NetApp pour AWS/VMC

NetApp Solutions

NetApp
September 26, 2024

Sommaire

NetApp pour AWS/VMC

Fonctionnalités NetApp pour AWS VMC

En savoir plus sur les fonctionnalités que NetApp propose à AWS VMware Cloud (VMC) : de NetApp en tant que système de stockage connecté à l'invité ou un datastore NFS supplémentaire pour migrer les flux de travail, étendre/bursting sur le cloud, la sauvegarde/restauration et la reprise après incident.

Passez directement à la section du contenu souhaité en sélectionnant l'une des options suivantes :

- "Configuration de VMC dans AWS"
- "Options de stockage NetApp pour VMC"
- "Solutions clouds NetApp/VMware"

Configuration de VMC dans AWS

Comme sur site, il est essentiel de planifier un environnement de virtualisation basé sur le cloud pour créer des machines virtuelles et migrer vers un environnement prêt pour la production.

Cette section décrit comment configurer et gérer VMware Cloud sur AWS SDDC et l'utiliser en association avec les options de connexion de stockage NetApp disponibles.

Le stockage invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP à AWS VMC.

Le processus de configuration peut être divisé en plusieurs étapes :

- Déploiement et configuration de VMware Cloud pour AWS
- Connectez le cloud VMware à FSX ONTAP

Afficher les détails "Étapes de configuration pour VMC".

Options de stockage NetApp pour VMC

Le stockage NetApp peut être utilisé de plusieurs façons - soit en tant que connexion soit en tant que datastore NFS supplémentaire - dans AWS VMC.

Visitez le site "Options de stockage NetApp prises en charge" pour en savoir plus.

AWS prend en charge le stockage NetApp dans les configurations suivantes :

- FSX ONTAP en tant que stockage invité connecté
- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- FSX ONTAP en tant que datastore NFS supplémentaire

Afficher les détails "Options de stockage à connexion invité pour VMC". Afficher les détails "Options supplémentaires des datastores NFS pour VMC".

Cas d'utilisation de la solution

Avec les solutions clouds NetApp et VMware, vous pouvez facilement déployer de nombreux cas d'utilisation dans votre système AWS VMC. Des cas d'utilisation sont définis pour chaque domaine de cloud défini par VMware :

- Protection (inclut la reprise après incident et la sauvegarde/restauration)
- Extension
- Migrer

"Découvrez les solutions NetApp pour AWS VMC"

Protection des workloads sur AWS/VMC

Tr-4931 : reprise après incident avec VMware Cloud sur Amazon Web Services et Guest Connect

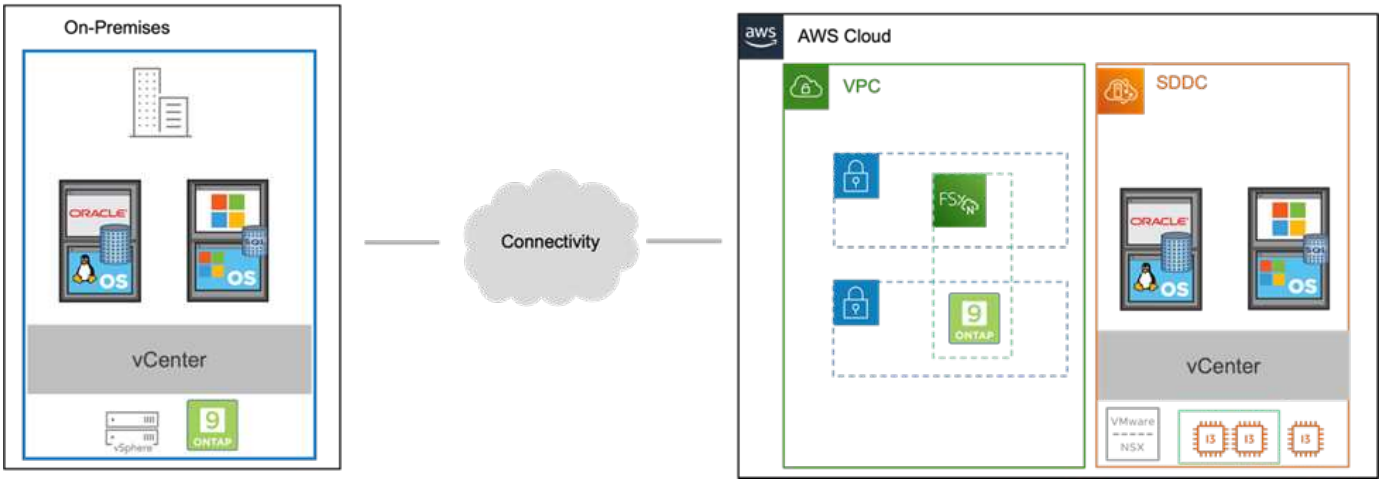
Un plan et un environnement de reprise après incident éprouvés sont essentiels pour les entreprises pour garantir la restauration rapide des applications stratégiques en cas de panne majeure. Cette solution a été axée sur une démonstration de cas d'utilisation de reprise après incident en mettant l'accent sur les technologies VMware et NetApp, à la fois sur site et avec VMware Cloud sur AWS.

Auteurs : Chris Reno, Josh Powell, Suresh Thoppay - Ingénierie de solutions NetApp

Présentation

NetApp dispose d'une longue expérience de l'intégration avec VMware, comme le prouvent les dizaines de milliers de clients qui ont choisi NetApp comme partenaire de stockage pour leur environnement virtualisé. Cette intégration continue également avec les options connectées à l'invité dans le cloud et les intégrations récentes avec les datastores NFS. Cette solution est axée sur l'utilisation communément appelée stockage connecté à l'invité.

Dans le cas d'un stockage connecté à l'invité, le VMDK invité est déployé sur un datastore provisionné par VMware. Les données d'application sont hébergées sur iSCSI ou NFS et mappées directement à la machine virtuelle. Les applications Oracle et MS SQL sont utilisées pour démontrer un scénario de reprise sur incident, comme illustré dans la figure suivante.



Hypothèses, conditions requises et présentation des composants

Avant de déployer cette solution, vérifiez la présentation des composants, les conditions préalables requises pour déployer la solution et les hypothèses fournies pour documenter cette solution.

"Besoins en solution DR, pré-requis et planification"

Effectuer une reprise après incident avec SnapCenter

Dans cette solution, SnapCenter fournit des snapshots cohérents au niveau des applications pour les données des applications SQL Server et Oracle. Combinée à la technologie SnapMirror, cette configuration assure une réplication des données ultra-rapide entre nos clusters AFF et FSX ONTAP sur site. De plus, Veeam Backup & Replication offre des fonctionnalités de sauvegarde et de restauration pour nos machines virtuelles.

Dans cette section, nous allons parler de la configuration de SnapCenter, SnapMirror et Veeam pour la sauvegarde et la restauration.

Les sections suivantes couvrent la configuration et les étapes nécessaires pour effectuer le basculement sur le site secondaire :

Configurez des relations SnapMirror et des planifications de conservation

SnapCenter peut mettre à jour les relations SnapMirror dans le système de stockage primaire (primaire > miroir) et vers des systèmes de stockage secondaires (primaire > archivage sécurisé) pour l'archivage et la conservation à long terme. Pour ce faire, vous devez établir et initialiser une relation de réplication des données entre un volume de destination et un volume source à l'aide de SnapMirror.

Les systèmes ONTAP source et destination doivent se trouver dans des réseaux qui sont peering via Amazon VPC, une passerelle de transit, AWS Direct Connect ou un VPN AWS.

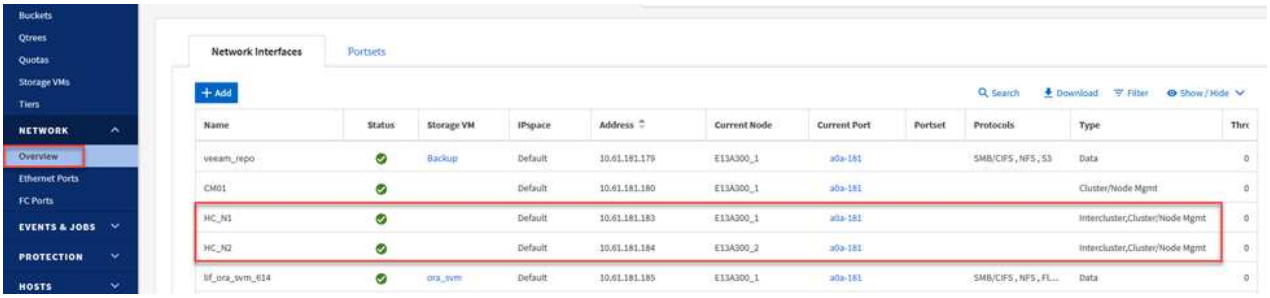
Les étapes suivantes sont requises pour la configuration des relations SnapMirror entre un système ONTAP sur site et FSX ONTAP :

Reportez-vous à la "FSX pour ONTAP – Guide de l'utilisateur ONTAP" Pour plus d'informations sur la création de relations SnapMirror avec FSX.

Enregistrer les interfaces logiques intercluster source et destination

Pour le système ONTAP source résidant sur site, vous pouvez récupérer les informations LIF inter-cluster depuis System Manager ou depuis l'interface de ligne de commandes.

1. Dans ONTAP System Manager, accédez à la page Network Overview et récupérez les adresses IP de type intercluster configurées pour communiquer avec le VPC AWS où FSX est installé.



2. Pour récupérer les adresses IP intercluster pour FSX, connectez-vous à l'interface de ligne de commande et exécutez la commande suivante :

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

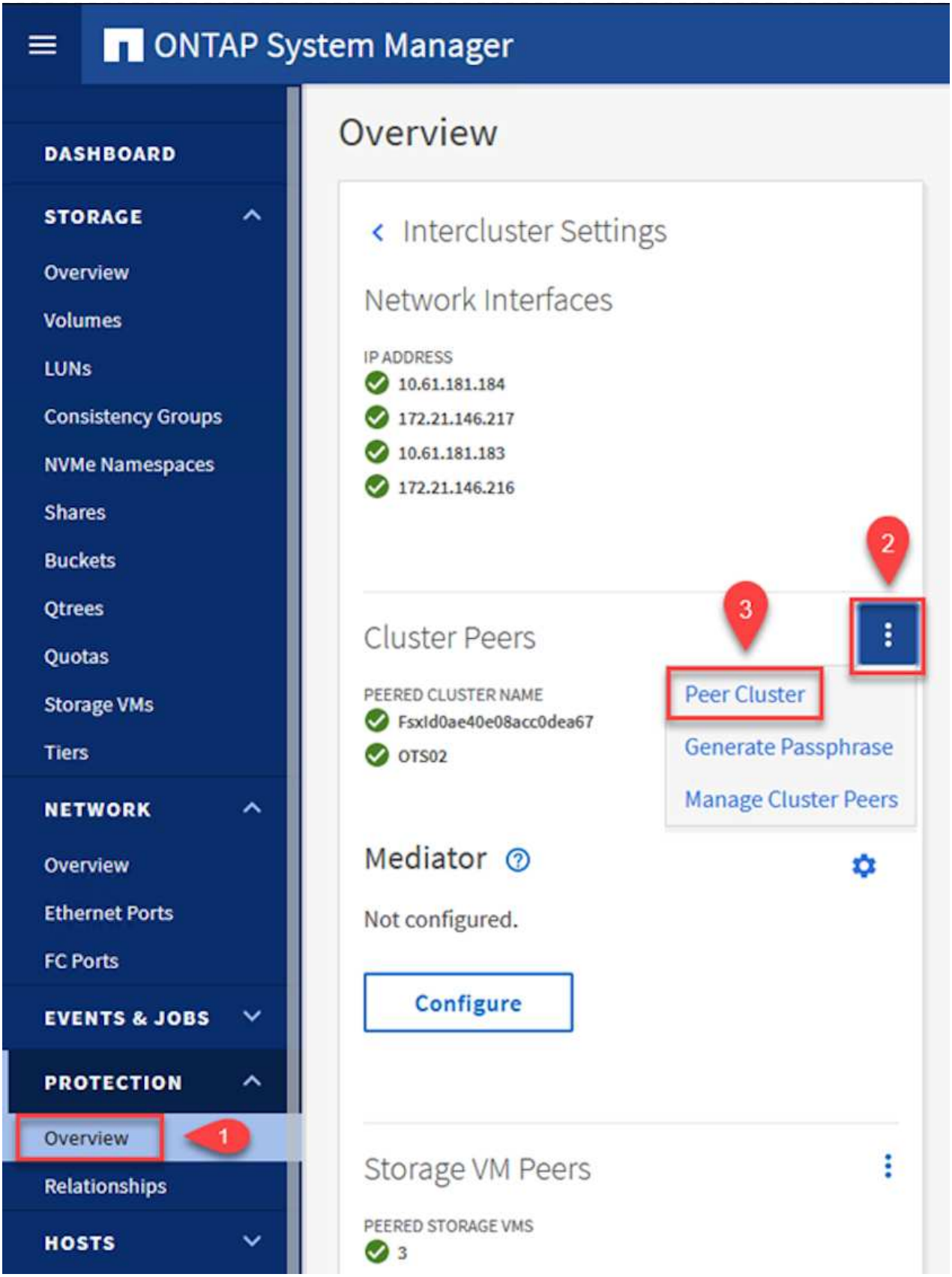
Établir le peering de cluster entre ONTAP et FSX

Pour établir le peering de cluster entre clusters ONTAP, une phrase secrète unique saisie au niveau du cluster ONTAP à l'origine doit être confirmée dans l'autre cluster.

1. Configurez le peering sur le cluster FSX de destination à l'aide de l' `cluster peer create` commande. Lorsque vous y êtes invité, saisissez une phrase secrète unique utilisée ultérieurement sur le cluster source pour finaliser le processus de création.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. Sur le cluster source, vous pouvez établir la relation de pairs de cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes. Dans ONTAP System Manager, accédez à protection > Présentation et sélectionnez Peer Cluster.

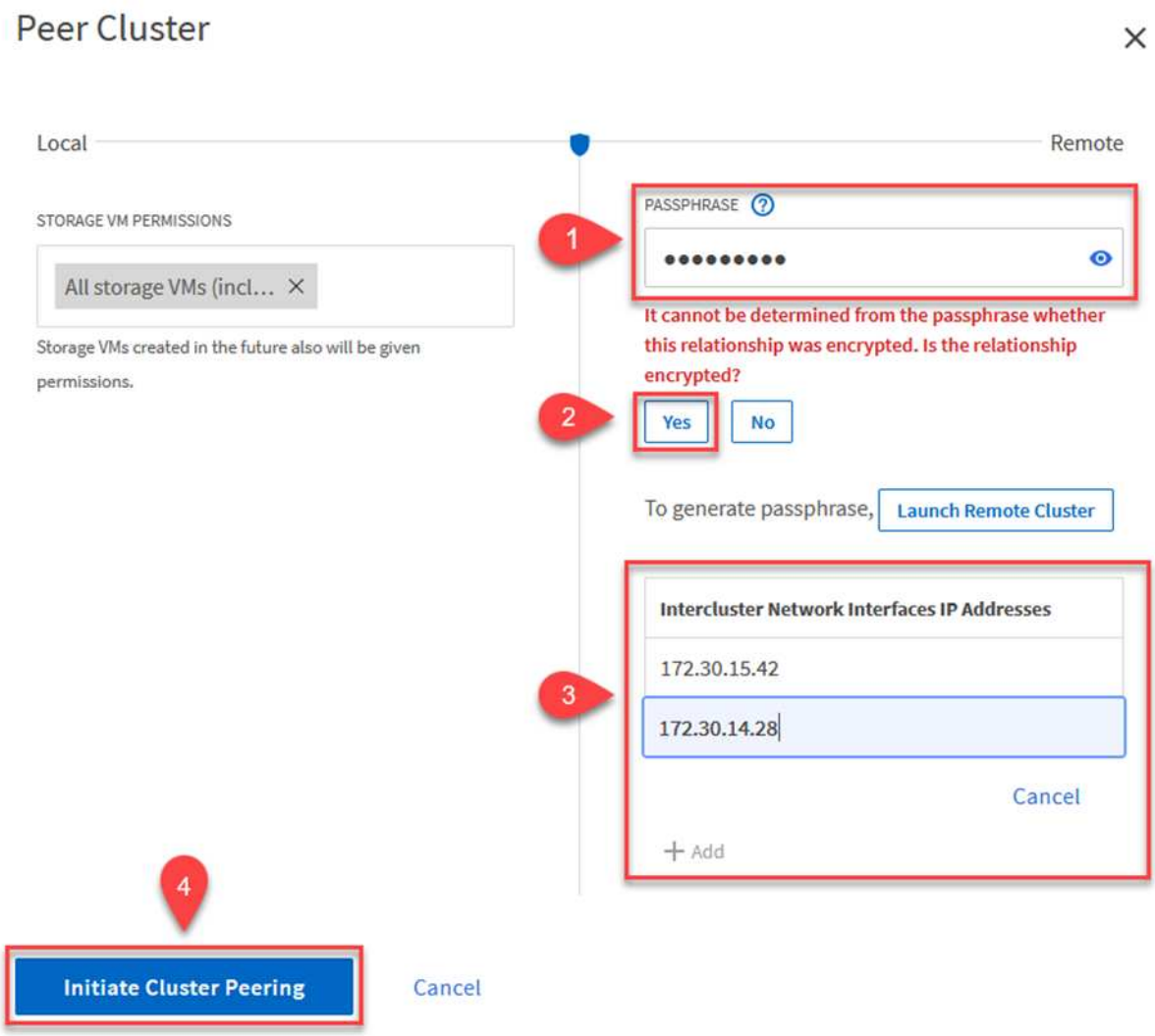


3. Dans la boîte de dialogue Peer Cluster, saisissez les informations requises :
   a. Saisissez la phrase de passe utilisée pour établir la relation de cluster homologue sur le cluster FSX de destination.

b. Sélectionnez `Yes` pour établir une relation chiffrée.

c. Entrer les adresses IP du LIF intercluster du cluster FSX de destination.

d. Cliquez sur initier le peering de cluster pour finaliser le processus.



4. Vérifiez l'état de la relation cluster peer à partir du cluster FSX avec la commande suivante :

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

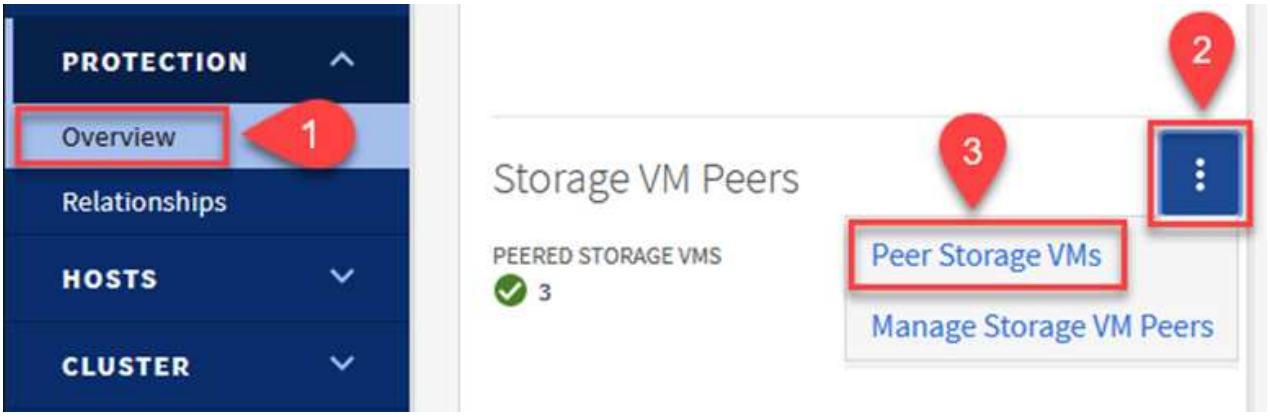
Établir une relation de peering de SVM

L'étape suivante consiste à configurer une relation de SVM entre les machines virtuelles de stockage de destination et source qui contiennent les volumes qui seront dans les relations SnapMirror.

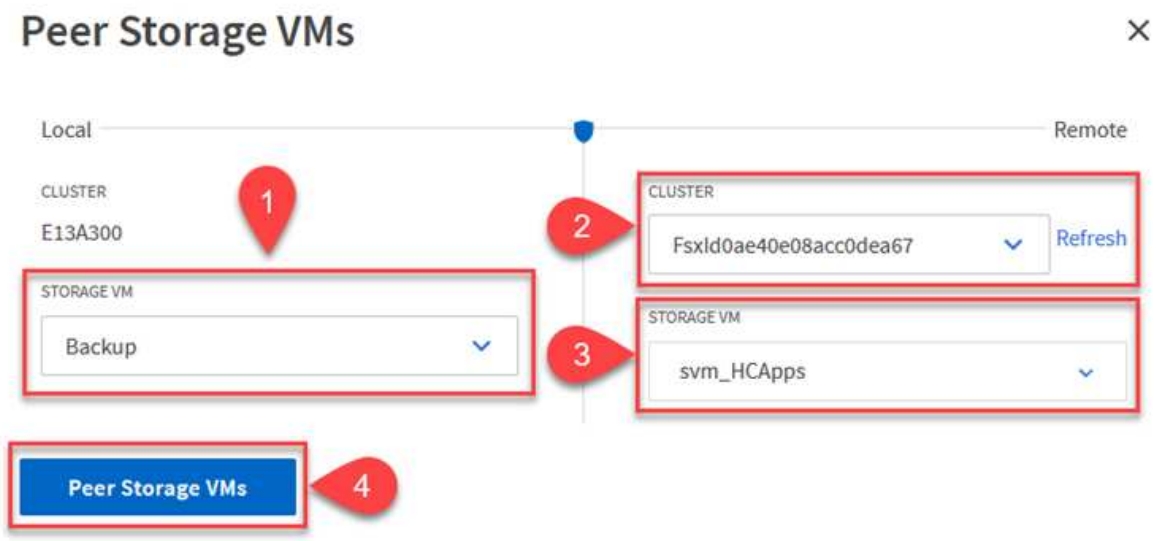
1. Depuis le cluster FSX source, utiliser la commande suivante depuis l'interface de ligne de commande afin de créer la relation SVM peer :

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Depuis le cluster ONTAP source, acceptez la relation de peering avec ONTAP System Manager ou l'interface de ligne de commandes.
3. Dans ONTAP System Manager, accédez à protection > Présentation et sélectionnez des VM de stockage homologues sous les pairs de machines virtuelles de stockage.



4. Dans la boîte de dialogue de la VM de stockage homologue, remplissez les champs requis :
   - La VM de stockage source
   - Cluster destination
   - L'VM de stockage de destination



5. Cliquez sur Peer Storage VM pour terminer le processus de peering de SVM.

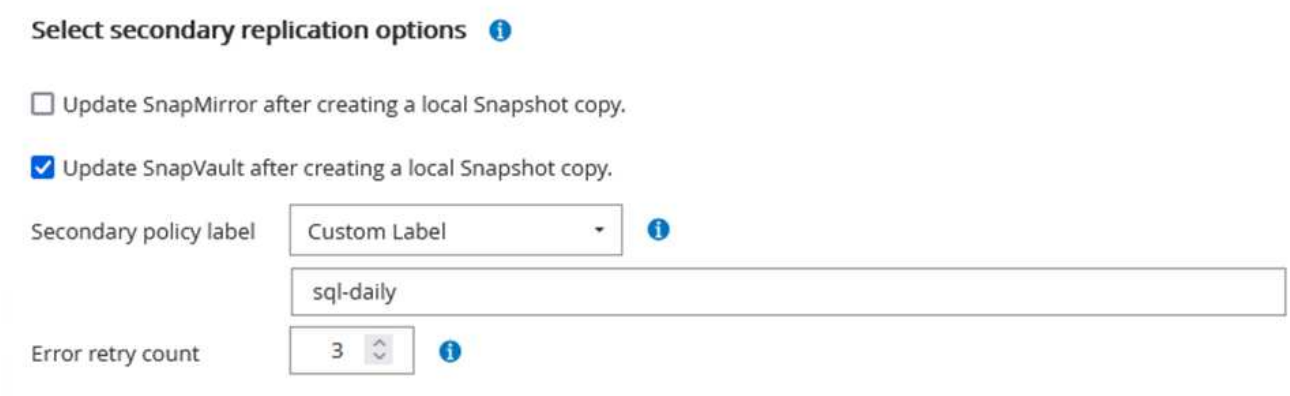
Création d'une règle de conservation des snapshots

SnapCenter gère les planifications de conservation pour les sauvegardes qui existent sous forme de copies Snapshot sur le système de stockage primaire. Ceci est établi lors de la création d'une règle dans SnapCenter. SnapCenter ne gère pas de stratégies de conservation pour les sauvegardes conservées sur des systèmes de stockage secondaires. Ces règles sont gérées séparément via une règle SnapMirror créée sur le cluster FSX secondaire et associée aux volumes de destination faisant partie d'une relation SnapMirror avec le volume source.

Lors de la création d'une règle SnapCenter, vous avez la possibilité de spécifier une étiquette de règle secondaire ajoutée au label SnapMirror de chaque Snapshot généré lors de la création d'une sauvegarde SnapCenter.

Sur le stockage secondaire, ces étiquettes sont mises en correspondance avec les règles de règle associées au volume de destination pour assurer la conservation des snapshots.

L'exemple suivant montre une étiquette SnapMirror présente sur tous les snapshots générés dans le cadre d'une règle utilisée pour les sauvegardes quotidiennes de notre base de données SQL Server et des volumes des journaux.



Pour plus d'informations sur la création de stratégies SnapCenter pour une base de données SQL Server, reportez-vous au "Documentation SnapCenter".

Vous devez d'abord créer une règle SnapMirror avec des règles qui imposent le nombre de copies Snapshot à conserver.

1. Création de la règle SnapMirror sur le cluster FSX

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Ajoutez des règles à la règle avec des étiquettes SnapMirror qui correspondent aux étiquettes de règles secondaires spécifiées dans les règles de SnapCenter.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Le script suivant fournit un exemple de règle qui peut être ajoutée à une règle :

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Créer des règles supplémentaires pour chaque étiquette SnapMirror et le nombre de snapshots à conserver (période de conservation).

Créer des volumes de destination

Pour créer un volume de destination sur FSX qui sera le destinataire des copies snapshot à partir de nos volumes source, exécutez la commande suivante sur FSX ONTAP :

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Création des relations SnapMirror entre les volumes source et de destination

Pour créer une relation SnapMirror entre un volume source et un volume de destination, exécutez la commande suivante sur FSX ONTAP :

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Initialiser les relations SnapMirror

Initialiser la relation SnapMirror Ce processus lance un nouveau snapshot généré à partir du volume source et le copie vers le volume de destination.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Déploiement et configuration de Windows SnapCenter Server sur site

Déploiement de Windows SnapCenter Server sur site

Cette solution utilise NetApp SnapCenter pour effectuer des sauvegardes cohérentes au niveau des applications de bases de données SQL Server et Oracle. Associé à Veeam Backup & Replication pour la sauvegarde des VMDK de machines virtuelles, cette solution assure une reprise après incident complète pour les data centers sur site et dans le cloud.

Le logiciel SnapCenter est disponible sur le site du support NetApp et peut être installé sur les systèmes Microsoft Windows résidant dans un domaine ou un groupe de travail. Un guide de planification détaillé et des instructions d'installation sont disponibles sur le "Centre de documentation NetApp".

Le logiciel SnapCenter est disponible à l'adresse "ce lien".

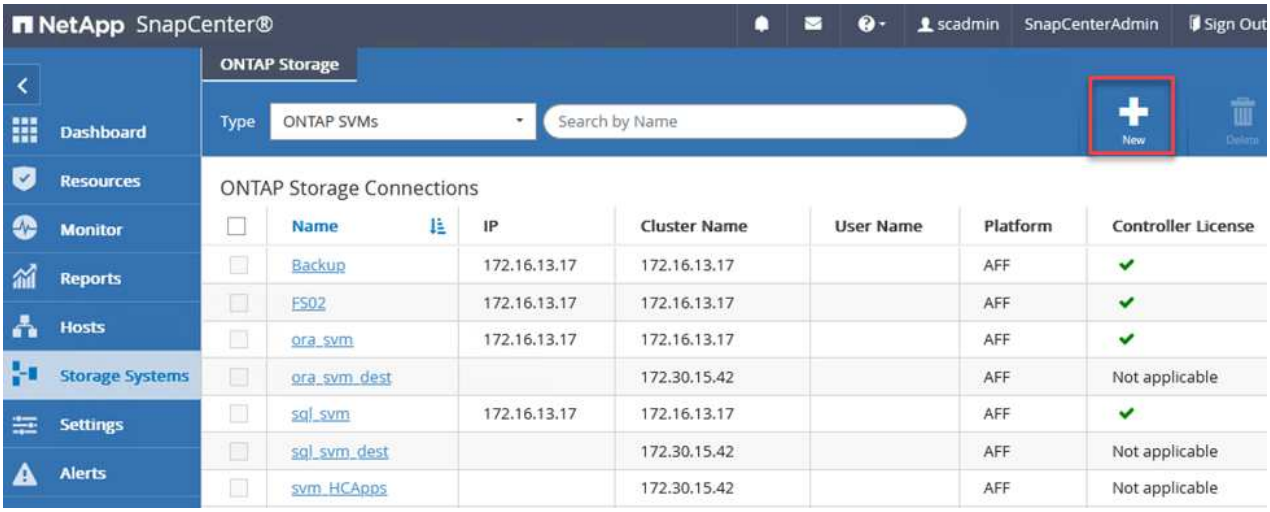
Une fois installé, vous pouvez accéder à la console SnapCenter à partir d'un navigateur Web en utilisant *https://Virtual_Cluster_IP_or_FQDN:8146*.

Une fois connecté à la console, vous devez configurer SnapCenter pour la sauvegarde des bases de données SQL Server et Oracle.

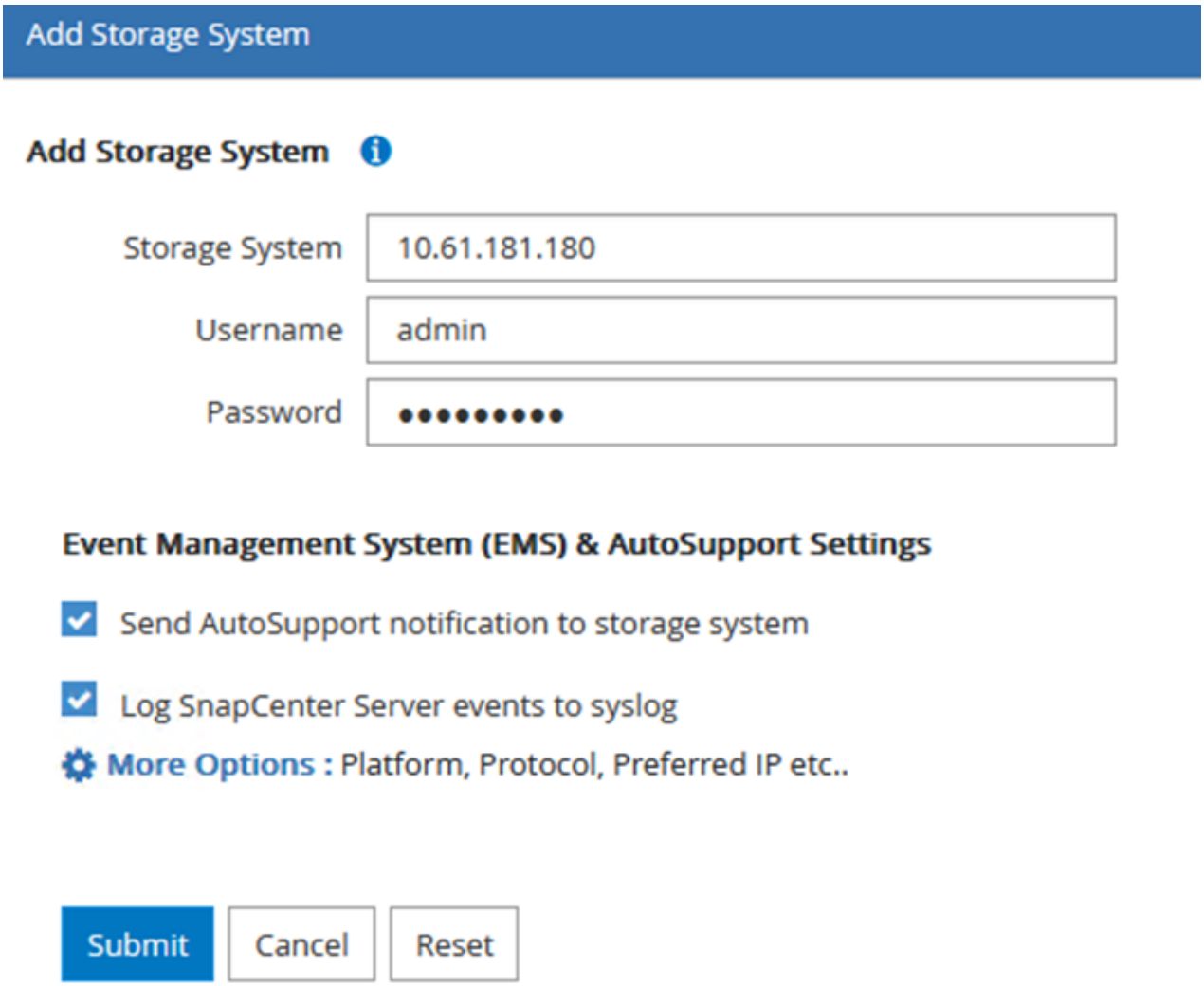
Ajout de contrôleurs de stockage à SnapCenter

Pour ajouter des contrôleurs de stockage à SnapCenter, procédez comme suit :

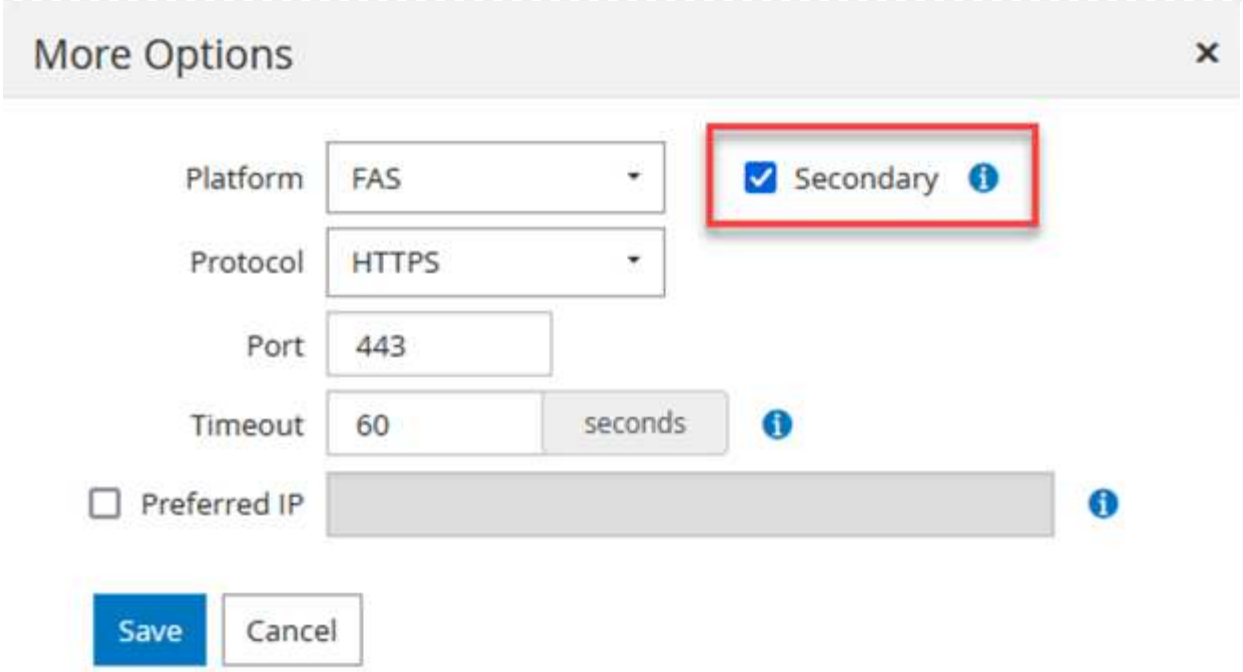
1. Dans le menu de gauche, sélectionnez systèmes de stockage, puis cliquez sur Nouveau pour lancer le processus d'ajout de vos contrôleurs de stockage à SnapCenter.



2. Dans la boîte de dialogue Ajouter un système de stockage, ajoutez l'adresse IP de gestion du cluster ONTAP local sur site, ainsi que le nom d'utilisateur et le mot de passe. Cliquez ensuite sur Submit pour lancer la détection du système de stockage.



3. Répétez cette procédure pour ajouter le système FSX ONTAP à SnapCenter. Dans ce cas, sélectionnez plus d'options en bas de la fenêtre Add Storage System (Ajouter un système de stockage), puis cliquez sur la case à cocher for Secondary afin de désigner le système FSX comme système de stockage secondaire mis à jour avec les copies SnapMirror ou nos snapshots de sauvegarde primaires.

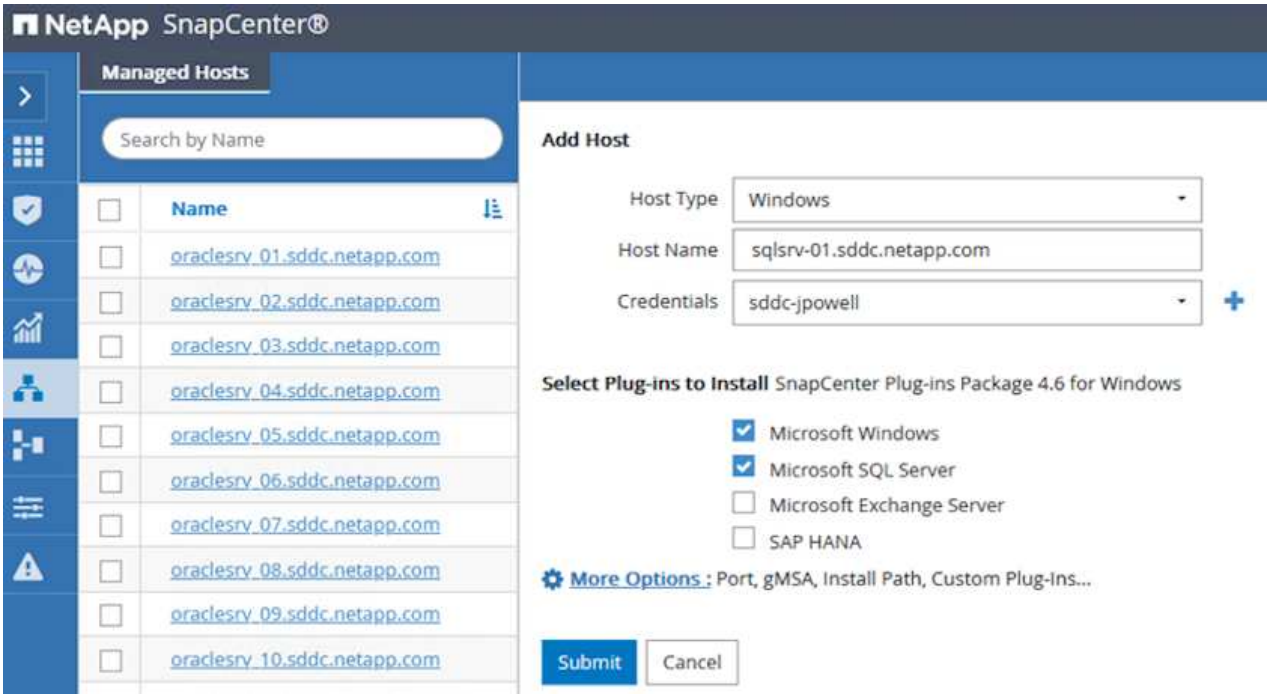


Pour plus d'informations sur l'ajout de systèmes de stockage à SnapCenter, reportez-vous à la documentation à l'adresse "ce lien".

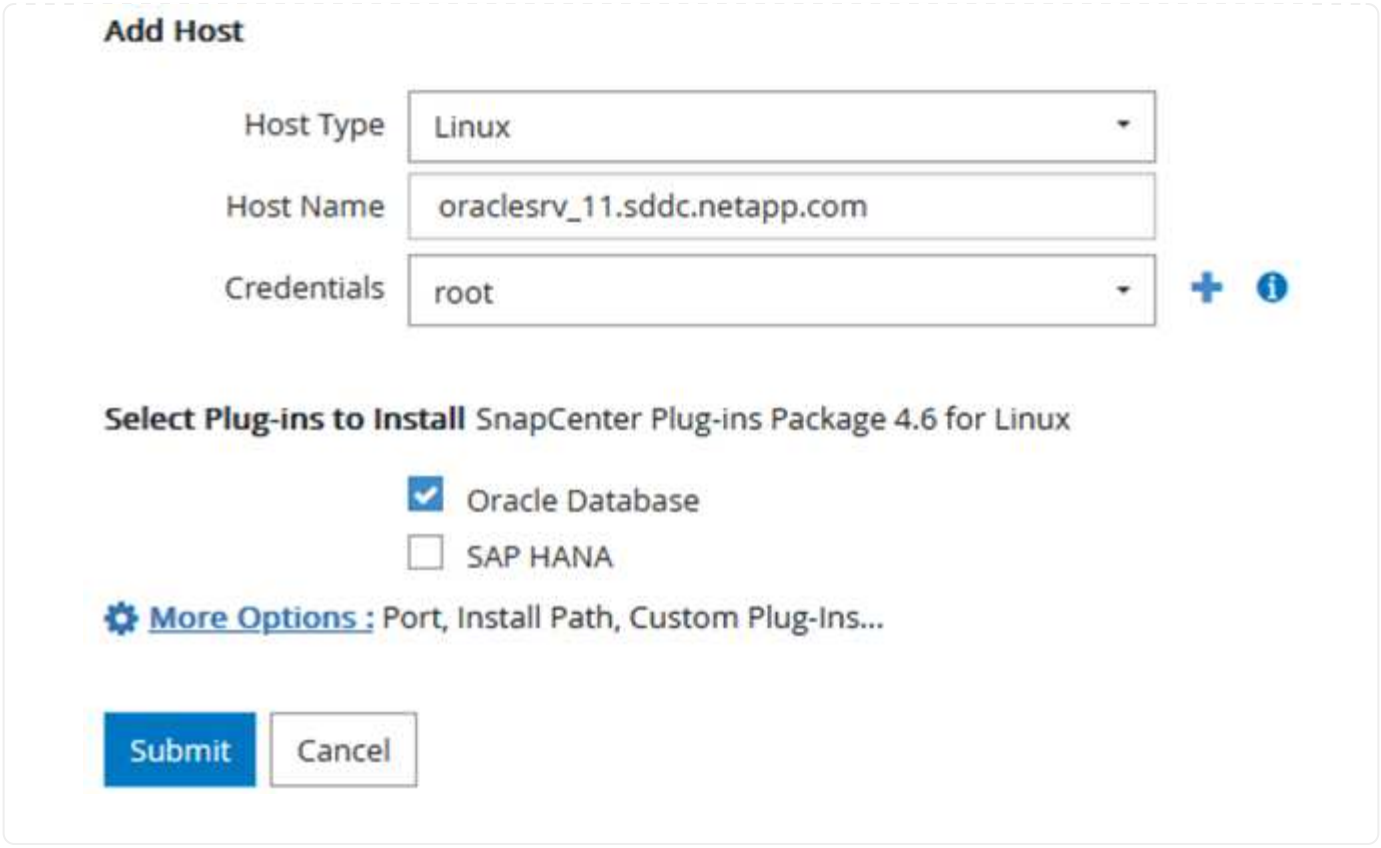
Ajouter des hôtes à SnapCenter

L'étape suivante consiste à ajouter des serveurs d'applications hôtes à SnapCenter. Le processus est similaire pour SQL Server et Oracle.

1. Dans le menu de gauche, sélectionnez hosts, puis cliquez sur Add pour lancer le processus d'ajout de contrôleurs de stockage à SnapCenter.
2. Dans la fenêtre Ajouter des hôtes, ajoutez le type d'hôte, le nom d'hôte et les informations d'identification du système hôte. Sélectionnez le type de plug-in. Pour SQL Server, sélectionnez le plug-in Microsoft Windows et Microsoft SQL Server.



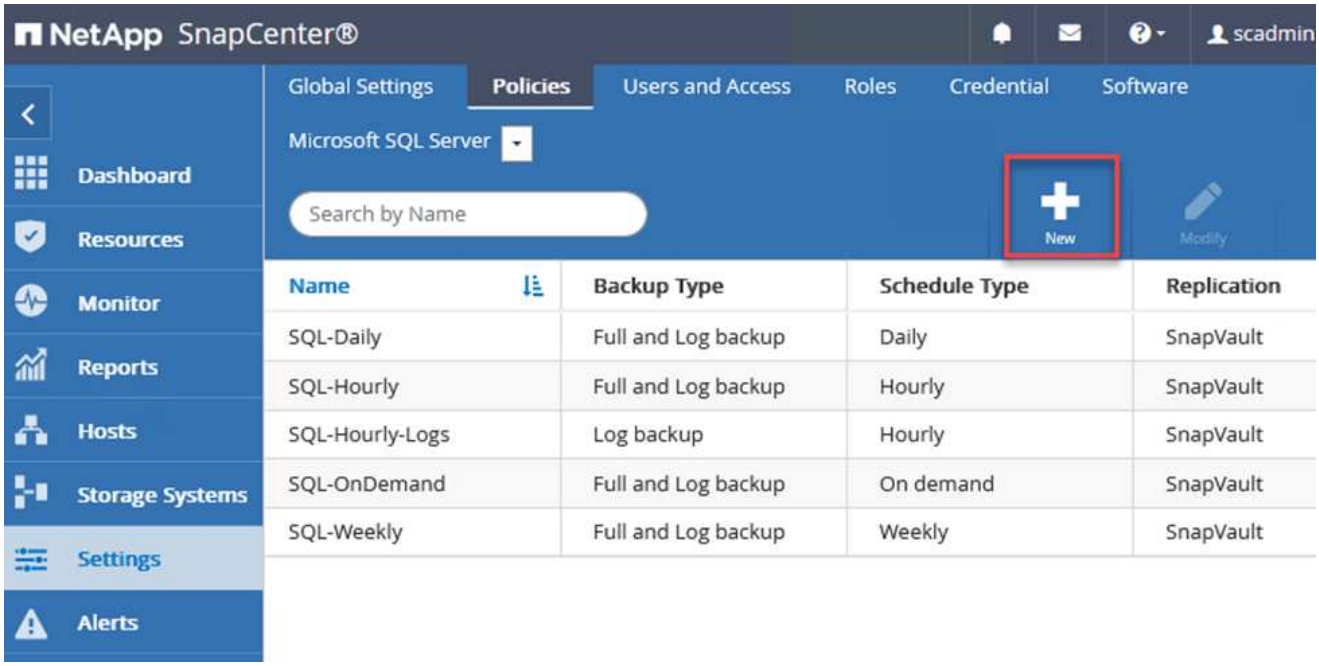
3. Pour Oracle, renseignez les champs requis dans la boîte de dialogue Ajouter un hôte et cochez la case du plug-in Oracle Database. Cliquez ensuite sur Envoyer pour lancer le processus de détection et ajouter l'hôte à SnapCenter.


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

Création de règles SnapCenter

Les stratégies définissent les règles spécifiques à suivre pour une tâche de sauvegarde. Notamment le calendrier de sauvegarde, le type de réplication et la manière dont SnapCenter gère la sauvegarde et la troncation des journaux de transactions.

Vous pouvez accéder aux stratégies dans la section Paramètres du client Web SnapCenter.



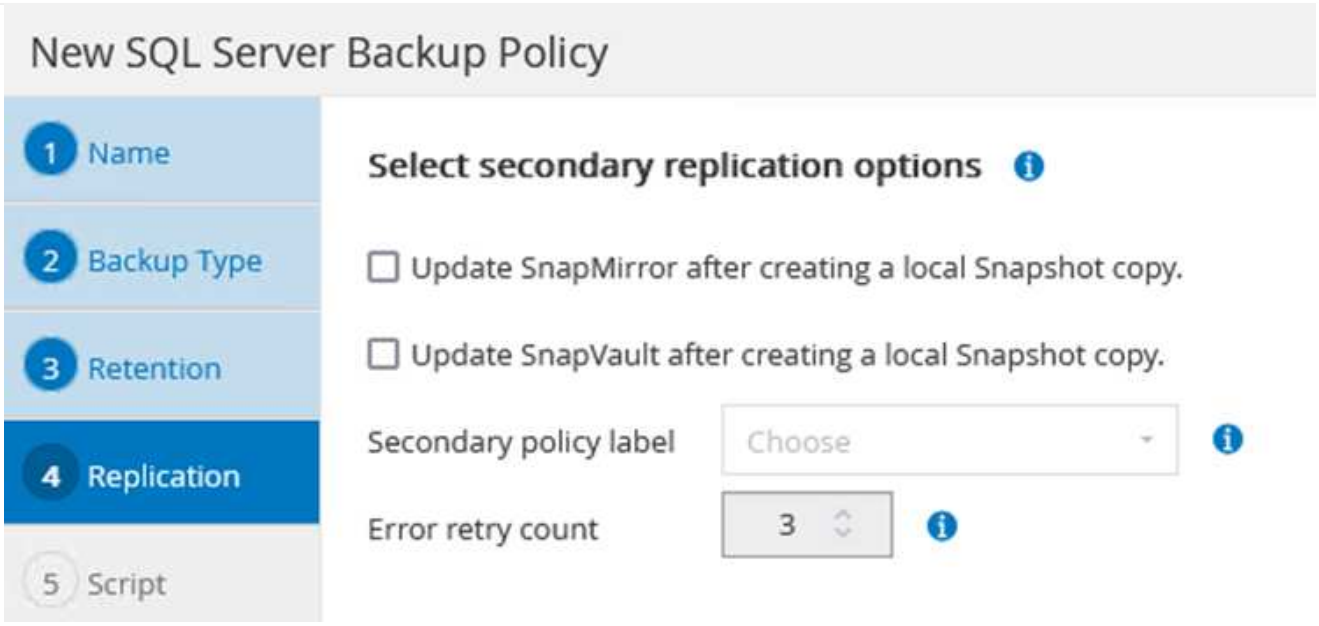
Pour obtenir des informations complètes sur la création de stratégies pour les sauvegardes SQL Server, reportez-vous à la section "Documentation SnapCenter".

Pour obtenir des informations complètes sur la création de stratégies pour les sauvegardes Oracle, reportez-vous au "Documentation SnapCenter".

Notes:

- Au fur et à mesure que vous progressez dans l'assistant de création de règles, prenez note spéciale de la section réplication. Dans cette section, vous devez spécifier les types de copies SnapMirror secondaires que vous souhaitez effectuer pendant le processus de sauvegarde.
- Le paramètre « mettre à jour SnapMirror après la création d'une copie Snapshot locale » fait référence à la mise à jour d'une relation SnapMirror lorsqu'il existe entre deux machines virtuelles de stockage résidant sur le même cluster.
- Le paramètre « Update SnapVault après création d'une copie Snapshot locale » permet de mettre à jour une relation SnapMirror entre deux clusters distincts et entre un système ONTAP sur site et Cloud Volumes ONTAP ou FSxN.

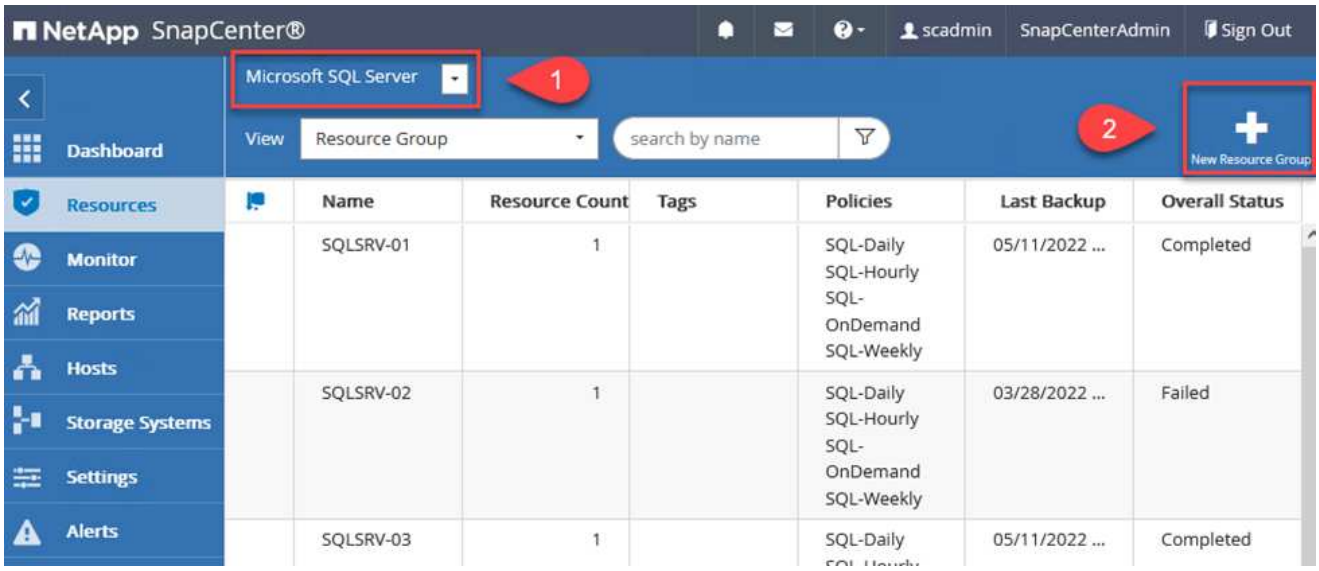
L'image suivante montre les options ci-dessus et leur apparence dans l'assistant de stratégie de sauvegarde.



Créer des groupes de ressources SnapCenter

Les groupes de ressources vous permettent de sélectionner les ressources de base de données que vous souhaitez inclure dans vos sauvegardes et les stratégies suivies pour ces ressources.

1. Accédez à la section Ressources du menu de gauche.
2. En haut de la fenêtre, sélectionnez le type de ressource à utiliser (dans ce cas, Microsoft SQL Server), puis cliquez sur Nouveau groupe de ressources.



La documentation SnapCenter fournit des informations détaillées sur la création de groupes de ressources pour les bases de données SQL Server et Oracle.

Pour la sauvegarde des ressources SQL, suivez "ce lien".

Pour la sauvegarde des ressources Oracle, suivez "ce lien".

Déploiement et configuration de Veeam Backup Server

Le logiciel Veeam Backup & Replication est utilisé dans la solution pour sauvegarder nos machines virtuelles d'applications et archiver une copie des sauvegardes dans un compartiment Amazon S3 à l'aide d'un référentiel de sauvegarde scale-out Veeam. Veeam est déployé sur un serveur Windows dans cette solution. Pour des conseils spécifiques sur le déploiement de Veeam, reportez-vous au "Documentation technique sur le centre d'assistance Veeam".

Configurez un référentiel de sauvegarde scale-out Veeam

Une fois que vous avez déployé et sous licence le logiciel, vous pouvez créer un référentiel de sauvegarde scale-out (SOBR) en tant que stockage cible pour les tâches de sauvegarde. Vous devez également inclure un compartiment S3 comme sauvegarde des données de machines virtuelles hors site pour la reprise après incident.

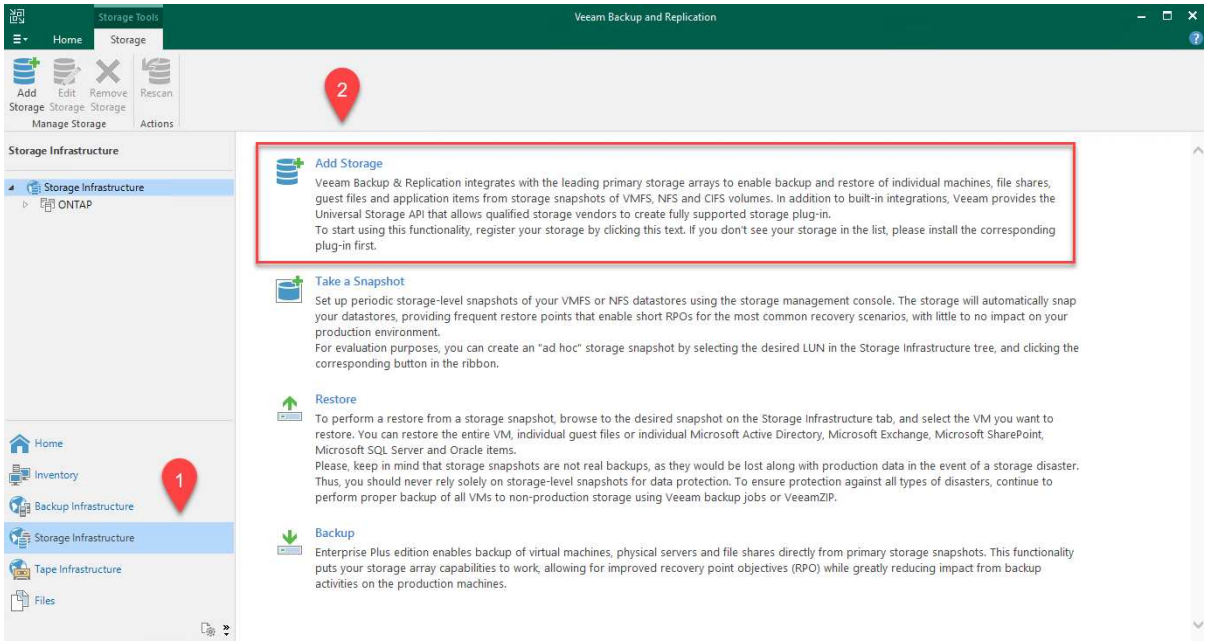
Consultez les conditions préalables suivantes avant de commencer.

1. Créez un partage de fichiers SMB sur votre système ONTAP sur site en tant que stockage cible pour les sauvegardes.
2. Créez un compartiment Amazon S3 à inclure dans le volume de stockage. Il s'agit d'un référentiel pour les sauvegardes hors site.

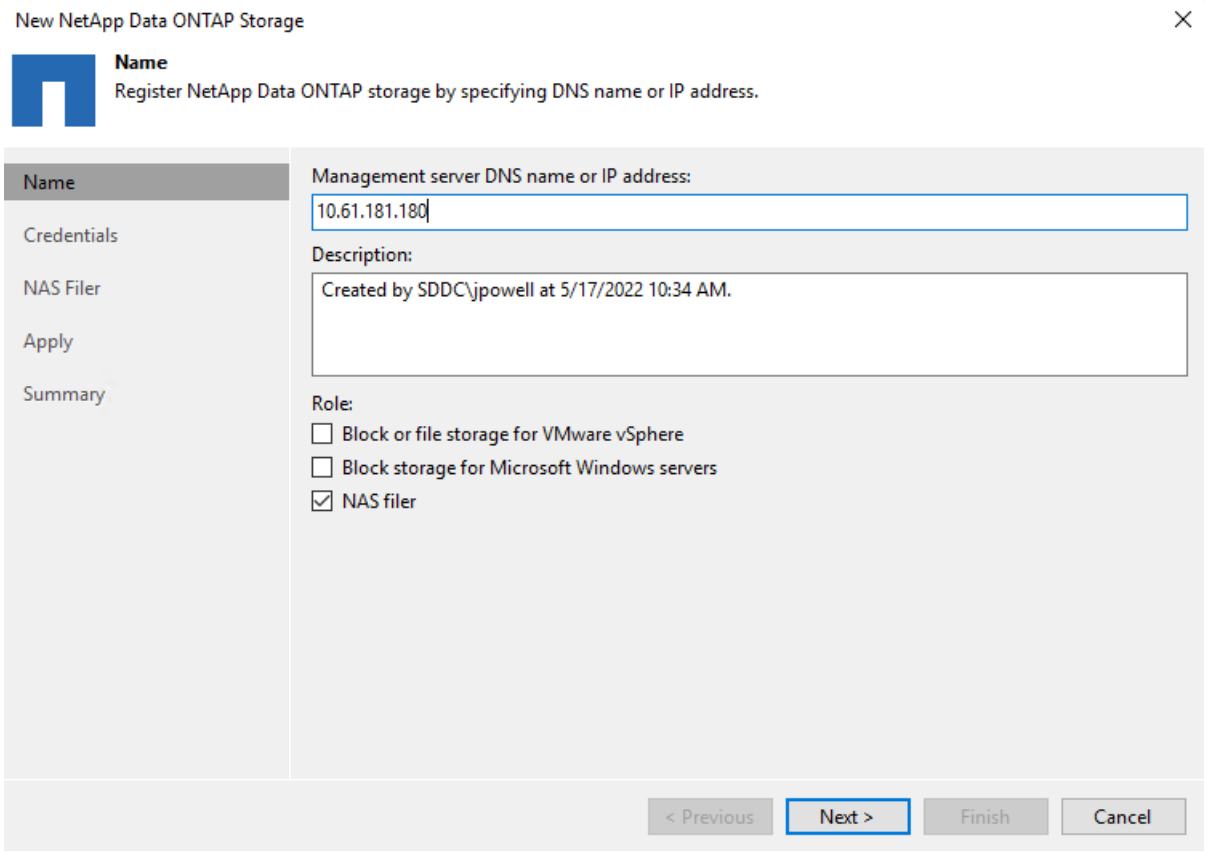
Ajout du stockage ONTAP à Veeam

Tout d'abord, ajoutez le cluster de stockage ONTAP et le système de fichiers SMB/NFS associé en tant qu'infrastructure de stockage dans Veeam.

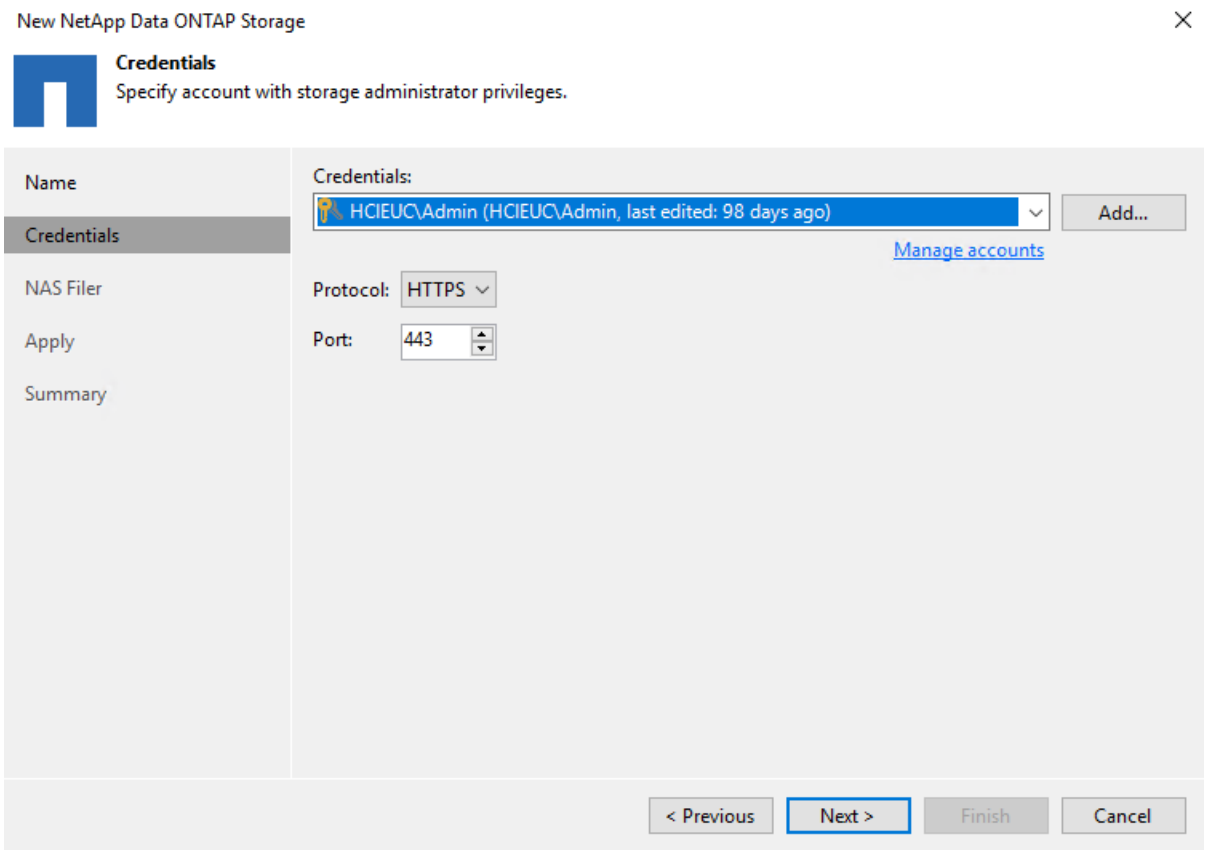
1. Ouvrez la console Veeam et connectez-vous. Accédez à Storage Infrastructure, puis sélectionnez Add Storage.



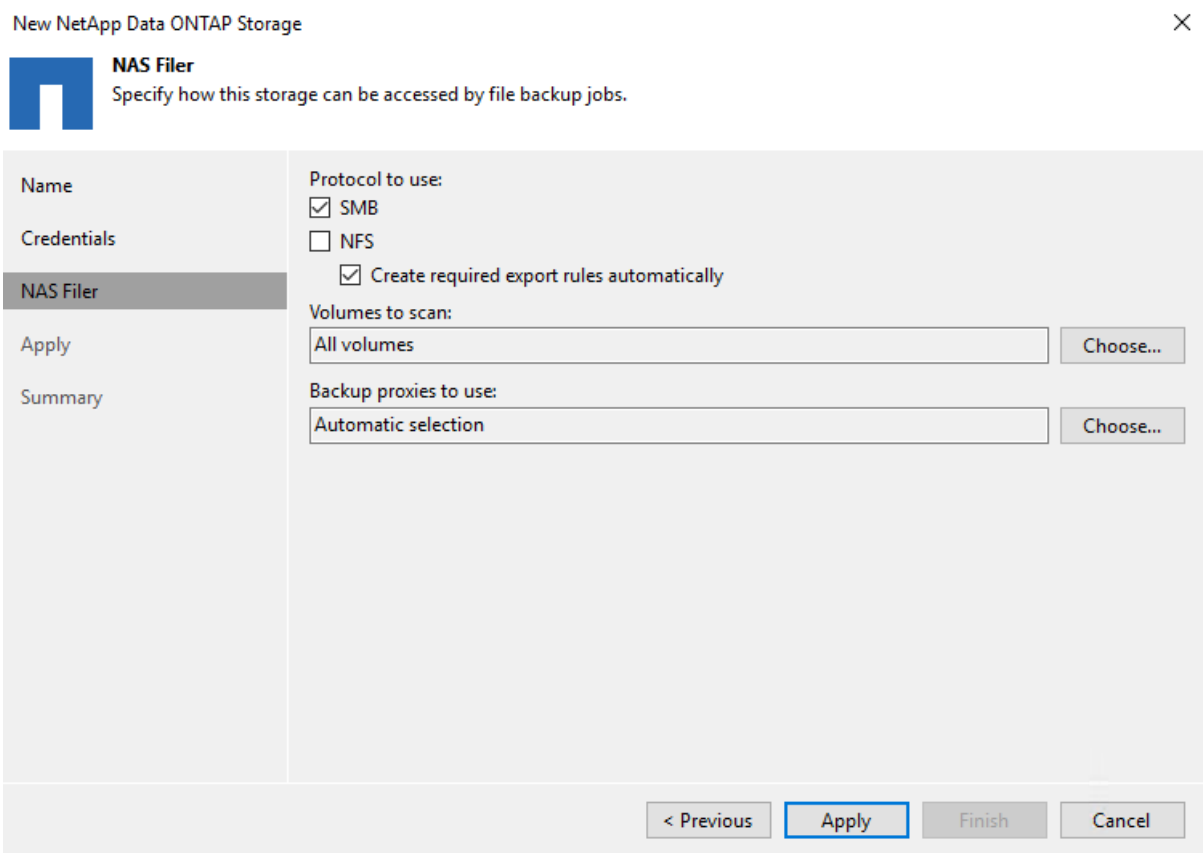
2. Dans l'assistant d'ajout de stockage, sélectionnez NetApp comme fournisseur de stockage, puis sélectionnez Data ONTAP.
3. Entrez l'adresse IP de gestion et cochez la case filer NAS. Cliquez sur Suivant.



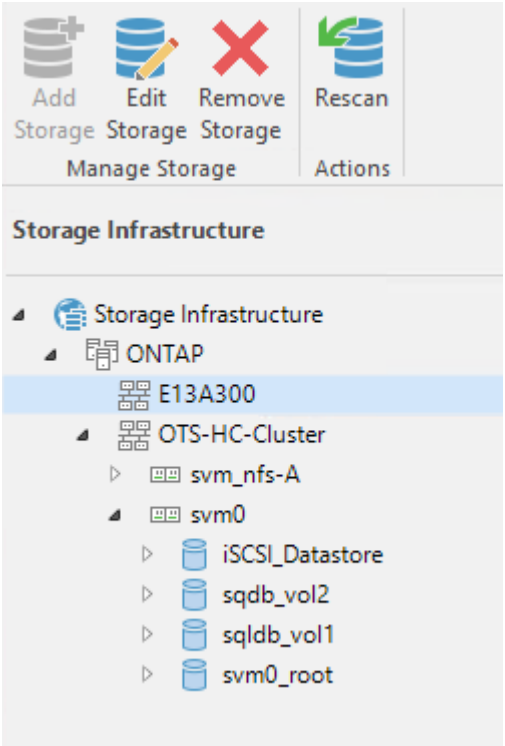
4. Ajoutez vos identifiants pour accéder au cluster ONTAP.



5. Sur la page NAS Filer, choisissez les protocoles à analyser et sélectionnez Suivant.

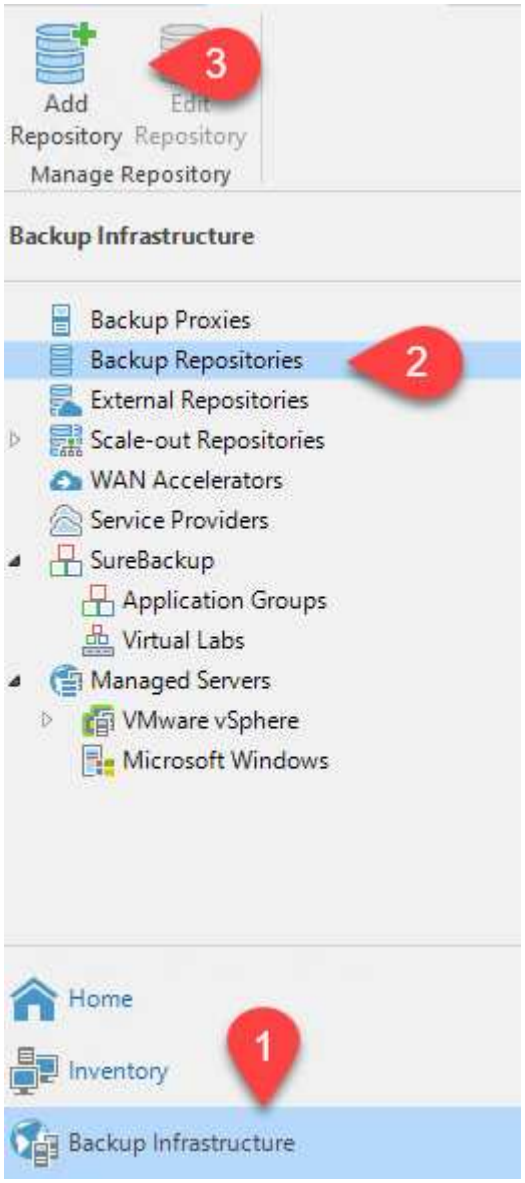


6. Complétez les pages appliquer et Résumé de l'assistant et cliquez sur Terminer pour lancer le processus de détection du stockage. Une fois le scan terminé, on ajoute le cluster ONTAP ainsi que les filers NAS en tant que ressources disponibles.

