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

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 :

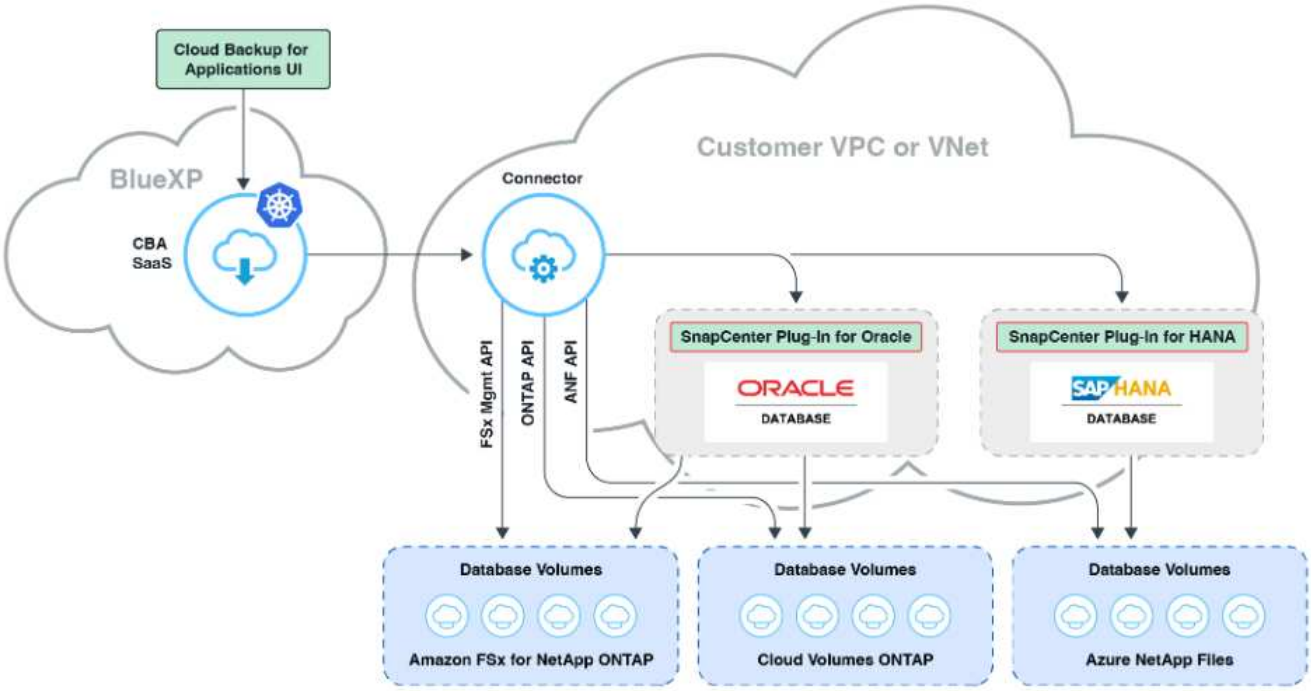
- L'administrateur de base de données qui gère les bases de données Oracle exécutées sur le stockage Amazon FSx ONTAP
- L'architecte de solutions qui souhaite tester la sauvegarde, la restauration et le clonage de bases de données Oracle dans le cloud public AWS
- L'administrateur de stockage qui prend 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

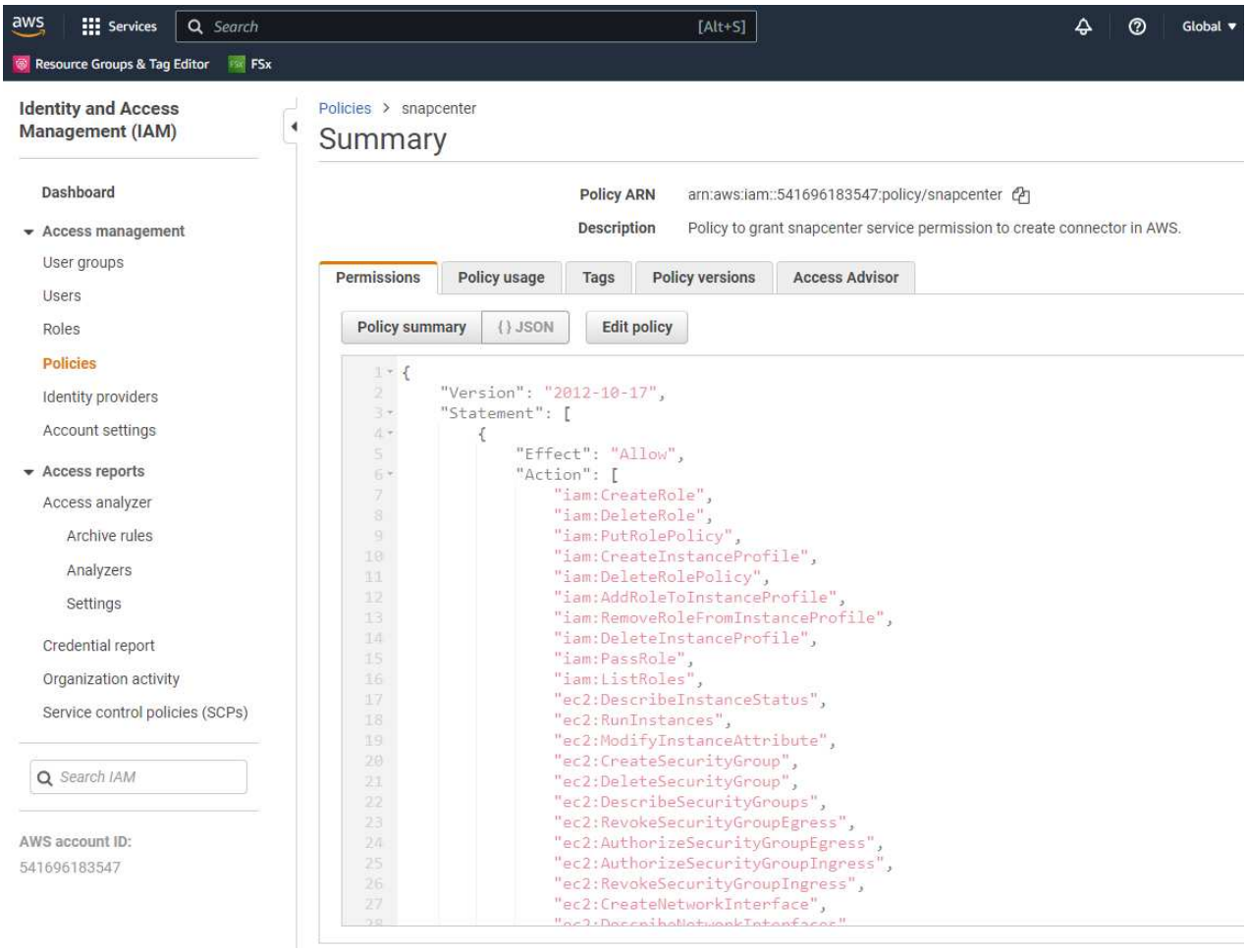
Conditions préalables au déploiement du service SnapCenter

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 .

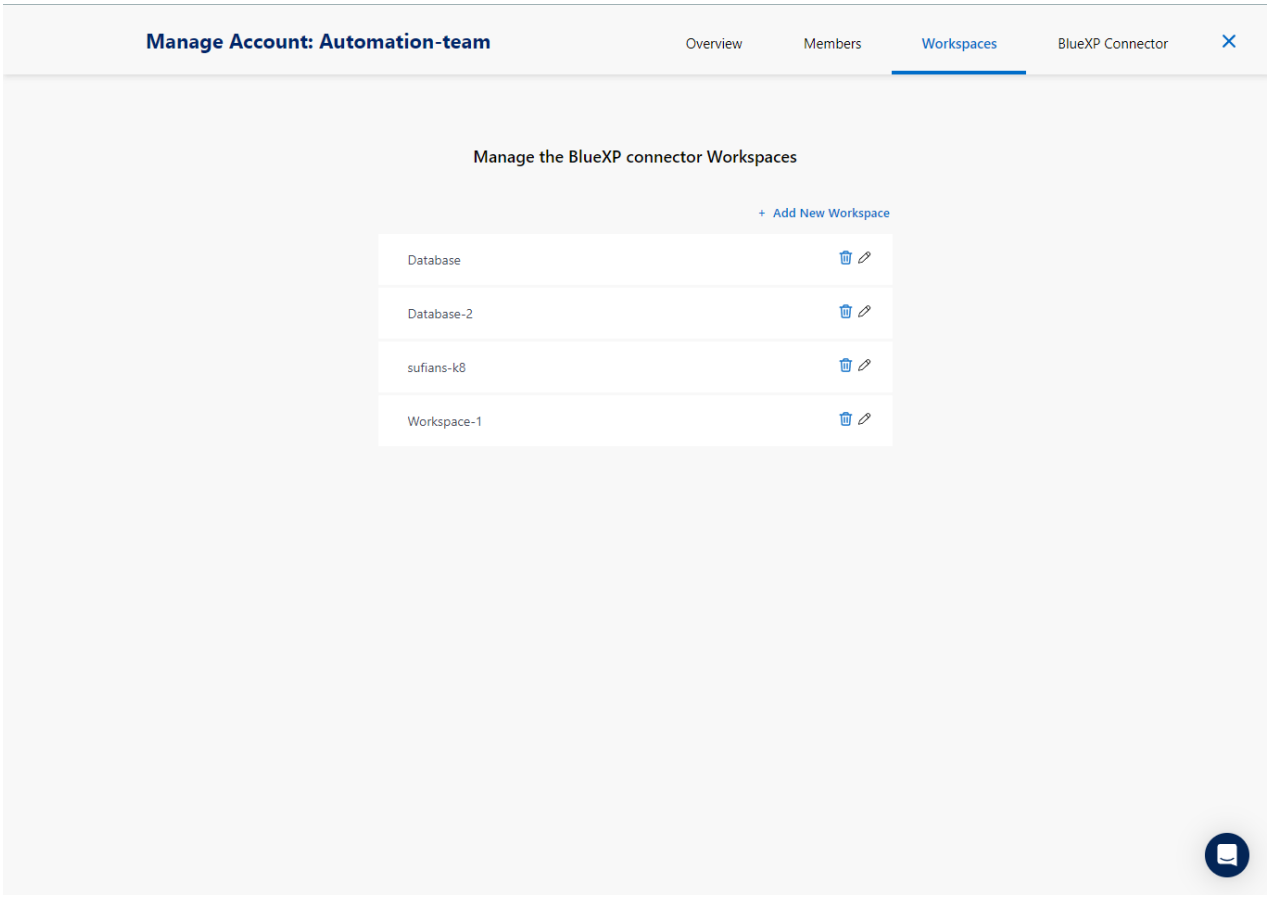


La politique doit être configurée avec une chaîne JSON disponible dans la documentation NetApp . La chaîne JSON peut également être récupérée à partir de la page lorsque le provisionnement du connecteur est lancé et que vous êtes invité à attribuer les autorisations préalables.

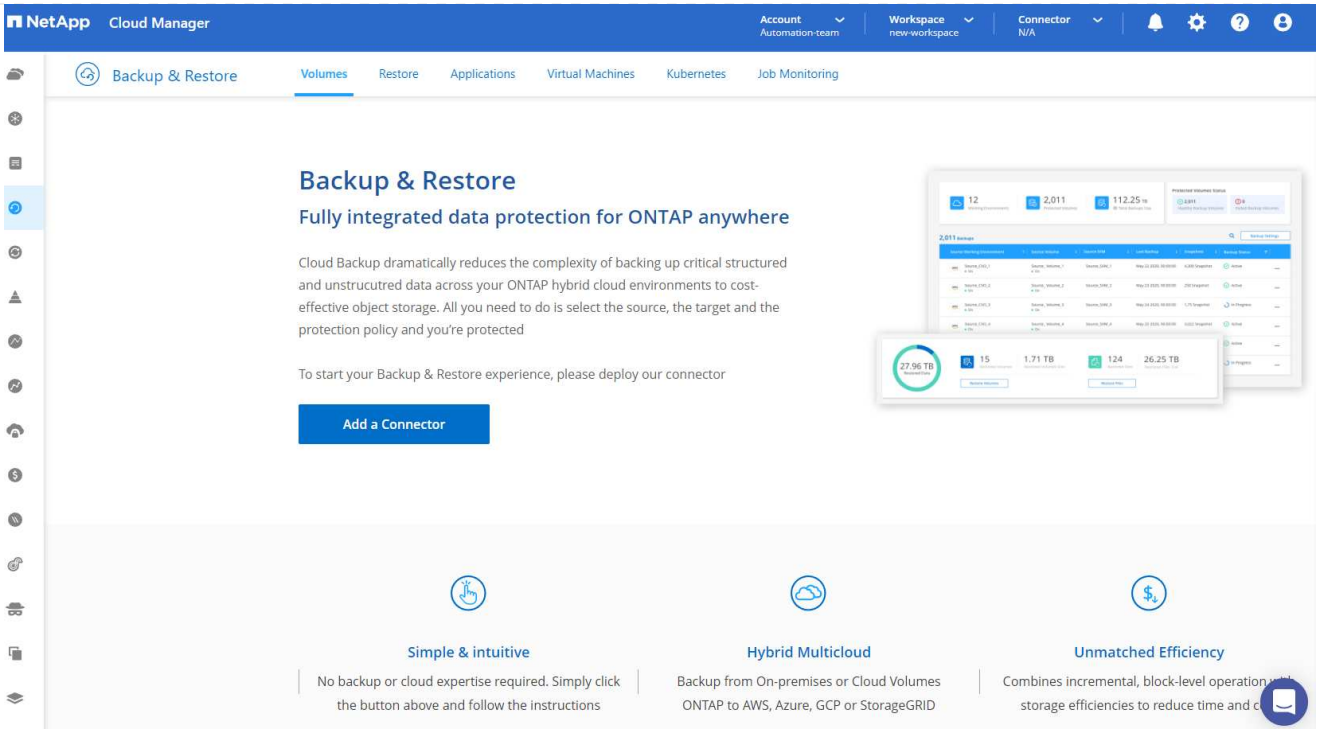
3. Vous avez également besoin du VPC AWS, du sous-réseau, du groupe de sécurité, d'une clé d'accès et de secrets de compte utilisateur AWS, d'une clé SSH pour ec2-user, etc., prêts pour le provisionnement du connecteur.

Déployer un connecteur pour les services SnapCenter

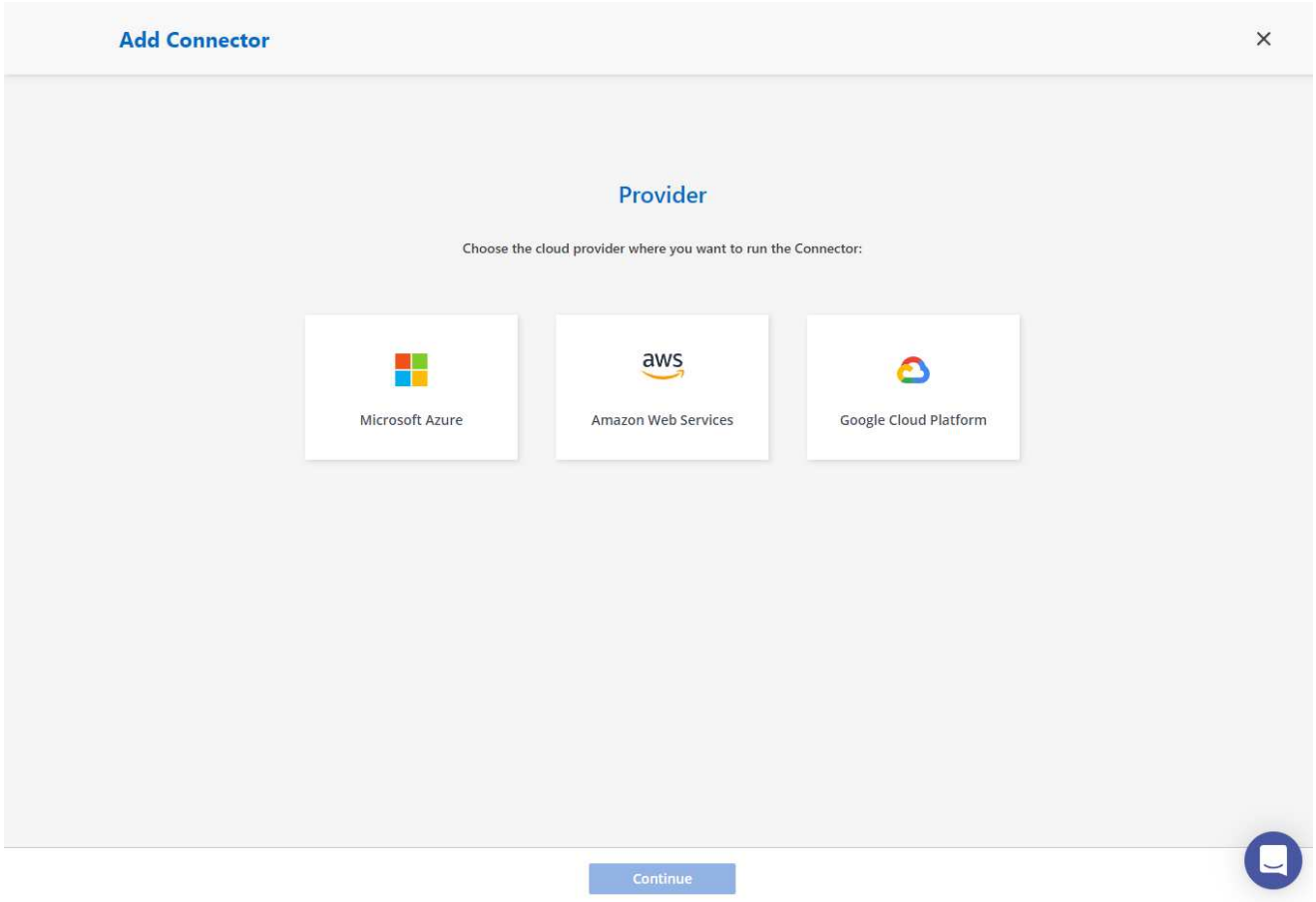
1. Connectez-vous à la console BlueXP . Pour un compte partagé, il est recommandé de créer un espace de travail individuel en cliquant sur **Compte** > **Gérer le compte** > **Espace de travail** pour ajouter un nouvel espace de travail.



