TR-4977 : Sauvegarde, restauration et clonage de bases de données Oracle avec SnapCenter Services – Azure

NetApp database solutions

NetApp
August 18, 2025

Sommaire

TR-4977 : Sauvegarde, restauration et clonage de bases de données Oracle avec SnapCenter Services – Azure

Allen Cao, Niyaz Mohamed, NetApp

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 .

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 cloud et de protection des données NetApp pour les bases de données telles qu'Oracle et HANA exécutées sur Azure NetApp Files. 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 SnapCenter Services pour sauvegarder, restaurer et cloner des bases de données Oracle déployées sur des volumes Azure NetApp Files et des instances de calcul Azure. Il est très facile de configurer la protection des données pour la base de données Oracle déployée sur Azure NetApp Files avec l'interface utilisateur BlueXP basée sur le Web.

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde de base de données avec instantanés pour les bases de données Oracle hébergées dans Azure NetApp Files et les machines virtuelles Azure
- Récupération de la base de données Oracle en cas de panne
- Clonage rapide de bases de données primaires pour les environnements de développement, de test ou d'autres cas d'utilisation

Public

Cette solution est destinée aux publics suivants :

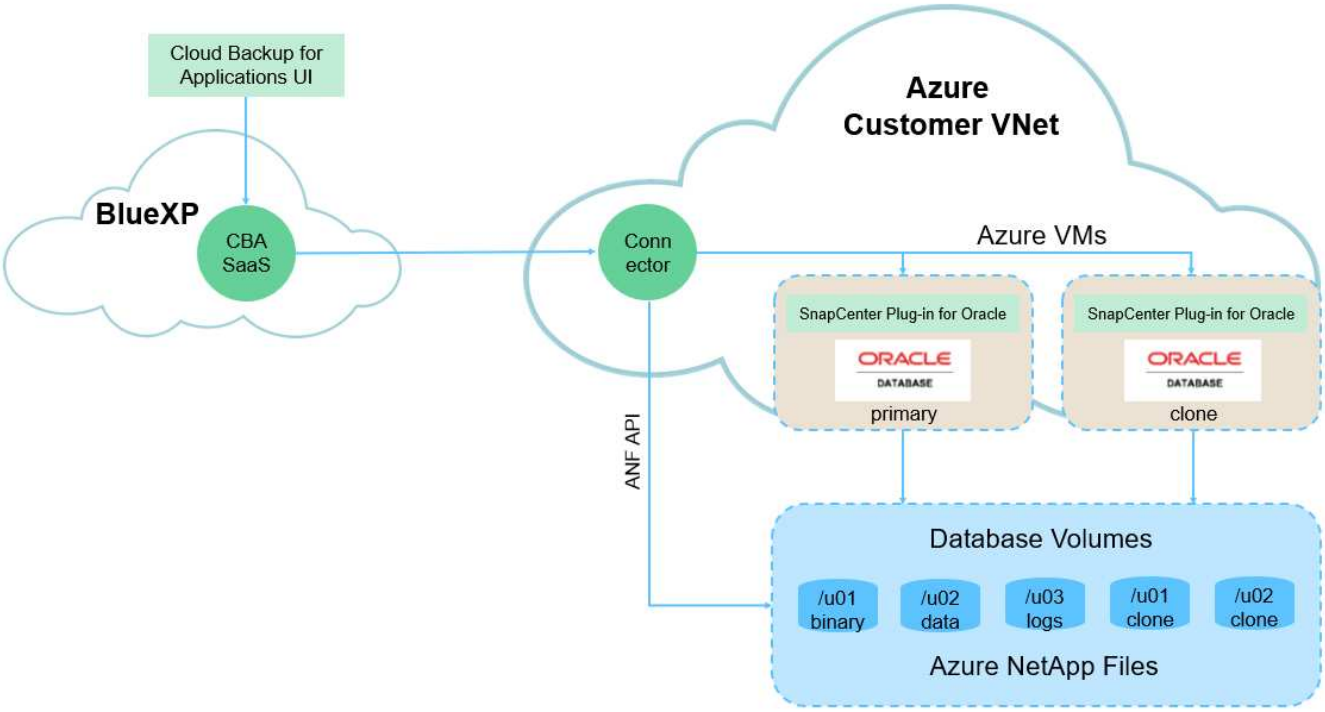
- L'administrateur de base de données qui gère les bases de données Oracle exécutées sur le stockage Azure NetApp Files
- L'architecte de solutions qui souhaite tester la sauvegarde, la restauration et le clonage de bases de données Oracle dans Azure
- L'administrateur de stockage qui prend en charge et gère le stockage Azure NetApp Files
- Le propriétaire de l'application qui possède les applications déployées sur le stockage Azure NetApp Files et les machines virtuelles Azure

Environnement de test et de validation de solutions

Les tests et la validation de cette solution ont été réalisés dans un environnement de laboratoire 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 Azure NetApp Files	Niveau de service Premium	Type de QoS automatique et capacité de stockage de 4 To lors des tests
Instance Azure pour le calcul	Standard B4ms (4 vcpus, 16 Gio de mémoire)	Deux instances déployées, l'une comme serveur de base de données principal et l'autre comme serveur de base de données clone

Logiciel

RedHat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Abonnement RedHat déployé pour les tests
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 v2.5.0-2822	Version de l'agent v2.5.0-2822

Facteurs clés à prendre en compte lors du déploiement

- **Connecteur à déployer dans le même réseau virtuel / sous-réseau que les bases de données et Azure NetApp Files.** Lorsque cela est possible, le connecteur doit être déployé dans les mêmes réseaux virtuels et groupes de ressources Azure, ce qui permet la connectivité au stockage Azure NetApp Files et aux instances de calcul Azure.
- **Un compte d'utilisateur Azure ou un principe de service Active Directory créé sur le portail Azure pour le connecteur SnapCenter .** Le déploiement d'un connecteur BlueXP nécessite des autorisations spécifiques pour créer et configurer une machine virtuelle et d'autres ressources de calcul, pour configurer la mise en réseau et pour accéder à l'abonnement Azure. Il nécessite également des autorisations pour créer ultérieurement des rôles et des autorisations pour que le connecteur fonctionne. Créez un rôle personnalisé dans Azure avec des autorisations et attribuez-le au compte utilisateur ou au principe de service. Consultez le lien suivant pour plus de détails :"Configurer les autorisations Azure" .
- **Une paire de clés SSH créée dans le groupe de ressources Azure.** La paire de clés SSH est attribuée à l'utilisateur de la machine virtuelle Azure pour la connexion à l'hôte du connecteur, ainsi qu'à l'hôte de la machine virtuelle de la base de données pour le déploiement et l'exécution d'un plug-in. L'interface utilisateur de la console BlueXP utilise la clé SSH pour déployer le plug-in du service SnapCenter sur l'hôte de la base de données, pour une installation en une seule étape du plug-in et la découverte de la base de données de l'hôte de l'application.
- **Un identifiant ajouté au paramètre de la console BlueXP .** Pour ajouter le stockage Azure NetApp Files à l'environnement de travail BlueXP , des informations d'identification qui accordent des autorisations pour accéder à Azure NetApp Files à partir de la console BlueXP doivent être configurées dans le paramètre de la console BlueXP .
- **java-11-openjdk installé sur l'hôte de l'instance de base de données de la machine virtuelle Azure.** 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 un stockage Azure NetApp Files et une instance de calcul Azure.

Pour commencer, procédez comme suit :

- Lire les instructions générales"Protégez les données de vos applications cloud natives" et les sections liées à Oracle et Azure NetApp Files.
- Regardez la vidéo suivante

  Vidéo du déploiement d'Oracle et d'ANF

Conditions préalables au déploiement du service SnapCenter

Le déploiement nécessite les prérequis suivants.

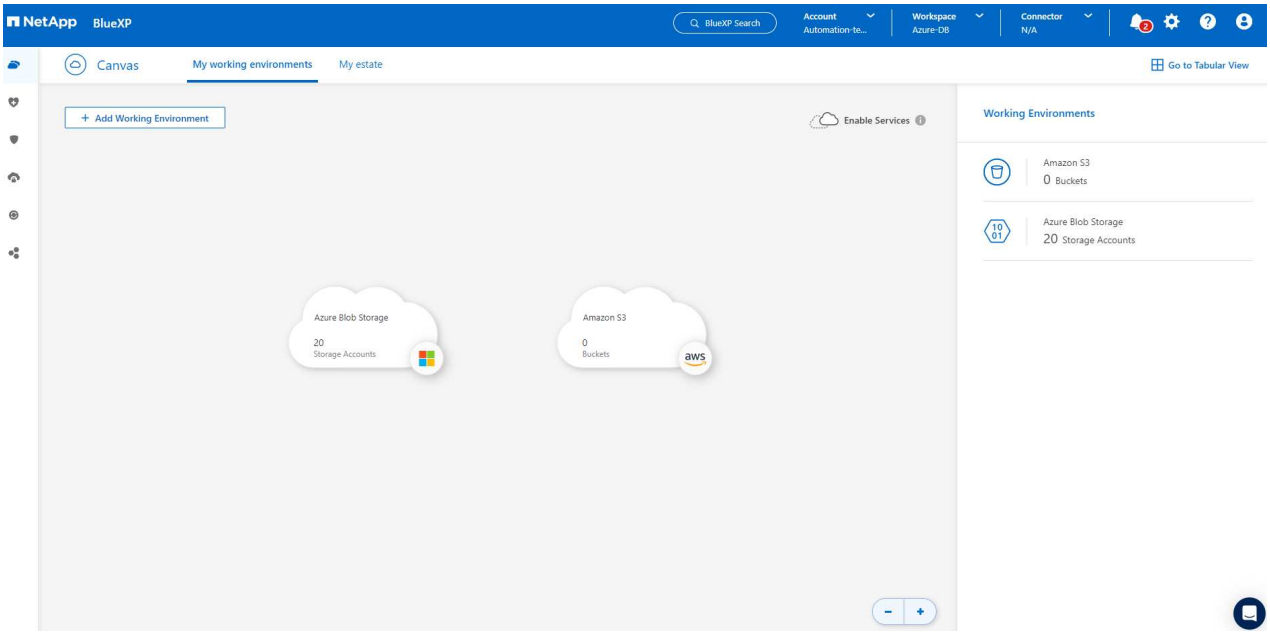
1. Un serveur de base de données Oracle principal sur une instance de machine virtuelle Azure avec une base de données Oracle entièrement déployée et en cours d'exécution.
2. Un pool de capacité de service de stockage Azure NetApp Files déployé dans Azure qui a la capacité de répondre aux besoins de stockage de base de données répertoriés dans la section des composants matériels.
3. Un serveur de base de données secondaire sur une instance de machine virtuelle Azure qui peut être utilisé pour tester le clonage d'une base de données Oracle sur un autre hôte dans le but de prendre en charge une charge de travail de développement/test ou tout cas d'utilisation nécessitant un ensemble complet de données de base de données Oracle de production.
4. Pour plus d'informations sur le déploiement de la base de données Oracle sur Azure NetApp Files et l'instance de calcul Azure, consultez"Déploiement et protection de la base de données Oracle sur Azure NetApp Files" .

Préparation à l'intégration de BlueXP

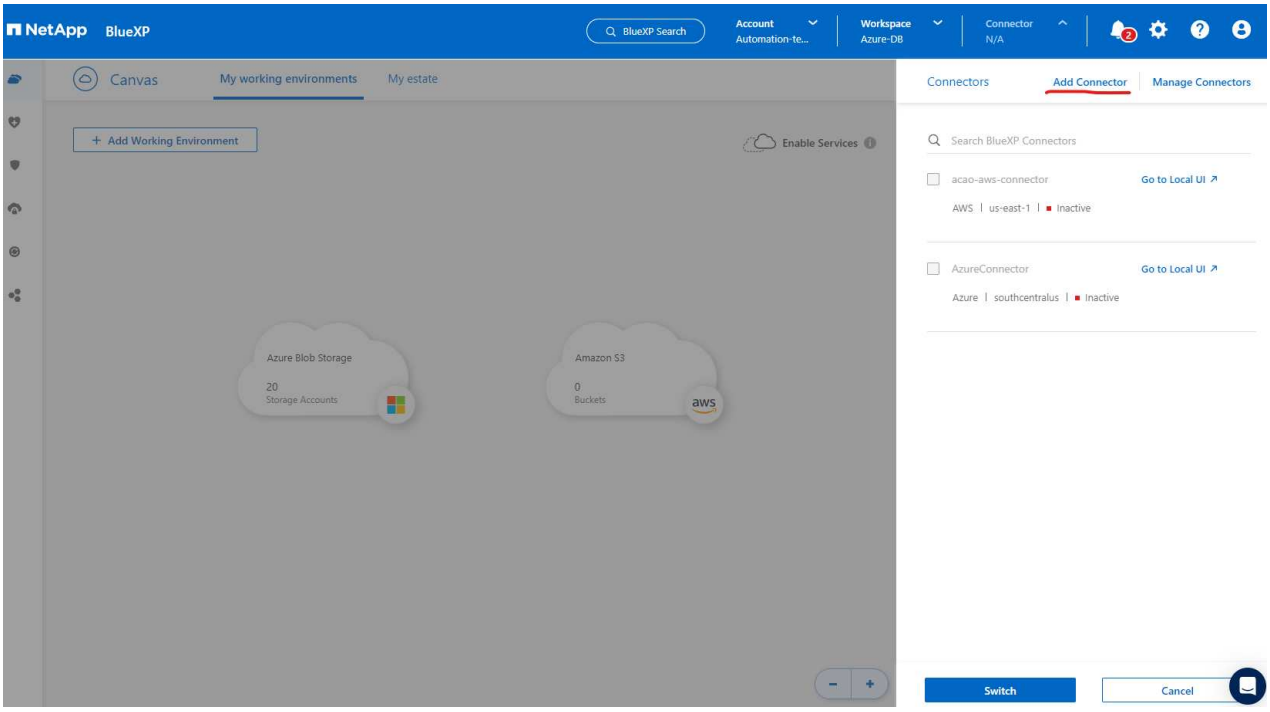
1. Utilisez le lien"NetApp BlueXP" pour vous inscrire à l'accès à la console BlueXP .
2. Créez un compte d'utilisateur Azure ou un principe de service Active Directory et accordez des autorisations avec un rôle dans le portail Azure pour le déploiement du connecteur Azure.
3. Pour configurer BlueXP afin de gérer les ressources Azure, ajoutez des informations d'identification BlueXP avec les détails d'un principal de service Active Directory que BlueXP peut utiliser pour s'authentifier auprès d'Azure Active Directory (ID client d'application), un secret client pour l'application principale de service (Secret client) et l'ID Active Directory de votre organisation (ID de locataire).
4. Vous avez également besoin du réseau virtuel Azure, du groupe de ressources, du groupe de sécurité, d'une clé SSH pour l'accès à la machine virtuelle, etc. prêts pour le provisionnement du connecteur et l'installation du plug-in de base de données.

Déployer un connecteur pour les services SnapCenter

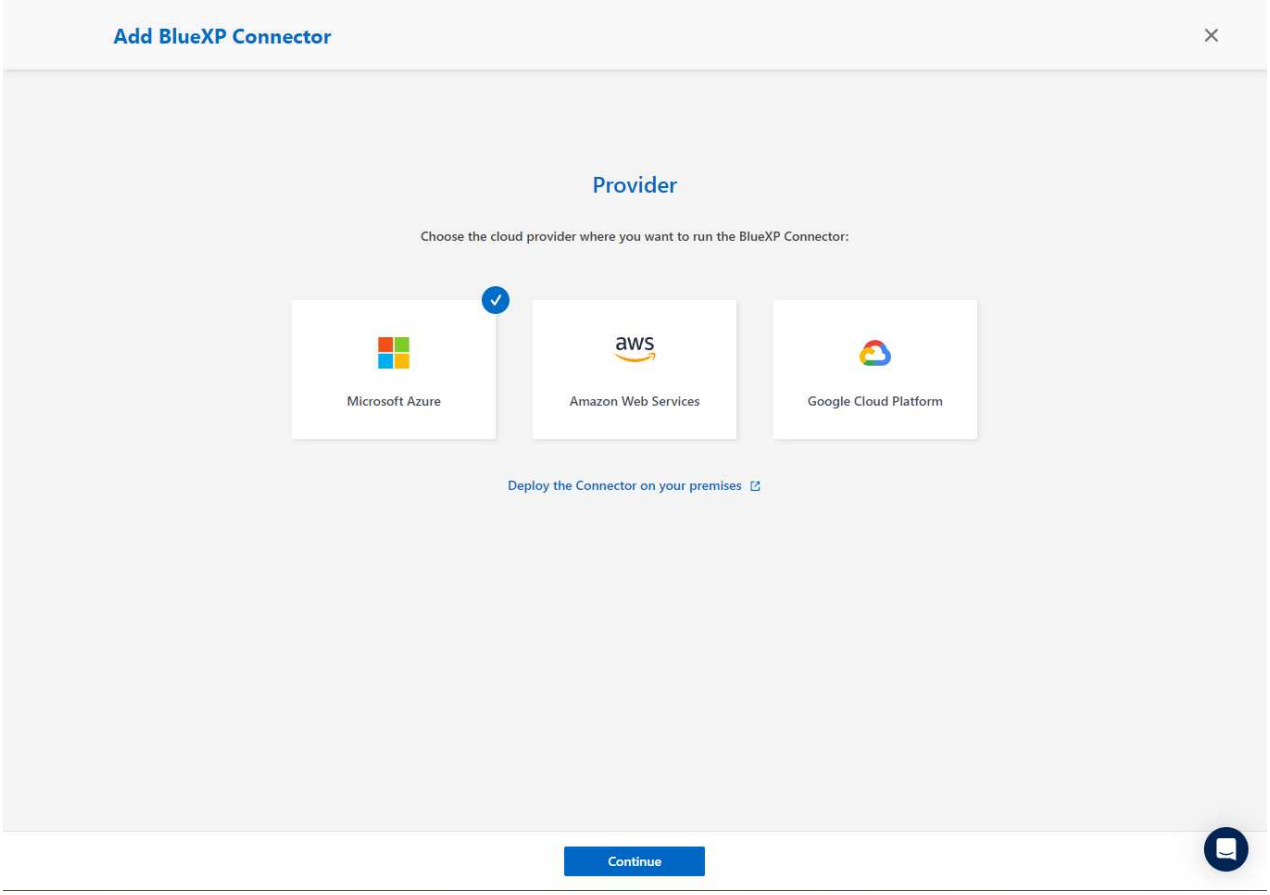
1. Connectez-vous à la console BlueXP .