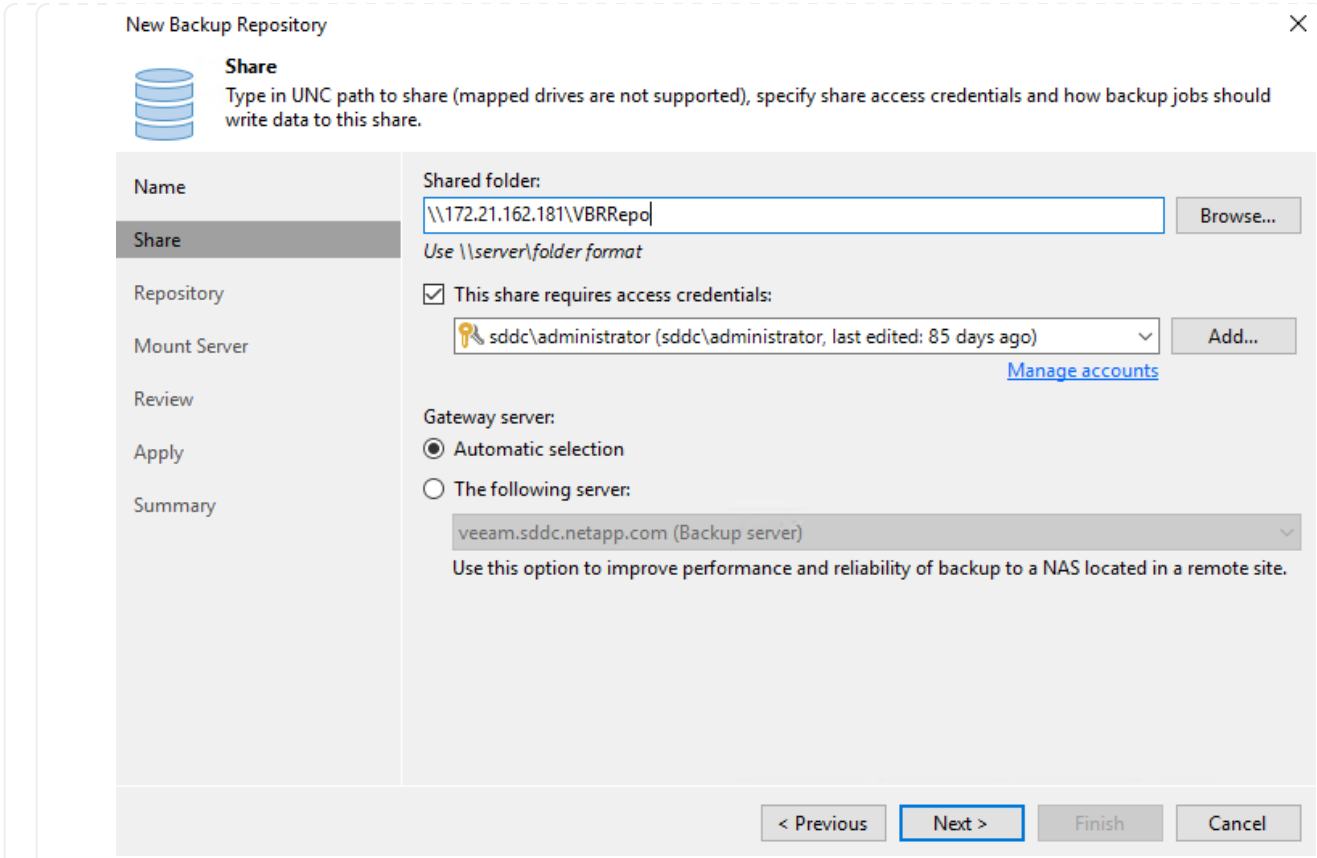


7. Créez un référentiel de sauvegarde à l'aide des partages NAS récemment découverts. Dans Backup Infrastructure, sélectionnez Sauvegarder les référentiels et cliquez sur l'élément de

menu Ajouter un référentiel.



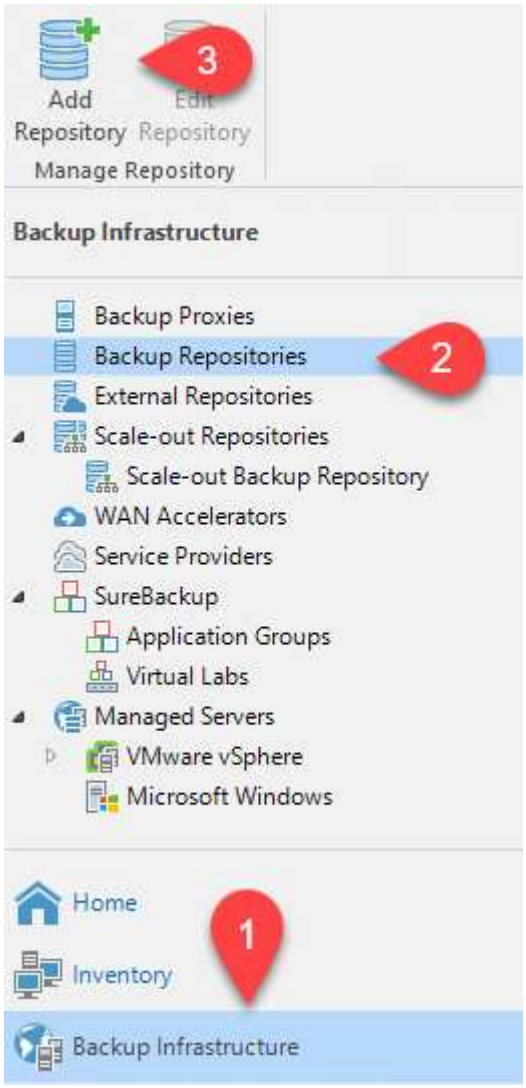
8. Suivez toutes les étapes de l'Assistant Nouveau référentiel de sauvegarde pour créer le référentiel. Pour plus d'informations sur la création des référentiels de sauvegarde Veeam, consultez le "Documentation Veeam".


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

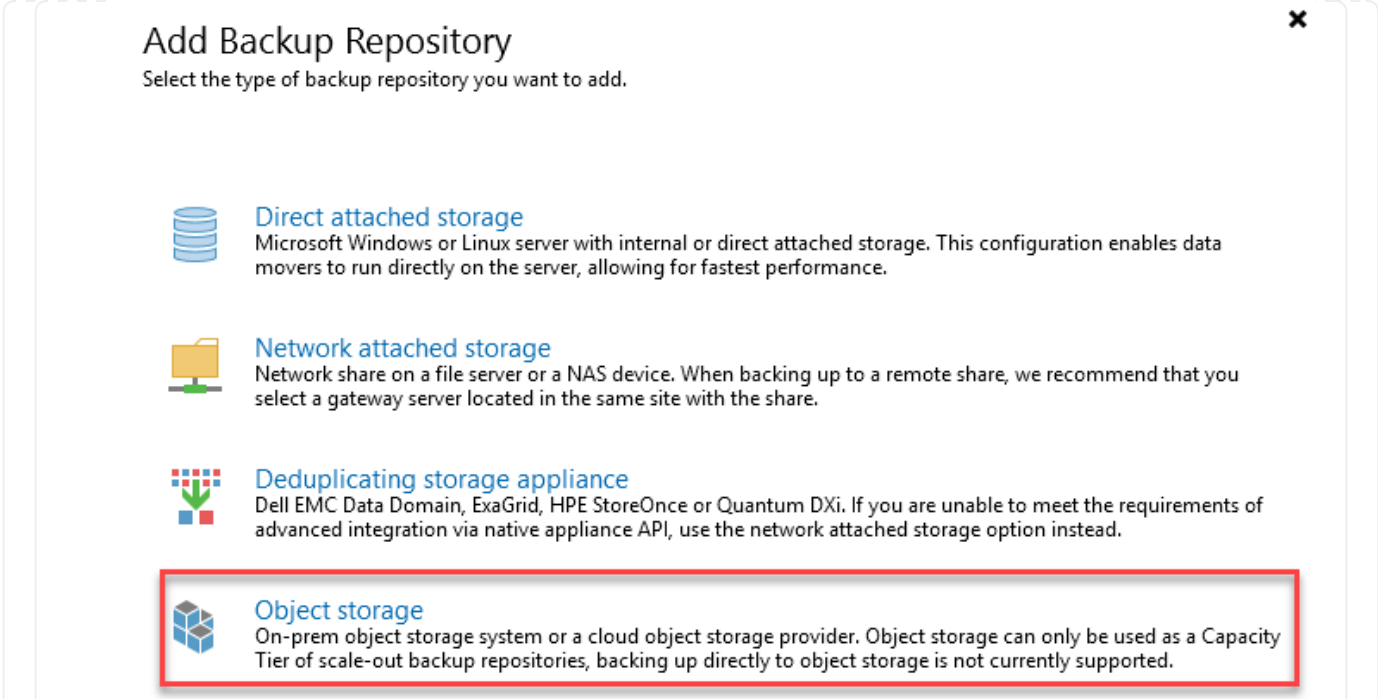
Ajoutez le compartiment Amazon S3 en tant que référentiel de sauvegarde

L'étape suivante consiste à ajouter le stockage Amazon S3 en tant que référentiel de sauvegarde.

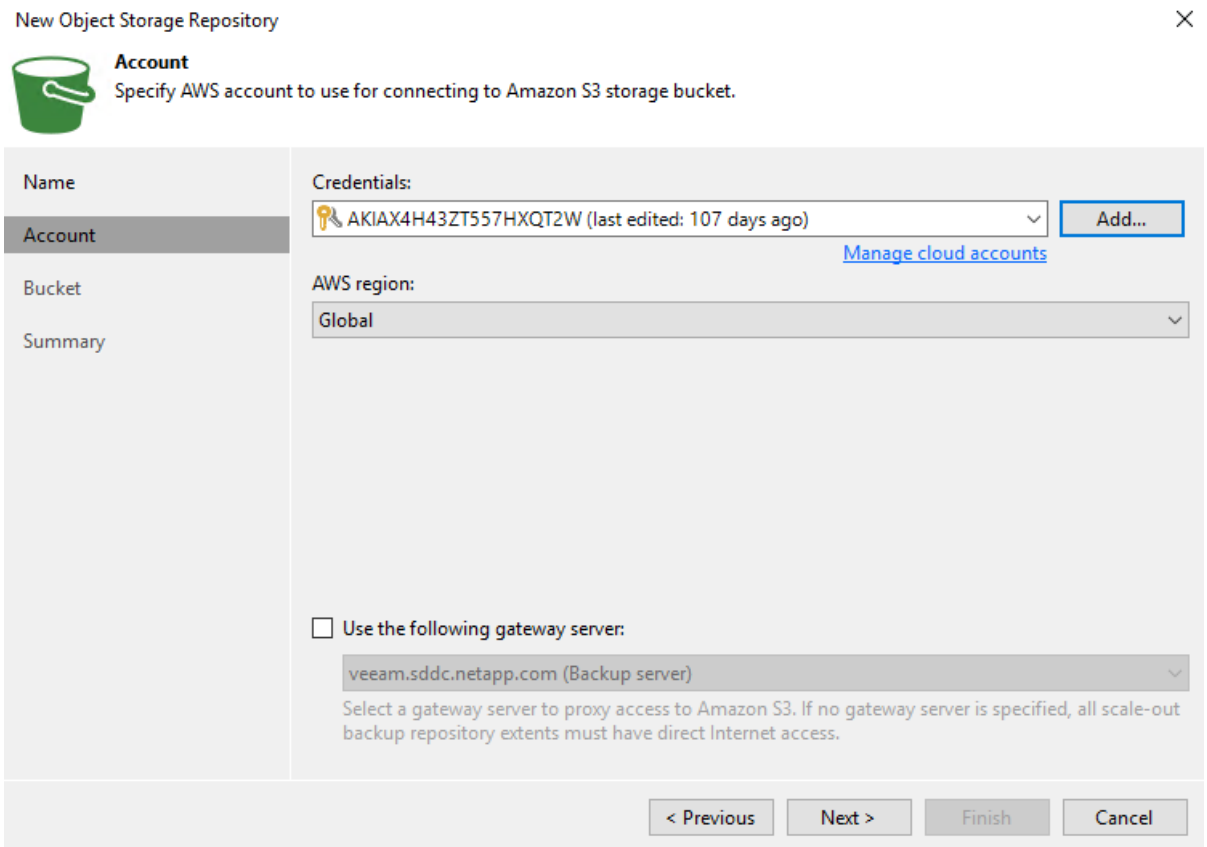
1. Accédez à Backup Infrastructure > référentiels de sauvegarde. Cliquez sur Ajouter un référentiel.



2. Dans l'assistant Ajouter un référentiel de sauvegarde, sélectionnez stockage objet, puis Amazon S3. L'assistant Nouveau référentiel de stockage objet démarre.



3. Fournissez un nom pour votre référentiel de stockage objet et cliquez sur Next (Suivant).
4. Dans la section suivante, indiquez vos identifiants. Vous avez besoin d'une clé d'accès et d'une clé secrète AWS.

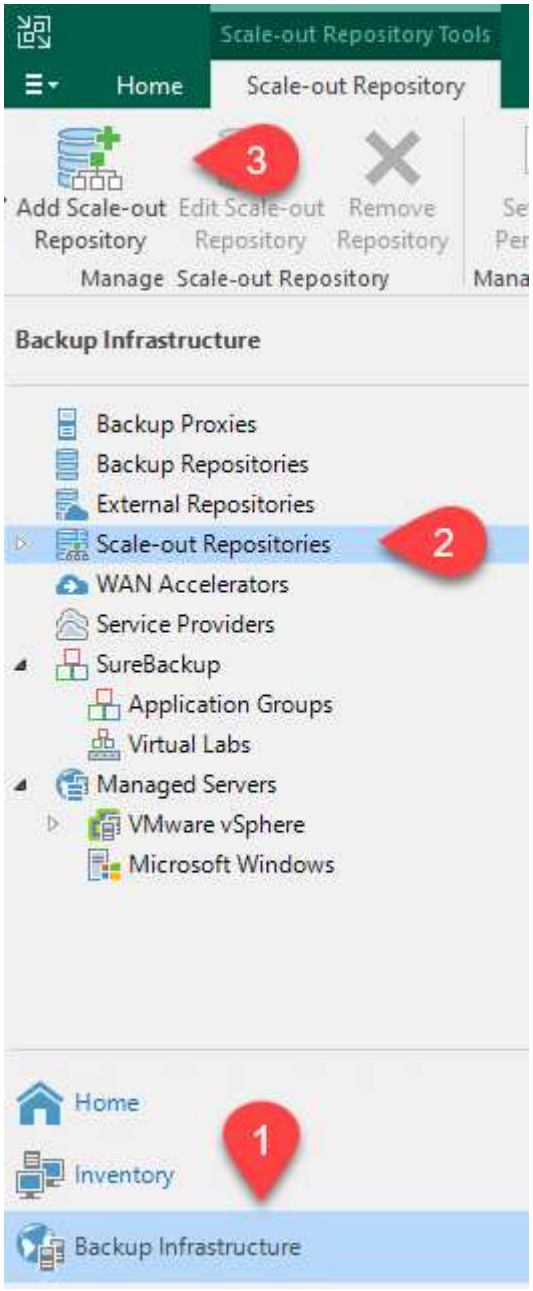


5. Une fois la configuration Amazon chargée, choisissez votre data Center, votre compartiment et votre dossier, puis cliquez sur « Apply » (appliquer). Enfin, cliquez sur Terminer pour fermer l'assistant.

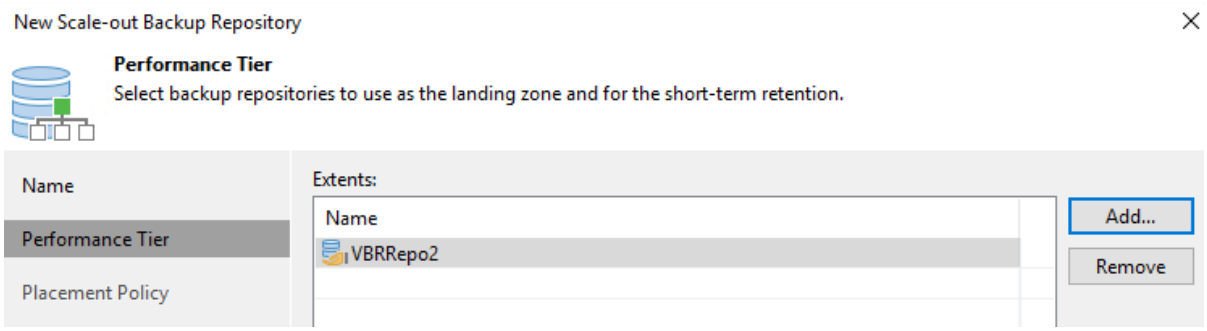
Création d'un référentiel de sauvegarde scale-out

Maintenant que nous avons ajouté nos référentiels de stockage à Veeam, nous pouvons créer la solution SOBR afin de hiérarchiser automatiquement les copies de sauvegarde dans notre stockage objet Amazon S3 hors site pour la reprise après incident.

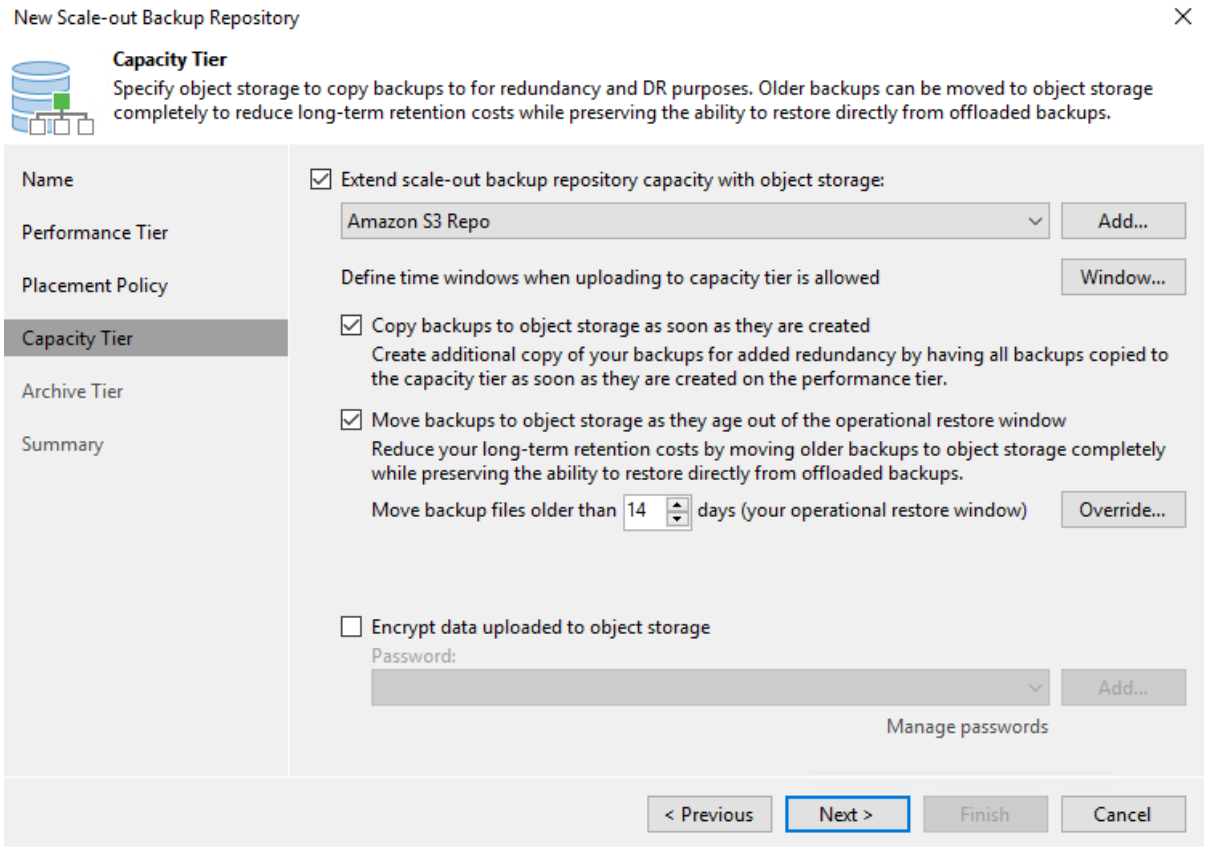
1. Dans l'infrastructure de sauvegarde, sélectionnez référentiels scale-out, puis cliquez sur l'élément de menu Ajouter un référentiel scale-out.



2. Dans le nouveau référentiel de sauvegarde scale-out, indiquez un nom pour le SOBR et cliquez sur Suivant.
3. Pour le niveau de performances, choisissez le référentiel de sauvegarde contenant le partage SMB résidant sur votre cluster ONTAP local.



4. Pour la stratégie de placement, choisissez l'emplacement des données ou les performances en fonction de vos besoins. Sélectionnez Next (Suivant).
5. Pour le niveau de capacité, nous avons étendu la solution SOBR avec le stockage objet Amazon S3. Pour les besoins de reprise après incident, sélectionnez Copier les sauvegardes vers le stockage objet dès leur création afin de fournir nos sauvegardes secondaires dans les délais.



6. Enfin, sélectionnez appliquer et Terminer pour finaliser la création du SOBR.

Création des tâches de référentiel de sauvegarde scale-out

La dernière étape de configuration de Veeam consiste à créer des tâches de sauvegarde en utilisant le SOBR nouvellement créé comme destination de sauvegarde. La création de travaux de sauvegarde fait partie intégrante du répertoire de tout administrateur de stockage et nous ne abordons pas les étapes détaillées ici. Pour plus d'informations sur la création de tâches de sauvegarde dans Veeam, consultez le "Documentation technique du centre d'aide Veeam".

Configuration et outils de sauvegarde et de restauration BlueXP

Pour effectuer un basculement des VM applicatives et des volumes de base de données vers les services VMware Cloud volumes exécutés dans AWS, vous devez installer et configurer une instance en cours d'exécution de SnapCenter Server et Veeam Backup and Replication Server. Une fois le basculement terminé, vous devez également configurer ces outils pour reprendre les opérations de sauvegarde normales jusqu'à ce que la restauration du data Center sur site soit planifiée et exécutée.

Déploiement d'un serveur Windows SnapCenter secondaire

Le serveur SnapCenter est déployé dans le SDDC VMware Cloud ou installé sur une instance EC2 résidant dans un VPC avec une connectivité réseau vers l'environnement VMware Cloud.

Le logiciel SnapCenter est disponible sur le site du support NetApp et peut être installé sur les systèmes Microsoft Windows résidant dans un domaine ou un groupe de travail. Un guide de planification détaillé et des instructions d'installation sont disponibles sur le "Centre de documentation NetApp".

Le logiciel SnapCenter est disponible sur la page "ce lien".

Configurez le serveur SnapCenter secondaire

Pour restaurer les données d'application en miroir vers FSX ONTAP, vous devez d'abord effectuer une restauration complète de la base de données SnapCenter sur site. Une fois ce processus terminé, la communication avec les machines virtuelles est rétablie, et les sauvegardes des applications peuvent maintenant reprendre en utilisant FSX ONTAP comme stockage primaire.

Pour ce faire, vous devez effectuer les opérations suivantes sur le serveur SnapCenter :

1. Configurez le nom de l'ordinateur pour qu'il soit identique au serveur SnapCenter sur site d'origine.
2. Configurez le réseau pour communiquer avec VMware Cloud et l'instance FSX ONTAP.
3. Terminez la procédure de restauration de la base de données SnapCenter.
4. Vérifiez que SnapCenter est en mode reprise après incident pour vous assurer que FSX est désormais le stockage principal pour les sauvegardes.
5. Confirmer que la communication est rétablie avec les machines virtuelles restaurées.

Déploiement du serveur de sauvegarde et de réplication Veeam secondaire

Vous pouvez installer le serveur Veeam Backup & Replication sur un serveur Windows dans le cloud VMware sur AWS ou sur une instance EC2. Pour obtenir des conseils détaillés sur la mise en œuvre, reportez-vous au "Documentation technique du centre d'aide Veeam".

Configuration du serveur Veeam Backup etamp secondaire ; Replication Server

Pour effectuer une restauration des machines virtuelles qui ont été sauvegardées sur le stockage Amazon S3, vous devez installer Veeam Server sur un serveur Windows et le configurer pour qu'il communique avec VMware Cloud, FSX ONTAP et le compartiment S3 qui contient le référentiel de sauvegarde d'origine. Le système informatique doit également configurer un nouveau référentiel de sauvegarde sur FSX ONTAP afin de réaliser de nouvelles sauvegardes des machines virtuelles après leur restauration.

Pour effectuer ce processus, les éléments suivants doivent être effectués :

1. Configuration du réseau pour communiquer avec VMware Cloud, FSX ONTAP et un compartiment S3 contenant le référentiel de sauvegarde d'origine
2. Configurez un partage SMB sur FSX ONTAP en tant que nouveau référentiel de sauvegarde.
3. Montez le compartiment S3 d'origine utilisé dans le référentiel de sauvegarde scale-out sur site.
4. Après la restauration de la machine virtuelle, établir de nouvelles tâches de sauvegarde afin de protéger les machines virtuelles SQL et Oracle.

Pour plus d'informations sur la restauration des VM à l'aide de Veeam, reportez-vous à la section "Restauration des VM applications avec Veeam Full Restore".

Sauvegarde des bases de données SnapCenter pour la reprise après incident

SnapCenter permet la sauvegarde et la récupération de sa base de données MySQL sous-jacente et des données de configuration afin de restaurer le serveur SnapCenter en cas d'incident. Pour notre solution, nous avons restauré la base de données et la configuration d'SnapCenter sur une instance EC2 AWS résidant sur notre VPC. Pour plus d'informations sur cette étape, reportez-vous à la section "ce lien".

Conditions préalables à la sauvegarde SnapCenter

Les prérequis suivants sont requis pour la sauvegarde SnapCenter :

- Un partage de volume et SMB créé sur le système ONTAP sur site pour localiser la base de données et les fichiers de configuration sauvegardés.
- Relation SnapMirror entre le système ONTAP sur site et FSX ou CVO dans le compte AWS. Cette relation est utilisée pour le transport de l'instantané contenant la base de données SnapCenter sauvegardée et les fichiers de configuration.
- Windows Server installé dans le compte cloud, soit sur une instance EC2, soit sur une VM dans le SDDC VMware Cloud.
- SnapCenter installé sur l'instance Windows EC2 ou le VM dans VMware Cloud.

Récapitulatif du processus de sauvegarde et de restauration SnapCenter

- Créez un volume sur le système ONTAP sur site pour héberger les fichiers de base de données de sauvegarde et de configuration.
- Configurer une relation SnapMirror entre le site et FSX/CVO.
- Montez le partage SMB.
- Récupérez le jeton d’autorisation de swagger pour effectuer des tâches API.
- Démarrez le processus de restauration de la base de données.
- Utilisez l’utilitaire xcopy pour copier le répertoire local du fichier de base de données et de configuration dans le partage SMB.
- Sur la plateforme FSX, créez un clone du volume ONTAP (copié via SnapMirror depuis sur site).
- Montez le partage SMB de FSX vers le cloud EC2/VMware.
- Copiez le répertoire de restauration du partage SMB dans un répertoire local.
- Exécutez le processus de restauration de SQL Server à partir de swagger.

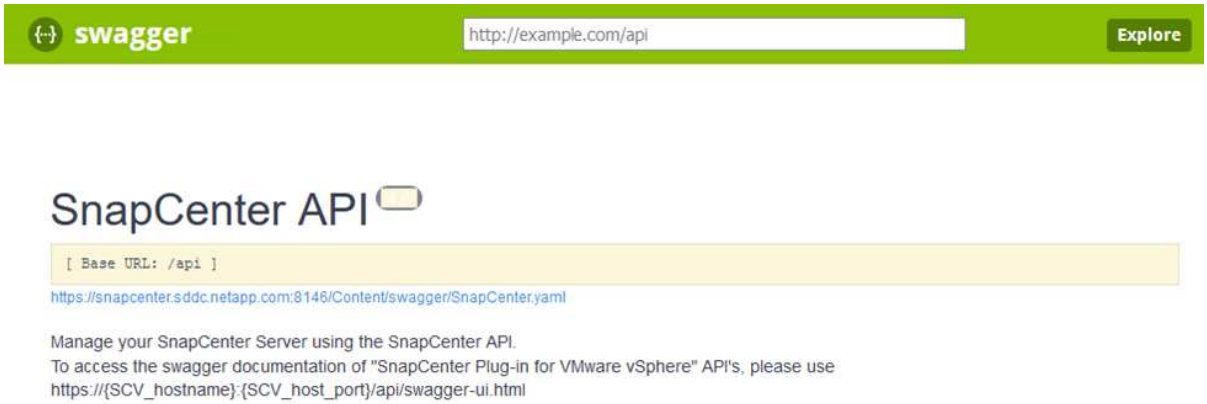
Sauvegarder la base de données et la configuration de SnapCenter

SnapCenter fournit une interface client Web pour l'exécution des commandes de l'API REST. Pour plus d'informations sur l'accès aux API REST via swagger, consultez la documentation SnapCenter à l'adresse "ce lien".

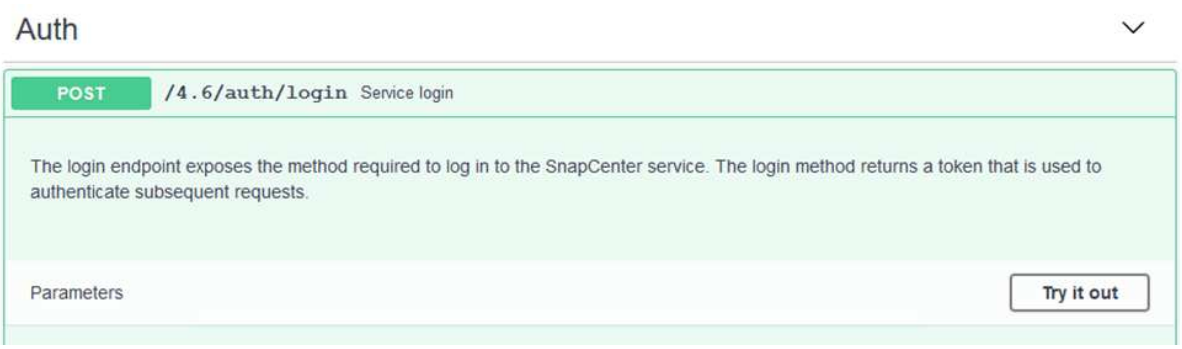
Connectez-vous à swagger et obtenez le jeton d'autorisation

Une fois que vous avez navigué vers la page swagger, vous devez récupérer un jeton d'autorisation pour lancer le processus de restauration de la base de données.

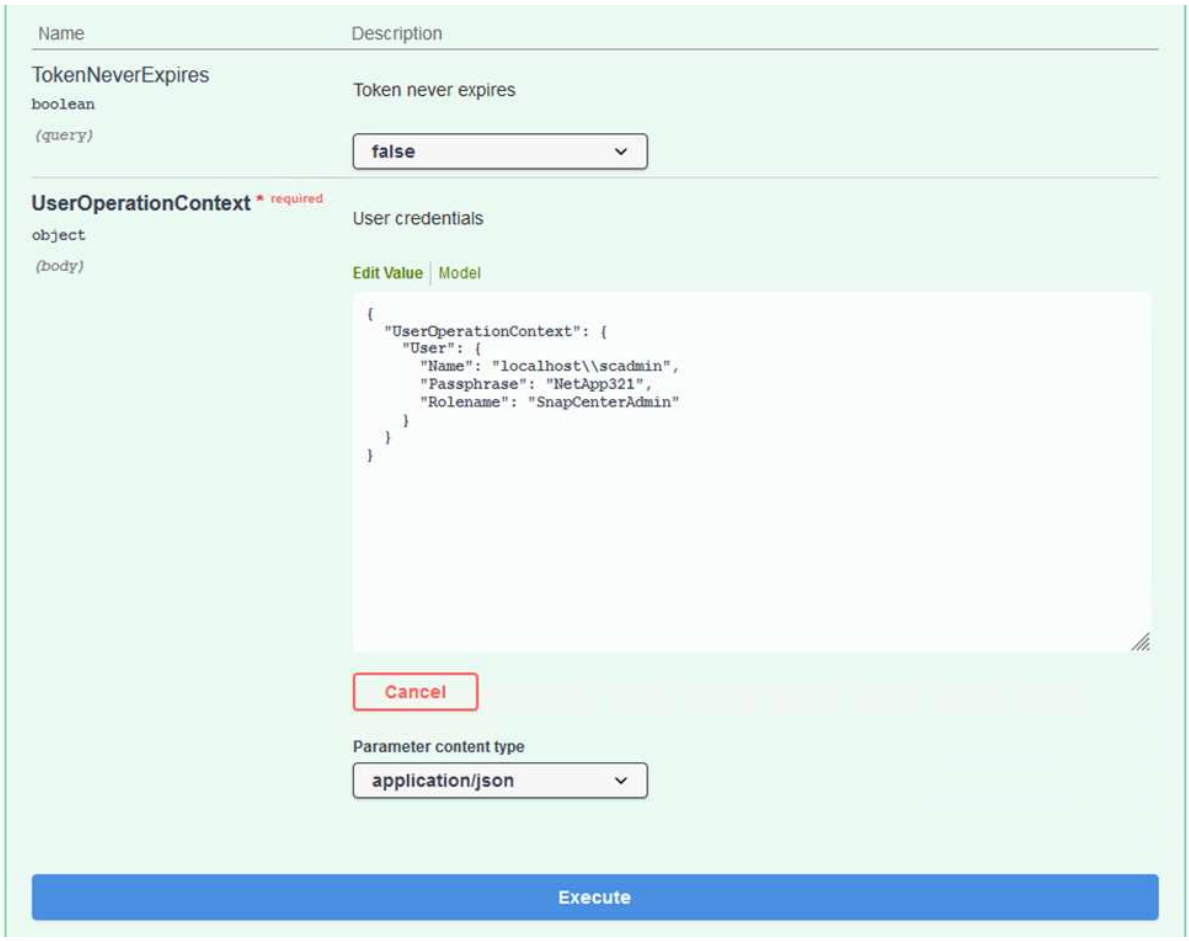
1. Accédez à la page Web de l'API SnapCenter swagger à l'adresse *https://<SnapCenter Server IP>:8146/swagger/*.



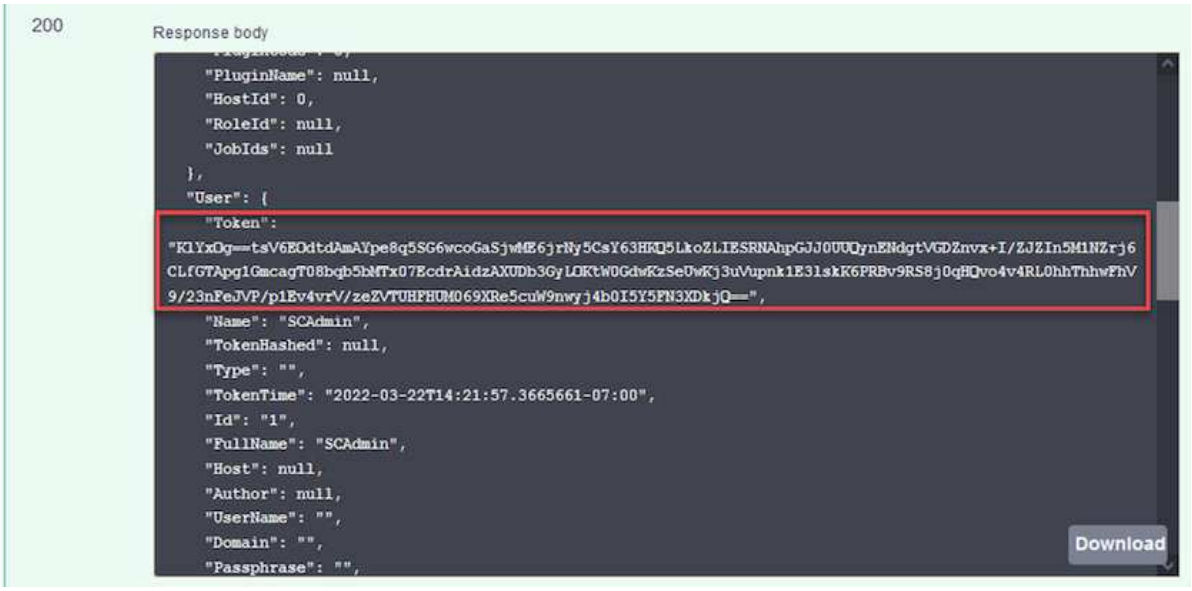
2. Développez la section Auth et cliquez sur le bouton essayer.



3. Dans la zone UserOperationContext, renseignez les informations d'identification et le rôle SnapCenter, puis cliquez sur Exécuter.



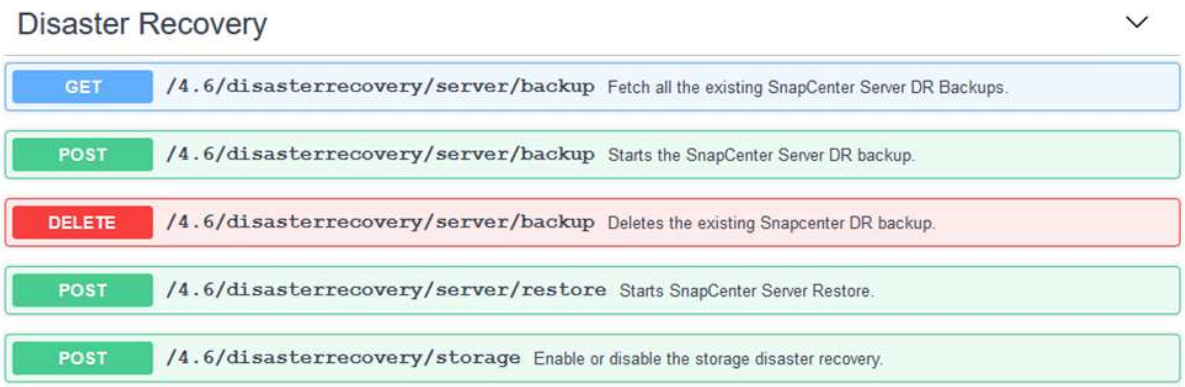
4. Dans le corps de réponse ci-dessous, vous pouvez voir le jeton. Copiez le texte du token pour l'authentification lors de l'exécution du processus de sauvegarde.



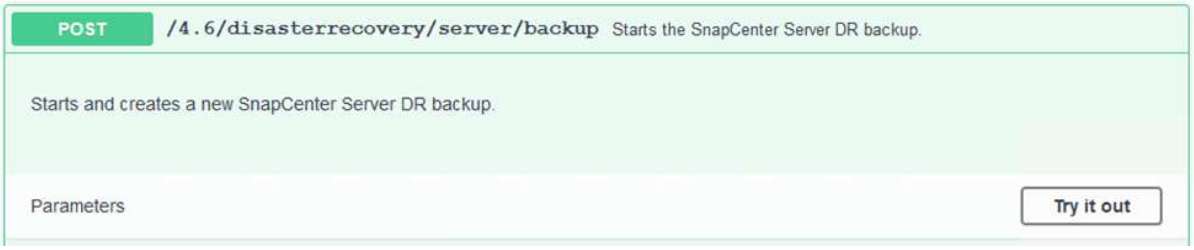
Effectuez une sauvegarde de base de données SnapCenter

Passez ensuite à la zone de reprise sur incident de la page swagger pour lancer le processus de sauvegarde SnapCenter.

1. Développez la zone de reprise après sinistre en cliquant dessus.

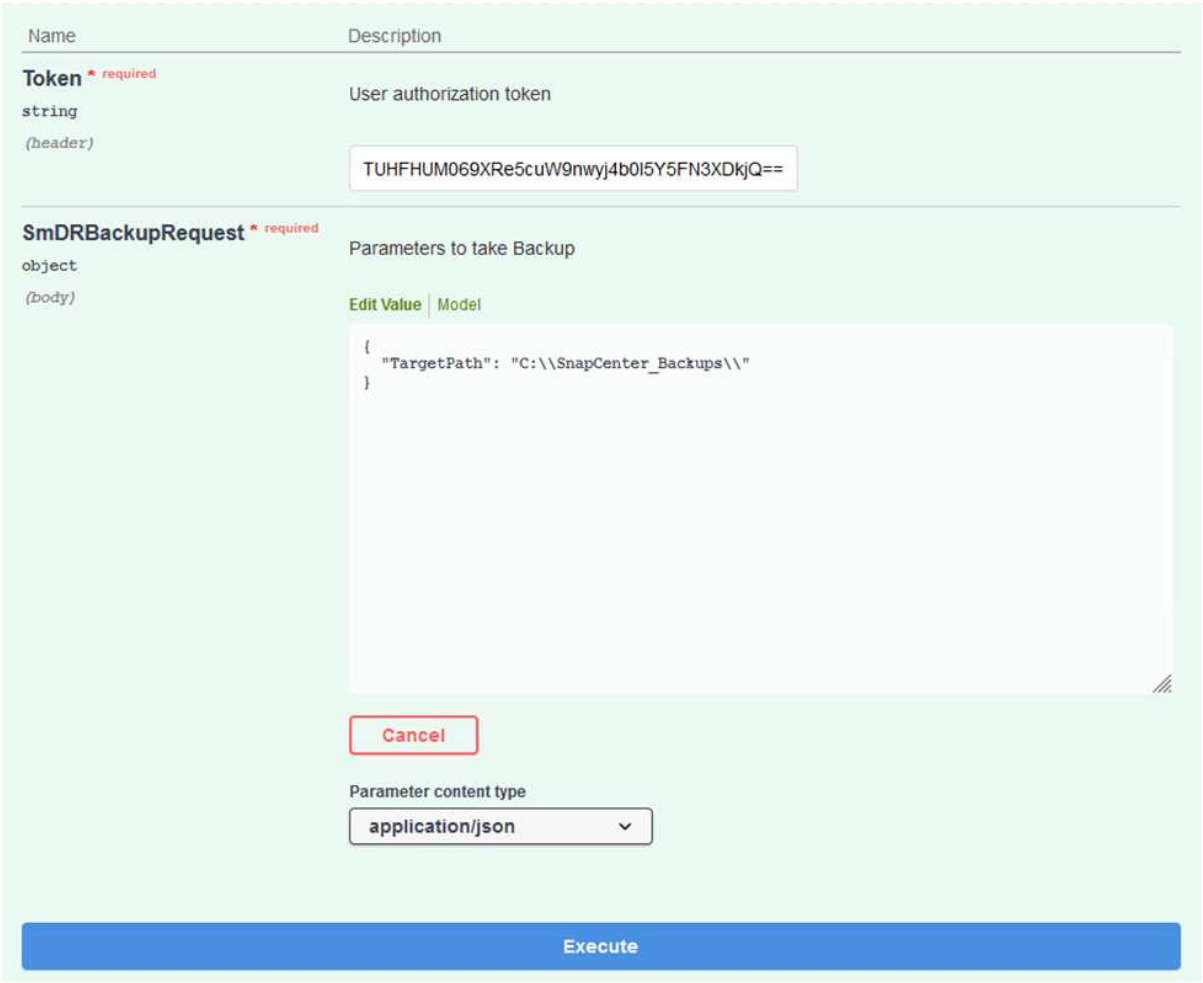


2. Développez le `/4.6/disasterrecovery/server/backup` Et cliquez sur essayer.



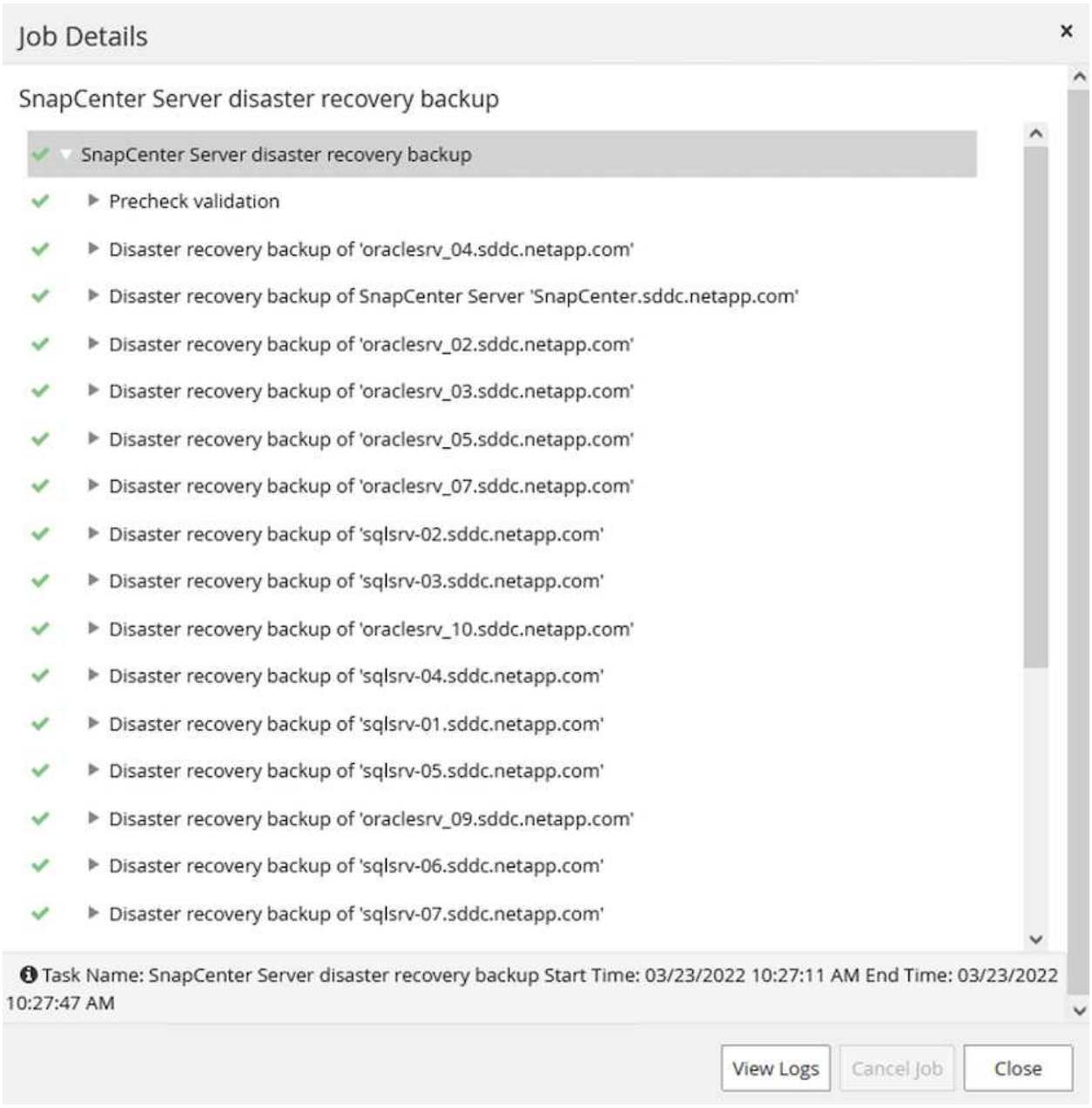
3. Dans la section SmDRBackupRequest, ajoutez le chemin cible local correct et sélectionnez Exécuter pour lancer la sauvegarde de la base de données et de la configuration SnapCenter.

> Le processus de sauvegarde ne permet pas de sauvegarder directement les données sur un partage de fichiers NFS ou CIFS.


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

Surveillez la procédure de sauvegarde depuis SnapCenter

Connectez-vous à SnapCenter pour consulter les fichiers journaux au démarrage du processus de restauration de la base de données. Dans la section moniteur, vous pouvez afficher les détails de la sauvegarde de reprise après incident du serveur SnapCenter.



Utilisez l'utilitaire XCOPY pour copier le fichier de sauvegarde de la base de données dans le partage SMB

Vous devez ensuite déplacer la sauvegarde du disque local du serveur SnapCenter vers le partage CIFS utilisé pour copier les données dans l'emplacement secondaire situé sur l'instance FSX d'AWS. Utilisez xcopy avec des options spécifiques qui conservent les autorisations des fichiers.

Ouvrez une invite de commande en tant qu'administrateur. Dans l'invite de commande, entrez les commandes suivantes :

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

Basculement

Un incident se produit sur le site primaire

En cas d'incident survenant dans le data Center principal sur site, notre scénario inclut un basculement vers un site secondaire résidant sur l'infrastructure Amazon Web Services à l'aide de VMware Cloud sur AWS. Nous partons du principe que les machines virtuelles et notre cluster ONTAP sur site ne sont plus accessibles. En outre, les machines virtuelles SnapCenter et Veeam ne sont plus accessibles et doivent être reconstruites dans notre site secondaire.

Cette section traite du basculement de notre infrastructure vers le cloud, et aborde les sujets suivants :

- Restauration de la base de données SnapCenter. Après l'établissement d'un nouveau serveur SnapCenter, restaurez la base de données MySQL et les fichiers de configuration, puis basculez la base de données en mode de reprise après sinistre afin de permettre au stockage FSX secondaire de devenir le périphérique de stockage principal.
- Restauration des machines virtuelles d'applications à l'aide de Veeam Backup & Replication Connectez le stockage S3 contenant les sauvegardes de machines virtuelles, importez les sauvegardes et restaurez-les dans VMware Cloud sur AWS.
- Restauration des données applicatives SQL Server à l'aide de SnapCenter
- Restaurez les données d'application Oracle à l'aide de SnapCenter.

Processus de restauration de la base de données SnapCenter

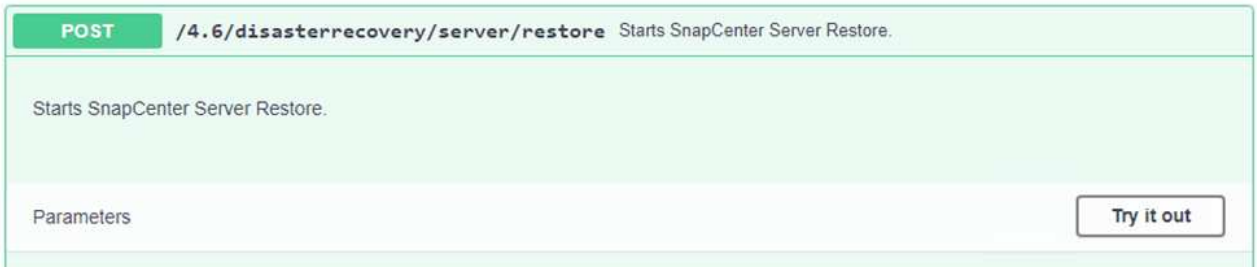
SnapCenter prend en charge les scénarios de reprise après incident en permettant la sauvegarde et la restauration de sa base de données MySQL et de ses fichiers de configuration. L'administrateur peut ainsi conserver des sauvegardes régulières de la base de données SnapCenter sur le data Center sur site et restaurer ensuite cette base de données vers une base de données SnapCenter secondaire.

Pour accéder aux fichiers de sauvegarde SnapCenter sur le serveur SnapCenter distant, procédez comme suit :

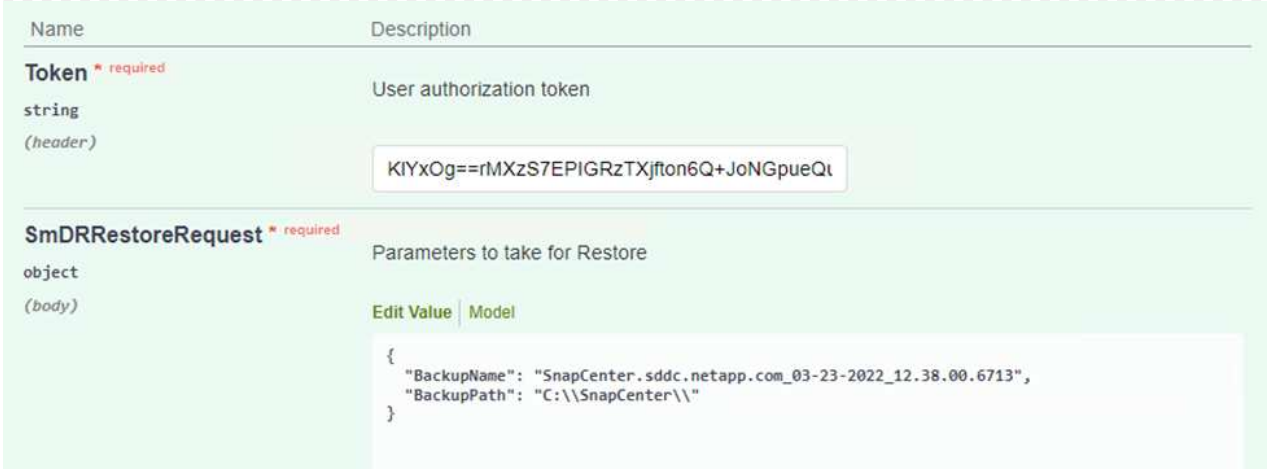
1. Faire un break de la relation SnapMirror depuis le cluster FSX, ce qui fait du volume la lecture/écriture.
2. Créer un serveur CIFS (si nécessaire) et créer un partage CIFS pointant vers la Junction path du volume cloné.
3. Utilisez xcopy pour copier les fichiers de sauvegarde dans un répertoire local sur le système SnapCenter secondaire.
4. Installez SnapCenter v4.6.
5. Assurez-vous que le serveur SnapCenter possède le même FQDN que le serveur d'origine. Cette opération est nécessaire pour que la restauration de la base de données soit réussie.

Pour démarrer le processus de restauration, procédez comme suit :

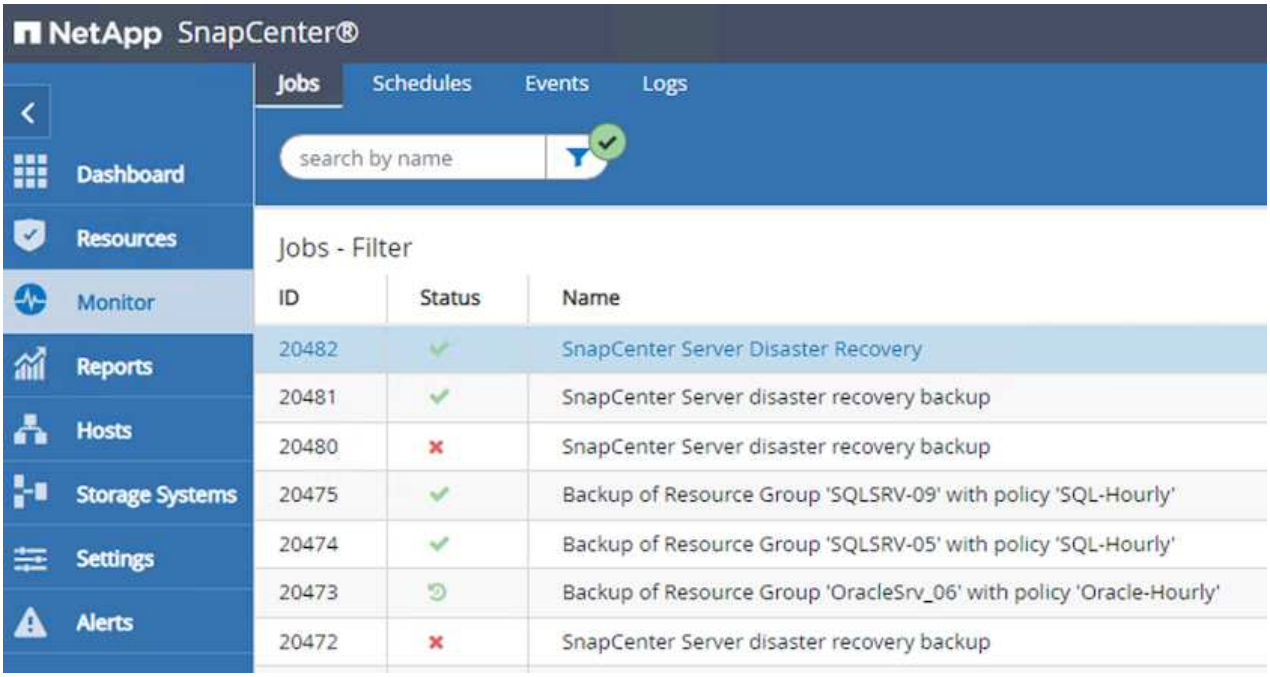
1. Accédez à la page Web de l'API swagger pour le serveur SnapCenter secondaire et suivez les instructions précédentes pour obtenir un jeton d'autorisation.
2. Accédez à la section récupération après sinistre de la page de swagger, puis sélectionnez `/4.6/disasterrecovery/server/restore`, Puis cliquez sur essayer.

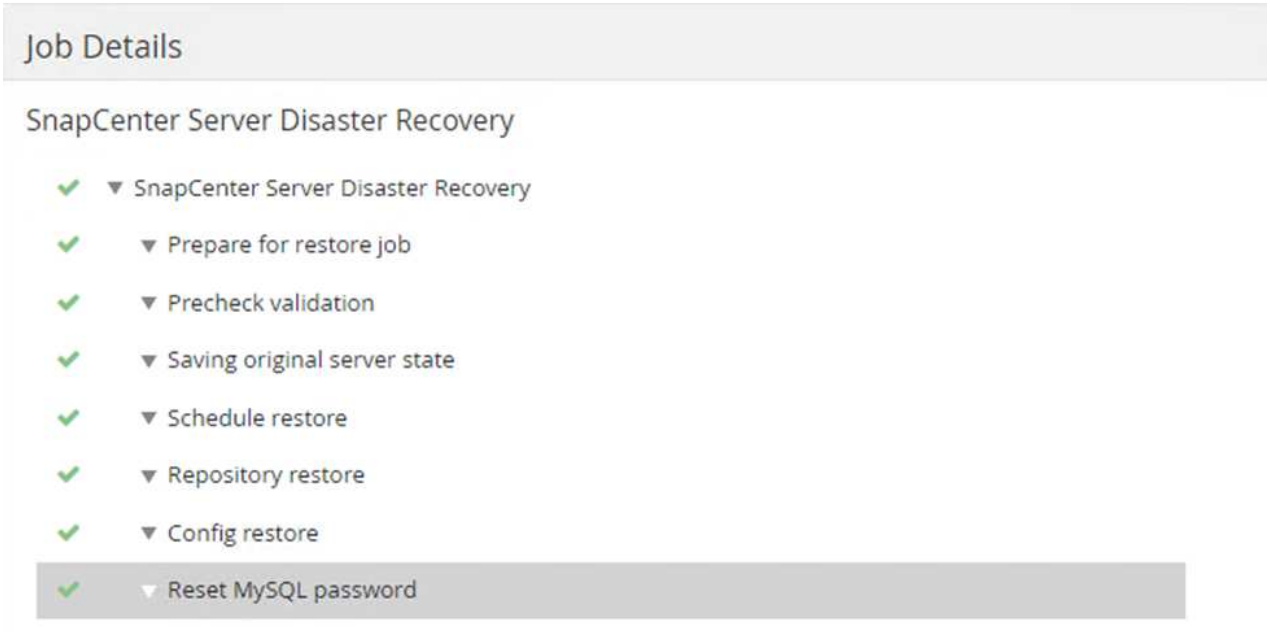


3. Collez le jeton d'autorisation et, dans la section SmDRResterRequest, collez le nom de la sauvegarde et le répertoire local sur le serveur SnapCenter secondaire.



4. Cliquez sur le bouton Exécuter pour lancer le processus de restauration.
5. Dans SnapCenter, accédez à la section moniteur pour afficher la progression de la tâche de restauration.





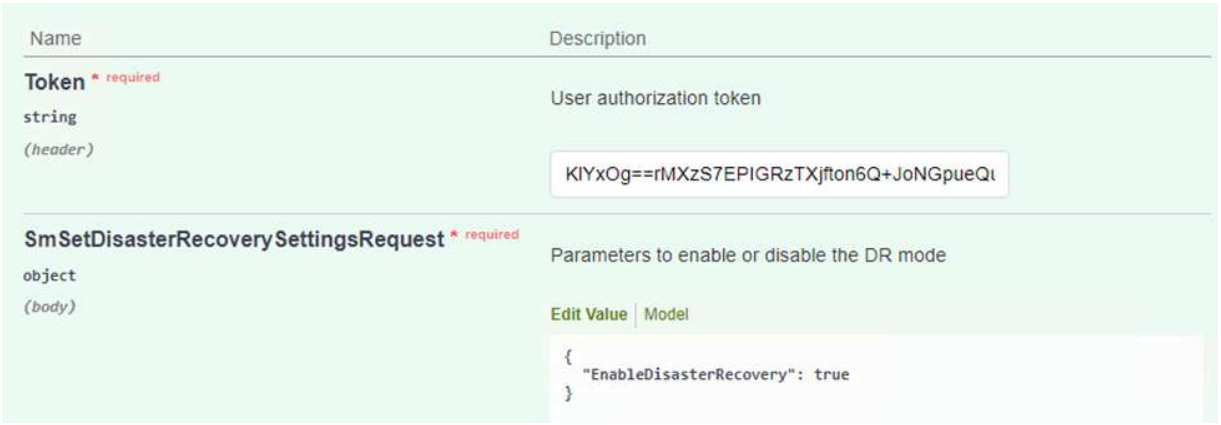
6. Pour activer les restaurations SQL Server à partir du stockage secondaire, vous devez basculer la base de données SnapCenter en mode de reprise après incident. Cette opération est exécutée séparément et lancée sur la page Web de l'API swagger.

   a. Accédez à la section reprise sur incident et cliquez sur `/4.6/disasterrecovery/storage`.

   b. Collez le jeton d'autorisation utilisateur.

   c. Dans la section SmSetDisasterRecovery ySettingRequest, modifiez `EnableDisasterRecover` à `true`.

   d. Cliquez sur Exécuter pour activer le mode de reprise après sinistre pour SQL Server.



Voir les commentaires concernant les procédures supplémentaires.

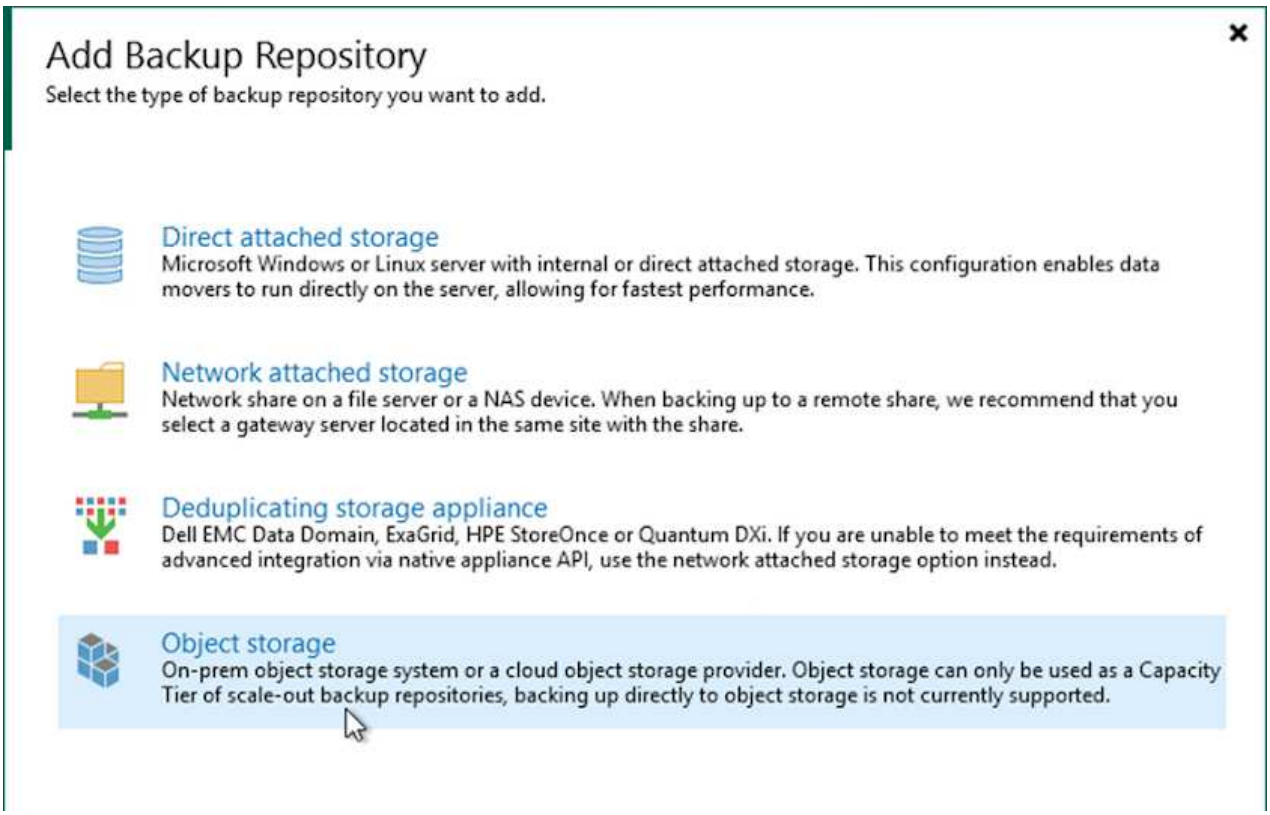
Restauration des VM applications grâce à la restauration complète Veeam

Création d'un référentiel de sauvegardes et importation des sauvegardes à partir de S3

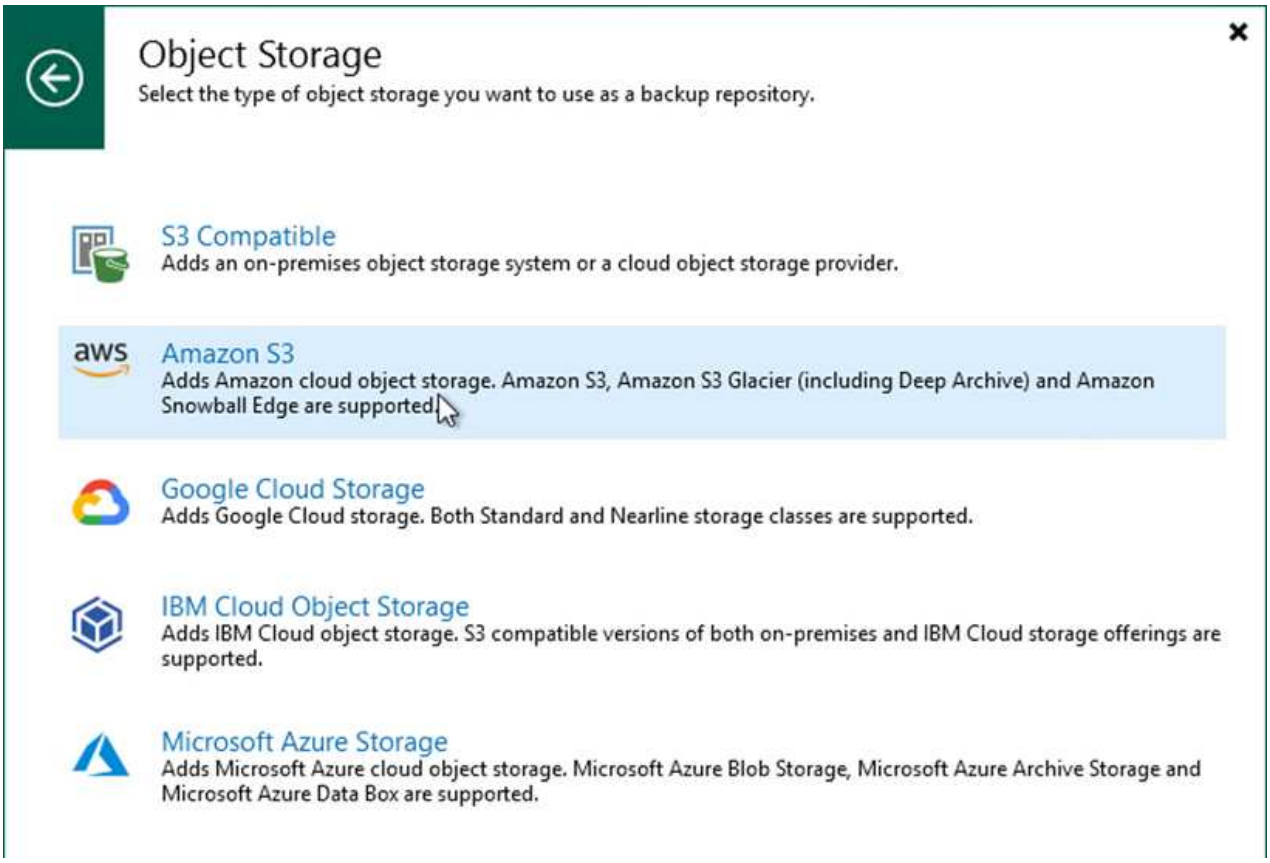
Depuis le serveur Veeam secondaire, importez les sauvegardes depuis le stockage S3 et restaurez les machines virtuelles SQL Server et Oracle sur votre cluster VMware Cloud.

Pour importer les sauvegardes à partir de l'objet S3 inclus dans le référentiel de sauvegarde scale-out sur site, procédez comme suit :

1. Accédez aux référentiels de sauvegarde et cliquez sur Ajouter un référentiel dans le menu supérieur pour lancer l'assistant Ajouter un référentiel de sauvegarde. Sur la première page de l'assistant, sélectionnez stockage objet comme type de référentiel de sauvegarde.

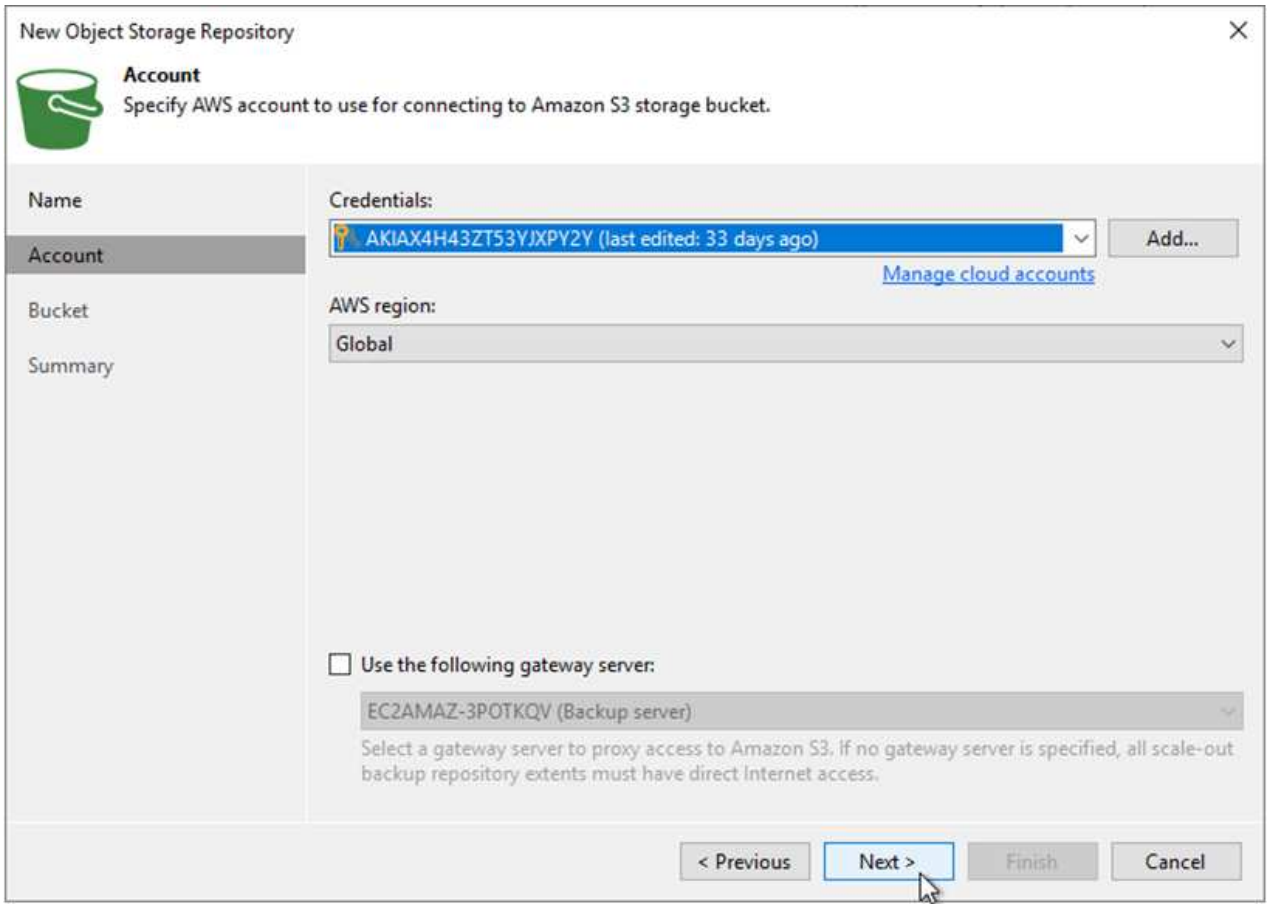


2. Sélectionnez Amazon S3 comme type de stockage objet.

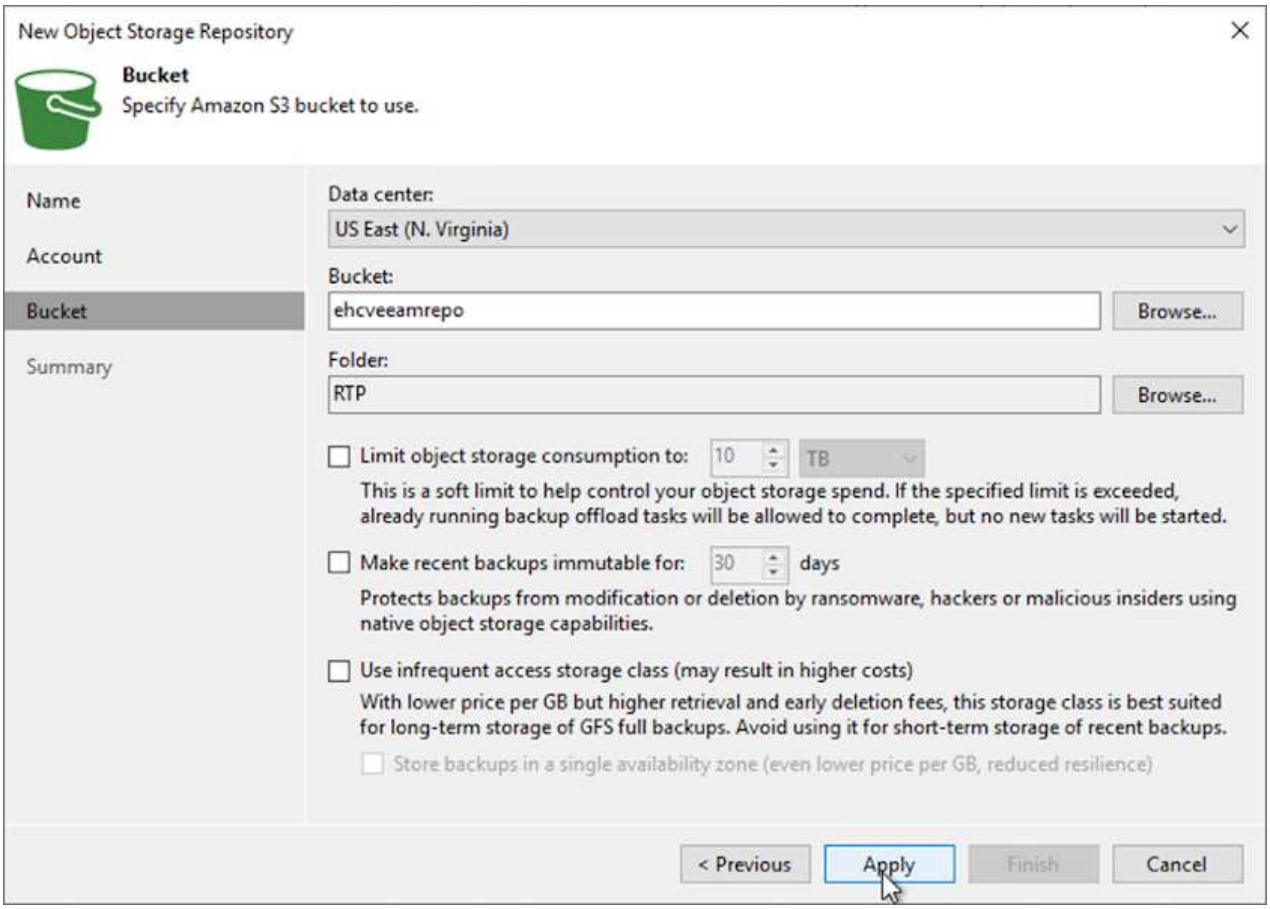


3. Dans la liste d'Amazon Cloud Storage Services, sélectionnez Amazon S3.

4. Sélectionnez vos identifiants pré-saisis dans la liste déroulante ou ajoutez de nouvelles informations d'identification pour accéder à la ressource de stockage cloud. Cliquez sur Suivant pour continuer.