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

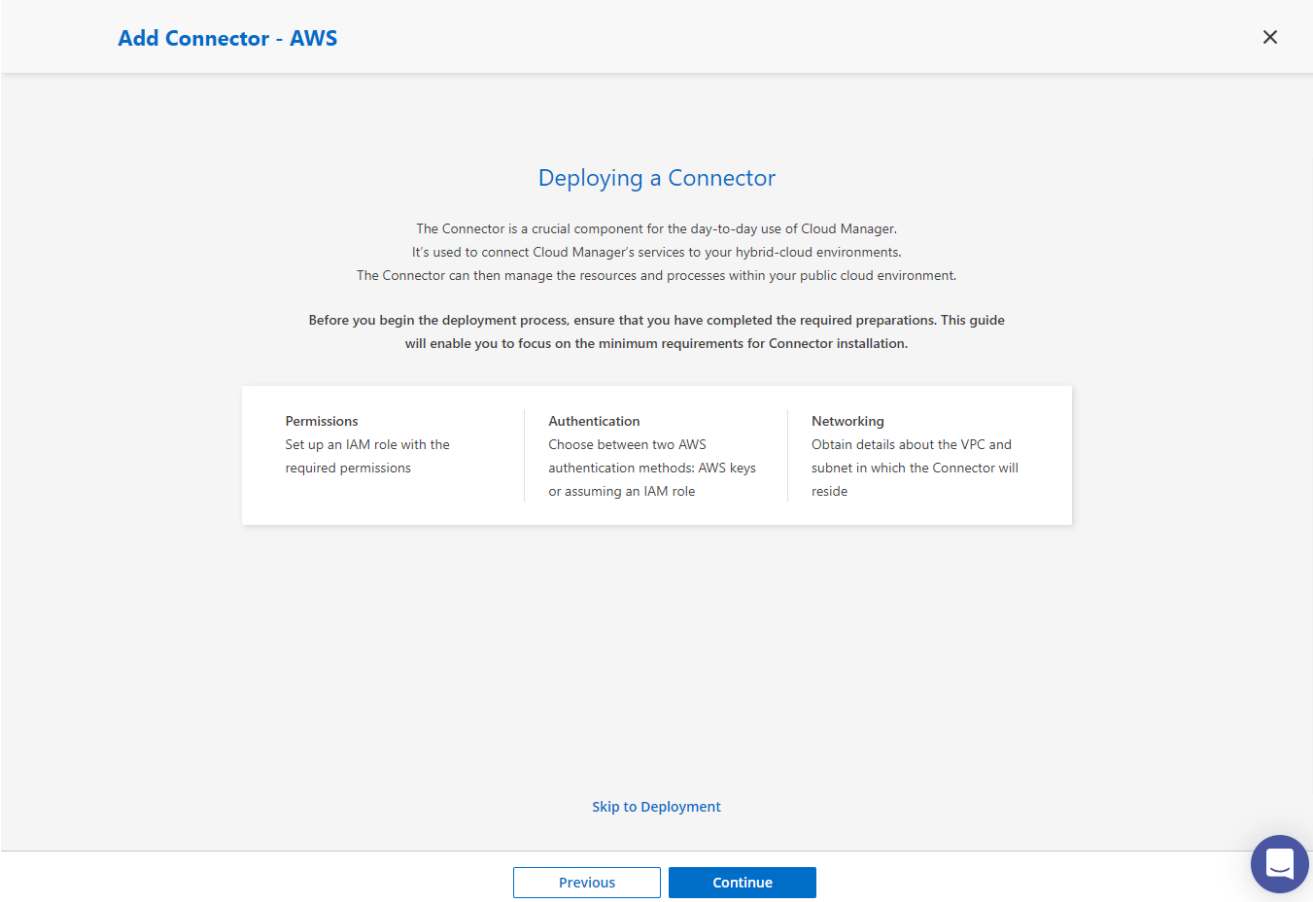


1. Choisissez votre fournisseur cloud (dans ce cas, **Amazon Web Services**).

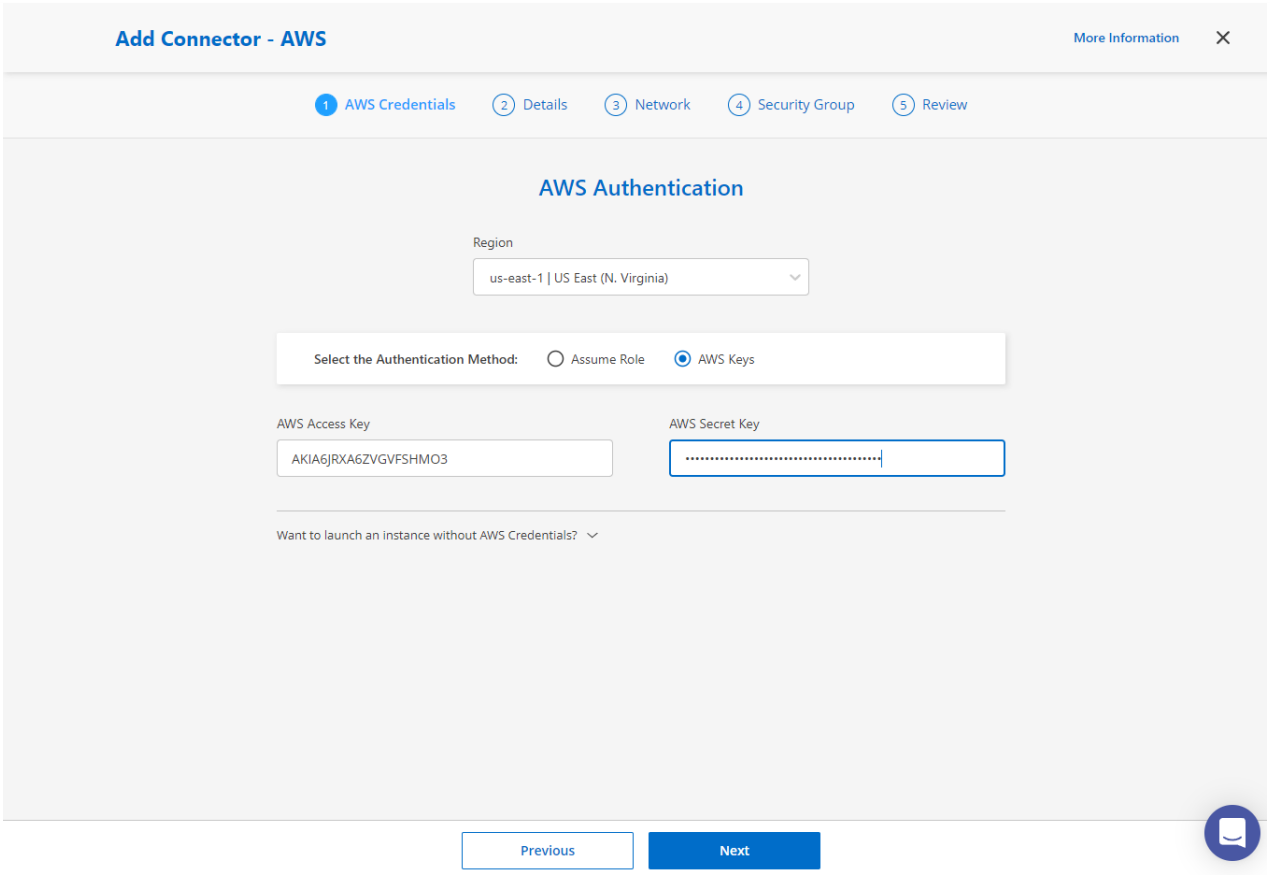


1. Ignorez les étapes **Autorisation**, **Authentification** et **Mise en réseau** si vous les avez déjà configurées dans votre compte AWS. Sinon, vous devez les configurer avant de continuer. À partir de là, vous pouvez également récupérer les autorisations pour la politique AWS référencée dans la

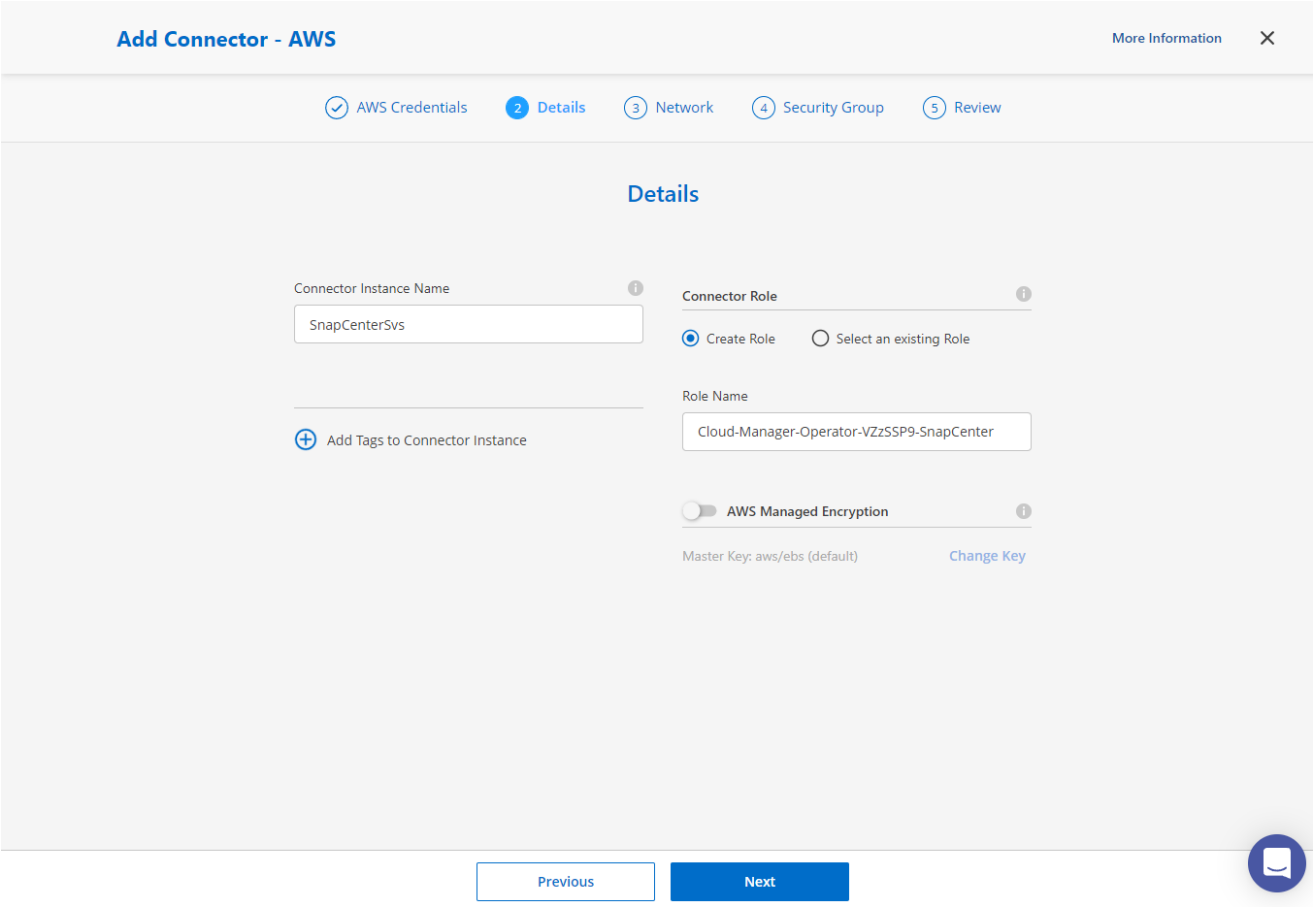
section précédente "Préparation à l'intégration de BlueXP ."



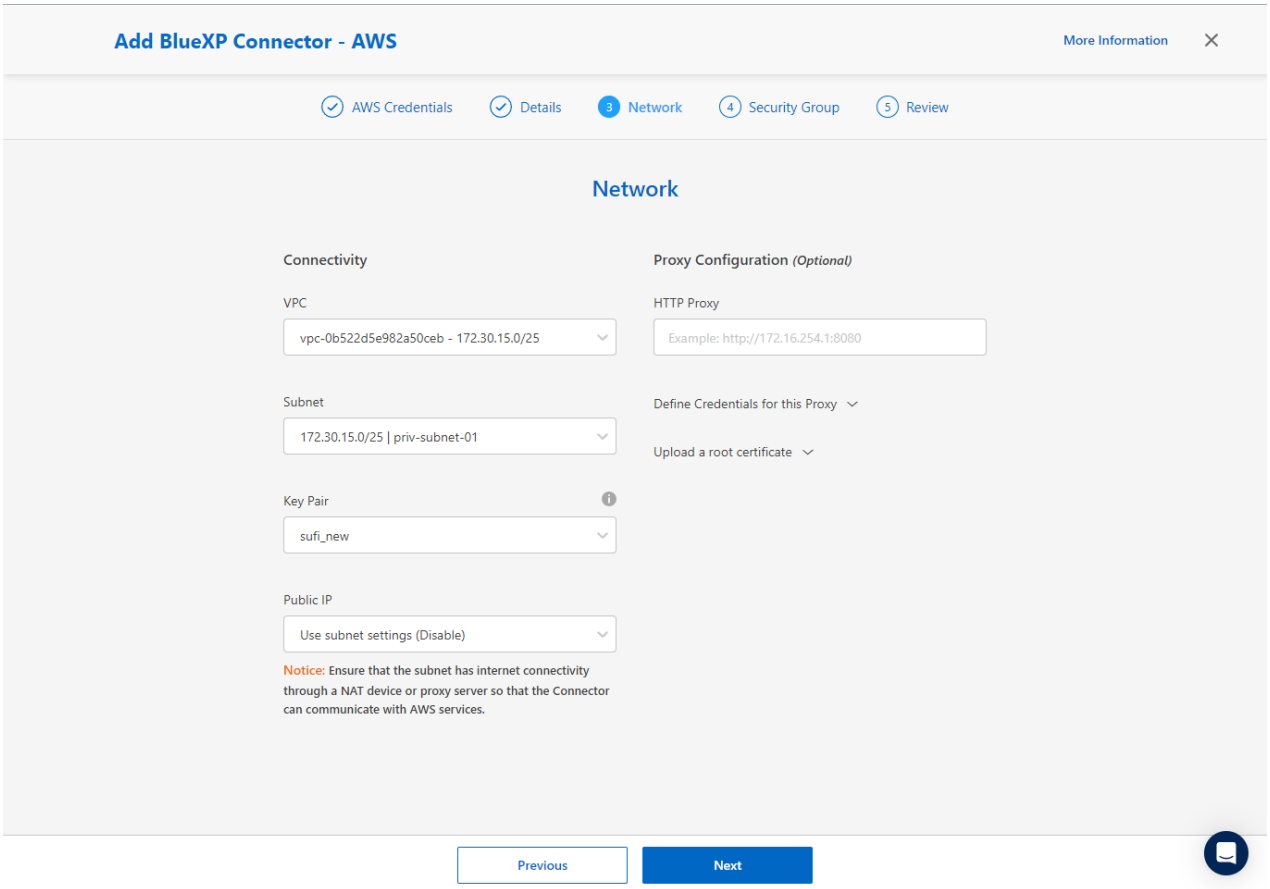
1. Saisissez l'authentification de votre compte AWS avec **Clé d'accès** et **Clé secrète**.



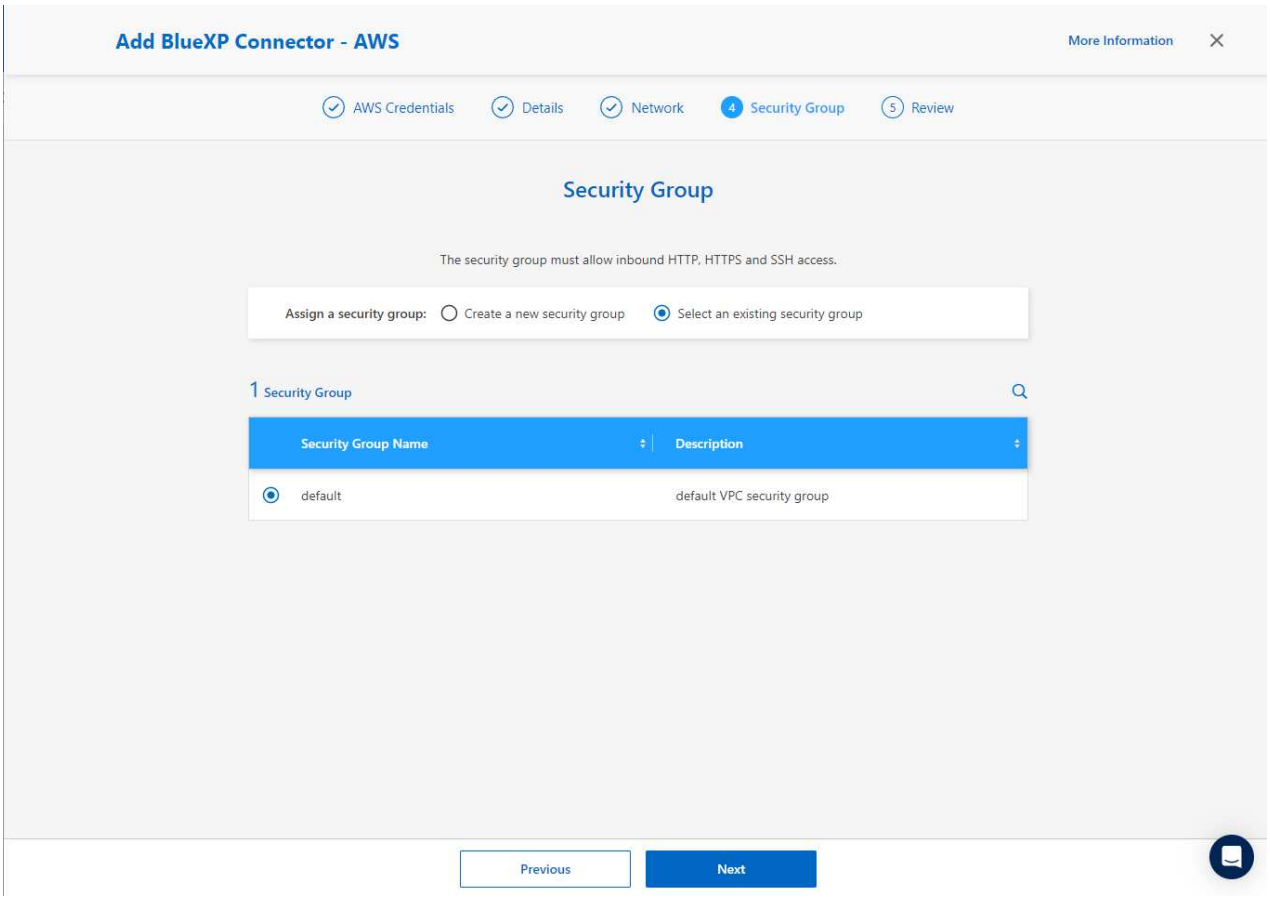
2. Nommez l'instance du connecteur et sélectionnez **Créer un rôle** sous **Détails**.



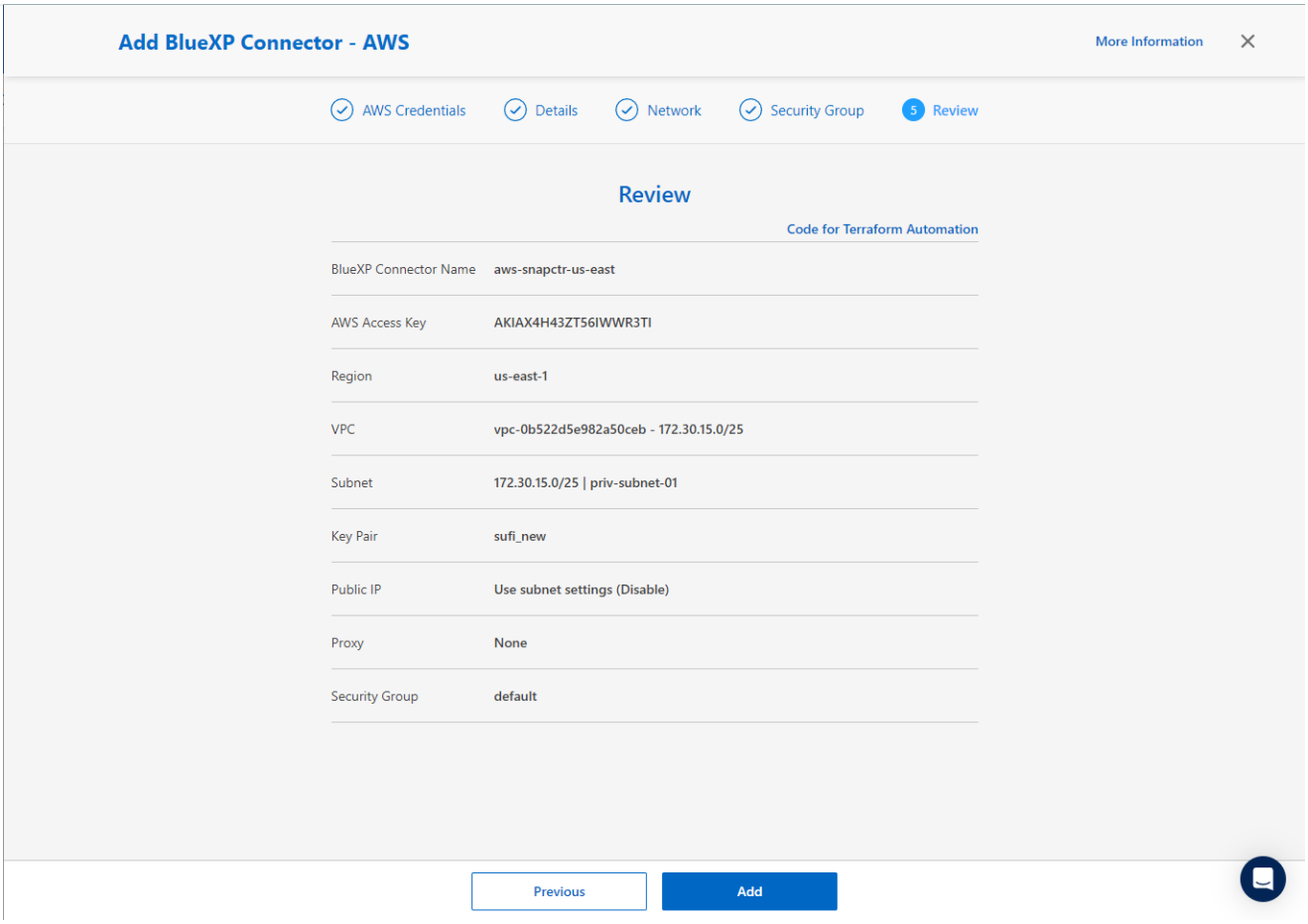
1. Configurez la mise en réseau avec la paire de clés **VPC**, **Sous-réseau** et SSH appropriée pour l'accès au connecteur.