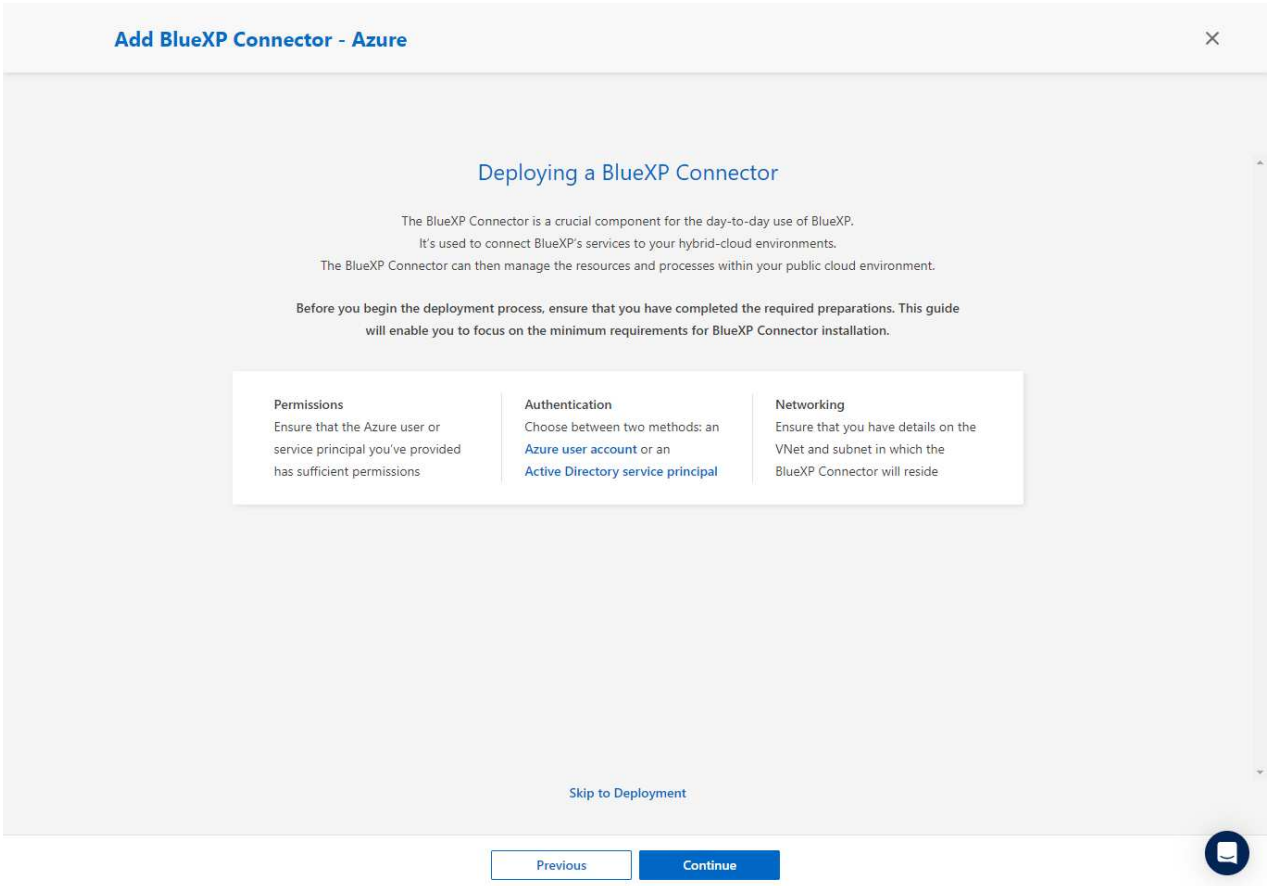
2. Cliquez sur la flèche déroulante **Connecteur** et sur **Ajouter un connecteur** pour lancer le flux de travail de provisionnement du connecteur.



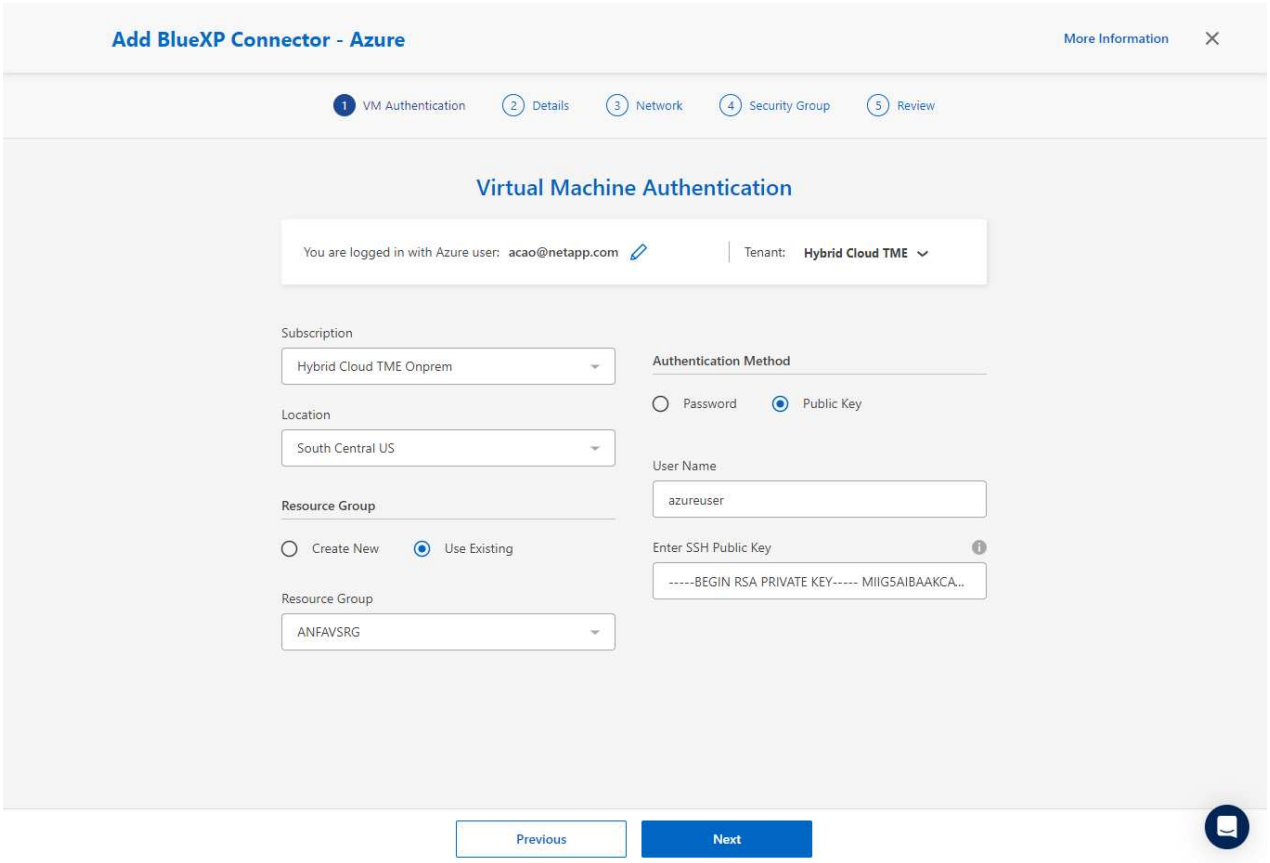
3. Choisissez votre fournisseur de cloud (dans ce cas, **Microsoft Azure**).



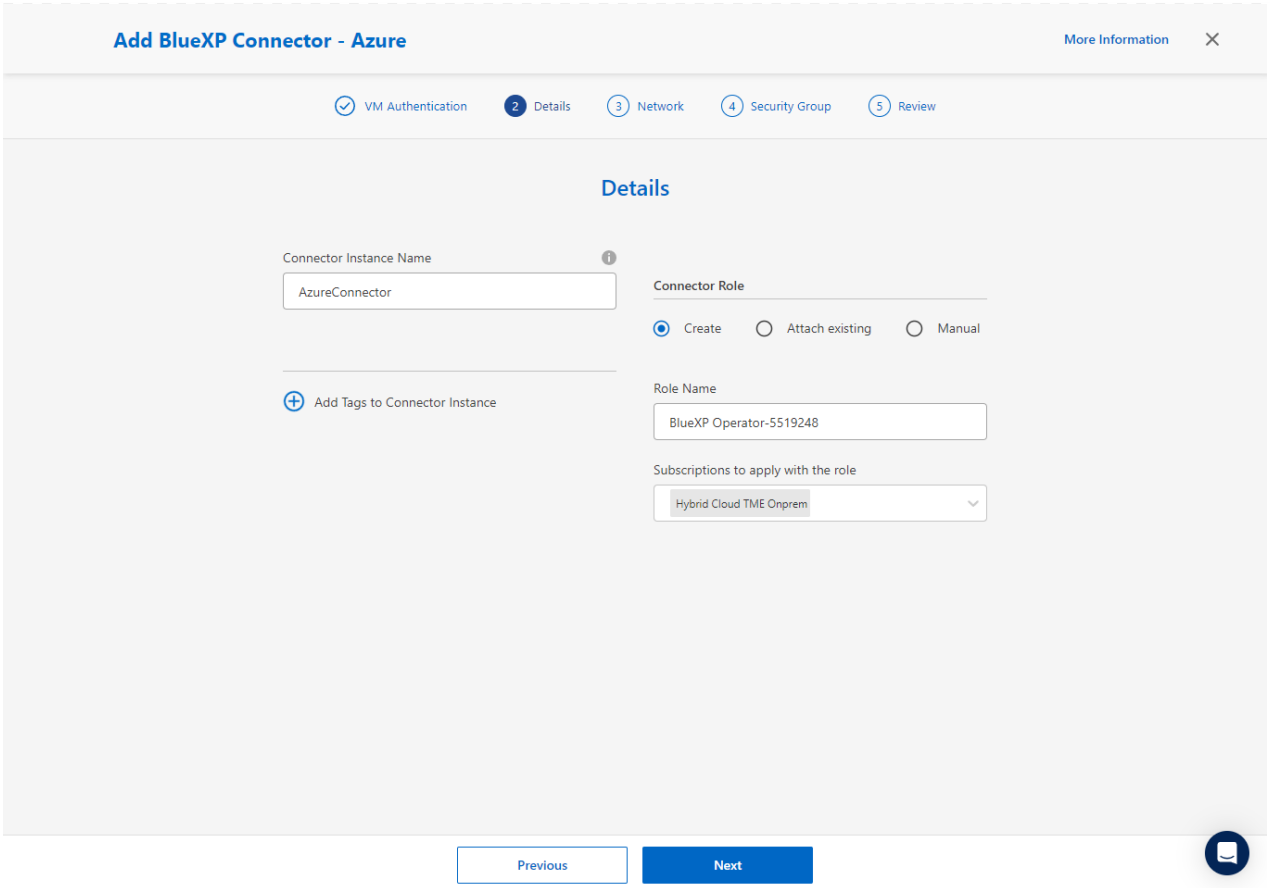
4. Ignorez les étapes **Autorisation**, **Authentification** et **Mise en réseau** si vous les avez déjà configurées dans votre compte Azure. Sinon, vous devez les configurer avant de continuer. À partir de là, vous pouvez également récupérer les autorisations pour la stratégie Azure référencée dans la section précédente "Préparation à l'intégration de BlueXP ."



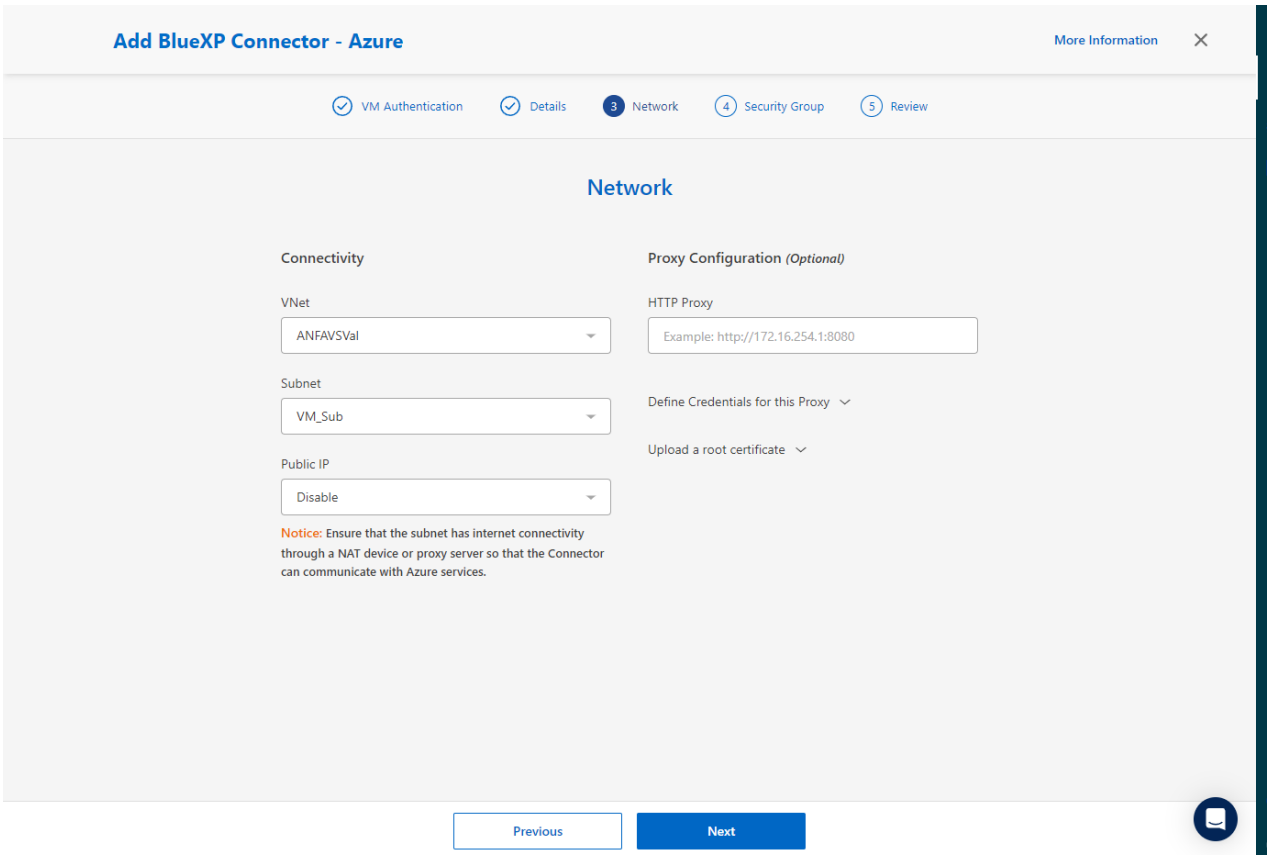
5. Cliquez sur **Passer au déploiement** pour configurer votre connecteur **Authentification de machine virtuelle**. Ajoutez la paire de clés SSH que vous avez créée dans le groupe de ressources Azure lors de l'intégration à la préparation BlueXP pour l'authentification du système d'exploitation du connecteur.



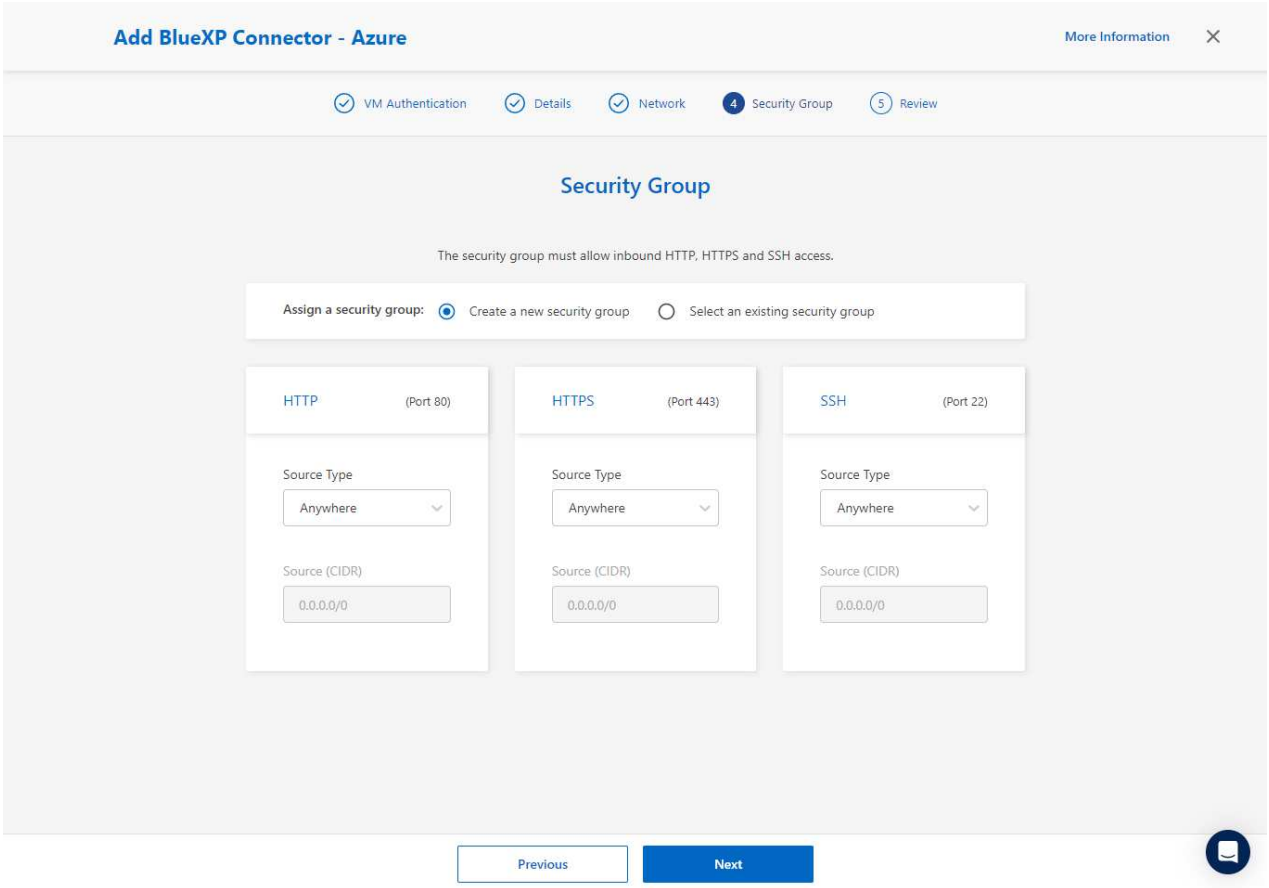
6. Fournissez un nom pour l'instance du connecteur, sélectionnez **Créer** et acceptez le **Nom du rôle** par défaut sous **Détails**, puis choisissez l'abonnement pour le compte Azure.



