SnapCenter pour bases de données

NetApp Solutions

NetApp
April 26, 2024

Sommaire

SnapCenter pour bases de données

SnapCenter automatisation du cycle de vie des clones Oracle

Allen Cao, Niyaz Mohamed, NetApp

Objectif

Les clients apprécient la fonctionnalité FlexClone du stockage NetApp ONTAP pour les bases de données, car elle permet de réaliser d'importantes économies en termes de coûts de stockage. Ce kit Ansible automatise la configuration, le clonage et l'actualisation des bases de données Oracle clonées selon un calendrier défini à l'aide des utilitaires de ligne de commande NetApp SnapCenter qui simplifient la gestion du cycle de vie. Ce kit s'applique aux bases de données Oracle déployées sur un système de stockage ONTAP sur site ou dans le cloud public, et gérées par l'outil d'interface utilisateur NetApp SnapCenter.

Cette solution répond aux cas d'utilisation suivants :

- Configurez le fichier de configuration de la spécification de clonage de la base de données Oracle.
- Créez et actualisez la base de données Oracle clone selon un planning défini par l'utilisateur.

Public

Cette solution est destinée aux personnes suivantes :

- Administrateur de bases de données qui gère les bases de données Oracle avec SnapCenter.
- Administrateur du stockage qui gère le stockage ONTAP avec SnapCenter.
- Propriétaire d'application ayant accès à l'interface utilisateur de SnapCenter.

Licence

En accédant au contenu de ce référentiel GitHub, en le téléchargeant, en l'installant ou en l'utilisant, vous acceptez les conditions de la licence énoncées dans "Fichier de licence".

> Il existe certaines restrictions concernant la production et/ou le partage de travaux dérivés avec le contenu de ce référentiel GitHub. Assurez-vous de lire les termes de la Licence avant d'utiliser le contenu. Si vous n'acceptez pas toutes les conditions, n'accédez pas au contenu de ce référentiel, ne le téléchargez pas et ne l'utilisez pas.

Déploiement de la solution

Conditions préalables au déploiement

Le déploiement nécessite les conditions préalables suivantes.

```
Ansible controller:
  Ansible v.2.10 and higher
  ONTAP collection 21.19.1
  Python 3
  Python libraries:
    netapp-lib
    xmltodict
    jmespath
```

```
SnapCenter server:
  version 5.0
  backup policy configured
  Source database protected with a backup policy
```

```
Oracle servers:
  Source server managed by SnapCenter
  Target server managed by SnapCenter
  Target server with identical Oracle software stack as source server
installed and configured
```

Téléchargez la boîte à outils

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-
bb/na_oracle_clone_lifecycle.git
```

Configuration des fichiers des hôtes cibles Ansible

Le kit d'outils inclut un fichier hosts qui définit les cibles sur lesquelles s'exécute un PlayBook Ansible. Il s'agit généralement des hôtes clones Oracle cibles. Voici un exemple de fichier. Une entrée d'hôte comprend l'adresse IP de l'hôte cible ainsi que la clé ssh permettant à un utilisateur admin d'accéder à l'hôte pour exécuter la commande clone ou refresh.

#Hôtes de clonage Oracle

```
[clone_1]
ora_04.cie.netapp.com ansible_host=10.61.180.29
ansible_ssh_private_key_file=ora_04.pem
```

```
[clone_2]
[clone_3]
```

Configuration des variables globales

Les playbooks Ansible prennent des entrées variables à partir de plusieurs fichiers variables. Vous trouverez ci-dessous un exemple de fichier de variable globale vars.yml.

```
# ONTAP specific config variables
# SnapCtr specific config variables
```

```
snapctr_usr: xxxxxxxx
snapctr_pwd: 'xxxxxxxx'
```

```
backup_policy: 'Oracle Full offline Backup'
# Linux specific config variables
# Oracle specific config variables
```

Configuration des variables hôte

Les variables hôtes sont définies dans le répertoire host_vars nommé {{ host_name }}.yml. Vous trouverez ci-dessous un exemple de fichier de variable hôte Oracle cible ora_04.cie.netapp.com.yml qui montre une configuration typique.

```
# User configurable Oracle clone db host specific parameters
```

```
# Source database to clone from
source_db_sid: NTAP1
source_db_host: ora_03.cie.netapp.com
```

```
# Clone database
clone_db_sid: NTAP1DEV
```

```
snapctr_obj_id: '{{ source_db_host }}\{{ source_db_sid }}'
```

Configuration du serveur Oracle cible de clone supplémentaire

La même pile logicielle Oracle doit être installée et corrigée pour le serveur Oracle cible de clone. $ORACLE_BASE et $ORACLE_HOME sont configurés pour l'utilisateur ORACLE .bash_profile. De plus, la variable $ORACLE_HOME doit correspondre au paramètre du serveur Oracle source. Voici un exemple.

```
# .bash_profile
```

```
# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi
```

```
# User specific environment and startup programs
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/NTAP1
```

Exécution de PlayBook

Au total, trois playbooks permettent d'exécuter le cycle de vie des clones d'une base de données Oracle avec les utilitaires de l'interface de ligne de commande SnapCenter.

1. Installez les prérequis du contrôleur Ansible, une seule fois.

```
ansible-playbook -i hosts ansible_requirements.yml
```

2. Fichier de spécification de clone de configuration - une seule fois.

```
ansible-playbook -i hosts clone_1_setup.yml -u admin -e
@vars/vars.yml
```

3. Créez et actualisez régulièrement la base de données de clones à partir de crontab avec un script shell pour appeler un PlayBook d'actualisation.

```
0 */4 * * * /home/admin/na_oracle_clone_lifecycle/clone_1_refresh.sh
```

Pour une base de données clone supplémentaire, créez un clone_n_setup.yml et un clone_n_refresh.yml et un clone_n_refresh.sh. Configurez les hôtes cibles Ansible et le fichier hostname.yml dans le répertoire host_vars en conséquence.

Où trouver des informations complémentaires

Pour en savoir plus sur l'automatisation de la solution NetApp, consultez ce site Web "Automatisation des solutions NetApp"

Tr-4988 : sauvegarde, restauration et clonage de bases de données Oracle sur ANF avec SnapCenter

Allen Cao, Niyaz Mohamed, NetApp

Objectif

Le logiciel SnapCenter est une plateforme qui permet de coordonner et de gérer facilement et en toute sécurité la protection de vos données sur l'ensemble des applications, bases de données et systèmes de fichiers. Elle simplifie la gestion du cycle de vie des sauvegardes, des restaurations et des clones en confiant ces tâches aux propriétaires des applications, tout en gardant leur capacité à superviser et réguler l'activité au niveau des systèmes de stockage. En exploitant la gestion des données de stockage, il améliore la performance et la disponibilité, tout en réduisant le temps consacré au développement et aux tests.

Dans le document TR-4987, "Déploiement Oracle simplifié et automatisé sur Azure NetApp Files avec NFS", Nous présentons le déploiement automatisé Oracle sur Azure NetApp Files (ANF) dans le cloud Azure. Dans cette documentation, nous présentons la protection et la gestion des bases de données Oracle sur ANF dans le cloud Azure grâce à un outil d'interface utilisateur SnapCenter très convivial.

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde et restauration des bases de données Oracle déployées sur ANF dans le cloud Azure avec SnapCenter.
- Gérez les copies Snapshot de base de données et les copies de clone pour accélérer le développement d'applications et améliorer la gestion du cycle de vie des données.

Public

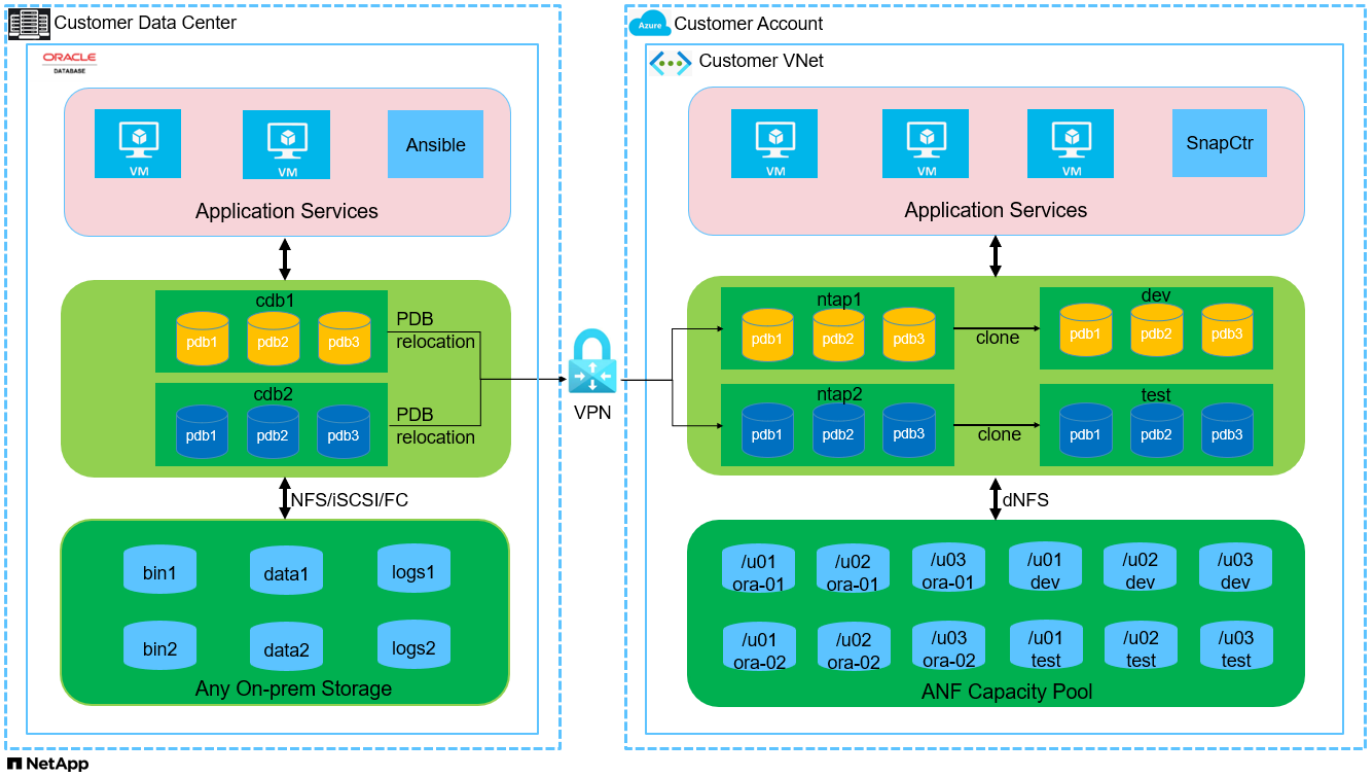
Cette solution est destinée aux personnes suivantes :

- Administrateur de base de données qui souhaite déployer des bases de données Oracle sur Azure NetApp Files.
- Architecte de solutions de bases de données qui souhaite tester les workloads Oracle sur Azure NetApp Files.
- Administrateur du stockage qui souhaite déployer et gérer des bases de données Oracle sur Azure NetApp Files.
- Propriétaire d'application qui souhaite créer une base de données Oracle sur Azure NetApp Files.

Environnement de test et de validation de la solution

Les tests et la validation de cette solution ont été réalisés dans un environnement de laboratoire qui ne correspond peut-être pas à l'environnement de déploiement final. Voir la section [Key Factors for Deployment Consideration] pour en savoir plus.

Architecture



Composants matériels et logiciels

Matériel		
Azure NetApp Files	Offre actuelle dans Azure de Microsoft	Un pool de capacité avec le niveau de service Premium
Serveur de base de données Azure VM	Standard_B4ms - 4 vCPU, 16 Gio	Deux instances de machine virtuelle Linux
Azure VM pour SnapCenter	Standard_B4ms - 4 vCPU, 16 Gio	Une instance de machine virtuelle Windows
Logiciel		
Red Hat Linux	RHEL Linux 8.6 (LVM) - x64 Gen2	Déploiement de l'abonnement Red Hat pour les tests
Serveur Windows	2022 datacenter ; correctif AE - x64 Gen2	Hébergement du serveur SnapCenter
Base de données Oracle	Version 19.18	Correctif p34765931_190000_Linux-x86-64.zip
OPICH Oracle	Version 12.2.0.1.36	Correctif p6880880_190000_Linux-x86-64.zip
Serveur SnapCenter	Version 5.0	Déploiement de groupes de travail
Ouvrez JDK	Version Java-11-openjdk	Plug-in SnapCenter requis sur les VM de base de données
NFS	Version 3.0	Oracle dNFS activé
Ansible	noyau 2.16.2	Python 3.6.8

Configuration de la base de données Oracle dans l'environnement de laboratoire

Serveur	Base de données	Stockage DB
ora-01	NTAP1(NTAP1_PDB1,NTAP1_PDB2,NTAP1_PDB3)	Montages NFS /u01, /u02, /u03 sur le pool de capacité d'ANF
ora-02	NTAP2(NTAP2_PDB1,NTAP2_PDB2,NTAP2_PDB3)	Montages NFS /u01, /u02, /u03 sur le pool de capacité d'ANF

Facteurs clés à prendre en compte lors du déploiement

- **Déploiement SnapCenter.** SnapCenter peut être déployé dans un domaine Windows ou un environnement de groupe de travail. Pour un déploiement basé sur un domaine, le compte utilisateur de domaine doit être un compte administrateur de domaine ou l'utilisateur de domaine appartient au groupe de l'administrateur local sur le serveur d'hébergement SnapCenter.
- **Résolution de nom.** le serveur SnapCenter doit résoudre le nom en adresse IP pour chaque hôte de serveur de base de données cible géré. Chaque hôte de serveur de base de données cible doit convertir le nom du serveur SnapCenter en adresse IP. Si un serveur DNS n'est pas disponible, ajoutez un nom aux fichiers hôte locaux pour la résolution.

- **Configuration du groupe de ressources.** le groupe de ressources dans SnapCenter est un regroupement logique de ressources similaires pouvant être sauvegardées ensemble. Il simplifie et réduit ainsi le nombre de tâches de sauvegarde dans un environnement de base de données volumineux.
- **Sauvegarde complète séparée de la base de données et du journal d'archives.** la sauvegarde complète de la base de données inclut les volumes de données et les volumes de journal des snapshots de groupe cohérents. Un Snapshot fréquent de base de données complète entraîne une consommation de stockage plus élevée, mais améliore le RTO. Il est également possible d'utiliser des copies Snapshot de base de données complètes moins fréquentes et des sauvegardes de journaux d'archivage plus fréquentes. Cela consomme moins de stockage et améliore le RPO, mais peut étendre le RTO. Tenez compte de vos objectifs RTO et RPO lors de la configuration du schéma de sauvegarde. Le nombre de sauvegardes Snapshot sur un volume est également limité (1023).
- **Délégation de privilèges.** tirer parti du contrôle d'accès basé sur les rôles intégré à l'interface utilisateur SnapCenter pour déléguer des privilèges aux équipes d'applications et de bases de données si nécessaire.

Déploiement de la solution

Les sections suivantes présentent des procédures détaillées pour le SnapCenter déploiement, la configuration et la sauvegarde, la restauration et le clonage de bases de données Oracle sur Azure NetApp Files dans le cloud Azure.

Conditions préalables au déploiement

Le déploiement nécessite l'exécution de bases de données Oracle sur ANF dans Azure. Si ce n'est pas le cas, suivez les étapes ci-dessous pour créer deux bases de données Oracle pour la validation de la solution. Pour en savoir plus sur le déploiement d'une base de données Oracle sur ANF dans le cloud Azure avec automatisation, consultez le document TR-4987 : "Déploiement Oracle simplifié et automatisé sur Azure NetApp Files avec NFS"

1. Un compte Azure a été configuré et les segments réseau et vnet nécessaires ont été créés dans votre compte Azure.
2. Depuis le portail cloud Azure, déployez les VM Azure Linux en tant que serveurs de base de données Oracle. Créez un pool de capacité Azure NetApp Files et des volumes de base de données pour la base de données Oracle. Activer l'authentification de clés privées/publiques SSH sur machine virtuelle pour l'azuretutilisateur vers les serveurs de base de données. Pour plus d'informations sur la configuration de l'environnement, reportez-vous au schéma d'architecture de la section précédente. Également mentionné à "Procédures détaillées de déploiement d'Oracle sur Azure VM et Azure NetApp Files" pour des informations détaillées.

   > Pour les machines virtuelles Azure déployées avec redondance de disque local, assurez-vous d'avoir alloué au moins 128 G au disque racine de la machine virtuelle pour disposer de l'espace suffisant pour préparer les fichiers d'installation Oracle et ajouter le fichier d'échange du système d'exploitation. Développez la partition /tmplv et /rootlv OS en conséquence. Assurez-vous que le nom du volume de la base de données respecte les conventions VMname-u01, VMname-u02 et VMname-u03.

   ```
   sudo lvresize -r -L +20G /dev/mapper/rootvg-rootlv
   ```

   ```
   sudo lvresize -r -L +10G /dev/mapper/rootvg-tmplv
   ```

3. Provisionnez un serveur Windows à partir du portail cloud Azure pour exécuter l'outil de l'interface utilisateur NetApp SnapCenter avec la dernière version. Pour plus de détails, cliquez sur le lien suivant : "Installez le serveur SnapCenter".
4. Provisionnez une VM Linux en tant que nœud de contrôleur Ansible avec la dernière version d'Ansible et de Git installée. Pour plus de détails, cliquez sur le lien suivant : "Commencer à utiliser l'automatisation des solutions NetApp" dans la section - `Setup the Ansible Control Node for CLI deployments on RHEL / CentOS` ou `Setup the Ansible Control Node for CLI deployments on Ubuntu / Debian`.

   > Le nœud de contrôleur Ansible peut localiser soit sur site, soit dans le cloud Azure jusqu'à ce qu'il puisse accéder aux VM de base de données Azure via le port ssh.

5. Clonez une copie du kit d'outils d'automatisation du déploiement NetApp pour Oracle pour NFS. Suivez les instructions de la section "TR-4887" pour exécuter les playbooks.

   ```
   git clone https://bitbucket.ngage.netapp.com/scm/ns-
   bb/na_oracle_deploy_nfs.git
   ```

6. Procédez comme suit : fichiers d'installation Oracle 19c sur le répertoire VM /tmp/archive du BDD

Azure avec l'autorisation 777.

```
installer_archives:
  - "LINUX.X64_193000_db_home.zip"
  - "p34765931_190000_Linux-x86-64.zip"
  - "p6880880_190000_Linux-x86-64.zip"
```

7. Regardez la vidéo suivante :

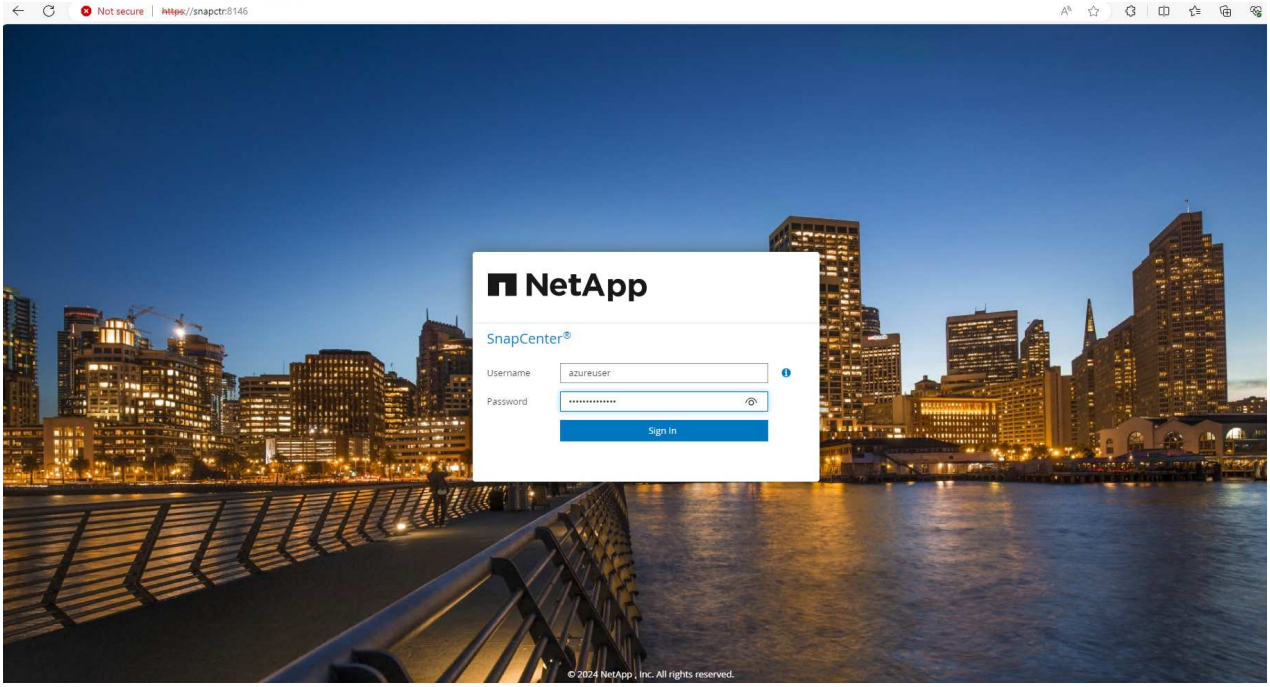
   Sauvegarde, restauration et clonage de bases de données Oracle sur ANF avec SnapCenter

8. Vérifiez le `Get Started` menu en ligne.

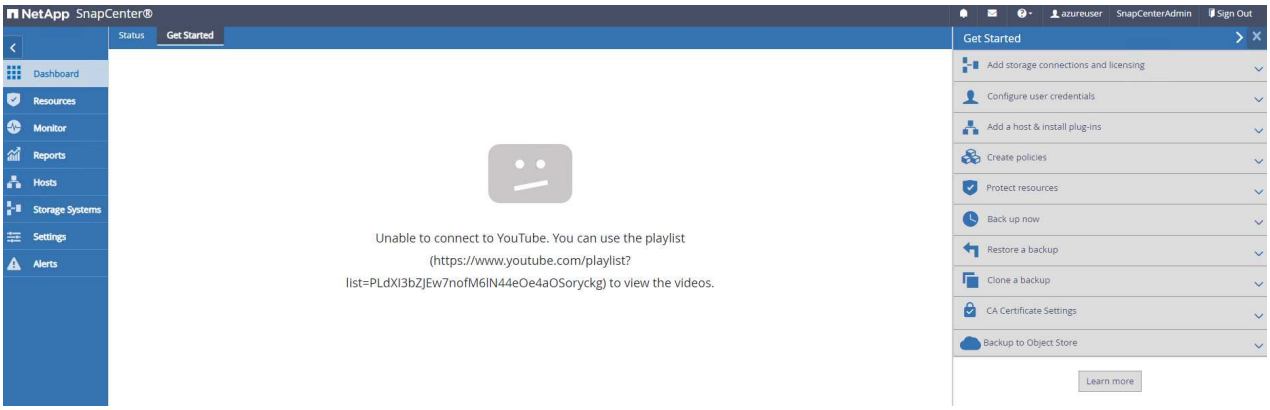
Installation et configuration de SnapCenter

Nous vous recommandons de consulter en ligne "Documentation du logiciel SnapCenter" Avant de passer à l'installation et à la configuration de SnapCenter : . Voici un résumé détaillé des étapes d'installation et de configuration du logiciel SnapCenter pour Oracle sur Azure ANF.

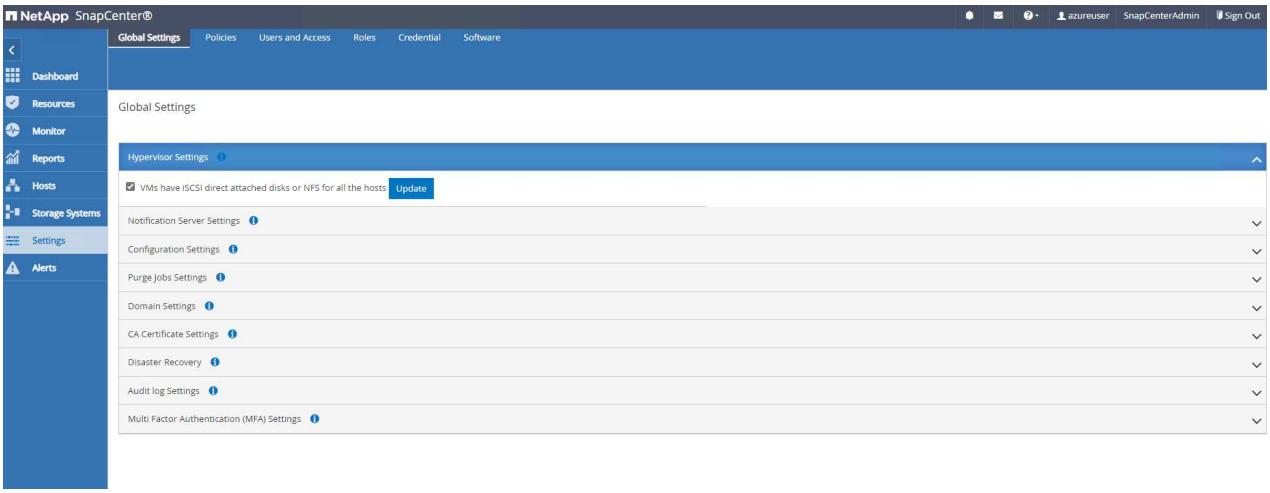
1. À partir du serveur Windows SnapCenter, téléchargez et installez le dernier JDK Java à partir de "Obtenir Java pour les applications de bureau".
2. À partir du serveur Windows SnapCenter, téléchargez et installez la dernière version (actuellement 5.0) du fichier exécutable d'installation SnapCenter sur le site de support NetApp : "NetApp | support".
3. Après l'installation du serveur SnapCenter, lancez le navigateur pour vous connecter à SnapCenter avec les informations d'identification de l'utilisateur administrateur local ou du domaine Windows via le port 8146.



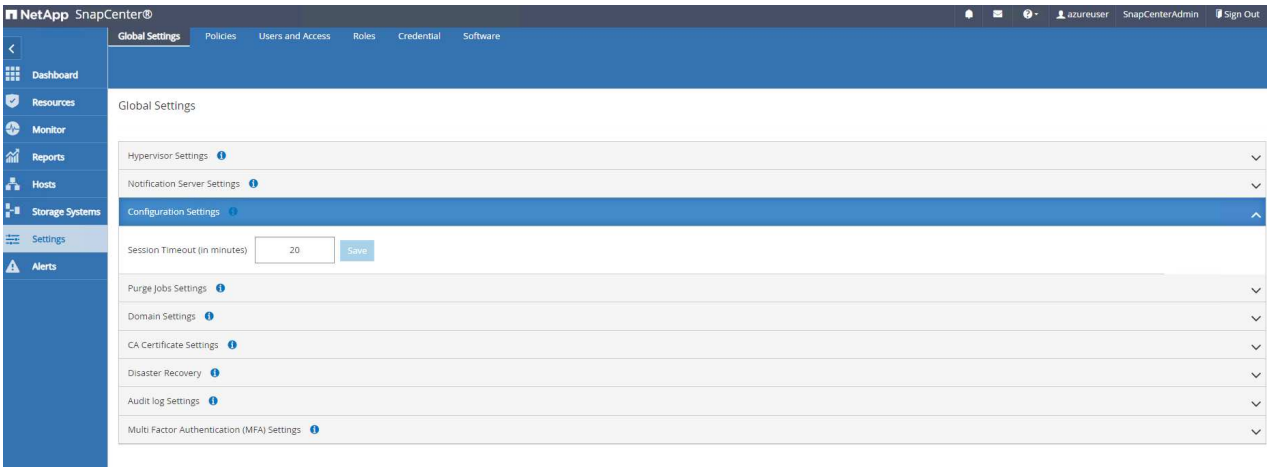
4. Révision `Get Started` menu en ligne.



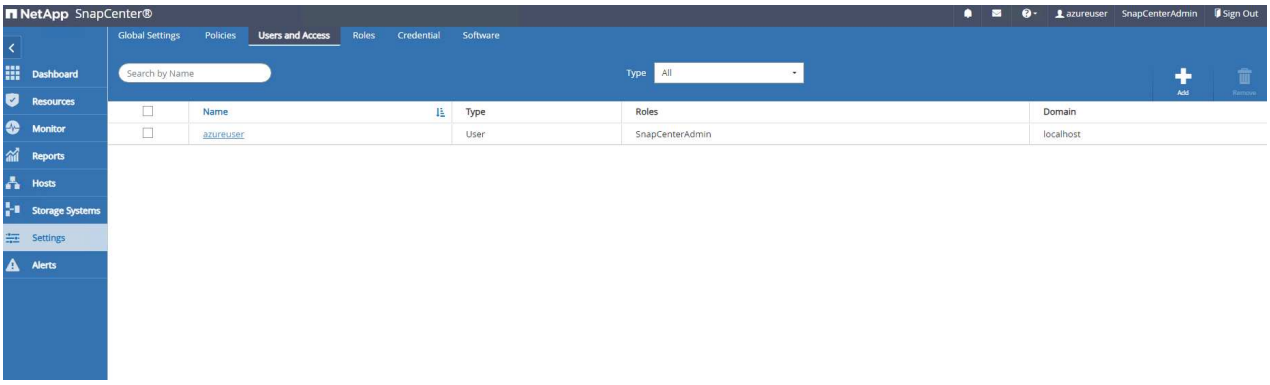
5. Dans `Settings-Global Settings`, vérifier `Hypervisor Settings` Et cliquez sur mettre à jour.



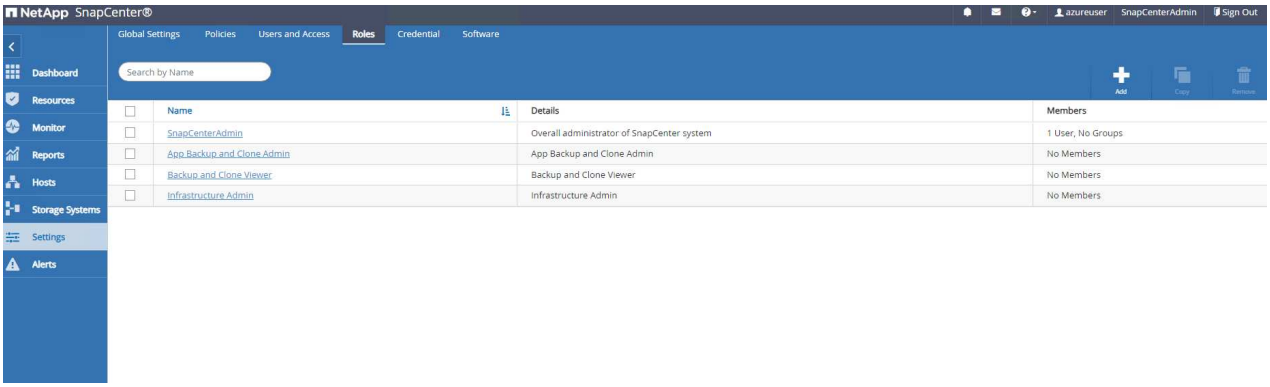
6. Au besoin, régler `Session Timeout` Pour l'interface utilisateur SnapCenter à l'intervalle souhaité.



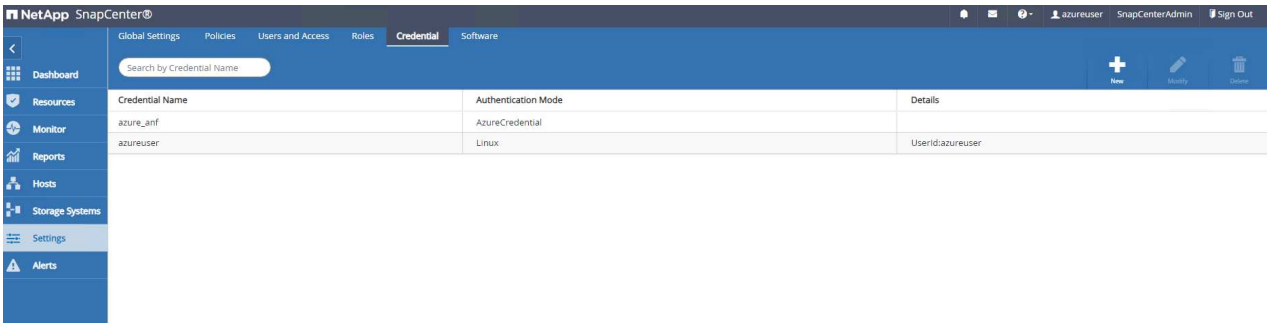
7. Ajoutez des utilisateurs supplémentaires à SnapCenter si nécessaire.

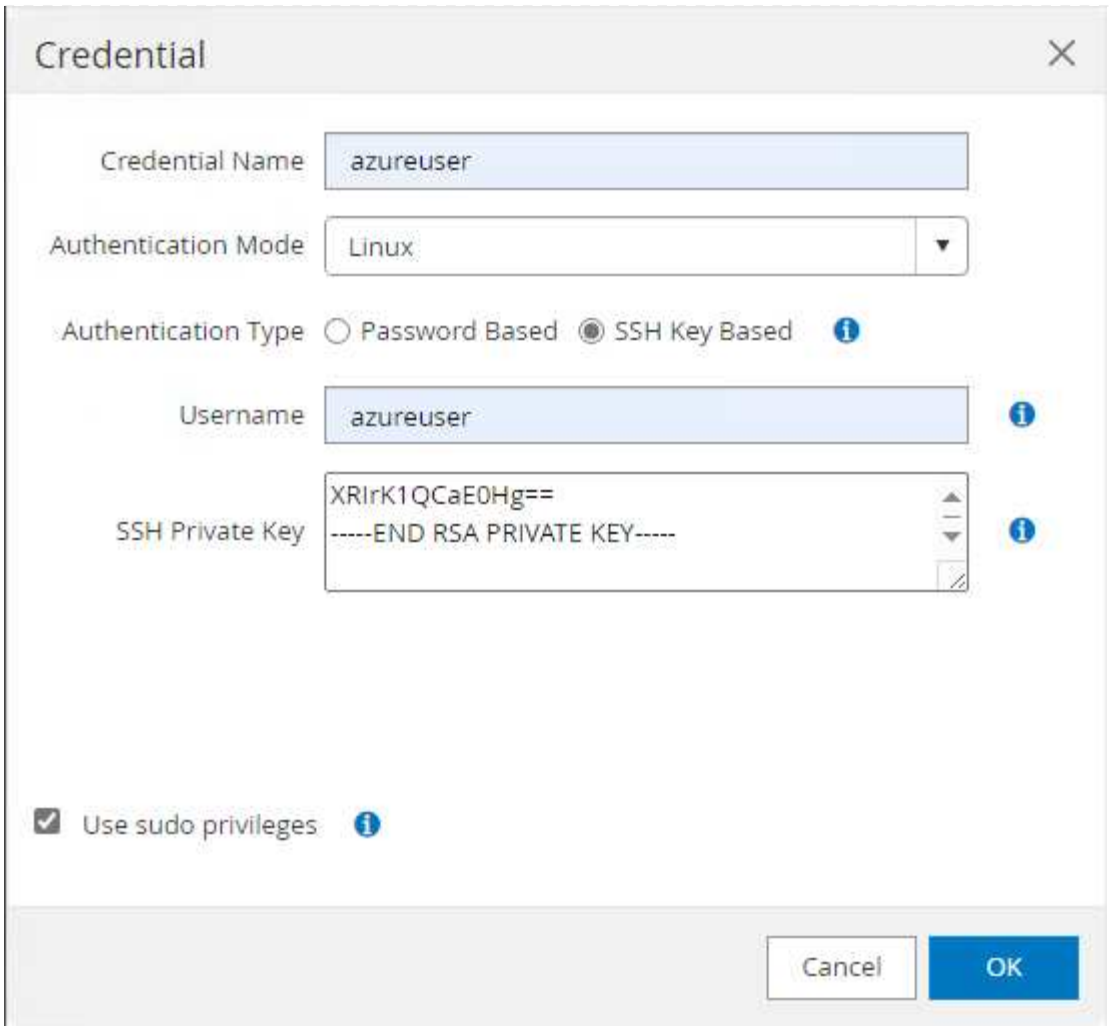


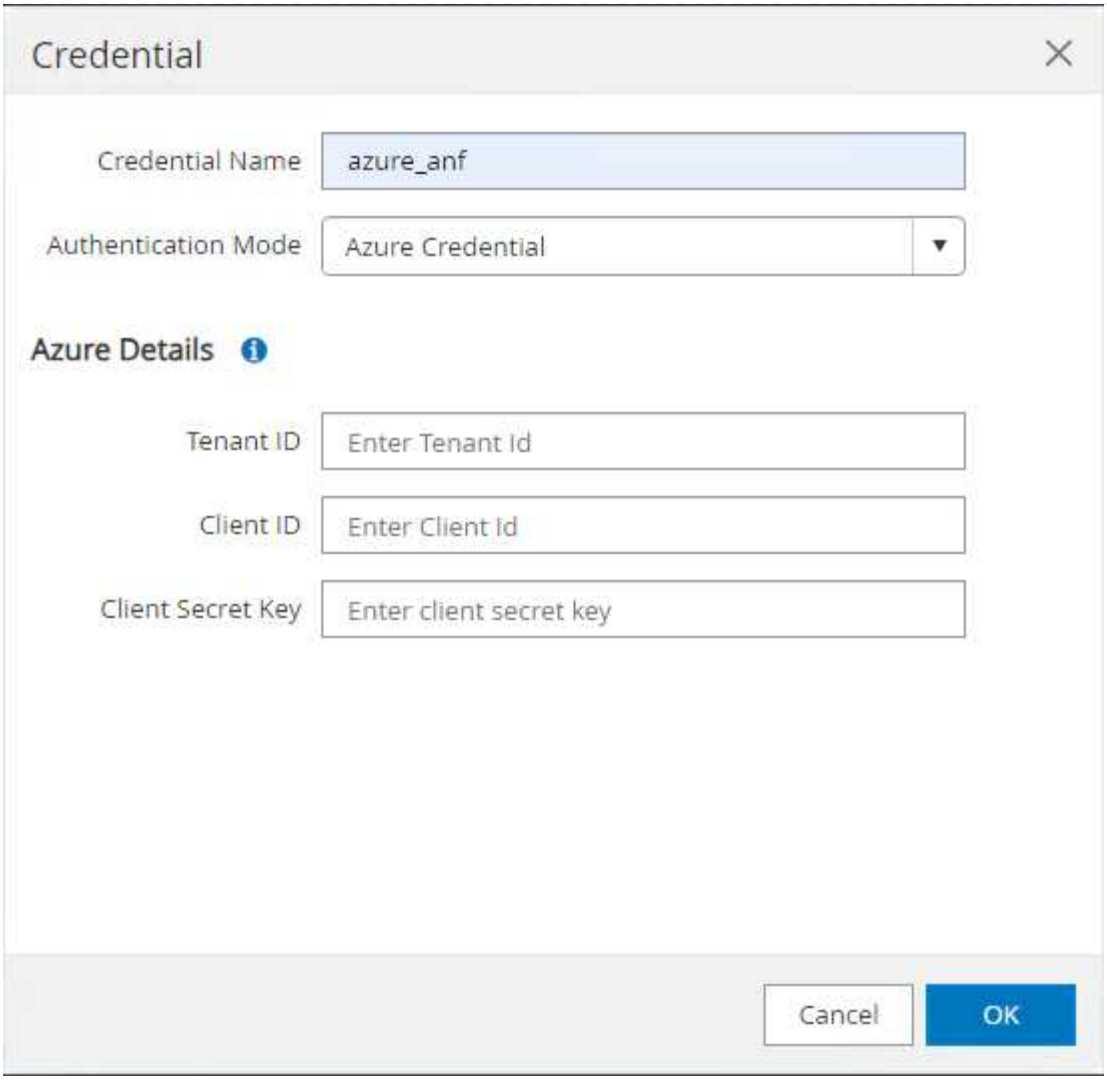
8. Le `Roles` Répertorie les rôles intégrés pouvant être attribués à différents utilisateurs SnapCenter. Les rôles personnalisés peuvent également être créés par l'utilisateur administrateur avec les privilèges souhaités.



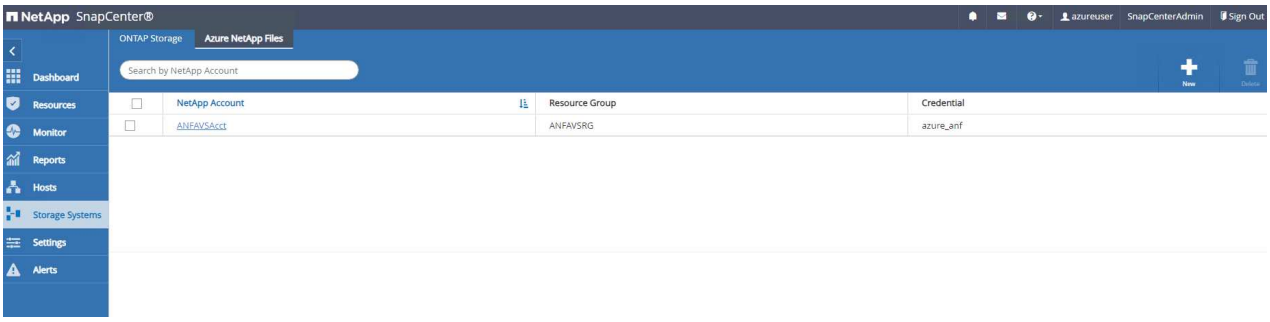
9. De `Settings-Credential`, Créez des informations d'identification pour les cibles de gestion SnapCenter. Dans cette démonstration, il s'agit d'un utilisateur linux qui se connecte à Azure VM et des informations d'identification ANF pour l'accès au pool de capacité.



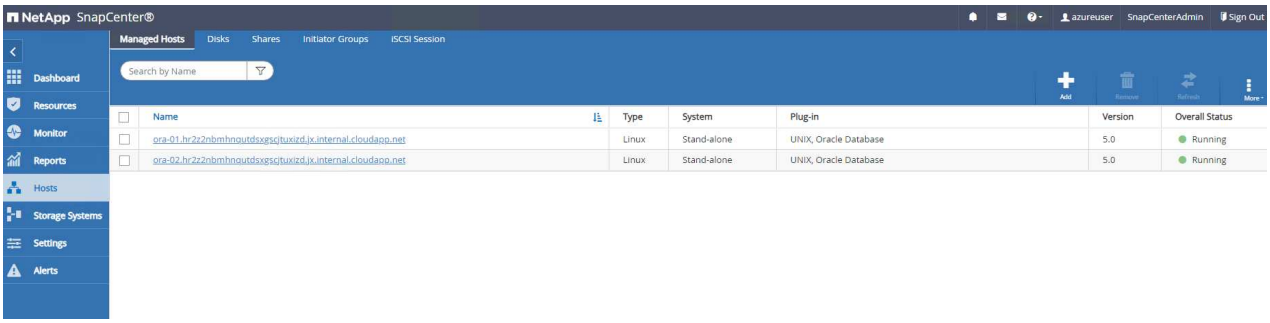

Credential
Credential Name
azureuser
Authentication Mode
Linux
Authentication Type
Password Based
SSH Key Based
Username
azureuser
SSH Private Key
XRIrK1QCaE0Hg==
-----END RSA PRIVATE KEY-----
Use sudo privileges
Cancel
OK

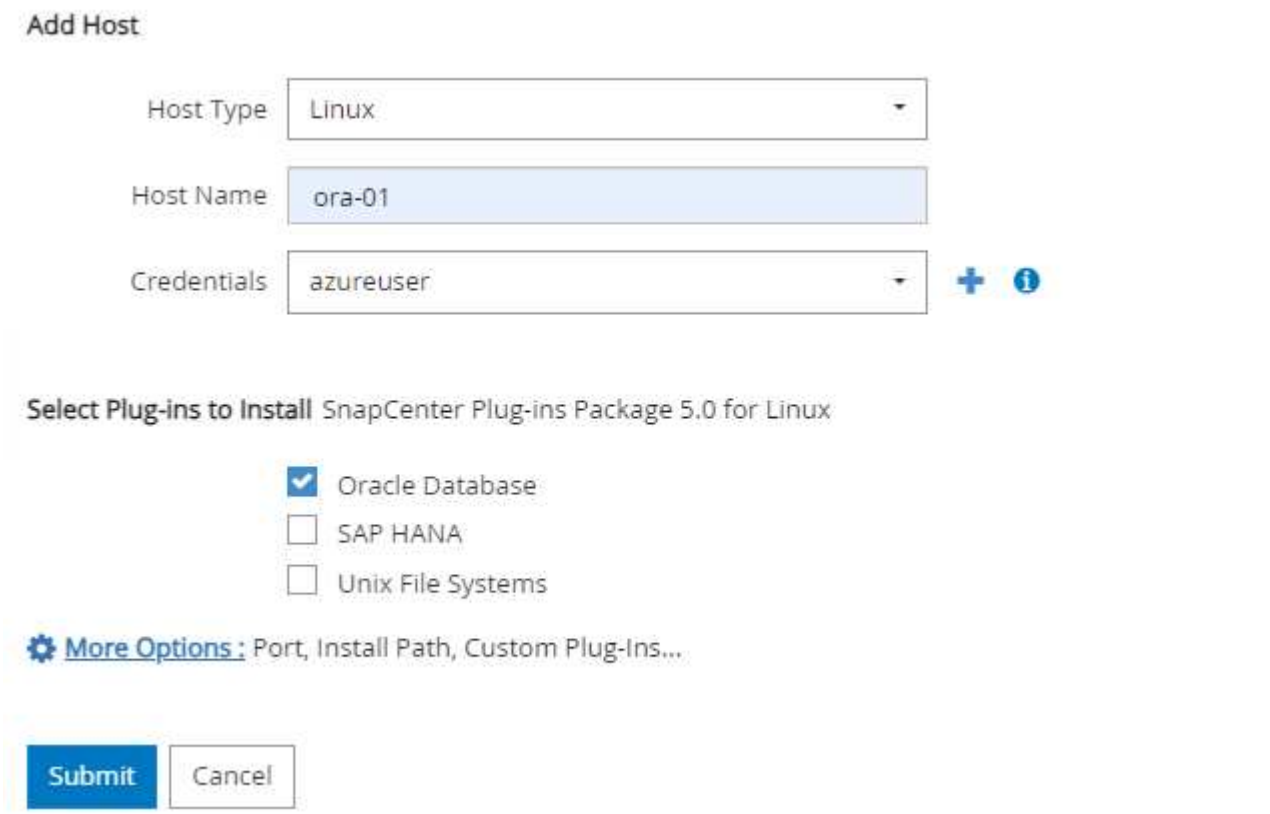


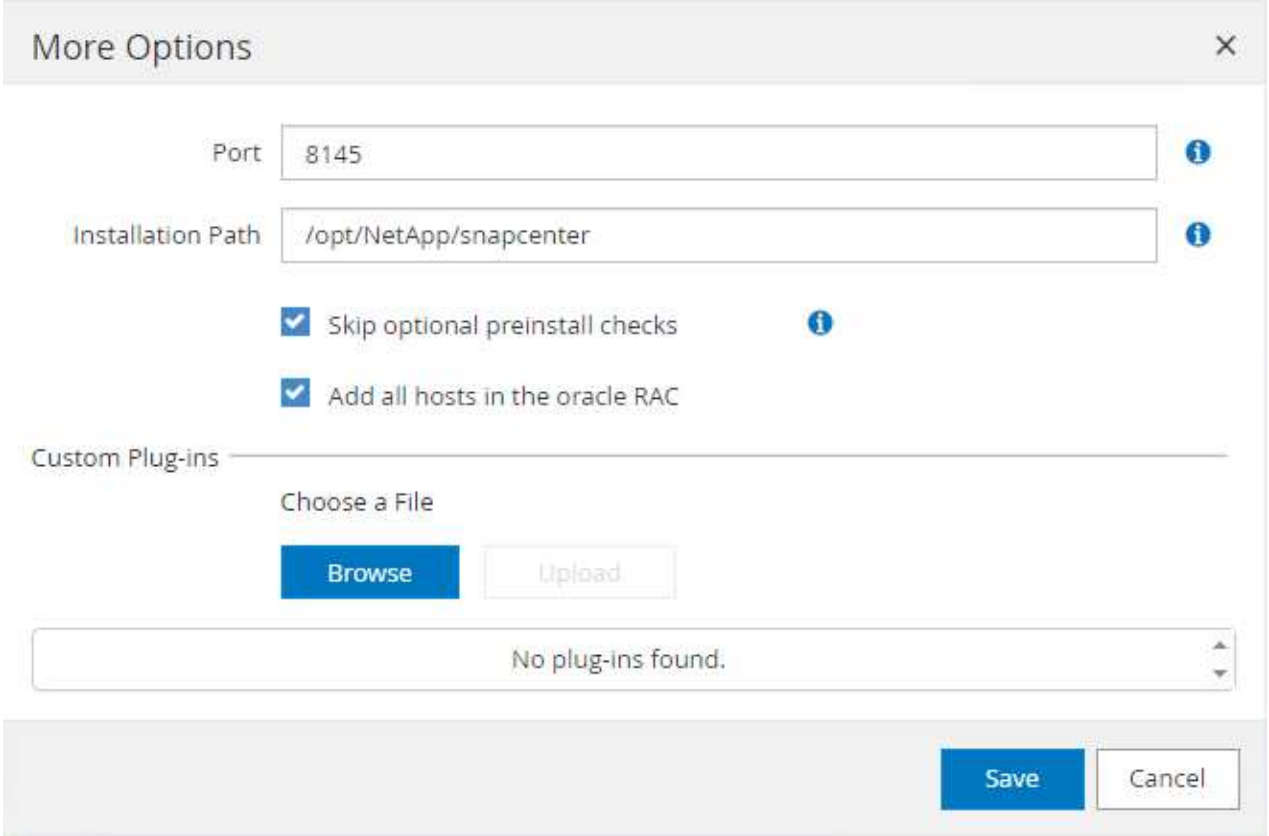
10. De `Storage Systems` ajouter `Azure NetApp Files` avec les informations d'identification créées ci-dessus.



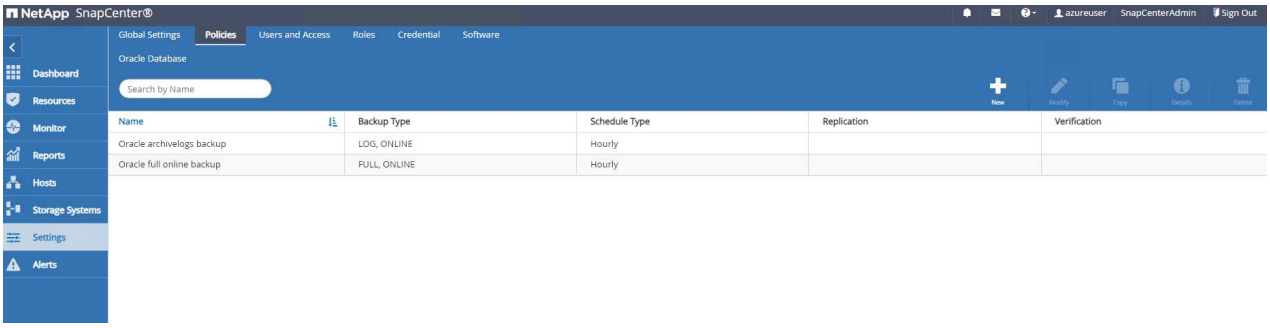
11. De `Hosts` Ajoutez les VM de base de données Azure, qui installent le plug-in SnapCenter pour Oracle sous Linux.







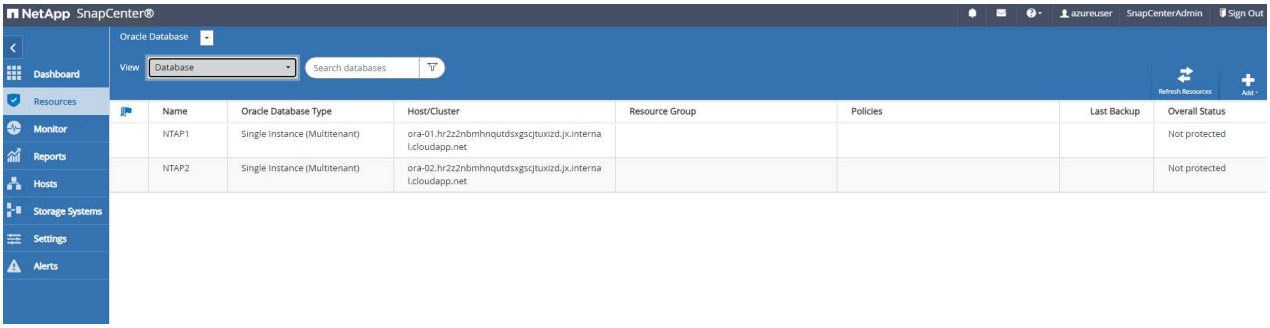
12. Une fois le plug-in hôte installé sur la machine virtuelle du serveur de base de données, les bases de données sur l'hôte sont automatiquement découvertes et visibles dans `Resources` onglet. Retour à `Settings-Polices`, Créez des stratégies de sauvegarde pour la sauvegarde complète en ligne de la base de données Oracle et la sauvegarde des journaux d'archivage uniquement. Reportez-vous à ce document "Créez des règles de sauvegarde pour les bases de données Oracle" pour les procédures détaillées étape par étape.



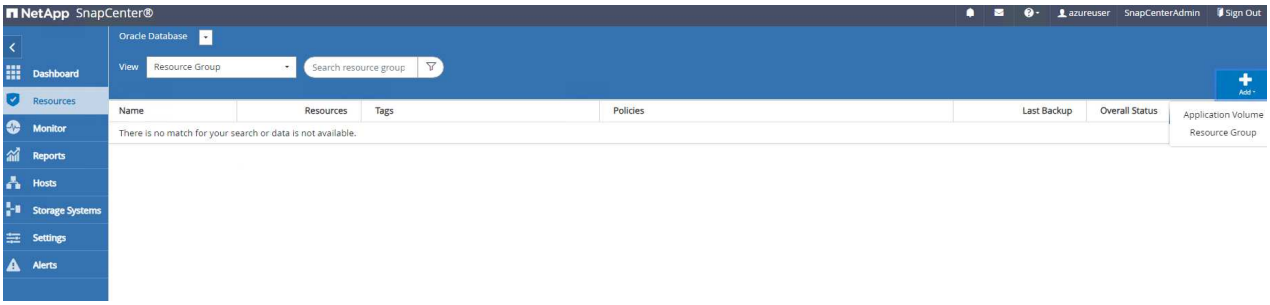
Sauvegarde de la base de données

Une sauvegarde Snapshot NetApp crée une image instantanée des volumes de base de données que vous pouvez utiliser pour restaurer en cas de panne système ou de perte de données. Les sauvegardes Snapshot prennent très peu de temps, généralement moins d'une minute. L'image de sauvegarde consomme un espace de stockage minimal et présente un impact négligeable sur les performances, car elle n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot. La section suivante décrit la mise en œuvre de snapshots pour la sauvegarde de bases de données Oracle dans SnapCenter.

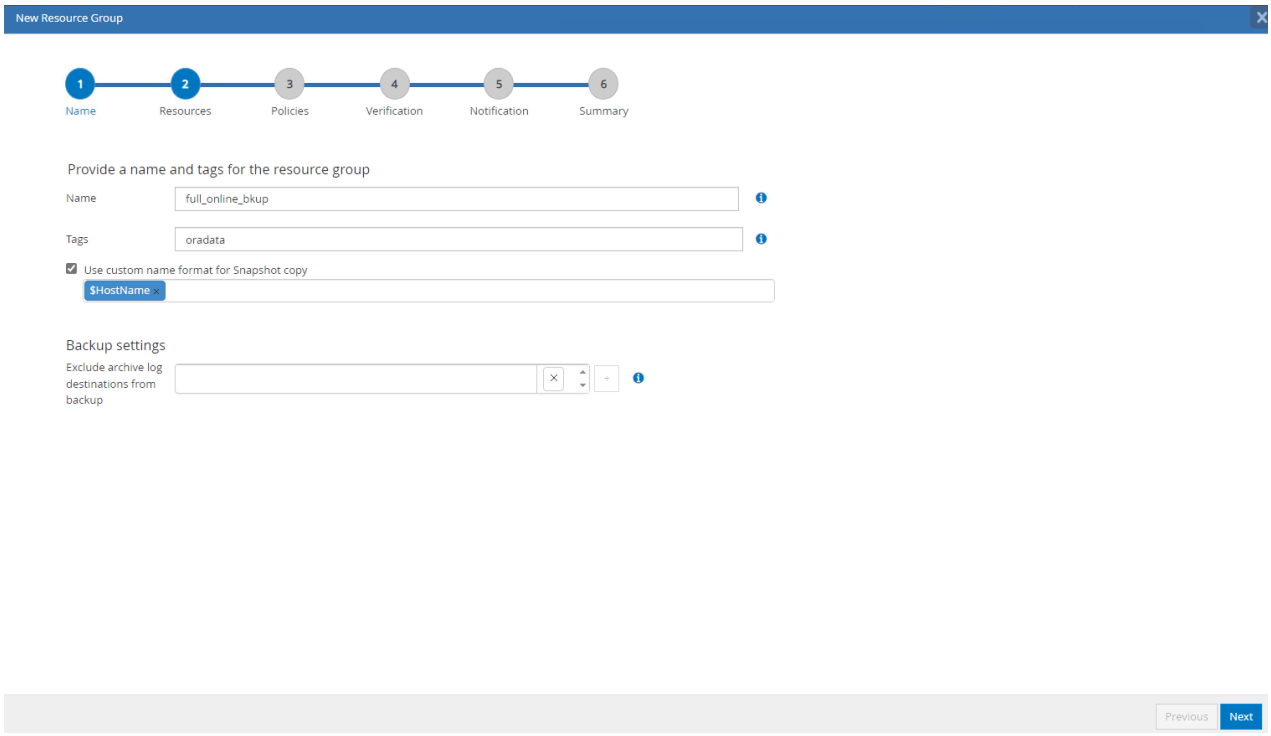
1. Accès à `Resources` Qui répertorie les bases de données découvertes une fois le plug-in SnapCenter installé sur la machine virtuelle de base de données. Au départ, le `Overall Status` de la base de données s'affiche sous la forme `Not protected`.



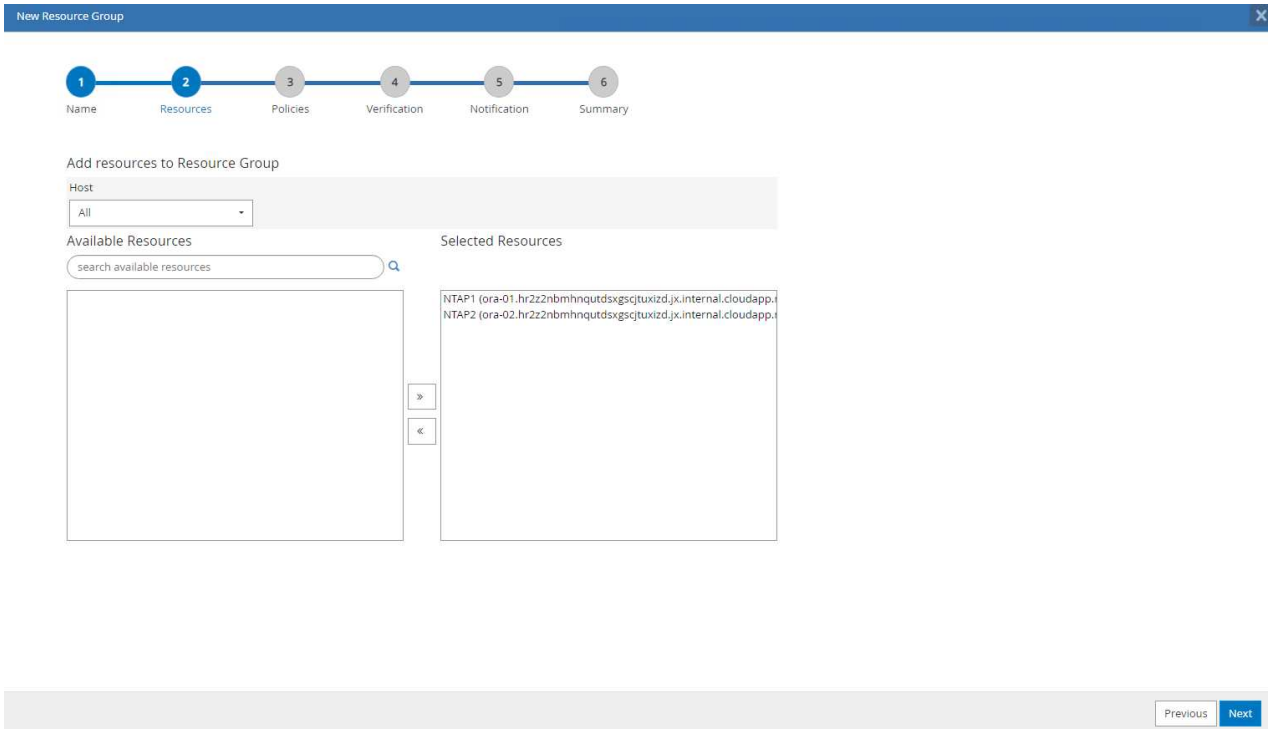
2. Cliquez sur `View` pour passer à `Resource Group`. Cliquez sur `Add` Connectez-vous à droite pour ajouter un groupe de ressources.



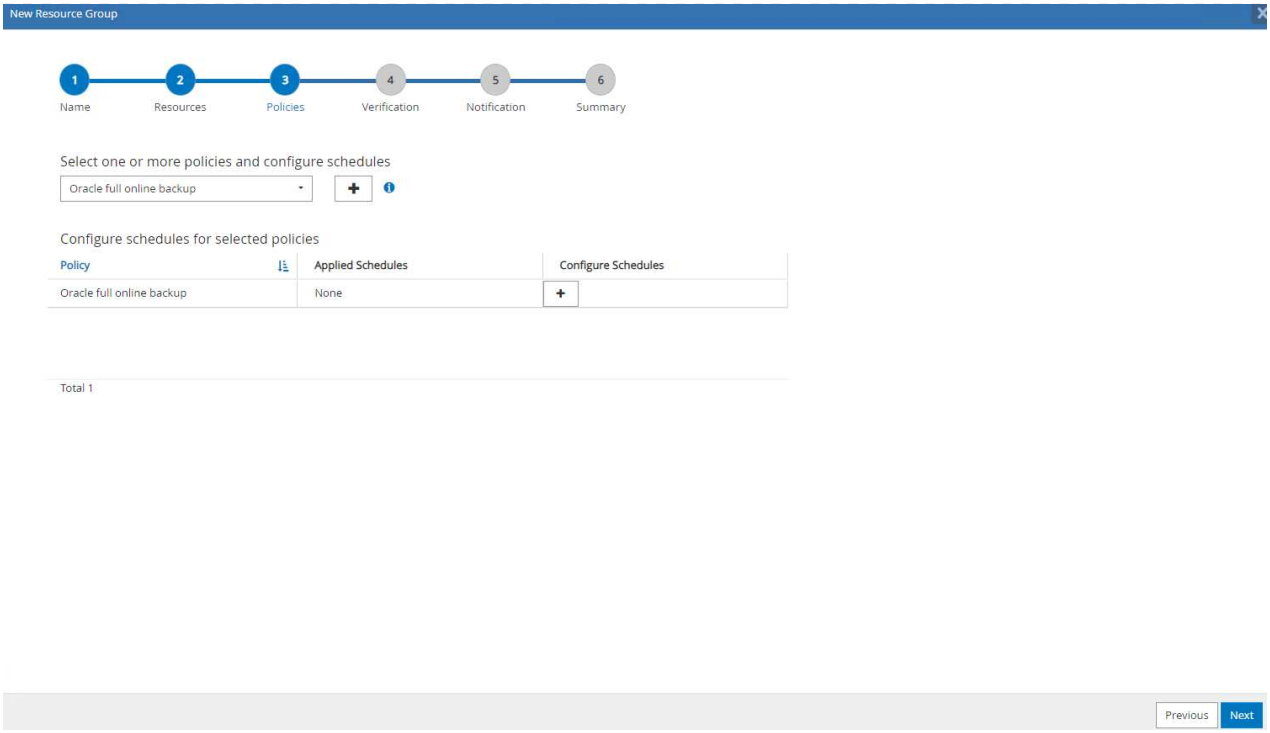
3. Nommez votre groupe de ressources, vos balises et toute dénomination personnalisée.

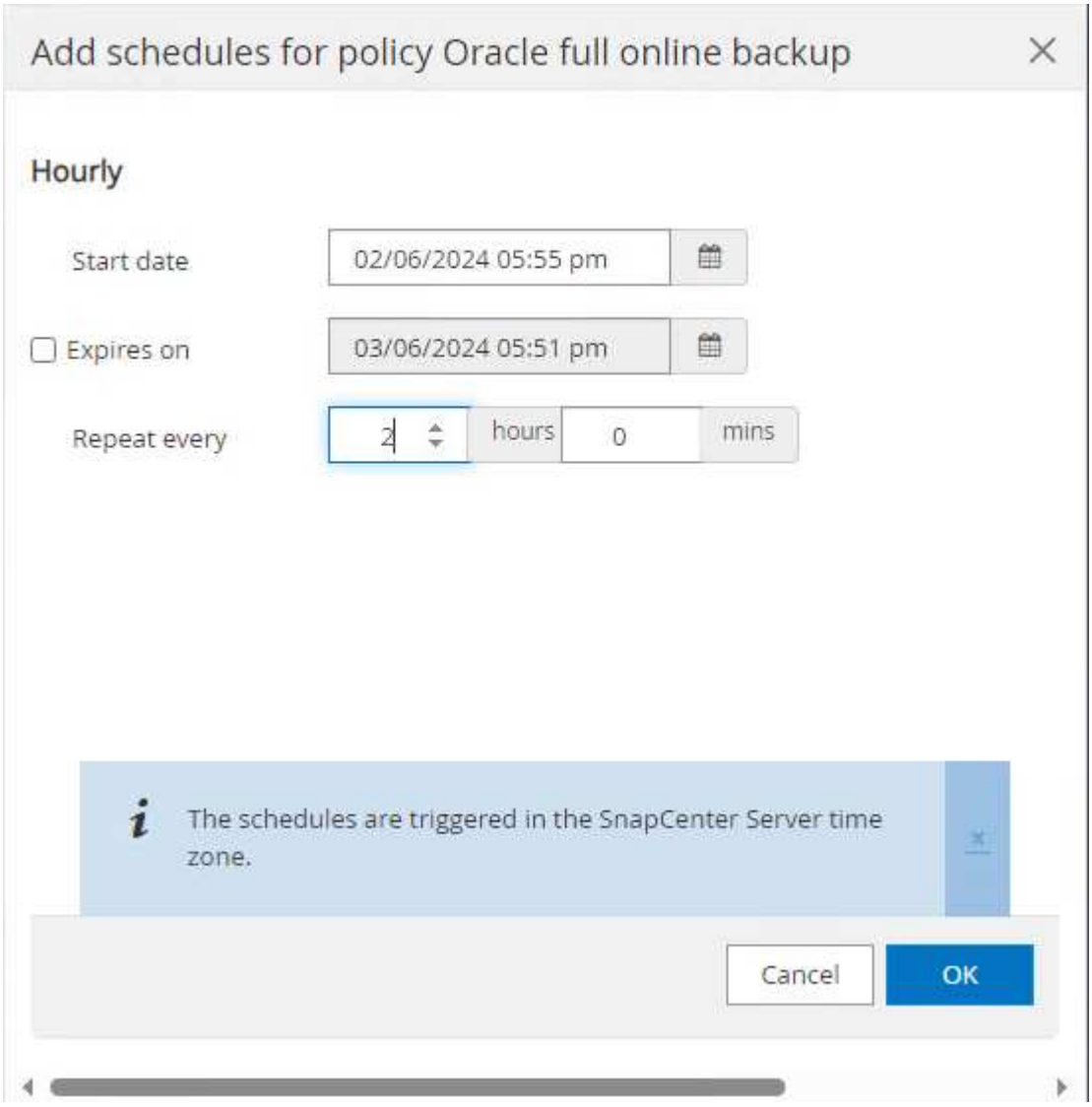


4. Ajoutez des ressources à votre `Resource Group`. Le regroupement de ressources similaires peut simplifier la gestion de la base de données dans un grand environnement.

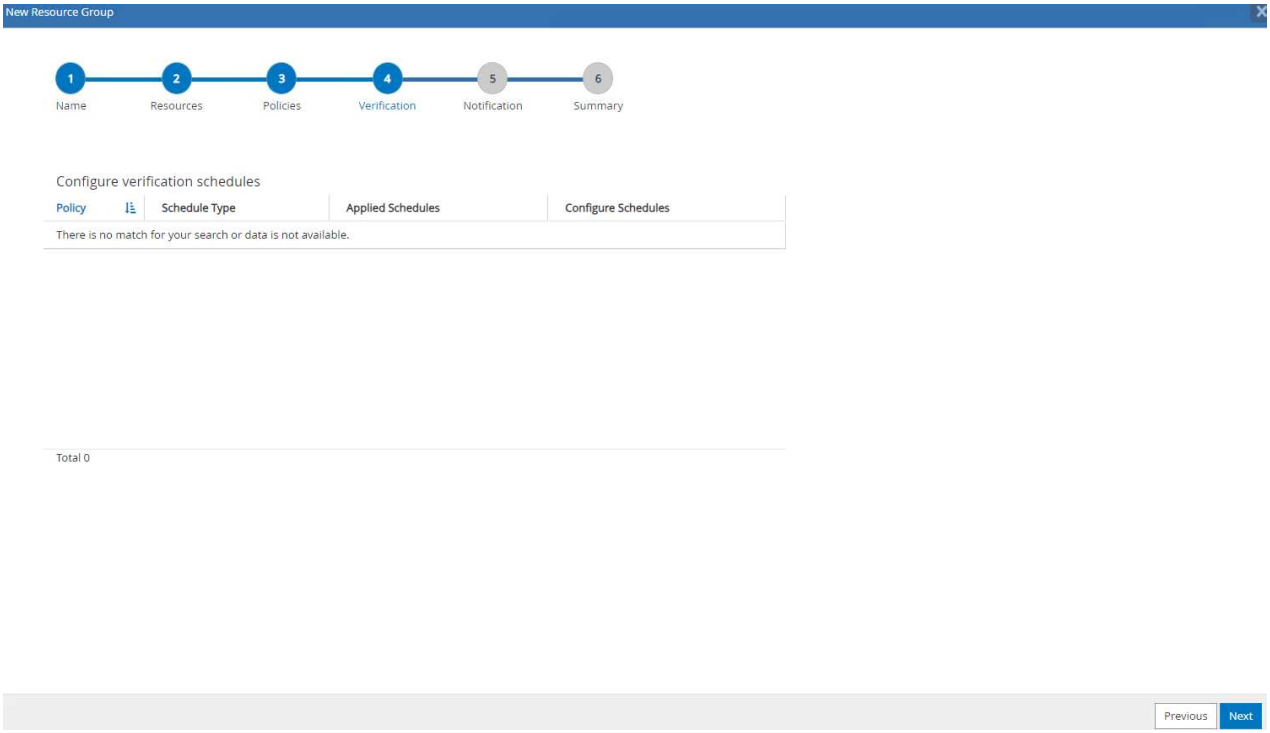


5. Sélectionnez la stratégie de sauvegarde et définissez un planning en cliquant sur le signe « + » sous `Configure Schedules`.

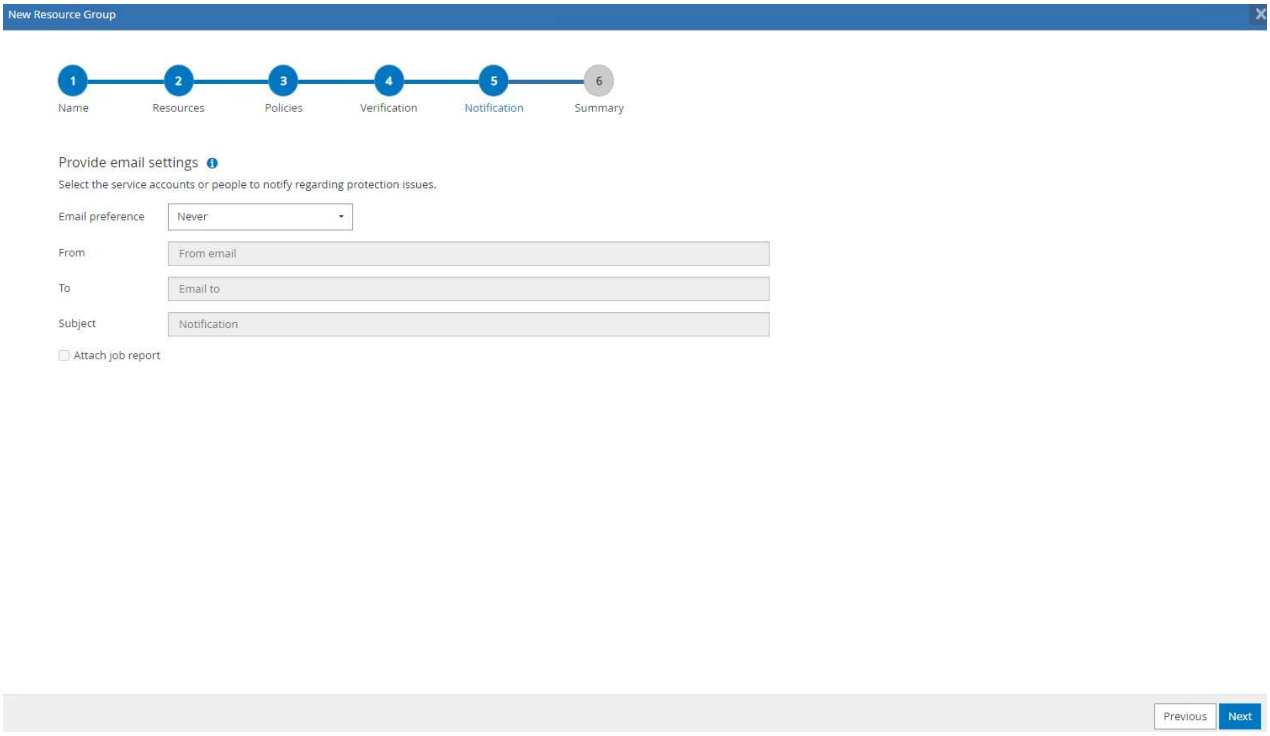

New Resource Group
1 Name
2 Resources
3 Policies
4 Verification
5 Notification
6 Summary
Select one or more policies and configure schedules
Oracle full online backup
Configure schedules for selected policies
Policy
Applied Schedules
Configure Schedules
Oracle full online backup
None
Total 1
Previous
Next


Add schedules for policy Oracle full online backup
Hourly
Start date
02/06/2024 05:55 pm
Expires on
03/06/2024 05:51 pm
Repeat every
2
hours
0
mins
The schedules are triggered in the SnapCenter Server time zone.
Cancel
OK

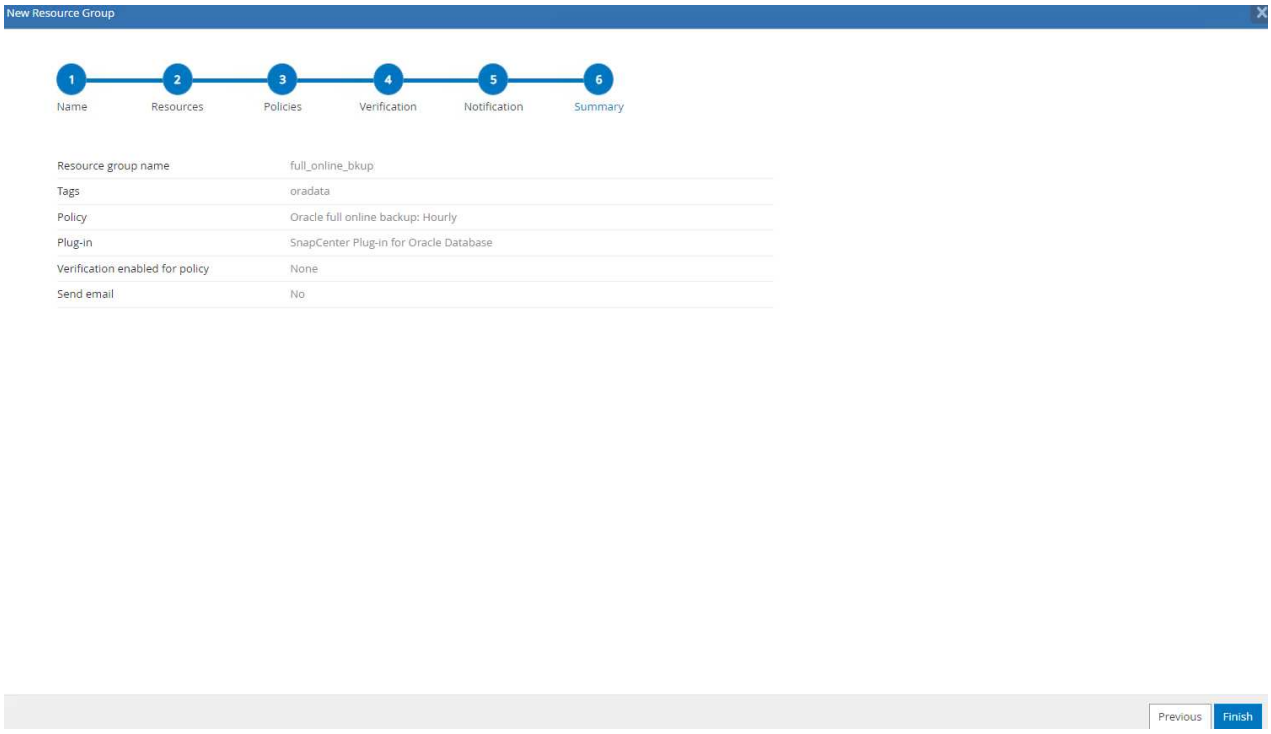
6. Si la vérification de sauvegarde n’est pas configurée dans la stratégie, laissez la page de vérification telle quel.



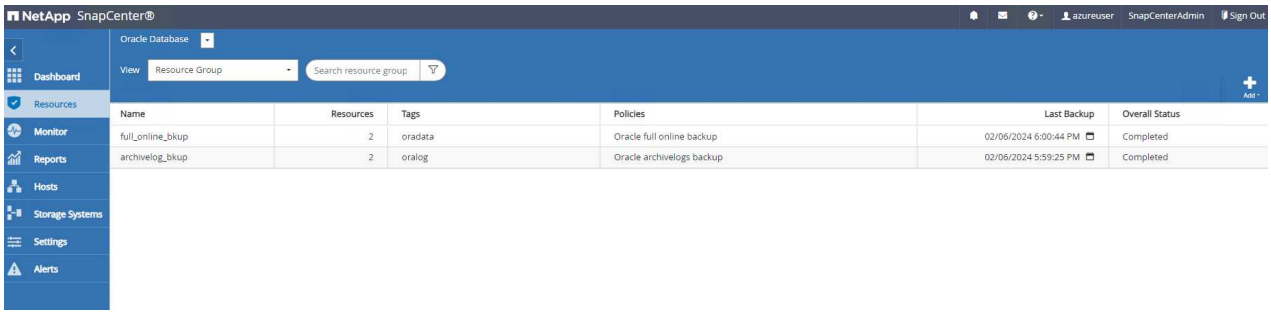
7. Pour envoyer un rapport de sauvegarde et une notification par e-mail, un serveur de messagerie SMTP est nécessaire dans l’environnement. Ou laissez-le noir si un serveur de messagerie n’est pas configuré.



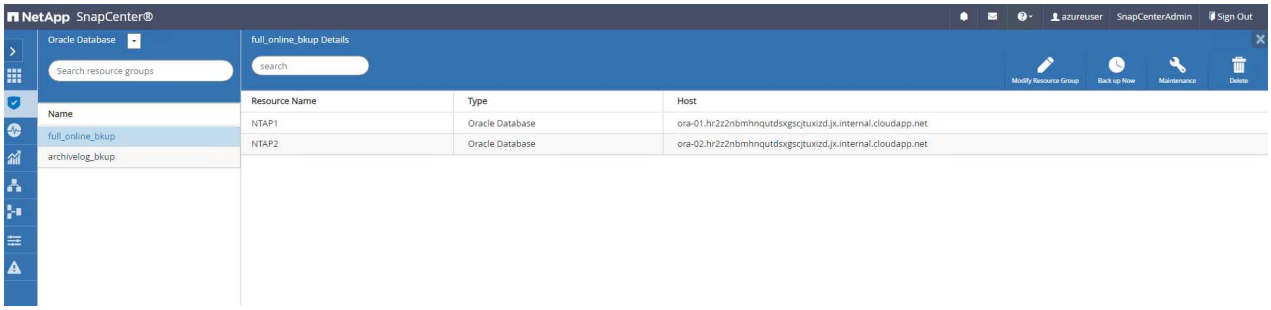
8. Résumé du nouveau groupe de ressources.

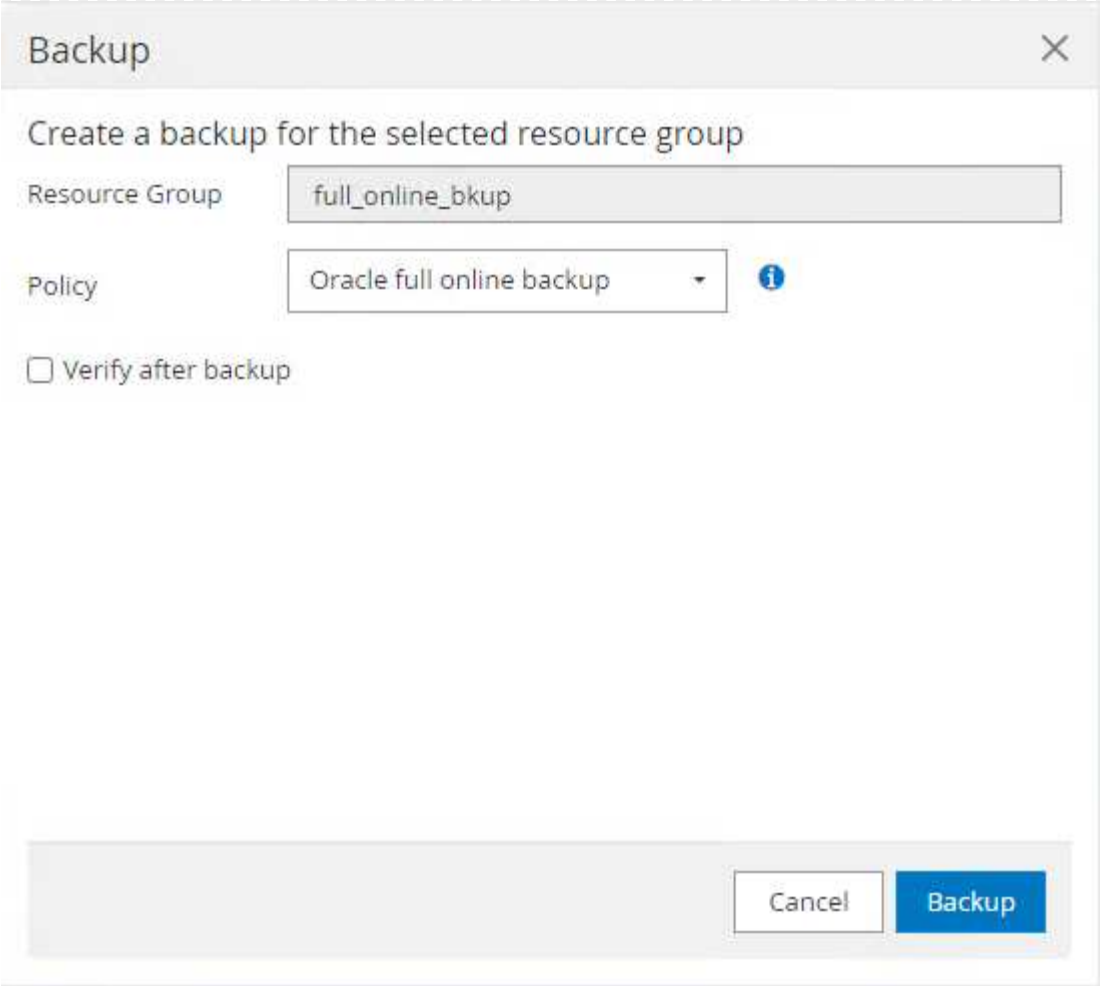


9. Répétez les procédures ci-dessus pour créer une sauvegarde du journal d'archive de base de données uniquement avec la stratégie de sauvegarde correspondante.

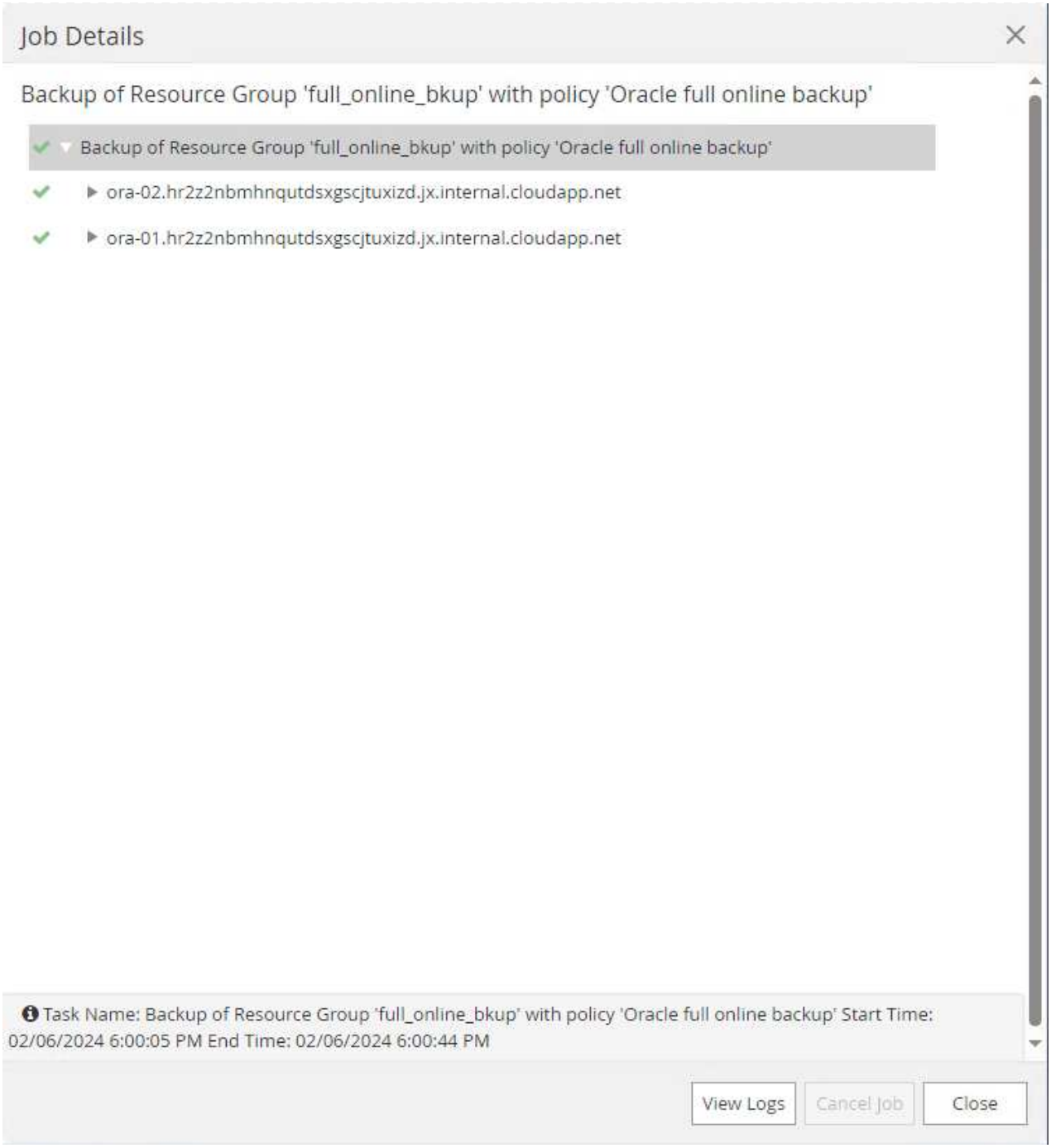


10. Cliquez sur un groupe de ressources pour afficher les ressources qu'il contient. Outre la procédure de sauvegarde planifiée, une sauvegarde unique peut être déclenchée en cliquant sur `Backup Now`.

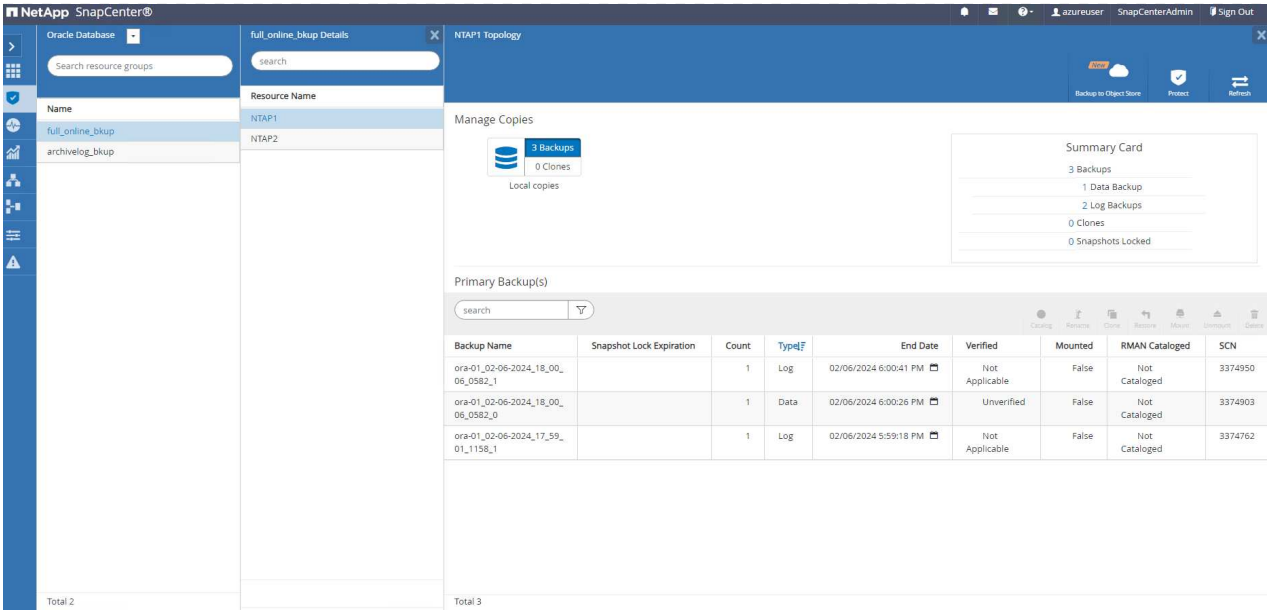




11. Cliquez sur le travail en cours pour ouvrir une fenêtre de surveillance, qui permet à l'opérateur de suivre la progression du travail en temps réel.



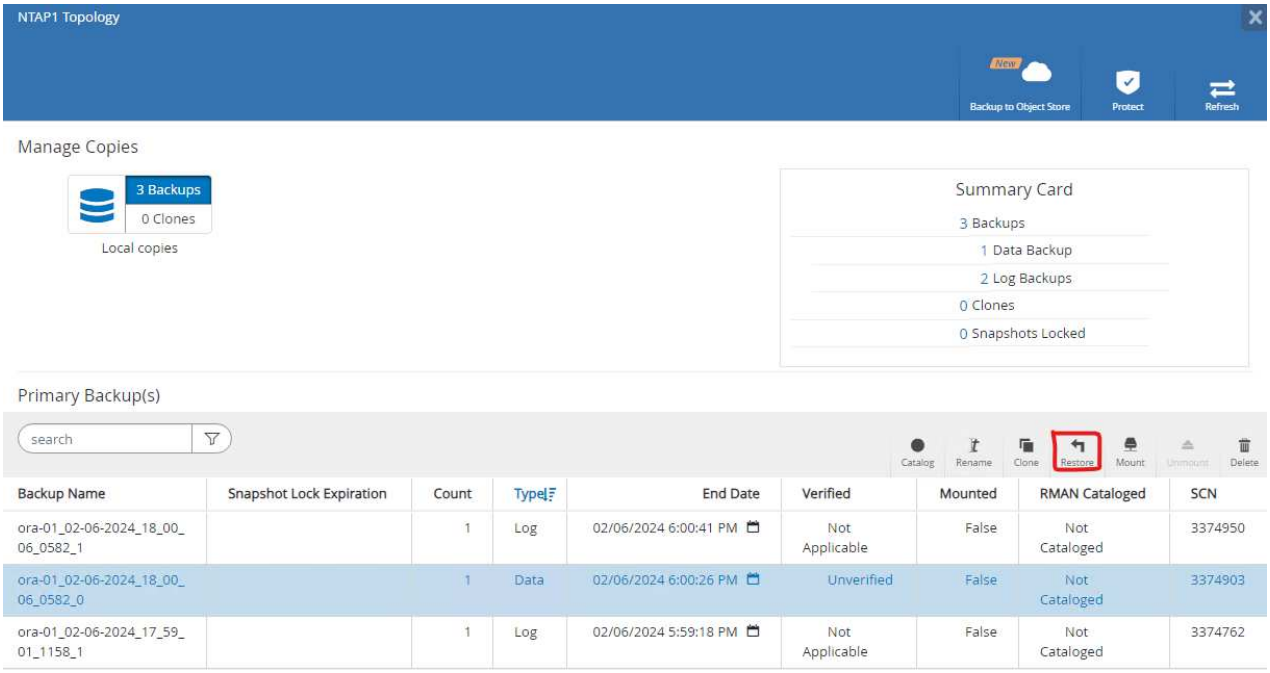
12. Un jeu de sauvegardes d'instantanés apparaît sous la topologie de la base de données une fois la procédure de sauvegarde terminée. Un jeu complet de sauvegardes de base de données inclut un instantané des volumes de données de base de données et un instantané des volumes de journaux de base de données. Une sauvegarde de journal uniquement contient uniquement un snapshot des volumes de journal de base de données.



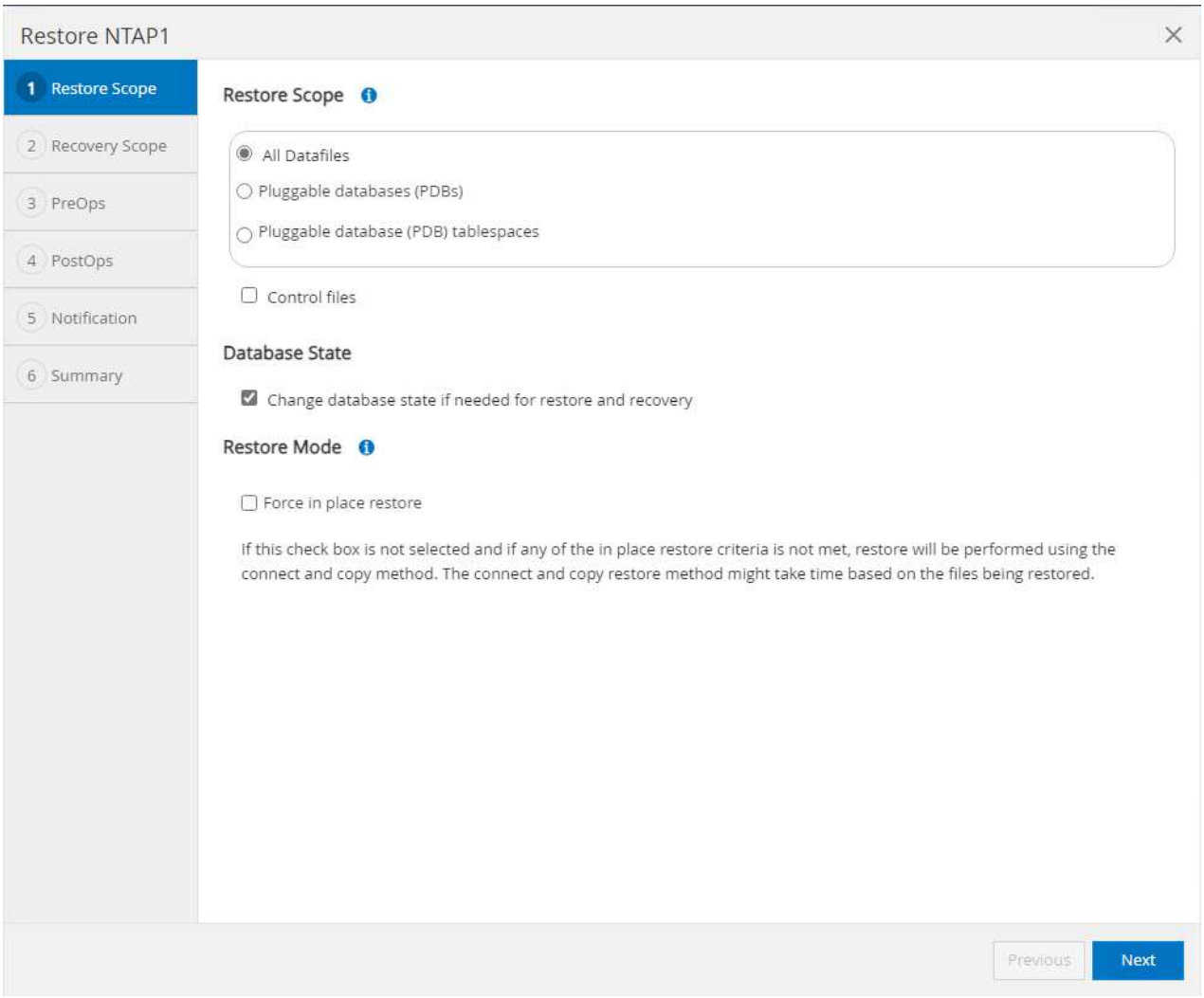
Restauration de la base de données

La restauration de la base de données via SnapCenter restaure une copie Snapshot de l'image du volume de la base de données à un point dans le temps. La base de données est ensuite reprise vers l'avant jusqu'au point souhaité par SCN/TIMESTAMP ou par un point autorisé par les journaux d'archive disponibles dans le jeu de sauvegarde. La section suivante décrit le workflow de restauration de base de données avec l'interface utilisateur de SnapCenter.

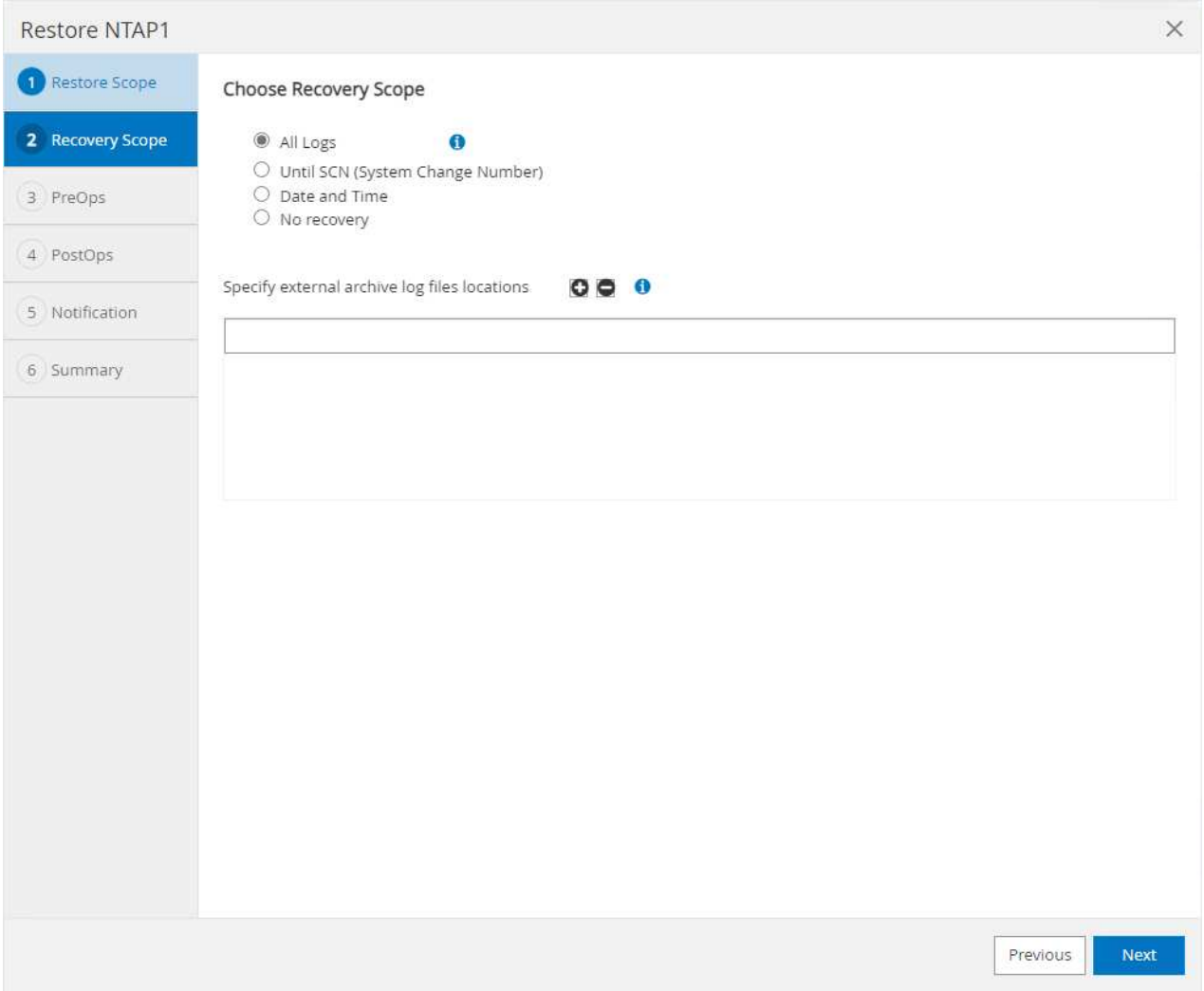
1. De `Resources` ouvrez la base de données `Primary Backup(s)` page. Choisissez l'instantané du volume de données de la base de données, puis cliquez sur `Restore` pour lancer le workflow de récupération de la base de données. Notez le numéro SCN ou l'horodatage dans les jeux de sauvegarde si vous souhaitez exécuter la restauration par le SCN Oracle ou l'horodatage.



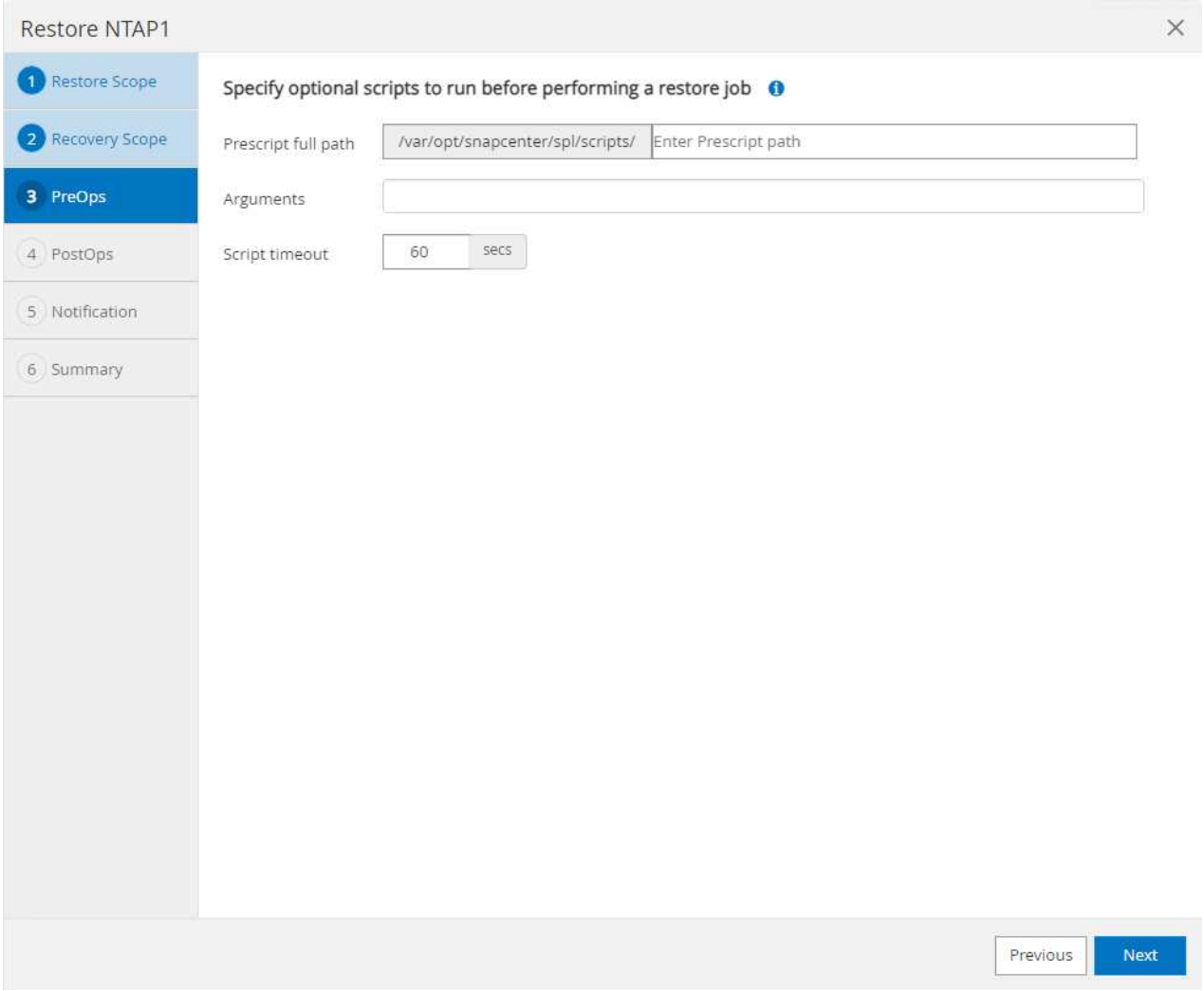
2. Sélectionnez `Restore Scope`. Pour une base de données de conteneurs, SnapCenter est flexible pour effectuer une restauration au niveau des bases de données de conteneurs complètes (tous les fichiers de données), des bases de données enfichables ou des espaces de stockage.



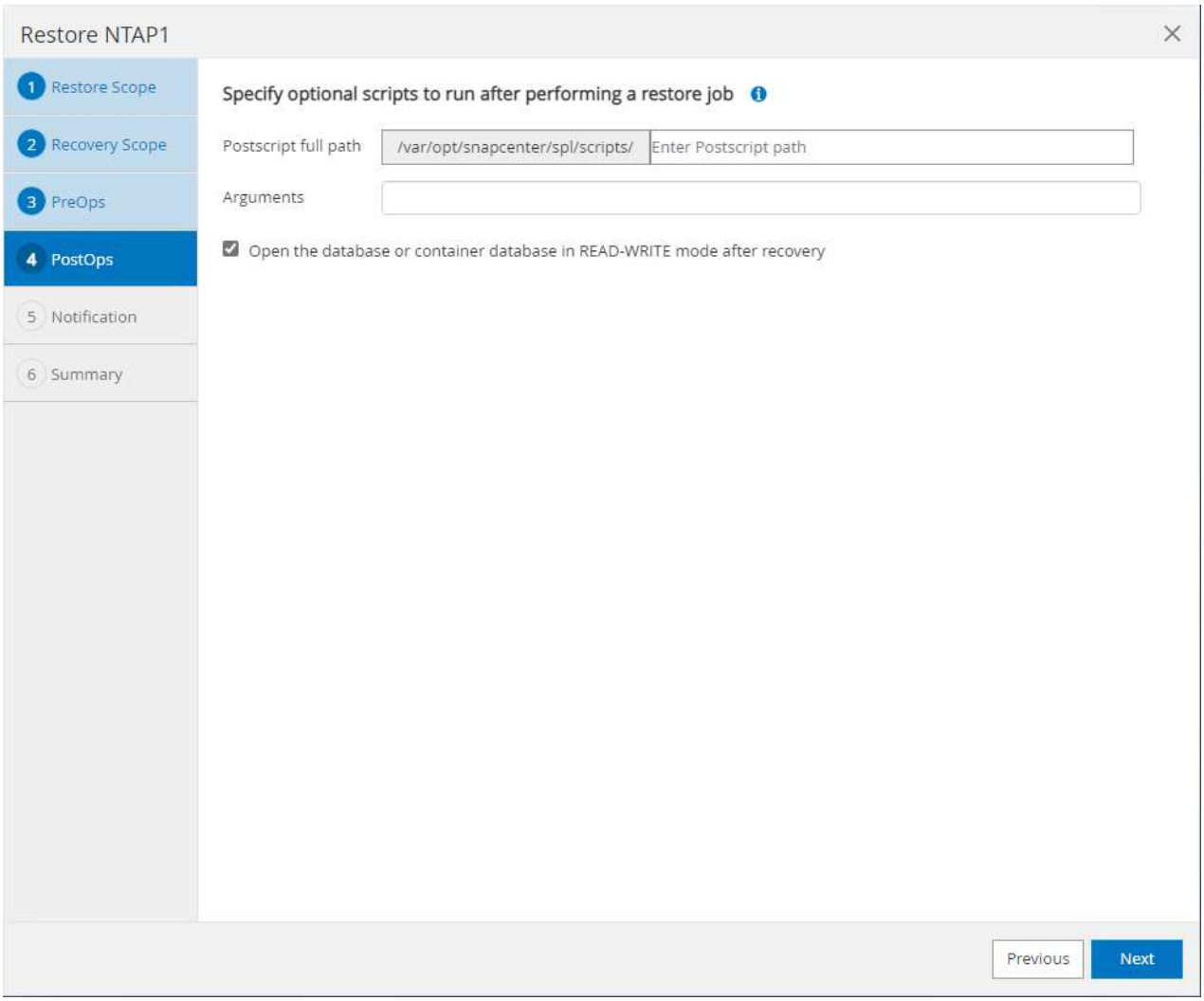
3. Sélectionnez `Recovery Scope`. `All logs` signifie appliquer tous les journaux d'archive disponibles dans le jeu de sauvegarde. La restauration instantanée par SCN ou par horodatage est également disponible.



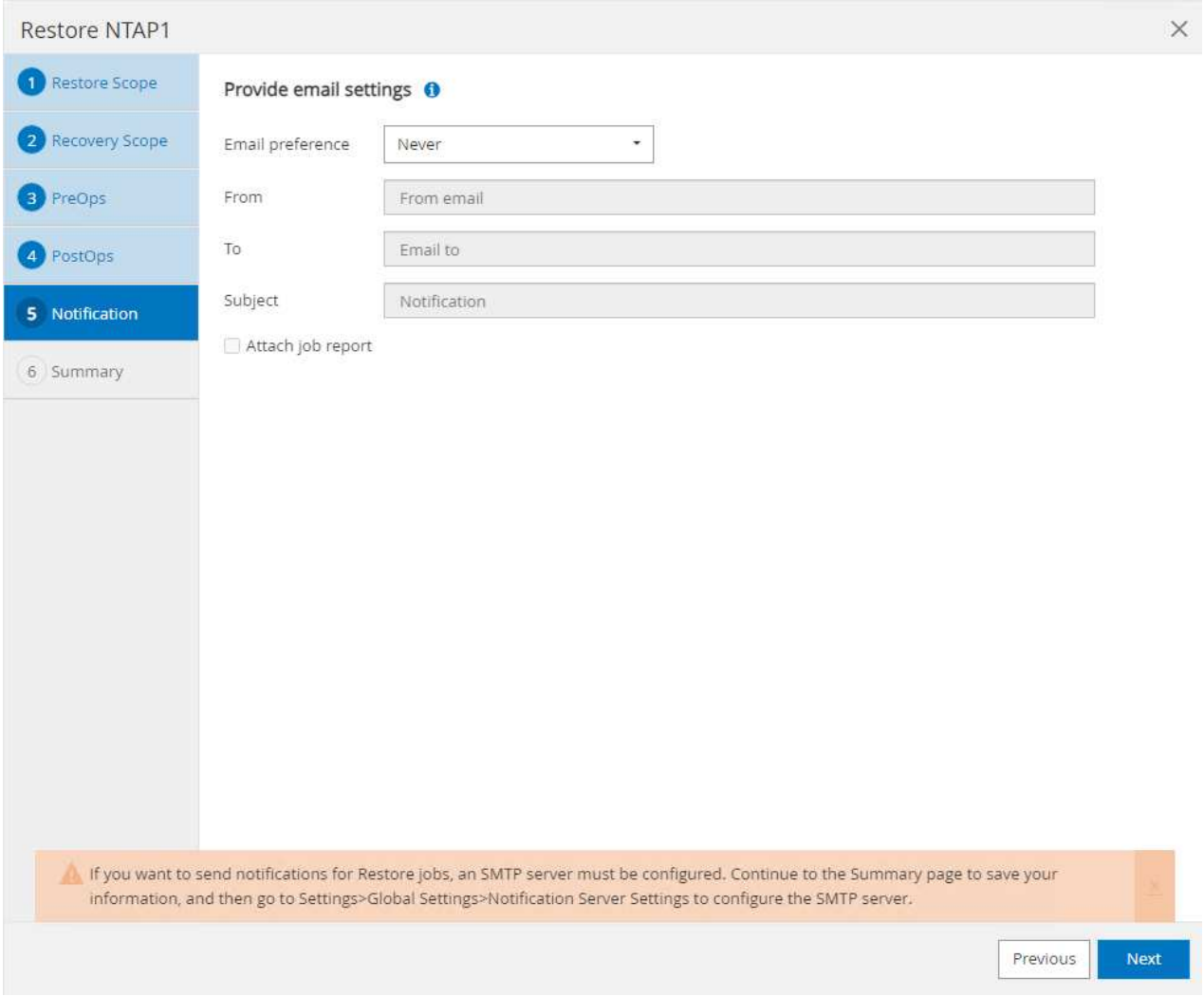
4. Le `PreOps` permet l'exécution de scripts sur la base de données avant l'opération de restauration/récupération.



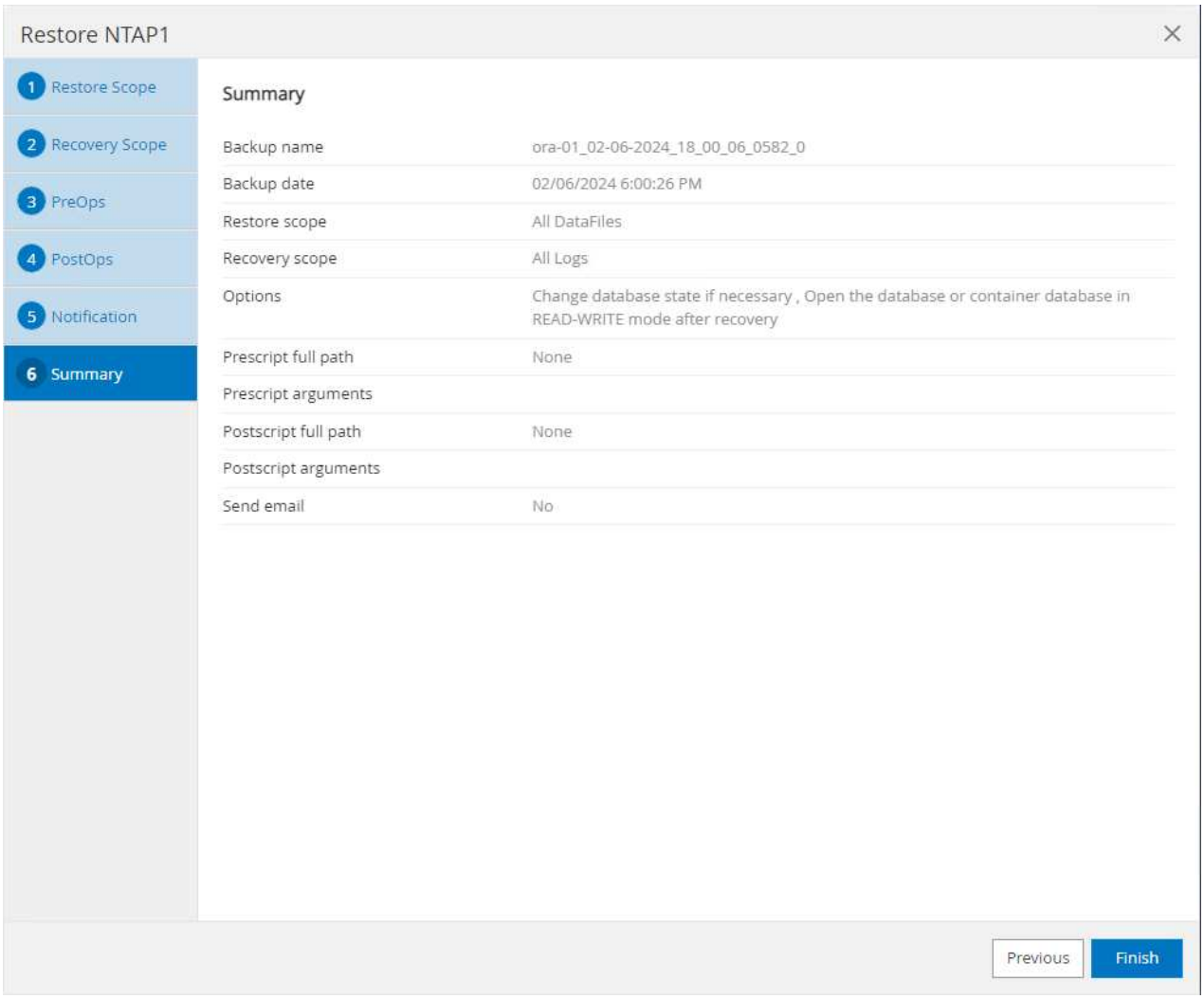
5. Le `PostOps` permet l'exécution de scripts sur la base de données après une opération de restauration/récupération.



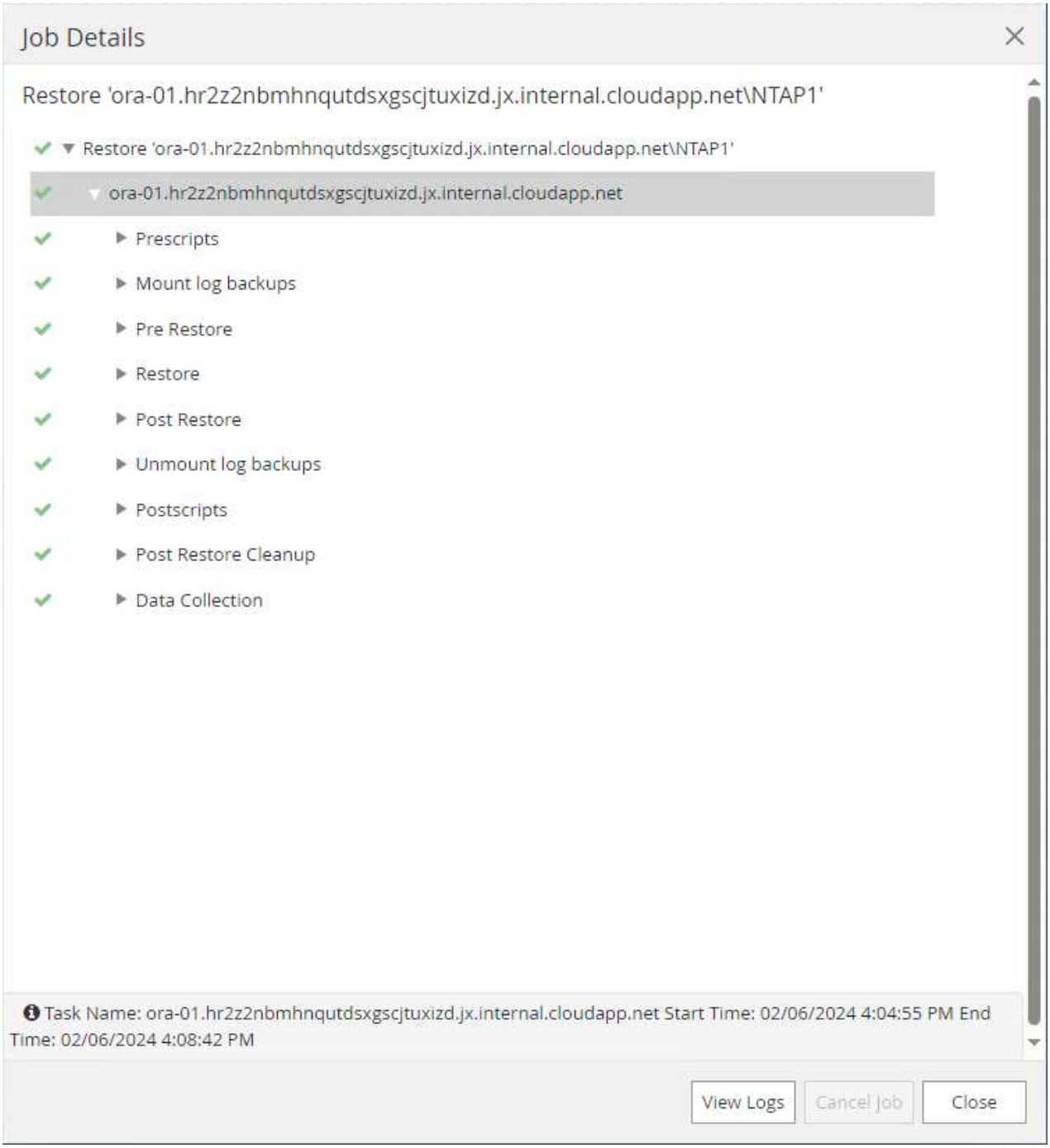
6. Notification par e-mail si vous le souhaitez.



7. Résumé de la tâche de restauration



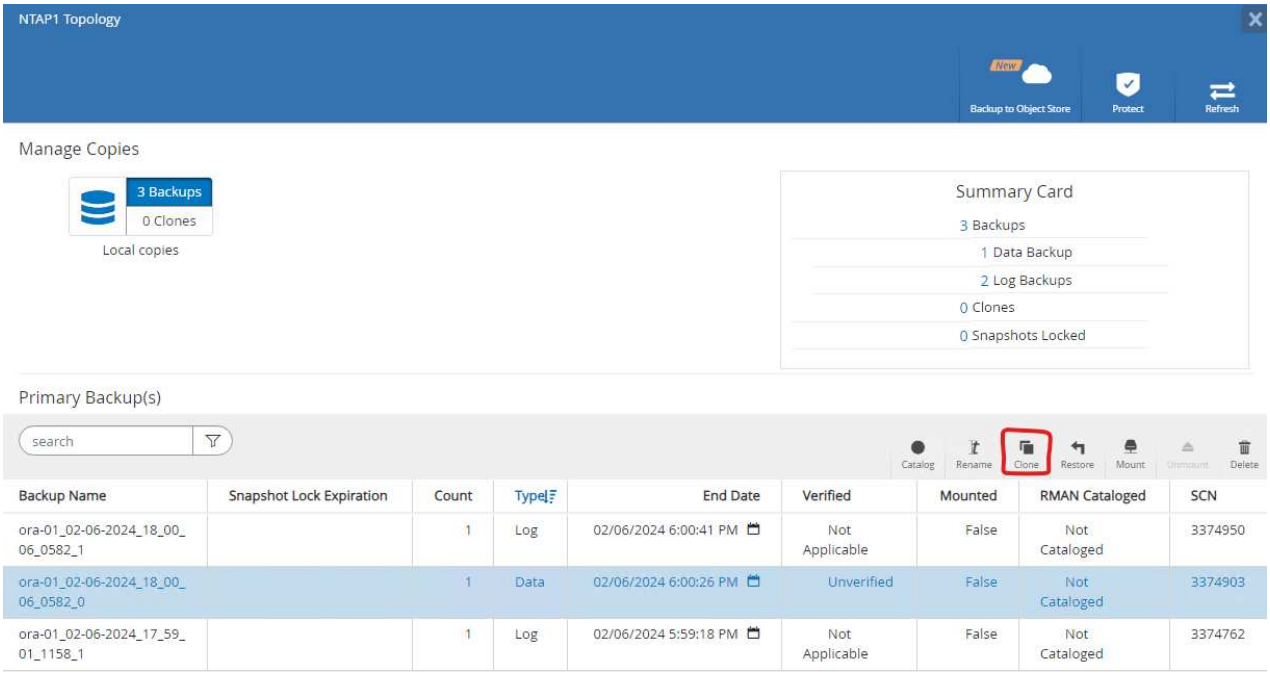
8. Cliquez sur exécution du travail pour l'ouvrir `Job Details` fenêtre. L'état du travail peut également être ouvert et affiché à partir du `Monitor` onglet.



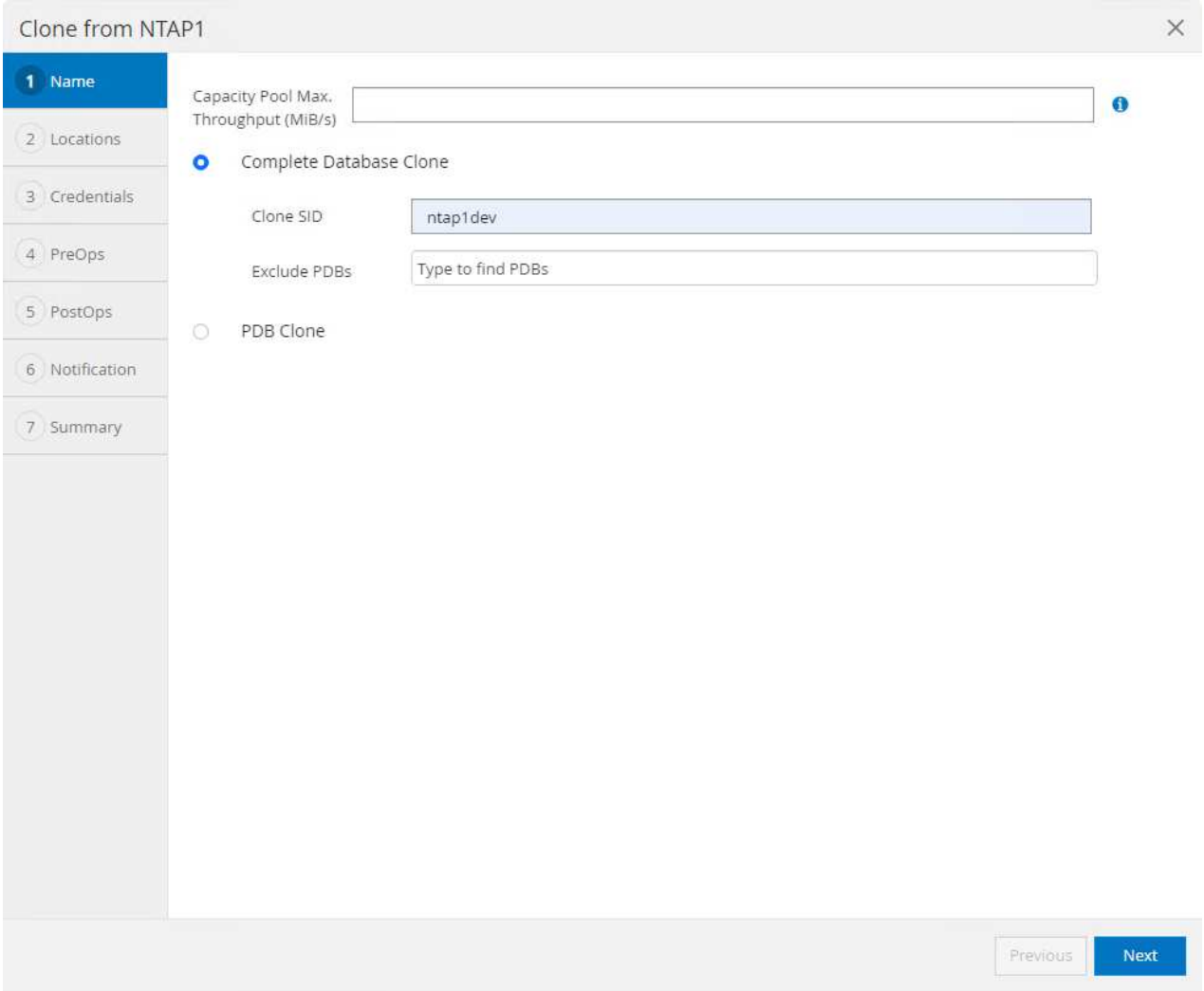
Clone de base de données

La création d'un nouveau volume à partir de la copie Snapshot d'un volume permet de cloner la base de données via SnapCenter. Le système utilise les informations de snapshot pour cloner un nouveau volume à l'aide des données du volume au moment de la prise de l'instantané. Plus important encore, il est rapide (quelques minutes) et efficace par rapport à d'autres méthodes d'effectuer une copie clonée de la base de données de production pour prendre en charge le développement ou le test. Vous pouvez ainsi améliorer considérablement la gestion du cycle de vie des applications de votre base de données. La section suivante décrit le workflow du clone de base de données avec l'interface utilisateur SnapCenter.

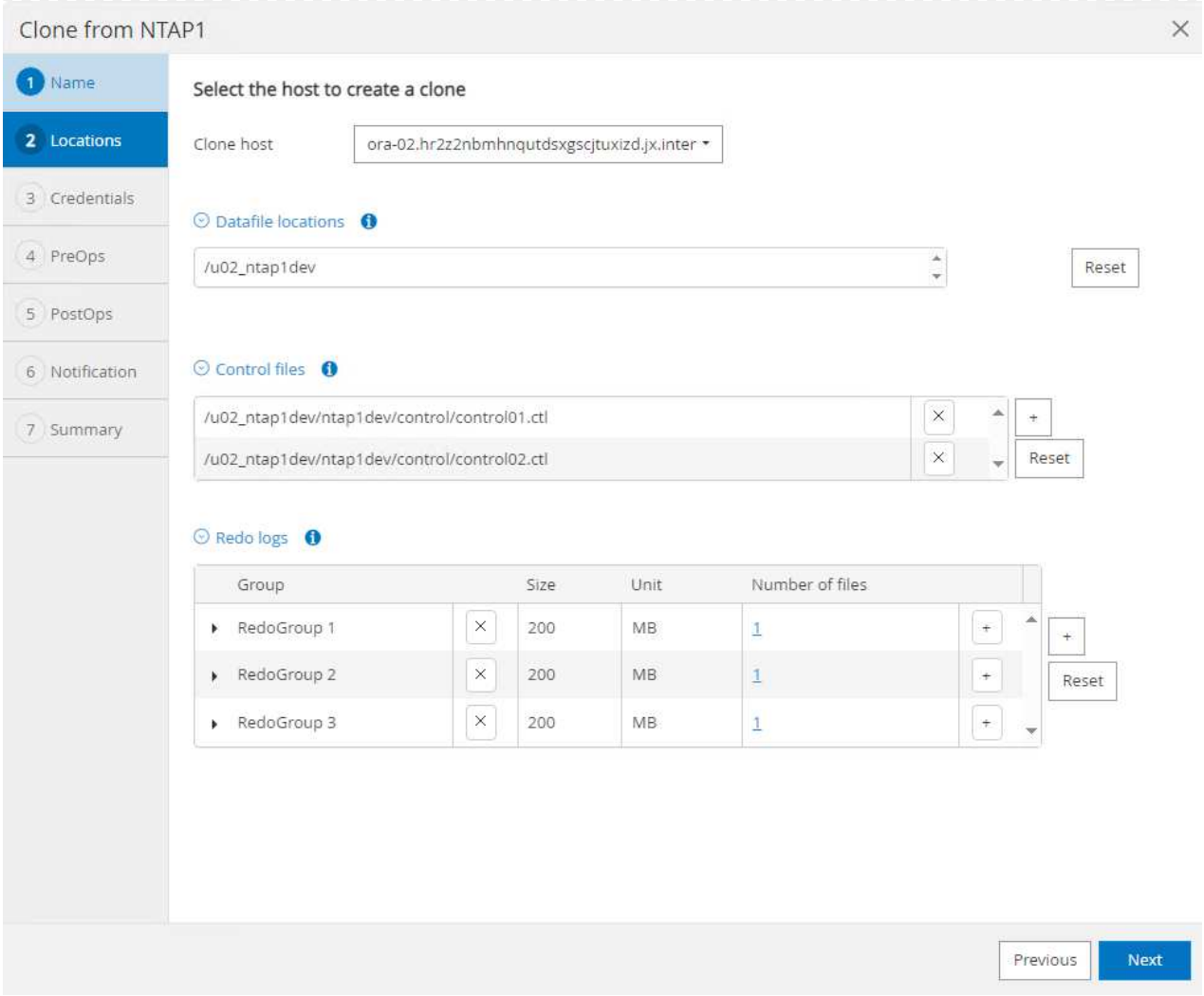
1. De `Resources` ouvrez la base de données `Primary Backup(s)` page. Choisissez l'instantané du volume de données de la base de données, puis cliquez sur `clone` pour lancer le flux de travail de clonage de base de données.



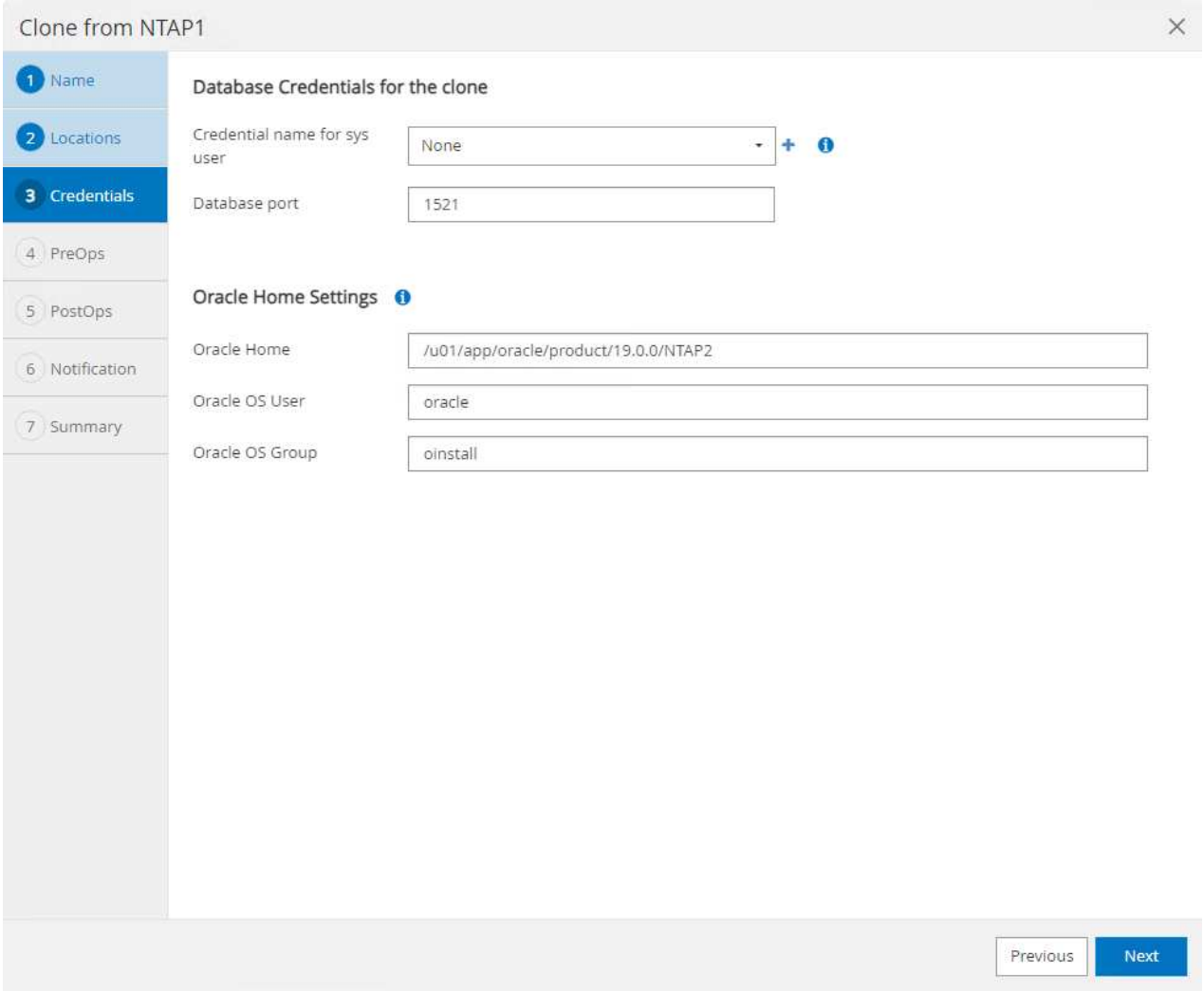
2. Nommer le SID de la base de données clone. En option, pour une base de données de conteneurs, le clonage peut également être effectué au niveau PDB.



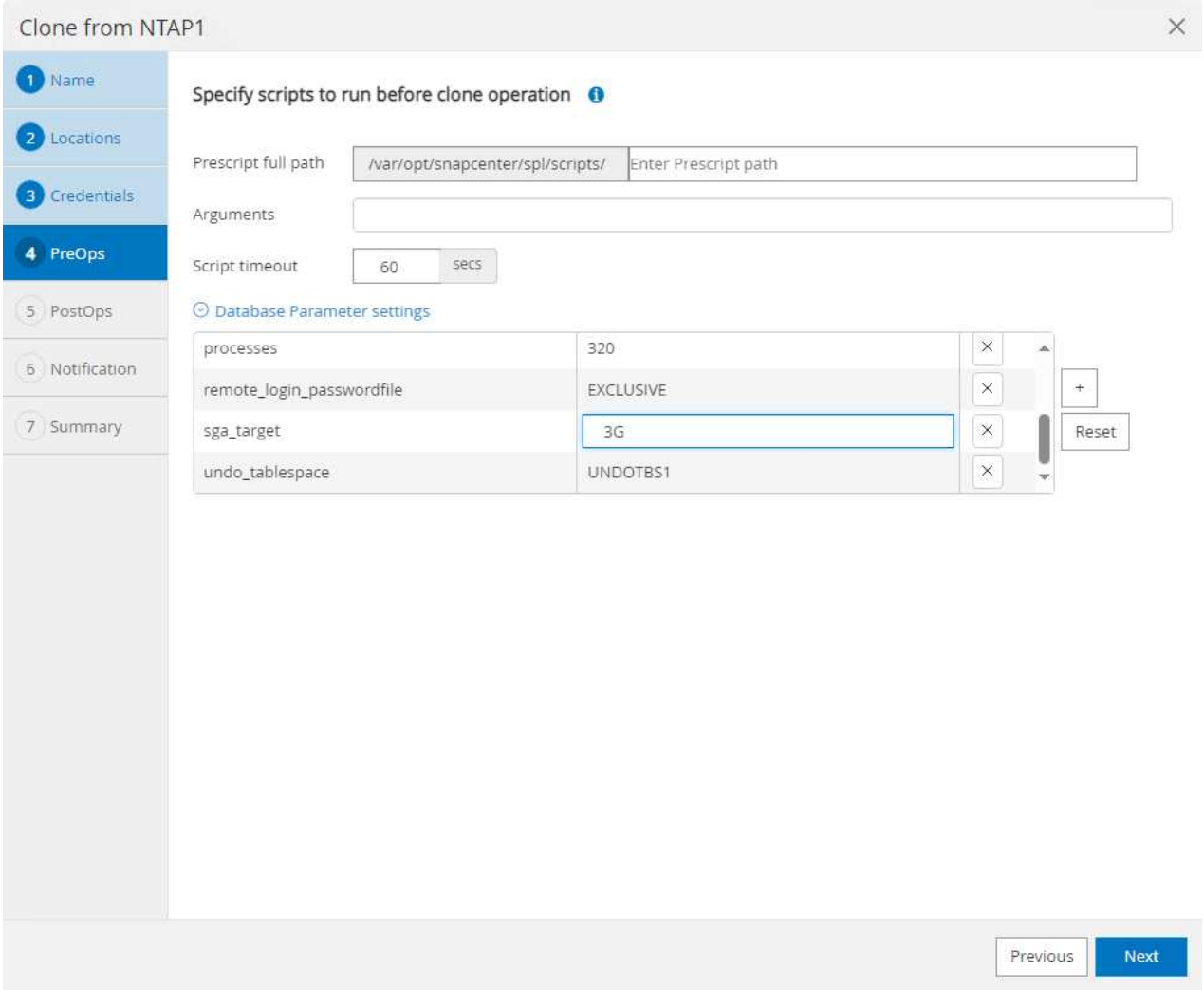
3. Sélectionnez le serveur de base de données sur lequel vous souhaitez placer la copie de la base de données clonée. Conservez les emplacements de fichier par défaut, sauf si vous voulez les nommer différemment.



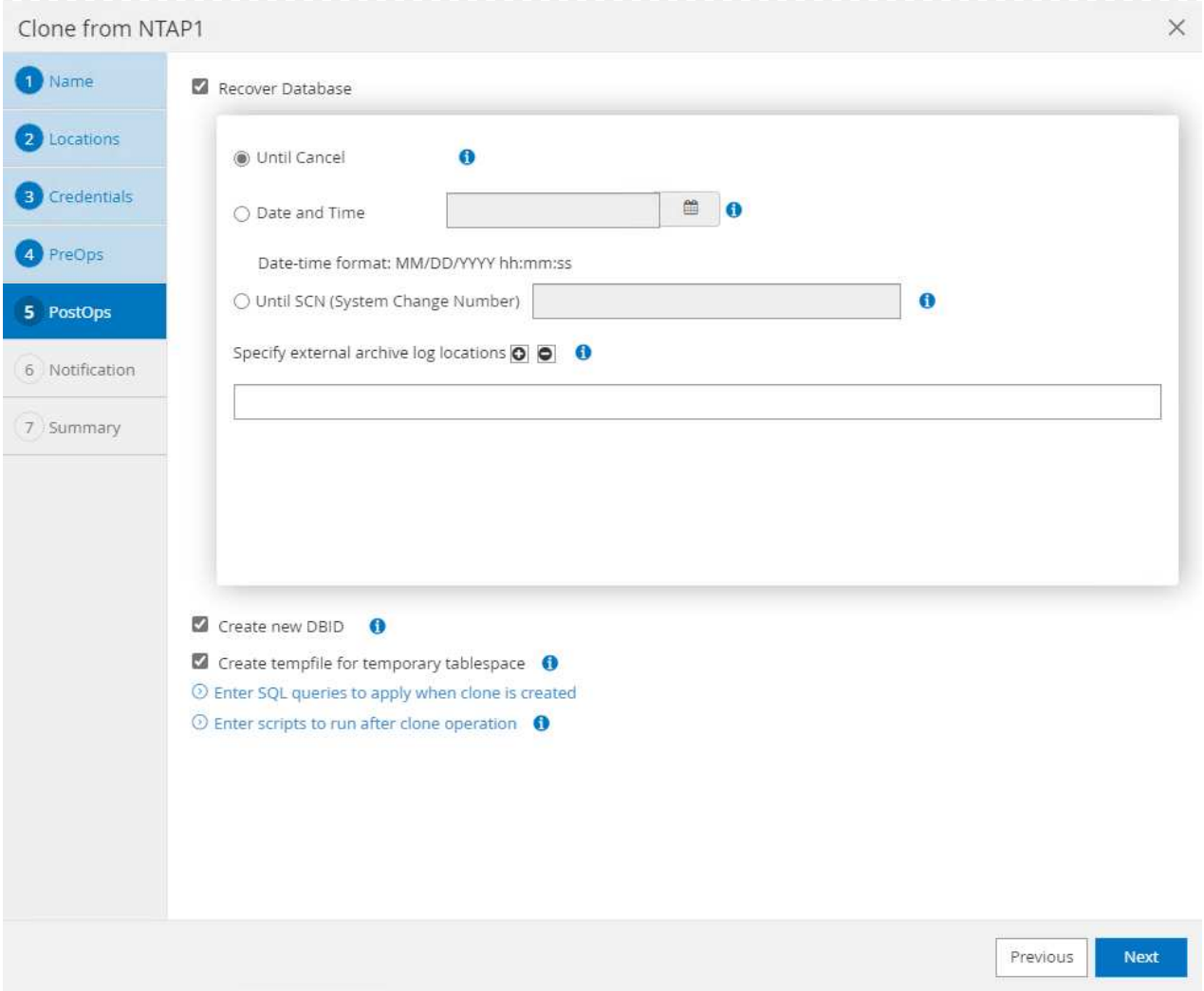
4. Une pile logicielle Oracle identique à celle de la base de données source doit avoir été installée et configurée sur l'hôte de base de données clone. Conservez les informations d'identification par défaut mais modifiez-les `Oracle Home Settings` Pour faire correspondre avec les paramètres sur l'hôte de base de données de clonage.



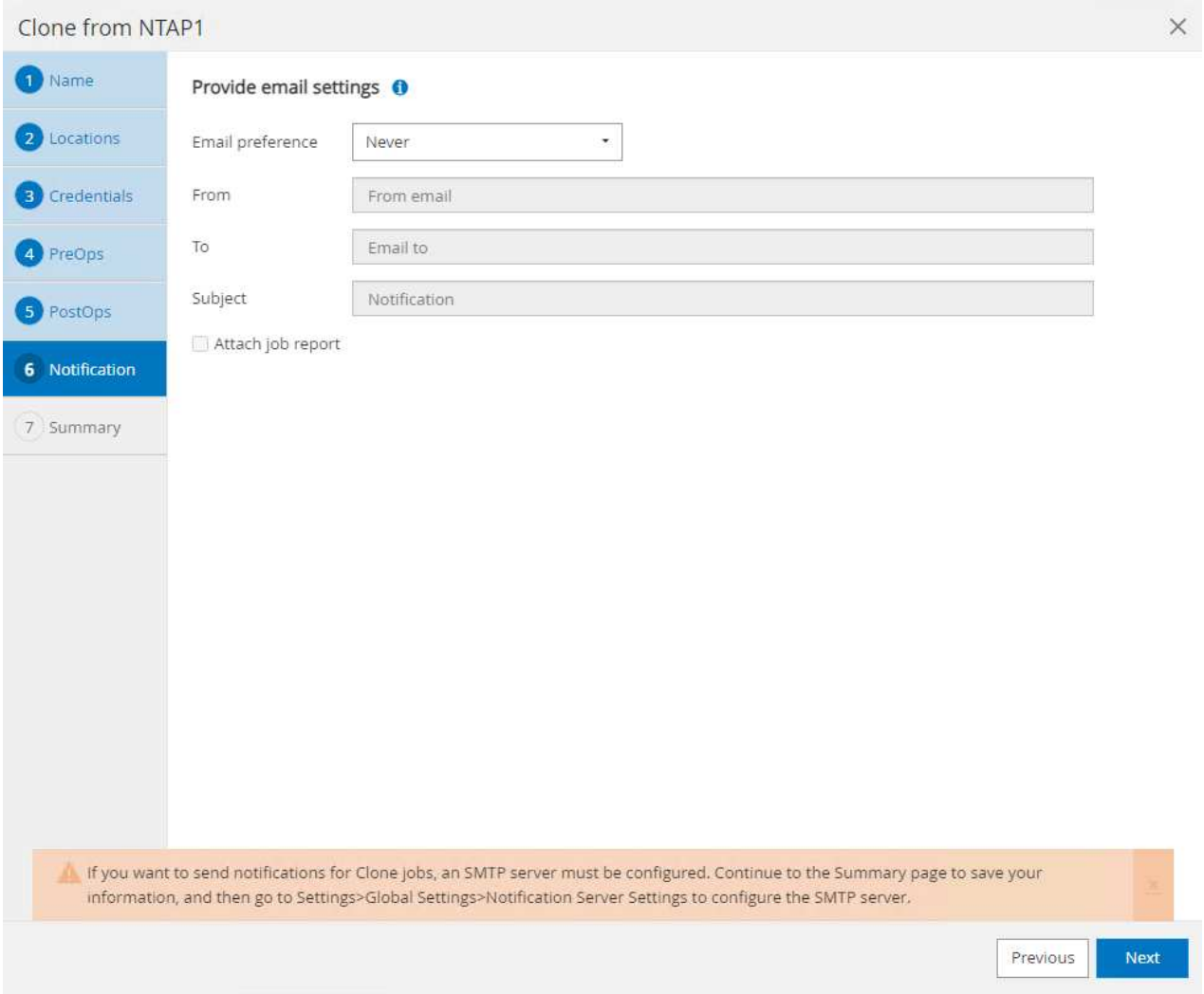
5. Le `PreOps` permet l'exécution de scripts avant l'opération de clonage. Les paramètres de base de données peuvent être ajustés pour répondre aux besoins de base de données de clonage par rapport à une base de données de production, comme une cible SGA réduite.



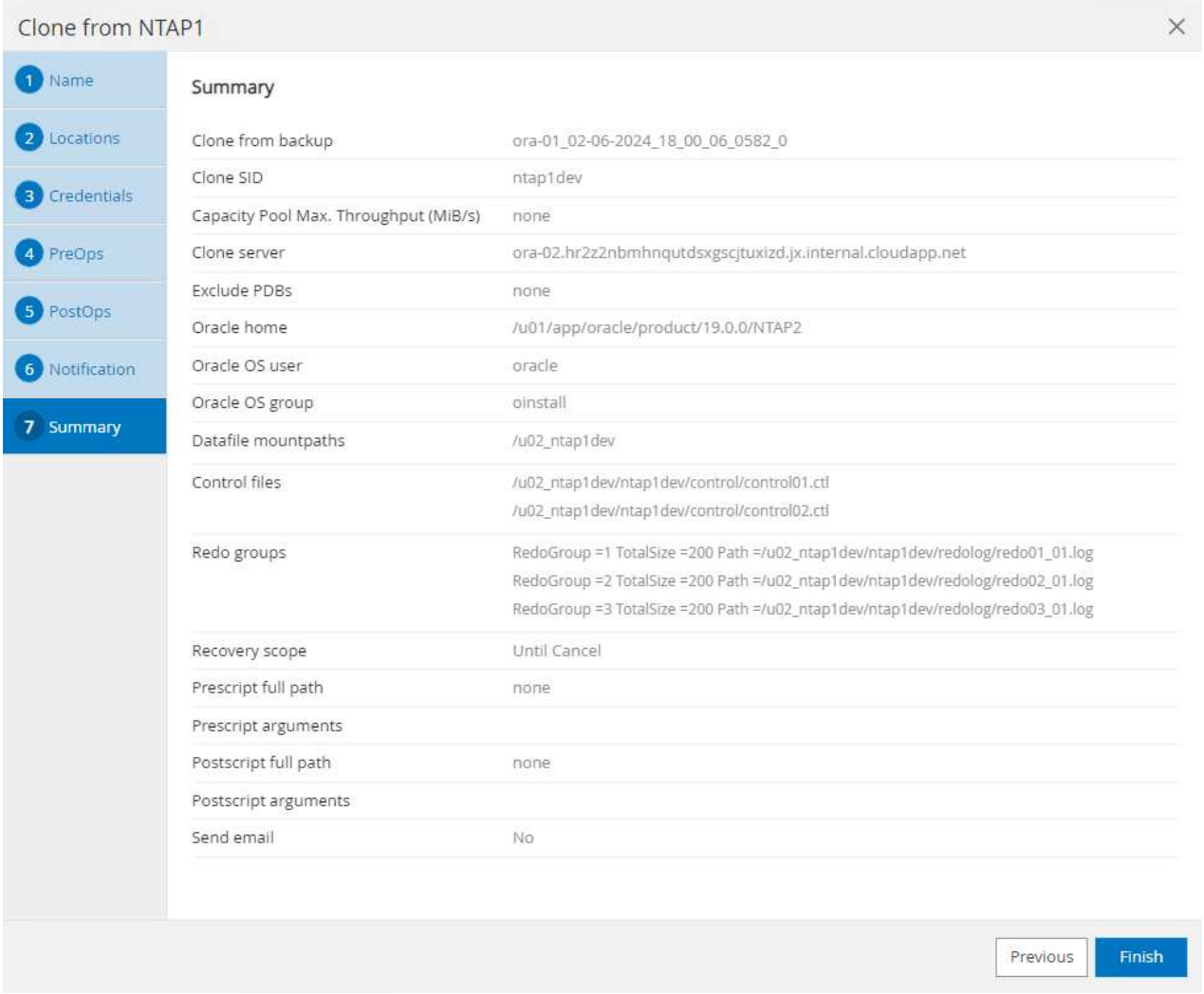
6. Le `PostOps` permet l'exécution de scripts sur la base de données après l'opération de clonage. La restauration de la base de données de clonage peut être basée sur SCN, l'horodatage ou jusqu'à l'annulation (reprise de la base de données vers le dernier journal archivé dans le jeu de sauvegarde).



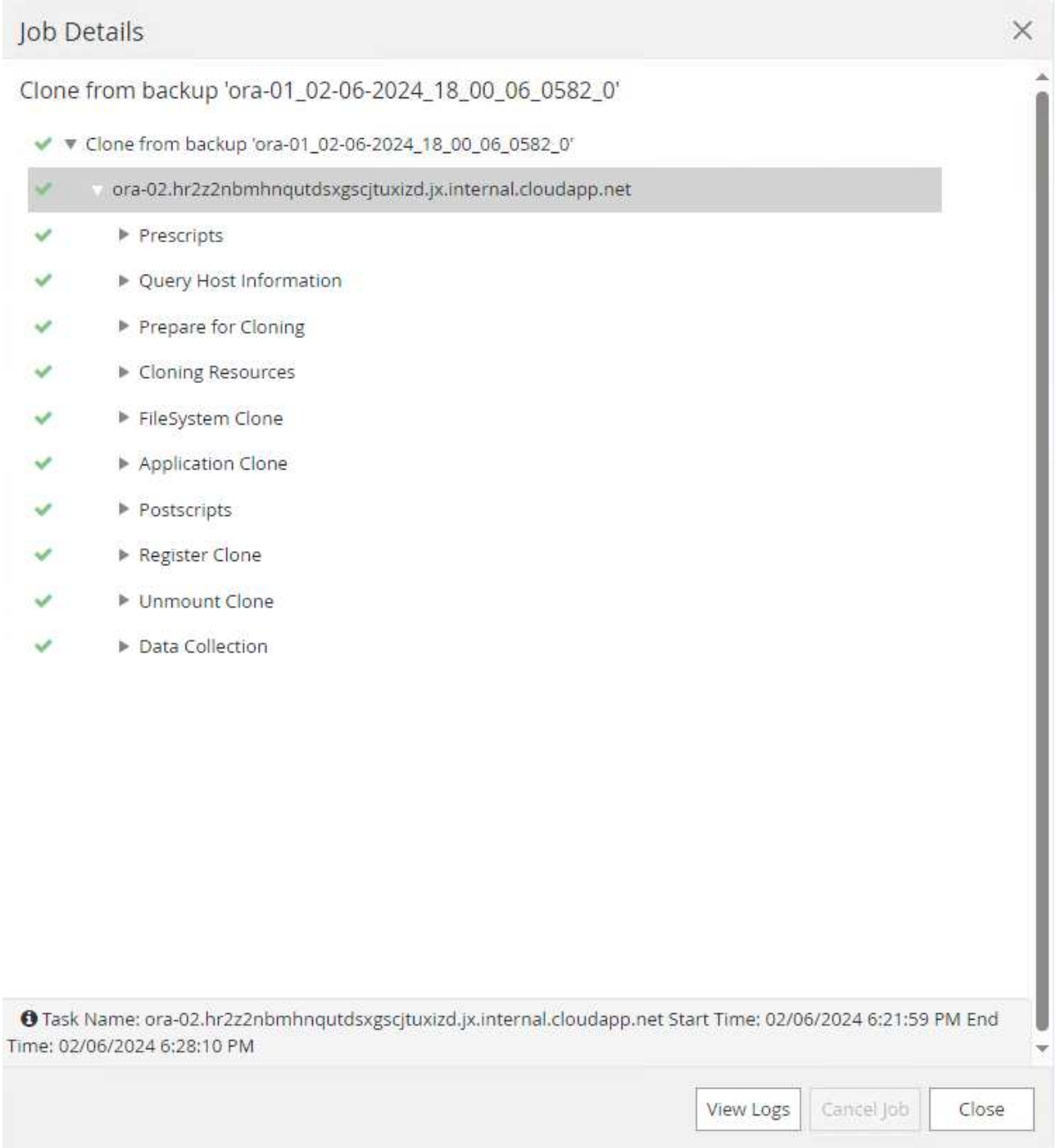
7. Notification par e-mail si vous le souhaitez.



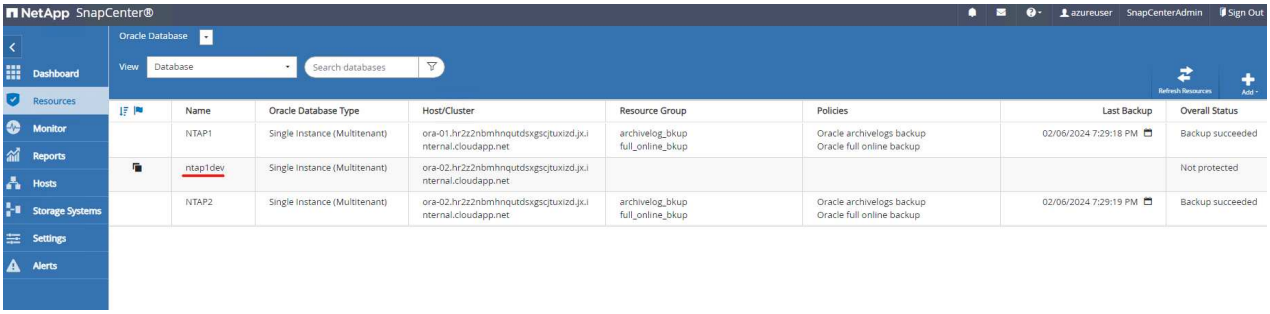
8. Résumé de la tâche de clonage.



9. Cliquez sur exécution du travail pour l'ouvrir `Job Details` fenêtre. L'état du travail peut également être ouvert et affiché à partir du `Monitor` onglet.



10. La base de données clonée s’enregistre immédiatement auprès de SnapCenter.



11. Validez la base de données de clonage sur l’hôte du serveur de base de données. Pour une base de données de développement clonée, le mode d’archivage de la base de données doit être désactivé.

