Solutions de bases de données cloud hybrides avec SnapCenter

NetApp database solutions

NetApp
August 18, 2025

Sommaire

Solutions de bases de données cloud hybrides avec SnapCenter

TR-4908 : Présentation des solutions de bases de données cloud hybrides avec SnapCenter

Alan Cao, Félix Melligan, NetApp

Cette solution fournit aux clients et aux équipes terrain de NetApp des instructions et des conseils pour la configuration, l'exploitation et la migration de bases de données vers un environnement de cloud hybride à l'aide de l'outil basé sur l'interface graphique utilisateur NetApp SnapCenter et du service de stockage NetApp CVO dans les clouds publics pour les cas d'utilisation suivants :

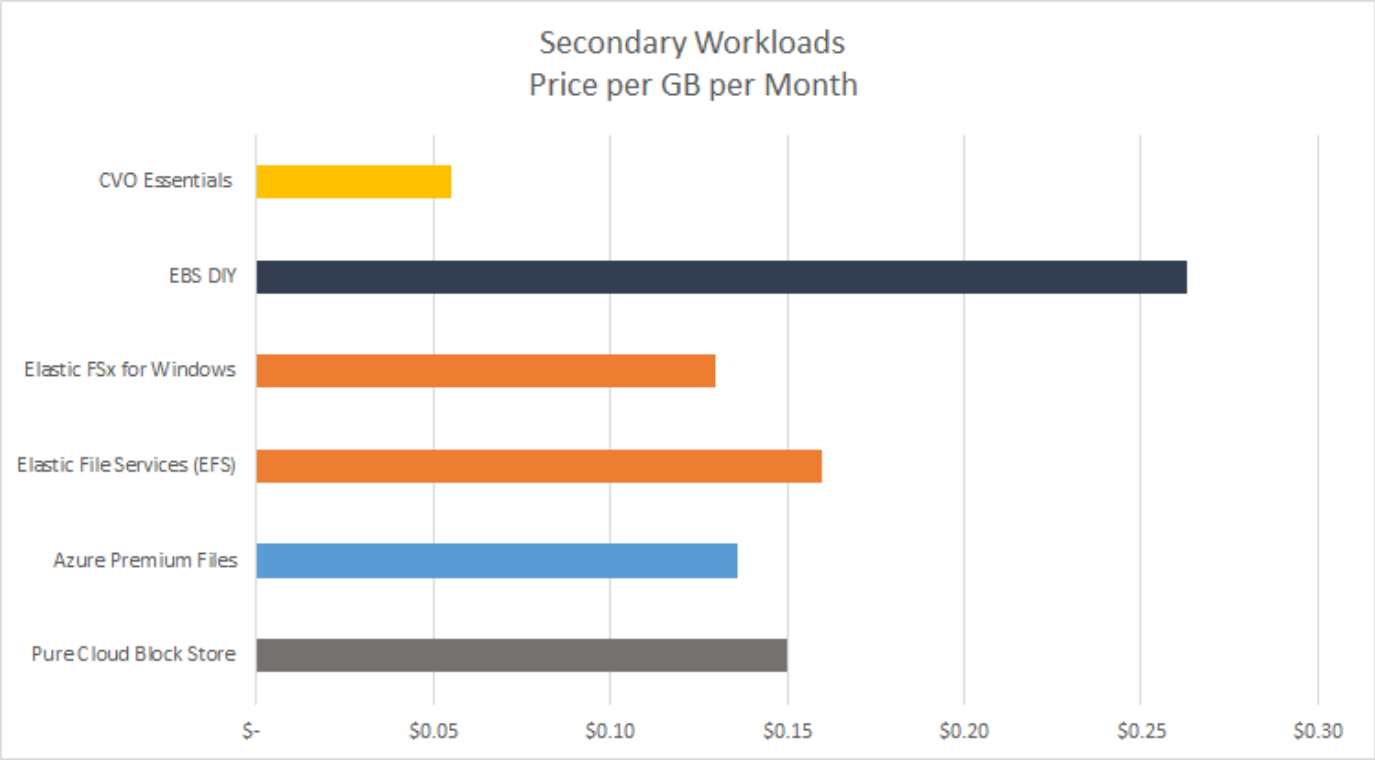
- Opérations de développement et de test de bases de données dans le cloud hybride
- Reprise après sinistre de la base de données dans le cloud hybride

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

De nombreuses bases de données d'entreprise, telles qu'Oracle, SQL Server, SAP HANA, etc., entraînent des coûts de licence et d'exploitation élevés. De nombreux clients paient des frais de licence uniques ainsi que des 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 sinistre. Il est possible que bon nombre de ces environnements ne soient pas pleinement utilisés tout au long du cycle de vie de l'application.

Les solutions offrent aux clients la possibilité de réduire potentiellement le nombre de cœurs sous licence en déplaçant leurs environnements de base de données dédiés au développement, aux tests ou à la reprise après sinistre vers le cloud. En utilisant l'évolutivité du cloud public, la redondance, la haute disponibilité et un modèle de facturation basé sur la consommation, les économies de coûts en matière de licences et d'exploitation peuvent être substantielles, sans sacrifier la convivialité ou la disponibilité des applications.

Au-delà des économies potentielles sur les coûts de licence de base de données, le modèle de licence CVO basé sur la capacité de NetApp permet aux clients de réduire les coûts de stockage par Go tout en leur offrant un niveau élevé de gestion de base de données qui n'est pas disponible auprès des services de stockage concurrents. Le graphique suivant présente une comparaison des coûts de stockage des services de stockage populaires disponibles dans le cloud public.



Cette solution démontre qu'en utilisant l'outil logiciel basé sur l'interface graphique SnapCenter et la technologie NetApp SnapMirror , les opérations de base de données cloud hybride peuvent être facilement configurées, mises en œuvre et exploitées.

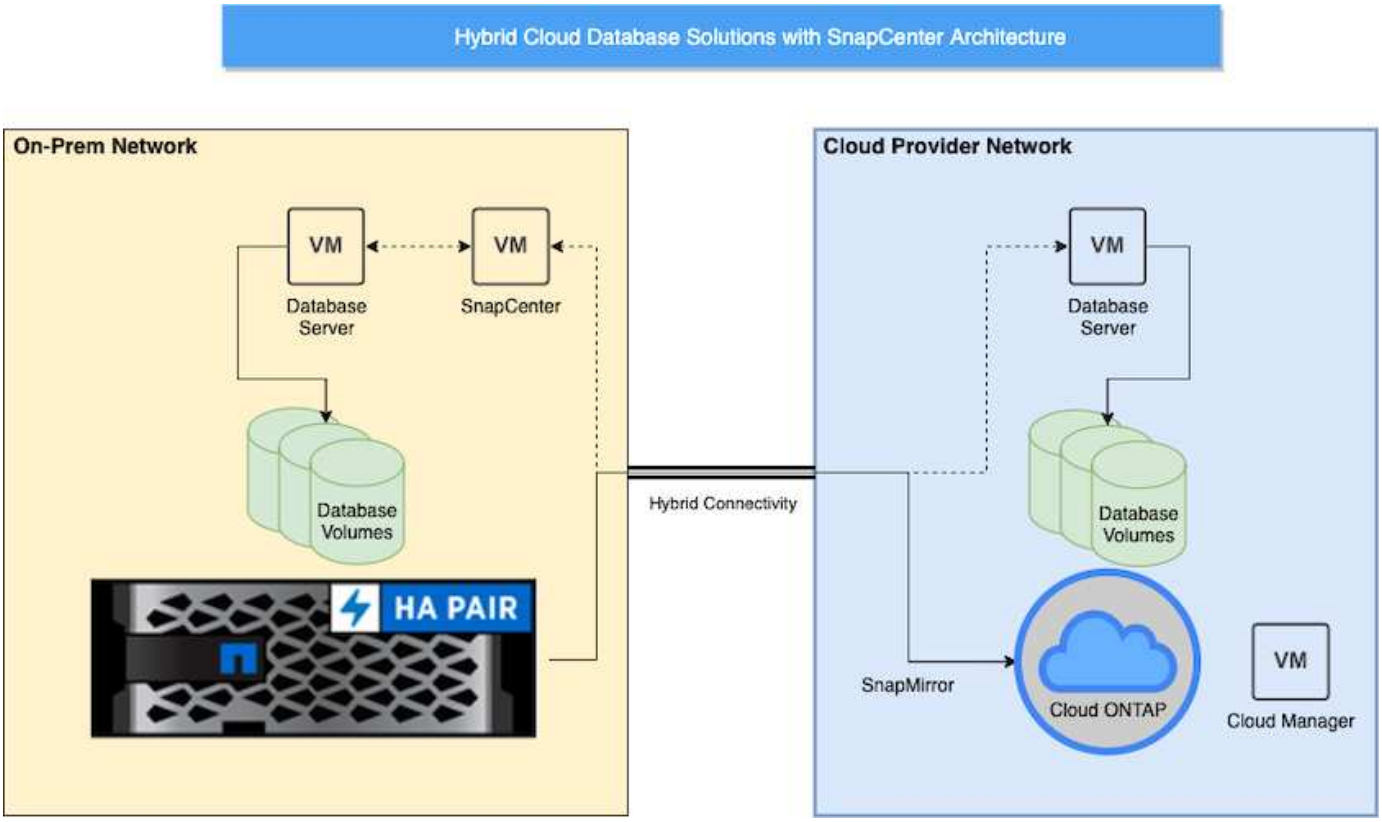
Les vidéos suivantes montrent SnapCenter en action :

- "Sauvegarde d'une base de données Oracle sur un cloud hybride à l'aide de SnapCenter"
- "SnapCenter- Cloner DEV/TEST vers AWS Cloud pour une base de données Oracle"

Il est à noter que, bien que les illustrations de ce document présentent CVO comme une 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.

Architecture de la solution

Le diagramme d'architecture suivant illustre une implémentation typique du fonctionnement d'une base de données d'entreprise dans un cloud hybride pour les opérations de développement/test et de reprise après sinistre.



Dans le cadre d'opérations commerciales normales, les volumes de base de données synchronisés dans le cloud peuvent être clonés et montés sur des instances de base de données de développement/test pour le développement ou le test d'applications. En cas de panne, les volumes de base de données synchronisés dans le cloud peuvent alors être activés pour la reprise après sinistre.

Configuration requise SnapCenter

Cette solution est conçue dans un environnement de cloud hybride pour prendre en charge les bases de données de production sur site qui peuvent être déployées sur tous les clouds publics populaires pour les opérations de développement/test et de reprise après sinistre.

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 présentées ici. Cette solution est validée avec des charges de travail de base de données virtualisées, bien que les charges de travail bare-metal soient également prises en charge.

Nous supposons que les serveurs de base de données de production sont hébergés sur site avec des volumes de base de données présentés aux hôtes de base de données à partir d'un cluster de stockage ONTAP . Le SnapCenter software est installé sur site pour la sauvegarde de la base de données et la réplication des données vers le cloud. Un contrôleur Ansible est recommandé mais pas requis pour l'automatisation du déploiement de la base de données ou la synchronisation de la configuration du noyau du système d'exploitation et de la base de données avec une instance DR de secours ou des instances de développement/test dans le cloud public.

Exigences

Environnement	Exigences
Sur place	Toutes les bases de données et versions prises en charge par SnapCenter
	SnapCenter v4.4 ou supérieur
	Ansible v2.09 ou supérieur
	Cluster ONTAP 9.x
	LIF intercluster configurés
	Connectivité depuis un site local vers un VPC 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 DB OS avec les instances sur site
Cloud - Azure	"Connecteur Cloud Manager"
	"Cloud Volumes ONTAP"
	Correspondance des machines virtuelles Azure DB OS avec les machines sur site
Cloud - GCP	"Connecteur Cloud Manager"
	"Cloud Volumes ONTAP"
	Correspondance des instances DB OS Google Compute Engine avec les instances sur site

Configuration des prérequis

Configuration des prérequis

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

Sur place

- Installation et configuration de SnapCenter
- Configuration du stockage du serveur de base de données sur site
- Conditions d'obtention de licence
- Réseau et sécurité
- Automation

Cloud public

- Une connexion NetApp Cloud Central
- Accès réseau depuis un navigateur Web vers plusieurs points de terminaison

- Un emplacement réseau pour un connecteur
- Autorisations du fournisseur de cloud
- Mise en réseau pour les services individuels

Considérations importantes :

1. Où déployer le connecteur Cloud Manager ?
2. Dimensionnement et architecture de Cloud Volume ONTAP
3. Nœud unique ou haute disponibilité ?

Les liens suivants fournissent plus de détails :

"Sur place"

"Cloud public"

Prérequis sur site

Les tâches suivantes doivent être effectuées sur site pour préparer l'environnement de charge de travail de la base de données cloud hybride SnapCenter .

Installation et configuration de SnapCenter

L'outil NetApp SnapCenter est une application Windows qui s'exécute généralement dans un environnement de domaine Windows, bien que le déploiement de groupe de travail soit également possible. Il est basé sur une architecture à plusieurs niveaux qui comprend un serveur de gestion centralisé (le serveur SnapCenter) et un plug-in SnapCenter sur les hôtes du serveur de base de données pour les charges de travail de base de données. Voici quelques considérations clés pour le déploiement d'un cloud hybride.

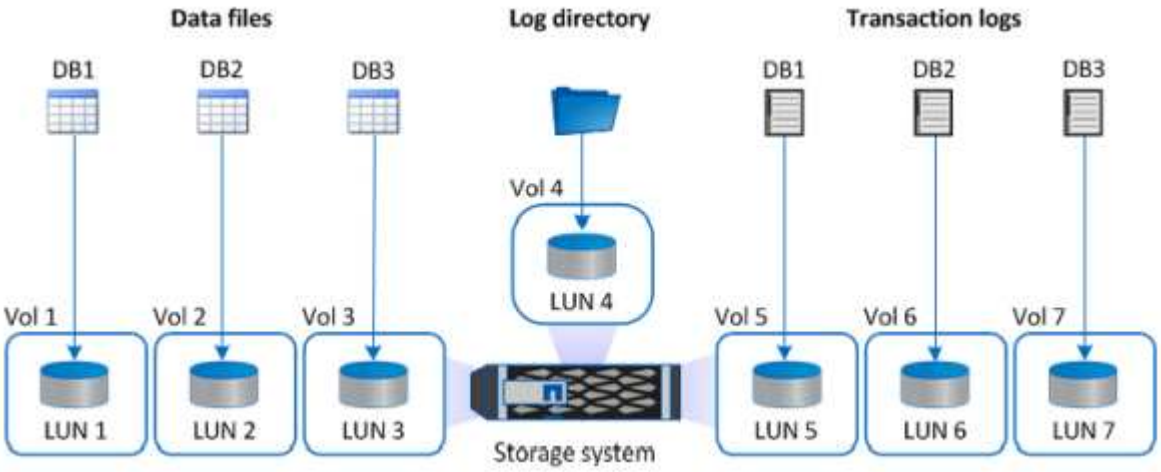
- **Instance unique ou déploiement HA.** Le déploiement HA fournit une redondance en cas de défaillance d'un seul serveur d'instance SnapCenter .
- **Résolution de nom.** Le DNS doit être configuré sur le serveur SnapCenter pour résoudre tous les hôtes de base de données ainsi que sur le SVM de stockage pour la recherche directe et inverse. Le DNS doit également être configuré sur les serveurs de base de données pour résoudre le serveur SnapCenter et le SVM de stockage pour la recherche directe et inverse.
- **Configuration du contrôle d'accès basé sur les rôles (RBAC).** Pour les charges de travail de base de données mixtes, vous souhaiterez peut-être utiliser RBAC pour séparer la responsabilité de gestion pour différentes plates-formes de base de données, telles qu'un administrateur pour la base de données Oracle ou un administrateur pour SQL Server. Les autorisations nécessaires doivent être accordées à l'utilisateur administrateur de la base de données.
- **Activer la stratégie de sauvegarde basée sur des politiques.** Pour garantir 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 de base de données cloud.
- **Les ports doivent être ouverts pour autoriser le trafic SnapMirror entre le cloud local et le cloud public.** Le serveur SnapCenter s'appuie sur ONTAP SnapMirror pour répliquer les sauvegardes Snapshot sur site vers les SVM de stockage CVO cloud.

Après une planification et une réflexion minutieuses avant l'installation, cliquez ici"Prérequis d'installation de SnapCenter" pour plus de détails sur l'installation et la configuration de SnapCenter .

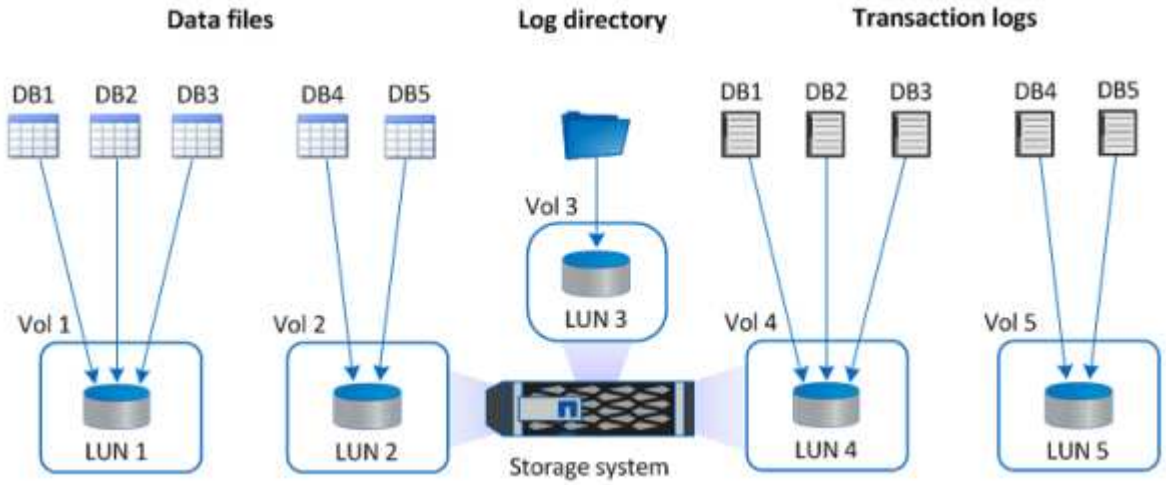
Configuration du stockage du serveur de base de données sur site

Les performances de 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 également faciliter la gestion de la sauvegarde et de la récupération de la base de données. Plusieurs facteurs doivent être pris en compte lors de la définition de votre configuration de stockage, notamment la taille de la base de données, le taux de modification des données attendu pour la base de données et la fréquence à laquelle vous effectuez des sauvegardes.

La connexion directe des LUN de stockage à la machine virtuelle invitée via NFS ou iSCSI pour les charges de travail de base de données virtualisées offre généralement de meilleures performances que le stockage alloué via VMDK. NetApp recommande la disposition de stockage pour une grande base de données SQL Server sur les LUN illustrée dans la figure suivante.



La figure suivante montre la disposition de stockage recommandée par NetApp pour les bases de données SQL Server de petite ou moyenne taille sur les LUN.



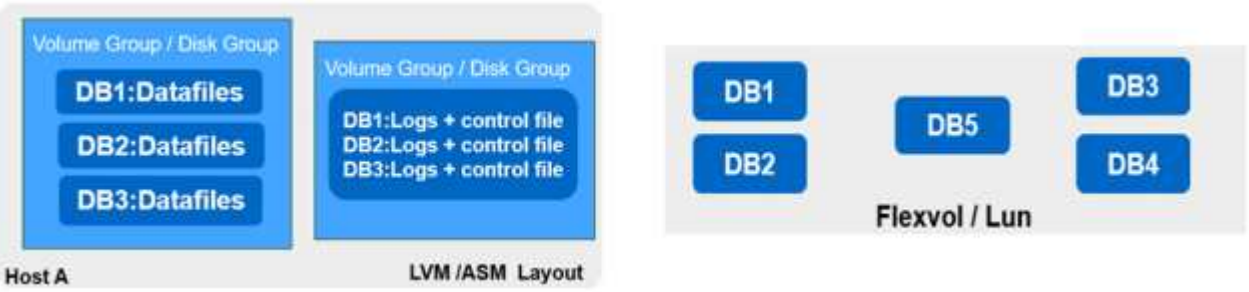
> Le répertoire Log est dédié à SnapCenter pour effectuer la récupération du journal des transactions pour la récupération de la base de données. Pour une base de données extra-large, plusieurs LUN peuvent être alloués à un volume pour de meilleures performances.

Pour les charges de travail de base de données Oracle, SnapCenter prend en charge les environnements de base de données sauvegardés par le stockage ONTAP qui sont montés sur l'hôte en tant que périphériques

physiques ou virtuels. Vous pouvez héberger l'intégralité de la base de données sur un ou plusieurs périphériques de stockage en fonction de la criticité de l'environnement. En règle générale, les clients isolent les fichiers de données sur un stockage dédié de tous les autres fichiers tels que les fichiers de contrôle, les fichiers de rétablissement et les fichiers journaux d'archivage. Cela aide les administrateurs à restaurer rapidement (fichier unique ONTAP SnapRestore) ou à cloner une grande base de données critique (échelle pétaoctet) à l'aide de la technologie Snapshot en quelques secondes à quelques minutes.

Pour les charges de travail critiques sensibles à la latence, un volume de stockage dédié doit être déployé sur différents types de fichiers Oracle pour obtenir la meilleure latence possible. Pour une base de données volumineuse, 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 une partie d'une base de données sur le même volume de stockage ou LUN. À titre d'exemple de cette disposition, vous pouvez héberger des fichiers de données pour toutes les bases de données sur un groupe de disques +DATA ASM ou un groupe de volumes. Le reste des fichiers (fichiers de rétablissement, 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 le déplacement des bases de données Oracle, le binaire Oracle doit être installé sur un LUN distinct inclus dans la politique de sauvegarde régulière. Cela garantit qu'en cas de déplacement de la base de données vers un nouvel hôte de serveur, la pile Oracle peut être démarrée pour la récupération sans aucun problème potentiel dû à un binaire Oracle désynchronisé.

Conditions d'obtention de licence

SnapCenter est un logiciel sous licence de NetApp. Il est généralement inclus dans une licence ONTAP sur site. Cependant, pour le déploiement de cloud hybride, une licence cloud pour SnapCenter est également

requise pour ajouter CVO à SnapCenter en tant que destination de réplication de données cible. Veuillez consulter les liens suivants pour la licence standard basée sur la capacité de SnapCenter pour plus de détails :

"Licences standard SnapCenter basées sur la capacité"

Réseau et sécurité

Dans une opération de base de données hybride qui nécessite une base de données de production sur site extensible vers le cloud pour le développement/test et la reprise après sinistre, la mise en réseau et la sécurité sont des facteurs importants à prendre en compte lors de la configuration de l'environnement et de la connexion au cloud public à partir d'un centre de données sur site.

Les clouds publics utilisent généralement un cloud privé virtuel (VPC) pour isoler différents utilisateurs au sein d'une plate-forme 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 du centre de données sur site au 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 entre les hôtes sur Internet et les hôtes à l'intérieur du centre de données de l'entreprise.

Pour les considérations de mise en réseau et de sécurité, examinez les règles CVO entrantes et sortantes pertinentes pour le cloud public de votre choix :

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

Utilisation de l'automatisation Ansible pour synchroniser les instances de base de données entre les locaux et le cloud (facultatif)

Pour simplifier la gestion d'un environnement de base de données cloud hybride, NetApp recommande fortement, mais n'exige pas, que vous déployiez un contrôleur Ansible pour automatiser certaines tâches de gestion, telles que la synchronisation des instances de calcul sur site et dans le cloud. Ceci est particulièrement important car une instance de calcul désynchronisée dans le cloud peut rendre la base de données récupérée dans le cloud sujette aux erreurs en raison de packages de noyau manquants et d'autres problèmes.

La capacité d'automatisation d'un contrôleur Ansible peut également être utilisée pour augmenter SnapCenter pour certaines tâches, telles que la division de l'instance SnapMirror pour activer la copie des données DR pour la production.

Suivez ces instructions pour configurer votre nœud de contrôle Ansible pour les machines RedHat ou CentOS :

1. Exigences pour le nœud de contrôle Ansible :
    a. Une machine RHEL/CentOS avec les packages suivants installés :
        i. Python3
        ii. Pip3
        iii. Ansible (version supérieure à 2.10.0)
        iv. Git

Si vous disposez d'une nouvelle machine RHEL/CentOS sans les exigences ci-dessus installées, suivez les étapes ci-dessous pour configurer cette machine comme nœud de contrôle Ansible :

1. Activer le référentiel Ansible pour RHEL-8/RHEL-7
   a. Pour RHEL-8 (exécutez la commande ci-dessous en tant que root)

```
subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-
rpms
```

   b. Pour RHEL-7 (exécutez la commande ci-dessous en tant que root)

```
subscription-manager repos --enable rhel-7-server-ansible-2.9-rpms
```

2. Collez le contenu ci-dessous dans le terminal

```
sudo yum -y install python3 >> install.log
sudo yum -y install python3-pip >> install.log
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
install.log
sudo yum -y install git >> install.log
```

Suivez ces instructions pour configurer votre nœud de contrôle Ansible pour les machines Ubuntu ou Debian :

1. Exigences pour le nœud de contrôle Ansible :
   a. Une machine Ubuntu/Debian avec les packages suivants installés :
      i. Python3
      ii. Pip3
      iii. Ansible (version supérieure à 2.10.0)
      iv. Git

Si vous disposez d'une nouvelle machine Ubuntu/Debian sans les exigences ci-dessus installées, suivez les étapes ci-dessous pour configurer cette machine comme nœud de contrôle Ansible :

1. Collez le contenu ci-dessous dans le terminal

```
sudo apt-get -y install python3 >> outputlog.txt
sudo apt-get -y install python3-pip >> outputlog.txt
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
outputlog.txt
sudo apt-get -y install git >> outputlog.txt
```

Prérequis pour le cloud public

Avant d'installer le connecteur Cloud Manager et Cloud Volumes ONTAP et de configurer SnapMirror, nous devons effectuer certaines préparations pour notre environnement cloud. Cette page décrit le travail à effectuer ainsi que les considérations à prendre en compte lors du déploiement de Cloud Volumes ONTAP.

Liste de contrôle des prérequis pour le déploiement de Cloud Manager et Cloud Volumes ONTAP

- Une connexion NetApp Cloud Central
- Accès réseau depuis un navigateur Web vers plusieurs points de terminaison
- Un emplacement réseau pour un connecteur
- Autorisations du fournisseur de cloud
- Mise en réseau pour les services individuels

Pour plus d'informations sur ce dont vous avez besoin pour commencer, visitez notre "documentation sur le 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. Le 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 sur le 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. Bien que bon nombre de ces valeurs puissent être modifiées ultérieurement sans interruption, certaines décisions clés doivent être prises avant le déploiement en fonction des charges de travail à déployer dans le cloud.

Chaque fournisseur de cloud dispose de différentes options de déploiement et presque chaque charge de travail possède ses propres propriétés uniques. NetApp a un "Calculateur de coût total de possession" qui peut aider à dimensionner correctement les déploiements en fonction de la capacité et des performances, mais il a été construit autour de certains concepts de base qui méritent d'être pris en compte :

- Capacité requise
- Capacité réseau de la machine virtuelle cloud
- Caractéristiques de performance du stockage cloud

La clé est de planifier une configuration qui non seulement répond aux exigences actuelles de capacité et de performances, mais qui prend également en compte la croissance future. C'est ce que l'on appelle généralement la marge de capacité et la marge de performance.

Si vous souhaitez plus d'informations, lisez la documentation sur la planification correcte pour "AWS" , "Azuré" , et "BPC" .

3. Nœud unique ou haute disponibilité ?

Dans tous les clouds, il existe la possibilité de déployer CVO soit dans un seul nœud, soit dans une paire de clusters à haute disponibilité avec deux nœuds. Selon le cas d'utilisation, vous souhaiterez peut-être déployer un seul nœud pour réduire les coûts ou une paire HA pour offrir davantage de disponibilité et de redondance.

Pour un cas d'utilisation DR ou pour la mise en place d'un stockage temporaire à des fins de développement et de test, les nœuds uniques sont courants, car l'impact d'une panne soudaine de zone ou d'infrastructure est plus faible. Cependant, pour tout cas d'utilisation de production, lorsque les données se trouvent dans un seul emplacement ou lorsque l'ensemble de données doit avoir plus de redondance et de disponibilité, une haute disponibilité est recommandée.

Pour plus d'informations sur l'architecture de la version de haute disponibilité de chaque cloud, consultez la documentation de "AWS" , "Azuré" et "BPC" .

Présentation de la mise en route

Présentation de la mise en route

Cette section fournit un résumé des tâches qui doivent être accomplies pour répondre aux exigences préalables décrites dans la section précédente. La section suivante fournit une liste de tâches de haut niveau 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 administrateur de la base de données dans SnapCenter
- Conditions préalables à l'installation du plugin SnapCenter
- Installation du plug-in hôte SnapCenter
- Découverte des ressources de la base de données
- Configurer l'appairage de clusters de stockage et la réplication de volumes de bases de données
- Ajouter un stockage de base de données CVO SVM à SnapCenter
- Configurer la politique de sauvegarde de la base de données dans SnapCenter
- Mettre en œuvre une politique de sauvegarde pour protéger la base de données
- Valider la sauvegarde

Cloud public AWS

- Contrôle pré-vol
- Étapes pour déployer Cloud Manager et Cloud Volumes ONTAP dans AWS
- Déployer une instance de calcul EC2 pour la charge de travail de la base de données

Cliquez sur les liens suivants pour plus de détails :

"Sur place","Cloud public - AWS"

Démarrer sur site

L'outil NetApp SnapCenter utilise le contrôle d'accès basé sur les rôles (RBAC) pour gérer l'accès aux ressources utilisateur et les octrois d'autorisations, et l'installation de SnapCenter crée des rôles préremplis. Vous pouvez également créer des rôles personnalisés en fonction de vos besoins ou de vos applications.

Sur place

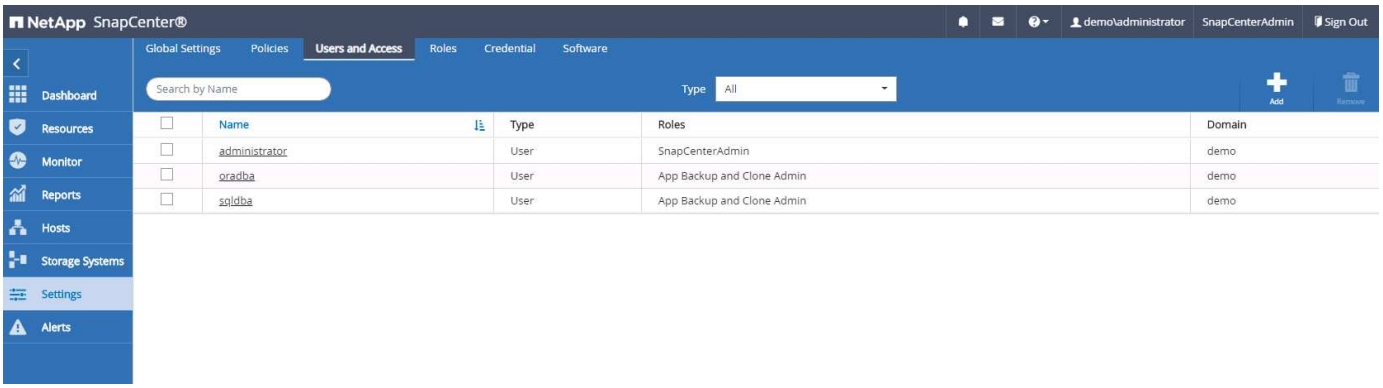
1. Configurer l'utilisateur administrateur de la base de données dans SnapCenter

Il est logique d'avoir un ID utilisateur administrateur dédié pour chaque plate-forme de base de données prise en charge par SnapCenter pour la sauvegarde, la restauration et/ou la reprise après sinistre de la base de données. Vous pouvez également utiliser un identifiant unique pour gérer toutes les bases de données. Dans nos cas de test et notre démonstration, nous avons créé un utilisateur administrateur dédié pour Oracle et SQL Server, respectivement.

Certaines ressources SnapCenter ne peuvent être provisionnées qu'avec le rôle SnapCenterAdmin. Les ressources peuvent ensuite être attribuées à d'autres identifiants d'utilisateur pour y accéder.

Dans un environnement SnapCenter sur site préinstallé et configuré, les tâches suivantes ont peut-être déjà été effectuées. Sinon, les étapes suivantes créent un utilisateur administrateur de base de données :

1. Ajoutez l'utilisateur administrateur à Windows Active Directory.
2. Connectez-vous à SnapCenter à l'aide d'un identifiant 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 administrateur 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 plugin SnapCenter

SnapCenter effectue la sauvegarde, la restauration, le clonage 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 de la base de données 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 exigences de privilèges 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 de base de données doivent être configurées avant l'installation du plug-in SnapCenter . En règle générale, vous souhaitez utiliser un compte d'utilisateur administrateur sur l'hôte

de base de données comme informations d'identification de connexion hôte pour l'installation du plug-in. Vous pouvez également accorder le même ID utilisateur pour l'accès à la base de données à l'aide de l'authentification basée sur le système d'exploitation. D'autre part, vous pouvez également utiliser l'authentification de base de données avec différents ID utilisateur de base de données pour l'accès à la gestion de la base de données. Si vous décidez d'utiliser l'authentification basée sur le système d'exploitation, l'ID utilisateur de l'administrateur du système d'exploitation doit avoir accès à la base de données. Pour l'installation de SQL Server basée sur un domaine Windows, un compte d'administrateur de domaine peut être utilisé pour gérer tous les serveurs SQL au sein du domaine.

Hôte Windows pour serveur SQL :

1. Si vous utilisez les informations d'identification Windows pour l'authentification, vous devez configurer vos informations d'identification avant d'installer les plug-ins.
2. Si vous utilisez une instance SQL Server pour l'authentification, vous devez ajouter les informations d'identification après l'installation 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 est affichée avec une icône de cadenas rouge. Si l'icône de verrouillage apparaît, vous devez spécifier les informations d'identification de l'instance ou de la base de données pour ajouter avec succès l'instance ou la base de données à un groupe de ressources.
4. Vous devez attribuer les informations d'identification à un utilisateur RBAC sans accès administrateur système lorsque les conditions suivantes sont remplies :
    - Les informations d'identification sont attribuées à une instance SQL.
    - L'instance ou l'hôte SQL est attribué à un utilisateur RBAC.
    - L'utilisateur administrateur de la base de données RBAC doit disposer à la fois des privilèges de groupe de ressources et de sauvegarde.

Hôte Unix pour Oracle :

1. Vous devez avoir activé la connexion SSH basée sur un 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 un mot de passe sur l'instance AWS est désactivée par défaut.
2. Configurez les privilèges sudo pour que l'utilisateur non root puisse installer et démarrer le processus du plugin. Après l'installation du plugin, les processus s'exécutent en tant qu'utilisateur root effectif.
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 plugin de base de données Oracle installe également le plugin SnapCenter pour Unix.

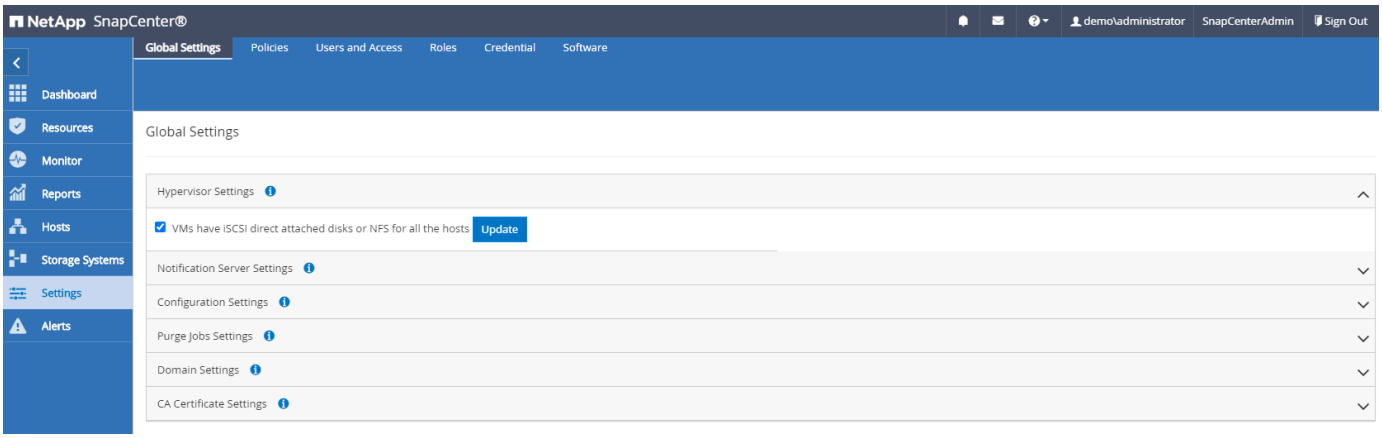
3. Installation du plug-in hôte SnapCenter

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

Les étapes suivantes illustrent comment 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.

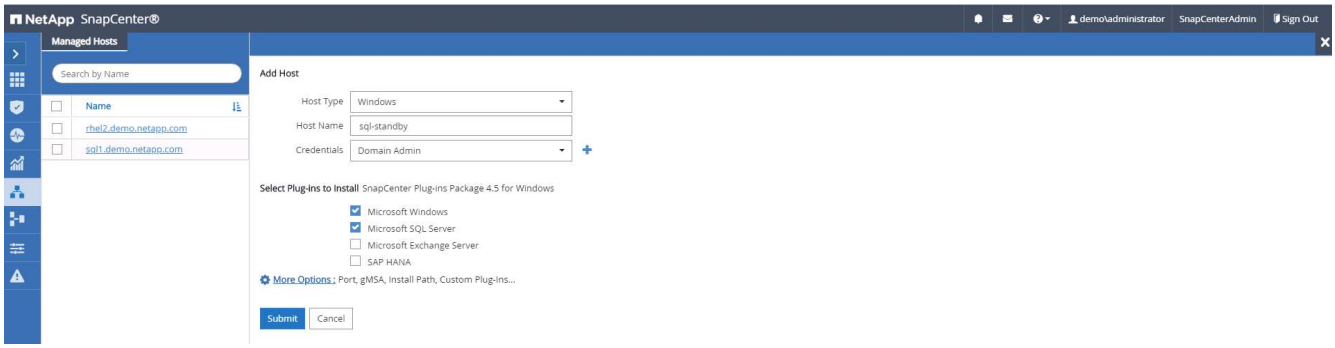
Configurer les paramètres globaux de SnapCenter VMware

Accédez à Paramètres > Paramètres globaux. Sélectionnez « Les machines virtuelles ont des disques iSCSI directement connectés ou NFS pour tous les hôtes » sous Paramètres de l'hyperviseur et cliquez sur Mettre à jour.



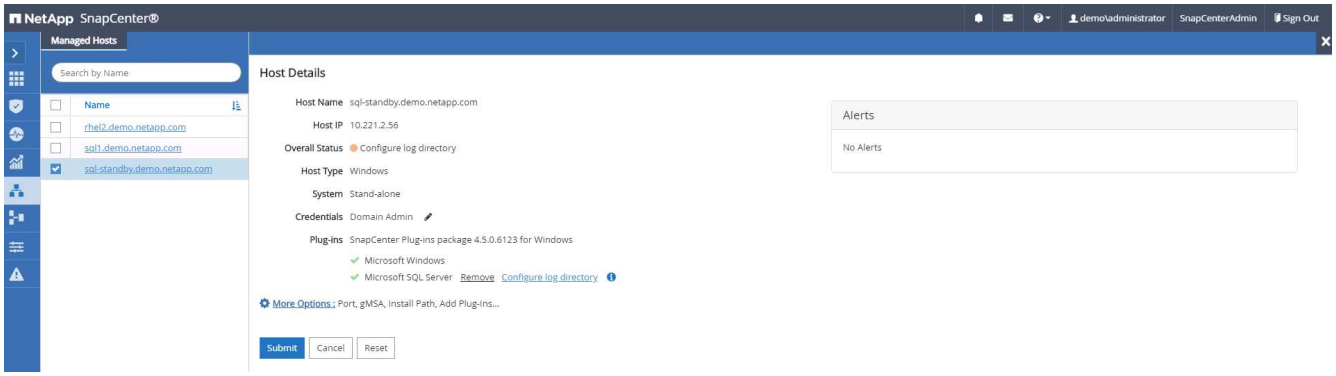
Ajout d'un hôte Windows et installation du plugin sur l'hôte

1. Connectez-vous à SnapCenter avec un identifiant 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 un hôte.
3. Choisissez Windows comme type d'hôte ; le nom d'hôte peut être un nom d'hôte ou une adresse IP. Le nom d'hôte doit être résolu en l'adresse IP d'hôte correcte à partir 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 packages de plug-ins à installer.

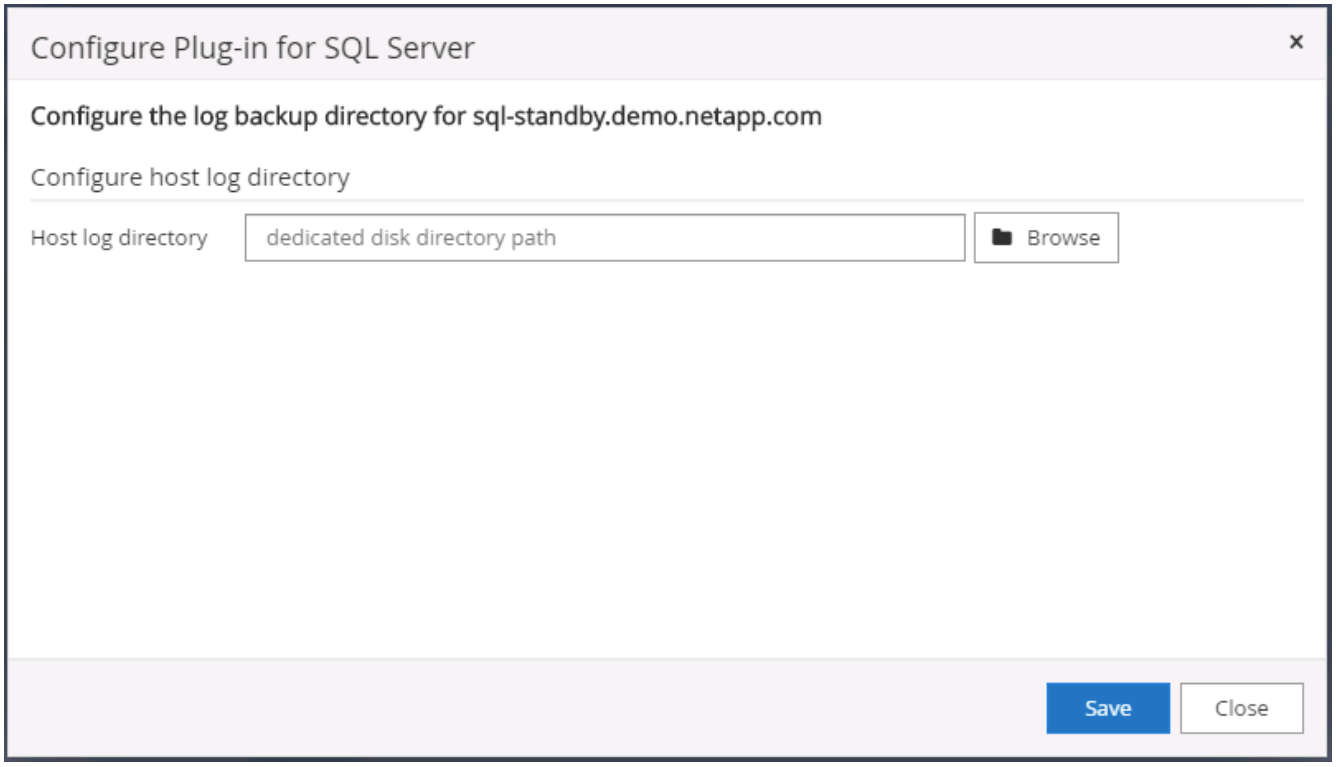


4. Une fois le plugin installé sur un hôte Windows, son état général est affiché comme « Configurer le répertoire des journaux ».

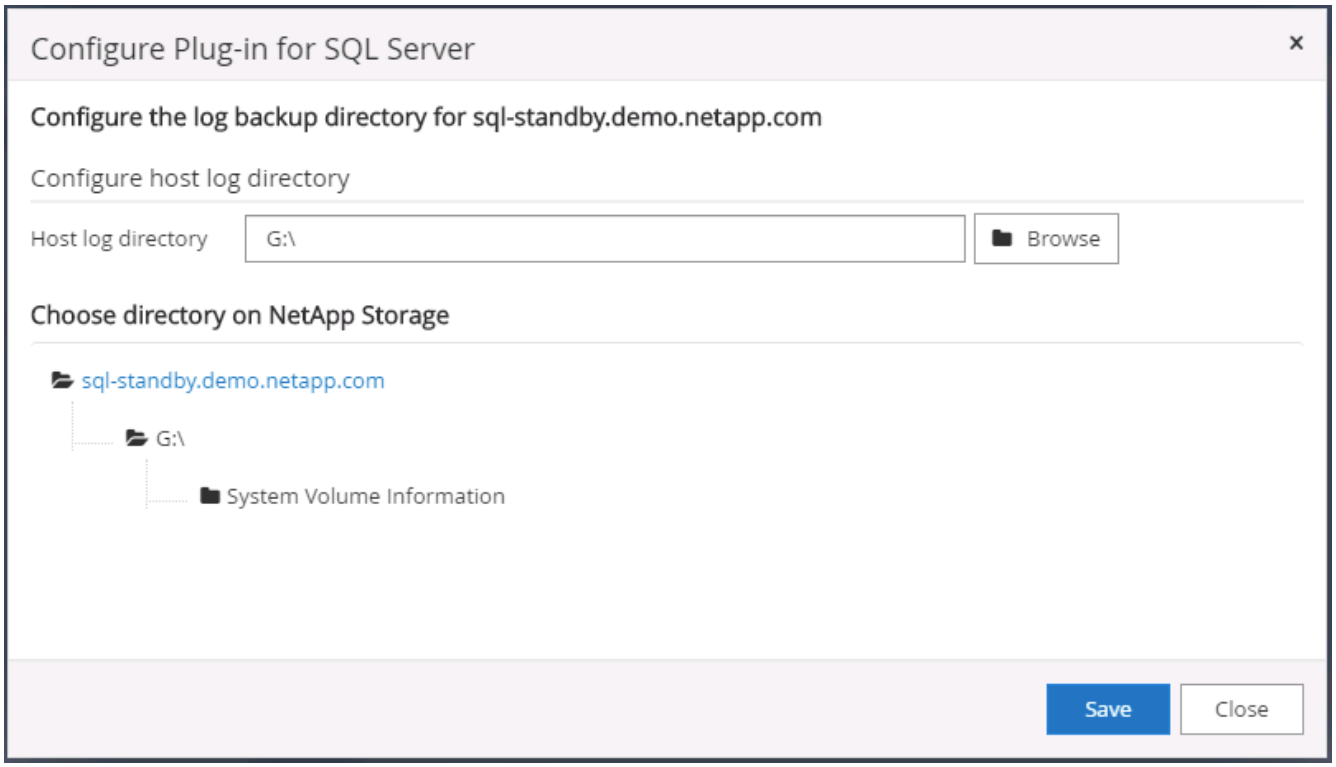
5. Cliquez sur le nom d'hôte pour ouvrir la configuration du répertoire de journaux SQL Server.



6. Cliquez sur « Configurer le répertoire des journaux » pour ouvrir « Configurer le plug-in pour SQL Server ».

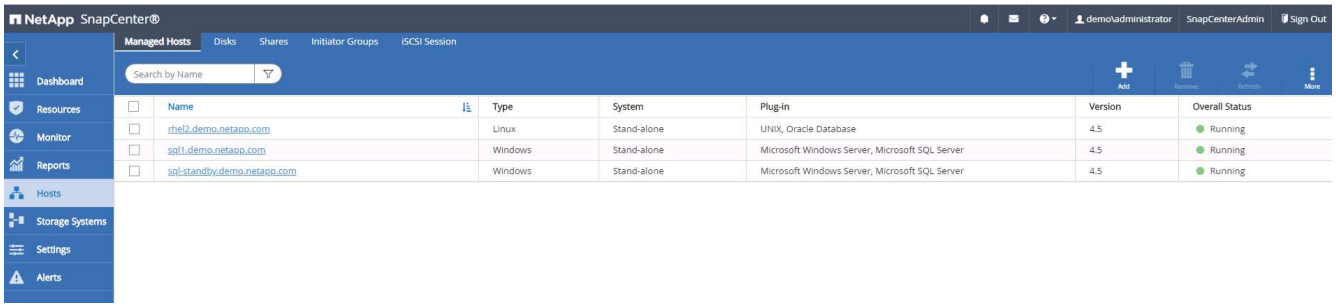


7. Cliquez sur Parcourir pour découvrir le stockage NetApp afin qu'un répertoire de journaux puisse être défini ; SnapCenter utilise ce répertoire de journaux pour regrouper les fichiers journaux des transactions du serveur SQL. Cliquez ensuite sur Enregistrer.

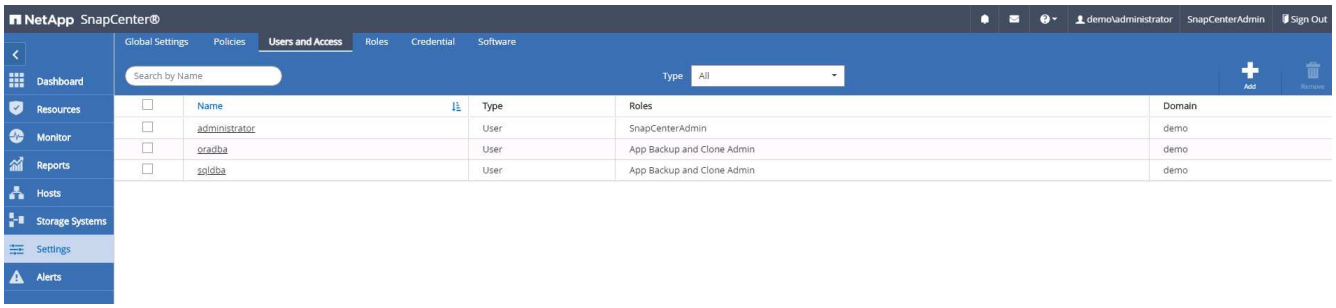


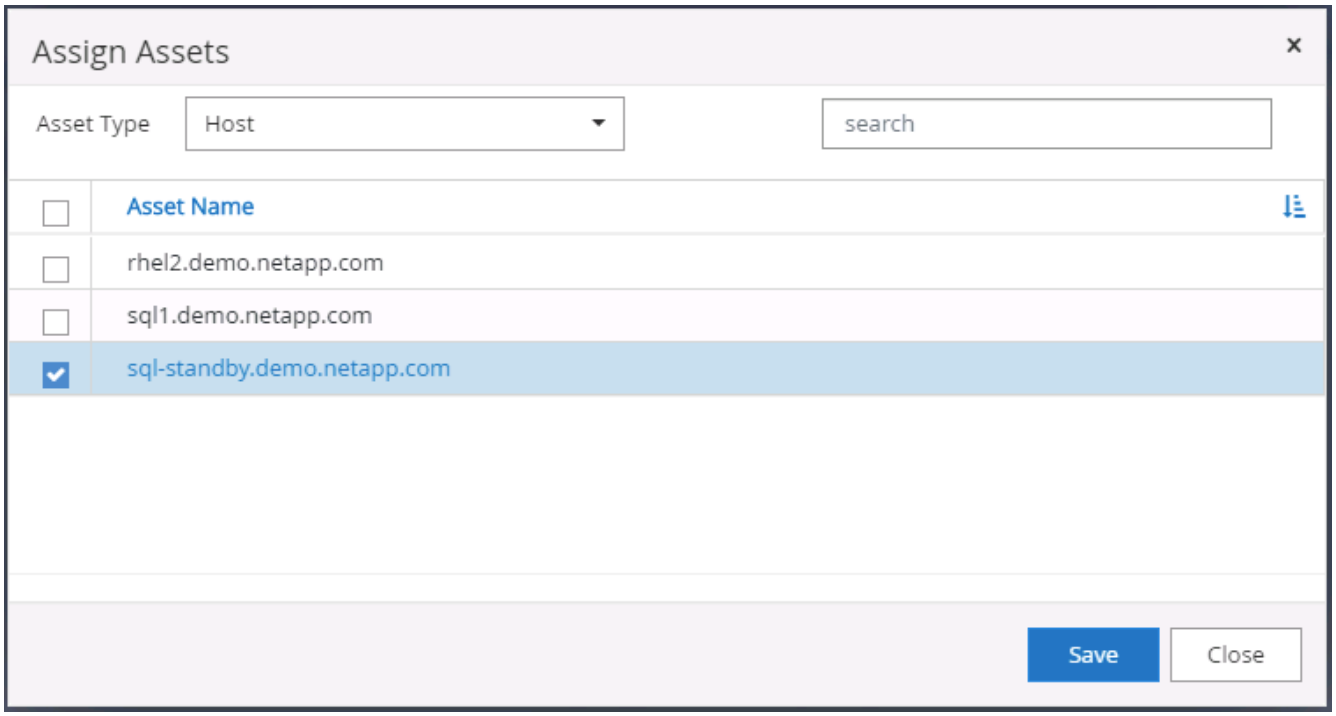
Pour que le stockage NetApp provisionné sur un hôte de base de données soit découvert, le stockage (sur site ou CVO) doit être ajouté à SnapCenter, comme illustré à l'étape 6 pour CVO à titre d'exemple.

8. Une fois le répertoire du journal configuré, l'état général du plug-in hôte Windows est modifié sur En cours d'exécution.



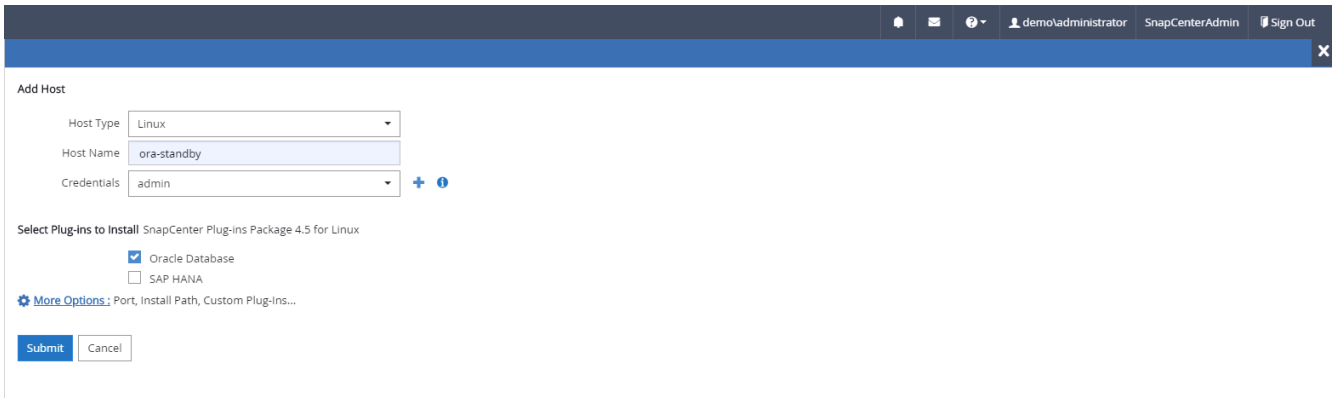
9. Pour affecter l'hôte à l'ID utilisateur de gestion de base de données, accédez à l'onglet Accès sous Paramètres et Utilisateurs, cliquez sur l'ID utilisateur de gestion de base de données (dans notre cas, le sqldba auquel l'hôte doit être affecté) et cliquez sur Enregistrer pour terminer l'affectation des ressources de l'hôte.



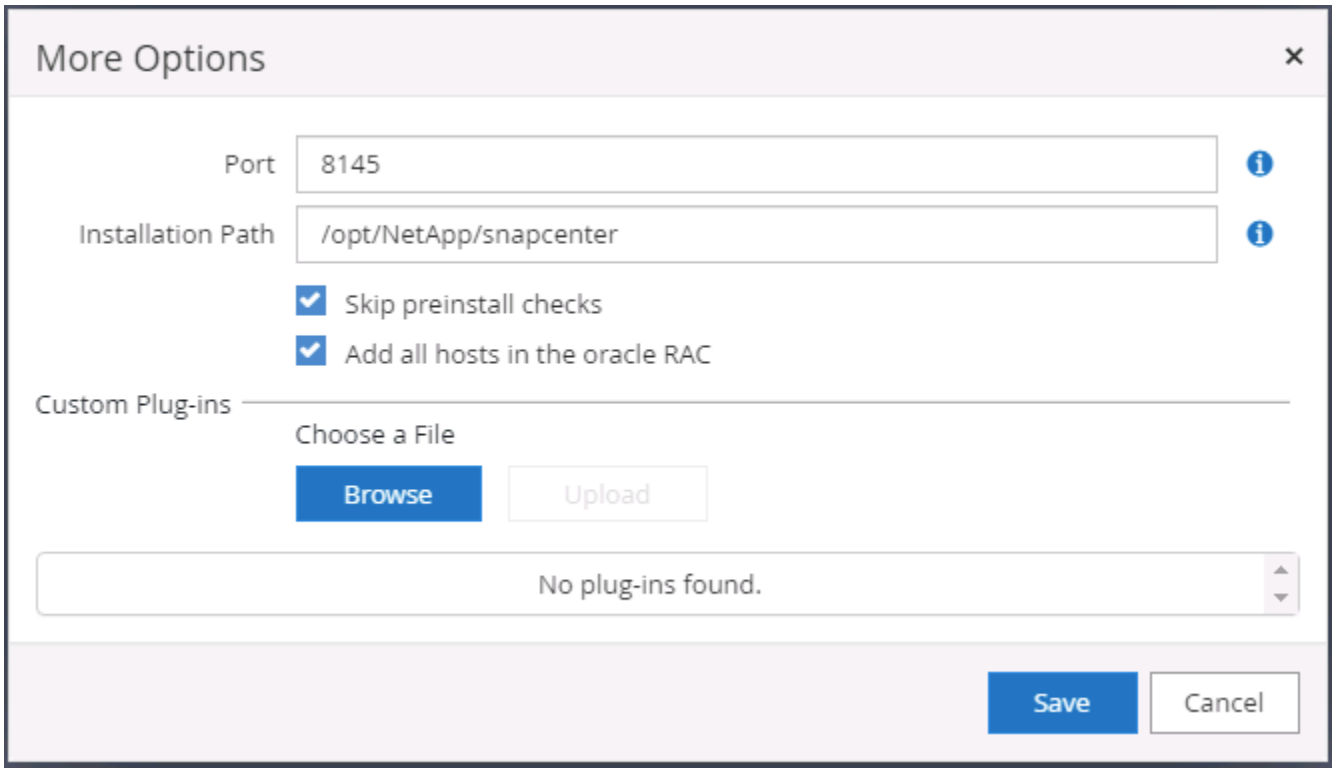


Ajout d'un hôte Unix et installation du plugin sur l'hôte

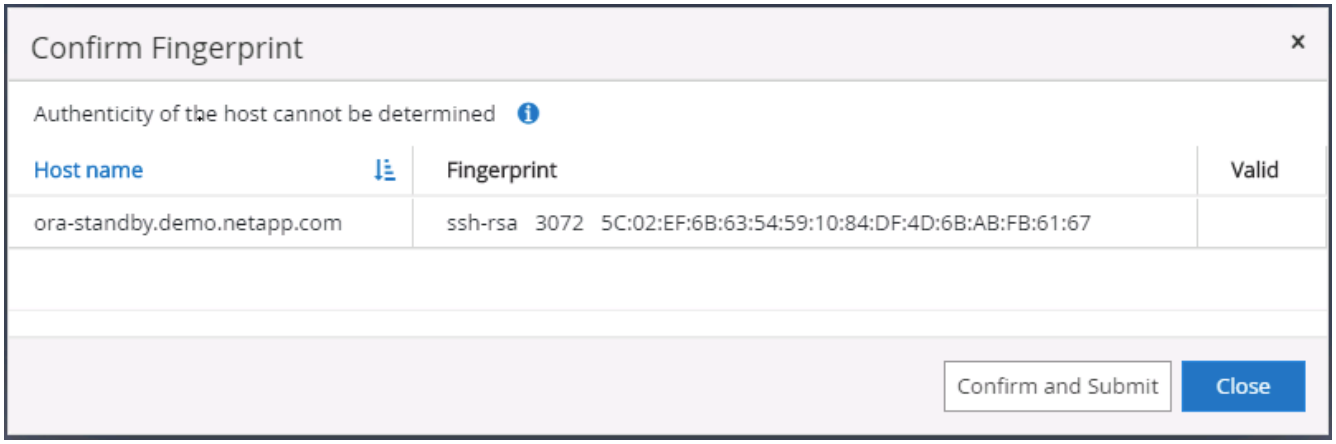
1. Connectez-vous à SnapCenter avec un identifiant utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet Hôtes dans le menu de gauche, puis cliquez sur Ajouter pour ouvrir le flux de travail Ajouter un hôte.
3. Choisissez Linux comme type d'hôte. Le nom d'hôte peut être soit le nom 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. Cochez Oracle Database comme plug-in à installer, qui installe les plug-ins hôtes Oracle et Linux.



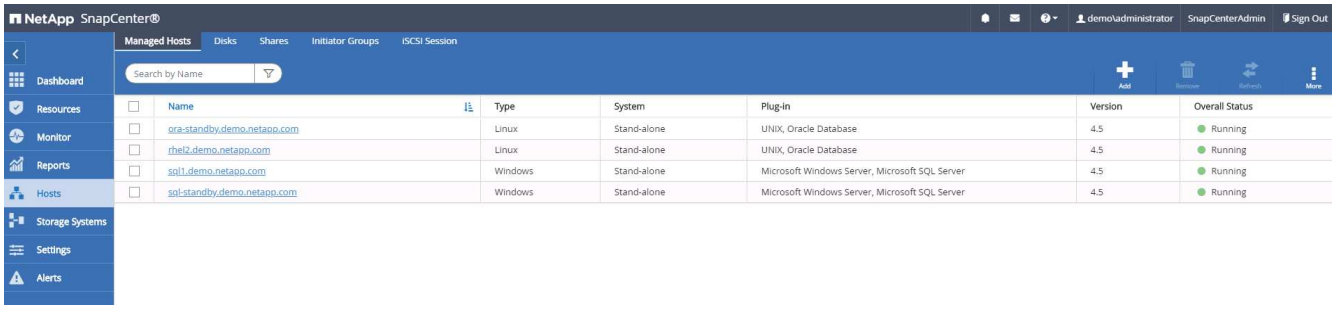
4. Cliquez sur Plus d'options et sélectionnez « Ignorer les vérifications de préinstallation ». Vous êtes invité à confirmer l'omission de la vérification de préinstallation. Cliquez sur Oui, puis sur Enregistrer.



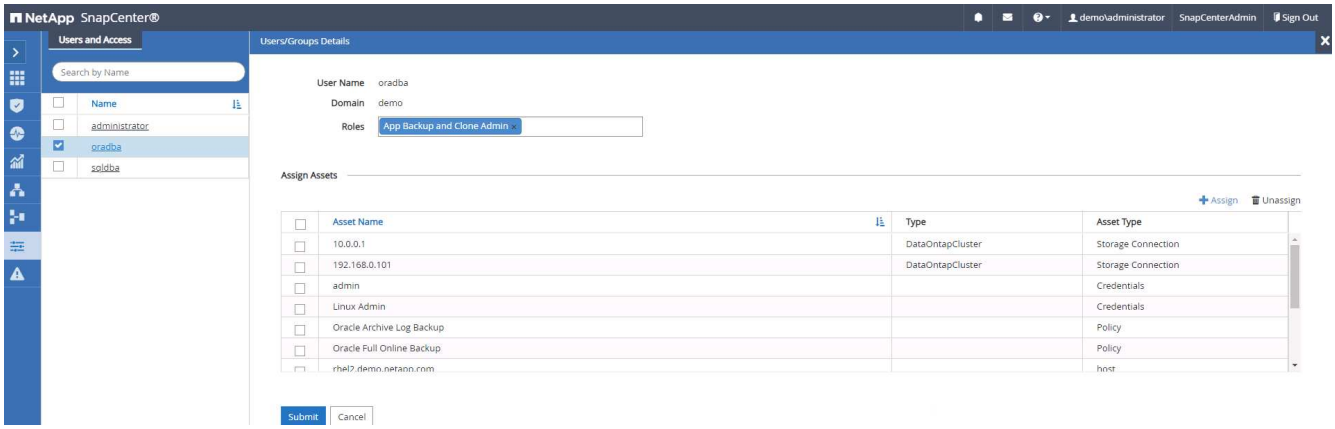
5. Cliquez sur Soumettre pour démarrer l'installation du plugin. Vous êtes invité à confirmer l'empreinte digitale comme indiqué ci-dessous.

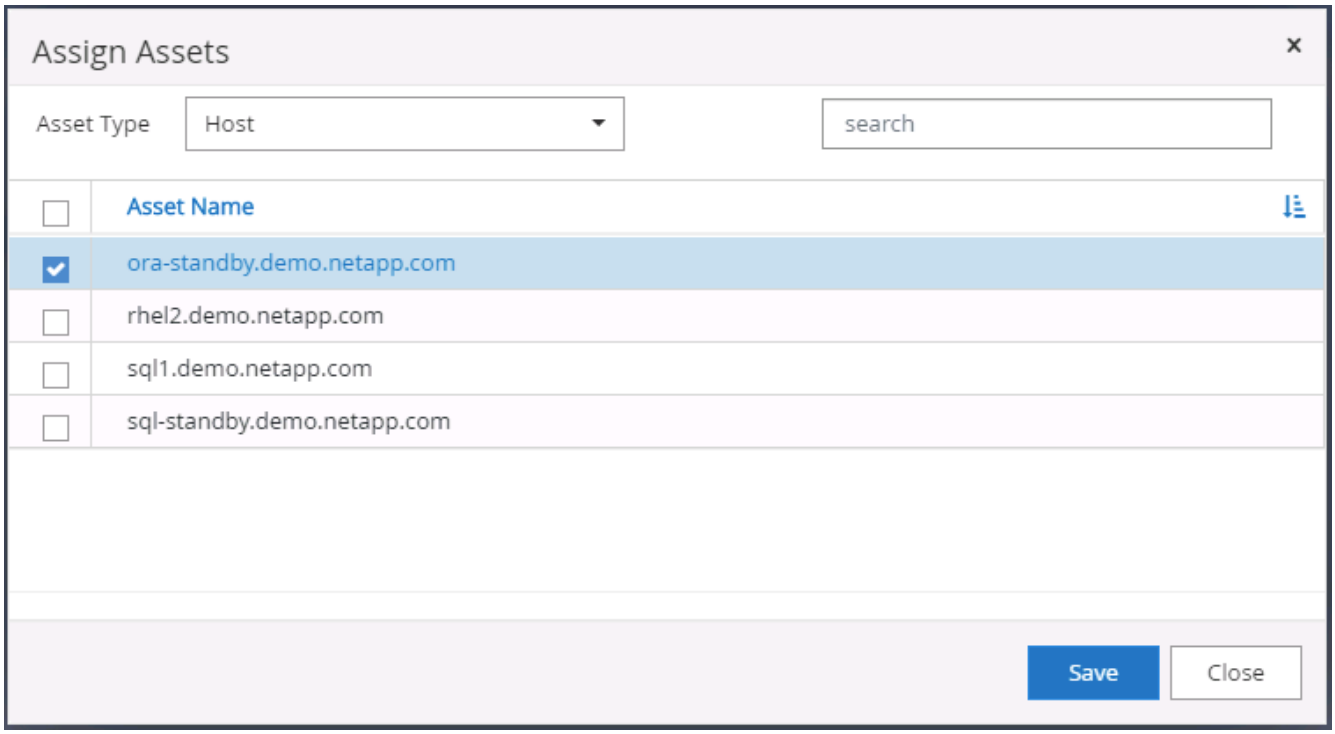


6. SnapCenter effectue la validation et l'enregistrement de l'hôte, puis le plug-in est installé sur l'hôte Linux. Le statut est passé de Installation du plugin à En cours d'exécution.



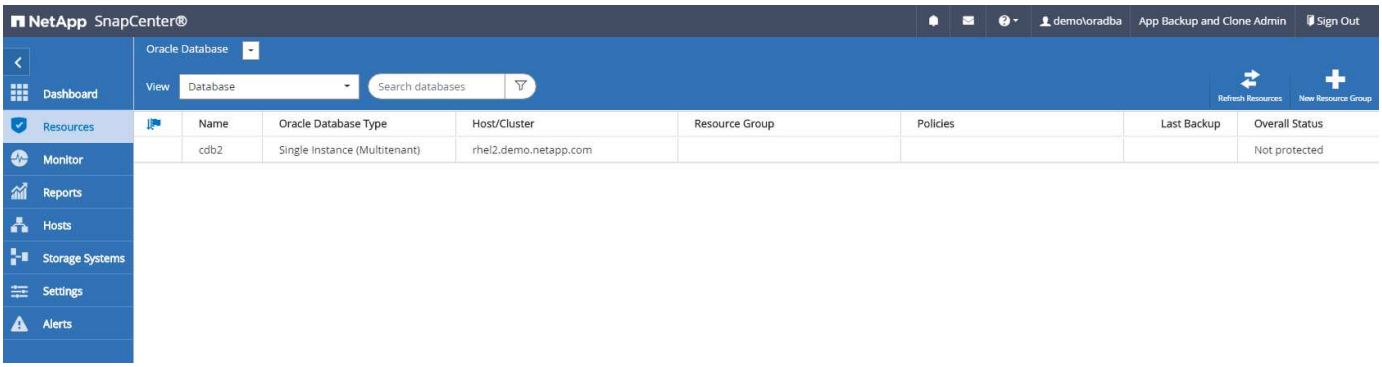
7. Affectez l'hôte nouvellement ajouté à l'ID utilisateur de gestion de base de données approprié (dans notre cas, oradba).





