



# **TR-4964 : Sauvegarde, restauration et clonage de bases de données Oracle avec SnapCenter Services – AWS**

NetApp database solutions

NetApp  
August 18, 2025

# Sommaire

TR-4964 : Sauvegarde, restauration et clonage de bases de données Oracle avec SnapCenter Services – AWS .....	1
But .....	1
Public .....	1
Environnement de test et de validation de solutions .....	1
Architecture .....	2
Composants matériels et logiciels .....	2
Facteurs clés à prendre en compte lors du déploiement .....	3
Déploiement de la solution .....	3
Conditions préalables au déploiement du service SnapCenter .....	3
Préparation à l'intégration de BlueXP .....	4
Déployer un connecteur pour les services SnapCenter .....	5
Définir des informations d'identification dans BlueXP pour l'accès aux ressources AWS .....	12
Configuration des services SnapCenter .....	16
Sauvegarde de la base de données Oracle .....	24
Restauration et récupération de bases de données Oracle .....	28
Clonage de base de données Oracle .....	31
Informations Complémentaires .....	36

# TR-4964 : Sauvegarde, restauration et clonage de bases de données Oracle avec SnapCenter Services – AWS

Cette solution fournit un aperçu et des détails sur la sauvegarde, la restauration et le clonage de la base de données Oracle à l'aide de NetApp SnapCenter SaaS à l'aide de la console BlueXP dans le cloud Azure.

Allen Cao, Niyaz Mohamed, NetApp

## But

SnapCenter Services est la version SaaS de l'outil d'interface utilisateur de gestion de base de données SnapCenter classique disponible via la console de gestion cloud NetApp BlueXP . Il fait partie intégrante de l'offre de sauvegarde et de protection des données dans le cloud NetApp pour les bases de données telles qu'Oracle et HANA exécutées sur le stockage cloud NetApp . Ce service basé sur SaaS simplifie le déploiement traditionnel du serveur autonome SnapCenter qui nécessite généralement un serveur Windows fonctionnant dans un environnement de domaine Windows.

Dans cette documentation, nous montrons comment configurer les services SnapCenter pour sauvegarder, restaurer et cloner des bases de données Oracle déployées sur des instances de stockage Amazon FSx ONTAP et de calcul EC2. Bien qu'il soit beaucoup plus facile à configurer et à utiliser, les services SnapCenter offrent des fonctionnalités clés disponibles dans l'ancien outil d'interface utilisateur SnapCenter .

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde de base de données avec instantanés pour les bases de données Oracle hébergées dans Amazon FSx ONTAP
- Récupération de la base de données Oracle en cas de panne
- Clonage rapide et efficace en termes de stockage de bases de données primaires pour un environnement de développement/test ou d'autres cas d'utilisation

## Public

Cette solution est destinée aux publics suivants :

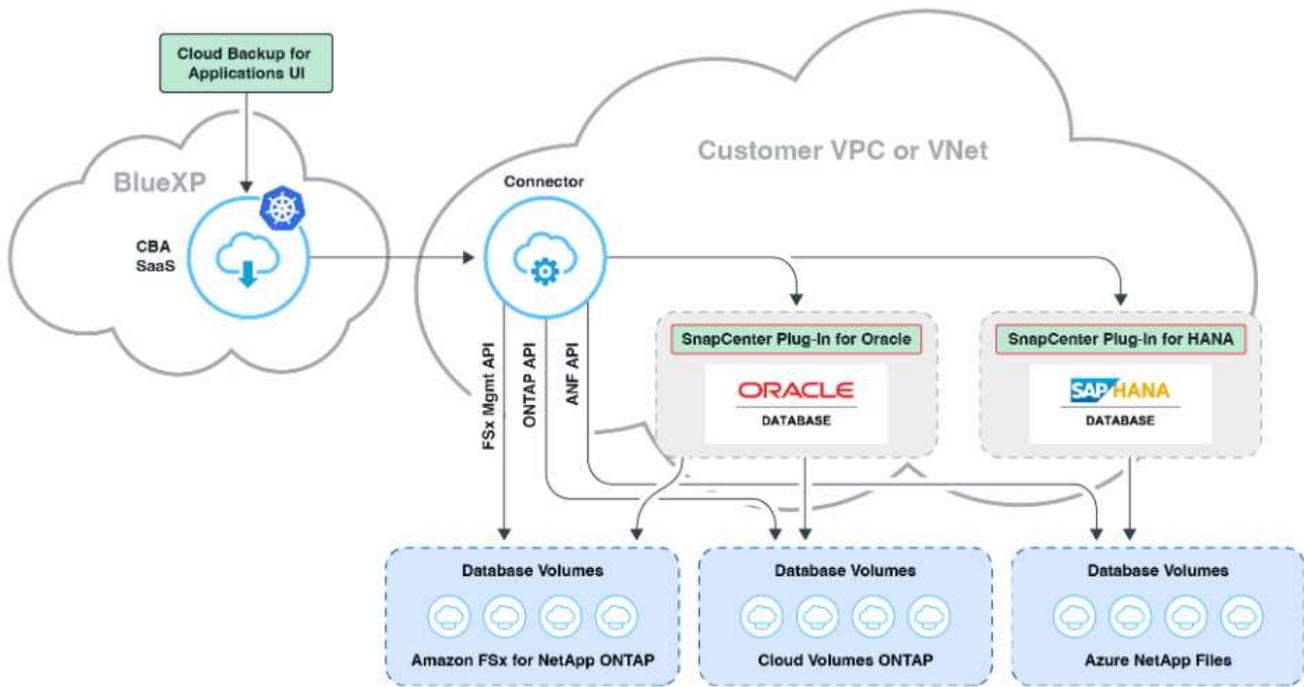
- L'administrateur de base de données qui gère les bases de données Oracle exécutées sur le stockage Amazon FSx ONTAP
- L'architecte de solutions qui souhaite tester la sauvegarde, la restauration et le clonage de bases de données Oracle dans le cloud public AWS
- L'administrateur de stockage qui prend en charge et gère le stockage Amazon FSx ONTAP
- Le propriétaire de l'application qui possède les applications déployées sur le stockage Amazon FSx ONTAP

## Environnement de test et de validation de solutions

Les tests et la validation de cette solution ont été effectués dans un environnement AWS FSx et EC2 qui

pourrait ne pas correspondre à l'environnement de déploiement final. Pour plus d'informations, consultez la section [Facteurs clés à prendre en compte lors du déploiement](#).

## Architecture



Cette image fournit une image détaillée de la BlueXP backup and recovery pour les applications dans la console BlueXP, y compris l'interface utilisateur, le connecteur et les ressources qu'elle gère.

## Composants matériels et logiciels

### Matériel

Stockage FSx ONTAP	Version actuelle proposée par AWS	Un cluster FSx HA dans le même VPC et la même zone de disponibilité
Instance EC2 pour le calcul	t2.xlarge/4vCPU/16G	Deux instances EC2 T2 xlarge EC2, une comme serveur de base de données principal et l'autre comme serveur de base de données clone

### Logiciel

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Abonnement RedHat déployé pour les tests
Infrastructure Oracle Grid	Version 19.18	Patch RU appliqué p34762026_190000_Linux-x86-64.zip

Base de données Oracle	Version 19.18	Patch RU appliqué p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Version 12.2.0.1.36	Dernier correctif p6880880_190000_Linux-x86-64.zip
Service SnapCenter	Version	v2.3.1.2324

## Facteurs clés à prendre en compte lors du déploiement

- **Connecteur à déployer dans le même VPC que la base de données et FSx.** Lorsque cela est possible, le connecteur doit être déployé dans le même VPC AWS, ce qui permet la connectivité au stockage FSx et à l'instance de calcul EC2.
- **Une politique AWS IAM créée pour le connecteur SnapCenter .** La politique au format JSON est disponible dans la documentation détaillée du service SnapCenter . Lorsque vous lancez le déploiement du connecteur avec la console BlueXP , vous êtes également invité à configurer les conditions préalables avec les détails de l'autorisation requise au format JSON. La politique doit être attribuée au compte utilisateur AWS propriétaire du connecteur.
- **La clé d'accès au compte AWS et la paire de clés SSH créées dans le compte AWS.** La paire de clés SSH est attribuée à l'utilisateur ec2 pour se connecter à l'hôte du connecteur, puis déployer un plug-in de base de données sur l'hôte du serveur de base de données EC2. La clé d'accès accorde l'autorisation de provisionner le connecteur requis avec la politique IAM ci-dessus.
- **Un identifiant ajouté au paramètre de la console BlueXP .** Pour ajouter Amazon FSx ONTAP à l'environnement de travail BlueXP , une information d'identification qui accorde à BlueXP des autorisations pour accéder à Amazon FSx ONTAP est configurée dans les paramètres de la console BlueXP .
- **java-11-openjdk installé sur l'hôte de l'instance de base de données EC2.** L'installation du service SnapCenter nécessite la version 11 de Java. Il doit être installé sur l'hôte de l'application avant la tentative de déploiement du plugin.

## Déploiement de la solution

Il existe une documentation NetApp complète avec une portée plus large pour vous aider à protéger vos données d'application cloud natives. L'objectif de cette documentation est de fournir des procédures étape par étape qui couvrent le déploiement du service SnapCenter avec la console BlueXP pour protéger votre base de données Oracle déployée sur Amazon FSx ONTAP et une instance de calcul EC2. Ce document complète certains détails qui pourraient manquer dans des instructions plus générales.

Pour commencer, procédez comme suit :

- Lire les instructions générales "[Protégez les données de vos applications cloud natives](#)" et les sections liées à Oracle et Amazon FSx ONTAP.
- Regardez la présentation vidéo suivante.

### [Déploiement de la solution](#)

## Conditions préalables au déploiement du service SnapCenter

Le déploiement nécessite les prérequis suivants.

1. Un serveur de base de données Oracle principal sur une instance EC2 avec une base de données Oracle entièrement déployée et en cours d'exécution.
2. Un cluster Amazon FSx ONTAP déployé dans AWS qui héberge les volumes de base de données ci-dessus.
3. Un serveur de base de données facultatif sur une instance EC2 qui peut être utilisé pour tester le clonage d'une base de données Oracle sur un hôte alternatif dans le but de prendre en charge une charge de travail de développement/test ou tout cas d'utilisation nécessitant un ensemble de données complet d'une base de données Oracle de production.
4. Si vous avez besoin d'aide pour répondre aux conditions préalables ci-dessus pour le déploiement de la base de données Oracle sur l'instance de calcul Amazon FSx ONTAP et EC2, consultez ["Déploiement et protection de la base de données Oracle dans AWS FSx/EC2 avec iSCSI/ASM"](#) ou livre blanc ["Meilleures pratiques de déploiement de bases de données Oracle sur EC2 et FSx"](#)

## Préparation à l'intégration de BlueXP

1. Utilisez le lien "NetApp BlueXP" pour vous inscrire à l'accès à la console BlueXP .
2. Connectez-vous à votre compte AWS pour créer une politique IAM avec les autorisations appropriées et attribuez la politique au compte AWS qui sera utilisé pour le déploiement du connecteur BlueXP .

The screenshot shows the AWS IAM console interface. On the left is the navigation menu for Identity and Access Management (IAM). The main content area shows the 'Summary' page for a policy named 'snapcenter'. The Policy ARN is 'arn:aws:iam::541696183547:policy/snapcenter'. The Description is 'Policy to grant snapcenter service permission to create connector in AWS.'. Below this are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Policy summary' tab is active, showing a JSON policy document. The JSON document is as follows:

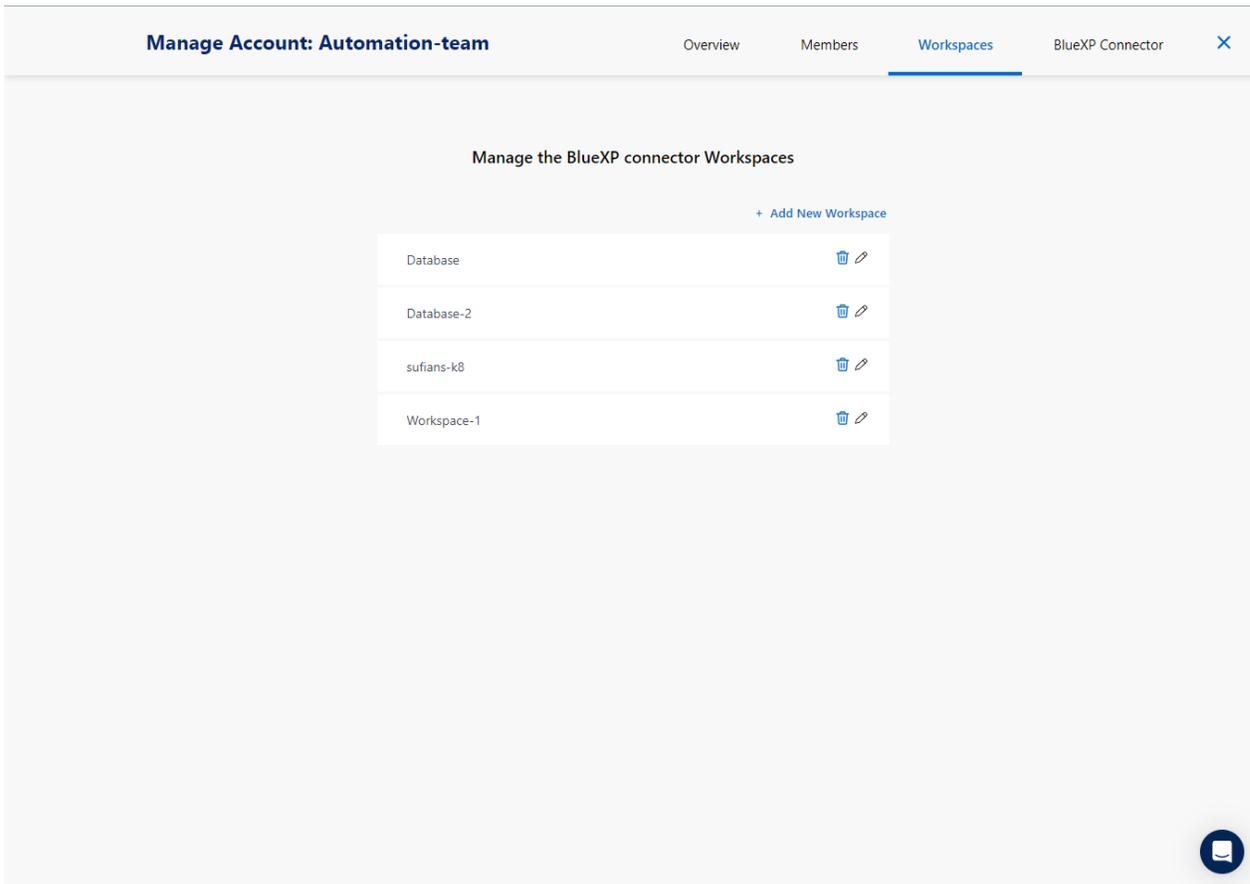
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:DeleteRole",
9         "iam:PutRolePolicy",
10        "iam:CreateInstanceProfile",
11        "iam:DeleteRolePolicy",
12        "iam:AddRoleToInstanceProfile",
13        "iam:RemoveRoleFromInstanceProfile",
14        "iam:DeleteInstanceProfile",
15        "iam:PassRole",
16        "iam:ListRoles",
17        "ec2:DescribeInstanceStatus",
18        "ec2:RunInstances",
19        "ec2:ModifyInstanceAttribute",
20        "ec2:CreateSecurityGroup",
21        "ec2>DeleteSecurityGroup",
22        "ec2:DescribeSecurityGroups",
23        "ec2:RevokeSecurityGroupEgress",
24        "ec2:AuthorizeSecurityGroupEgress",
25        "ec2:AuthorizeSecurityGroupIngress",
26        "ec2:RevokeSecurityGroupIngress",
27        "ec2:CreateNetworkInterface",
28        "ec2:DescribeNetworkInterfaces"
```

La politique doit être configurée avec une chaîne JSON disponible dans la documentation NetApp . La chaîne JSON peut également être récupérée à partir de la page lorsque le provisionnement du connecteur est lancé et que vous êtes invité à attribuer les autorisations préalables.

3. Vous avez également besoin du VPC AWS, du sous-réseau, du groupe de sécurité, d'une clé d'accès et de secrets de compte utilisateur AWS, d'une clé SSH pour ec2-user, etc., prêts pour le provisionnement du connecteur.

## Déployer un connecteur pour les services SnapCenter

1. Connectez-vous à la console BlueXP . Pour un compte partagé, il est recommandé de créer un espace de travail individuel en cliquant sur **Compte > Gérer le compte > Espace de travail** pour ajouter un nouvel espace de travail.



2. Cliquez sur **Ajouter un connecteur** pour lancer le workflow de provisionnement du connecteur.

1. Choisissez votre fournisseur cloud (dans ce cas, **Amazon Web Services**).

1. Ignorez les étapes **Autorisation**, **Authentification** et **Mise en réseau** si vous les avez déjà configurées dans votre compte AWS. Sinon, vous devez les configurer avant de continuer. À partir de là, vous pouvez également récupérer les autorisations pour la politique AWS référencée dans la

section précédente "Préparation à l'intégration de BlueXP . "

## Add Connector - AWS



### 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. Saisissez l'authentification de votre compte AWS avec **Clé d'accès** et **Clé secrète**.

- 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  
AKIA6JRXA6ZVGVFUSHMO3

AWS Secret Key  
.....