```
[azureuser@ora-02 ~]$ sudo su
[root@ora-02 azureuser]# su - oracle
Last login: Tue Feb  6 16:26:28 UTC 2024 on pts/0

[oracle@ora-02 ~]$ uname -a
Linux ora-02 4.18.0-372.9.1.el8.x86_64 #1 SMP Fri Apr 15 22:12:19
EDT 2022 x86_64 x86_64 x86_64 GNU/Linux
[oracle@ora-02 ~]$ df -h
Filesystem                                          Size  Used Avail
Use% Mounted on
devtmpfs                                            7.7G     0  7.7G
0% /dev
tmpfs                                               7.8G     0  7.8G
0% /dev/shm
tmpfs                                               7.8G   49M  7.7G
1% /run
tmpfs                                               7.8G     0  7.8G
0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv                            22G   17G  5.6G
75% /
/dev/mapper/rootvg-usrlv                             10G  2.0G  8.1G
20% /usr
/dev/mapper/rootvg-homelv                          1014M   40M  975M
4% /home
/dev/sda1                                           496M  106M  390M
22% /boot
/dev/mapper/rootvg-varlv                            8.0G  958M  7.1G
12% /var
/dev/sda15                                          495M  5.9M  489M
2% /boot/efi
/dev/mapper/rootvg-tmplv                             12G  8.4G  3.7G
70% /tmp
tmpfs                                               1.6G     0  1.6G
0% /run/user/54321
172.30.136.68:/ora-02-u03                           250G  2.1G  248G
1% /u03
172.30.136.68:/ora-02-u01                           100G   10G   91G
10% /u01
172.30.136.68:/ora-02-u02                           250G  7.5G  243G
3% /u02
tmpfs                                               1.6G     0  1.6G
0% /run/user/1000
tmpfs                                               1.6G     0  1.6G
0% /run/user/0
172.30.136.68:/ora-01-u02-Clone-020624161543077  250G  8.2G  242G
```

```
4% /u02_ntap1dev

[oracle@ora-02 ~]$ 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.
#
#
NTAP2:/u01/app/oracle/product/19.0.0/NTAP2:Y
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT
REMOVE THIS LINE)
ntap1dev:/u01/app/oracle/product/19.0.0/NTAP2:N


[oracle@ora-02 ~]$ export ORACLE_SID=ntap1dev
[oracle@ora-02 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Feb 6 16:29:02 2024
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
--------- -------------------- ------------
NTAP1DEV  READ WRITE           ARCHIVELOG


SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup mount;
ORACLE instance started.

Total System Global Area 3221223168 bytes
Fixed Size                  9168640 bytes
Variable Size             654311424 bytes
Database Buffers         2550136832 bytes
Redo Buffers                7606272 bytes
Database mounted.

SQL> alter database noarchivelog;

Database altered.

SQL> alter database open;

Database altered.

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

NAME      OPEN_MODE            LOG_MODE
--------- -------------------- ------------
NTAP1DEV  READ WRITE           NOARCHIVELOG

SQL> show pdbs

    CON_ID CON_NAME                        OPEN MODE  RESTRICTED
---------- ------------------------------ ---------- ----------
         2 PDB$SEED                       READ ONLY  NO
         3 NTAP1_PDB1                     MOUNTED
         4 NTAP1_PDB2                     MOUNTED
         5 NTAP1_PDB3                     MOUNTED

SQL> alter pluggable database all open;
```

Où trouver des informations complémentaires

Pour en savoir plus sur les informations fournies dans ce document, consultez ces documents et/ou sites web :

- Azure NetApp Files

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

- Documentation du logiciel SnapCenter

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- Tr-4987 : déploiement Oracle simplifié et automatisé sur Azure NetApp Files avec NFS

  "https://docs.netapp.com/us-en/netapp-solutions/databases/automation_ora_anf_nfs.html"

Tr-4977 : sauvegarde, restauration et clonage des bases de données Oracle avec les services SnapCenter - Azure

Allen Cao, Niyaz Mohamed, NetApp

Objectif

Les services SnapCenter sont la version SaaS de l'outil classique de gestion de bases de données SnapCenter disponible via la console de gestion cloud NetApp BlueXP. Il fait partie intégrante de l'offre NetApp de sauvegarde et de protection des données dans le cloud pour les bases de données telles qu'Oracle et HANA s'exécutant sur Azure NetApp Files. Ce service SaaS simplifie le déploiement traditionnel de serveurs autonomes SnapCenter qui nécessite généralement un serveur Windows fonctionnant dans un environnement de domaine Windows.

Dans cette documentation, nous vous démontrons comment configurer les services SnapCenter pour sauvegarder, restaurer et cloner les 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 web BlueXP.

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde de bases de données avec des snapshots pour les bases de données Oracle hébergées dans des machines virtuelles Azure NetApp Files et Azure
- Restauration de la base de données Oracle en cas de défaillance
- Clonage rapide des bases de données primaires pour le développement, les environnements de test ou d'autres utilisations

Public

Cette solution est destinée aux publics suivants :

- Administrateur de bases de données gérant les bases de données Oracle exécutées sur un système de stockage Azure NetApp Files
- Architecte de solutions qui souhaite tester la sauvegarde, la restauration et le clonage des bases de données Oracle dans Azure

- L'administrateur du stockage qui prend en charge et gère le stockage Azure NetApp Files
- 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 la solution

Les tests et la validation de cette solution ont été réalisés dans un environnement de laboratoire qui ne correspond peut-être pas à l'environnement de déploiement final. Pour plus d'informations, reportez-vous à la section [Key Factors for Deployment Consideration].

Architecture

Cette image fournit une vue détaillée de la sauvegarde et de la restauration BlueXP pour les applications de la console BlueXP, notamment l'interface utilisateur, le connecteur et les ressources qu'il gère.

Composants matériels et logiciels

Matériel

Le stockage Azure NetApp Files	Niveau de service Premium	Le type de QoS automatique et une capacité de stockage de 4 To ont été testés
Instance Azure pour le calcul	Standard B4ms (4 vcpu, 16 Gio de mémoire)	Deux instances déployées, l'une en tant que serveur de base de données principal et l'autre en tant que serveur de base de données clone

Logiciel

Red Hat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Déploiement de l'abonnement Red Hat pour les tests
Base de données Oracle	Version 19.18	Patch RU appliqué p34765931_190000_Linux-x86-64.zip
OPICH Oracle	Version 12.2.0.1.36	Dernier correctif p6880880_190000_Linux-x86-64.zip
Service SnapCenter	Version v2.5.0-2822	Agent version v2.5.0-2822

Facteurs clés à prendre en compte lors du déploiement

- **Le connecteur doit être déployé 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 utilisateur Azure ou un principe de service Active Directory créé sur le portail Azure pour SnapCenter Connector.** le déploiement d'un connecteur BlueXP nécessite des autorisations spécifiques pour créer et configurer une machine virtuelle et d'autres ressources de calcul, configurer la mise en réseau et accéder à l'abonnement Azure. Il requiert également des autorisations pour créer ultérieurement des rôles et des autorisations pour que le connecteur puisse fonctionner. Créez un rôle personnalisé dans Azure avec des autorisations et affectez-le au compte utilisateur ou au principe de

service. Pour plus d'informations, cliquez sur le lien suivant :"Configurez 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 VM Azure pour se connecter à l'hôte du connecteur et également à l'hôte de la VM de base de données pour déployer et exécuter un plug-in. L'interface utilisateur de la console BlueXP utilise la clé ssh pour déployer le plug-in de service SnapCenter sur l'hôte de base de données pour l'installation du plug-in en une étape et la découverte de la base de données des hôtes d'application.
- **Une information d'identification a été ajoutée au paramètre de la console BlueXP.** pour ajouter du stockage Azure NetApp Files à l'environnement de travail BlueXP, une information d'identification qui accorde des autorisations d'accès à Azure NetApp Files à partir de la console BlueXP doit être configurée dans le paramètre de la console BlueXP.
- **Java-11-openjdk installé sur l'hôte d'instance de base de données de la VM Azure.** l'installation du service SnapCenter nécessite la version Java 11. Il doit être installé sur l'hôte d'application avant la tentative de déploiement du plug-in.

Déploiement de la solution

La documentation NetApp étendue offre une portée plus large pour vous aider à protéger les données de vos applications cloud natives. L'objectif de cette documentation est de fournir des procédures détaillées qui couvrent le déploiement des services SnapCenter avec la console BlueXP afin de protéger votre base de données Oracle déployée sur un stockage Azure NetApp Files et une instance de calcul Azure.

Pour commencer, procédez comme suit :

- Lisez les instructions générales "Protégez vos données applicatives cloud natives" Et les sections relatives à Oracle et Azure NetApp Files.
- Regardez la vidéo de présentation suivante

  Vidéo du déploiement d'Oracle et d'ANF

Conditions préalables au déploiement du service SnapCenter

Le déploiement nécessite les conditions préalables suivantes.

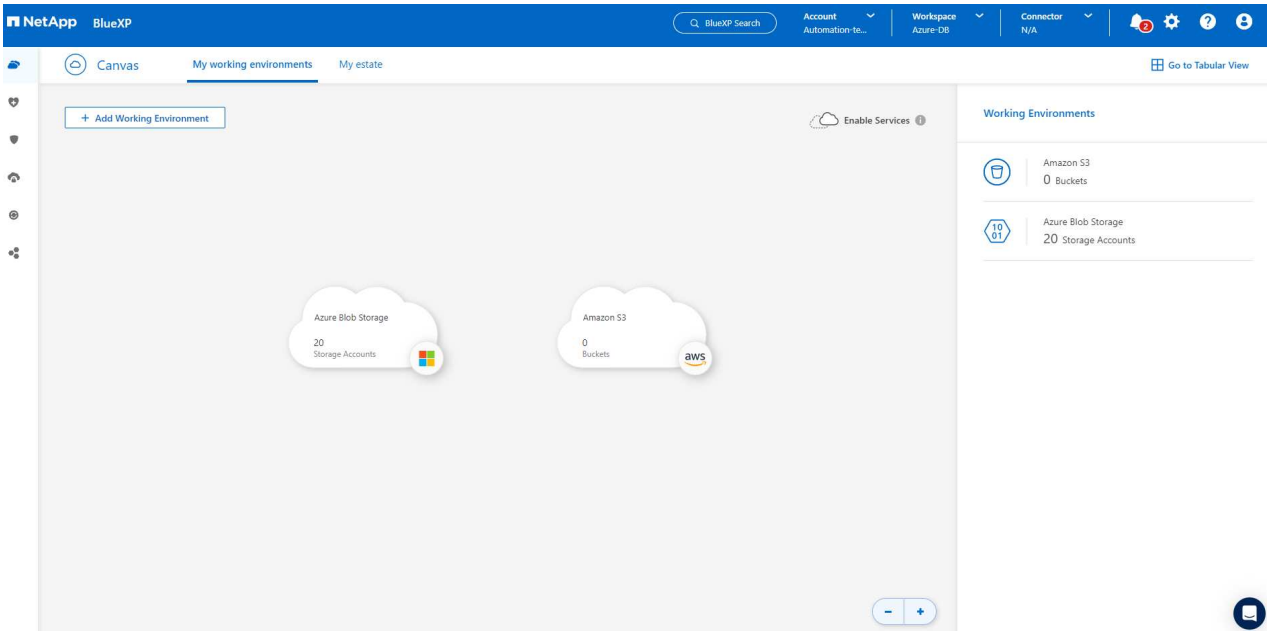
1. Serveur de base de données Oracle primaire sur une instance de machine virtuelle Azure avec une base de données Oracle entièrement déployée et en cours d'exécution.
2. Pool de capacité du service de stockage Azure NetApp Files déployé dans Azure qui peut répondre aux besoins de stockage de la base de données répertoriés dans la section des composants matériels.
3. 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 afin de prendre en charge une charge de travail de développement/test ou tout cas d'utilisation nécessitant un jeu de données complet de la base de données Oracle de production.
4. Pour plus d'informations sur le déploiement de bases de données Oracle sur Azure NetApp Files et l'instance de calcul Azure, reportez-vous à la section "Déploiement et protection de bases de données Oracle sur Azure NetApp Files".

Intégration de la préparation à BlueXP

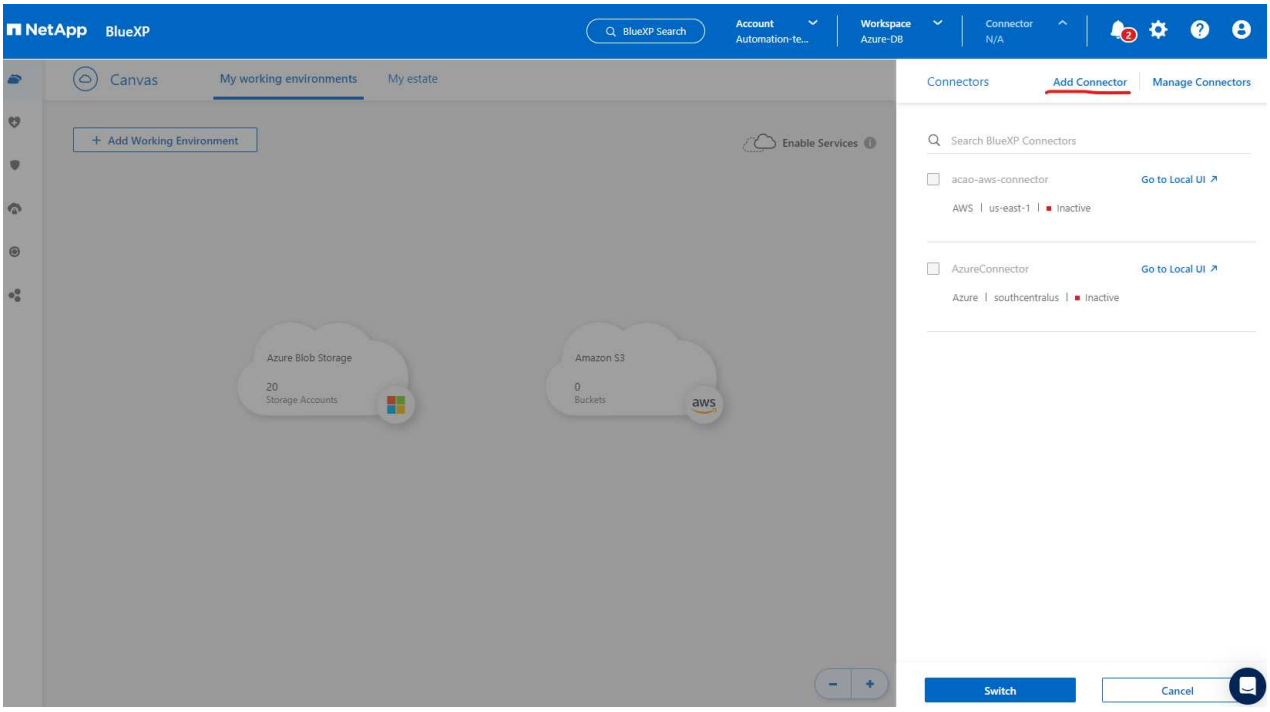
1. Utilisez le lien "NetApp BlueXP" Pour vous inscrire à l'accès à la console BlueXP.
2. Créez un compte utilisateur Azure ou un principe de service Active Directory et octroyez des autorisations avec un rôle dans le portail Azure pour le déploiement du connecteur Azure.
3. Pour configurer BlueXP afin de gérer les ressources Azure, ajoutez une information 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 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 VM, etc. Prêt pour le provisionnement des connecteurs et l'installation des plug-ins de base de données.

Déployez un connecteur pour les services SnapCenter

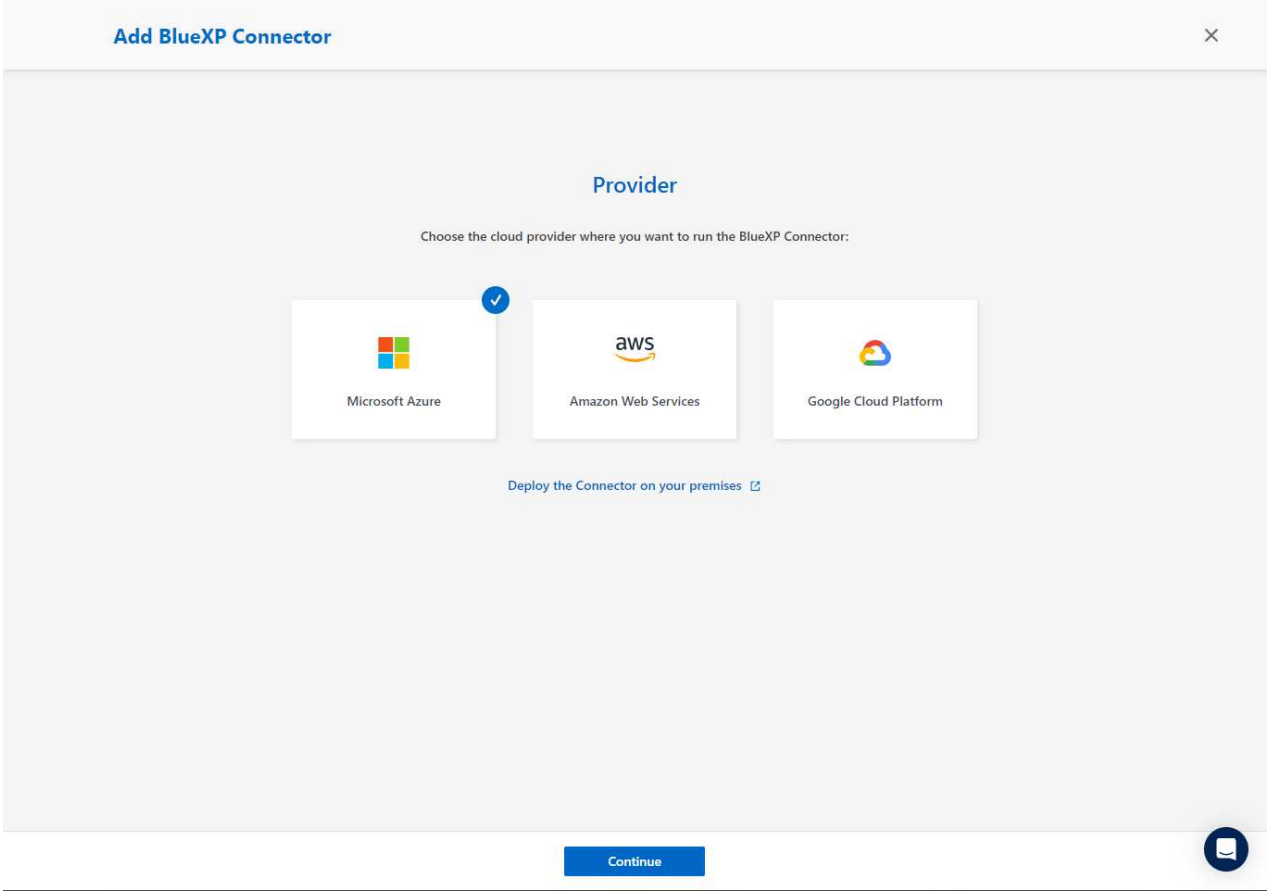
1. Connectez-vous à la console BlueXP.



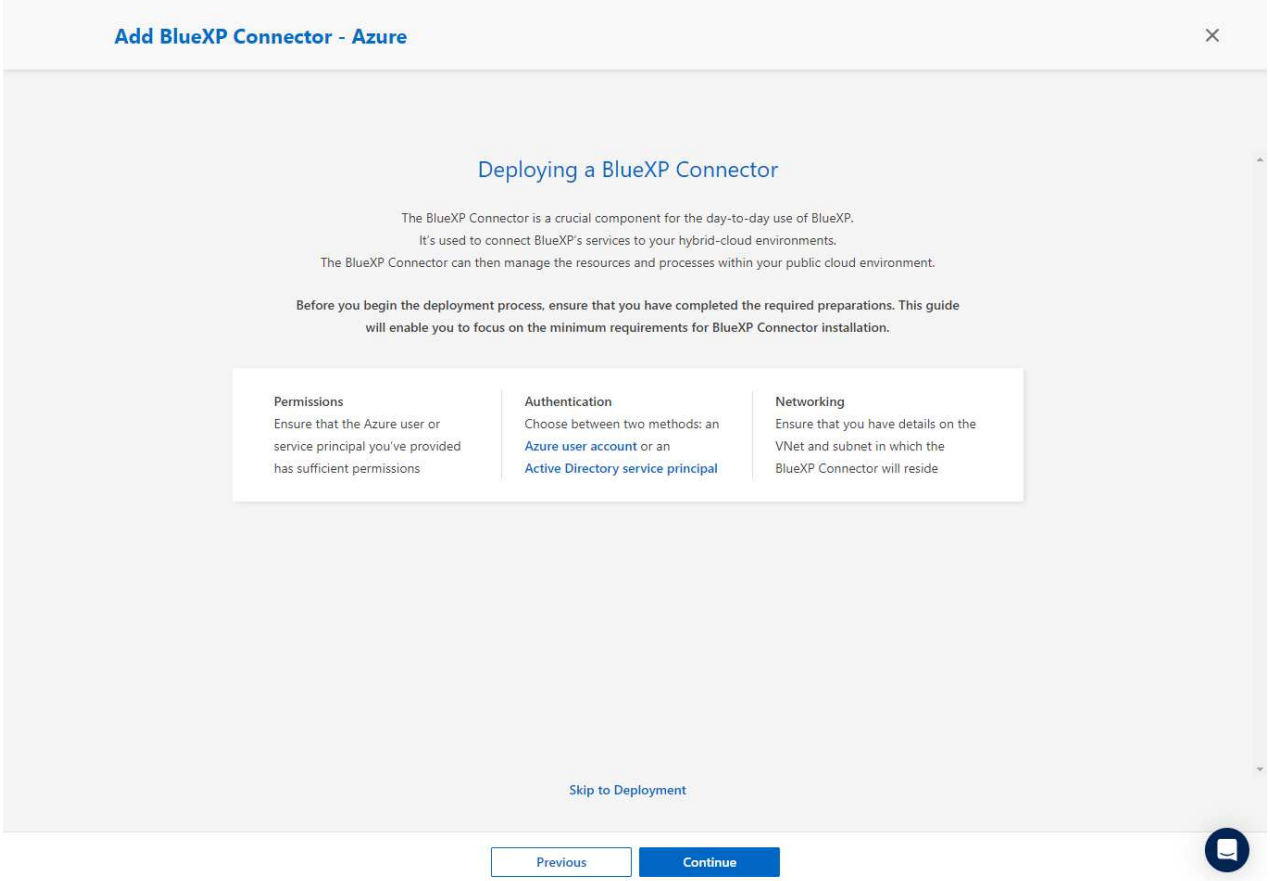
2. Cliquez sur la flèche déroulante **Connector** et sur **Add Connector** pour lancer le flux de production de provisionnement de connecteur.



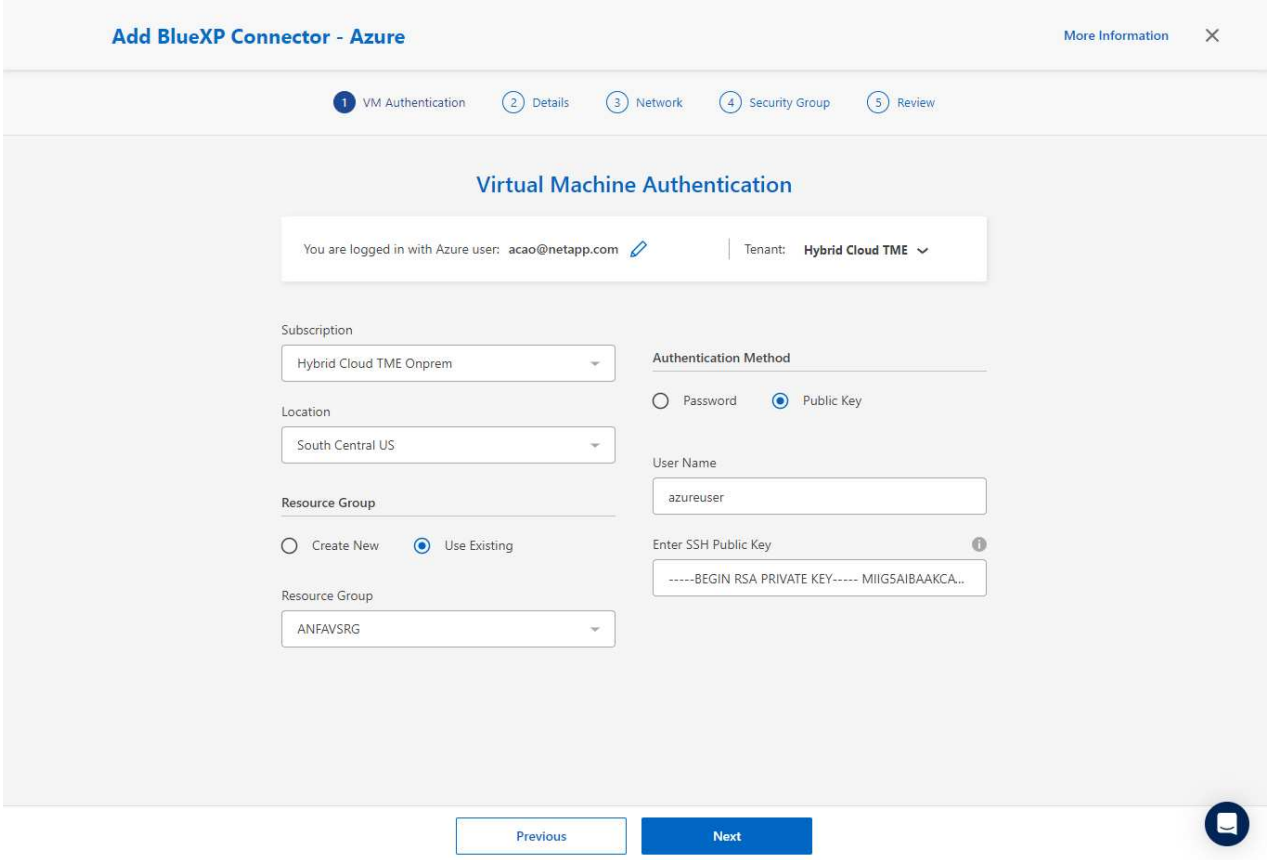
3. Choisissez votre fournisseur de cloud (dans ce cas, **Microsoft Azure**).



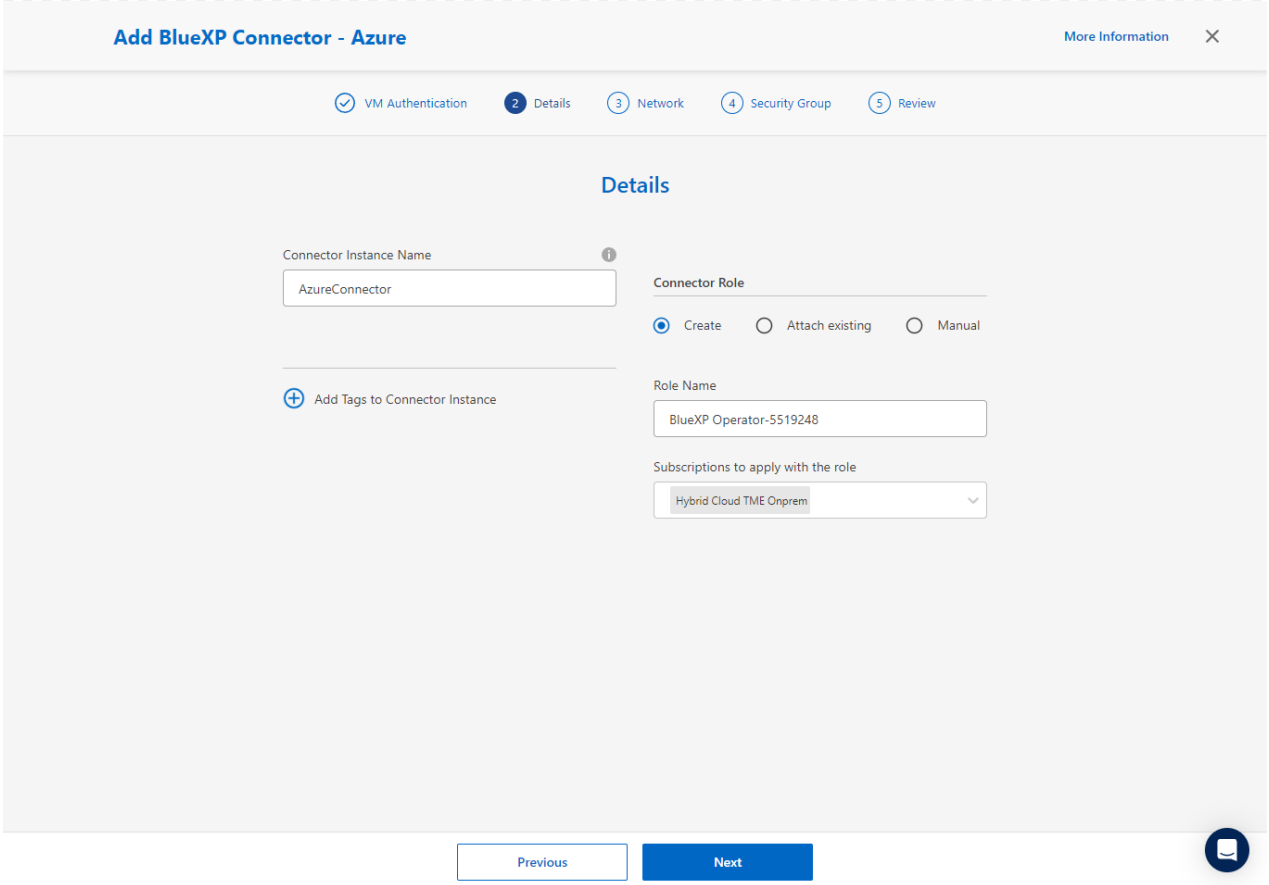
4. Ignorez les étapes **permission**, **authentification** et **mise en réseau** si vous les avez déjà configurées dans votre compte Azure. Si ce n’est pas le cas, vous devez les configurer avant de continuer. À partir de là, vous pouvez également récupérer les autorisations de la règle Azure référencée dans la section précédente "Intégration de la préparation à BlueXP."



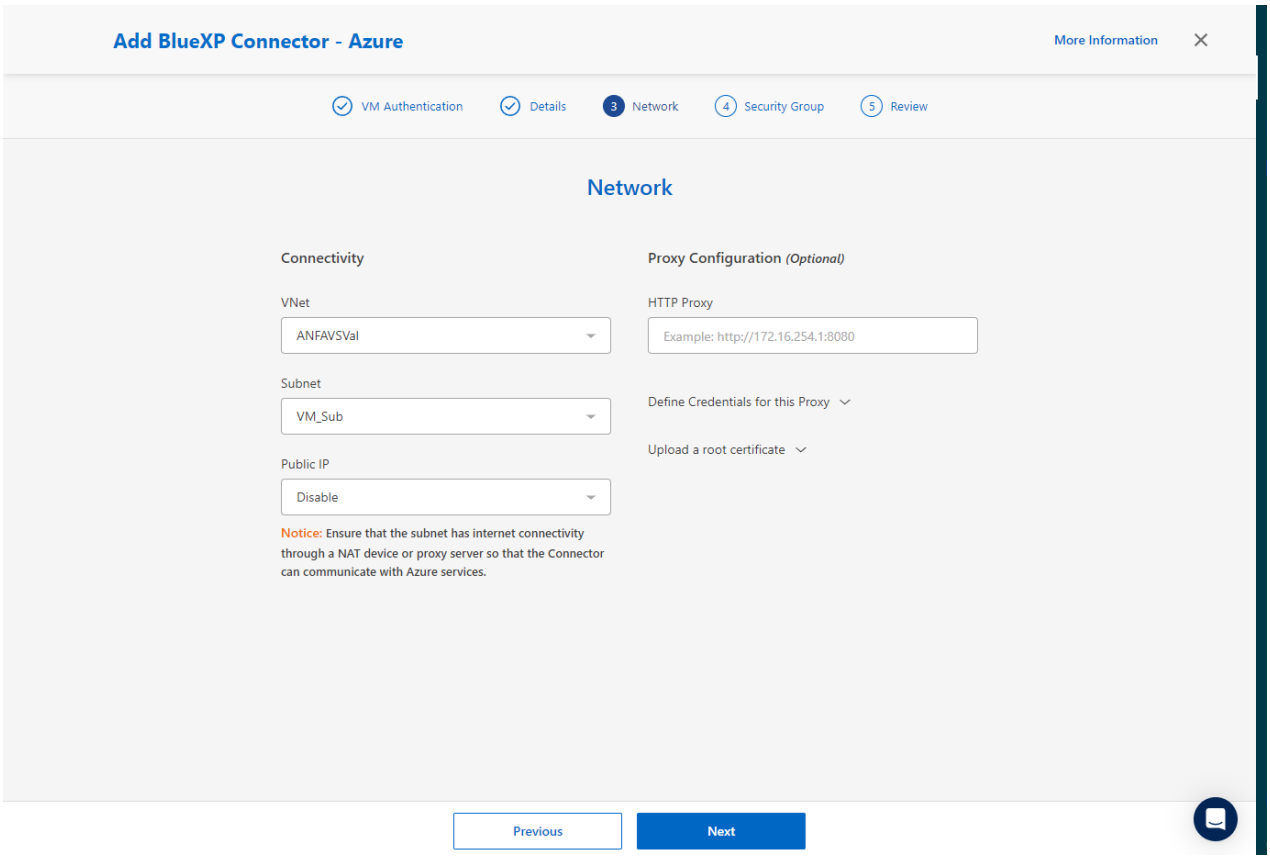
5. Cliquez sur **passer au déploiement** pour configurer votre connecteur **authentification de la machine virtuelle**. Ajoutez la paire de clés SSH que vous avez créée dans le groupe de ressources Azure lors de l'intégration à la préparation BlueXP pour l'authentification du connecteur OS.



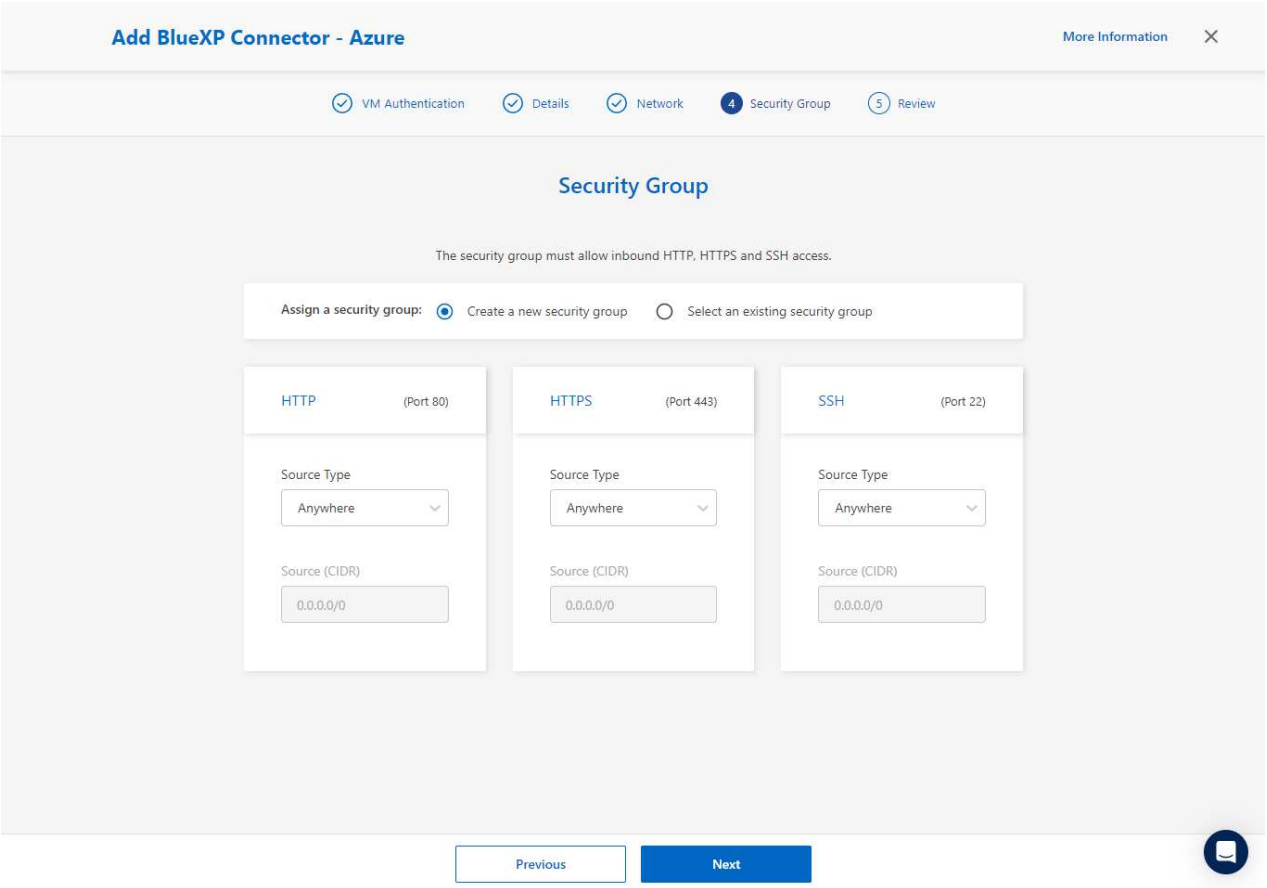
6. Indiquez un nom pour l'instance de connecteur, sélectionnez **Create** et acceptez par défaut **Role Name** sous **Details**, puis choisissez l'abonnement pour le compte Azure.



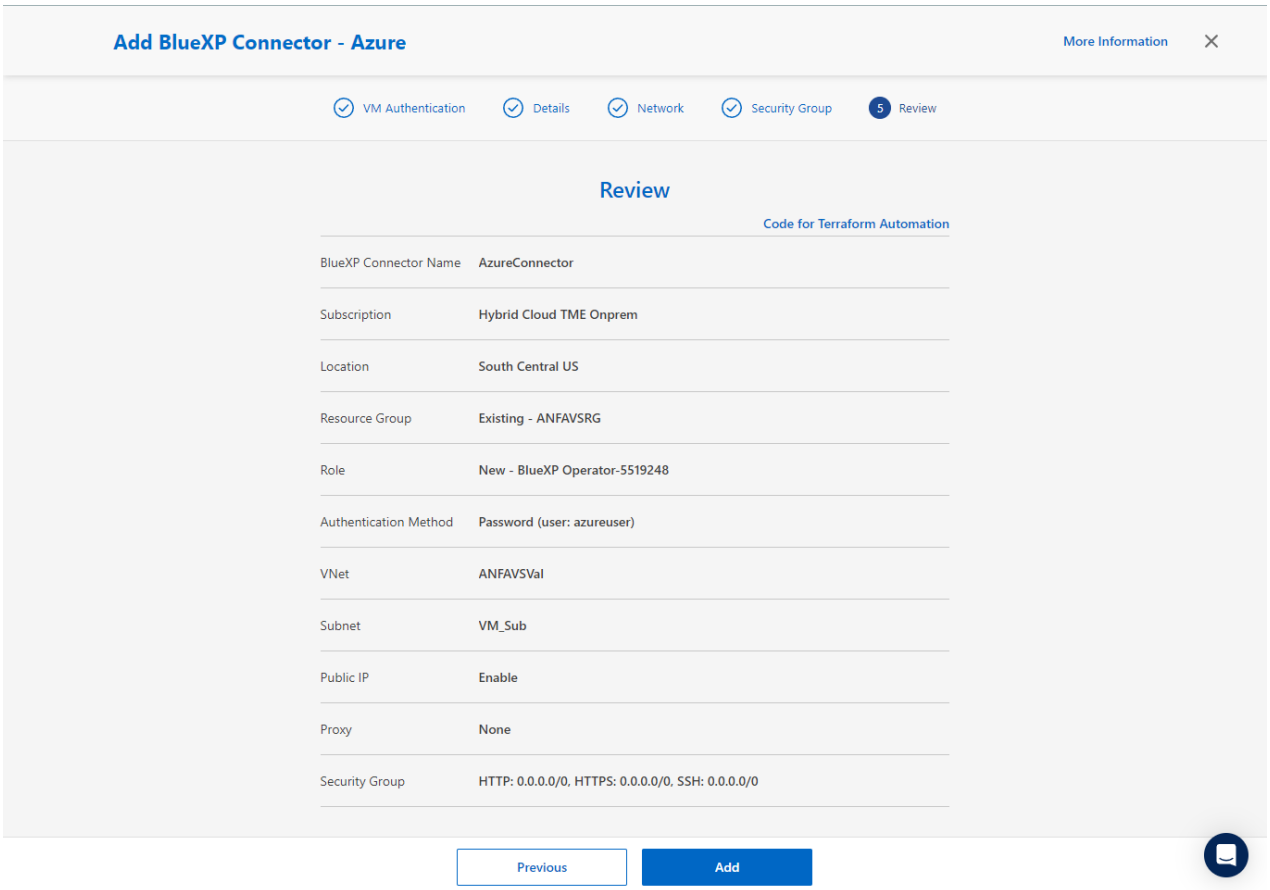
7. Configurez la mise en réseau avec le **vnet**, **Subnet** et désactivez **public IP**, mais assurez-vous que le connecteur dispose de l'accès à Internet dans votre environnement Azure.



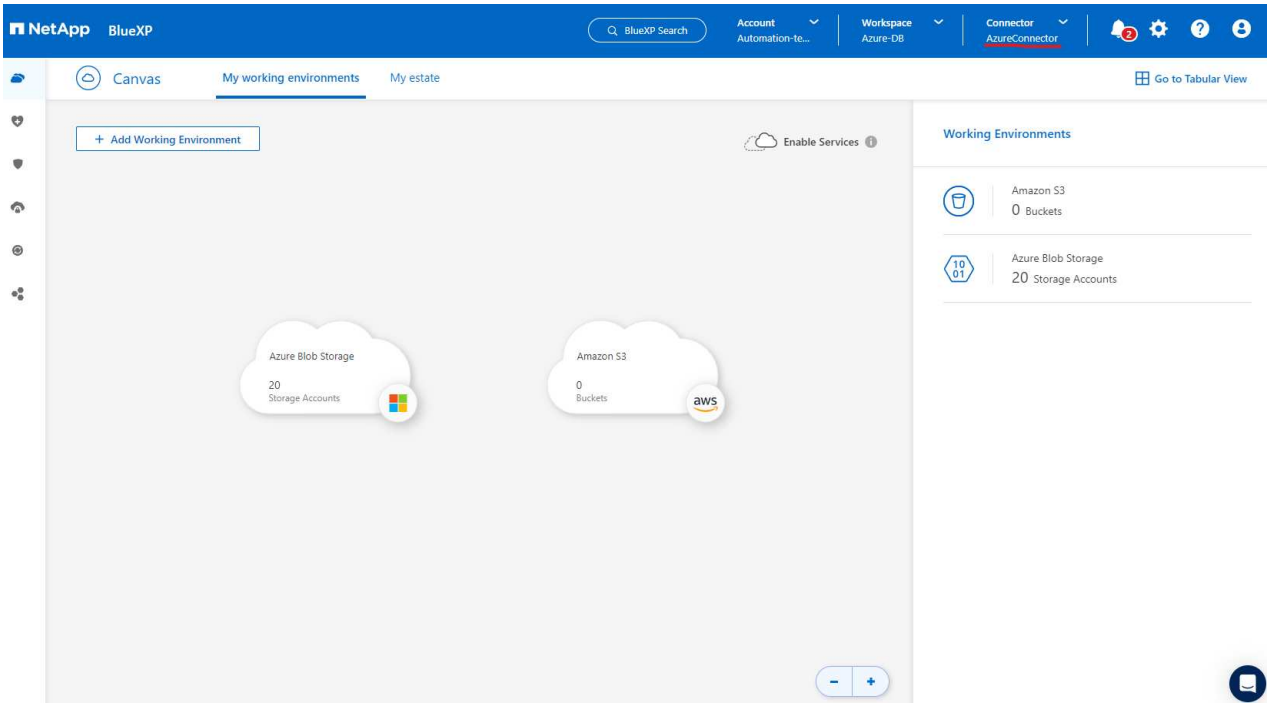
8. Configurez le **Groupe de sécurité** pour le connecteur qui autorise l'accès HTTP, HTTPS et SSH.



9. Passez en revue la page de résumé et cliquez sur **Ajouter** pour lancer la création du connecteur. Le déploiement prend généralement environ 10 minutes. Une fois l'opération terminée, la machine virtuelle de l'instance de connecteur apparaît sur le portail Azure.

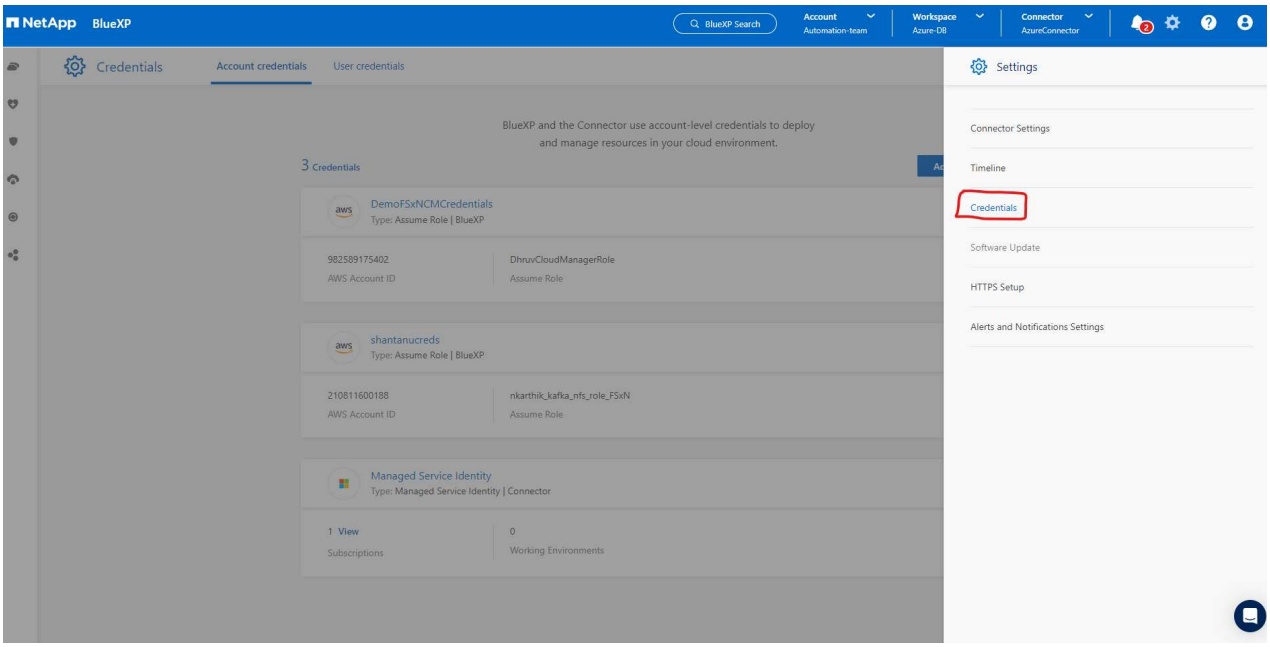


10. Une fois le connecteur déployé, le nouveau connecteur apparaît sous la liste déroulante **Connector**.

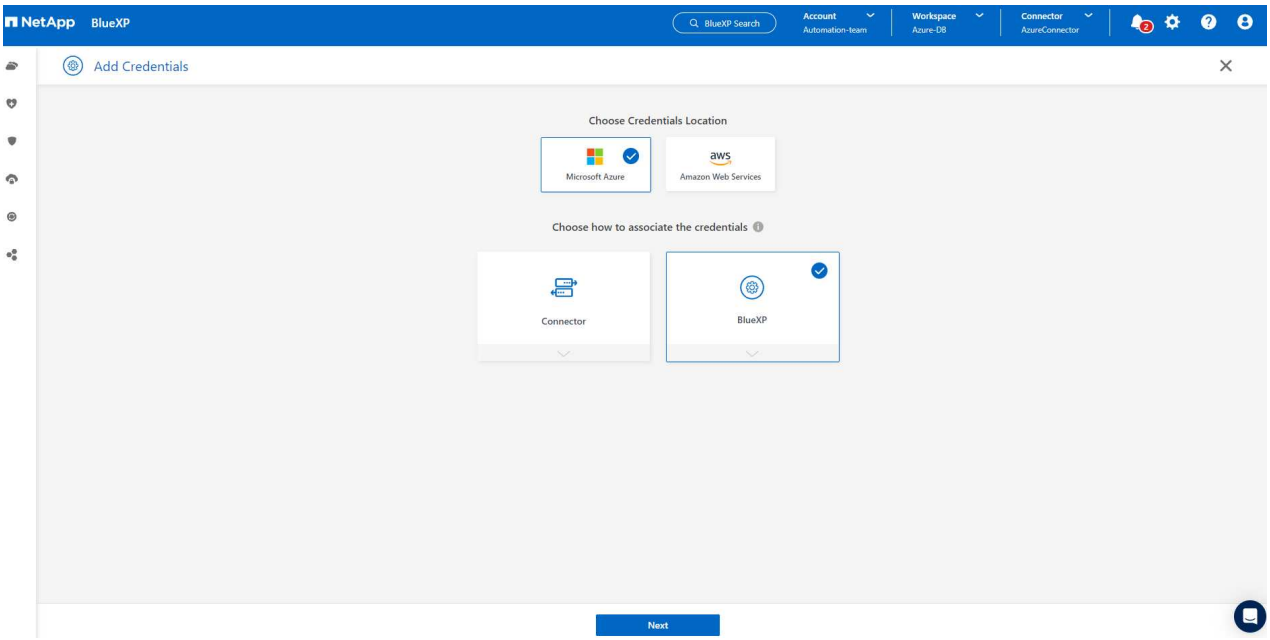


Définissez des identifiants dans BlueXP pour l’accès aux ressources Azure

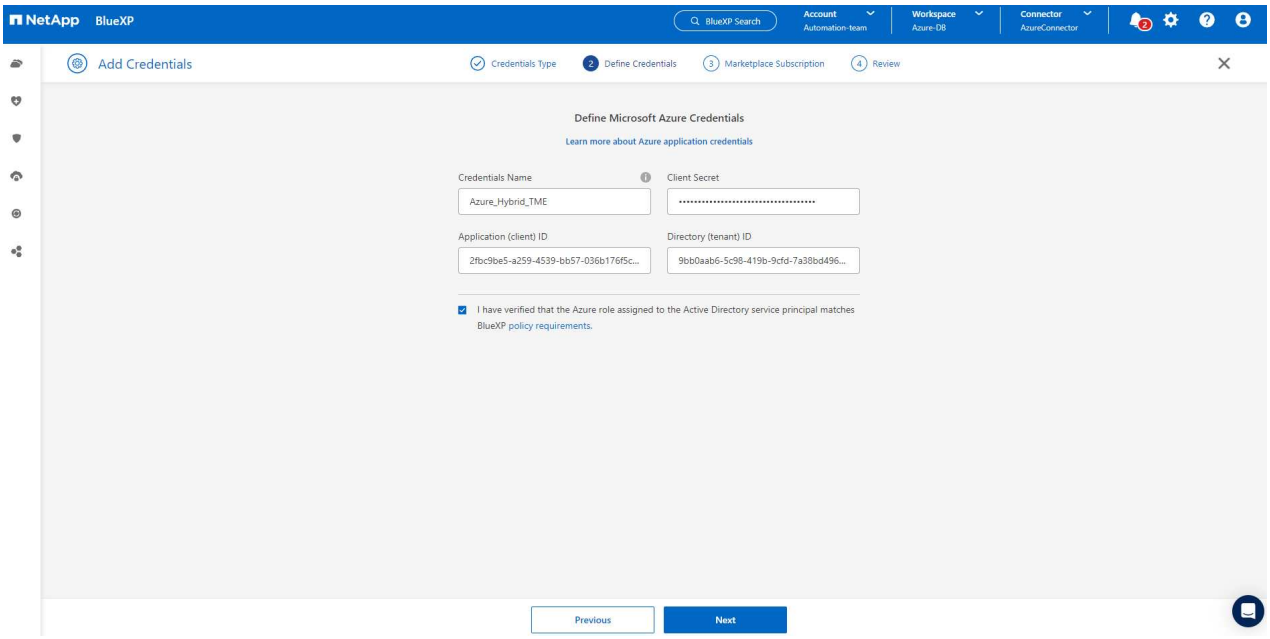
1. Cliquez sur l'icône de configuration dans le coin supérieur droit de la console BlueXP pour ouvrir la page **informations d'identification du compte**, cliquez sur **Ajouter des informations d'identification** pour démarrer le workflow de configuration des informations d'identification.



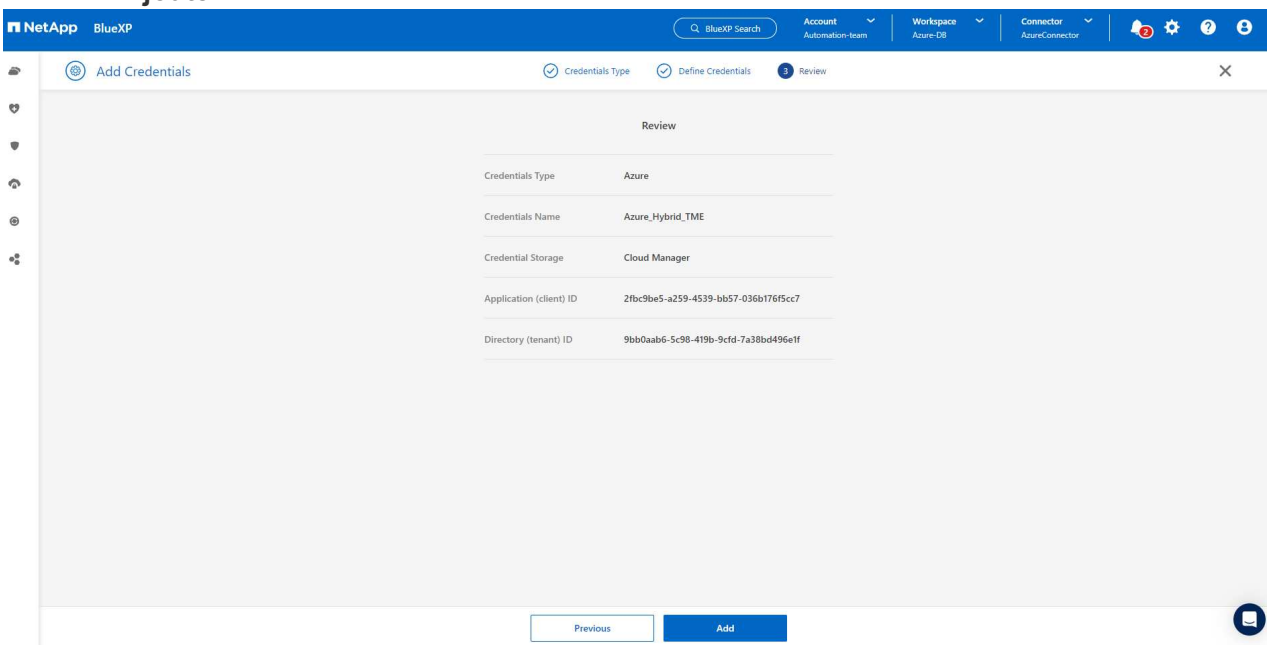
2. Choisissez l'emplacement des identifiants - **Microsoft Azure - BlueXP**.



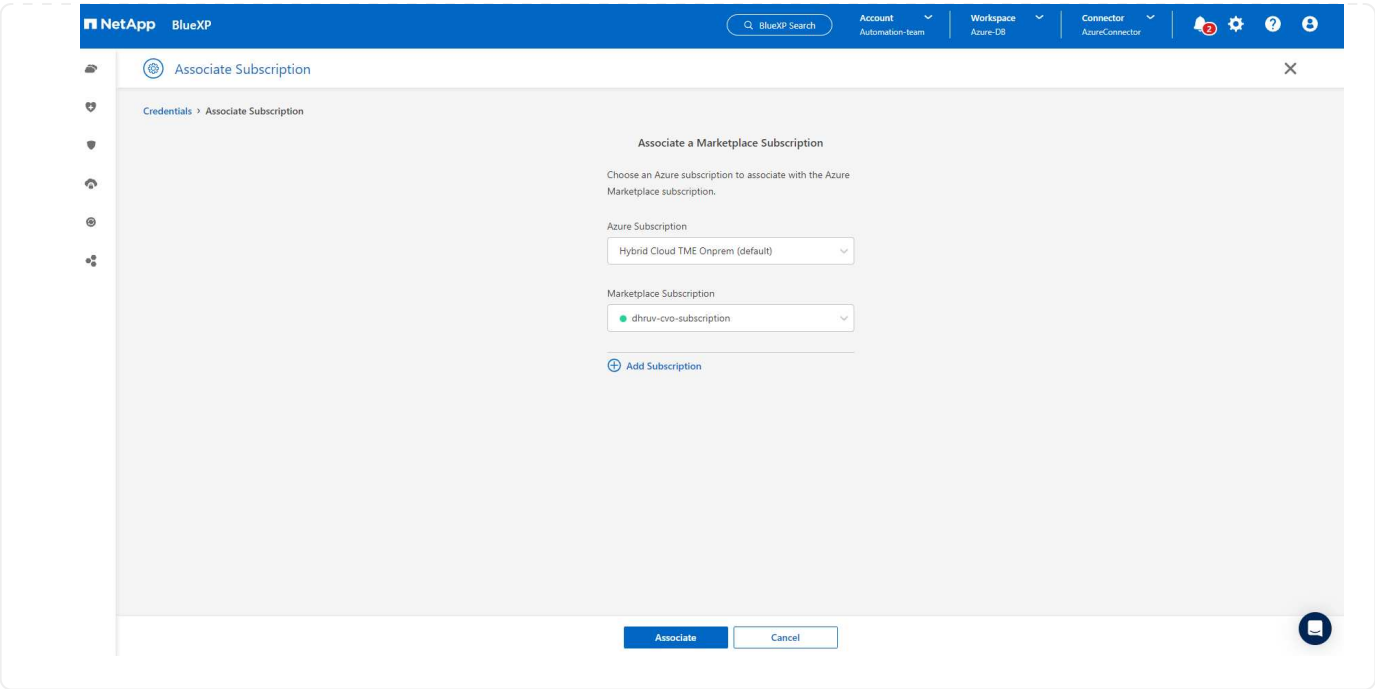
3. Définissez les informations d'identification Azure avec **client Secret**, **client ID** et **tenant ID** appropriés, qui doivent avoir été recueillies lors du processus d'intégration BlueXP précédent.



4. Revoir et **Ajouter**.



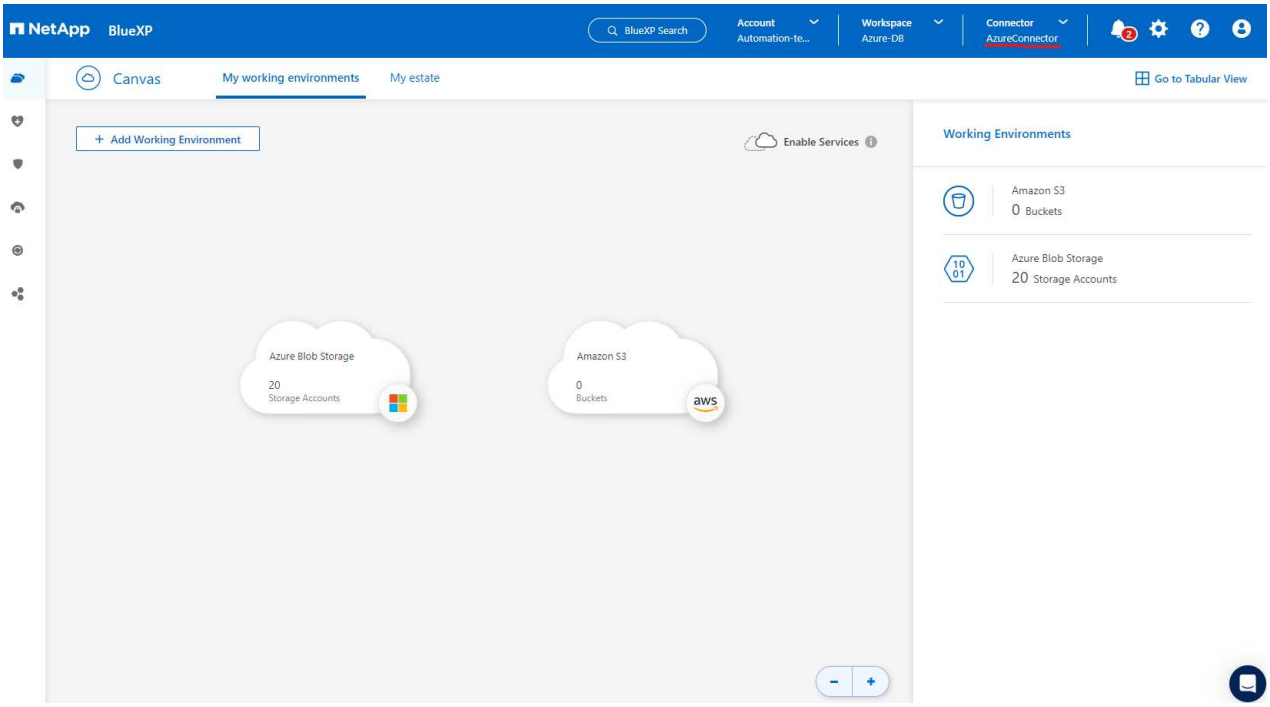
5. Vous devrez peut-être également associer un **abonnement Marketplace** à l'information d'identification.



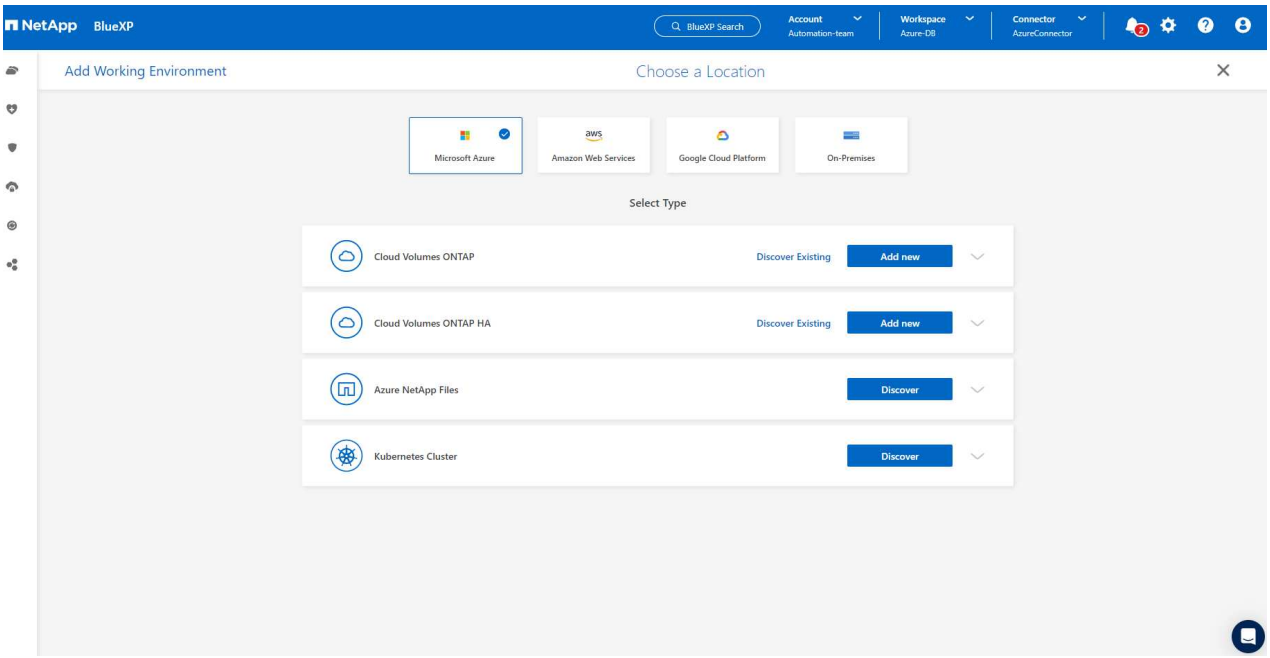
Configuration des services SnapCenter

Une fois les informations d'identification Azure configurées, les services SnapCenter peuvent maintenant être configurés avec les procédures suivantes :

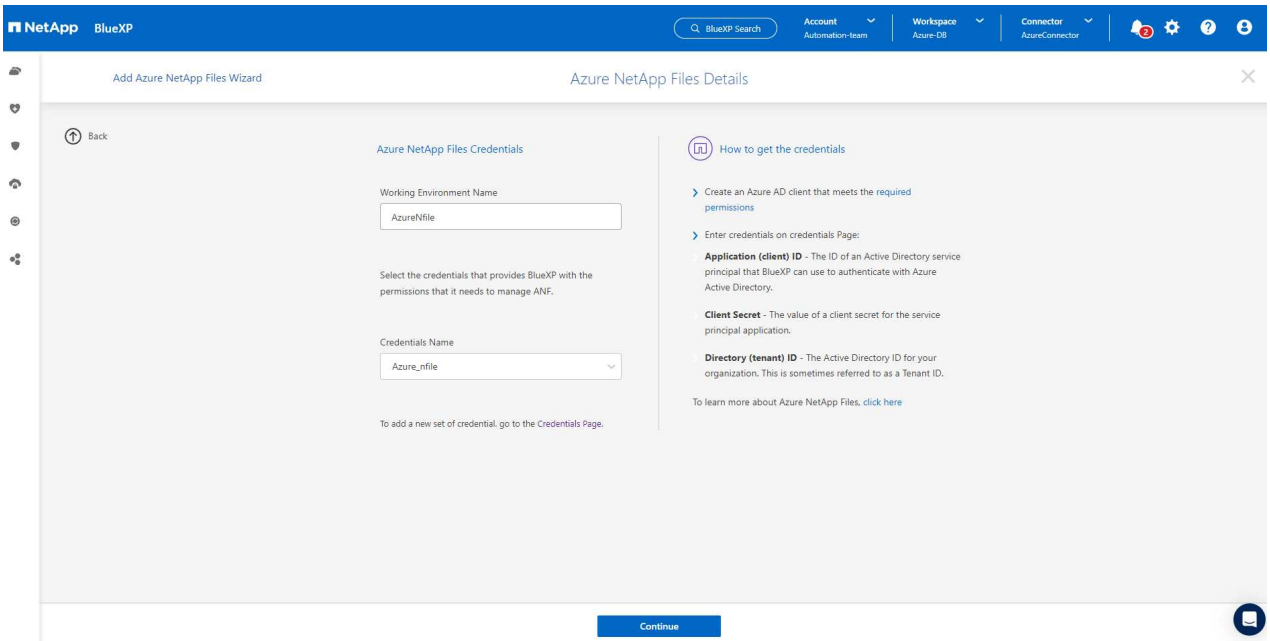
1. Retour à la page Canvas, à partir de **mon environnement de travail** cliquez sur **Ajouter un environnement de travail** pour découvrir Azure NetApp Files déployé dans Azure.



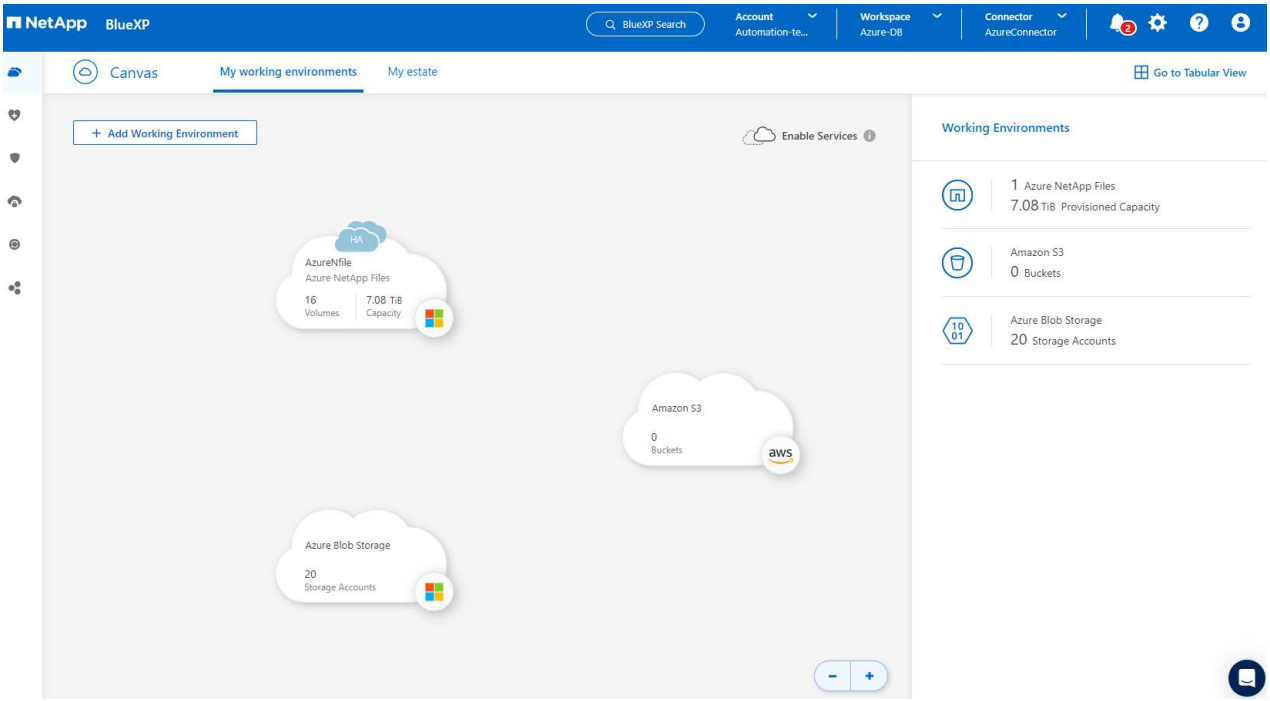
2. Choisissez **Microsoft Azure** comme emplacement et cliquez sur **découvrir**.



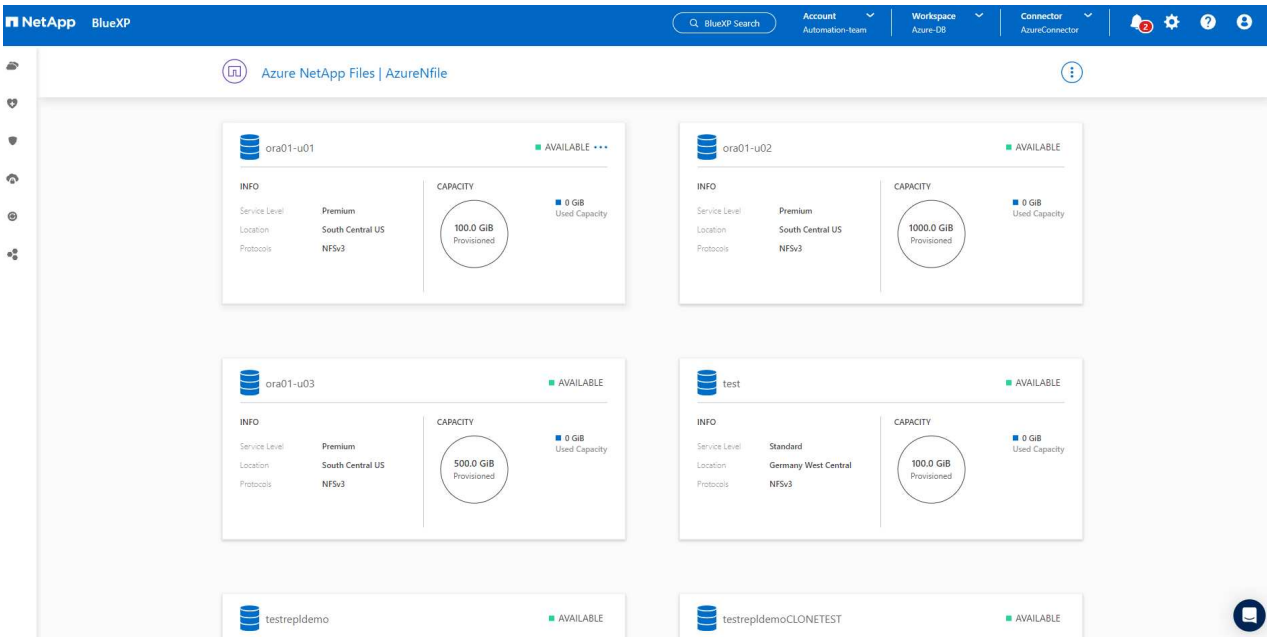
3. Nommez **Environnement de travail** et choisissez **Nom d'identification** créé dans la section précédente, puis cliquez sur **Continuer**.



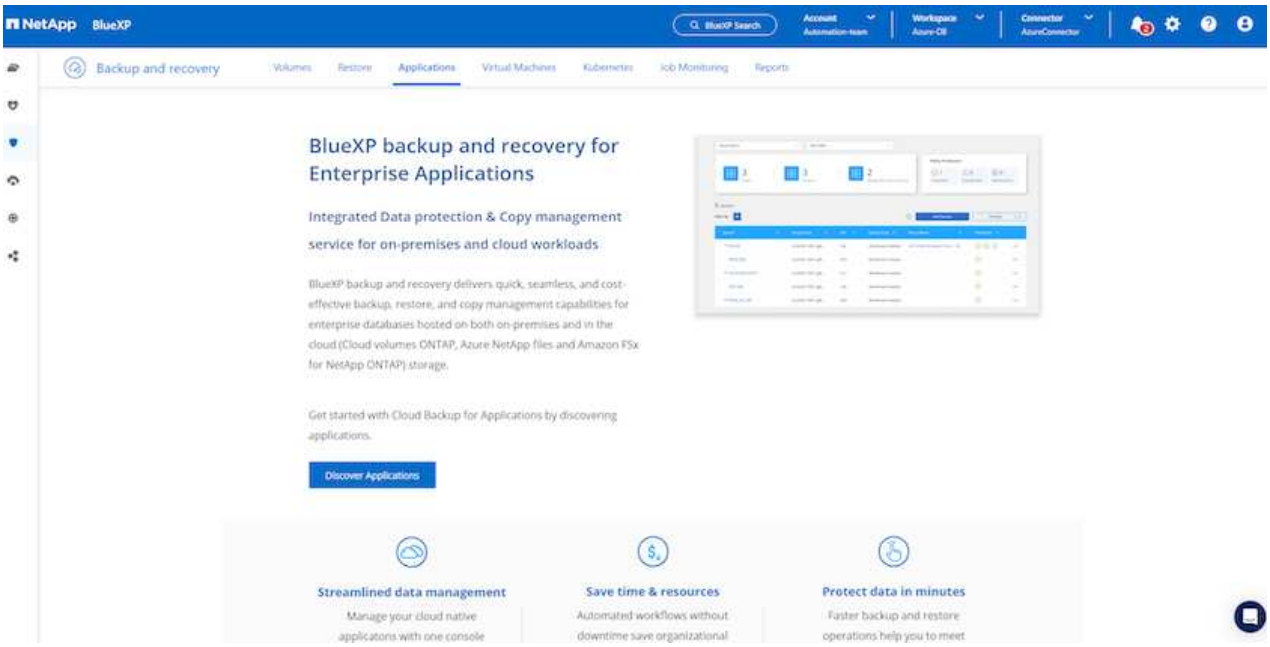
4. La console BlueXP revient à **Mes environnements de travail** et Azure NetApp Files découvert à partir d'Azure apparaît maintenant sur **Canvas**.



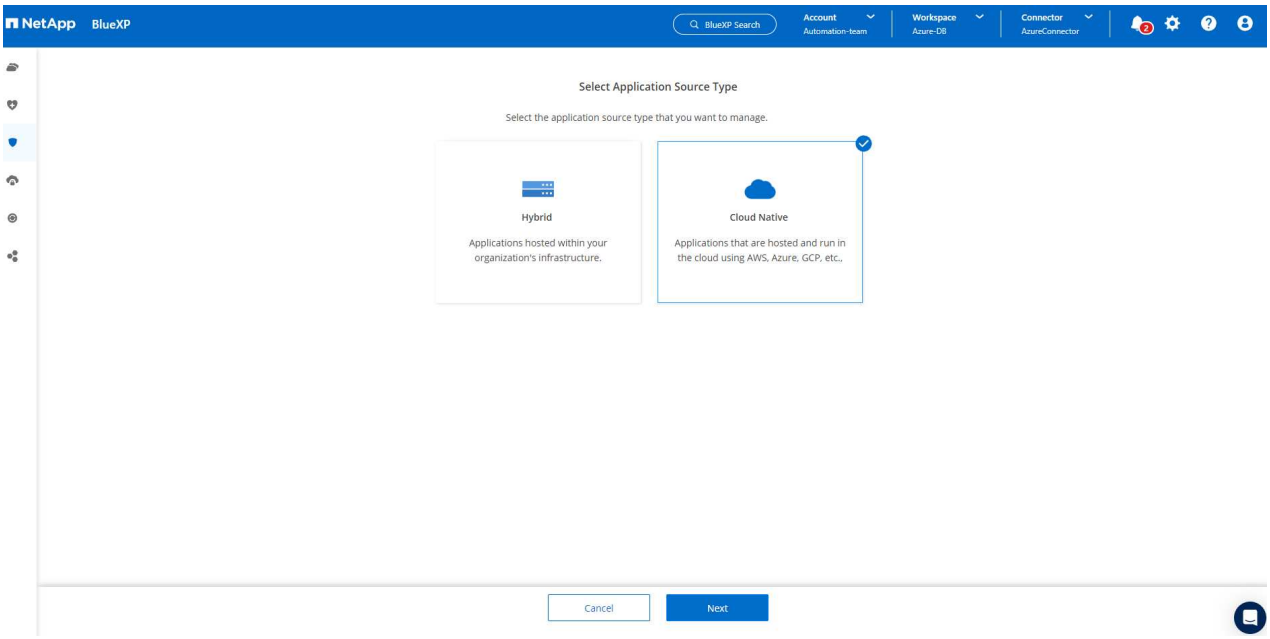
5. Cliquez sur l'icône **Azure NetApp Files**, puis sur **entrer dans l'environnement de travail** pour afficher les volumes de base de données Oracle déployés dans le stockage Azure NetApp Files.



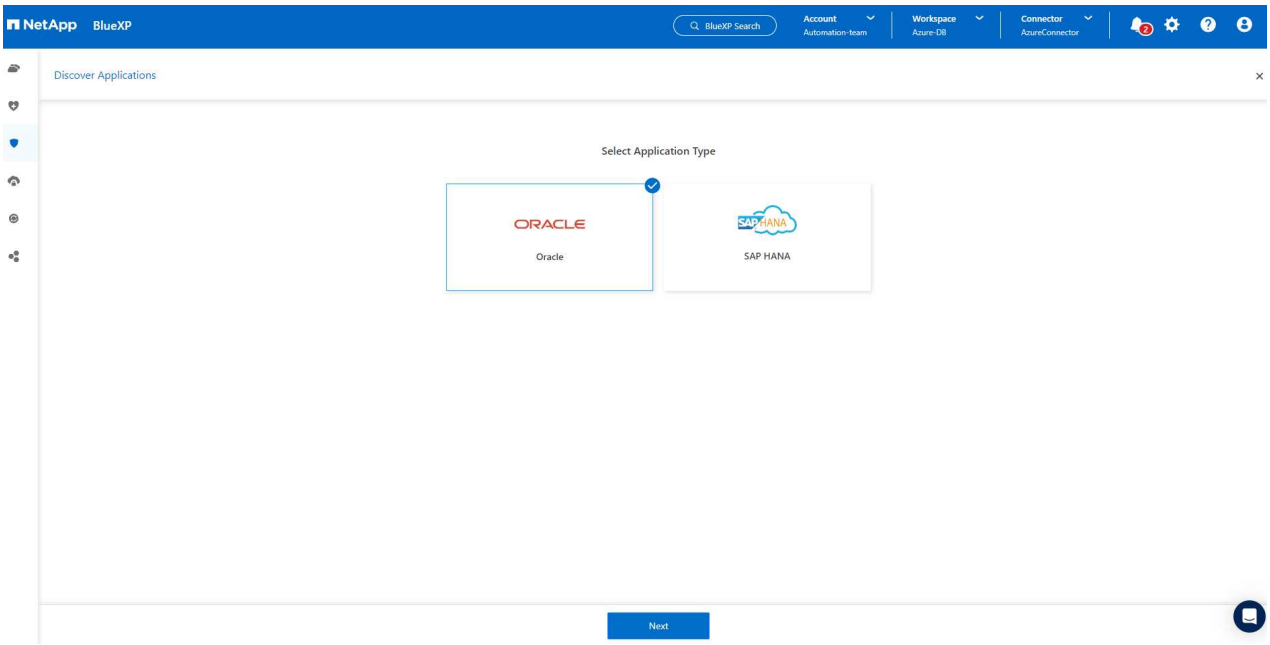
6. Dans la barre latérale gauche de la console, passez votre souris sur l'icône de protection, puis cliquez sur **protection** > **applications** pour ouvrir la page de lancement applications. Cliquez sur **découvrir les applications**.



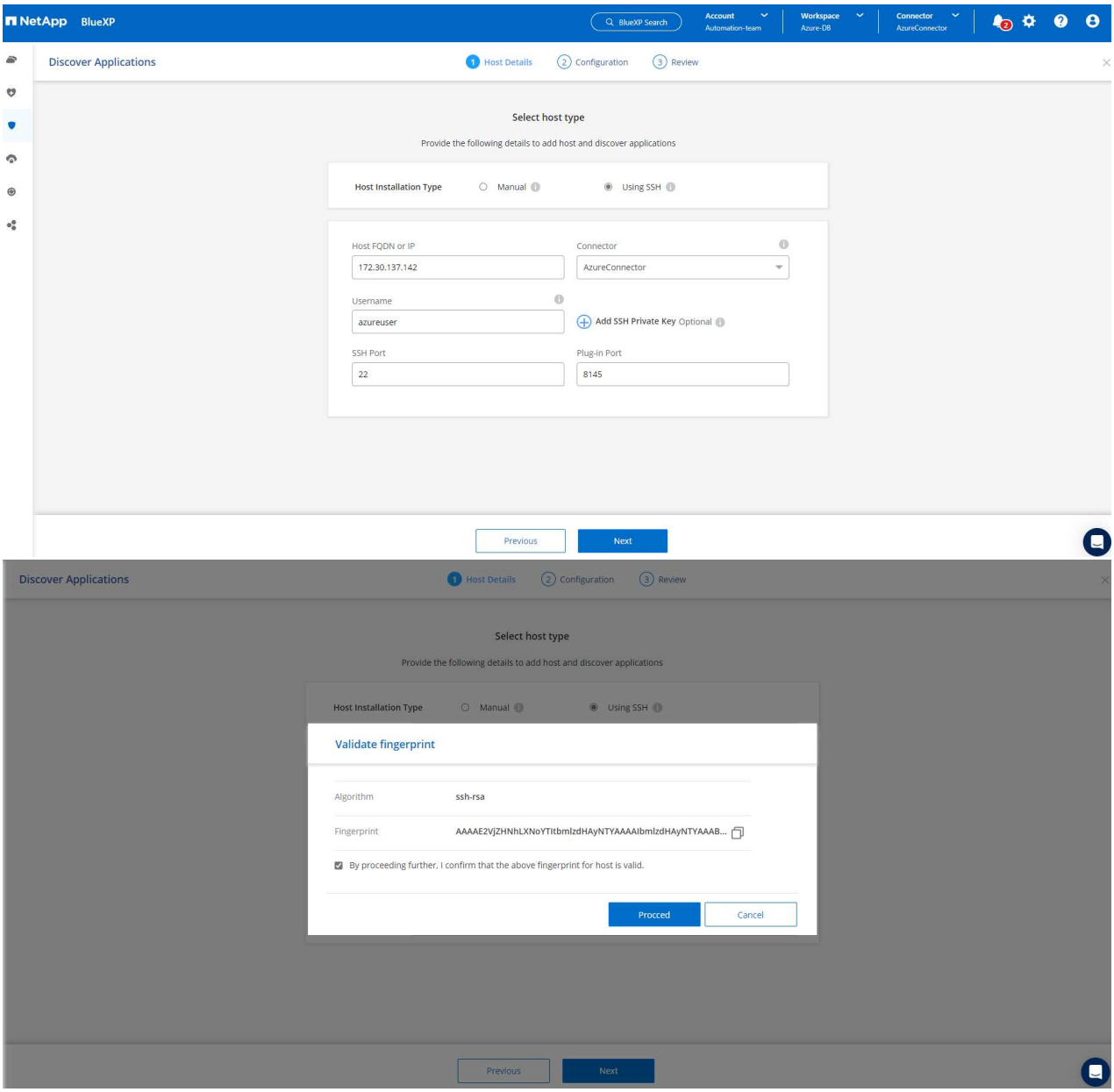
7. Sélectionnez **Cloud Native** comme type de source d'application.



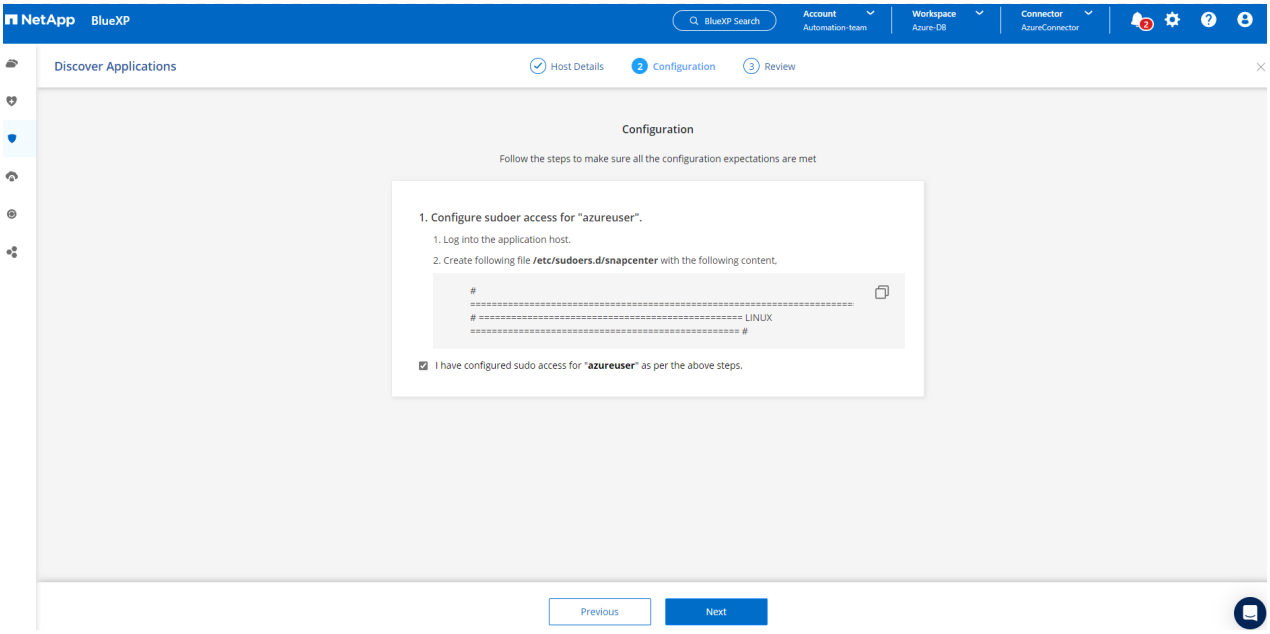
8. Choisissez **Oracle** pour le type d'application, cliquez sur **Suivant** pour ouvrir la page de détails de l'hôte.



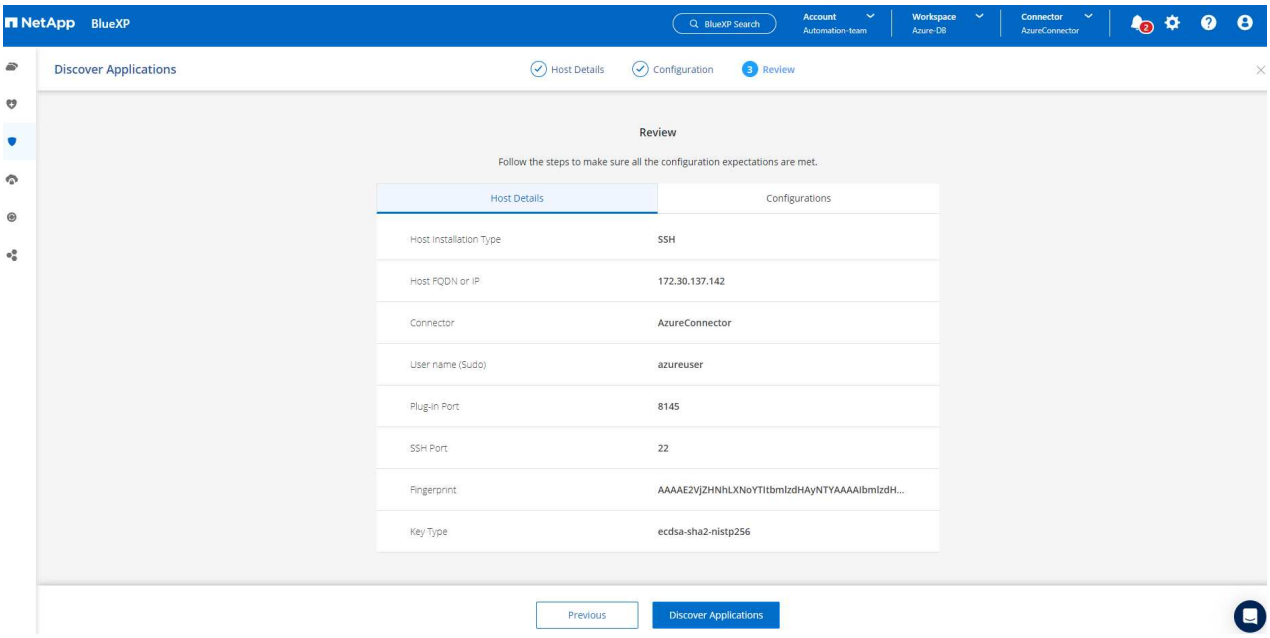
9. Sélectionnez **à l'aide de SSH** et fournissez les détails de la machine virtuelle Oracle Azure tels que **adresse IP**, **connecteur**, gestion de la machine virtuelle Azure **Nom d'utilisateur** tel qu'azuretuser. Cliquez sur **Ajouter une clé privée SSH** pour coller dans la paire de clés SSH que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



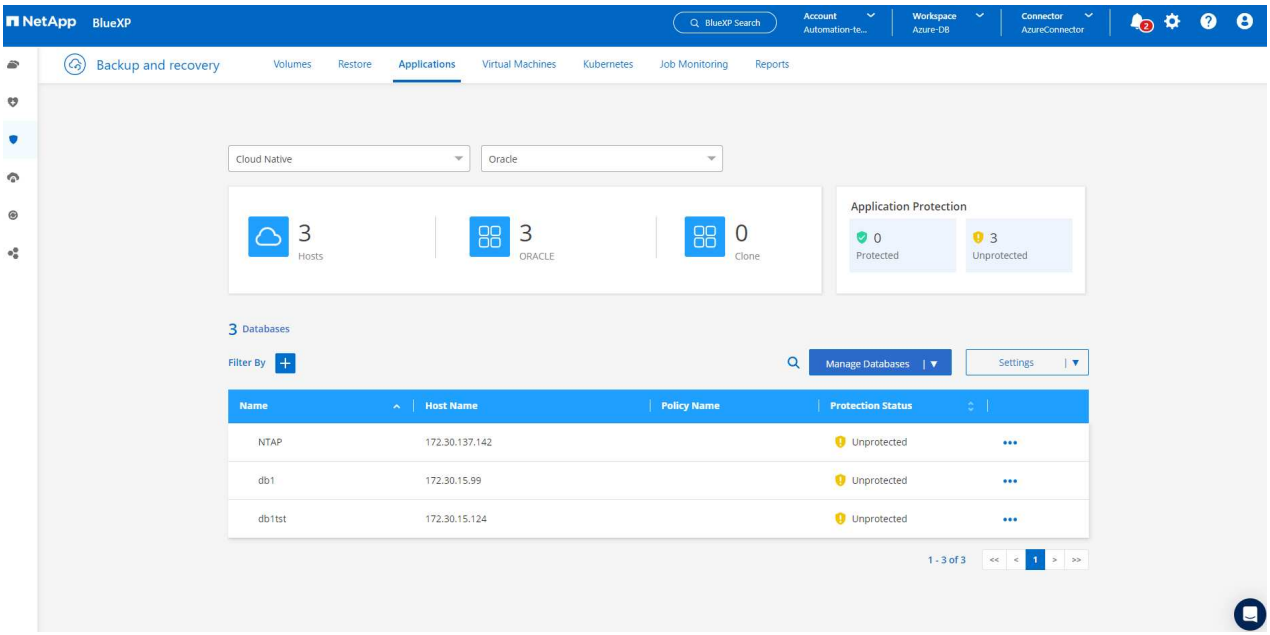
10. Passez à la page **Configuration** suivante pour configurer l'accès du sudoer sur la machine virtuelle Oracle Azure.



11. Passez en revue et cliquez sur **Discover applications** pour installer un plug-in 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** indique le nombre d'hôtes et de bases de données Oracle au sein de l'environnement. La base de données **Etat de protection** s'affiche initialement sous la forme **non protégé**.



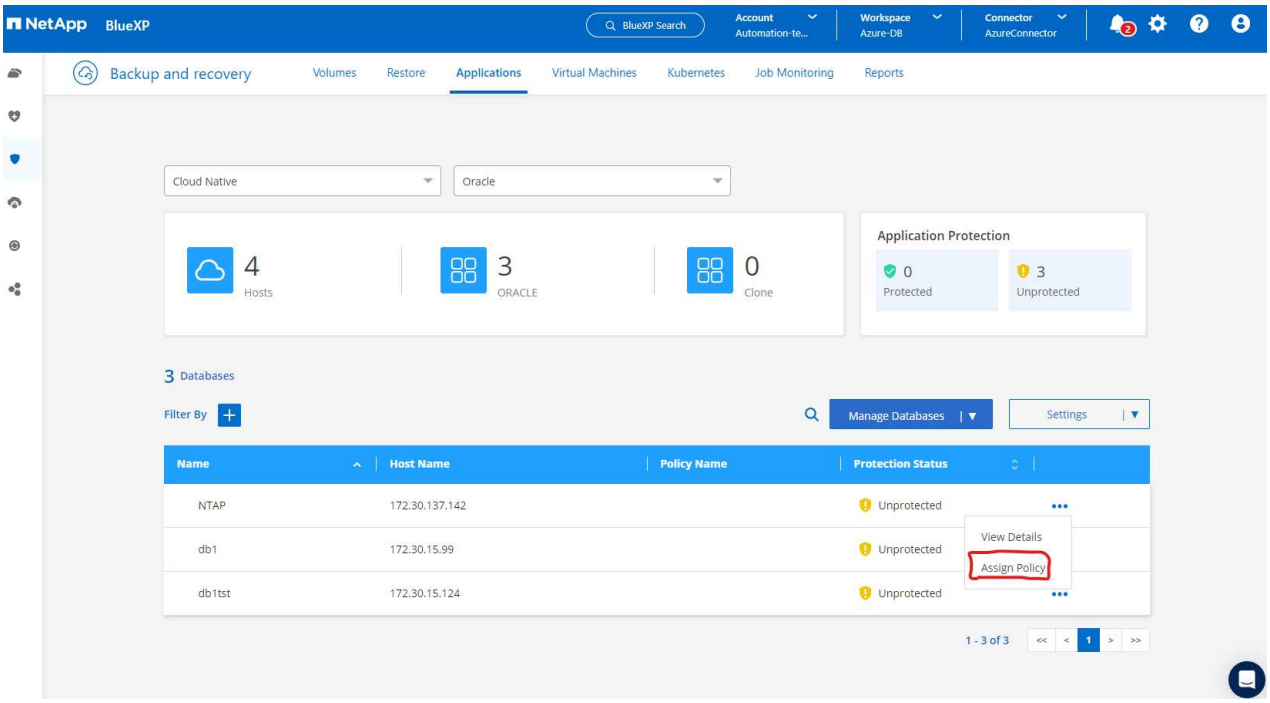
La configuration initiale des services SnapCenter pour Oracle est terminée. Les trois sections suivantes de ce document décrivent les opérations de sauvegarde, de restauration et de clonage de bases de données Oracle.

Sauvegarde de la base de données Oracle

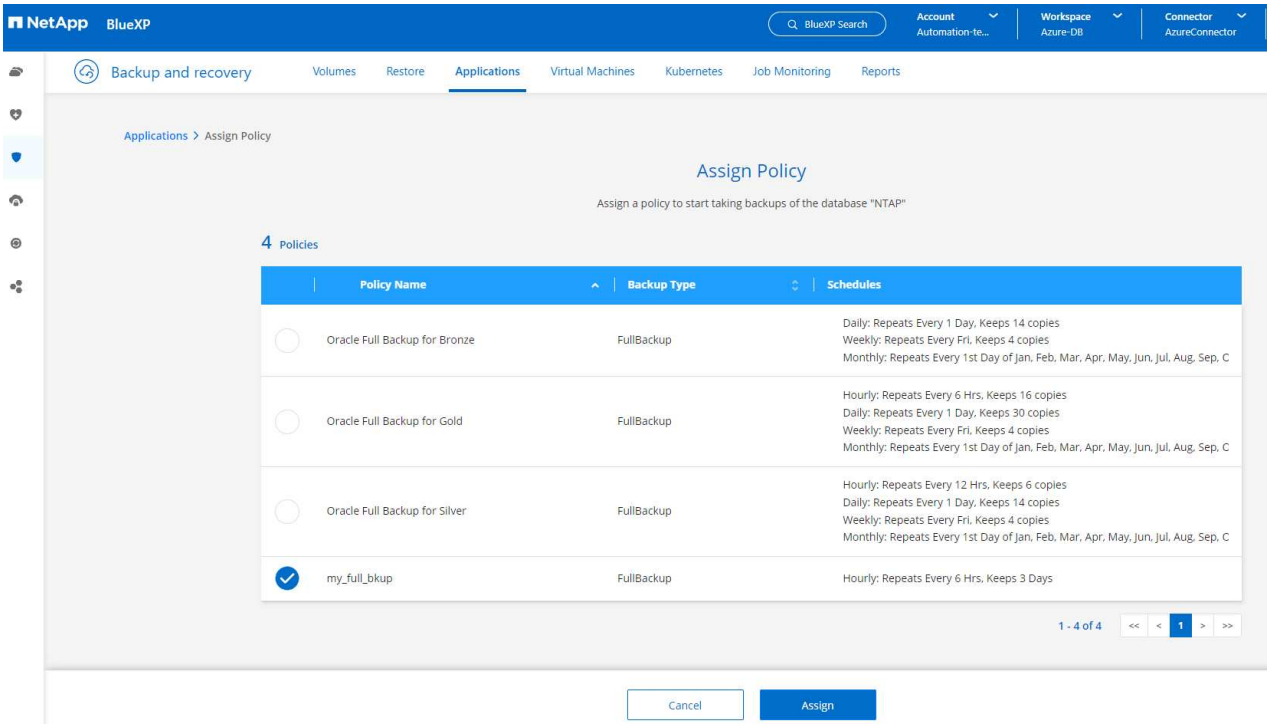
1. Notre base de données Oracle de test dans Azure VM est configurée avec trois volumes, avec un stockage total global d'environ 1.6 Tio. Cela donne un contexte sur la durée de la sauvegarde, de la restauration et du clonage d'un snapshot d'une base de données de cette taille.