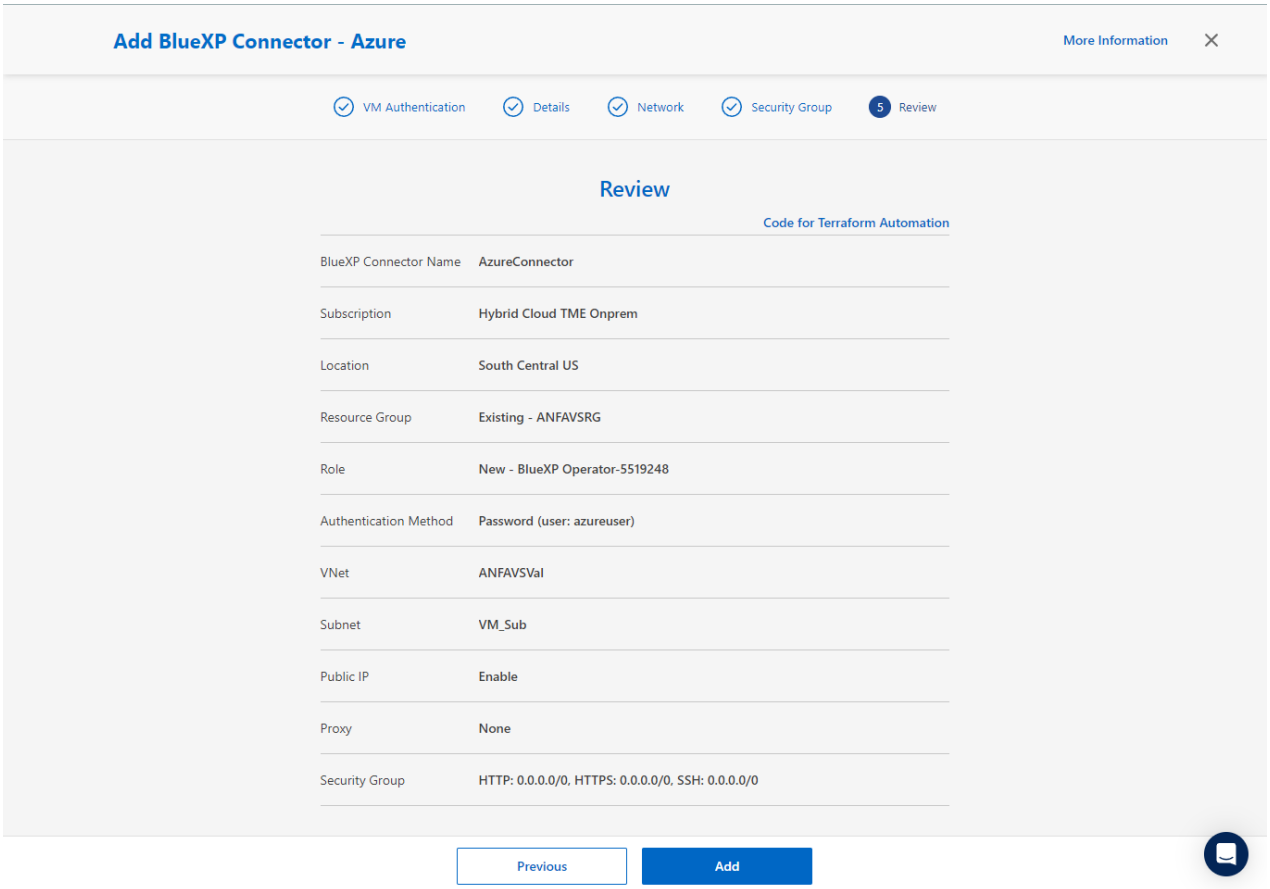
7. Configurez la mise en réseau avec le **VNet**, le **Sous-réseau** appropriés et désactivez l'**IP publique**, mais assurez-vous que le connecteur dispose d'un accès Internet dans votre environnement Azure.



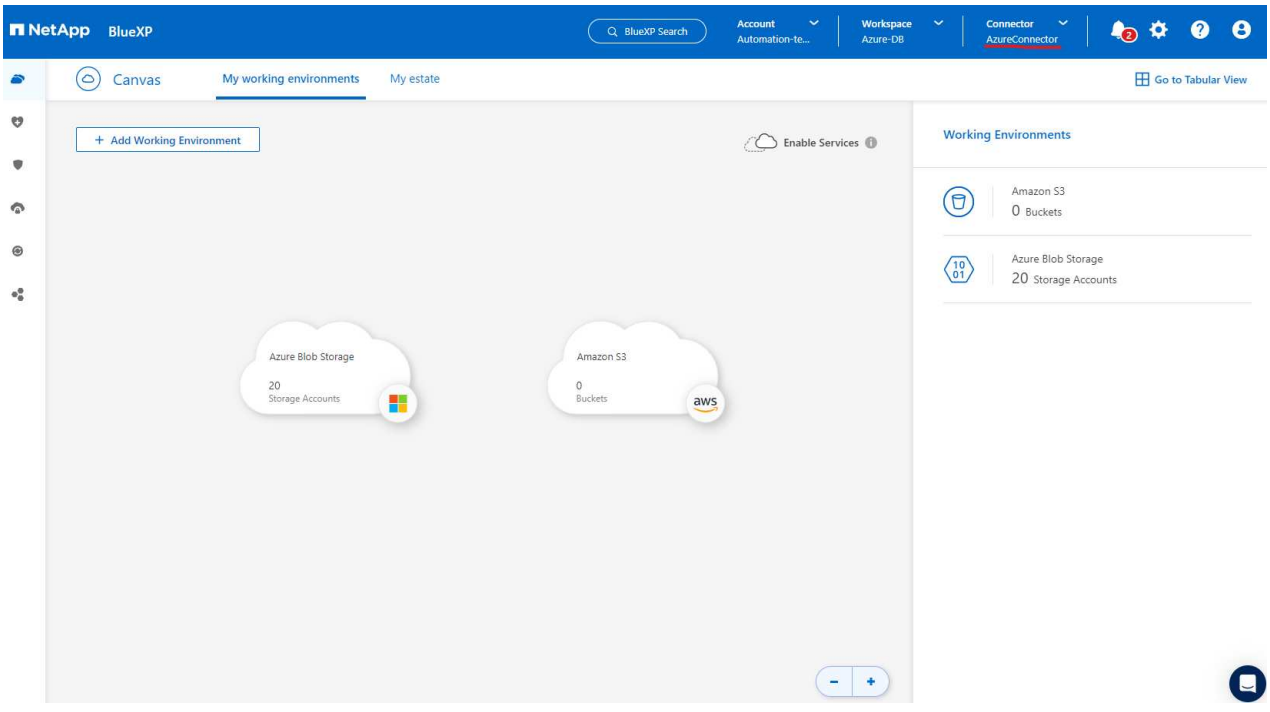
8. Configurez le **groupe de sécurité** pour le connecteur qui autorise l'accès HTTP, HTTPS et SSH.



9. 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 de connecteur VM apparaît dans le portail Azure.

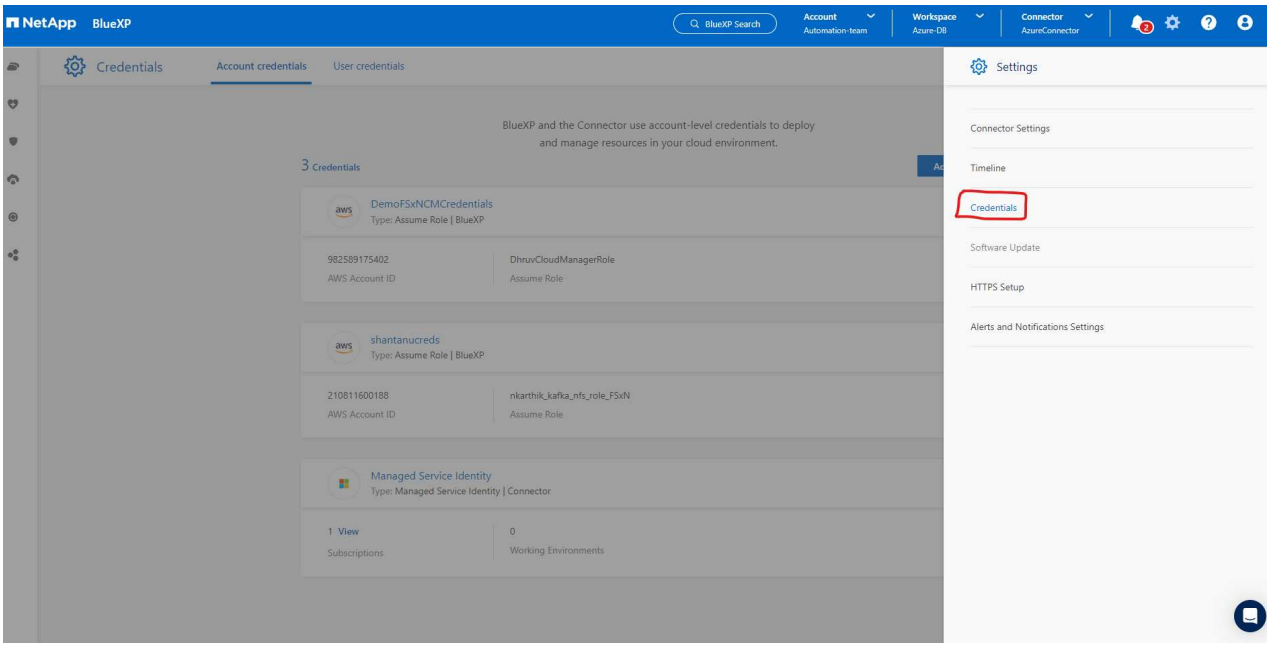


10. Une fois le connecteur déployé, le connecteur nouvellement créé apparaît sous la liste déroulante **Connecteur**.

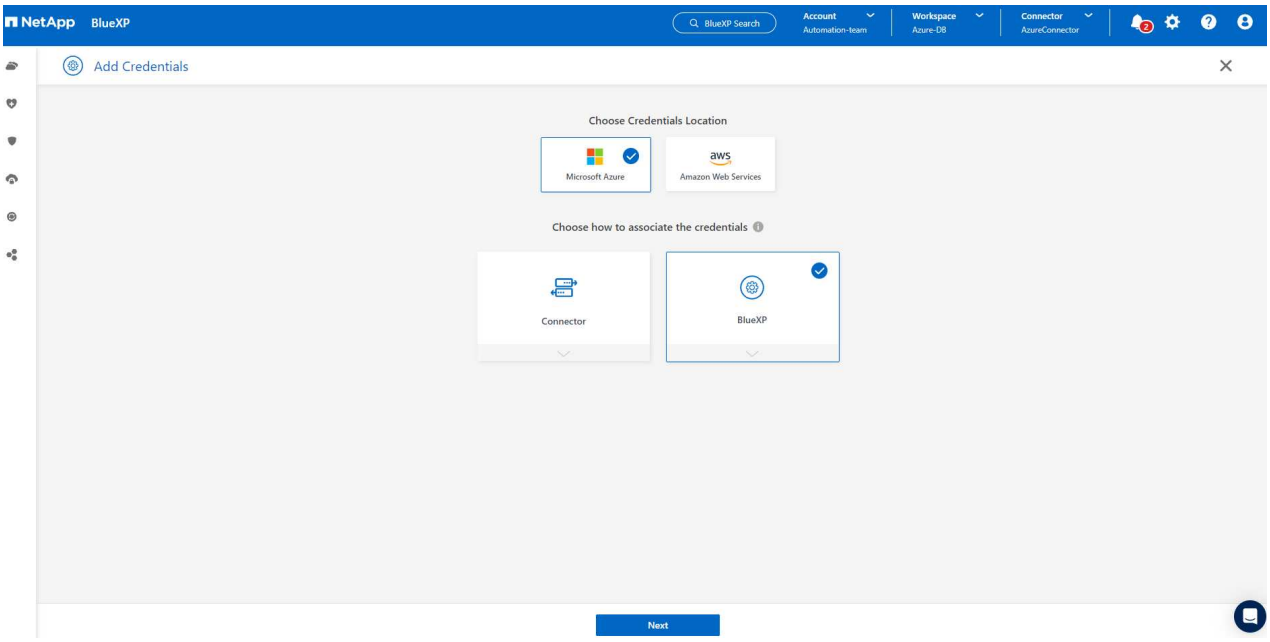


Définir des informations d’identification dans BlueXP pour accéder aux ressources Azure

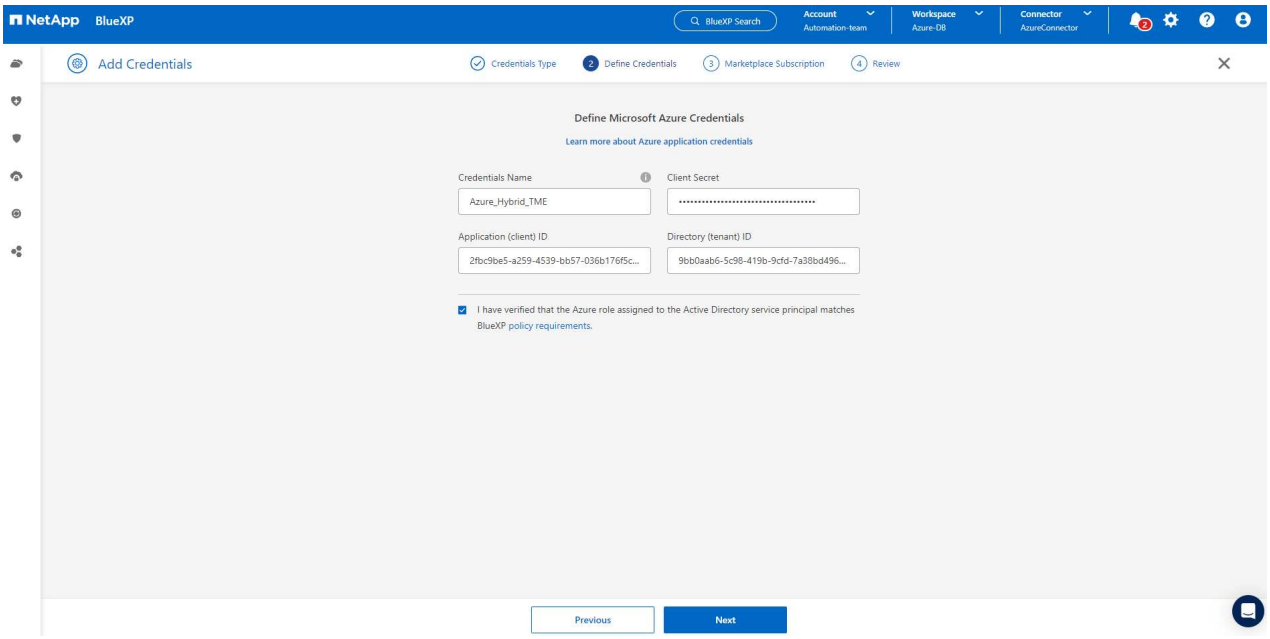
1. Cliquez sur l'icône de configuration dans le coin supérieur droit de la console BlueXP pour ouvrir la page **Informations d'identification du compte**, cliquez sur **Ajouter des informations d'identification** pour démarrer le flux de travail de configuration des informations d'identification.



2. Choisissez l'emplacement des informations d'identification comme - **Microsoft Azure - BlueXP**.

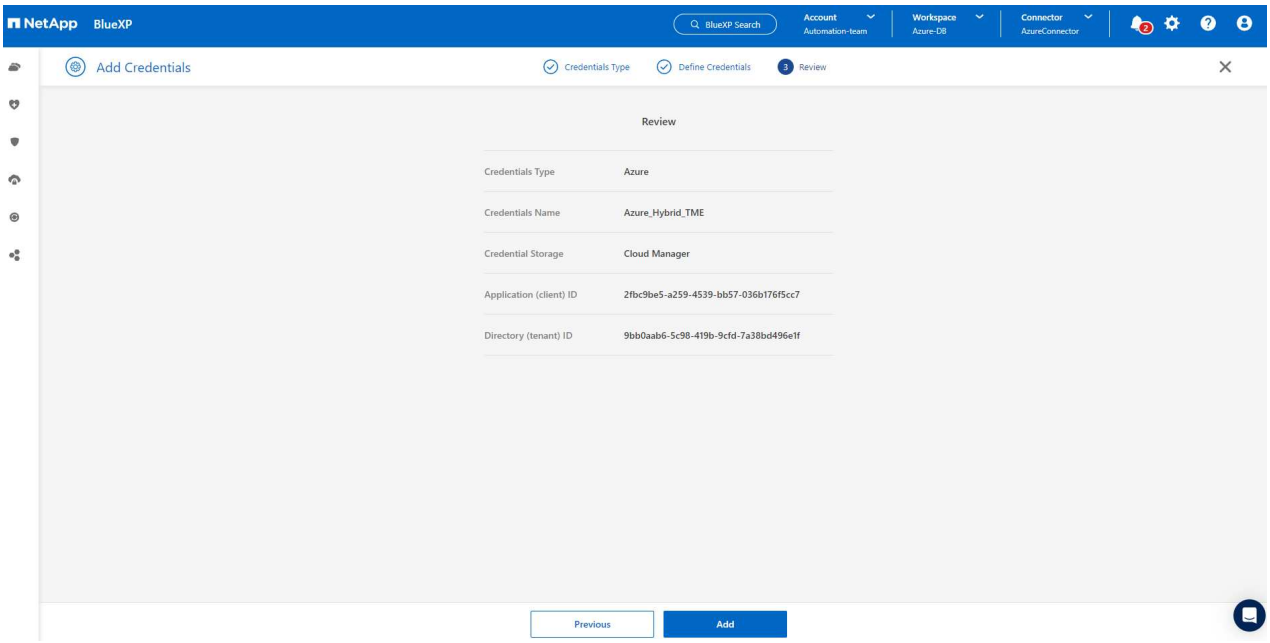


3. Définissez les informations d'identification Azure avec le **Client Secret**, l'**ID client** et l'**ID locataire** appropriés, qui auraient dû être collectés lors du processus d'intégration BlueXP précédent.