4. Découverte de ressources de base de données

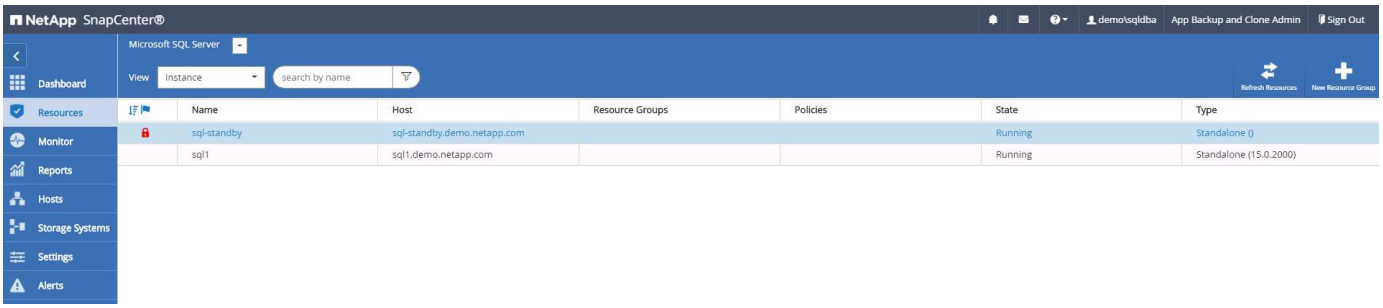
Avec une installation réussie du plugin, les ressources de la base de données sur l'hôte peuvent être immédiatement découvertes. Cliquez sur l'onglet Ressources dans le menu de gauche. Selon le type de plate-forme de base de données, un certain nombre de vues sont disponibles, telles que la base de données,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

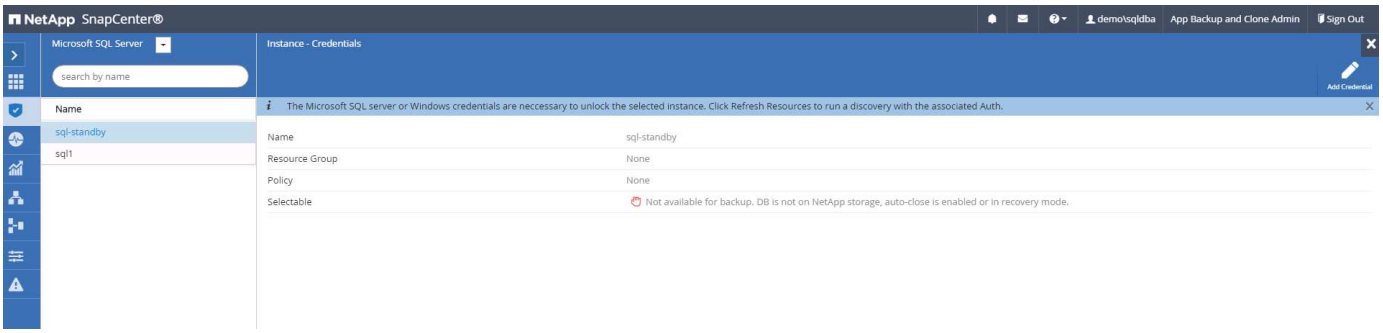


Lorsque la base de données est initialement découverte, l'état général est affiché comme « Non protégé ». La capture d'écran précédente montre une base de données Oracle non encore protégée par une politique de sauvegarde.

Lorsqu'une configuration ou une politique de sauvegarde est configurée et qu'une sauvegarde a été exécutée, l'état général de la base de données affiche l'état de la sauvegarde comme « 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 administrateur système à une instance de base de données, les informations d'identification de la base de données doivent être reconfigurées pour déverrouiller le verrou rouge.





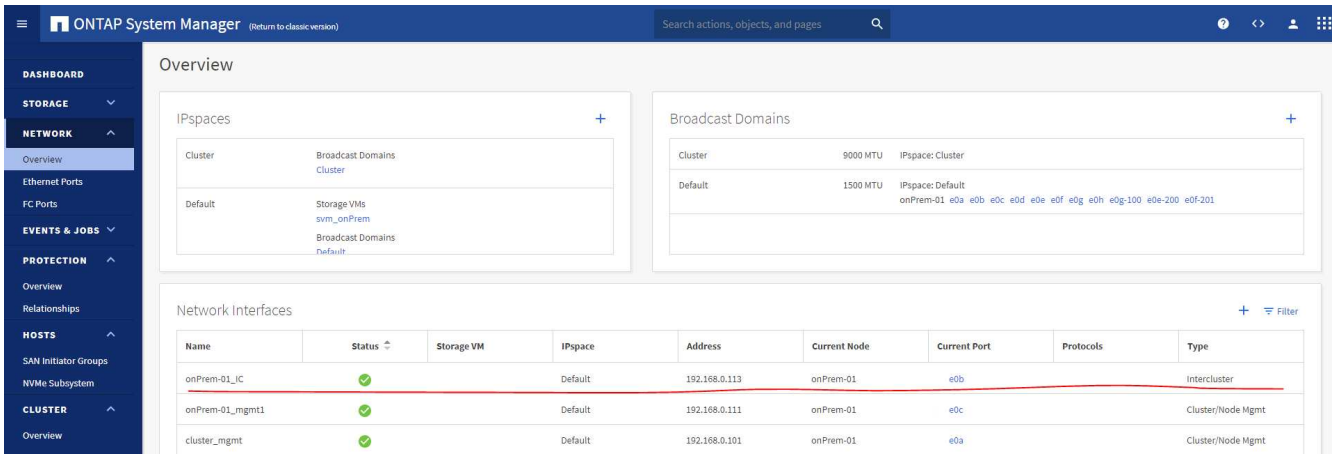
Une fois les informations d'identification appropriées configurées au niveau Windows ou au niveau de la base de données, le cadenas rouge disparaît et les informations de type SQL Server sont collectées et examinées.

5. Configurer l'appairage des clusters de stockage et la réplication des volumes de base de données

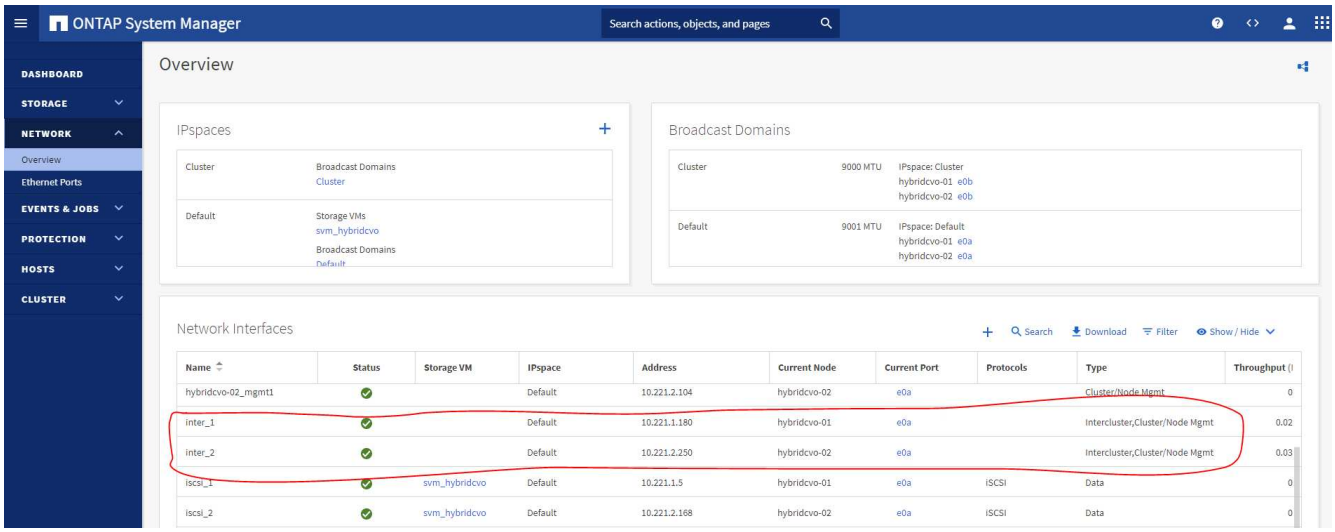
Pour protéger vos données de base de données sur site en utilisant un cloud public comme destination cible, les volumes de base de données de cluster ONTAP sur site sont répliqués sur le CVO cloud à l'aide de la technologie NetApp SnapMirror . Les volumes cibles répliqués peuvent ensuite être clonés pour DEV/OPS ou la reprise après sinistre. Les étapes de haut niveau suivantes vous permettent de configurer l'appairage de cluster et la réplication des volumes de base de données.

1. Configurez les LIF intercluster pour l'appairage de cluster sur le cluster local et l'instance de cluster CVO. Cette étape peut être réalisée avec ONTAP System Manager. Un déploiement CVO par défaut a des LIF inter-cluster configurés automatiquement.

   Cluster sur site :



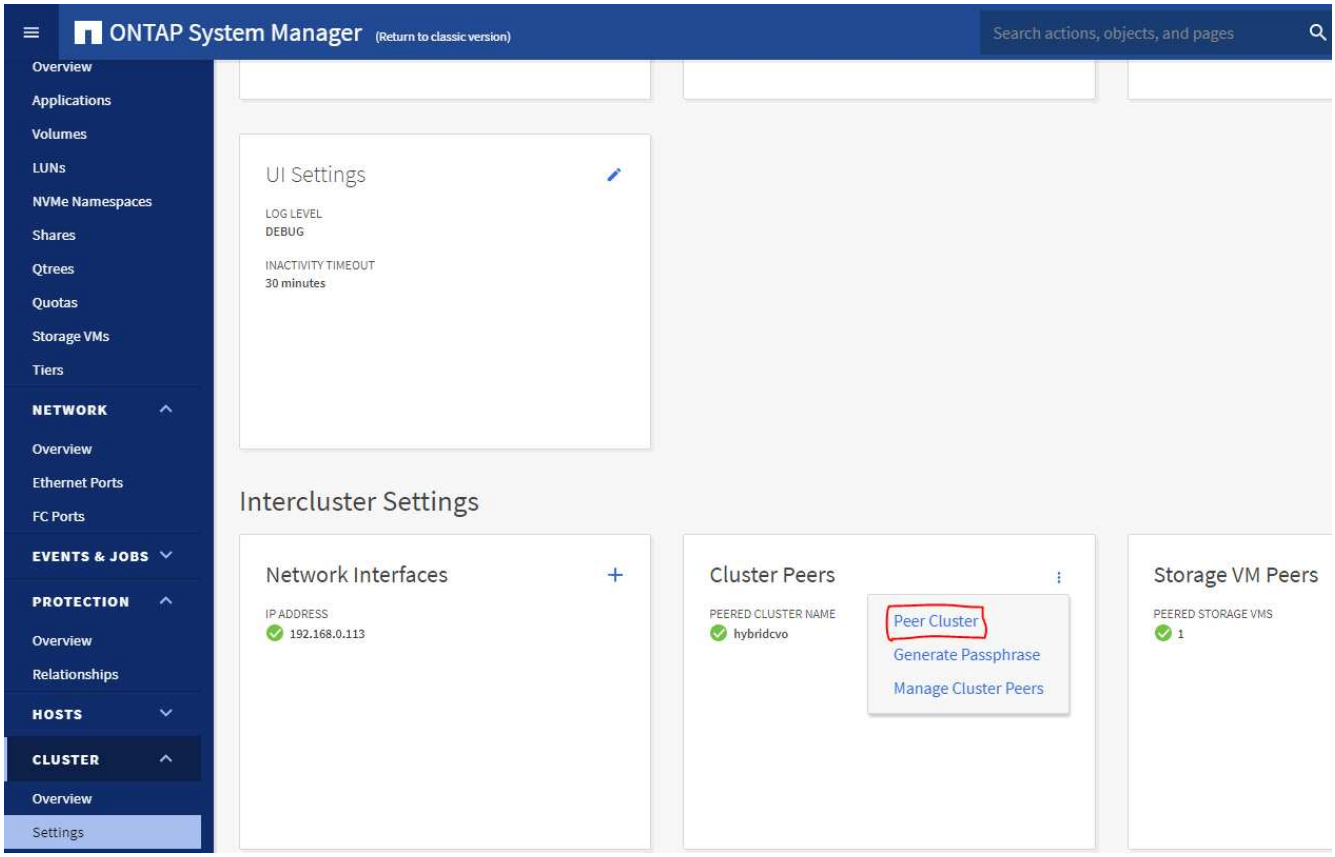
   Cluster CVO cible :



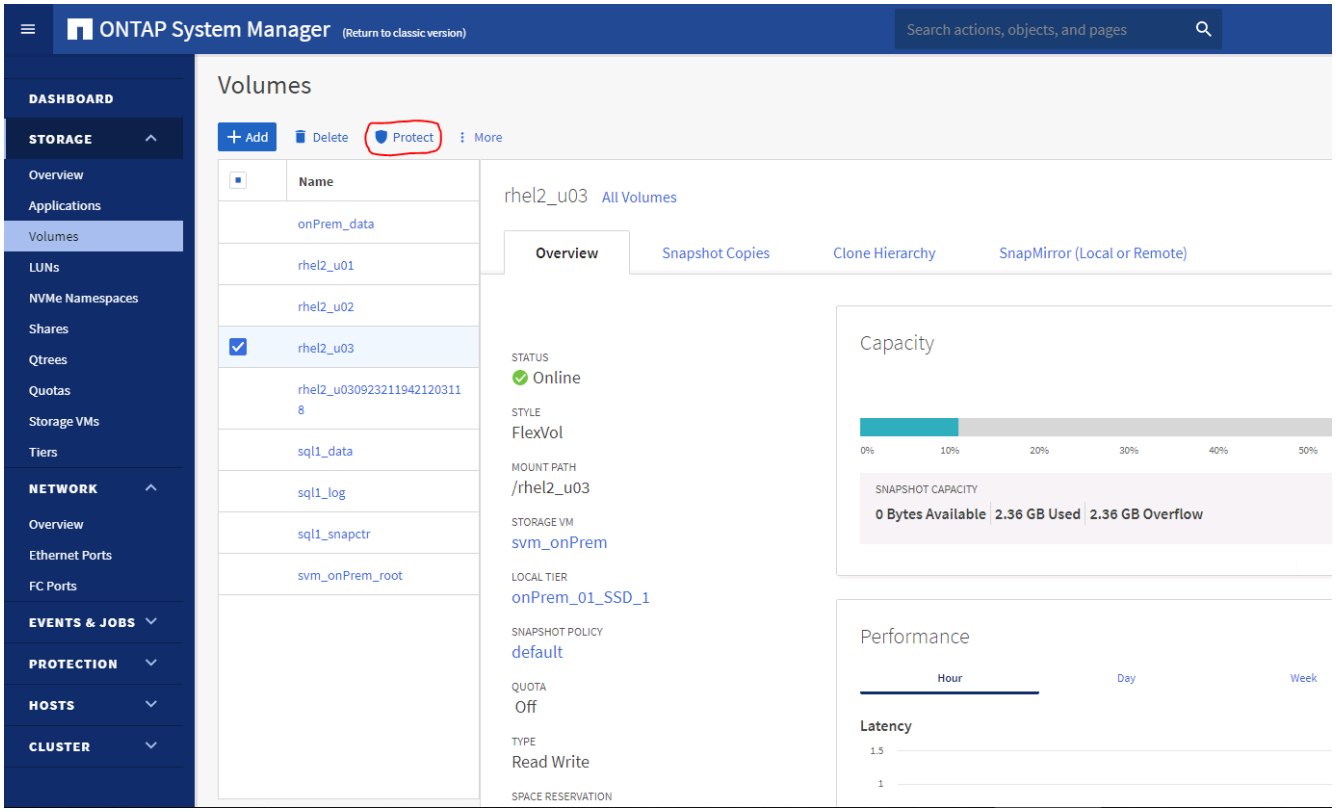
2. Une fois les LIF intercluster configurés, l'appairage de cluster et la réplication de volume peuvent être configurés à l'aide de la fonction glisser-déposer dans NetApp Cloud Manager. Voir"Premiers pas - Cloud public AWS" pour plus de détails.

   Alternativement, l'appairage de cluster et la réplication de volume de base de données peuvent être effectués à l'aide d' ONTAP System Manager comme suit :

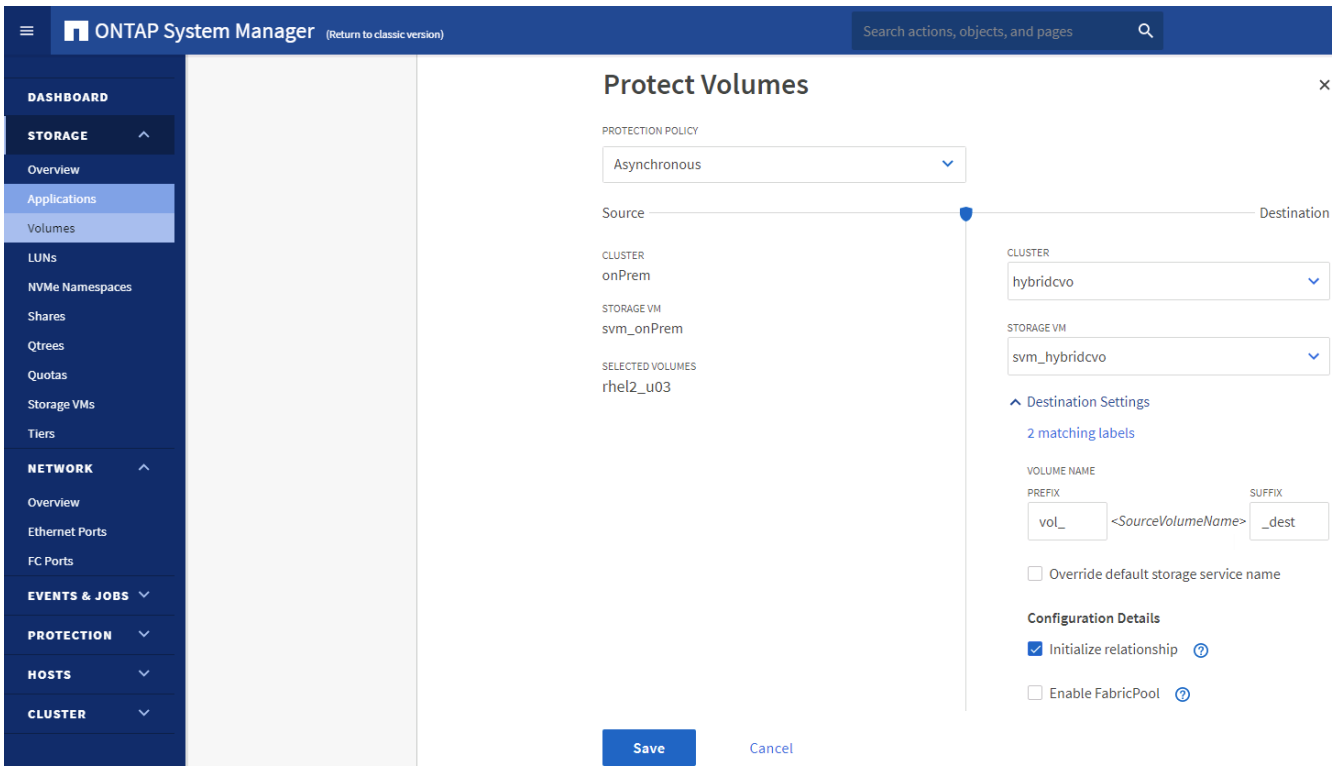
3. Connectez-vous à ONTAP System Manager. Accédez à Cluster > Paramètres et cliquez sur Cluster homologue pour configurer l'appairage de cluster avec l'instance CVO dans le cloud.



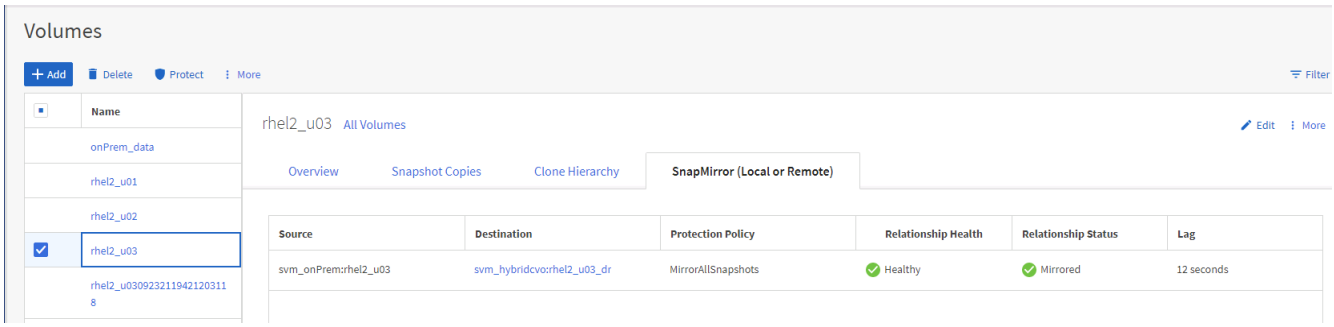
4. Accédez à l'onglet Volumes. Sélectionnez le volume de base de données à répliquer et cliquez sur Protéger.



5. Définissez la politique de protection sur Asynchrone. Sélectionnez le cluster de destination et le SVM de stockage.

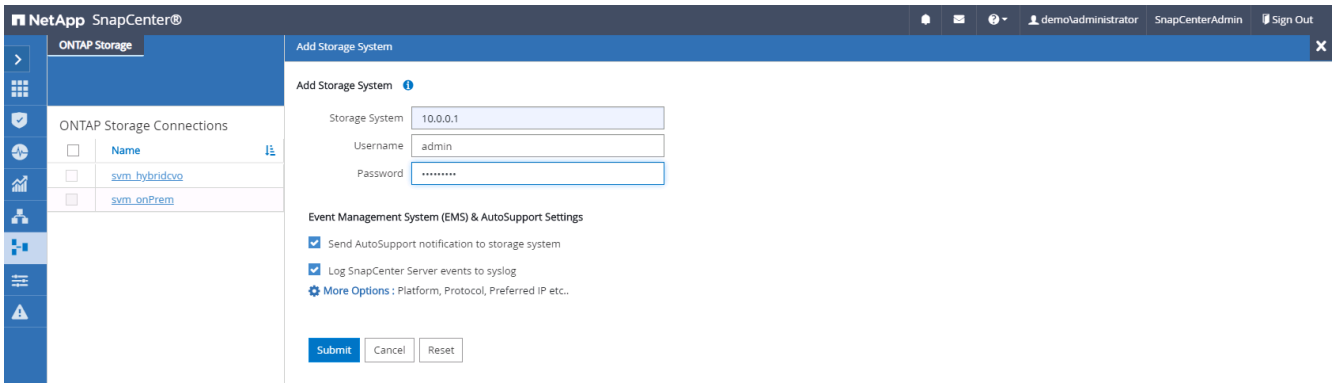


6. Validez que le volume est synchronisé entre la source et la cible et que la relation de réplication est saine.

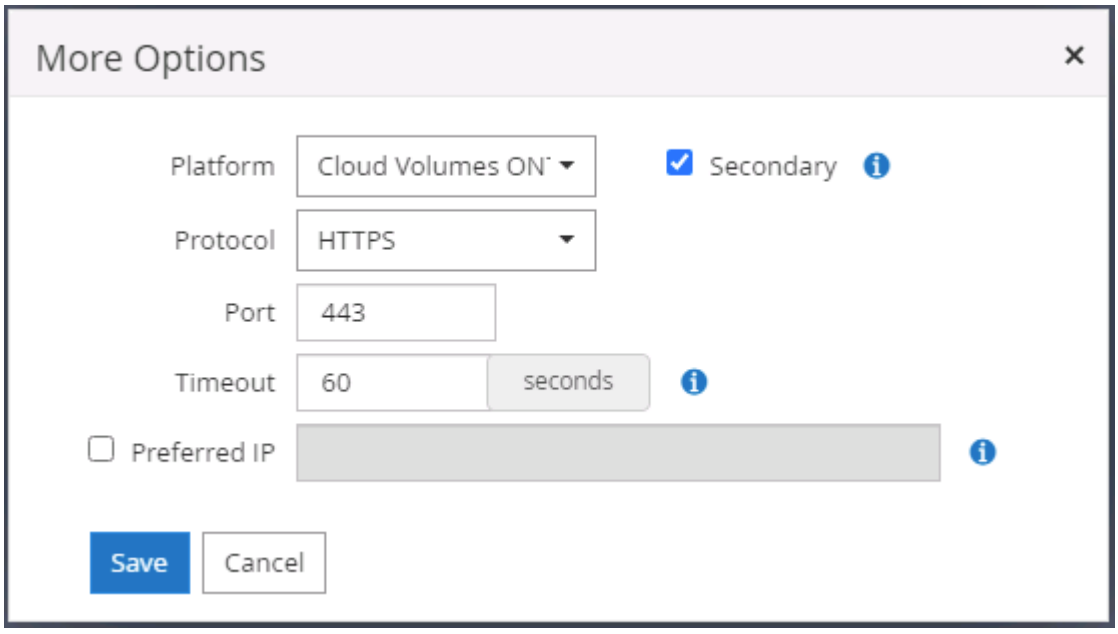


6. Ajouter un stockage de base de données CVO SVM à SnapCenter

1. Connectez-vous à SnapCenter avec un identifiant utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet Système de stockage dans le menu, puis cliquez sur Nouveau pour ajouter une SVM de stockage CVO qui héberge des volumes de base de données cibles répliqués à SnapCenter. Saisissez l'adresse IP de gestion du cluster dans le champ Système de stockage, puis saisissez le nom d'utilisateur et le mot de passe appropriés.

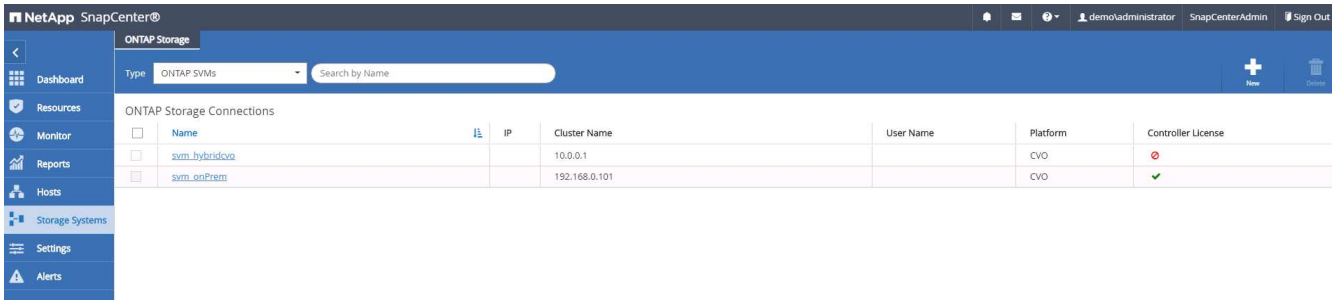


3. Cliquez sur Plus d'options pour ouvrir des options de configuration de stockage supplémentaires. Dans le champ Plateforme, sélectionnez Cloud Volumes ONTAP, cochez Secondaire, puis cliquez sur Enregistrer.



4. Affectez les systèmes de stockage aux ID utilisateur de gestion de base de données SnapCenter comme

indiqué dans3. Installation du plug-in hôte SnapCenter .

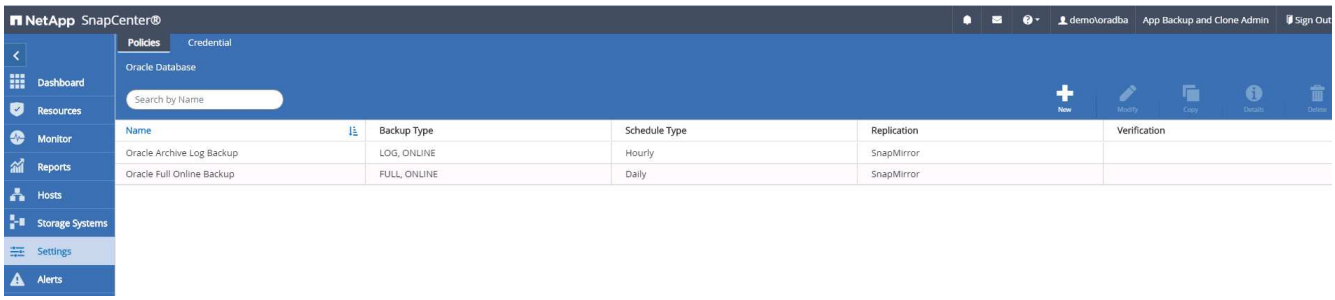


7. Configurer la politique de sauvegarde de la base de données dans SnapCenter

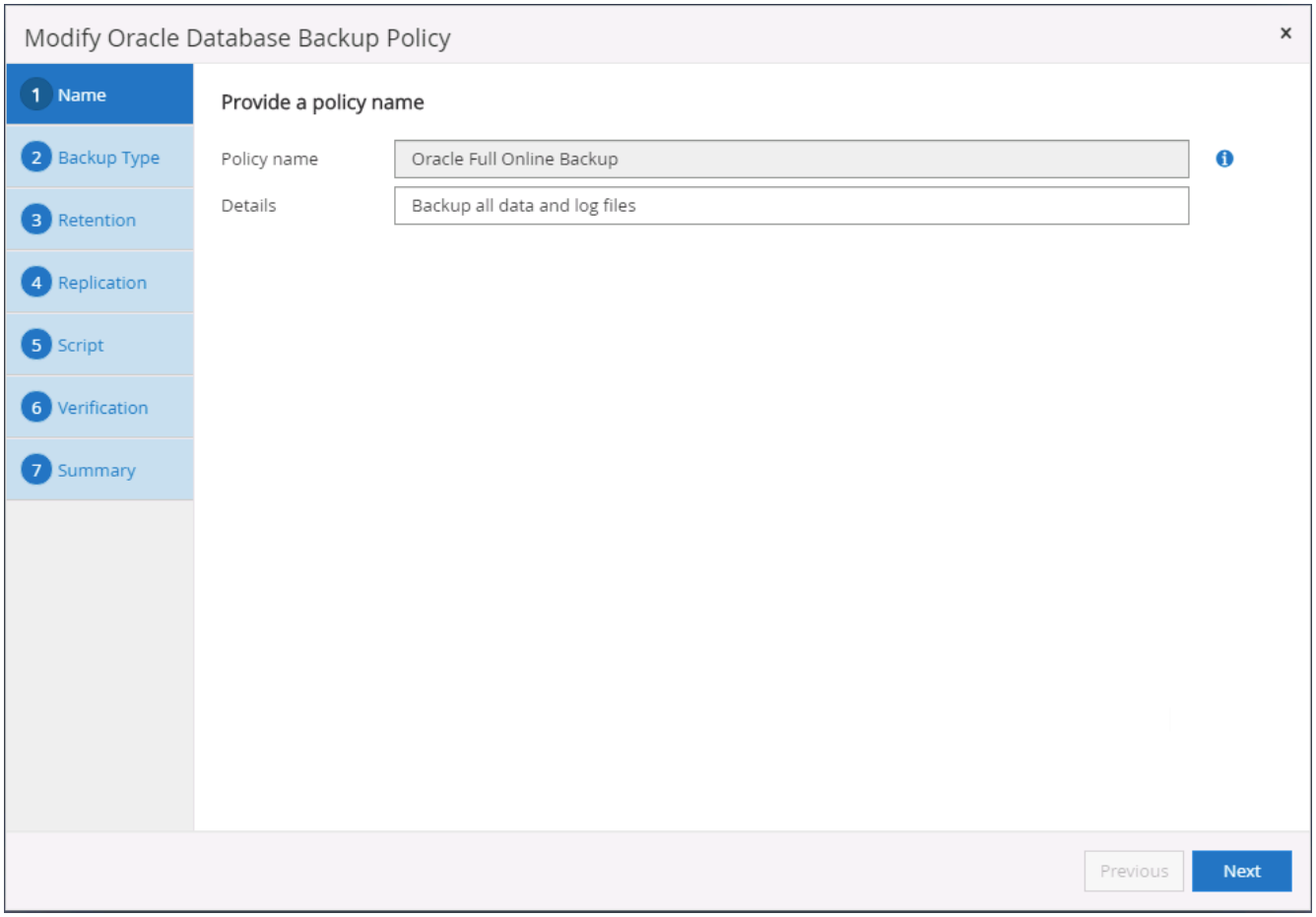
Les procédures suivantes montrent comment créer une politique de sauvegarde complète de base de données ou de fichier journal. La politique peut ensuite être mise en œuvre pour protéger les ressources des bases de données. L'objectif de point de récupération (RPO) ou l'objectif de temps de récupération (RTO) dicte la fréquence des sauvegardes de la base de données et/ou du journal.

Créer une politique de sauvegarde complète de la base de données pour Oracle

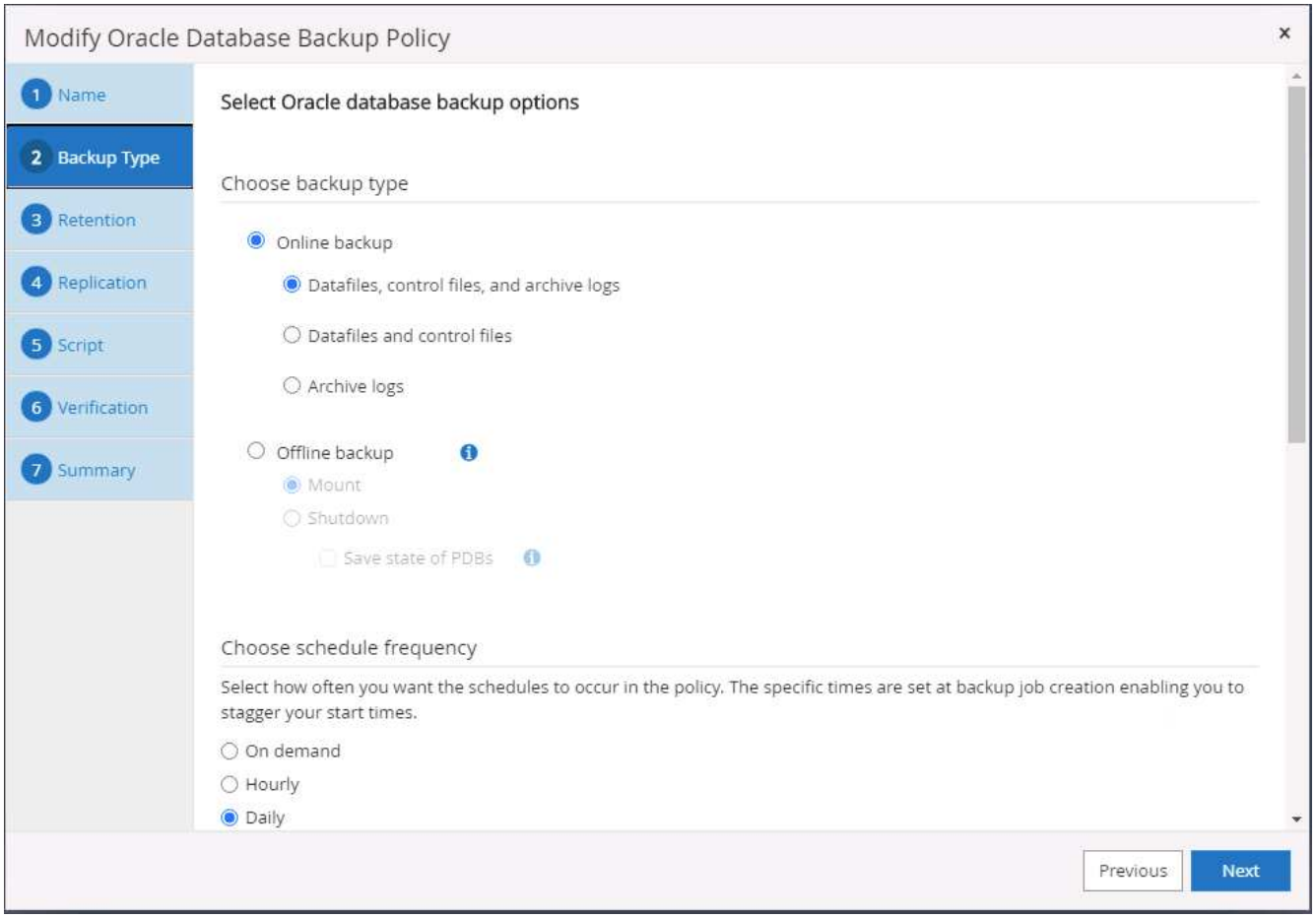
1. Connectez-vous à SnapCenter en tant qu'ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur Politiques.



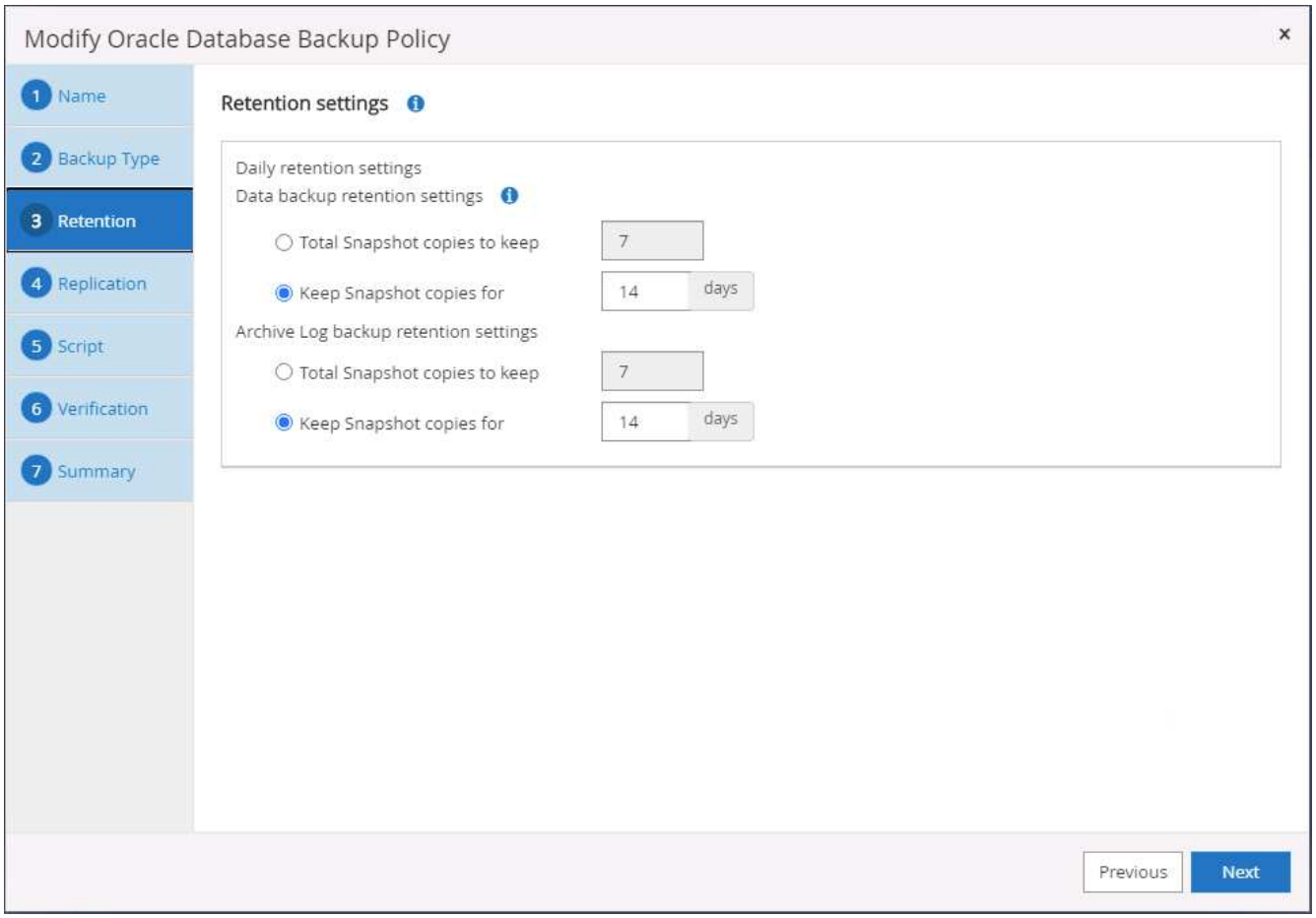
2. Cliquez sur Nouveau pour lancer un nouveau flux de travail de création de politique de sauvegarde ou choisissez une politique existante à modifier.



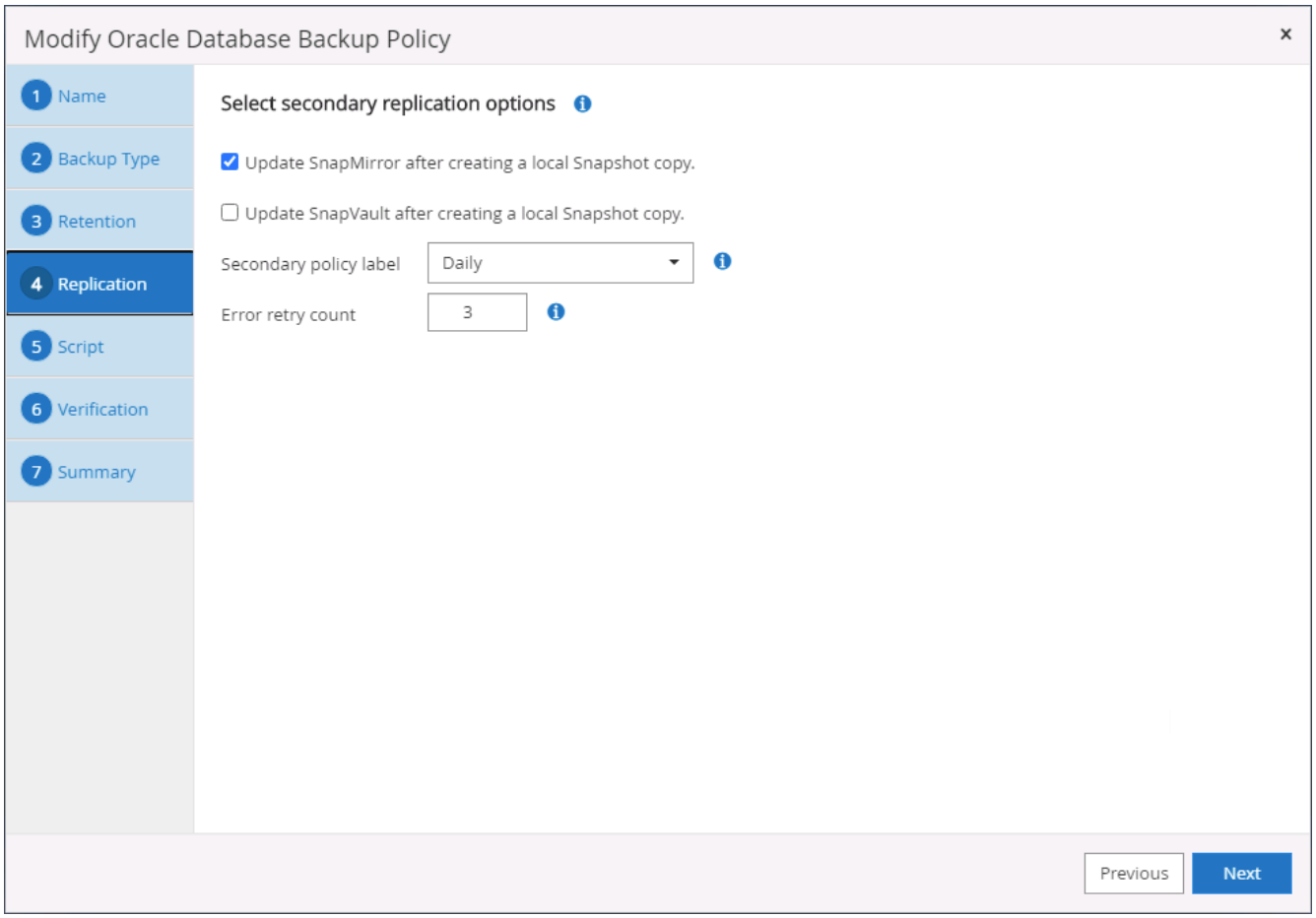
3. Sélectionnez le type de sauvegarde et la fréquence de planification.



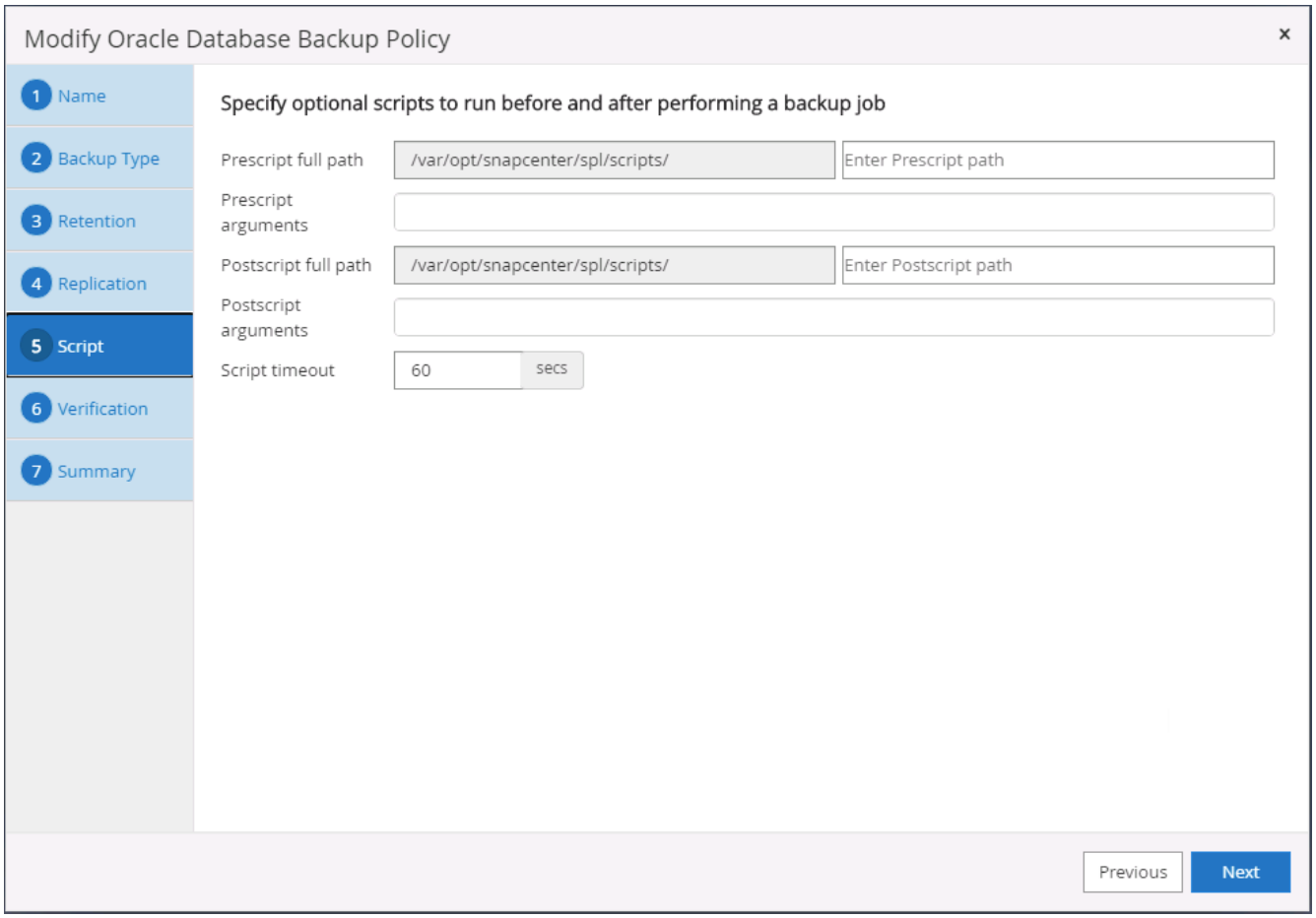
4. Définissez le paramètre de conservation des sauvegardes. Cela définit le nombre de copies de sauvegarde complètes de la base de données à conserver.



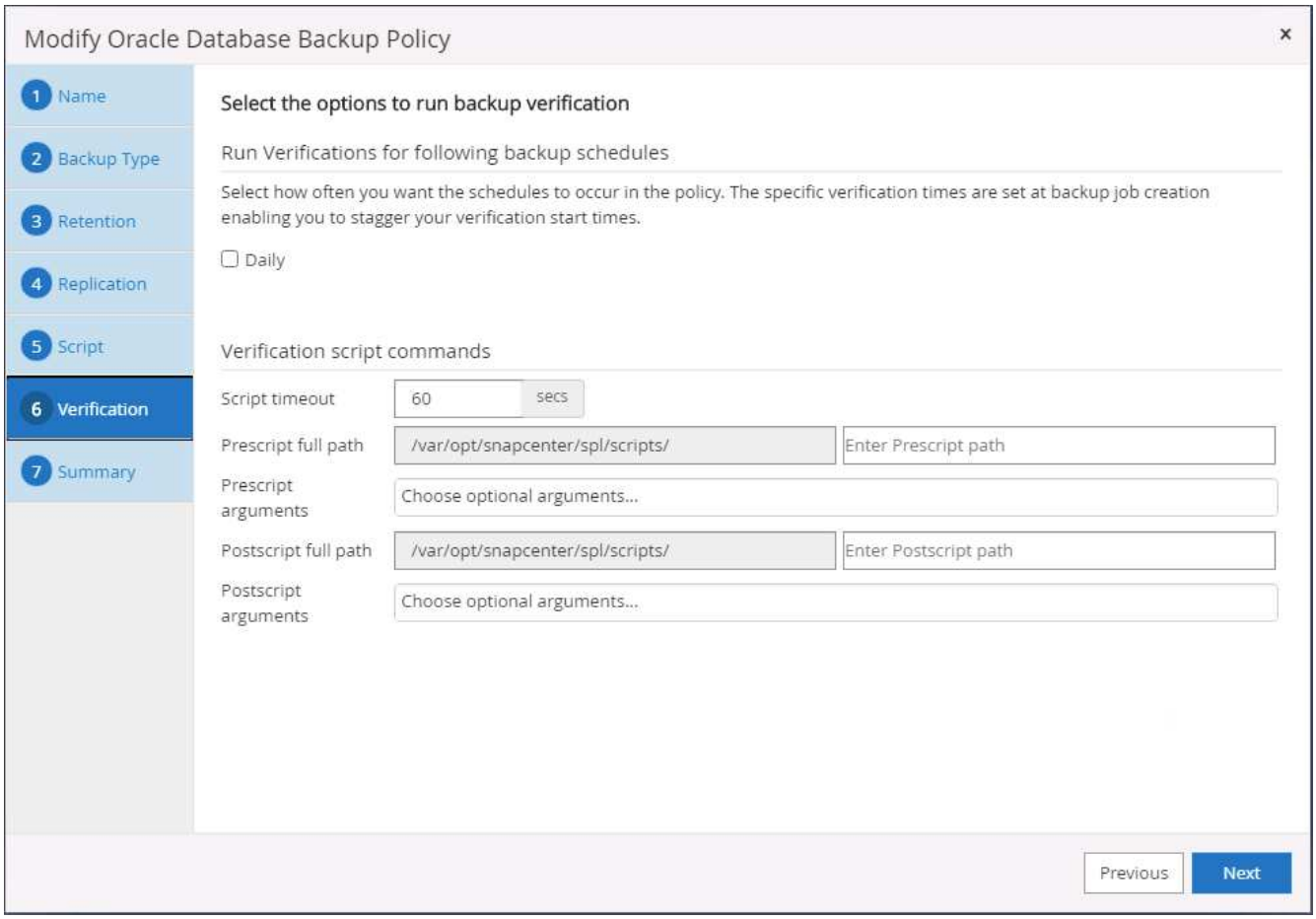
5. Sélectionnez les options de réplication secondaire pour pousser les sauvegardes de snapshots principaux locaux à répliquer vers un emplacement secondaire dans le cloud.



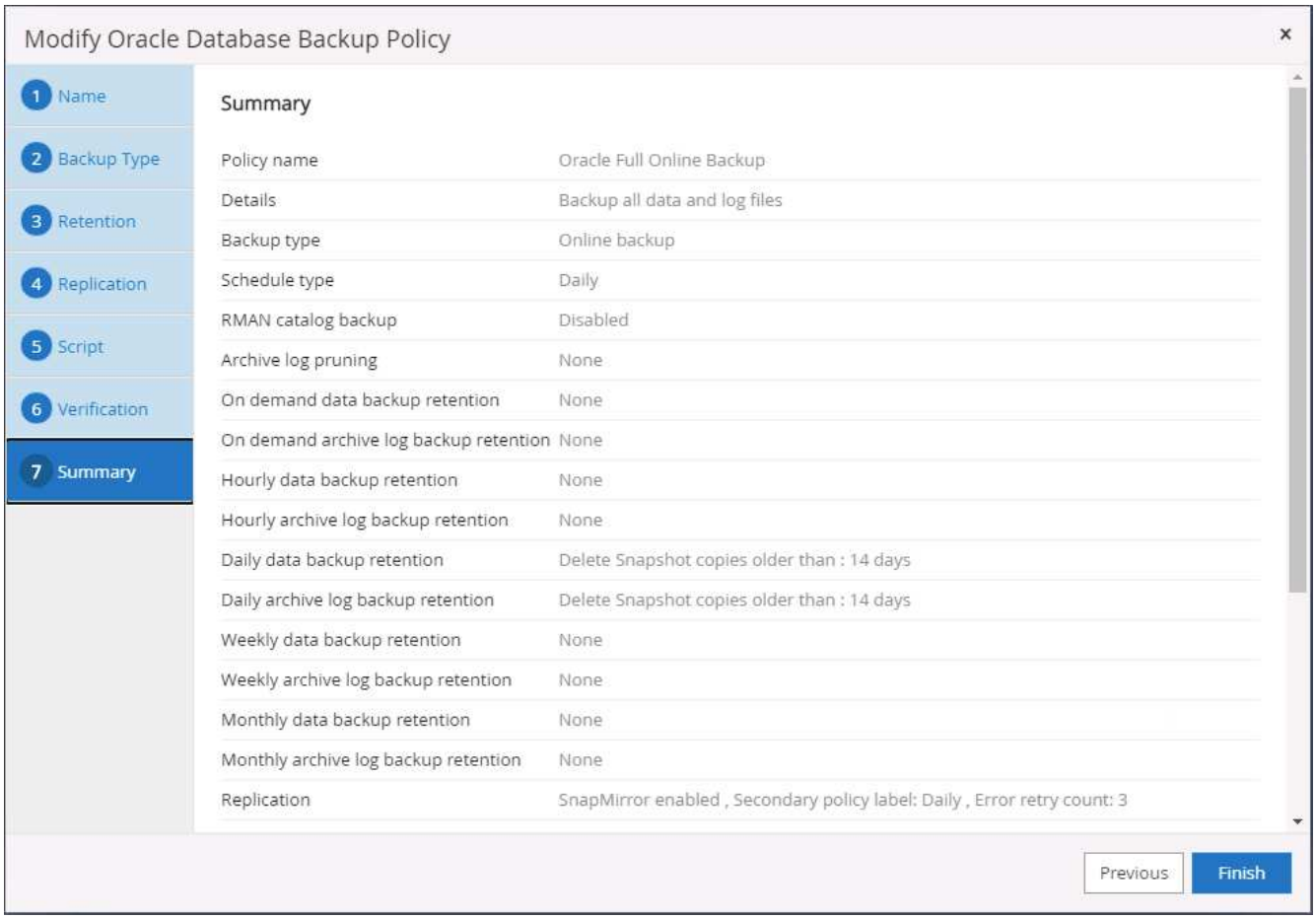
6. Spécifiez tout script facultatif à exécuter avant et après une exécution de sauvegarde.



7. Exécutez la vérification de sauvegarde si vous le souhaitez.

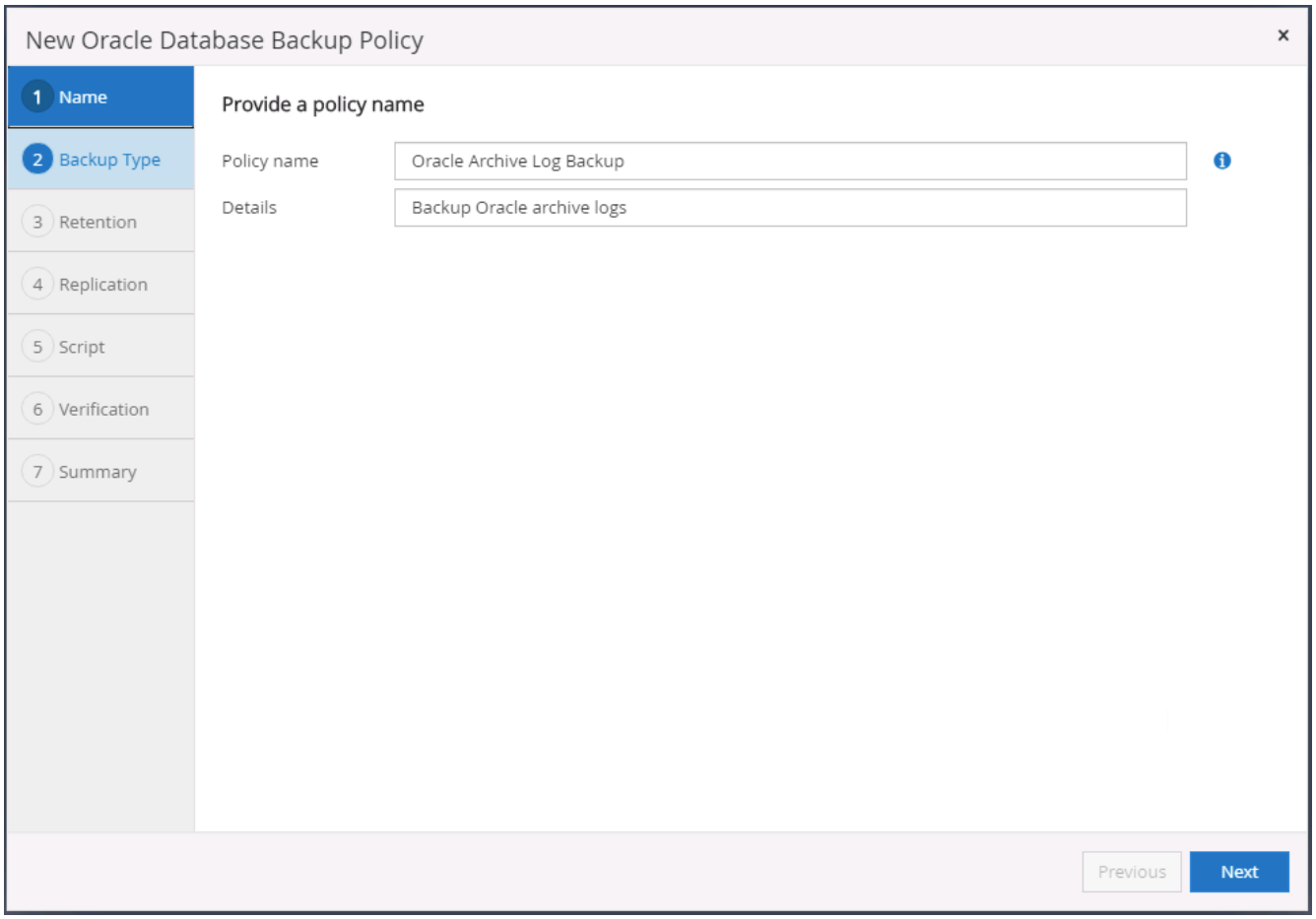

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Verification script commands
Script timeout
60
secs
Prescript full path
/var/opt/snapcenter/spl/scripts/
Enter Prescript path
Prescript arguments
Choose optional arguments...
Postscript full path
/var/opt/snapcenter/spl/scripts/
Enter Postscript path
Postscript arguments
Choose optional arguments...
Previous
Next

8. Résumé.

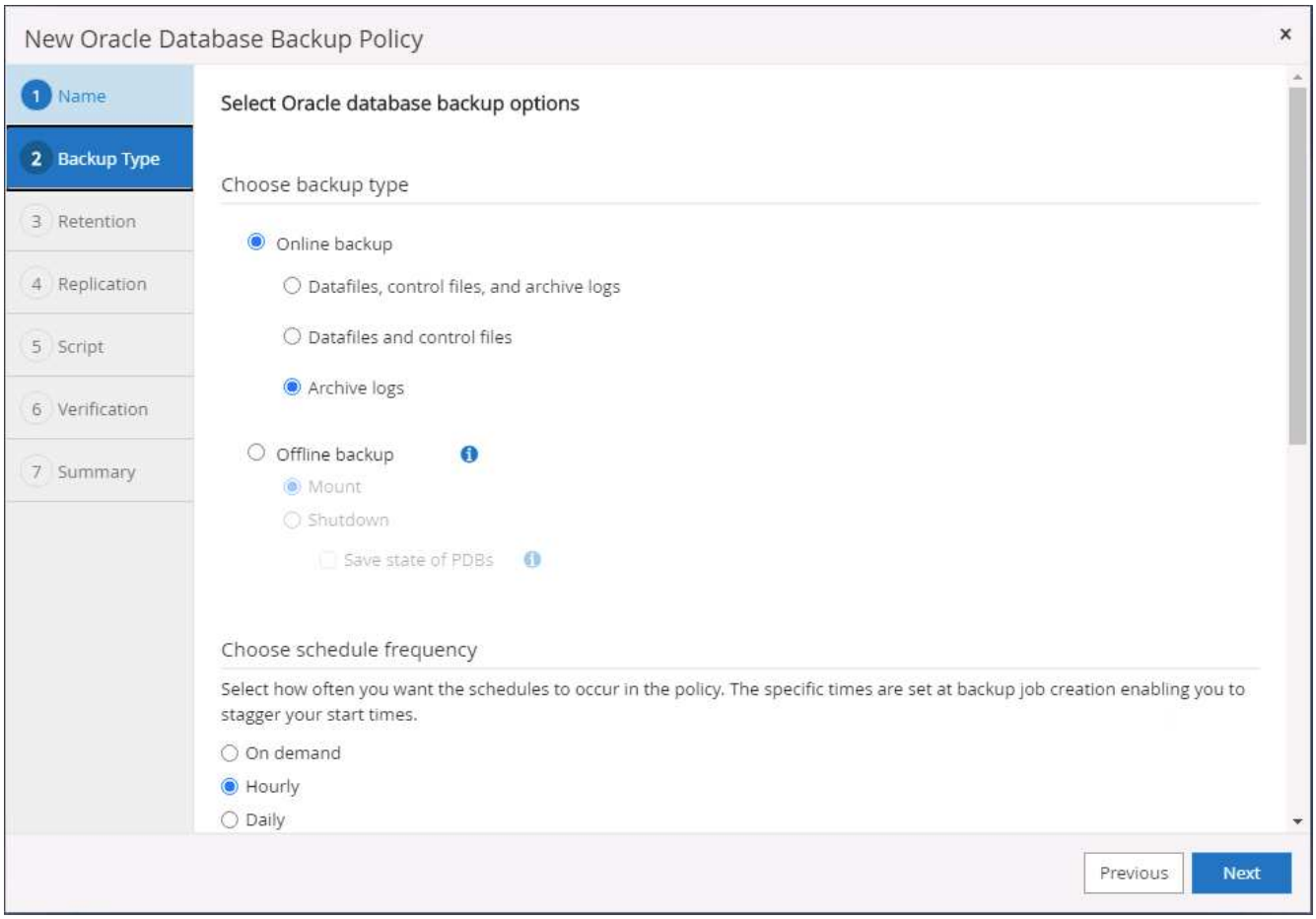


Créer une politique de sauvegarde du journal de base de données pour Oracle

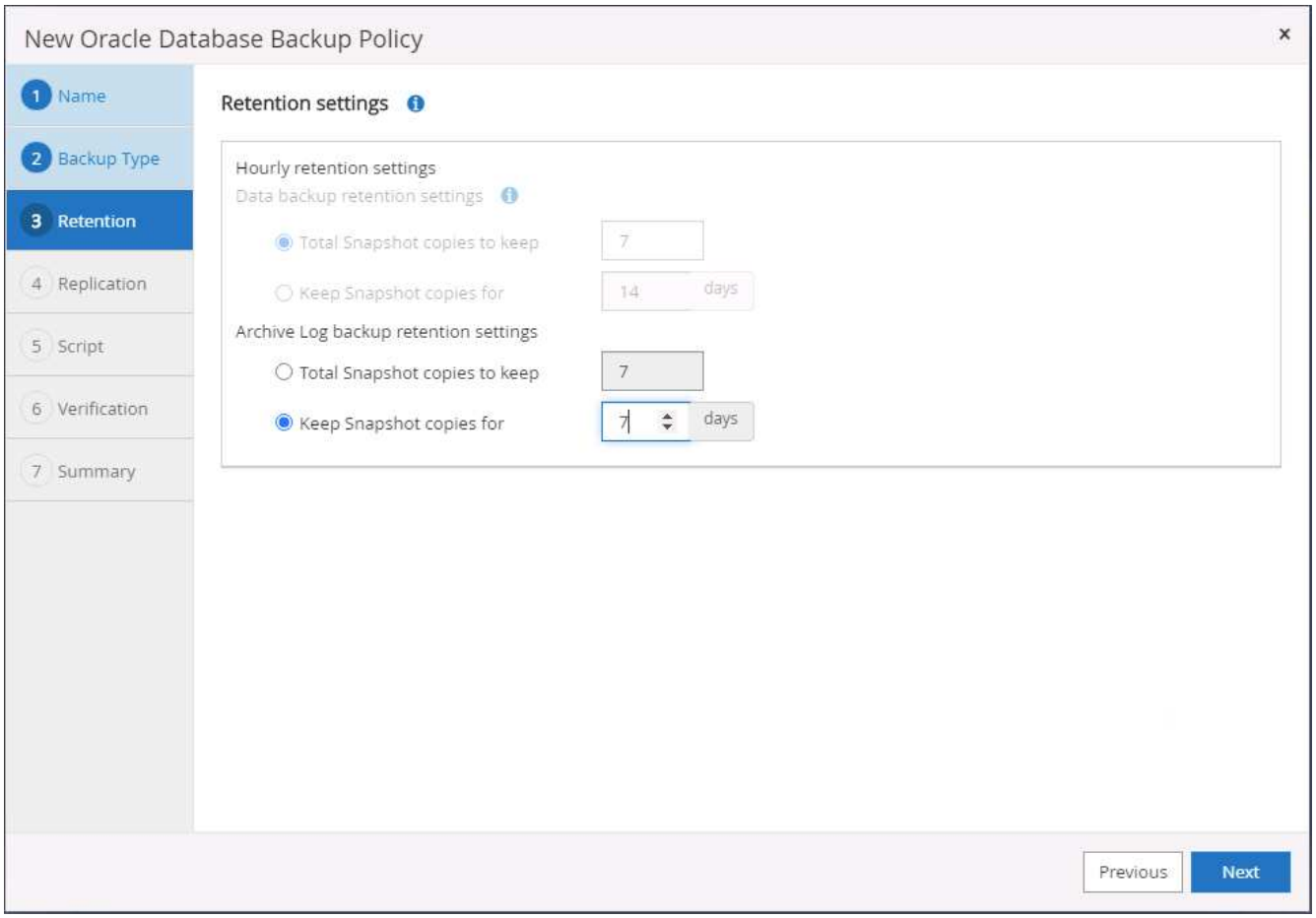
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur Politiques.
2. Cliquez sur Nouveau pour lancer un nouveau flux de travail de création de politique de sauvegarde ou choisissez une politique existante à modifier.



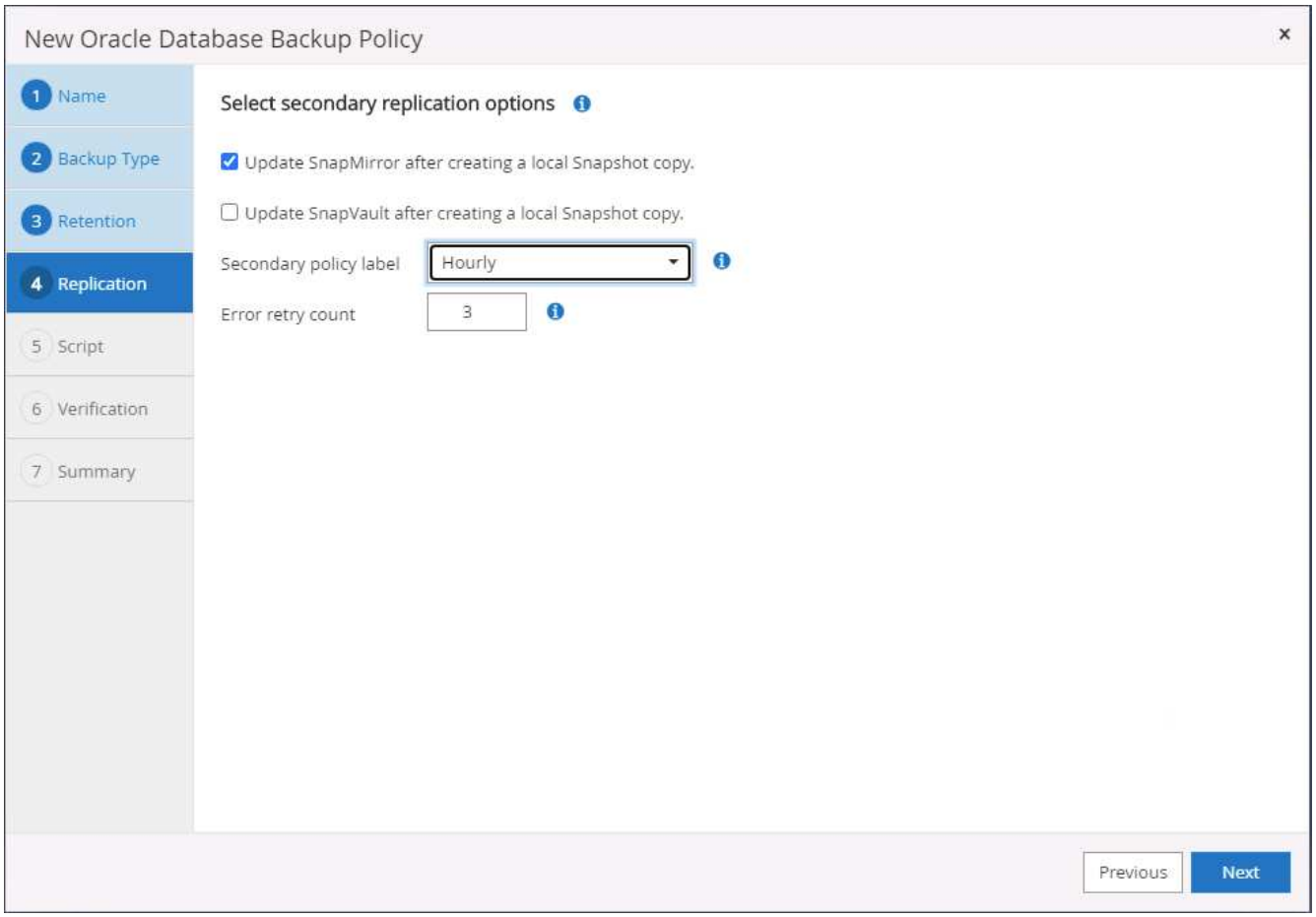
3. Sélectionnez le type de sauvegarde et la fréquence de planification.