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

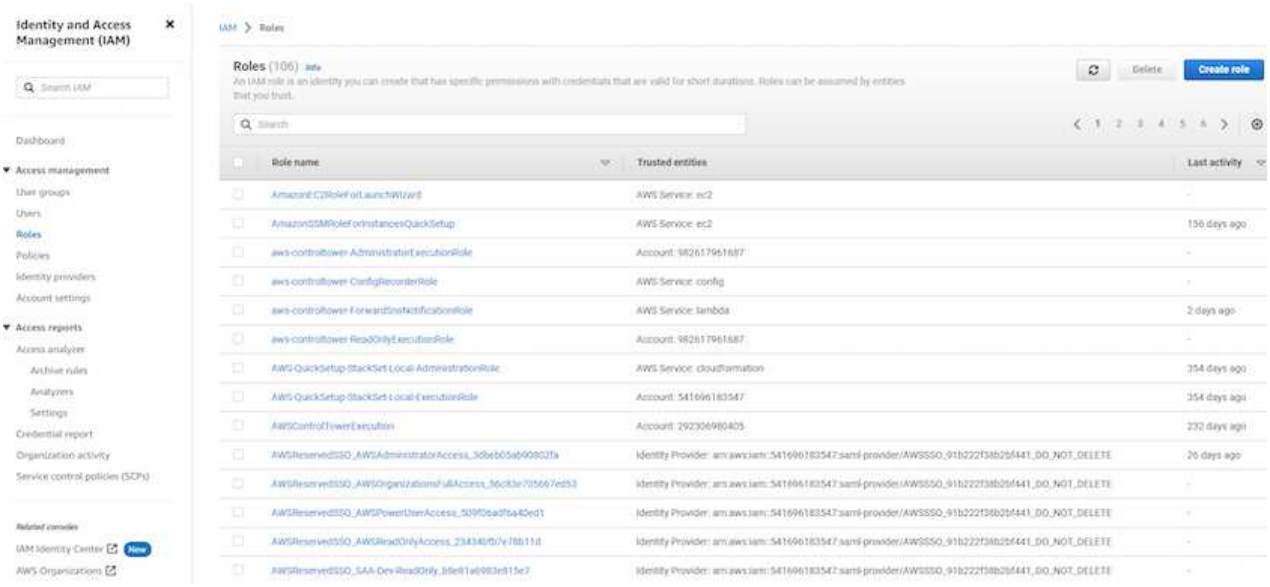


3. Consultez la page récapitulative et cliquez sur **Ajouter** pour démarrer la création du connecteur. Le déploiement prend généralement environ 10 minutes. Une fois terminée, l'instance du connecteur apparaît dans le tableau de bord AWS EC2.

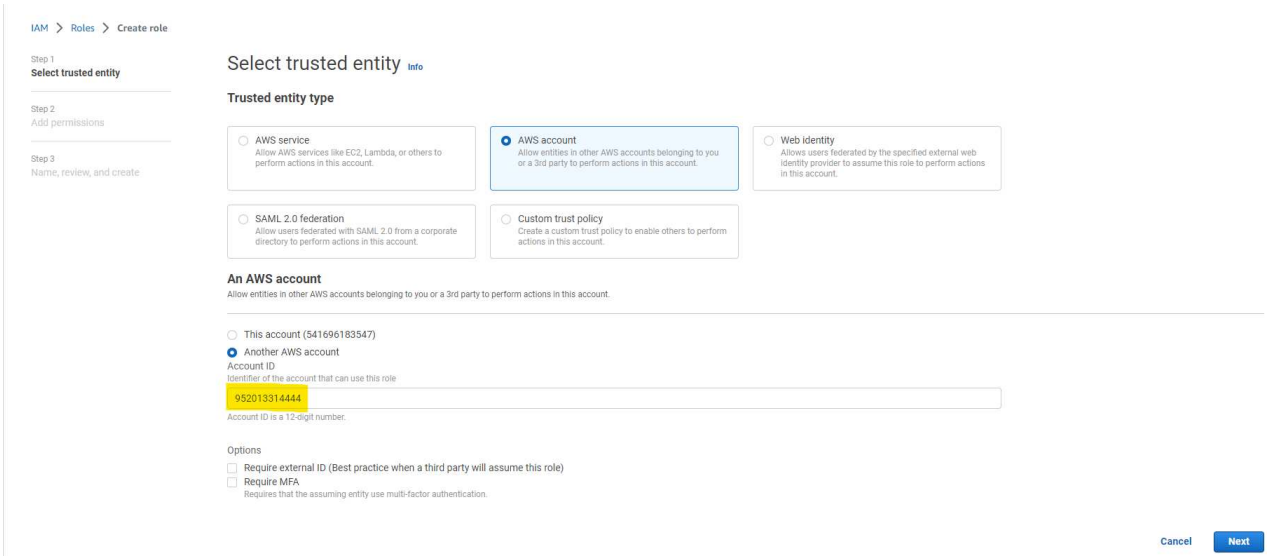


Définir des informations d’identification dans BlueXP pour l’accès aux ressources AWS

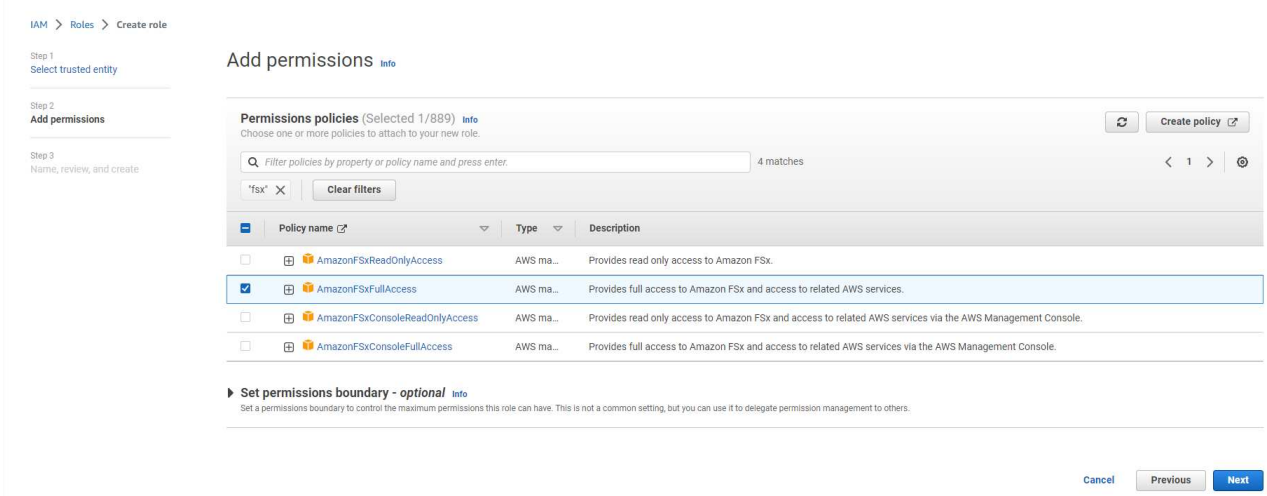
1. Tout d'abord, à partir de la console AWS EC2, créez un rôle dans le menu **Identity and Access Management (IAM) Rôles**, **Créer un rôle** pour démarrer le flux de travail de création de rôle.



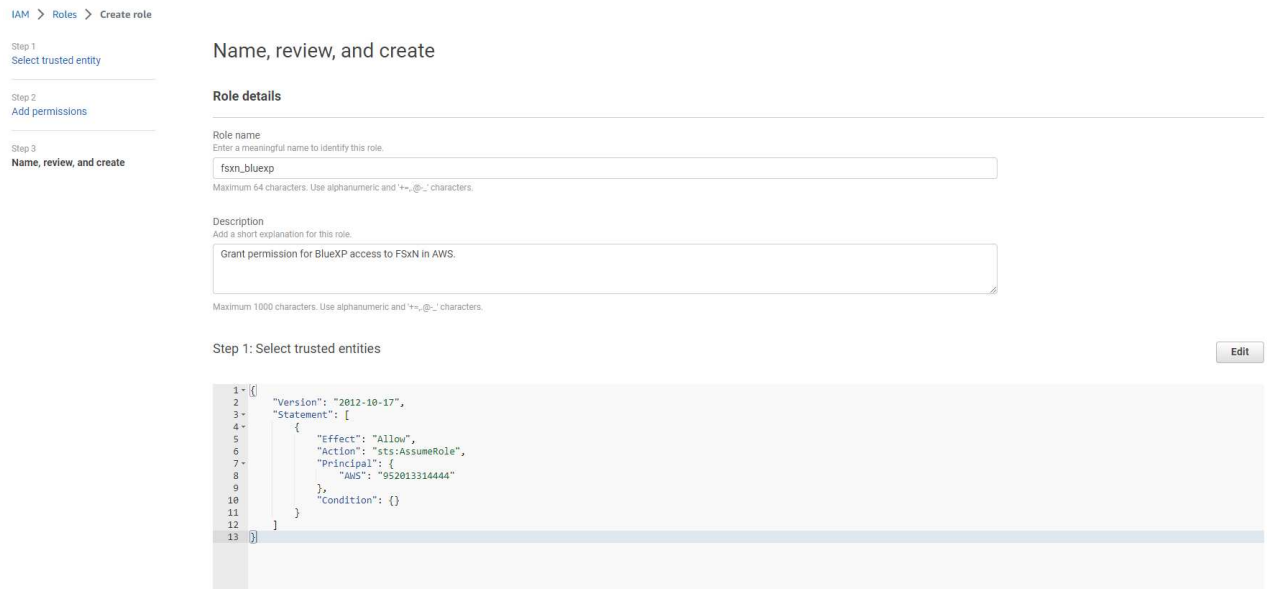
2. Dans la page **Sélectionner une entité de confiance**, choisissez **Compte AWS**, **Un autre compte AWS** et collez l'ID de compte BlueXP , qui peut être récupéré à partir de la console BlueXP .



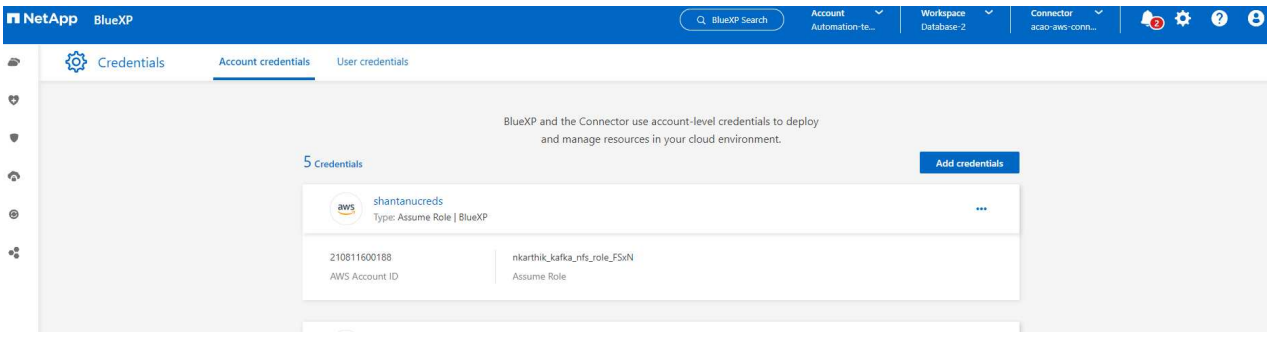
3. Filtrez les politiques d'autorisation par fsx et ajoutez des **politiques d'autorisation** au rôle.



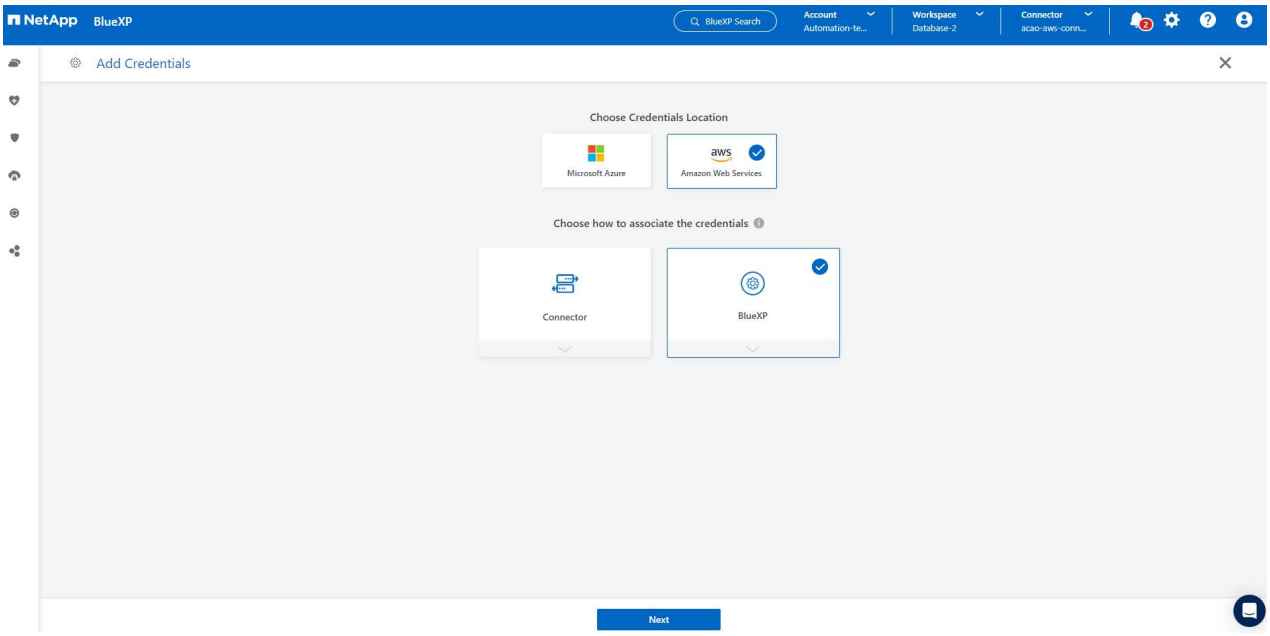
4. Dans la page **Détails du rôle**, nommez le rôle, ajoutez une description, puis cliquez sur **Créer un rôle**.



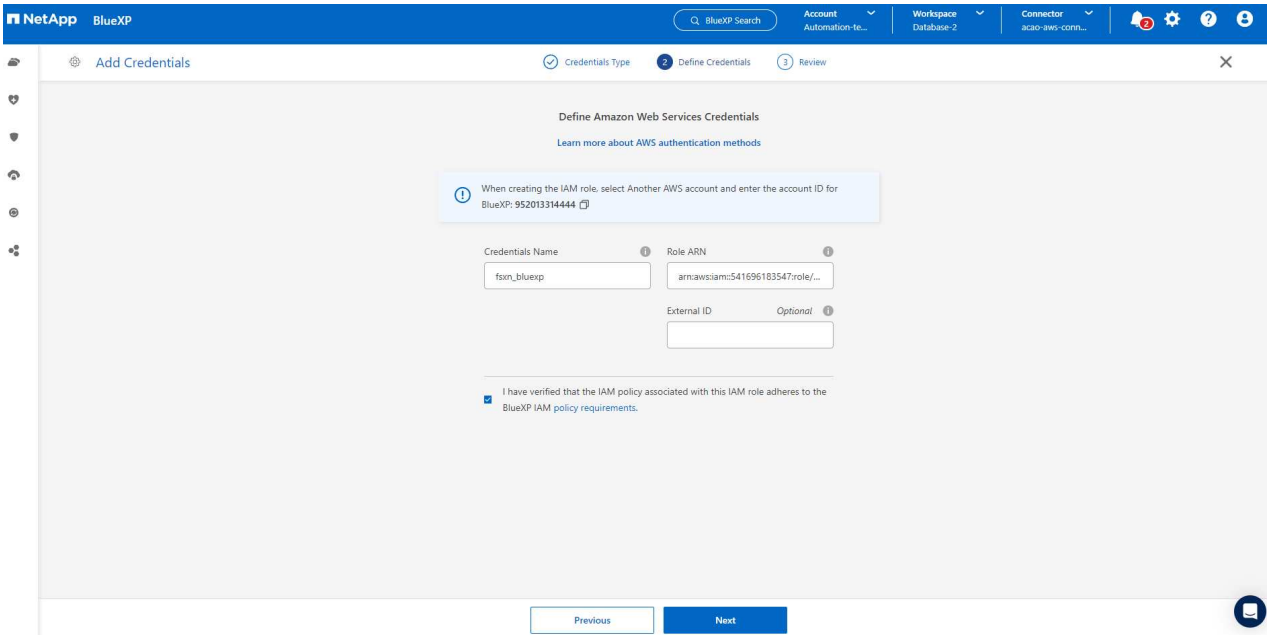
5. De retour à la console BlueXP , cliquez sur l'icône de configuration dans le coin supérieur droit de la console pour ouvrir la page **Informations d'identification du compte**, cliquez sur **Ajouter des informations d'identification** pour démarrer le flux de travail de configuration des informations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



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

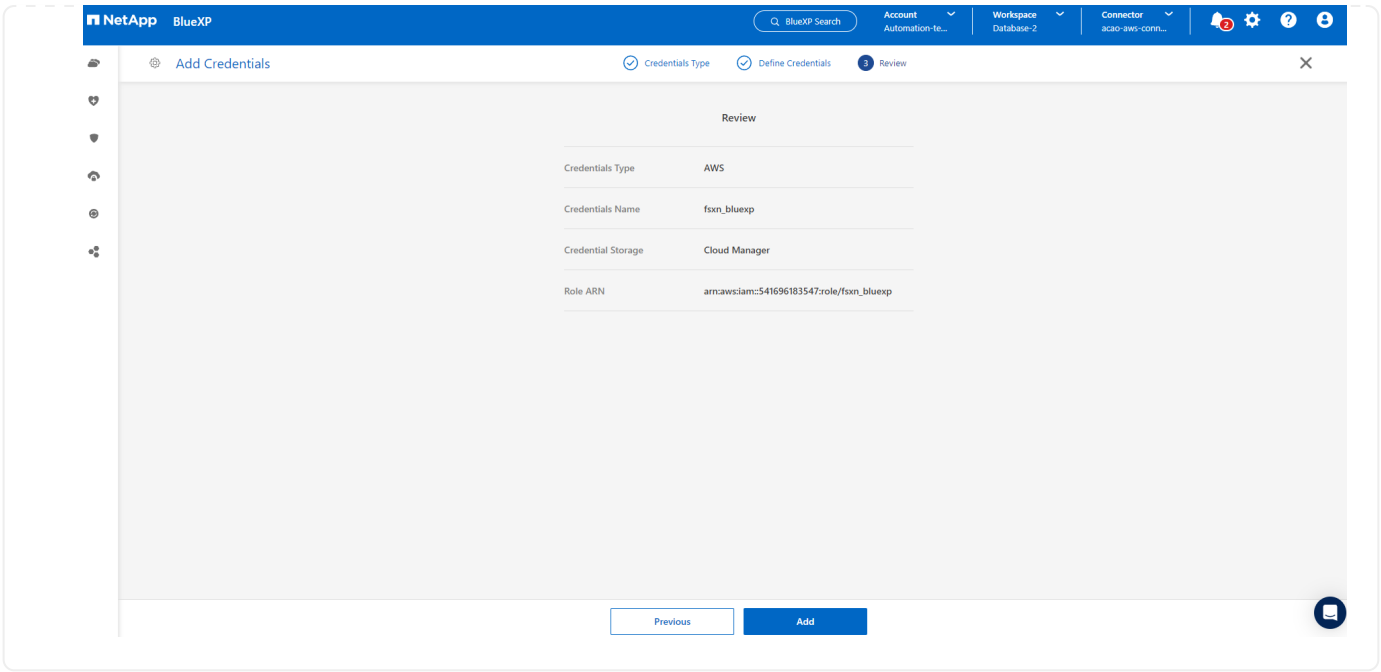


7. Définissez les informations d'identification AWS avec le **Role ARN** approprié, qui peut être récupéré à partir du rôle AWS IAM créé à l'étape 1 ci-dessus. BlueXP **ID de compte**, qui est utilisé pour créer le rôle AWS IAM à la première étape.