5. Sur la page compartiment, entrez le data Center, le compartiment, le dossier et les options souhaitées. Cliquez sur appliquer.

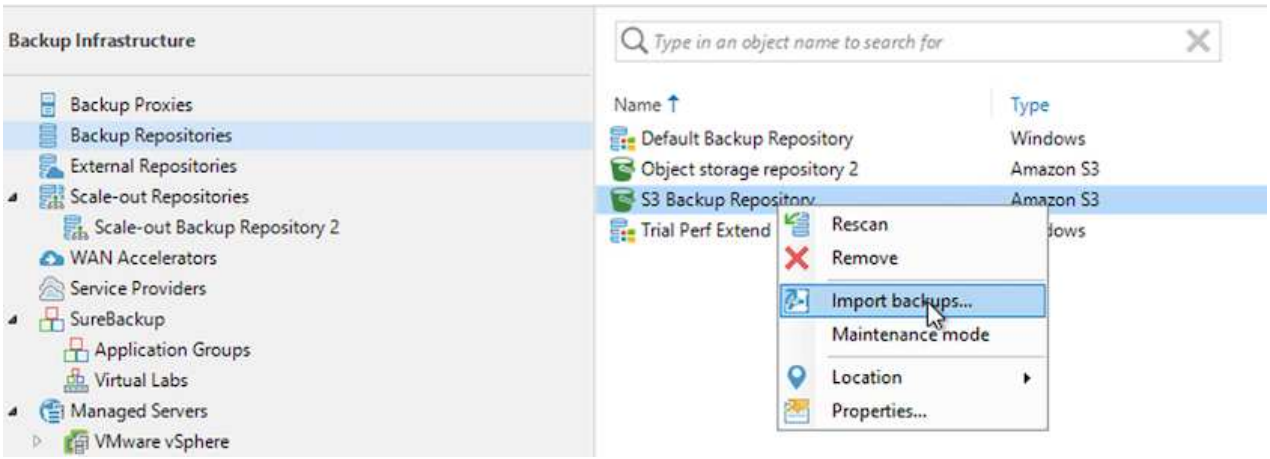


6. Enfin, sélectionnez Terminer pour terminer le processus et ajouter le référentiel.

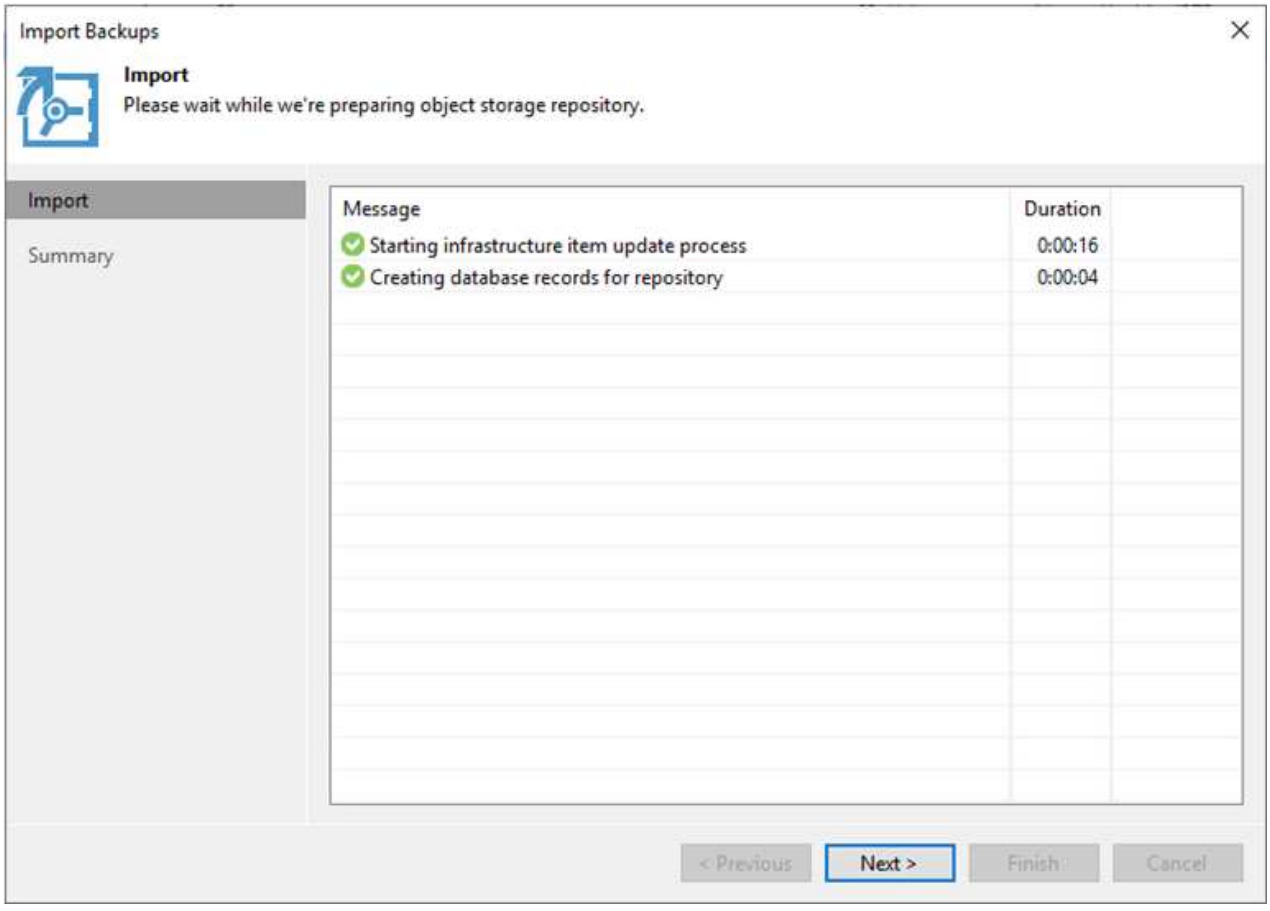
Importation des sauvegardes à partir du stockage objet S3

Pour importer les sauvegardes à partir du référentiel S3 ajouté à la section précédente, procédez comme suit.

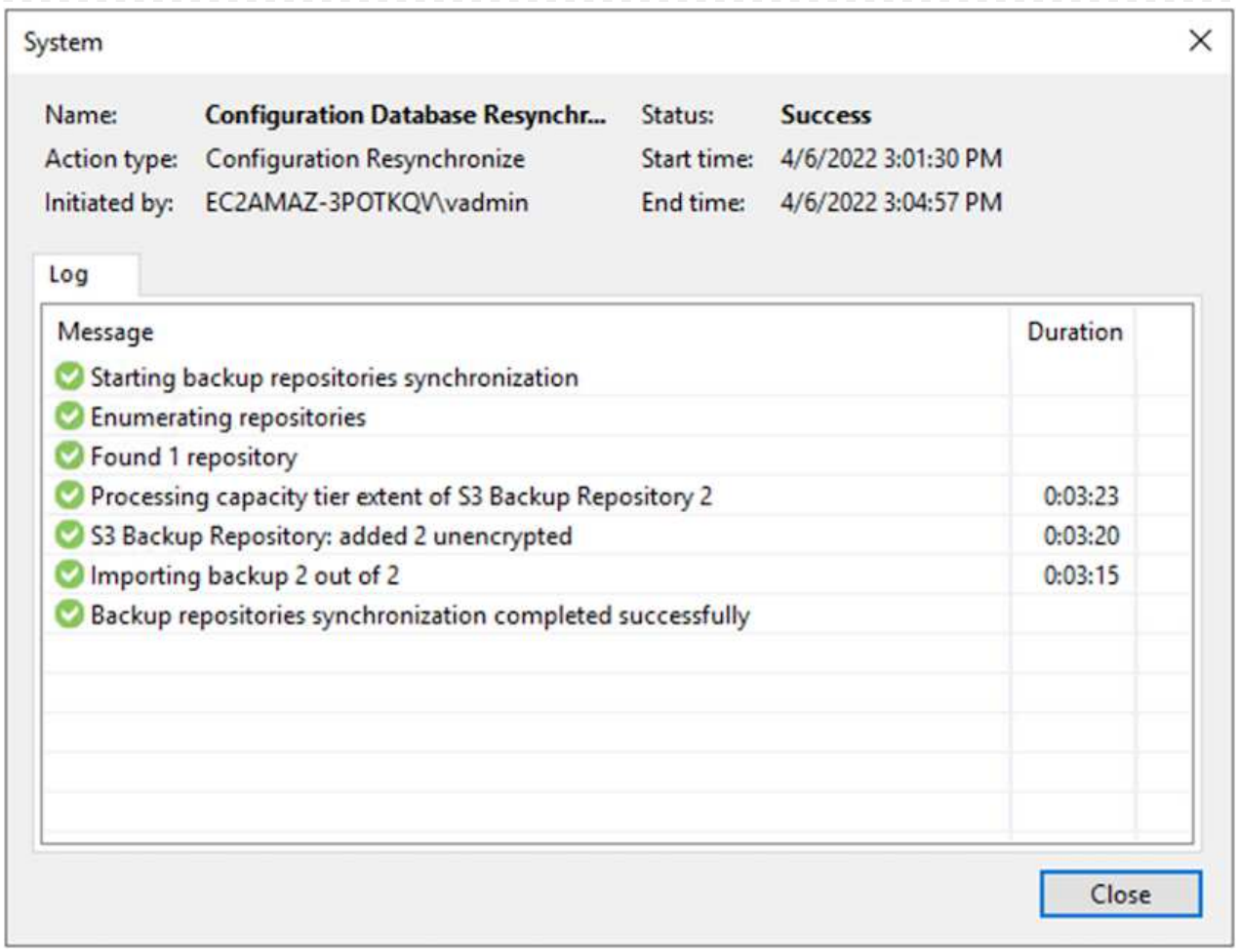
1. Dans le référentiel de sauvegardes S3, sélectionnez Importer les sauvegardes pour lancer l'assistant Importer les sauvegardes.



2. Une fois les enregistrements de la base de données pour l'importation créés, sélectionnez Suivant, puis Terminer à l'écran de résumé pour lancer le processus d'importation.



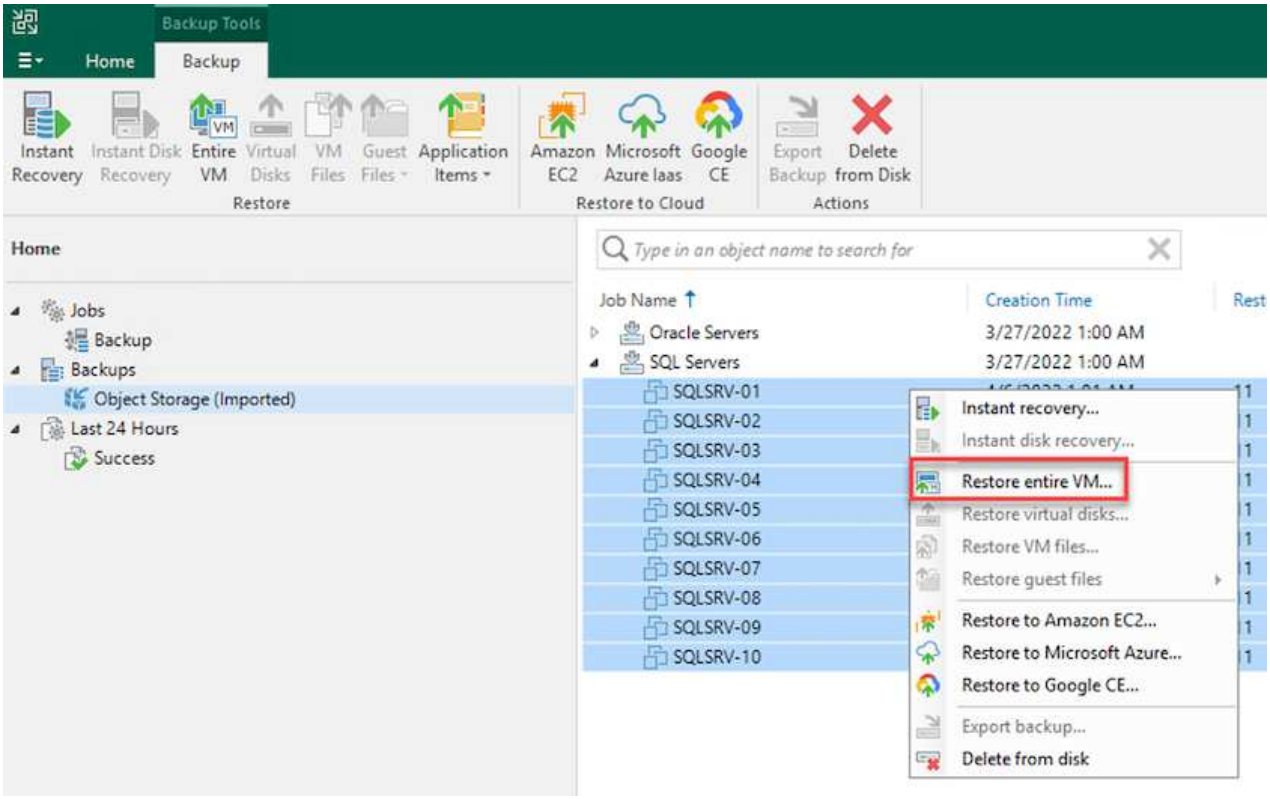
3. Une fois l'importation terminée, vous pouvez restaurer les machines virtuelles dans le cluster VMware Cloud.


System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

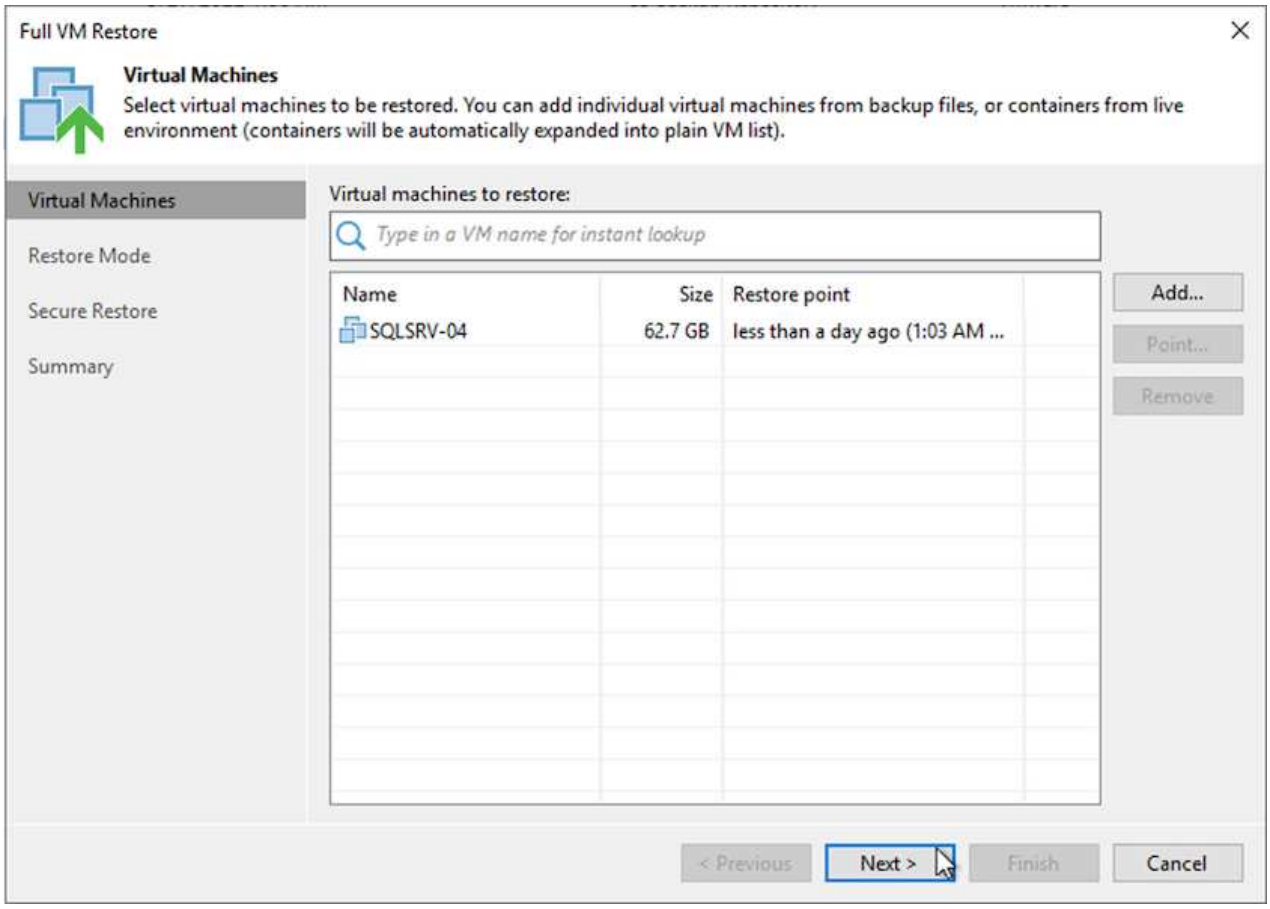
Restauration des VM applicatives avec restauration complète Veeam dans VMware Cloud

Pour restaurer des machines virtuelles SQL et Oracle vers VMware Cloud sur un domaine ou un cluster de workloads avec AWS, effectuez les étapes suivantes.

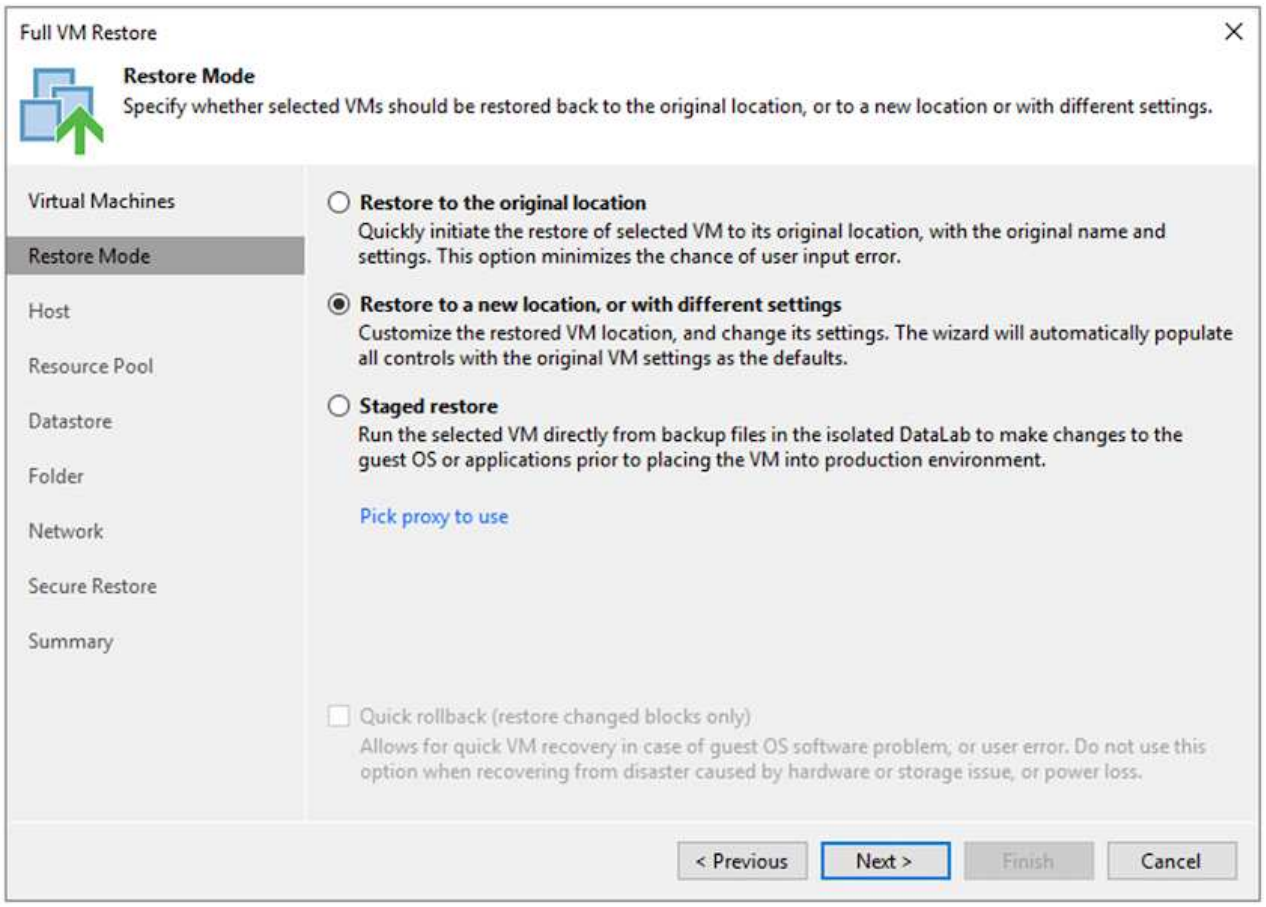
1. Dans la page d'accueil Veeam, sélectionnez le stockage d'objets contenant les sauvegardes importées, sélectionnez les machines virtuelles à restaurer, puis cliquez avec le bouton droit de la souris et sélectionnez Restaurer la machine virtuelle entière.



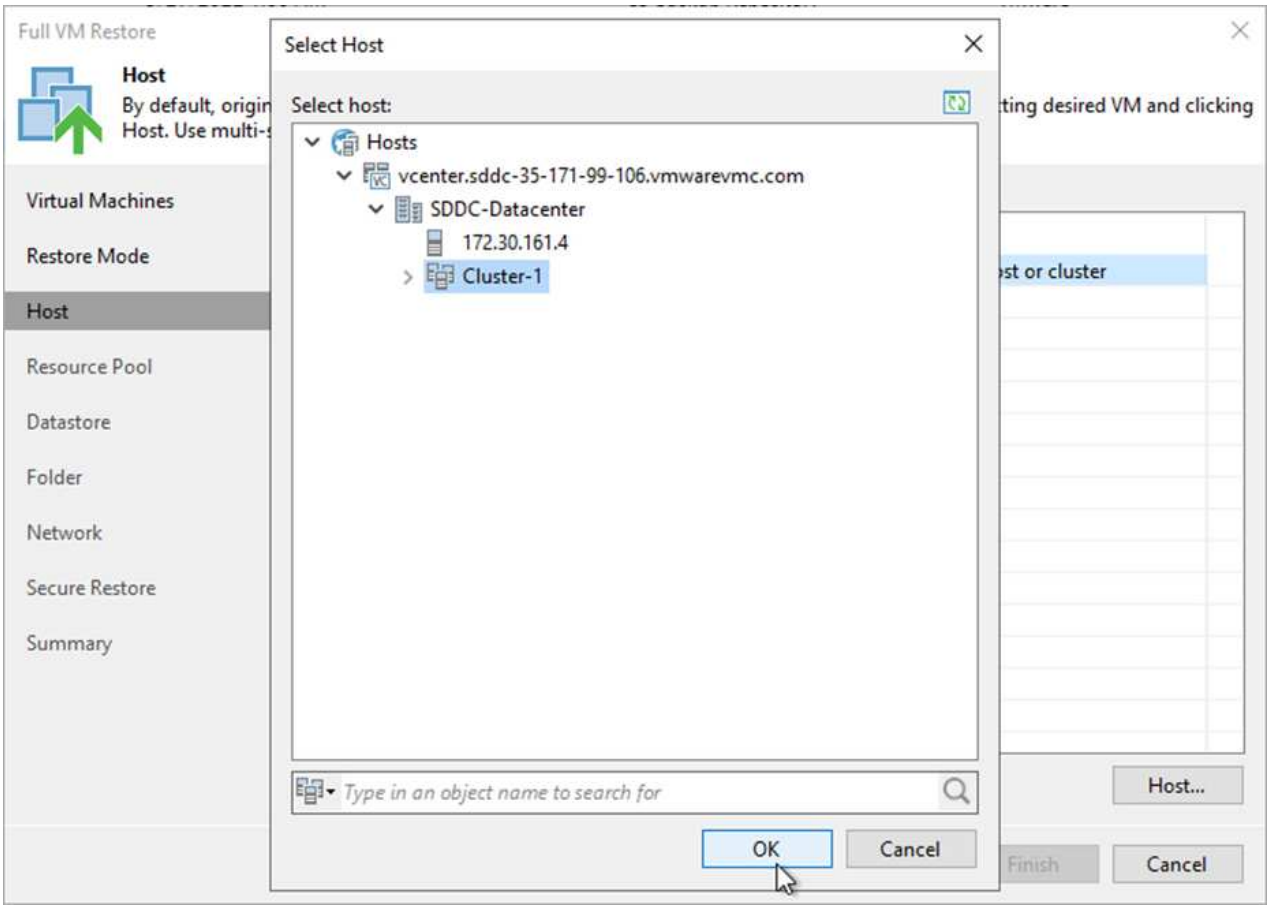
2. Sur la première page de l'assistant de restauration complète de VM, modifiez les VM à sauvegarder si vous le souhaitez et sélectionnez Suivant.



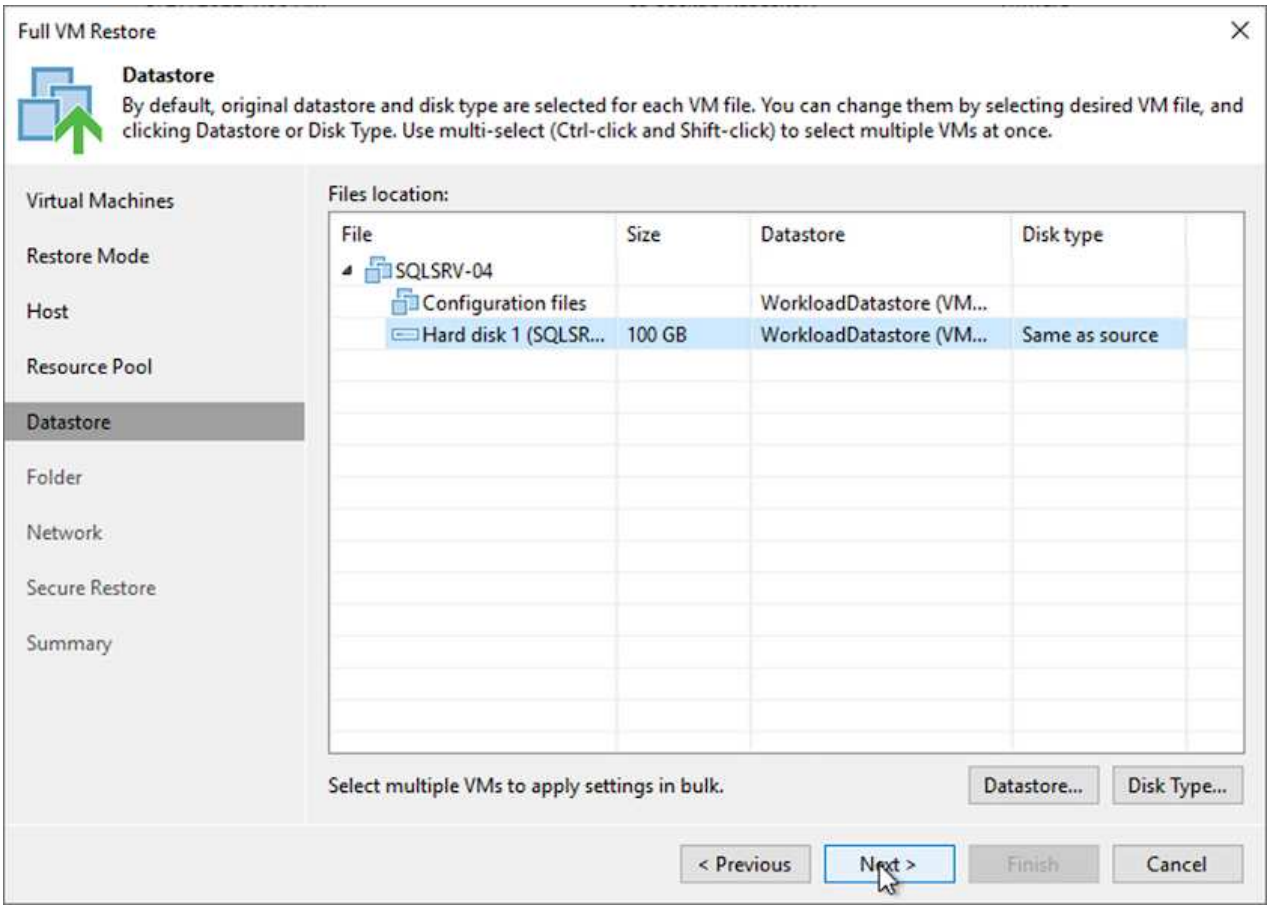
3. Sur la page mode de restauration, sélectionnez Restaurer à un nouvel emplacement ou avec des paramètres différents.



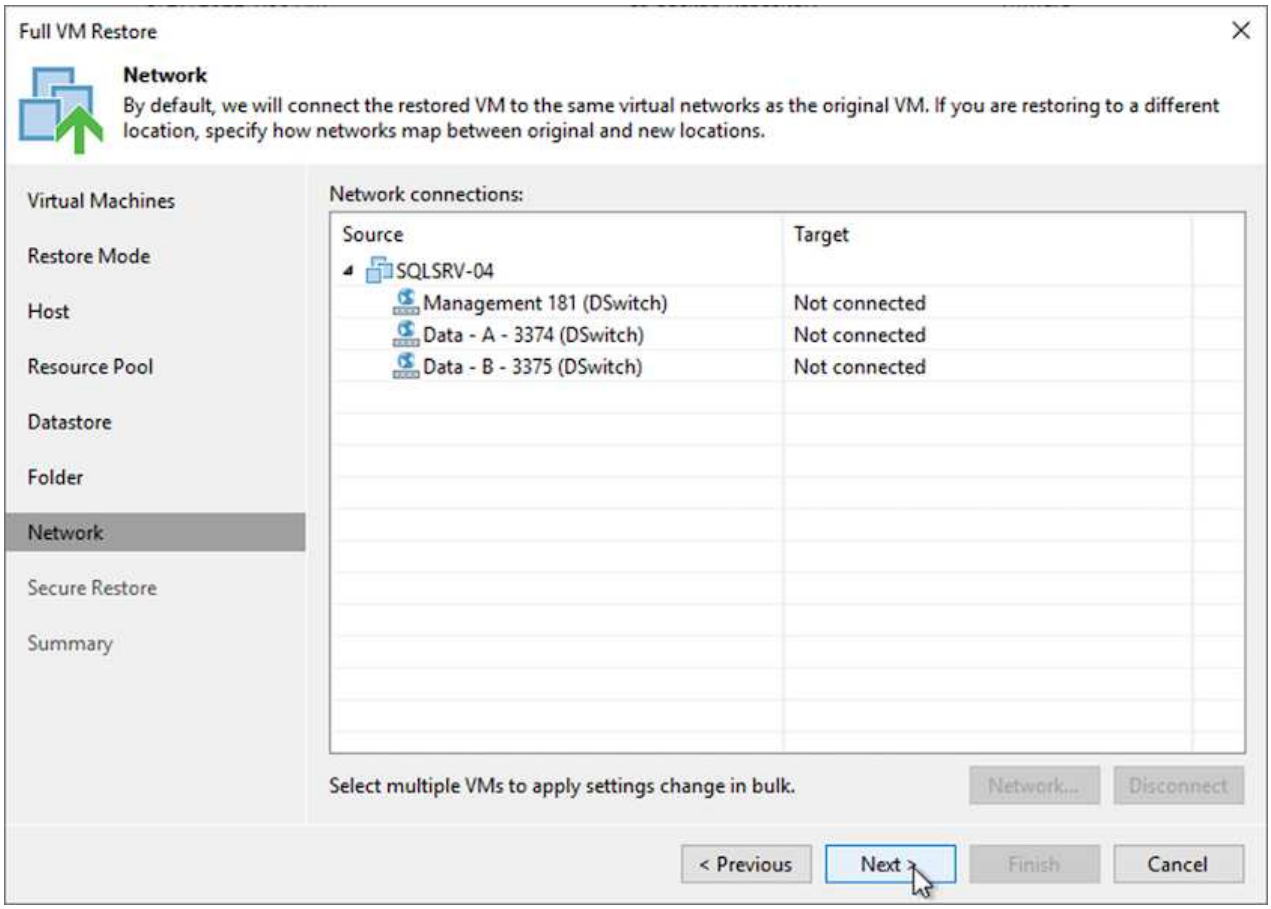
4. Sur la page hôte, sélectionnez l'hôte ou le cluster ESXi cible pour restaurer la machine virtuelle.

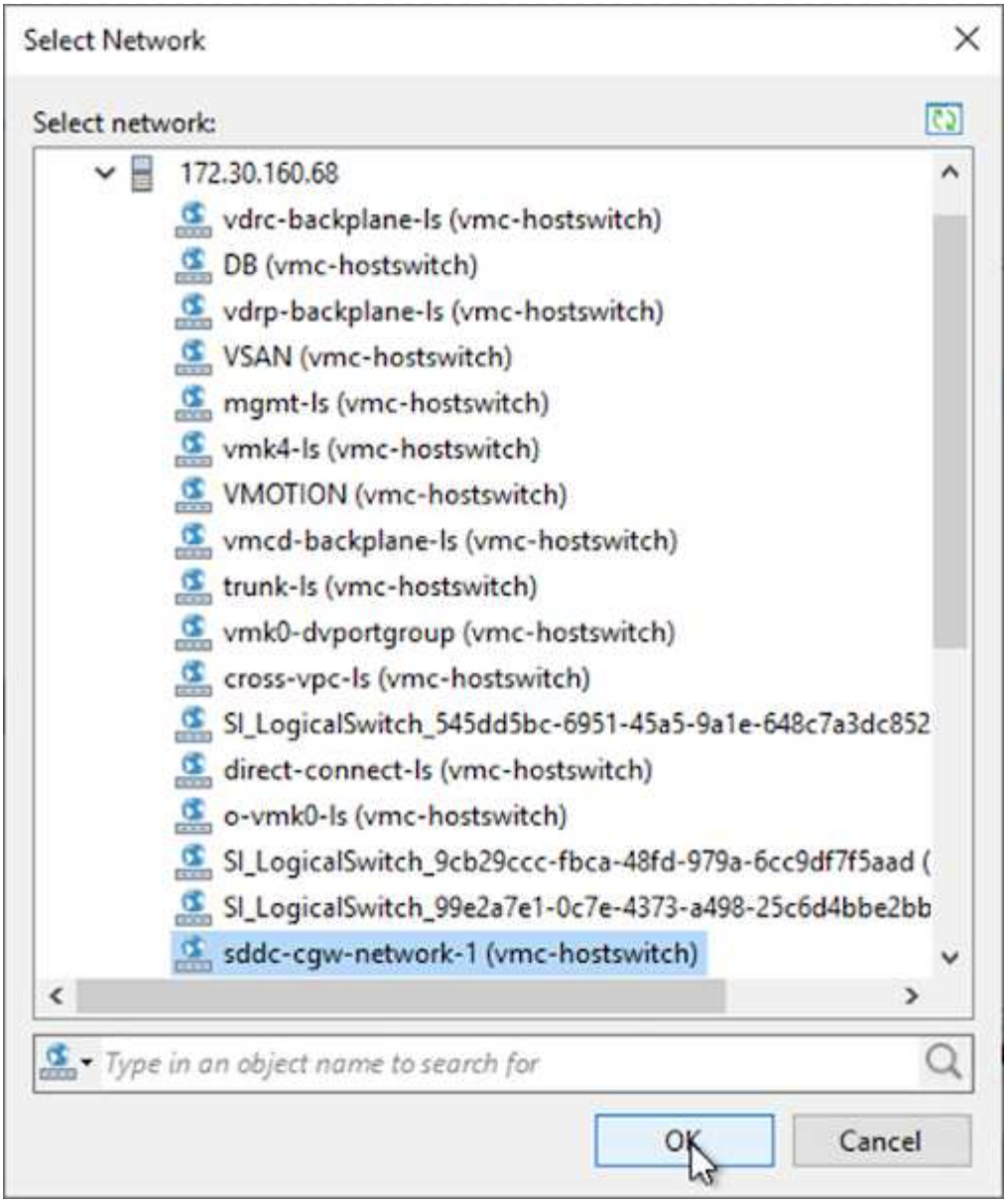


5. Sur la page datastores, sélectionnez l'emplacement du datastore cible pour les fichiers de configuration et le disque dur.



6. Sur la page réseau, mappez les réseaux d'origine sur la machine virtuelle aux réseaux du nouvel emplacement cible.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. Sélectionnez si vous souhaitez analyser la machine virtuelle restaurée à la recherche d'un programme malveillant, consultez la page de résumé et cliquez sur Terminer pour lancer la restauration.

Restaurez les données applicatives SQL Server

Le processus suivant explique comment restaurer un serveur SQL dans VMware Cloud Services dans AWS en cas d'incident rendant le site inutilisable.

Les prérequis suivants sont supposés être terminés pour poursuivre les étapes de restauration :

1. La machine virtuelle Windows Server a été restaurée dans le SDDC VMware Cloud à l'aide de Veeam Full Restore.
2. Un serveur SnapCenter secondaire a été établi et la restauration et la configuration de la base de données SnapCenter ont été effectuées en suivant les étapes décrites dans la section "Récapitulatif du processus de sauvegarde et de restauration SnapCenter."

VM : configuration post-restauration pour SQL Server VM

Une fois la restauration de la machine virtuelle terminée, vous devez configurer la mise en réseau et d'autres éléments en vue de redécouvrir la machine virtuelle hôte dans SnapCenter.

1. Attribuez de nouvelles adresses IP pour la gestion et iSCSI ou NFS.
2. Joignez l'hôte au domaine Windows.
3. Ajoutez les noms d'hôte au serveur DNS ou au fichier hosts du serveur SnapCenter.

> Si le plug-in SnapCenter a été déployé avec des informations d'identification de domaine différentes du domaine actuel, vous devez modifier le compte connexion pour le service Plug-in pour Windows sur la machine virtuelle SQL Server. Après avoir modifié le compte de connexion, redémarrez SnapCenter les services SMCore, Plug-in pour Windows et Plug-in pour SQL Server.

> Pour redécouvrir automatiquement les machines virtuelles restaurées dans SnapCenter, le FQDN doit être identique à la machine virtuelle qui a été ajoutée à l'origine au système SnapCenter sur site.

Configurez le stockage FSX pour la restauration SQL Server

Pour mettre en œuvre le processus de restauration de reprise après incident pour une machine virtuelle SQL Server, vous devez interrompre la relation SnapMirror existante à partir du cluster FSX et accorder l'accès au volume. Pour ce faire, procédez comme suit.

1. Pour interrompre la relation SnapMirror existante pour les volumes de base de données SQL Server et de journaux, exécutez la commande suivante à partir de la CLI FSX :

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Autoriser l'accès à la LUN en créant un groupe initiateur contenant l'IQN iSCSI de la machine virtuelle SQL Server Windows :

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

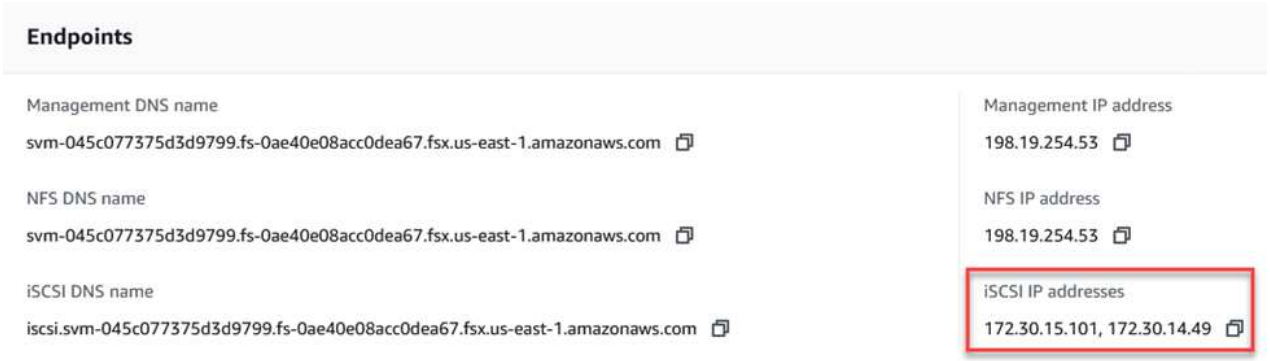
3. Enfin, mappez les LUN sur le groupe initiateur que vous venez de créer :

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

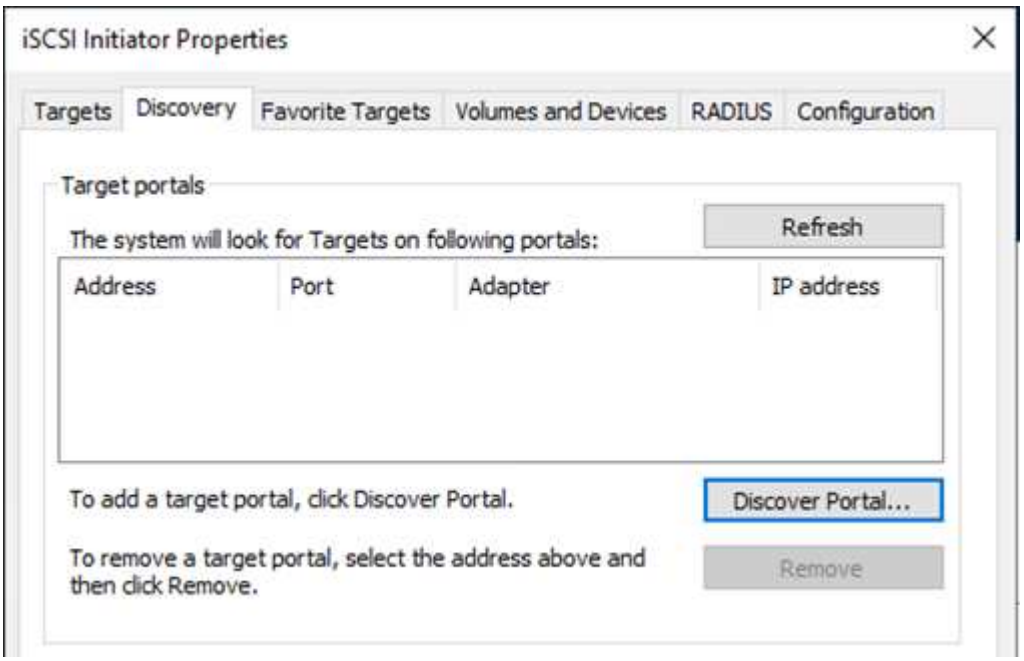
4. Pour trouver le nom du chemin d'accès, exécutez le `lun show` commande.

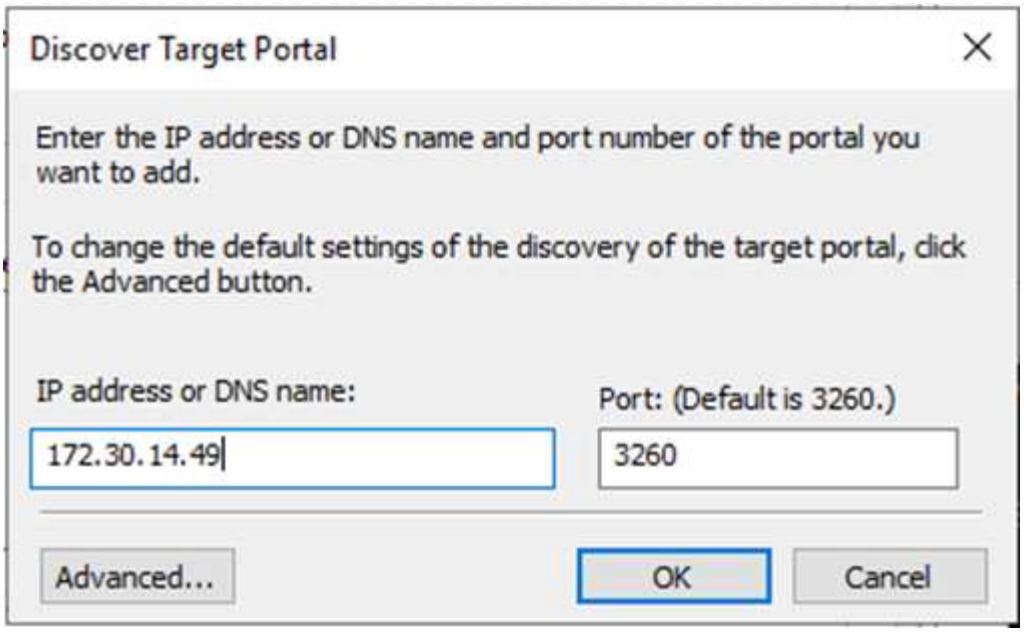
Configurer la machine virtuelle Windows pour l'accès iSCSI et découvrir les systèmes de fichiers

1. À partir de la VM SQL Server, configurez votre carte réseau iSCSI pour communiquer sur le Port Group VMware qui a été établi avec la connectivité aux interfaces cibles iSCSI de votre instance FSX.
2. Ouvrez l'utilitaire iSCSI Initiator Properties (Propriétés de l'initiateur iSCSI) et effacez les anciens paramètres de connectivité dans les onglets Discovery, Favorite Targets (cibles favorites) et Targets (cibles).
3. Recherchez les adresses IP permettant d'accéder à l'interface logique iSCSI sur l'instance/le cluster FSX. Cela peut être trouvé dans la console AWS, sous Amazon FSX > ONTAP > Storage Virtual machines.

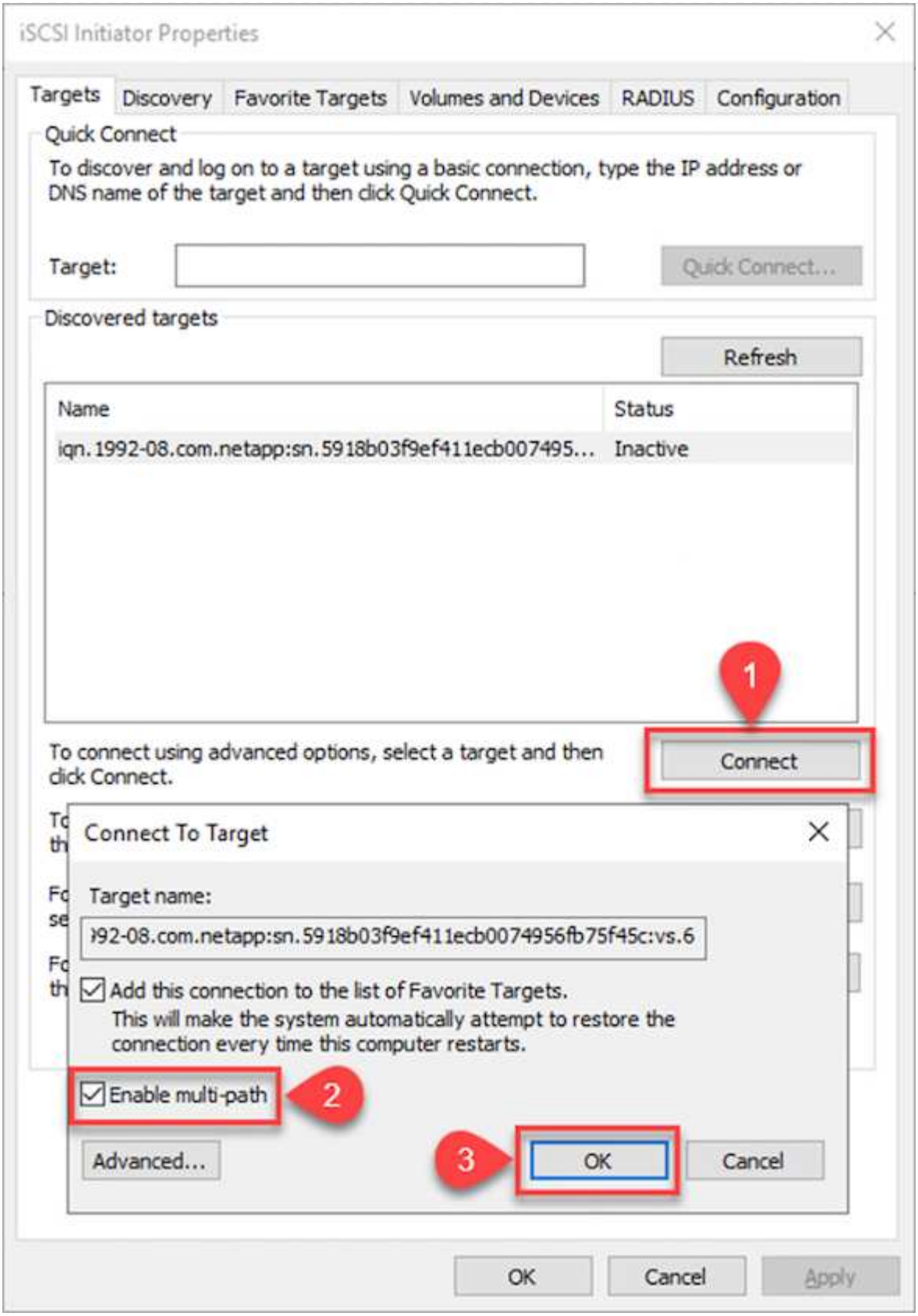


4. Dans l'onglet découverte, cliquez sur Discover Portal et entrez les adresses IP de vos cibles iSCSI FSX.

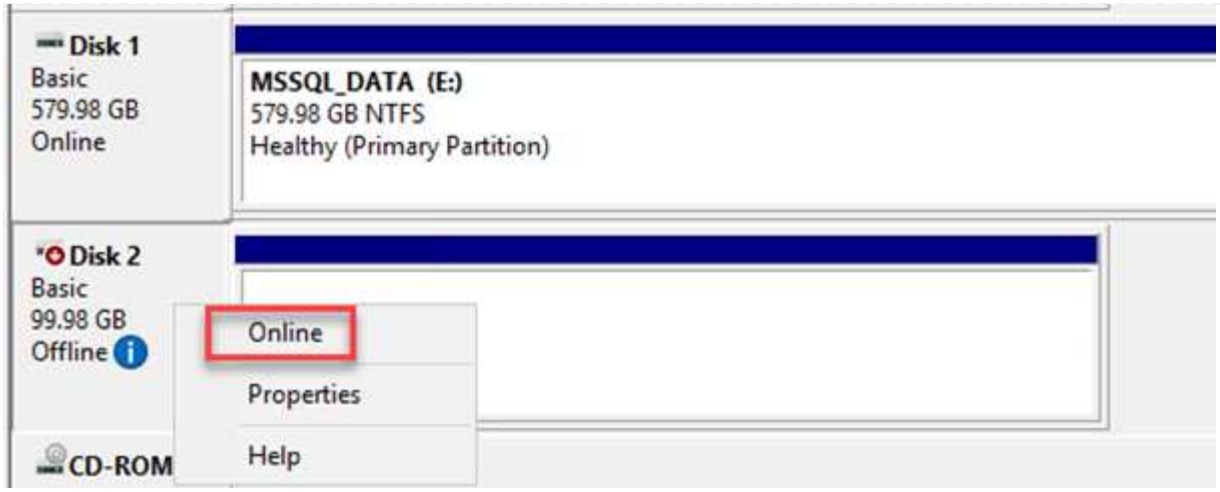




5. Dans l'onglet cible, cliquez sur connecter, sélectionnez Activer le multichemin si nécessaire pour votre configuration, puis cliquez sur OK pour vous connecter à la cible.

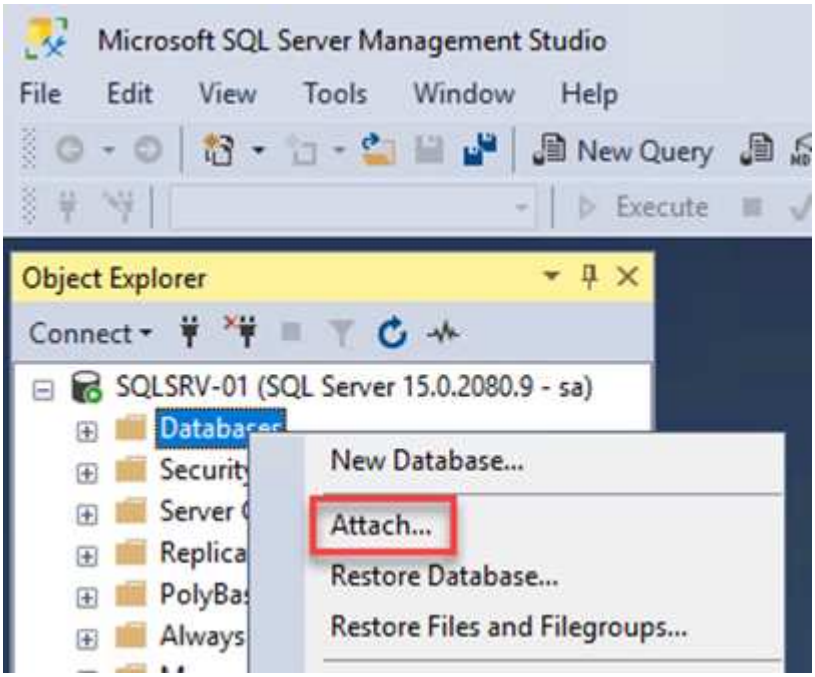


6. Ouvrez l’utilitaire gestion de l’ordinateur et connectez les disques. Vérifiez qu’ils conservent les mêmes lettres de lecteur qu’ils étaient auparavant.

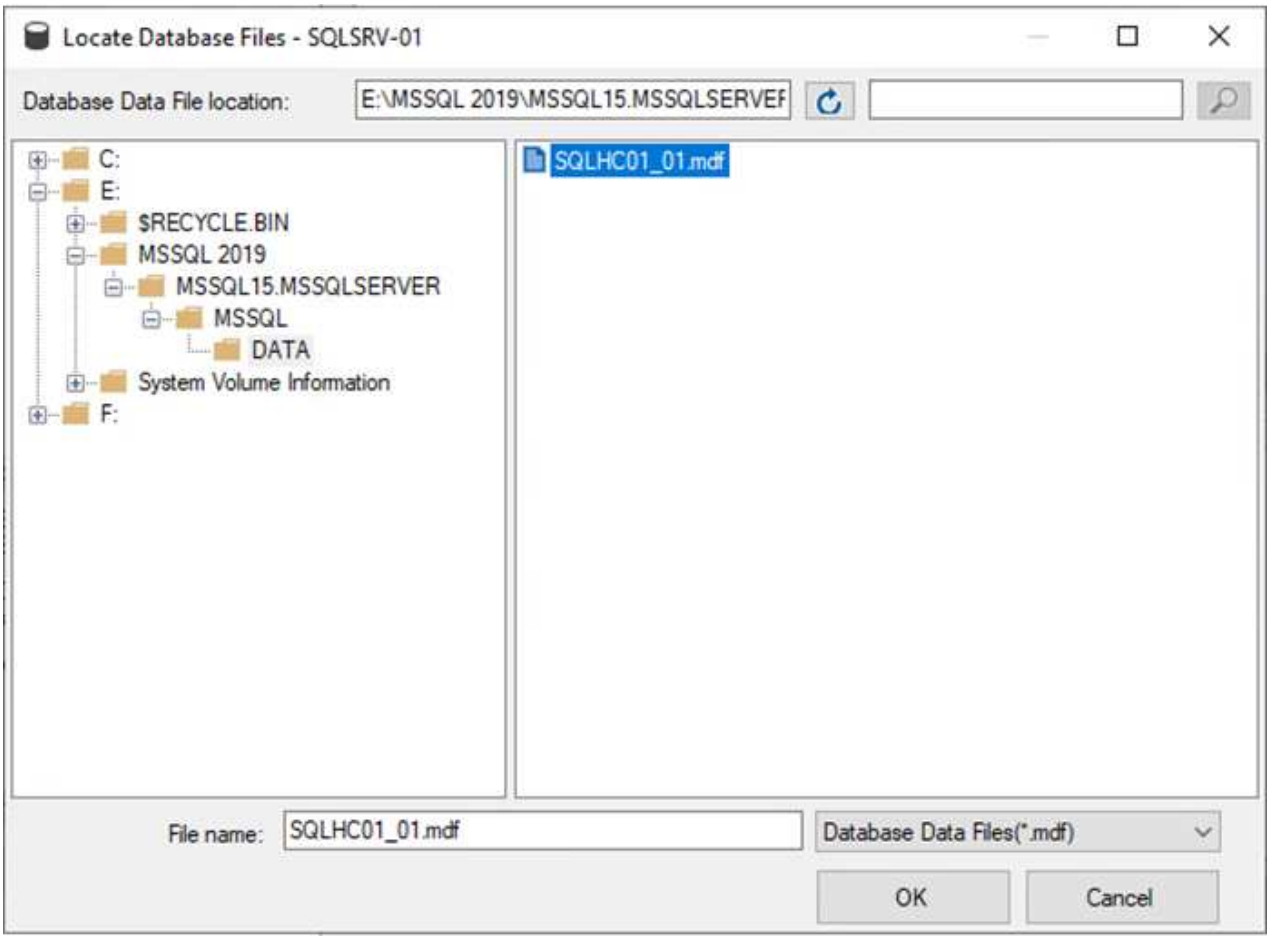

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Reliez les bases de données SQL Server

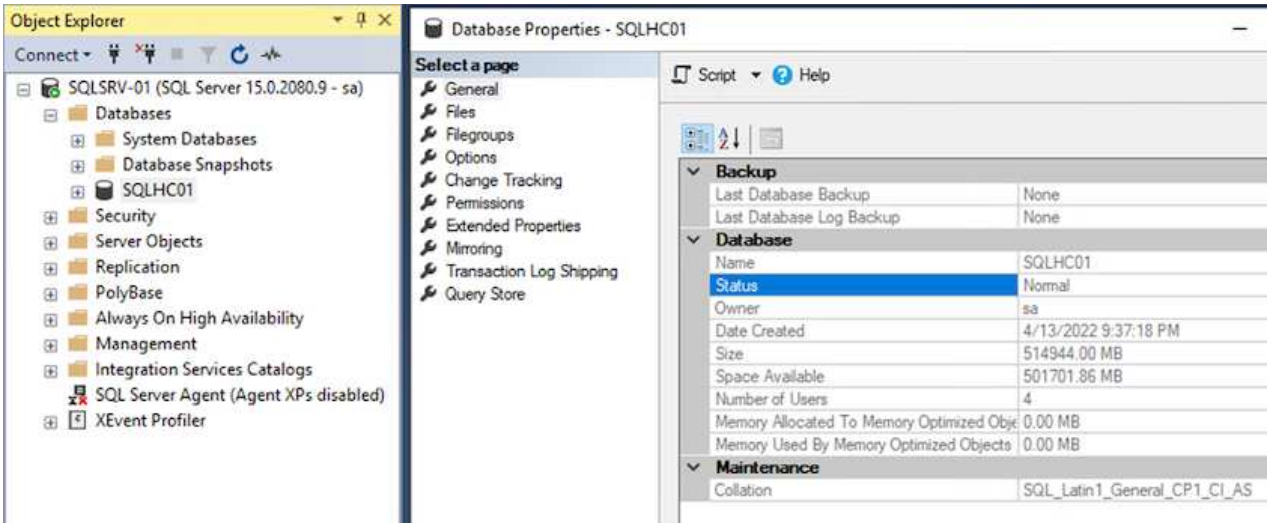
1. À partir de la VM SQL Server, ouvrez Microsoft SQL Server Management Studio et sélectionnez attacher pour démarrer le processus de connexion à la base de données.



2. Cliquez sur Ajouter et naviguez jusqu'au dossier contenant le fichier de base de données primaire SQL Server, sélectionnez-le, puis cliquez sur OK.



3. Si les journaux de transactions se trouvent sur un lecteur distinct, choisissez le dossier qui contient le journal de transactions.
4. Lorsque vous avez terminé, cliquez sur OK pour joindre la base de données.

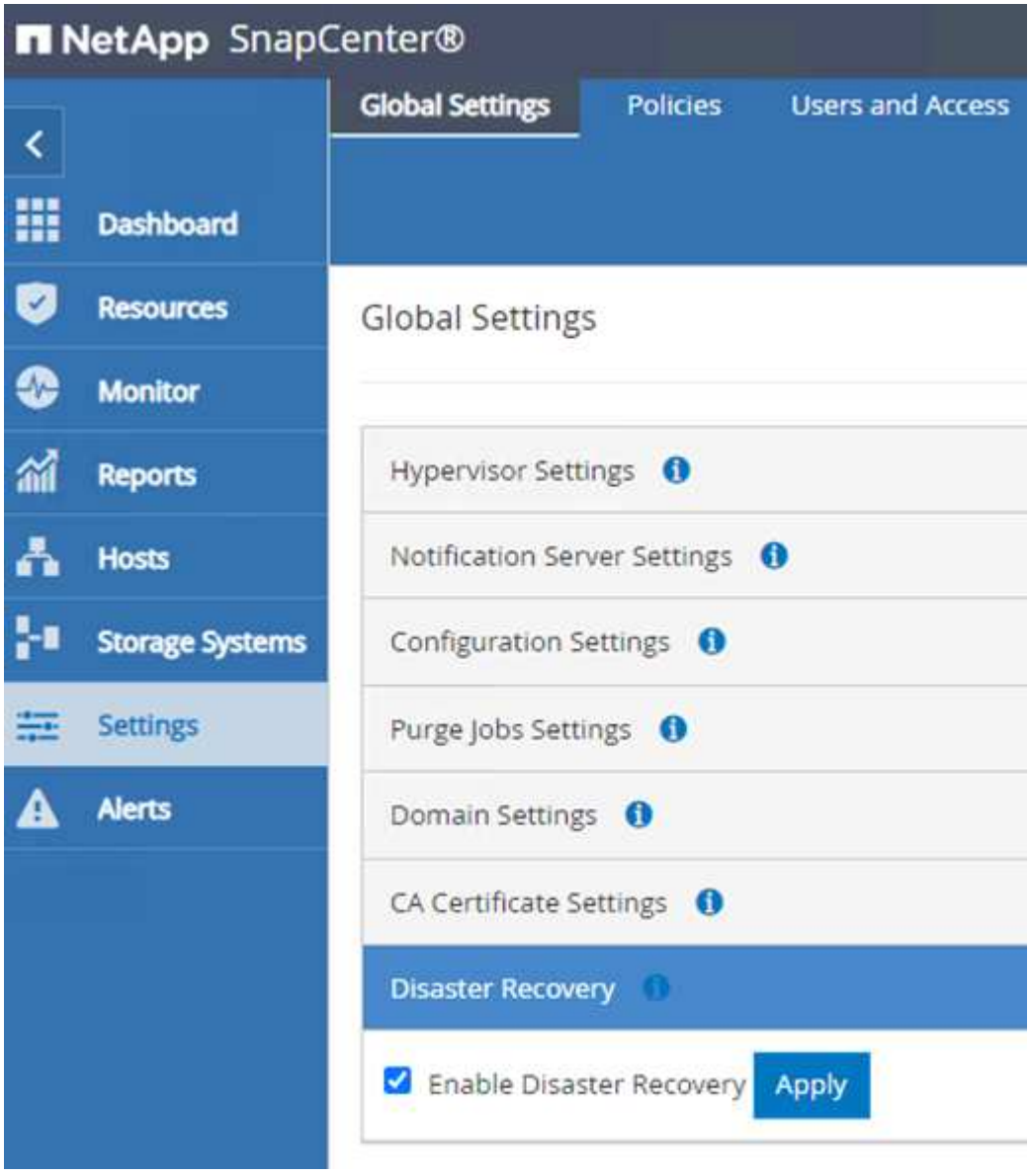


Confirmez la communication SnapCenter avec le plug-in SQL Server

Une fois la base de données SnapCenter restaurée à son état précédent, elle redécouvre automatiquement les hôtes SQL Server. Pour que cela fonctionne correctement, gardez à l'esprit les conditions préalables suivantes :

- SnapCenter doit être placé en mode de reprise après incident. Ceci peut être réalisé via l'API swagger ou dans Paramètres globaux sous récupération après sinistre.
- Le FQDN de SQL Server doit être identique à l'instance qui s'exécutait dans le data Center sur site.
- La relation SnapMirror d'origine doit être rompue.
- Les LUN contenant la base de données doivent être montés sur l'instance SQL Server et la base de données attachée.

Pour confirmer que SnapCenter est en mode reprise après sinistre, accédez à Paramètres depuis le client Web SnapCenter. Accédez à l'onglet Paramètres globaux, puis cliquez sur reprise après sinistre. Assurez-vous que la case Activer la reprise après sinistre est activée.



Restaurez les données de l'application Oracle

Le processus suivant explique comment restaurer les données d'application Oracle dans VMware Cloud Services dans AWS en cas d'incident rendant le site inutilisable.

Pour continuer les étapes de récupération, suivez les conditions préalables suivantes :

1. La machine virtuelle du serveur Oracle Linux a été restaurée dans le SDDC VMware Cloud à l'aide de Veeam Full Restore.
2. Un serveur SnapCenter secondaire a été établi et la base de données SnapCenter et les fichiers de configuration ont été restaurés à l'aide des étapes décrites dans cette section "Récapitulatif du processus de sauvegarde et de restauration SnapCenter."

Configurer FSX pour la restauration Oracle – interrompre la relation SnapMirror

Pour rendre les volumes de stockage secondaire hébergés sur l'instance FSxN accessibles aux serveurs Oracle, vous devez d'abord interrompre la relation SnapMirror existante.