```
[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 ~]$
```

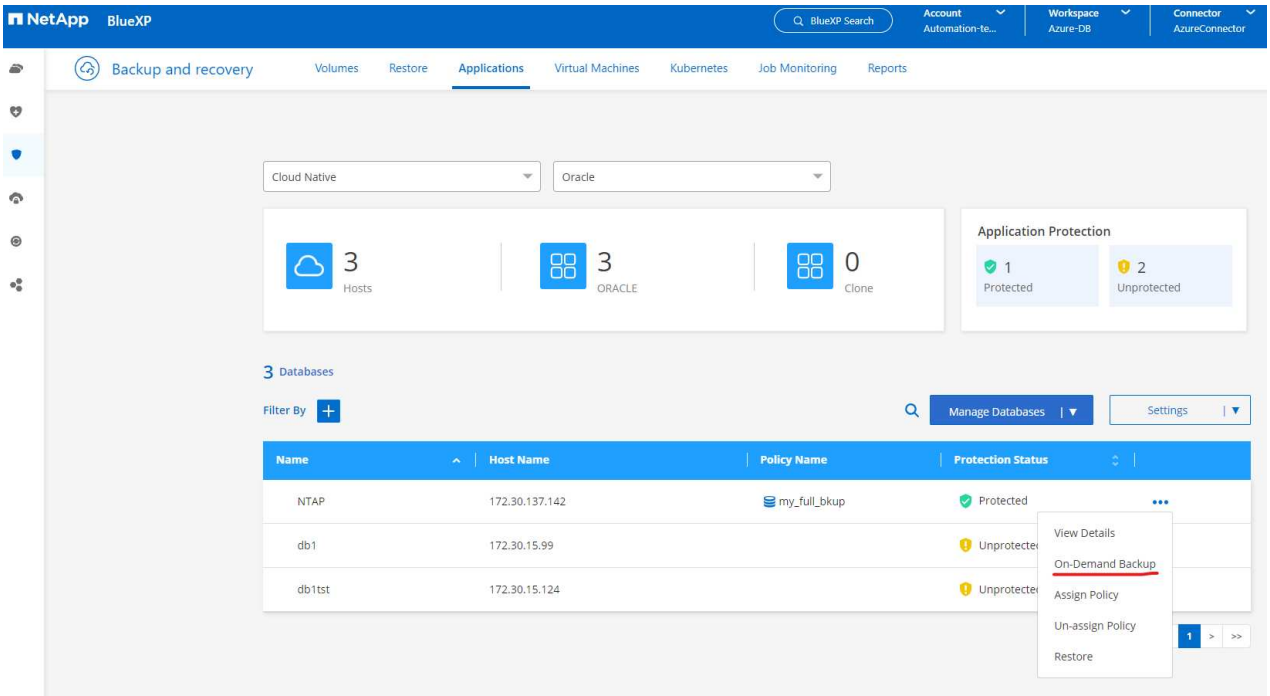
1. Pour protéger la base de données, cliquez sur les trois points en regard de la base de données **Etat de protection**, puis cliquez sur **affecter une stratégie** pour afficher les stratégies de protection de base de données préchargées ou définies par l'utilisateur par défaut qui peuvent être appliquées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



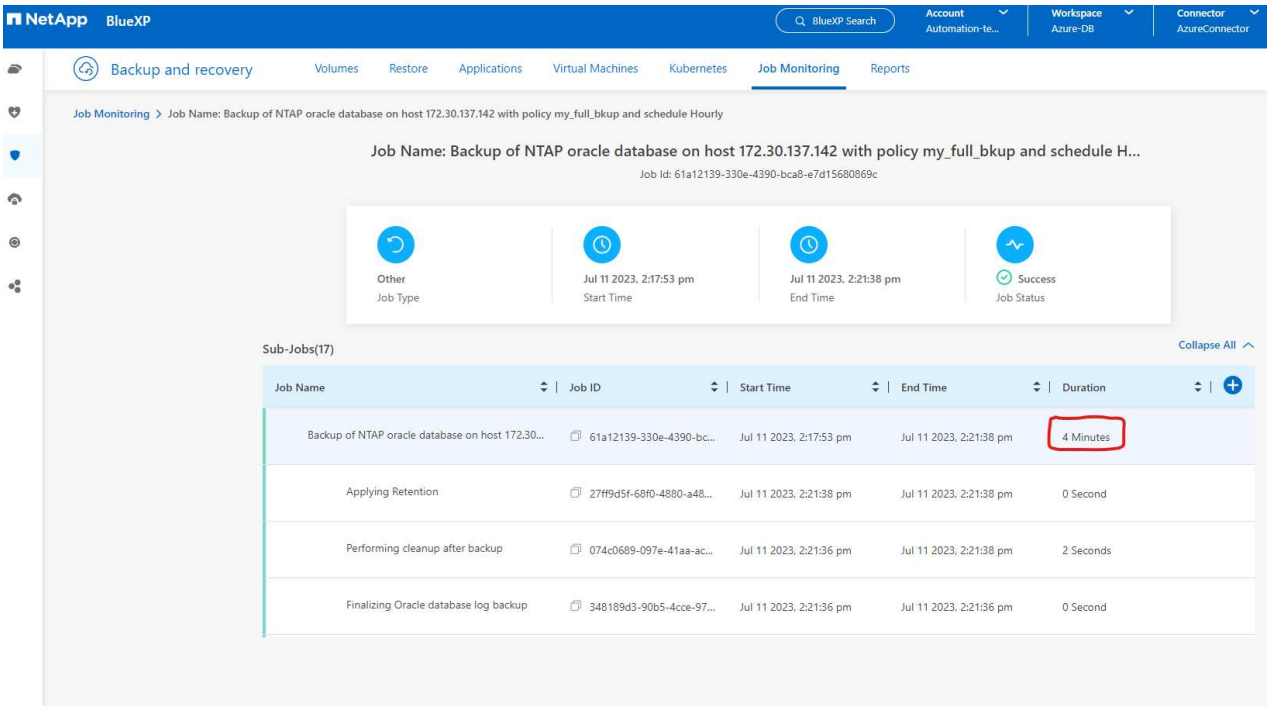
2. Lorsque vous êtes satisfait de la configuration de la stratégie, vous pouvez **affecter** la stratégie de votre choix pour protéger la base de données.



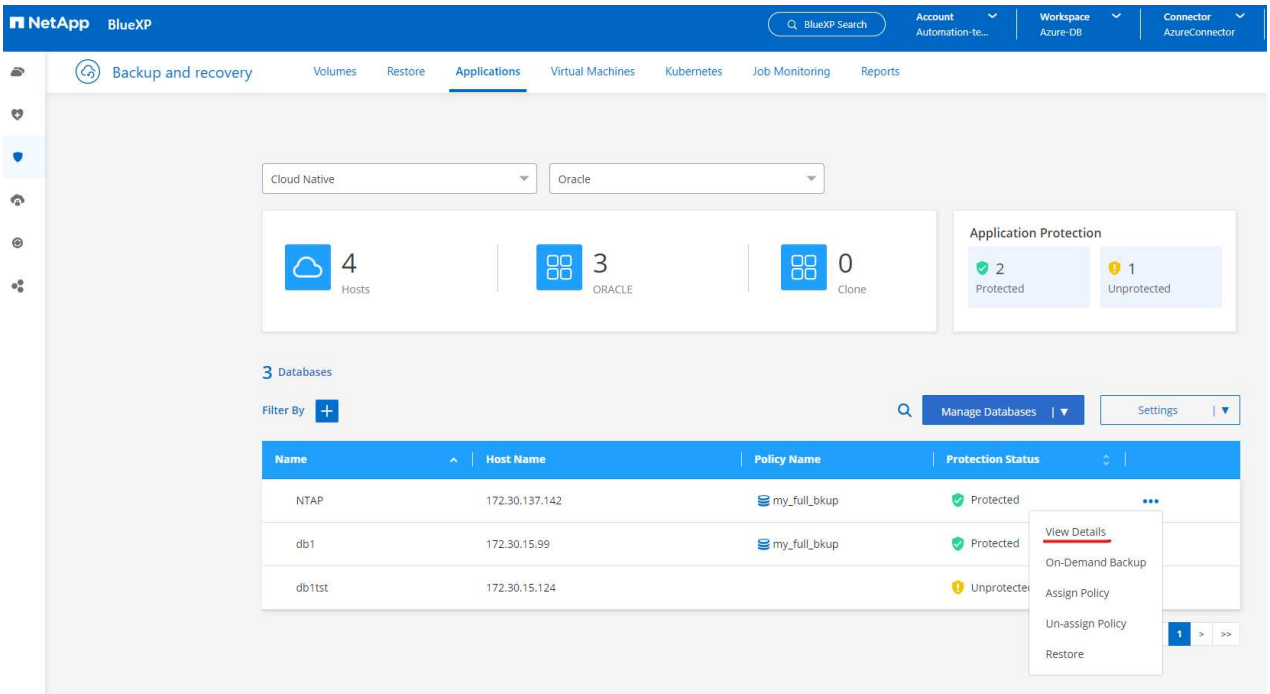
3. Une fois la règle appliquée, l'état de protection de la base de données passe à **protégé** avec une coche verte. BlueXP exécute la sauvegarde Snapshot conformément au calendrier défini. De plus, **ON-Demand Backup** est disponible dans le menu déroulant à trois points, comme illustré ci-dessous.



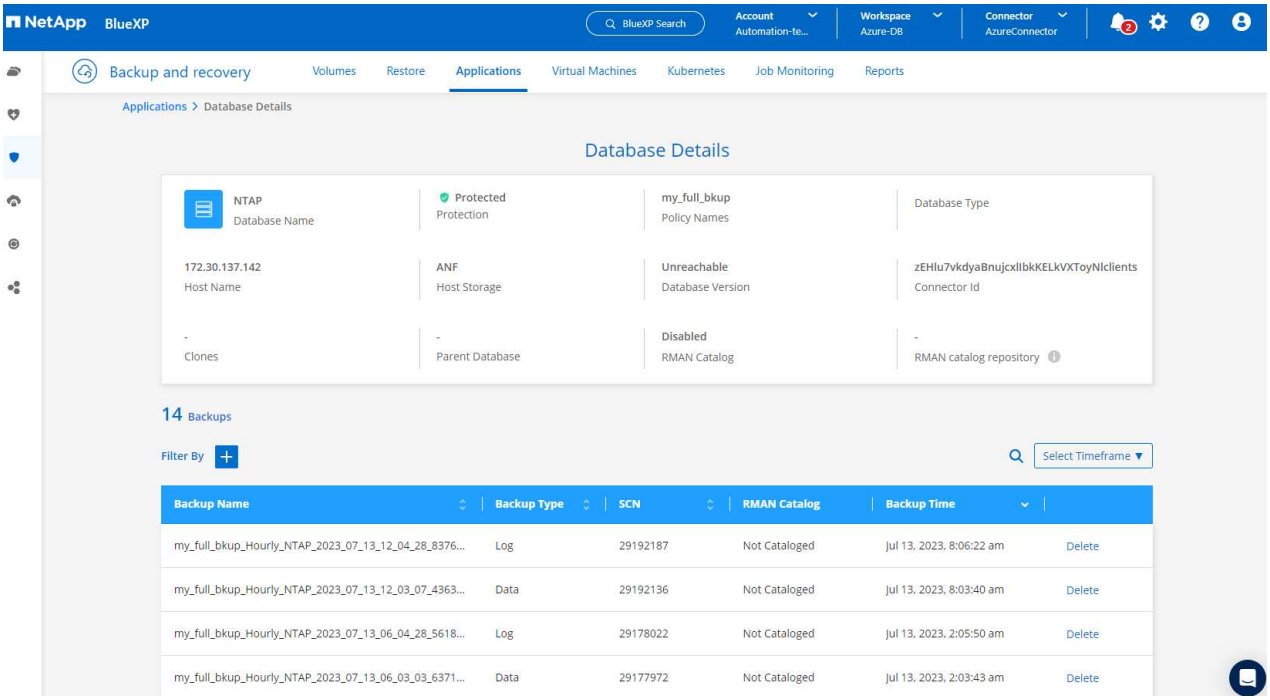
4. Dans l'onglet **Job Monitoring**, les détails de la tâche de sauvegarde peuvent être affichés. D'après les résultats de nos tests, la sauvegarde d'une base de données Oracle a pris environ 4 minutes, soit environ 1.6 Tio.



5. Dans le menu déroulant à trois points **Afficher les détails**, vous pouvez afficher les jeux de sauvegarde créés à partir de la sauvegarde de snapshot.

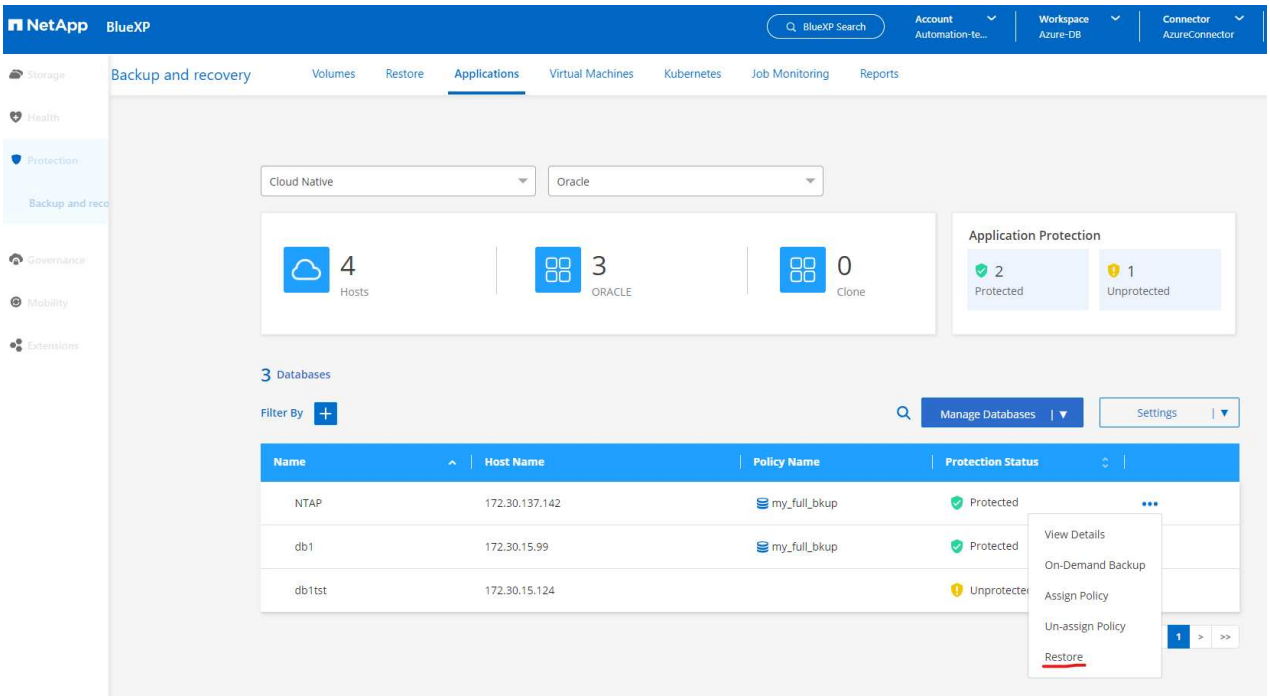


6. Les détails de la sauvegarde de la base de données incluent **Nom de la sauvegarde**, **Type de sauvegarde**, **SCN**, **Catalogue RMAN** et **temps de sauvegarde**. Un jeu de sauvegarde contient respectivement des snapshots cohérents au niveau des applications pour le volume de données et le volume de journal. Un snapshot de volume de journaux a lieu juste après un snapshot de volume de données de base de données. Vous pouvez appliquer un filtre si vous recherchez une sauvegarde particulière dans la liste de sauvegarde.

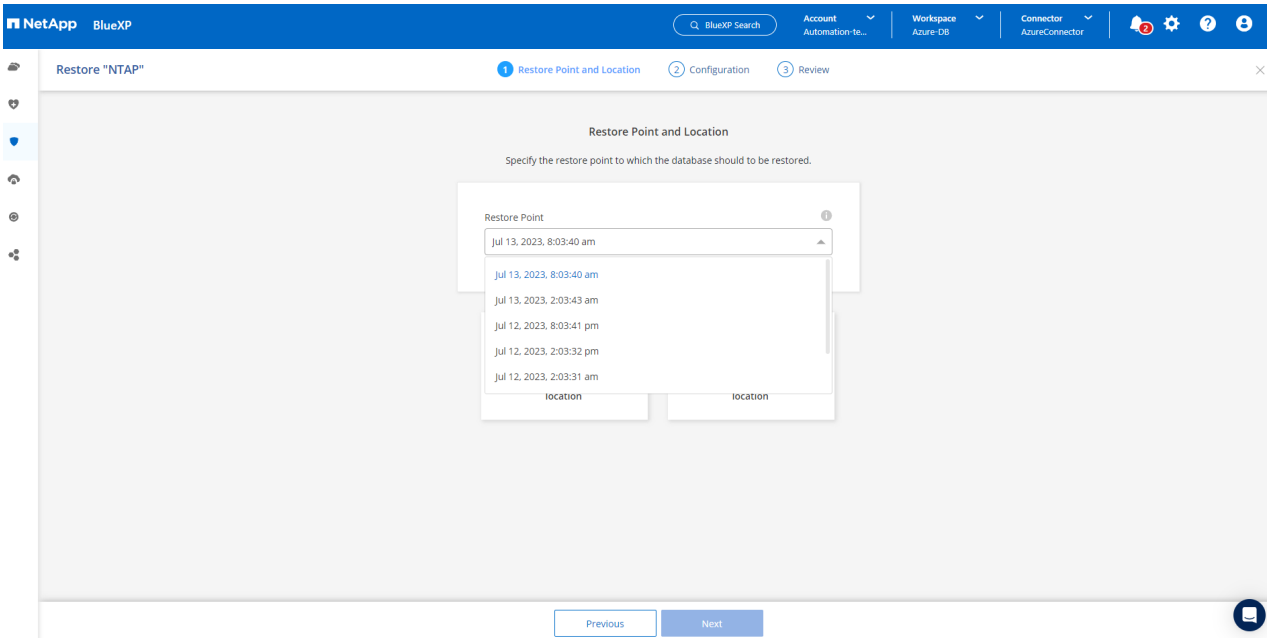


Restauration et récupération de la base de données Oracle

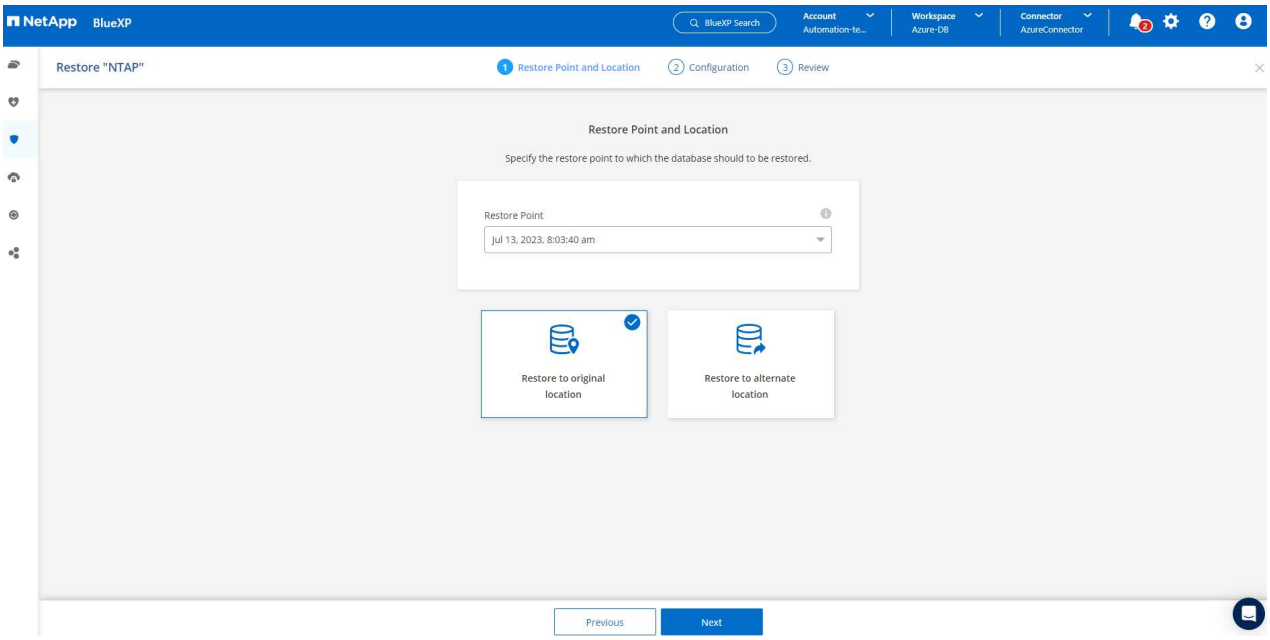
1. Pour une restauration de base de données, cliquez sur le menu déroulant à trois points de la base de données à restaurer dans **applications**, puis cliquez sur **Restaurer** pour lancer le workflow de restauration et de récupération de la base de données.



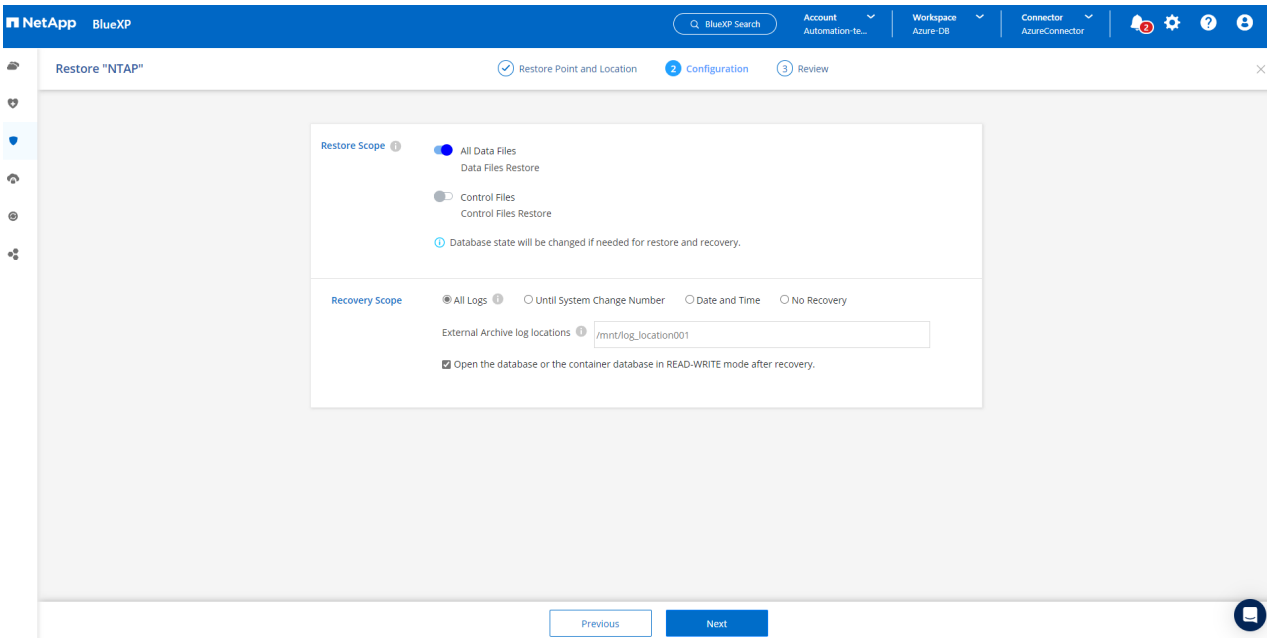
2. Choisissez votre **point de restauration** par horodatage. Chaque horodatage dans la liste représente un jeu de sauvegarde de base de données disponible.



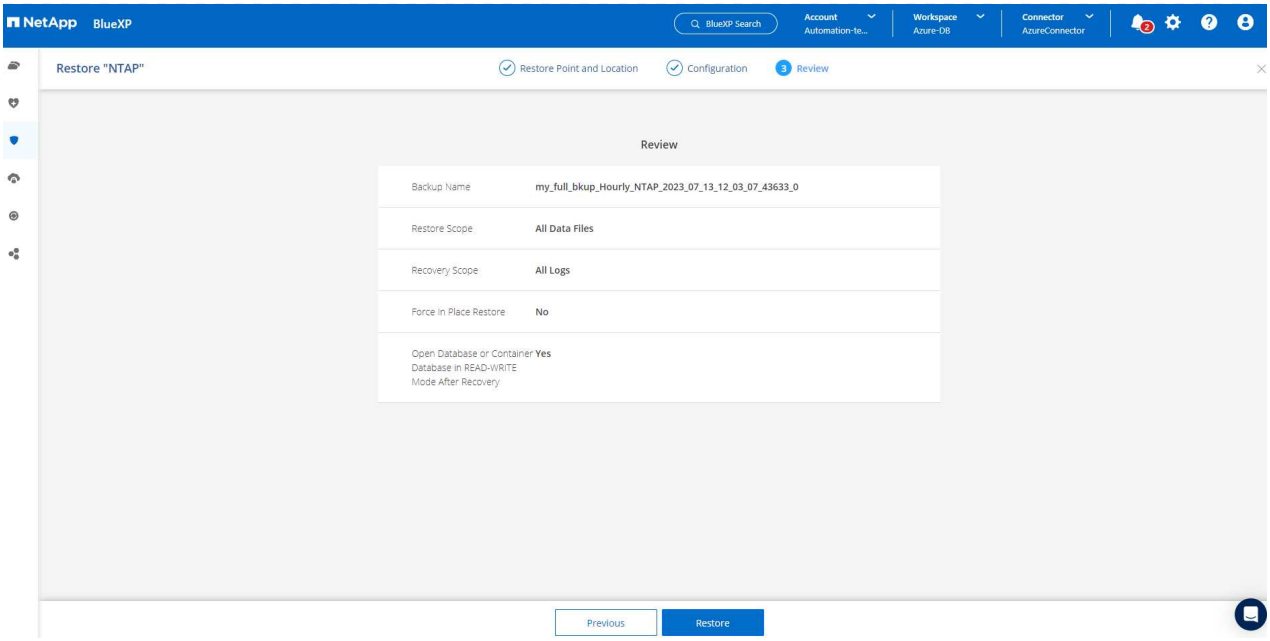
3. Choisissez votre **emplacement de restauration** à **emplacement d'origine** pour une restauration et une récupération de base de données Oracle sur place.



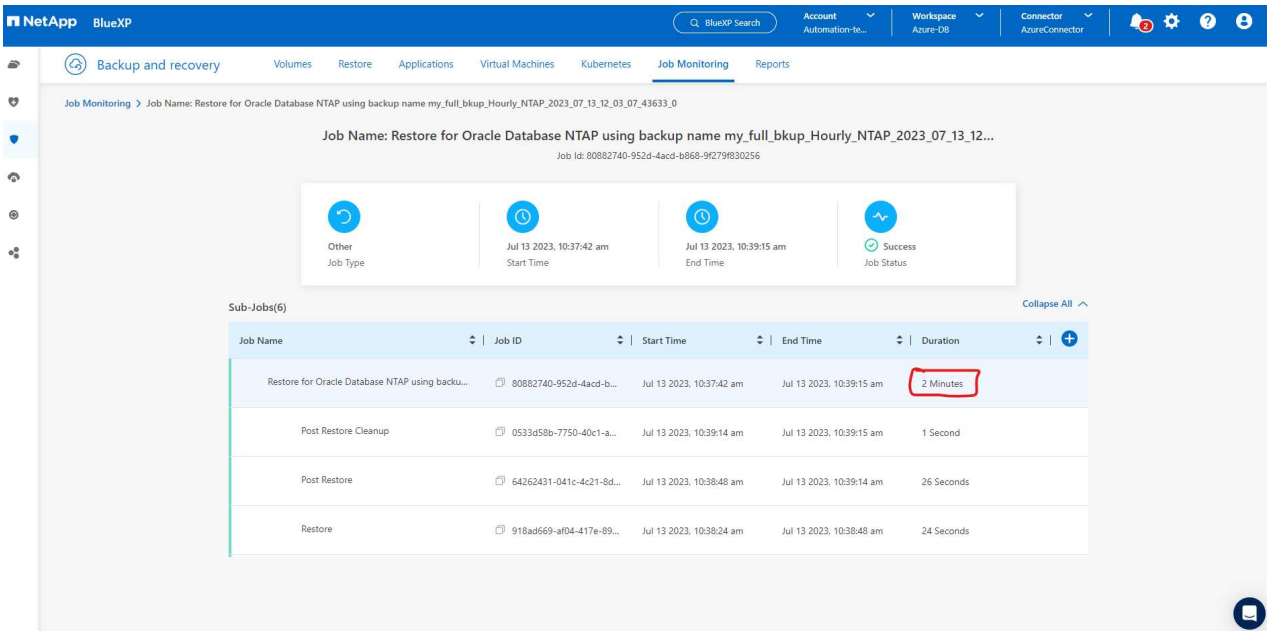
4. Définissez votre **domaine de restauration** et votre **étendue de récupération**. Tous les journaux signifient une restauration complète à jour, y compris les journaux actuels.



5. Consultez et **Restore** pour démarrer la restauration et la récupération de la base de données.



6. Dans l'onglet **Job Monitoring**, nous avons constaté qu'il fallait 2 minutes pour exécuter une restauration complète de la base de données et une restauration à jour.

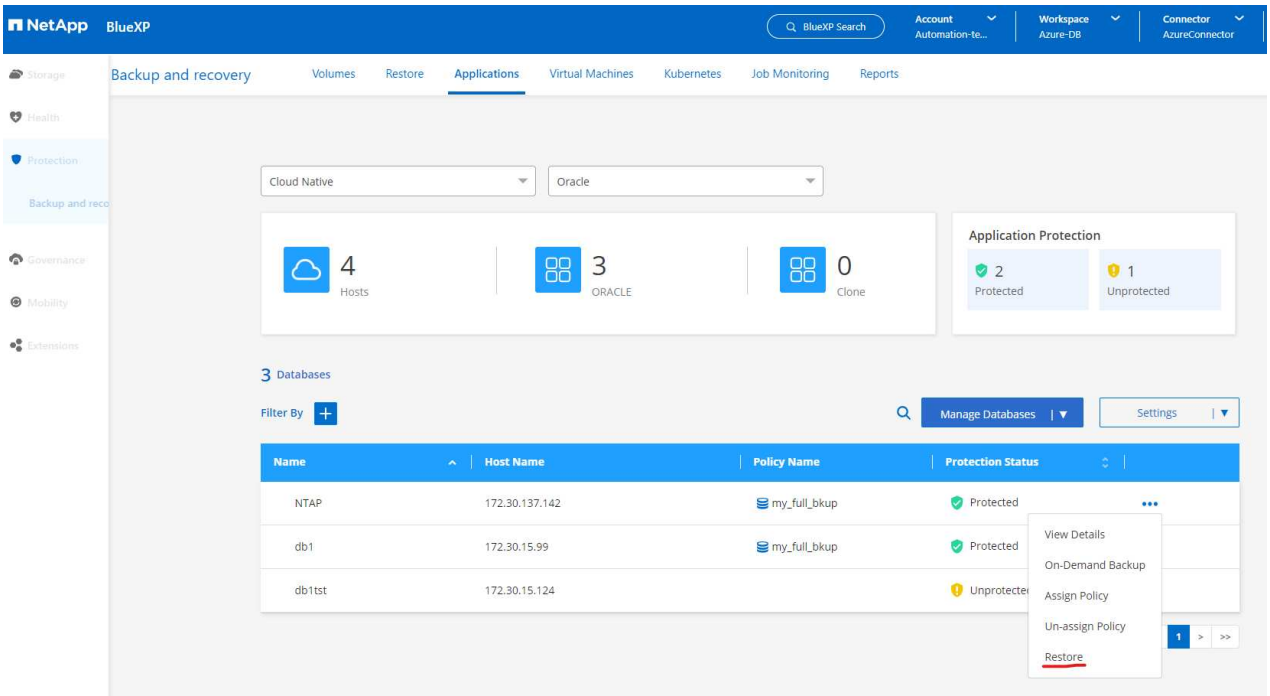


Clone de la base de données Oracle

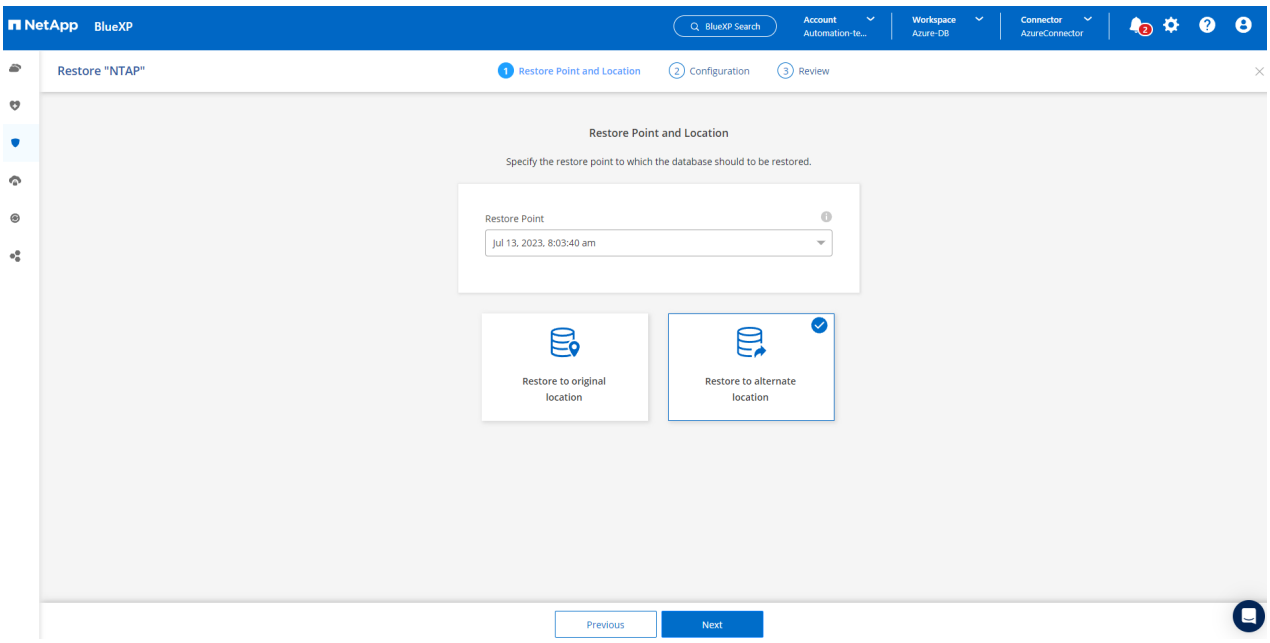
Les procédures de clonage de base de données sont similaires à la restauration, mais sur une autre machine virtuelle Azure avec une pile logicielle Oracle identique préinstallée et configurée.

> Assurez-vous que votre stockage de fichiers Azure NetApp dispose de suffisamment de capacité pour qu'une base de données clonée soit de la même taille que la base de données primaire à cloner. La machine virtuelle Azure secondaire a été ajoutée à **applications**.

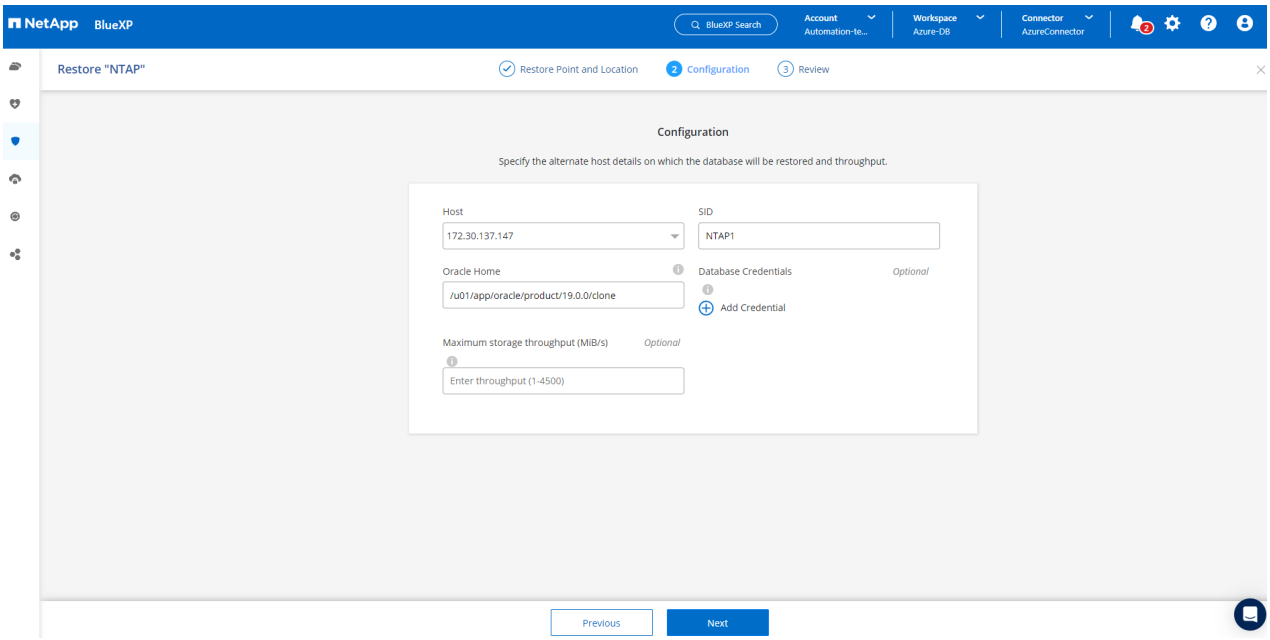
1. Cliquez sur le menu déroulant à trois points de la base de données à cloner dans **applications**, puis cliquez sur **Restaurer** pour lancer le flux de travail de clonage.



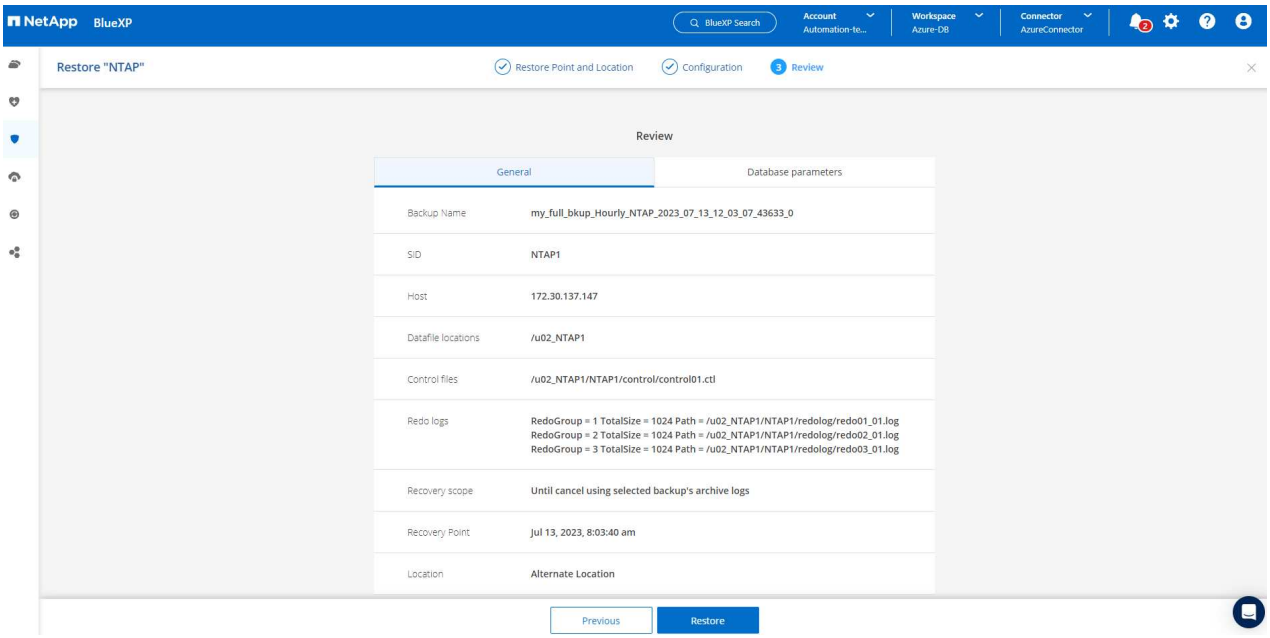
2. Sélectionnez le **point de restauration** et cochez la **Restaurer à un autre emplacement**.



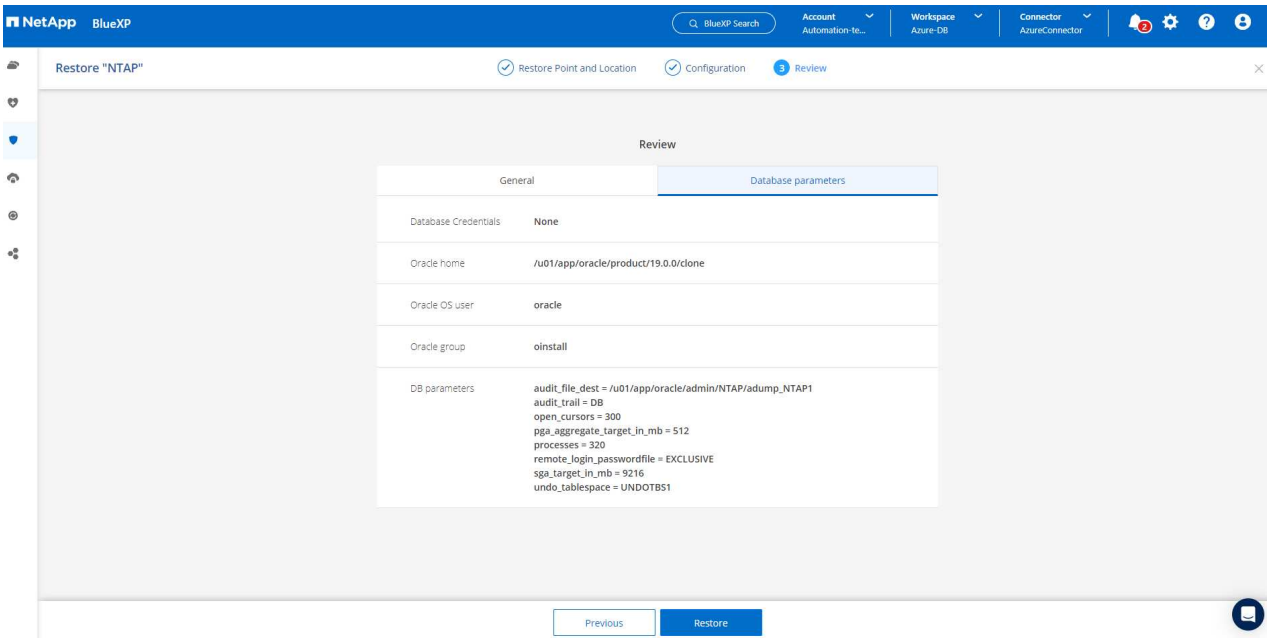
3. Dans la page **Configuration** suivante, définissez autre **hôte**, nouvelle base de données **SID** et **Oracle Home** comme configuré sur une autre machine virtuelle Azure.



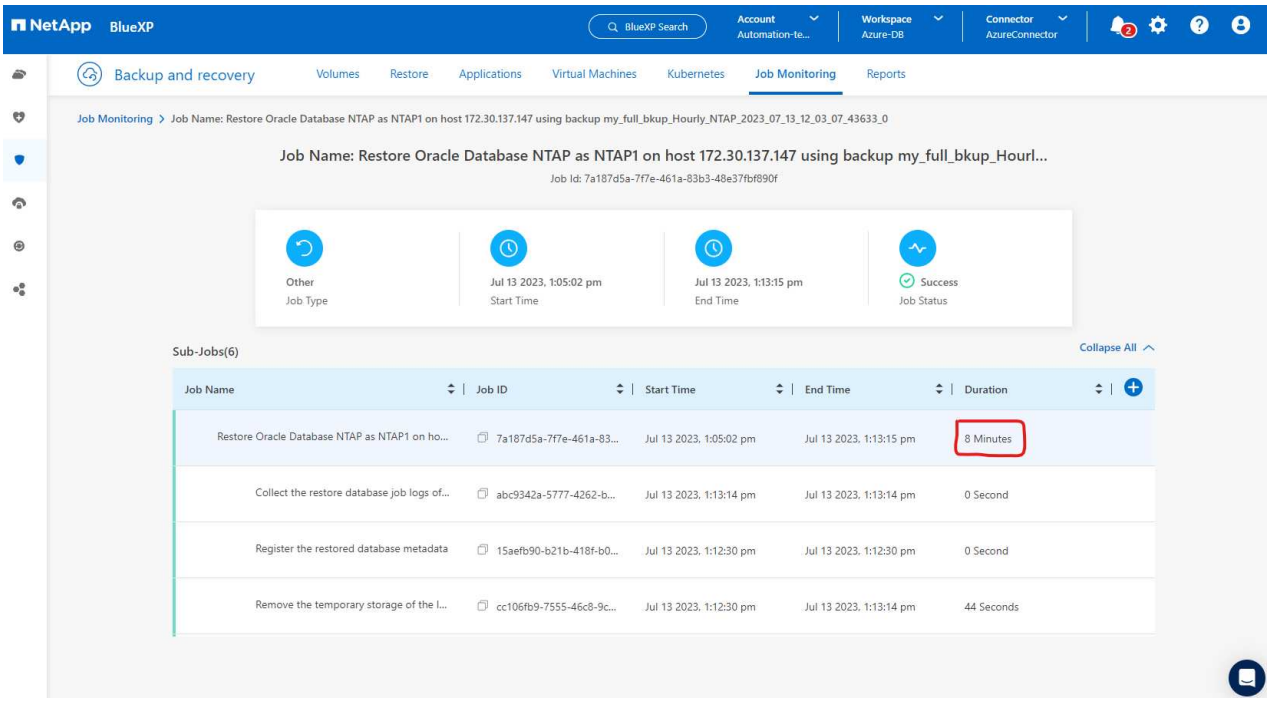
4. La page consulter **général** affiche les détails de la base de données clonée, tels que SID, hôte secondaire, emplacements des fichiers de données, étendue de récupération, etc



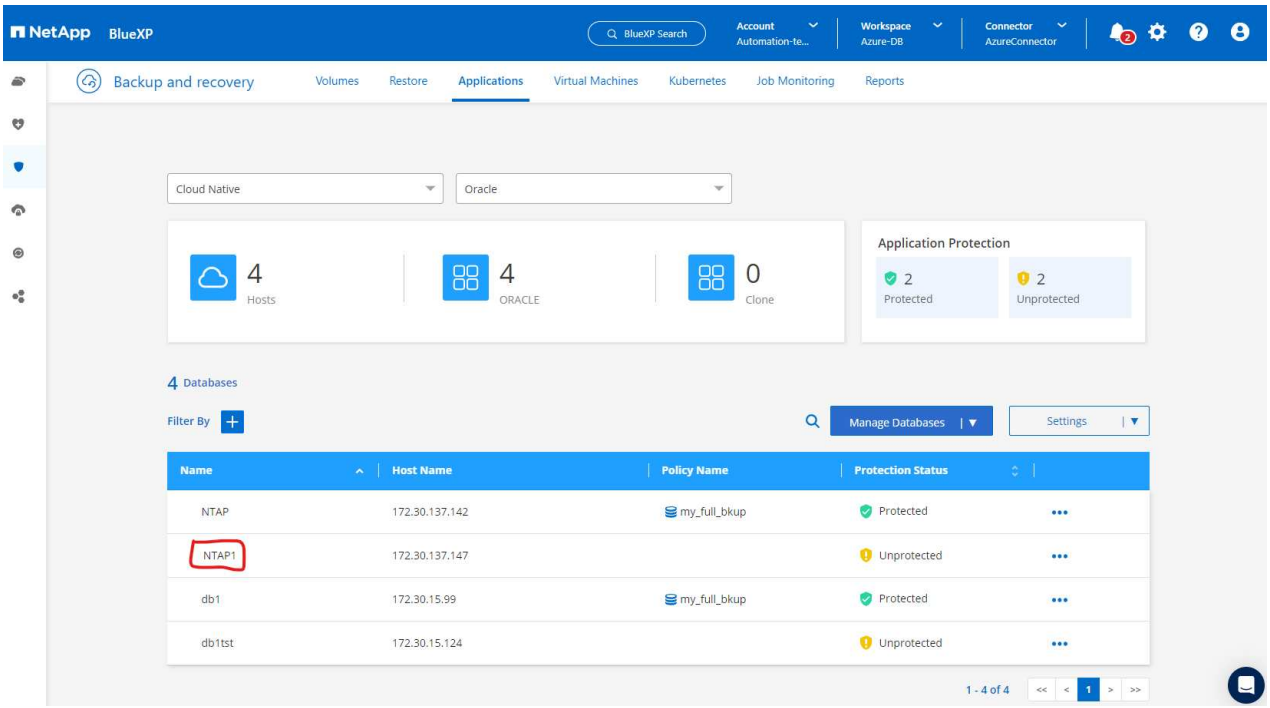
5. Page Review **Database parameters** affiche les détails de la configuration de base de données clonée ainsi que certains paramètres de base de données.



6. Surveillez l'état des tâches de clonage à partir de l'onglet **Job Monitoring**, nous avons constaté qu'il fallait 8 minutes pour cloner une base de données Oracle de 1.6 Tio.



7. Validez la base de données clonée sur la page BlueXP **applications** qui indique que la base de données clonée a été immédiatement enregistrée avec BlueXP.



8. Validez la base de données clonée sur la machine virtuelle Oracle Azure qui indique que la base de données clonée s'exécutait 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
```

Cette étape complète la démonstration de la sauvegarde, de la restauration et du clonage d'une base de données Oracle dans Azure avec la console NetApp BlueXP via le service SnapCenter.

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Configuration et administration de BlueXP

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

- Documentation sur la sauvegarde et la restauration BlueXP

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

- Azure NetApp Files

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

- Commencez avec Azure

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

Tr-4964 : sauvegarde, restauration et clonage des bases de données Oracle avec les services SnapCenter - AWS

Allen Cao, Niyaz Mohamed, NetApp

Objectif

Les services SnapCenter sont la version SaaS de l'outil classique de gestion de bases de données SnapCenter disponible via la console de gestion cloud NetApp BlueXP. Il fait partie intégrante de l'offre NetApp de sauvegarde et de protection des données dans le cloud pour les bases de données telles qu'Oracle et HANA s'exécutant sur le stockage cloud NetApp. Ce service SaaS simplifie le déploiement traditionnel de serveurs autonomes SnapCenter qui nécessite généralement un serveur Windows fonctionnant dans un environnement de domaine Windows.

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

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde de bases de données avec des snapshots pour les bases de données Oracle hébergées dans Amazon FSX pour ONTAP
- Restauration de la base de données Oracle en cas de défaillance
- Clonage rapide et efficace des bases de données primaires pour un environnement de développement/test ou d'autres cas d'utilisation

Public

Cette solution est destinée aux publics suivants :

- Administrateur de bases de données qui gère les bases de données Oracle s'exécutant sur Amazon FSX pour le stockage ONTAP
- Architecte de solutions qui souhaite tester la sauvegarde, la restauration et le clonage des bases de données Oracle dans le cloud AWS public
- L'administrateur du stockage qui prend en charge et gère le stockage Amazon FSX pour ONTAP
- Propriétaire des applications qui sont déployées sur le stockage Amazon FSX pour ONTAP

Environnement de test et de validation de la solution

Le test et la validation de cette solution ont été réalisés dans un environnement AWS FSX et EC2 qui ne correspond pas à l'environnement de déploiement final. Pour plus d'informations, reportez-vous à la section [Key Factors for Deployment Consideration].

Architecture

Cette image fournit une vue détaillée de la sauvegarde et de la restauration BlueXP pour les applications de la console BlueXP, notamment l'interface utilisateur, le connecteur et les ressources qu'il gère.

Composants matériels et logiciels

Matériel

Stockage ONTAP FSX	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/4 vCPU/16 Gbit/s	Deux instances EC2 T2 xlarge EC2, l'une en tant que serveur de base de données principal et l'autre en tant que serveur de base de données clone

Logiciel

Red Hat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Déploiement de l'abonnement Red Hat 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
OPICH Oracle	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, qui permet la connectivité au stockage FSX et à l'instance de calcul EC2.
- **Une politique IAM AWS créée pour SnapCenter Connector.** la règle 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 prérequis avec les détails des autorisations requises au format JSON. La règle doit être attribuée au compte utilisateur AWS propriétaire du connecteur.
- **La clé d'accès du 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.
- **Une information d'identification a été ajoutée au paramètre de la console BlueXP.** pour ajouter

Amazon FSX pour ONTAP à l'environnement de travail BlueXP, une information d'identification qui accorde des autorisations BlueXP pour accéder à Amazon FSX pour ONTAP est configurée dans le paramètre 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 Java version 11. Il doit être installé sur l'hôte d'application avant la tentative de déploiement du plug-in.

Déploiement de la solution

La documentation NetApp étendue offre une portée plus large pour vous aider à protéger les données de vos applications cloud natives. L'objectif de cette documentation est de fournir des procédures détaillées qui couvrent le déploiement des services SnapCenter avec la console BlueXP pour protéger votre base de données Oracle déployée dans Amazon FSX pour ONTAP et une instance de calcul EC2. Ce document contient certains détails qui peuvent être manquants dans des instructions plus générales.

Pour commencer, procédez comme suit :

- Lisez les instructions générales "Protégez vos données applicatives cloud natives" Et les sections relatives à Oracle et Amazon FSX pour ONTAP.
- Regardez la vidéo de présentation suivante.

Déploiement de la solution

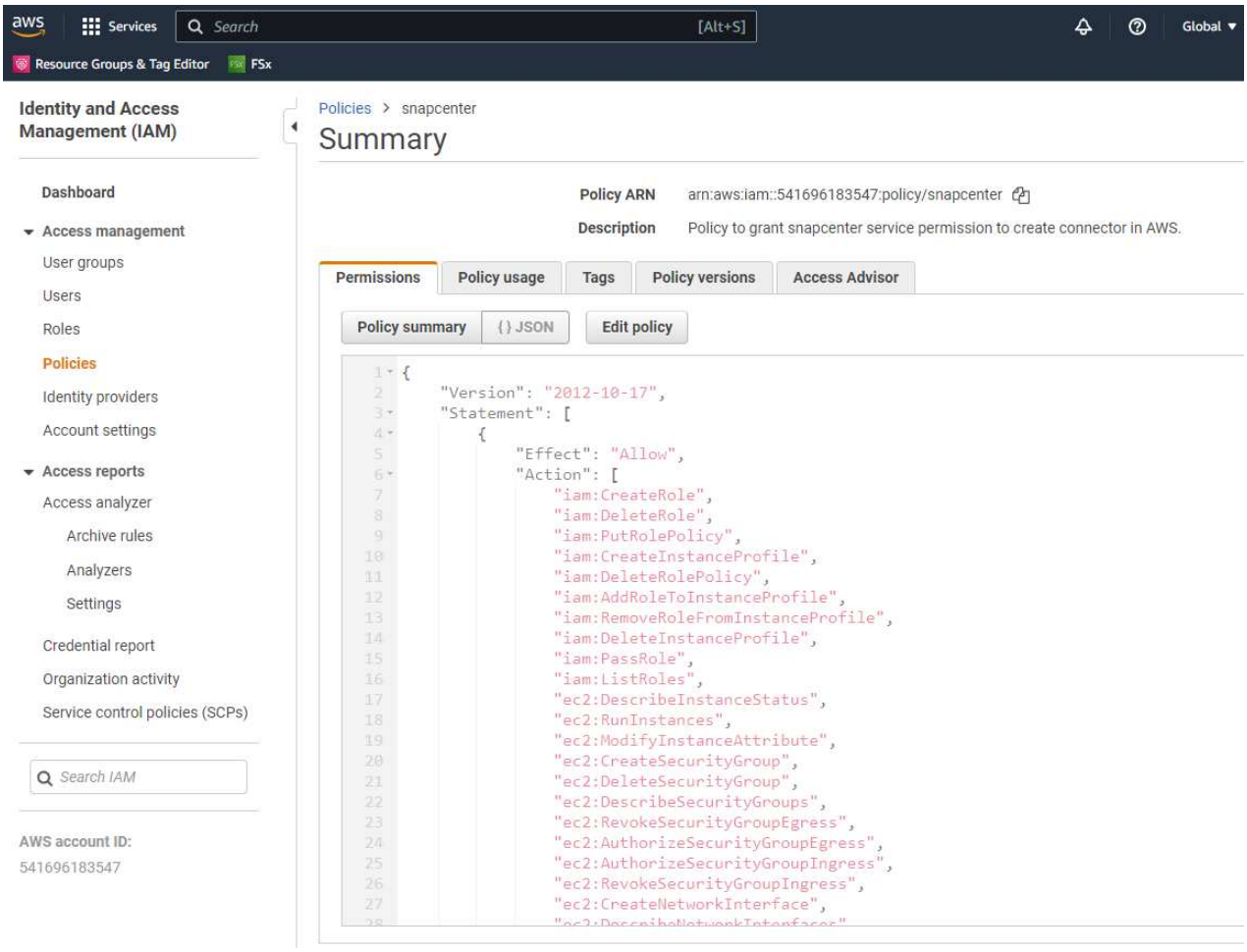
Conditions préalables au déploiement du service SnapCenter

Le déploiement nécessite les conditions préalables suivantes.

1. Serveur de base de données Oracle primaire sur une instance EC2 avec une base de données Oracle entièrement déployée et en cours d'exécution.
2. Cluster Amazon FSX pour ONTAP déployé dans AWS qui héberge les volumes de base de données ci-dessus.
3. Serveur de base de données en option sur une instance EC2 qui peut être utilisé pour tester le clonage d'une base de données Oracle sur un autre hôte afin de prendre en charge une charge de travail de développement/test ou tout cas d'utilisation nécessitant un jeu de données complet d'une base de données Oracle de production.
4. Si vous avez besoin d'aide pour remplir les conditions préalables ci-dessus pour le déploiement de bases de données Oracle sur Amazon FSX pour ONTAP et l'instance de calcul EC2, reportez-vous à la section "Déploiement et protection des bases de données Oracle dans AWS FSX/EC2 avec iSCSI/ASM" ou livre blanc "Déploiement de bases de données Oracle sur EC2 et FSX : bonnes pratiques"

Intégration de la préparation à 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 attribuer la règle au compte AWS qui sera utilisé pour le déploiement du connecteur BlueXP.

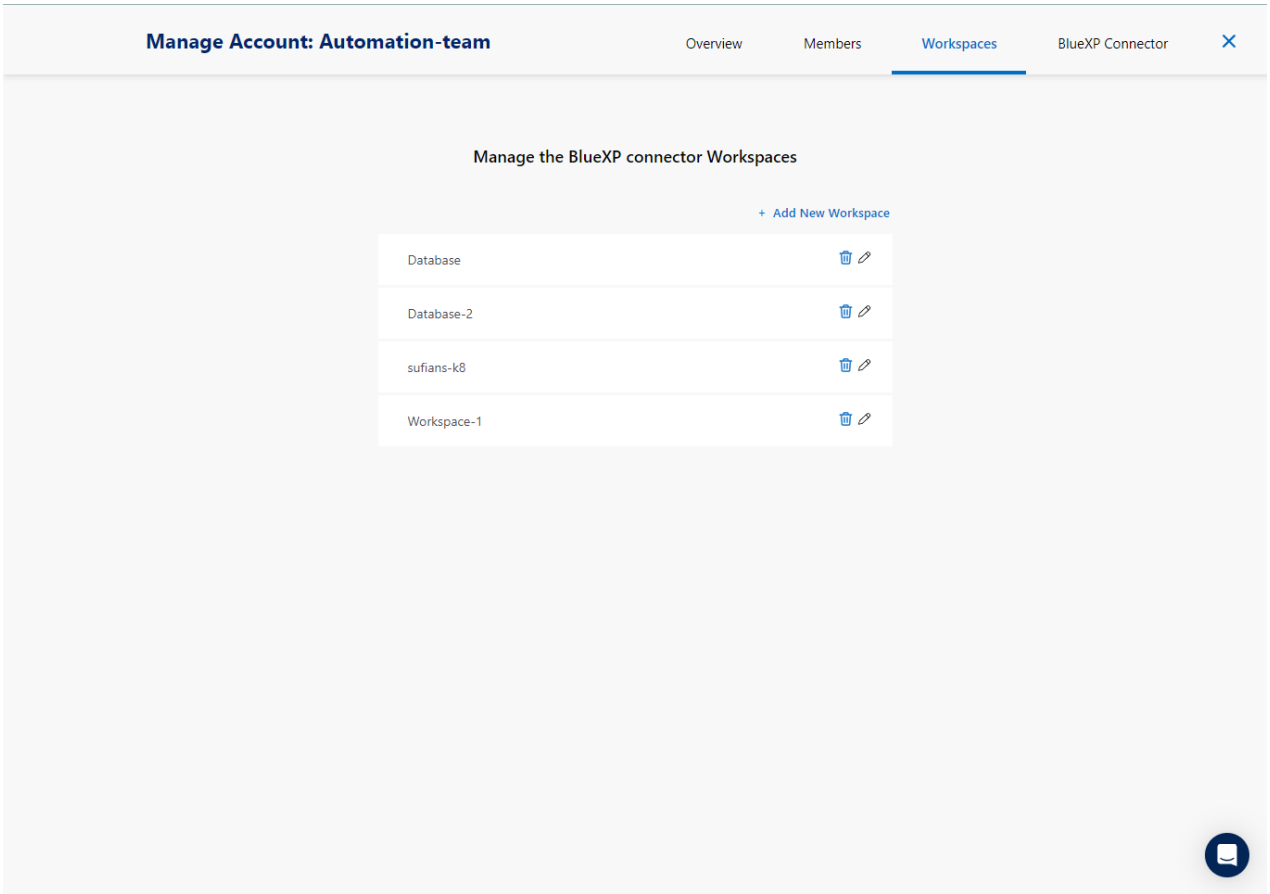


   La règle doit être configurée avec une chaîne JSON disponible dans la documentation de NetApp. La chaîne JSON peut également être extraite de la page lorsque la mise en service du connecteur est lancée et que vous êtes invité à indiquer les autorisations requises.

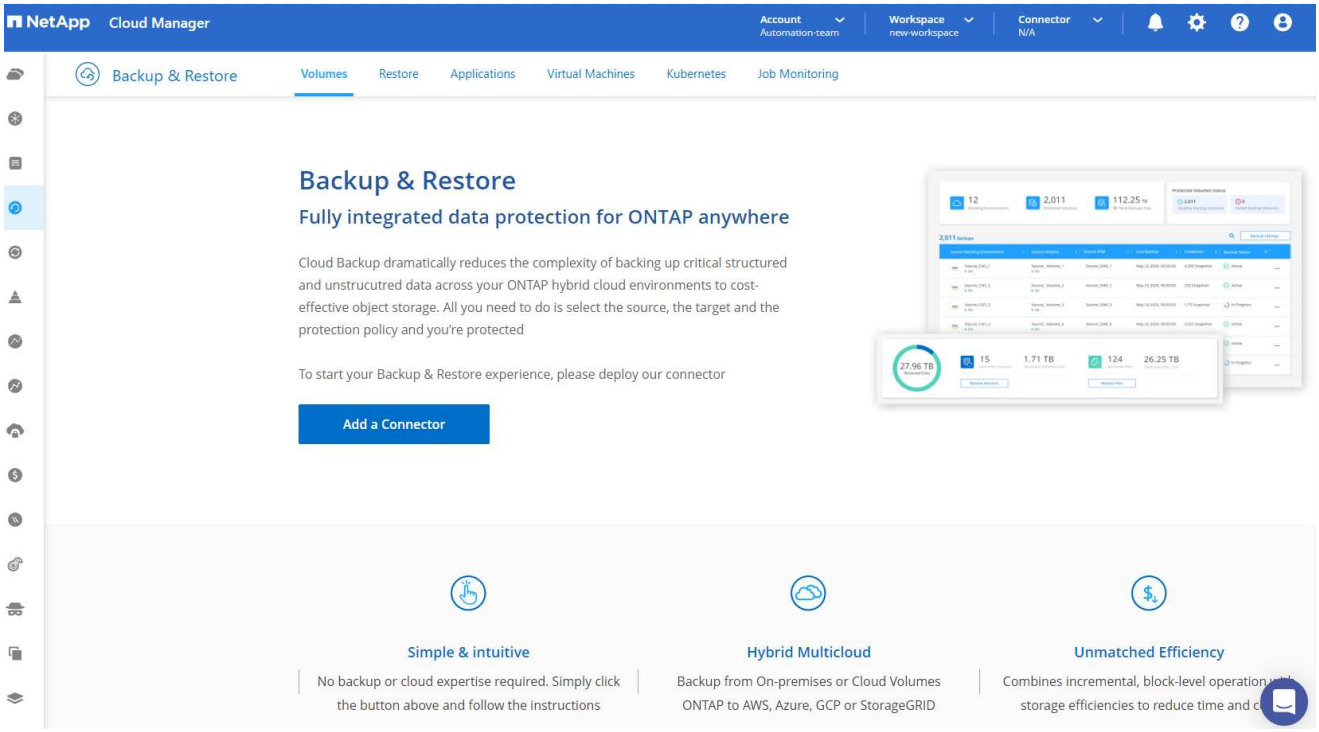
3. Vous avez également besoin du VPC AWS, du sous-réseau, du groupe de sécurité, d'une clé d'accès au compte utilisateur AWS et des secrets, d'une clé SSH pour l'utilisateur ec2, etc. Prêt pour le provisionnement des connecteurs.

Déployez un connecteur pour les services SnapCenter

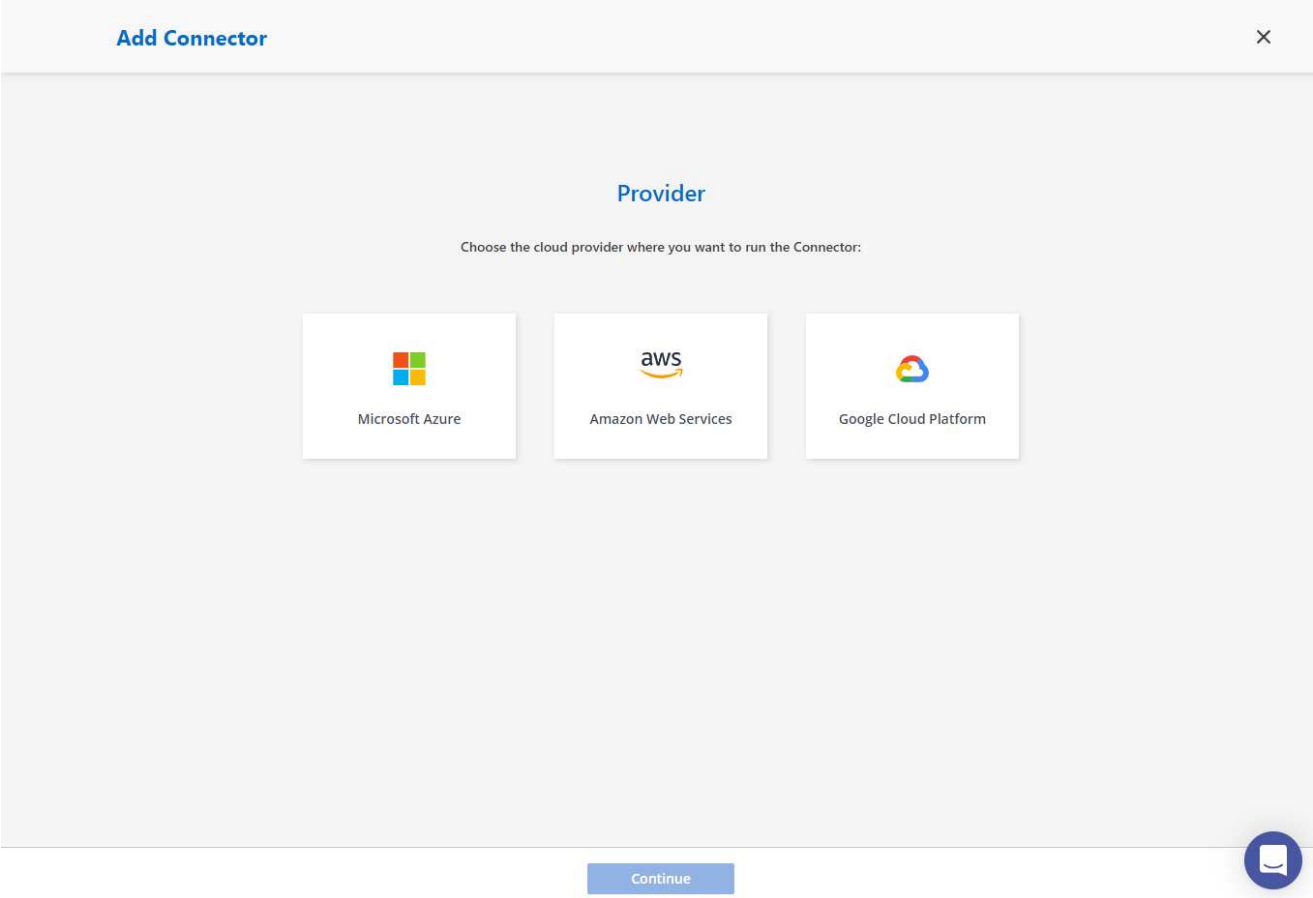
1. Connectez-vous à la console BlueXP. Pour un compte partagé, il est recommandé de créer un espace de travail individuel en cliquant sur **compte** > **gérer le compte** > **espace de travail** pour ajouter un nouvel espace de travail.



2. Cliquez sur **Ajouter un connecteur** pour lancer le flux de production de provisionnement de connecteur.

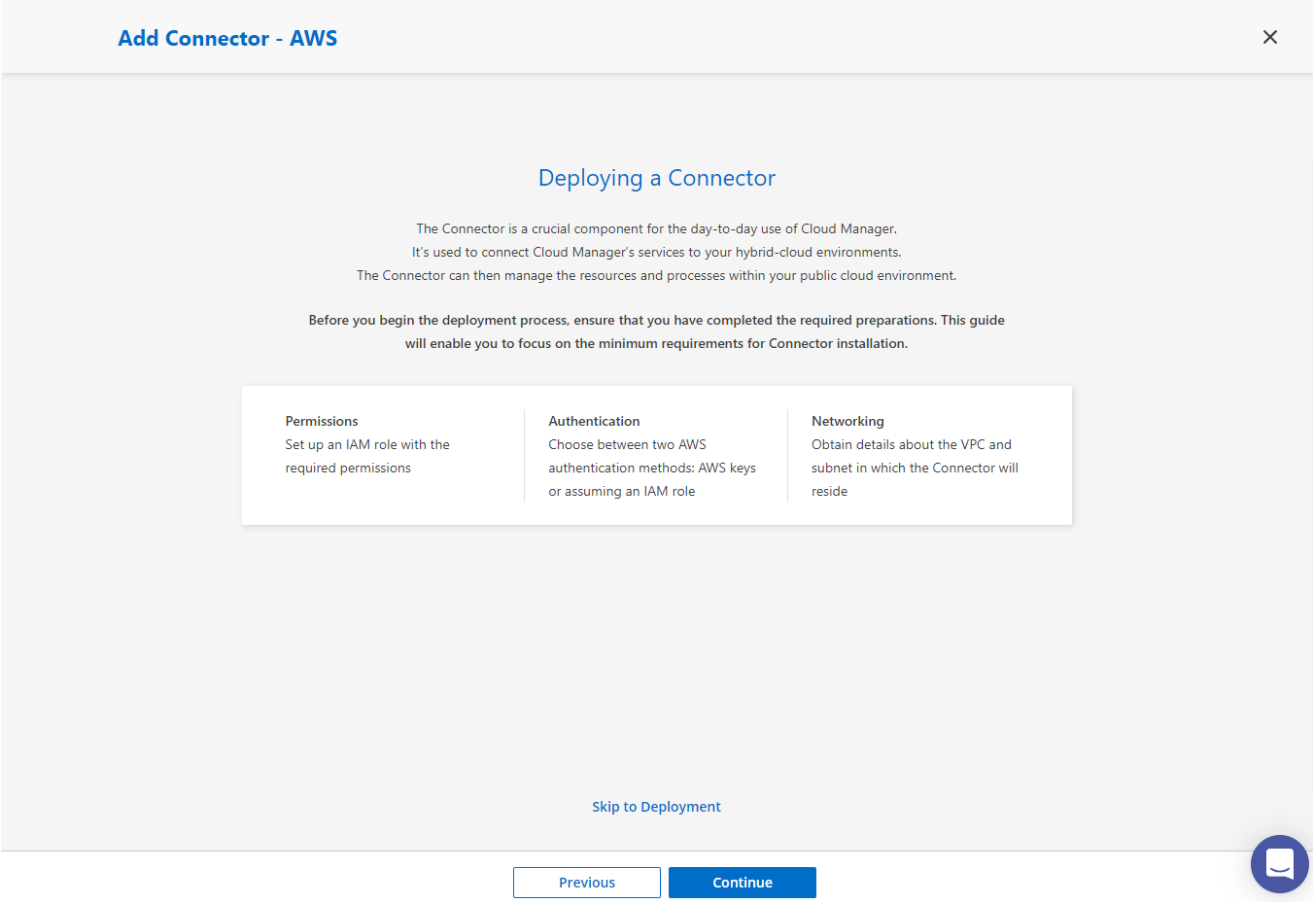


1. Choisissez votre fournisseur de cloud (dans ce cas, **Amazon Web Services**).

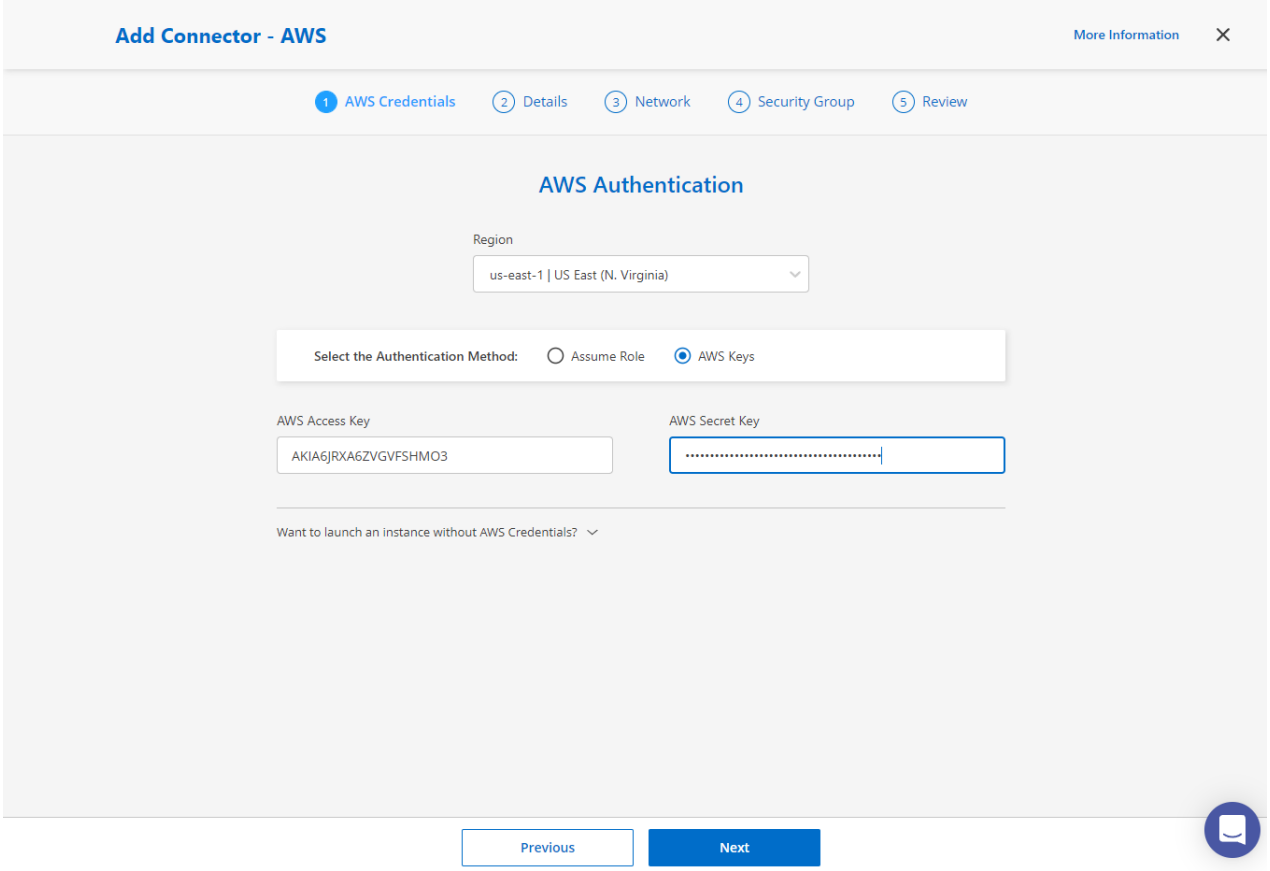


1. Ignorez les étapes **permission**, **authentification** et **mise en réseau** si vous les avez déjà configurées dans votre compte AWS. Si ce n'est pas le cas, vous devez les configurer avant de continuer. À partir de là, vous pouvez également récupérer les autorisations pour la règle AWS

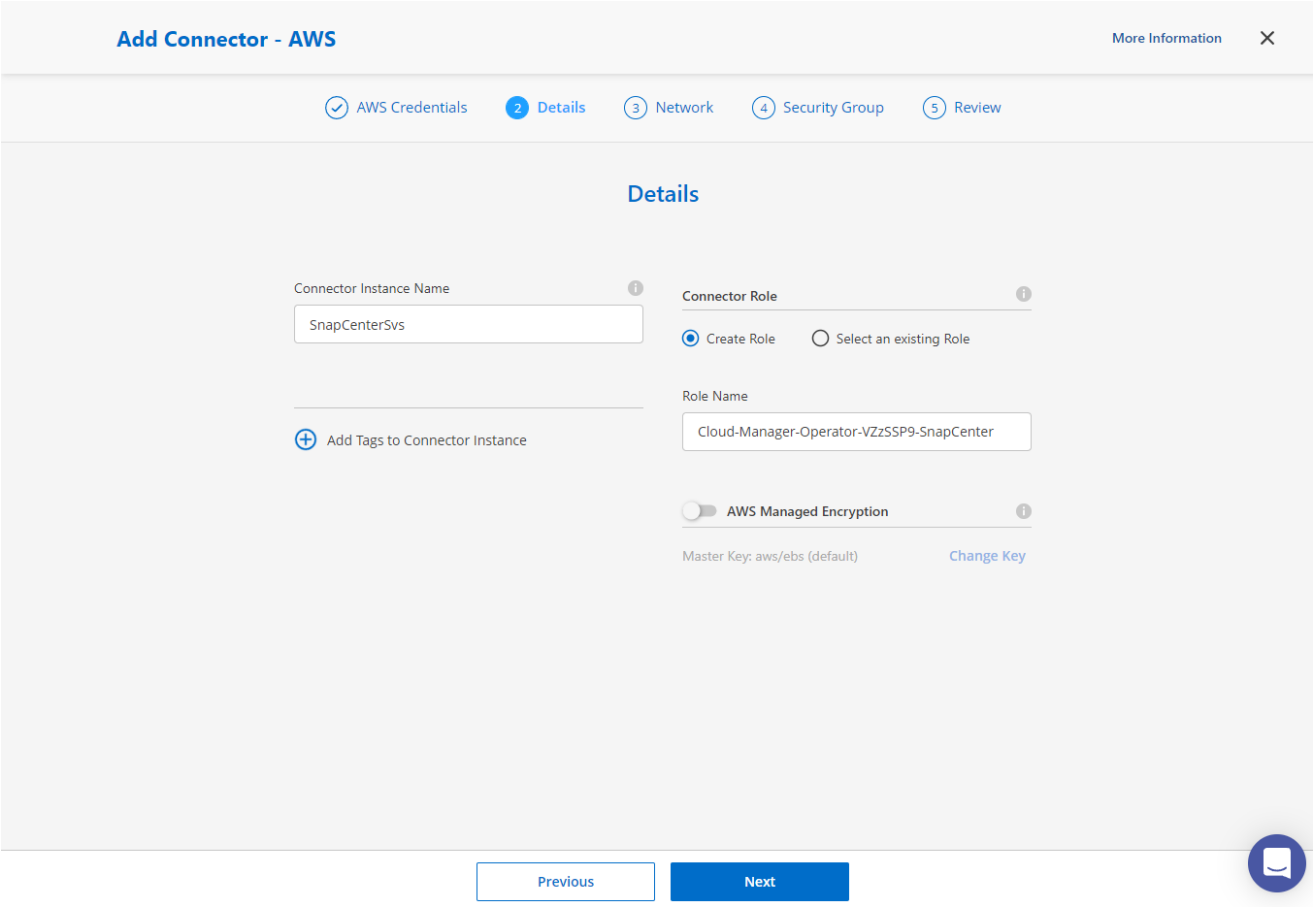
référencée dans la section précédente.Intégration de la préparation à BlueXP."



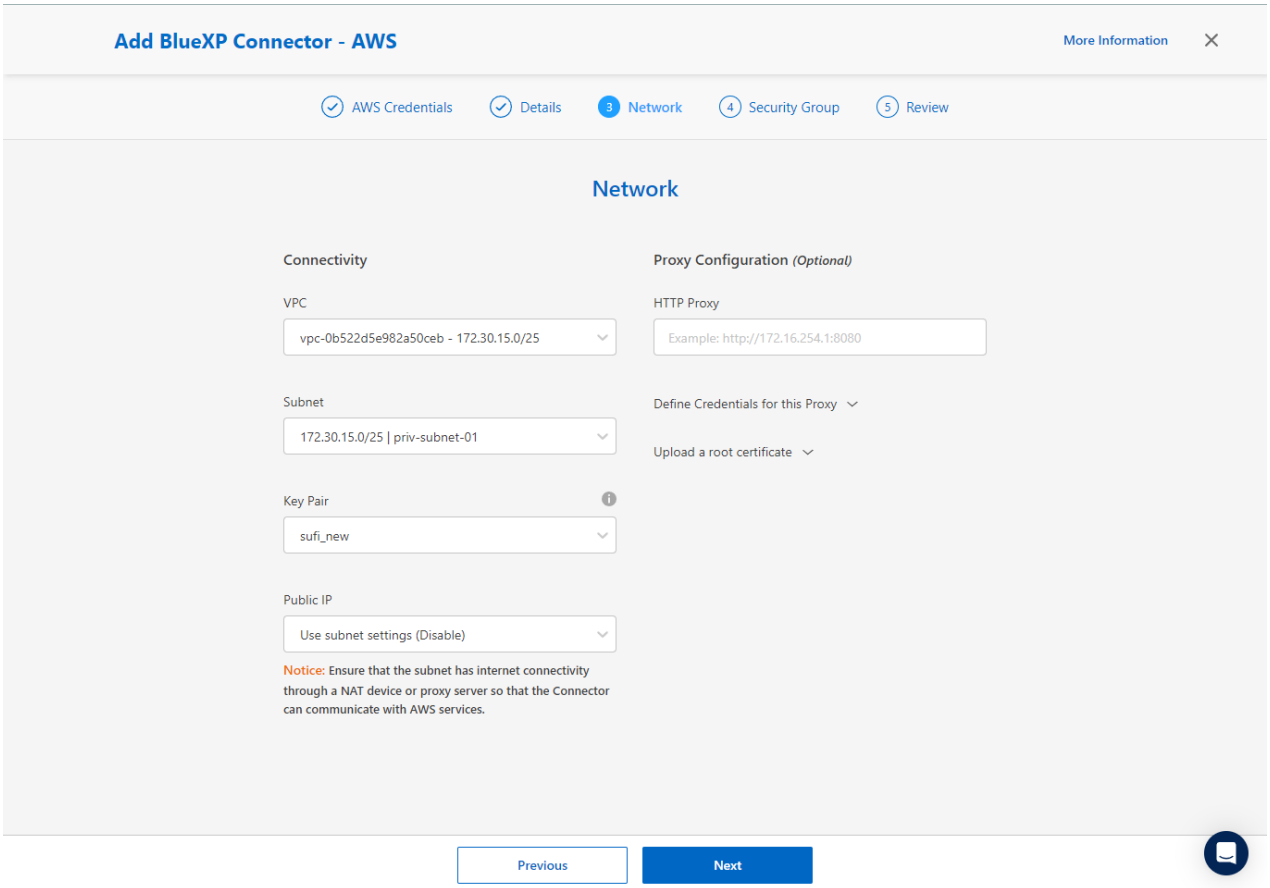
1. Entrez l'authentification de votre compte AWS avec **Access Key** et **Secret Key**.



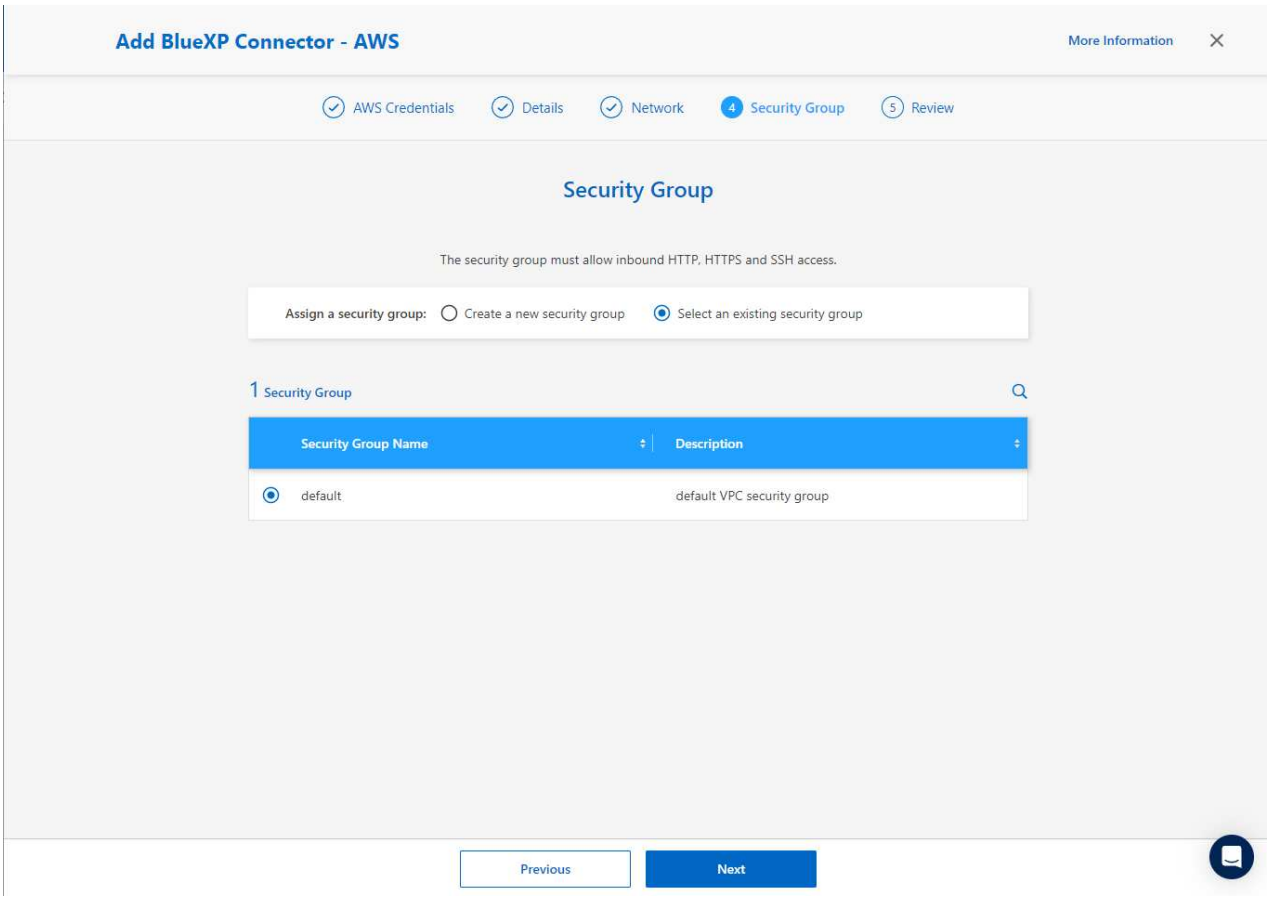
2. Nommez l'instance de connecteur et sélectionnez **Créer un rôle** sous **Détails**.



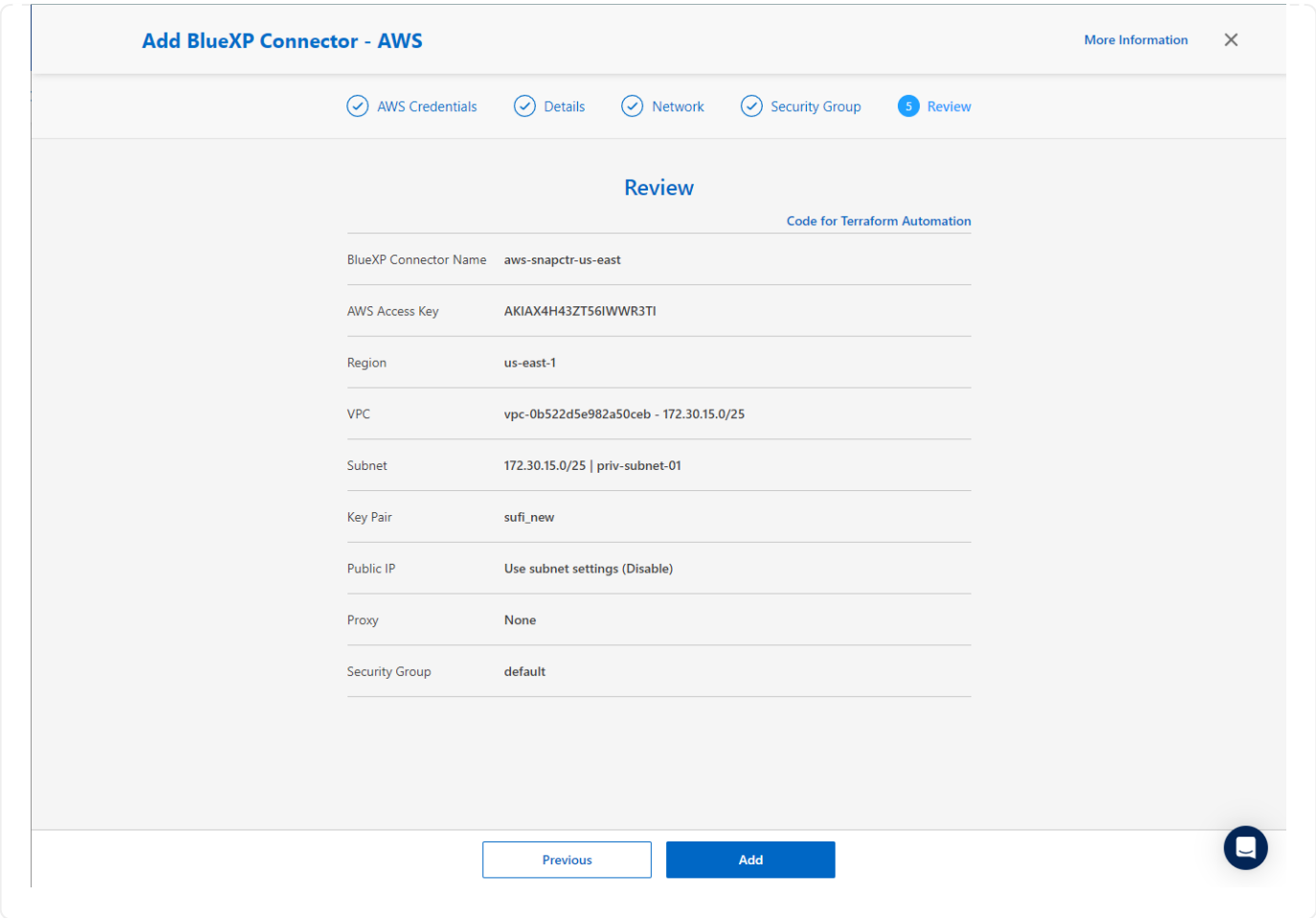
1. Configurez le réseau avec les **VPC**, **Subnet** et SSH **Key pair** appropriés pour l'accès au connecteur.



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

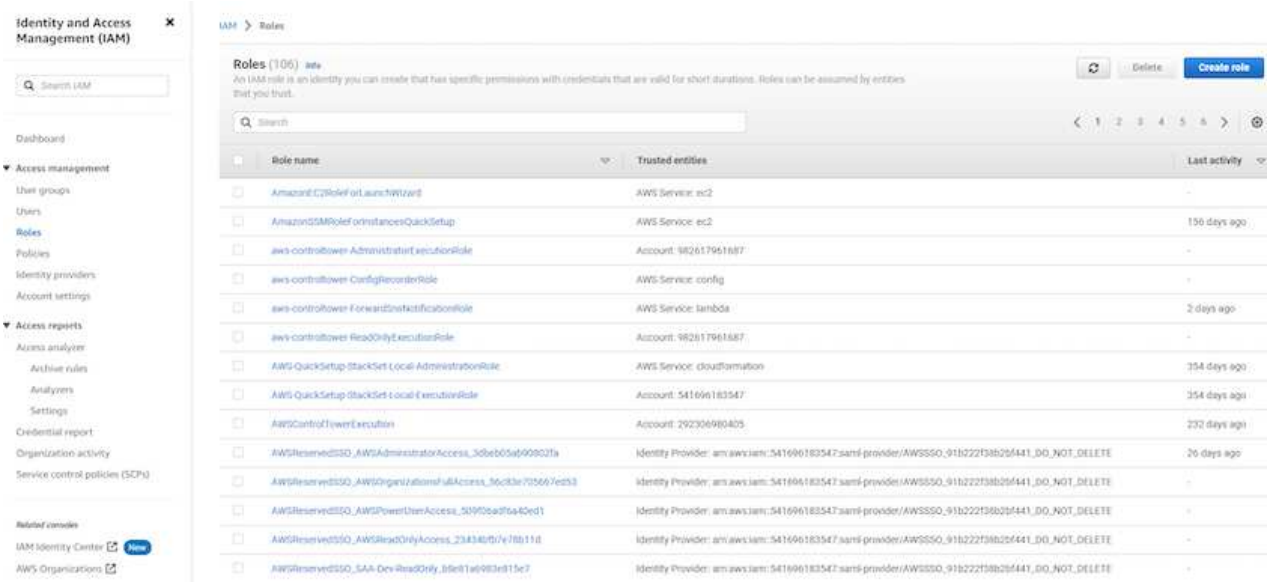


3. Passez en revue la page de résumé et cliquez sur **Ajouter** pour lancer la création du connecteur. Le déploiement prend généralement environ 10 minutes. Une fois la configuration terminée, l'instance de connecteur s'affiche dans le tableau de bord AWS EC2.

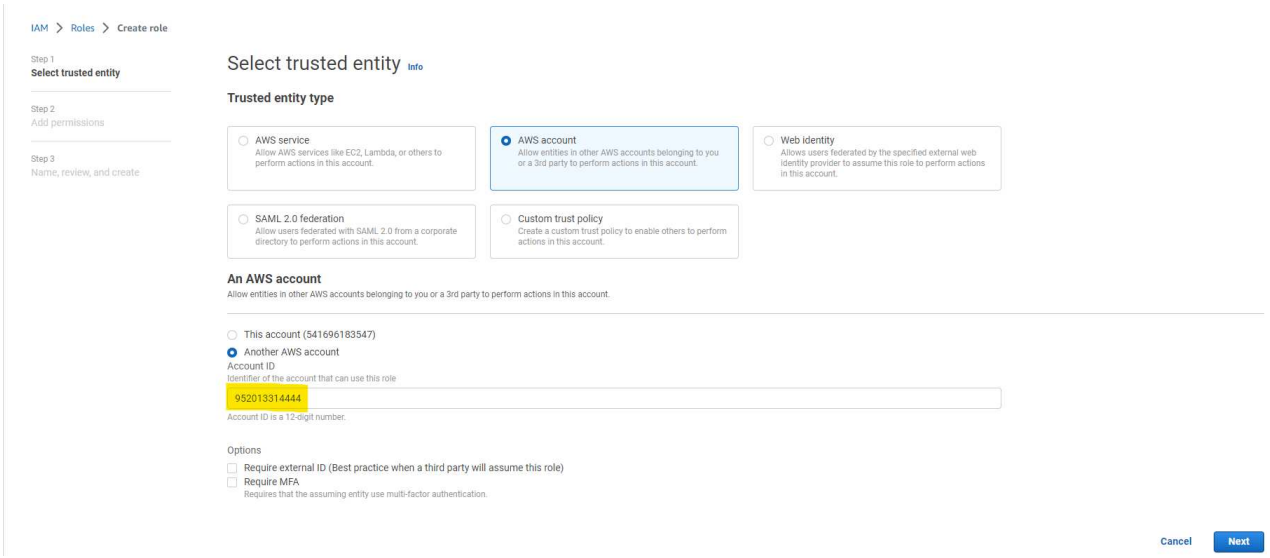


Définissez une référence dans BlueXP pour l'accès aux ressources AWS

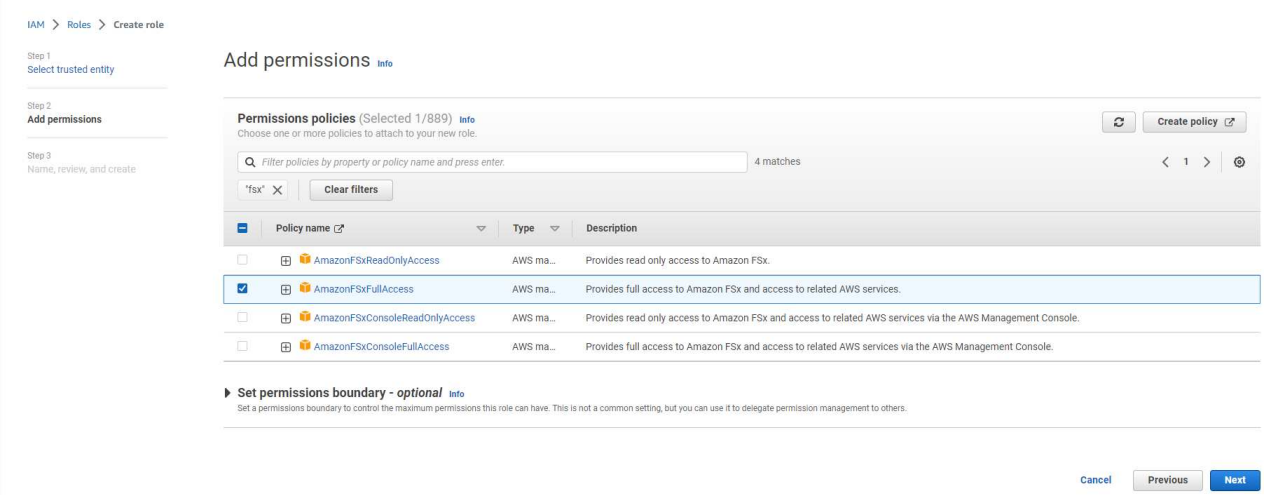
1. Tout d'abord, à partir de la console AWS EC2, créez un rôle dans le menu **Identity and Access Management (IAM) Roles**, **Create role** pour démarrer le workflow de création de rôles.



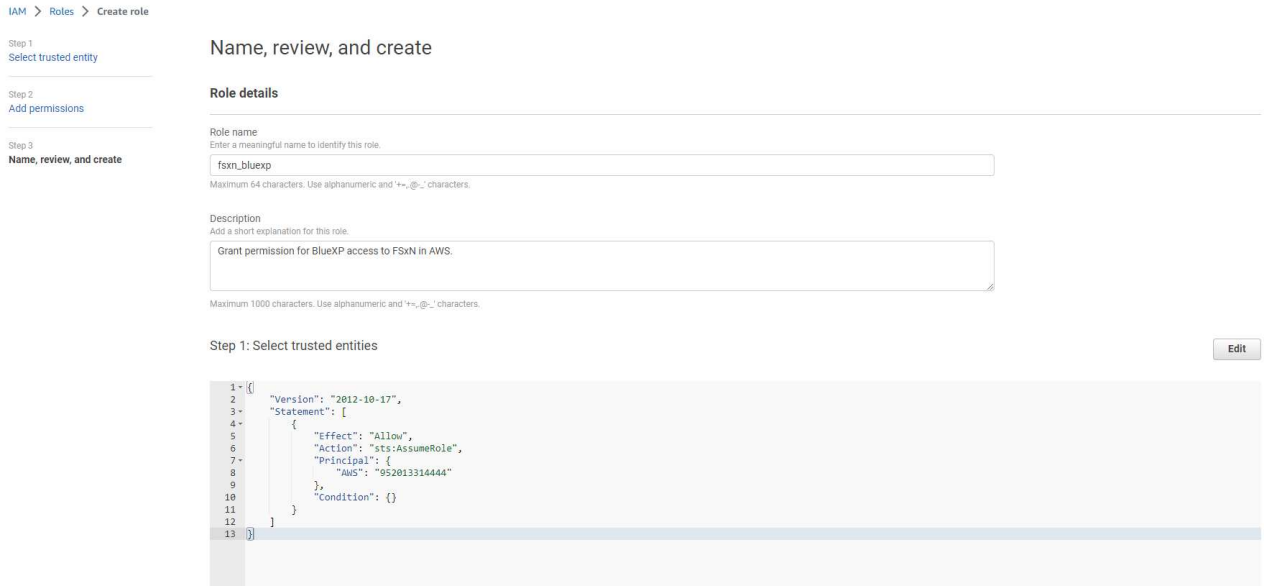
2. Sur la page **Select Trusted entity**, choisissez **AWS account**, **autre compte AWS**, puis collez l'ID de compte BlueXP, qui peut être récupéré depuis la console BlueXP.



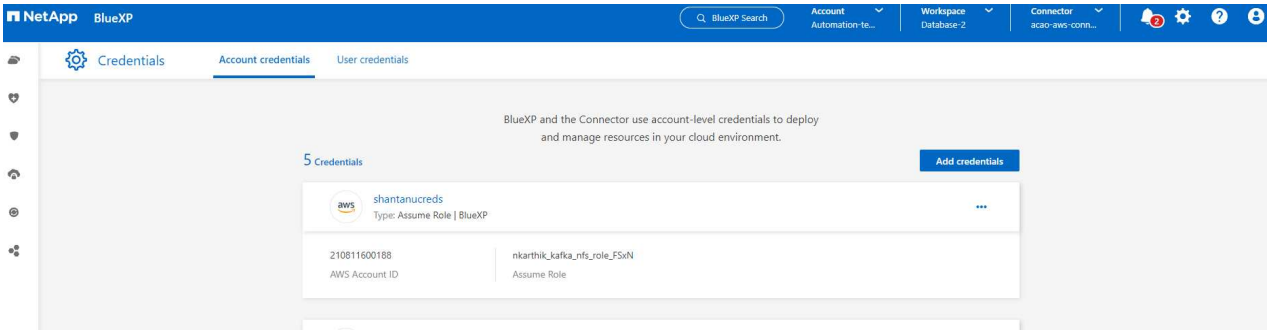
3. Filtrez les stratégies d'autorisation par fsx et ajoutez **stratégies d'autorisations** au rôle.



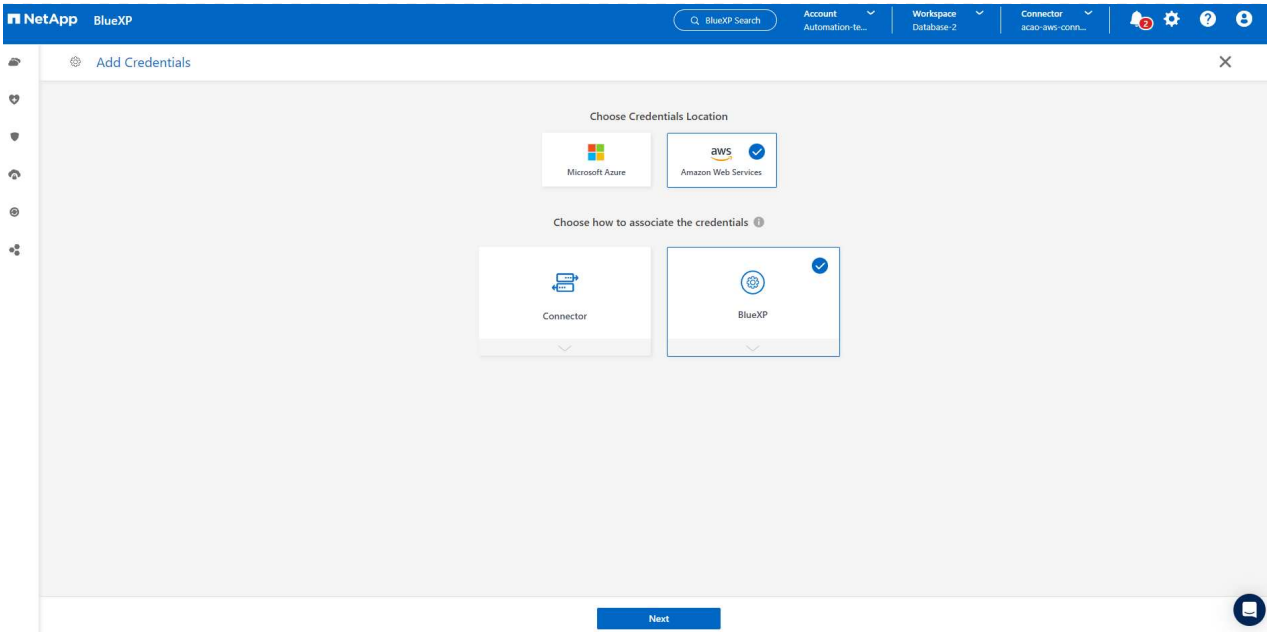
4. Dans la page **Role details**, nommez le rôle, ajoutez une description, puis cliquez sur **Create Role**.



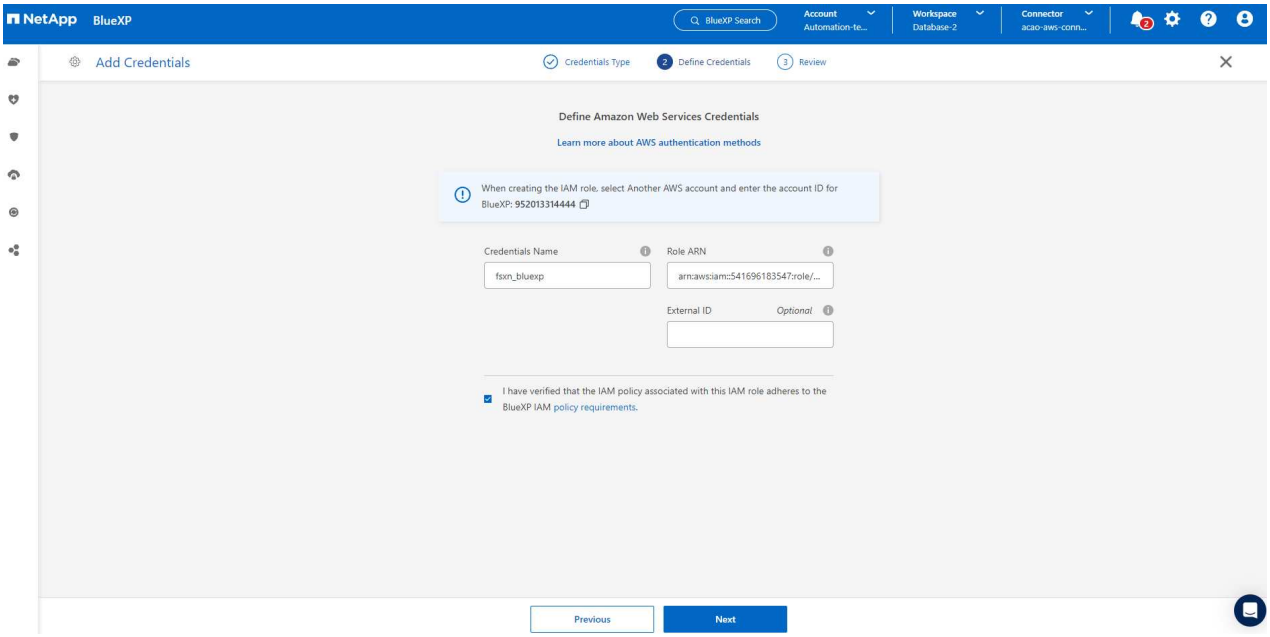
5. Retour à la console BlueXP, cliquez sur l'icône de paramètre en haut à droite de la console pour ouvrir la page **informations d'identification du compte**, cliquez sur **Ajouter des informations d'identification** pour démarrer le flux de travail de configuration des informations d'identification.



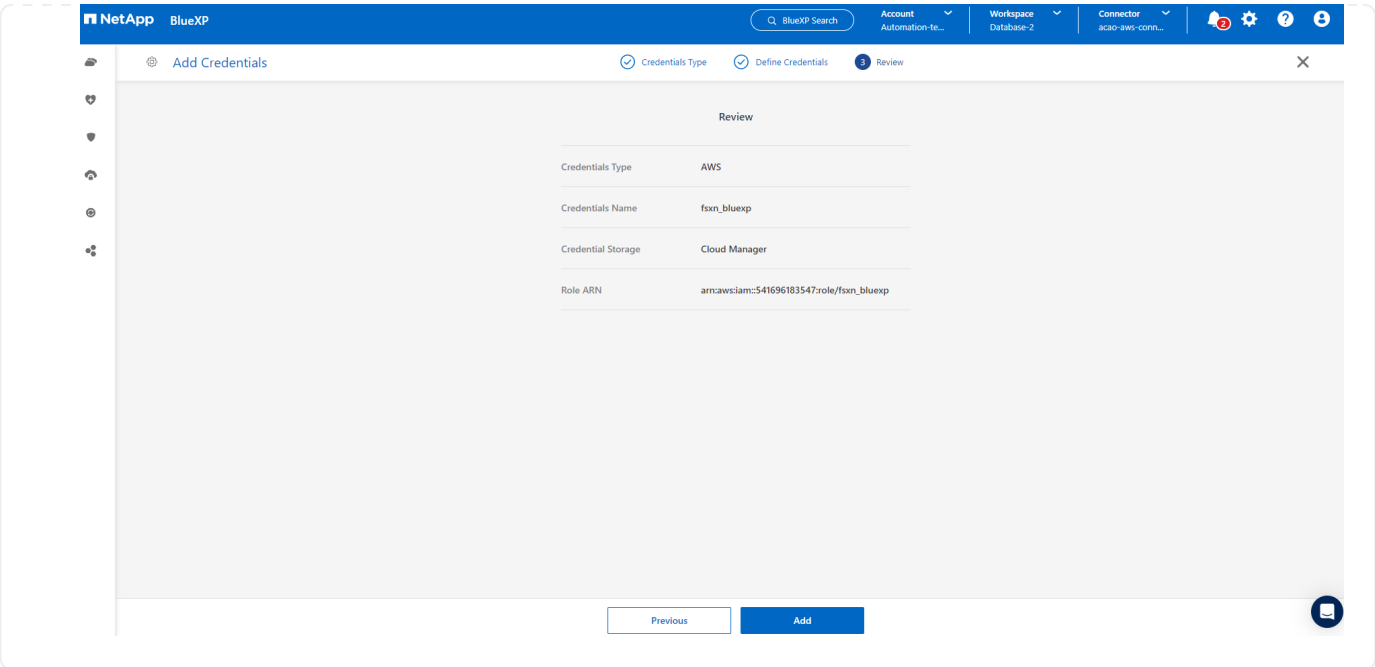
6. Choisissez l'emplacement des informations d'identification comme - **Amazon Web Services - BlueXP**.



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



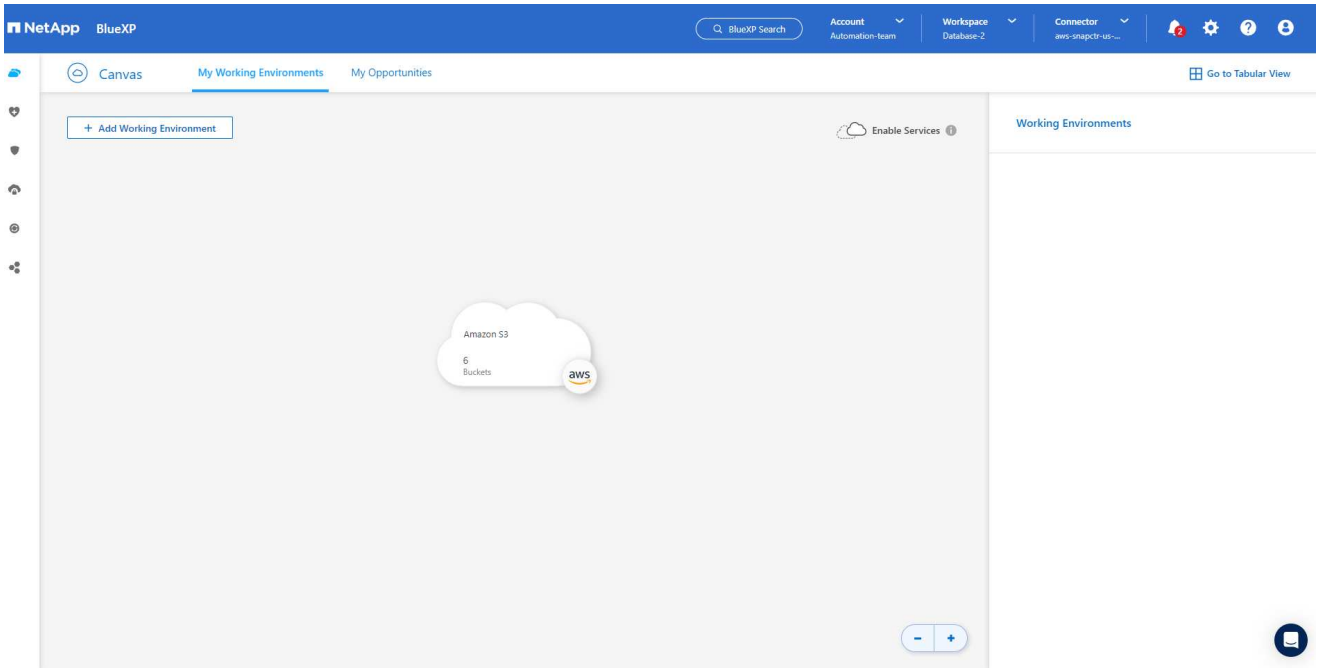
8. Revoir et **Ajouter**.



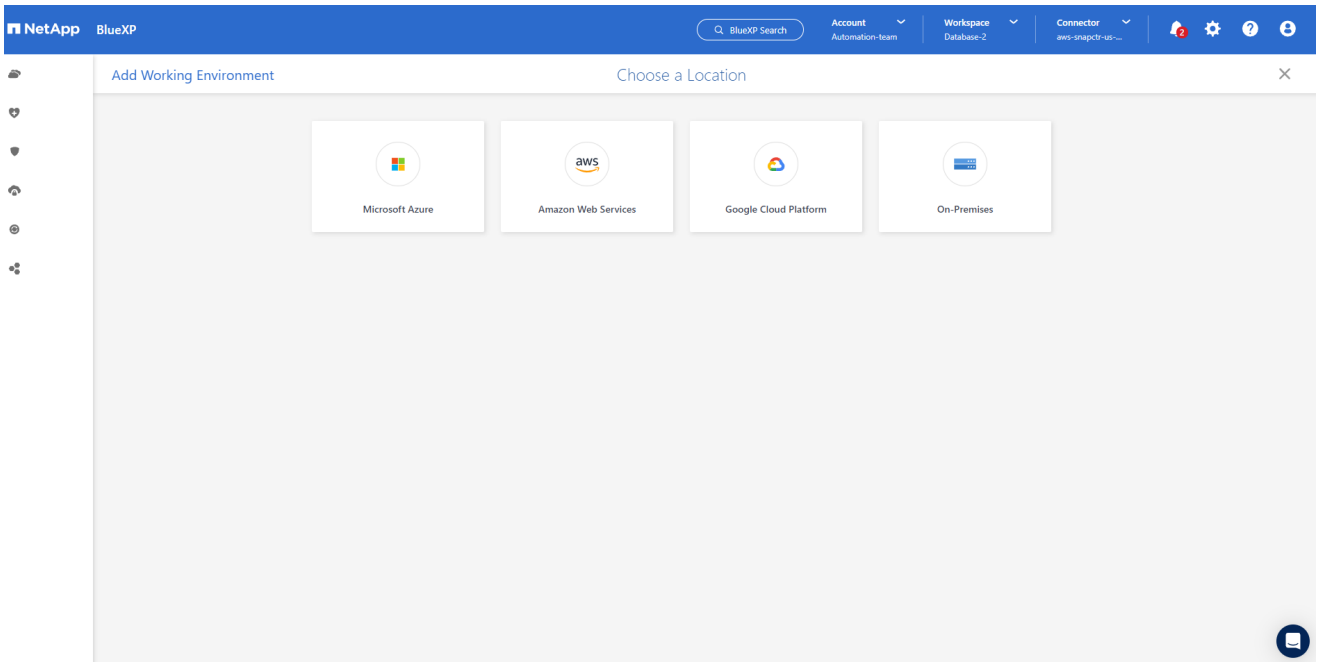
Configuration des services SnapCenter

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

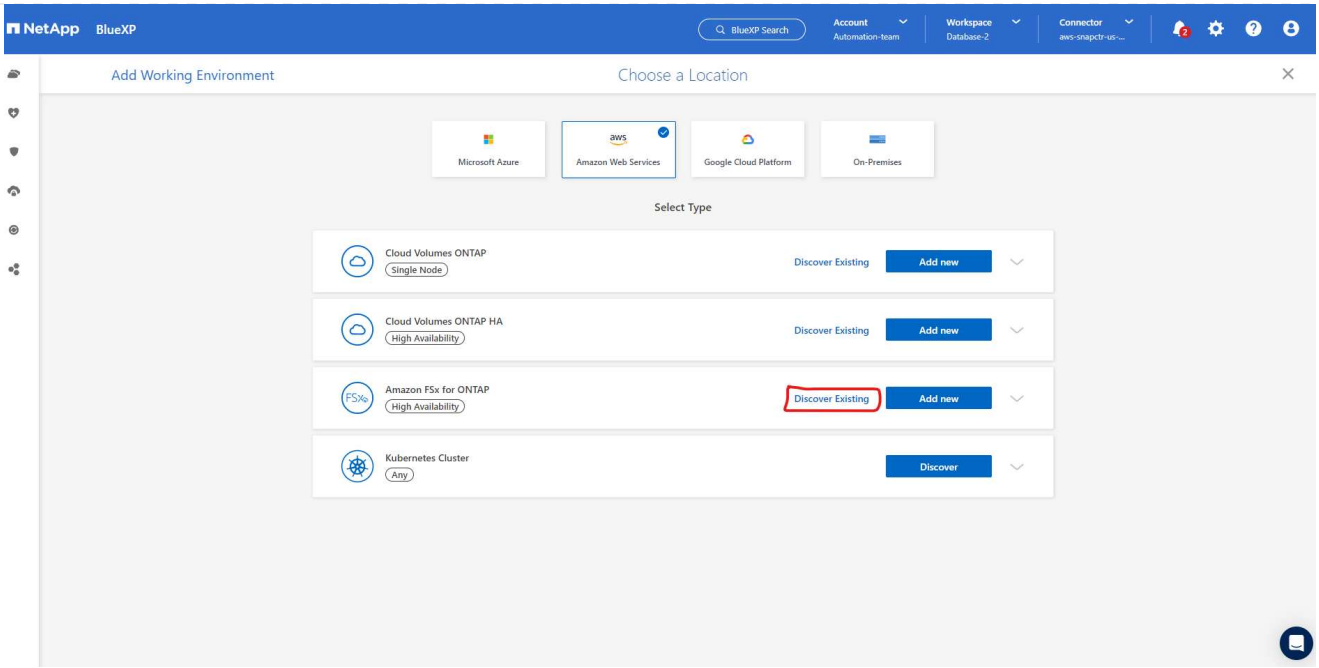
1. Dans **mon environnement de travail**, cliquez sur **Ajouter un environnement de travail** pour découvrir FSX déployé dans AWS.



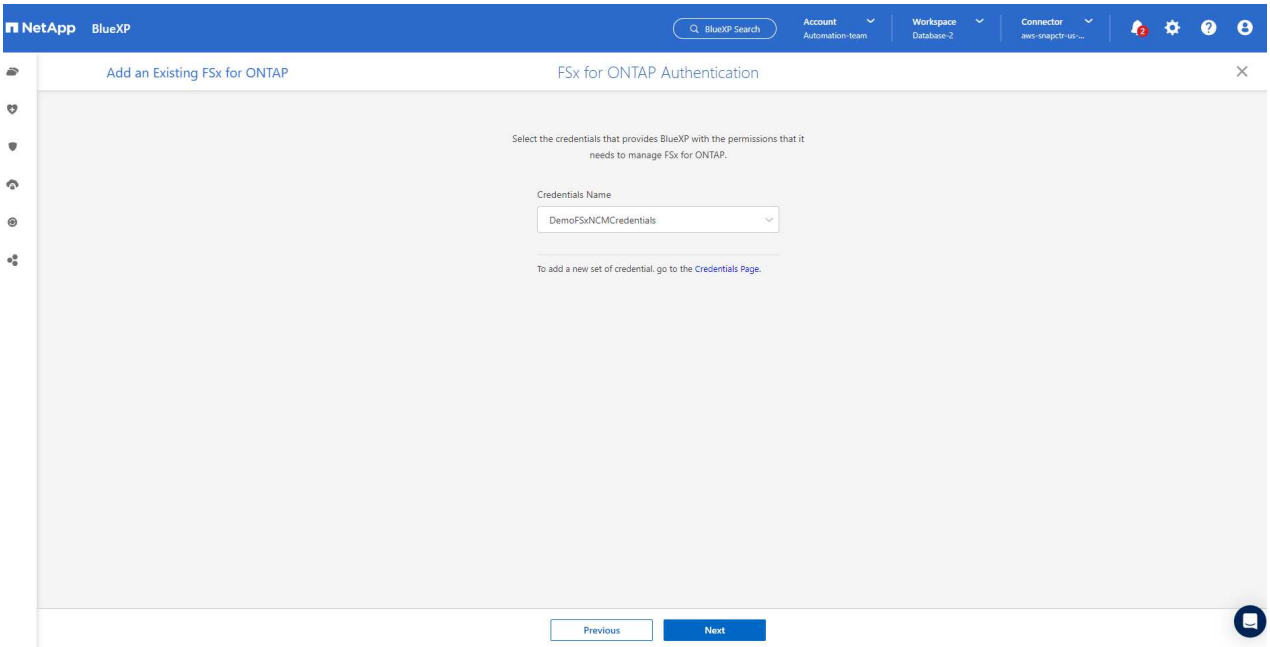
1. Choisissez **Amazon Web Services** comme emplacement.



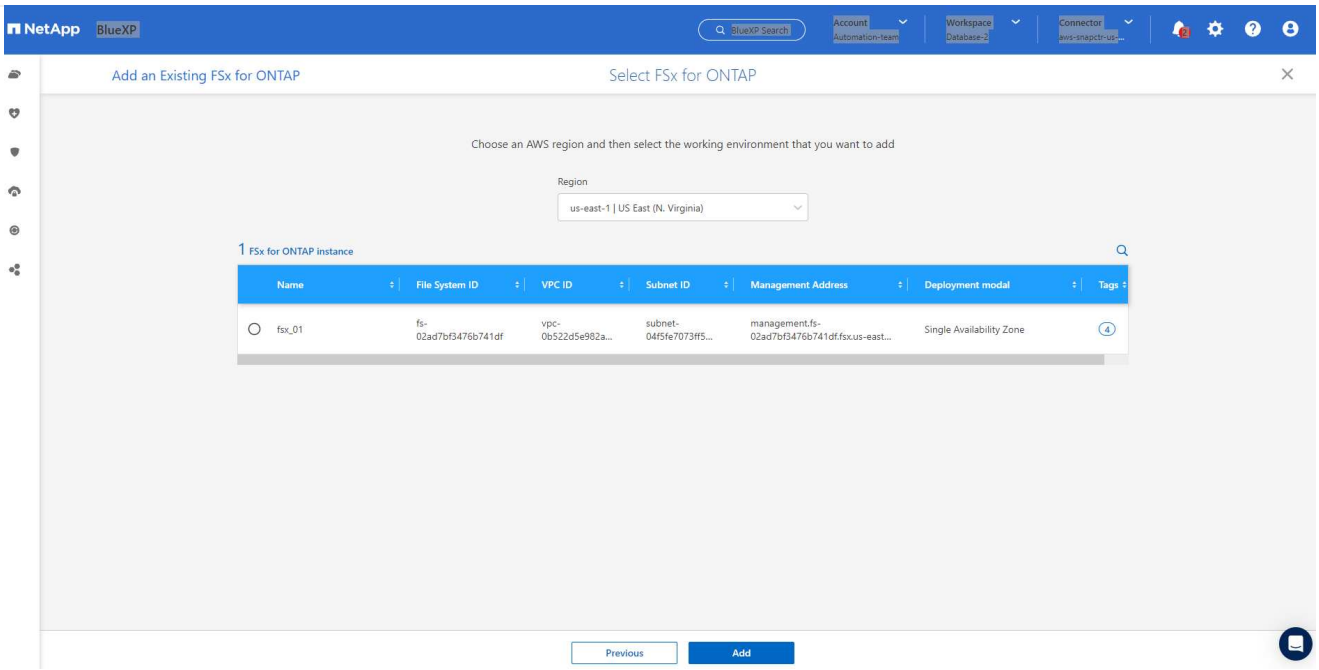
1. Cliquez sur **découvrir existant** en regard de **Amazon FSX pour ONTAP**.



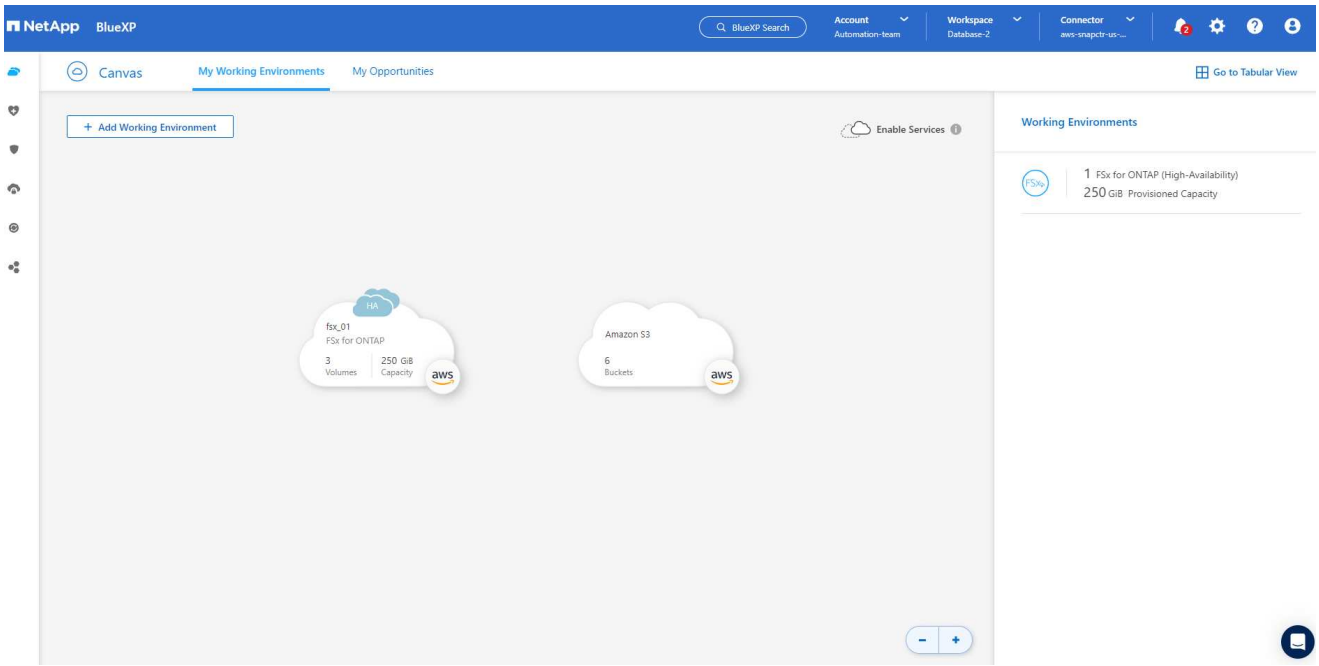
1. Sélectionnez le **Nom d'identification** que vous avez créé dans la section précédente pour accorder à BlueXP les autorisations dont il a besoin pour gérer FSX pour ONTAP. Si vous n'avez pas ajouté d'informations d'identification, vous pouvez l'ajouter à partir du menu **Settings** situé dans le coin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



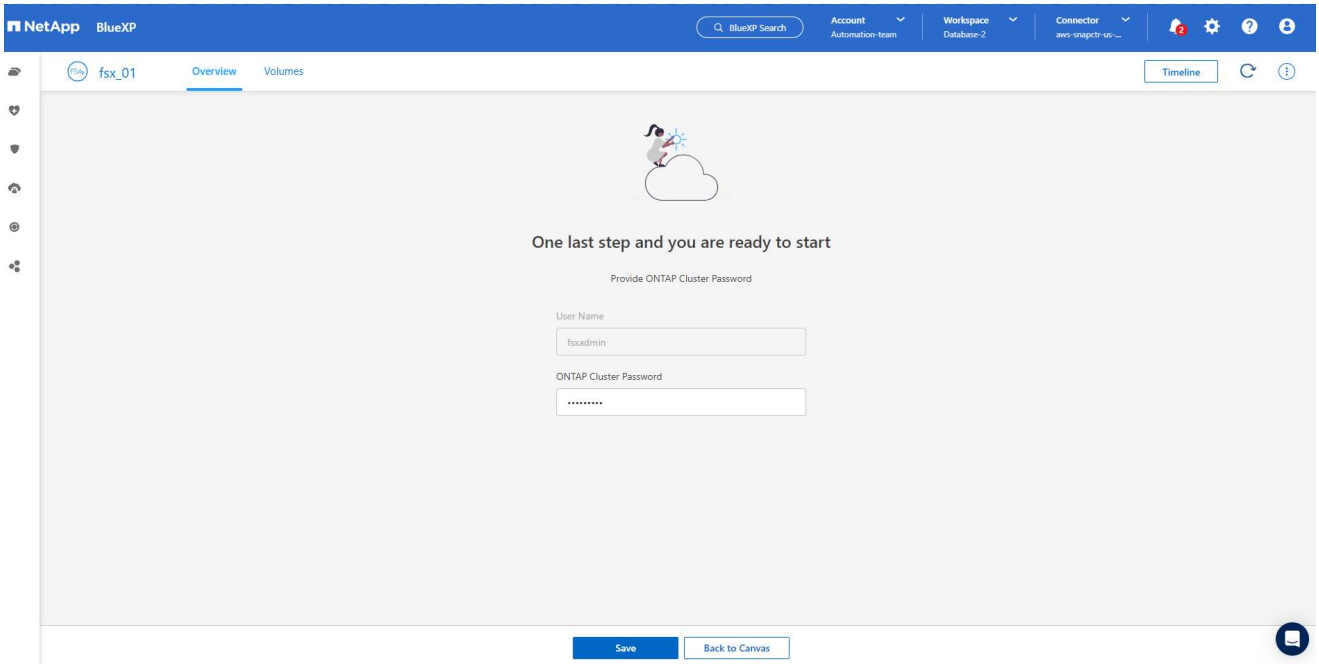
2. Choisissez la région AWS dans laquelle Amazon FSX pour ONTAP est déployé, sélectionnez le cluster FSX qui héberge la base de données Oracle et cliquez sur Ajouter.