8. Réviser et **Ajouter**

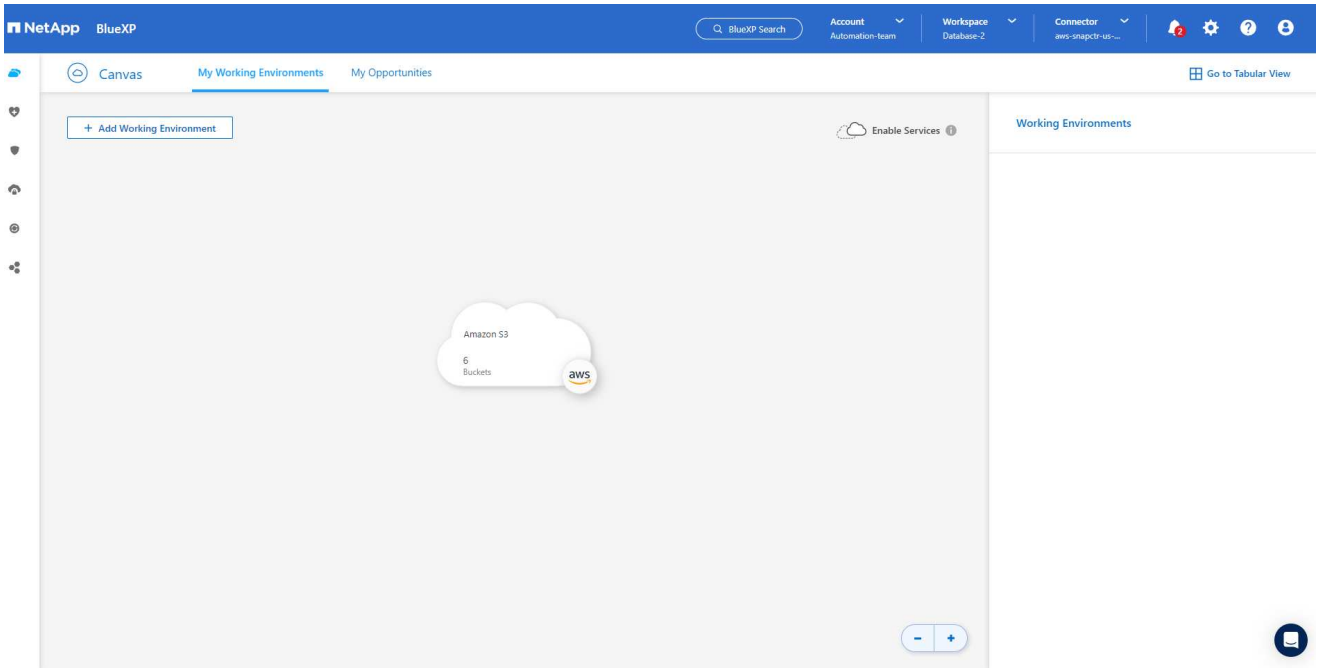
.



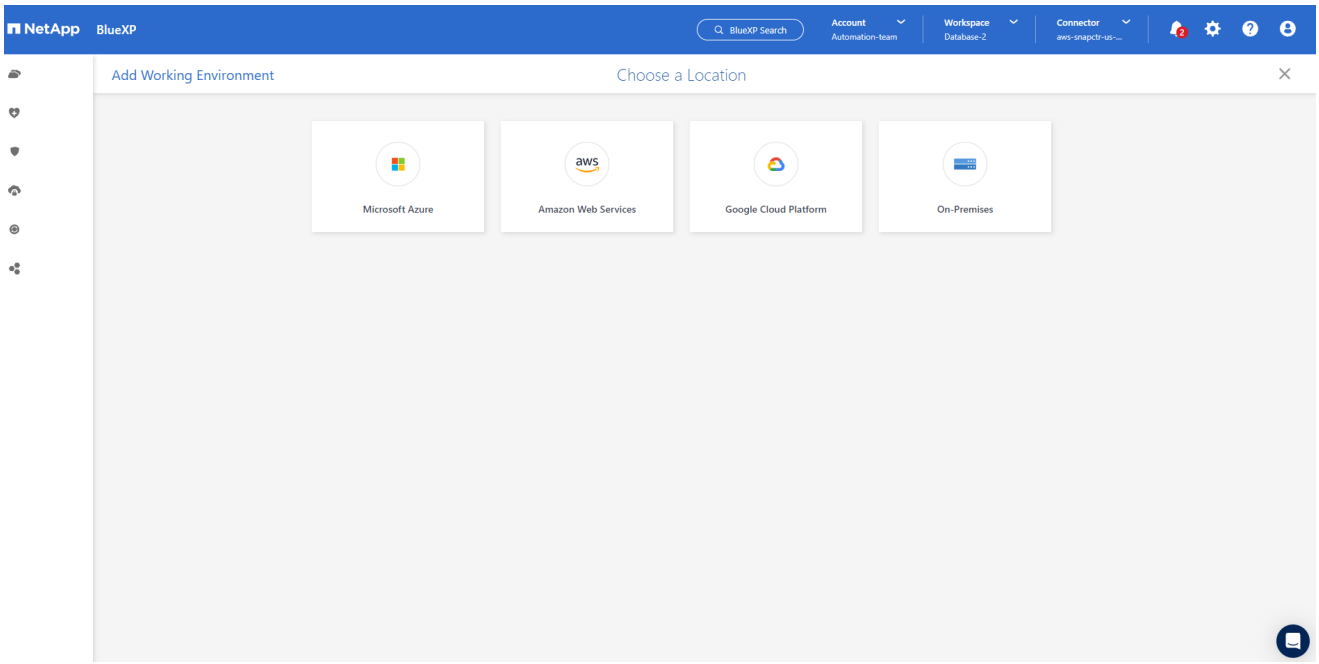
Configuration des services SnapCenter

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

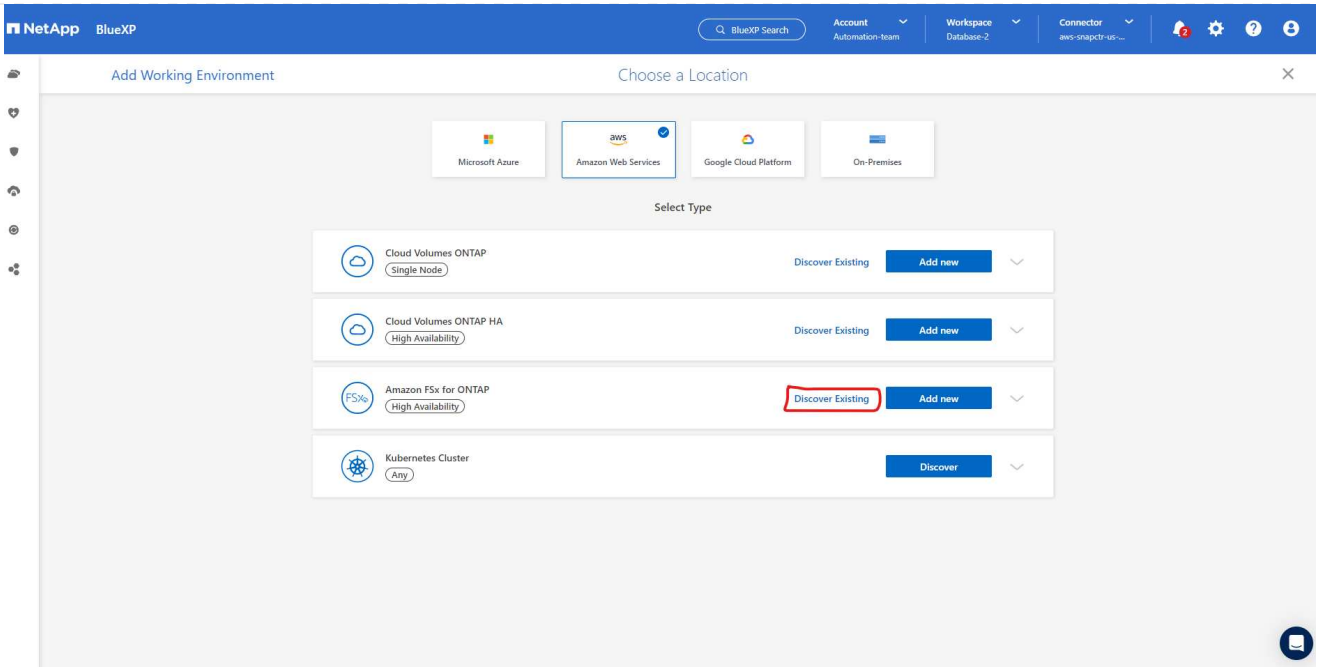
1. Depuis **Mon environnement de travail**, cliquez sur **Ajouter un environnement de travail** pour découvrir FSx déployé dans AWS.



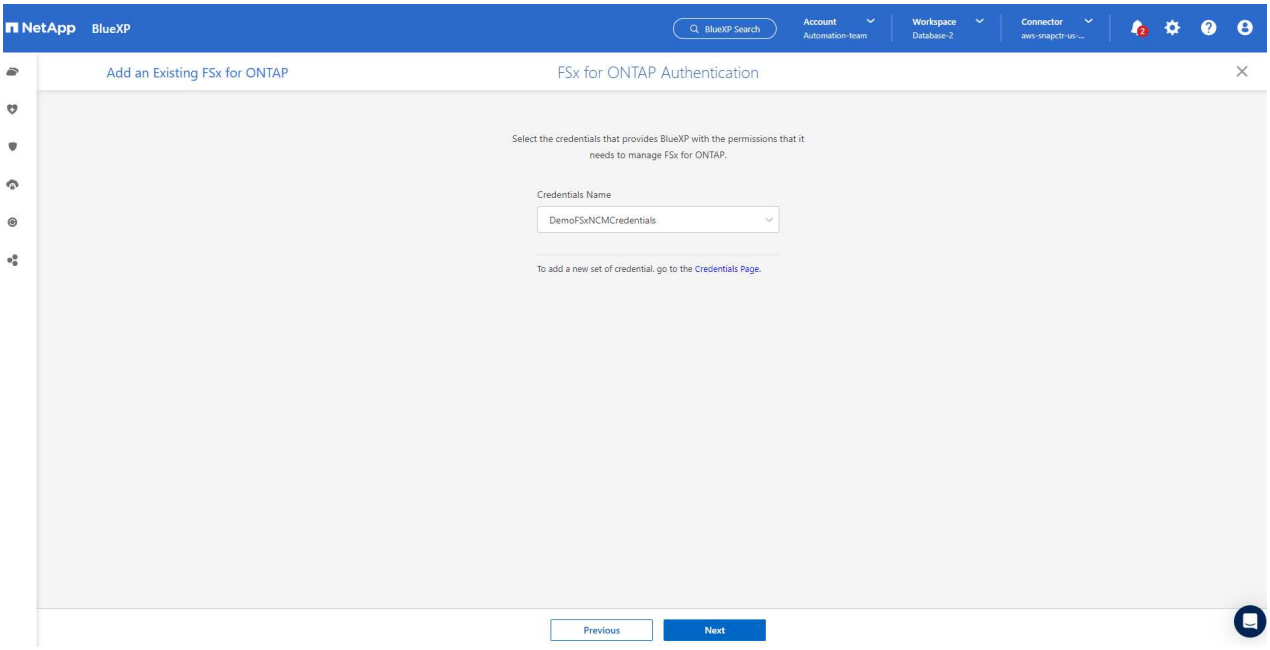
1. Choisissez **Amazon Web Services** comme emplacement.



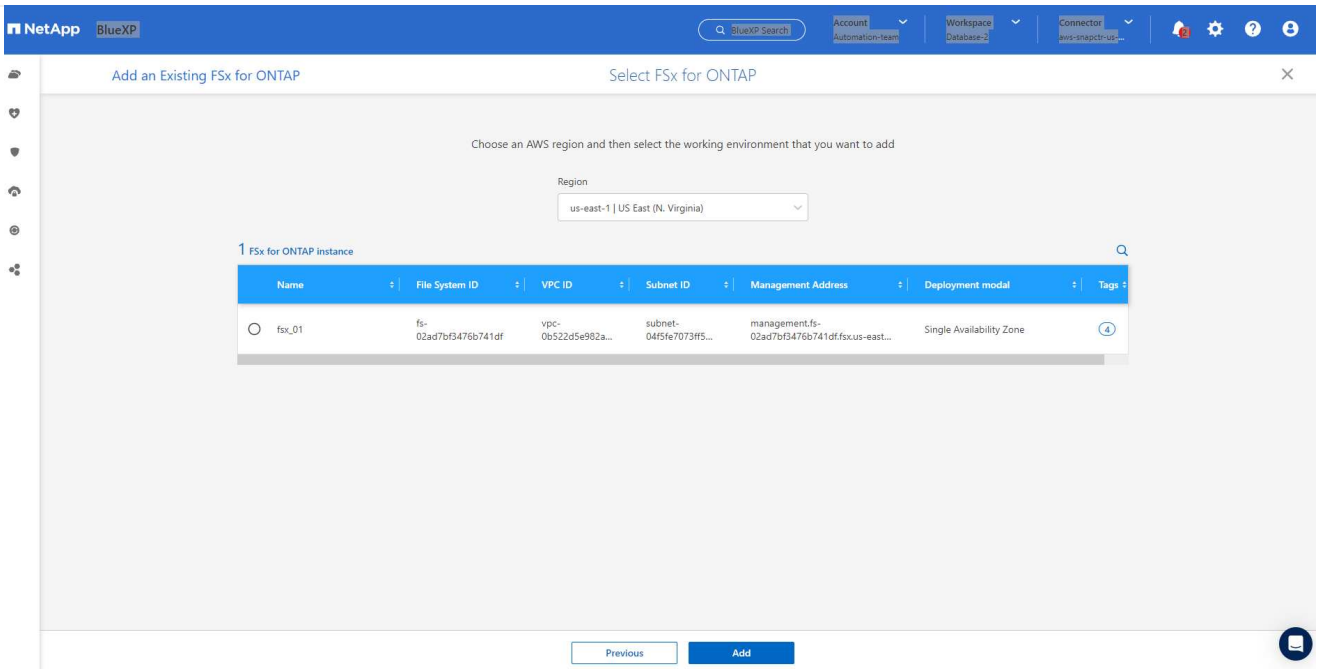
1. Cliquez sur **Découvrir l'existant** à côté de * Amazon FSx ONTAP*.



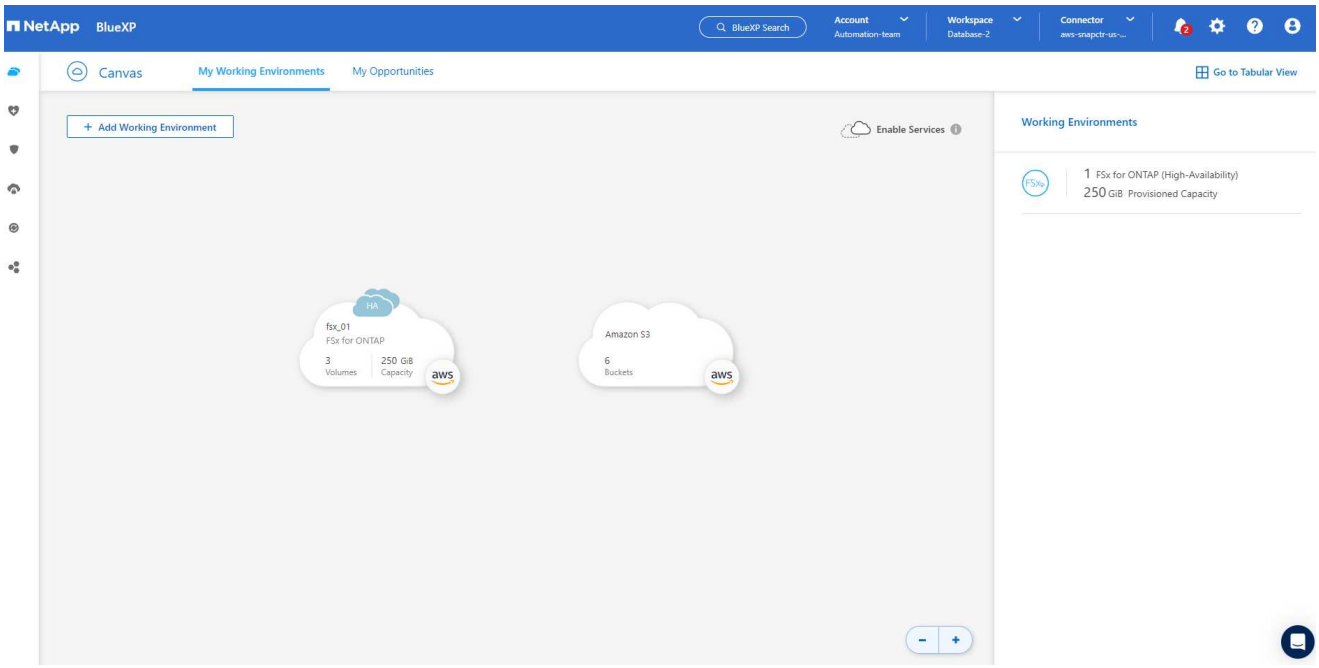
1. Sélectionnez le **Nom des informations d'identification** que vous avez créé dans la section précédente pour accorder à BlueXP les autorisations dont il a besoin pour gérer FSx ONTAP. Si vous n'avez pas ajouté d'informations d'identification, vous pouvez les ajouter à partir du menu **Paramètres**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