Want to launch an instance without AWS Credentials? v

Previous

Next



2. Nommez l'instance du connecteur et sélectionnez **Créer un rôle** sous **Détails**.

- 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

+ Add Tags to Connector Instance

Role Name  
Cloud-Manager-Operator-VZzSSP9-SnapCenter

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

Previous

Next



1. Configurez la mise en réseau avec la paire de clés **VPC**, **Sous-réseau** et SSH appropriée pour l'accès au connecteur.

### 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. Définissez le **Groupe de sécurité** pour le connecteur.

 AWS Credentials  Details  Network ** Security Group**  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. Consultez la page récapitulative et cliquez sur **Ajouter** pour démarrer la création du connecteur. Le déploiement prend généralement environ 10 minutes. Une fois terminée, l'instance du connecteur apparaît dans le tableau de bord AWS EC2.

**Add BlueXP Connector - AWS** More Information ×

✓ AWS Credentials ✓ Details ✓ Network ✓ Security Group 5 Review

### Review

[Code for Terraform Automation](#)

BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAH4H43ZT5GIWWR3TI
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 

## Définir des informations d'identification dans BlueXP pour l'accès aux ressources AWS

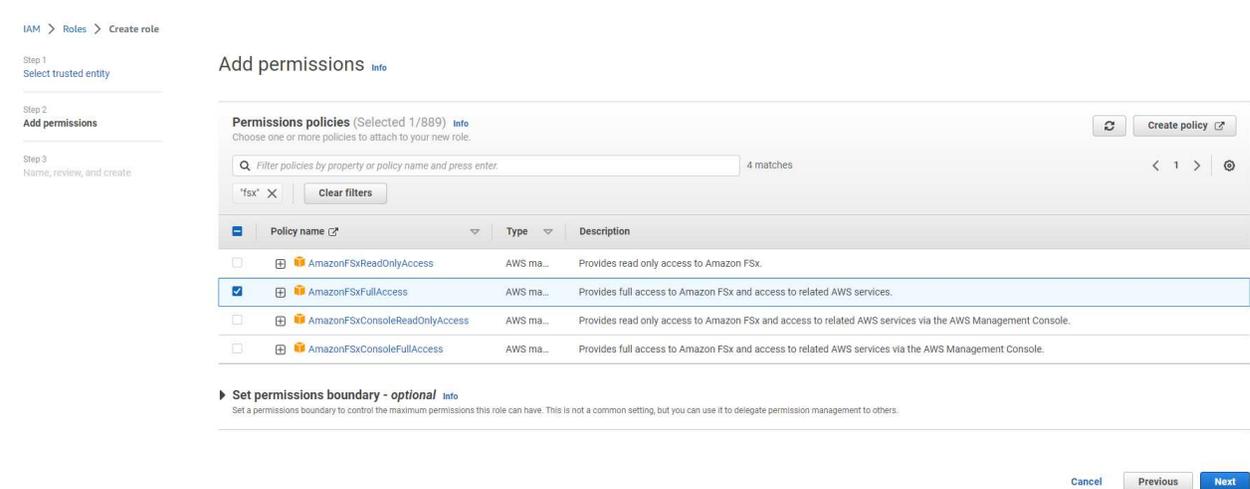
1. Tout d'abord, à partir de la console AWS EC2, créez un rôle dans le menu **Identity and Access Management (IAM) Rôles**, **Créer un rôle** pour démarrer le flux de travail de création de rôle.

The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains navigation options like 'Dashboard', 'Access management', 'Users', 'Policies', and 'Access reports'. The main content area displays a list of roles with columns for 'Role name', 'Trusted entities', and 'Last activity'. The roles listed include various AWS service roles and custom roles.

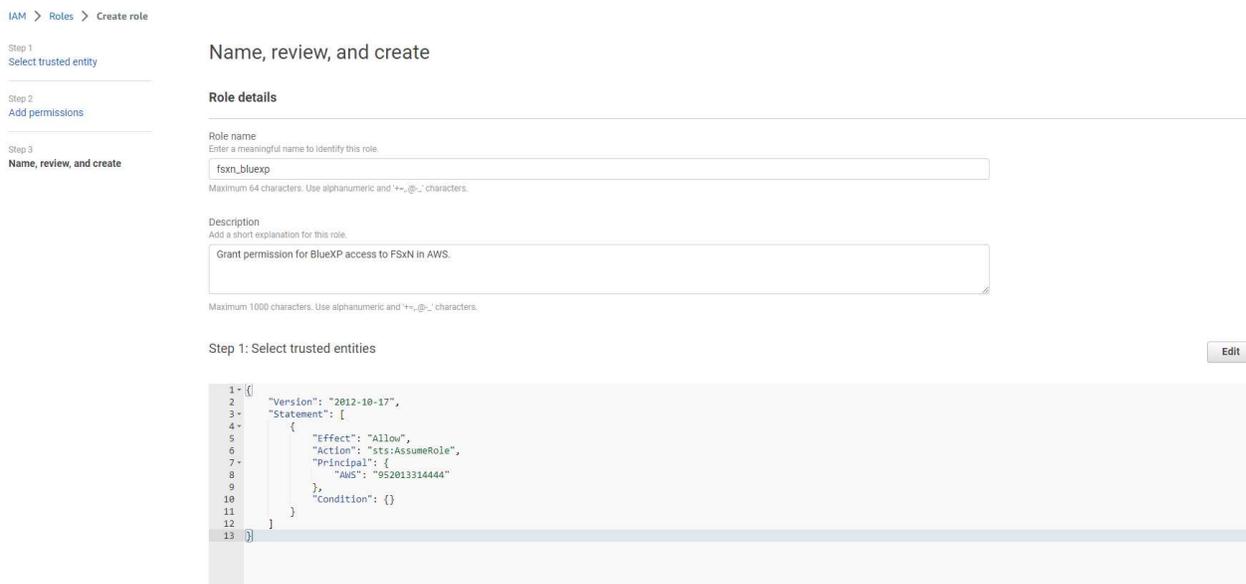
2. Dans la page **Sélectionner une entité de confiance**, choisissez **Compte AWS, Un autre compte AWS** et collez l'ID de compte BlueXP , qui peut être récupéré à partir de la console BlueXP .

The screenshot shows the 'Create role' wizard in the AWS IAM console, specifically the 'Select trusted entity' step. The 'Trusted entity type' section has 'AWS account' selected. Under 'An AWS account', the 'Another AWS account' option is chosen, and the 'Account ID' field is populated with '952013314444'. The 'Options' section includes checkboxes for 'Require external ID', 'Require MFA', and 'Require MFA'.