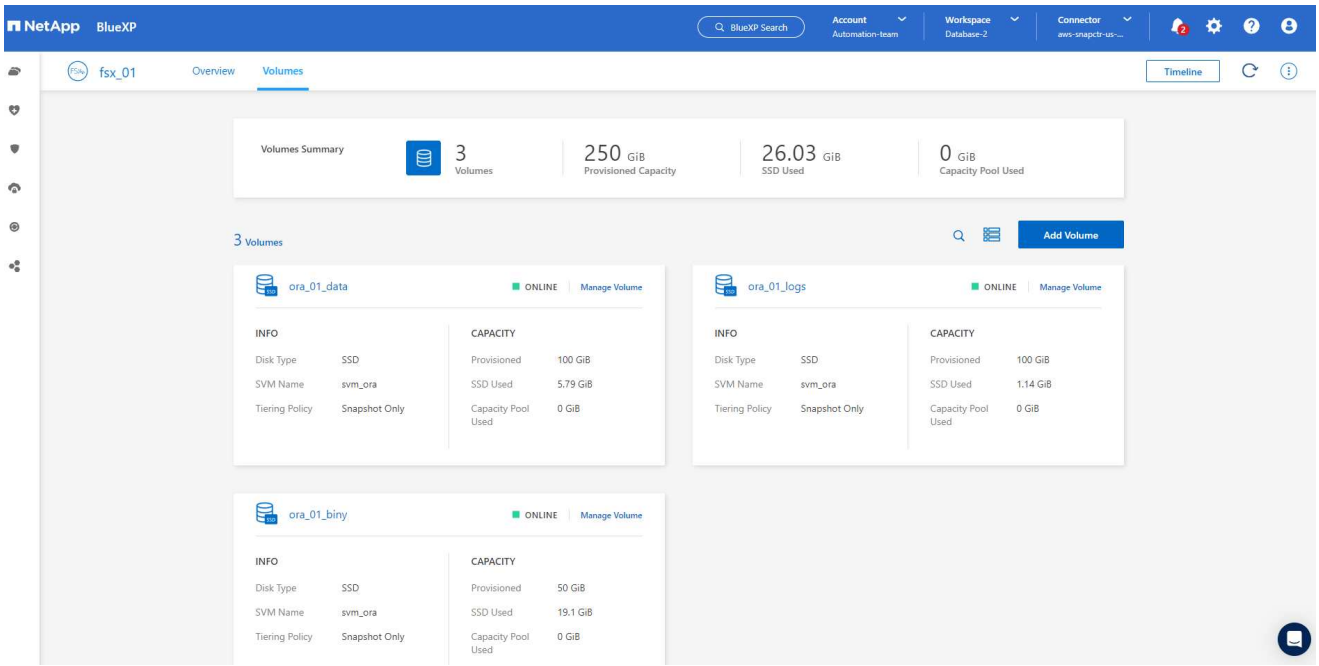
1. L'instance Amazon FSX for ONTAP détectée apparaît désormais dans l'environnement de travail.



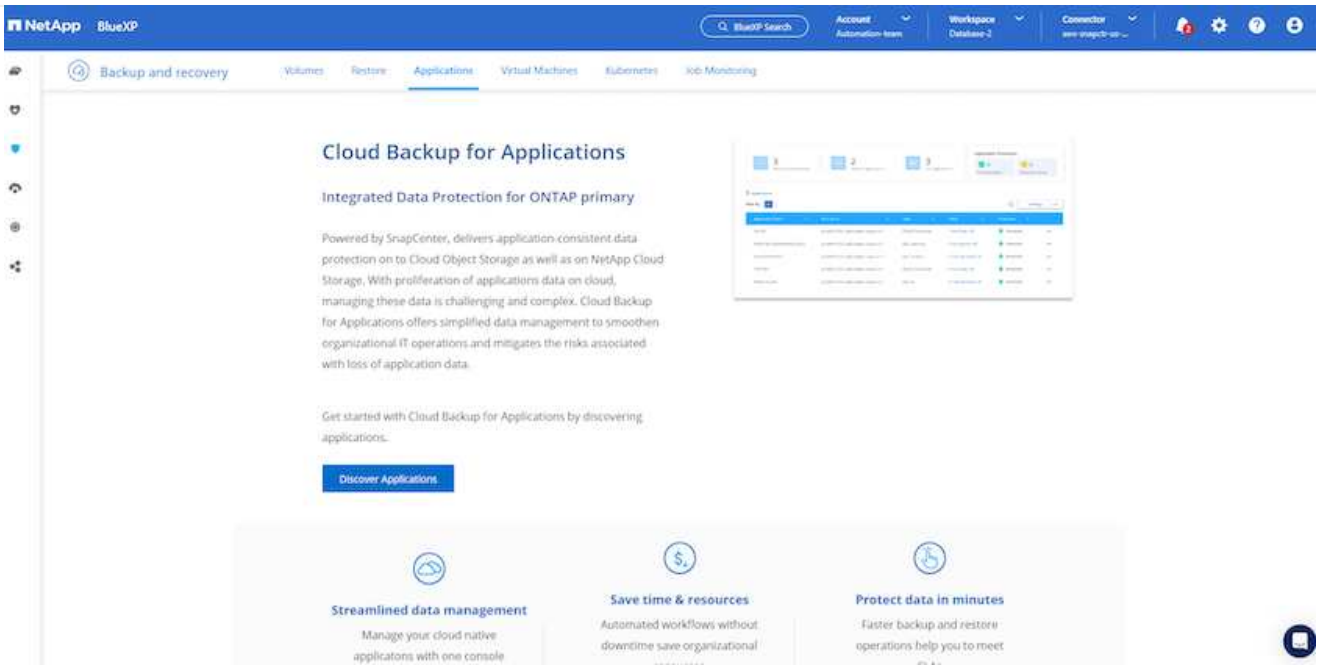
1. Vous pouvez vous connecter au cluster FSX à l'aide de vos informations d'identification de compte fsxadmin.



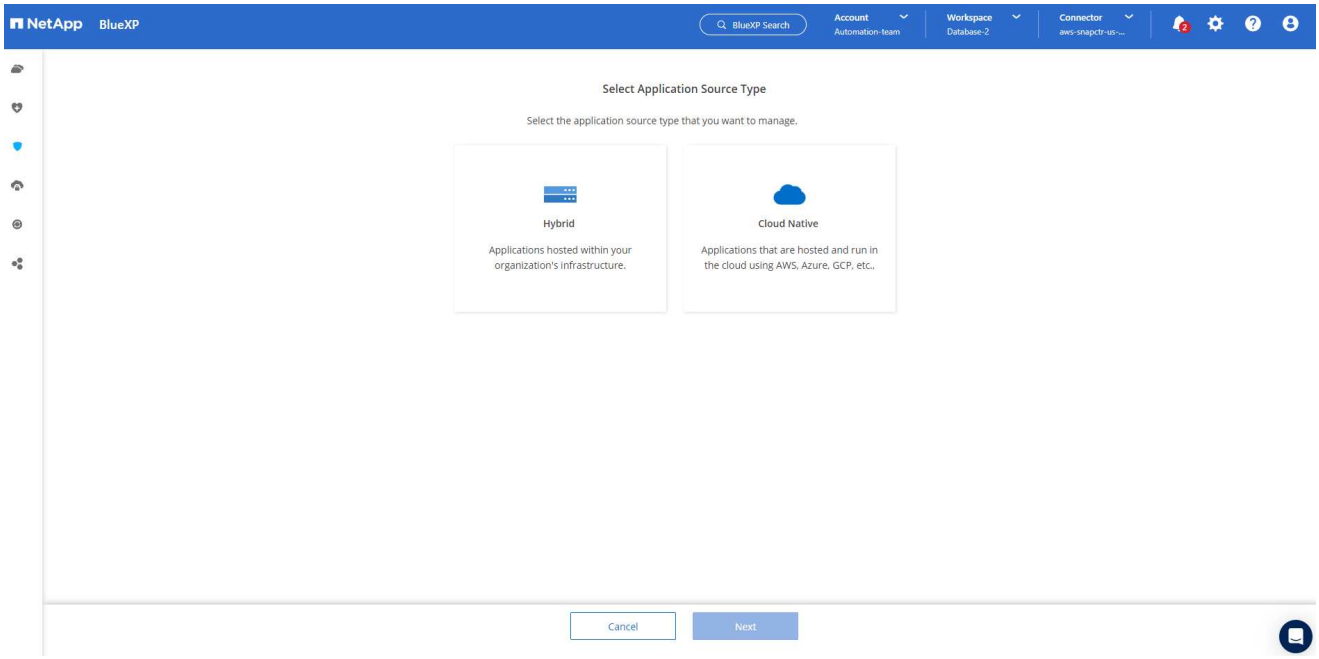
1. Une fois connecté à Amazon FSX pour ONTAP, vérifiez les informations relatives au stockage de votre base de données (comme les volumes de base de données).



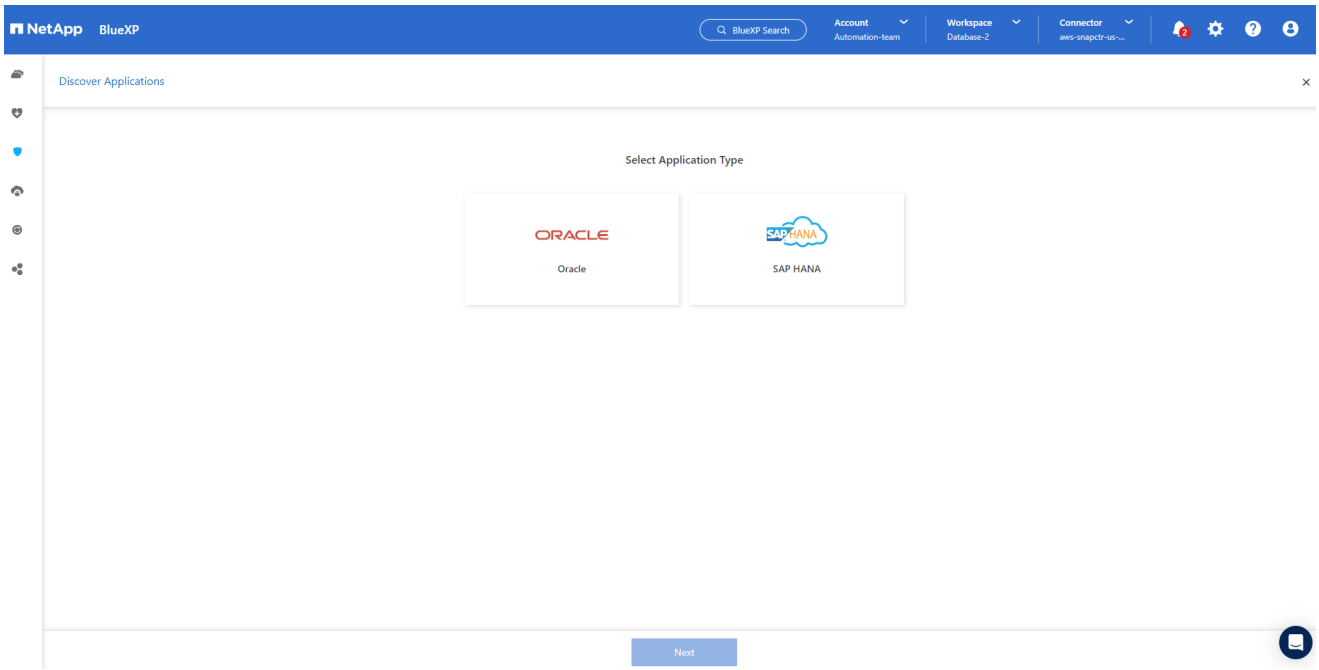
1. Dans la barre latérale gauche de la console, passez votre souris sur l'icône de protection, puis cliquez sur **protection** > **applications** pour ouvrir la page de lancement applications. Cliquez sur **découvrir les applications**.



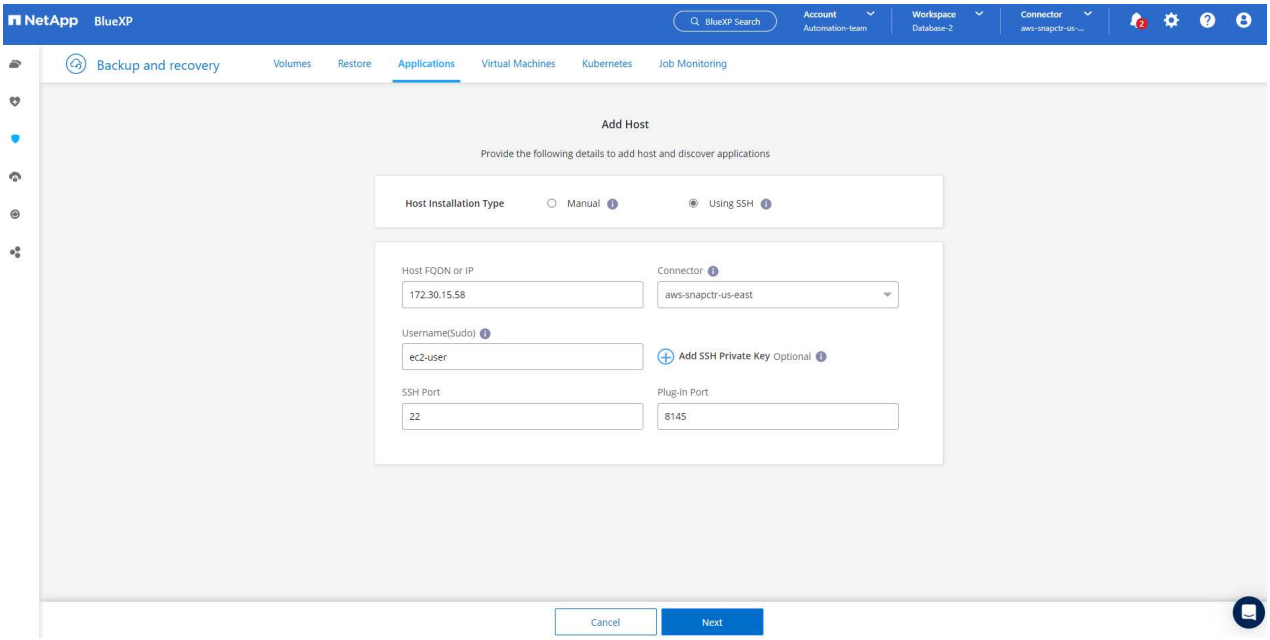
1. Sélectionnez **Cloud Native** comme type de source d'application.



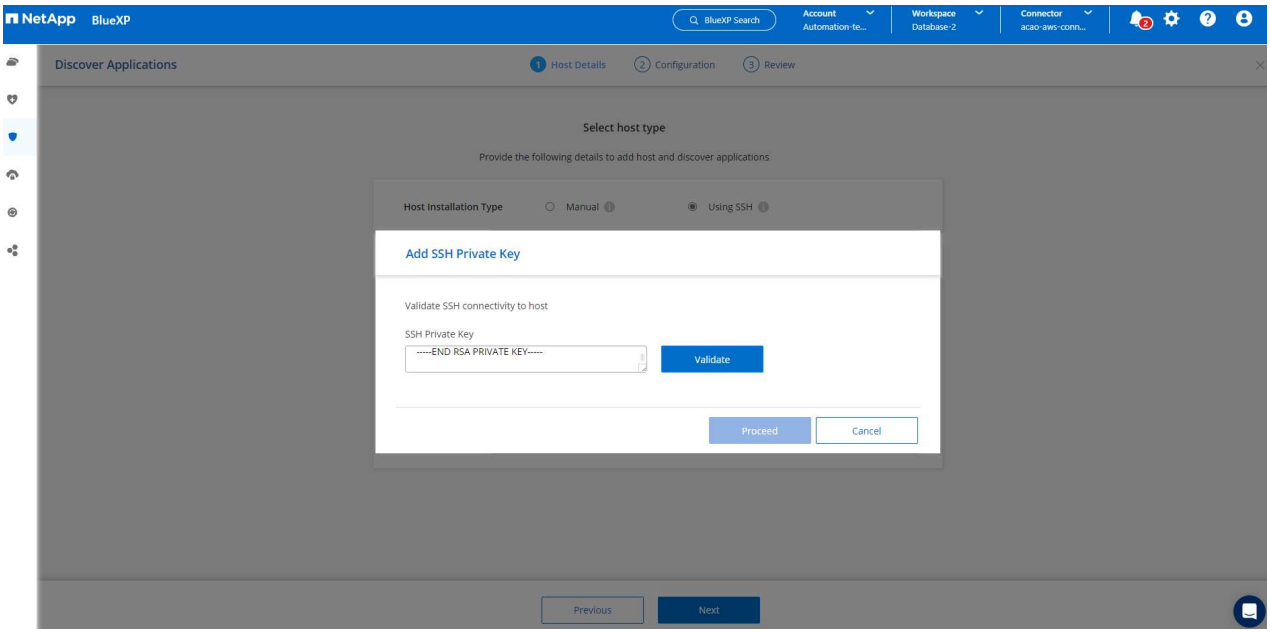
1. Choisissez **Oracle** comme type d'application.



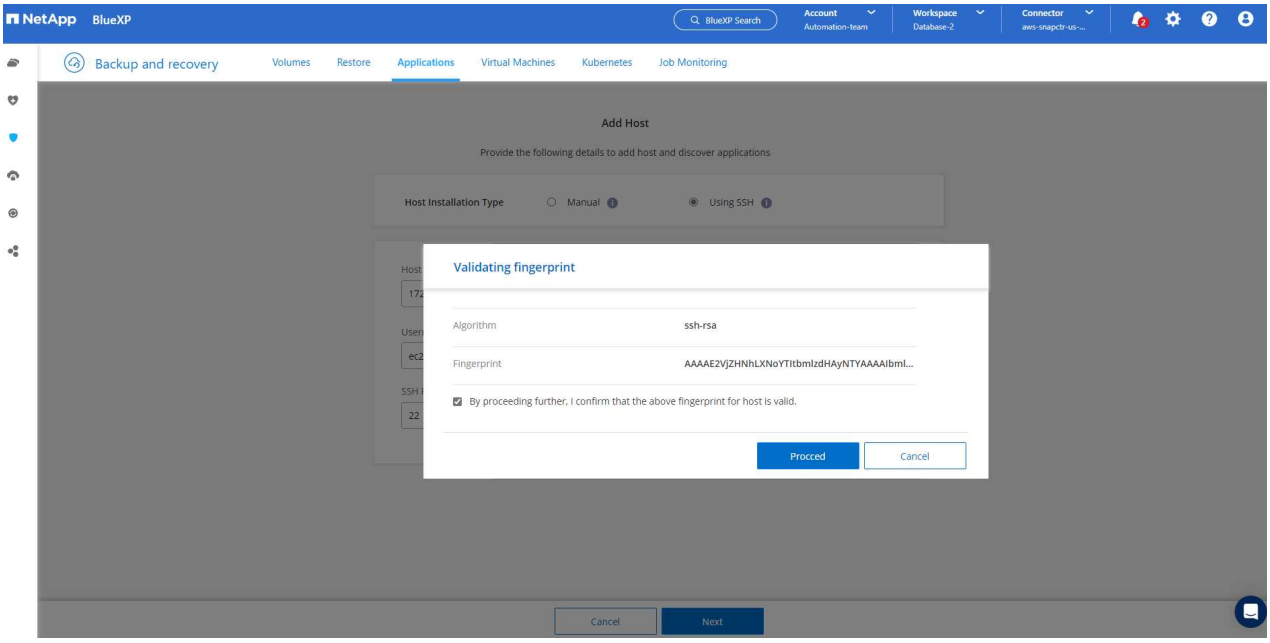
1. Renseignez les détails sur l'hôte d'application Oracle AWS EC2. Choisissez **en utilisant SSH** comme **Type d'installation hôte** pour l'installation du plug-in en une étape et la découverte de la base de données. Cliquez ensuite sur **Ajouter une clé privée SSH**.



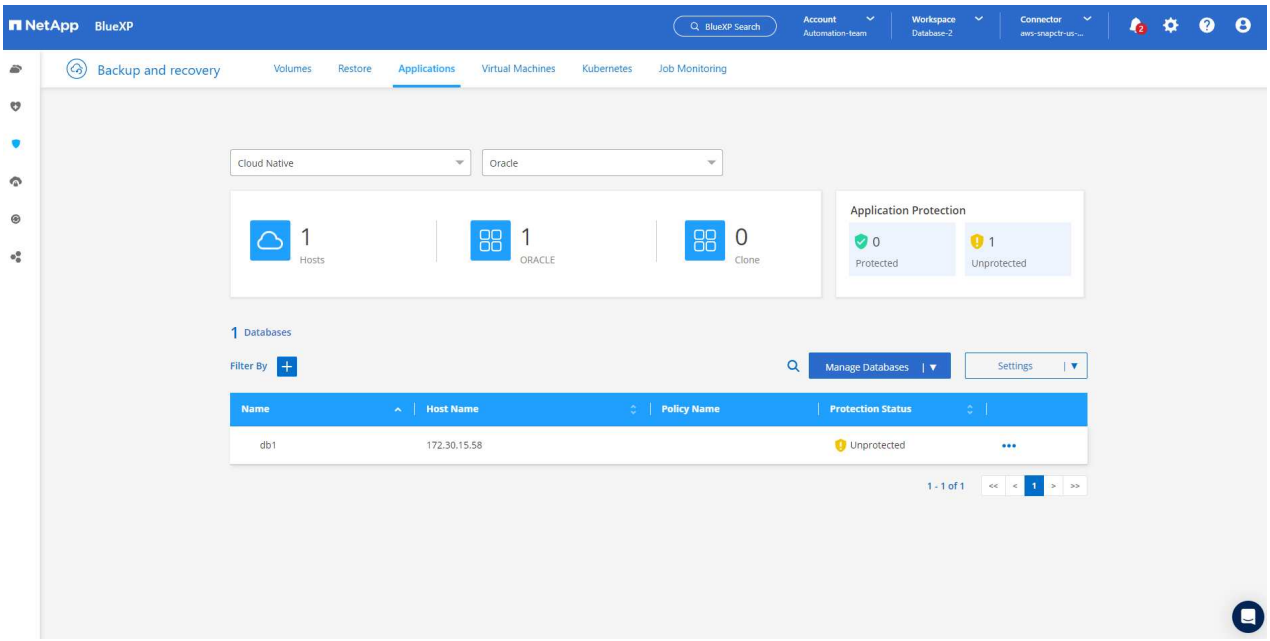
2. Collez votre clé SSH ec2-user pour l'hôte ec2 de la base de données et cliquez sur **Valider** pour continuer.



3. Vous serez invité à indiquer **la validation de l'empreinte digitale** pour continuer.



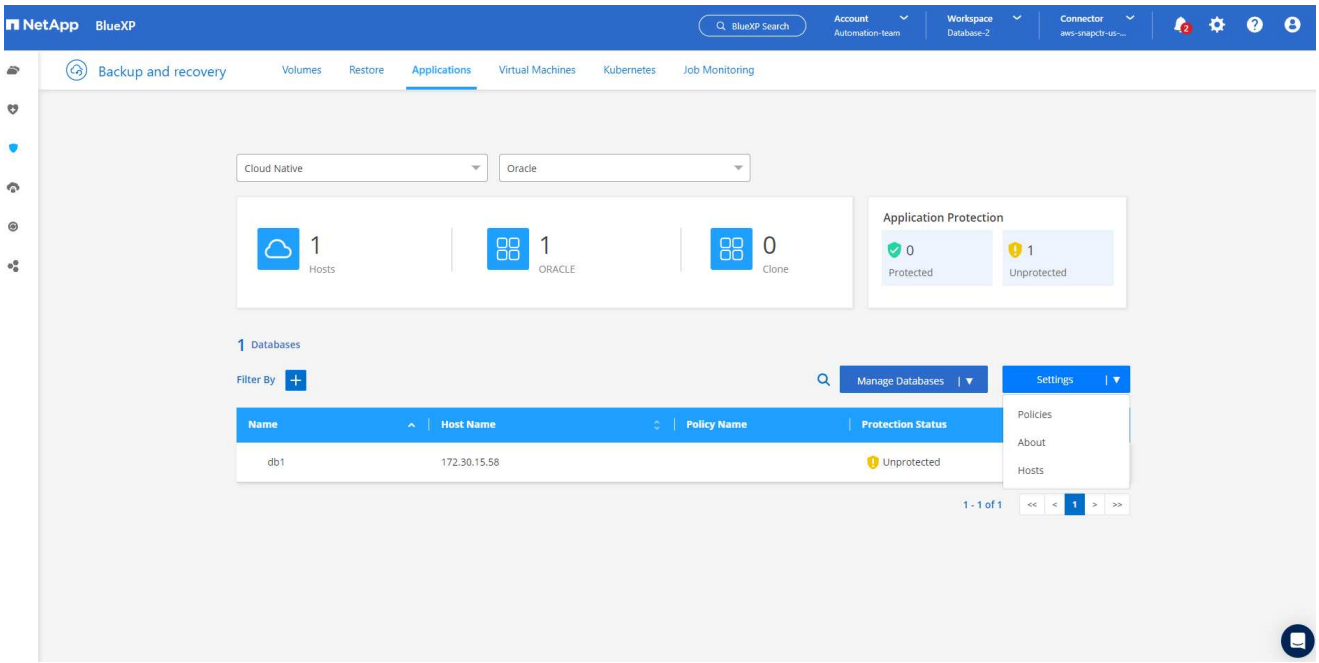
4. Cliquez sur **Suivant** pour installer un plug-in de base de données Oracle et découvrir les bases de données Oracle sur l'hôte EC2. Les bases de données découvertes sont ajoutées à **applications**. La base de données **Etat de protection** s'affiche sous la forme **non protégé** lors de la découverte initiale.



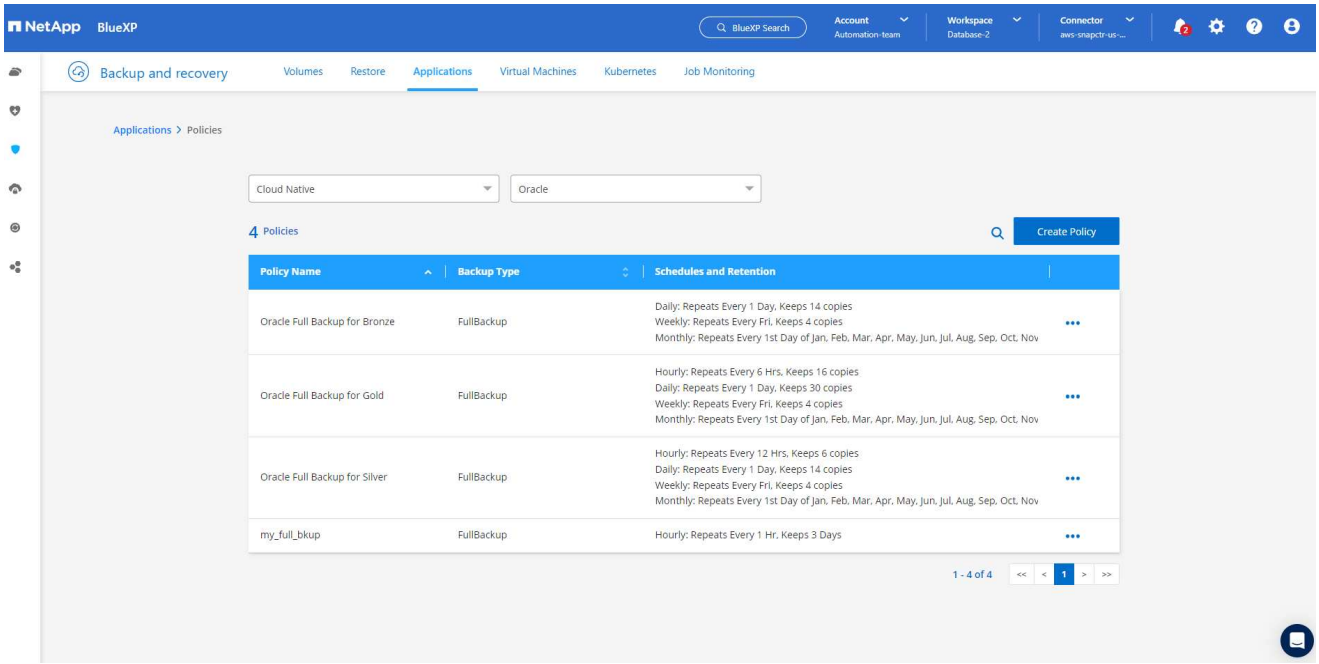
La configuration initiale des services SnapCenter pour Oracle est terminée. Les trois sections suivantes de ce document décrivent les opérations de sauvegarde, de restauration et de clonage de bases de données Oracle.

Sauvegarde de la base de données Oracle

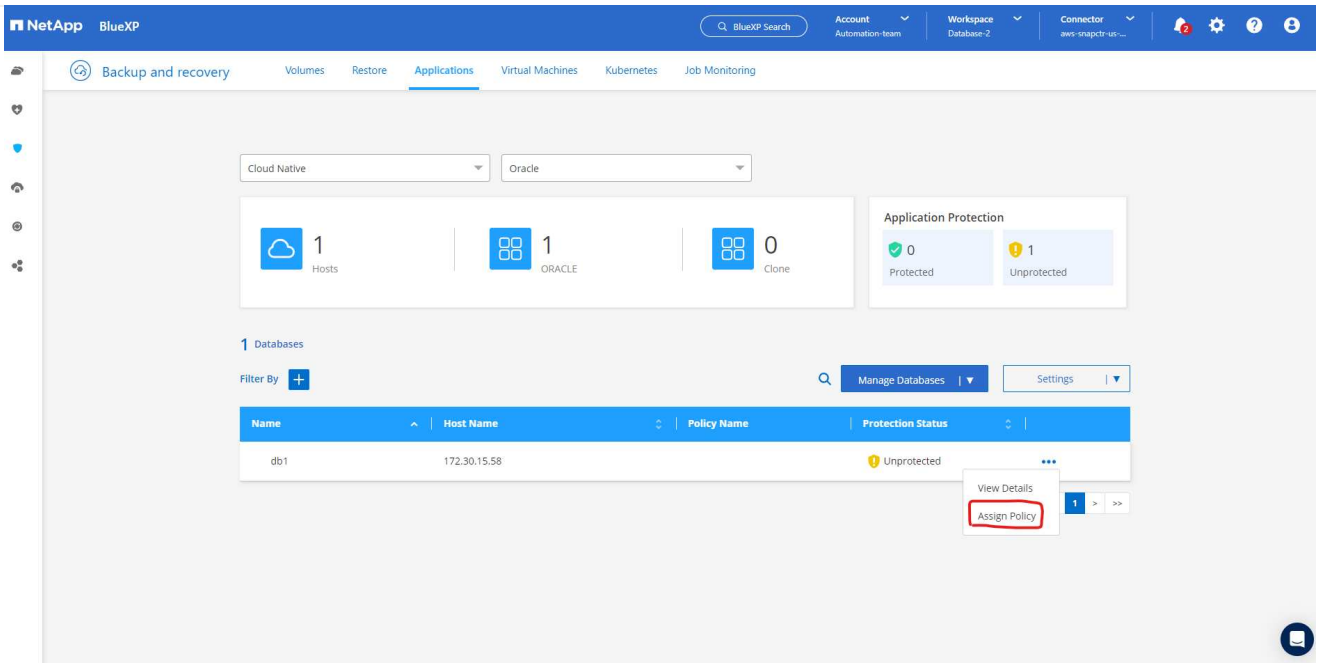
1. Cliquez sur les trois points en regard de la base de données **Etat de la protection**, puis cliquez sur **stratégies** pour afficher les stratégies de protection de base de données préchargées par défaut qui peuvent être appliquées pour protéger vos bases de données Oracle.



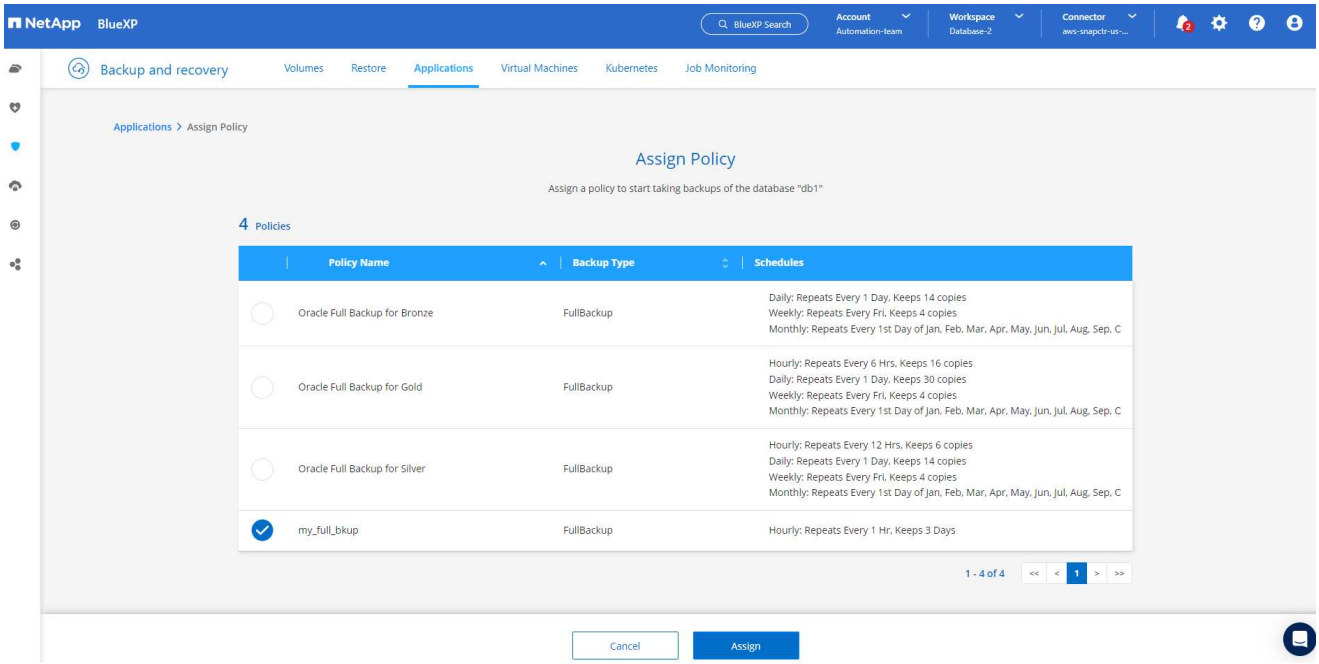
1. Vous pouvez également créer votre propre règle avec une fréquence de sauvegarde personnalisée et une fenêtre de conservation des données de sauvegarde personnalisée.



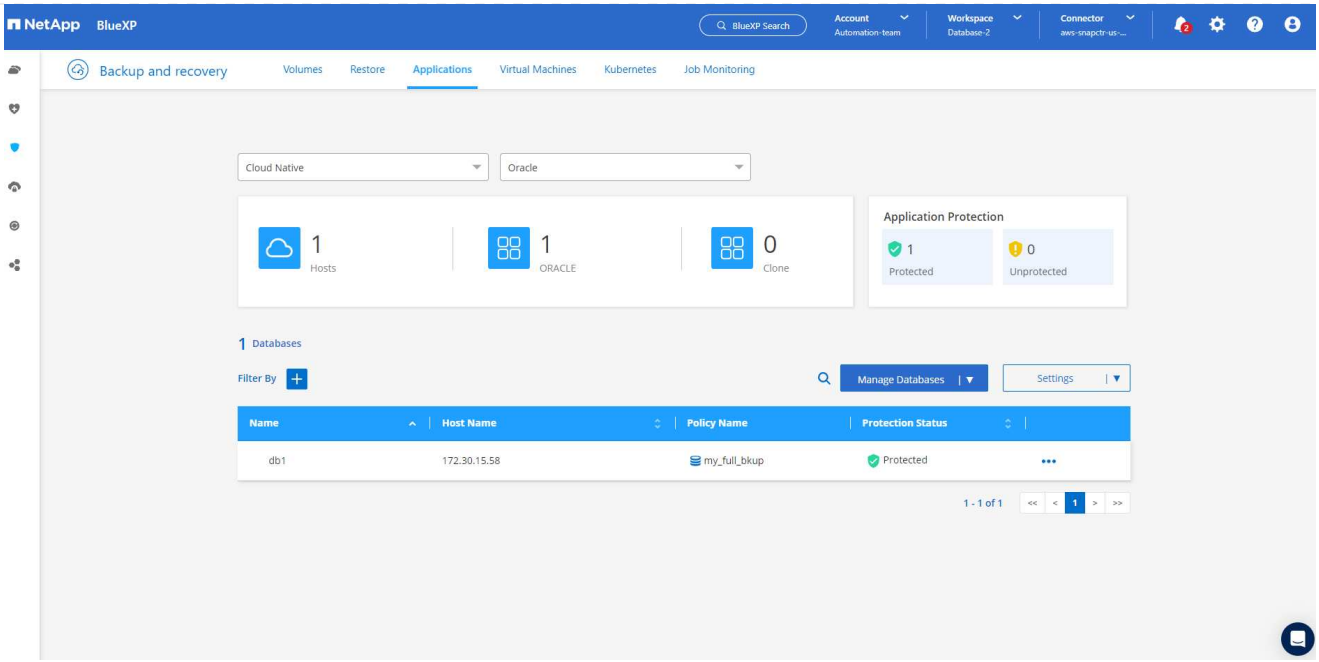
1. Lorsque vous êtes satisfait de la configuration de la stratégie, vous pouvez ensuite attribuer la stratégie de votre choix pour protéger la base de données.



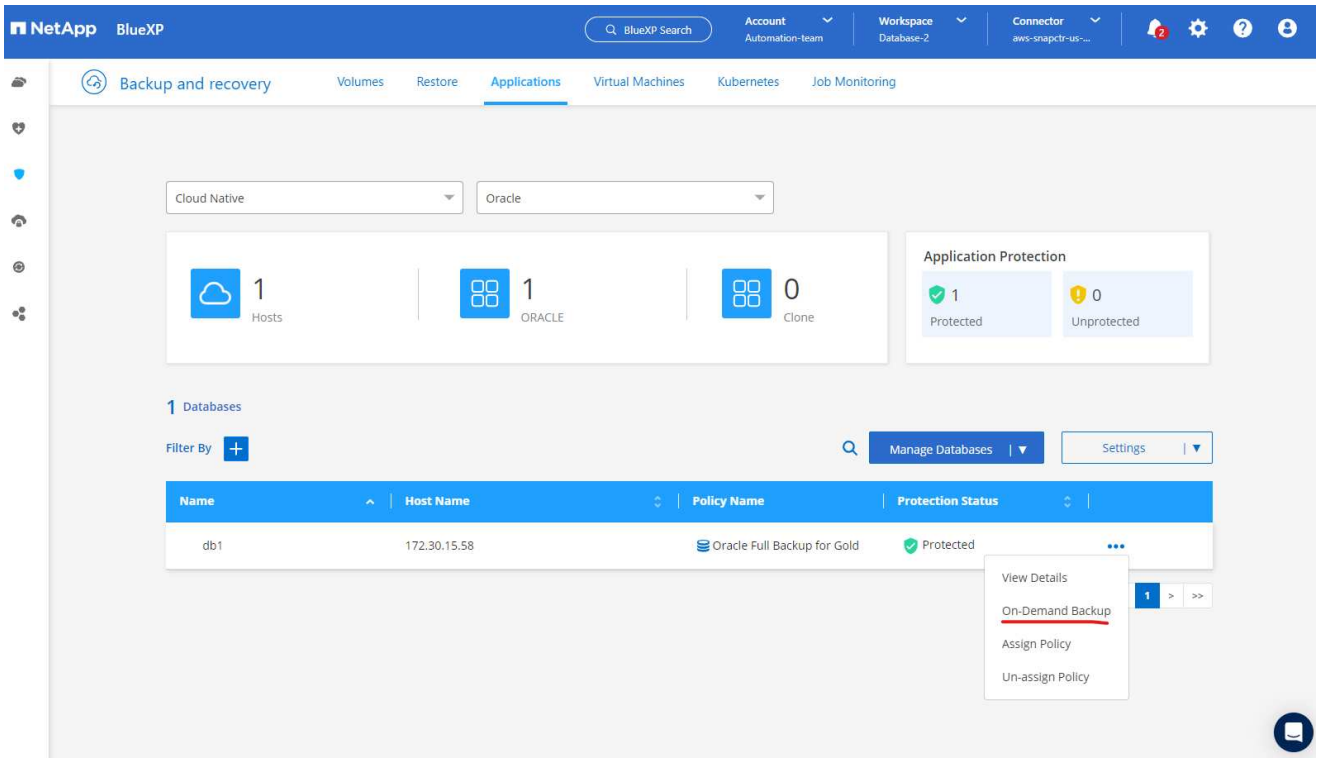
1. Choisissez la stratégie à affecter à la base de données.



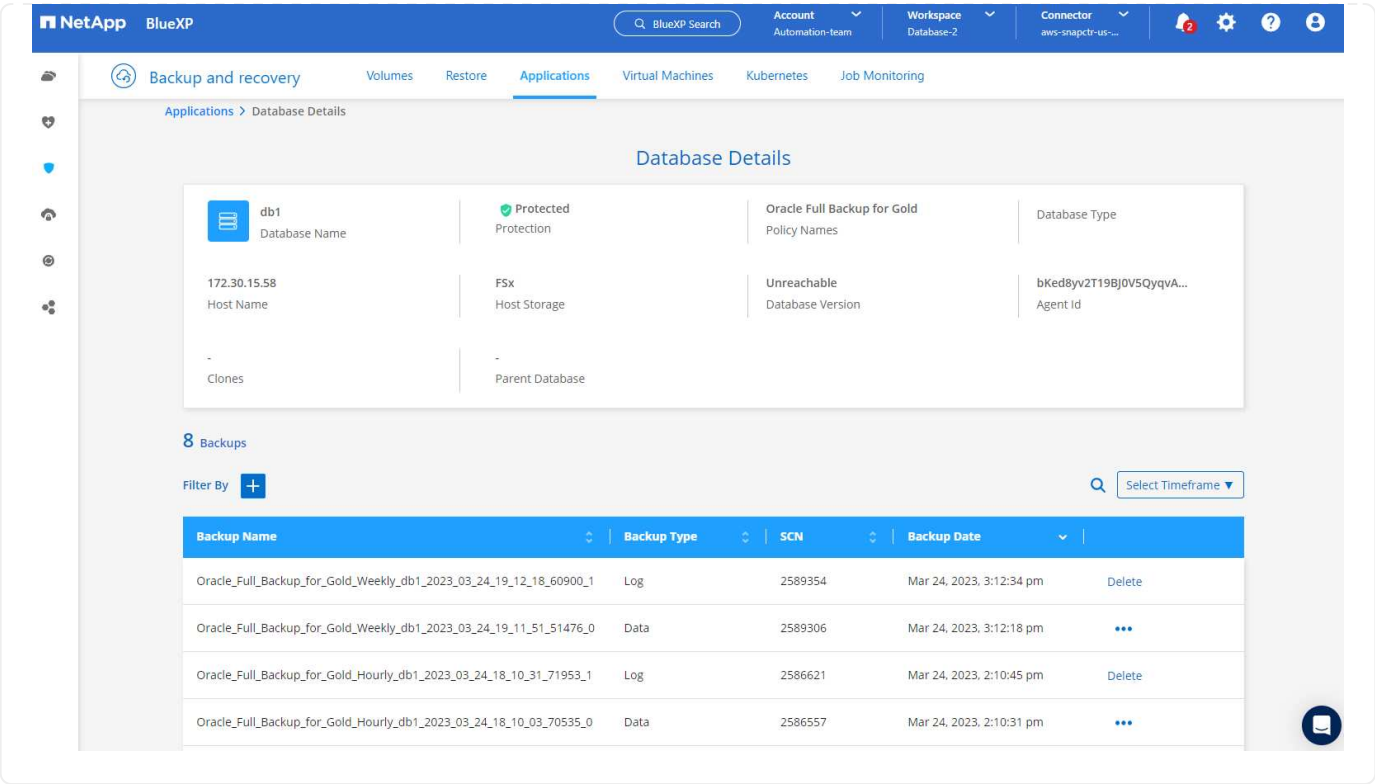
1. Une fois la règle appliquée, l'état de protection de la base de données passe à **protégé** avec une coche verte.



1. La sauvegarde de la base de données s'exécute selon un planning prédéfini. Vous pouvez également exécuter une sauvegarde à la demande unique, comme illustré ci-dessous.

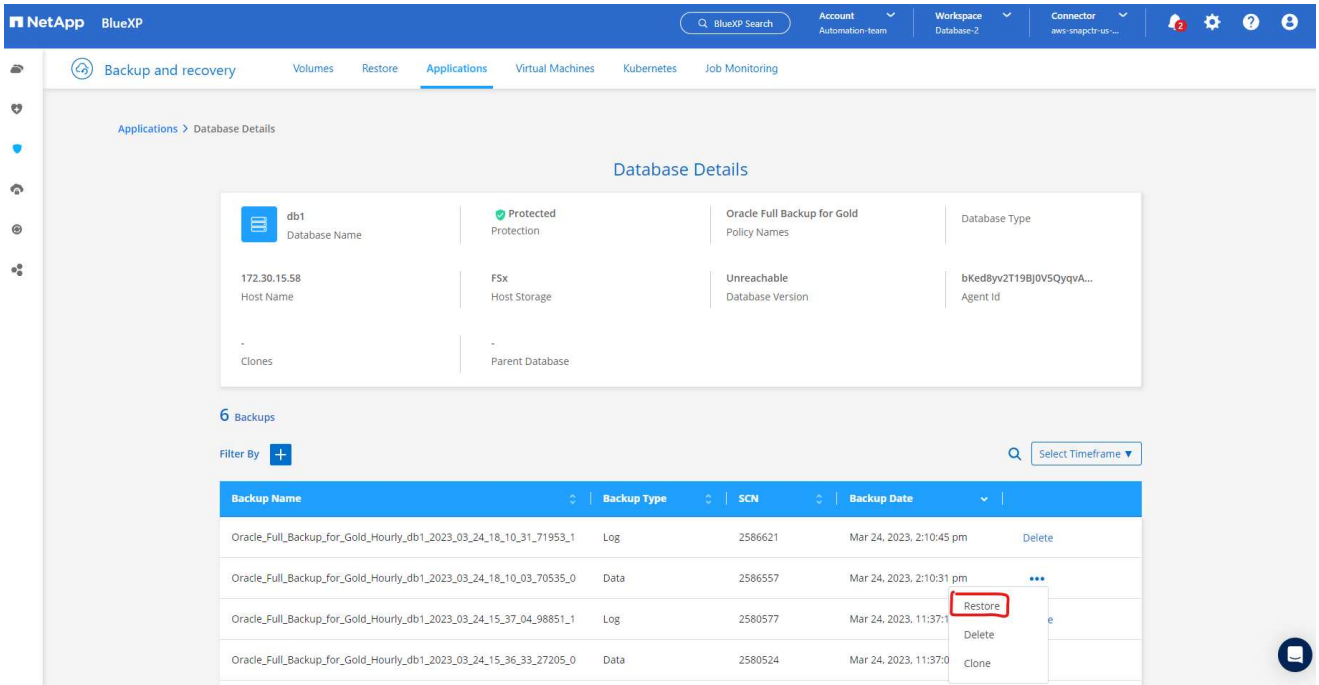


1. Vous pouvez afficher les détails des sauvegardes de la base de données en cliquant sur **Afficher les détails** dans la liste de menus. Cela inclut le nom de la sauvegarde, le type de sauvegarde, le SCN et la date de sauvegarde. Un jeu de sauvegardes couvre un snapshot pour le volume de données et le volume de journaux. Un snapshot de volume de journaux a lieu juste après un snapshot de volume de base de données. Vous pouvez appliquer un filtre si vous recherchez une sauvegarde particulière dans une longue liste.

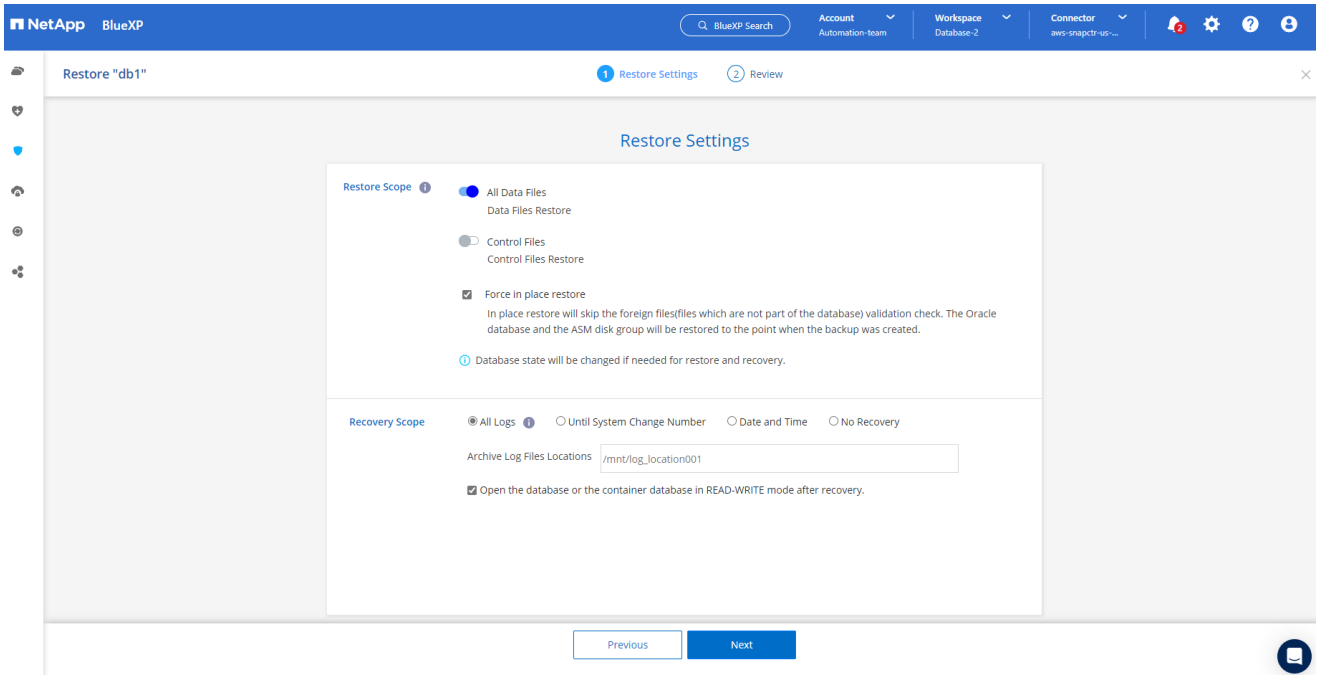


Restauration et récupération de la base de données Oracle

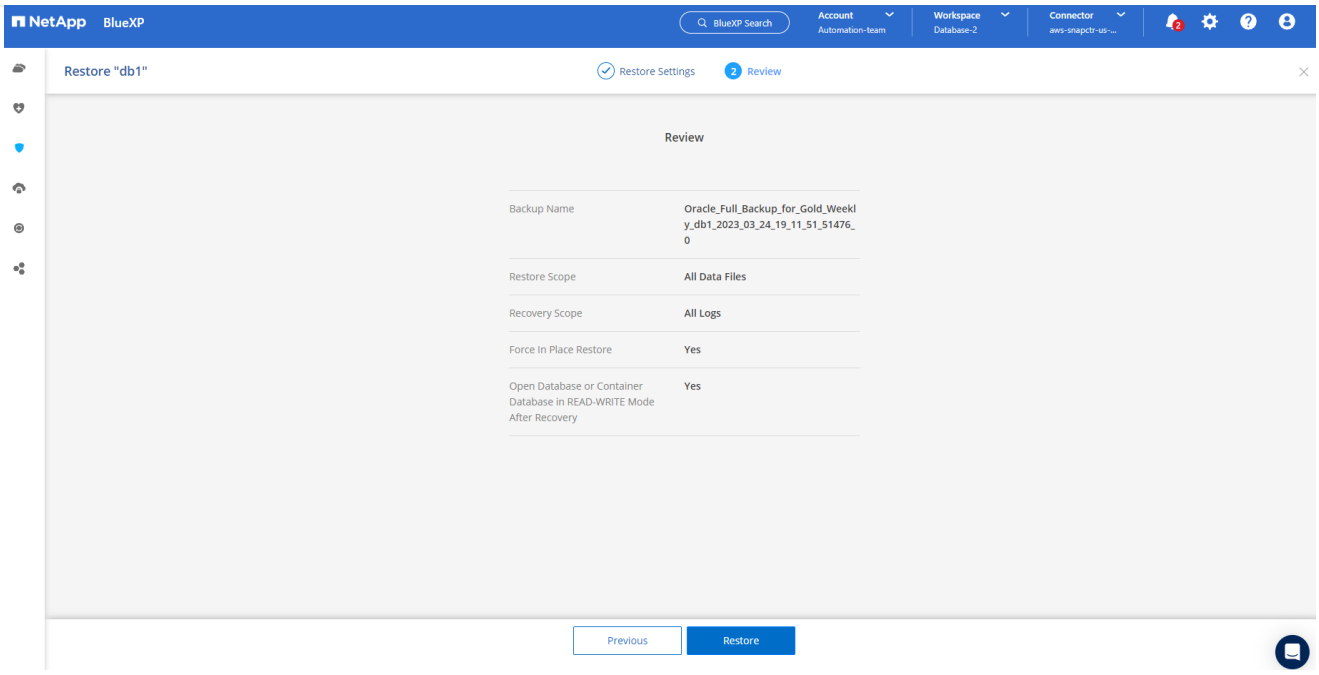
1. Pour une restauration de base de données, choisissez la sauvegarde appropriée, soit par le SCN, soit par le temps de sauvegarde. Cliquez sur les trois points de la sauvegarde des données de la base de données, puis cliquez sur **Restaurer** pour lancer la restauration et la récupération de la base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



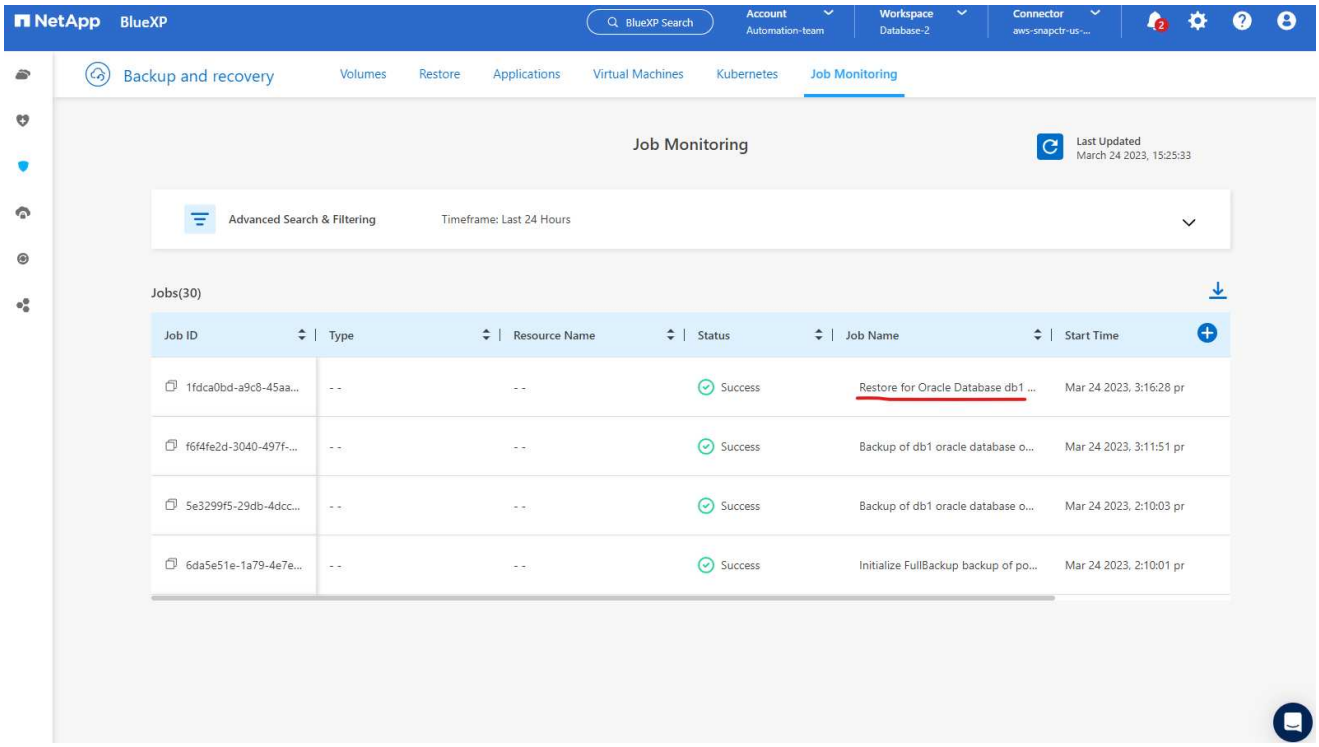
1. Choisissez votre paramètre de restauration. Si vous êtes sûr que rien n'a changé dans la structure de base de données physique après la sauvegarde (par exemple, l'ajout d'un fichier de données ou d'un groupe de disques), vous pouvez utiliser l'option **forcer la restauration en place**, qui est généralement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

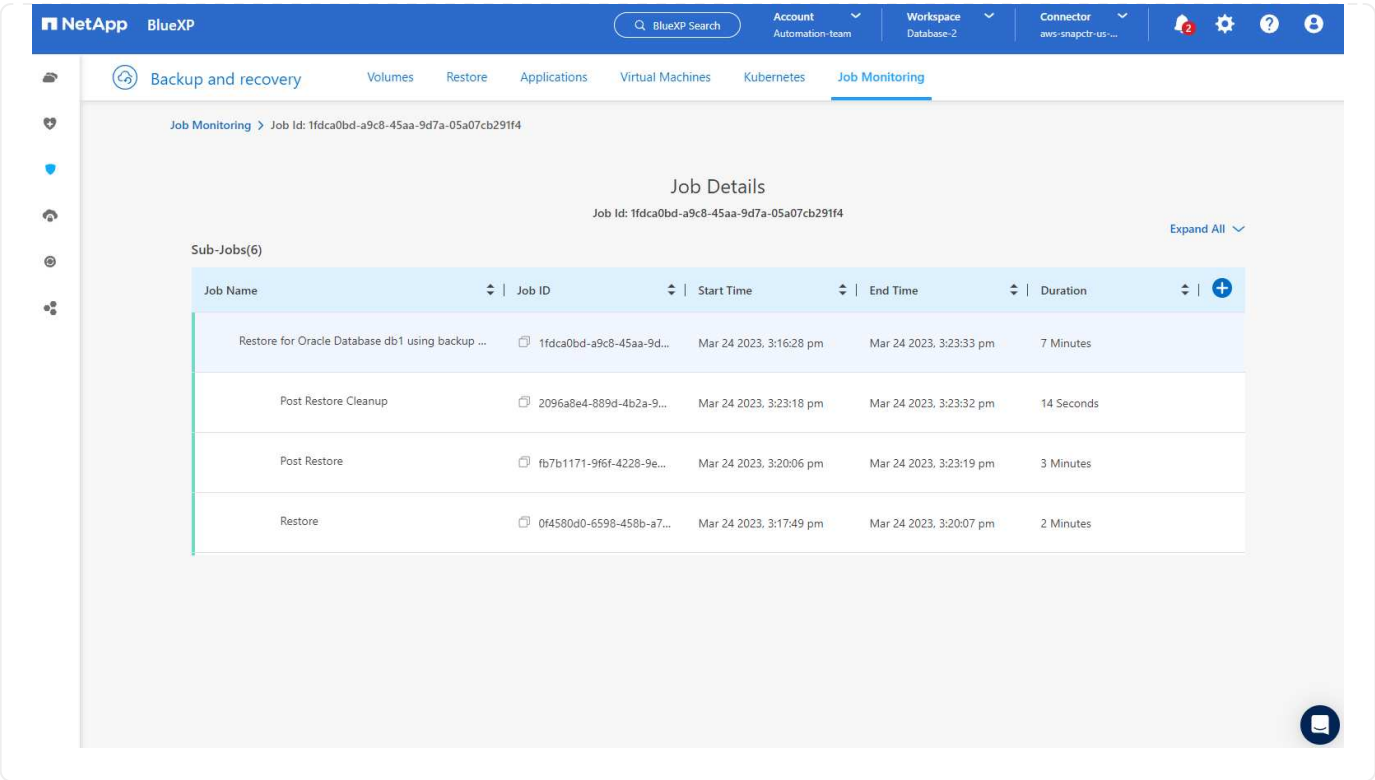


1. Vérifiez et démarrez la restauration et la récupération de la base de données.



1. Dans l'onglet **Job Monitoring**, vous pouvez afficher l'état de la tâche de restauration ainsi que tous les détails pendant son exécution.

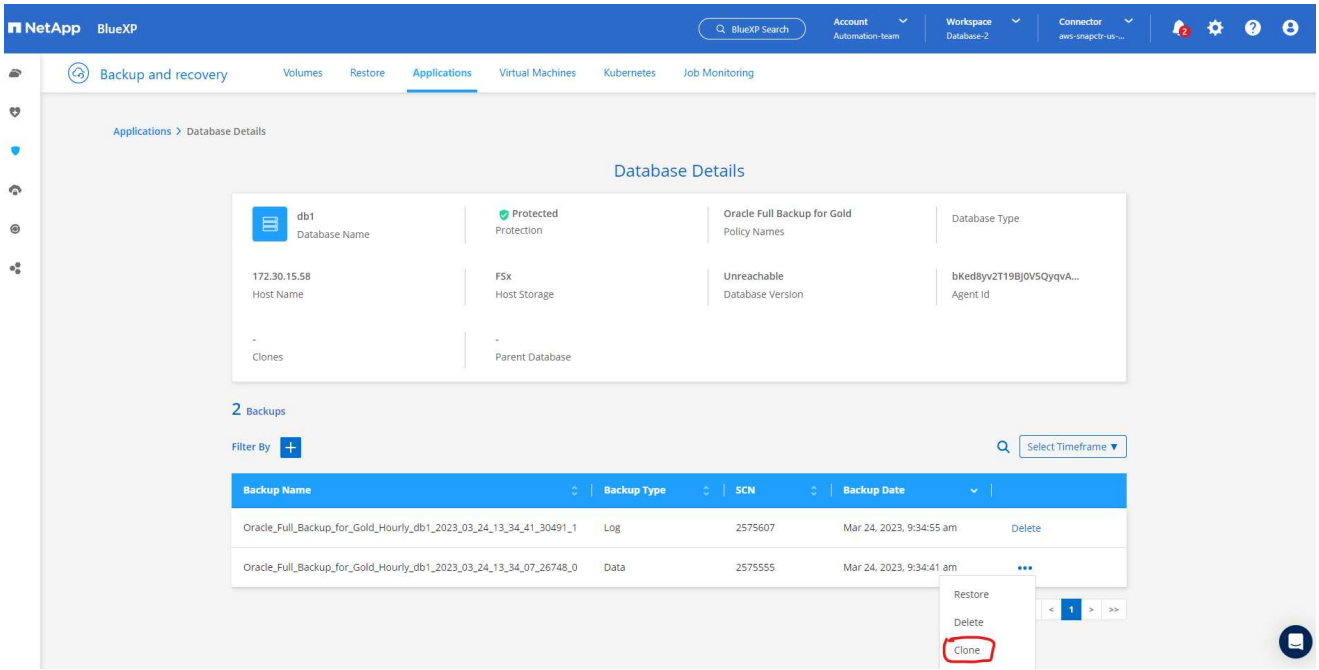




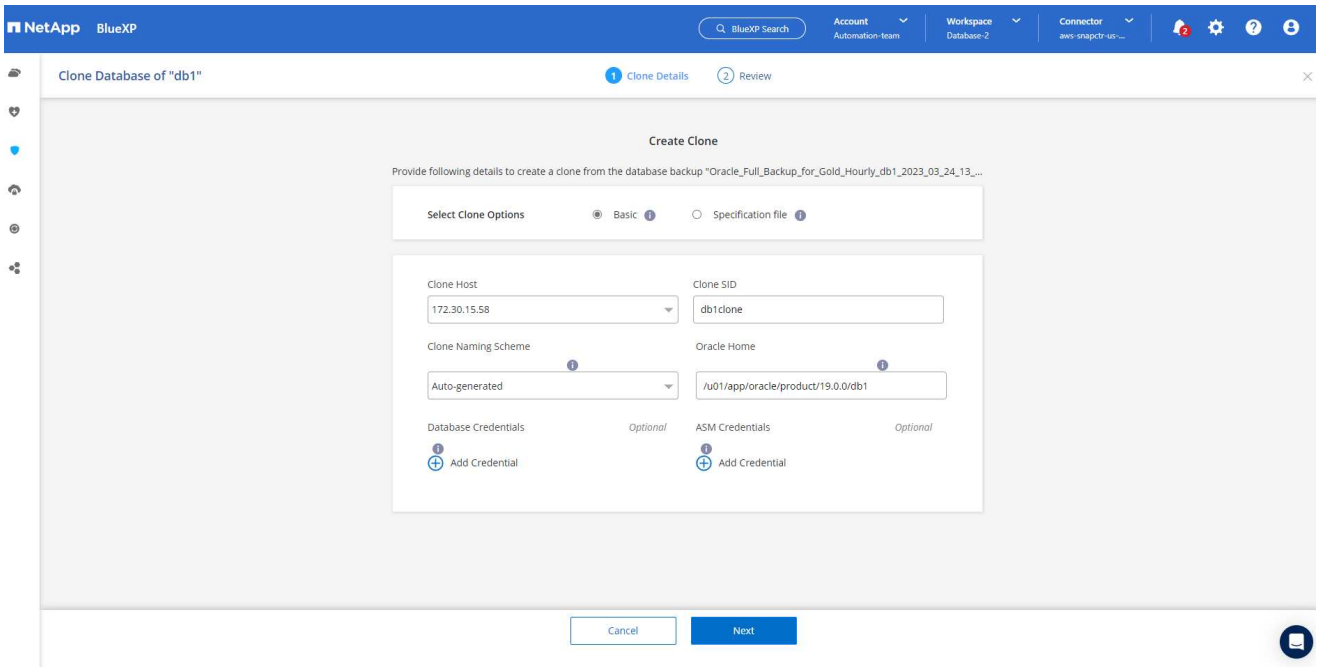
Clone de la base de données Oracle

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

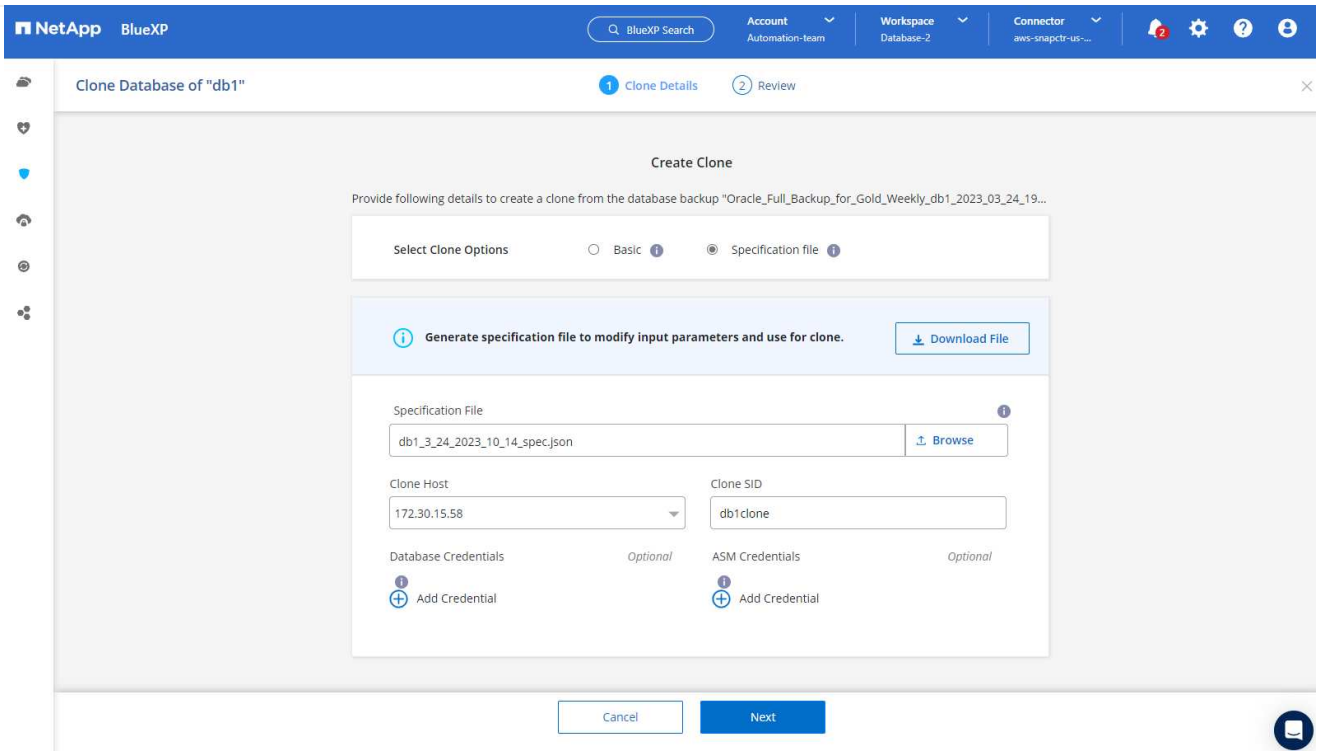
1. Sélectionnez la copie de sauvegarde de base de données appropriée, cliquez sur les trois points pour afficher le menu, puis choisissez l'option **Clone**.



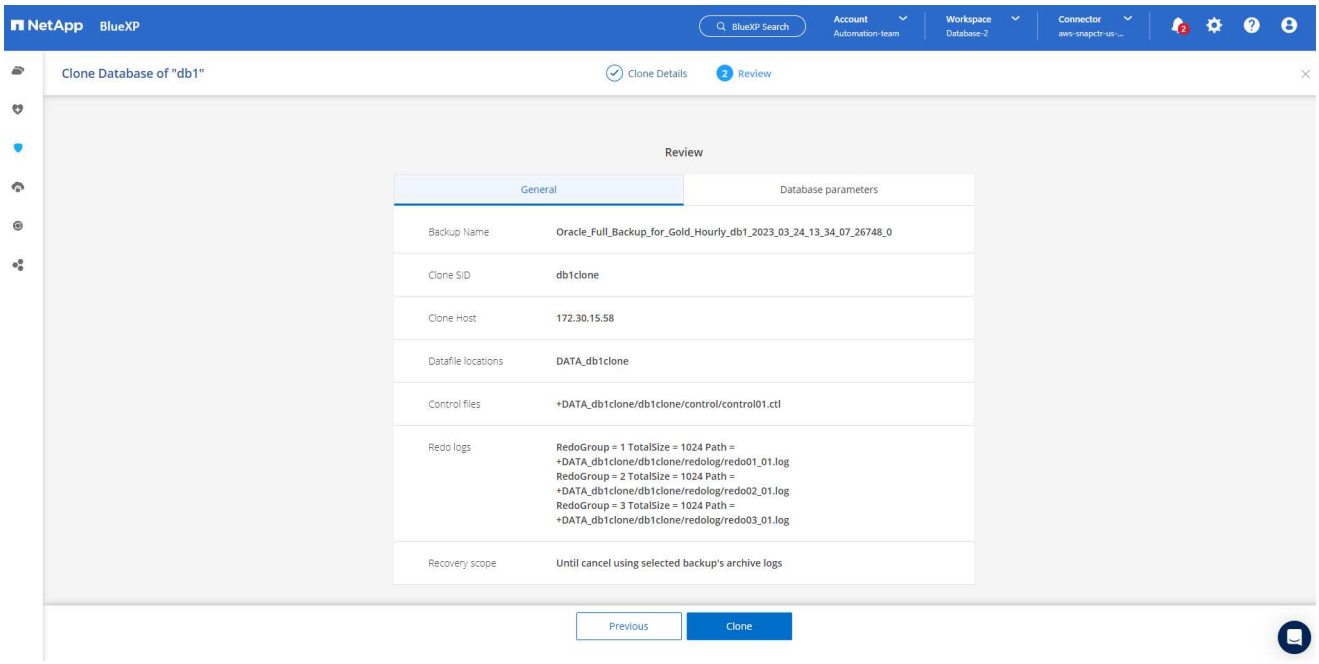
1. Sélectionnez l'option **Basic** si vous n'avez pas besoin de modifier les paramètres de base de données clonés.



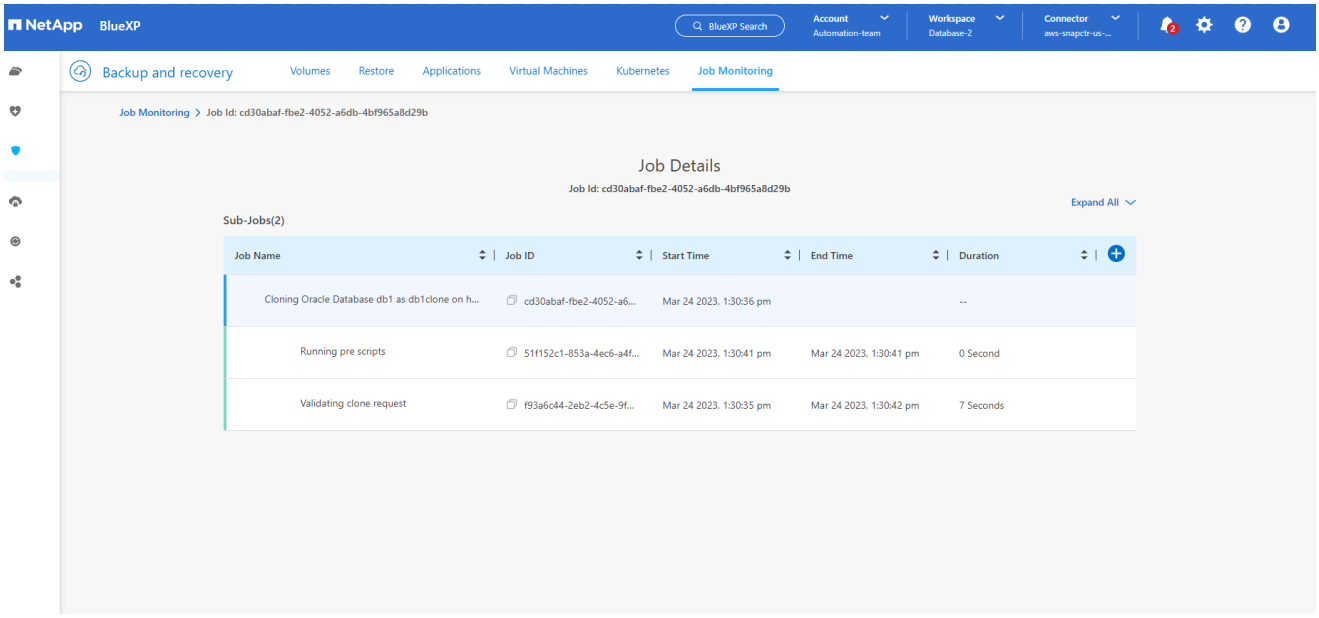
1. Vous pouvez également sélectionner **fichier de spécification**, ce qui vous donne la possibilité de télécharger le fichier init actuel, d'apporter des modifications, puis de le télécharger à nouveau dans le travail.



1. Vérifiez et lancez le travail.



1. Surveillez l’état du travail de clonage à partir de l’onglet **Job Monitoring**.



1. Validez la base de données clonée sur l’hôte d’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 supplémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Configuration et administration de BlueXP

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

- Documentation sur la sauvegarde et la restauration BlueXP

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

- Amazon FSX pour NetApp ONTAP

"https://aws.amazon.com/fsx/netapp-ontap/"

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

Solutions de base de données pour le cloud hybride avec SnapCenter

Tr-4908 : Présentation des solutions de base de données dans le cloud hybride avec SnapCenter

Alan Cao, Felix Melligan, NetApp

Cette solution fournit aux clients et aux équipes terrain de NetApp des instructions et des conseils pour configurer, exploiter et migrer les bases de données vers un environnement de cloud hybride à l'aide de l'outil graphique de NetApp SnapCenter et du service de stockage CVO pour les clouds publics pour les utilisations suivantes :

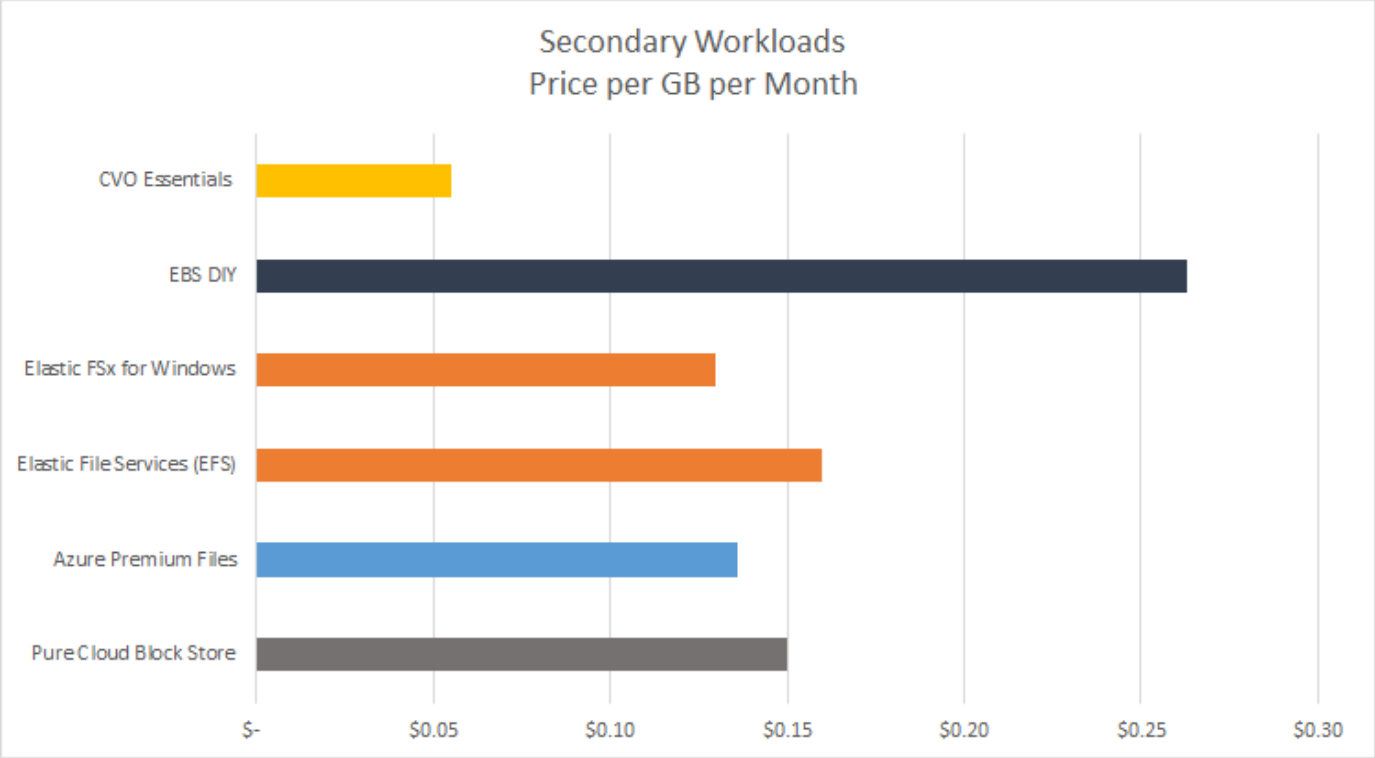
- Les opérations de développement et de test des bases de données dans le cloud hybride
- Reprise après incident des bases de données dans le cloud hybride

Aujourd'hui, de nombreuses bases de données d'entreprise résident toujours dans les data centers privés pour des raisons de performance, de sécurité et/ou autres. Cette solution de base de données de cloud hybride permet aux entreprises d'exploiter leurs bases de données principales sur site, tout en utilisant un cloud public pour les opérations des bases de données de développement/test, ainsi que pour la reprise après incident afin de réduire les coûts de licence et d'exploitation.

De nombreuses bases de données d'entreprise, comme Oracle, SQL Server, SAP HANA, etc., vos coûts de licence et d'exploitation sont élevés. De nombreux clients paient une licence unique et les coûts de support annuels en fonction du nombre de cœurs de calcul dans leur environnement de base de données, que les cœurs soient utilisés pour le développement, les tests, la production ou la reprise après incident. Il est possible que certains de ces environnements ne soient pas pleinement utilisés tout au long du cycle de vie des applications.

Ces solutions permettent aux clients de réduire le nombre de cœurs pouvant être concédants en déplaçant dans le cloud leurs environnements de base de données dédiés au développement, au test ou à la reprise après incident. Grâce à l'évolutivité du cloud public, la redondance, la haute disponibilité et un modèle de facturation basé sur la consommation, les économies réalisées en termes de licence et d'exploitation peuvent être importantes, sans sacrifier la disponibilité ou la facilité d'utilisation des applications.

Outre les économies potentielles en termes de licences pour les bases de données, le modèle de licence CVO basé sur la capacité de NetApp permet aux clients d'économiser les coûts de stockage par Go, tout en leur permettant de gérer de façon optimale les bases de données qui ne sont pas disponibles dans les services de stockage de la concurrence. Le tableau suivant montre une comparaison des coûts de stockage des services de stockage les plus courants disponibles dans le cloud public.



Cette solution montre que, grâce à l'outil logiciel avec interface graphique SnapCenter et à la technologie NetApp SnapMirror, les opérations de base de données de cloud hybride peuvent être facilement configurées, mises en œuvre et exploitées.

Les vidéos suivantes présentent SnapCenter en action :

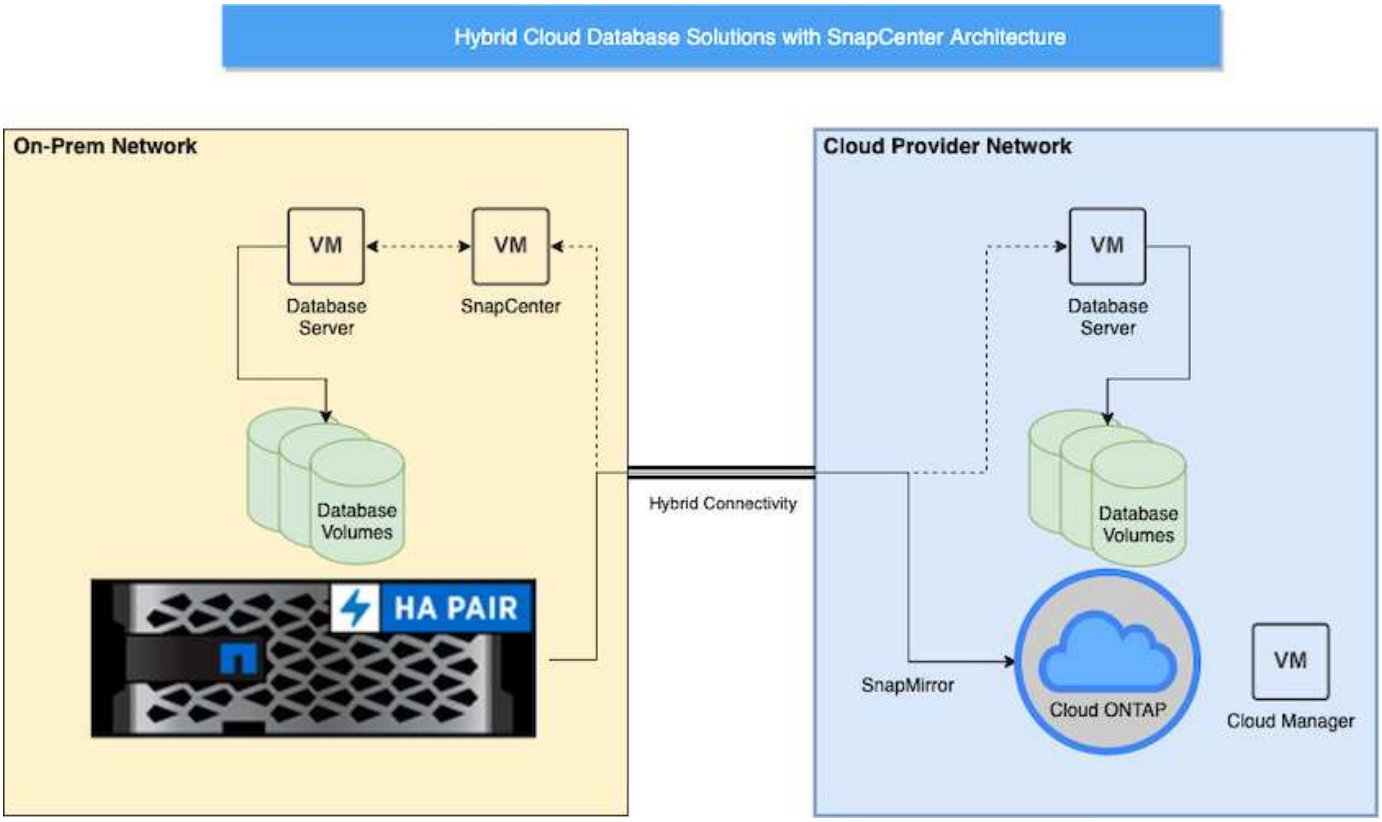
- "Sauvegarde d'une base de données Oracle sur un cloud hybride avec SnapCenter"
- "SnapCenter : clonez DES OPÉRATIONS DE DÉVELOPPEMENT/TEST dans AWS Cloud pour une base de données Oracle"

Bien que les illustrations de ce document montrent Cloud volumes ONTAP comme instance de stockage cible dans le cloud public, la solution est également entièrement validée pour la nouvelle version du moteur de stockage FSX ONTAP pour AWS.

Pour tester vous-même la solution et ses cas d'utilisation, un laboratoire NetApp sur demande SL10680 peut être demandé via le lien suivant : https://labondemand.netapp.com/lod3/labtest/request?nodeid=68761&destination=lod3/testlabs[TL_AWS_004 HCoD : AWS - NW, SnapCenter (Onsite)^.

Architecture de la solution

Le schéma d'architecture suivant illustre la mise en œuvre standard du fonctionnement des bases de données d'entreprise dans un cloud hybride pour les opérations de développement/test et de reprise après incident.



Dans des opérations business normales, les volumes synchronisés des bases de données dans le cloud peuvent être clonés et montés sur des instances de bases de données de développement/test pour le développement ou les tests d'applications. En cas de défaillance, les volumes de base de données synchronisés dans le cloud peuvent ensuite être activés pour la reprise d'activité.

Conditions requises pour le SnapCenter

Cette solution est conçue dans un environnement de cloud hybride pour prendre en charge les bases de données de production sur site pouvant atteindre l'ensemble des clouds publics populaires pour les opérations de développement/test et de reprise d'activité.

Cette solution prend en charge toutes les bases de données actuellement prises en charge par SnapCenter, bien que seules les bases de données Oracle et SQL Server soient démontrées ici. Cette solution est validée pour les charges de travail de base de données virtualisées, bien que les charges de travail sans système d'exploitation soient également prises en charge.

Nous supposons que les serveurs de base de données de production sont hébergés sur site et que les volumes BDD sont présentés aux hôtes BDD à partir d'un cluster de stockage ONTAP. Le logiciel SnapCenter est installé sur site pour la sauvegarde des bases de données et la réplication des données dans le cloud. Un contrôleur Ansible est recommandé, mais pas nécessaire pour l'automatisation du déploiement de bases de données ou la synchronisation de la configuration des bases de données et des noyaux du système

d'exploitation avec une instance de reprise d'activité en attente ou des instances de développement/test dans le cloud public.

De formation

De production	De formation
Sur place	Toutes les bases de données et versions prises en charge par SnapCenter
	SnapCenter v4.4 ou version ultérieure
	Ansible v2.09 ou version ultérieure
	Cluster ONTAP 9.x
	LIFs intercluster configurées
	Connectivité sur site vers un VPC dans le cloud (VPN, interconnexion, etc.)
	Ports réseau ouverts - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
Cloud - AWS	"Connecteur Cloud Manager"
	"Cloud Volumes ONTAP"
	Correspondance des instances EC2 du système d'exploitation de base de données avec sur site
Cloud - Azure	"Connecteur Cloud Manager"
	"Cloud Volumes ONTAP"
	Correspondance des serveurs virtuels Azure du système d'exploitation de base de données sur site
Cloud - GCP	"Connecteur Cloud Manager"
	"Cloud Volumes ONTAP"
	Mise en correspondance des instances de DB OS Google Compute Engine avec sur site

Configuration des prérequis

Certaines conditions préalables doivent être configurées à la fois sur site et dans le cloud avant d'exécuter des workloads de base de données de cloud hybride. La section suivante fournit un résumé de ce processus de haut niveau et les liens suivants fournissent des informations supplémentaires sur la configuration du système nécessaire.

Sur site

- Installation et configuration de SnapCenter
- Configuration du stockage du serveur de bases de données sur site
- Licences requises
- Mise en réseau et sécurité
- Automatisation

Cloud public

- Identifiant NetApp Cloud Central
- Accès au réseau à partir d'un navigateur Web vers plusieurs noeuds finaux
- Emplacement réseau d'un connecteur
- Les autorisations du fournisseur cloud
- Mise en réseau pour des services individuels

Remarques importantes :

1. Où déployer Cloud Manager Connector ?
2. Architecture et dimensionnement de Cloud volumes ONTAP
3. Un seul nœud ou une haute disponibilité ?

Vous trouverez des informations supplémentaires sur les liens suivants :

"Sur site"

"Cloud public"

Conditions préalables sur site

Pour préparer l'environnement de workload de base de données de cloud hybride SnapCenter, les tâches suivantes doivent être réalisées sur site.

Installation et configuration de SnapCenter

L'outil NetApp SnapCenter est une application Windows qui s'exécute généralement dans un environnement de domaine Windows, mais aussi dans un déploiement de groupe de travail. Elle est basée sur une architecture multiniveaux, incluant un serveur de gestion centralisée (le serveur SnapCenter) et un plug-in SnapCenter sur les hôtes du serveur de base de données pour les charges de travail de la base de données. Voici quelques éléments à prendre en compte pour le déploiement du cloud hybride.

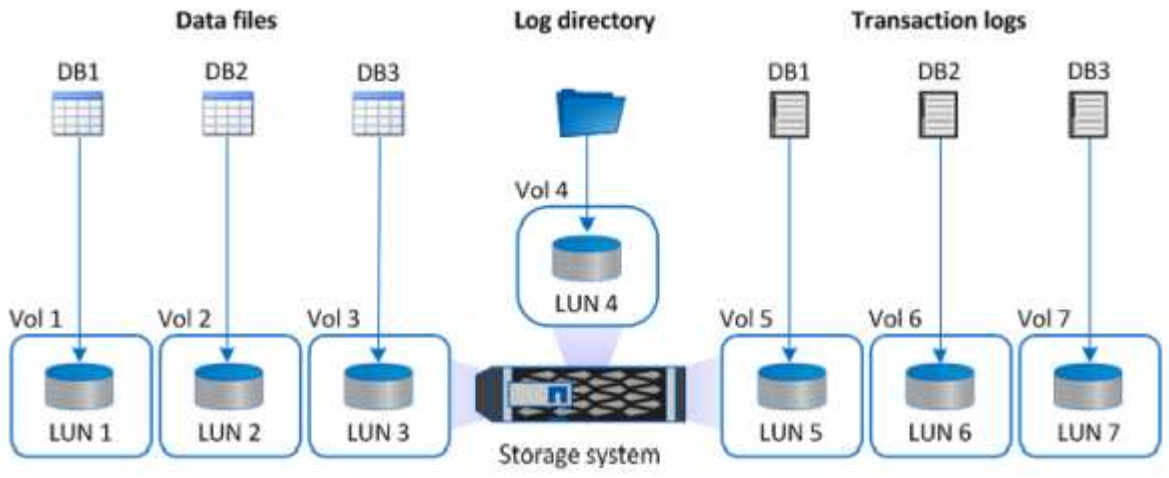
- **Déploiement d'instance unique ou de haute disponibilité.** le déploiement de haute disponibilité fournit une redondance en cas de défaillance d'un serveur d'instance SnapCenter unique.
- **Résolution du nom.** le DNS doit être configuré sur le serveur SnapCenter pour résoudre tous les hôtes de base de données ainsi que sur le SVM de stockage pour la recherche avant et arrière. Le serveur DNS doit également être configuré sur des serveurs de base de données pour résoudre le serveur SnapCenter et la SVM de stockage pour la recherche avant et arrière.
- **Configuration du contrôle d'accès basé sur les rôles (RBAC).** pour les charges de travail de bases de données mixtes, vous pouvez utiliser RBAC pour isoler la responsabilité de gestion de différentes plates-formes de bases de données telles qu'une base de données admin pour Oracle ou un administrateur pour SQL Server. Les autorisations nécessaires doivent être accordées à l'utilisateur DB admin.
- **Activer la stratégie de sauvegarde basée sur des stratégies.** pour renforcer la cohérence et la fiabilité des sauvegardes.
- **Ouvrez les ports réseau nécessaires sur le pare-feu.** pour que le serveur SnapCenter sur site communique avec les agents installés sur l'hôte DB cloud.
- **Les ports doivent être ouverts pour permettre le trafic SnapMirror entre le cloud sur site et le cloud public.** le serveur SnapCenter utilise ONTAP SnapMirror pour répliquer les sauvegardes Snapshot sur site vers les SVM de stockage Cloud volumes ONTAP.

Après avoir soigneusement étudié et planifié la pré-installation, cliquez sur ce bouton "Workflow d'installation de SnapCenter" Pour plus d'informations sur l'installation et la configuration de SnapCenter.

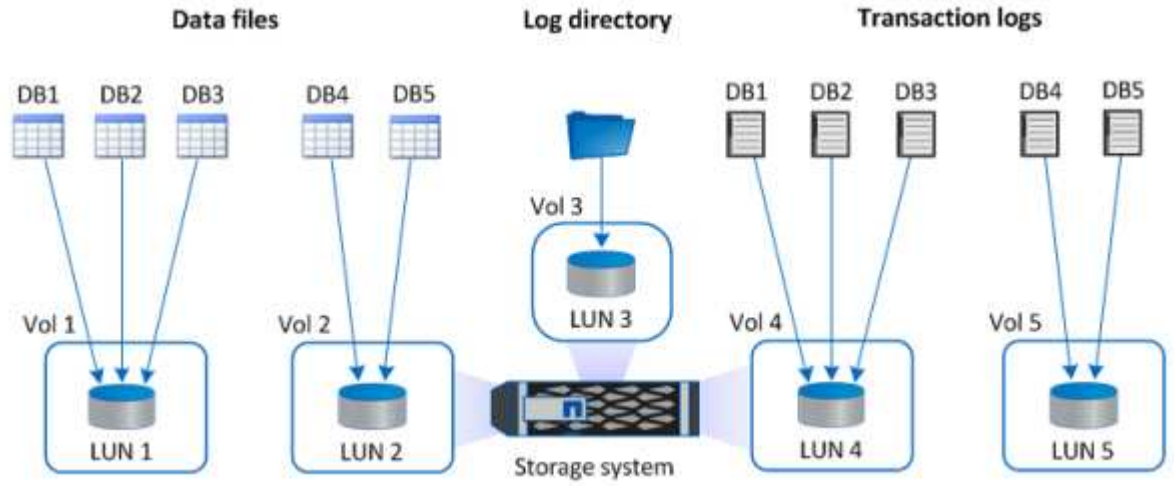
Configuration du stockage du serveur de bases de données sur site

Les performances du stockage jouent un rôle important dans les performances globales des bases de données et des applications. Une disposition de stockage bien conçue peut non seulement améliorer les performances de la base de données, mais aussi faciliter la gestion de la sauvegarde et de la restauration de la base de données. Plusieurs facteurs doivent être pris en compte lors de la définition de l'organisation du stockage, notamment la taille de la base de données, le taux de modification attendu des données pour la base de données et la fréquence avec laquelle vous effectuez des sauvegardes.

En reliant directement des LUN de stockage à la machine virtuelle invitée par NFS ou iSCSI pour les charges de travail de bases de données virtualisées, vous bénéficiez généralement de performances supérieures à celles du stockage alloué via VMDK. NetApp recommande l'organisation de stockage d'une importante base de données SQL Server sur les LUN décrits dans la figure suivante.



La figure suivante présente l'organisation de stockage recommandée par NetApp pour les bases de données SQL Server de petite ou moyenne taille sur des LUN.

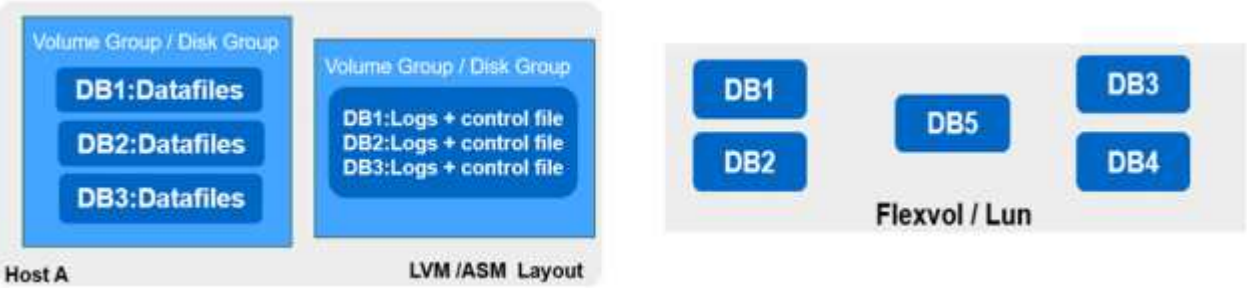


Le répertoire des journaux est dédié à SnapCenter pour effectuer une synthèse du journal des transactions pour la récupération de la base de données. Pour une base de données très volumineuse, plusieurs LUN peuvent être allouées à un volume pour améliorer les performances.

Pour les charges de travail de bases de données Oracle, SnapCenter prend en charge les environnements de bases de données bénéficiant d'un stockage ONTAP monté sur l'hôte en tant que périphériques physiques ou virtuels. Vous pouvez héberger toute la base de données sur un ou plusieurs périphériques de stockage en fonction du caractère stratégique de l'environnement. Généralement, les clients isolent les fichiers de données sur un système de stockage dédié de tous les autres fichiers comme les fichiers de contrôle, les fichiers de reprise et les fichiers journaux d'archivage. Cela permet aux administrateurs de restaurer rapidement (ONTAP Single-File SnapRestore) ou de cloner une grande base de données stratégique (de plusieurs pétaoctets) à l'aide de la technologie Snapshot en quelques secondes à quelques minutes.

Pour optimiser la latence, un volume de stockage dédié doit être déployé sur différents types de fichiers Oracle afin d'optimiser la latence. Pour une grande base de données, plusieurs LUN (NetApp recommande jusqu'à huit) par volume doivent être alloués aux fichiers de données.

Pour les bases de données Oracle plus petites, SnapCenter prend en charge les dispositions de stockage partagé dans lesquelles vous pouvez héberger plusieurs bases de données ou faire partie d'une base de données sur le même volume de stockage ou LUN. Par exemple, vous pouvez héberger des fichiers de données pour toutes les bases de données d'un groupe de disques + DATA ASM ou d'un groupe de volumes. Le reste des fichiers (fichiers de reprise, journaux d'archivage et fichiers de contrôle) peut être hébergé sur un autre groupe de disques ou groupe de volumes dédié (LVM). Un tel scénario de déploiement est illustré ci-dessous.



Pour faciliter la relocalisation des bases de données Oracle, le binaire Oracle doit être installé sur un LUN distinct inclus dans la stratégie de sauvegarde régulière. Cela permet de garantir que, dans le cas du transfert

de la base de données vers un nouvel hôte serveur, la pile Oracle peut être démarrée pour la restauration sans problèmes potentiels dus à un binaire Oracle désynchronisé.

Licences requises

SnapCenter est un logiciel sous licence de NetApp. Elle est généralement incluse dans une licence ONTAP sur site. Cependant, pour le déploiement d'un cloud hybride, une licence cloud pour SnapCenter doit également ajouter CVO à SnapCenter comme destination de réplication des données cible. Veuillez consulter les liens ci-dessous pour en savoir plus sur la licence standard basée sur la capacité SnapCenter :

"Licences standard basées sur la capacité SnapCenter"

Mise en réseau et sécurité

Dans le cas d'une base de données de production sur site nécessitant une stabilité accrue dans le cloud pour les opérations de développement/test et de reprise d'activité, la mise en réseau et la sécurité sont des facteurs essentiels à prendre en compte lors de la configuration de l'environnement et de la connexion au cloud public à partir d'un data Center sur site.

Les clouds publics utilisent généralement un cloud privé virtuel (VPC) pour isoler différents utilisateurs au sein d'une plateforme de cloud public. Au sein d'un VPC individuel, la sécurité est contrôlée à l'aide de mesures telles que des groupes de sécurité configurables en fonction des besoins des utilisateurs pour le verrouillage d'un VPC.

La connectivité entre le data Center sur site et le VPC peut être sécurisée via un tunnel VPN. Sur la passerelle VPN, la sécurité peut être renforcée à l'aide de règles NAT et de pare-feu qui bloquent les tentatives d'établissement de connexions réseau à partir d'hôtes sur Internet vers des hôtes à l'intérieur du data Center de l'entreprise.

Pour les considérations relatives au réseau et à la sécurité, consultez les règles Cloud volumes ONTAP entrantes et sortantes pour votre cloud public :

- "Règles du groupe de sécurité pour CVO - AWS"
- "Règles du groupe de sécurité pour CVO - Azure"
- "Règles de pare-feu pour CVO - GCP"

Utilisation de l'automatisation Ansible pour la synchronisation facultative des instances de BDD entre l'environnement sur site et le cloud

Pour simplifier la gestion d'un environnement de base de données de cloud hybride, NetApp vous recommande vivement, mais ne vous demande pas de déployer un contrôleur Ansible afin d'automatiser certaines tâches de gestion, comme le maintien des instances de calcul sur site et dans le cloud en mode synchrone. Cela est particulièrement important, car une instance de calcul désynchronisée dans le cloud peut entraîner l'erreur de la base de données récupérée dans le cloud en raison de l'absence de packages du noyau et d'autres problèmes.

La fonctionnalité d'automatisation d'un contrôleur Ansible peut également être utilisée pour étendre SnapCenter à certaines tâches, comme l'interruption de l'instance SnapMirror pour activer la copie de données de reprise après incident en production.

Suivez ces instructions pour configurer votre nœud de contrôle Ansible pour les machines RedHat ou CentOS : "Configuration du contrôleur Red Hat/CentOS Ansible". Suivez ces instructions pour configurer votre nœud de contrôle Ansible pour les machines Ubuntu ou Debian : "Configuration du contrôleur Ansible Ubuntu/Debian".

Conditions préalables au cloud public

Avant d'installer Cloud Manager Connector et Cloud Volumes ONTAP et de configurer SnapMirror, nous devons préparer notre environnement cloud. Cette page décrit le travail à effectuer, ainsi que les considérations relatives au déploiement de Cloud Volumes ONTAP.

Liste de contrôle des conditions préalables au déploiement de Cloud Manager et de Cloud Volumes ONTAP

- Identifiant NetApp Cloud Central
- Accès au réseau à partir d'un navigateur Web vers plusieurs noeuds finaux
- Emplacement réseau d'un connecteur
- Les autorisations du fournisseur cloud
- Mise en réseau pour des services individuels

Pour en savoir plus sur ce dont vous avez besoin pour démarrer, consultez le site "documentation cloud".

Considérations

1. Qu'est-ce qu'un connecteur Cloud Manager ?

Dans la plupart des cas, un administrateur de compte Cloud Central doit déployer un connecteur dans votre réseau cloud ou sur site. Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Pour plus d'informations sur les connecteurs, visitez notre "documentation cloud".

2. Dimensionnement et architecture de Cloud Volumes ONTAP

Lors du déploiement de Cloud Volumes ONTAP, vous avez le choix entre un package prédéfini ou la création de votre propre configuration. Bon nombre de ces valeurs peuvent être modifiées ultérieurement, sans interrompre l'activité, mais certaines décisions clés doivent être prises avant le déploiement, en fonction des charges de travail à déployer dans le cloud.

Chaque fournisseur de cloud propose différentes options de déploiement et chaque workload dispose de ses propres propriétés. NetApp a une "Outil de dimensionnement CVO" cela peut aider à dimensionner correctement les déploiements en fonction de la capacité et des performances, mais il a été conçu autour de certains concepts de base qui méritent d'être pris en compte :

- Capacité requise
- Capacité réseau de la machine virtuelle du cloud
- Les caractéristiques de performances du stockage cloud

L'essentiel est de planifier une configuration qui non seulement répond aux besoins actuels en termes de capacité et de performances, mais qui étudie également la croissance future. Ce chiffre est généralement appelé marge de capacité et marge de performance.

Si vous souhaitez des informations complémentaires, lisez la documentation sur la planification correcte "AWS", "Azure", et "GCP".

3. Un seul nœud ou haute disponibilité ?

Dans tous les clouds, il est possible de déployer Cloud volumes ONTAP dans un seul nœud ou dans une paire haute disponibilité en cluster avec deux nœuds. Selon le cas de figure, vous pouvez déployer un nœud unique pour réduire les coûts ou une paire haute disponibilité pour améliorer la disponibilité et la redondance.

Pour une reprise après incident ou l'exécution de systèmes de stockage temporaires pour le développement et le test, des nœuds uniques sont courants, car l'impact d'une panne d'infrastructure soudaine ou d'un zone est moindre. Toutefois, pour toutes les utilisations de production, et lorsque les données ne se trouvent que dans un seul emplacement ou que le dataset doit avoir plus de redondance et de disponibilité, la haute disponibilité est recommandée.

Pour plus d'informations sur l'architecture de la version haute disponibilité de chaque Cloud, consultez la documentation pour "AWS", "Azure" et "GCP".

Présentation de mise en route

Cette section présente un récapitulatif des tâches à accomplir pour répondre aux exigences préalables requises, comme indiqué dans la section précédente. La section suivante énumère les tâches générales, à la fois pour les opérations sur site et dans le cloud public. Les processus et procédures détaillés sont accessibles en cliquant sur les liens correspondants.

Sur site

- Configurer l'utilisateur admin de la base de données dans SnapCenter
- Conditions préalables à l'installation du plug-in SnapCenter
- Installation du plug-in hôte SnapCenter
- Découverte de ressources DE BASE DE DONNÉES
- Configuration de la réplication du volume de peering de clusters et de BDD
- Ajouter le SVM de stockage de base de données CVO à SnapCenter
- Configurez la stratégie de sauvegarde de la base de données dans SnapCenter
- Mise en œuvre d'une stratégie de sauvegarde pour protéger la base de données
- Validation de la sauvegarde

Cloud public AWS

- Contrôle avant vol
- Étapes de déploiement de Cloud Manager et de Cloud Volumes ONTAP dans AWS
- Déployez l'instance de calcul EC2 pour les workloads de base de données

Cliquez sur les liens suivants pour plus d'informations :

"Sur site", "Cloud public - AWS"

Pour commencer sur site

L'outil NetApp SnapCenter utilise le contrôle d'accès basé sur des rôles (RBAC) pour

gérer l'accès aux ressources utilisateur et les autorisations, et l'installation d'SnapCenter crée des rôles préremplis. Vous pouvez également créer des rôles personnalisés en fonction de vos besoins ou de vos applications.

Sur site

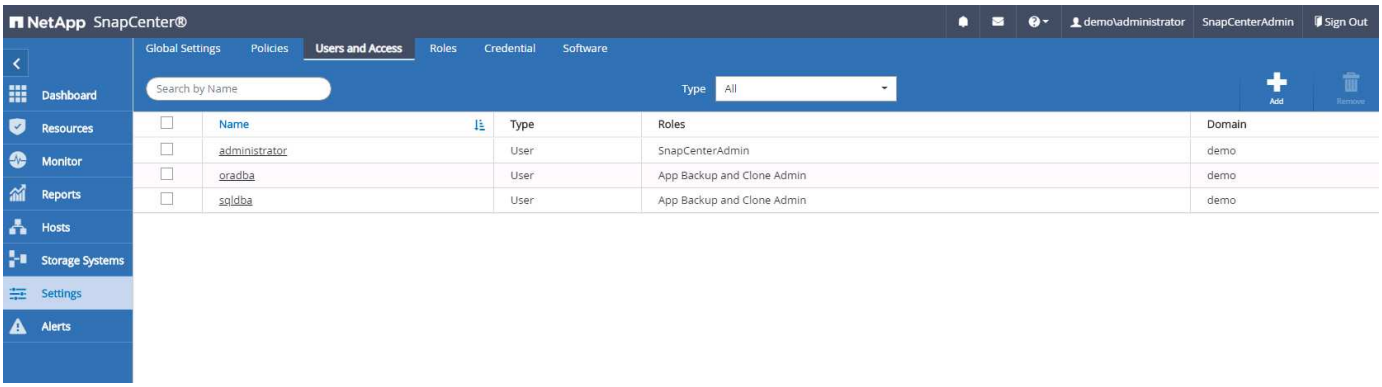
1. Configurer l'utilisateur administrateur de la base de données dans SnapCenter

Il est judicieux de disposer d'un ID utilisateur d'administration dédié pour chaque plateforme de base de données prise en charge par SnapCenter pour la sauvegarde, la restauration de bases de données et/ou la reprise après incident. Vous pouvez également utiliser un ID unique pour gérer toutes les bases de données. Dans nos tests de cas et notre démonstration, nous avons créé un utilisateur administratif dédié respectivement à Oracle et à SQL Server.

Certaines ressources SnapCenter ne peuvent être provisionnées que avec le rôle SnapCenter. Les ressources peuvent ensuite être attribuées à d'autres ID d'utilisateur pour l'accès.

Dans un environnement SnapCenter sur site préinstallé et configuré, les tâches suivantes peuvent déjà avoir été effectuées. Si ce n'est pas le cas, procédez comme suit pour créer un utilisateur administrateur de base de données :

1. Ajoutez l'utilisateur admin à Windows Active Directory.
2. Connectez-vous à SnapCenter à l'aide d'un ID attribué avec le rôle SnapCenterAdmin.
3. Accédez à l'onglet accès sous Paramètres et utilisateurs, puis cliquez sur Ajouter pour ajouter un nouvel utilisateur. Le nouvel ID utilisateur est lié à l'utilisateur admin créé dans Windows Active Directory à l'étape 1. . Attribuez le rôle approprié à l'utilisateur selon les besoins. Affectez des ressources à l'utilisateur administrateur, le cas échéant.



2. Conditions préalables à l'installation du plug-in SnapCenter

SnapCenter effectue des sauvegardes, des restaurations, des clones et d'autres fonctions à l'aide d'un agent de plug-in exécuté sur les hôtes de base de données. Il se connecte à l'hôte et à la base de données via les informations d'identification configurées sous l'onglet Paramètres et informations d'identification pour l'installation du plug-in et d'autres fonctions de gestion. Il existe des conditions de privilège spécifiques en fonction du type d'hôte cible, tel que Linux ou Windows, ainsi que du type de base de données.

Les informations d'identification des hôtes DB doivent être configurées avant l'installation du plug-in SnapCenter. En général, vous souhaitez utiliser un compte d'utilisateur administrateur sur l'hôte DB comme informations d'identification de connexion hôte pour l'installation du plug-in. Vous pouvez également attribuer le même ID utilisateur pour l'accès à la base de données à l'aide de l'authentification basée sur le système d'exploitation. En revanche, vous pouvez également utiliser l'authentification de base de données avec

différents ID d'utilisateur de base de données pour l'accès à la gestion de base de données. Si vous décidez d'utiliser l'authentification basée sur le système d'exploitation, l'ID utilisateur admin du système d'exploitation doit disposer d'un accès DB. Pour l'installation de SQL Server sous domaine Windows, un compte d'administrateur de domaine peut être utilisé pour gérer tous les serveurs SQL du domaine.

Hôte Windows pour SQL Server :

1. Si vous utilisez des informations d'identification Windows pour l'authentification, vous devez configurer vos informations d'identification avant d'installer des plug-ins.
2. Si vous utilisez une instance SQL Server pour l'authentification, vous devez ajouter les informations d'identification après avoir installé des plug-ins.
3. Si vous avez activé l'authentification SQL lors de la configuration des informations d'identification, l'instance ou la base de données découverte s'affiche avec une icône de verrouillage rouge. Si l'icône de verrouillage apparaît, vous devez spécifier les informations d'identification de l'instance ou de la base de données pour pouvoir ajouter l'instance ou la base de données à un groupe de ressources.
4. Vous devez affecter ces informations d'identification à un utilisateur RBAC sans accès sysadmin lorsque les conditions suivantes sont remplies :
    - Les informations d'identification sont affectées à une instance SQL.
    - L'instance ou l'hôte SQL est affecté à un utilisateur RBAC.
    - L'utilisateur administrateur de BD RBAC doit disposer à la fois du groupe de ressources et des privilèges de sauvegarde.

Hôte UNIX pour Oracle :

1. Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root en modifiant sshd.conf et en redémarrant le service sshd. L'authentification SSH basée sur le mot de passe sur une instance AWS est désactivée par défaut.
2. Configurez les privilèges sudo pour que l'utilisateur non-root installe et démarre le processus de plug-in. Après avoir installé le plug-in, les processus s'exécutent en tant qu'utilisateur root efficace.
3. Créez des informations d'identification avec le mode d'authentification Linux pour l'utilisateur d'installation.
4. Vous devez installer Java 1.8.x (64 bits) sur votre hôte Linux.
5. L'installation du plug-in de base de données Oracle installe également le plug-in SnapCenter pour Unix.

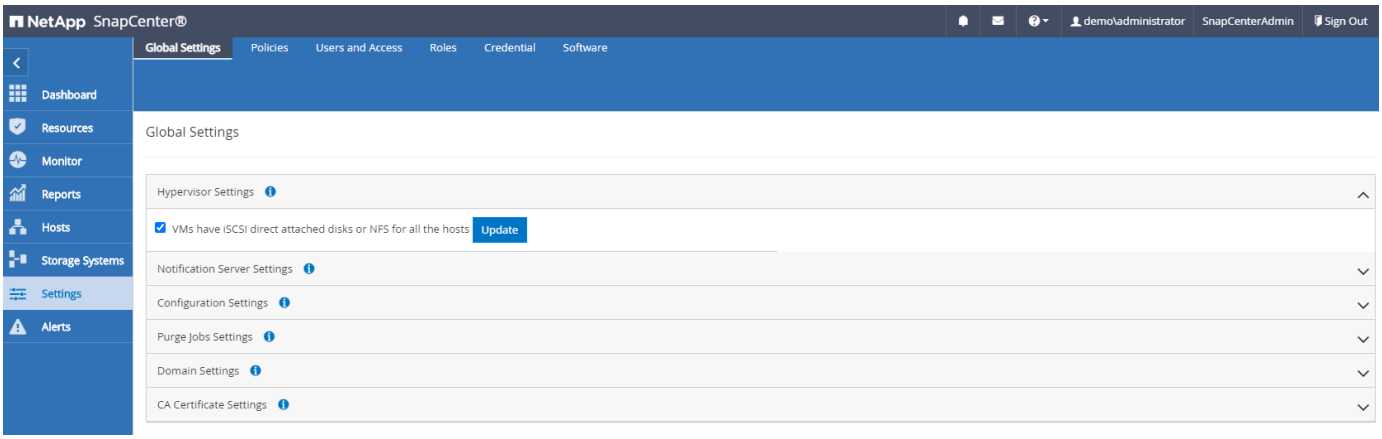
3. Installation du plug-in hôte SnapCenter

> Avant de tenter d'installer des plug-ins SnapCenter sur des instances de serveur BDD cloud, assurez-vous que toutes les étapes de configuration sont terminées, comme indiqué dans la section cloud appropriée pour le déploiement de l'instance de calcul.

Les étapes suivantes illustrent la manière dont un hôte de base de données est ajouté à SnapCenter pendant qu'un plug-in SnapCenter est installé sur l'hôte. La procédure s'applique à l'ajout d'hôtes sur site et d'hôtes cloud. La démonstration suivante ajoute un hôte Windows ou Linux résidant dans AWS.

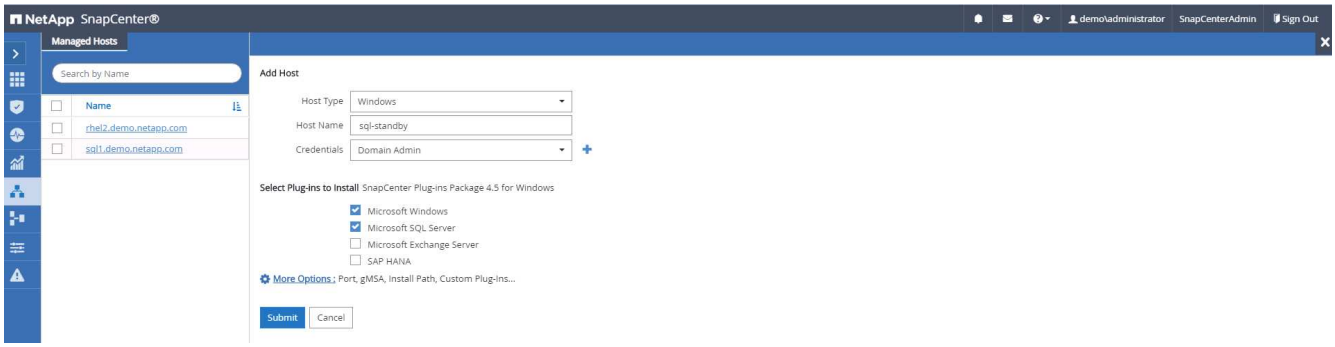
Configurez les paramètres globaux de SnapCenter VMware

Accédez à Paramètres > Paramètres globaux. Sous Paramètres de l'hyperviseur, sélectionnez « les machines virtuelles ont des disques iSCSI à connexion directe ou NFS pour tous les hôtes », puis cliquez sur mettre à jour.



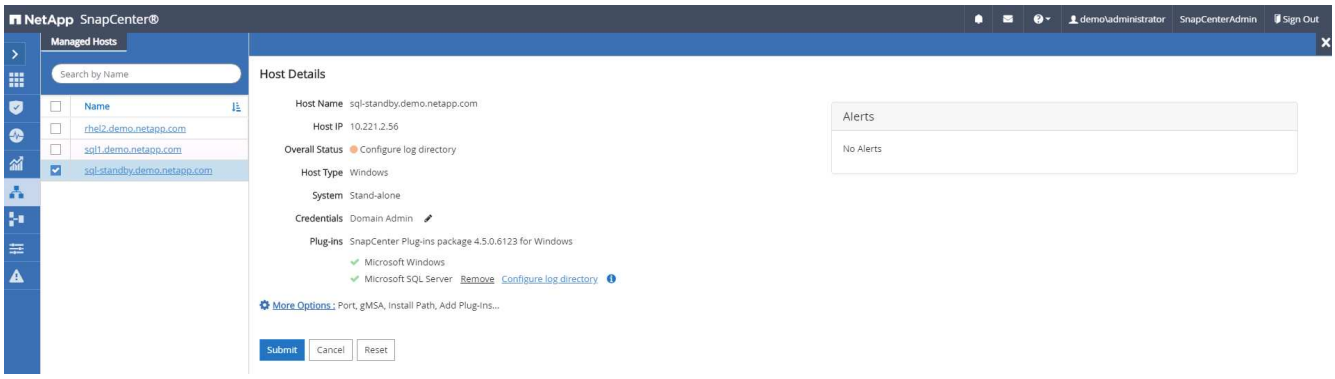
Ajoutez l'hôte Windows et l'installation du plug-in sur l'hôte

1. Connectez-vous à SnapCenter avec un ID utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet hôtes dans le menu de gauche, puis cliquez sur Ajouter pour ouvrir le flux de travail Ajouter hôte.
3. Choisissez Windows pour le type d'hôte ; le nom d'hôte peut être un nom d'hôte ou une adresse IP. Le nom d'hôte doit être résolu à l'adresse IP d'hôte correcte de l'hôte SnapCenter. Choisissez les informations d'identification de l'hôte créées à l'étape 2. Choisissez Microsoft Windows et Microsoft SQL Server comme modules d'extension à installer.

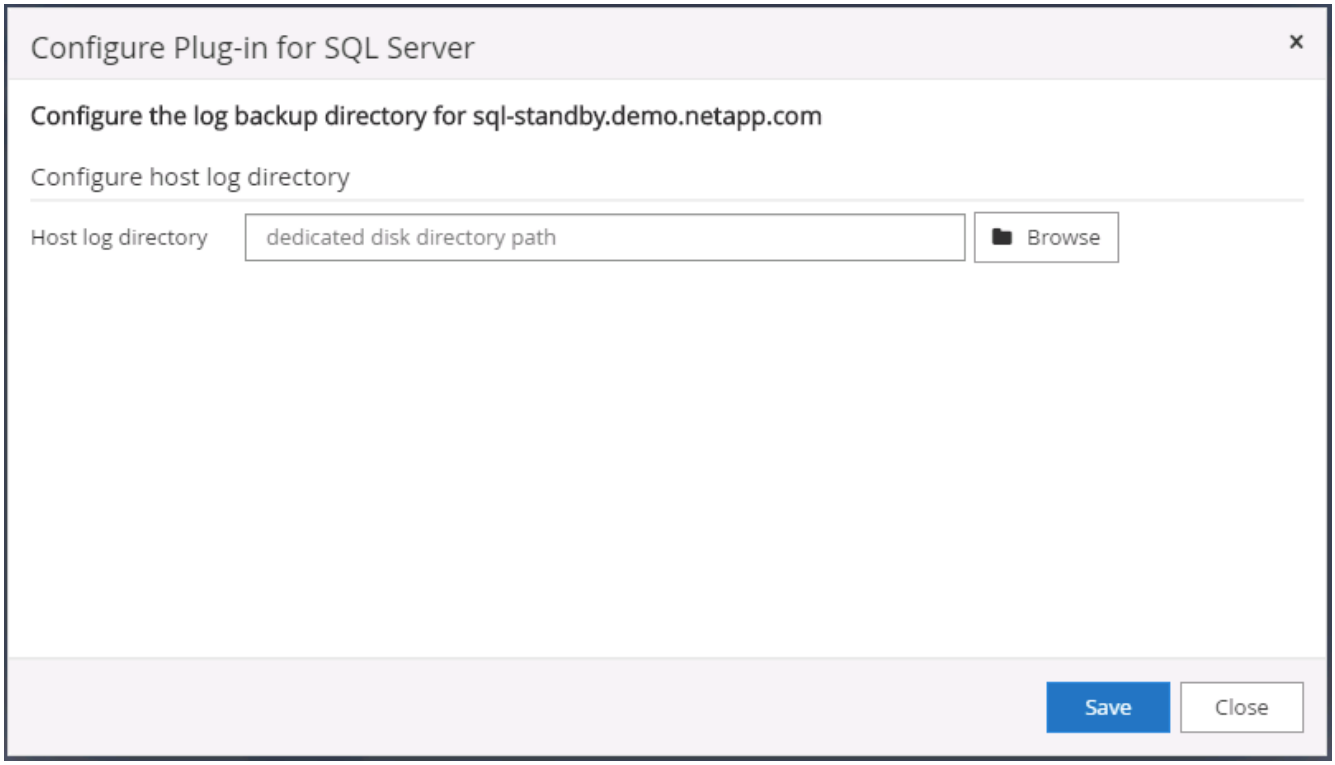


4. Une fois le plug-in installé sur un hôte Windows, son état global s'affiche sous la forme "configurer le répertoire du journal".

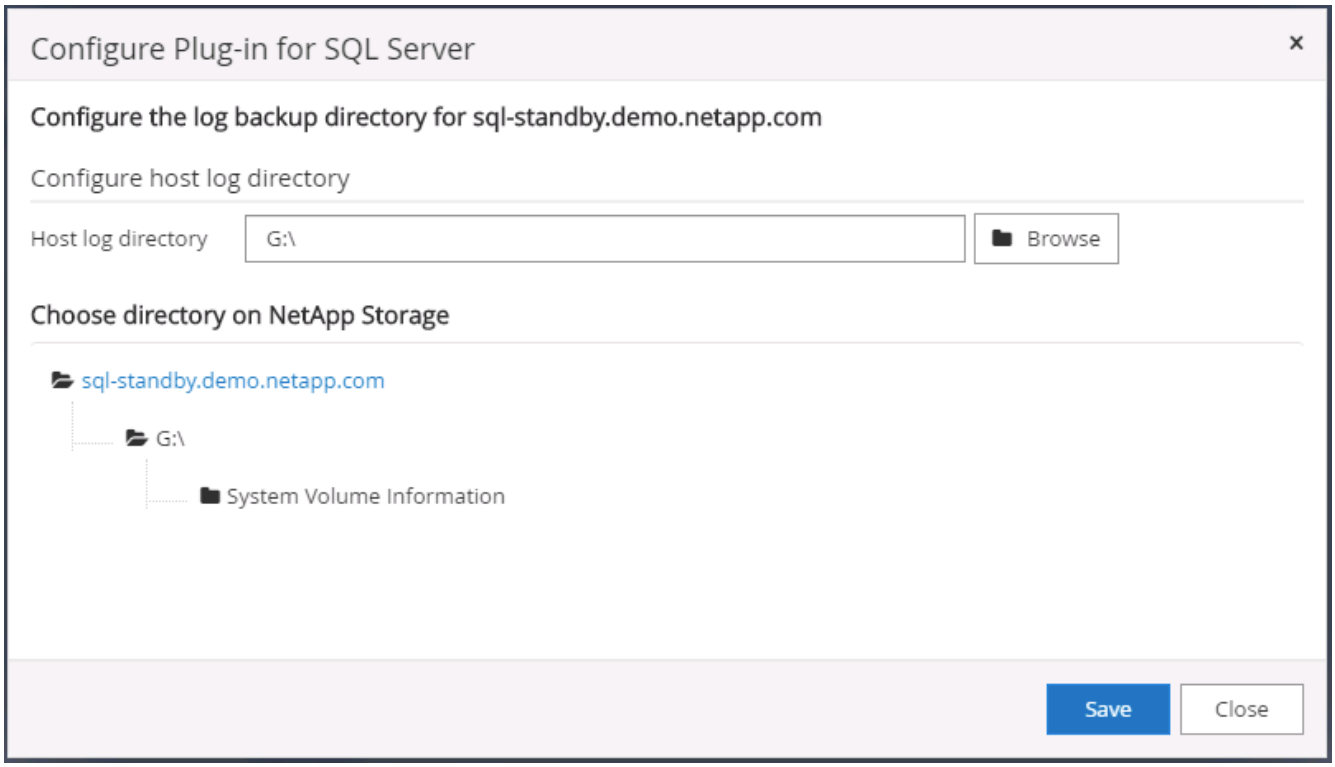
5. Cliquez sur le nom d'hôte pour ouvrir la configuration du répertoire du journal de SQL Server.



6. Cliquez sur « configurer le répertoire du journal » pour ouvrir « configurer le plug-in pour SQL Server ».

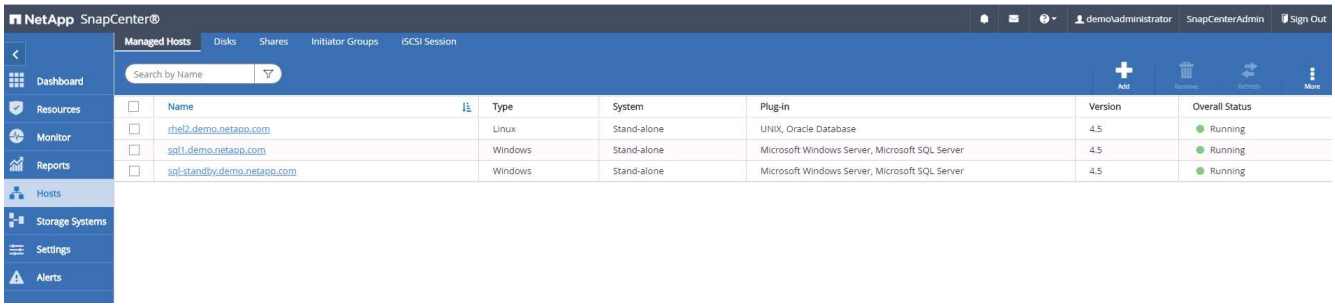


7. Cliquez sur Parcourir pour découvrir le stockage NetApp afin de définir un répertoire de journaux ; SnapCenter utilise ce répertoire de journaux pour restaurer les fichiers journaux de transactions du serveur SQL. Cliquez ensuite sur Enregistrer.