1. Après avoir ouvert une session dans la CLI FSX, exécutez la commande suivante pour afficher les volumes filtrés par le nom correct.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

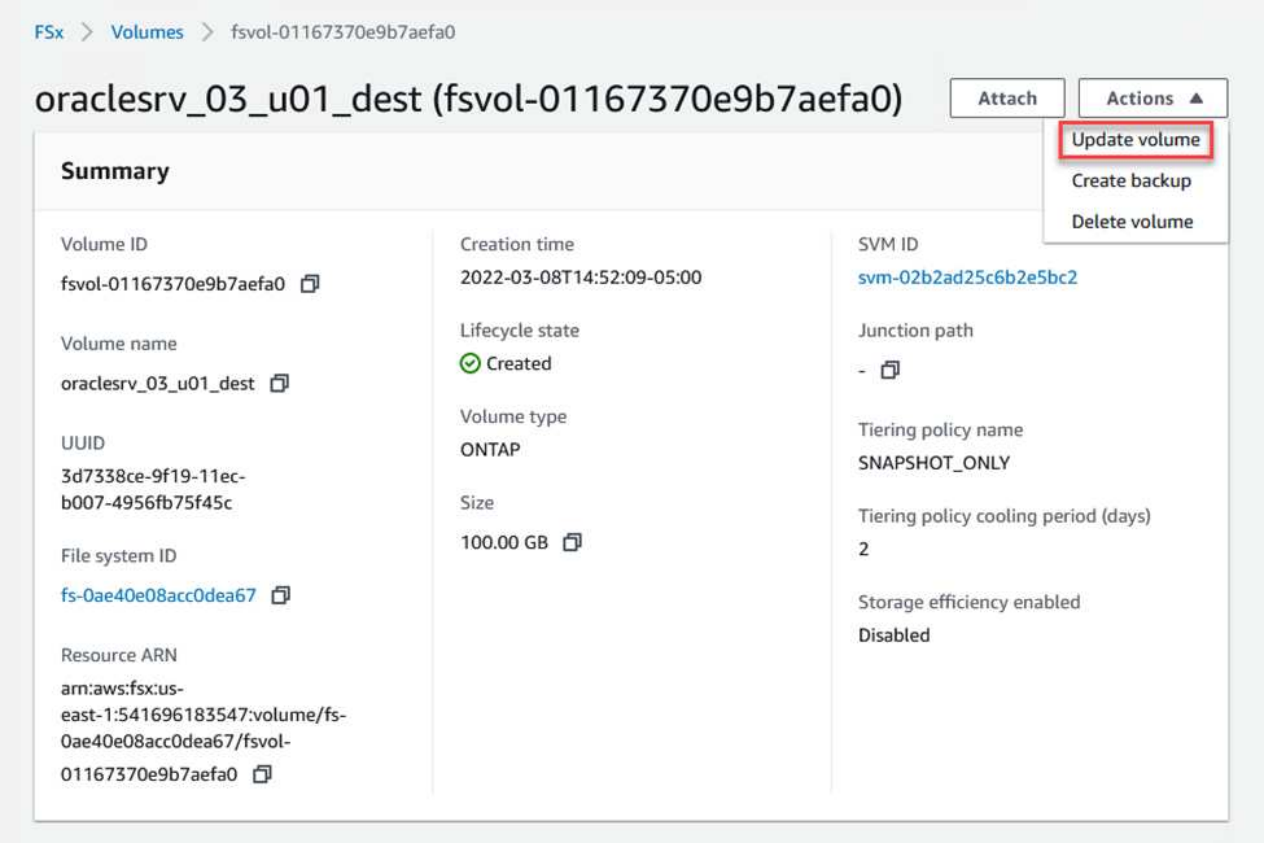
2. Exécutez la commande suivante pour interrompre les relations SnapMirror existantes.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

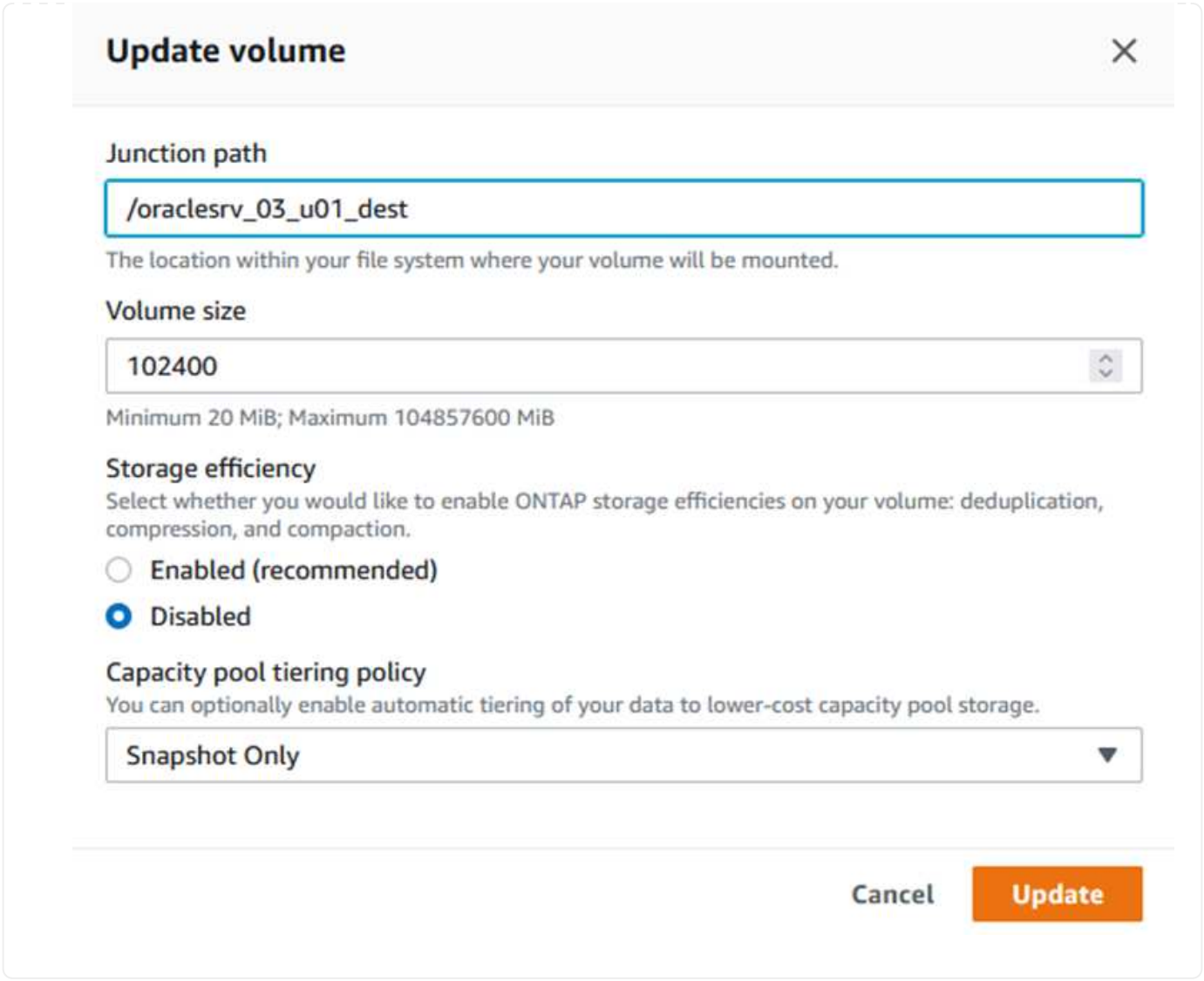
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Mettez à jour le chemin de jonction dans le client Web Amazon FSX :



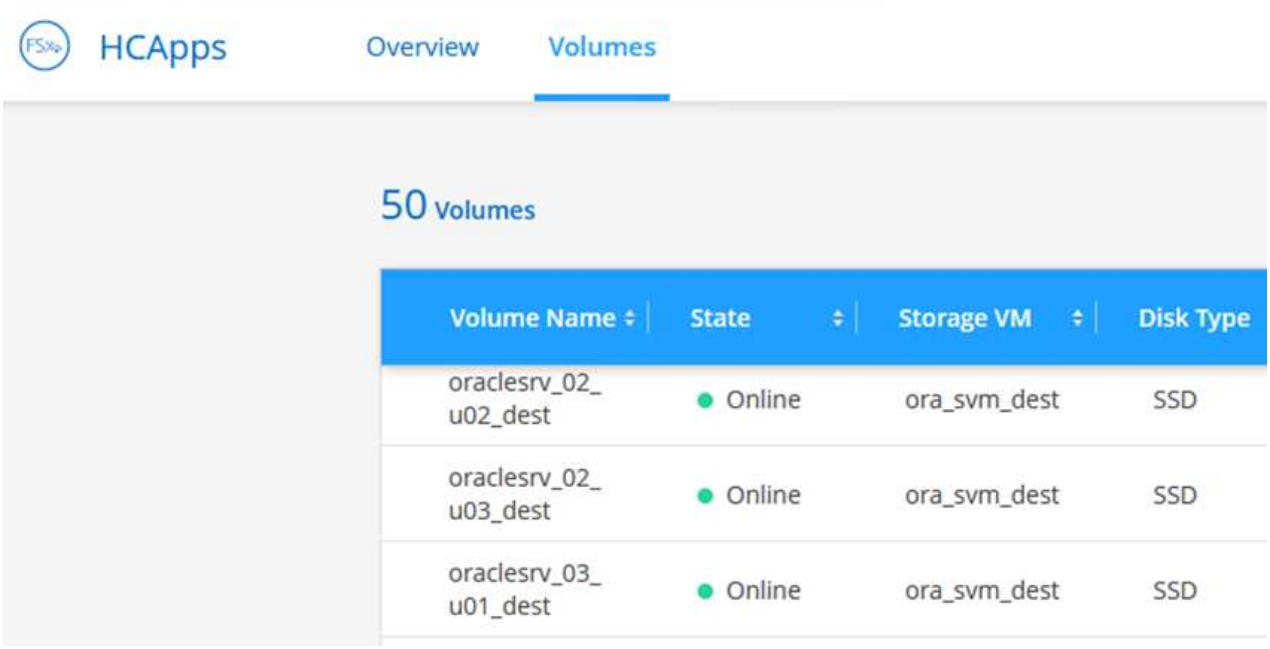
4. Ajoutez le nom du chemin de jonction et cliquez sur mettre à jour. Préciser cette Junction path lors du montage du volume NFS depuis le serveur Oracle.


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

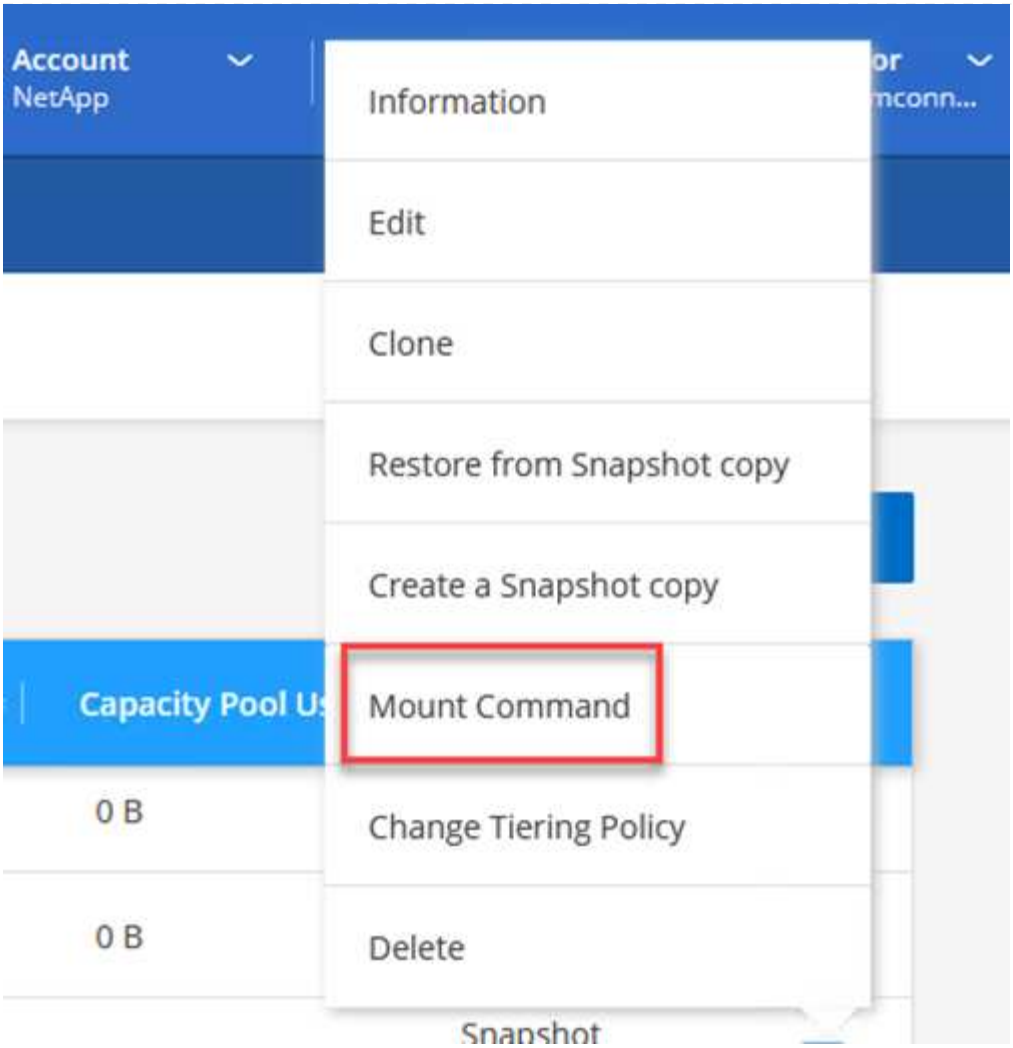
Montez les volumes NFS sur Oracle Server

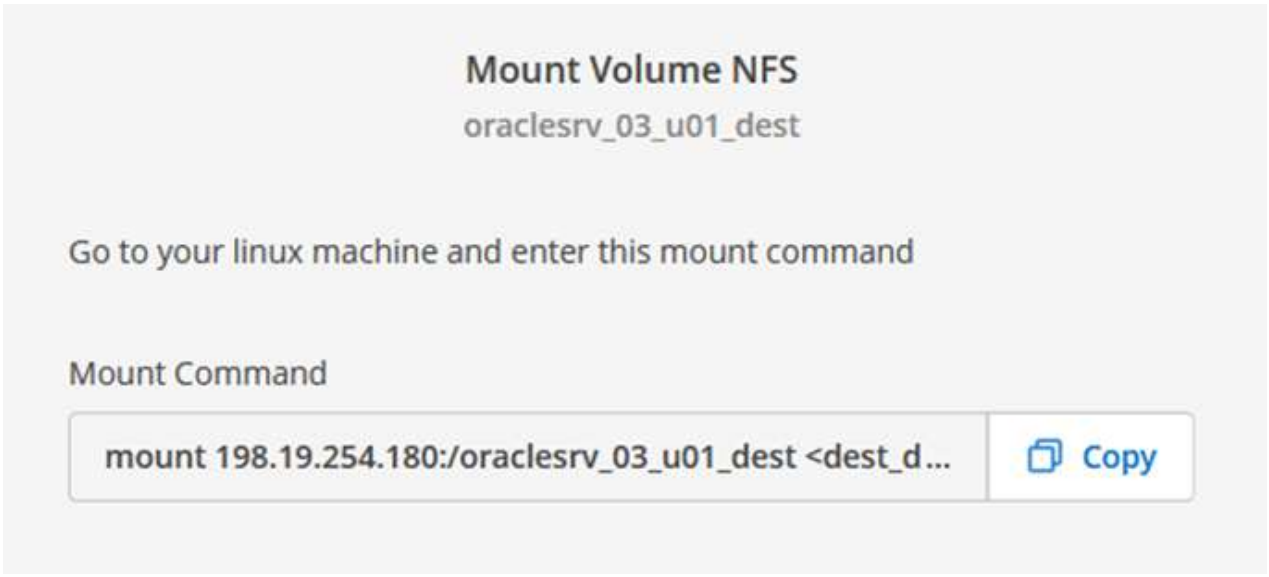
Dans Cloud Manager, vous pouvez obtenir la commande mount avec l'adresse IP correcte de la LIF NFS pour le montage des volumes NFS qui contiennent les fichiers et les journaux de la base de données Oracle.

1. Dans Cloud Manager, accédez à la liste des volumes de votre cluster FSX.



2. Dans le menu d'action, sélectionnez la commande Mount pour afficher et copier la commande mount à utiliser sur notre serveur Oracle Linux.





3. Montez le système de fichiers NFS sur le serveur Oracle Linux. Les répertoires de montage du partage NFS existent déjà sur l'hôte Oracle Linux.
4. À partir du serveur Oracle Linux, utilisez la commande mount pour monter les volumes NFS.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Répétez cette étape pour chaque volume associé aux bases de données Oracle.

Pour rendre le montage NFS persistant au redémarrage, modifiez le `/etc/fstab` fichier à inclure les commandes de montage.

5. Redémarrez le serveur Oracle. Les bases de données Oracle doivent démarrer normalement et être disponibles pour une utilisation.

Du rétablissement

Une fois le processus de basculement terminé avec succès dans cette solution, SnapCenter et Veeam reprendre leurs fonctions de sauvegarde s'exécutant dans AWS, et FSX pour ONTAP est désormais désigné comme stockage principal sans relation SnapMirror avec le data Center sur site d'origine. Une fois le fonctionnement normal rétabli sur site, vous pouvez utiliser un processus identique à celui décrit dans la présente documentation pour reproduire les données sur le système de stockage ONTAP sur site.

Comme indiqué dans cette documentation, vous pouvez configurer SnapCenter de manière à mettre en miroir les volumes de données d'application de FSX pour ONTAP vers un système de stockage ONTAP résidant sur site. De la même façon, vous pouvez configurer Veeam pour répliquer les copies de sauvegarde vers Amazon S3 à l'aide d'un référentiel de sauvegarde scale-out. Ainsi, ces sauvegardes sont accessibles à un serveur de sauvegarde Veeam résidant dans le data Center sur site.

Le basculement automatique ne fait pas partie du périmètre de ces documents, mais le retour arrière diffère légèrement du processus détaillé présenté ici.

Conclusion

Le cas d'utilisation présenté dans cette documentation est axé sur les technologies de reprise sur incident qui ont fait leurs preuves et qui mettent en avant l'intégration entre NetApp et VMware. Les systèmes de stockage NetApp ONTAP fournissent des technologies de mise en miroir des données éprouvées qui permettent aux entreprises de concevoir des solutions de reprise après incident s'intégrant aux technologies ONTAP et sur site des principaux fournisseurs cloud.

La solution FSX pour ONTAP sur AWS est un outil qui permet une intégration transparente avec SnapCenter et SyncMirror pour la réplication des données d'application vers le cloud. Veeam Backup & Replication est une autre technologie connue qui s'intègre bien aux systèmes de stockage NetApp ONTAP et peut fournir un basculement vers le stockage natif vSphere.

Cette solution de reprise après incident a présentée un stockage « Guest Connect » à partir d'un système ONTAP hébergeant les données d'applications SQL Server et Oracle. SnapCenter avec SnapMirror constitue une solution simple à gérer pour protéger les volumes d'applications dans les systèmes ONTAP et les répliquer vers FSX ou CVO résidant dans le cloud. SnapCenter est une solution de reprise d'activité pour le basculement de toutes les données applicatives vers VMware Cloud sur AWS.

Où trouver des informations complémentaires

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

- Liens vers la documentation de la solution

  "Multicloud hybride NetApp avec les solutions VMware"

  "Les solutions NetApp"

Sauvegarde et restauration Veeam dans VMware Cloud, avec Amazon FSX pour ONTAP

Veeam Backup & Replication est une solution efficace et fiable pour la protection des données dans VMware Cloud. Cette solution présente l'installation et la configuration adéquates pour l'utilisation de Veeam Backup and Replication afin de sauvegarder et de restaurer des machines virtuelles d'application résidant dans des datastores NFS FSX pour ONTAP dans VMware Cloud.

Auteur : Josh Powell - Ingénierie de solutions NetApp

Présentation

VMware Cloud (dans AWS) prend en charge l'utilisation des datastores NFS en tant que stockage supplémentaire, et FSX pour NetApp ONTAP est une solution sécurisée pour les clients qui ont besoin de stocker d'importants volumes de données pour leurs applications cloud pouvant évoluer indépendamment du nombre d'hôtes ESXi dans le cluster SDDC. Ce service de stockage AWS intégré offre un stockage ultra efficace avec toutes les fonctionnalités NetApp ONTAP classiques.

Cas d'utilisation

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde et restauration des machines virtuelles Windows et Linux hébergées dans VMC à l'aide de FSX pour NetApp ONTAP comme référentiel de sauvegarde.
- Sauvegardez et restaurez les données applicatives de Microsoft SQL Server en utilisant FSX pour NetApp ONTAP comme référentiel de sauvegarde.
- Sauvegardez et restaurez les données applicatives Oracle en utilisant FSX pour NetApp ONTAP comme référentiel de sauvegarde.

Datastores NFS avec Amazon FSX pour ONTAP

Toutes les machines virtuelles de cette solution résident dans les datastores NFS supplémentaires FSX pour ONTAP. L'utilisation de FSX pour ONTAP en tant que datastore NFS supplémentaire présente plusieurs avantages. Elle vous permet par exemple de :

- Créez un système de fichiers évolutif et hautement disponible dans le cloud sans nécessiter de configuration et de gestion complexes.
- Intégration dans votre environnement VMware existant, ce qui vous permet d'utiliser des outils et des processus familiers pour gérer vos ressources cloud.
- Vous bénéficiez des fonctionnalités avancées de gestion des données de ONTAP, telles que les copies Snapshot et la réplication, pour protéger vos données et en assurer la disponibilité.

Présentation du déploiement de la solution

Vous trouverez ci-dessous les étapes générales nécessaires pour configurer Veeam Backup & Replication, exécuter des tâches de sauvegarde et de restauration à l'aide de FSX for ONTAP en tant que référentiel de sauvegarde et effectuer des restaurations de machines virtuelles et de bases de données SQL Server et Oracle :

1. Créez le système de fichiers FSX pour ONTAP qui servira de référentiel de sauvegarde iSCSI pour Veeam Backup & Replication.
2. Déployez le proxy Veeam pour distribuer les workloads de sauvegarde et monter des référentiels de sauvegarde iSCSI hébergés sur FSX pour ONTAP.
3. Configuration des tâches de sauvegarde Veeam pour sauvegarder les machines virtuelles SQL Server, Oracle, Linux et Windows.
4. Restaurer des machines virtuelles SQL Server et des bases de données individuelles
5. Restaurer des machines virtuelles Oracle et des bases de données individuelles

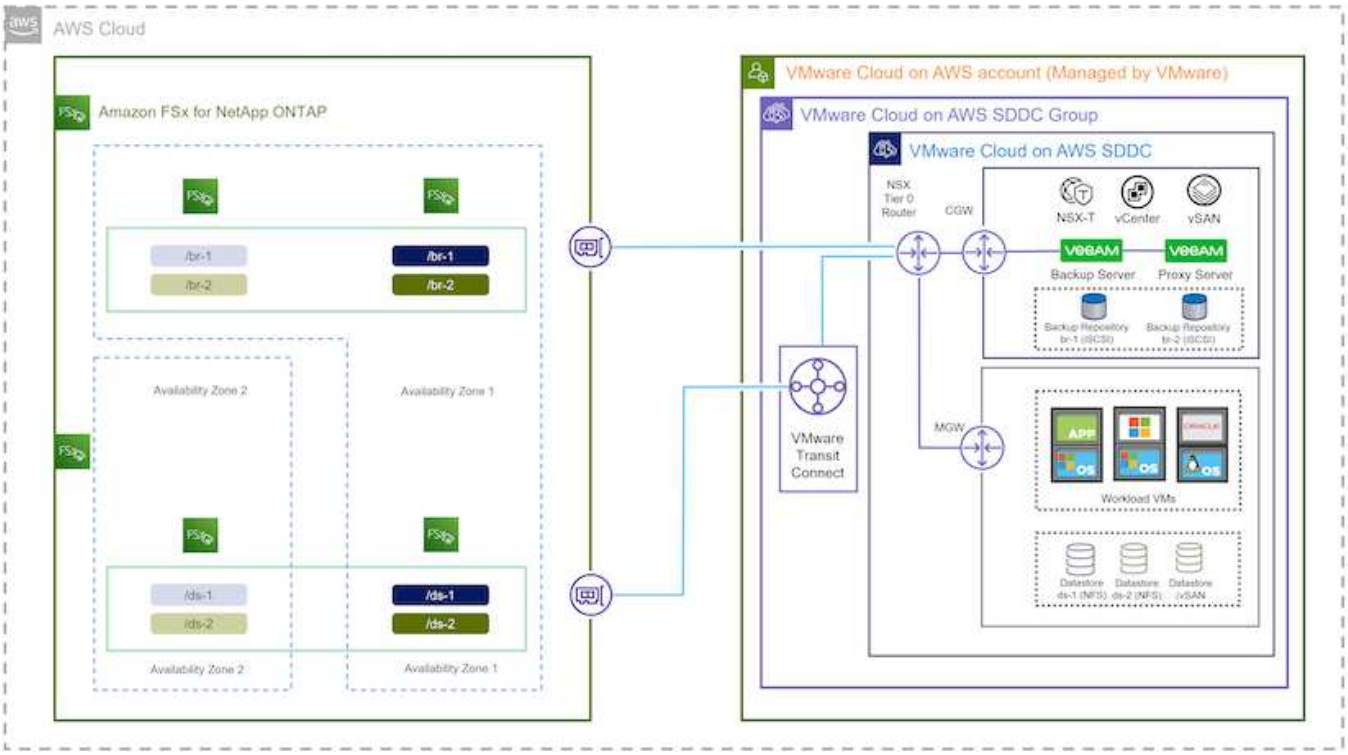
Prérequis

L'objectif de cette solution est de démontrer la protection des données des machines virtuelles s'exécutant dans VMware Cloud et situées sur des datastores NFS hébergés par FSX pour NetApp ONTAP. Cette solution suppose que les composants suivants sont configurés et prêts à l'emploi :

1. FSX pour le système de fichiers ONTAP avec un ou plusieurs datastores NFS connectés au cloud VMware.
2. Serveur virtuel Microsoft Windows Server avec le logiciel Veeam Backup & Replication installé.
    - Le serveur vCenter a été détecté par le serveur Veeam Backup & Replication à l'aide de son adresse IP ou de son nom de domaine complet.
3. La machine virtuelle Microsoft Windows Server doit être installée avec les composants Veeam Backup Proxy lors du déploiement de la solution.
4. Machines virtuelles Microsoft SQL Server avec VMDK et données d'application résidant sur FSX pour les datastores NFS ONTAP. Pour cette solution, nous avions deux bases de données SQL sur deux VMDK distincts.
    - Remarque : les fichiers de base de données et de journal des transactions sont placés sur des lecteurs distincts, ce qui améliore les performances et la fiabilité. Cela est dû en partie au fait que les journaux de transactions sont écrits séquentiellement, alors que les fichiers de base de données sont écrits de façon aléatoire.
5. Machines virtuelles de bases de données Oracle avec VMDK et données d'application résidant sur FSX pour les datastores NFS ONTAP.
6. Machines virtuelles de serveurs de fichiers Linux et Windows avec VMDK résidant sur les datastores NFS FSX pour ONTAP.
7. Veeam requiert des ports TCP spécifiques pour la communication entre les serveurs et les composants de l'environnement de sauvegarde. Sur les composants de l'infrastructure de sauvegarde Veeam, les règles de pare-feu requises sont automatiquement créées. Pour obtenir la liste complète des ports réseau requis, reportez-vous à la section ports du "Guide de l'utilisateur Veeam Backup and Replication pour VMware vSphere".

Architecture de haut niveau

Le test/validation de cette solution a été effectué dans un laboratoire qui peut correspondre ou non à l'environnement de déploiement final. Pour plus d'informations, reportez-vous aux sections suivantes.



Composants matériels/logiciels

L'objectif de cette solution est de démontrer la protection des données des machines virtuelles s'exécutant dans VMware Cloud et situées sur des datastores NFS hébergés par FSX pour NetApp ONTAP. Cette solution suppose que les composants suivants sont déjà configurés et prêts à l'emploi :

- Les VM Microsoft Windows se trouvent sur un datastore NFS FSX pour ONTAP
- Machines virtuelles Linux (CentOS) situées dans un datastore NFS FSX pour ONTAP
- Les VM Microsoft SQL Server se trouvent sur un datastore NFS FSX pour ONTAP
  - Deux bases de données hébergées sur des VMDK distincts
- Machines virtuelles Oracle situées sur un datastore NFS FSX pour ONTAP

Déploiement de la solution

Cette solution contient des instructions détaillées pour le déploiement et la validation d'une solution utilisant le logiciel Veeam Backup and Replication afin d'effectuer la sauvegarde et la restauration des machines virtuelles de serveurs de fichiers SQL Server, Oracle et Windows et Linux dans un SDDC VMware Cloud sur AWS. Les machines virtuelles de cette solution résident sur un datastore NFS supplémentaire hébergé par FSX pour ONTAP. En outre, un système de fichiers FSX for ONTAP distinct est utilisé pour héberger les volumes iSCSI qui seront utilisés pour les référentiels de sauvegarde Veeam.

Nous allons passer en revue FSX pour la création de système de fichiers ONTAP, le montage de volumes iSCSI à utiliser comme référentiels de sauvegarde, la création et l'exécution de tâches de sauvegarde, et les

restaurations de machines virtuelles et de bases de données.

Pour plus d'informations sur FSX pour NetApp ONTAP, reportez-vous au "Guide de l'utilisateur de FSX pour ONTAP".

Pour plus d'informations sur Veeam Backup and Replication, reportez-vous au "Documentation technique du centre d'aide Veeam" le site.

Pour connaître les points à prendre en compte et les limites lors de l'utilisation de Veeam Backup and Replication avec VMware Cloud on AWS, reportez-vous à la section "Support de VMware Cloud sur AWS et de VMware Cloud sur Dell EMC. Considérations et limitations".

Déployez le serveur proxy Veeam

Un serveur proxy Veeam est un composant du logiciel Veeam Backup & Replication qui sert d'intermédiaire entre la source et la cible de sauvegarde ou de réplication. Le serveur proxy permet d'optimiser et d'accélérer le transfert de données pendant les tâches de sauvegarde en traitant les données localement et peut utiliser différents modes de transport pour accéder aux données à l'aide des API VMware vStorage pour la protection des données ou via un accès direct au stockage.

Lors du choix d'une conception de serveur proxy Veeam, il est important de tenir compte du nombre de tâches simultanées et du mode de transport ou du type d'accès au stockage souhaité.

Pour le dimensionnement du nombre de serveurs proxy et pour connaître la configuration système requise, reportez-vous au "Guide des meilleures pratiques Veeam VMware vSphere".

Veeam Data Mover est un composant du serveur proxy Veeam et utilise un mode de transport comme méthode pour obtenir les données VM de la source et les transférer vers la cible. Le mode de transport est spécifié lors de la configuration de la tâche de sauvegarde. Il est possible d'augmenter l'efficacité des sauvegardes à partir des datastores NFS en utilisant un accès direct au stockage.

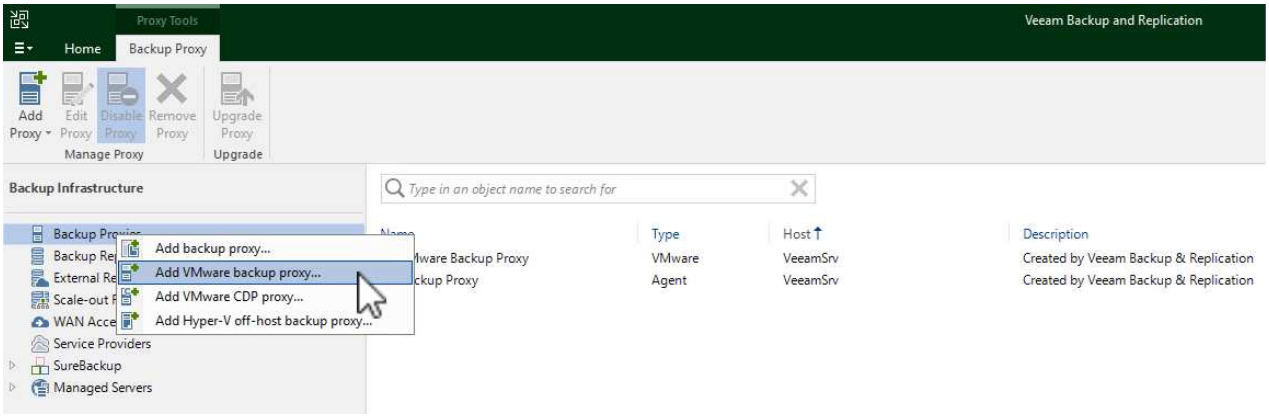
Pour plus d'informations sur les modes de transport, reportez-vous au "Guide de l'utilisateur Veeam Backup and Replication pour VMware vSphere".

L'étape suivante porte sur le déploiement de Veeam Proxy Server sur une machine virtuelle Windows dans le SDDC VMware Cloud.

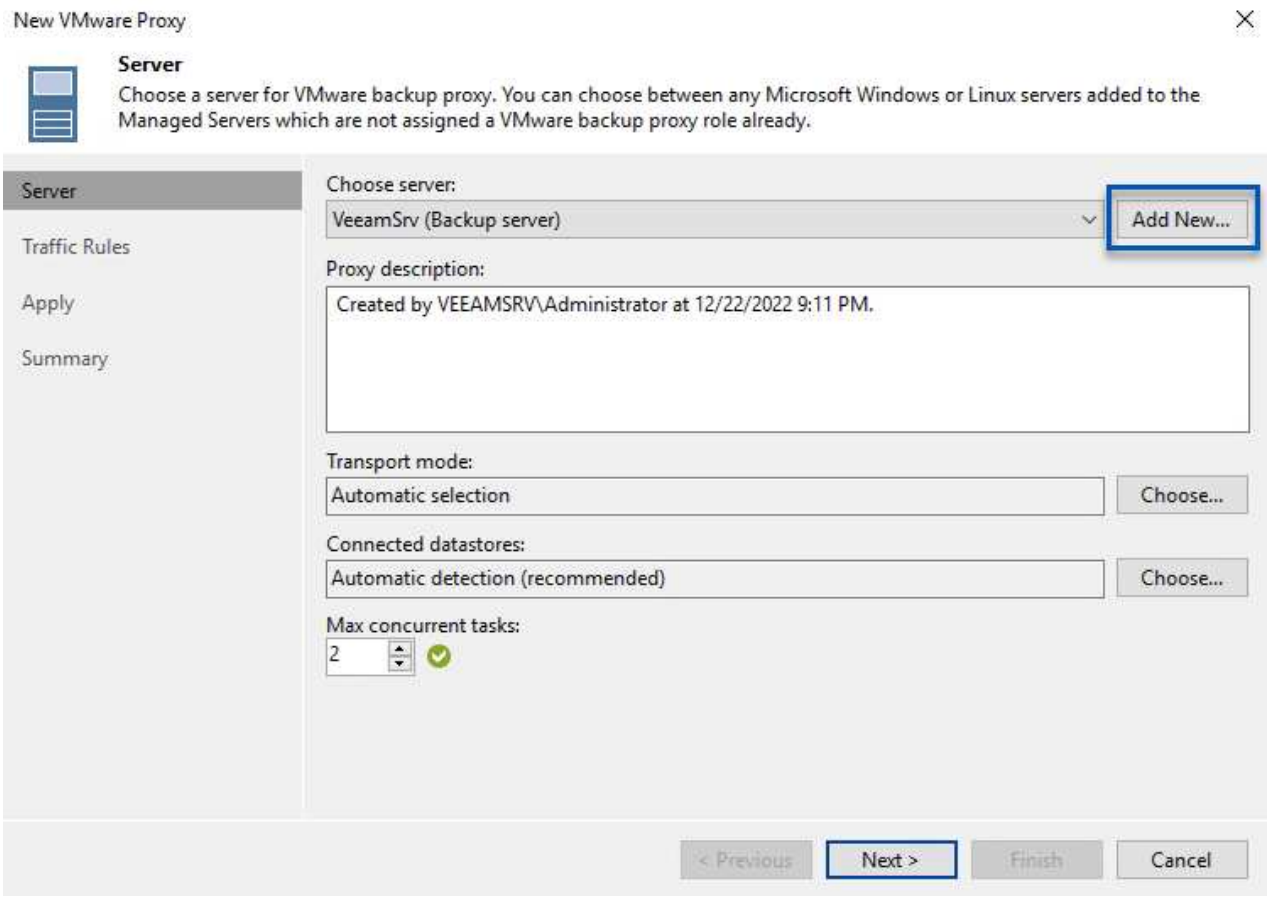
Déployez Veeam Proxy pour distribuer les workloads de sauvegarde

Au cours de cette étape, le proxy Veeam est déployé sur une machine virtuelle Windows existante. Les tâches de sauvegarde peuvent ainsi être réparties entre le serveur Veeam Backup Server principal et le proxy Veeam.

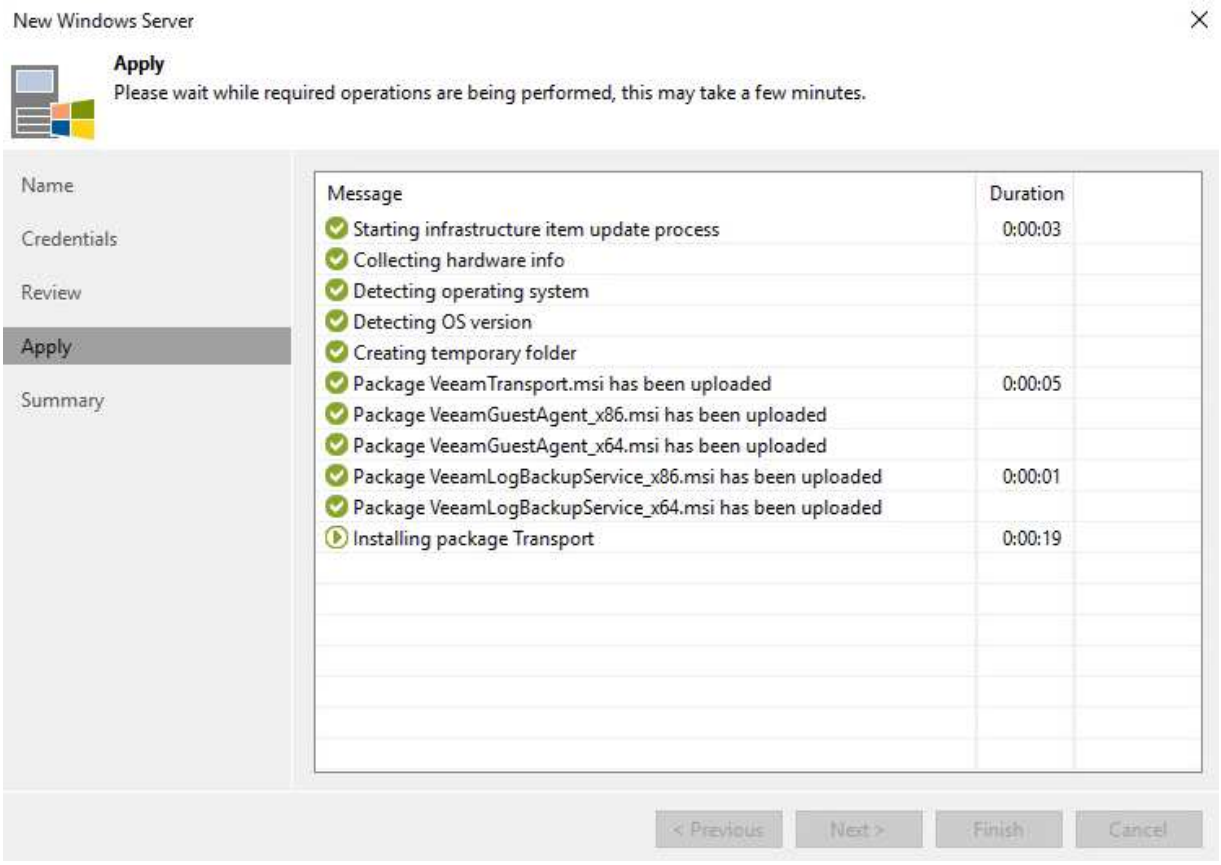
1. Sur le serveur Veeam Backup and Replication, ouvrez la console d'administration et sélectionnez **Backup Infrastructure** dans le menu inférieur gauche.
2. Cliquez avec le bouton droit de la souris sur **Backup Proxies** et cliquez sur **Ajouter un proxy de sauvegarde VMware…** pour ouvrir l'assistant.



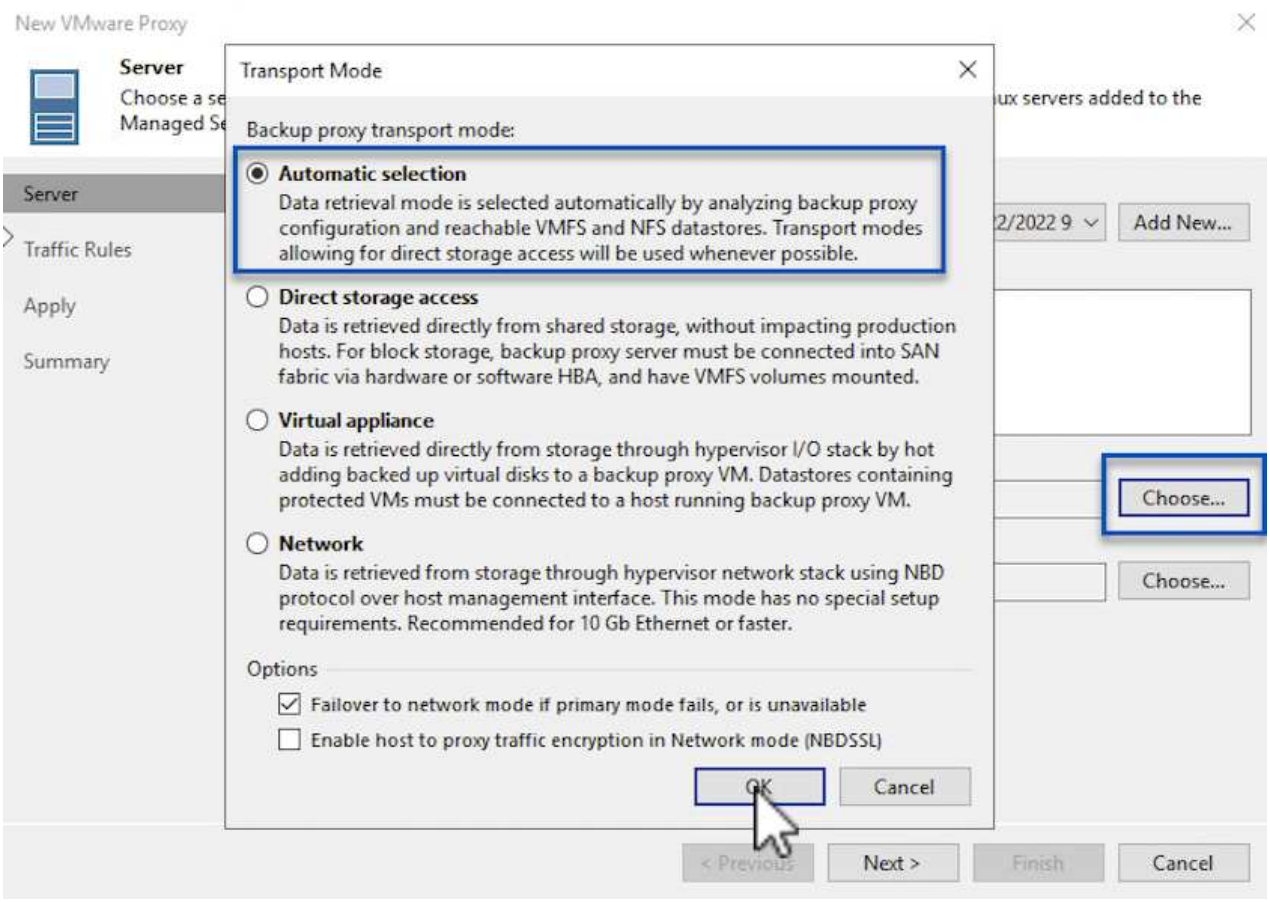
3. Dans l'assistant **Ajouter un proxy VMware**, cliquez sur le bouton **Ajouter un nouveau…** pour ajouter un nouveau serveur proxy.



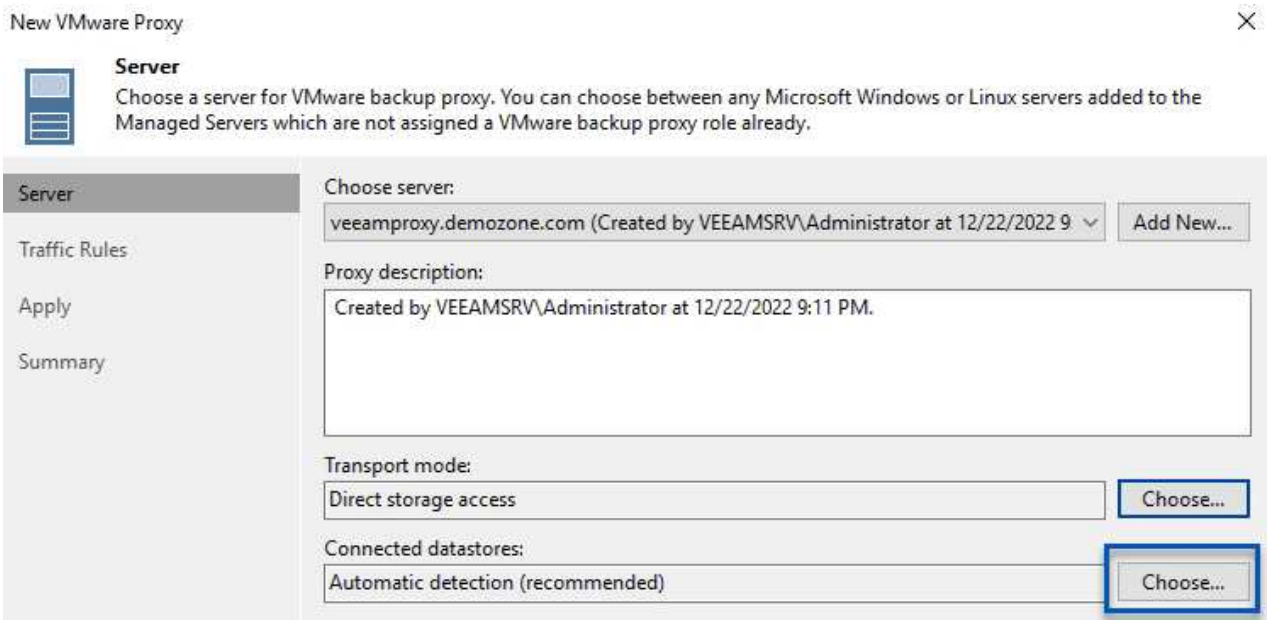
4. Sélectionnez pour ajouter Microsoft Windows et suivez les invites pour ajouter le serveur :
   - Indiquez le nom DNS ou l'adresse IP
   - Sélectionnez un compte à utiliser pour les informations d'identification sur le nouveau système ou ajoutez de nouvelles informations d'identification
   - Vérifiez les composants à installer, puis cliquez sur **appliquer** pour commencer le déploiement

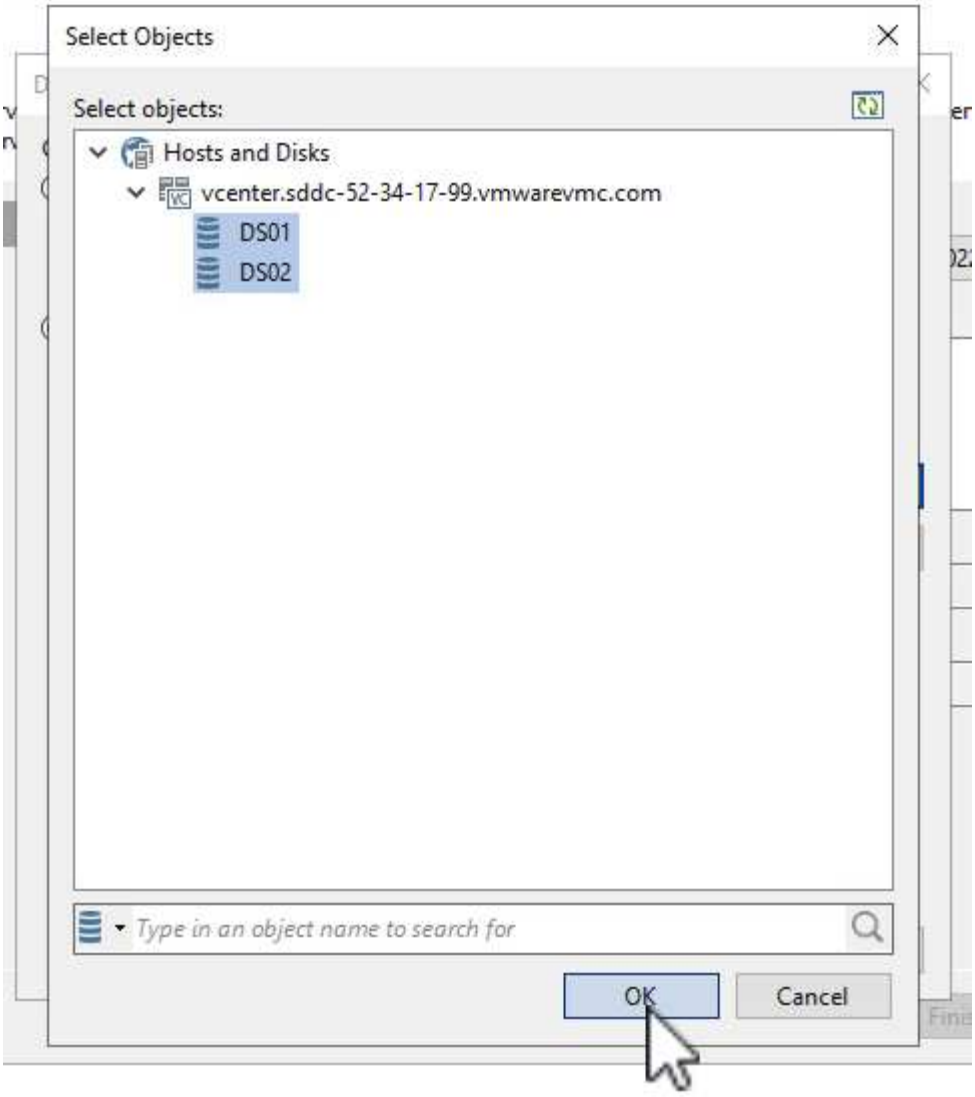


5. De retour dans l'assistant **Nouveau proxy VMware**, choisissez un mode de transport. Dans notre cas, nous avons choisi **sélection automatique**.

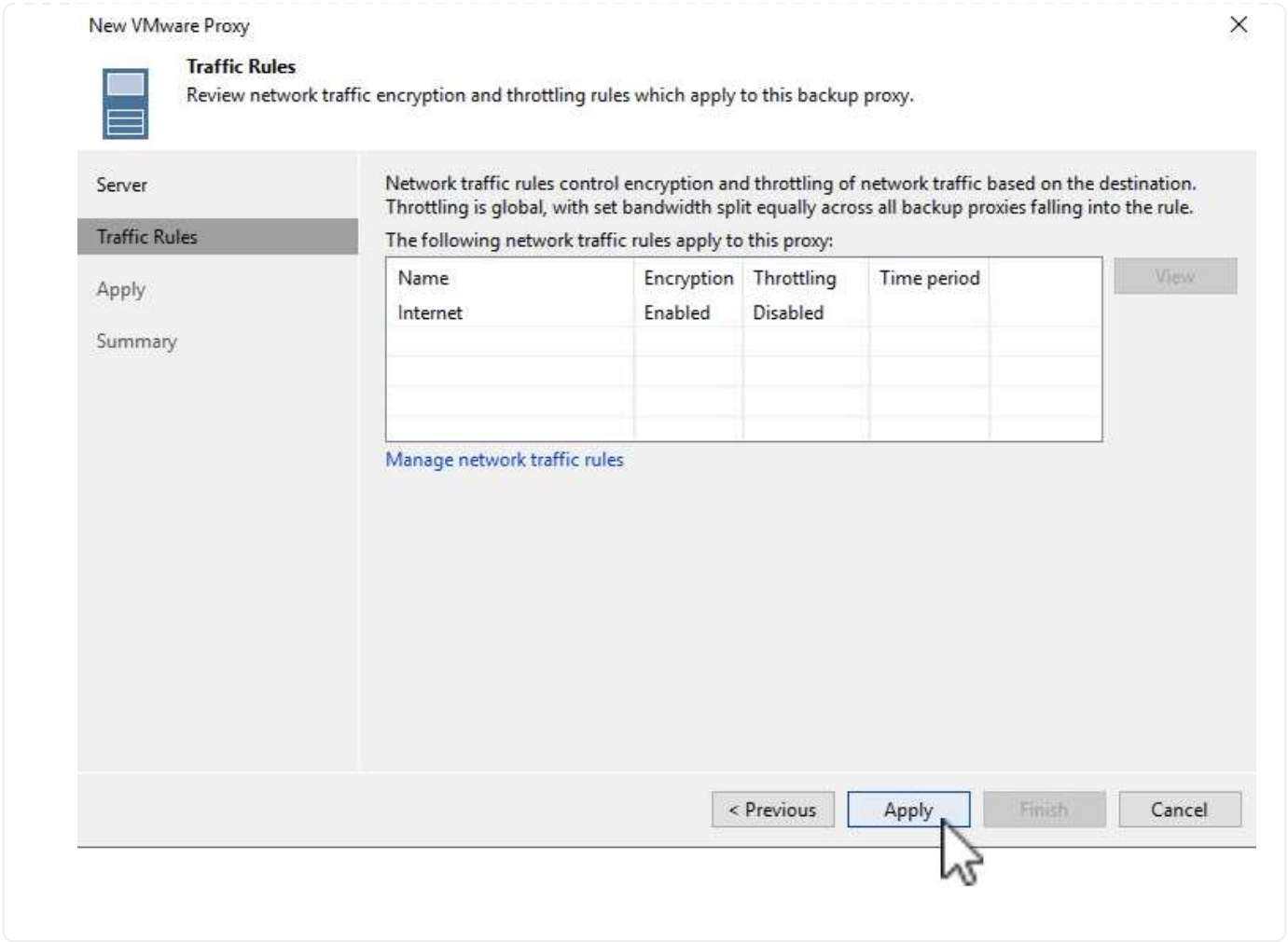


6. Sélectionnez les datastores connectés auxquels vous souhaitez que le proxy VMware dispose d'un accès direct.





7. Configurez et appliquez toutes les règles de trafic réseau spécifiques telles que le cryptage ou l'accélération. Lorsque vous avez terminé, cliquez sur le bouton **appliquer** pour terminer le déploiement.



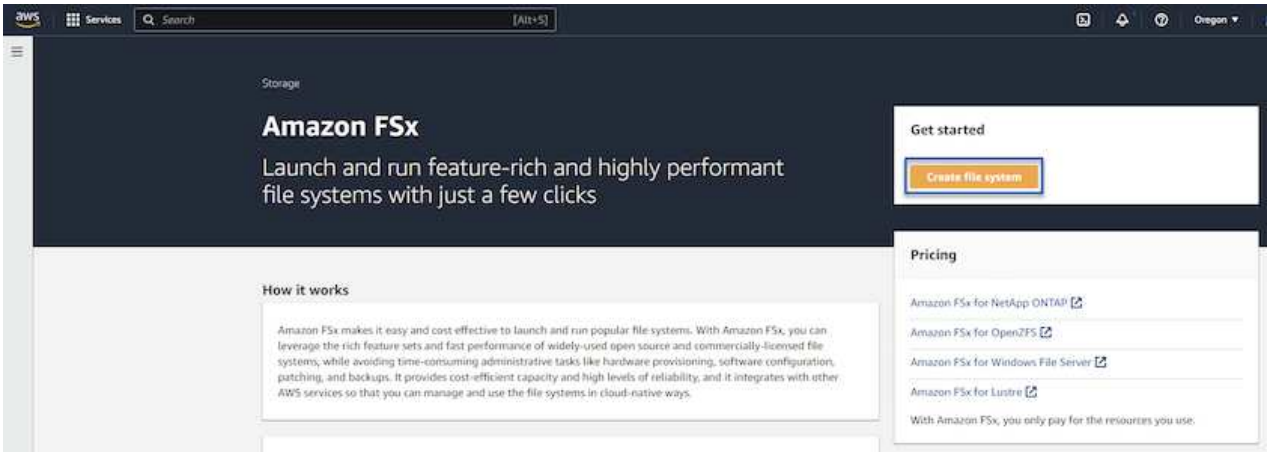
Configuration des référentiels de stockage et de sauvegarde

Le serveur Veeam Backup principal et le serveur Veeam Proxy ont accès à un référentiel de sauvegarde sous la forme d'un système de stockage à connexion directe. Dans cette section, nous allons aborder la création d'un système de fichiers FSX pour ONTAP, le montage de LUN iSCSI sur les serveurs Veeam et la création de référentiels de sauvegarde.

Créez un système de fichiers FSX pour ONTAP

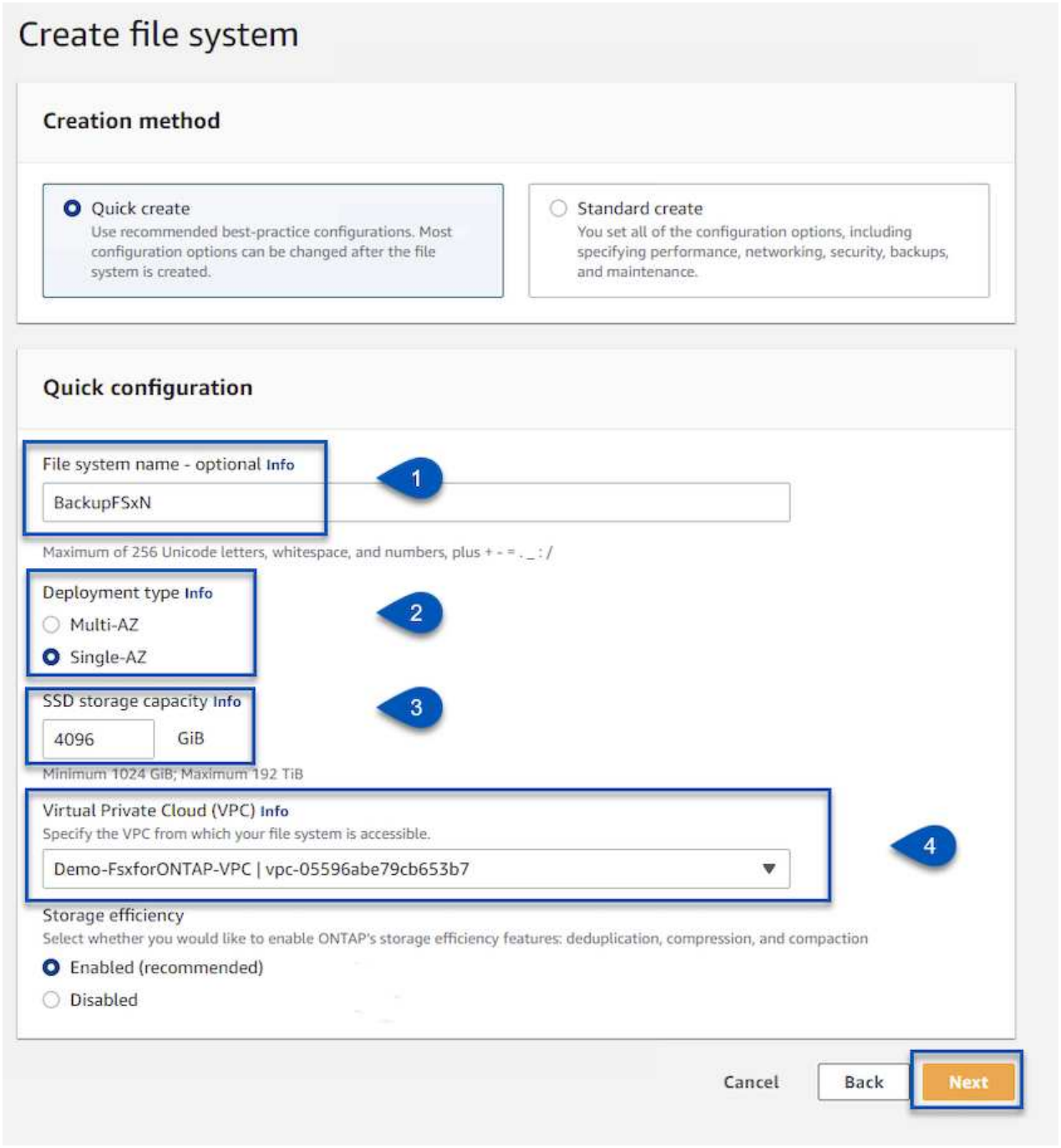
Créez un système de fichiers FSX pour ONTAP qui sera utilisé pour héberger les volumes iSCSI des référentiels de sauvegarde Veeam.

1. Dans la console AWS, accédez à FSX, puis à **Créer un système de fichiers**



2. Sélectionnez **Amazon FSX pour NetApp ONTAP**, puis **Suivant** pour continuer.

3. Renseignez le nom du système de fichiers, le type de déploiement, la capacité de stockage SSD et le VPC dans lequel le cluster FSX pour ONTAP doit résider. Il doit s'agir d'un VPC configuré pour communiquer avec le réseau des machines virtuelles dans VMware Cloud. Cliquez sur **Suivant**.



4. Passez en revue les étapes de déploiement et cliquez sur **Créer un système de fichiers** pour lancer le processus de création du système de fichiers.

Configuration et montage de LUN iSCSI

Créez et configurez les LUN iSCSI sur FSX pour ONTAP et montez sur les serveurs de sauvegarde et proxy Veeam. Ces LUN seront ensuite utilisées pour créer des référentiels de sauvegarde Veeam.

> La création d'une LUN iSCSI sur FSX pour ONTAP est un processus en plusieurs étapes. La première étape de la création des volumes peut être effectuée dans la console Amazon FSX ou avec l'interface de ligne de commande NetApp ONTAP.

> Pour plus d'informations sur l'utilisation de FSX pour ONTAP, consultez le "Guide de l'utilisateur de FSX pour ONTAP".

1. Depuis l'interface de ligne de commandes de NetApp ONTAP, créer les volumes initiaux à l'aide de la commande suivante :

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Créez des LUN en utilisant les volumes créés à l'étape précédente :

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Octroyer l'accès aux LUN en créant un groupe initiateur contenant le IQN iSCSI des serveurs de sauvegarde et proxy Veeam :

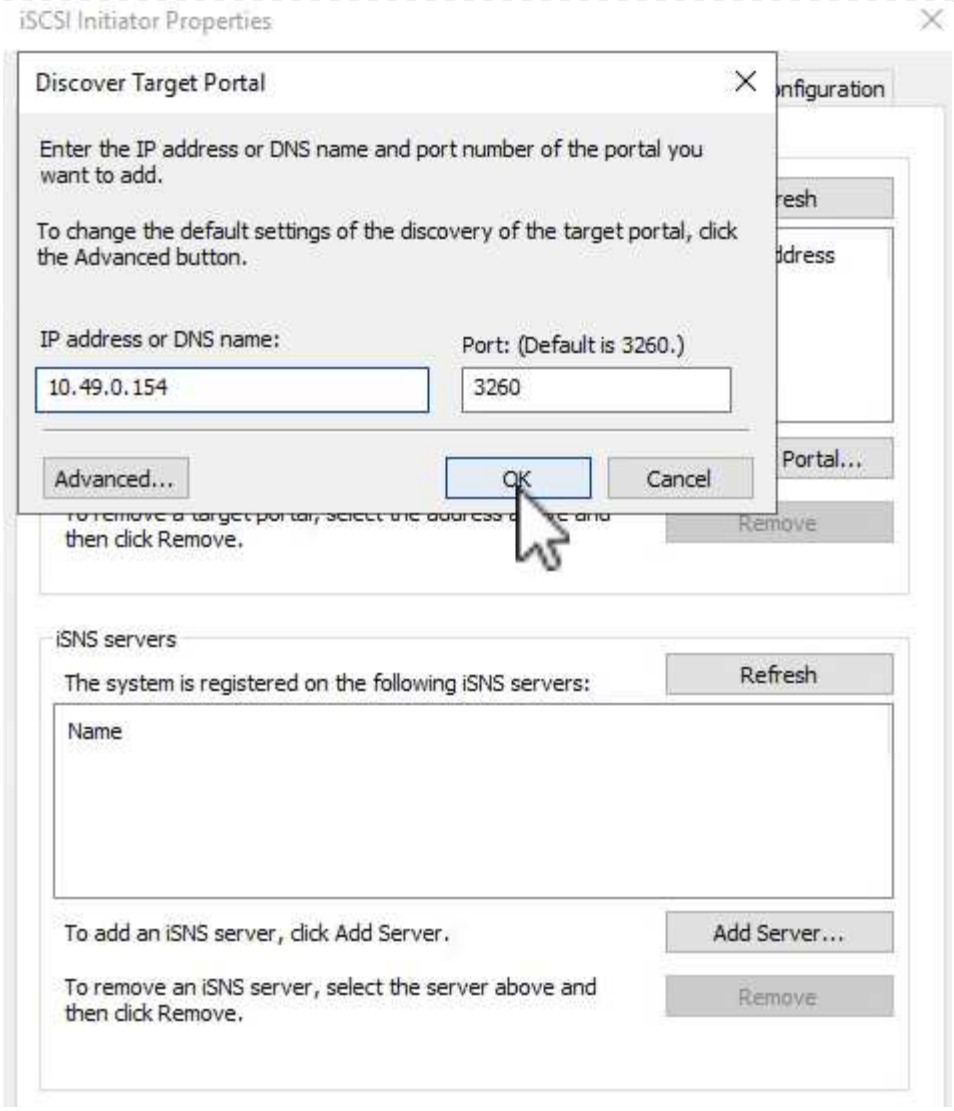
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

> Pour terminer l'étape précédente, vous devez d'abord récupérer l'IQN à partir des propriétés de l'initiateur iSCSI sur les serveurs Windows.

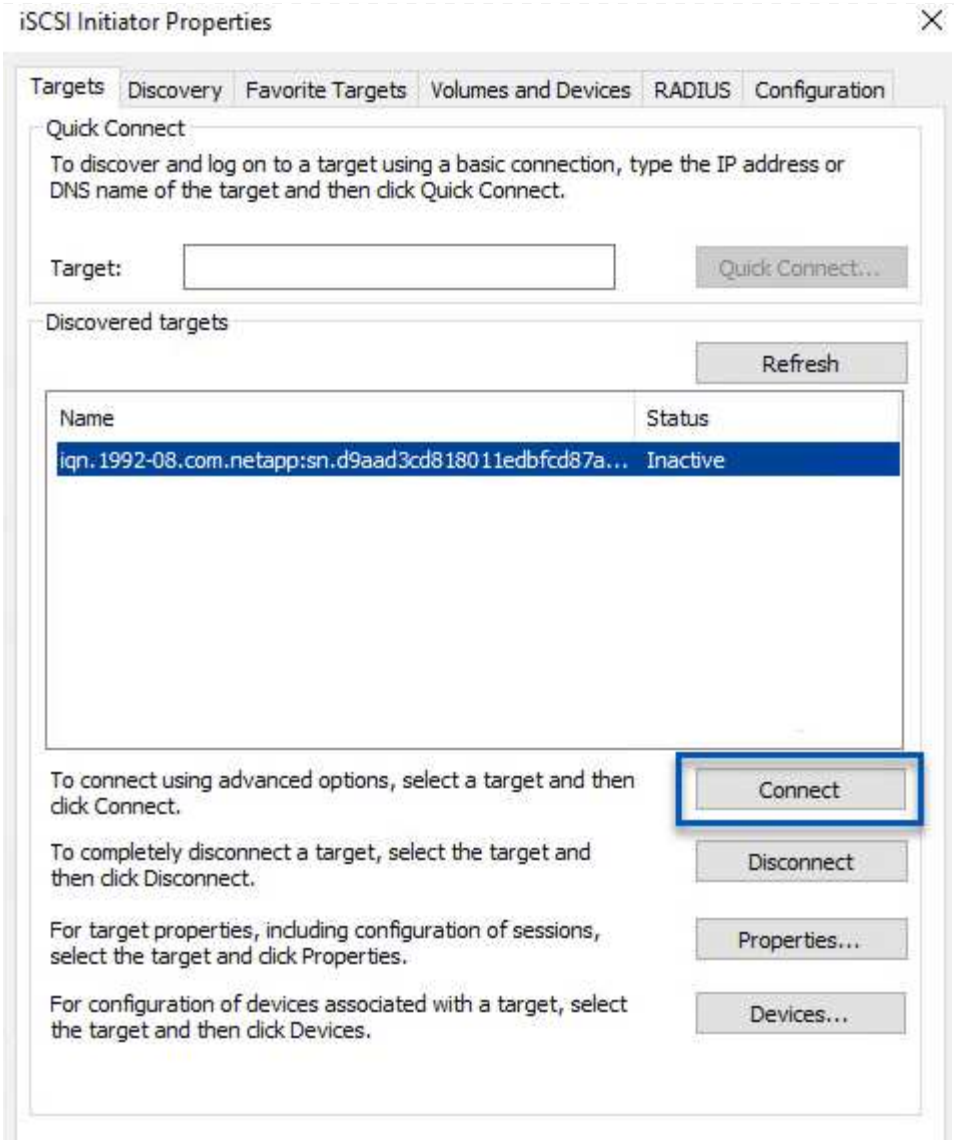
4. Enfin, mappez les LUN sur le groupe initiateur que vous venez de créer :

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

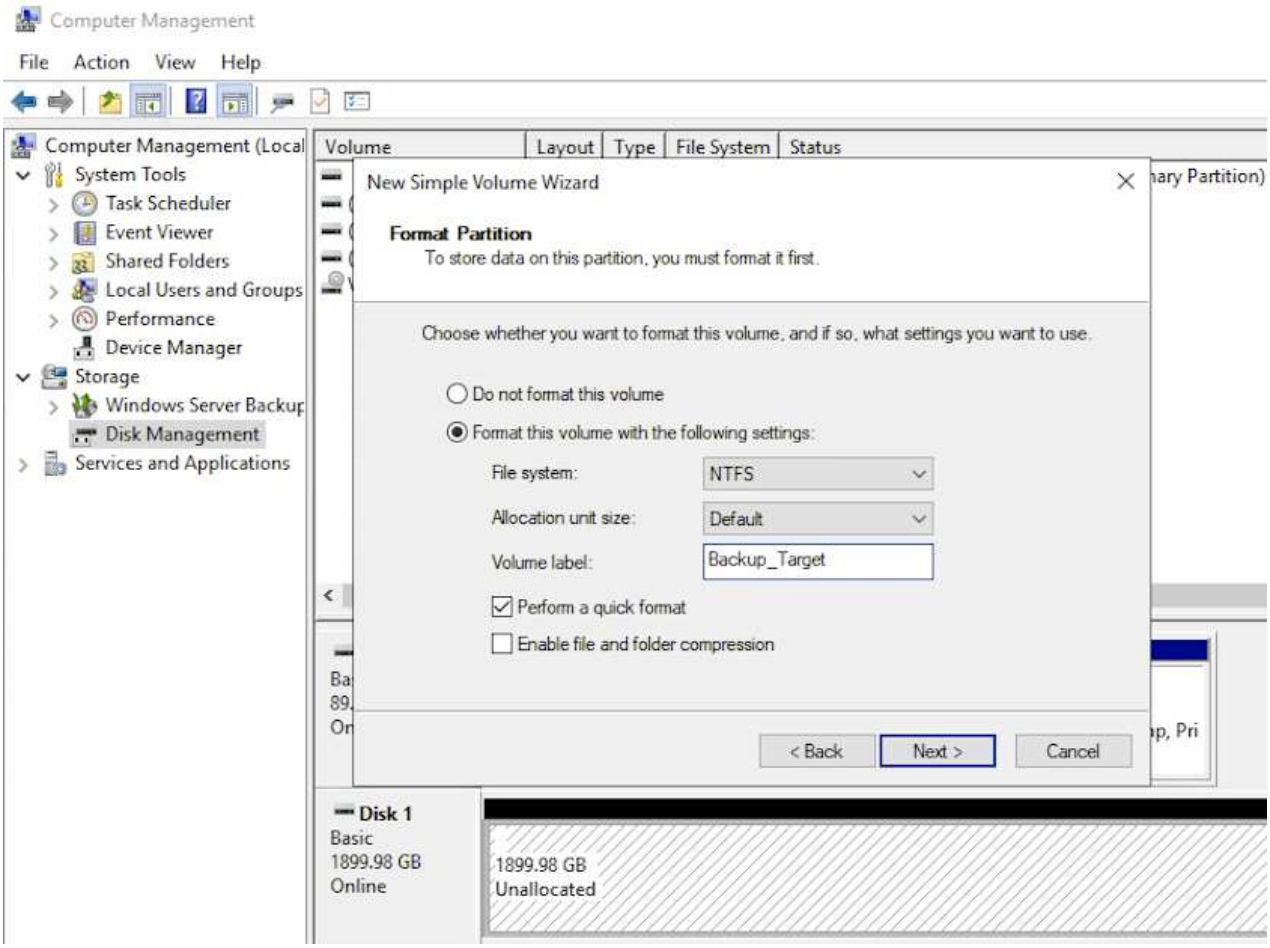
5. Pour monter les LUN iSCSI, connectez-vous à Veeam Backup & Replication Server et ouvrez iSCSI Initiator Properties. Accédez à l'onglet **Discover** et entrez l'adresse IP de la cible iSCSI.



6. Dans l'onglet **cibles**, mettez en surbrillance le LUN inactif et cliquez sur **connecter**. Cochez la case **Activer multi-chemin** et cliquez sur **OK** pour vous connecter à la LUN.



7. Dans l'utilitaire gestion des disques, initialisez la nouvelle LUN et créez un volume avec le nom et la lettre de lecteur souhaités. Cochez la case **Activer multi-chemin** et cliquez sur **OK** pour vous connecter à la LUN.