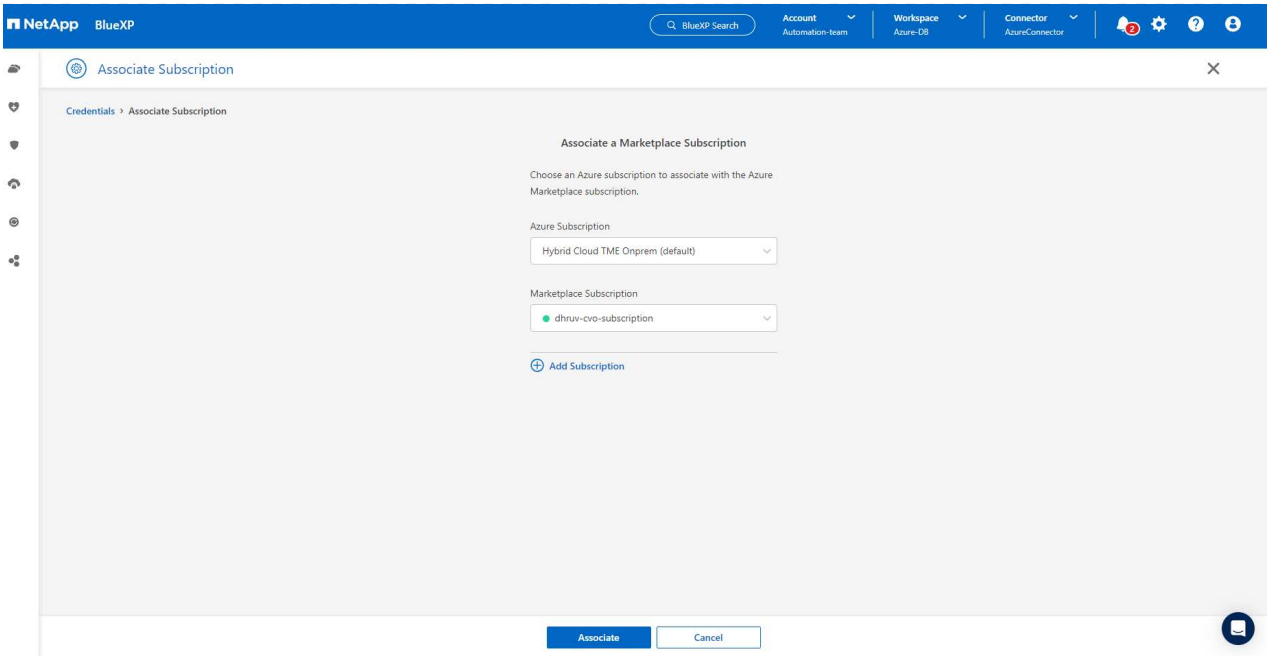


4. Réviser et **Ajouter**

.



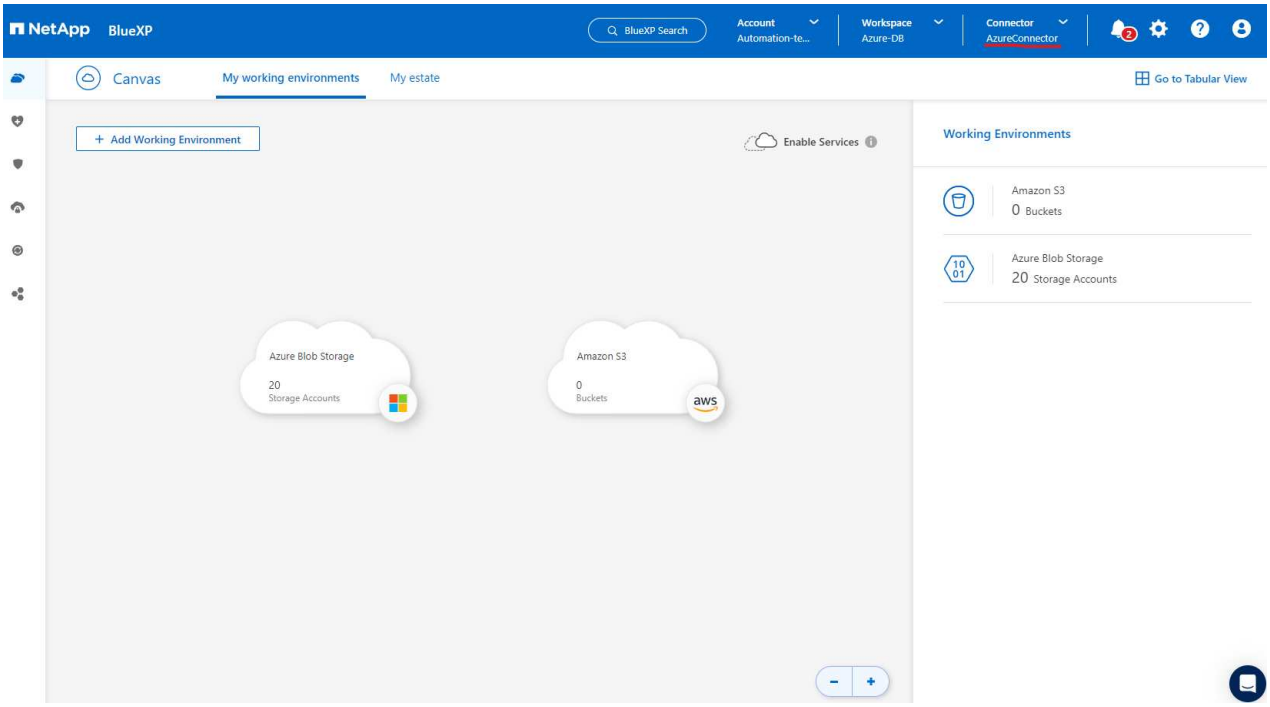
5. Vous devrez peut-être également associer un **abonnement Marketplace** aux informations d'identification.



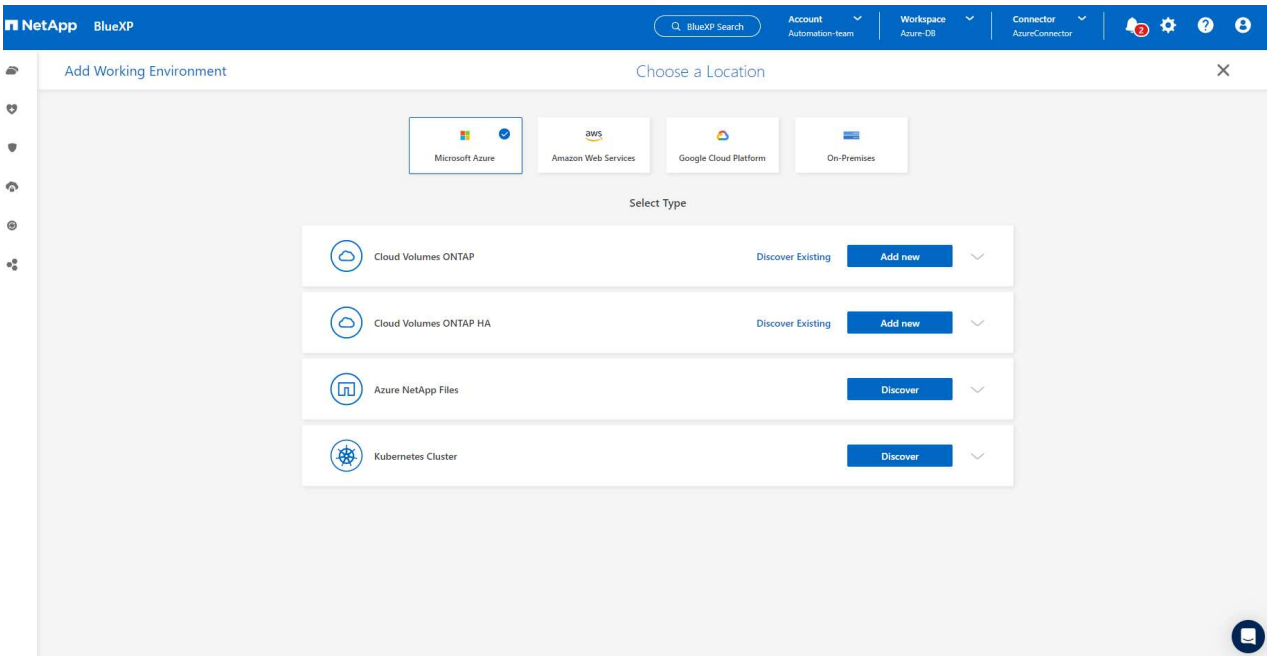
Configuration des services SnapCenter

Une fois les informations d'identification Azure configurées, les services SnapCenter peuvent désormais être configurés à l'aide des procédures suivantes :

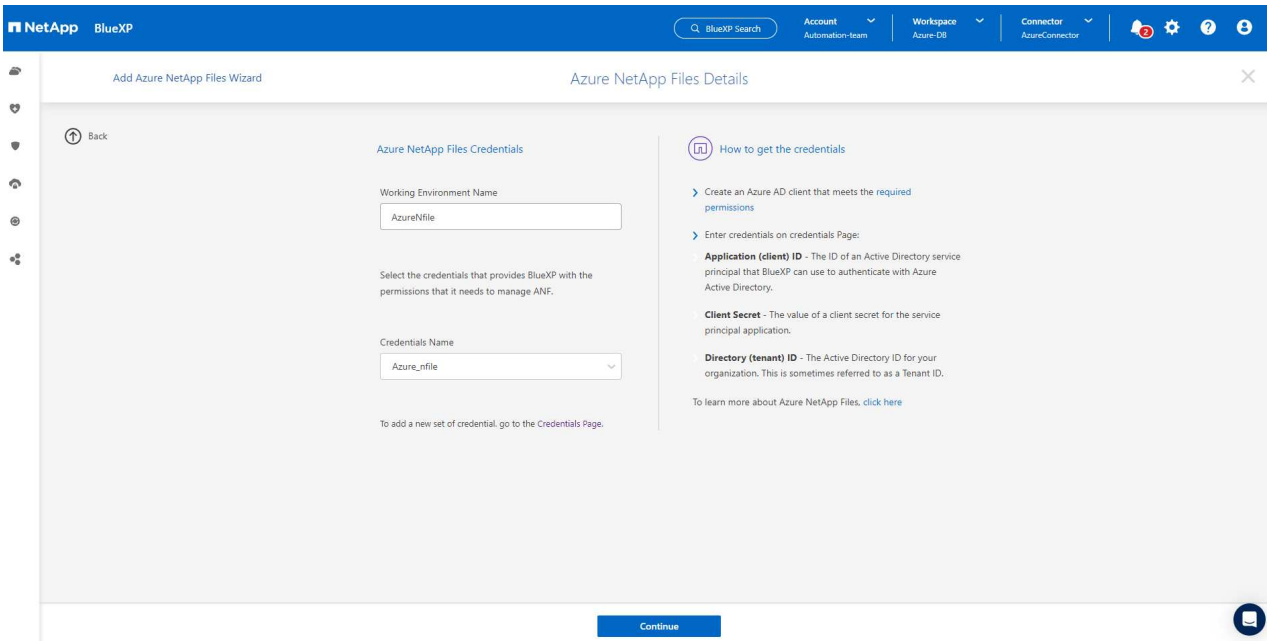
1. De retour à la page Canvas, depuis **Mon environnement de travail**, cliquez sur **Ajouter un environnement de travail** pour découvrir Azure NetApp Files déployé dans Azure.



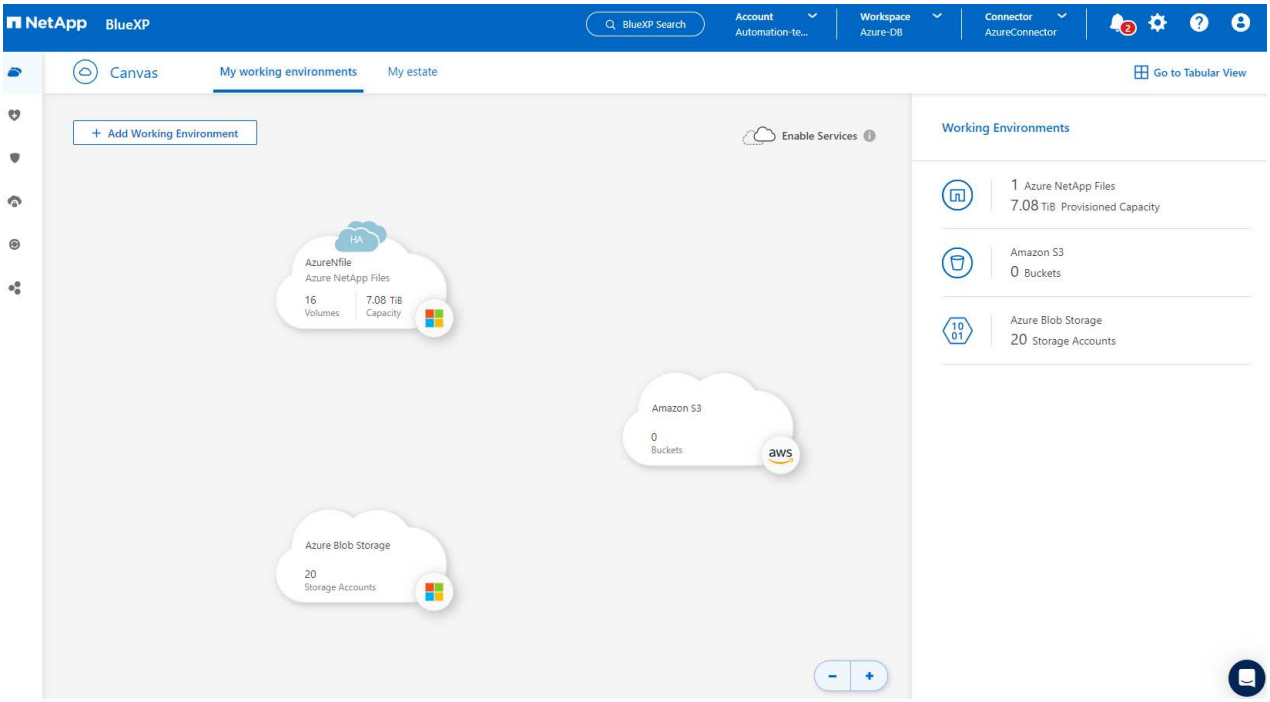
2. Choisissez **Microsoft Azure** comme emplacement et cliquez sur **Découvrir**.



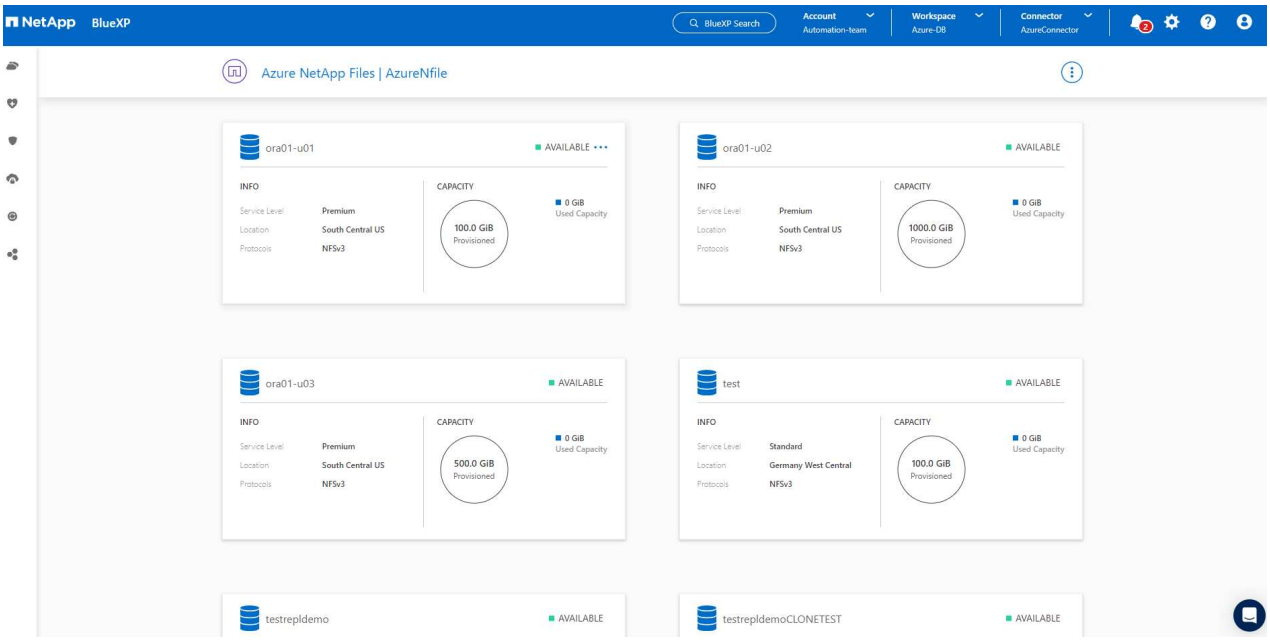
3. Nommez **Environnement de travail** et choisissez **Nom d'identification** créé dans la section précédente, puis cliquez sur **Continuer**.



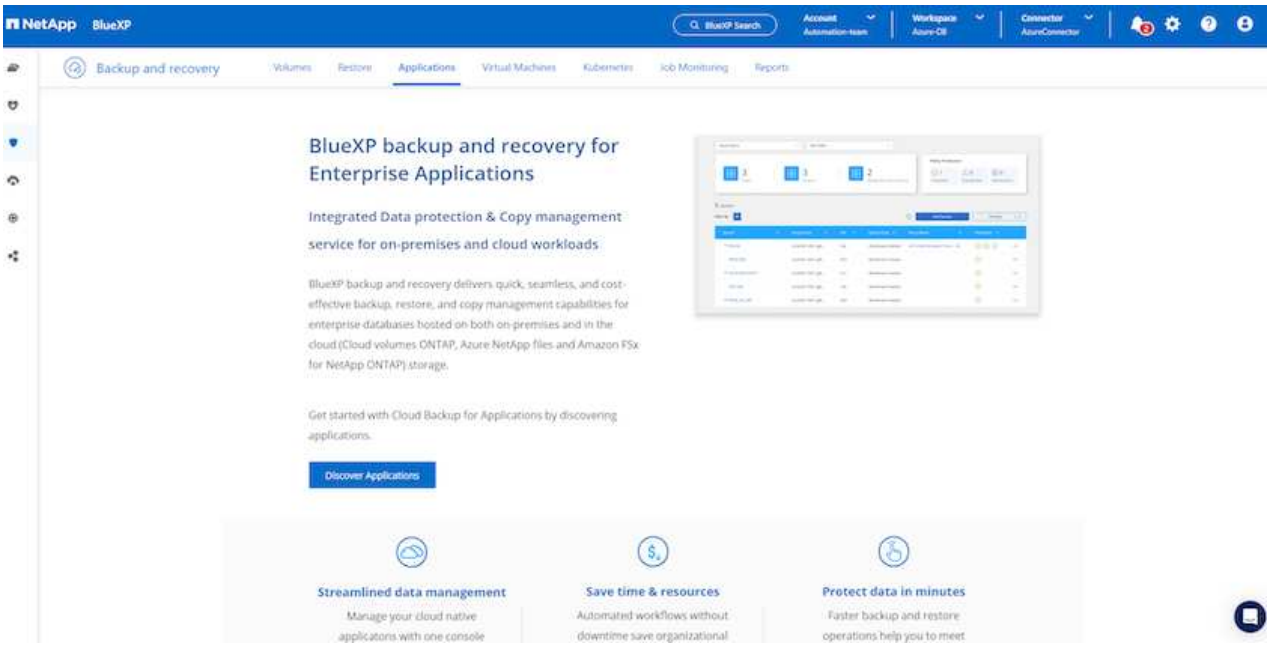
4. La console BlueXP revient à **Mes environnements de travail** et les Azure NetApp Files découverts à partir d'Azure apparaissent désormais sur **Canvas**.