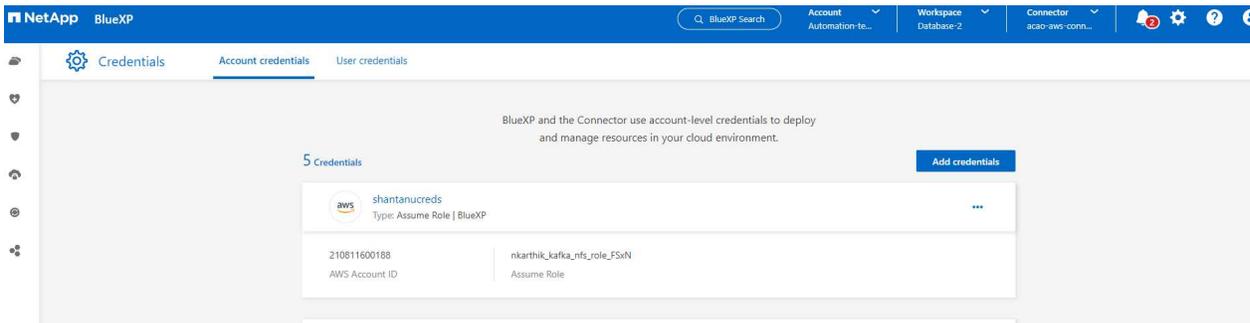
3. Filtrez les politiques d'autorisation par fsx et ajoutez des **politiques d'autorisation** au rôle.



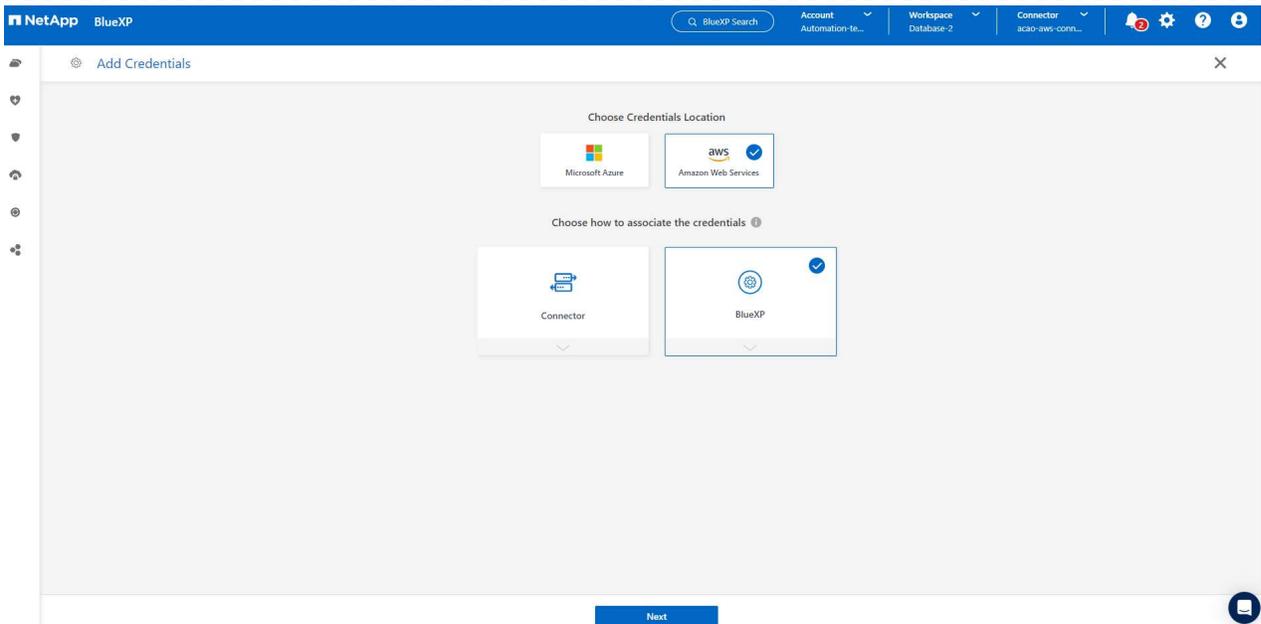
4. Dans la page **Détails du rôle**, nommez le rôle, ajoutez une description, puis cliquez sur **Créer un rôle**.



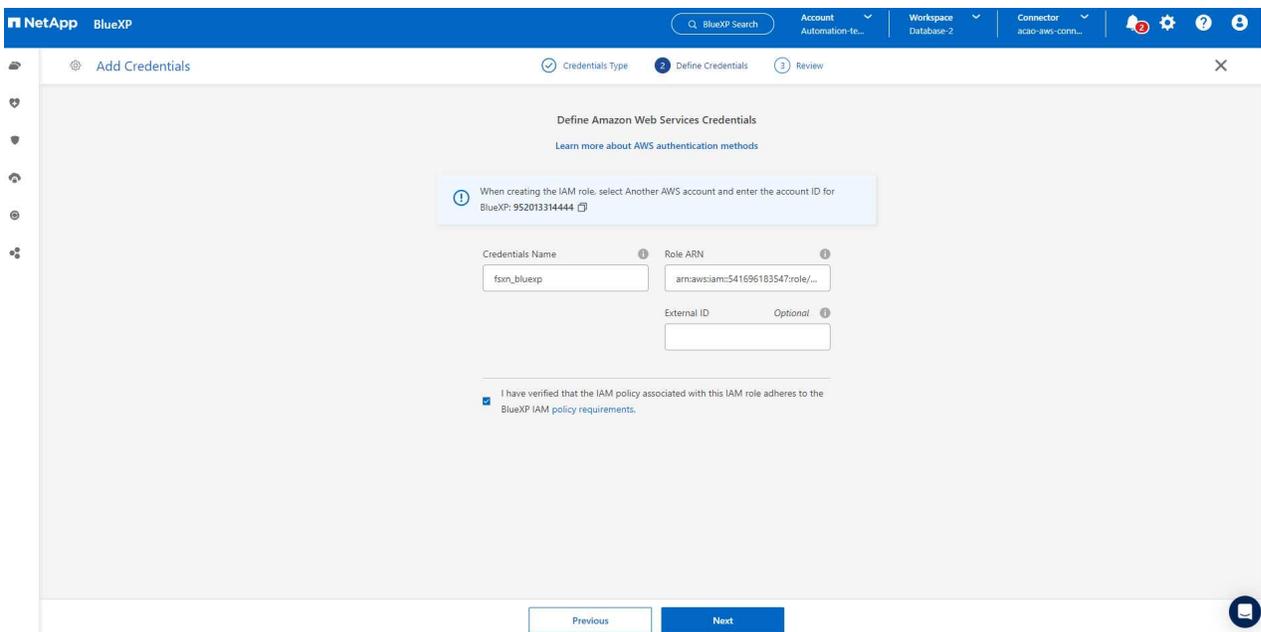
5. De retour à la console BlueXP, cliquez sur l'icône de configuration dans le coin supérieur droit de la console pour ouvrir la page **Informations d'identification du compte**, cliquez sur **Ajouter des informations d'identification** pour démarrer le flux de travail de configuration des informations d'identification.



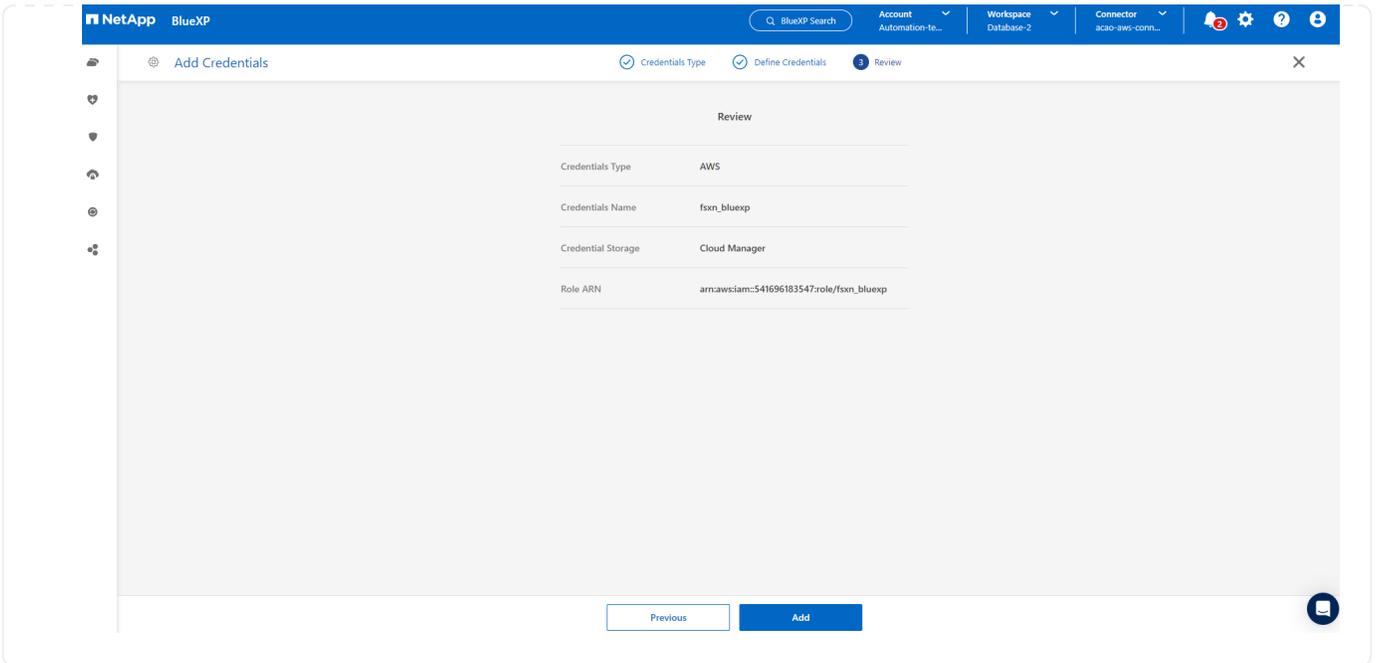
6. Choisissez l'emplacement des informations d'identification comme - **Amazon Web Services - BlueXP**.



7. Définissez les informations d'identification AWS avec le **Role ARN** approprié, qui peut être récupéré à partir du rôle AWS IAM créé à l'étape 1 ci-dessus. BlueXP ID de compte, qui est utilisé pour créer le rôle AWS IAM à la première étape.



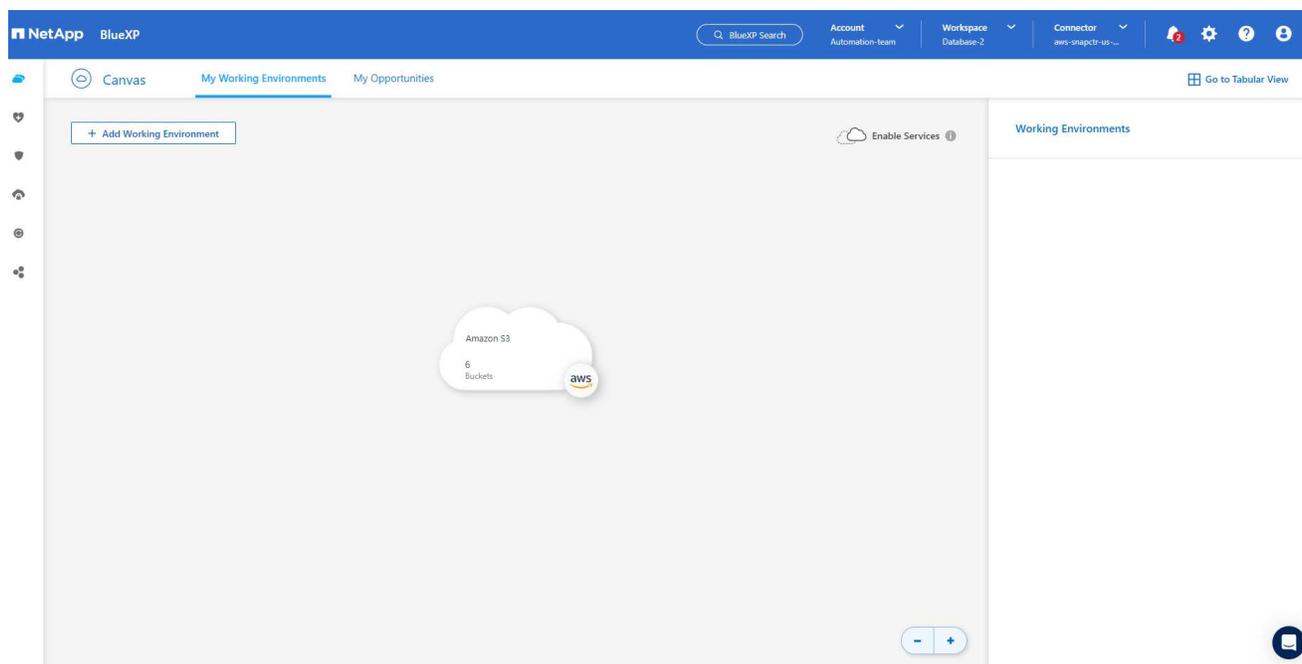
8. Réviser et **Ajouter**



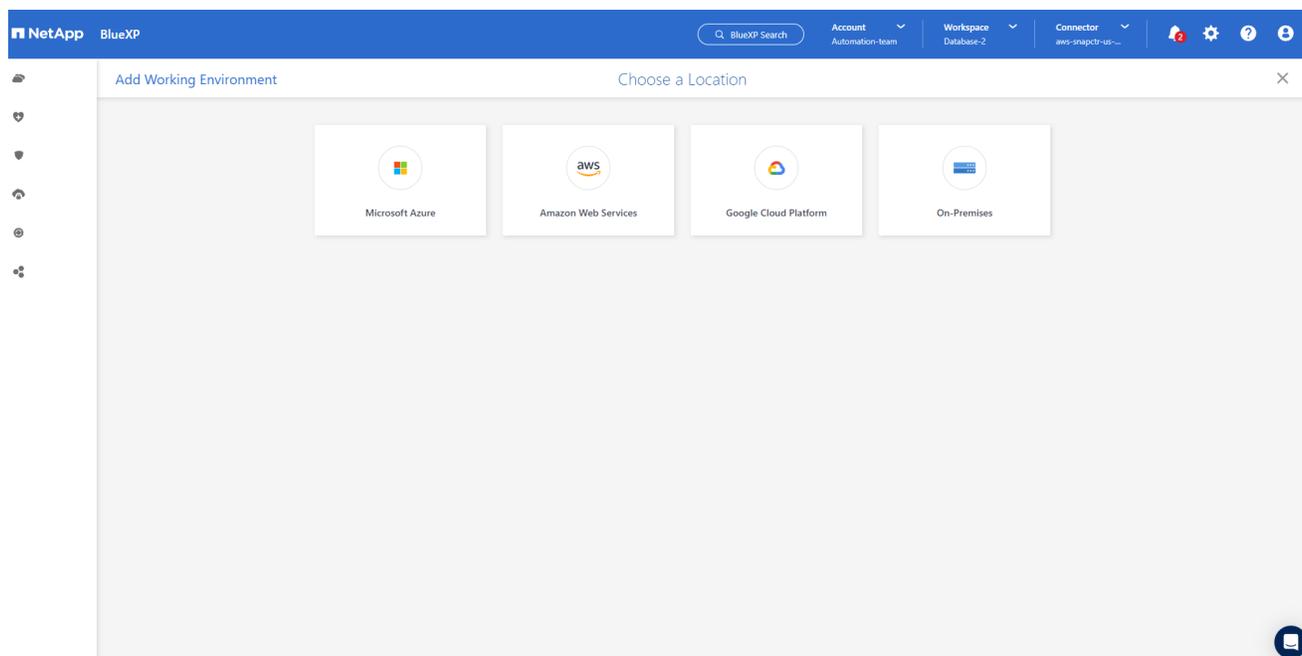
## Configuration des services SnapCenter

Une fois le connecteur déployé et les informations d'identification ajoutées, les services SnapCenter peuvent désormais être configurés avec la procédure suivante :

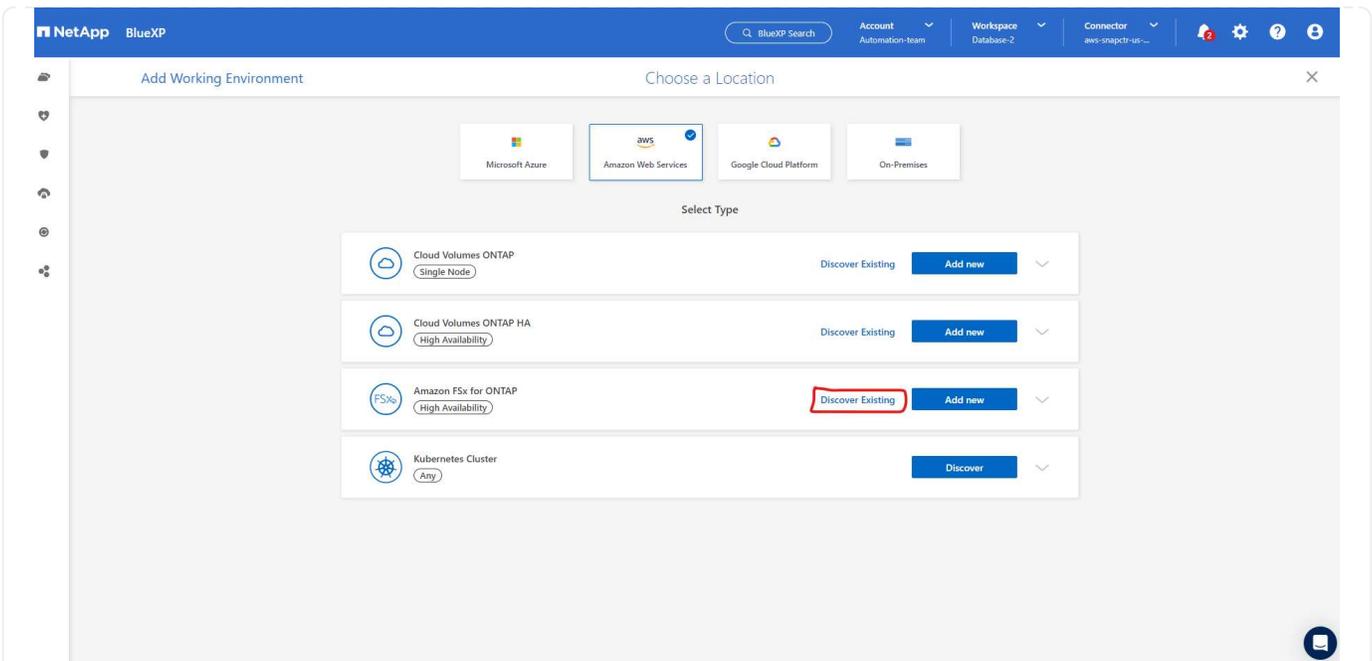
1. Depuis **Mon environnement de travail**, cliquez sur **Ajouter un environnement de travail** pour découvrir FSx déployé dans AWS.



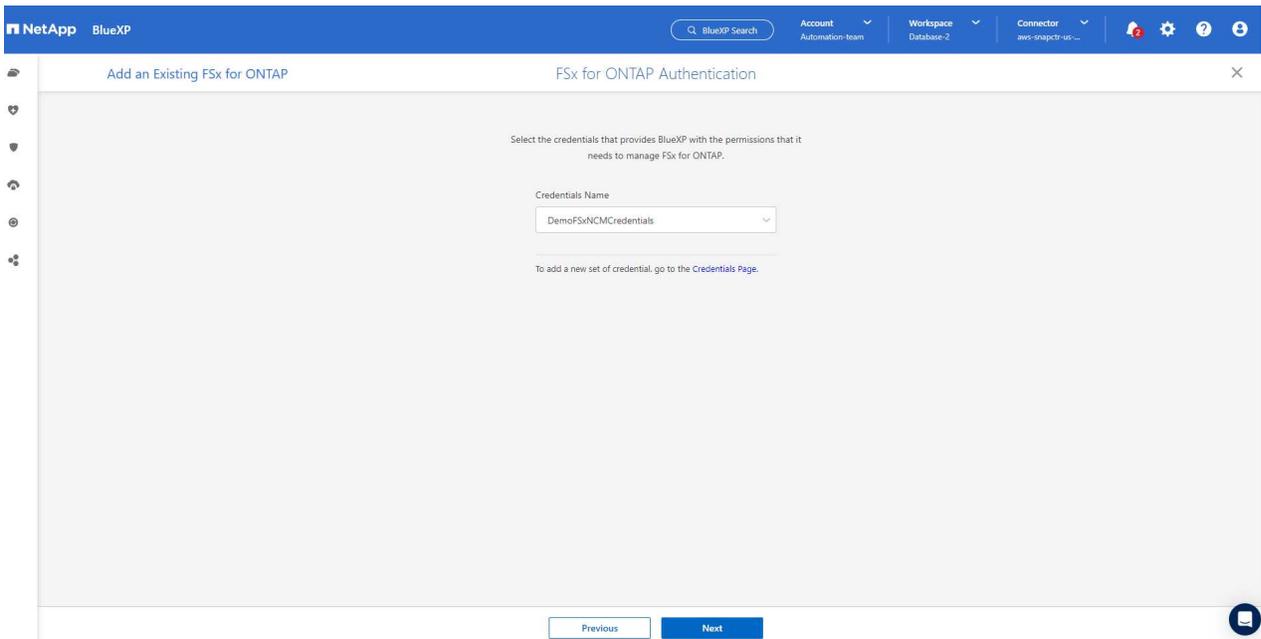
1. Choisissez **Amazon Web Services** comme emplacement.



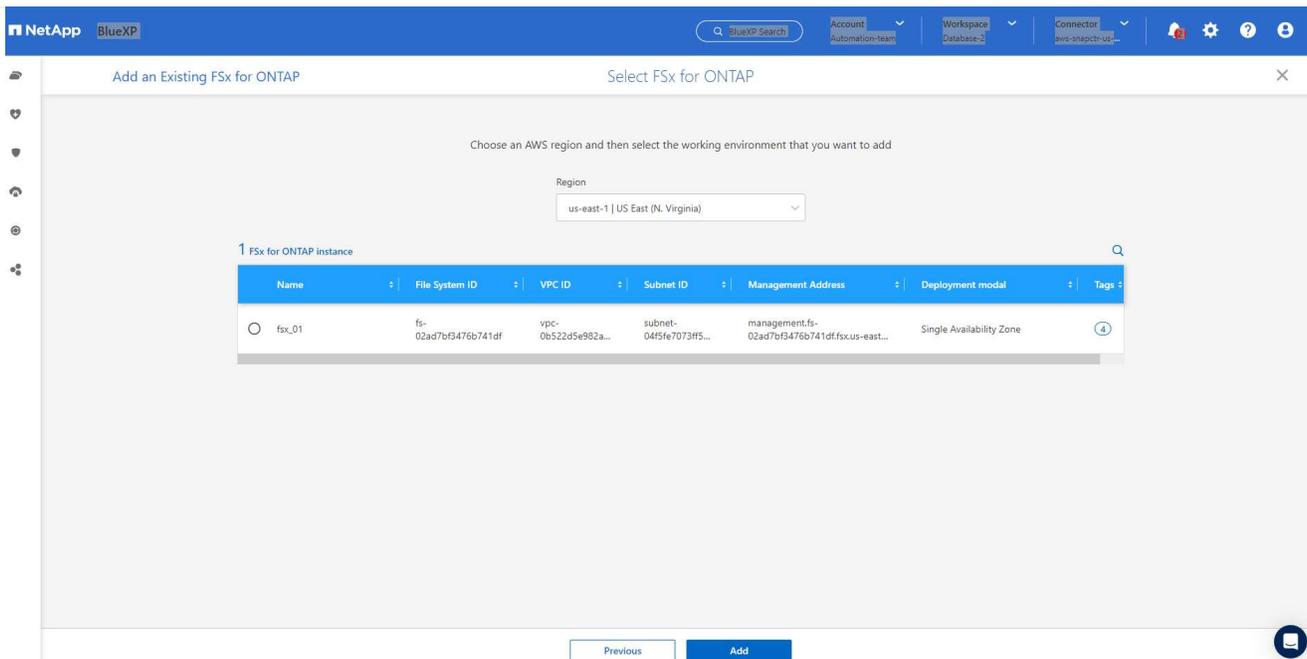
1. Cliquez sur **Découvrir l'existant** à côté de \* Amazon FSx ONTAP\*.



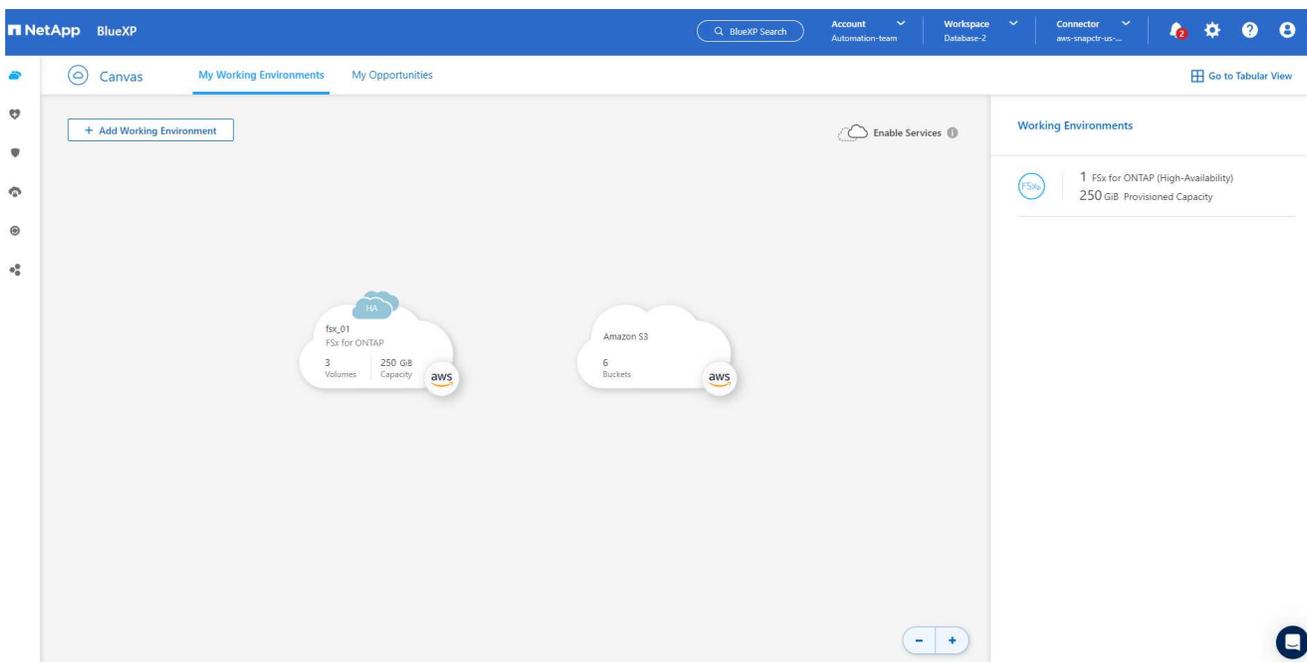
1. Sélectionnez le **Nom des informations d'identification** que vous avez créé dans la section précédente pour accorder à BlueXP les autorisations dont il a besoin pour gérer FSx ONTAP. Si vous n'avez pas ajouté d'informations d'identification, vous pouvez les ajouter à partir du menu **Paramètres** dans le coin supérieur droit de la console BlueXP .



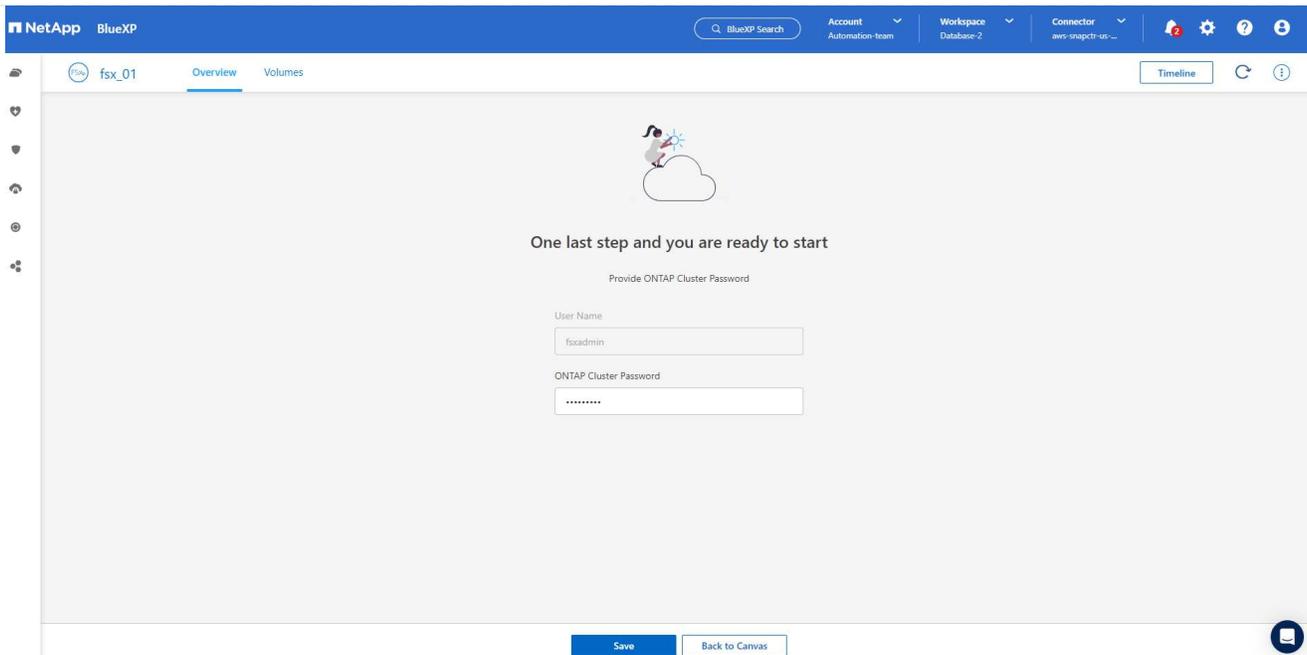
2. Choisissez la région AWS dans laquelle Amazon FSx ONTAP est déployé, sélectionnez le cluster FSx qui héberge la base de données Oracle et cliquez sur Ajouter.



