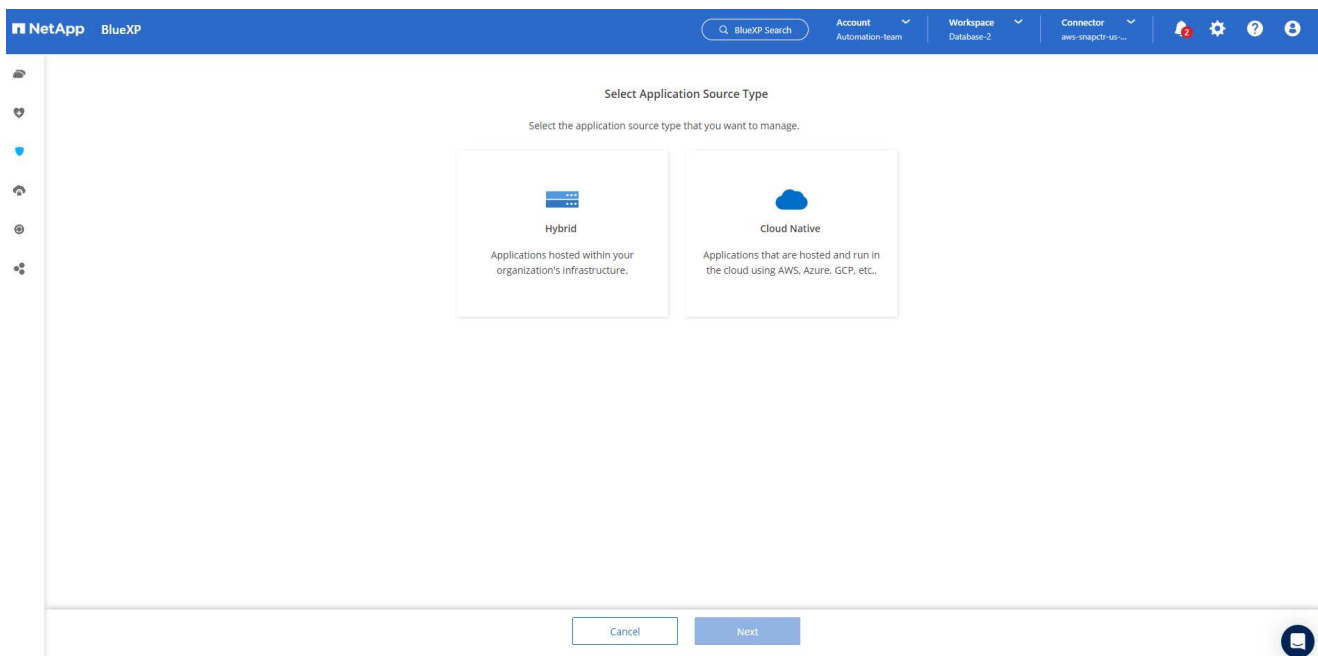
1. After you log into Amazon FSx for ONTAP, review your database storage information (such as database volumes).



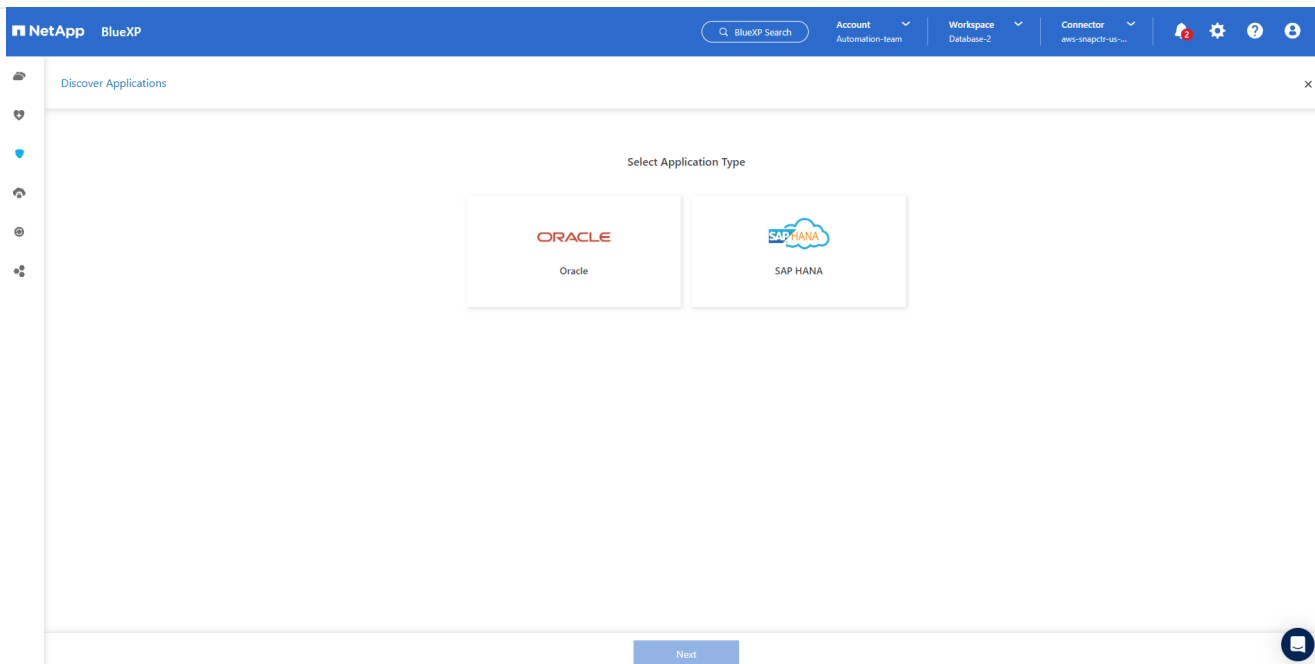
1. From the left-hand sidebar of the console, hover your mouse over the protection icon, and then click **Protection > Applications** to open the Applications launch page. Click **Discover Applications**.