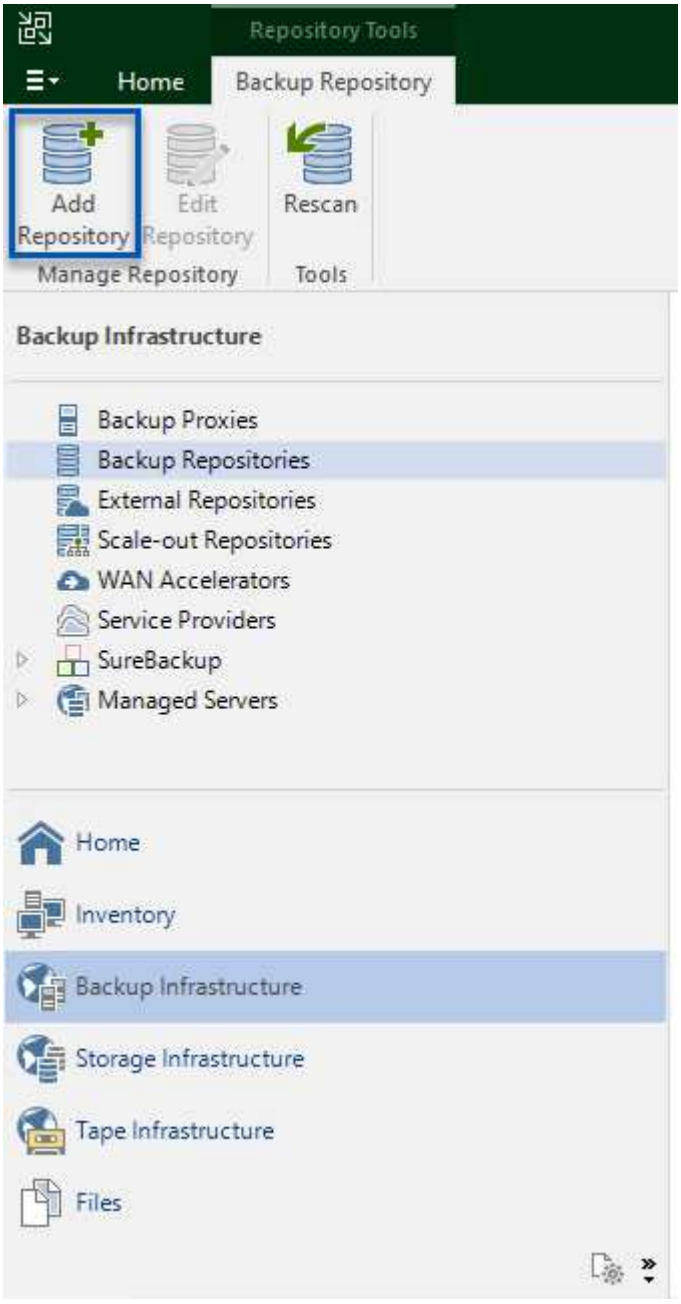


8. Répétez ces étapes pour monter les volumes iSCSI sur le serveur proxy Veeam.

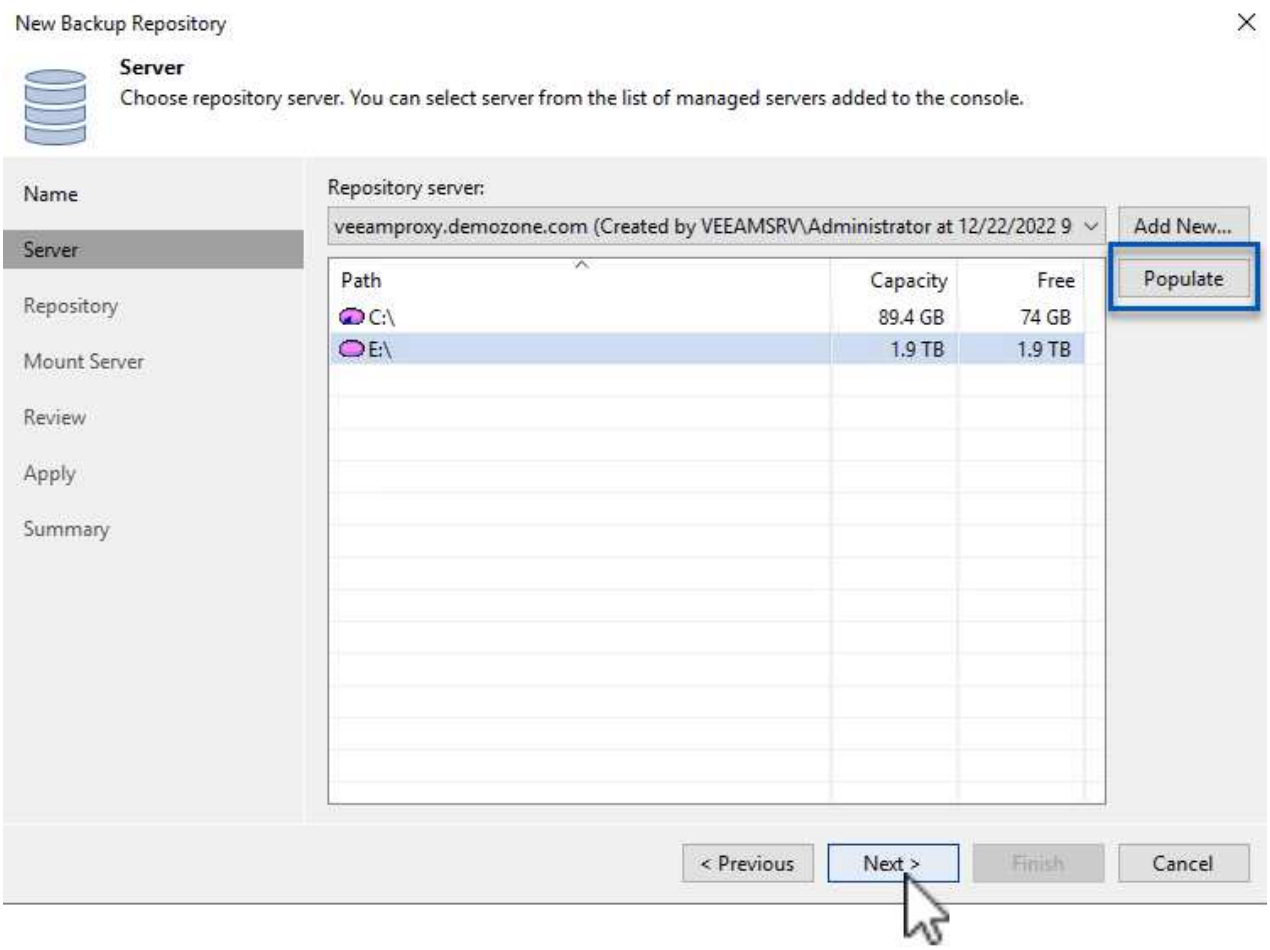
Création de référentiels de sauvegarde Veeam

Dans la console Veeam Backup and Replication, créez des référentiels de sauvegarde pour les serveurs Veeam Backup et Veeam Proxy. Ces référentiels seront utilisés comme cibles de sauvegarde pour les sauvegardes des machines virtuelles.

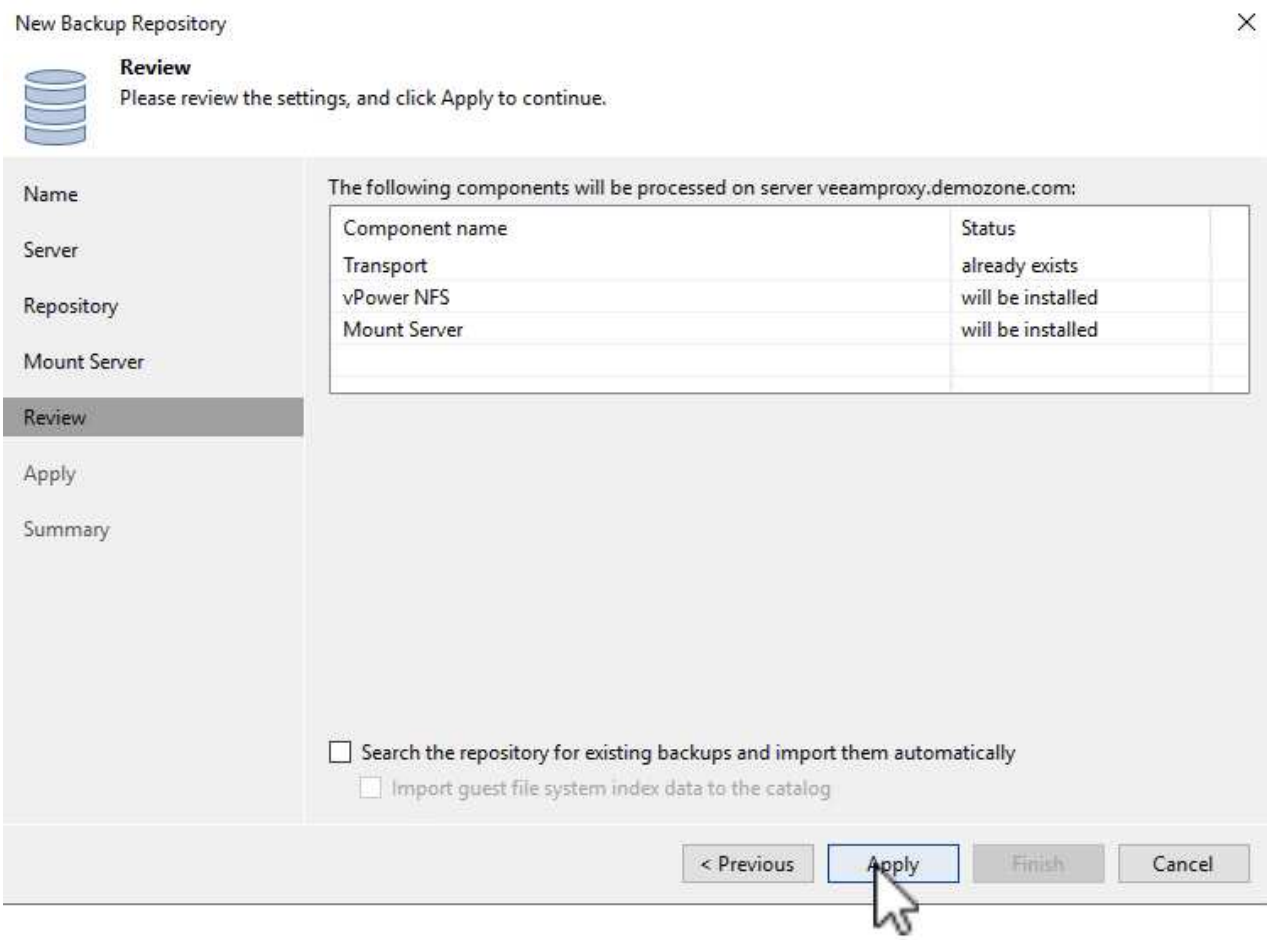
1. Dans la console de sauvegarde et de réplication Veeam, cliquez sur **Backup Infrastructure** en bas à gauche, puis sélectionnez **Add Repository**



2. Dans l'assistant Nouveau référentiel de sauvegarde, entrez un nom pour le référentiel, puis sélectionnez le serveur dans la liste déroulante et cliquez sur le bouton **alimenter** pour choisir le volume NTFS qui sera utilisé.



3. Sur la page suivante, choisissez un serveur de montage qui sera utilisé pour monter des sauvegardes sur lors de restaurations avancées. Par défaut, il s'agit du même serveur sur lequel le stockage du référentiel est connecté.
4. Vérifiez vos sélections et cliquez sur **appliquer** pour lancer la création du référentiel de sauvegarde.



5. Répétez ces étapes pour tous les serveurs proxy supplémentaires.

Configurer les tâches de sauvegarde Veeam

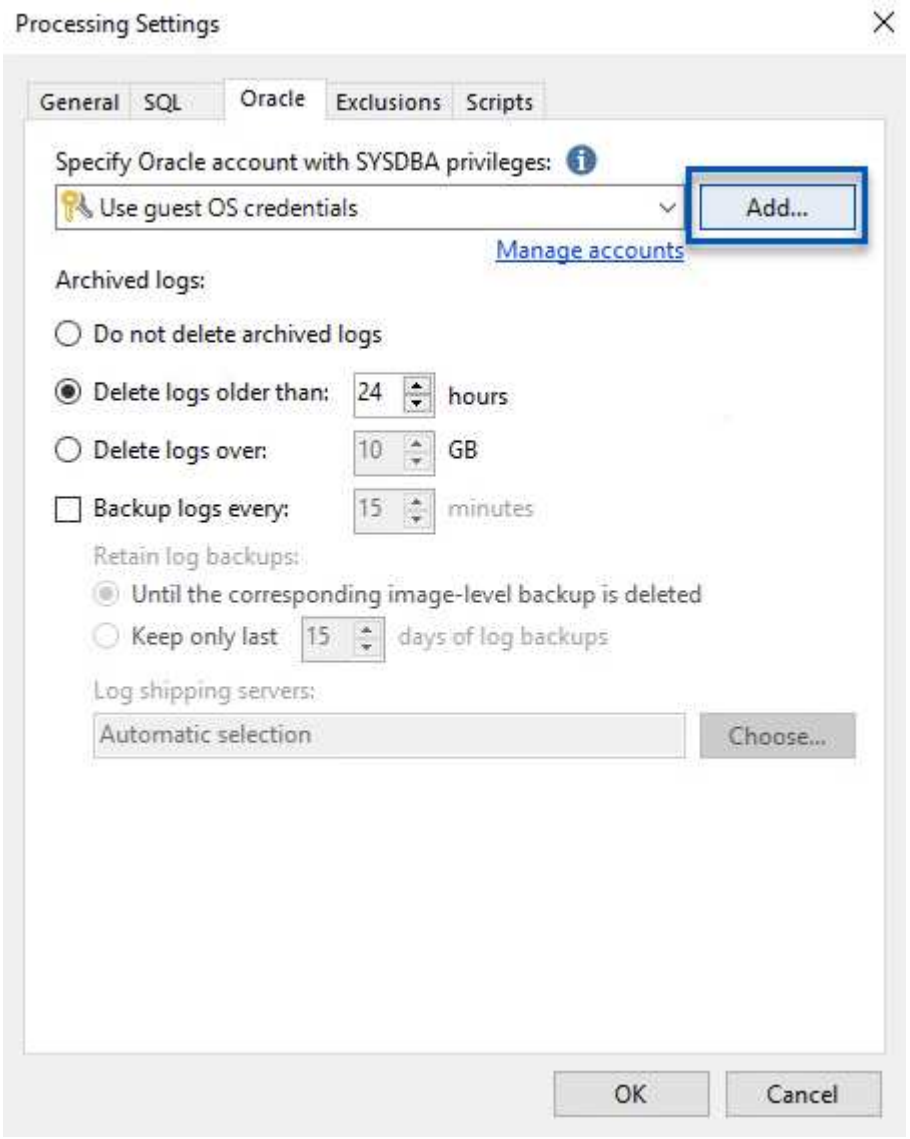
Les tâches de sauvegarde doivent être créées à l'aide des référentiels de sauvegarde de la section précédente. La création de tâches de sauvegarde fait partie intégrante du répertoire des administrateurs de stockage et ne couvre pas toutes les étapes. Pour plus d'informations sur la création de tâches de sauvegarde dans Veeam, consultez le "Documentation technique du centre d'aide Veeam".

Dans cette solution, des tâches de sauvegarde distinctes ont été créées pour :

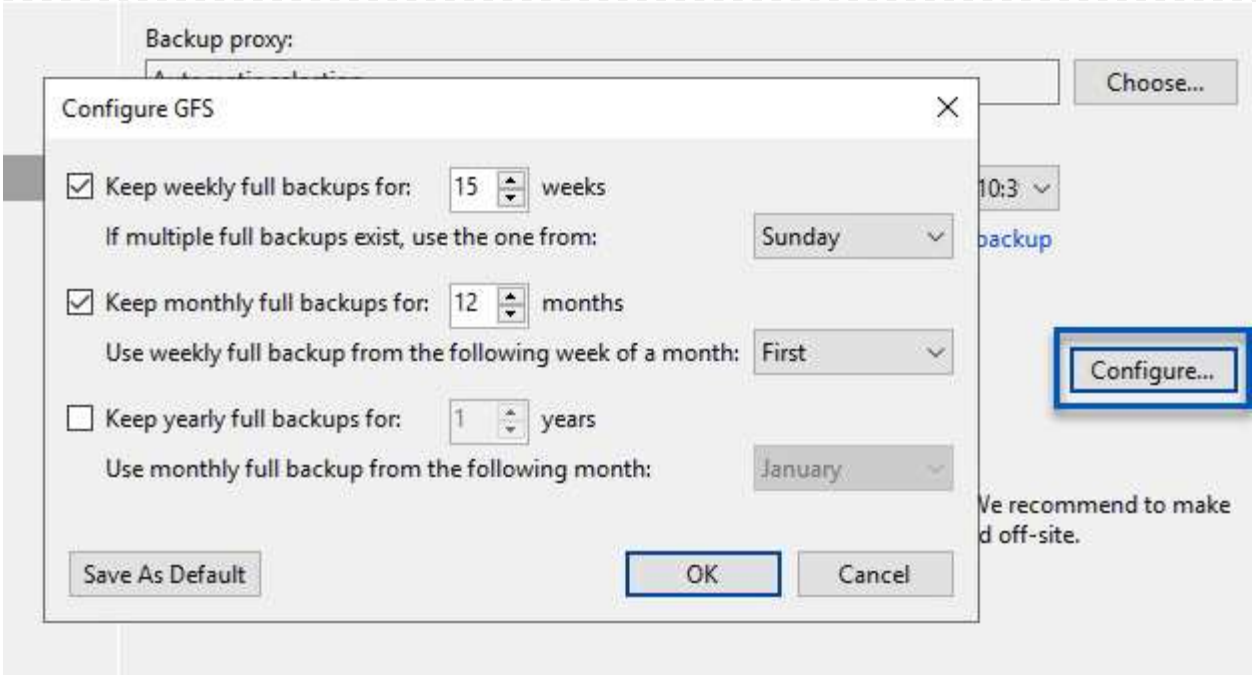
- Serveurs Microsoft Windows SQL Server
- Serveurs de base de données Oracle
- Serveurs de fichiers Windows
- Serveurs de fichiers Linux

Considérations générales lors de la configuration des tâches de sauvegarde Veeam

1. Activez le traitement intégrant la cohérence applicative pour créer des sauvegardes cohérentes et effectuer le traitement du journal des transactions.
2. Après avoir activé le traitement basé sur les applications, ajoutez les informations d'identification correctes avec des privilèges d'administrateur à l'application car elles peuvent être différentes des informations d'identification du système d'exploitation invité.



3. Pour gérer la stratégie de rétention pour la sauvegarde, cochez la case **conserver certaines sauvegardes complètes plus longtemps à des fins d'archivage** et cliquez sur le bouton **configurer…** pour configurer la stratégie.



Restauration des machines virtuelles d'application avec la restauration complète Veeam

Une restauration complète avec Veeam constitue la première étape de la restauration d'une application. Nous avons confirmé que des restaurations complètes de nos machines virtuelles sous tension et que tous les services s'exécutaient normalement.

La restauration des serveurs fait partie intégrante du répertoire des administrateurs de stockage et nous ne couvrons pas toutes les étapes. Pour plus d'informations sur les restaurations complètes dans Veeam, reportez-vous au "Documentation technique du centre d'aide Veeam".

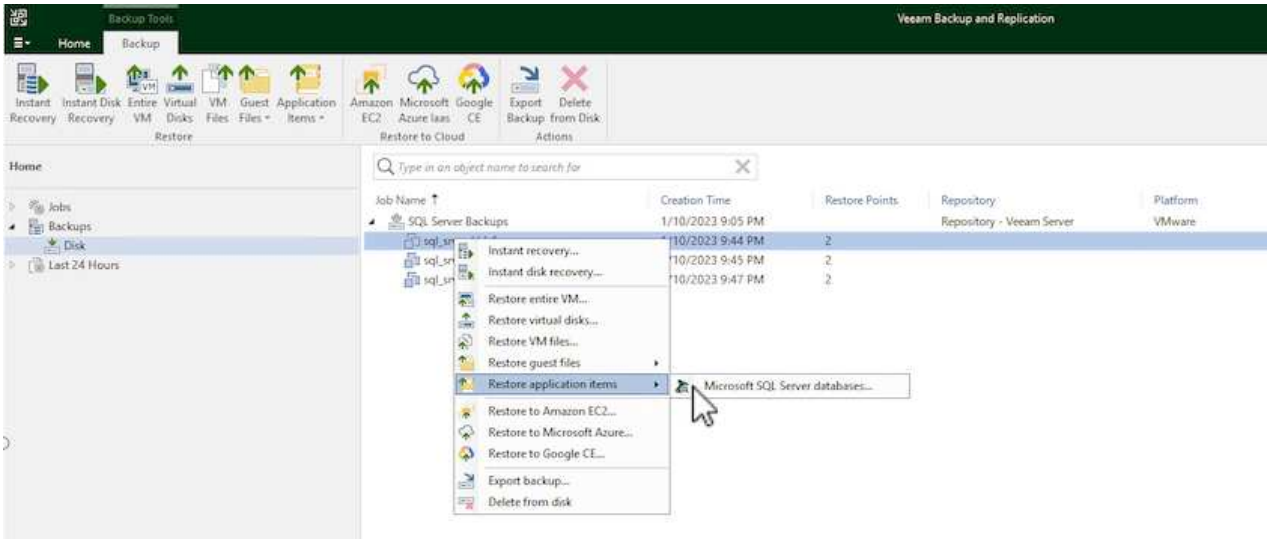
Restaurer les bases de données SQL Server

Veeam Backup & Replication propose plusieurs options de restauration des bases de données SQL Server. Pour cette validation, nous avons utilisé Veeam Explorer for SQL Server with Instant Recovery pour exécuter les restaurations de nos bases de données SQL Server. SQL Server Instant Recovery est une fonctionnalité qui vous permet de restaurer rapidement les bases de données SQL Server sans avoir à attendre la restauration complète de la base de données. Ce processus de restauration rapide réduit les interruptions et assure la continuité de l'activité. Voici comment cela fonctionne :

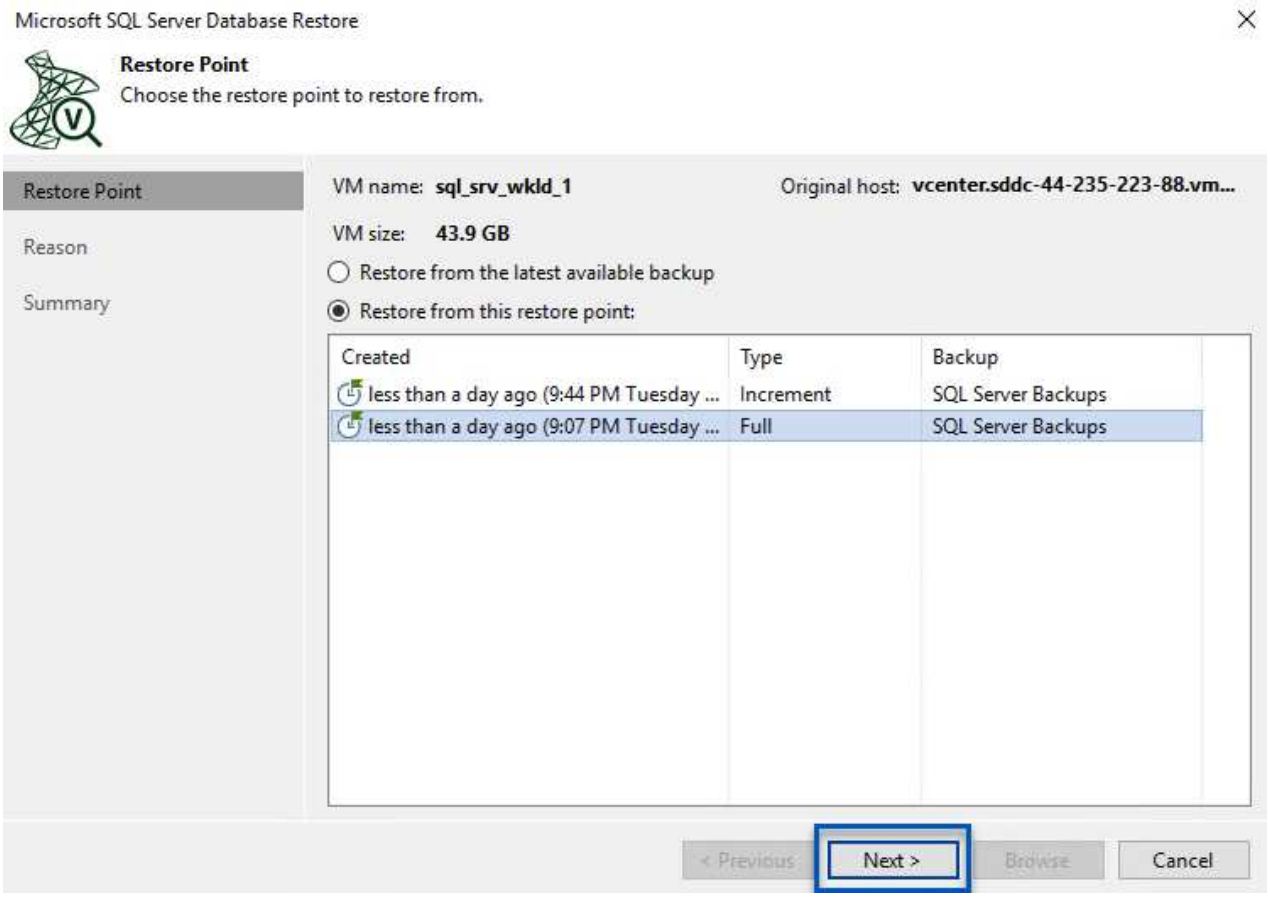
- Veeam Explorer **monte la sauvegarde** contenant la base de données SQL Server à restaurer.
- Le logiciel **publie la base de données** directement à partir des fichiers montés, ce qui la rend accessible en tant que base de données temporaire sur l'instance SQL Server cible.
- Pendant que la base de données temporaire est en cours d'utilisation, Veeam Explorer **redirige les requêtes utilisateur** vers cette base de données, ce qui permet aux utilisateurs de continuer à accéder aux données et à les utiliser.
- En arrière-plan, Veeam **effectue une restauration complète de la base de données**, transférant les données de la base de données temporaire vers l'emplacement d'origine de la base de données.
- Une fois la restauration complète de la base de données terminée, Veeam Explorer **restaure les requêtes utilisateur à la base de données d'origine** et supprime la base de données temporaire.

Restaurer une base de données SQL Server avec Veeam Explorer Instant Recovery

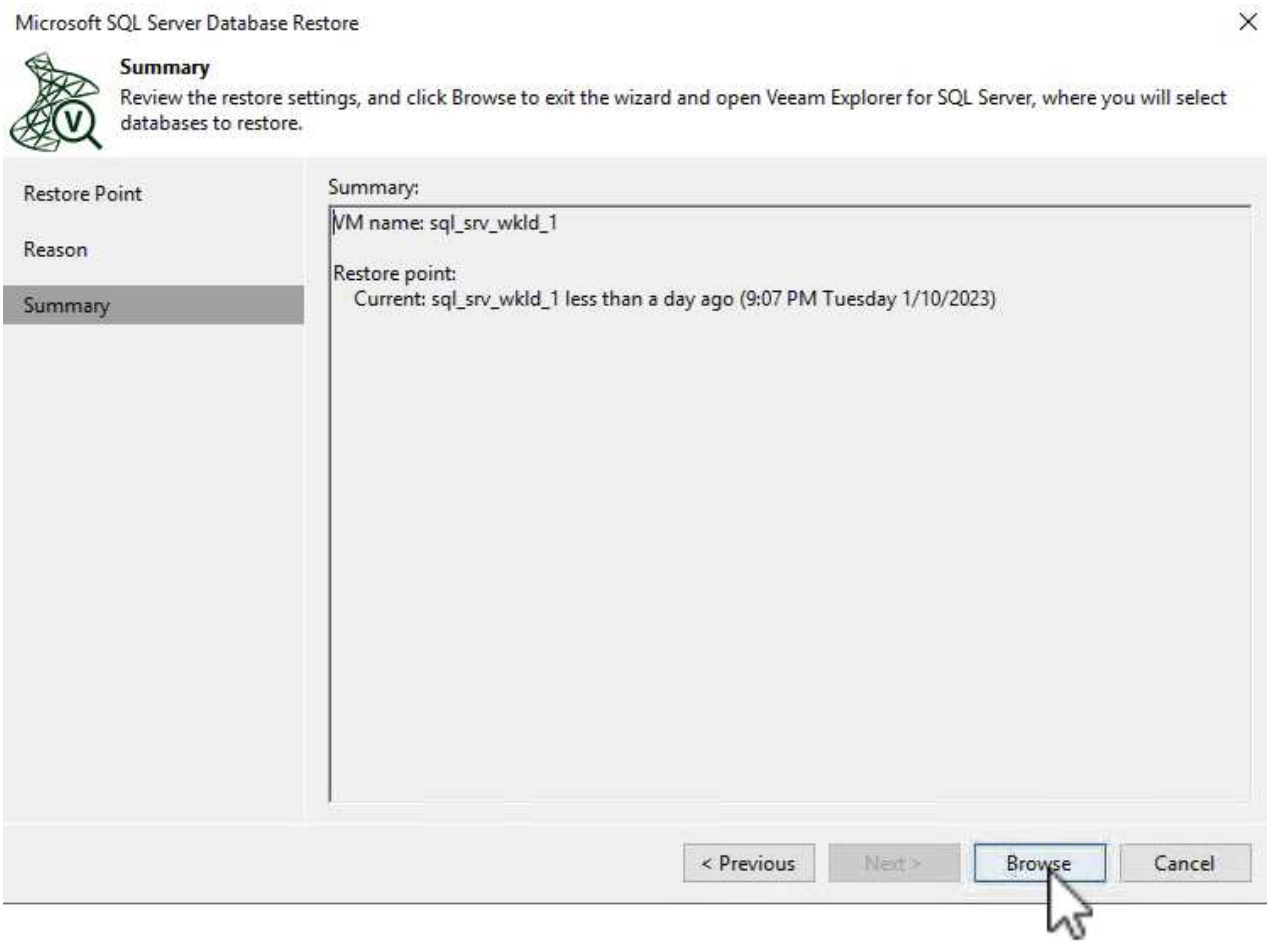
1. Dans la console Veeam Backup and Replication, naviguez jusqu'à la liste des sauvegardes SQL Server, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments d'application**, puis **bases de données Microsoft SQL Server…**.



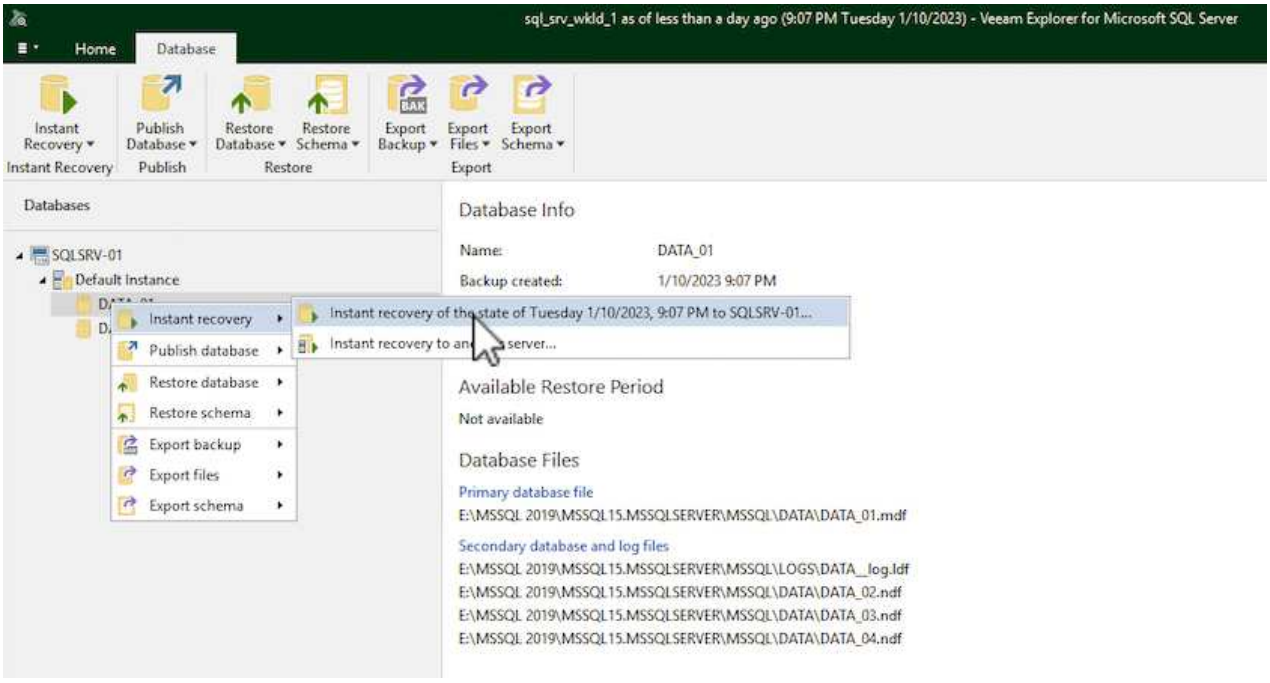
2. Dans l'Assistant de restauration de base de données Microsoft SQL Server, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.



3. Entrez un **motif de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer for Microsoft SQL Server.

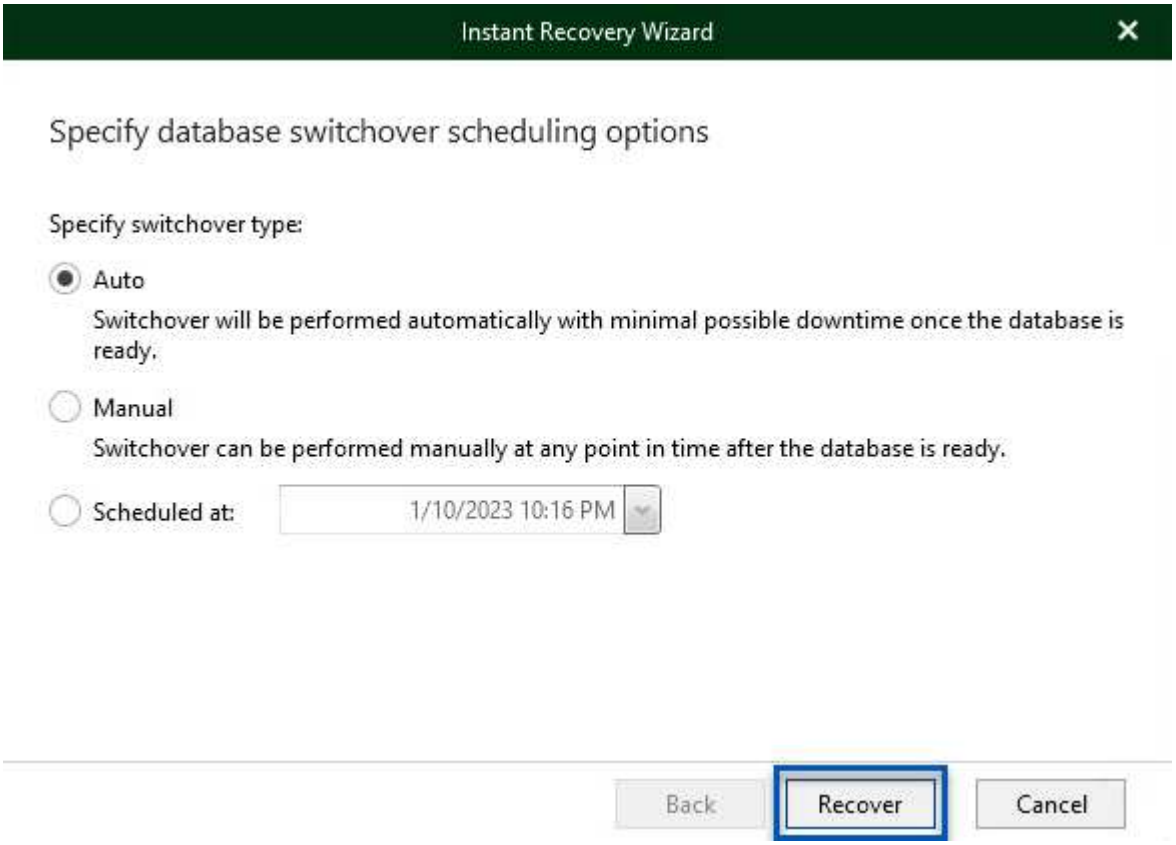


4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez avec le bouton droit de la souris et sélectionnez **Instant Recovery**, puis le point de restauration spécifique vers lequel effectuer la restauration.

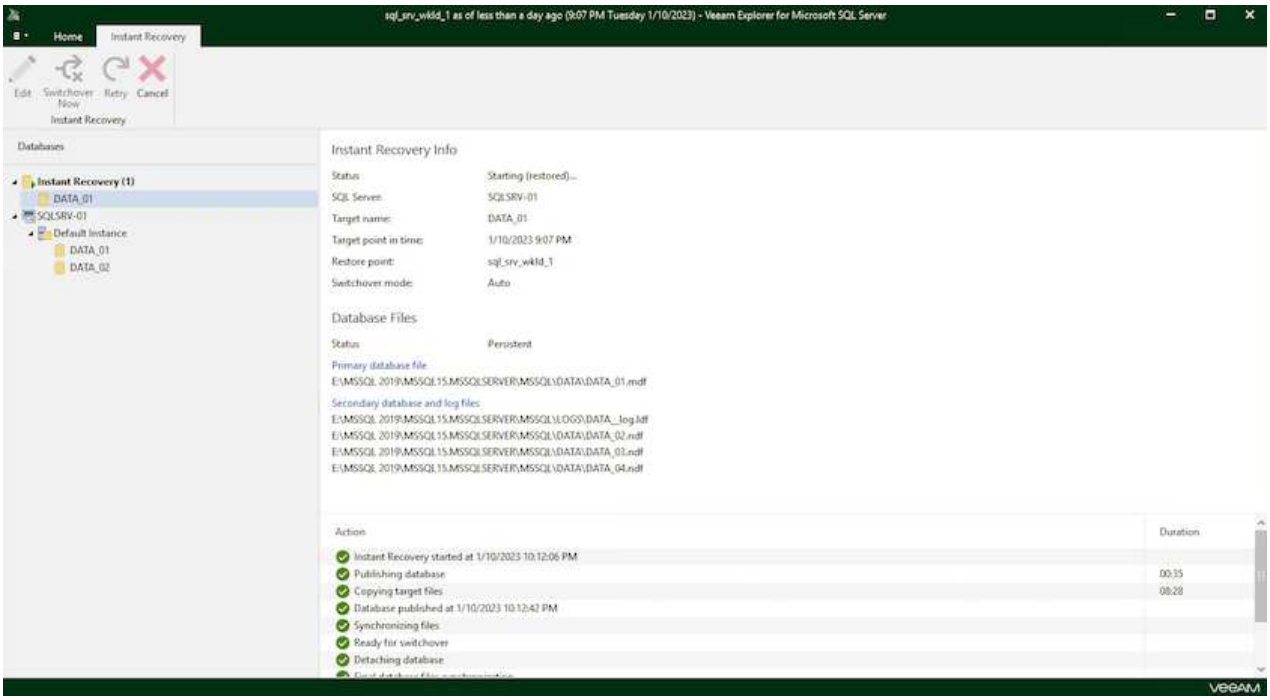


5. Dans l'Assistant de récupération instantanée, spécifiez le type de basculement. Ce processus peut

être automatique avec un temps d'arrêt minimal, manuellement ou à un moment donné. Cliquez ensuite sur le bouton **Recover** pour lancer le processus de restauration.



6. Le processus de restauration peut être surveillé depuis Veeam Explorer.



Pour plus d'informations sur les opérations de restauration SQL Server avec Veeam Explorer, reportez-vous à la section Microsoft SQL Server du "Guide de l'utilisateur de Veeam Explorers".

Restaurer des bases de données Oracle avec Veeam Explorer

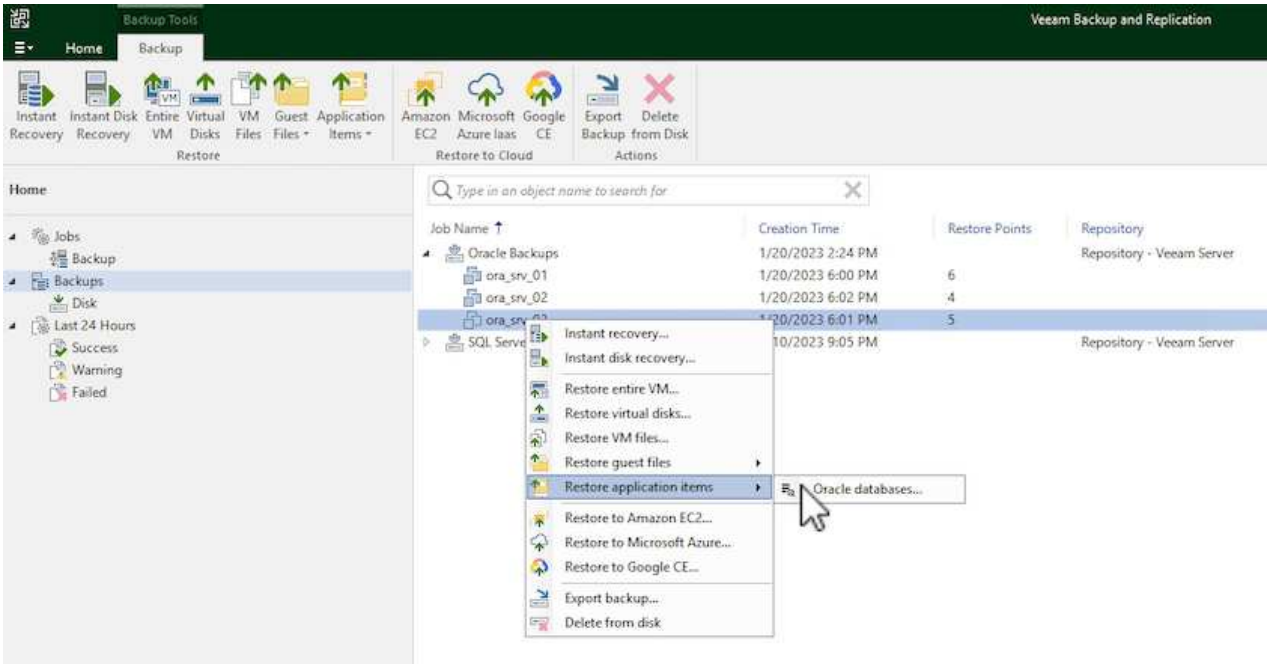
Veeam Explorer for Oracle Database offre la possibilité d'effectuer une restauration standard de base de données Oracle ou une restauration ininterrompue à l'aide d'Instant Recovery. Il prend également en charge les bases de données de publication pour un accès et une restauration rapides des bases de données Data Guard, ainsi que des restaurations à partir de sauvegardes RMAN.

Pour plus d'informations sur les opérations de restauration de bases de données Oracle avec Veeam Explorer, reportez-vous à la section Oracle du "Guide de l'utilisateur de Veeam Explorers".

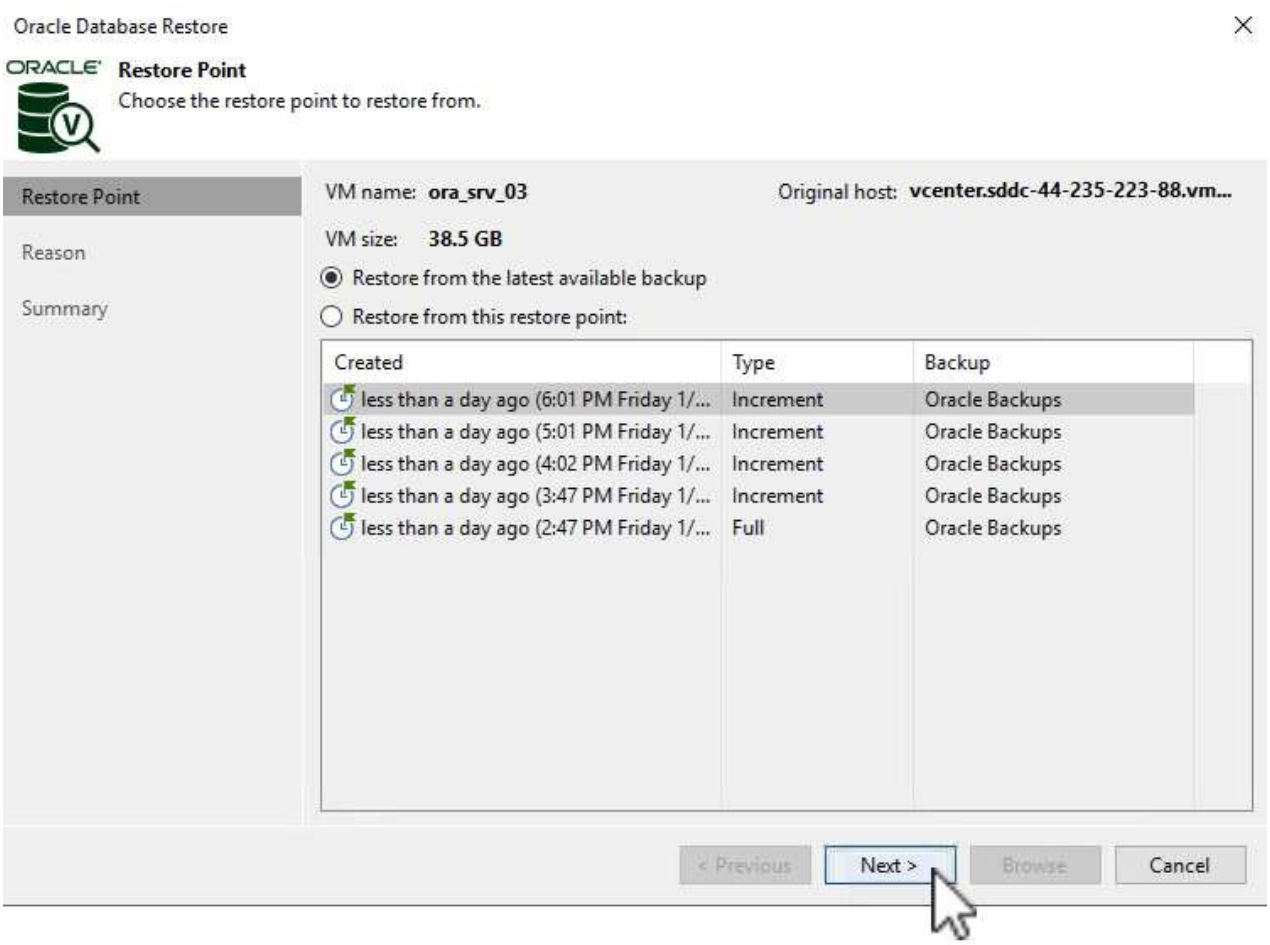
Restaurez la base de données Oracle avec Veeam Explorer

Dans cette section, la restauration d'une base de données Oracle sur un autre serveur est traitée à l'aide de Veeam Explorer.

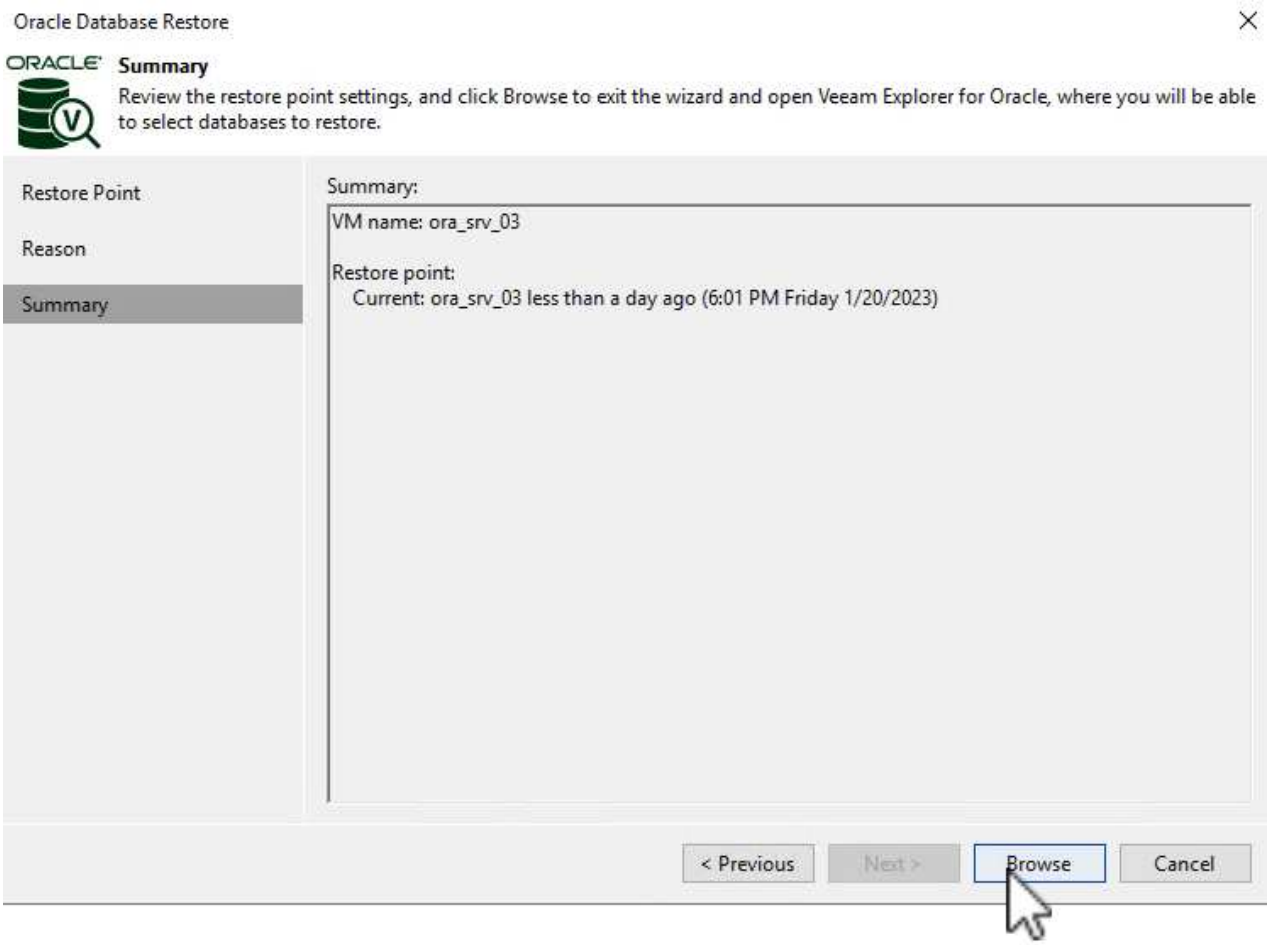
1. Dans la console Veeam Backup and Replication, naviguez jusqu'à la liste des sauvegardes Oracle, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments de l'application**, puis **bases de données Oracle…**.



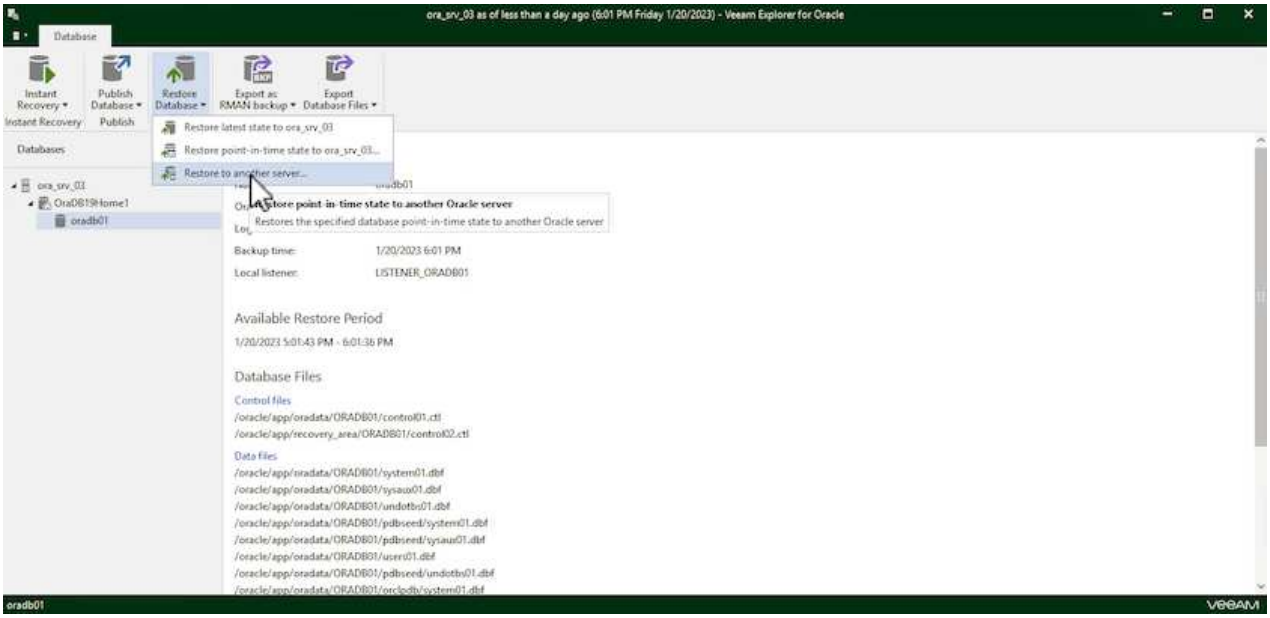
2. Dans l'assistant de restauration de la base de données Oracle, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.



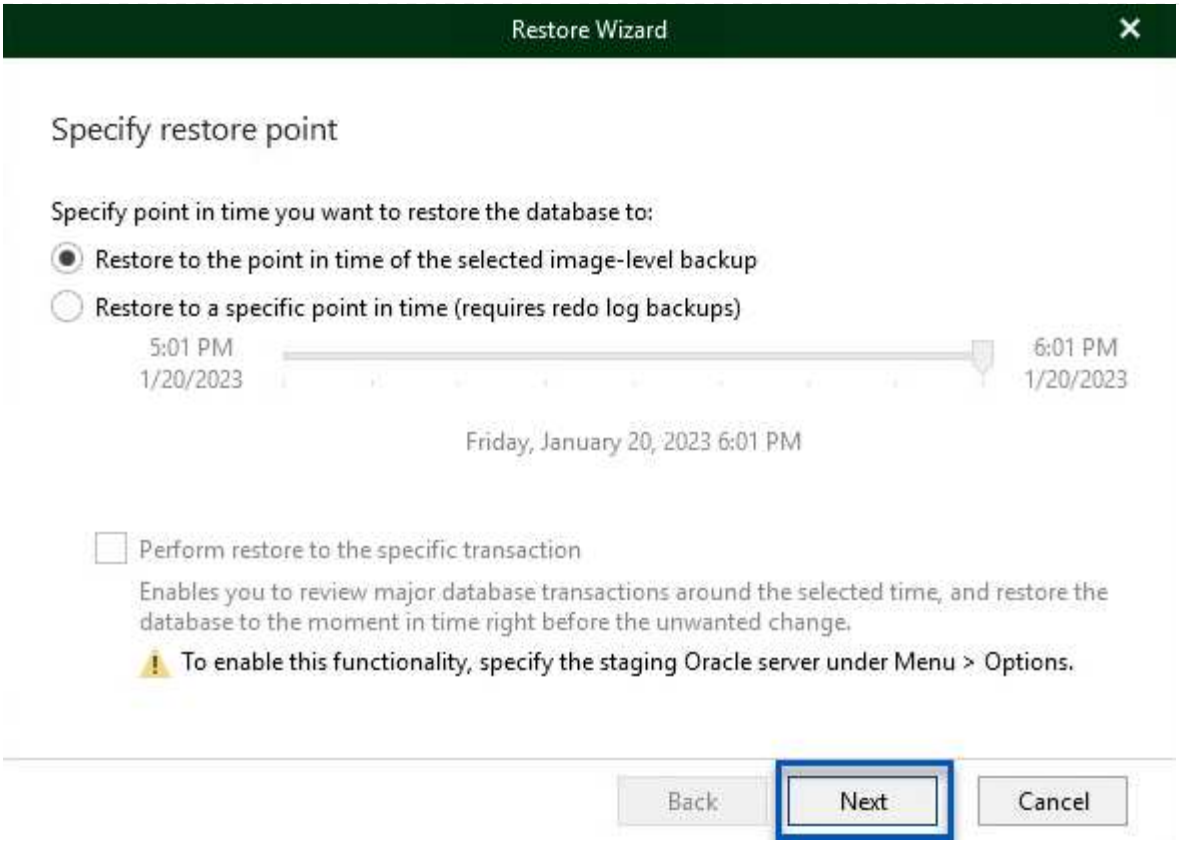
3. Entrez un **motif de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer for Oracle.



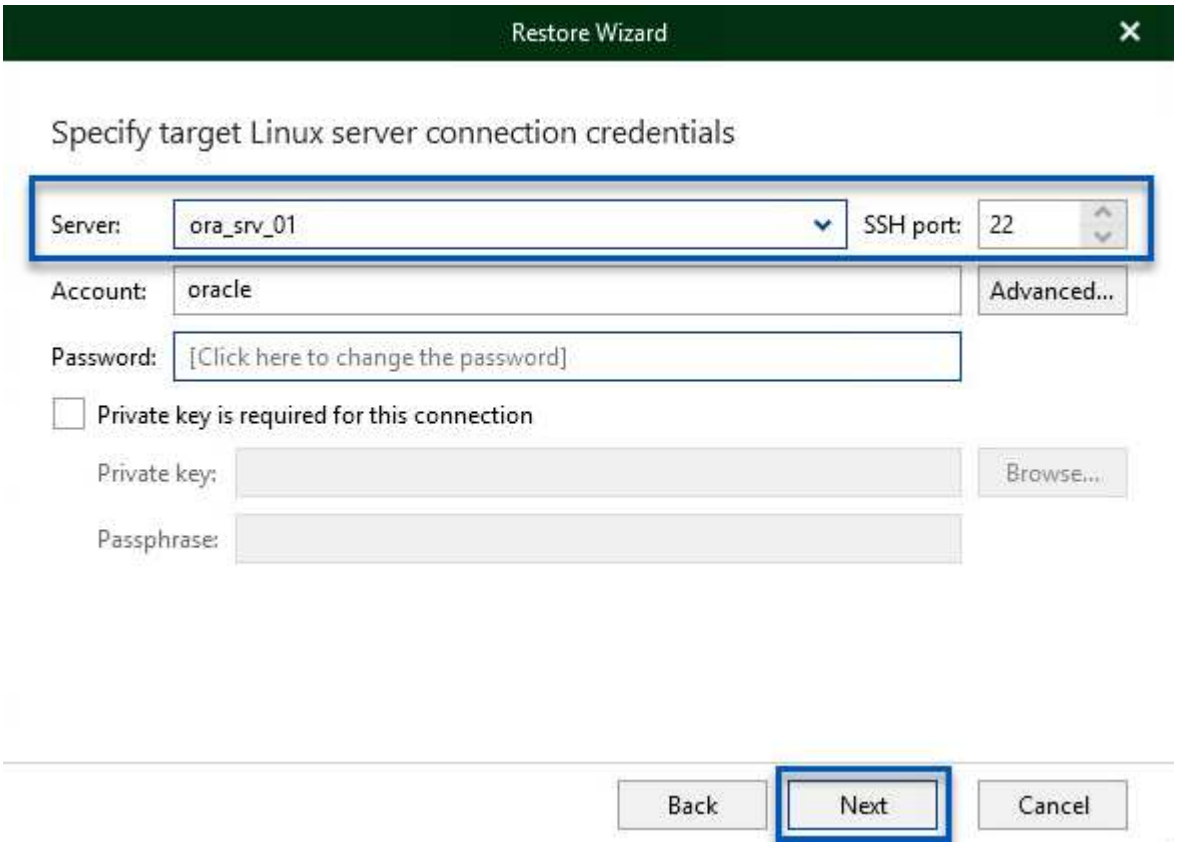
4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez sur la base de données à restaurer, puis dans le menu déroulant **Restaurer la base de données** en haut, sélectionnez **Restaurer sur un autre serveur…**.



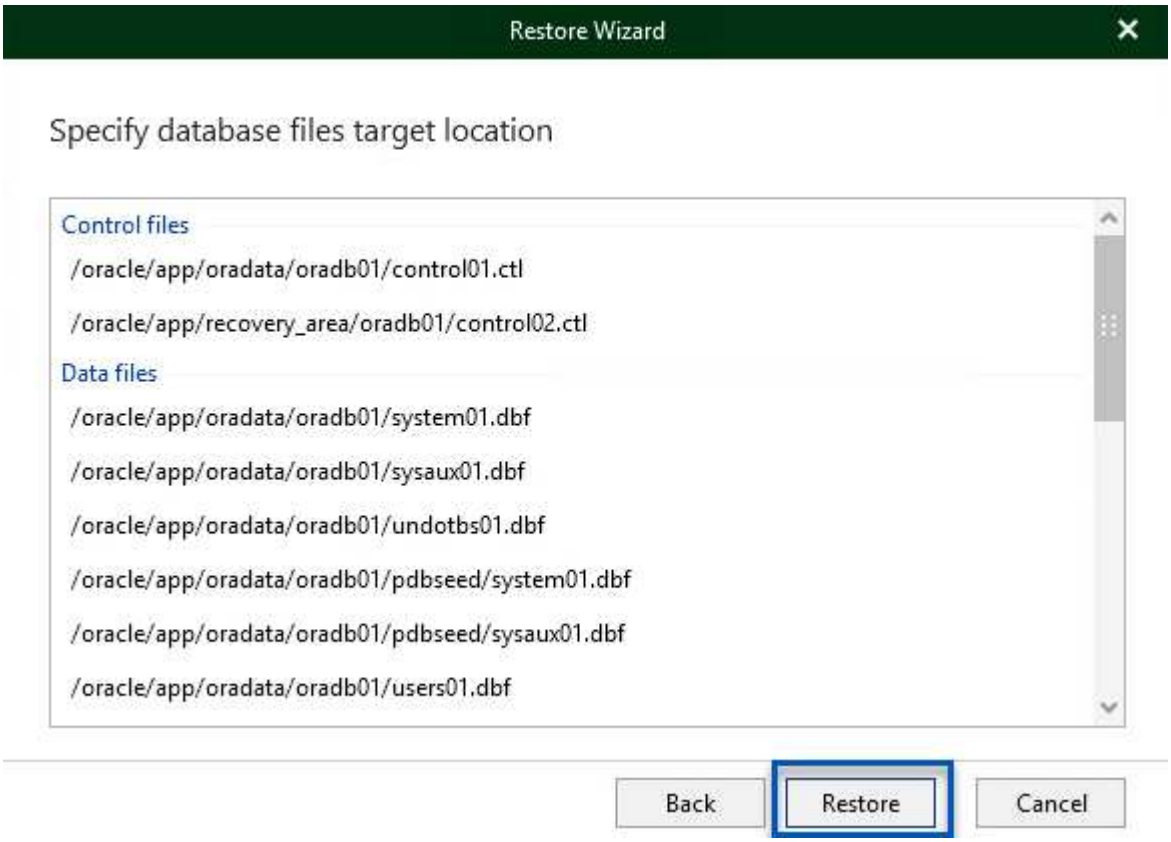
5. Dans l'Assistant de restauration, spécifiez le point de restauration à partir duquel effectuer la restauration et cliquez sur **Suivant**.



6. Spécifiez le serveur cible vers lequel la base de données sera restaurée et les informations d'identification du compte, puis cliquez sur **Suivant**.



7. Enfin, spécifiez l'emplacement cible des fichiers de base de données et cliquez sur le bouton **Restaurer** pour lancer le processus de restauration.

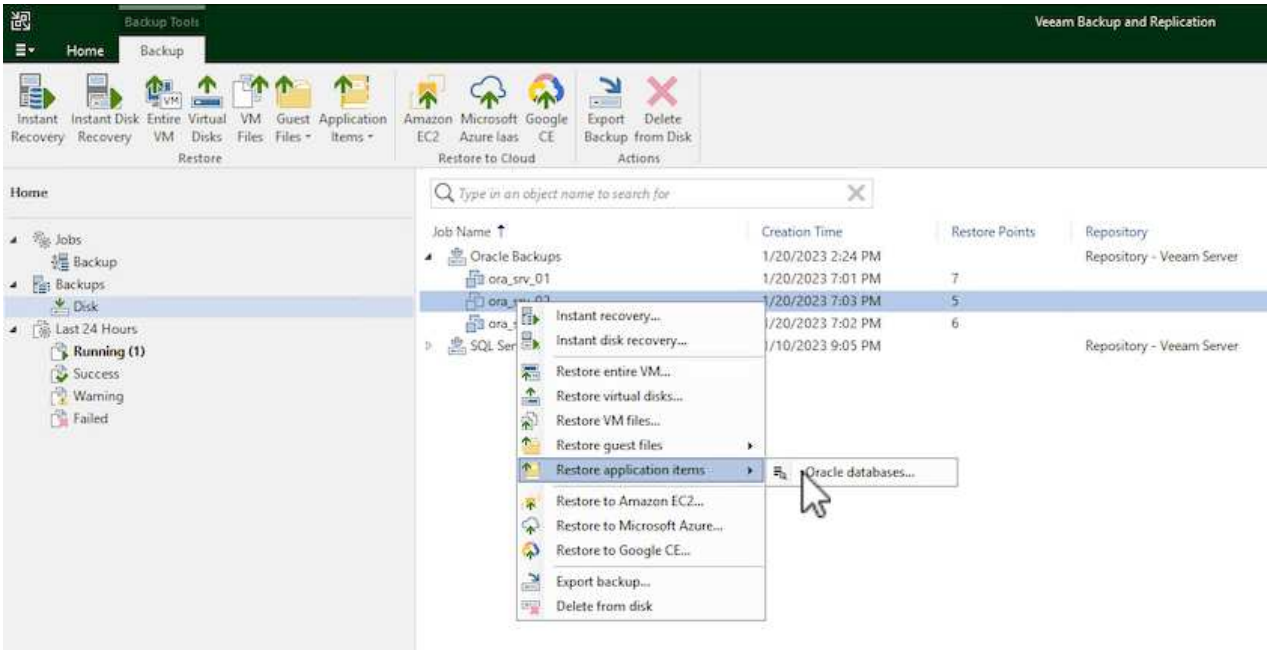


8. Une fois la restauration de la base de données terminée, vérifiez que la base de données Oracle démarre correctement sur le serveur.

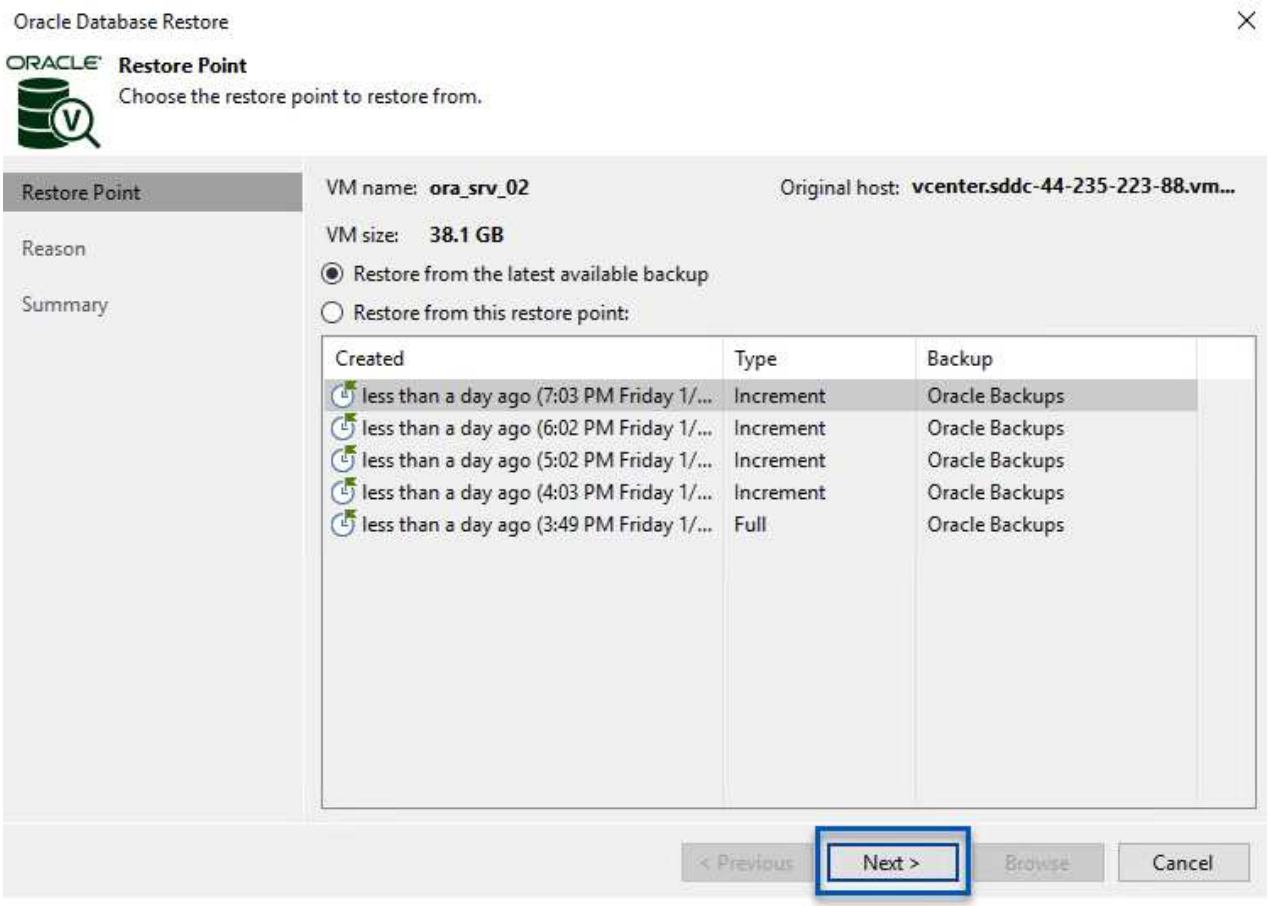
Publier la base de données Oracle sur un autre serveur

Dans cette section, une base de données est publiée sur un autre serveur pour un accès rapide sans lancer de restauration complète.

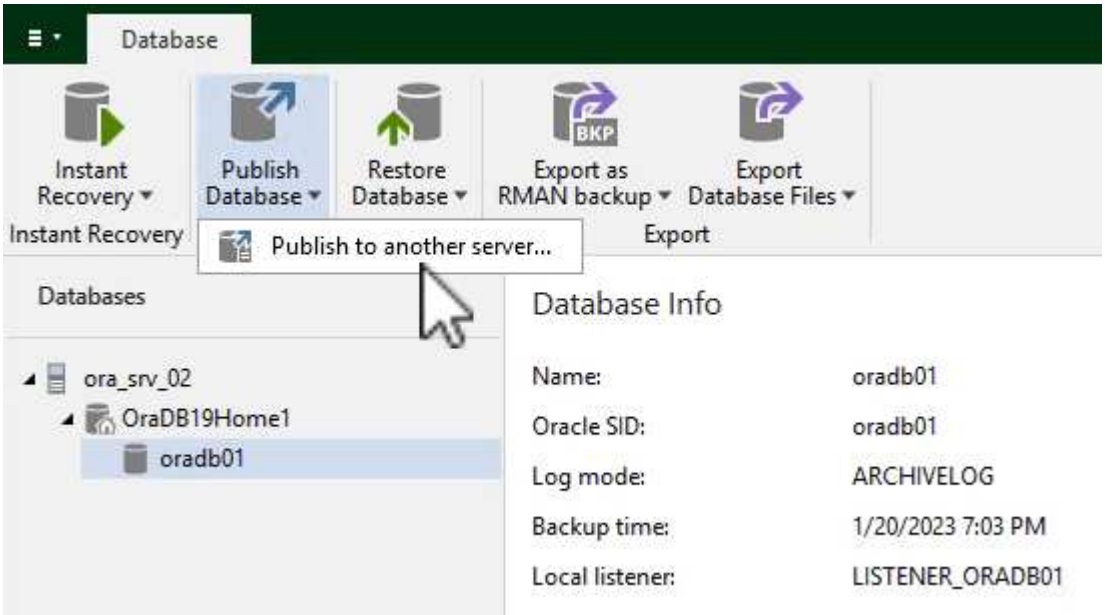
1. Dans la console Veeam Backup and Replication, naviguez jusqu'à la liste des sauvegardes Oracle, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments de l'application**, puis **bases de données Oracle…**.



2. Dans l'assistant de restauration de la base de données Oracle, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.

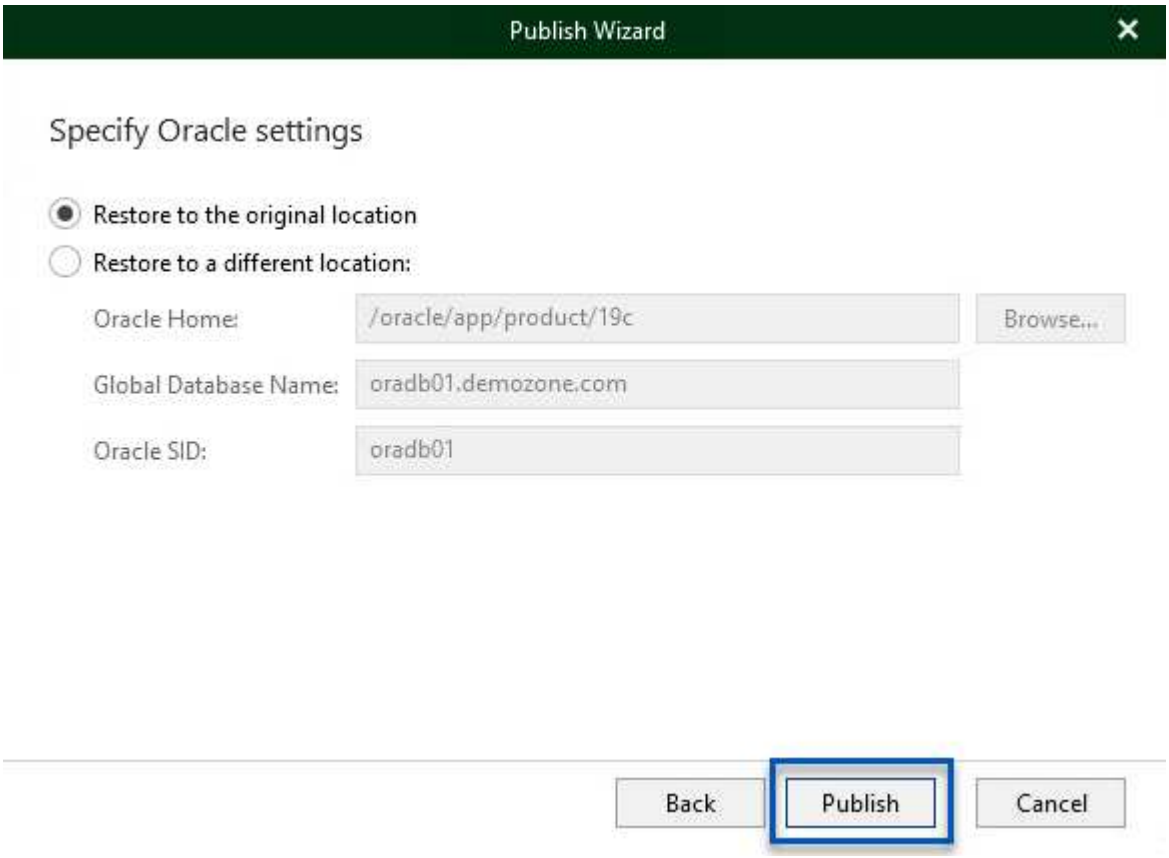


3. Entrez un **motif de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer for Oracle.
4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez sur la base de données à restaurer, puis dans le menu déroulant **publier la base de données** en haut, sélectionnez **publier sur un autre serveur…**.