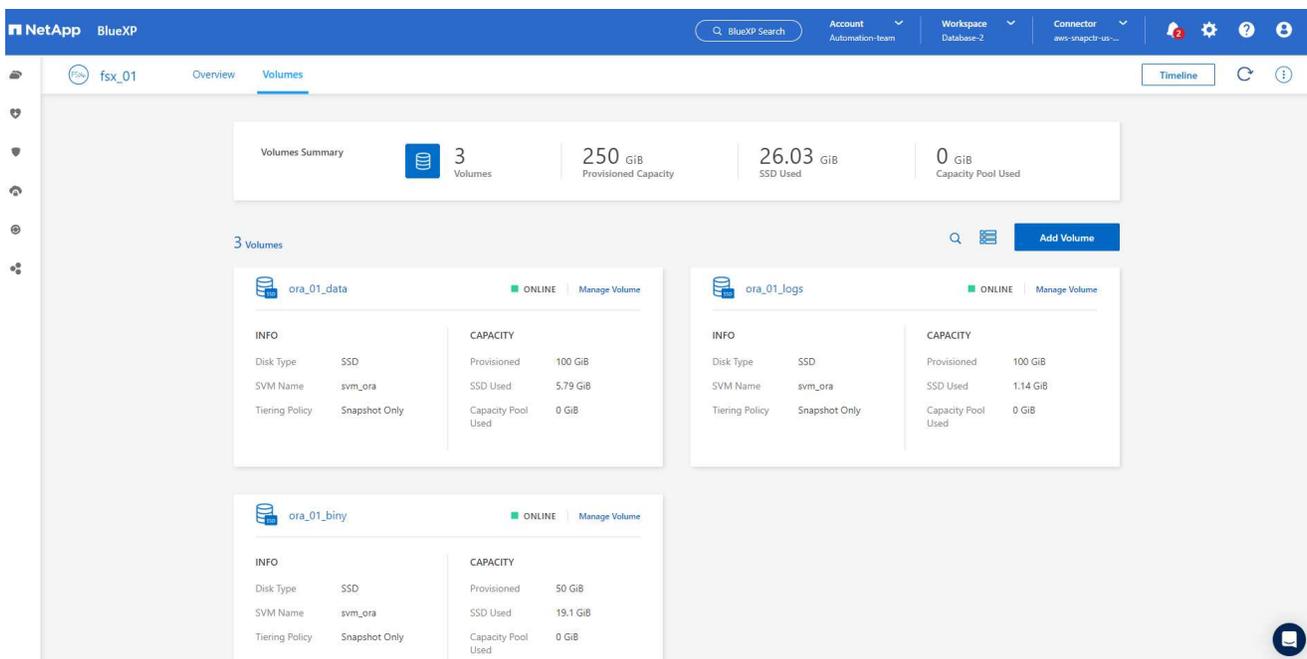
1. L'instance Amazon FSx ONTAP découverte apparaît désormais dans l'environnement de travail.



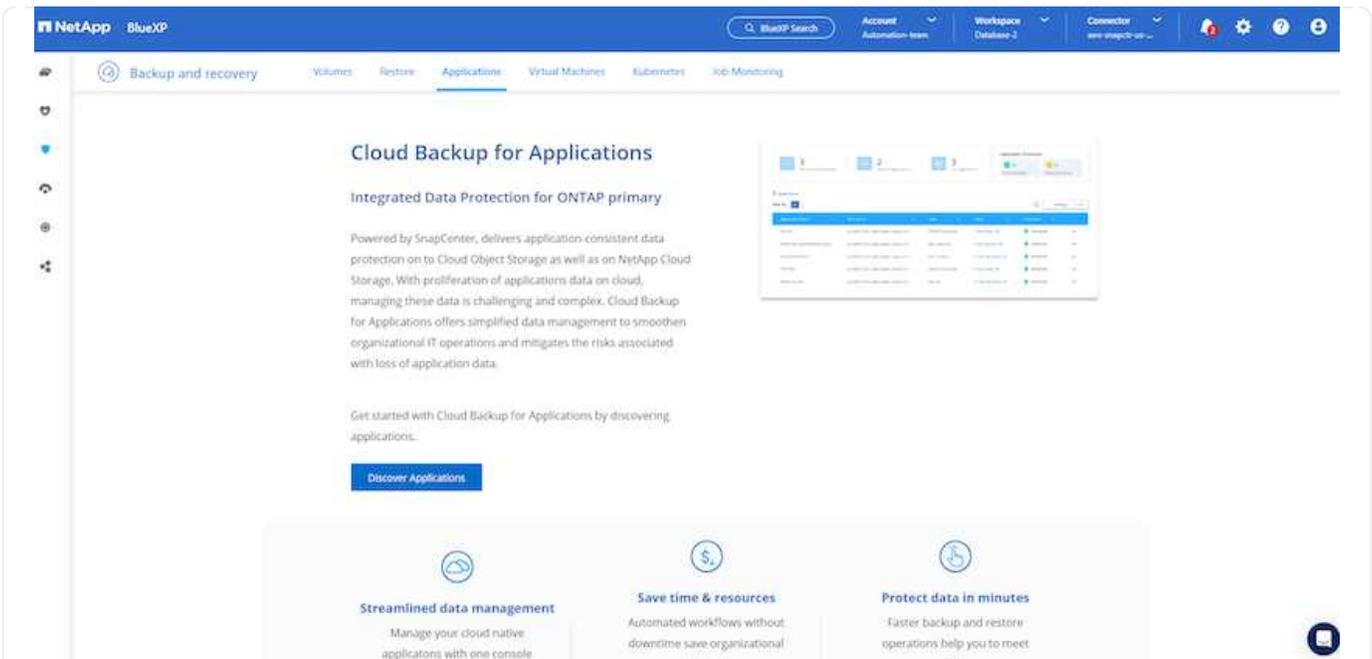
1. Vous pouvez vous connecter au cluster FSx avec les informations d'identification de votre compte fsxadmin.



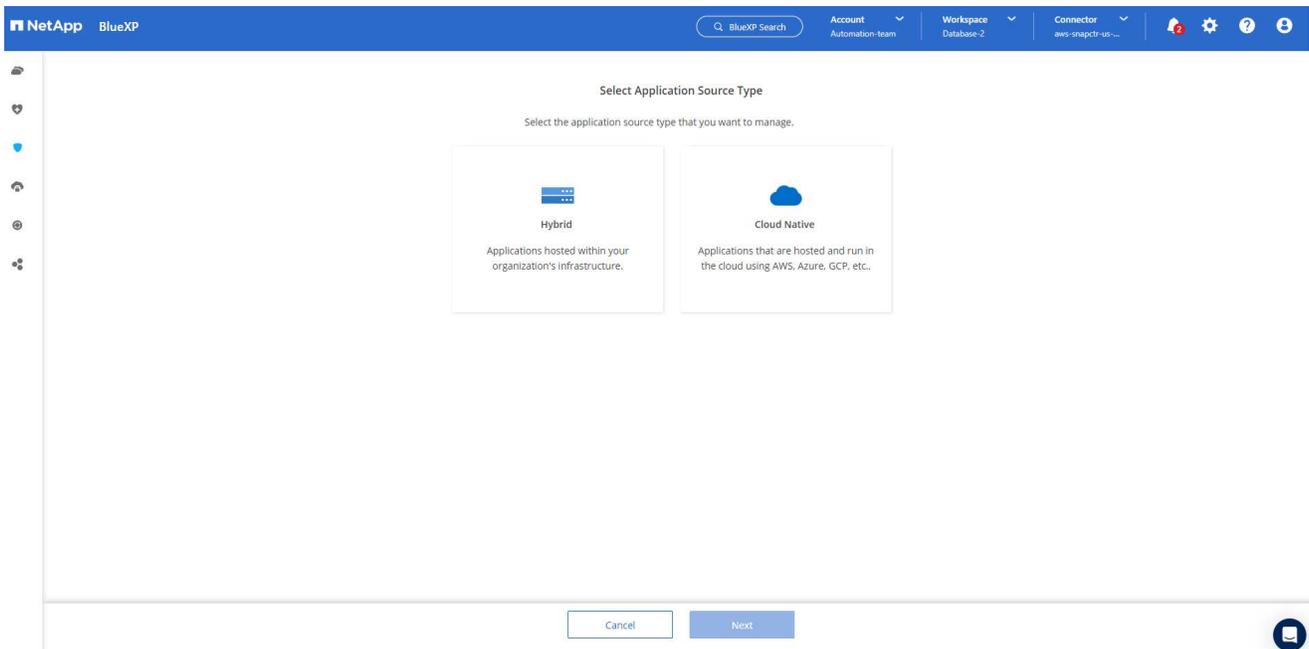
1. Après vous être connecté à Amazon FSx ONTAP, vérifiez les informations de stockage de votre base de données (telles que les volumes de base de données).



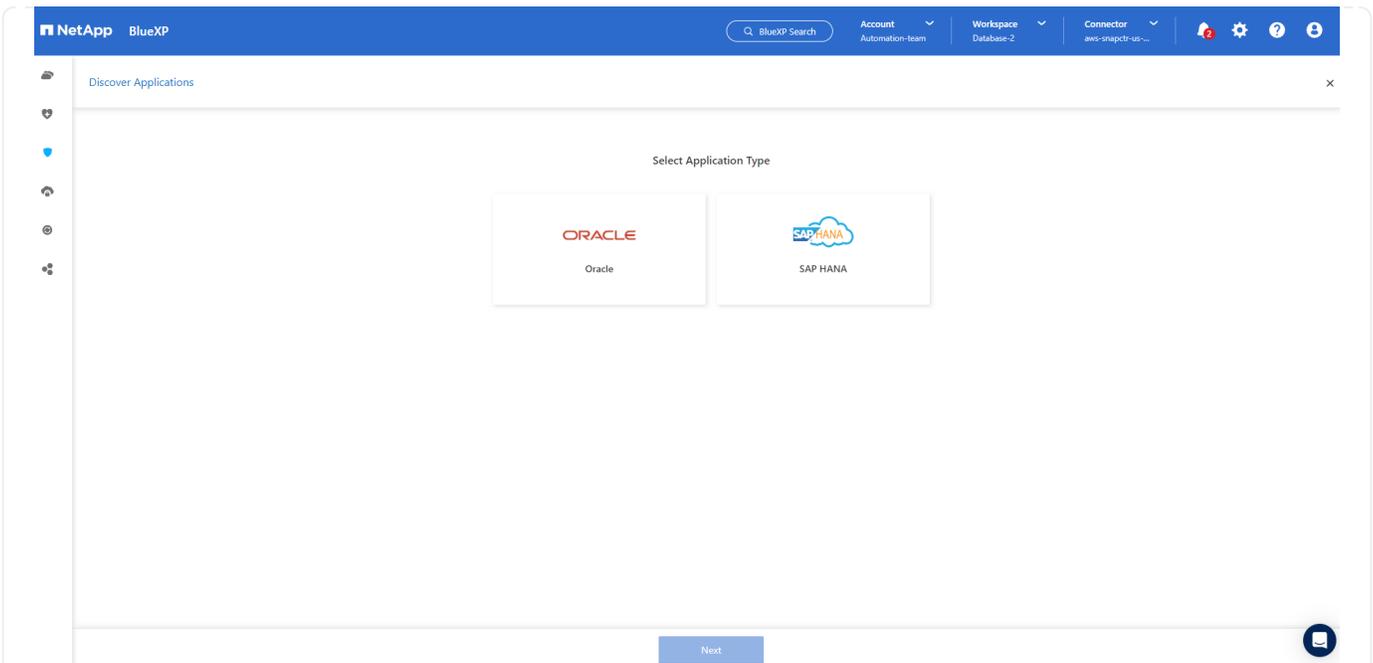
1. Dans la barre latérale gauche de la console, passez votre souris sur l'icône de protection, puis cliquez sur **Protection > Applications** pour ouvrir la page de lancement des applications. Cliquez sur **Découvrir les applications**.



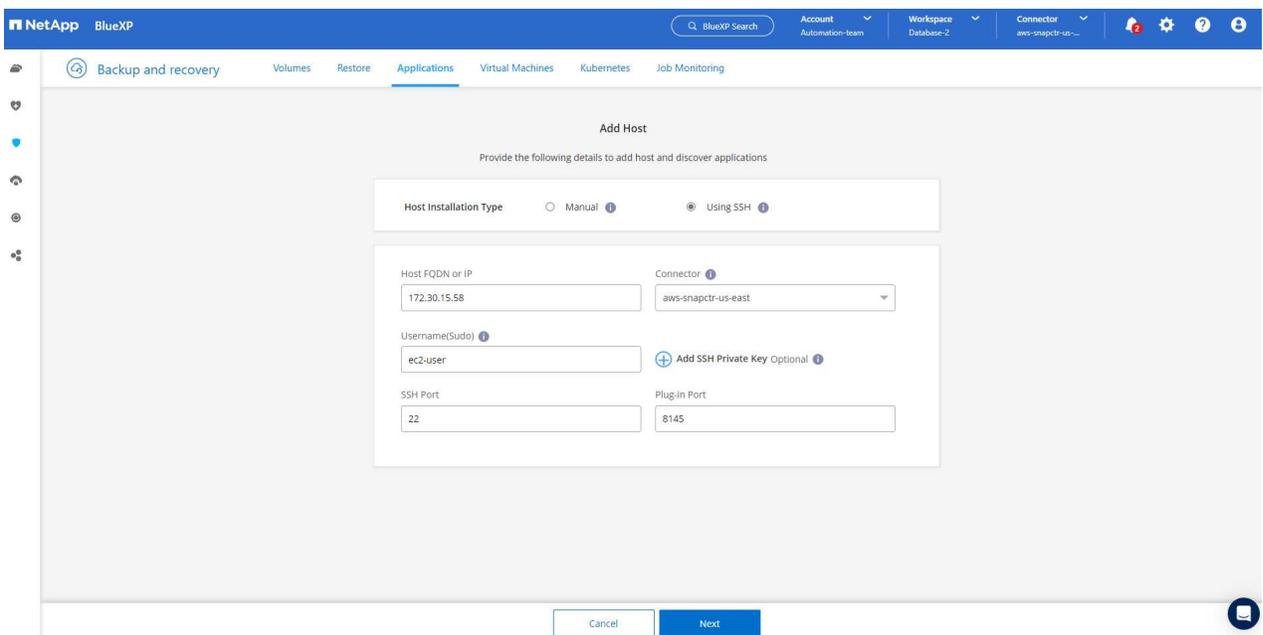
1. Sélectionnez **Cloud Native** comme type de source d'application.



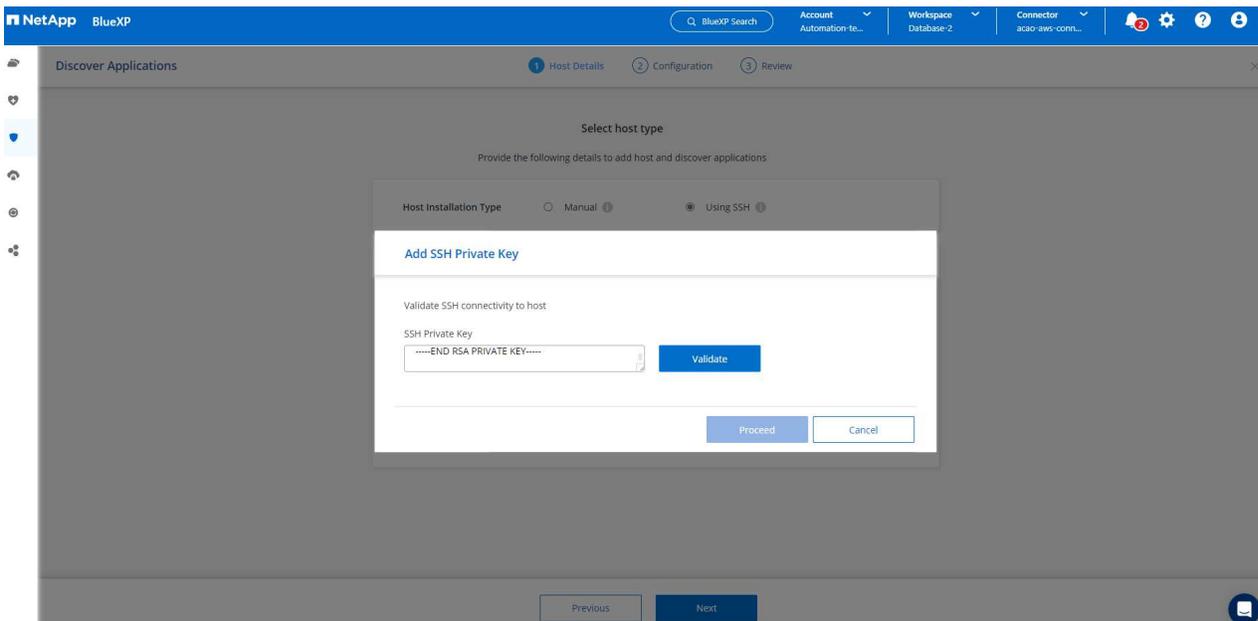
1. Choisissez **Oracle** comme type d'application.



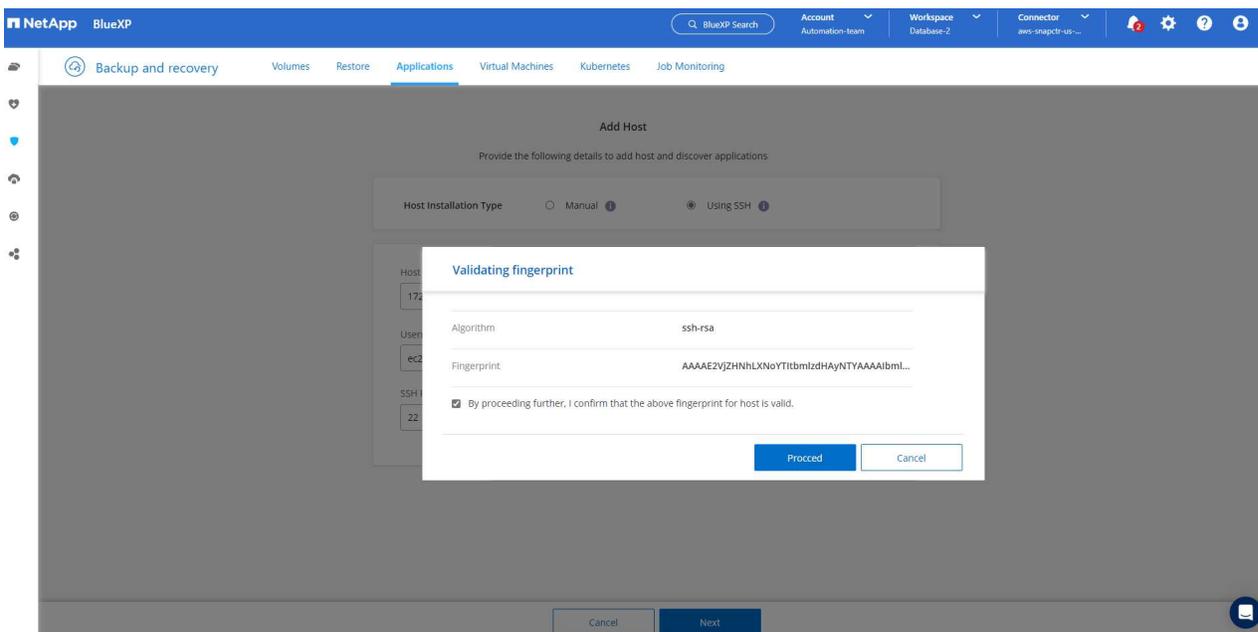
1. Remplissez les détails de l'hôte de l'application Oracle AWS EC2. Choisissez **Utilisation de SSH** comme **Type d'installation de l'hôte** pour l'installation du plug-in en une étape et la découverte de la base de données. Ensuite, cliquez sur **Ajouter une clé privée SSH**.



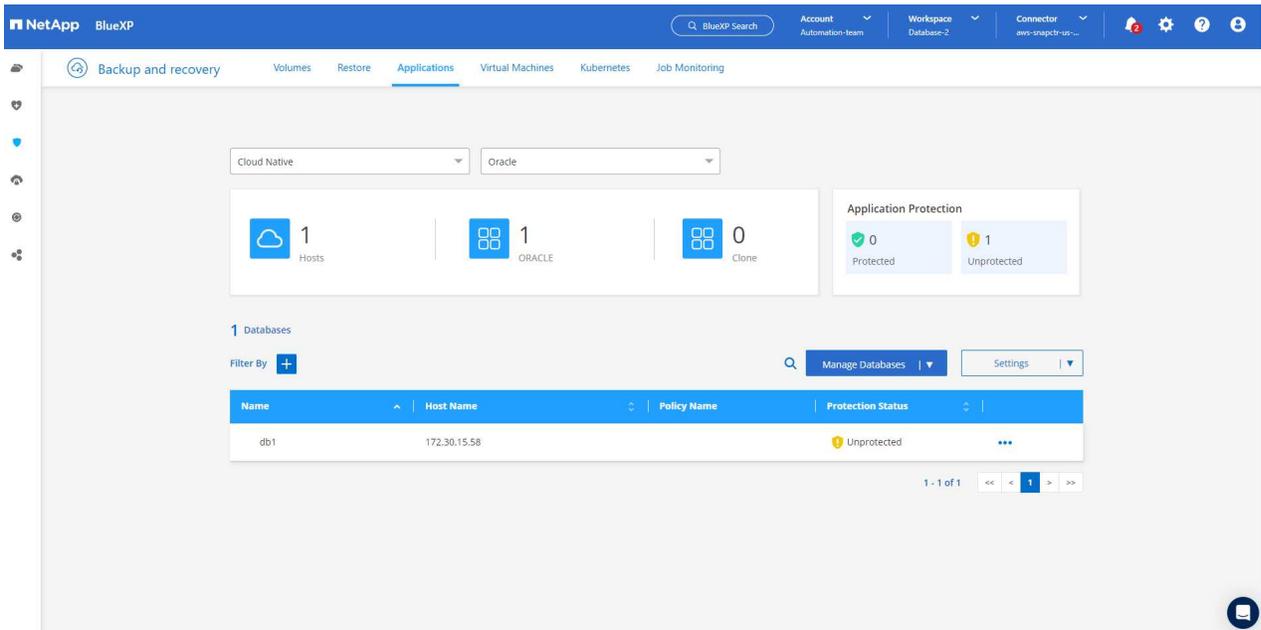
2. Collez votre clé SSH ec2-user pour l'hôte EC2 de la base de données et cliquez sur **Valider** pour continuer.



3. Vous serez invité à **Valider l'empreinte digitale** pour continuer.



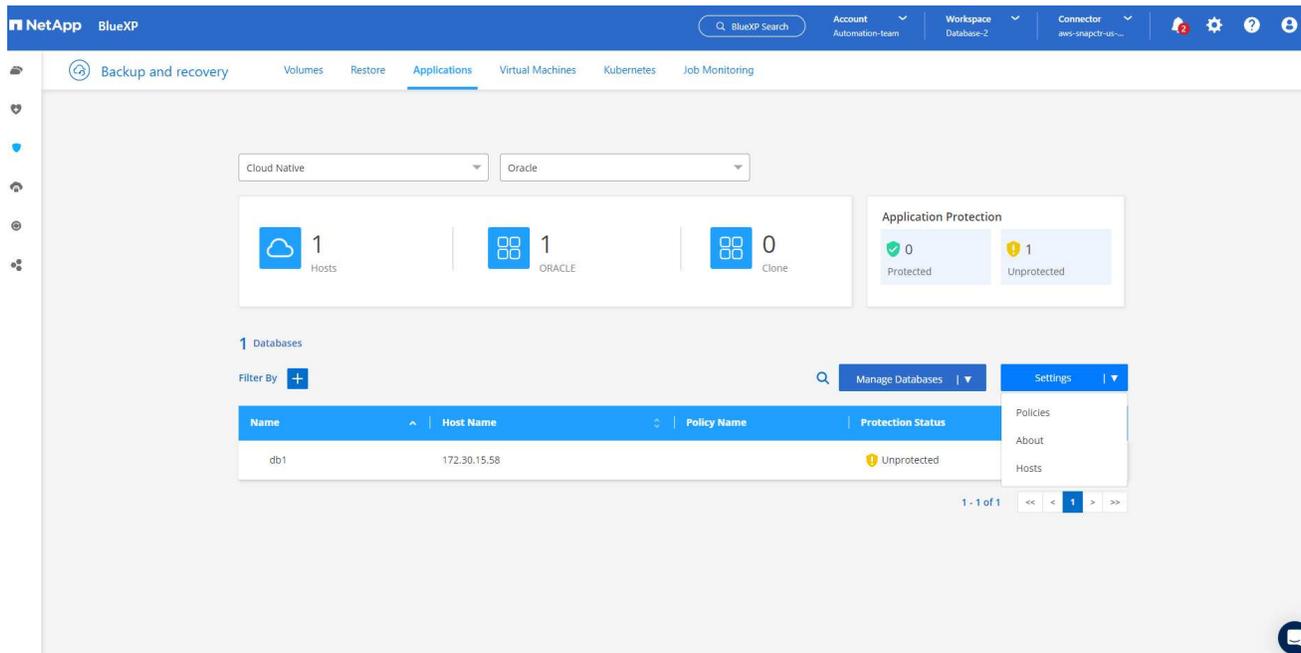
4. Cliquez sur **Suivant** pour installer un plugin de base de données Oracle et découvrir les bases de données Oracle sur l'hôte EC2. Les bases de données découvertes sont ajoutées aux **Applications**. La base de données **État de protection** s'affiche comme **Non protégée** lors de sa découverte initiale.



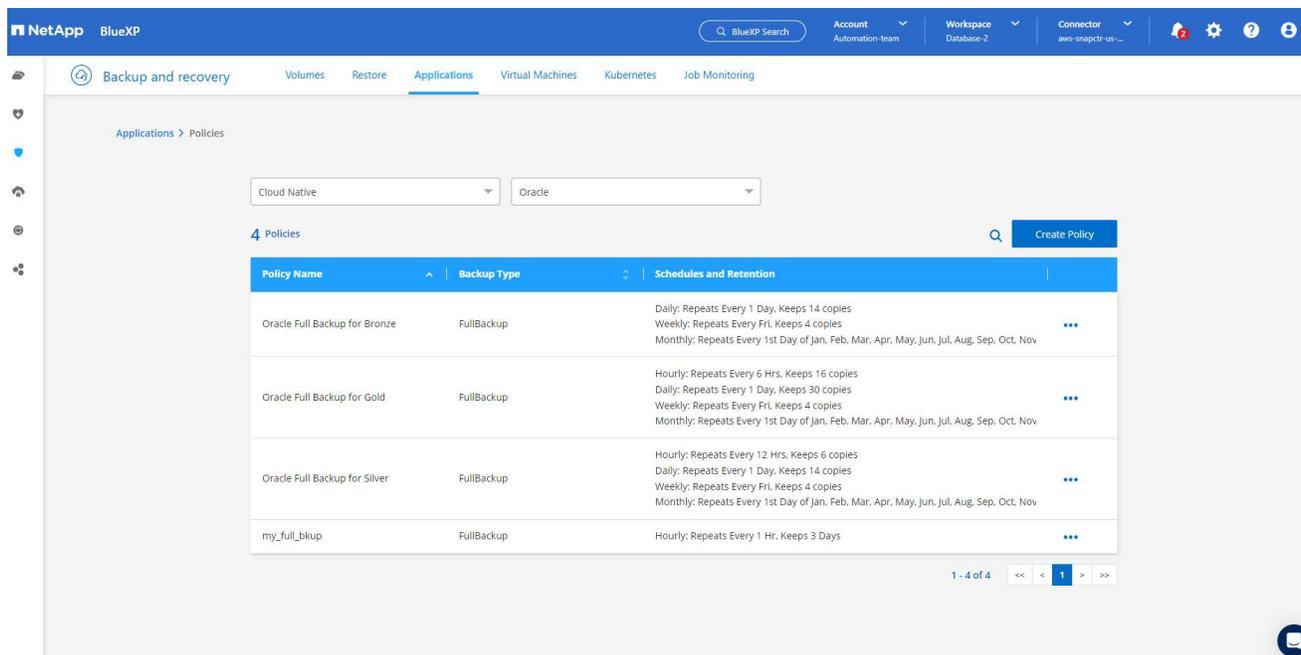
Ceci termine la configuration initiale des services SnapCenter pour Oracle. Les trois sections suivantes de ce document décrivent les opérations de sauvegarde, de restauration et de clonage de la base de données Oracle.

## Sauvegarde de la base de données Oracle

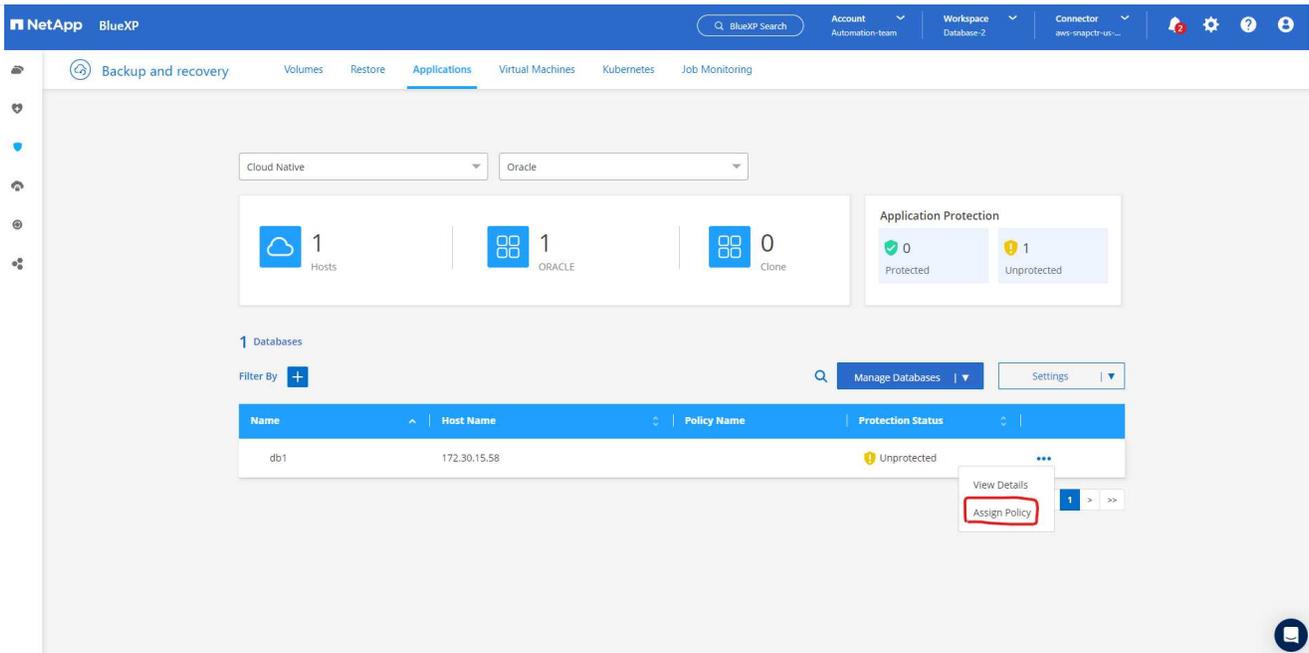
1. Cliquez sur les trois points à côté de l'état de protection de la base de données, puis cliquez sur **Stratégies** pour afficher les stratégies de protection de base de données préchargées par défaut qui peuvent être appliquées pour protéger vos bases de données Oracle.