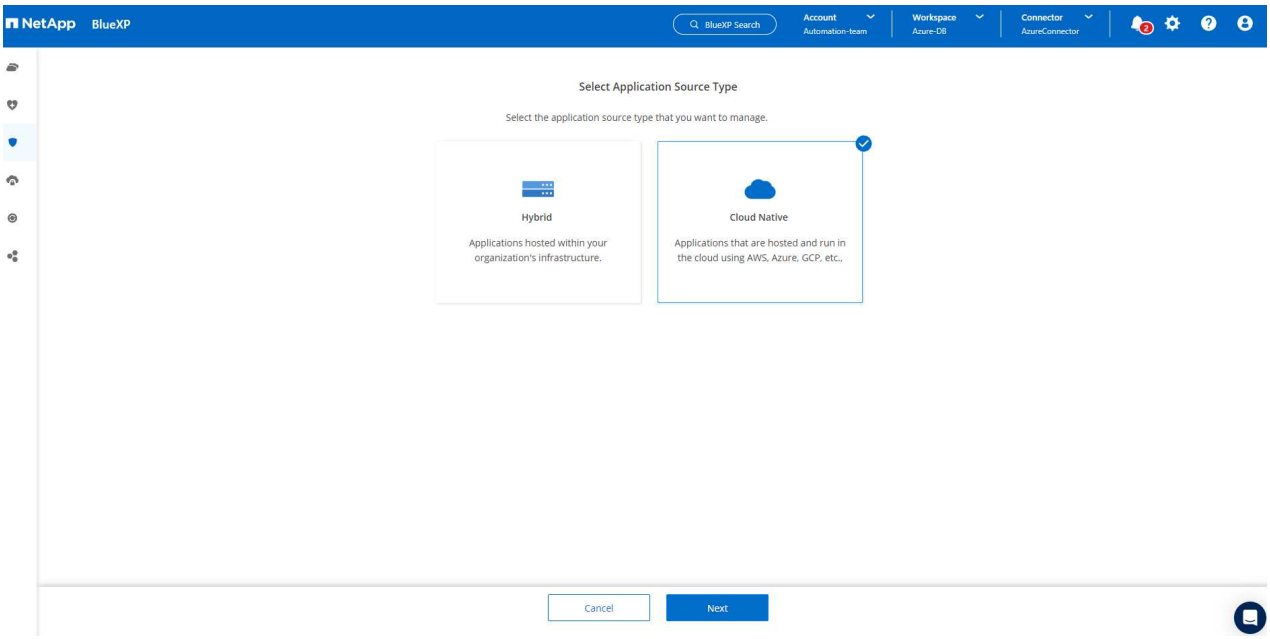
5. Cliquez sur l'icône * Azure NetApp Files*, puis **Entrer dans l'environnement de travail** pour afficher les volumes de base de données Oracle déployés dans le stockage Azure NetApp Files .



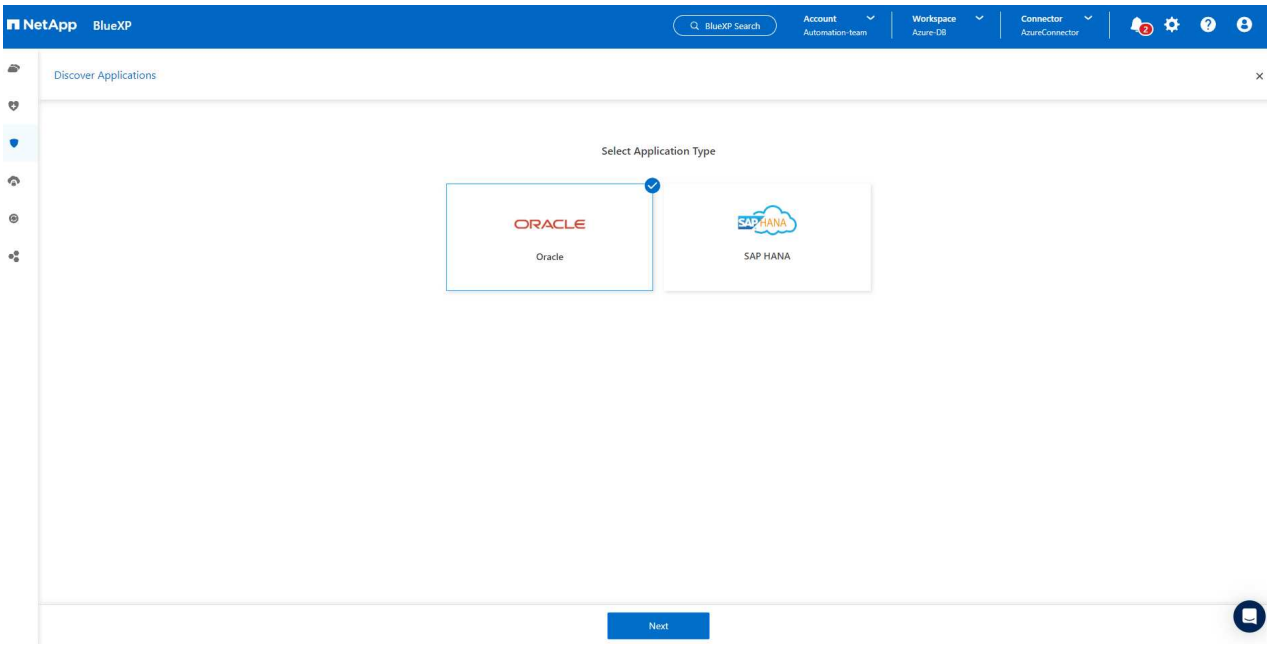
6. Dans la barre latérale gauche de la console, passez votre souris sur l'icône de protection, puis cliquez sur **Protection** > **Applications** pour ouvrir la page de lancement des applications. Cliquez sur **Découvrir les applications**.



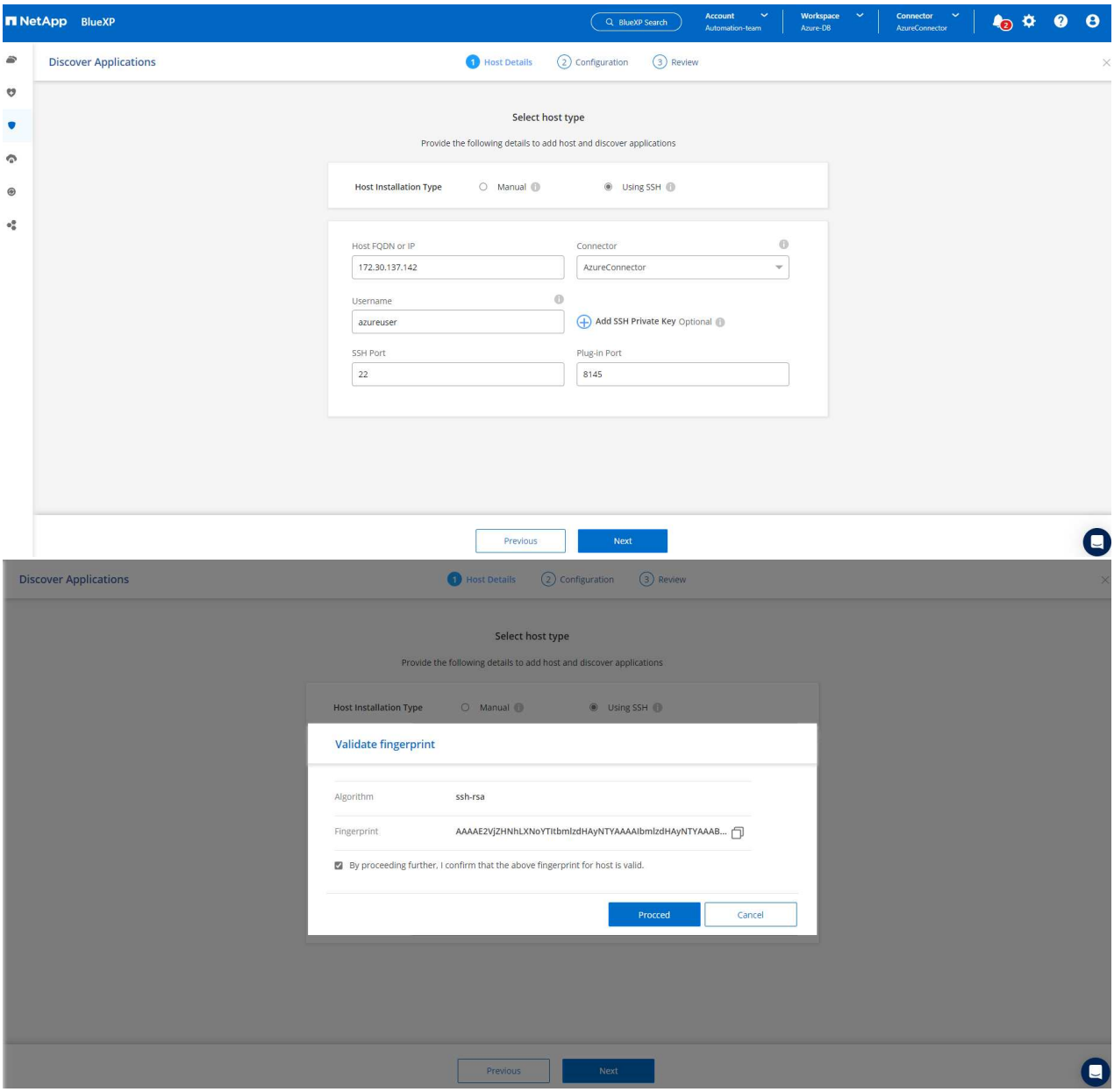
7. Sélectionnez **Cloud Native** comme type de source d'application.



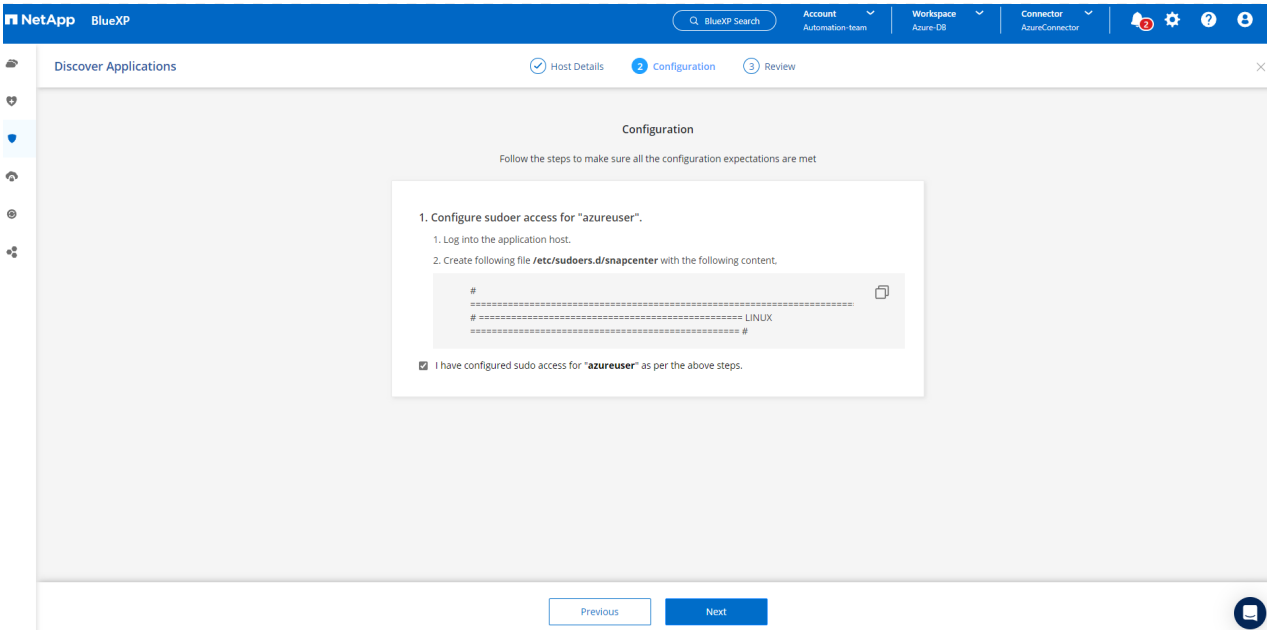
8. Choisissez **Oracle** pour le type d'application, cliquez sur **Suivant** pour ouvrir la page des détails de l'hôte.



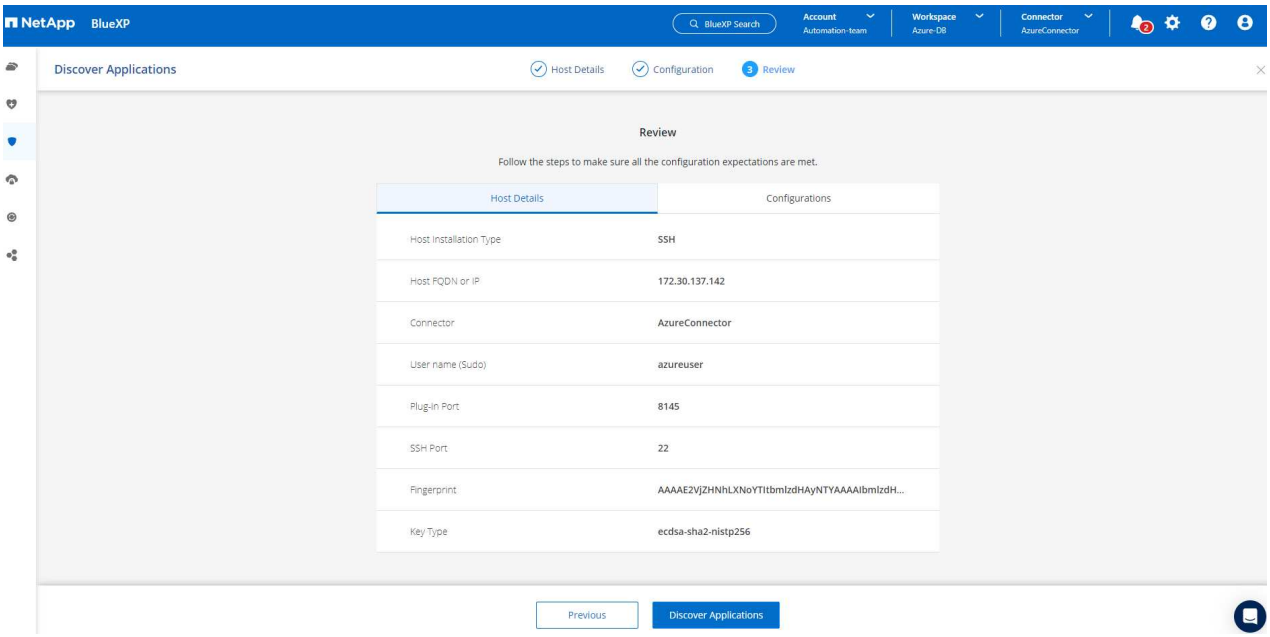
9. Sélectionnez **Utilisation de SSH** et fournissez les détails de la machine virtuelle Oracle Azure tels que **l'adresse IP**, **le connecteur**, **le nom d'utilisateur** de gestion de la machine virtuelle Azure tel que azureuser. Cliquez sur **Ajouter une clé privée SSH** pour coller la paire de clés SSH que vous avez utilisée pour déployer la machine virtuelle Oracle Azure. Vous serez également invité à confirmer l'empreinte digitale.



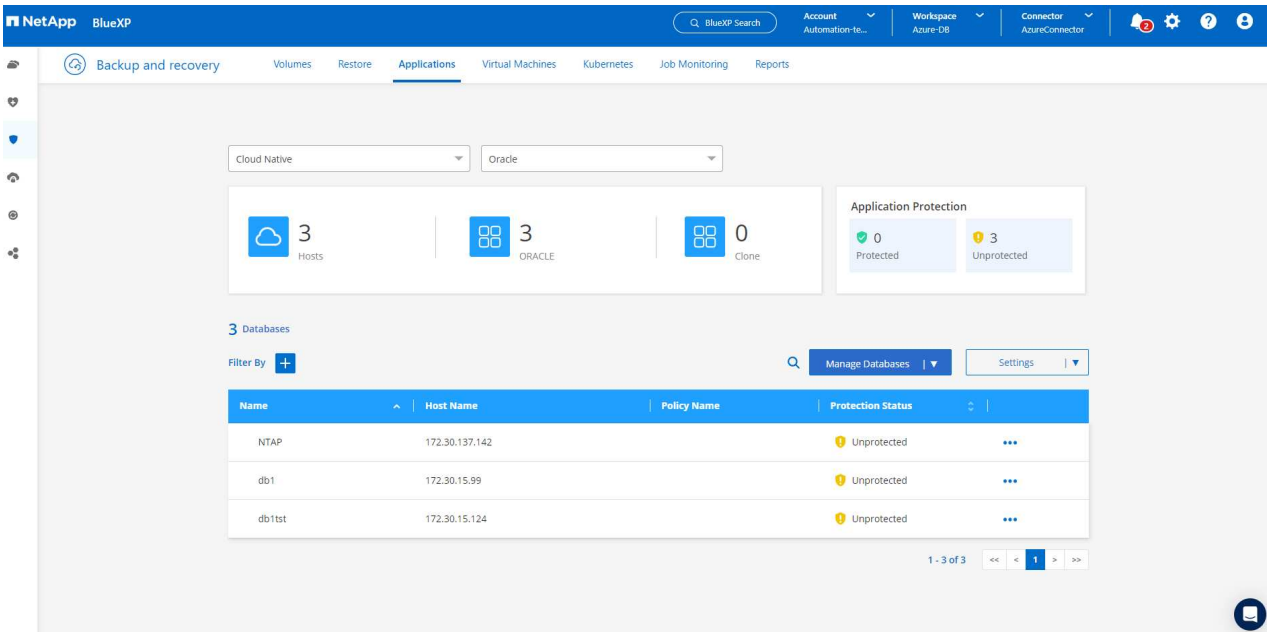
10. Passez à la page **Configuration** suivante pour configurer l'accès sudoer sur la machine virtuelle Oracle Azure.



11. Consultez et cliquez sur **Découvrir les applications** pour installer un plugin sur la machine virtuelle Oracle Azure et découvrir la base de données Oracle sur la machine virtuelle en une seule étape.



12. Les bases de données Oracle découvertes sur la machine virtuelle Azure sont ajoutées à **Applications**, et la page **Applications** répertorie le nombre d'hôtes et de bases de données Oracle dans l'environnement. La base de données **État de protection** s'affiche initialement comme **Non protégé**.



