Cloud public et cloud hybride

NetApp Solutions

NetApp
May 10, 2024

Sommaire

Cloud public et cloud hybride

Multicloud hybride NetApp avec les solutions VMware

VMware pour le cloud public

Présentation du multicloud hybride NetApp avec VMware

La plupart des départements IT adoptent une approche axée sur le cloud hybride. Ces entreprises sont en phase de transformation. Les clients évaluent leur environnement IT actuel, puis migrent leurs charges de travail vers le cloud à partir de l'évaluation et de l'exercice de découverte.

Les clients qui migrent vers le cloud peuvent inclure l'élasticité et les pics d'utilisation, la sortie du data Center, la consolidation du data Center, des scénarios de fin de vie, des fusions, des acquisitions, etc. La raison de cette migration peut varier en fonction de chaque entreprise et de leurs priorités business. Lors de la migration vers le cloud hybride, il est primordial de choisir le bon stockage dans le cloud pour bénéficier de la puissance du déploiement et de l'élasticité du cloud.

Options clouds VMware dans le cloud public

Cette section décrit comment chaque fournisseur de cloud prend en charge une pile de data Center Software-defined VMware (SDDC) et/ou VMware Cloud Foundation (VCF) dans ses offres de cloud public respectives.

Solution Azure VMware

Azure VMware solution est un service de cloud hybride qui permet d'assurer un fonctionnement optimal des SDDC VMware dans le cloud public Microsoft Azure. Azure VMware solution est une solution première entièrement gérée et prise en charge par Microsoft, vérifiée par VMware exploitant l'infrastructure Azure. Cela signifie qu'lors du déploiement de la solution Azure VMware, les clients bénéficient de VMware ESXi pour la virtualisation du calcul, de VSAN pour le stockage hyper-convergé, Enfin, NSX pour la mise en réseau et la sécurité, tout en exploitant la présence mondiale de Microsoft Azure, d'installations de data Center de premier plan et à proximité de notre riche écosystème de services et de solutions Azure natifs.

VMware Cloud sur AWS

VMware Cloud sur AWS permet au logiciel SDDC de VMware d'entreprise d'accéder au cloud AWS grâce à un accès optimisé aux services AWS natifs. Optimisée par VMware Cloud Foundation, VMware Cloud sur AWS intègre les produits de virtualisation du réseau, du stockage et de calcul de VMware (VMware vSphere, VMware VSAN et VMware NSX), ainsi que la solution de gestion de VMware vCenter Server, optimisée pour s'exécuter sur une infrastructure AWS dédiée, flexible et sans système d'exploitation.

Moteur VMware Google Cloud

Google Cloud VMware Engine est une offre d'infrastructure en tant que service (IaaS) basée sur l'infrastructure évolutive haute performance de Google Cloud et sur la pile VMware Cloud Foundation : VMware vSphere, vCenter, VSAN et NSX-T. Ce service permet une migration rapide vers le cloud, et ceci de migrer ou d'étendre les charges de travail VMware existantes d'un environnement sur site à Google Cloud Platform sans le coût, les efforts ou le risque de modifier l'architecture des applications ou d'exploiter de nouveau les opérations. Il s'agit d'un service vendu et pris en charge par Google, en étroite collaboration avec VMware.

Un cloud privé SDDC et la colocation NetApp Cloud volumes offrent les meilleures performances avec une latence réseau minimale.

Le saviez-vous ?

Quel que soit le cloud utilisé lorsqu'un SDDC VMware est déployé, le cluster initial inclut les produits suivants :

- Hôtes VMware ESXi pour la virtualisation du calcul avec une appliance vCenter Server à gérer
- Stockage hyper-convergé VMware VSAN incluant les ressources de stockage physique de chaque hôte ESXi
- VMware NSX pour la mise en réseau virtuelle et la sécurité avec un cluster NSX Manager à des fins de gestion

Configuration de stockage sous-jacente

Pour les clients qui prévoient d'héberger des charges de travail exigeantes en stockage et de faire évoluer horizontalement sur n'importe quelle solution VMware hébergée dans le cloud, l'infrastructure hyperconvergée par défaut impose que l'extension soit sur les ressources de calcul et de stockage.

En s'intégrant avec NetApp Cloud volumes, comme Azure NetApp Files, Amazon FSX pour NetApp ONTAP, Cloud Volumes ONTAP (disponible dans les trois principaux hyperscalers) et Cloud Volumes Service pour Google Cloud, les clients peuvent désormais faire évoluer leur stockage séparément Il suffit d'ajouter des nœuds de calcul au cluster SDDC selon les besoins.

Remarques :

- VMware ne recommande pas de configurations de cluster non équilibrées. L'extension du stockage entraîne donc un ajout d'hôtes, ce qui implique un coût total de possession plus élevé.
- Un seul environnement VSAN est possible. Par conséquent, tout le trafic de stockage sera directement en concurrence avec les workloads de production.
- Il n'est pas possible de fournir plusieurs tiers de performance pour répondre aux exigences des applications, aux performances et aux coûts.
- Il est très facile d'atteindre les limites de capacité de stockage de VSAN basées sur le cluster hôtes. Utilisez NetApp Cloud volumes pour faire évoluer le stockage soit pour héberger des datasets actifs, soit pour hiérarchiser les données inactives dans un stockage persistant.

Azure NetApp Files, Amazon FSX pour NetApp ONTAP, Cloud Volumes ONTAP (disponible dans les trois principaux hyperscalers) et Cloud Volumes Service pour Google Cloud peuvent être associés à des VM invités. Cette architecture de stockage hybride est composée d'un datastore VSAN qui contient le système

d'exploitation invité et les données binaires des applications. Les données d'application sont reliées à la machine virtuelle via un initiateur iSCSI basé sur l'invité ou des montages NFS/SMB qui communiquent directement avec Amazon FSX pour NetApp ONTAP, Cloud Volume ONTAP, Azure NetApp Files et Cloud Volumes Service pour Google Cloud respectivement. Cette configuration vous permet de relever facilement les défis en matière de capacité de stockage. Comme avec VSAN, l'espace libre disponible dépend de l'espace Slack et des règles de stockage utilisées.

Considérons un cluster SDDC à trois nœuds sous VMware Cloud sur AWS :

- La capacité brute totale d'un SDDC à trois nœuds = 31 To (environ 10 To pour chaque nœud).
- L'espace Slack à conserver avant d'ajouter des hôtes supplémentaires = 25 % = (.25 x 31,1 To) = 7,7 To.
- La capacité brute utilisable après la perte d'espace Slack = 23.4 To
- L'espace disponible effectif dépend de la stratégie de stockage appliquée.

  Par exemple :

  - RAID 0 = espace libre effectif = 23,4 To (capacité brute utilisable/1)
  - RAID 1 = espace libre effectif = 11,7 To (capacité brute utilisable/2)
  - RAID 5 = espace libre effectif = 17,5 To (capacité brute utilisable/1.33)

Ainsi, l'utilisation de NetApp Cloud volumes en tant que stockage connecté à l'invité permettrait d'étendre le stockage et d'optimiser le TCO tout en répondant aux exigences de performances et de protection des données.

Le stockage invité était la seule option disponible au moment de l'écriture de ce document. Une documentation supplémentaire sera disponible lors de la prise en charge des datastores NFS "ici".

Points à retenir

- Dans les modèles de stockage hybride, placez des workloads de Tier 1 ou hautement prioritaires sur le datastore VSAN pour répondre aux exigences de latence spécifiques, car ils font partie de l'hôte lui-même et à proximité. Utilisation de mécanismes In-Guest pour les machines virtuelles de charges de travail pour lesquelles les latences transactionnelles sont acceptables
- Utilisez la technologie NetApp SnapMirror® pour répliquer les données des workloads depuis le système ONTAP sur site vers Cloud Volumes ONTAP ou Amazon FSX pour NetApp ONTAP afin de faciliter la migration à l'aide de mécanismes de niveau bloc. Cela ne s'applique pas aux services Azure NetApp Files et Cloud volumes. Pour la migration des données vers Azure NetApp Files ou Cloud volumes Services, utilisez NetApp XCP, BlueXP Copy and Sync, rysnc ou robocopy, en fonction du protocole de fichier utilisé.
- Les tests montrent une latence supplémentaire de 2 à 4 ms lors de l'accès au stockage à partir des data centers SDDC respectifs. Tenez compte de cette latence supplémentaire dans les exigences des applications lors du mappage du stockage.
- Pour le montage du stockage connecté à l'invité pendant le basculement test et le basculement réel, assurez-vous que les initiateurs iSCSI sont reconfigurés, que le DNS est mis à jour pour les partages SMB et que les points de montage NFS sont mis à jour dans fstab.
- Assurez-vous que les paramètres du registre d'expiration des disques (MPIO), de pare-feu et de chemins d'accès E/S multiples (Multipath I/O) intégré à l'invité sont correctement configurés à l'intérieur de la machine virtuelle.

Ceci s'applique uniquement au stockage connecté à l'invité.

Avantages du stockage cloud NetApp

Le stockage cloud NetApp offre plusieurs avantages :

- Améliore la densité de calcul à stockage en faisant évoluer le stockage indépendamment de la puissance de calcul.
- Permet de réduire le nombre d'hôtes, ce qui réduit le coût total de possession global.
- La défaillance du nœud de calcul n'a aucune incidence sur les performances du stockage.
- La réorganisation des volumes et la fonctionnalité de niveau de service dynamique d'Azure NetApp Files permettent d'optimiser les coûts par le dimensionnement des charges de travail prévisibles, tout en empêchant le surprovisionnement.
- L'efficacité du stockage, le Tiering cloud et les fonctionnalités de modification du type d'instance de Cloud Volumes ONTAP offrent des moyens optimaux d'ajouter et de faire évoluer le stockage.
- Les capacités de surprovisionnement ne sont ajoutées qu'en cas de besoin.
- Des copies et des clones efficaces Snapshot vous permettent de créer rapidement des copies sans affecter les performances.
- Aide à contrer les attaques par ransomware grâce à la restauration rapide à partir de copies Snapshot.
- Assure une reprise après incident régionale et un niveau de bloc de sauvegarde intégré efficaces par transfert de blocs entre les régions pour un meilleur RPO et RTO.

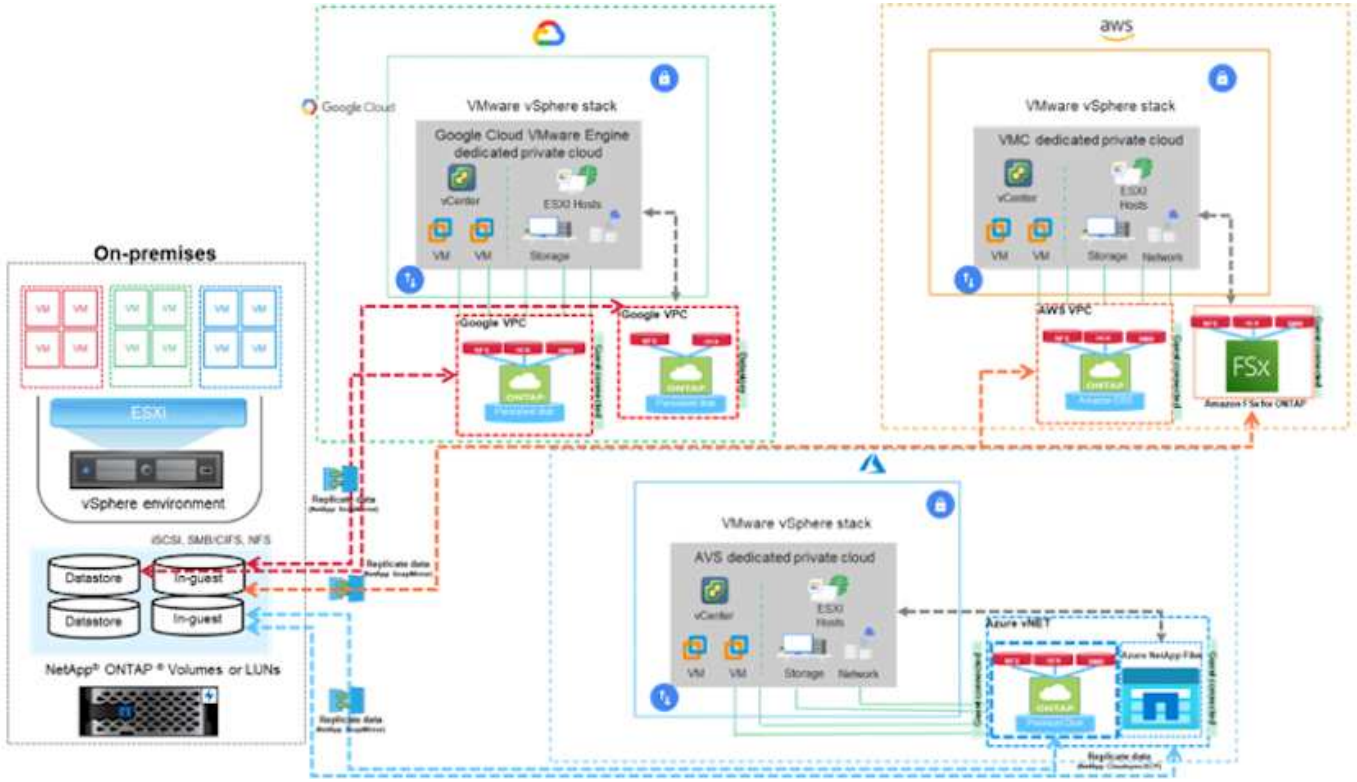
Hypothèses

- La technologie SnapMirror ou d'autres mécanismes pertinents de migration des données sont activés. De nombreuses options de connectivité sont disponibles, sur site comme dans tout cloud hyperscale. Utilisez le parcours approprié et collaborez avec les équipes de mise en réseau concernées.
- Le stockage invité était la seule option disponible au moment de l'écriture de ce document. Une documentation supplémentaire sera disponible lors de la prise en charge des datastores NFS "ici".

> Faites appel aux architectes de solutions NetApp et aux architectes de cloud hyperscale pour planifier et dimensionner le stockage et le nombre d'hôtes requis. NetApp recommande d'identifier les exigences en matière de performances de stockage avant d'utiliser le dimensionnement Cloud Volumes ONTAP pour finaliser le type d'instance de stockage ou le niveau de service approprié avec le débit adéquat.

Architecture détaillée

Sur un plan général, cette architecture (illustrée dans la figure ci-dessous) explique comment bénéficier d'une connectivité multicloud hybride et de la portabilité des applications entre plusieurs fournisseurs de cloud utilisant NetApp Cloud Volumes ONTAP, Cloud Volumes Service pour Google Cloud et Azure NetApp Files comme option de stockage invité supplémentaire.



Solutions NetApp pour les fournisseurs de cloud hyperscale

Découvrez les fonctionnalités que NetApp propose aux trois (3) principaux hyperscalers : qu'il s'agisse d'un système de stockage connecté à l'invité ou d'un datastore NFS supplémentaire pour migrer les flux de travail, étendre/bursting sur le cloud, la sauvegarde/restauration et la reprise après incident.

Choisissez votre cloud et laissez NetApp faire le reste !

Pour afficher les fonctionnalités d'un hyperscaler, cliquez sur l'onglet approprié.

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

- "VMware dans la configuration des hyperscalers"
- "Options de stockage NetApp"

- "Solutions clouds NetApp/VMware"

VMware dans la configuration des hyperscalers

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.

AWS/VMC

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".

Azure/AVS

Cette section décrit comment configurer et gérer Azure VMware solution et l'utiliser en association avec les options disponibles pour connecter le stockage NetApp.

> Le stockage In-guest est la seule méthode prise en charge de connexion de Cloud Volumes ONTAP à Azure VMware solution.

Le processus de configuration peut être divisé en plusieurs étapes :

- Enregistrez le fournisseur de ressources et créez un cloud privé
- Connectez-vous à une passerelle réseau virtuelle ExpressRoute nouvelle ou existante
- Validation de la connectivité réseau et accès au cloud privé

Afficher les détails "Étapes de configuration de AVS".

GCP/GCVE

Cette section décrit comment configurer et gérer GCVE et l'utiliser en association avec les options disponibles pour la connexion du stockage NetApp.

> Le stockage « en invité » est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP et Cloud volumes Services à GCVE.

Le processus de configuration peut être divisé en plusieurs étapes :

- Déployer et configurer GCVE
- Activez l'accès privé à GCVE

Afficher les détails "Étapes de configuration pour GCVE".

Options de stockage NetApp

Le stockage NetApp peut être utilisé de plusieurs façons, en tant que datastore NFS supplémentaire ou connecté par un invité, dans chacun des 3 principaux hyperscalers.

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

AWS/VMC

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".

Azure/AVS

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

- Azure NetApp Files (ANF) comme stockage connecté invité
- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- Azure NetApp Files (ANF) comme datastore NFS supplémentaire

Afficher les détails "Option de stockage avec connexion invité pour AVS". Afficher les détails "Options supplémentaires de datastore NFS pour AVS".

GCP/GCVE

Google Cloud prend en charge le stockage NetApp dans les configurations suivantes :

- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- Cloud Volumes Service (CVS) comme stockage connecté invité
- Cloud Volumes Service (CVS) comme datastore NFS supplémentaire

Afficher les détails "Options de stockage de connexion invité pour GCVE".

En savoir plus sur "Prise en charge du datastore NetApp Cloud Volumes Service pour Google Cloud VMware Engine (blog NetApp)" ou "Comment utiliser NetApp CVS en tant que datastores pour Google Cloud VMware Engine (blog Google)"

Solutions clouds NetApp/VMware

Avec les solutions cloud NetApp et VMware, vous pouvez facilement déployer dans l'hyperscaler de votre choix. VMware définit les principales utilisations des workloads cloud comme suit :

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

AWS/VMC

"Découvrez les solutions NetApp pour AWS/VMC"

Azure/AVS

"Découvrez les solutions NetApp pour Azure/AVS"

GCP/GCVE

"Découvrez les solutions NetApp pour Google Cloud Platform (GCP) / GCVE"

Configurations prises en charge pour l'environnement multicloud hybride NetApp avec VMware

Comprendre les combinaisons de la prise en charge du stockage NetApp dans les principaux hyperscalers.

	Invité connecté	Datastore NFS supplémentaire
AWS	ONTAP CVO FSX"Détails"	ONTAP FSX"Détails"
Azure	ANF CVO"Détails"	ANF"Détails"
GCP	CVS DE CVO"Détails"	CVS"Détails"

Configuration de l'environnement de virtualisation dans le fournisseur cloud

Vous trouverez plus d'informations sur la configuration de l'environnement de virtualisation dans chacun des hyperscalers pris en charge.

AWS/VMC

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".

Azure/AVS

Cette section décrit comment configurer et gérer Azure VMware solution et l'utiliser en association avec les options disponibles pour connecter le stockage NetApp.

Le stockage In-guest est la seule méthode prise en charge de connexion de Cloud Volumes ONTAP à Azure VMware solution.

Le processus de configuration peut être divisé en plusieurs étapes :

- Enregistrez le fournisseur de ressources et créez un cloud privé
- Connectez-vous à une passerelle réseau virtuelle ExpressRoute nouvelle ou existante
- Validation de la connectivité réseau et accès au cloud privé

Afficher les détails "Étapes de configuration de AVS".

GCP/GCVE

Cette section décrit comment configurer et gérer GCVE et l'utiliser en association avec les options disponibles pour la connexion du stockage NetApp.

Le stockage « en invité » est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP et Cloud volumes Services à GCVE.

Le processus de configuration peut être divisé en plusieurs étapes :

- Déployer et configurer GCVE
- Activez l'accès privé à GCVE

Afficher les détails "Étapes de configuration pour GCVE".

Déploiement et configuration de l'environnement de virtualisation sur AWS

Comme sur site, la planification de VMware Cloud sur AWS est cruciale pour la réussite d'un environnement prêt à la production à créer des machines virtuelles et à migrer.

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 actuellement la seule méthode prise en charge pour connecter Cloud Volumes ONTAP (CVO) à AWS VMC.

Le processus de configuration peut être divisé en plusieurs étapes :

Déploiement et configuration de VMware Cloud pour 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 à vos charges de travail.

Cette section décrit comment configurer et gérer VMware Cloud sur AWS et l'utiliser en association avec Amazon FSX pour NetApp ONTAP et/ou Cloud Volumes ONTAP sur AWS avec un système de stockage invité.

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

Le processus de configuration peut être divisé en trois parties :

Créez un compte AWS

S'inscrire pour obtenir un "Compte Amazon Web Services".

Vous avez besoin d'un compte AWS pour démarrer, à condition qu'il n'y en ait pas encore créé. Nouveau ou existant, vous avez besoin de privilèges d'administration dans le compte pour de nombreuses étapes de cette procédure. Voir ceci "lien" Pour plus d'informations sur les identifiants AWS.

Créez un compte My VMware

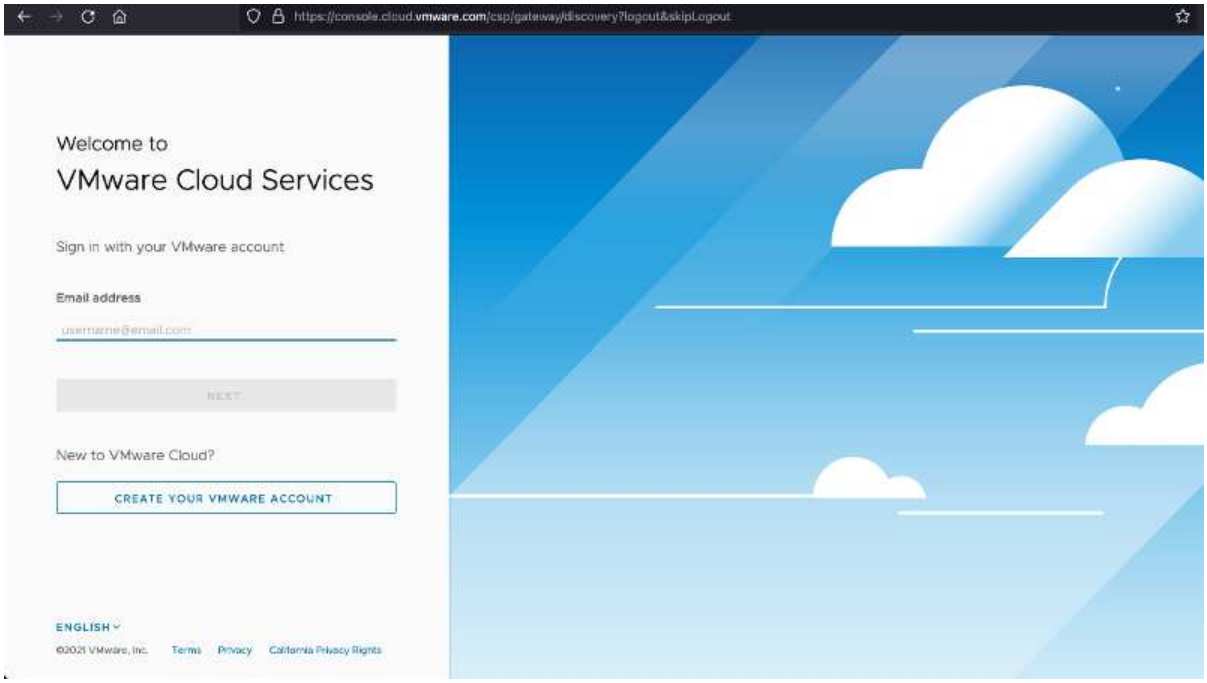
S'inscrire à un "Mon infrastructure VMware" compte.

Pour accéder au portefeuille cloud de VMware (y compris VMware Cloud sur AWS), vous avez besoin d'un compte client VMware ou d'un compte My VMware. Si ce n'est déjà fait, créez un compte VMware "ici".

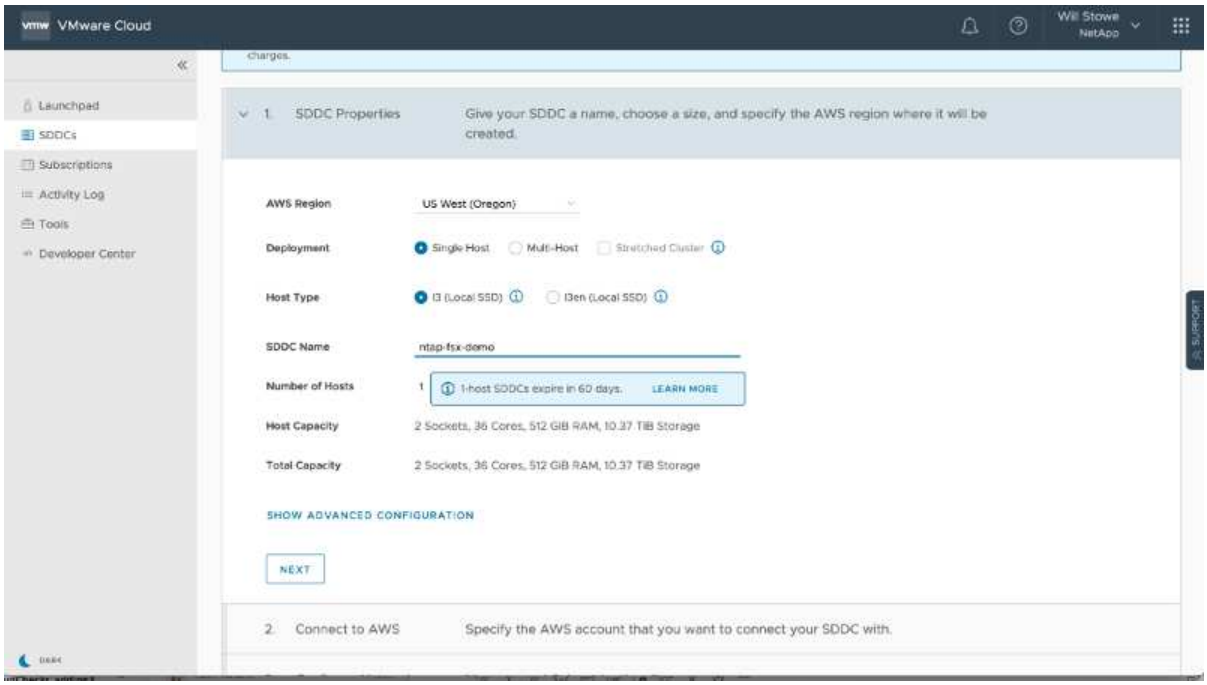
Provisionner le SDDC dans VMware Cloud

Une fois le compte VMware configuré et le dimensionnement approprié effectués, le déploiement d'un Software-Defined Data Center constitue l'étape suivante évidente pour l'utilisation du service VMware Cloud sur AWS. Pour créer un SDDC, choisissez une région AWS qui l'héberge, donnez un nom au SDDC et spécifiez le nombre d'hôtes ESXi que vous souhaitez que le SDDC contienne. Si vous ne possédez pas encore de compte AWS, vous pouvez toujours créer un SDDC de configuration de démarrage contenant un hôte ESXi unique.

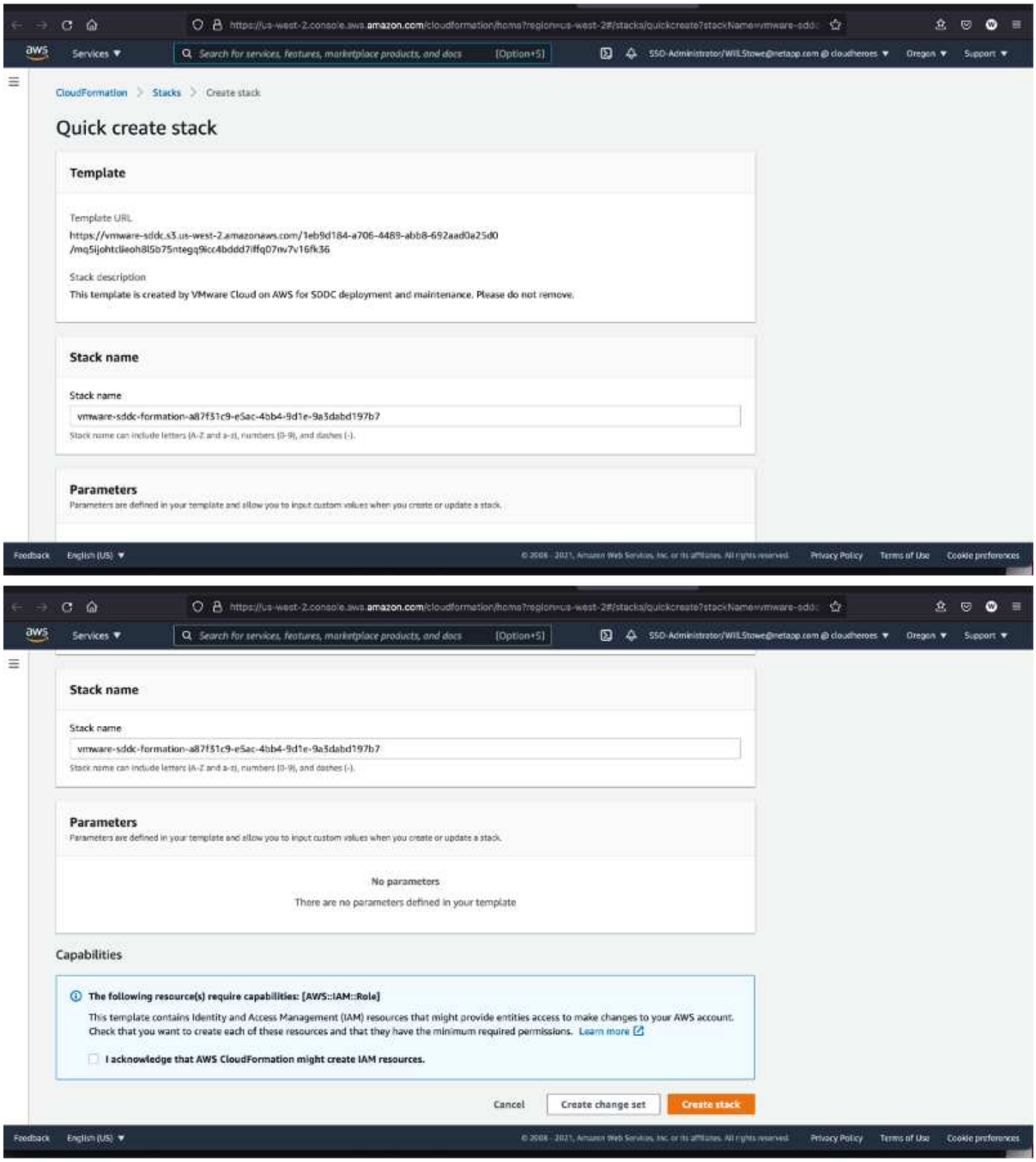
1. Connectez-vous à VMware Cloud Console à l'aide de vos informations d'identification VMware existantes ou nouvellement créées.

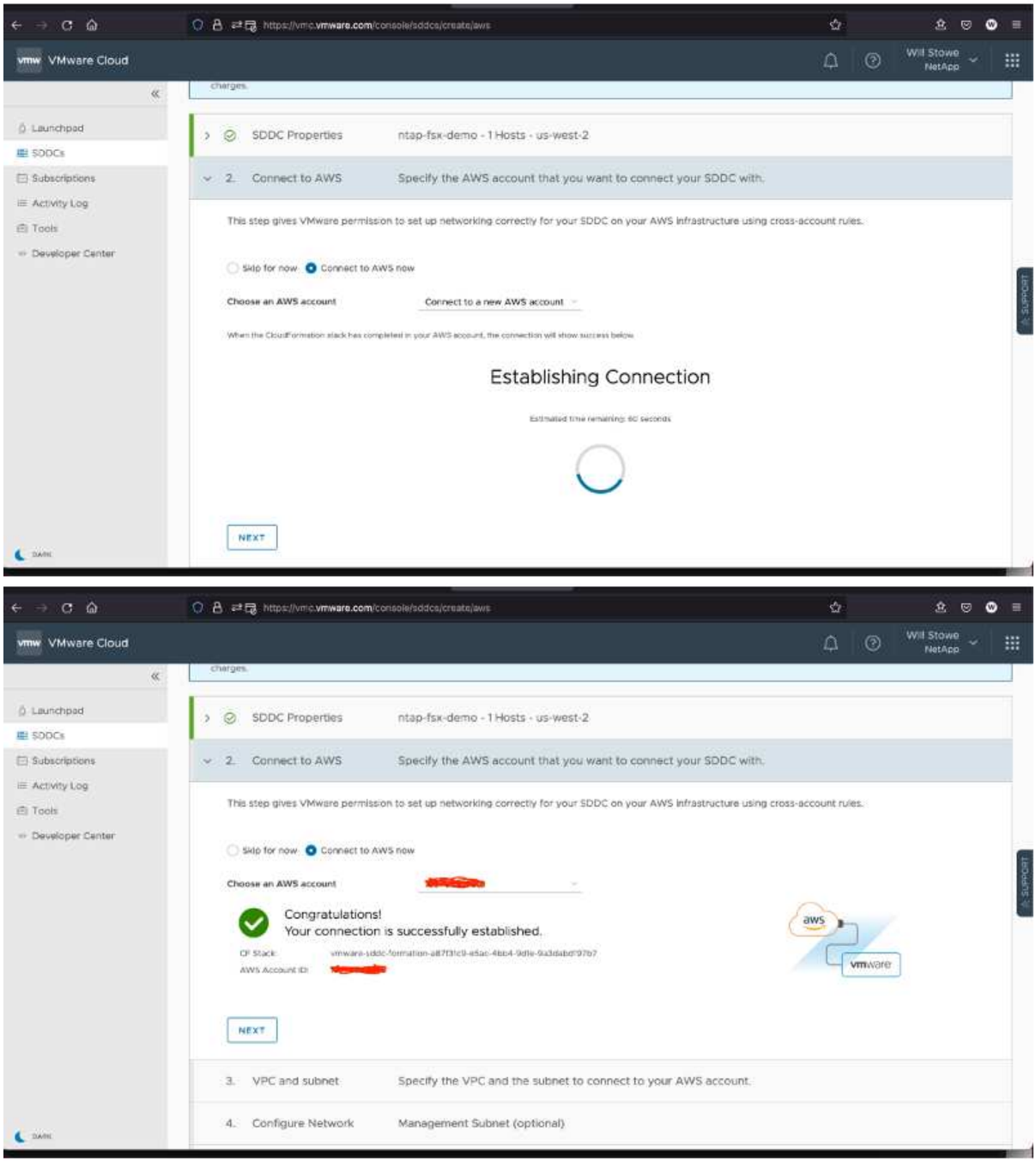


2. Configurer la région, le déploiement, le type d'hôte et le nom du SDDC :



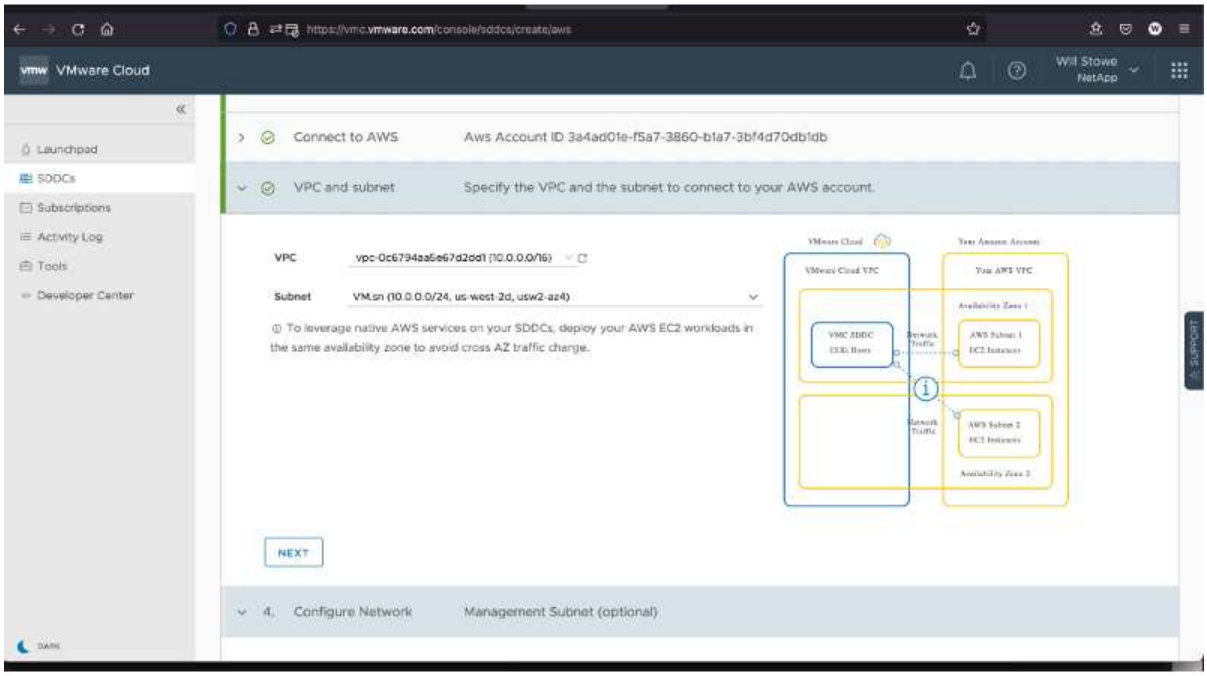
3. Vous connecter au compte AWS souhaité et exécuter la pile AWS Cloud formation.



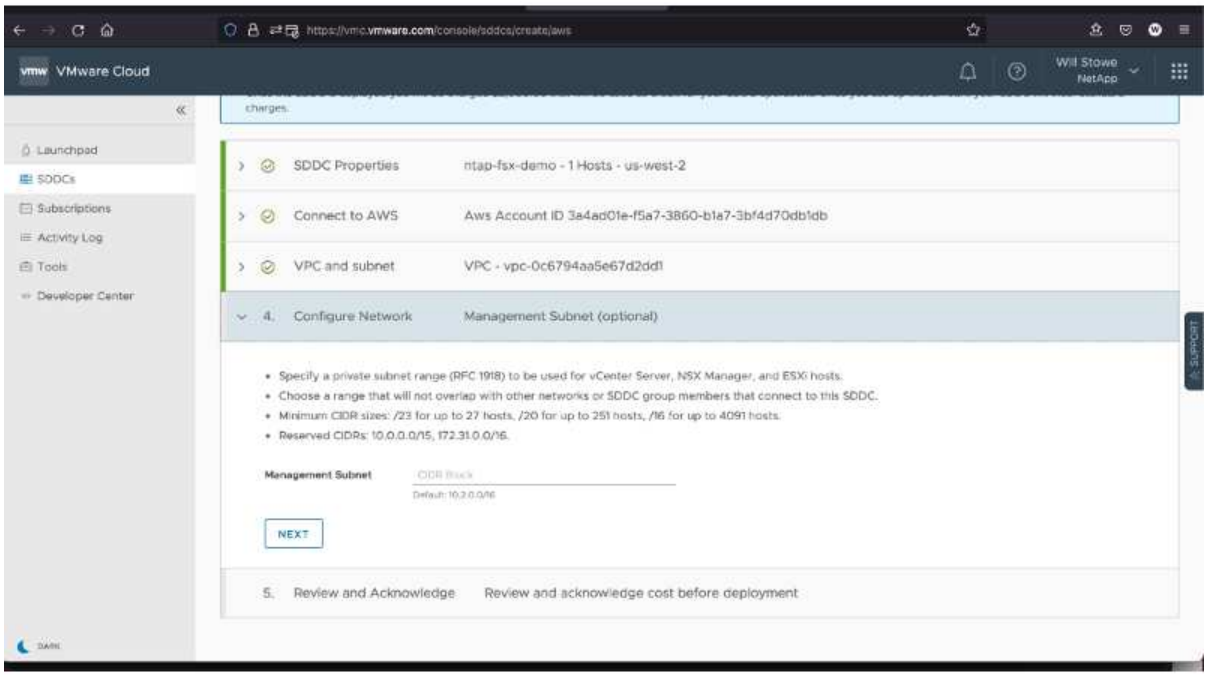


La configuration à hôte unique est utilisée dans cette validation.

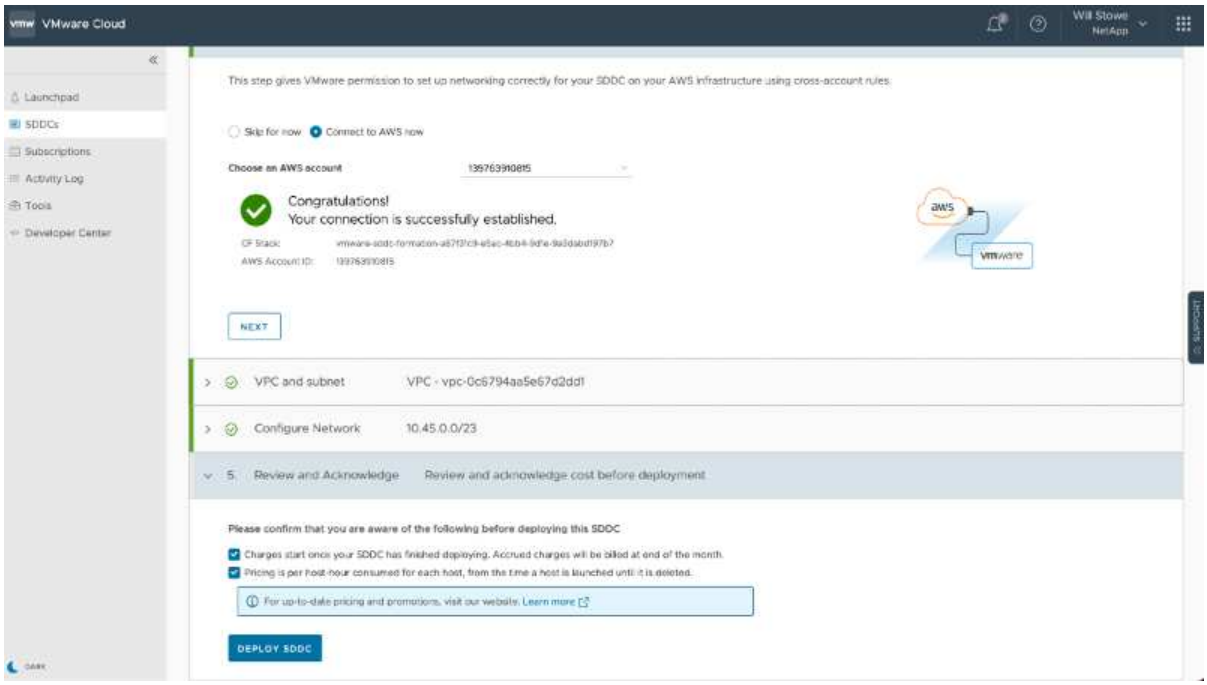
4. Sélectionnez le VPC AWS souhaité pour connecter l'environnement VMC à.



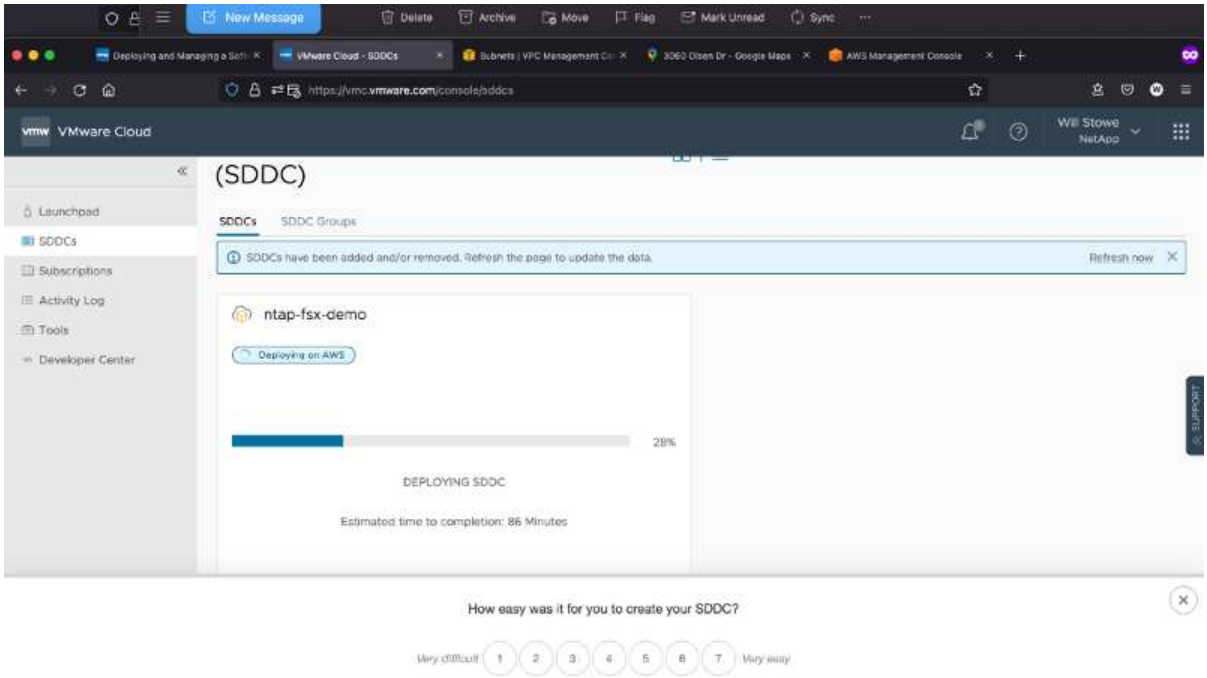
5. Configurez le sous-réseau de gestion VMC ; ce sous-réseau contient des services gérés par VMC tels que vCenter, NSX, etc. Ne choisissez pas un espace d'adressage qui se chevauchent avec les autres réseaux qui nécessitent une connexion à l'environnement SDDC. Enfin, suivez les recommandations relatives à la taille du CIDR indiquée ci-dessous.



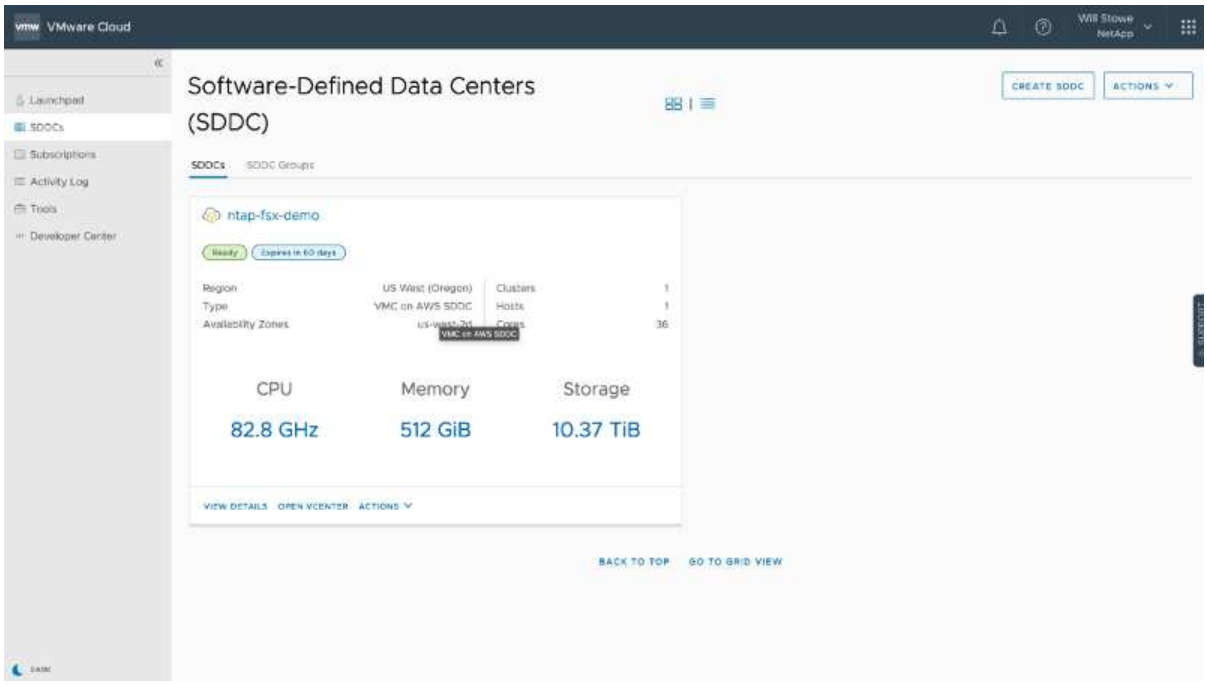
6. Examinez et acceptez la configuration SDDC, puis cliquez sur déployer le SDDC.



Le processus de déploiement prend généralement entre deux heures.



7. Une fois cette opération terminée, le SDDC est prêt à l'emploi.

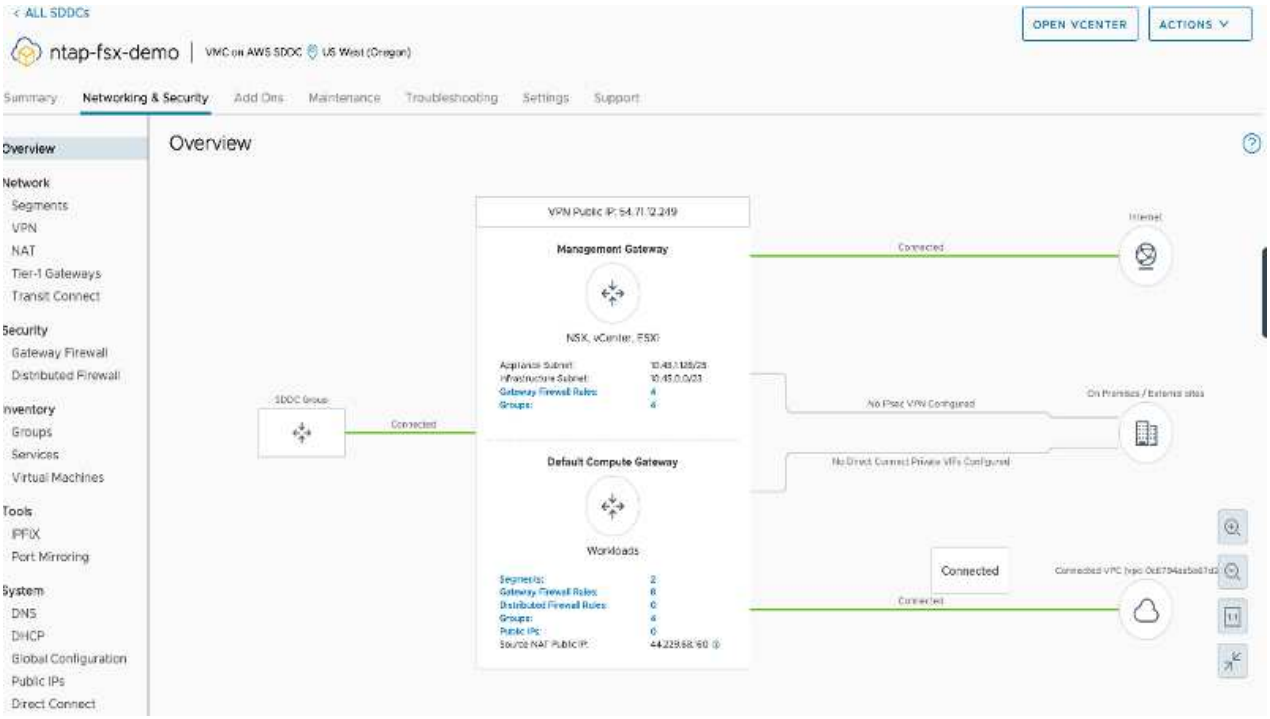


Pour un guide détaillé de déploiement d'un SDDC, consultez la section "Déployer un SDDC depuis la console VMC".

Connectez le cloud VMware à FSX ONTAP

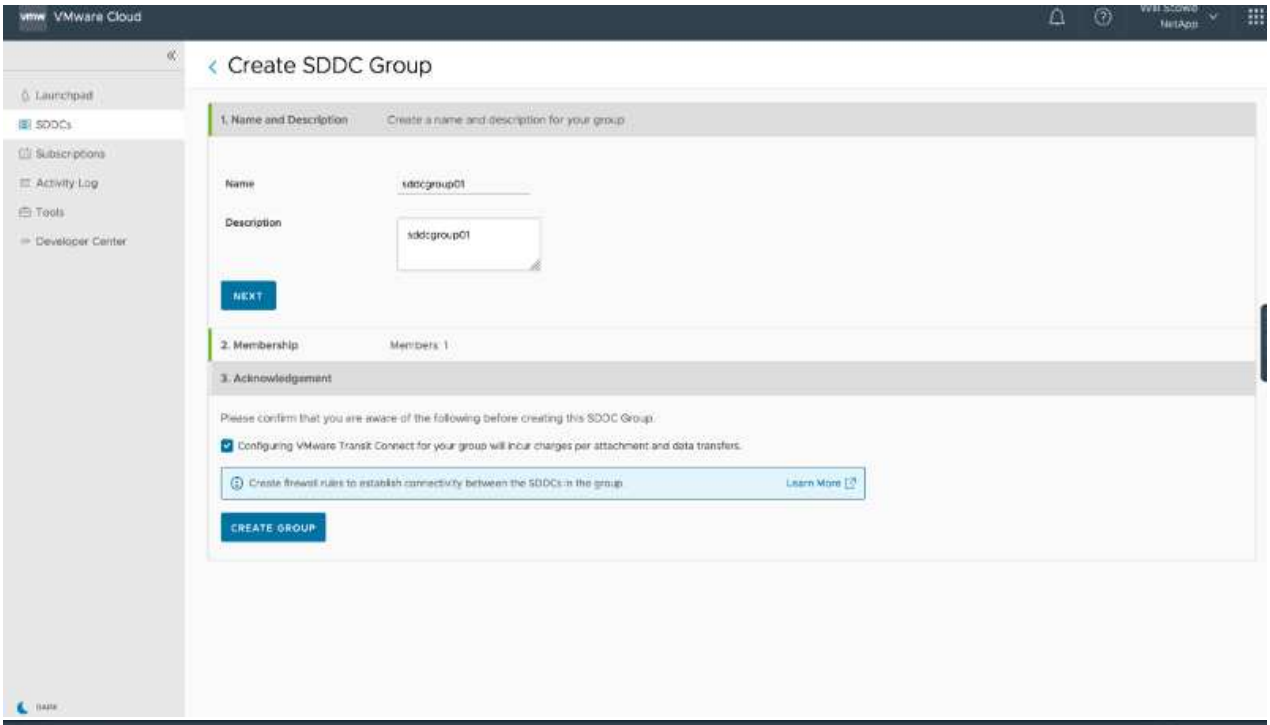
Pour connecter VMware Cloud à FSX ONTAP, procédez comme suit :

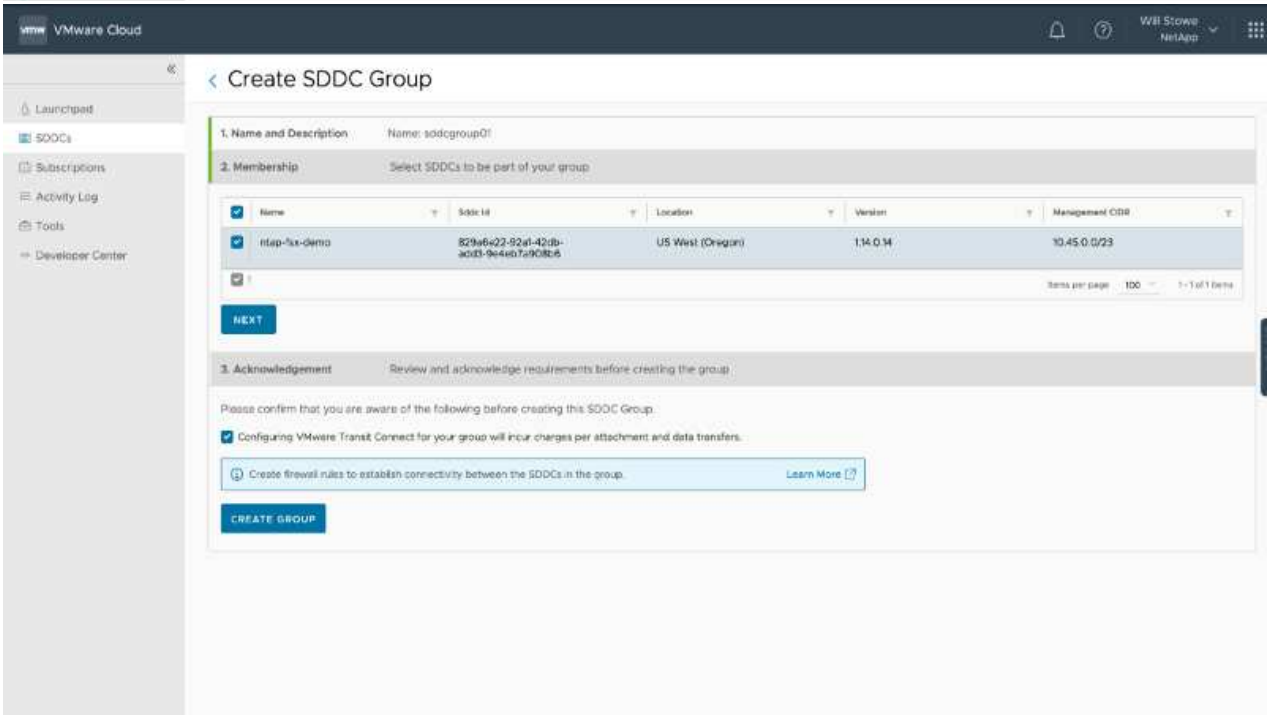
1. Une fois le déploiement de VMware Cloud terminé et connecté à AWS VPC, vous devez déployer Amazon FSX pour NetApp ONTAP dans un nouveau VPC plutôt que le VPC initial connecté (voir la capture d'écran ci-dessous). FSX (IP flottantes NFS et SMB) n'est pas accessible s'il est déployé sur le VPC connecté. Gardez à l'esprit que les terminaux ISCSI tels que Cloud Volumes ONTAP fonctionnent correctement du VPC connecté.

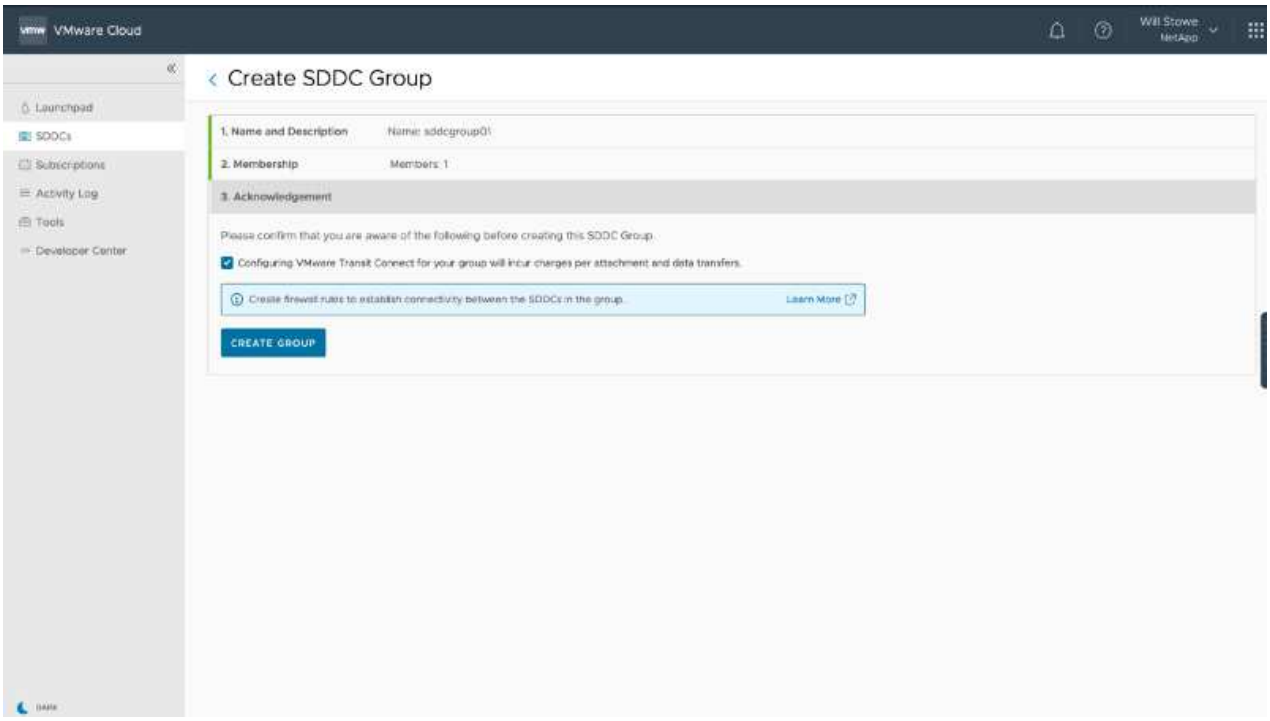


2. Déployez un VPC supplémentaire dans la même région, puis déployez Amazon FSX pour NetApp ONTAP dans le nouveau VPC.

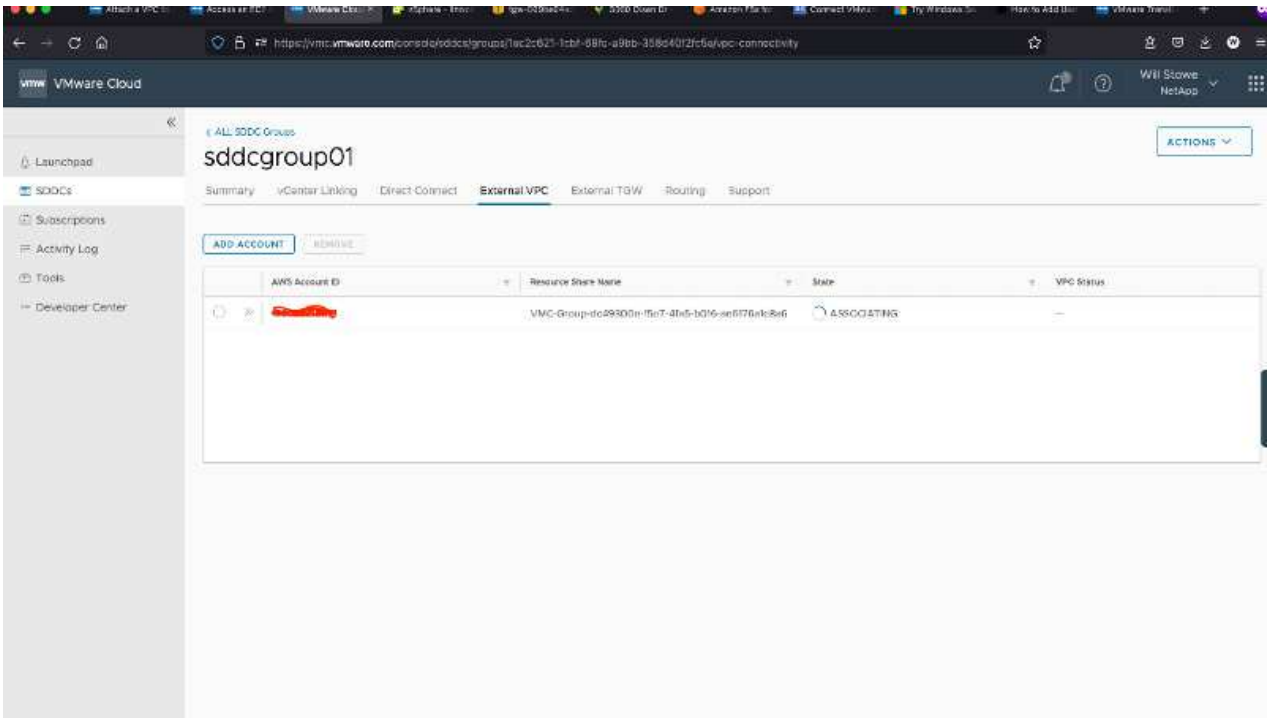
   La configuration d'un groupe SDDC dans la console VMware Cloud permet d'utiliser les options de configuration réseau requises pour se connecter au nouveau VPC où FSX est déployé. À l'étape 3, vérifiez que "la configuration de VMware Transit Connect pour votre groupe entraînera des frais par pièce jointe et transfert de données" est cochée, puis choisissez Créer un groupe. Ce processus peut prendre quelques minutes.

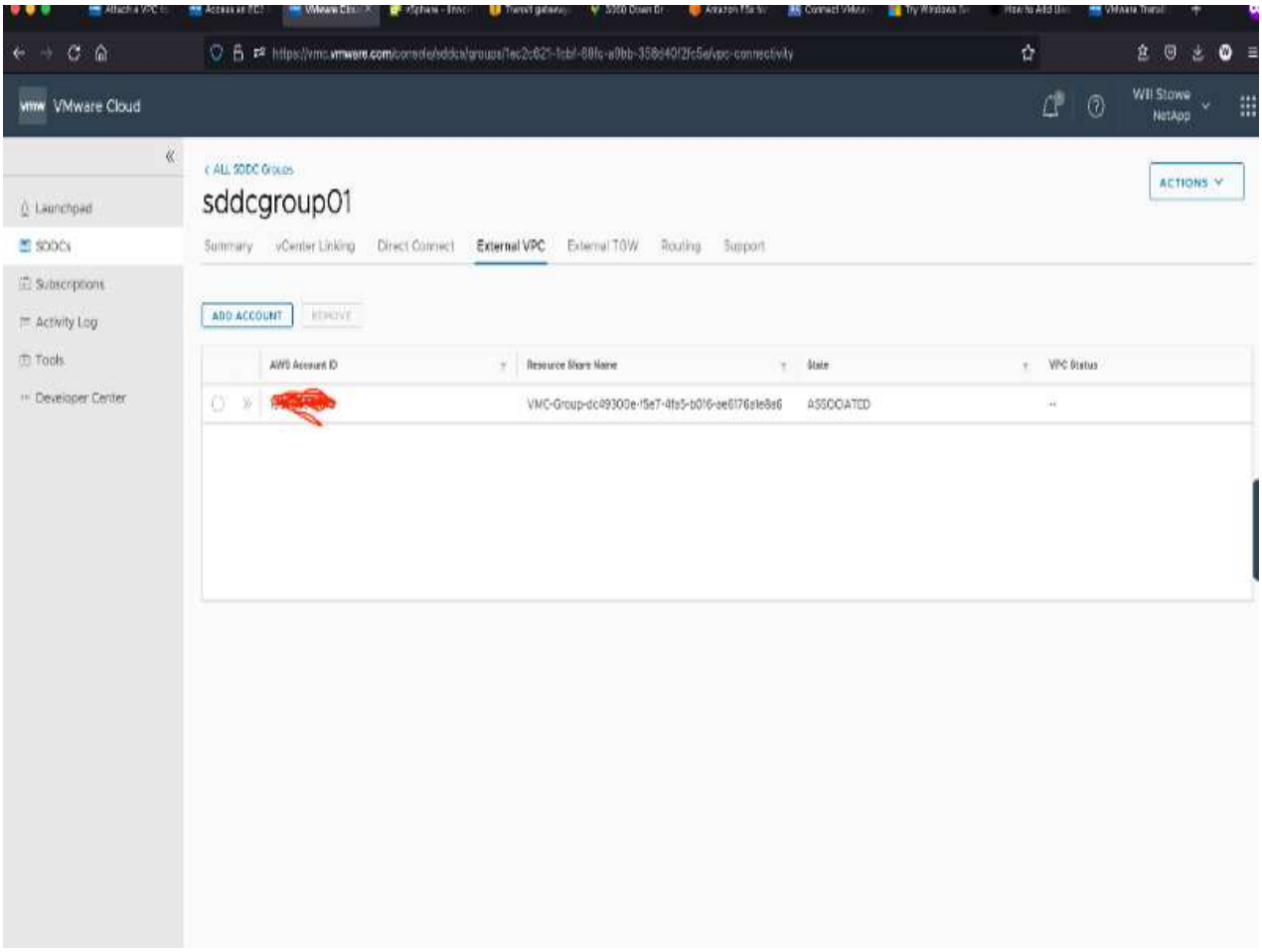

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-
acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

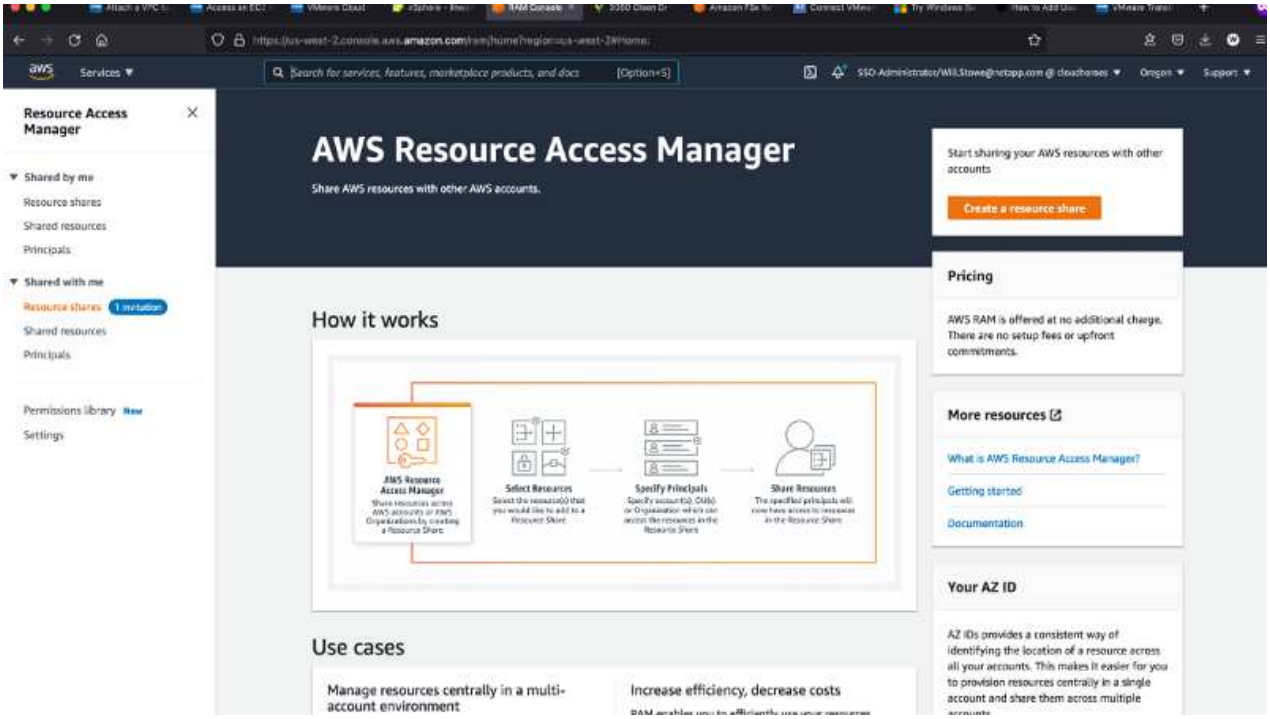


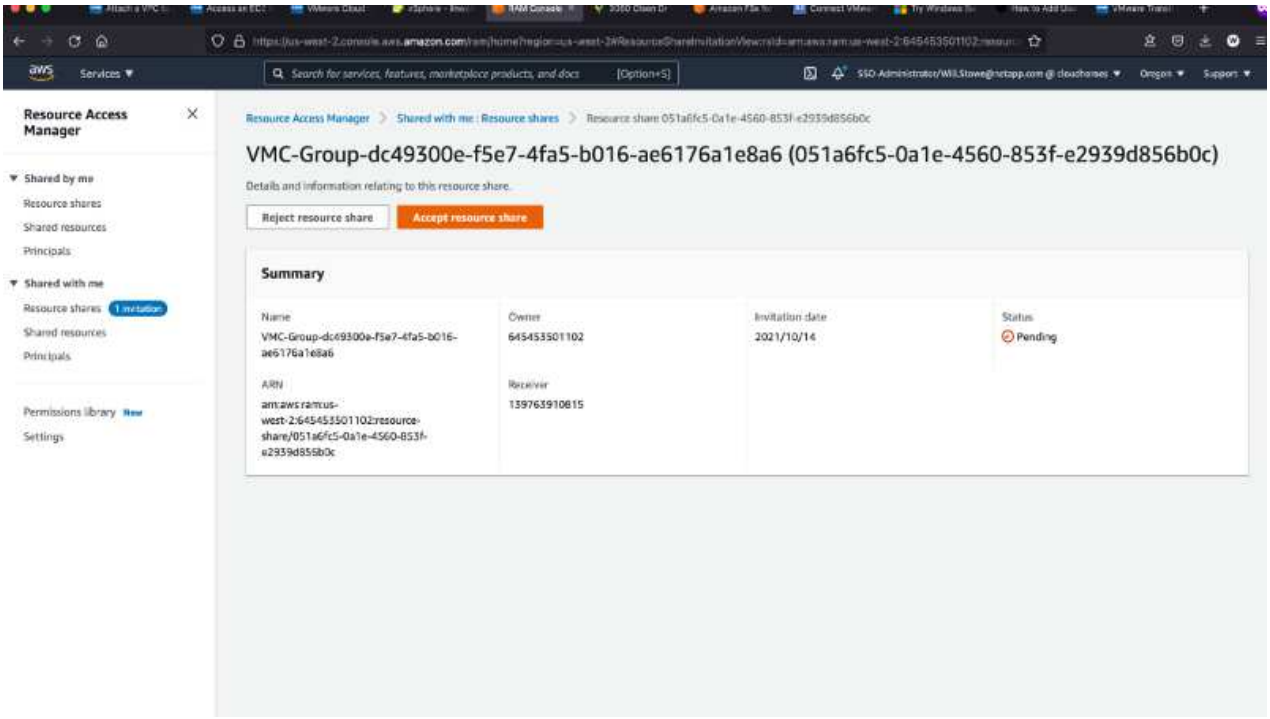
3. Reliez le nouveau VPC créé au groupe SDDC juste créé. Sélectionnez l'onglet VPC externe et suivez la "Instructions pour connecter un VPC externe" au groupe. Ce processus peut prendre entre 10 et 15 minutes.



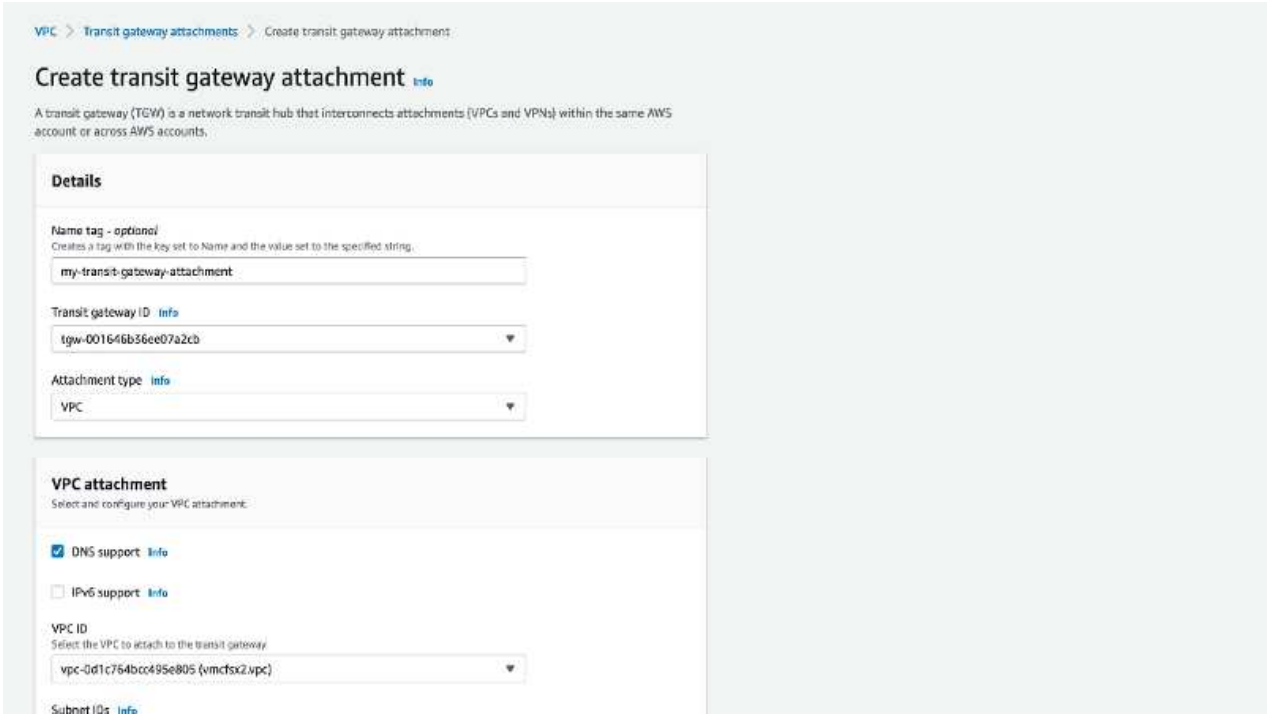


4. Dans le cadre du processus VPC externe, vous êtes invité par le biais de la console AWS à accéder à une nouvelle ressource partagée via Resource Access Manager. La ressource partagée est le "Passerelle AWS Transit" Géré par VMware Transit Connect.

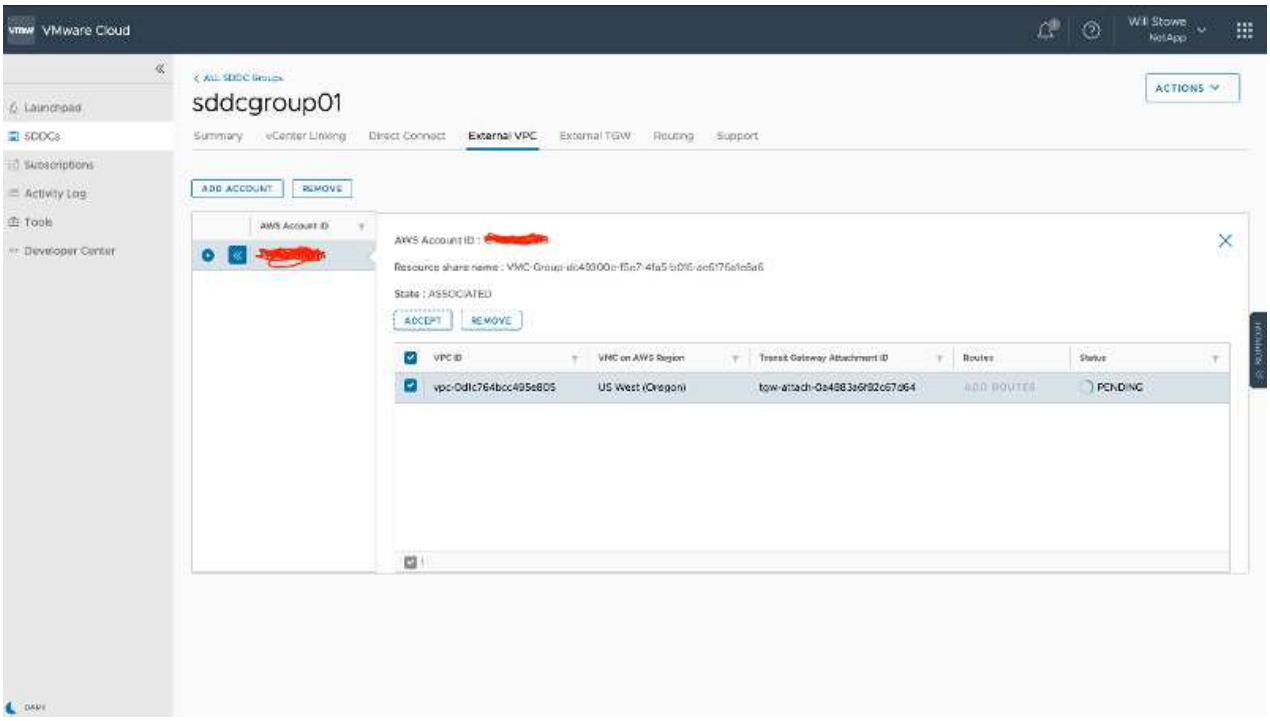




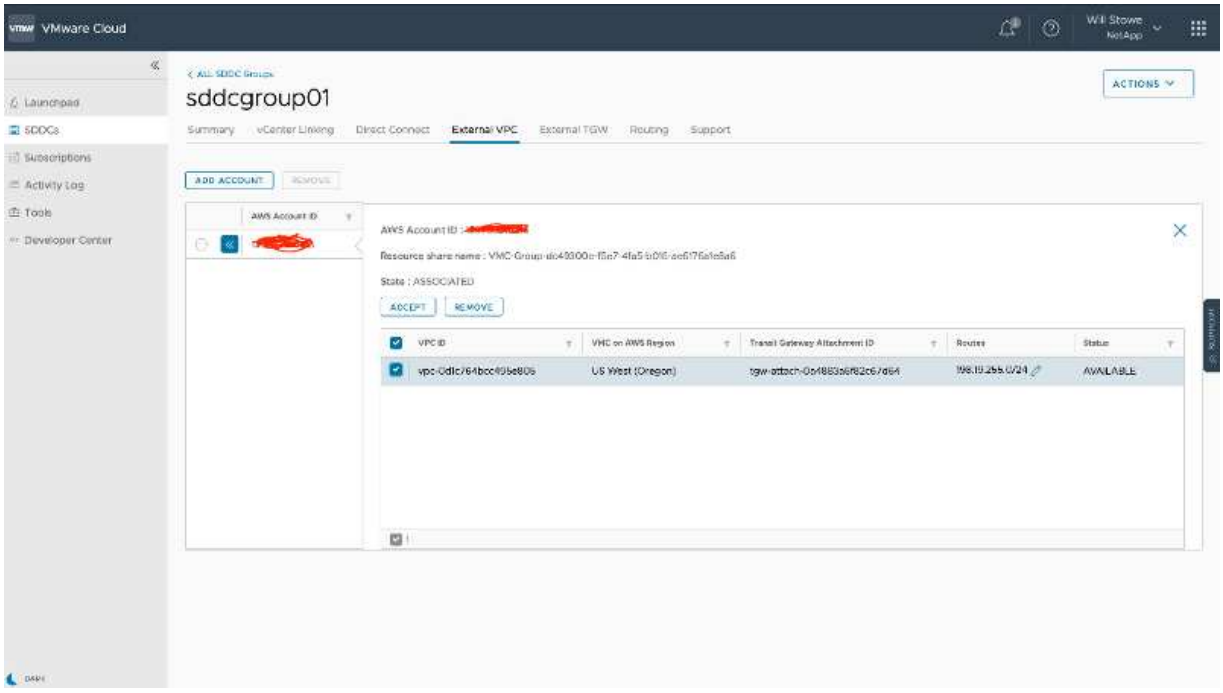
5. Créez la pièce jointe de la passerelle de transit.



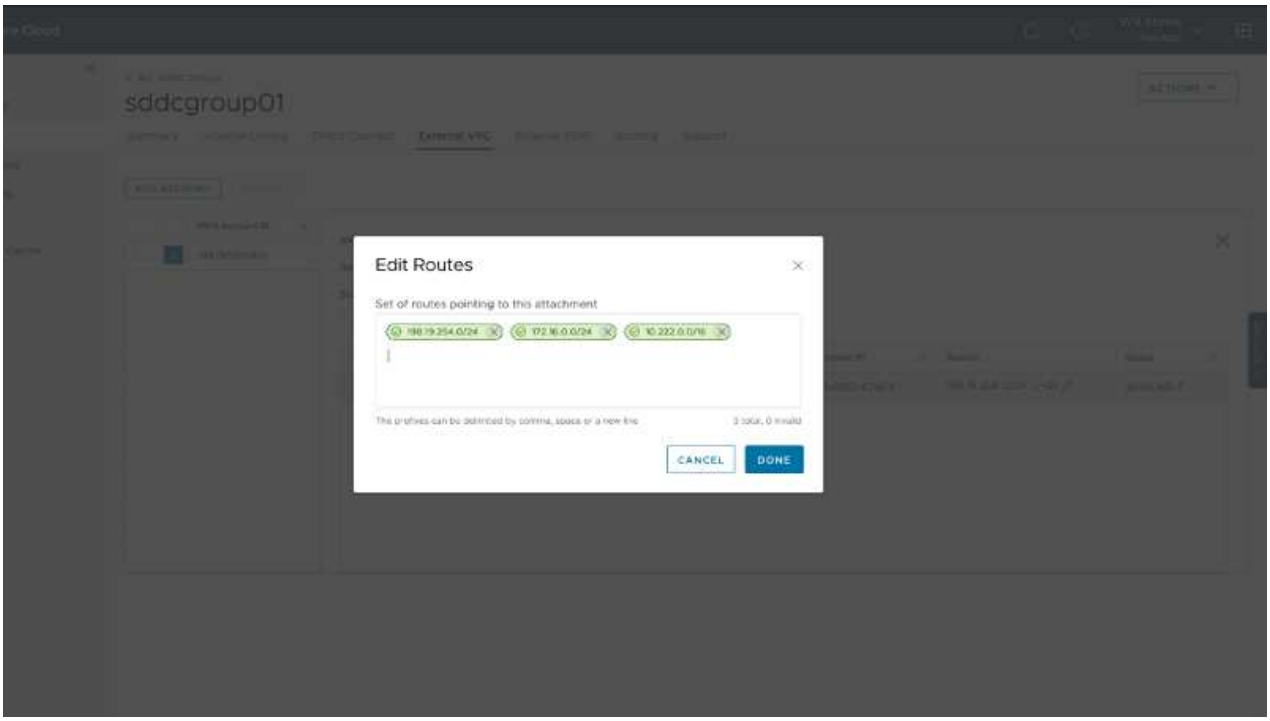
6. De retour sur la console VMC, acceptez la connexion VPC. Ce processus peut prendre environ 10 minutes.



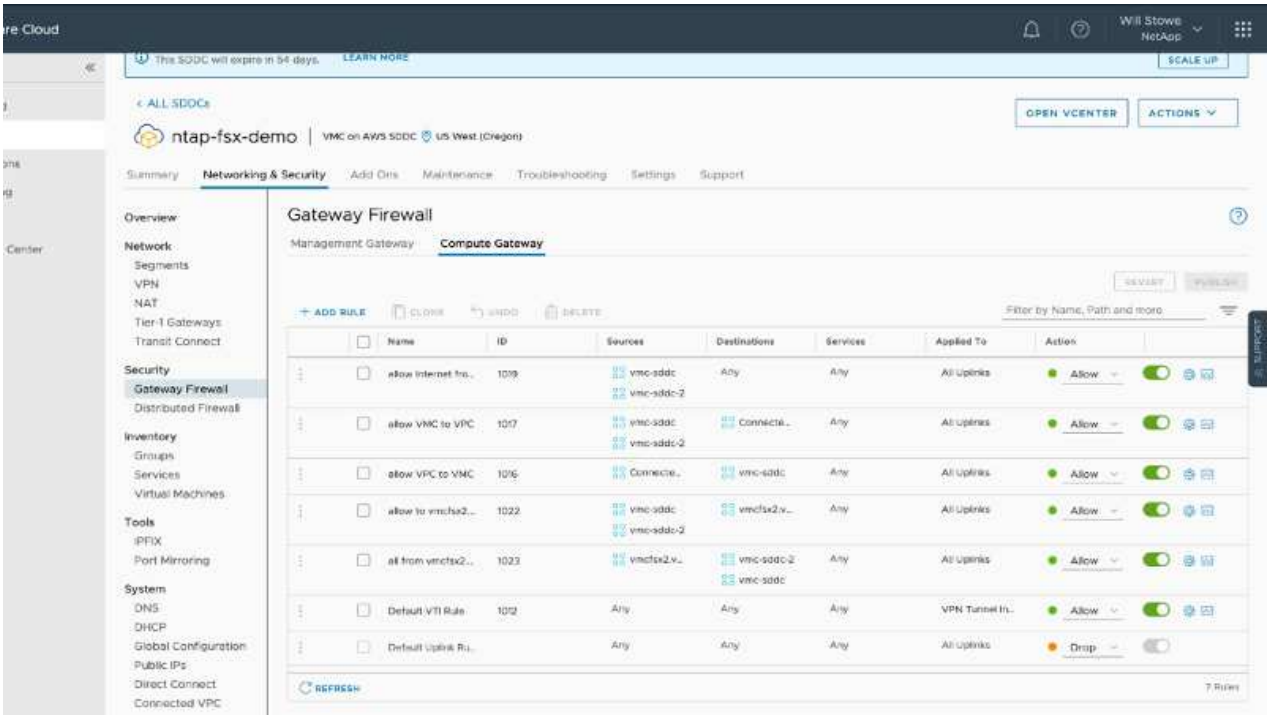
7. Dans l'onglet VPC externe, cliquez sur l'icône Modifier dans la colonne routes et ajoutez les routes requises suivantes :
   - Route pour la plage IP flottante pour Amazon FSX pour NetApp ONTAP "Adresses IP flottantes".
   - Route pour la plage IP flottante pour Cloud Volumes ONTAP (le cas échéant).
   - Route pour l'espace d'adresse VPC externe récemment créé.



8. Enfin, autoriser le trafic bidirectionnel "règles de pare-feu" Pour l'accès à FSX/CVO. Suivez-les "étapes détaillées" Pour le calcul des règles de pare-feu de passerelle pour la connectivité de charge de travail SDDC.



9. Une fois les groupes de pare-feu configurés pour la passerelle de gestion et de calcul, vCenter est accessible de la manière suivante :



L’étape suivante consiste à vérifier que Amazon FSX ONTAP ou Cloud Volumes ONTAP est configuré en fonction de vos besoins et que les volumes sont provisionnés pour décharger les composants de stockage de VSAN afin d’optimiser le déploiement.

Comme sur site, la planification d’Azure VMware solution est cruciale pour la réussite d’un environnement prêt à la production à créer des machines virtuelles et à migrer.