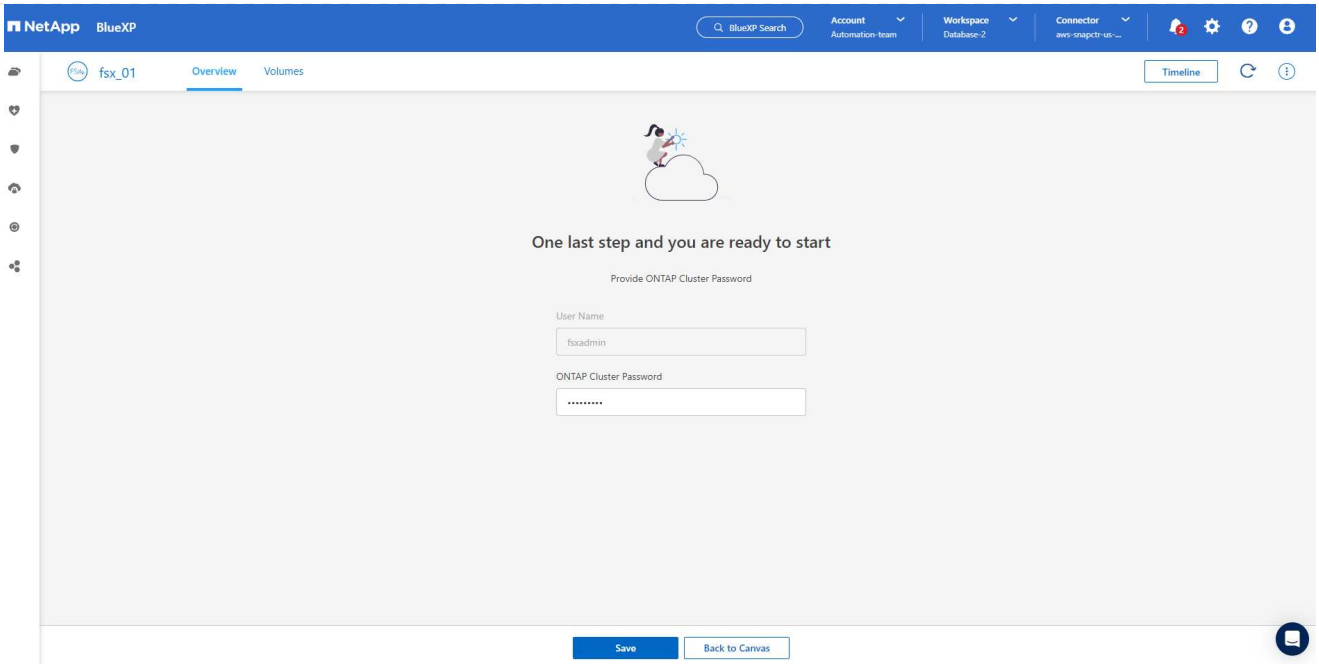
2. Choisissez la région AWS dans laquelle Amazon FSx ONTAP est déployé, sélectionnez le cluster FSx qui héberge la base de données Oracle et cliquez sur Ajouter.



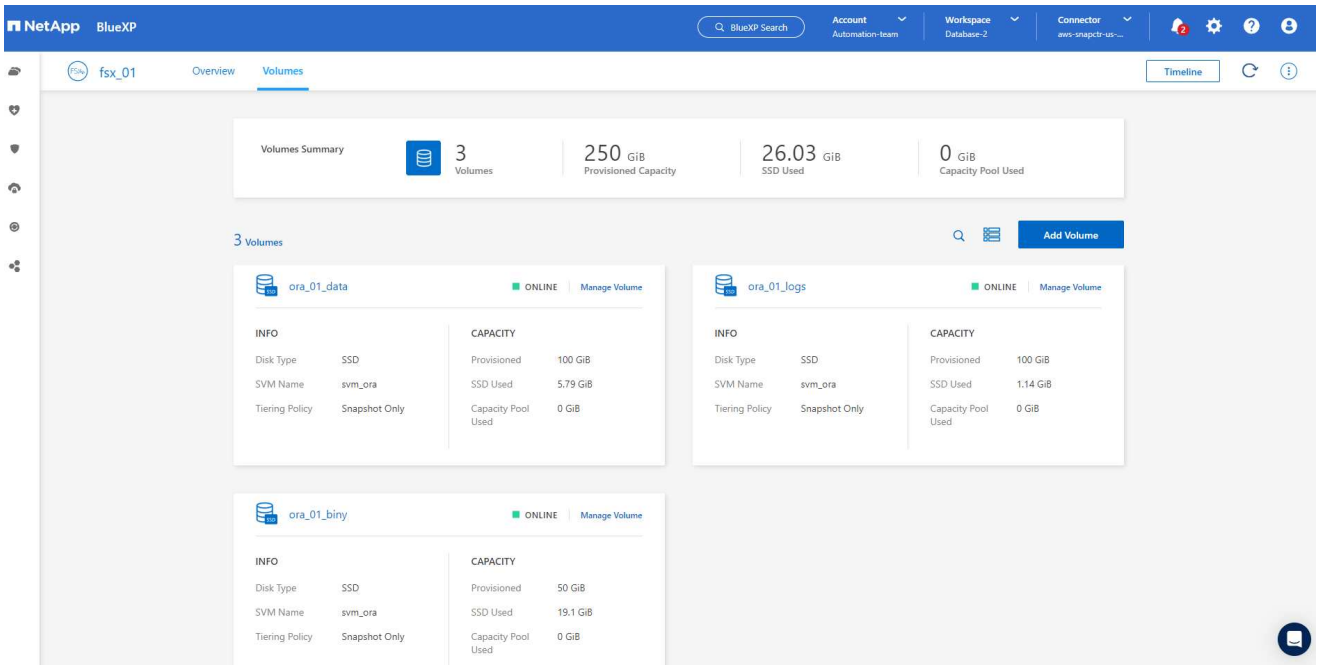
1. L’instance Amazon FSx ONTAP découverte apparaît désormais dans l’environnement de travail.



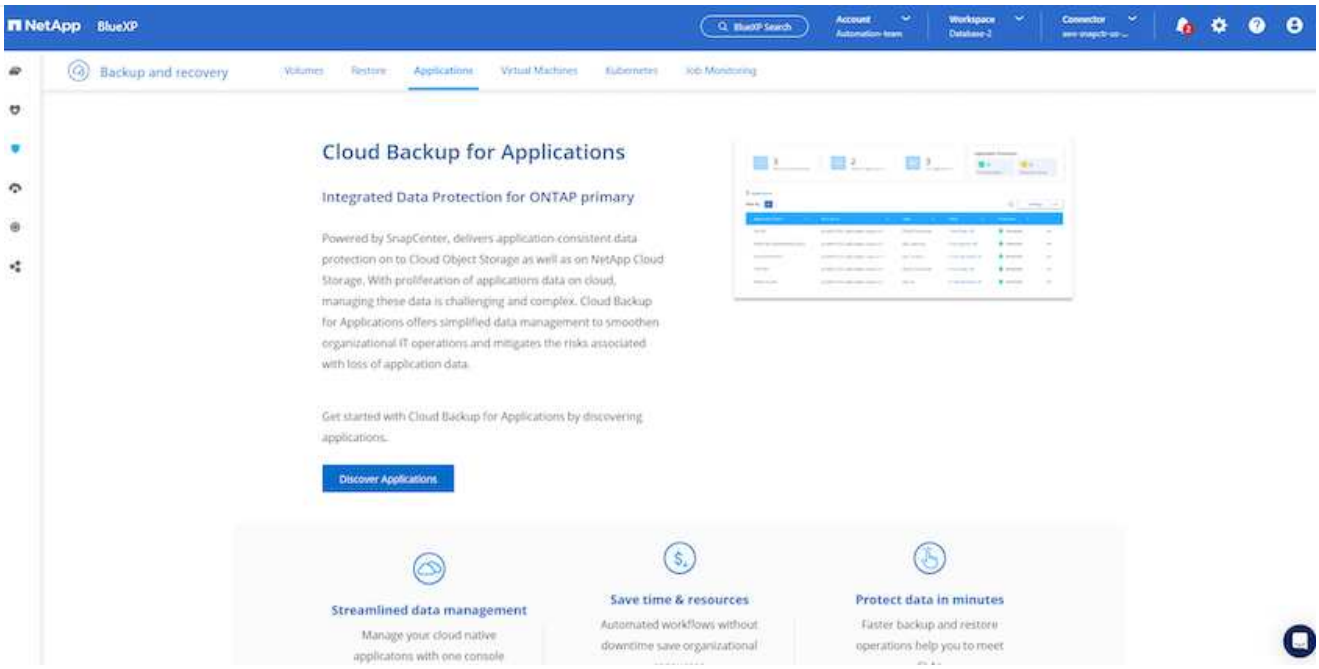
1. Vous pouvez vous connecter au cluster FSx avec les informations d’identification de votre compte fsxadmin.



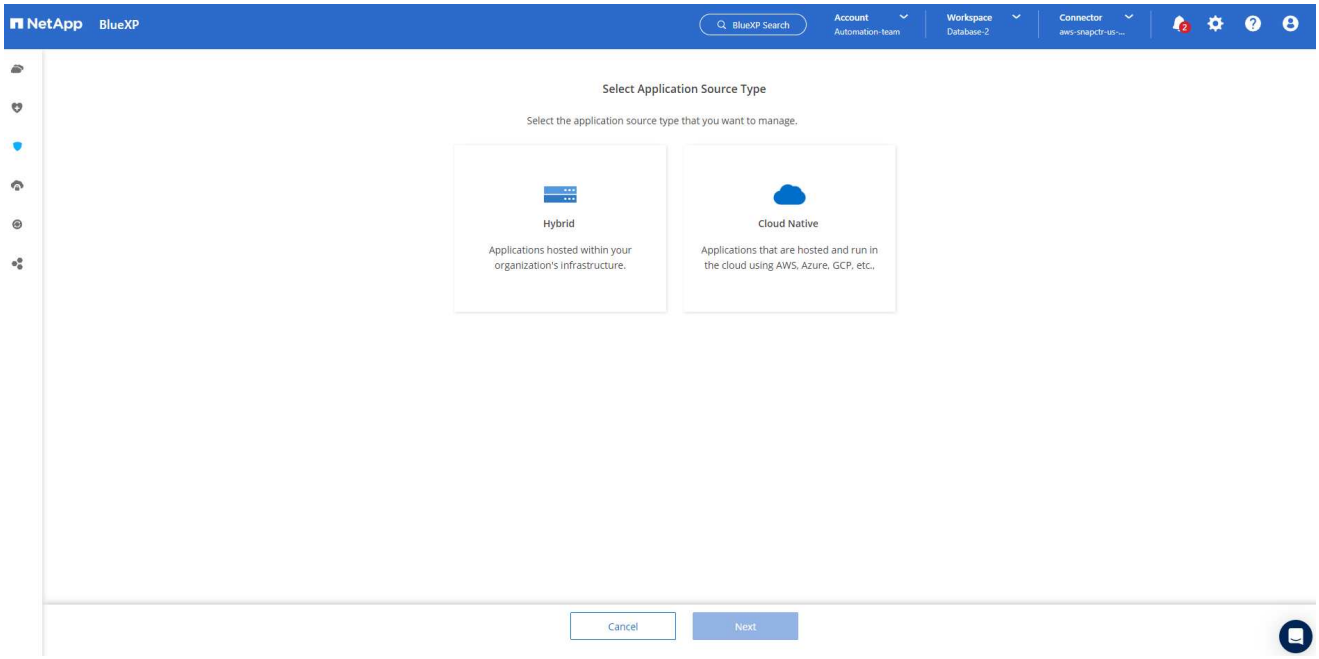
1. Après vous être connecté à Amazon FSx ONTAP, vérifiez les informations de stockage de votre base de données (telles que les volumes de base de données).



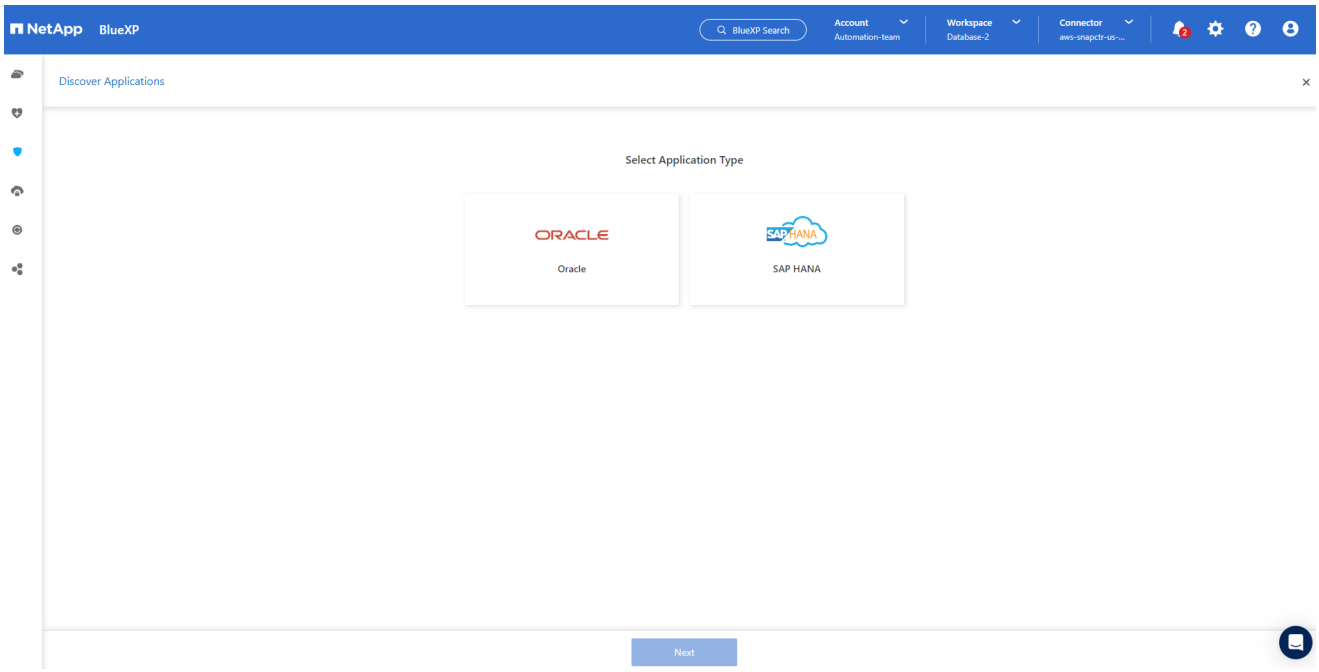
1. Dans la barre latérale gauche de la console, passez votre souris sur l'icône de protection, puis cliquez sur **Protection** > **Applications** pour ouvrir la page de lancement des applications. Cliquez sur **Découvrir les applications**.



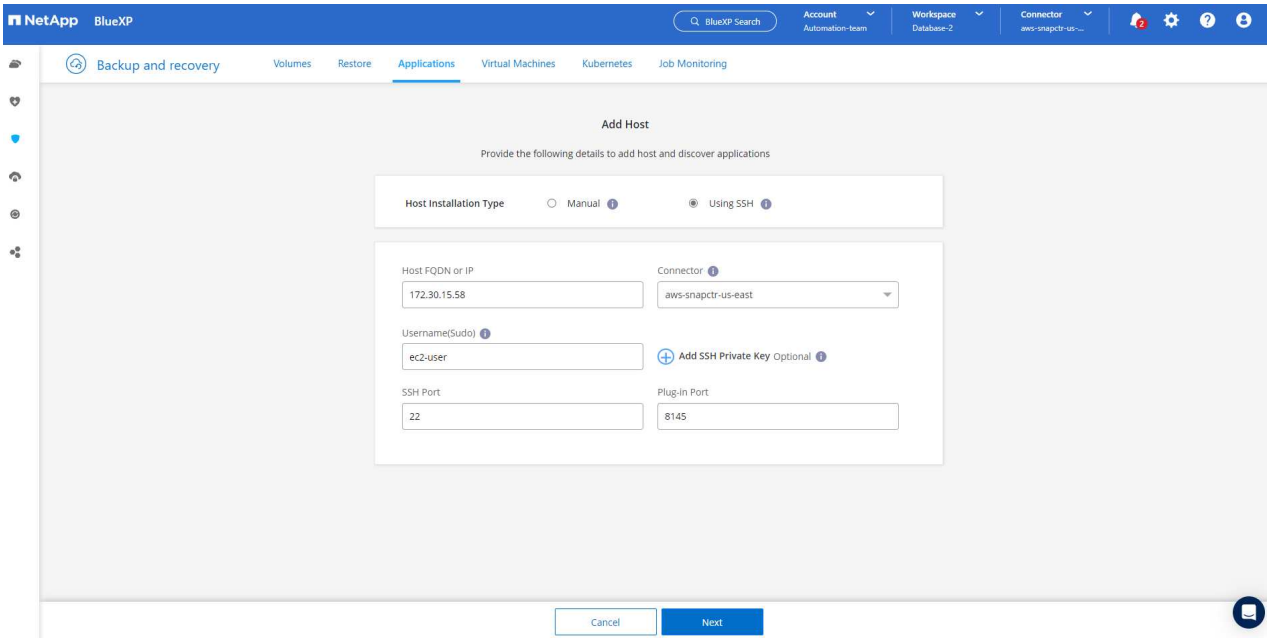
1. Sélectionnez **Cloud Native** comme type de source d'application.



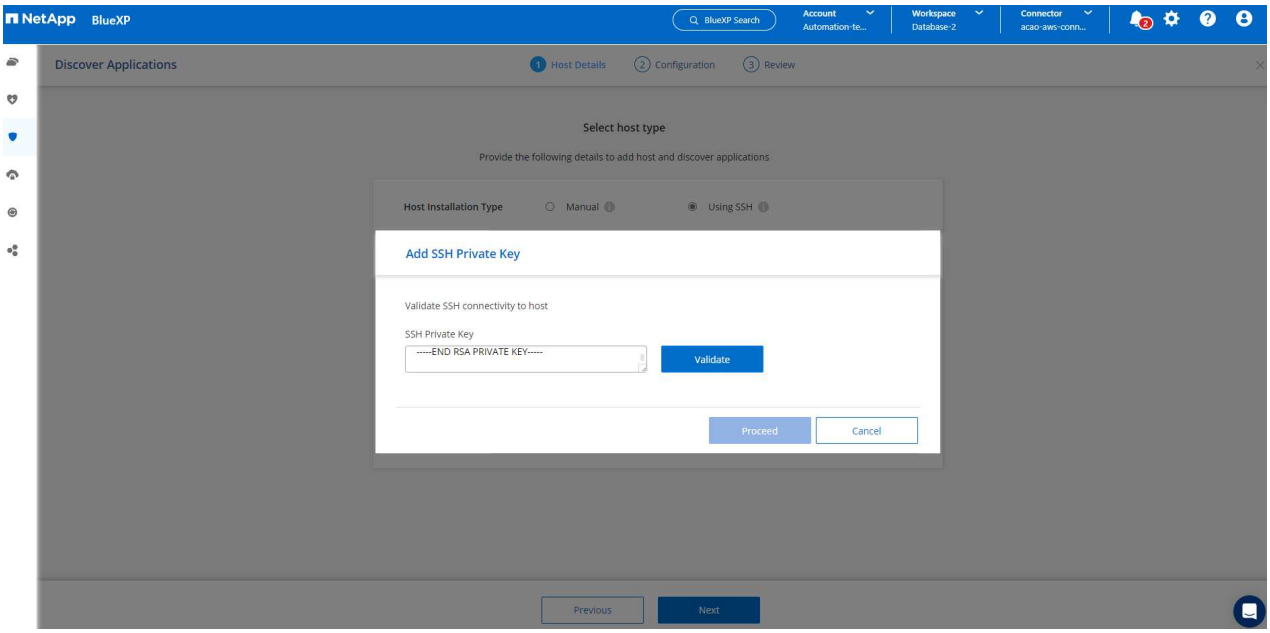
1. Choisissez **Oracle** comme type d'application.