5. Dans l'assistant de publication, spécifiez le point de restauration à partir duquel publier la base de données et cliquez sur **Suivant**.

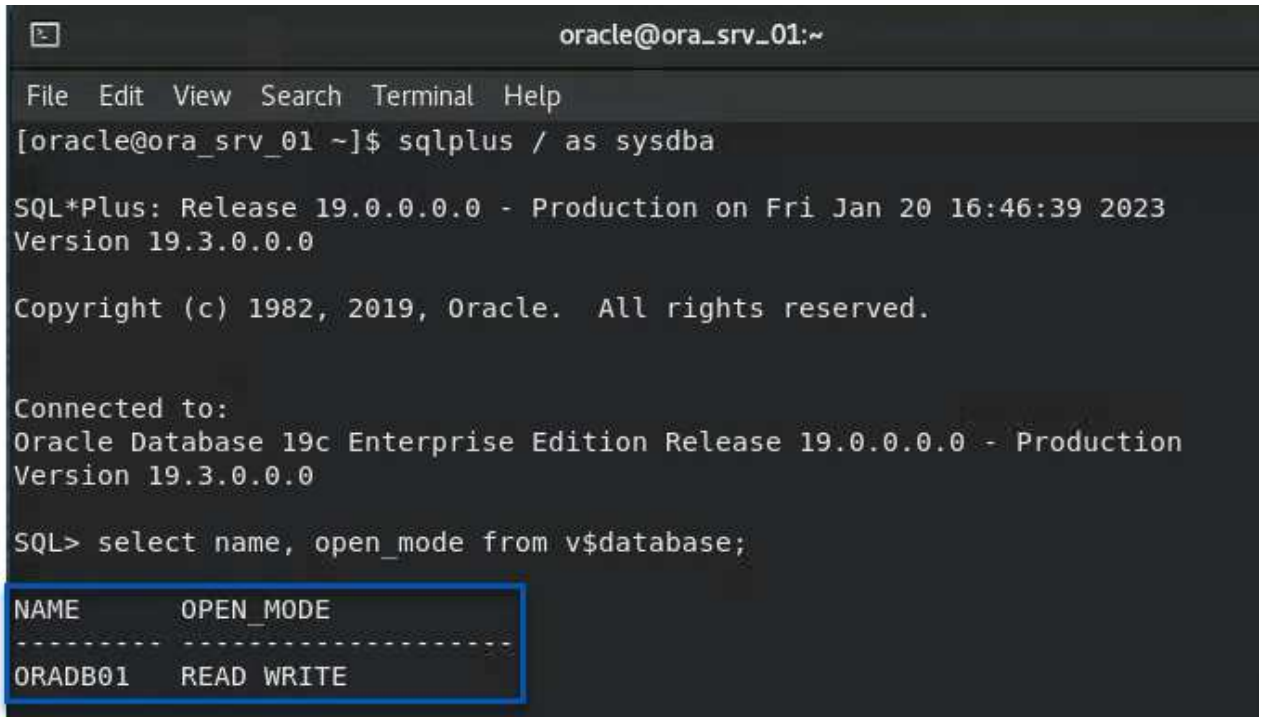
6. Enfin, spécifiez l'emplacement du système de fichiers linux cible et cliquez sur **publier** pour lancer le processus de restauration.



7. Une fois la publication terminée, connectez-vous au serveur cible et exécutez les commandes suivantes pour vous assurer que la base de données est en cours d'exécution :

```
oracle@ora_srv_01> sqlplus / as sysdba
```

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



Conclusion

VMware Cloud est une plateforme puissante pour exécuter des applications stratégiques et stocker des données sensibles. Pour assurer la continuité de l'activité et protéger les entreprises contre les cybermenaces et la perte de données, les entreprises qui font confiance à VMware Cloud ont besoin d'une solution de protection sécurisée des données. En optant pour une solution fiable et robuste de protection des données, les entreprises ont l'assurance que leurs données stratégiques sont sécurisées et sécurisées, en toutes circonstances.

Le cas d'utilisation présenté dans cette documentation est axé sur les technologies de protection des données à l'efficacité prouvée, qui mettent en avant l'intégration entre NetApp, VMware et Veeam. FSX pour ONTAP est pris en charge en tant que datastores NFS supplémentaires pour VMware Cloud dans AWS et est utilisé pour toutes les données des machines virtuelles et des applications. Veeam Backup & Replication est une solution complète de protection des données conçue pour aider les entreprises à améliorer, automatiser et rationaliser leurs processus de sauvegarde et de restauration. Veeam est utilisé conjointement avec les volumes cibles de sauvegarde iSCSI, hébergés sur FSX pour ONTAP, afin de fournir une solution de protection des données sécurisée et facile à gérer pour les données d'application résidant dans VMware Cloud.

Informations supplémentaires

Pour en savoir plus sur les technologies présentées dans cette solution, consultez les informations complémentaires suivantes.

- "Guide de l'utilisateur de FSX pour ONTAP"
- "Documentation technique du centre d'aide Veeam"
- "Prise en charge de VMware Cloud sur AWS. Considérations et limitations"

Tr-4955 : reprise après incident avec FSX pour ONTAP et VMC (AWS VMware Cloud)

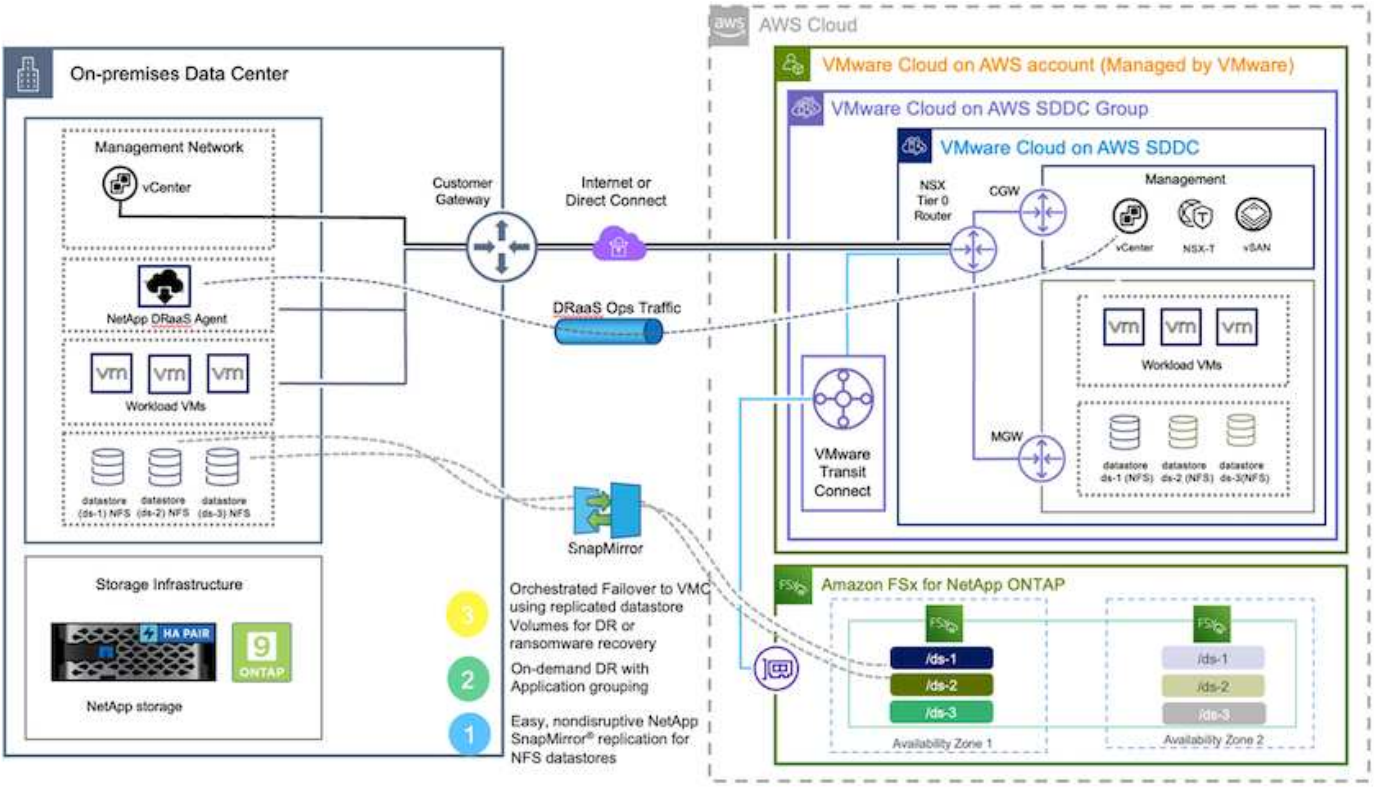
L'orchestrateur de reprise après incident (DRO, solution avec interface utilisateur) permet de restaurer de manière fluide les workloads répliqués depuis une infrastructure sur site vers FSX pour ONTAP. DRO automatise la restauration depuis le niveau SnapMirror, via l'enregistrement des machines virtuelles vers VMC, en passant par les mappages du réseau directement sur NSX-T. Cette fonction est incluse dans tous les environnements VMC.

Niyaz Mohamed, NetApp

Présentation

La reprise d'activité dans le cloud est une solution résiliente et économique de protection des workloads contre les pannes sur site et la corruption des données, par exemple, par ransomware. Avec la technologie NetApp SnapMirror, les charges de travail VMware sur site peuvent être répliquées vers FSX pour ONTAP exécutées dans AWS.

L'orchestrateur de reprise après incident (DRO, solution avec interface utilisateur) permet de restaurer de manière fluide les workloads répliqués depuis une infrastructure sur site vers FSX pour ONTAP. DRO automatise la restauration depuis le niveau SnapMirror, via l'enregistrement des machines virtuelles vers VMC, en passant par les mappages du réseau directement sur NSX-T. Cette fonction est incluse dans tous les environnements VMC.



Pour commencer

Déploiement et configuration de VMware Cloud sur AWS

"VMware Cloud sur AWS" Offre une expérience cloud native pour les charges de travail VMware dans l'écosystème AWS. Chaque SDDC (VMware Software-Defined Data Center) s'exécute dans un Amazon Virtual Private Cloud (VPC) et offre une pile VMware complète (y compris vCenter Server), la mise en réseau Software-defined NSX-T, le stockage Software-defined VSAN et un ou plusieurs hôtes ESXi qui fournissent des ressources de calcul et de stockage aux charges de travail. Pour configurer un environnement VMC sur AWS, procédez comme suit "lien". Un cluster de lampe témoin peut également être utilisé pour la reprise après incident.

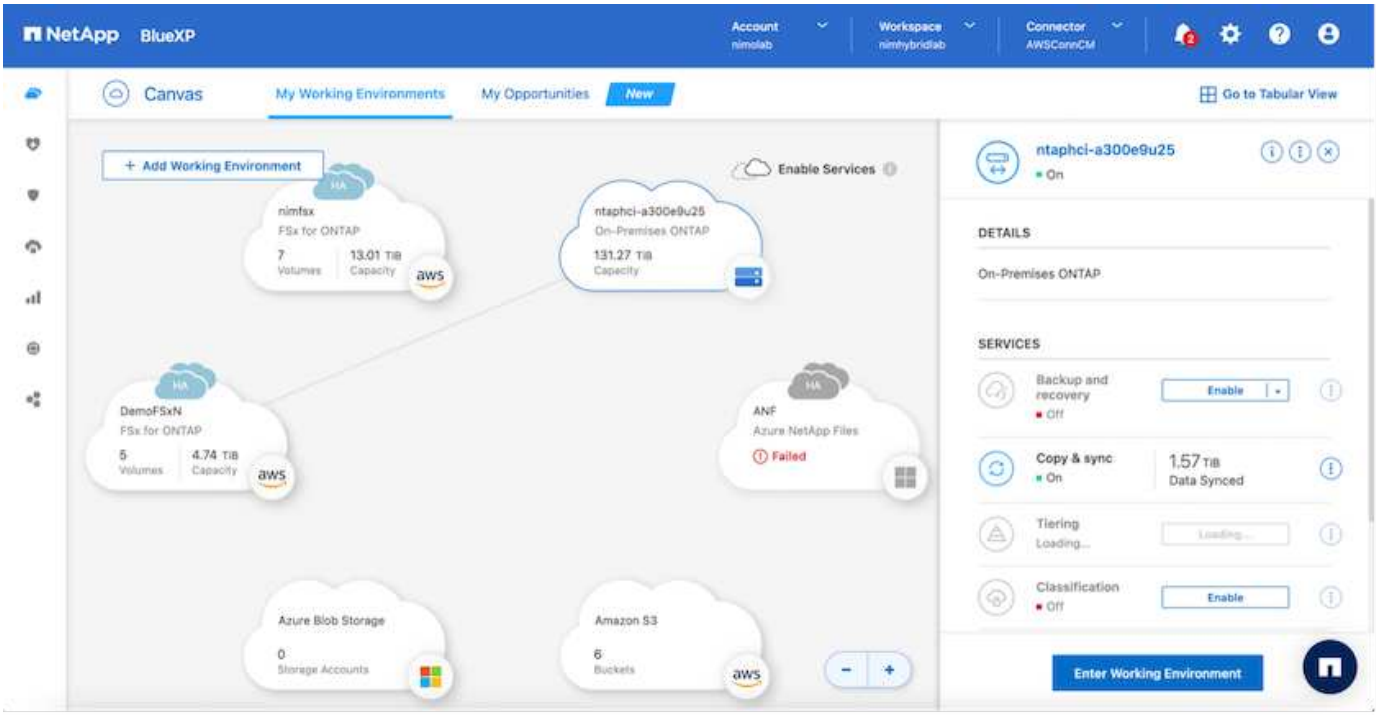
Dans la version initiale, l'analyseur DRO prend en charge un bloc de feux de pilotage existant. La création d'un SDDC à la demande sera disponible dans une prochaine version.

Provisionnement et configuration de FSX pour ONTAP

Amazon FSX pour NetApp ONTAP est un service entièrement géré qui offre un stockage de fichiers extrêmement fiable, évolutif, haute performance et riche en fonctionnalités basé sur le système de fichiers populaire NetApp ONTAP. Suivez les étapes à cet effet "lien" Pour provisionner et configurer FSX pour ONTAP.

Déploiement et configuration de SnapMirror vers FSX pour ONTAP

L'étape suivante consiste à utiliser NetApp BlueXP et à découvrir le FSX provisionné pour ONTAP sur une instance AWS, ainsi que à répliquer les volumes de datastore souhaités depuis un environnement sur site vers FSX pour ONTAP à la fréquence appropriée et à conserver les copies NetApp Snapshot :



Suivez les étapes de ce lien pour configurer BlueXP. Vous pouvez également utiliser l'interface de ligne de commande de NetApp ONTAP pour planifier la réplication en suivant ce lien.

Une relation SnapMirror est un prérequis qui doit être créée au préalable.

Installation de DRO

Pour commencer avec DRO, utilisez le système d'exploitation Ubuntu sur une instance EC2 ou une machine virtuelle désignée pour vous assurer que vous respectez les conditions préalables. Installez ensuite le package.

Prérequis

- Vérifiez l'existence d'une connectivité entre le vCenter source et le système de stockage et les systèmes de vCenter source et de destination.
- La résolution DNS doit être en place si vous utilisez des noms DNS. Sinon, vous devez utiliser des adresses IP pour vCenter et les systèmes de stockage.
- Créez un utilisateur avec des autorisations root. Vous pouvez également utiliser sudo avec une instance EC2.

Configuration requise pour le système d'exploitation

- Ubuntu 20.04 (LTS) avec au moins 2 Go et 4 CPU virtuels
- Les packages suivants doivent être installés sur la machine virtuelle de l'agent désigné :
  - Docker
  - Docker-composer
  - JQ

Modifiez les autorisations `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

Le `deploy.sh` le script exécute toutes les conditions préalables requises.

Installez l'emballage

1. Téléchargez le package d'installation sur la machine virtuelle désignée :

```
git clone https://github.com/NetApp/DRO-AWS.git
```

L'agent peut être installé sur site ou dans un VPC AWS.

2. Décompressez le package, exécutez le script de déploiement et saisissez l'adresse IP de l'hôte (par exemple, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Accédez au répertoire et exécutez le script de déploiement comme suit :

```
sudo sh deploy.sh
```

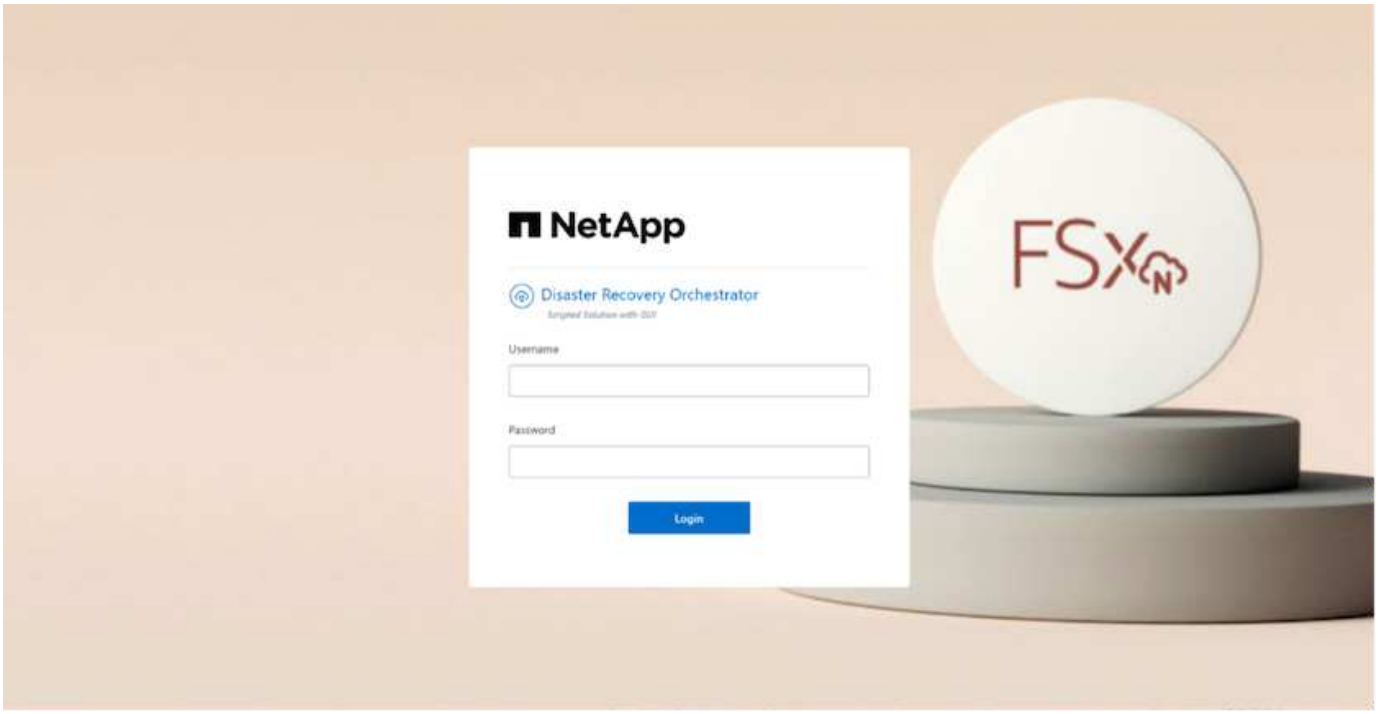
4. Pour accéder à l'interface utilisateur, procédez comme suit :

```
https://<host-ip-address>
```

avec les informations d'identification par défaut suivantes :

```
Username: admin
Password: admin
```

Le mot de passe peut être modifié à l'aide de l'option « Modifier le mot de passe ».



Configuration DRO

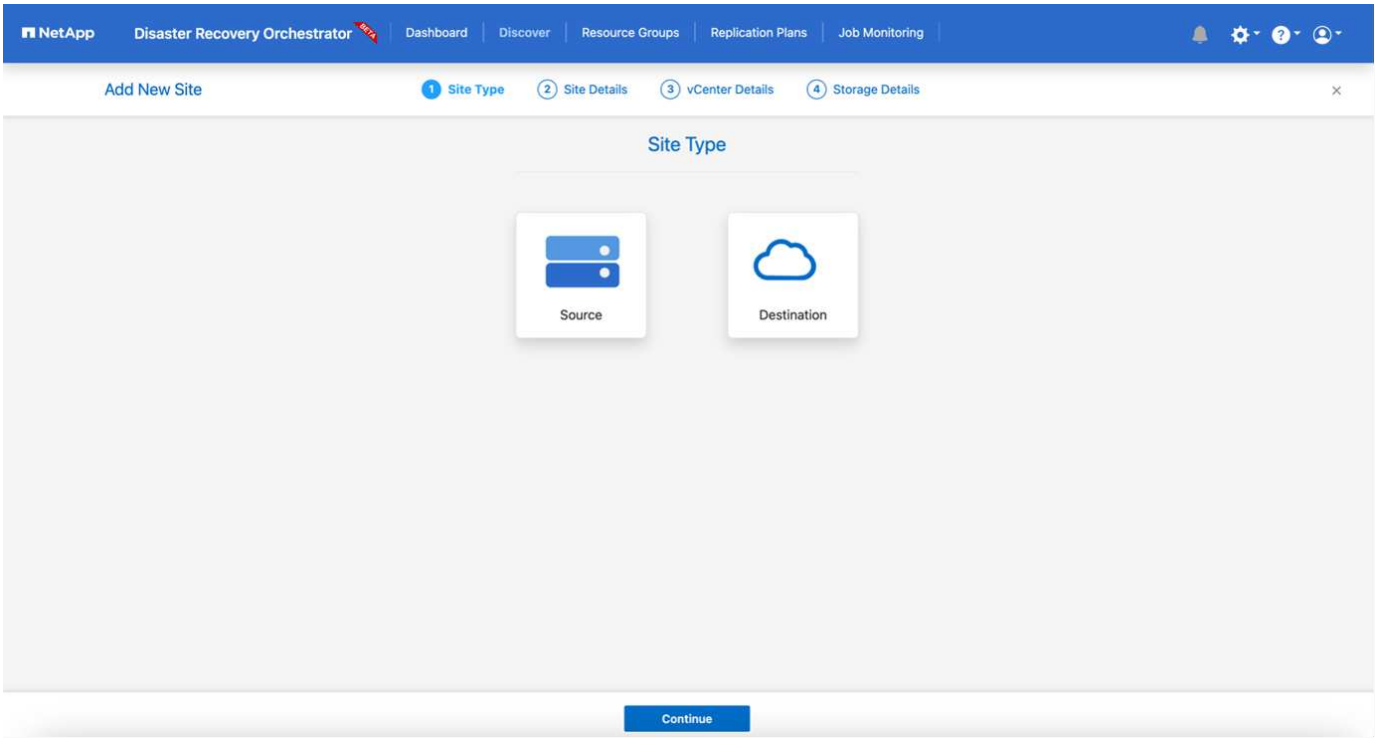
Une fois que FSX pour ONTAP et VMC ont été configurés correctement, vous pouvez commencer à configurer DRO pour automatiser la restauration des charges de travail sur site vers VMC à l'aide des copies SnapMirror en lecture seule sur FSX pour ONTAP.

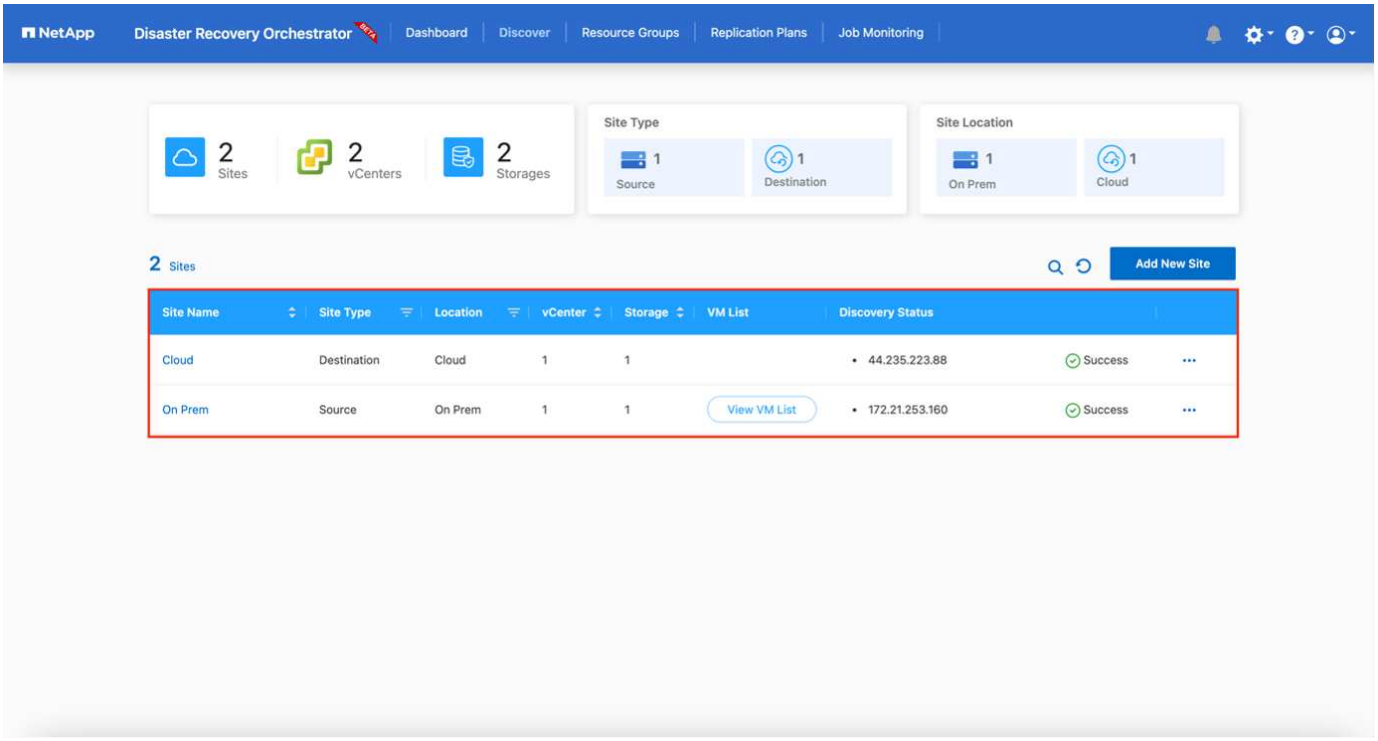
NetApp recommande de déployer l'agent DRO dans AWS et de choisir le même VPC où FSX pour ONTAP est déployé (qui peut également être connecté à des pairs), Afin que l'agent DRO puisse communiquer via le réseau avec vos composants sur site ainsi qu'avec les ressources FSX pour ONTAP et VMC.

La première étape consiste à découvrir et à ajouter les ressources cloud et sur site (vCenter et du stockage) à DRO. Ouvrez DRO dans un navigateur pris en charge et utilisez le nom d'utilisateur et le mot de passe par défaut (admin/admin) et Ajouter des sites. Vous pouvez également ajouter des sites à l'aide de l'option découverte. Ajoutez les plates-formes suivantes :

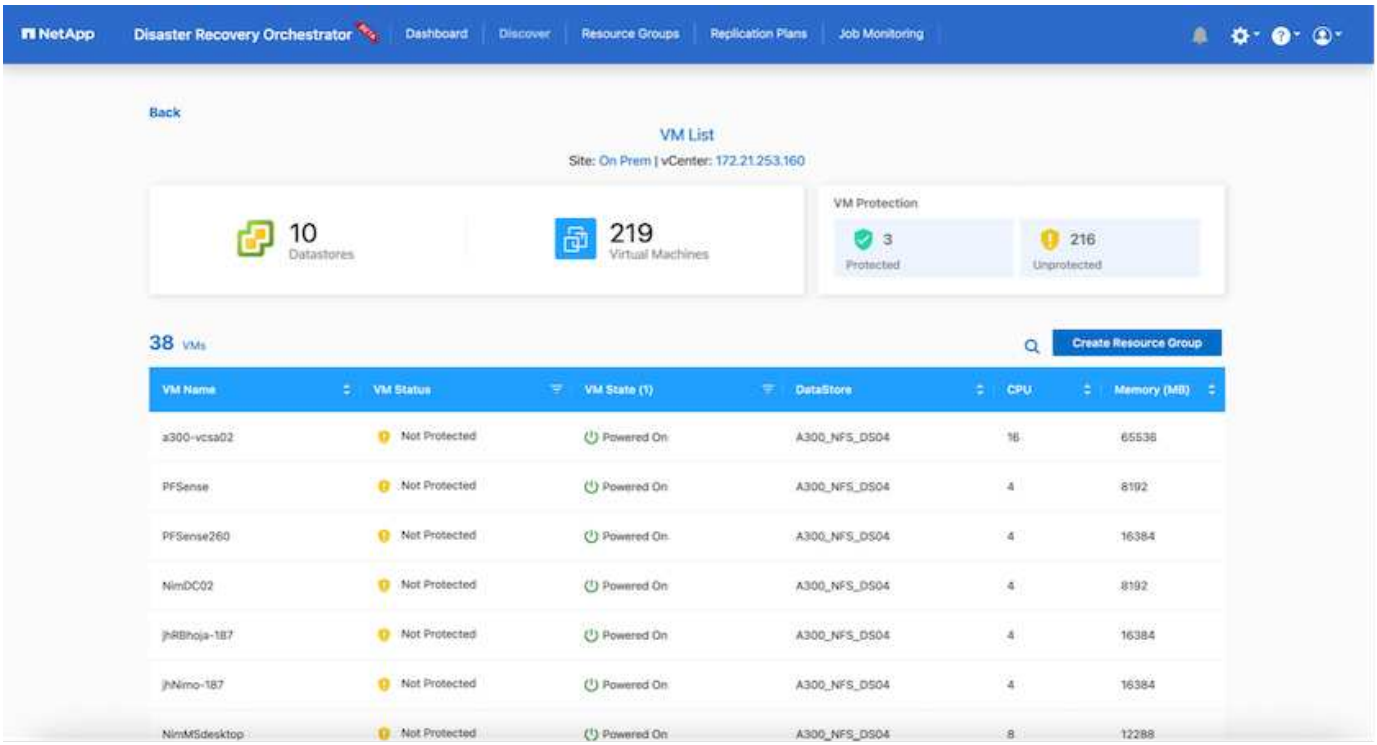
- Sur site
  - VCenter sur site
  - Système de stockage ONTAP

- Le cloud
  - VMC vCenter
  - FSX pour ONTAP





Une fois ajouté, DRO effectue une détection automatique et affiche les machines virtuelles sur lesquelles les répliques SnapMirror correspondantes s'effectuent depuis le stockage source vers FSX pour ONTAP. DRO détecte automatiquement les réseaux et les groupes de ports utilisés par les VM et les remplit.



L'étape suivante consiste à regrouper les machines virtuelles requises dans des groupes fonctionnels pour servir de groupes de ressources.

Regroupements de ressources

Une fois les plates-formes ajoutées, vous pouvez regrouper les machines virtuelles que vous souhaitez restaurer dans des groupes de ressources. Les groupes de ressources DRO vous permettent de regrouper un ensemble de VM dépendants en groupes logiques contenant leurs ordres de démarrage, leurs délais de démarrage et les validations d'applications facultatives qui peuvent être exécutées lors de la récupération.

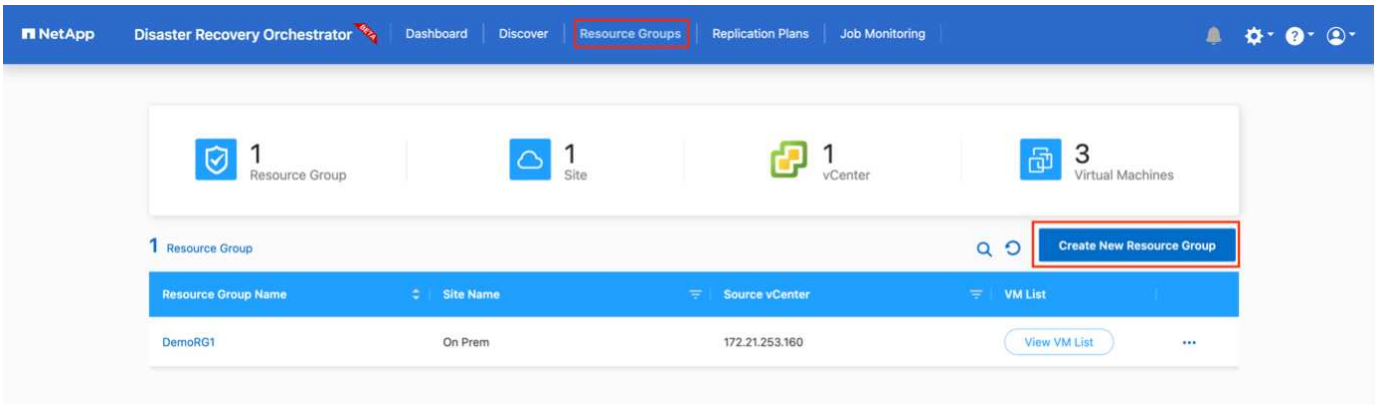
Pour commencer à créer des groupes de ressources, procédez comme suit :

1. Accédez à **groupes de ressources**, puis cliquez sur **Créer un nouveau groupe de ressources**.
2. Sous **Nouveau groupe de ressources**, sélectionnez le site source dans la liste déroulante et cliquez sur **Créer**.
3. Fournissez **Détails du groupe de ressources** et cliquez sur **Continuer**.
4. Sélectionnez les machines virtuelles appropriées à l'aide de l'option de recherche.
5. Sélectionnez l'ordre de démarrage et le délai de démarrage (s) pour les machines virtuelles sélectionnées. Définissez l'ordre de mise sous tension en sélectionnant chaque VM et en définissant sa priorité. La valeur par défaut est Three pour toutes les machines virtuelles.

   Les options sont les suivantes :

   1 – première machine virtuelle à mettre sous tension 3 – valeur par défaut 5 – dernière machine virtuelle à mettre sous tension

6. Cliquez sur **Créer un groupe de ressources**.

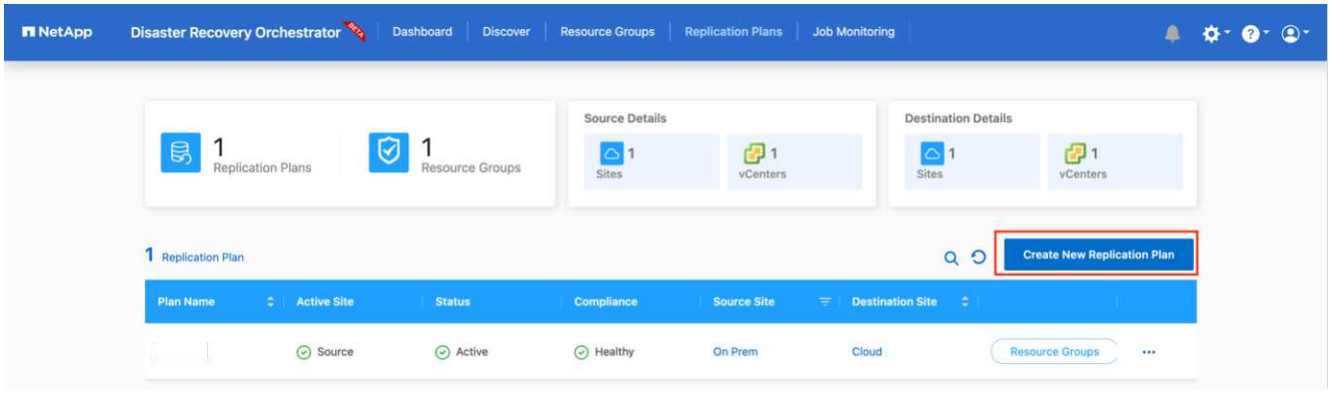


Plans de réplication

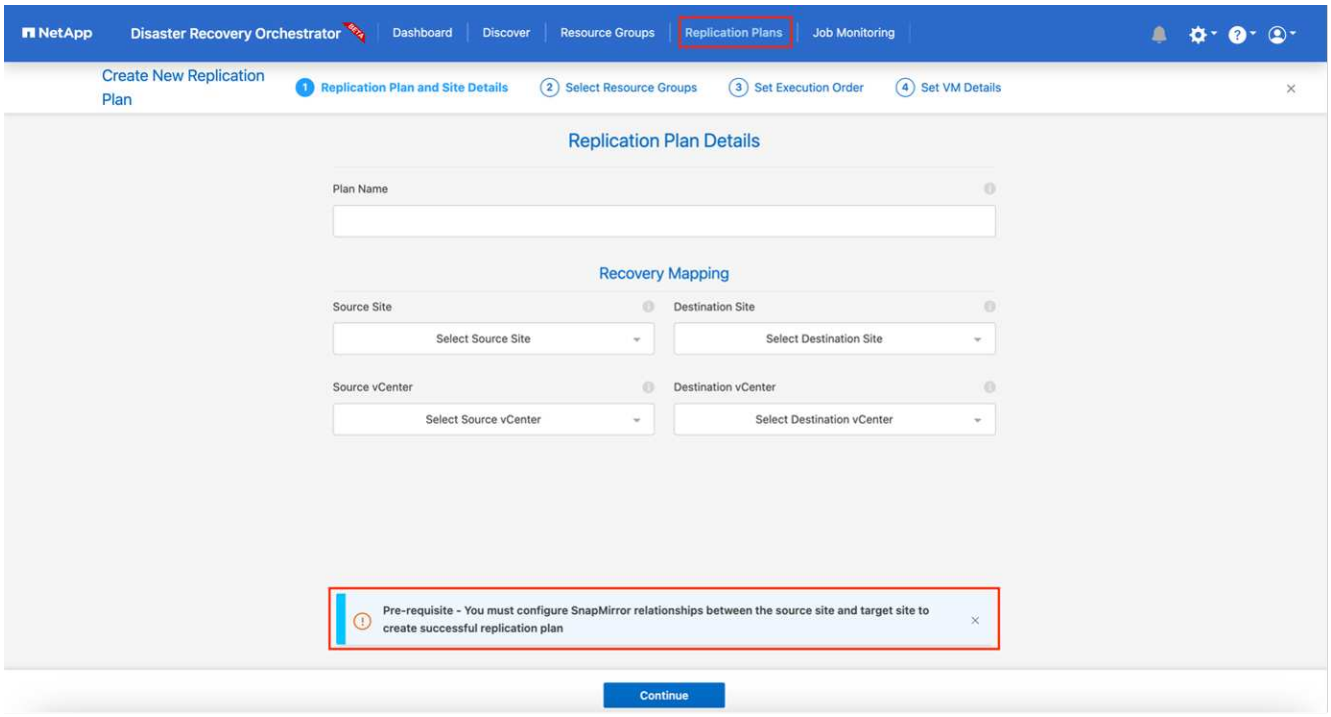
Vous devez disposer d'un plan de restauration des applications en cas d'incident. Sélectionnez les plates-formes vCenter source et cible dans la liste déroulante et sélectionnez les groupes de ressources à inclure dans ce plan, ainsi que le regroupement de la manière dont les applications doivent être restaurées et mises sous tension (par exemple, contrôleurs de domaine, puis niveau 1, niveau 2, etc.). De tels plans sont parfois appelés des plans de projet. Pour définir le plan de reprise, accédez à l'onglet **Plan de réplication** et cliquez sur **Nouveau Plan de réplication**.

Pour commencer à créer un plan de réplication, procédez comme suit :

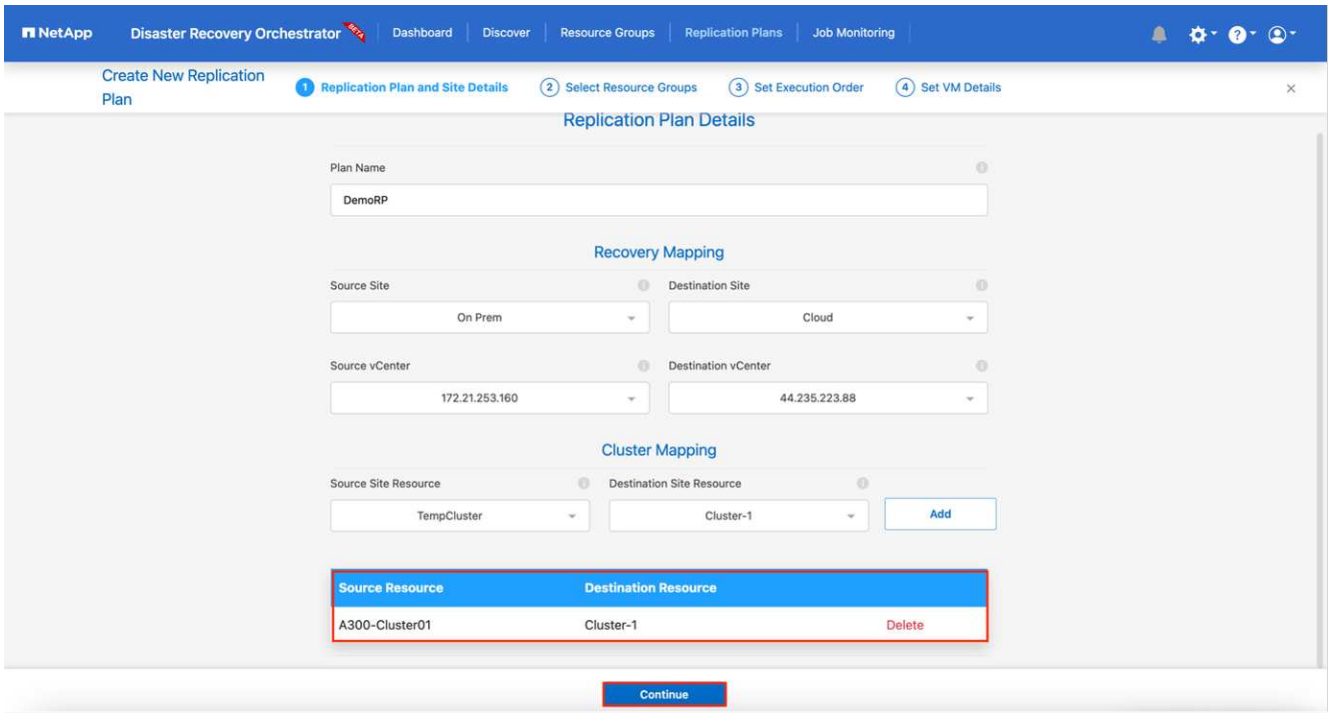
1. Accédez à **plans de réplication**, puis cliquez sur **Créer un nouveau plan de réplication**.



2. Sous **Nouveau plan de réplication**, indiquez un nom pour le plan et ajoutez des mappages de reprise en sélectionnant le site source, le serveur vCenter associé, le site de destination et le serveur vCenter associé.

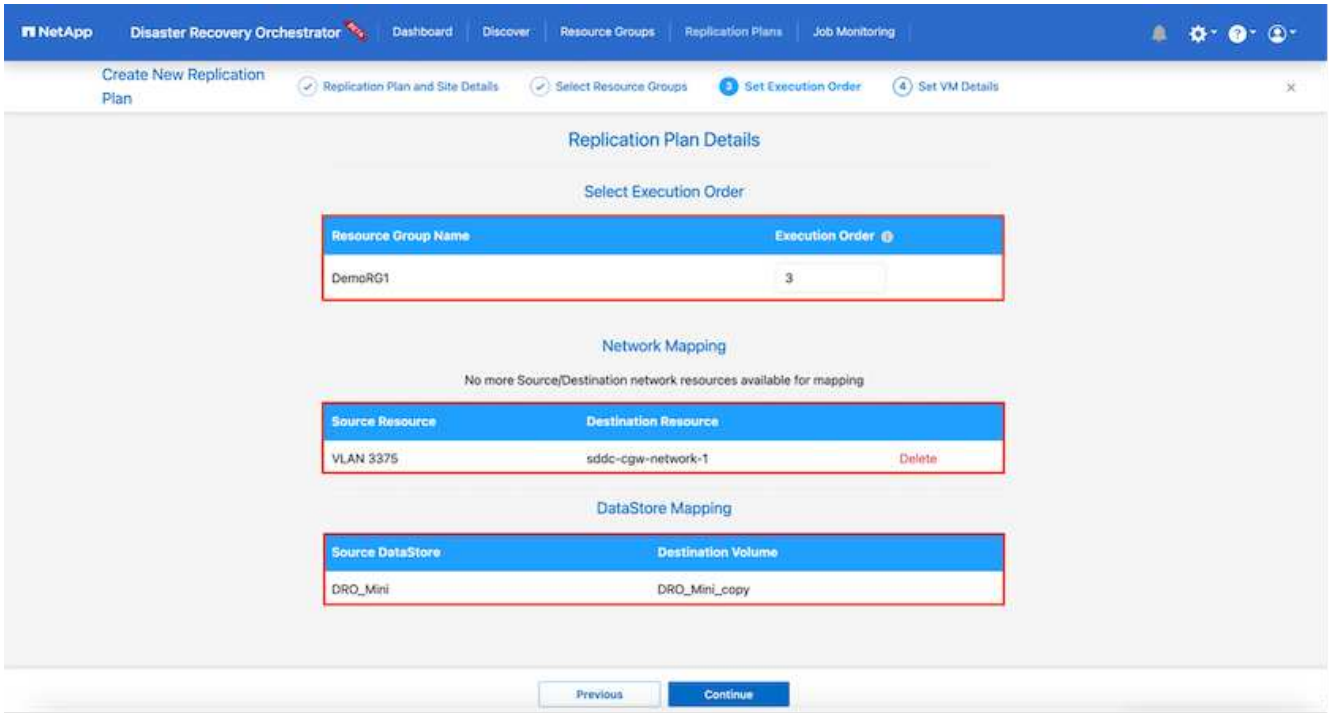


3. Une fois le mappage de restauration terminé, sélectionnez le mappage de cluster.

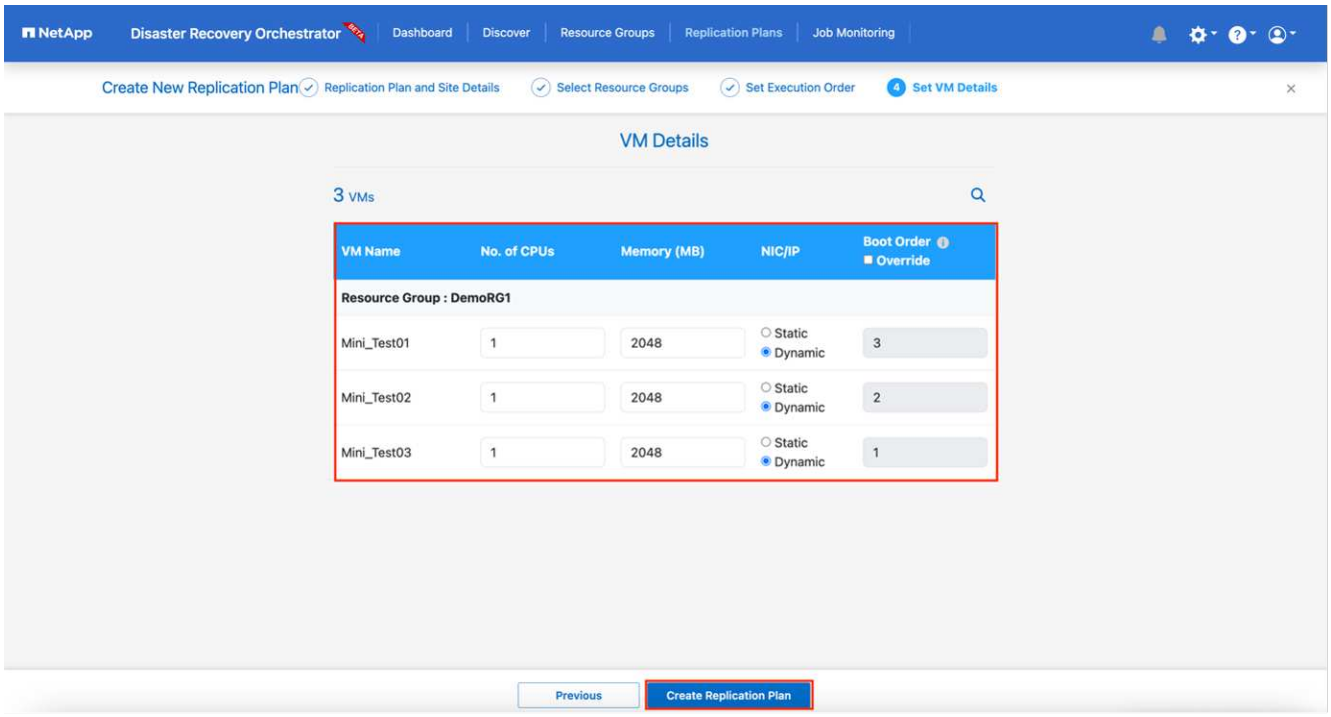


4. Sélectionnez **Détails du groupe de ressources** et cliquez sur **Continuer**.
5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsqu'il existe plusieurs groupes de ressources.
6. Une fois que vous avez terminé, sélectionnez le mappage réseau au segment approprié. Les segments doivent déjà être configurés dans VMC, sélectionnez donc le segment approprié pour mapper la VM.
7. En fonction de la sélection des machines virtuelles, les mappages des datastores sont sélectionnés automatiquement.

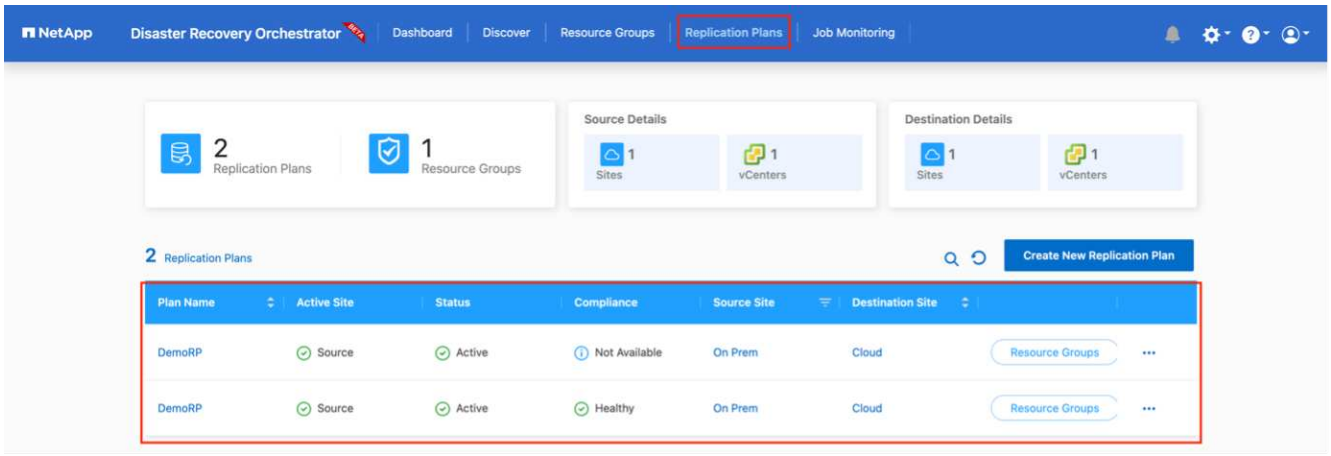
SnapMirror est au niveau du volume. Par conséquent, tous les VM sont répliqués sur la destination de réplication. Veillez à sélectionner toutes les machines virtuelles faisant partie du datastore. Si elles ne sont pas sélectionnées, seules les machines virtuelles qui font partie du plan de réplication sont traitées.



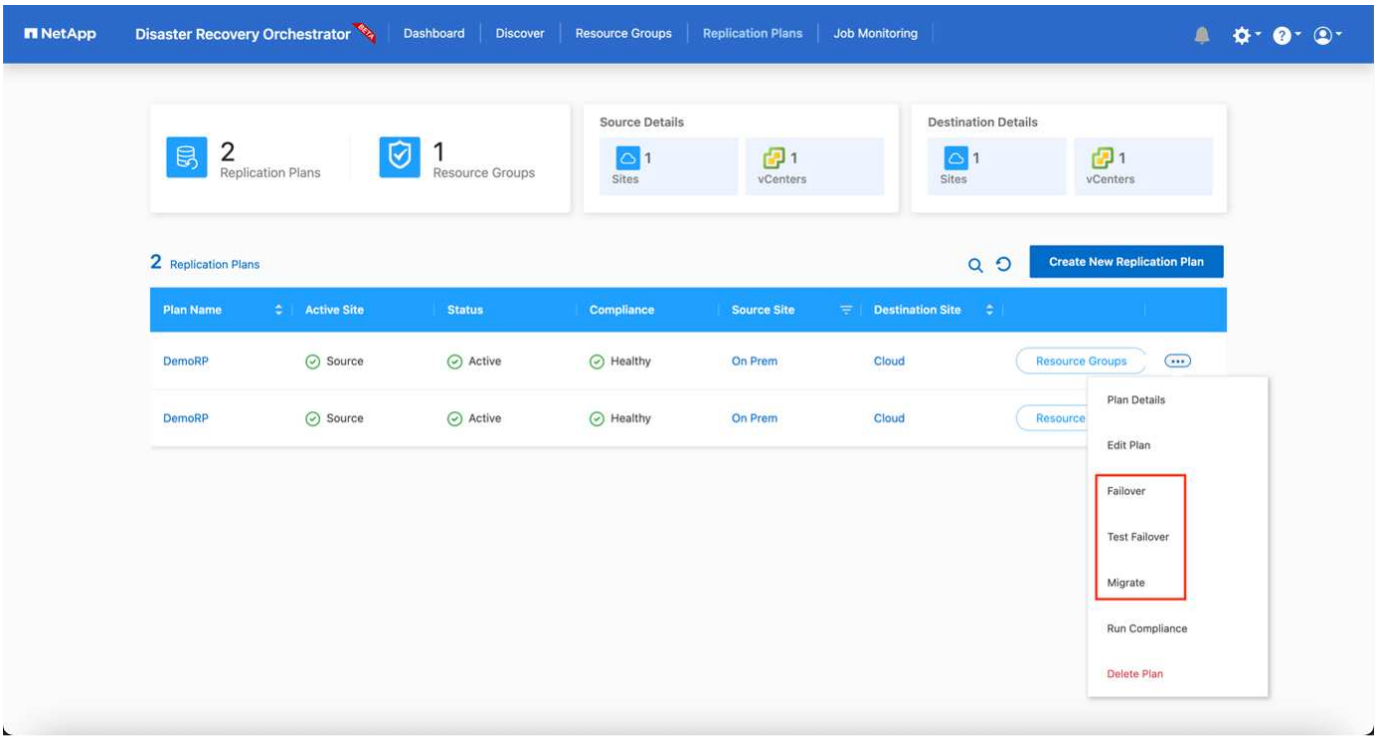
8. Sous les détails de la machine virtuelle, vous pouvez éventuellement redimensionner les paramètres de CPU et de RAM de la machine virtuelle. Cette approche peut être très utile pour restaurer de grands environnements sur des clusters cibles plus petits ou pour effectuer des tests de reprise sur incident sans avoir à provisionner une infrastructure physique VMware individuelle. Vous pouvez également modifier l'ordre de démarrage et le délai de démarrage (en secondes) de toutes les machines virtuelles sélectionnées au sein des groupes de ressources. Il existe une option supplémentaire permettant de modifier l'ordre de démarrage si des modifications sont requises de celles sélectionnées lors de la sélection de l'ordre de démarrage du groupe de ressources. Par défaut, l'ordre de démarrage sélectionné lors de la sélection du groupe de ressources est utilisé ; toutefois, les modifications peuvent être effectuées à ce stade.

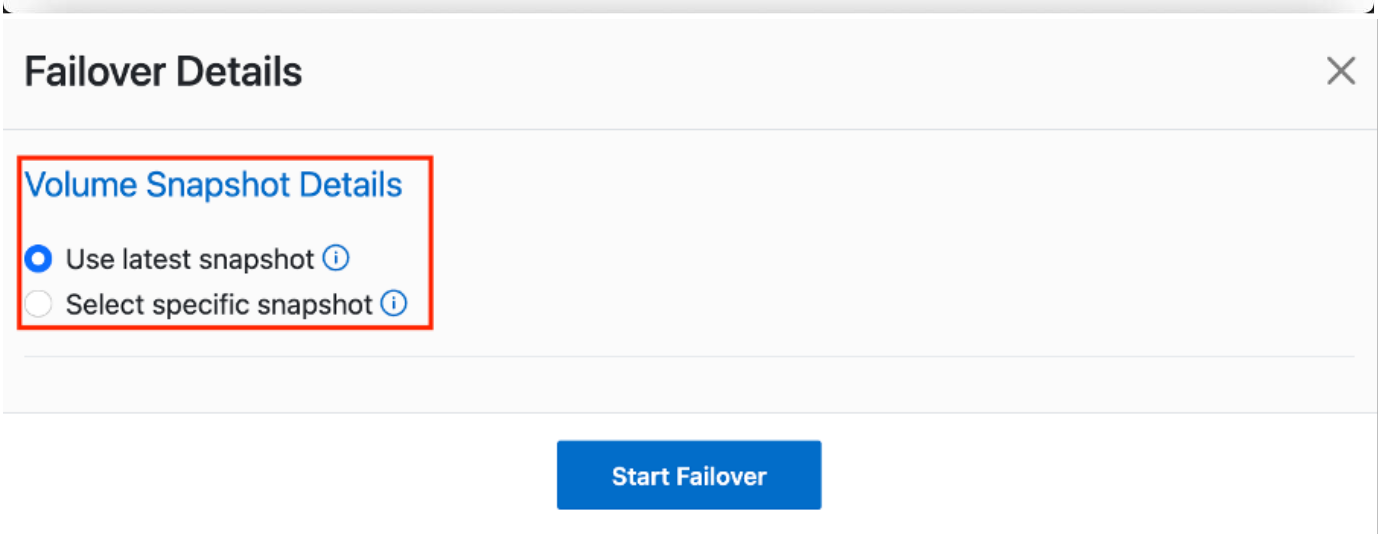


9. Cliquez sur **Créer un plan de réplication**.

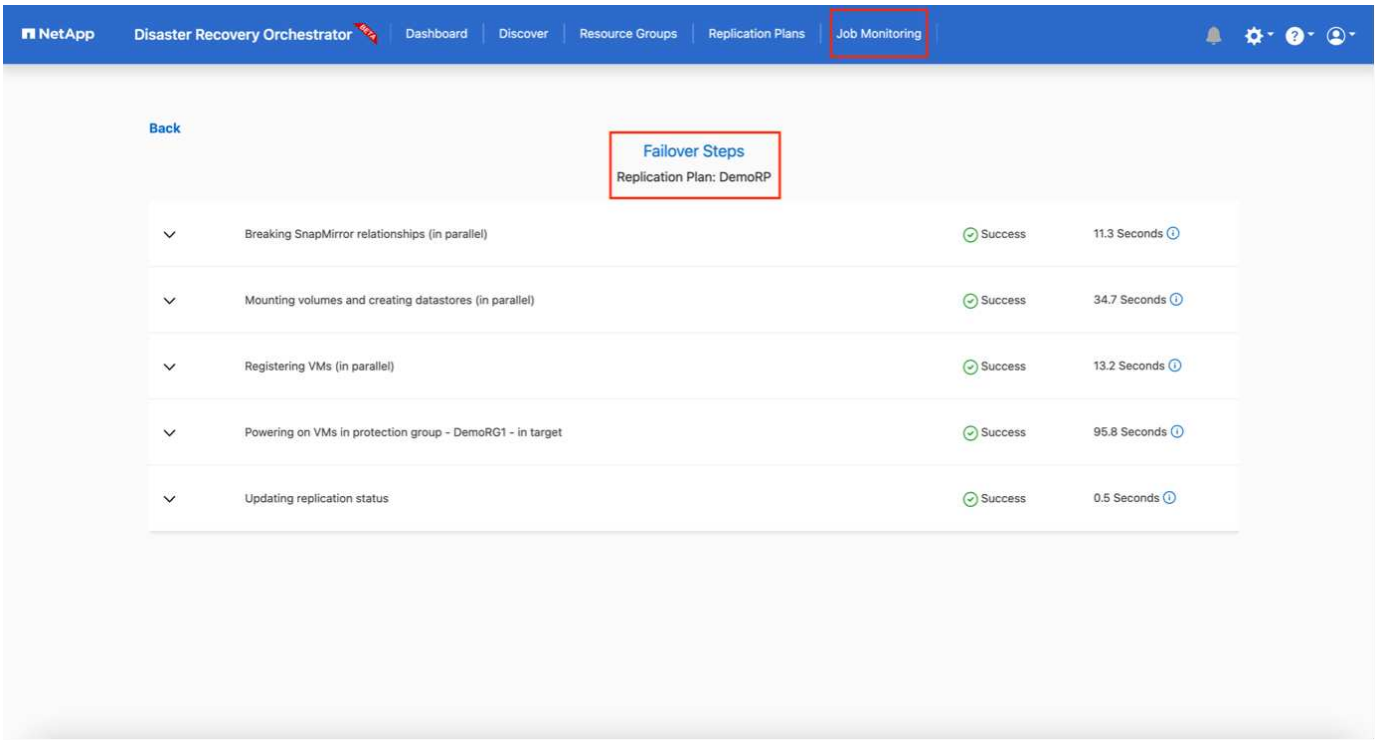


Une fois le plan de réplication créé, l'option de basculement, l'option test-failover ou l'option de migration peuvent être exercées en fonction des exigences. Lors des options de basculement et de test/basculement, la copie Snapshot la plus récente est utilisée ou une copie Snapshot spécifique peut être sélectionnée à partir d'une copie Snapshot instantanée (conformément à la règle de conservation de SnapMirror). L'option instantanée peut être utile si vous êtes confronté à un événement de corruption comme les ransomwares, où les répliques les plus récentes sont déjà compromises ou chiffrées. DRO affiche tous les points disponibles dans le temps. Pour déclencher un basculement ou un basculement de test avec la configuration spécifiée dans le plan de réplication, vous pouvez cliquer sur **basculement** ou **Test basculement**.

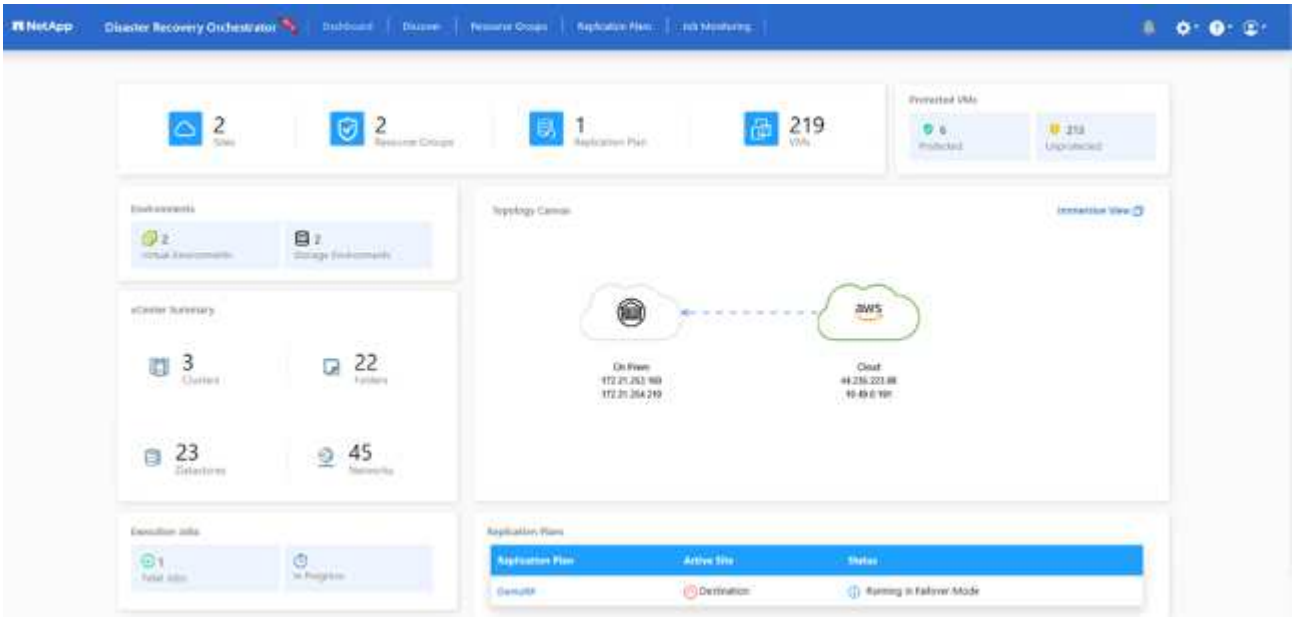




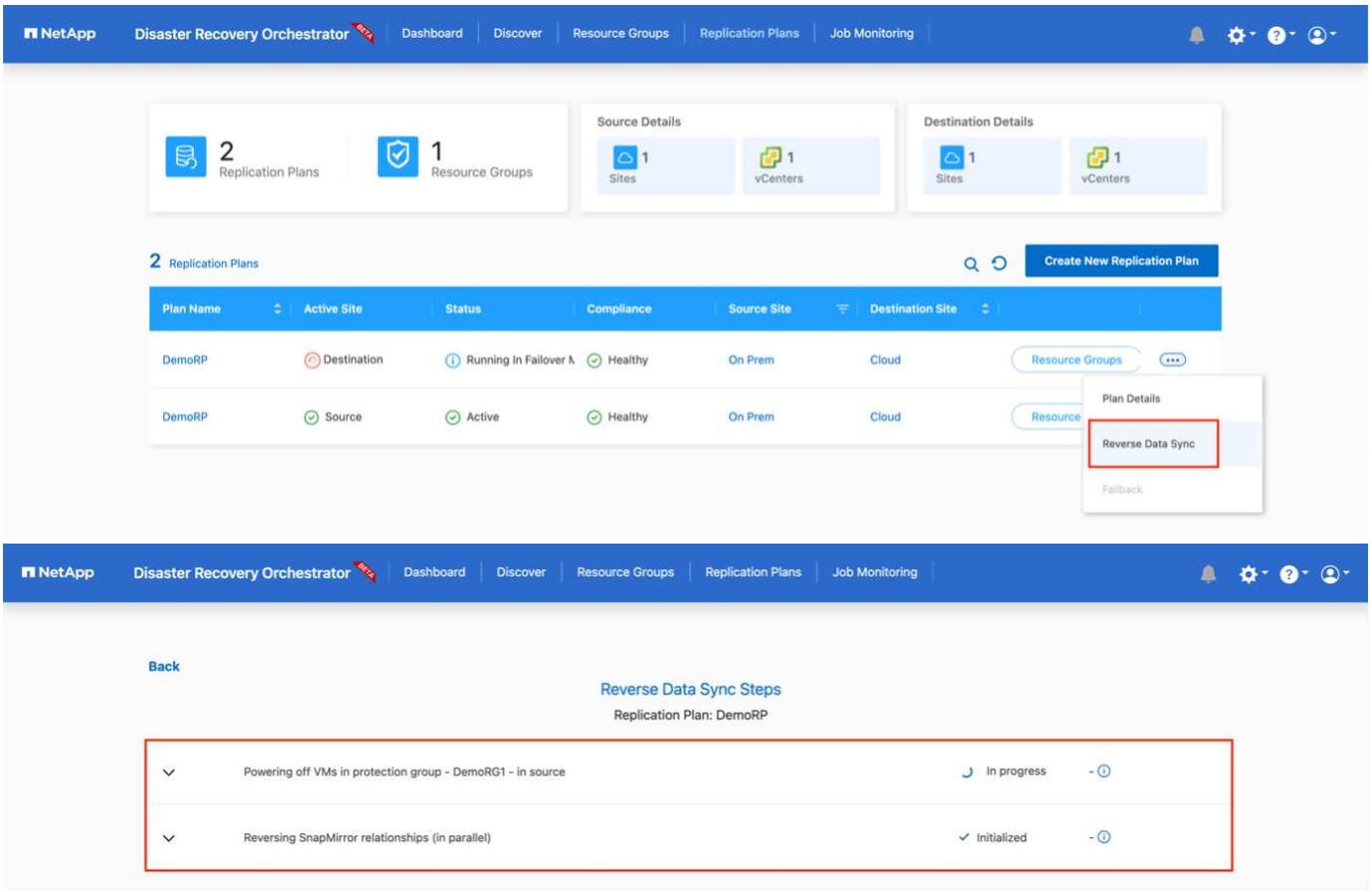
Le plan de réplication peut être surveillé dans le menu des tâches :



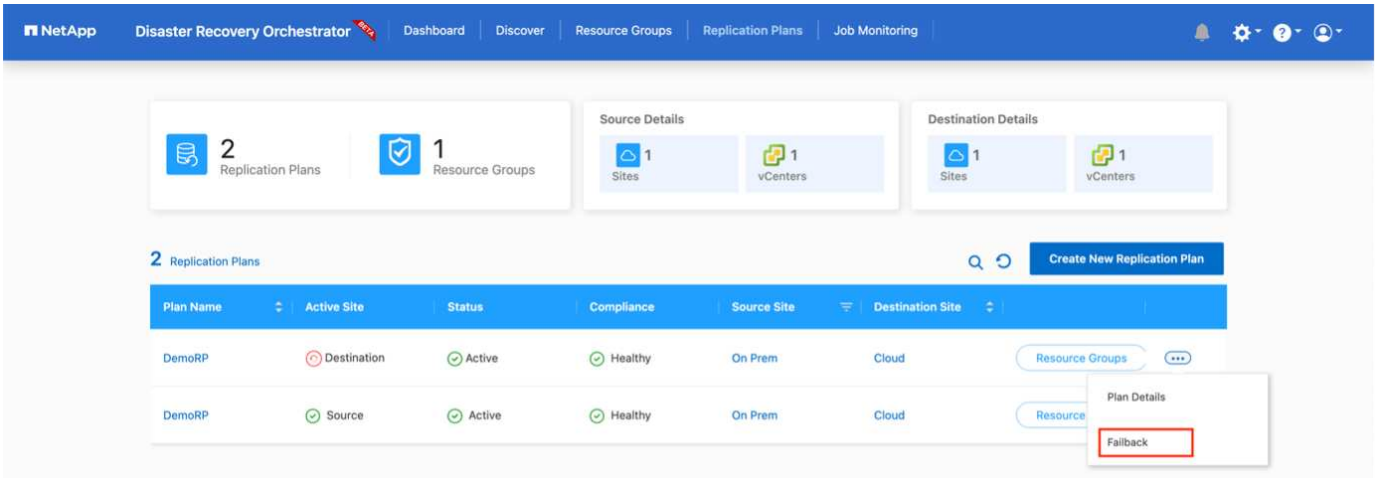
Après le déclenchement du basculement, les éléments restaurés sont visibles dans le vCenter du VMC (machines virtuelles, réseaux, datastores). Par défaut, les machines virtuelles sont restaurées dans le dossier Workload.