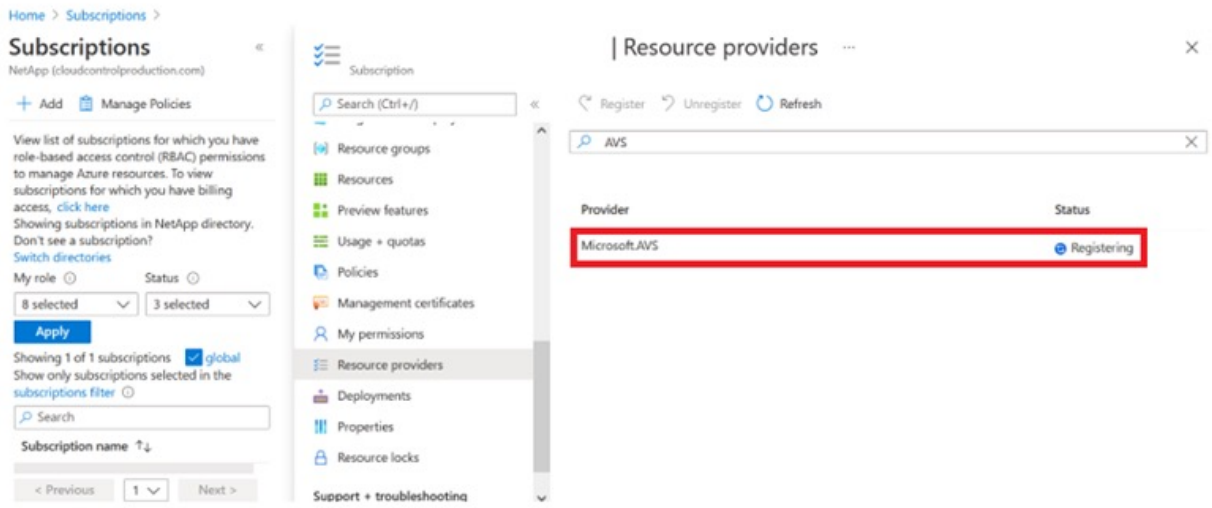
Cette section décrit comment configurer et gérer Azure VMware solution et l’utiliser en association avec les options disponibles pour connecter le stockage NetApp.

Le processus de configuration peut être divisé en plusieurs étapes :

Enregistrez le fournisseur de ressources et créez un cloud privé

Pour utiliser Azure VMware solution, commencez par inscrire le fournisseur de ressources dans l'abonnement identifié :

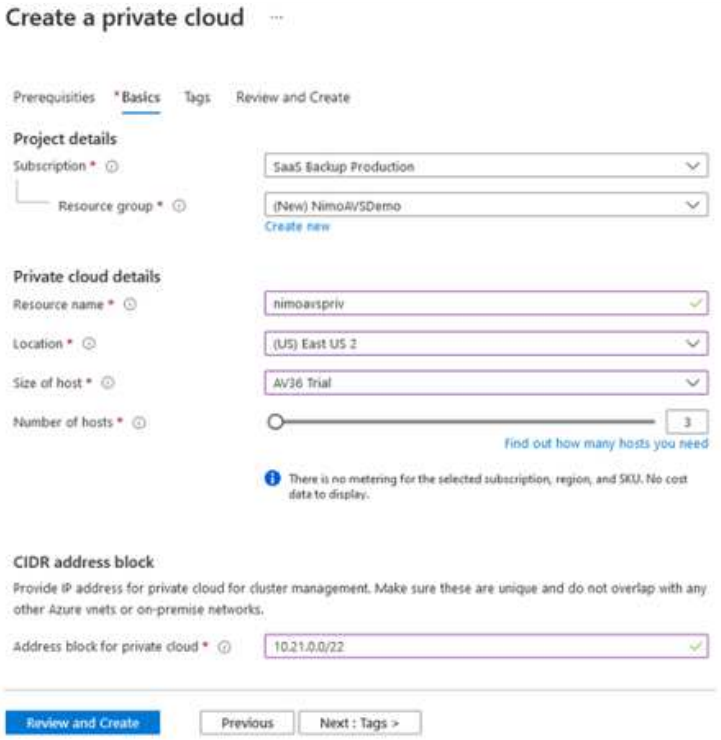
1. Connectez-vous au portail Azure.
2. Dans le menu du portail Azure, sélectionnez tous les services.
3. Dans la boîte de dialogue tous les services, entrez l'abonnement, puis sélectionnez abonnements.
4. Pour afficher l'abonnement, sélectionnez-le dans la liste des abonnements.
5. Sélectionnez Resource Providers et saisissez Microsoft.AVS dans la recherche.
6. Si le fournisseur de ressources n'est pas enregistré, sélectionnez Enregistrer.



7. Une fois le fournisseur de ressources enregistré, créez un cloud privé Azure VMware solution à l'aide du portail Azure.
8. Connectez-vous au portail Azure.
9. Sélectionnez Créer une nouvelle ressource.
10. Dans la zone de texte Rechercher sur le Marketplace, entrez Azure VMware solution et sélectionnez-la dans les résultats.
11. Sur la page solution Azure VMware, sélectionnez Create.
12. Dans l'onglet Basics, entrez les valeurs dans les champs et sélectionnez Revue + Créer.

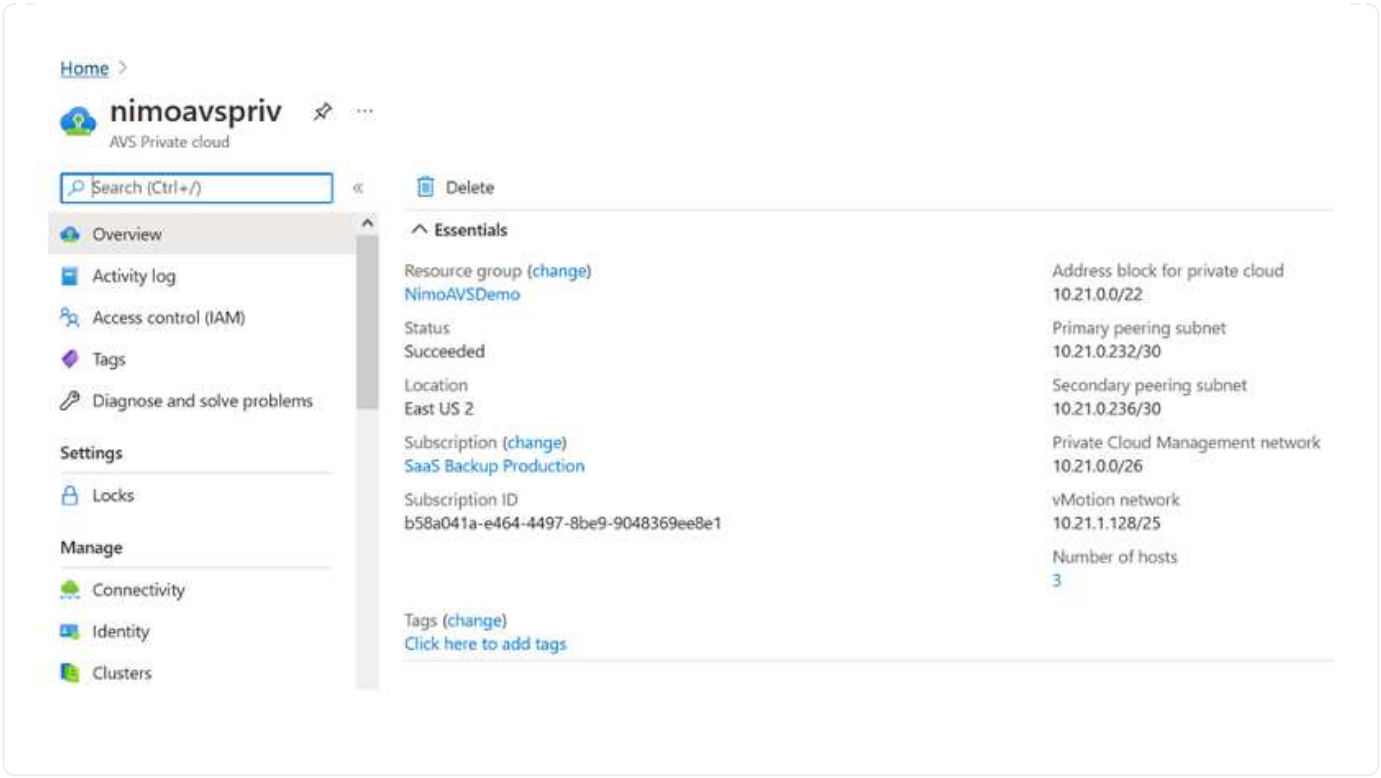
Remarques :

- Pour un démarrage rapide, rassemblez les informations requises pendant la phase de planification.
- Sélectionnez un groupe de ressources existant ou créez un nouveau groupe de ressources pour le cloud privé. Un groupe de ressources est un conteneur logique dans lequel les ressources Azure sont déployées et gérées.
- Assurez-vous que l'adresse CIDR est unique et qu'elle ne se superpose pas aux autres réseaux Azure Virtual Networks ou sur site. Le CIDR est le réseau de gestion de cloud privé utilisé pour les services de gestion de cluster, tels que vCenter Server et NSX-T Manager. NetApp recommande d'utiliser un espace d'adressage /22. Dans cet exemple, 10.21.0.0/22 est utilisé.



Le processus de provisionnement prend entre 4 et 5 heures. Une fois le processus terminé, vérifiez que le déploiement a abouti en accédant au cloud privé à partir du portail Azure. L'état « réussi » s'affiche lorsque le déploiement est terminé.

Un cloud privé pour solution Azure VMware nécessite un réseau virtuel Azure. Étant donné que la solution Azure VMware ne prend pas en charge vCenter sur site, des étapes supplémentaires sont requises pour l'intégration avec un environnement existant sur site. Il est également nécessaire de configurer un circuit ExpressRoute et une passerelle réseau virtuelle. En attendant la fin du provisionnement du cluster, créez un nouveau réseau virtuel ou utilisez un réseau existant pour vous connecter à la solution Azure VMware.


Home
nimoavspriv
AVS Private cloud
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Identity
Clusters
Delete
Essentials
Resource group (change)
NimoAVSDemo
Status
Succeeded
Location
East US 2
Subscription (change)
SaaS Backup Production
Subscription ID
b58a041a-e464-4497-8be9-9048369ee8e1
Tags (change)
Click here to add tags
Address block for private cloud
10.21.0.0/22
Primary peering subnet
10.21.0.232/30
Secondary peering subnet
10.21.0.236/30
Private Cloud Management network
10.21.0.0/26
vMotion network
10.21.1.128/25
Number of hosts
3

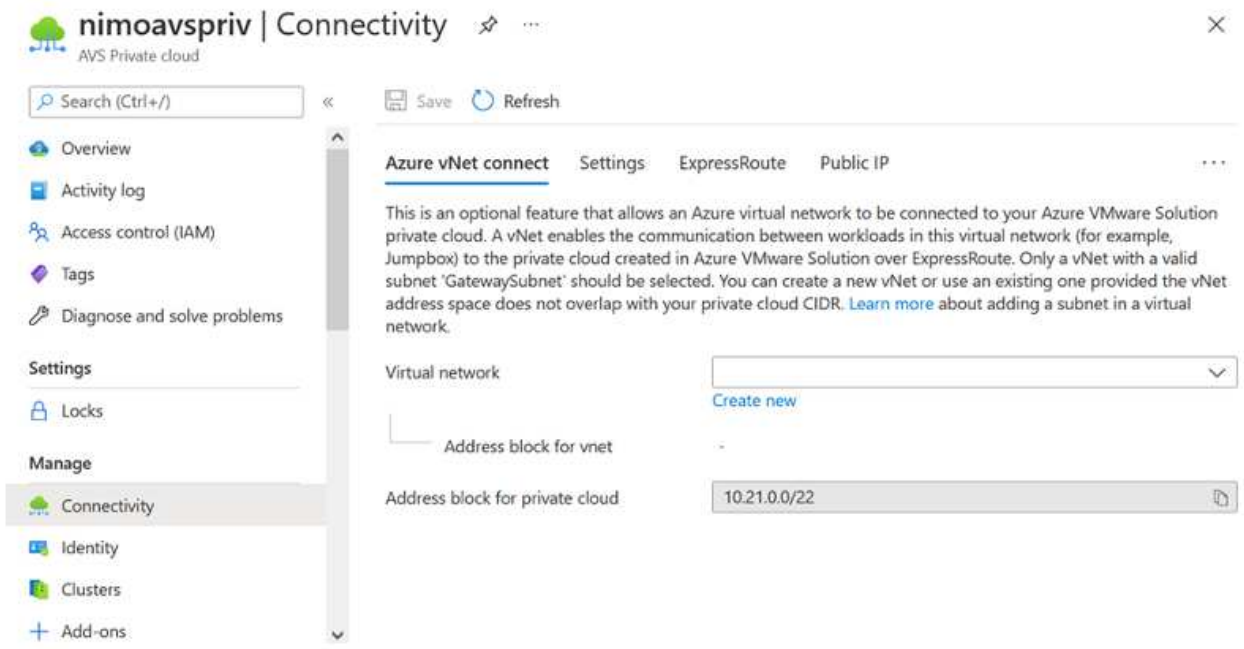
Connectez-vous à une passerelle réseau virtuelle ExpressRoute nouvelle ou existante

Pour créer un nouveau réseau virtuel Azure (vNet), sélectionnez l'onglet Azure vNet Connect. Vous pouvez également en créer un manuellement à partir du portail Azure à l'aide de l'assistant de création de réseau virtuel :

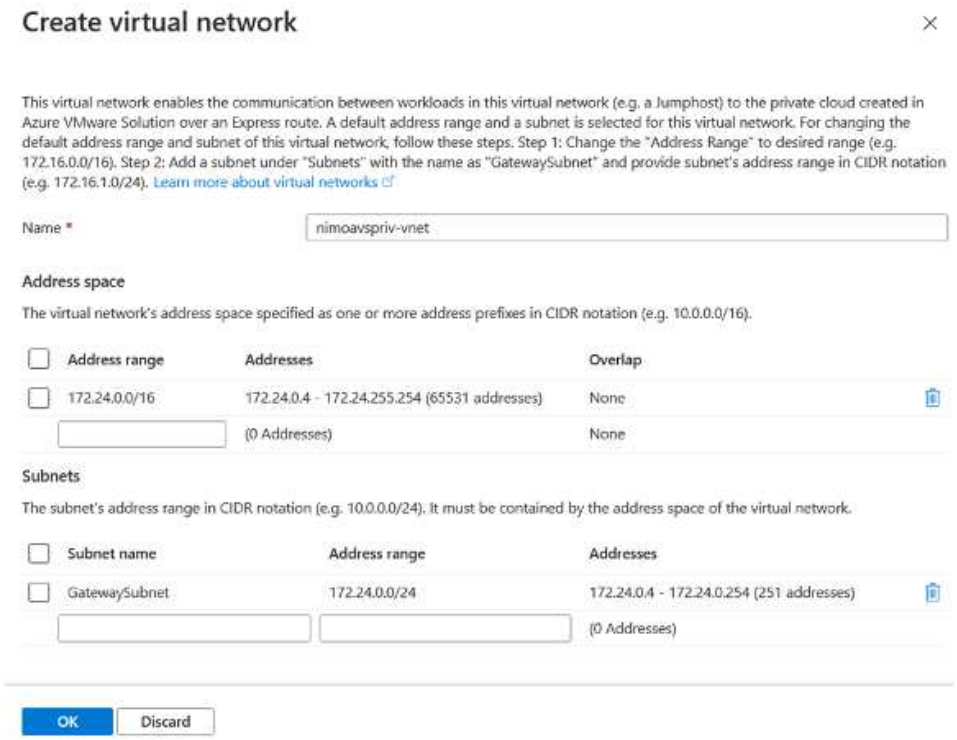
1. Accédez à Azure VMware solution cloud privé et à Access Connectivity sous l'option Manage.
2. Sélectionnez Azure VNet Connect.
3. Pour créer un nouveau vnet, sélectionnez l'option Créer nouveau.

   Cette fonctionnalité permet de connecter un vnet au cloud privé Azure VMware solution. Il permet la communication entre les charges de travail sur ce réseau virtuel en créant automatiquement les composants nécessaires (par exemple, sauter le pas, les services partagés tels qu'Azure NetApp Files et Cloud Volume ONTAP) vers le cloud privé créé dans Azure VMware solution over ExpressRoute.

   Remarque : l'espace d'adressage VNet ne doit pas se chevaucher avec le CIDR sur le Cloud privé.



4. Fournissez ou mettez à jour les informations relatives au nouveau VNet et sélectionnez OK.

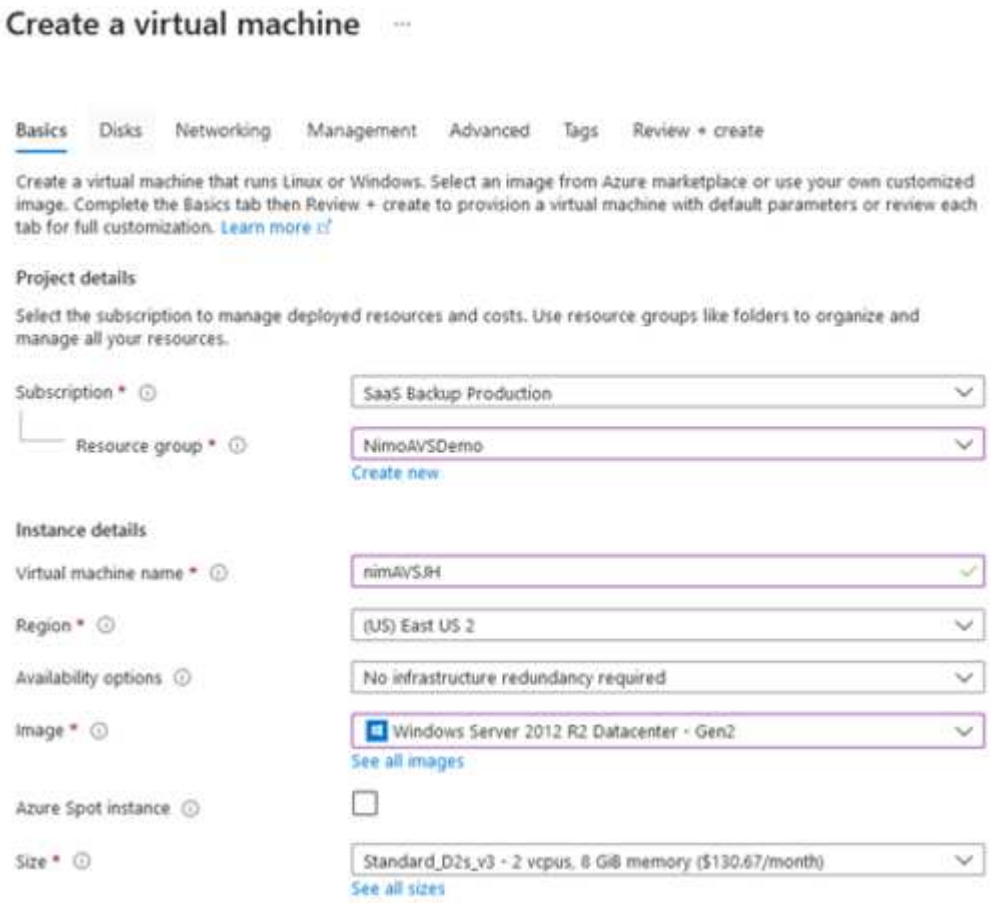


Le vnet avec la plage d'adresses et le sous-réseau de passerelle fournis est créé dans le groupe d'abonnement et de ressources désigné.

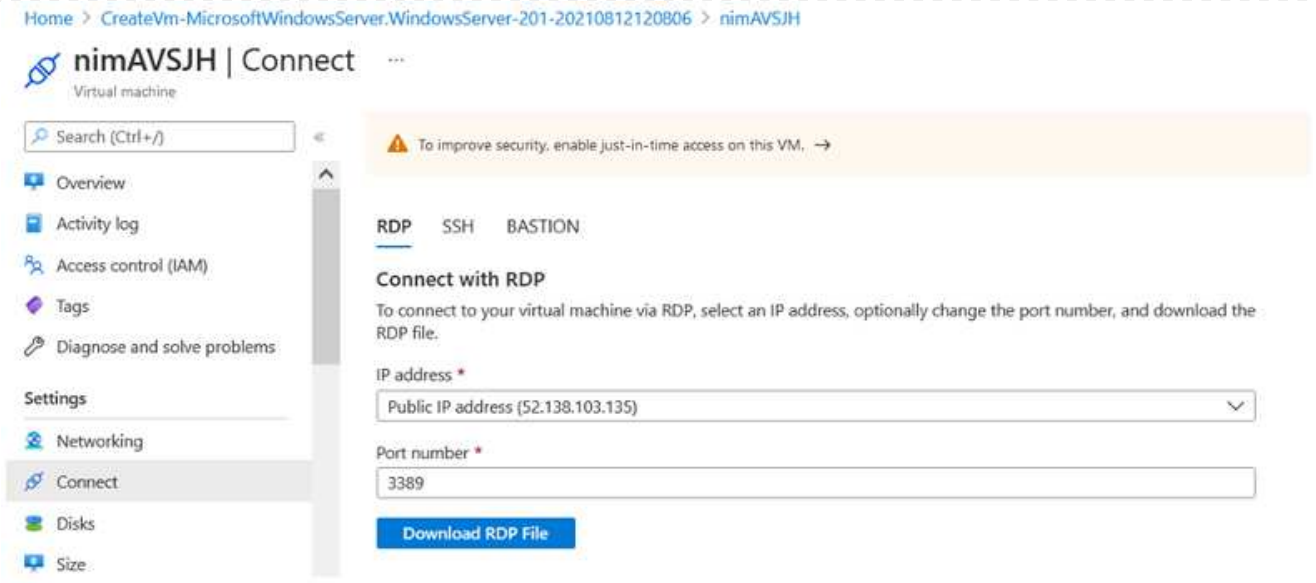
Si vous créez un VNet manuellement, créez une passerelle réseau virtuelle avec le SKU approprié et ExpressRoute comme type de passerelle. Une fois le déploiement terminé, connectez la connexion ExpressRoute à la passerelle de réseau virtuel contenant le cloud privé Azure VMware solution à l'aide de la clé d'autorisation. Pour plus d'informations, voir "Configurez le réseau pour votre cloud privé VMware dans Azure".

Validation de la connexion réseau et de l'accès au cloud privé Azure VMware solution

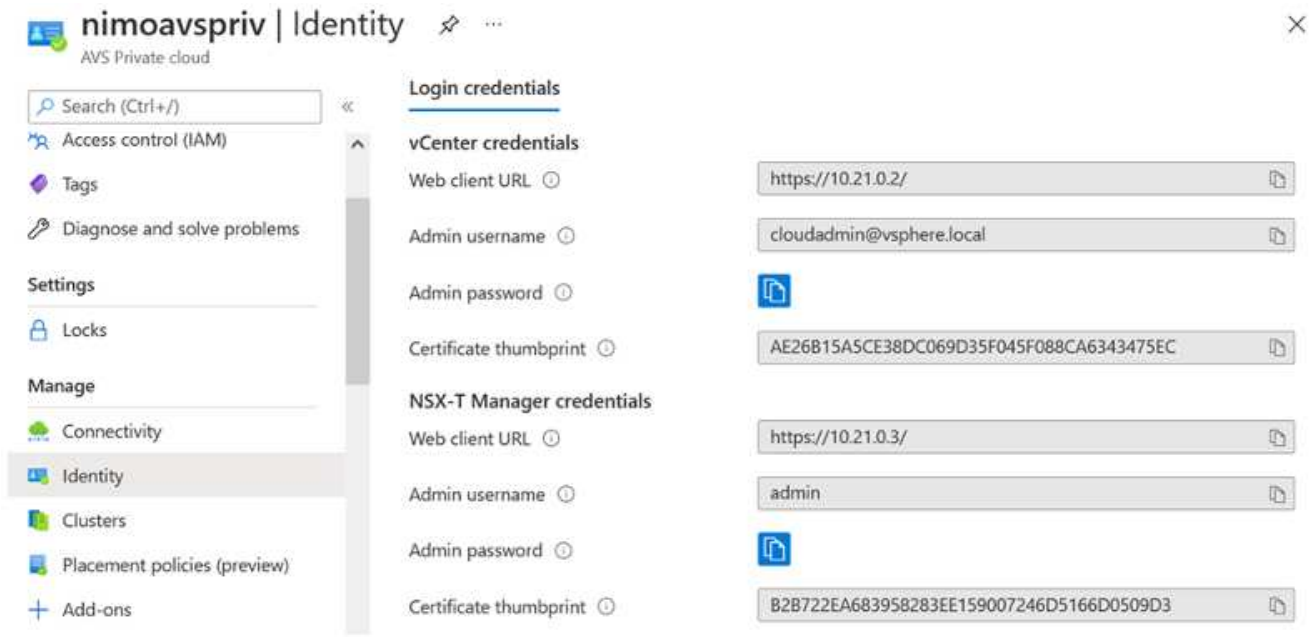
Azure VMware solution ne vous permet pas de gérer un cloud privé avec VMware vCenter sur site. Un hôte saut est alors nécessaire pour la connexion à l'instance Azure VMware solution vCenter. Créez un hôte de démarrage dans le groupe de ressources désigné et connectez-vous à Azure VMware solution vCenter. Cet hôte de saut doit être une machine virtuelle Windows sur le même réseau virtuel créé pour la connectivité et doit fournir un accès à vCenter et à NSX Manager.



Une fois la machine virtuelle provisionnée, utilisez l'option Connect pour accéder à RDP.

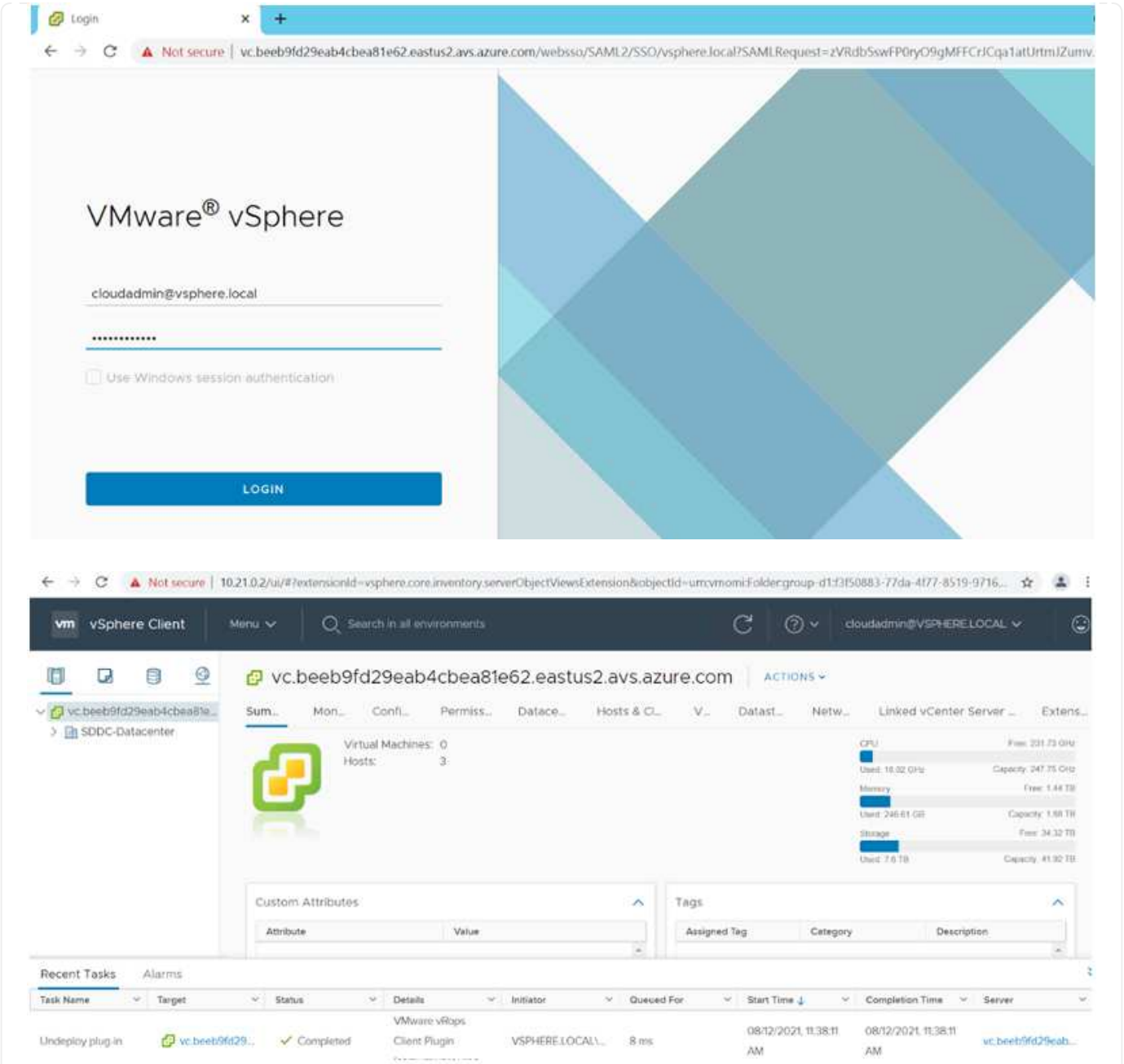


Connectez-vous à vCenter à partir de cette nouvelle machine virtuelle hôte de démarrage en utilisant l'utilisateur d'administration du cloud . Pour accéder aux identifiants, accédez au portail Azure et recherchez Identity (sous l'option Manage (gérer dans le cloud privé). Les URL et les informations d'identification de l'utilisateur pour le cloud privé vCenter et NSX-T Manager peuvent être copiés à partir d'ici.



Dans la machine virtuelle Windows, ouvrez un navigateur et accédez à l'URL du client Web vCenter et utilisez le nom d'utilisateur admin comme **cloudadmin@vsphere.locumbip** et collez le mot de passe copié. De même, NSX-T Manager est également accessible à l'aide de l'URL du client Web utilisez le nom d'utilisateur admin et collez le mot de passe copié pour créer de nouveaux segments ou modifier les passerelles de niveau existantes.

Les URL des clients Web sont différentes pour chaque SDDC provisionné.



Le SDDC Azure VMware solution est désormais déployé et configuré. Tirez parti d'ExpressRoute Global Reach pour relier l'environnement sur site au cloud privé Azure VMware solution. Pour plus d'informations, voir "Concevez des environnements sur site vers la solution Azure VMware".

Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)

Comme pour les environnements sur site, la planification de Google Cloud VMware Engine (GCVE) est essentielle pour la réussite de l'environnement de production pour la création de VM et la migration.

Cette section décrit comment configurer et gérer GCVE et l'utiliser en association avec les options disponibles pour la connexion du stockage NetApp.

Le processus de configuration peut être divisé en plusieurs étapes :

Déployer et configurer GCVE

Pour configurer un environnement GCVE dans GCP, connectez-vous à la console GCP et accédez au portail VMware Engine.

Cliquez sur le bouton "Nouveau Cloud privé" et entrez la configuration souhaitée pour le Cloud privé GCVE. Sur « Location », veillez à déployer le Cloud privé dans la même région/zone où CVS/CVO est déployé, afin d'assurer les meilleures performances et la plus faible latence.

Conditions préalables :

- Configurer le rôle IAM d'administration des services VMware Engine
- "Activez l'accès à l'API VMware Engine et le quota de nœuds"
- Assurez-vous que la plage CIDR ne se chevauchent pas avec vos sous-réseaux locaux ou dans le cloud. La gamme CIDR doit être /27 ou supérieure.

Remarque : la création d'un cloud privé peut prendre entre 30 minutes et 2 heures.

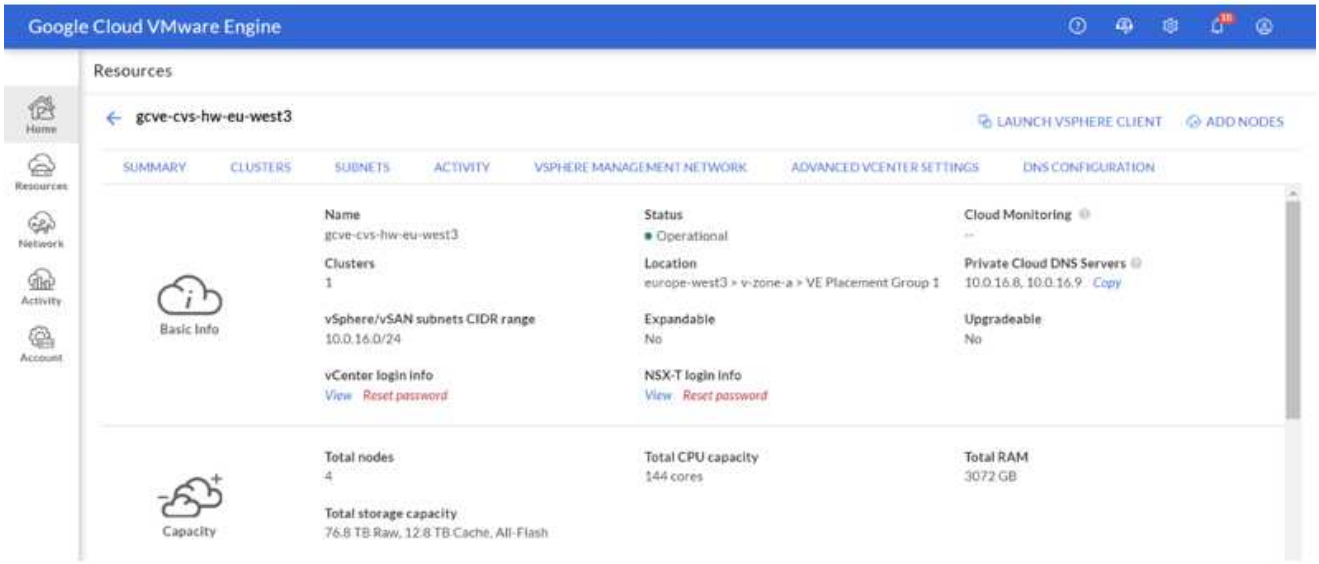
Activez l’accès privé à GCVE

Une fois le cloud privé provisionné, configurez l’accès privé au cloud privé pour obtenir un débit élevé et une connexion à faible latence du chemin d’accès aux données.

Cela permet de s’assurer que le réseau VPC dans lequel des instances Cloud Volumes ONTAP sont en cours d’exécution peut communiquer avec le Cloud privé GCVE. Pour ce faire, suivez le "Documentation GCP". Pour le service de volume cloud, établissez une connexion entre VMware Engine et Cloud Volumes Service en effectuant un peering unique entre les projets hôtes du locataire. Pour obtenir des instructions détaillées, suivez cette procédure "lien".

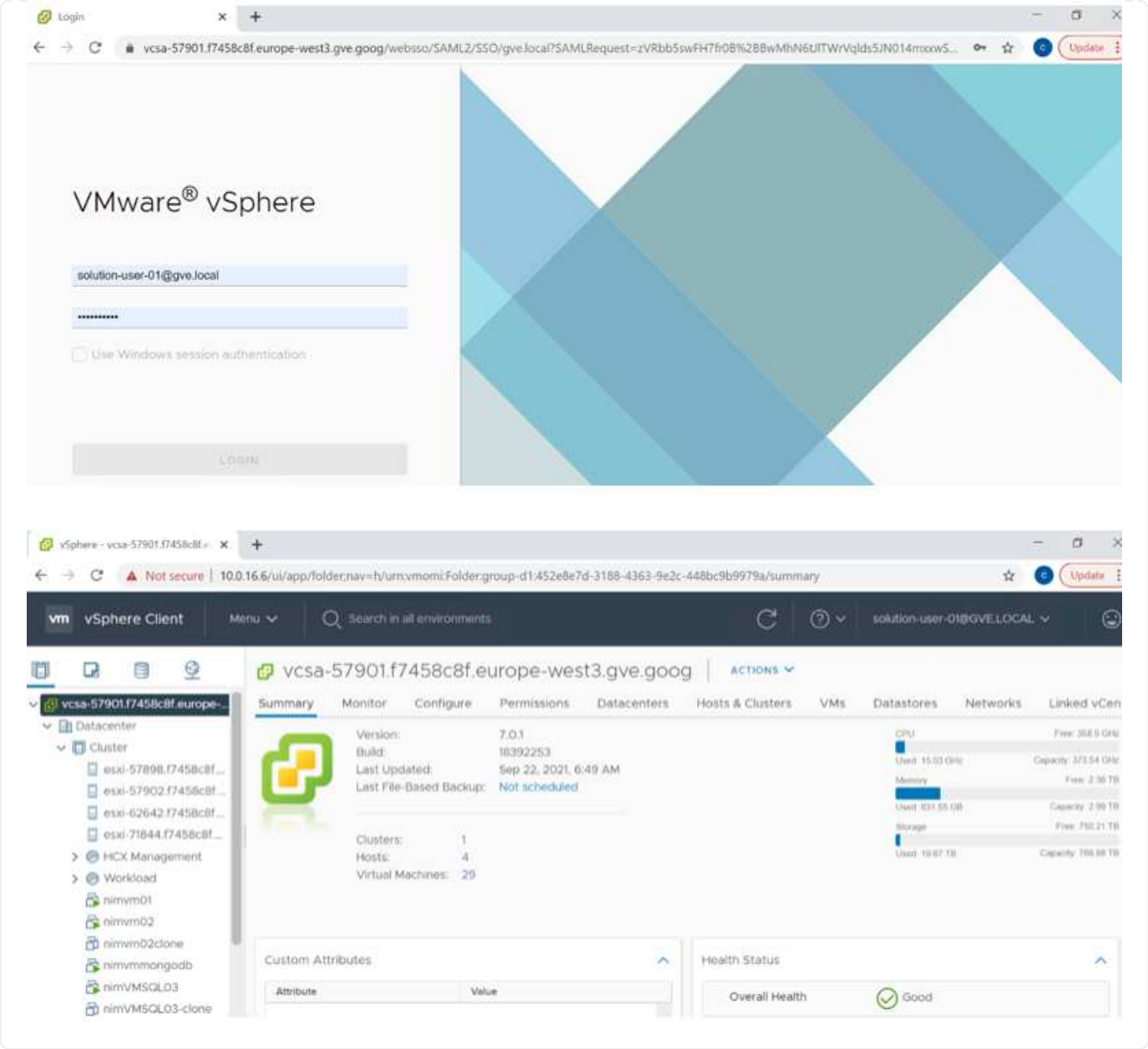
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

Connectez-vous à vcenter à l’aide de l’utilisateur CloudOwner@gve.llocabmabl. Pour accéder aux identifiants, rendez-vous sur le portail VMware Engine, accédez à Ressources et sélectionnez le cloud privé approprié. Dans la section informations de base, cliquez sur le lien View pour accéder aux informations de connexion vCenter (vCenter Server, HCX Manager) ou aux informations de connexion NSX-T (NSX Manager).



Dans une machine virtuelle Windows, ouvrez un navigateur et accédez à l’URL du client Web vCenter Et utilisez le nom d’utilisateur admin tel que CloudOwner@gve.locusmabl et collez le mot de passe copié. De même, NSX-T Manager est également accessible à l’aide de l’URL du client Web utilisez le nom d’utilisateur admin et collez le mot de passe copié pour créer de nouveaux segments ou modifier les passerelles de niveau existantes.

Pour la connexion à partir d’un réseau sur site vers un cloud privé VMware Engine, utilisez un VPN cloud ou une interconnexion de cloud pour assurer la connectivité appropriée et assurez-vous que les ports requis sont ouverts. Pour obtenir des instructions détaillées, suivez cette procédure "lien".



Déployez le datastore supplémentaire de NetApp Cloud Volume Service dans GCVE

Reportez-vous à "Procédure de déploiement d'un datastore NFS supplémentaire avec NetApp CVS dans GCVE"

Fournisseurs de cloud public : options de stockage NetApp

Découvrez les options de NetApp en tant que stockage dans les trois principaux hyperscalers.

AWS/VMC

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".

Azure/AVS

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

- Azure NetApp Files (ANF) comme stockage connecté invité
- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- Azure NetApp Files (ANF) comme datastore NFS supplémentaire

Afficher les détails "Option de stockage avec connexion invité pour AVS". Afficher les détails "Options supplémentaires de datastore NFS pour AVS".

GCP/GCVE

Google Cloud prend en charge le stockage NetApp dans les configurations suivantes :

- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- Cloud Volumes Service (CVS) comme stockage connecté invité
- Cloud Volumes Service (CVS) comme datastore NFS supplémentaire

Afficher les détails "Options de stockage de connexion invité pour GCVE".

En savoir plus sur "Prise en charge du datastore NetApp Cloud Volumes Service pour Google Cloud VMware Engine (blog NetApp)" ou "Comment utiliser NetApp CVS en tant que datastores pour Google Cloud VMware Engine (blog Google)"

Tr-4938 : monter Amazon FSX pour ONTAP en tant que datastore NFS avec VMware Cloud sur AWS

Niyaz Mohamed, NetApp

Introduction

Chaque organisation réussie est sur le chemin de la transformation et de la modernisation. Dans le cadre de ce processus, les entreprises utilisent généralement leurs investissements VMware existants pour tirer parti des avantages du cloud et étudier comment migrer, rafale, étendre et garantir la reprise sur incident de manière aussi transparente que possible. Les clients qui migrent vers le cloud doivent évaluer les cas d'utilisation en termes de flexibilité et de rafale, de sortie de data Center, de consolidation de data Center, de scénarios de fin de vie, de fusion, des acquisitions, etc.

Même si VMware Cloud sur AWS est l'option de prédilection de la plupart des clients, c'est parce qu'il fournit des fonctionnalités hybrides uniques à un client, les options de stockage natif limitées ont limité son utilité pour les entreprises qui utilisent des charges de travail fortement lourdes. Le stockage étant directement lié aux

hôtes, la seule façon de faire évoluer le stockage consiste à ajouter d'autres hôtes, ce qui permet d'augmenter les coûts de 35 à 40 % ou plus pour les charges de travail consommatrices de stockage. Ces charges de travail ont besoin de stockage supplémentaire et de performances isolées, sans puissance supplémentaire, ce qui signifie que des frais supplémentaires sont en charge des hôtes. C'est là que le "intégration récente" La solution FSX pour ONTAP est disponible pour les workloads de stockage et exigeants en performances avec VMware Cloud sur AWS.

Examinons le scénario suivant : un client nécessite huit hôtes pour la puissance (vCPU/vmem), mais qui doivent également présenter des exigences importantes en matière de stockage. En fonction de leur évaluation, ils nécessitent 16 hôtes pour répondre aux besoins en stockage. Cela augmente le coût total de possession global car ils doivent acheter toute cette puissance supplémentaire lorsque c'est la capacité de stockage requise. Cette fonctionnalité est applicable à toutes les utilisations, y compris la migration, la reprise sur incident, l'bursting, le développement/test, et ainsi de suite.

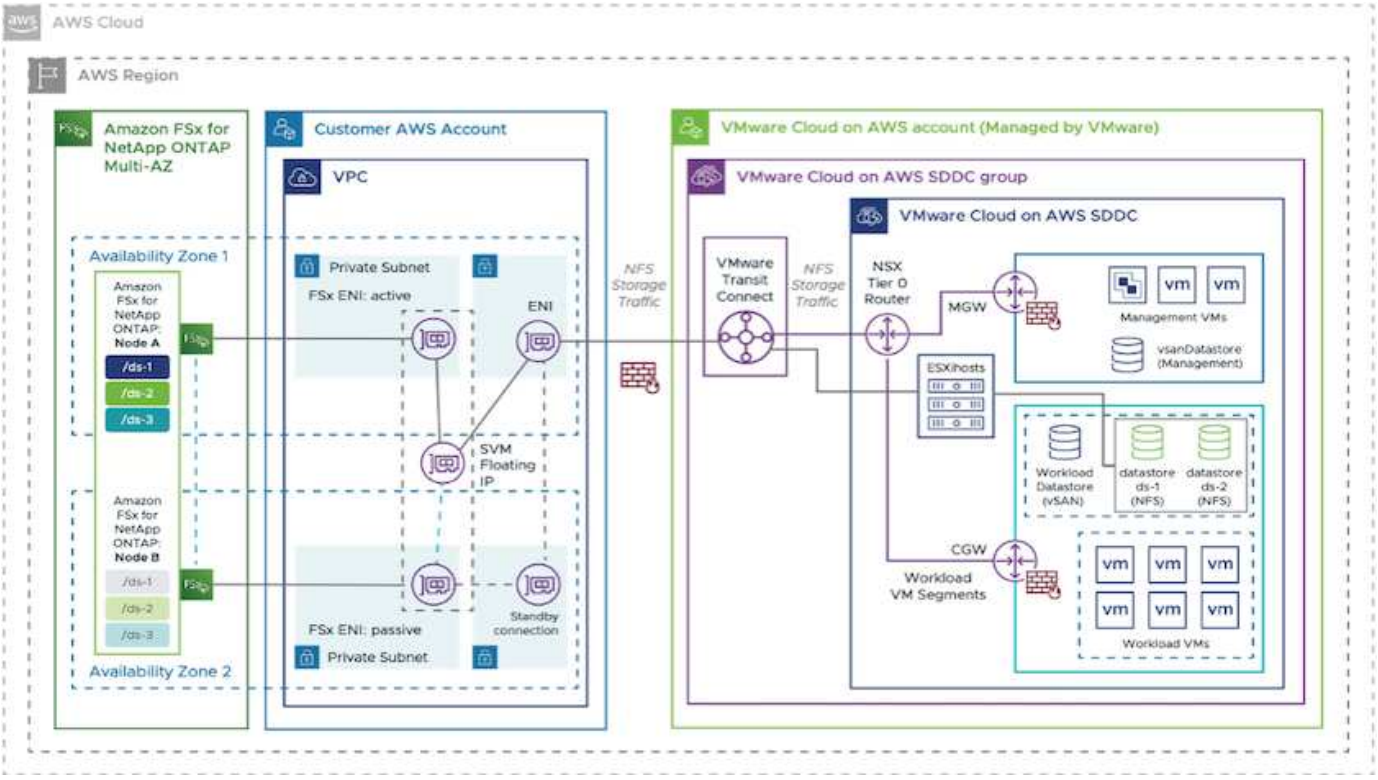
Ce document vous présente les étapes de provisionnement et de connexion de FSX pour ONTAP en tant que datastore NFS pour VMware Cloud sur AWS.

Cette solution est également disponible auprès de VMware. Veuillez visiter le "Zone technique cloud VMware" pour en savoir plus.

Options de connectivité

VMware Cloud sur AWS prend en charge les déploiements FSX pour ONTAP à plusieurs zones de disponibilité et même zone d'accès.

Cette section décrit l'architecture de connectivité de haut niveau et les étapes nécessaires à la mise en œuvre de la solution pour étendre le stockage dans un cluster SDDC sans ajouter d'hôtes supplémentaires.



Les étapes de déploiement de haut niveau sont les suivantes :

1. Créez Amazon FSX pour ONTAP dans un nouveau VPC désigné.
2. Créer un groupe SDDC.
3. Créez VMware Transit Connect et une pièce jointe TGW.
4. Configuration du routage (VPC AWS et SDDC) et des groupes de sécurité
5. Joignez un volume NFS en tant que datastore au cluster SDDC.

Avant de provisionner et de connecter FSX pour ONTAP en tant que datastore NFS, vous devez d'abord configurer un environnement VMware sur un cloud SDDC ou obtenir une mise à niveau existante vers v1.20 ou une version ultérieure. Pour plus d'informations, reportez-vous à la section "Mise en route de VMware Cloud sur AWS".

FSX pour ONTAP n'est actuellement pas pris en charge avec les clusters étirés.

Conclusion

Ce document aborde les étapes nécessaires à la configuration d'Amazon FSX pour ONTAP avec VMware Cloud sur AWS. Amazon FSX pour ONTAP offre d'excellentes options pour déployer et gérer les charges de travail applicatives et les services de fichiers, tout en réduisant le coût total de possession en rendant les données requises transparentes pour la couche applicative. Quel que soit le cas d'utilisation, choisissez VMware Cloud sur AWS et Amazon FSX pour ONTAP pour bénéficier rapidement des avantages du cloud, d'une infrastructure cohérente et des opérations sur site vers AWS, de la portabilité bidirectionnelle des charges de travail, et d'une capacité et des performances élevées. Il s'agit du même processus et des mêmes procédures que ceux utilisés pour connecter le stockage. N'oubliez pas que c'est seulement la position des données qui ont changé avec de nouveaux noms. Les outils et les processus restent les mêmes, et Amazon FSX pour ONTAP contribue à optimiser le déploiement global.

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

Amazon FSX pour ONTAP Cloud VMware

Options de stockage connecté à un système invité NetApp pour AWS

AWS prend en charge le stockage NetApp connecté à l'invité avec le service FSX natif (FSX ONTAP) ou avec Cloud Volumes ONTAP (CVO).

ONTAP FSX

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 ONTAP de NetApp. FSX for ONTAP associe les fonctionnalités, performances, capacités et opérations d'API connues des systèmes de fichiers NetApp, ainsi que l'agilité, l'évolutivité et la simplicité d'un service AWS entièrement géré.

FSX pour ONTAP offre un stockage de fichiers partagés riche en fonctionnalités, rapide et flexible, accessible depuis les instances de calcul Linux, Windows et MacOS exécutées dans AWS ou sur site. La solution FSX pour ONTAP offre un stockage SSD hautes performances avec des latences inférieures à la milliseconde. La solution FSX pour ONTAP vous permet d'atteindre des niveaux SSD de performances pour votre charge de travail tout en payant le stockage SSD pour une fraction seulement de vos données.

La gestion de vos données avec FSX pour ONTAP est plus simple car vous pouvez effectuer des instantanés, cloner et répliquer vos fichiers en un seul clic. De plus, FSX for ONTAP hiérarchise automatiquement vos données vers un stockage flexible et moins coûteux, en réduisant les besoins en matière de provisionnement

ou de gestion de la capacité.

FSX pour ONTAP fournit également un stockage durable et haute disponibilité avec des sauvegardes entièrement gérées et prend en charge la reprise après incident inter-région. Afin de simplifier la protection et la sécurité de vos données, FSX pour ONTAP prend en charge les applications courantes de sécurité de données et antivirus.

FSX ONTAP en tant que stockage invité connecté

Configuration d'Amazon FSX pour NetApp ONTAP avec VMware Cloud sur AWS

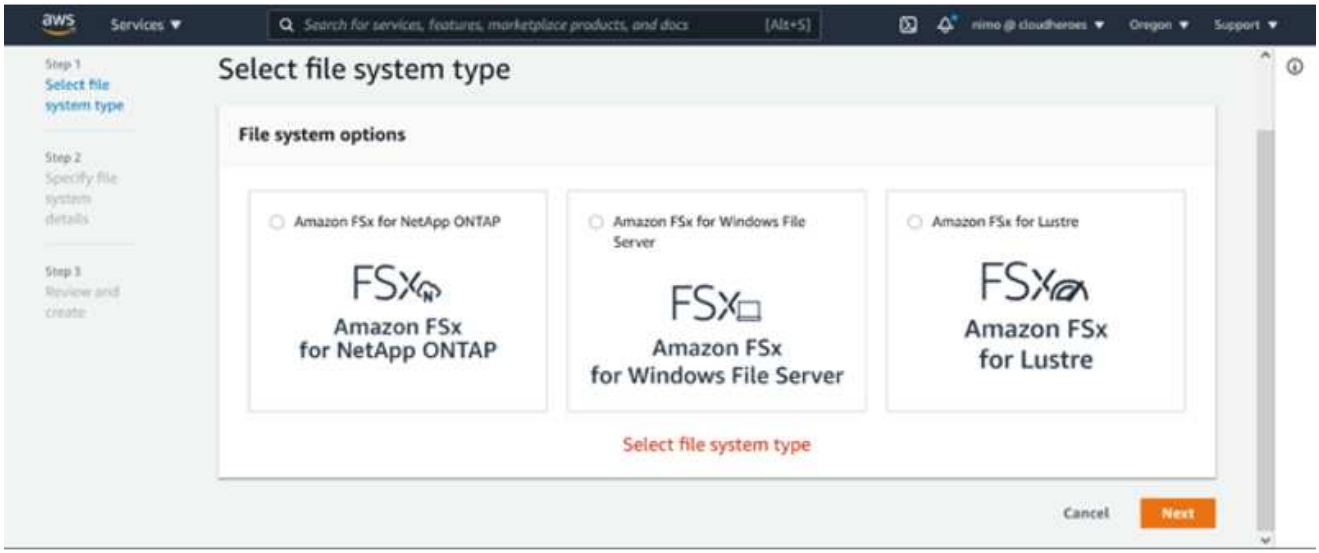
Amazon FSX pour NetApp ONTAP Files partages et LUN peuvent être montés depuis les machines virtuelles créées dans l'environnement VMware SDDC au sein de VMware Cloud au sein d'AWS. Les volumes peuvent également être montés sur le client Linux et mappés sur le client Windows à l'aide du protocole NFS ou SMB. Les LUN sont accessibles sur les clients Linux ou Windows sous forme de périphériques de bloc lorsqu'ils sont montés sur iSCSI. Vous pouvez configurer rapidement Amazon FSX pour le système de fichiers NetApp ONTAP en procédant comme suit.

Amazon FSX pour NetApp ONTAP et VMware Cloud sur AWS doivent se trouver dans la même zone de disponibilité afin d'améliorer les performances et d'éviter les frais de transfert de données entre les zones de disponibilité.

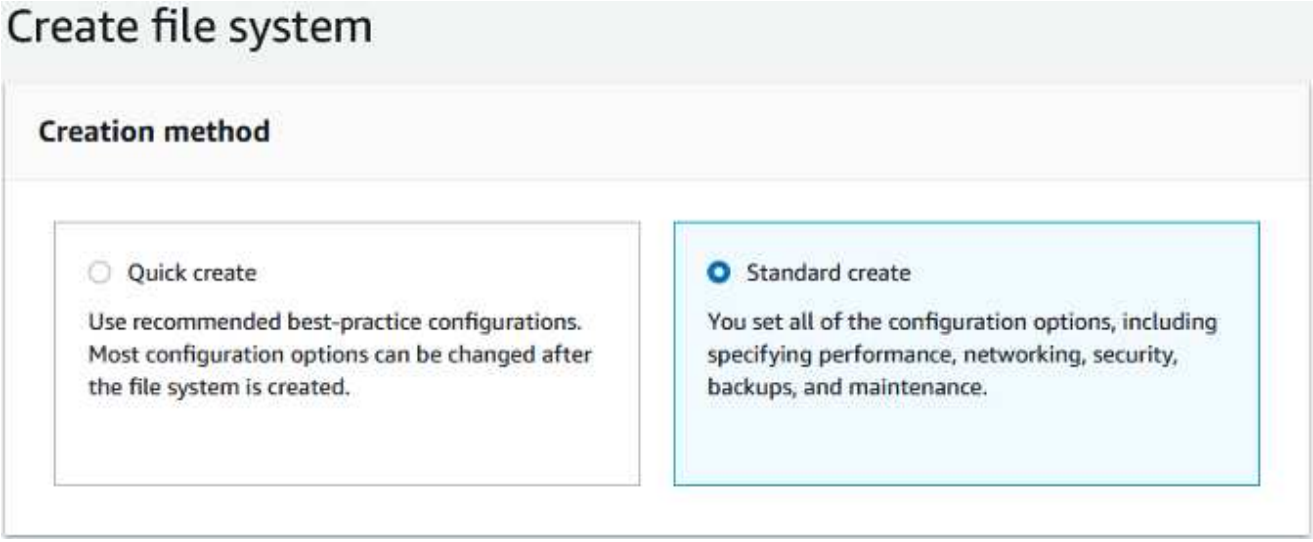
Création et montage d'Amazon FSX pour les volumes ONTAP

Pour créer et monter un système de fichiers Amazon FSX pour NetApp ONTAP, procédez comme suit :

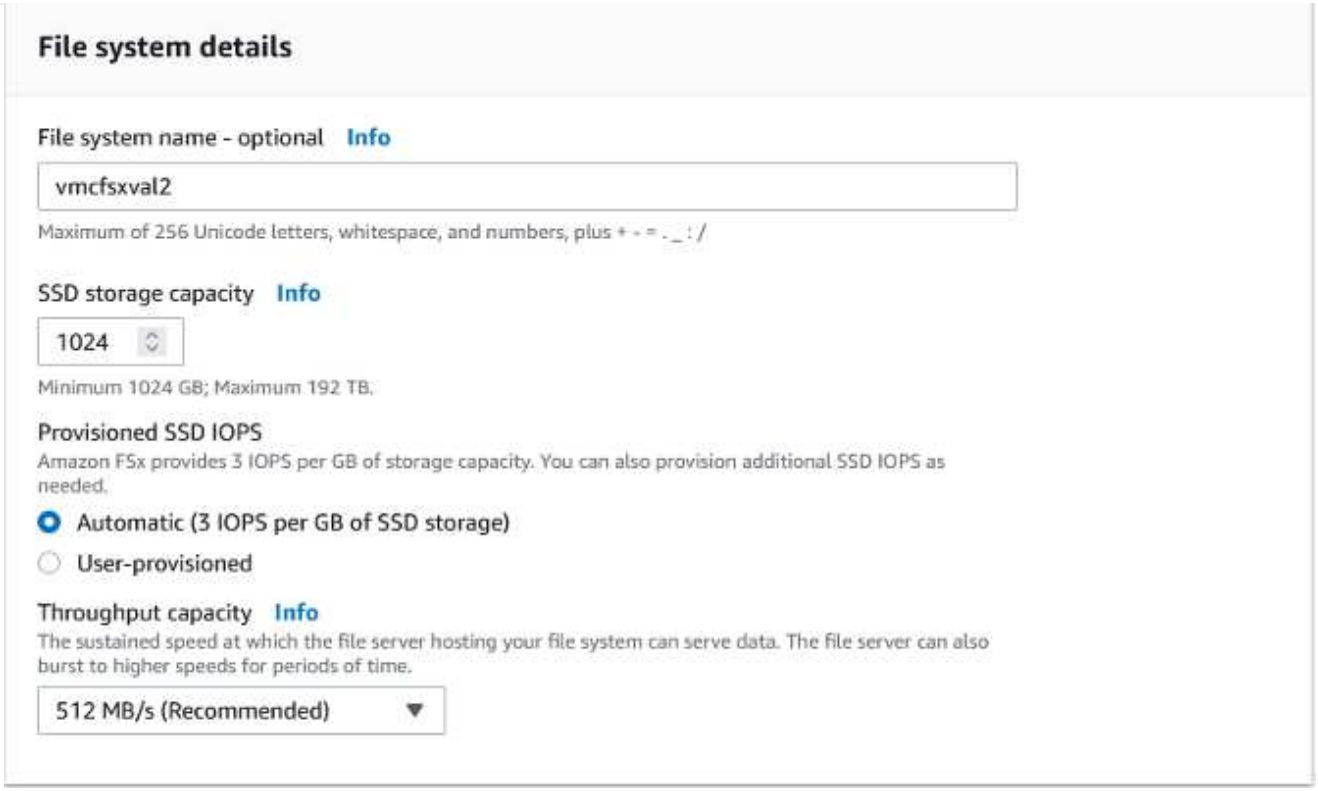
1. Ouvrez le "Console Amazon FSX" Et choisissez Créer un système de fichiers pour démarrer l'assistant de création de système de fichiers.
2. Sur la page Select File System Type, choisissez Amazon FSX pour NetApp ONTAP, puis cliquez sur Next. La page Créer un système de fichiers s'affiche.



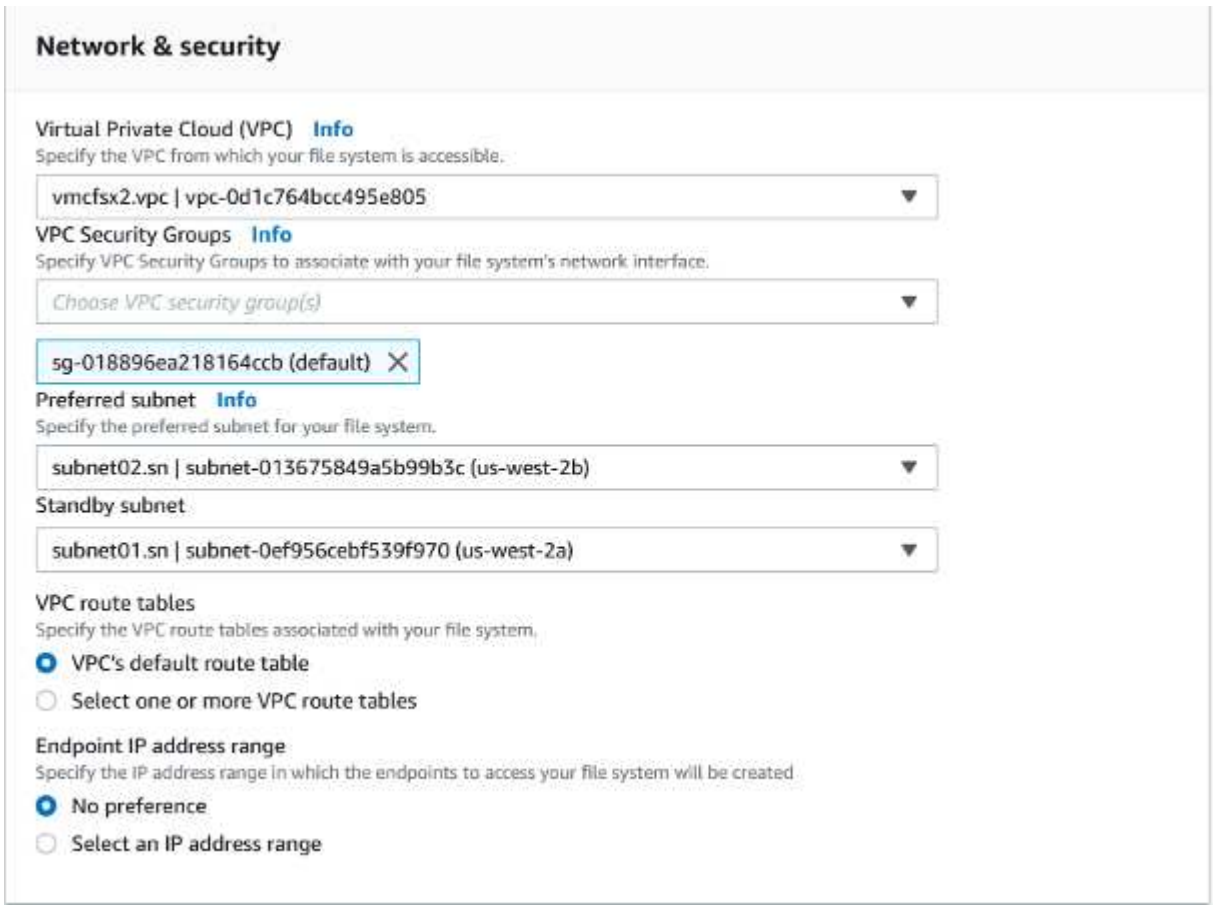
1. Dans la section mise en réseau, pour le cloud privé virtuel (VPC), choisissez le VPC (Virtual Private Cloud) approprié et les sous-réseaux préférés, ainsi que la table de routage. Dans ce cas, vmcfsx2.vpc est sélectionné dans la liste déroulante.



1. Pour la méthode de création, choisissez création standard. Vous pouvez également choisir création rapide, mais ce document utilise l'option création standard.

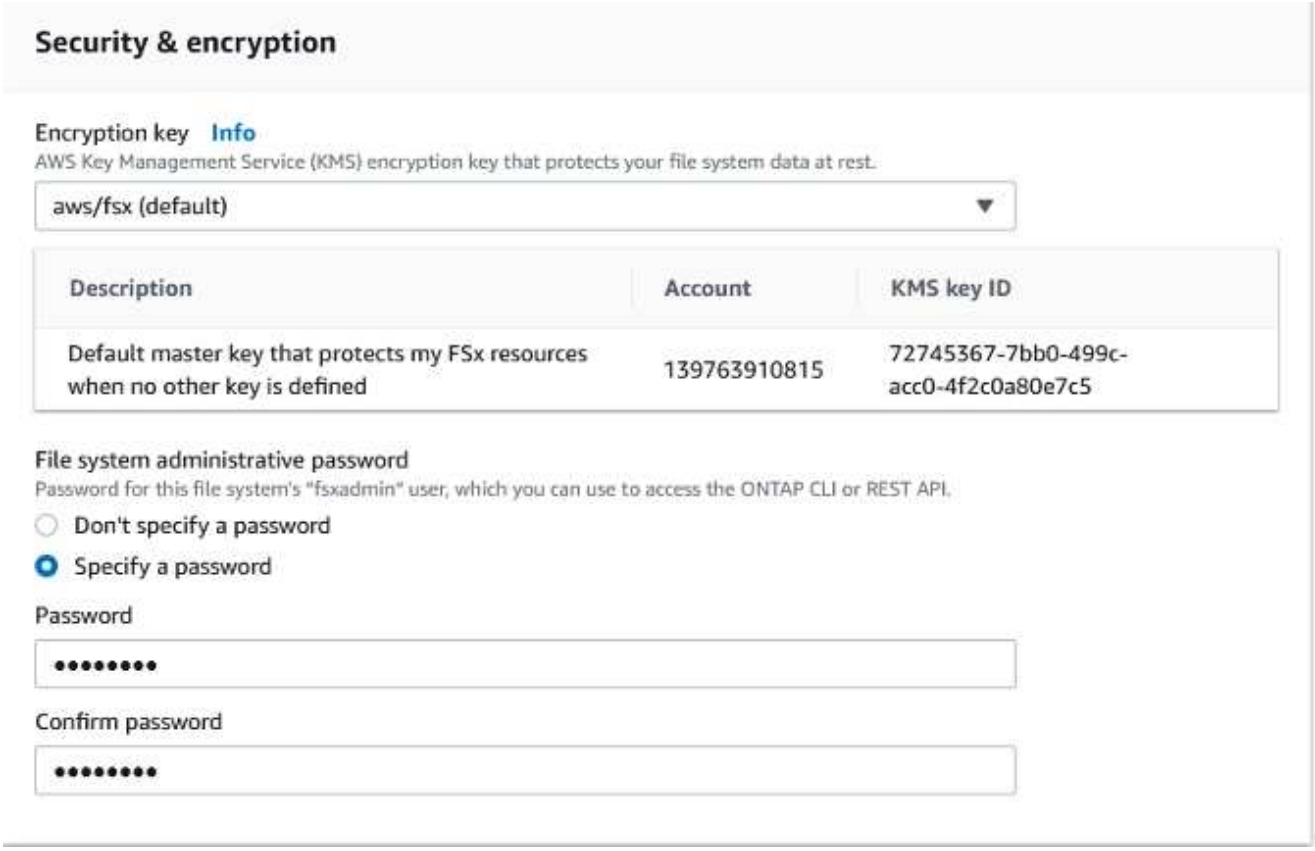


1. Dans la section mise en réseau, pour le cloud privé virtuel (VPC), choisissez le VPC (Virtual Private Cloud) approprié et les sous-réseaux préférés, ainsi que la table de routage. Dans ce cas, vmcfsx2.vpc est sélectionné dans la liste déroulante.

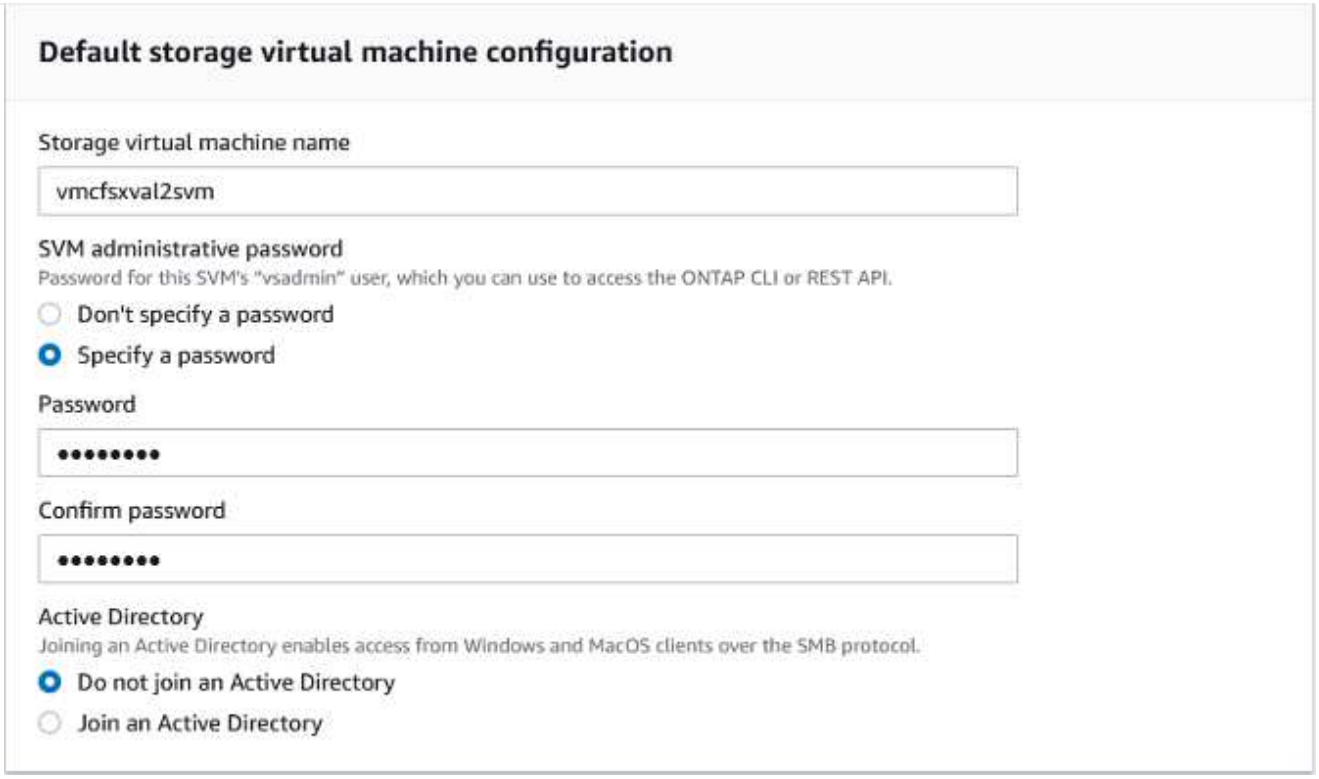


Dans la section mise en réseau, pour le cloud privé virtuel (VPC), choisissez le VPC (Virtual Private Cloud) approprié et les sous-réseaux préférés, ainsi que la table de routage. Dans ce cas, vmcfsx2.vpc est sélectionné dans la liste déroulante.

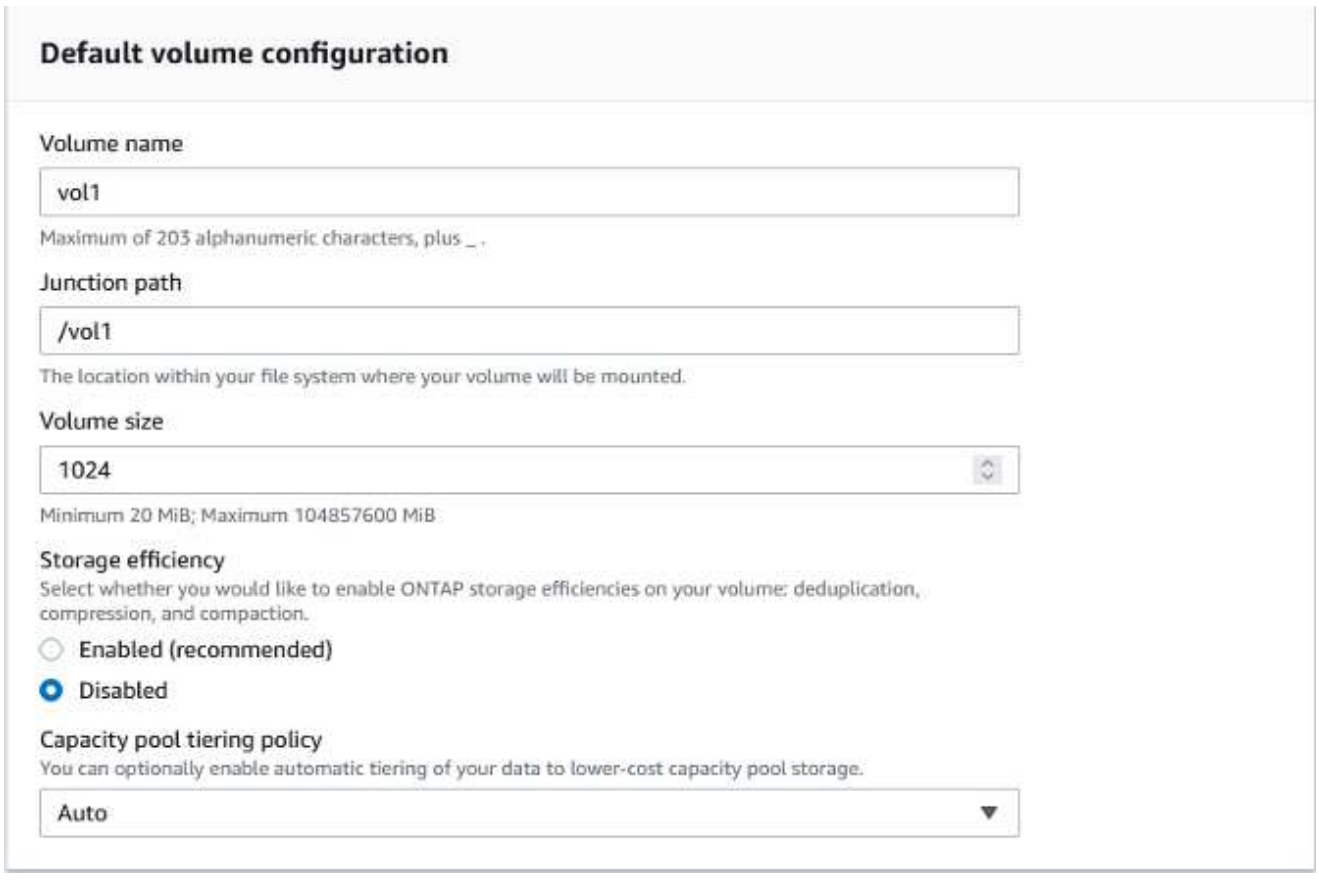
1. Dans la section sécurité et chiffrement, pour la clé de chiffrement, choisissez la clé de chiffrement AWS Key Management Service (KMS AWS) qui protège les données du système de fichiers au repos. Pour le mot de passe administrateur système de fichiers, entrez un mot de passe sécurisé pour l'utilisateur fsxadmin.



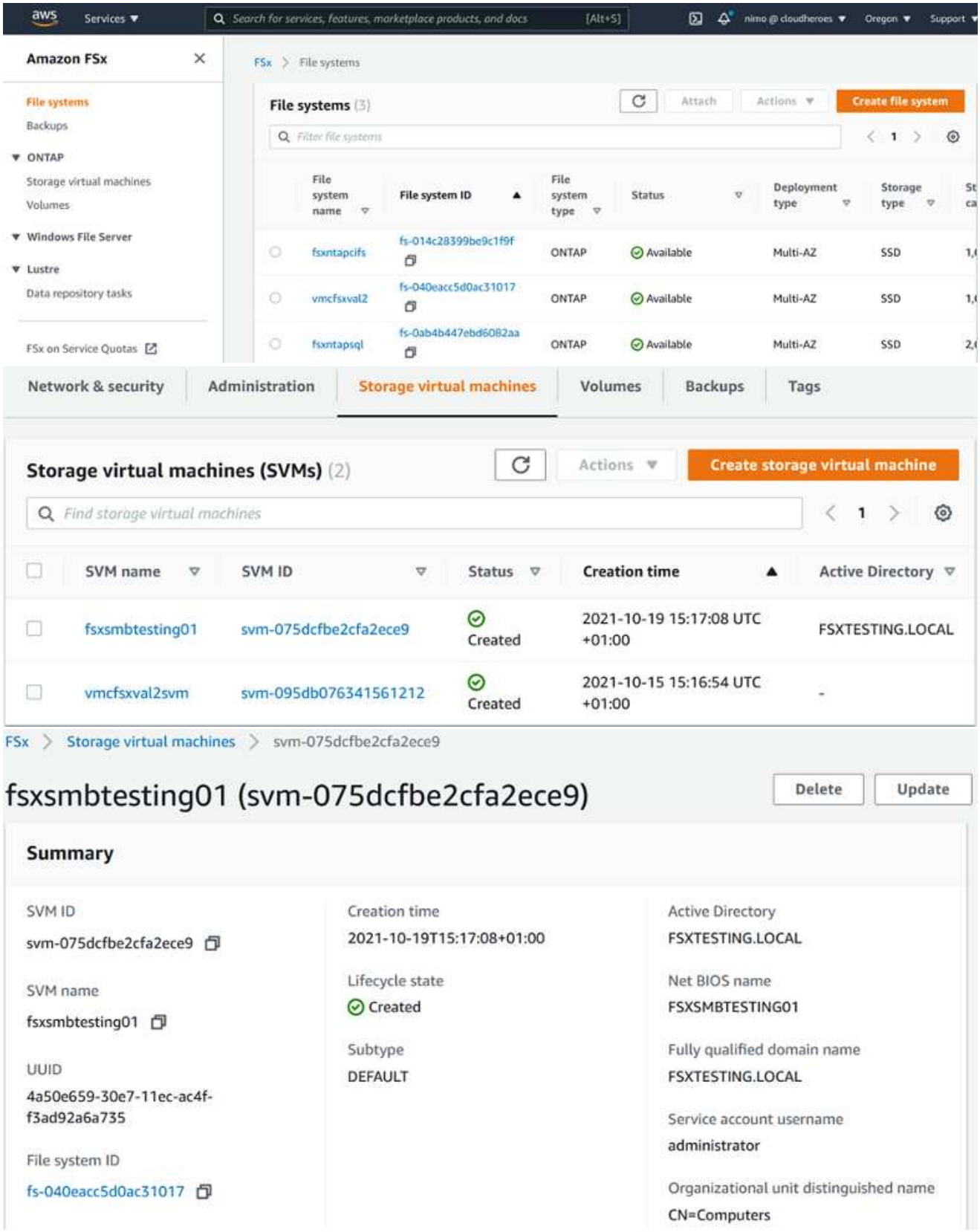
1. Sous l'ordinateur virtuel et spécifiez le mot de passe à utiliser avec vsadmin pour administrer le ONTAP via les API REST ou l'interface de ligne de commande. Si aucun mot de passe n'est spécifié, un utilisateur fsxadmin peut être utilisé pour administrer la SVM. Dans la section Active Directory, veillez à joindre Active Directory au SVM pour le provisionnement des partages SMB. Dans la section Configuration de Storage Virtual machine par défaut, indiquez un nom pour le stockage dans cette validation, les partages SMB sont provisionnés à l'aide d'un domaine Active Directory autogéré.



1. Dans la section Configuration du volume par défaut, spécifiez le nom et la taille du volume. Il s'agit d'un volume NFS. Pour l'efficacité du stockage, choisissez activé pour activer les fonctionnalités d'efficacité du stockage ONTAP (compression, déduplication et compaction) ou désactivez-les.



1. Vérifiez la configuration du système de fichiers indiquée sur la page Créer un système de fichiers.
2. Cliquez sur Créer un système de fichiers.

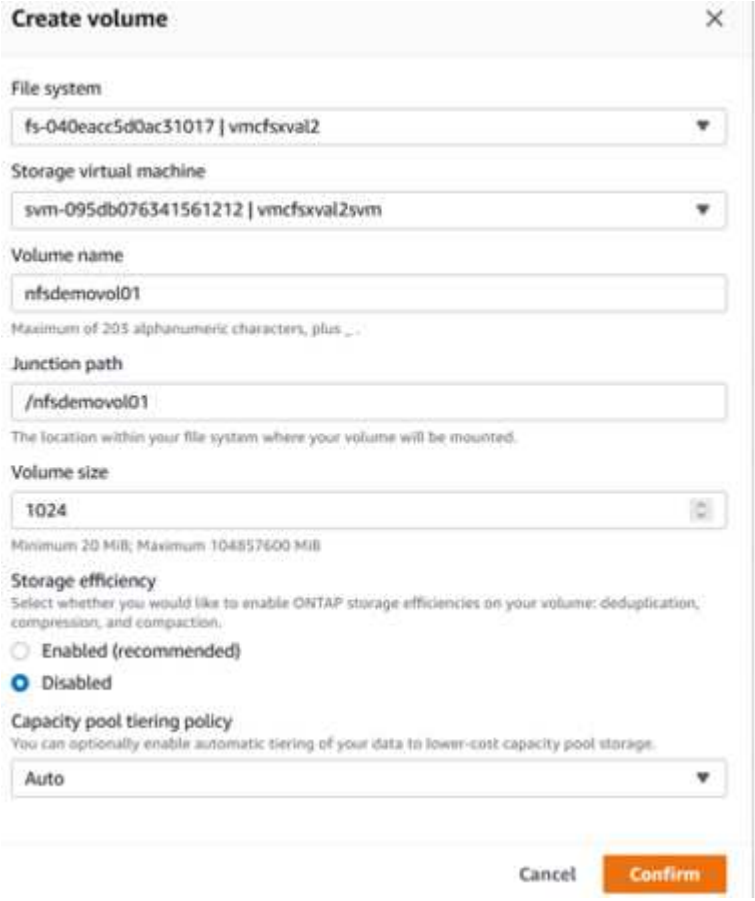


Pour plus d'informations, reportez-vous à la section "Mise en route avec Amazon FSX pour NetApp ONTAP".

Une fois le système de fichiers créé comme ci-dessus, créez le volume avec la taille et le protocole requis.

1. Ouvrez le "Console Amazon FSX".
2. Dans le volet de navigation de gauche, choisissez systèmes de fichiers, puis choisissez le système de fichiers ONTAP pour lequel vous souhaitez créer un volume.
3. Sélectionnez l'onglet volumes.
4. Sélectionnez l'onglet Créer un volume.
5. La boîte de dialogue Créer un volume s'affiche.

À des fins de démonstration, un volume NFS est créé dans cette section, sur laquelle il peut être facilement monté sur des machines virtuelles qui s'exécutent sur VMware Cloud sur AWS. nfsdemovol01 est créé comme décrit ci-dessous :



Montez le volume ONTAP FSX sur le client Linux

Pour monter le volume ONTAP FSX créé à l'étape précédente. Depuis les VM Linux dans VMC sur AWS SDDC, effectuez les opérations suivantes :

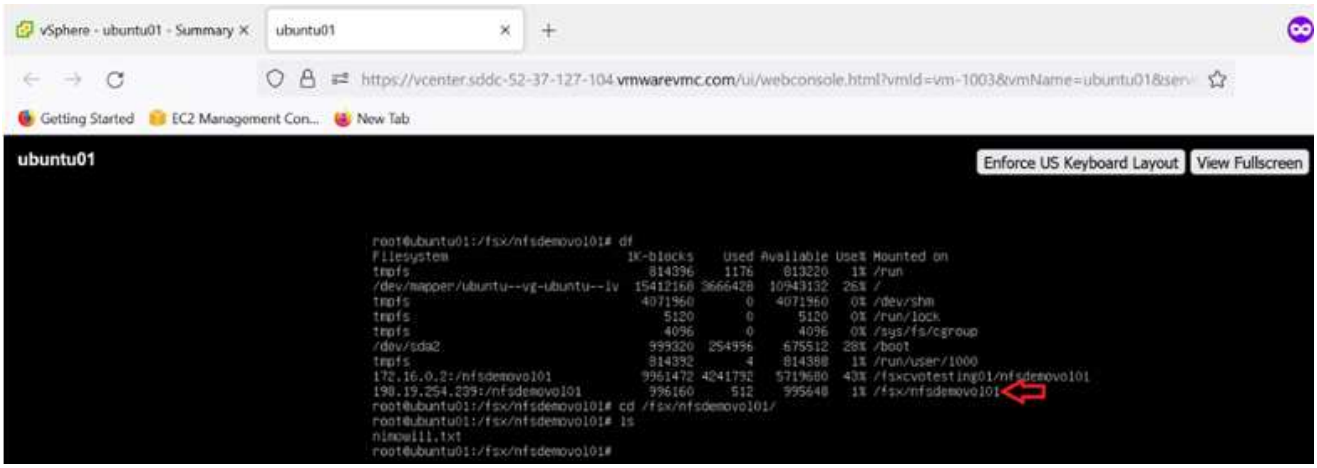
1. Connectez-vous à l'instance Linux désignée.
2. Ouvrez un terminal sur l'instance à l'aide de Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
3. Créer un répertoire pour le point de montage du volume avec la commande suivante :

```
 $ sudo mkdir /fsx/nfsdemovol01
. Montez le volume NFS Amazon FSX pour NetApp ONTAP dans le
répertoire créé à l'étape précédente.
```

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. Une fois exécutée, exécutez la commande df pour valider le montage.



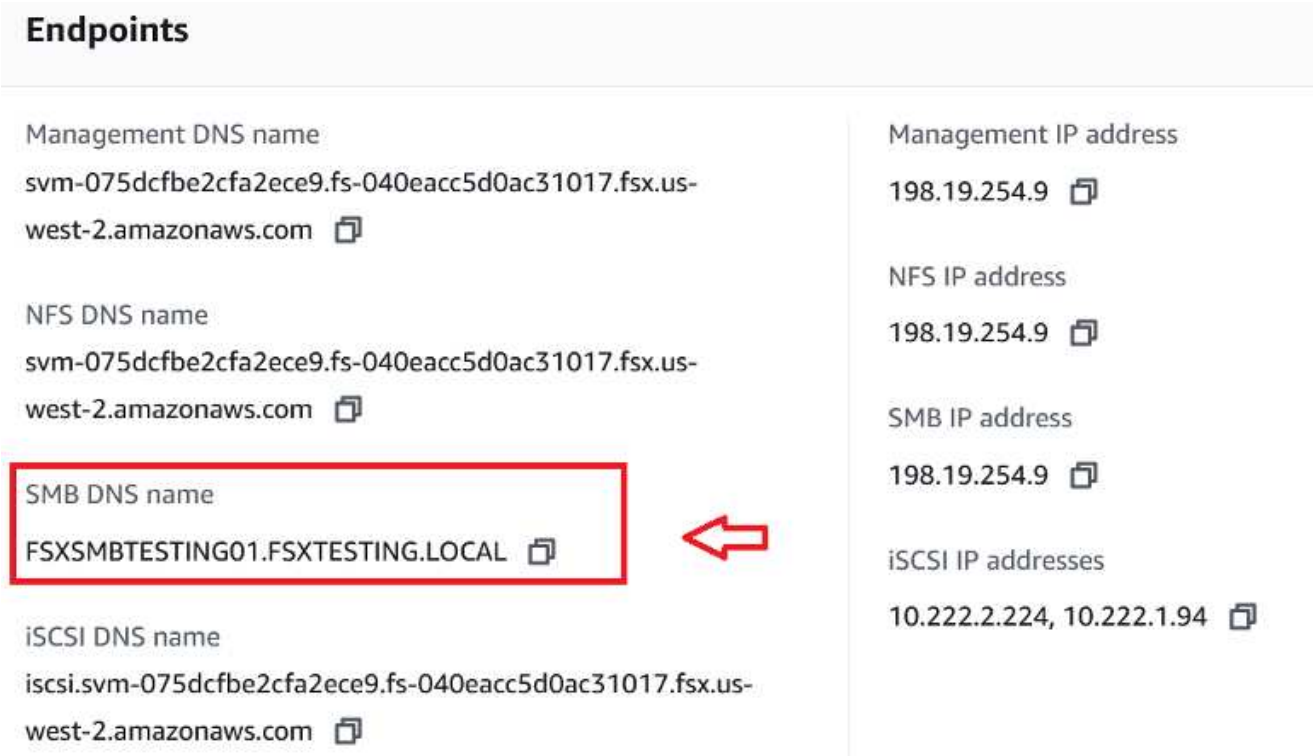
Montez le volume ONTAP FSX sur le client Linux

Connexion de volumes ONTAP FSX aux clients Microsoft Windows

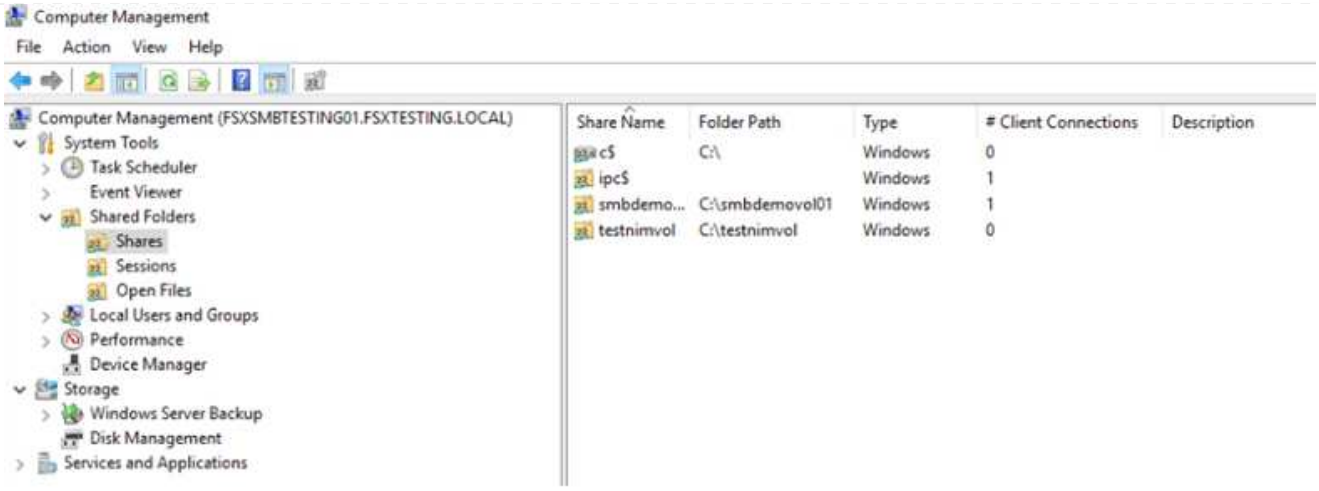
Pour gérer et mapper des partages de fichiers sur un système de fichiers Amazon FSX, l'interface graphique dossiers partagés doit être utilisée.