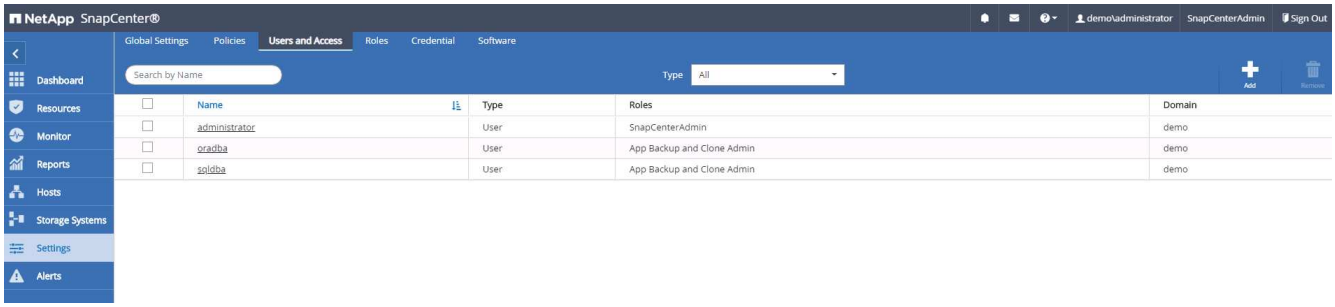


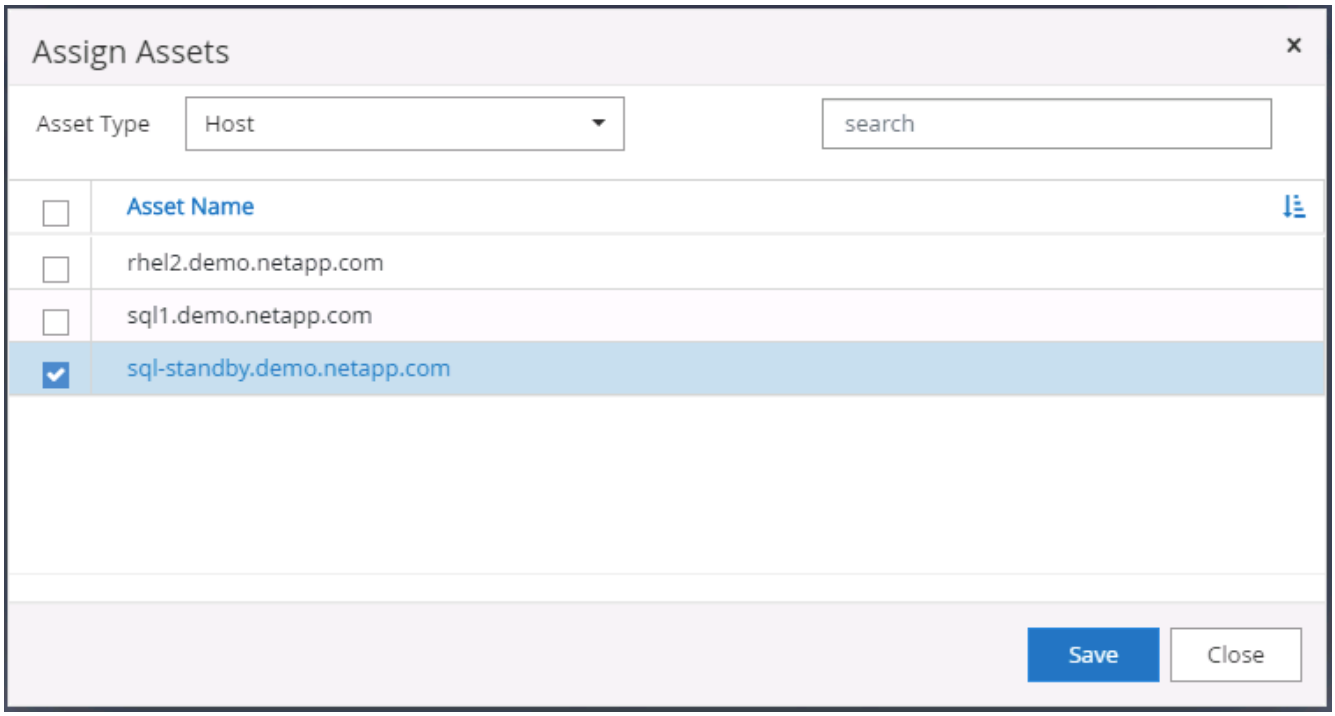
Pour que le stockage NetApp provisionné sur un hôte de base de données soit découvert, le stockage (sur site ou CVO) doit être ajouté à SnapCenter, comme illustré à l'étape 6 pour CVO.

8. Une fois le répertoire du journal configuré, l'état global du plug-in hôte Windows est défini sur en cours d'exécution.



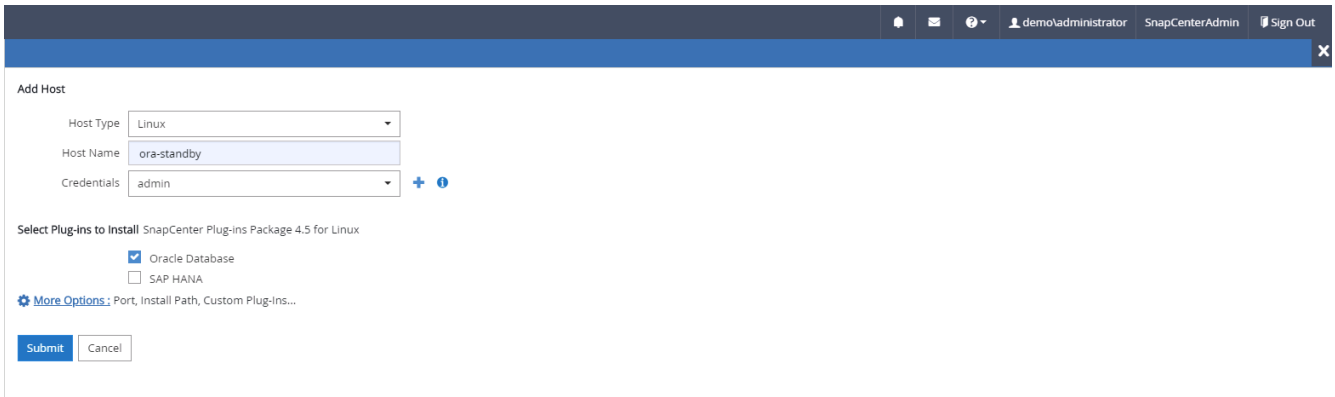
9. Pour attribuer l'hôte à l'ID utilisateur de gestion de base de données, accédez à l'onglet accès sous Paramètres et utilisateurs, cliquez sur l'ID utilisateur de gestion de base de données (dans notre cas, l'ID utilisateur de gestion de base de données à affecter à l'hôte), puis cliquez sur Enregistrer pour terminer l'affectation de ressources hôte.



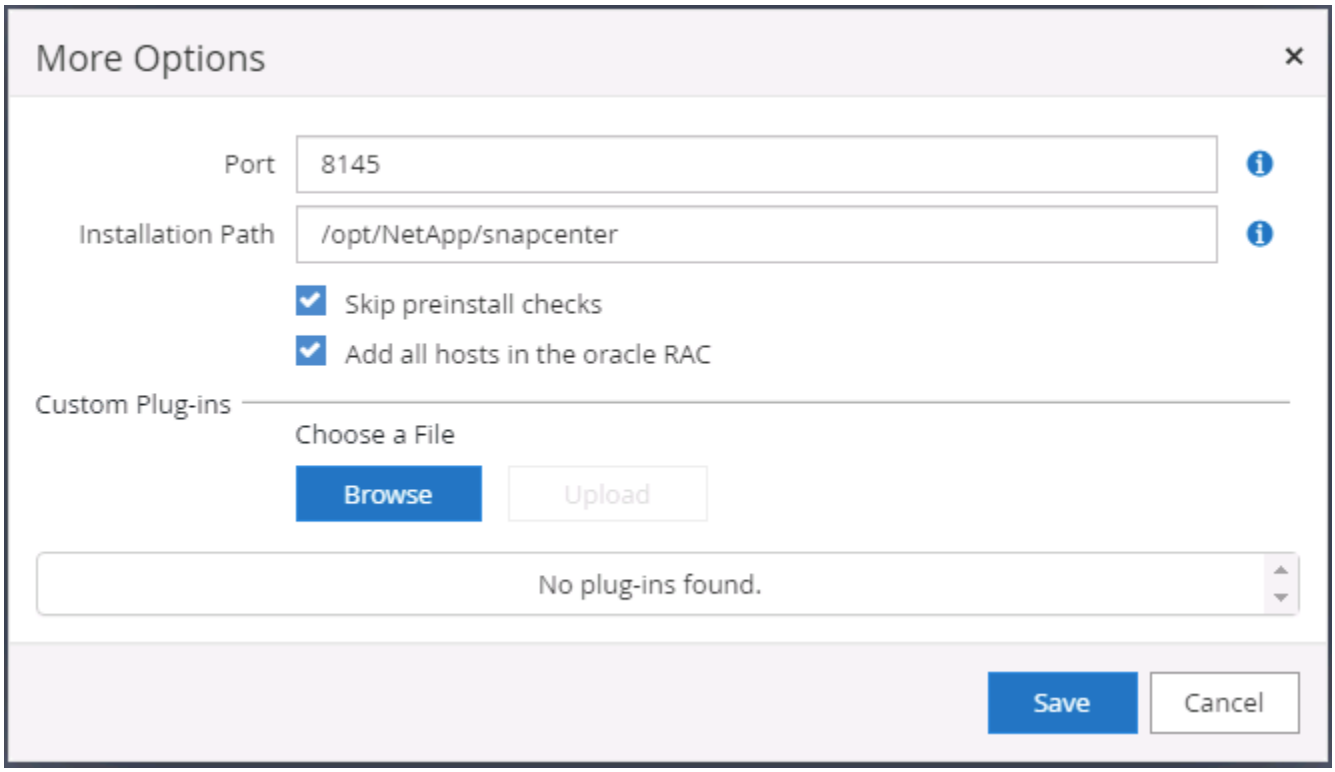


Ajoutez l'hôte Unix et l'installation du plug-in sur l'hôte

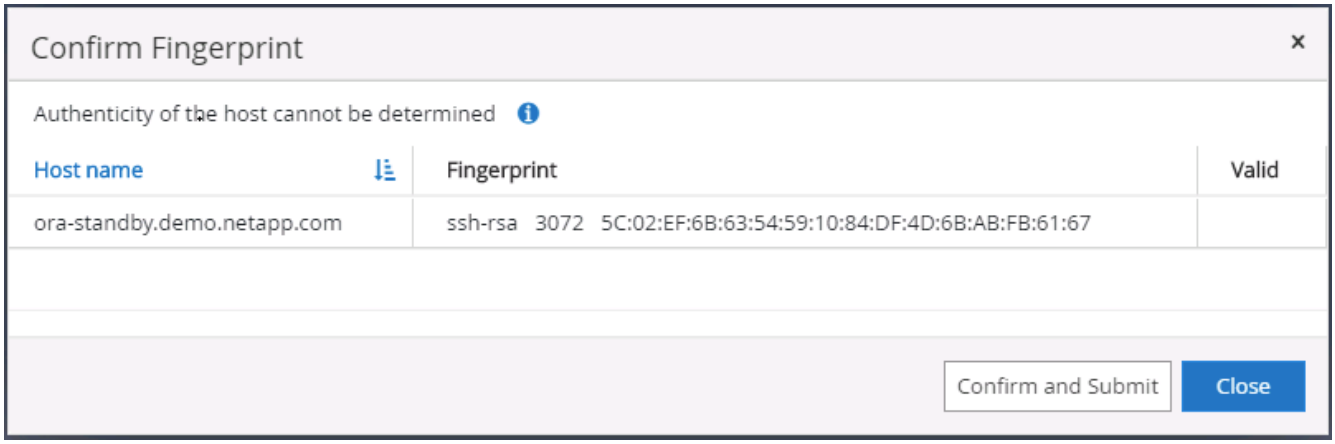
1. Connectez-vous à SnapCenter avec un ID utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet hôtes dans le menu de gauche, puis cliquez sur Ajouter pour ouvrir le flux de travail Ajouter hôte.
3. Choisissez Linux comme Type d'hôte. Le nom d'hôte peut être soit le nom d'hôte, soit une adresse IP. Cependant, le nom d'hôte doit être résolu pour corriger l'adresse IP de l'hôte SnapCenter. Choisissez les informations d'identification de l'hôte créées à l'étape 2. Les informations d'identification de l'hôte nécessitent des privilèges sudo. Vérifiez Oracle Database en tant que plug-in à installer, qui installe à la fois les plug-ins hôtes Oracle et Linux.



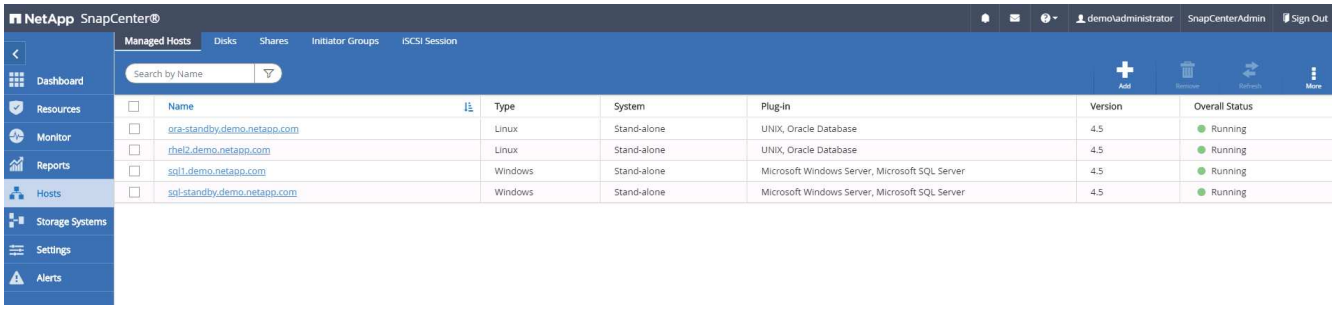
4. Cliquez sur plus d'options et sélectionnez « Ignorer les vérifications de préinstallation ». Vous êtes invité à confirmer l'omission de la vérification de préinstallation. Cliquez sur Oui, puis sur Enregistrer.



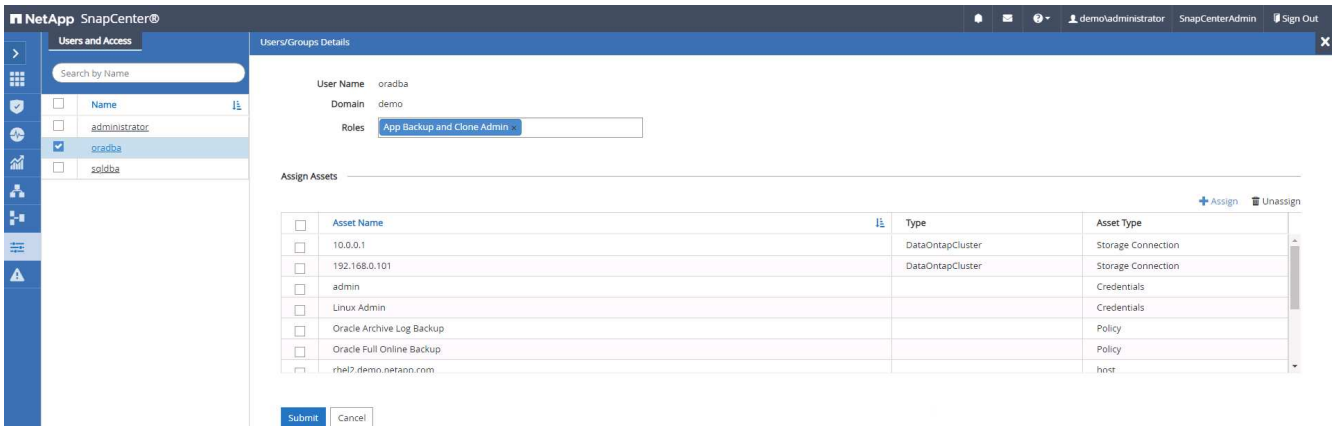
5. Cliquez sur soumettre pour démarrer l'installation du plug-in. Vous êtes invité à confirmer l'empreinte digitale comme indiqué ci-dessous.

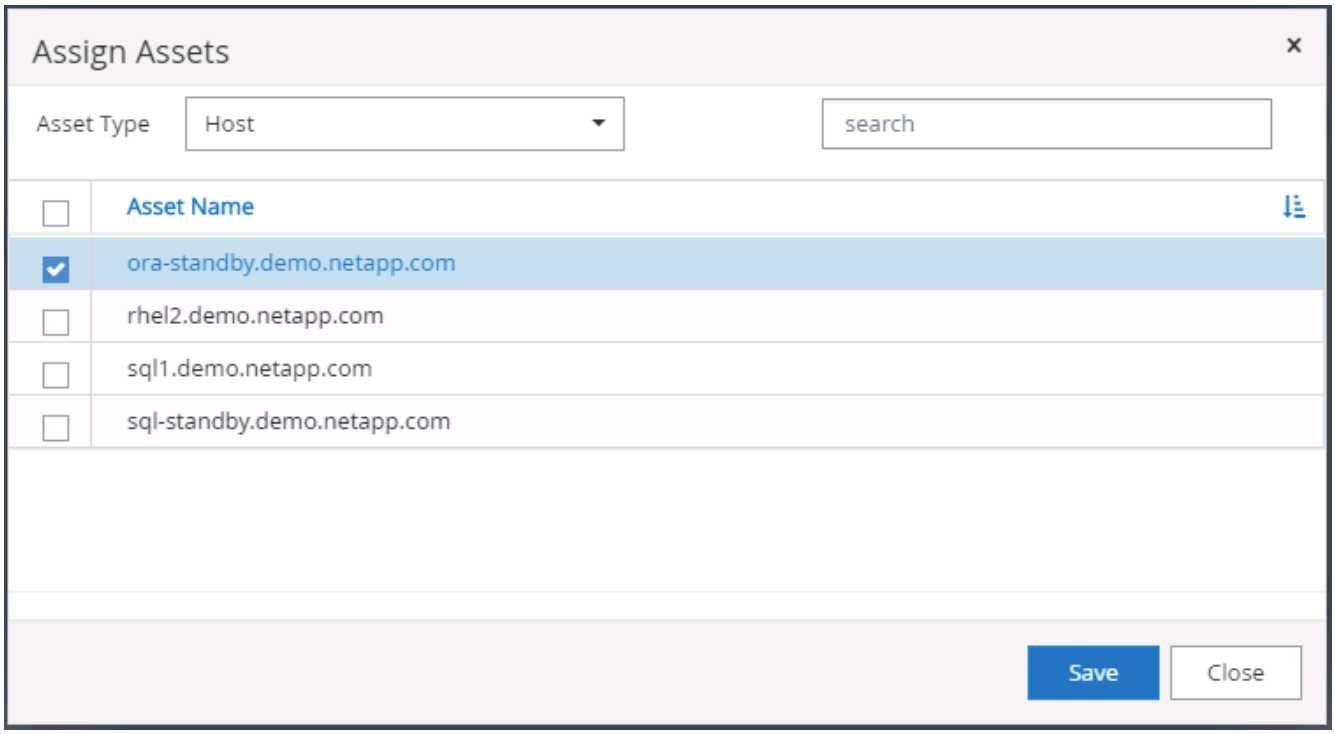


6. SnapCenter effectue la validation et l'enregistrement des hôtes, puis le plug-in est installé sur l'hôte Linux. L'état passe de installation du plug-in à exécution.



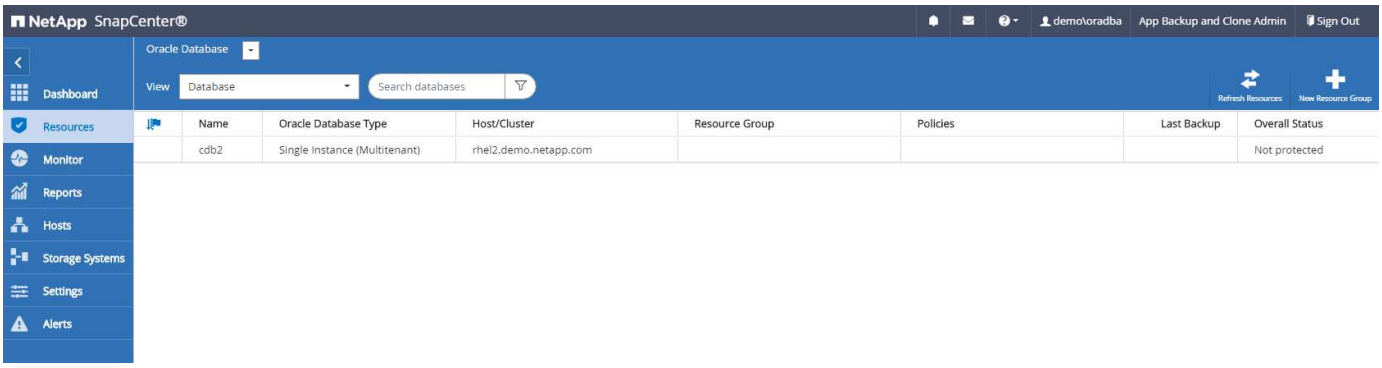
7. Affectez l'hôte nouvellement ajouté à l'ID utilisateur de gestion de base de données approprié (dans notre cas, oradba).





4. Découverte de ressources de base de données

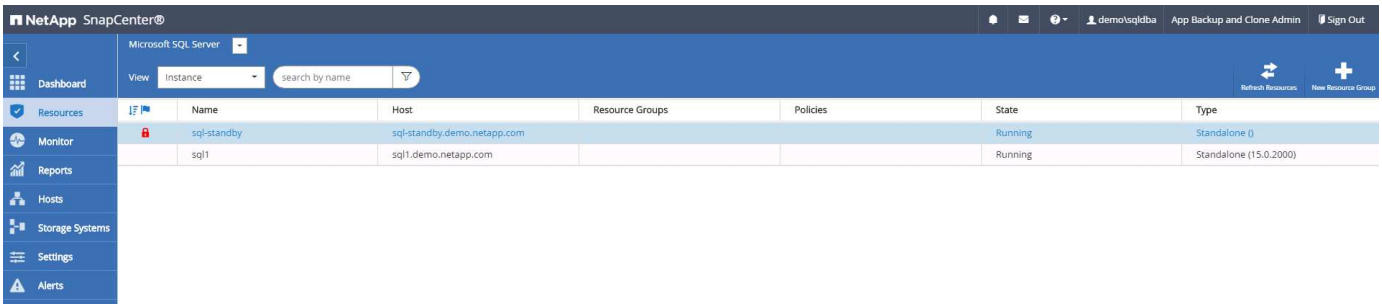
Une fois l'installation du plug-in réussie, les ressources de la base de données sur l'hôte peuvent être immédiatement découvertes. Cliquez sur l'onglet Ressources dans le menu de gauche. Selon le type de plate-forme de base de données, un certain nombre de vues sont disponibles, comme la base de données, le groupe de ressources, etc. Vous devrez peut-être cliquer sur l'onglet Actualiser les ressources si les ressources de l'hôte ne sont pas découvertes et affichées.

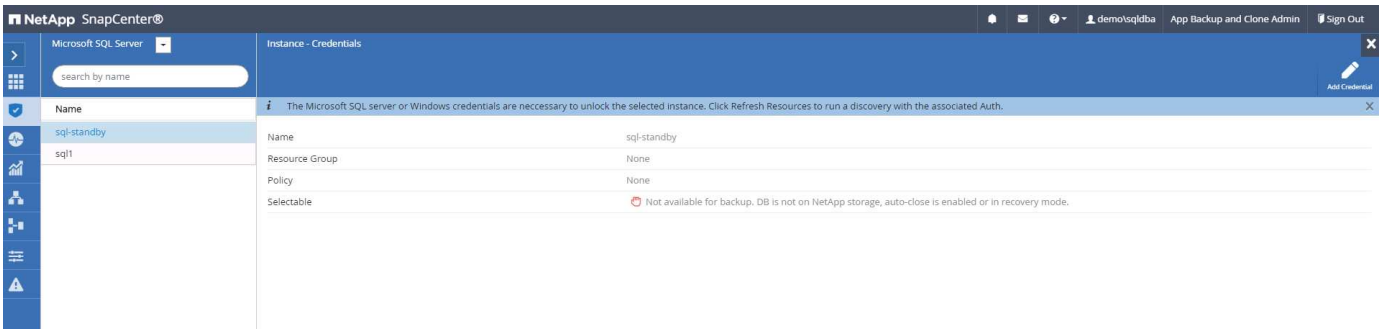


Lorsque la base de données est initialement découverte, l'état global est indiqué comme « non protégé ». La capture d'écran précédente montre qu'une base de données Oracle n'est pas encore protégée par une règle de sauvegarde.

Lorsqu'une configuration ou une stratégie de sauvegarde est configurée et qu'une sauvegarde a été exécutée, l'état général de la base de données affiche l'état de sauvegarde « sauvegarde réussie » et l'horodatage de la dernière sauvegarde. La capture d'écran suivante montre l'état de sauvegarde d'une base de données utilisateur SQL Server.

Si les informations d'identification d'accès à la base de données ne sont pas correctement configurées, un bouton de verrouillage rouge indique que la base de données n'est pas accessible. Par exemple, si les informations d'identification Windows ne disposent pas d'un accès sysadmin à une instance de base de données, les informations d'identification de la base de données doivent être reconfigurées pour déverrouiller le verrou rouge.





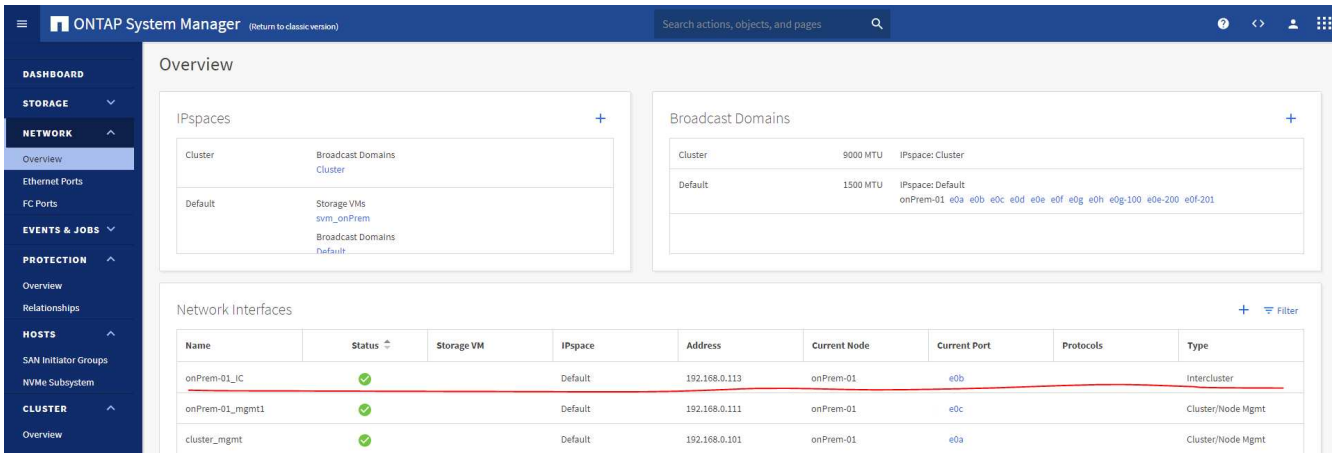
Une fois que les informations d'identification appropriées sont configurées soit au niveau de Windows, soit au niveau de la base de données, le verrou rouge disparaît et les informations de type de serveur SQL sont rassemblées et vérifiées.

5. Configuration de la réplication des volumes de peering de cluster de stockage et de BDD

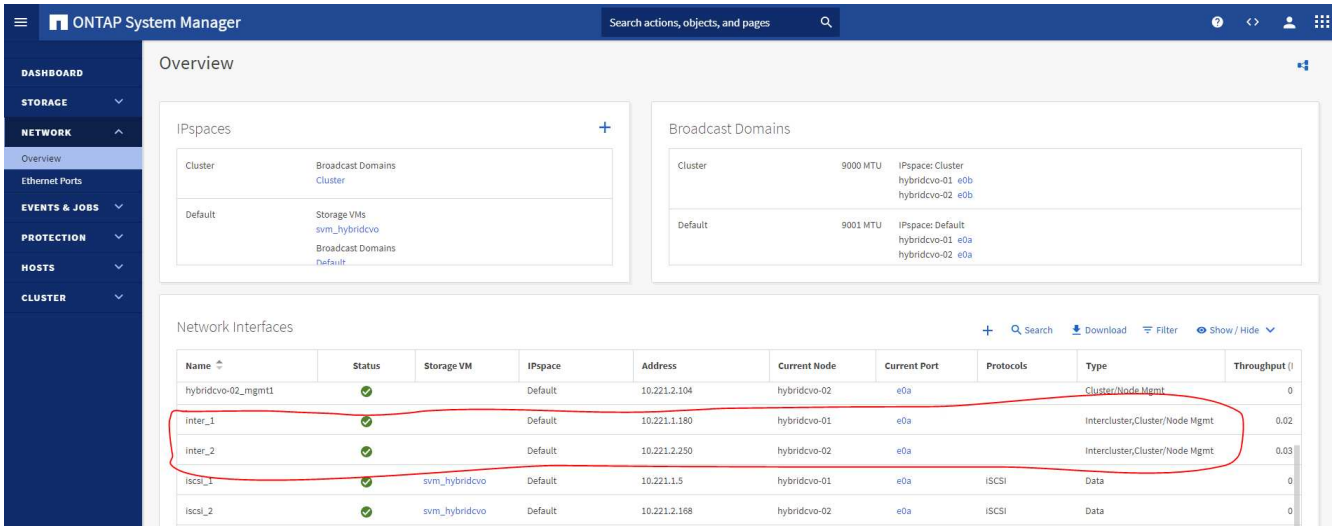
Pour protéger vos données de base de données sur site à l'aide d'un cloud public comme destination cible, les volumes de base de données du cluster ONTAP sur site sont répliqués dans Cloud volumes CVO à l'aide de la technologie NetApp SnapMirror. Les volumes cibles répliqués peuvent ensuite être clonés pour LE DÉVELOPPEMENT/opérations ou la reprise après incident. Les étapes de haut niveau suivantes vous permettent de configurer le peering de clusters et la réplication des volumes de la base de données.

1. Configurer les LIF intercluster pour le peering de cluster sur le cluster sur site et sur l'instance du cluster CVO. Cette étape peut être réalisée avec ONTAP System Manager. Un déploiement CVO par défaut est configuré automatiquement pour les LIF inter-cluster.

   Cluster sur site :



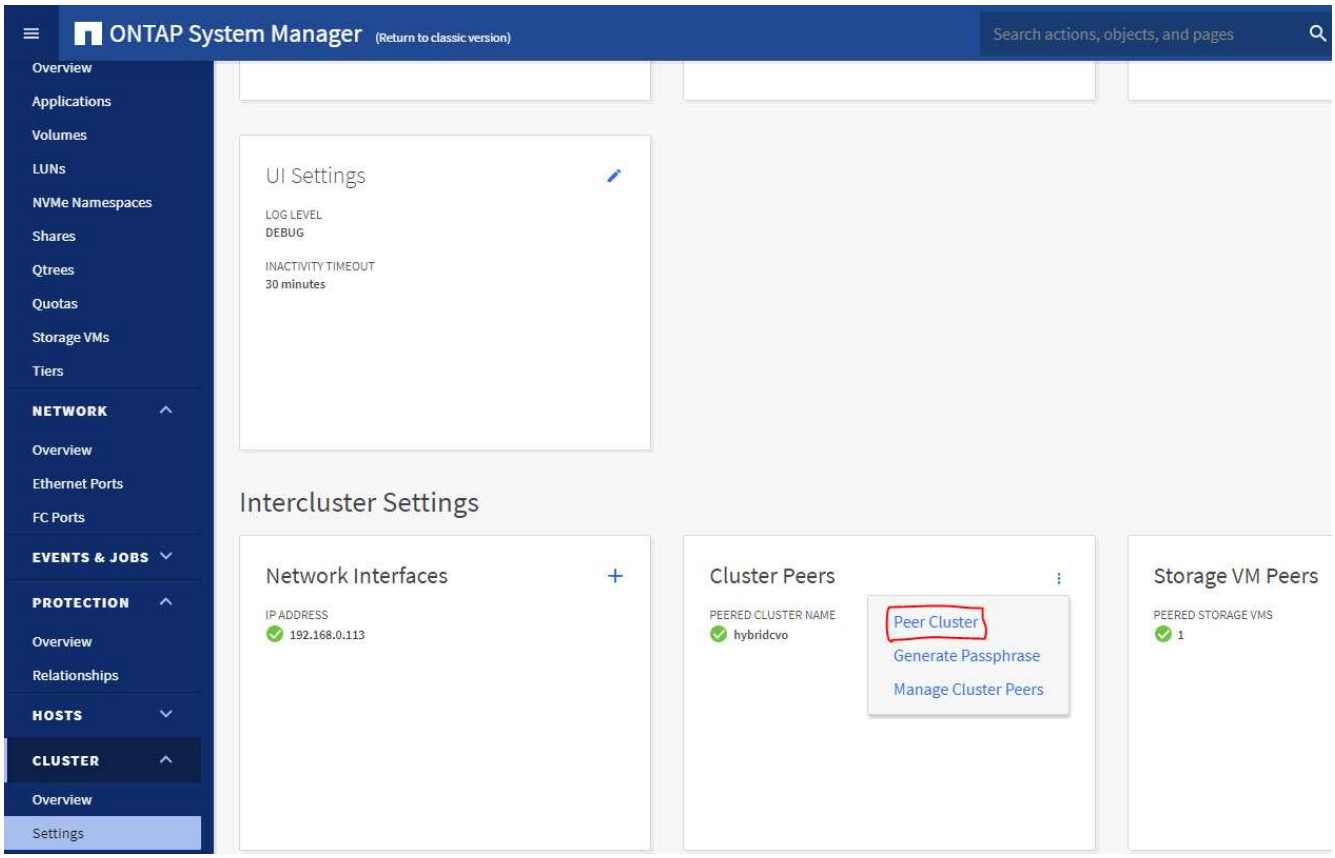
   Cluster CVO cible :



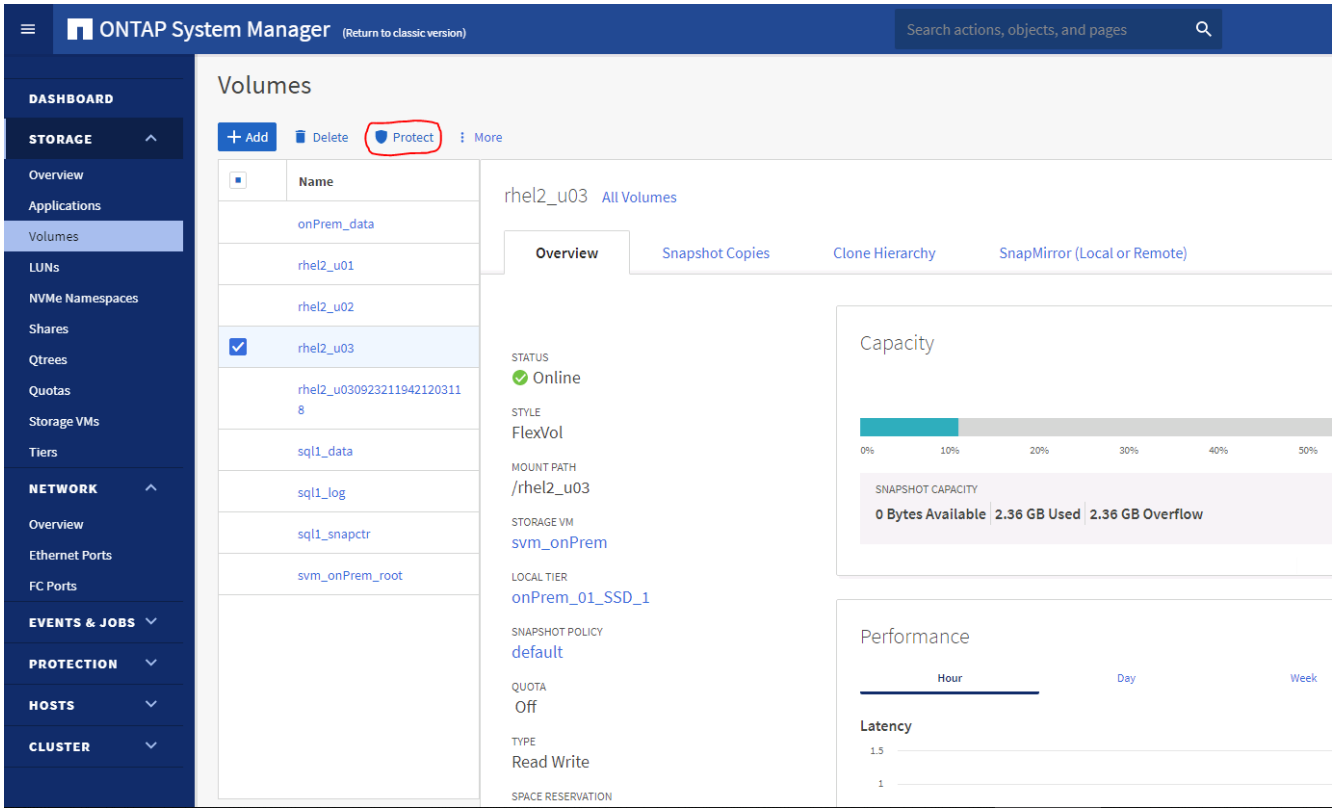
2. Lorsque les LIF intercluster sont configurées, le peering de clusters et la réplication des volumes peuvent être configurés en utilisant le glisser-déposer dans NetApp Cloud Manager. Voir "Mise en route - Cloud public AWS" pour plus d'informations.

   Vous pouvez également effectuer la réplication de volume de peering de clusters et de bases de données à l'aide de ONTAP System Manager, comme suit :

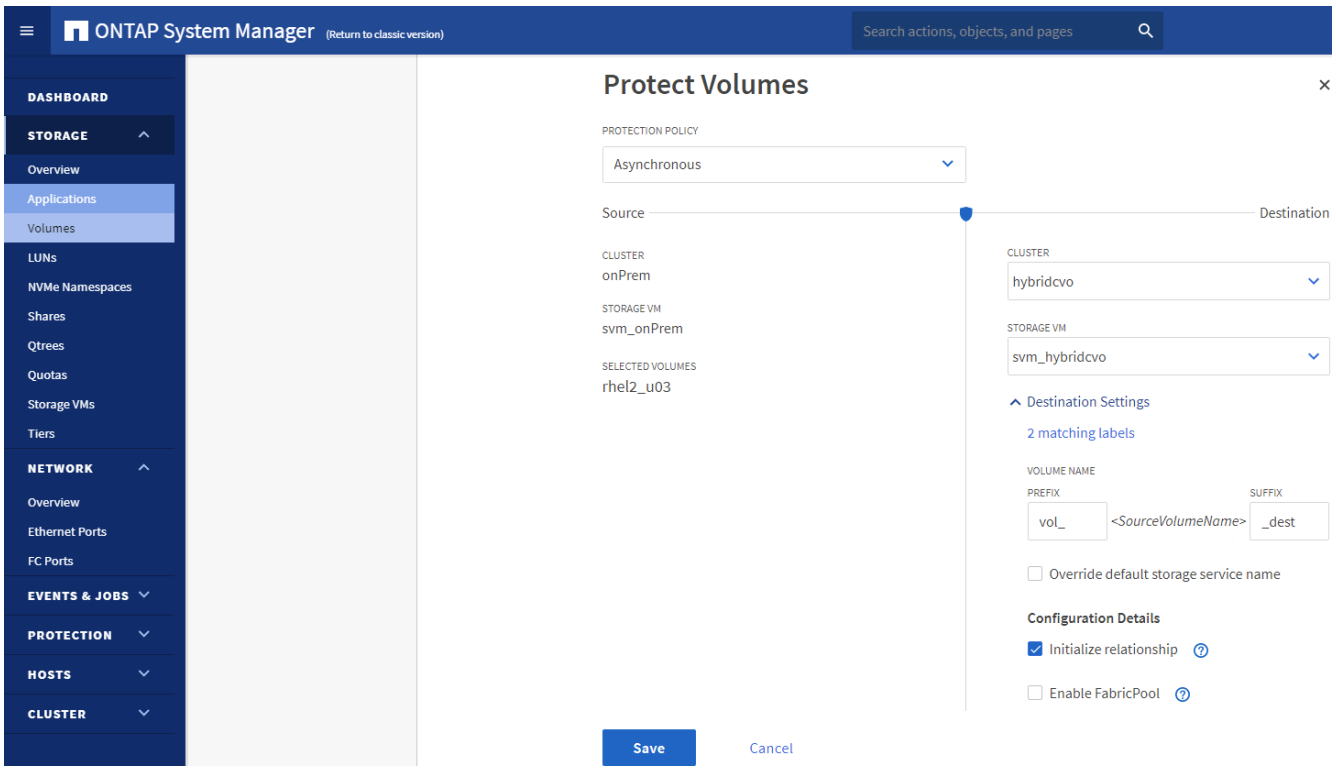
3. Connectez-vous à ONTAP System Manager. Naviguez jusqu'à Cluster > Paramètres et cliquez sur Peer Cluster pour configurer le cluster peering avec l'instance CVO dans le cloud.



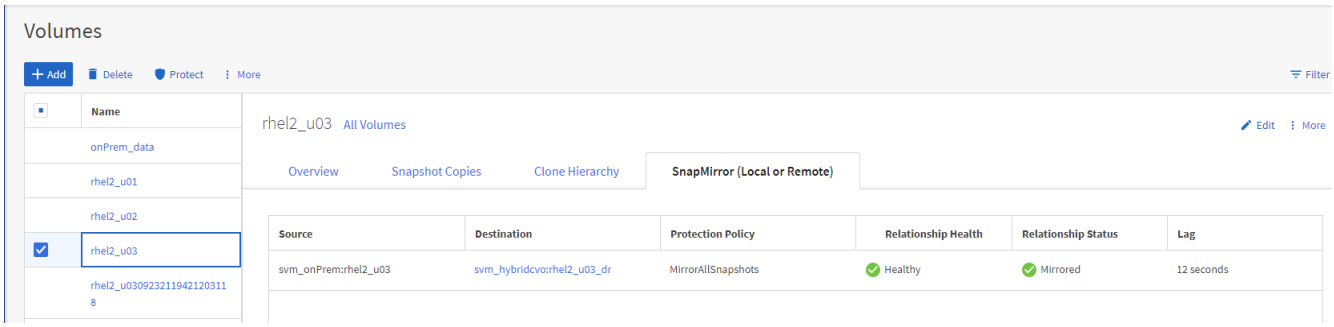
4. Accédez à l'onglet volumes. Sélectionnez le volume de la base de données à répliquer et cliquez sur protéger.



5. Définissez la règle de protection sur asynchrone. Sélectionner le cluster de destination et le SVM de stockage.

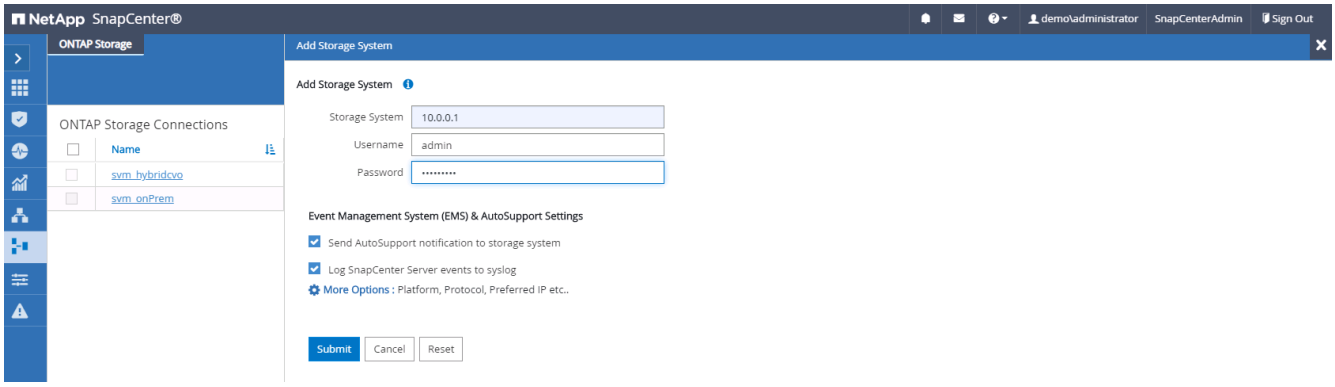


6. Vérifier que le volume est synchronisé entre la source et la cible et que la relation de réplication fonctionne correctement.

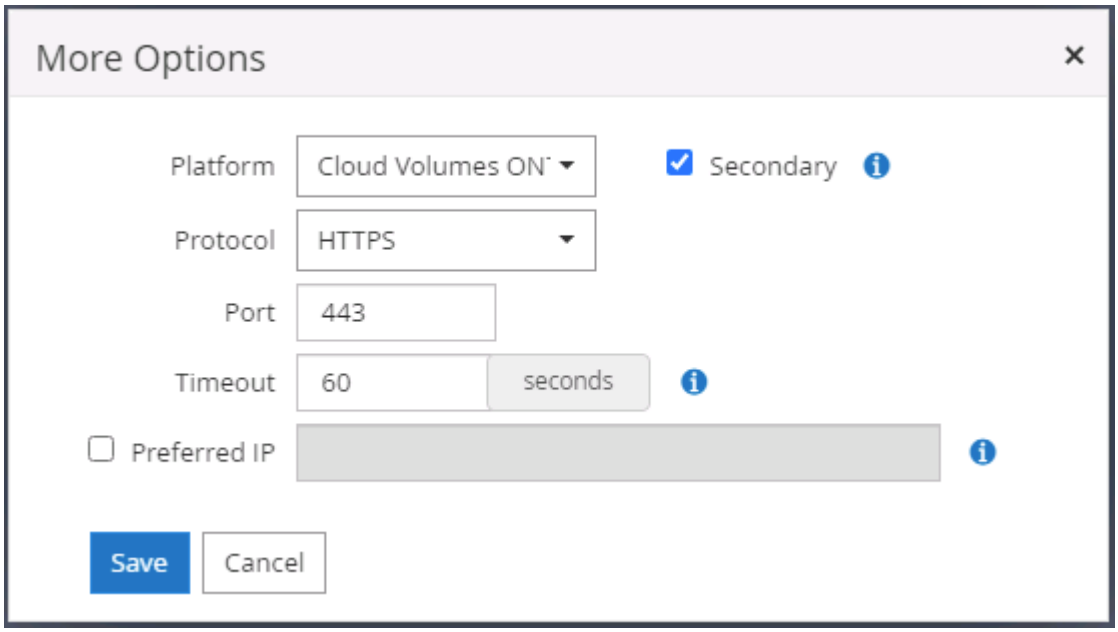


6. Ajouter le SVM de stockage de base de données CVO à SnapCenter

1. Connectez-vous à SnapCenter avec un ID utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet Storage System dans le menu, puis sur New pour ajouter un SVM de stockage CVO qui héberge les volumes de base de données cible répliqués dans SnapCenter. Saisissez l'IP de gestion de cluster dans le champ Storage System, puis saisissez le nom d'utilisateur et le mot de passe appropriés.

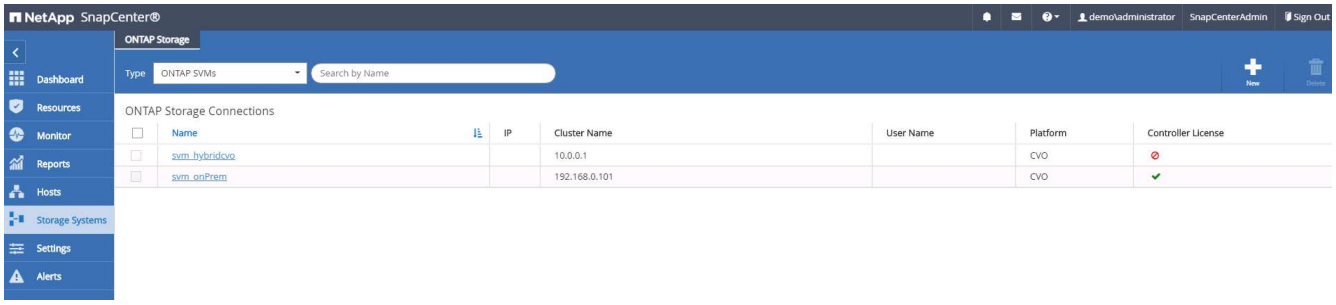


3. Cliquez sur plus d'options pour ouvrir d'autres options de configuration de stockage. Dans le champ plate-forme, sélectionnez Cloud Volumes ONTAP, cochez secondaire, puis cliquez sur Enregistrer.



4. Attribuez les systèmes de stockage aux ID d'utilisateur de gestion de la base de données SnapCenter,

comme indiqué dans la 3. Installation du plug-in hôte SnapCenter.

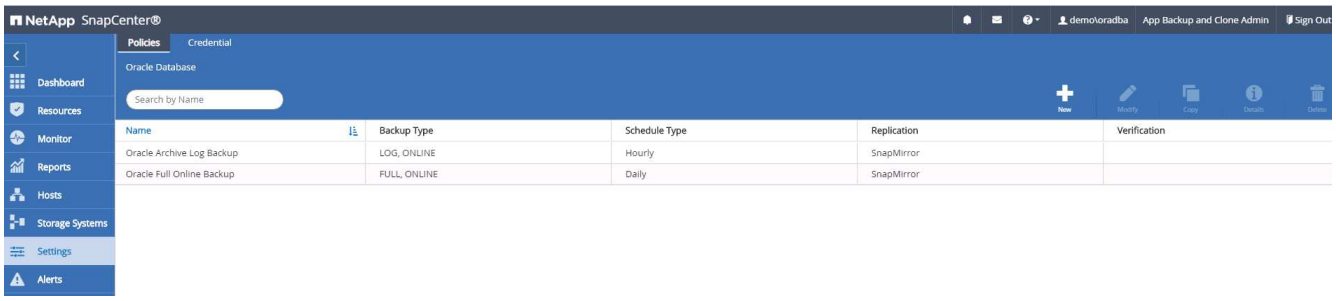


7. Configurer la politique de sauvegarde de la base de données dans SnapCenter

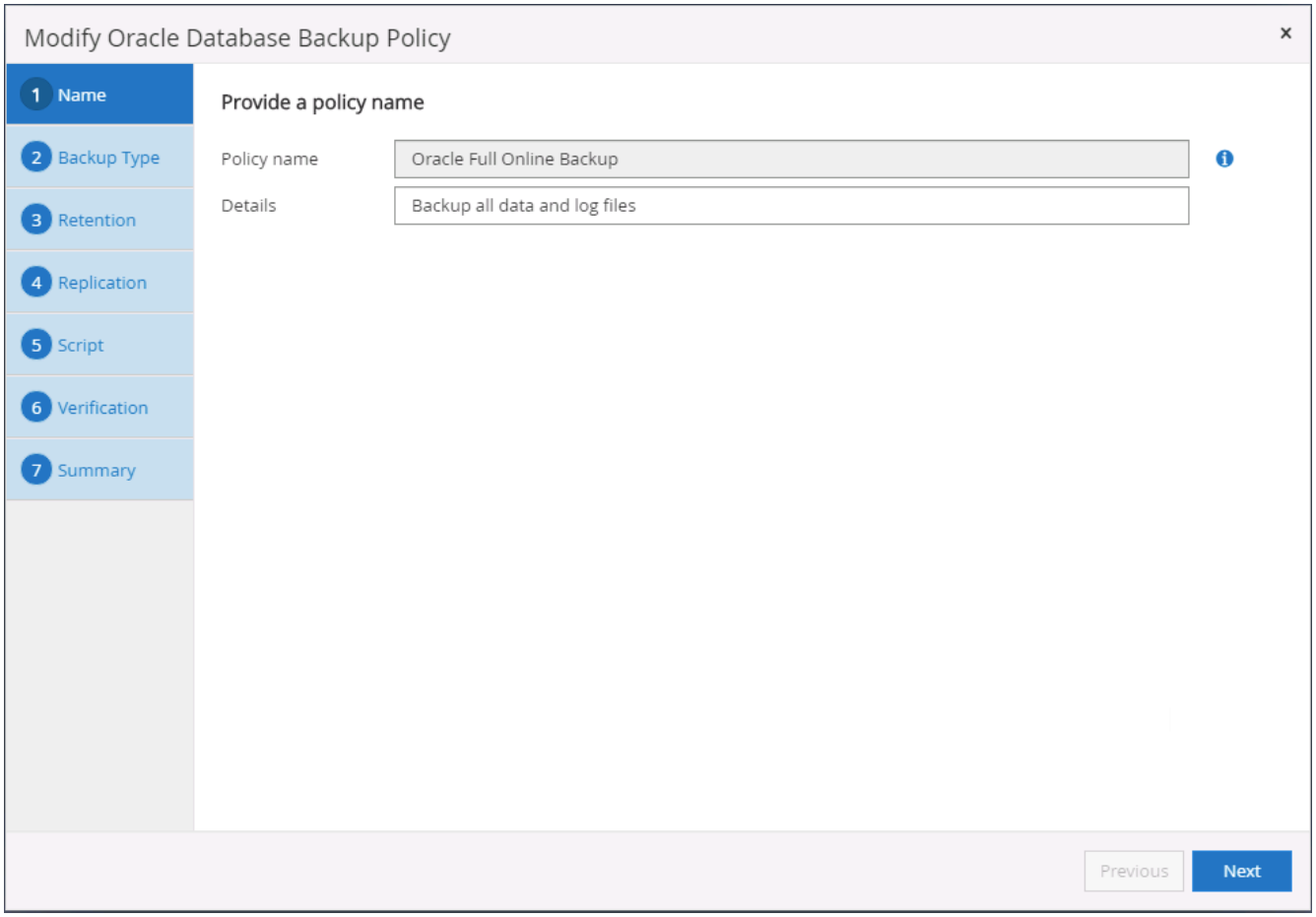
Les procédures suivantes montrent comment créer une stratégie de sauvegarde complète de base de données ou de fichiers journaux. La stratégie peut ensuite être mise en œuvre pour protéger les ressources des bases de données. L'objectif de point de récupération (RPO) ou l'objectif de délai de restauration (RTO) détermine la fréquence des sauvegardes de bases de données et/ou de journaux.

Créez une stratégie de sauvegarde complète de la base de données pour Oracle

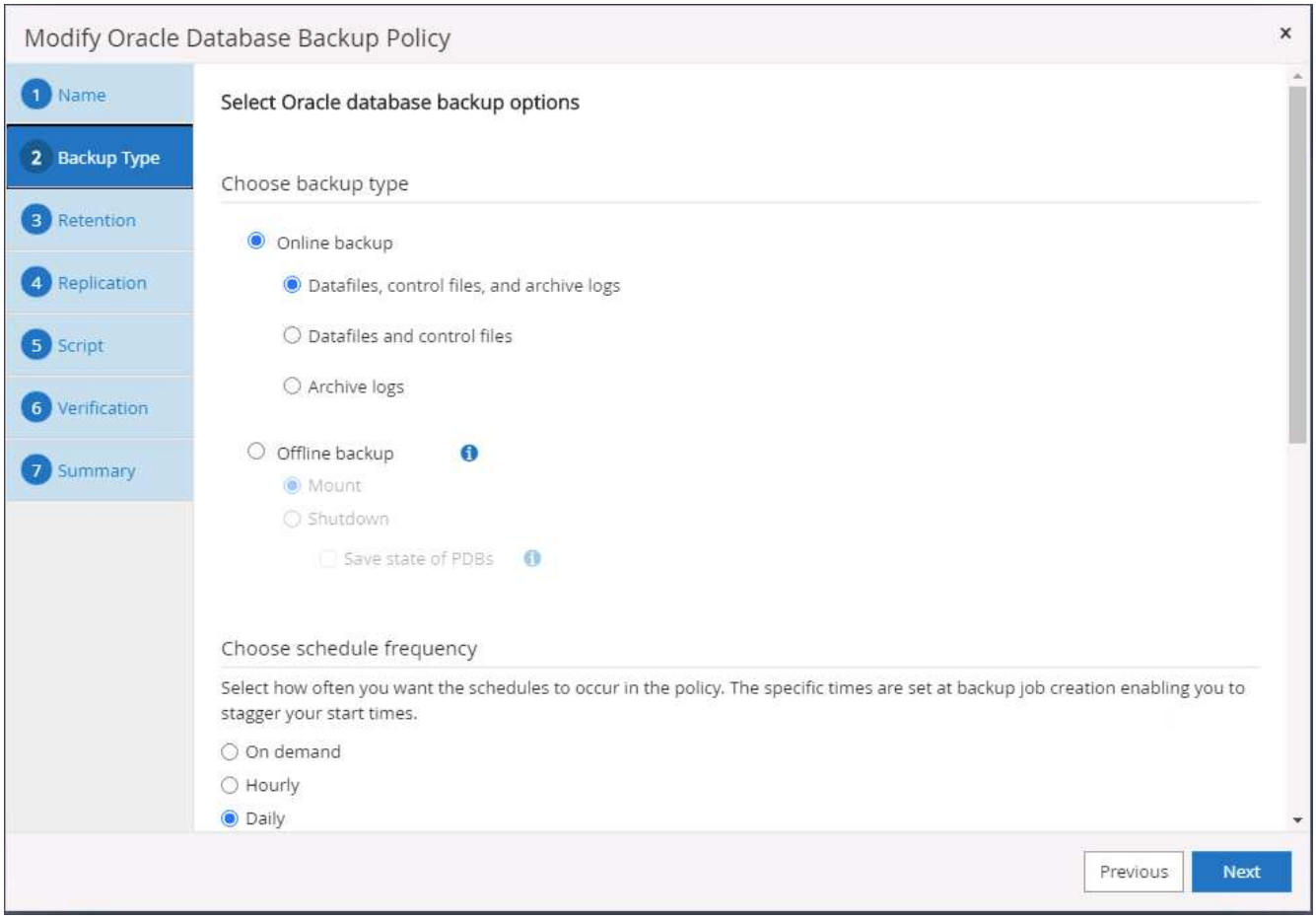
1. Connectez-vous à SnapCenter en tant qu'ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur stratégies.



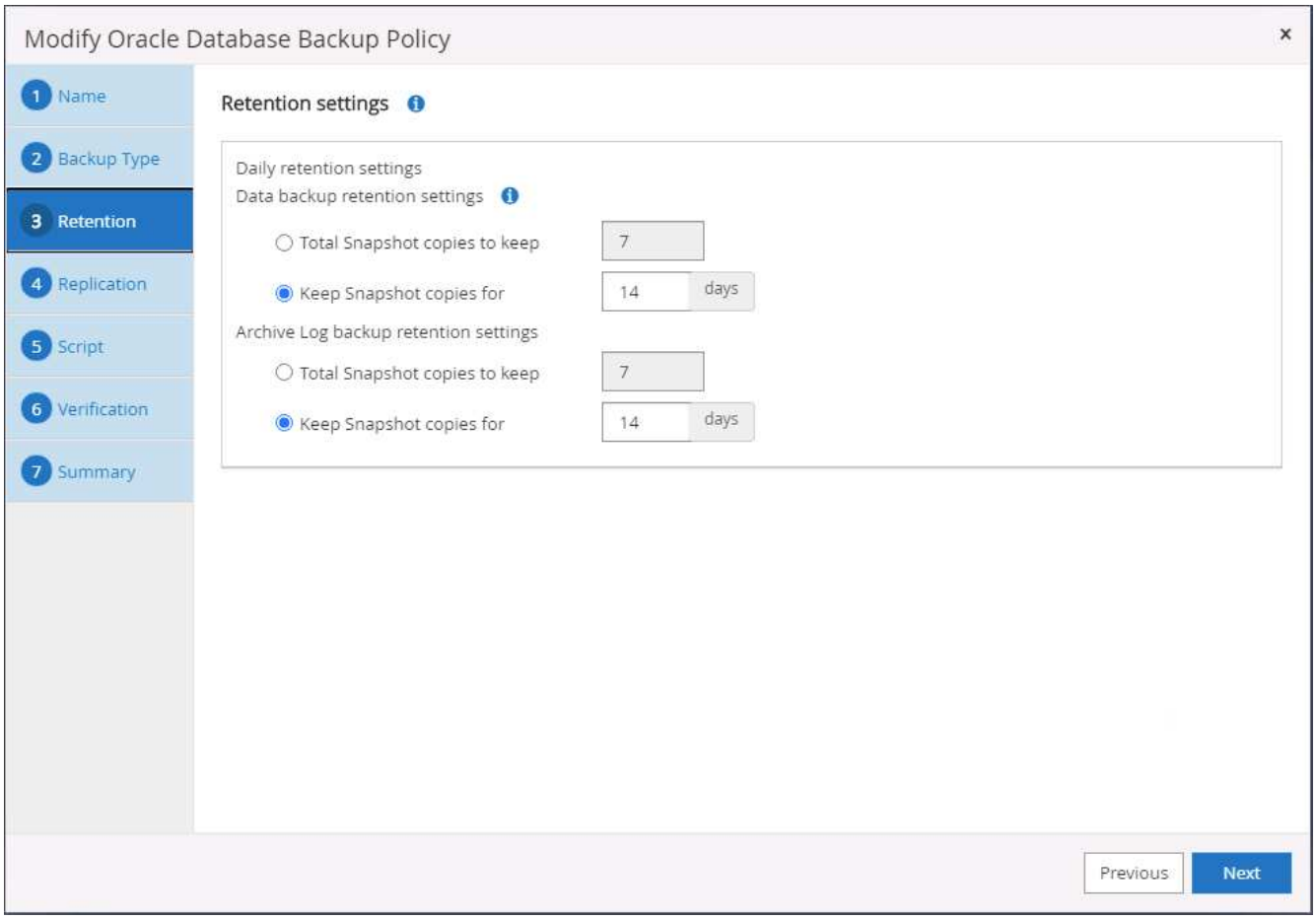
2. Cliquez sur Nouveau pour lancer un nouveau workflow de création de stratégie de sauvegarde ou choisir une stratégie existante pour la modification.



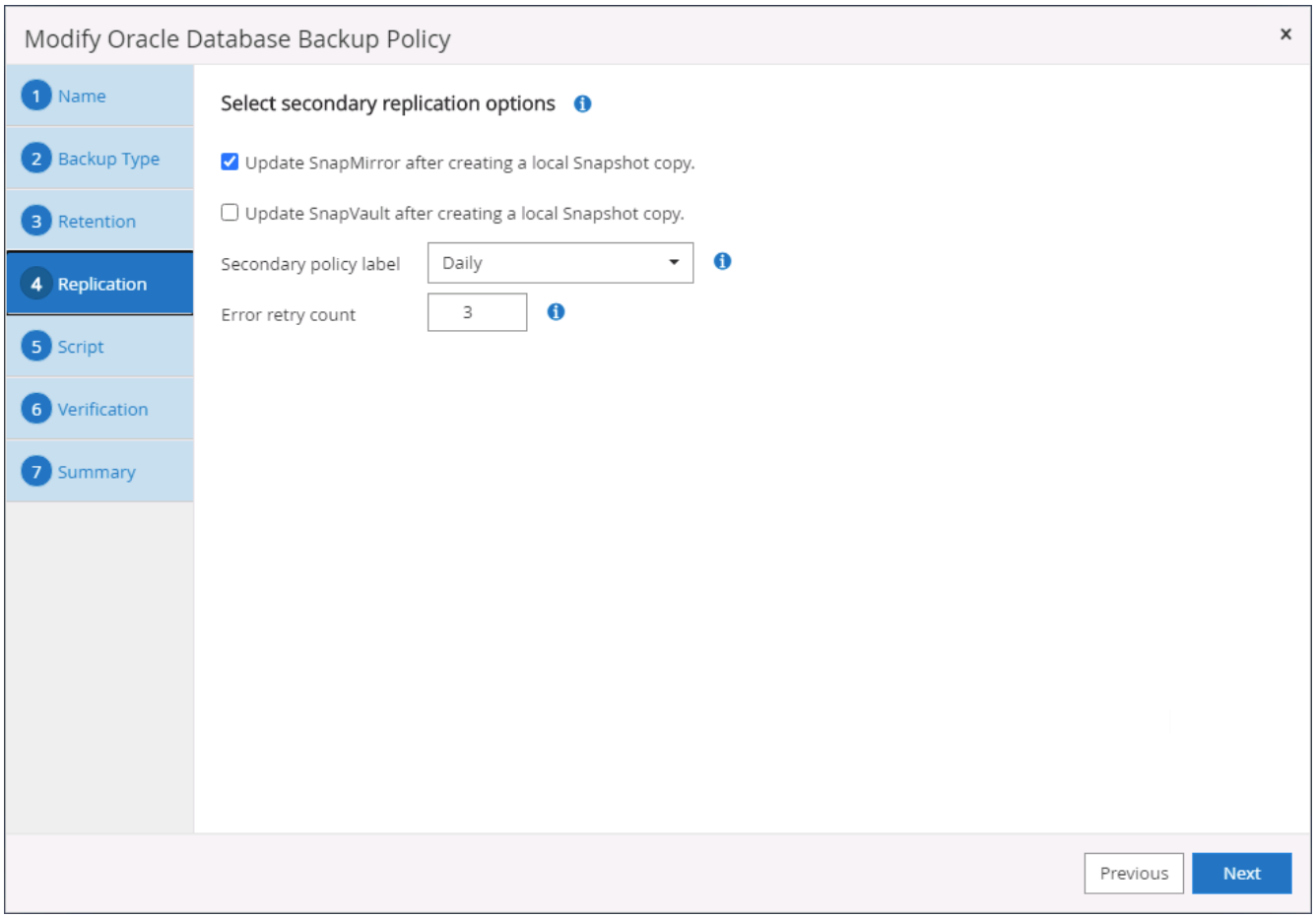
3. Sélectionnez le type de sauvegarde et la fréquence de planification.



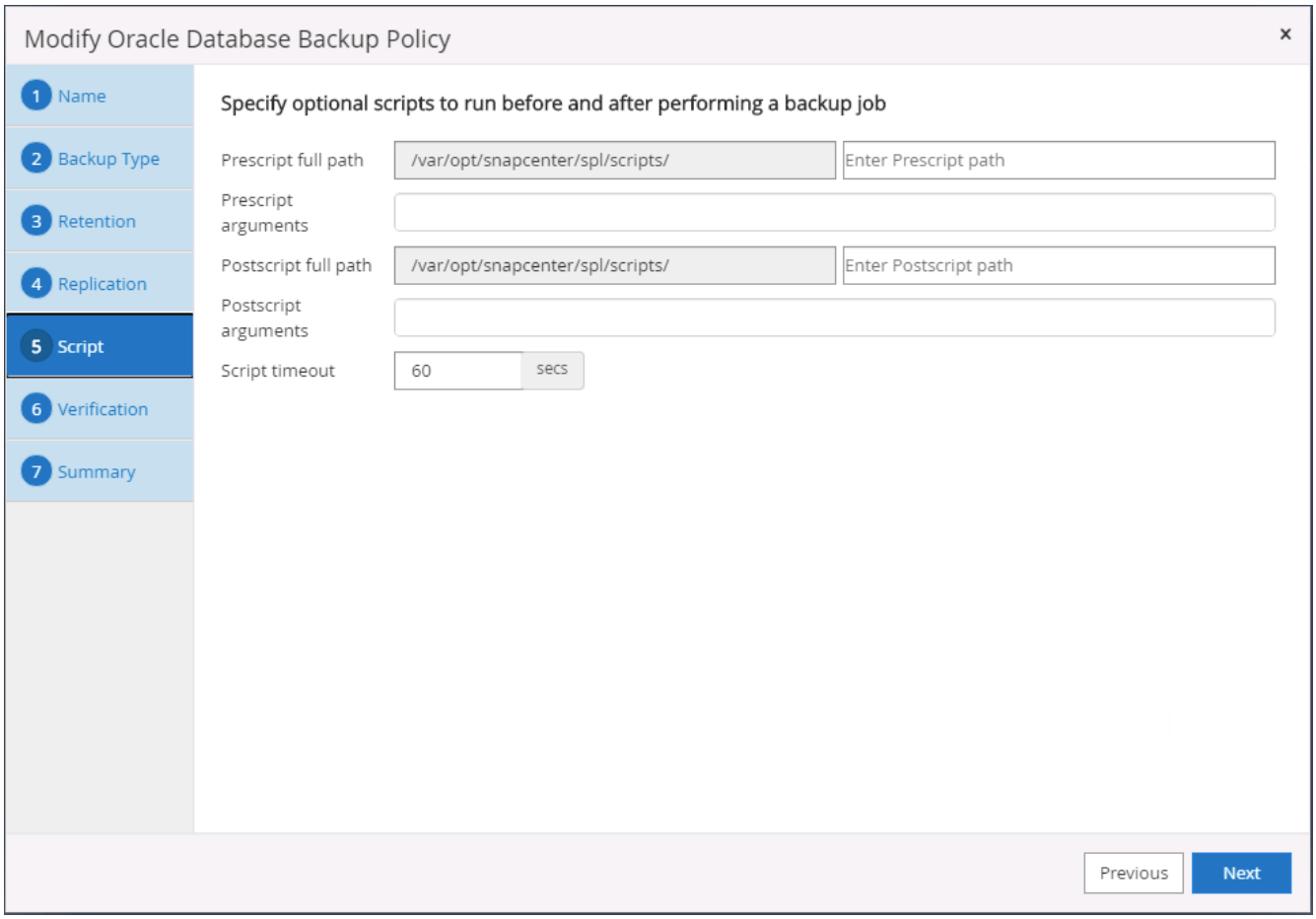
4. Définissez le paramètre de conservation de sauvegarde. Cet objectif définit le nombre de copies de sauvegarde complètes à conserver dans une base de données.



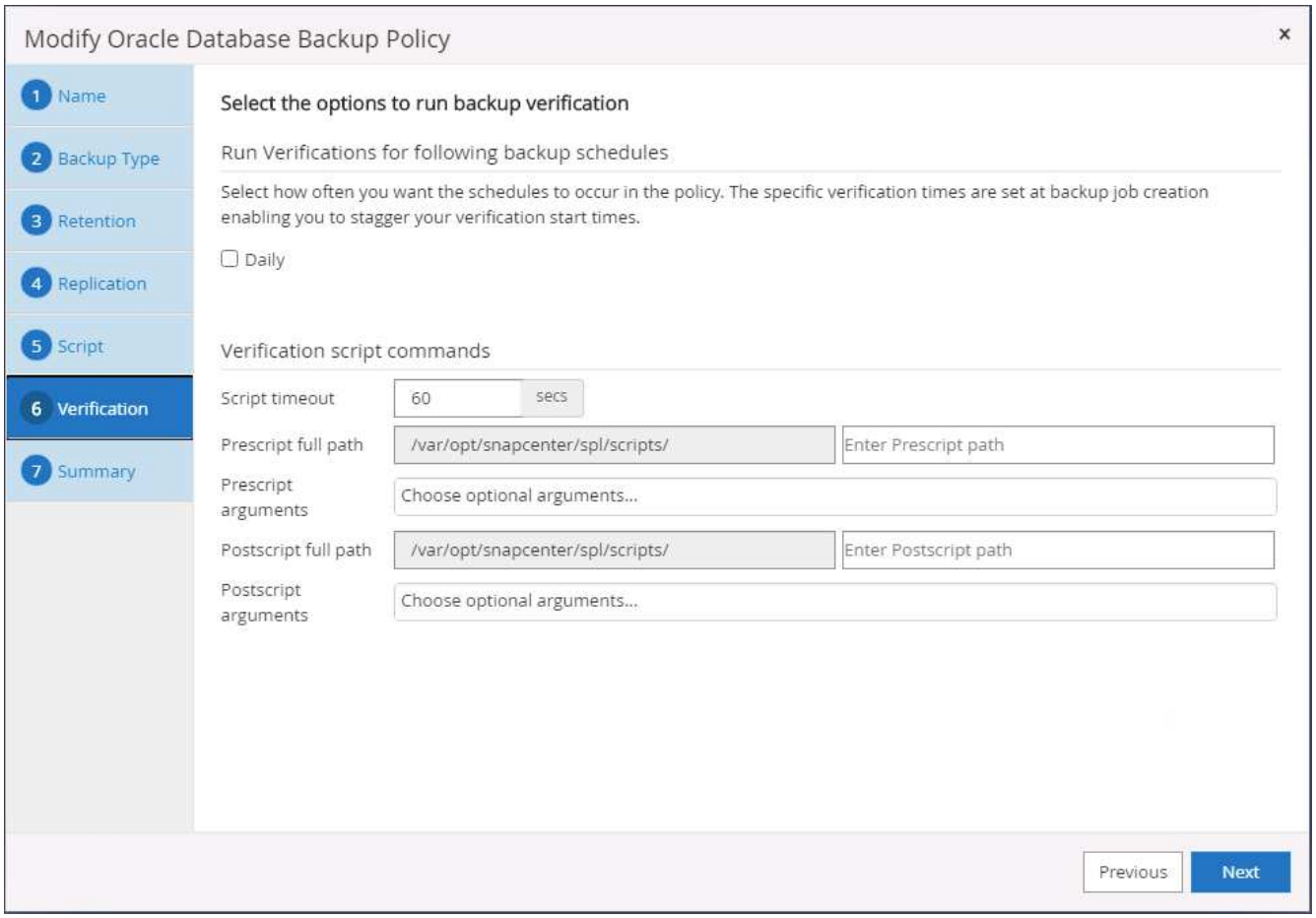
5. Sélectionnez les options de réplication secondaires pour envoyer les sauvegardes de snapshots primaires locaux à répliquer vers un emplacement secondaire dans le cloud.



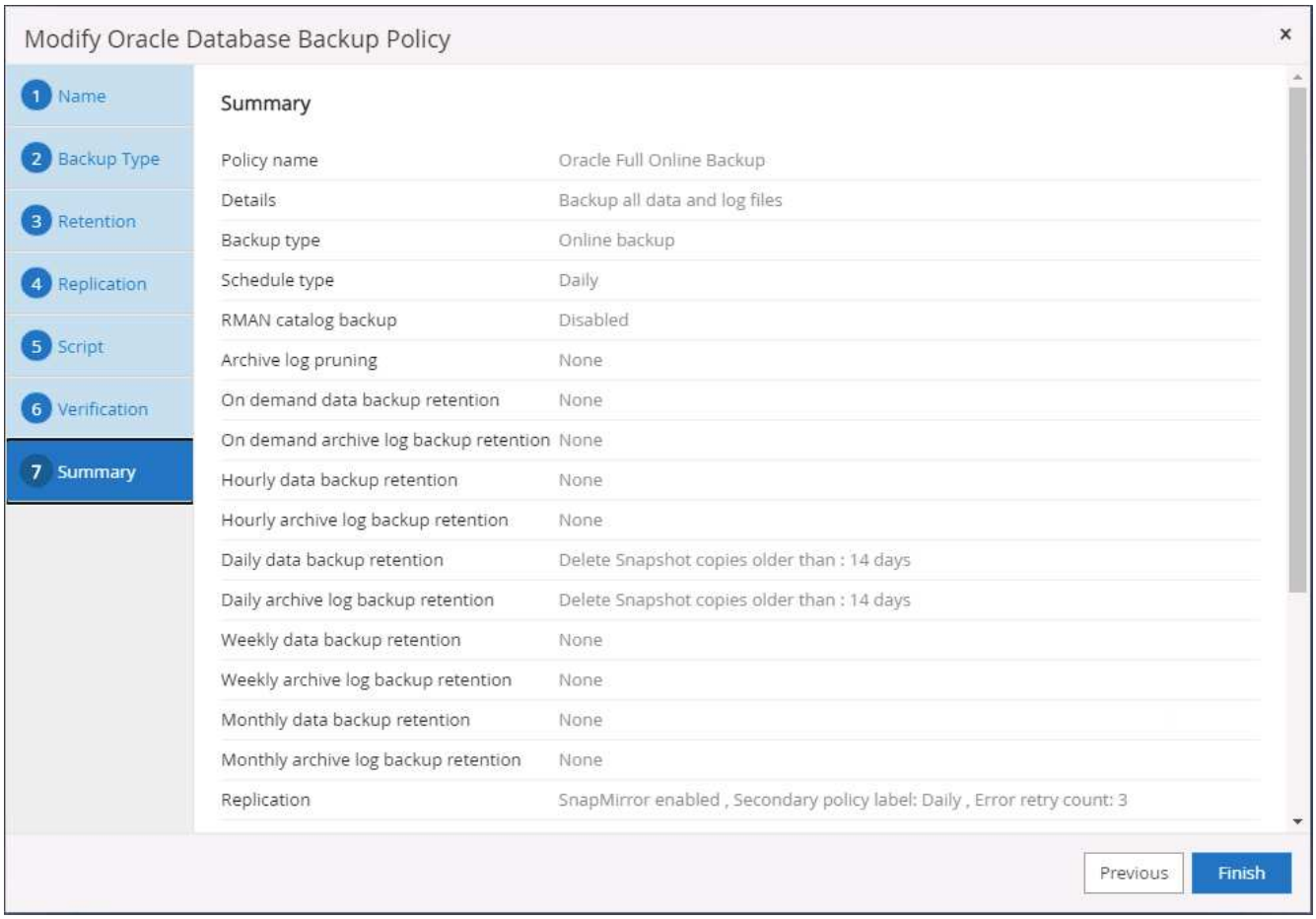
6. Spécifiez tout script facultatif à exécuter avant et après l'exécution d'une sauvegarde.



7. Exécutez la vérification des sauvegardes si nécessaire.

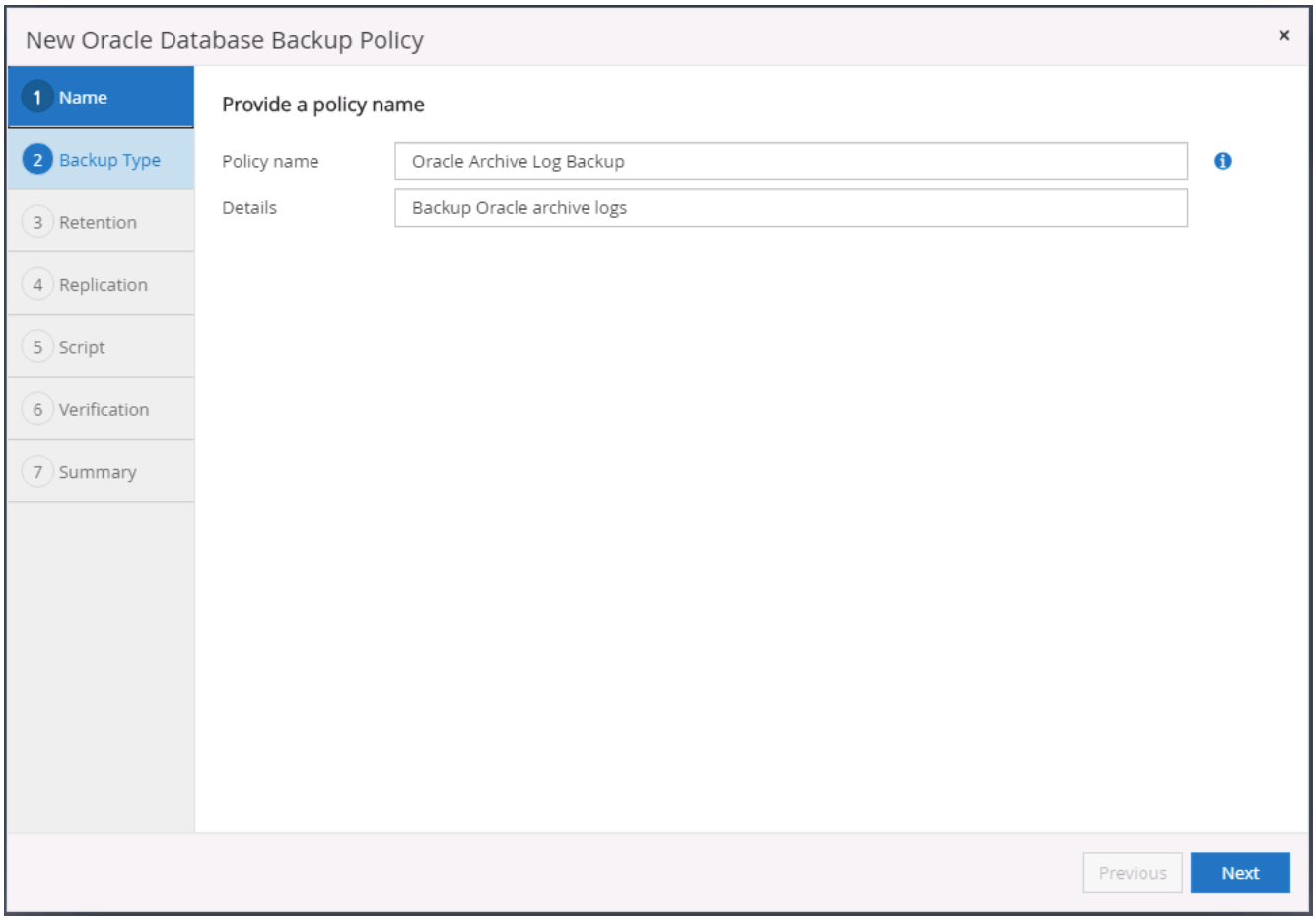


8. Récapitulatif.

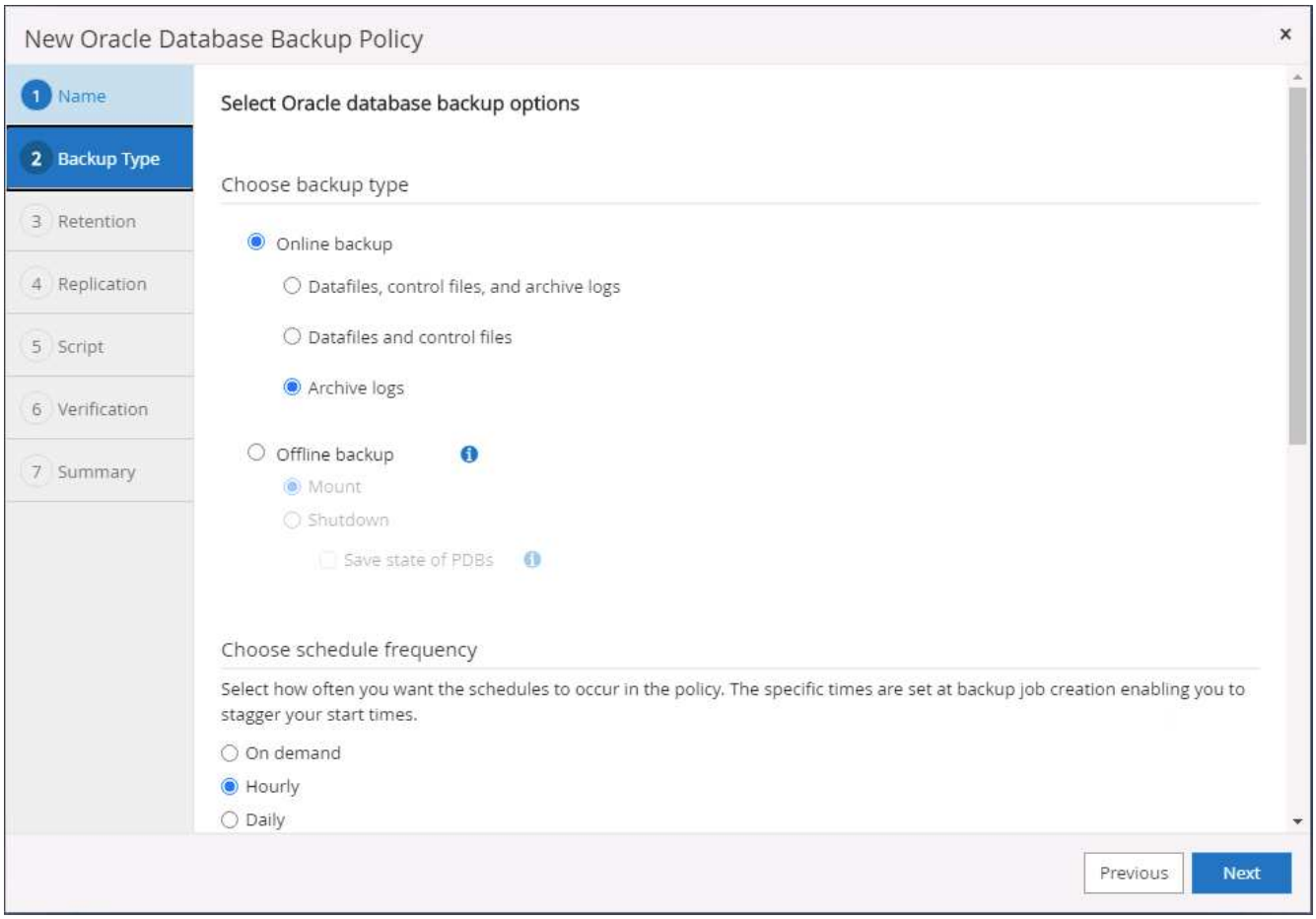


Créez une stratégie de sauvegarde du journal de base de données pour Oracle

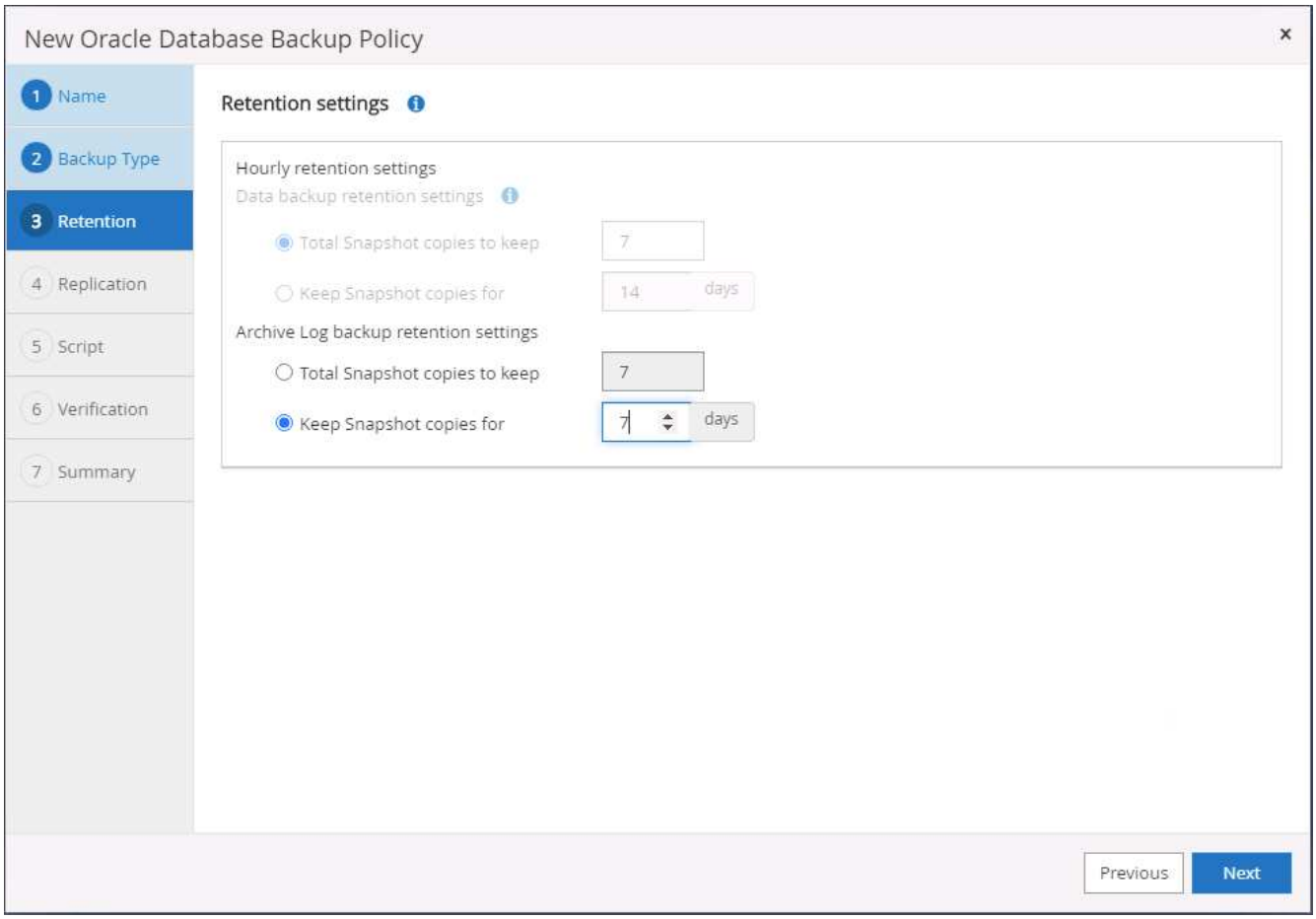
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur stratégies.
2. Cliquez sur Nouveau pour lancer un nouveau workflow de création de stratégie de sauvegarde ou choisissez une stratégie existante à modifier.



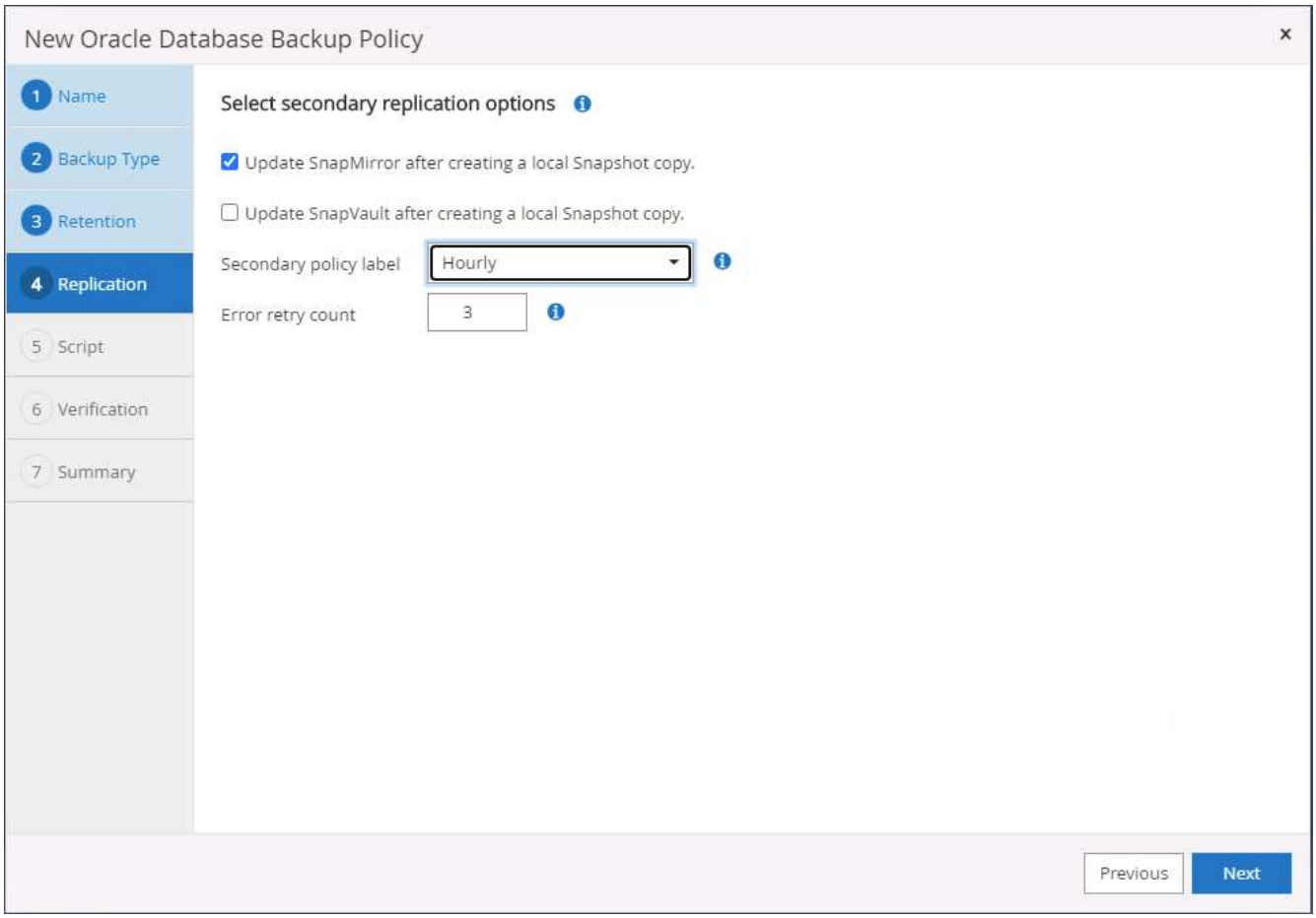
3. Sélectionnez le type de sauvegarde et la fréquence de planification.



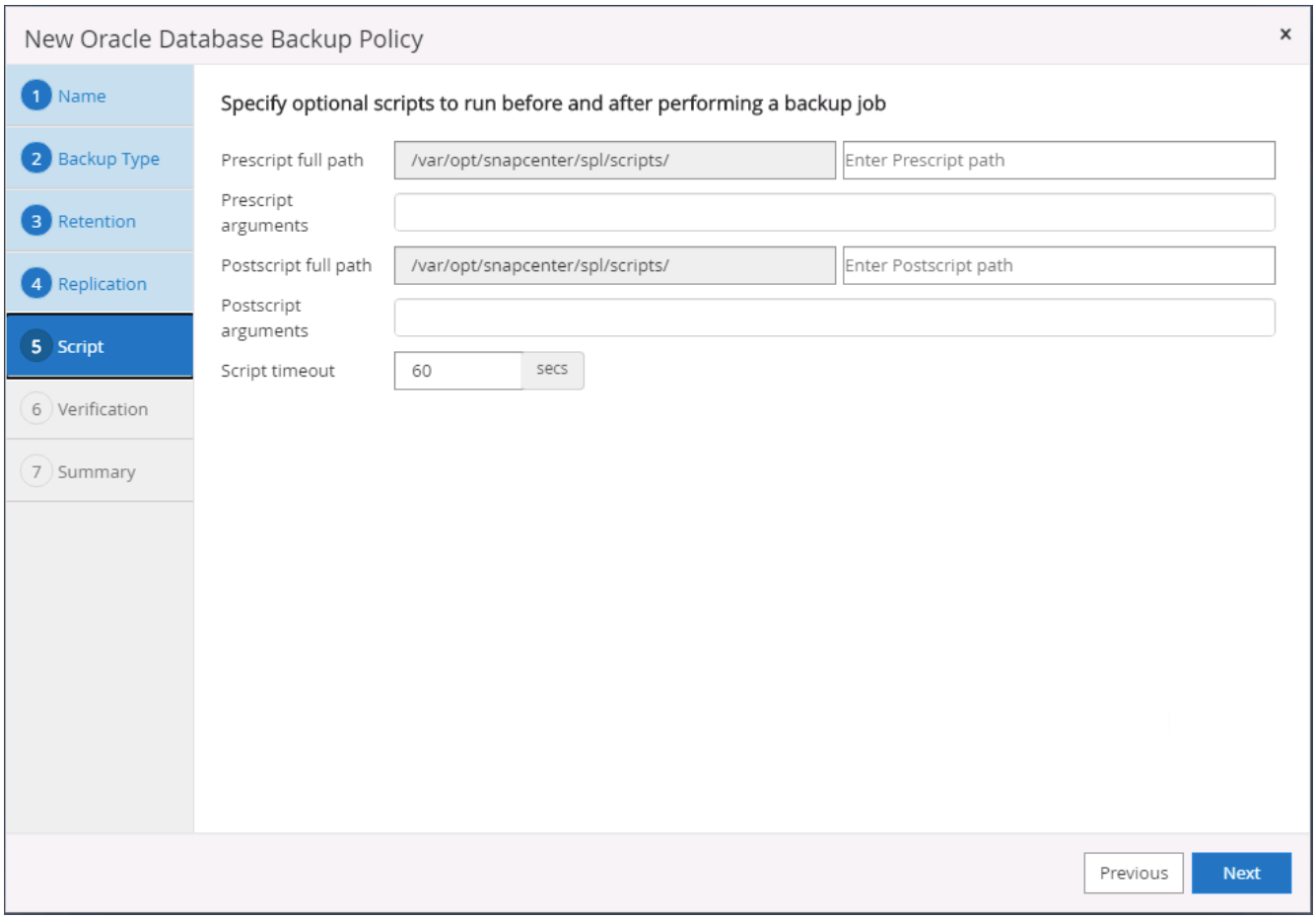
4. Définissez la période de conservation du journal.



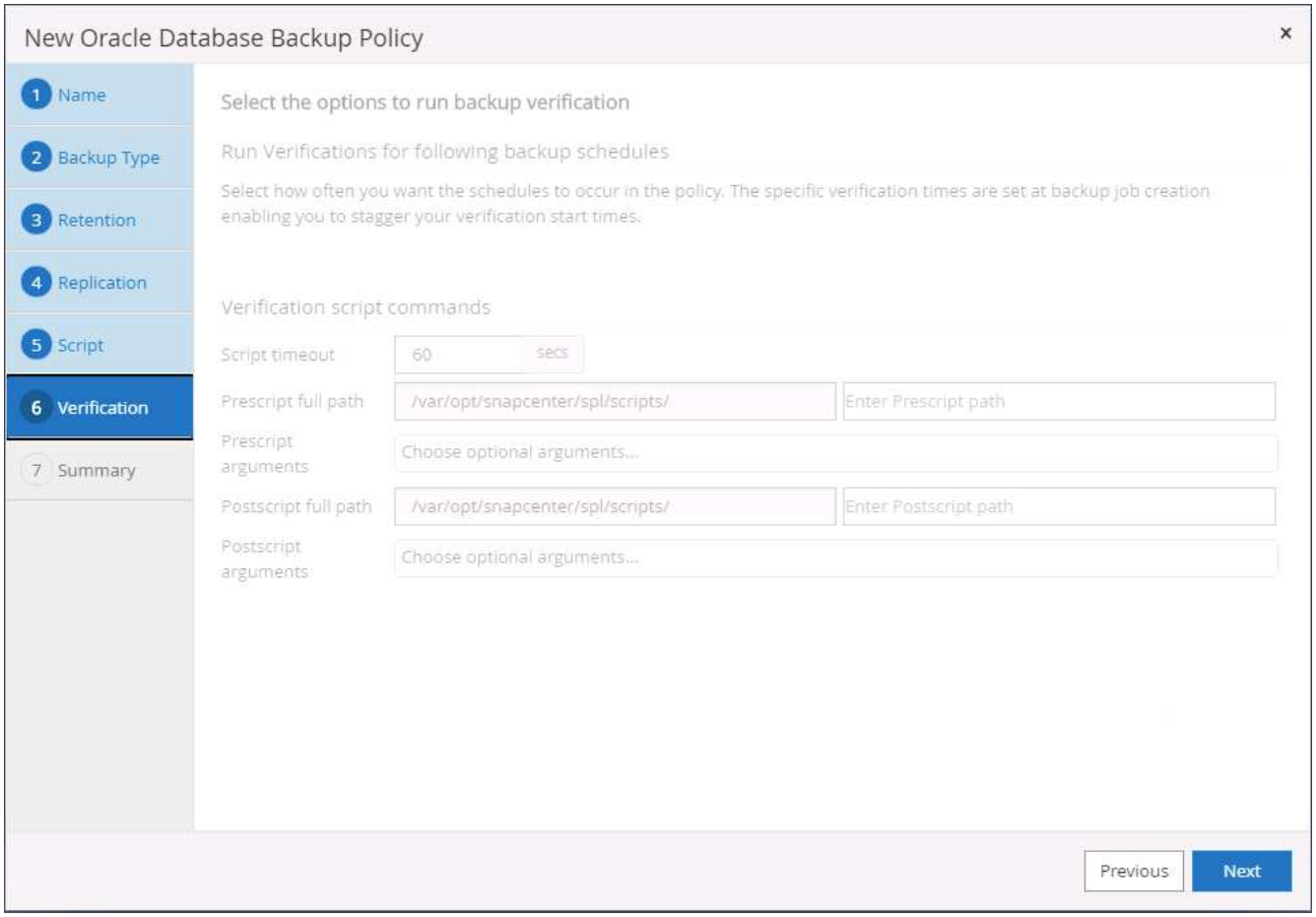
5. Répliquez la réplication dans un emplacement secondaire dans le cloud public.



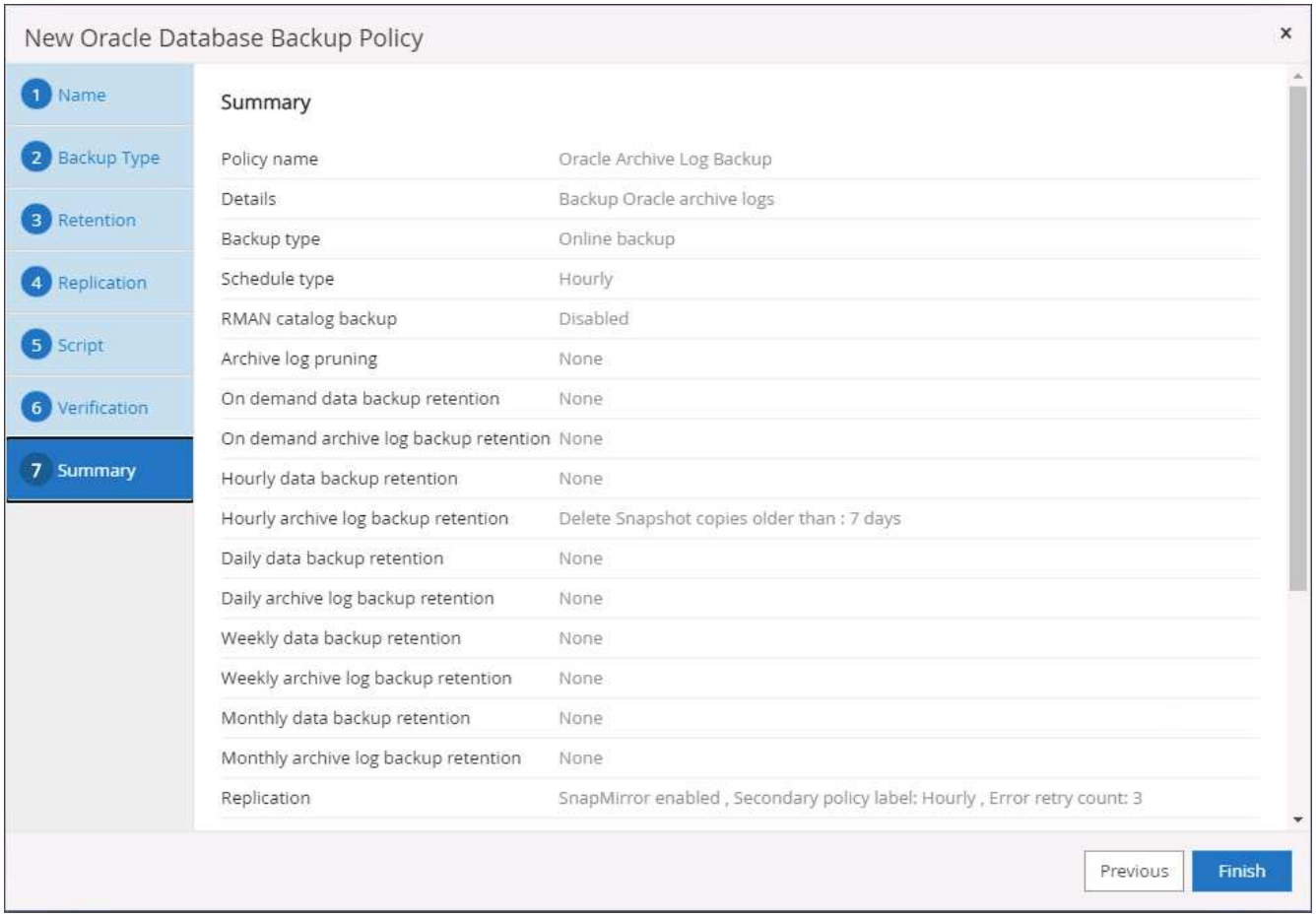
6. Spécifiez tous les scripts facultatifs à exécuter avant et après la sauvegarde du journal.



7. Spécifiez tous les scripts de vérification de sauvegarde.

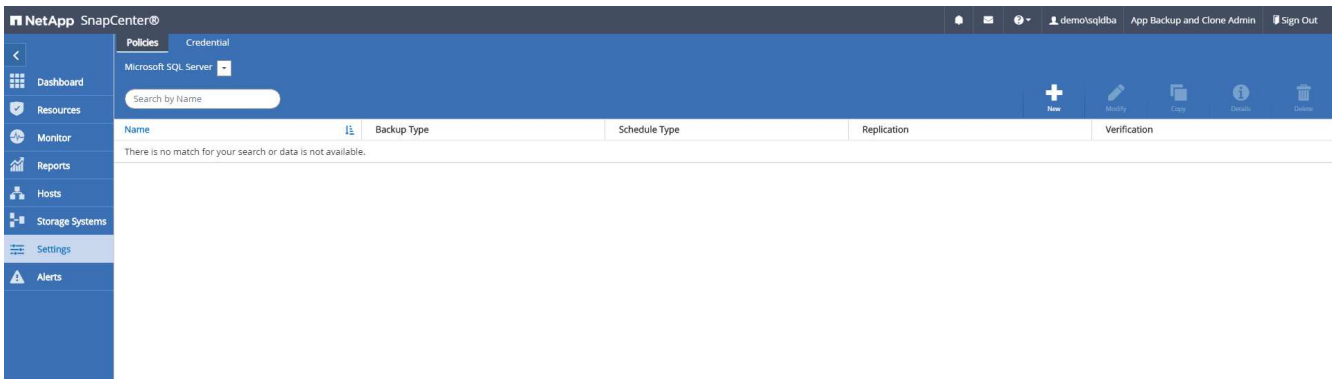


8. Récapitulatif.

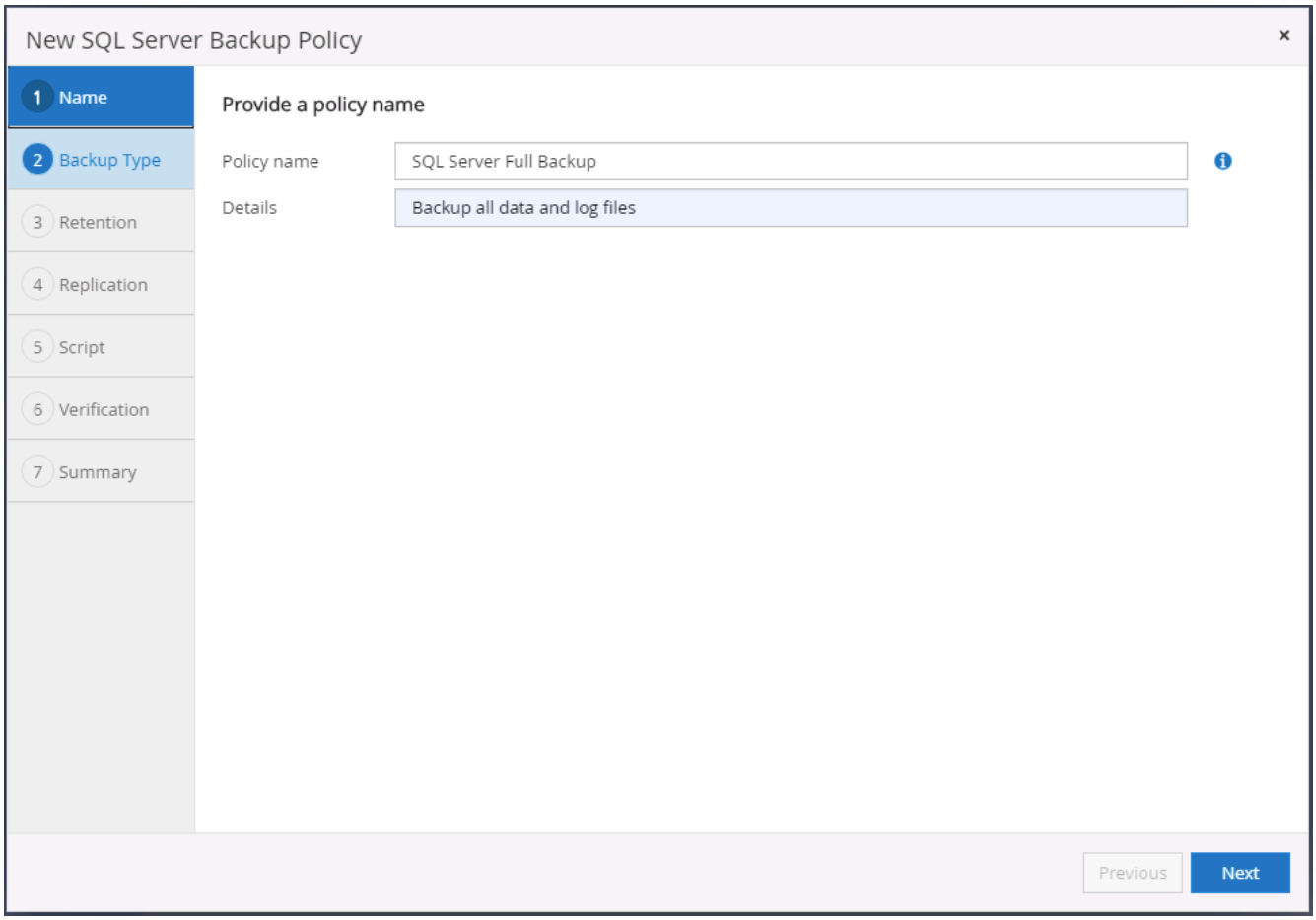


Créez une stratégie de sauvegarde complète de la base de données pour SQL

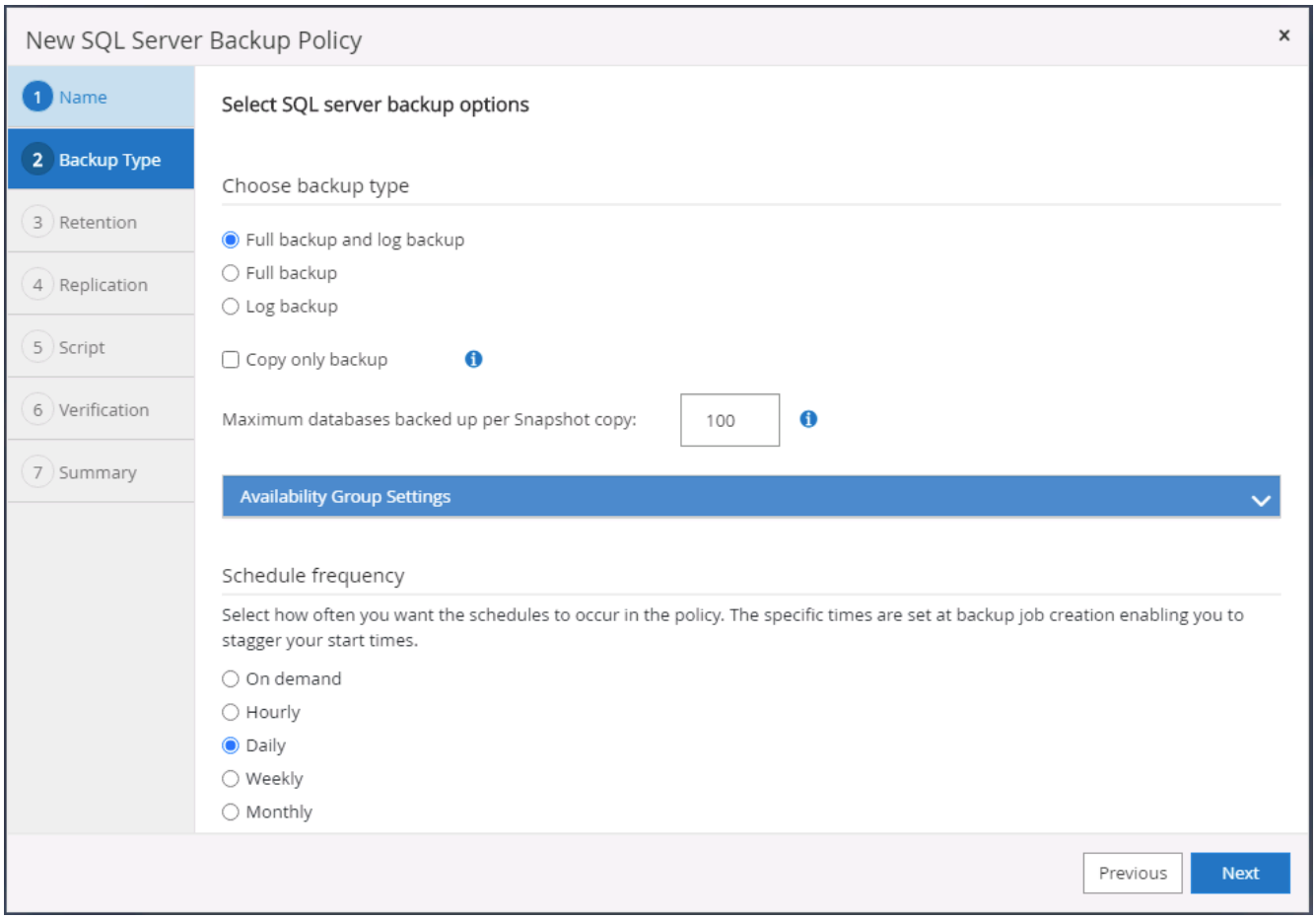
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur stratégies.



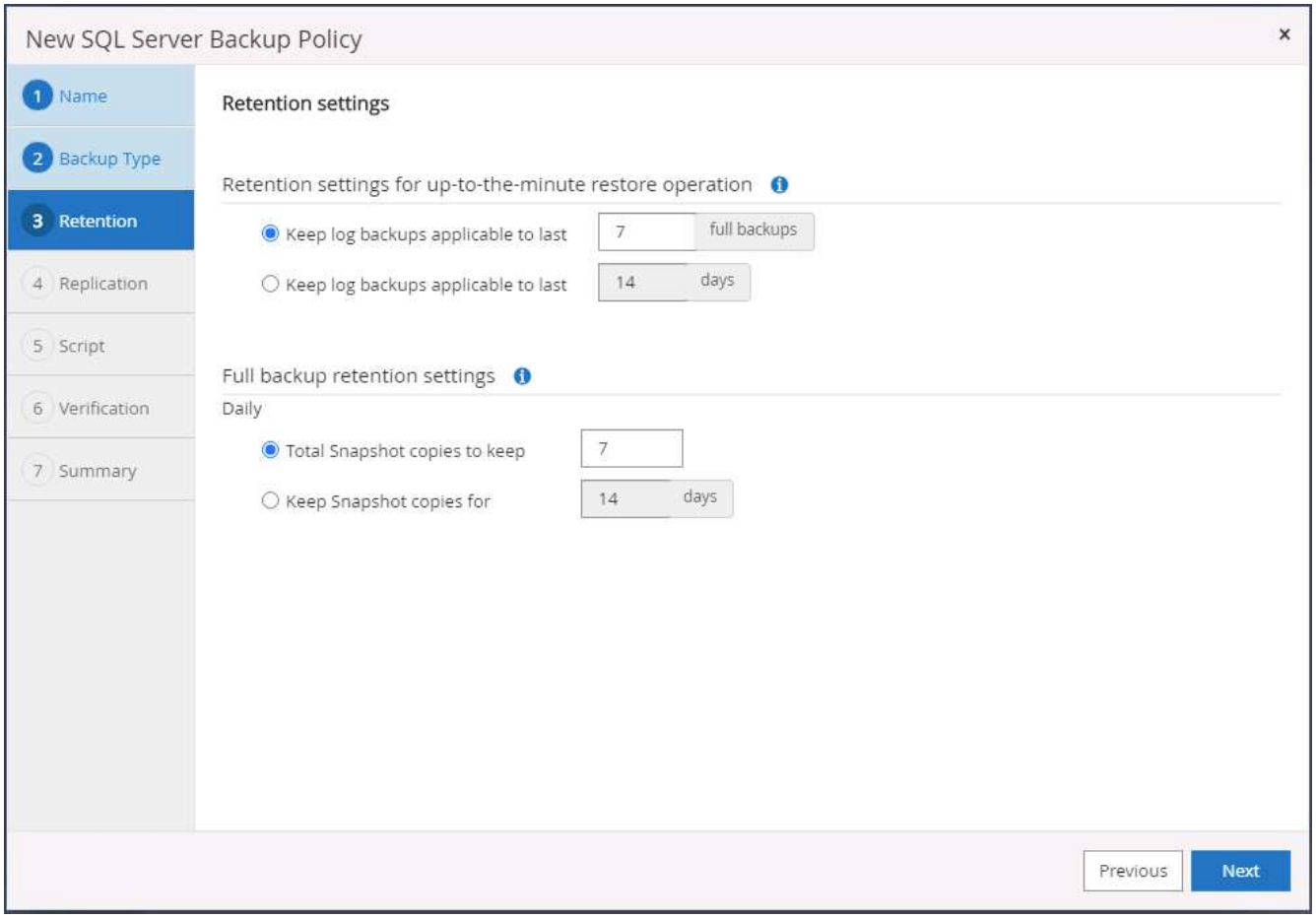
2. Cliquez sur Nouveau pour lancer un nouveau workflow de création de stratégie de sauvegarde ou choisissez une stratégie existante à modifier.



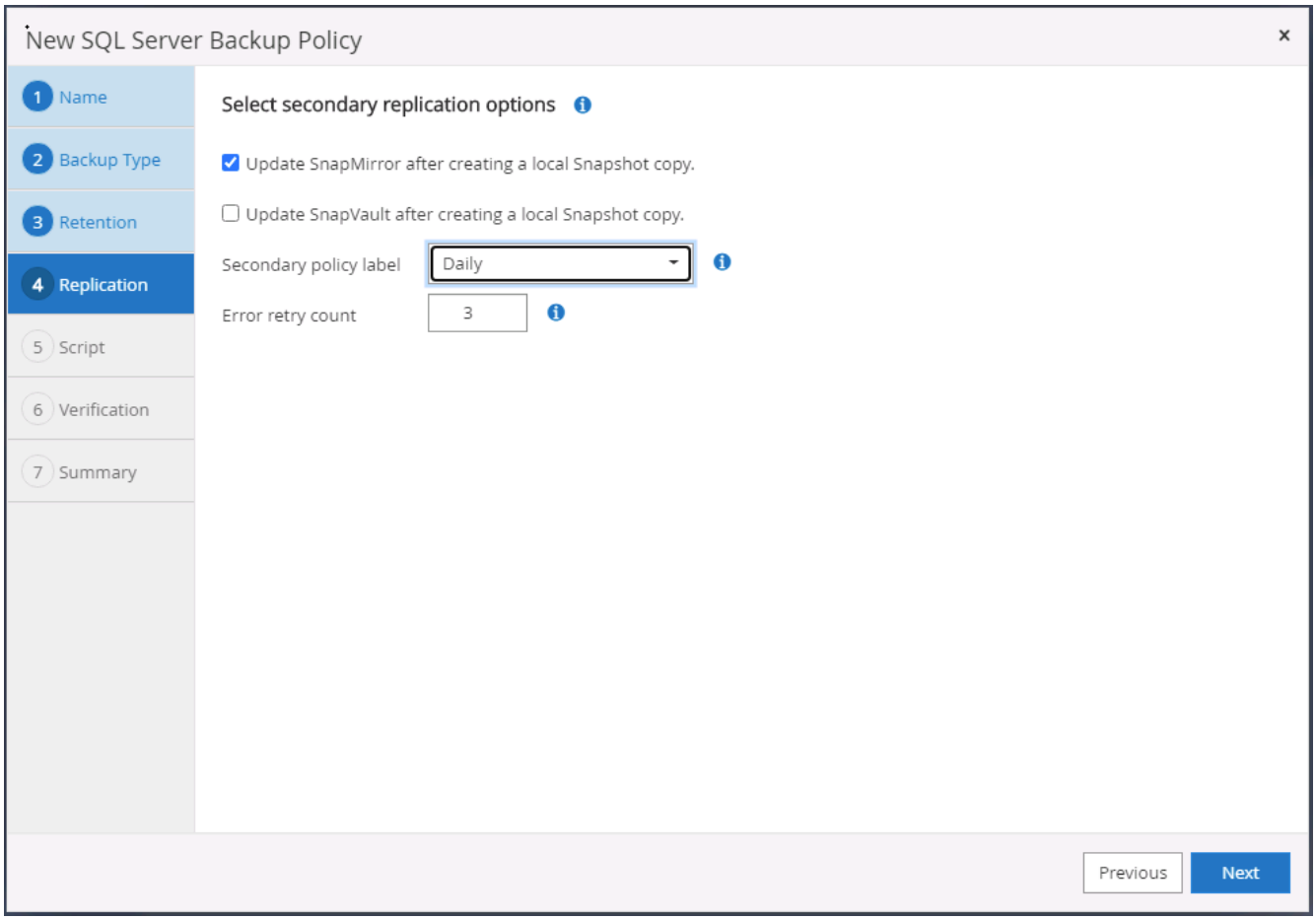
3. Définissez l'option de sauvegarde et la fréquence de planification. Pour SQL Server configuré avec un groupe de disponibilité, il est possible de définir une réplique de sauvegarde préférée.



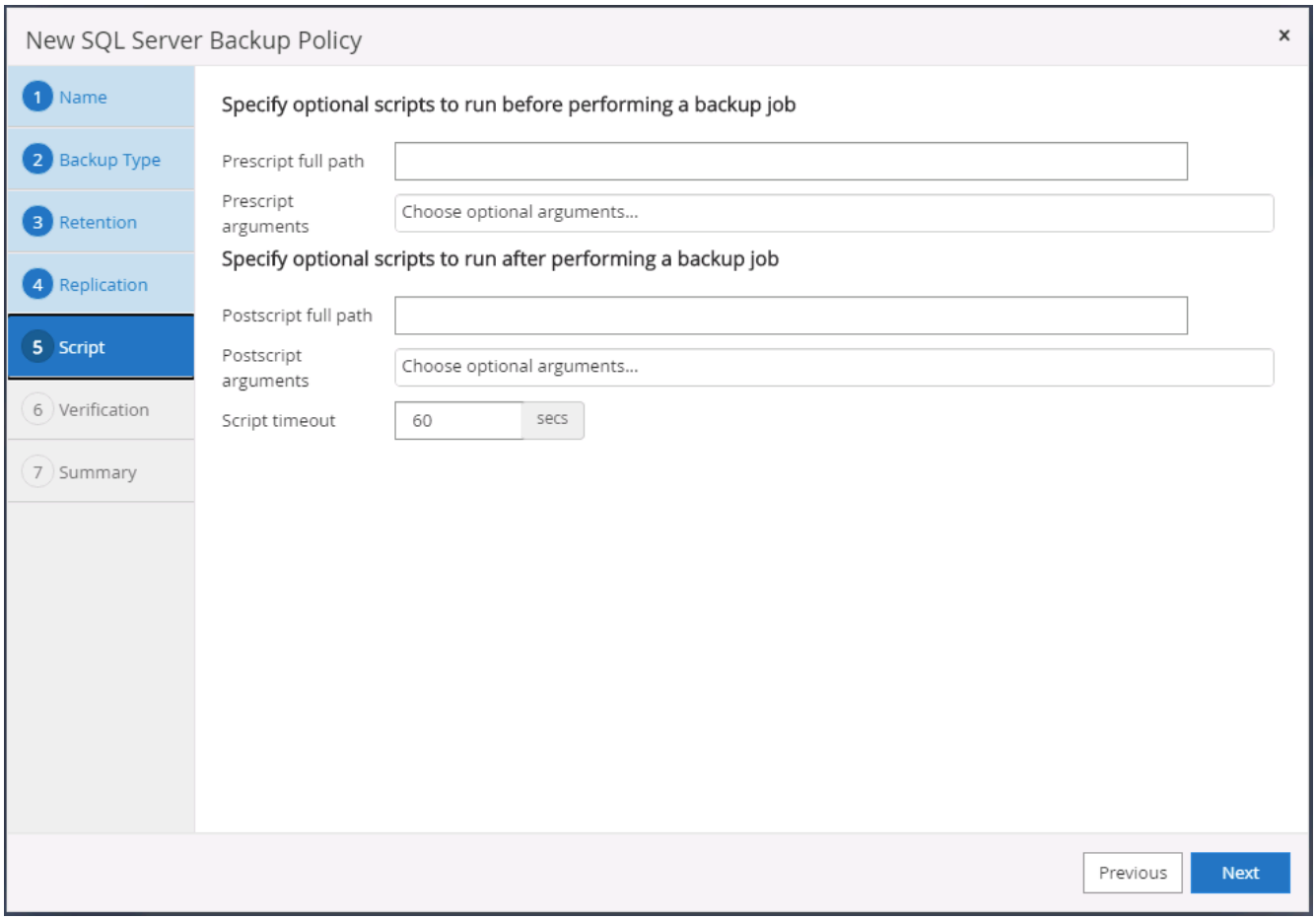
4. Définissez la période de conservation des sauvegardes.



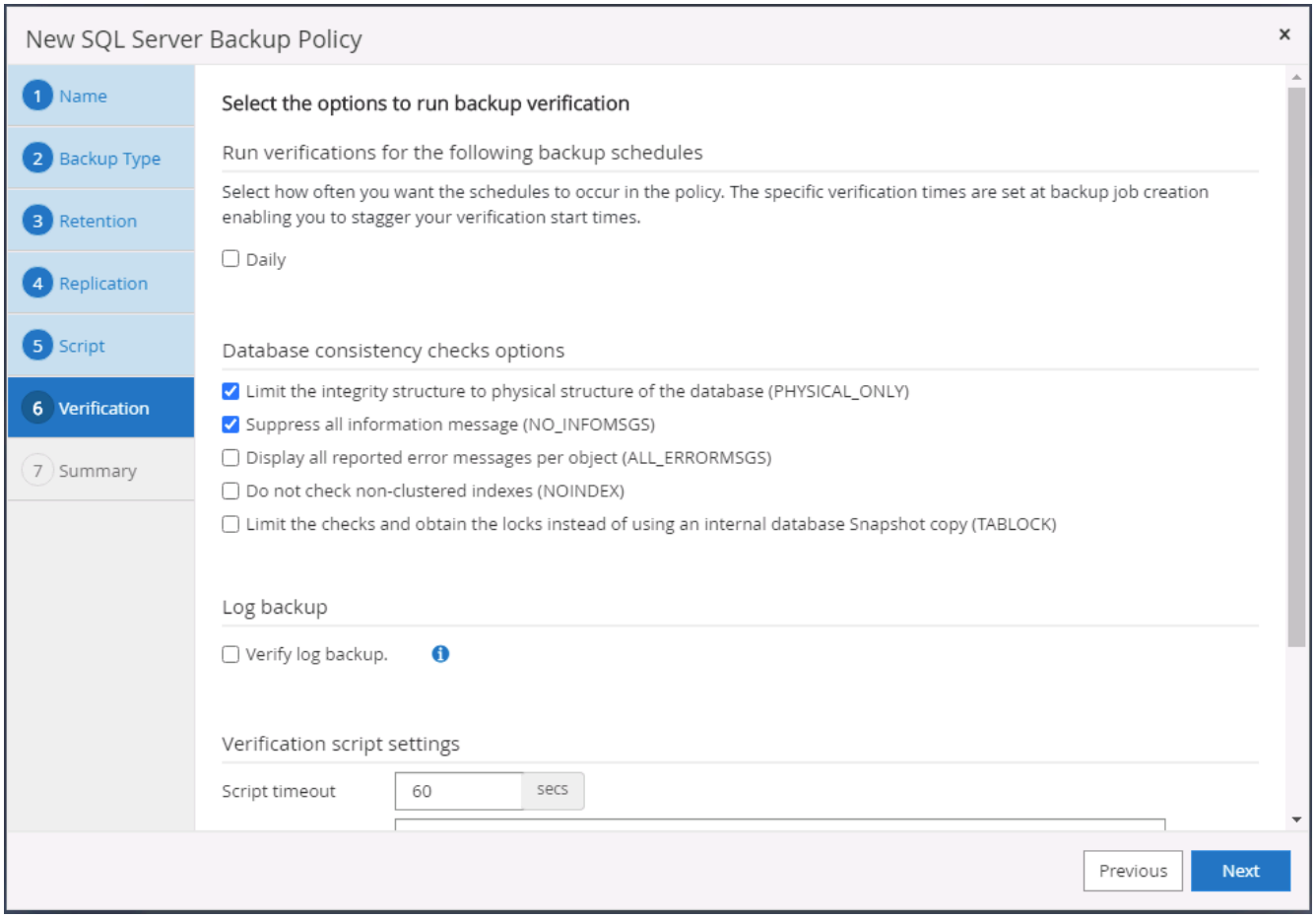
5. Intégrez la réplication de copie de sauvegarde à un emplacement secondaire dans le cloud.