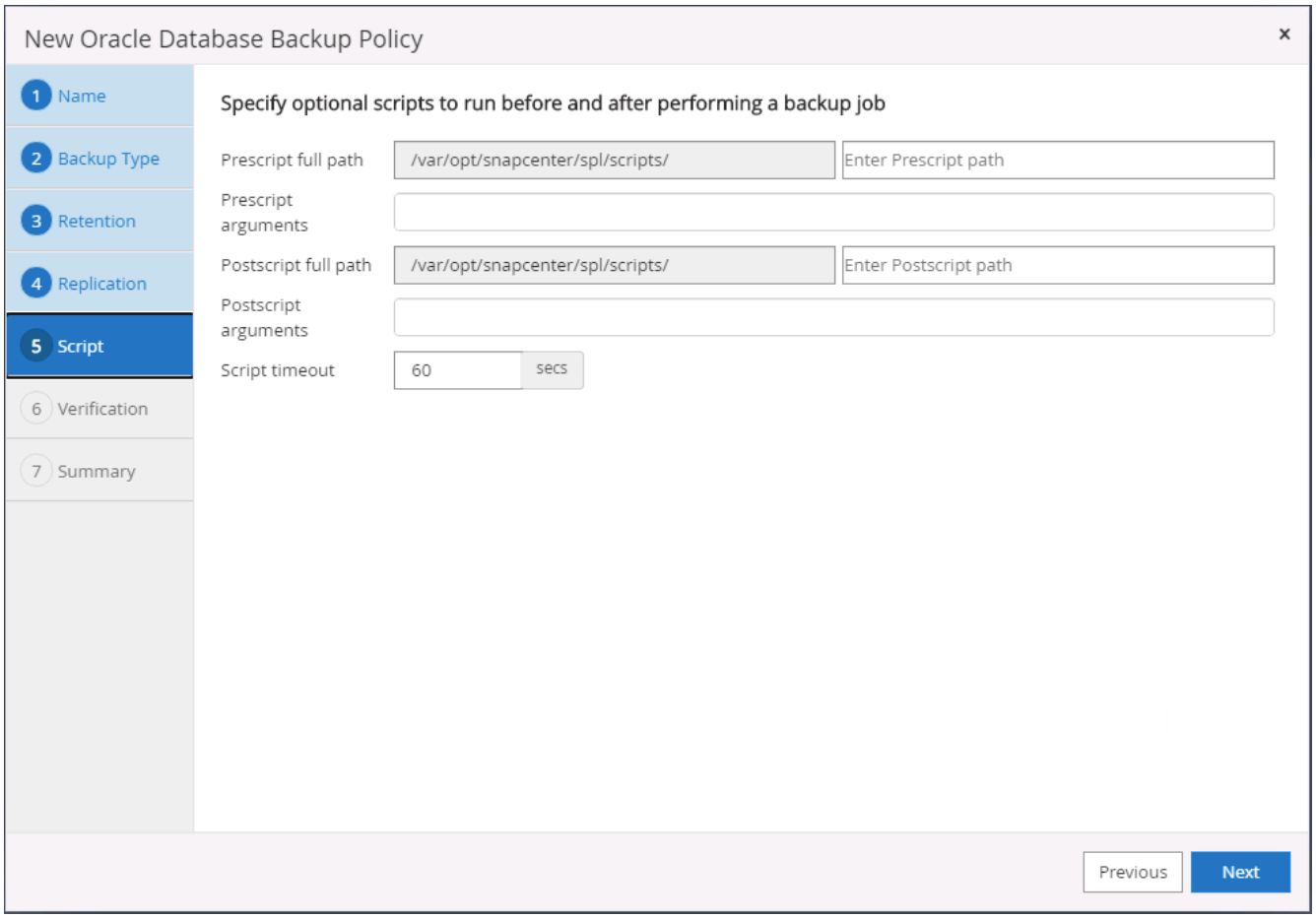
4. Définissez la période de conservation du journal.



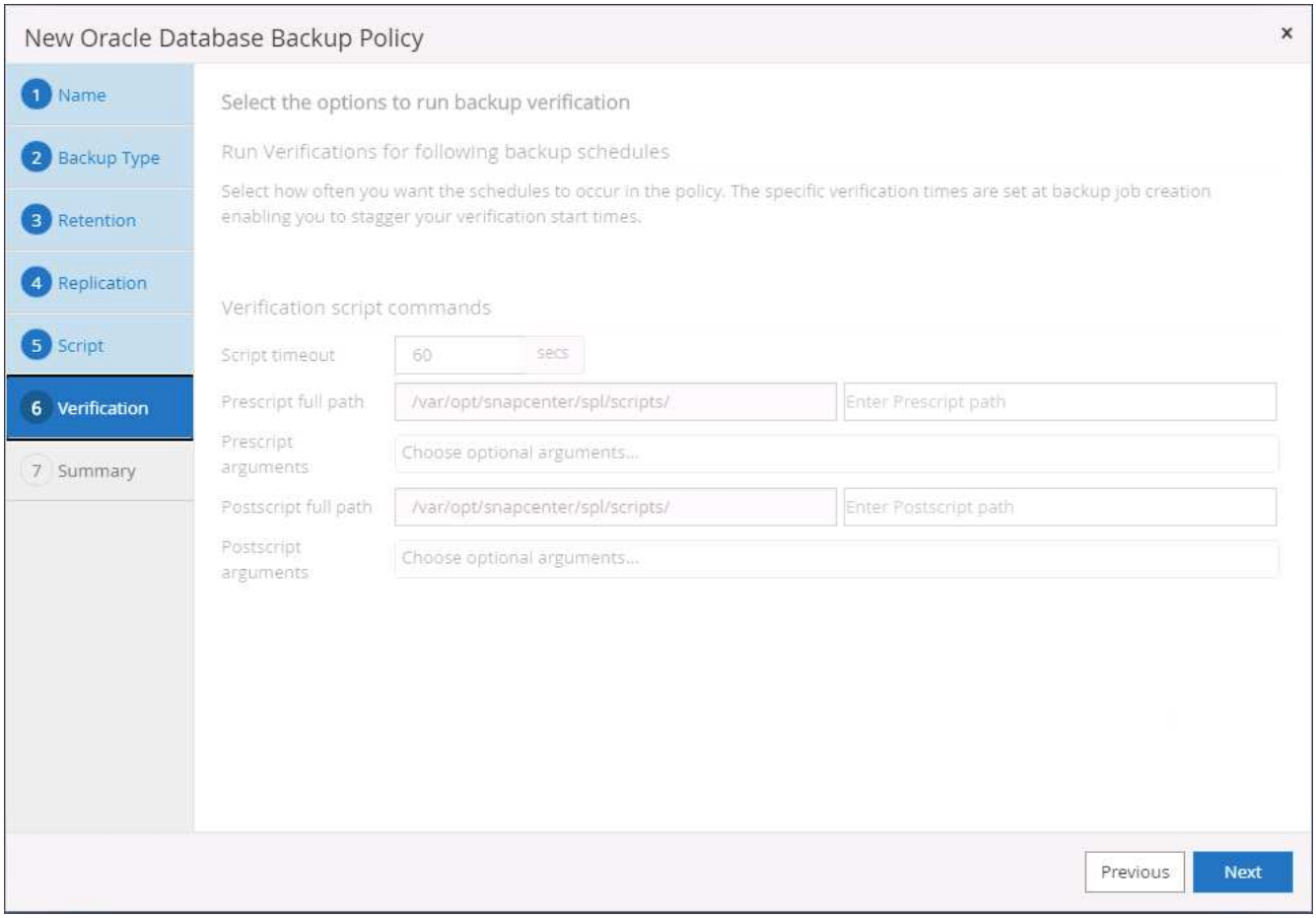
5. Activer la réplication vers un emplacement secondaire dans le cloud public.



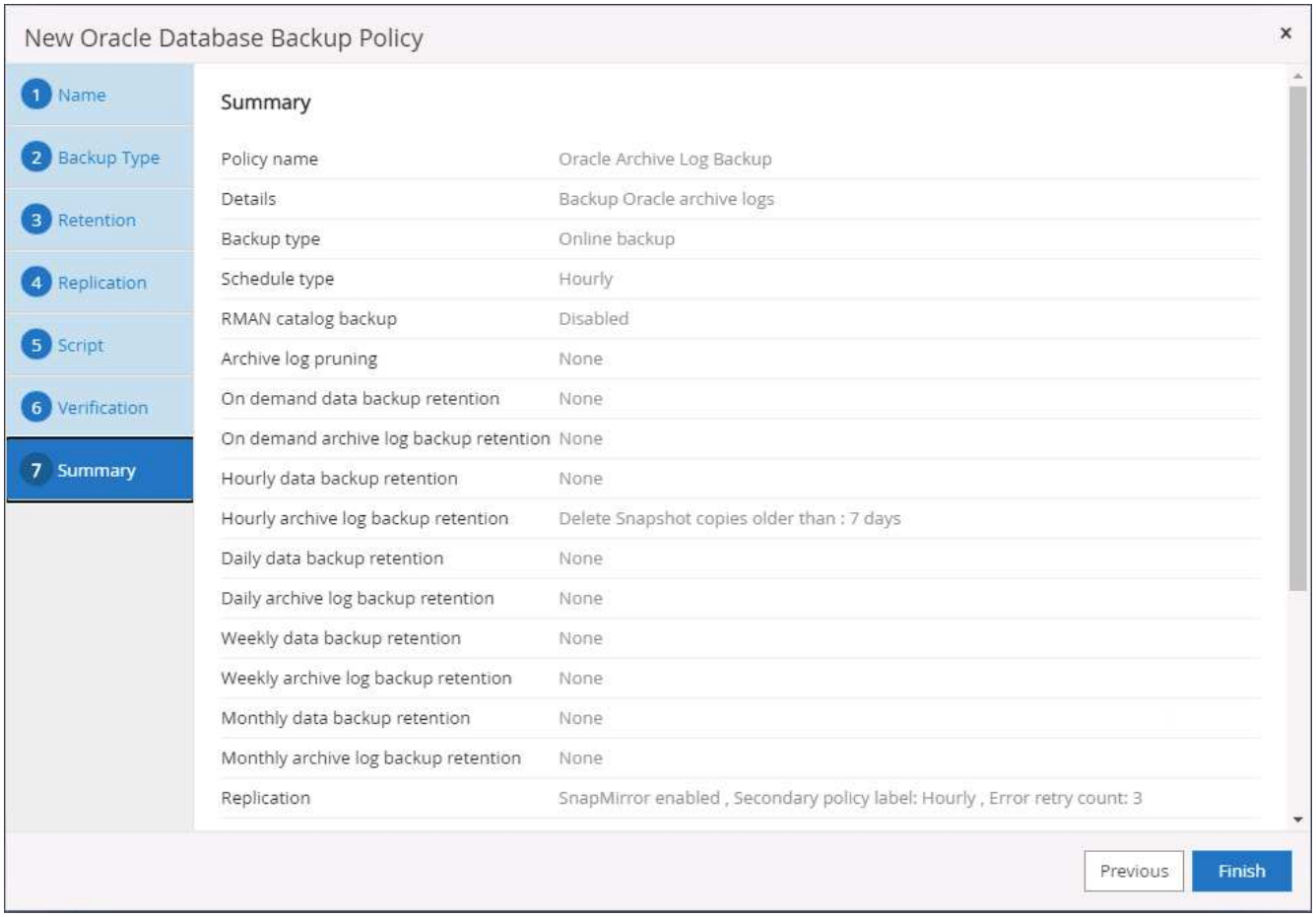
6. Spécifiez les scripts facultatifs à exécuter avant et après la sauvegarde du journal.



7. Spécifiez tous les scripts de vérification de sauvegarde.

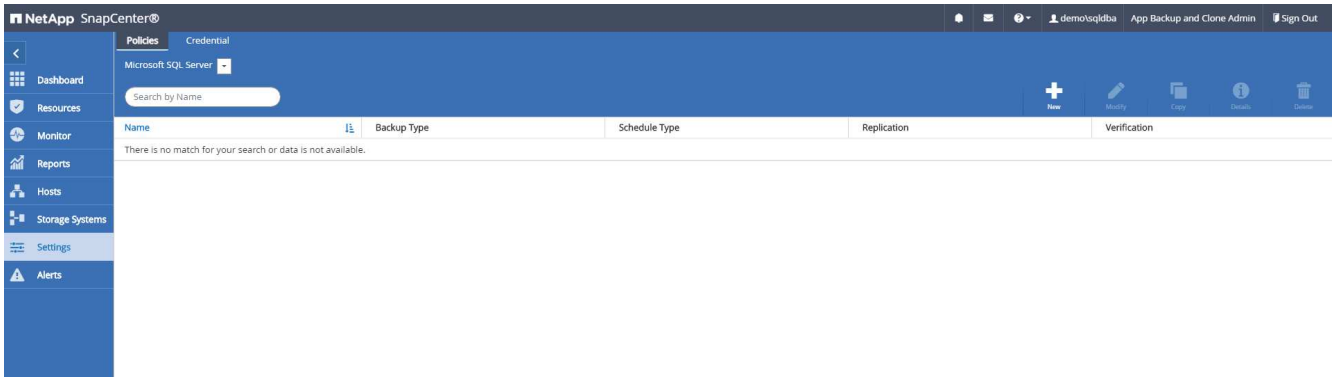

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Verification script commands
Script timeout
60
secs
Prescript full path
/var/opt/snapcenter/spl/scripts/
Enter Prescript path
Prescript arguments
Choose optional arguments...
Postscript full path
/var/opt/snapcenter/spl/scripts/
Enter Postscript path
Postscript arguments
Choose optional arguments...
Previous
Next

8. Résumé.

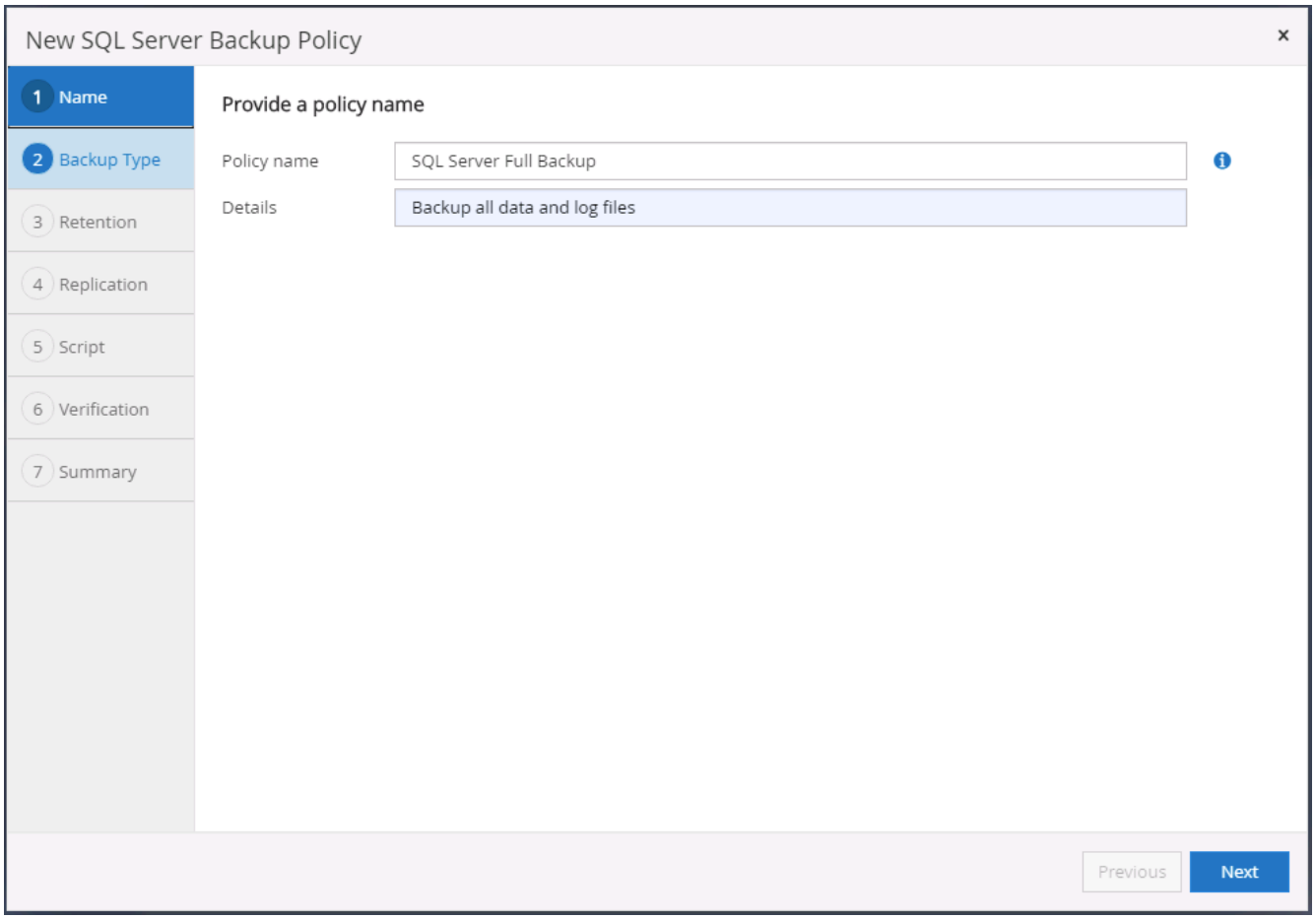


Créer une politique de sauvegarde complète de la base de données pour SQL

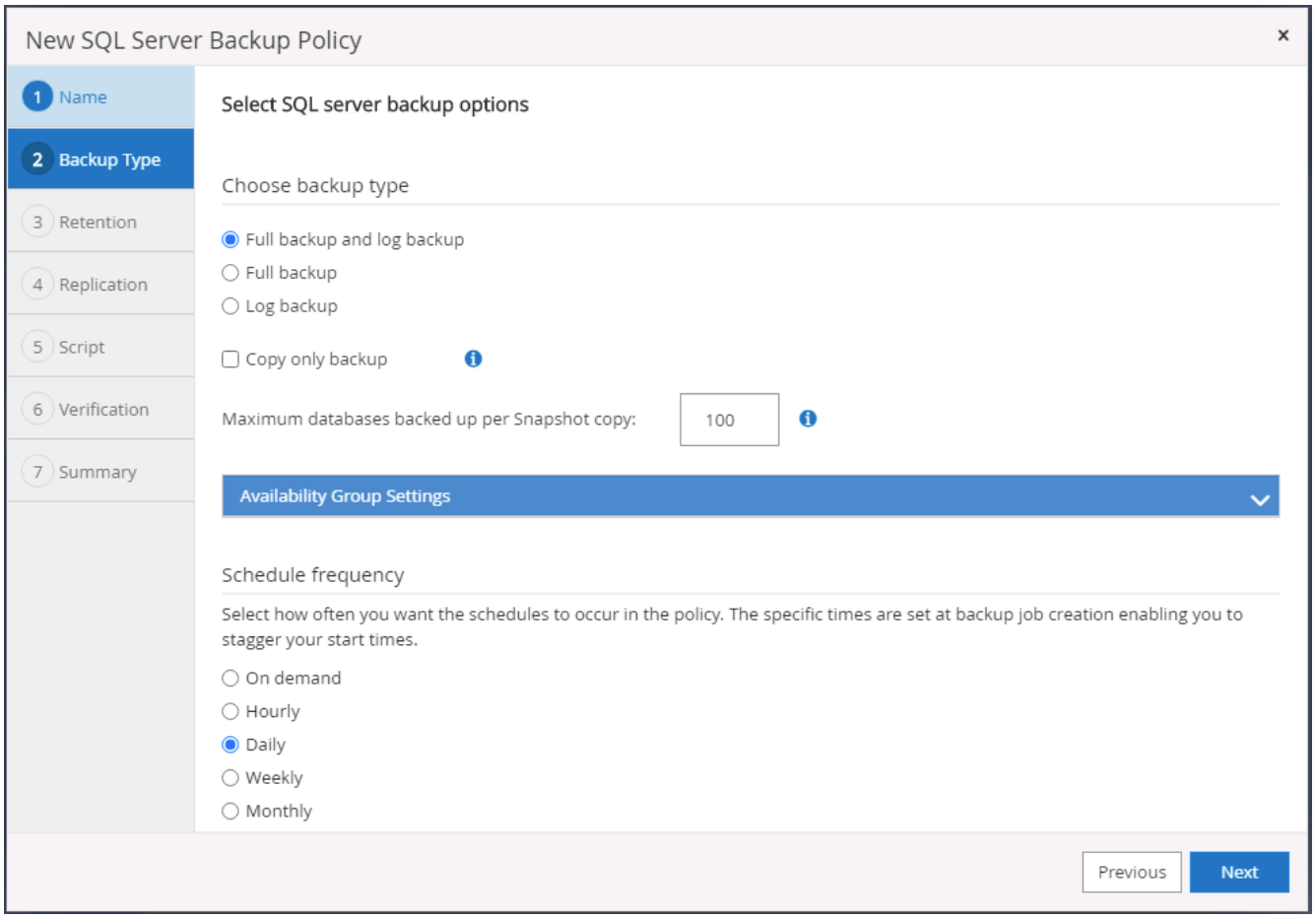
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur Politiques.



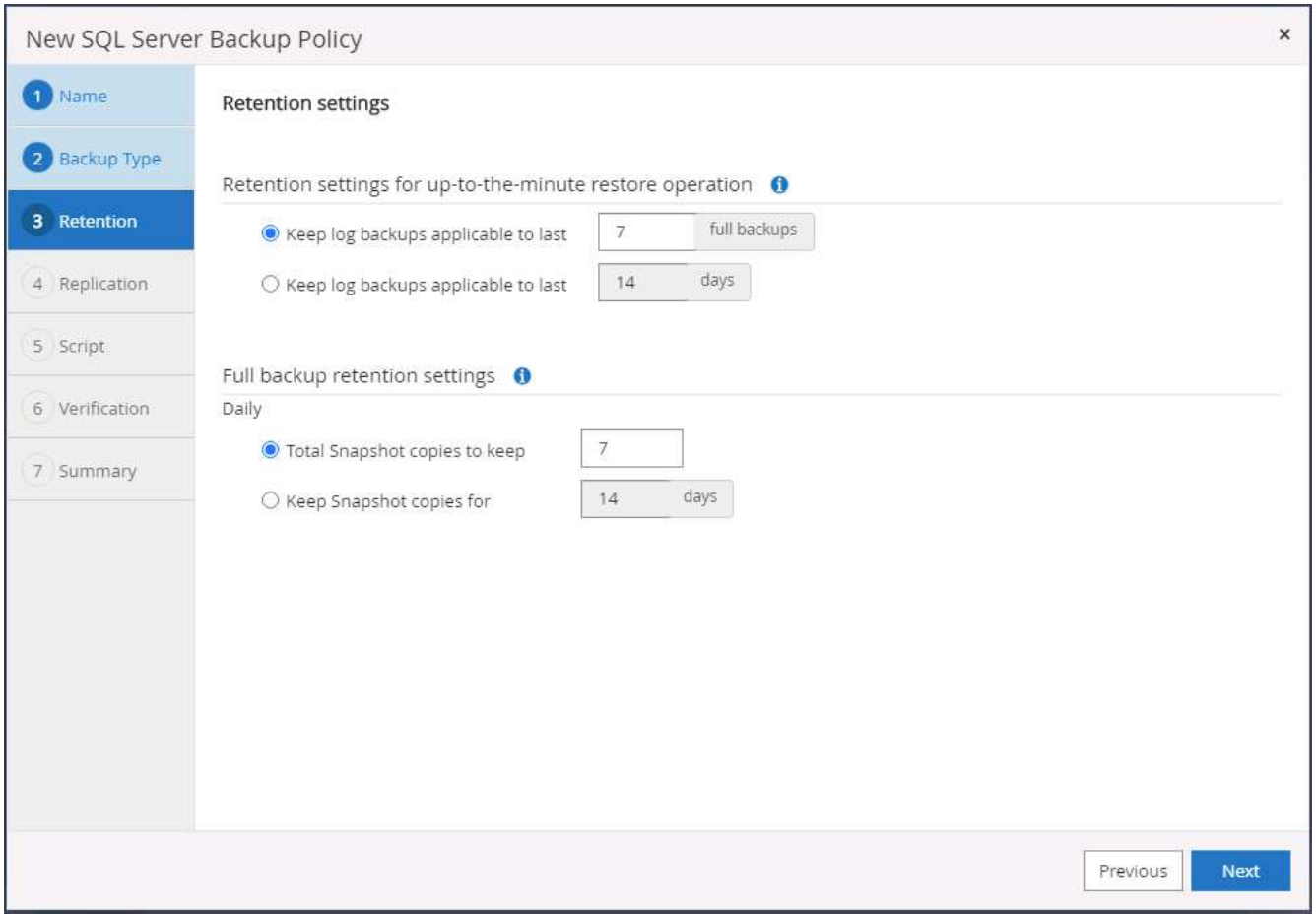
2. Cliquez sur Nouveau pour lancer un nouveau flux de travail de création de politique de sauvegarde ou choisissez une politique existante à modifier.



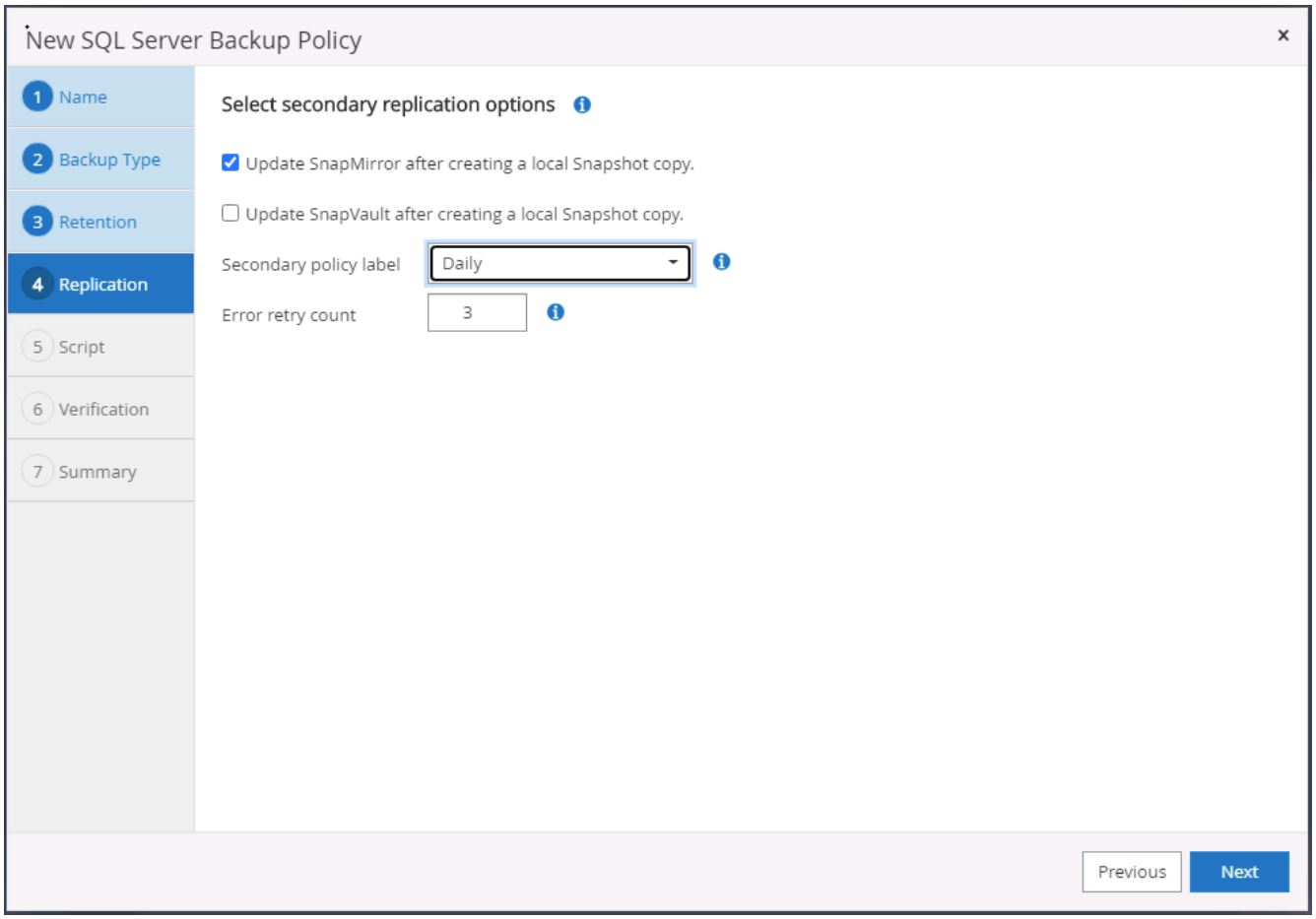
3. Définissez l'option de sauvegarde et la fréquence de planification. Pour SQL Server configuré avec un groupe de disponibilité, une réplique de sauvegarde préférée peut être définie.



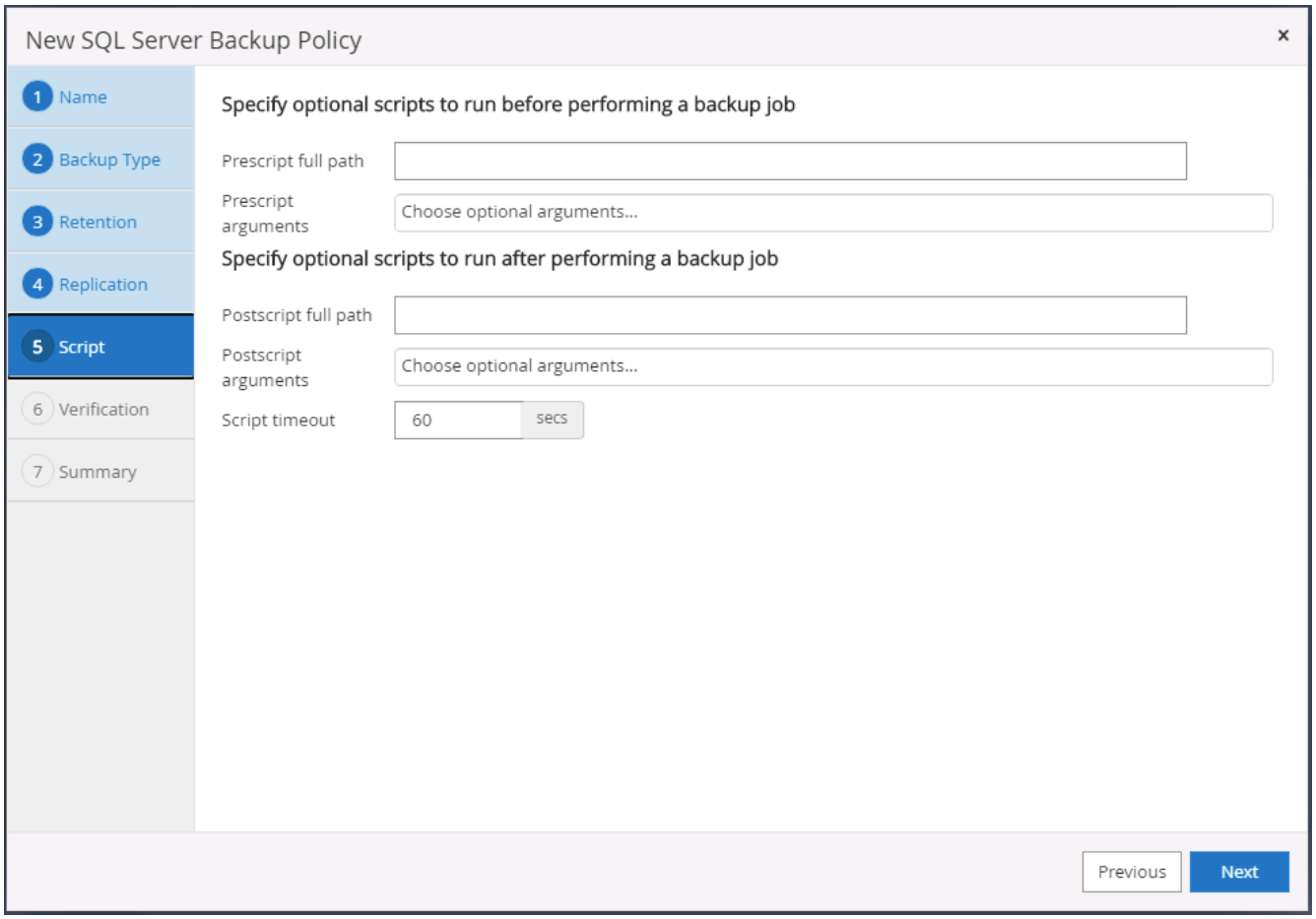
4. Définissez la période de conservation des sauvegardes.



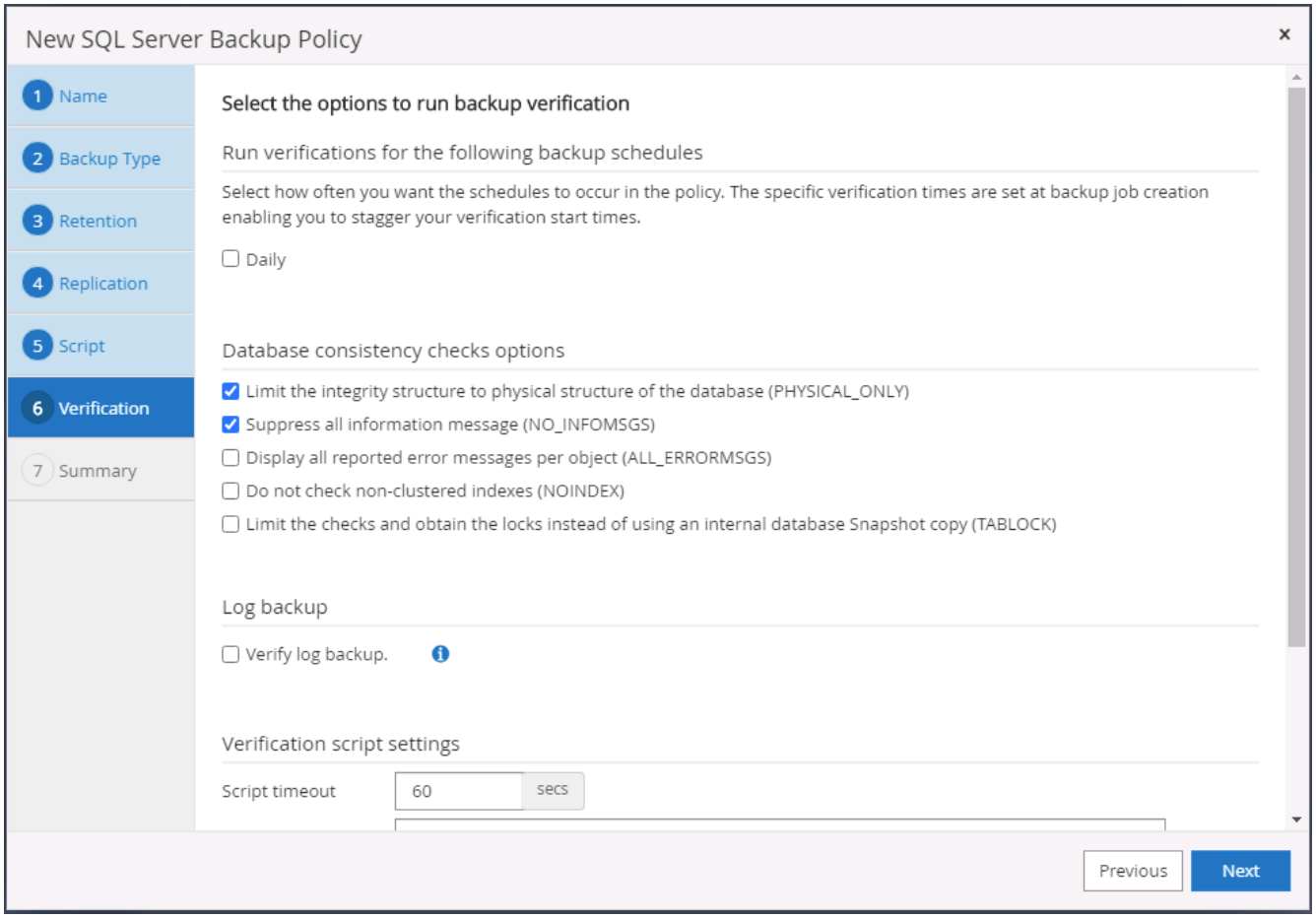
5. Activer la réplication de la copie de sauvegarde vers un emplacement secondaire dans le cloud.



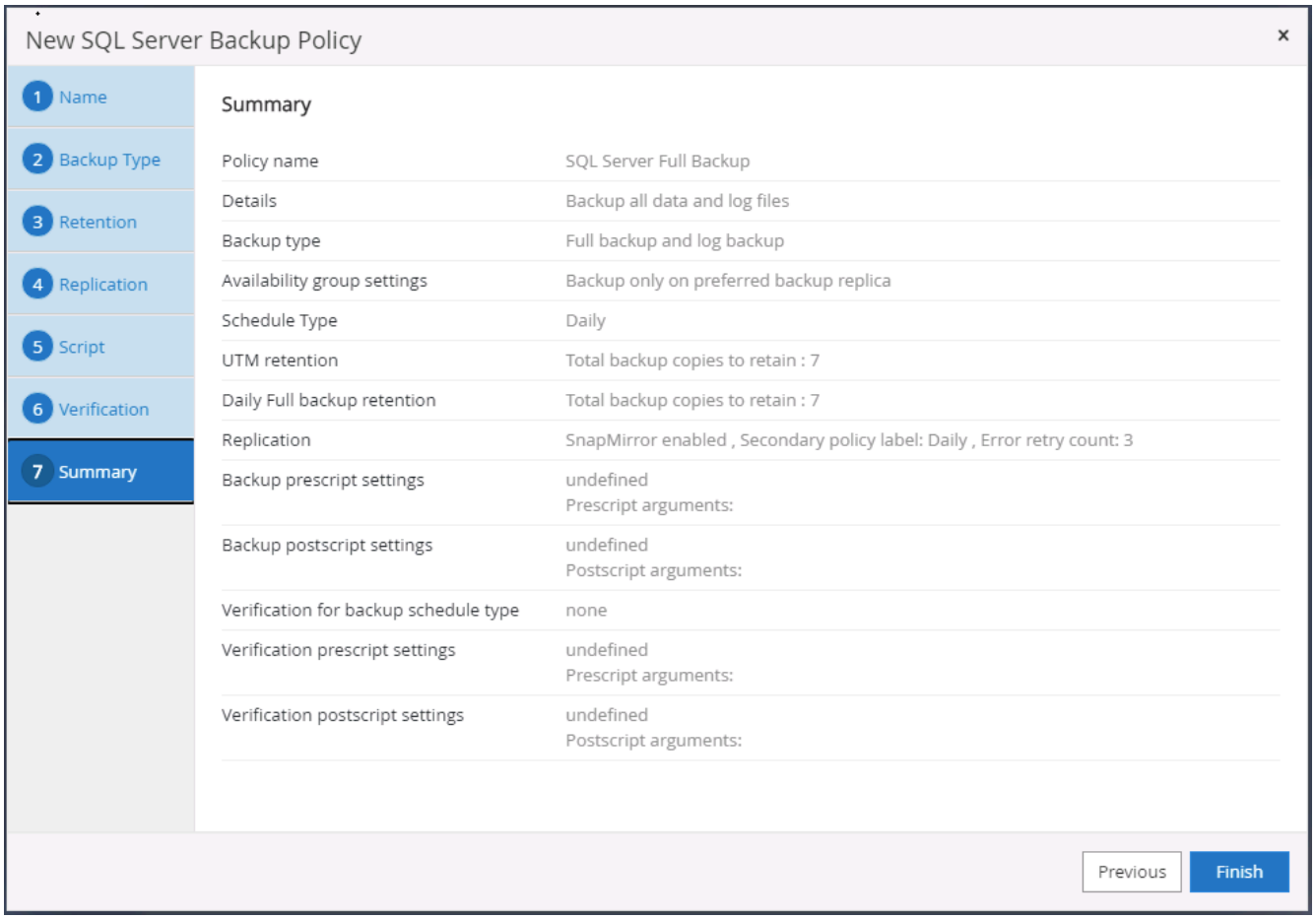
6. Spécifiez les scripts facultatifs à exécuter avant ou après une tâche de sauvegarde.



7. Spécifiez les options pour exécuter la vérification de sauvegarde.

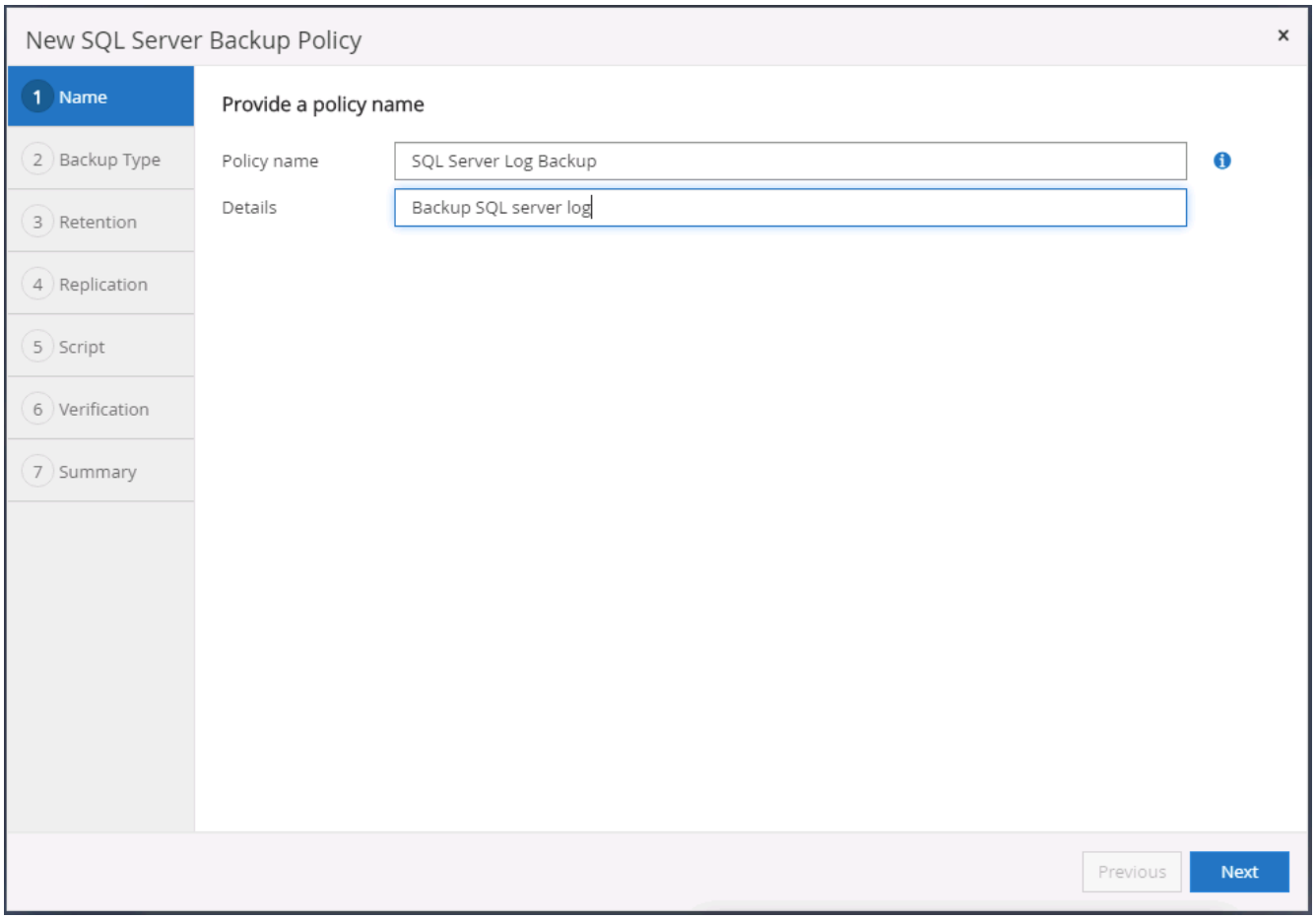

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Database consistency checks options
Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)
Suppress all information message (NO_INFOMSGS)
Display all reported error messages per object (ALL_ERRORMSGS)
Do not check non-clustered indexes (NOINDEX)
Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)
Log backup
Verify log backup.
Verification script settings
Script timeout
60
secs
Previous
Next

8. Résumé.

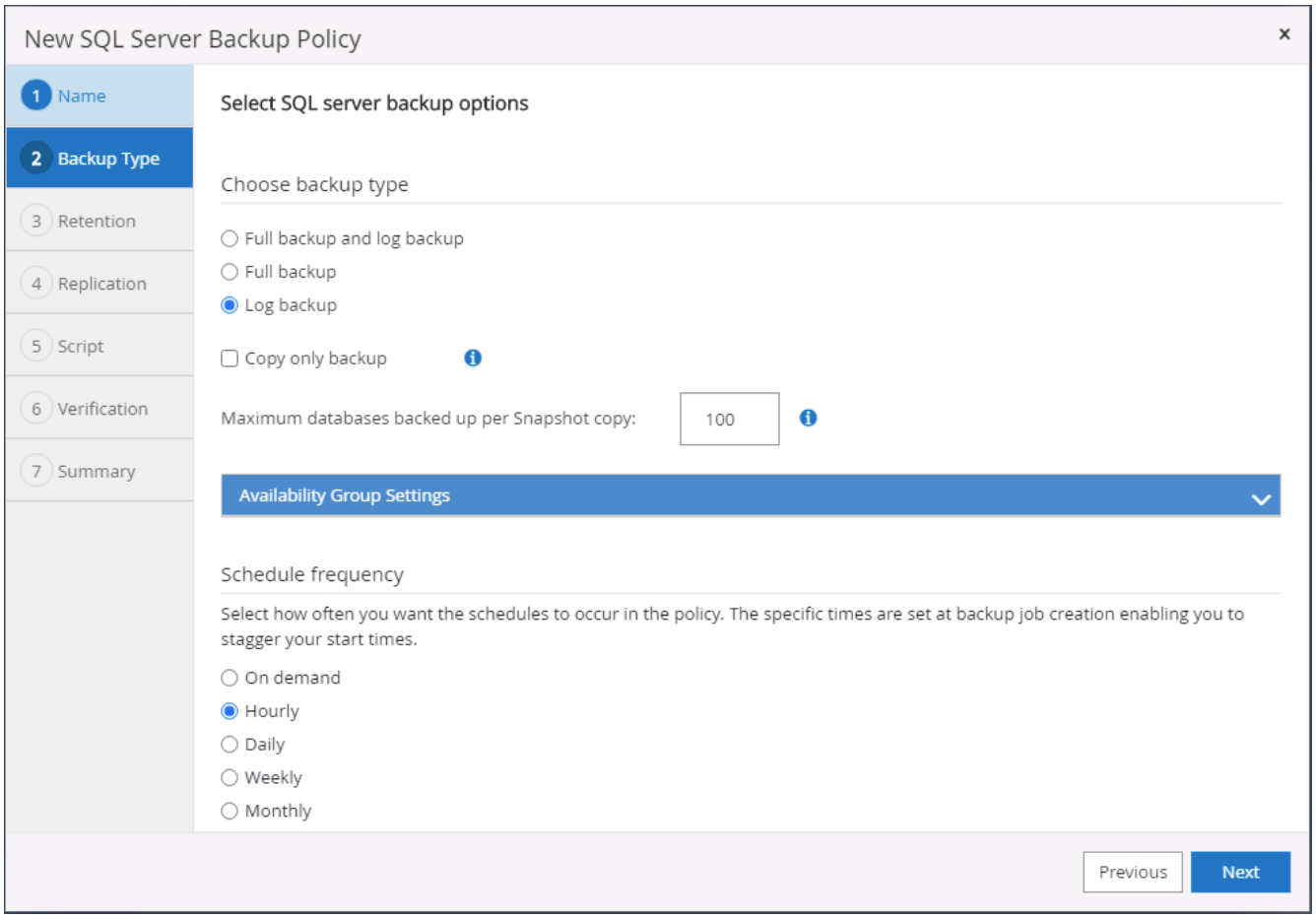


Créez une politique de sauvegarde du journal de base de données pour SQL.

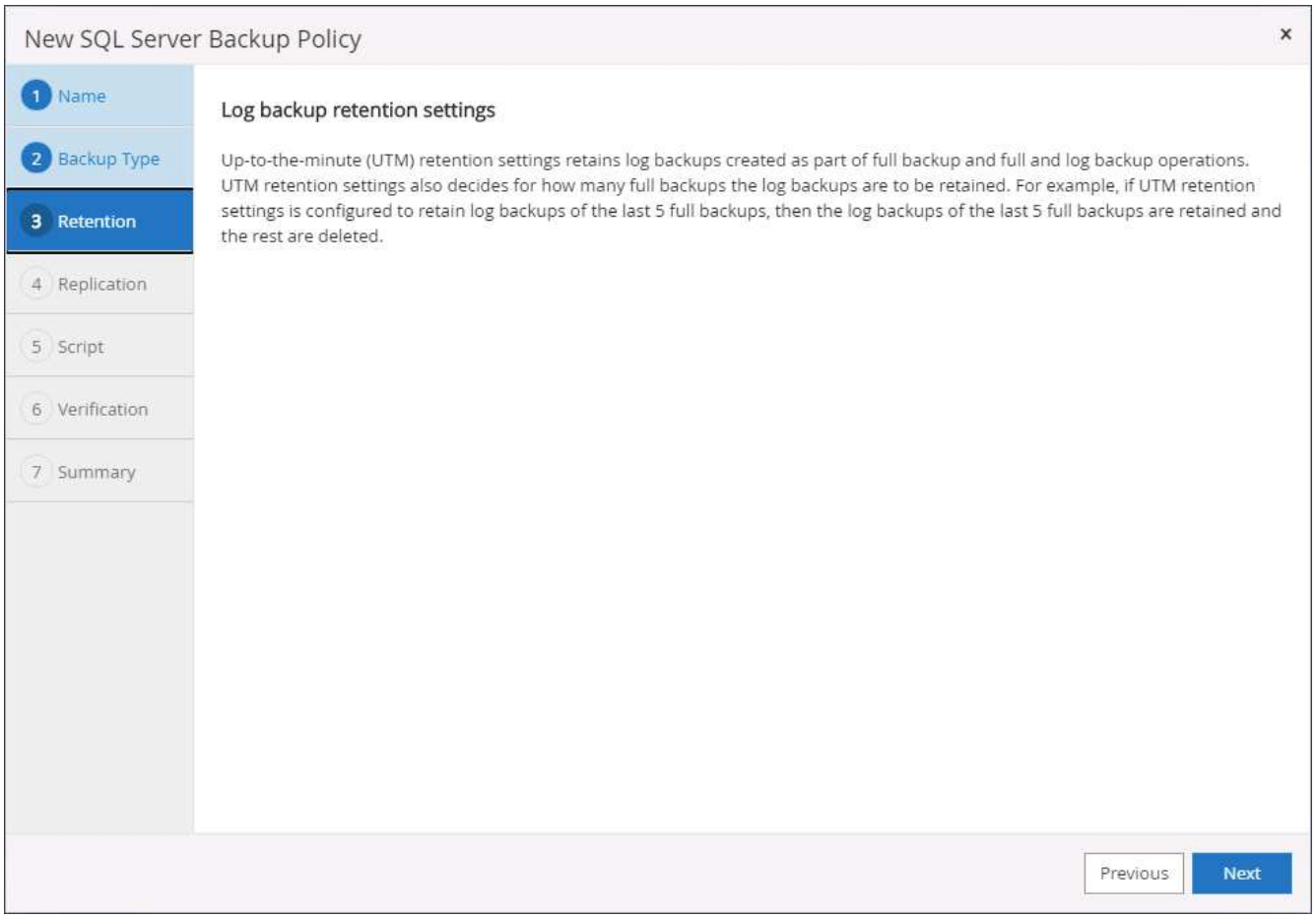
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données, cliquez sur Paramètres > Politiques, puis sur Nouveau pour lancer un nouveau flux de travail de création de politique.



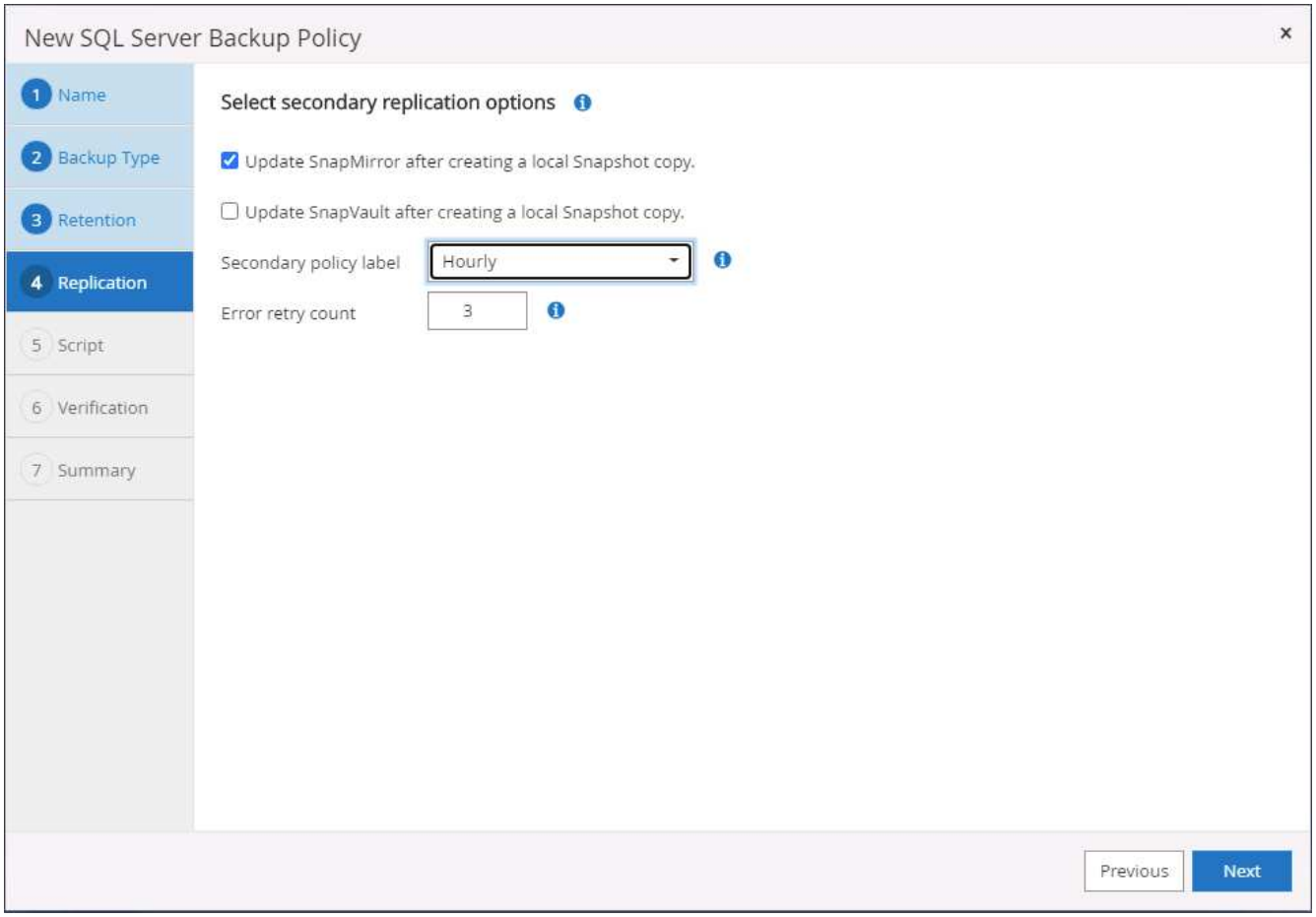
2. Définissez l'option de sauvegarde du journal et la fréquence de planification. Pour SQL Server configuré avec un groupe de disponibilité, une réplique de sauvegarde préférée peut être définie.



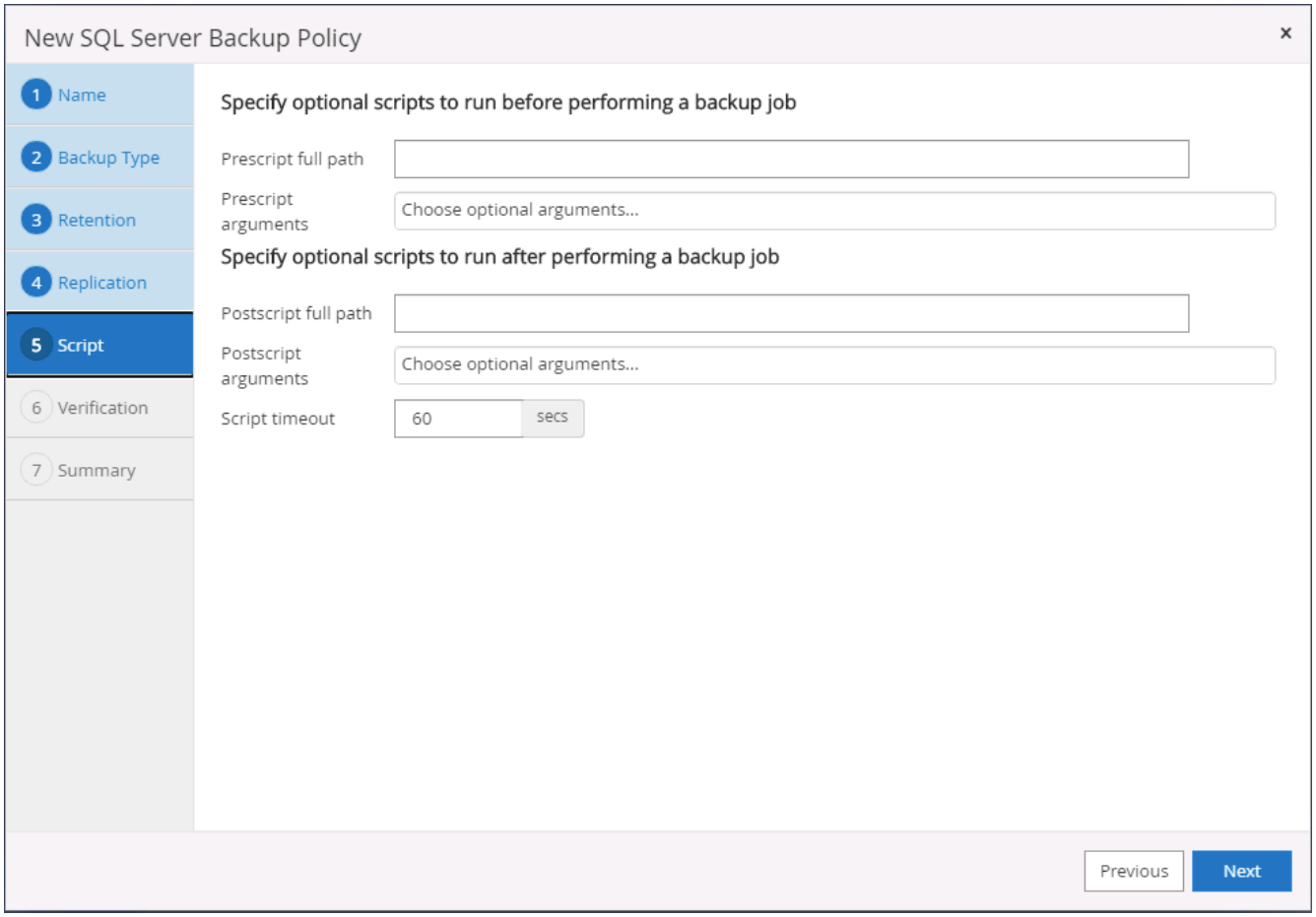
3. La politique de sauvegarde des données du serveur SQL définit la conservation des sauvegardes de journaux ; acceptez les valeurs par défaut ici.



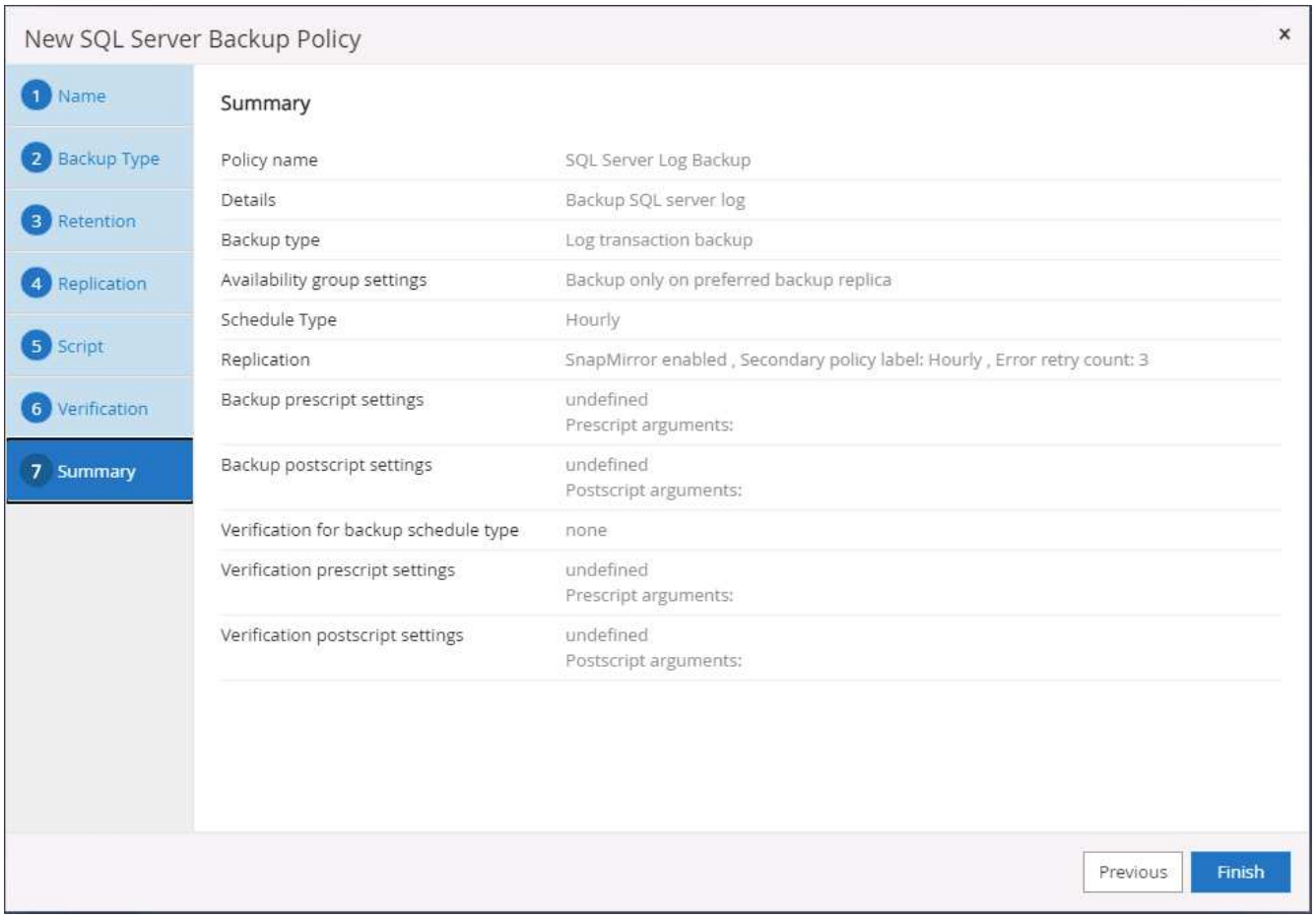
4. Activer la réplication de sauvegarde du journal vers le secondaire dans le cloud.



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


New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Specify optional scripts to run before performing a backup job
Prescript full path
Prescript arguments
Choose optional arguments...
Specify optional scripts to run after performing a backup job
Postscript full path
Postscript arguments
Choose optional arguments...
Script timeout
60
secs
Previous
Next

6. Résumé.

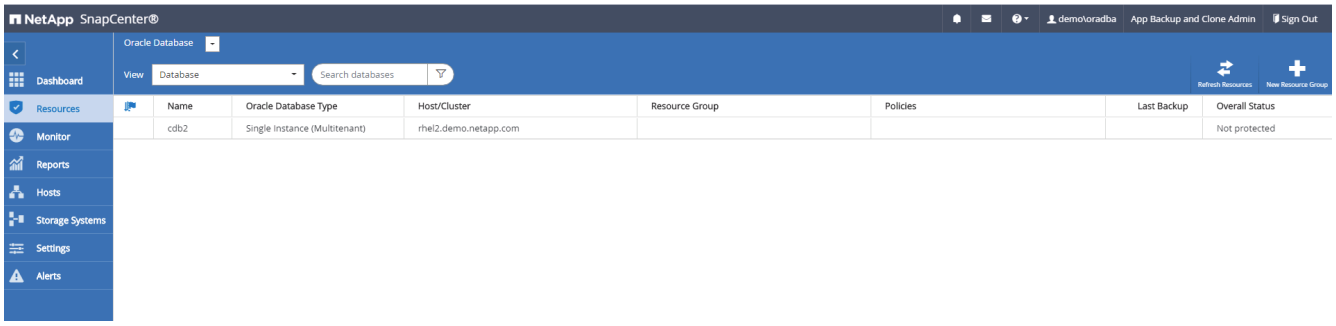


8. Mettre en œuvre une politique de sauvegarde pour protéger la base de données

SnapCenter utilise un groupe de ressources pour sauvegarder une base de données dans un regroupement logique de ressources de base de données, comme 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 métier, etc. La protection d'une seule base de données crée son propre groupe de ressources. Les procédures suivantes montrent comment mettre en œuvre une politique de sauvegarde créée dans la section 7 pour protéger les bases de données Oracle et SQL Server.

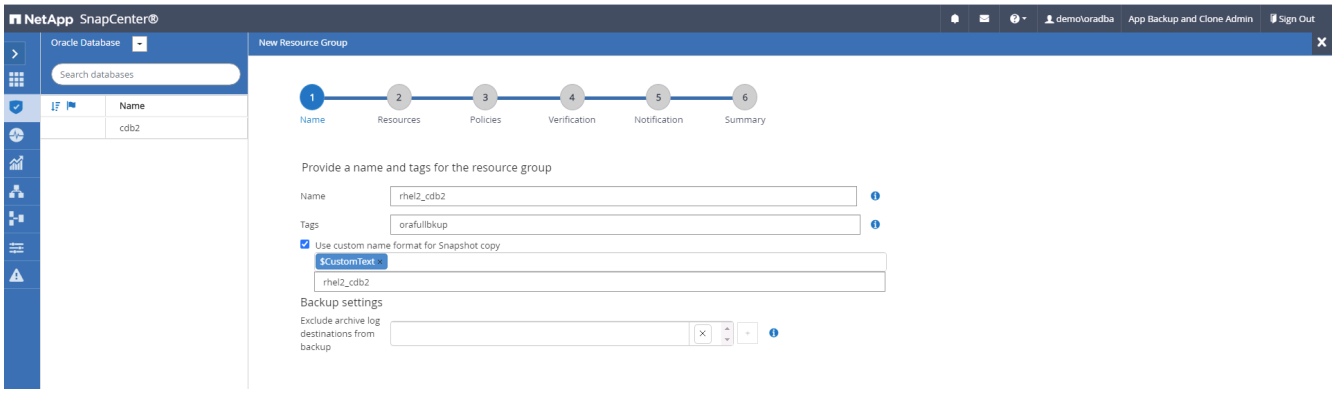
Créer un groupe de ressources pour la sauvegarde complète d'Oracle

1. Connectez-vous à SnapCenter avec 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 du groupe de ressources.

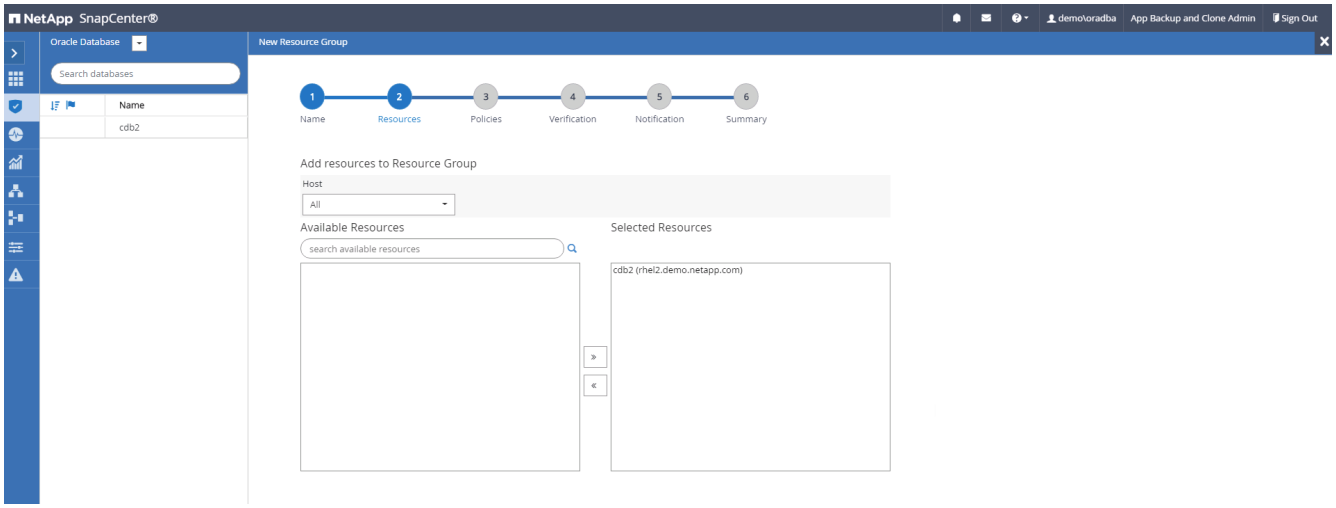


2. Fournissez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format de

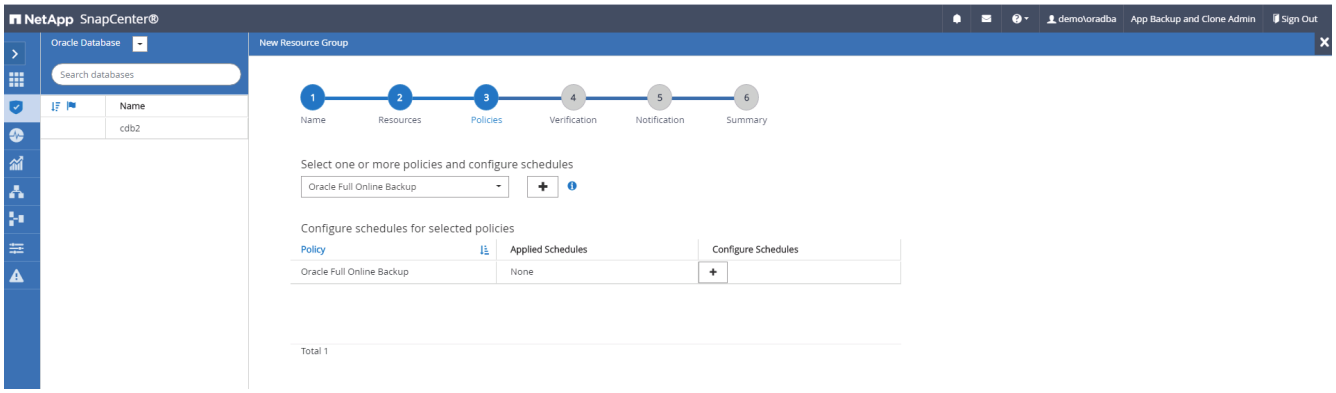
dénomination pour la copie instantanée et contourner la destination du journal d'archive redondant si elle est configurée.