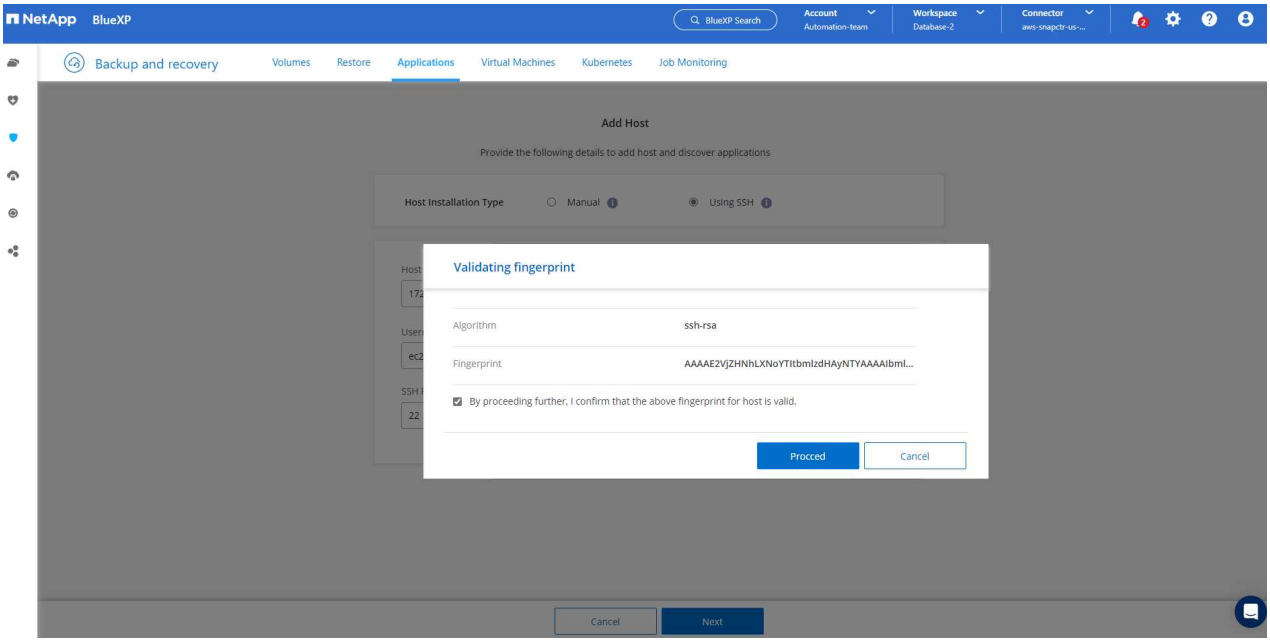
1. Remplissez les détails de l'hôte de l'application Oracle AWS EC2. Choisissez **Utilisation de SSH** comme **Type d'installation de l'hôte** pour l'installation du plug-in en une étape et la découverte de la base de données. Ensuite, cliquez sur **Ajouter une clé privée SSH**.



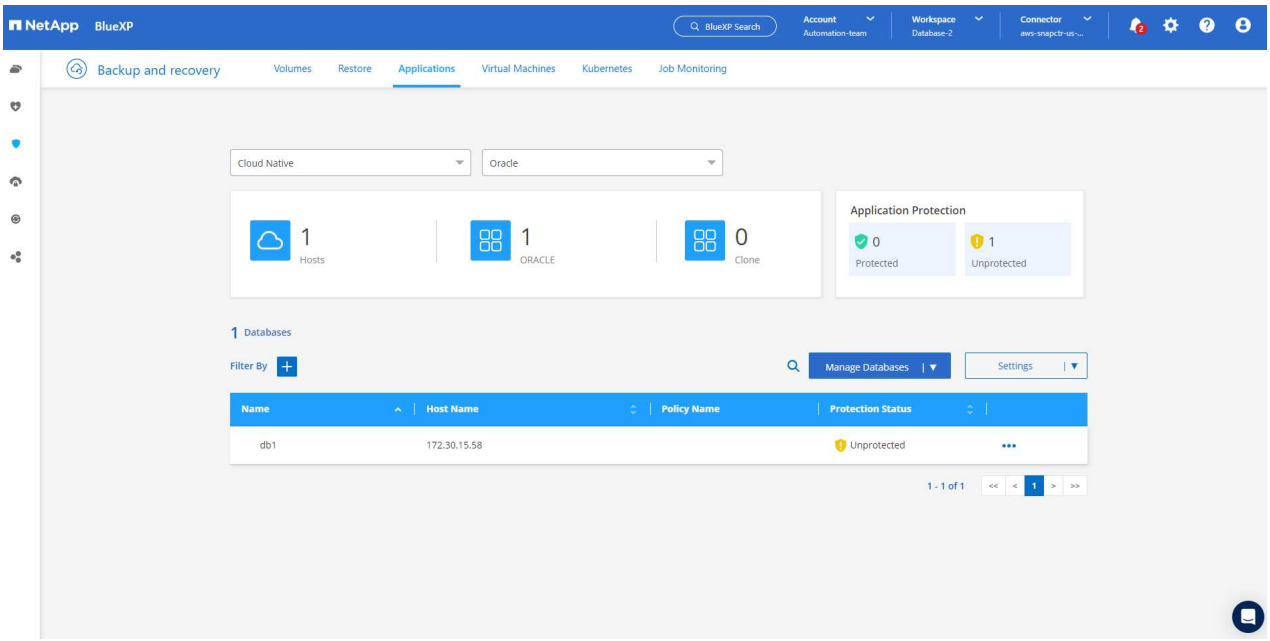
2. Collez votre clé SSH ec2-user pour l'hôte EC2 de la base de données et cliquez sur **Valider** pour continuer.



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



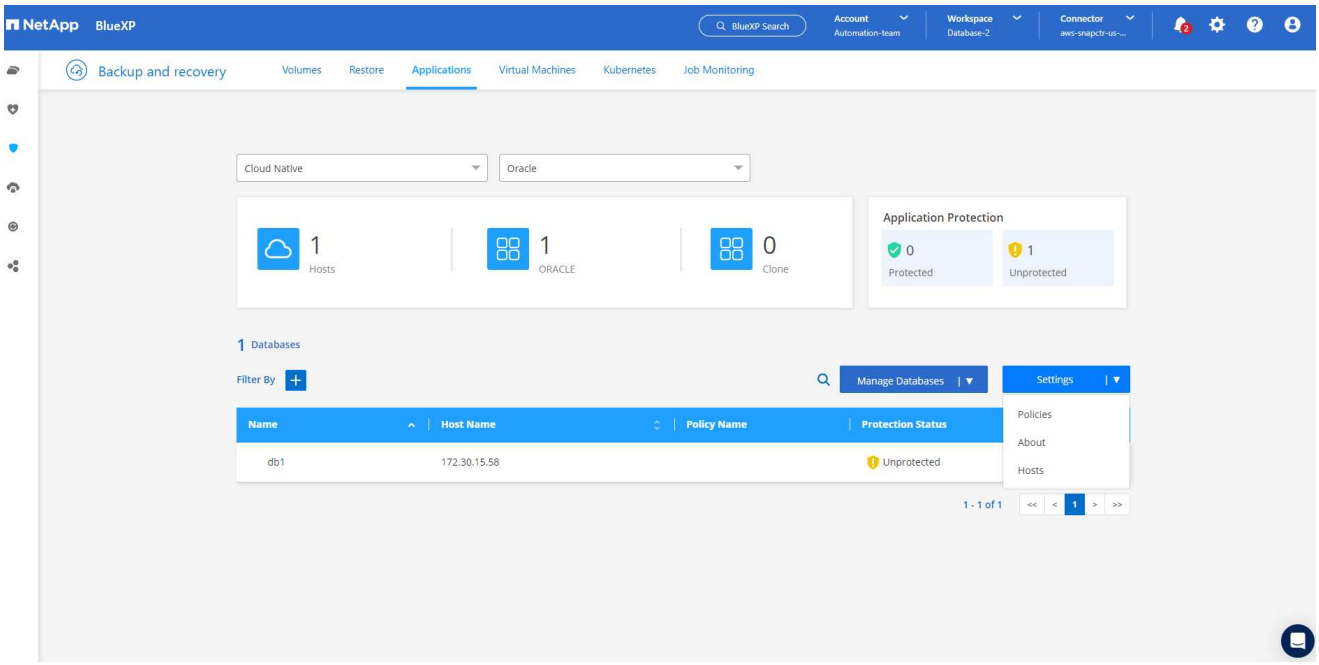
4. Cliquez sur **Suivant** pour installer un plugin de base de données Oracle et découvrir les bases de données Oracle sur l'hôte EC2. Les bases de données découvertes sont ajoutées aux **Applications**. La base de données **État de protection** s'affiche comme **Non protégée** lors de sa découverte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



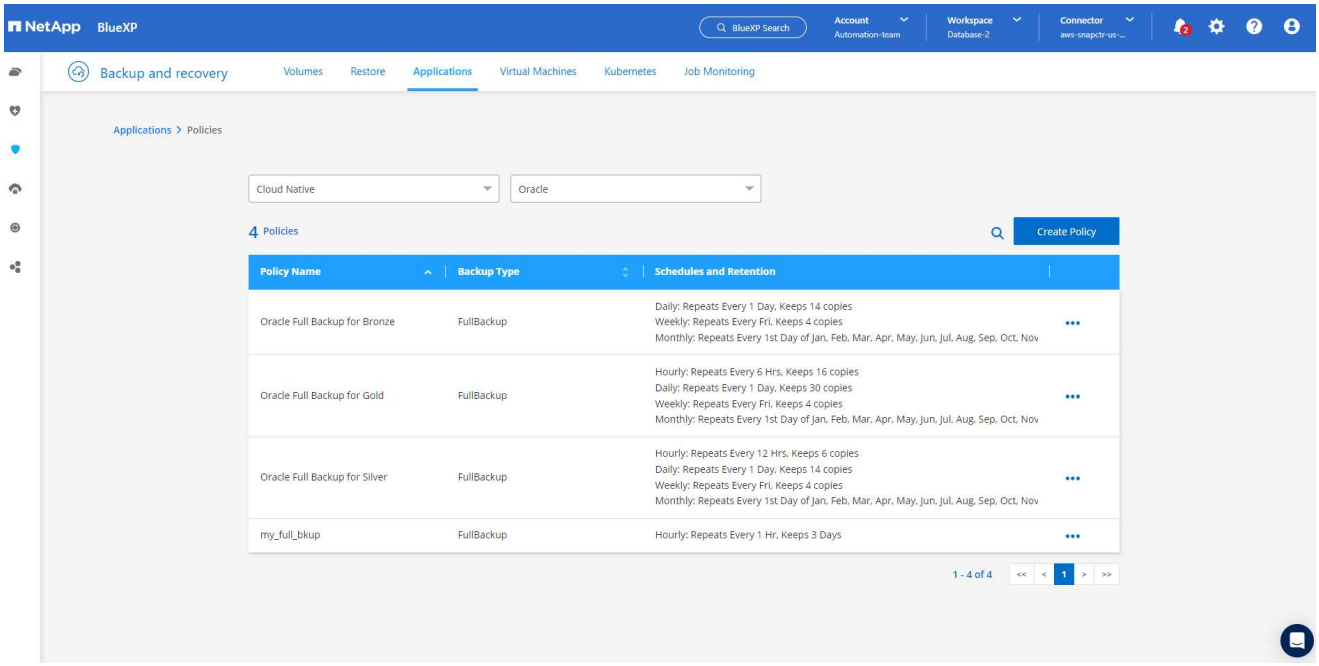
Ceci termine la configuration initiale des services SnapCenter pour Oracle. Les trois sections suivantes de ce document décrivent les opérations de sauvegarde, de restauration et de clonage de la base de données Oracle.

Sauvegarde de la base de données Oracle

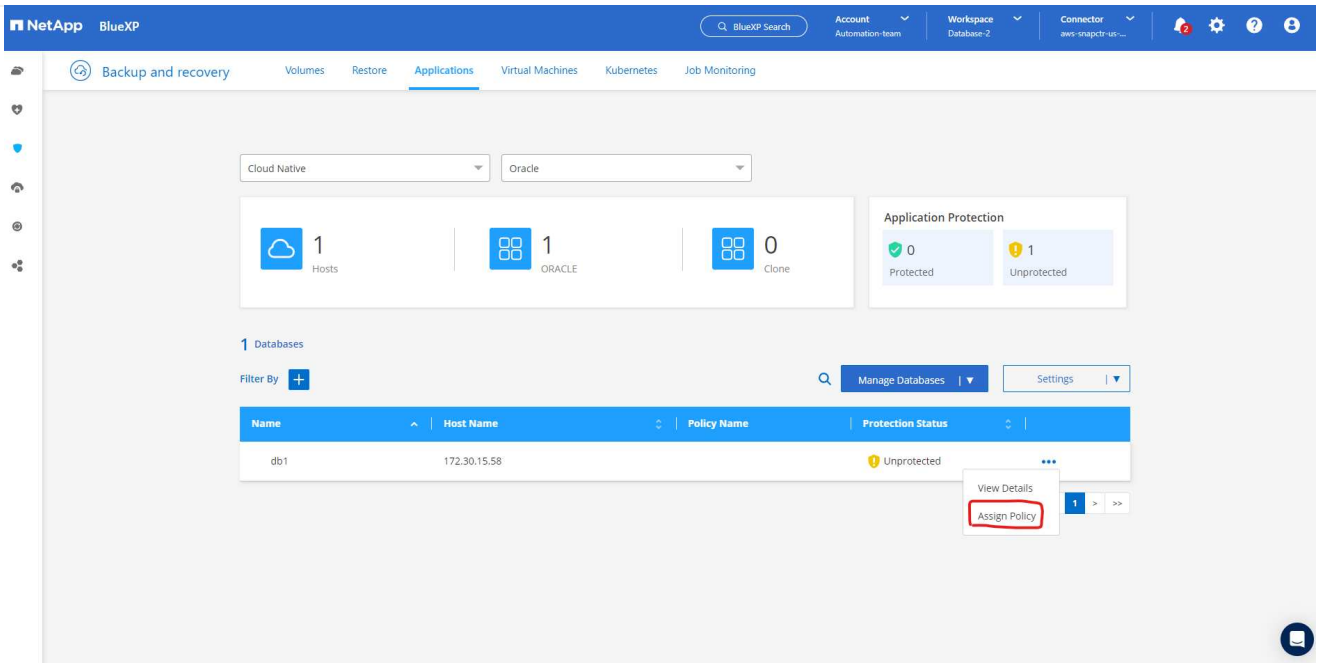
1. Cliquez sur les trois points à côté de l'état de protection de la base de données, puis cliquez sur **Stratégies** pour afficher les stratégies de protection de base de données préchargées par défaut qui peuvent être appliquées pour protéger vos bases de données Oracle.



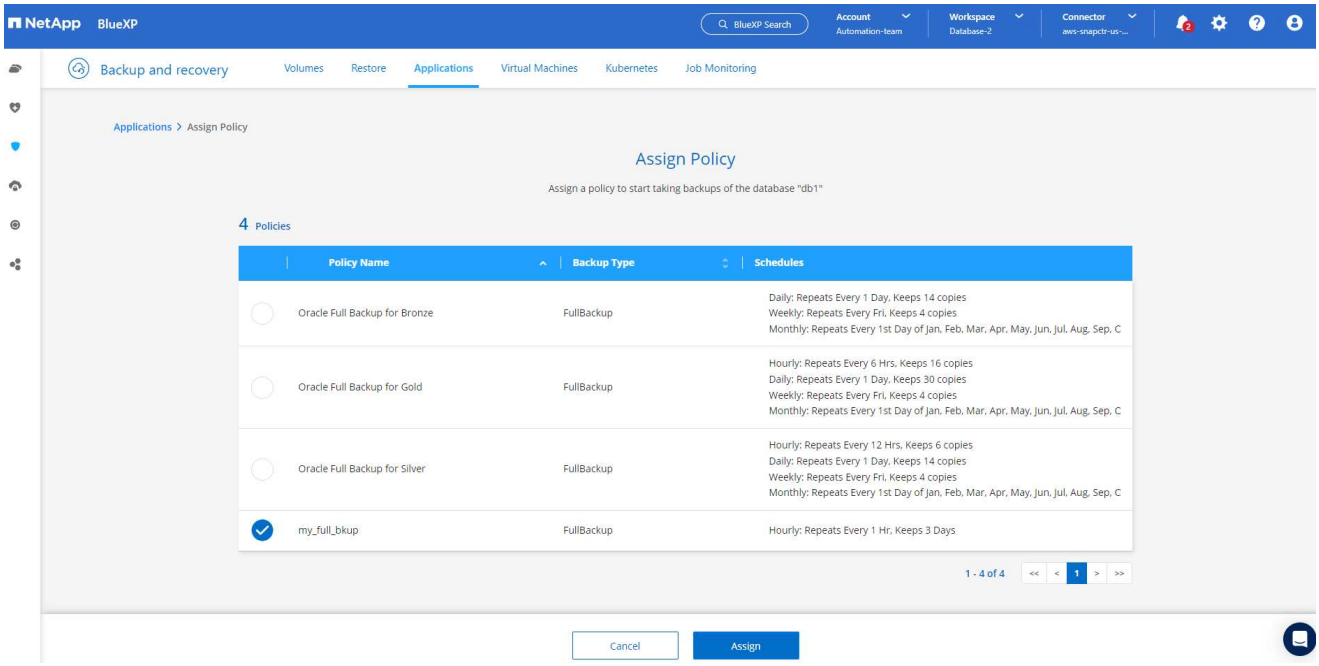
1. Vous pouvez également créer votre propre politique avec une fréquence de sauvegarde personnalisée et une fenêtre de conservation des données de sauvegarde.



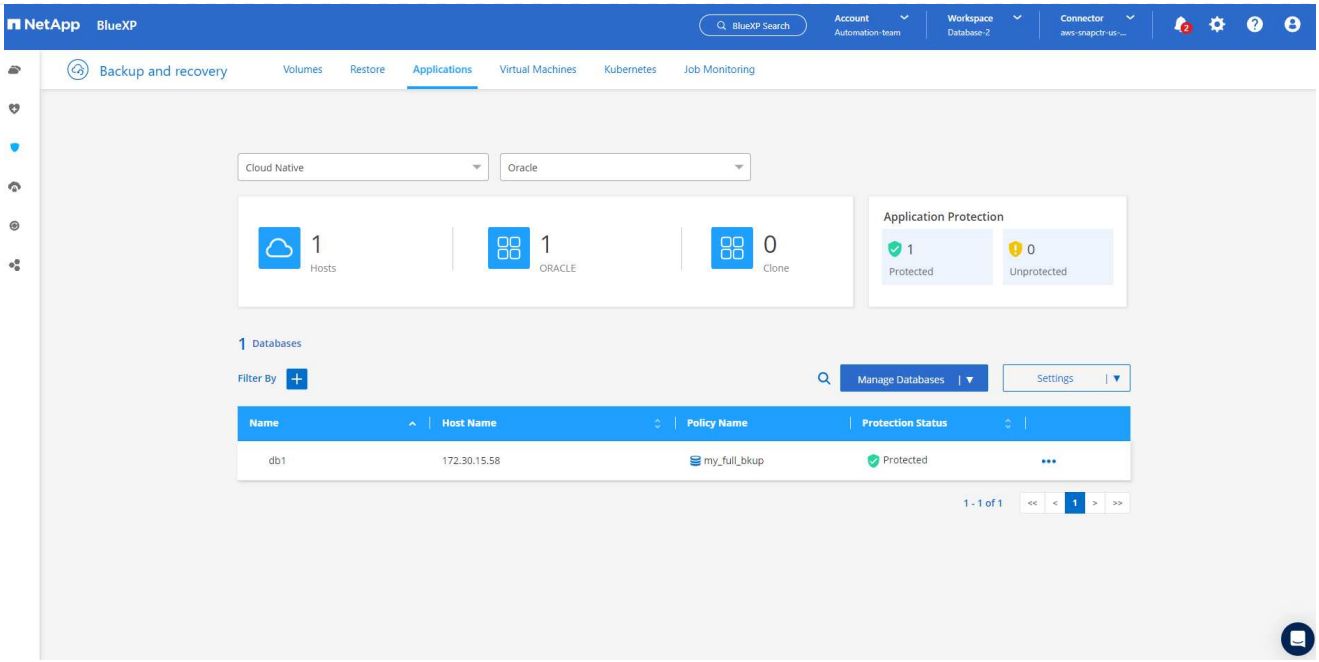
1. Lorsque vous êtes satisfait de la configuration de la politique, vous pouvez ensuite attribuer la politique de votre choix pour protéger la base de données.