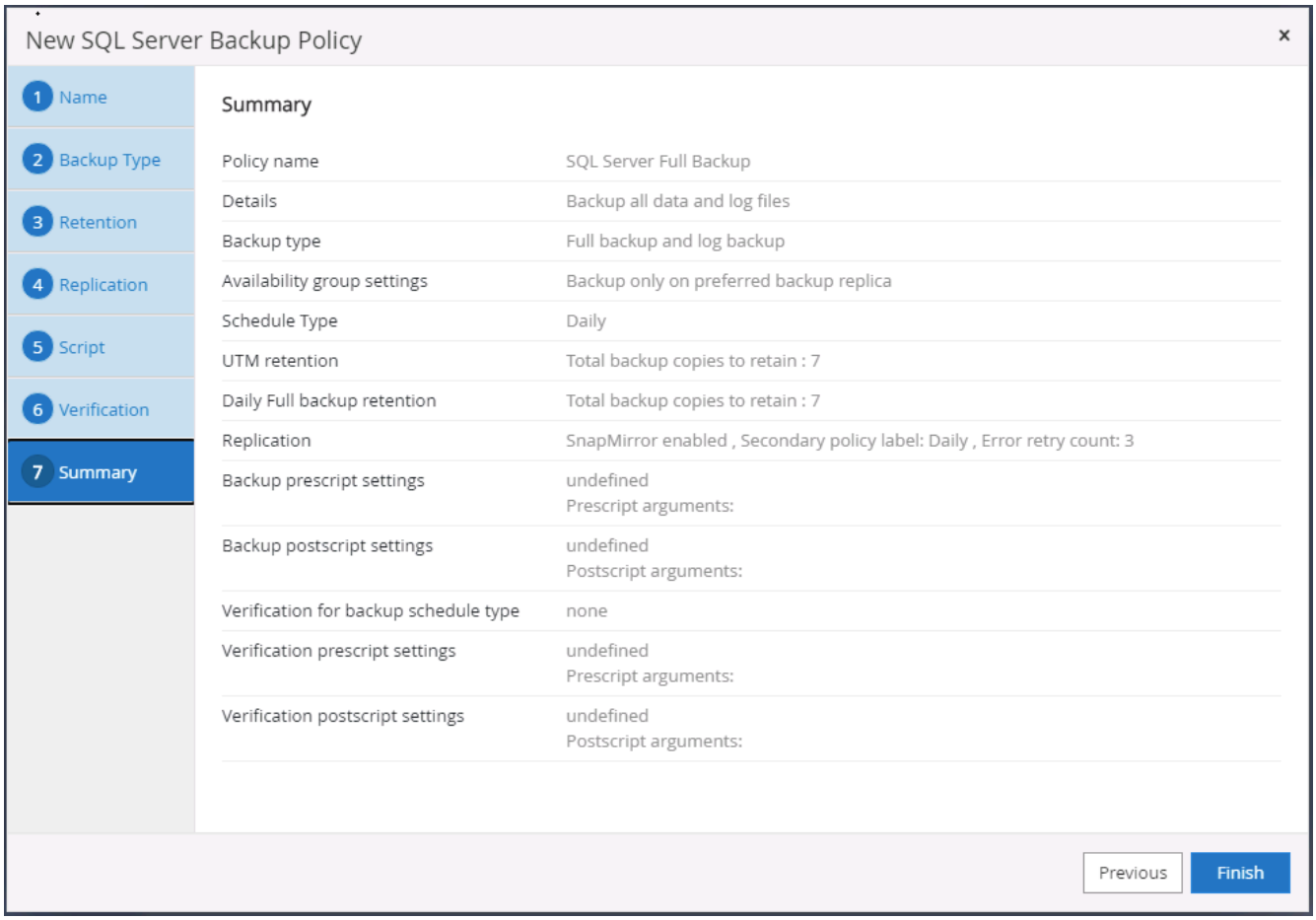
6. Spécifiez tous les scripts facultatifs à exécuter avant ou après une procédure de sauvegarde.



7. Spécifiez les options d’exécution de la vérification de sauvegarde.

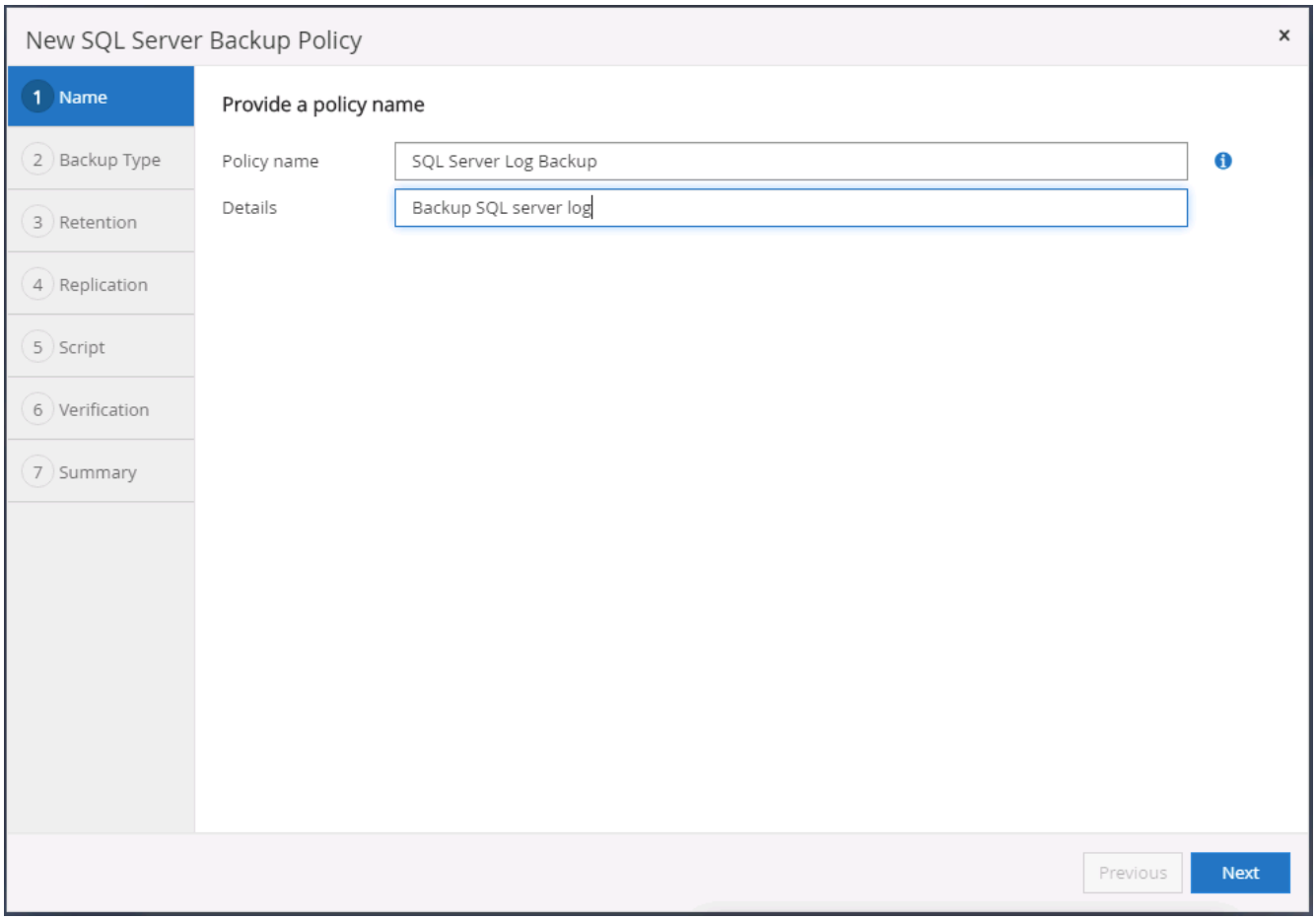


8. Récapitulatif.

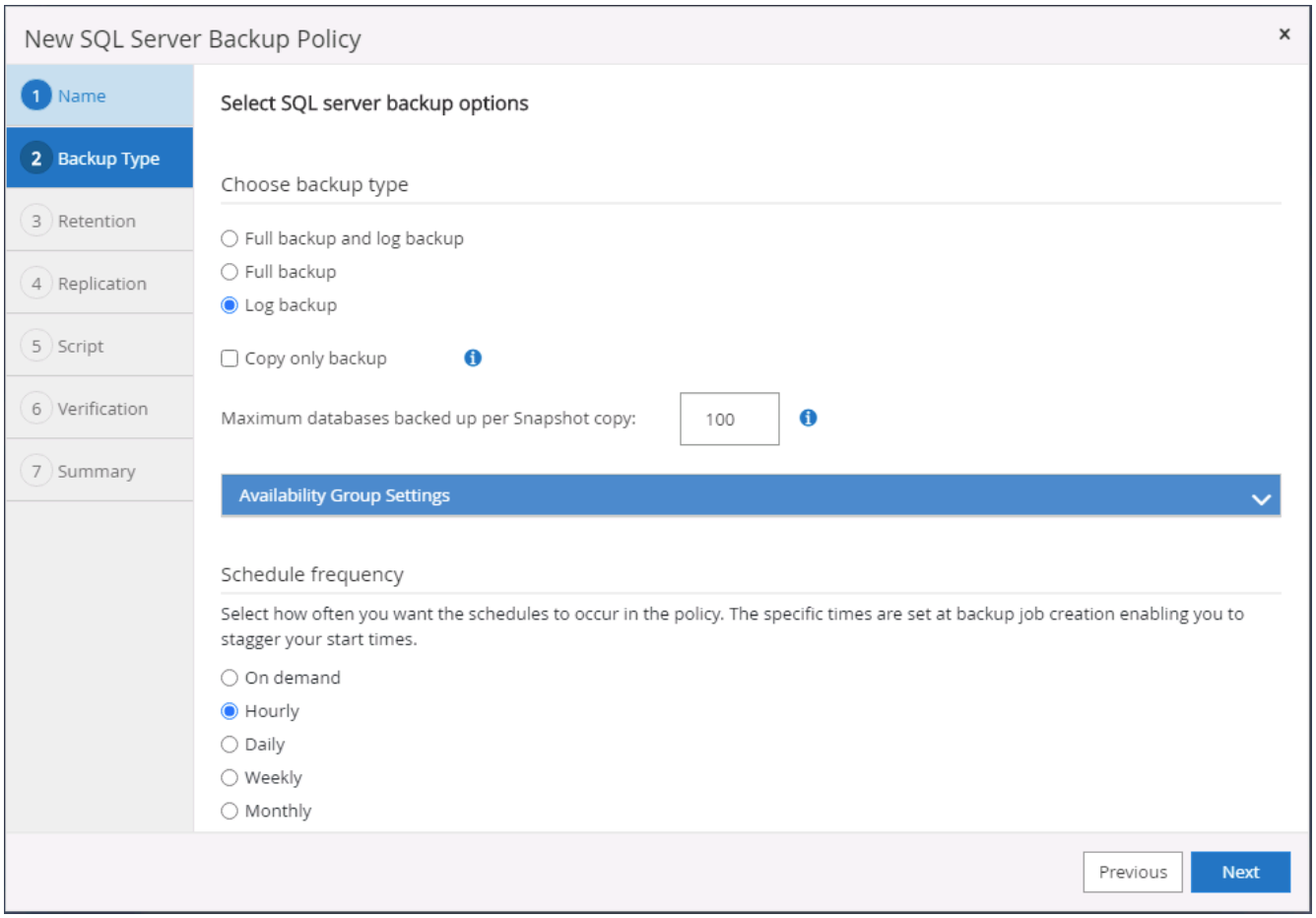


Créez une stratégie de sauvegarde du journal de base de données pour SQL.

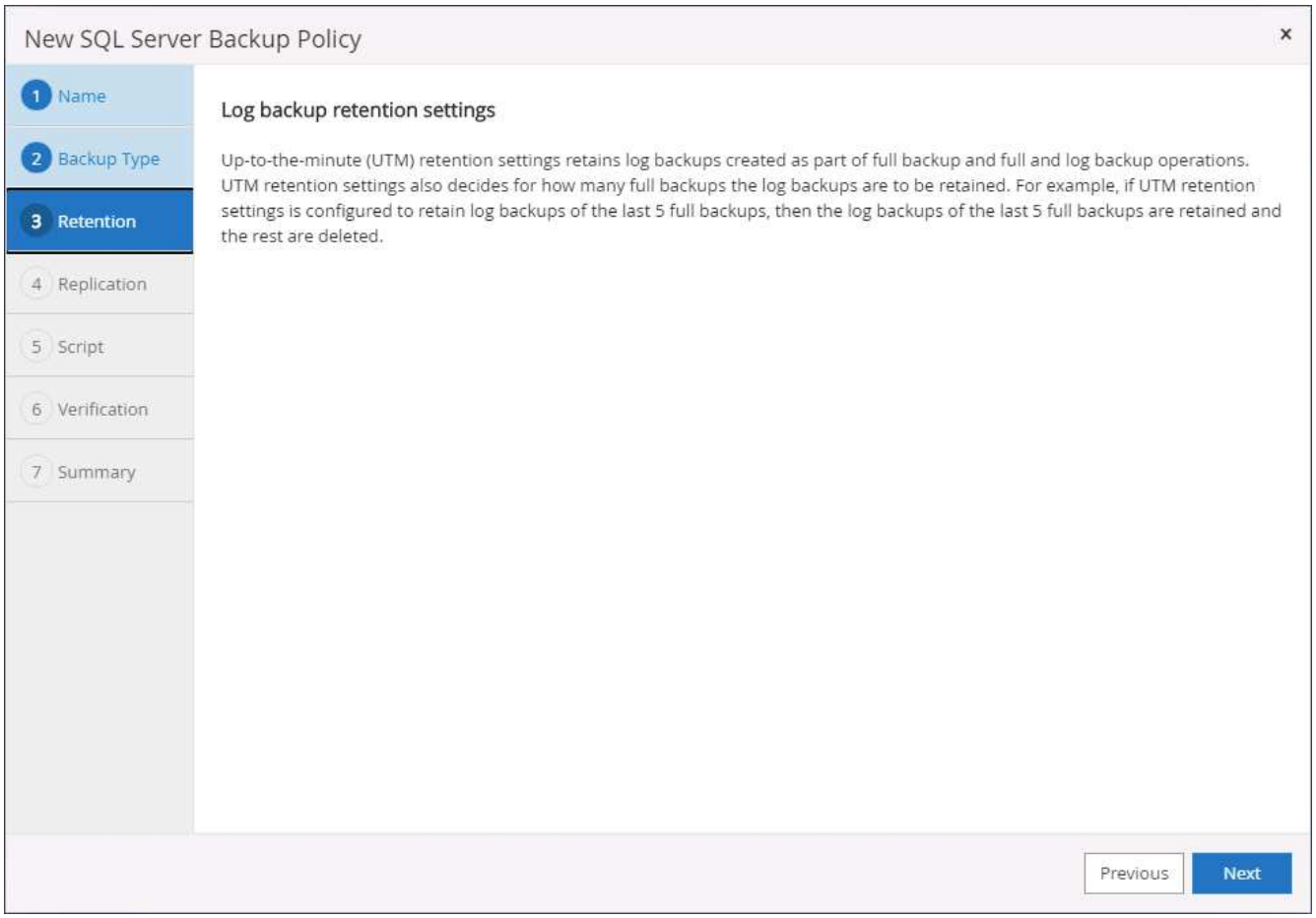
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données, cliquez sur Paramètres > règles, puis sur Nouveau pour lancer un nouveau workflow de création de règles.



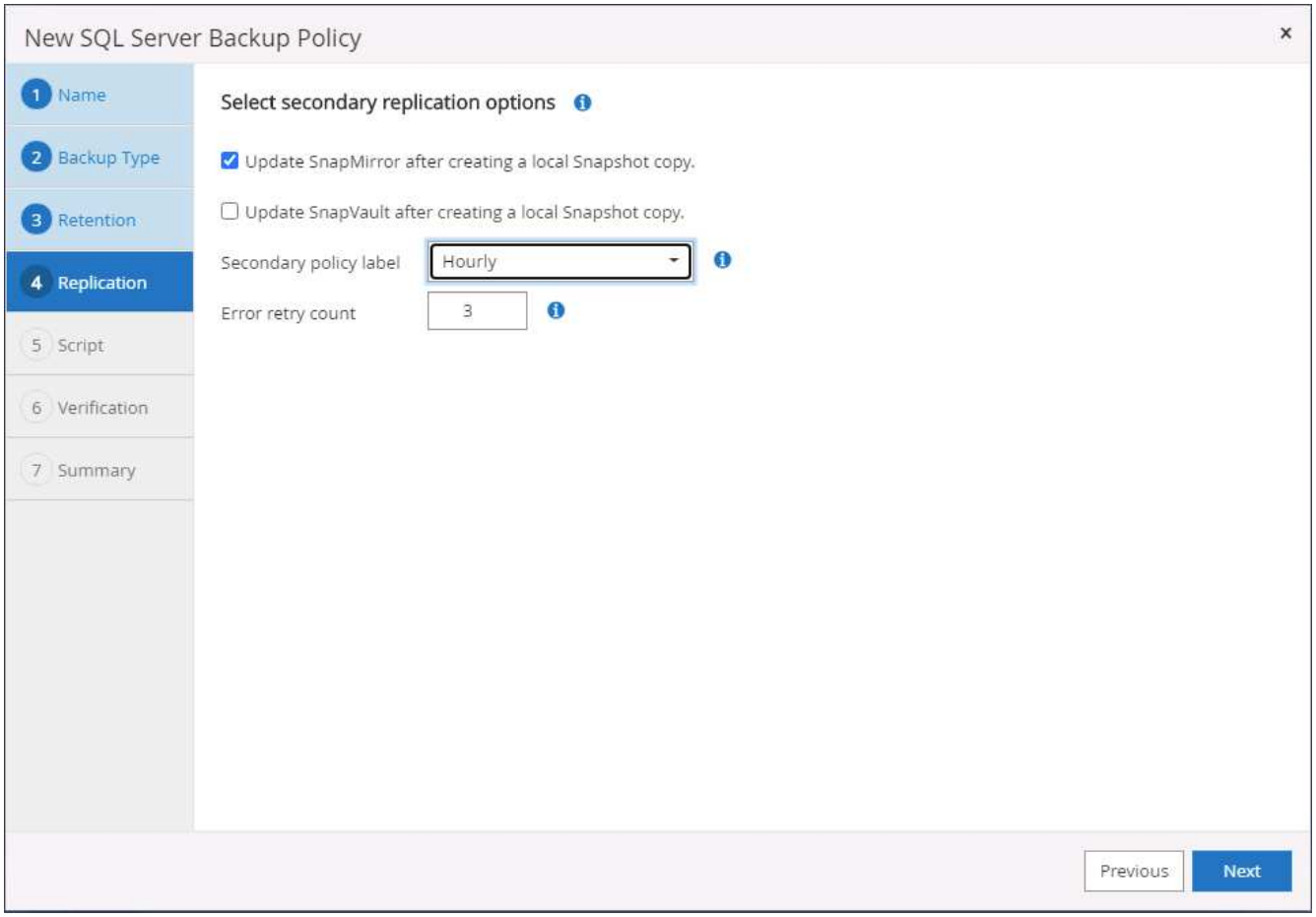
2. Définissez l'option de sauvegarde du journal et la fréquence de planification. Pour SQL Server configuré avec un groupe de disponibilité, une réplique de sauvegarde préférée peut être définie.



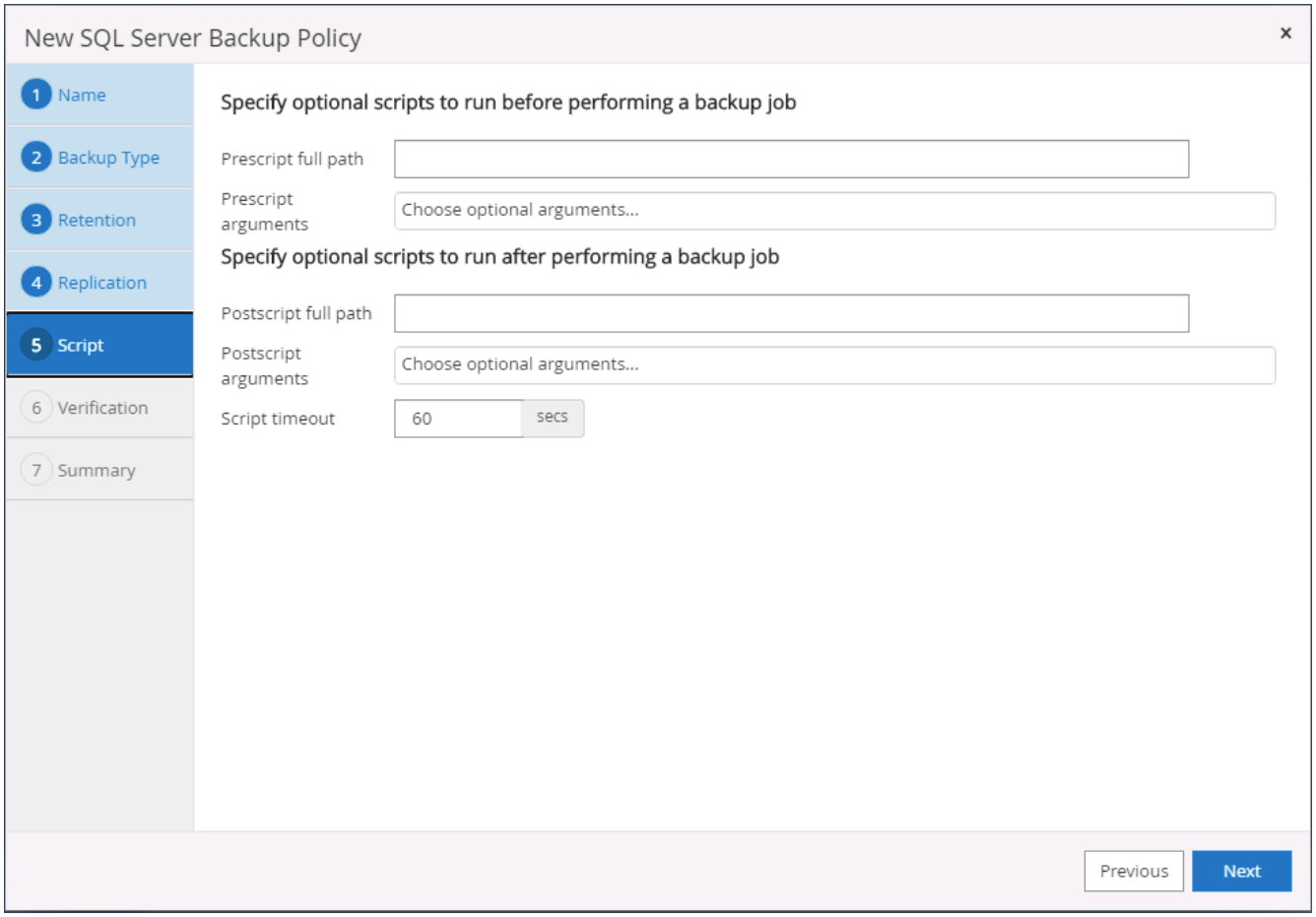
3. La stratégie de sauvegarde des données de SQL Server définit la rétention de la sauvegarde des journaux ; acceptez les valeurs par défaut ici.



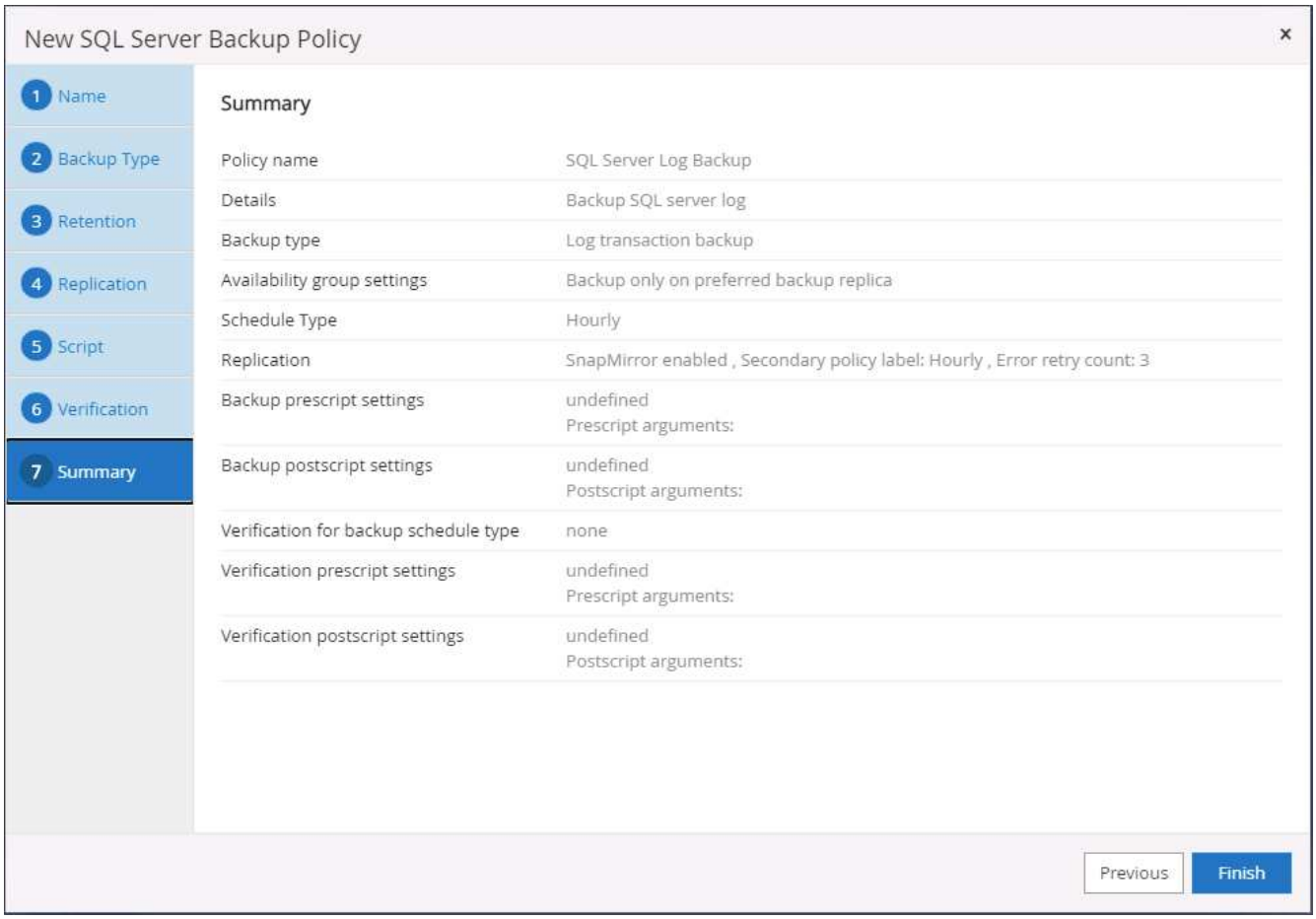
4. Réplication de sauvegardes de journaux sur un stockage secondaire dans le cloud.



5. Spécifiez tous les scripts facultatifs à exécuter avant ou après une procédure de sauvegarde.



6. Récapitulatif.

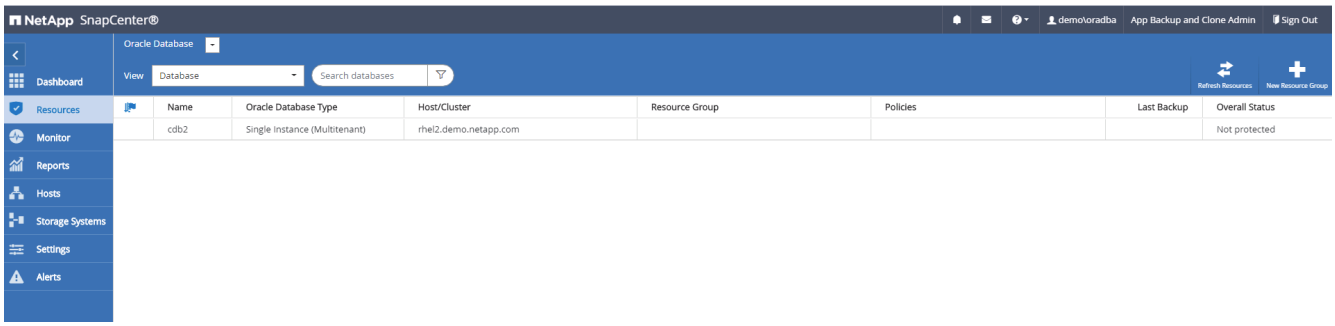


8. Mettre en œuvre une politique de sauvegarde pour protéger la base de données

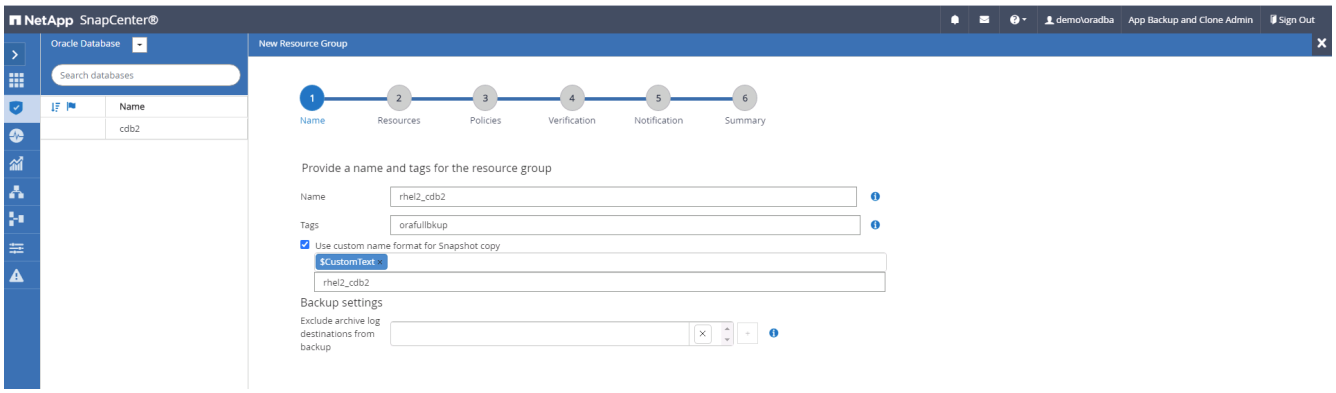
SnapCenter utilise un groupe de ressources pour sauvegarder une base de données dans un groupe logique de ressources de bases de données, par exemple plusieurs bases de données hébergées sur un serveur, une base de données partageant les mêmes volumes de stockage, plusieurs bases de données prenant en charge une application professionnelle, etc. La protection d'une base de données unique crée un groupe de ressources lui-même. Les procédures suivantes montrent comment mettre en œuvre une stratégie de sauvegarde créée à la section 7 pour protéger les bases de données Oracle et SQL Server.

Créez un groupe de ressources pour la sauvegarde complète d'Oracle

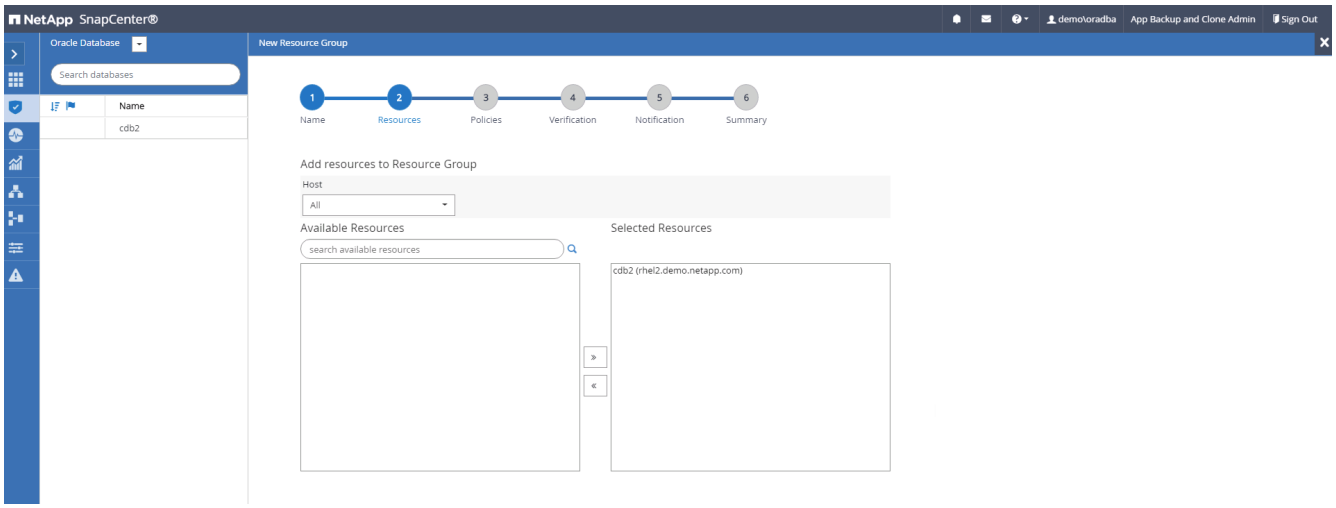
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez base de données ou Groupe de ressources pour lancer le flux de travail de création de groupe de ressources.



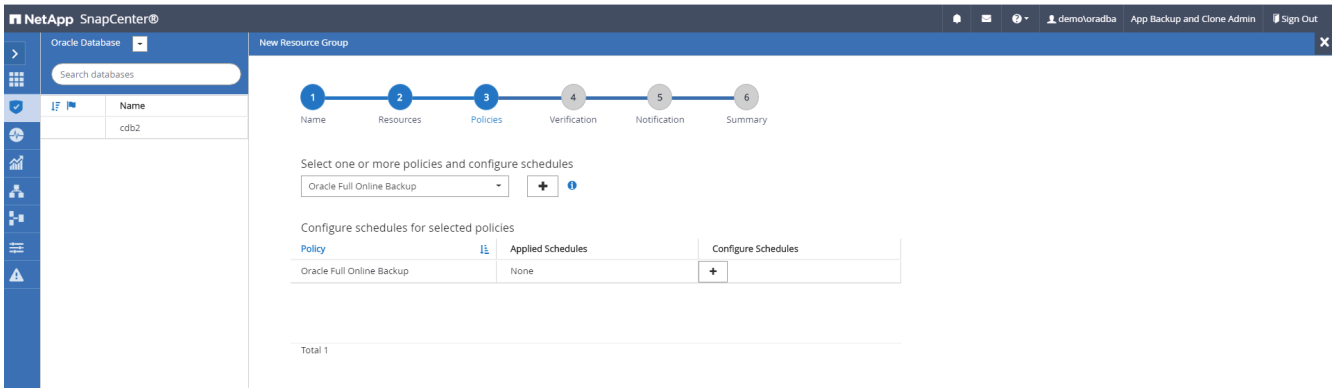
2. Indiquez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format de nommage pour la copie Snapshot et contourner la destination redondante du journal d'archivage si elle est configurée.



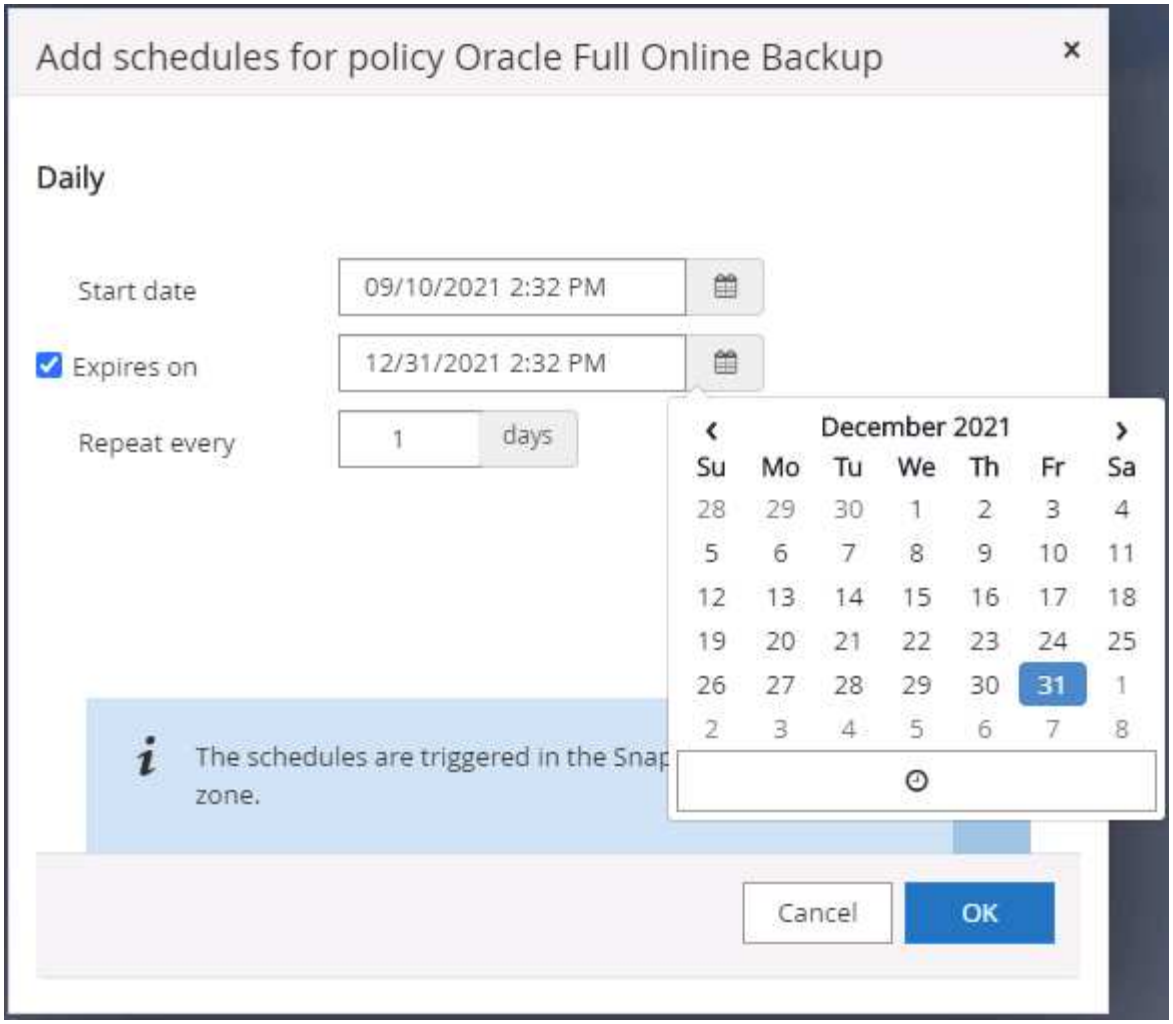
3. Ajoutez des ressources de base de données au groupe de ressources.



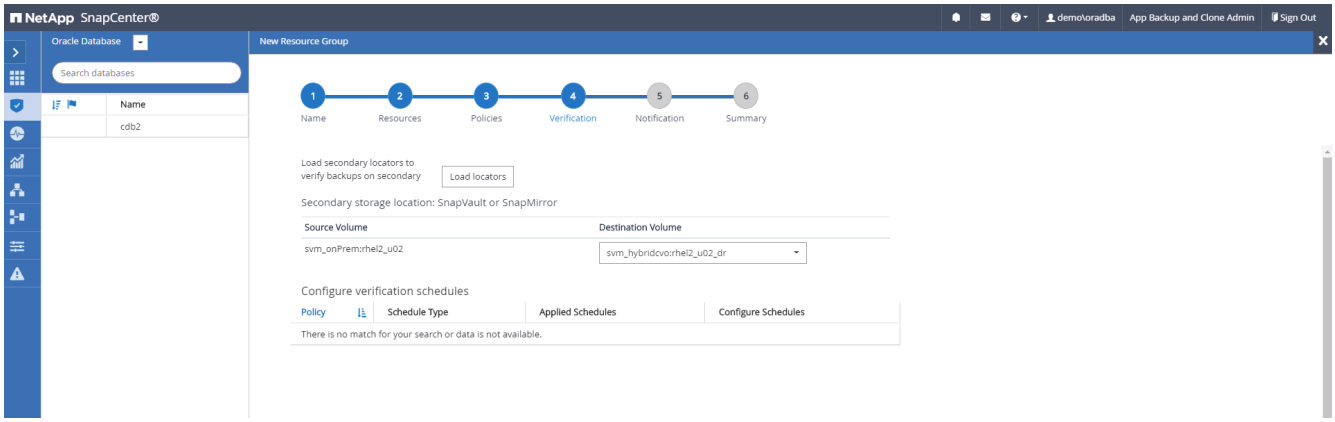
4. Sélectionnez une stratégie de sauvegarde complète créée dans la section 7 dans la liste déroulante.



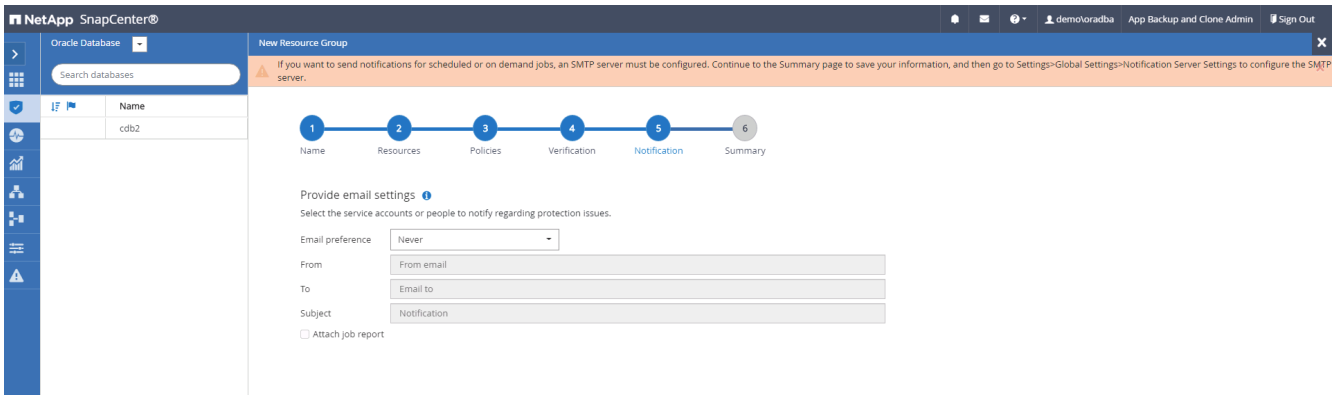
5. Cliquez sur le signe (+) pour configurer le programme de sauvegarde souhaité.



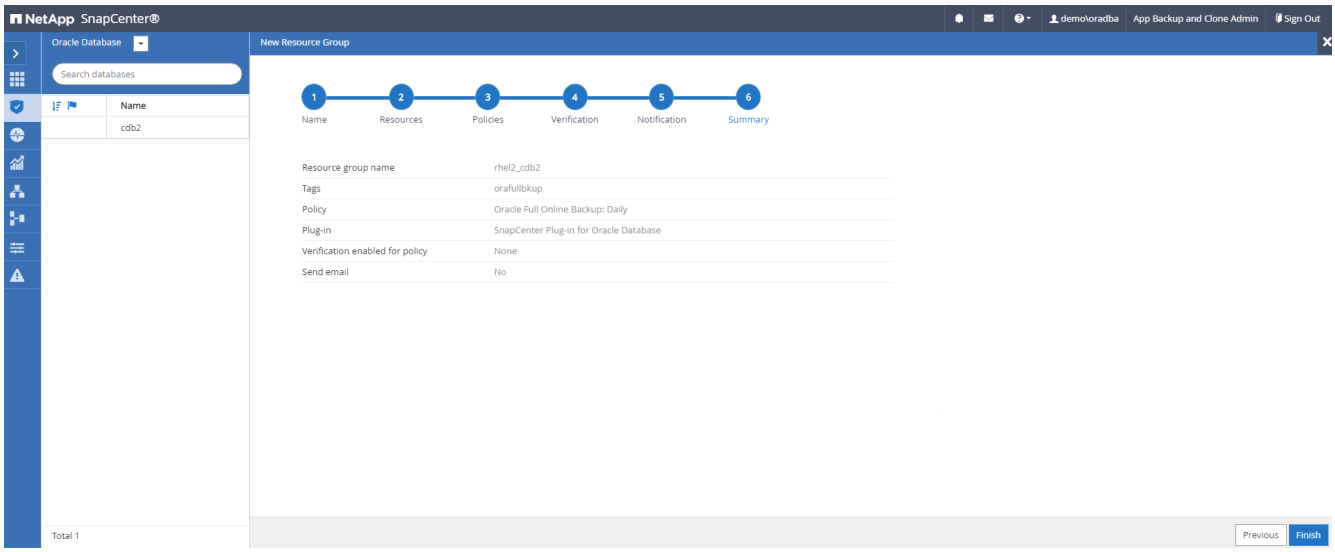
6. Cliquez sur Charger les localisateurs pour charger le volume source et le volume de destination.



7. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.

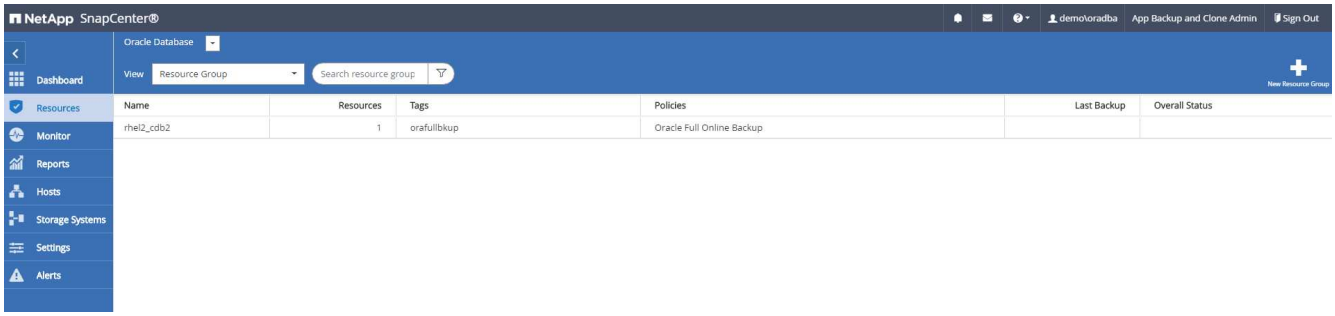


8. Récapitulatif.

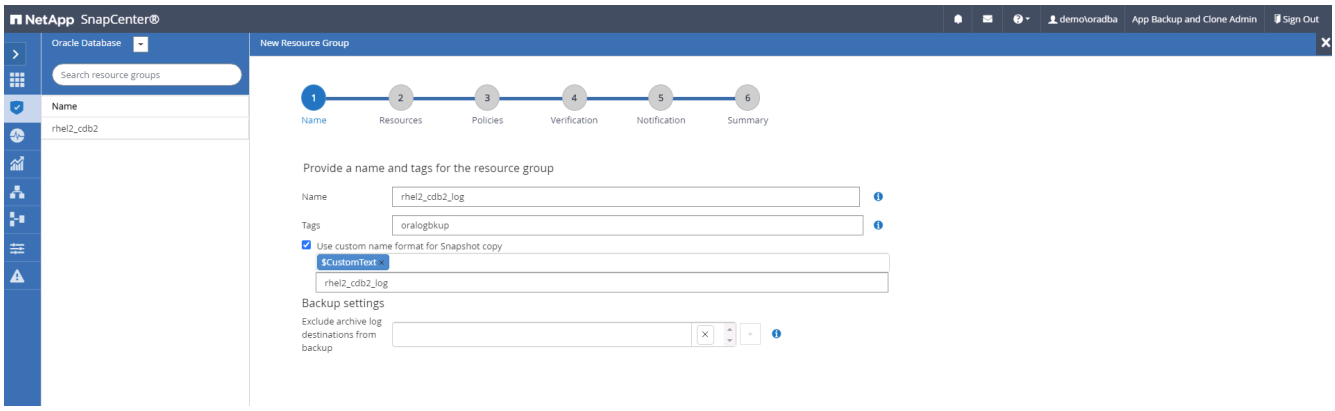


Créez un groupe de ressources pour la sauvegarde du journal d'Oracle

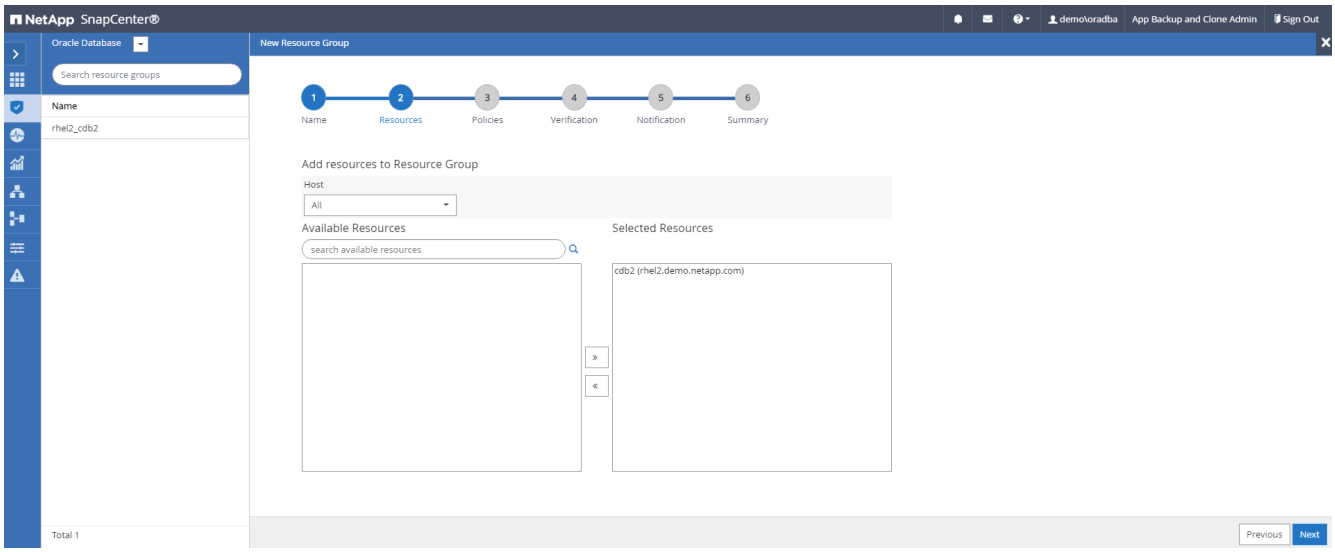
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez base de données ou Groupe de ressources pour lancer le flux de travail de création de groupe de ressources.



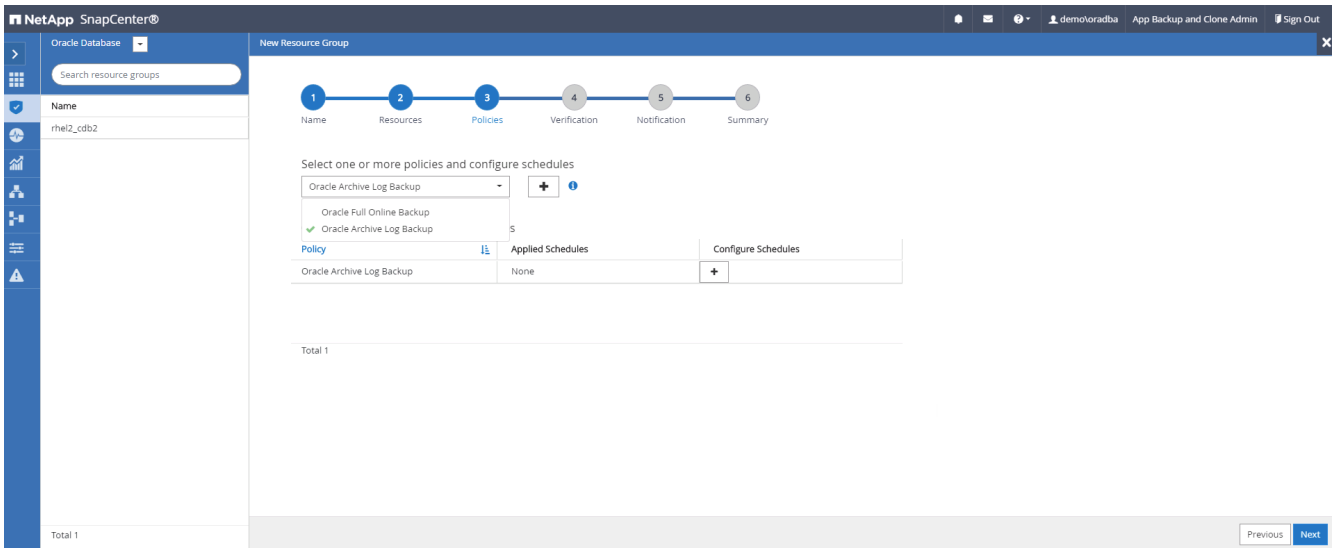
2. Indiquez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format de nommage pour la copie Snapshot et contourner la destination redondante du journal d'archivage si elle est configurée.



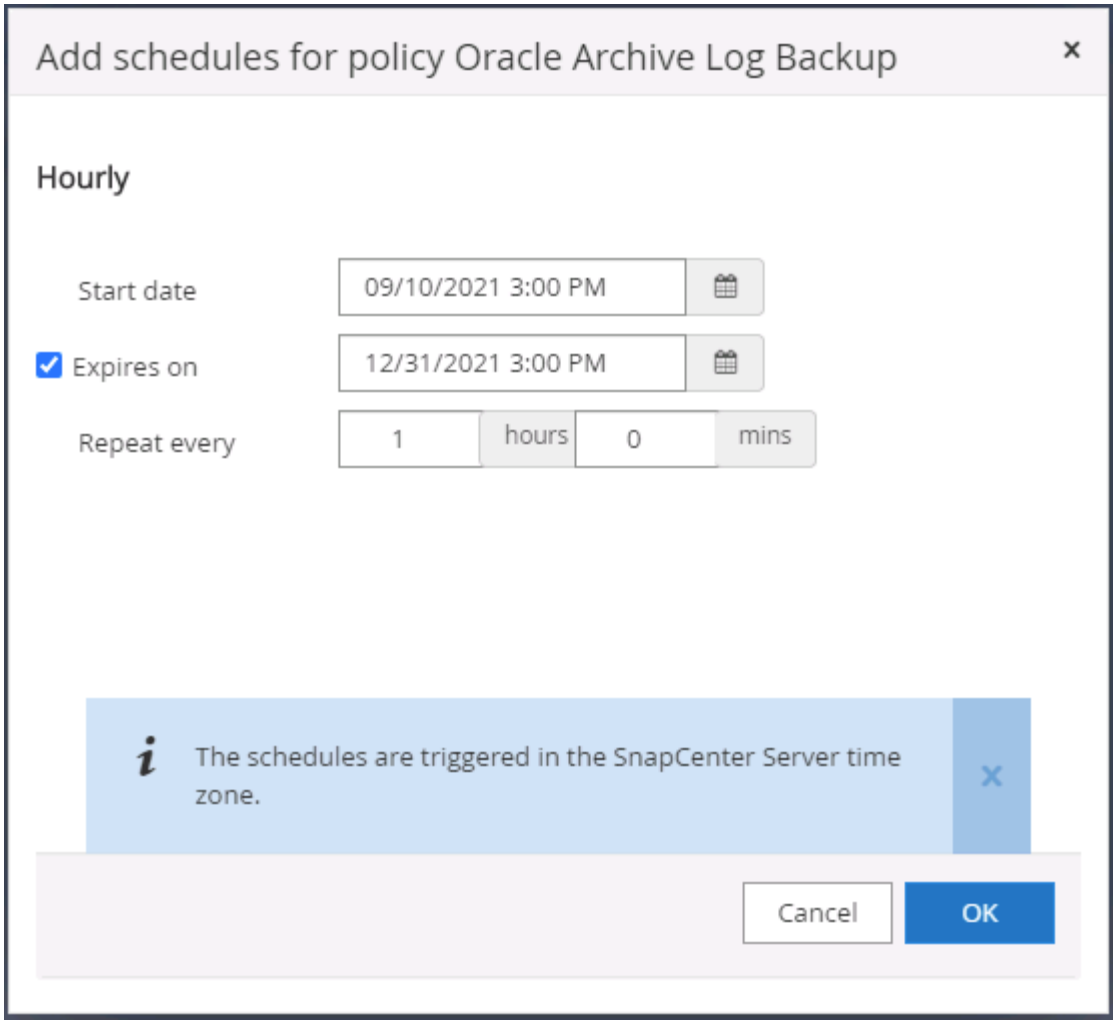
3. Ajoutez des ressources de base de données au groupe de ressources.



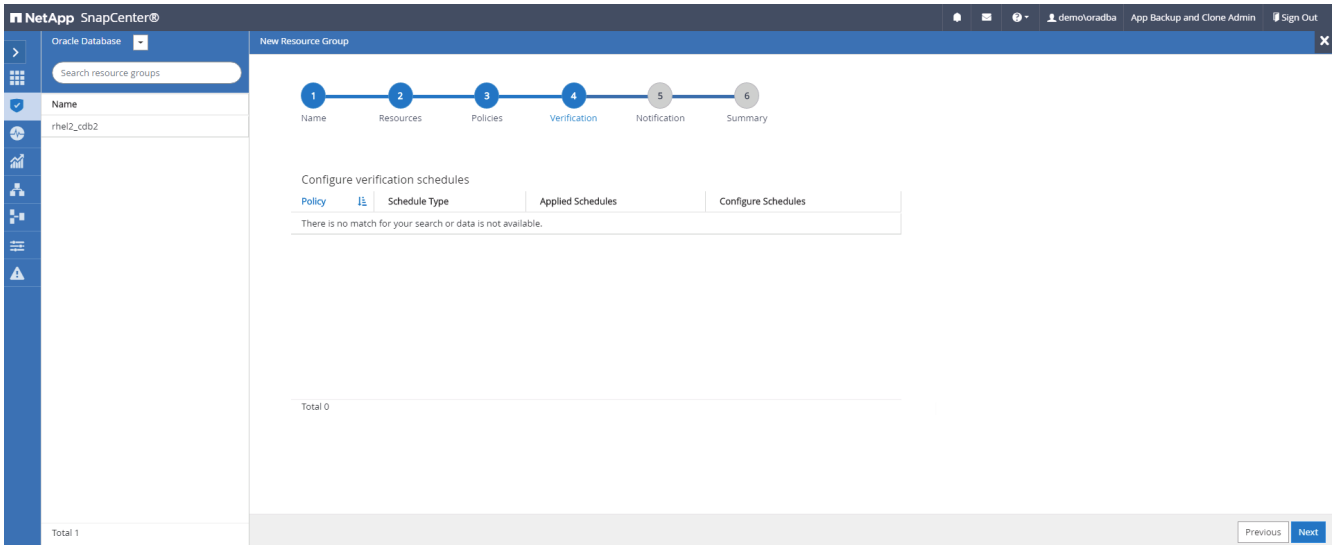
4. Sélectionnez une stratégie de sauvegarde de journal créée dans la section 7 dans la liste déroulante.



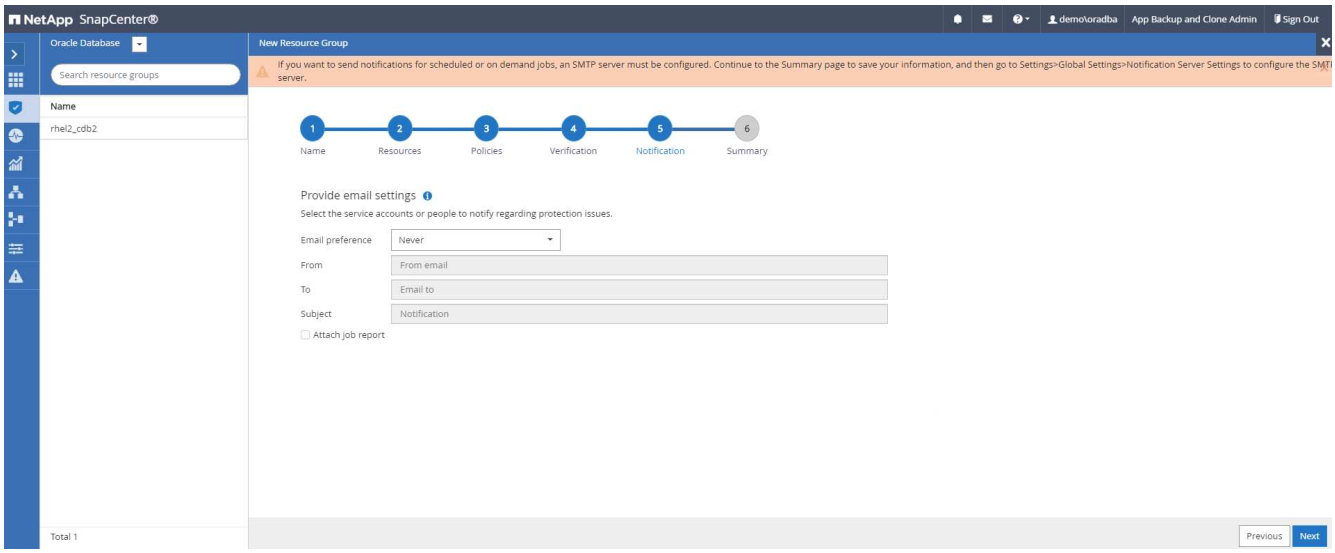
5. Cliquez sur le signe (+) pour configurer le programme de sauvegarde souhaité.



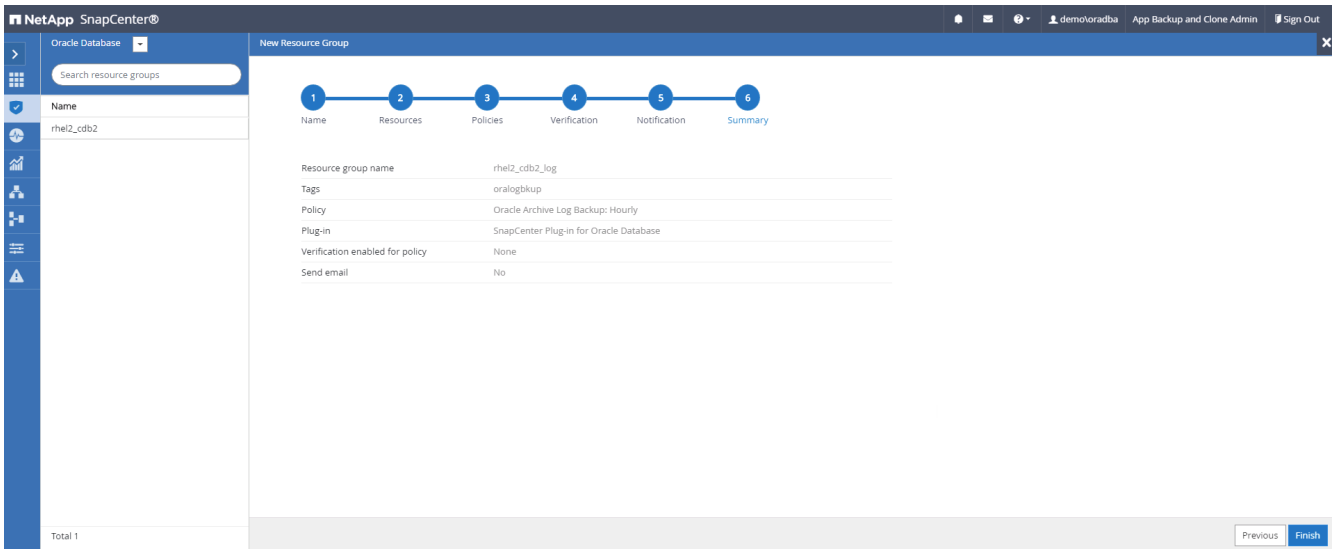
6. Si la vérification de sauvegarde est configurée, elle s'affiche ici.



7. Configurez un serveur SMTP pour la notification par e-mail si vous le souhaitez.

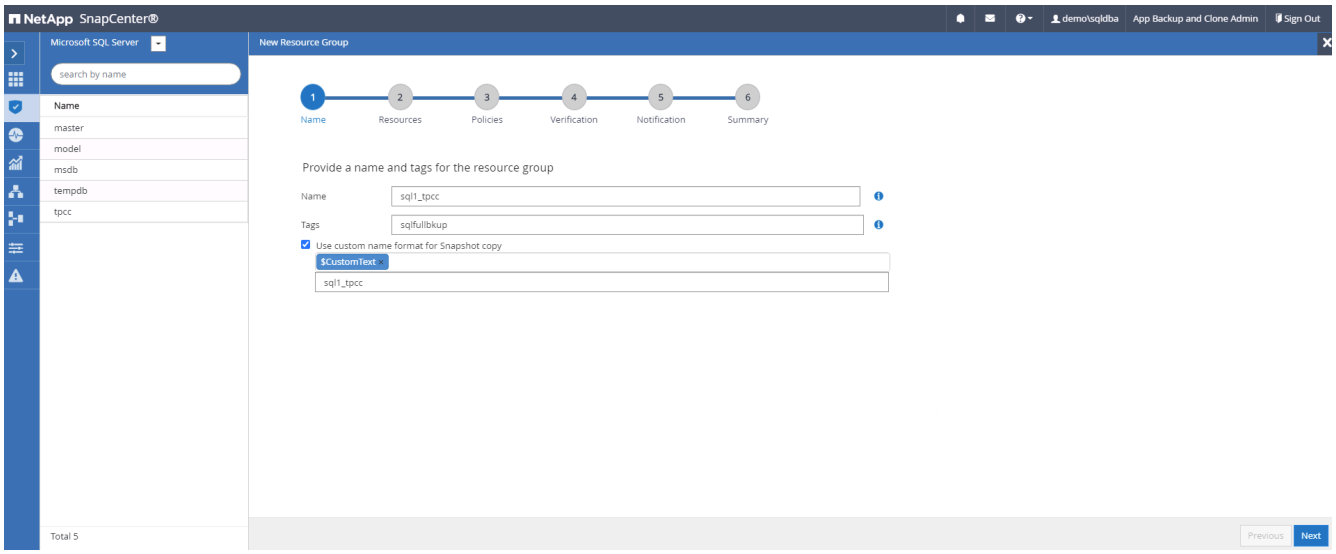


8. Récapitulatif.

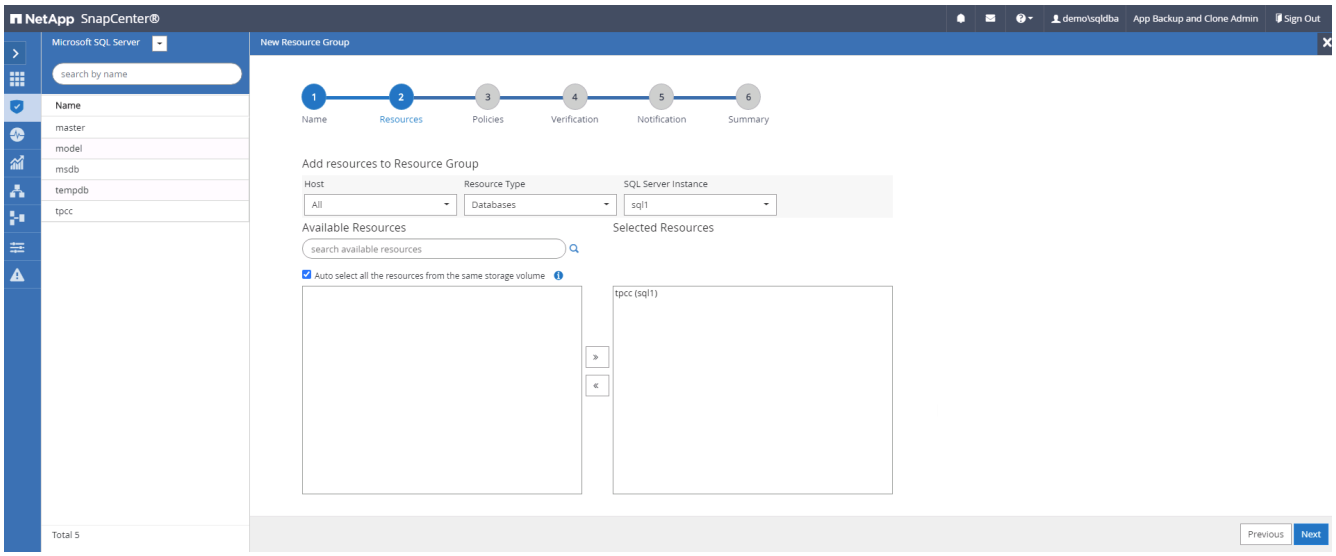


Créez un groupe de ressources pour la sauvegarde complète de SQL Server

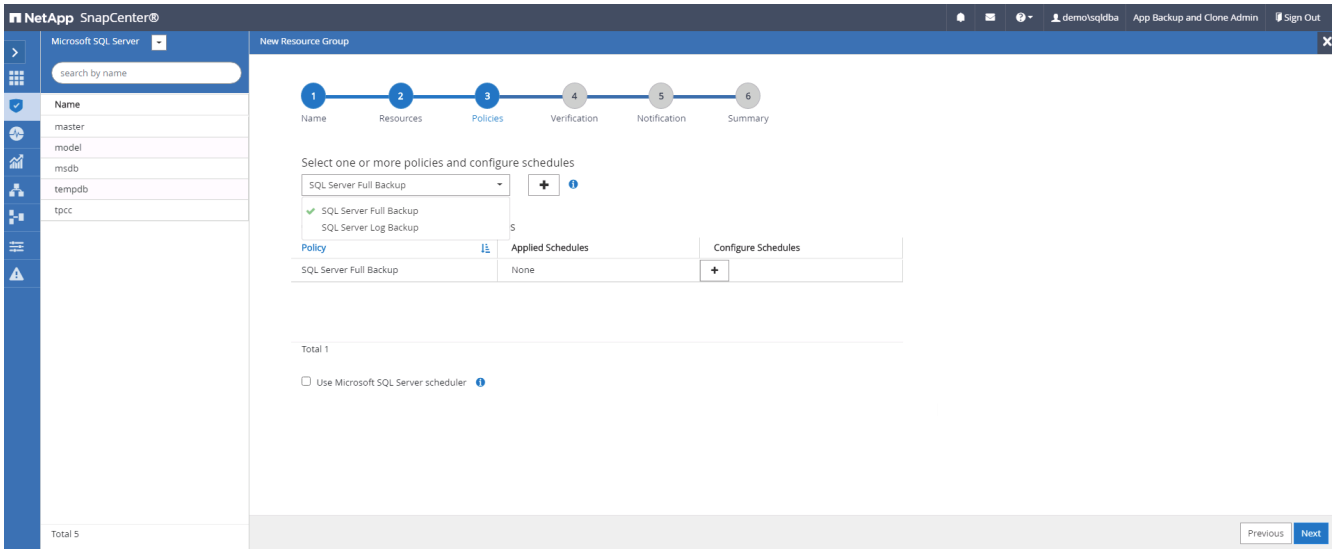
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez une base de données ou un groupe de ressources pour lancer le flux de travail de création de groupe de ressources. Indiquez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format d'attribution de nom à la copie Snapshot.



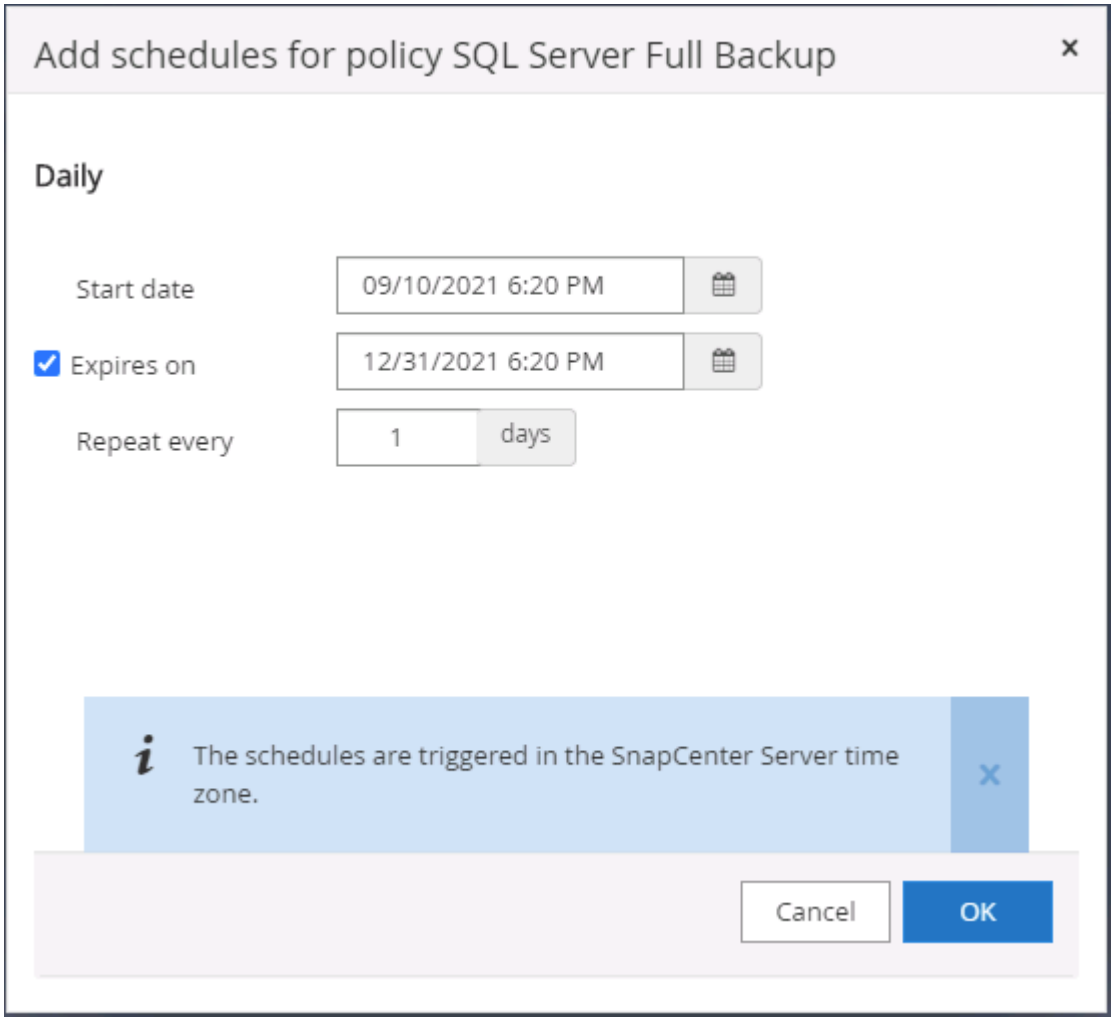
2. Sélectionnez les ressources de base de données à sauvegarder.



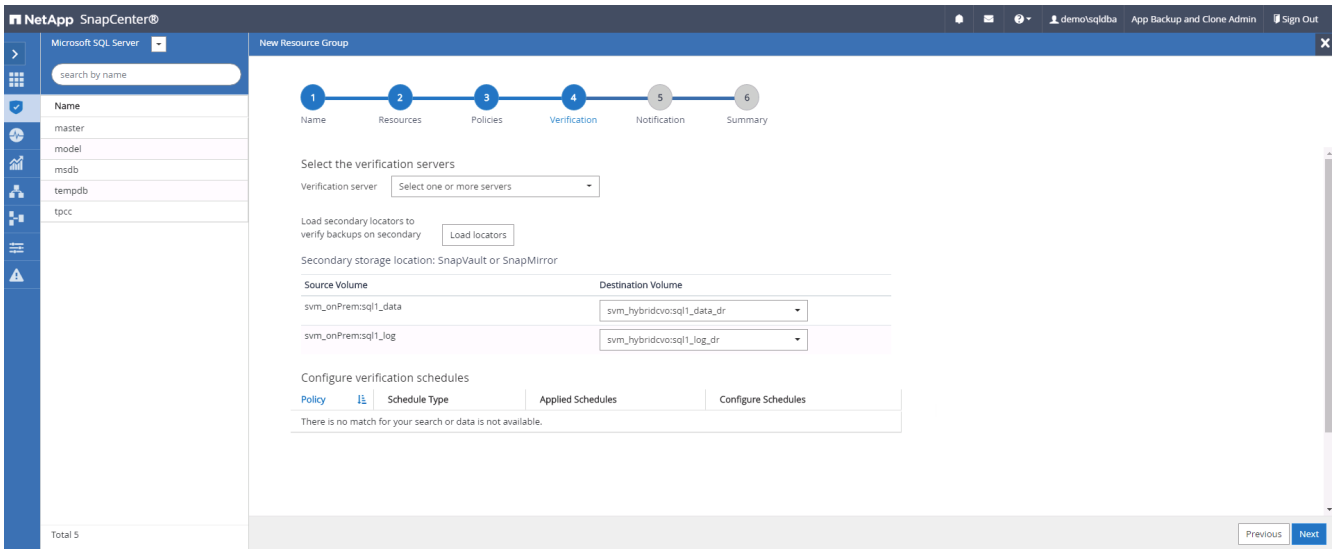
3. Sélectionnez une stratégie de sauvegarde SQL complète créée dans la section 7.



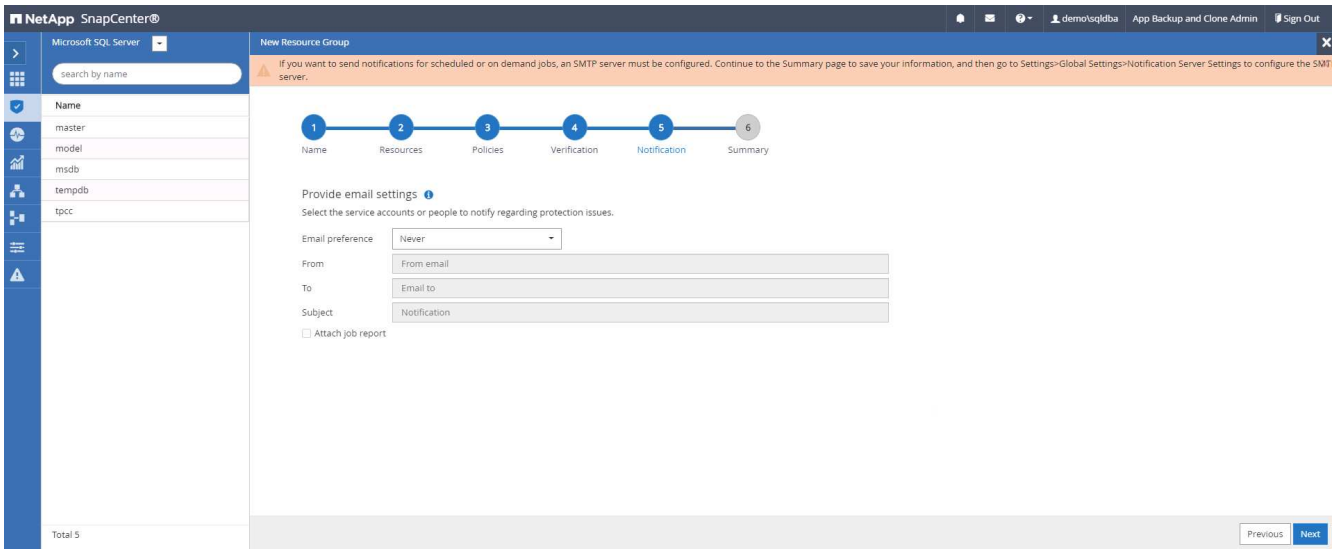
4. Ajoutez la durée exacte des sauvegardes ainsi que la fréquence.



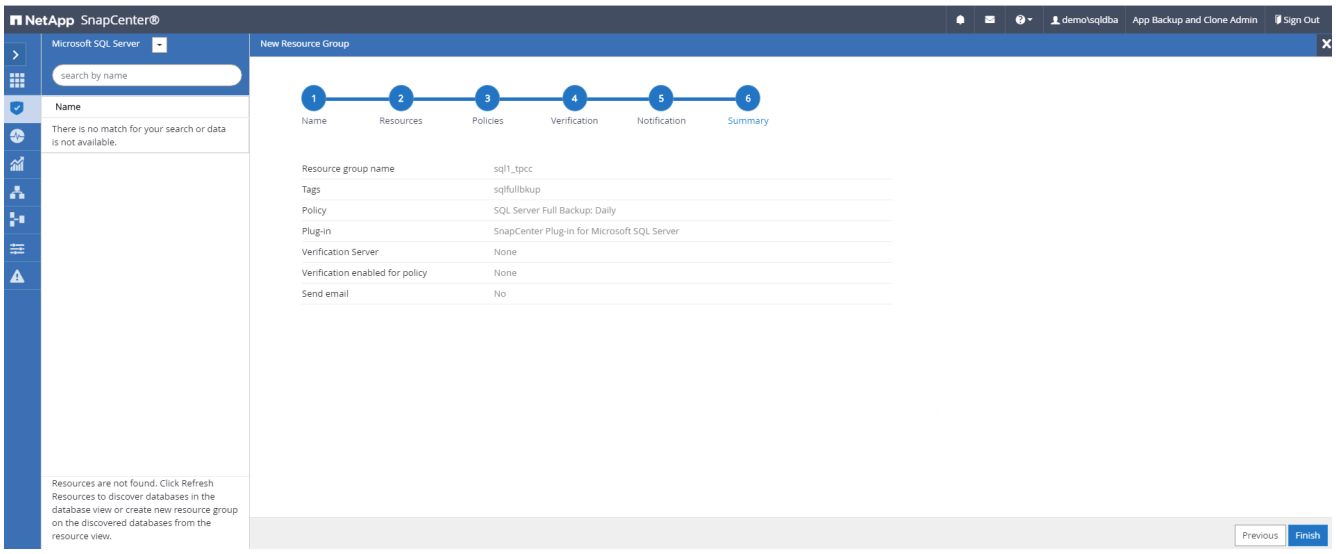
5. Choisissez le serveur de vérification pour la sauvegarde sur secondaire si la vérification de sauvegarde doit être effectuée. Cliquez sur Charger le localisateur pour renseigner l'emplacement de stockage secondaire.



6. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.

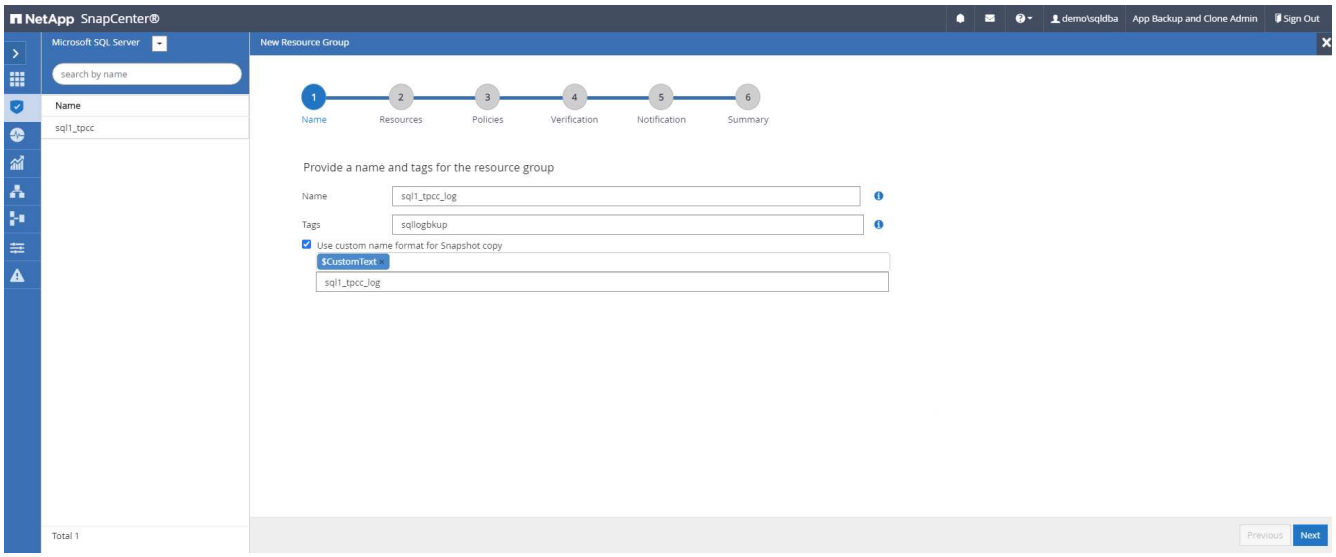


7. Récapitulatif.

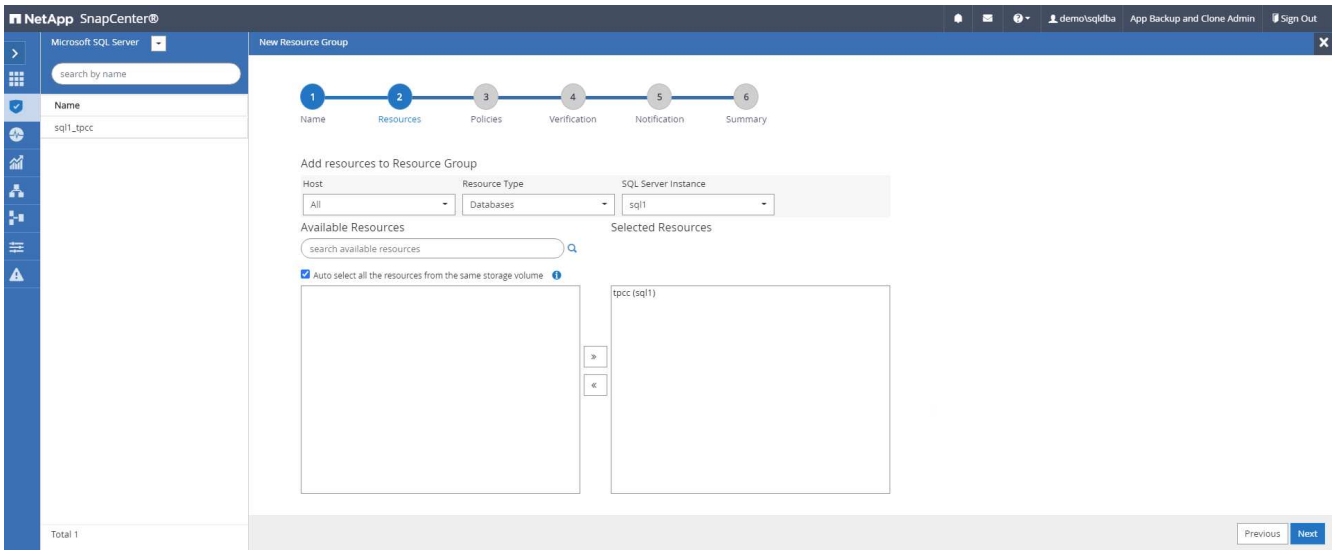


Créez un groupe de ressources pour la sauvegarde des journaux de SQL Server

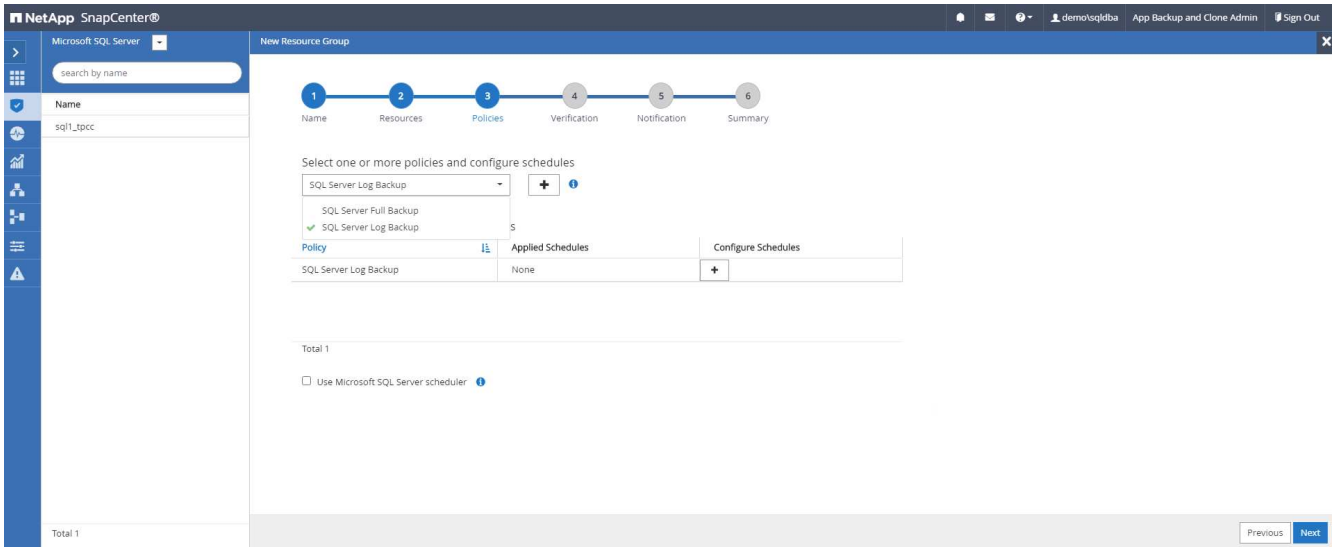
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez une base de données ou un groupe de ressources pour lancer le flux de travail de création de groupe de ressources. Indiquez le nom et les balises du groupe de ressources. Vous pouvez définir un format d'attribution de nom à la copie Snapshot.



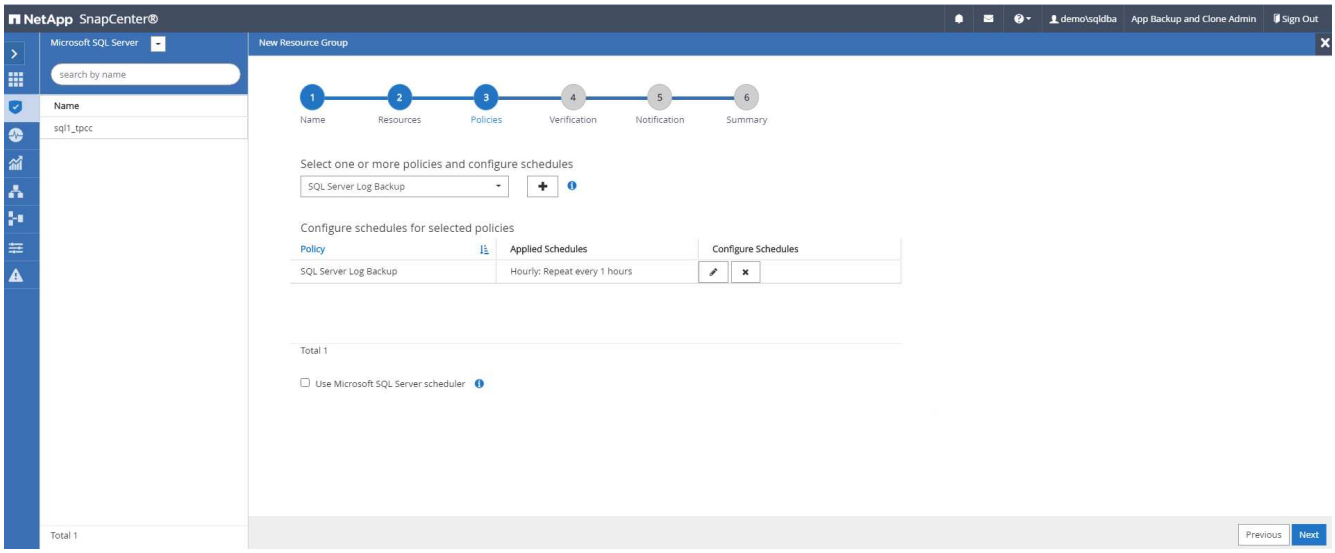
2. Sélectionnez les ressources de base de données à sauvegarder.



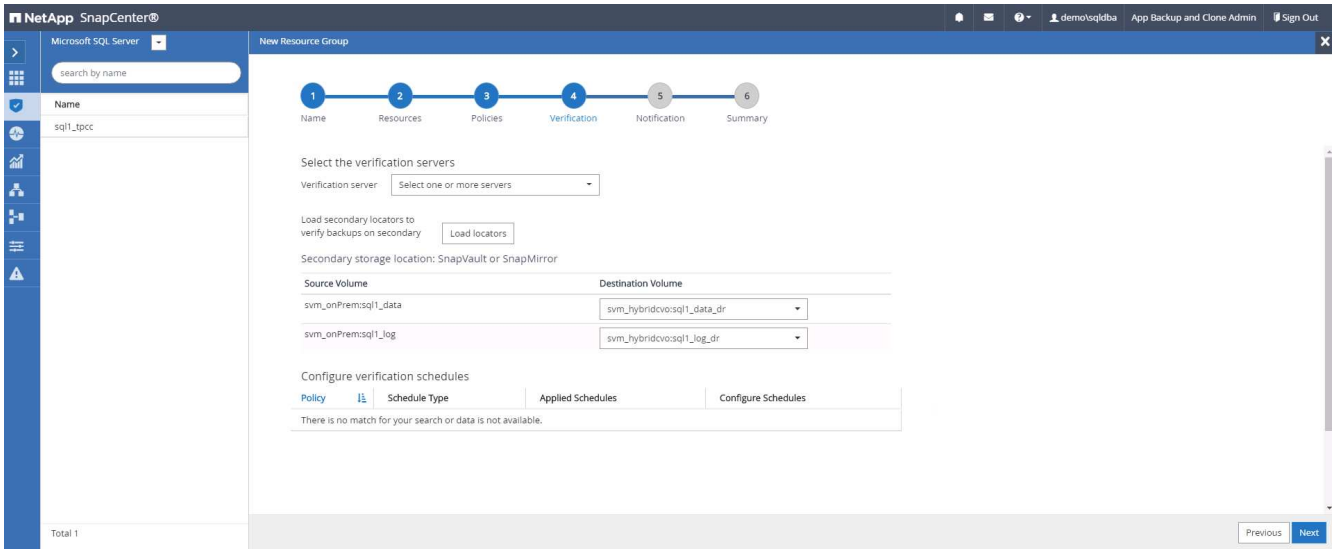
3. Sélectionnez une stratégie de sauvegarde du journal SQL créée à la section 7.



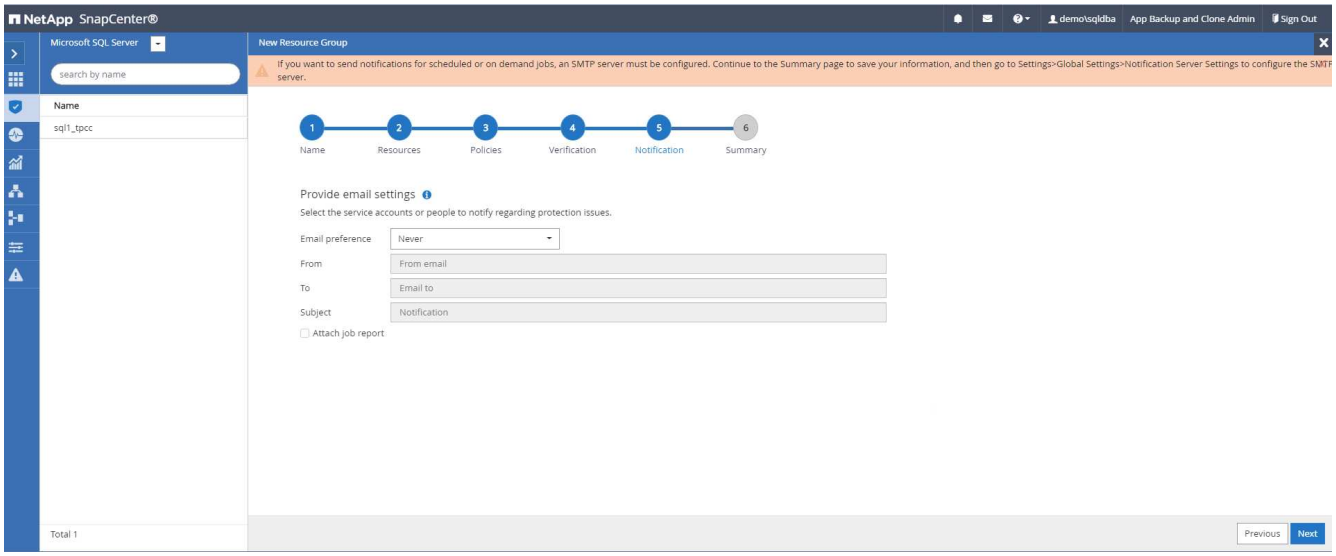
4. Ajoutez la synchronisation exacte pour la sauvegarde ainsi que la fréquence.



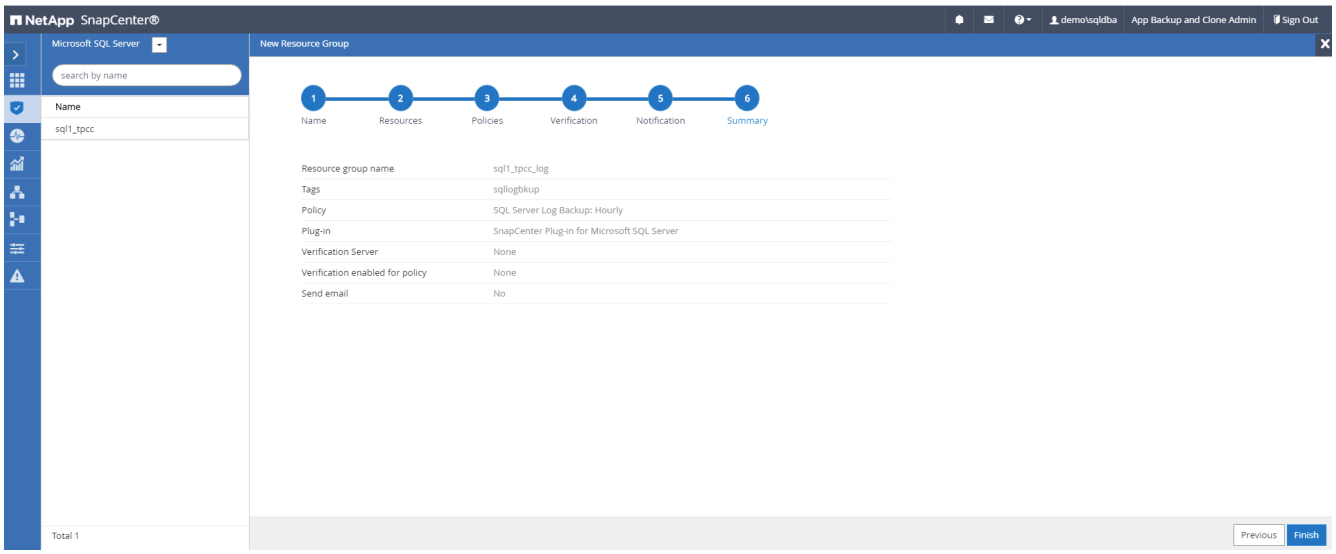
5. Choisissez le serveur de vérification pour la sauvegarde sur secondaire si la vérification de sauvegarde doit être effectuée. Cliquez sur le localisateur de charge pour renseigner l'emplacement de stockage secondaire.



6. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.

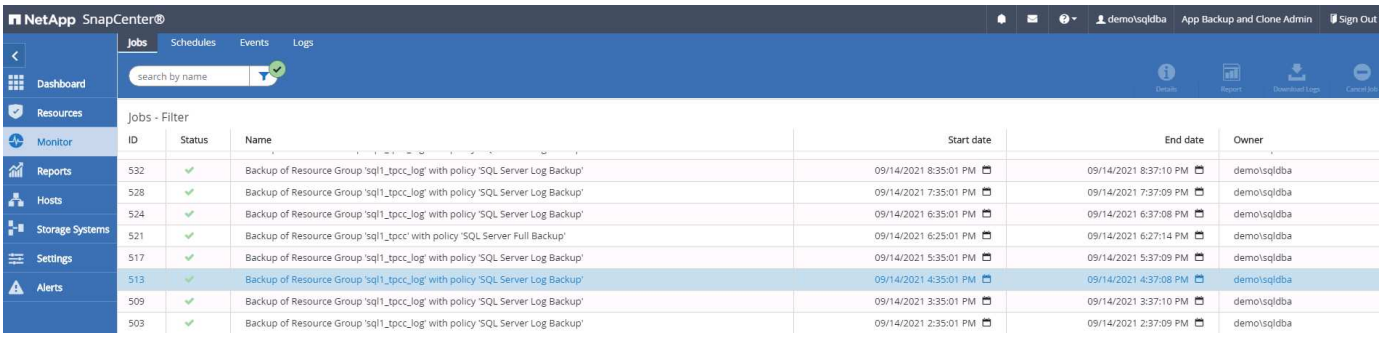


7. Récapitulatif.



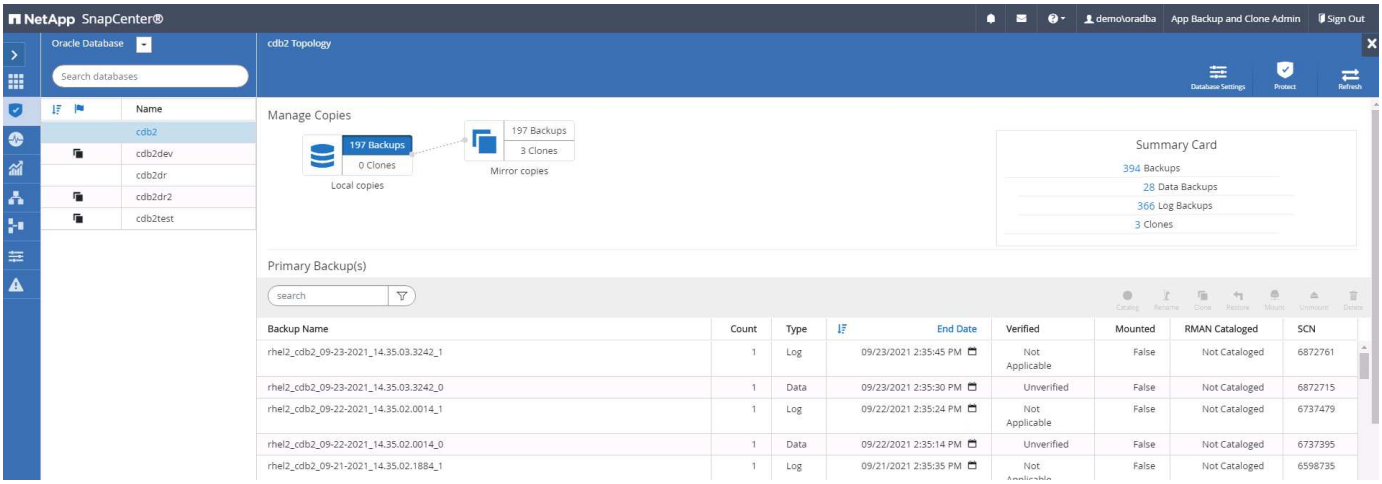
9. Valider la sauvegarde

Une fois que des groupes de ressources de sauvegarde de base de données sont créés pour protéger les ressources de base de données, les tâches de sauvegarde s'exécutent en fonction du planning prédéfini. Vérifiez l'état d'exécution du travail sous l'onglet moniteur.



Accédez à l'onglet Ressources, cliquez sur le nom de la base de données pour afficher les détails de la

sauvegarde de la base de données, et basculez entre les copies locales et les copies miroir pour vérifier que les sauvegardes Snapshot sont répliquées dans un emplacement secondaire du cloud public.



À ce stade, les copies de sauvegarde de base de données dans le cloud sont prêtes à cloner pour exécuter des processus de développement/test ou pour la reprise après incident en cas de panne principale.

Mise en route du cloud public AWS

Cette section décrit le processus de déploiement de Cloud Manager et de Cloud Volumes ONTAP dans AWS.

Cloud public AWS

> Pour simplifier l'suivi, nous avons créé ce document en nous basant sur le déploiement dans AWS. Cependant, ce processus est très similaire pour Azure et GCP.

1. Contrôle avant vol

Avant le déploiement, s'assurer que l'infrastructure permet le déploiement à l'étape suivante. Ceci inclut les éléments suivants :

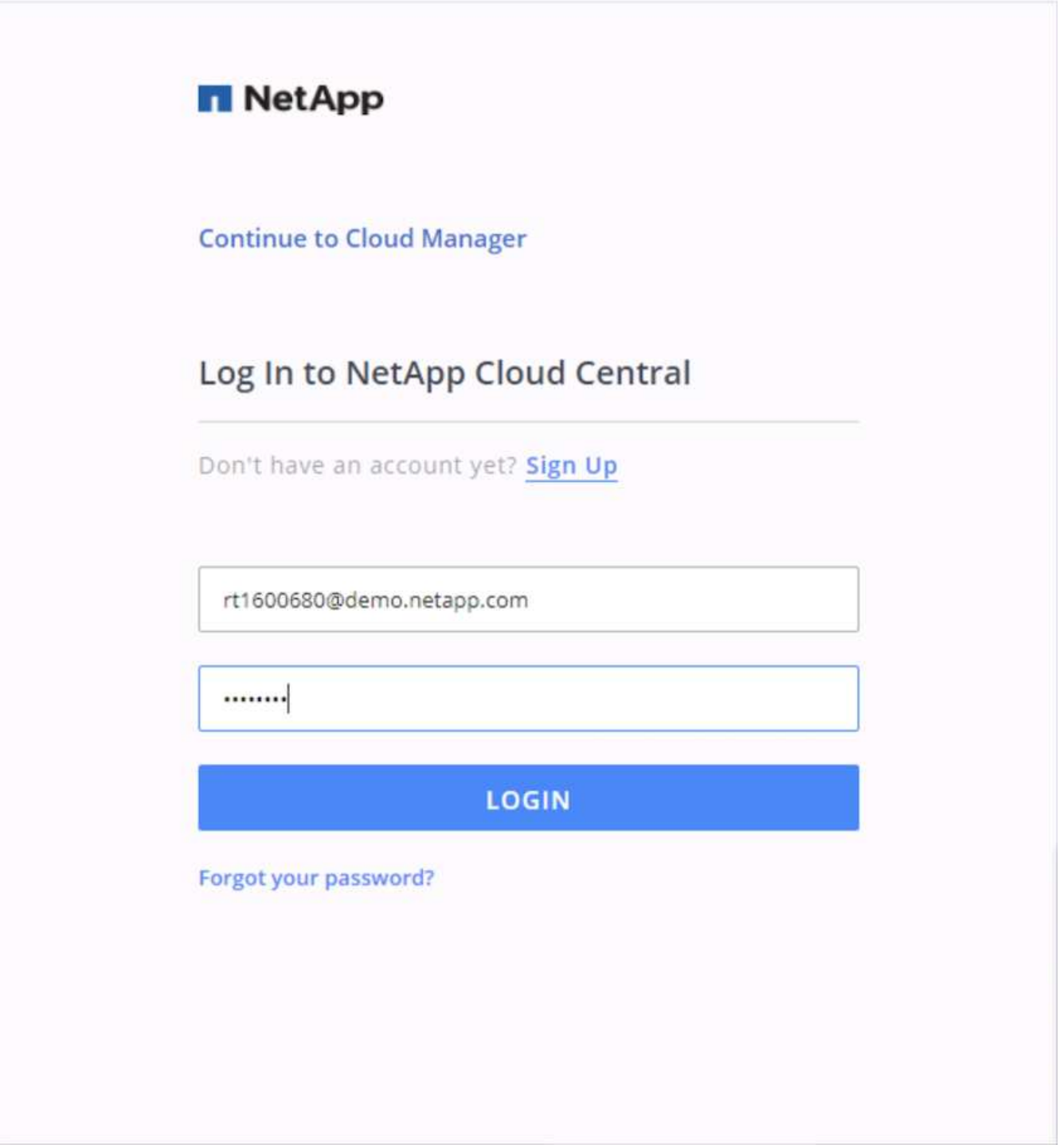
- Compte AWS
- VPC dans votre région
- Sous-réseau avec accès à l'Internet public
- Autorisations permettant d'ajouter des rôles IAM à votre compte AWS
- Une clé secrète et une clé d'accès pour votre utilisateur AWS

2. Étapes de déploiement de Cloud Manager et de Cloud Volumes ONTAP dans AWS

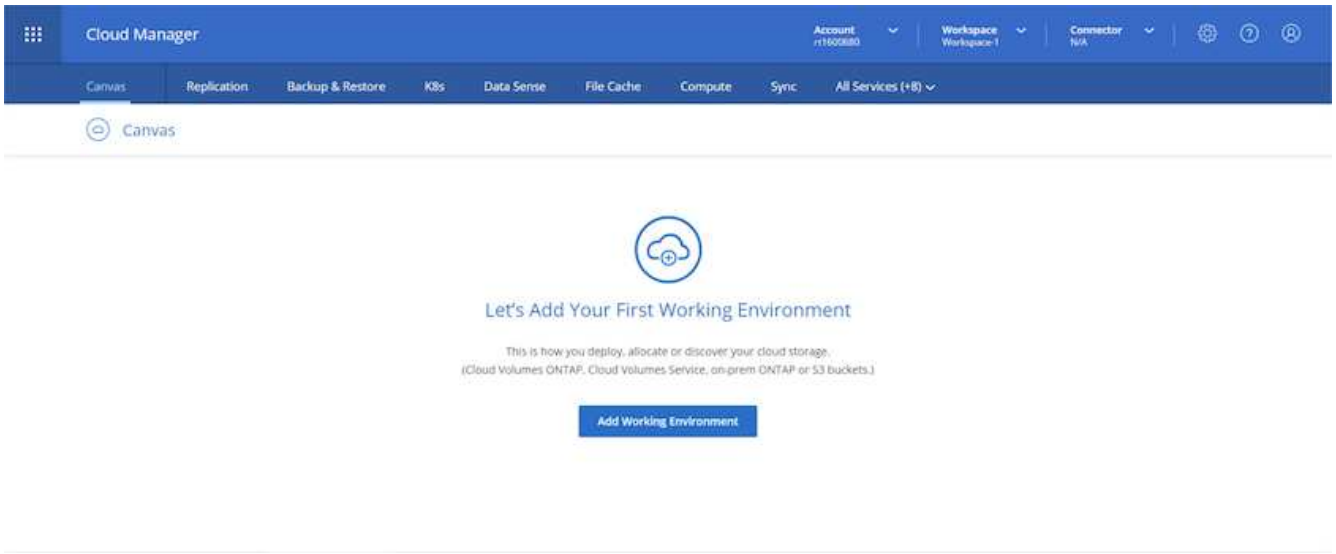
> De nombreuses méthodes de déploiement de Cloud Manager et de Cloud Volumes ONTAP sont disponibles. Cette méthode est la plus simple, mais requiert la plupart des autorisations. Si cette méthode n'est pas adaptée à votre environnement AWS, consultez le "Documentation cloud NetApp".

Déployez Cloud Manager Connector

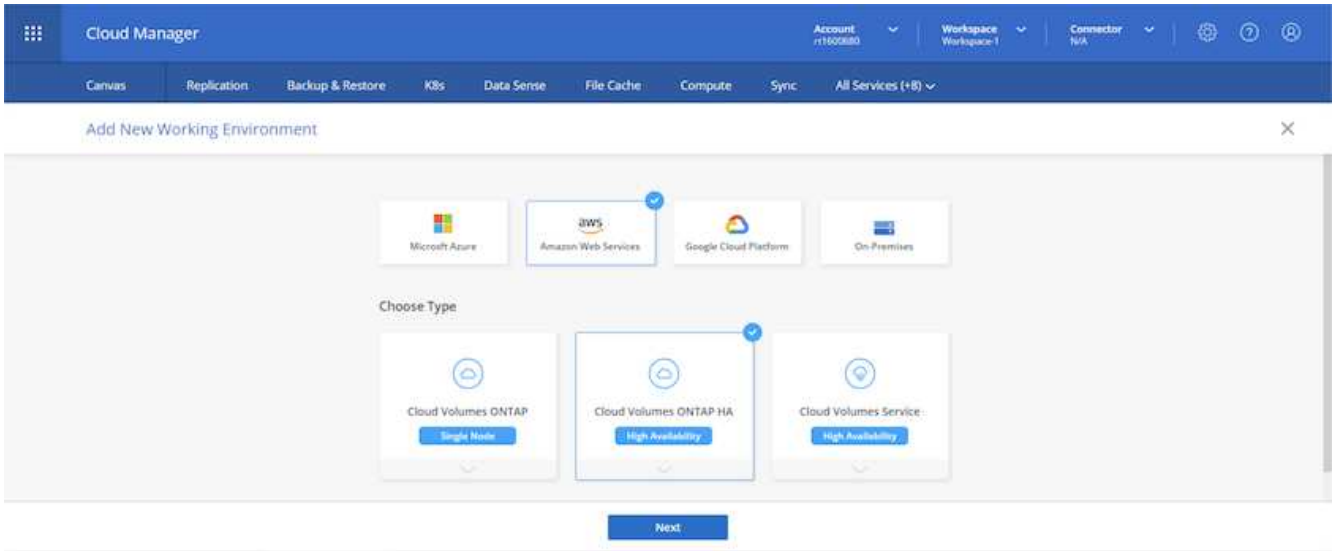
1. Accédez à "NetApp Cloud Central" et connectez-vous ou inscrivez-vous.



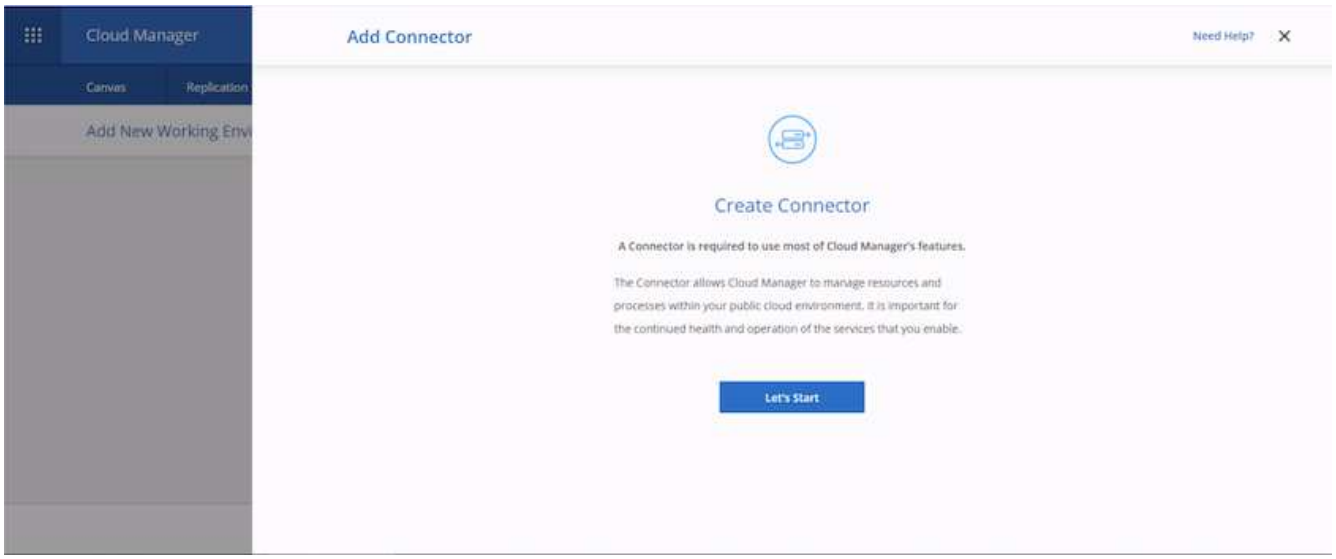
2. Une fois connecté, vous devez être redirigé vers la toile.



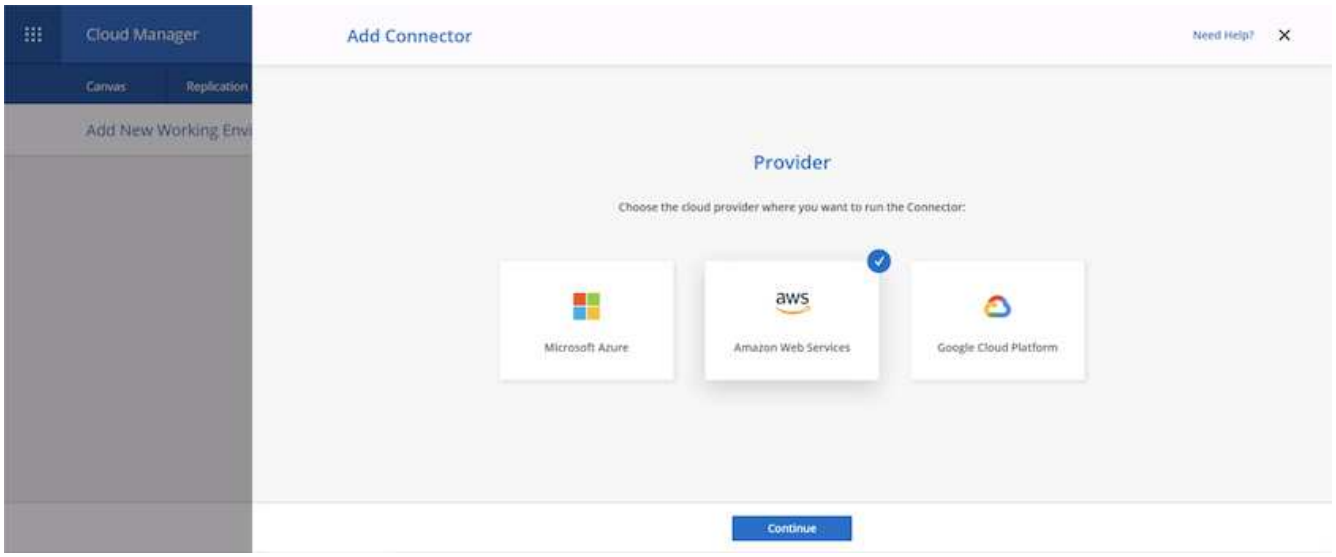
3. Cliquez sur Add Working Environment (Ajouter un environnement de travail) et choisissez Cloud Volumes ONTAP in AWS. Vous pouvez également choisir de déployer un système à un seul nœud ou une paire haute disponibilité. J'ai choisi de déployer une paire haute disponibilité.



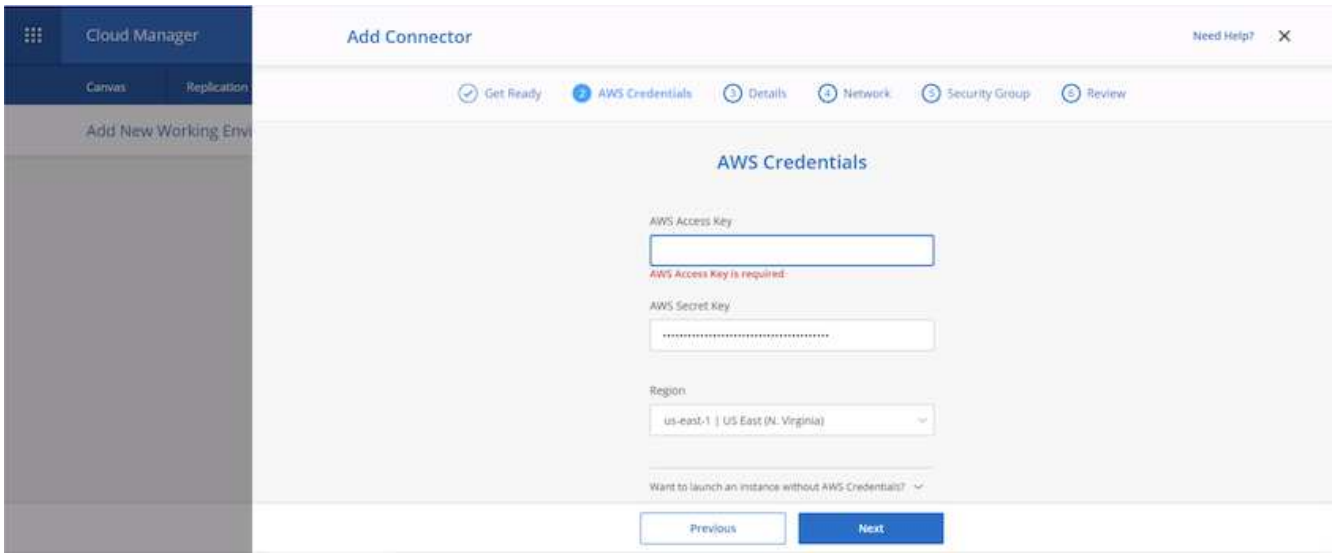
4. Si aucun connecteur n'a été créé, une fenêtre contextuelle s'affiche vous demandant de créer un connecteur.



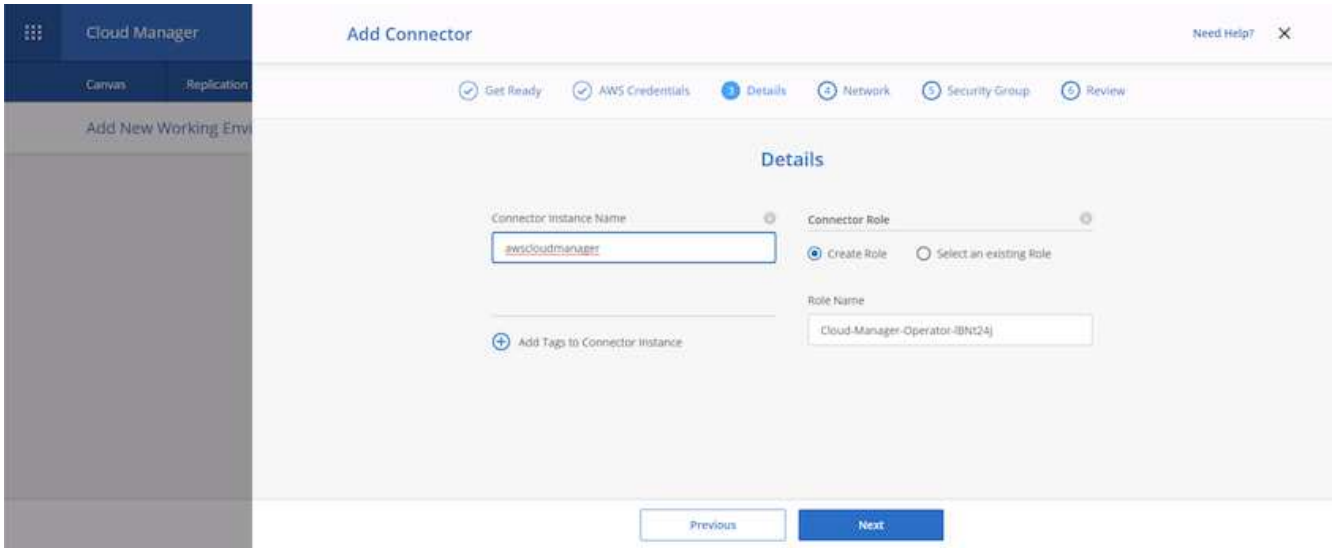
5. Cliquez sur Oui, puis choisissez AWS.



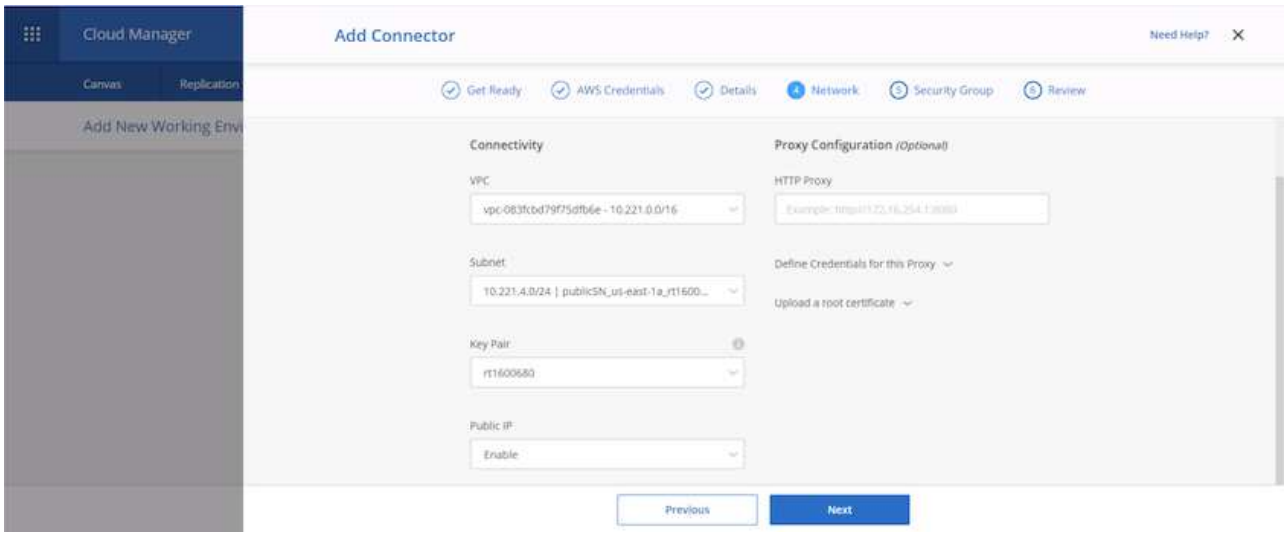
6. Saisissez votre clé secrète et votre clé d'accès. Assurez-vous que votre utilisateur dispose des autorisations appropriées indiquées sur le "Page règles NetApp".



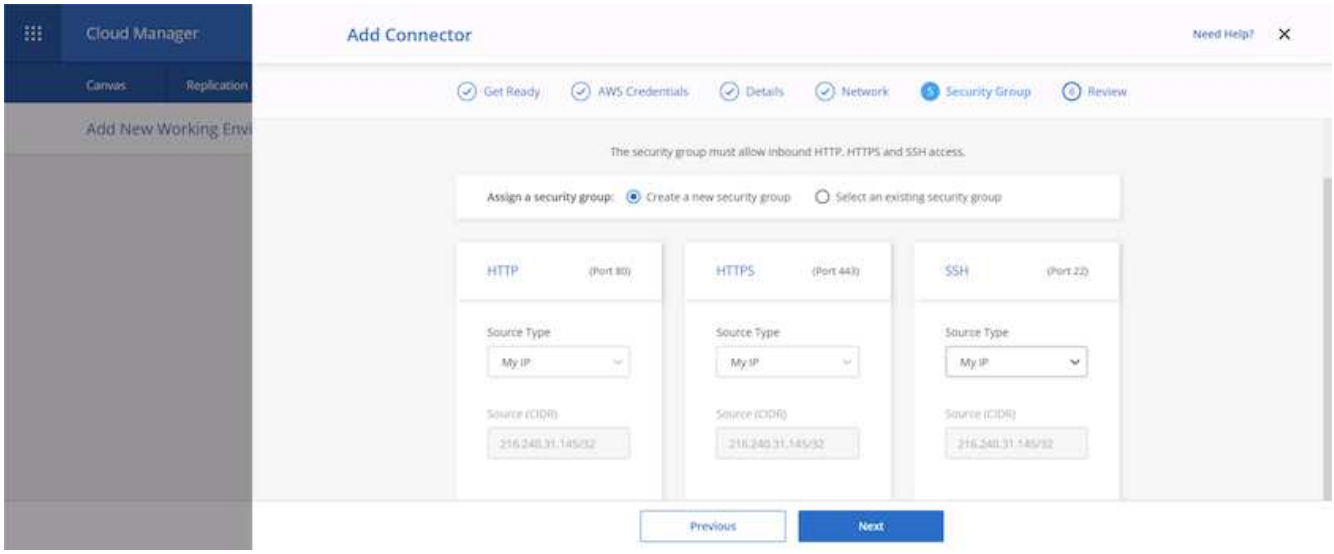
7. Attribuez un nom au connecteur et utilisez un rôle prédéfini comme décrit sur le "Page règles NetApp" Vous pouvez également demander à Cloud Manager de créer le rôle dont vous avez besoin.