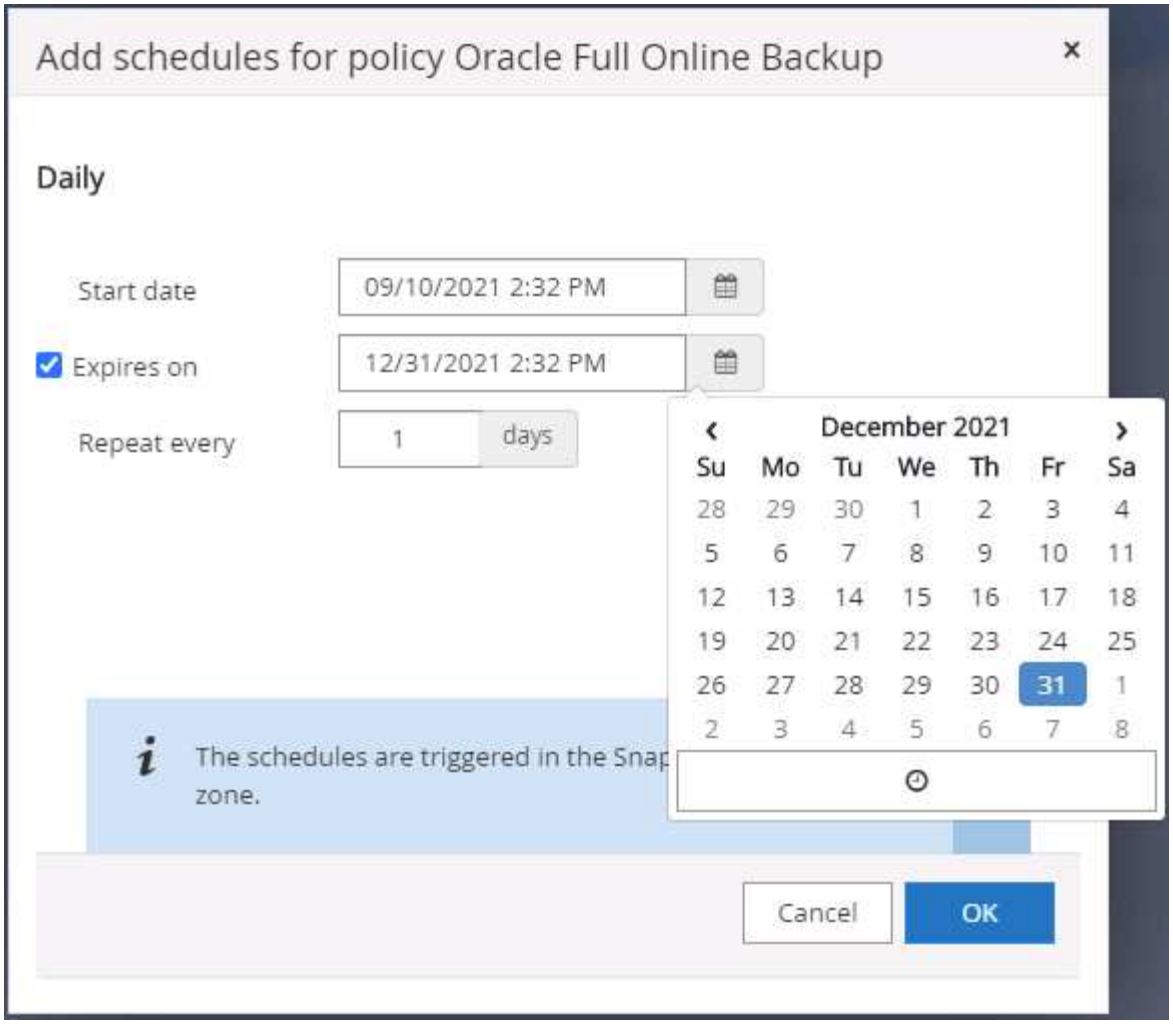
3. Ajoutez des ressources de base de données au groupe de ressources.



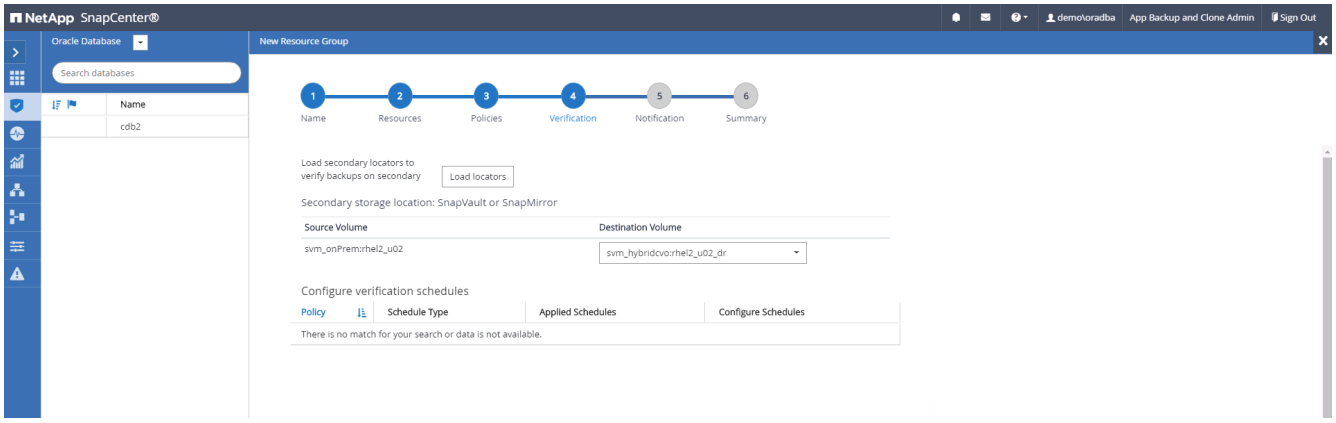
4. Sélectionnez une politique de sauvegarde complète créée dans la section 7 dans la liste déroulante.



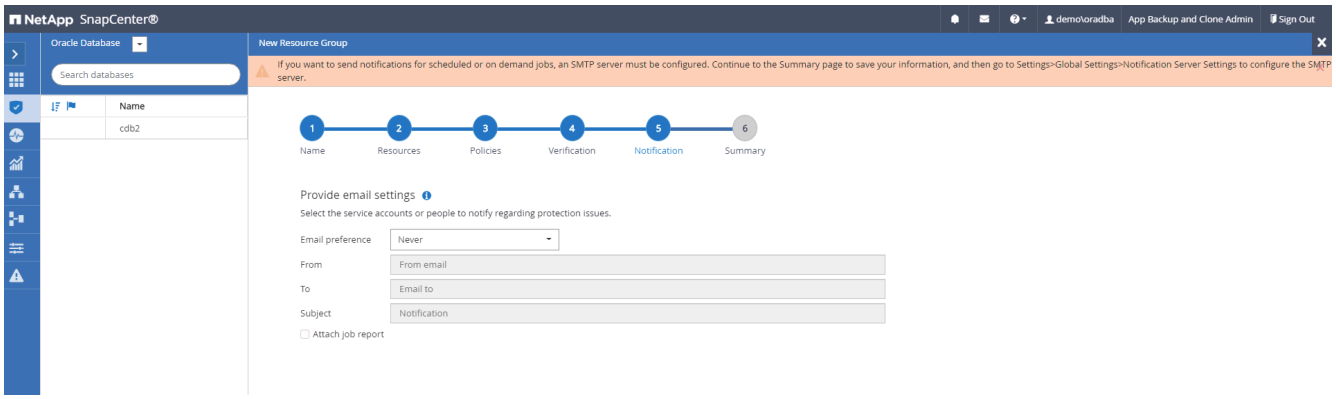
5. Cliquez sur le signe (+) pour configurer la planification de sauvegarde souhaitée.



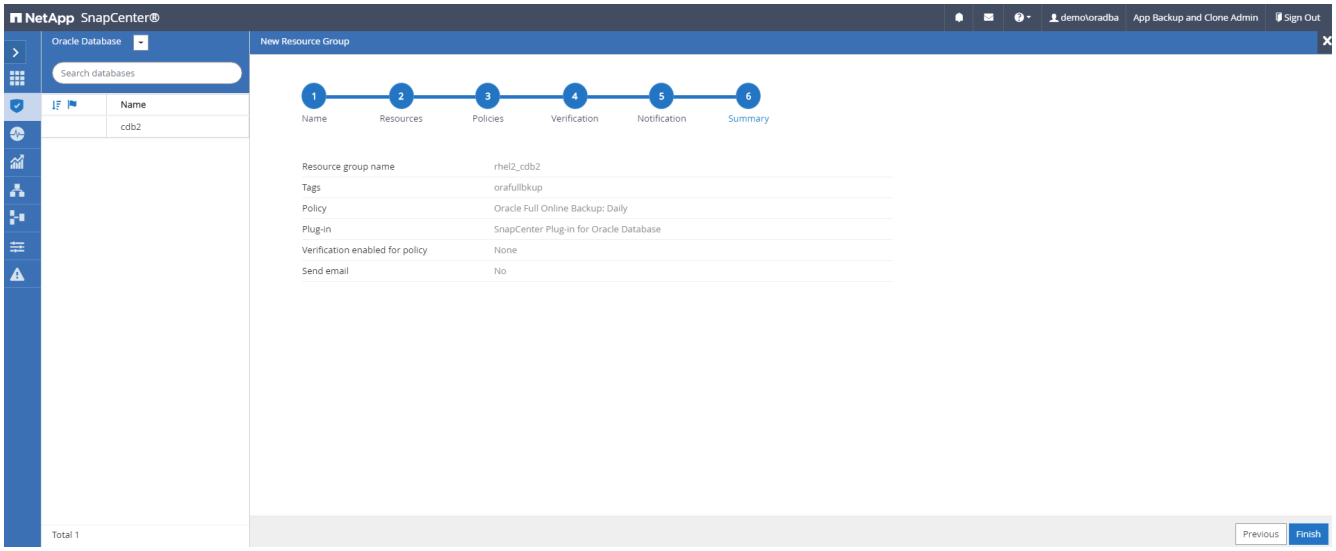
6. Cliquez sur Charger les localisateurs pour charger le volume source et de destination.



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

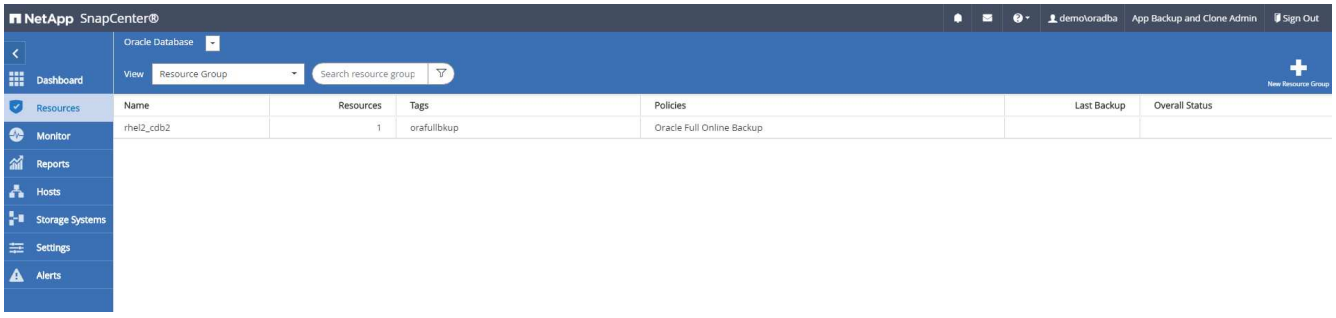


8. Résumé.

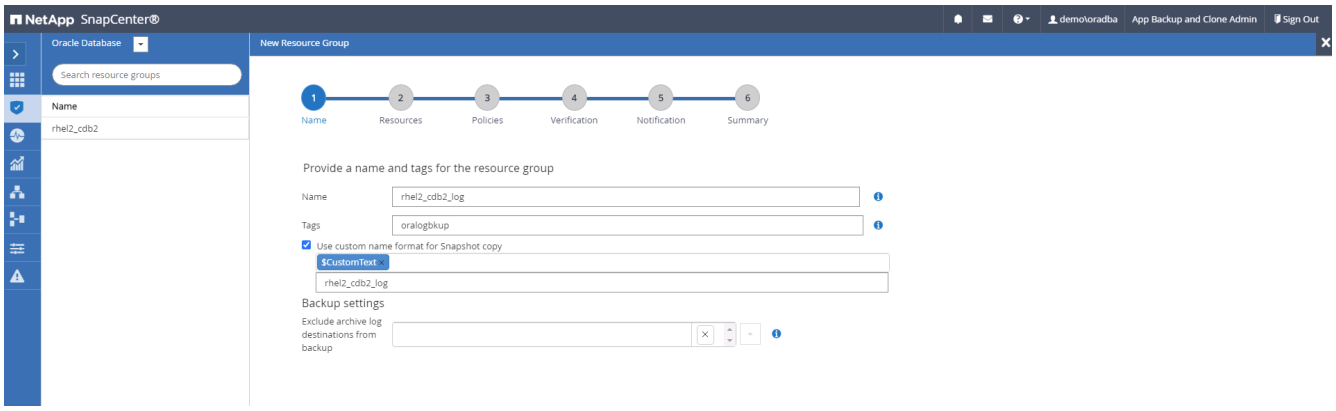


Créer un groupe de ressources pour la sauvegarde des journaux d'Oracle

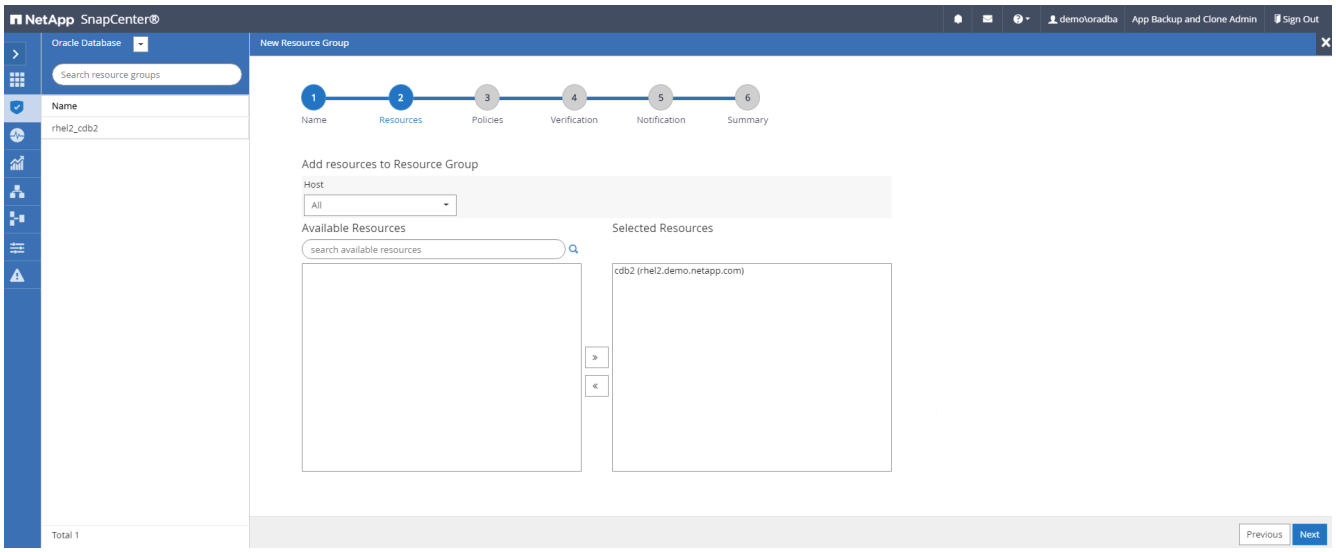
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez Base de données ou Groupe de ressources pour lancer le flux de travail de création du groupe de ressources.



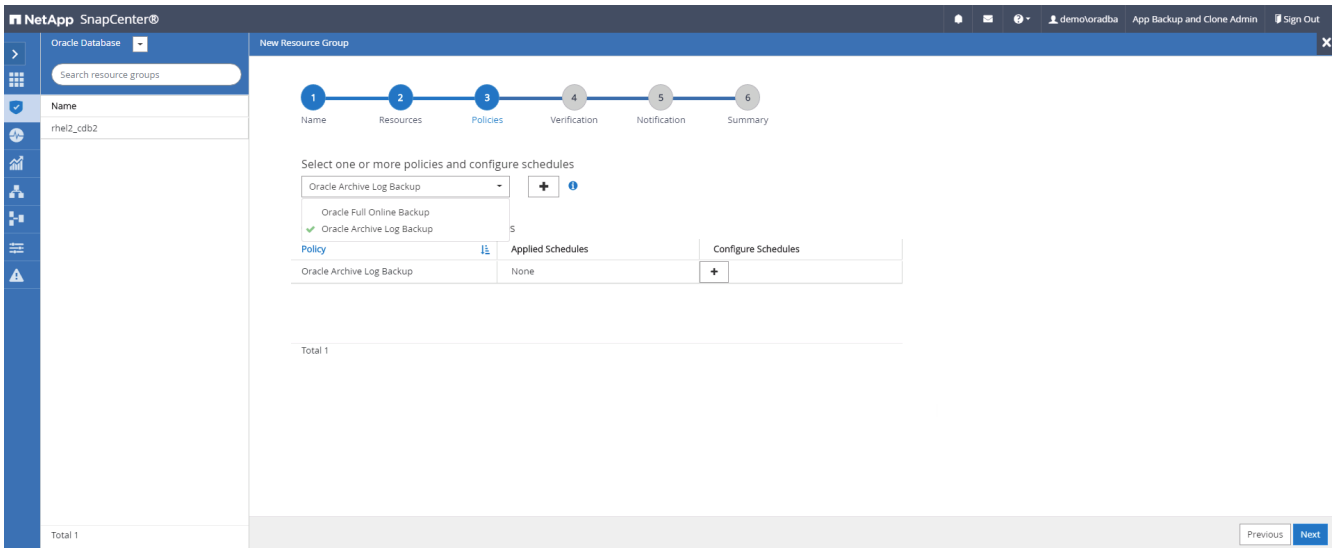
2. Fournissez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format de dénomination pour la copie instantanée et contourner la destination du journal d'archive redondant si elle est configurée.



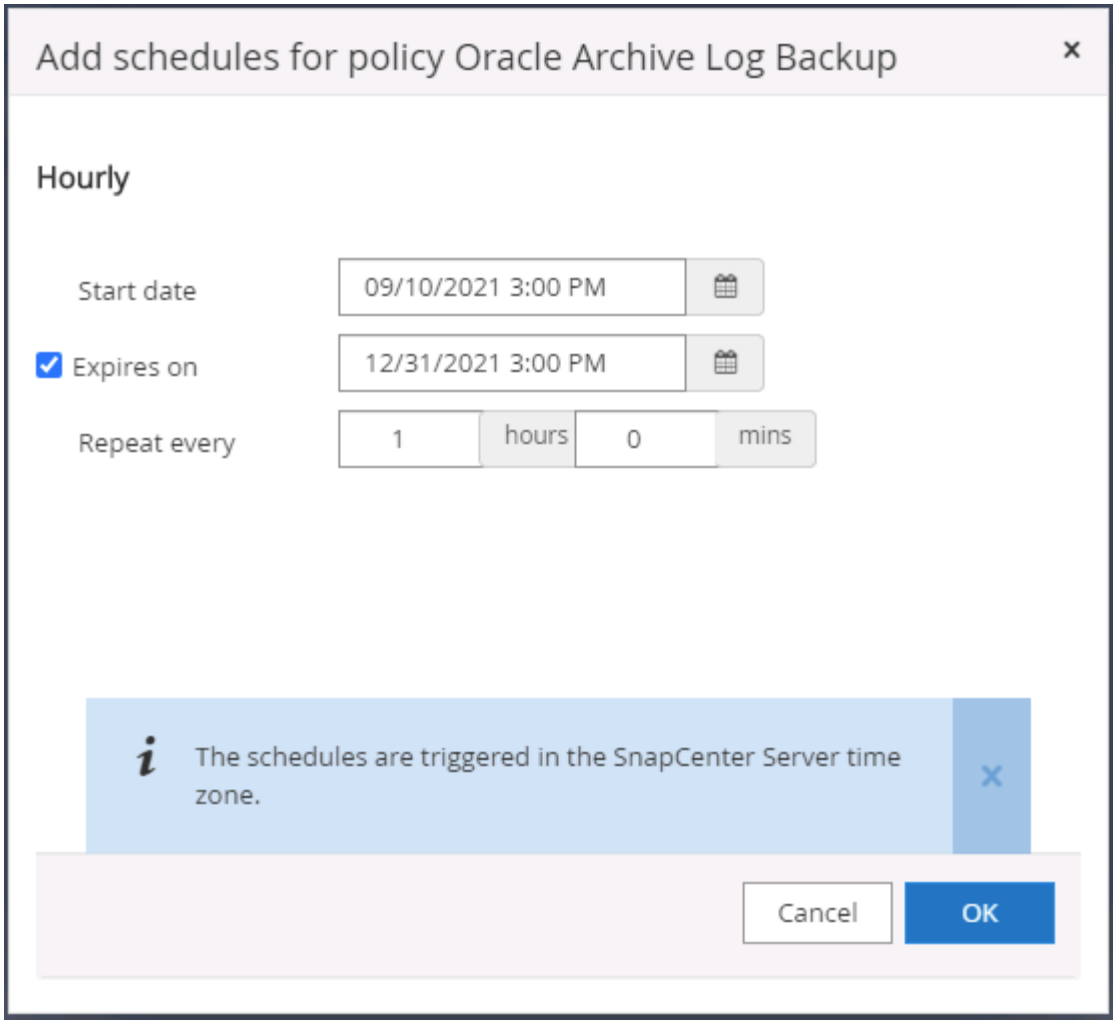
3. Ajoutez des ressources de base de données au groupe de ressources.



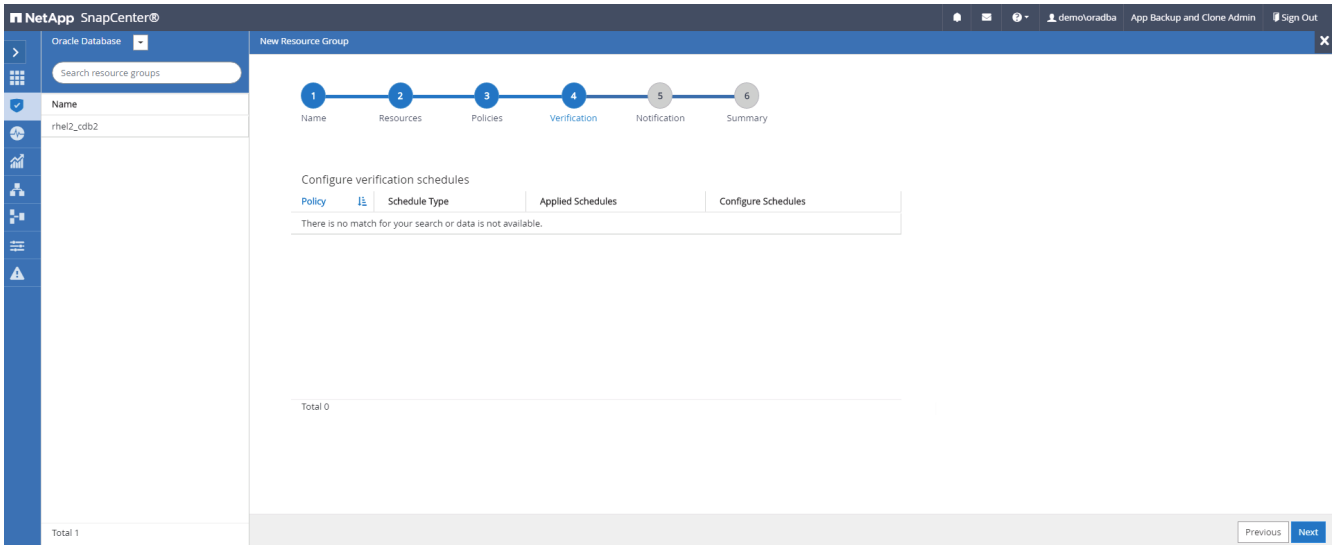
4. Sélectionnez une politique de sauvegarde de journal créée dans la section 7 dans la liste déroulante.



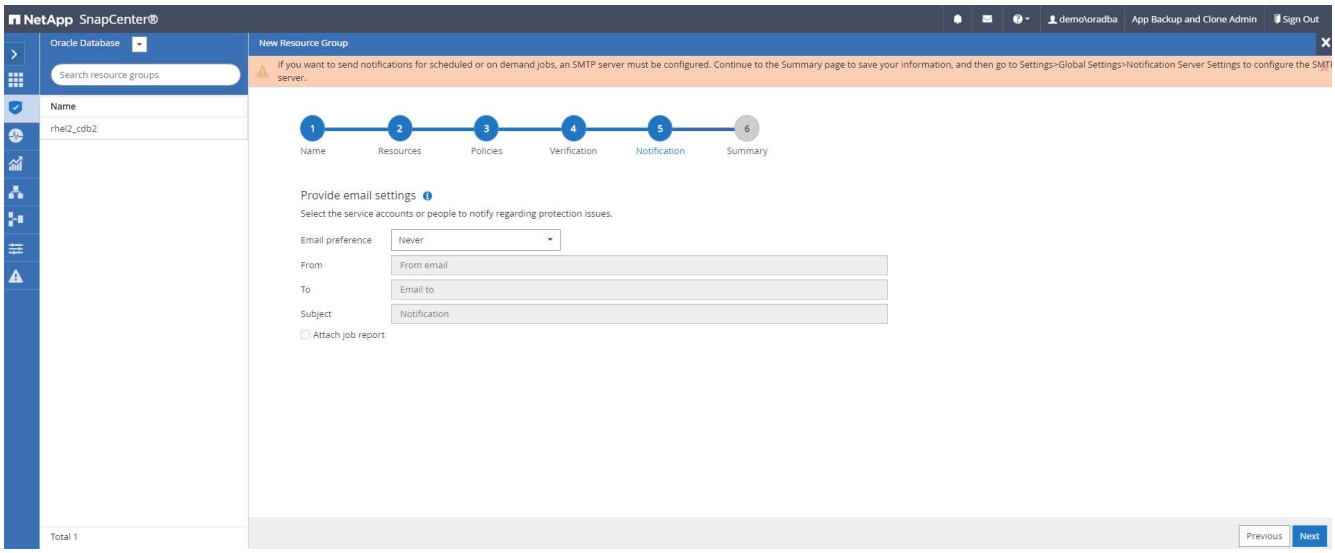
5. Cliquez sur le signe (+) pour configurer la planification de sauvegarde souhaitée.



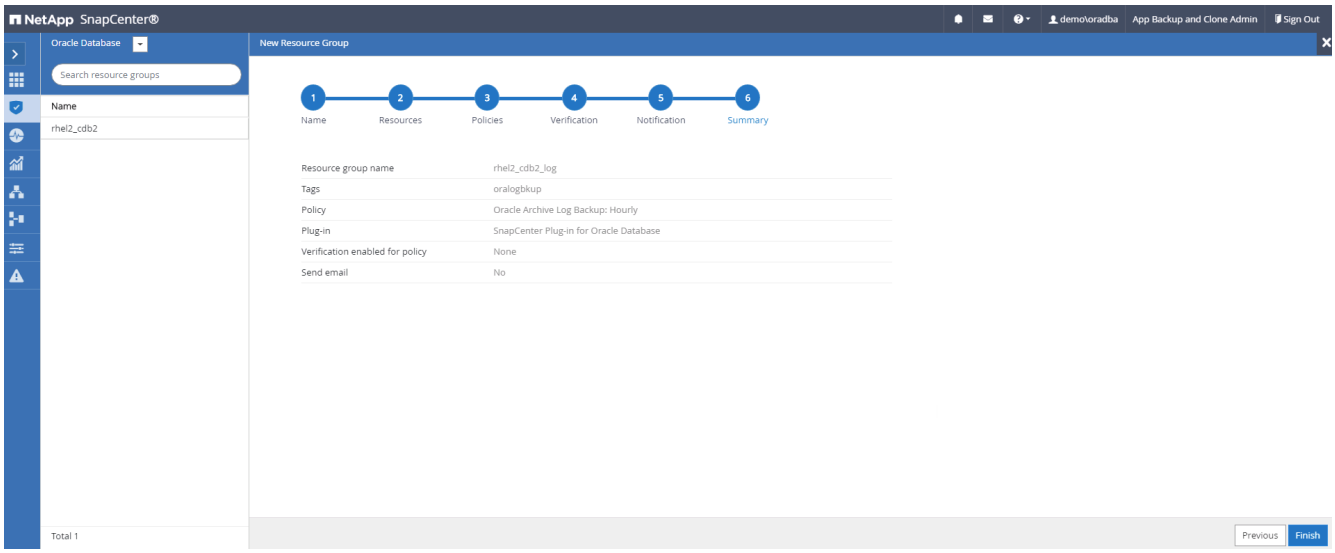
6. Si la vérification de sauvegarde est configurée, elle s'affiche ici.



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

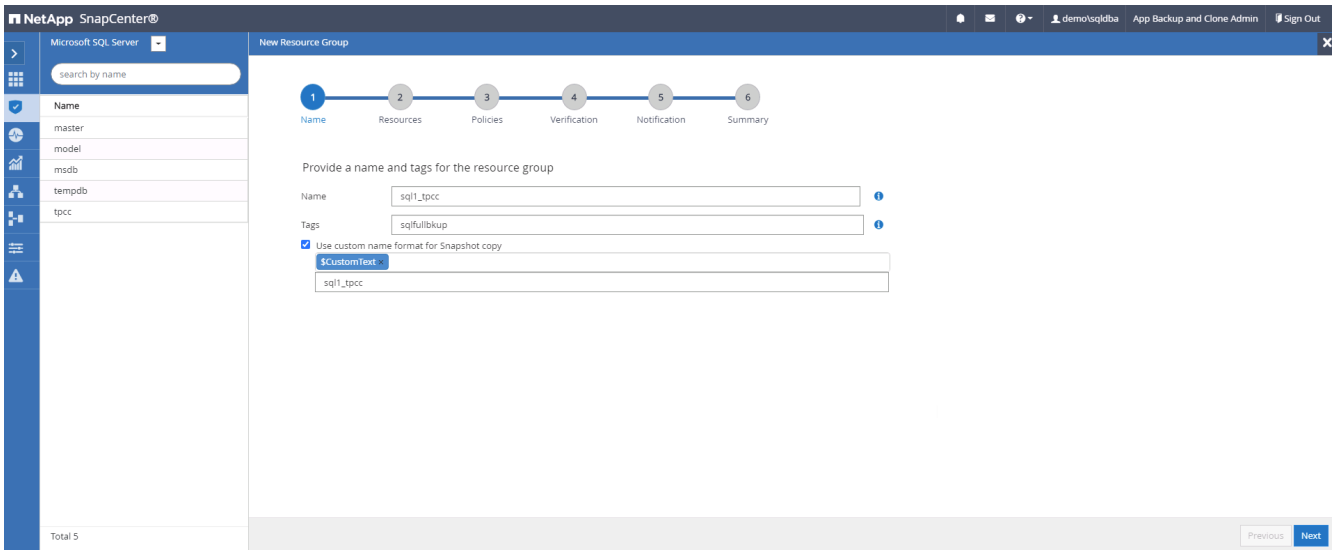


8. Résumé.

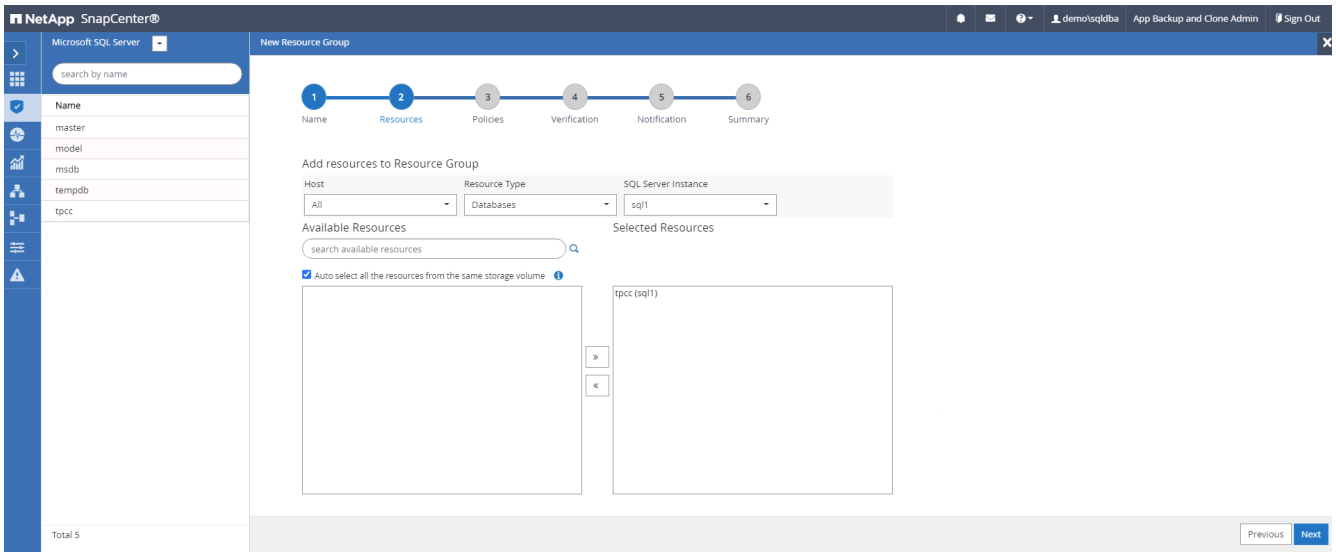


Créer un groupe de ressources pour la sauvegarde complète de SQL Server

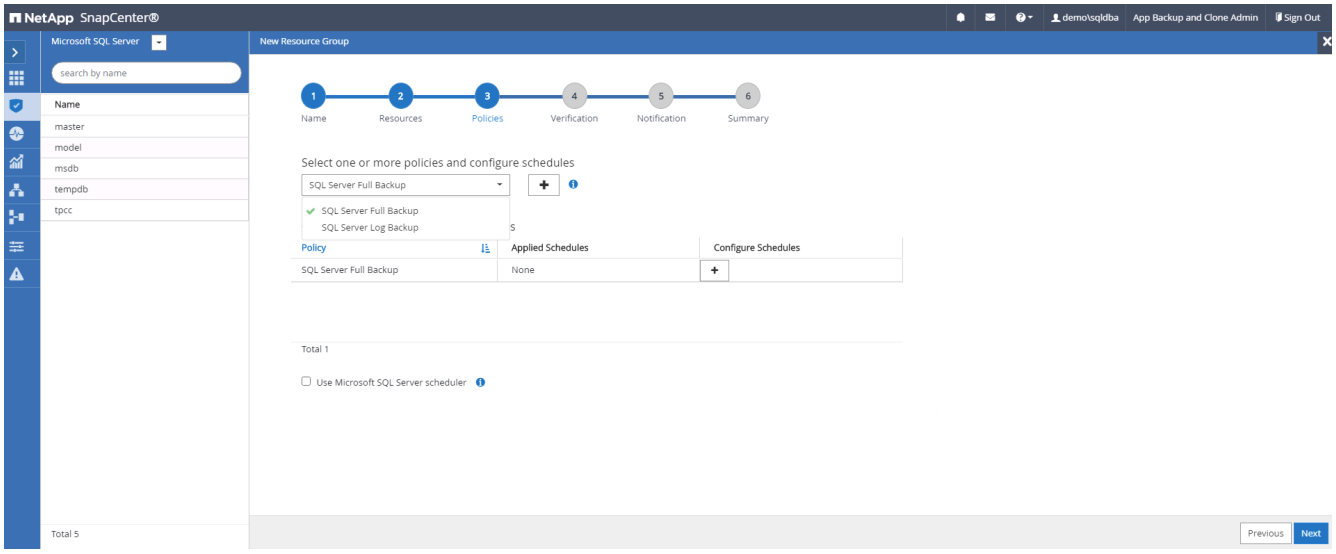
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez une base de données ou un groupe de ressources pour lancer le flux de travail de création du groupe de ressources. Fournissez un nom et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



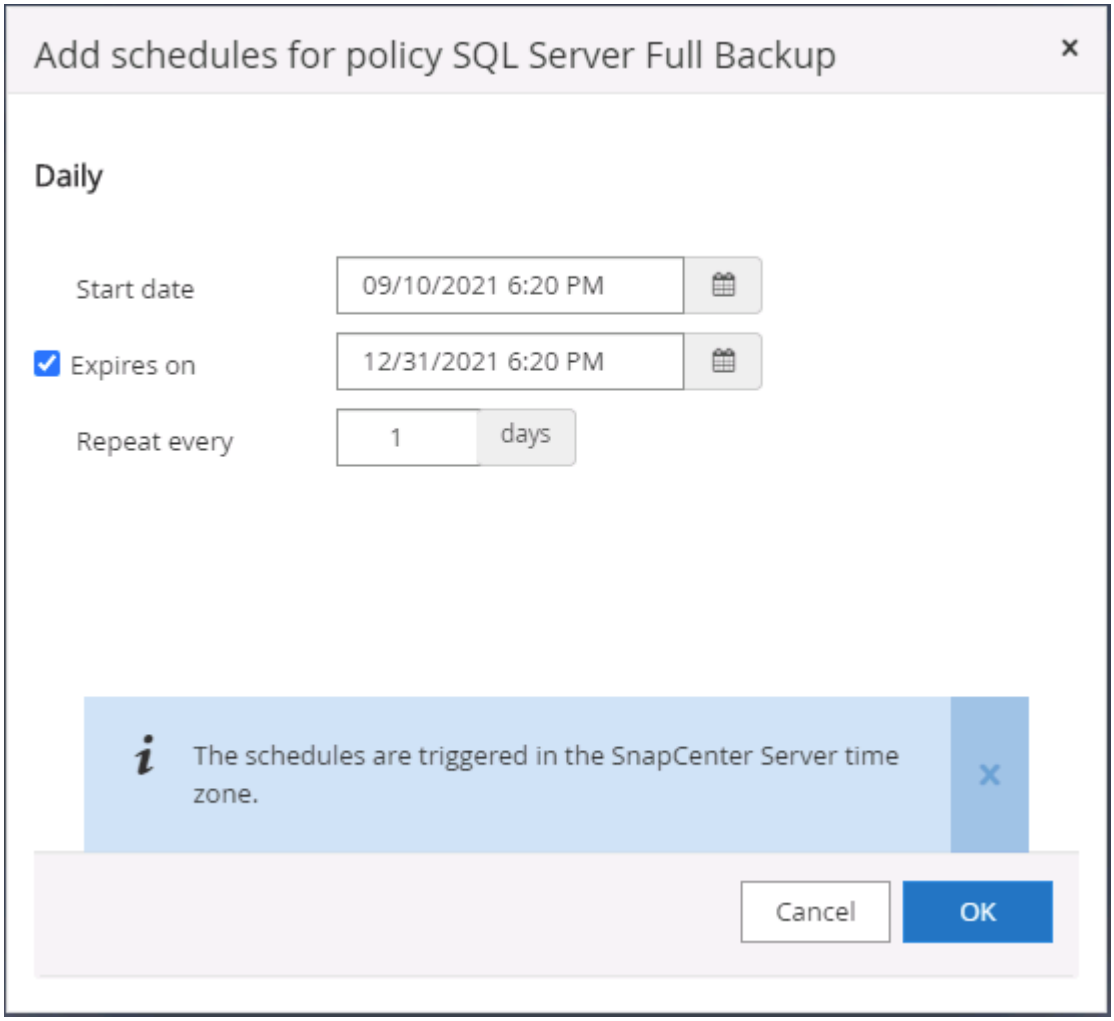
2. Sélectionnez les ressources de base de données à sauvegarder.



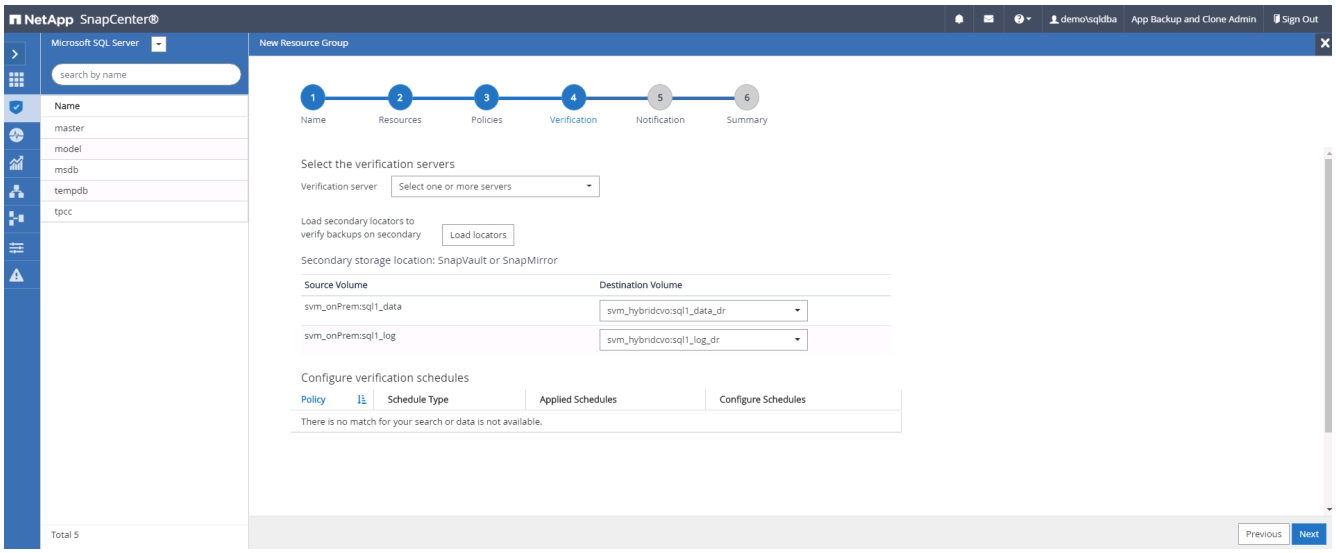
3. Sélectionnez une politique de sauvegarde SQL complète créée dans la section 7.



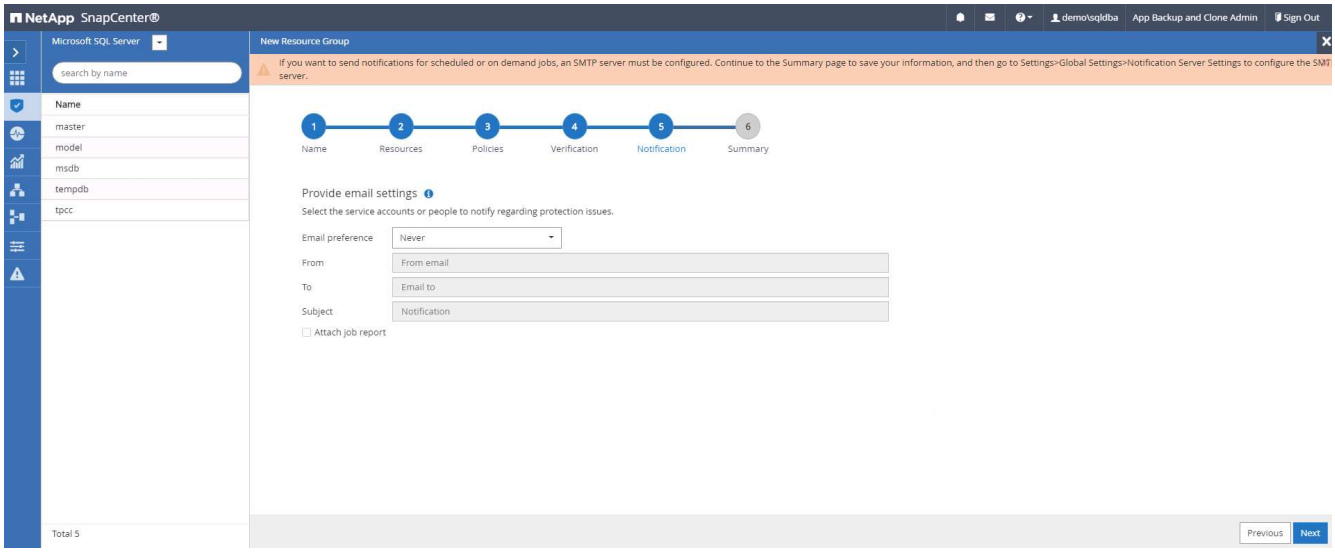
4. Ajoutez le timing exact des sauvegardes ainsi que la fréquence.



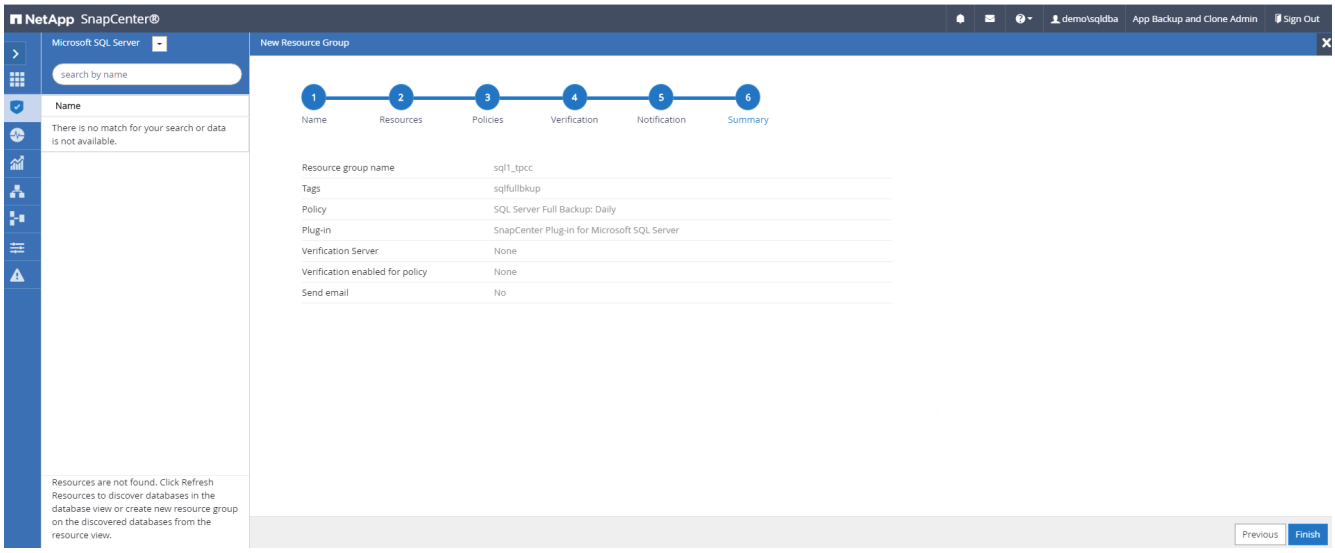
5. Choisissez le serveur de vérification pour la sauvegarde sur le serveur secondaire si la vérification de la sauvegarde doit être effectuée. Cliquez sur Charger le localisateur pour renseigner l'emplacement de stockage secondaire.



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

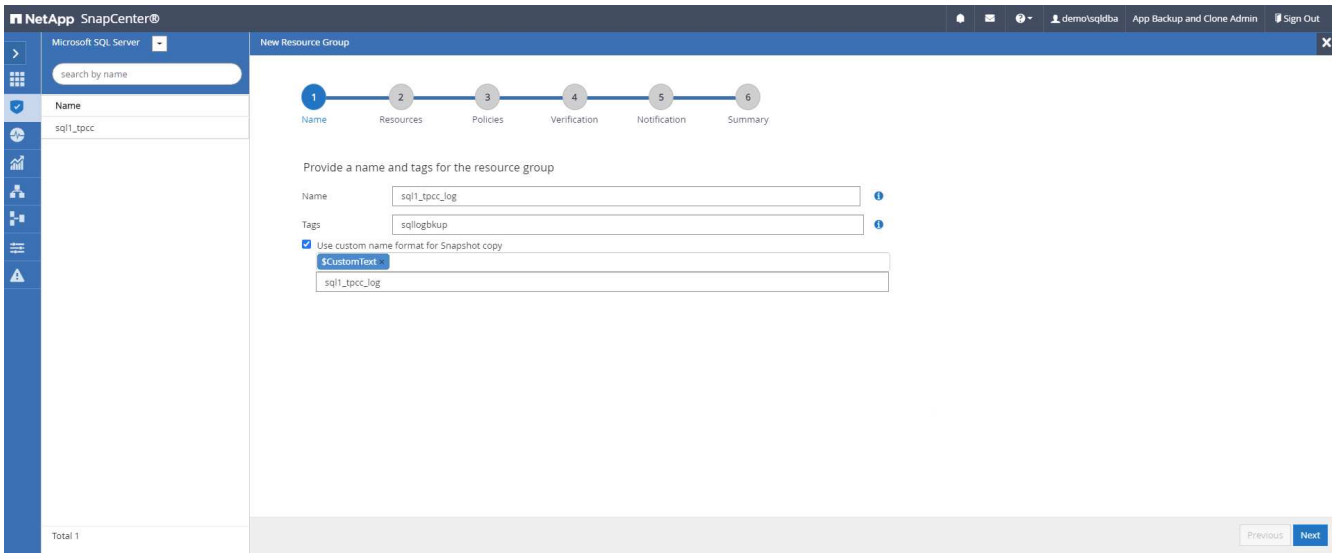


7. Résumé.

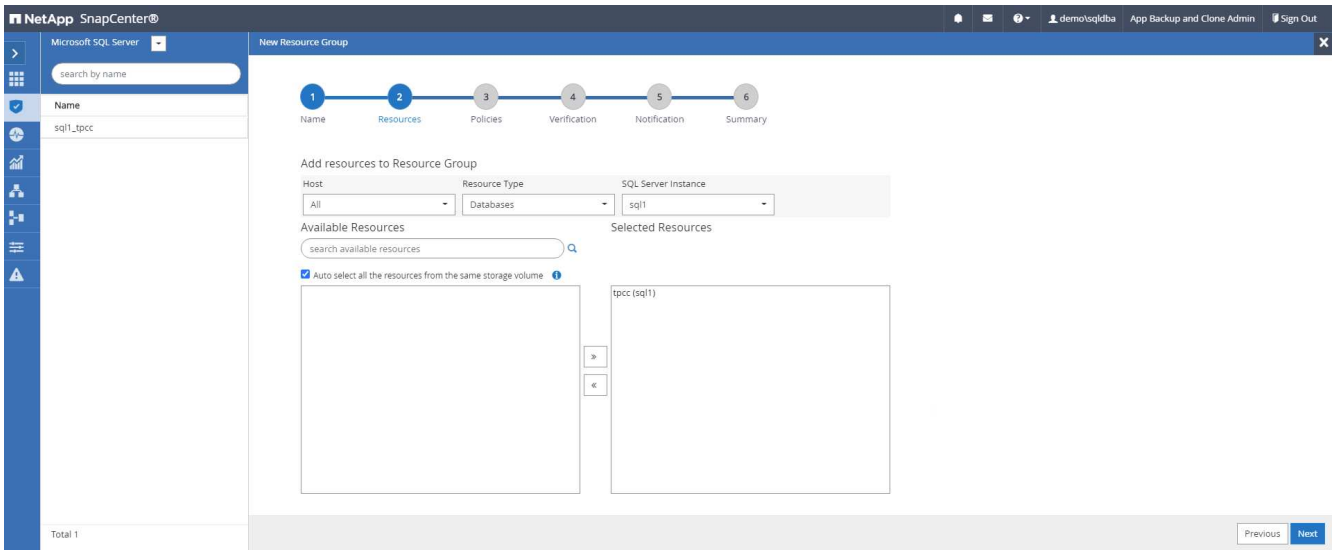


Créer un groupe de ressources pour la sauvegarde des journaux de SQL Server

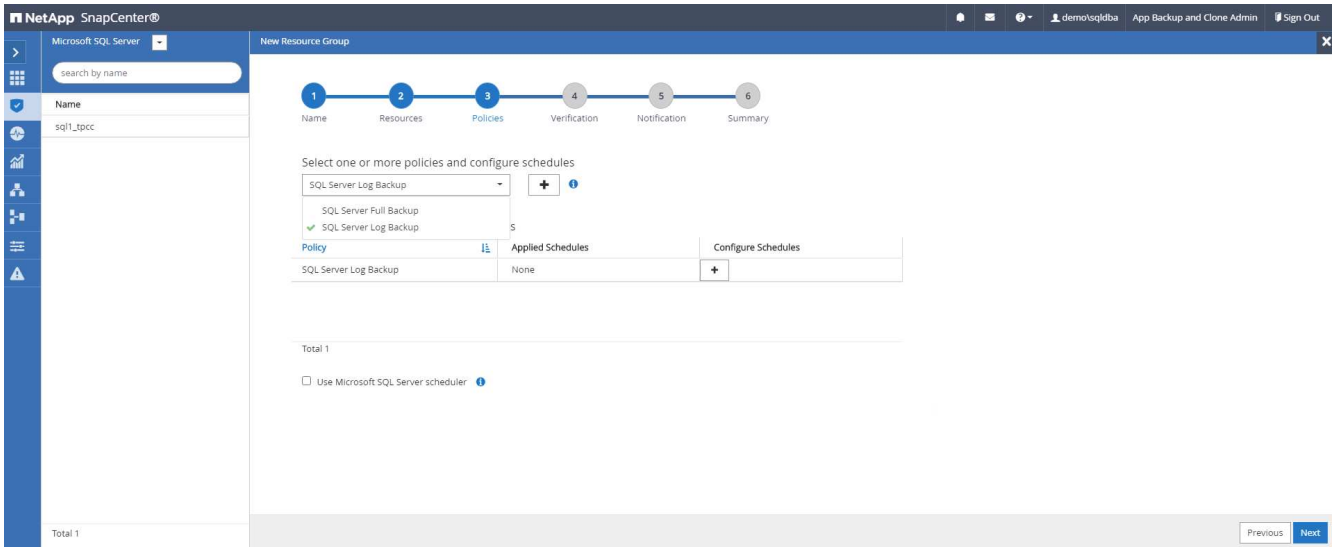
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez une base de données ou un groupe de ressources pour lancer le flux de travail de création du groupe de ressources. Fournissez le nom et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



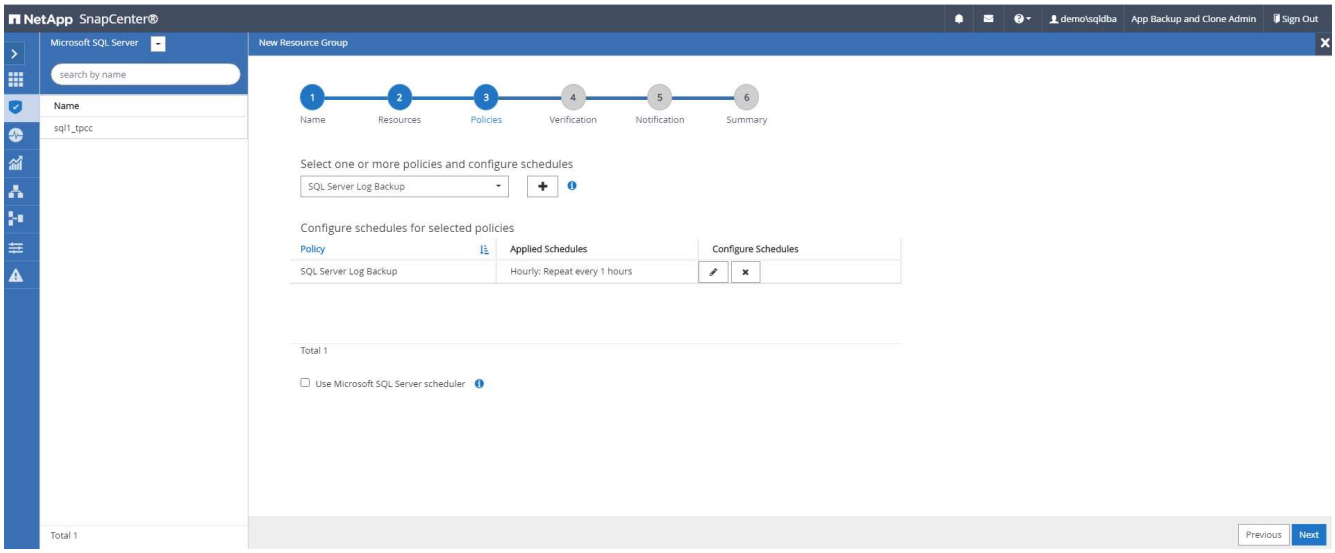
2. Sélectionnez les ressources de base de données à sauvegarder.



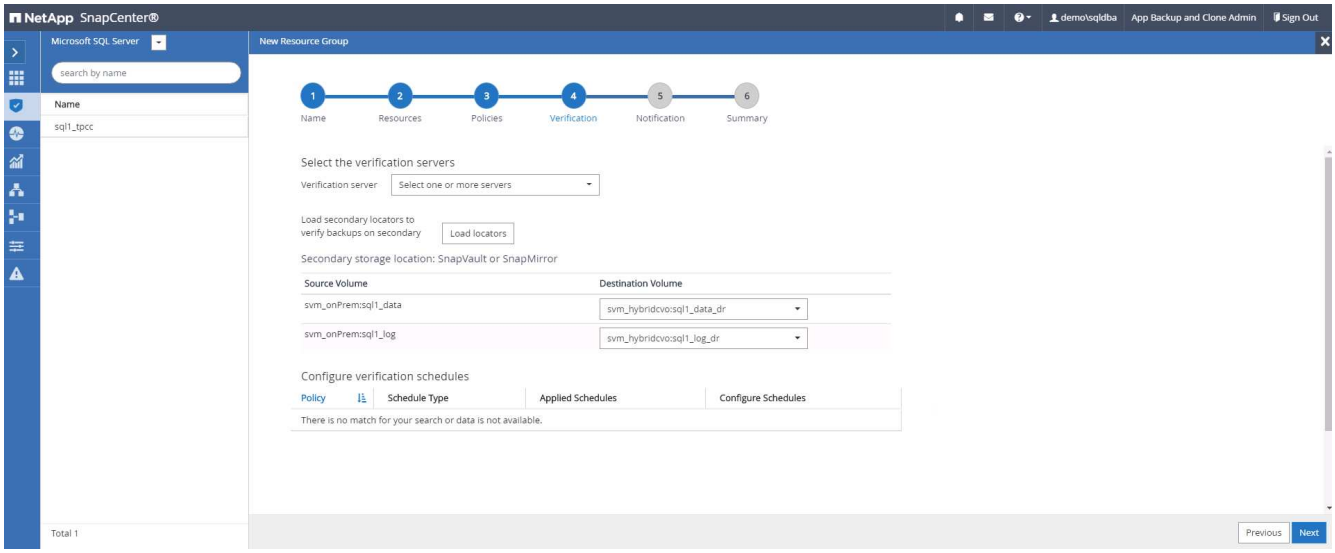
3. Sélectionnez une politique de sauvegarde du journal SQL créée dans la section 7.



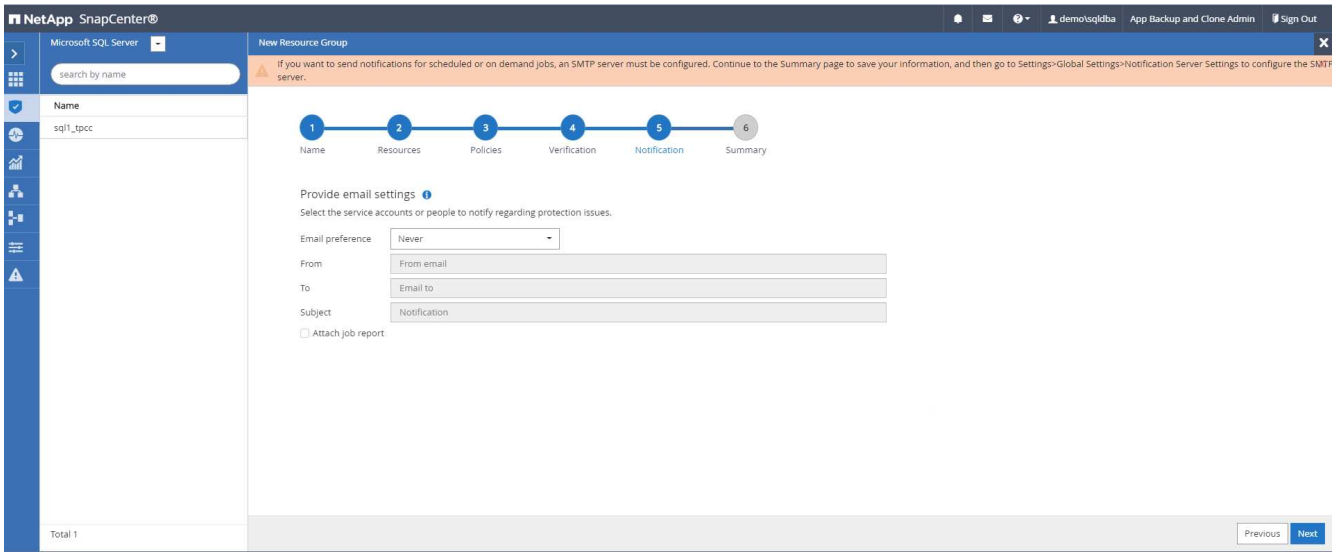
4. Ajoutez le timing exact de la sauvegarde ainsi que la fréquence.



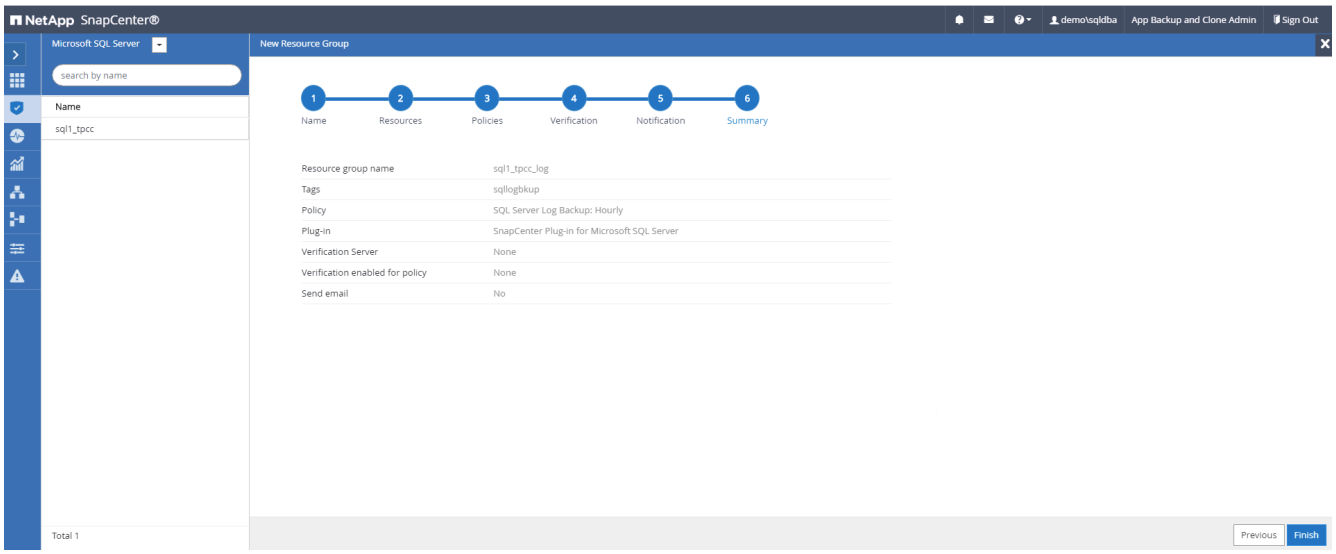
5. Choisissez le serveur de vérification pour la sauvegarde sur le serveur secondaire si la vérification de la sauvegarde doit être effectuée. Cliquez sur le localisateur de charge pour renseigner l'emplacement de stockage secondaire.



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



7. Résumé.

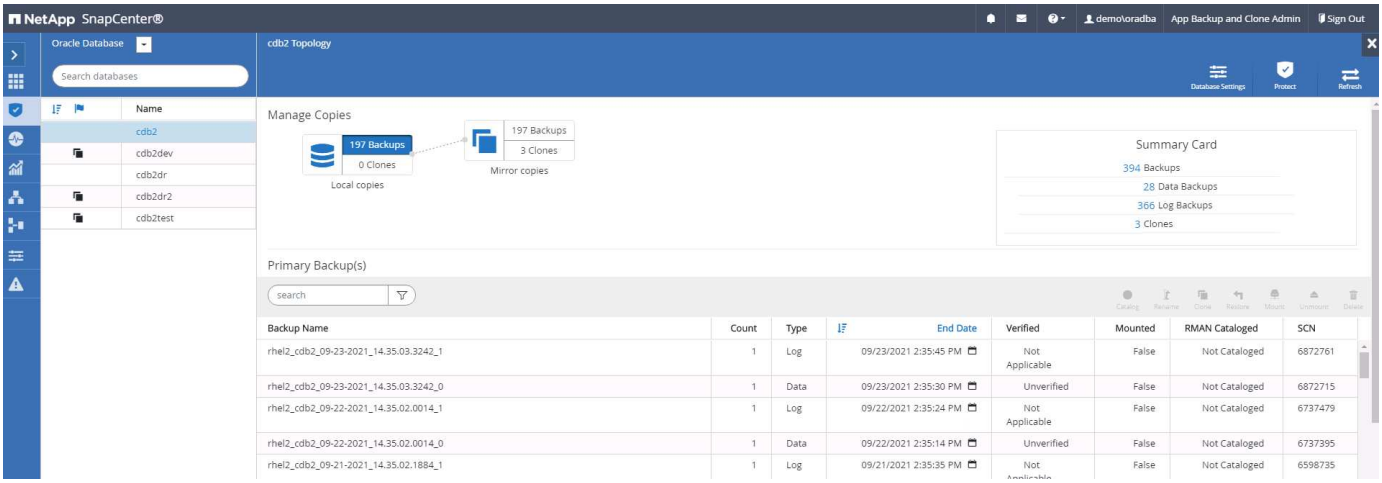


9. Valider la sauvegarde

Une fois les groupes de ressources de sauvegarde de base de données créés pour protéger les ressources de base de données, les tâches de sauvegarde s'exécutent selon la planification prédéfinie. Vérifiez l'état d'exécution du travail sous l'onglet Surveiller.

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 vers un emplacement secondaire dans le cloud public.



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

Premiers pas avec le cloud public AWS

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

Cloud public AWS

Pour faciliter le suivi, nous avons créé ce document basé sur un déploiement dans AWS. Cependant, le processus est très similaire pour Azure et GCP.

1. Contrôle pré-vol

Avant le déploiement, assurez-vous que l'infrastructure est en place pour permettre le déploiement à l'étape suivante. Cela comprend les éléments suivants :

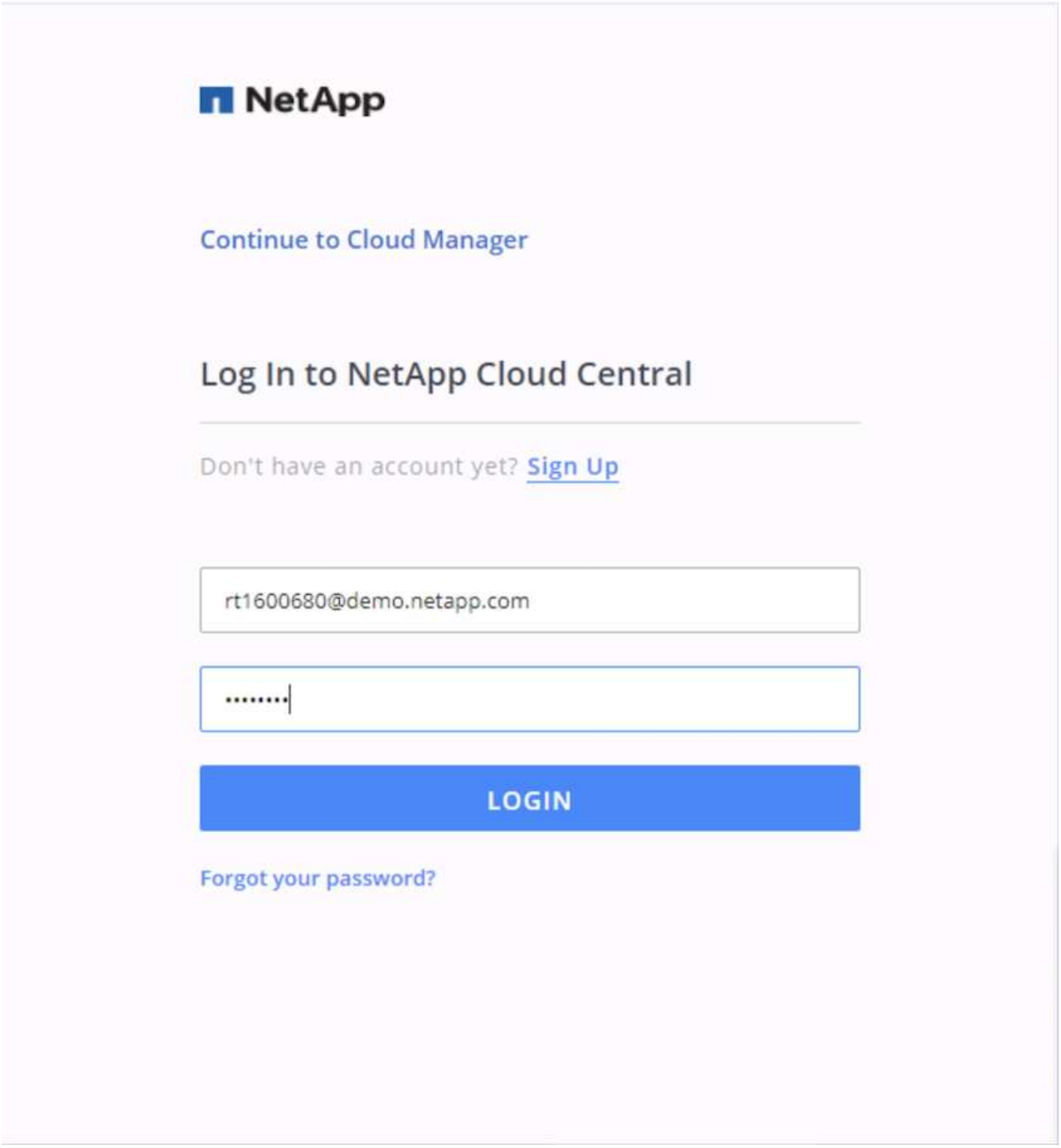
- compte AWS
- VPC dans la région de votre choix
- Sous-réseau avec accès à l'Internet public
- Autorisations pour ajouter des rôles IAM à votre compte AWS
- Une clé secrète et une clé d'accès pour votre utilisateur AWS

2. Étapes pour déployer Cloud Manager et Cloud Volumes ONTAP dans AWS

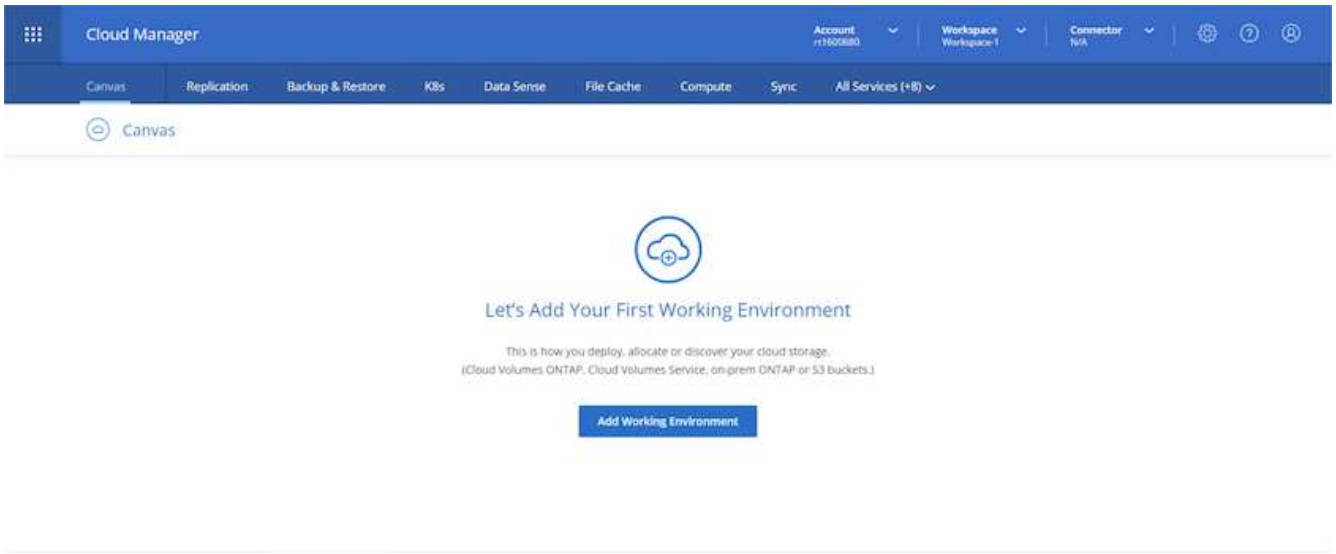
Il existe de nombreuses méthodes pour déployer Cloud Manager et Cloud Volumes ONTAP; cette méthode est la plus simple mais nécessite le plus d'autorisations. Si cette méthode n'est pas adaptée à votre environnement AWS, veuillez consulter le "Documentation NetApp Cloud" .