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



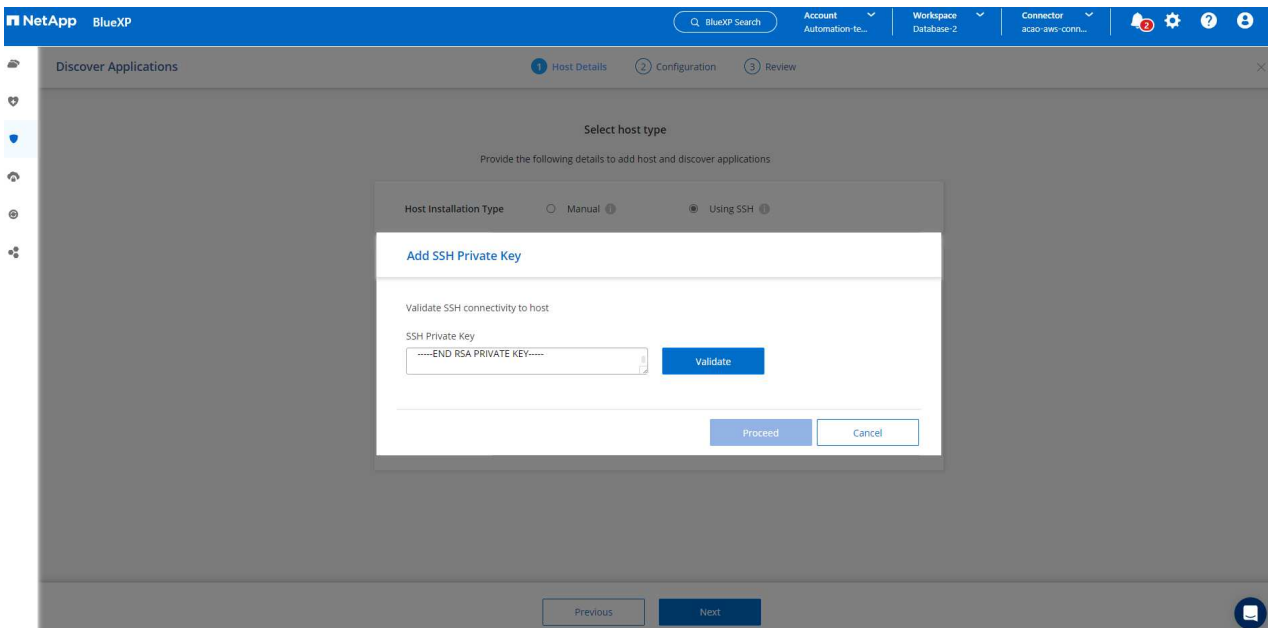
1. Choose **Oracle** for the application type.



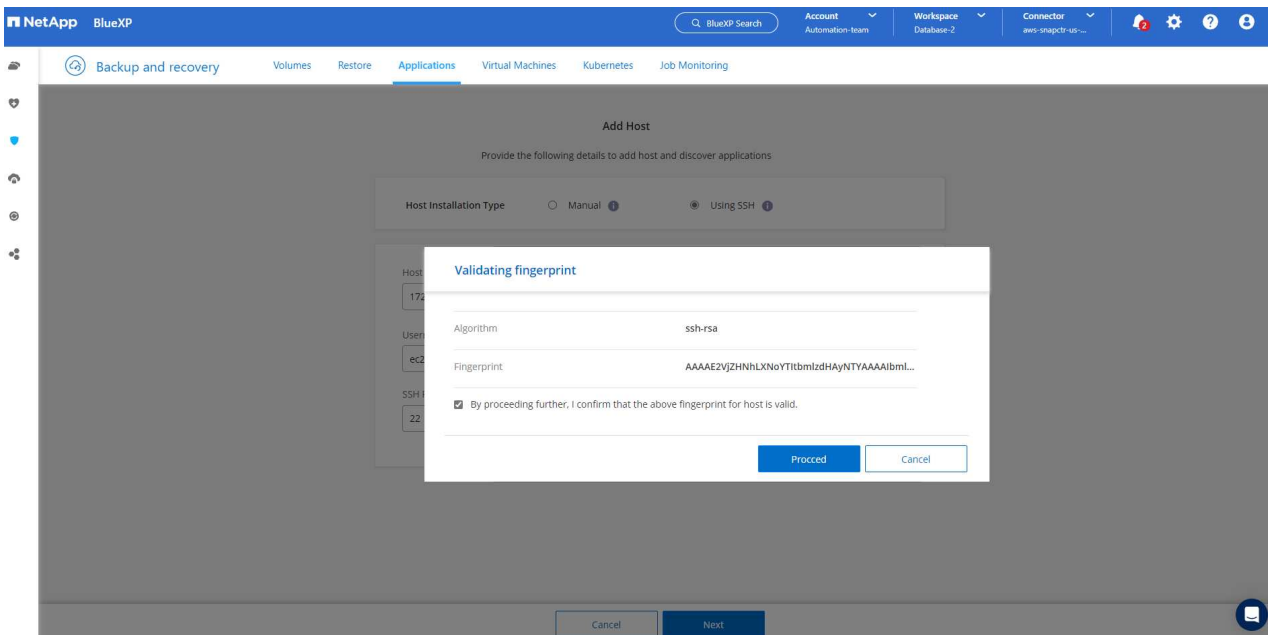
1. Fill in the AWS EC2 Oracle application host details. Choose **Using SSH** as **Host Installation Type** for one step plugin installation and database discovery. Then, click on **Add SSH Private Key**.