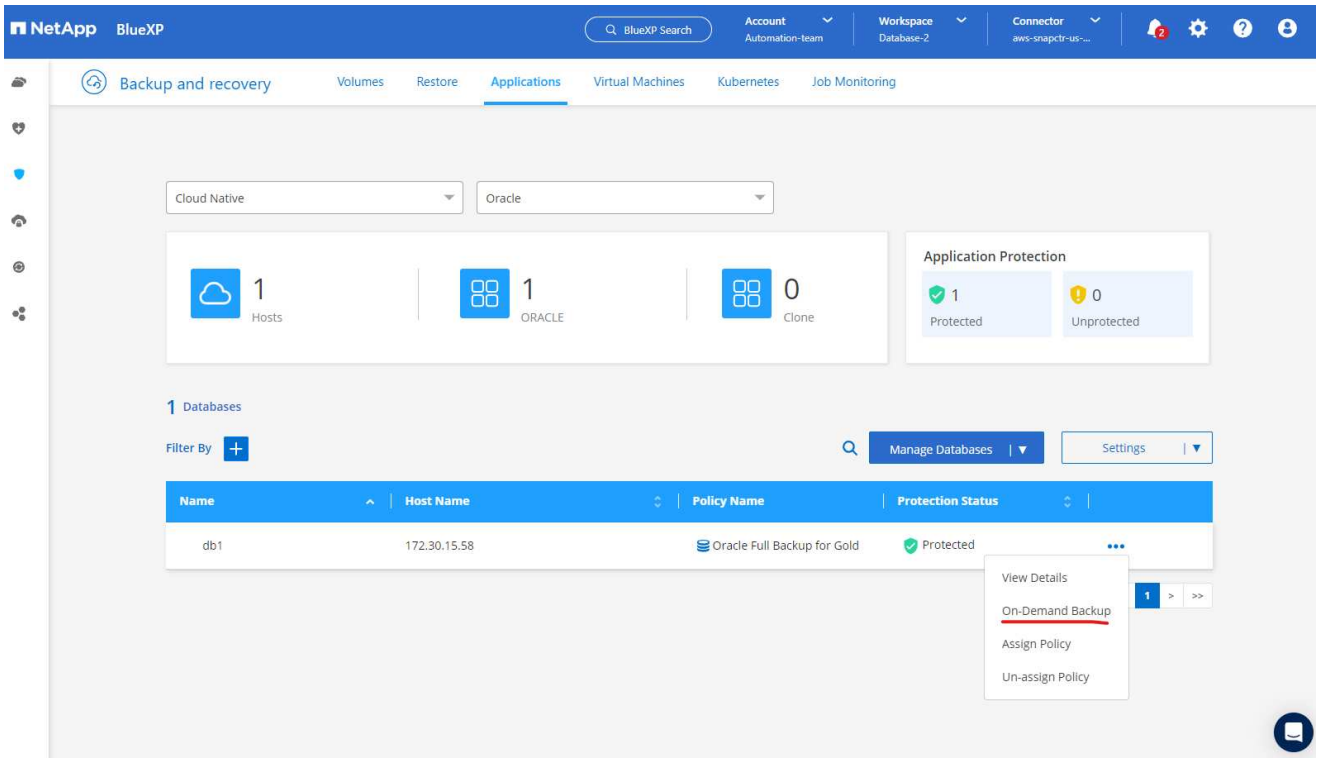
1. Choisissez la politique à attribuer à la base de données.



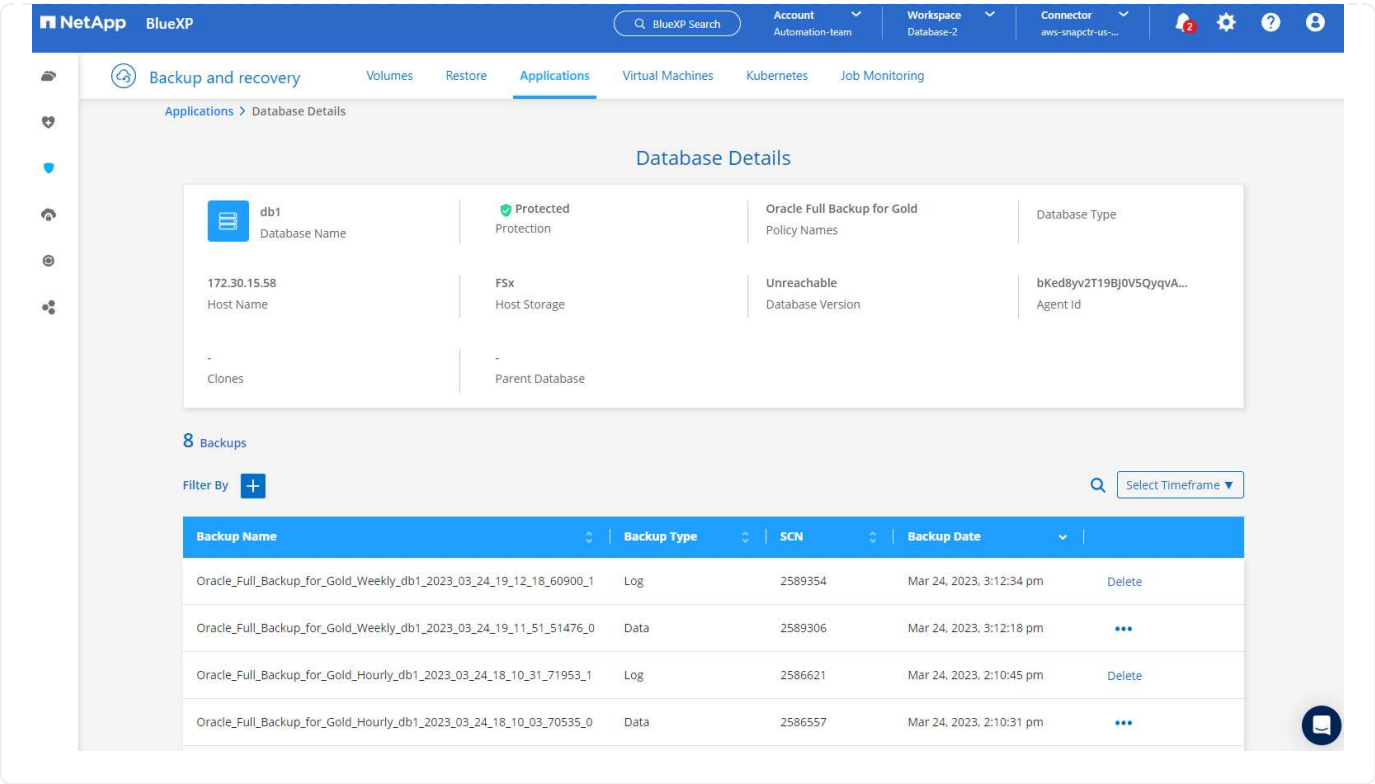
1. Une fois la politique appliquée, l'état de protection de la base de données est passé à **Protégé** avec une coche verte.



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.

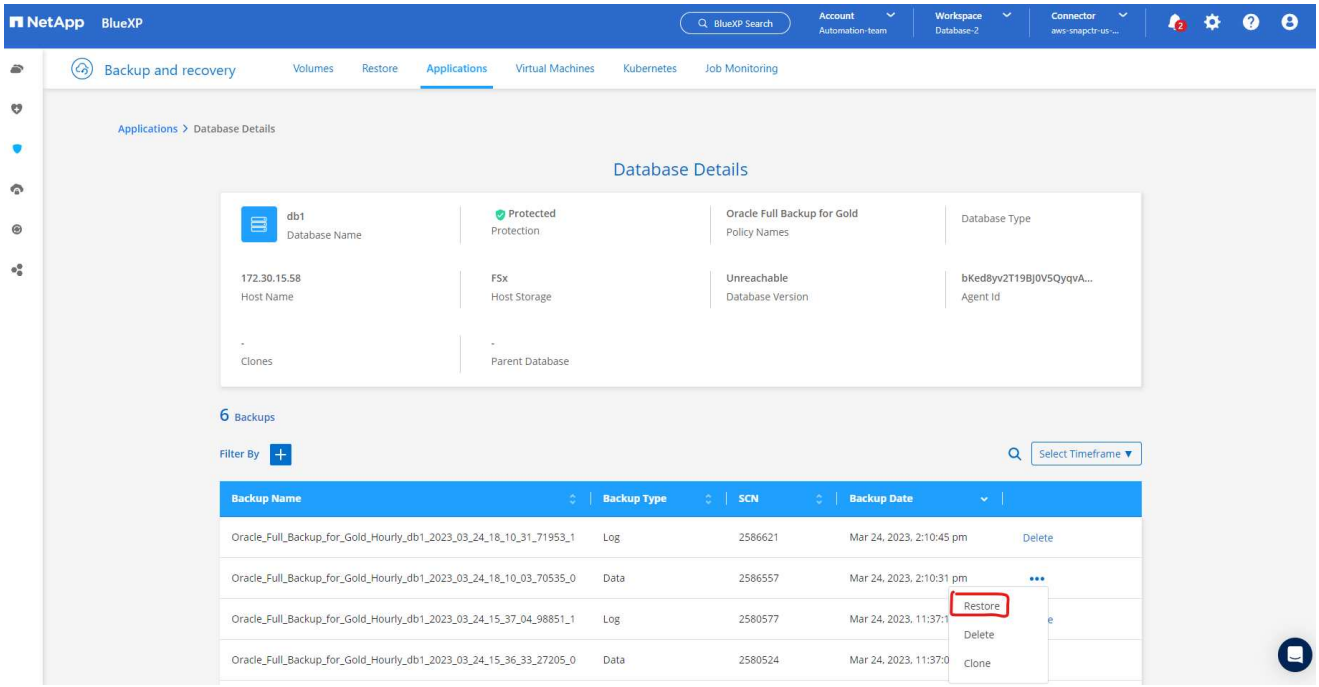


1. Les détails des sauvegardes de la base de données peuvent être consultés en cliquant sur **Afficher les détails** dans la liste du menu. Cela inclut le nom de la sauvegarde, le type de sauvegarde, le SCN et la date de sauvegarde. Un ensemble de sauvegarde couvre un instantané du volume de données 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.

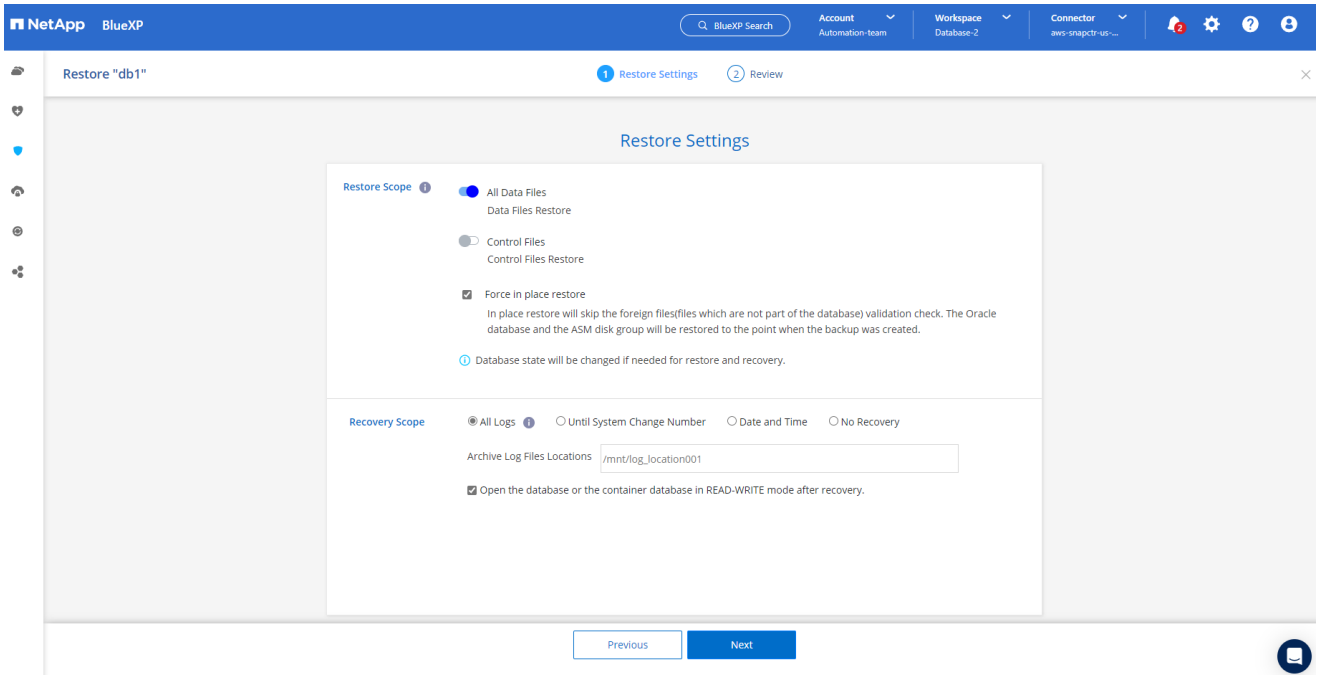


Restauration et récupération de bases de données Oracle

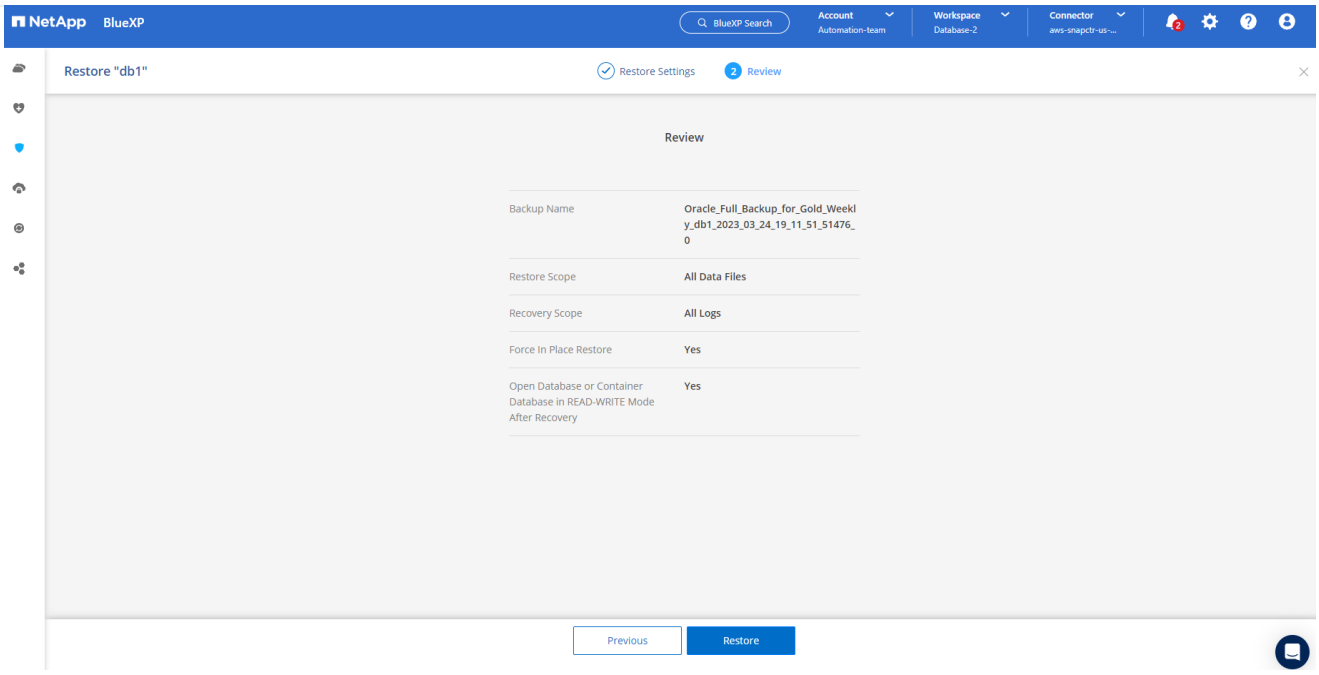
1. Pour une restauration de base de données, choisissez la bonne sauvegarde, soit par le SCN, soit par l'heure de sauvegarde. Cliquez sur les trois points de la sauvegarde des données de la base de données, puis cliquez sur **Restaurer** pour lancer la restauration et la récupération de la base de données.