Déployer le connecteur Cloud Manager

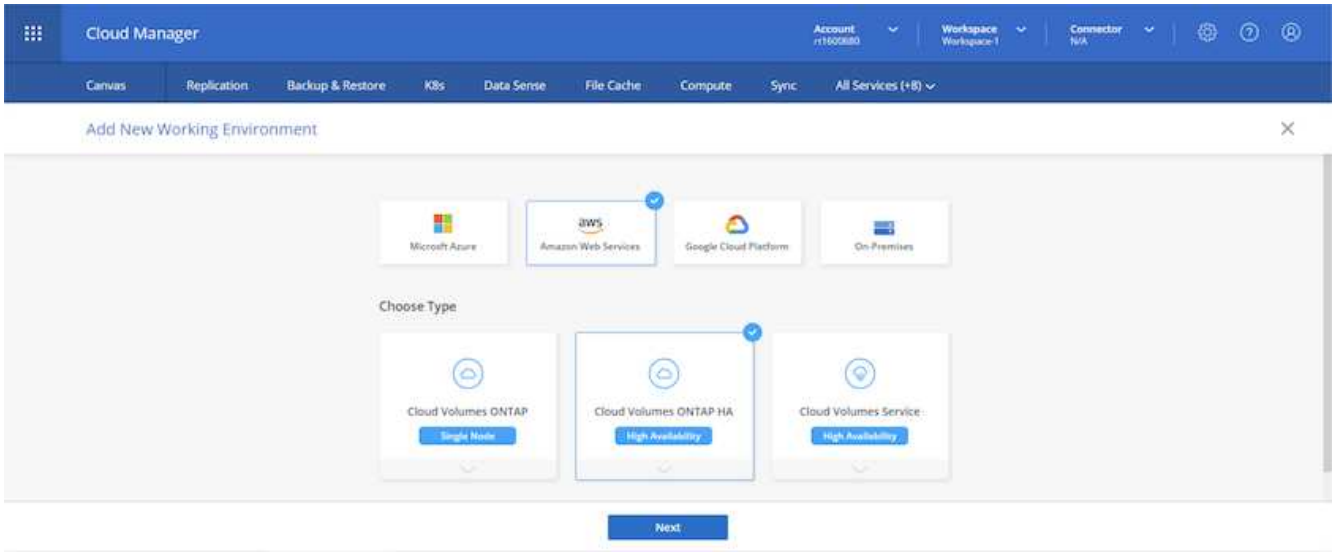
1. Accéder à "NetApp BlueXP" et connectez-vous ou inscrivez-vous.



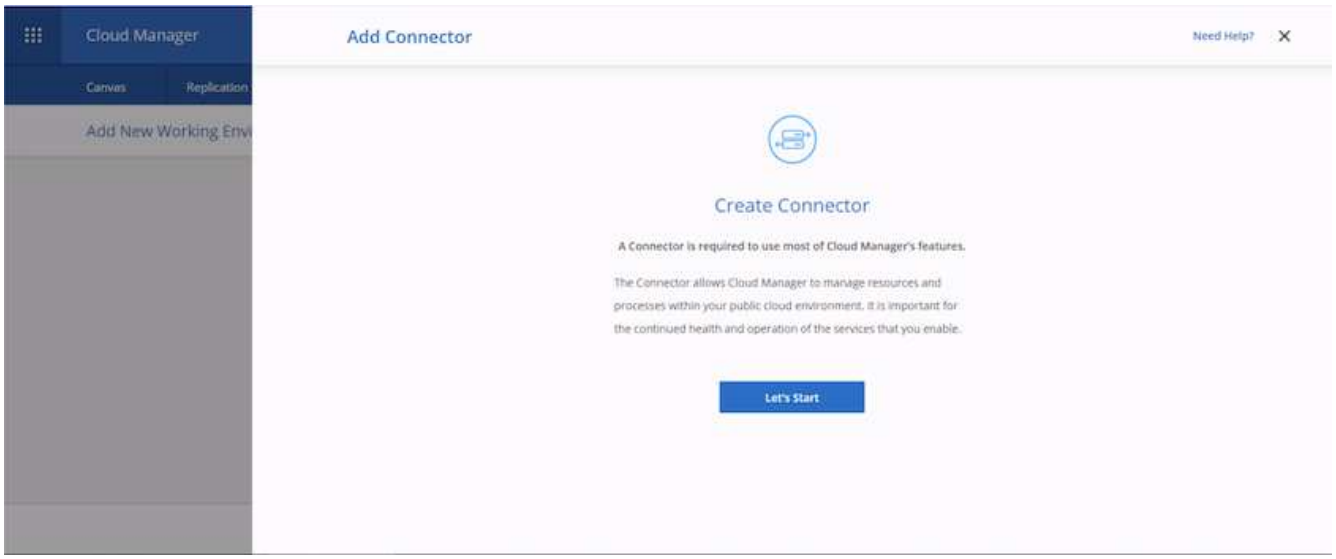
2. Après vous être connecté, vous devriez être redirigé vers le Canvas.



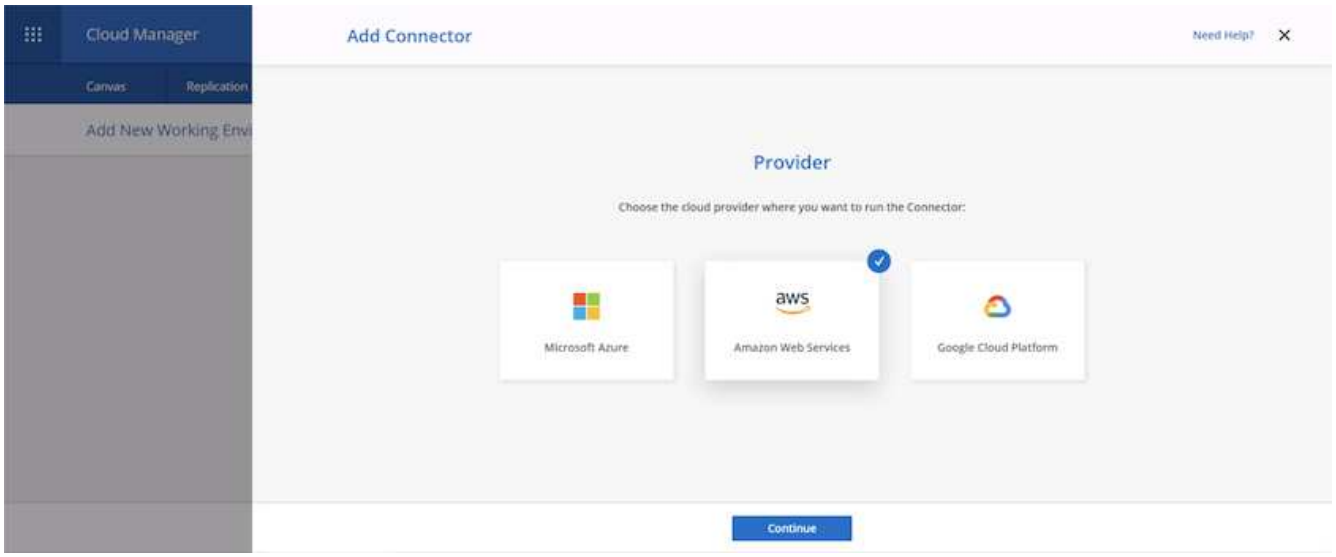
3. Cliquez sur « Ajouter un environnement de travail » et choisissez Cloud Volumes ONTAP dans AWS. Ici, vous choisissez également si vous souhaitez déployer un système à nœud unique ou une paire à haute disponibilité. J'ai choisi de déployer une paire haute disponibilité.



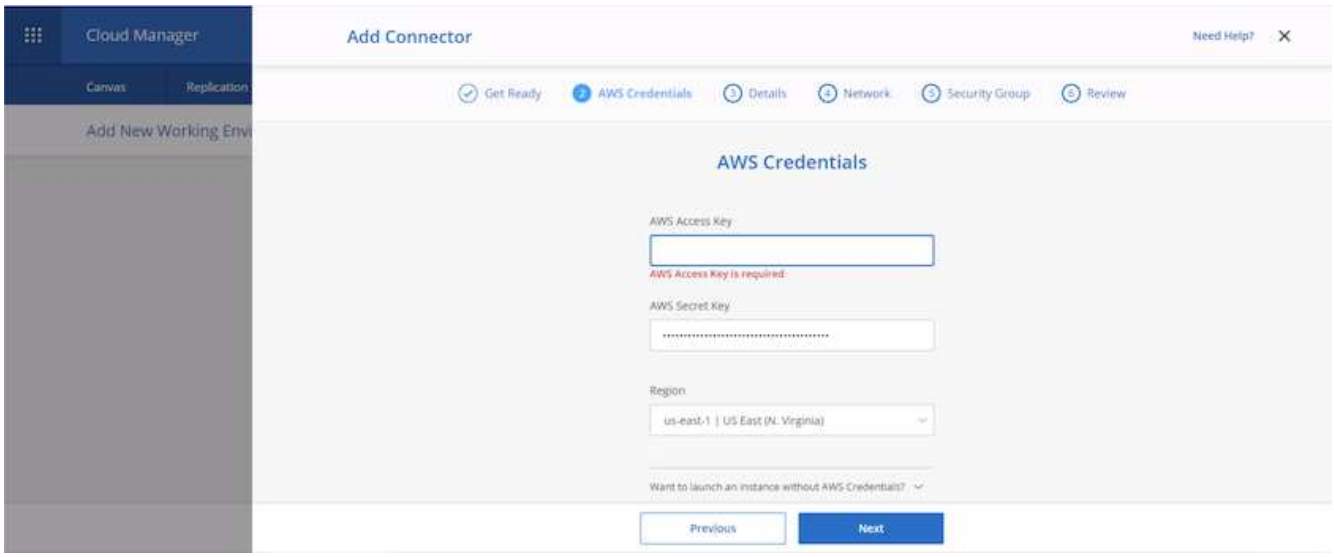
4. Si aucun connecteur n'a été créé, une fenêtre contextuelle apparaît vous demandant de créer un connecteur.



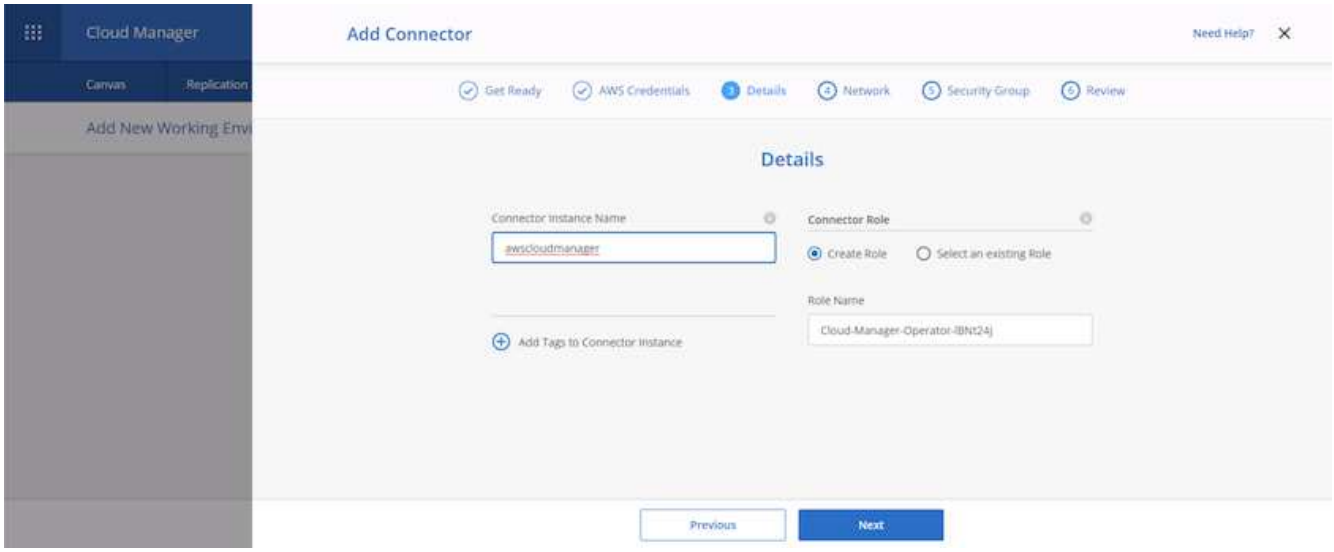
5. Cliquez sur Commencer, puis choisissez AWS.



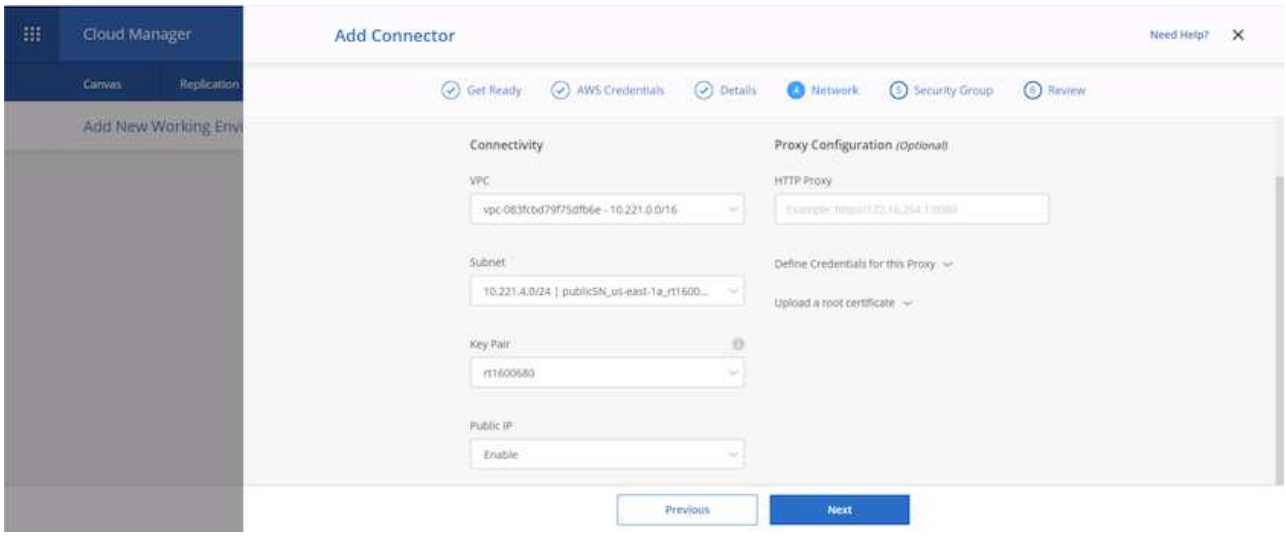
6. Entrez votre clé secrète et votre clé d'accès. Assurez-vous que votre utilisateur dispose des autorisations appropriées décrites sur le "Page des politiques NetApp" .



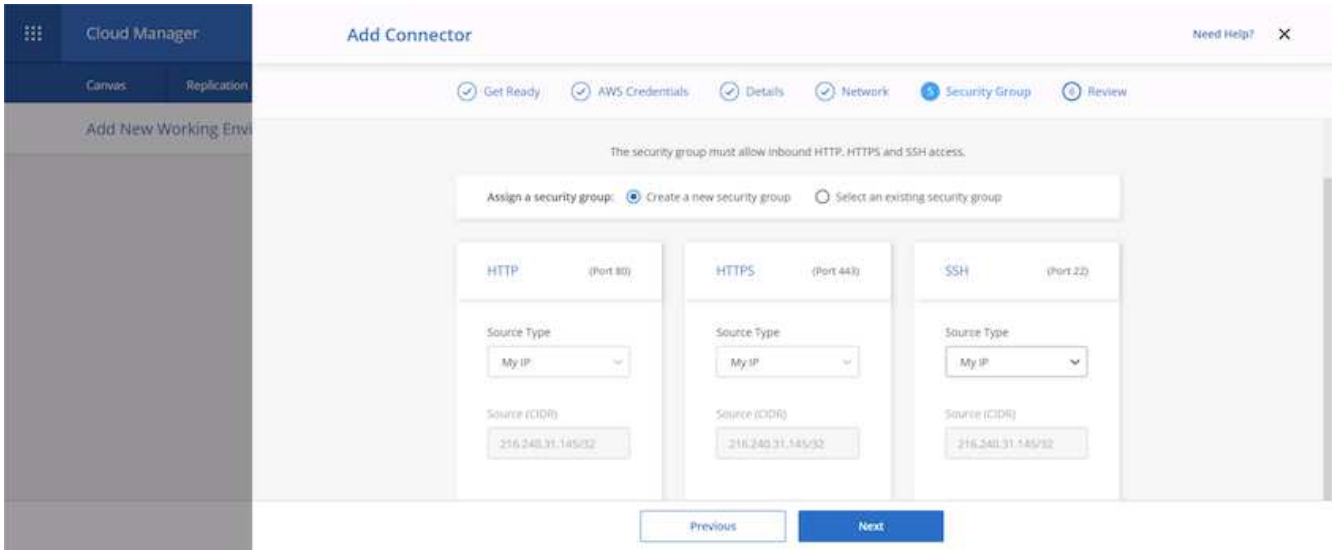
7. Donnez un nom au connecteur et utilisez un rôle prédéfini comme décrit sur le "Page des politiques NetApp" ou demandez à Cloud Manager de créer le rôle pour vous.



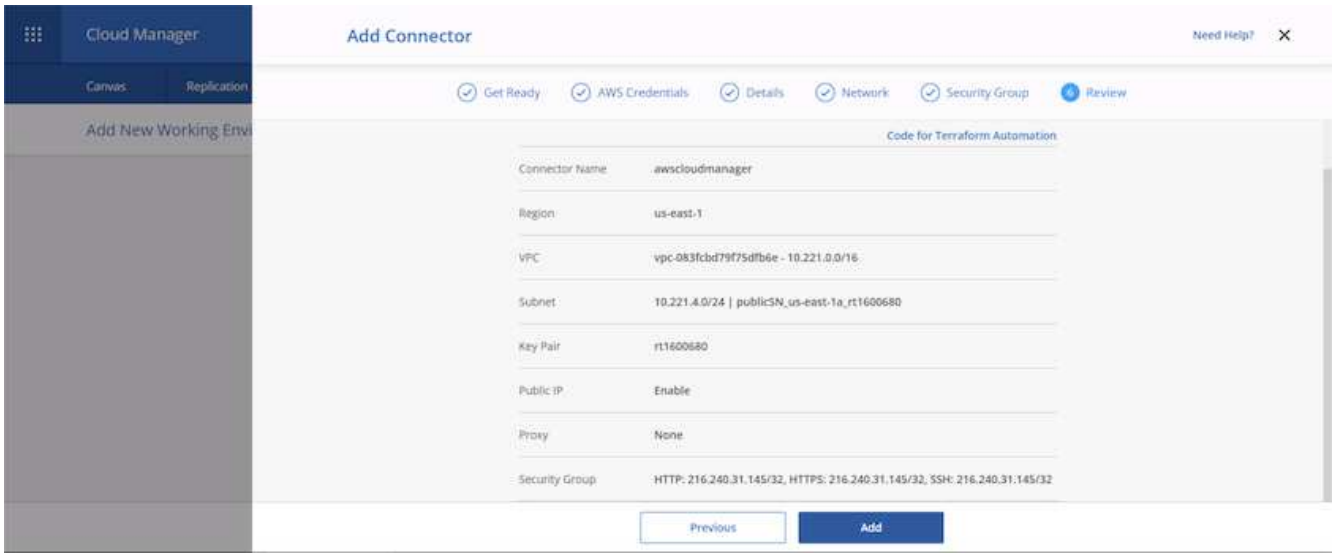
8. Fournissez les informations réseau nécessaires au déploiement du connecteur. Vérifiez que l'accès Internet sortant est activé en :
   a. Attribuer au connecteur une adresse IP publique
   b. Donner au connecteur un proxy pour fonctionner
   c. Donner au connecteur un itinéraire vers l'Internet public via une passerelle Internet



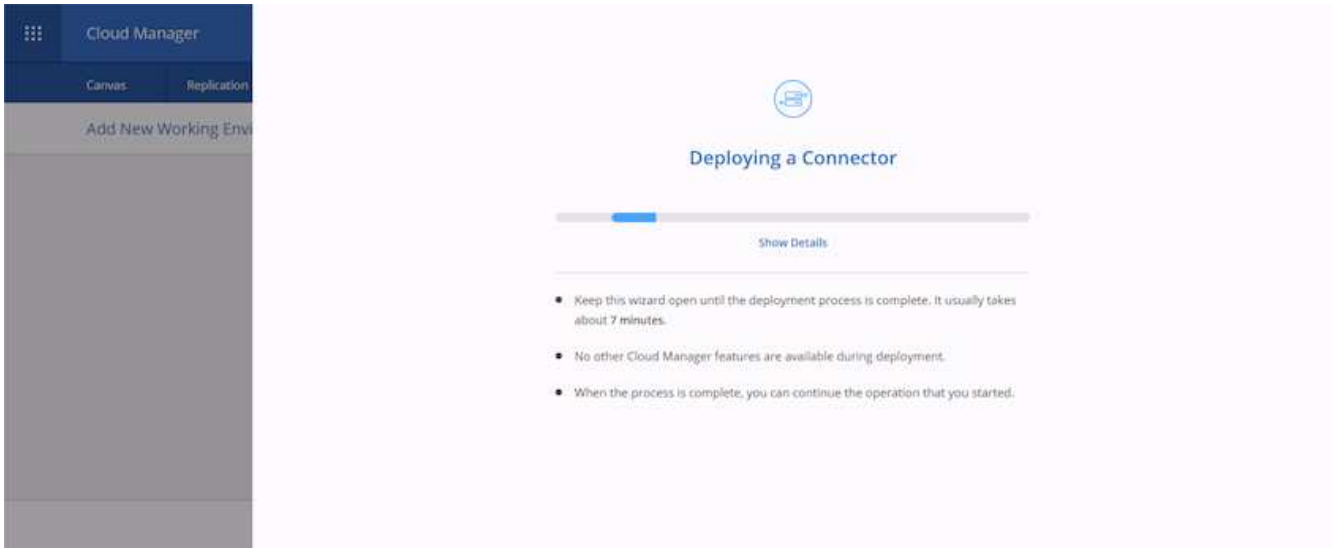
9. Assurez la communication avec le connecteur via SSH, HTTP et HTTPS en fournissant un groupe de sécurité ou en créant un nouveau groupe de sécurité. J'ai activé l'accès au connecteur à partir de mon adresse IP uniquement.



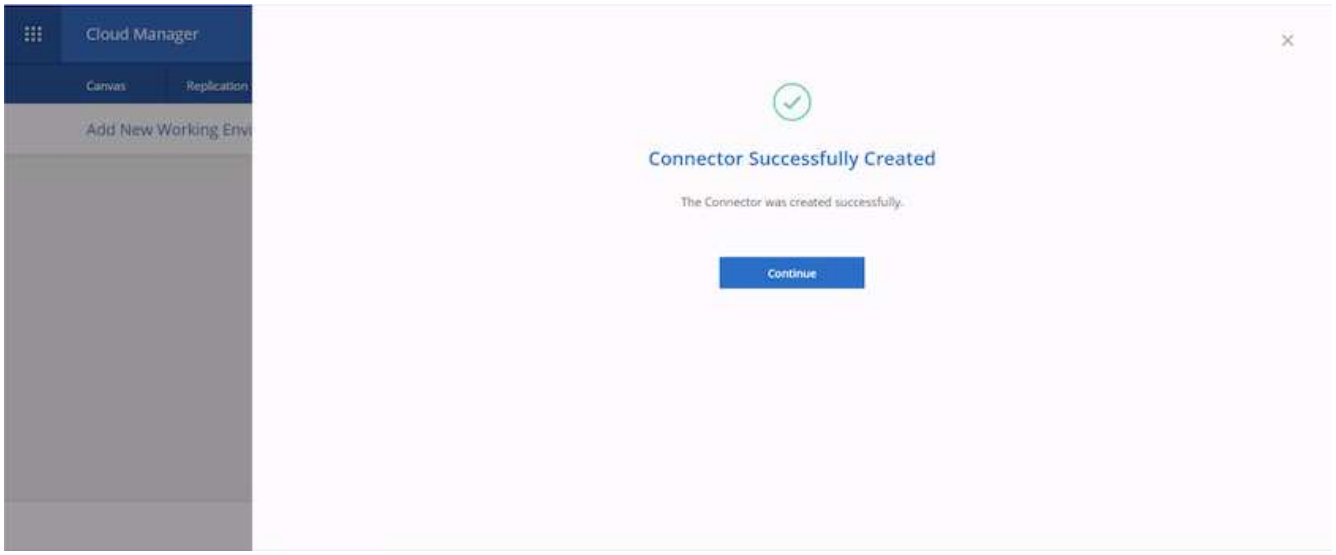
10. Consultez les informations sur la page récapitulative et cliquez sur Ajouter pour déployer le connecteur.



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

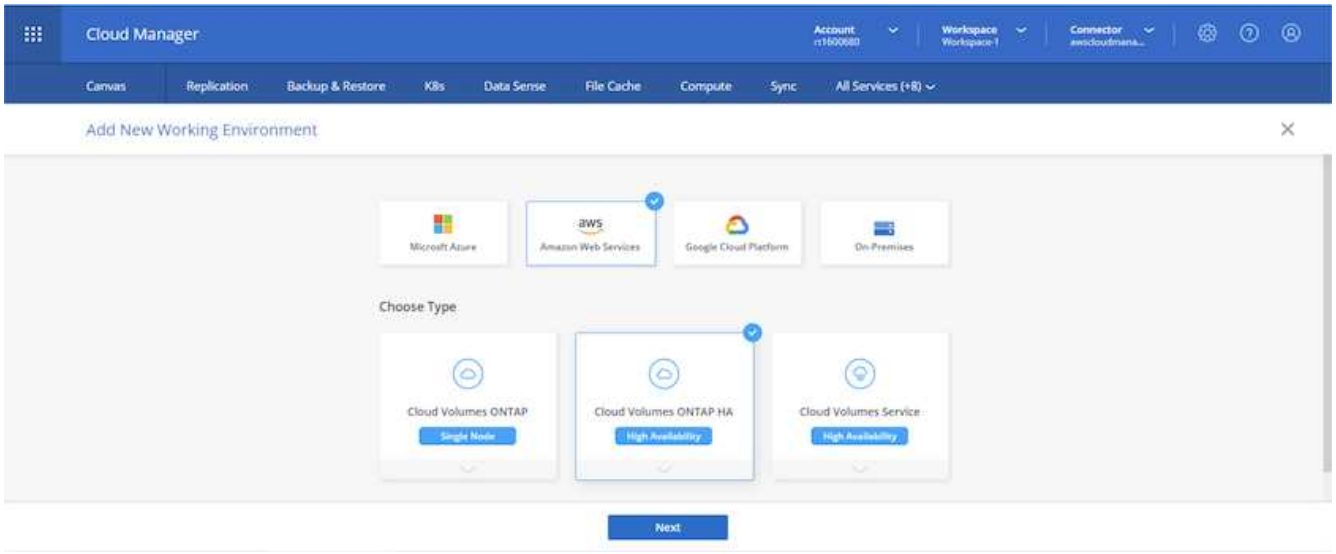


12. Une fois le déploiement terminé, une page de réussite s'affiche.

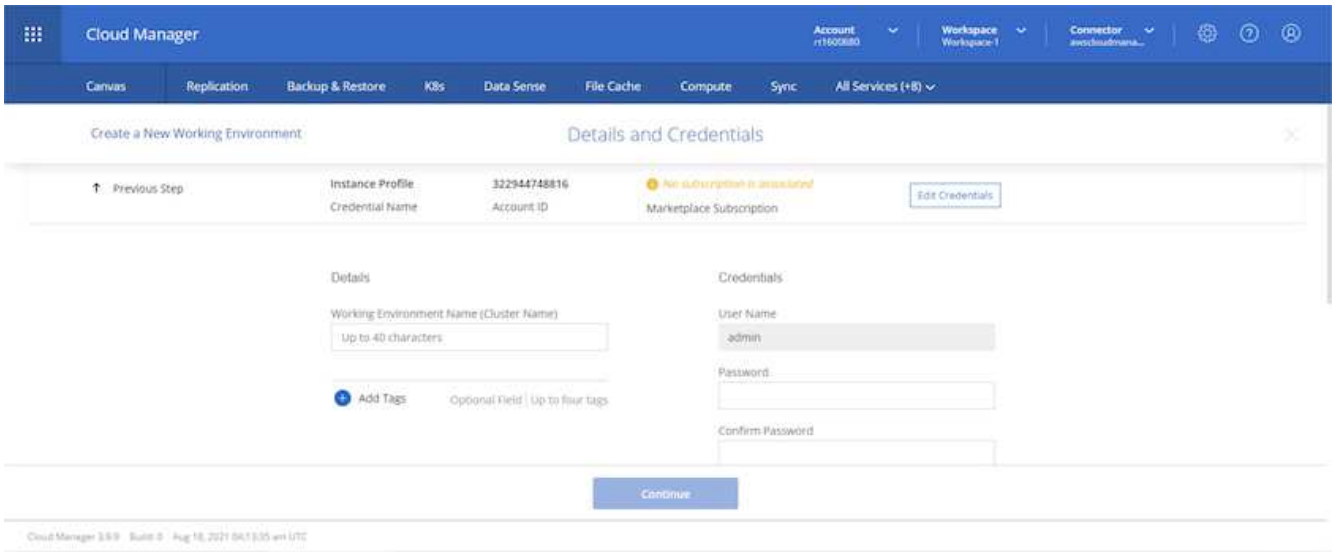


Déployer Cloud Volumes ONTAP

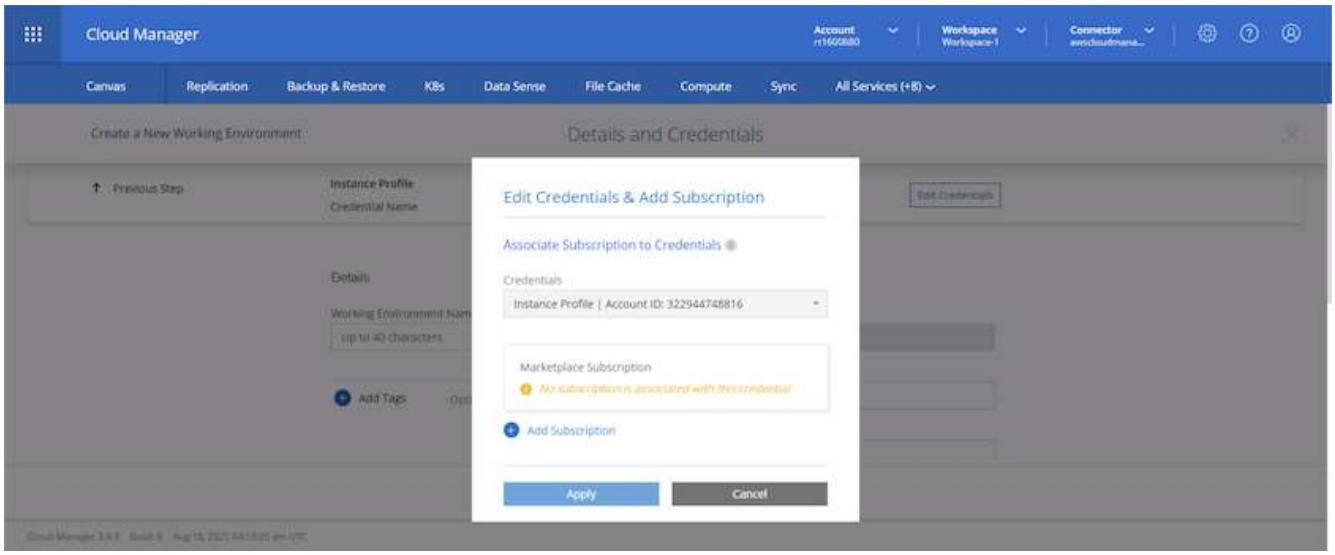
1. Sélectionnez AWS et le type de déploiement en fonction de vos besoins.



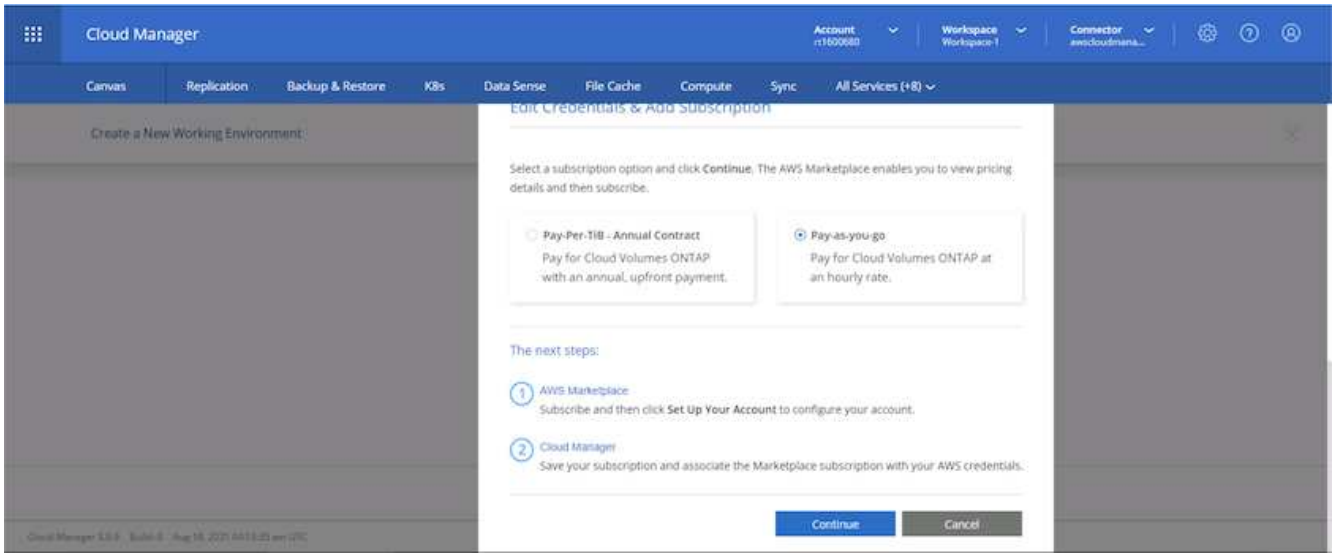
2. Si aucun abonnement n'a été attribué et que vous souhaitez acheter avec PAYGO, choisissez Modifier les informations d'identification.



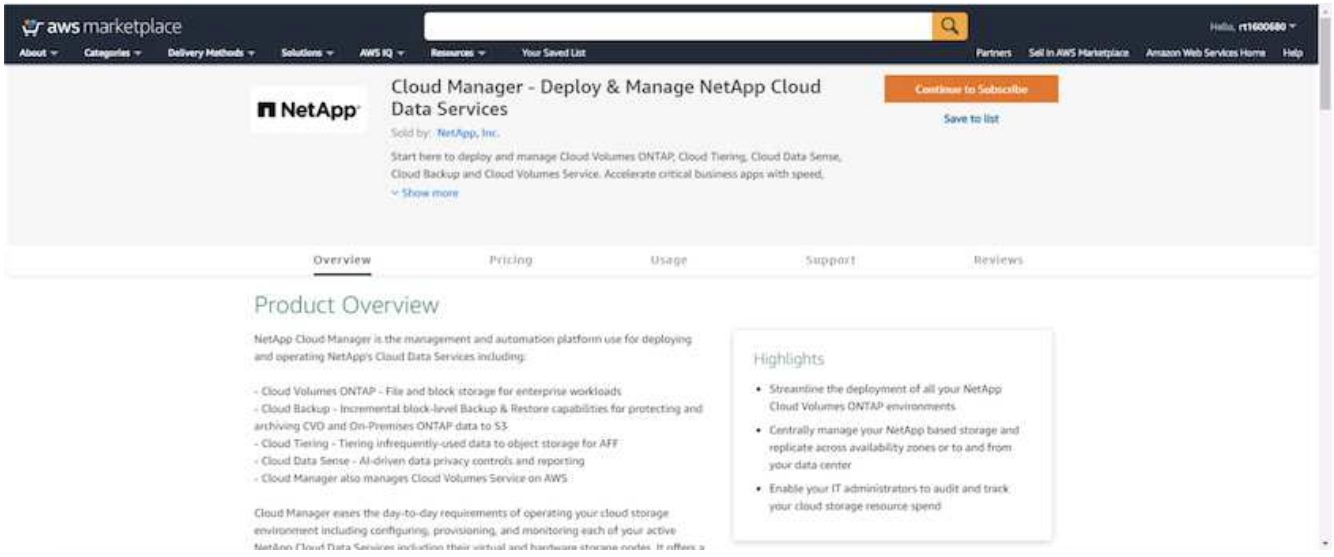
3. Choisissez Ajouter un abonnement.



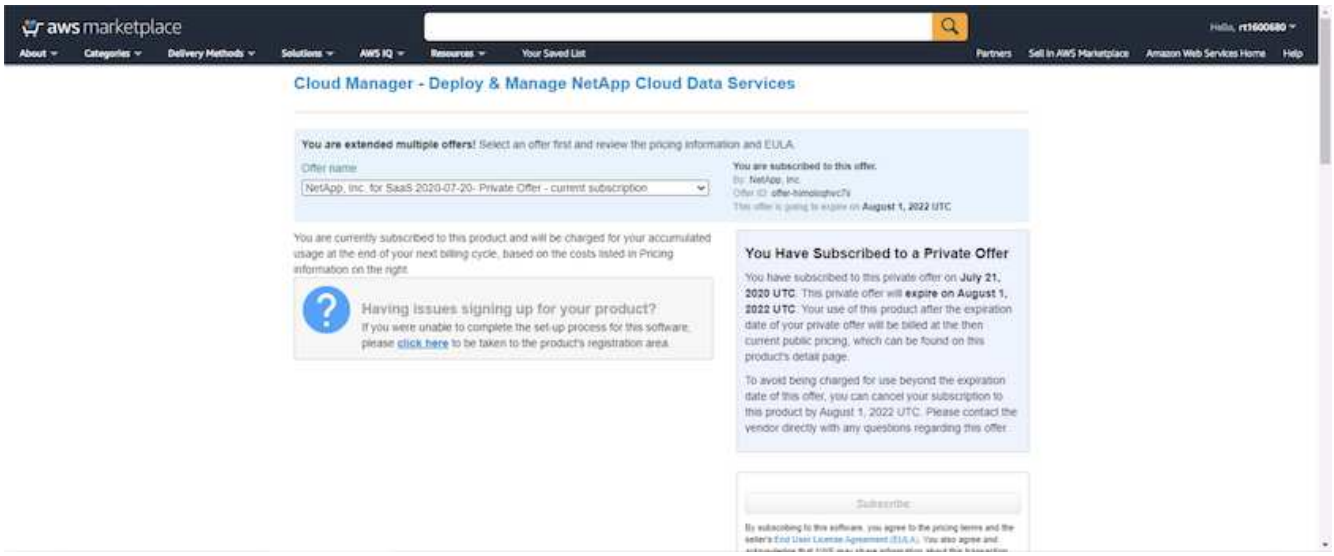
4. Choisissez le type de contrat auquel vous souhaitez souscrire. J'ai choisi le paiement à l'utilisation.



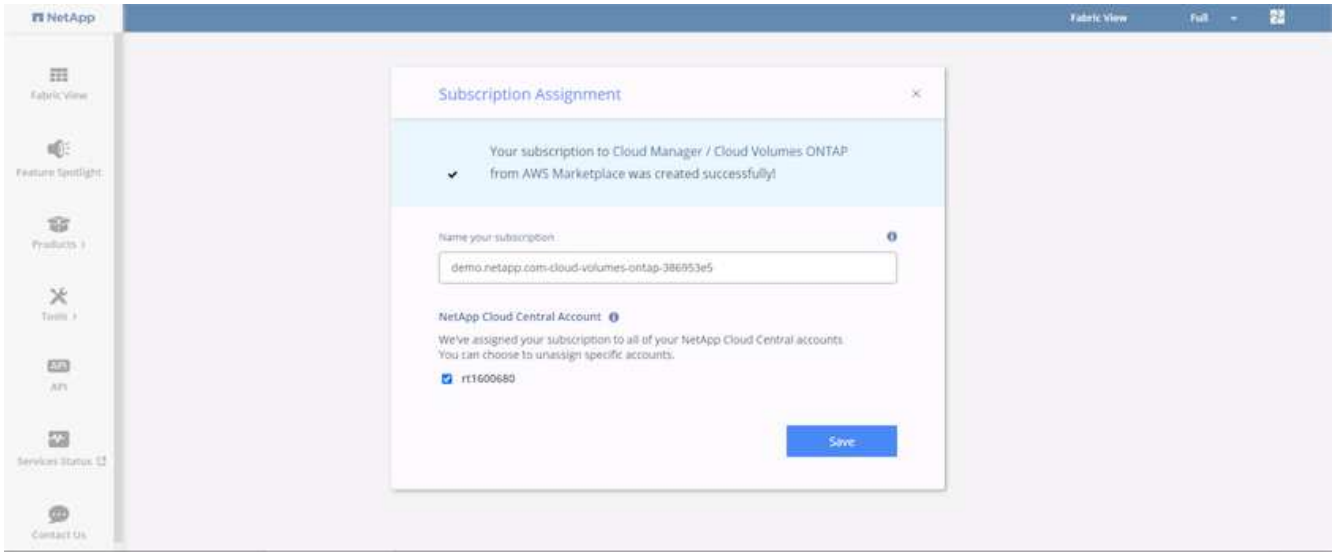
5. Vous êtes redirigé vers AWS ; choisissez Continuer pour vous abonner.



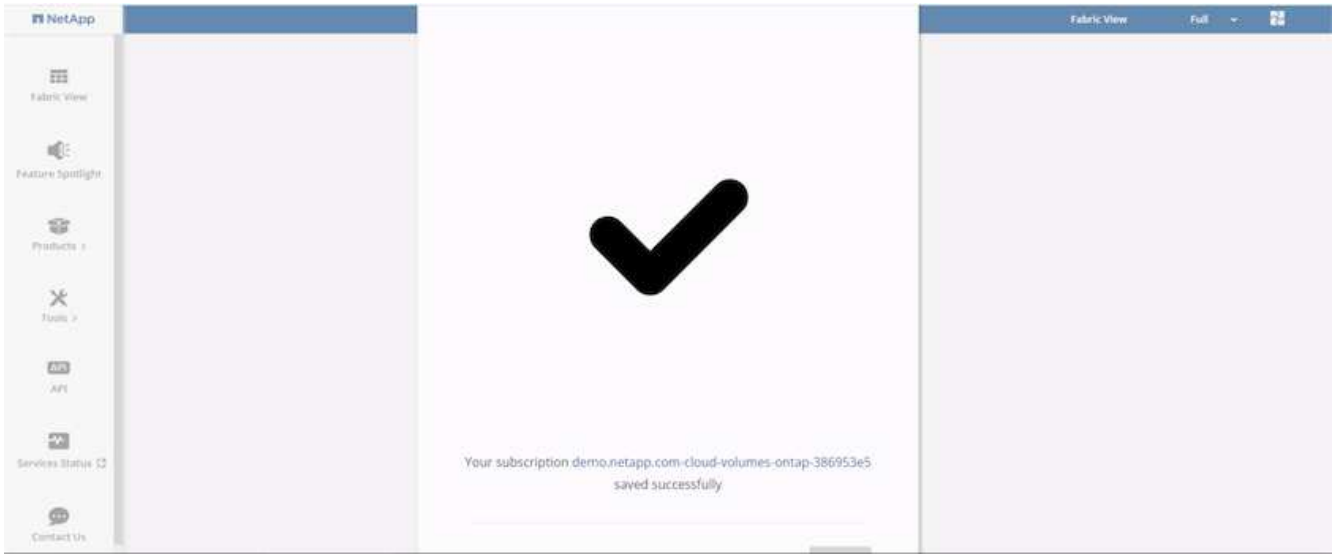
6. Abonnez-vous et vous serez redirigé vers NetApp Cloud Central. Si vous êtes déjà abonné et que vous n'êtes pas redirigé, choisissez le lien « Cliquez ici ».



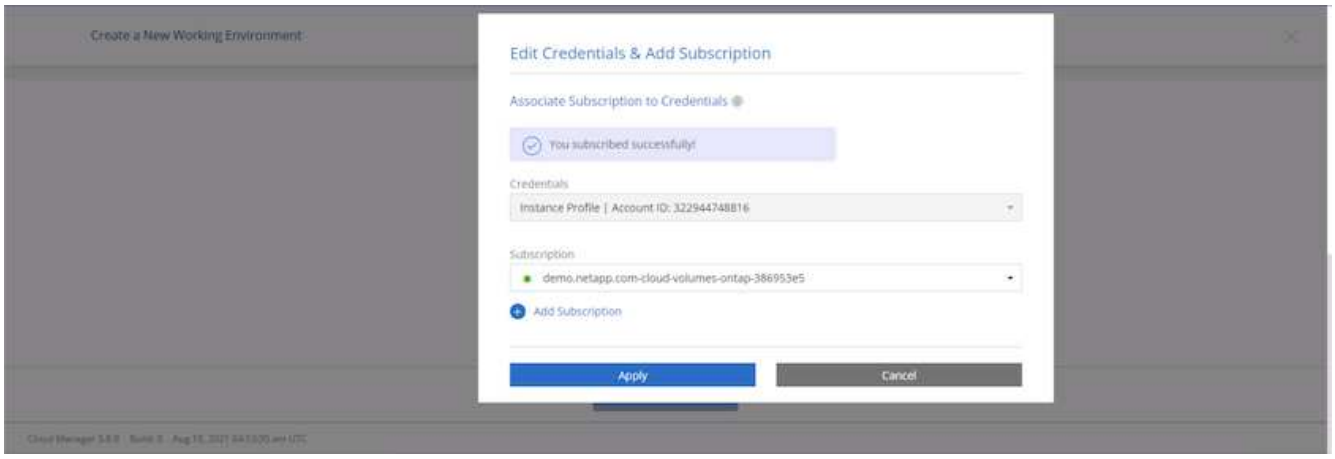
7. Vous êtes redirigé vers Cloud Central où vous devez nommer votre abonnement et l'attribuer à votre compte Cloud Central.



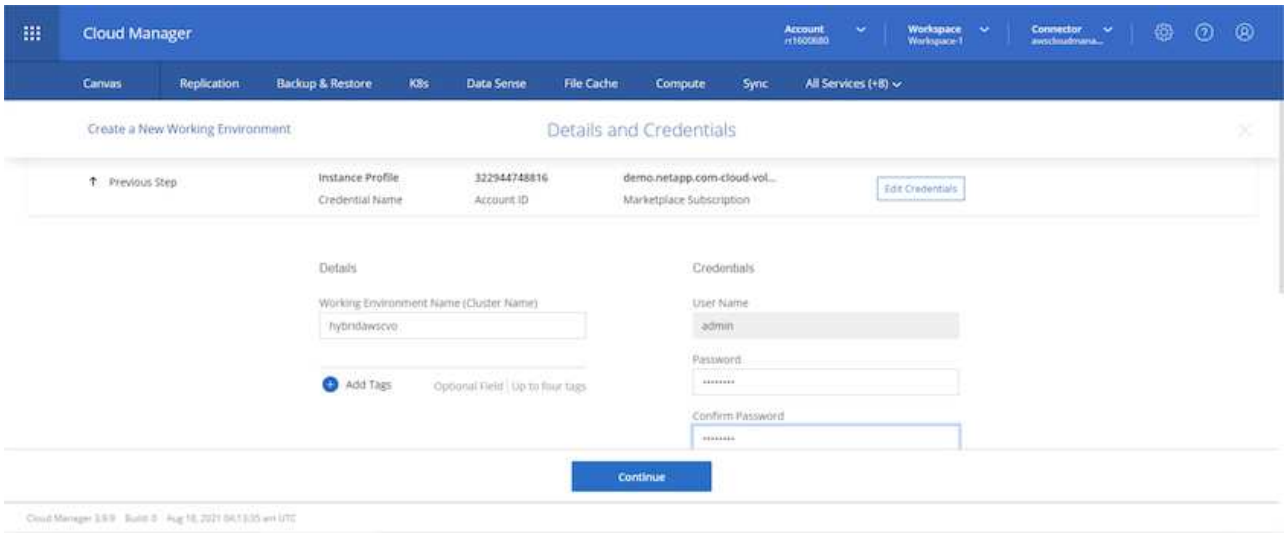
8. En cas de réussite, une page de coche apparaît. Revenez à votre onglet Gestionnaire de Cloud.



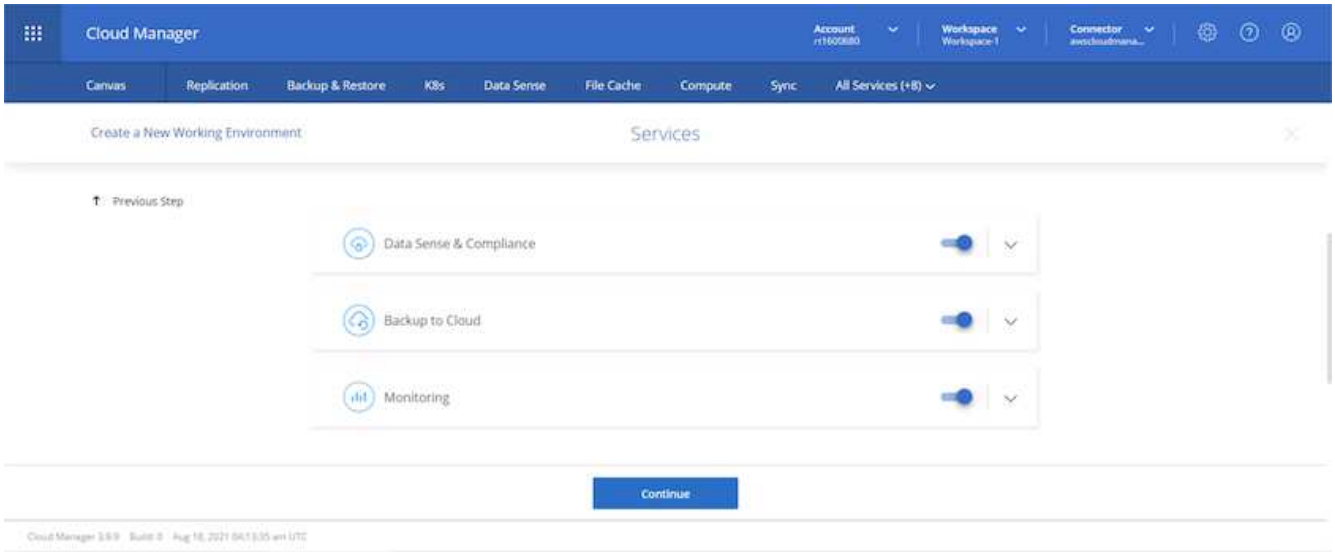
9. L’abonnement apparaît désormais dans Cloud Central. Cliquez sur Appliquer pour continuer.



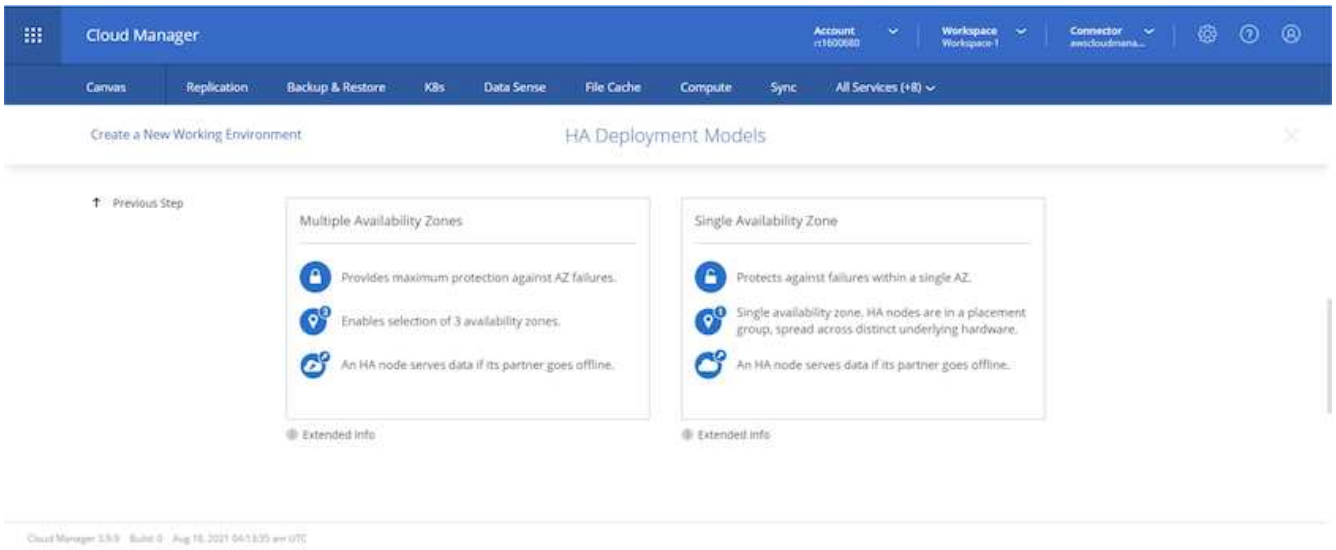
10. Saisissez les détails de l’environnement de travail tels que :
    a. Nom du cluster
    b. Mot de passe du cluster
    c. Balises AWS (facultatif)



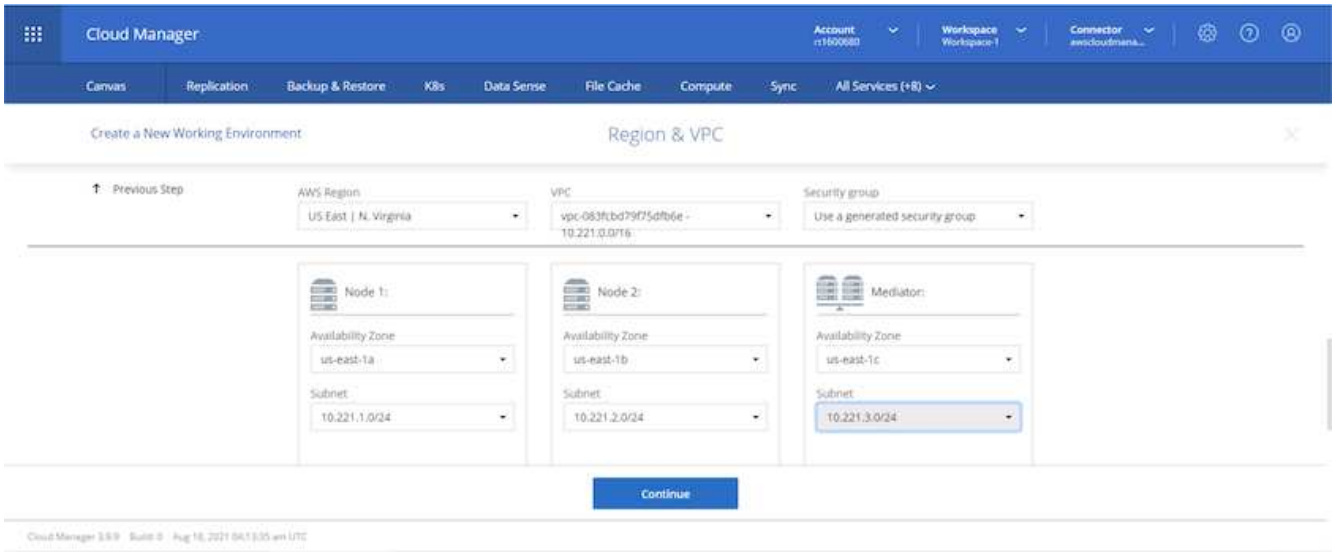
11. Choisissez les services supplémentaires que vous souhaitez déployer. Pour en savoir plus sur ces services, visitez le "BlueXP: des opérations de gestion de données modernes simplifiées" .



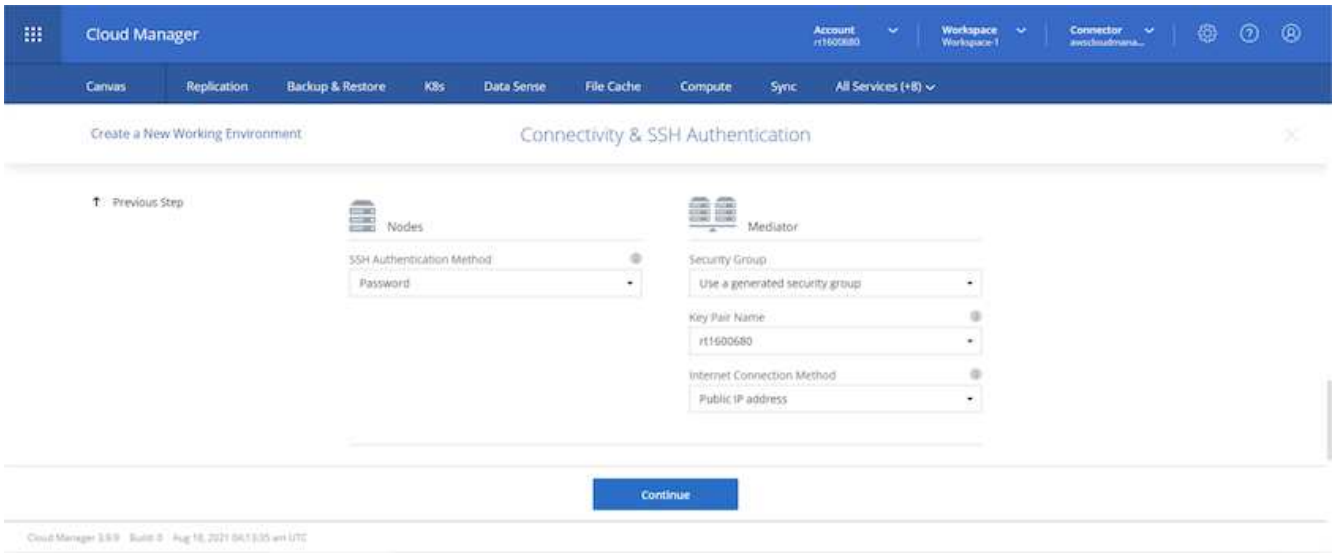
12. Choisissez de déployer dans plusieurs zones de disponibilité (nécessite trois sous-réseaux, chacun dans une zone de disponibilité différente) ou dans une seule zone de disponibilité. J'ai choisi plusieurs AZ.



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

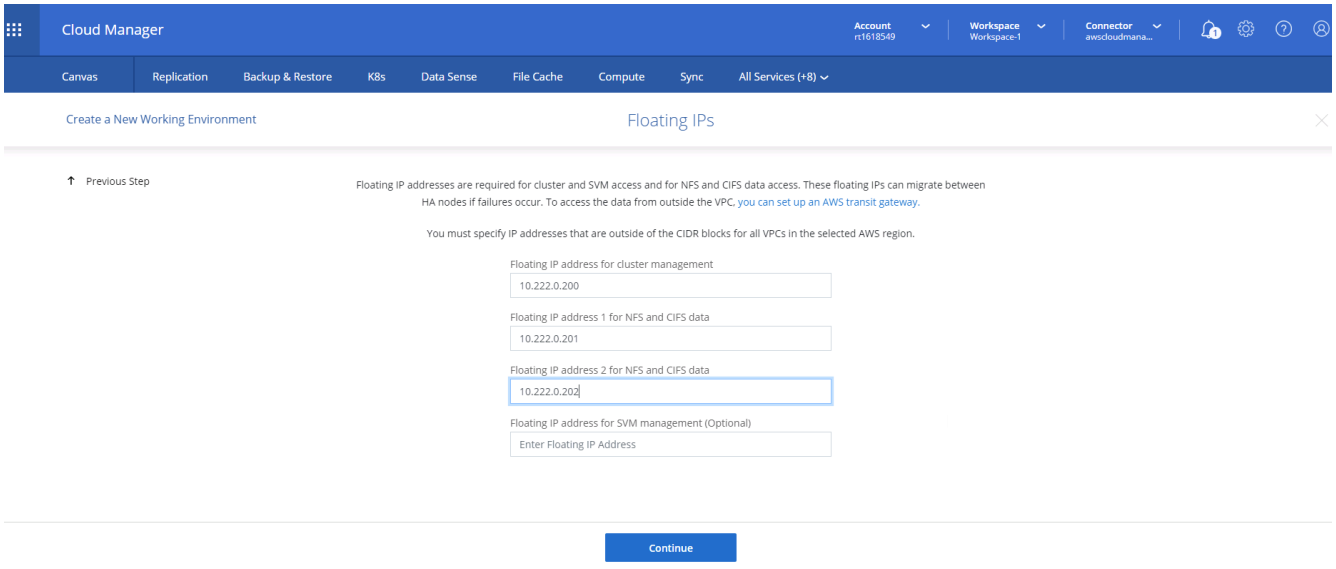


14. Choisissez les méthodes de connexion pour les nœuds ainsi que le médiateur.

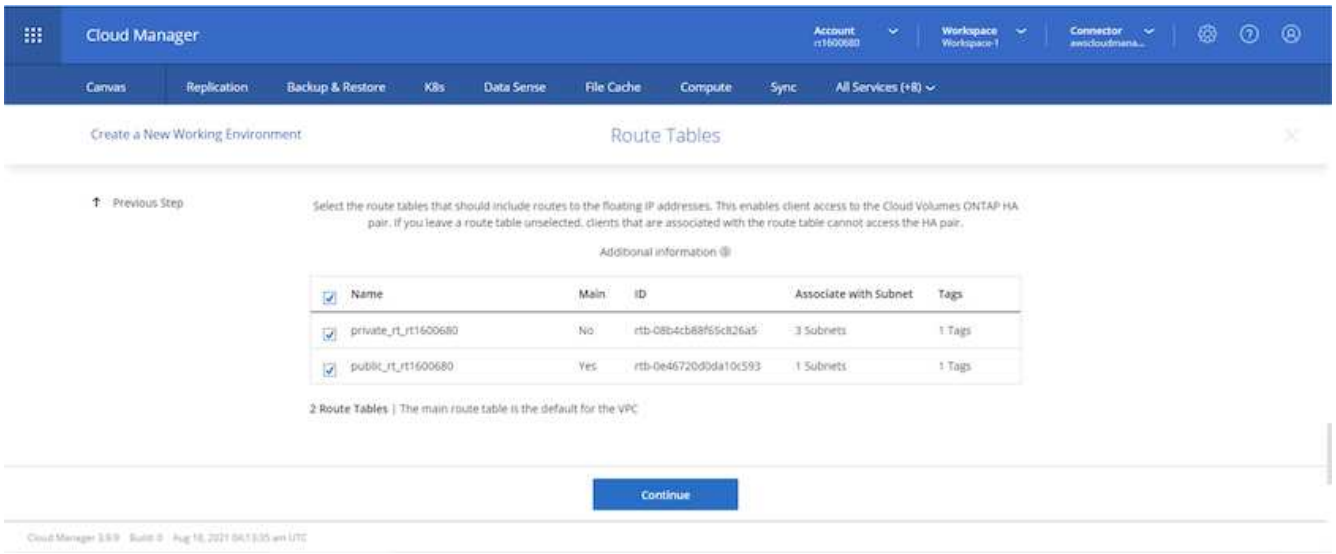


Le médiateur nécessite une communication avec les API AWS. Une adresse IP publique n'est pas requise tant que les API sont accessibles après le déploiement de l'instance EC2 du médiateur.

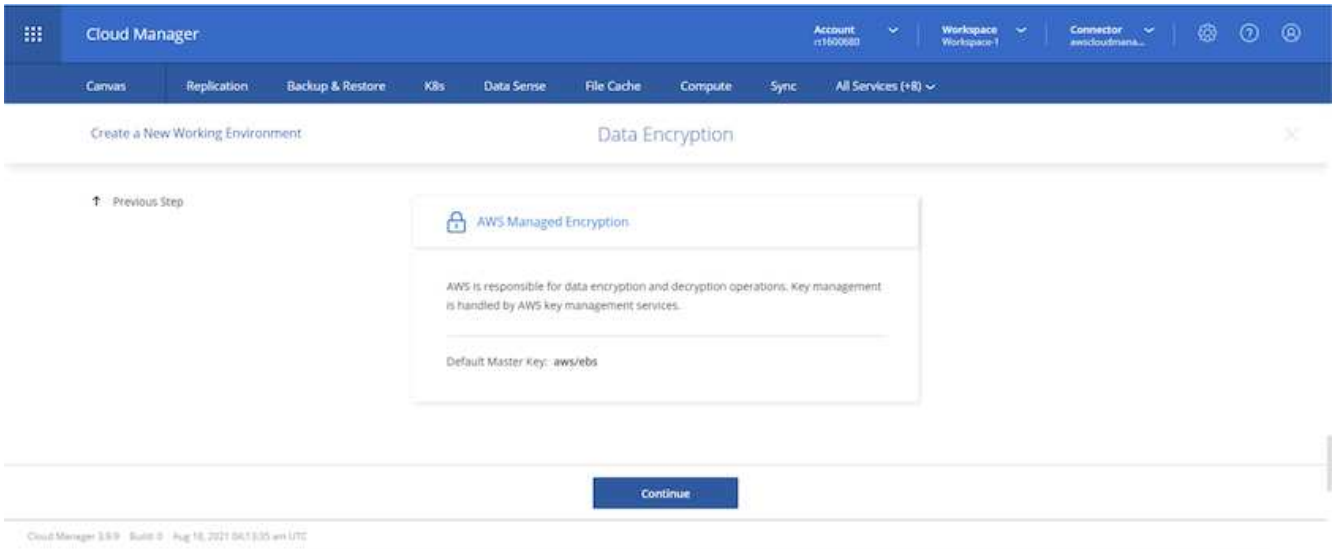
1. Les adresses IP flottantes sont utilisées pour permettre l'accès aux différentes adresses IP utilisées par Cloud Volumes ONTAP , y compris la gestion des clusters et les adresses IP de service de données. Il doit s'agir d'adresses qui ne sont pas déjà routables au sein de votre réseau et qui sont ajoutées aux tables de routage de votre environnement AWS. Ces éléments sont nécessaires pour permettre des adresses IP cohérentes pour une paire HA lors du basculement. Vous trouverez plus d'informations sur les adresses IP flottantes dans le "Documentation NetApp Cloud" .



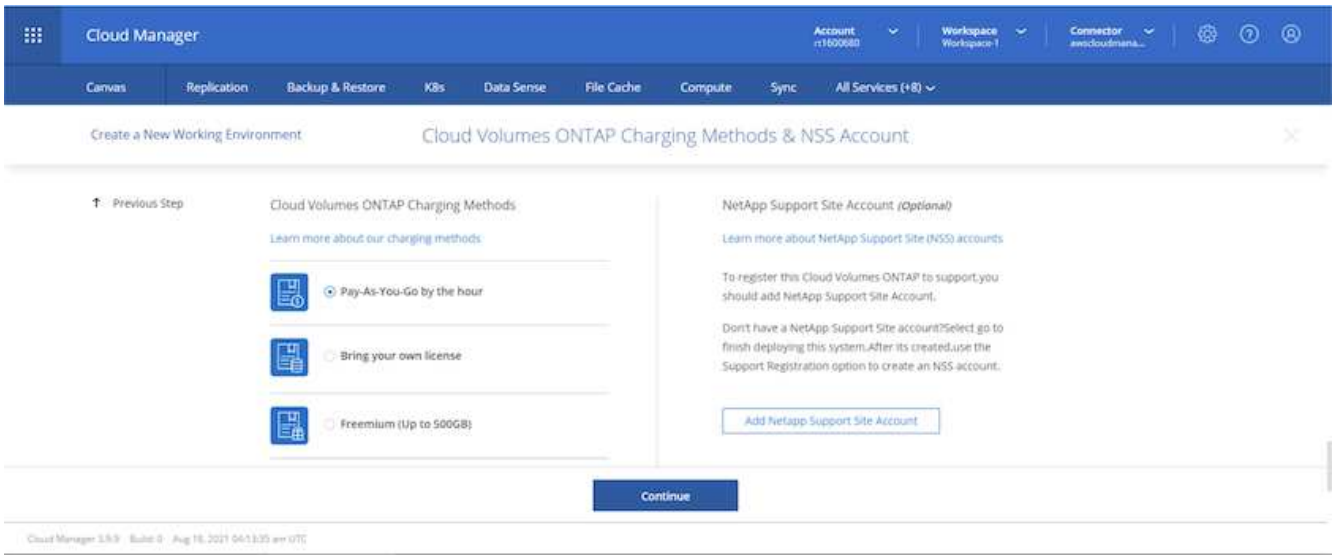
2. Sélectionnez les tables de routage auxquelles les adresses IP flottantes sont ajoutées. Ces tables de routage sont utilisées par les clients pour communiquer avec Cloud Volumes ONTAP.