The screenshot shows the 'Add Host' form in NetApp BlueXP. The form is titled 'Add Host' and has a subtitle 'Provide the following details to add host and discover applications'. The 'Host Installation Type' is set to 'Using SSH'. The form contains several input fields: 'Host FQDN or IP' (172.30.15.58), 'Connector' (aws-snapctr-us-east), 'Username(Sudo)' (ec2-user), 'SSH Port' (22), and 'Plug-in Port' (8145). There is a link to 'Add SSH Private Key Optional'. At the bottom, there are 'Cancel' and 'Next' buttons.

2. Paste in your ec2-user SSH key for the database EC2 host and click on **Validate** to proceed.



3. You will be prompted for **Validating fingerprint** to proceed.



4. Click on **Next** to install an Oracle database plugin and discover the Oracle databases on the EC2 host. Discovered databases are added to **Applications**. The database **Protection Status** shows as **Unprotected** when initially discovered.

NetApp
BlueXP

BlueXP Search

Account Automation-team

Workspace Database-2

Connector aws-snapctr-us...

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Cloud Native

Oracle

1 Hosts

1 ORACLE

0 Clone

Application Protection

0 Protected

1 Unprotected

1 Databases

Filter By

Manage Databases

Settings

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

1 - 1 of 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. Click the three dots next to the database **Protection Status**, and then click **Policies** to view the default preloaded database protection policies that can be applied to protect your Oracle databases.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below the navigation bar, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '1 Hosts', '1 ORACLE', and '0 Clone'. An 'Application Protection' section shows '0 Protected' and '1 Unprotected'. A table lists databases with columns 'Name', 'Host Name', 'Policy Name', and 'Protection Status'. The table shows one database 'db1' with host '172.30.15.58' and status 'Unprotected'. A dropdown menu is open next to the 'Protection Status' column, showing options: 'Policies', 'About', and 'Hosts'.

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

1. You can also create your own policy with a customized backup frequency and backup data-retention window.

The screenshot shows the NetApp BlueXP interface with the 'Applications > Policies' view. The top navigation bar is the same as the previous screenshot. Below the navigation bar, there are filters for 'Cloud Native' and 'Oracle'. A 'Create Policy' button is visible. A table lists policies with columns 'Policy Name', 'Backup Type', and 'Schedules and Retention'. The table shows four policies: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy has a 'FullBackup' type and specific schedules and retention settings. A dropdown menu is open next to the 'Schedules and Retention' column, showing options: 'Policies', 'About', and 'Hosts'.

Policy Name	Backup Type	Schedules and Retention
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, Oct, Nov
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, Oct, Nov
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, Oct, Nov
my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

1. When you are happy with the policy configuration, you can then assign your policy of choice to protect the database.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' section displays a summary for 'Cloud Native' and 'Oracle' environments. Below this, a table lists databases. The database 'db1' is shown with a protection status of 'Unprotected'. A context menu is open over the 'Unprotected' status, with the 'Assign Policy' option highlighted.