1. Ouvrez le menu Démarrer et exécutez fsmgmt.msc en utilisant Exécuter en tant qu'administrateur. Cette opération ouvre l'outil GUI dossiers partagés.
2. Cliquez sur action > toutes les tâches et choisissez connexion à un autre ordinateur.
3. Pour un autre ordinateur, entrez le nom DNS de la machine virtuelle de stockage (SVM). Par exemple, FSXSMBTESTIN01.FSXTESTING.LOCAL est utilisé dans cet exemple.

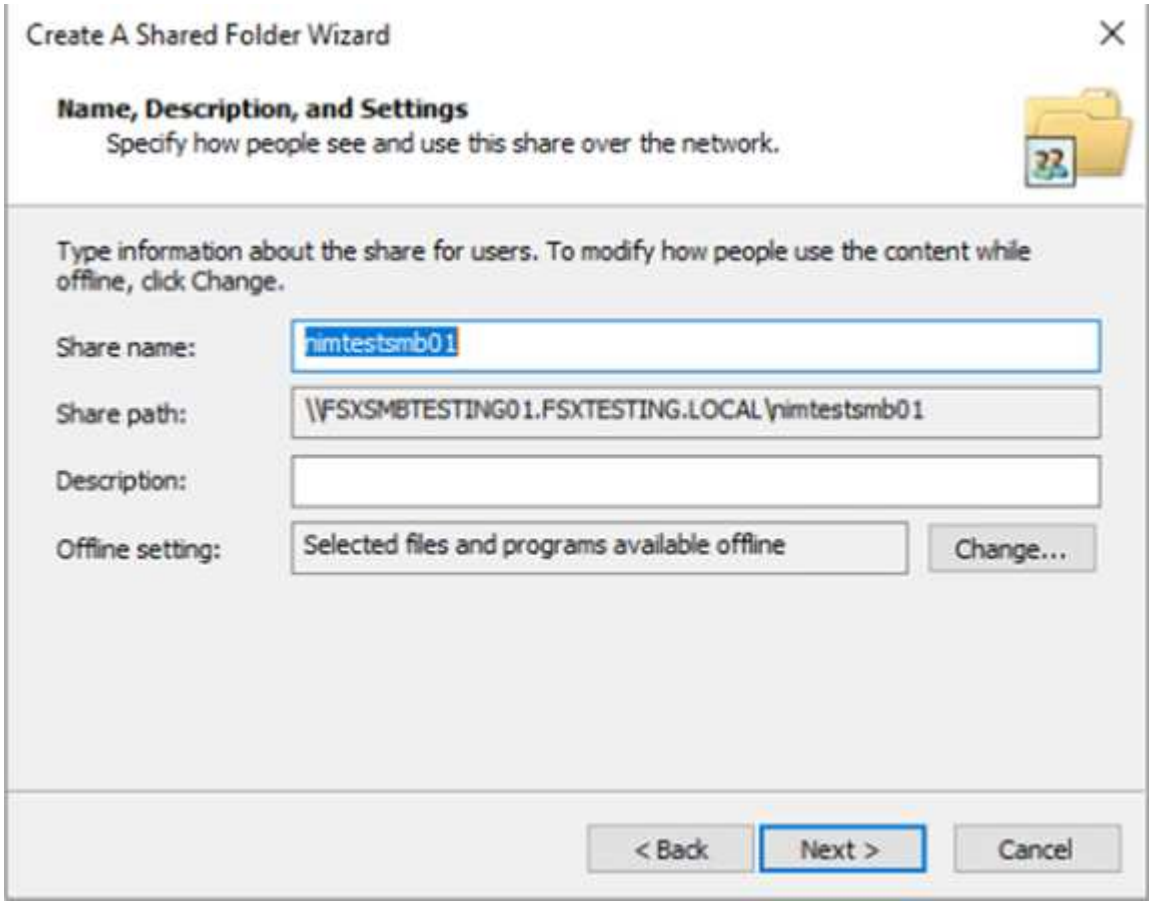
> TP recherchez le nom DNS du SVM sur la console Amazon FSX, choisissez Storage Virtual machines, choisissez SVM, puis faites défiler jusqu'aux terminaux pour trouver le nom DNS SMB. Cliquez sur OK. Le système de fichiers Amazon FSX s'affiche dans la liste des dossiers partagés.



1. Dans l'outil dossiers partagés, choisissez partages dans le volet gauche pour afficher les partages actifs pour le système de fichiers Amazon FSX.

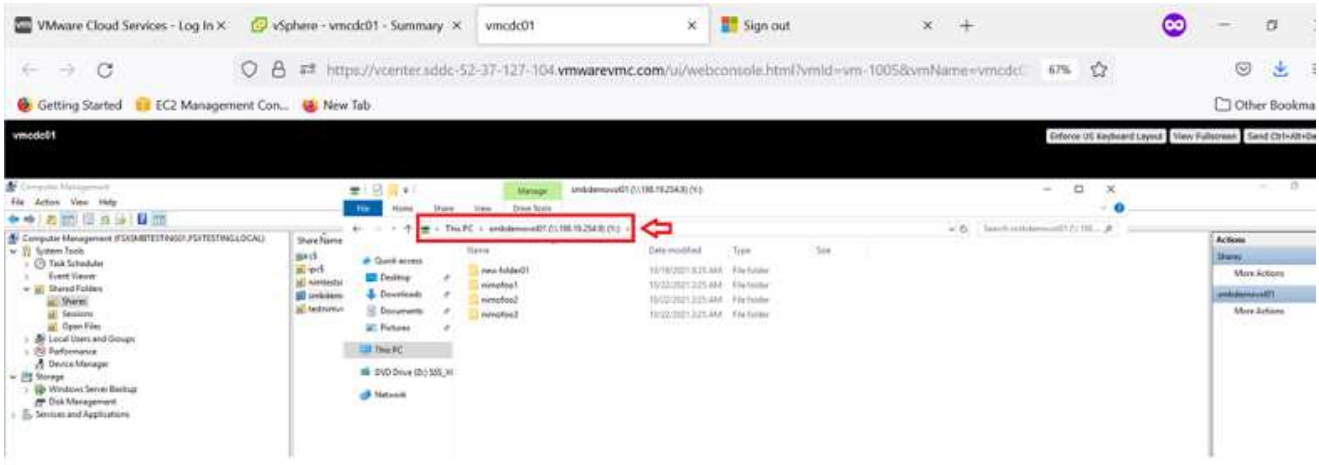


1. Choisissez un nouveau partage et suivez l'assistant Créer un dossier partagé.



Pour en savoir plus sur la création et la gestion de partages SMB sur un système de fichiers Amazon FSX, reportez-vous à la section "Création de partages SMB".

1. Une fois la connectivité en place, le partage SMB peut être connecté et utilisé pour les données d'application. Pour ce faire, copiez le chemin du partage et utilisez l'option Map Network Drive pour monter le volume sur la machine virtuelle exécutée sur VMware Cloud sur le SDDC AWS.



Connectez un LUN FSX pour NetApp ONTAP à un hôte utilisant iSCSI

Connectez un LUN FSX pour NetApp ONTAP à un hôte utilisant iSCSI

Le trafic iSCSI pour FSX traverse la passerelle de transit VMware Transit Connect/AWS via les routes fournies dans la section précédente. Pour configurer un LUN dans Amazon FSX pour NetApp ONTAP, suivez la documentation qui s'y trouve "ici".

Sur les clients Linux, assurez-vous que le démon iSCSI est en cours d'exécution. Une fois les LUN provisionnées, reportez-vous aux conseils détaillés sur la configuration iSCSI avec Ubuntu (par exemple) "ici".

Dans ce document, la connexion du LUN iSCSI à un hôte Windows est décrite ci-dessous :

Provisionnement d'un LUN dans FSX pour NetApp ONTAP :

1. Accédez à l'interface de ligne de commande de NetApp ONTAP à l'aide du port de gestion du système FSX pour le système de fichiers ONTAP.
2. Créer les LUN avec la taille requise, comme indiqué dans la sortie du dimensionnement.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

Dans cet exemple, nous avons créé une LUN de taille 5g (5368709120).

1. Créez les igroups nécessaires pour contrôler quels hôtes ont accès à des LUN spécifiques.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
-----------------------------------

vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

Deux entrées ont été affichées.

1. Mappez les LUN sur des igroups à l'aide de la commande suivante :

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------- ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

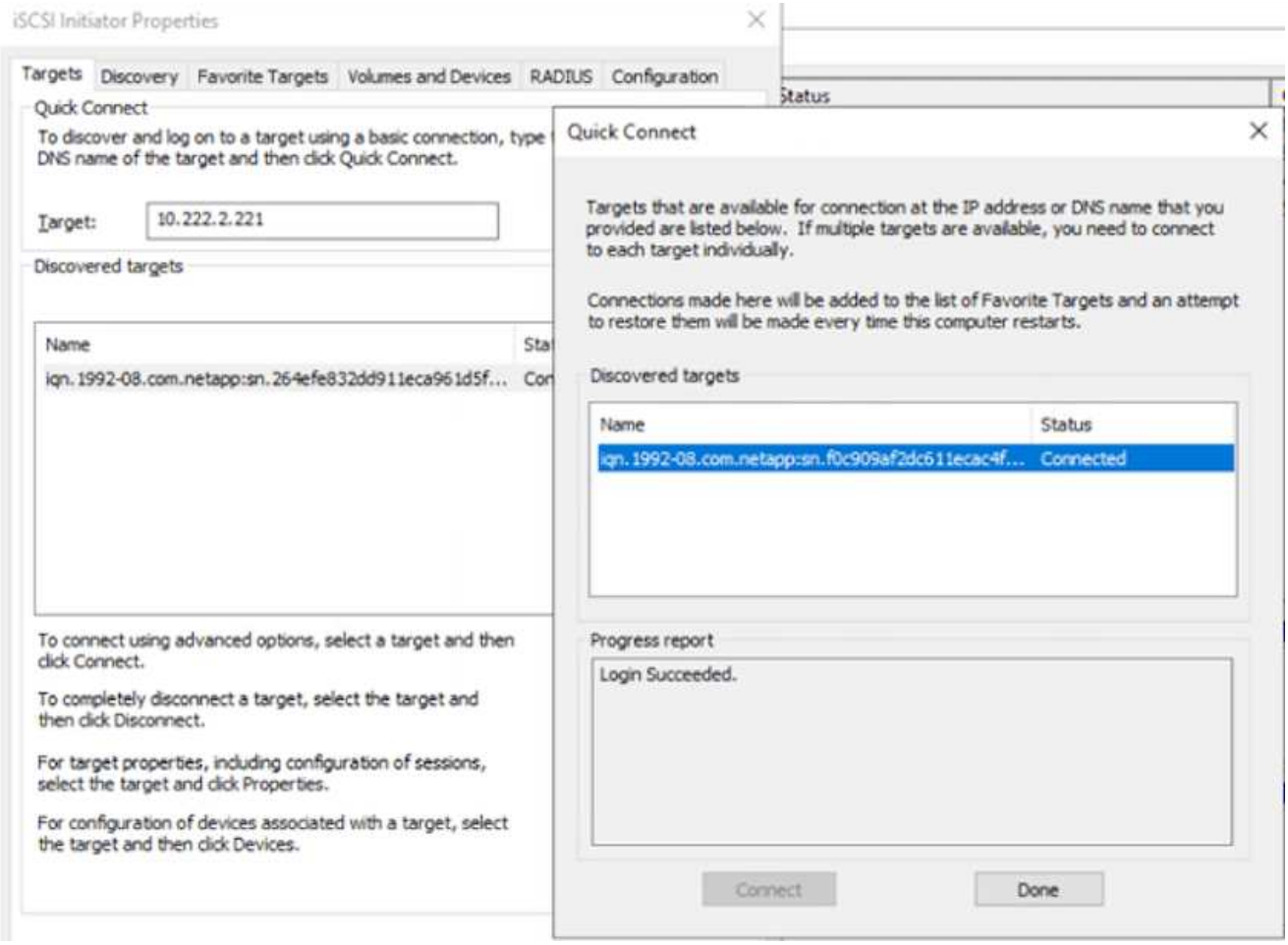
Deux entrées ont été affichées.

1. Connectez le nouveau LUN provisionné à une machine virtuelle Windows :

Pour connecter le nouveau LUN tor à un hôte Windows résidant sur le cloud VMware dans AWS SDDC, effectuez les opérations suivantes :

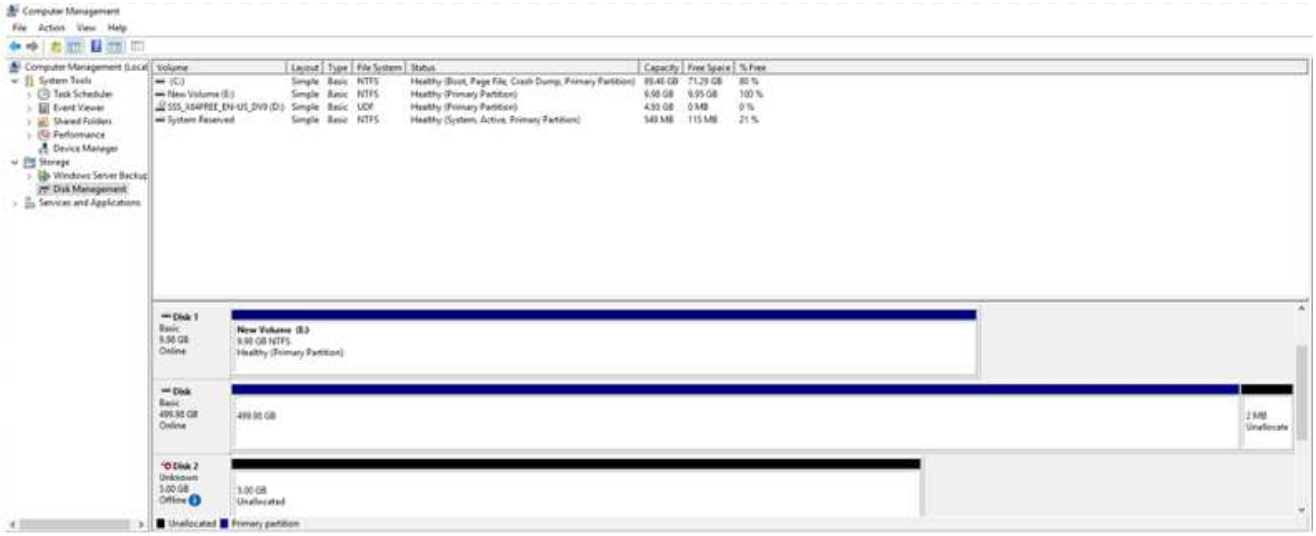
1. RDP sur la machine virtuelle Windows hébergée sur le SDDC VMware Cloud pour AWS.
2. Accédez à Server Manager > Tableau de bord > Outils > initiateur iSCSI pour ouvrir la boîte de dialogue Propriétés de l'initiateur iSCSI.
3. Dans l'onglet découverte, cliquez sur Discover Portal ou Add Portal, puis entrez l'adresse IP du port cible iSCSI.
4. Dans l'onglet cibles, sélectionnez la cible découverte, puis cliquez sur connexion ou connexion.
5. Sélectionnez Activer Multipath, puis sélectionnez "Restaurer automatiquement cette connexion au démarrage de l'ordinateur" ou "Ajouter cette connexion à la liste des cibles favorites". Cliquez sur Avancé.

> L'hôte Windows doit disposer d'une connexion iSCSI à chaque nœud du cluster. Le DSM natif sélectionne les meilleurs chemins d'accès à utiliser.



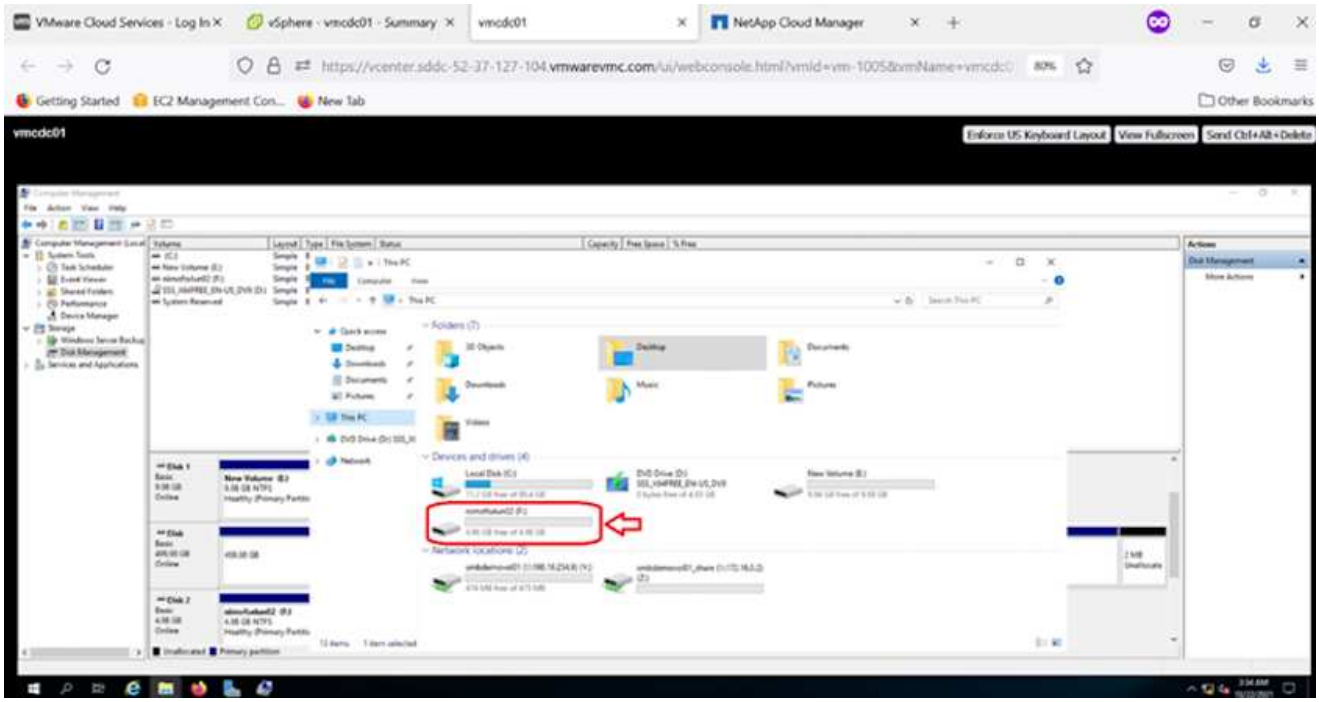
Les LUN de la machine virtuelle de stockage (SVM) apparaissent sous forme de disques pour l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclencher une nouvelle analyse manuelle pour détecter les disques en procédant comme suit :

1. Ouvrez l'utilitaire de gestion de l'ordinateur Windows : Démarrer > Outils d'administration > gestion de l'ordinateur.
2. Développez le nœud stockage dans l'arborescence de navigation.
3. Cliquez sur gestion des disques.
4. Cliquez sur action > Rescan Disks.



Lorsqu'un nouvel LUN est accédé pour la première fois par l'hôte Windows, il n'a pas de partition ni de système de fichiers. Initialisez la LUN et, éventuellement, formatez-la avec un système de fichiers en effectuant la procédure suivante :

1. Démarrez Windows Disk Management.
2. Cliquez avec le bouton droit de la souris sur la LUN, puis sélectionnez le type de disque ou de partition requis.
3. Suivez les instructions de l'assistant. Dans cet exemple, le lecteur F: Est monté.



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, ou CVO, est la solution de gestion des données cloud leader qui repose sur le logiciel de stockage ONTAP de NetApp, disponible de façon native dans Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s’agit d’une version Software-defined de ONTAP qui utilise le stockage cloud natif. Vous pouvez ainsi utiliser le même logiciel de stockage dans le cloud et sur site, limitant ainsi la nécessité de former à nouveau votre personnel IT à des méthodes entièrement nouvelles de gestion des données.

Ce logiciel permet au client de déplacer des données de la périphérie, vers le data Center, puis vers le cloud, et inversement, en réunissant votre cloud hybride, le tout géré à l’aide d’une console de gestion centralisée, NetApp Cloud Manager.

De par sa conception, CVO fournit des performances extrêmes et des fonctionnalités avancées de gestion de données pour répondre aux applications les plus exigeantes dans le cloud

Cloud Volumes ONTAP (CVO) comme stockage connecté à l’invité

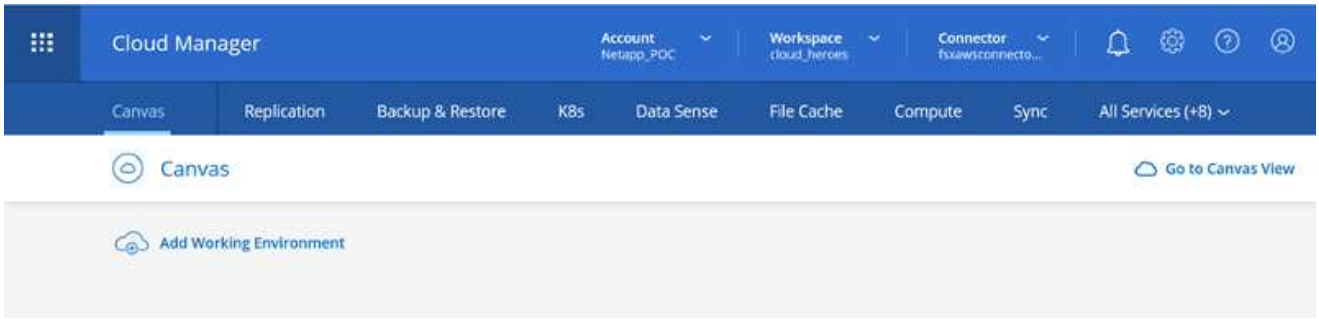
Déploiement de la nouvelle instance Cloud Volumes ONTAP dans AWS (faites vous-même)

Les partages et les LUN Cloud Volumes ONTAP peuvent être montés sur les VM créées dans le cloud VMware dans un environnement SDDC d'AWS. Les volumes peuvent également être montés sur des clients Windows Linux natifs d'AWS VM, et les LUN sont accessibles sur des clients Linux ou Windows en tant que périphériques de blocs lorsqu'ils sont montés sur iSCSI, car Cloud Volumes ONTAP prend en charge les protocoles iSCSI, SMB et NFS. Les volumes Cloud Volumes ONTAP peuvent être configurés en quelques étapes simples.

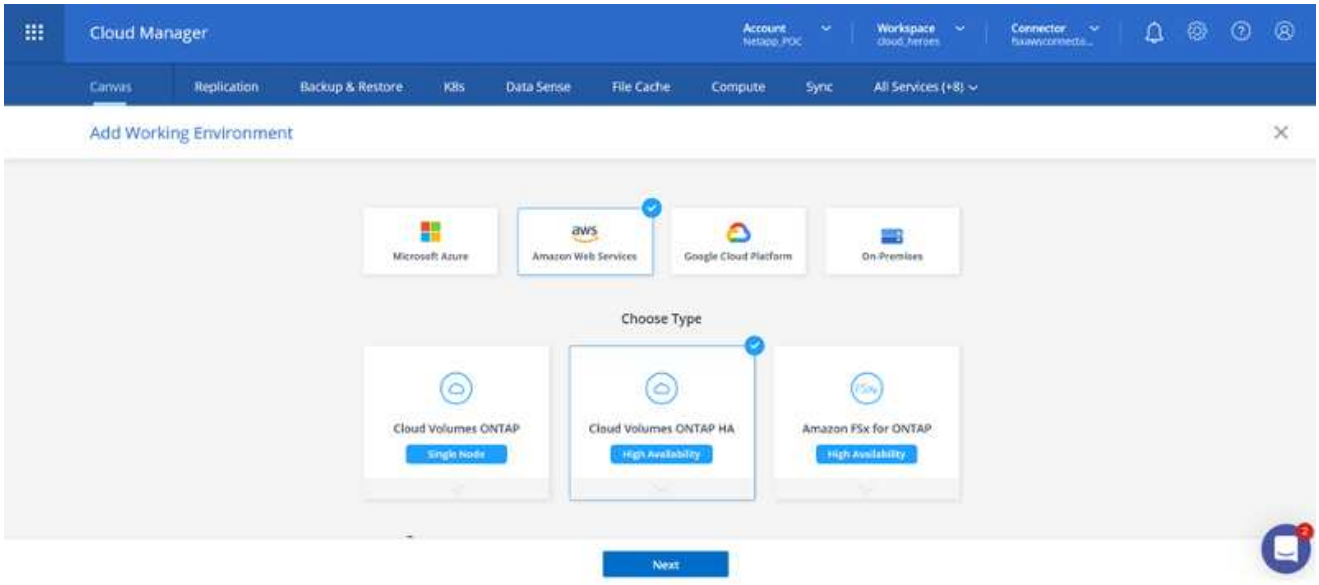
Pour répliquer des volumes depuis un environnement sur site vers le cloud à des fins de reprise d'activité ou de migration, établissez une connectivité réseau vers AWS à l'aide d'un VPN site à site ou de DirectConnect. La réplication des données entre les sites et Cloud Volumes ONTAP n'est pas traitée dans ce document. Pour répliquer les données entre les systèmes Cloud Volumes ONTAP et sur site, consultez la section "Configuration de la réplication des données entre les systèmes".

Utilisez le "Plus outil de dimensionnement Cloud Volumes ONTAP" Pour dimensionner précisément les instances Cloud Volumes ONTAP. Surveillez également les performances sur site pour les utiliser comme entrées dans le dimensionnement Cloud Volumes ONTAP.

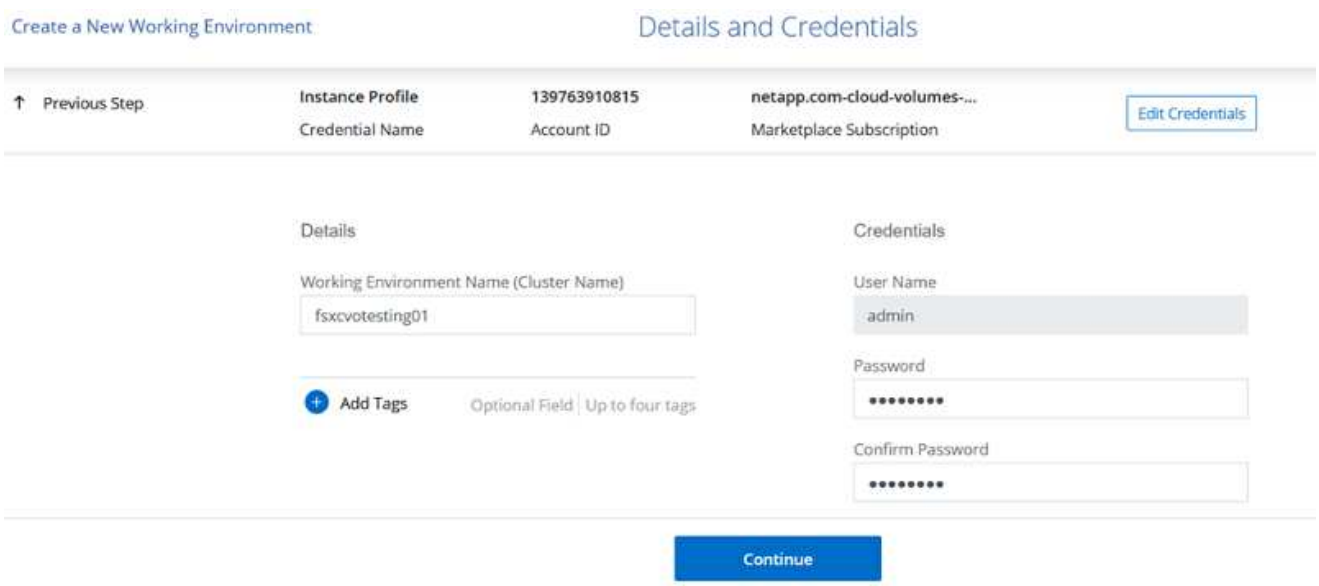
1. Connectez-vous à NetApp Cloud Central ; l'écran Fabric View s'affiche. Localisez l'onglet Cloud Volumes ONTAP et sélectionnez accéder à Cloud Manager. Une fois connecté, l'écran Canvas s'affiche.



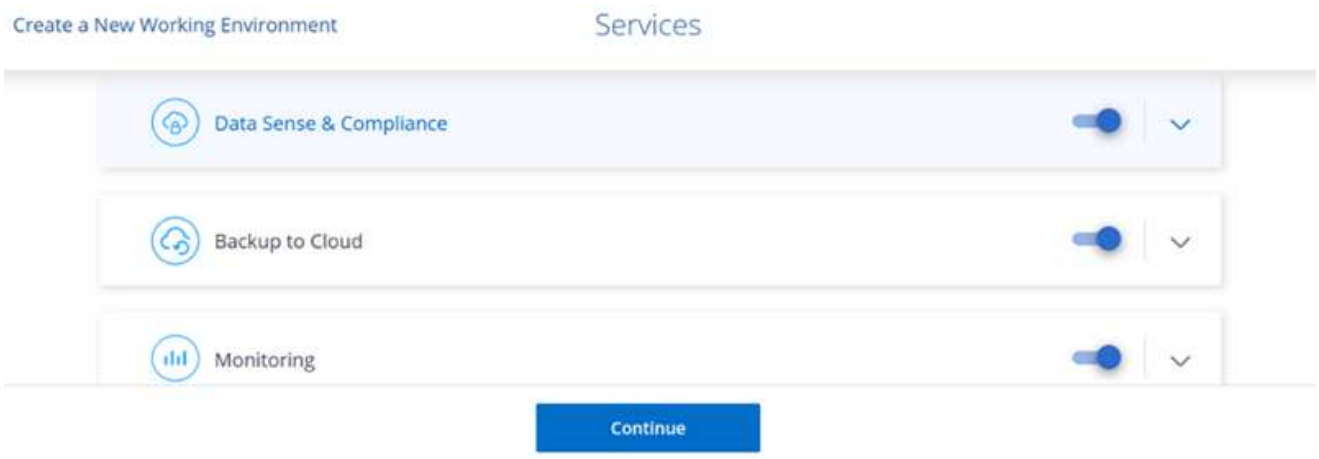
1. Sur la page d'accueil de Cloud Manager, cliquez sur Add a Working Environment, puis sélectionnez AWS comme cloud et le type de configuration système.



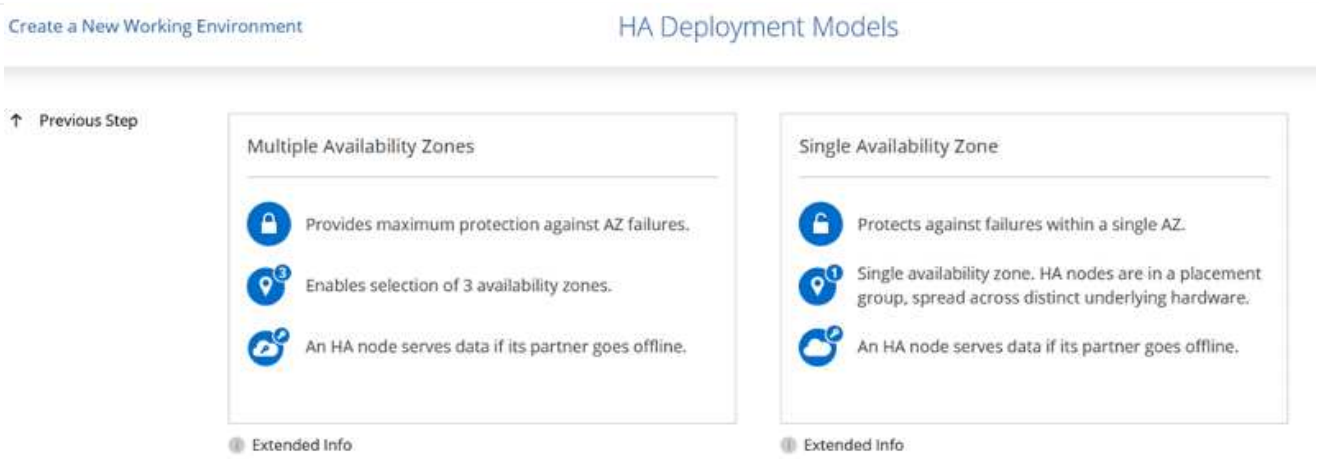
1. Fournissez les détails de l'environnement à créer, y compris le nom de l'environnement et les identifiants d'administrateur. Cliquez sur Continuer .



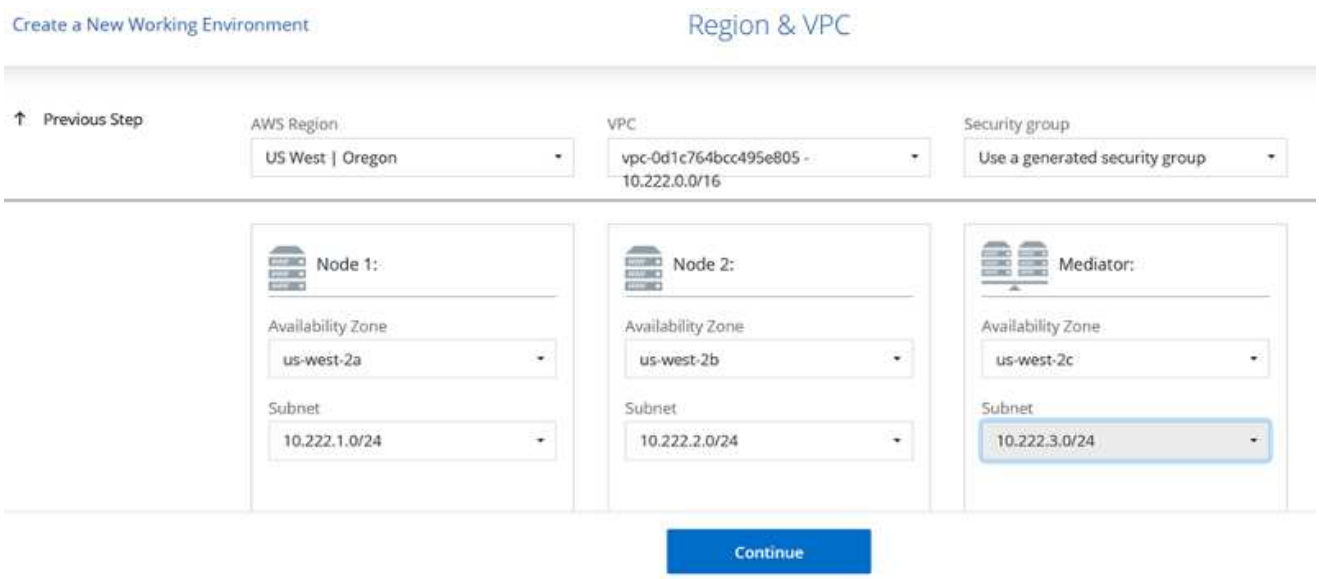
1. Sélectionnez les services complémentaires pour le déploiement Cloud Volumes ONTAP, notamment le classement BlueXP, la sauvegarde et la restauration BlueXP et Cloud Insights. Cliquez sur Continuer .



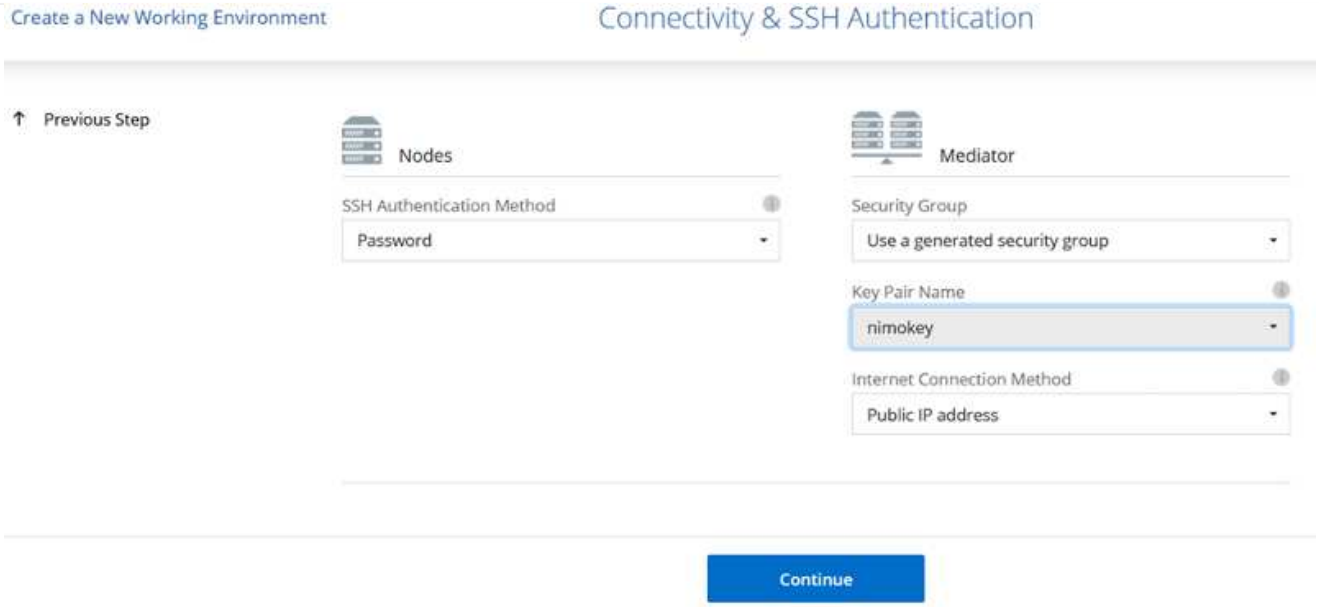
1. Sur la page modèles de déploiement HA, choisissez la configuration plusieurs zones de disponibilité.



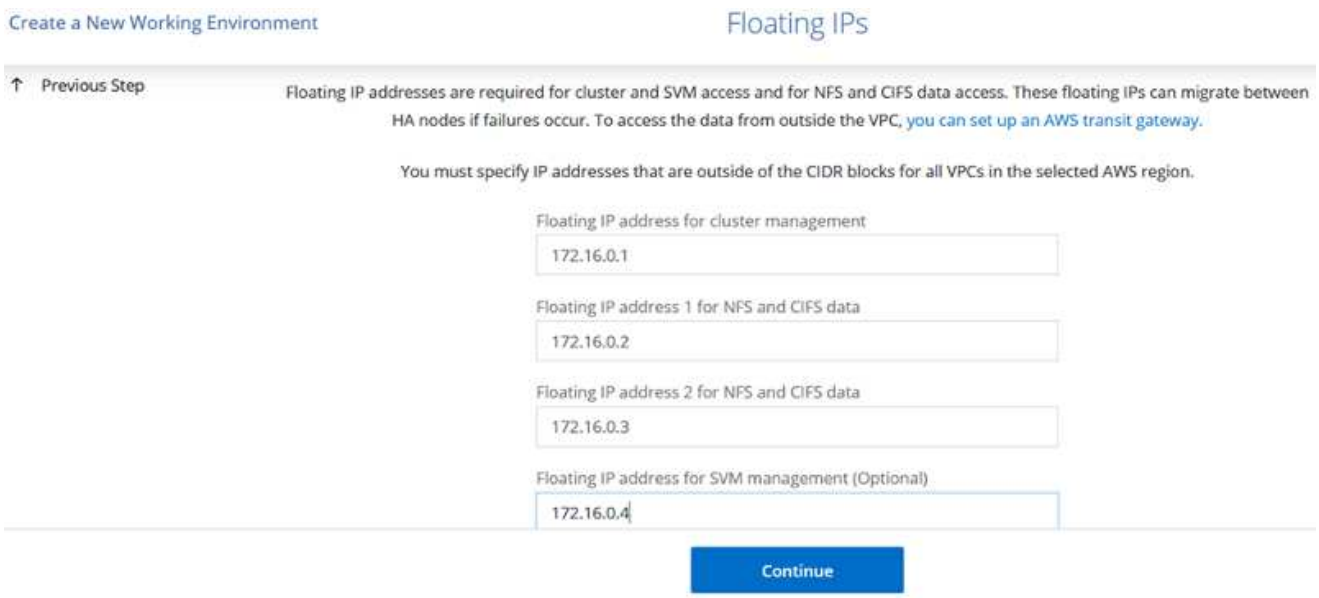
1. Sur la page région et VPC, entrez les informations du réseau, puis cliquez sur Continuer.



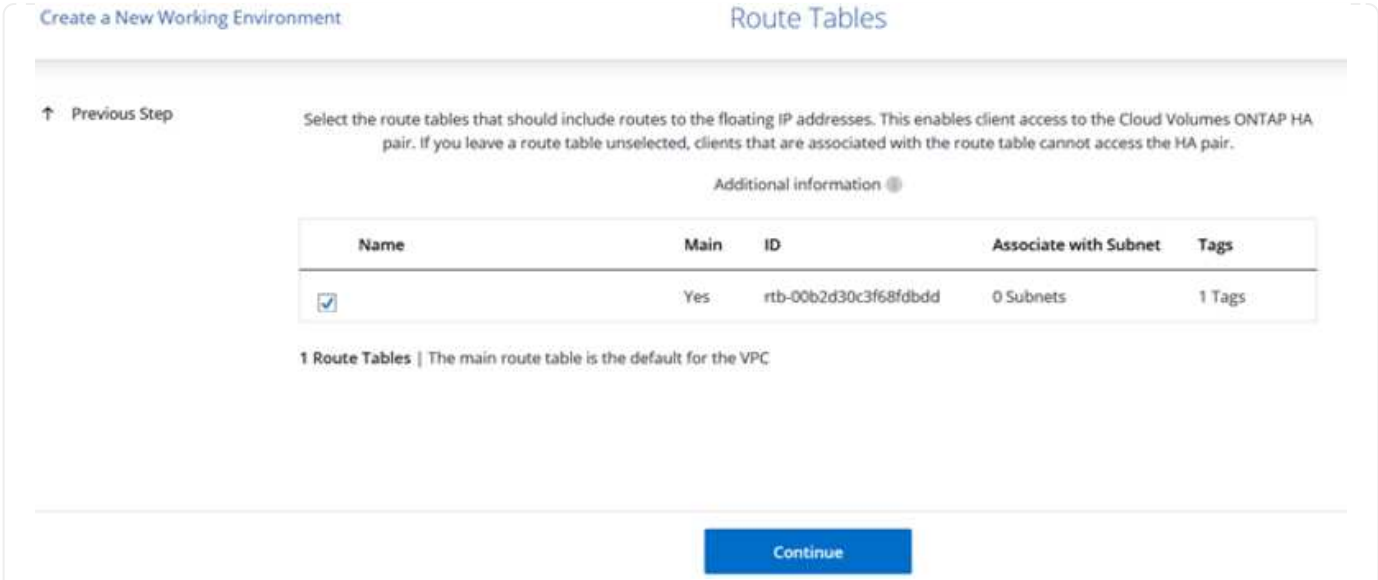
1. Sur la page Connectivité et authentification SSH, choisissez les méthodes de connexion pour la paire HA et le médiateur.



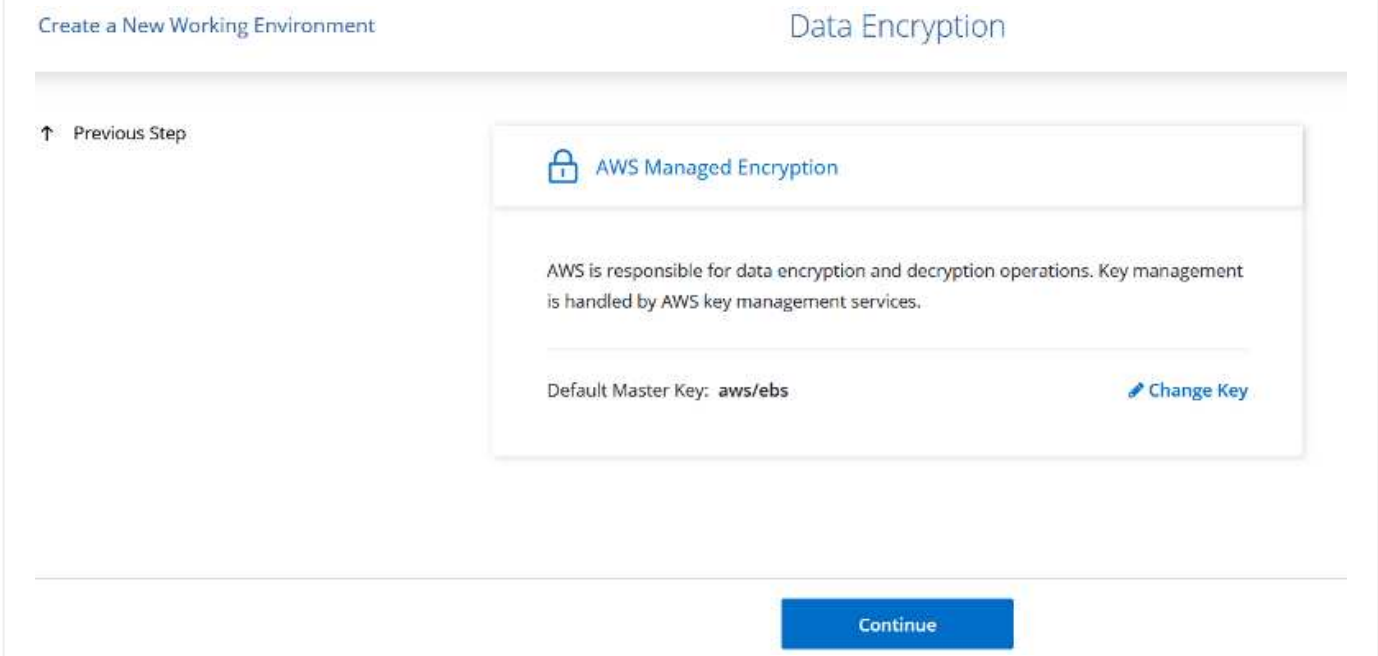
1. Spécifiez les adresses IP flottantes, puis cliquez sur Continuer.



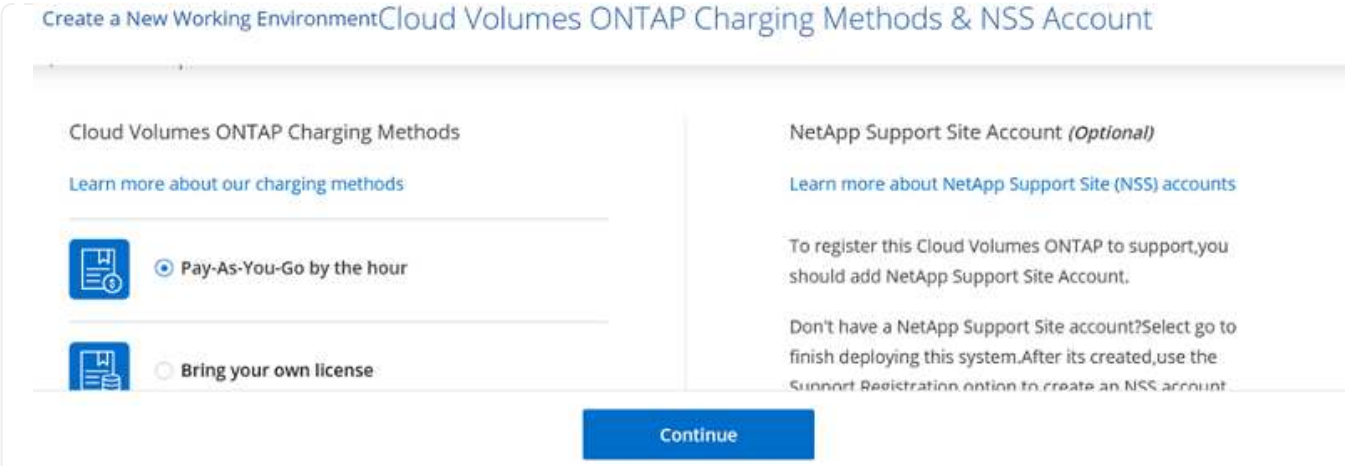
1. Sélectionnez les tables de routage appropriées pour inclure des routes vers les adresses IP flottantes, puis cliquez sur Continuer.



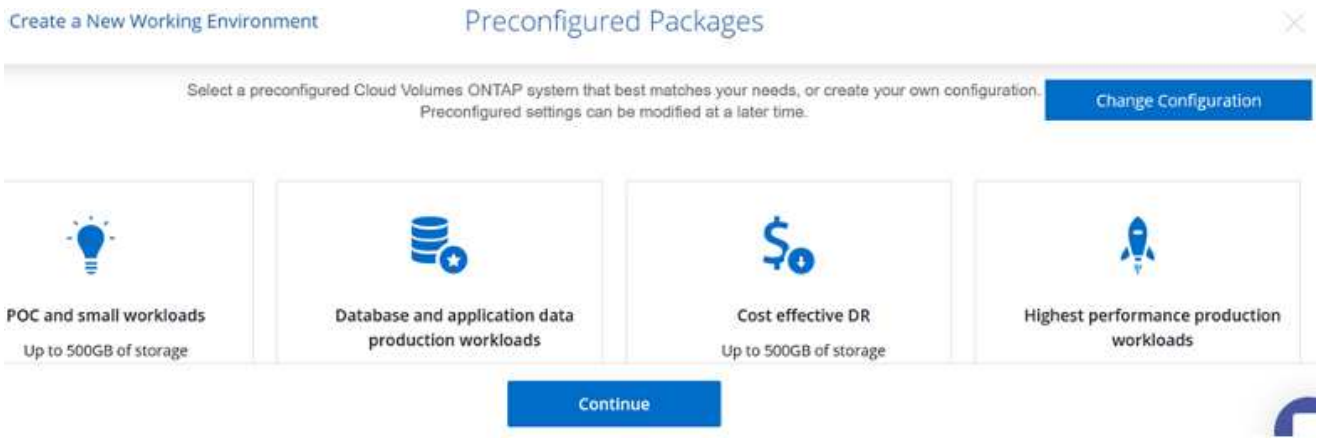
1. Sur la page chiffrement des données, choisissez le chiffrement géré par AWS.



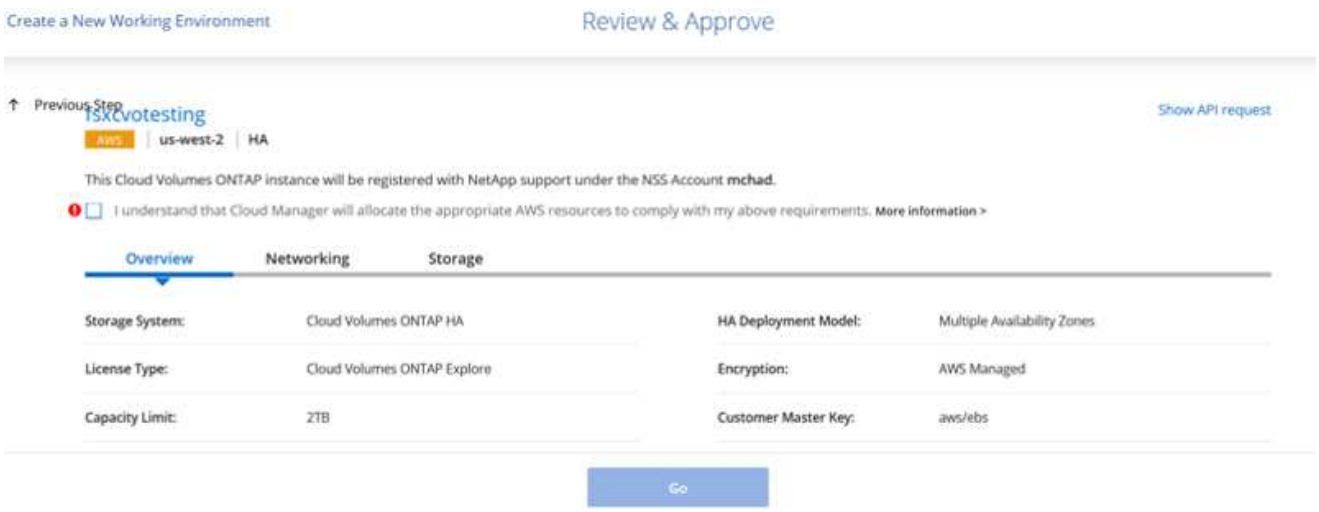
1. Sélectionnez l'option de licence : paiement à l'utilisation ou BYOL pour l'utilisation d'une licence existante. Dans cet exemple, l'option paiement à l'utilisation est utilisée.



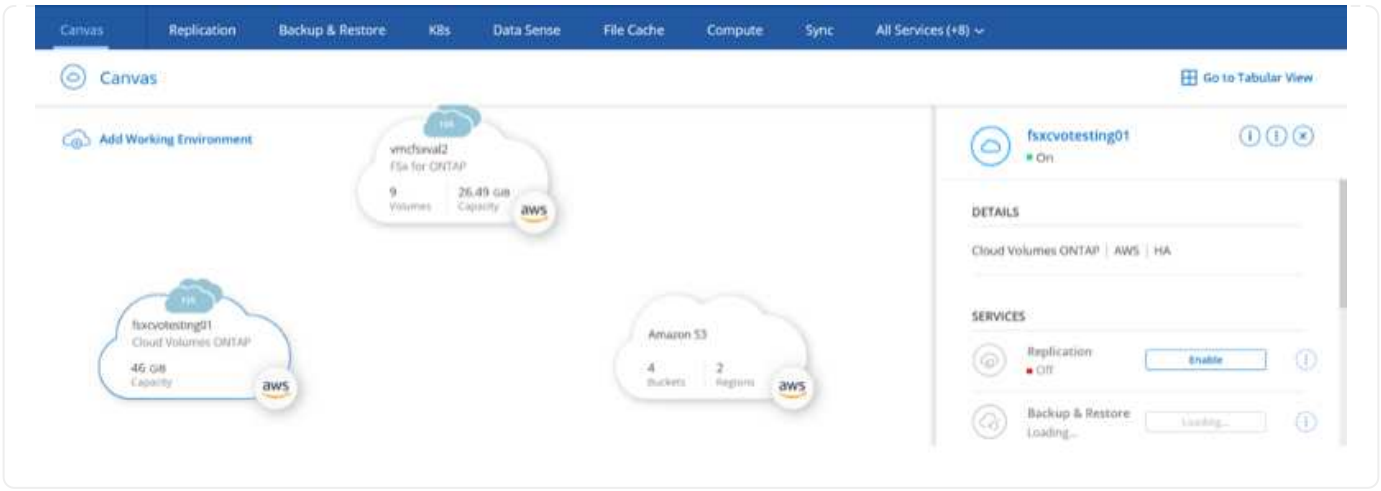
1. Sélectionnez parmi plusieurs packages préconfigurés disponibles en fonction du type de workload à déployer sur les machines virtuelles exécutées sur le cloud VMware sur AWS SDDC.



1. Sur la page révision et approbation, vérifiez et confirmez les sélections.pour créer l'instance Cloud Volumes ONTAP, cliquez sur Go.

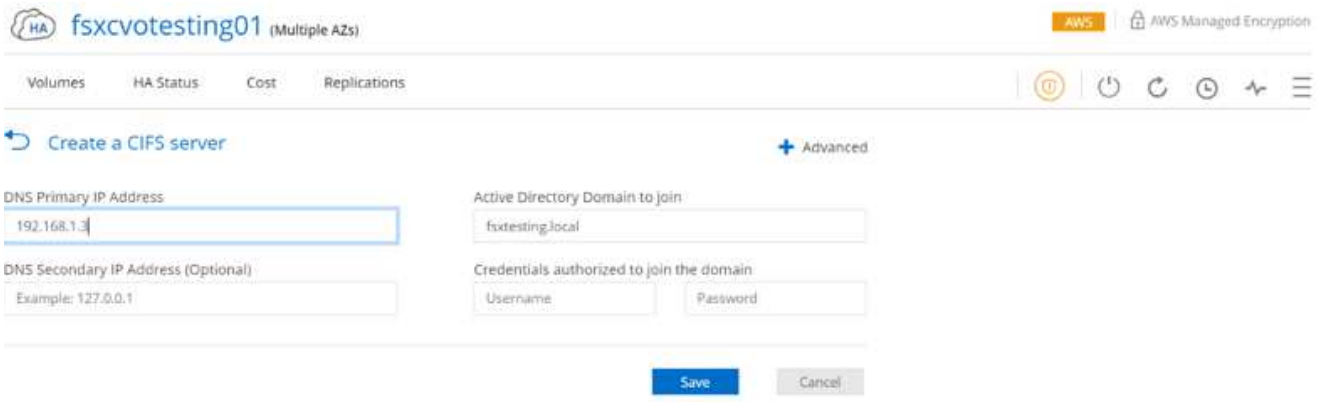


1. Une fois Cloud Volumes ONTAP provisionné, il apparaît dans les environnements de travail sur la page Canvas.

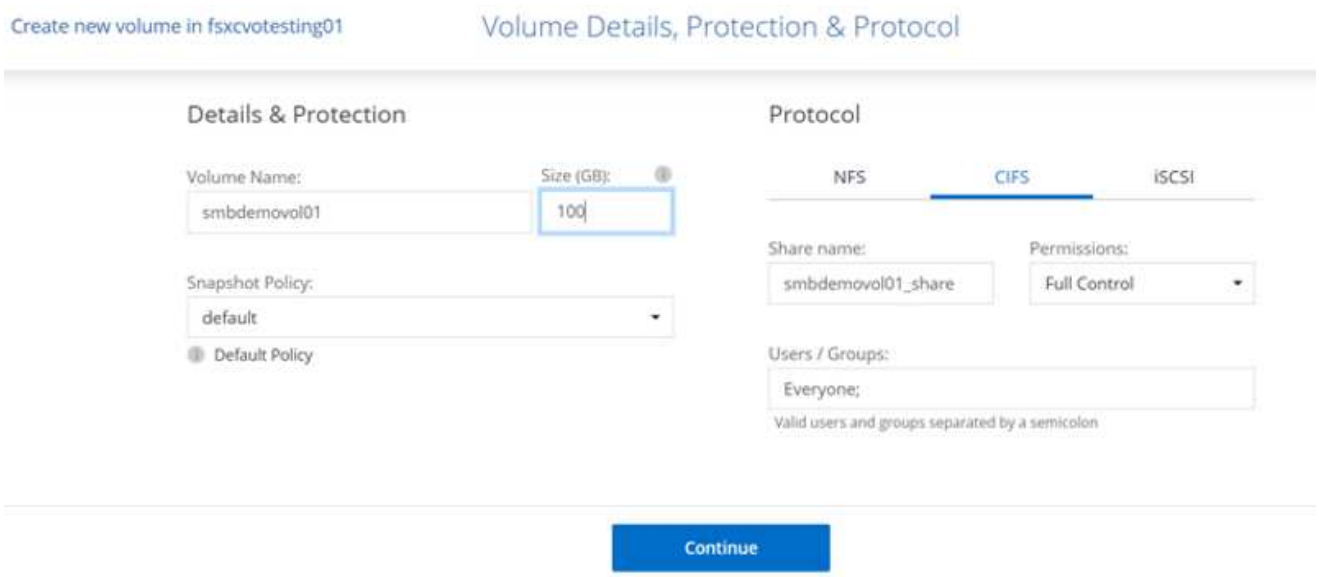

Canvas
Replication
Backup & Restore
K8s
Data Sense
File Cache
Compute
Sync
All Services (+8)
Canvas
Go to Tabular View
Add Working Environment
vmcfsaval2
FSx for ONTAP
9
Volumes
26.49 GiB
Capacity
fsxcvotesting01
Cloud Volumes ONTAP
46 GiB
Capacity
Amazon S3
4
Buckets
2
Regions
fsxcvotesting01
On
DETAILS
Cloud Volumes ONTAP | AWS | HA
SERVICES
Replication
Off
Enable
Backup & Restore
Loading...

Configurations supplémentaires pour les volumes SMB

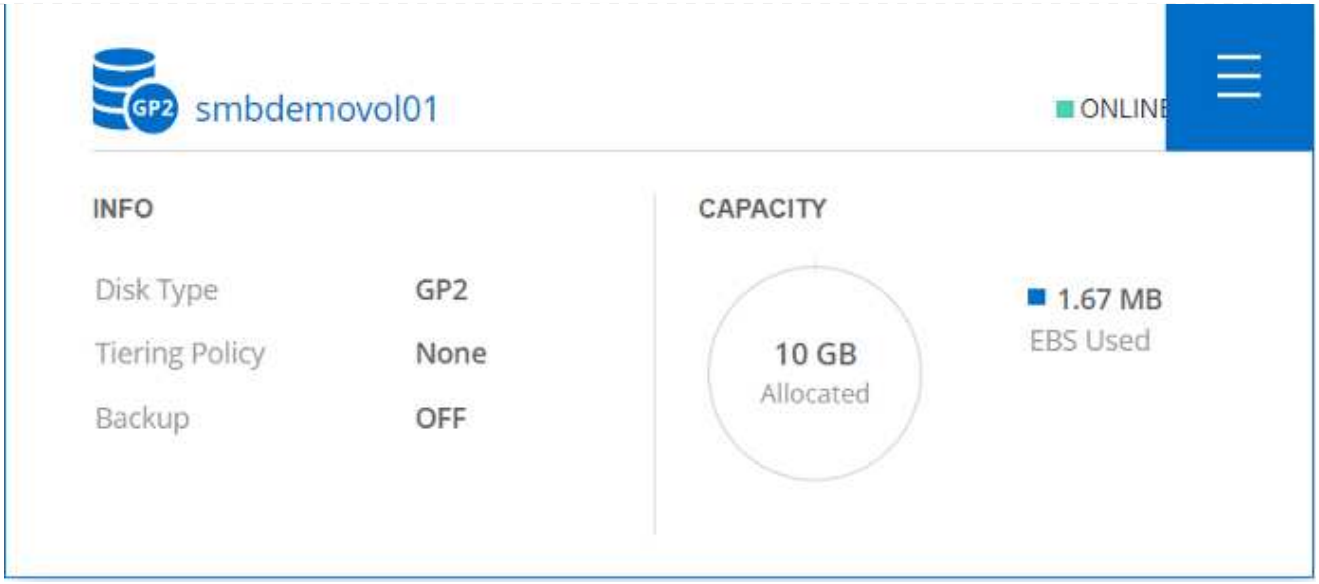
1. Une fois l'environnement de travail prêt, assurez-vous que le serveur CIFS est configuré avec les paramètres de configuration DNS et Active Directory appropriés. Cette étape est requise avant de pouvoir créer le volume SMB.



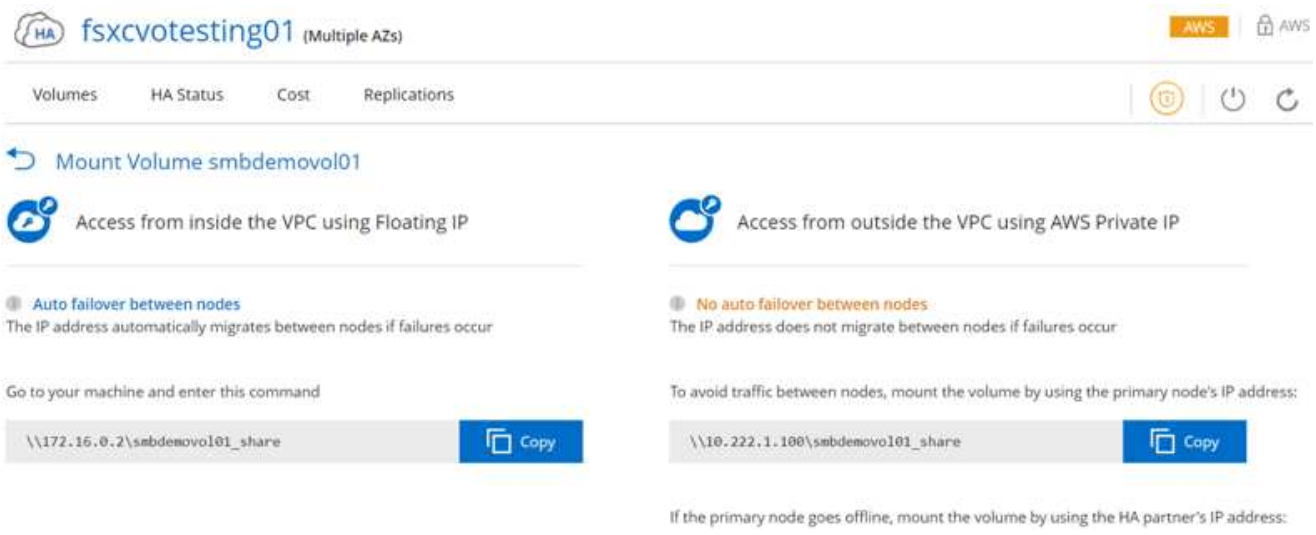
1. Sélectionnez l'instance CVO pour créer le volume, puis cliquez sur l'option Create Volume. Choisissez la taille appropriée et Cloud Manager choisit l'agrégat contenant ou utilisez un mécanisme d'allocation avancée pour placer sur un agrégat spécifique. Pour cette démonstration, SMB est sélectionné comme protocole.

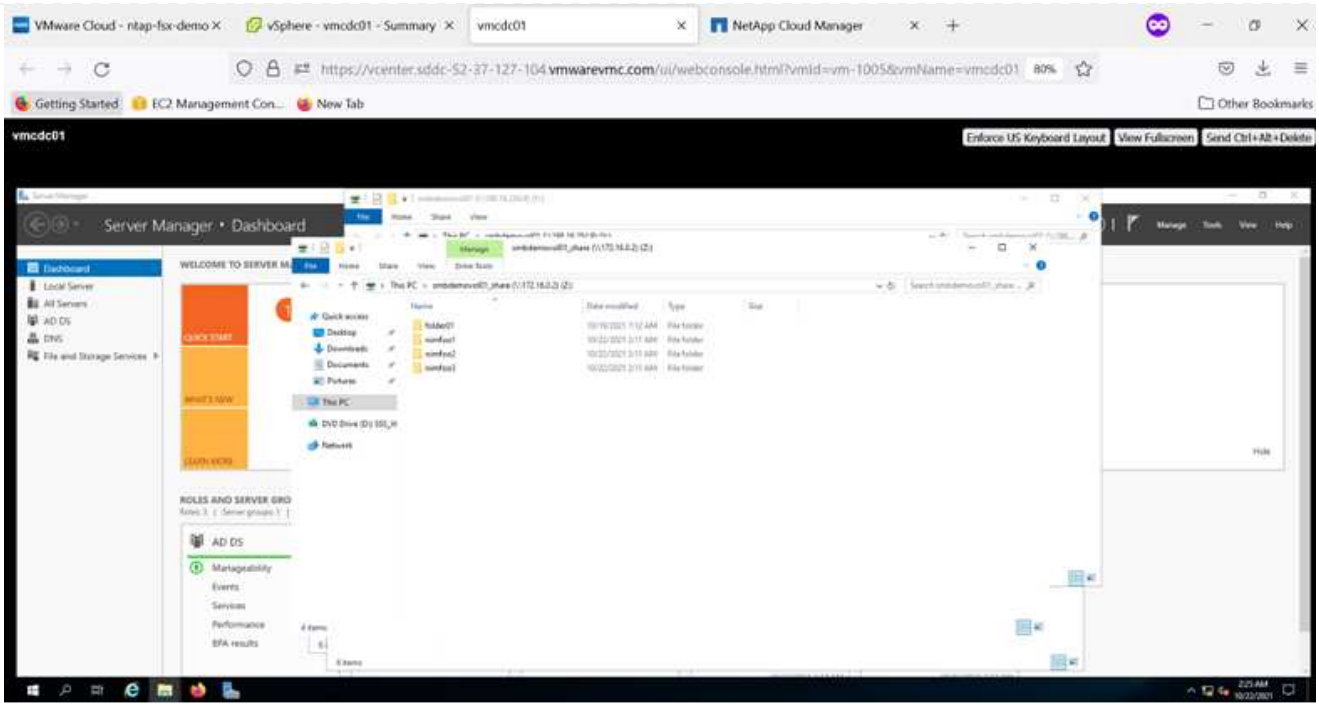


1. Une fois le volume provisionné, celui-ci est disponible sous le volet volumes. Comme un partage CIFS est provisionné, vous devez donner à vos utilisateurs ou groupes une autorisation aux fichiers et dossiers et vérifier que ces utilisateurs peuvent accéder au partage et créer un fichier.



1. Une fois le volume créé, utilisez la commande mount pour vous connecter au partage à partir de la machine virtuelle exécutée sur VMware Cloud dans les hôtes SDDC AWS.
2. Copiez le chemin suivant et utilisez l'option Map Network Drive pour monter le volume sur la machine virtuelle exécutée sur VMware Cloud dans AWS SDDC.

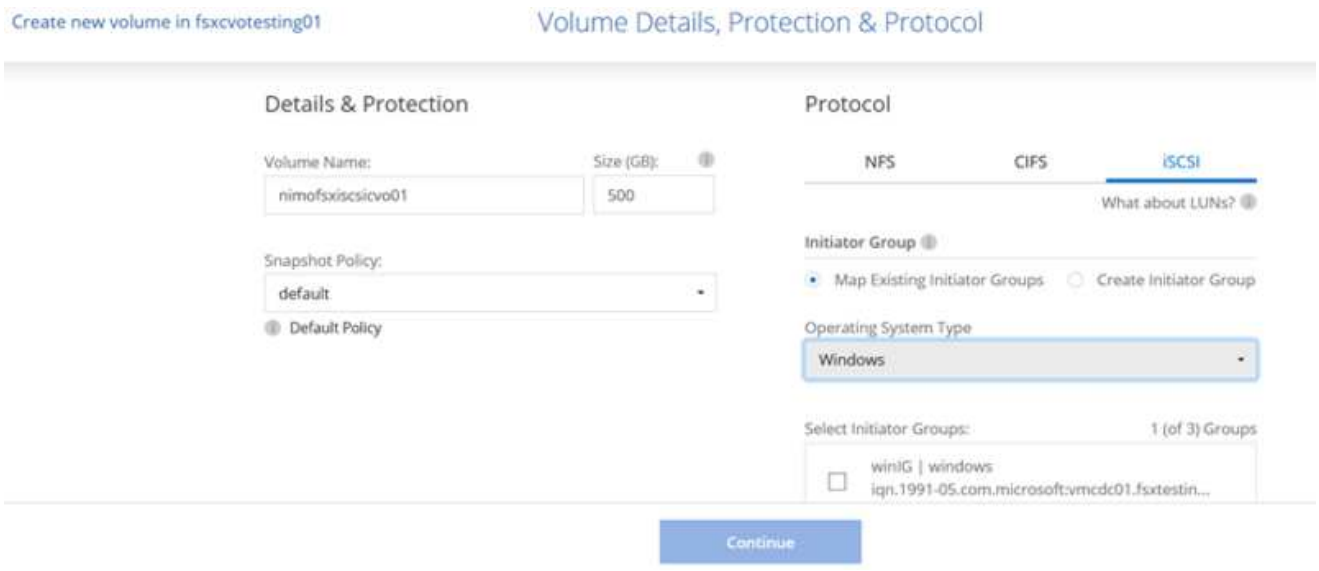


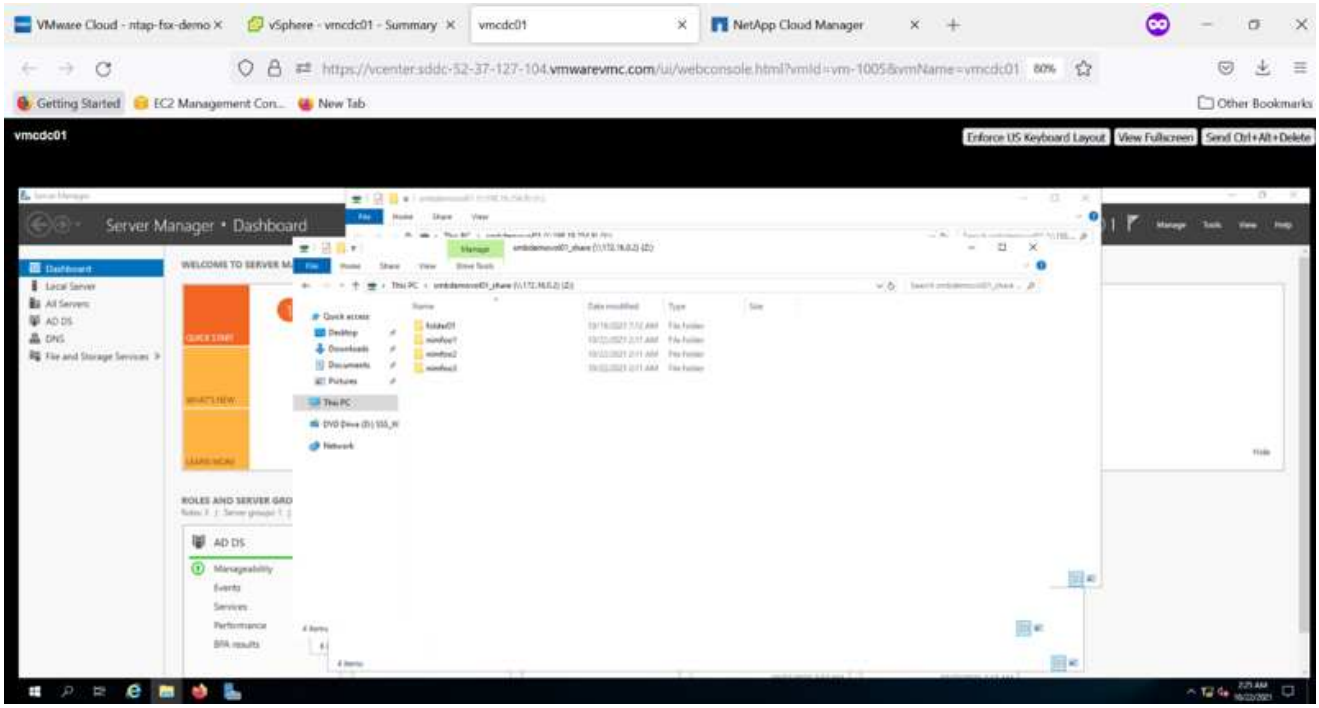

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER GROUPS
AD DS
Manageability
Events
Services
Performance
BPA results
This PC
Network
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_X
Manage
Tools
View
Help

Connectez la LUN à un hôte

Pour connecter le LUN Cloud Volumes ONTAP à un hôte, procédez comme suit :

1. Sur la page Canvas de Cloud Manager, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP pour créer et gérer des volumes.
2. Cliquez sur Ajouter un volume > Nouveau volume, sélectionnez iSCSI, puis cliquez sur Créer un groupe d'initiateurs. Cliquez sur Continuer .





1. Une fois le volume provisionné, sélectionnez le volume, puis cliquez sur IQN cible. Pour copier le nom qualifié iSCSI (IQN), cliquez sur Copier. Configurez une connexion iSCSI de l'hôte vers le LUN.

Pour appliquer la même opération à l'hôte résidant sur le SDDC VMware Cloud basé sur AWS, effectuez les opérations suivantes :

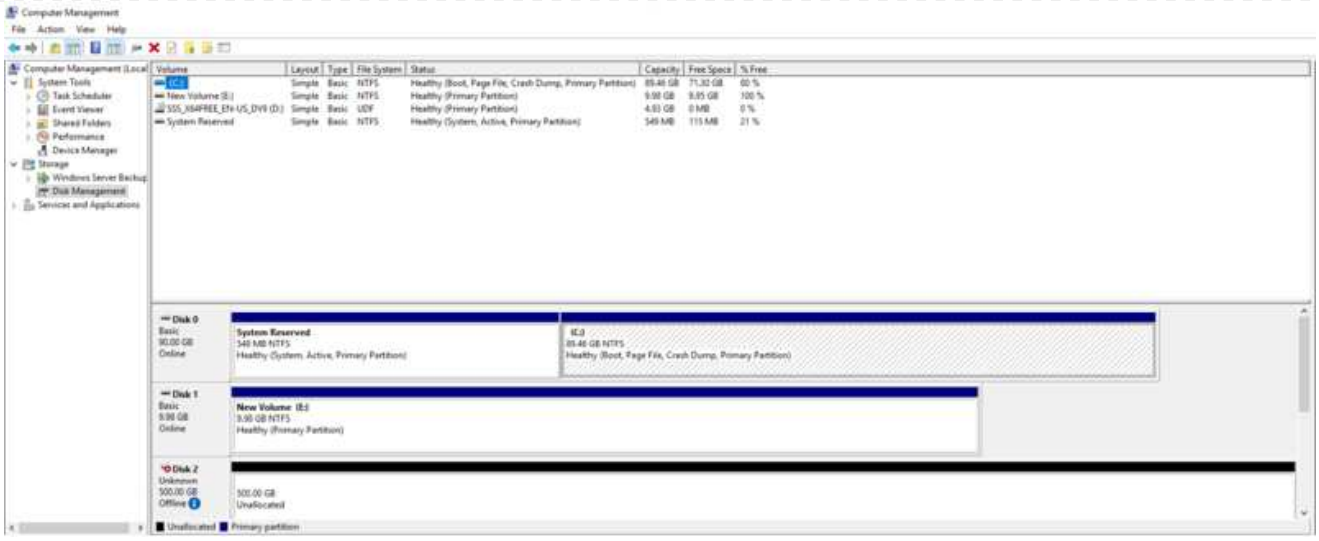
1. RDP vers la VM hébergée sur VMware Cloud sur AWS.

2. Ouvrez la boîte de dialogue Propriétés de l'initiateur iSCSI : Gestionnaire de serveur > Tableau de bord > Outils > initiateur iSCSI.
3. Dans l'onglet découverte, cliquez sur Discover Portal ou Add Portal, puis entrez l'adresse IP du port cible iSCSI.
4. Dans l'onglet cibles, sélectionnez la cible découverte, puis cliquez sur connexion ou connexion.
5. Sélectionnez Activer Multipath, puis sélectionnez Restaurer automatiquement cette connexion au démarrage de l'ordinateur ou Ajouter cette connexion à la liste des cibles favorites. Cliquez sur Avancé.

L'hôte Windows doit disposer d'une connexion iSCSI à chaque nœud du cluster. Le DSM natif sélectionne les meilleurs chemins d'accès à utiliser.

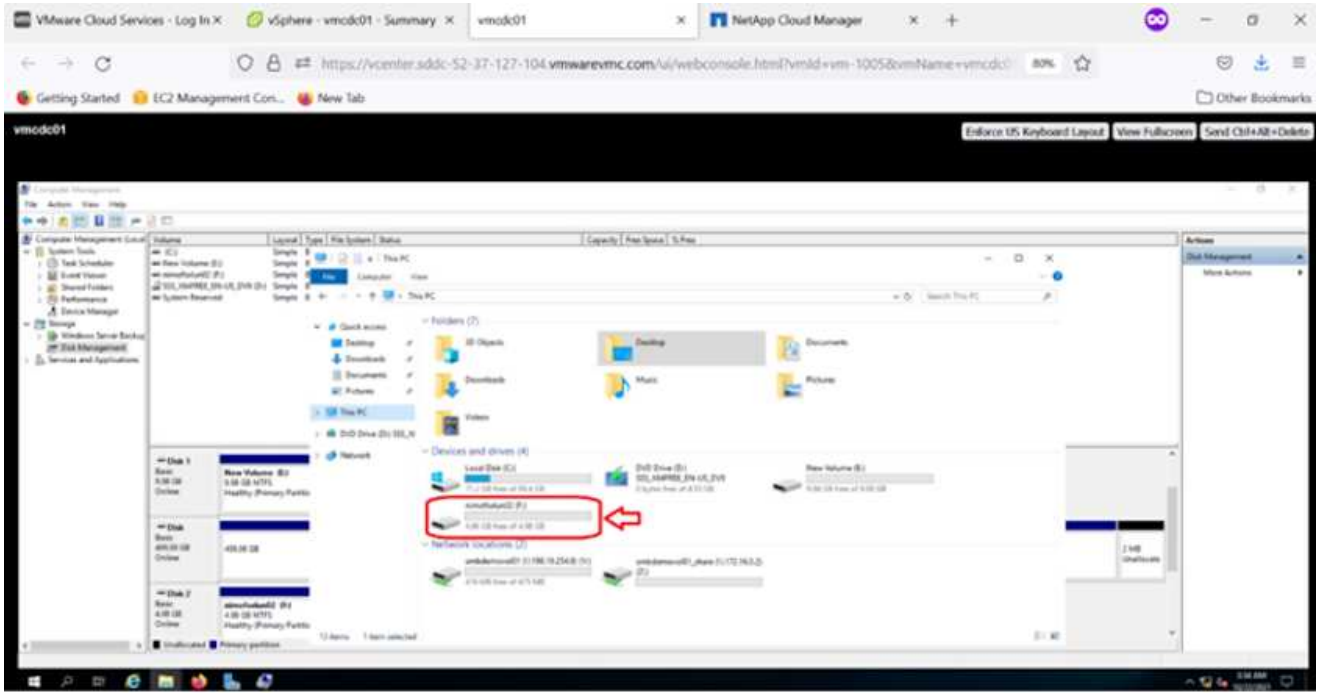
Les LUN du SVM apparaissent comme des disques vers l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclencher une nouvelle analyse manuelle pour détecter les disques en procédant comme suit :

1. Ouvrez l'utilitaire de gestion de l'ordinateur Windows : Démarrer > Outils d'administration > gestion de l'ordinateur.
2. Développez le nœud stockage dans l'arborescence de navigation.
3. Cliquez sur gestion des disques.
4. Cliquez sur action > Rescan Disks.



Lorsqu'un nouvel LUN est accédé pour la première fois par l'hôte Windows, il n'a pas de partition ni de système de fichiers. Initialiser la LUN ; et éventuellement formater la LUN avec un système de fichiers en effectuant la procédure suivante :

1. Démarrez Windows Disk Management.
2. Cliquez avec le bouton droit de la souris sur la LUN, puis sélectionnez le type de disque ou de partition requis.
3. Suivez les instructions de l'assistant. Dans cet exemple, le lecteur F: Est monté.



Sur les clients Linux, assurez-vous que le démon iSCSI est en cours d'exécution. Une fois les LUN provisionnées, reportez-vous aux instructions détaillées sur la configuration iSCSI pour votre distribution Linux. Par exemple, la configuration iSCSI Ubuntu est disponible "ici". Pour vérifier, exécutez lsblk cmd à partir du shell.

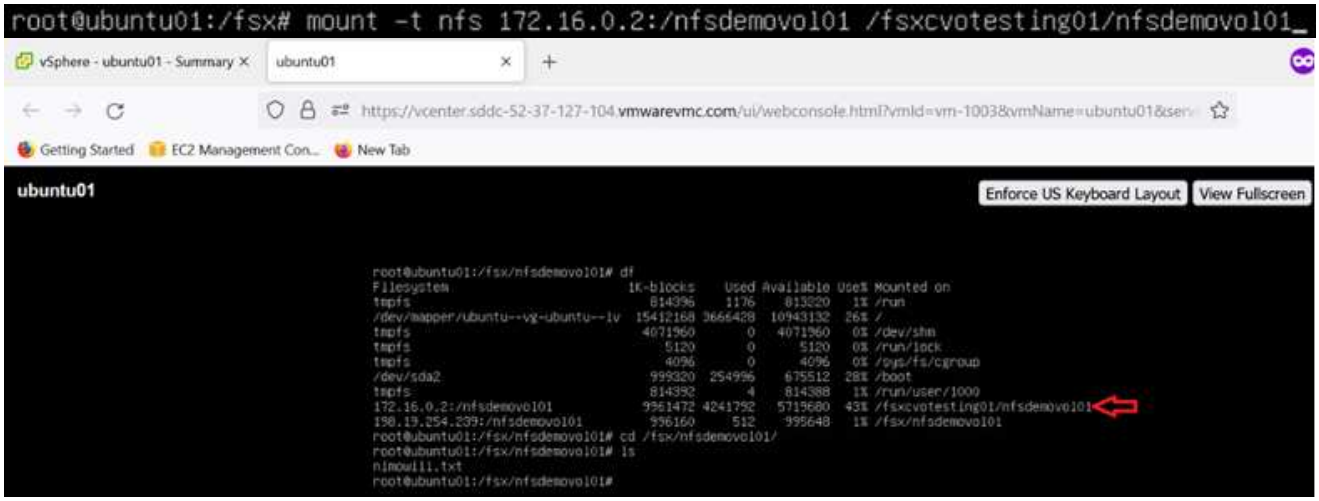
Montez un volume NFS Cloud Volumes ONTAP sur un client Linux

Pour monter le système de fichiers Cloud Volumes ONTAP (DIY) depuis des VM dans le VMC sur le SDDC AWS, effectuez la procédure suivante :

1. Connectez-vous à l'instance Linux désignée.
2. Ouvrez un terminal sur l'instance à l'aide du shell sécurisé (SSH) et connectez-vous avec les informations d'identification appropriées.
3. Créer un répertoire pour le point de montage du volume avec la commande suivante.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Montez le volume NFS Amazon FSX pour NetApp ONTAP dans le
répertoire créé à l'étape précédente.
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```



Présentation des solutions de datastores ANF

Chaque organisation réussie est sur le chemin de la transformation et de la modernisation. Dans le cadre de ce processus, les entreprises utilisent généralement leurs investissements VMware existants tout en tirant parti des avantages du cloud et en explorant comment rendre les processus de migration, de rafale, d'extension et de reprise sur incident aussi transparents que possible. Les clients qui migrent vers le cloud doivent évaluer les difficultés liées à la flexibilité et aux bursting, à la sortie du data Center, à la consolidation des data centers, aux scénarios de fin de vie, aux fusions, aux acquisitions, etc. L'approche adoptée par chaque organisation peut varier en fonction de leurs priorités commerciales respectives. Lors du choix des opérations basées sur le cloud, il est essentiel de choisir un modèle économique aux performances appropriées et à un obstacle minimal. Si vous choisissez la plateforme appropriée, l'orchestration du

stockage et des workflows est particulièrement importante pour exploiter toute la puissance du déploiement cloud et de l'élasticité.

Cas d'utilisation

Bien que la solution Azure VMware offre des fonctionnalités hybrides uniques à un client, les options de stockage natives limitées n'ont pas de utilité pour les entreprises qui utilisent de lourdes charges de travail. Le stockage étant directement lié aux hôtes, la seule façon de faire évoluer le stockage consiste à ajouter d'autres hôtes, ce qui permet d'augmenter les coûts de 35 à 40 % ou plus pour les charges de travail consommatrices de stockage. Ces charges de travail ont besoin d'un système de stockage supplémentaire, sans puissance supplémentaire, mais cela implique de payer pour des hôtes supplémentaires.

Examinons le scénario suivant : un client nécessite six hôtes pour la puissance (CPU virtuel/vmem), mais il a également des exigences importantes en matière de stockage. En fonction de leur évaluation, ils nécessitent 12 hôtes pour répondre aux besoins en stockage. Cela augmente le coût total de possession global car ils doivent acheter toute cette puissance supplémentaire lorsque c'est la capacité de stockage requise. Cette fonctionnalité est applicable à toutes les utilisations, y compris la migration, la reprise sur incident, l'bursting, le développement/test, et ainsi de suite.

La reprise après incident est un autre scénario commun à la solution Azure VMware. La plupart des entreprises ne disposent pas d'une stratégie de reprise après incident trop fiable ou peinent à justifier l'exécution d'un data Center fantôme pour la reprise après incident. Les administrateurs peuvent explorer les options de reprise après incident sans encombrement avec un cluster à lampe témoin ou un cluster à la demande. La capacité de stockage peut ensuite évoluer sans ajouter d'hôtes supplémentaires, ce qui représente une option intéressante.

Pour résumer, les cas d'utilisation peuvent être classés de deux façons :

- Évolutivité de la capacité de stockage avec les datastores ANF
- Utilisation des datastores ANF en tant que cible de reprise après incident pour un workflow de restauration optimisé en termes de coût depuis des sites ou des régions Azure entre les data centers Software-defined (SDDC).ce guide fournit des informations sur l'utilisation de Azure NetApp Files pour fournir un stockage optimisé aux datastores (actuellement dans une présentation publique) Avec les meilleures fonctionnalités de protection des données et de reprise après incident dans une solution Azure VMware, vous pouvez décharger la capacité de stockage du stockage VSAN.

Pour plus d'informations sur l'utilisation des datastores ANF, contactez les architectes de solutions NetApp ou Microsoft de votre région.

Options VMware Cloud dans Azure

Solution Azure VMware

Azure VMware solution (AVS) est un service de cloud hybride qui permet de bénéficier pleinement des SDDC VMware d'un cloud public Microsoft Azure. AVS est une solution première entièrement gérée et prise en charge par Microsoft, puis vérifiée par VMware qui utilise l'infrastructure Azure. Par conséquent, les clients bénéficient de VMware ESXi pour la virtualisation du calcul, de VSAN pour le stockage hyper-convergé et de NSX pour la mise en réseau et la sécurité, tout en exploitant la présence mondiale de Microsoft Azure, des sites de data Center leaders de pointe et de notre écosystème de services et solutions Azure natifs. La combinaison d'Azure VMware solution SDDC et d'Azure NetApp Files offre les meilleures performances et une latence réseau minimale.

Quel que soit le cloud utilisé lorsqu'un SDDC VMware est déployé, le cluster initial inclut les composants

suivants :

- Hôtes VMware ESXi pour la virtualisation du calcul avec une appliance vCenter Server à gérer.
- Stockage hyper-convergé VMware VSAN incluant les ressources de stockage physique de chaque hôte ESXi.
- VMware NSX pour la mise en réseau virtuelle et la sécurité avec un cluster NSX Manager à des fins de gestion.