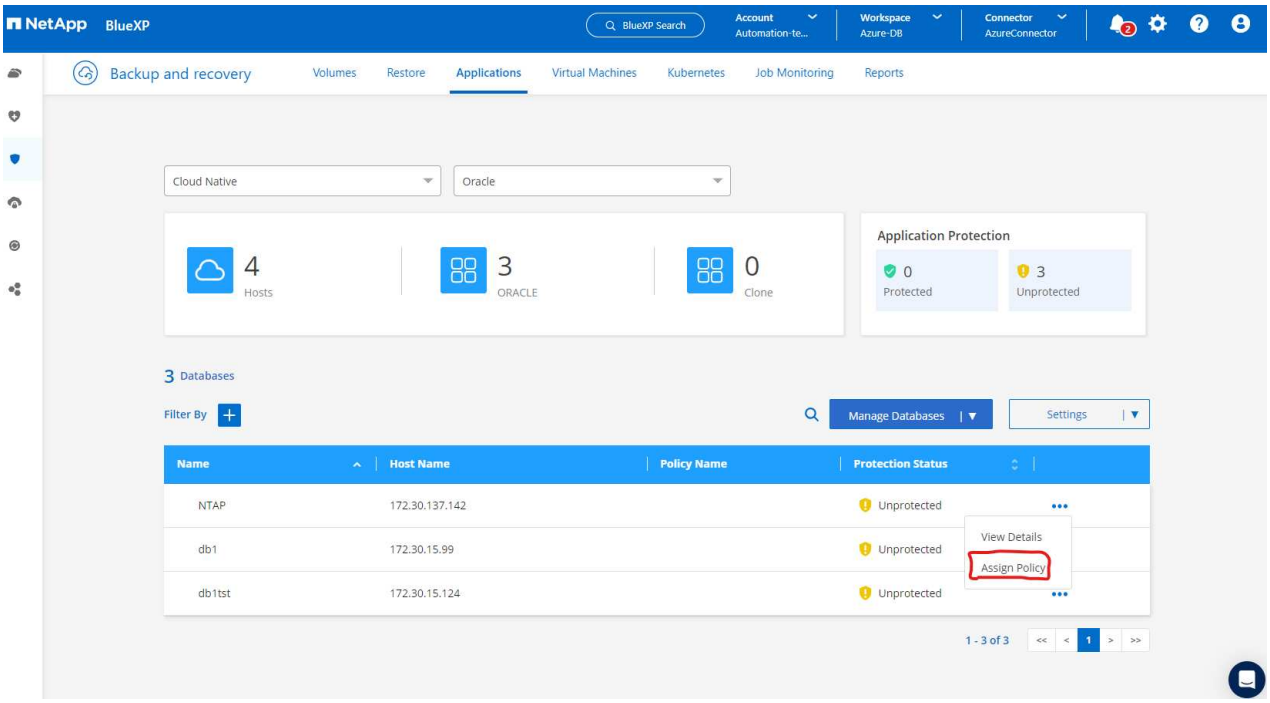
Ceci termine la configuration initiale des services SnapCenter pour Oracle. Les trois sections suivantes de ce document décrivent les opérations de sauvegarde, de restauration et de clonage de la base de données Oracle.

Sauvegarde de la base de données Oracle

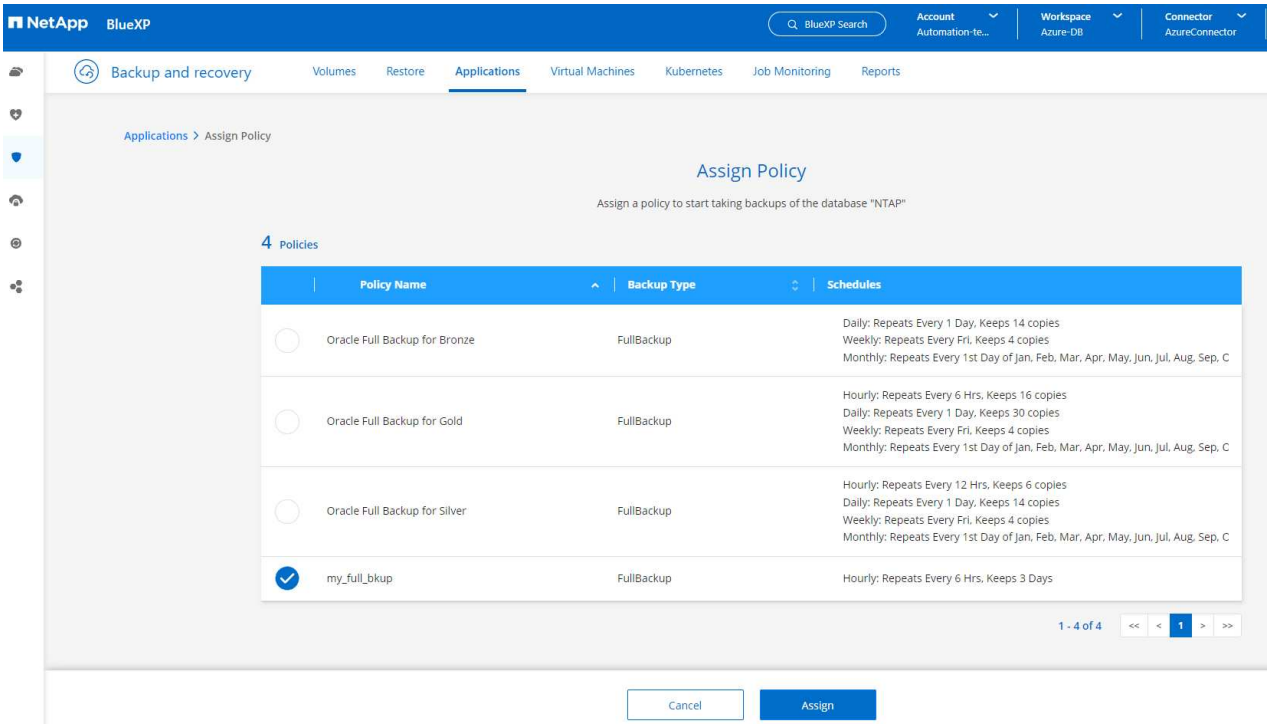
1. Notre base de données Oracle de test dans Azure VM est configurée avec trois volumes avec un stockage total agrégé d'environ 1,6 Tio. Cela donne un contexte sur le calendrier de sauvegarde, de restauration et de clonage d'une base de données de cette taille.

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

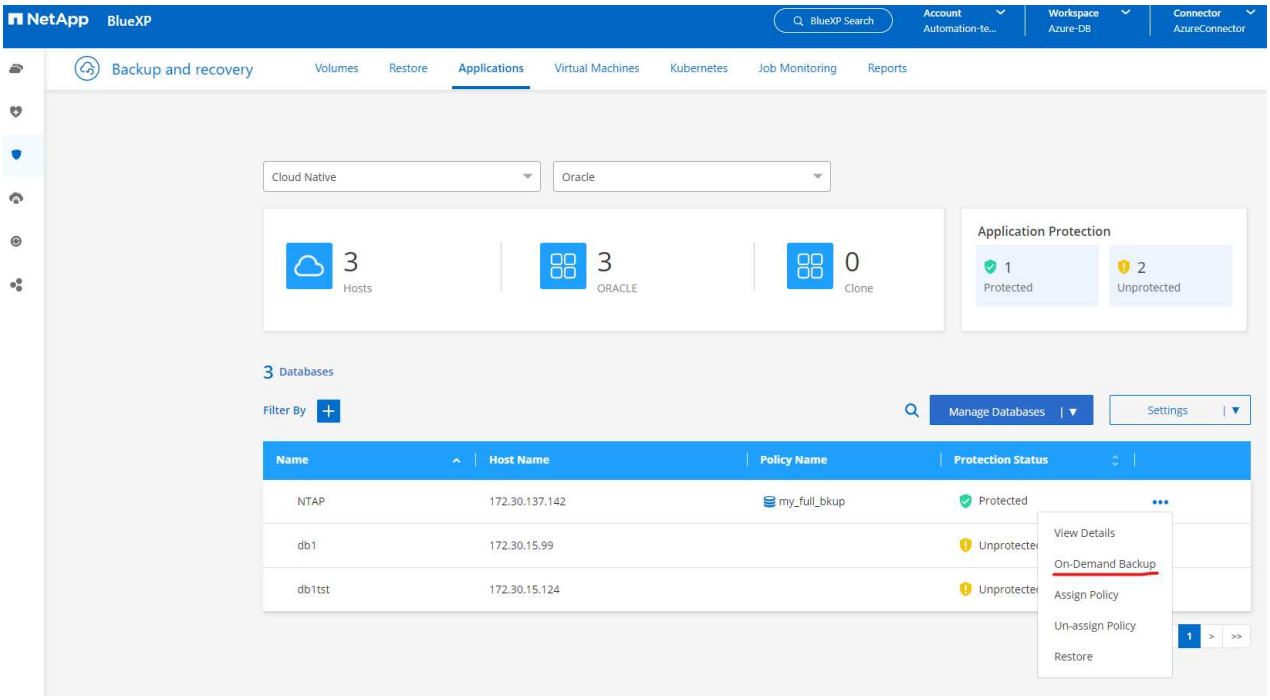
1. Pour protéger la base de données, cliquez sur les trois points à côté de l'état de protection de la base de données, puis cliquez sur **Attribuer une stratégie** pour afficher les stratégies de protection de base de données préchargées ou définies par l'utilisateur par défaut qui peuvent être appliquées à vos bases de données Oracle. Sous **Paramètres** - **Politiques**, vous avez la possibilité de créer votre propre politique avec une fréquence de sauvegarde personnalisée et une fenêtre de conservation des données de sauvegarde.



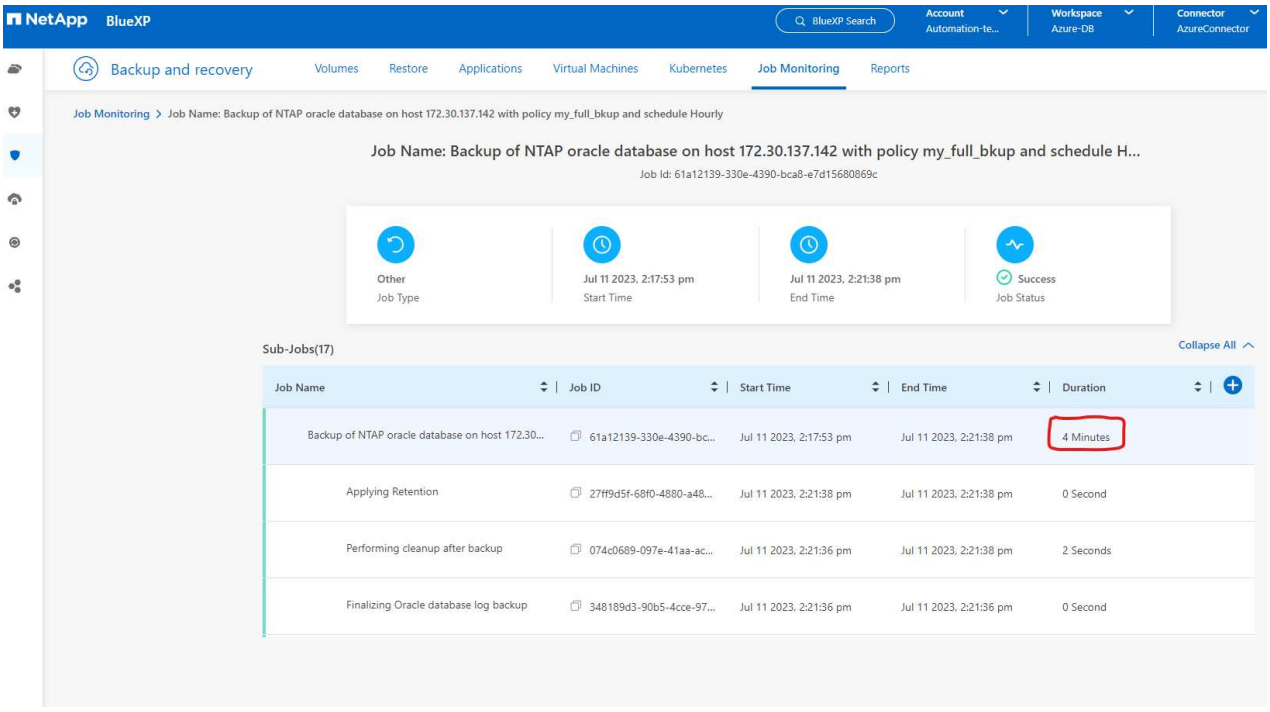
2. Lorsque vous êtes satisfait de la configuration de la politique, vous pouvez ensuite **Attribuer** la politique de votre choix pour protéger la base de données.



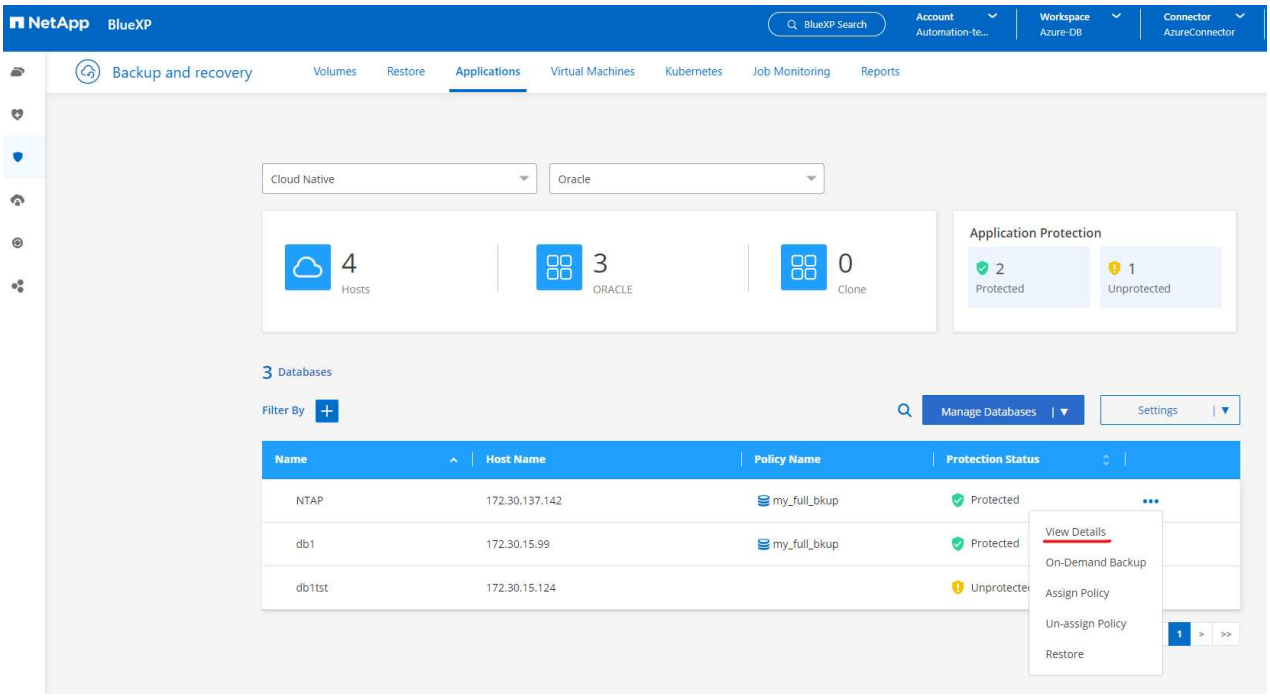
3. Une fois la politique appliquée, l'état de protection de la base de données est passé à **Protégé** avec une coche verte. BlueXP exécute la sauvegarde instantanée selon la planification définie. De plus, la **sauvegarde à la demande** est disponible à partir du menu déroulant à trois points comme indiqué ci-dessous.



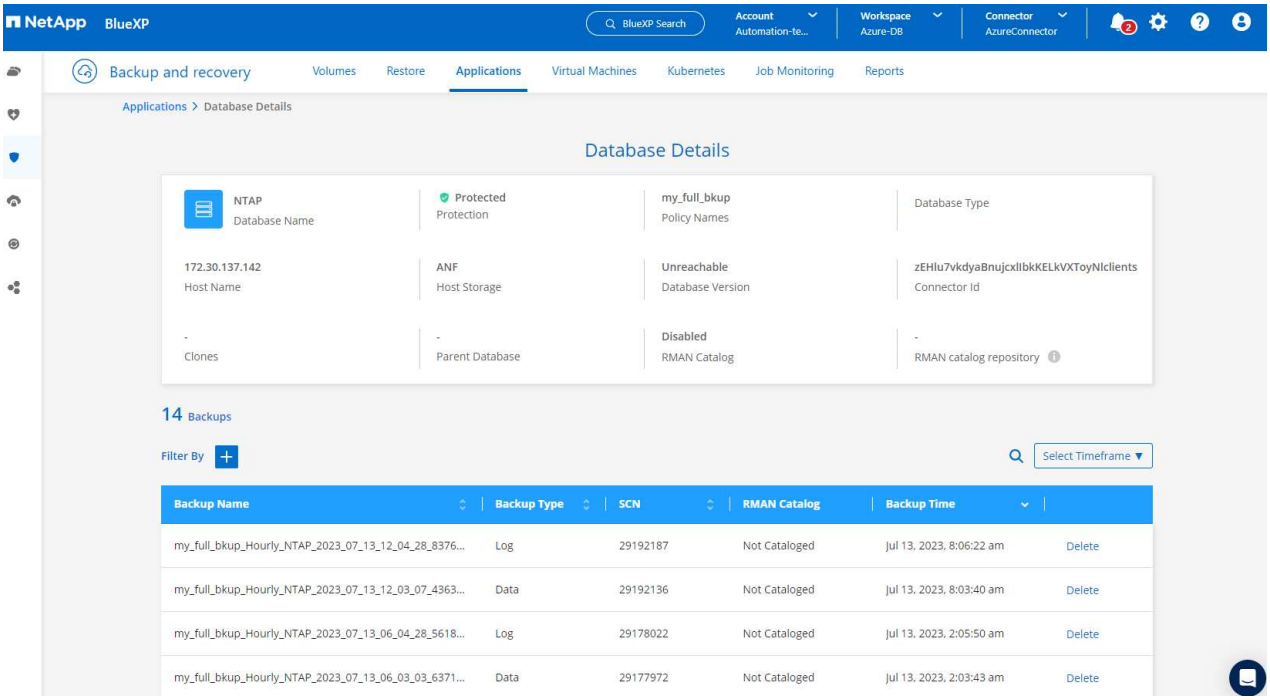
4. Depuis l'onglet **Surveillance des tâches**, les détails des tâches de sauvegarde peuvent être affichés. Nos résultats de test ont montré qu'il fallait environ 4 minutes pour sauvegarder une base de données Oracle d'environ 1,6 Tio.



5. À partir du menu déroulant à trois points **Afficher les détails**, vous pouvez afficher les jeux de sauvegarde créés à partir de la sauvegarde instantanée.