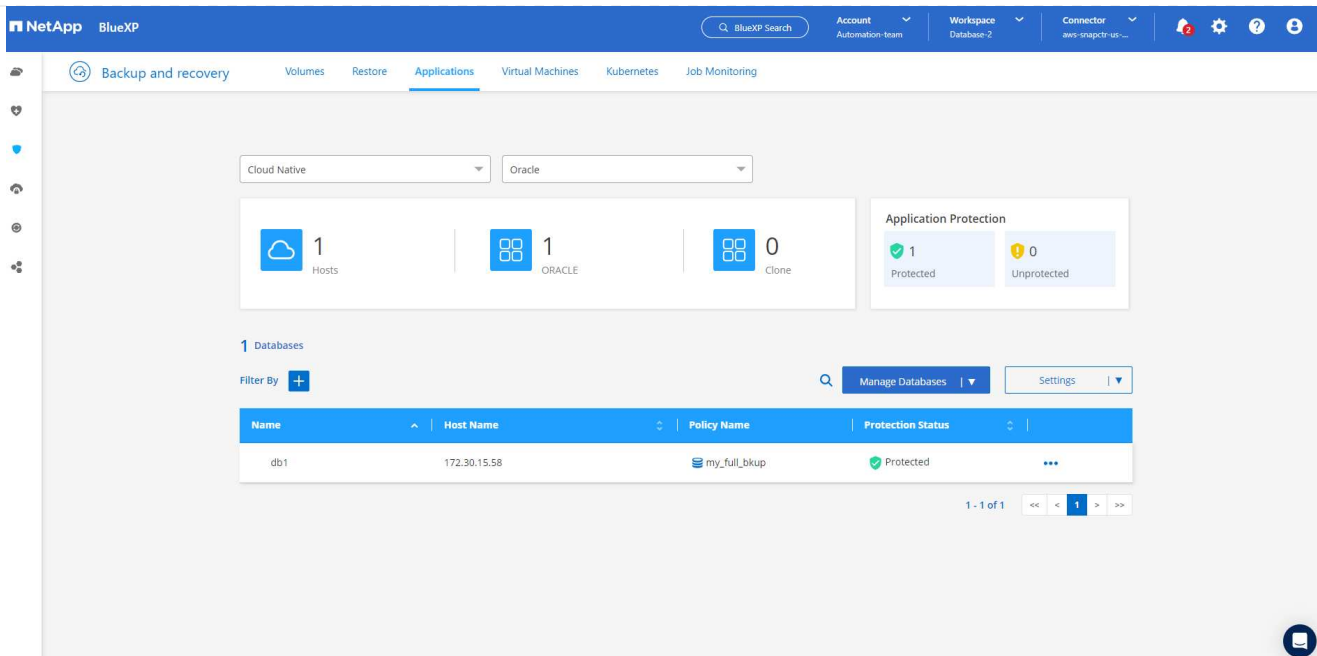
Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

1. Choose the policy to assign to the database.

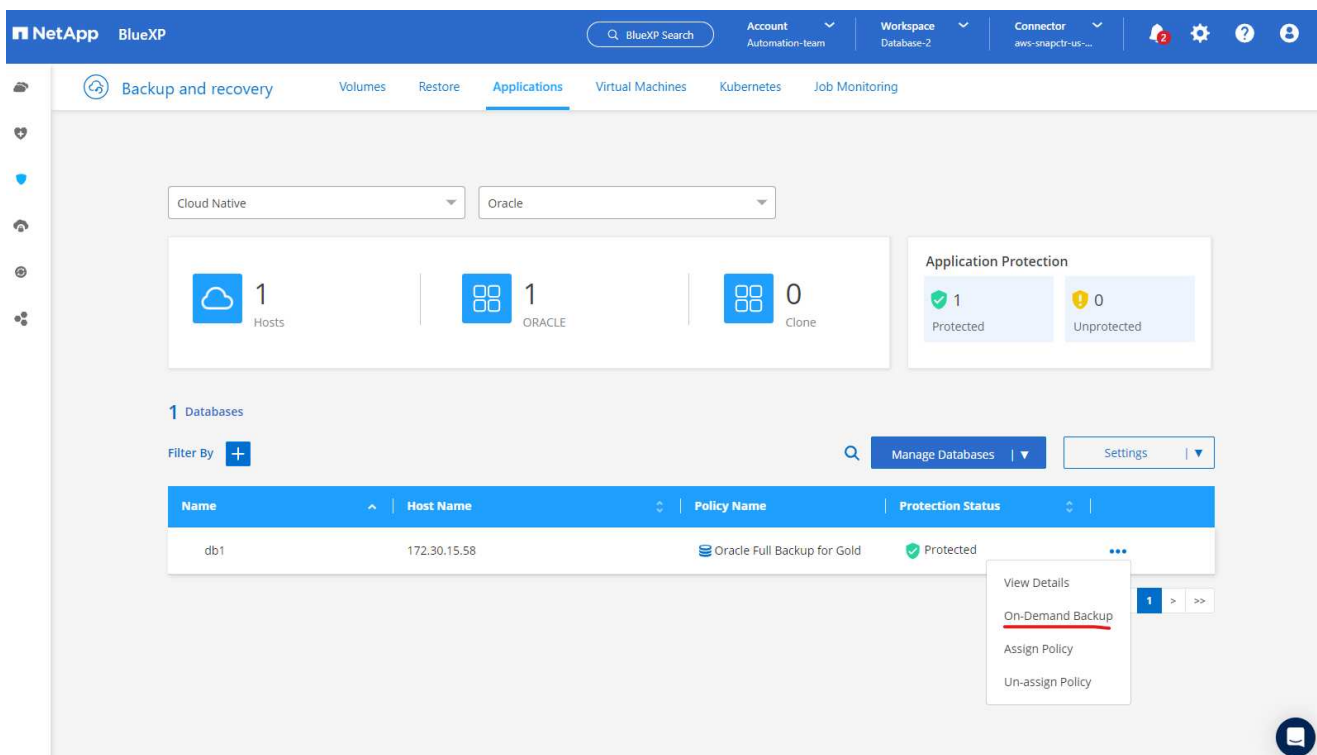
The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. The dialog title is 'Assign Policy' with the subtitle 'Assign a policy to start taking backups of the database "db1"'. It displays a list of 4 policies. The policy 'my_full_bkup' is selected, indicated by a blue checkmark in the selection column.