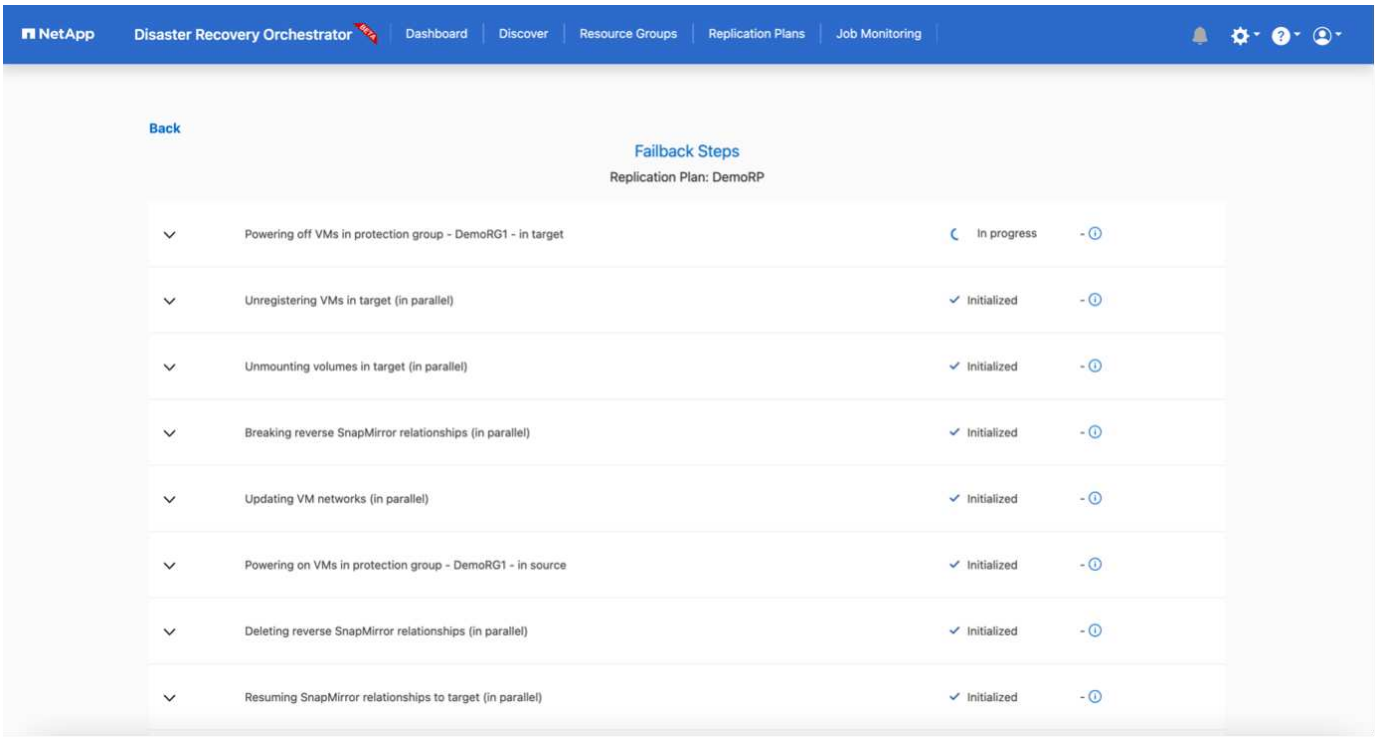


Le retour arrière peut être déclenché au niveau du plan de réplication. Dans le cas d'un basculement test, l'option redescendre peut être utilisée pour annuler les modifications et supprimer la relation FlexClone. La restauration liée au basculement est un processus en deux étapes. Sélectionnez le plan de réplication et sélectionnez **Inverser la synchronisation des données**.

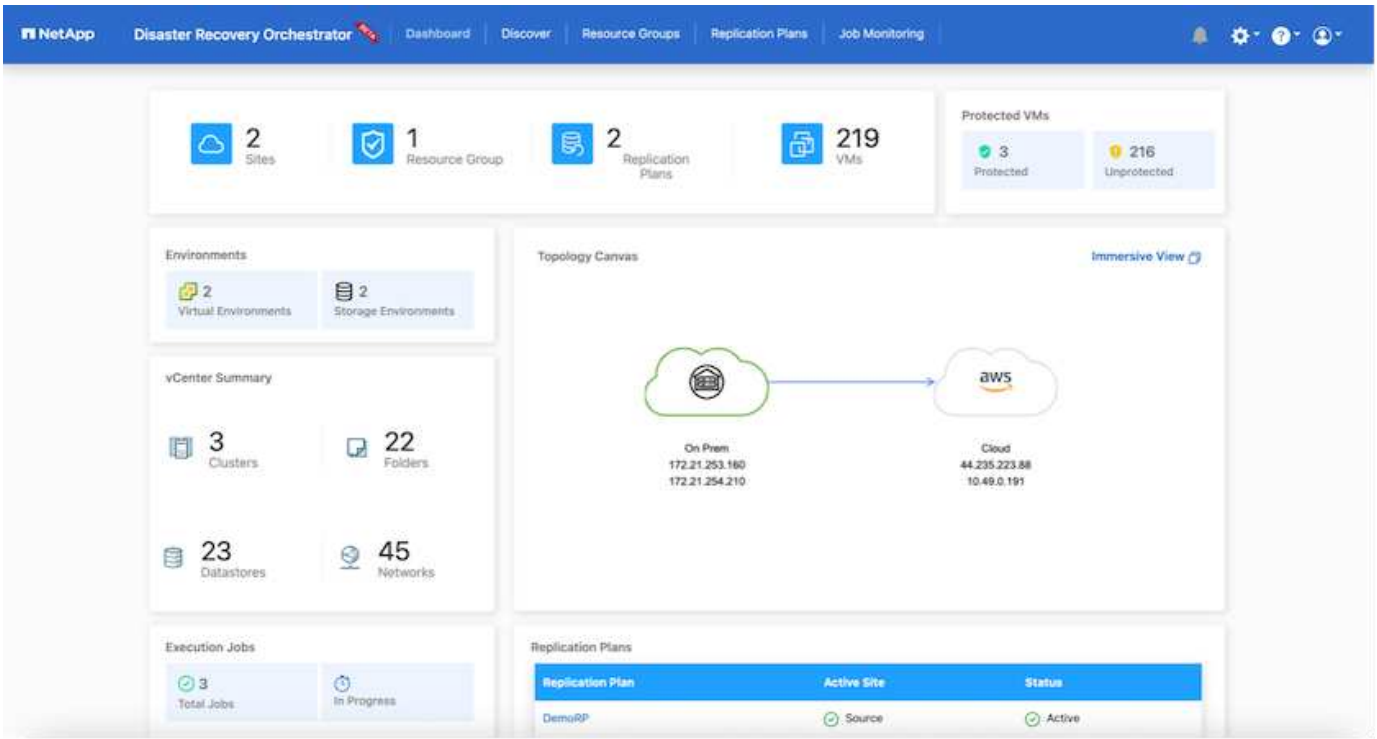


Une fois cette opération terminée, vous pouvez déclencher un retour arrière pour revenir au site de production d'origine.





De NetApp BlueXP, nous pouvons constater que la réplication est défaillante pour les volumes appropriés (ceux qui ont été mappés à VMC comme volumes en lecture-écriture). Pendant le basculement de test, DRO ne mappe pas le volume de destination ou de réplica. Il effectue plutôt une copie FlexClone de l'instance SnapMirror (ou Snapshot) requise et expose l'instance FlexClone, qui ne consomme pas de capacité physique supplémentaire pour FSX pour ONTAP. Ce processus permet de s'assurer que le volume n'est pas modifié et que les tâches de réplication peuvent se poursuivre même pendant les tests de reprise d'activité ou les workflows de triage. En outre, ce processus garantit que, si des erreurs se produisent ou si des données corrompues sont récupérées, la récupération peut être nettoyée sans le risque de destruction de la réplique.



Restauration par ransomware

Récupérer des données suite à un ransomware peut être une tâche extrêmement fastidieuse. En particulier, il peut être difficile pour les services INFORMATIQUES d'identifier le point de retour sécurisé et, une fois déterminé, de protéger les charges de travail récupérées contre les attaques de réexécution, par exemple, des programmes malveillants en sommeil ou des applications vulnérables.

DRO résout ces problèmes en vous permettant de récupérer votre système à partir de n'importe quel point disponible dans le temps. Vous pouvez également restaurer les charges de travail sur des réseaux fonctionnels mais isolés pour que les applications puissent fonctionner et communiquer entre elles à un endroit où elles ne sont pas exposées au trafic du nord du sud. Votre équipe de sécurité dispose ainsi d'un endroit sûr pour mener des analyses et s'assurer qu'il n'y a aucun programme malveillant caché ou en veille.

Avantages

- Utilisation de la réplication SnapMirror efficace et résiliente.
- Restauration à tout point dans le temps avec la conservation des copies Snapshot
- Automatisation complète de toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles à partir des étapes de validation du stockage, du calcul, du réseau et des applications.
- Restauration de charge de travail avec la technologie ONTAP FlexClone utilisant une méthode qui ne modifie pas le volume répliqué.
  - Évite le risque de corruption des données pour les volumes et les copies Snapshot.
  - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Utilisation potentielle des données de reprise d'activité avec des ressources de cloud computing pour les workflows hors reprise d'activité, comme DevTest, les tests de sécurité, les tests de correctifs ou de mise à niveau, et les tests de résolution de problèmes.
- L'optimisation du processeur et de la RAM pour réduire les coûts liés au cloud grâce à la restauration sur des clusters de calcul plus petits.

Utilisation de Veeam Replication et FSX for ONTAP pour la reprise d'activité vers VMware Cloud on AWS

L'intégration d'Amazon FSX for NetApp ONTAP à VMware Cloud on AWS est un datastore NFS externe géré par AWS basé sur le système de fichiers ONTAP de NetApp qui peut être relié à un cluster dans le SDDC. Elle fournit aux clients une infrastructure de stockage virtualisée flexible et haute performance qui peut évoluer indépendamment des ressources de calcul.

Auteur: Niyaz Mohamed - NetApp Solutions Engineering

Présentation

Pour les clients qui cherchent à utiliser VMware Cloud sur AWS SDDC comme cible de reprise d'activité, les datastores FSX pour ONTAP peuvent être utilisés pour répliquer les données depuis un environnement sur site à l'aide d'une solution tierce validée offrant des fonctionnalités de réplication de machines virtuelles. En ajoutant le datastore FSX for ONTAP, il permet un déploiement optimisé par les coûts que la création du cloud VMware sur un SDDC AWS avec un énorme nombre d'hôtes ESXi uniquement pour prendre en charge le stockage.

Cette approche aide également les clients à utiliser un cluster pilote dans VMC avec FSX pour les datastores

ONTAP pour héberger les répliques de machine virtuelle. Le même processus peut également être étendu en tant qu'option de migration vers VMware Cloud sur AWS en basculant avec fluidité le plan de réplication.

Énoncé du problème

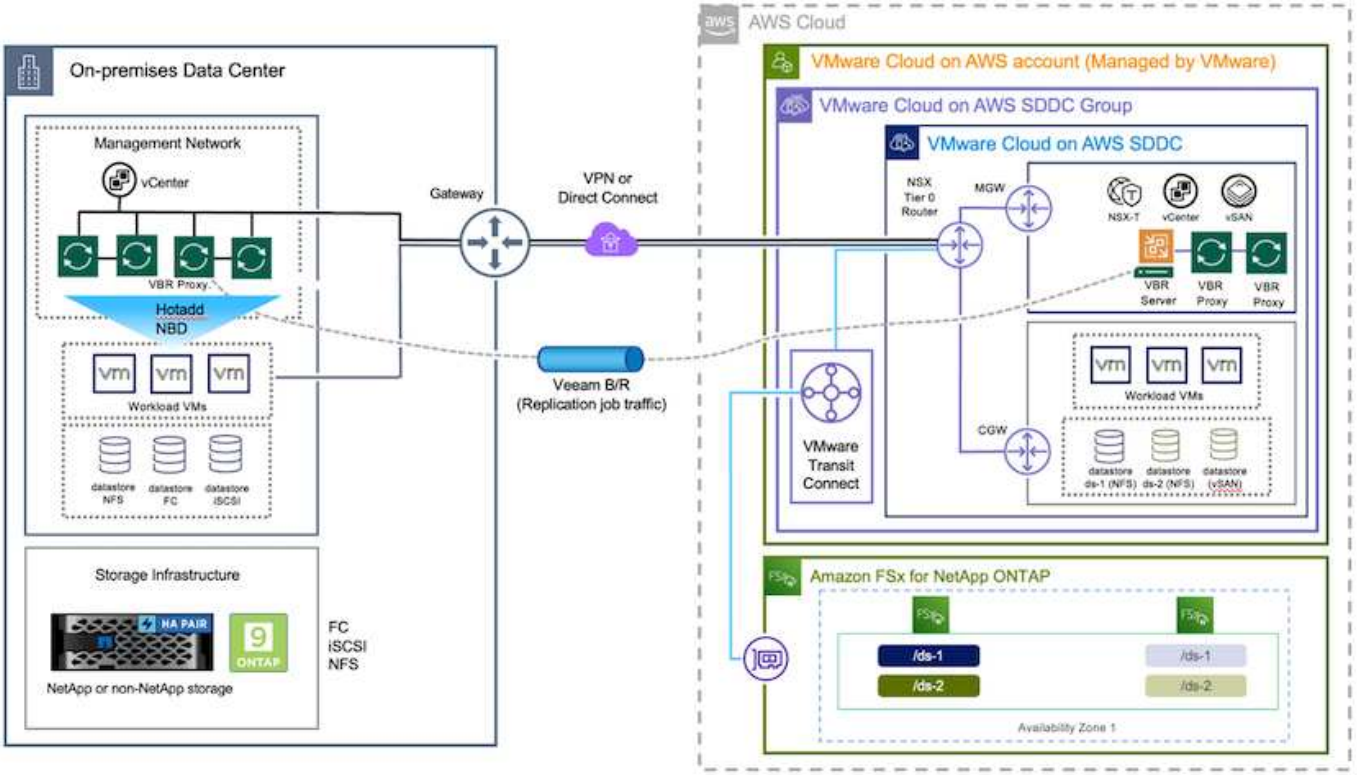
Ce document décrit comment utiliser le datastore FSX pour ONTAP et Veeam Backup and Replication pour configurer la reprise d'activité pour les machines virtuelles VMware sur site vers VMware Cloud on AWS à l'aide de la fonctionnalité de réplication de machine virtuelle.

Veeam Backup & Replication permet la réplication sur site et à distance pour la reprise après incident. Lors de la réplication des machines virtuelles, Veeam Backup & Replication crée une copie exacte des machines virtuelles au format VMware vSphere natif sur le cluster SDDC cible VMware Cloud on AWS et synchronise la copie avec la machine virtuelle d'origine.

La réplication offre les meilleures valeurs d'objectif de délai de restauration (RTO), car une copie d'une machine virtuelle est prête à démarrer. Ce mécanisme de réplication permet de s'assurer que les workloads peuvent démarrer rapidement dans VMware Cloud sur AWS SDDC en cas d'incident. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. De plus, il filtre les blocs de données dupliqués, les blocs de données nuls, les fichiers swap et les fichiers du système d'exploitation invité des machines virtuelles exclus, et compresse le trafic des répliques.

Pour empêcher les tâches de réplication de consommer la totalité de la bande passante réseau, des accélérateurs WAN et des règles de restriction réseau peuvent être mis en place. Dans Veeam Backup & Replication, le processus de réplication est piloté par des tâches, ce qui signifie que la réplication est effectuée via la configuration des tâches de réplication. En cas d'incident, le basculement peut être déclenché pour restaurer les machines virtuelles en basculant vers la copie de réplica.

Lors d'un basculement, une machine virtuelle répliquée prend le rôle de la machine virtuelle d'origine. Le basculement peut être effectué vers l'état le plus récent d'une réplique ou vers l'un de ses points de restauration connus. La restauration est ainsi possible en cas d'attaque par ransomware ou de tests isolés les cas échéant. Dans Veeam Backup & Replication, le basculement et la restauration sont des étapes intermédiaires temporaires qui doivent être finalisées davantage. Veeam Backup & Replication propose plusieurs options pour gérer différents scénarios de reprise d'activité.



Déploiement de la solution

Marches de haut niveau

1. Le logiciel Veeam Backup and Replication s'exécute dans un environnement sur site avec une connectivité réseau appropriée.
2. Configurez VMware Cloud on AWS, consultez l'article VMware Cloud Tech zone "Guide de déploiement de l'intégration de VMware Cloud on AWS avec Amazon FSX for NetApp ONTAP" Pour le déploiement, configurez VMware Cloud sur AWS SDDC et FSX pour ONTAP en tant que datastore NFS. (Un environnement de pilote léger configuré avec une configuration minimale peut être utilisé à des fins de reprise sur incident. Les machines virtuelles basculeront vers ce cluster en cas d'incident et d'autres nœuds pourront être ajoutés.)
3. Configuration des tâches de réplication pour créer des répliques de machine virtuelle à l'aide de Veeam Backup and Replication
4. Création d'un plan de basculement et basculement
5. Revenez aux machines virtuelles de production une fois l'incident terminé et le site principal en marche.

Pré-requis pour la réplication de VM Veeam vers VMC et FSX pour les datastores ONTAP

1. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée au vCenter source et au cloud VMware cible sur les clusters SDDC AWS.
2. Le serveur de sauvegarde doit pouvoir résoudre les noms abrégés et se connecter aux vCenters source et cible.
3. Le datastore FSX pour ONTAP cible doit disposer de suffisamment d'espace libre pour stocker des VMDK de machines virtuelles répliquées

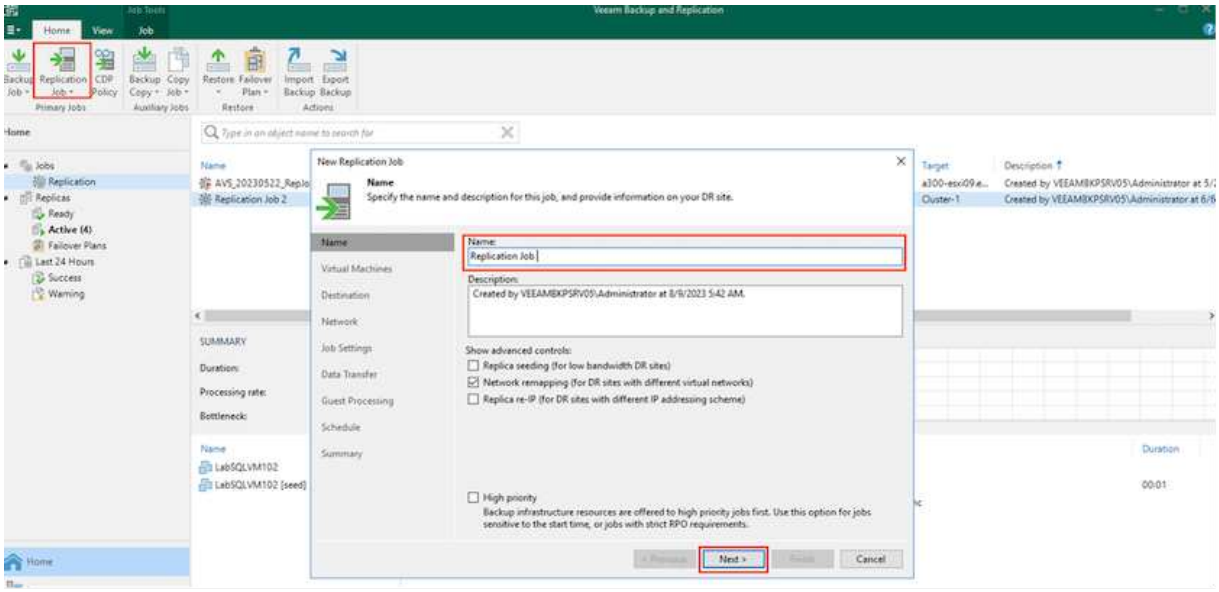
Pour plus d'informations, reportez-vous à la section « considérations et limitations » "ici".

Étape 1 : réplication des machines virtuelles

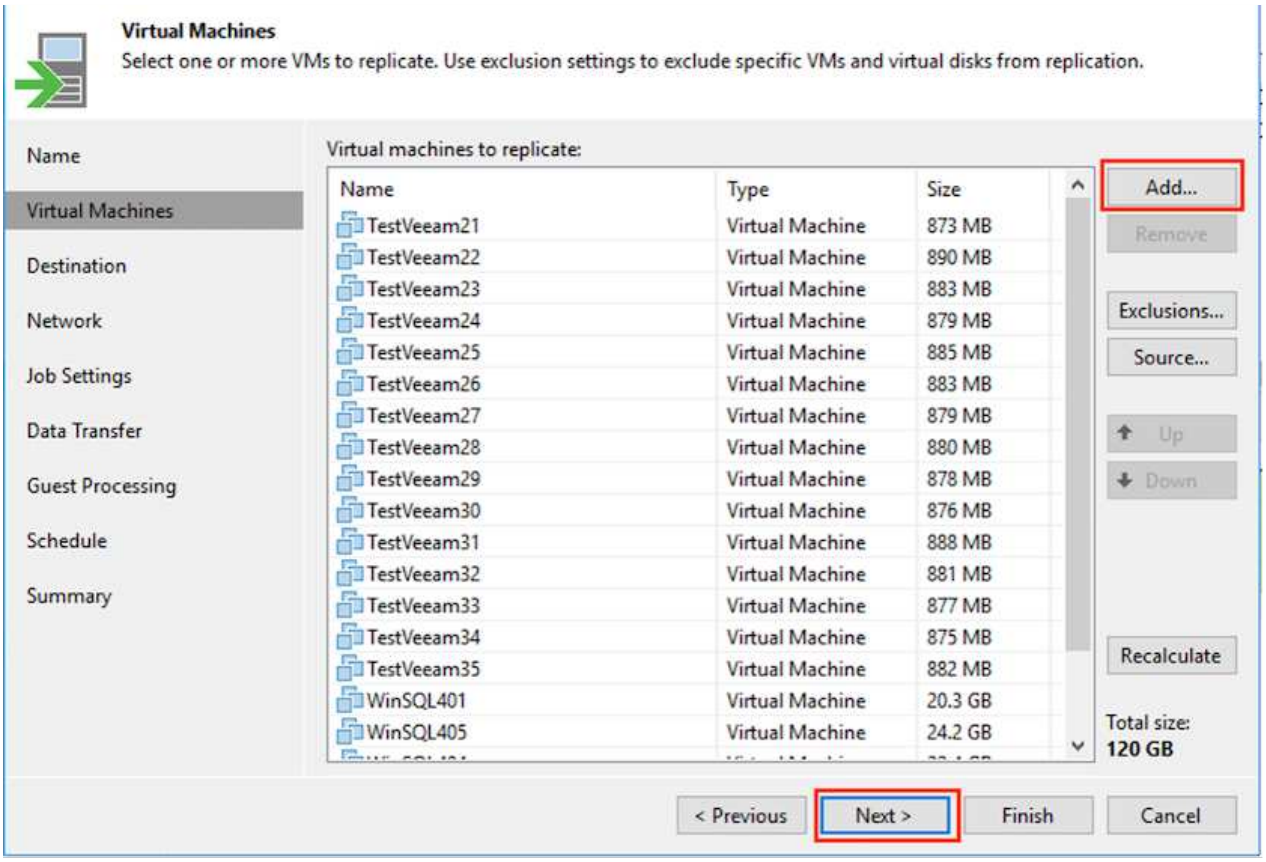
Veeam Backup & Replication exploite les fonctionnalités Snapshot de VMware vSphere et, pendant la réplication, Veeam Backup & Replication demande à VMware vSphere de créer un Snapshot de machine virtuelle. Le snapshot de machine virtuelle est la copie instantanée d'une machine virtuelle, qui comprend des disques virtuels, l'état du système, la configuration, etc. Veeam Backup & Replication utilise le snapshot comme source de données pour la réplication.

Pour répliquer des machines virtuelles, procédez comme suit :

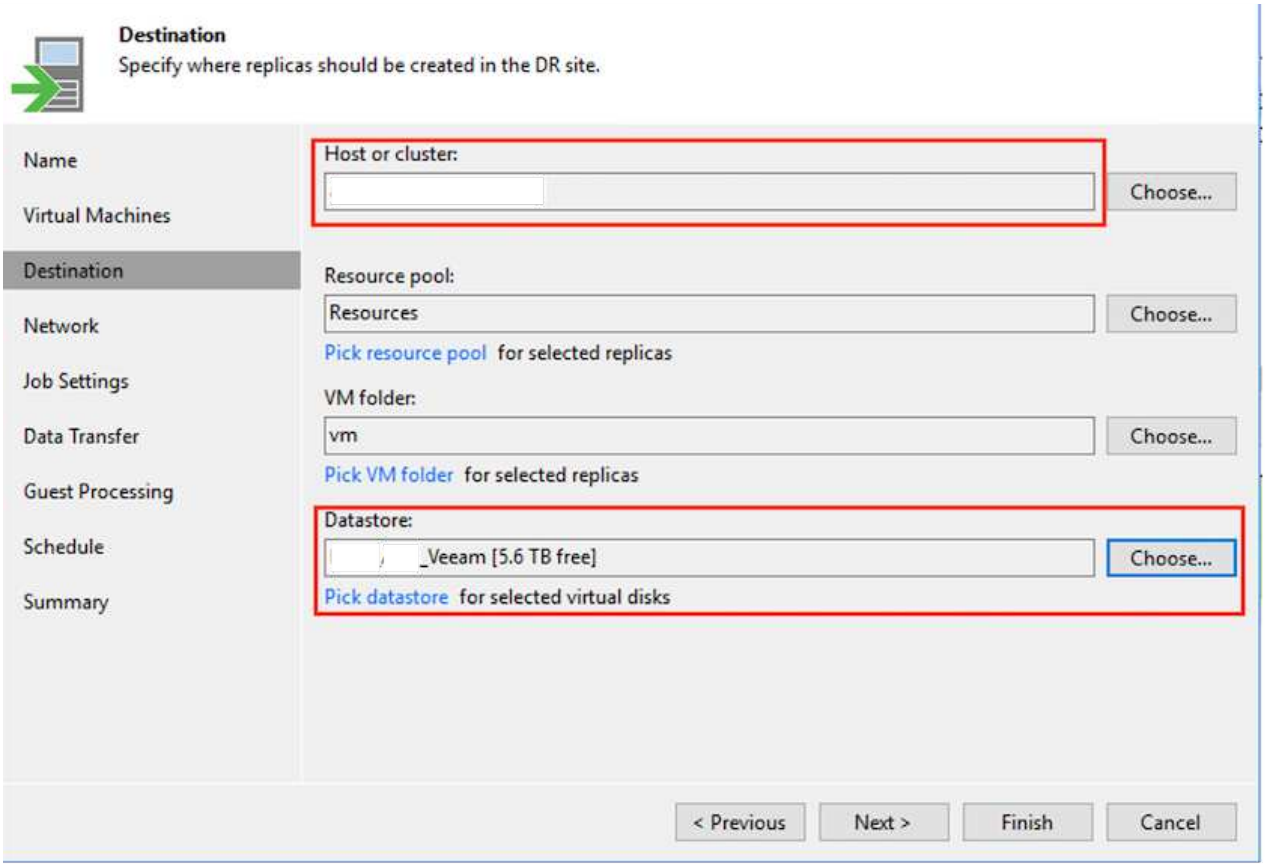
1. Ouvrez Veeam Backup & Replication Console.
2. Dans la vue d'accueil, sélectionnez Replication Job > Virtual machine > VMware vSphere.
3. Spécifiez un nom de travail et cochez la case de contrôle avancé appropriée. Cliquez sur Suivant.
   - Cochez la case amorçage du réplica si la connectivité entre le site et AWS a une bande passante limitée.
   - Cochez la case Remapping réseau (pour les sites VMC AWS avec différents réseaux) si les segments du SDDC VMware Cloud on AWS ne correspondent pas à ceux des réseaux sur site.
   - Si le schéma d'adressage IP du site de production sur site diffère du schéma du site VMC AWS, cochez la case Replica re-IP (pour les sites DR avec un schéma d'adressage IP différent).



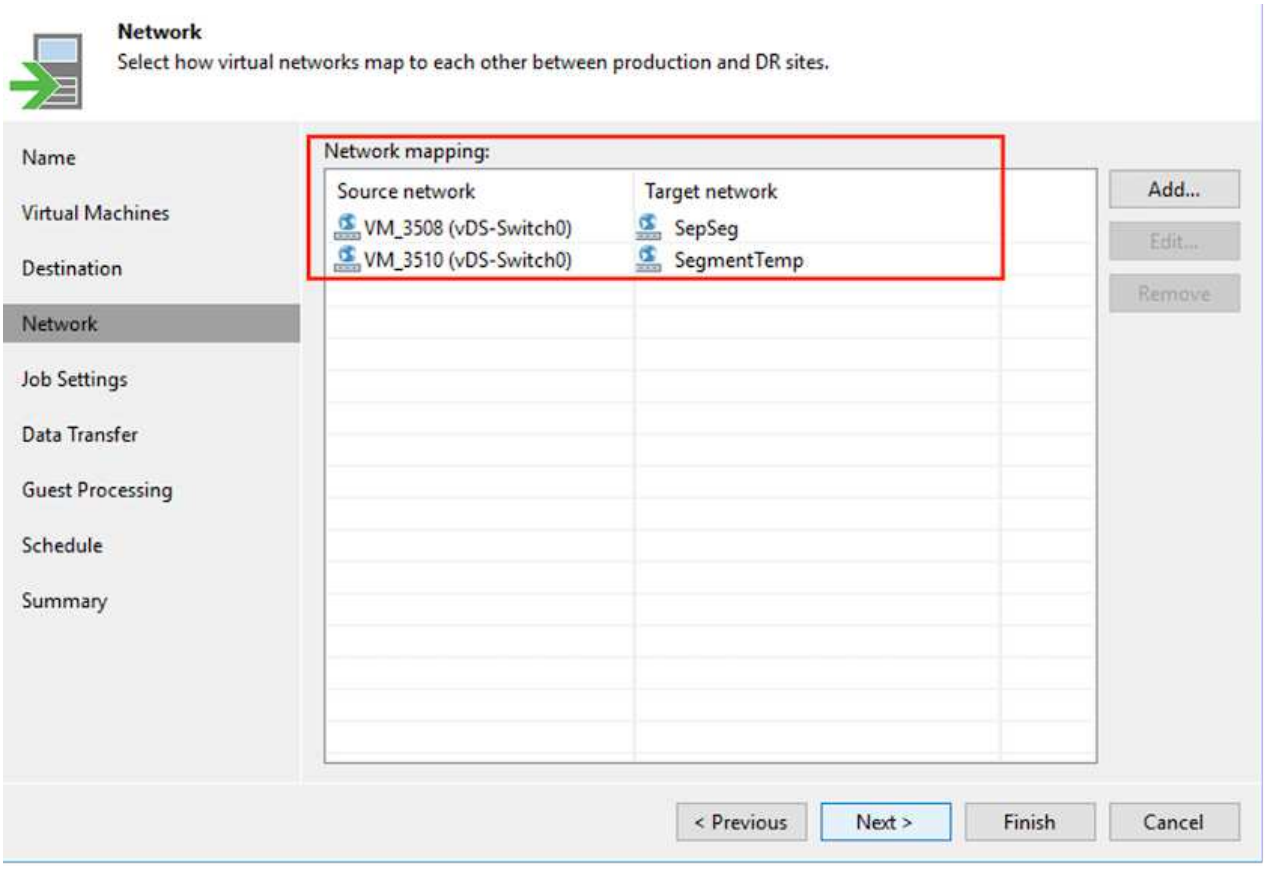
4. Sélectionnez les machines virtuelles qui doivent être répliquées vers le datastore FSX for ONTAP connecté au SDDC VMware Cloud on AWS à l'étape **machines virtuelles**. Les machines virtuelles peuvent être placées sur VSAN pour remplir la capacité de datastore VSAN disponible. Dans un cluster à voyants, la capacité utilisable d'un cluster à 3 nœuds sera limitée. Le reste des données peut être répliqué dans des datastores FSX for ONTAP. Cliquez sur **Ajouter**, puis dans la fenêtre **Ajouter un objet**, sélectionnez les machines virtuelles ou les conteneurs VM nécessaires et cliquez sur **Ajouter**. Cliquez sur **Suivant**.



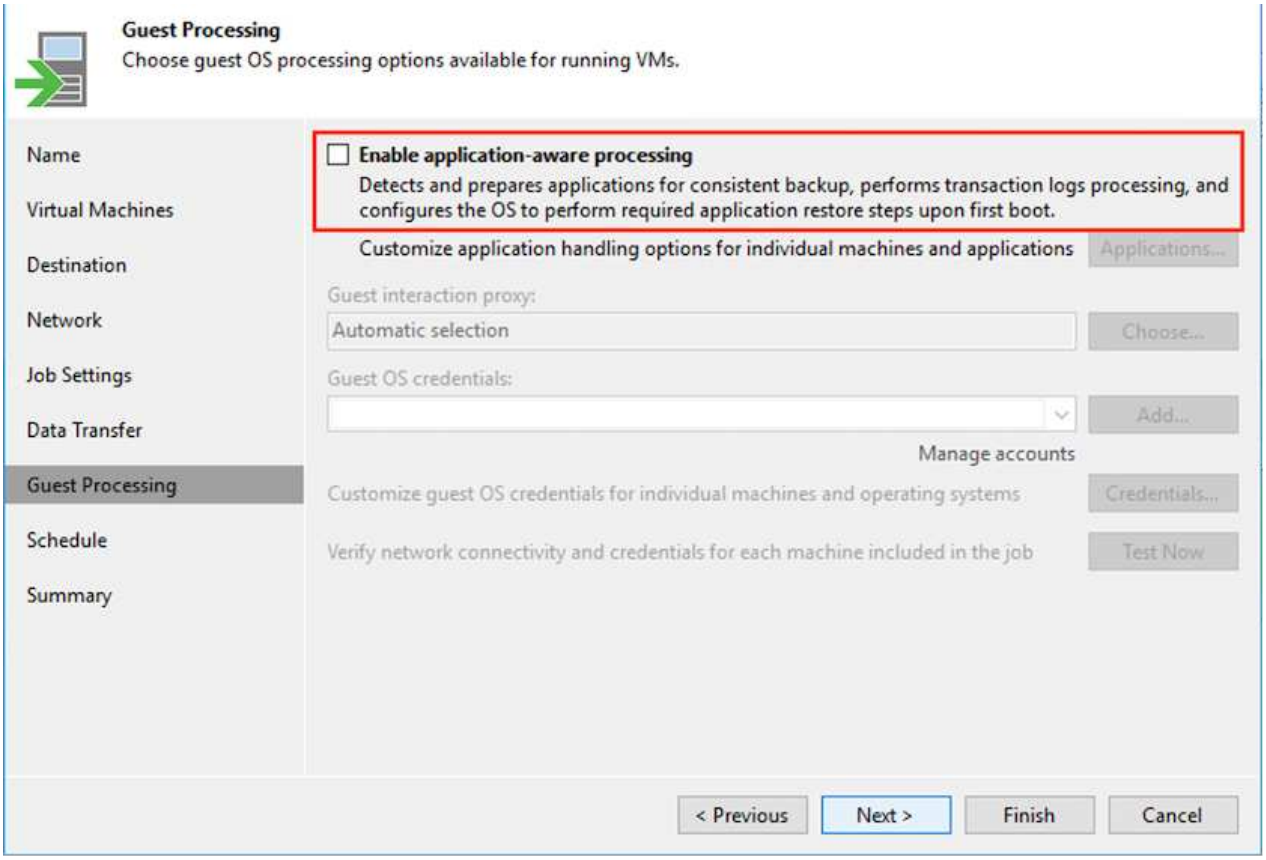
5. Ensuite, sélectionnez la destination en tant que cluster/hôte SDDC pour VMware Cloud sur AWS et le pool de ressources, le dossier VM et le datastore FSX pour ONTAP pour les répliques de VM. Cliquez ensuite sur **Suivant**.



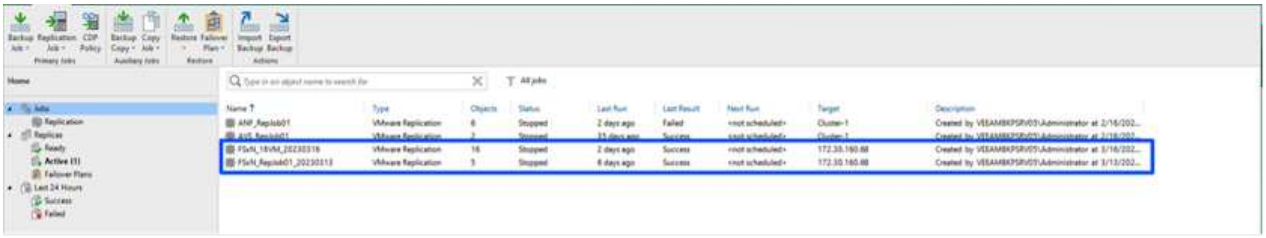
6. Dans l'étape suivante, créez le mappage entre le réseau virtuel source et le réseau virtuel de destination, selon vos besoins.



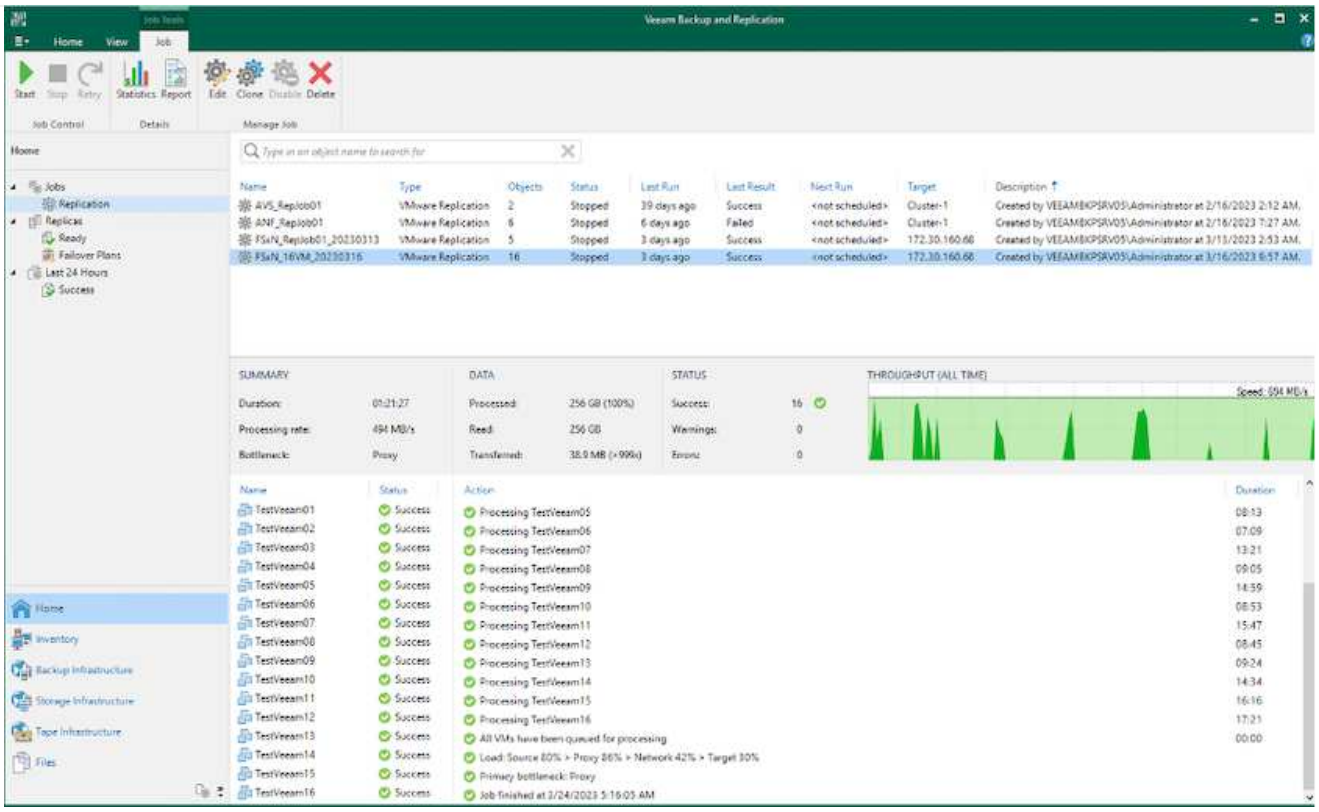
7. À l'étape **Job Settings**, spécifiez le référentiel de sauvegarde qui stocke les métadonnées pour les répliques de VM, la stratégie de rétention, etc.
8. Mettez à jour les serveurs proxy **Source** et **cible** à l'étape **transfert de données** et laissez la sélection **automatique** (par défaut) et conservez l'option **Direct** sélectionnée, puis cliquez sur **Suivant**.
9. À l'étape **Guest Processing**, sélectionnez l'option **Activer le traitement compatible avec les applications** selon les besoins. Cliquez sur **Suivant**.



10. Choisissez la planification de réplication pour exécuter la procédure de réplication à exécuter régulièrement.
11. À l'étape **Résumé** de l'assistant, passez en revue les détails de la procédure de réplication. Pour démarrer le travail juste après la fermeture de l'assistant, cochez la case **Exécuter le travail lorsque je clique sur Terminer**, sinon ne cochez pas la case. Cliquez ensuite sur **Terminer** pour fermer l'assistant.



Une fois la procédure de réplication lancée, les machines virtuelles dont le suffixe est spécifié sont renseignées sur le cluster/l'hôte VMC SDDC de destination.



Pour plus d'informations sur la réplication Veeam, reportez-vous à la section "Fonctionnement de la réplication".

Étape 2 : création d'un plan de basculement

Lorsque la réplication ou l'amorçage initial est terminé, créez le plan de basculement. Le plan de basculement permet d'effectuer automatiquement le basculement des machines virtuelles dépendantes une par une ou en tant que groupe. La planification de basculement est la référence pour l'ordre dans lequel les machines virtuelles sont traitées, y compris les retards de démarrage. Le plan de basculement permet également de s'assurer que les machines virtuelles dépendantes critiques sont déjà en cours d'exécution.

Pour créer le plan, accédez à la nouvelle sous-section intitulée répliques et sélectionnez Plan de basculement. Choisissez les machines virtuelles appropriées. Veeam Backup & Replication recherche les points de restauration les plus proches à ce point dans le temps et les utilise pour démarrer les répliques de machine virtuelle.

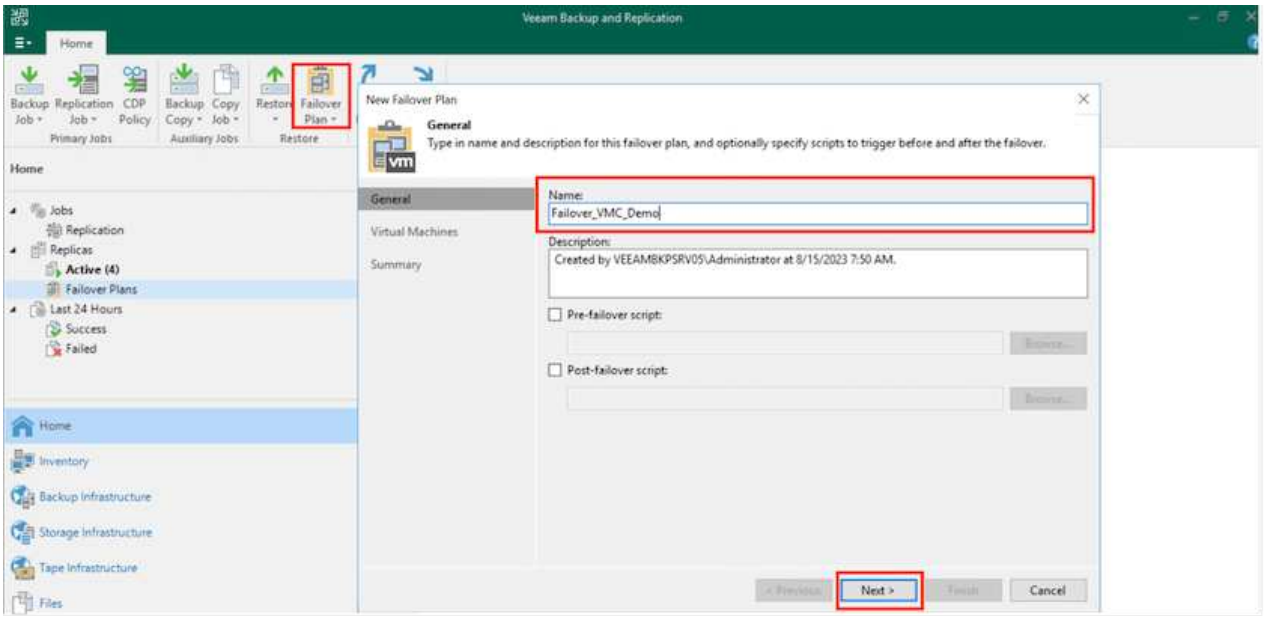
ⓘ Le plan de basculement ne peut être ajouté qu'une fois la réplication initiale terminée et les répliques de machine virtuelle à l'état prêt.

ⓘ Le nombre maximum de machines virtuelles pouvant être démarrées simultanément lors de l'exécution d'un plan de basculement est de 10.

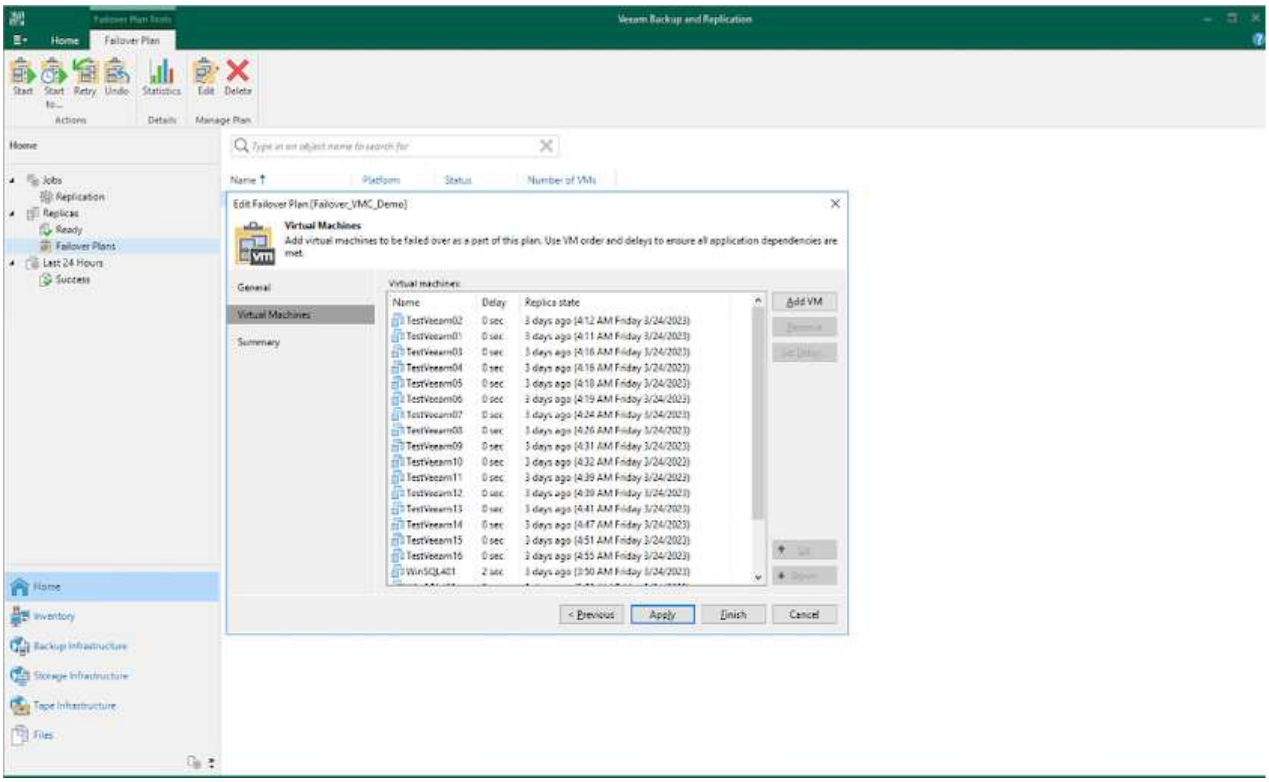
ⓘ Pendant le processus de basculement, les machines virtuelles source ne sont pas hors tension.

Pour créer le **Plan de basculement**, procédez comme suit :

1. Dans la vue Accueil, sélectionnez **Plan de basculement > VMware vSphere**.
2. Ensuite, donnez un nom et une description au plan. Des scripts de pré-basculement et de post-basculement peuvent être ajoutés si nécessaire. Par exemple, exécutez un script pour arrêter les machines virtuelles avant de démarrer les machines virtuelles répliquées.



3. Ajoutez les machines virtuelles au plan et modifiez l'ordre de démarrage de la machine virtuelle et les délais de démarrage afin de répondre aux dépendances des applications.



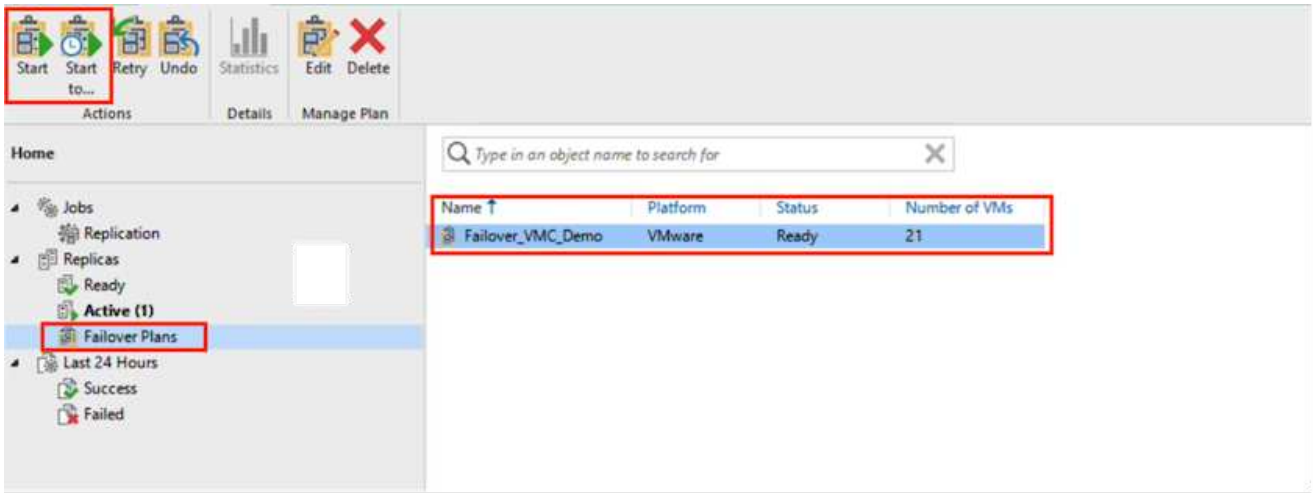
Pour plus d’informations sur la création de tâches de réplication, reportez-vous à la section "Création de travaux de réplication".

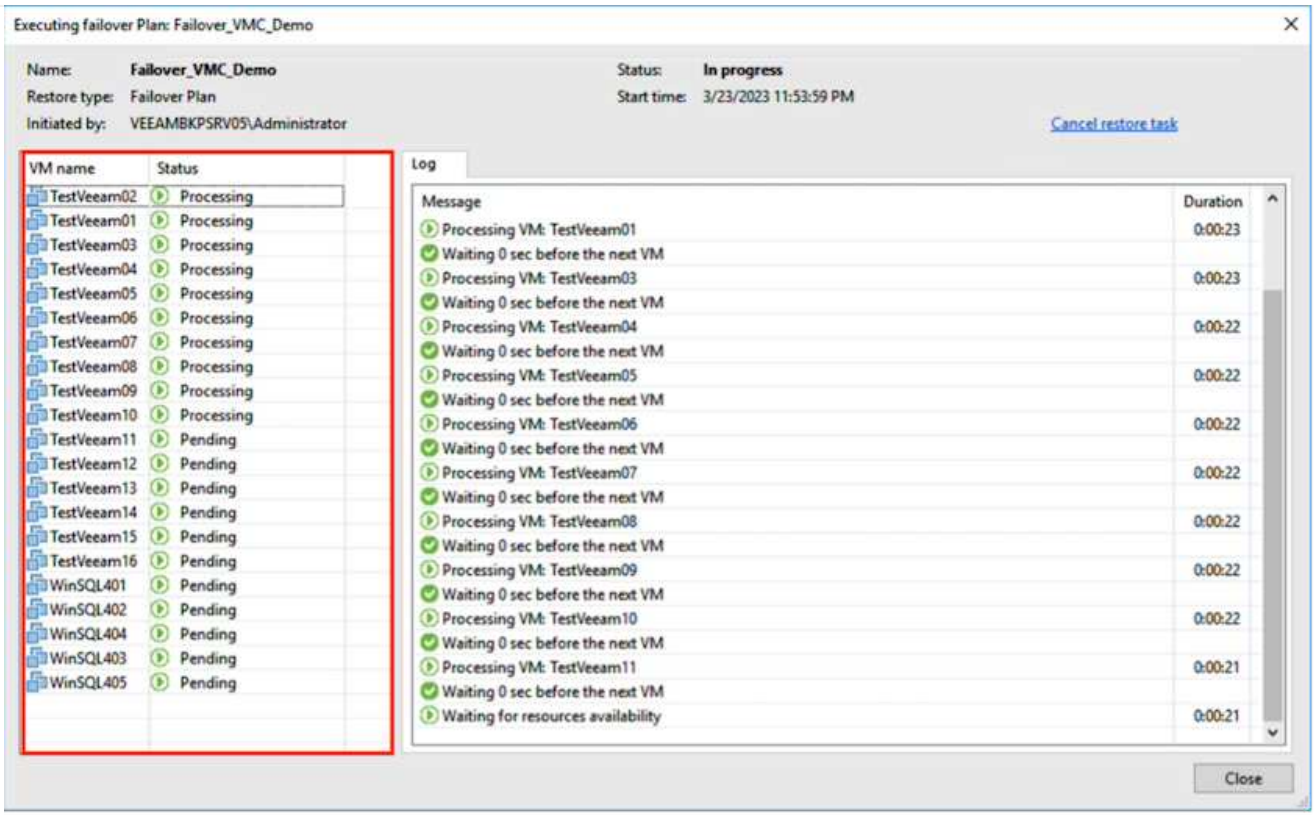
Étape 3 : exécutez le plan de basculement

Lors du basculement, la machine virtuelle source du site de production est basculée vers sa réplique sur le site de reprise après incident. Dans le cadre du processus de basculement, Veeam Backup & Replication restaure le réplica de la machine virtuelle vers le point de restauration requis et déplace toutes les activités d'E/S de la machine virtuelle source vers son réplica. Les répliques peuvent être utilisées non seulement en cas d'incident, mais aussi pour simuler des exercices de DR. Pendant la simulation de basculement, la machine virtuelle source reste en cours d'exécution. Une fois tous les tests nécessaires effectués, vous pouvez annuler le basculement et revenir aux opérations normales.

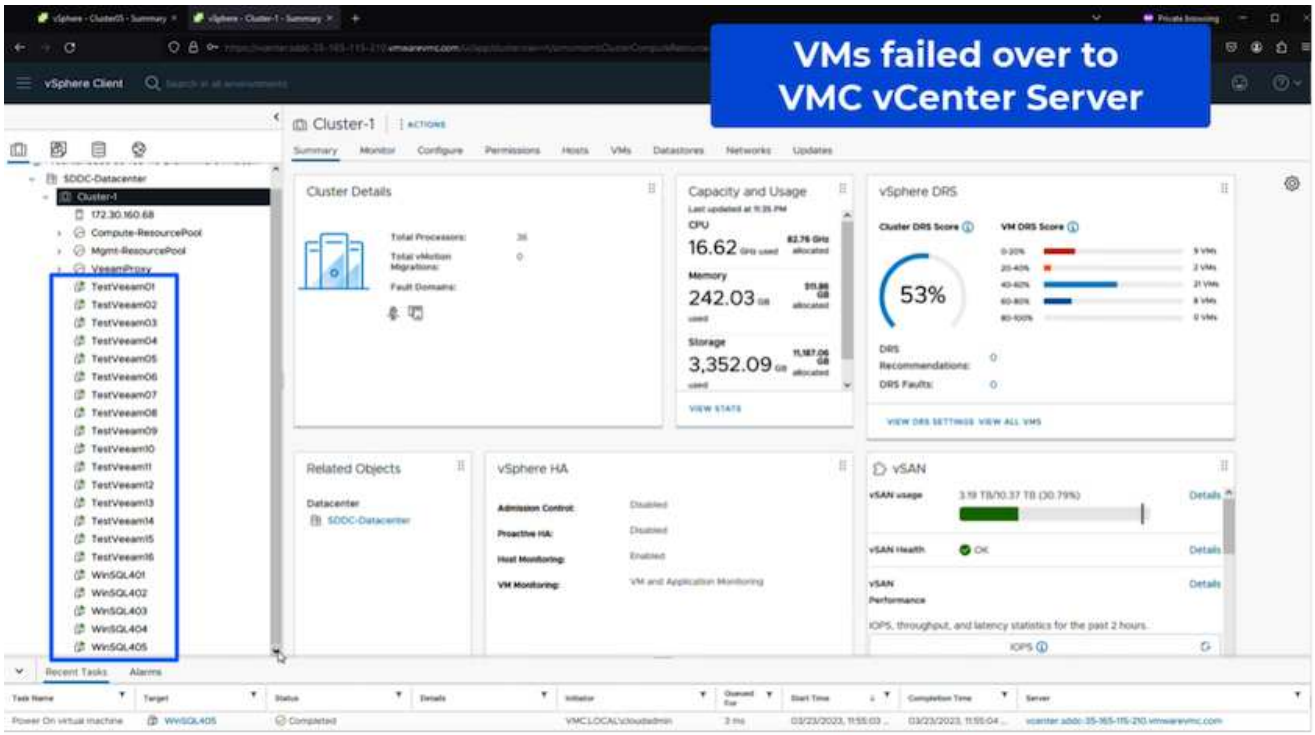
Assurez-vous que la segmentation réseau est en place pour éviter les conflits d'adresses IP pendant les tests de DR.

Pour démarrer le plan de basculement, cliquez simplement sur l'onglet **plans de basculement** et cliquez avec le bouton droit de la souris sur le plan de basculement. Sélectionnez **Démarrer**. Cette opération basculera en utilisant les derniers points de restauration des répliques de machine virtuelle. Pour basculer vers des points de restauration spécifiques de répliques de machines virtuelles, sélectionnez **Démarrer à**.

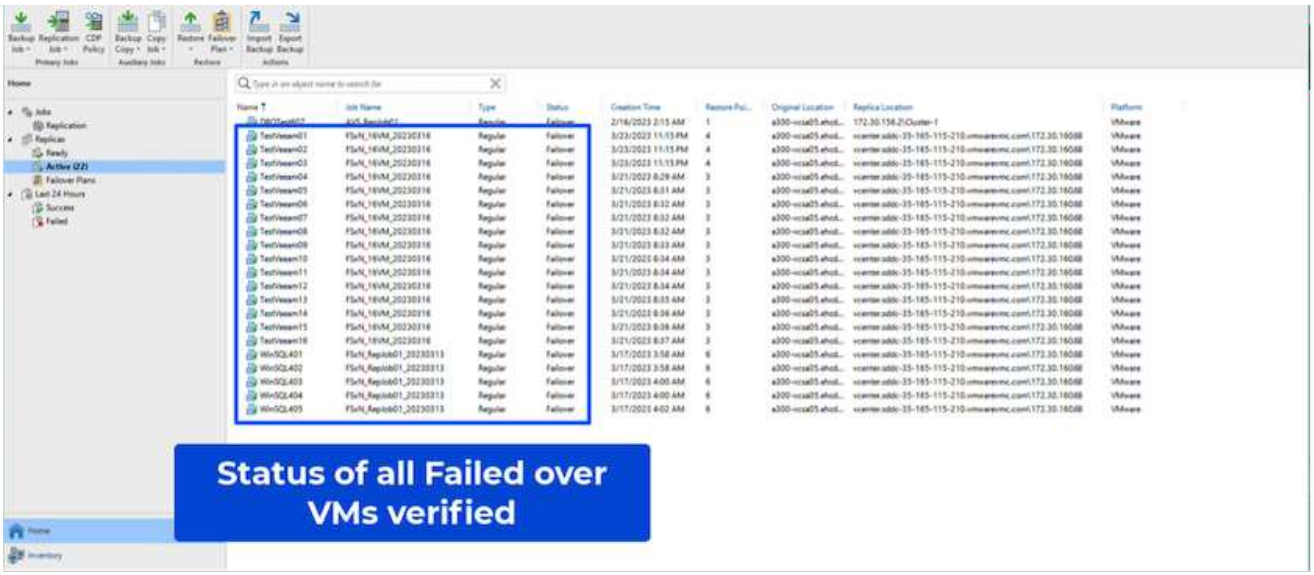




L'état du réplica de la machine virtuelle passe de Ready à Failover et les machines virtuelles démarrent sur le cluster/hôte SDDC AWS de destination VMware Cloud.



Une fois le basculement terminé, l'état des machines virtuelles passe à « basculement ».



Veeam Backup & Replication arrête toutes les activités de réplication de la machine virtuelle source jusqu'à ce que son réplica revienne à l'état prêt.

Pour plus d'informations sur les plans de basculement, reportez-vous à la section "Plans de basculement".

Étape 4 : retour arrière vers le site de production

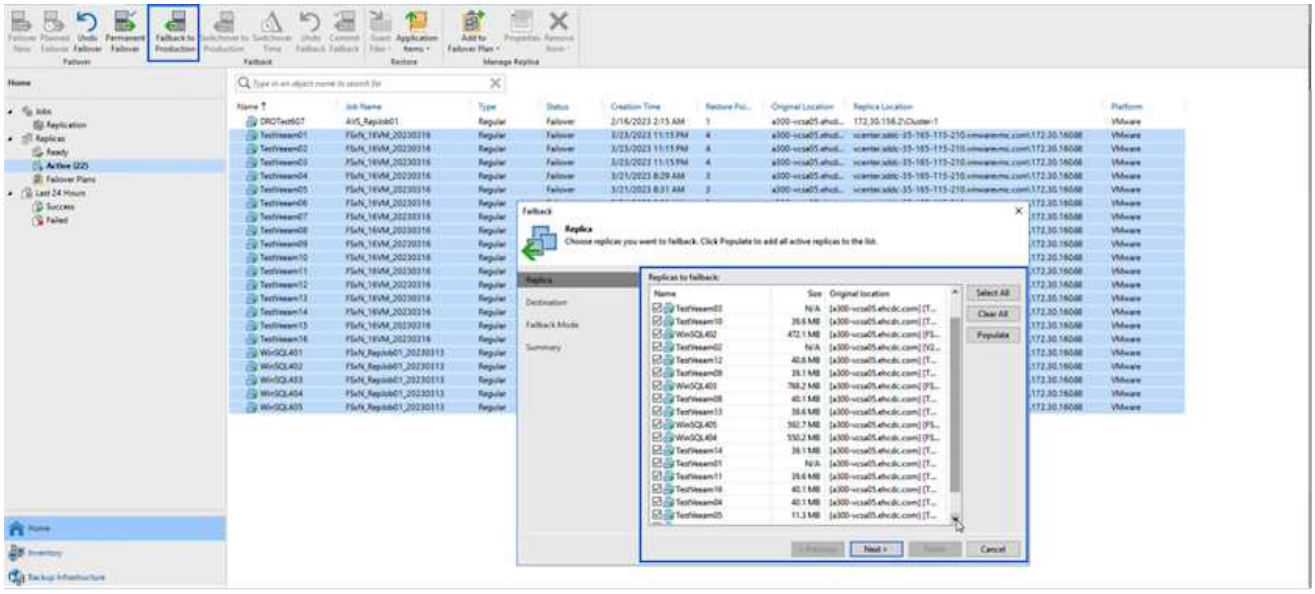
Lorsque le plan de basculement est en cours d'exécution, il est considéré comme une étape intermédiaire et doit être finalisé en fonction de l'exigence. Les options sont les suivantes :

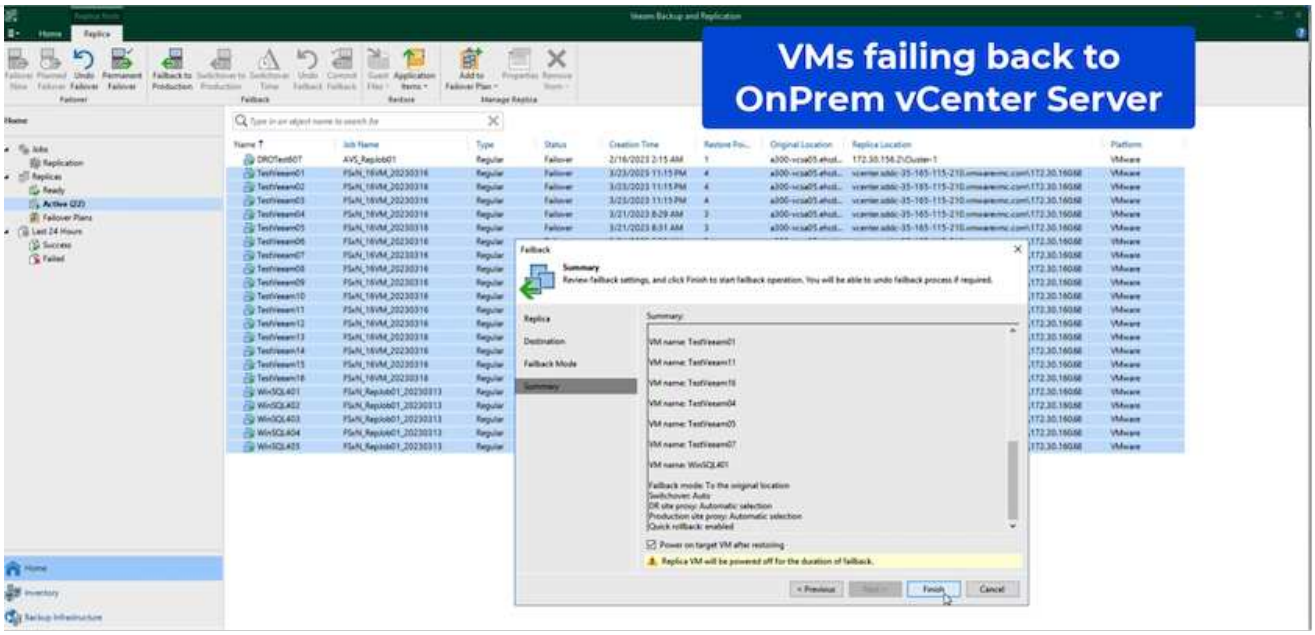
- **Retour en production** - revenez à la machine virtuelle d'origine et transférez toutes les modifications qui ont eu lieu pendant que la réplique de la machine virtuelle était en cours d'exécution sur la machine virtuelle d'origine.

> ⓘ Lorsque vous effectuez un retour arrière, les modifications sont uniquement transférées, mais pas publiées. Choisissez **commit readback** (une fois que la machine virtuelle d'origine a été confirmée pour fonctionner comme prévu) ou **Undo readback** pour revenir au réplica de la machine virtuelle si la machine virtuelle d'origine ne fonctionne pas comme prévu.

- **Annuler le basculement** - revenez à la machine virtuelle d'origine et supprimez toutes les modifications apportées à la réplique de la machine virtuelle pendant son exécution.
- **Basculement permanent** - basculez de manière permanente de la machine virtuelle d'origine vers une réplique de machine virtuelle et utilisez cette réplique comme machine virtuelle d'origine.

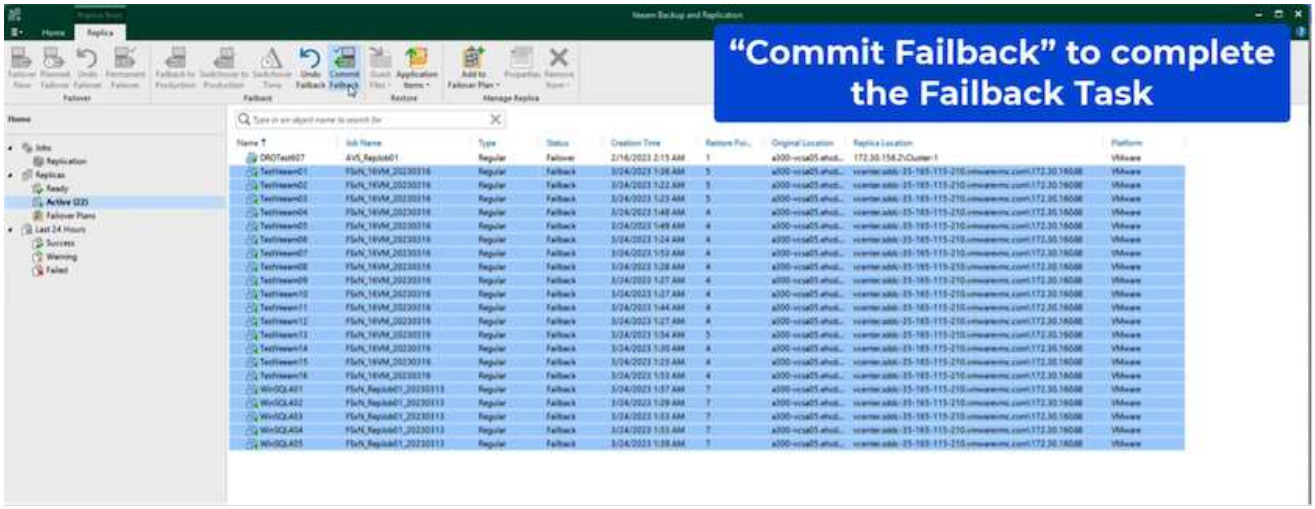
Dans cette démo, le retour arrière à la production a été choisi. Le basculement vers la machine virtuelle d'origine a été sélectionné lors de l'étape destination de l'assistant et la case à cocher « mettre la machine virtuelle sous tension après la restauration » a été activée.

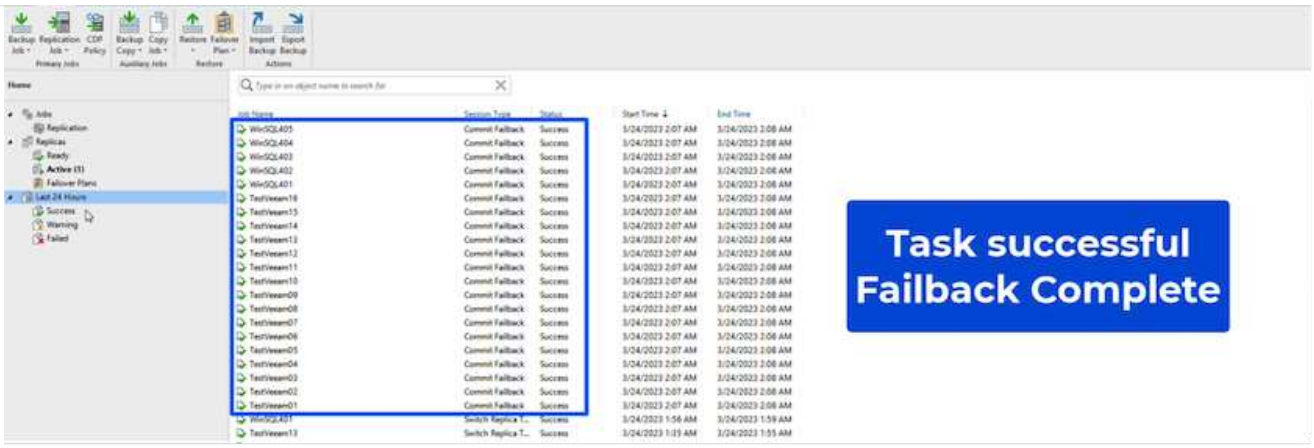




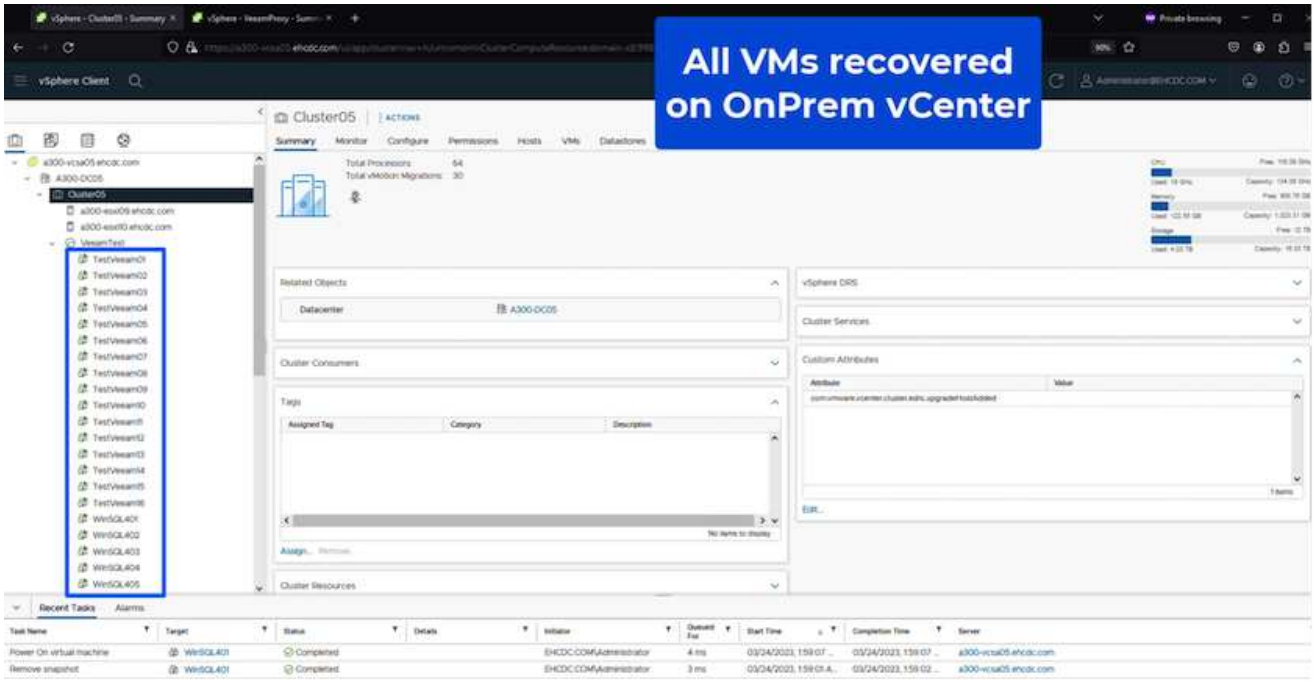
La validation du retour arrière est l'une des méthodes permettant de finaliser l'opération de restauration. Lorsque le retour arrière est validé, il vérifie que les modifications envoyées à la machine virtuelle qui est en retour (la machine virtuelle de production) fonctionnent comme prévu. Après l'opération de validation, Veeam Backup & Replication reprend les activités de réplication pour la machine virtuelle de production.