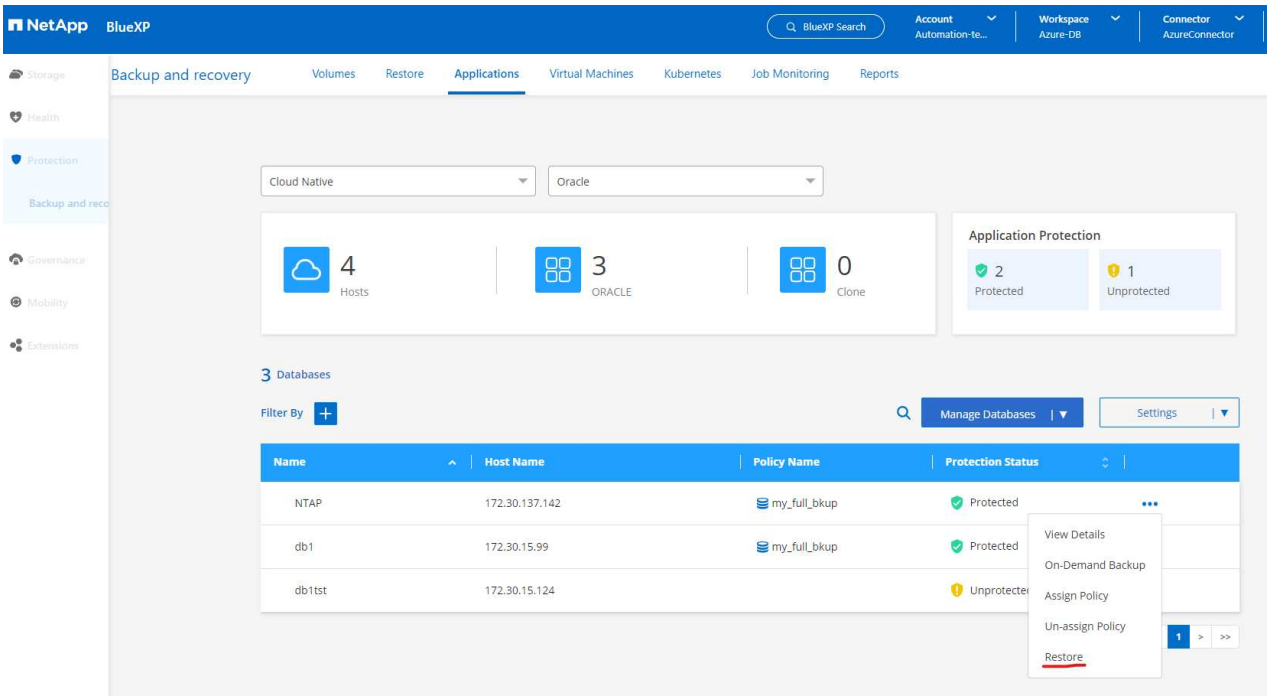


6. Les détails de sauvegarde de la base de données incluent le **Nom de la sauvegarde**, le **Type de sauvegarde**, le **SCN**, le **Catalogue RMAN** et l'**Heure de sauvegarde**. Un ensemble de sauvegarde contient des instantanés cohérents avec l'application pour le volume de données et le volume de journal respectivement. Un instantané du volume de journal a lieu juste après un instantané du volume de données de base de données. Vous pouvez appliquer un filtre si vous recherchez une sauvegarde particulière dans la liste de sauvegarde.

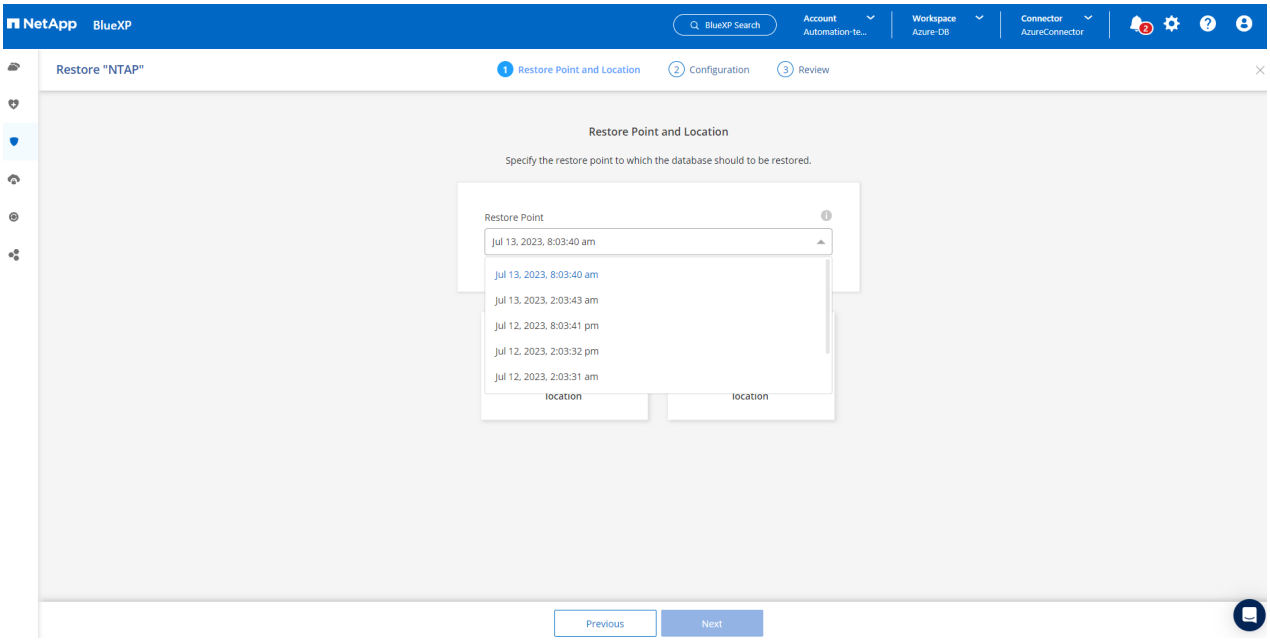


Restauration et récupération de bases de données Oracle

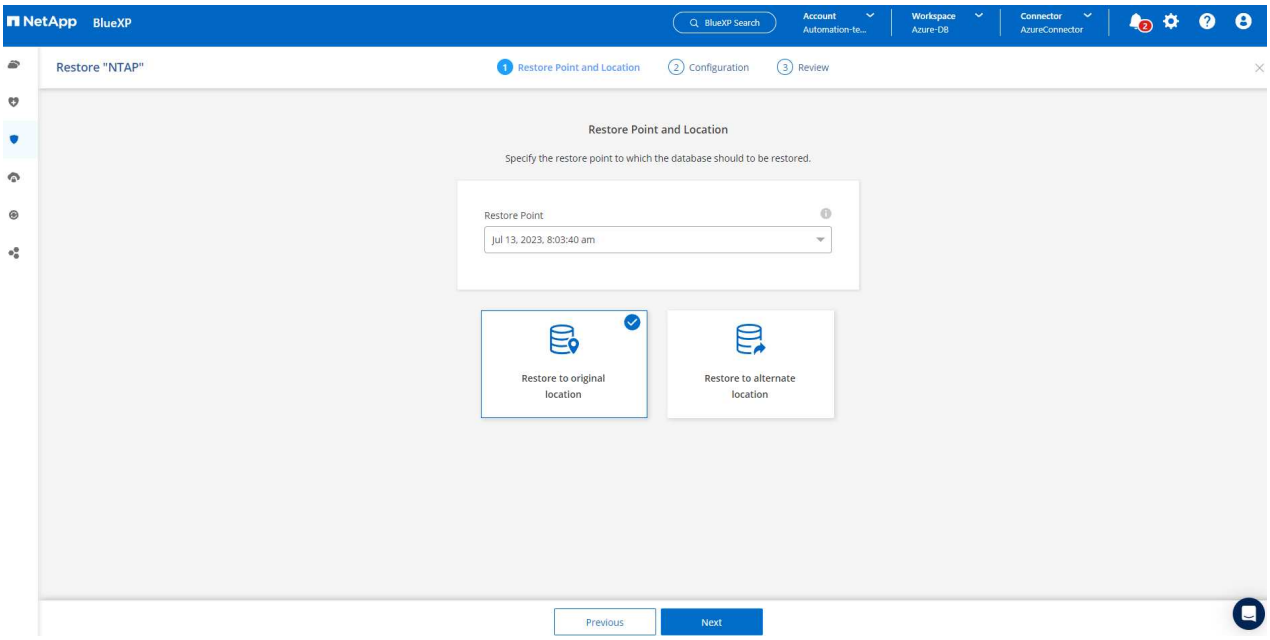
1. Pour restaurer une base de données, cliquez sur le menu déroulant à trois points correspondant à la base de données particulière à restaurer dans **Applications**, puis cliquez sur **Restaurer** pour lancer le flux de travail de restauration et de récupération de la base de données.



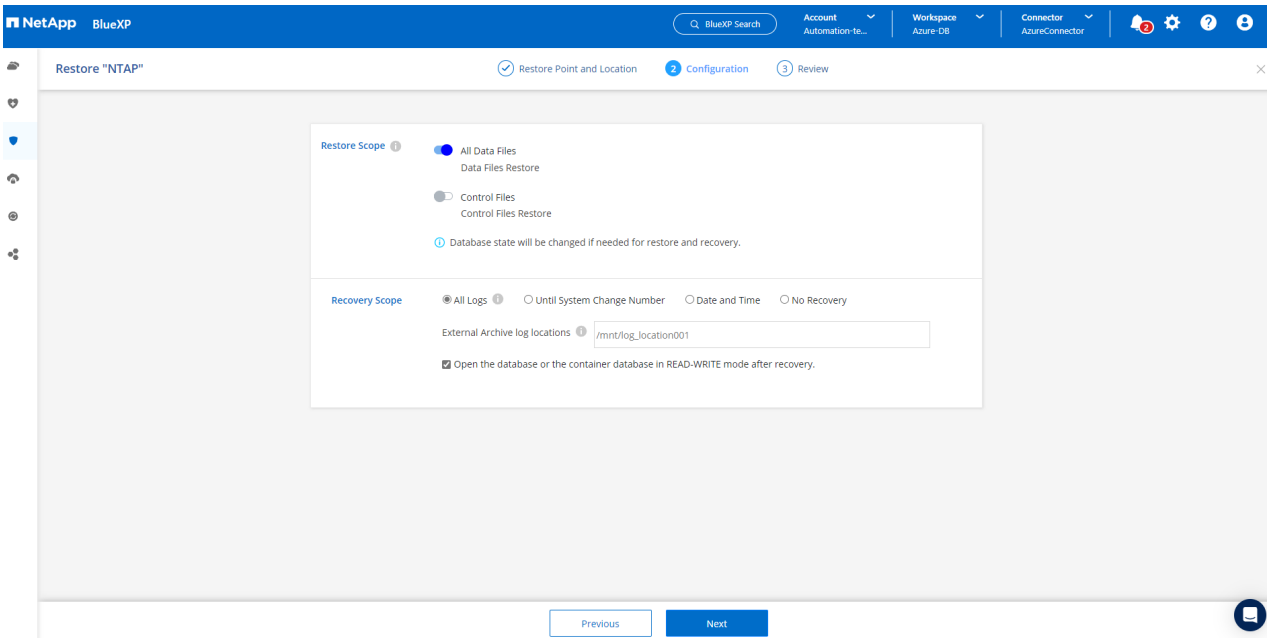
2. Choisissez votre **Point de restauration** par horodatage. Chaque horodatage de la liste représente un ensemble de sauvegarde de base de données disponible.



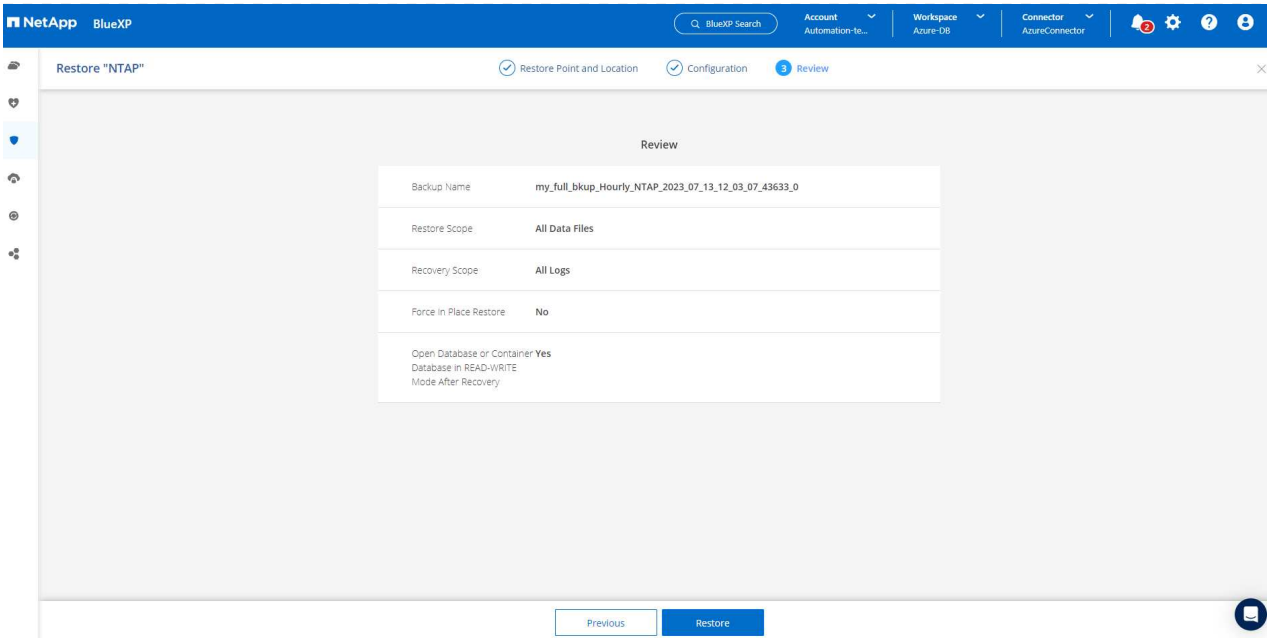
3. Choisissez votre **emplacement de restauration** vers **l'emplacement d'origine** pour une restauration et une récupération de base de données Oracle sur place.



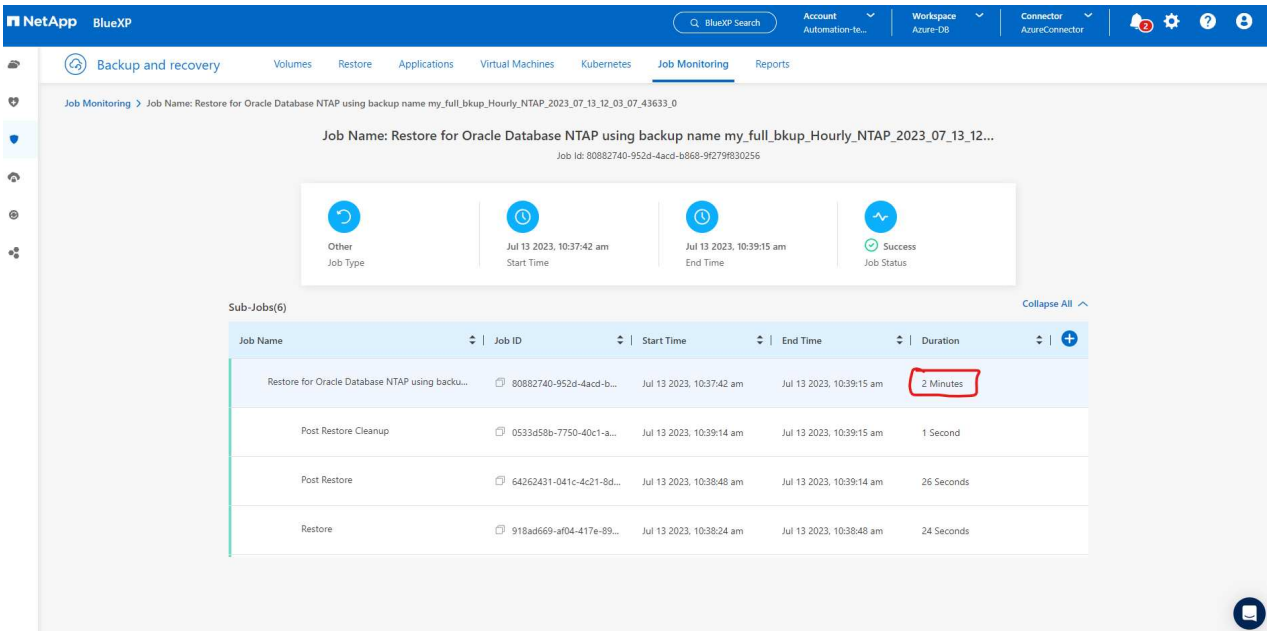
4. Définissez votre **étendue de restauration** et votre **étendue de récupération**. Tous les journaux signifient une récupération complète à jour, y compris les journaux actuels.



5. Révisez et **Restaurez** pour démarrer la restauration et la récupération de la base de données.



6. À partir de l'onglet **Surveillance des tâches**, nous avons observé qu'il fallait 2 minutes pour exécuter une restauration et une récupération complètes de la base de données à jour.