Policy Name	Backup Type	Schedules
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
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
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
my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

1. After the policy is applied, the database protection status changed to **Protected** with a green check mark.



1. The database backup runs on a predefined schedule. You can also run a one-off on-demand backup as shown below.



1. The database backups details can be viewed by clicking **View Details** from the menu list. This includes the backup name, backup type, SCN, and backup date. A backup set covers a snapshot for both data volume and log volume. A log volume snapshot takes place right after a database volume snapshot. You can apply a filter if you are looking for a particular backup in a long list.

NetApp
BlueXP

Q

BlueXP Search

Account

Automation-team

Workspace

Database-2

Connector

aws-snapctr-us...

2

⚙️

?

👤

🏠

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Applications >

Database Details

Database Details

db1

Database Name

Protected

Protection

Oracle Full Backup for Gold

Policy Names

Database Type

172.30.15.58

Host Name

FSx

Host Storage

Unreachable

Database Version

bKed8yv2T19Bj0V5QyqvA...

Agent Id

-

Clones

-

Parent Database

8 Backups

Filter By

+

🔍

Select Timeframe

▼

Backup Name	Backup Type	SCN	Backup Date	
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_12_18_60900_1	Log	2589354	Mar 24, 2023, 3:12:34 pm	Delete
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_11_51_51476_0	Data	2589306	Mar 24, 2023, 3:12:18 pm	...
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	...

💬

Oracle database restore and recovery

27

1. For a database restore, choose the right backup, either by the SCN or backup time. Click the three dots from the database data backup, and then click **Restore** to initiate database restore and recovery.

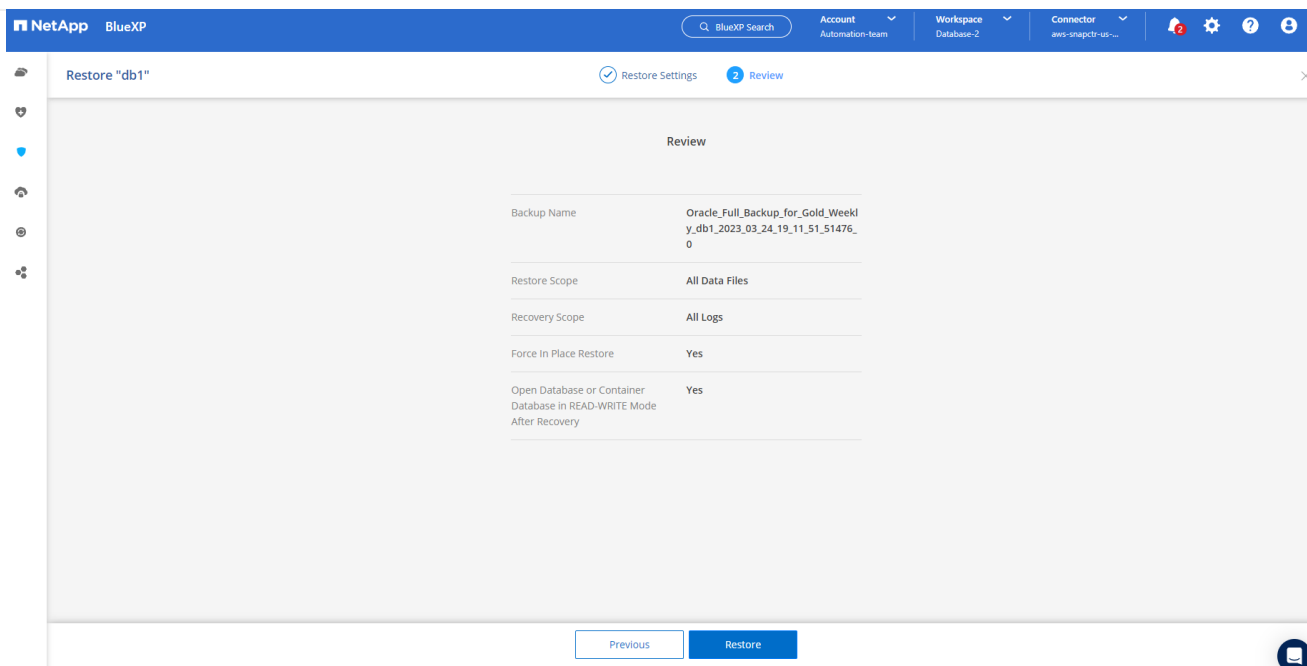
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' tab is selected, leading to 'Database Details' for a database named 'db1'. The details card shows information such as Host Name (172.30.15.58), Host Storage (FSx), Database Version (Unreachable), and Agent Id (bKed8yv2T19BJ0V5Qyqva...). Below this, a 'Backups' section shows a table of backups. The table has columns for Backup Name, Backup Type, SCN, Backup Date, and a 'Delete' button. The backup 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1' is selected, and a context menu is open with the 'Restore' button highlighted.