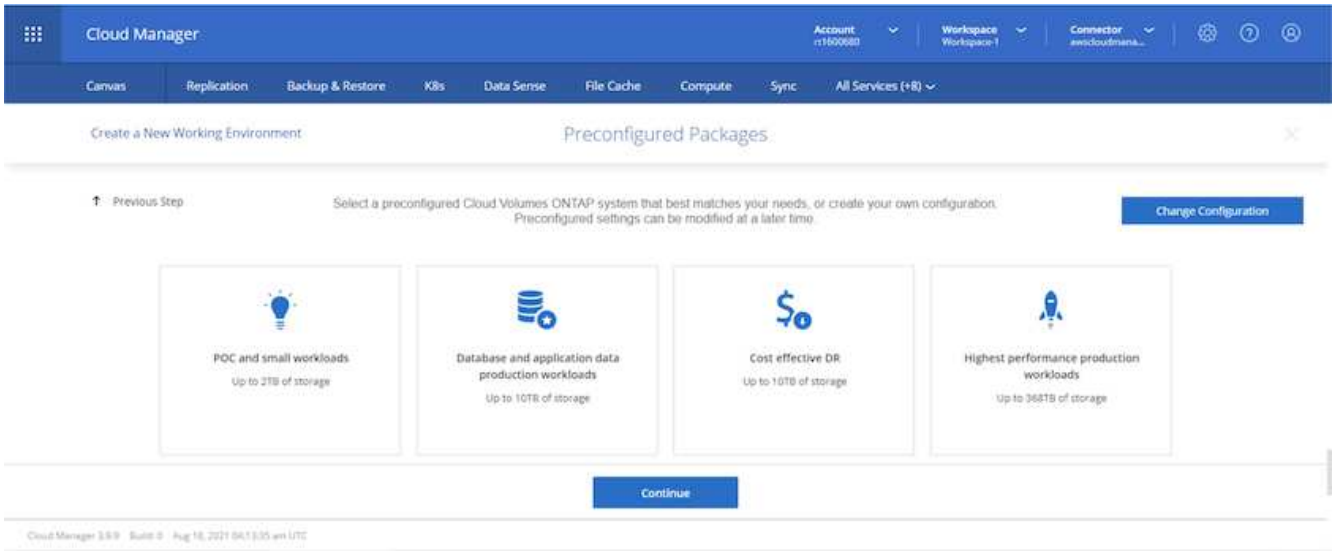
3. Choisissez d'activer le chiffrement géré par AWS ou AWS KMS pour chiffrer les disques racine, de démarrage et de données ONTAP .



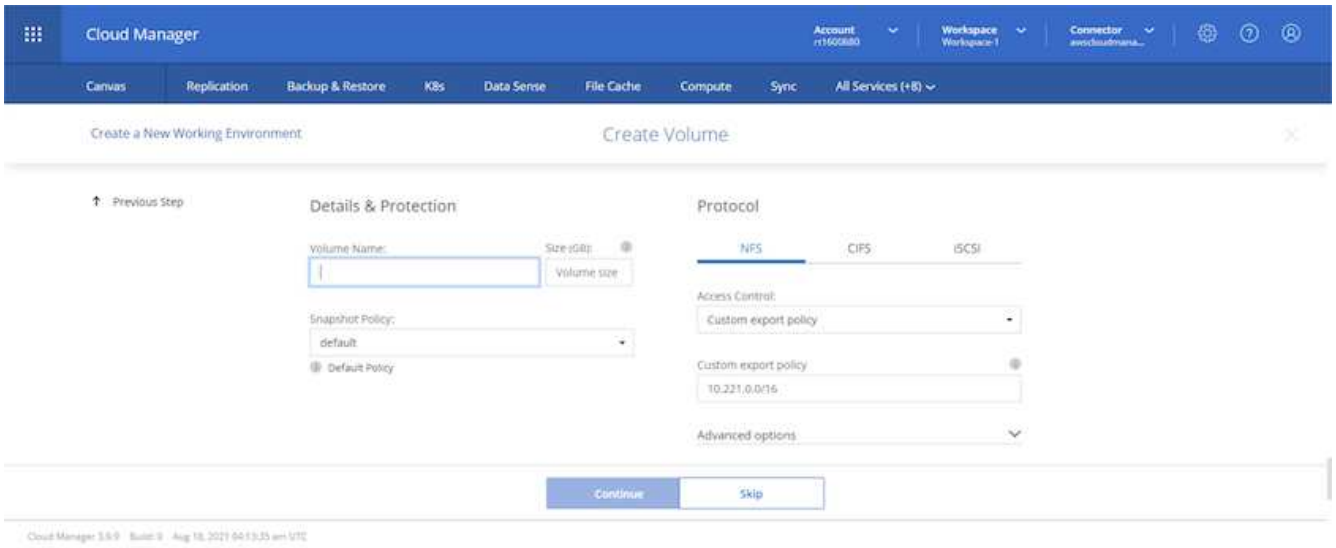
4. Choisissez votre modèle de licence. Si vous ne savez pas lequel choisir, contactez votre représentant NetApp .



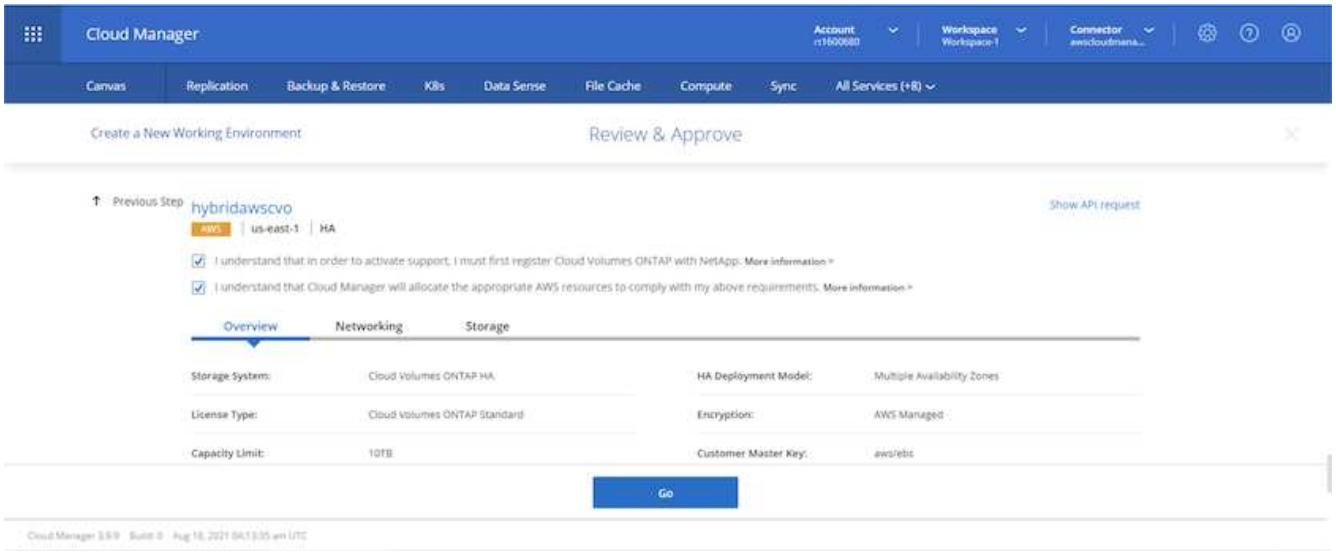
5. Sélectionnez la configuration la mieux adaptée à votre cas d'utilisation. Ceci est lié aux considérations de dimensionnement abordées dans la page des prérequis.



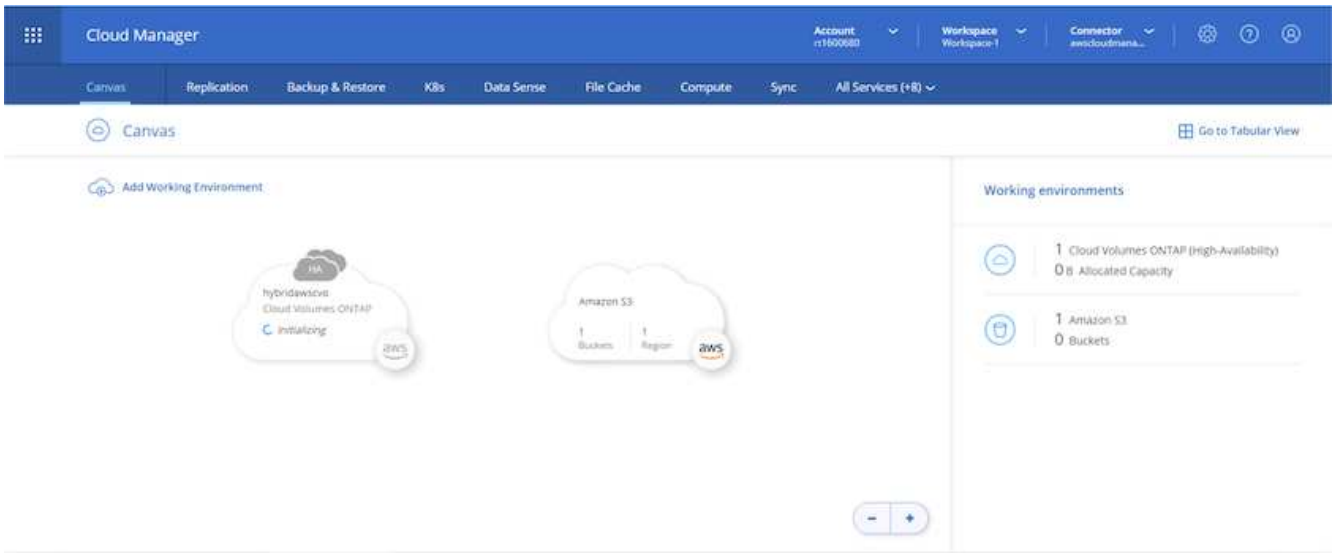
6. En option, créez un volume. Ce n'est pas obligatoire, car les étapes suivantes utilisent SnapMirror, qui crée les volumes pour nous.



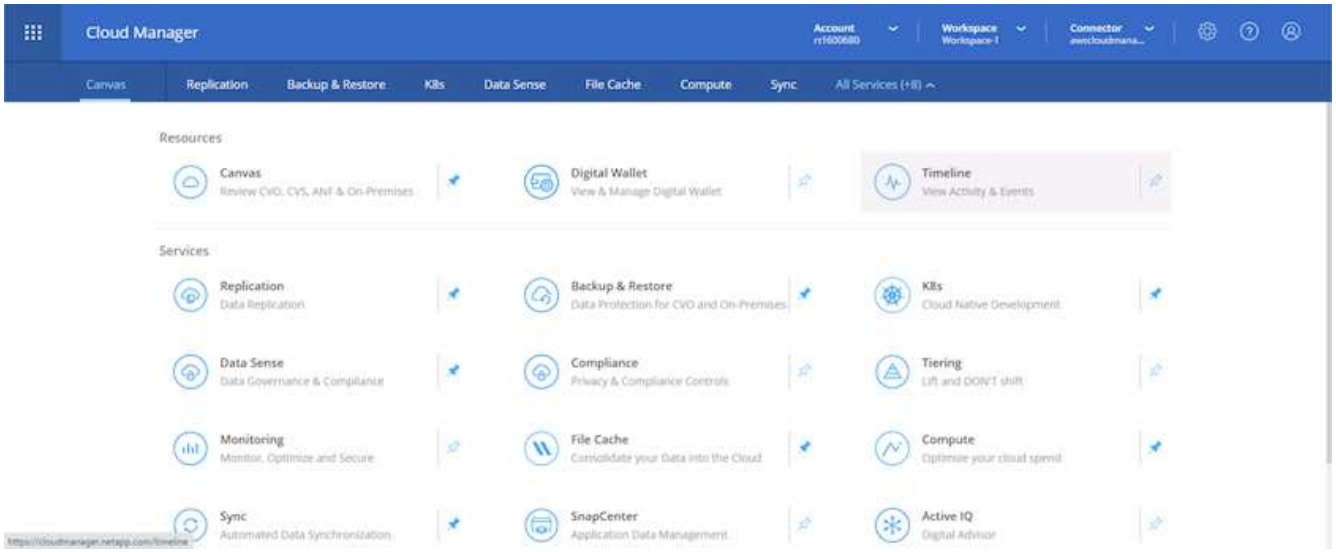
7. Passez en revue les sélections effectuées et cochez les cases pour vérifier que vous comprenez que Cloud Manager déploie des ressources dans votre environnement AWS. Lorsque vous êtes prêt, cliquez sur Aller.



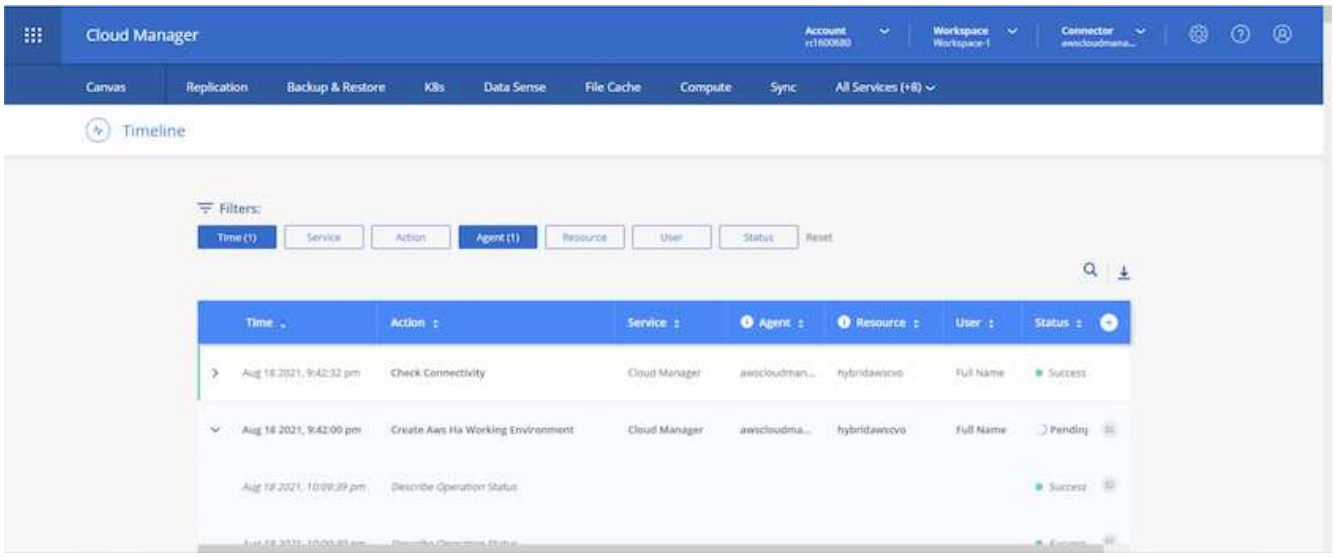
8. Cloud Volumes ONTAP démarre maintenant son processus de déploiement. Cloud Manager utilise les API AWS et les piles de formation cloud pour déployer Cloud Volumes ONTAP. Il configure ensuite le système selon vos spécifications, vous offrant ainsi un système prêt à l'emploi qui peut être utilisé instantanément. Le calendrier de ce processus varie en fonction des sélections effectuées.



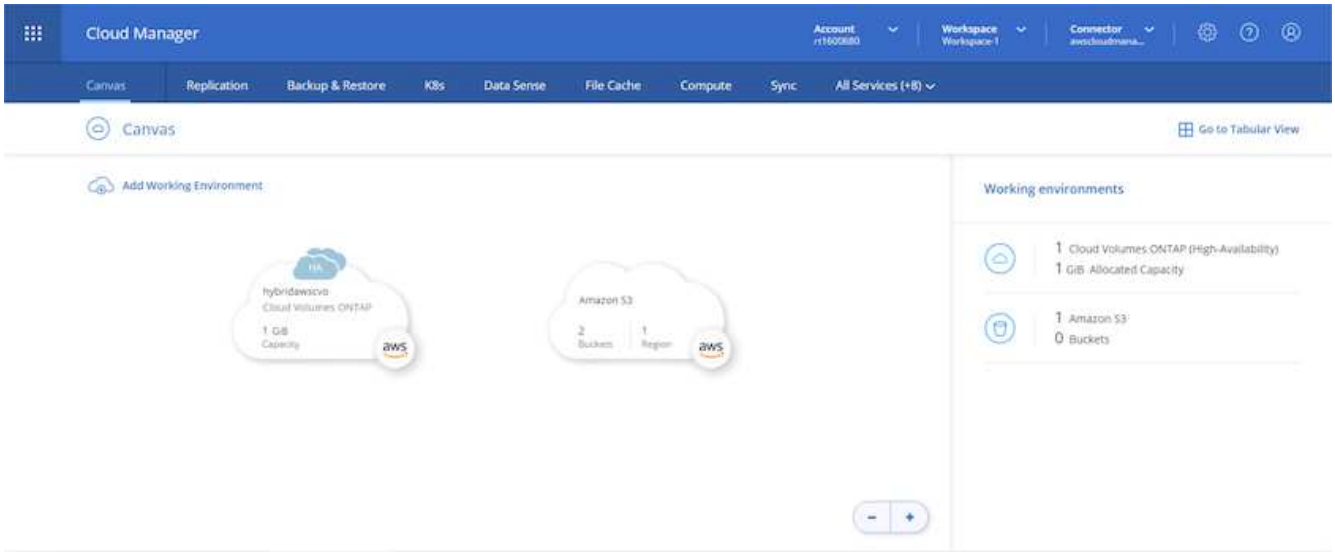
9. Vous pouvez suivre la progression en accédant à la chronologie.



10. La chronologie agit comme 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 ainsi que sur le cluster ONTAP . Cela peut également être utilisé efficacement pour résoudre tous les problèmes auxquels vous êtes confronté.



11. Une fois le déploiement terminé, le cluster CVO apparaît sur le canevas, avec la capacité actuelle. Le cluster ONTAP dans son état actuel est entièrement configuré pour permettre une véritable expérience prête à l'emploi.

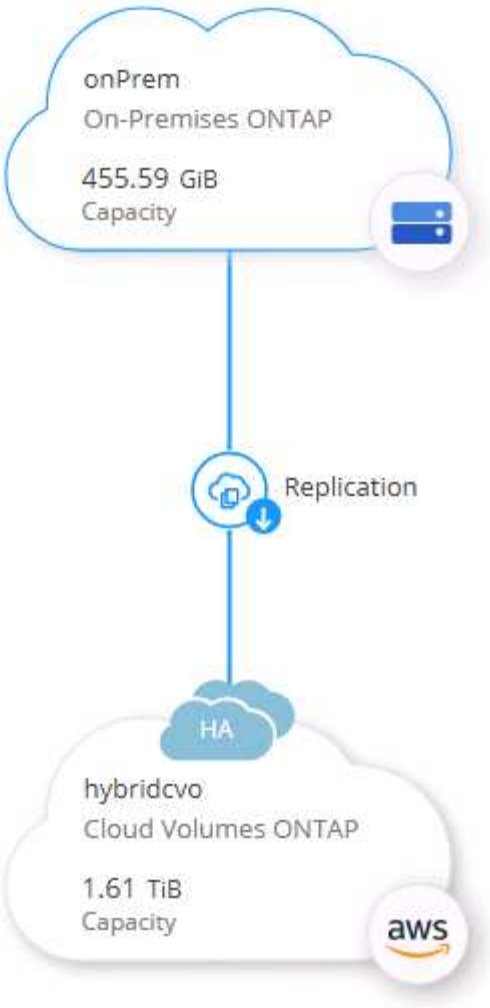


Configurer SnapMirror depuis le site vers le cloud

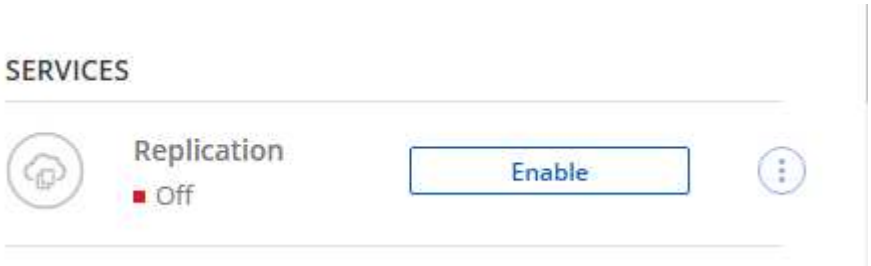
Maintenant que vous disposez d'un système ONTAP source et d'un système ONTAP de destination déployés, vous pouvez répliquer des volumes contenant des données de base de données dans le cloud.

Pour un guide sur les versions ONTAP compatibles pour SnapMirror, consultez le "Matrice de compatibilité SnapMirror" .

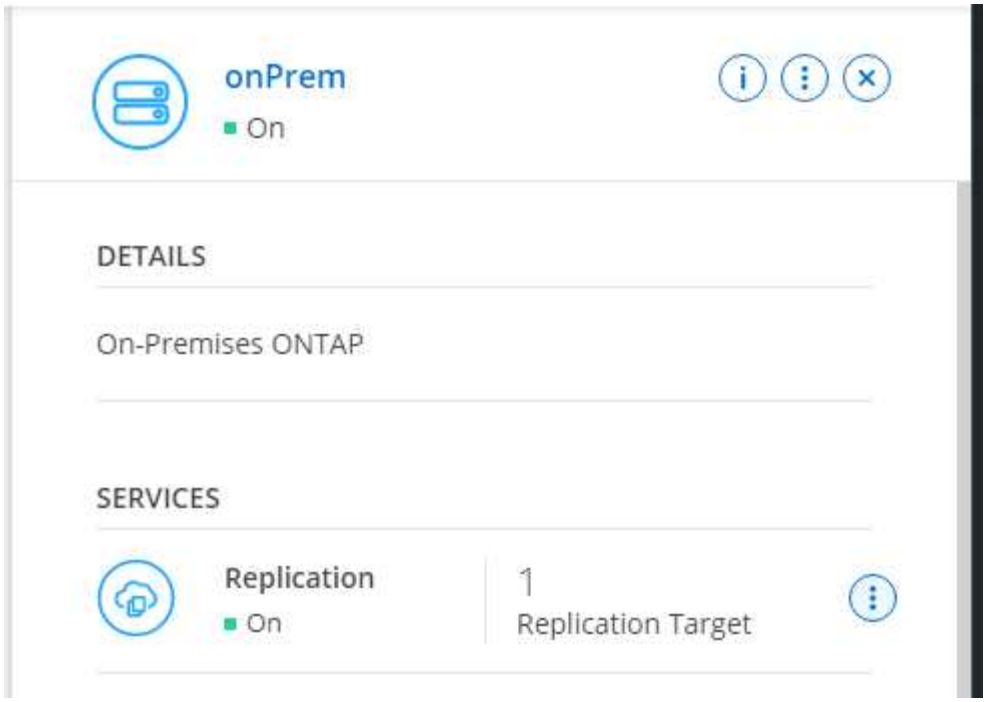
1. Cliquez sur le système ONTAP source (sur site) et faites-le glisser vers la destination, sélectionnez Réplication > Activer ou sélectionnez Réplication > Menu > Répliquer.



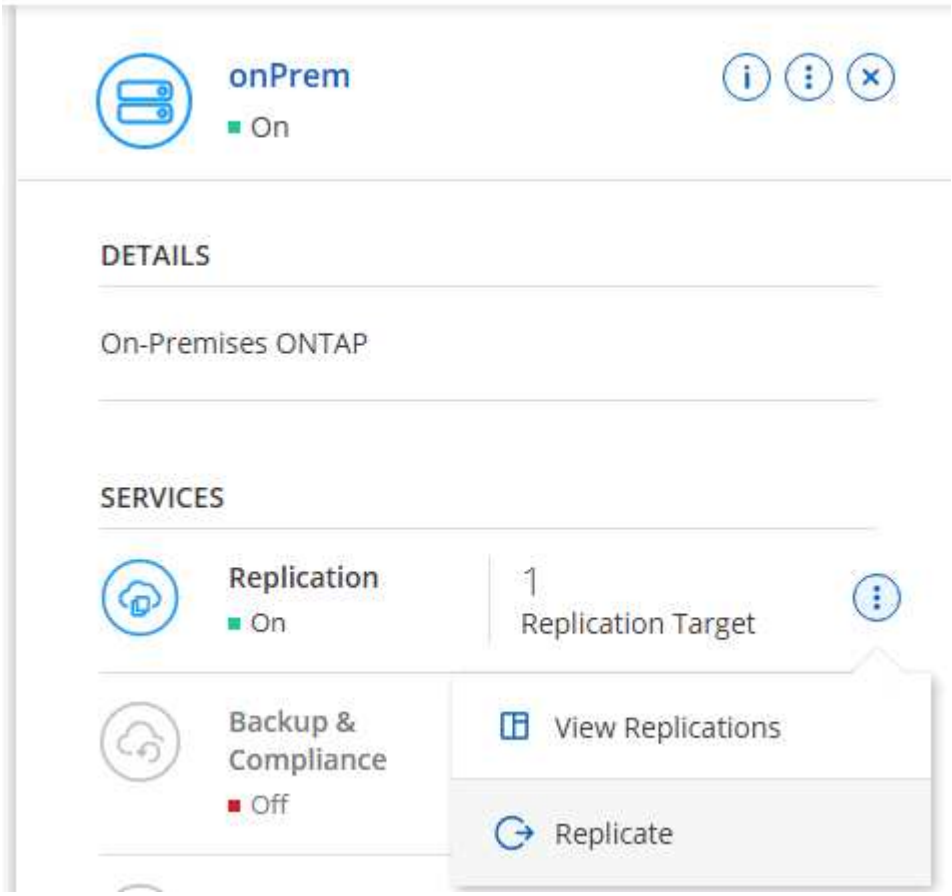
Sélectionnez Activer.



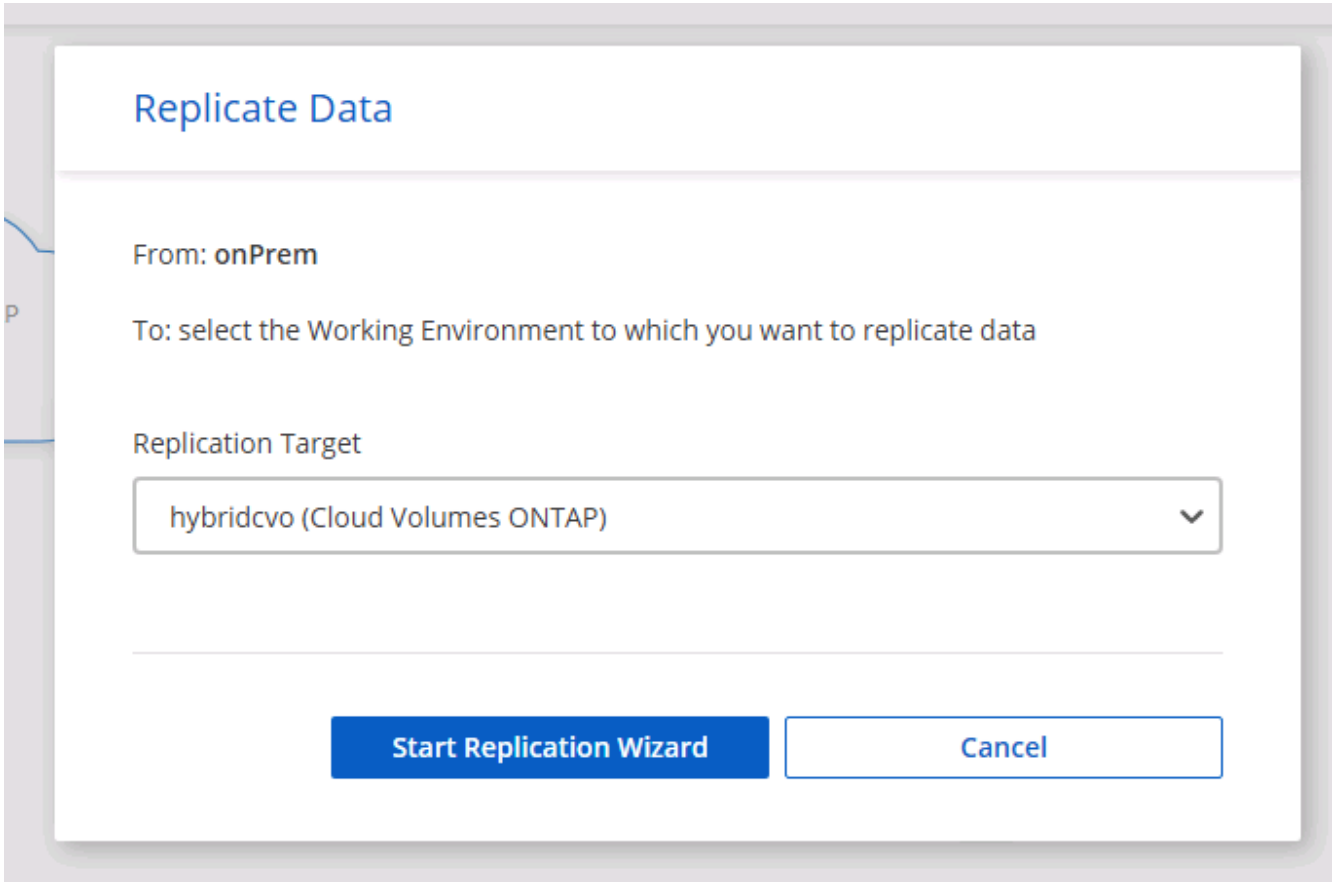
Ou Options.



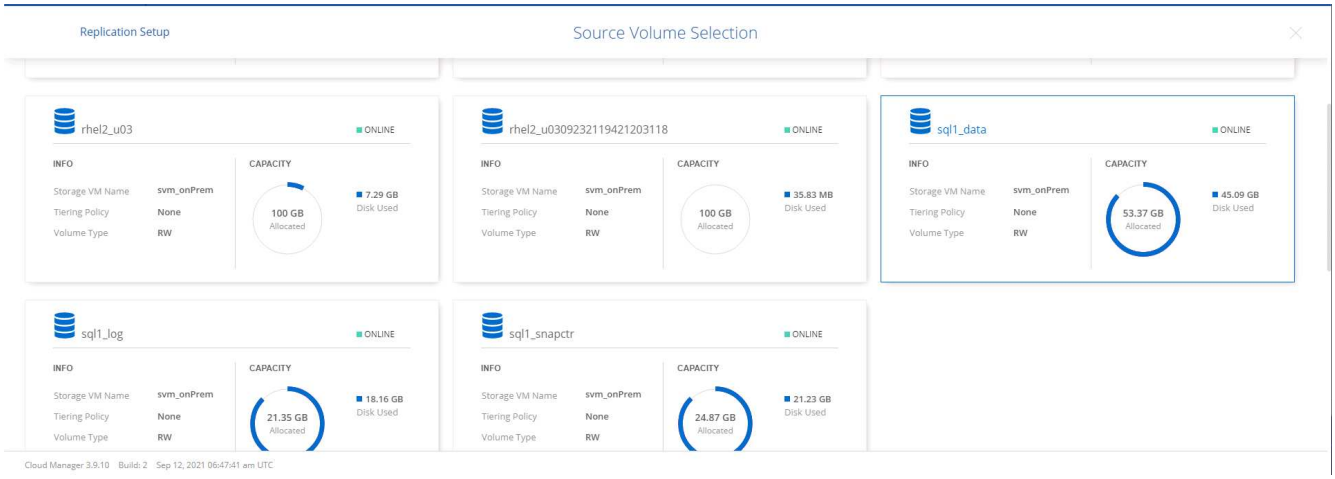
Reproduire.



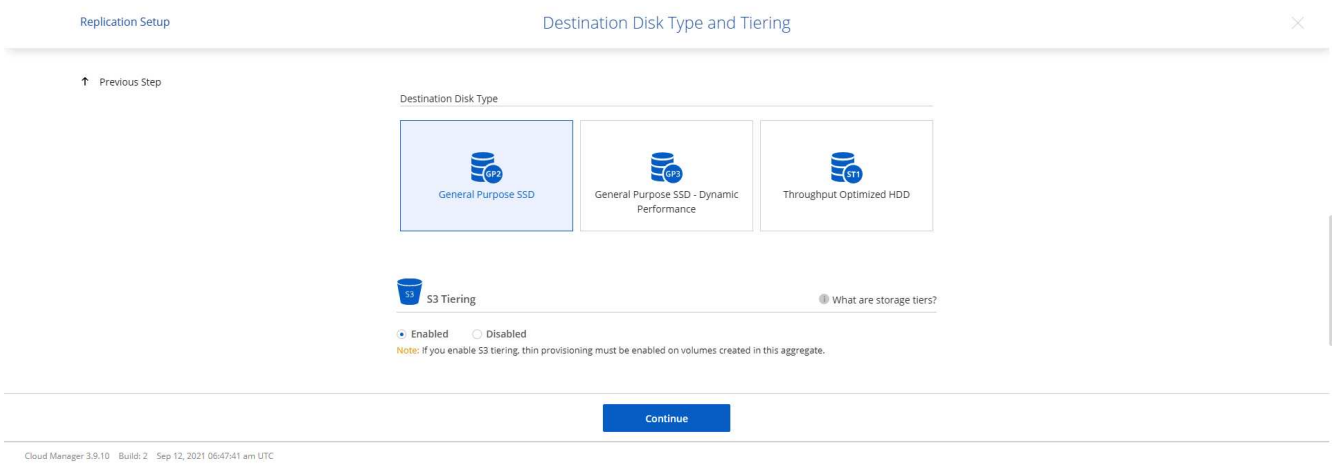
2. Si vous n'avez pas fait de glisser-déposer, choisissez le cluster de destination vers lequel répliquer.



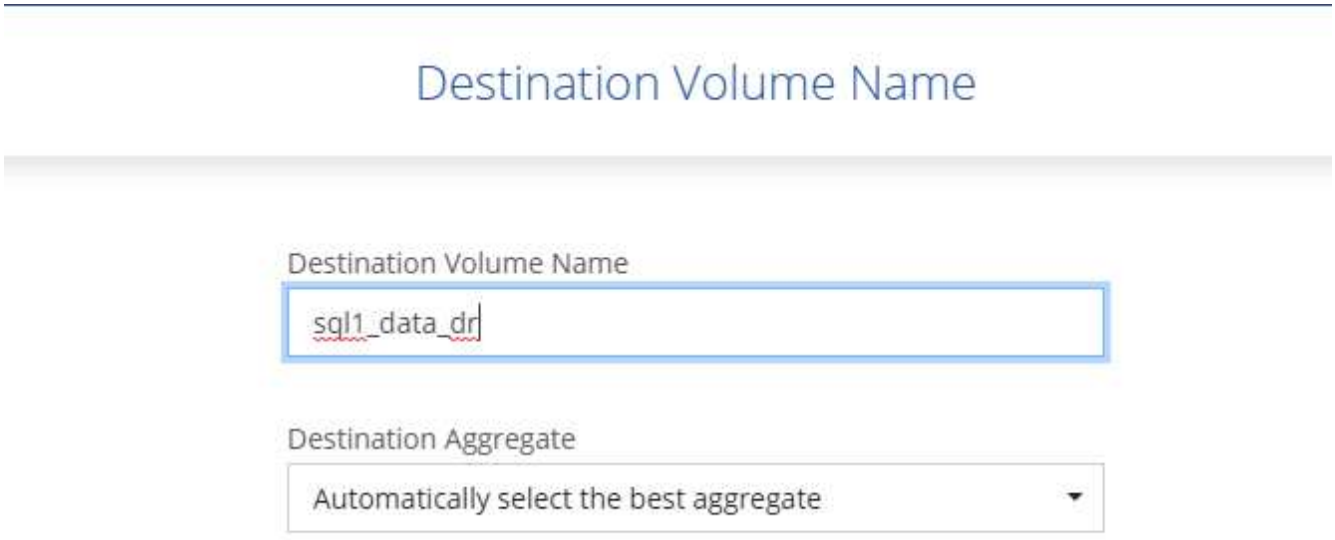
3. Choisissez le volume que vous souhaitez répliquer. Nous avons répliqué les données et tous les volumes de journaux.



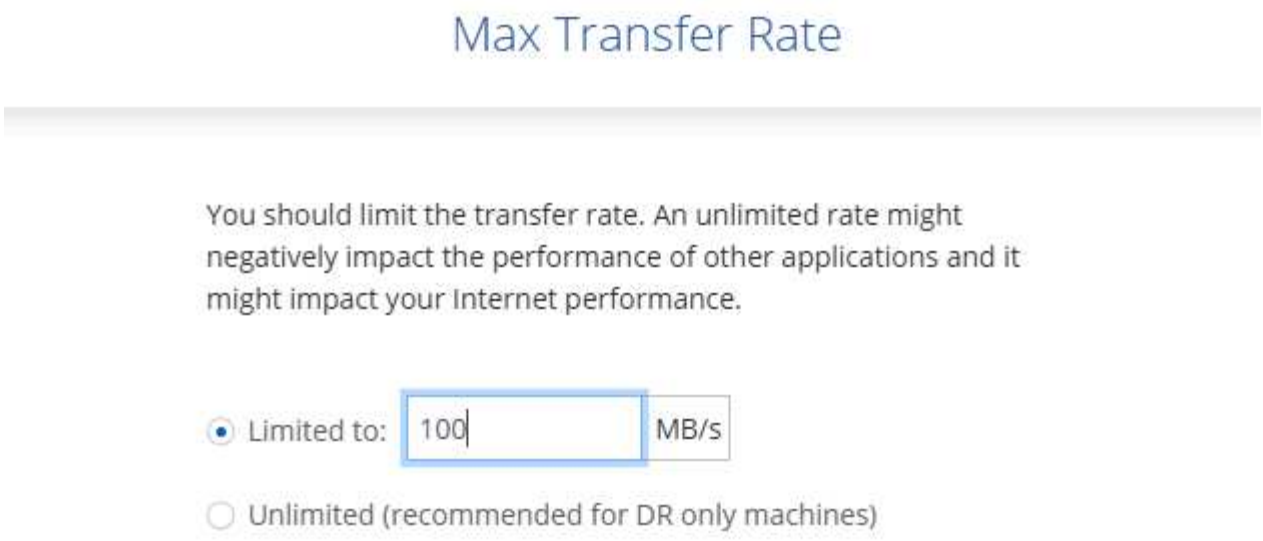
4. Choisissez le type de disque de destination et la politique de hiérarchisation. Pour la reprise après sinistre, nous recommandons un SSD comme type de disque et pour maintenir la hiérarchisation des données. La hiérarchisation des données hiérarchise les données en miroir dans un stockage d'objets à faible coût et vous permet d'économiser de l'argent sur les disques locaux. Lorsque vous rompez la relation ou clonez le volume, les données utilisent le stockage local rapide.



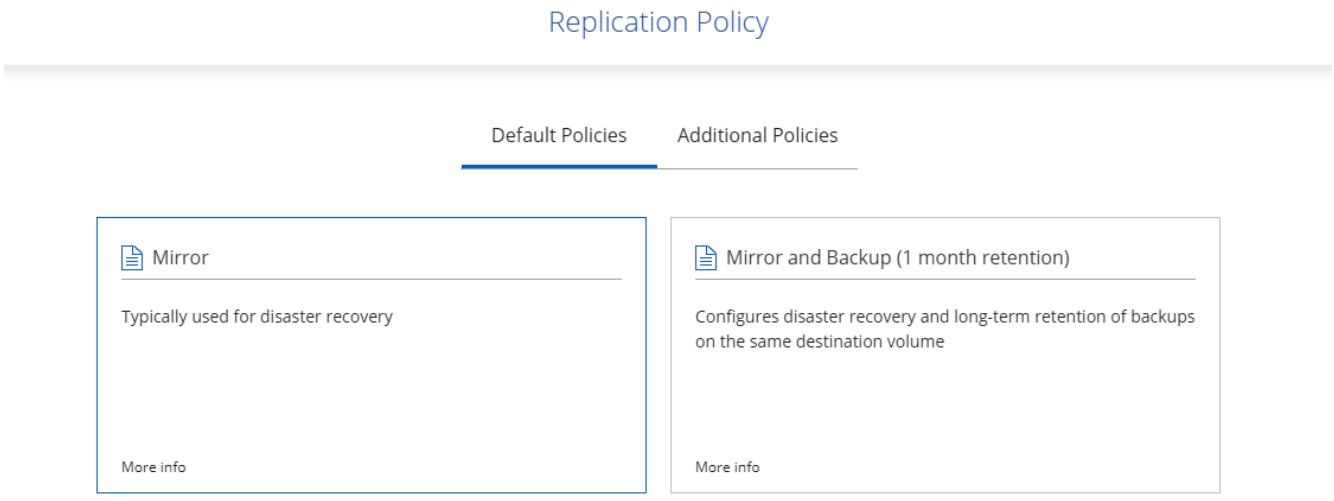
5. Sélectionnez le nom du volume de destination : nous avons choisi `[source_volume_name]_dr`.



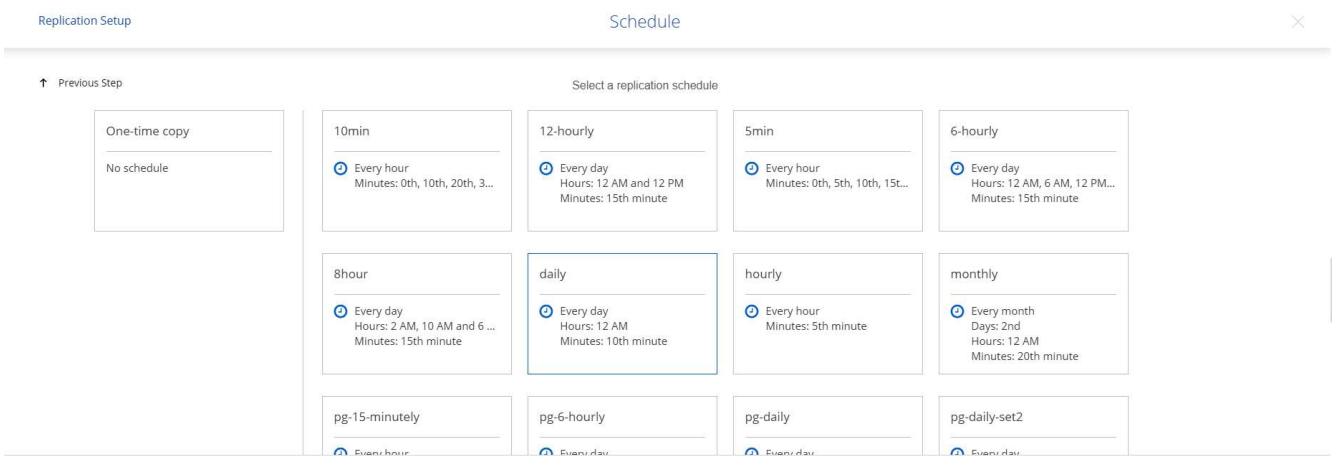
6. Sélectionnez le taux de transfert maximal pour la réplication. Cela vous permet d'économiser de la bande passante si vous disposez d'une connexion à faible bande passante au cloud, comme un VPN.



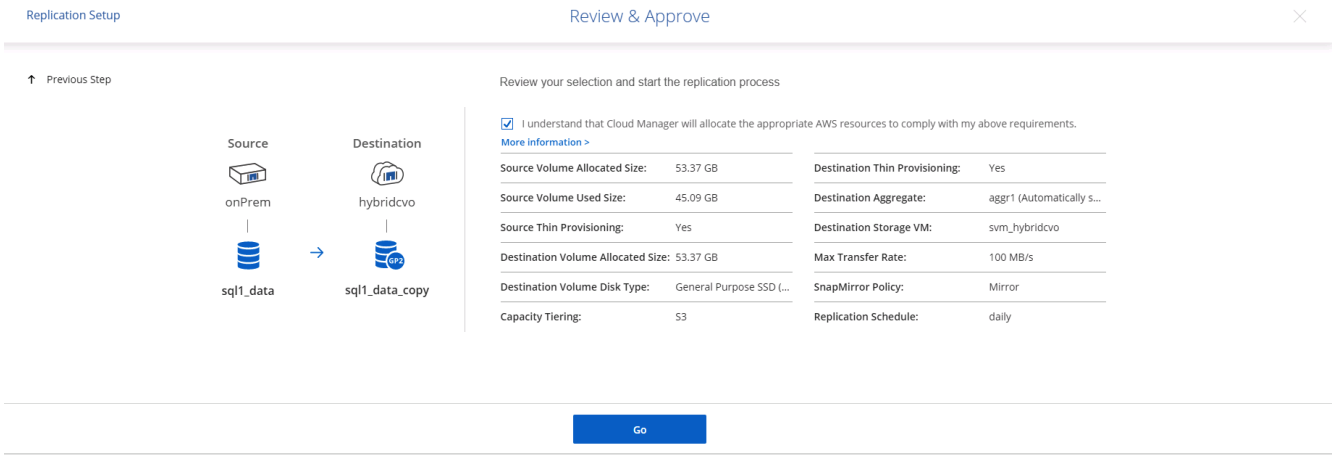
7. Définir la politique de réplication. Nous avons choisi un miroir, qui prend l'ensemble de données le plus récent et le réplique dans le volume de destination. Vous pouvez également choisir une politique différente en fonction de vos besoins.



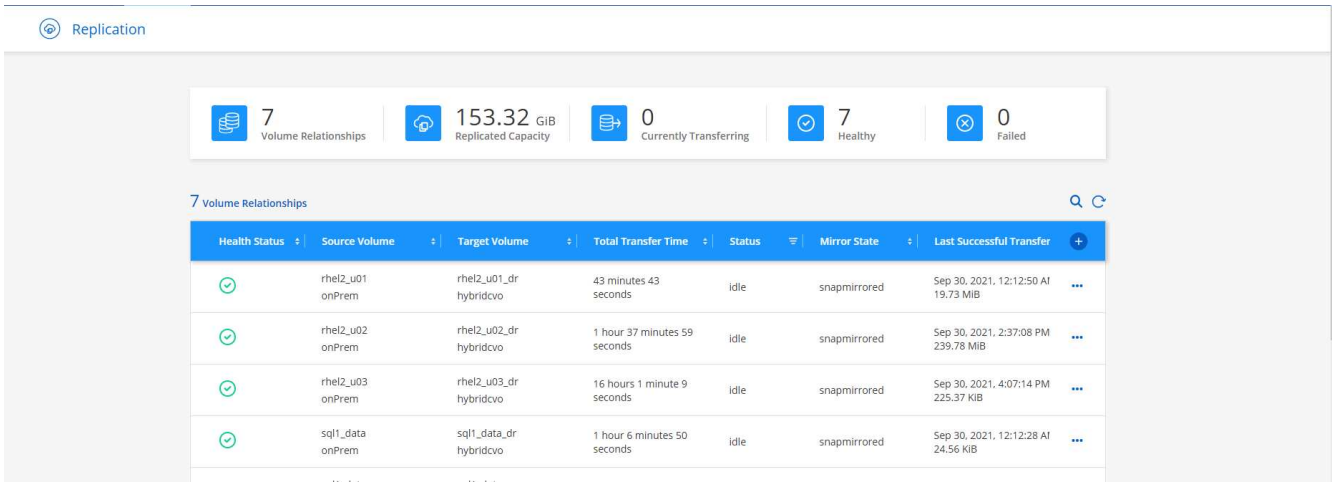
8. Choisissez le calendrier de déclenchement de la réplication. NetApp recommande de définir une planification « quotidienne » pour le volume de données et une planification « horaire » pour les volumes de journaux, bien que cela puisse être modifié en fonction des besoins.



9. Vérifiez les informations saisies, cliquez sur Accéder pour déclencher l'homologue du cluster et l'homologue SVM (s'il s'agit de votre première réplication entre les deux clusters), puis implémentez et initialisez la relation SnapMirror .



10. Continuez ce processus pour les volumes de données et les volumes de journaux.
11. Pour vérifier toutes vos relations, accédez à l'onglet Réplication dans Cloud Manager. Ici, vous pouvez gérer vos relations et vérifier 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 sinistre et de développement/test.

3. Déployer une instance de calcul EC2 pour la charge de travail de la base 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 et la capacité de stockage, ainsi que les performances du réseau. Pour les cas d'utilisation, à l'exception de la partition du système d'exploitation, le stockage principal pour exécuter 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 typiques peuvent être trouvés 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, la taille de l'ensemble de données, etc.
2. Le déploiement de l'instance EC2 peut être lancé via le tableau de bord EC2. Les procédures de déploiement exactes dépassent le cadre de cette solution. Voir "Amazon EC2" pour plus de détails.

Configuration d'instance Linux pour la charge de travail 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 noms dans le domaine de gestion SnapCenter .
2. Ajoutez un ID utilisateur de gestion Linux comme informations d'identification du système d'exploitation SnapCenter 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 sudo sans mot de passe sont désactivés sur les instances EC2.)
3. Configurez l'installation d'Oracle pour qu'elle corresponde à l'installation Oracle sur site, comme les correctifs du système d'exploitation, les versions et correctifs Oracle, etc.
4. Les rôles d'automatisation de base de données NetApp Ansible peuvent être exploités pour configurer des instances EC2 pour les cas d'utilisation de développement/test de base de données et de reprise après sinistre. Le code d'automatisation peut être téléchargé à partir du site GitHub public de NetApp : "Déploiement automatisé d'Oracle 19c" . L'objectif est d'installer et de configurer une pile logicielle de base de données sur une instance EC2 pour correspondre aux configurations de système d'exploitation et de base de données sur site.

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

Cette section répertorie les étapes de configuration supplémentaires après le déploiement initial d'une instance Windows EC2.

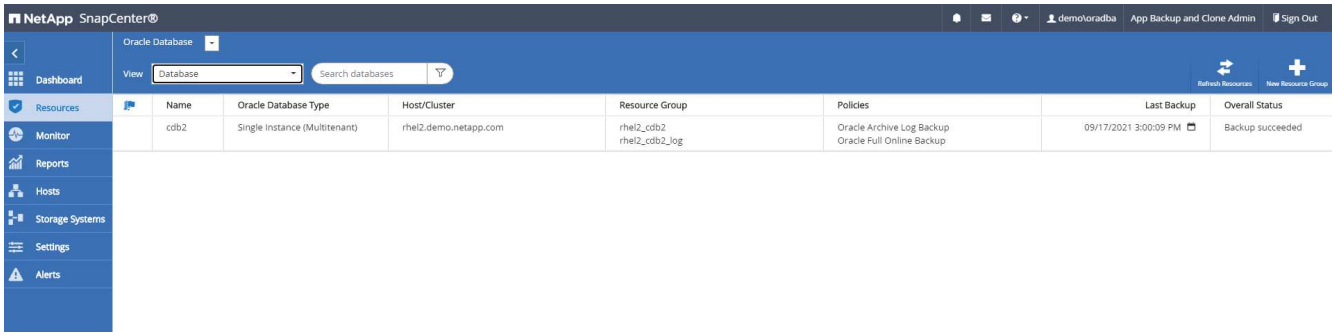
1. Récupérez le mot de passe administrateur Windows pour vous connecter à une instance via RDP.
2. Désactivez le pare-feu Windows, joignez l'hôte au domaine Windows SnapCenter et ajoutez l'instance au serveur DNS pour la résolution de noms.
3. Provisionnez un volume de journal SnapCenter pour stocker les fichiers journaux SQL Server.
4. Configurez iSCSI sur l'hôte Windows pour monter le volume et formater le lecteur de disque.
5. Encore une fois, de nombreuses 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 rôles et solutions récemment publiés : "Automatisation NetApp" .

Workflow pour le développement/test en explosant vers le cloud

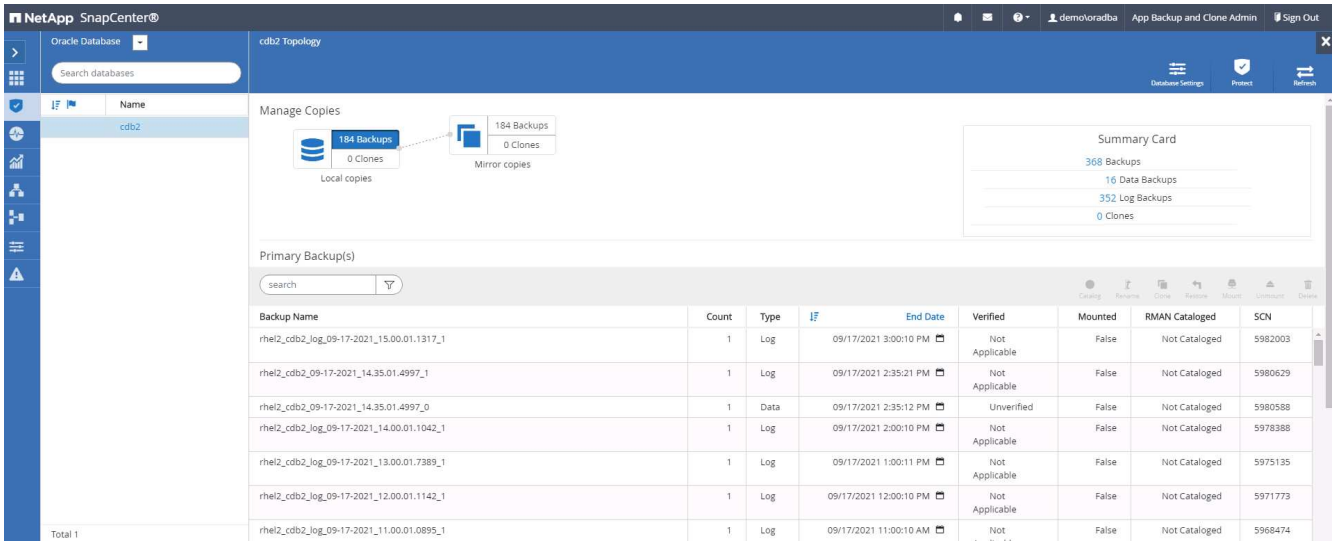
L'agilité du cloud public, le délai de rentabilisation et les économies de coûts sont autant de propositions de valeur significatives pour les entreprises qui adoptent le cloud public pour le développement et les tests d'applications de base de données. Il n'existe pas de meilleur outil que SnapCenter pour faire de cela une réalité. SnapCenter peut non seulement protéger votre base de données de production sur site, mais peut également cloner rapidement une copie pour le développement d'applications ou les tests de code dans le cloud public tout en consommant très peu de stockage supplémentaire. Vous trouverez ci-dessous des détails sur les processus étape par étape pour utiliser cet outil.

Cloner une base de données Oracle pour le développement/test à partir d'une sauvegarde instantanée répliquée

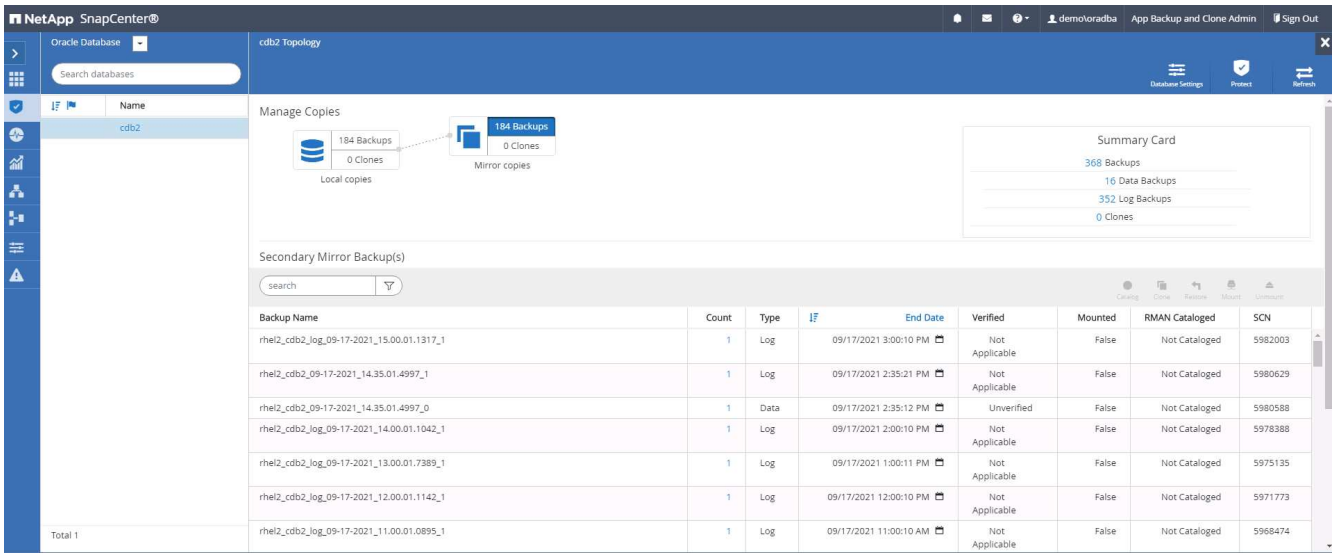
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données pour Oracle. Accédez à l'onglet Ressources, qui affiche les bases de données Oracle protégées par SnapCenter.



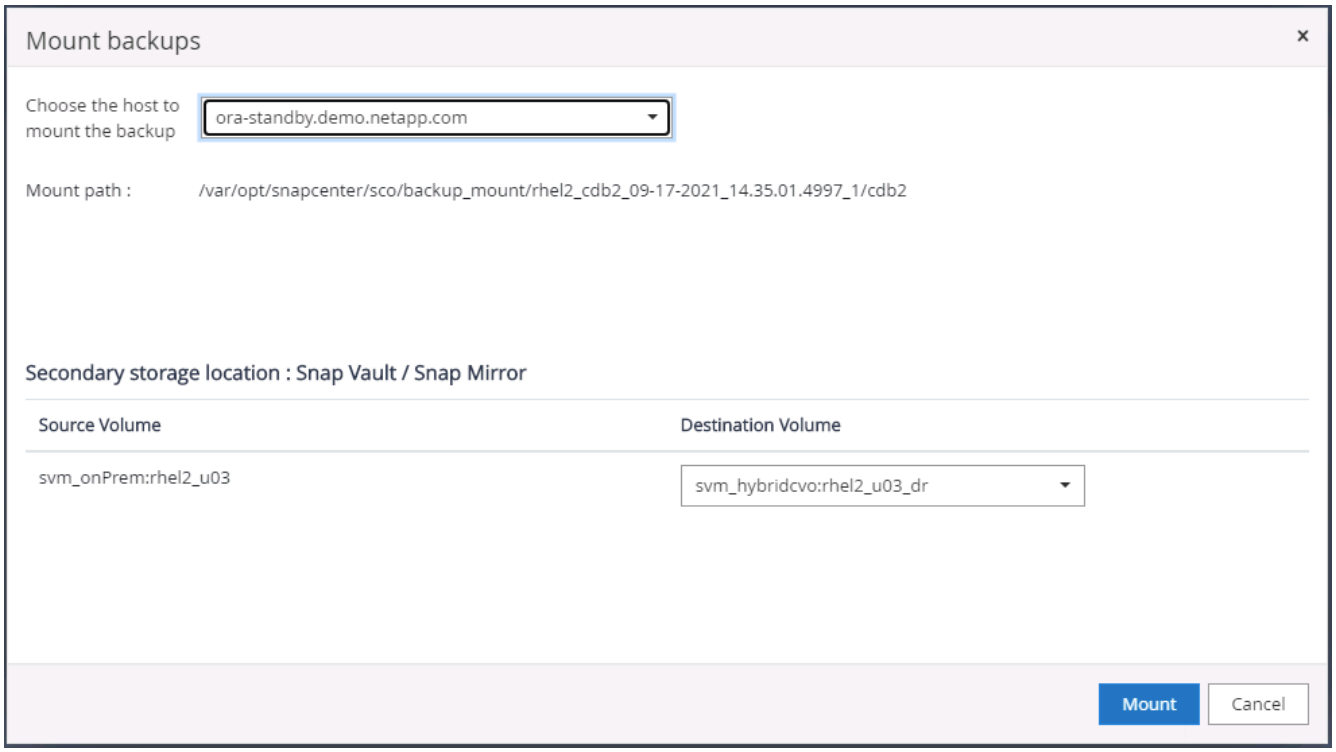
2. Cliquez sur le nom de la base de données locale prévue pour la topologie de sauvegarde et la vue détaillée. Si un emplacement répliqué secondaire est activé, il affiche les sauvegardes miroir liées.

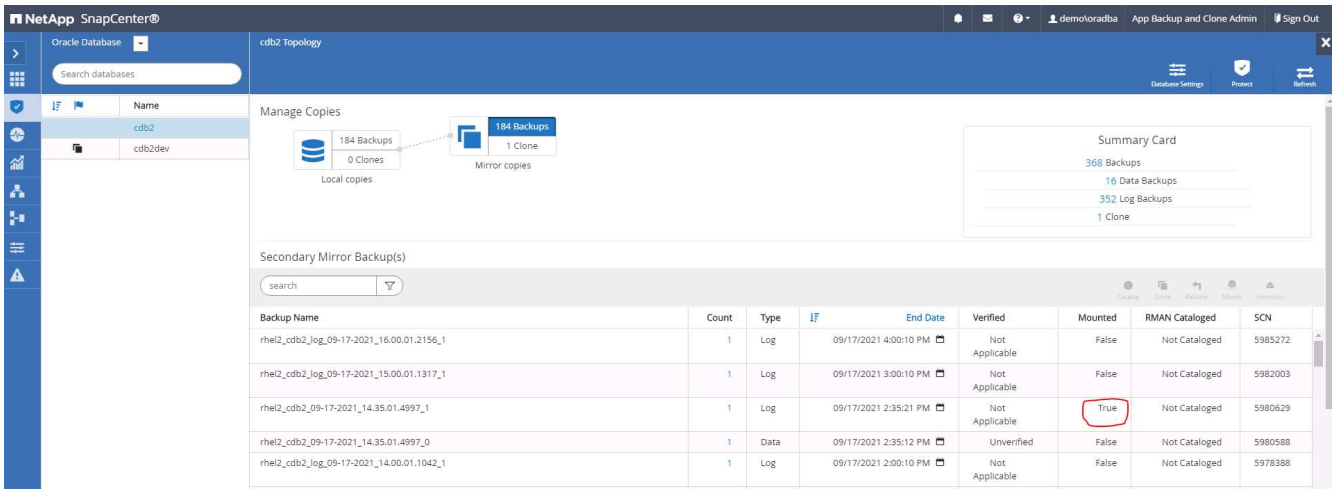


3. Basculez vers la vue des sauvegardes en miroir en cliquant sur les sauvegardes en miroir. La ou les sauvegardes miroir secondaires sont alors affichées.



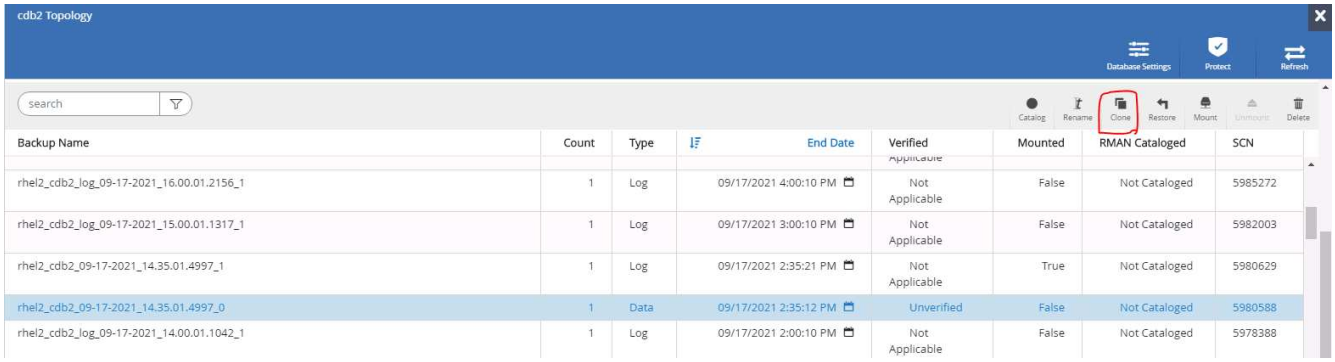
4. Choisissez une copie de sauvegarde de base de données secondaire en miroir à cloner et déterminez un point de récupération soit par heure et numéro de modification du système, soit par SCN. En règle générale, le point de récupération doit suivre le temps de sauvegarde complet de la base de données ou le SCN à cloner. Une fois le point de récupération déterminé, la sauvegarde du fichier journal requise doit être montée pour la récupération. La sauvegarde du fichier journal doit être montée sur le serveur de base de données cible sur lequel la base de données clonée doit être hébergée.



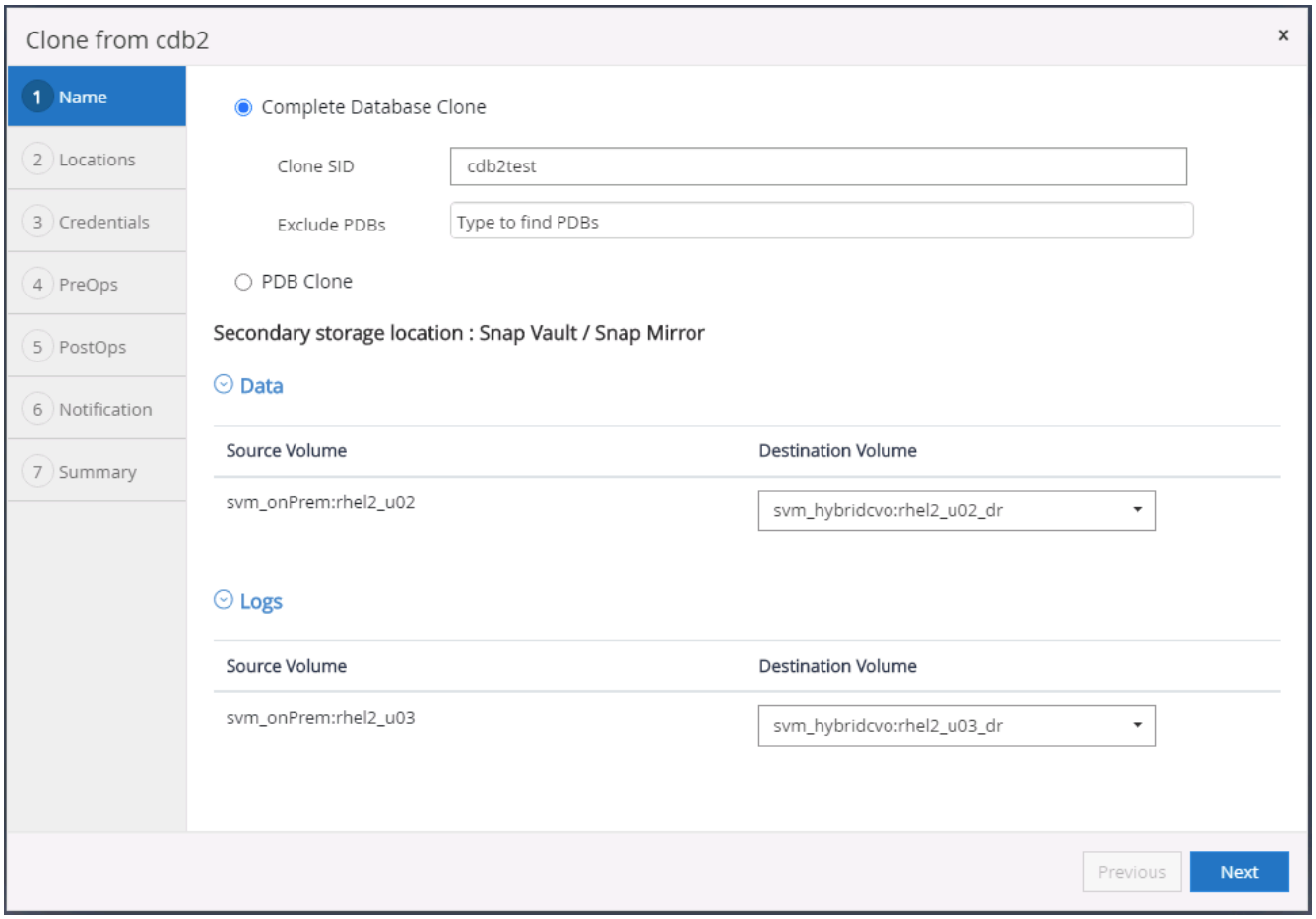


Si l'élagage des journaux est activé et que le point de récupération est étendu au-delà du dernier élagage des journaux, plusieurs sauvegardes de journaux d'archive peuvent devoir être montées.

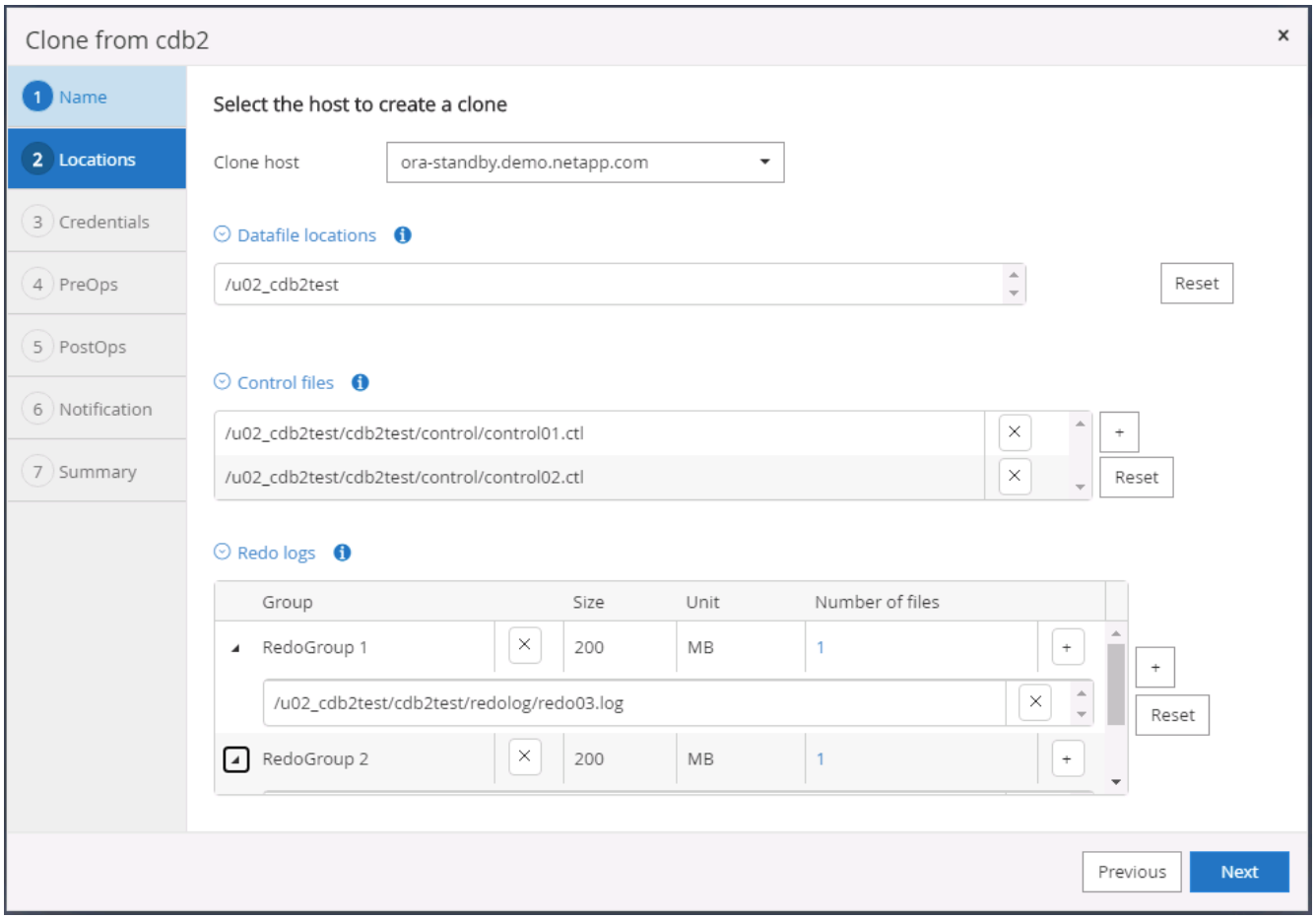
5. Mettez en surbrillance la copie de sauvegarde complète de la base de données à cloner, puis cliquez sur le bouton Cloner pour démarrer le flux de travail de clonage de la base de données.