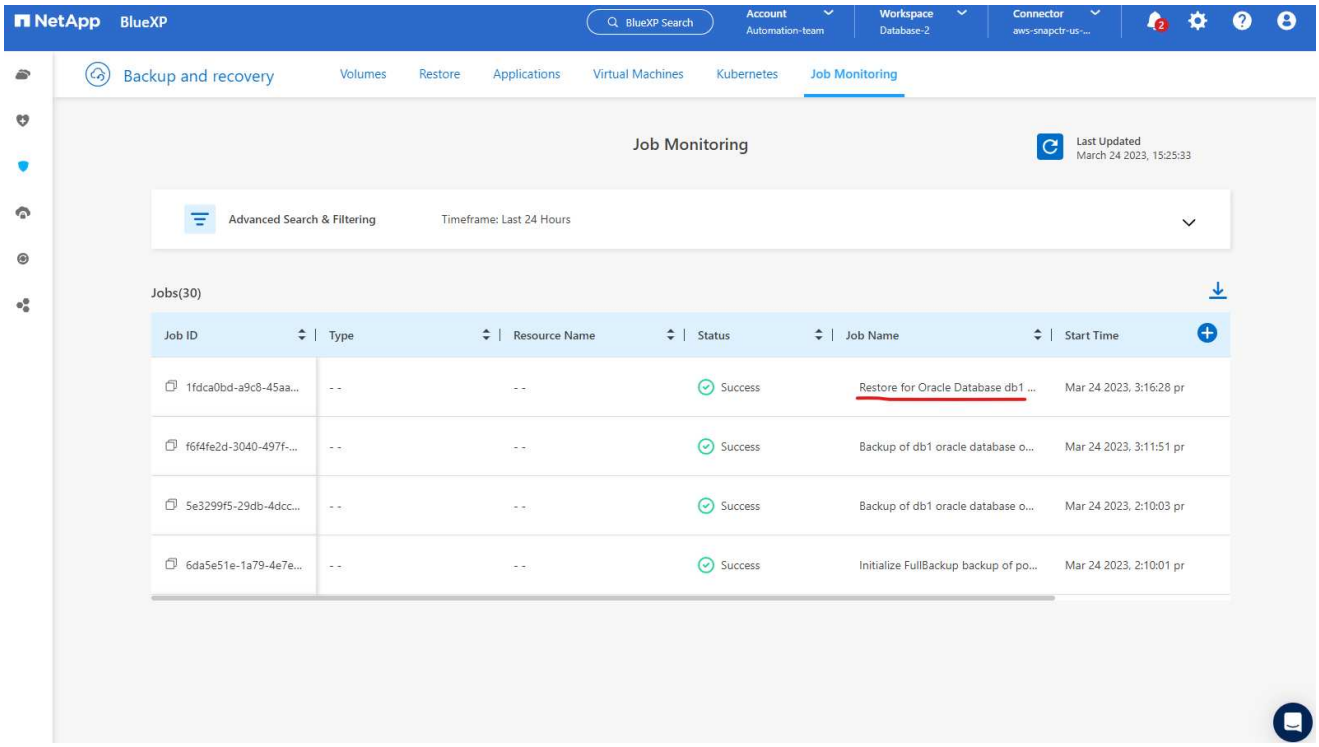
1. Choisissez votre paramètre de restauration. Si vous êtes sûr que rien n'a changé dans la structure physique de la base de données après la sauvegarde (comme l'ajout d'un fichier de données ou d'un groupe de disques), vous pouvez utiliser l'option **Forcer la restauration sur place**, qui est généralement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

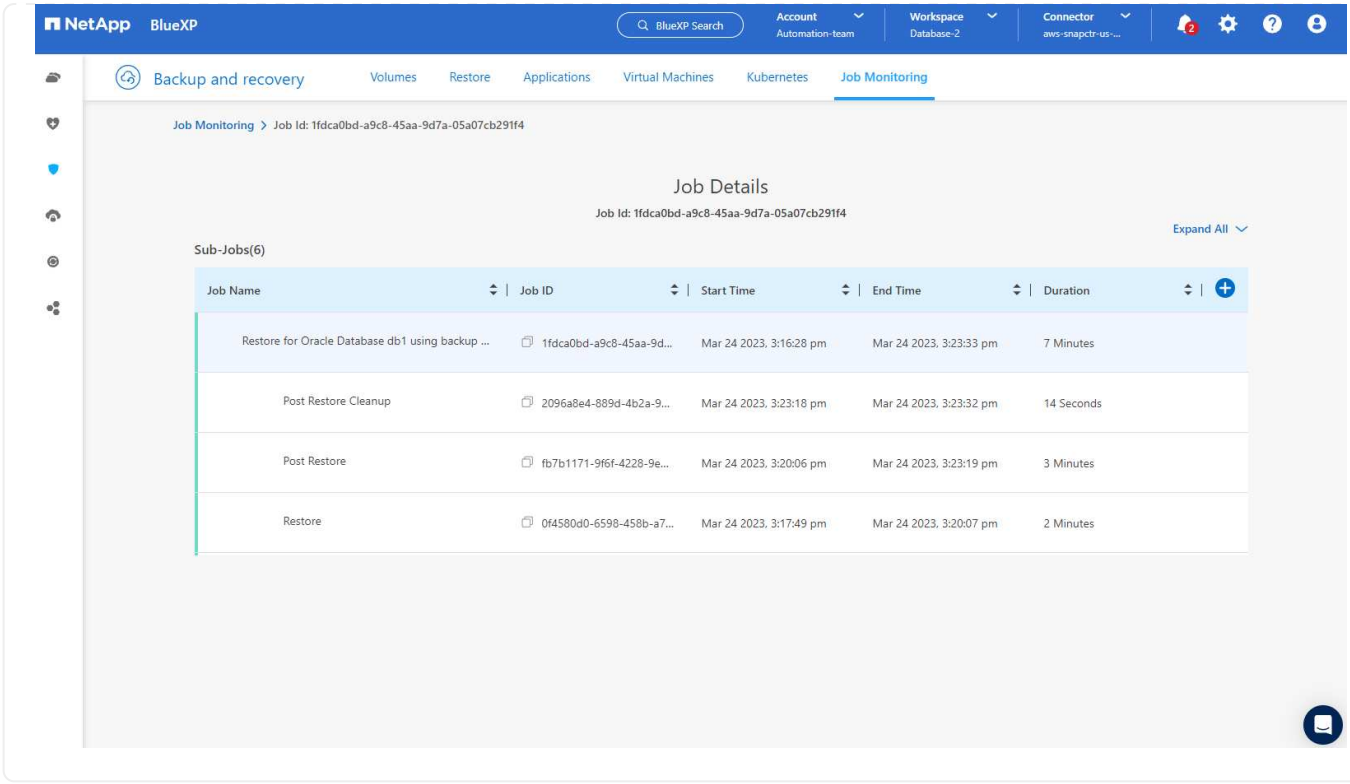


1. Examinez et démarrez la restauration et la récupération de la base de données.



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.

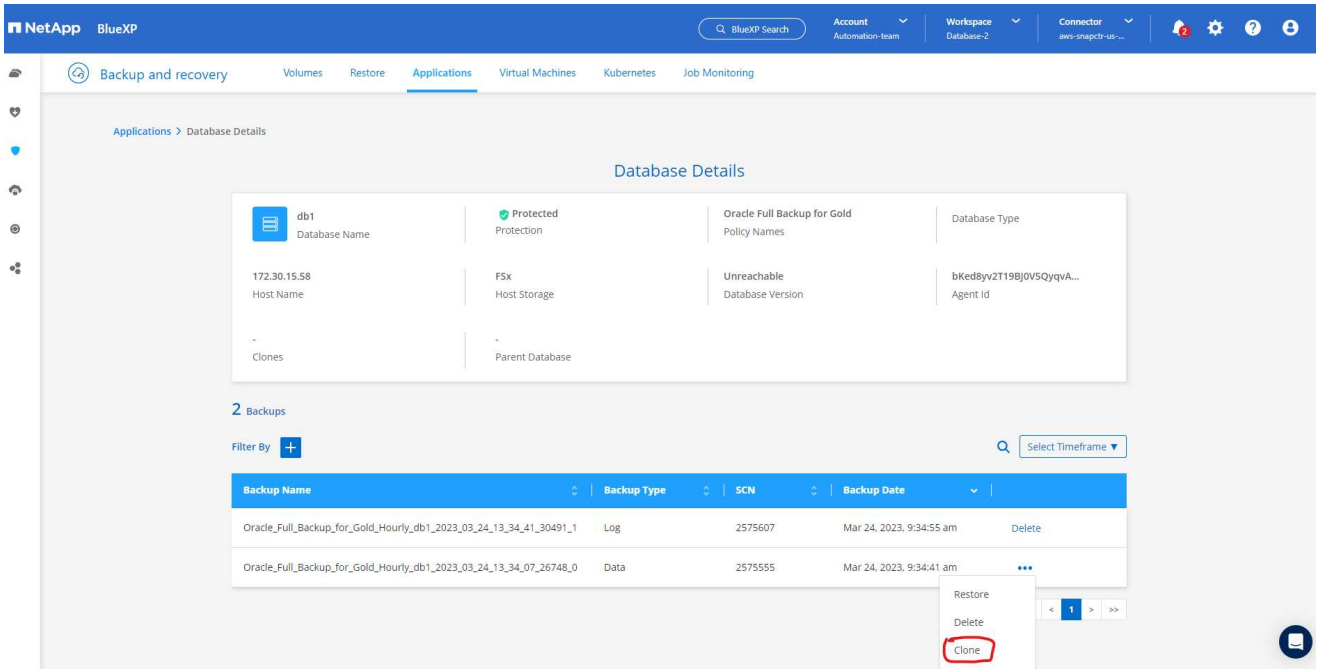




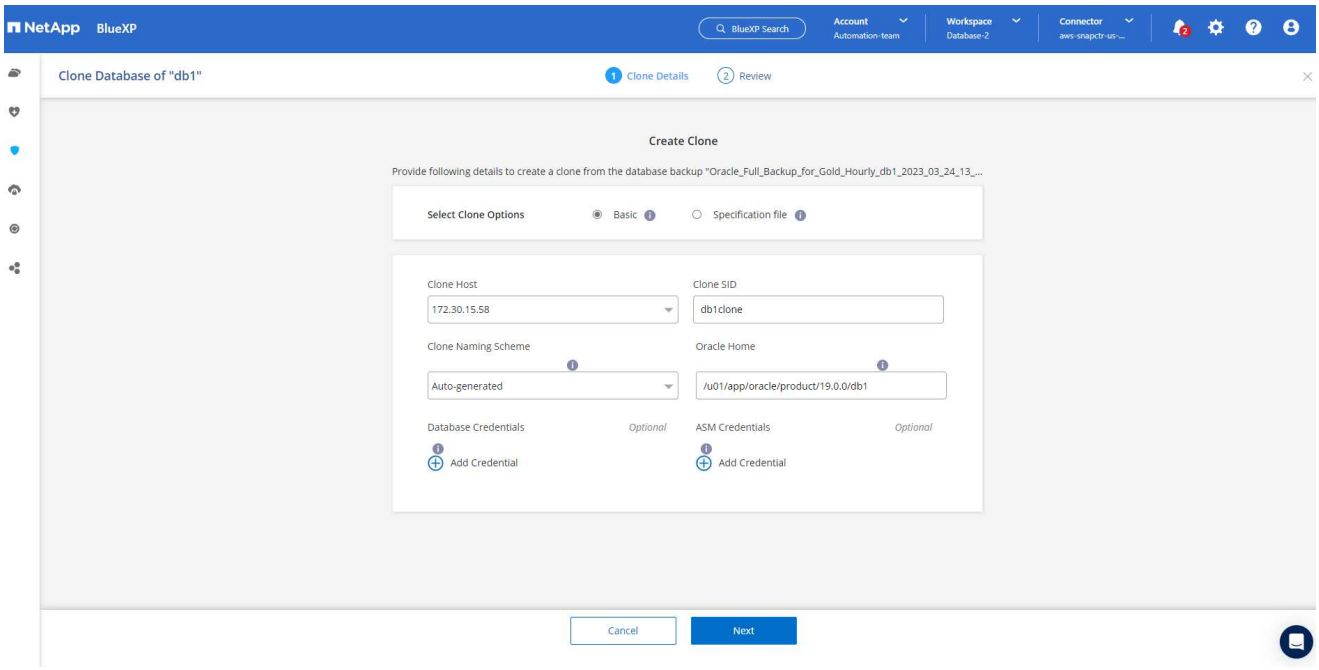
Clonage de base de données Oracle

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.

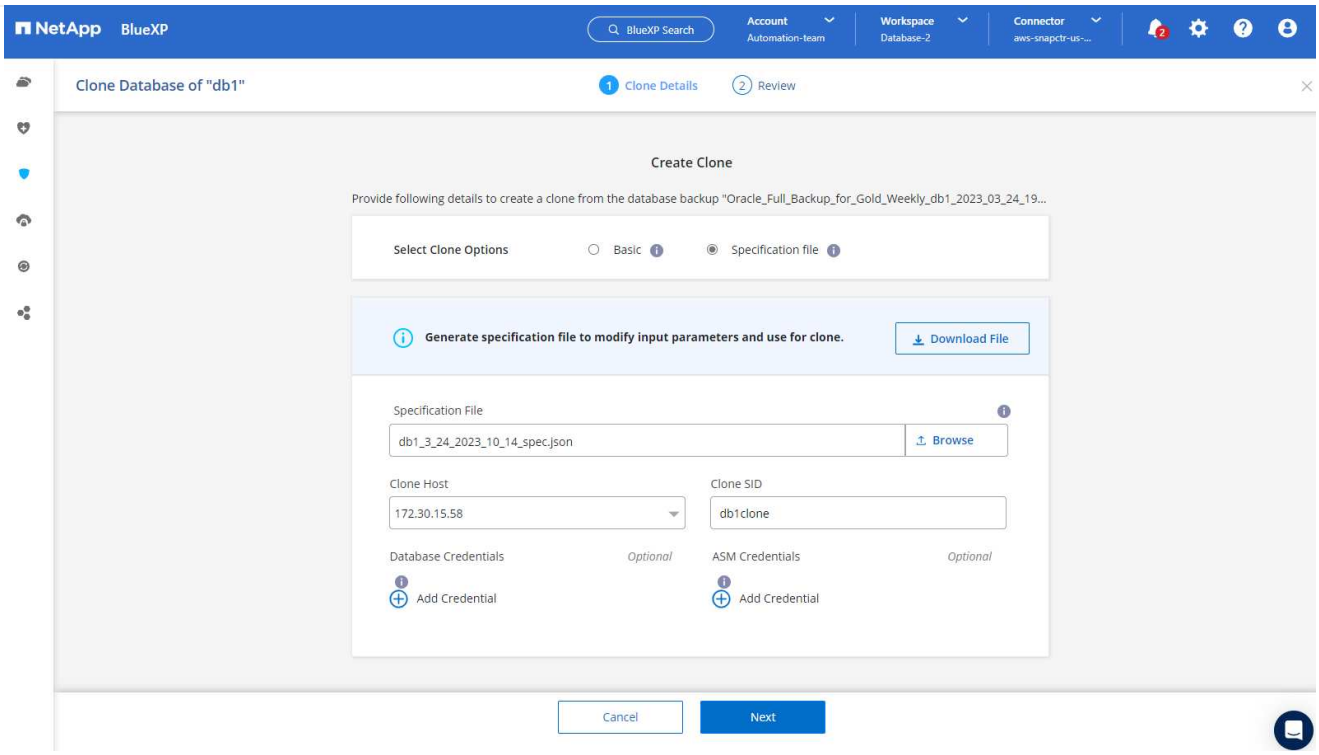
1. Sélectionnez la bonne copie de sauvegarde de la base de données, cliquez sur les trois points pour afficher le menu et choisissez l'option **Cloner**.



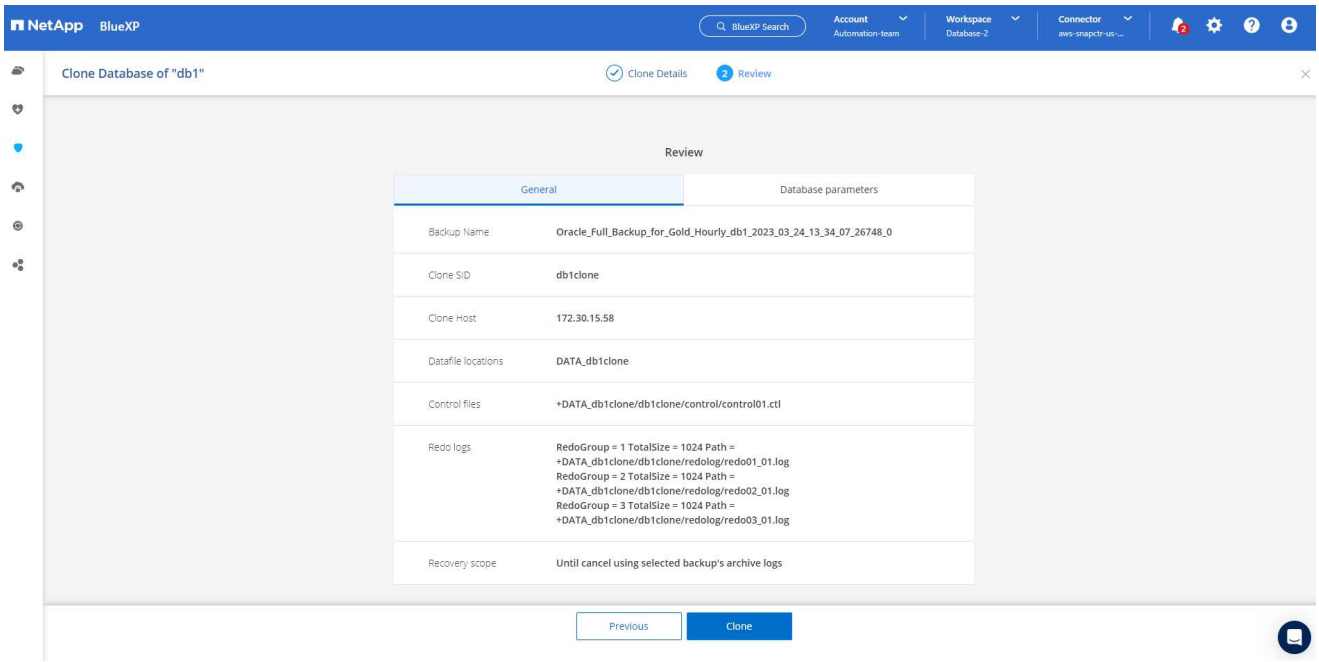
1. Sélectionnez l'option **Basique** si vous n'avez pas besoin de modifier les paramètres de la base de données clonée.



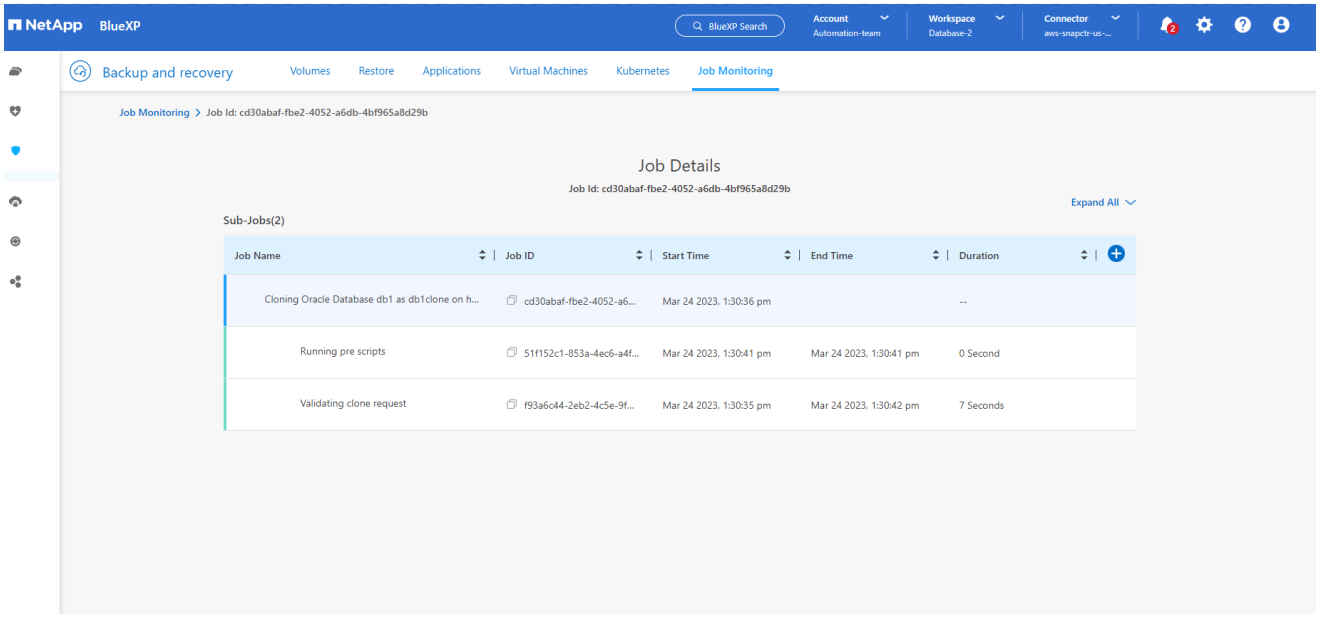
1. Vous pouvez également sélectionner **Fichier de spécifications**, ce qui vous donne la possibilité de télécharger le fichier d'initialisation actuel, d'y apporter des modifications, puis de le télécharger à nouveau dans le travail.



1. Révisez et lancez le travail.



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



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/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                               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$database;

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"

- Documentation de BlueXP backup and recovery

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

- Amazon FSx 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=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2