Backup Name	Backup Type	SCN	Backup Date	Actions
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	...
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1	Log	2580577	Mar 24, 2023, 11:37:11	Restore, Delete, Clone
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_36_33_27205_0	Data	2580524	Mar 24, 2023, 11:37:00	

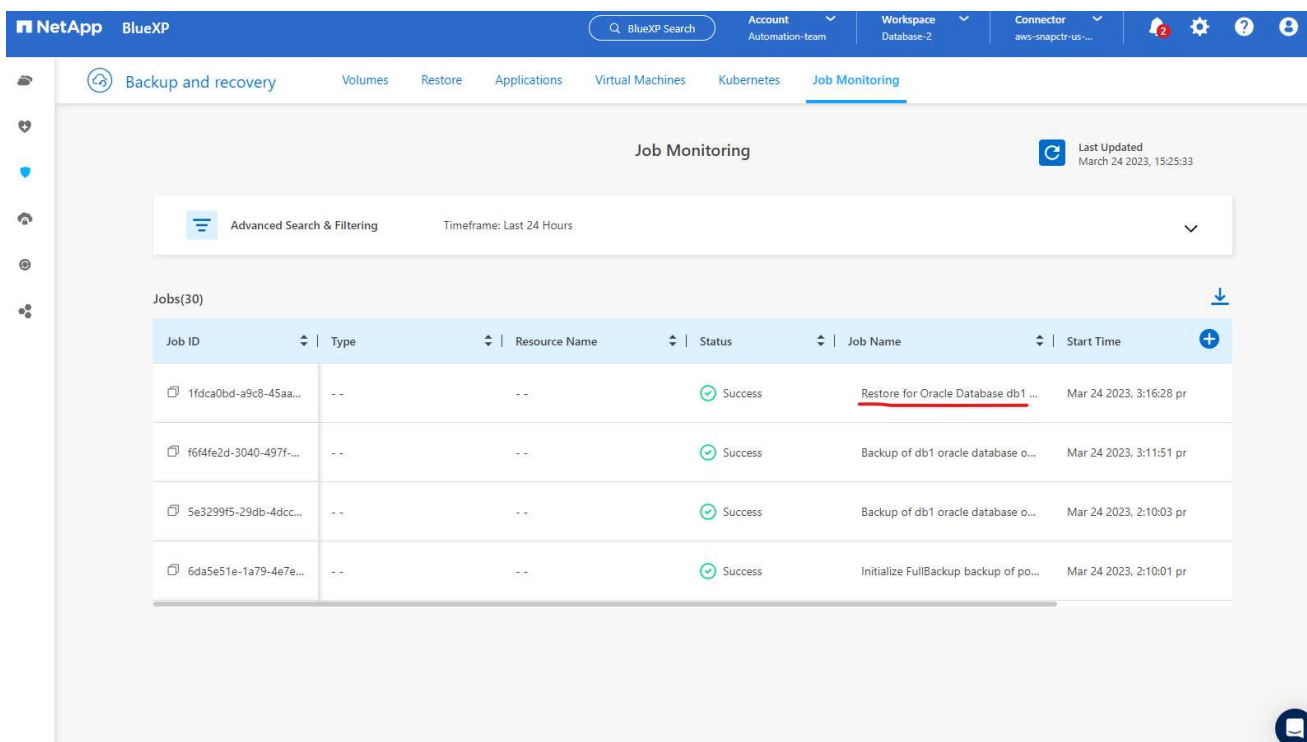
1. Choose your restore setting. If you are sure that nothing has changed in the physical database structure after the backup (such as the addition of a data file or a disk group), you can use the **Force in place restore** option, which is generally faster. Otherwise, do not check this box.

The screenshot shows the 'Restore "db1"' dialog in the NetApp BlueXP interface. The 'Restore Settings' tab is active. Under 'Restore Scope', the 'All Data Files' option is selected, and the 'Force in place restore' checkbox is checked. A note explains that in place restore will skip the foreign files validation check. Under 'Recovery Scope', the 'All Logs' option is selected. The 'Archive Log Files Locations' field is set to '/mnt/log_location001'. The 'Open the database or the container database in READ-WRITE mode after recovery' checkbox is also checked. At the bottom, there are 'Previous' and 'Next' buttons.

1. Review and start database restore and recovery.



1. From the **Job Monitoring** tab, you can view the status of the restore job as well as any details while it is running.



NetAppBlueXP

BlueXP Search

AccountAutomation team

WorkspaceDatabase-2

Connectoraws-snapctr-us-...

2

?