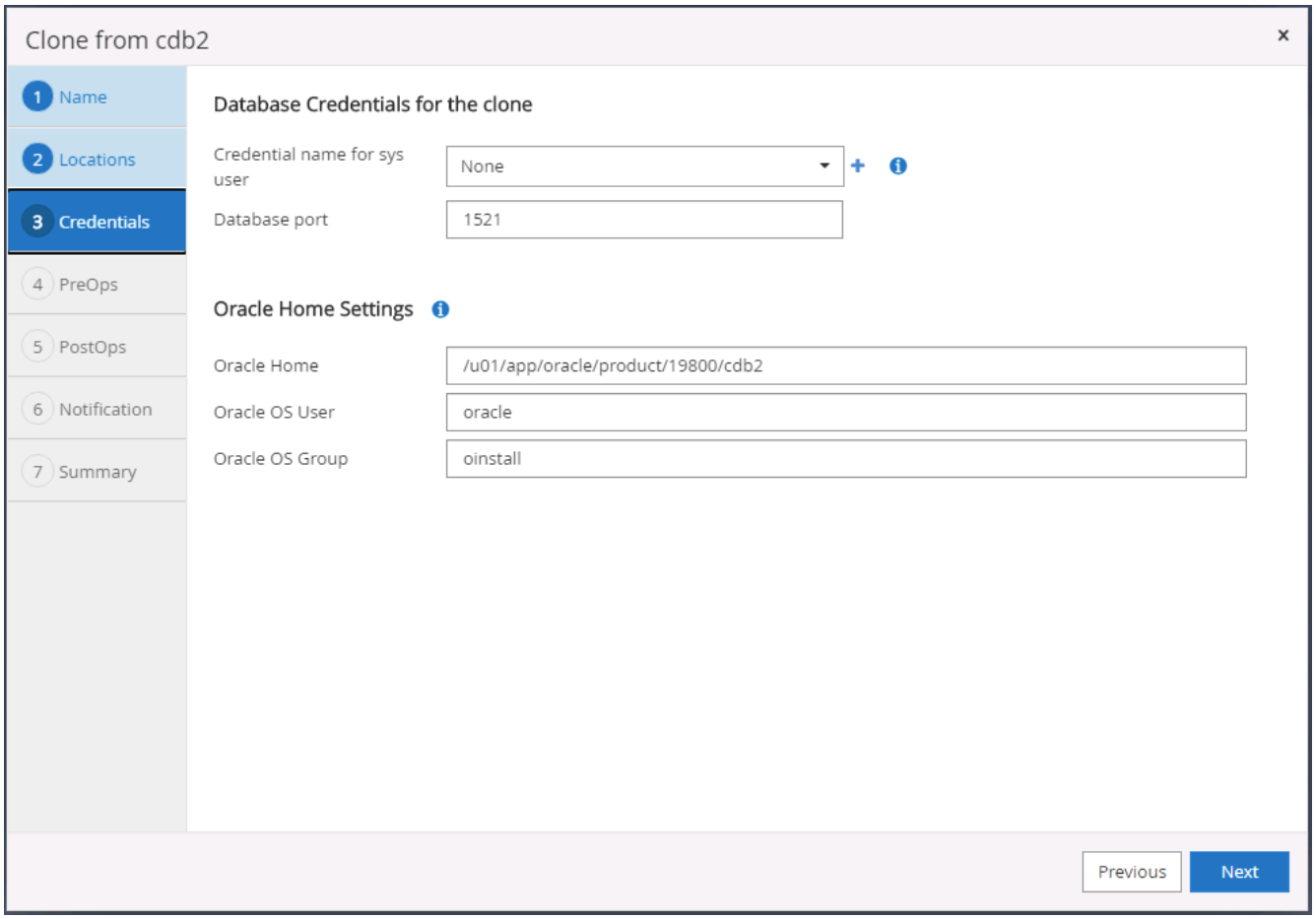
6. Choisissez un SID de base de données clone approprié pour une base de données de conteneur complète ou un clone CDB.



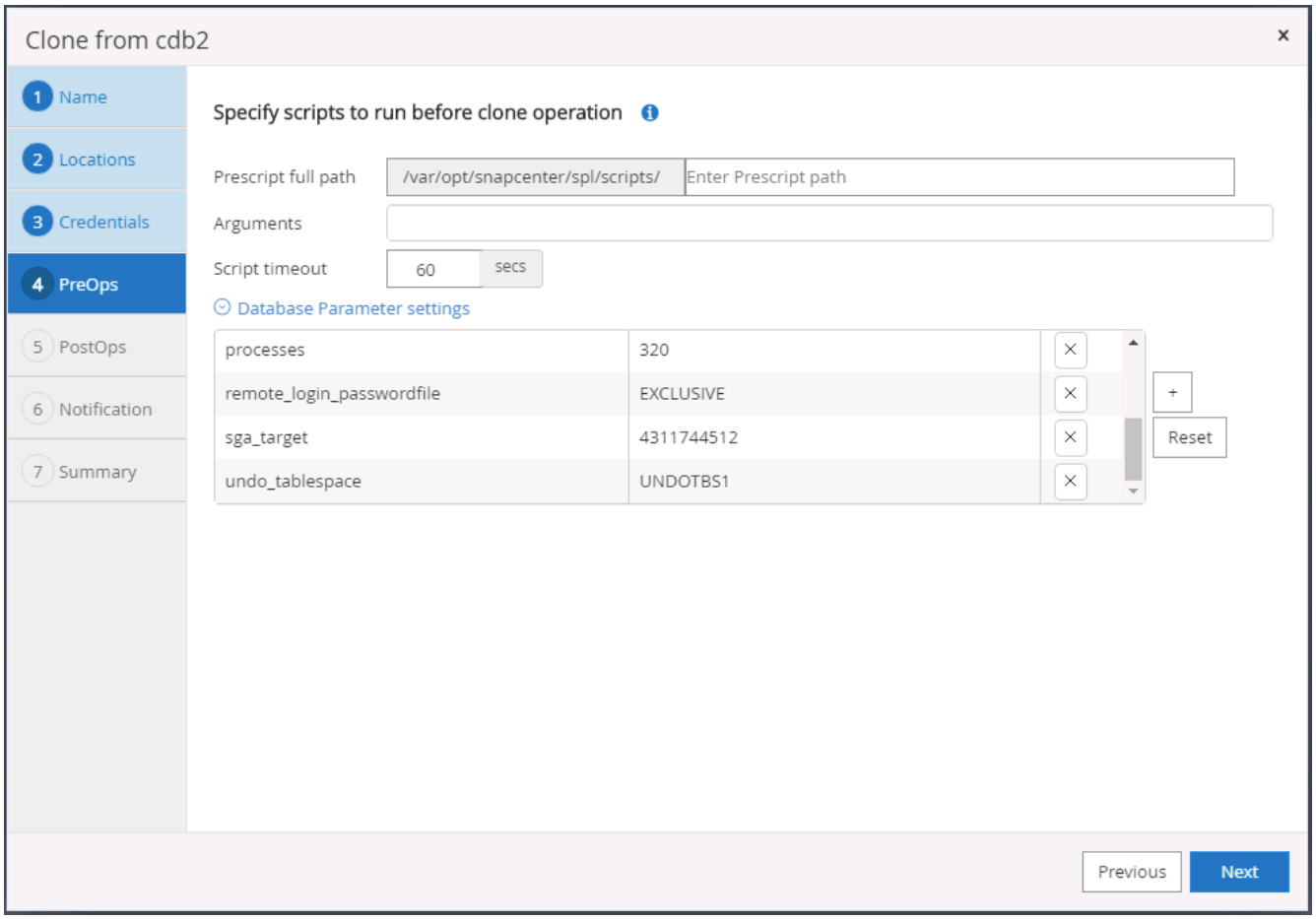
7. Sélectionnez l'hôte de clonage cible dans le cloud, et les répertoires de fichiers de données, de fichiers de contrôle et de journaux de rétablissement sont créés par le flux de travail de clonage.



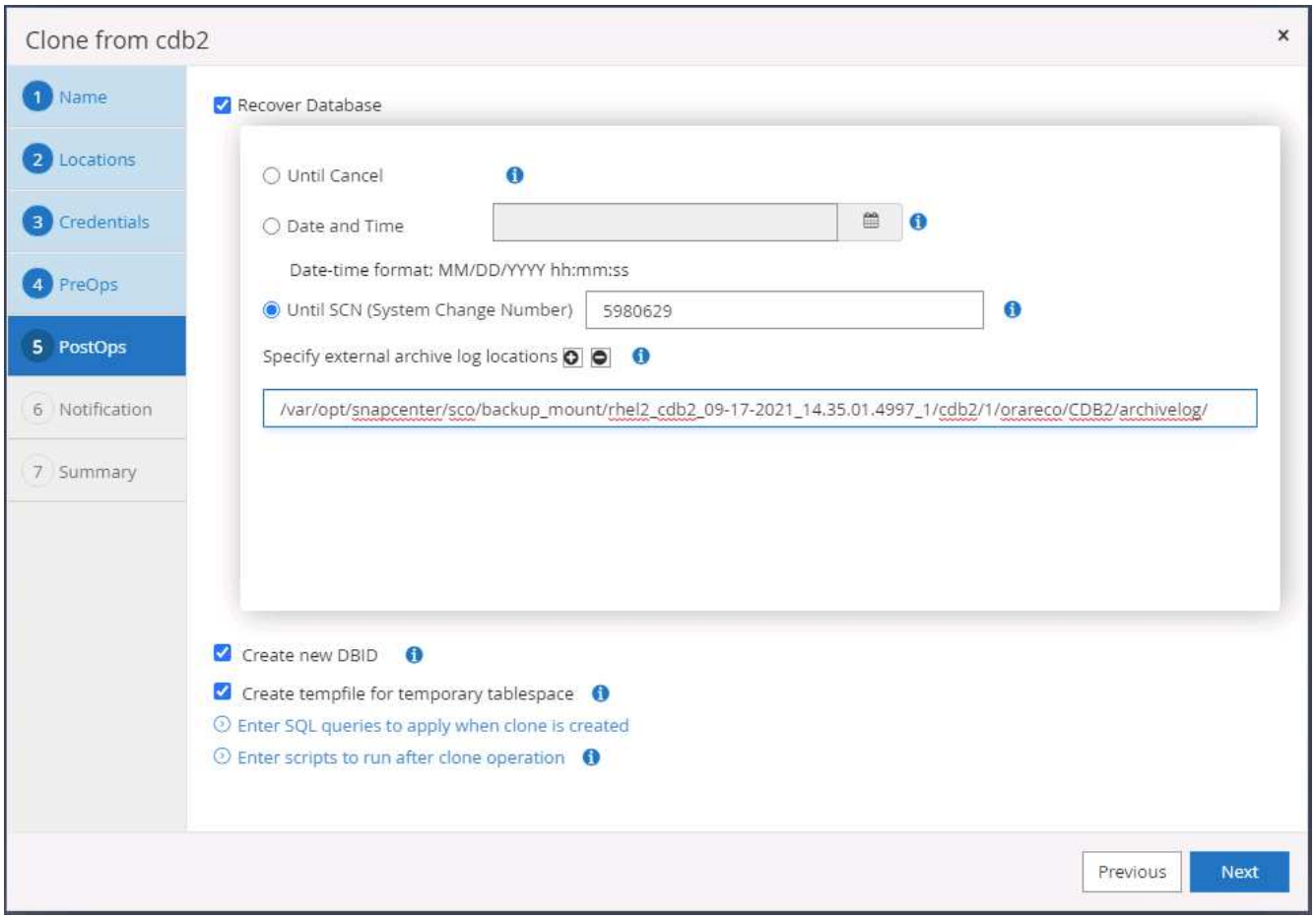
8. Le nom d'identification None est utilisé pour l'authentification basée sur le système d'exploitation, ce qui rend le port de base de données non pertinent. Renseignez les champs Oracle Home, Oracle OS User et Oracle OS Group appropriés tels que configurés dans le serveur de base de données clone cible.

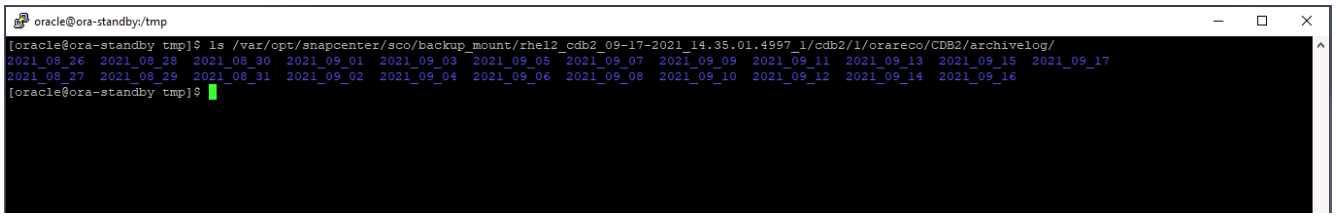


9. Spécifiez les scripts à exécuter avant l'opération de clonage. Plus important encore, le paramètre d'instance de base de données peut être ajusté ou défini ici.

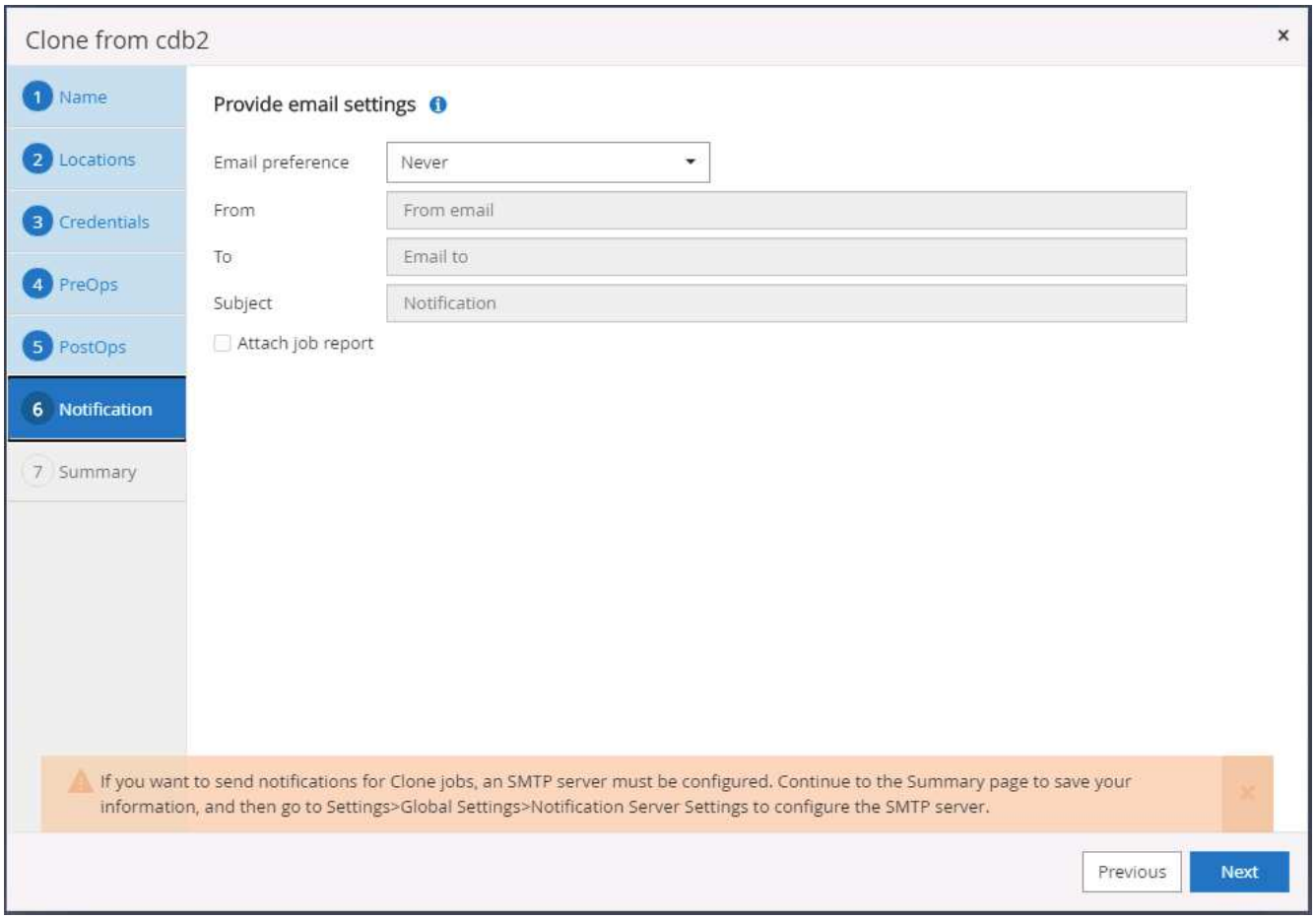


10. Spécifiez le point de récupération soit par la date et l'heure, soit par le SCN. Jusqu'à ce que Cancel récupère la base de données jusqu'aux journaux d'archives disponibles. Spécifiez l'emplacement du journal d'archive externe à partir de l'hôte cible sur lequel le volume du journal d'archive est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

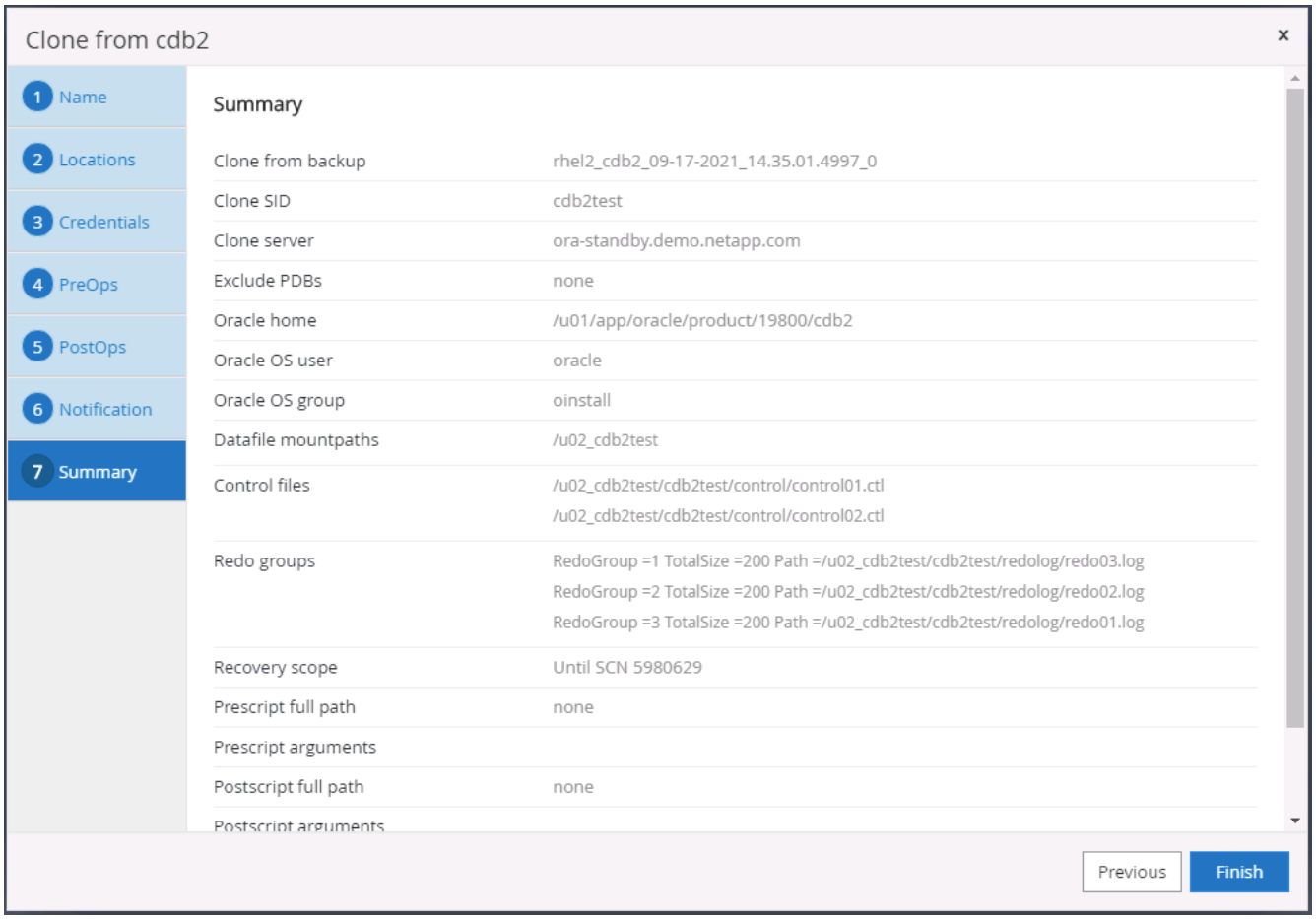




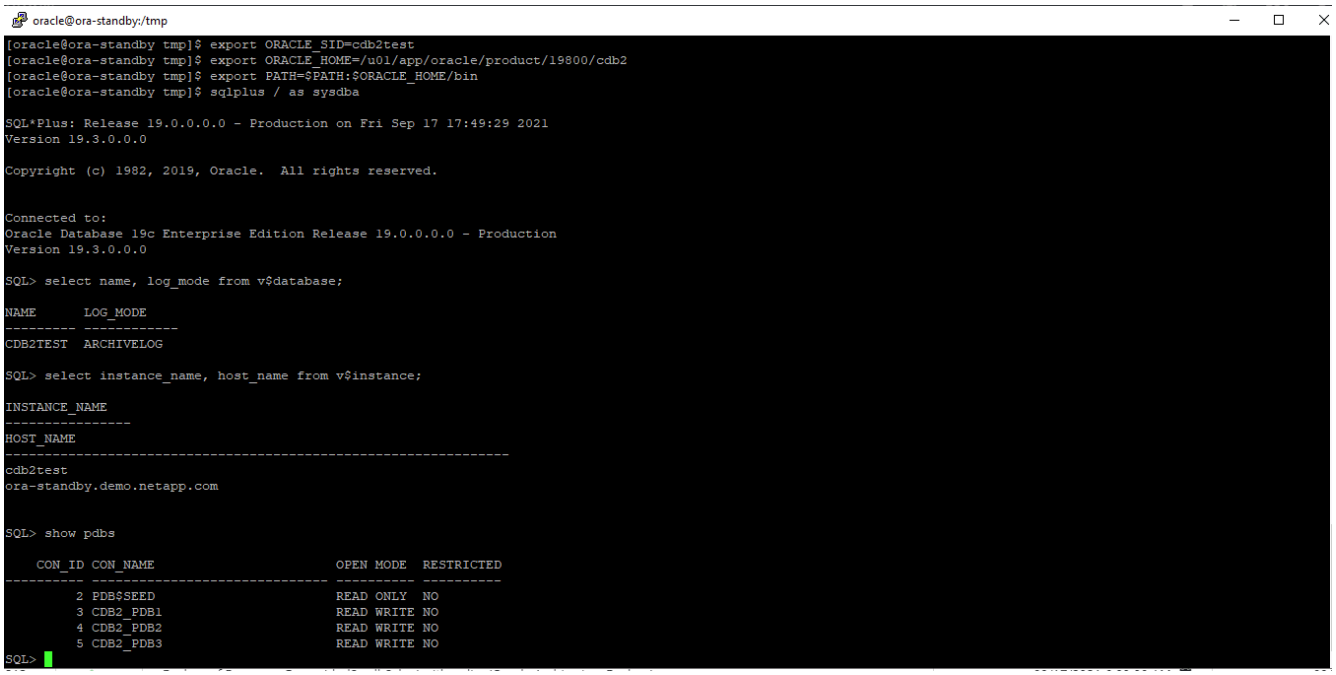
11. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.



12. Résumé du clone.

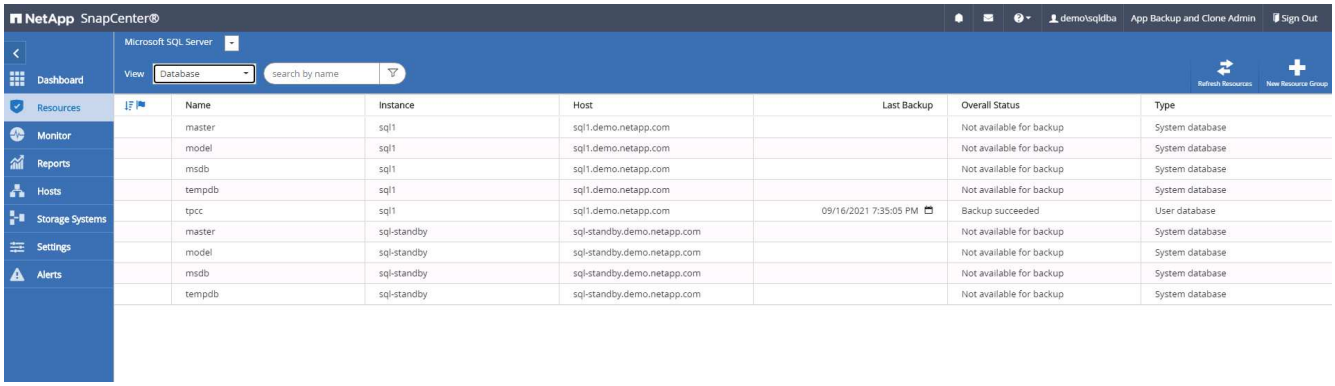


13. Vous devez valider après le clonage pour vous assurer que la base de données clonée est opérationnelle. Certaines tâches supplémentaires, telles que le démarrage de l'écouteur ou la désactivation du mode d'archivage du journal de la base de données, peuvent être effectuées sur la base de données dev/test.

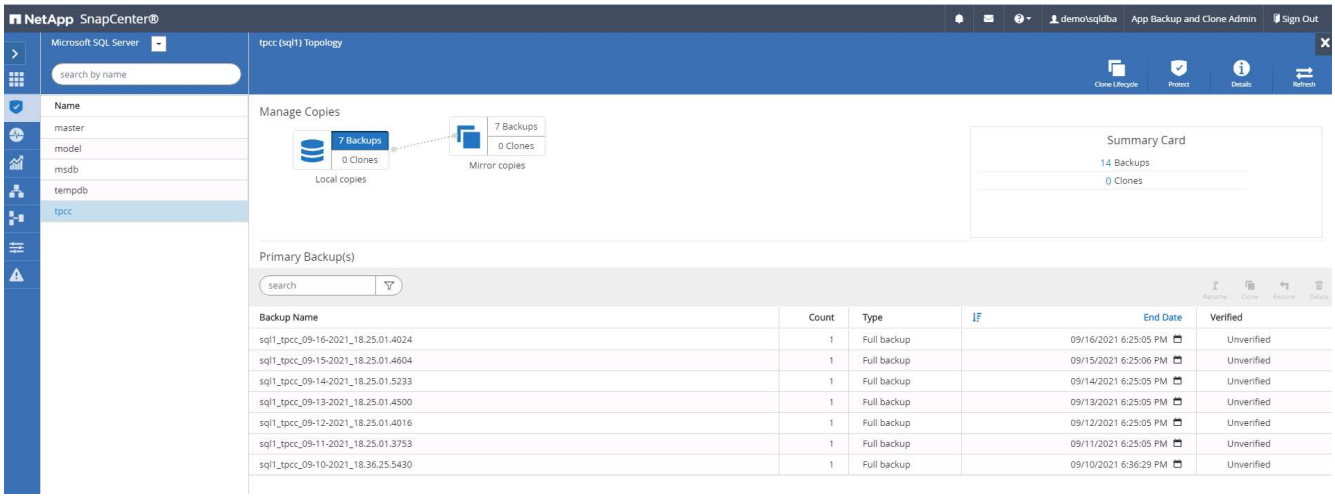


Cloner une base de données SQL pour le développement/test à partir d'une sauvegarde Snapshot répliquée

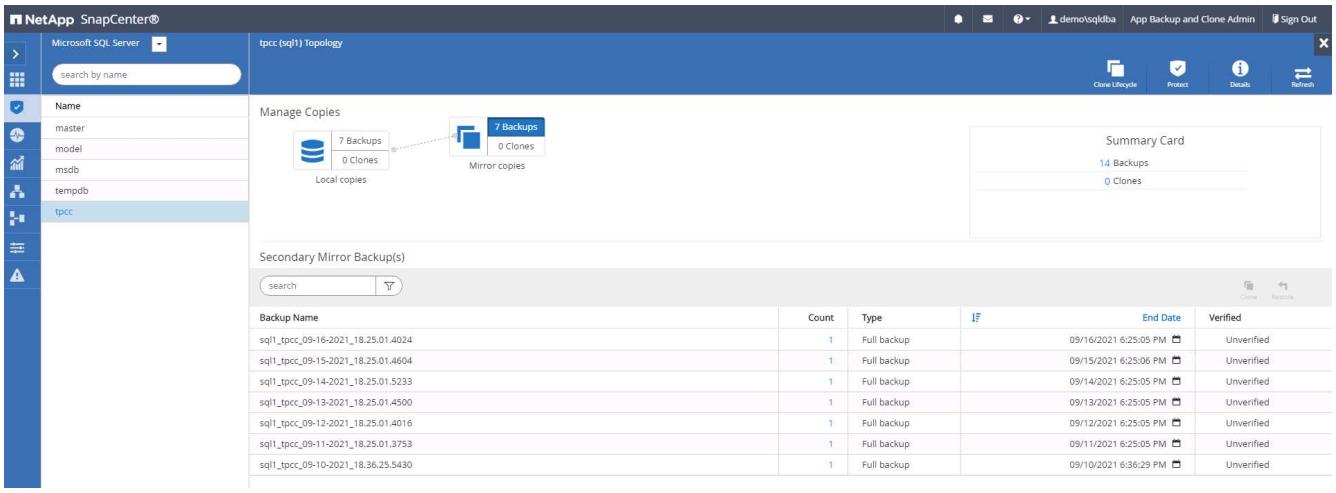
1. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données pour SQL Server. Accédez à l'onglet Ressources, qui affiche les bases de données utilisateur SQL Server protégées par SnapCenter et une instance SQL de secours cible dans le cloud public.



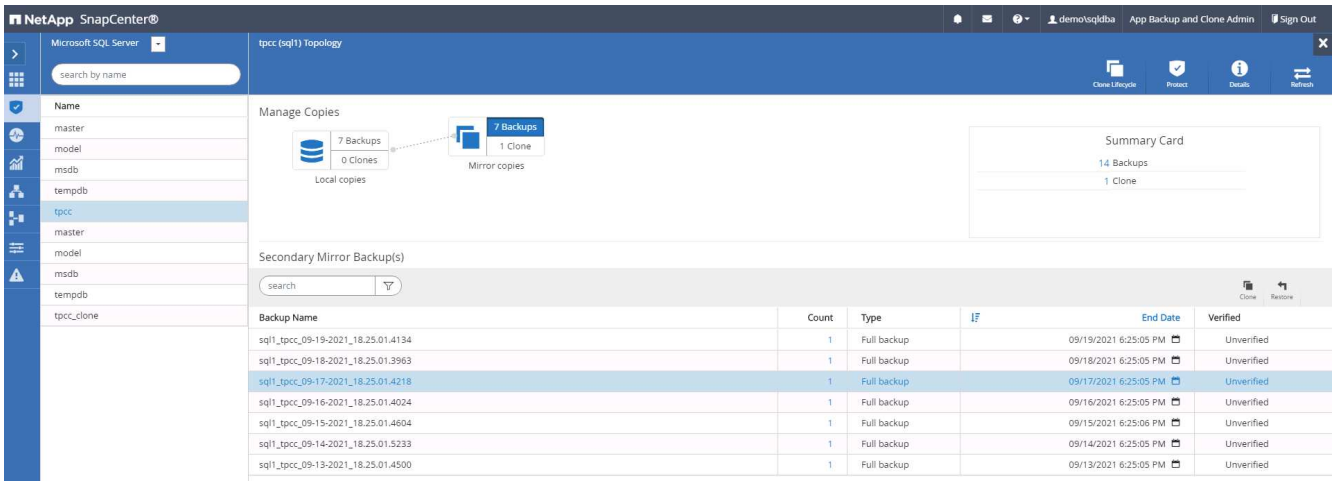
2. Cliquez sur le nom de la base de données utilisateur SQL Server sur site prévue pour la topologie des sauvegardes et la vue détaillée. Si un emplacement répliqué secondaire est activé, il affiche les sauvegardes miroir liées.

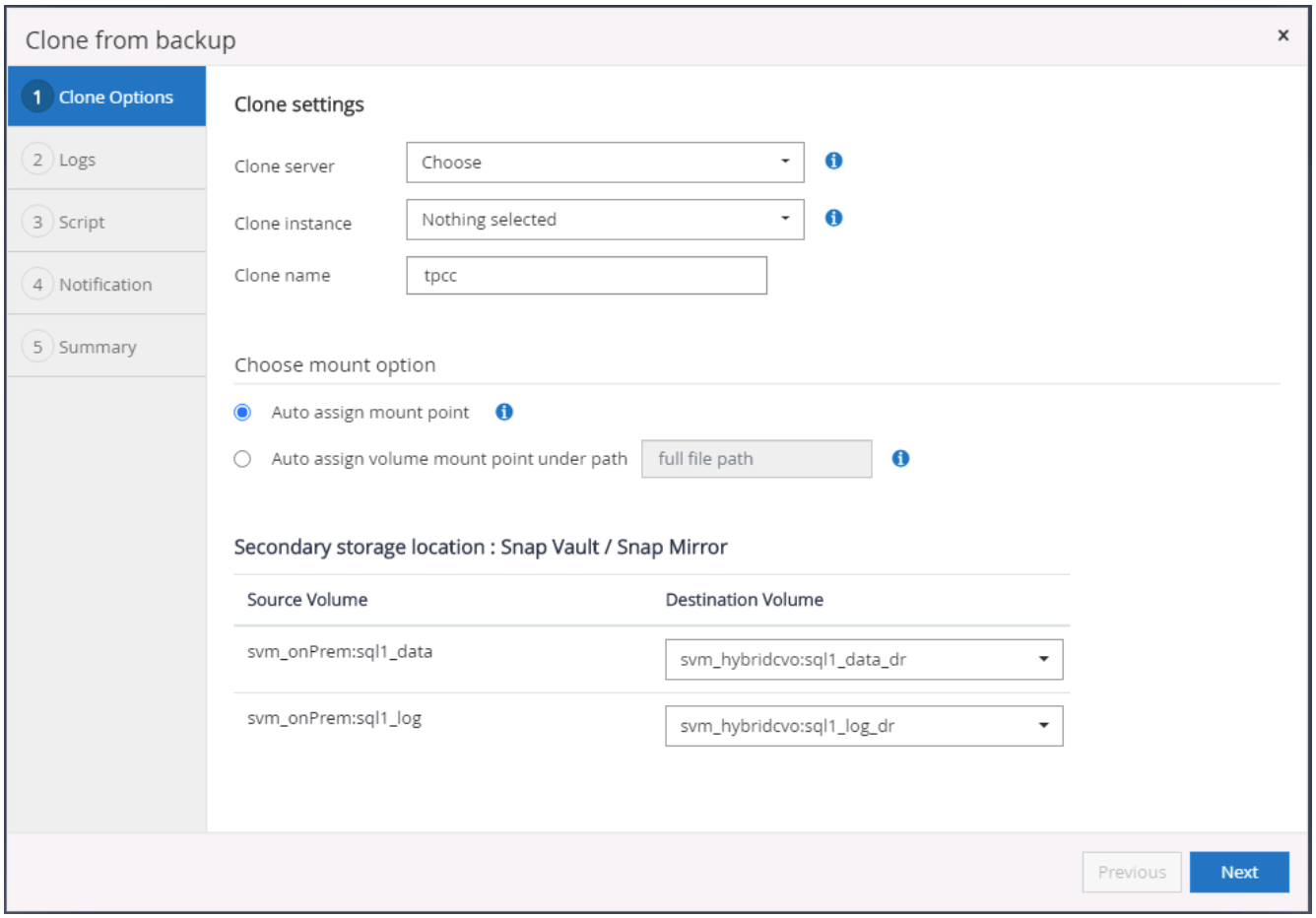


3. Basculez vers la vue Sauvegardes en miroir en cliquant sur Sauvegardes en miroir. Les sauvegardes miroir secondaires sont alors affichées. Étant donné que SnapCenter sauvegarde le journal des transactions SQL Server sur un lecteur dédié pour la récupération, seules les sauvegardes complètes de la base de données sont affichées ici.

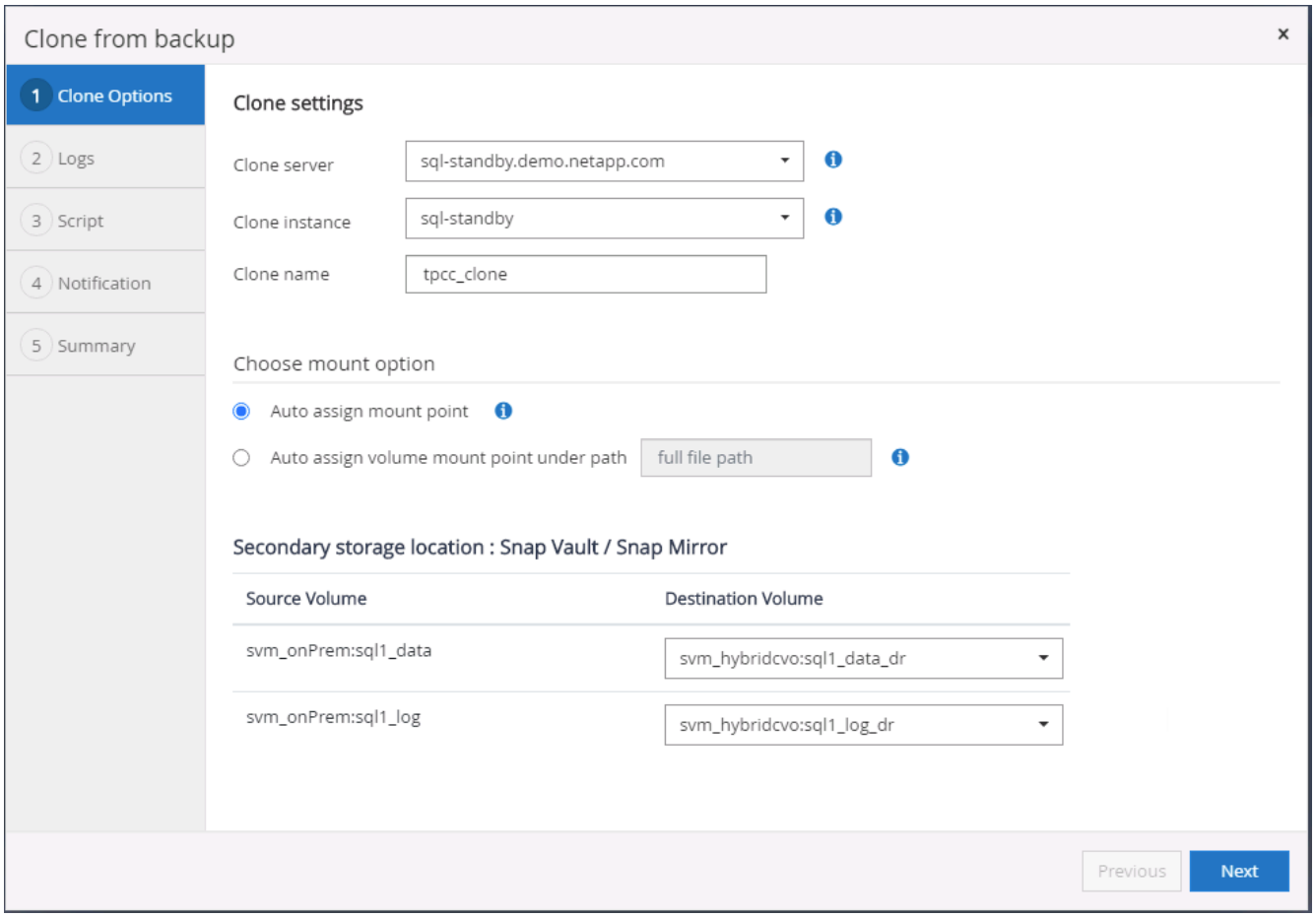


4. Choisissez une copie de sauvegarde, puis cliquez sur le bouton Cloner pour lancer le flux de travail Cloner à partir de la sauvegarde.

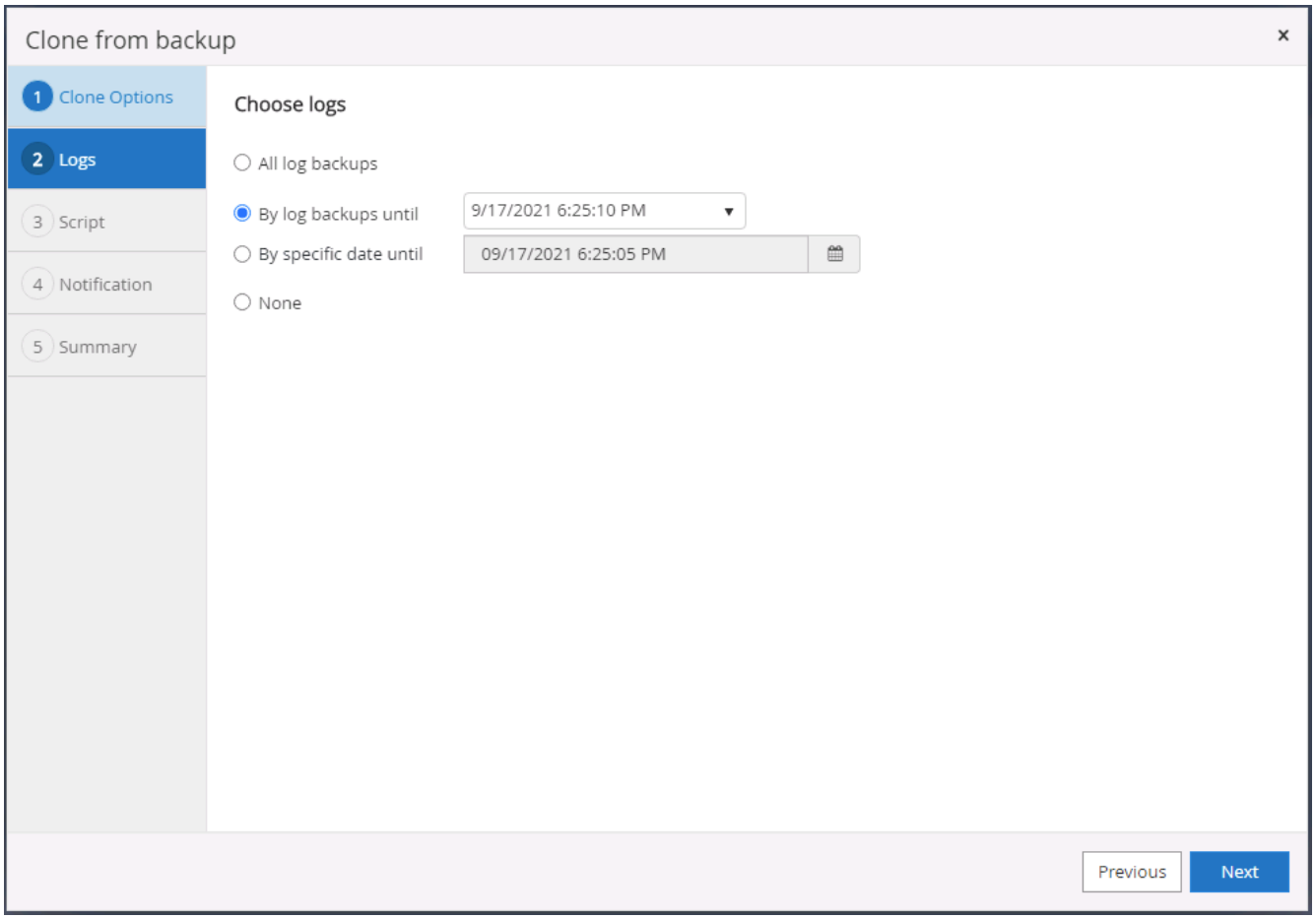




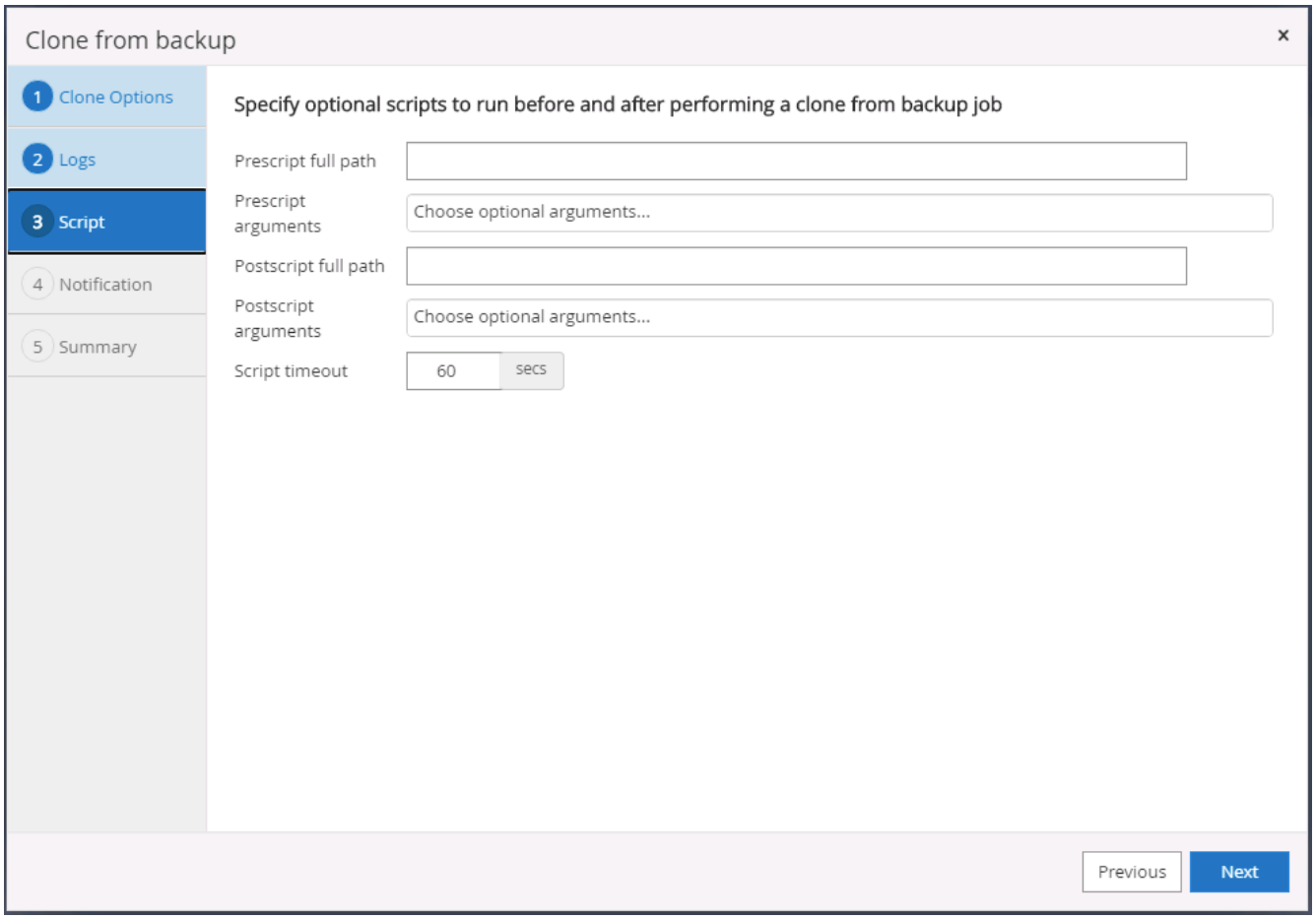
5. Sélectionnez un serveur cloud comme serveur clone cible, le nom de l'instance de clonage et le nom de la base de données de clonage. Choisissez soit un point de montage à attribution automatique, soit un chemin de point de montage défini par l'utilisateur.



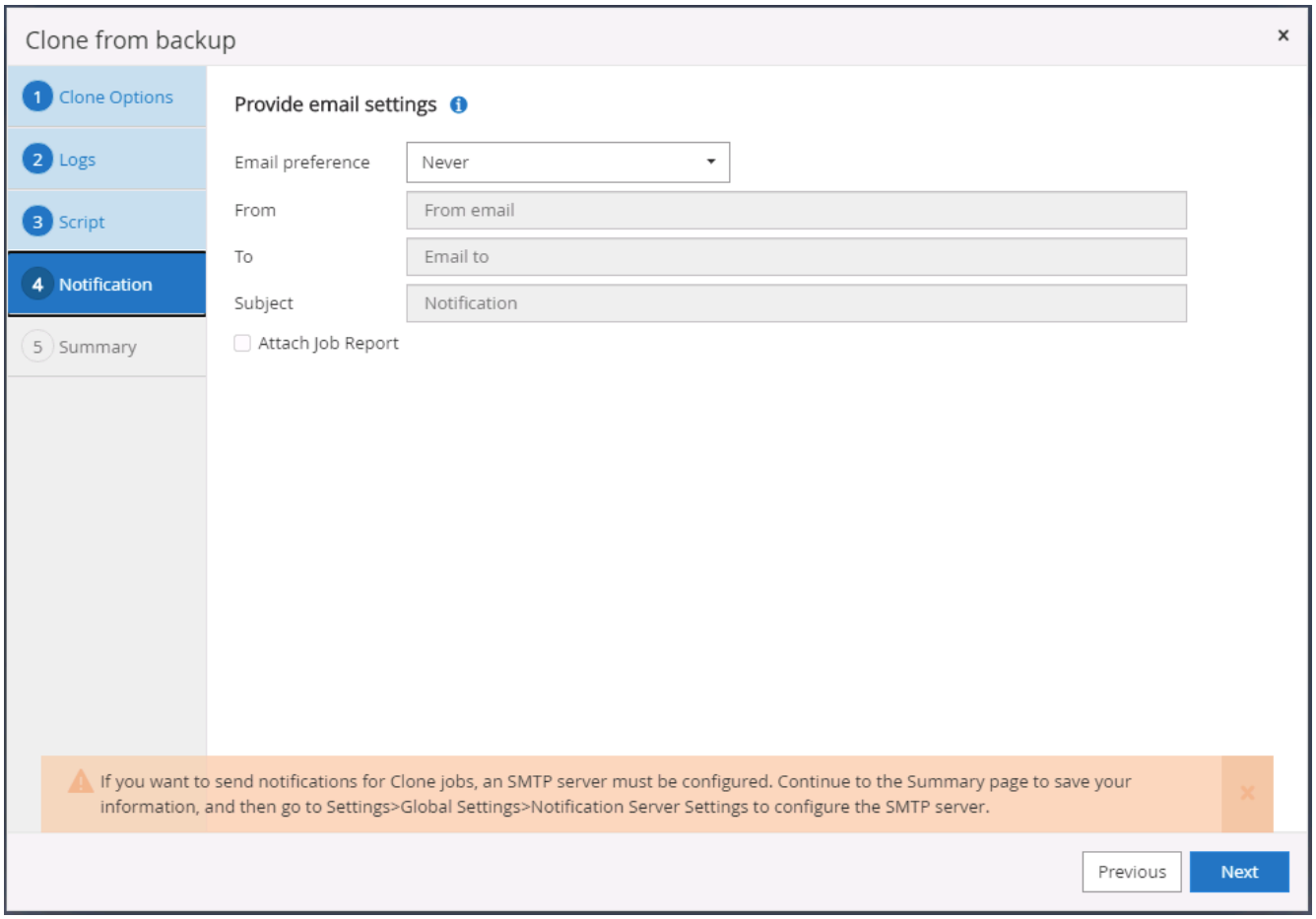
6. Déterminez un point de récupération soit par une heure de sauvegarde du journal, soit par une date et une heure spécifiques.



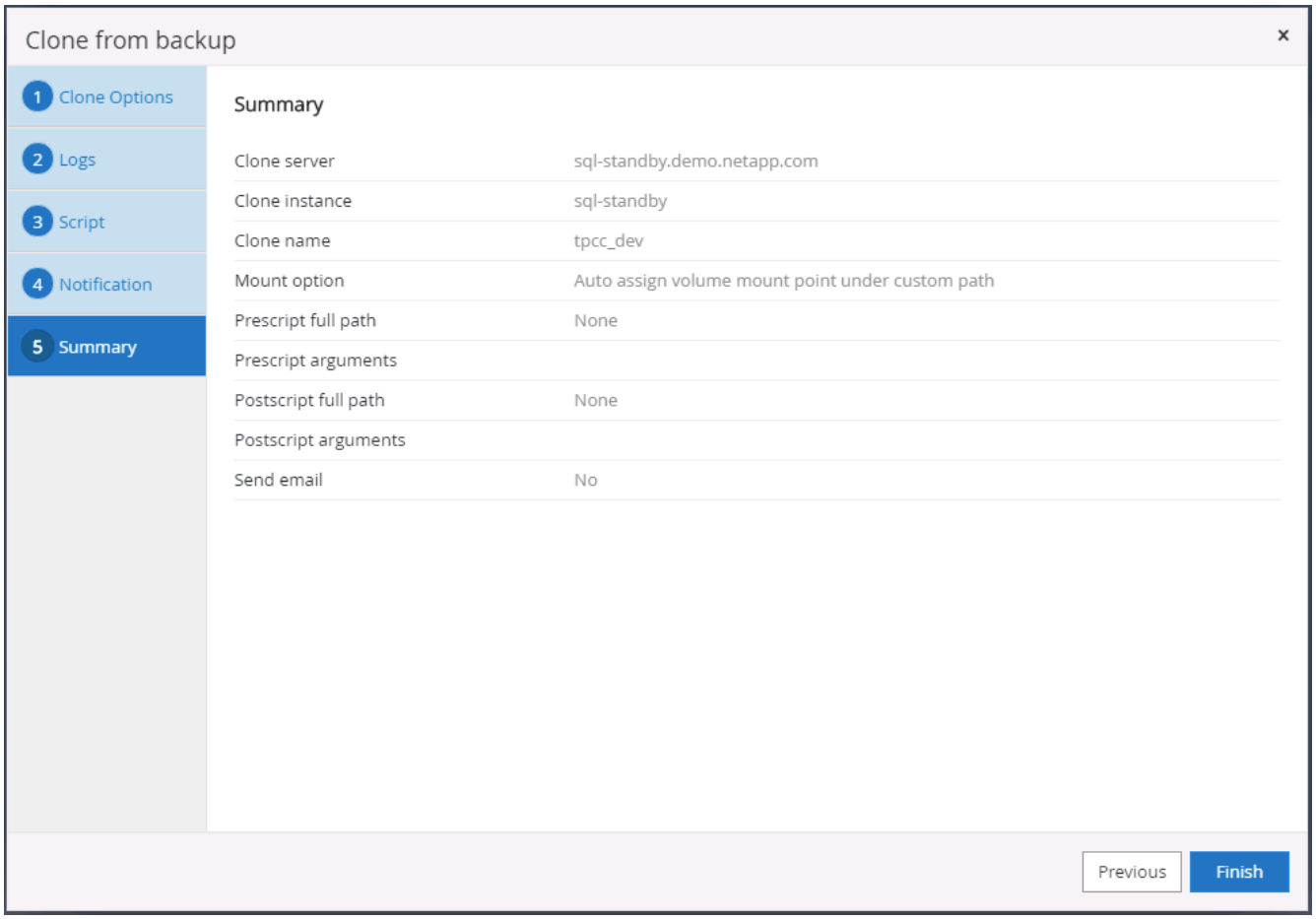
7. Spécifiez les scripts facultatifs à exécuter avant et après l'opération de clonage.



8. Configurez un serveur SMTP si une notification par e-mail est souhaitée.



9. Résumé du clone.



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

Configuration post-clonage

1. Une base de données de production Oracle sur site s'exécute généralement 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 du journal, connectez-vous à la base de données Oracle en tant que sysdba, exécutez une commande de changement de mode de journal et démarrez la base de données pour y accéder.
2. Configurez un écouteur Oracle ou enregistrez la base de données nouvellement clonée avec un écouteur existant pour l'accès utilisateur.
3. Pour SQL Server, modifiez le mode de journalisation de Complet à Facile afin que le fichier journal de développement/test SQL Server puisse être facilement réduit lorsqu'il remplit le volume du journal.

Actualiser la base de données clonée

1. Supprimez les bases de données clonées et nettoyez l'environnement du serveur de base de données cloud. Suivez ensuite les procédures précédentes pour cloner une nouvelle base de données avec de nouvelles données. Il ne faut que quelques minutes pour cloner une nouvelle base de données.
2. Arrêtez la base de données clonée, exécutez une commande d'actualisation de clone à l'aide de la CLI. Consultez la documentation SnapCenter suivante pour plus de détails :"Rafraîchir un clone" .

Où aller chercher de l'aide ?

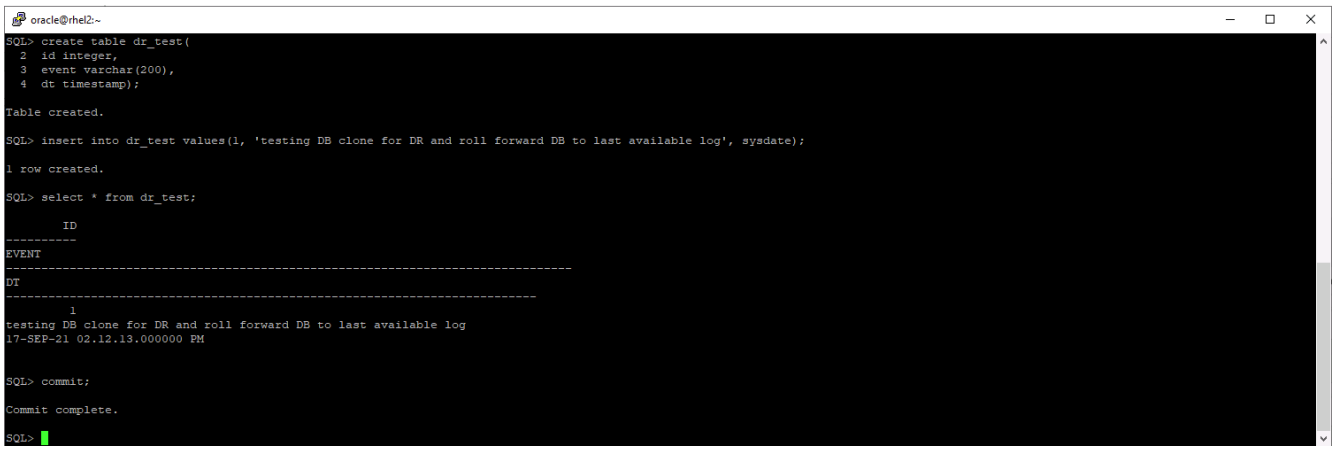
Si vous avez besoin d'aide avec cette solution et ces cas d'utilisation, rejoignez le"Canal Slack d'assistance de la communauté NetApp Solution Automation" et recherchez le canal solution-automatisation pour poster vos questions ou demandes de renseignements.

Flux de travail de reprise après sinistre

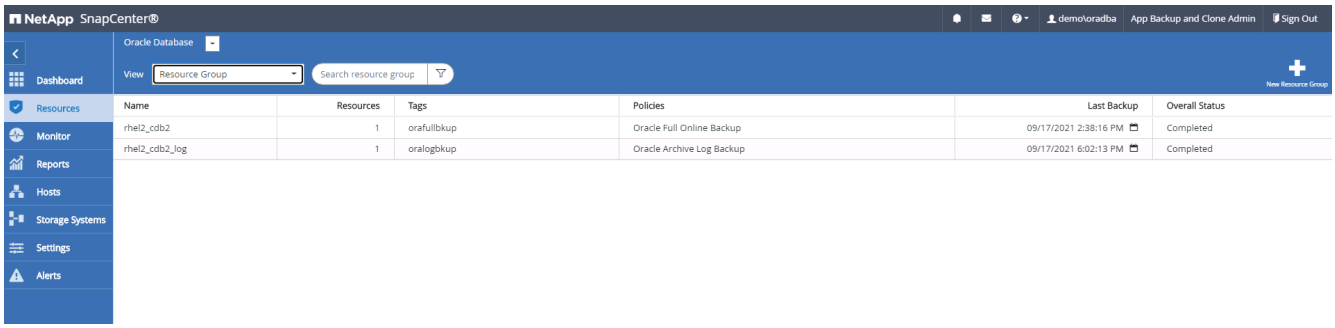
Les entreprises ont adopté le cloud public comme une ressource viable et une destination pour la reprise après sinistre. SnapCenter rend ce processus aussi transparent que possible. Ce flux de travail de récupération après sinistre est très similaire au flux de travail de clonage, mais la récupération de la base de données s'exécute sur le dernier journal disponible qui a été répliqué dans le cloud pour récupérer toutes les transactions commerciales possibles. Cependant, il existe des étapes de pré-configuration et de post-configuration supplémentaires spécifiques à la reprise après sinistre.

Cloner une base de données de production Oracle sur site vers le cloud pour la reprise après sinistre

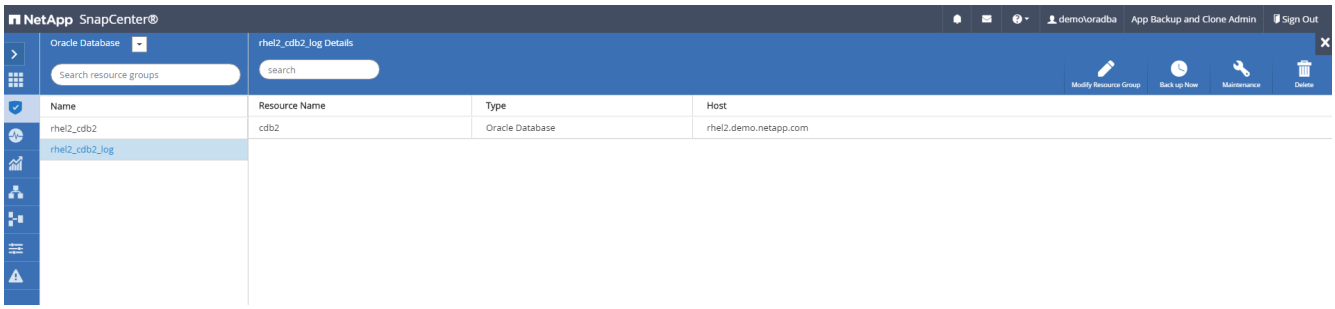
1. Pour valider que la récupération du clone s'exécute via le dernier journal disponible, nous avons créé une petite table de test et inséré une ligne. Les données de test seront récupérées après une récupération complète du dernier journal disponible.

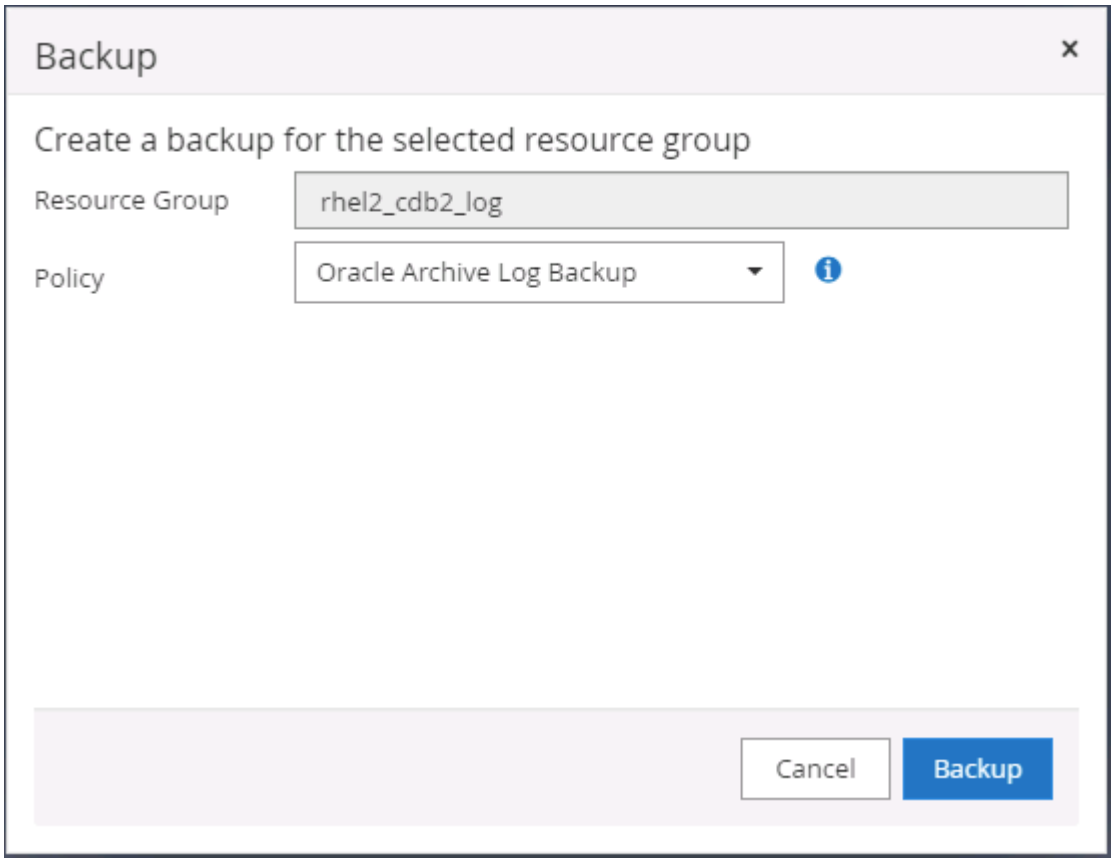


2. Connectez-vous à SnapCenter en tant qu'ID utilisateur de gestion de base de données pour Oracle. Accédez à l'onglet Ressources, qui affiche les bases de données Oracle protégées par SnapCenter.



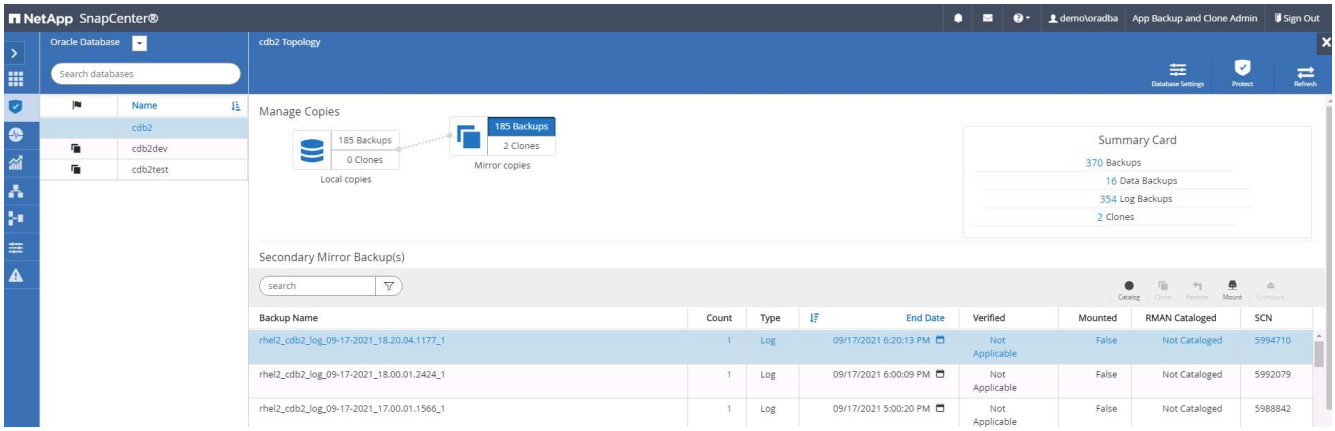
3. Sélectionnez le groupe de ressources de journal Oracle et cliquez sur Sauvegarder maintenant pour exécuter manuellement une sauvegarde du journal Oracle afin de vider la dernière transaction vers la destination dans le cloud. Dans un scénario DR réel, la dernière transaction récupérable dépend de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

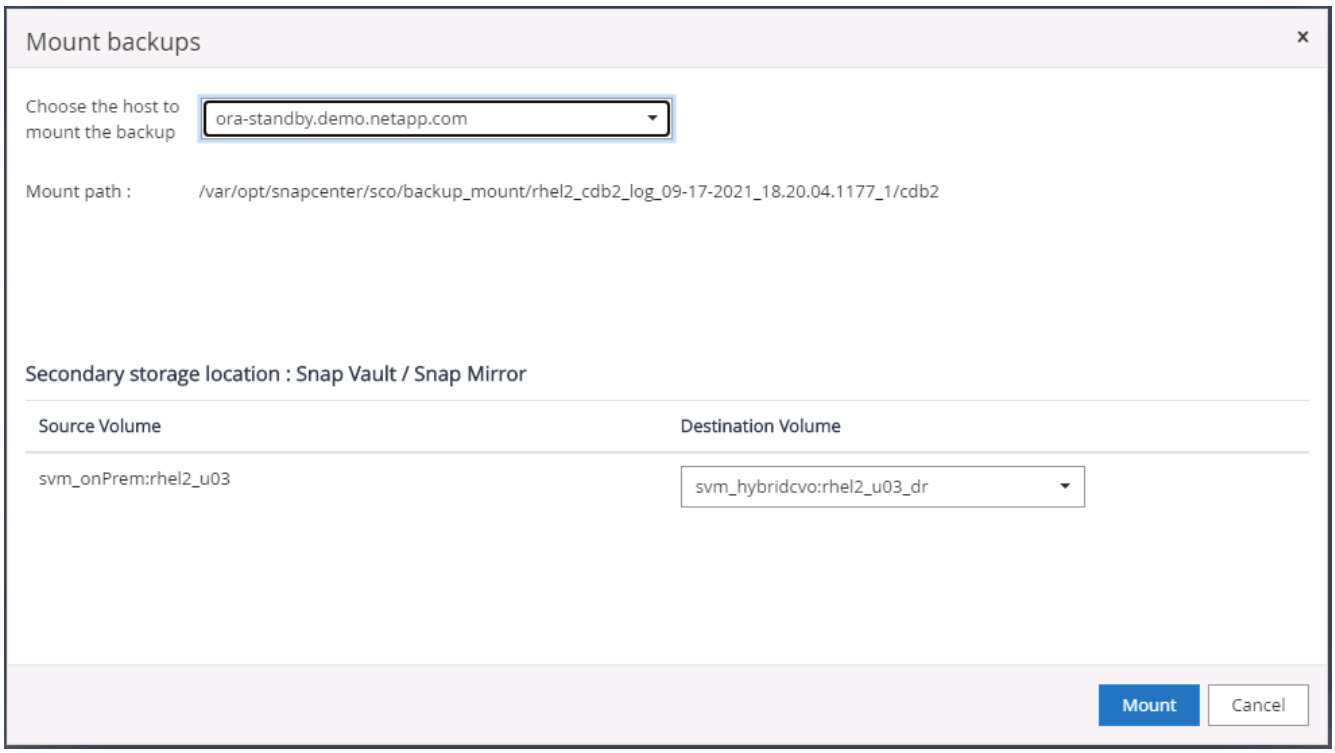




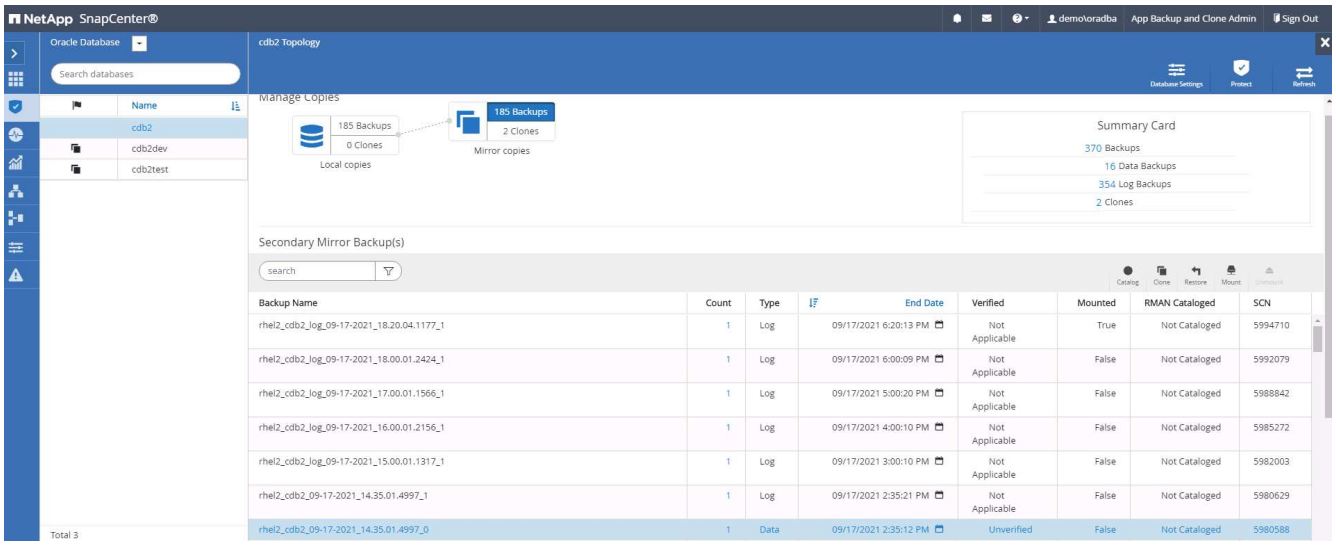
SnapMirror asynchrone perd les données qui n'ont pas atteint la destination cloud dans l'intervalle de sauvegarde du journal de base de données dans un scénario de reprise après sinistre. Pour minimiser la perte de données, des sauvegardes de journaux plus fréquentes peuvent être planifiées. Cependant, il existe une limite à la fréquence de sauvegarde des journaux qui est techniquement réalisable.