Conclusion

Qu'il s'agisse d'un cloud ou d'un cloud hybride, Azure NetApp Files constitue une excellente option pour déployer et gérer les workloads applicatifs et les services de fichiers tout en réduisant le coût total de possession, en rendant les exigences de données transparentes pour la couche applicative. Quelle que soit l'utilisation, optez pour Azure VMware solution et Azure NetApp Files pour bénéficier rapidement des avantages du cloud, d'une infrastructure cohérente et des opérations en local et dans plusieurs clouds, de la portabilité bidirectionnelle des charges de travail, ainsi que de la capacité et des performances élevées. Il s'agit du même processus que celui utilisé pour connecter le stockage. N'oubliez pas que la position des données a changé avec de nouveaux noms. Les outils et les processus restent les mêmes, et Azure NetApp Files contribue à optimiser le déploiement global.

Messages clés

Les points clés de ce document sont les suivants :

- Vous pouvez désormais utiliser Azure NetApp Files comme datastore sur AVS SDDC.
- Améliorez les temps de réponse des applications et offrez une plus grande disponibilité pour accéder aux données des workloads à tout moment où qu'elles soient.
- Simplifiez la complexité globale du stockage VSAN grâce à des fonctionnalités de redimensionnement simple et instantané.
- Performances garanties pour les charges de travail stratégiques grâce aux fonctionnalités de remaniement dynamique.
- Si Azure VMware solution Cloud est la destination incontournable, Azure NetApp Files est la solution de stockage idéale pour optimiser le déploiement.

Où trouver des informations complémentaires

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

- Documentation sur la solution Azure VMware

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Documentation Azure NetApp Files

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

- Connexion des datastores Azure NetApp Files aux hôtes de solution Azure VMware (aperçu)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

Azure prend en charge le stockage NetApp connecté par l'invité grâce au service natif Azure NetApp Files (ANF) ou à Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure NetApp Files apporte des fonctionnalités haute performance de stockage et de gestion des données à Azure afin de faciliter la gestion des workloads et des applications. Migrez vos workloads vers le cloud et exécutez-les sans sacrifier les performances.

Azure NetApp Files lève les obstacles pour vous aider à déplacer dans le cloud toutes vos applications basées sur des fichiers. Pour la première fois, vous n'avez pas à modifier l'architecture de vos applications. En outre, vous bénéficiez d'un stockage persistant sans aucune complexité.

Comme ce service est proposé via le portail Microsoft Azure, les utilisateurs profitent d'une expérience entièrement gérée dans le cadre de leur contrat Microsoft Enterprise. Le support de premier ordre, régi par Microsoft, vous assure une tranquillité d'esprit totale. Cette solution unique vous permet d'ajouter des workloads multiprotocoles de manière simple et rapide. Vous pouvez créer et déployer des applications basées sur des fichiers à la fois pour Windows et Linux, même pour les environnements hérités.

Azure NetApp Files (ANF) comme stockage connecté invité

Configurer Azure NetApp Files avec Azure VMware solution (AVS)

Les partages Azure NetApp Files peuvent être montés à partir des VM créées dans l'environnement Azure VMware solution SDDC. Les volumes peuvent également être montés sur le client Linux et mappés sur le client Windows, car Azure NetApp Files prend en charge les protocoles SMB et NFS. Les volumes Azure NetApp Files peuvent être configurés en cinq étapes simples.

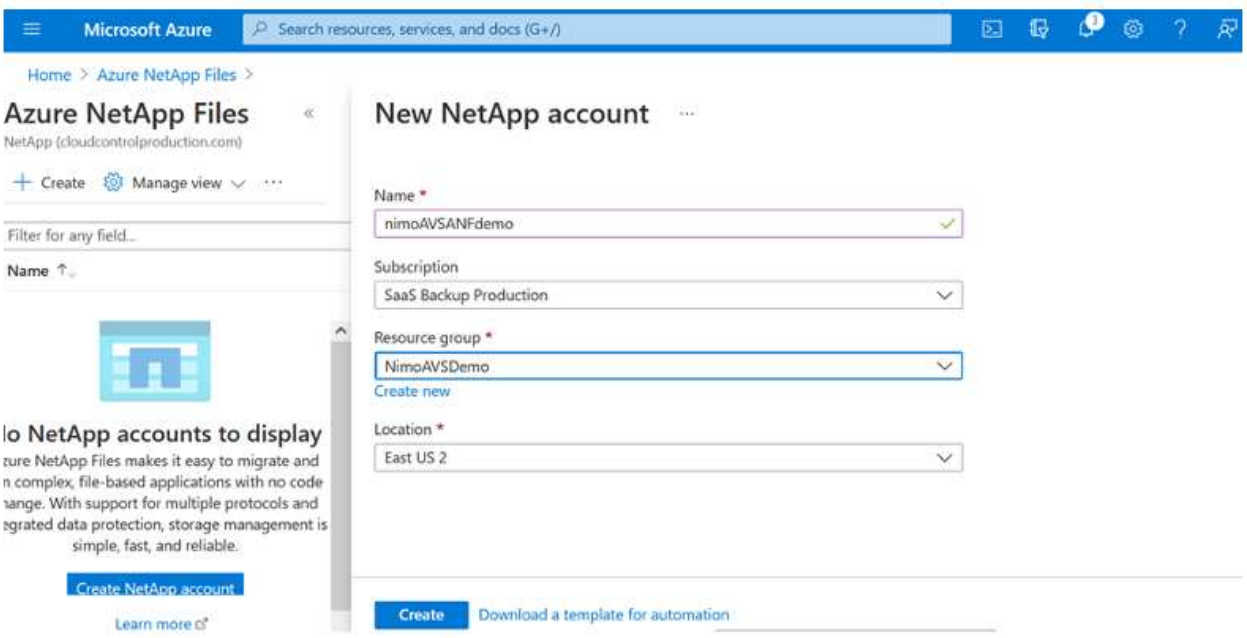
Azure NetApp Files et Azure VMware solution doivent se trouver dans la même région Azure.

Création et montage de volumes Azure NetApp Files

Pour créer et monter des volumes Azure NetApp Files, procédez comme suit :

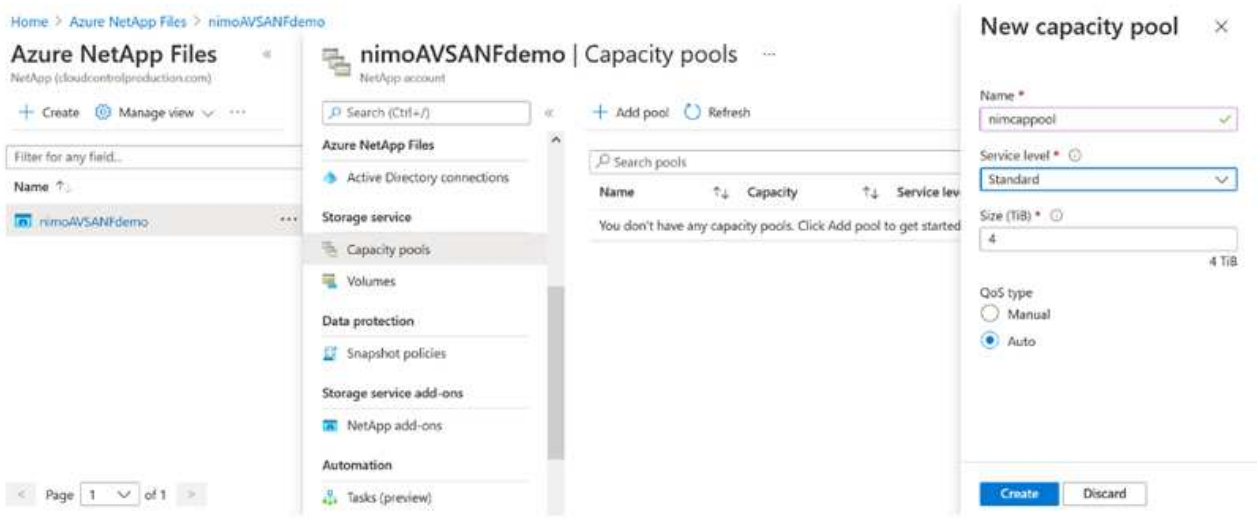
1. Connectez-vous au portail Azure et accédez à Azure NetApp Files. Vérifiez l'accès au service Azure NetApp Files et enregistrez le fournisseur de ressources Azure NetApp Files à l'aide de la commande *az Provider Register --namespace Microsoft.NetApp –wait*. Une fois l'inscription terminée, créez un compte NetApp.

   Pour obtenir des instructions détaillées, reportez-vous à la section "Partages Azure NetApp Files". Cette page vous guidera tout au long du processus étape par étape.

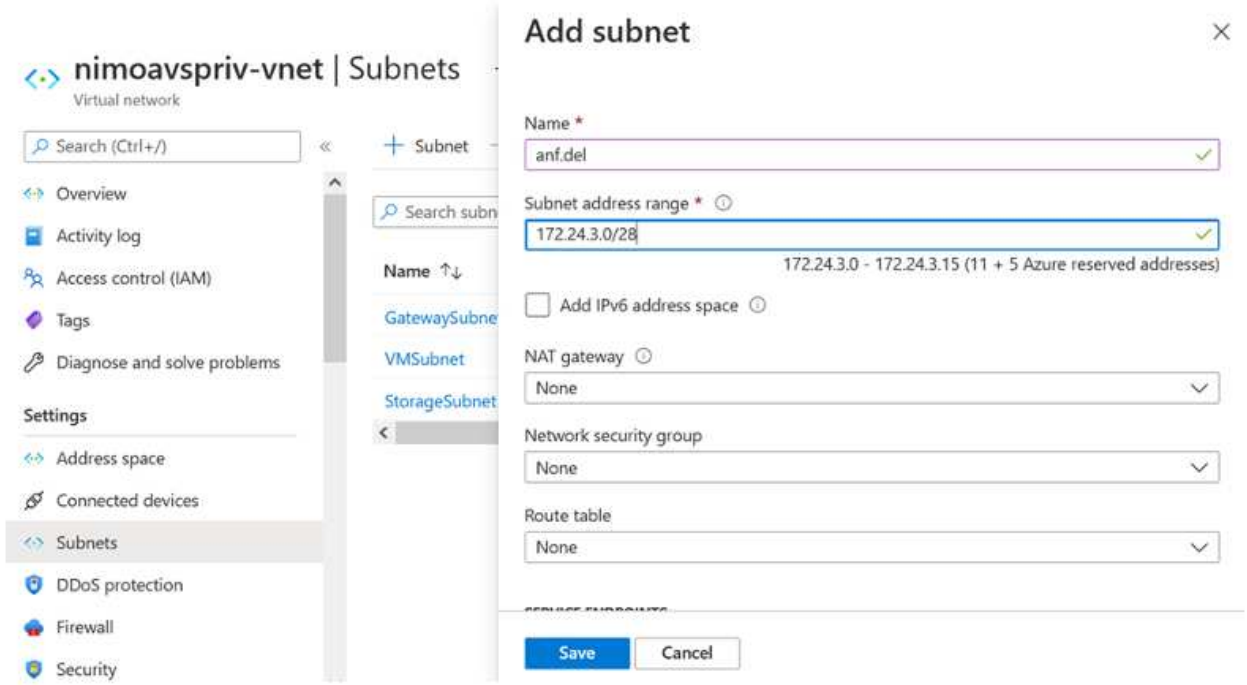


2. Une fois le compte NetApp créé, configurez les pools de capacité avec le niveau et la taille de service requis.

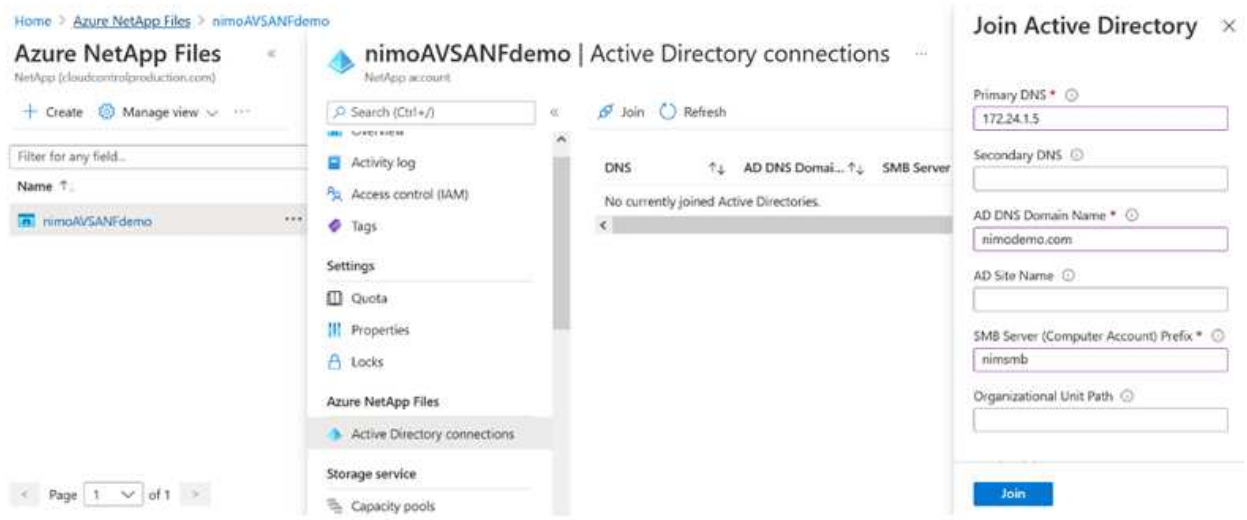
   Pour plus d'informations, voir "Configurez un pool de capacité".



3. Configurez le sous-réseau délégué pour Azure NetApp Files et spécifiez ce sous-réseau lors de la création des volumes. Pour obtenir des instructions détaillées sur la création d'un sous-réseau délégué, reportez-vous à la section "Déléguer un sous-réseau à Azure NetApp Files".

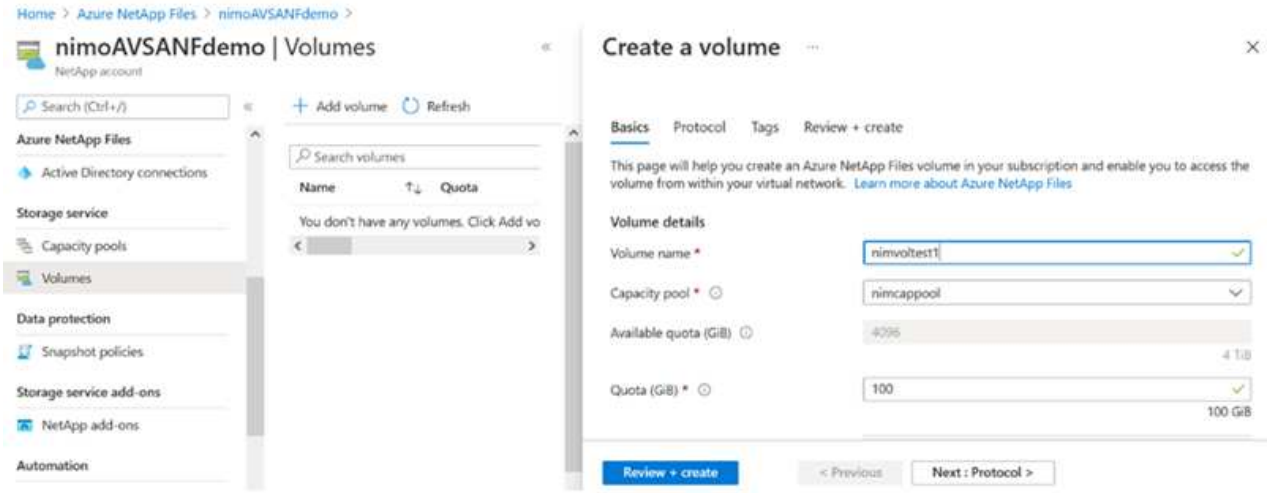


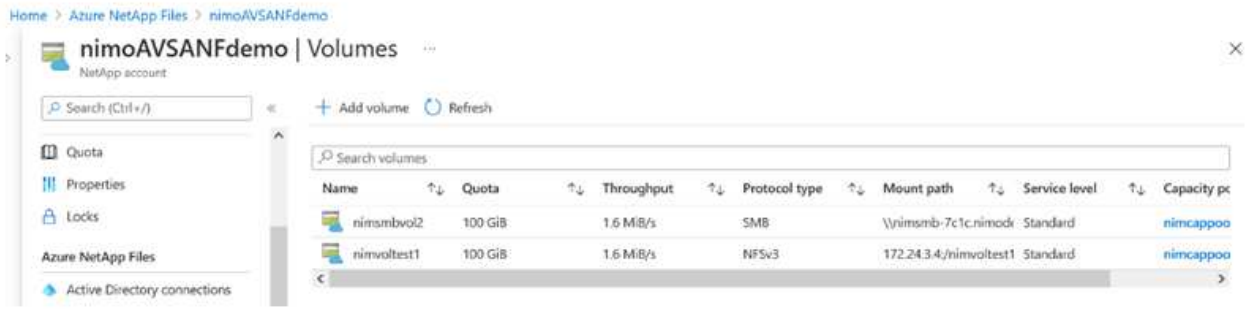
4. Ajoutez un volume SMB en utilisant le serveur lame volumes sous le serveur lame Capacity pools. Assurez-vous que Active Directory Connector est configuré avant de créer le volume SMB.



5. Cliquez sur Revue + Créer pour créer le volume SMB.

   Si l'application est SQL Server, activez la disponibilité continue SMB.

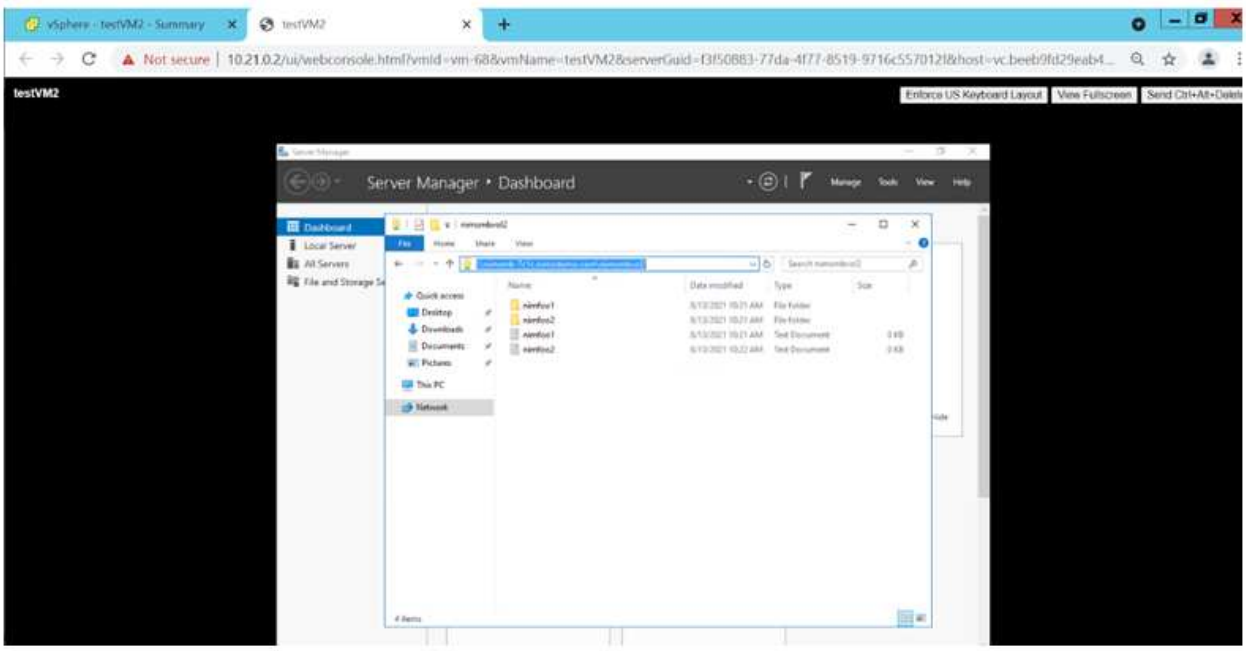


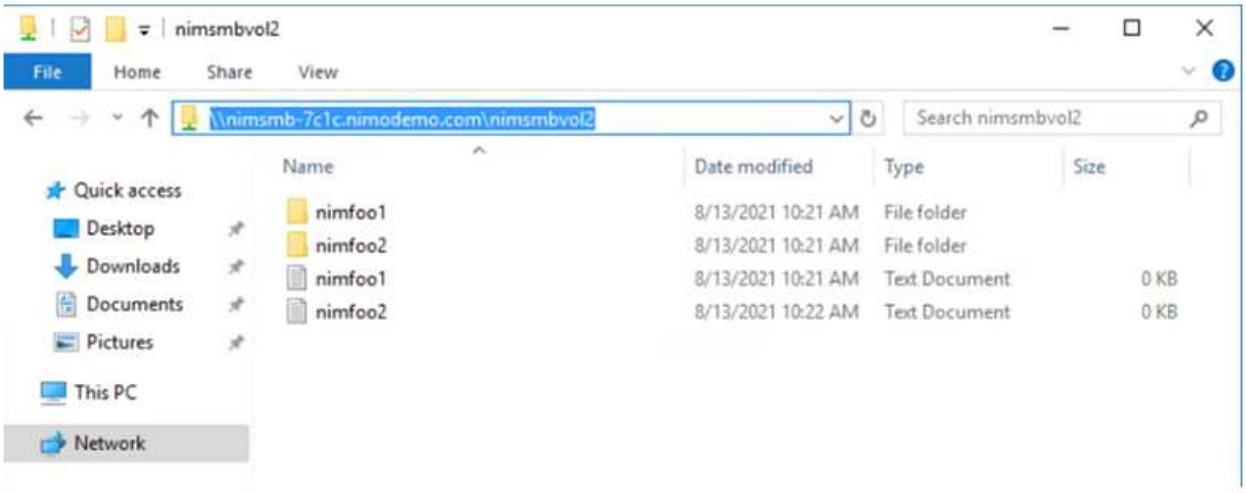


Pour en savoir plus sur les performances des volumes Azure NetApp Files par taille ou quota, reportez-vous à la section "Performances de Azure NetApp Files".

6. Une fois la connectivité en place, le volume peut être monté et utilisé pour les données d'application.

   Pour ce faire, cliquez sur le portail Azure puis sur le serveur lame volumes, puis sélectionnez le volume à monter et accédez aux instructions de montage. Copiez le chemin d'accès et utilisez l'option Map Network Drive pour monter le volume sur la machine virtuelle exécutée sur Azure VMware solution SDDC.





7. Pour monter des volumes NFS sur des machines virtuelles Linux s'exécutant sur Azure VMware solution SDDC, utilisez ce processus. Adaptation des volumes ou fonctionnalité de niveau de service dynamique pour répondre aux demandes des charges de travail

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                 1K-blocks     Used Available Use% Mounted on
udev                         8168112        0   8168112   0% /dev
tmpfs                        1639548     1488   1638060   1% /run
/dev/sda5                   50824704  7902752  40310496  17% /
tmpfs                        8197728        0   8197728   0% /dev/shm
tmpfs                           5120        0      5120   0% /run/lock
tmpfs                        8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                     56832    56832         0 100% /snap/core18/2128
/dev/loop2                     66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                    224256   224256         0 100% /snap/gnome-3-34-180
4/72
/dev/loop3                     52224    52224         0 100% /snap/snap-store/547
/dev/loop4                     33152    33152         0 100% /snap/snapd/12704
/dev/sda1                     523248        4    523244   1% /boot/efi
tmpfs                        1639544       52   1639492   1% /run/user/1000
/dev/sr0                       54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

Pour plus d'informations, voir "Modification dynamique du niveau de service d'un volume".

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, ou CVO, est la solution de gestion des données cloud leader qui repose sur le logiciel de stockage ONTAP de NetApp, disponible de façon native dans Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version Software-defined de ONTAP qui utilise le stockage cloud natif. Vous pouvez ainsi utiliser le même logiciel de stockage dans le cloud et sur site, limitant ainsi la nécessité de former à nouveau votre

personnel IT à des méthodes entièrement nouvelles de gestion des données.

Ce logiciel permet au client de déplacer des données de la périphérie, vers le data Center, puis vers le cloud, et inversement, en réunissant votre cloud hybride, le tout géré à l'aide d'une console de gestion centralisée, NetApp Cloud Manager.

De par sa conception, CVO fournit des performances extrêmes et des fonctionnalités avancées de gestion de données pour répondre aux applications les plus exigeantes dans le cloud

Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité

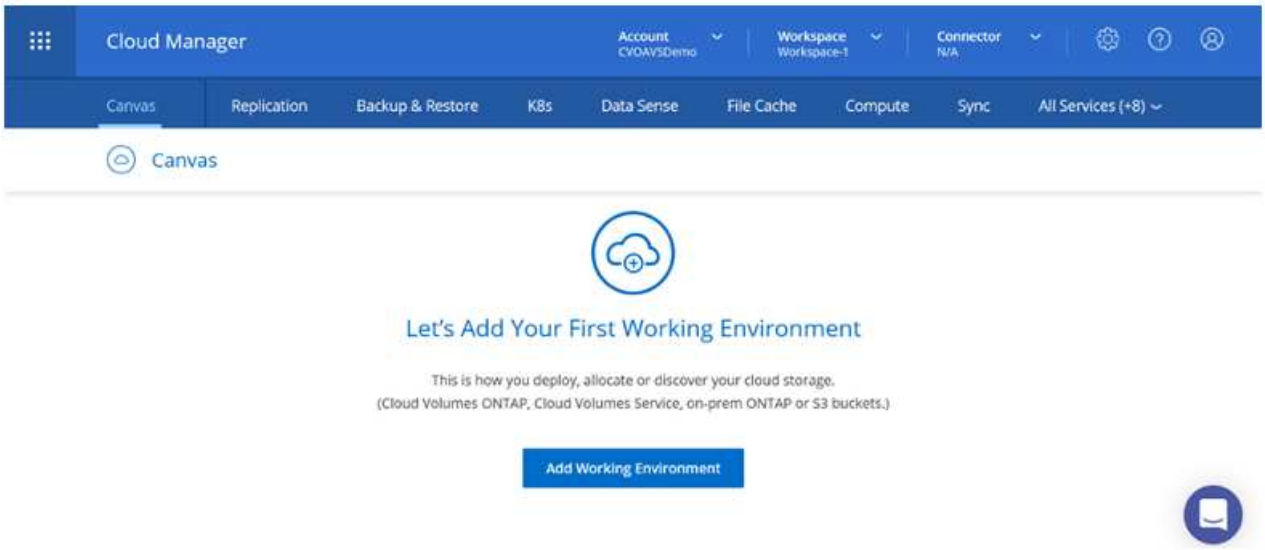
Déploiement du nouveau système Cloud Volumes ONTAP dans Azure

Les partages et les LUN Cloud Volumes ONTAP peuvent être montés sur les VM créées dans l'environnement Azure VMware solution SDDC. Les volumes peuvent également être montés sur le client Linux et sur le client Windows, car Cloud Volumes ONTAP prend en charge les protocoles iSCSI, SMB et NFS. Les volumes Cloud Volumes ONTAP peuvent être configurés en quelques étapes simples.

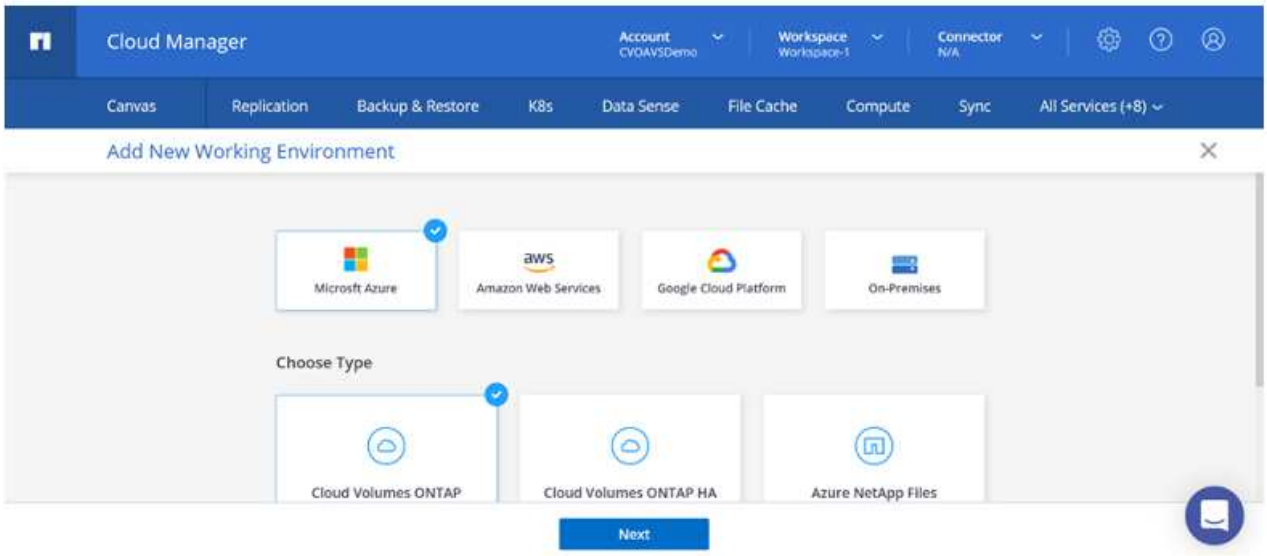
Pour répliquer des volumes depuis un environnement sur site vers le cloud à des fins de reprise d'activité ou de migration, établissez une connectivité réseau à Azure via un VPN site à site ou ExpressRoute. La réplication des données entre les sites et Cloud Volumes ONTAP n'est pas traitée dans ce document. Pour répliquer les données entre les systèmes Cloud Volumes ONTAP et sur site, consultez la section "Configuration de la réplication des données entre les systèmes".

Utiliser "Plus outil de dimensionnement Cloud Volumes ONTAP" Pour dimensionner précisément les instances Cloud Volumes ONTAP. Surveillez également les performances sur site et utilisez-les comme entrées dans le dimensionnement Cloud Volumes ONTAP.

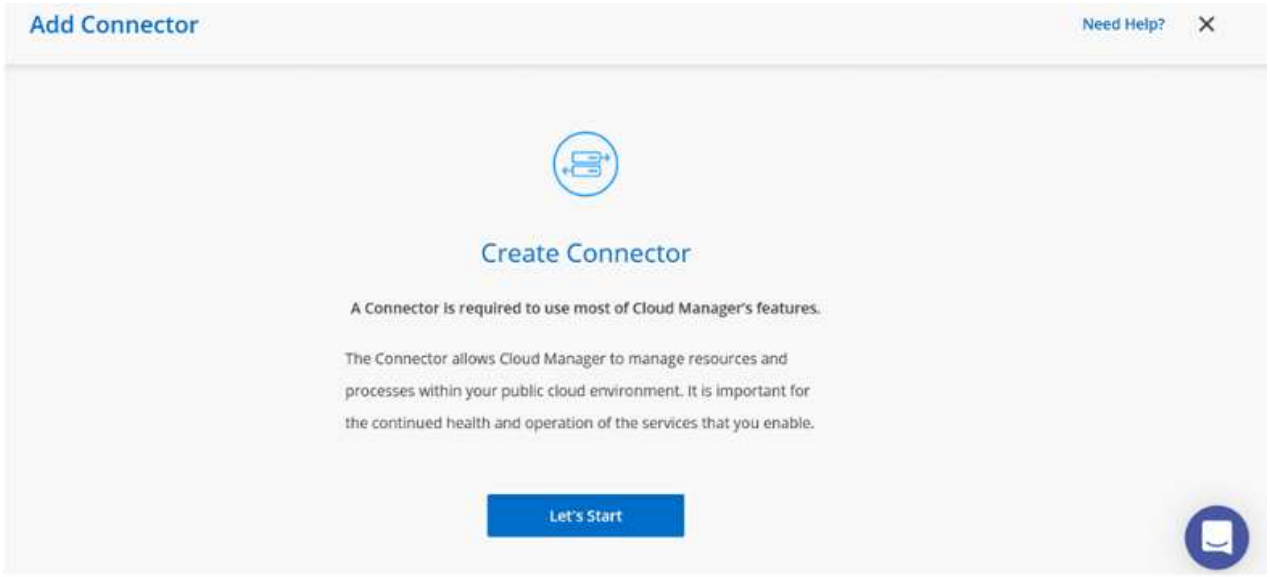
1. Connectez-vous à NetApp Cloud Central ; l'écran Fabric View s'affiche. Localisez l'onglet Cloud Volumes ONTAP et sélectionnez accéder à Cloud Manager. Une fois connecté, l'écran Canvas s'affiche.



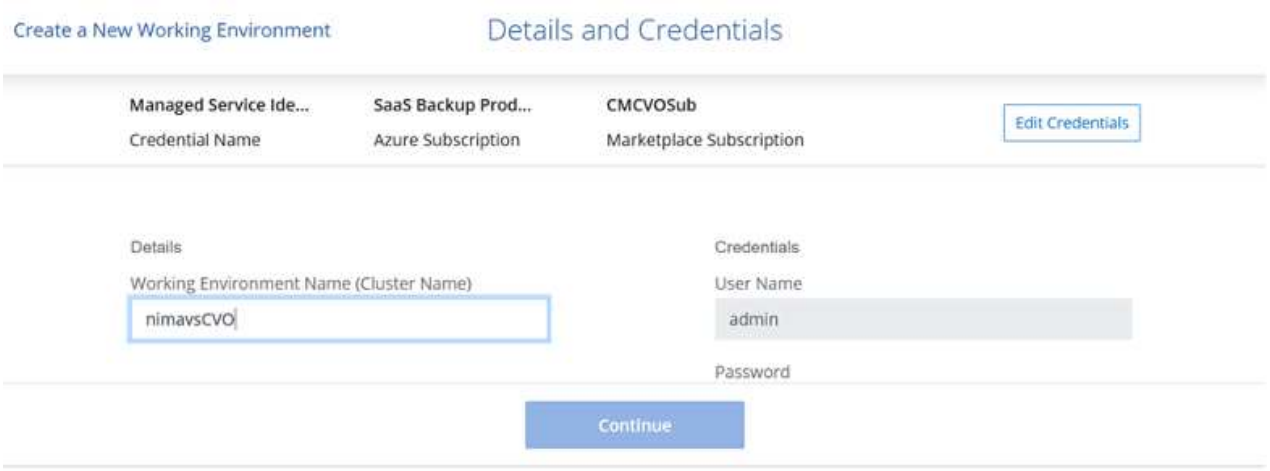
2. Sur la page d'accueil de Cloud Manager, cliquez sur Add a Working Environment, puis sélectionnez Microsoft Azure comme cloud et le type de configuration du système.



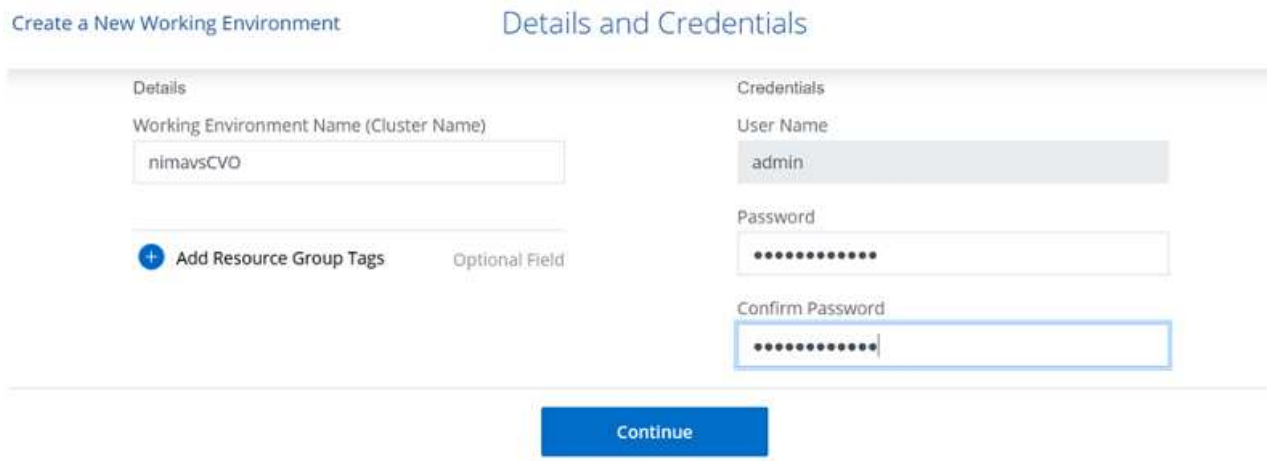
3. Lorsque vous créez le premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à déployer un connecteur.



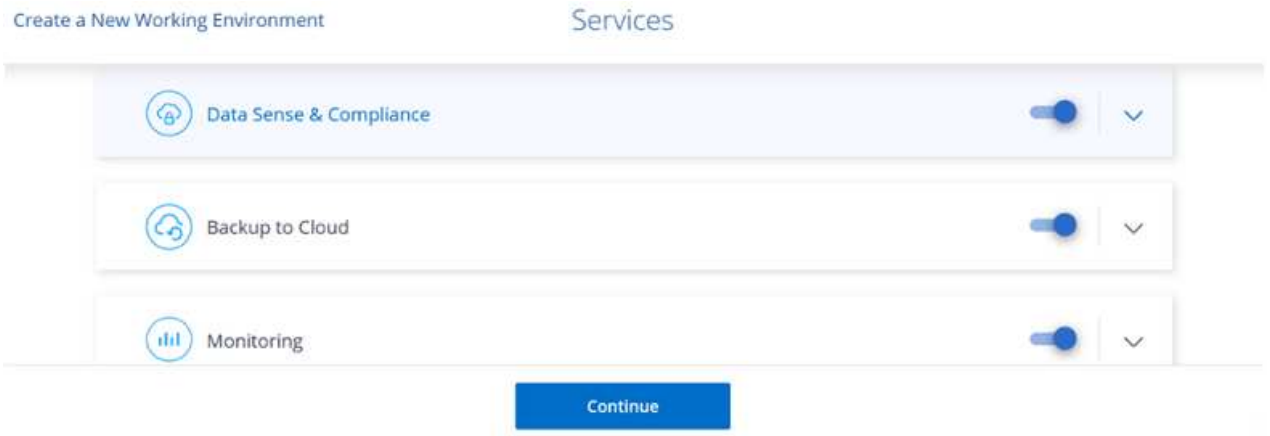
4. Une fois le connecteur créé, mettez à jour les champs Détails et informations d'identification.



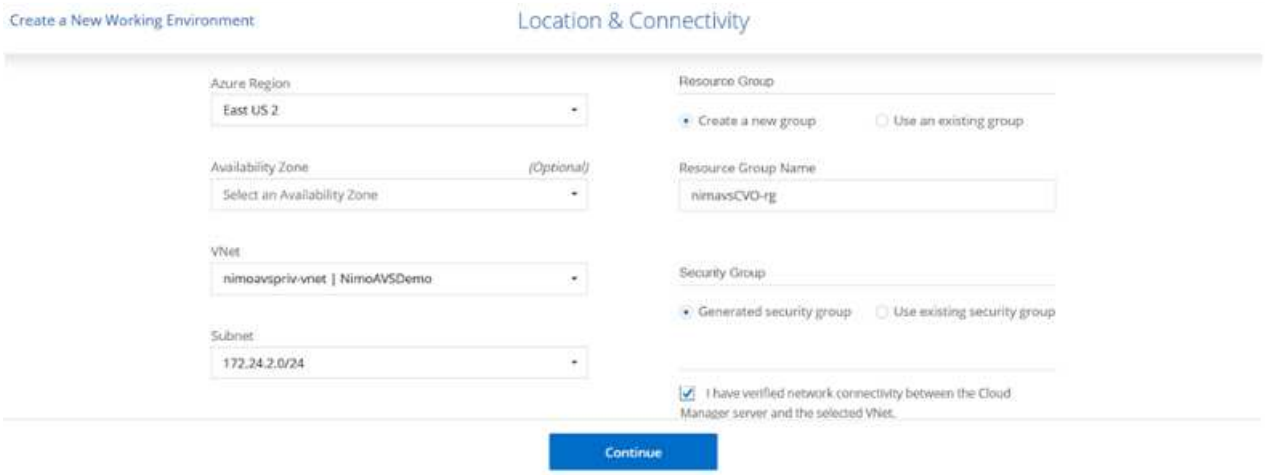
5. Fournissez les détails de l'environnement à créer, y compris le nom de l'environnement et les identifiants d'administrateur. Ajoutez des balises de groupe de ressources pour l'environnement Azure en tant que paramètre facultatif. Une fois que vous avez terminé, cliquez sur Continuer.



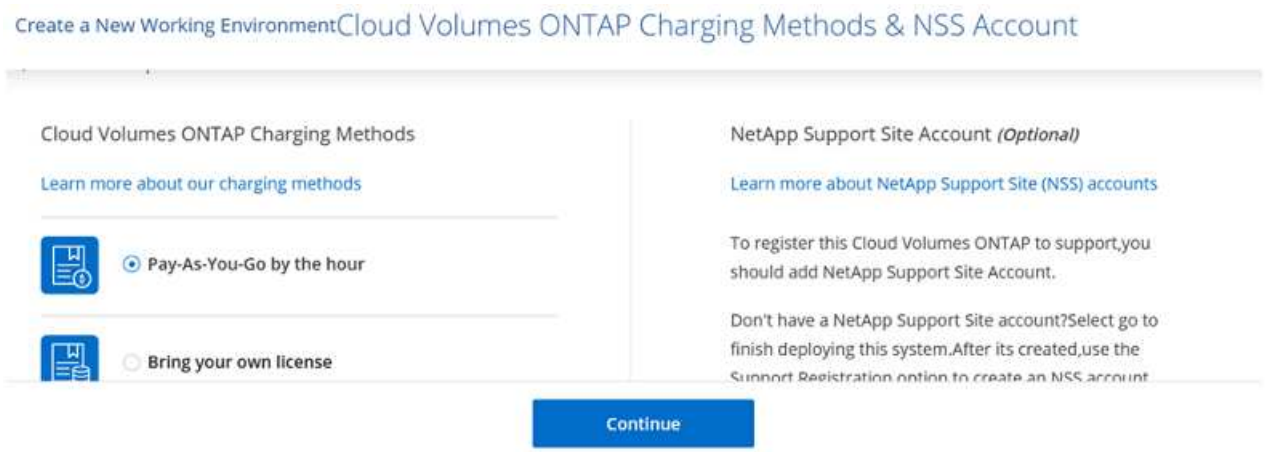
6. Sélectionnez les services complémentaires pour le déploiement Cloud Volumes ONTAP, notamment le classement BlueXP, la sauvegarde et la restauration BlueXP et Cloud Insights. Sélectionnez les services, puis cliquez sur Continuer.



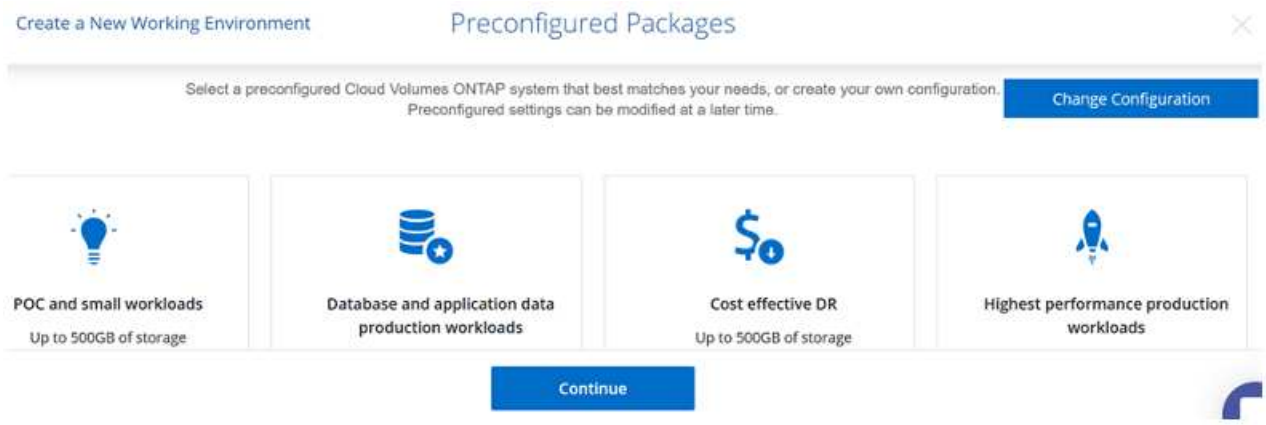
7. Configurez l'emplacement et la connectivité Azure. Sélectionnez la région Azure, le groupe de ressources, le réseau vnet et le sous-réseau à utiliser.



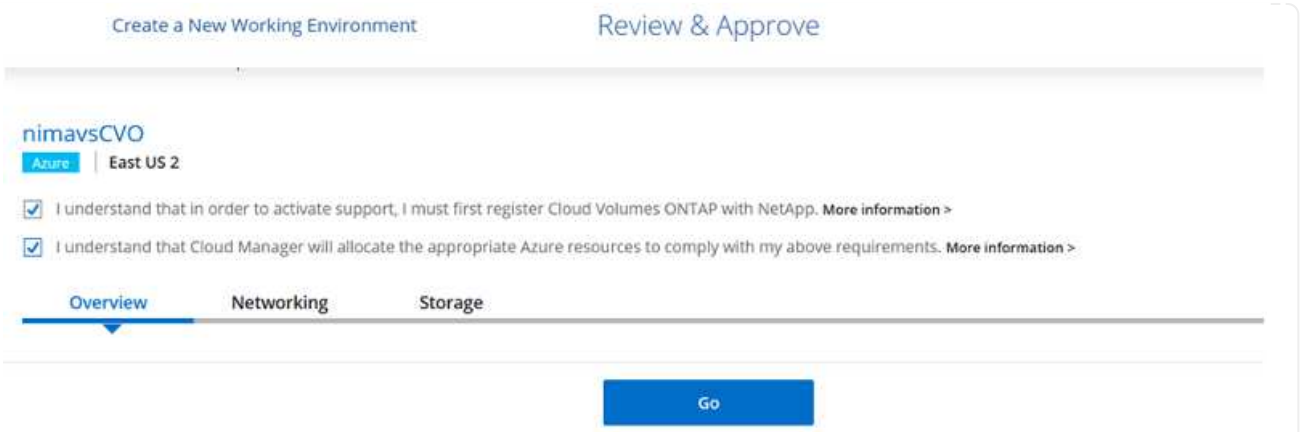
8. Sélectionnez l'option de licence : paiement à l'utilisation ou BYOL pour l'utilisation des licences existantes. Dans cet exemple, l'option paiement à l'utilisation est utilisée.



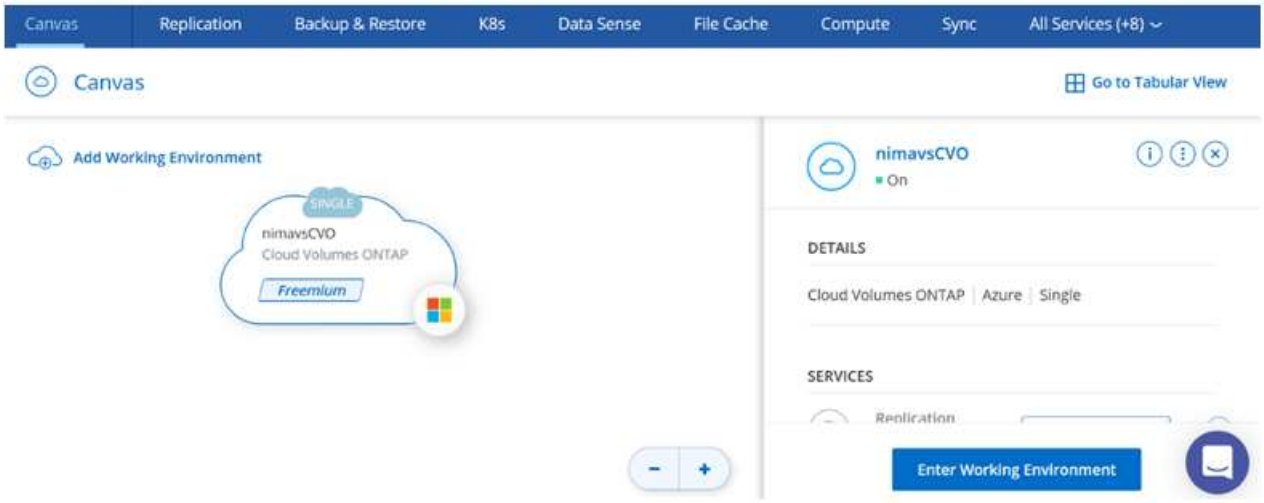
9. Sélectionnez l'un des packages préconfigurés disponibles pour les différents types de charges de travail.



10. Acceptez les deux accords concernant l'activation du support et l'allocation des ressources Azure.pour créer l'instance Cloud Volumes ONTAP, cliquez sur Go.

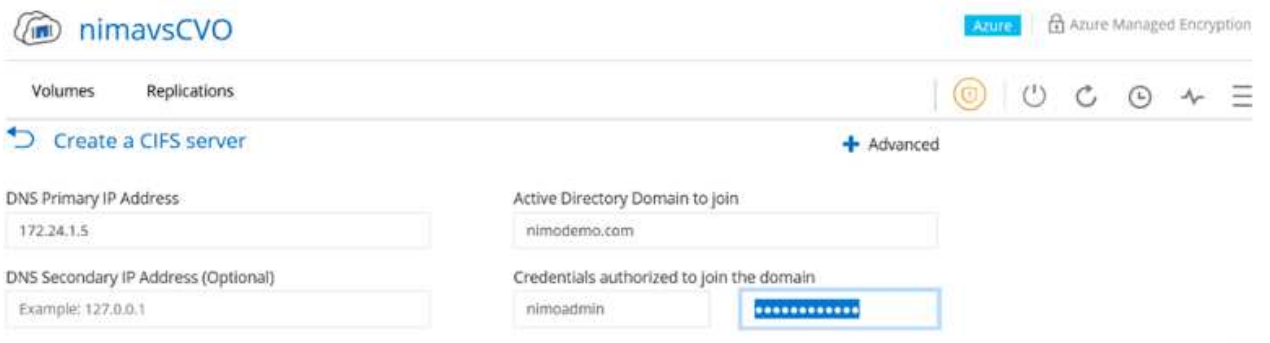


11. Une fois Cloud Volumes ONTAP provisionné, il apparaît dans les environnements de travail sur la page Canvas.

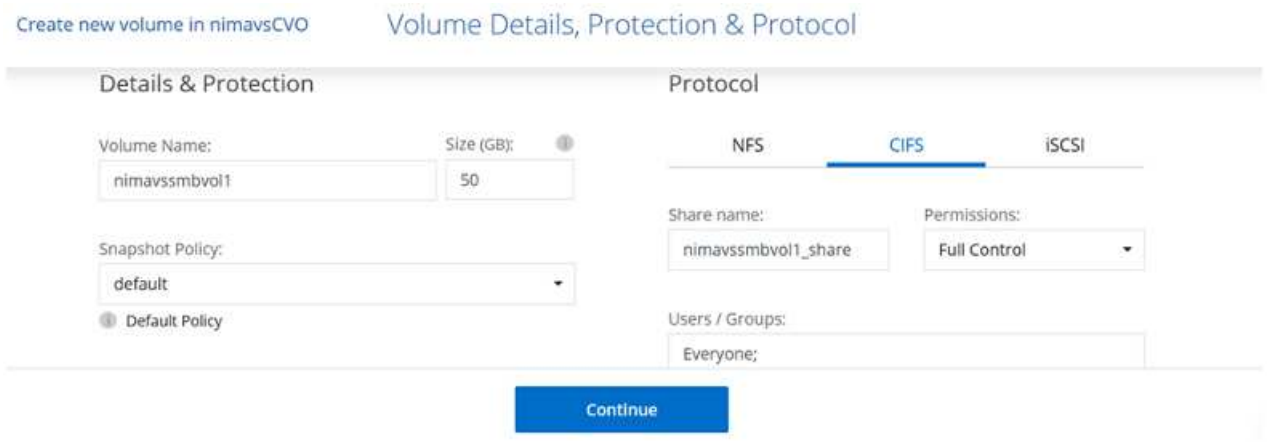


Configurations supplémentaires pour les volumes SMB

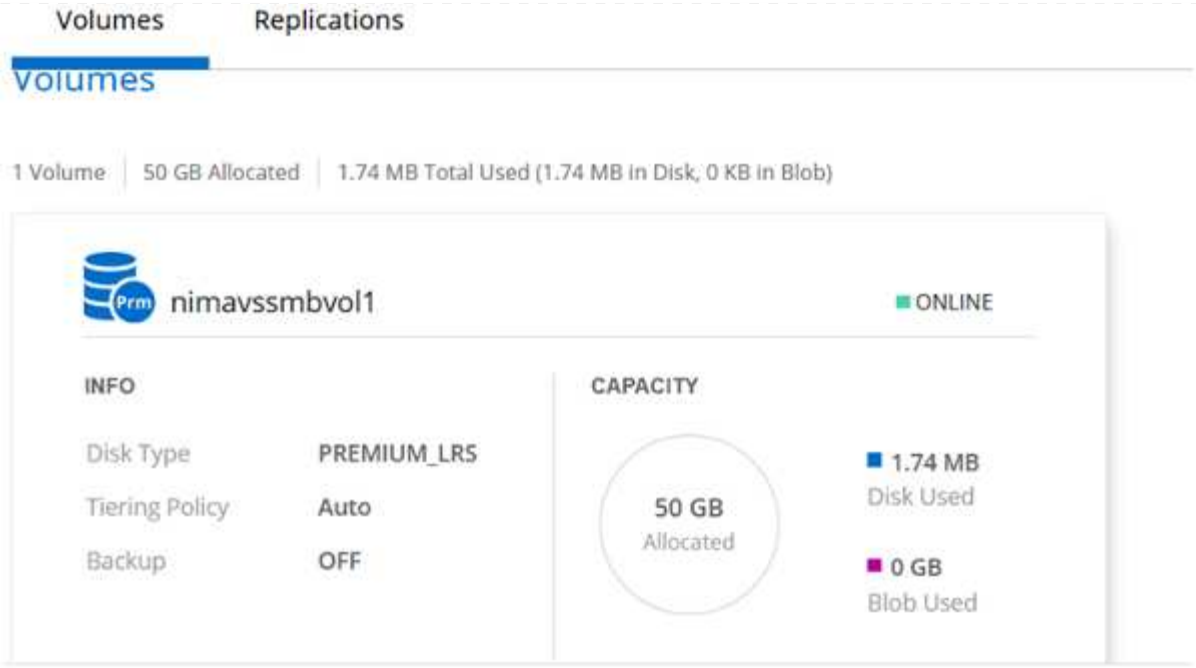
1. Une fois l'environnement de travail prêt, assurez-vous que le serveur CIFS est configuré avec les paramètres de configuration DNS et Active Directory appropriés. Cette étape est requise avant de pouvoir créer le volume SMB.



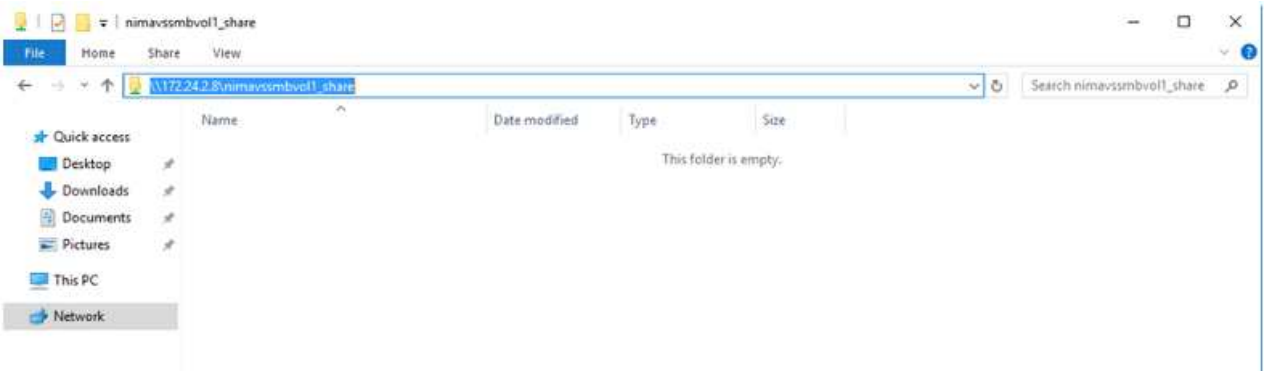
2. La création du volume SMB est un processus simple. Sélectionnez l'instance CVO pour créer le volume, puis cliquez sur l'option Create Volume. Choisissez la taille appropriée et Cloud Manager choisit l'agrégat contenant ou utilisez un mécanisme d'allocation avancée pour placer sur un agrégat spécifique. Pour cette démonstration, SMB est sélectionné comme protocole.



3. Une fois le volume provisionné, celui-ci est disponible sous le volet volumes. Comme un partage CIFS est provisionné, donnez à vos utilisateurs ou groupes l'autorisation d'accéder aux fichiers et dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier. Cette étape n'est pas requise si le volume est répliqué à partir d'un environnement sur site, car les autorisations liées aux fichiers et aux dossiers sont toutes conservées dans le cadre de la réplication SnapMirror.



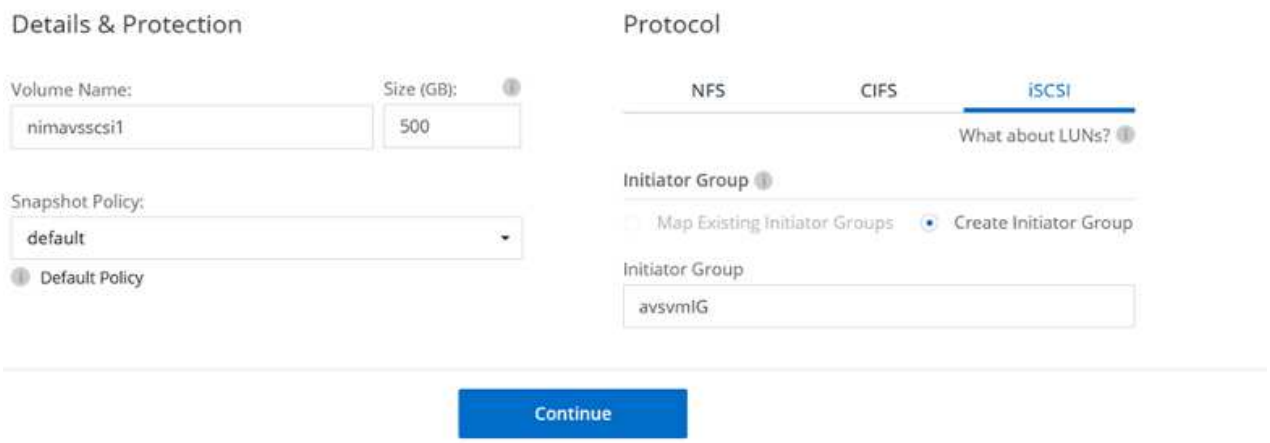
4. Une fois le volume créé, utilisez la commande mount pour vous connecter au partage à partir de la machine virtuelle exécutée sur les hôtes Azure VMware solution SDDC.
5. Copiez le chemin suivant et utilisez l'option Map Network Drive pour monter le volume sur la machine virtuelle exécutée sur Azure VMware solution SDDC.



Connectez la LUN à un hôte

Pour connecter le LUN à un hôte, procédez comme suit :

1. Sur la page Canevas, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP pour créer et gérer des volumes.
2. Cliquez sur Ajouter un volume > Nouveau volume, sélectionnez iSCSI et cliquez sur Créer un groupe d'initiateurs. Cliquez sur Continuer .



3. Une fois le volume provisionné, sélectionnez le volume, puis cliquez sur IQN cible. Pour copier le nom qualifié iSCSI (IQN), cliquez sur Copier. Configurez une connexion iSCSI de l'hôte vers le LUN.

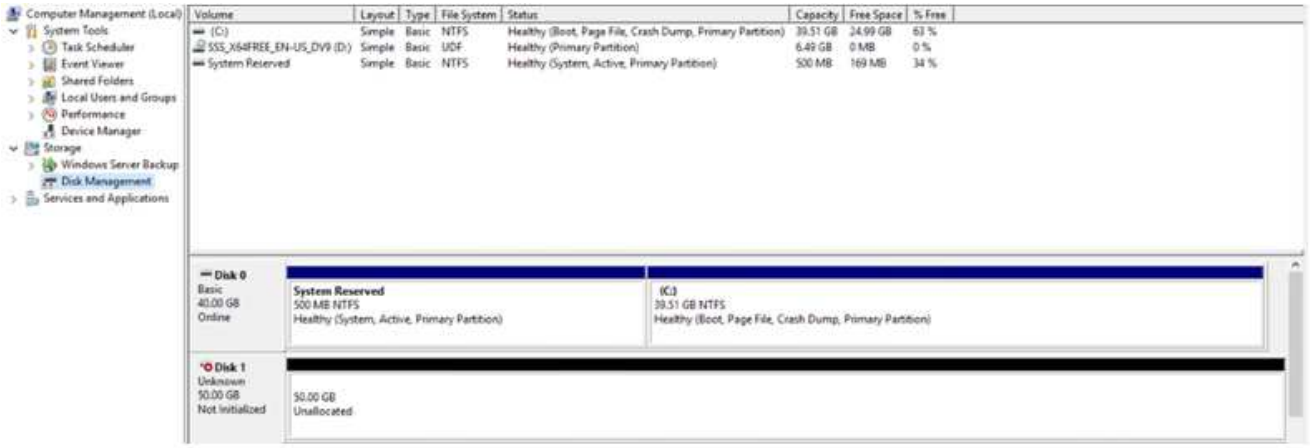
   Pour en faire de même pour l'hôte résidant sur Azure VMware solution SDDC :

   a. RDP vers la machine virtuelle hébergée sur Azure VMware solution SDDC.
   b. Ouvrez la boîte de dialogue Propriétés de l'initiateur iSCSI : Gestionnaire de serveur > Tableau de bord > Outils > initiateur iSCSI.
   c. Dans l'onglet découverte, cliquez sur Discover Portal ou Add Portal, puis entrez l'adresse IP du port cible iSCSI.
   d. Dans l'onglet cibles, sélectionnez la cible découverte, puis cliquez sur connexion ou connexion.
   e. Sélectionnez Activer le multichemin, puis sélectionnez Restaurer automatiquement cette connexion lorsque l'ordinateur démarre ou Ajouter cette connexion à la liste des cibles favorites. Cliquez sur Avancé.

      Remarque : l'hôte Windows doit disposer d'une connexion iSCSI à chaque nœud du cluster. Le DSM natif sélectionne les meilleurs chemins d'accès à utiliser.

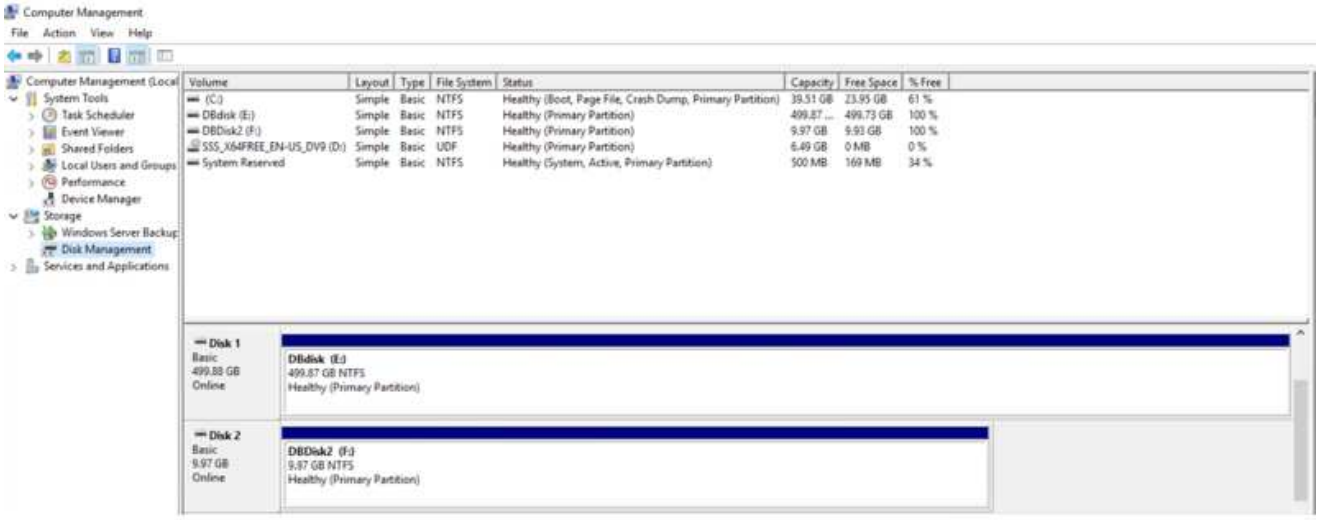
Les LUN présentes sur la machine virtuelle de stockage (SVM) apparaissent sous forme de disques pour l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclencher une nouvelle analyse manuelle pour détecter les disques en procédant comme suit :

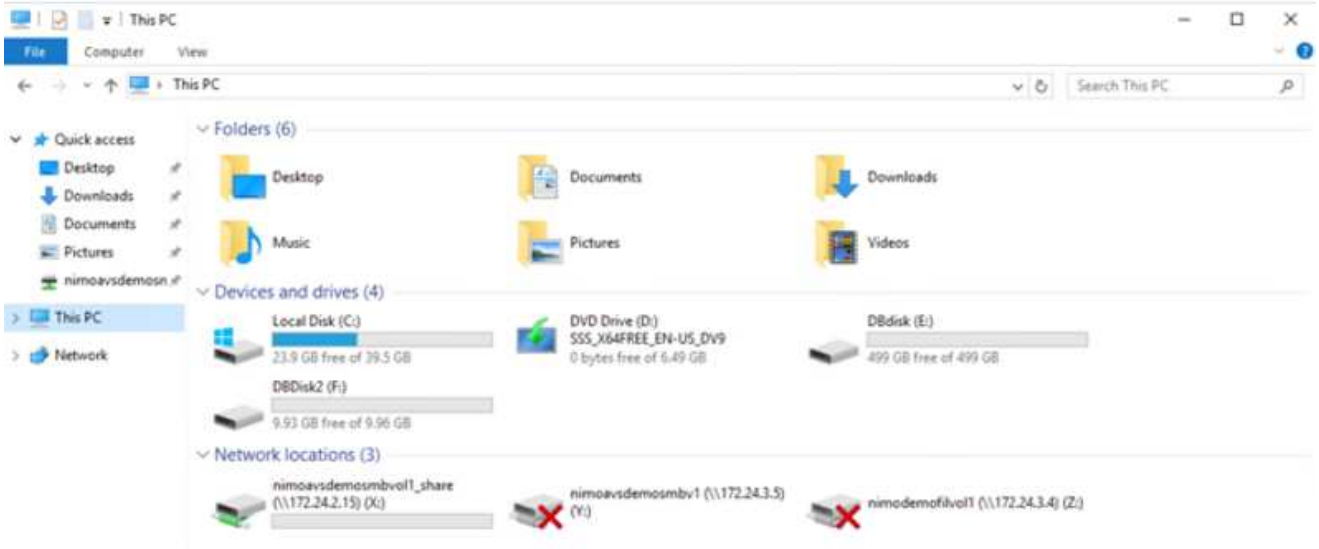
1. Ouvrez l'utilitaire de gestion de l'ordinateur Windows : Démarrer > Outils d'administration > gestion de l'ordinateur.
2. Développez le nœud stockage dans l'arborescence de navigation.
3. Cliquez sur gestion des disques.
4. Cliquez sur action > Rescan Disks.



Lorsqu'un nouvel LUN est accédé pour la première fois par l'hôte Windows, il n'a pas de partition ni de système de fichiers. Initialiser la LUN ; et éventuellement formater la LUN avec un système de fichiers en effectuant la procédure suivante :

1. Démarrez Windows Disk Management.
2. Cliquez avec le bouton droit de la souris sur la LUN, puis sélectionnez le type de disque ou de partition requis.
3. Suivez les instructions de l'assistant. Dans cet exemple, le lecteur E: Est monté



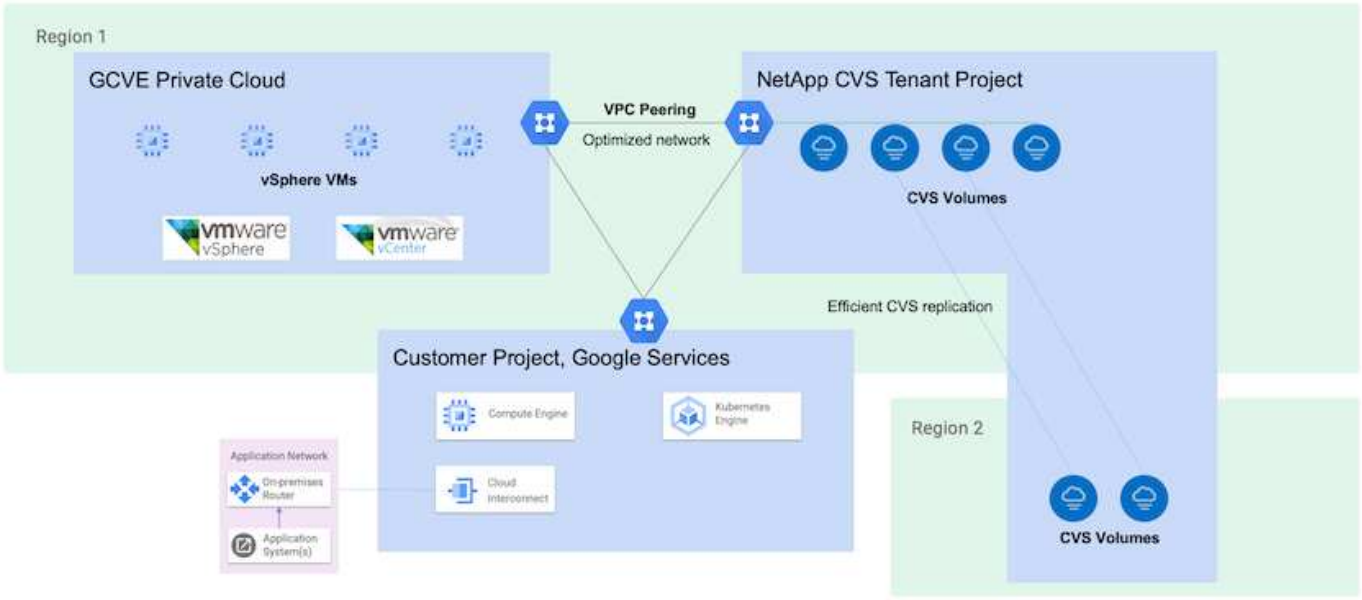


Datastore NFS supplémentaire pour Google Cloud VMware Engine avec NetApp Cloud Volume Service

Présentation

Auteurs : Suresh Thoppay, NetApp

Les clients qui ont besoin de capacité de stockage supplémentaire dans leur environnement Google Cloud VMware Engine (GCVE) peuvent utiliser NetApp Cloud Volume Service pour le montage en tant que datastore NFS supplémentaire.
Le stockage des données sur le service NetApp Cloud volumes permet aux clients de répliquer entre différentes régions pour les protéger contre les données de tramage.



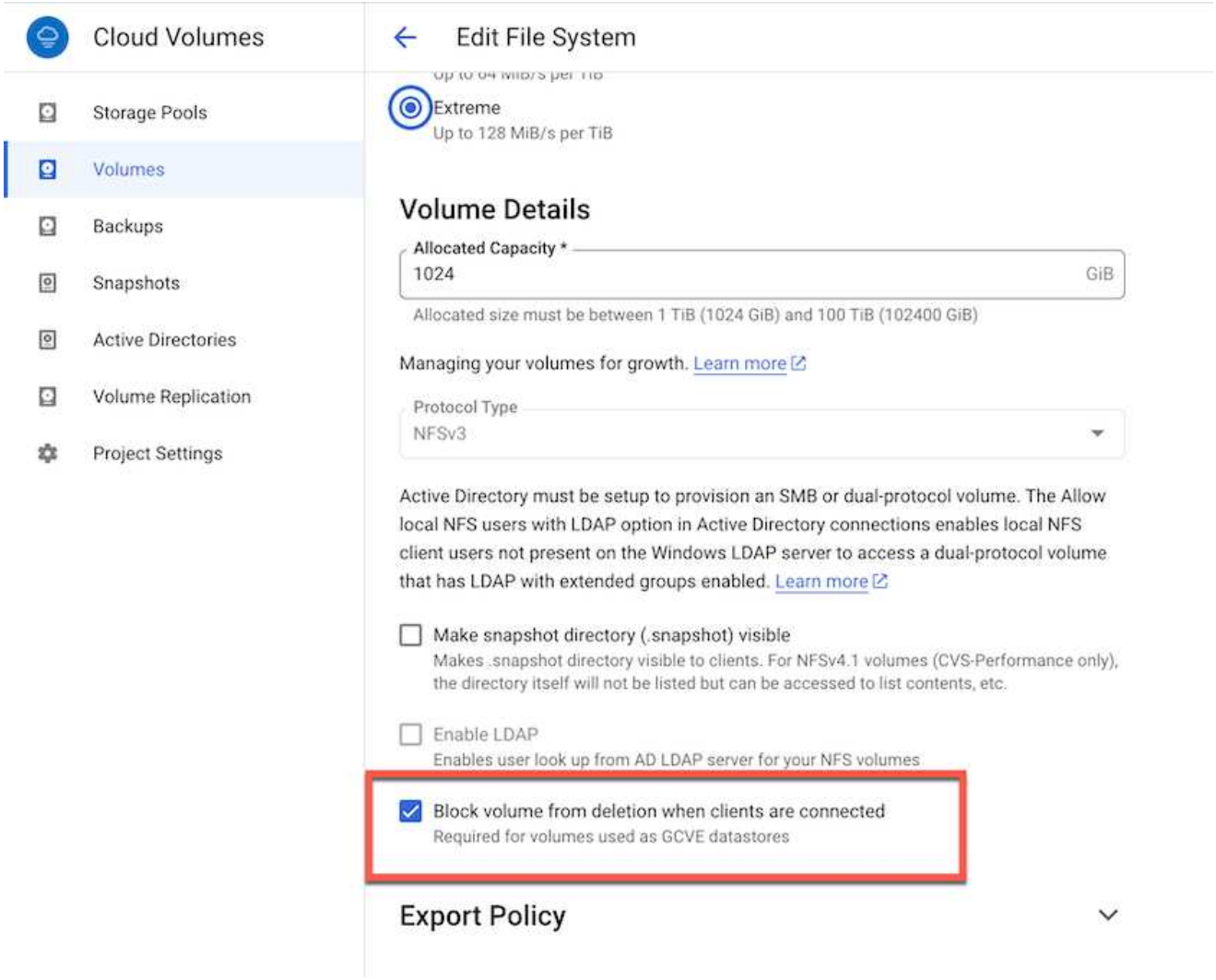
Étapes de déploiement pour monter un datastore NFS à partir de NetApp CVS sur GCVE

Provisionnement du volume CVS-Performance

Le volume du service NetApp Cloud Volume peut être provisionné par
"Via la console Google Cloud"
"À l'aide du portail ou de l'API NetApp BlueXP"

Marquez ce volume CVS comme non supprimable

Pour éviter toute suppression accidentelle du volume pendant l'exécution de la machine virtuelle, assurez-vous que le volume est marqué comme non supprimable, comme illustré dans la capture d'écran ci-dessous.



Pour plus d'informations, reportez-vous à la section "Création d'un volume NFS" documentation :

Assurez-vous que la connexion privée sur GCVE existe pour le VPC de tenant CVS NetApp.

Pour monter un datastore NFS, une connexion privée doit exister entre GCVE et le projet CVS NetApp. Pour plus d'informations, reportez-vous à la section "Comment configurer l'accès au service privé"

Montez le datastore NFS

Pour obtenir des instructions sur le montage d'un datastore NFS sur GCVE, reportez-vous à la section "Comment créer un datastore NFS avec NetApp CVS"

> Étant donné que les hôtes vSphere sont gérés par Google, vous n'avez pas accès à l'installation du pack d'installation vSphere (VIB) de l'API NFS vSphere pour l'intégration de baies (VAAI).
> Si vous avez besoin de la prise en charge des volumes virtuels (vVol), contactez-nous.
> Si vous souhaitez utiliser les trames Jumbo, reportez-vous à la section "Tailles MTU maximales prises en charge sur GCP"

Économies réalisées grâce au service NetApp Cloud volumes

Pour en savoir plus sur les économies que vous pouvez réaliser avec NetApp Cloud Volume Service pour répondre à vos besoins en stockage dans GCVE, veuillez consulter "Calculateur de ROI de NetApp"

Liens de référence

- "Blog Google - Comment utiliser NetApp CVS en tant que datastores pour Google Cloud VMware Engine"
- "Blog NetApp : un meilleur moyen de migrer vos applications riches en stockage vers Google Cloud"

Options de stockage NetApp pour GCP

GCP prend en charge le stockage NetApp connecté par l'invité avec Cloud Volumes ONTAP (CVO) ou Cloud Volumes Service (CVS).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, ou CVO, est la solution de gestion des données cloud leader qui repose sur le logiciel de stockage ONTAP de NetApp, disponible de façon native dans Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version Software-defined de ONTAP qui utilise le stockage cloud natif. Vous pouvez ainsi utiliser le même logiciel de stockage dans le cloud et sur site, limitant ainsi la nécessité de former à nouveau votre personnel IT à des méthodes entièrement nouvelles de gestion des données.

Ce logiciel permet au client de déplacer des données de la périphérie, vers le data Center, puis vers le cloud, et inversement, en réunissant votre cloud hybride, le tout géré à l'aide d'une console de gestion centralisée, NetApp Cloud Manager.

De par sa conception, CVO fournit des performances extrêmes et des fonctionnalités avancées de gestion de données pour répondre aux applications les plus exigeantes dans le cloud

Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité

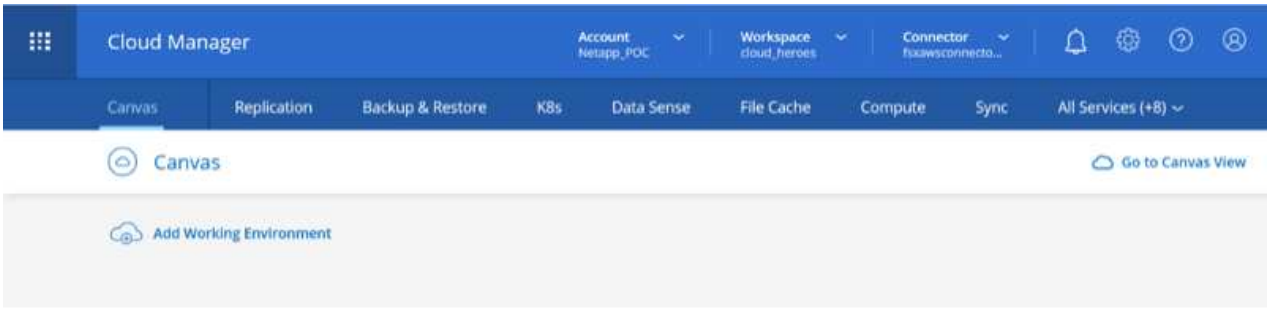
Déploiement de Cloud Volumes ONTAP dans Google Cloud (faites vous-même)

Les partages Cloud Volumes ONTAP et les LUN peuvent être montés à partir de machines virtuelles créées dans l'environnement de Cloud privé GCVE. Les volumes peuvent également être montés sur le client Linux, ainsi que sur les clients Windows et LES LUN, accessibles sur les clients Linux ou Windows en tant que périphériques de bloc lorsqu'ils sont montés sur iSCSI, car Cloud Volumes ONTAP prend en charge les protocoles iSCSI, SMB et NFS. Les volumes Cloud Volumes ONTAP peuvent être configurés en quelques étapes simples.

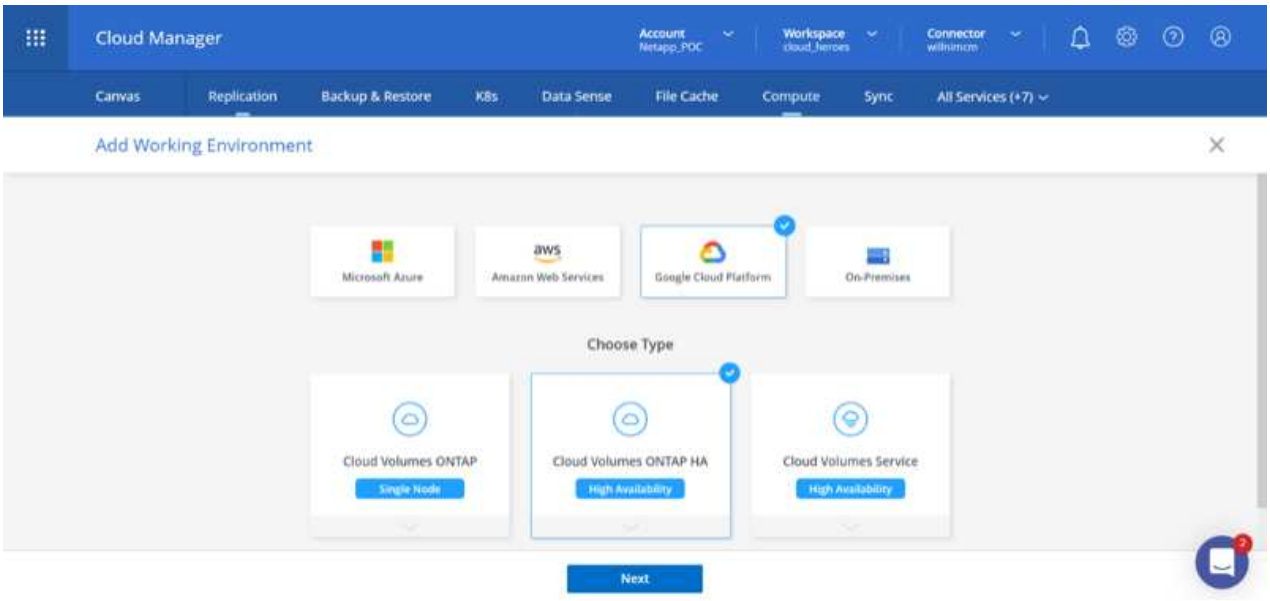
Pour répliquer des volumes depuis un environnement sur site vers le cloud à des fins de reprise d'activité ou de migration, établissez une connectivité réseau vers Google Cloud en utilisant un VPN site à site ou une interconnexion cloud. La réplication des données entre les sites et Cloud Volumes ONTAP n'est pas traitée dans ce document. Pour répliquer les données entre les systèmes Cloud Volumes ONTAP et sur site, consultez la section xref:./ehc/"Configuration de la réplication des données entre les systèmes".

Utiliser "Plus outil de dimensionnement Cloud Volumes ONTAP" Pour dimensionner précisément les instances Cloud Volumes ONTAP. Surveillez également les performances sur site et utilisez-les comme entrées dans le dimensionnement Cloud Volumes ONTAP.

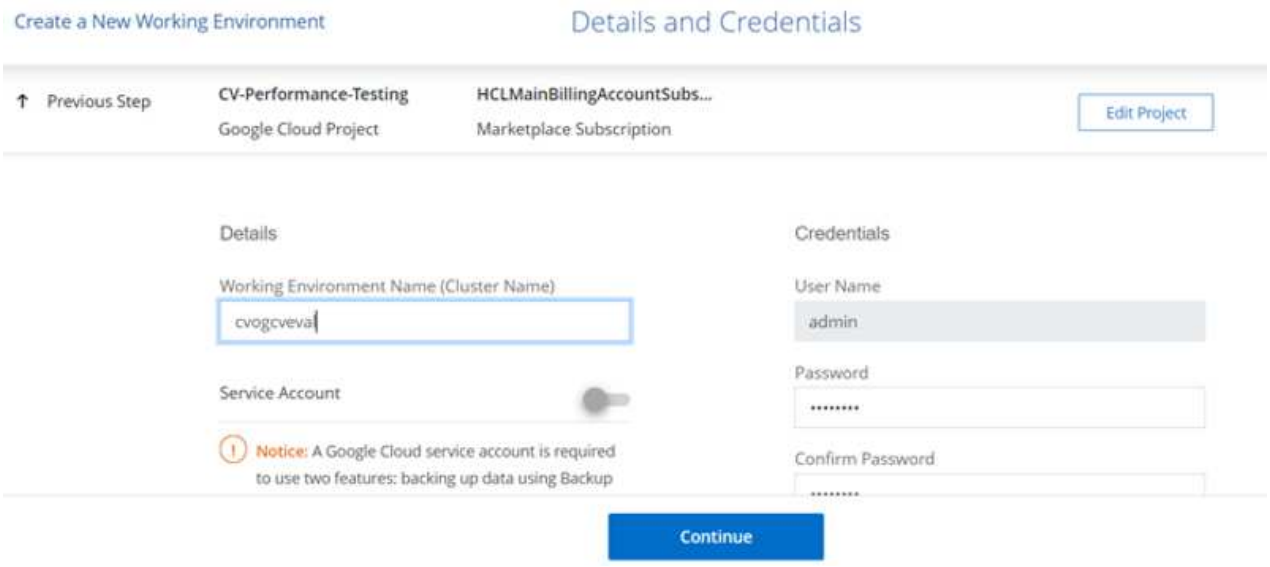
1. Connectez-vous à NetApp Cloud Central ; l'écran Fabric View s'affiche. Localisez l'onglet Cloud Volumes ONTAP et sélectionnez accéder à Cloud Manager. Une fois connecté, l'écran Canvas s'affiche.



2. Dans l'onglet Canvas de Cloud Manager, cliquez sur Ajouter un environnement de travail, puis sélectionnez Google Cloud Platform comme cloud et le type de configuration du système. Cliquez ensuite sur Suivant.

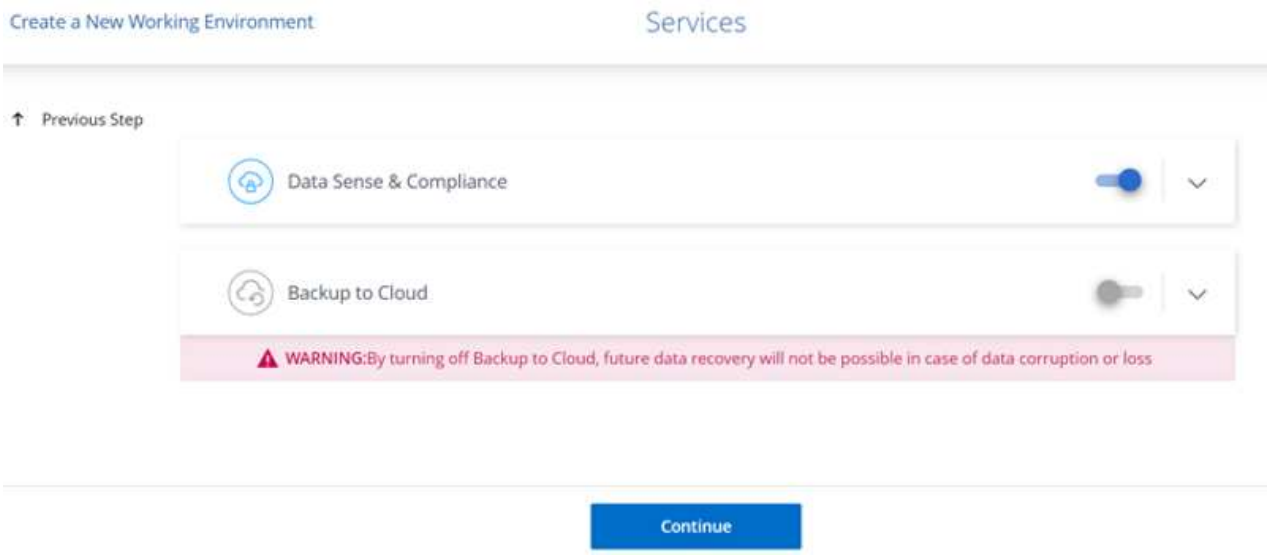


3. Fournissez les détails de l'environnement à créer, y compris le nom de l'environnement et les identifiants d'administrateur. Une fois que vous avez terminé, cliquez sur Continuer.

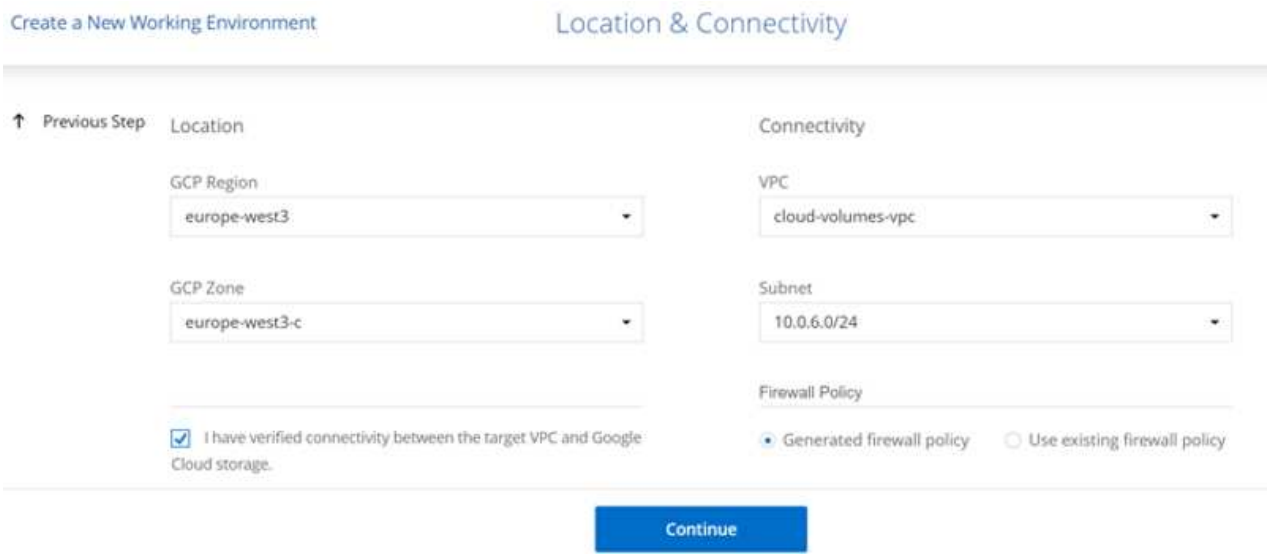


4. Sélectionnez ou désélectionnez les services complémentaires pour le déploiement Cloud Volumes ONTAP, y compris Data Sense & Compliance ou Backup to Cloud. Cliquez ensuite sur Continuer.