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring > Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4

Job Details

Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4

Expand All

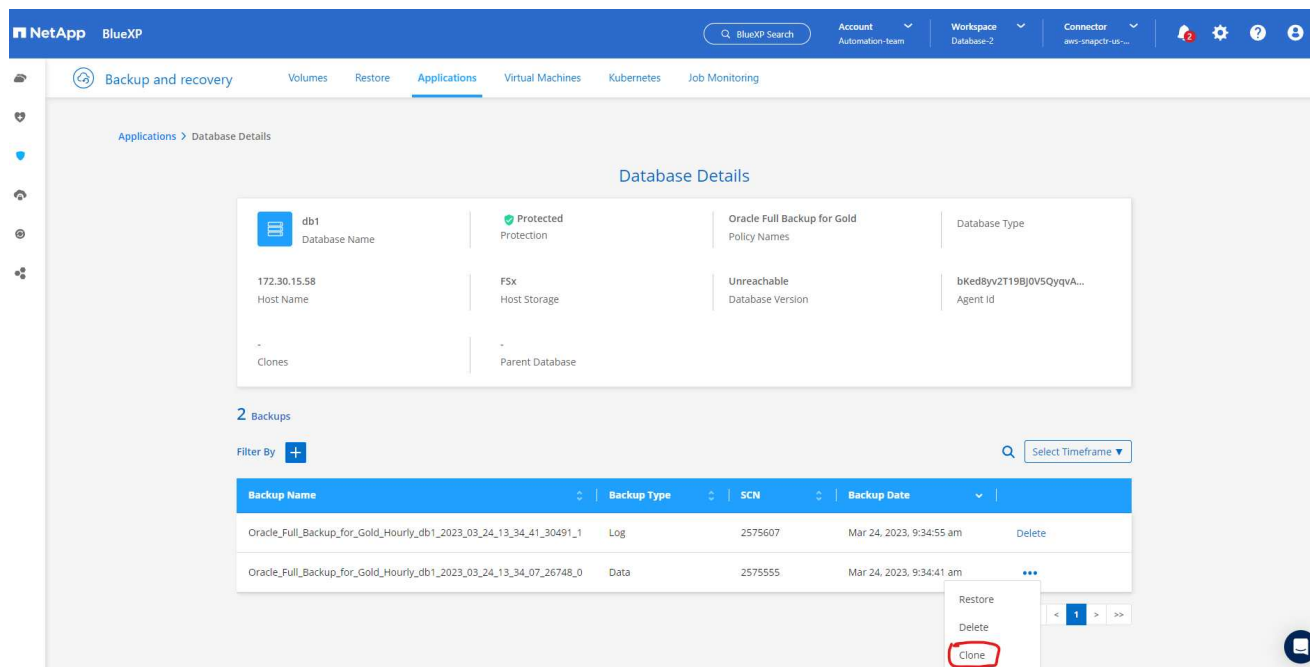
Sub-Jobs(6)

Job Name	Job ID	Start Time	End Time	Duration
Restore for Oracle Database db1 using backup ...	1fdca0bd-a9c8-45aa-9d...	Mar 24 2023, 3:16:28 pm	Mar 24 2023, 3:23:33 pm	7 Minutes
Post Restore Cleanup	2096a8e4-889d-4b2a-9...	Mar 24 2023, 3:23:18 pm	Mar 24 2023, 3:23:32 pm	14 Seconds
Post Restore	fb7b1171-9f6f-4228-9e...	Mar 24 2023, 3:20:06 pm	Mar 24 2023, 3:23:19 pm	3 Minutes
Restore	0f4580d0-6598-458b-a7...	Mar 24 2023, 3:17:49 pm	Mar 24 2023, 3:20:07 pm	2 Minutes