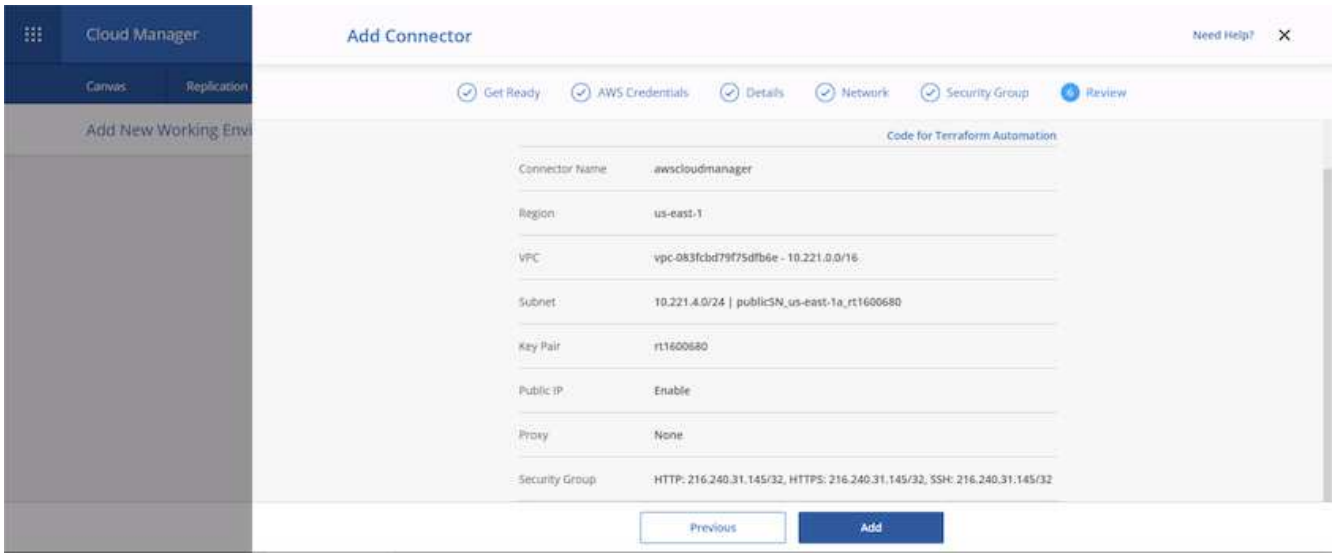
8. Fournissez les informations de mise en réseau nécessaires au déploiement du connecteur. Vérifiez que l'accès Internet sortant est activé par :
   a. En donnant au connecteur une adresse IP publique
   b. Donner au connecteur un proxy pour fonctionner
   c. Donner au connecteur une route vers l'Internet public par le biais d'une passerelle Internet



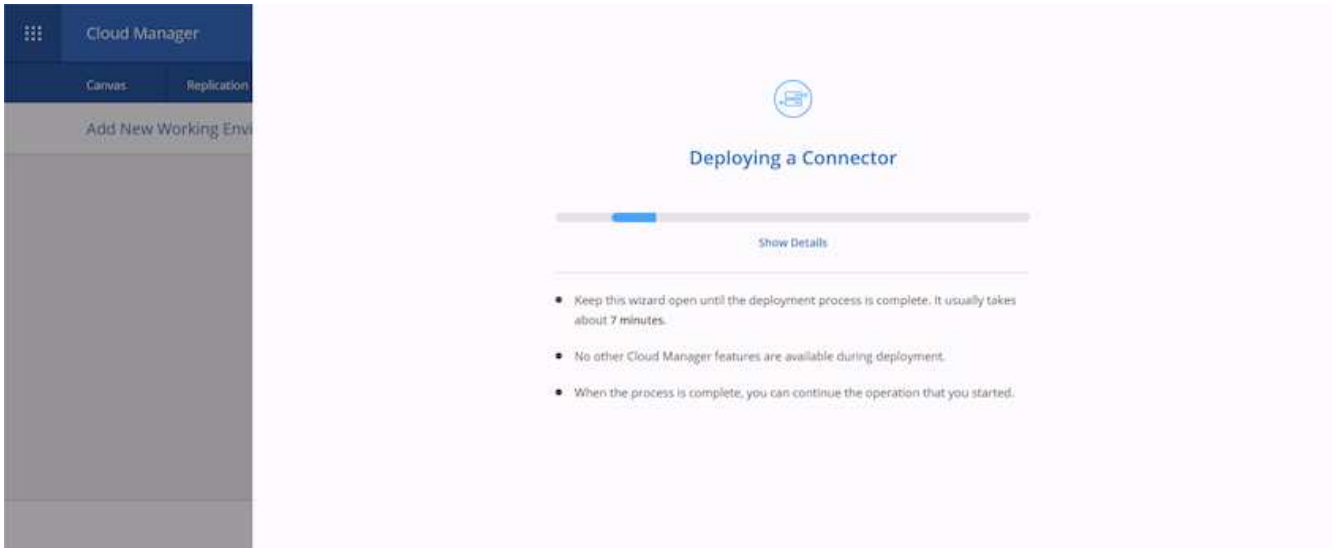
9. Établir une communication avec le connecteur via SSH, HTTP et HTTPS en fournissant un groupe de sécurité ou en créant un nouveau groupe de sécurité. J'ai activé l'accès au connecteur à partir de mon adresse IP uniquement.



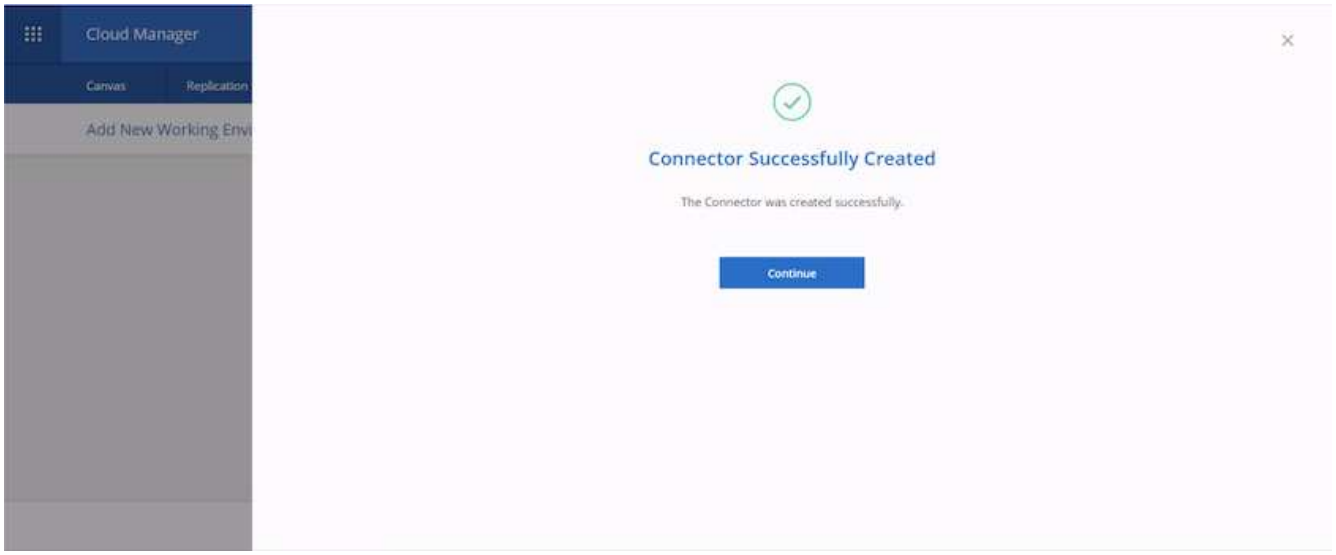
10. Vérifiez les informations de la page de résumé et cliquez sur Ajouter pour déployer le connecteur.



11. Le connecteur se déploie à présent à l'aide d'une pile de formation de nuages. Vous pouvez contrôler sa progression depuis Cloud Manager ou via AWS.

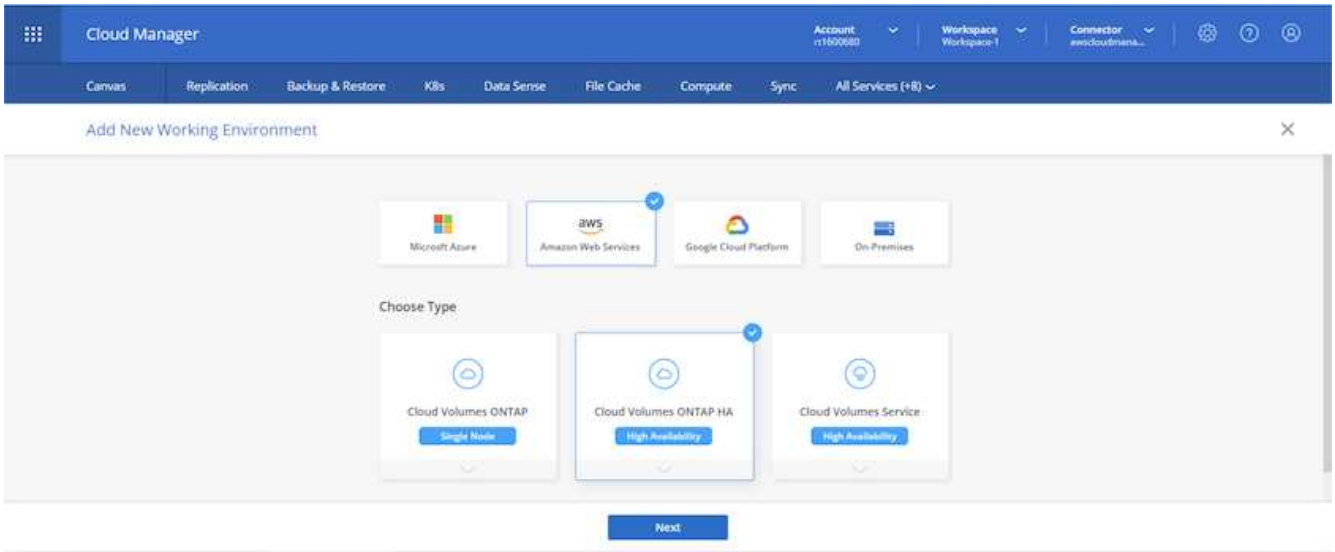


12. Une fois le déploiement terminé, une page de réussite s'affiche.

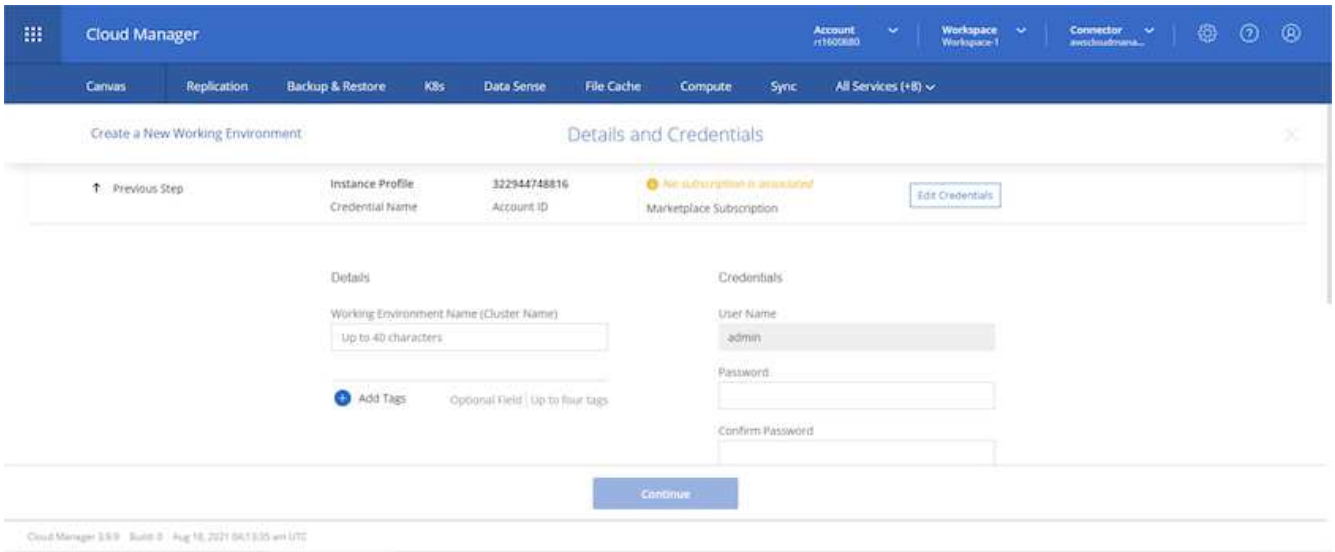


Déployez Cloud Volumes ONTAP

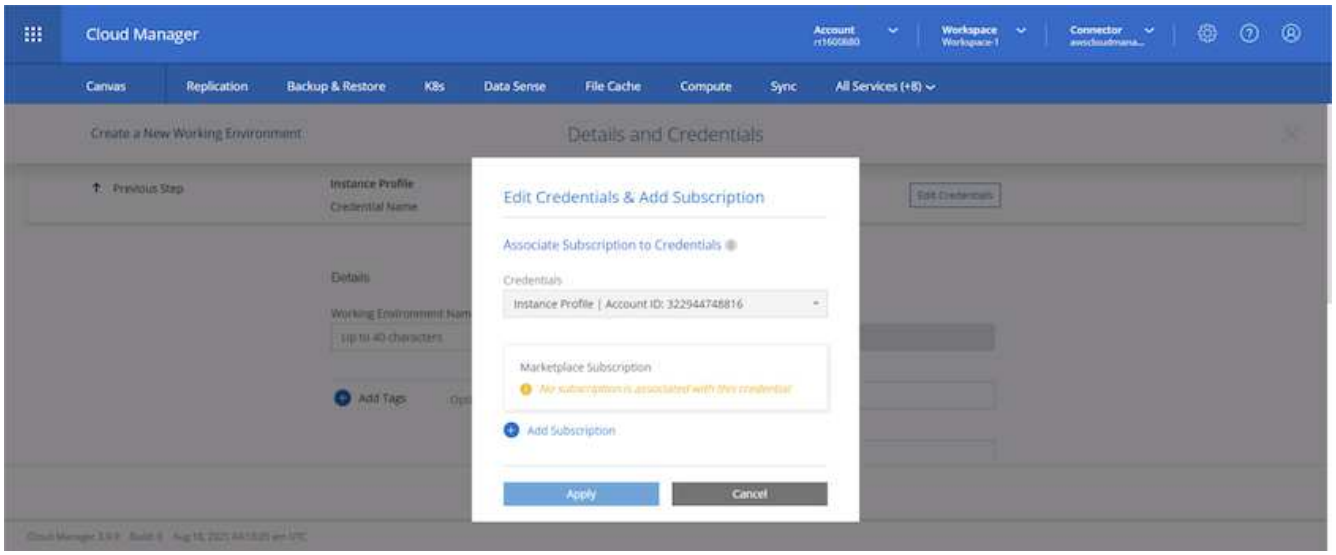
1. Sélectionnez AWS et le type de déploiement selon vos besoins.



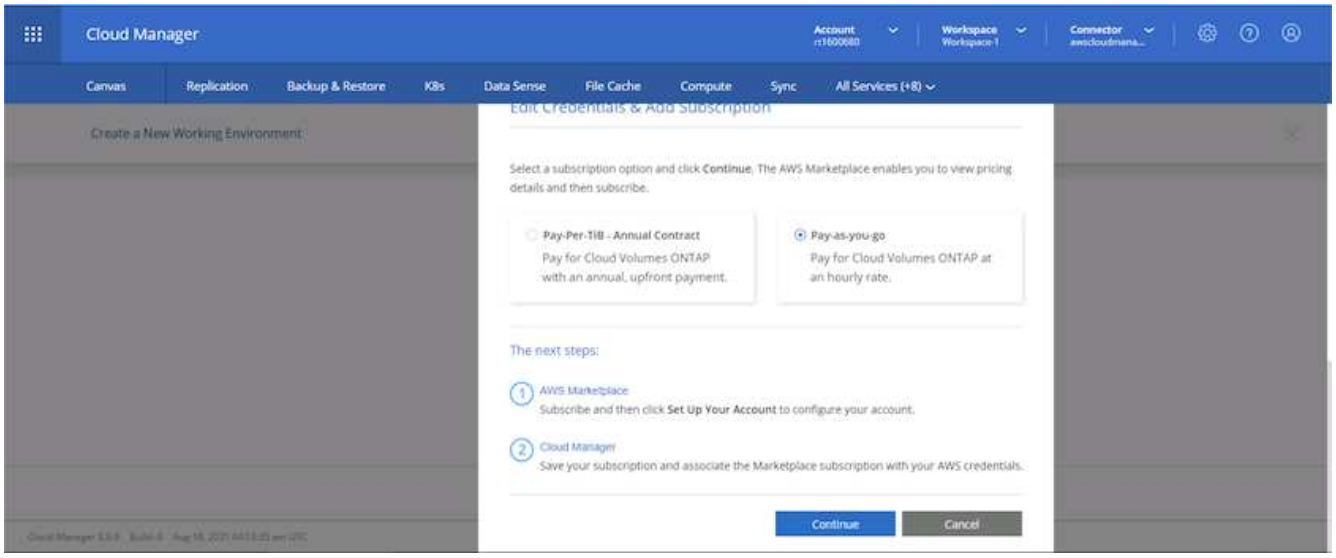
2. Si aucun abonnement n’a été attribué et que vous souhaitez acheter avec PAYGO, choisissez Modifier les informations d’identification.



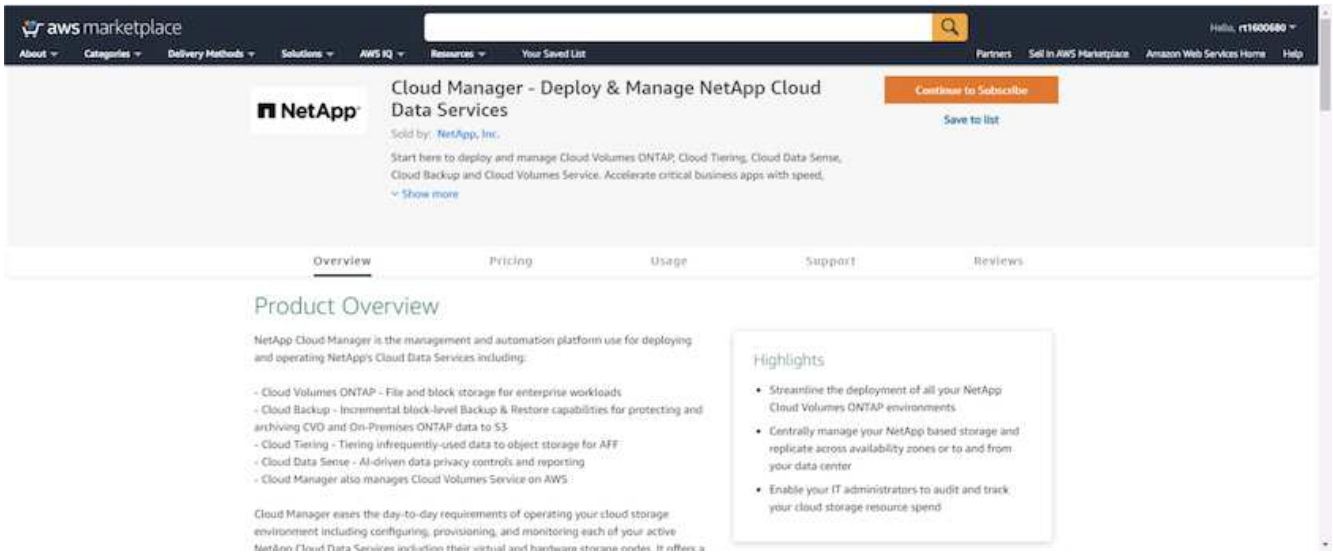
3. Choisissez Ajouter un abonnement.



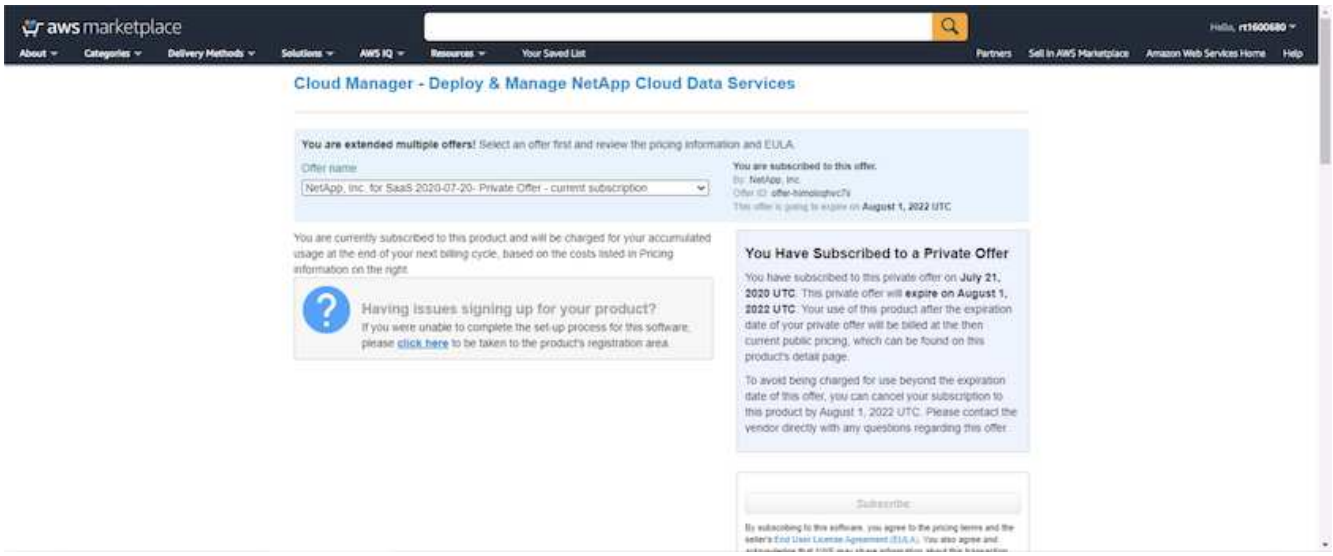
4. Choisissez le type de contrat auquel vous souhaitez vous abonner. J'ai choisi le paiement à l'utilisation.



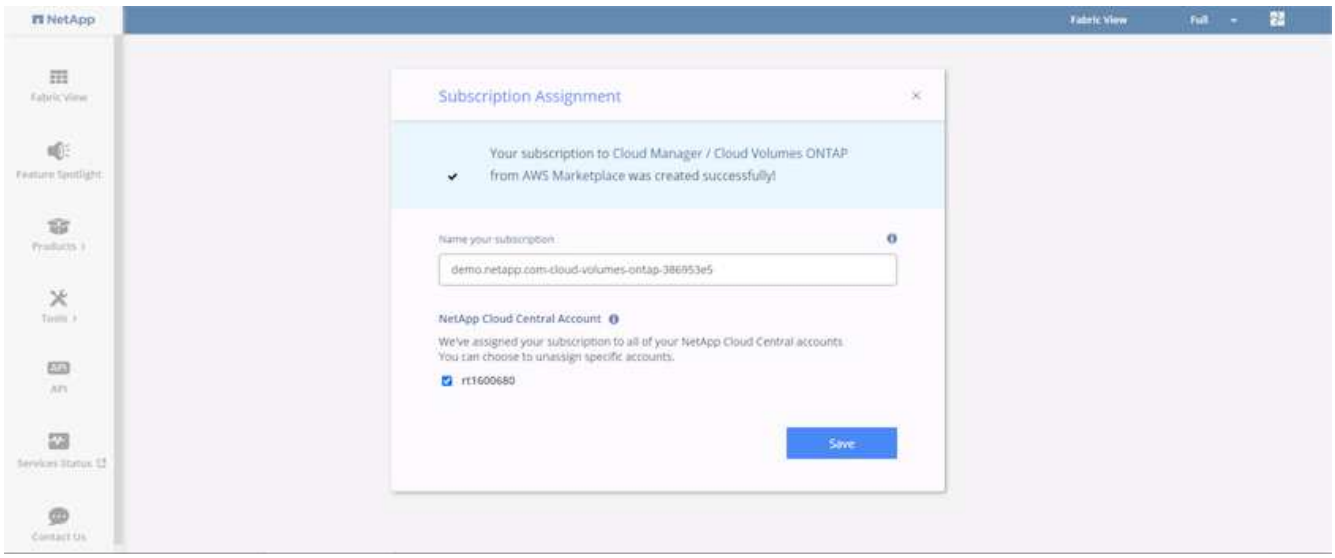
5. Vous êtes redirigé vers AWS ; sélectionnez Continuer pour vous inscrire.



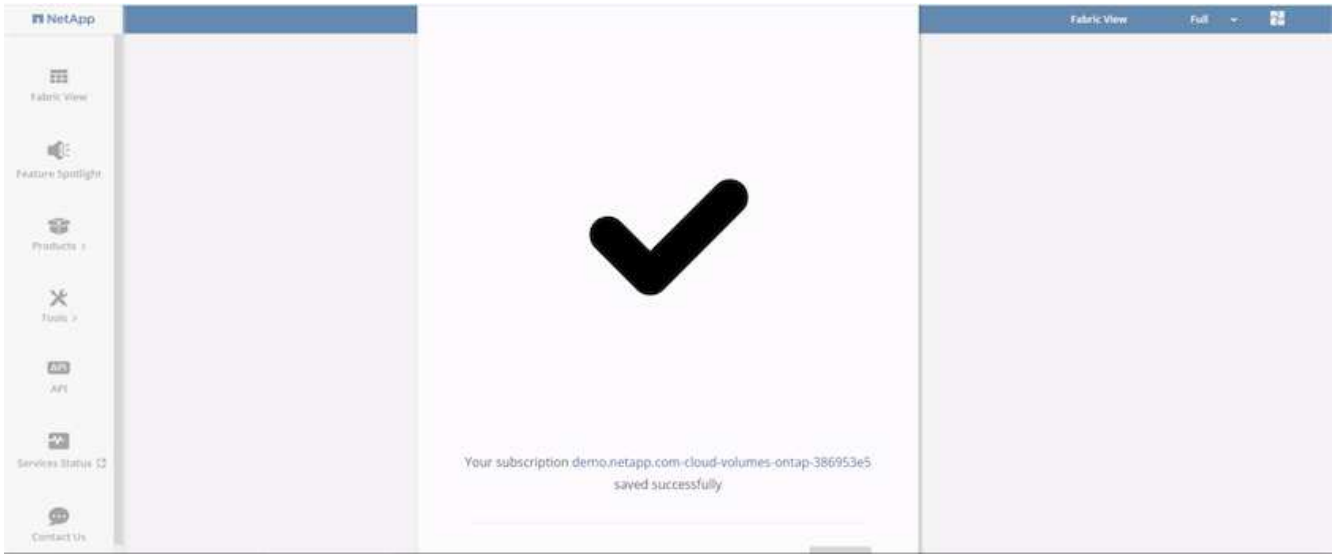
6. Vous allez être redirigé vers NetApp Cloud Central. Si vous êtes déjà abonné et que vous n'êtes pas redirigé, cliquez ici.



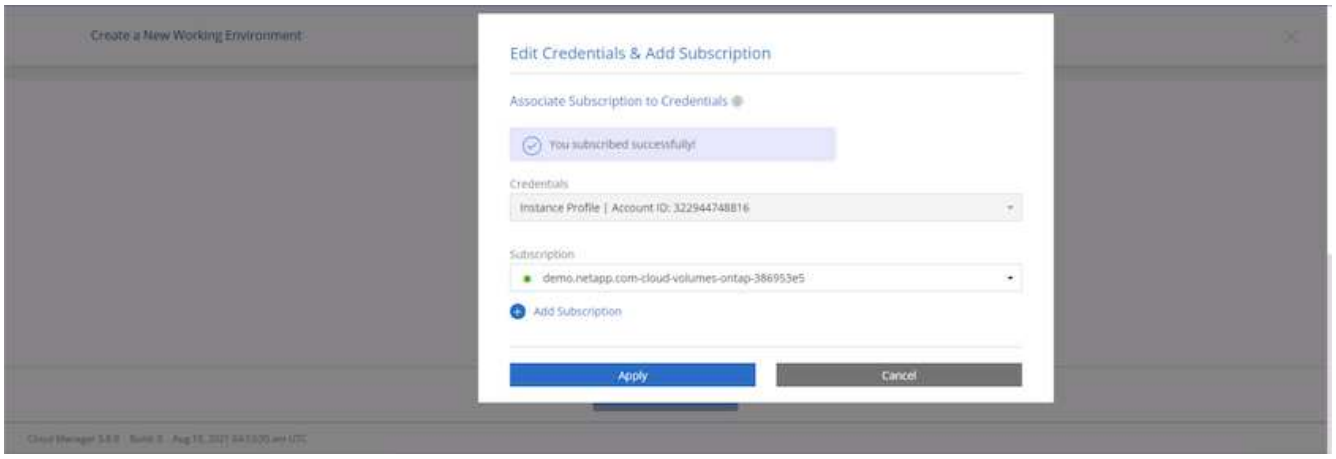
7. Vous êtes redirigé vers Cloud Central, où vous devez nommer votre abonnement et l'attribuer à votre compte Cloud Central.



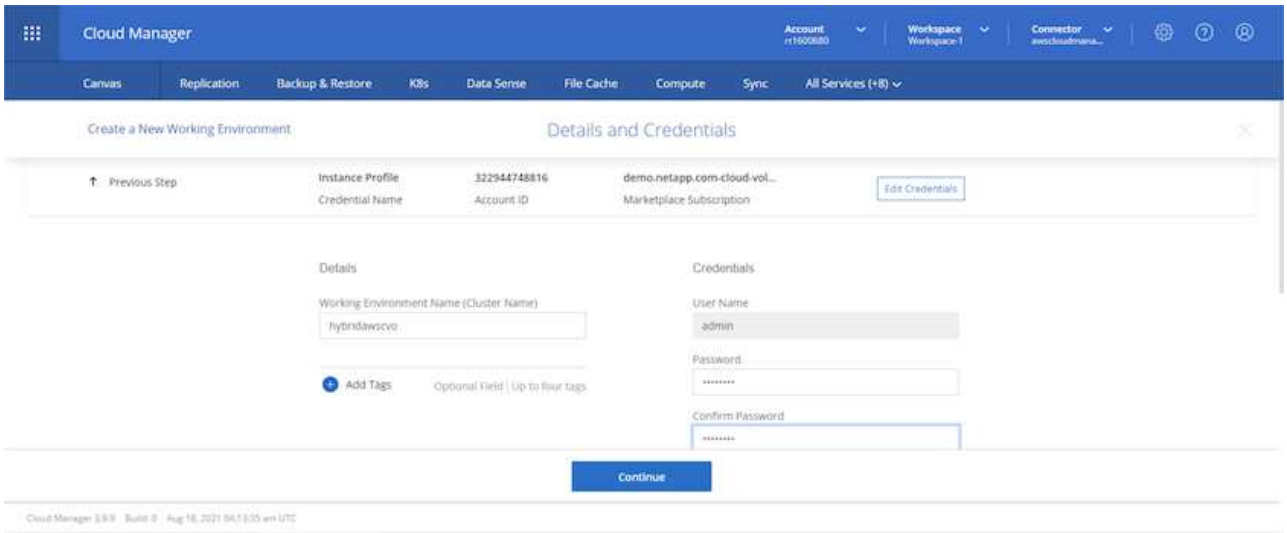
8. Une fois réussi, une page de coche s'affiche. Revenez à l'onglet Cloud Manager.



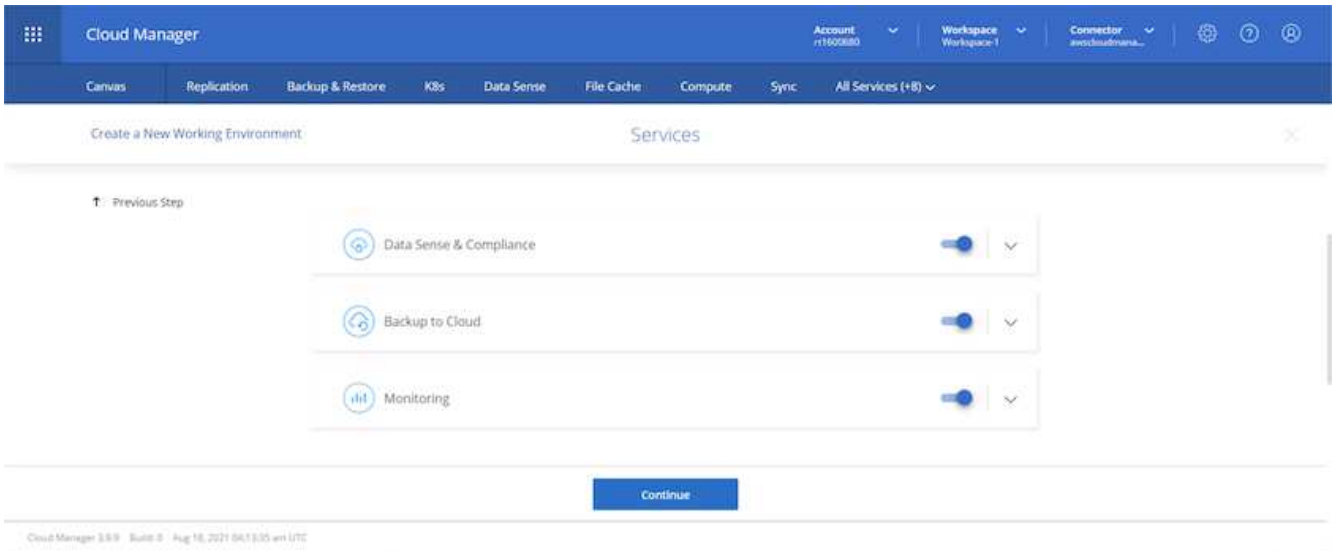
9. L’abonnement s’affiche désormais dans Cloud Central. Cliquez sur appliquer pour continuer.



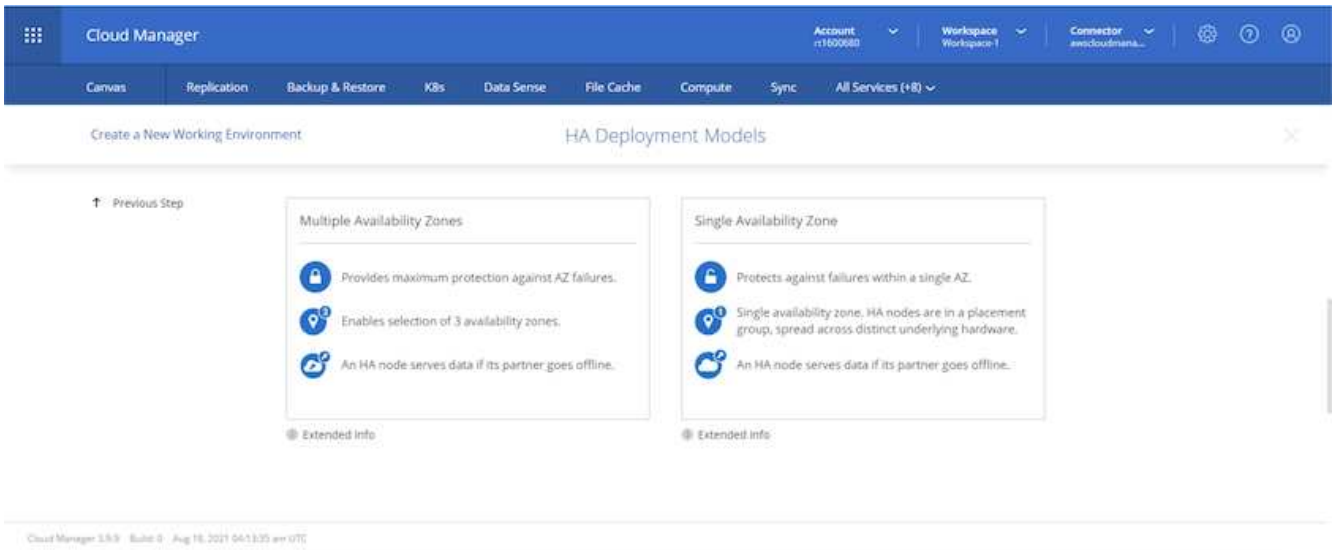
10. Saisissez les détails de l’environnement de travail, notamment :
    a. Nom du cluster
    b. Mot de passe du cluster
    c. Balises AWS (en option)



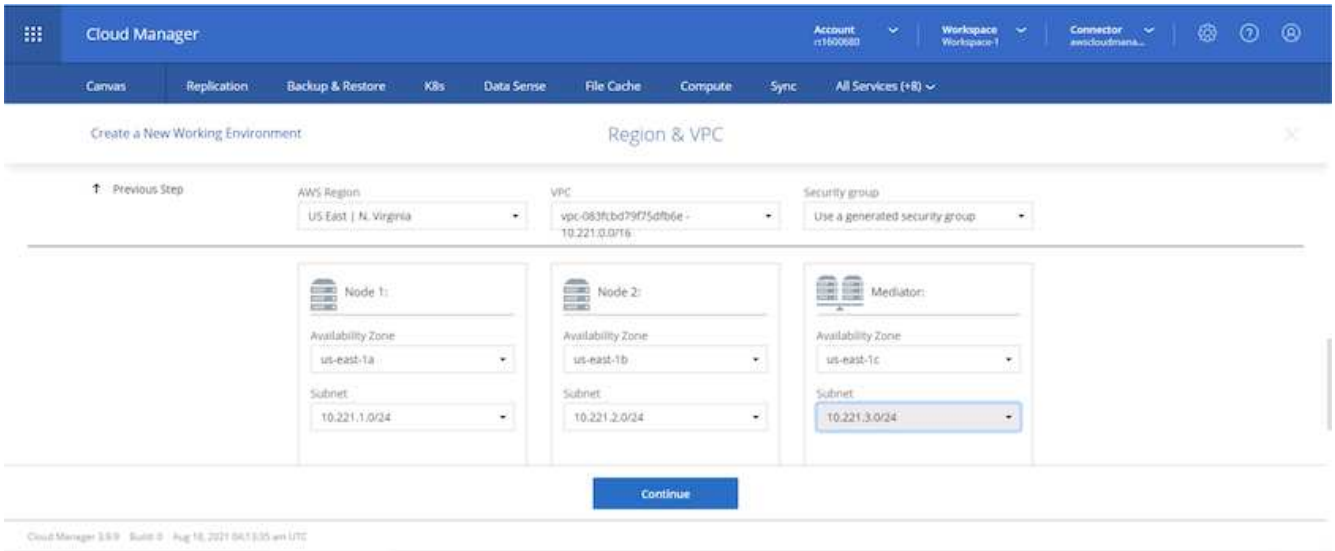
11. Choisissez les services supplémentaires que vous souhaitez déployer. Pour en savoir plus sur ces services, rendez-vous sur la "Page d'accueil de NetApp Cloud".



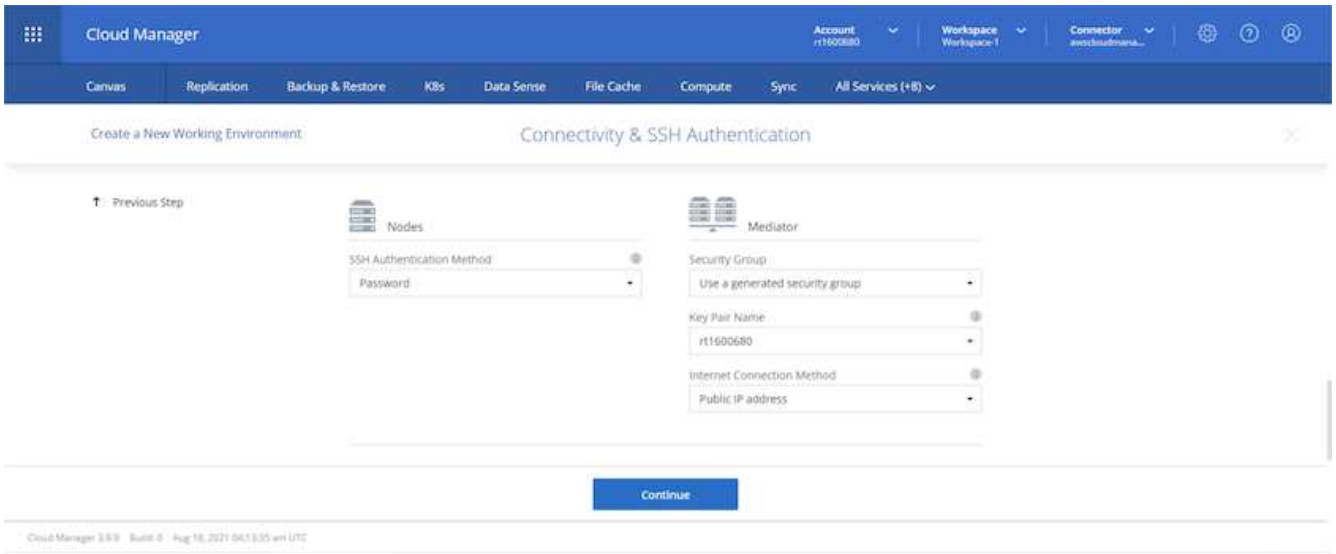
12. Choisissez si vous souhaitez le déployer dans plusieurs zones de disponibilité (trois sous-réseaux, chacun dans une zone AZ différente) ou dans une seule zone de disponibilité. J'ai choisi plusieurs AZS.



13. Choisissez la région, le VPC et le groupe de sécurité dans lequel le cluster doit être déployé. Dans cette section, vous affectez également les zones de disponibilité par nœud (et médiateur) ainsi que les sous-réseaux qu'ils occupent.

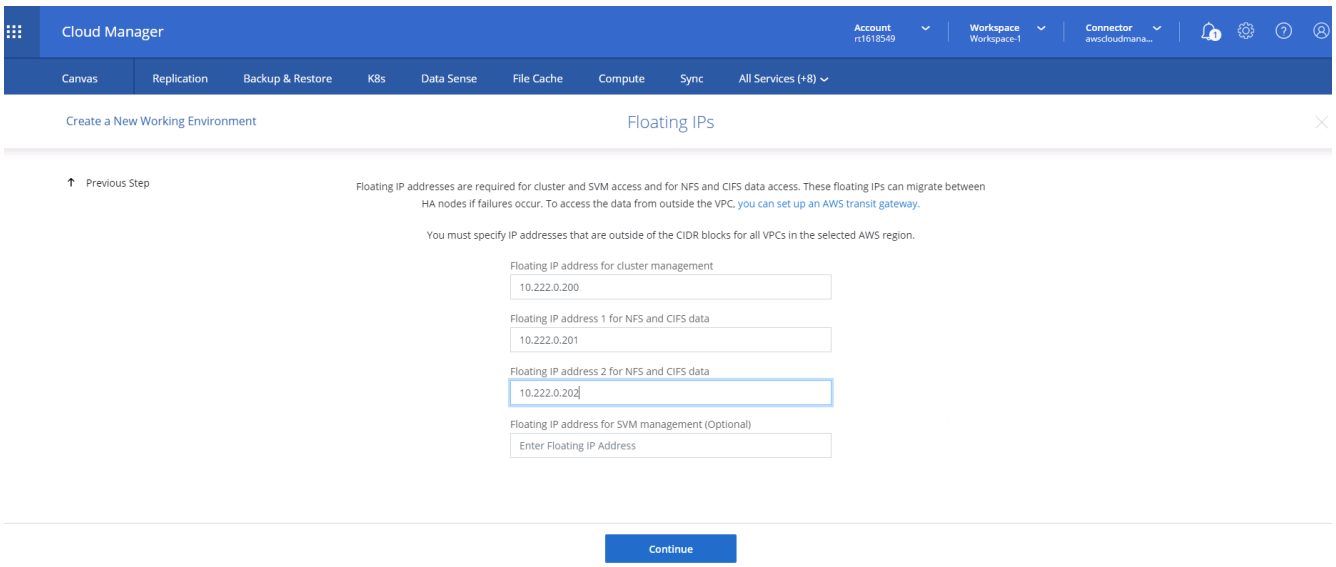


14. Choisissez les méthodes de connexion pour les nœuds et le médiateur.

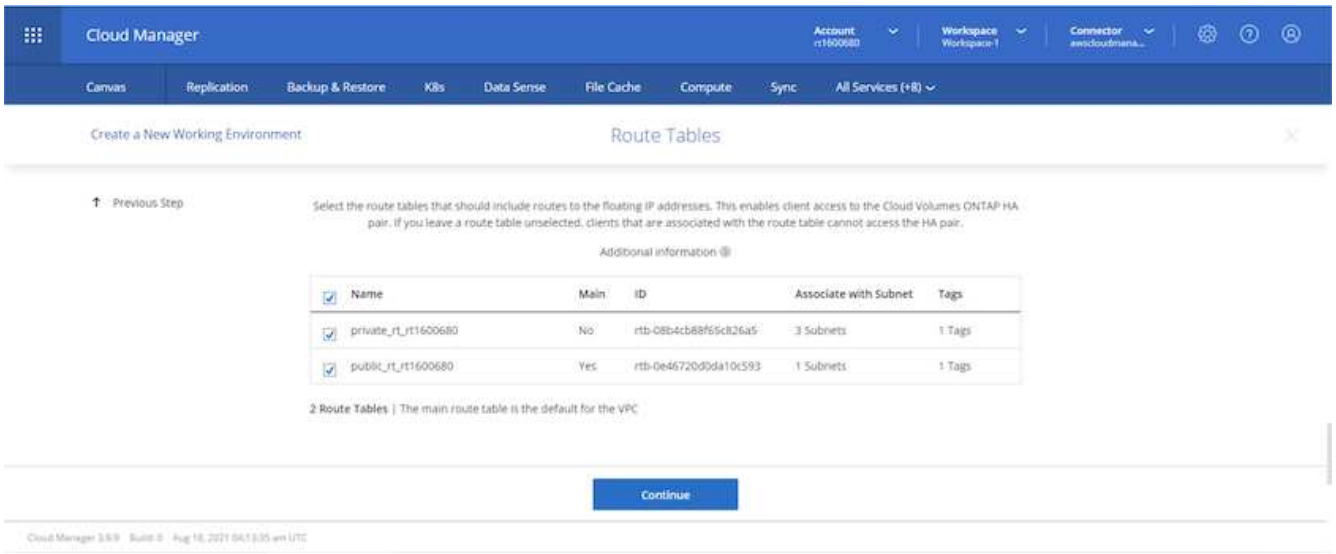


Le médiateur requiert la communication avec les API AWS. Une adresse IP publique n'est pas requise tant que les API sont accessibles après le déploiement de l'instance EC2 médiateur.

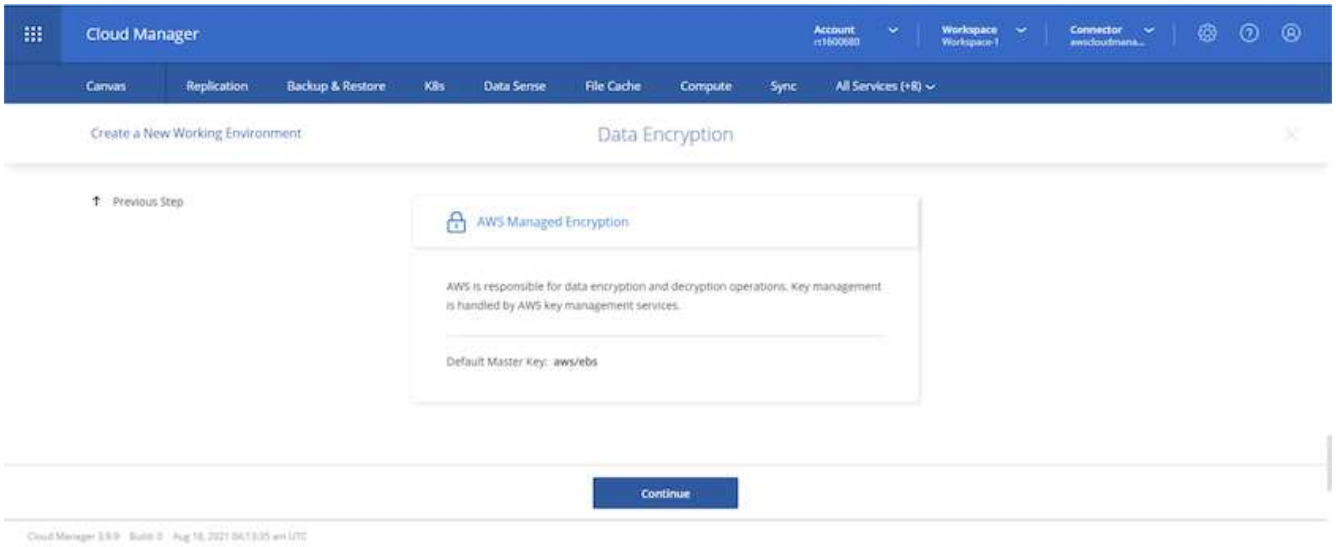
1. Les adresses IP flottantes sont utilisées pour permettre l'accès aux différentes adresses IP utilisées par Cloud Volumes ONTAP, y compris la gestion du cluster et le traitement des adresses IP. Ces adresses doivent être déjà routables sur votre réseau et ajoutées aux tables d'acheminement dans votre environnement AWS. Ils sont nécessaires pour activer des adresses IP cohérentes pour une paire haute disponibilité lors du basculement. Vous trouverez plus d'informations sur les adresses IP flottantes dans le "Documentation cloud NetApp".



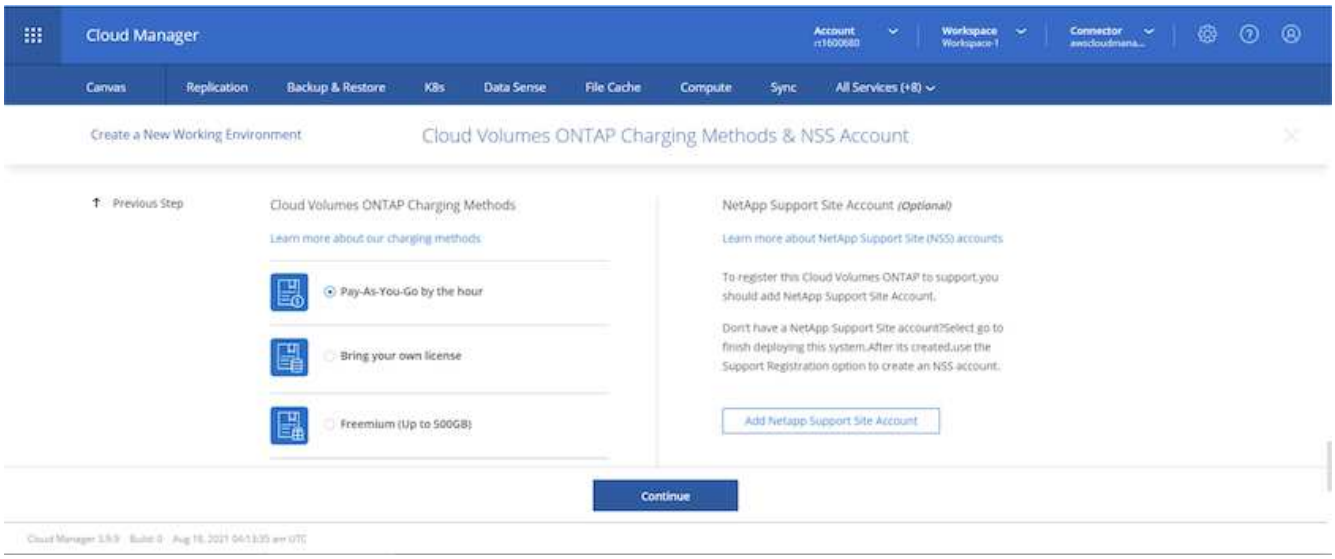
2. Sélectionnez les tables de routage auxquelles les adresses IP flottantes sont ajoutées. Ces tables de routage sont utilisées par les clients pour communiquer avec Cloud Volumes ONTAP.



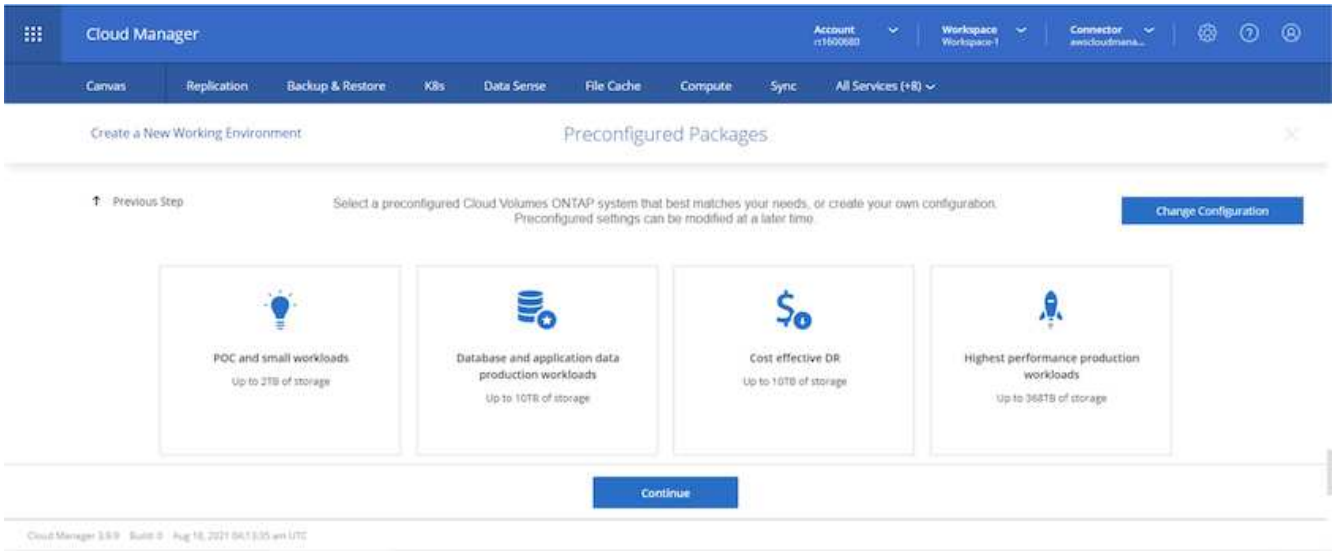
3. Elles peuvent choisir d'activer le chiffrement géré par AWS ou le KMS AWS pour chiffrer la racine ONTAP, le démarrage et les disques de données.



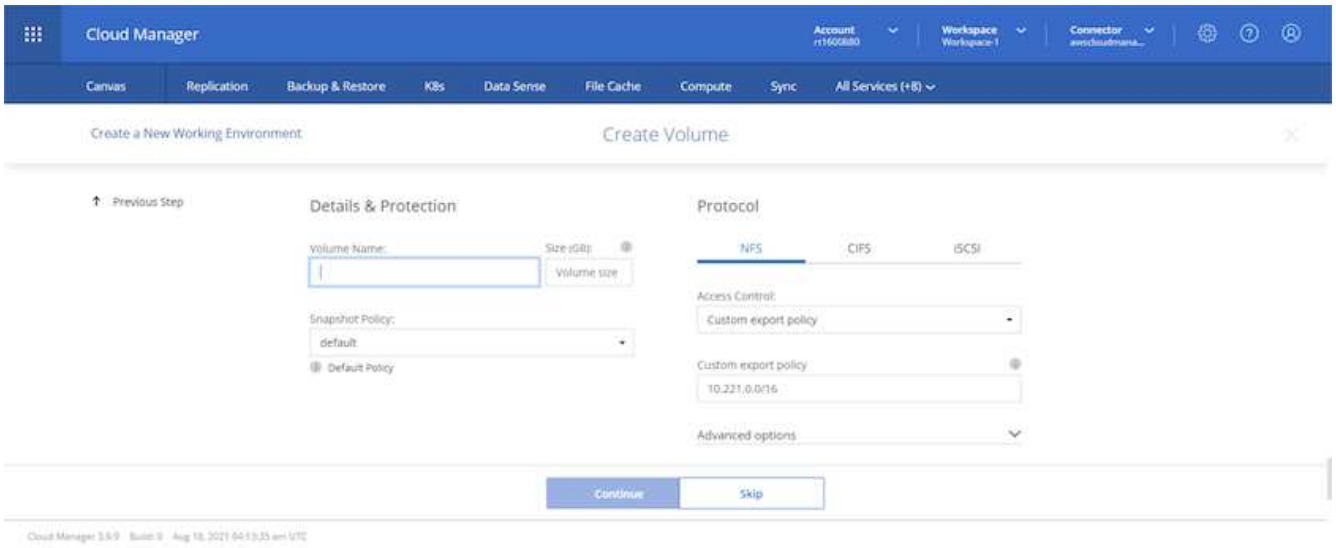
4. Choisissez votre modèle de licence. Si vous ne savez pas quel choix choisir, contactez votre représentant NetApp.



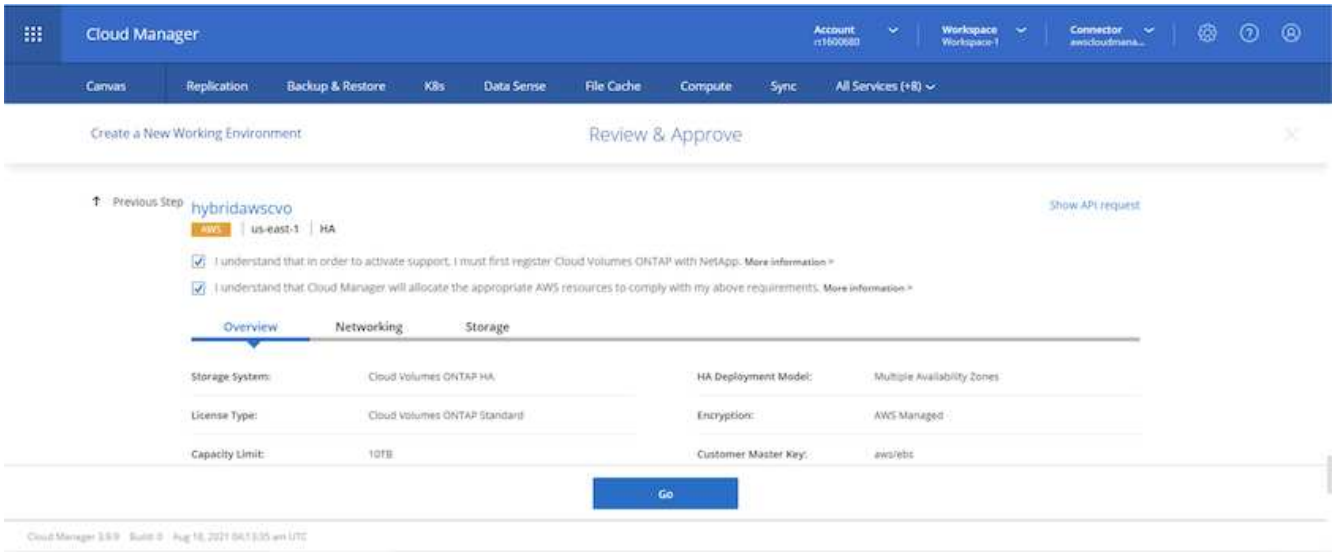
5. Sélectionnez la configuration la mieux adaptée à votre utilisation. Cela est lié aux considérations de dimensionnement décrites dans la page des prérequis.



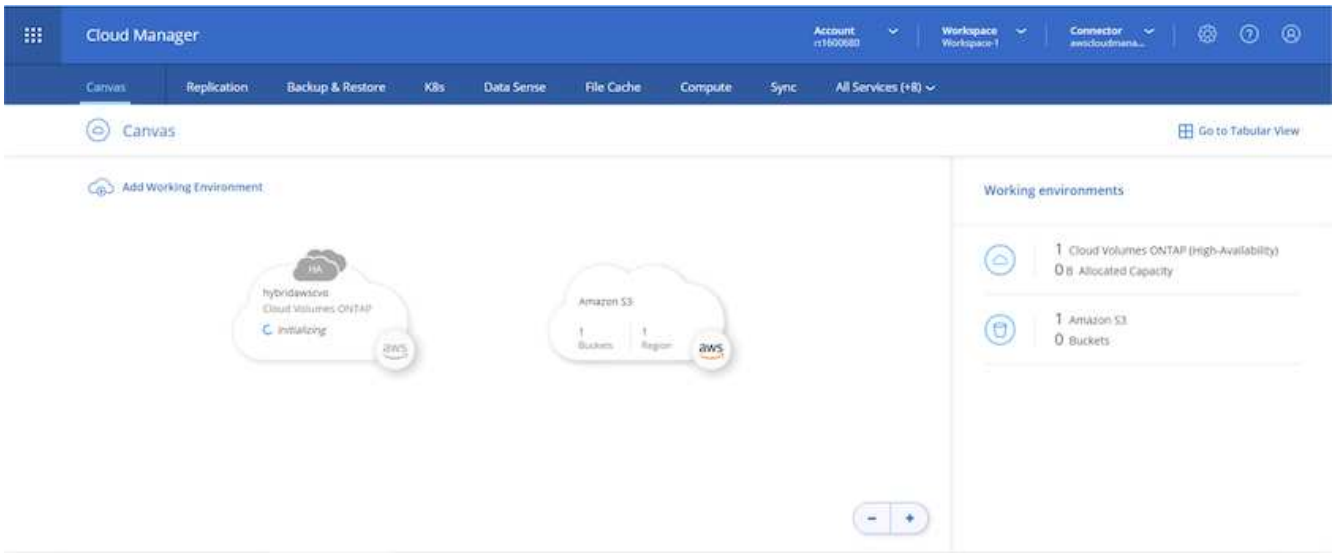
6. Créer un volume (facultatif) Cette opération n’est pas requise, car les étapes suivantes utilisent SnapMirror, qui crée les volumes pour nous.



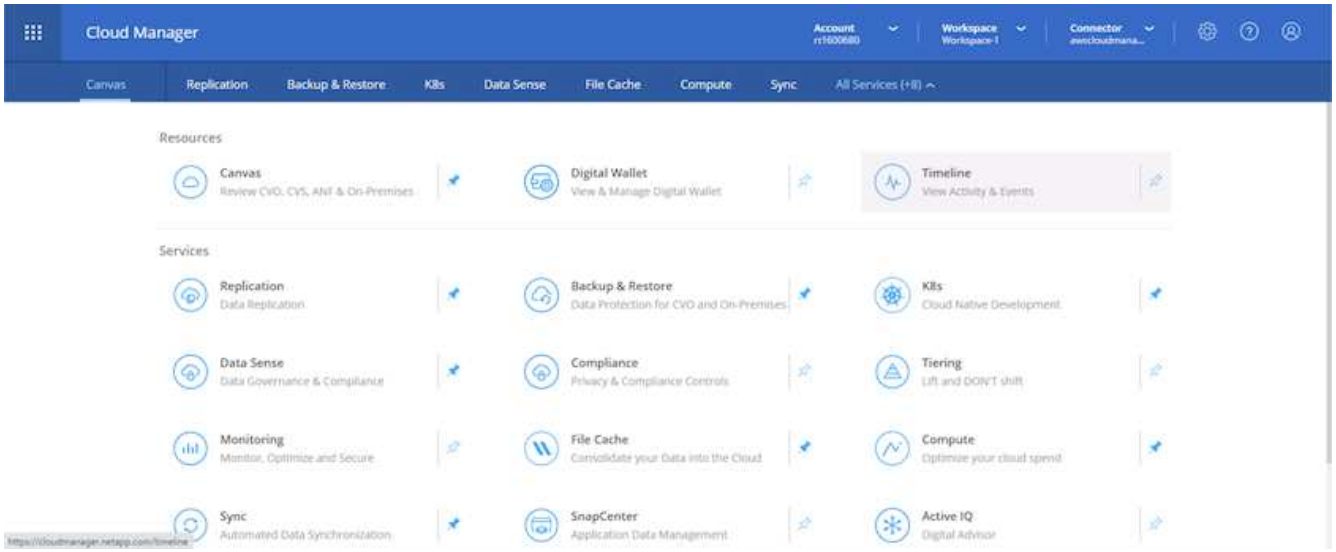
7. Vérifiez les sélections effectuées et cochez les cases pour vérifier que Cloud Manager déploie des ressources dans votre environnement AWS. Une fois terminé, cliquez sur Go.



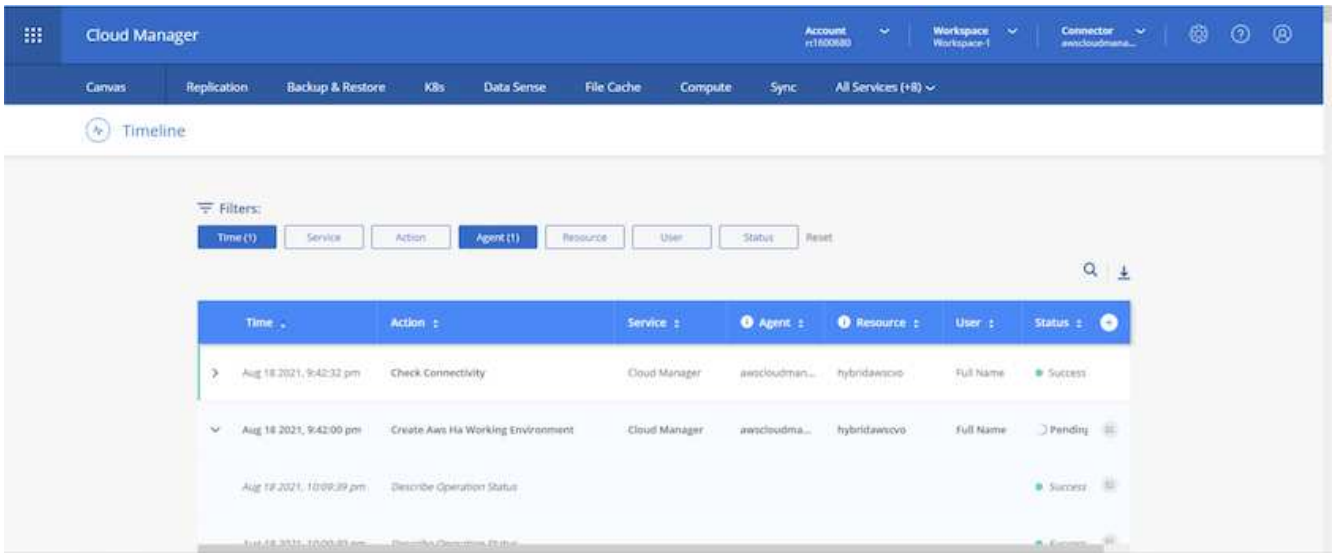
8. Le processus de déploiement commence maintenant par Cloud Volumes ONTAP. Cloud Manager utilise les API AWS et les piles de formation cloud pour déployer Cloud Volumes ONTAP. Il configure ensuite le système selon vos spécifications, vous offrant ainsi un système prêt à l'emploi qu'il est possible d'utiliser instantanément. La durée de ce processus varie en fonction des sélections effectuées.



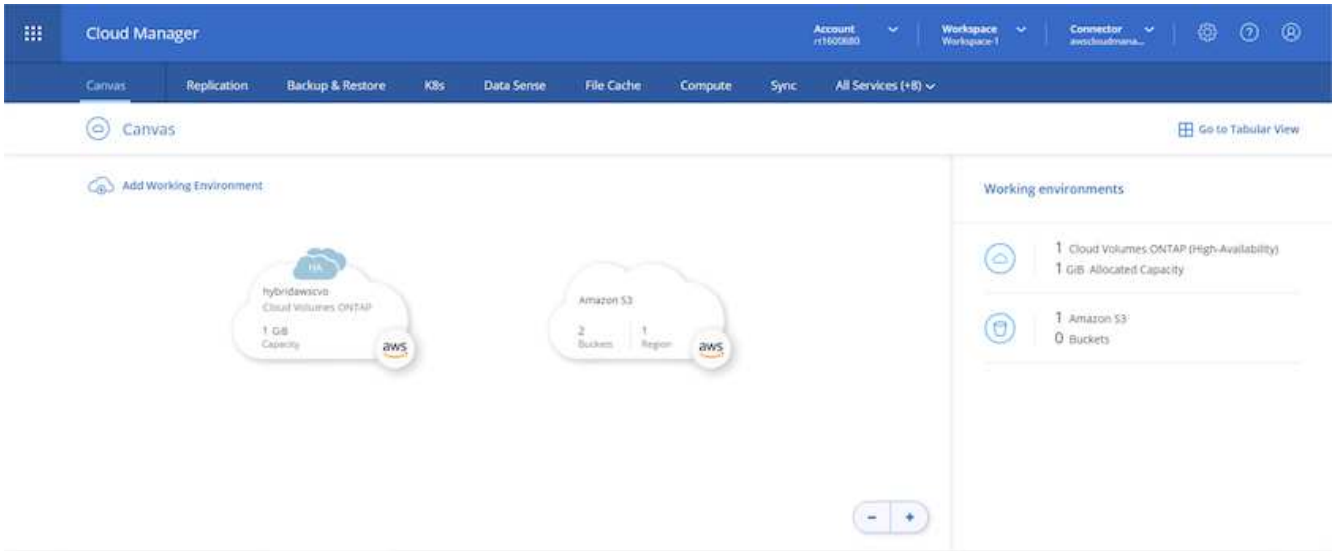
9. Vous pouvez contrôler la progression en accédant à la chronologie.



10. La chronologie représente un audit de toutes les actions effectuées dans Cloud Manager. Vous pouvez afficher tous les appels d'API effectués par Cloud Manager lors de la configuration sur AWS et sur le cluster ONTAP. Elle peut également être utilisée efficacement pour résoudre tous les problèmes auxquels vous êtes confronté.



11. Une fois le déploiement terminé, le cluster CVO s'affiche dans Canvas, pour lequel la capacité actuelle est de. Le cluster ONTAP à l'état actuel est entièrement configuré pour offrir une véritable expérience prête à l'emploi.

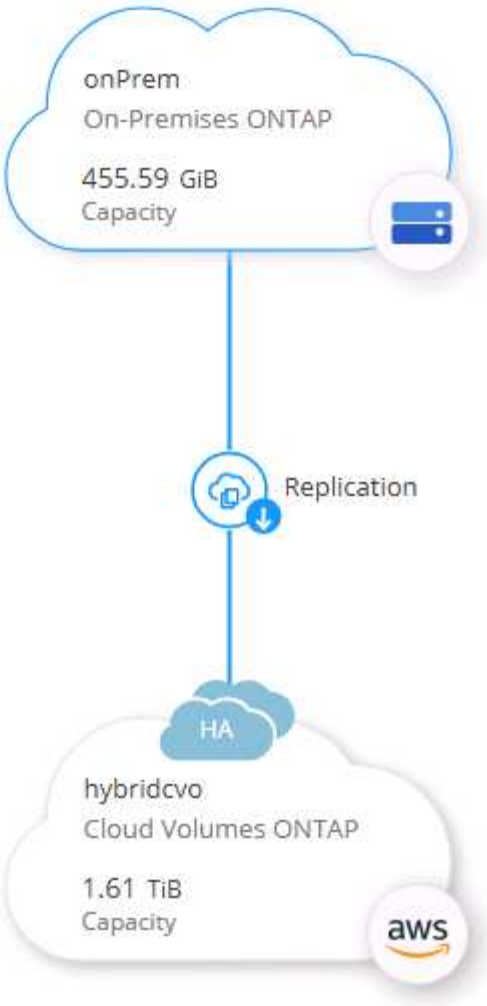


Configurez SnapMirror sur site vers le cloud

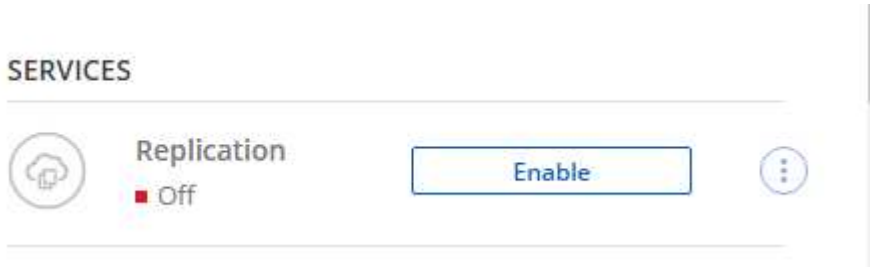
Dès lors que vous disposez d'un système ONTAP source et d'un système ONTAP de destination déployés, vous pouvez répliquer des volumes contenant des données de base de données dans le cloud.

Pour obtenir un guide sur les versions ONTAP compatibles avec SnapMirror, reportez-vous à la "Matrice de compatibilité SnapMirror".

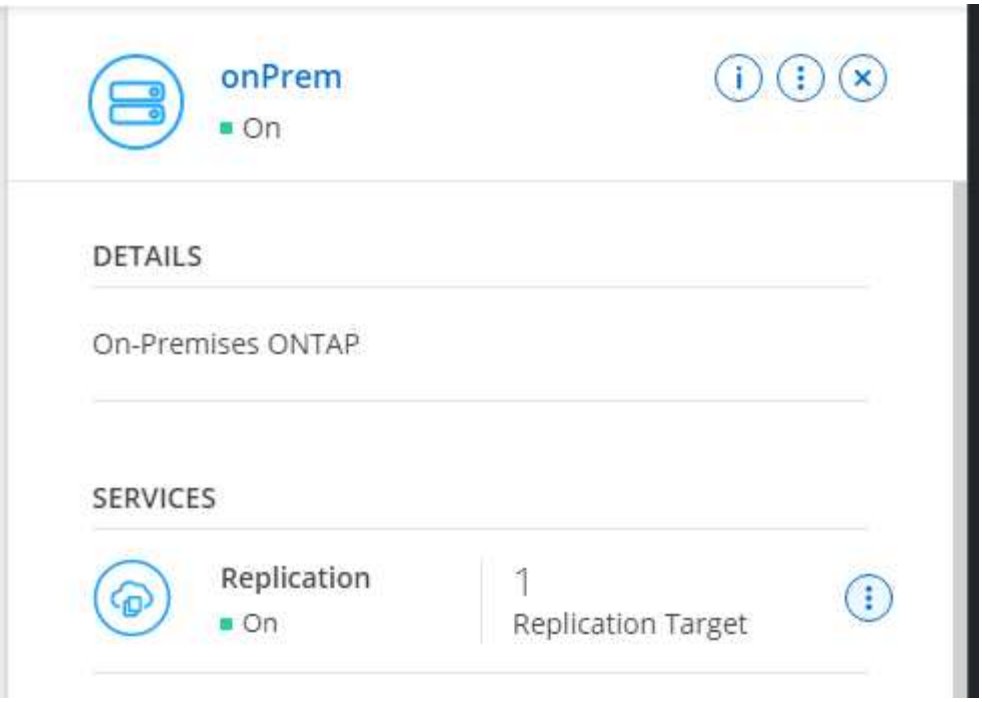
1. Cliquez sur le système ONTAP source (sur site) et faites-le glisser vers la destination, sélectionnez réplication > Activer ou sélectionnez réplication > Menu > répliquer.



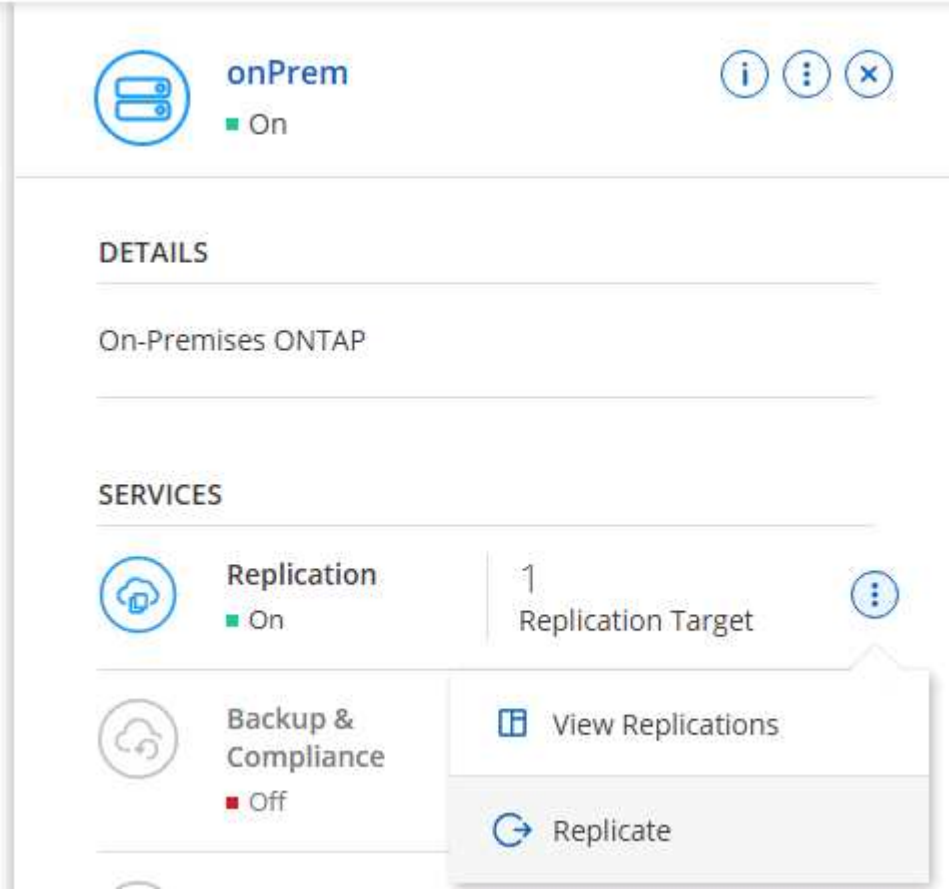
Sélectionnez Activer.



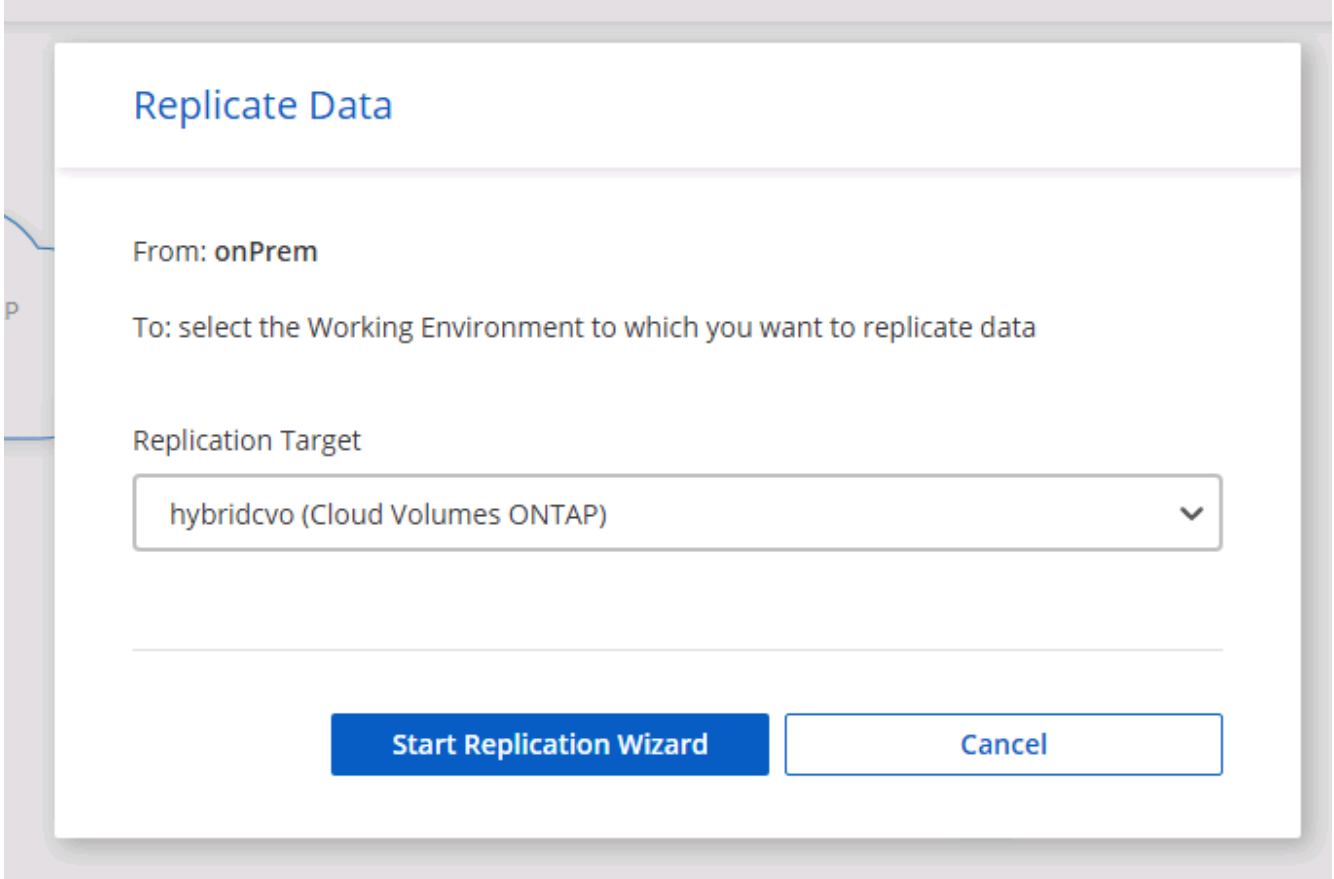
Ou Options.



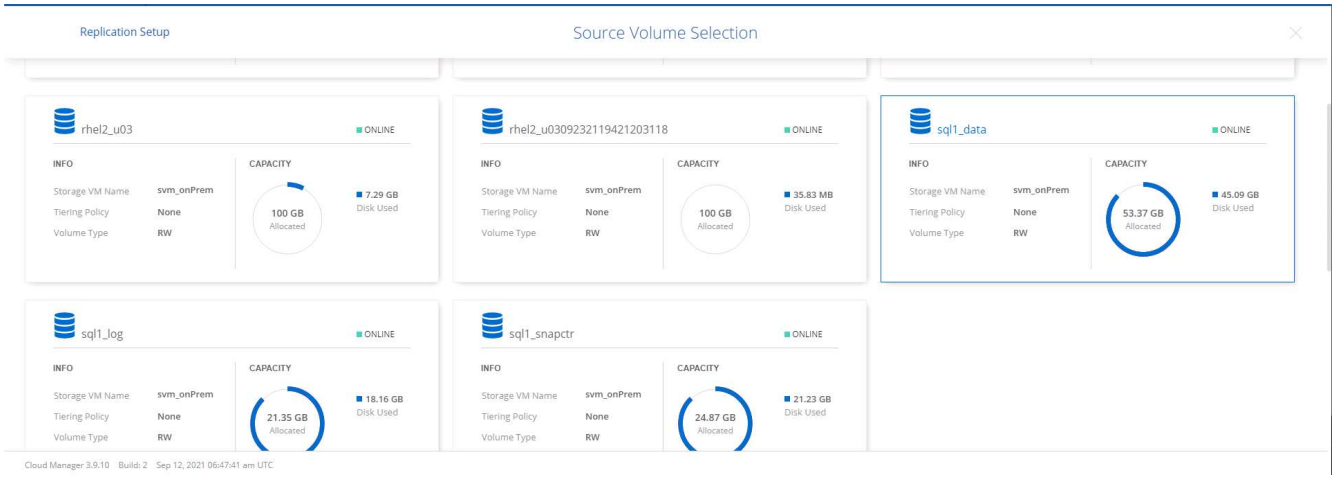
Répliquer.



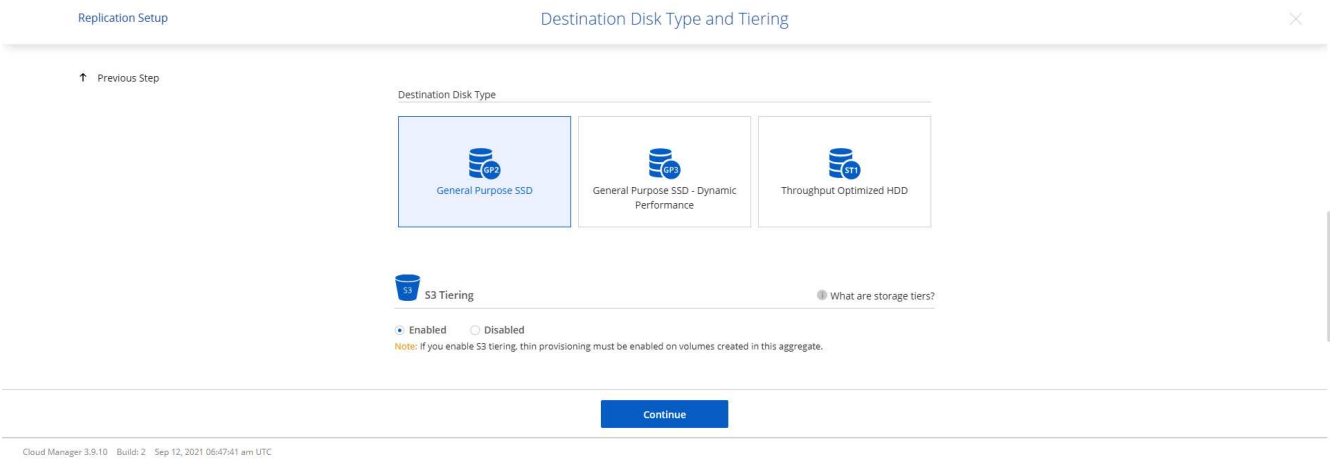
2. Si vous n'avez pas effectué de glisser-déposer, choisissez le cluster de destination vers lequel effectuer la réplication.



3. Choisissez le volume que vous souhaitez répliquer. Nous avons répliqué les données et tous les volumes des journaux.

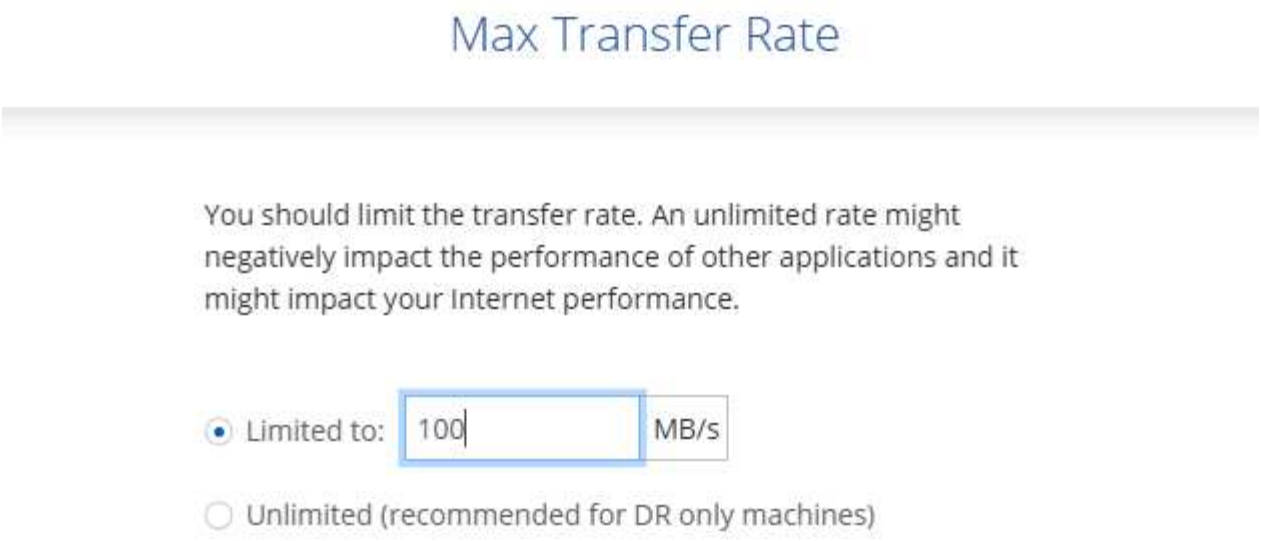


4. Choisissez le type de disque de destination et la règle de hiérarchisation. Pour la reprise après incident, nous recommandons l'utilisation d'un disque SSD comme type de disque et pour maintenir le Tiering des données. Le Tiering des données procède au Tiering des données en miroir dans un stockage objet à faible coût et vous permet d'économiser de l'argent sur des disques locaux. Lorsque vous rompez la relation ou que vous clonez le volume, les données utilisent le stockage local rapide.

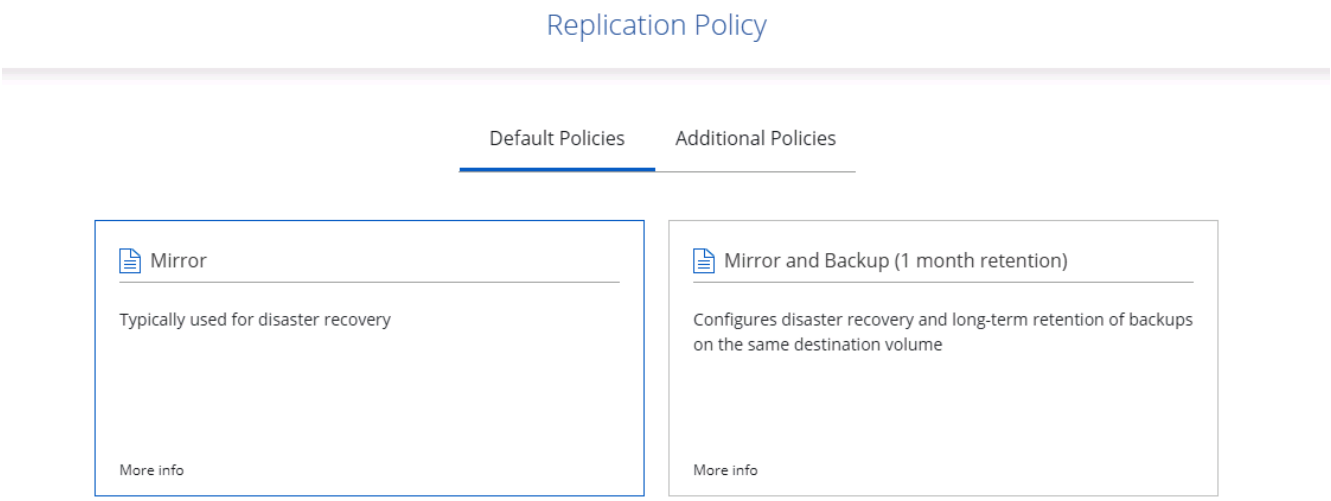


5. Sélectionnez le nom du volume de destination : nous avons choisi `[source_volume_name]_dr`.

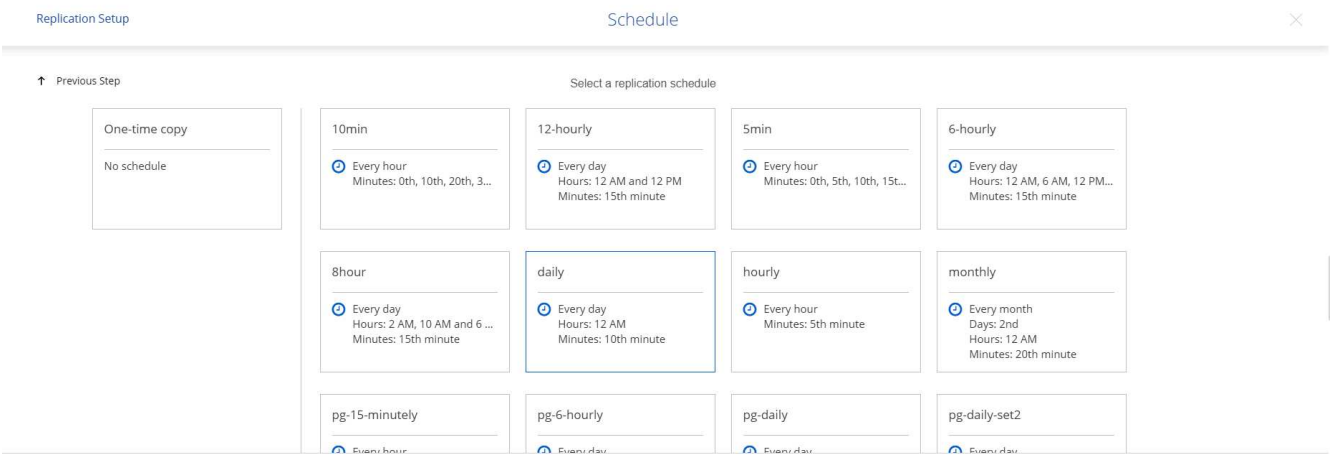
6. Sélectionnez la vitesse de transfert maximale pour la réplication. Cela vous permet d’économiser de la bande passante si vous disposez d’une connexion à faible bande passante au cloud, par exemple un VPN.



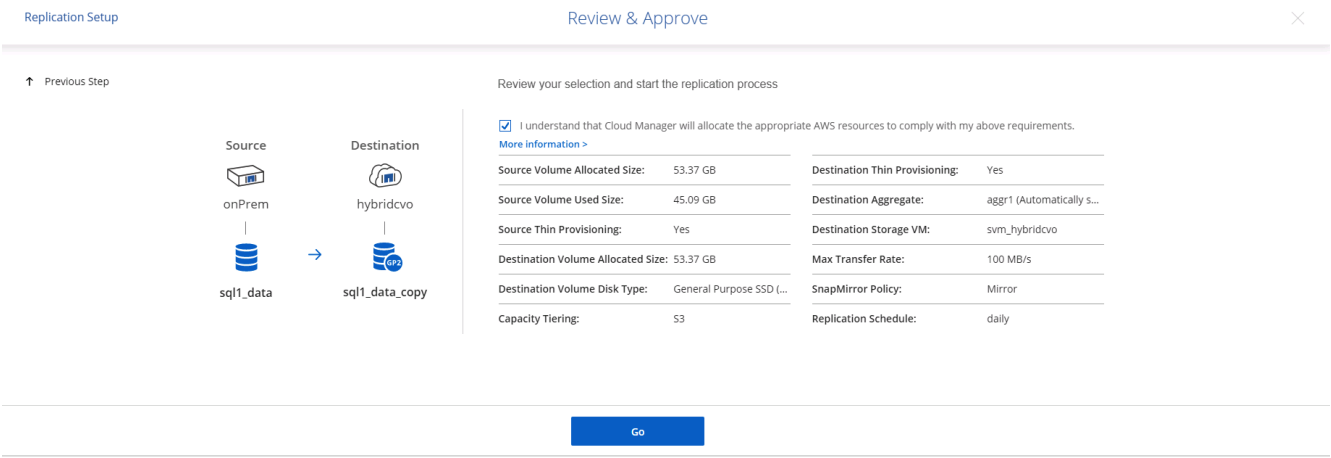
7. Définissez la règle de réplication. Nous avons choisi un miroir, qui prend le jeu de données le plus récent et le réplique dans le volume de destination. Vous pouvez également choisir une politique différente en fonction de vos besoins.



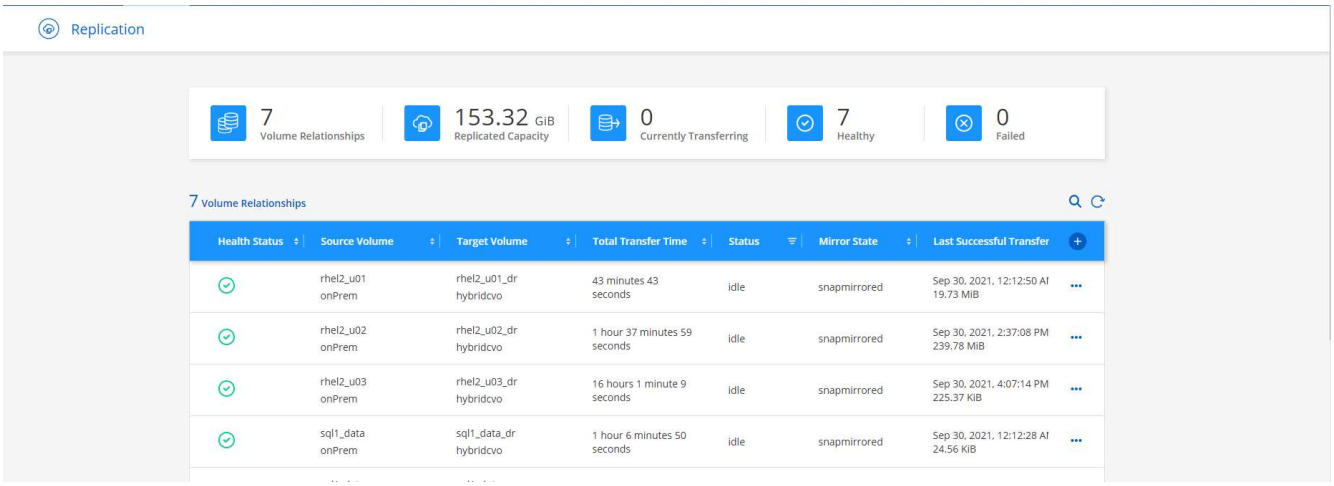
8. Choisissez la planification du déclenchement de la réplication. NetApp recommande de définir une planification « journalière » pour le volume de données et une planification « horaire » pour les volumes de journaux, même si cela peut être modifié en fonction des besoins.



9. Vérifier les informations saisies, cliquer sur Go pour déclencher l'homologue du cluster et l'homologue SVM (si c'est votre première réplication entre les deux clusters), puis mettre en œuvre et initialiser la relation SnapMirror.



10. Poursuivez ce processus pour les volumes de données et de journaux.
11. Pour vérifier toutes vos relations, accédez à l'onglet réplication dans Cloud Manager. Vous pouvez ici gérer vos relations et connaître leur statut.



12. Une fois tous les volumes répliqués, vous êtes dans un état stable et prêt à passer aux flux de travail de reprise après incident et de développement/test.

3. Déployez l’instance de calcul EC2 pour les workloads de bases de données

AWS a préconfiguré des instances de calcul EC2 pour diverses charges de travail. Le choix du type d’instance détermine le nombre de cœurs de processeur, la capacité de mémoire, le type de stockage et la capacité, ainsi que la performance du réseau. Pour ces cas d’usage, à l’exception de la partition OS, le stockage principal permettant l’exécution de la charge de travail de la base de données est alloué à partir de CVO ou du moteur de stockage FSX ONTAP. Par conséquent, les principaux facteurs à prendre en compte sont le choix des cœurs de processeur, de la mémoire et du niveau de performance du réseau. Les types d’instances AWS EC2 classiques sont disponibles ici : "Type d’instance EC2".

Dimensionnement de l’instance de calcul

1. Sélectionnez le type d’instance approprié en fonction de la charge de travail requise. Les facteurs à prendre en compte incluent le nombre de transactions commerciales à prendre en charge, le nombre d’utilisateurs simultanés, le dimensionnement des jeux de données, etc.
2. Le déploiement d’instances EC2 peut être lancé via le tableau de bord EC2. Les procédures de déploiement précises dépassent le cadre de cette solution. Voir "Amazon EC2" pour plus d’informations.

Configuration de l’instance Linux pour le workload Oracle

Cette section contient des étapes de configuration supplémentaires après le déploiement d’une instance EC2 Linux.

1. Ajoutez une instance de secours Oracle au serveur DNS pour la résolution de nom dans le domaine de gestion SnapCenter.
2. Ajoutez un ID utilisateur de gestion Linux en tant que identifiants SnapCenter OS avec des autorisations sudo sans mot de passe. Activez l’ID avec l’authentification par mot de passe SSH sur l’instance EC2. (Par défaut, l’authentification par mot de passe SSH et le sudo sans mot de passe sont désactivés sur les instances EC2.)
3. Configurez l’installation Oracle pour qu’elle corresponde à l’installation Oracle sur site, par exemple les correctifs du système d’exploitation, les versions et correctifs d’Oracle, etc.
4. Les rôles d’automatisation de la base de données NetApp Ansible peuvent être utilisés pour configurer les instances EC2 pour le développement/test des bases de données et la reprise après incident. Le code d’automatisation peut être téléchargé sur le site GitHub public de NetApp : "Déploiement automatisé Oracle 19c". L’objectif est d’installer et de configurer une pile logicielle de base de données sur une instance EC2 afin qu’elle corresponde aux configurations du système d’exploitation et de la base de données sur site.

Configuration de l’instance Windows pour la charge de travail SQL Server

Cette section répertorie d’autres étapes de configuration après le déploiement initial d’une instance de Windows EC2.

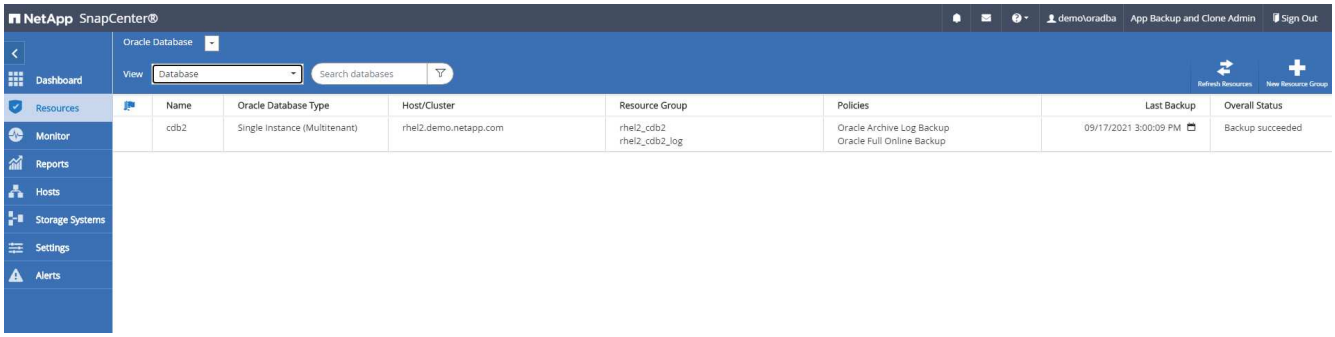
1. Récupérez le mot de passe administrateur Windows pour vous connecter à une instance via RDP.
2. Désactivez le pare-feu Windows, rejoignez l’hôte dans le domaine SnapCenter de Windows et ajoutez l’instance au serveur DNS pour la résolution du nom.
3. Provisionnez un volume log SnapCenter pour stocker les fichiers log de SQL Server.
4. Configurez iSCSI sur l’hôte Windows pour monter le volume et formater le lecteur de disque.
5. Là encore, une grande partie des tâches précédentes peuvent être automatisées avec la solution d’automatisation NetApp pour SQL Server. Consultez le site GitHub public d’automatisation NetApp pour connaître les nouveaux rôles et solutions publiés : "Automatisation NetApp".

Workflow de développement/test bursting vers le cloud

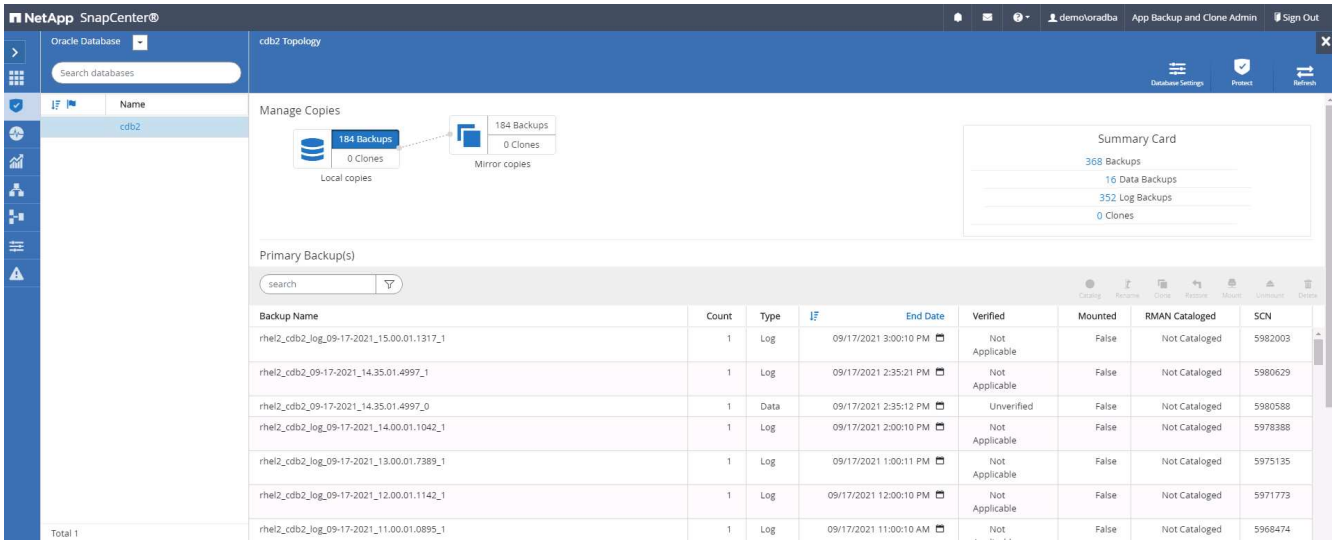
L'agilité du cloud public, le retour sur investissement et les économies générées sont toutes des propositions de valeur pertinentes pour les entreprises qui adoptent le cloud public pour les efforts de développement et de test des applications de bases de données. SnapCenter est le meilleur outil pour faire de cette vision une réalité. SnapCenter peut non seulement protéger votre base de données de production sur site, mais aussi cloner rapidement une copie pour le développement d'applications ou les tests de code dans le cloud public, tout en consommant très peu d'espace de stockage supplémentaire. Vous trouverez ci-après des détails sur les processus étape par étape d'utilisation de cet outil.

Cloner une base de données Oracle à des fins de développement et de test à partir d'une sauvegarde snapshot répliquée

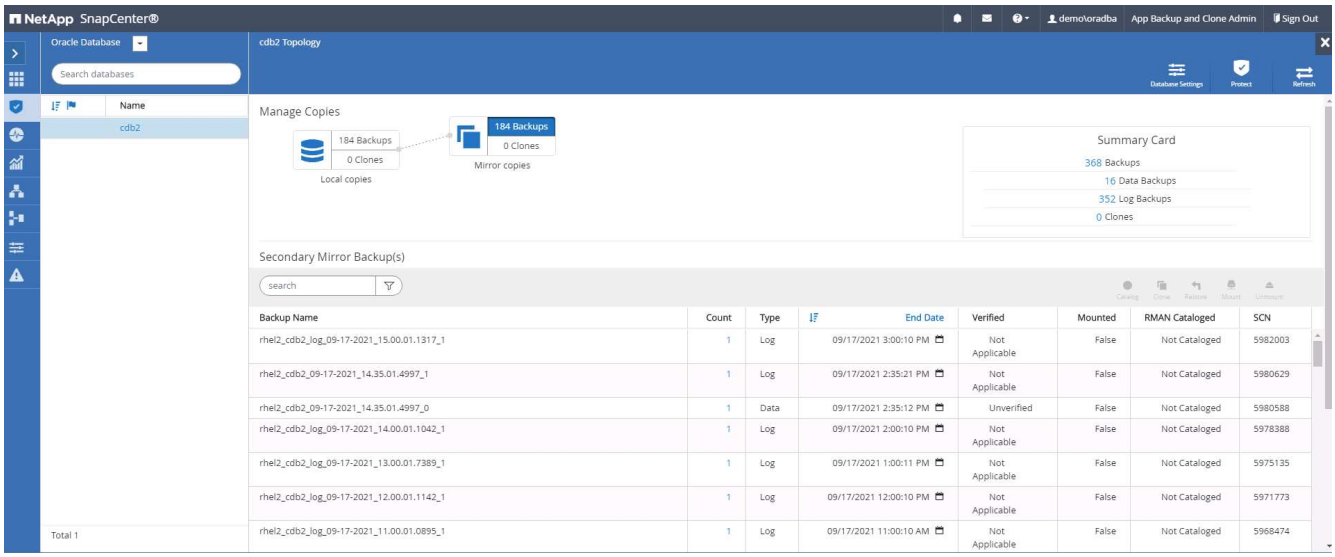
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données pour Oracle. Accédez à l'onglet Ressources, qui affiche les bases de données Oracle protégées par SnapCenter.



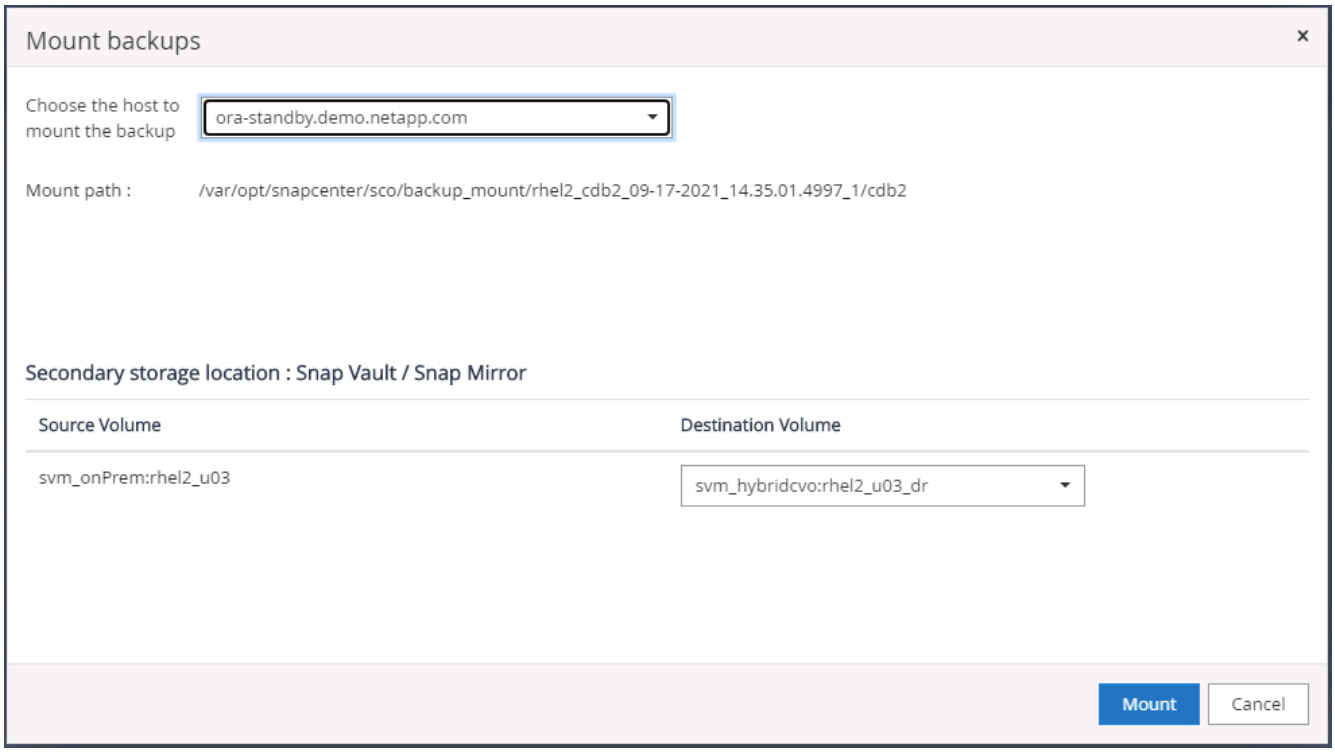
2. Cliquez sur le nom de la base de données sur site prévue pour la topologie de sauvegarde et la vue détaillée. Si un emplacement répliqué secondaire est activé, les sauvegardes miroir liées s'affichent.

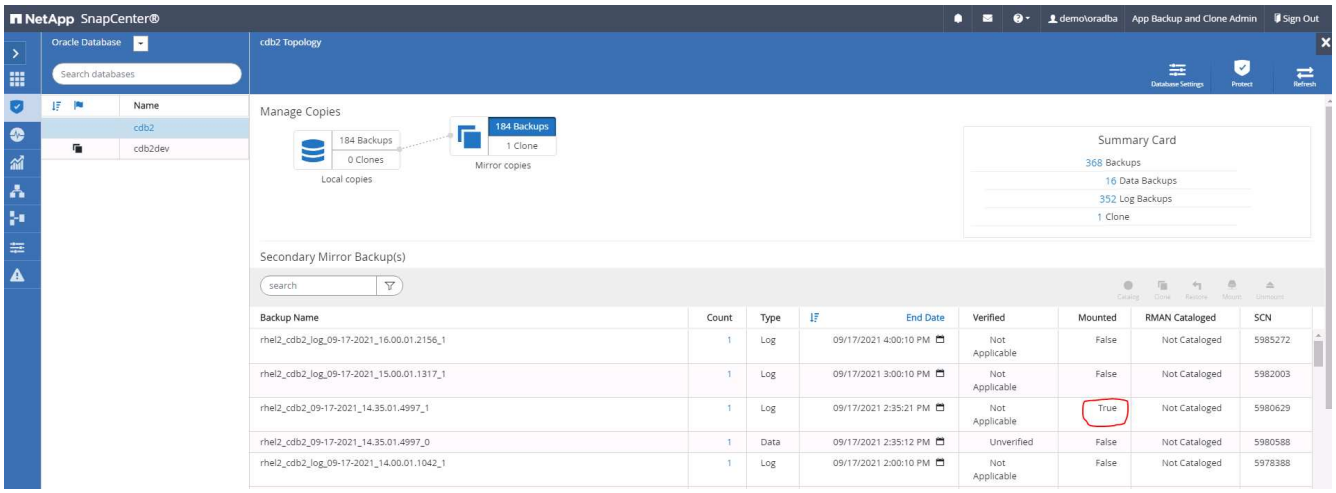


3. Basculez vers la vue sauvegardes en miroir en cliquant sur sauvegardes en miroir. La ou les sauvegardes du miroir secondaire s'affichent alors.



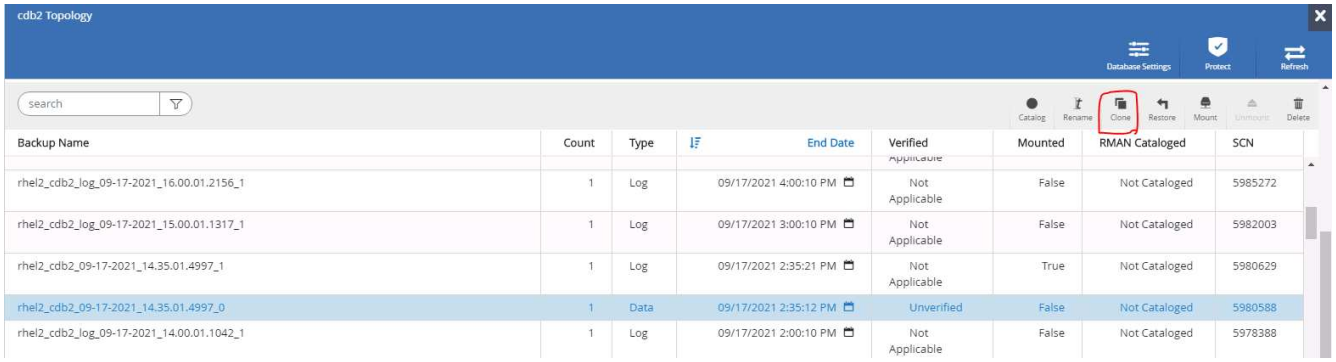
4. Choisissez une copie de sauvegarde de base de données secondaire en miroir à cloner et déterminez un point de récupération par heure et numéro de modification du système ou par SCN. Généralement, le point de restauration doit faire l'objet d'une sauvegarde complète de la base de données ou d'un SCN à cloner. Une fois qu'un point de récupération a été déterminé, la sauvegarde du fichier journal requis doit être montée pour la restauration. La sauvegarde du fichier journal doit être montée sur le serveur de base de données cible sur lequel la base de données clone doit être hébergée.



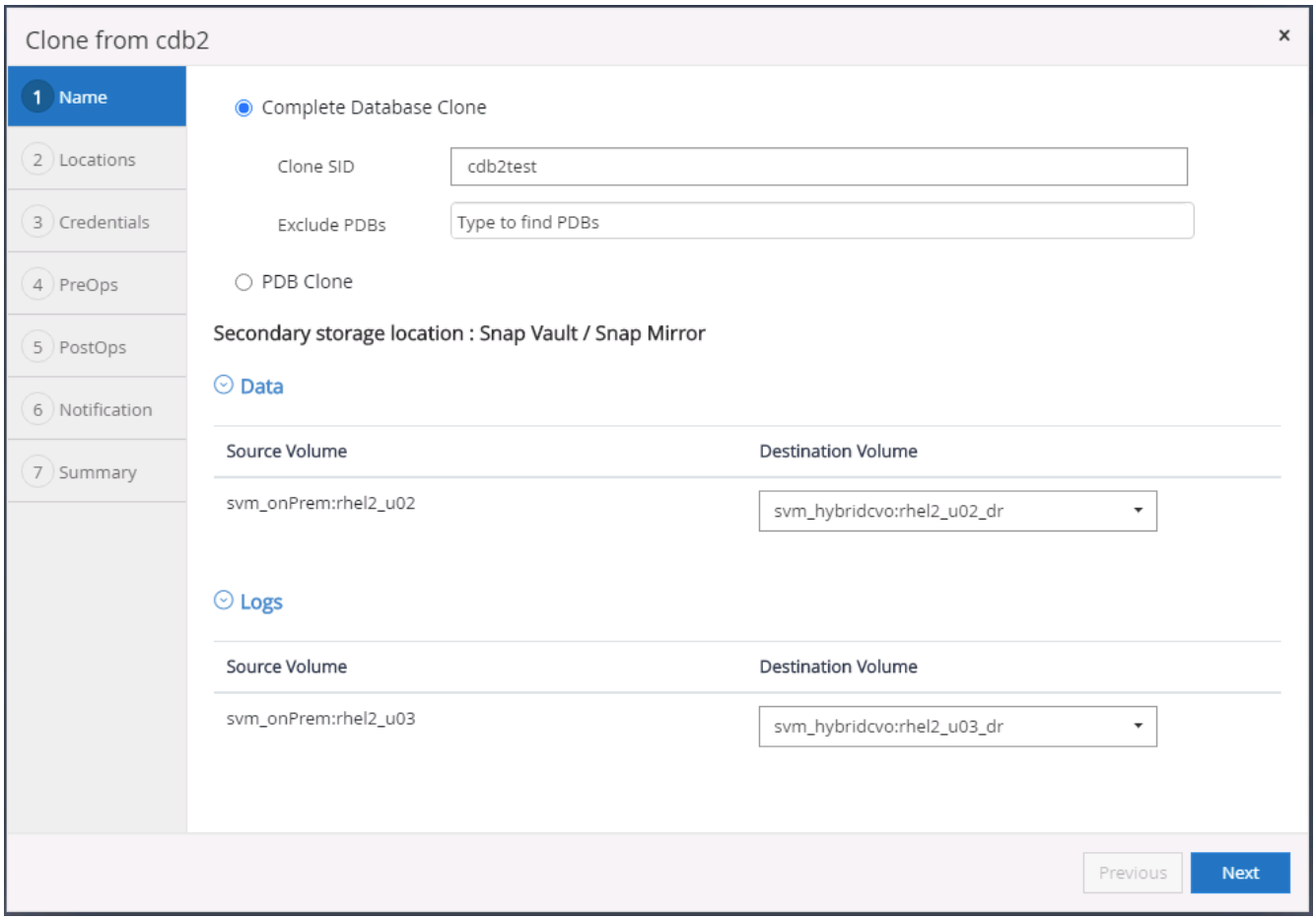


Si l'élagage des journaux est activé et que le point de restauration est étendu au-delà de la dernière taille des journaux, il peut être nécessaire de monter plusieurs sauvegardes des journaux d'archives.

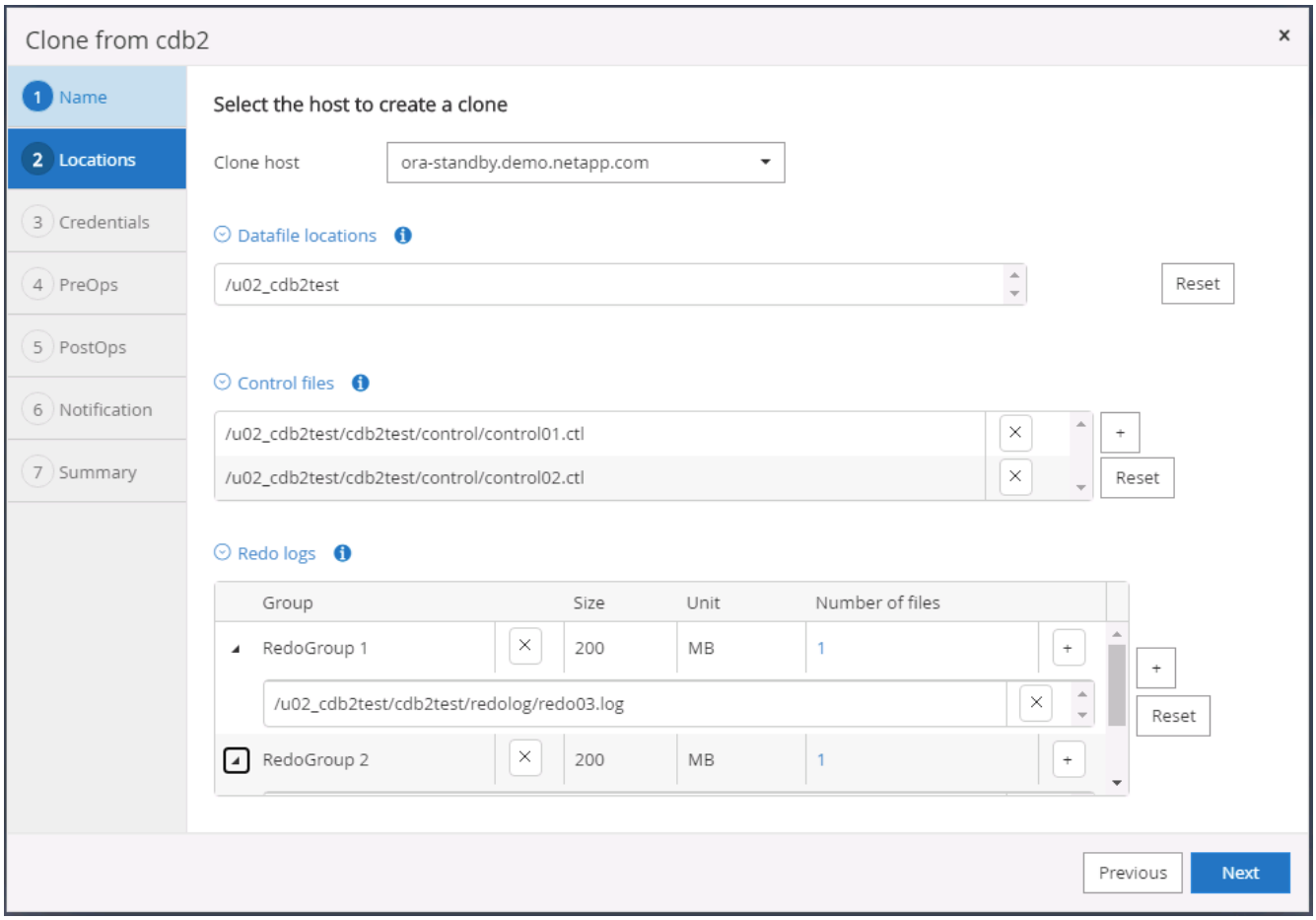
5. Mettez en surbrillance la copie de sauvegarde complète de la base de données à cloner, puis cliquez sur le bouton clone pour démarrer le workflow du clone de base de données.



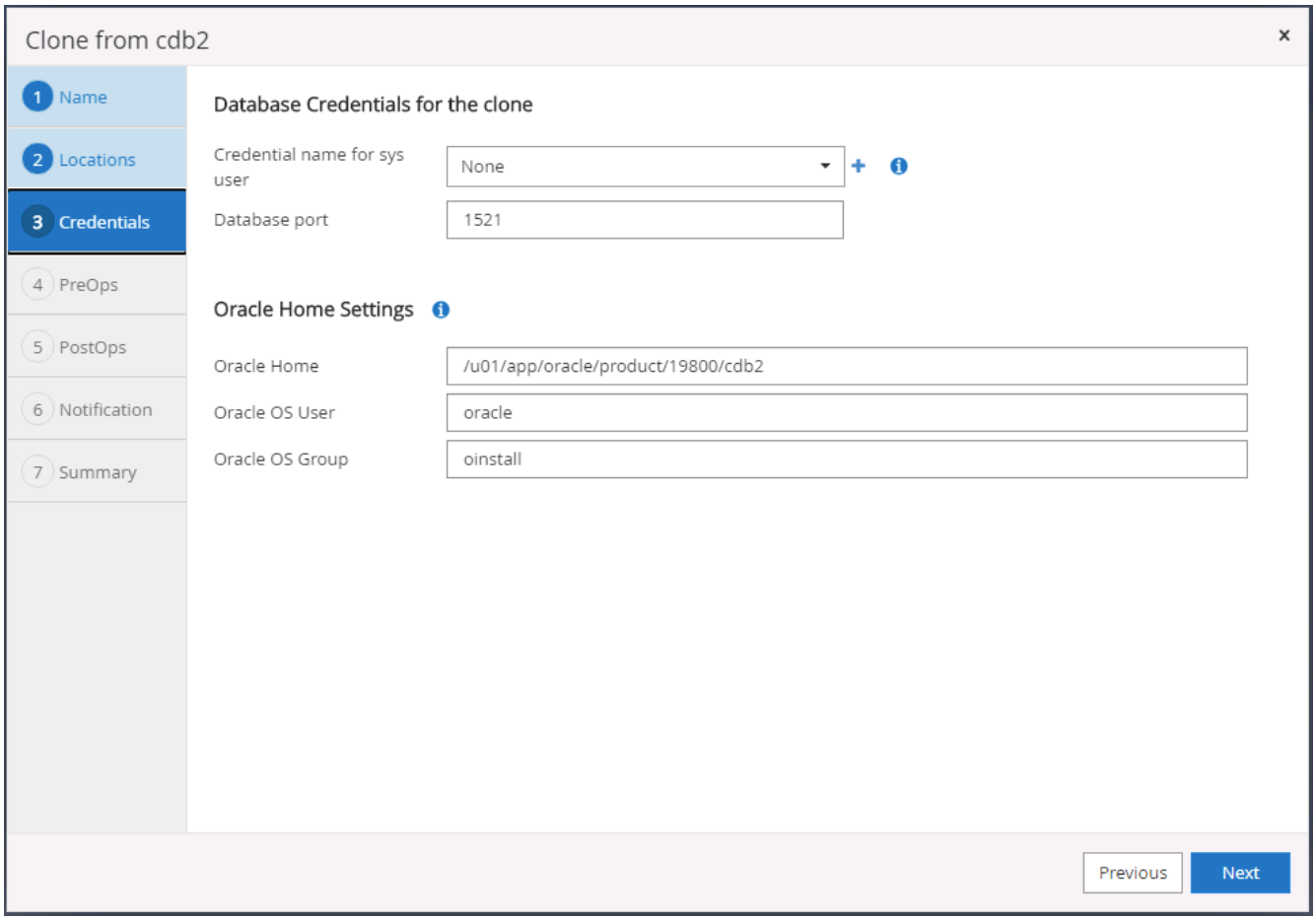
6. Choisissez un SID de base de données de clonage approprié pour une base de données de conteneur complète ou un clone CDB.



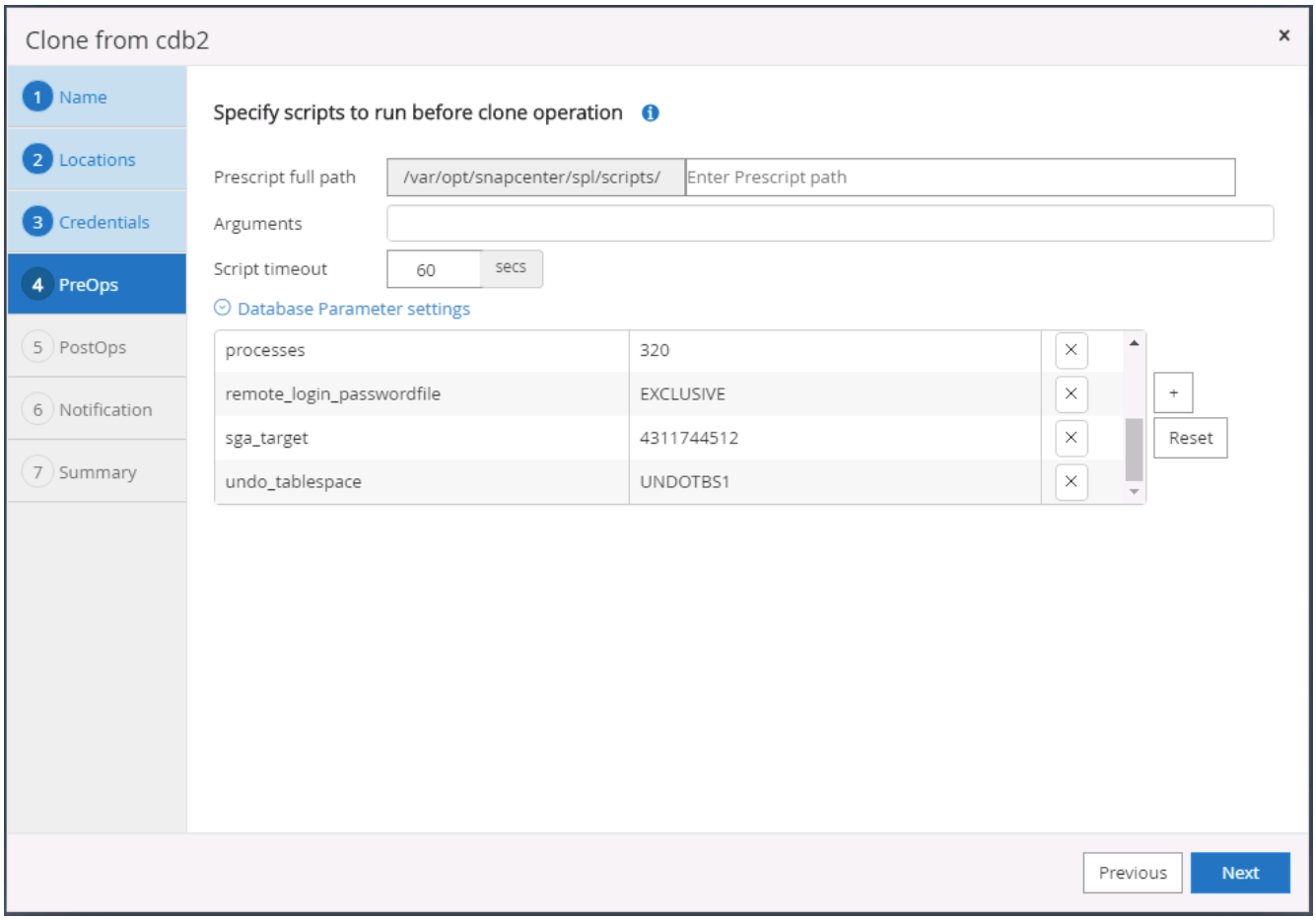
7. Sélectionnez l'hôte de clone cible dans le cloud. Les répertoires des fichiers de données, des fichiers de contrôle et des journaux de reprise sont créés par le workflow de clonage.