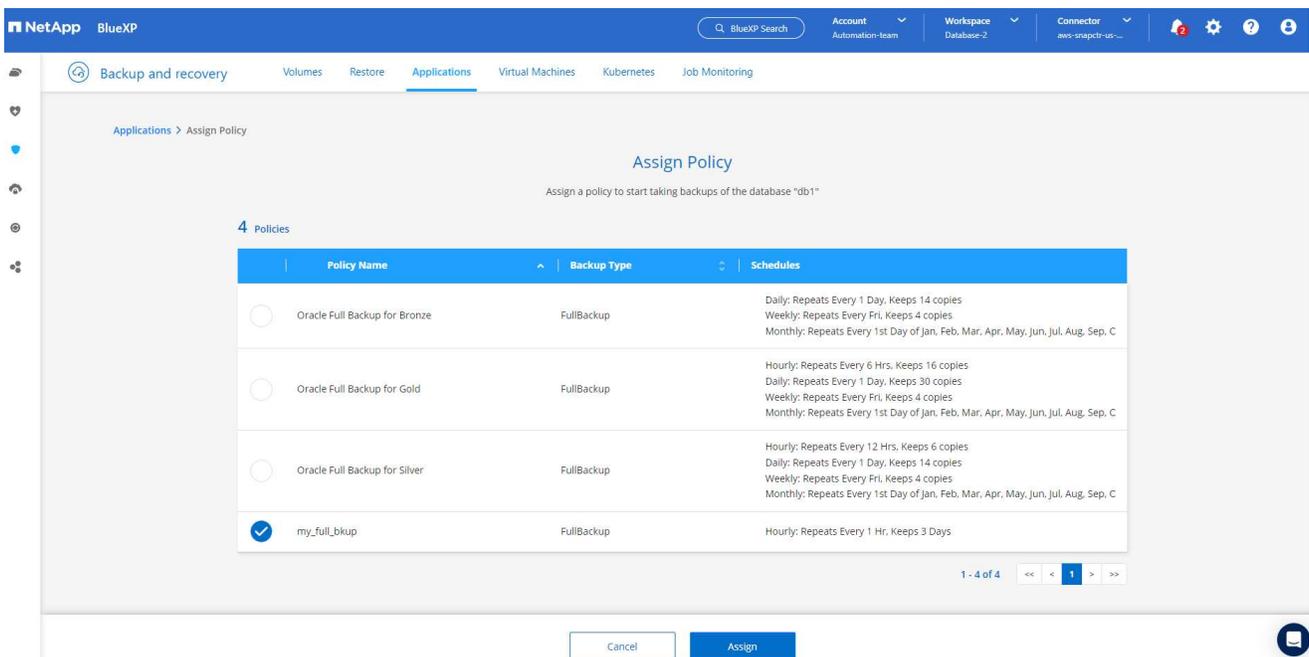
1. Vous pouvez également créer votre propre politique avec une fréquence de sauvegarde personnalisée et une fenêtre de conservation des données de sauvegarde.



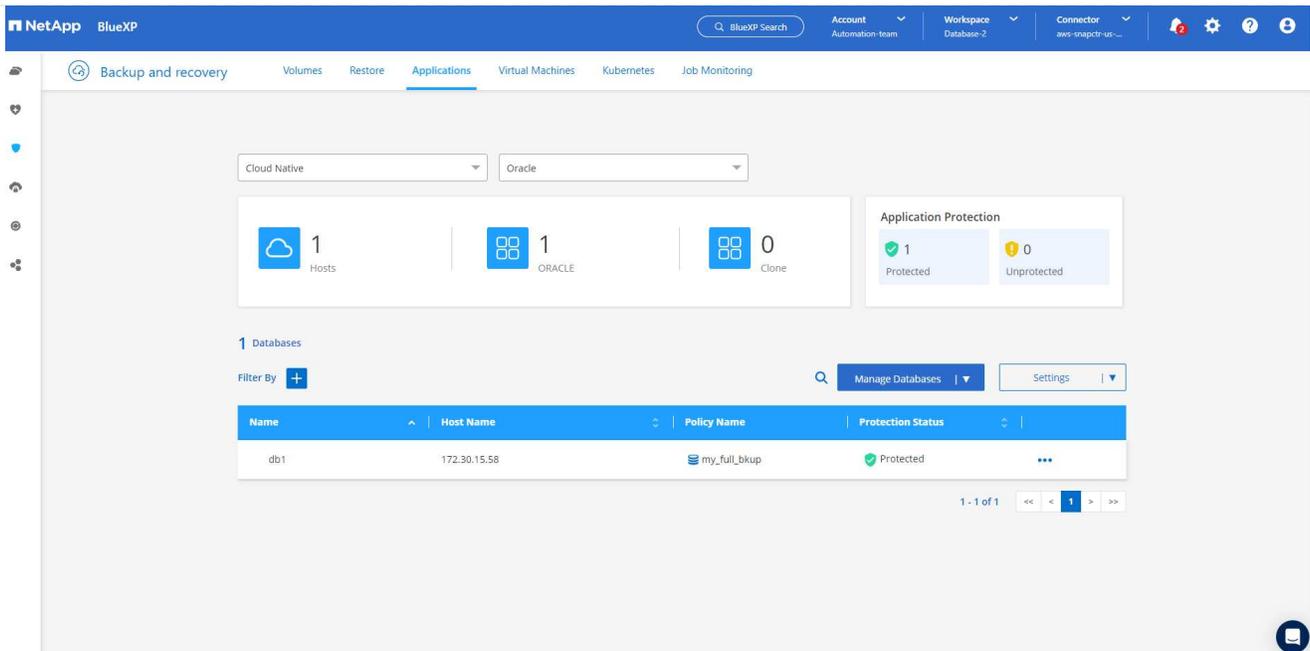
1. Lorsque vous êtes satisfait de la configuration de la politique, vous pouvez ensuite attribuer la politique de votre choix pour protéger la base de données.



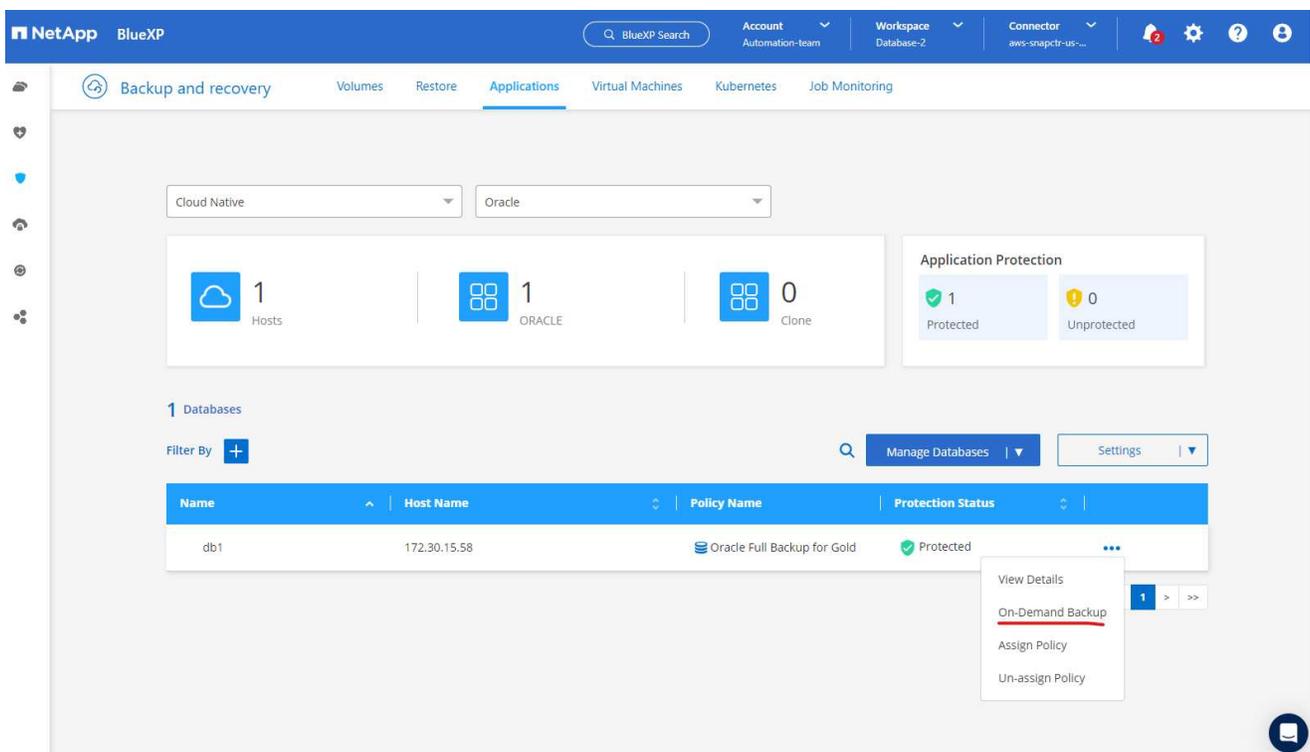
1. Choisissez la politique à attribuer à la base de données.



1. Une fois la politique appliquée, l'état de protection de la base de données est passé à **Protégé** avec une coche verte.



1. La sauvegarde de la base de données s'exécute selon un calendrier prédéfini. Vous pouvez également exécuter une sauvegarde ponctuelle à la demande comme indiqué ci-dessous.



1. Les détails des sauvegardes de la base de données peuvent être consultés en cliquant sur **Afficher les détails** dans la liste du menu. Cela inclut le nom de la sauvegarde, le type de sauvegarde, le SCN et la date de sauvegarde. Un ensemble de sauvegarde couvre un instantané du volume de données et du volume de journal. Un instantané du volume de journal a lieu juste après un instantané du volume de base de données. Vous pouvez appliquer un filtre si vous recherchez une sauvegarde particulière dans une longue liste.

NetApp BlueXP

Account Automation-team | Workspace Database-2 | Connector aws-snapctr-us...

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	...

## Restauration et récupération de bases de données Oracle

1. Pour une restauration de base de données, choisissez la bonne sauvegarde, soit par le SCN, soit par l'heure de sauvegarde. Cliquez sur les trois points de la sauvegarde des données de la base de données, puis cliquez sur **Restaurer** pour lancer la restauration et la récupération de la base de données.

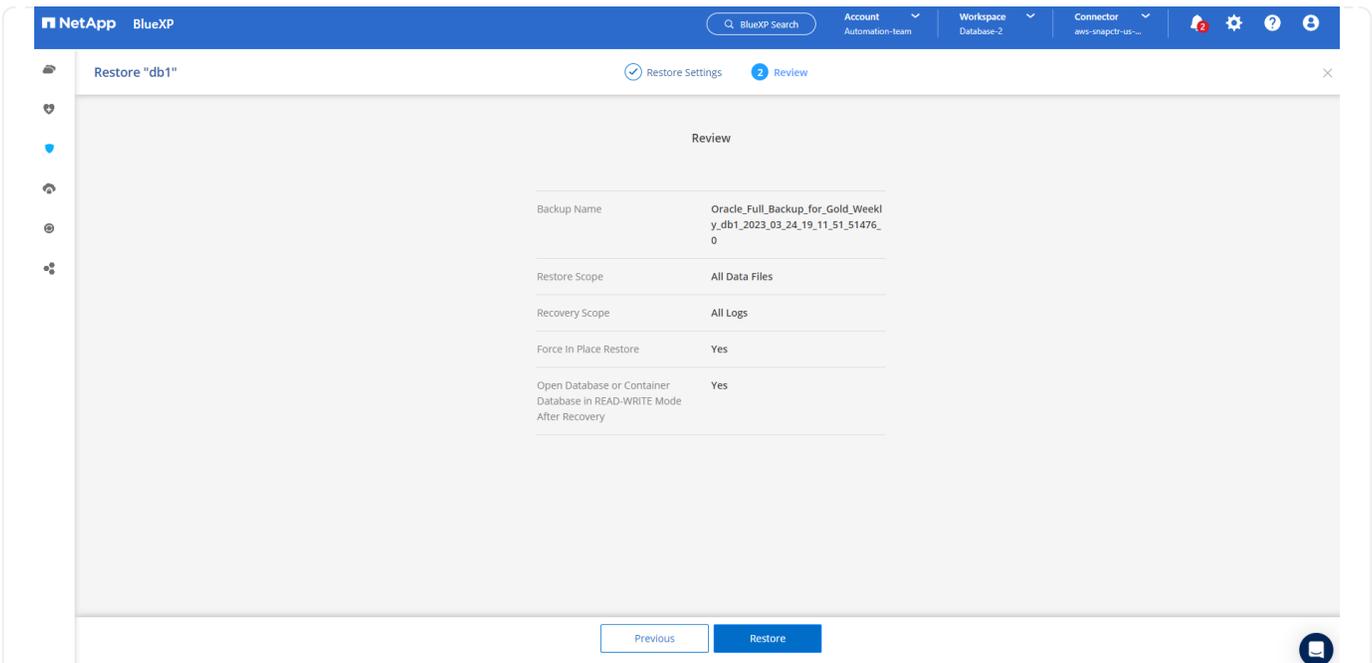
The screenshot shows the NetApp BlueXP interface. At the top, there's a navigation bar with 'Backup and recovery' selected. Below it, the 'Database Details' section for 'db1' is visible, showing fields like Database Name, Host Name, Clones, Protected Protection, Host Storage, Parent Database, Oracle Full Backup for Gold Policy Names, Database Version, Database Type, and Agent Id. Below the details is a 'Backups' section with a table of backup records. The table has columns for Backup Name, Backup Type, SCN, Backup Date, and a 'Delete' button. The 'Restore' button for the backup 'Oracle\_Full\_Backup\_for\_Gold\_Hourly\_db1\_2023\_03\_24\_15\_37\_04\_98851\_1' is highlighted with a red box.