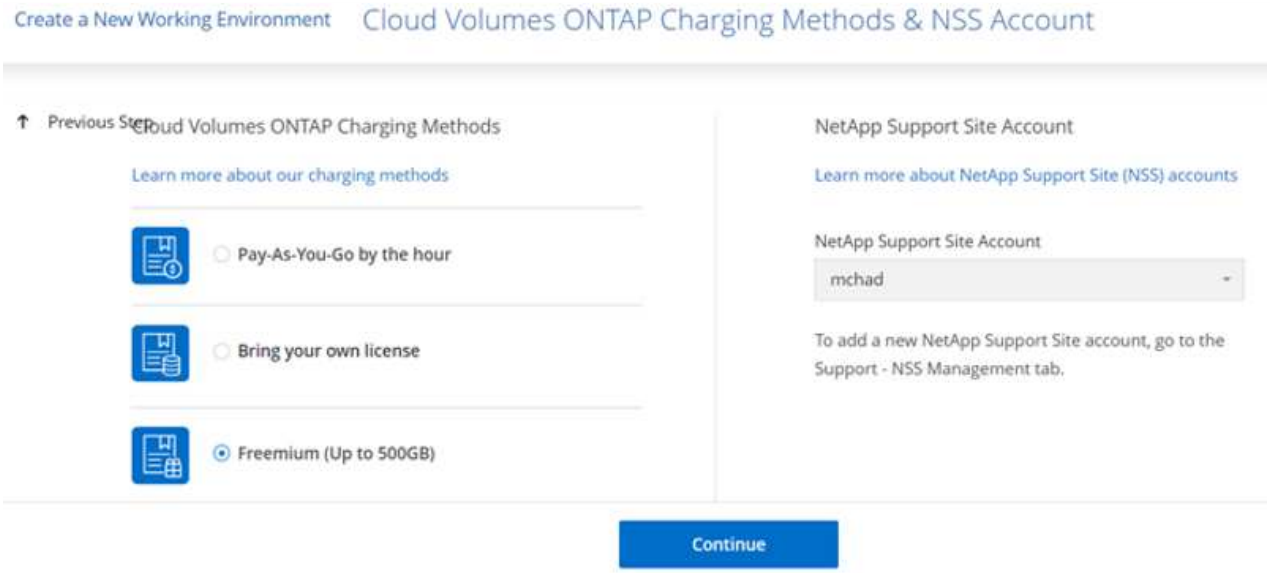
   CONSEIL : un message contextuel de vérification s'affiche lors de la désactivation des services complémentaires. Des services d'extension peuvent être ajoutés/supprimés après le déploiement de Cloud volumes ONTAP. Pour éviter les coûts, il est possible de les désélectionner à la fois si nécessaire.



5. Sélectionnez un emplacement, choisissez une politique de pare-feu et cochez la case pour confirmer la connectivité réseau au stockage Google Cloud.

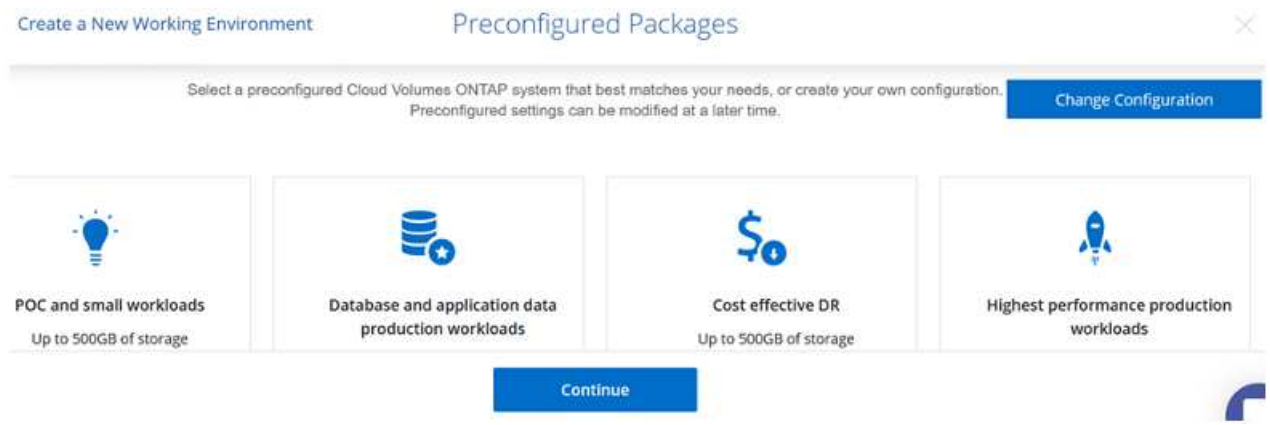


6. Sélectionnez l'option de licence : paiement à l'utilisation ou BYOL pour l'utilisation des licences existantes. Dans cet exemple, l'option Freemium est utilisée. Cliquez ensuite sur Continuer.

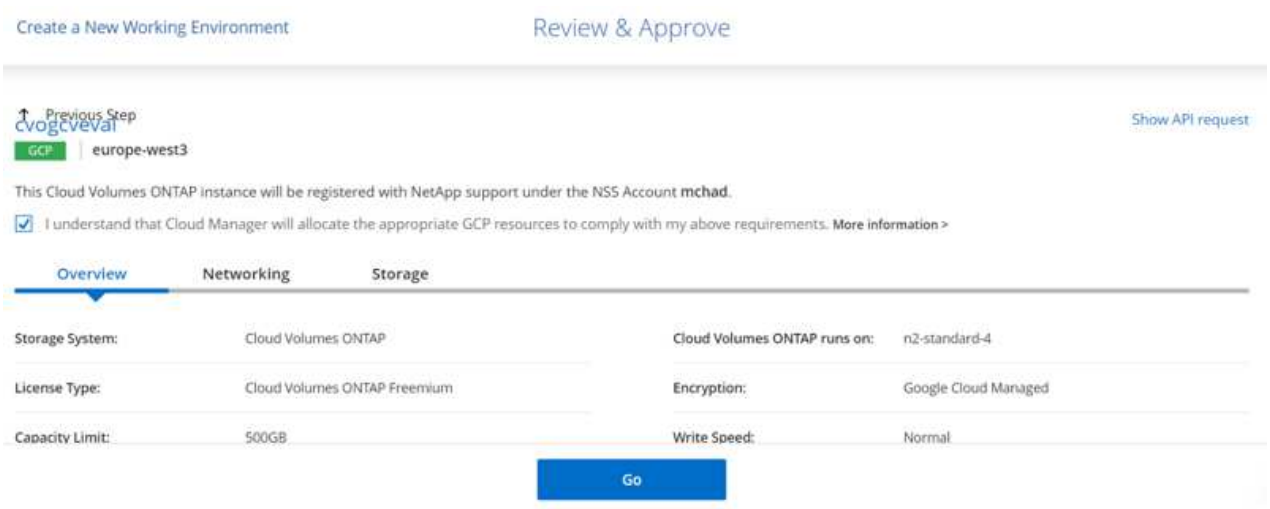


7. Sélectionnez un des packages préconfigurés disponibles en fonction du type de charge de travail qui sera déployé sur les machines virtuelles exécutées sur VMware Cloud sur AWS SDDC.

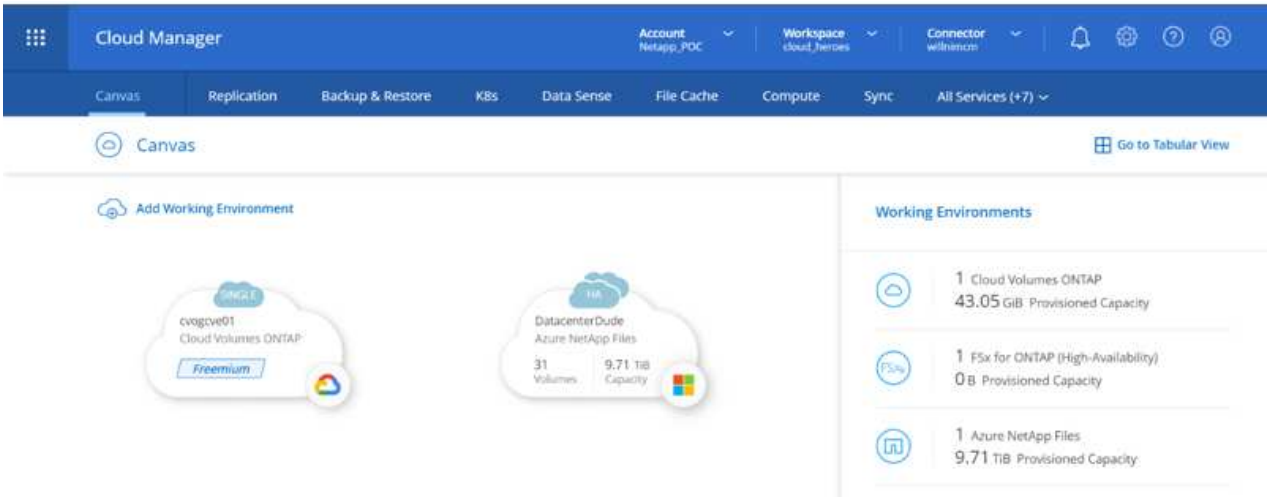
   CONSEIL : passez votre souris sur les mosaïques pour plus de détails ou personnalisez les composants CVO et la version de ONTAP en cliquant sur Modifier la configuration.



8. Sur la page révision et approbation, vérifiez et confirmez les sélections.pour créer l'instance Cloud Volumes ONTAP, cliquez sur Go.



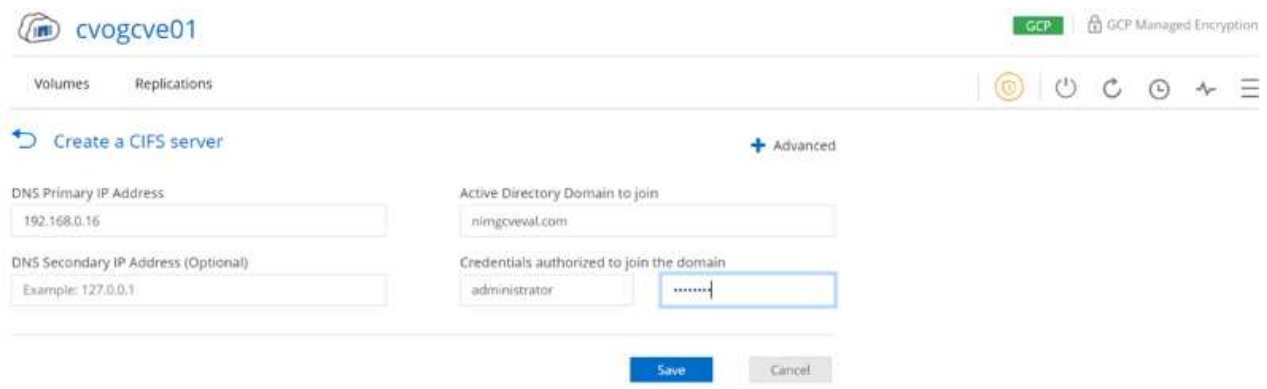
9. Une fois Cloud Volumes ONTAP provisionné, il apparaît dans les environnements de travail sur la page Canvas.



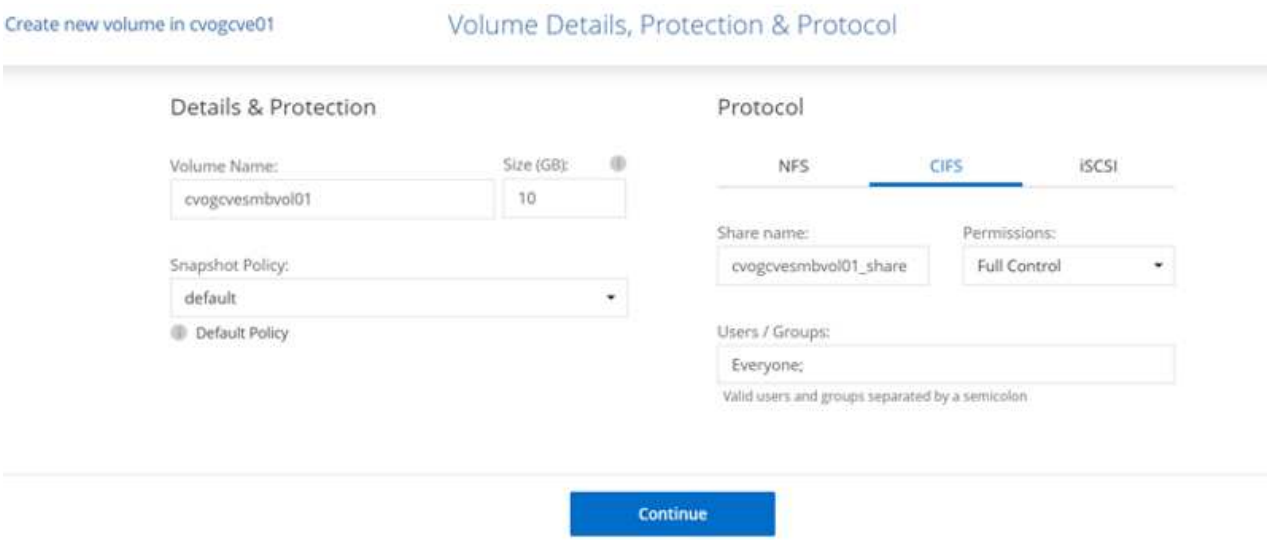
Configurations supplémentaires pour les volumes SMB

1. Une fois l'environnement de travail prêt, assurez-vous que le serveur CIFS est configuré avec les paramètres de configuration DNS et Active Directory appropriés. Cette étape est requise avant de pouvoir créer le volume SMB.

   CONSEIL : cliquez sur l'icône Menu (º), sélectionnez Avancé pour afficher plus d'options et sélectionnez Configuration CIFS.



2. La création du volume SMB est un processus simple. Dans Canvas, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP pour créer et gérer des volumes, puis cliquez sur l'option Créer un volume. Choisissez la taille appropriée et Cloud Manager choisit l'agrégat contenant ou utilisez un mécanisme d'allocation avancée pour placer sur un agrégat spécifique. Pour cette démonstration, CIFS/SMB est sélectionné comme protocole.

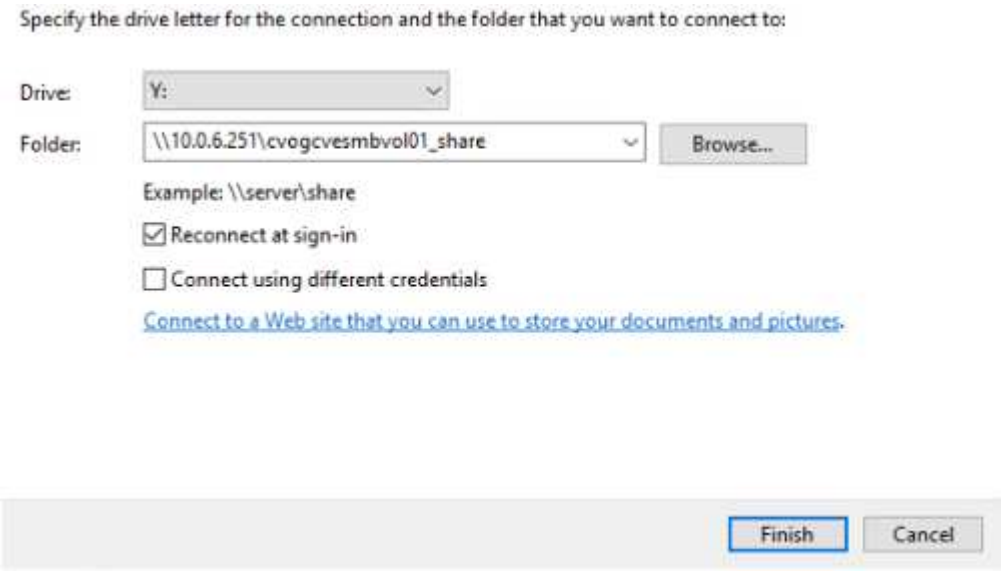


3. Une fois le volume provisionné, celui-ci est disponible sous le volet volumes. Comme un partage CIFS est provisionné, donnez à vos utilisateurs ou groupes l'autorisation d'accéder aux fichiers et dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier. Cette étape n'est pas requise si le volume est répliqué à partir d'un environnement sur site, car les autorisations liées aux fichiers et aux dossiers sont toutes conservées dans le cadre de la réplication SnapMirror.

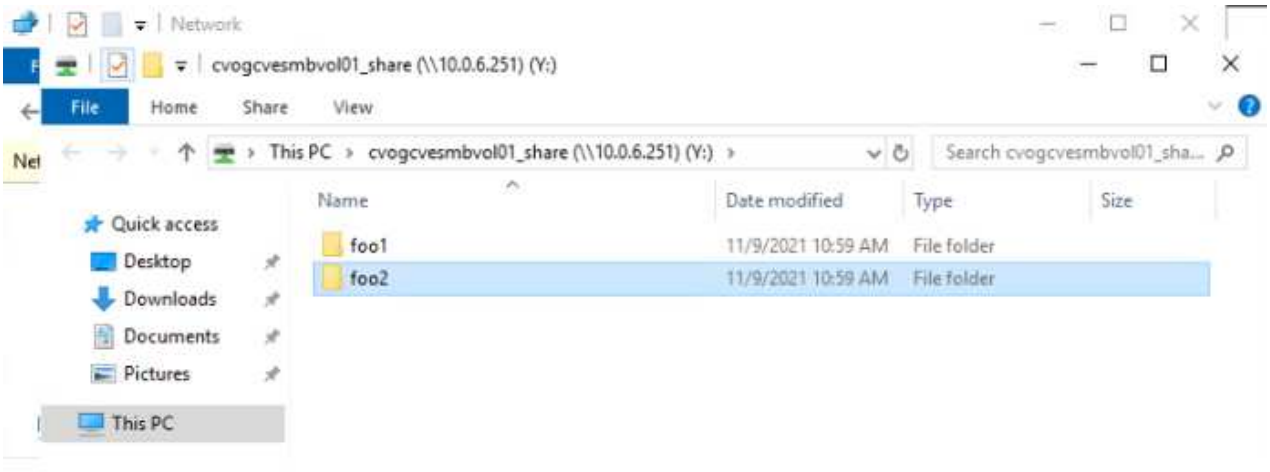
   CONSEIL : cliquez sur le menu du volume (º) pour afficher ses options.

4. Une fois le volume créé, utilisez la commande mount pour afficher les instructions de connexion du volume, puis connectez-vous au partage des machines virtuelles sur Google Cloud VMware Engine.

5. Copiez le chemin suivant et utilisez l'option Map Network Drive pour monter le volume sur la machine virtuelle exécutée sur Google Cloud VMware Engine.



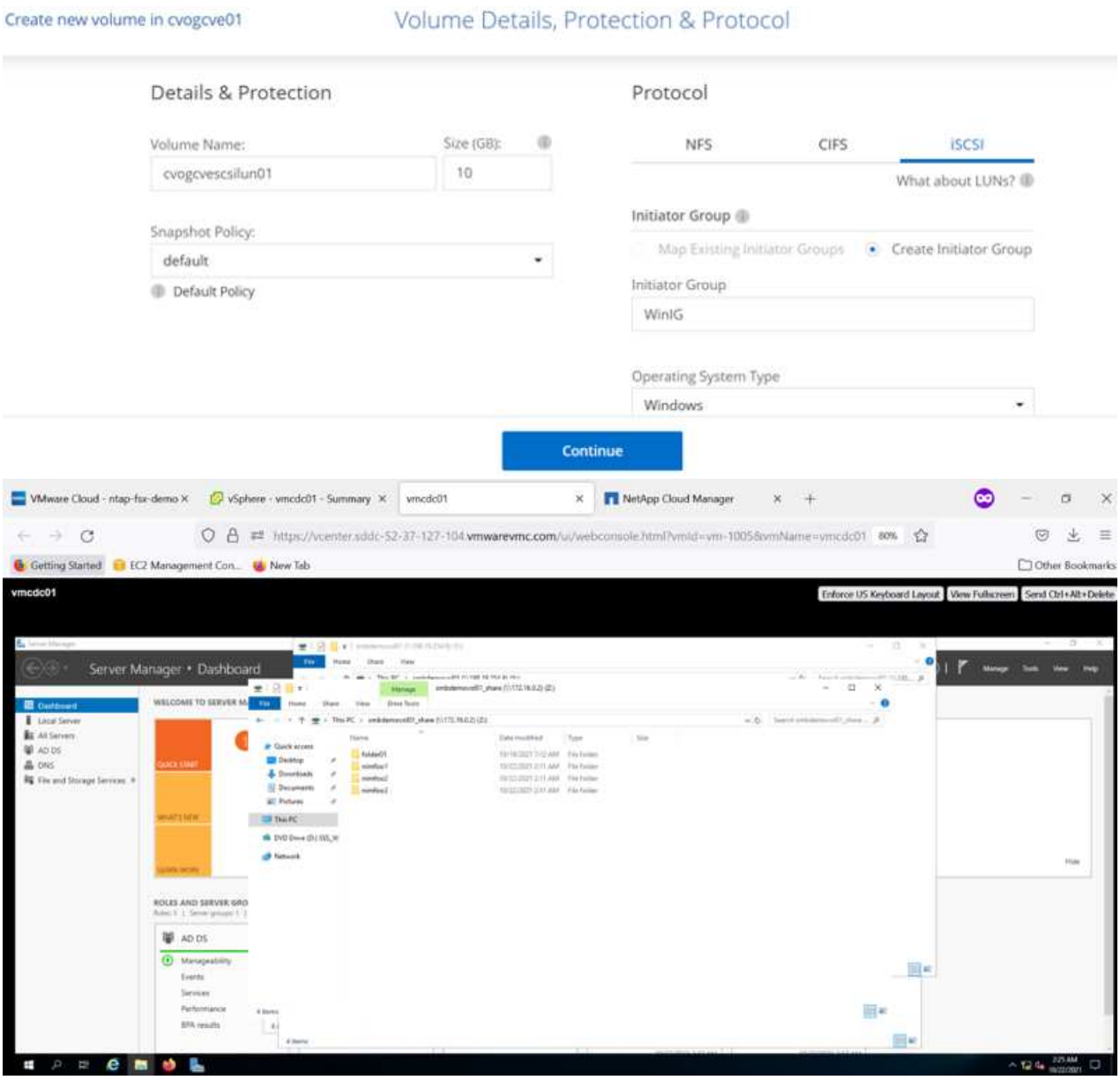
Une fois mappé, il est facilement accessible et les autorisations NTFS peuvent être définies en conséquence.



Connectez le LUN de Cloud Volumes ONTAP à un hôte

Pour connecter le LUN Cloud Volumes ONTAP à un hôte, procédez comme suit :

1. Sur la page Canevas, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP pour créer et gérer des volumes.
2. Cliquez sur Ajouter un volume > Nouveau volume, sélectionnez iSCSI et cliquez sur Créer un groupe d'initiateurs. Cliquez sur Continuer .



3. Une fois le volume provisionné, sélectionnez le menu volume (º), puis cliquez sur IQN cible. Pour copier le nom qualifié iSCSI (IQN), cliquez sur Copier. Configurez une connexion iSCSI de l'hôte vers le LUN.

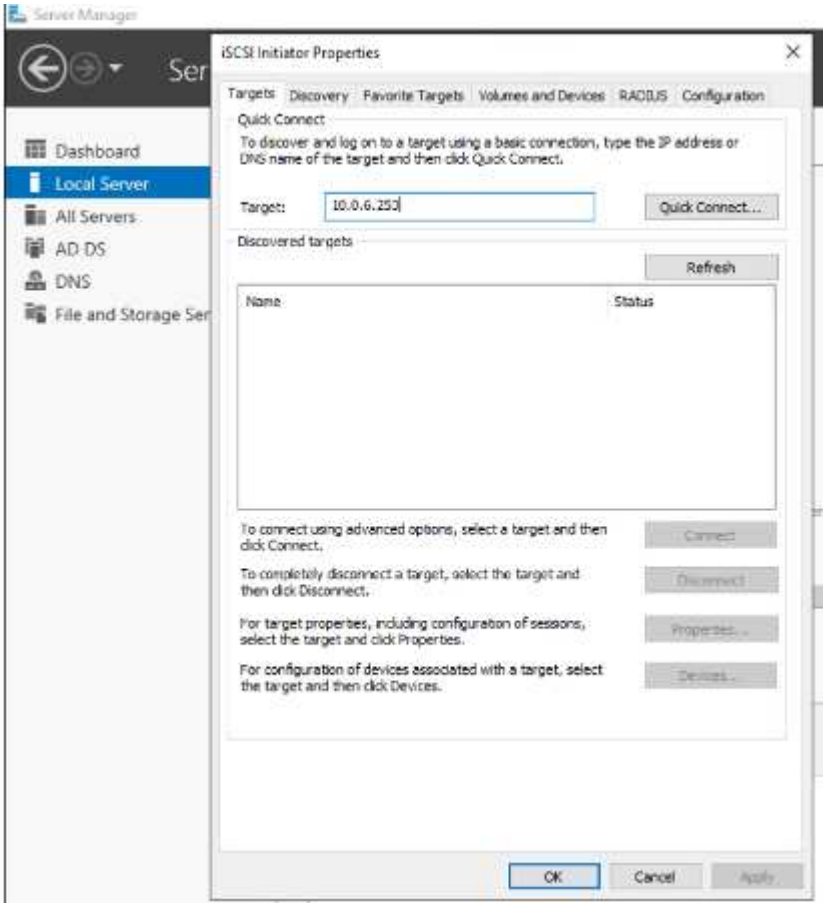
Pour procéder de la même manière pour l'hôte résidant sur Google Cloud VMware Engine :

1. RDP sur la machine virtuelle hébergée sur Google Cloud VMware Engine.
2. Ouvrez la boîte de dialogue Propriétés de l'initiateur iSCSI : Gestionnaire de serveur > Tableau de

bord > Outils > initiateur iSCSI.

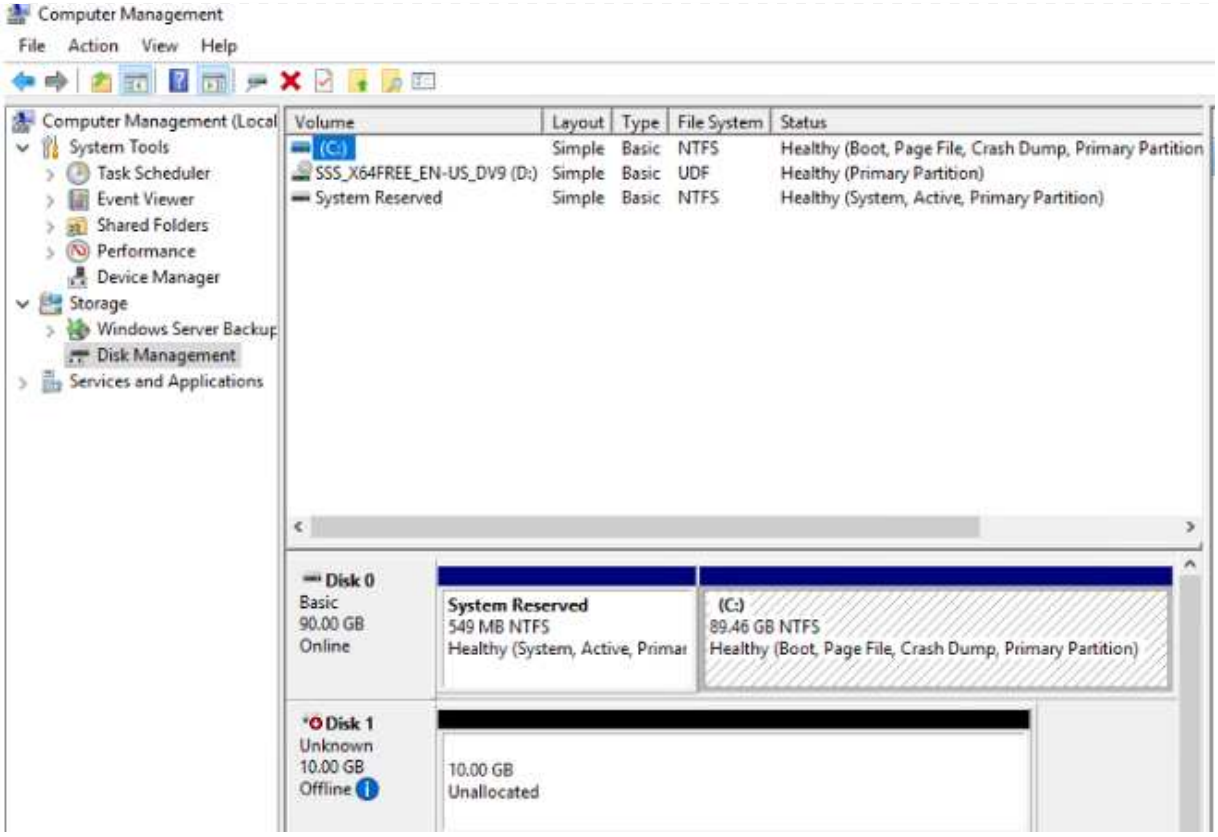
3. Dans l'onglet découverte, cliquez sur Discover Portal ou Add Portal, puis entrez l'adresse IP du port cible iSCSI.
4. Dans l'onglet cibles, sélectionnez la cible découverte, puis cliquez sur connexion ou connexion.
5. Sélectionnez Activer le multichemin, puis sélectionnez Restaurer automatiquement cette connexion lorsque l'ordinateur démarre ou Ajouter cette connexion à la liste des cibles favorites. Cliquez sur Avancé.

> L'hôte Windows doit disposer d'une connexion iSCSI à chaque nœud du cluster. Le DSM natif sélectionne les meilleurs chemins d'accès à utiliser.



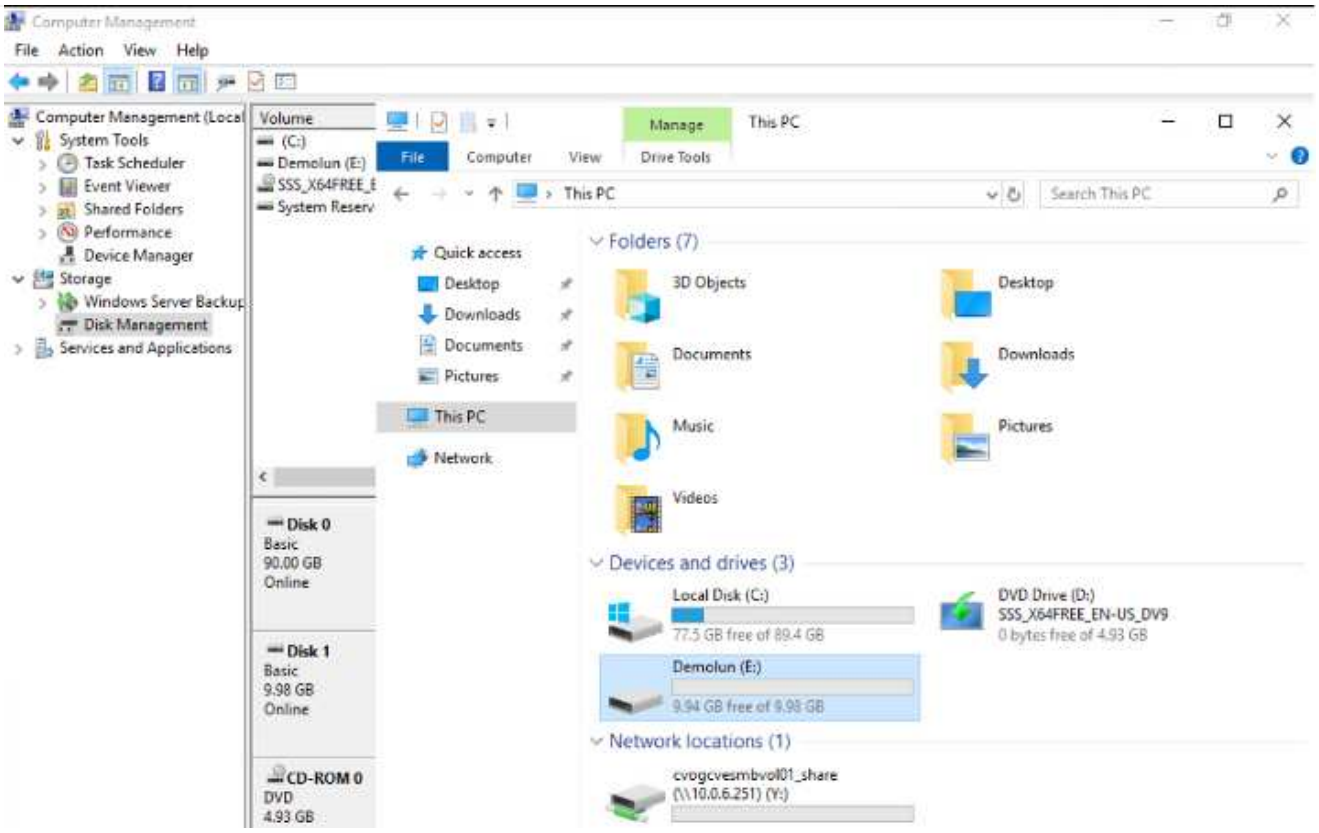
Les LUN présentes sur la machine virtuelle de stockage (SVM) apparaissent sous forme de disques pour l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclencher une nouvelle analyse manuelle pour détecter les disques en procédant comme suit :

a. Ouvrez l'utilitaire de gestion de l'ordinateur Windows : Démarrer > Outils d'administration > gestion de l'ordinateur.
b. Développez le nœud stockage dans l'arborescence de navigation.
c. Cliquez sur gestion des disques.
d. Cliquez sur action > Rescan Disks.



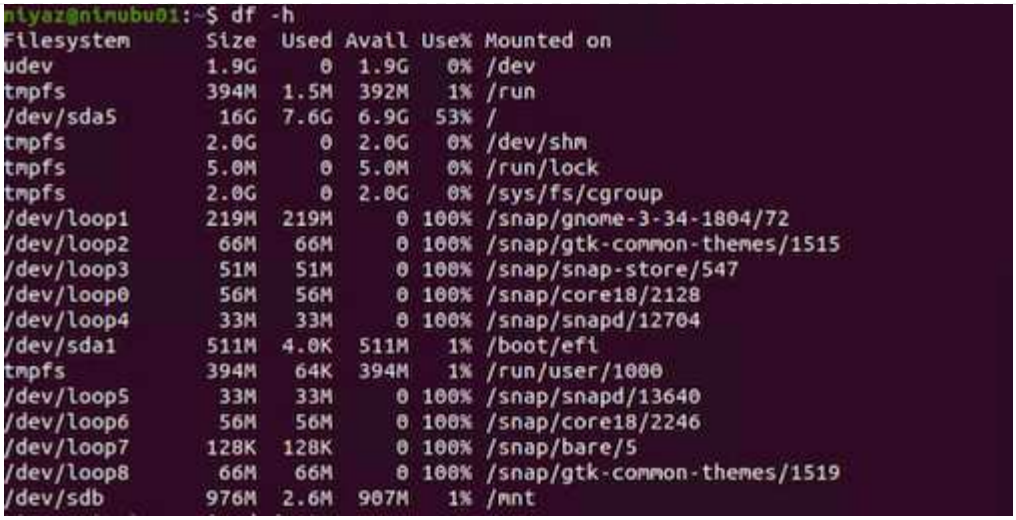
Lorsqu'un nouvel LUN est accédé pour la première fois par l'hôte Windows, il n'a pas de partition ni de système de fichiers. Initialiser la LUN ; et éventuellement formater la LUN avec un système de fichiers en effectuant la procédure suivante :

a. Démarrez Windows Disk Management.
b. Cliquez avec le bouton droit de la souris sur la LUN, puis sélectionnez le type de disque ou de partition requis.
c. Suivez les instructions de l'assistant. Dans cet exemple, le lecteur F: Est monté.



Sur les clients Linux, assurez-vous que le démon iSCSI est en cours d'exécution. Une fois les LUN provisionnées, consultez ici les conseils détaillés sur la configuration iSCSI avec Ubuntu. Pour vérifier, exécutez lsblk cmd à partir du shell.

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

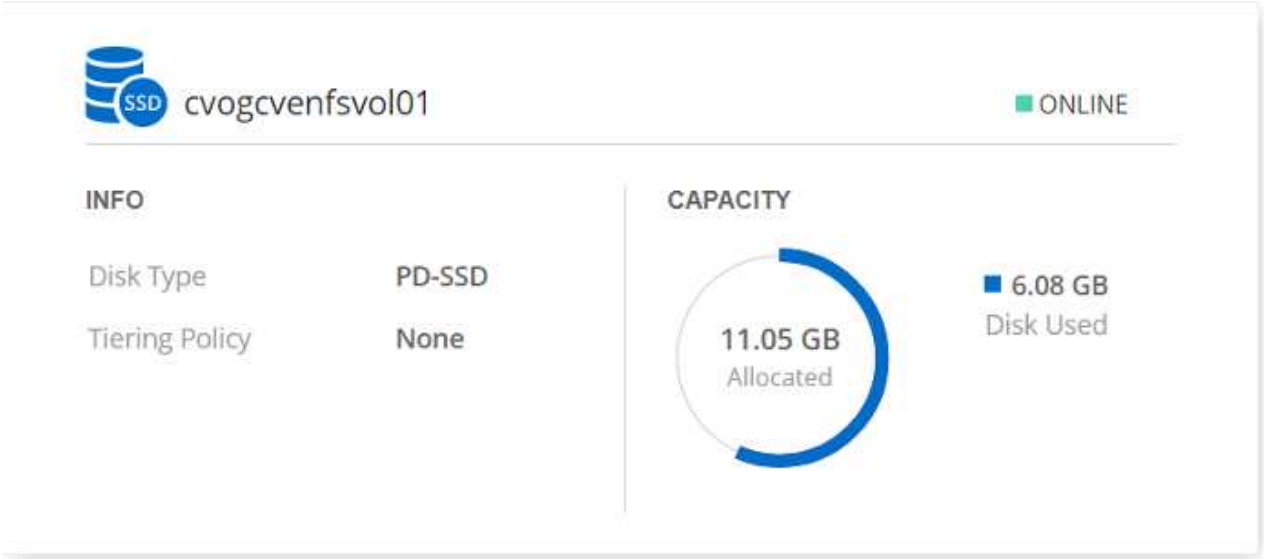

niyaz@ninubu01:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.5M 392M 1% /run
/dev/sda5 16G 7.6G 6.9G 53% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop1 219M 219M 0 100% /snap/gnome-3-34-1804/72
/dev/loop2 66M 66M 0 100% /snap/gtk-common-themes/1515
/dev/loop3 51M 51M 0 100% /snap/snap-store/547
/dev/loop0 56M 56M 0 100% /snap/core18/2128
/dev/loop4 33M 33M 0 100% /snap/snapd/12704
/dev/sda1 511M 4.0K 511M 1% /boot/efi
tmpfs 394M 64K 394M 1% /run/user/1000
/dev/loop5 33M 33M 0 100% /snap/snapd/13640
/dev/loop6 56M 56M 0 100% /snap/core18/2246
/dev/loop7 128K 128K 0 100% /snap/bare/5
/dev/loop8 66M 66M 0 100% /snap/gtk-common-themes/1519
/dev/sdb 976M 2.6M 907M 1% /mnt

Montez un volume NFS Cloud Volumes ONTAP sur un client Linux

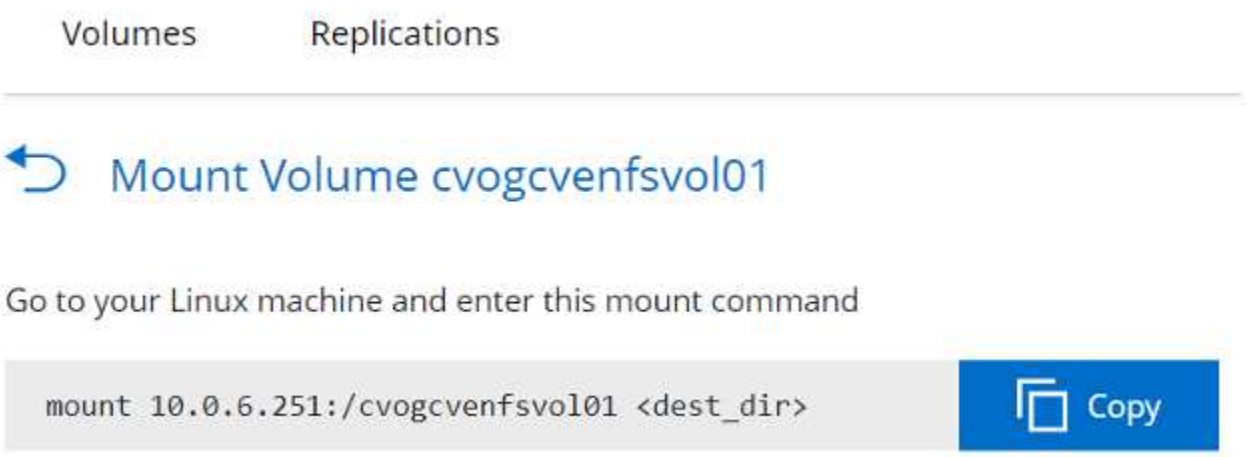
Pour monter le système de fichiers Cloud Volumes ONTAP (DIY) depuis des VM dans Google Cloud VMware Engine, effectuez la procédure suivante :

Procédez au provisionnement du volume en suivant les étapes ci-dessous

1. Dans l'onglet Volumes , cliquez sur Créer un nouveau volume .
2. Sur la page Créer un nouveau volume, sélectionnez un type de volume :



3. Dans l'onglet volumes, placez le curseur de la souris sur le volume, sélectionnez l'icône de menu (º), puis cliquez sur commande de montage.



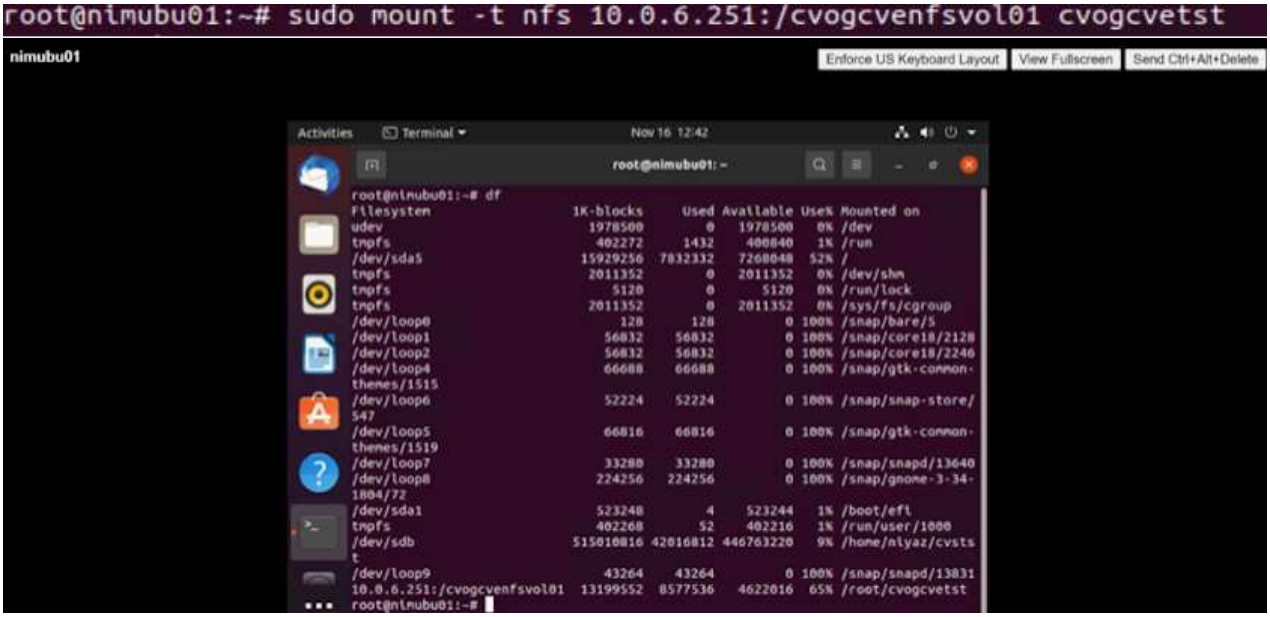
4. Cliquez sur Copier .
5. Connectez-vous à l'instance Linux désignée.
6. Ouvrez un terminal sur l'instance à l'aide du shell sécurisé (SSH) et connectez-vous avec les informations d'identification appropriées.
7. Créer un répertoire pour le point de montage du volume avec la commande suivante.

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. Montez le volume NFS Cloud Volumes ONTAP dans le répertoire créé à l'étape précédente.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Cloud Volumes Service (CVS)

Cloud volumes Services (CVS) est un portefeuille complet de services de données pour proposer des solutions cloud avancées. Cloud volumes Services prend en charge plusieurs protocoles d'accès aux fichiers pour les principaux fournisseurs de cloud (prise en charge NFS et SMB).

Les autres avantages et fonctionnalités sont les suivants : protection et restauration des données avec Snapshot, fonctionnalités spéciales de réplication, de synchronisation et de migration des données sur site ou dans le cloud, et haute performance prévisible au niveau d'un système de stockage Flash dédié.

Cloud Volumes Service (CVS) comme stockage connecté invité

Configurez Cloud Volumes Service avec VMware Engine

Les partages Cloud Volumes Service peuvent être montés sur les machines virtuelles qui sont créées dans l'environnement VMware Engine. Les volumes peuvent également être montés sur le client Linux et mappés sur le client Windows, car Cloud Volumes Service prend en charge les protocoles SMB et NFS. Les volumes Cloud Volumes Service peuvent être configurés en étapes simples.

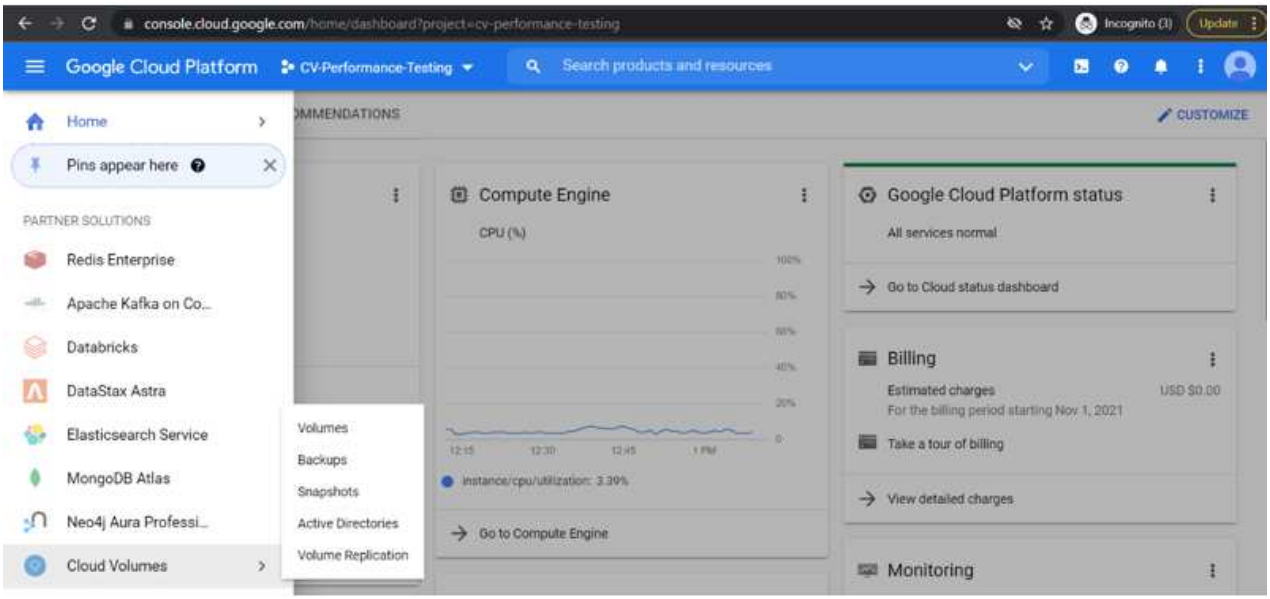
Cloud volumes Service et le cloud privé Google Cloud VMware Engine doivent se trouver dans la même région.

Pour acheter, activer et configurer NetApp Cloud Volumes Service pour Google Cloud depuis Google Cloud Marketplace, suivez cette section "guide".

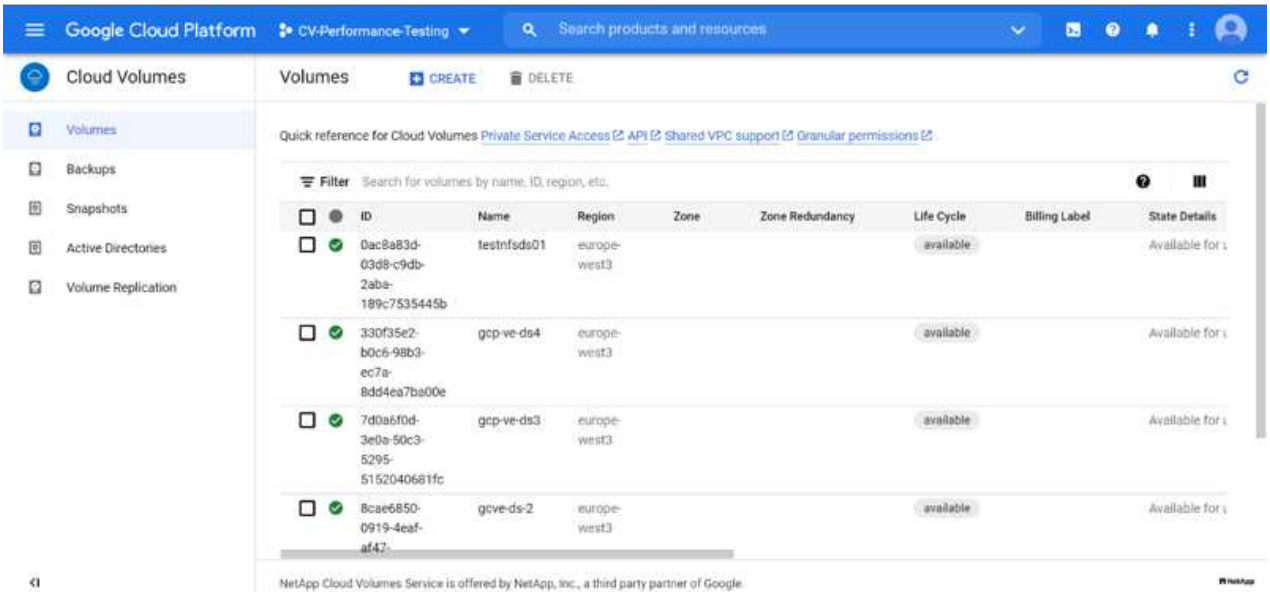
Créez un volume NFS CVS dans le Cloud privé GCVE

Pour créer et monter des volumes NFS, procédez comme suit :

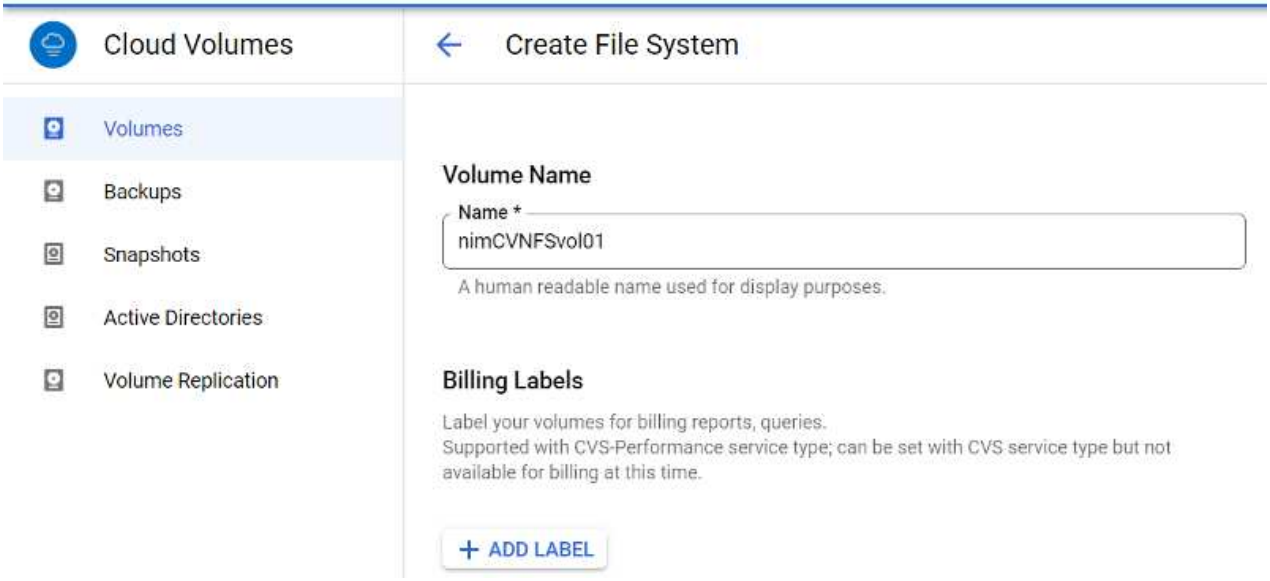
1. Accédez à Cloud volumes à partir des solutions partenaires dans la console Google Cloud.



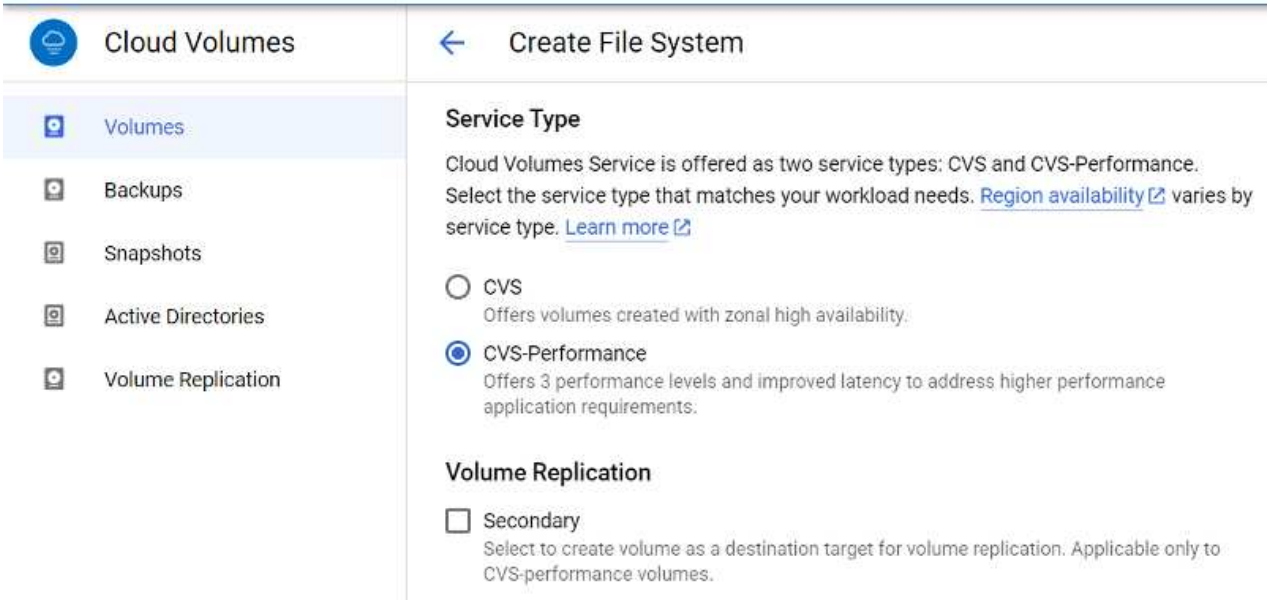
2. Dans la console Cloud volumes, accédez à la page volumes et cliquez sur Créer.



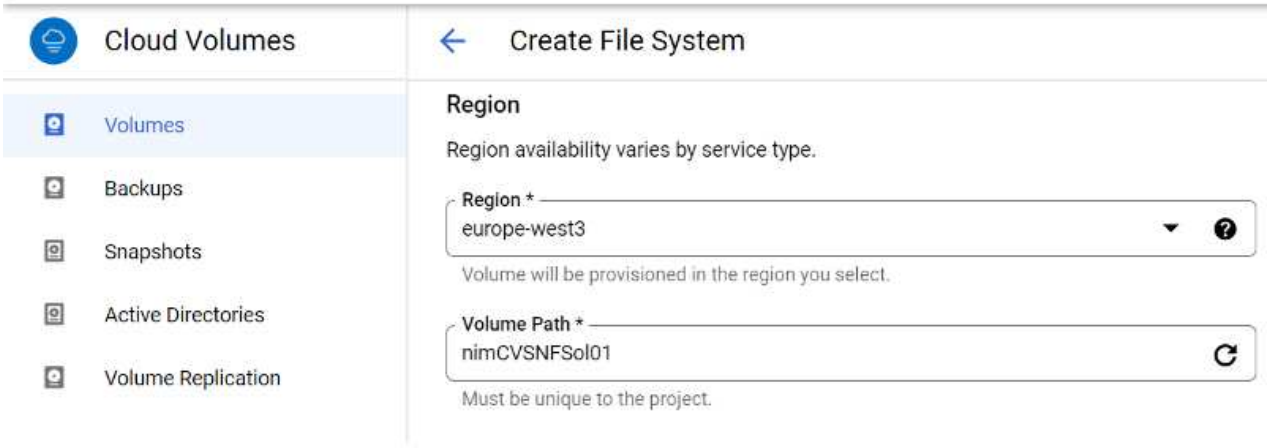
3. Sur la page Créer un système de fichiers, spécifiez le nom du volume et les libellés de facturation requis pour les mécanismes de refacturation.



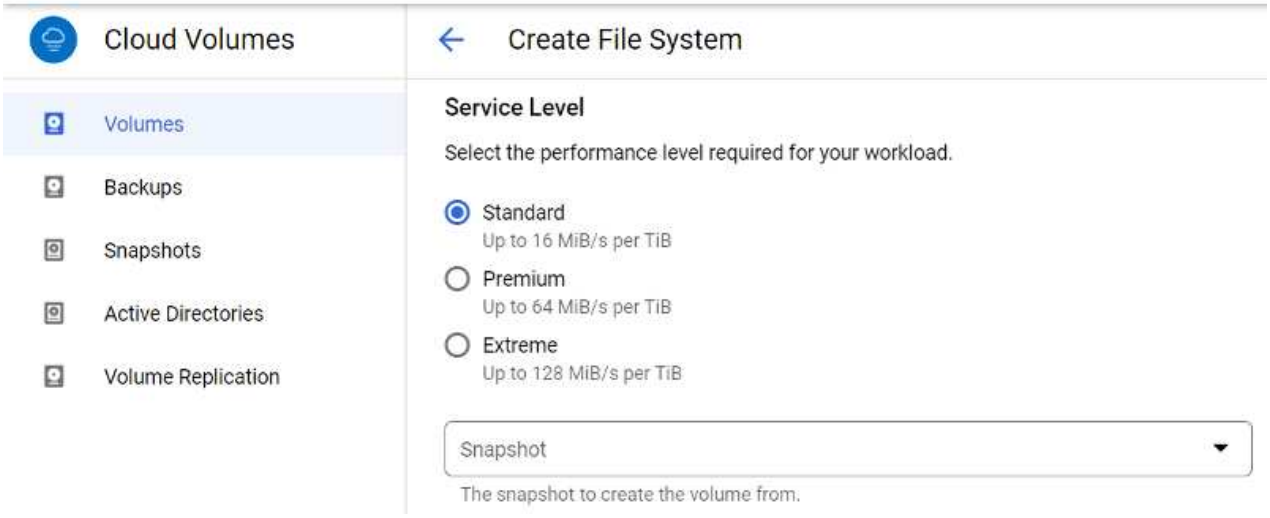
4. Sélectionnez le service approprié. Pour GCVE, choisissez CVS-Performance et le niveau de service souhaité pour une latence améliorée et des performances supérieures en fonction des exigences des charges de travail applicatives.



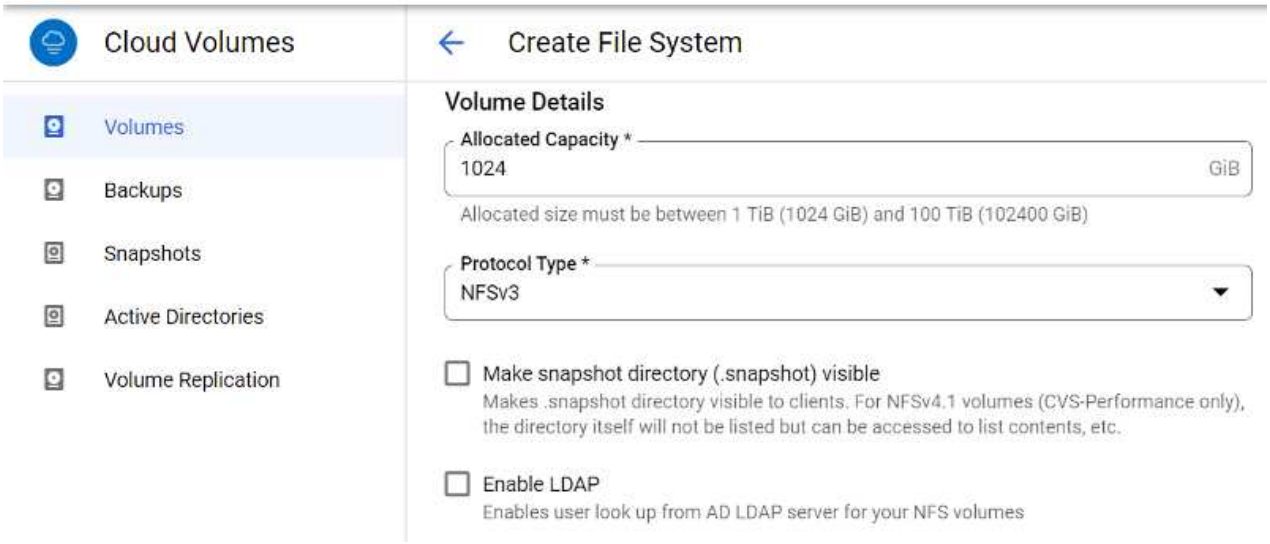
5. Spécifier la région Google Cloud pour le chemin de volume et de volume (le chemin du volume doit être unique sur l'ensemble des volumes cloud du projet)



6. Sélectionnez le niveau de performances du volume.

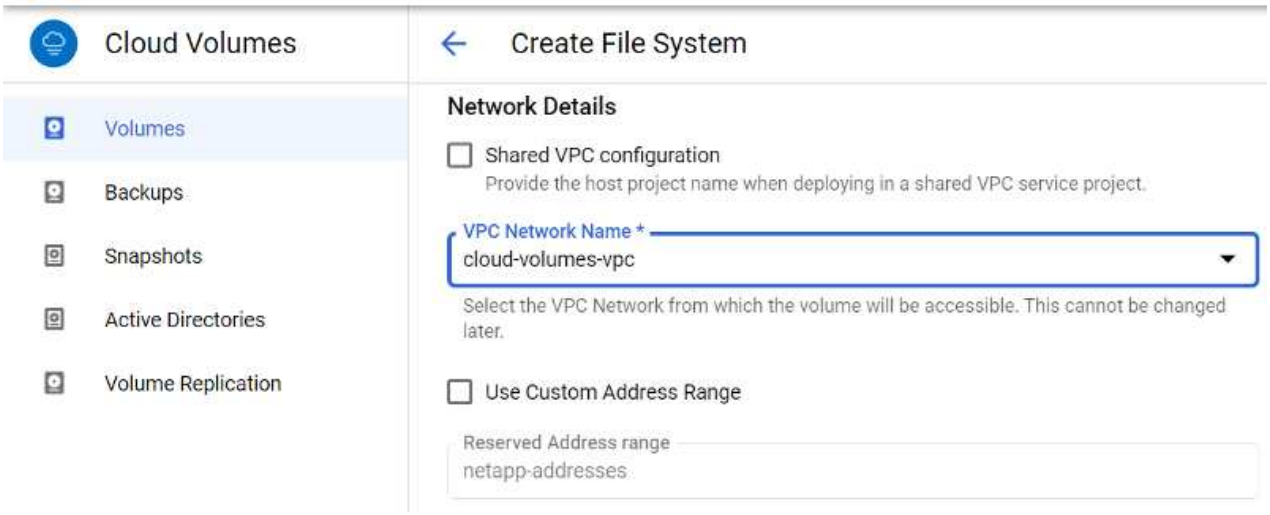


7. Spécifiez la taille du volume et le type de protocole. Lors de ce test, NFSv3 est utilisé.



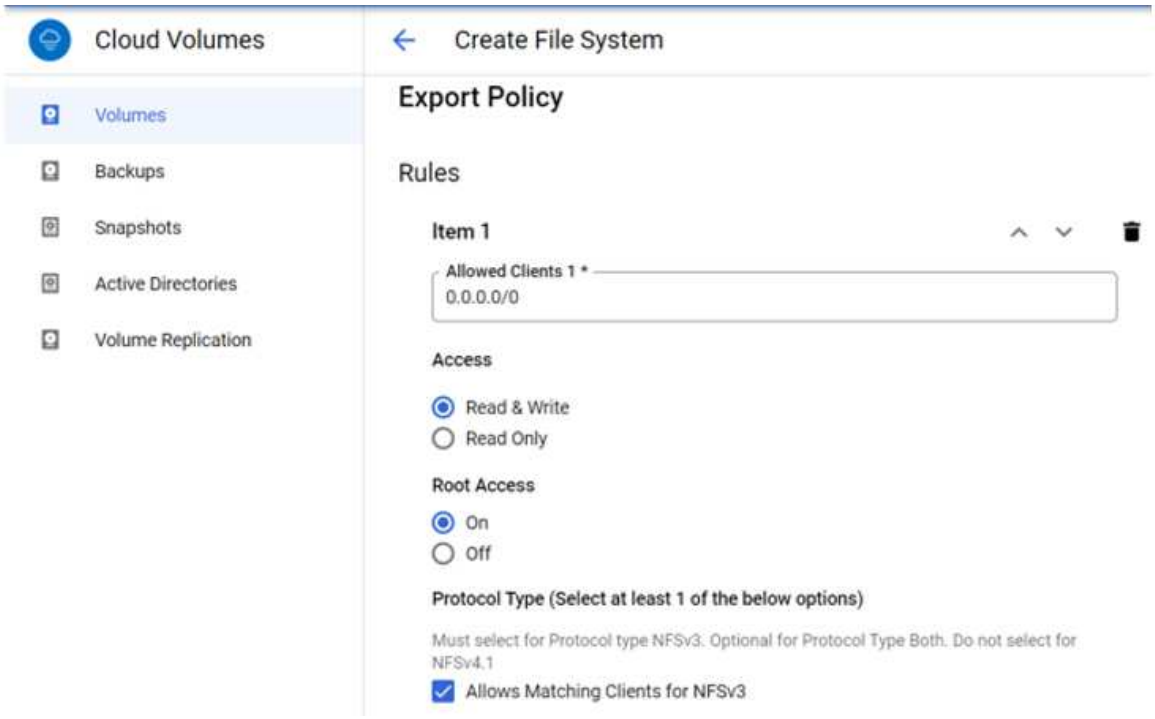
8. Au cours de cette étape, sélectionnez le réseau VPC à partir duquel le volume sera accessible. Assurez-vous que le peering VPC est en place.

CONSEIL : si le peering VPC n'a pas été effectué, un bouton contextuel s'affiche pour vous guider à travers les commandes de peering. Ouvrez une session Cloud Shell et exécutez les commandes appropriées pour peer-to-peer votre VPC avec le producteur Cloud Volumes Service. Au cas où vous décidiez de préparer le peering de VPC au préalable, reportez-vous à ces instructions.



9. Gérez les règles de stratégie d'exportation en ajoutant les règles appropriées et cochez la case correspondant à la version NFS correspondante.

   Remarque : l'accès aux volumes NFS n'est possible que si une export policy est ajoutée.



10. Cliquez sur Enregistrer pour créer le volume.

Montage des exportations NFS vers les machines virtuelles s'exécutant sur VMware Engine

Avant de préparer le montage du volume NFS, assurez-vous que l'état de peering de la connexion privée est défini sur actif. Une fois l'état actif, utilisez la commande mount.

Pour monter un volume NFS, procédez comme suit :

1. Dans Cloud Console, accédez à Cloud volumes > volumes.
2. Accédez à la page volumes
3. Cliquez sur le volume NFS pour lequel vous souhaitez monter les exports NFS.
4. Faites défiler vers la droite, sous Afficher plus, cliquez sur instructions de montage.

Pour effectuer le processus de montage à partir du système d'exploitation invité de la machine virtuelle VMware, procédez comme suit :

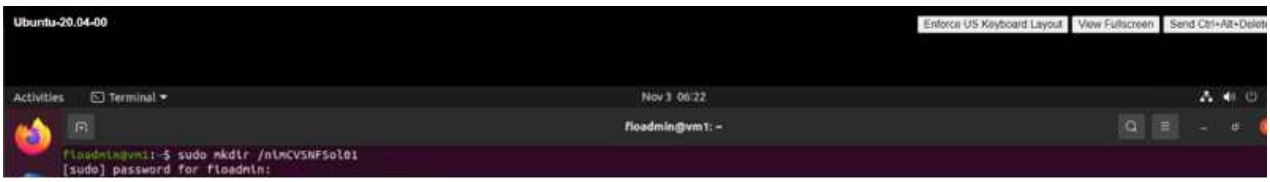
1. Utilisez le client SSH et SSH sur la machine virtuelle.
2. Installez le client nfs sur l'instance.
   a. Sur l'instance Red Hat Enterprise Linux ou SUSE Linux :

```
 sudo yum install -y nfs-utils
.. Sur une instance Ubuntu ou Debian :
```

```
sudo apt-get install nfs-common
```

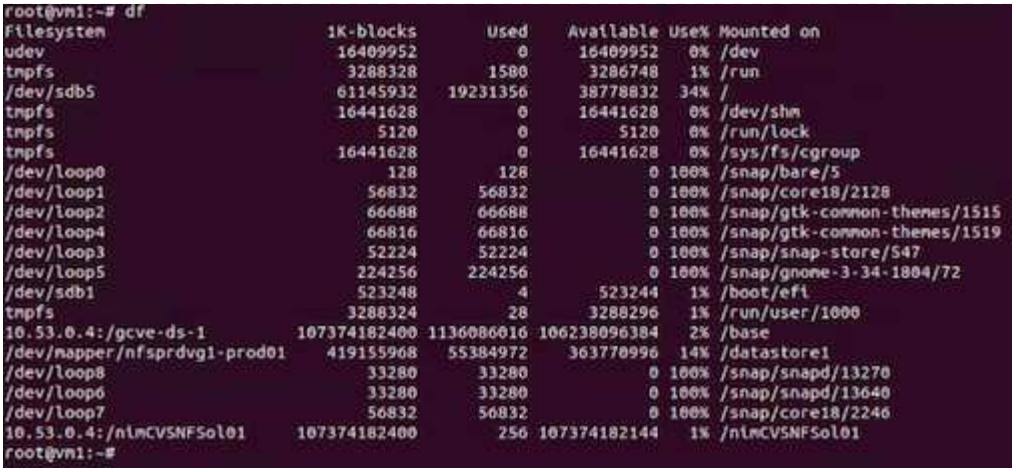
3. Créer un nouveau répertoire sur l'instance, tel que "/CVnimSNFSol01" :

```
sudo mkdir /nimCVSNFSol01
```



4. Montez le volume à l'aide de la commande appropriée. L'exemple de commande de l'exercice pratique est ci-dessous :

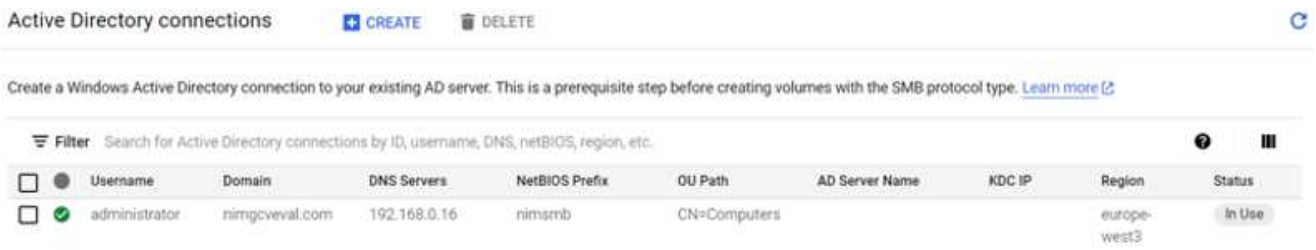
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400  1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01     419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

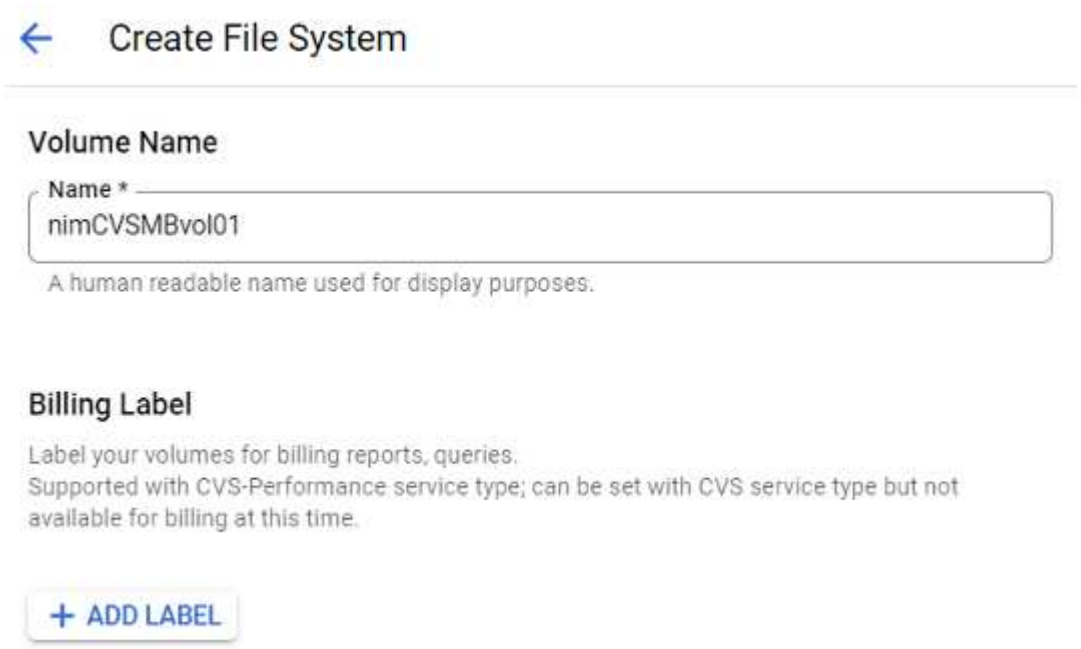
Création et montage du partage SMB sur des machines virtuelles exécutées sur VMware Engine

Pour les volumes SMB, assurez-vous que les connexions Active Directory sont configurées avant de créer le volume SMB.

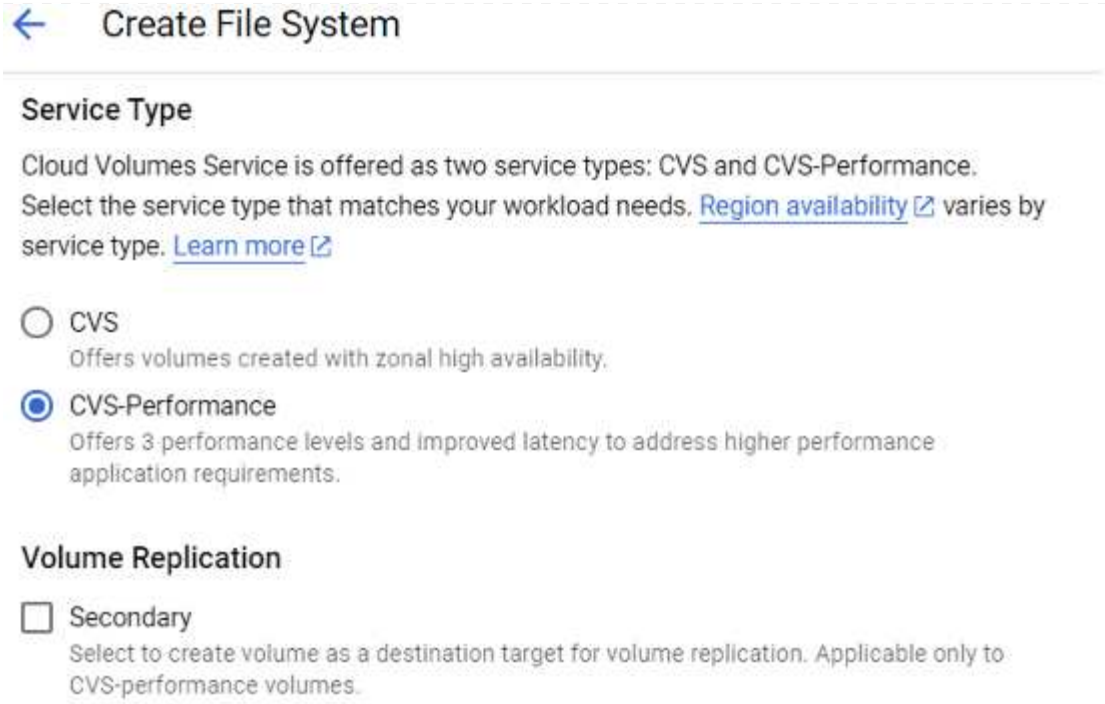


Une fois la connexion AD en place, créez le volume avec le niveau de service souhaité. Les étapes sont telles que la création du volume NFS, sauf la sélection du protocole approprié.

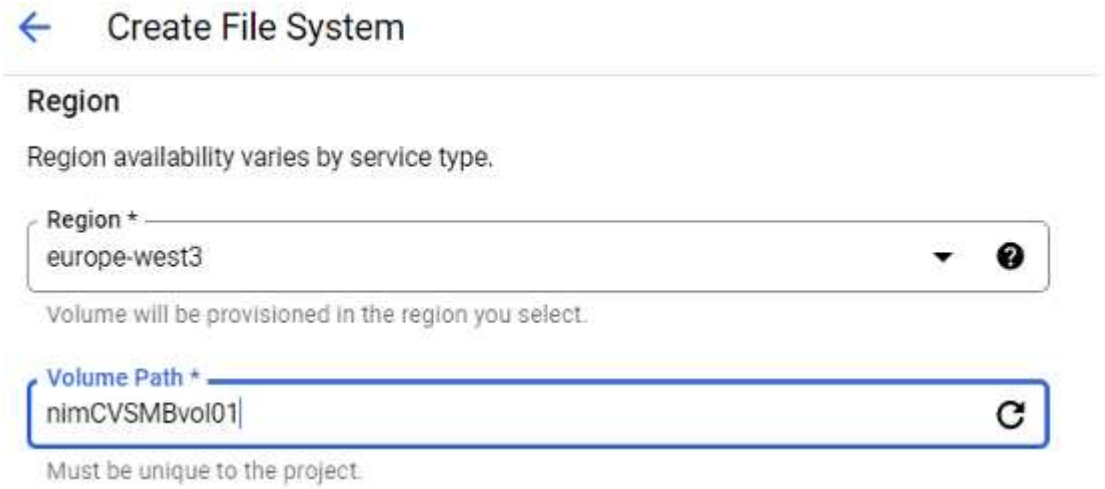
1. Dans la console Cloud volumes, accédez à la page volumes et cliquez sur Créer.
2. Sur la page Créer un système de fichiers, spécifiez le nom du volume et les libellés de facturation requis pour les mécanismes de refacturation.



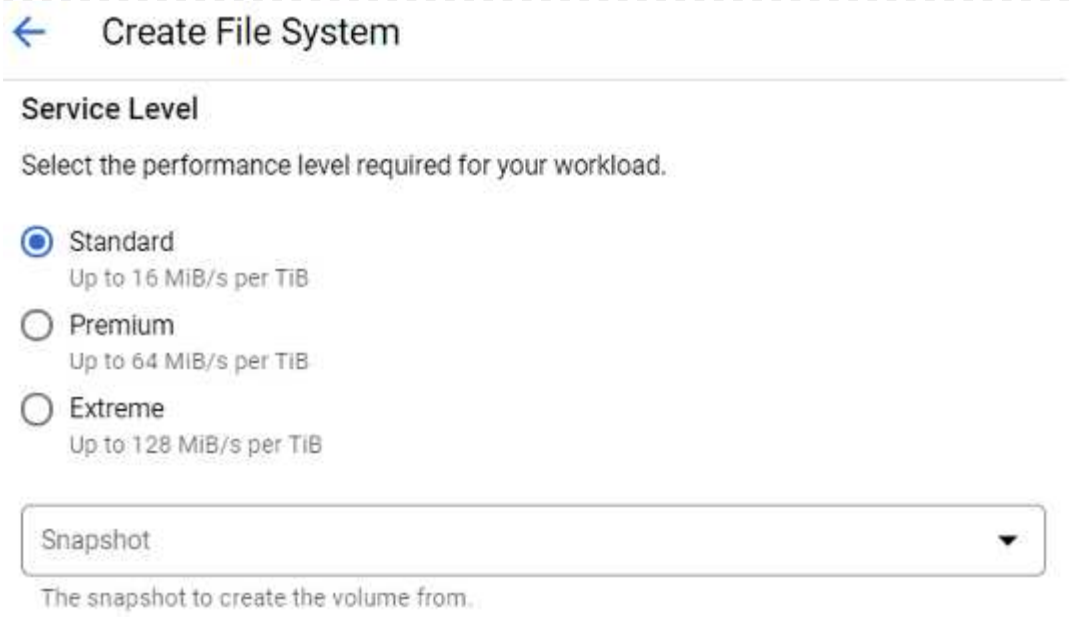
3. Sélectionnez le service approprié. Pour GCVE, choisissez CVS-Performance et le niveau de service souhaité pour une latence améliorée et des performances supérieures en fonction des exigences des charges de travail.



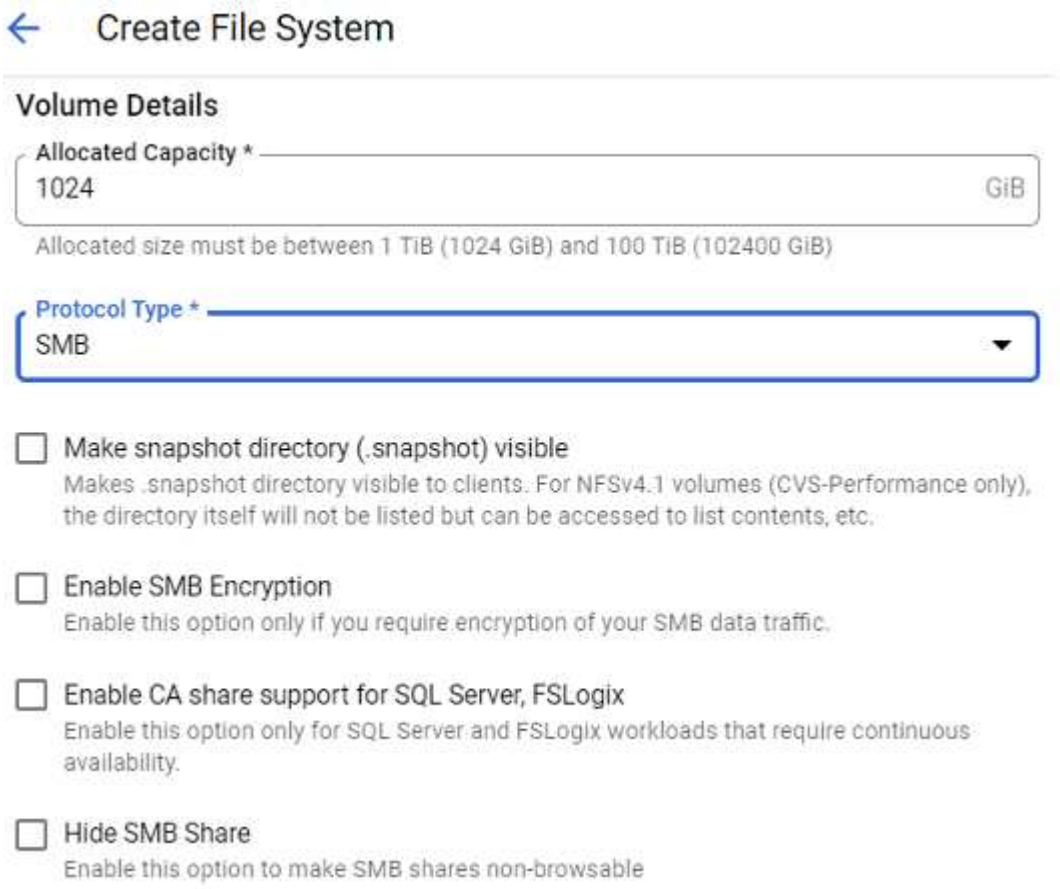
4. Spécifier la région Google Cloud pour le chemin de volume et de volume (le chemin du volume doit être unique sur l'ensemble des volumes cloud du projet)



5. Sélectionnez le niveau de performances du volume.



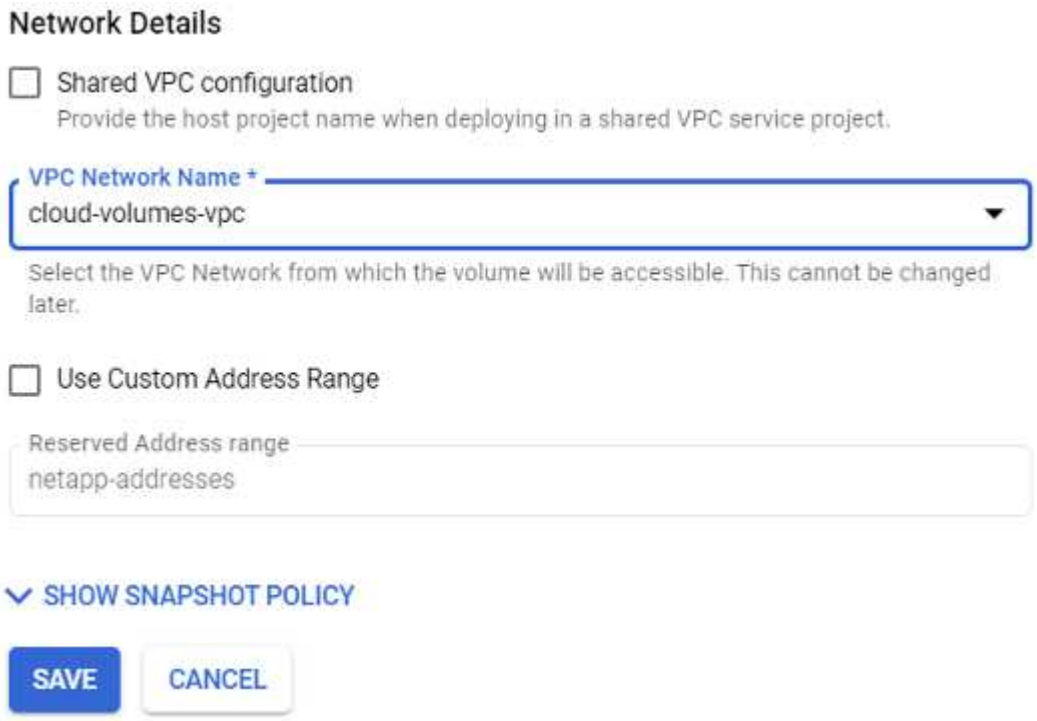
6. Spécifiez la taille du volume et le type de protocole. SMB est utilisé lors de ce test.



7. Au cours de cette étape, sélectionnez le réseau VPC à partir duquel le volume sera accessible. Assurez-vous que le peering VPC est en place.

   CONSEIL : si le peering VPC n'a pas été effectué, un bouton contextuel s'affiche pour vous guider à travers les commandes de peering. Ouvrez une session Cloud Shell et exécutez les commandes appropriées pour peer-to-peer votre VPC avec le producteur Cloud Volumes Service. Au cas où vous

décidiez de préparer le peering de VPC au préalable, reportez-vous à ces "instructions".