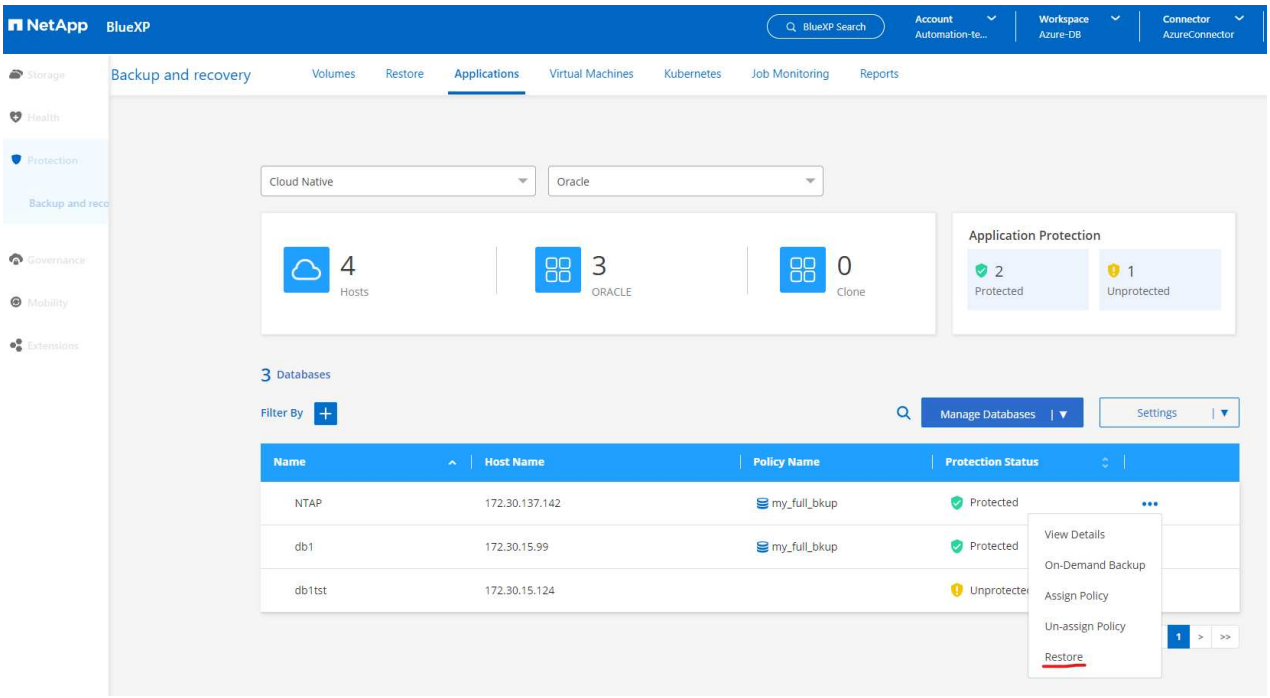


Clonage de base de données Oracle

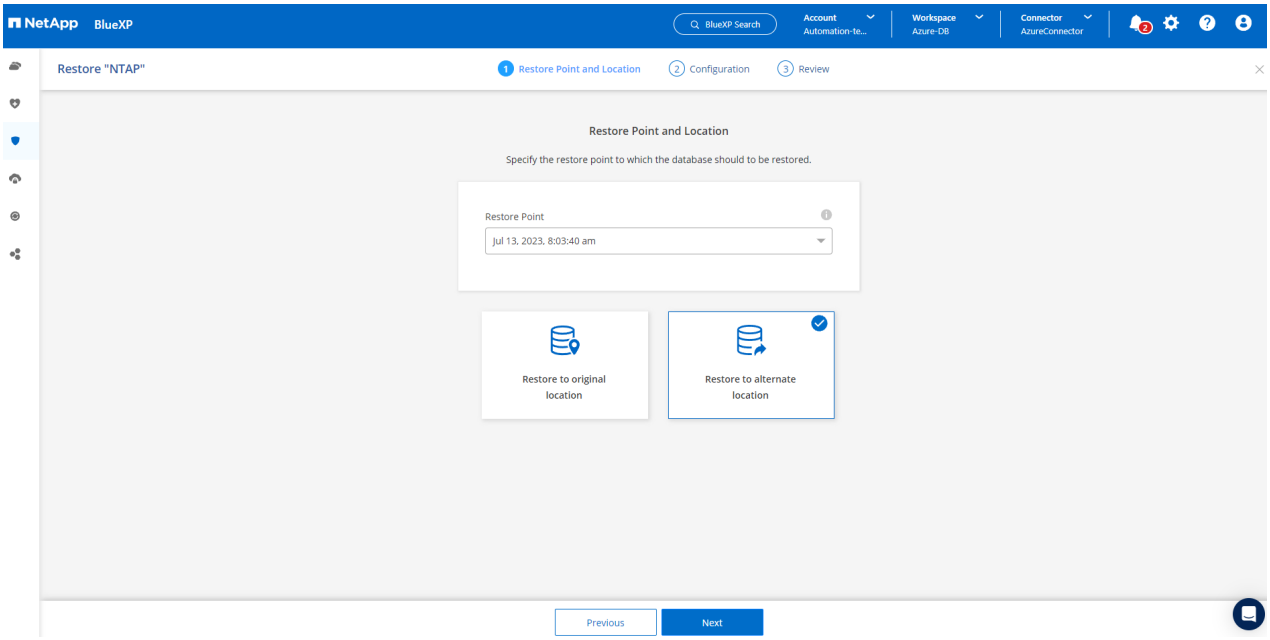
Les procédures de clonage de base de données sont similaires à la restauration, mais vers une machine virtuelle Azure alternative avec une pile logicielle Oracle identique préinstallée et configurée.

Assurez-vous que votre stockage Azure NetApp File dispose d'une capacité suffisante pour une base de données clonée de la même taille que la base de données principale à cloner. La machine virtuelle Azure alternative a été ajoutée à **Applications**.

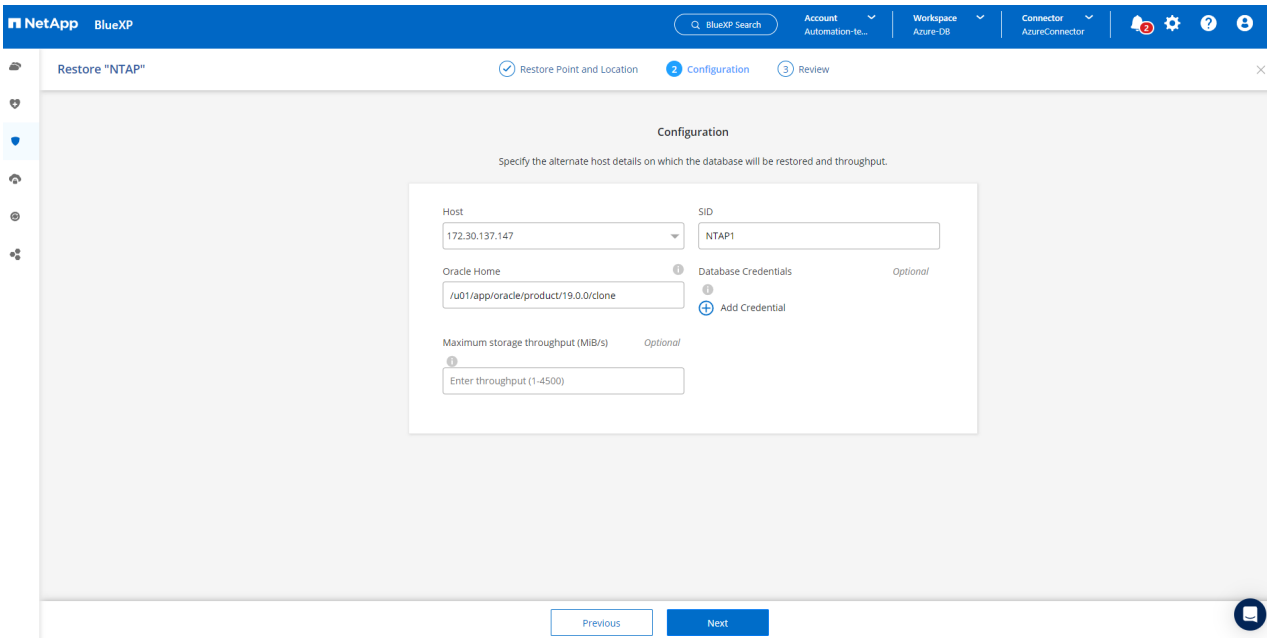
1. Cliquez sur le menu déroulant à trois points correspondant à la base de données particulière à cloner dans **Applications**, puis cliquez sur **Restaurer** pour lancer le flux de travail de clonage.



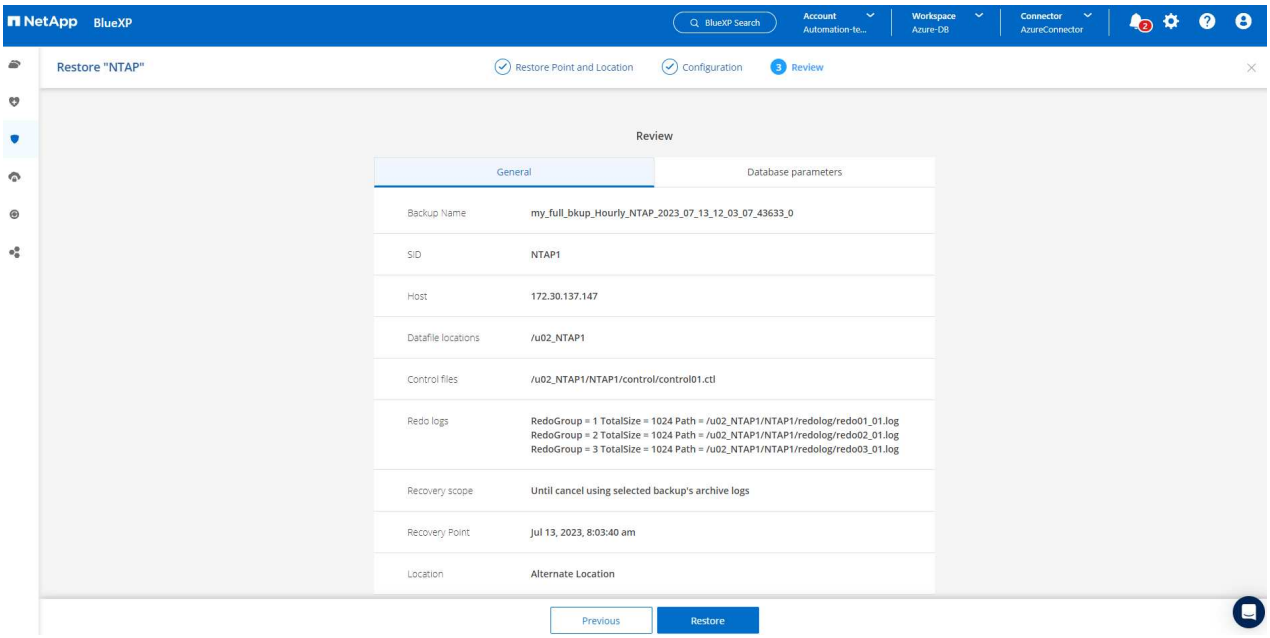
2. Sélectionnez le **Point de restauration** et cochez la case **Restaurer vers un autre emplacement**.



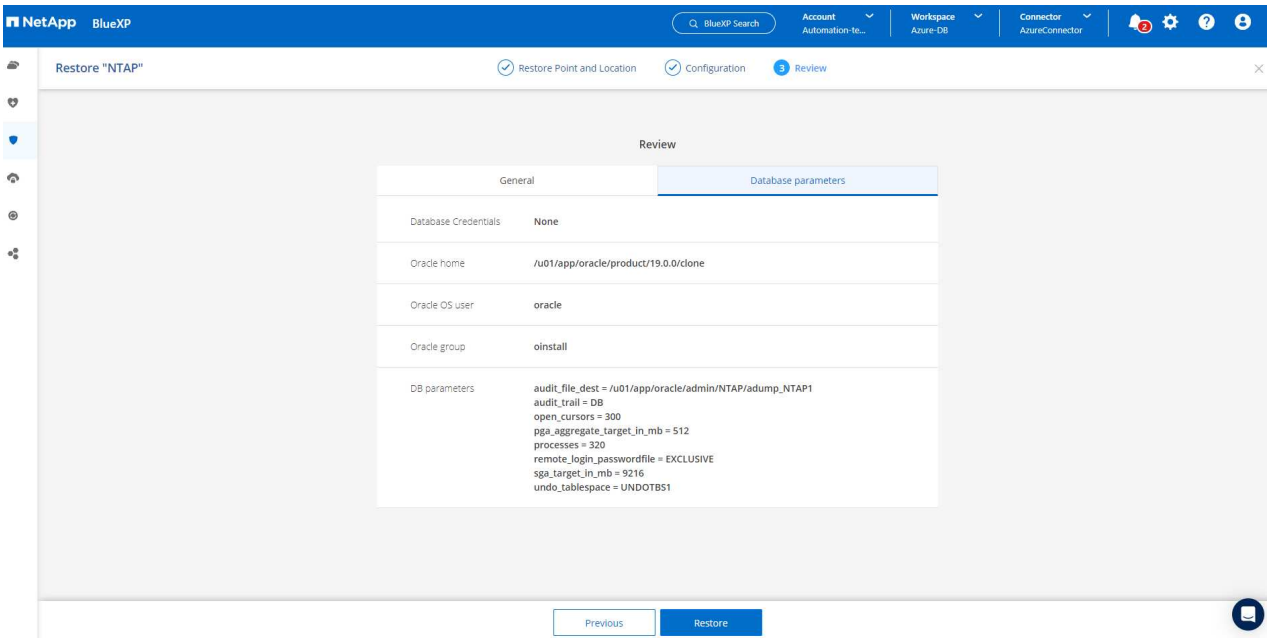
3. Dans la page **Configuration** suivante, définissez l'**Hôte** alternatif, le nouveau **SID** de base de données et **Oracle Home** comme configurés sur la machine virtuelle Azure alternative.



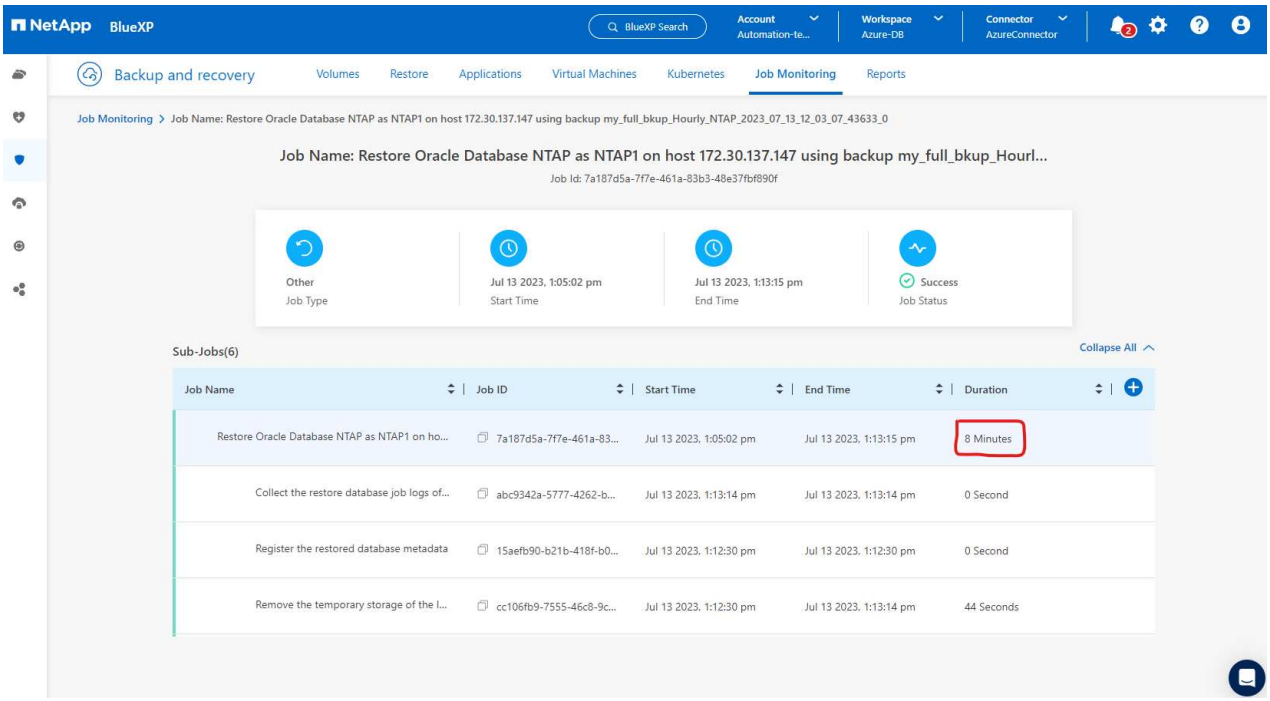
4. La page **Général** affiche les détails de la base de données clonée tels que le SID, l'hôte alternatif, les emplacements des fichiers de données, la portée de récupération, etc.



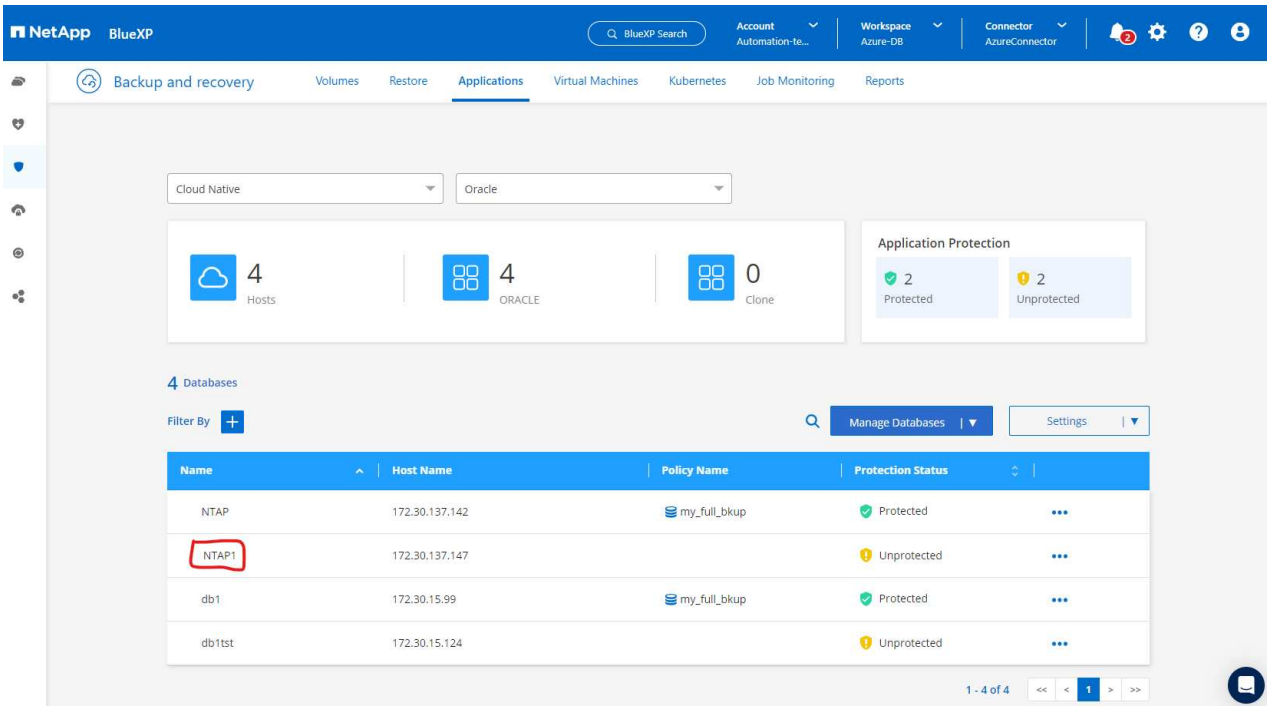
5. La page **Paramètres de la base de données** affiche les détails de la configuration de la base de données clonée ainsi que certains paramètres de la base de données.



6. Surveillez l'état du travail de clonage à partir de l'onglet **Surveillance des travaux**, nous avons observé qu'il fallait 8 minutes pour cloner une base de données Oracle de 1,6 Tio.



7. Validez la base de données clonée dans la page **Applications** de BlueXP qui a montré que la base de données clonée a été immédiatement enregistrée auprès de BlueXP.



8. Validez la base de données clonée sur la machine virtuelle Oracle Azure qui a montré que la base de données clonée fonctionnait comme prévu.

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



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

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

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

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


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

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

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

Ceci termine la démonstration d'une sauvegarde, d'une restauration et d'un clonage de base de données Oracle dans Azure avec la console NetApp BlueXP à l'aide de SnapCenter Service.

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"

- Azure NetApp Files

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

- Démarrer avec Azure

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

Informations sur le copyright

Informations sur les marques commerciales