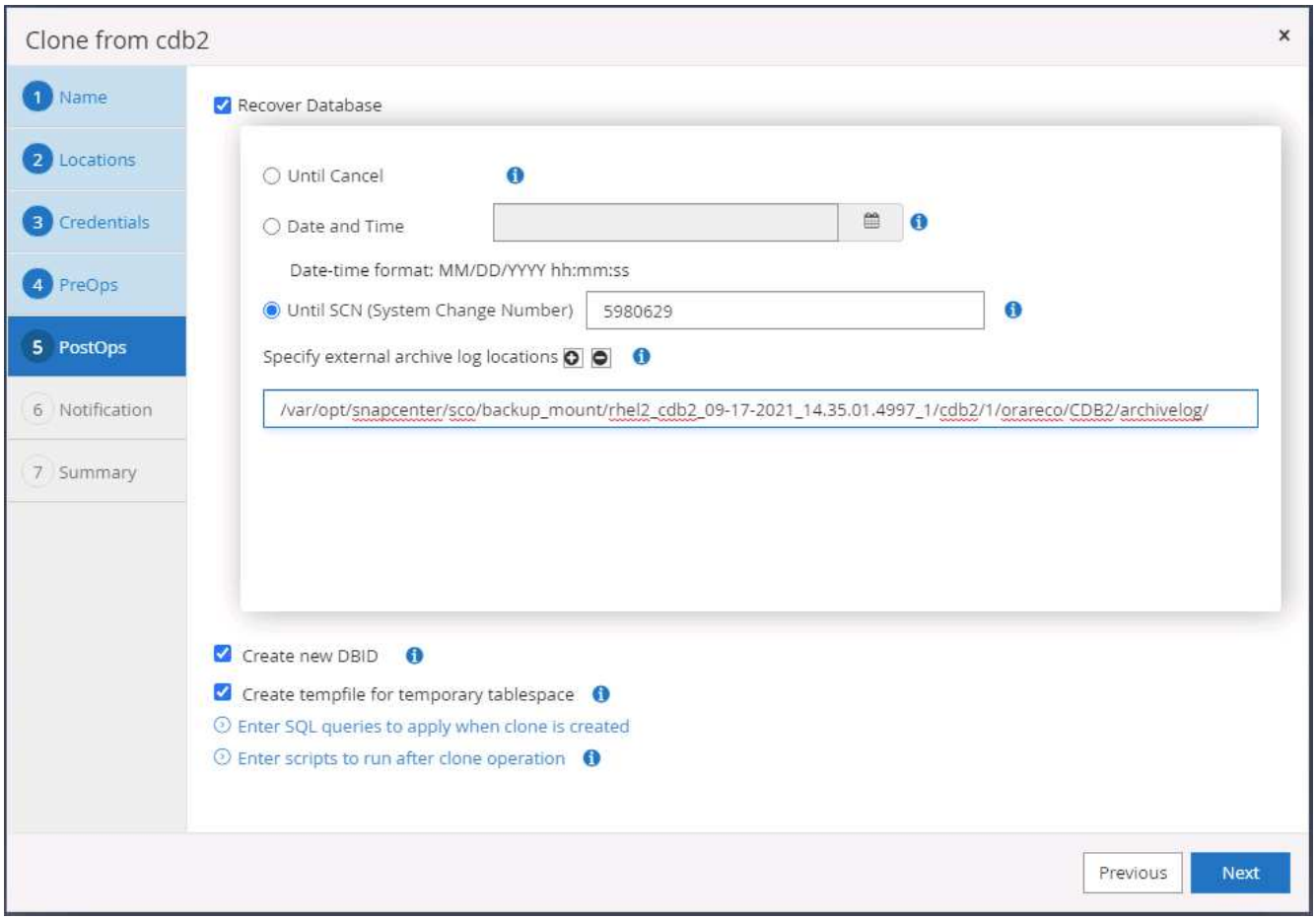
8. Le nom d'identification aucun est utilisé pour l'authentification basée sur le système d'exploitation, ce qui rend le port de base de données non pertinent. Remplissez le répertoire Oracle Home, Oracle OS User et Oracle OS Group approprié tel qu'il est configuré dans le serveur de base de données clone cible.

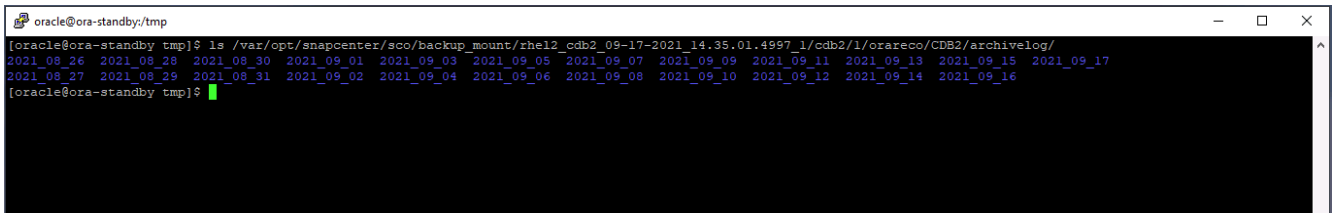


9. Spécifiez les scripts à exécuter avant l'opération de clonage. Plus important encore, le paramètre d'instance de base de données peut être ajusté ou défini ici.

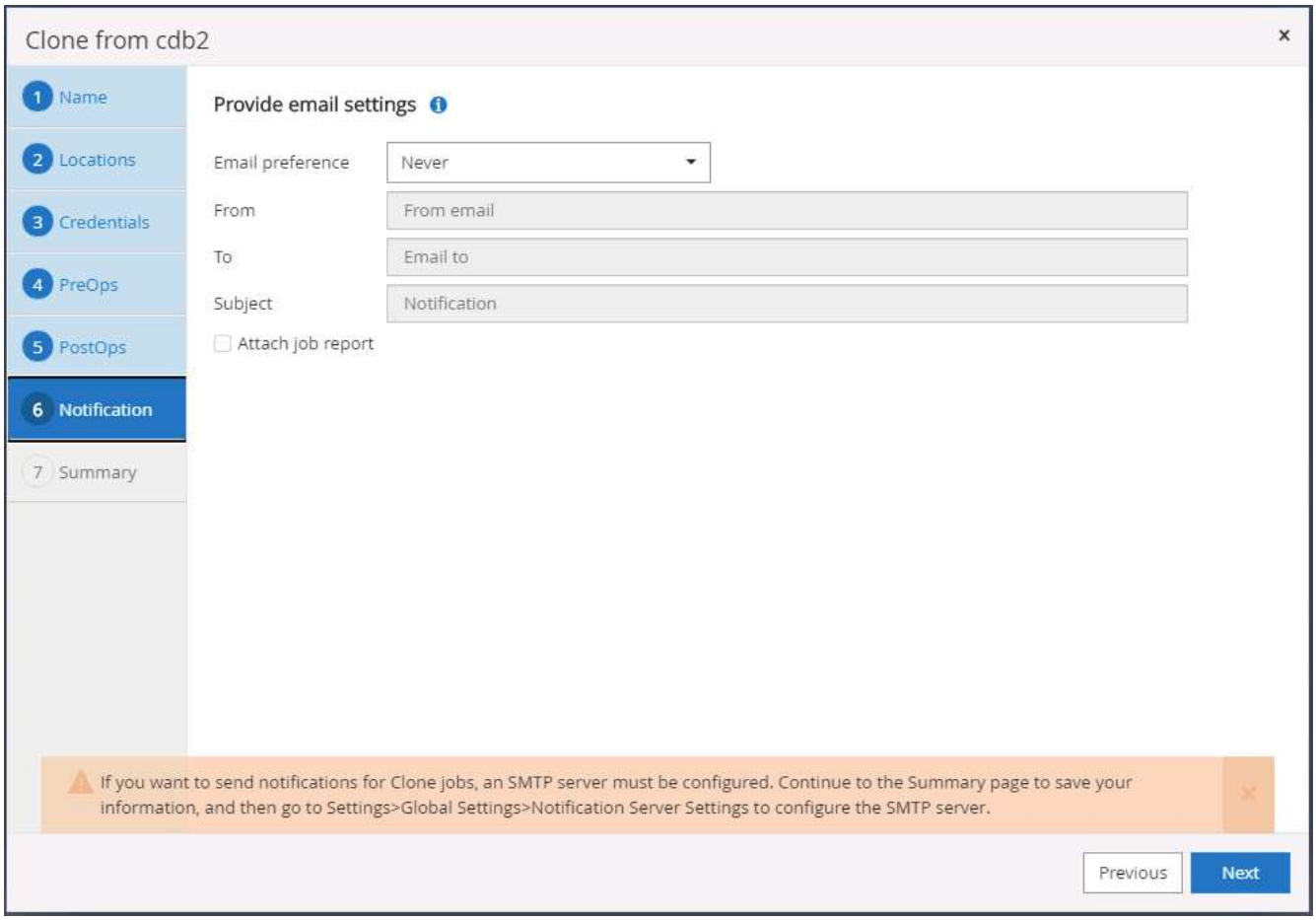


10. Spécifiez le point de récupération par date et heure ou par SCN. Jusqu'à ce que Annuler récupère la base de données jusqu'aux journaux d'archivage disponibles. Spécifiez l'emplacement du journal d'archivage externe à partir de l'hôte cible sur lequel le volume du journal d'archivage est monté. Si le propriétaire Oracle du serveur cible est différent du serveur de production sur site, vérifiez que le répertoire du journal d'archivage est lisible par le propriétaire Oracle du serveur cible.

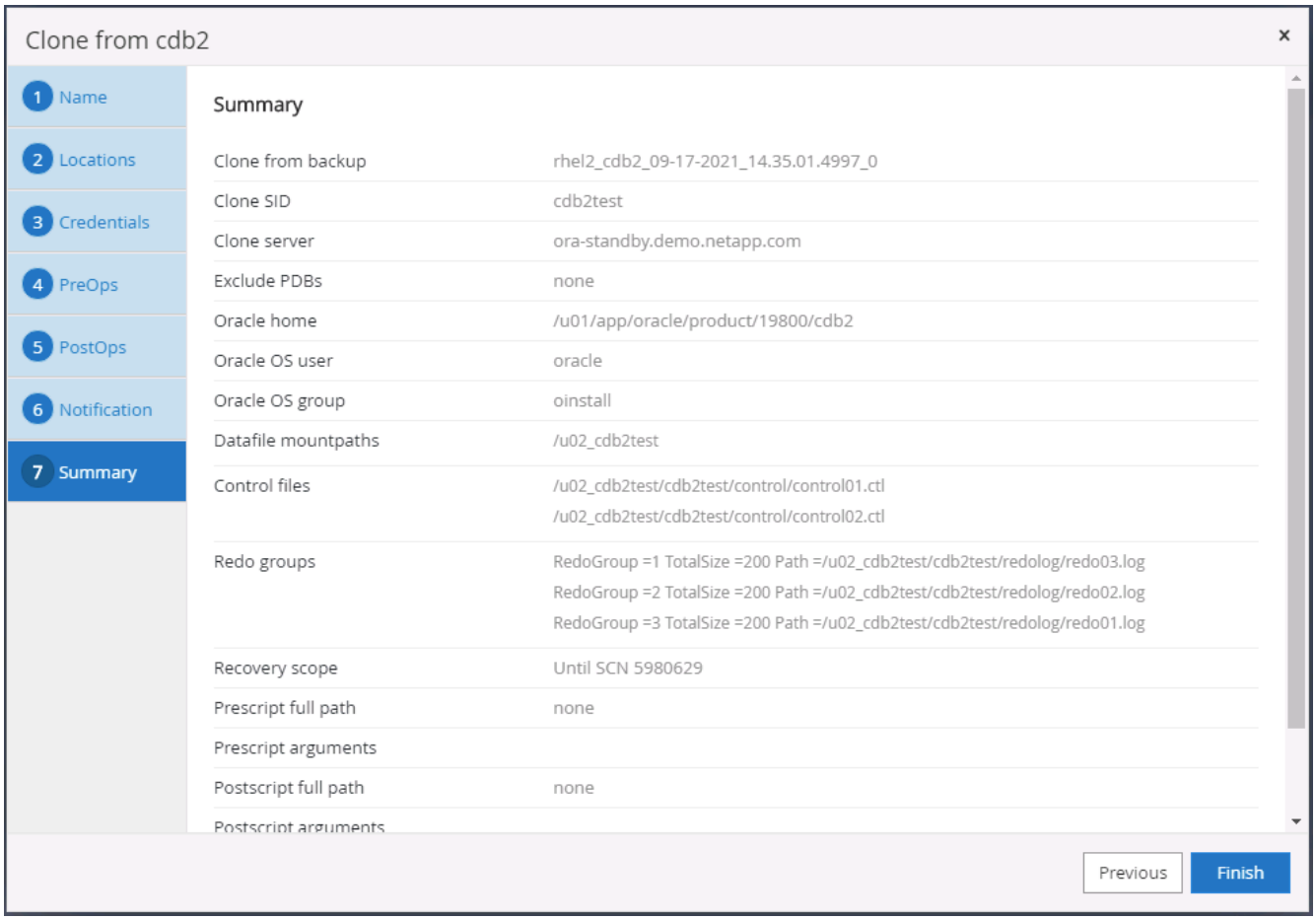




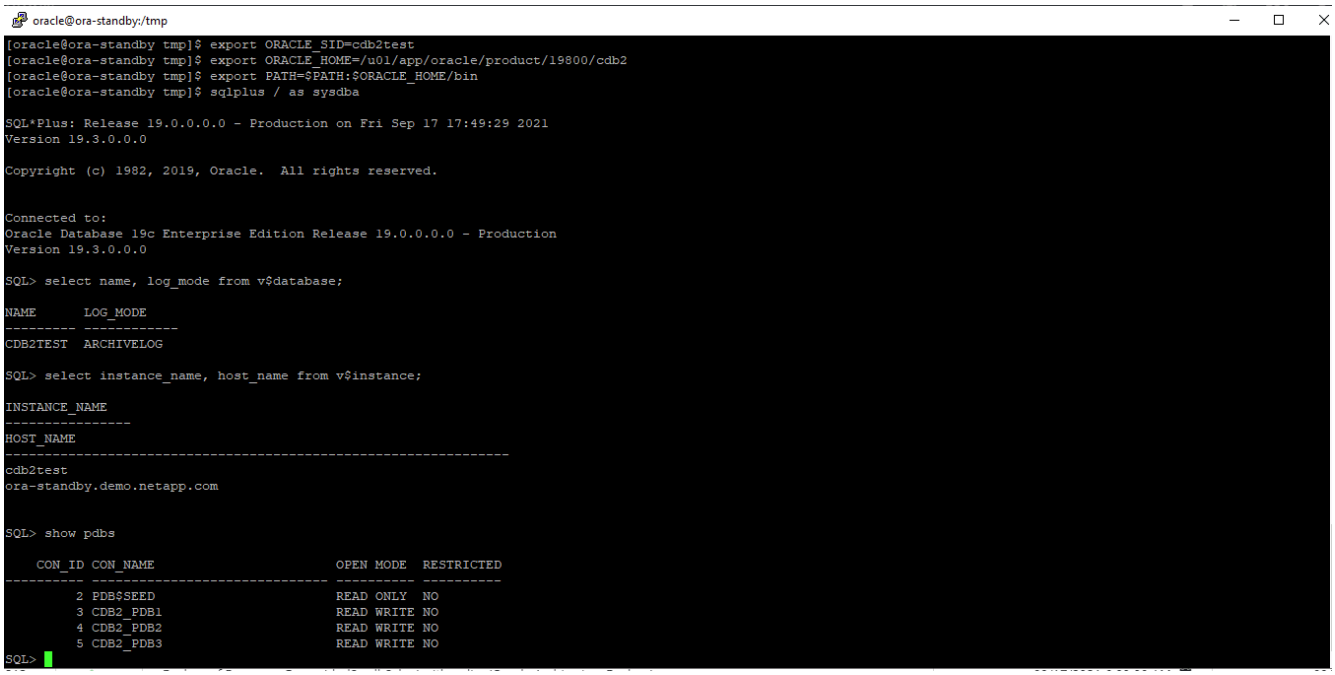
11. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.



12. Récapitulatif du clonage.

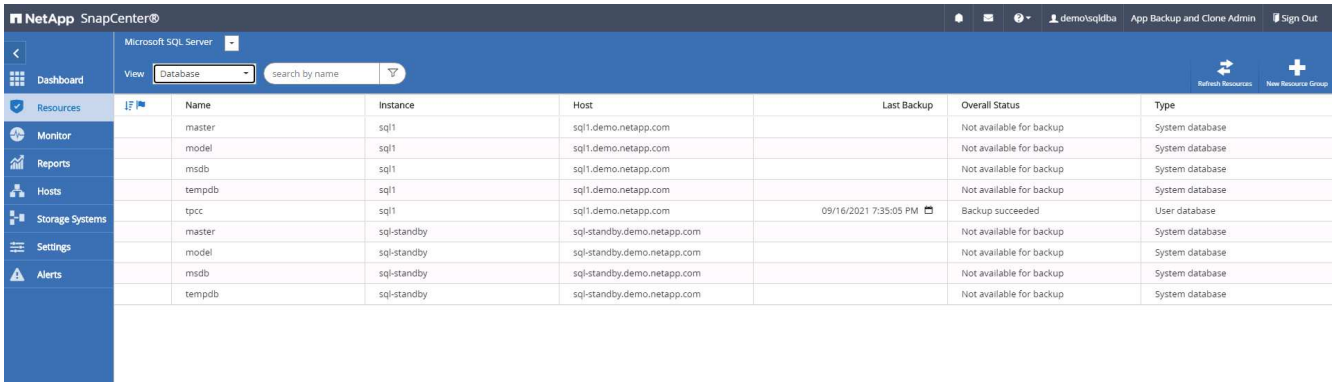


13. Après le clonage, vous devez vérifier que la base de données clonée est opérationnelle. Certaines tâches supplémentaires, telles que le démarrage de l'écouteur ou la désactivation du mode d'archivage du journal DB, peuvent être effectuées sur la base de données de développement/test.

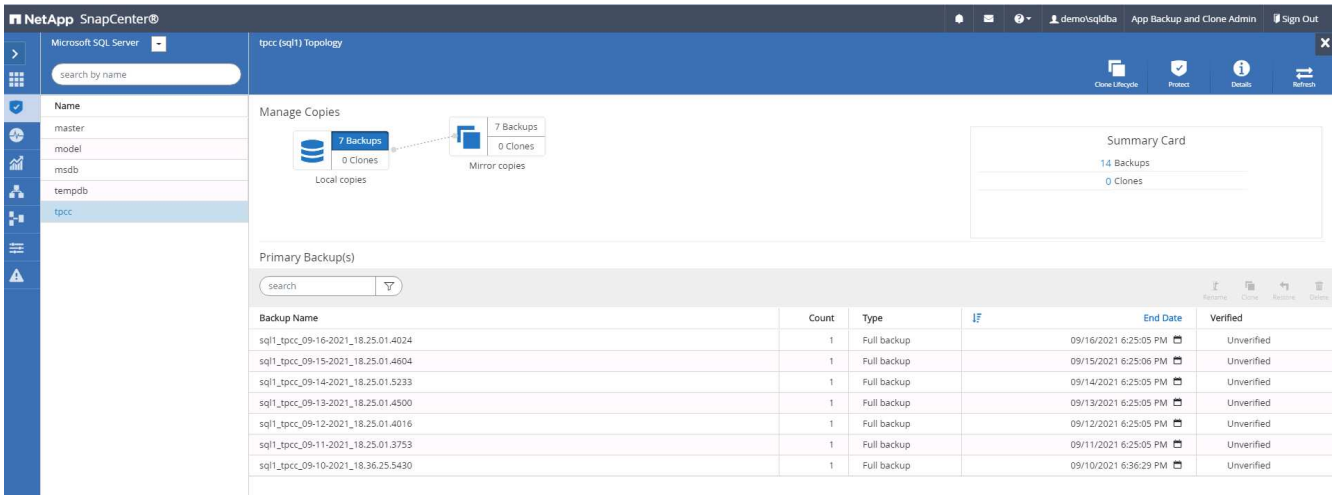


Cloner une base de données SQL à des fins de développement et de test à partir d'une sauvegarde Snapshot répliquée

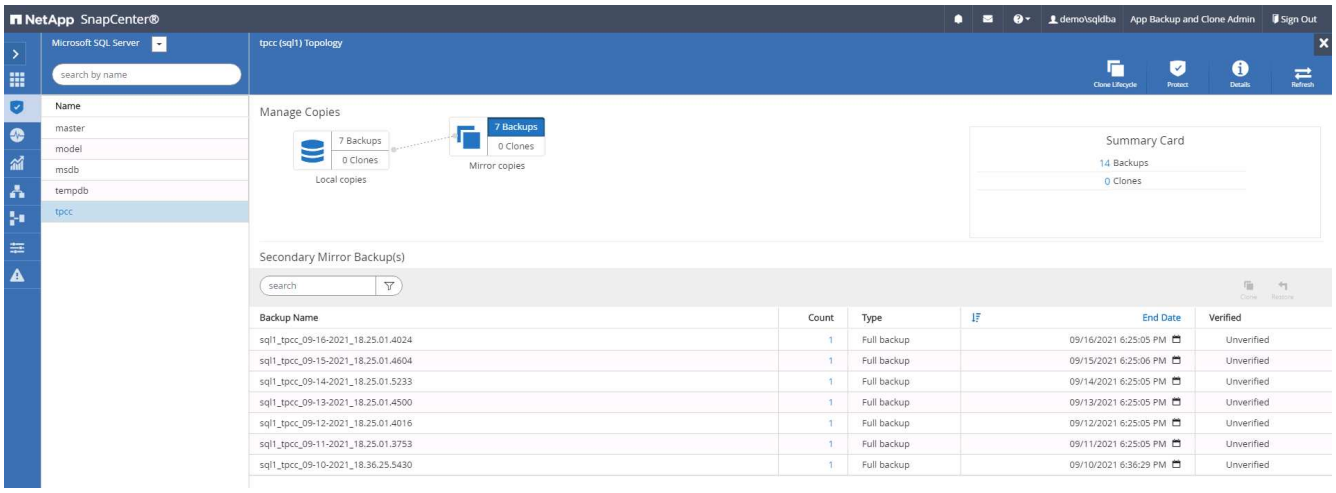
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données pour SQL Server. Accédez à l'onglet Ressources, qui affiche les bases de données utilisateur SQL Server protégées par SnapCenter et une instance SQL de secours cible dans le cloud public.



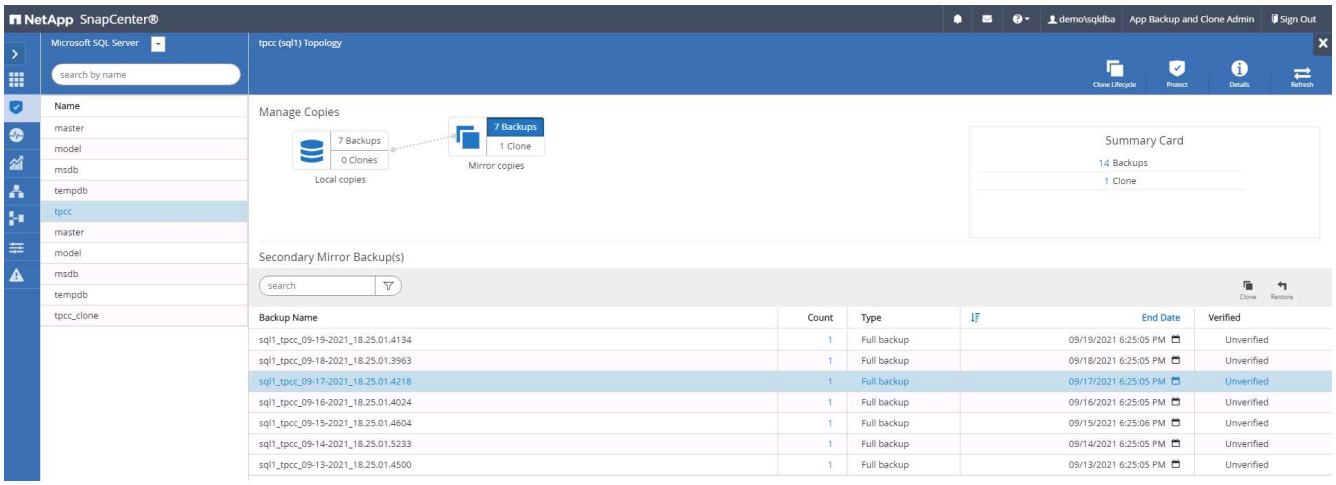
2. Cliquez sur le nom de base de données utilisateur SQL Server sur site prévu pour la topologie des sauvegardes et la vue détaillée. Si un emplacement répliqué secondaire est activé, les sauvegardes miroir liées s'affichent.

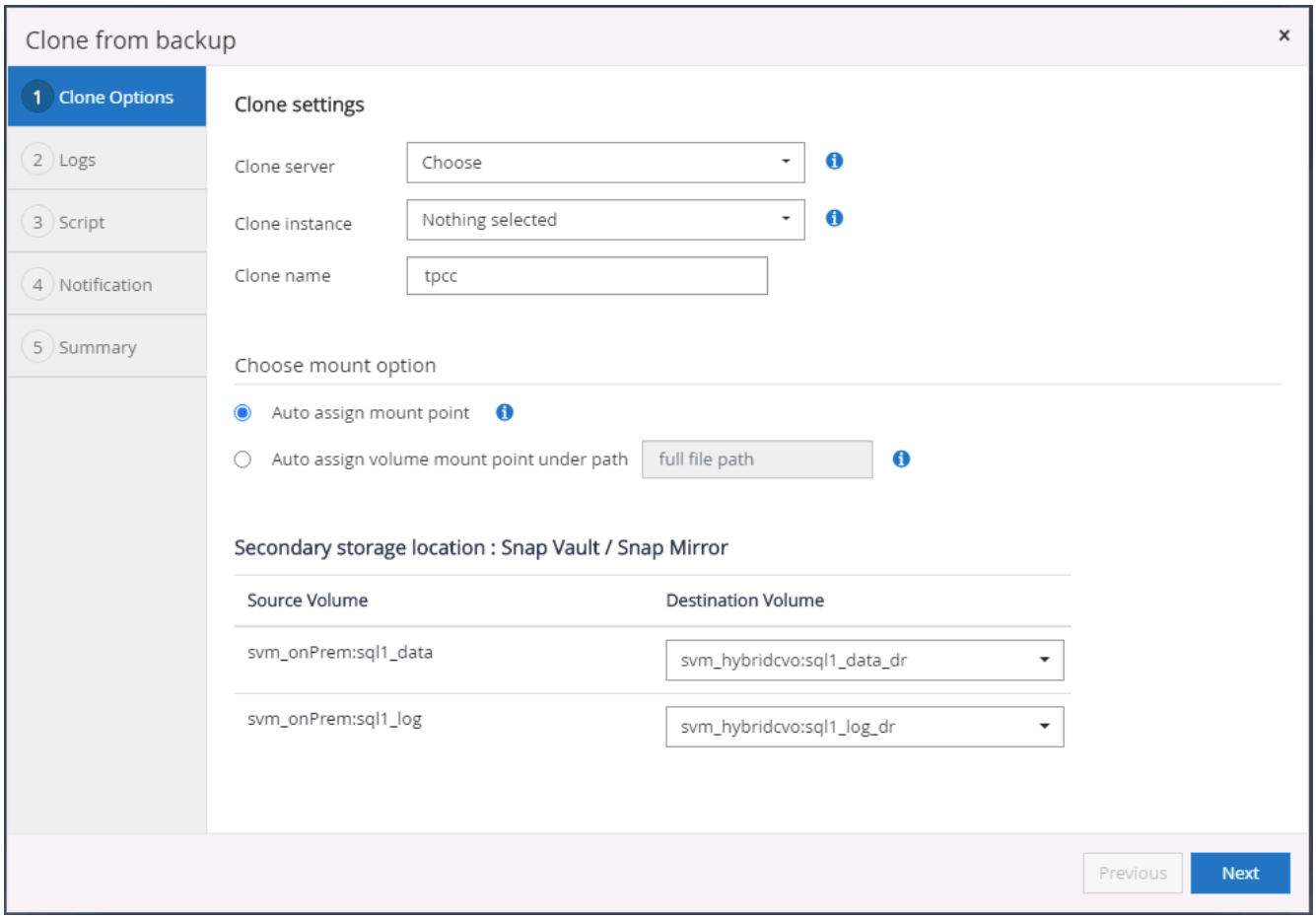


3. Basculer vers la vue sauvegardes mises en miroir en cliquant sur sauvegardes mises en miroir. Les sauvegardes de miroir secondaire sont alors affichées. Étant donné que SnapCenter sauvegarde le journal de transactions SQL Server sur un disque dédié à la restauration, seules les sauvegardes complètes de la base de données sont affichées ici.

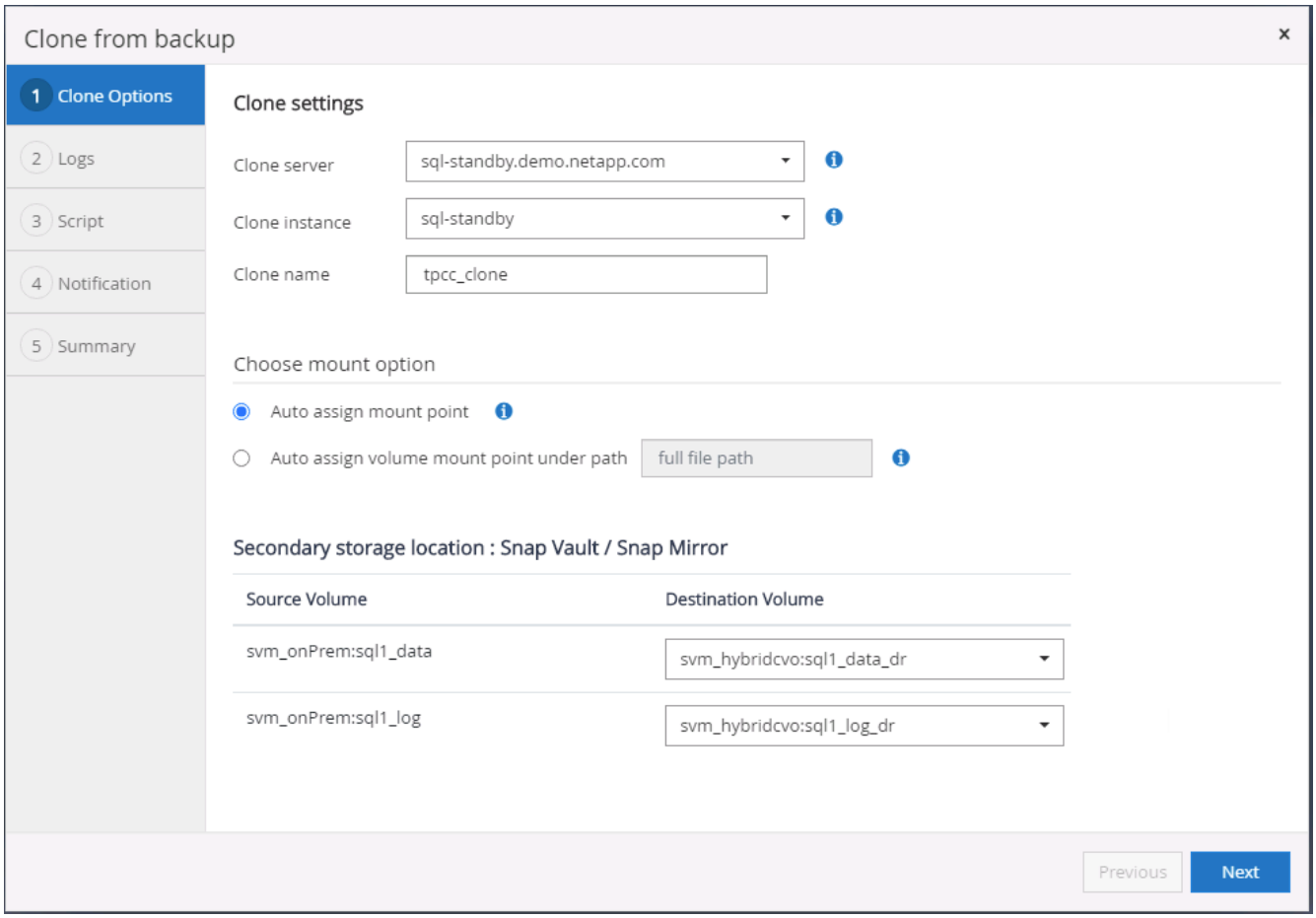


4. Choisissez une copie de sauvegarde, puis cliquez sur le bouton Cloner pour lancer le flux de travail Cloner à partir de la sauvegarde.

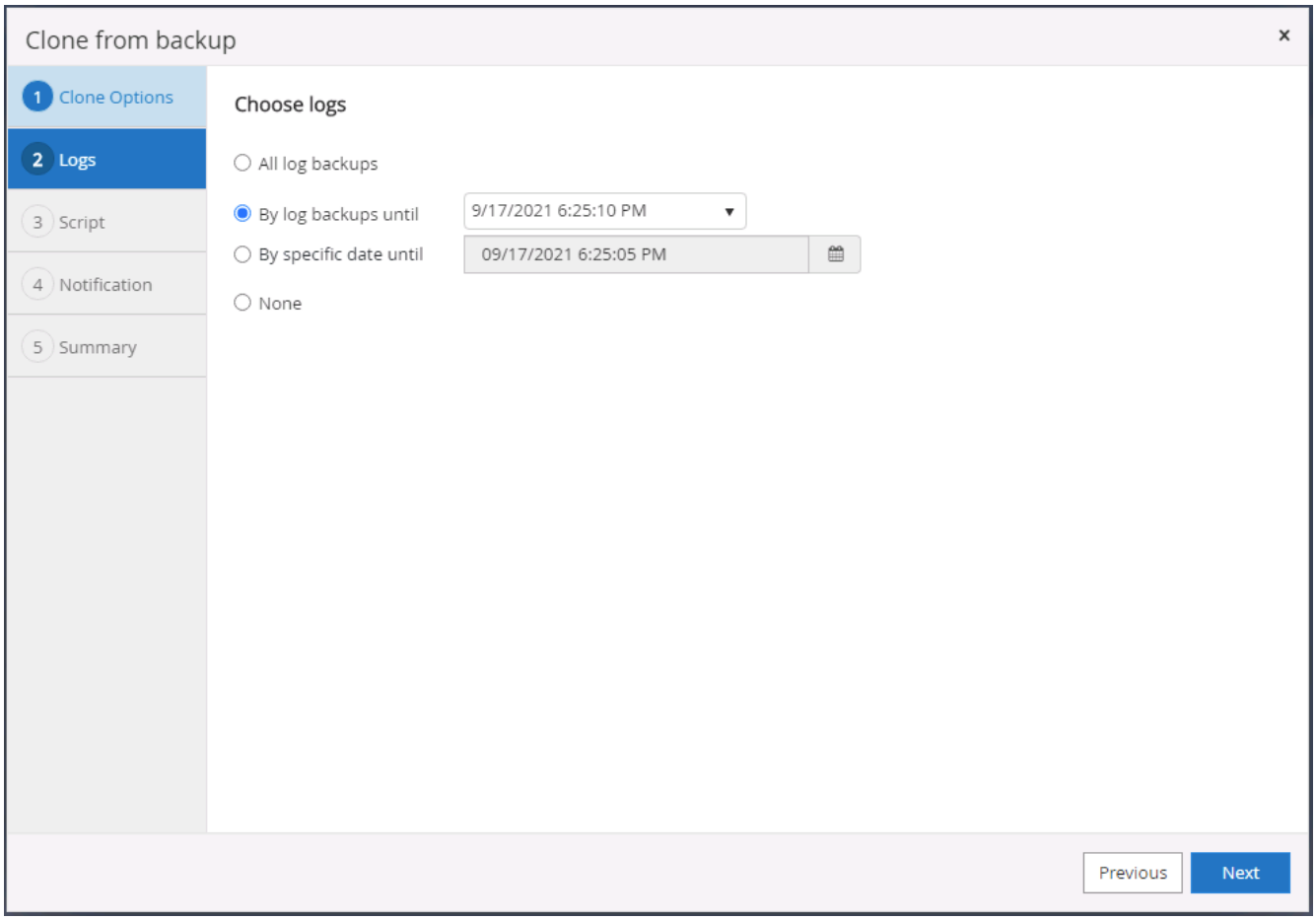




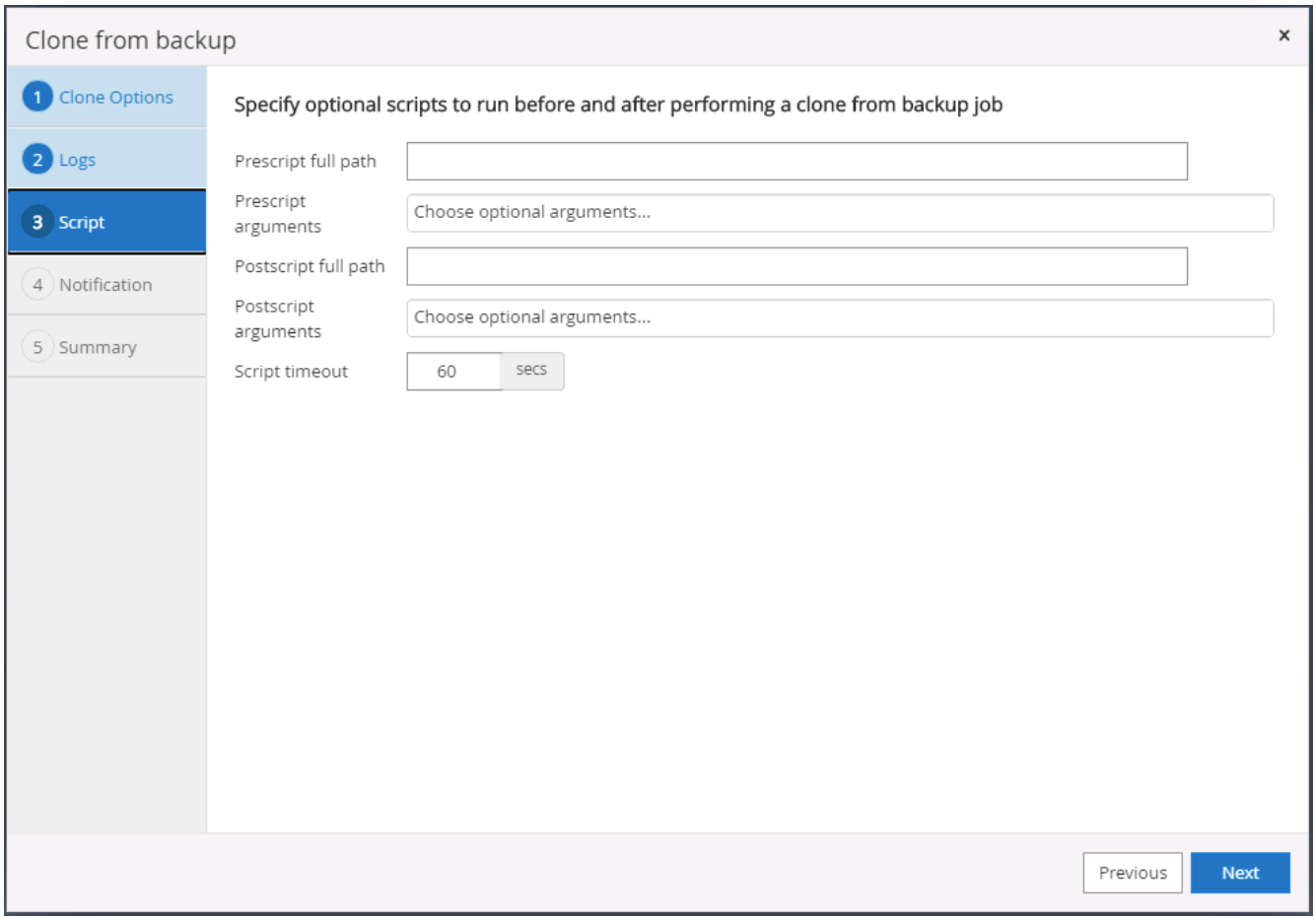
5. Sélectionnez un serveur cloud comme serveur de clonage cible, nom d'instance de clone et nom de base de données clone. Choisissez un point de montage à affectation automatique ou un chemin de point de montage défini par l'utilisateur.



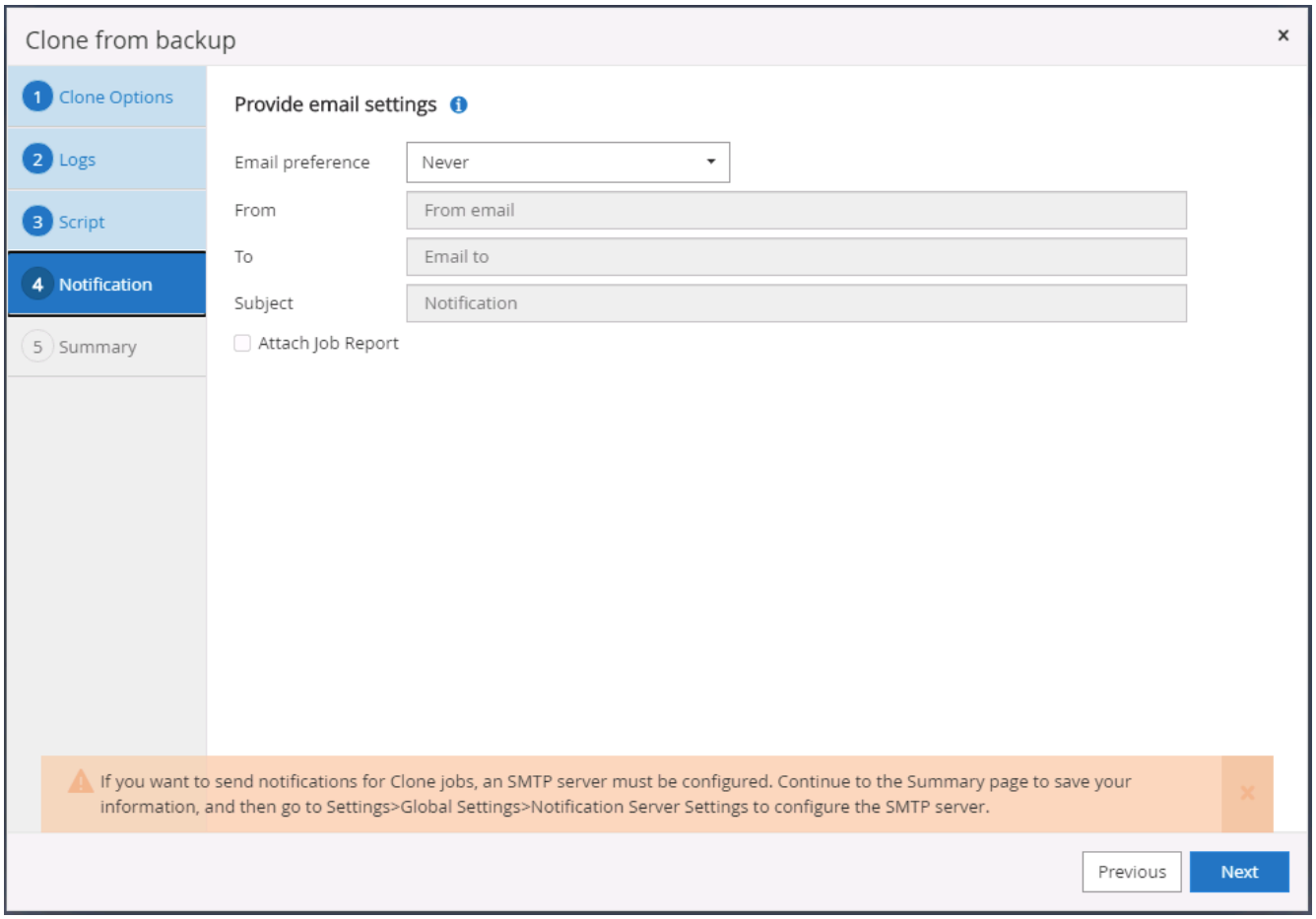
6. Déterminez un point de restauration par heure de sauvegarde du journal ou par date et heure spécifiques.



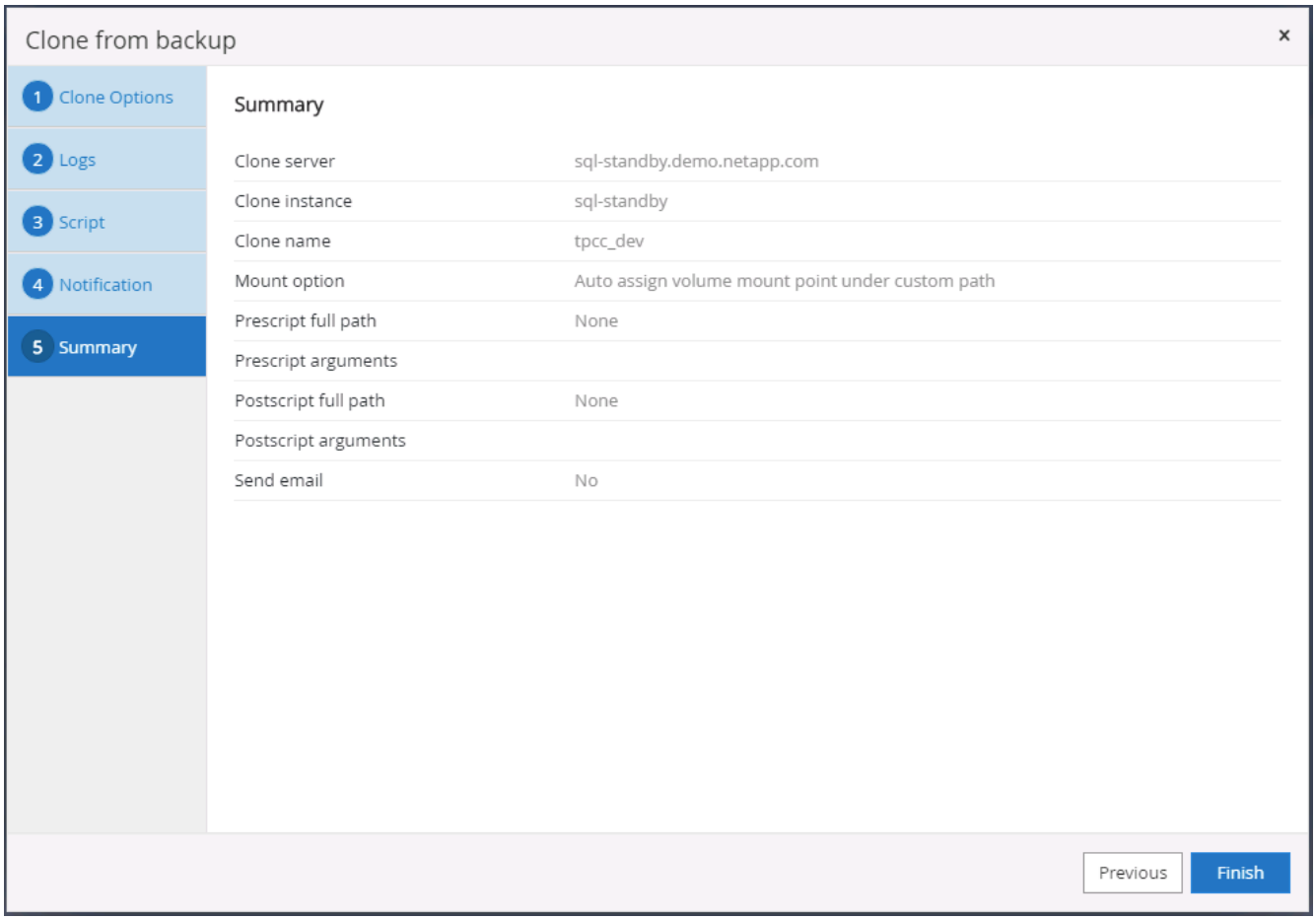
7. Spécifiez les scripts facultatifs à exécuter avant et après l'opération de clonage.



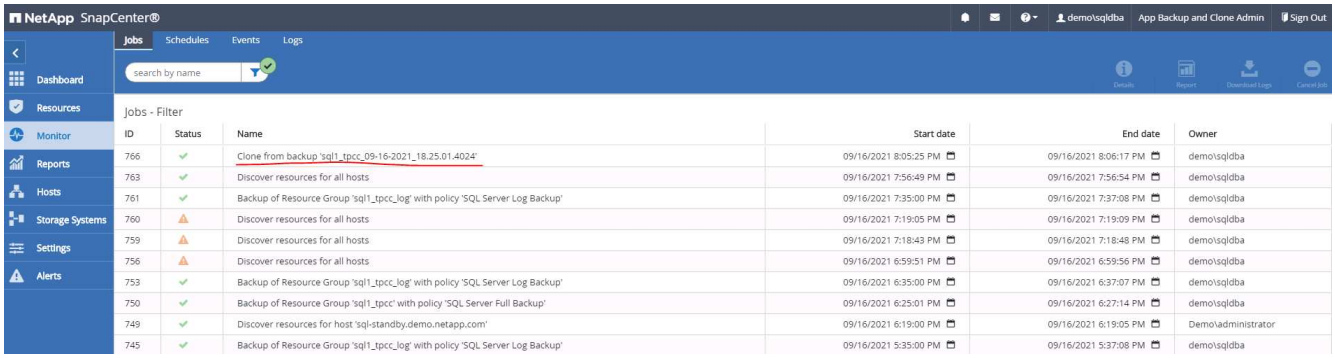
8. Configurez un serveur SMTP si vous souhaitez recevoir une notification par e-mail.



9. Synthèse des clones.



10. Surveillez l'état du travail et vérifiez que la base de données utilisateur prévue a été associée à une instance SQL cible dans le serveur clone du cloud.



Configuration post-clonage

1. Une base de données de production Oracle sur site est généralement exécutée en mode d'archivage des journaux. Ce mode n'est pas nécessaire pour une base de données de développement ou de test. Pour désactiver le mode d'archivage des journaux, connectez-vous à la base de données Oracle sous sysdba, exécutez une commande de changement du mode de journalisation et démarrez la base de données pour accéder à.
2. Configurez un écouteur Oracle ou enregistrez la base de données nouvellement clonée avec un écouteur existant pour accéder à l'utilisateur.
3. Pour SQL Server, passez du mode de journal complet à facile afin que le fichier journal de développement/test SQL Server puisse être facilement réduit lorsqu'il remplit le volume de journal.

Actualiser la base de données de clonage

1. Déposez les bases de données clonées et nettoyez l'environnement de serveur Cloud DB. Suivez ensuite les procédures précédentes pour cloner une nouvelle base de données avec des données récentes. Le clonage d'une nouvelle base de données ne prend que quelques minutes.
2. Arrêtez la base de données clone, exécutez une commande de mise à jour du clone à l'aide de l'interface de ligne de commandes. Pour plus d'informations, consultez la documentation SnapCenter suivante : "Actualiser un clone".

Où obtenir de l'aide ?

Si vous avez besoin d'aide pour utiliser cette solution, rejoignez la "La communauté NetApp solution Automation prend en charge le Channel Slack" et recherchez le canal solution-automation pour poser vos questions ou vos questions.

Flux de travail de reprise après incident

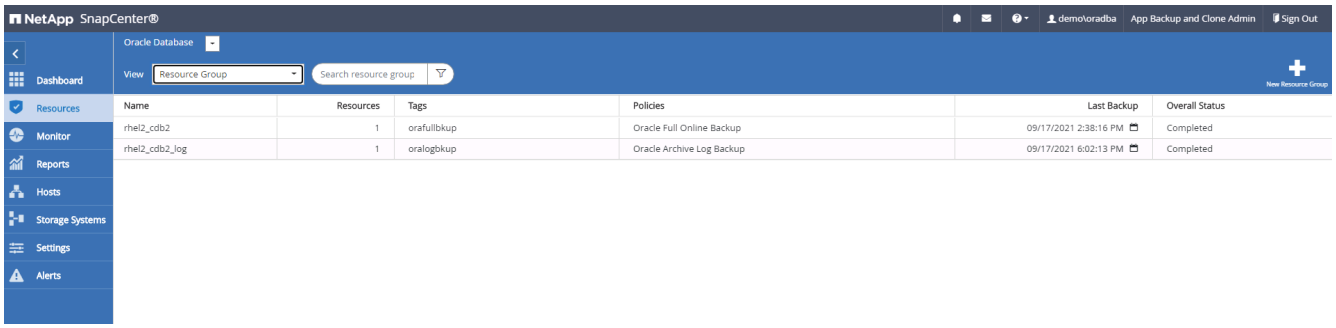
Les entreprises ont adopté le cloud public comme ressource et destination viables pour la reprise après incident. SnapCenter rend ce processus aussi transparent que possible. Ce workflow de reprise d'activité est très similaire au workflow de clonage, mais la restauration de base de données s'exécute via le dernier journal disponible répliqué dans le cloud afin de restaurer toutes les transactions d'entreprise possibles. Toutefois, des étapes supplémentaires de préconfiguration et de post-configuration sont propres à la reprise sur incident.

Clonez une base de données de production Oracle sur site dans le cloud pour la reprise après incident

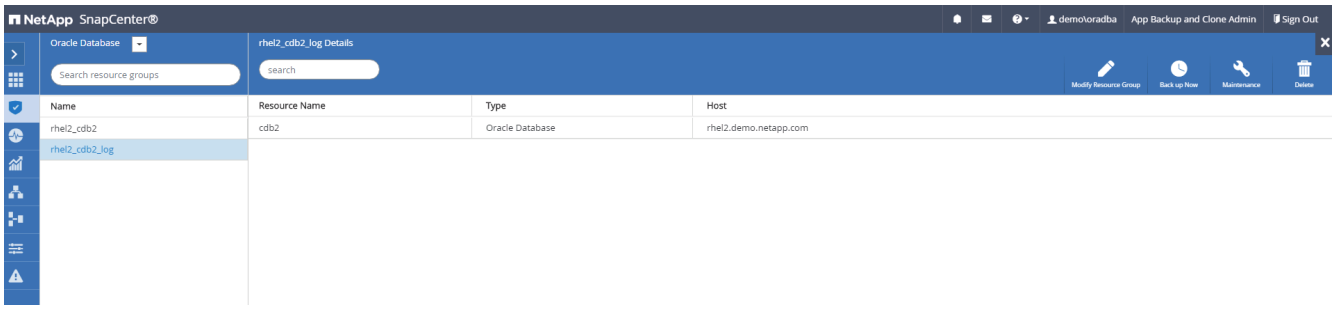
1. Pour vérifier que la restauration des clones s'exécute via le dernier journal disponible, nous avons créé une petite table de test et inséré une ligne. Les données de test seront récupérées après une récupération complète du dernier journal disponible.

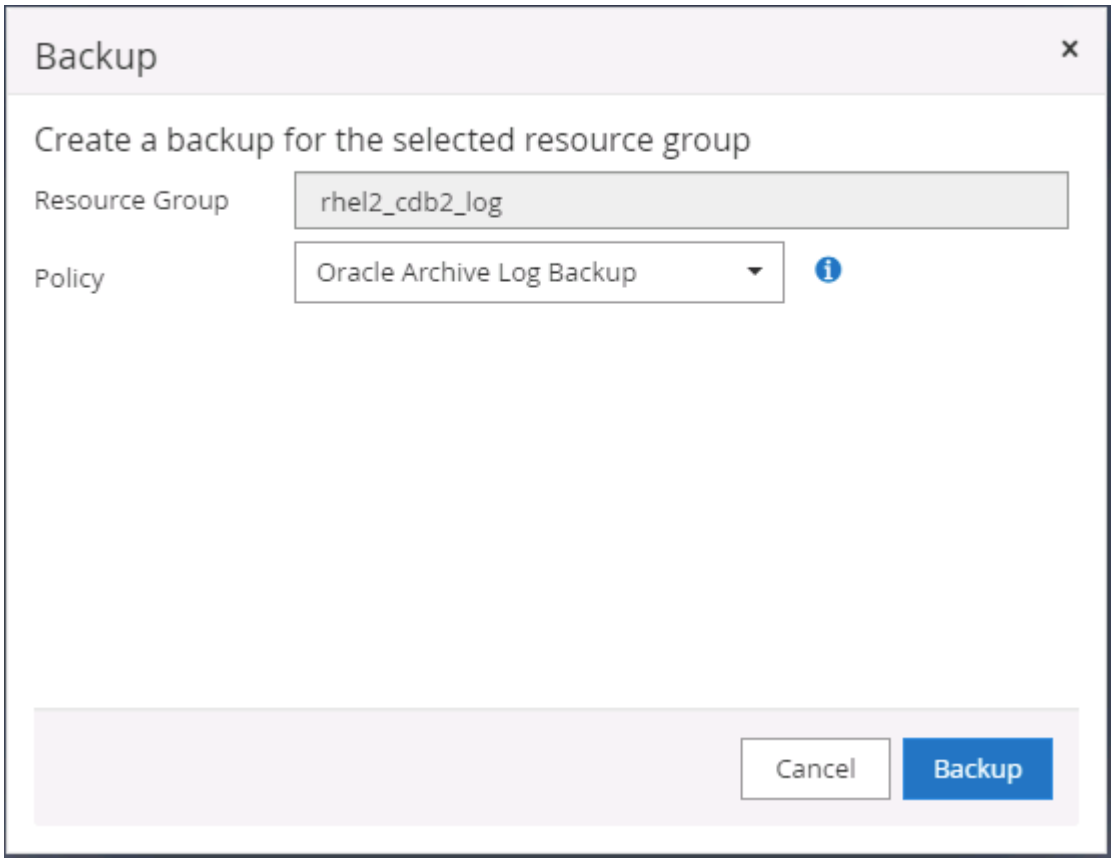
```
oracle@rhel2:~
SQL> create table dr_test(
  2  id integer,
  3  event varchar(200),
  4  dt timestamp);

Table created.

SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);

1 row created.

SQL> select * from dr_test;

        ID
----------
EVENT
--------------------------------------------------------------------------------
DT
---------------------------------------------------------------------------
         1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM


SQL> commit;

Commit complete.

SQL>
```

2. Connectez-vous à SnapCenter en tant qu'ID utilisateur de gestion de base de données pour Oracle. Accédez à l'onglet Ressources, qui affiche les bases de données Oracle protégées par SnapCenter.



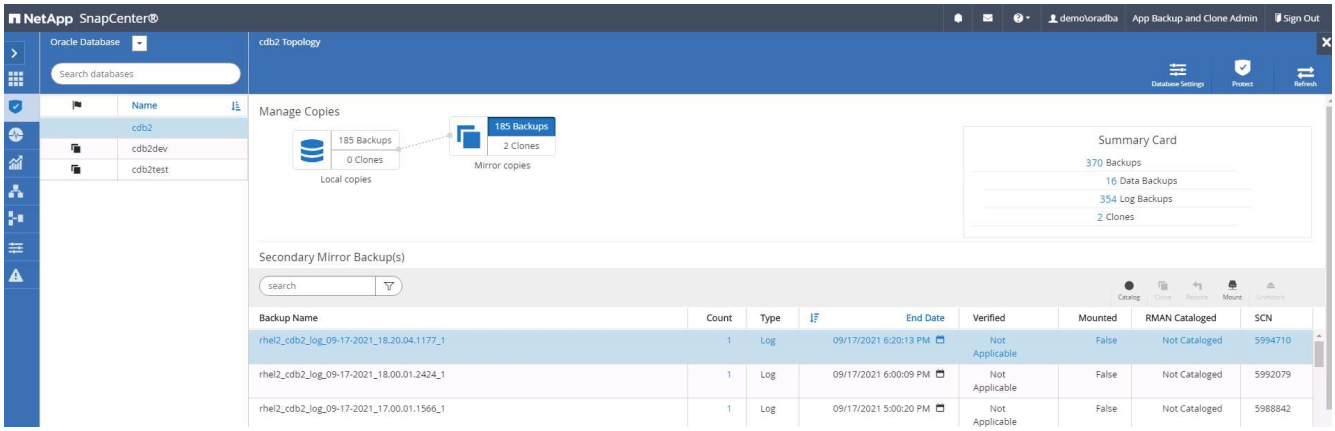
3. Sélectionnez le groupe de ressources du journal Oracle et cliquez sur Sauvegarder maintenant pour exécuter manuellement une sauvegarde du journal Oracle afin de vider la dernière transaction vers la destination dans le cloud. Dans un scénario de reprise d'activité réel, la dernière transaction récupérable dépend de la fréquence de réplication du volume des journaux de base de données vers le cloud, qui dépend à son tour de la politique RTO ou RPO de l'entreprise.

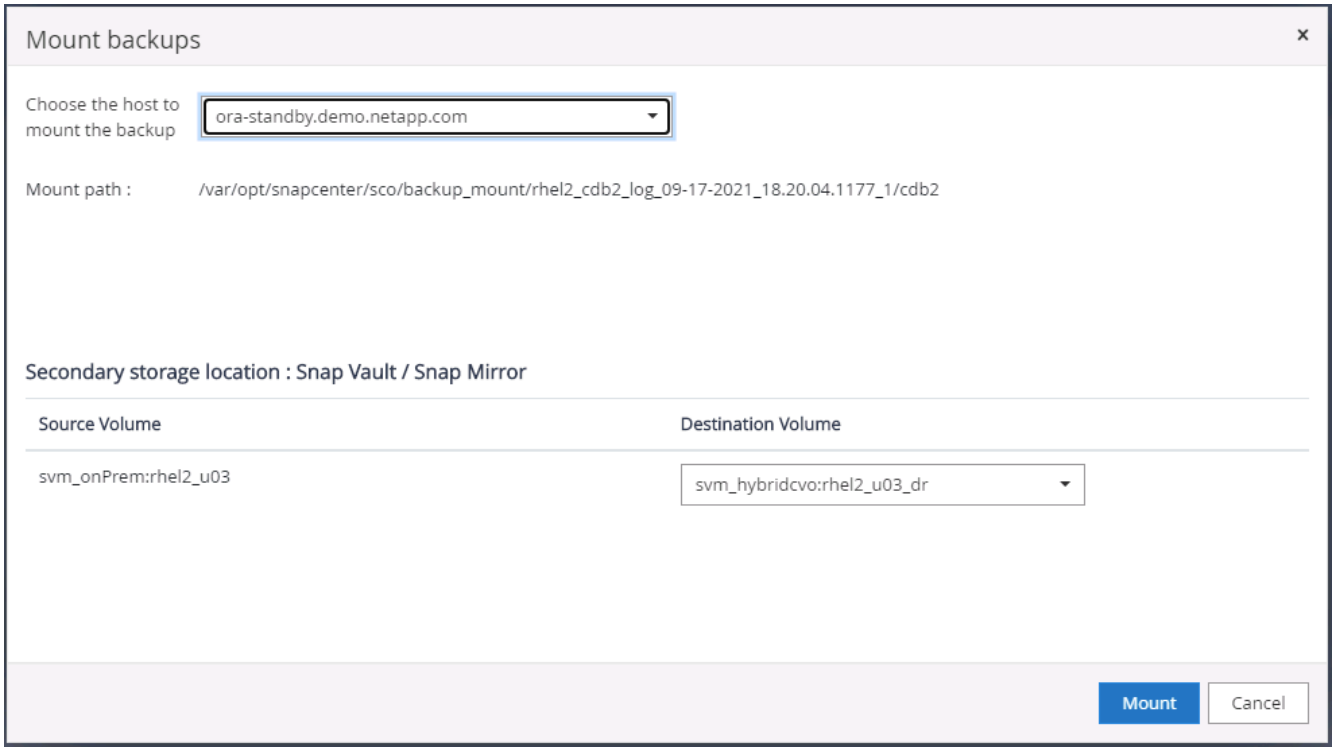




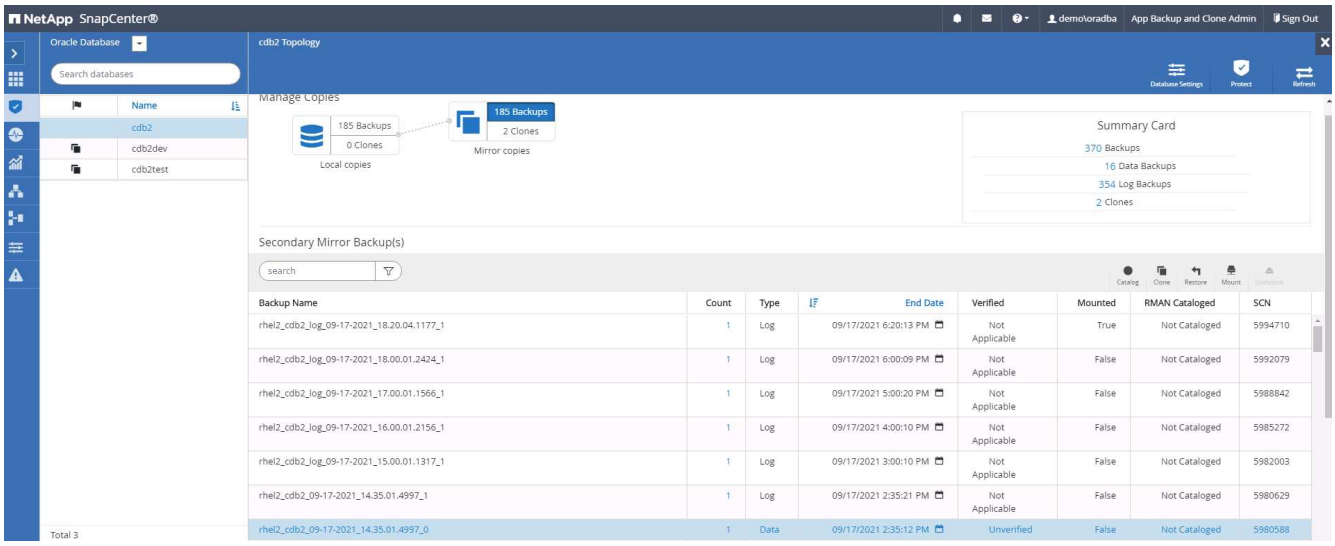
En cas de reprise d'activité, SnapMirror asynchrone perd les données qui n'ont pas été effectuées vers la destination cloud dans l'intervalle de sauvegarde du journal de base de données. Il est possible de programmer des sauvegardes plus fréquentes des journaux pour limiter les pertes de données. Cependant, la fréquence de sauvegarde des journaux est limitée, techniquement réalisable.

4. Sélectionnez la dernière sauvegarde du journal sur la ou les sauvegarde(s) miroir secondaire et montez la sauvegarde du journal.

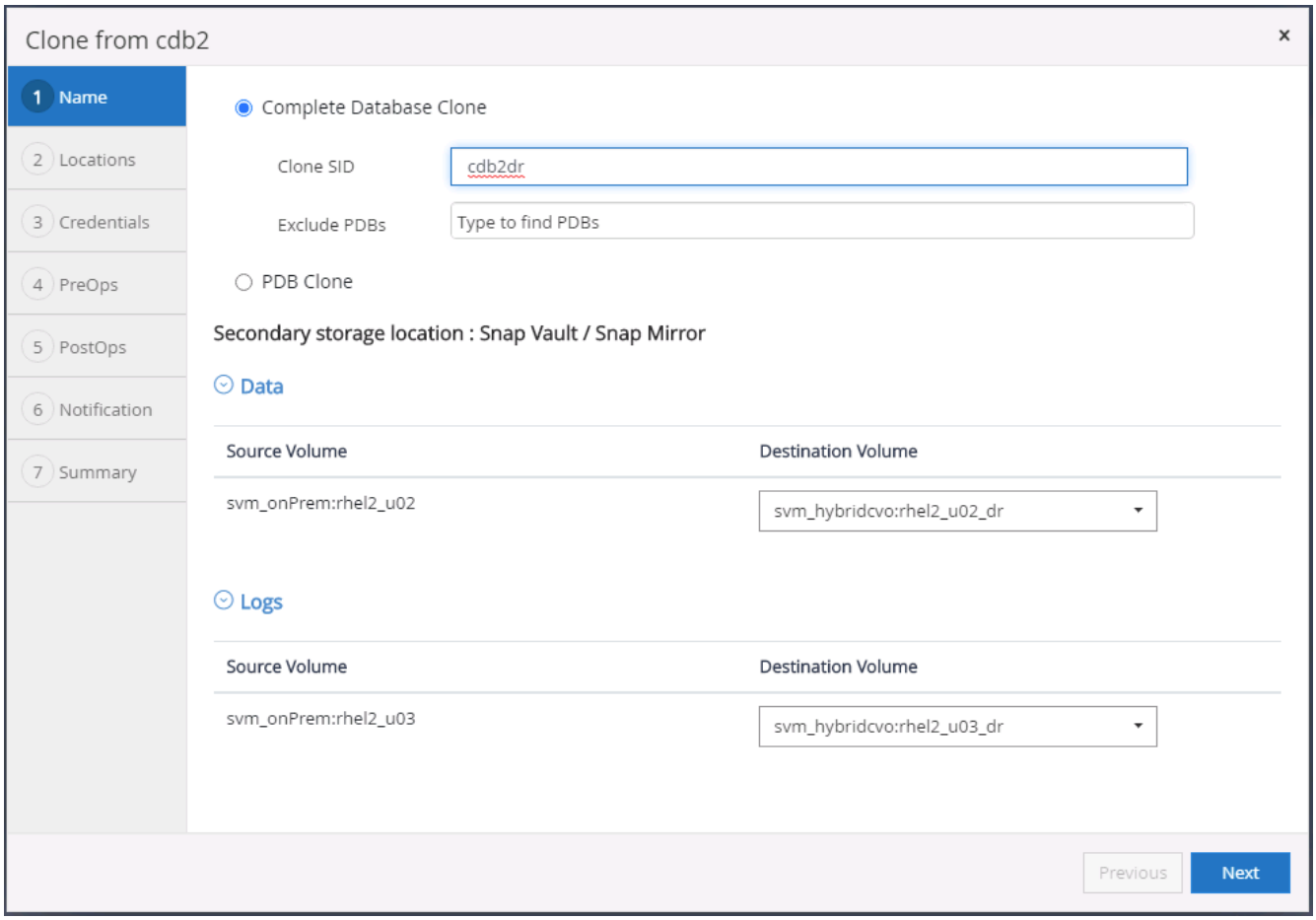




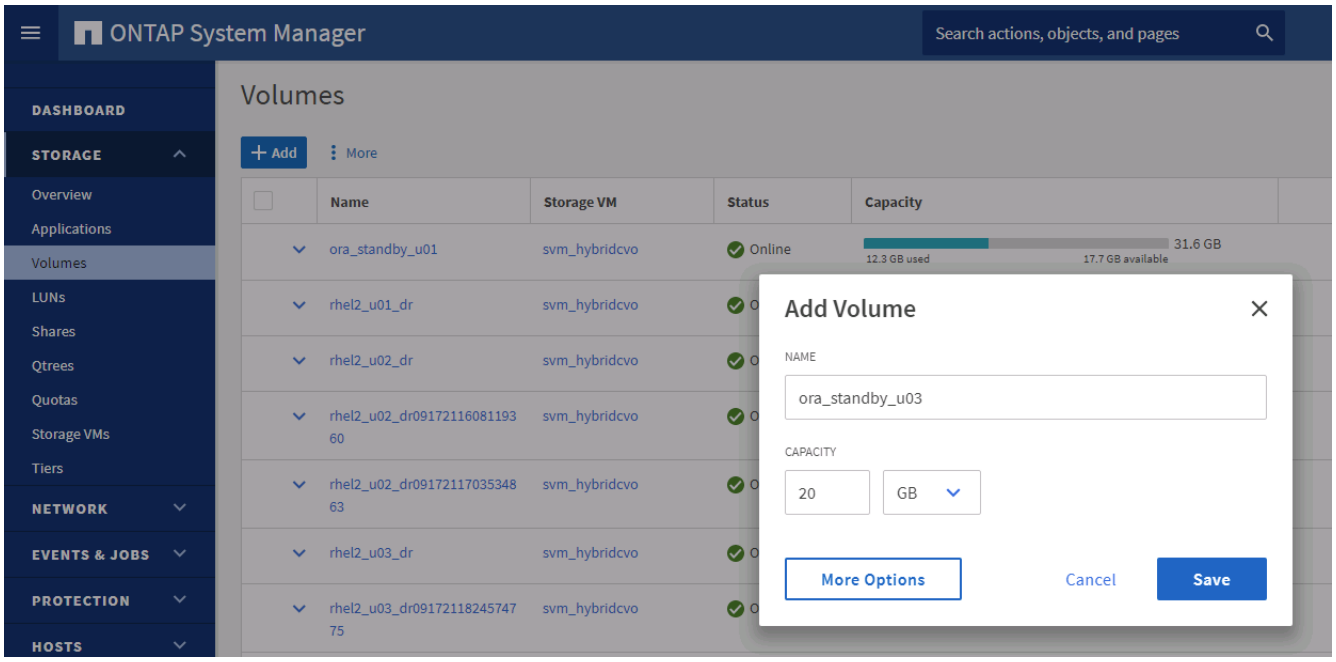
5. Sélectionnez la dernière sauvegarde complète de la base de données et cliquez sur Cloner pour lancer le flux de travail de clonage.

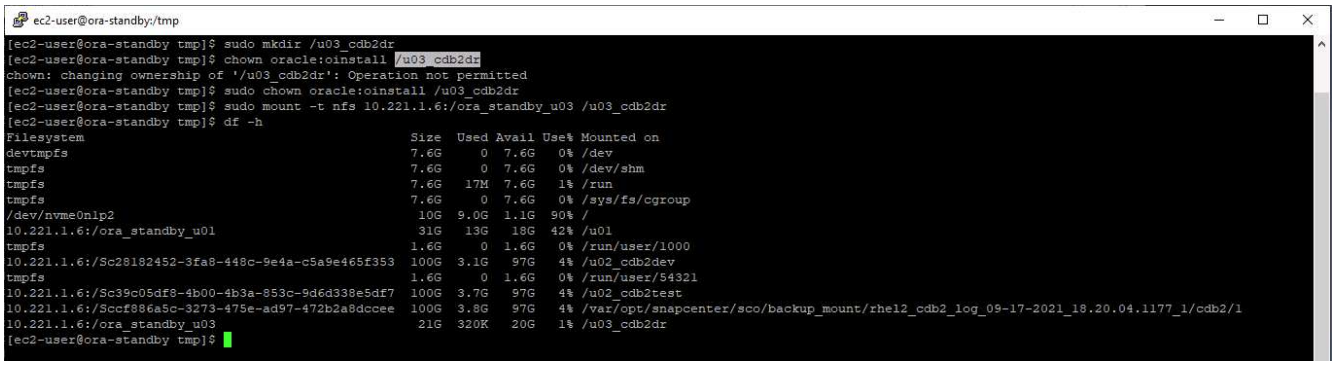


6. Sélectionnez un ID unique de base de données de clone sur l'hôte.



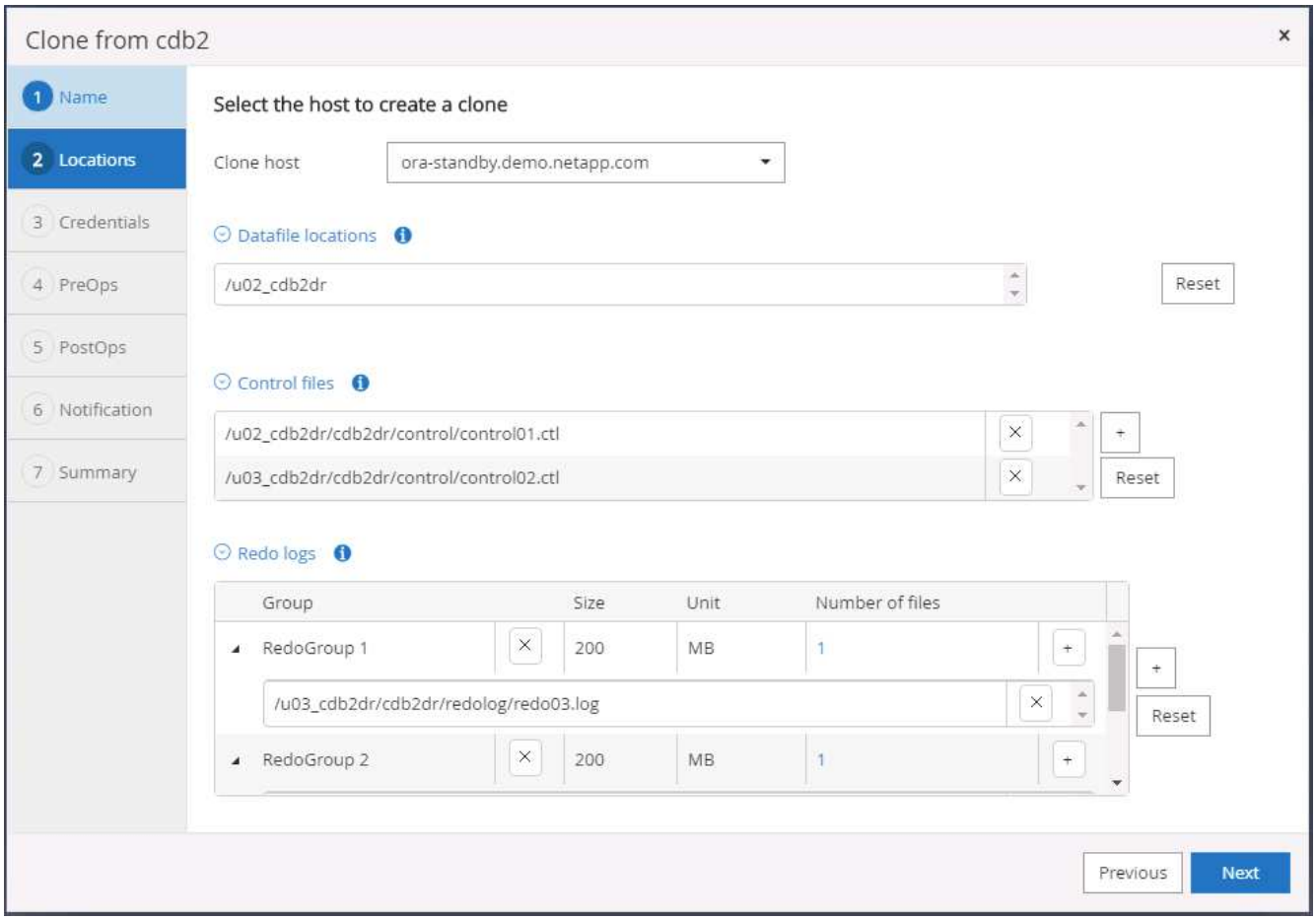
7. Provisionnez un volume de journalisation et montez-le sur le serveur de reprise après incident cible pour la zone de restauration Flash Oracle et les journaux en ligne.



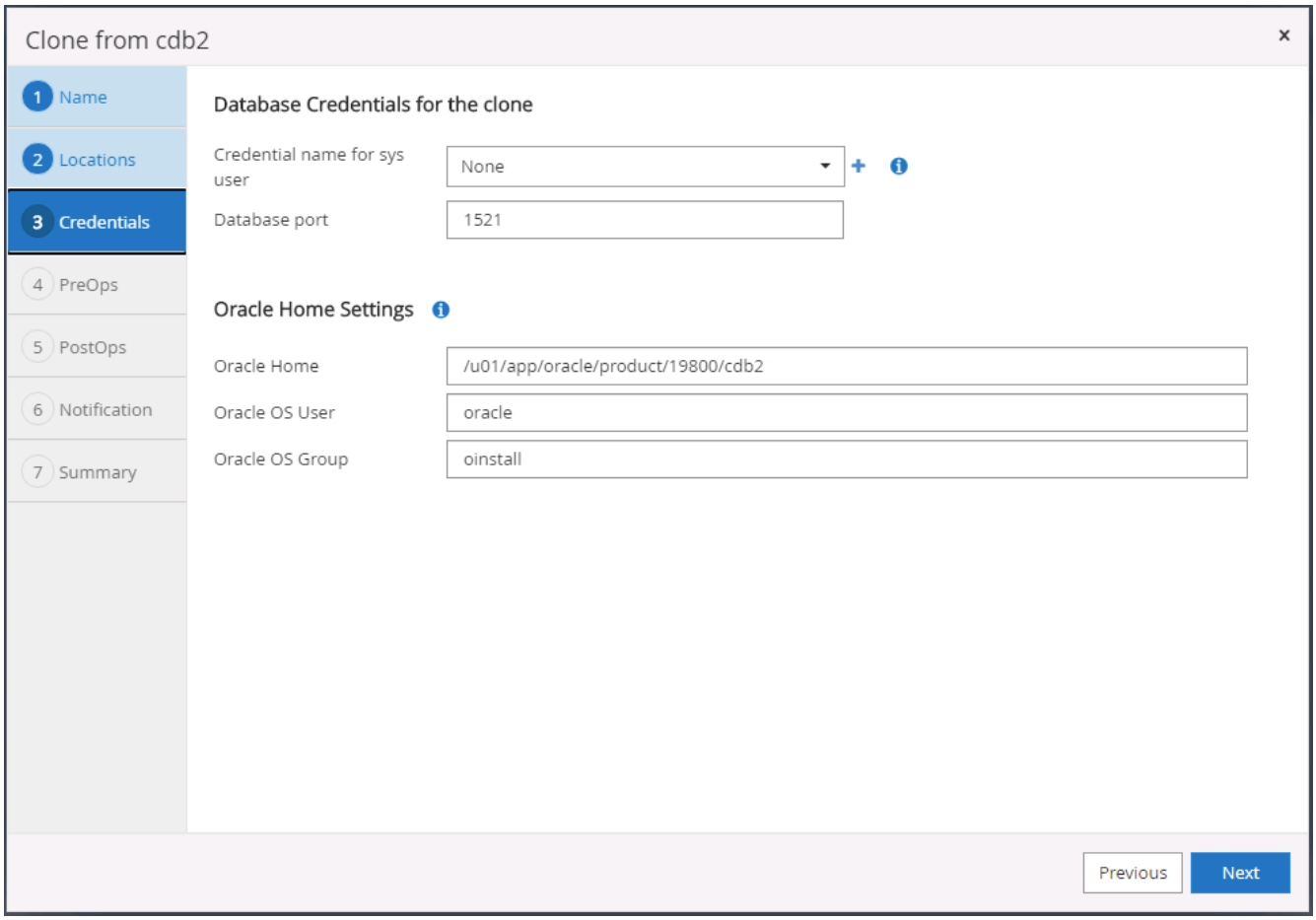


> La procédure de clonage Oracle ne crée pas de volume de journaux qui doit être provisionné sur le serveur de reprise après incident avant le clonage.

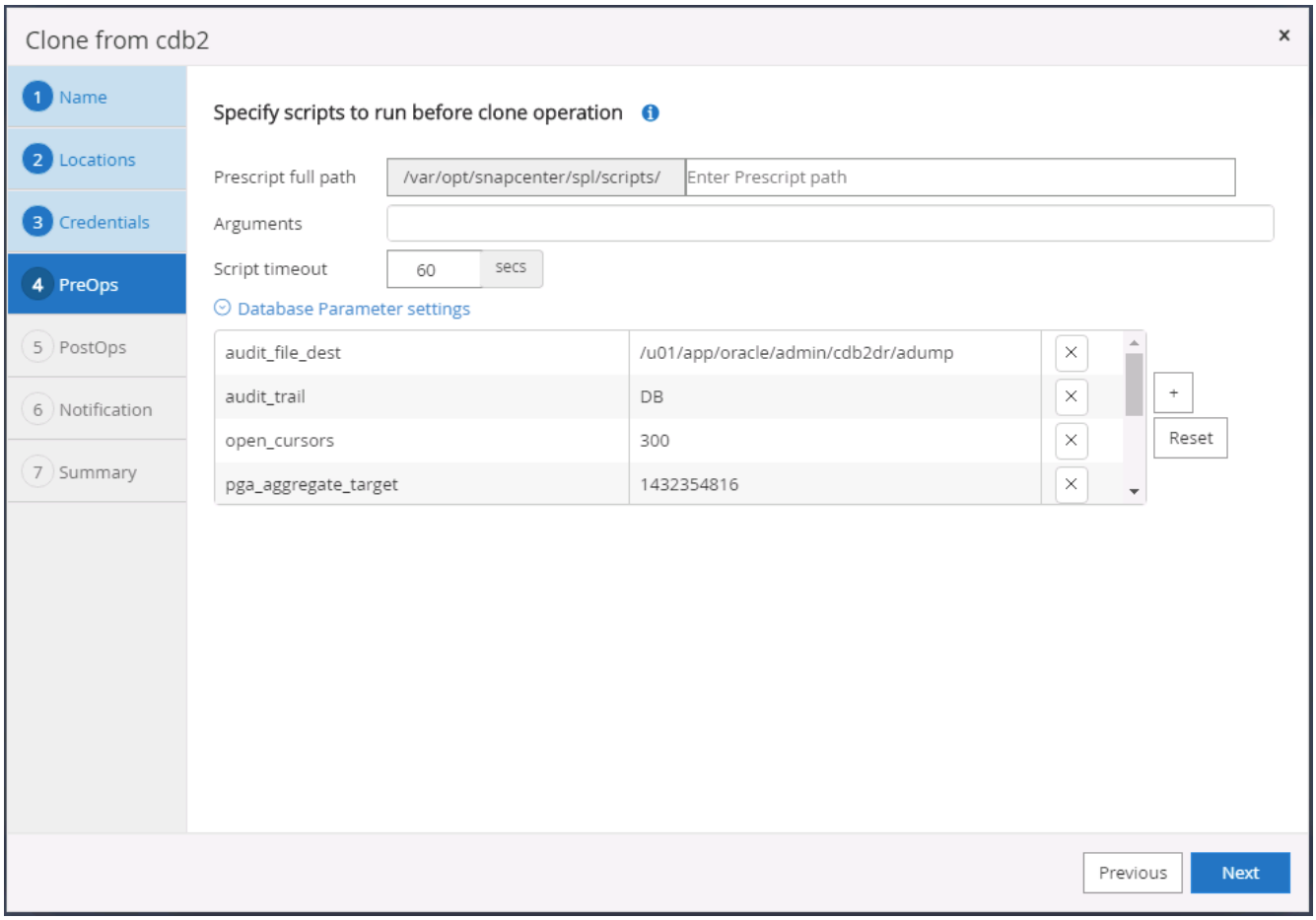
8. Sélectionnez l'hôte et l'emplacement du clone cible pour placer les fichiers de données, les fichiers de contrôle et les journaux de reprise.



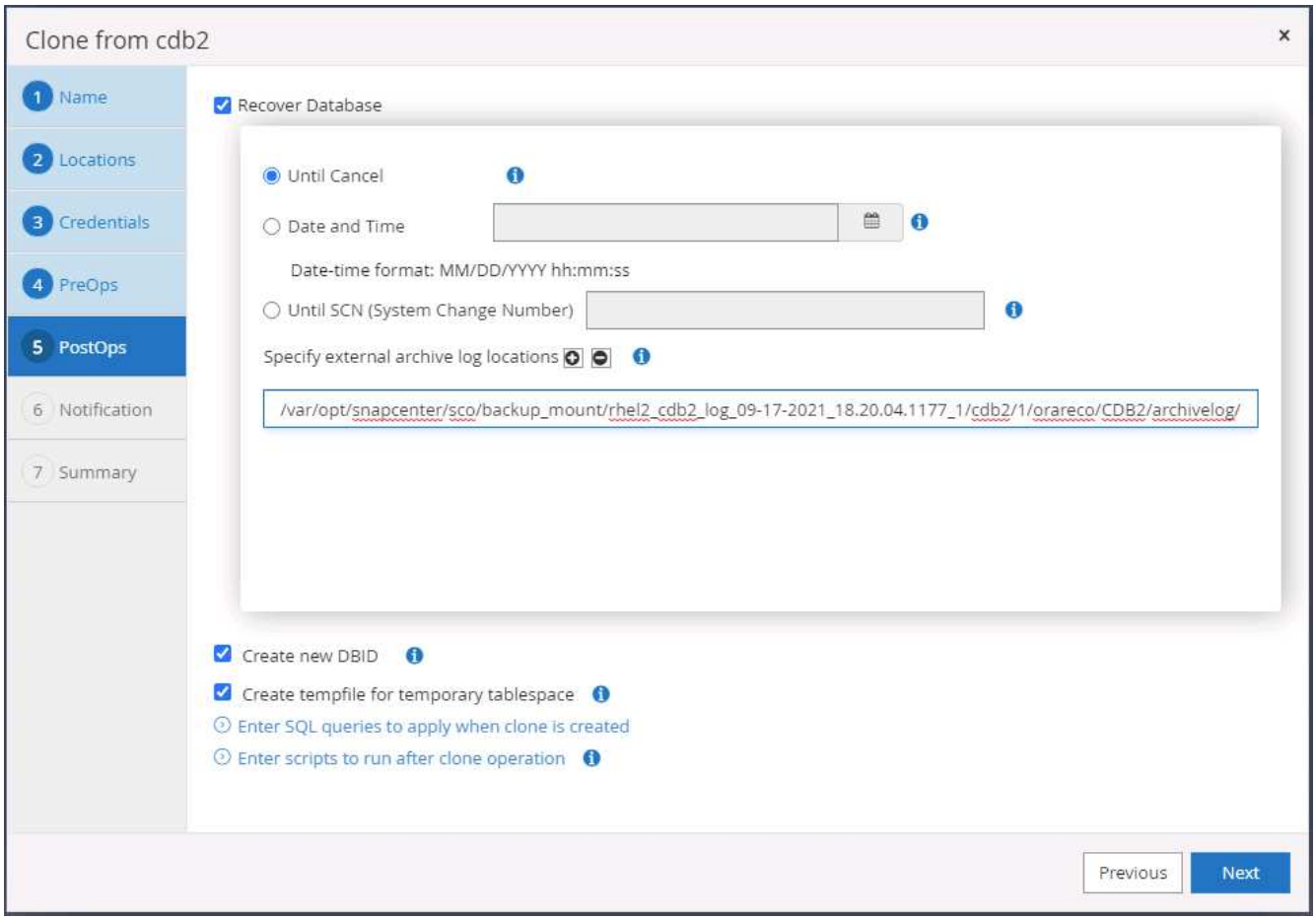
9. Sélectionnez les informations d'identification du clone. Renseignez les détails de la configuration initiale d'Oracle sur le serveur cible.



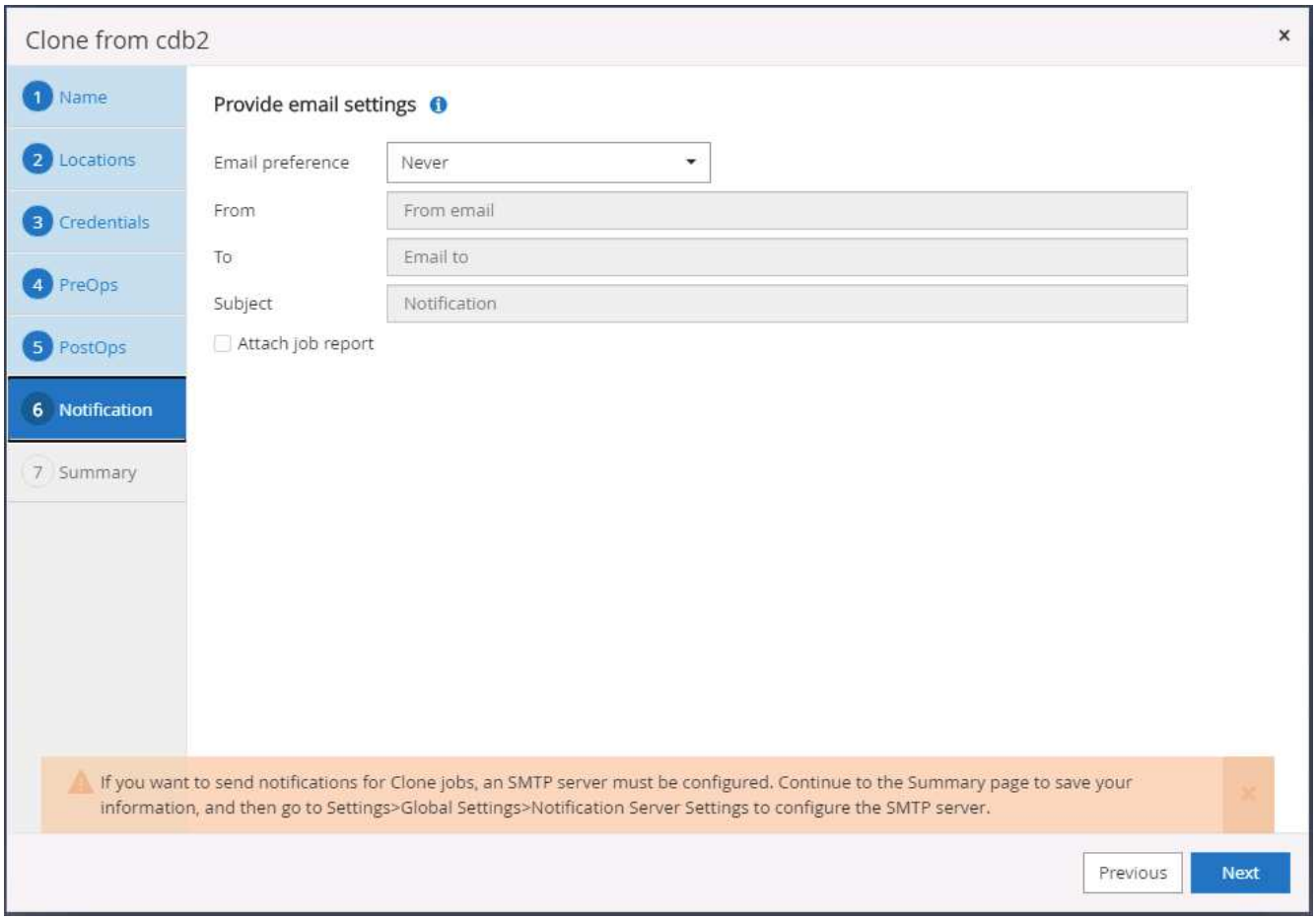
10. Spécifiez les scripts à exécuter avant le clonage. Les paramètres de la base de données peuvent être ajustés si nécessaire.



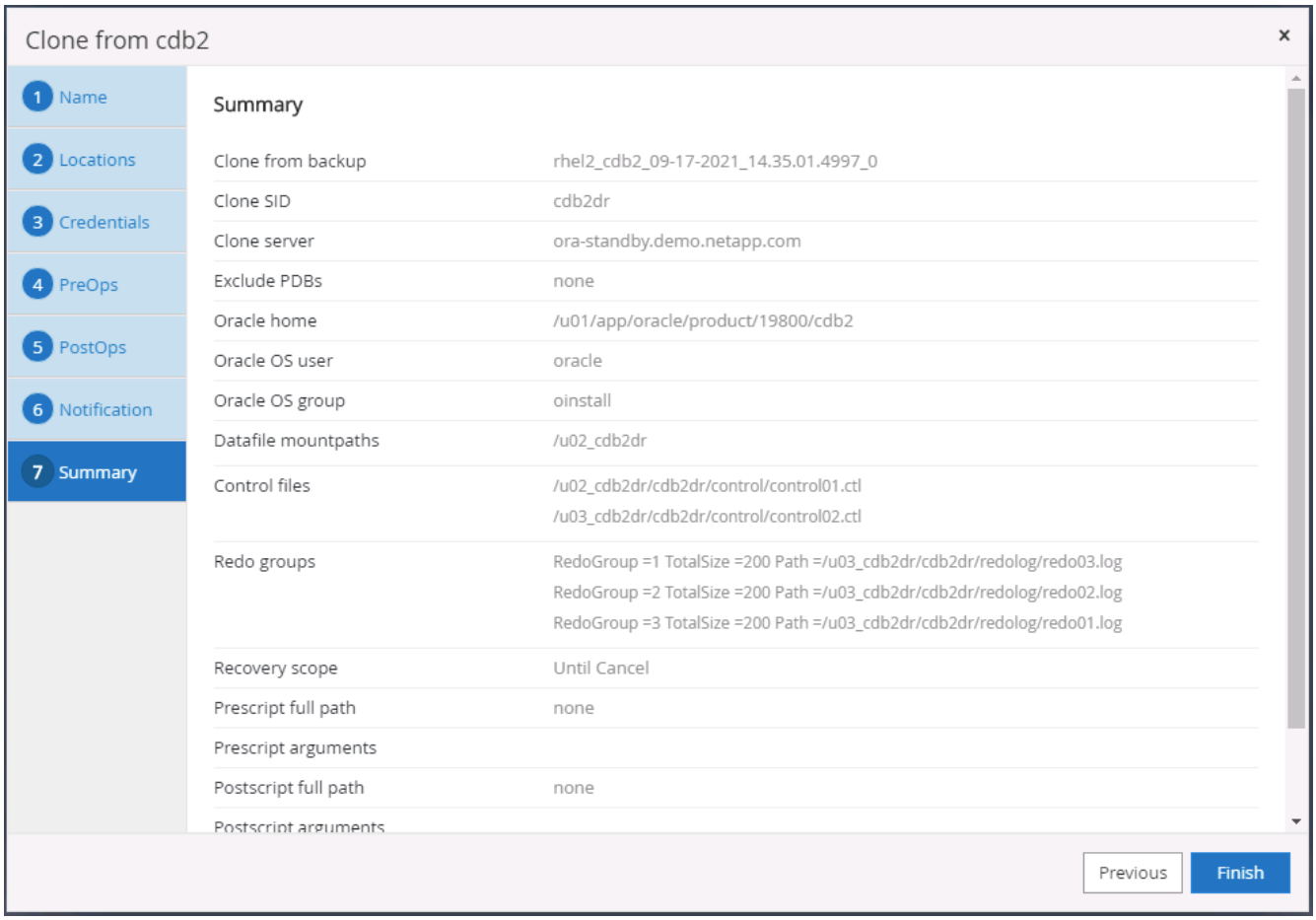
11. Sélectionnez jusqu'à Annuler comme option de restauration pour que la restauration s'exécute dans tous les journaux d'archivage disponibles pour récupérer la dernière transaction répliquée vers l'emplacement du cloud secondaire.



12. Configurez le serveur SMTP pour la notification par e-mail si nécessaire.



13. Récapitulatif sur le clone de DR.



14. Les bases de données clonées sont enregistrées avec SnapCenter immédiatement après la fin du clonage, puis sont disponibles pour la protection de sauvegarde.

Validation et configuration des clones après reprise après incident pour Oracle

1. Valider la dernière transaction de test qui a été vidée, répliquée et restaurée sur le site de DR dans le cloud.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME    HOST_NAME
---------------- ----------------------------------------------------------------
cdb2dr           ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;

Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;

Session altered.

SQL> select * from pdbadmin.dr_test;

        ID
----------
EVENT
--------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------
DT
---------------------------------------------------------------------------
         1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>
```

2. Configurer la zone de récupération flash.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
[oracle@ora-standby dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
db_recovery_file_dest                string
db_recovery_file_dest_size           big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
db_recovery_file_dest                string      /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size           big integer 17208M
SQL>
```

3. Configurez le programme d'écoute Oracle pour l'accès des utilisateurs.
4. Séparer le volume cloné du volume source répliqué
5. La réplication inverse du cloud sur site, puis reconstruisez le serveur de base de données sur site en panne.

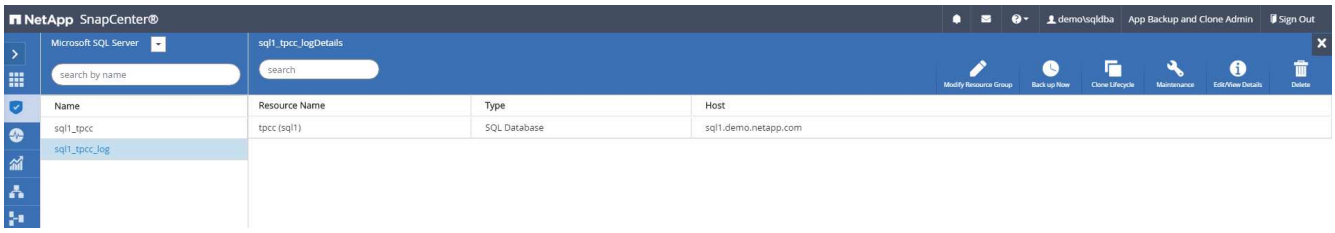
> Le fractionnement des clones peut entraîner une utilisation temporaire de l'espace de stockage qui dépasse de loin la normale. Cependant, après la reconstruction du serveur de bases de données sur site, vous pouvez libérer de l'espace supplémentaire.

Clonez une base de données de production SQL sur site dans le cloud pour la reprise après incident

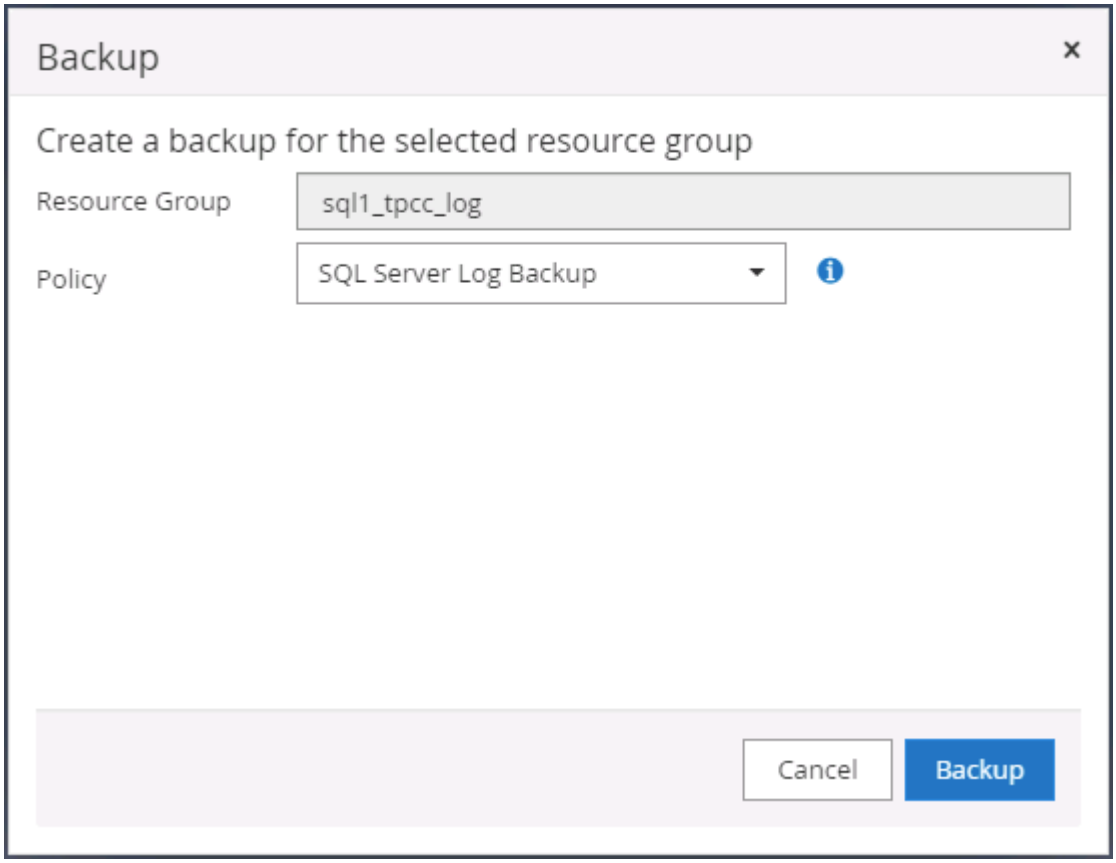
1. De la même façon, pour vérifier que la restauration des clones SQL a été exécutée par le dernier journal disponible, nous avons créé une petite table de tests et inséré une ligne. Les données de test seront récupérées après une récupération complète du dernier journal disponible.

```
Administrator: Command Prompt - sqlcmd - SQLCMD

C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

----------------------------------------------------------------------------------------------------------------------------
SQL1

(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

(1 rows affected)
1> select * from snap_sync
2> go
event                                              dt
-------------------------------------------------- -----------------------
test snap mirror DR for SQL                        2021-09-20 14:23:04.533

(1 rows affected)
1>
```

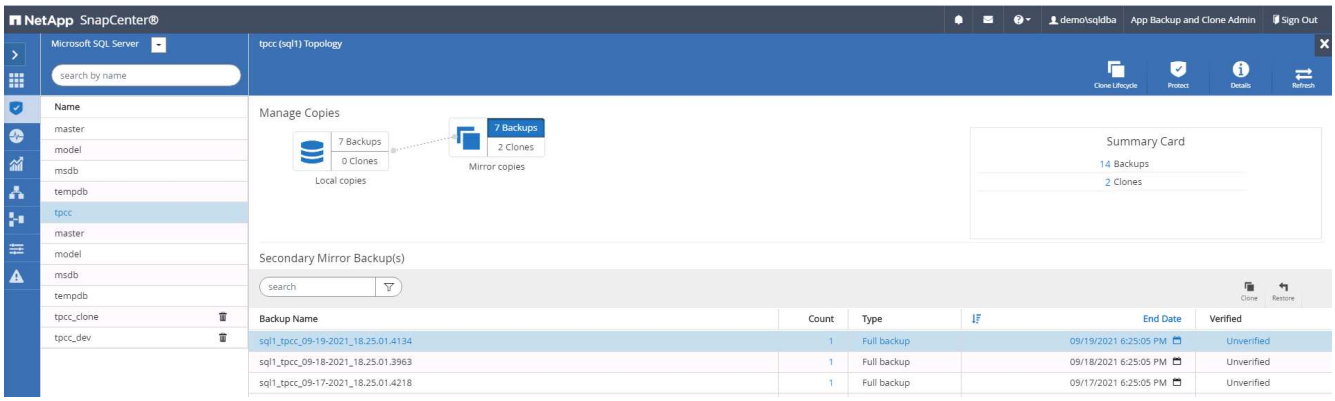
2. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données pour SQL Server. Accédez à l'onglet Ressources, qui affiche le groupe de ressources de protection SQL Server.



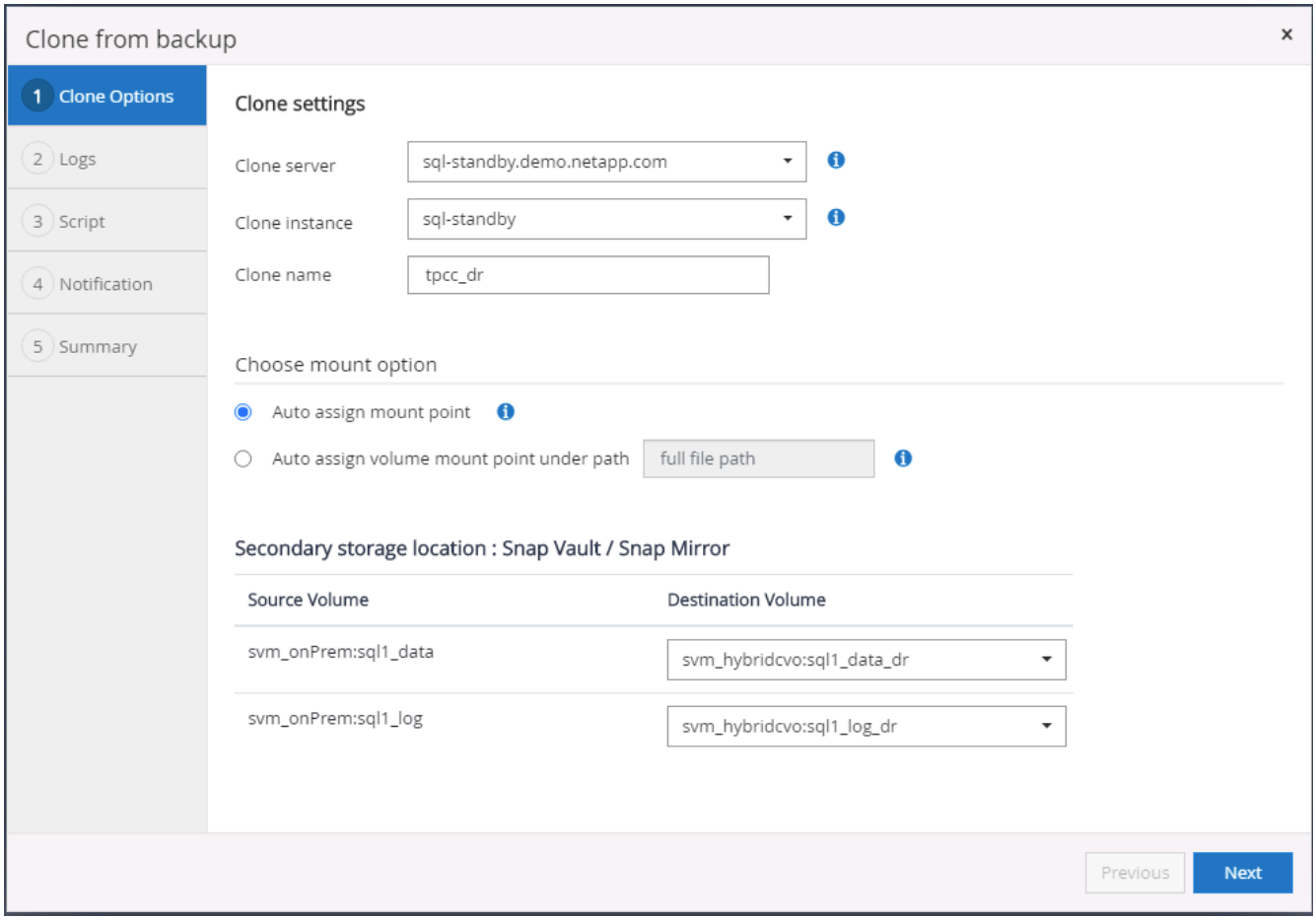
3. Exécutez manuellement une sauvegarde de journal pour vider la dernière transaction à répliquer sur un stockage secondaire dans le cloud public.



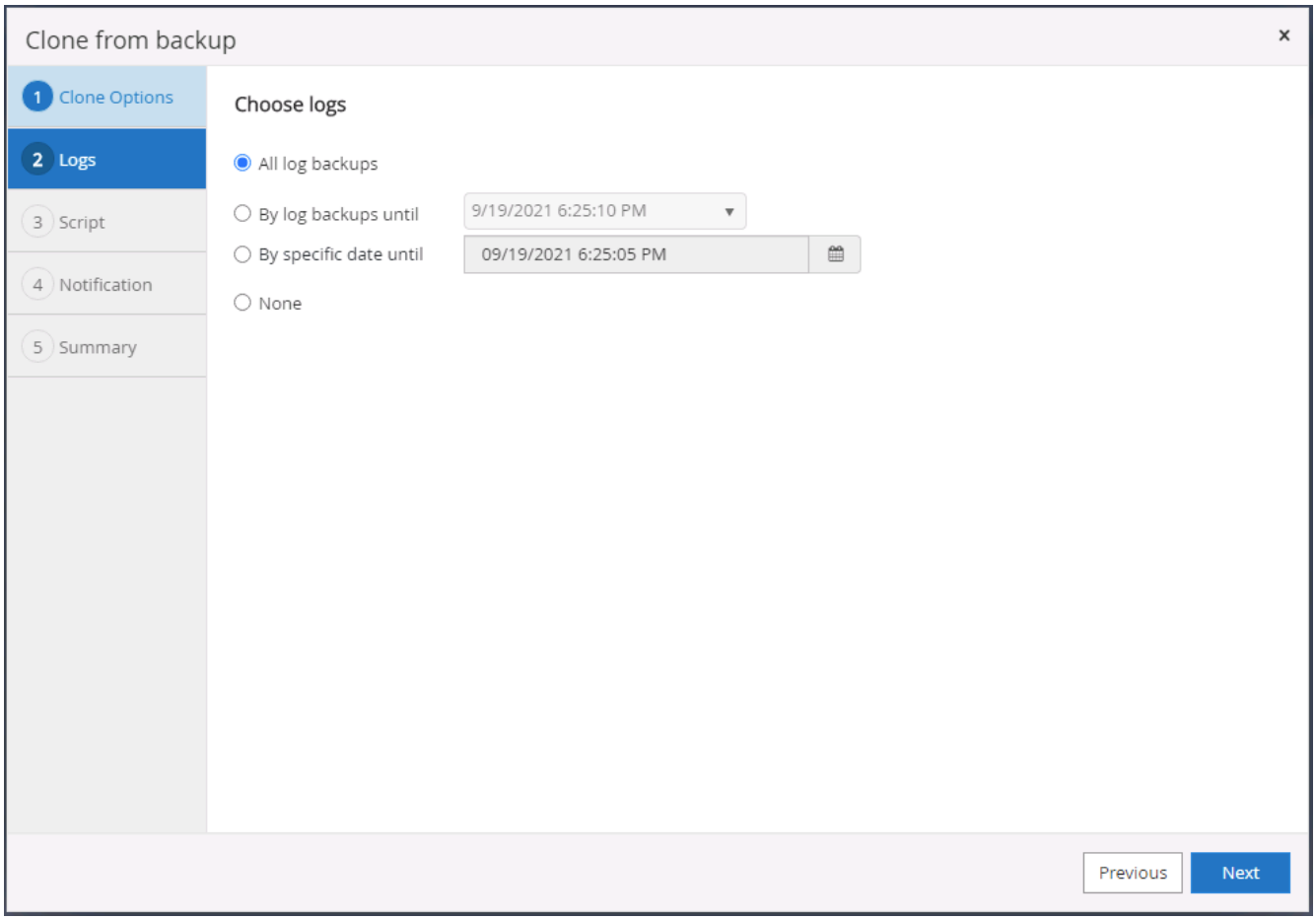
4. Sélectionnez la dernière sauvegarde complète SQL Server du clone.



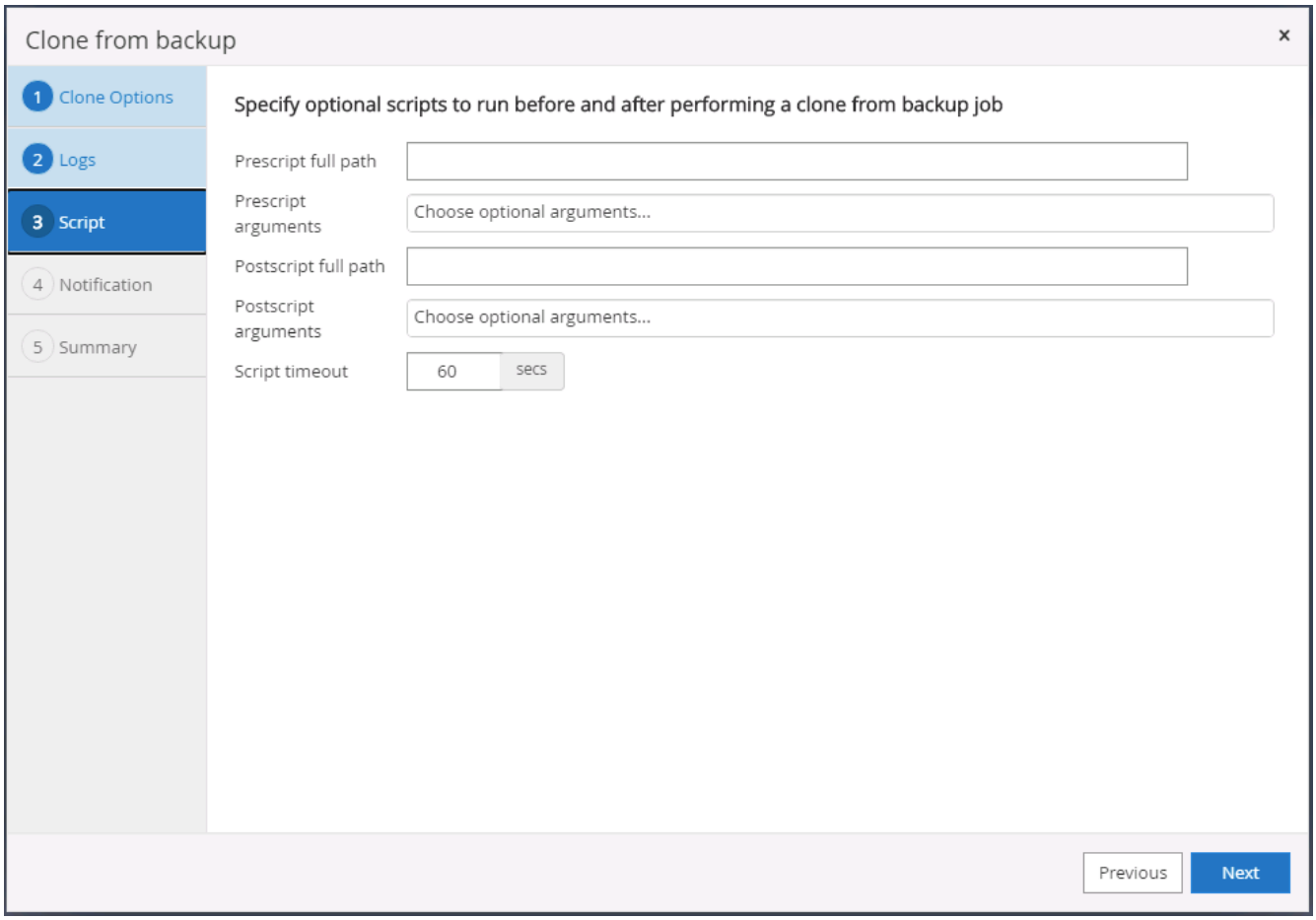
5. Définissez le paramètre de clonage comme le serveur de clonage, l'instance de clonage, le nom du clone et l'option de montage. L'emplacement de stockage secondaire où le clonage est effectué est rempli automatiquement.



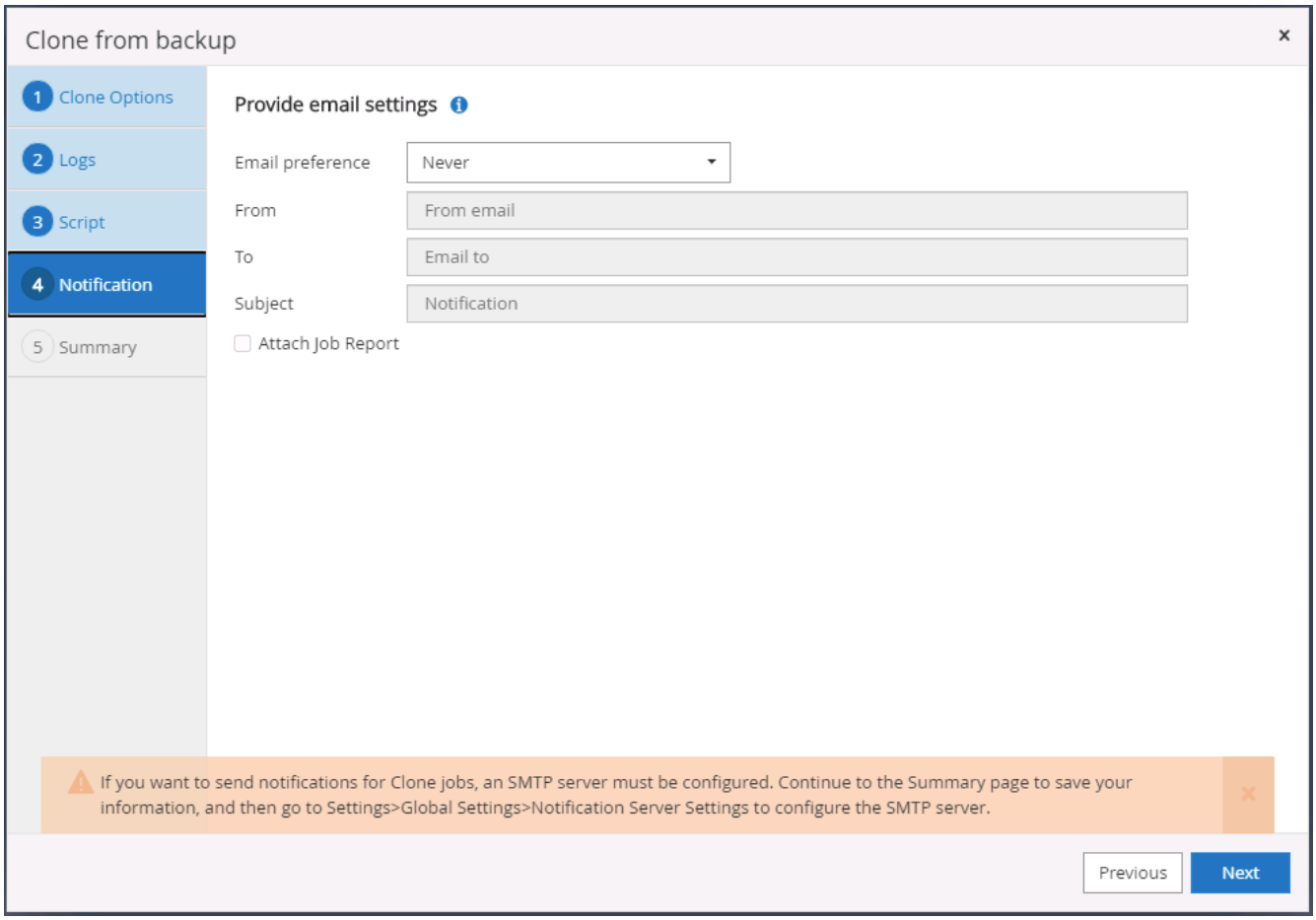
6. Sélectionnez toutes les sauvegardes de journaux à appliquer.



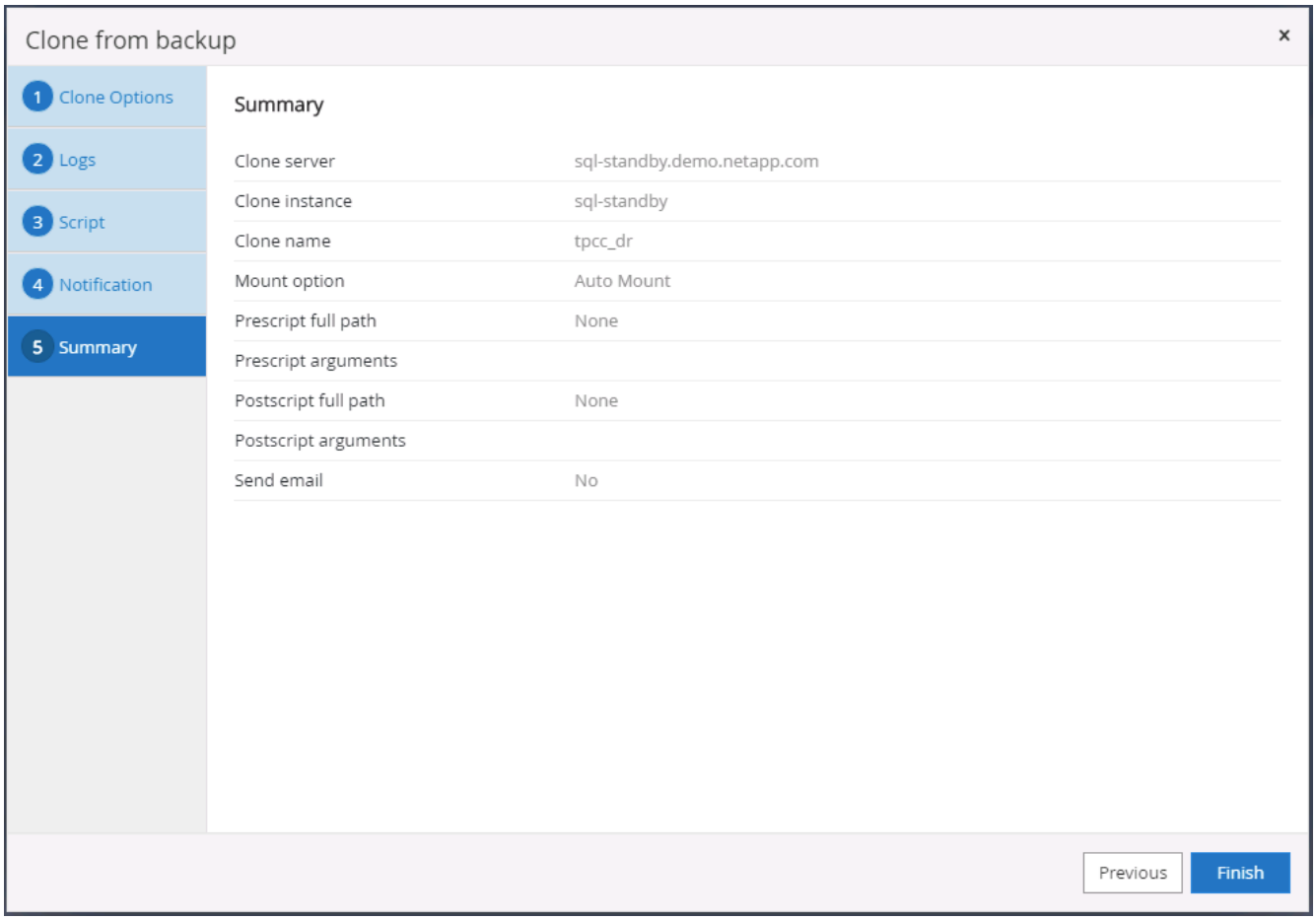
7. Spécifiez tous les scripts facultatifs à exécuter avant ou après le clonage.

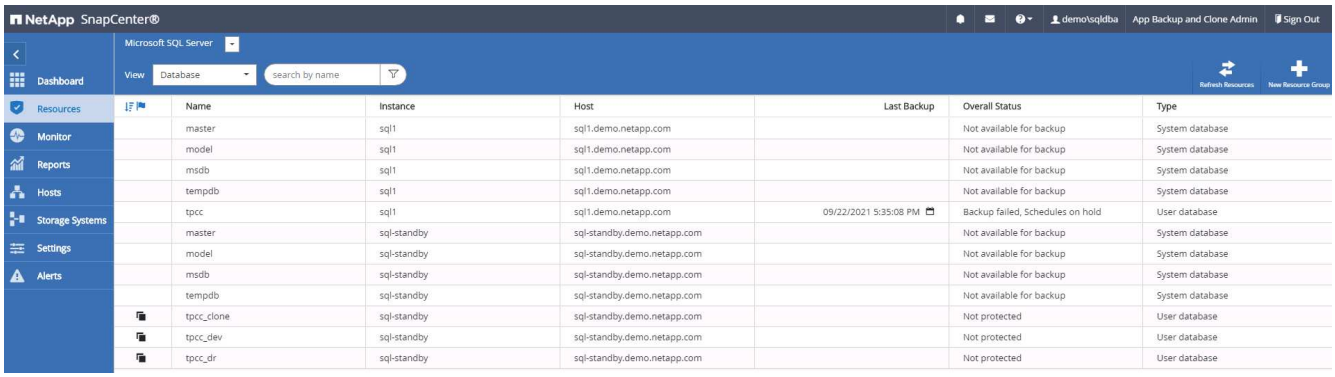


8. Spécifiez un serveur SMTP si vous souhaitez recevoir une notification par e-mail.



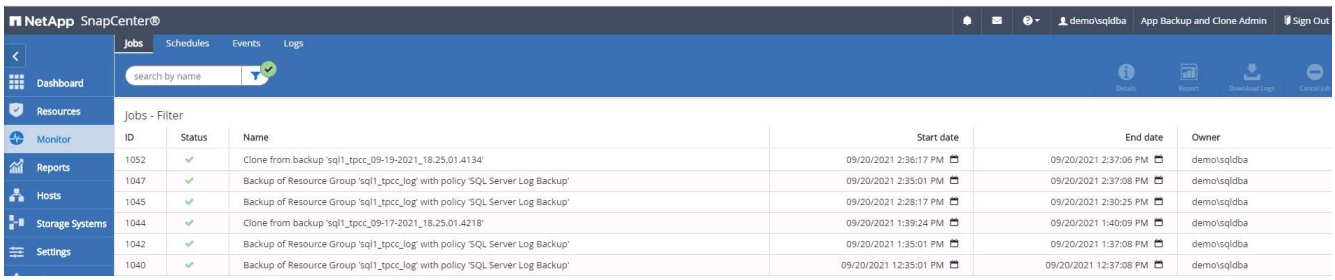
9. Récapitulatif sur le clone de DR. Les bases de données clonées sont immédiatement enregistrées auprès de SnapCenter et disponibles pour la protection des sauvegardes.





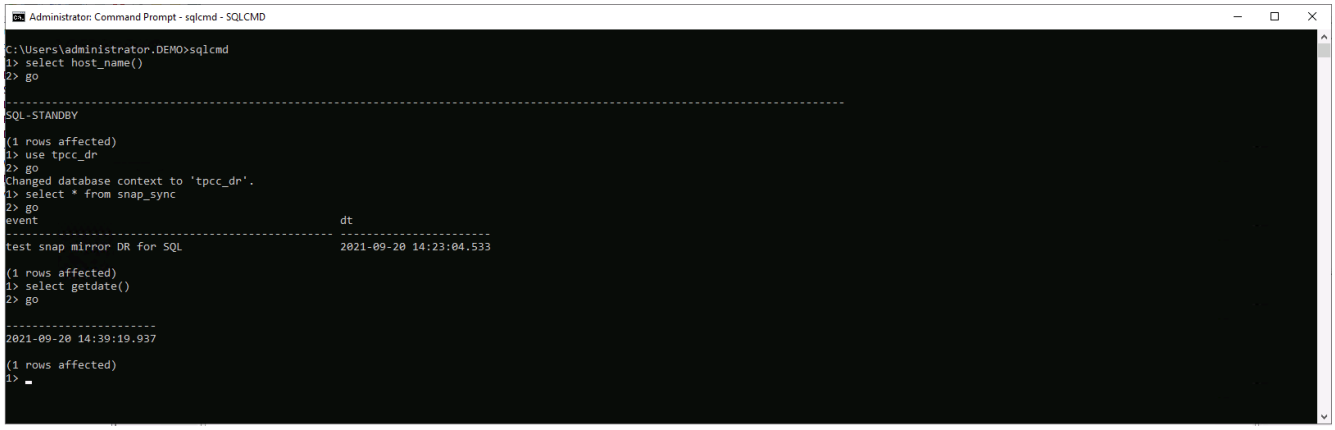
Validation et configuration des clones après reprise après incident pour SQL

1. Surveillez l’état des tâches de clonage.



2. Vérifier que la dernière transaction a été répliquée et restaurée avec l’ensemble des clones et des

restaurations des fichiers journaux



3. Configurez un nouveau répertoire journal SnapCenter sur le serveur DR pour la sauvegarde des journaux SQL Server.
4. Séparer le volume cloné du volume source répliqué
5. La réplication inverse du cloud sur site, puis reconstruisez le serveur de base de données sur site en panne.

Où obtenir de l'aide ?

Si vous avez besoin d'aide pour cette solution et ces cas d'utilisation, rejoignez le "La communauté NetApp solution Automation prend en charge le Channel Slack" et recherchez le canal solution-automation pour poser vos questions ou vos questions.