8. Cliquez sur Enregistrer pour créer le volume.

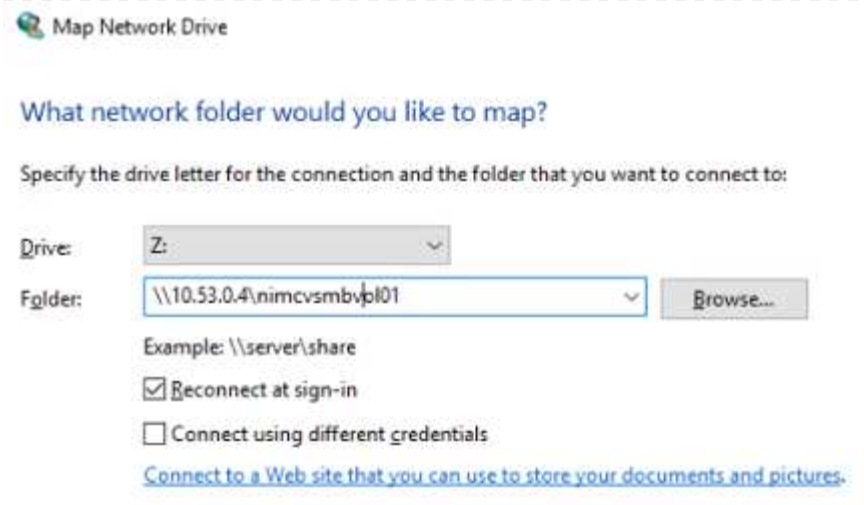
Pour monter le volume SMB, procédez comme suit :

1. Dans Cloud Console, accédez à Cloud volumes > volumes.
2. Accédez à la page volumes
3. Cliquez sur le volume SMB pour lequel vous souhaitez mapper un partage SMB.
4. Faites défiler vers la droite, sous Afficher plus, cliquez sur instructions de montage.

Pour effectuer le processus de montage à partir du système d'exploitation invité Windows de la machine virtuelle VMware, procédez comme suit :

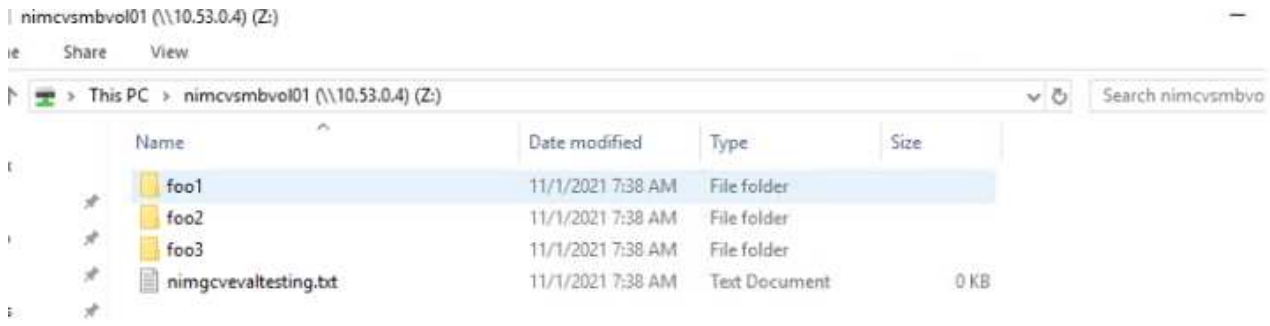
1. Cliquez sur le bouton Démarrer, puis sur ordinateur.
2. Cliquez sur carte lecteur réseau.
3. Dans la liste lecteur, cliquez sur n'importe quelle lettre de lecteur disponible.
4. Dans la zone dossier, saisissez :

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



Pour vous connecter chaque fois que vous vous connectez à votre ordinateur, cochez la case reconnecter à la connexion.

5. Cliquez sur Terminer.



Disponibilité des régions pour les datastores NFS supplémentaires sur AWS, Azure et GCP

En savoir plus sur la prise en charge par la région mondiale des datastores NFS supplémentaires sur AWS, Azure et Google Cloud Platform (GCP).

Disponibilité de la région AWS

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.

Disponibilité de la région Azure

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

- Vérifier la disponibilité de AVS et ANF "ici".
- Vérifier la disponibilité du datastore NFS supplémentaire ANF "ici".

Disponibilité d'une région GCP

La disponibilité de la région GCP sera disponible lors de l'entrée en fonction du public de GCP.

Synthèse et conclusion : pourquoi NetApp offre un multicloud hybride avec VMware

NetApp Cloud volumes et les solutions VMware pour les principaux hyperscalers offrent un grand potentiel aux entreprises qui cherchent à exploiter le cloud hybride. Le reste de cette section présente des cas d'utilisation permettant l'intégration de NetApp Cloud volumes offre de véritables fonctionnalités multicloud hybrides.

Cas d'utilisation n° 1 : optimisation du stockage

Lors d'un exercice de dimensionnement à l'aide des outils RVTools, il est toujours évident que l'évolutivité de la puissance (vCPU/vmem) est parallèle au stockage. Elles sont souvent nombreuses à se retrouver dans une situation où l'espace de stockage nécessaire permet de définir la taille du cluster bien au-delà de ce qui est nécessaire en puissance.

L'intégration de NetApp Cloud volumes permet aux entreprises de réaliser une solution cloud vSphere selon une approche de migration simple, sans changement de plateforme, ni modification de l'architecture. De plus, cette optimisation vous permet de faire évoluer l'empreinte du stockage tout en réduisant le nombre d'hôtes à un volume minimal dans vSphere, sans modification de la hiérarchie de stockage, de la sécurité ou des fichiers disponibles. Vous pouvez ainsi optimiser le déploiement et réduire le coût total de possession de 35 à 45 %. Cette intégration vous permet également de faire évoluer le stockage depuis le stockage chaud jusqu'au niveau de production en quelques secondes.

Cas d'utilisation n°2 : migration vers le cloud

Les entreprises subissent une pression considérable pour migrer les applications depuis les data centers sur site vers le cloud public pour de nombreuses raisons : une expiration de bail imminente, une directive financière pour passer des dépenses d'investissement aux dépenses d'exploitation (OpEx) ou simplement un mandat descendante pour déplacer l'ensemble du cloud.

Lorsque la vitesse est essentielle, seule une approche de migration rationalisée est possible, car le changement de plateforme et le remaniement d'applications pour l'adapter à la plateforme IaaS spécifique au cloud sont lents et onéreux, et prennent souvent des mois. En associant NetApp Cloud volumes à la réplication SnapMirror économe en bande passante pour les systèmes de stockage connectés à l'invité (dont RDM avec des copies Snapshot cohérentes au niveau des applications et HCX, par exemple, pour la migration

vers le cloud Azure Migrate) ou produits tiers pour la réplication des machines virtuelles), cette transition est encore plus simple que s'appuyant sur des mécanismes de filtres d'E/S chronophages.

Cas d'utilisation n°3 : extension du data Center

Lorsqu'un data Center atteint ses limites de capacité en raison de pics de demande saisonniers ou simplement d'une croissance organique soutenue, il est facile de migrer vers le cloud VMware avec NetApp Cloud volumes. En exploitant NetApp Cloud volumes, vous pouvez créer, répliquer et étendre votre stockage très facilement en assurant une haute disponibilité sur les zones de disponibilité et des fonctionnalités d'évolutivité dynamique. En exploitant NetApp Cloud volumes, vous pouvez minimiser la capacité des clusters hôtes en surpassant la nécessité de clusters étendus.

Cas d'utilisation n°4 : reprise après incident dans le cloud

Dans une approche classique, en cas d'incident, les machines virtuelles répliquées dans le cloud nécessitent une conversion vers la propre plateforme d'hyperviseur du cloud avant qu'elles ne puissent être restaurées, pas une tâche à traiter en cas de crise.

L'utilisation de NetApp Cloud volumes pour le stockage connecté à l'invité via la réplication SnapCenter et SnapMirror depuis des systèmes sur site ainsi que des solutions de virtualisation de cloud public améliore la reprise d'activité. De cette manière, les réplicas de VM peuvent être récupérés sur une infrastructure VMware SDDC entièrement cohérente, ainsi que sur des outils de restauration spécifiques au cloud (par exemple Azure site Recovery) ou des outils tiers équivalents tels que Veeam. Ainsi, vous pouvez réaliser rapidement des tests de reprise après incident et des opérations de reprise après incident en cas d'attaque par ransomware. Cela vous permet également d'évoluer vers une production complète à des fins de test ou lors d'un incident en ajoutant des hôtes à la demande.

Cas d'utilisation n°5 : modernisation des applications

Une fois que les applications sont dans le cloud public, les entreprises voudront exploiter des centaines de services cloud puissants pour les moderniser et les étendre. Avec NetApp Cloud volumes, la modernisation est un processus simple, car les données applicatives ne sont pas verrouillées dans VSAN et permet la mobilité des données pour un large éventail d'utilisations, y compris Kubernetes.

Conclusion

Que vous cibliez un cloud hybride ou 100 % cloud, NetApp Cloud volumes offre une excellente option pour déployer et gérer les charges de travail applicatives avec les services de fichiers et les protocoles de bloc, tout en réduisant le coût total de possession grâce à une intégration transparente des données à la couche applicative.

Quelles que soient les utilisations, vous pouvez choisir votre cloud/hyperscaler favori et NetApp Cloud volumes 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 workloads, et de la capacité et des performances élevées.

Il s'agit du même processus et procédures que ceux utilisés pour connecter le stockage. N'oubliez pas que la position des données a changé de nom. Les outils et les processus restent identiques, et NetApp Cloud volumes contribue à optimiser le déploiement global.

Cas d'utilisation du cloud hybride VMware

Présentation des cas d’utilisation importants pour les ÉQUIPES IT lors de la planification de déploiements de cloud hybride ou premier cloud.

Cas d’utilisation populaires

Cas d’utilisation :

- Reprise sur incident,
- Hébergement de charges de travail pendant la maintenance du data Center, * rafale rapide dans laquelle des ressources supplémentaires sont requises au-delà de ce qui est provisionné dans le data Center local,
- L’extension de site VMware,
- Migration rapide vers le cloud,
- Développement/test et
- La modernisation des applications en tirant parti de technologies complémentaires du cloud.

Dans cette documentation, les références aux charges de travail cloud seront détaillées dans les cas d’utilisation de VMware. Ces utilisations sont les suivantes :

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

Inside ® le parcours DE L’IT

La plupart des entreprises sont en voie de transformation et de modernisation. Dans le cadre de ce processus, les entreprises tentent d’utiliser leurs investissements VMware existants, tout en tirant parti des avantages du cloud et en explorant les façons de rendre le processus de migration aussi transparent que possible. Cette approche facilite grandement la tâche de modernisation, car les données sont déjà dans le cloud.

La réponse la plus simple à ce scénario est d’utiliser des offres VMware pour chaque hyperscaler. Comme NetApp® Cloud volumes, VMware offre un moyen de déplacer ou d’étendre les environnements VMware sur site vers n’importe quel cloud. Vous pouvez ainsi conserver vos ressources, compétences et outils sur site existants tout en exécutant les charges de travail de façon native dans le cloud. Les risques sont réduits, car aucun service n’est disponible ni modifié IP. De plus, l’équipe INFORMATIQUE est en mesure de gérer ses pratiques sur site à l’aide des compétences et des outils existants. Cela permet d’accélérer les migrations vers le cloud et de faciliter la transition vers une architecture multicloud hybride.

Comprendre l’importance d’autres options de stockage NFS

Même si VMware quel que soit le cloud offre des fonctionnalités hybrides uniques à chaque client, les options de stockage NFS supplémentaires limitées ne sont pas utiles pour les entreprises qui traite de charges de travail très exigeantes en termes de stockage. Comme le stockage est directement lié aux hôtes, le seul moyen de faire évoluer le stockage consiste à ajouter d’autres hôtes, ce qui représente une augmentation des coûts de 35 à 40 % ou plus pour les charges de travail consommatrices de stockage. Ces charges de travail ont simplement besoin d’espace de stockage supplémentaire et ne sont pas de puissance supplémentaire. Mais cela signifie que les hôtes supplémentaires sont payants.

Examinons ce scénario :

Un client ne requiert que cinq hôtes pour le processeur et la mémoire, mais ses besoins en stockage sont nombreux et doit disposer de 12 hôtes pour répondre aux besoins en stockage. En fin de compte, il est indispensable de faire évoluer l'infrastructure financière en achetant de la puissance supplémentaire si nécessaire.

Lorsque vous planifiez l'adoption et les migrations du Cloud, il est toujours important d'évaluer la meilleure approche et de prendre le chemin le plus simple qui réduit les investissements totaux. L'approche la plus courante et la plus simple pour toute migration d'applications est le réhébergement (aussi appelé lift and shift) où il n'existe pas de machine virtuelle (VM) ou de conversion des données. L'utilisation de NetApp Cloud volumes avec le Software-Defined Data Center VMware (SDDC), tout en complétant VSAN, offre une option facile à déplacer.

Solutions NetApp pour Amazon VMware Managed Cloud (VMC)

En savoir plus sur les solutions NetApp pour AWS.

VMware définit les workloads cloud en trois catégories :

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

Parcourez les solutions disponibles dans les sections suivantes.

Protéger

- "Reprise après incident avec VMC sur AWS (connecté à l'invité)"
- "Sauvegarde Veeam ; Restauration dans VMC avec FSX for ONTAP"
- "Reprise après sinistre (DRO) avec FSX pour ONTAP et VMC"
- "Utilisation de Veeam Replication et FSX for ONTAP pour la reprise d'activité vers VMware Cloud on AWS"

Migrer

- "Migrez vos charges de travail vers le datastore FSxN à l'aide de VMware HCX"

Extension

DISPONIBLE PROCHAINEMENT !

Solutions NetApp pour Azure VMware solution (AVS)

En savoir plus sur les solutions NetApp pour Azure.

VMware définit les workloads cloud en trois catégories :

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

Parcourez les solutions disponibles dans les sections suivantes.

Protéger

- "Reprise après incident avec ANF et JetStream (datastore NFS supplémentaire)"
- "Reprise après incident avec ANF et CVO (stockage connecté à l'invité)"
- "Reprise d'activité (DRO) avec ANF et AVS"
- "Utilisation de la réplication Veeam et du datastore Azure NetApp Files pour la reprise après incident vers la solution Azure VMware"

Migrer

- "Migrez les charges de travail vers le datastore Azure NetApp Files avec VMware HCX"

Extension

DISPONIBLE PROCHAINEMENT !

Solutions NetApp pour Google Cloud VMware Engine (GCVE)

En savoir plus sur les solutions NetApp pour GCP.

VMware définit les workloads cloud en trois catégories :

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

Parcourez les solutions disponibles dans les sections suivantes.

Protéger

- "Reprise après incident des applications avec SnapCenter, Cloud Volumes ONTAP et Veeam Replication"
- "Reprise d'activité cohérente avec les applications avec NetApp SnapCenter et réplication Veeam vers NetApp CVS sur GCVE"

Migrer

- "Migration de la charge de travail à l'aide de VMware HCX vers le datastore NFS NetApp Cloud Volume Service"
- "Réplication de machine virtuelle à l'aide de Veeam vers le datastore NFS du service Cloud Volume NetApp"

Extension

DISPONIBLE PROCHAINEMENT !

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

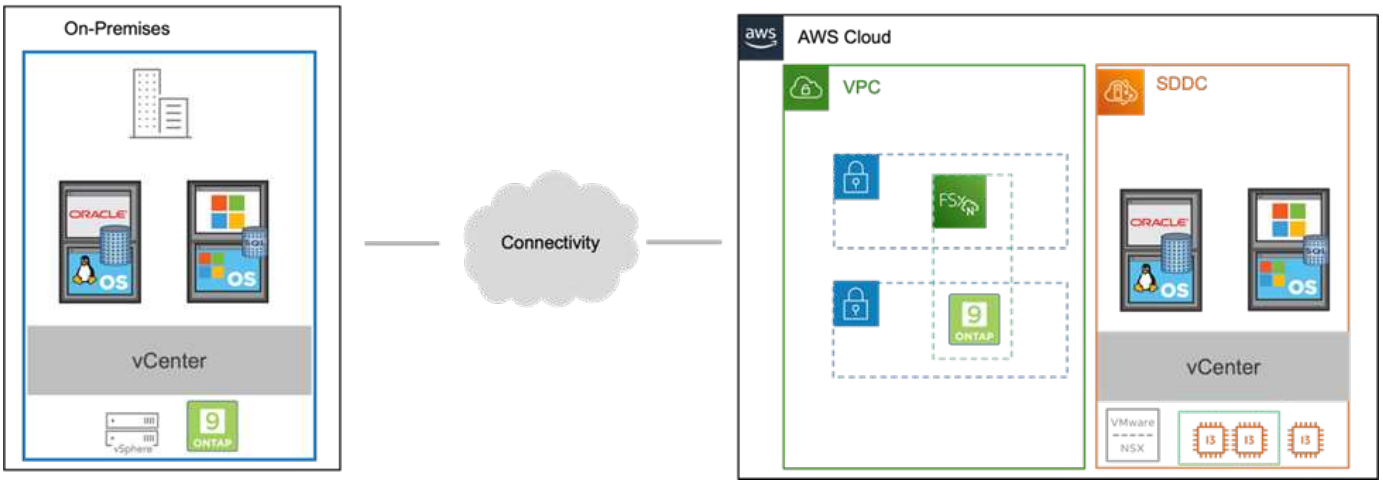
Auteurs : Chris Reno, Josh Powell, Suresh Thoppay - Ingénierie de solutions NetApp

Présentation

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.

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.

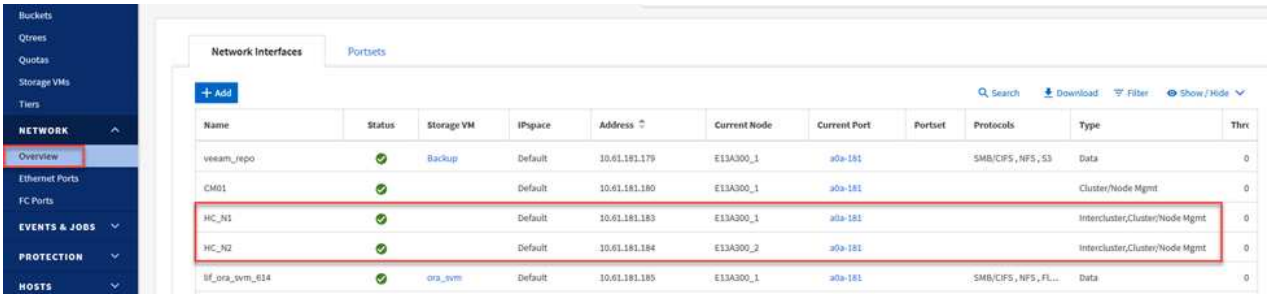
Les étapes suivantes sont requises pour la configuration des relations SnapMirror entre un système ONTAP sur site et FSX ONTAP :

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.
```

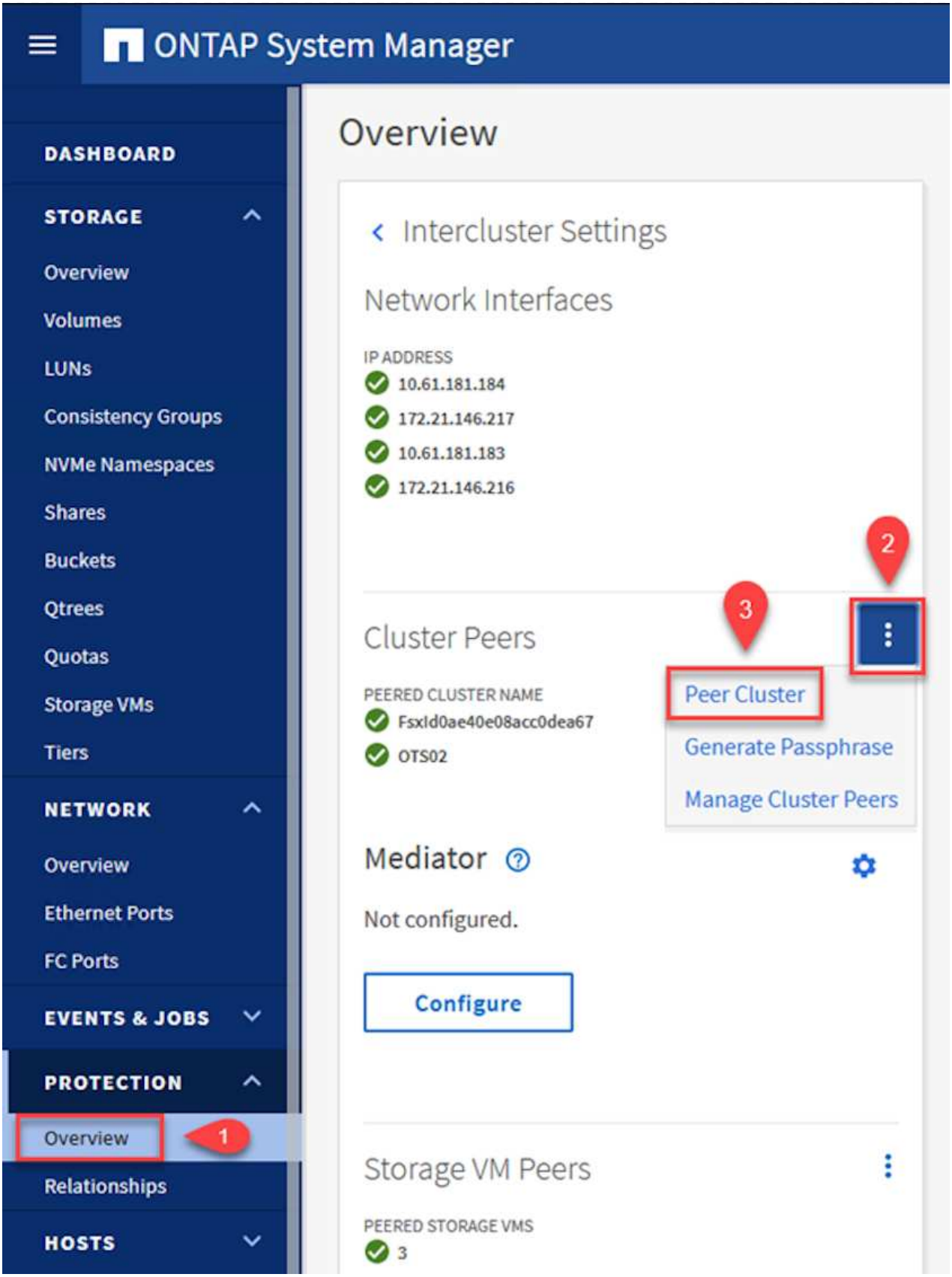
Établir le peering de cluster entre ONTAP et FSX

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.

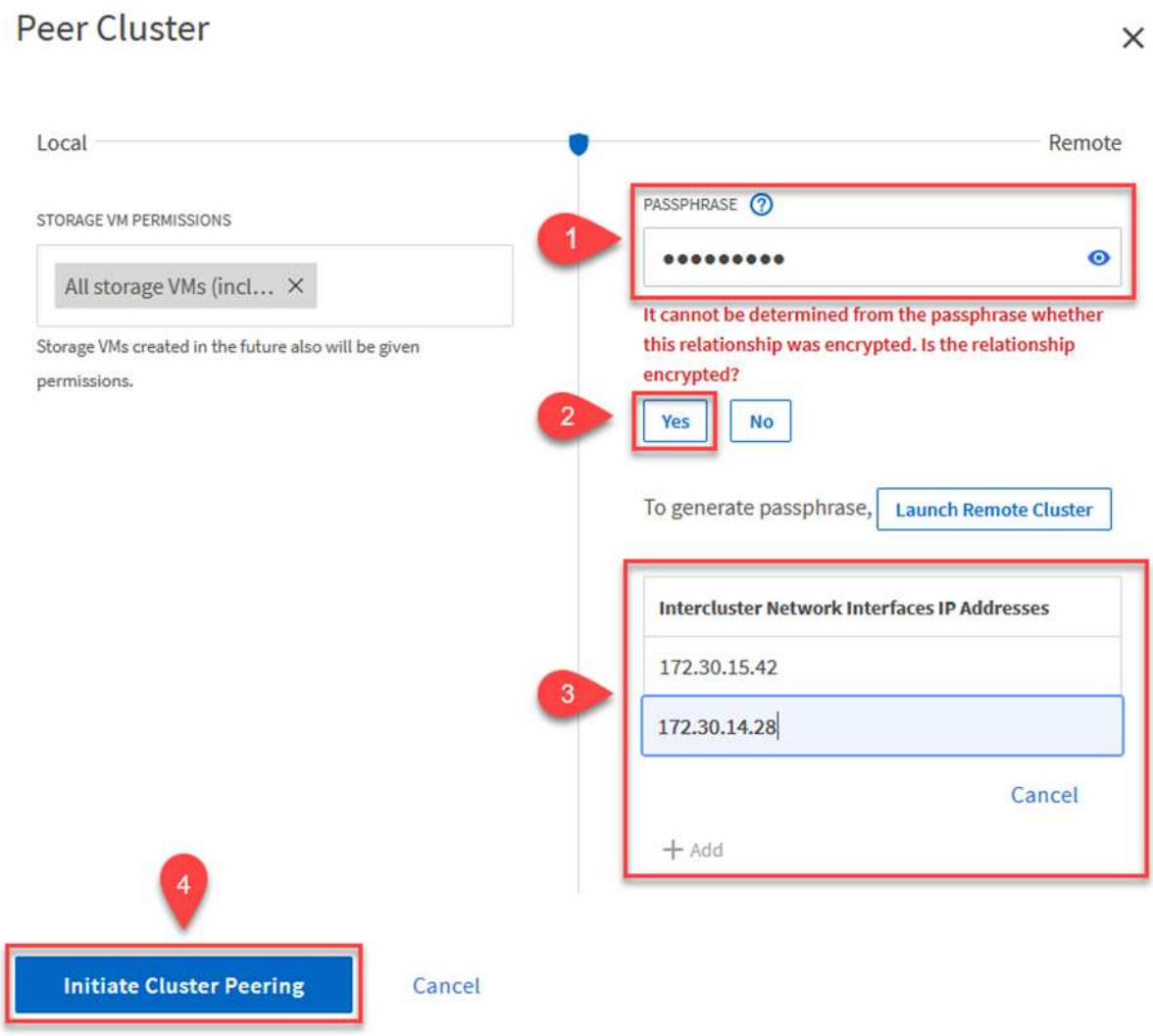


3. Dans la boîte de dialogue Peer Cluster, saisissez les informations requises :
   a. Saisissez la phrase de passe utilisée pour établir la relation de cluster homologue sur le cluster FSX de destination.

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
```

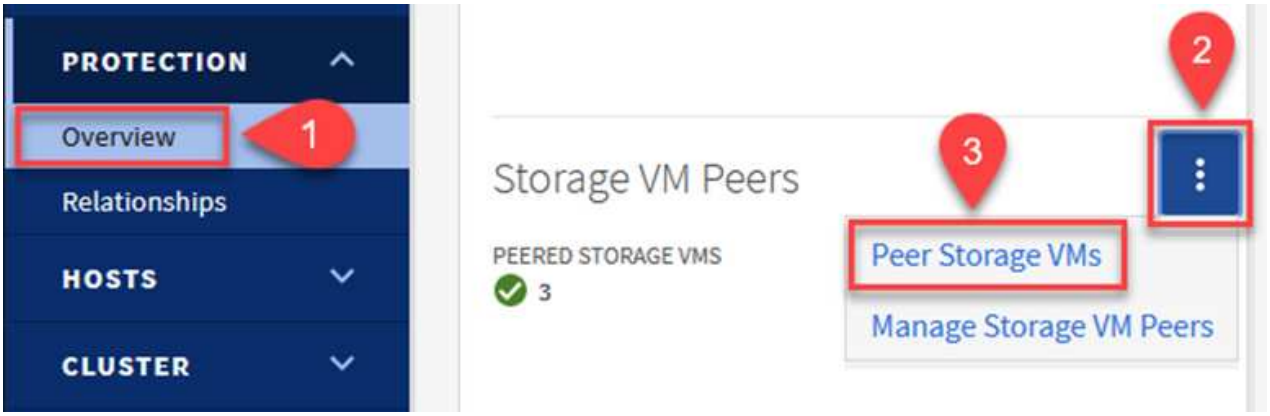
Établir une relation de peering de SVM

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.