4. Sélectionnez la dernière sauvegarde du journal sur la ou les sauvegardes du miroir secondaire et montez la sauvegarde du journal.

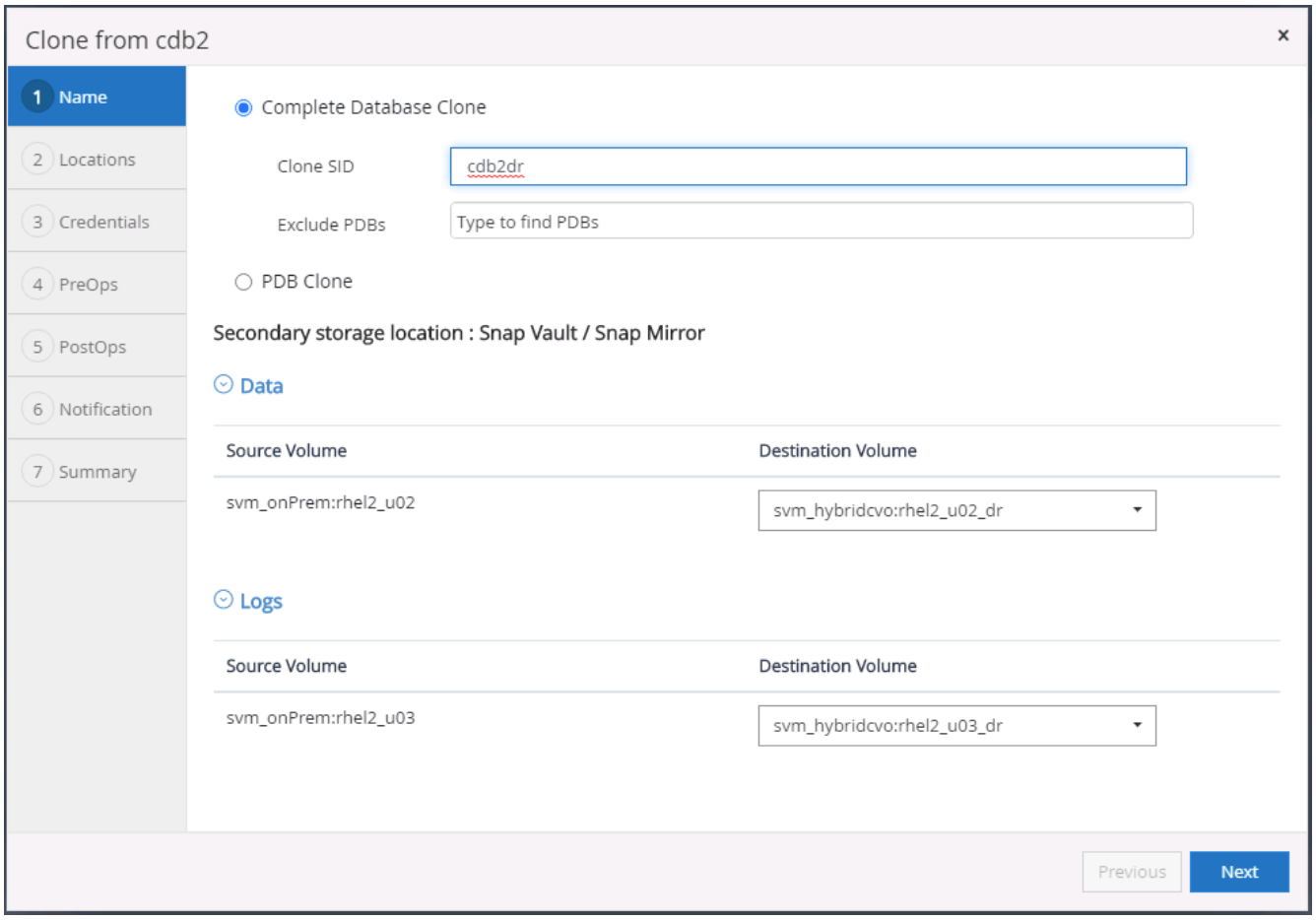




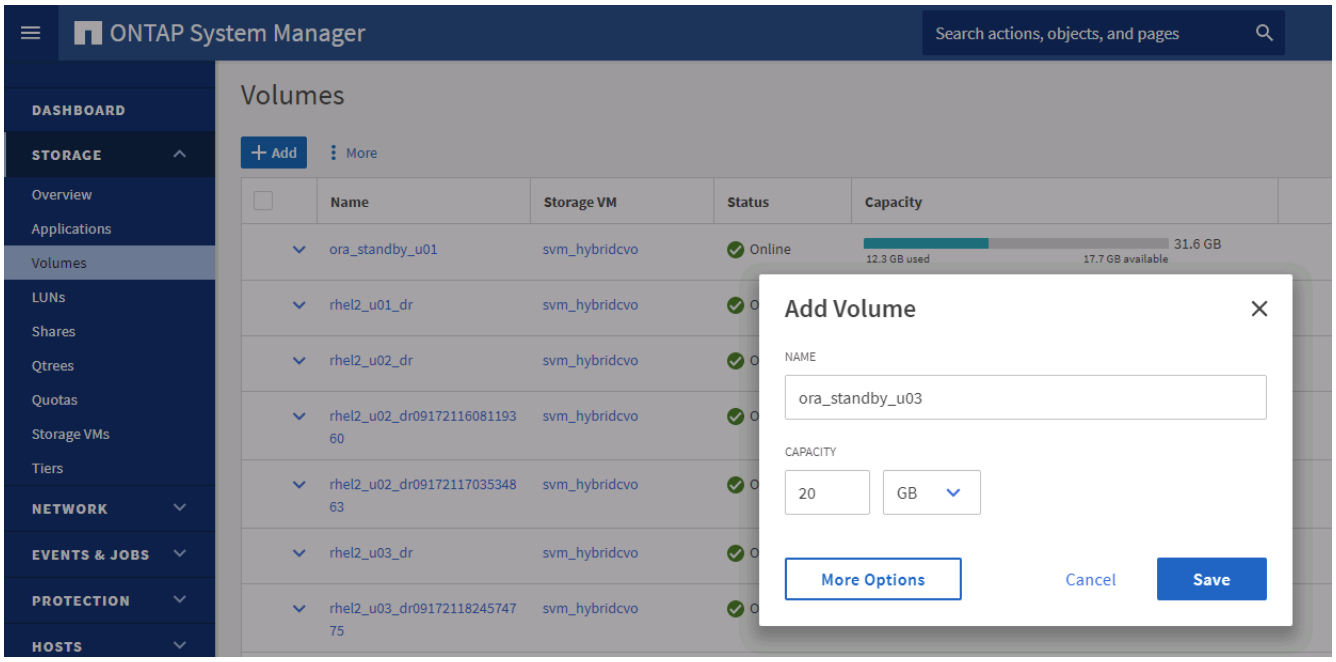
5. Sélectionnez la dernière sauvegarde complète de la base de données et cliquez sur Cloner pour lancer le flux de travail de clonage.

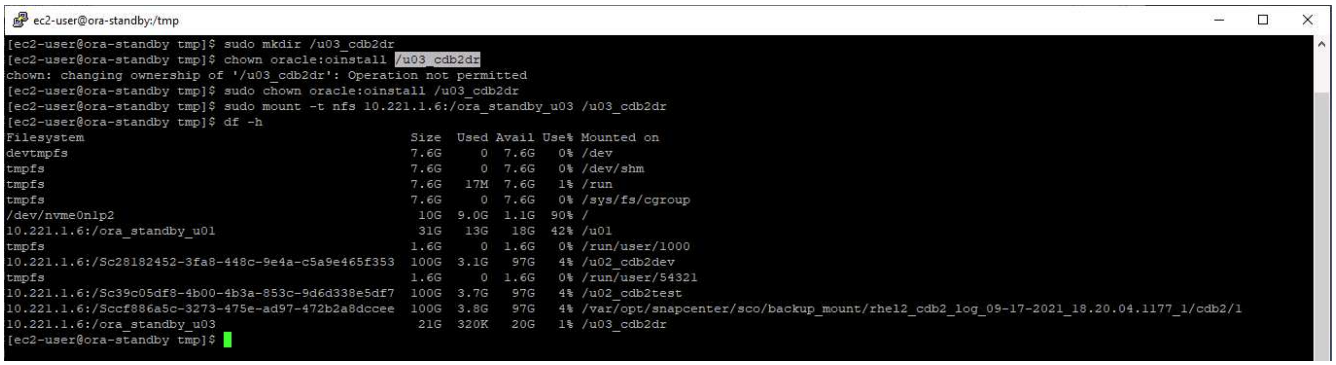


6. Sélectionnez un ID de base de données clone unique sur l'hôte.



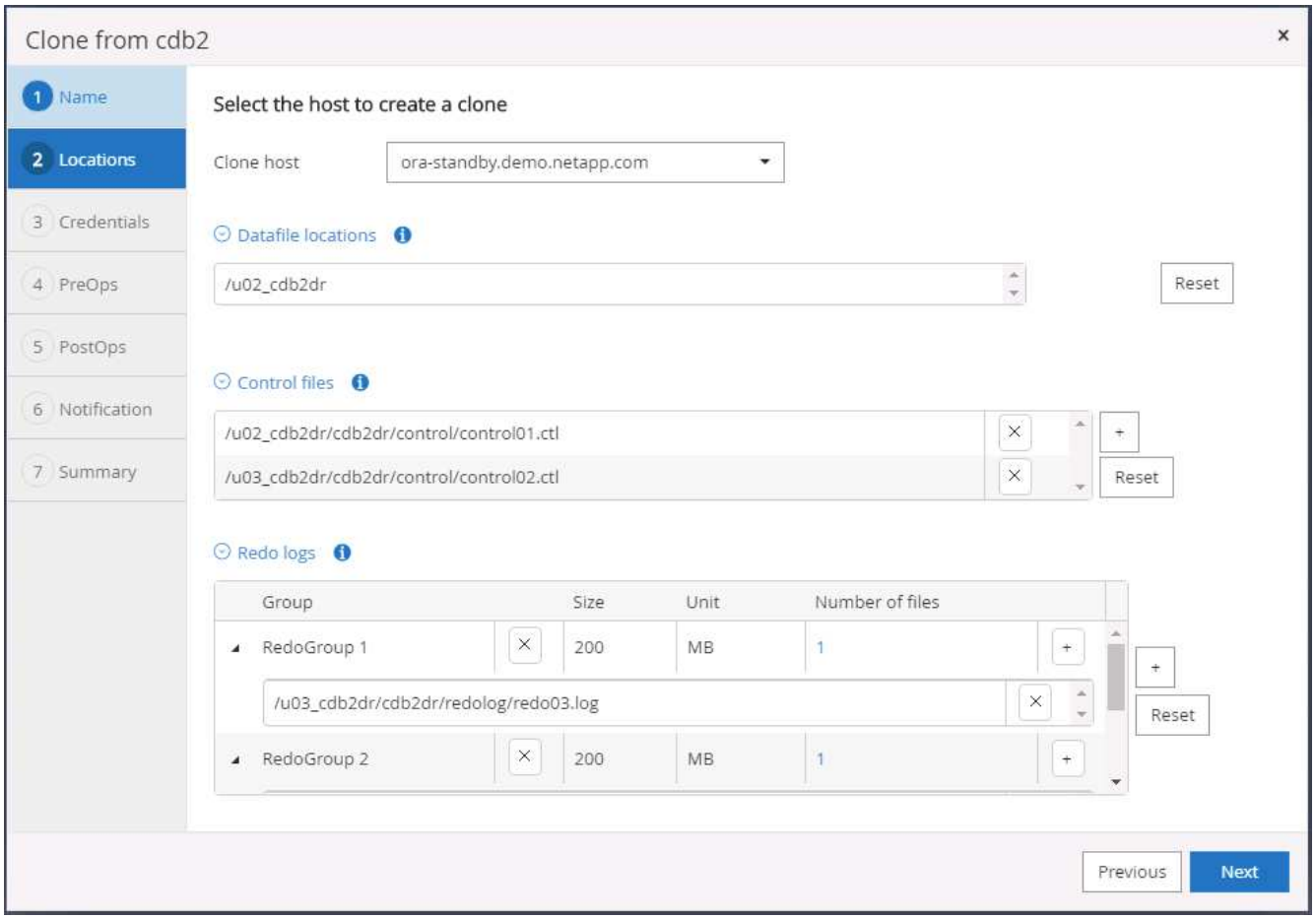
7. Provisionnez un volume de journal et montez-le sur le serveur DR cible pour la zone de récupération flash Oracle et les journaux en ligne.



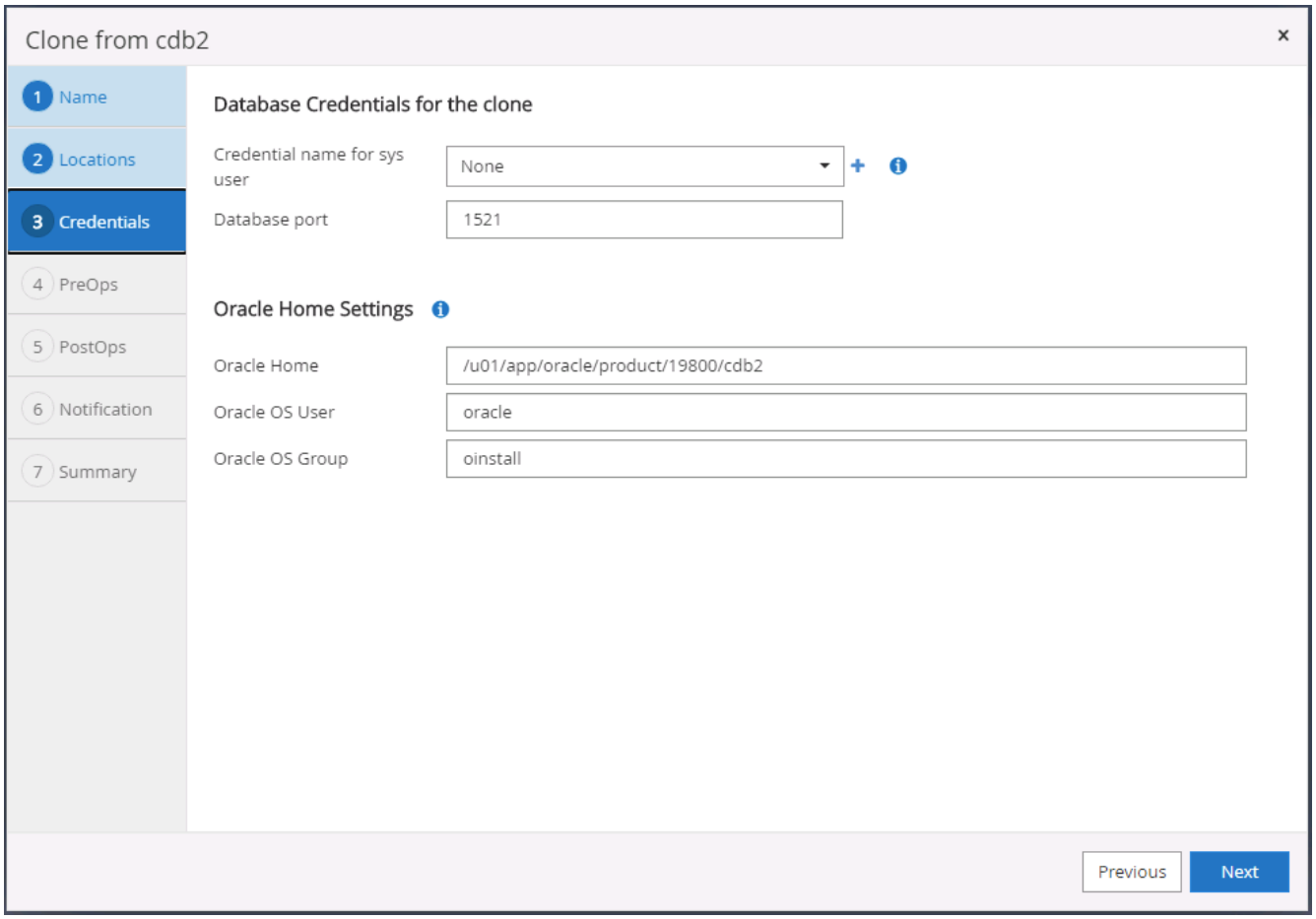


La procédure de clonage Oracle ne crée pas de volume de journal, qui doit être provisionné sur le serveur DR avant le clonage.

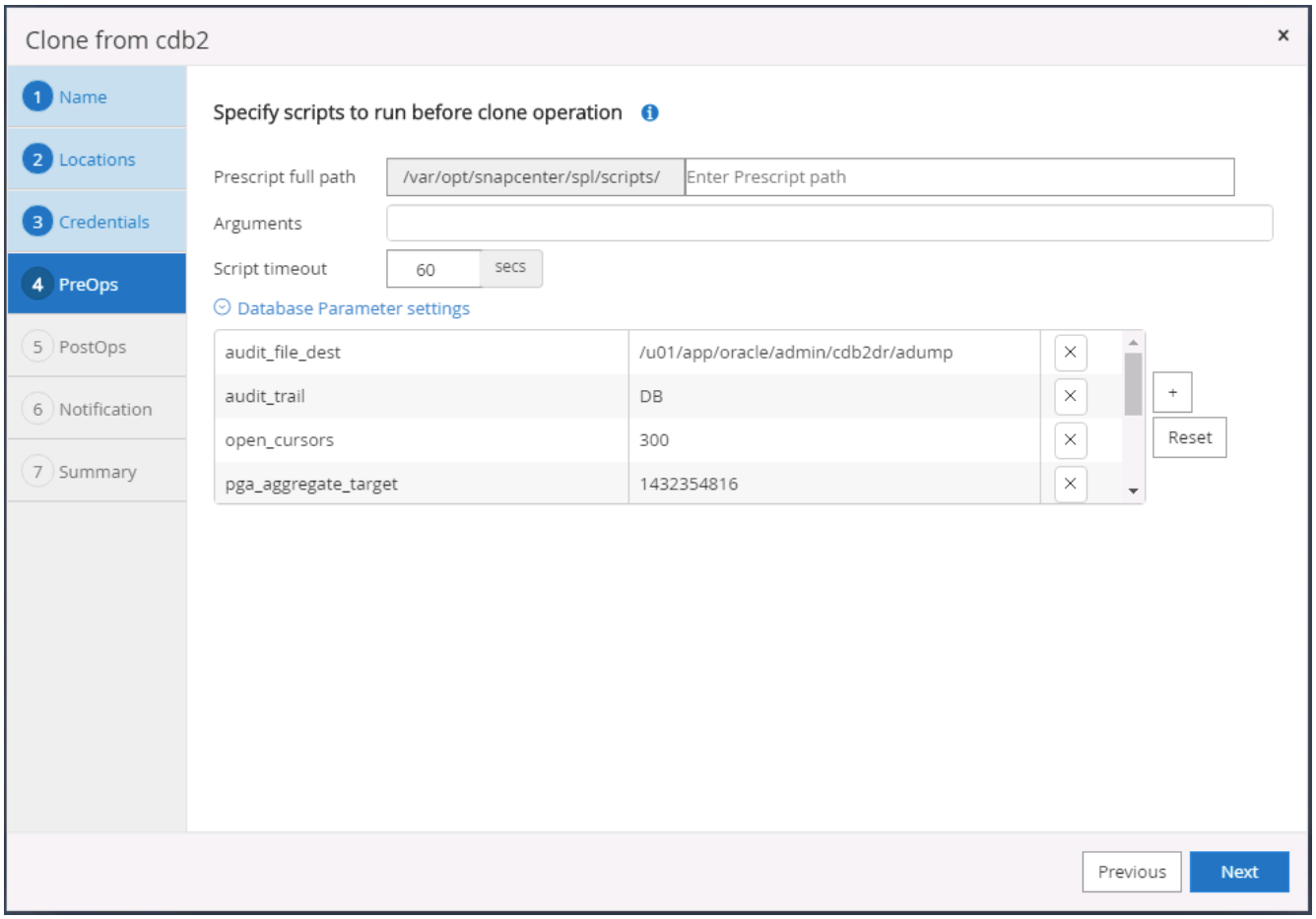
8. Sélectionnez l'hôte de clonage cible et l'emplacement où placer les fichiers de données, les fichiers de contrôle et les journaux de rétablissement.



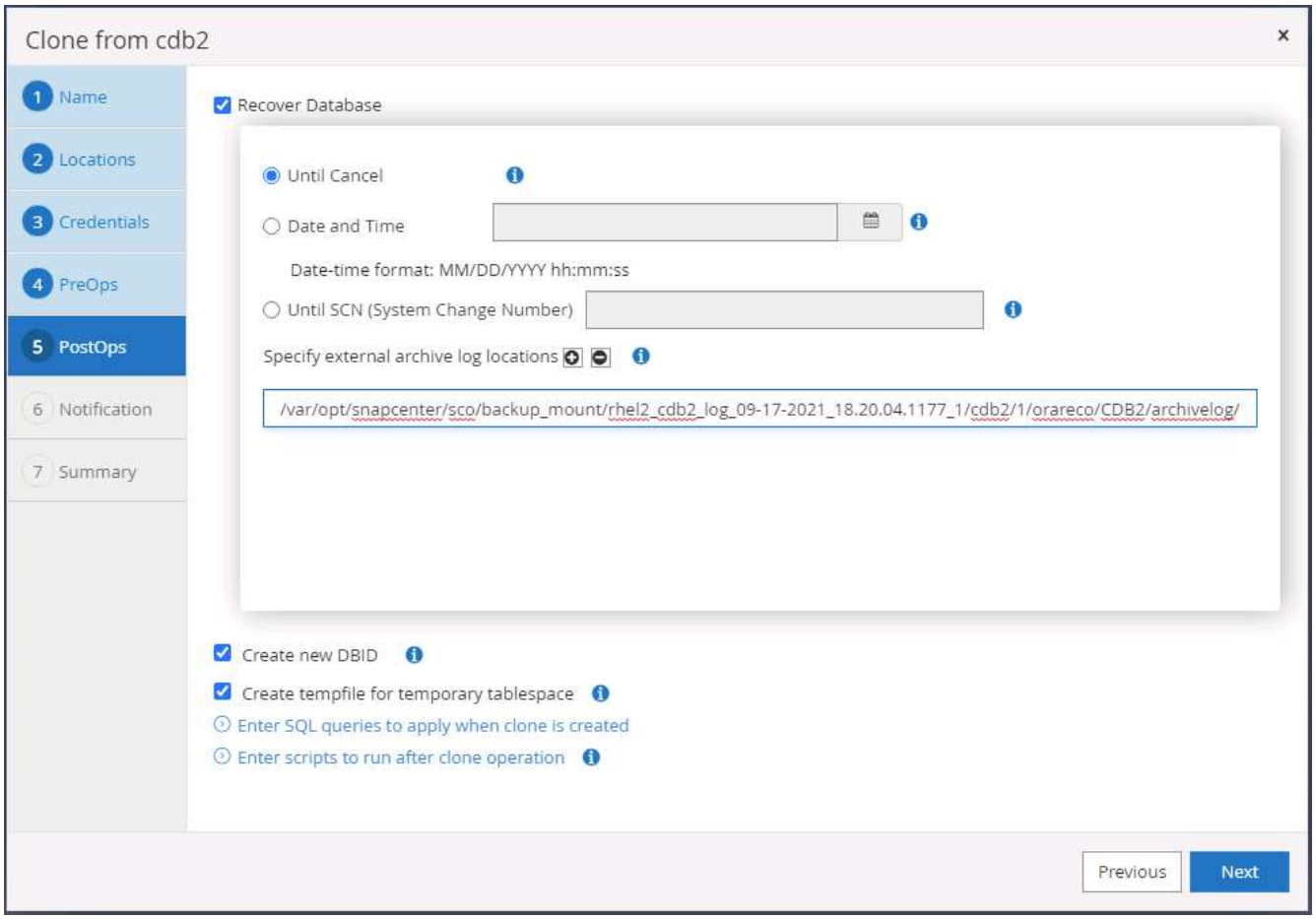
9. Sélectionnez les informations d'identification pour le clone. Renseignez les détails de la configuration Oracle Home sur le serveur cible.



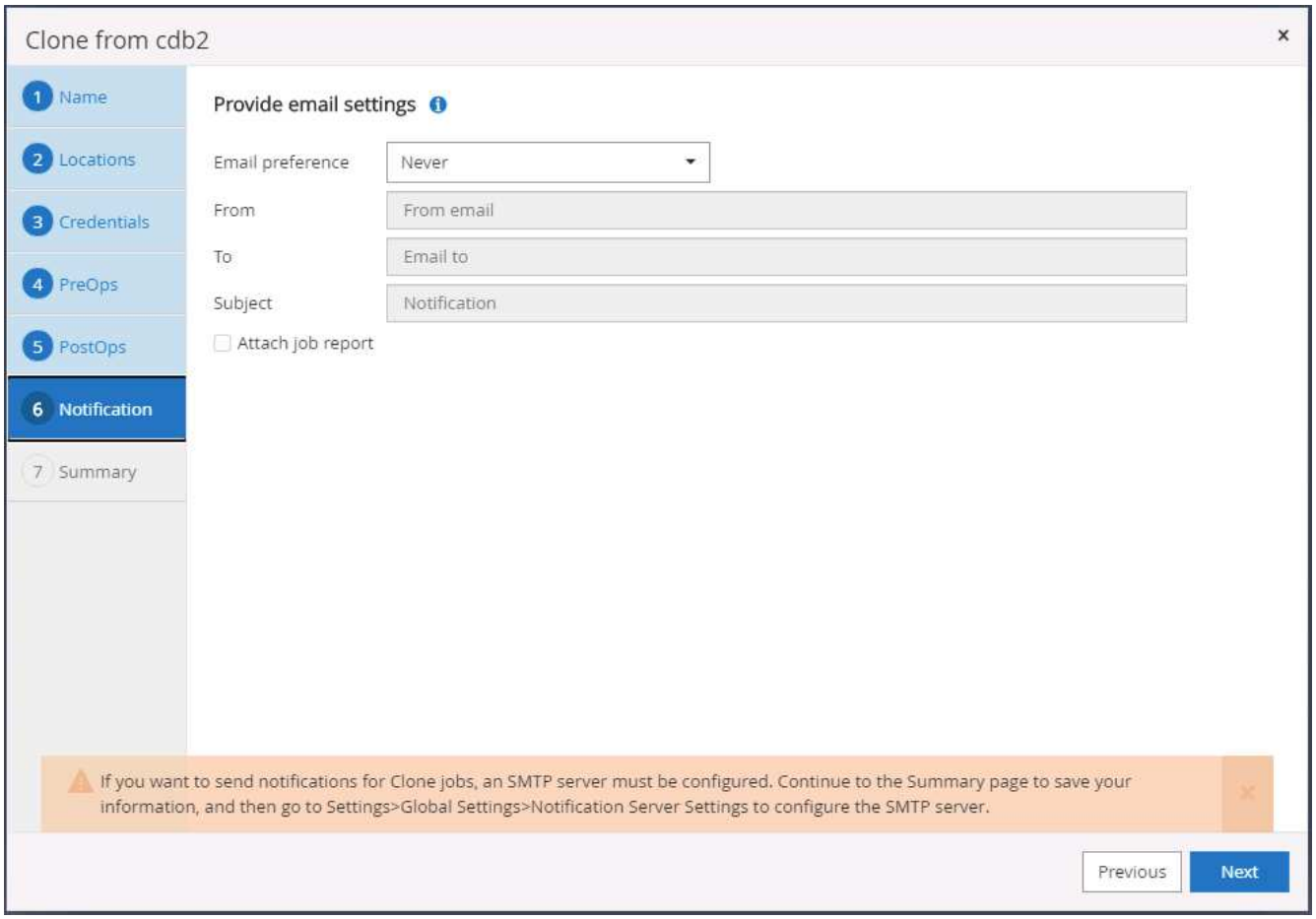
10. Spécifiez les scripts à exécuter avant le clonage. Les paramètres de la base de données peuvent être ajustés si nécessaire.



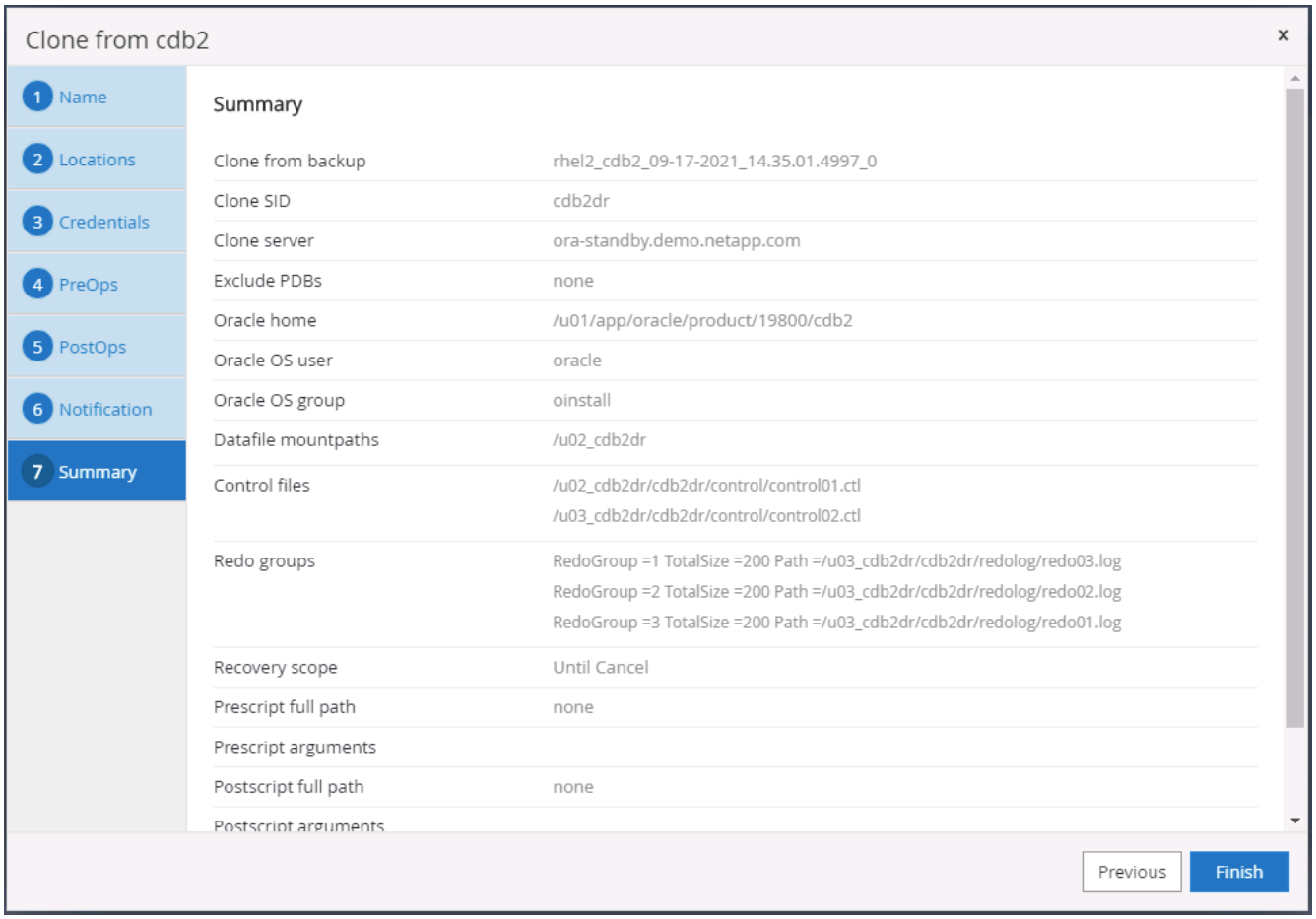
11. Sélectionnez Jusqu'à annulation comme option de récupération afin que la récupération parcoure tous les journaux d'archives disponibles pour récupérer la dernière transaction répliquée vers l'emplacement cloud secondaire.



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



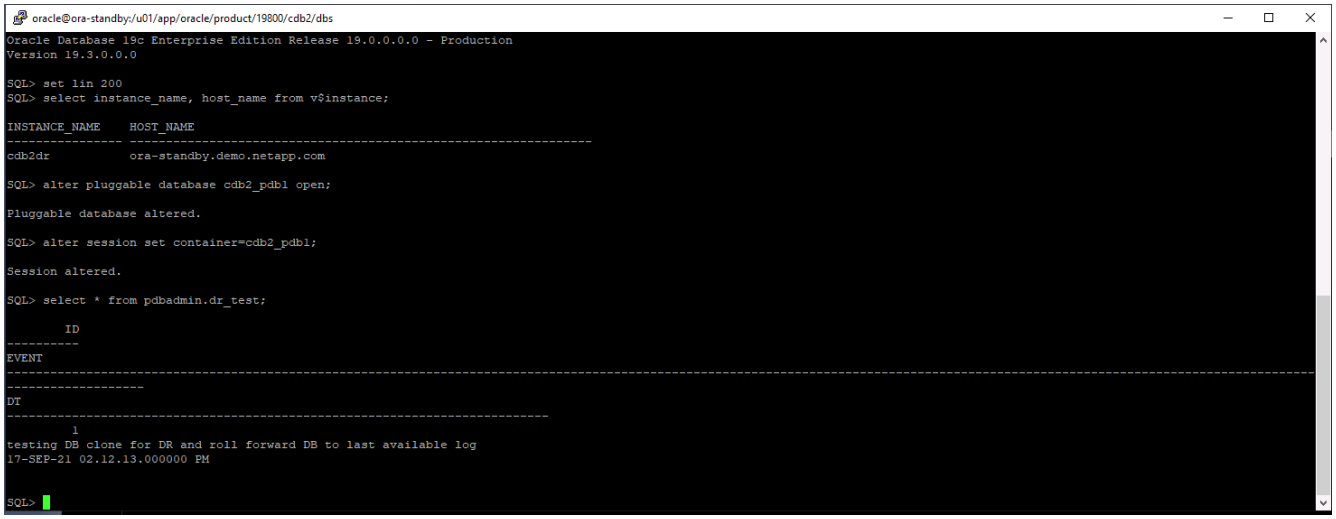
13. Résumé du clone DR.



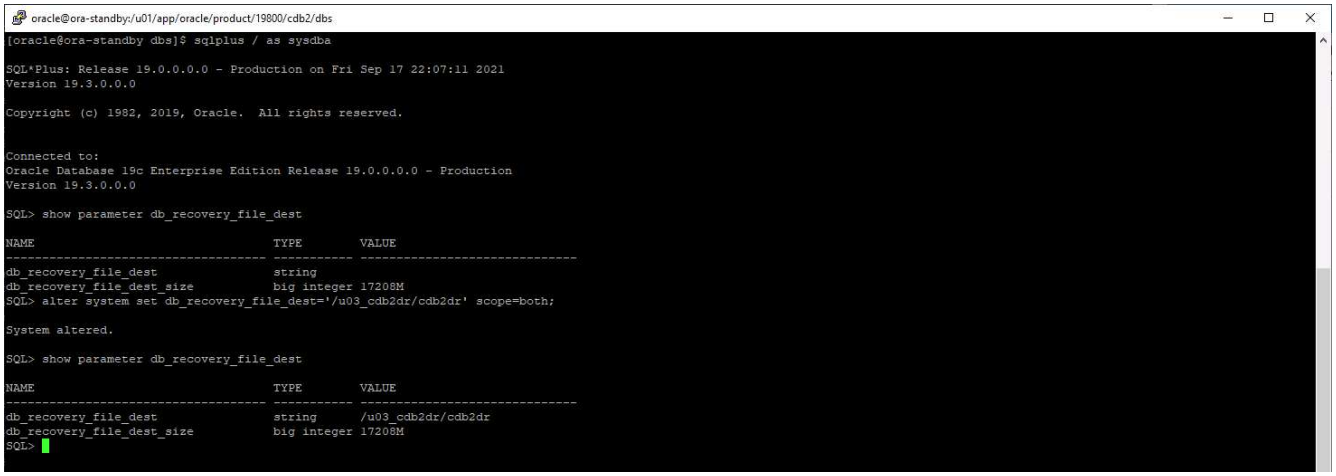
14. Les bases de données clonées sont enregistrées auprès de SnapCenter immédiatement après la fin du clonage et sont ensuite disponibles pour la protection de sauvegarde.

Validation et configuration du clone post-DR pour Oracle

1. Validez la dernière transaction de test qui a été vidée, répliquée et récupérée à l'emplacement DR dans le cloud.



2. Configurer la zone de récupération flash.

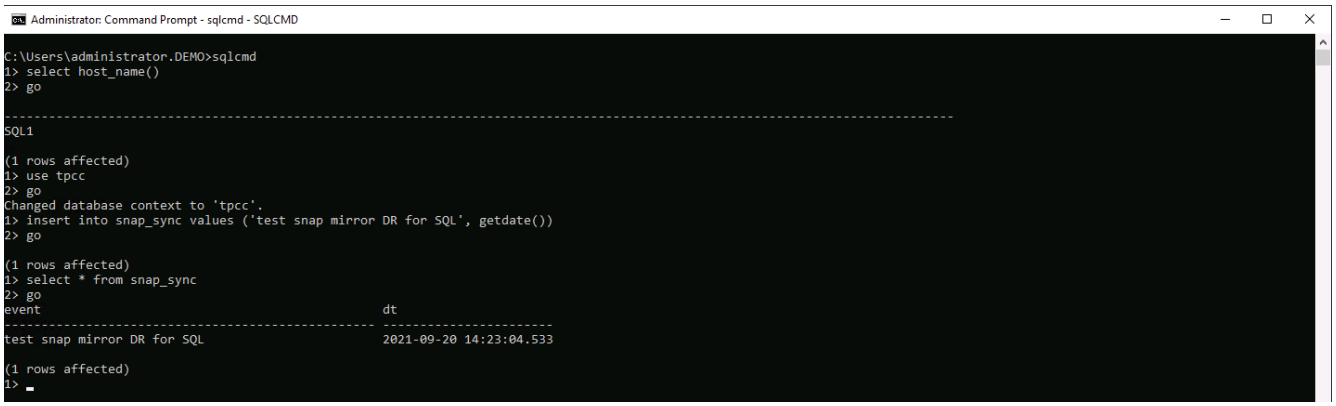


3. Configurez l'écouteur Oracle pour l'accès utilisateur.
4. Séparez le volume cloné du volume source répliqué.
5. Réplication inversée du cloud vers le serveur local et reconstruction du serveur de base de données local défaillant.

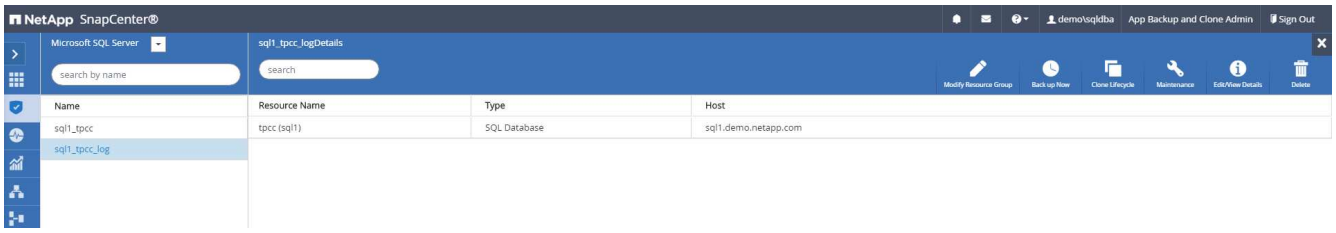
> La division du clone peut entraîner une utilisation temporaire de l'espace de stockage bien supérieure au fonctionnement normal. Cependant, une fois le serveur de base de données sur site reconstruit, de l'espace supplémentaire peut être libéré.

Cloner une base de données de production SQL sur site vers le cloud pour la reprise après sinistre

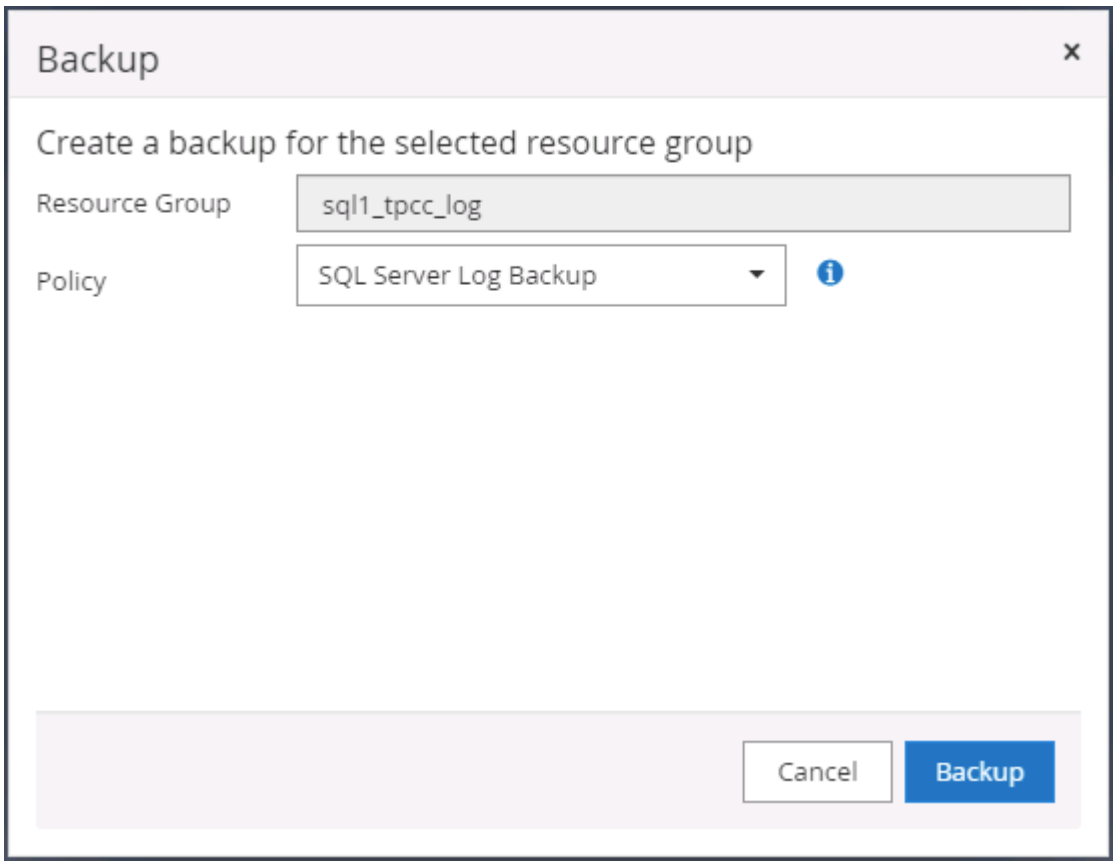
1. De même, pour valider que la récupération du clone SQL a été exécutée via le dernier journal disponible, nous avons créé une petite table de test et inséré une ligne. Les données de test seront récupérées après une récupération complète du dernier journal disponible.



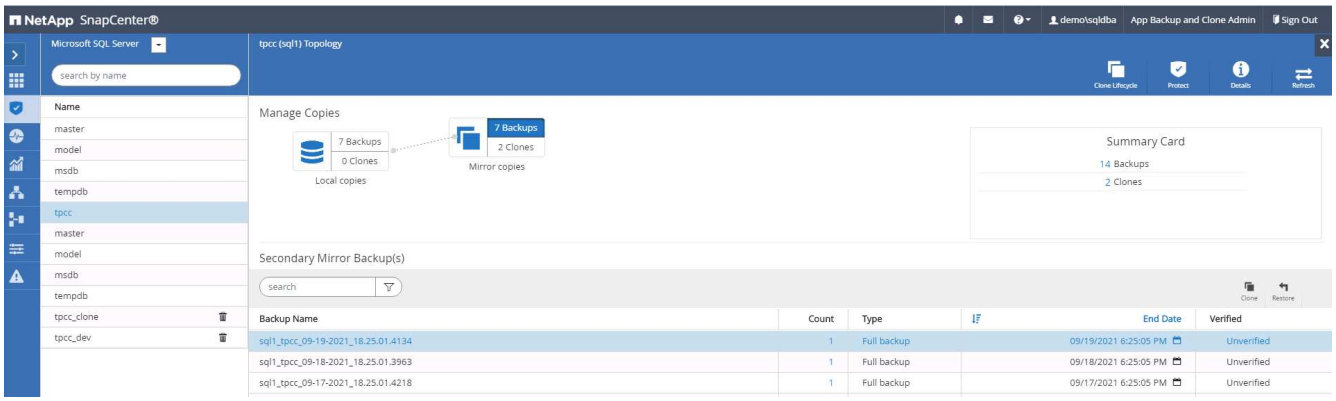
2. Connectez-vous à SnapCenter avec un ID utilisateur de gestion de base de données pour SQL Server. Accédez à l'onglet Ressources, qui affiche le groupe de ressources de protection SQL Server.



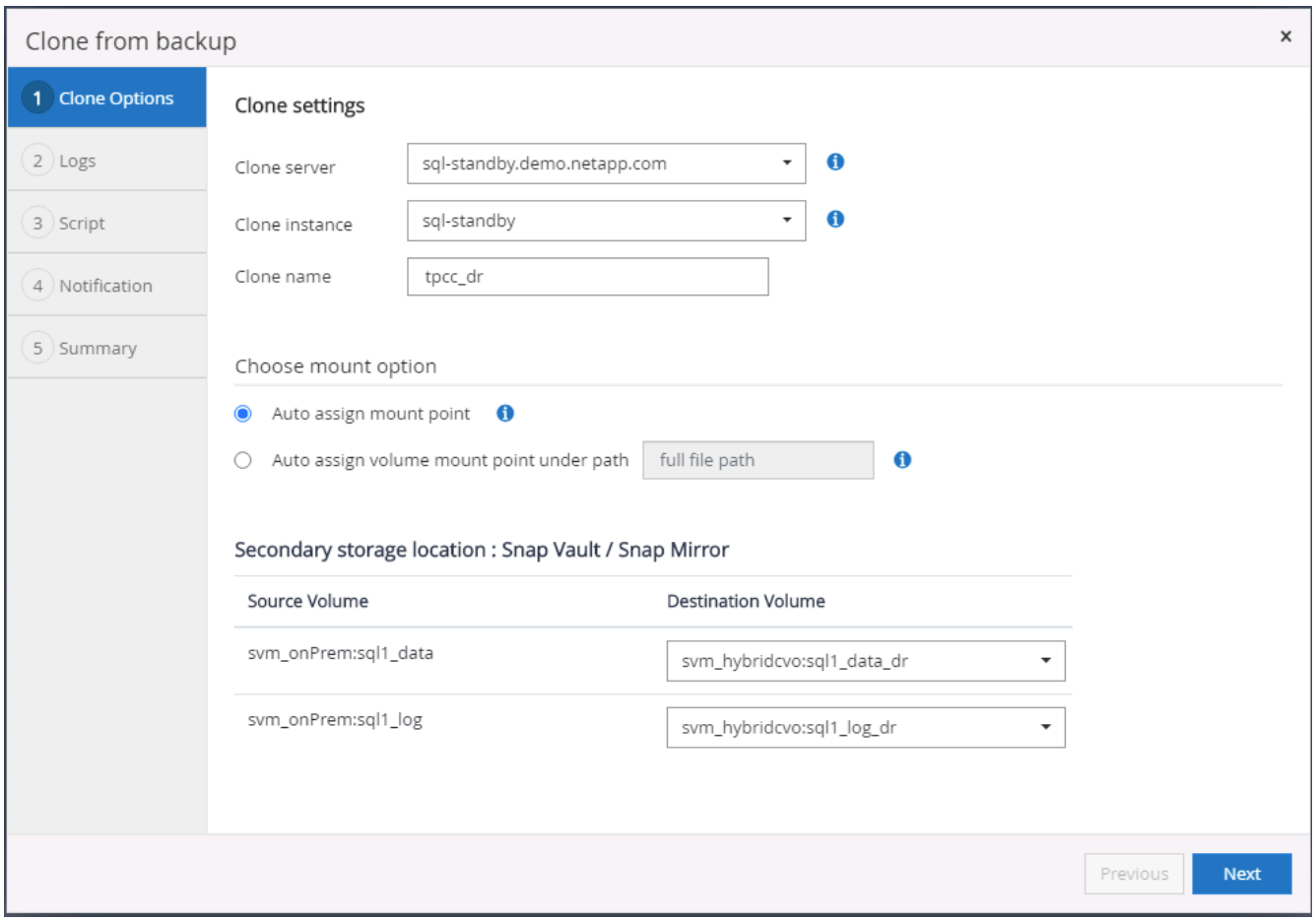
3. Exécutez manuellement une sauvegarde du journal pour vider la dernière transaction à répliquer vers le stockage secondaire dans le cloud public.



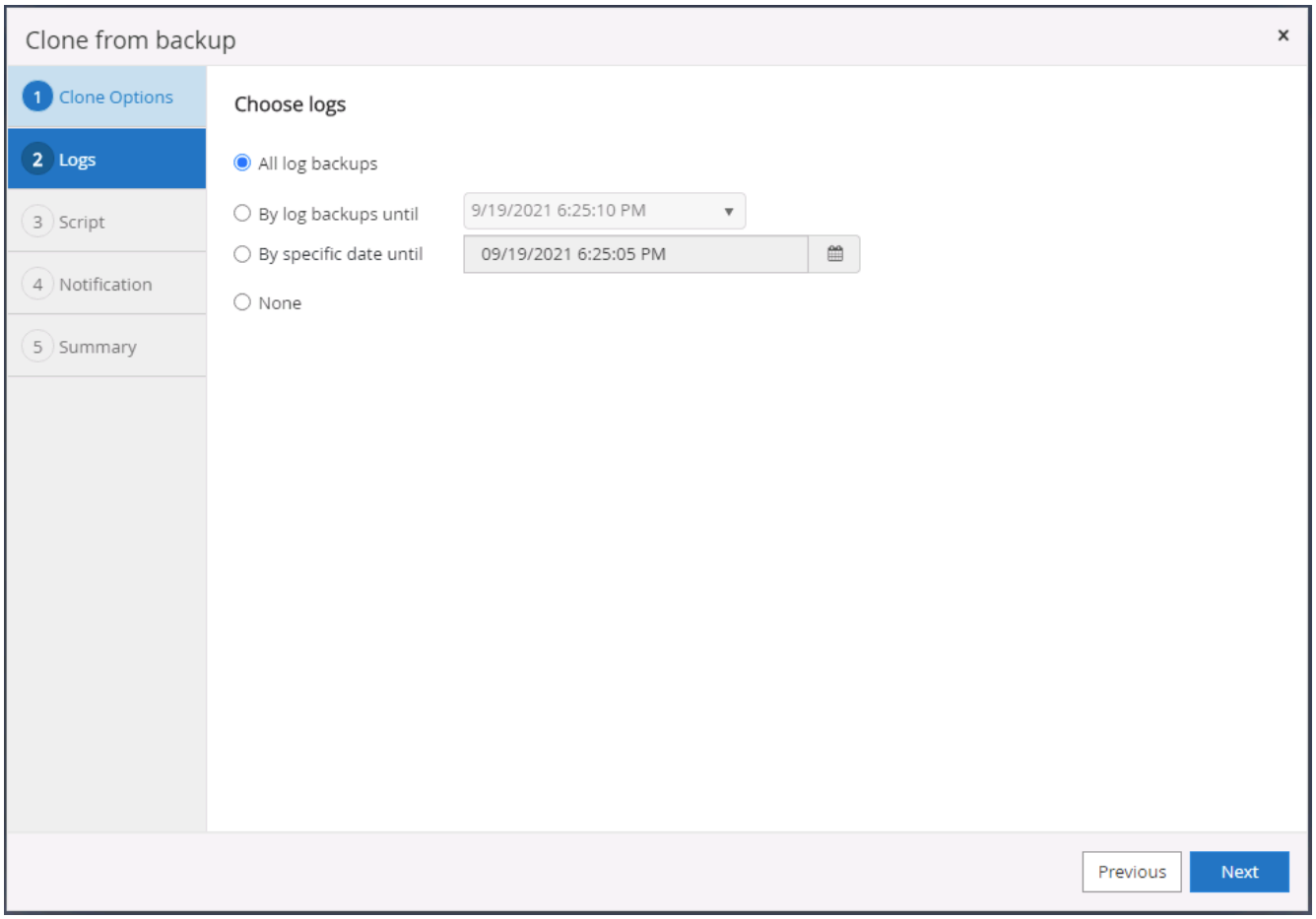
4. Sélectionnez la dernière sauvegarde complète de SQL Server pour le clone.



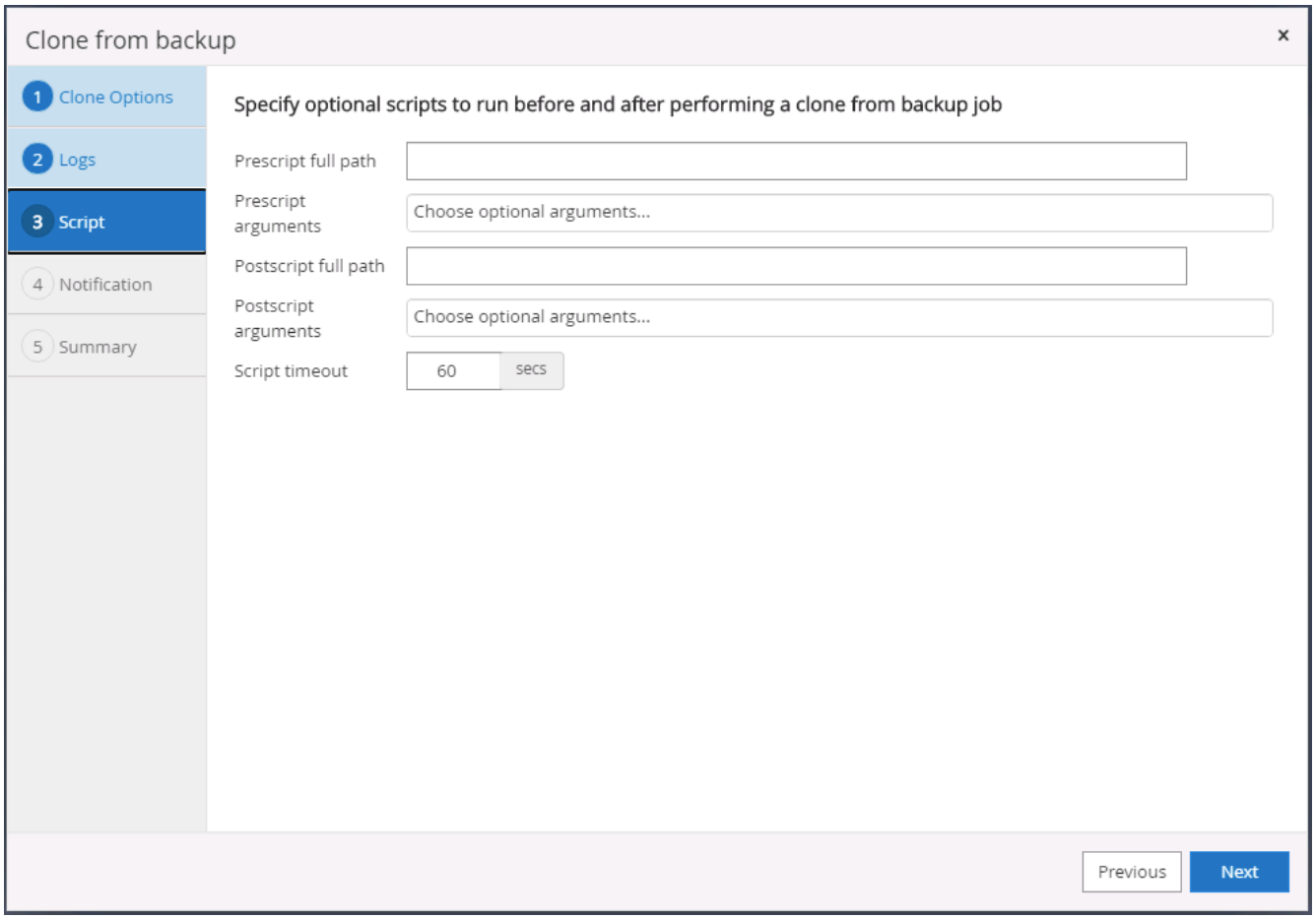
5. Définissez les paramètres de clonage tels que le serveur de clonage, l'instance de clonage, le nom de clonage et l'option de montage. L'emplacement de stockage secondaire où le clonage est effectué est renseigné automatiquement.



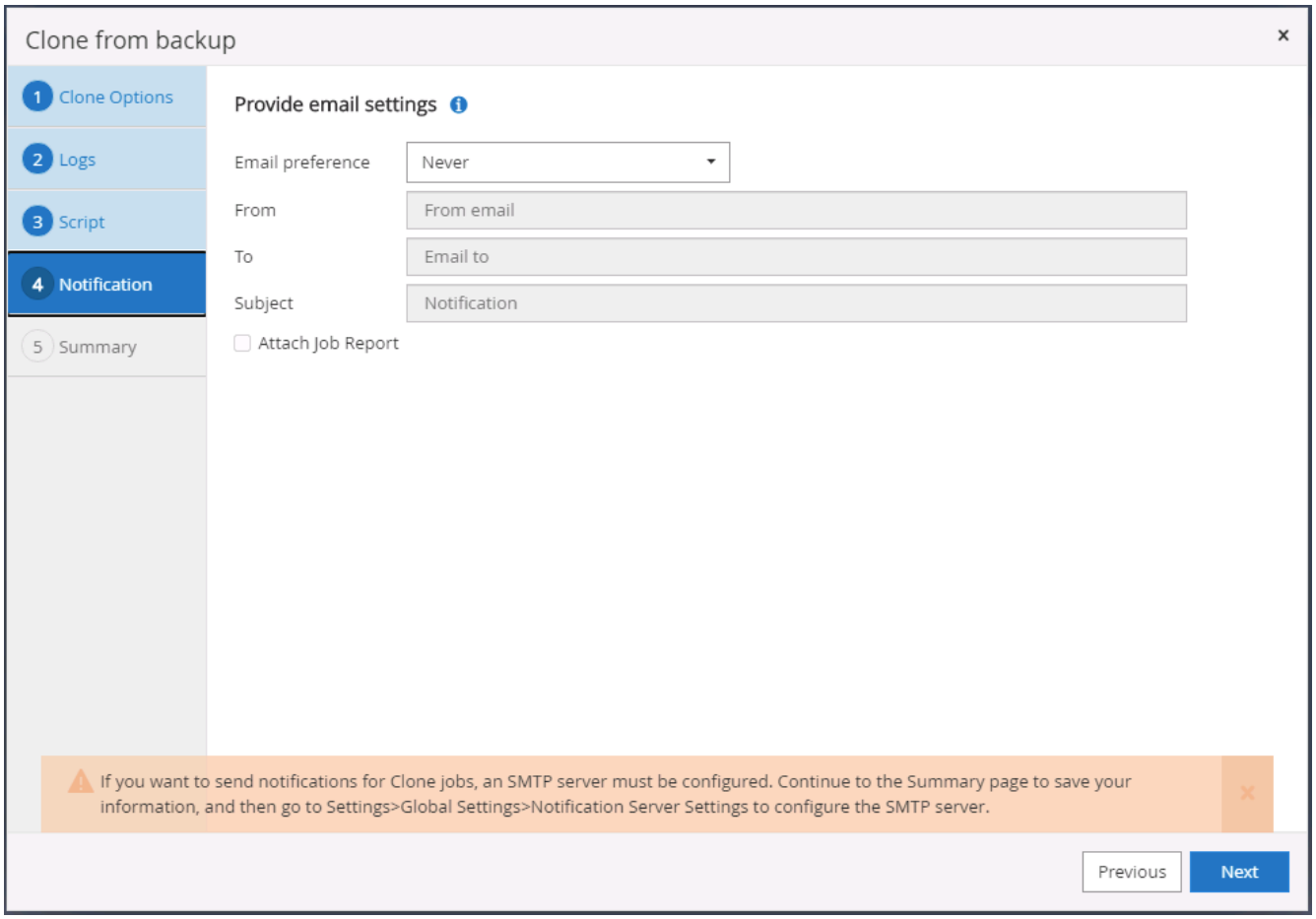
6. Sélectionnez toutes les sauvegardes de journaux à appliquer.



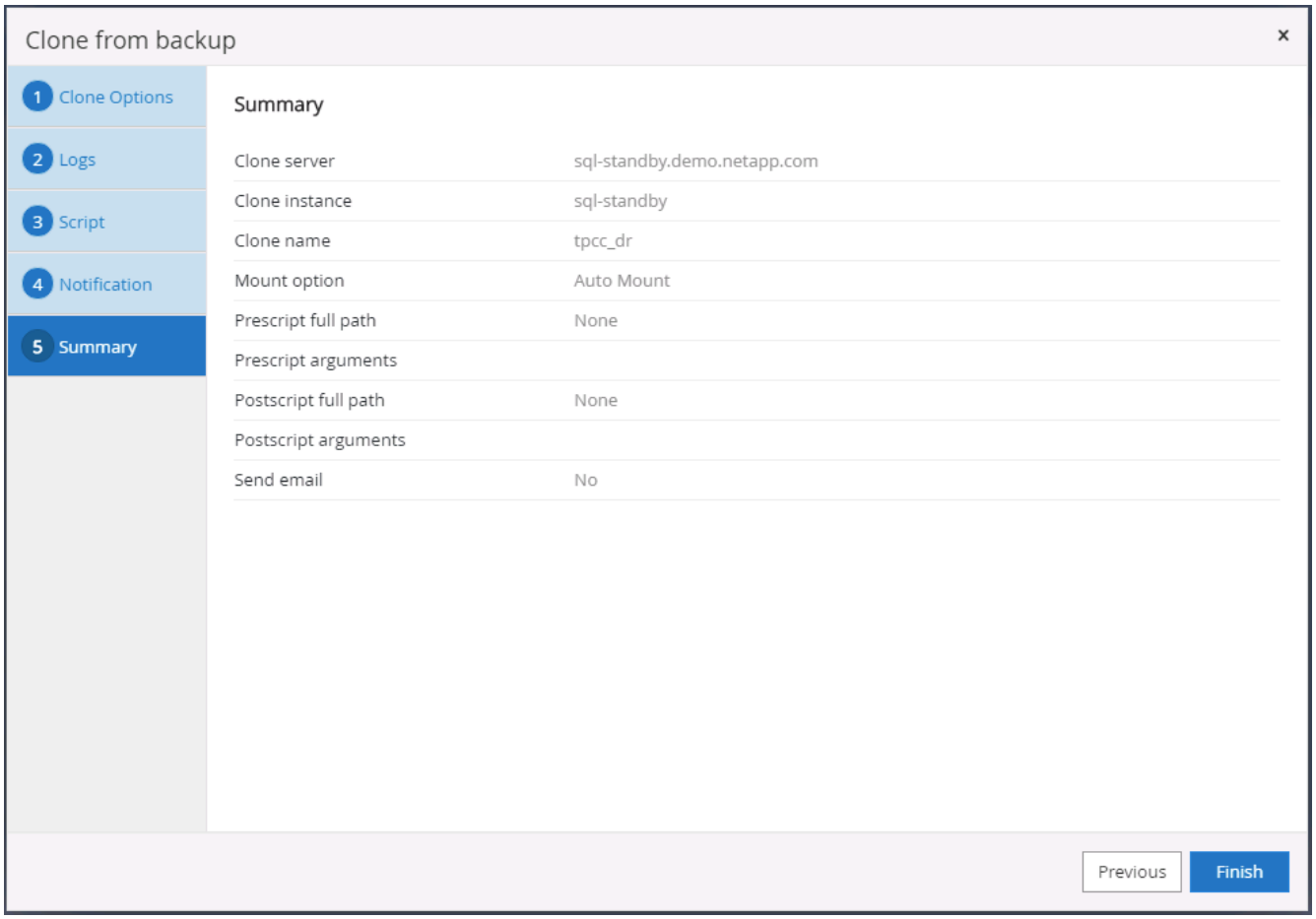
7. Spécifiez les scripts facultatifs à exécuter avant ou après le clonage.

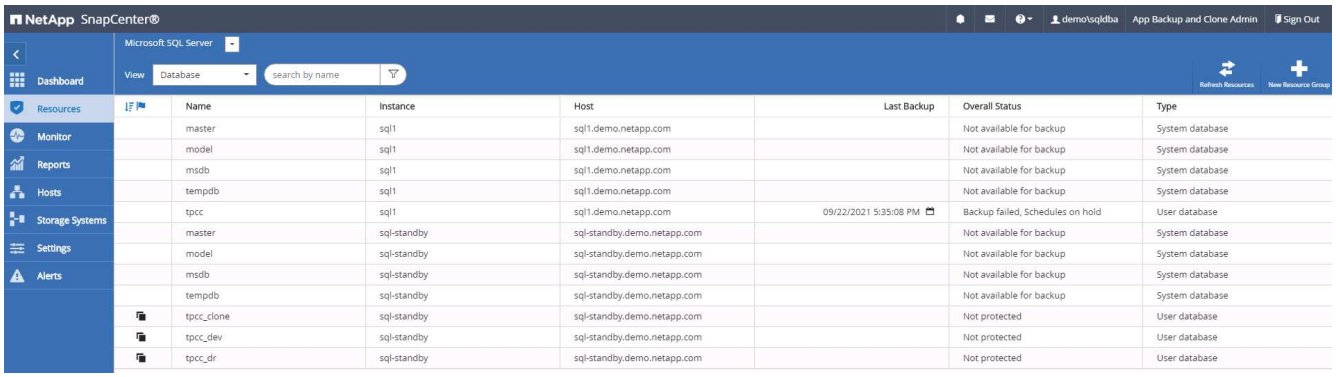


8. Spécifiez un serveur SMTP si une notification par e-mail est souhaitée.



9. Résumé du clone DR. Les bases de données clonées sont immédiatement enregistrées auprès de SnapCenter et disponibles pour la protection de sauvegarde.



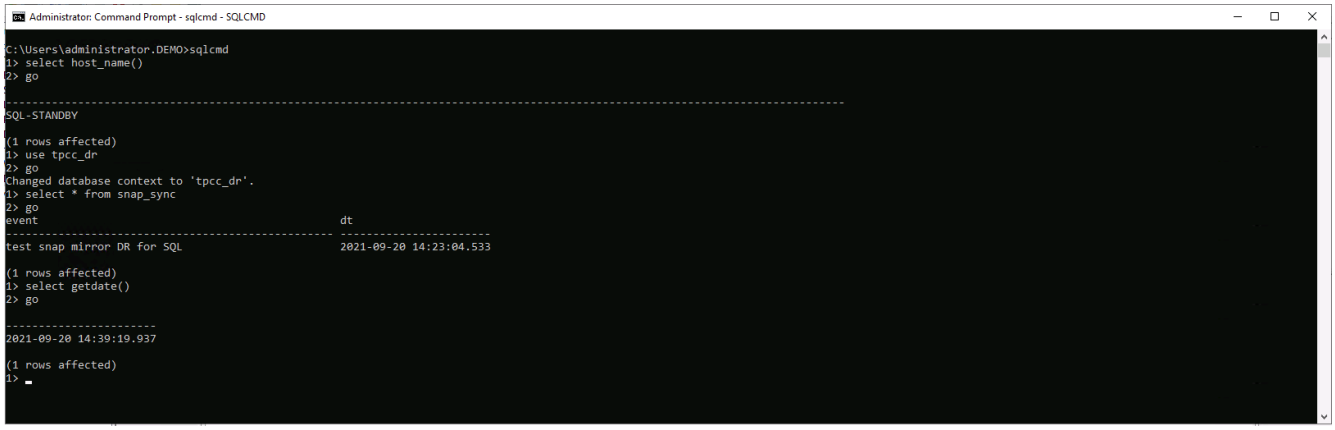


Validation et configuration du clone post-DR pour SQL

1. Surveiller l'état du travail de clonage.

2. Validez que la dernière transaction a été répliquée et récupérée avec tous les clones de fichiers journaux

et la récupération.



3. Configurez un nouveau répertoire de journaux SnapCenter sur le serveur DR pour la sauvegarde des journaux SQL Server.
4. Séparez le volume cloné du volume source répliqué.
5. Réplication inversée du cloud vers le serveur local et reconstruction du serveur de base de données local défaillant.

Où aller chercher de l’aide ?

Si vous avez besoin d’aide avec cette solution et ces cas d’utilisation, veuillez rejoindre le"Canal Slack d’assistance de la communauté NetApp Solution Automation" et recherchez le canal solution-automatisation pour poster vos questions ou demandes de renseignements.

Informations sur le copyright

Informations sur les marques commerciales