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, 11:37:1	Restore
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_36_33_27205_0	Data	2580524	Mar 24, 2023, 11:37:0	Delete Clone

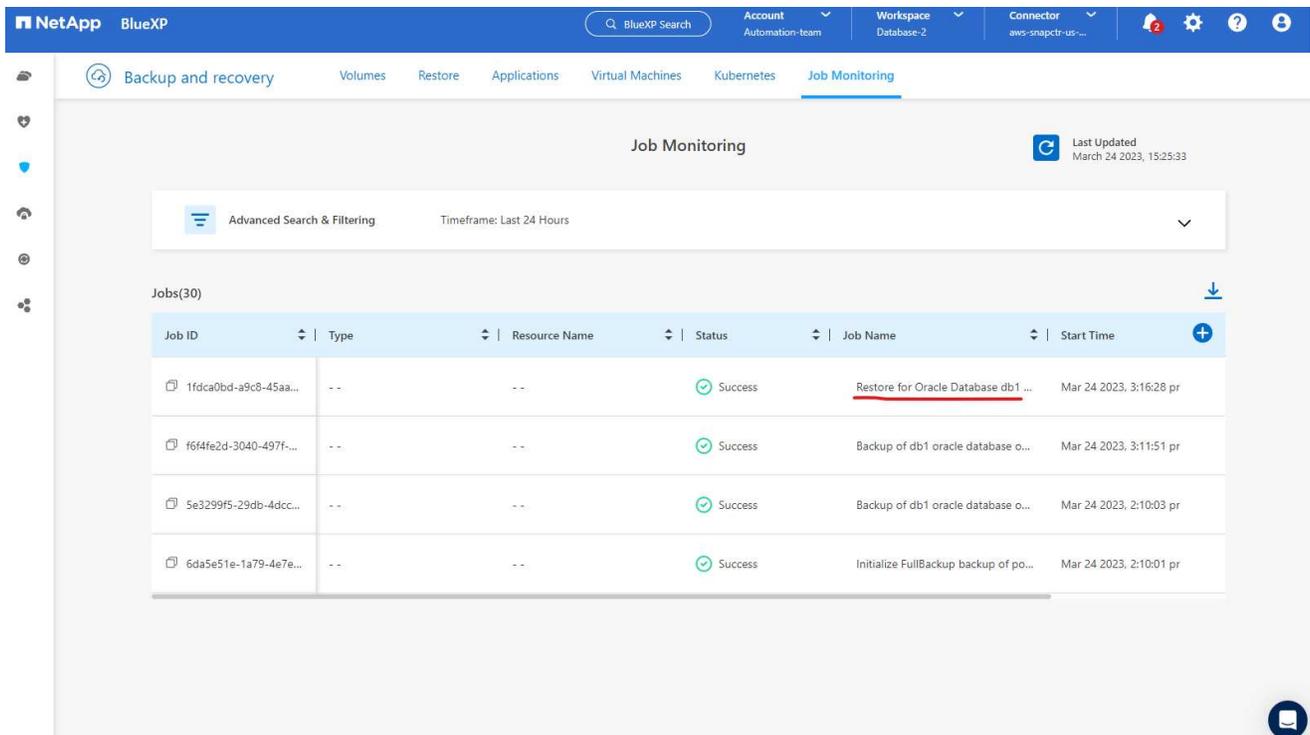
1. Choisissez votre paramètre de restauration. Si vous êtes sûr que rien n'a changé dans la structure physique de la base de données après la sauvegarde (comme l'ajout d'un fichier de données ou d'un groupe de disques), vous pouvez utiliser l'option **Forcer la restauration sur place**, qui est généralement plus rapide. Sinon, ne cochez pas cette case.

The screenshot shows the 'Restore Settings' dialog box in the NetApp BlueXP interface. The 'Restore Scope' section has three options: 'All Data Files' (selected), 'Control Files', and 'Force in place restore' (checked). Below this, there's a note: 'In place restore will skip the foreign files (files which are not part of the database) validation check. The Oracle database and the ASM disk group will be restored to the point when the backup was created.' The 'Recovery Scope' section has four options: 'All Logs' (selected), 'Until System Change Number', 'Date and Time', and 'No Recovery'. There's a text input field for 'Archive Log Files Locations' with the value '/mnt/log\_location001'. At the bottom, there's a checkbox 'Open the database or the container database in READ-WRITE mode after recovery.' and 'Previous' and 'Next' buttons.

1. Examinez et démarrez la restauration et la récupération de la base de données.



1. À partir de l'onglet **Surveillance des tâches**, vous pouvez afficher l'état de la tâche de restauration ainsi que tous les détails pendant son exécution.



NetApp BlueXP Account Automation-team Workspace Database-2 Connector aws-snapctr-us-...

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

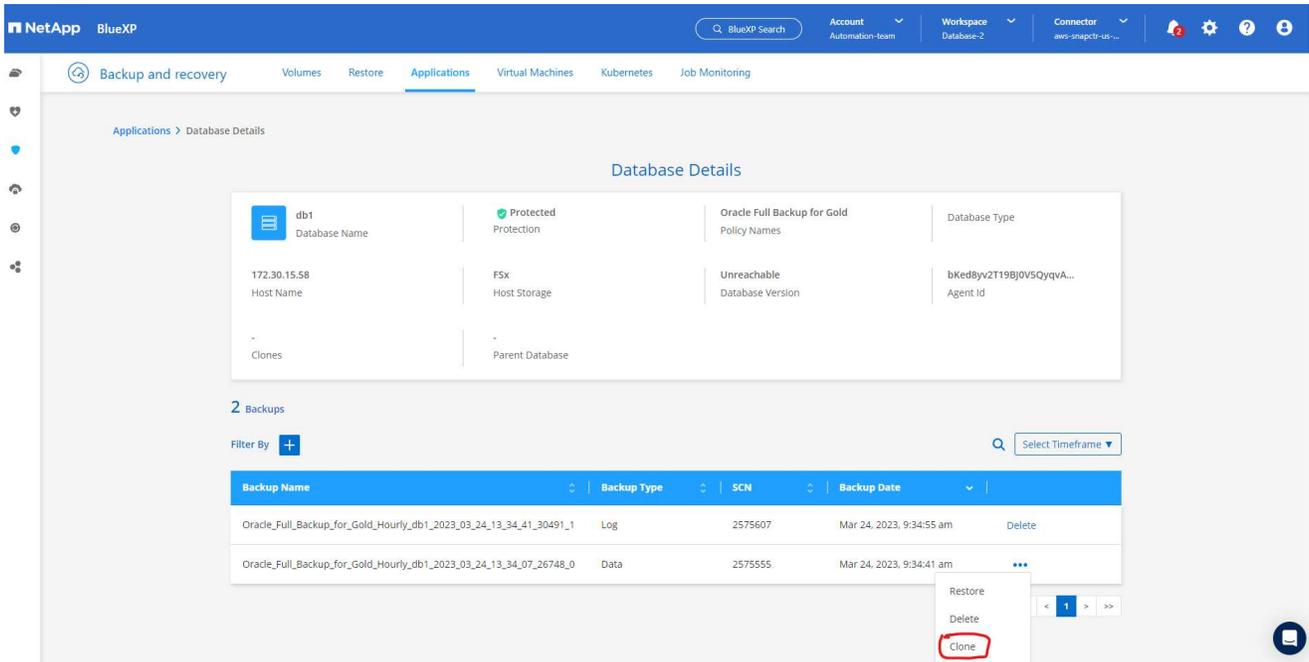
Sub-Jobs(6)

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	fb7b1171-966f-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

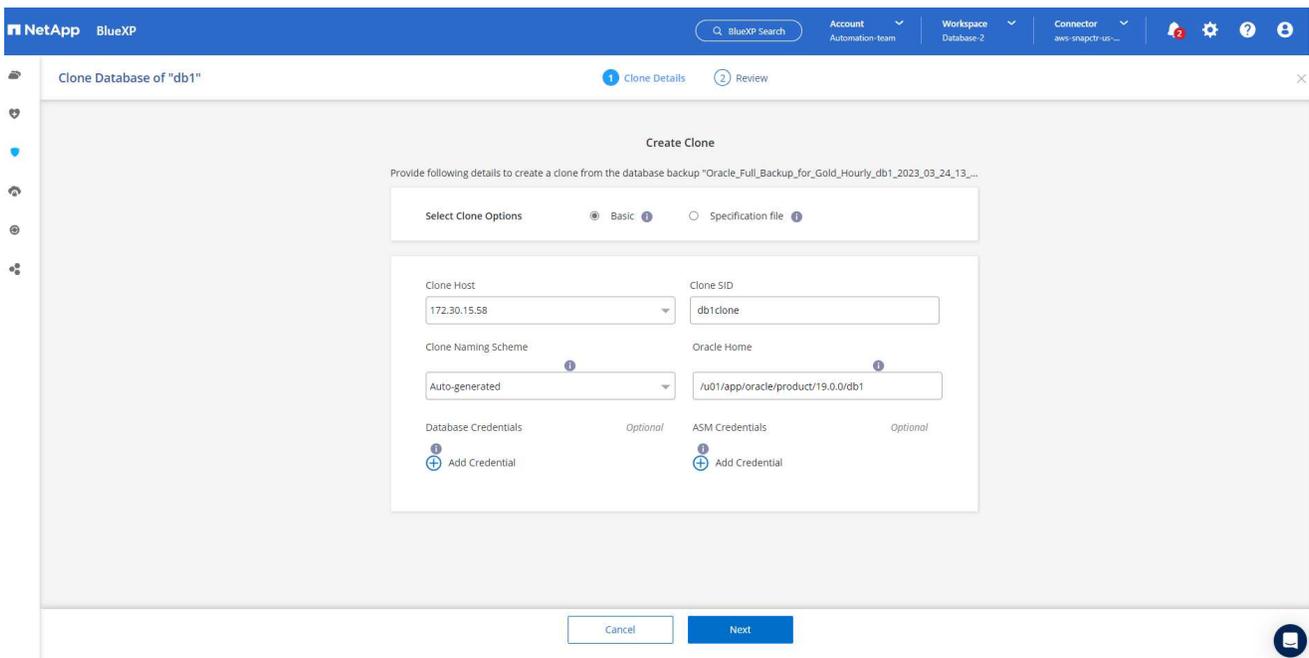
## Clonage de base de données Oracle

Pour cloner une base de données, lancez le workflow de clonage à partir de la même page de détails de sauvegarde de la base de données.

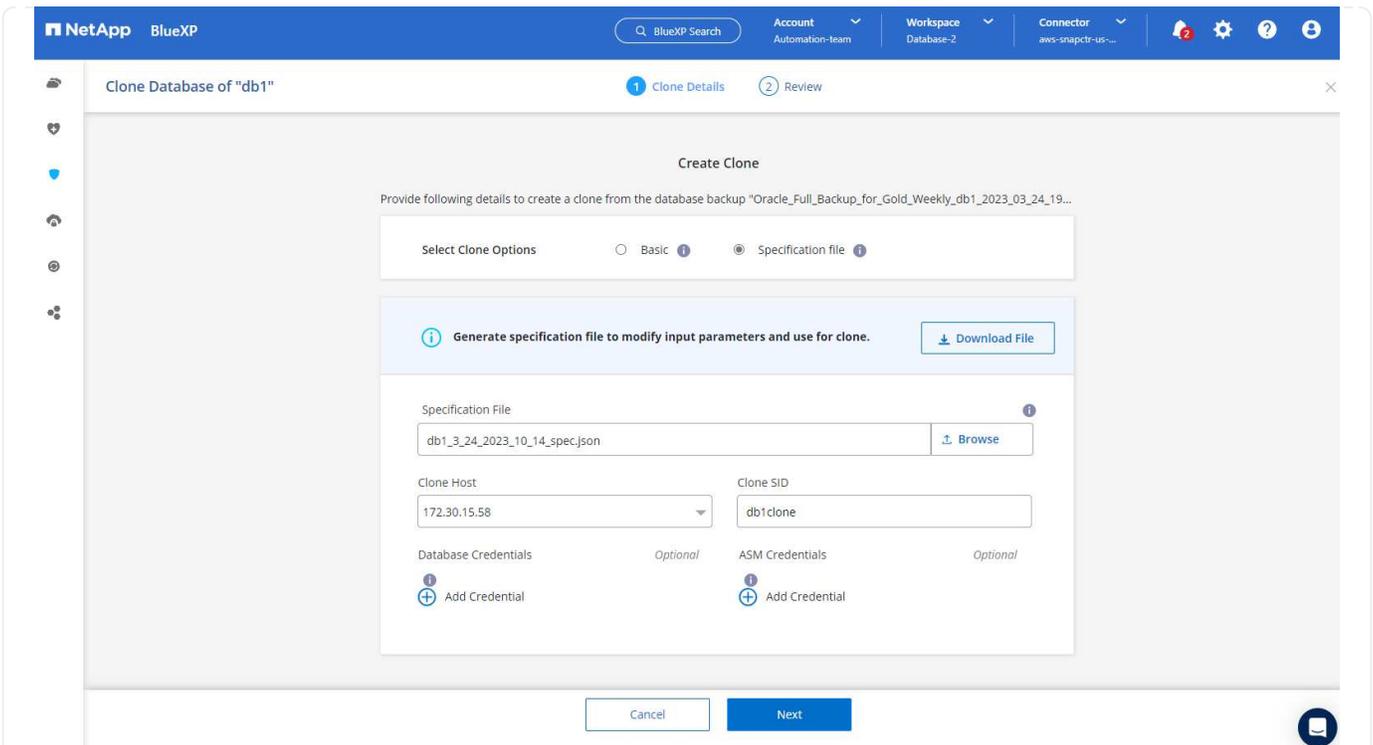
1. Sélectionnez la bonne copie de sauvegarde de la base de données, cliquez sur les trois points pour afficher le menu et choisissez l'option **Cloner**.