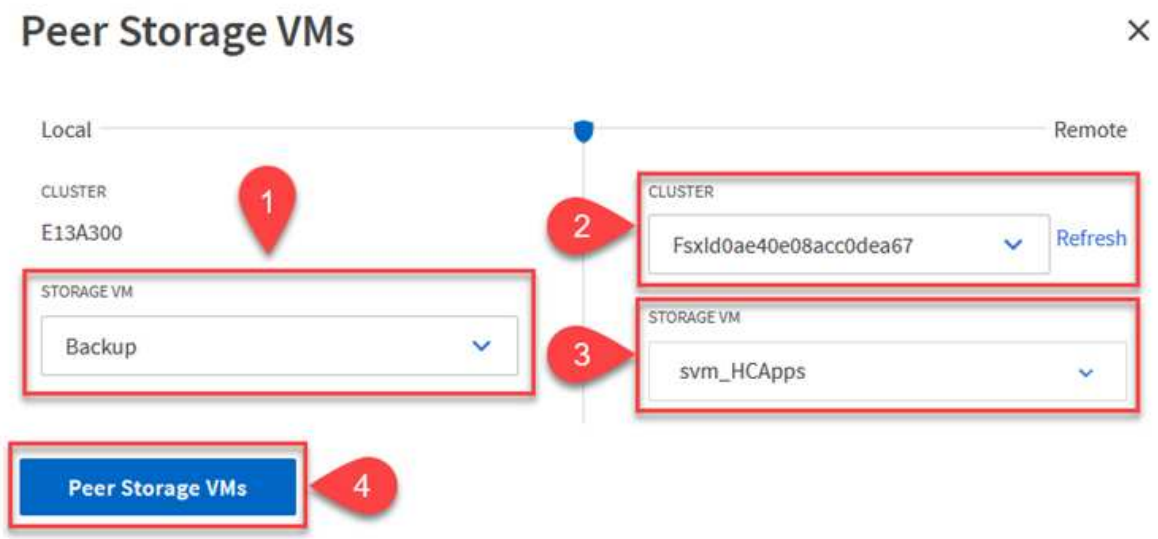
1. Depuis le cluster FSX source, utiliser la commande suivante depuis l'interface de ligne de commande afin de créer la relation SVM peer :

```
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.

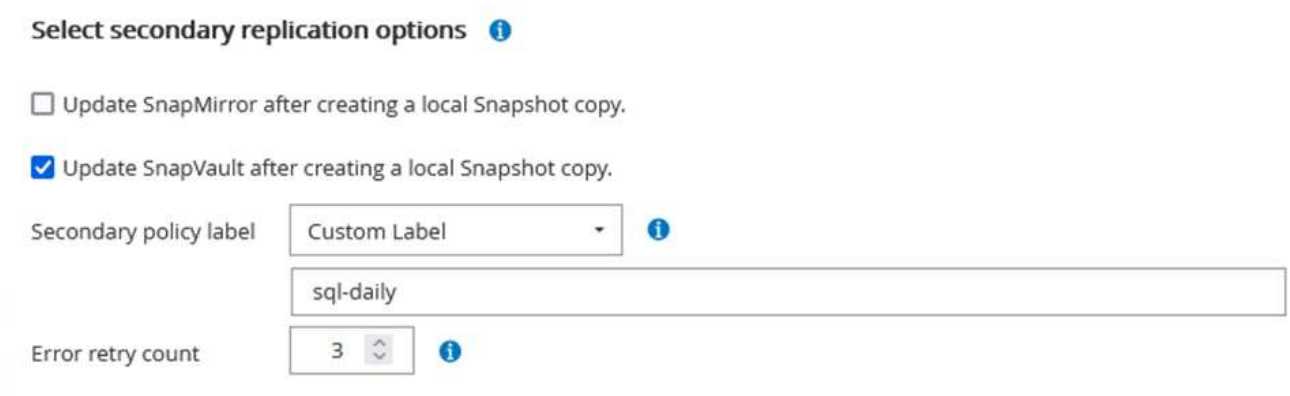
Création d'une règle de conservation des snapshots

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".

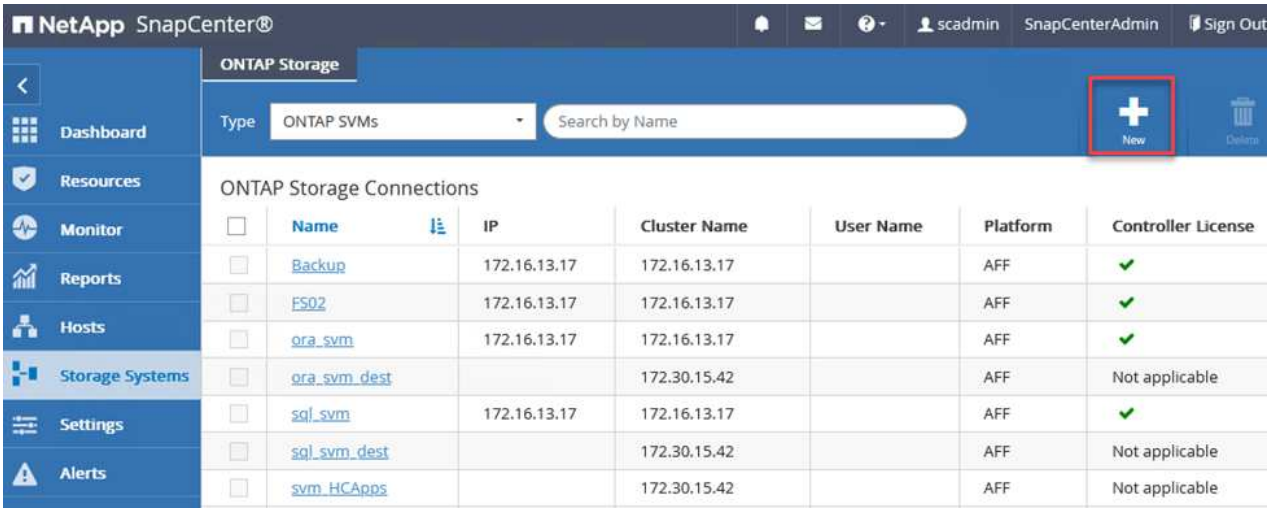
Une fois installé, vous pouvez accéder à la console SnapCenter à partir d'un navigateur Web en utilisant *https://Virtual_Cluster_IP_or_FQDN:8146*.

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

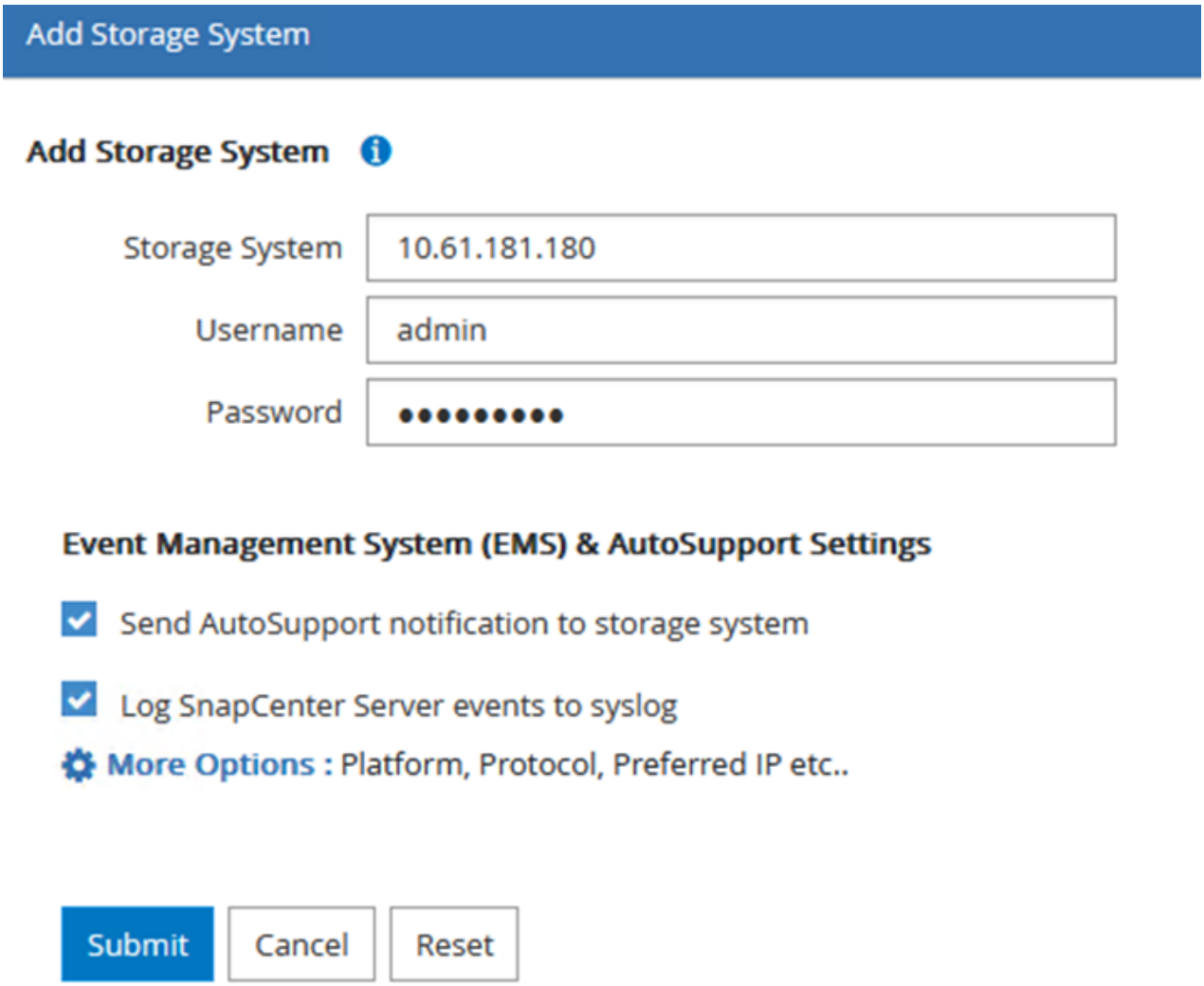
Ajout de contrôleurs de stockage à SnapCenter

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

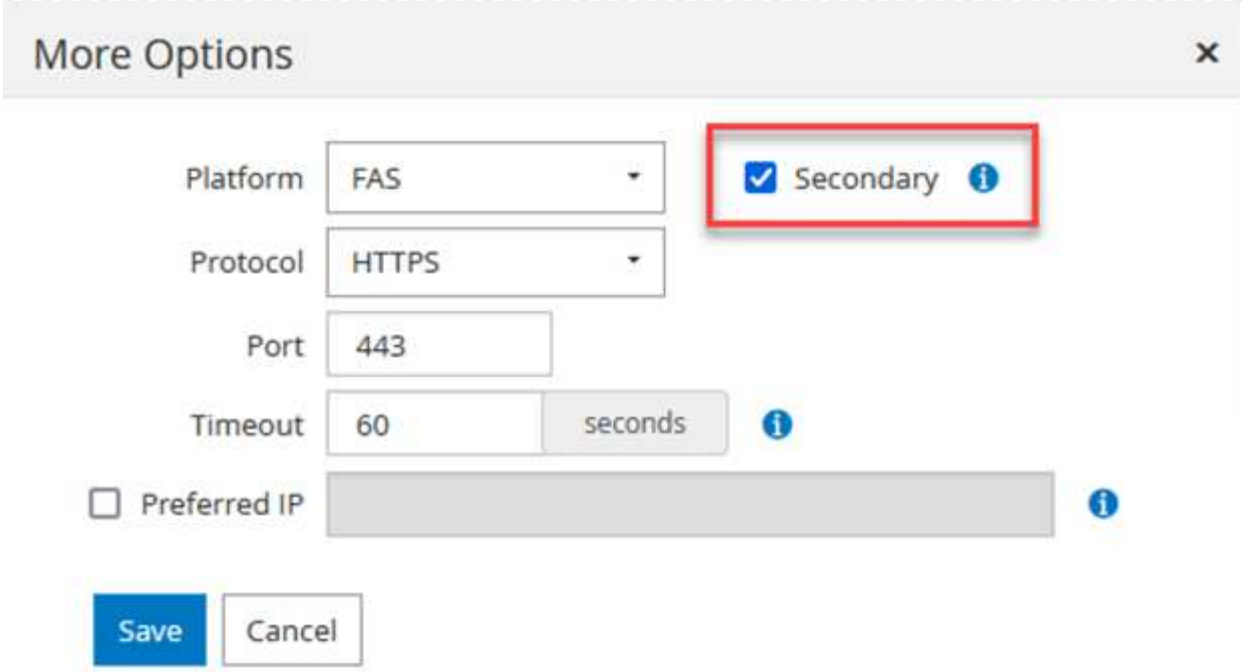
1. Dans le menu de gauche, sélectionnez systèmes de stockage, puis cliquez sur Nouveau pour lancer le processus d'ajout de vos contrôleurs de stockage à SnapCenter.



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.

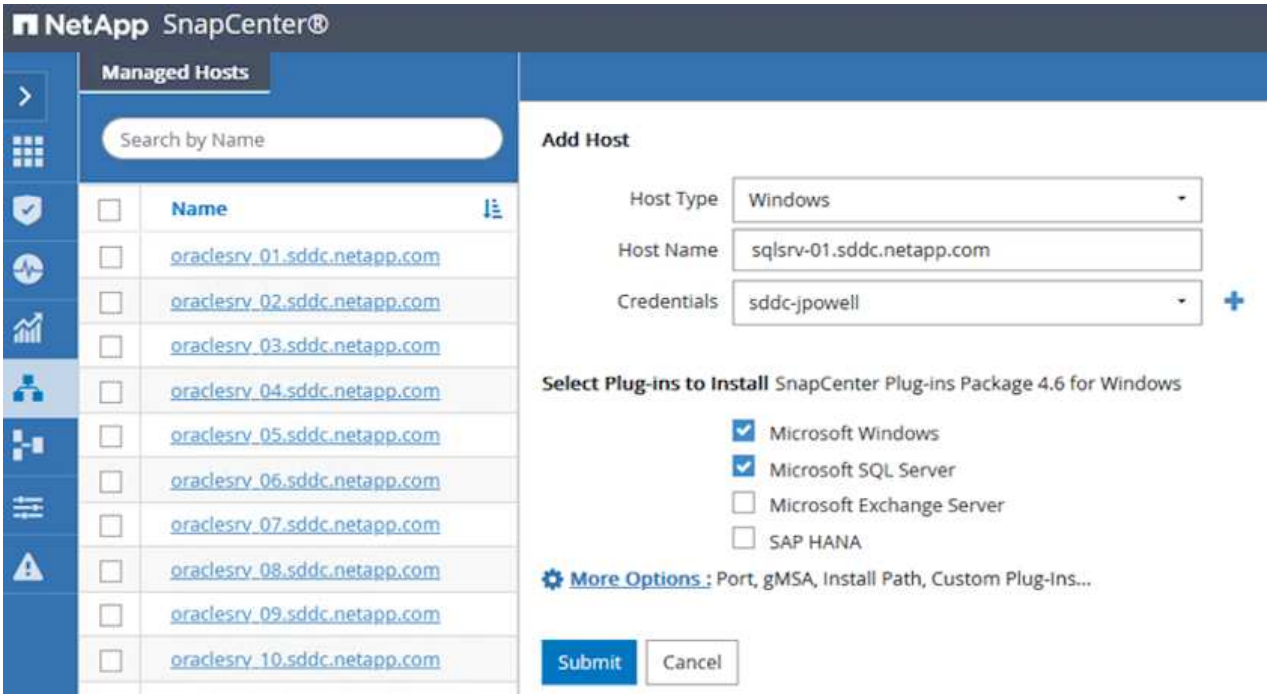


Pour plus d'informations sur l'ajout de systèmes de stockage à SnapCenter, reportez-vous à la documentation à l'adresse "ce lien".

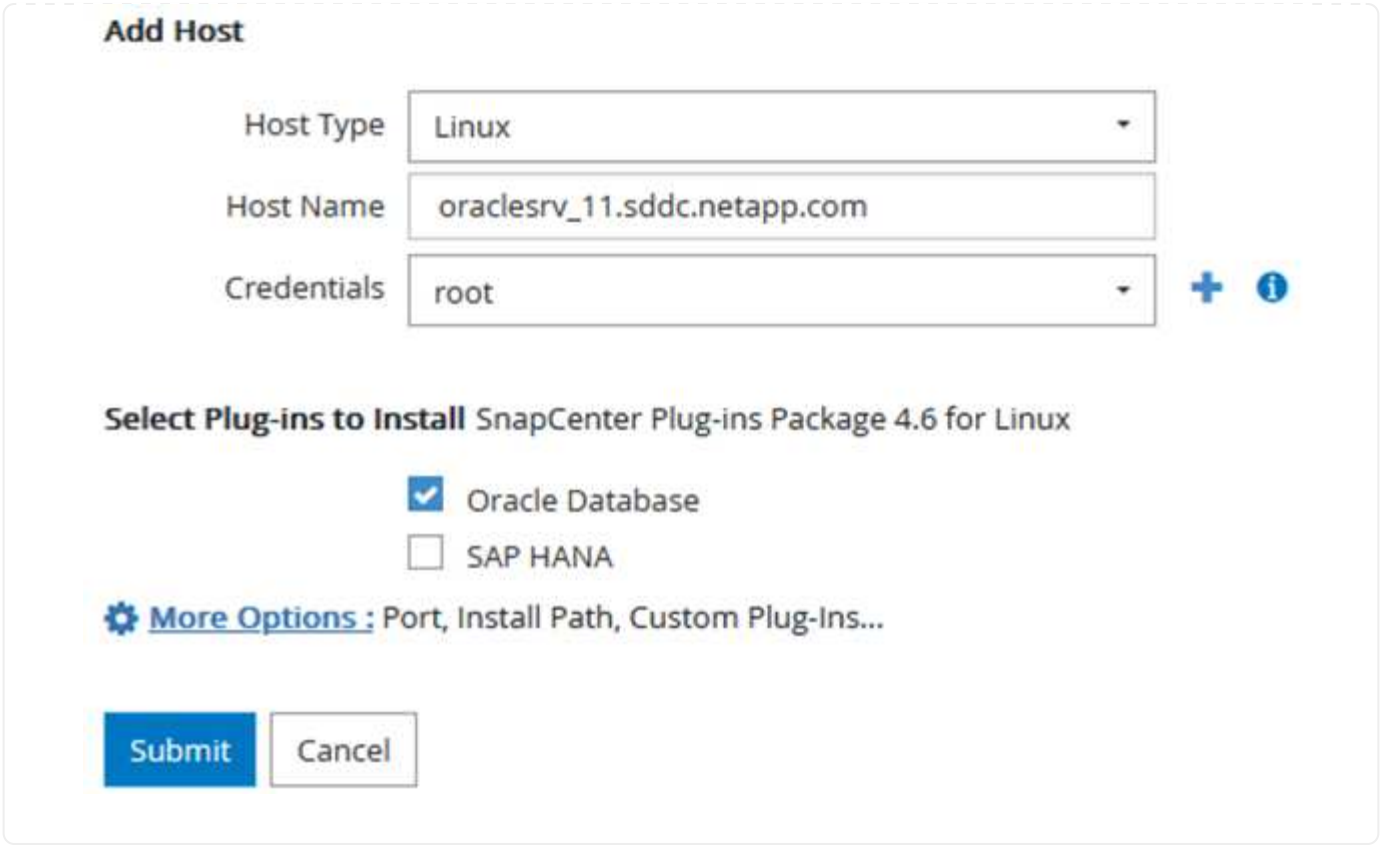
Ajouter des hôtes à SnapCenter

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.



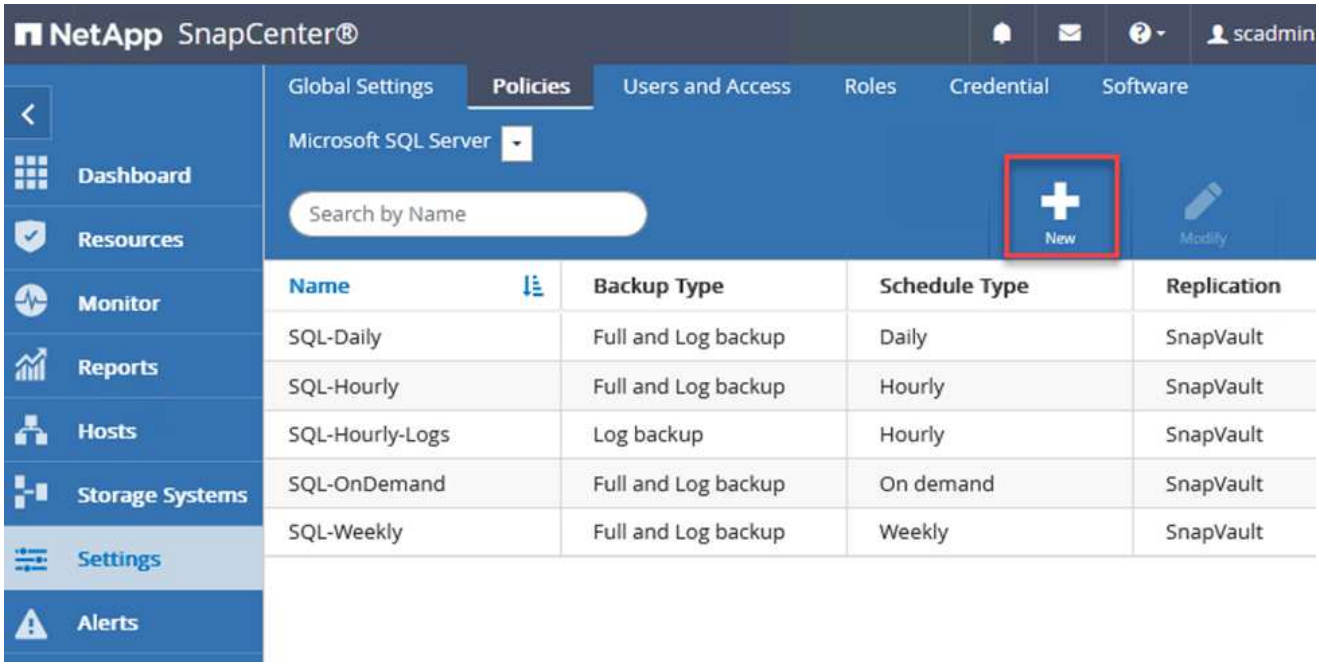
3. Pour Oracle, renseignez les champs requis dans la boîte de dialogue Ajouter un hôte et cochez la case du plug-in Oracle Database. Cliquez ensuite sur Envoyer pour lancer le processus de détection et ajouter l'hôte à SnapCenter.


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.



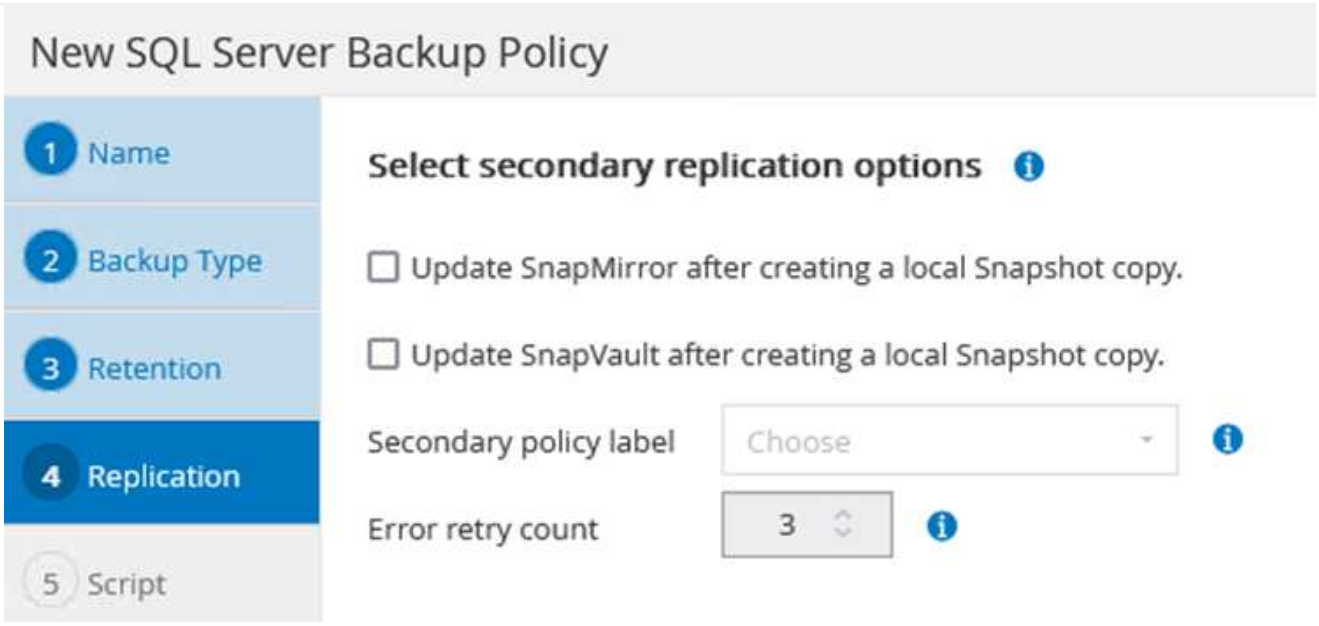
Pour obtenir des informations complètes sur la création de stratégies pour les sauvegardes SQL Server, reportez-vous à la section "Documentation SnapCenter".

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.

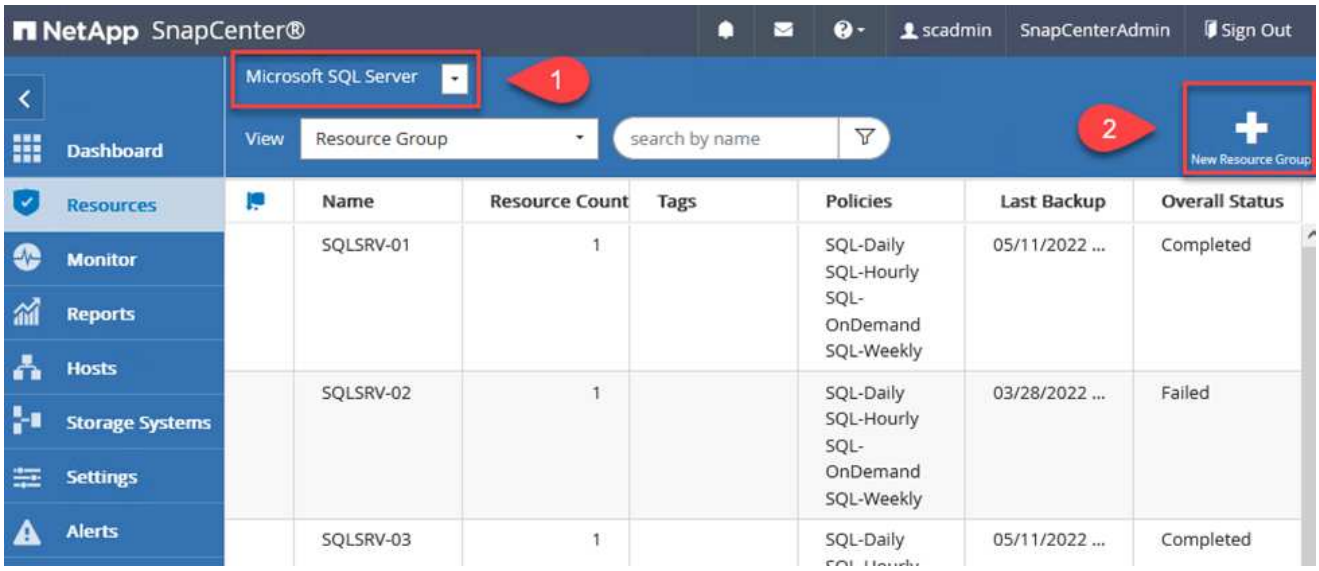
L'image suivante montre les options ci-dessus et leur apparence dans l'assistant de stratégie de sauvegarde.



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.

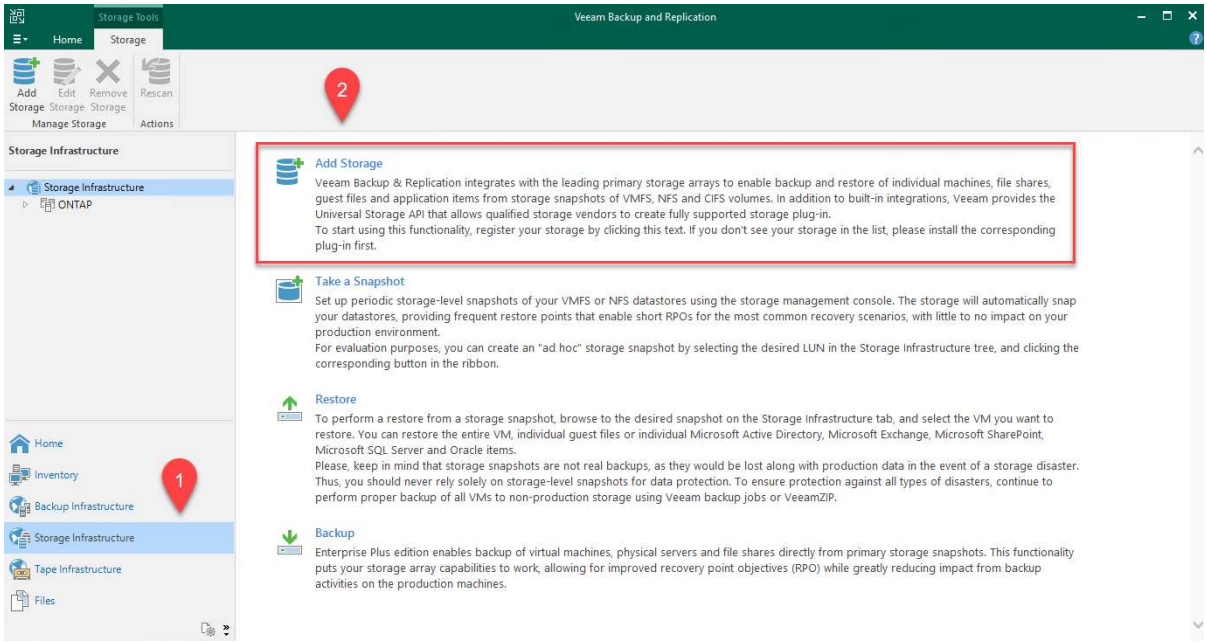
Consultez les conditions préalables suivantes avant de commencer.

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.

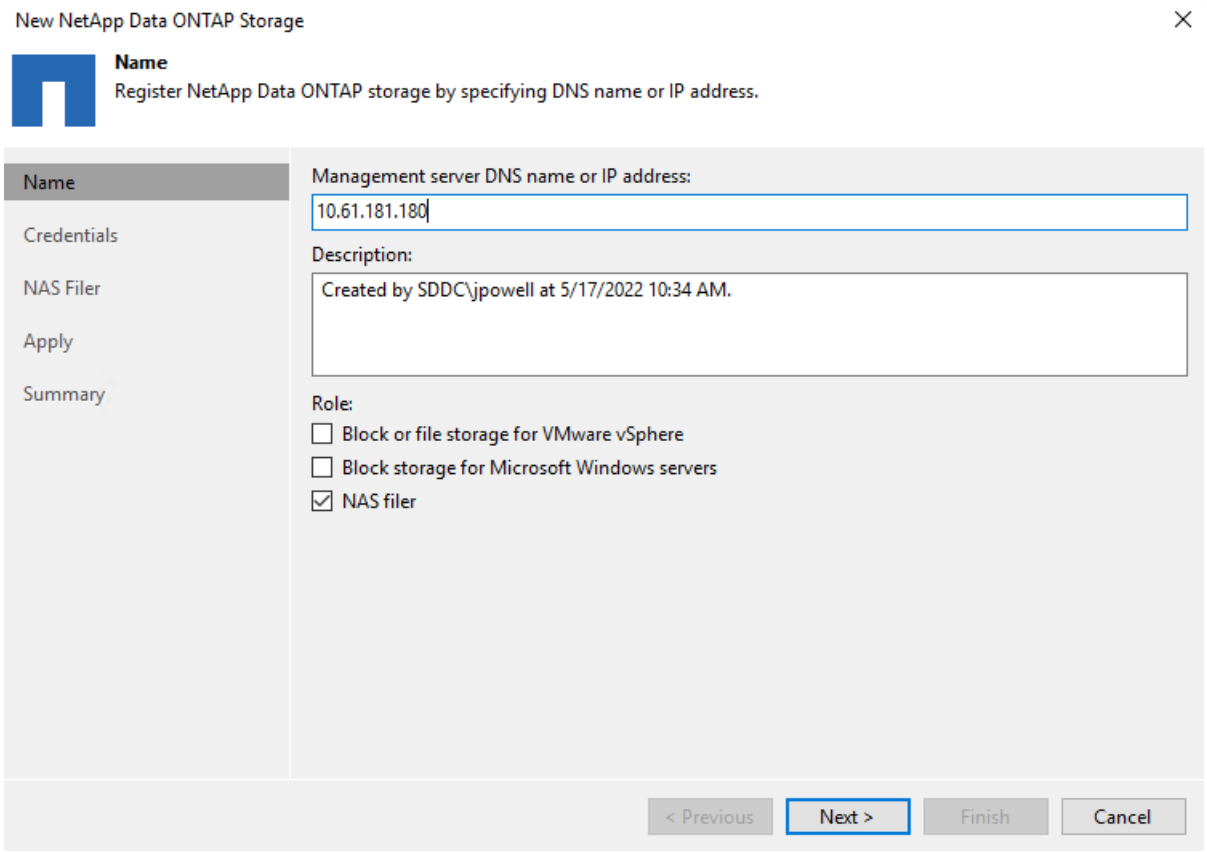
Ajout du stockage ONTAP à Veeam

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.

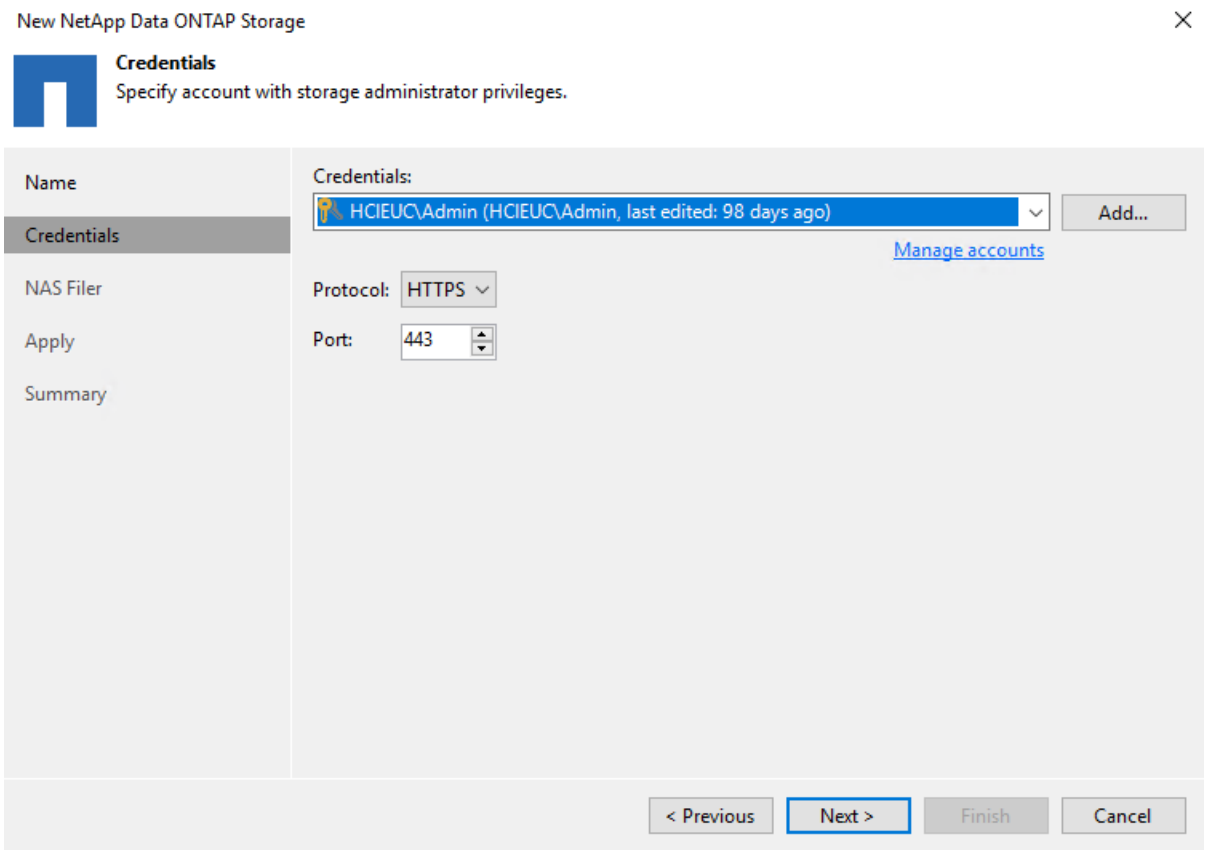
1. Ouvrez la console Veeam et connectez-vous. Accédez à Storage Infrastructure, puis sélectionnez Add Storage.



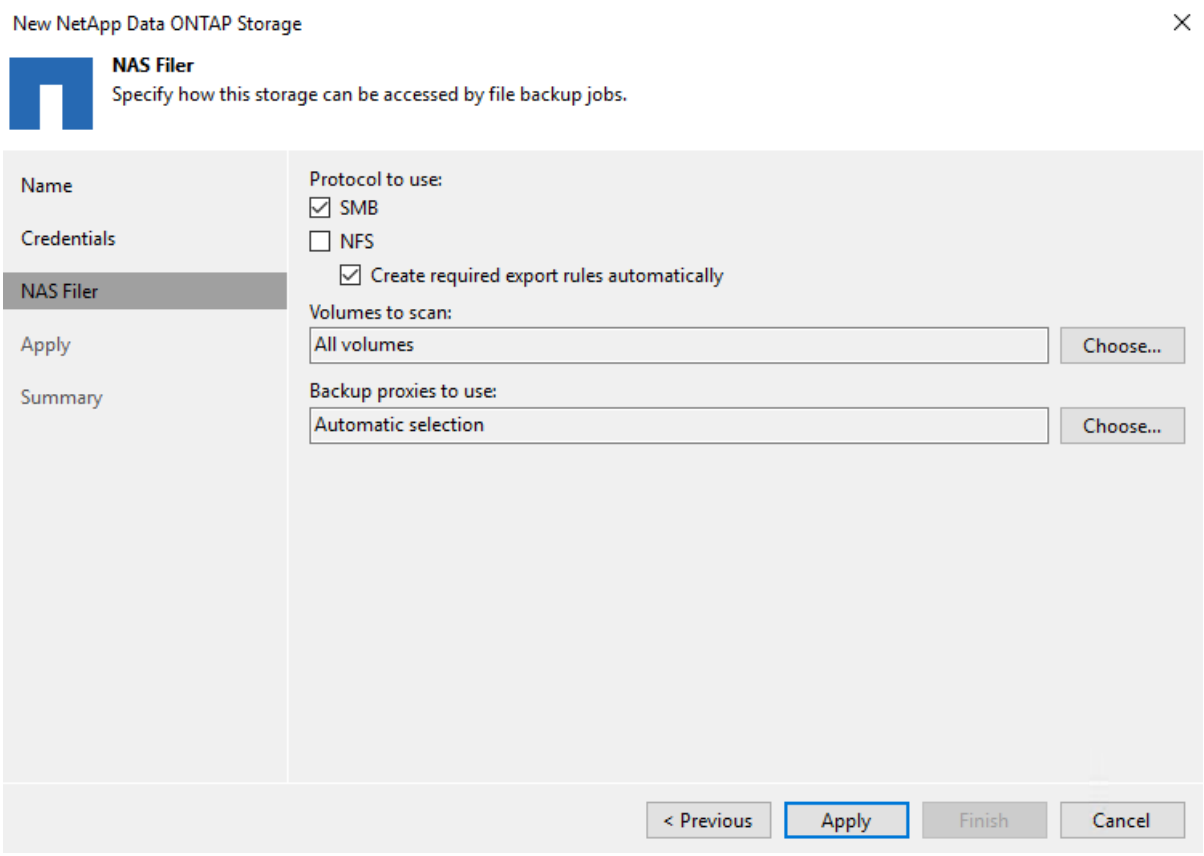
2. Dans l'assistant d'ajout de stockage, sélectionnez NetApp comme fournisseur de stockage, puis sélectionnez Data ONTAP.
3. Entrez l'adresse IP de gestion et cochez la case filer NAS. Cliquez sur Suivant.



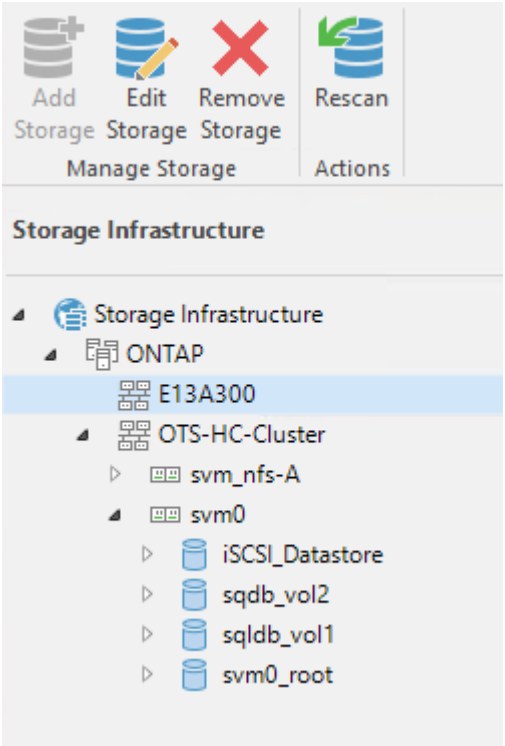
4. Ajoutez vos identifiants pour accéder au cluster ONTAP.



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

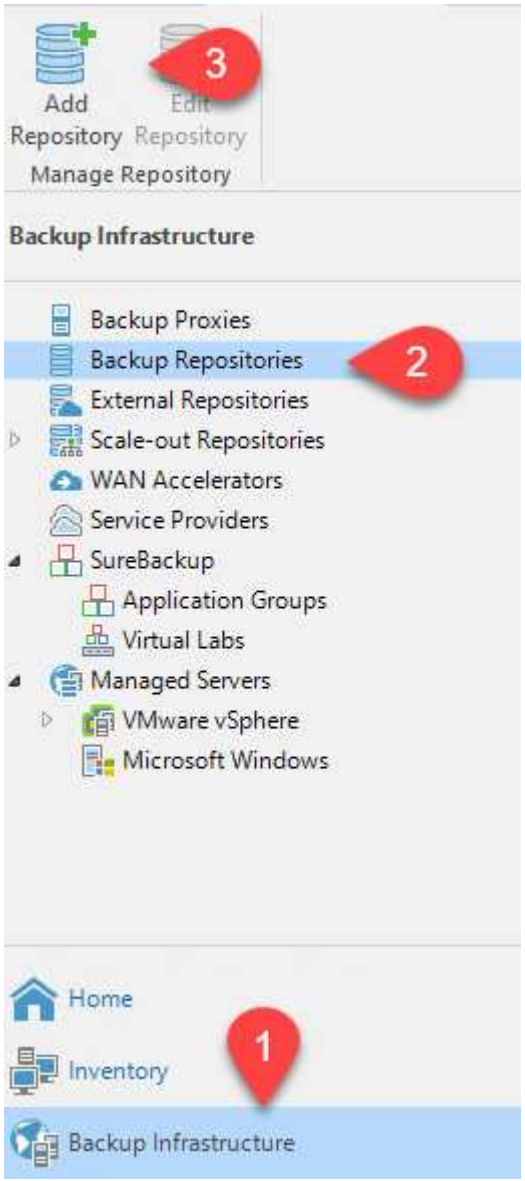


6. Complétez les pages appliquer et Résumé de l'assistant et cliquez sur Terminer pour lancer le processus de détection du stockage. Une fois le scan terminé, on ajoute le cluster ONTAP ainsi que les filers NAS en tant que ressources disponibles.

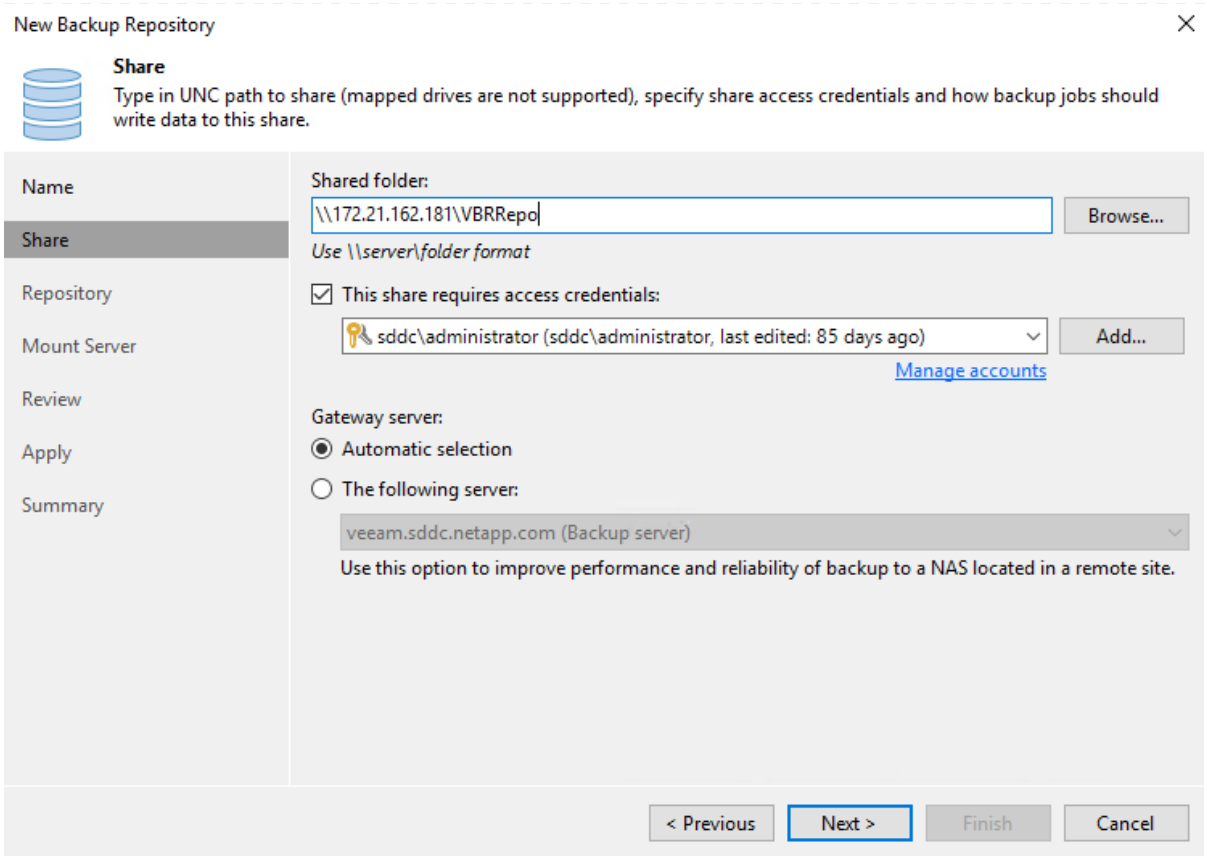


7. Créez un référentiel de sauvegarde à l'aide des partages NAS récemment découverts. Dans Backup Infrastructure, sélectionnez Sauvegarder les référentiels et cliquez sur l'élément de

menu Ajouter un référentiel.



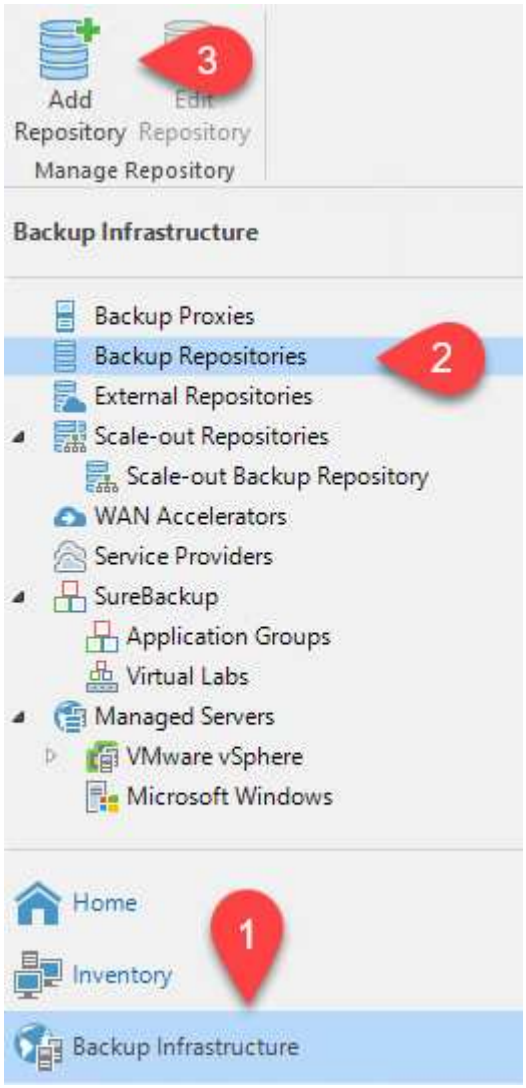
8. Suivez toutes les étapes de l'Assistant Nouveau référentiel de sauvegarde pour créer le référentiel. Pour plus d'informations sur la création des référentiels de sauvegarde Veeam, consultez le "Documentation Veeam".


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

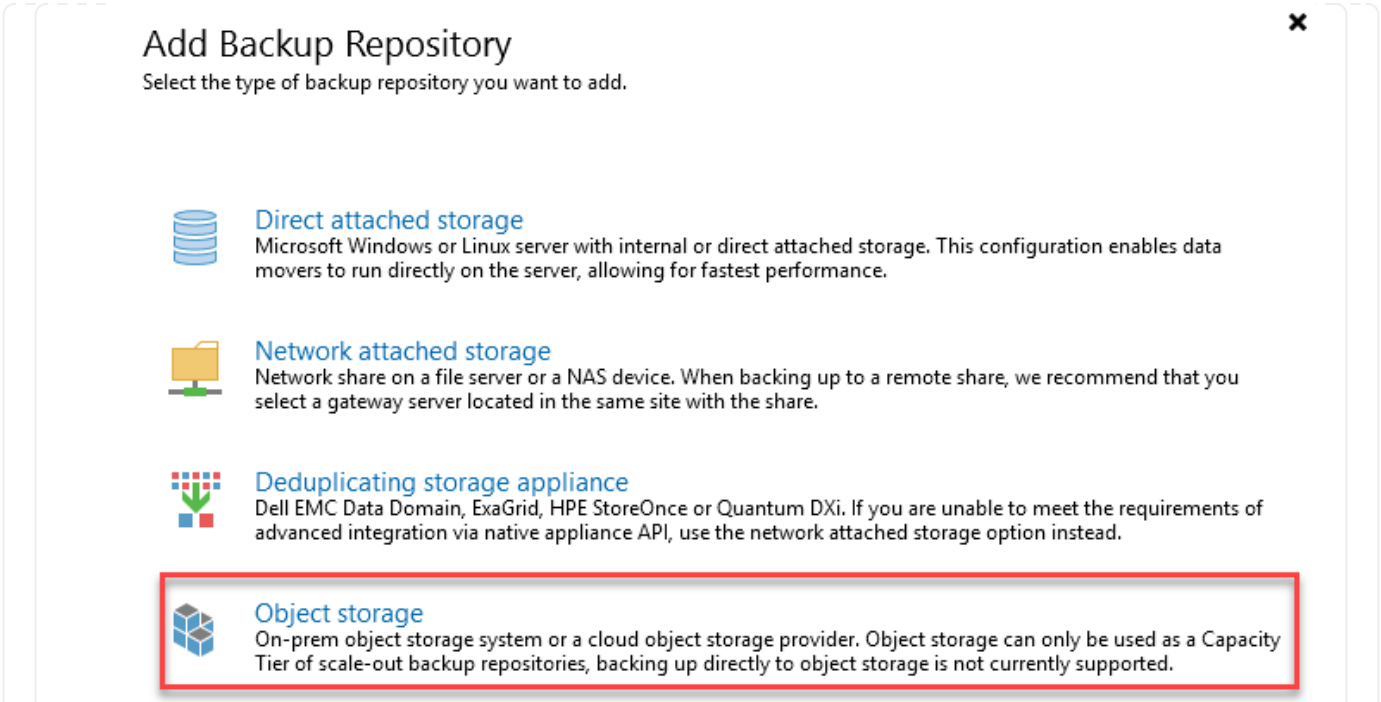
Ajoutez le compartiment Amazon S3 en tant que référentiel de sauvegarde

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

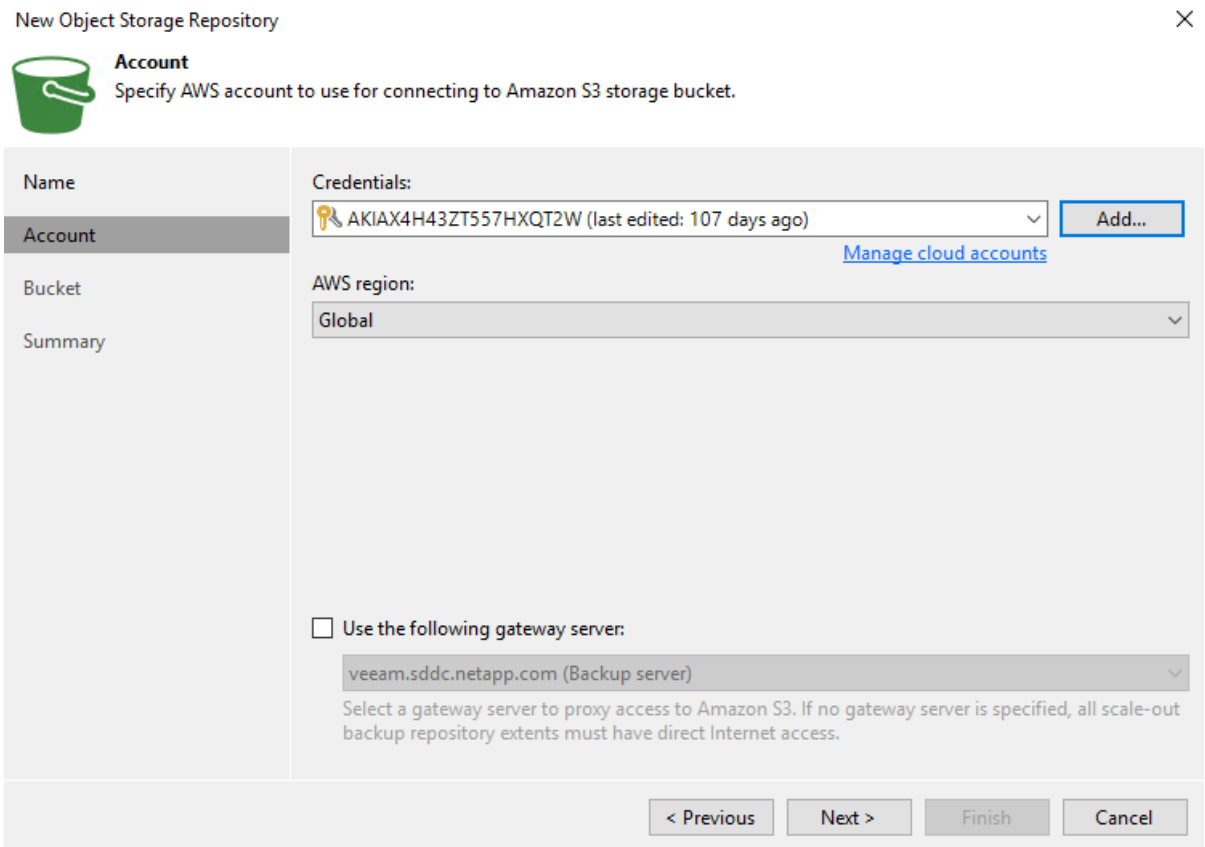
1. Accédez à Backup Infrastructure > référentiels de sauvegarde. Cliquez sur Ajouter un référentiel.



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.

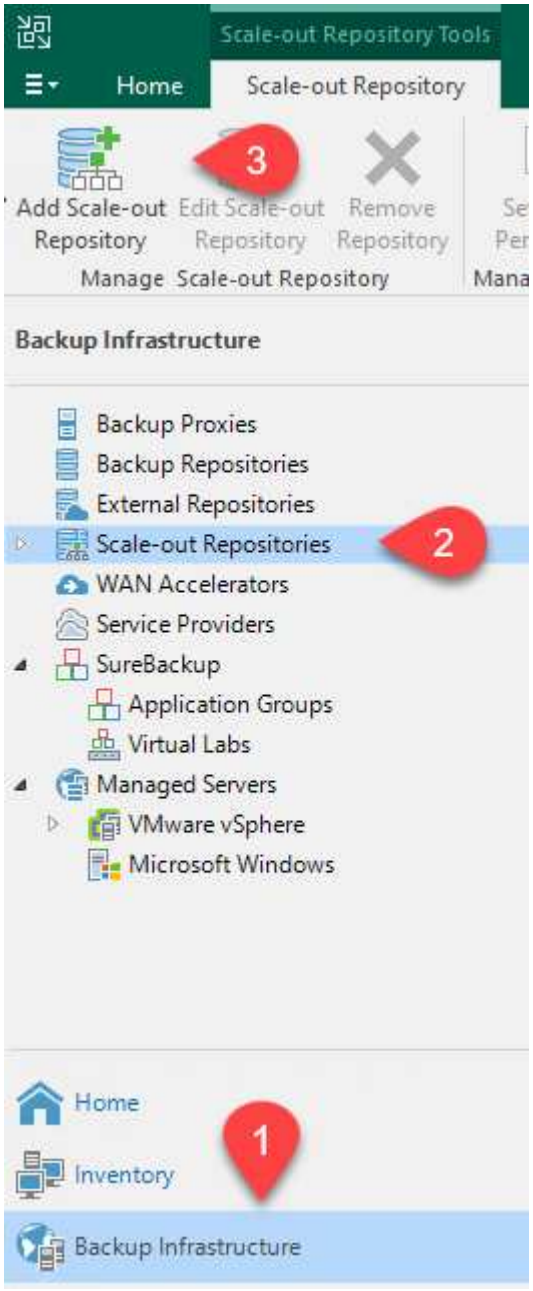


5. Une fois la configuration Amazon chargée, choisissez votre data Center, votre compartiment et votre dossier, puis cliquez sur « Apply » (appliquer). Enfin, cliquez sur Terminer pour fermer l'assistant.

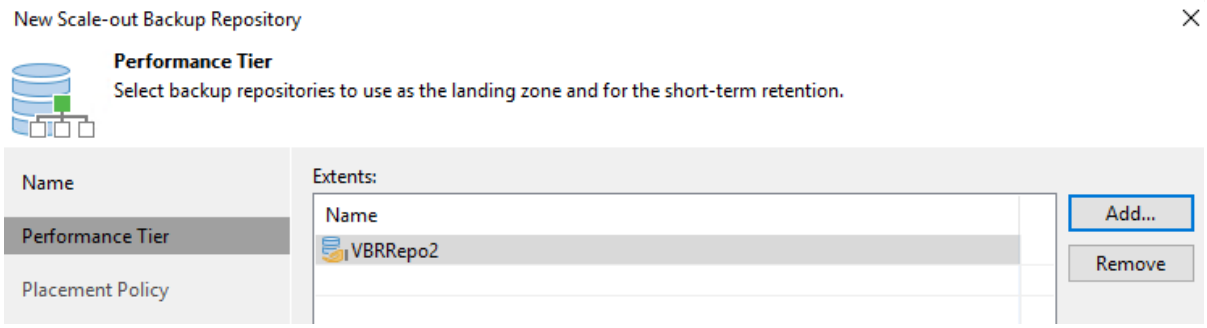
Création d'un référentiel de sauvegarde scale-out

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.

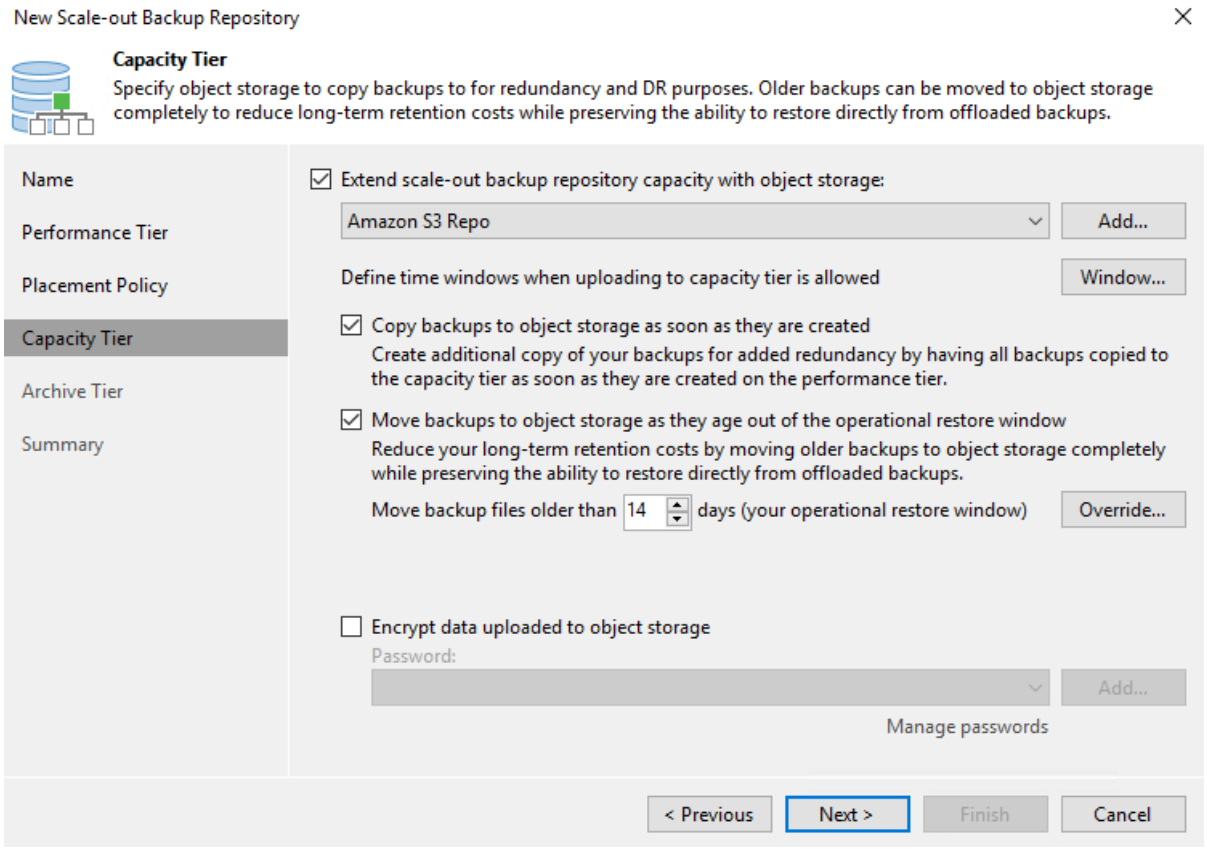
1. Dans l'infrastructure de sauvegarde, sélectionnez référentiels scale-out, puis cliquez sur l'élément de menu Ajouter un référentiel scale-out.



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.

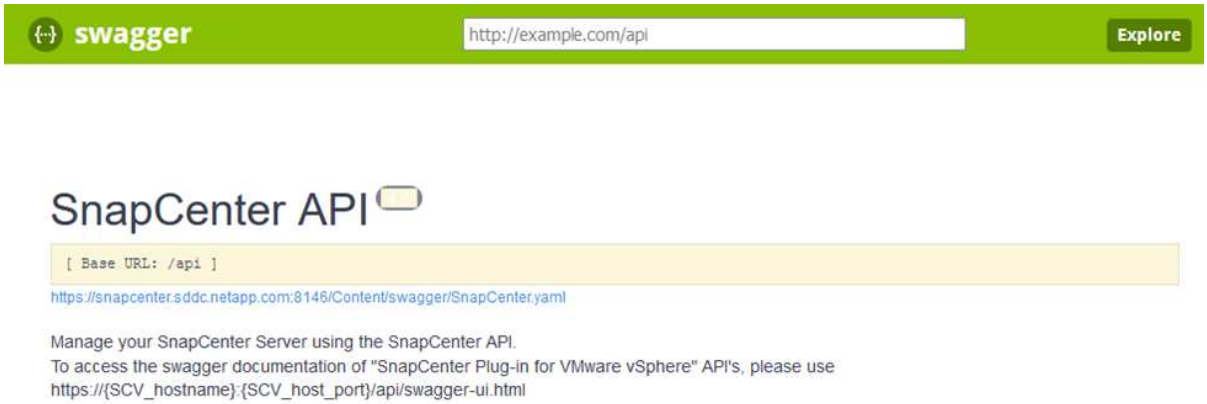
Sauvegarder la base de données et la configuration de SnapCenter

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".

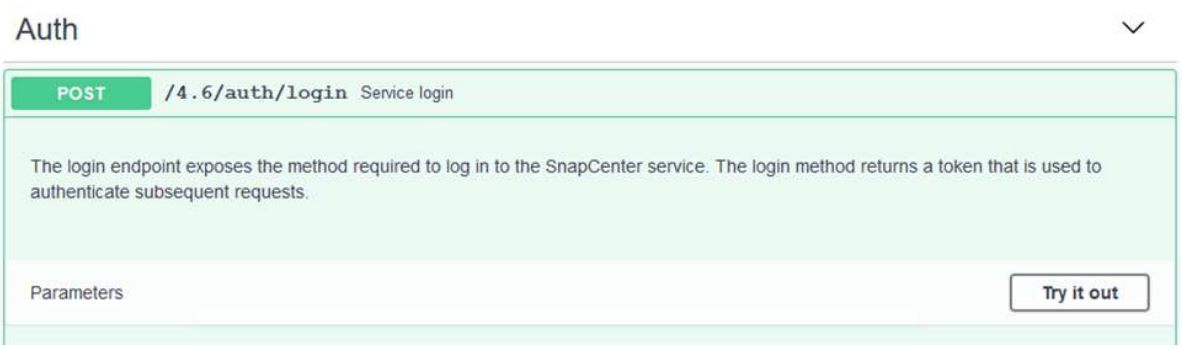
Connectez-vous à swagger et obtenez le jeton d'autorisation

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.

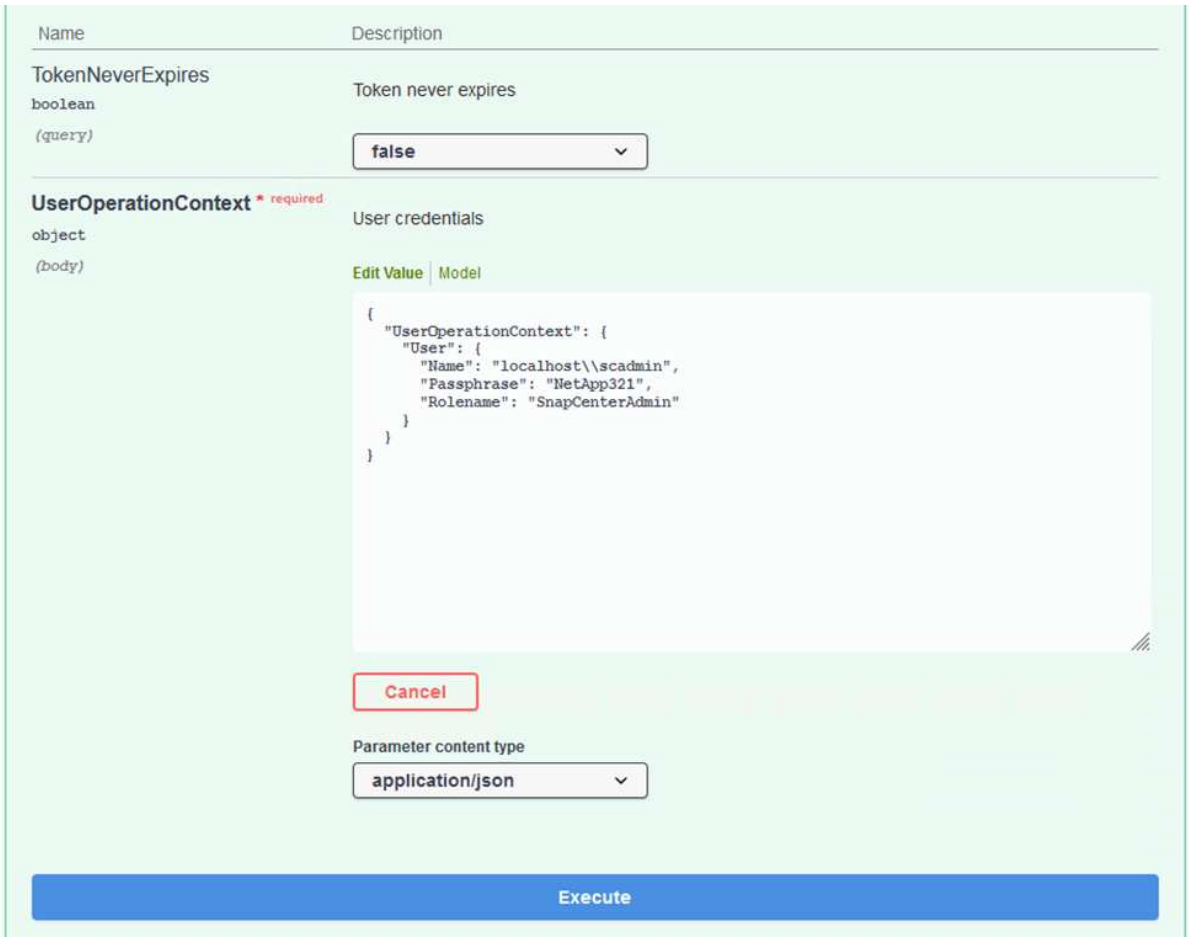
1. Accédez à la page Web de l'API SnapCenter swagger à l'adresse *https://<SnapCenter Server IP>:8146/swagger/*.



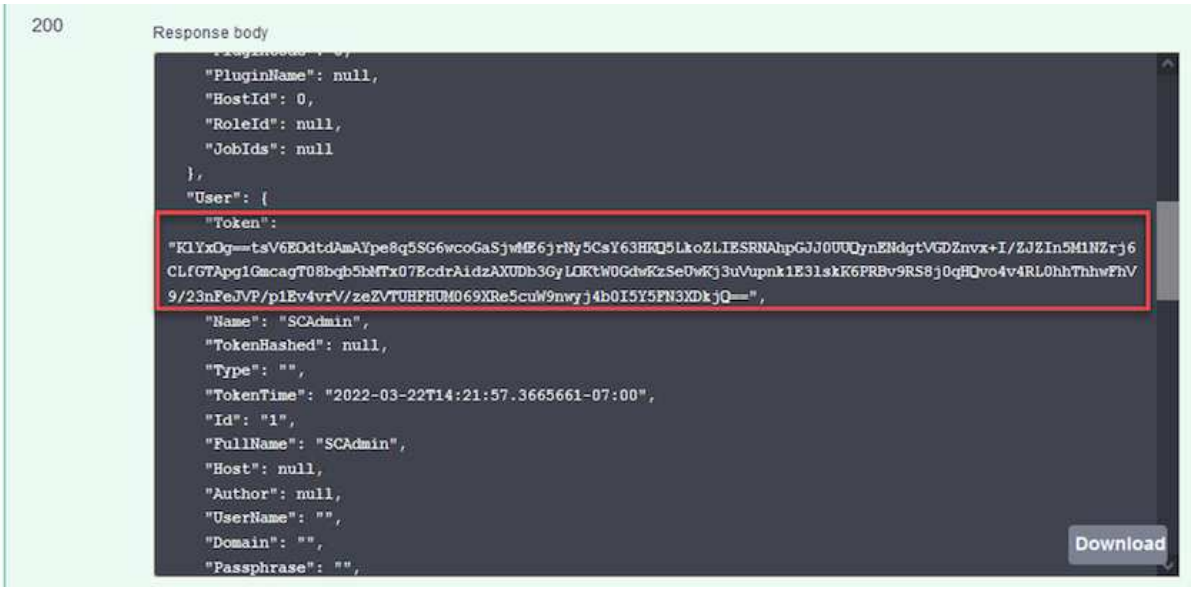
2. Développez la section Auth et cliquez sur le bouton essayer.



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



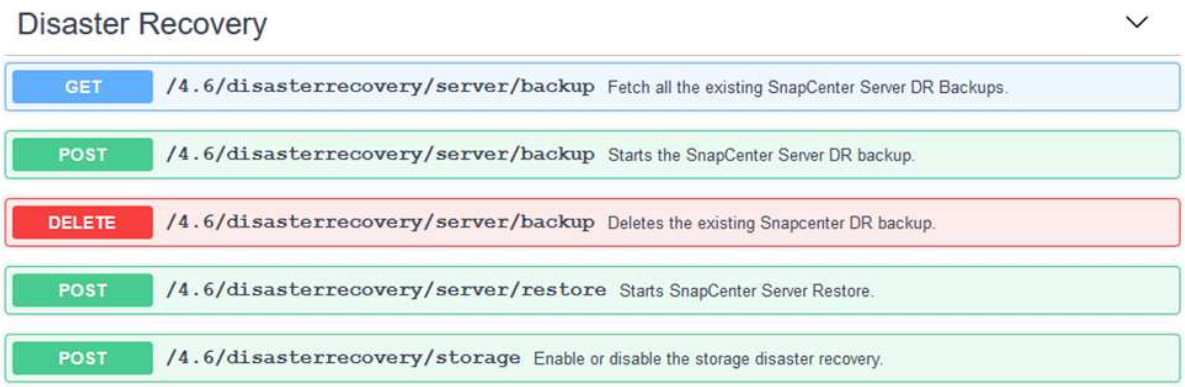
4. Dans le corps de réponse ci-dessous, vous pouvez voir le jeton. Copiez le texte du token pour l'authentification lors de l'exécution du processus de sauvegarde.



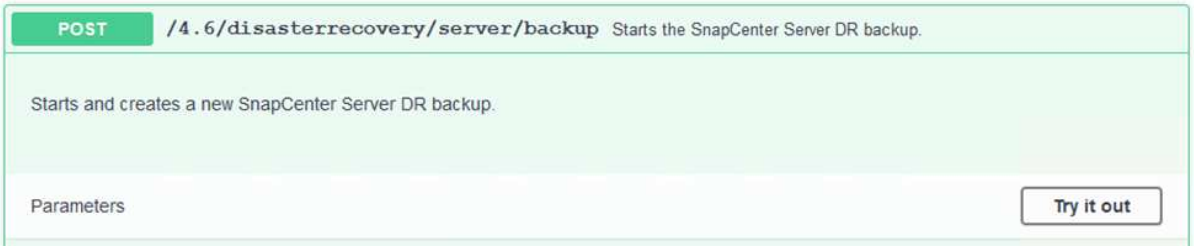
Effectuez une sauvegarde de base de données SnapCenter

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.

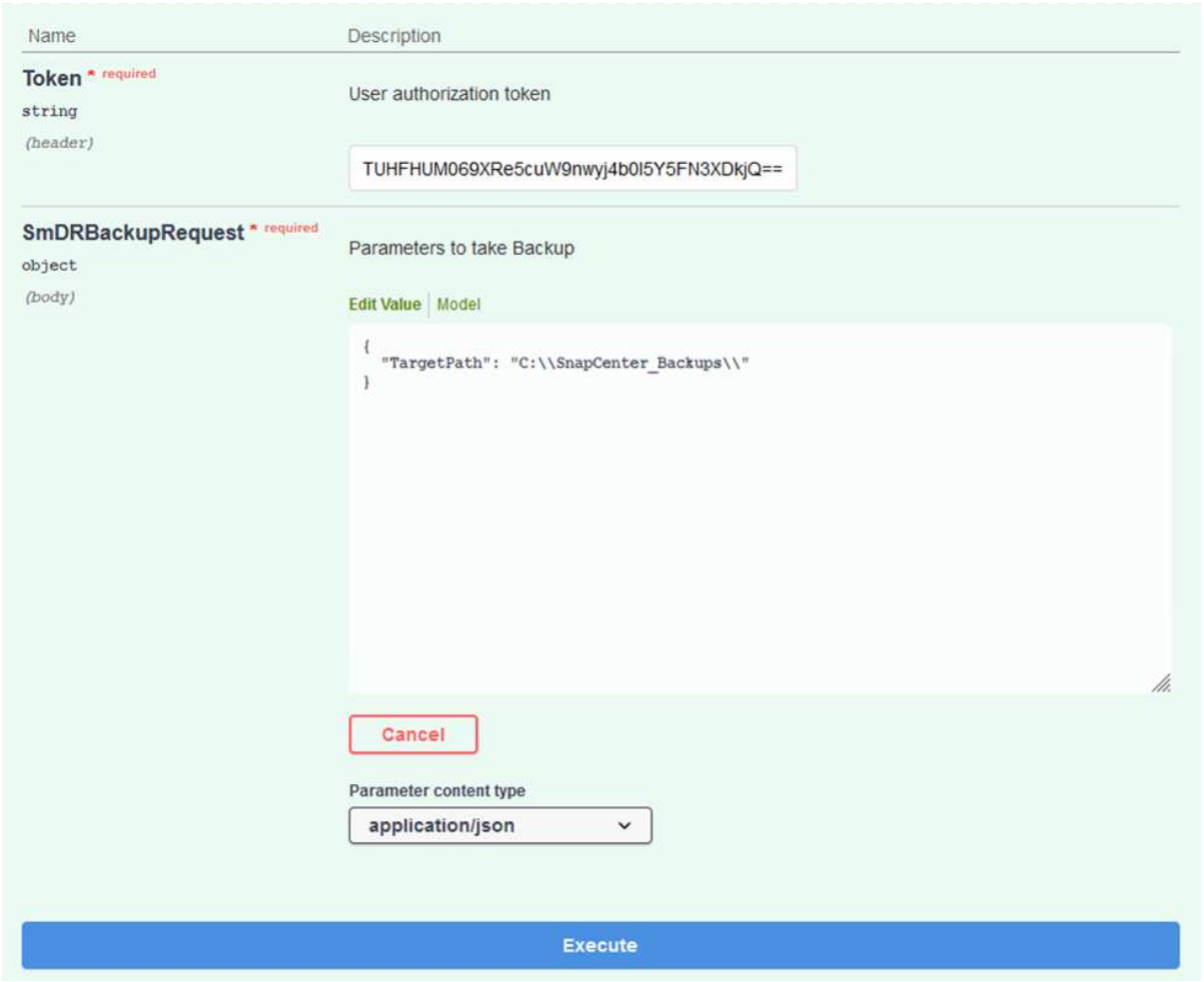


2. Développez le `/4.6/disasterrecovery/server/backup` Et cliquez sur essayer.



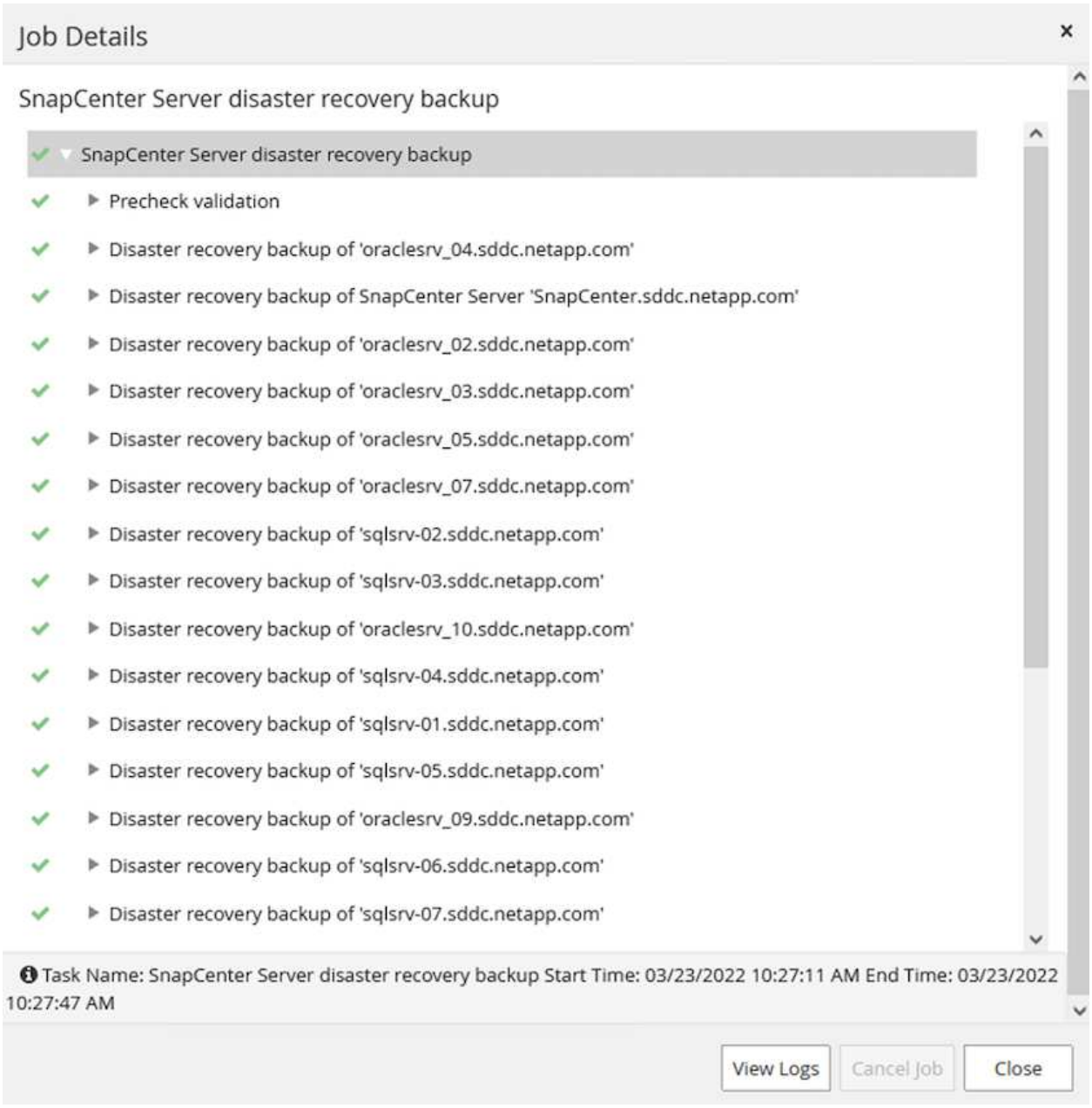
3. Dans la section SmDRBackupRequest, ajoutez le chemin cible local correct et sélectionnez Exécuter pour lancer la sauvegarde de la base de données et de la configuration SnapCenter.

> 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

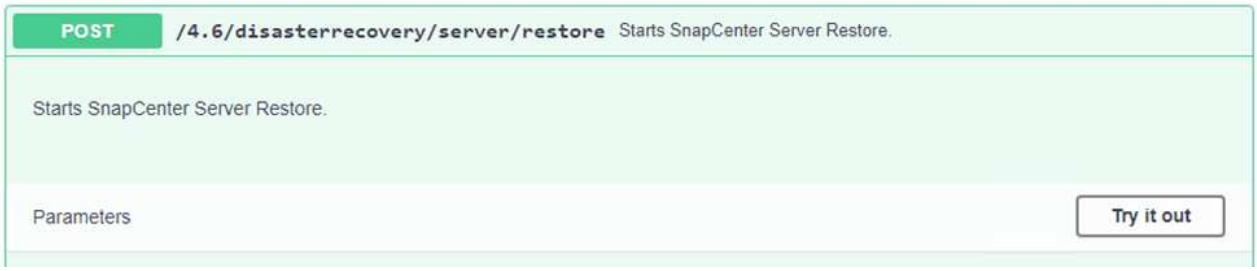
SnapCenter prend en charge les scénarios de reprise après incident en permettant la sauvegarde et la restauration de sa base de données MySQL et de ses fichiers de configuration. L'administrateur peut ainsi conserver des sauvegardes régulières de la base de données SnapCenter sur le data Center sur site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

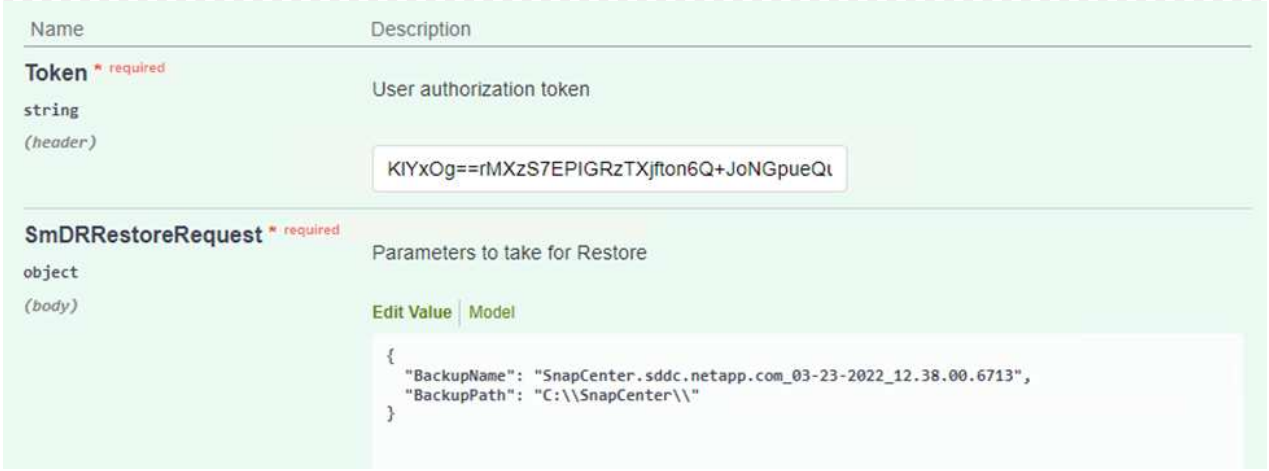
1. Faire un break de la relation SnapMirror depuis le cluster FSX, ce qui fait du volume la lecture/écriture.
2. Créer un serveur CIFS (si nécessaire) et créer un partage CIFS pointant vers la Junction path du volume cloné.
3. Utilisez xcopy pour copier les fichiers de sauvegarde dans un répertoire local 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 :

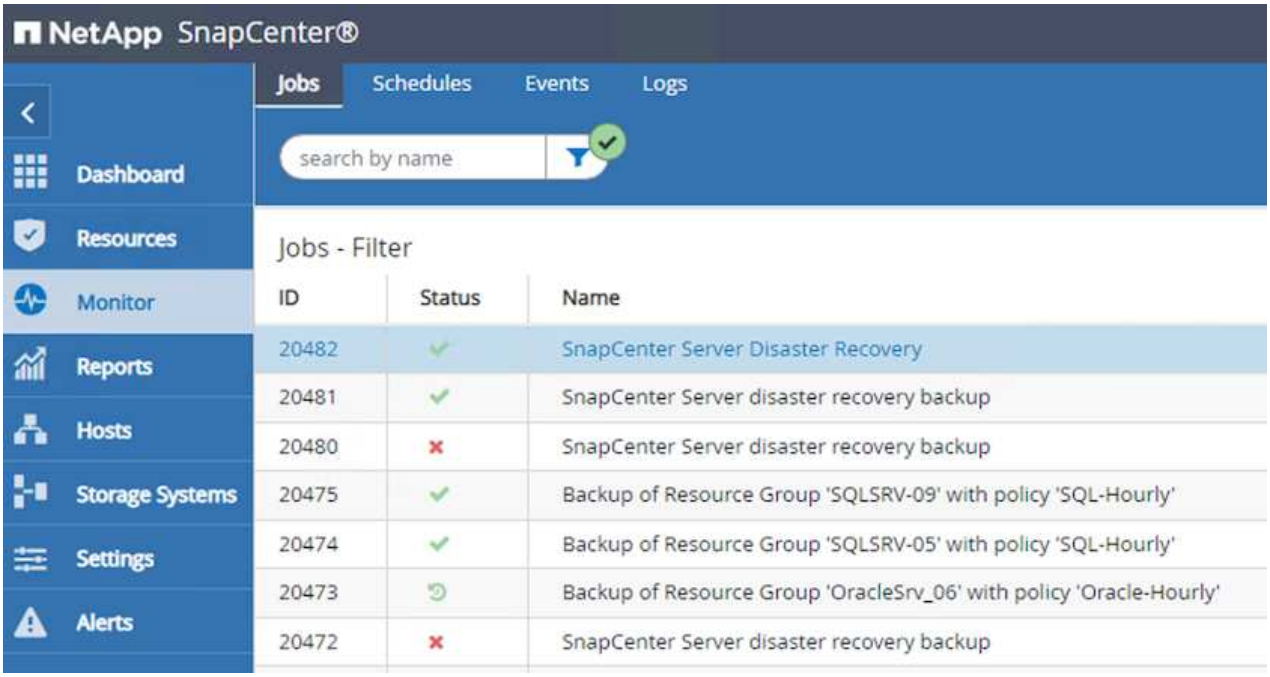
1. Accédez à la page Web de l'API swagger pour le serveur SnapCenter secondaire et suivez les instructions précédentes pour obtenir un jeton d'autorisation.
2. Accédez à la section récupération après sinistre de la page de swagger, puis sélectionnez `/4.6/disasterrecovery/server/restore`, Puis cliquez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

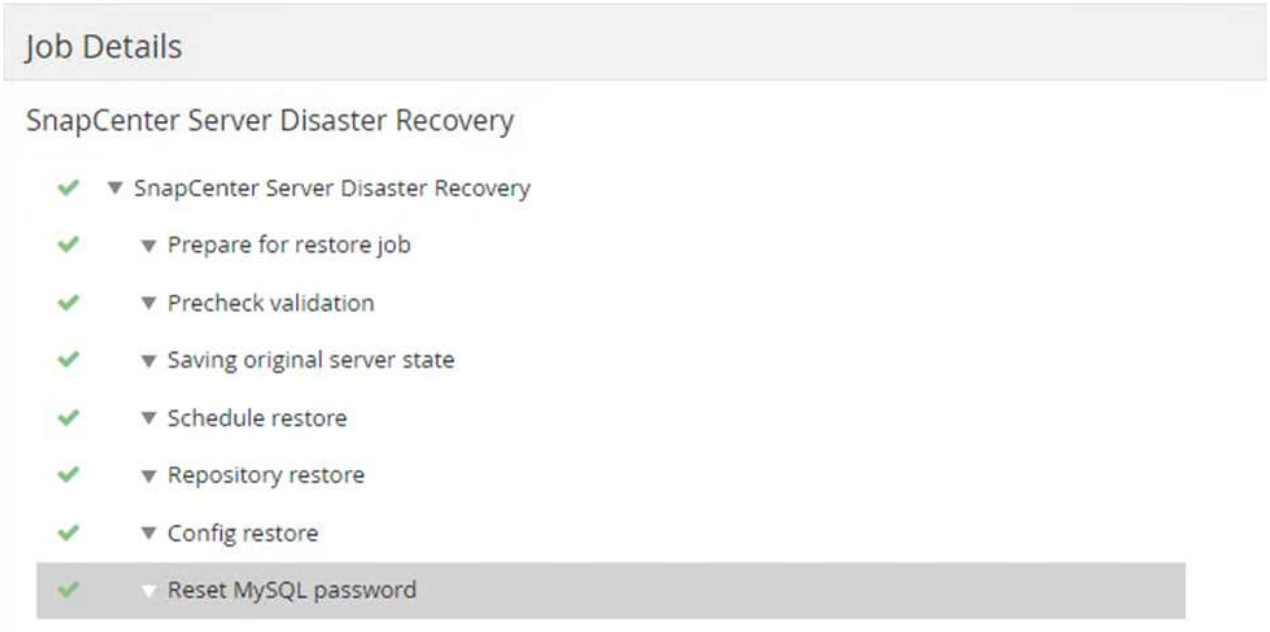


3. Collez le jeton d'autorisation et, dans la section SmDRResterRequest, collez le nom de la sauvegarde et le répertoire local sur le serveur SnapCenter secondaire.



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.





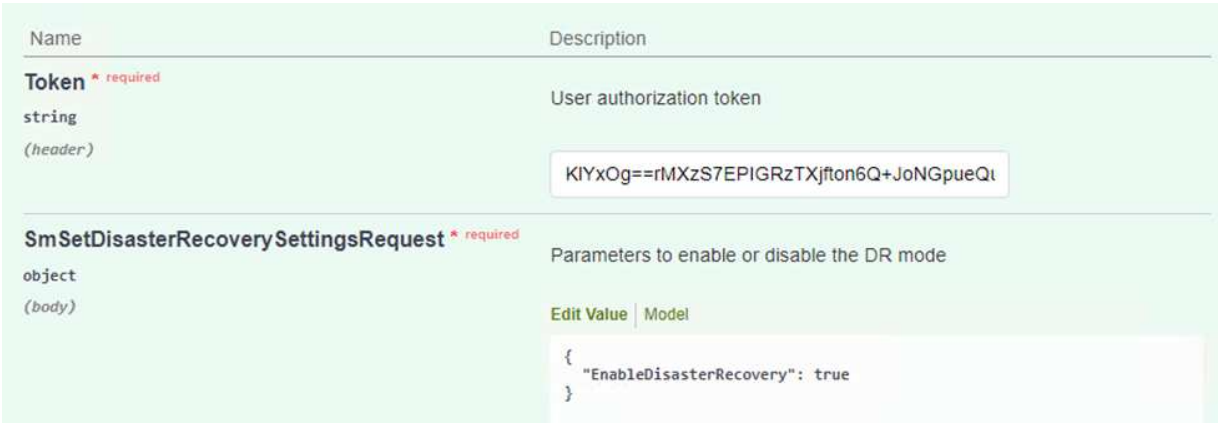
6. Pour activer les restaurations SQL Server à partir du stockage secondaire, vous devez basculer la base de données SnapCenter en mode de reprise après incident. Cette opération est exécutée séparément et lancée sur la page Web de l'API swagger.

   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.

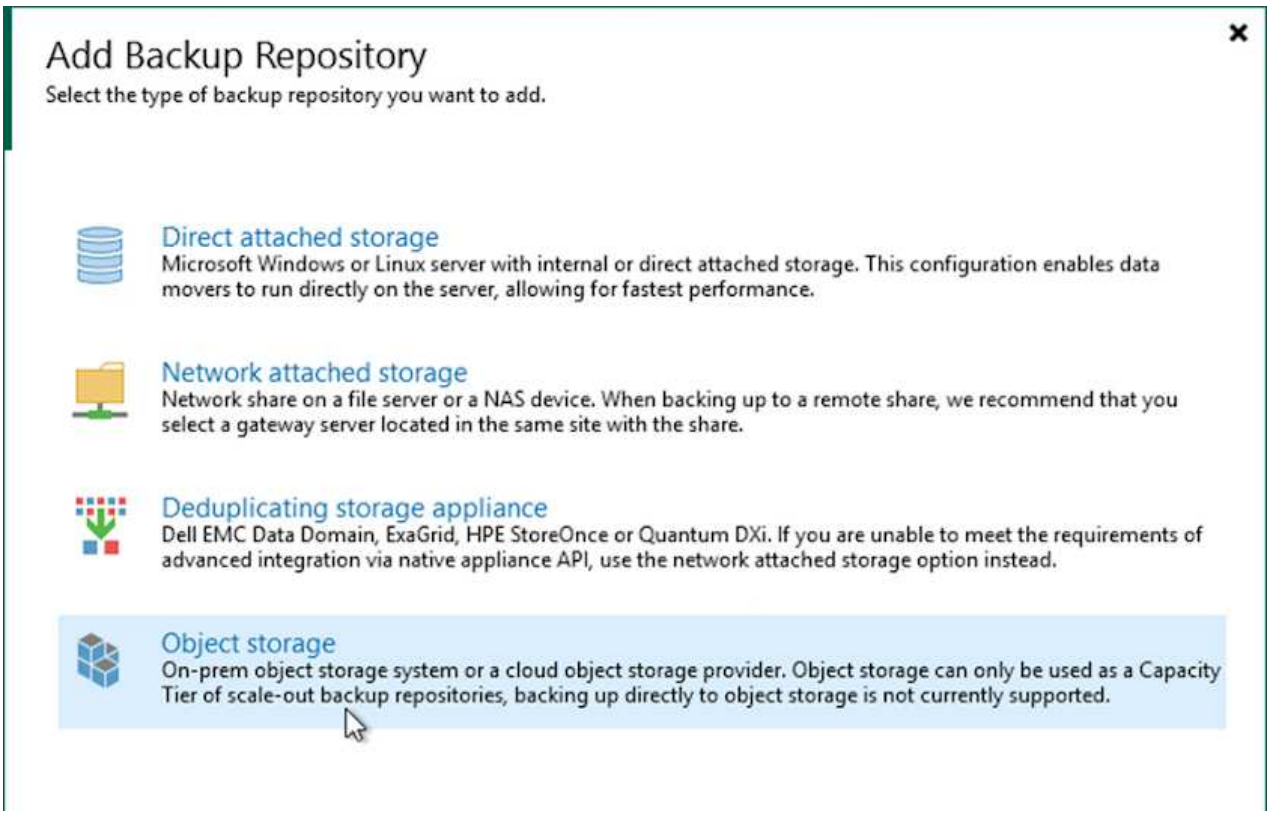
Restauration des VM applications grâce à la restauration complète Veeam

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

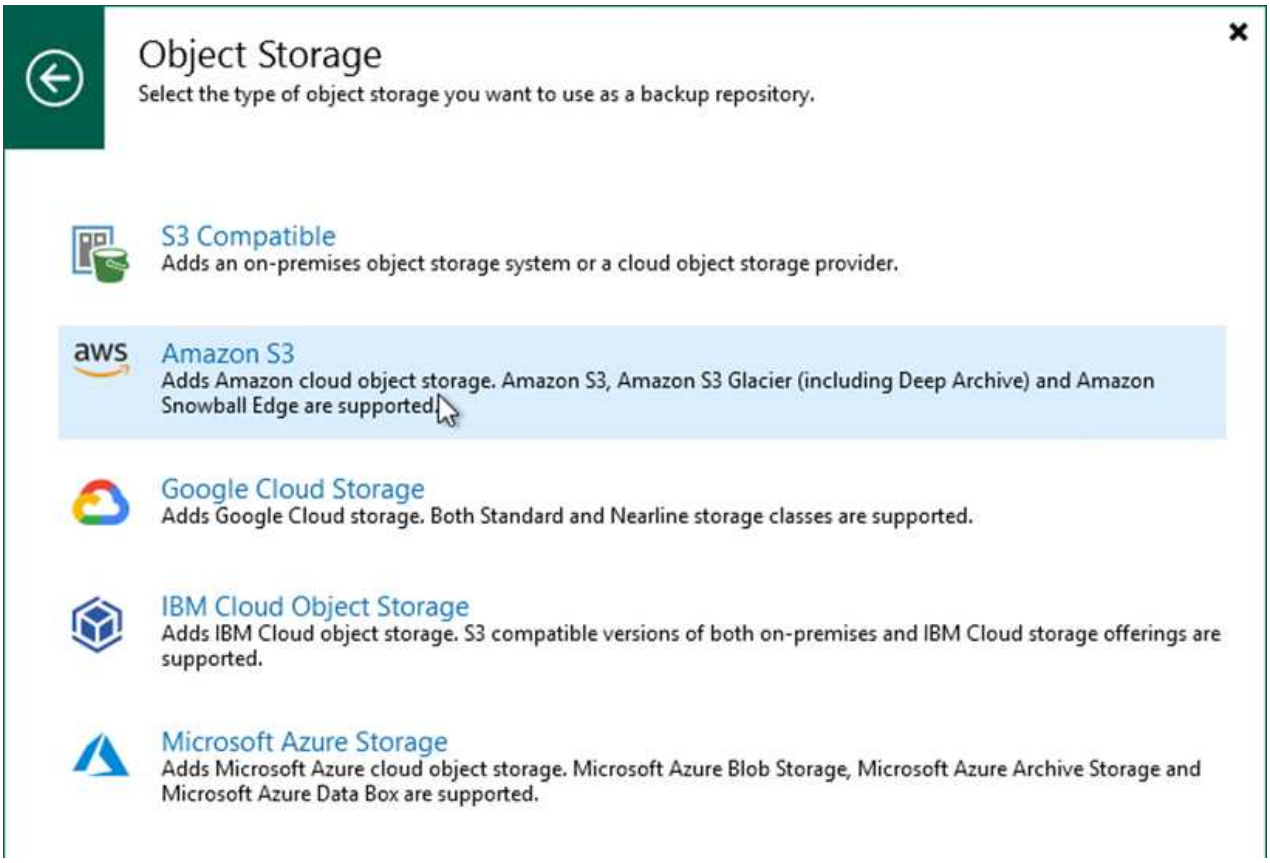
Depuis le serveur Veeam secondaire, importez les sauvegardes depuis le stockage S3 et restaurez les machines virtuelles SQL Server et Oracle sur votre cluster VMware Cloud.

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.

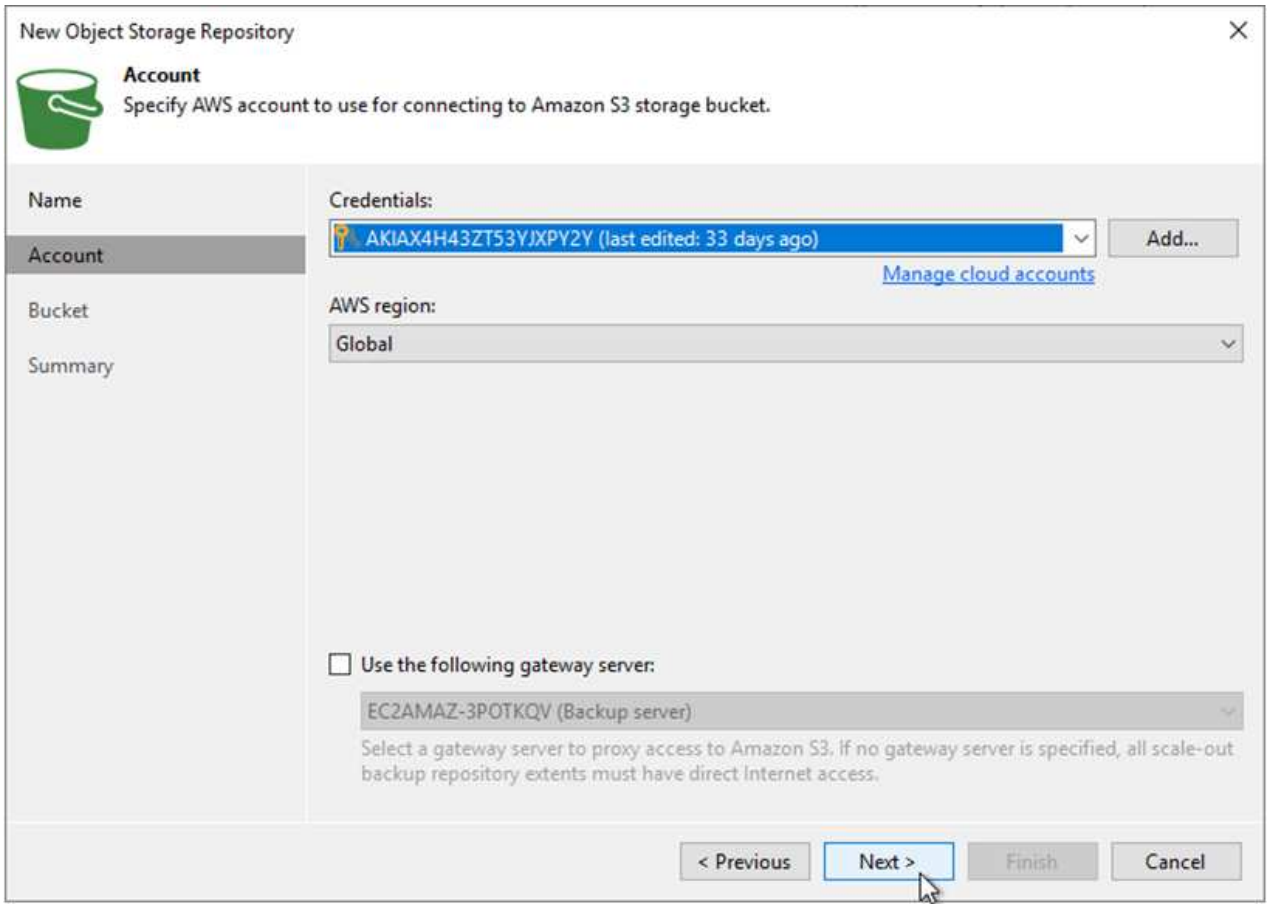


2. Sélectionnez Amazon S3 comme type de stockage objet.

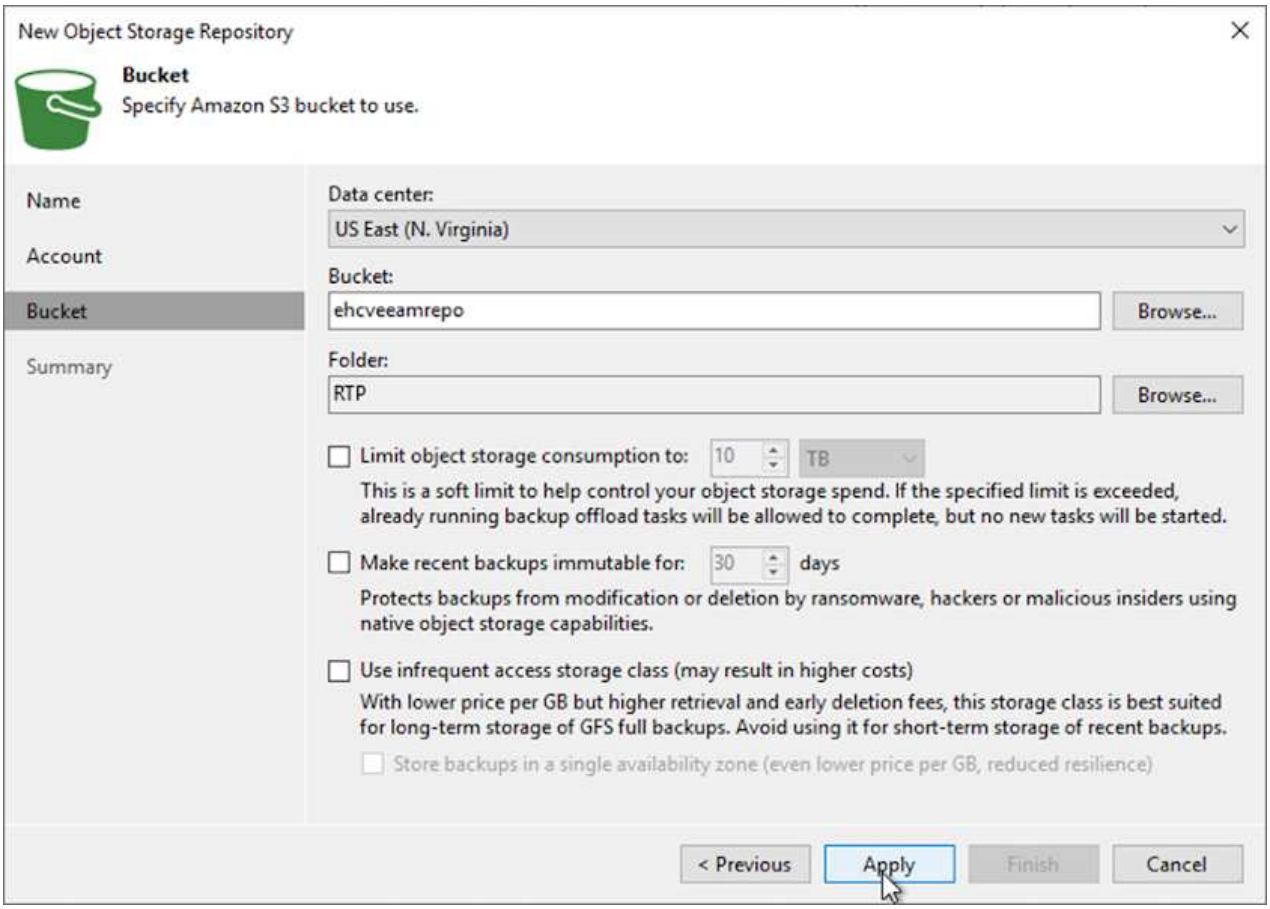


3. Dans la liste d'Amazon Cloud Storage Services, sélectionnez Amazon S3.

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.

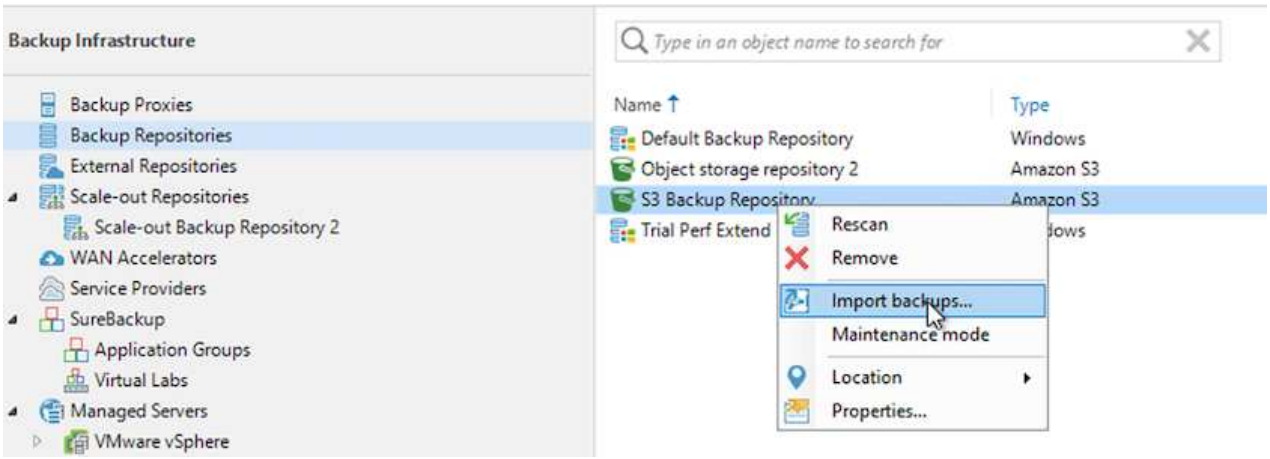


6. Enfin, sélectionnez Terminer pour terminer le processus et ajouter le référentiel.

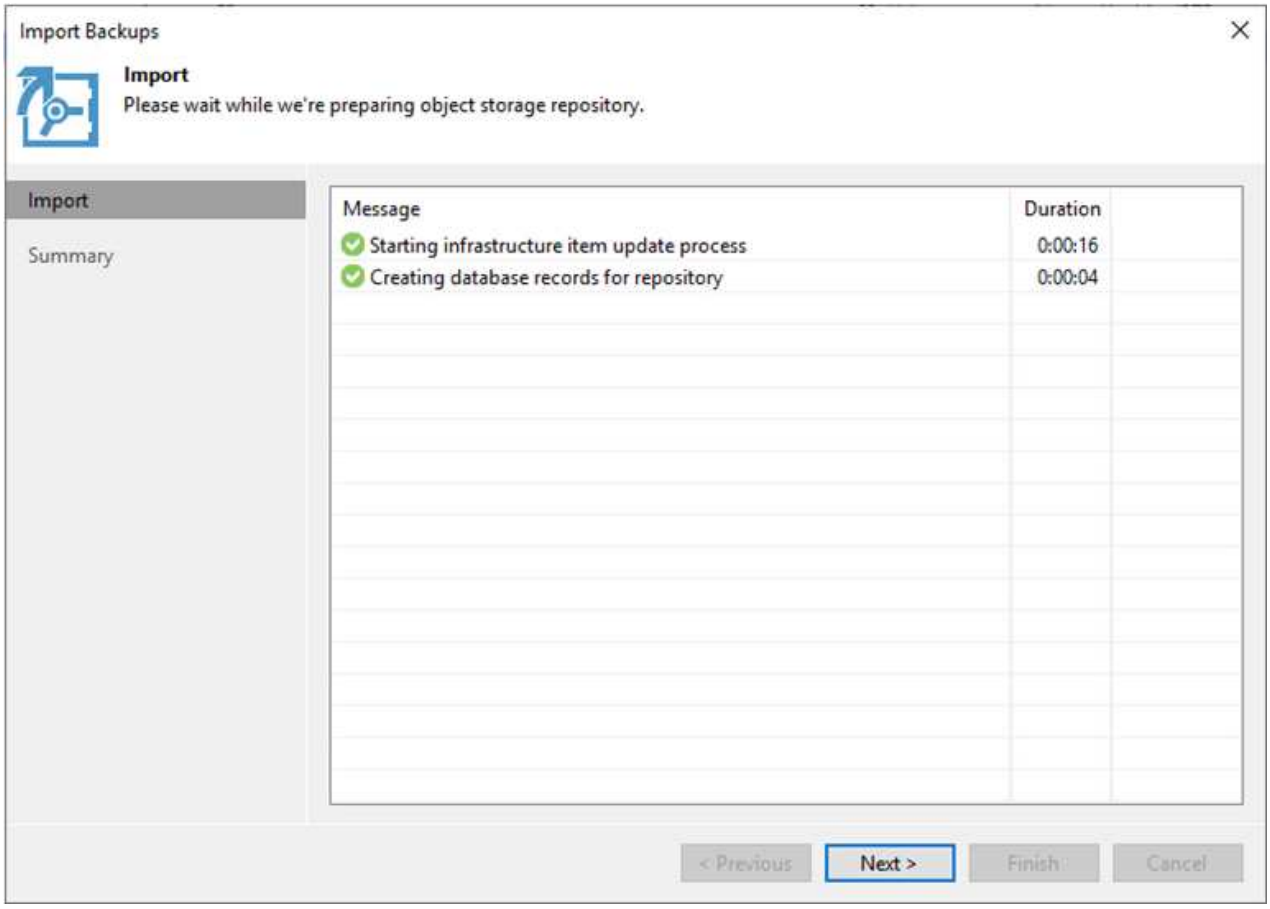
Importation des sauvegardes à partir du stockage objet S3

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

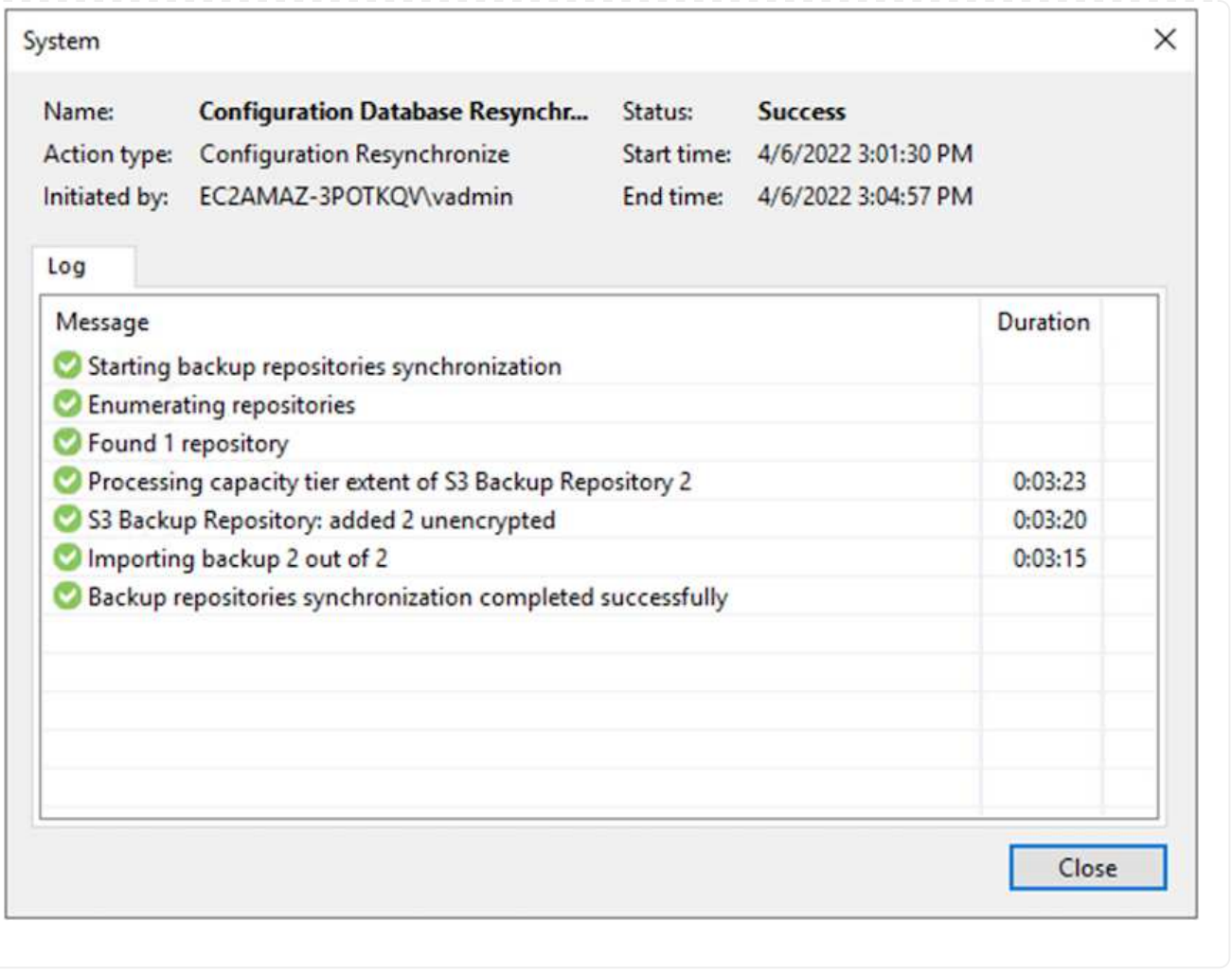
1. Dans le référentiel de sauvegardes S3, sélectionnez Importer les sauvegardes pour lancer l'assistant Importer les sauvegardes.



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.



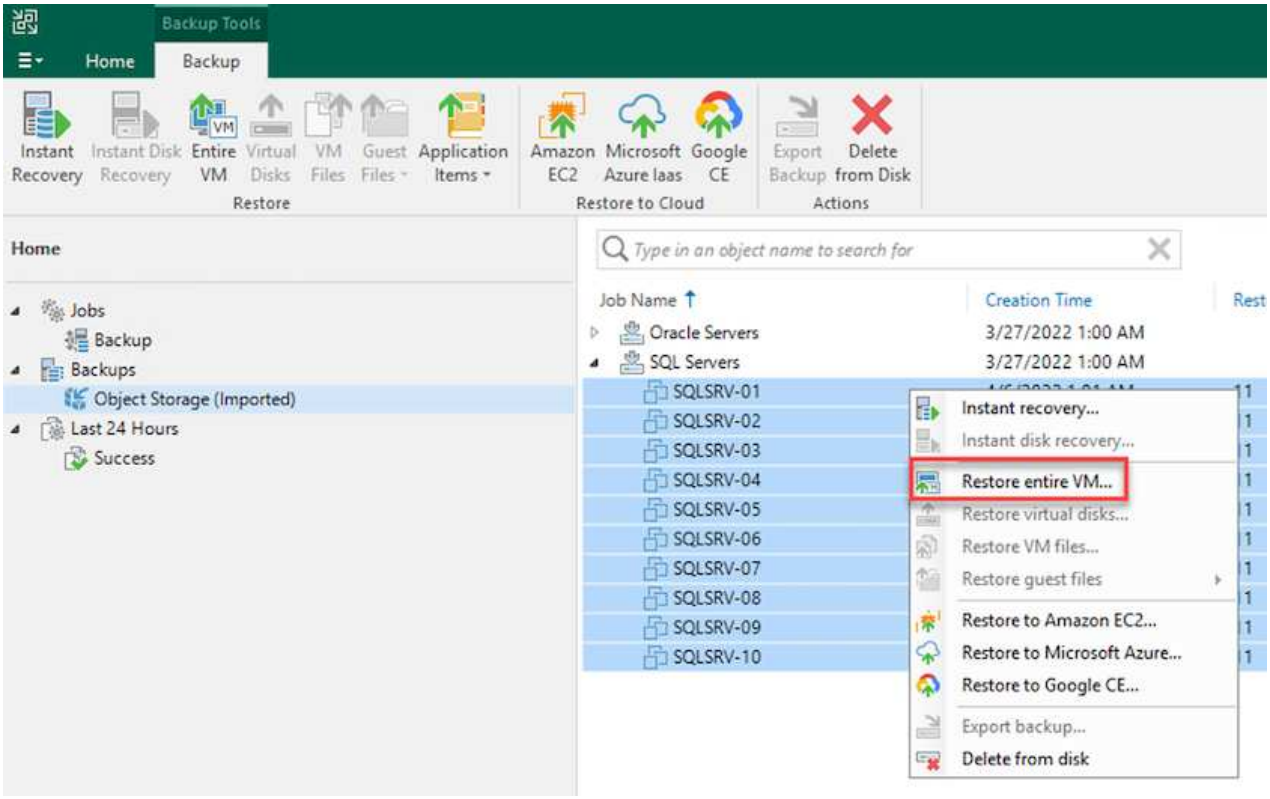
3. Une fois l'importation terminée, vous pouvez restaurer les machines virtuelles dans le cluster VMware Cloud.


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

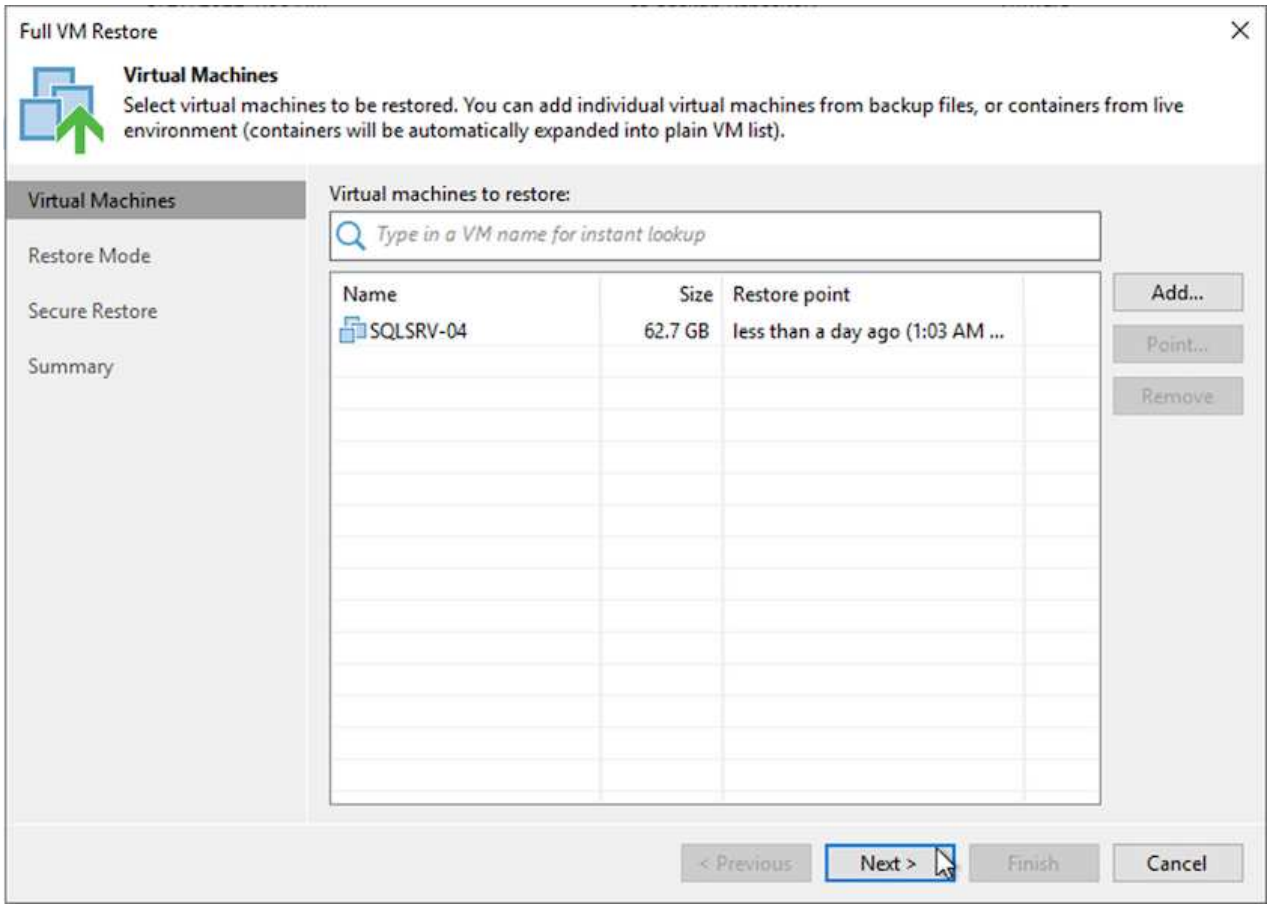
Restauration des VM applicatives avec restauration complète Veeam dans VMware Cloud

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.

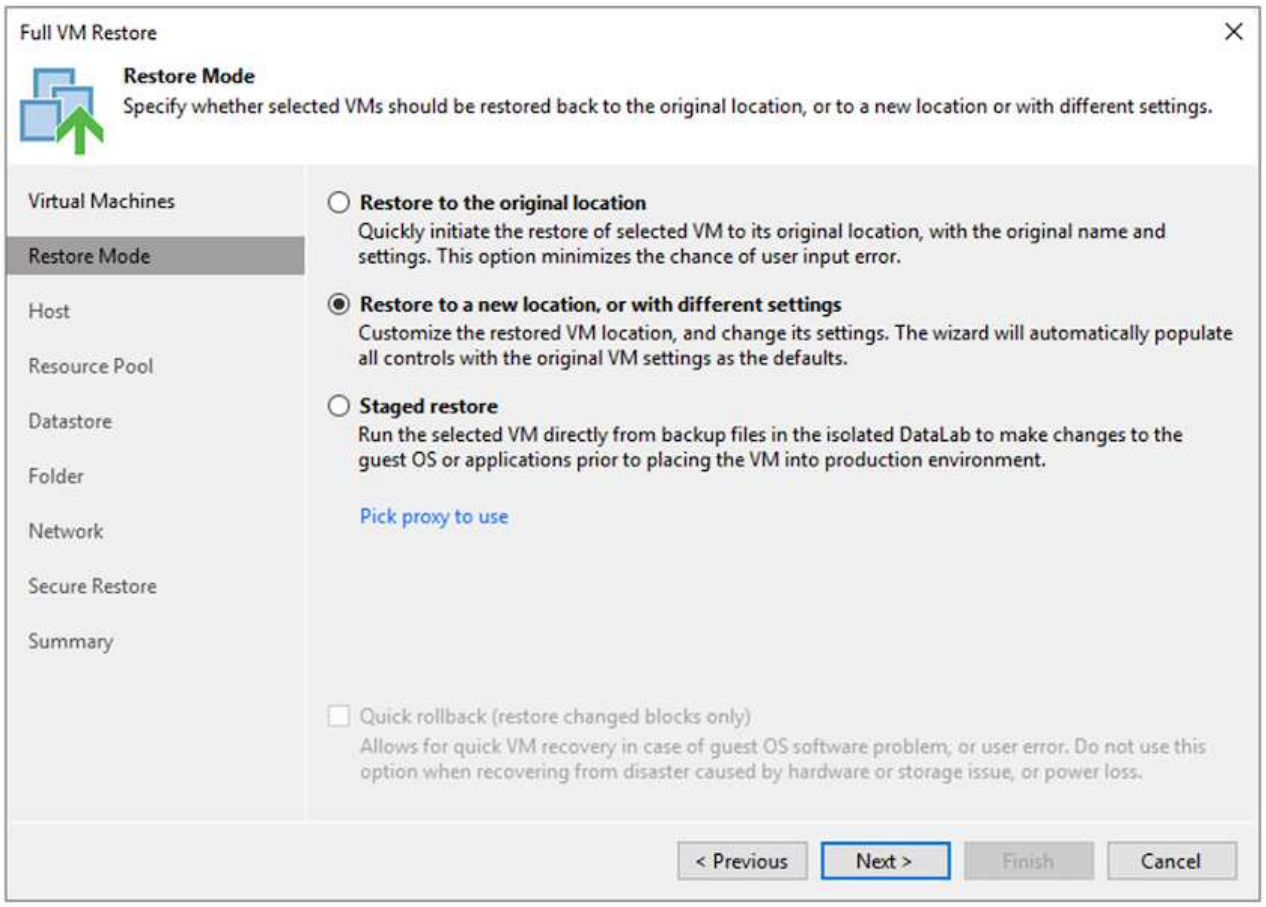
1. Dans la page d'accueil Veeam, sélectionnez le stockage d'objets contenant les sauvegardes importées, sélectionnez les machines virtuelles à restaurer, puis cliquez avec le bouton droit de la souris et sélectionnez Restaurer la machine virtuelle entière.



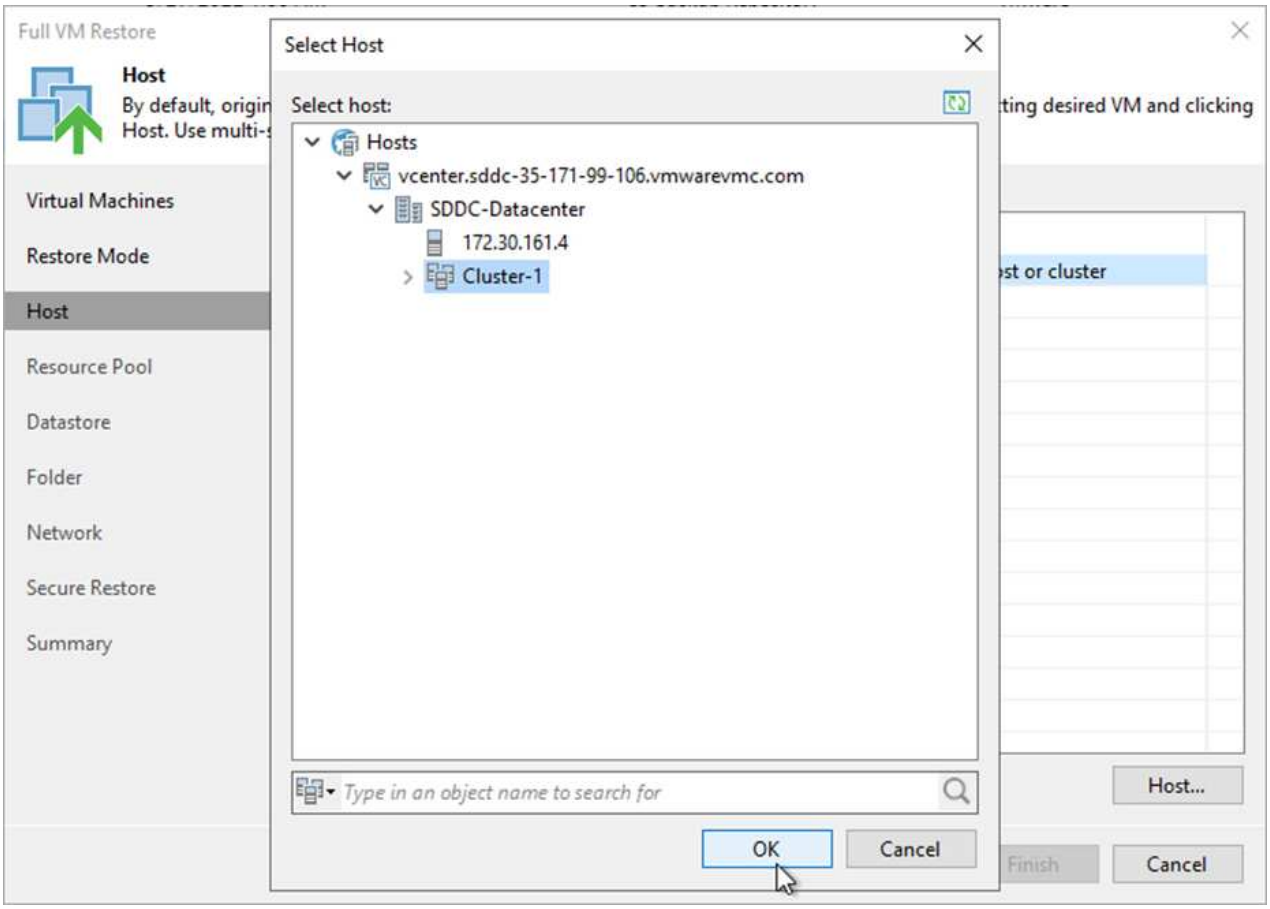
2. Sur la première page de l'assistant de restauration complète de VM, modifiez les VM à sauvegarder si vous le souhaitez et sélectionnez Suivant.



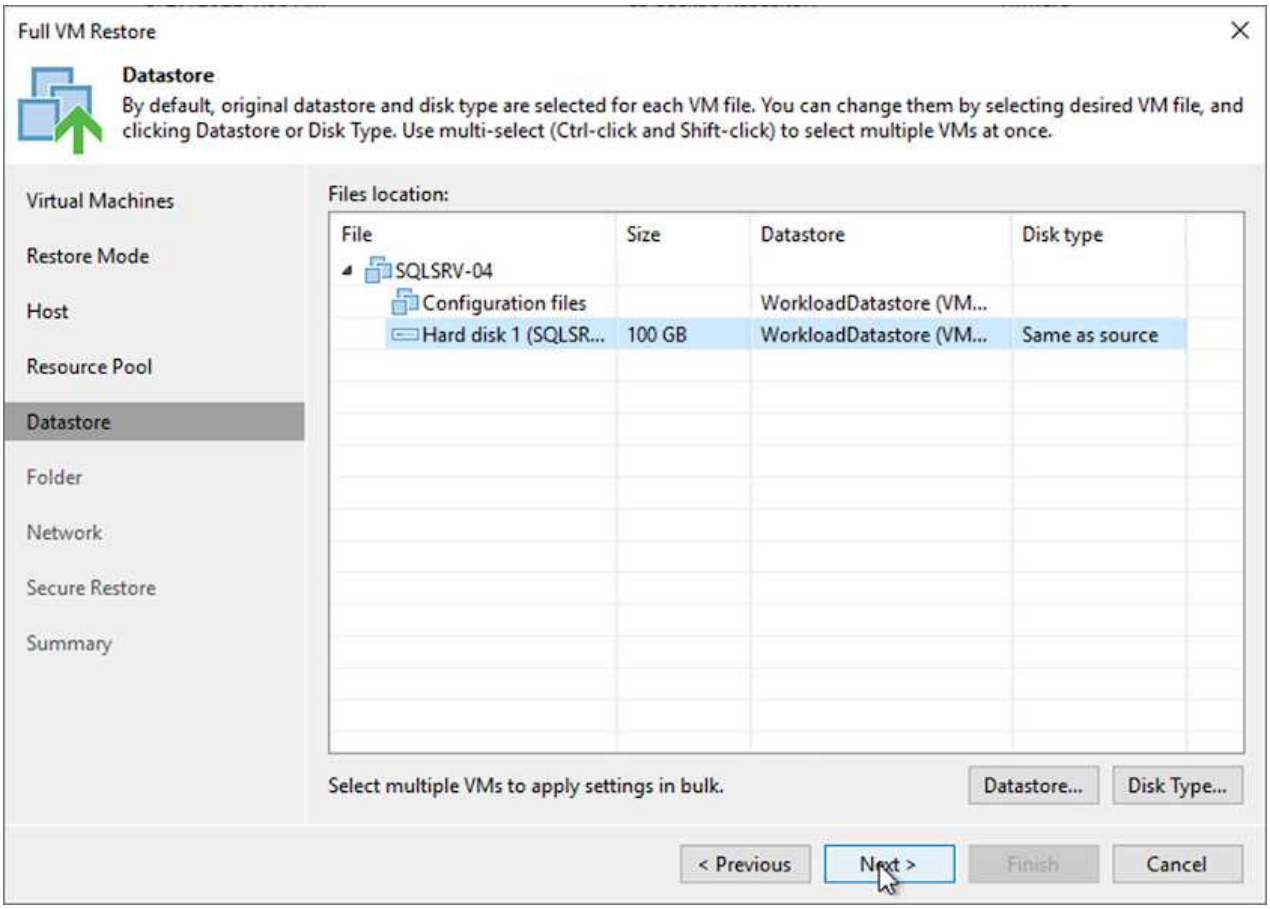
3. Sur la page mode de restauration, sélectionnez Restaurer à un nouvel emplacement ou avec des paramètres différents.



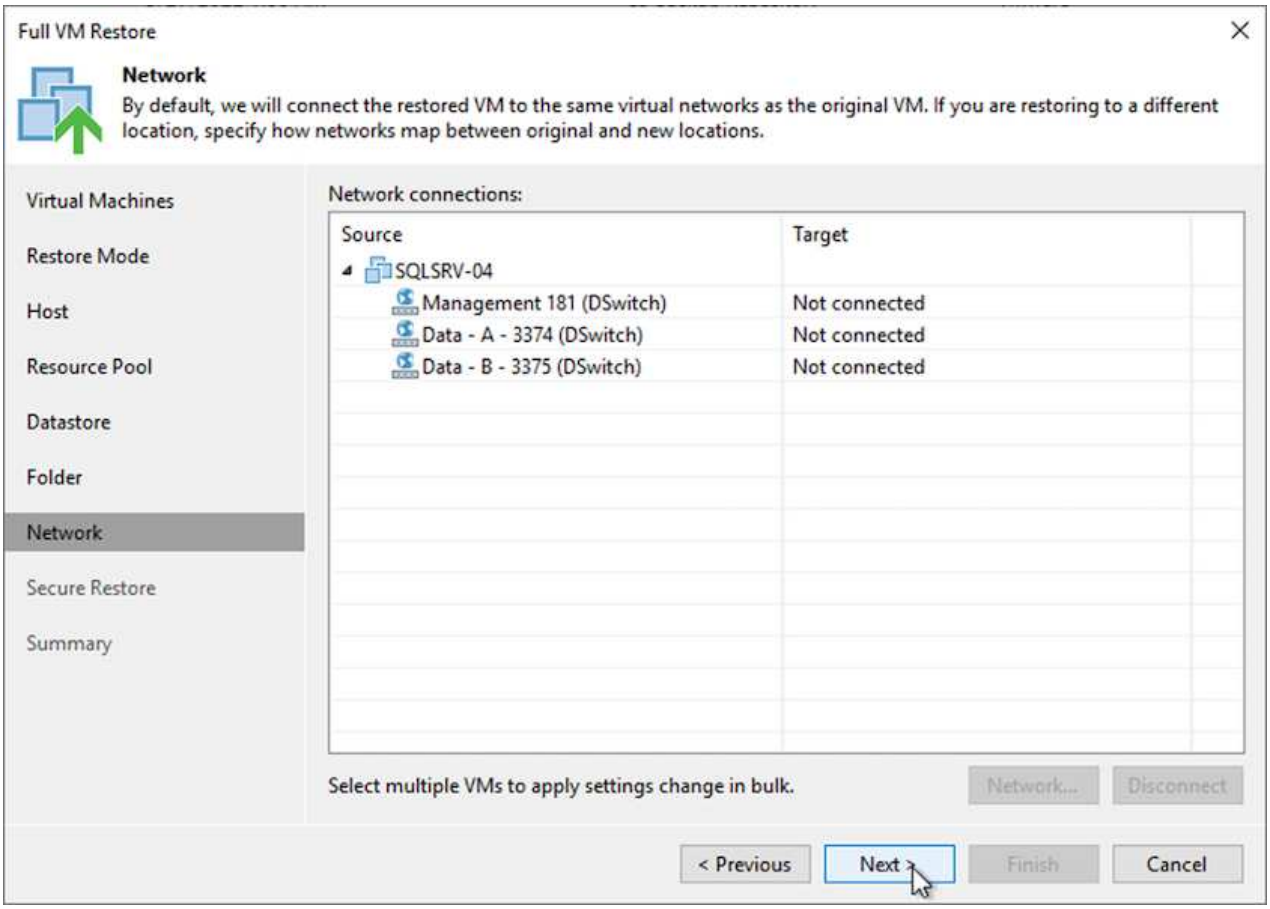
4. Sur la page hôte, sélectionnez l'hôte ou le cluster ESXi cible pour restaurer la machine virtuelle.

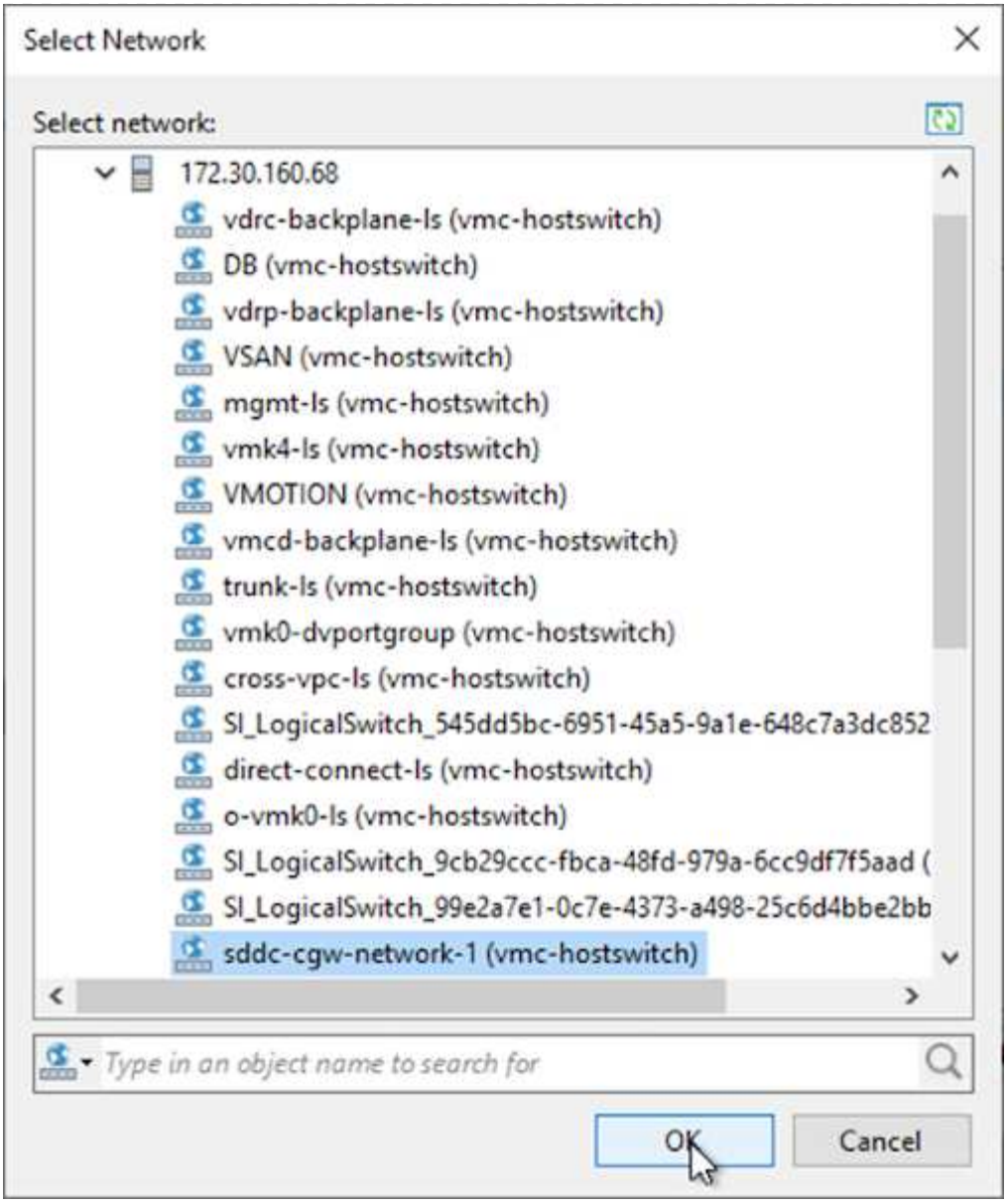


5. Sur la page datastores, sélectionnez l'emplacement du datastore cible pour les fichiers de configuration et le disque dur.



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
```

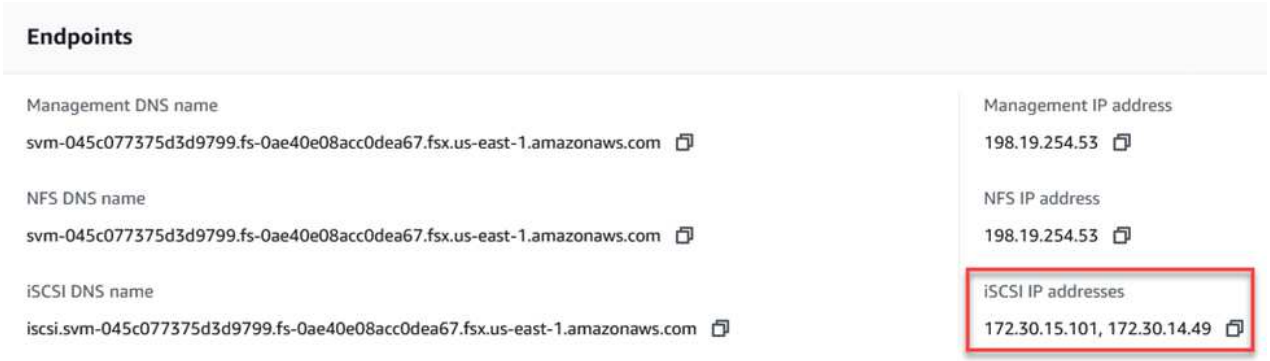
3. Enfin, mappez les LUN sur le groupe initiateur que vous venez de créer :

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

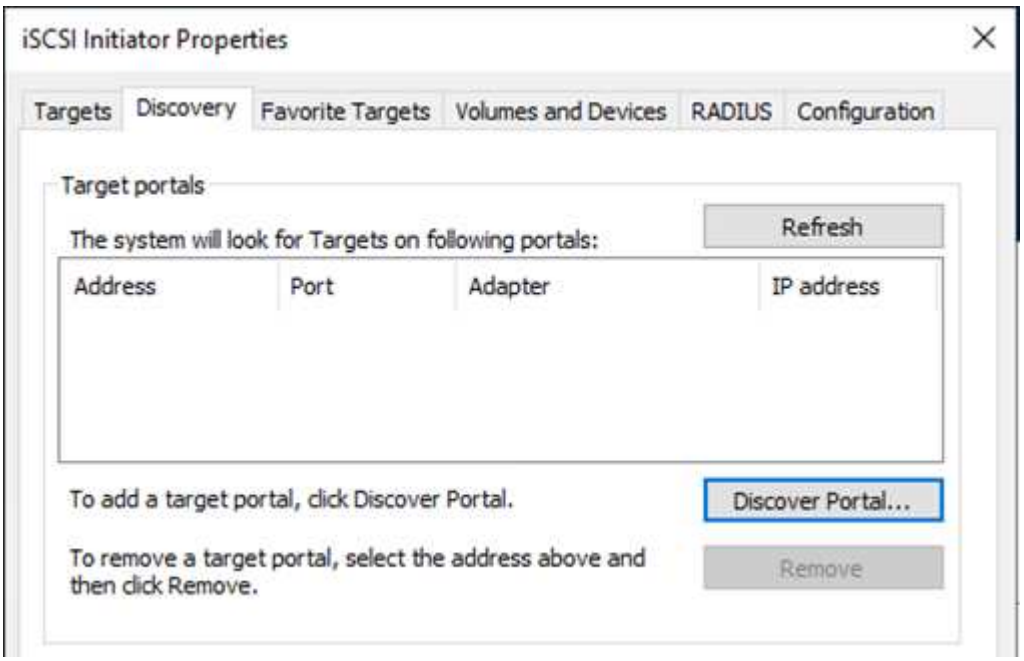
4. Pour trouver le nom du chemin d'accès, exécutez le `lun show` commande.

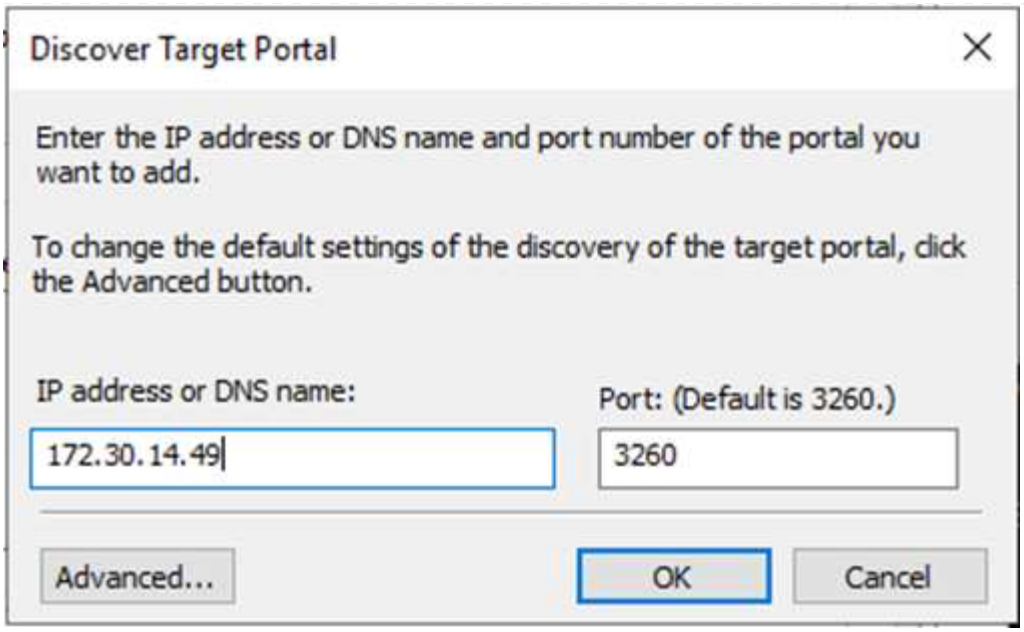
Configurer la machine virtuelle Windows pour l'accès iSCSI et découvrir les systèmes de fichiers

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.