Pour plus d'informations sur le processus de restauration, reportez-vous à la documentation Veeam pour "Basculement et retour arrière pour la réplication".





Une fois la restauration en production réussie, les machines virtuelles sont toutes restaurées vers le site de production d'origine.



Conclusion

La fonctionnalité de datastore FSX pour ONTAP permet à Veeam ou à tout outil tiers validé de fournir une solution de reprise après incident à faible coût avec un cluster Pilot light et sans avoir besoin de disposer d'un grand nombre d'hôtes dans le cluster uniquement pour prendre en charge la copie de réplica de la machine virtuelle. Cette solution puissante permet de gérer un plan de reprise d'activité personnalisé et de réutiliser les produits de sauvegarde existants en interne pour répondre aux besoins de reprise après incident. Ainsi, la reprise après incident basée sur le cloud est possible en quittant les data centers de reprise après incident sur site. Le basculement peut s'effectuer en cas de basculement planifié ou de basculement d'un simple clic en cas d'incident. La décision d'activer le site de reprise après incident est prise.

Pour en savoir plus sur ce processus, n'hésitez pas à suivre la vidéo de présentation détaillée.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

Migration de workloads sur AWS/VMC

Tr 4942 : migrer les charges de travail vers le datastore ONTAP FSX à l'aide de VMware HCX

L'une des utilisations courantes de VMware Cloud (VMC) sur Amazon Web Services (AWS) et de son datastore NFS supplémentaire sur Amazon FSX pour NetApp ONTAP est la migration des charges de travail VMware. VMware HCX est l'option privilégiée : il offre plusieurs méthodes de migration pour déplacer des machines virtuelles sur site et leurs données, s'exécutant sur n'importe quel datastore VMware pris en charge, vers des datastores VMC, notamment des datastores NFS supplémentaires sur FSX pour ONTAP.

Auteur(s) : Ingénierie de solutions NetApp

Présentation : migration de machines virtuelles avec VMware HCX, les datastores supplémentaires FSX ONTAP et VMware Cloud

VMware HCX est principalement une plateforme de mobilité conçue pour simplifier la migration des charges de travail, le rééquilibrage des charges de travail et la continuité de l'activité dans les clouds. Il est inclus dans VMware Cloud sur AWS et offre de nombreuses façons de migrer les charges de travail, et peut être utilisé pour les opérations de reprise après incident.

Ce document fournit des recommandations détaillées pour le déploiement et la configuration de VMware HCX, notamment tous ses principaux composants, sur site et côté data Center dans le cloud, qui permet d'utiliser divers mécanismes de migration de VM.

Pour plus d'informations, voir "Introduction aux déploiements HCX" et "Installer la liste de contrôle B - HCX avec un environnement VMware Cloud sur AWS SDDC destination".

Étapes générales

Cette liste fournit les étapes générales d'installation et de configuration de VMware HCX :

1. Activer HCX pour le Software-Defined Data Center (SDDC) du VMC via VMware Cloud Services Console
2. Téléchargez et déployez le programme d'installation OVA du connecteur HCX dans le serveur vCenter sur site.
3. Activer HCX avec une clé de licence.
4. Couplez le connecteur VMware HCX sur site avec VMC HCX Cloud Manager.
5. Configurez le profil réseau, le profil de calcul et le maillage de service.
6. (Facultatif) exécutez l'extension réseau pour étendre le réseau et éviter une nouvelle adresse IP.
7. Validez l'état du système et assurez-vous que la migration est possible.
8. Migrer les workloads de VM.

Prérequis

Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, voir "Préparation de l'installation HCX". Une fois les prérequis en place, y compris la connectivité, configurez et activez HCX en générant une clé de licence à partir de la console VMware HCX sur VMC. Une fois que HCX est activé, le plug-in vCenter est déployé et est accessible via la console vCenter pour la gestion.

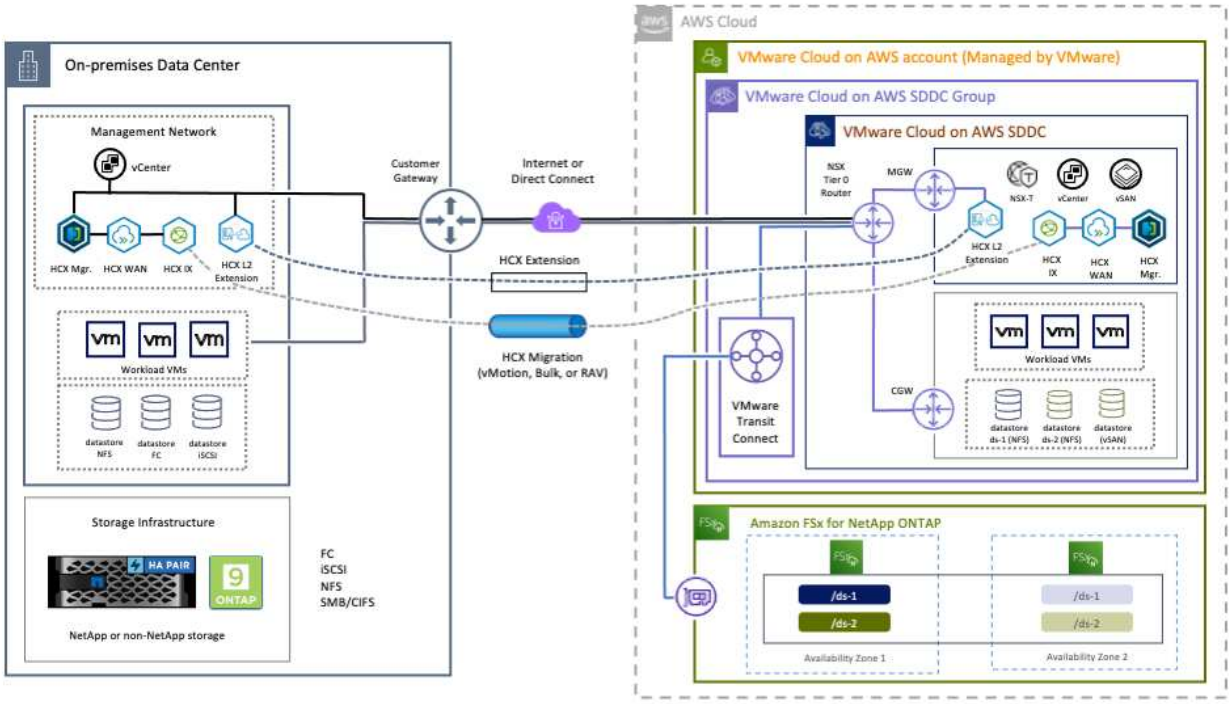
Les étapes d'installation suivantes doivent être effectuées avant de procéder à l'activation et au déploiement du système HCX :

1. Nous utilisons un SDDC VMC existant ou créons un SDDC après ce processus "Lien NetApp" ou ceci "Lien VMware".
2. Le chemin réseau depuis l'environnement vCenter sur site vers le SDDC VMC doit prendre en charge la migration des VM à l'aide de vMotion.
3. Assurez-vous que le nécessaire "règles et ports de pare-feu" Sont autorisées pour le trafic vMotion entre vCenter Server sur site et SDDC vCenter.
4. Le volume FSX pour ONTAP NFS doit être monté en tant que datastore supplémentaire dans le SDDC VMC. Pour attacher les datastores NFS au cluster approprié, suivez les étapes décrites dans ce document "Lien NetApp" ou ceci "Lien VMware".

Architecture de haut niveau

À des fins de test, l'environnement de laboratoire sur site utilisé pour cette validation a été connecté par le biais d'un VPN site à site vers AWS VPC, qui permettait la connectivité sur site à AWS et au SDDC cloud VMware via une passerelle de transport externe. La migration HCX et le trafic des extensions réseau transitent par Internet entre le SDDC de destination sur site et le SDDC de destination sur le cloud VMware. Cette architecture peut être modifiée pour utiliser les interfaces virtuelles privées Direct Connect.

L'image suivante représente l'architecture de haut niveau.



Déploiement de la solution

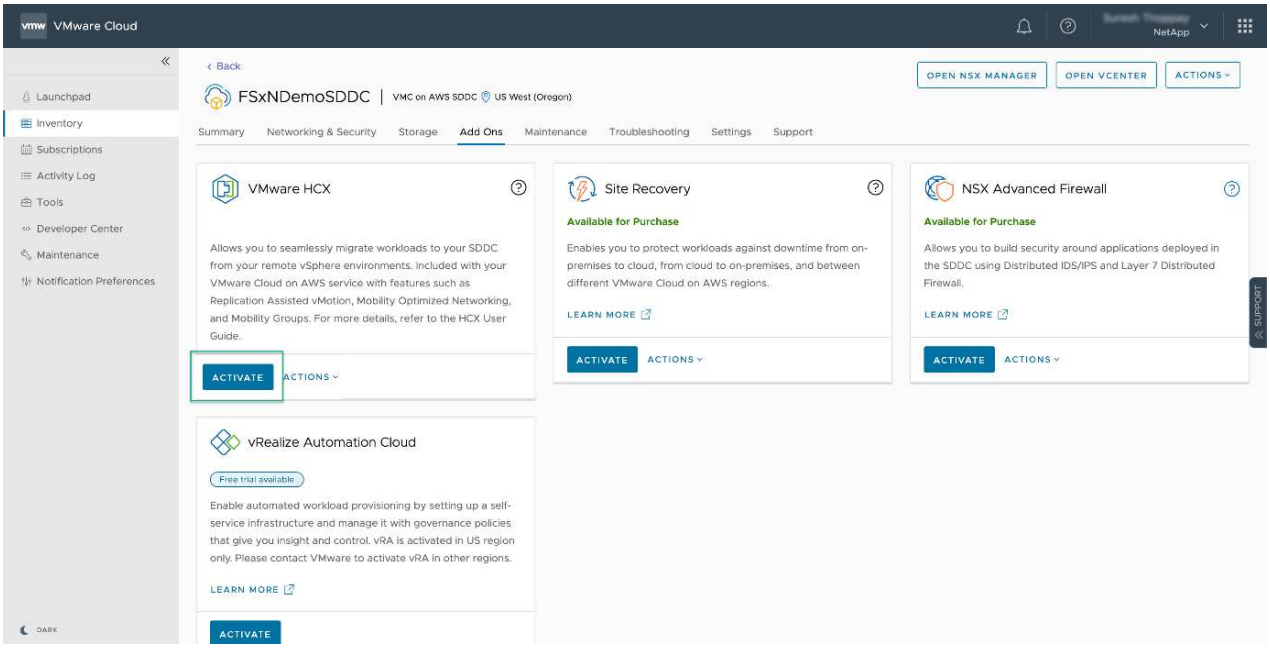
Suivez les étapes du déploiement de cette solution :

Étape 1 : activez HCX via VMC SDDC en utilisant l'option Add-ons

Pour effectuer l'installation, procédez comme suit :

1. Connectez-vous à la console VMC à "vmc.vmware.com" Et accéder à l'inventaire.
2. Pour sélectionner le SDDC approprié et accéder aux Add- ons, cliquez sur View Details dans SDDC et sélectionnez l'onglet Add ans.
3. Cliquez sur Activer pour VMware HCX.

   Cette étape peut prendre jusqu'à 25 minutes.

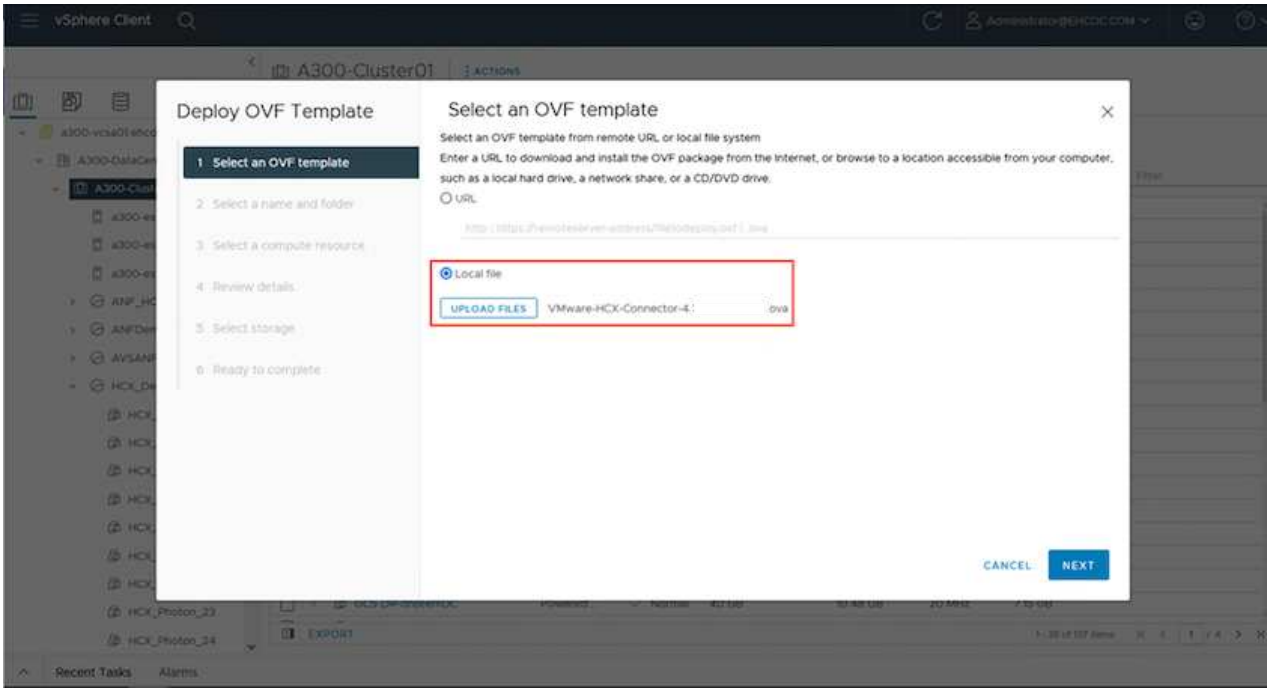


4. Une fois le déploiement terminé, validez le déploiement en vérifiant que HCX Manager et les plug-ins associés sont disponibles dans vCenter Console.
5. Créez les pare-feu de passerelle de gestion appropriés pour ouvrir les ports nécessaires pour accéder à HCX Cloud Manager.HCX Cloud Manager est maintenant prêt pour les opérations HCX.

Étape 2 : déployer le fichier OVA du programme d'installation dans le serveur vCenter sur site

Pour que le connecteur sur site communique avec HCX Manager dans VMC, assurez-vous que les ports pare-feu appropriés sont ouverts dans l'environnement sur site.

1. Dans la console VMC, accédez au tableau de bord HCX, allez à Administration et sélectionnez l'onglet mise à jour des systèmes. Cliquez sur demander un lien de téléchargement pour l'image OVA du connecteur HCX.
2. Avec le connecteur HCX téléchargé, déployez le fichier OVA dans le serveur vCenter sur site. Cliquez avec le bouton droit de la souris sur cluster vSphere et sélectionnez l'option déployer le modèle OVF.

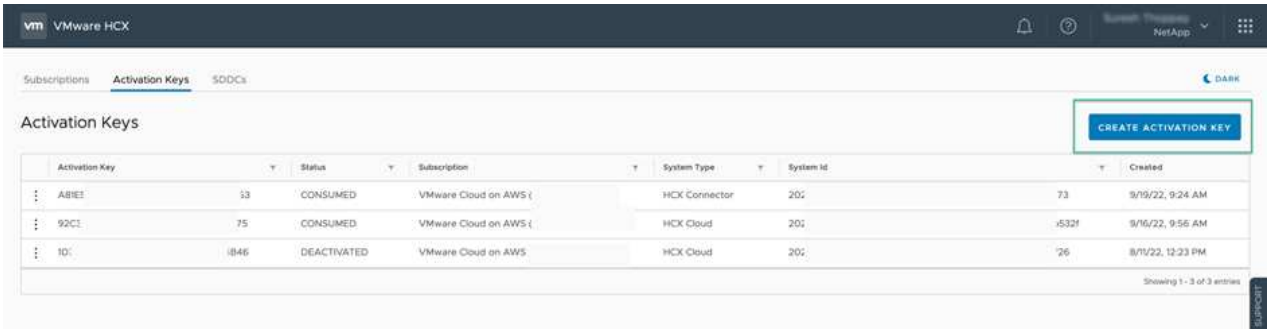


3. Entrez les informations requises dans l'assistant déployer modèle OVF, cliquez sur Suivant, puis sur Terminer pour déployer le connecteur OVA VMware HCX.
4. Mettez l'appliance virtuelle sous tension manuellement.pour obtenir des instructions détaillées, reportez-vous à la section "Guide de l'utilisateur VMware HCX".

Étape 3 : activez le connecteur HCX avec la clé de licence

Après avoir déployé le connecteur OVA VMware HCX sur site et démarré l'appliance, procédez comme suit pour activer le connecteur HCX. Générez la clé de licence à partir de la console VMware HCX sur VMC et entrez la licence lors de la configuration du connecteur VMware HCX.

1. Dans VMware Cloud Console, allez dans Inventory, sélectionnez le SDDC et cliquez sur View Details. Dans l'onglet Add ans, dans la mosaïque VMware HCX, cliquez sur Ouvrir HCX.
2. Dans l'onglet clés d'activation, cliquez sur Créer une clé d'activation. Sélectionnez le type de système comme connecteur HCX et cliquez sur confirmer pour générer la clé. Copier la clé d'activation.



> Une clé distincte est requise pour chaque connecteur HCX déployé sur site.

3. Connectez-vous au connecteur VMware HCX sur site à `"https://hcxconnectorIP:9443"` utilisation des informations d'identification administrateur.

> Utiliser le mot de passe défini lors du déploiement de l'OVA.

4. Dans la section Licence, entrez la clé d'activation copiée à partir de l'étape 2 et cliquez sur Activer.

> Le connecteur HCX sur site doit disposer d'un accès Internet pour que l'activation puisse s'effectuer correctement.

5. Sous Datacenter Location, indiquez l'emplacement souhaité pour l'installation sur site de VMware HCX Manager. Cliquez sur Continuer .
6. Sous Nom du système, mettez à jour le nom et cliquez sur Continuer.
7. Sélectionnez Oui, puis Continuer.
8. Sous connecter votre vCenter, indiquez l'adresse IP ou le nom de domaine complet (FQDN), ainsi que les informations d'identification du serveur vCenter, puis cliquez sur Continuer.

> Utilisez le FQDN pour éviter les problèmes de communication plus tard.

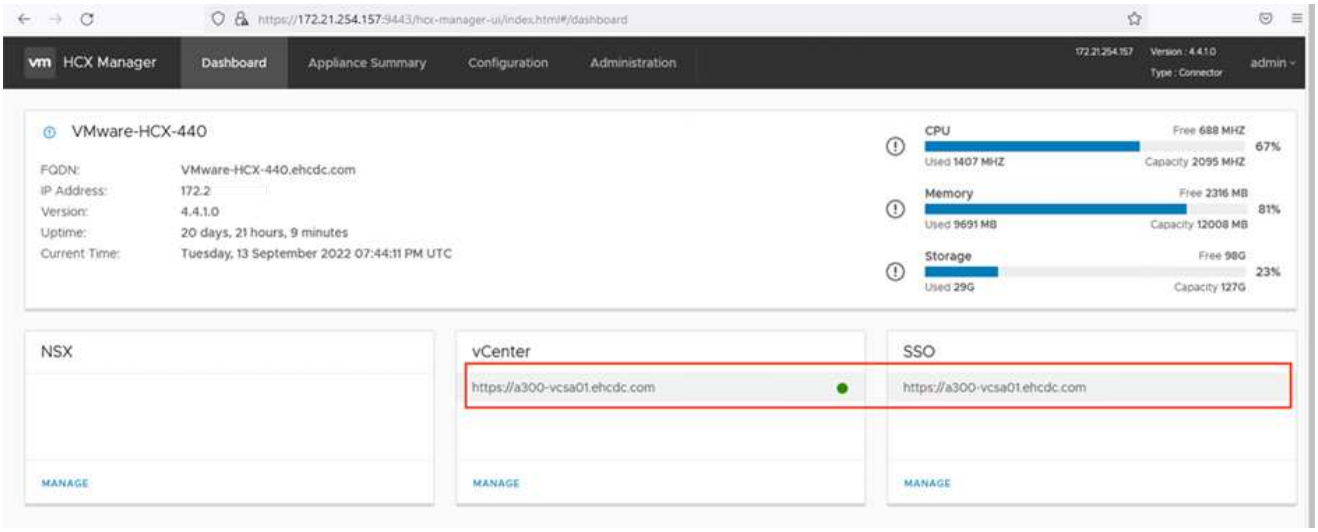
9. Sous configurer SSO/PSC, indiquez le FQDN ou l'adresse IP du contrôleur Platform Services Controller et cliquez sur Continuer.

> Entrez l'adresse IP ou le FQDN du serveur vCenter.

10. Vérifiez que les informations saisies sont correctes et cliquez sur redémarrer.
11. Une fois l'opération terminée, le serveur vCenter s'affiche en vert. VCenter Server et SSO doivent

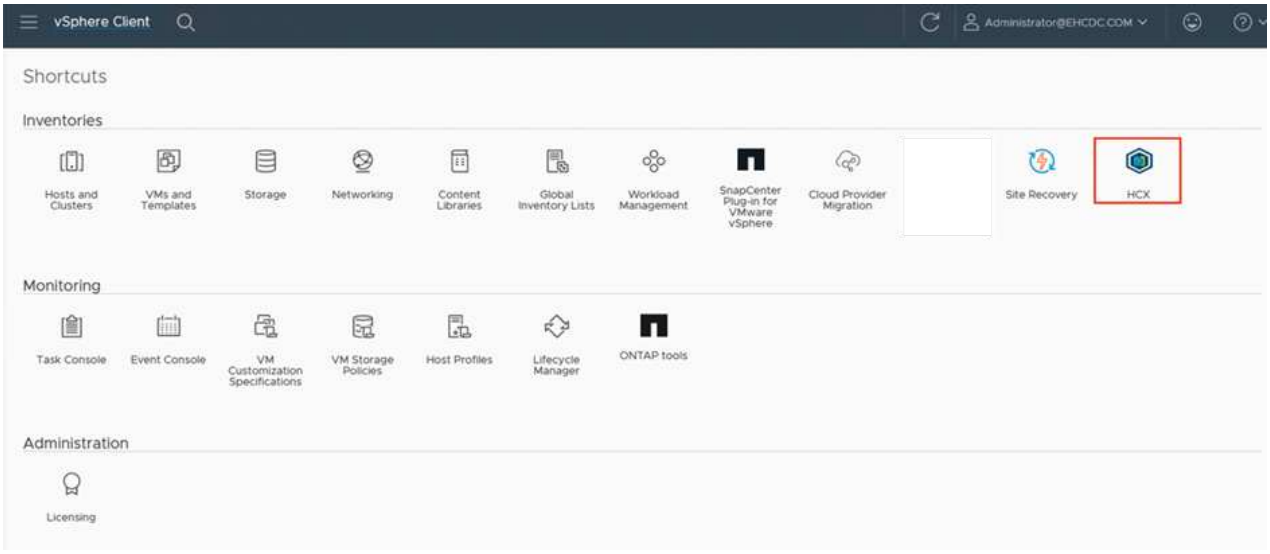
avoir les paramètres de configuration corrects, qui doivent être identiques à la page précédente.

Ce processus dure environ 10 à 20 minutes et le plug-in peut être ajouté à vCenter Server.

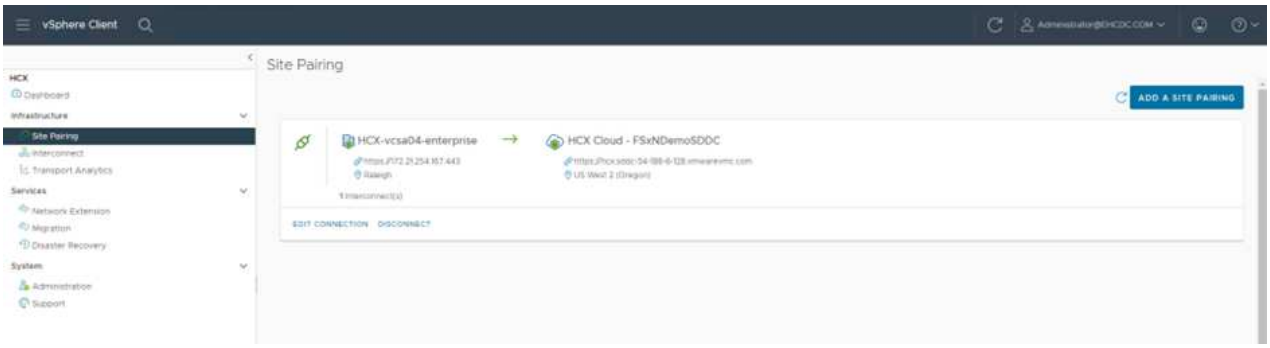


Étape 4 : coupler le connecteur VMware HCX sur site avec VMC HCX Cloud Manager

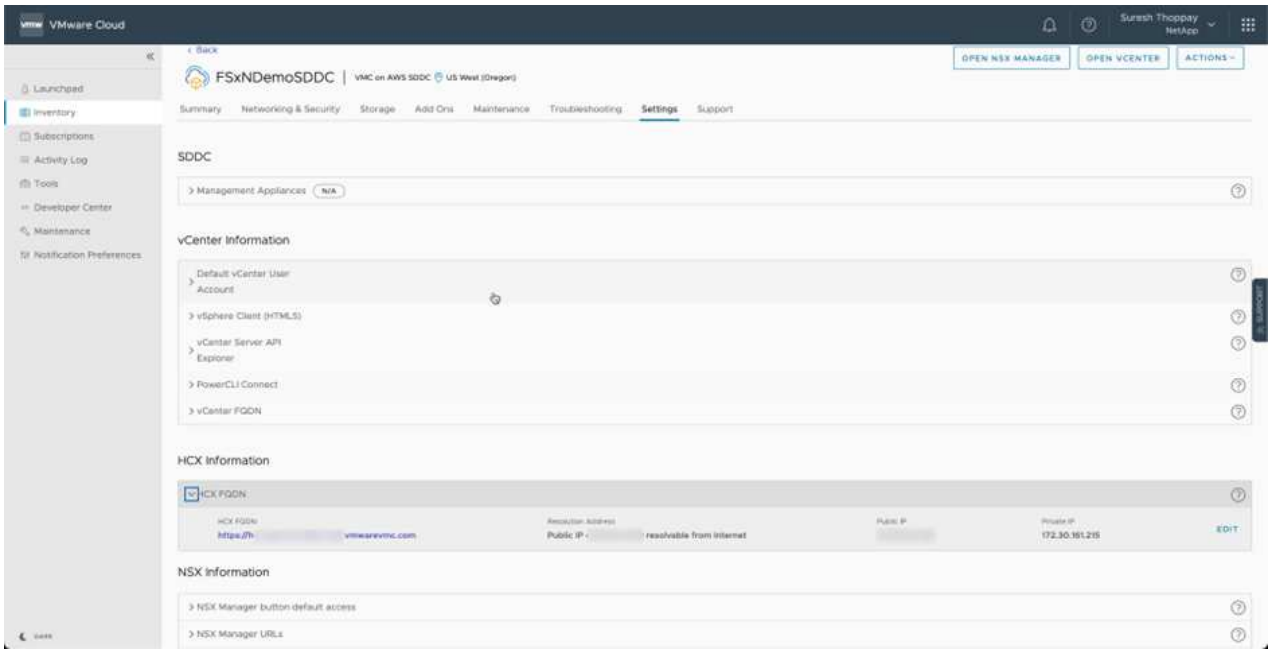
1. Pour créer une paire de sites entre vCenter Server sur site et le SDDC VMC, connectez-vous au serveur vCenter sur site et accédez au plug-in client Web HCX vSphere.

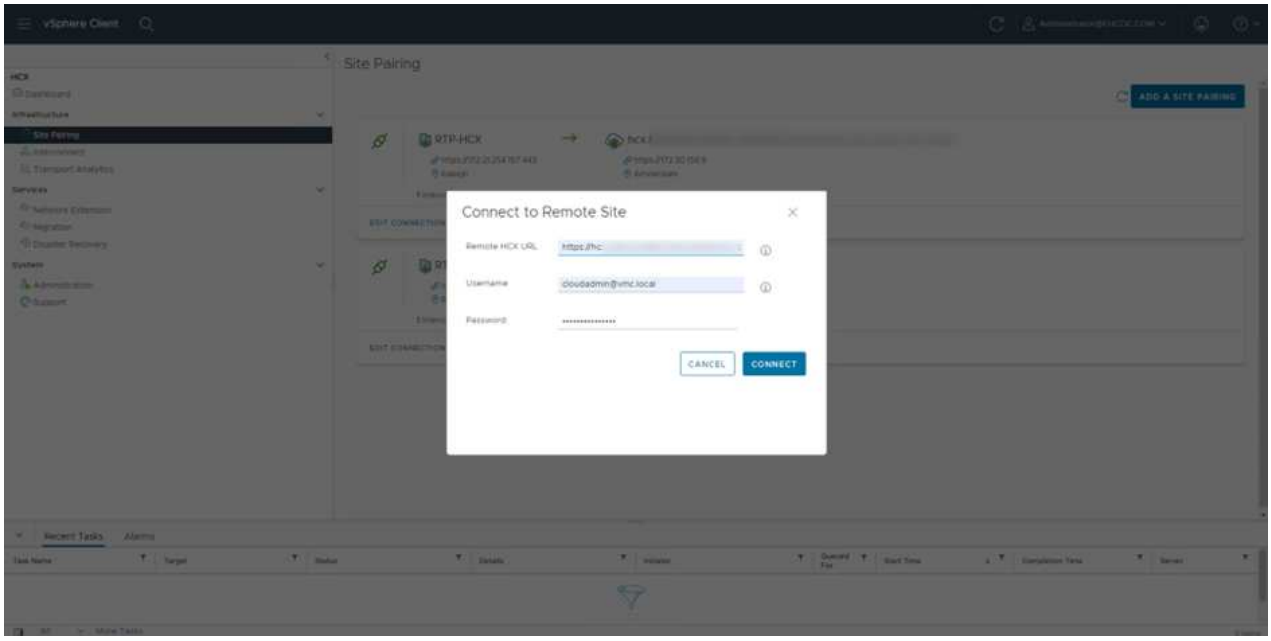


2. Sous Infrastructure, cliquez sur Ajouter un couplage de site. Pour authentifier le site distant, entrez l'URL ou l'adresse IP du VMC HCX Cloud Manager et les informations d'identification du rôle CloudAdmin.



Les informations HCX peuvent être récupérées à partir de la page des paramètres SDDC.





3. Pour lancer le couplage du site, cliquez sur connecter.

> Le connecteur VMware HCX doit pouvoir communiquer avec l'IP HCX Cloud Manager via le port 443.

4. Une fois le couplage créé, le couplage de site nouvellement configuré est disponible sur le tableau de bord HCX.

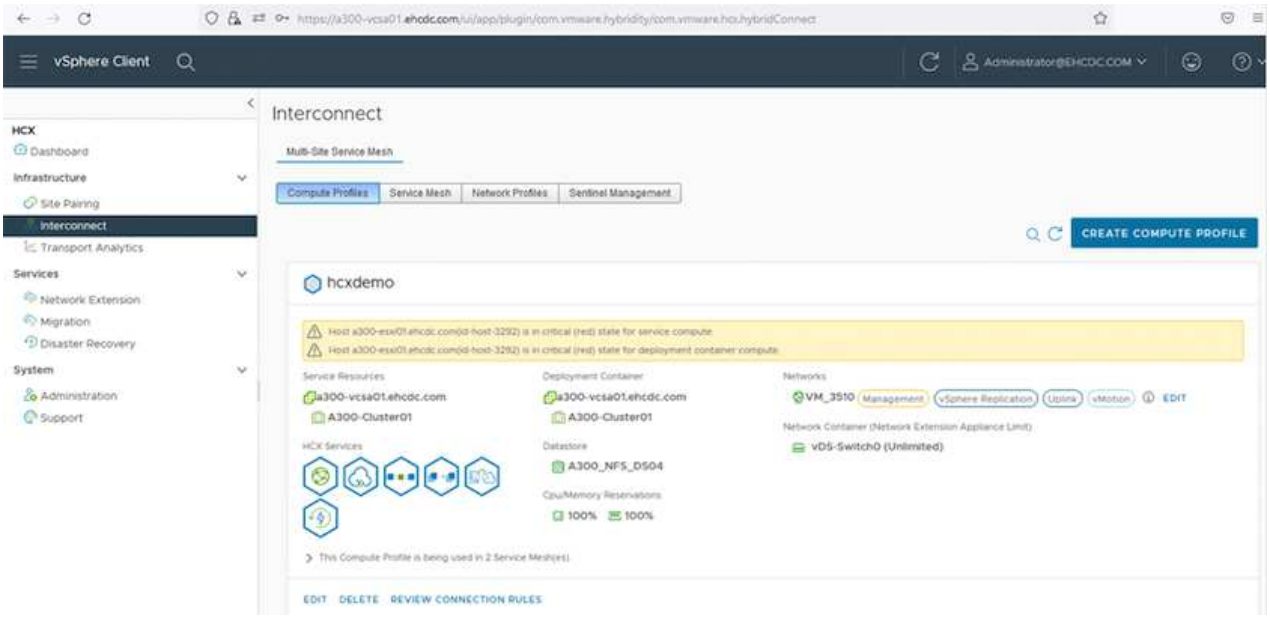
Étape 5 : configurer le profil réseau, le profil de calcul et le maillage de service

Le dispositif VMware HCX Interconnect (HCX-IX) offre des fonctionnalités de tunnel sécurisées par Internet et des connexions privées au site cible qui permettent la réplication et les fonctionnalités vMotion. L'interconnexion permet le cryptage, l'ingénierie du trafic et un réseau SD-WAN. Pour créer l'appliance d'interconnexion HCI-IX, effectuez les opérations suivantes :

1. Sous Infrastructure, sélectionnez Interconnexion > maillage de service multisite > profils de calcul > Créer un profil de calcul.

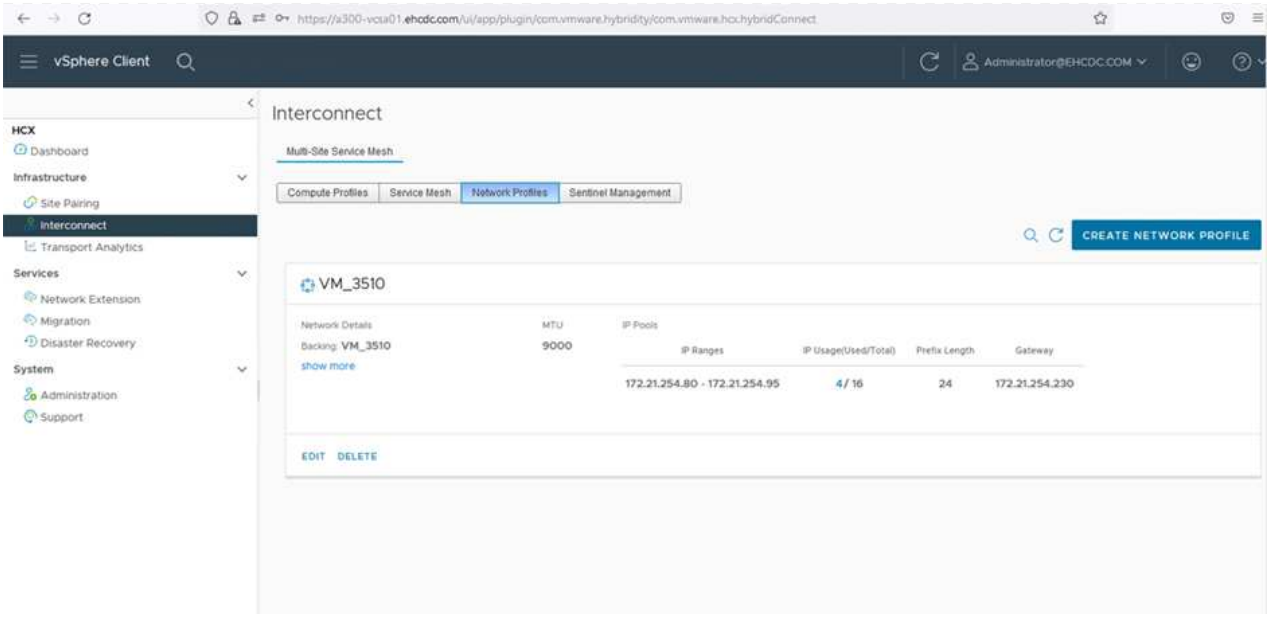
   Les profils de calcul contiennent les paramètres de déploiement de calcul, de stockage et de réseau requis pour déployer une appliance virtuelle d'interconnexion. Ils précisent également quelle partie du data Center VMware sera accessible au service HCX.

   Pour obtenir des instructions détaillées, reportez-vous à la section "Création d'un profil de calcul".



2. Une fois le profil de calcul créé, créez le profil réseau en sélectionnant maillage de service multisite > profils réseau > Créer un profil réseau.
3. Le profil réseau définit une plage d'adresses IP et de réseaux qui seront utilisés par HCX pour ses appliances virtuelles.

   Cela nécessite au moins deux adresses IP. Ces adresses IP seront attribuées du réseau de gestion aux appliances virtuelles.

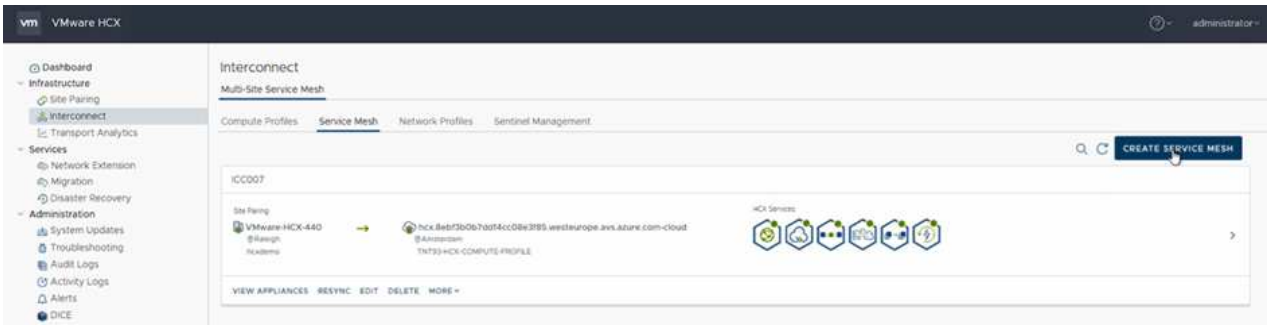


Pour obtenir des instructions détaillées, reportez-vous à la section "Création d'un profil réseau".

Si vous vous connectez à un réseau SD-WAN via Internet, vous devez réserver des adresses IP publiques dans la section réseau et sécurité.

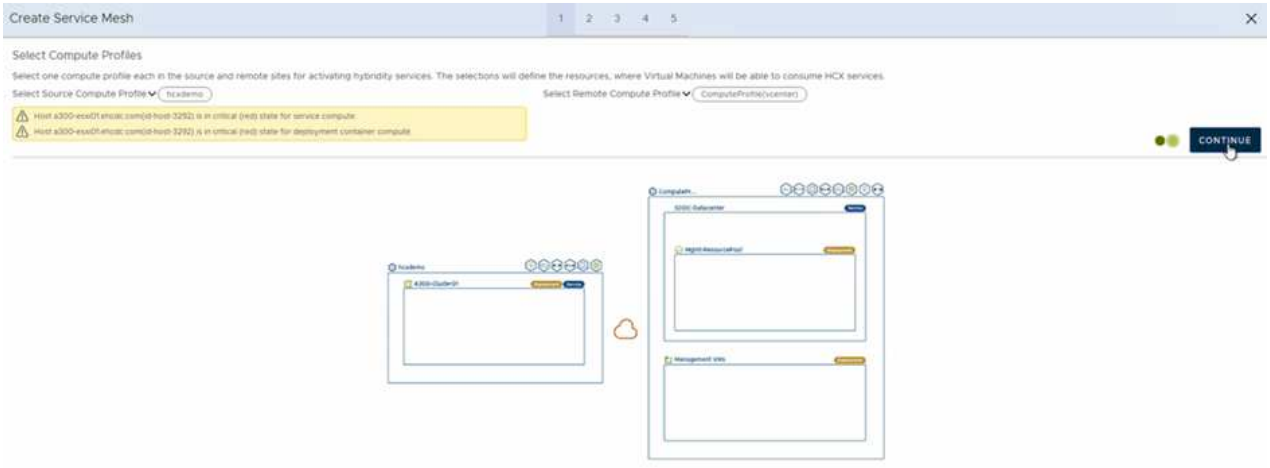
4. Pour créer un maillage de service, sélectionnez l'onglet maillage de service dans l'option interconnexion et sélectionnez sites SDDC locaux et VMC.

   Le maillage de service établit une paire de profils réseau et de calcul locale et distante.

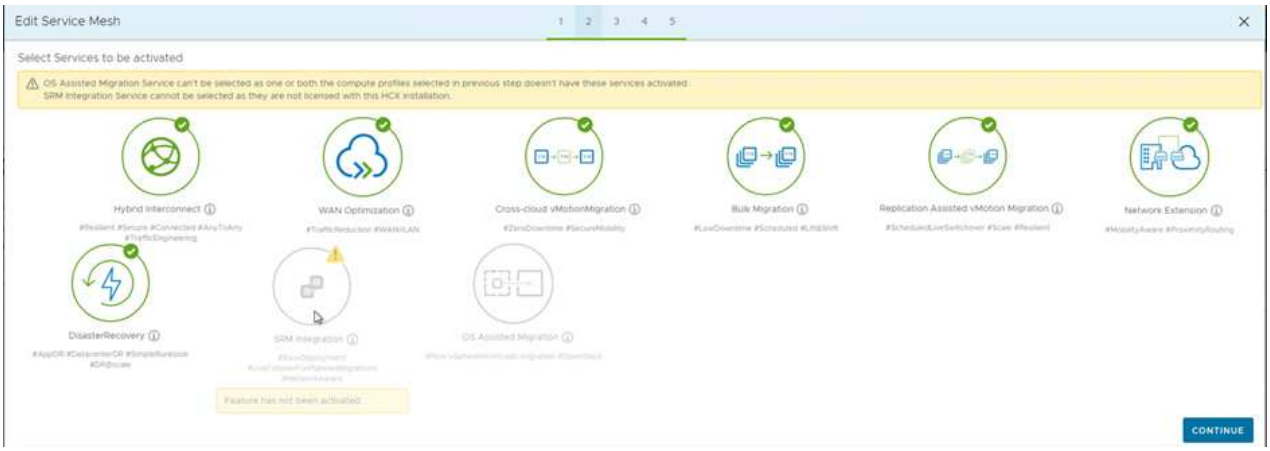


Ce processus implique notamment le déploiement d'appliances HCX qui seront automatiquement configurées sur les sites source et cible, créant ainsi une structure de transport sécurisée.

5. Sélectionnez les profils de calcul source et distant, puis cliquez sur Continuer.

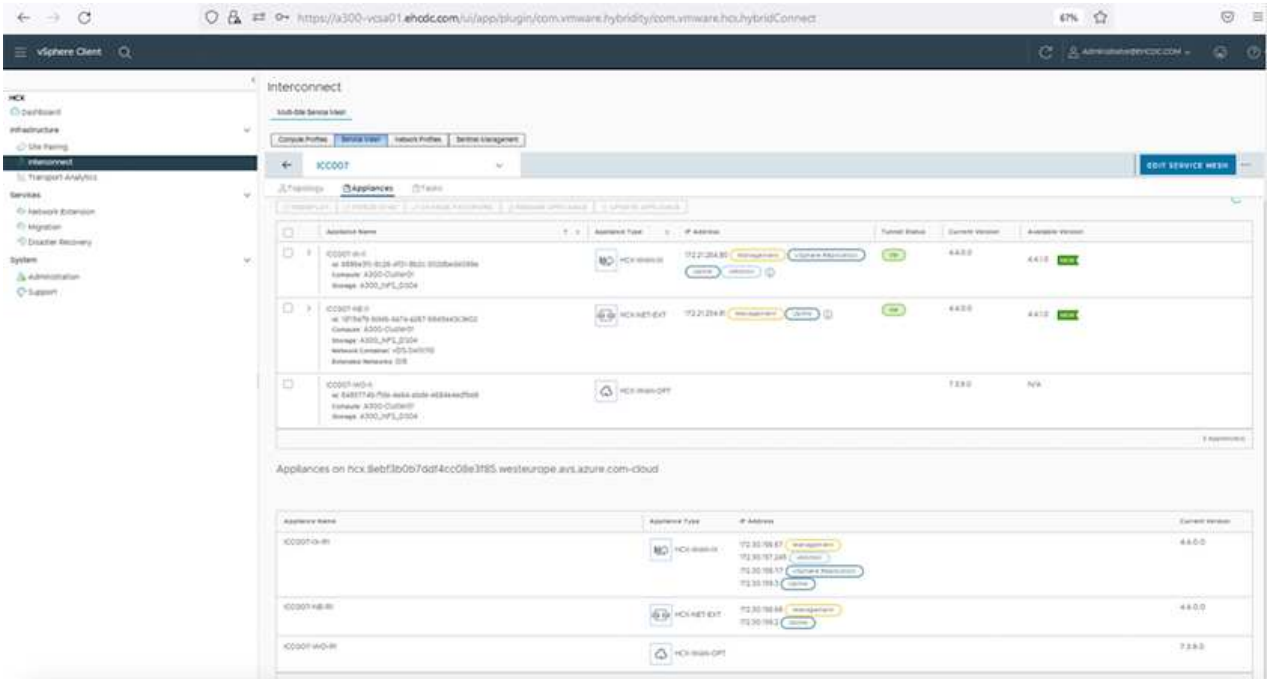


6. Sélectionnez le service à activer et cliquez sur Continuer.



Une licence HCX Enterprise est requise pour la migration par réplication assistée vMotion, l'intégration SRM et la migration assistée par système d'exploitation.

7. Créez un nom pour le maillage de service et cliquez sur Terminer pour lancer le processus de création. Le déploiement devrait prendre environ 30 minutes. Une fois le maillage de service configuré, l'infrastructure virtuelle et la mise en réseau nécessaires pour migrer les VM de la charge de travail ont été créées.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

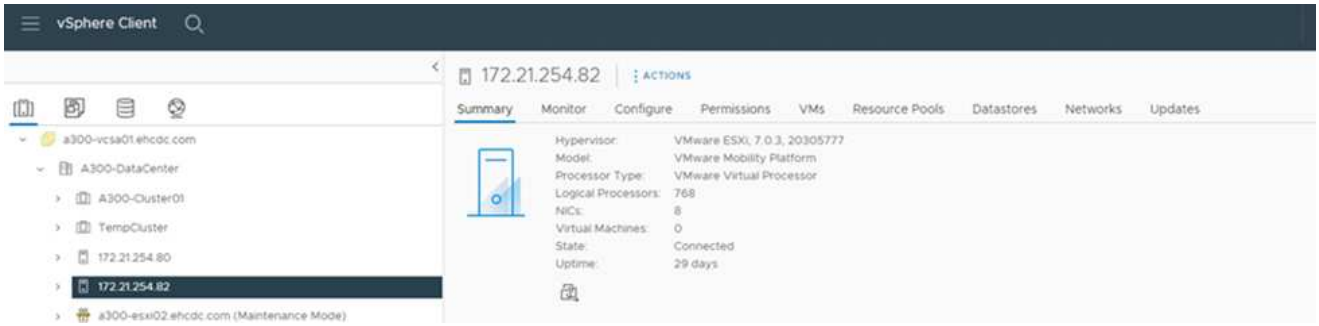
Étape 6 : migration des workloads

HCX offre des services de migration bidirectionnels entre deux environnements distincts ou plus, tels que les SDDC sur site et VMC. Les charges de travail applicatives peuvent être migrées depuis et vers des sites activés HCX à l'aide de diverses technologies de migration telles que la migration en bloc HCX, HCX vMotion, la migration à froid HCX, l'option vMotion par réplication assistée par HCX (disponible avec HCX Enterprise Edition) et la migration assistée par système d'exploitation HCX (disponible avec l'édition HCX Enterprise).

Pour en savoir plus sur les technologies de migration HCX disponibles, consultez "Types de migration VMware HCX"

L'appliance HCX-IX utilise le service Mobility Agent pour effectuer des migrations vMotion, Cold et Replication Assisted vMotion (RAV).

> L'appliance HCX-IX ajoute le service Mobility Agent en tant qu'objet hôte dans vCenter Server. Les ressources processeur, mémoire, stockage et réseau affichées sur cet objet ne représentent pas la consommation réelle sur l'hyperviseur physique hébergeant l'appliance IX.

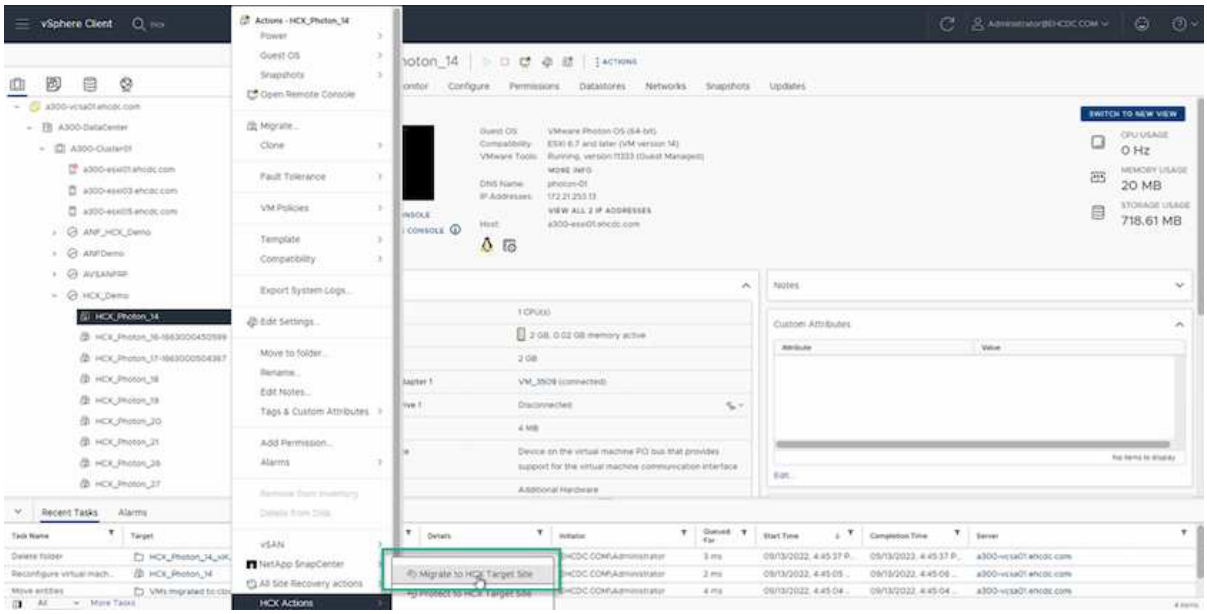


VMware HCX vMotion

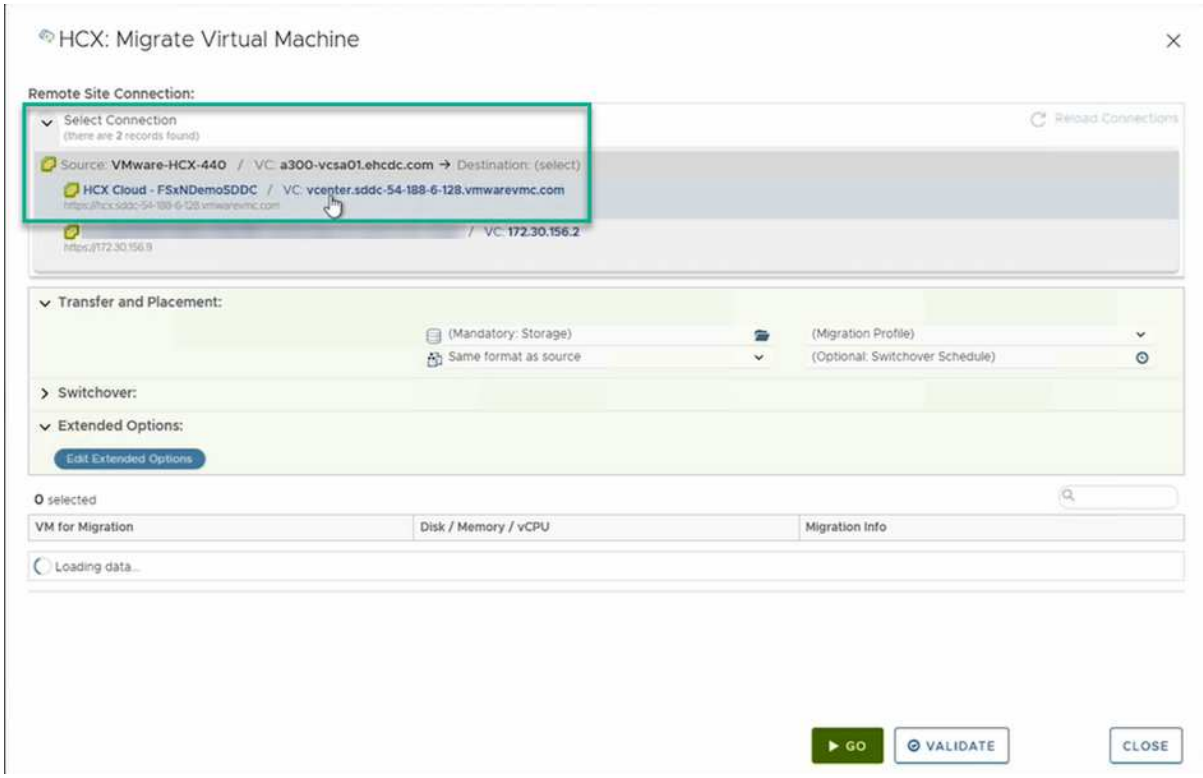
Cette section décrit le mécanisme HCX vMotion. Cette technologie de migration utilise le protocole VMware vMotion pour migrer une machine virtuelle vers un SDDC VMC. L'option de migration vMotion permet de migrer l'état d'une machine virtuelle unique à la fois. Il n'y a pas d'interruption de service pendant cette méthode de migration.

> L'extension réseau doit être en place (pour le groupe de ports dans lequel la machine virtuelle est connectée) afin de migrer la machine virtuelle sans avoir à modifier l'adresse IP.

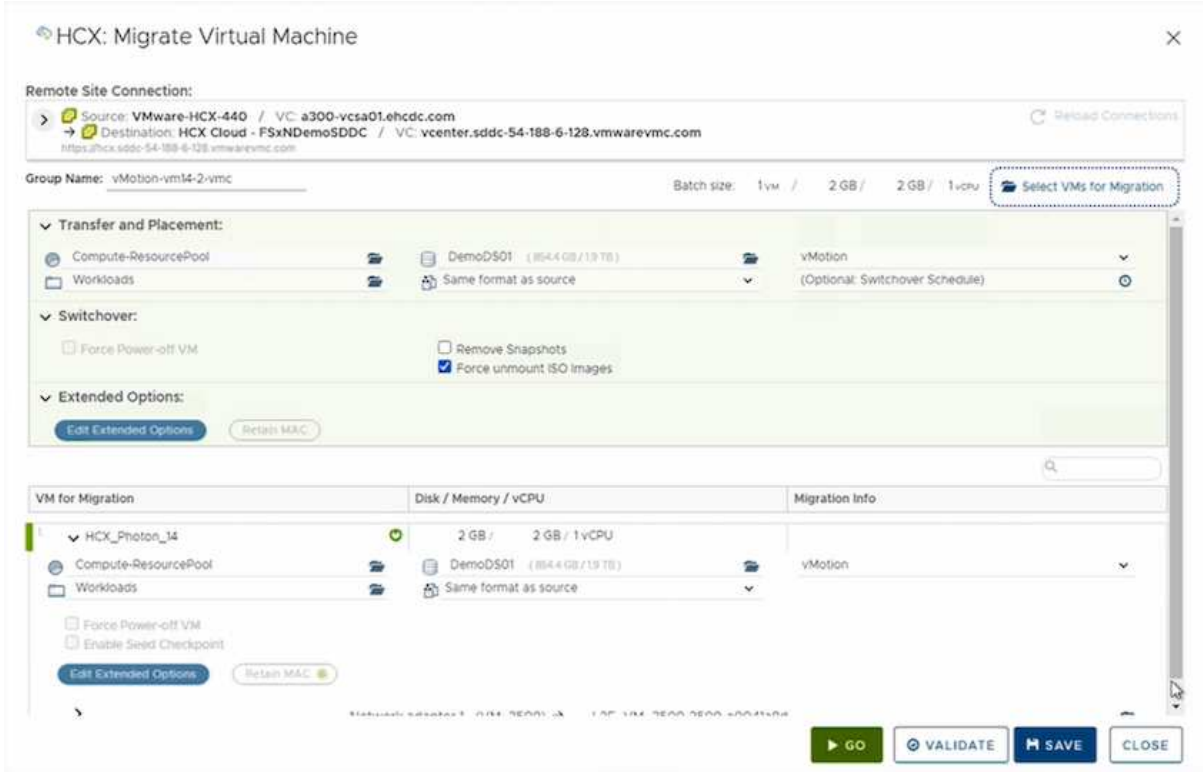
1. Depuis le client vSphere sur site, accédez à Inventory, faites un clic droit sur la machine virtuelle à migrer, puis sélectionnez HCX actions > Migrate to HCX site cible.



2. Dans l'assistant de migration d'ordinateur virtuel, sélectionner Remote site Connection (VMC SDDC cible).



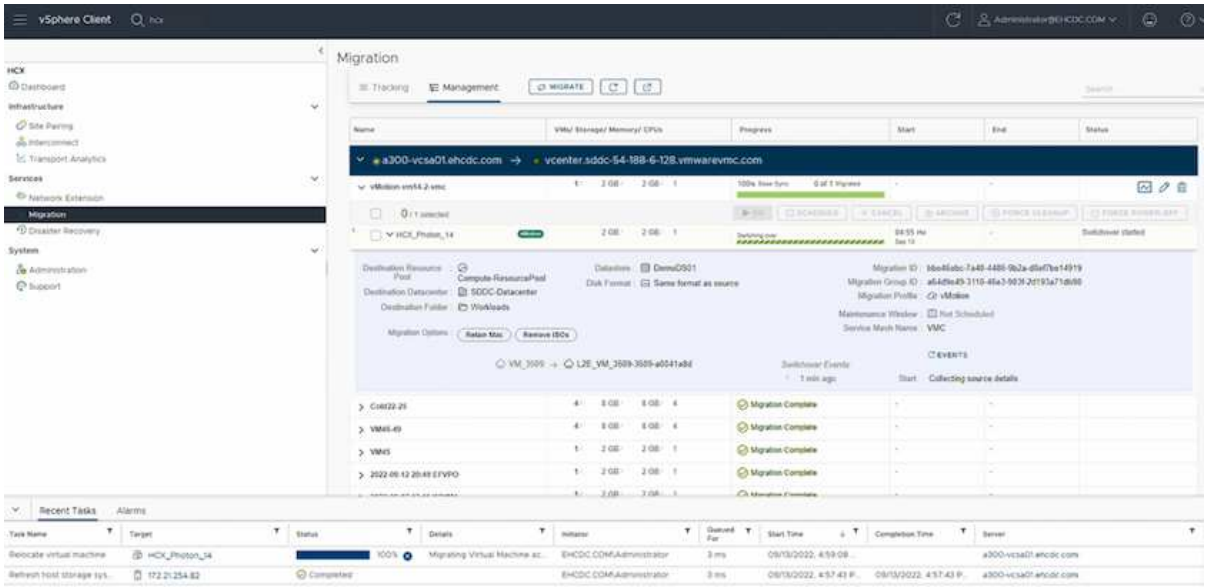
3. Ajoutez un nom de groupe et sous transfert et placement, mettez à jour les champs obligatoires (réseau de cluster, de stockage et de destination), puis cliquez sur Valider.



4. Une fois les vérifications de validation terminées, cliquez sur Go pour lancer la migration.

Le transfert vMotion capture la mémoire active de la machine virtuelle, son état d'exécution, son adresse IP et son adresse MAC. Pour plus d'informations sur les exigences et les limites de HCX vMotion, voir "Comprendre VMware HCX vMotion et la migration à froid".

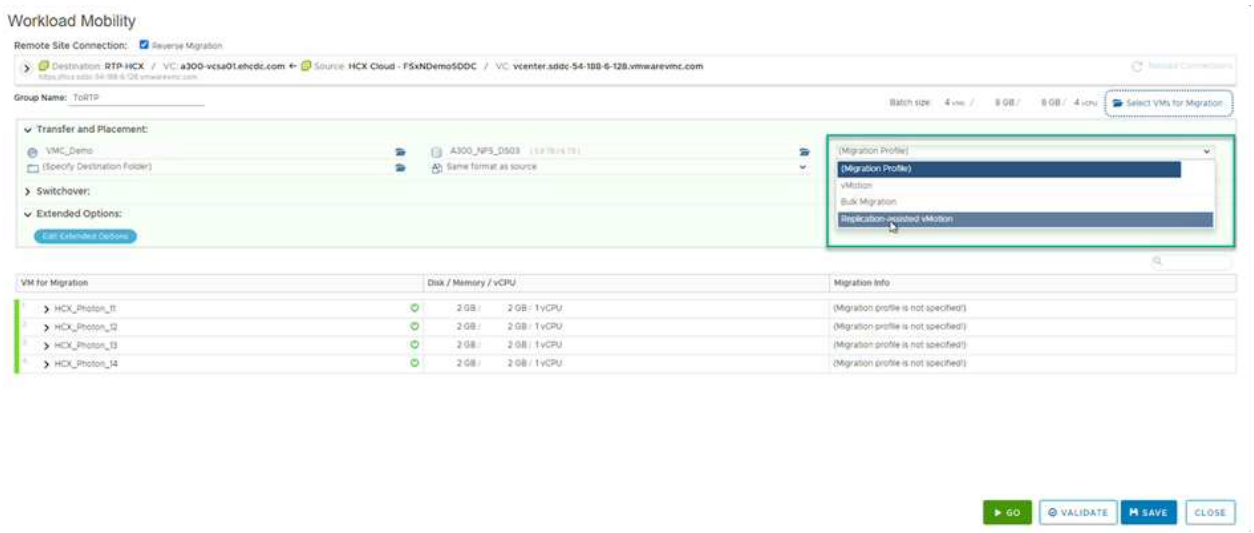
5. Vous pouvez contrôler la progression et l'achèvement de vMotion dans le tableau de bord HCX > migration.



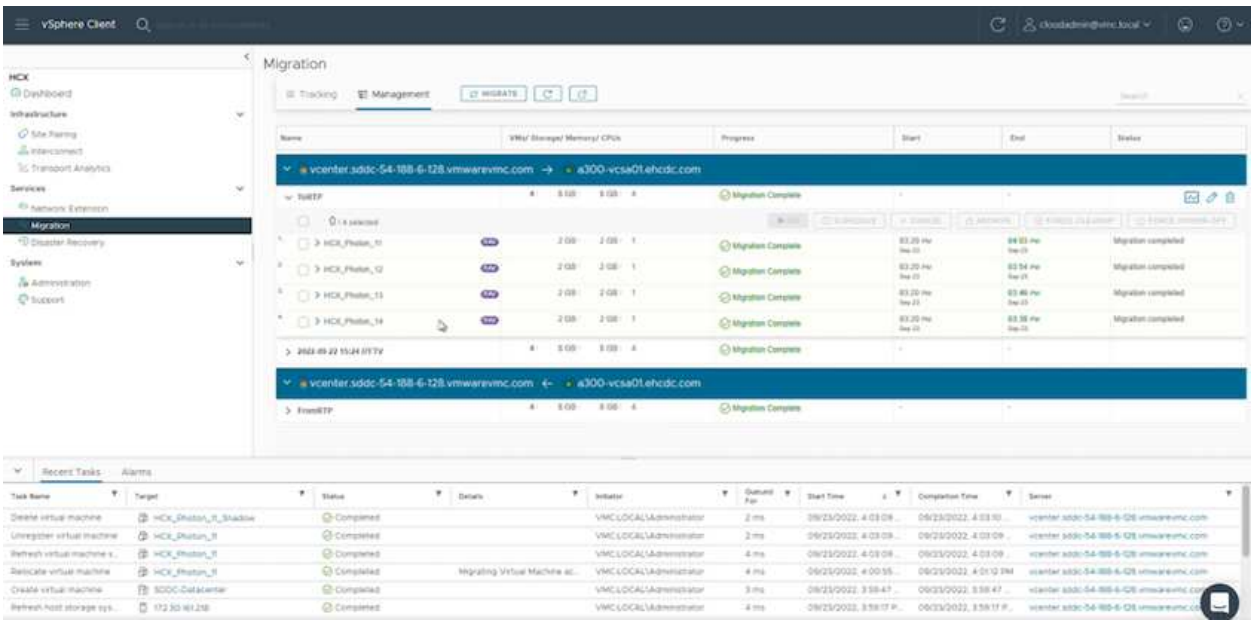
VMware Replication Assisted vMotion

Comme vous l'avez peut-être remarqué dans la documentation VMware, VMware HCX Replication Assisted vMotion (RAV) combine les avantages de la migration en bloc et de vMotion. La migration en bloc utilise la réplication vSphere pour migrer plusieurs machines virtuelles en parallèle : la machine virtuelle est redémarrée lors du basculement. HCX vMotion migre sans temps d'indisponibilité, mais il est exécuté en série une machine virtuelle à la fois dans un groupe de réplication. RAV réplique la machine virtuelle en parallèle et la synchronise jusqu'à ce que la fenêtre de basculement s'affiche. Lors du processus de basculement, il migre une machine virtuelle à la fois, sans temps d'indisponibilité pour la machine virtuelle.

La capture d'écran suivante montre le profil de migration sous la forme Replication Assisted vMotion.



La durée de la réplication peut être plus longue que celle de vMotion d'un petit nombre de machines virtuelles. Avec RAV, synchronisez uniquement les données modifiées et incluez le contenu de la mémoire. Voici une capture d'écran du statut de migration : elle montre comment l'heure de début de la migration est identique et l'heure de fin est différente pour chaque machine virtuelle.



Pour plus d'informations sur les options de migration HCX et sur la façon de migrer des workloads sur site vers VMware Cloud sur AWS à l'aide du modèle HCX, consultez le "Guide de l'utilisateur VMware HCX".

VMware HCX vMotion nécessite un débit de 100 Mbit/s ou plus.

L'espace nécessaire au datastore VMC FSX cible pour ONTAP doit être suffisant pour prendre en charge la migration.

Conclusion

Que vous cibliez les clouds 100 % cloud ou hybrides et les données résidant sur un stockage de n'importe quel type ou fournisseur sur site, Amazon FSX pour NetApp ONTAP et HCX offrent d'excellentes options pour déployer et migrer les charges de travail tout en réduisant le coût total de possession grâce à une intégration transparente des données à la couche applicative. Quels que soient les cas d'utilisation, choisissez la solution VMC et la solution FSX pour ONTAP datastore pour bénéficier rapidement des avantages du cloud, d'une infrastructure cohérente et des opérations entre plusieurs clouds et sur site, de la portabilité bidirectionnelle des charges de travail, et de la capacité et des performances de grande qualité. Il s'agit du même processus et procédures que celui utilisé pour connecter le stockage et migrer les machines virtuelles à l'aide de la réplication VMware vSphere, de VMware vMotion ou même de la copie NFC.

Messages clés

Les points clés de ce document sont les suivants :

- Il est désormais possible d'utiliser Amazon FSX ONTAP en tant que datastore avec VMC SDDC.
- Vous pouvez facilement migrer des données depuis n'importe quel data Center sur site vers VMC exécuté avec FSX pour le datastore ONTAP
- Vous pouvez facilement étendre et réduire le datastore ONTAP FSX en vue de répondre aux exigences en termes de capacités et de performances lors de l'activité de migration.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations fournies dans ce document, visitez nos sites web :

- Documentation VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Documentation Amazon FSX pour NetApp ONTAP

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  Guide de l'utilisateur VMware HCX

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Disponibilité de région : datastore NFS supplémentaire pour VMC

En savoir plus sur la prise en charge par région pour AWS, VMC et FSX ONTAP.

Le datastore NFS sera disponible dans les régions où les deux services (VMC et FSX ONTAP) sont disponibles.

La disponibilité des datastores NFS supplémentaires sur AWS/VMC est définie par Amazon. Tout d'abord, vous devez déterminer si VMC et FSxN sont disponibles dans une région spécifique. Ensuite, vous devez déterminer si le datastore NFS supplémentaire FSxN est pris en charge dans cette région.

- Vérifier la disponibilité du VMC "ici".
- Le guide des tarifs d'Amazon fournit des informations sur les domaines où FSxN (FSX ONTAP) est disponible. Vous trouverez cette information "ici".
- La disponibilité du datastore NFS supplémentaire FSxN pour VMC sera bientôt disponible.

Bien que les informations soient encore publiées, le tableau suivant identifie la prise en charge actuelle de VMC, FSxN et FSxN comme datastore NFS supplémentaire.

Amériques

Région AWS	Disponibilité VMC	Disponibilité ONTAP FSX	Disponibilité des datastores NFS
EST DES ÉTATS-UNIS (Virginie du Nord)	Oui.	Oui.	Oui.
États-Unis Est (Ohio)	Oui.	Oui.	Oui.
USA Ouest (Californie du Nord)	Oui.	Non	Non
US West (Oregon)	Oui.	Oui.	Oui.
GovCloud (USA West)	Oui.	Oui.	Oui.
Canada (Centre)	Oui.	Oui.	Oui.
Amérique du Sud (São Paulo)	Oui.	Oui.	Oui.

Dernière mise à jour : 2 juin 2022.

EMEA

Région AWS	Disponibilité VMC	Disponibilité ONTAP FSX	Disponibilité des datastores NFS
Europe (Irlande)	Oui.	Oui.	Oui.
Europe (Londres)	Oui.	Oui.	Oui.
Europe (Francfort)	Oui.	Oui.	Oui.
Europe (Paris)	Oui.	Oui.	Oui.
Europe (Milan)	Oui.	Oui.	Oui.
Europe (Stockholm)	Oui.	Oui.	Oui.

Dernière mise à jour : 2 juin 2022.

Asie Pacifique

Région AWS	Disponibilité VMC	Disponibilité ONTAP FSX	Disponibilité des datastores NFS
Asie-Pacifique (Sydney)	Oui.	Oui.	Oui.
Asie-Pacifique (Tokyo)	Oui.	Oui.	Oui.
Asie-Pacifique (Osaka)	Oui.	Non	Non
Asie-Pacifique (Singapour)	Oui.	Oui.	Oui.
Asie-Pacifique (Séoul)	Oui.	Oui.	Oui.
Asie-Pacifique (Mumbai)	Oui.	Oui.	Oui.
Asie-Pacifique (Jakarta)	Non	Non	Non

Asie-Pacifique (Hong Kong)	Oui.	Oui.	Oui.

Dernière mise à jour : 28 septembre 2022.

Informations sur le copyright

Informations sur les marques commerciales