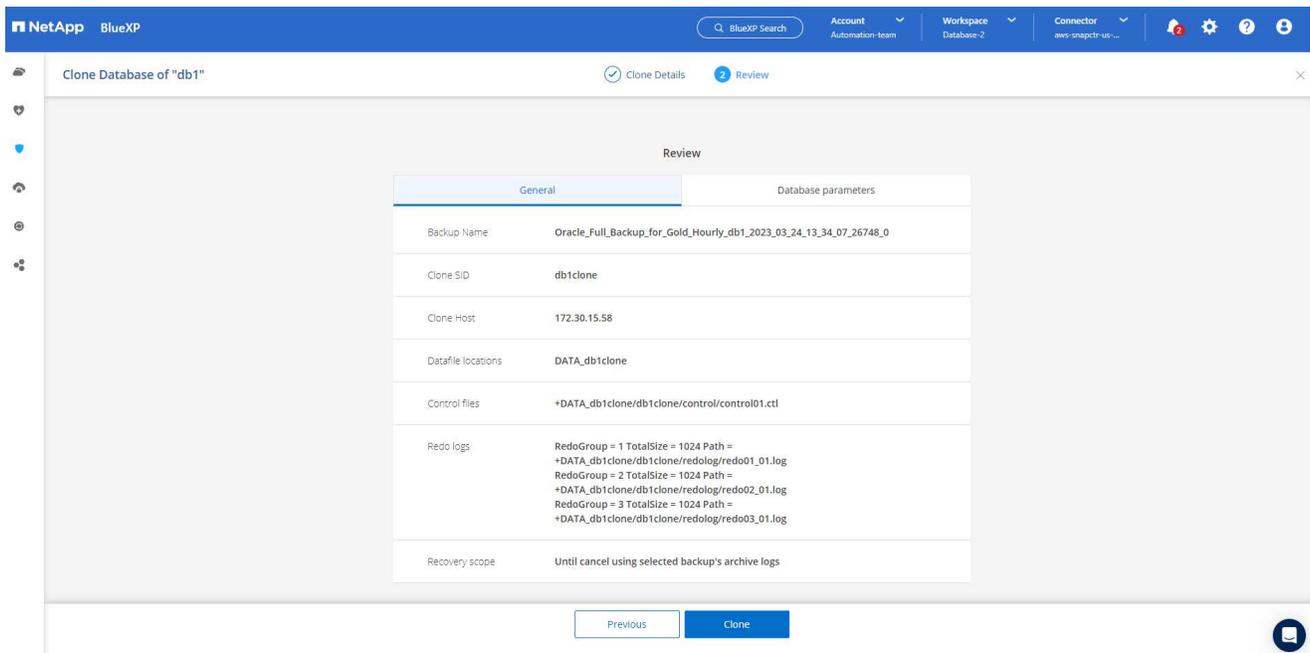
1. Sélectionnez l'option **Basique** si vous n'avez pas besoin de modifier les paramètres de la base de données clonée.



1. Vous pouvez également sélectionner **Fichier de spécifications**, ce qui vous donne la possibilité de télécharger le fichier d'initialisation actuel, d'y apporter des modifications, puis de le télécharger à nouveau dans le travail.



1. Révisez et lancez le travail.



1. Surveillez l'état du travail de clonage à partir de l'onglet **Surveillance des travaux**.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and dropdown menus for 'Account Automation-team', 'Workspace Database-2', and 'Connector aws-snapc1r-1b...'. The main menu has 'Backup and recovery' selected, with sub-menus for 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Job Monitoring' page displays 'Job Details' for Job ID: cd30abaf-fbe2-4052-a6db-4bf965a8d29b. It shows 'Sub-Jobs(2)' in a table:

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	511f52c1-853a-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. Validez la base de données clonée sur l'hôte de l'instance EC2.

```

#
# 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/oracle/product/19.0.0/db1,STABLE
ora.db1clone.db
      1        ONLINE  ONLINE      ip-172-30-15-58          Open,HOME=/u01/app/oracle/product/19.0.0/db1,STABLE
ora.diskmon
      1        OFFLINE OFFLINE
      STABLE
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$databases;

NAME                OPEN_MODE
-----
DB1CLONE            READ WRITE

SQL> █

```

# Informations Complémentaires

Pour en savoir plus sur les informations décrites dans ce document, consultez les documents et/ou sites Web suivants :

- Configurer et administrer BlueXP

["https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html"](https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html)

- Documentation de BlueXP backup and recovery

["https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html"](https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html)

- Amazon FSx ONTAP

["https://aws.amazon.com/fsx/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\\_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef\\_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw\\_wcB:G:s&s\\_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2](https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2)

## Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.