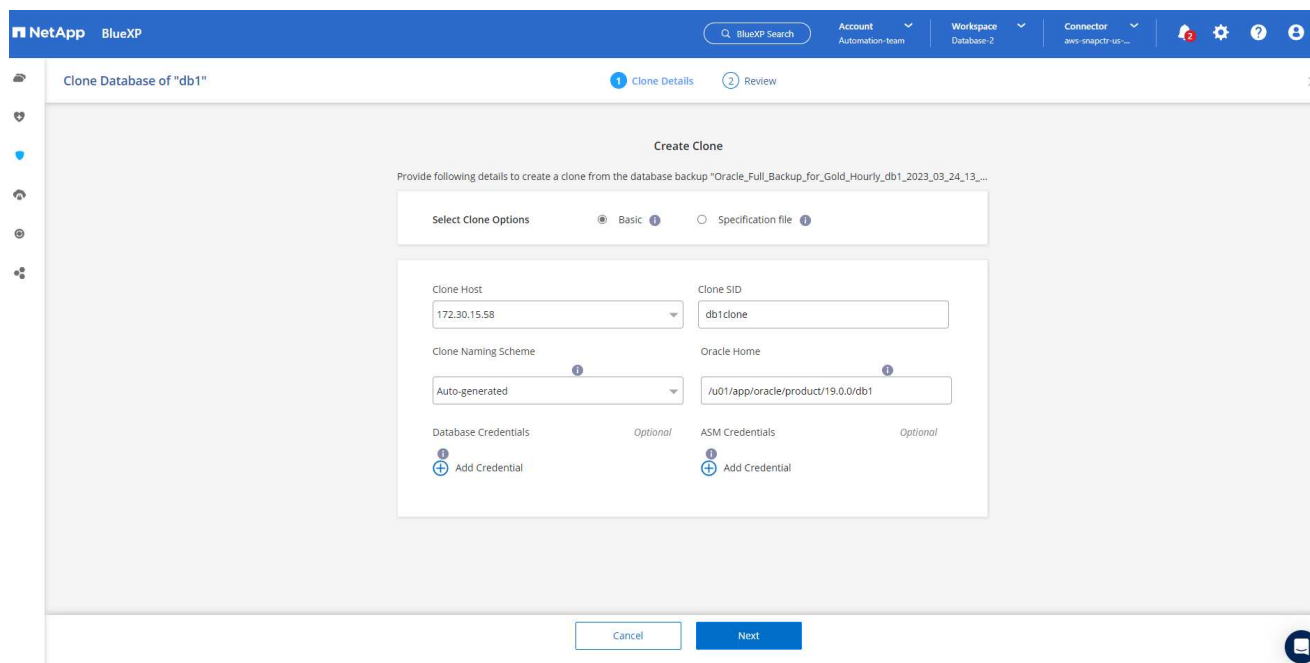
Oracle database clone

To clone a database, launch the clone workflow from the same database backup details page.

1. Select the right database backup copy, click the three dots to view the menu, and choose the **Clone** option.



1. Select the **Basic** option if you don't need to change any cloned database parameters.



1. Alternatively, select **Specification file**, which gives you the option of downloading the current init file, making changes, and then uploading it back to the job.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

1 Clone Details

2 Review

Create Clone

Provide following details to create a clone from the database backup "Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19..."

Select Clone Options

Basic

Specification file

Generate specification file to modify input parameters and use for clone.

Download File

Specification File

db1_3_24_2023_10_14_spec.json

Browse

Clone Host

172.30.15.58

Clone SID

db1clone

Database Credentials

Optional

Add Credential

ASM Credentials

Optional

Add Credential

Cancel

Next

1. Review and launch the job.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

Clone Details

2 Review

Review

General

Database parameters

Backup Name	Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_07_26748_0
Clone SID	db1clone
Clone Host	172.30.15.58
Datafile locations	DATA_db1clone
Control files	+DATA_db1clone/db1clone/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redo/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redo/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redo/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs

Previous

Clone

1. Monitor the cloning job status from the **Job Monitoring** tab.

NetAppBlueXP

BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapc1r18-...

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring > Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Job Details

Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Expand All

Sub-Jobs(2)

Job Name	Job ID	Start Time	End Time	Duration
Cloning Oracle Database db1 as db1clone on h...	cd30abaf-fbe2-4052-a6...	Mar 24 2023, 1:30:36 pm		--
Running pre scripts	51f152c1-853a-4ec6-a4f...	Mar 24 2023, 1:30:41 pm	Mar 24 2023, 1:30:41 pm	0 Second
Validating clone request	f93a6c44-2eb2-4c5e-9f...	Mar 24 2023, 1:30:35 pm	Mar 24 2023, 1:30:42 pm	7 Seconds

1. Validate the cloned database on the EC2 instance host.

```
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
+ASM:/u01/app/oracle/product/19.0.0/grid:N
db1:/u01/app/oracle/product/19.0.0/db1:N
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
db1clone:/u01/app/oracle/product/19.0.0/db1:N
[oracle@ip-172-30-15-58 ~]$ crsctl stat res -t
-----
Name                Target    State        Server                State details
-----
Local Resources
-----
ora.DATA.dg
      ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.DATA_DB1CLONE.dg
      ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.LISTENER.lsnr
      ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.LOGS.dg
      ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.LOGS_SCO_2748138658.dg
      ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.asm
      ONLINE    ONLINE      ip-172-30-15-58      Started,STABLE
ora.ons
      OFFLINE   OFFLINE      ip-172-30-15-58      STABLE
-----
Cluster Resources
-----
ora.cssd
      1          ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.db1.db
      1          ONLINE    ONLINE      ip-172-30-15-58      Open,HOME=/u01/app/o
                        racle/product/19.0.0
                        /db1,STABLE
ora.db1clone.db
      1          ONLINE    ONLINE      ip-172-30-15-58      Open,HOME=/u01/app/o
                        racle/product/19.0.0
                        /db1,STABLE
ora.diskmon
      1          OFFLINE   OFFLINE
ora.driver.afd
      1          ONLINE    ONLINE      ip-172-30-15-58      STABLE
ora.evmd
      1          ONLINE    ONLINE      ip-172-30-15-58      STABLE
-----
[oracle@ip-172-30-15-58 ~]$
```

```
[oracle@ip-172-30-15-58 ~]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
[oracle@ip-172-30-15-58 ~]$ export ORACLE_SID=db1clone
[oracle@ip-172-30-15-58 ~]$ export PATH=$ORACLE_HOME/bin:$PATH
[oracle@ip-172-30-15-58 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 24 18:32:21 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 from v$database;
```

```
NAME          OPEN_MODE
-----
DB1CLONE      READ WRITE
```

```
SQL>
```

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>

- Amazon FSx for NetApp ONTAP

<https://aws.amazon.com/fsx/netapp-ontap/>

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

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.