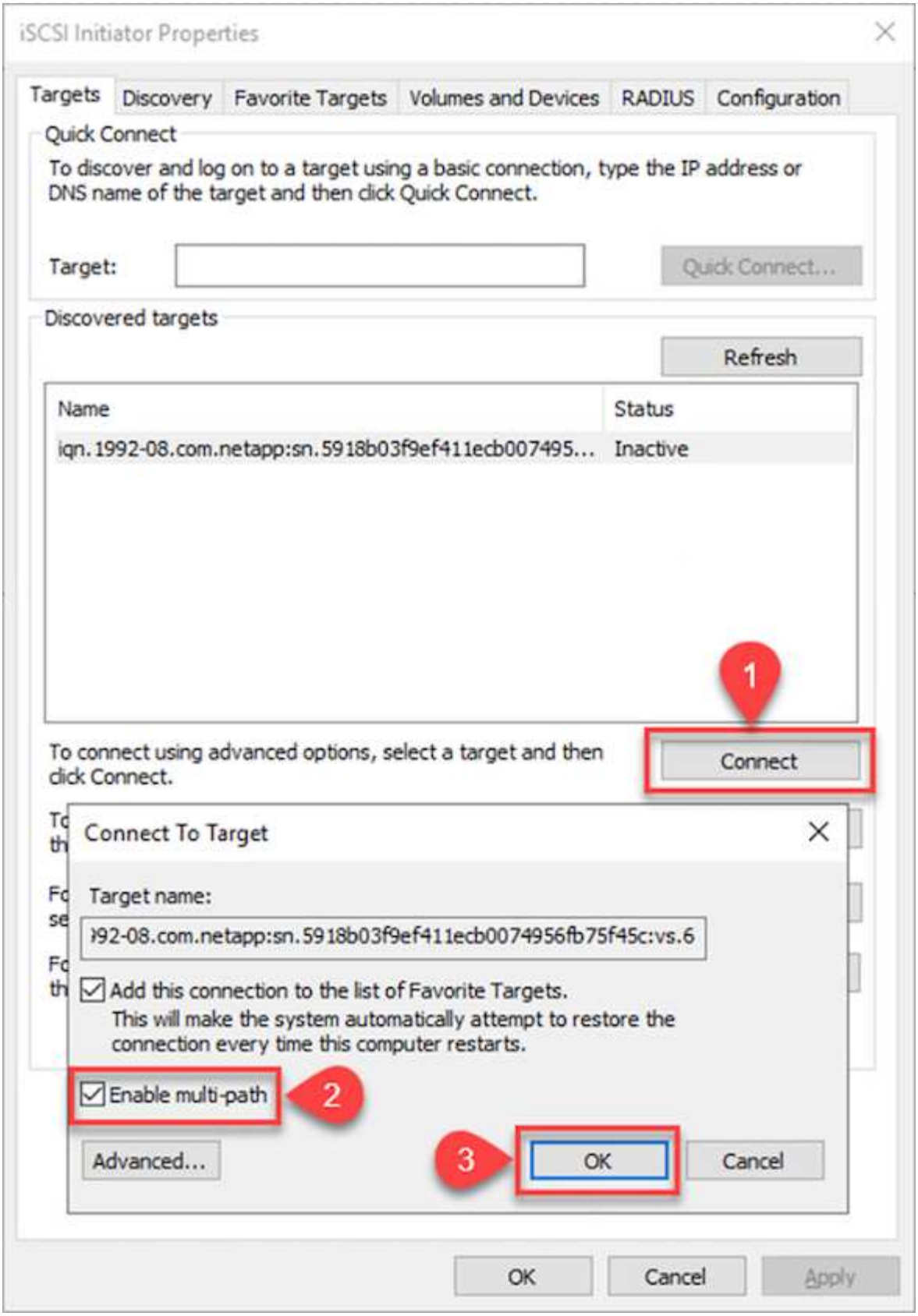


4. Dans l'onglet découverte, cliquez sur Discover Portal et entrez les adresses IP de vos cibles iSCSI FSX.

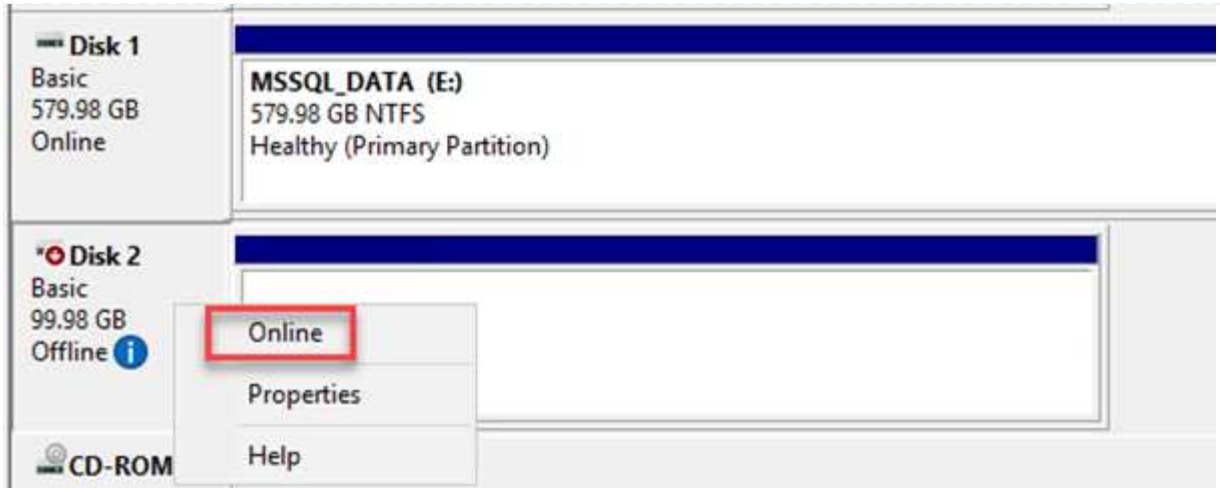




5. Dans l'onglet cible, cliquez sur connecter, sélectionnez Activer le multichemin si nécessaire pour votre configuration, puis cliquez sur OK pour vous connecter à la cible.

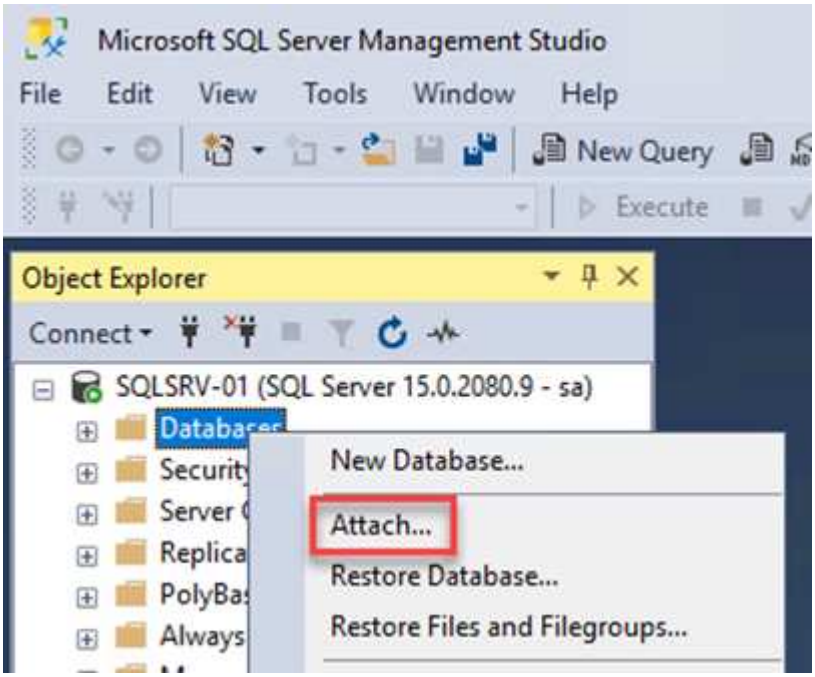


6. Ouvrez l'utilitaire gestion de l'ordinateur et connectez les disques. Vérifiez qu'ils conservent les mêmes lettres de lecteur qu'ils étaient auparavant.

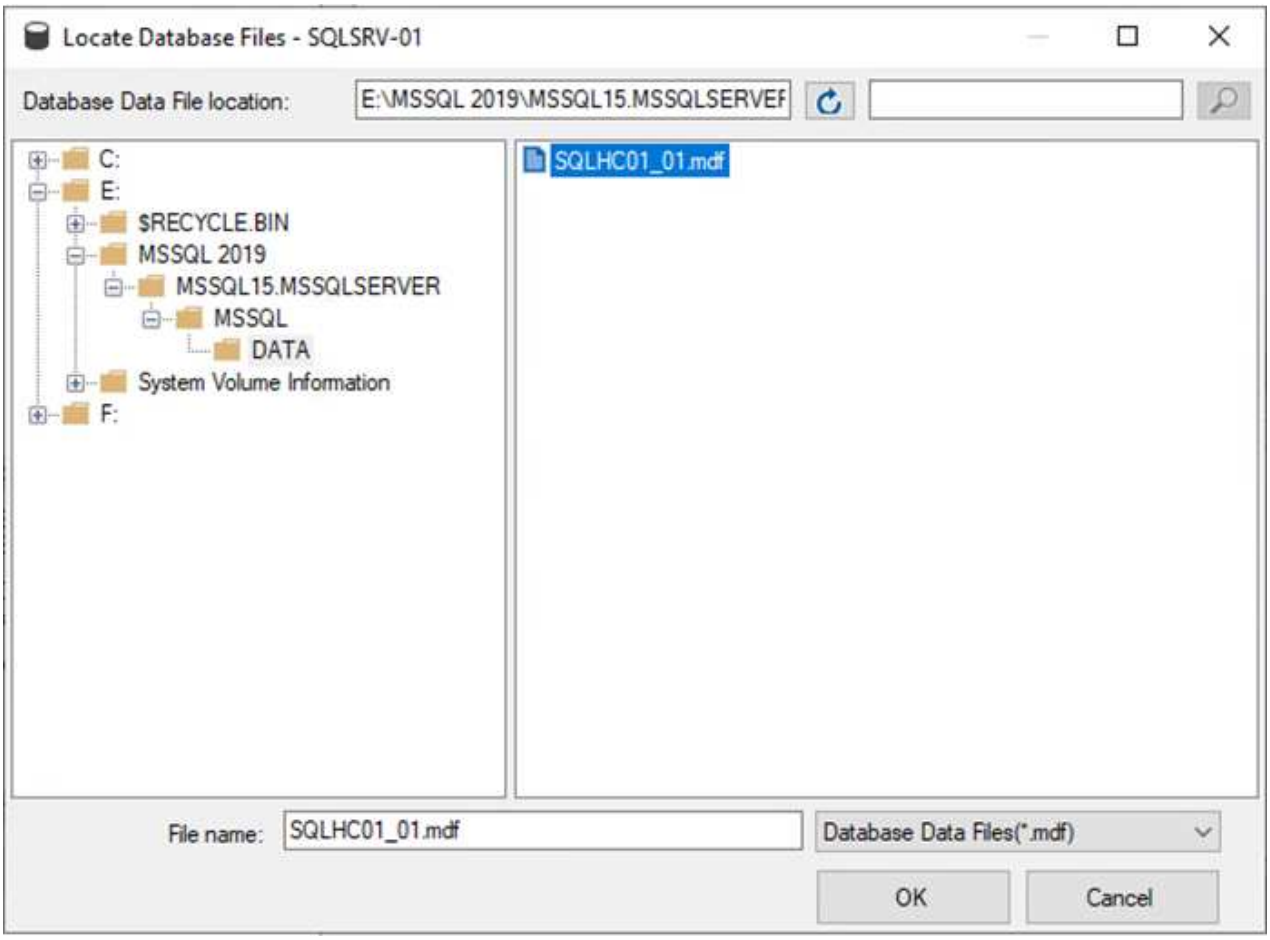

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Reliez les bases de données SQL Server

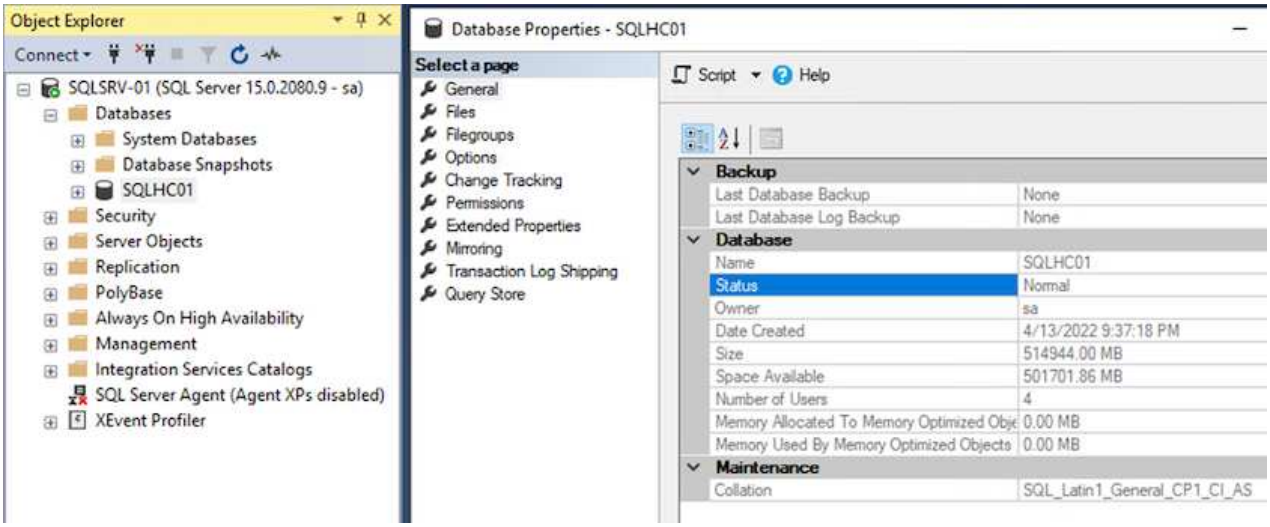
1. À partir de la VM SQL Server, ouvrez Microsoft SQL Server Management Studio et sélectionnez attacher pour démarrer le processus de connexion à la base de données.



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.

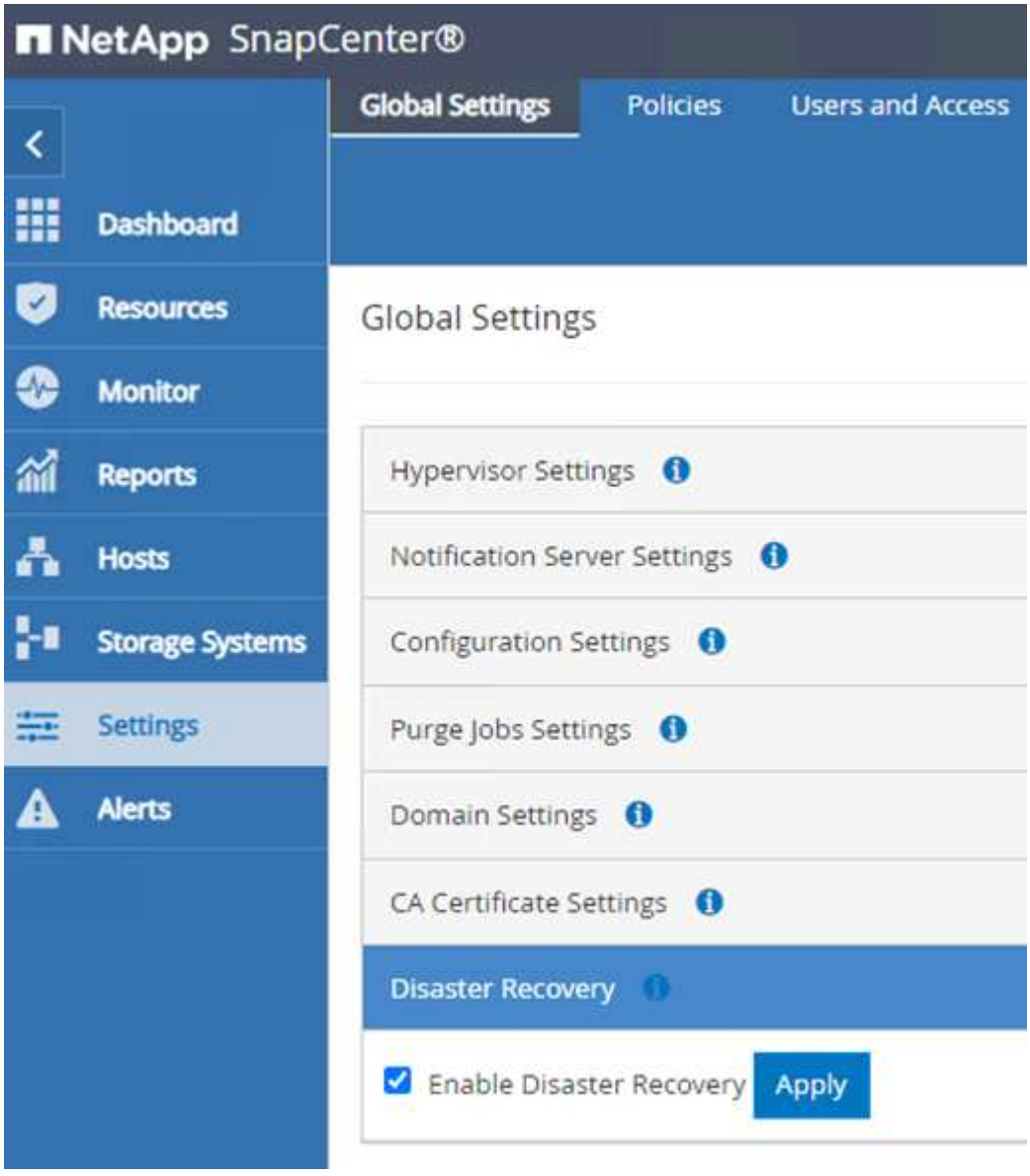


Confirmez la communication SnapCenter avec le plug-in SQL Server

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*
```

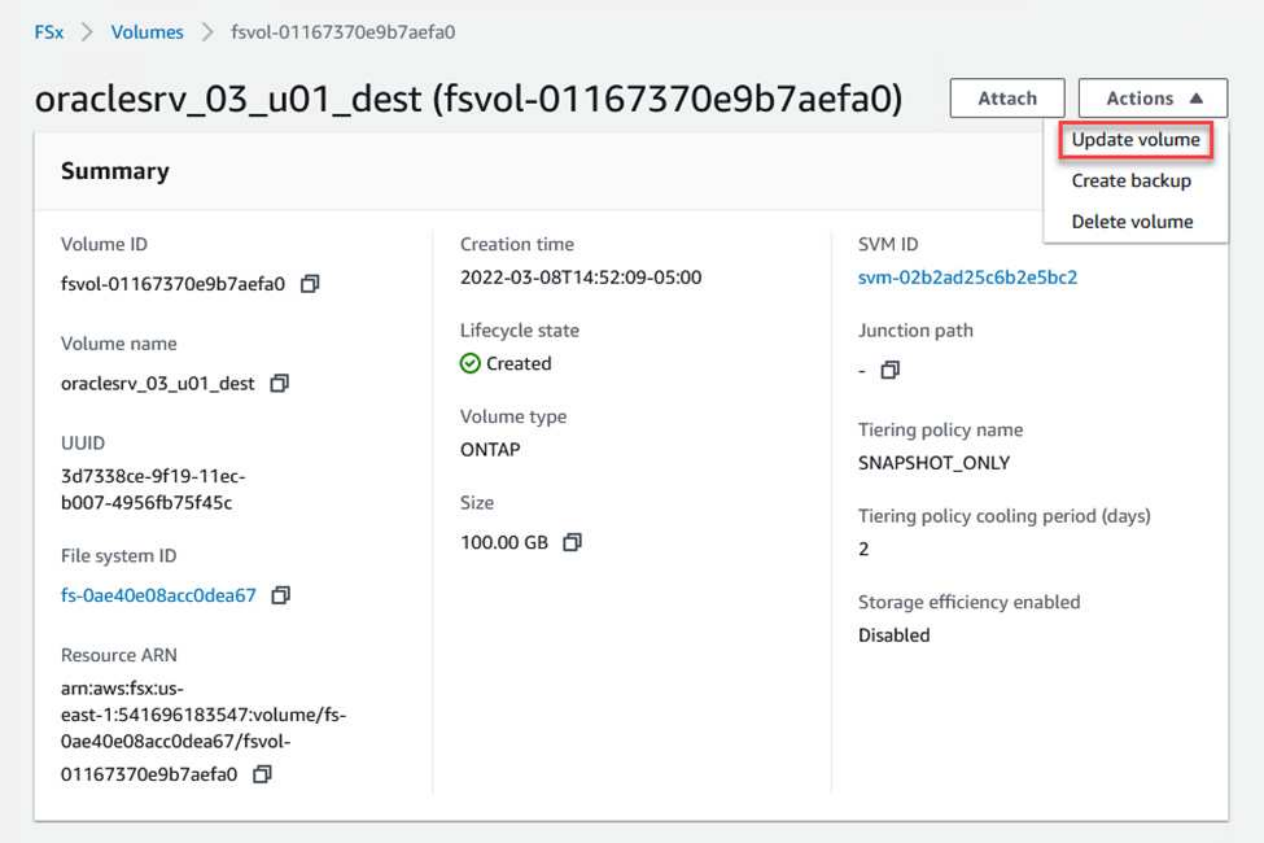
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        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.

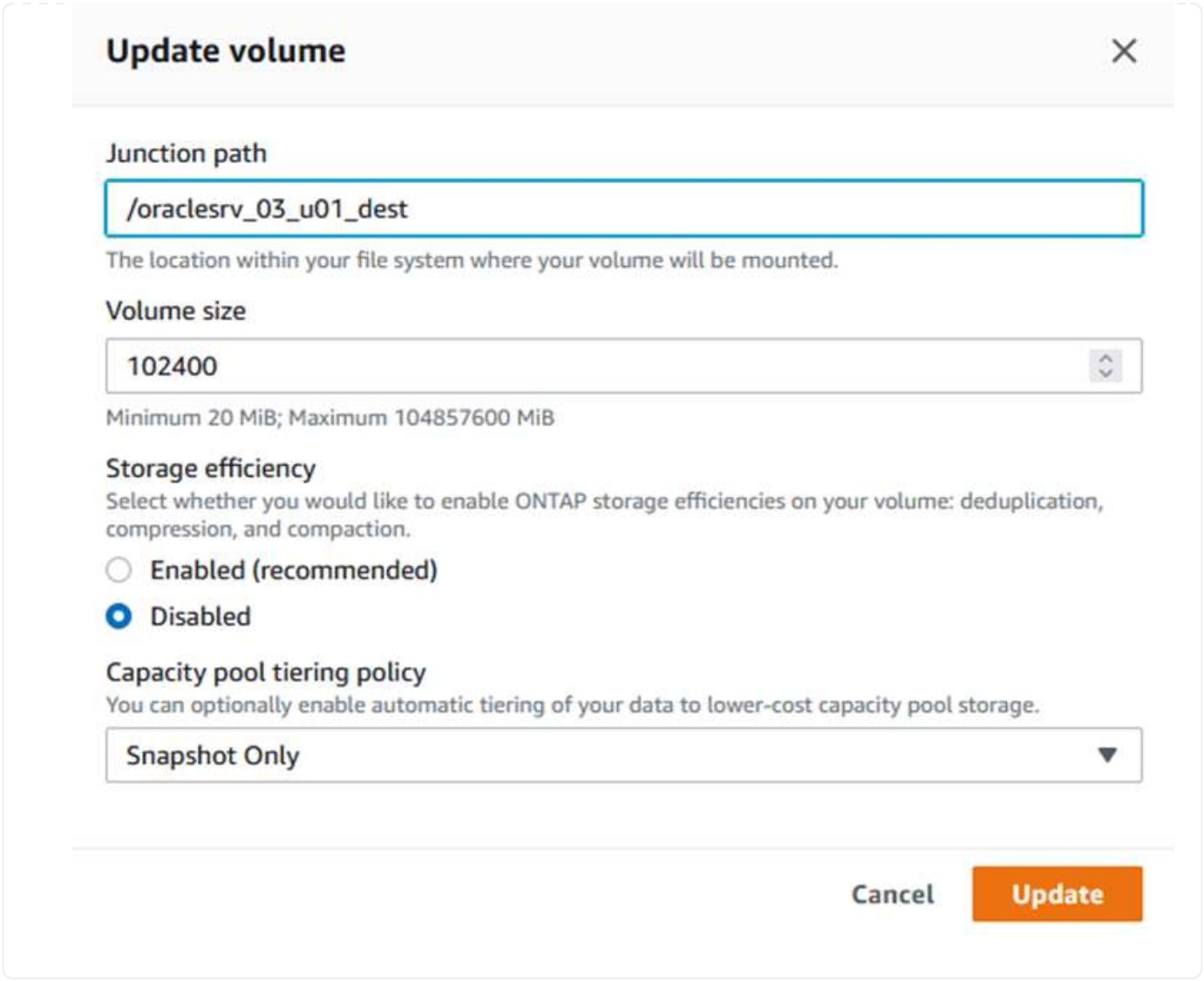
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
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 :



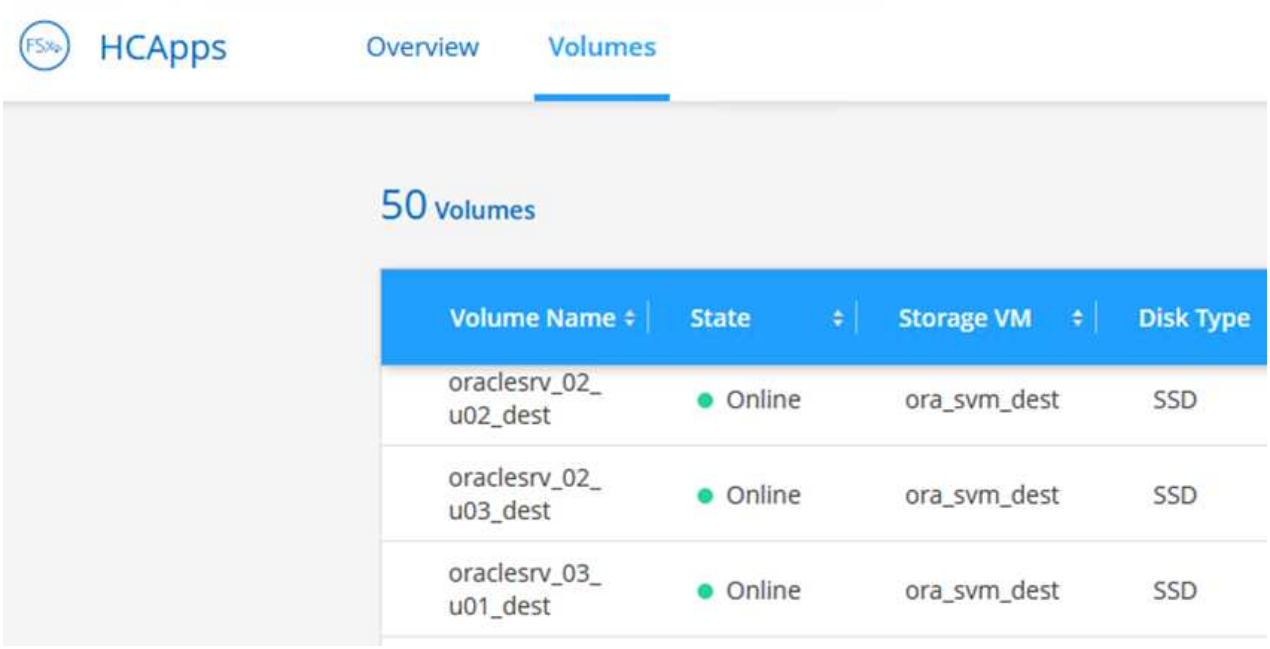
4. Ajoutez le nom du chemin de jonction et cliquez sur mettre à jour. Préciser cette Junction path lors du montage du volume NFS depuis le serveur Oracle.


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

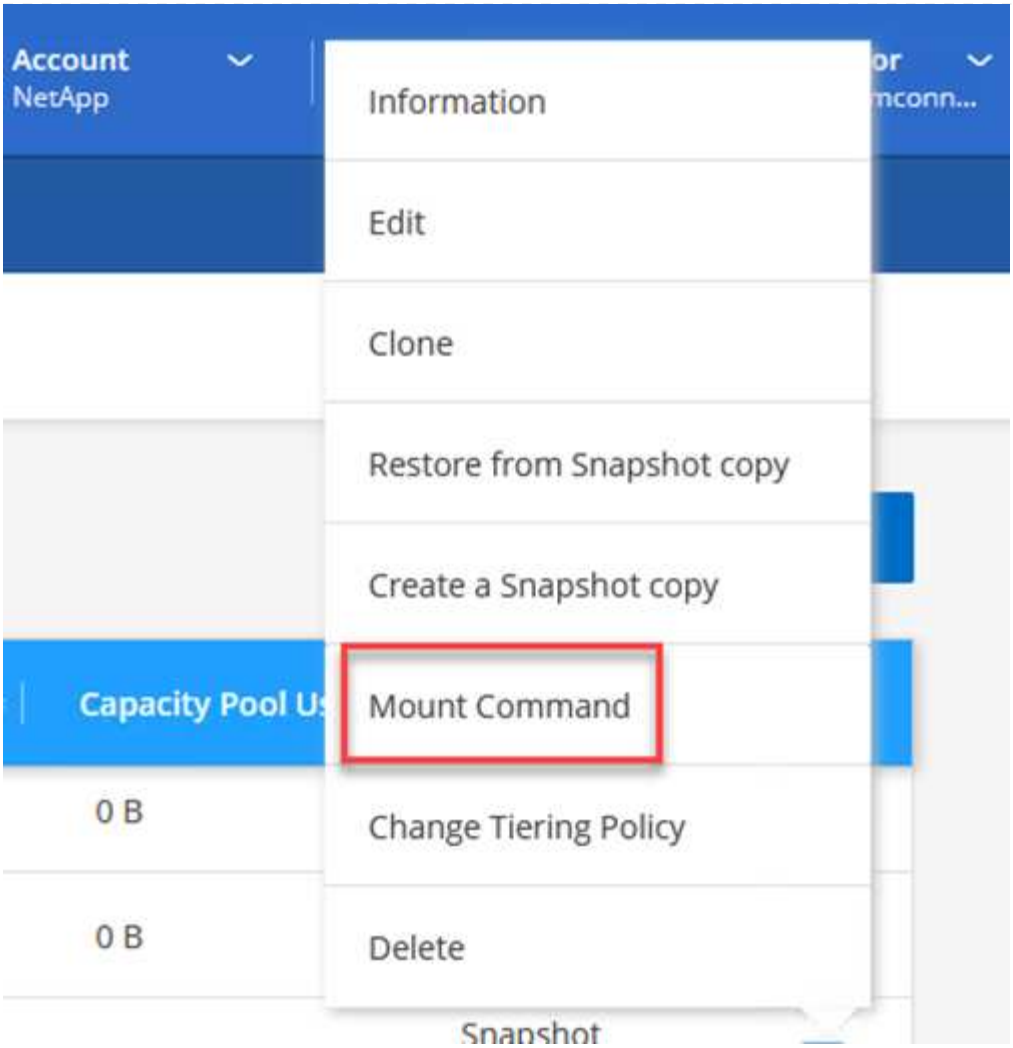
Montez les volumes NFS sur Oracle Server

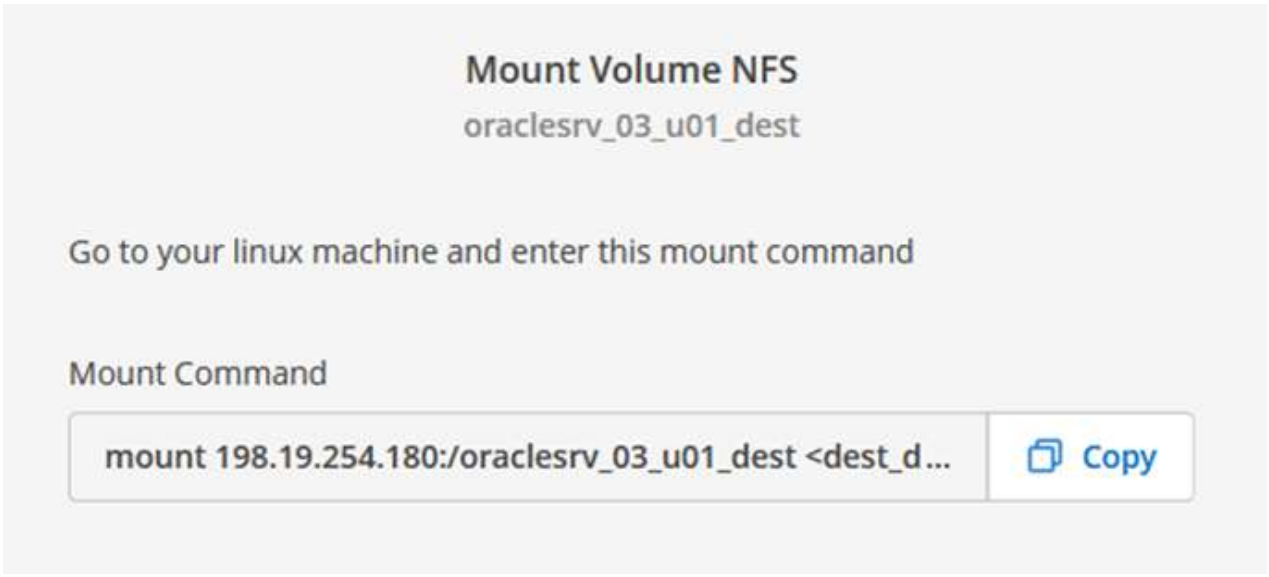
Dans Cloud Manager, vous pouvez obtenir la commande mount avec l'adresse IP correcte de la LIF NFS pour le montage des volumes NFS qui contiennent les fichiers et les journaux de la base de données Oracle.

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

Auteur : Josh Powell - Ingénierie de solutions NetApp

Présentation

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.

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

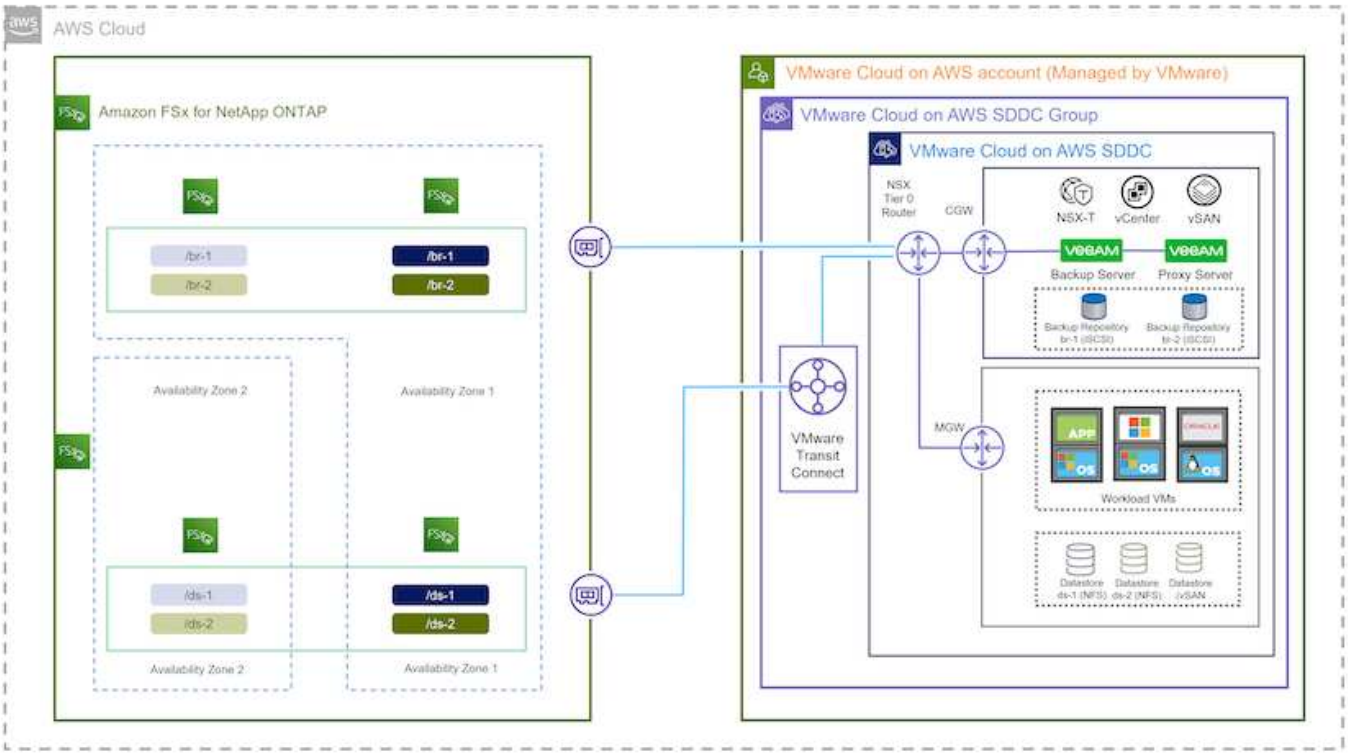
Prérequis

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.

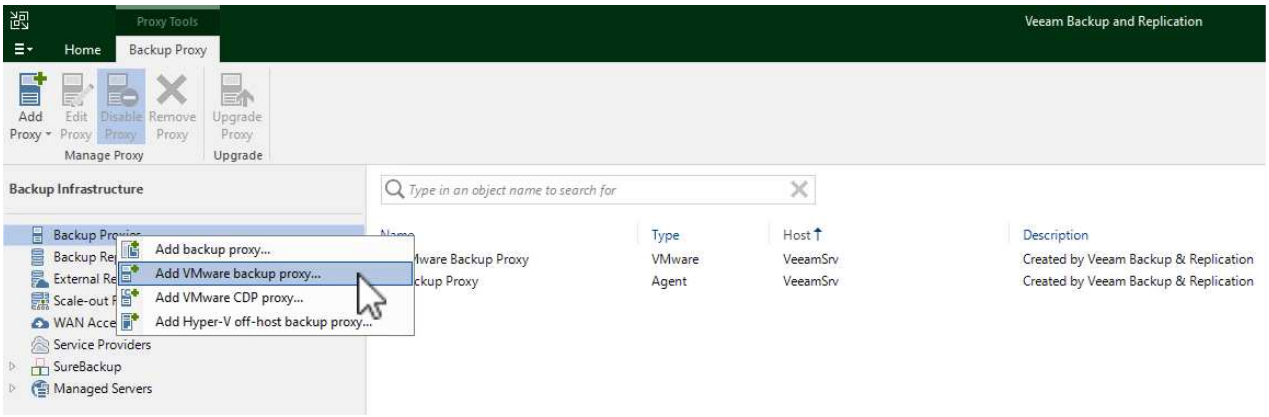
Pour plus d'informations sur les modes de transport, reportez-vous au "Guide de l'utilisateur Veeam Backup and Replication pour VMware vSphere".

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

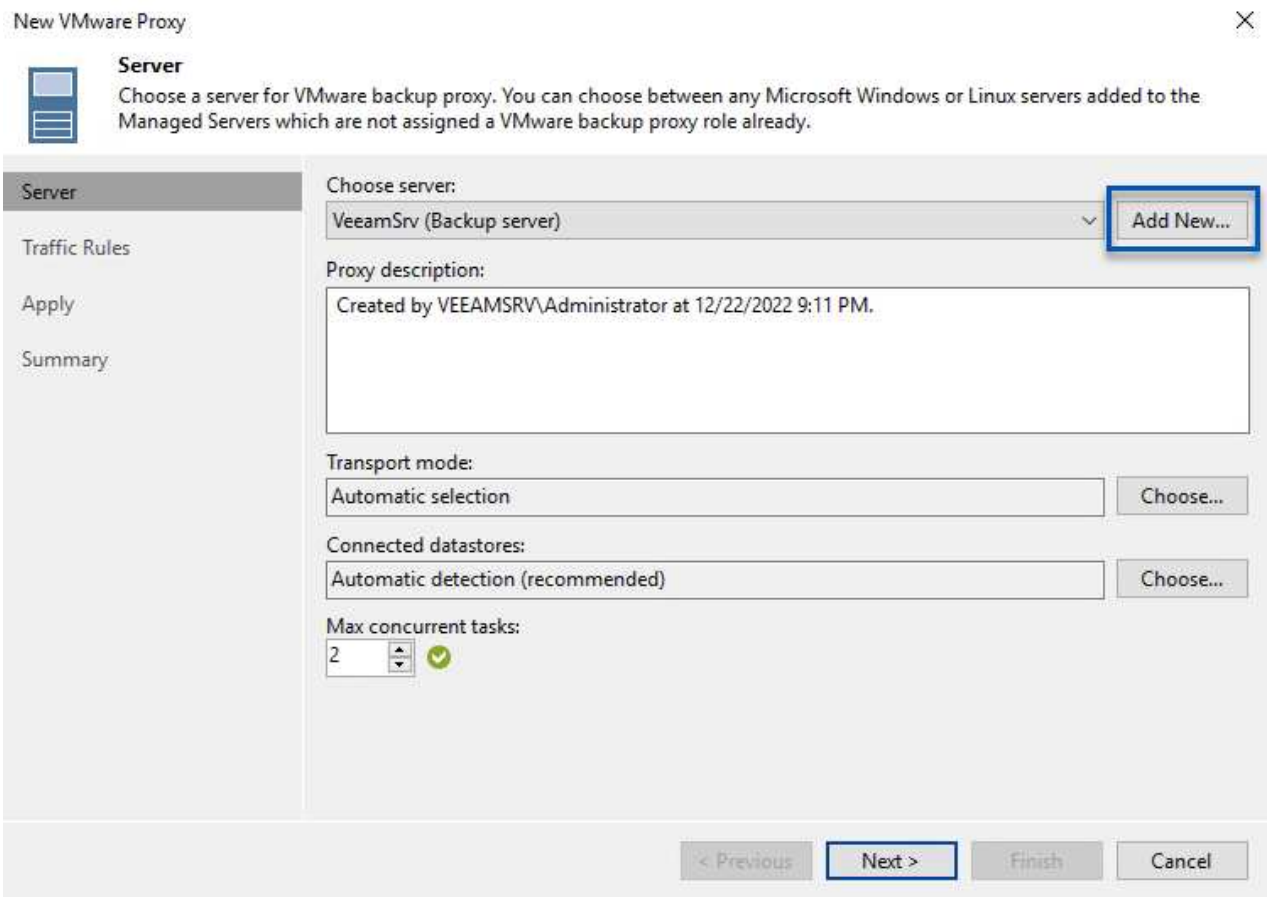
Déployez Veeam Proxy pour distribuer les workloads de sauvegarde

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.

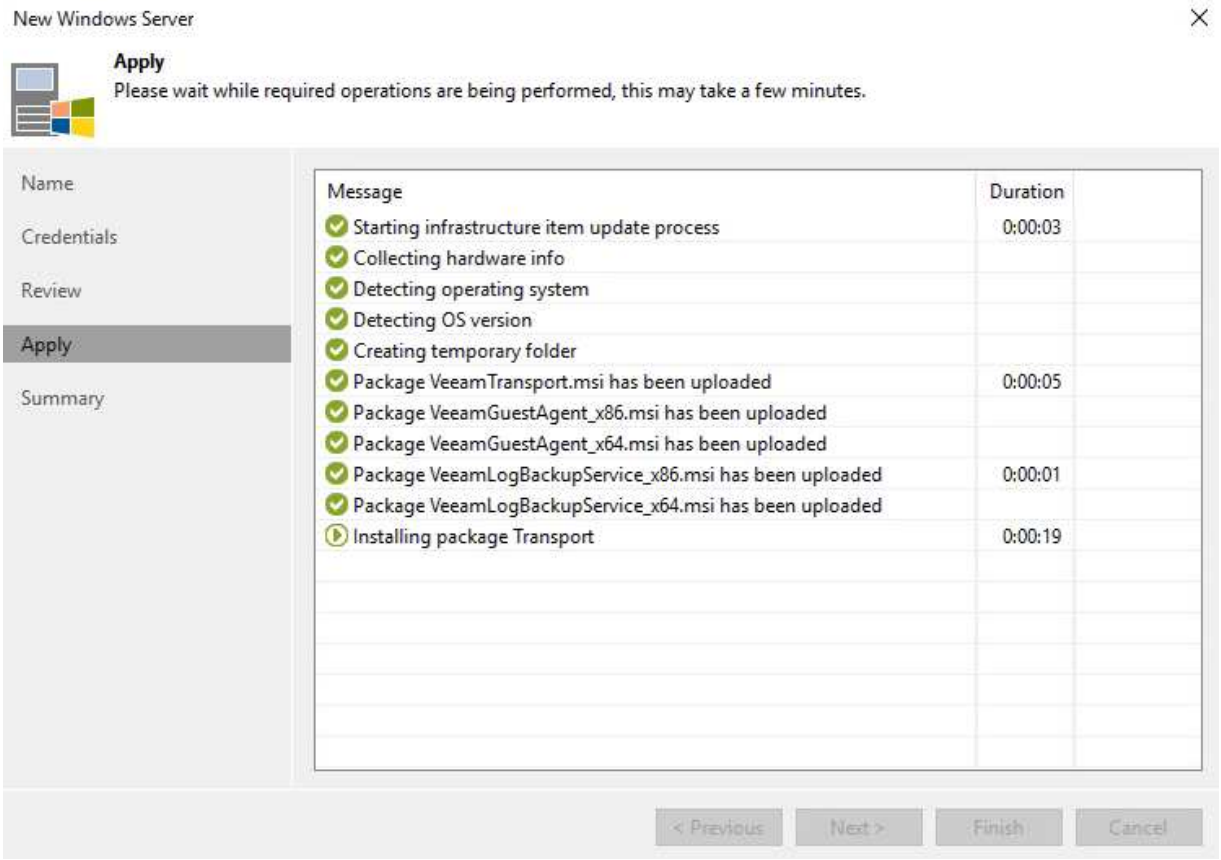
1. Sur le serveur Veeam Backup and Replication, ouvrez la console d'administration et sélectionnez **Backup Infrastructure** dans le menu inférieur gauche.
2. Cliquez avec le bouton droit de la souris sur **Backup Proxies** et cliquez sur **Ajouter un proxy de sauvegarde VMware…** pour ouvrir l'assistant.



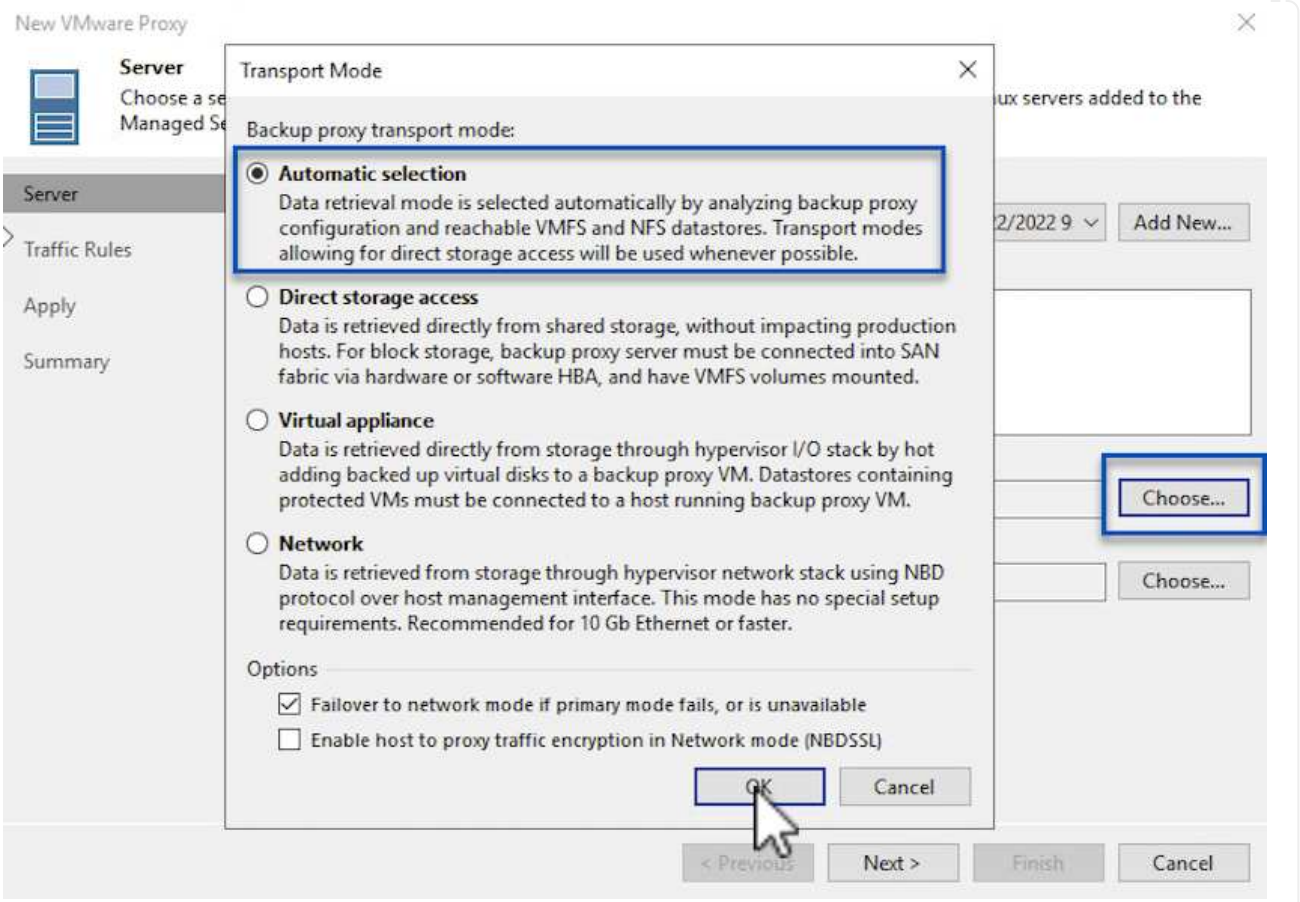
3. Dans l'assistant **Ajouter un proxy VMware**, cliquez sur le bouton **Ajouter un nouveau…** pour ajouter un nouveau serveur proxy.



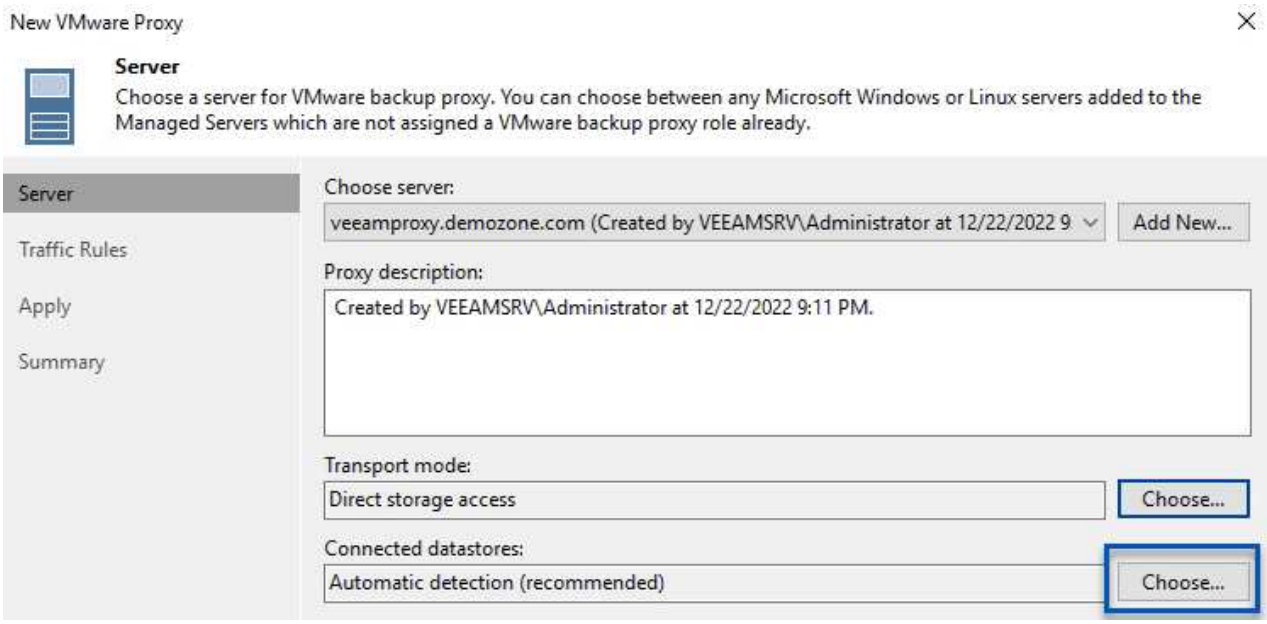
4. Sélectionnez pour ajouter Microsoft Windows et suivez les invites pour ajouter le serveur :
   - Indiquez le nom DNS ou l'adresse IP
   - Sélectionnez un compte à utiliser pour les informations d'identification sur le nouveau système ou ajoutez de nouvelles informations d'identification
   - Vérifiez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

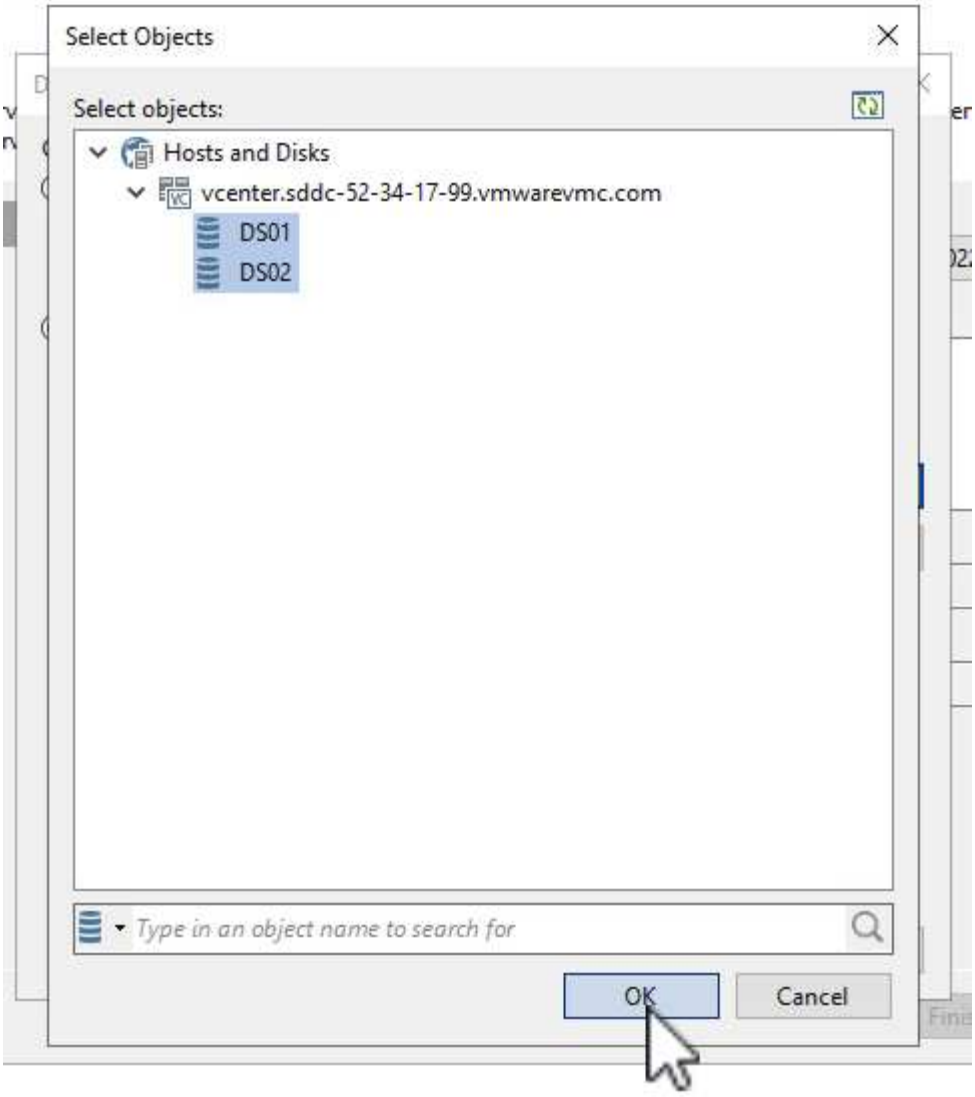


5. De retour dans l'assistant **Nouveau proxy VMware**, choisissez un mode de transport. Dans notre cas, nous avons choisi **sélection automatique**.

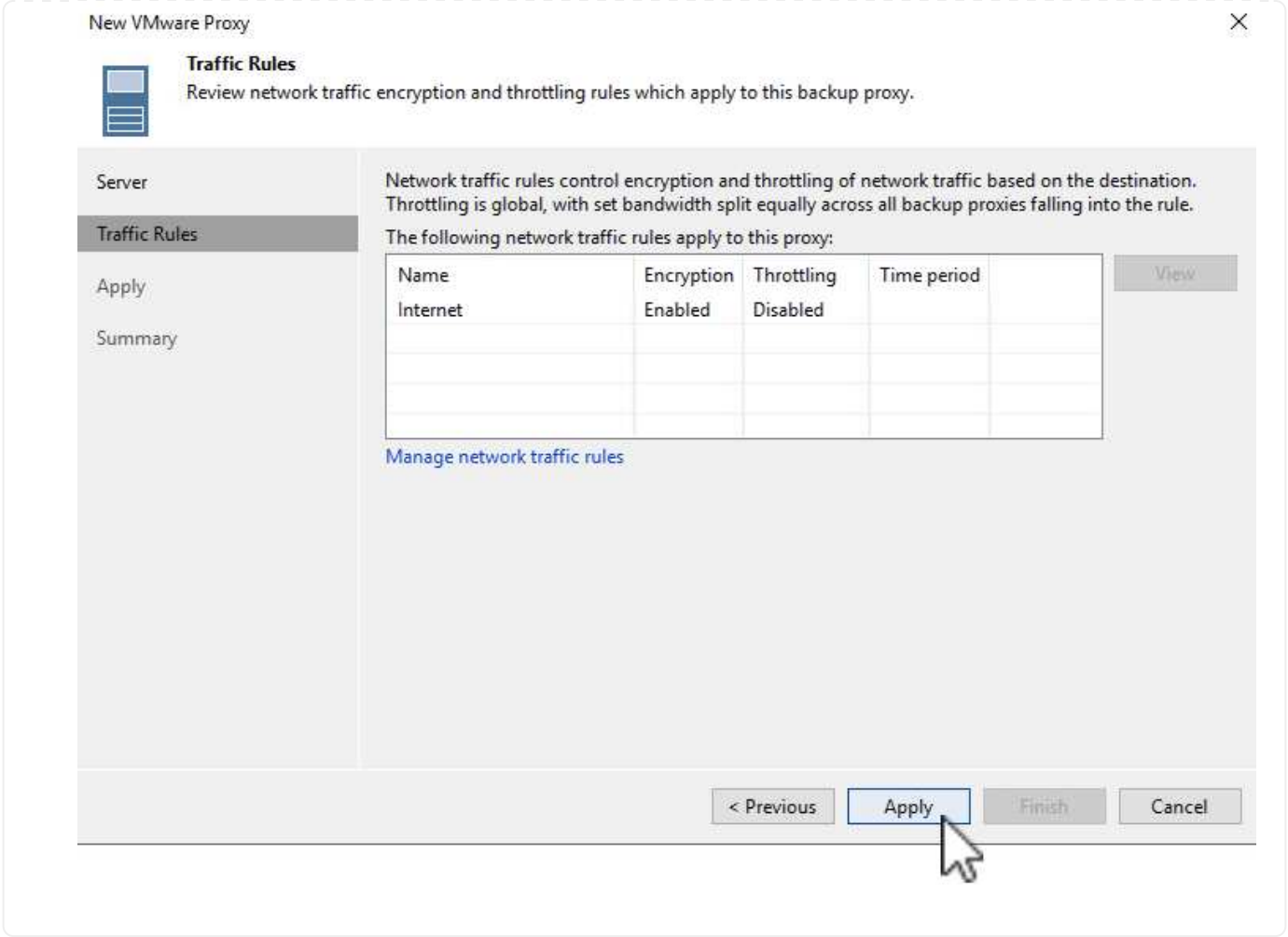


6. Sélectionnez les datastores connectés auxquels vous souhaitez que le proxy VMware dispose d'un accès direct.





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.



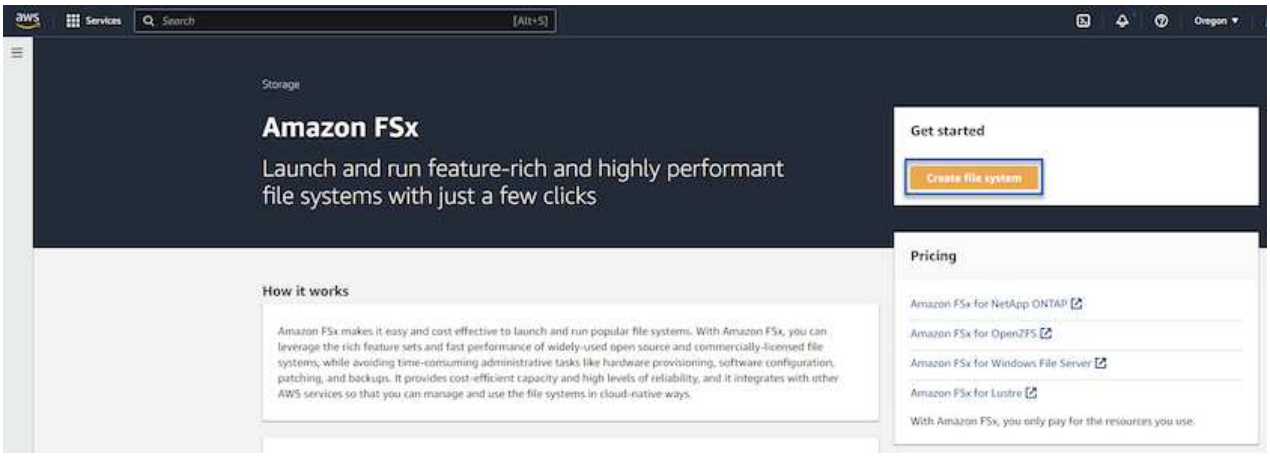
Configuration des référentiels de stockage et de sauvegarde

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

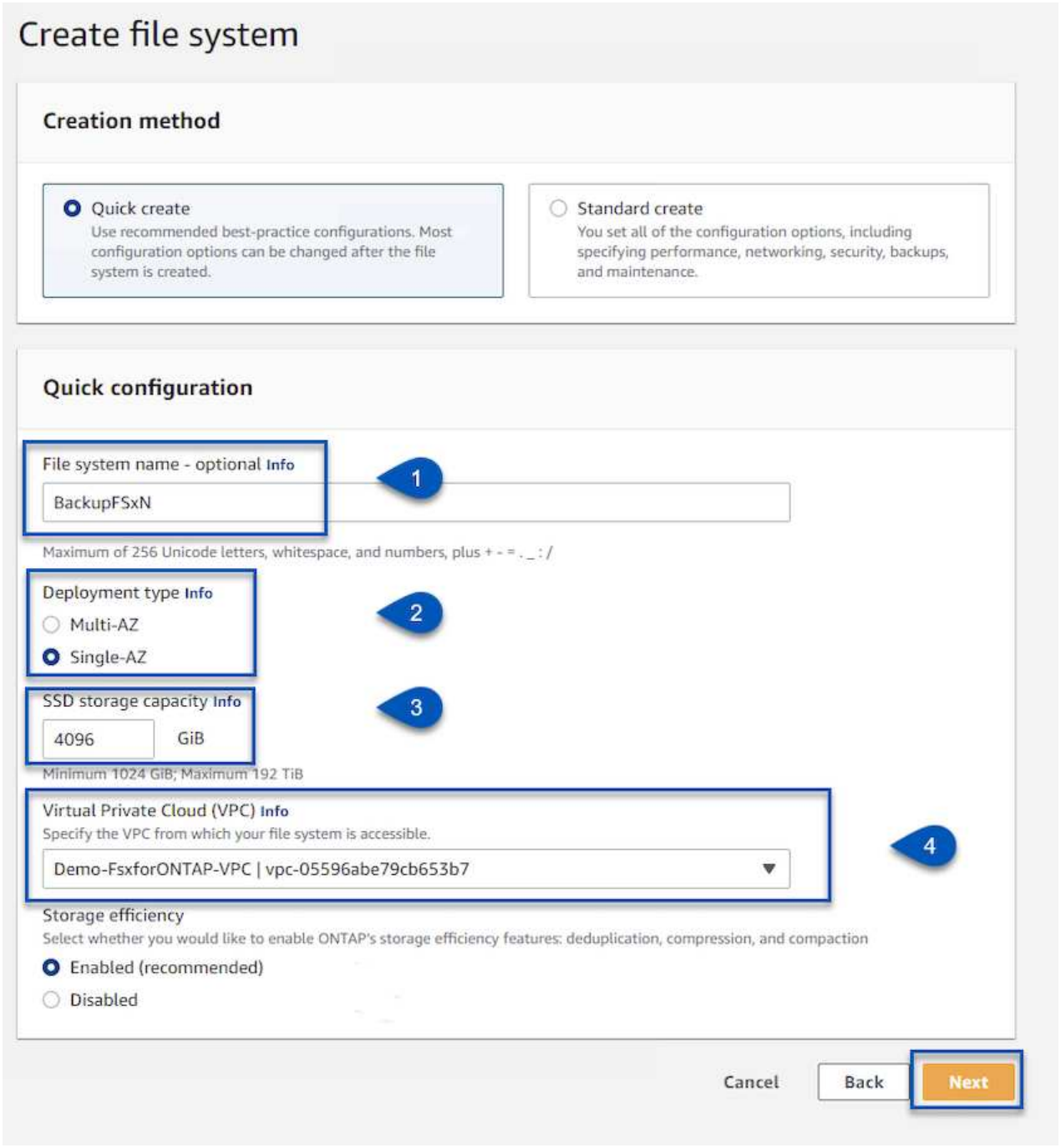
Créez un système de fichiers FSX pour ONTAP qui sera utilisé pour héberger les volumes iSCSI des référentiels de sauvegarde Veeam.

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 :

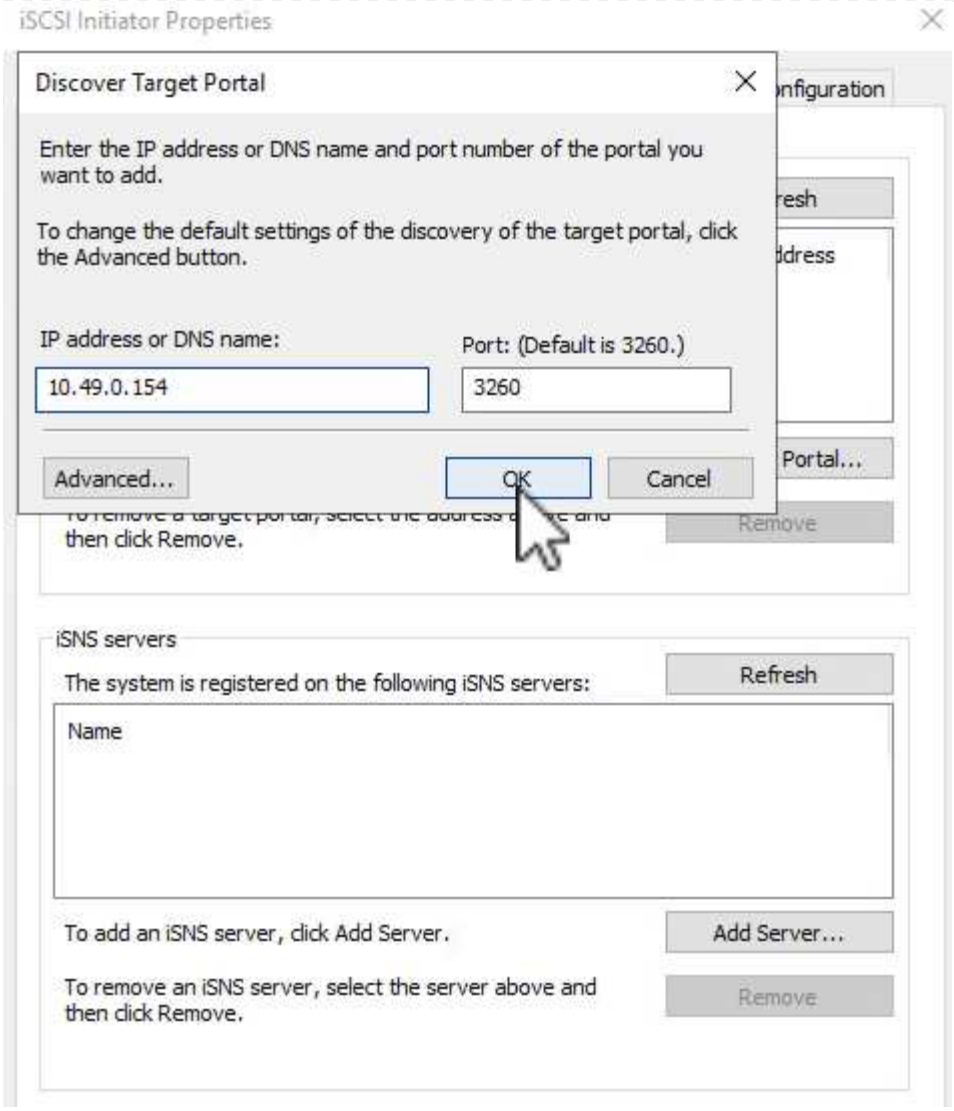
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

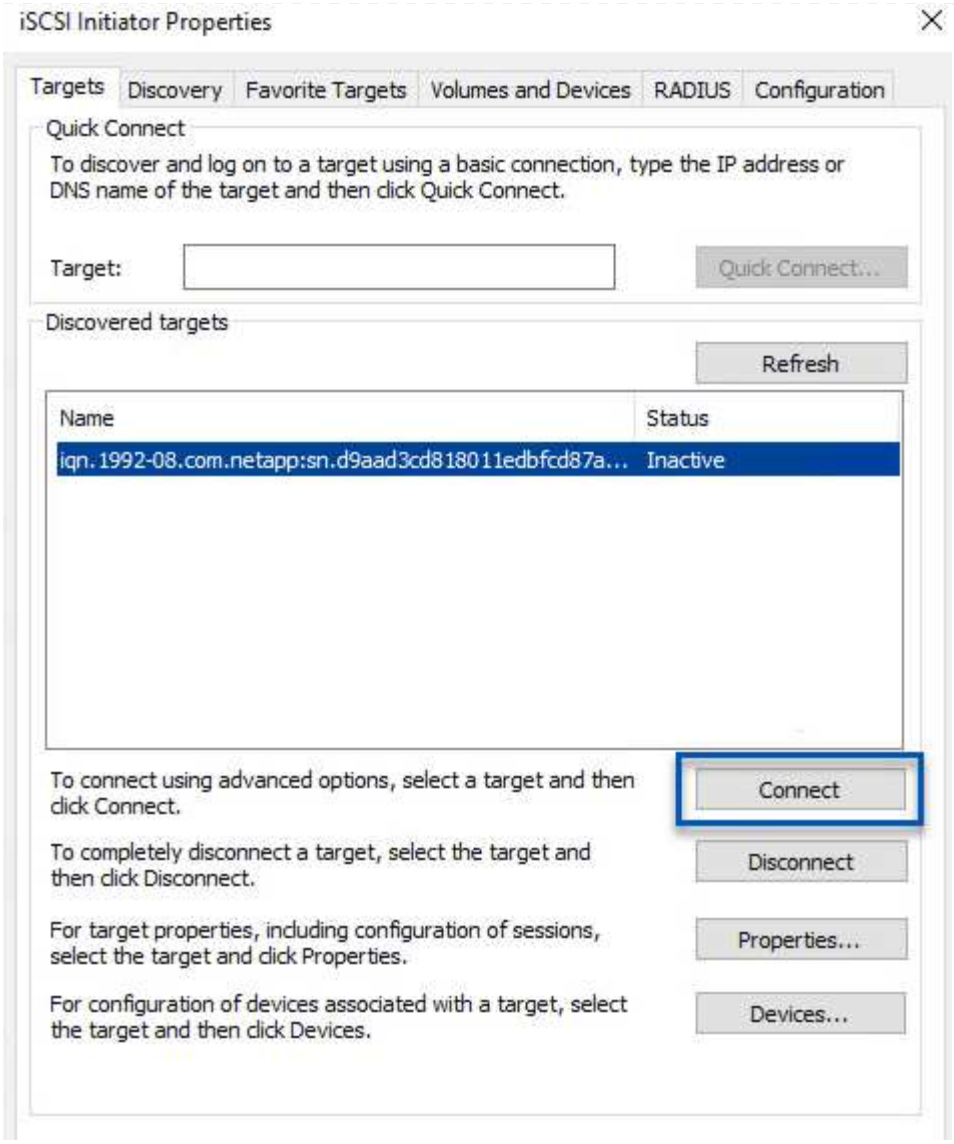
4. Enfin, mappez les LUN sur le groupe initiateur que vous venez de créer :

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

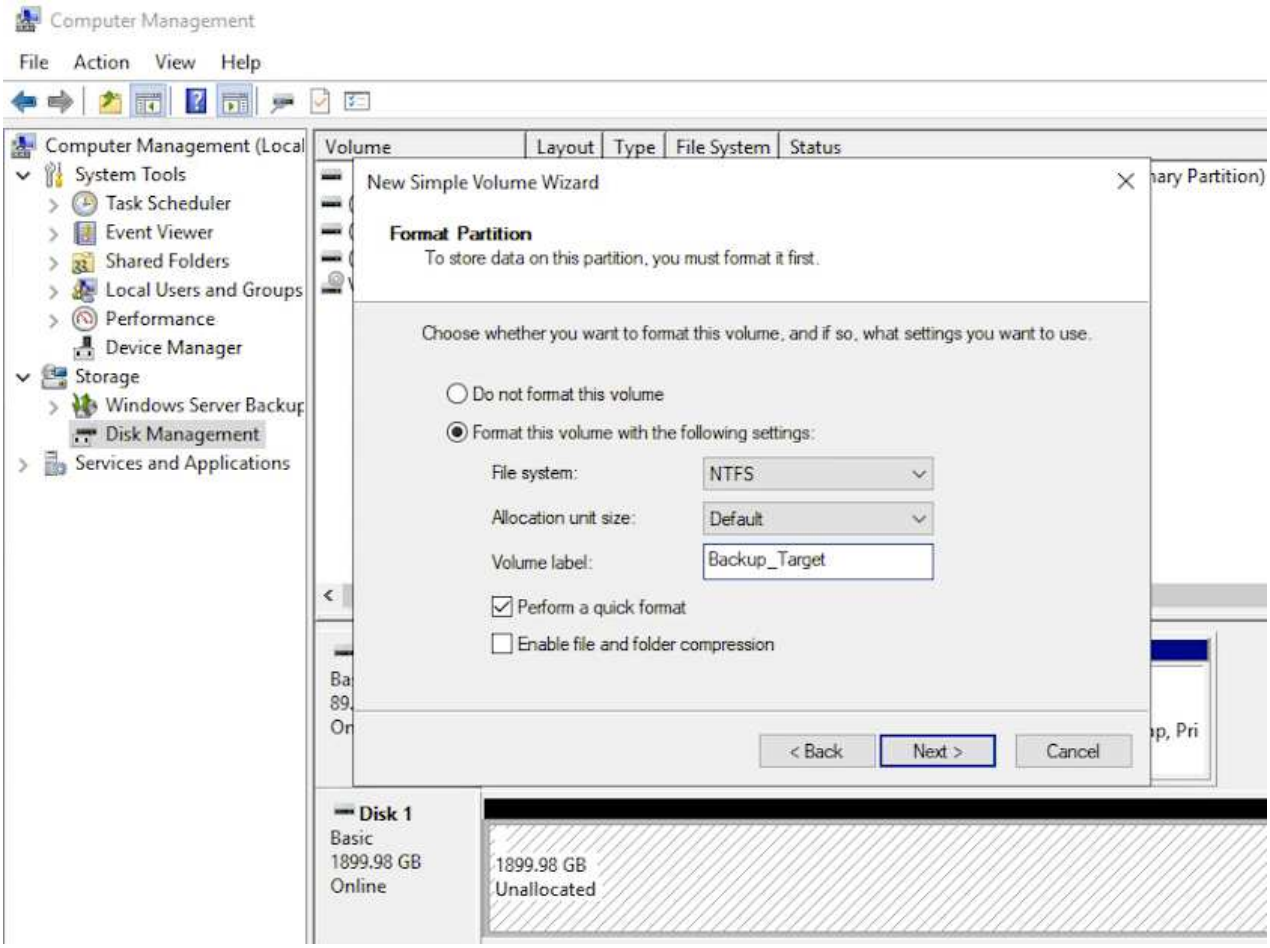
5. Pour monter les LUN iSCSI, connectez-vous à Veeam Backup & Replication Server et ouvrez iSCSI Initiator Properties. Accédez à l'onglet **Discover** et entrez l'adresse IP de la cible iSCSI.



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.

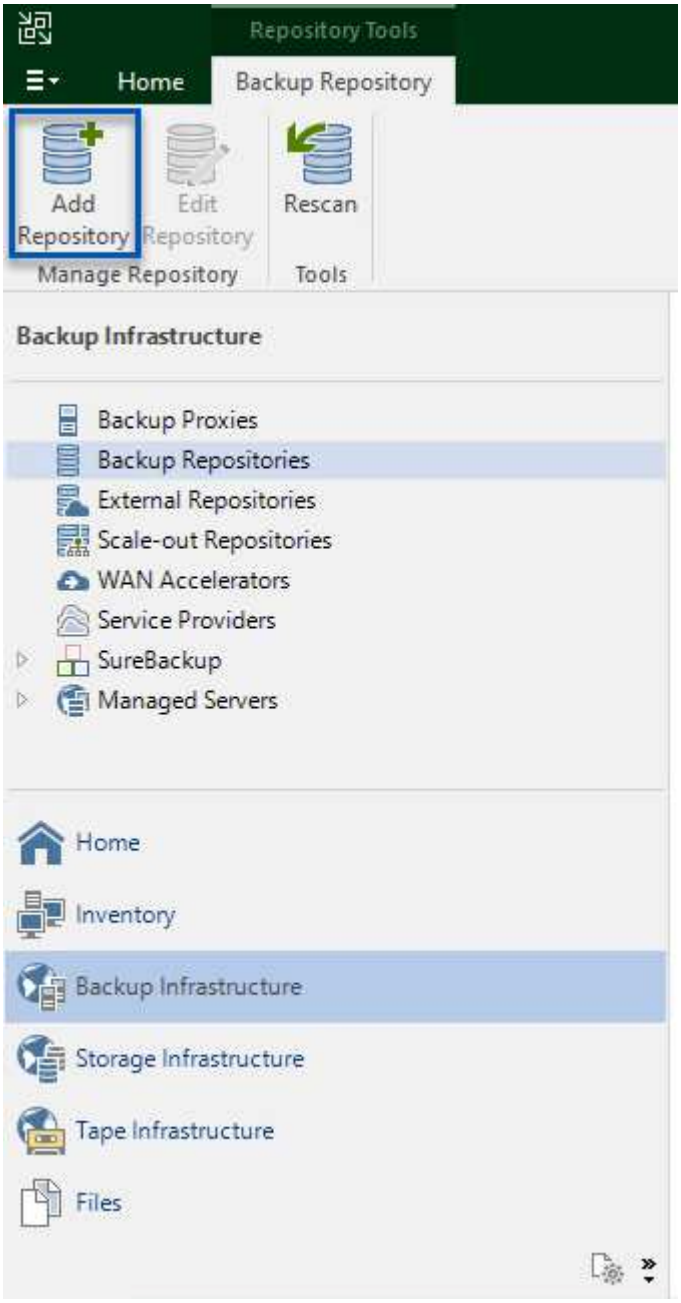


8. Répétez ces étapes pour monter les volumes iSCSI sur le serveur proxy Veeam.

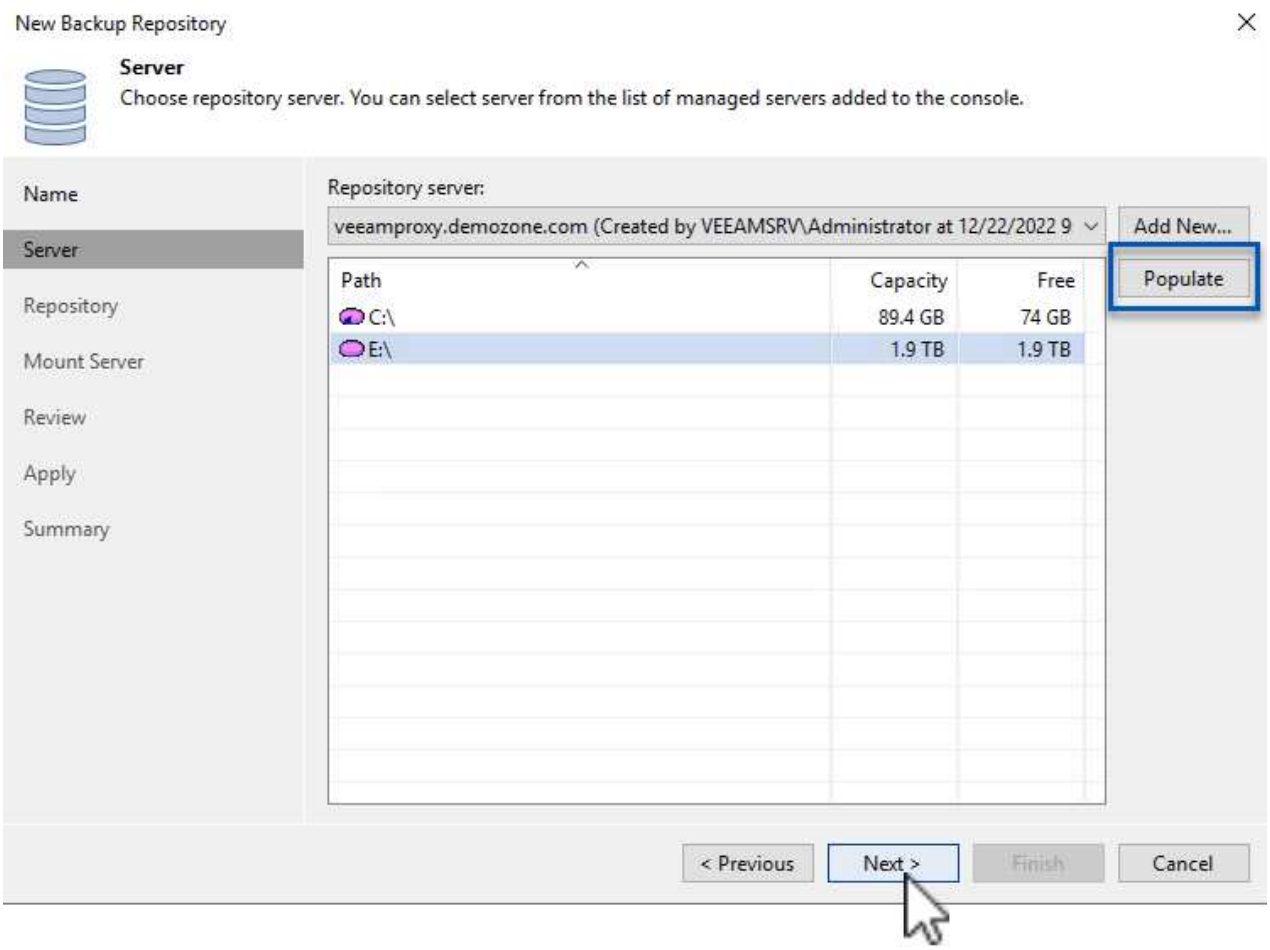
Création de référentiels de sauvegarde Veeam

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.

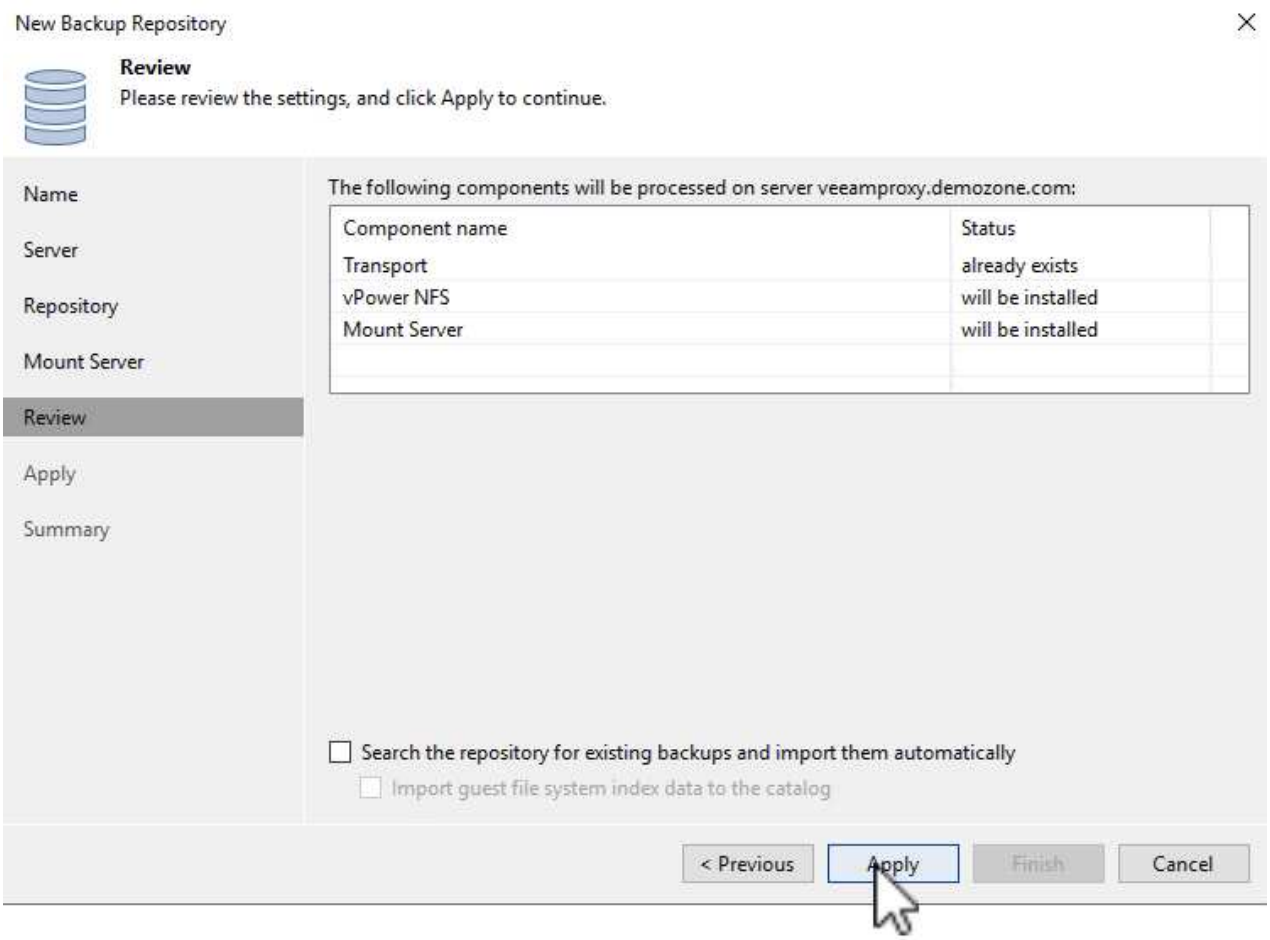
1. Dans la console de sauvegarde et de réplication Veeam, cliquez sur **Backup Infrastructure** en bas à gauche, puis sélectionnez **Add Repository**



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

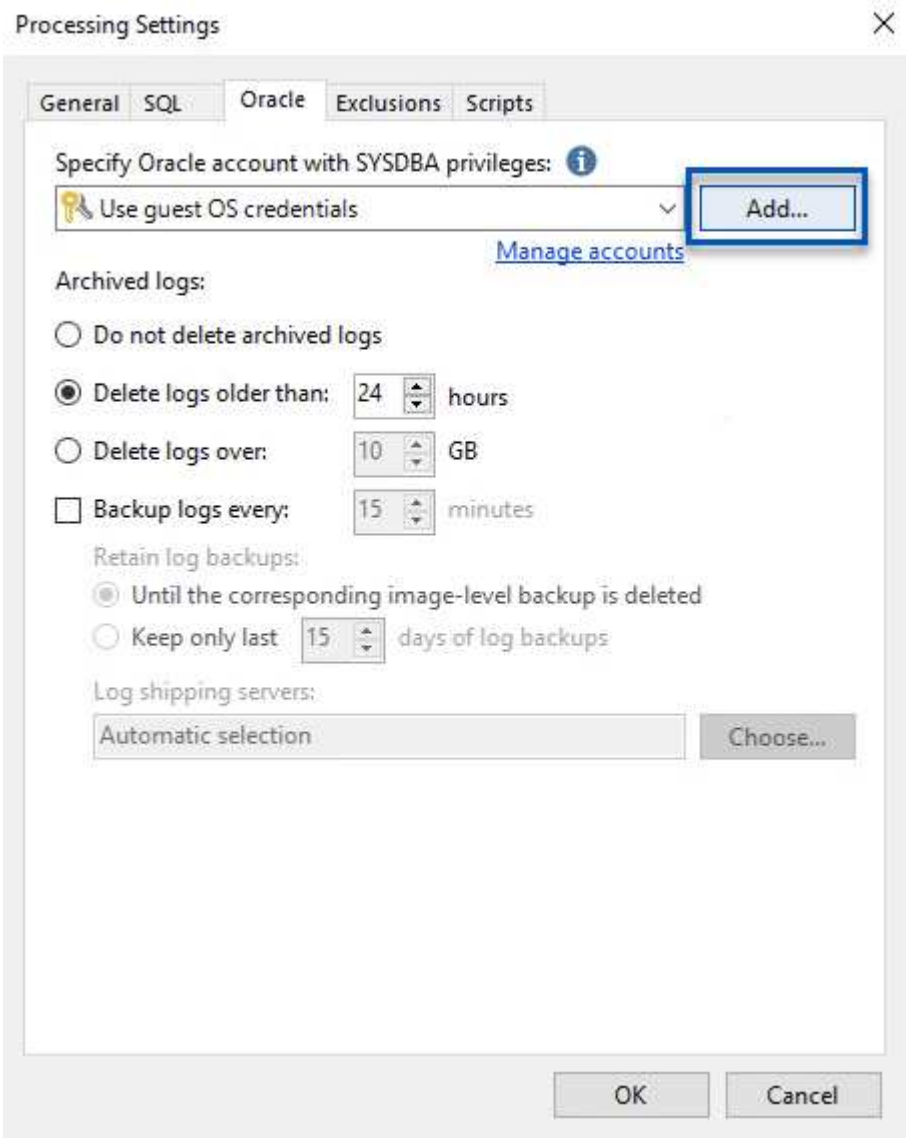
Les tâches de sauvegarde doivent être créées à l'aide des référentiels de sauvegarde de la section précédente. La création de tâches de sauvegarde fait partie intégrante du répertoire des administrateurs de stockage et ne couvre pas toutes les étapes. Pour plus d'informations sur la création de tâches 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 :

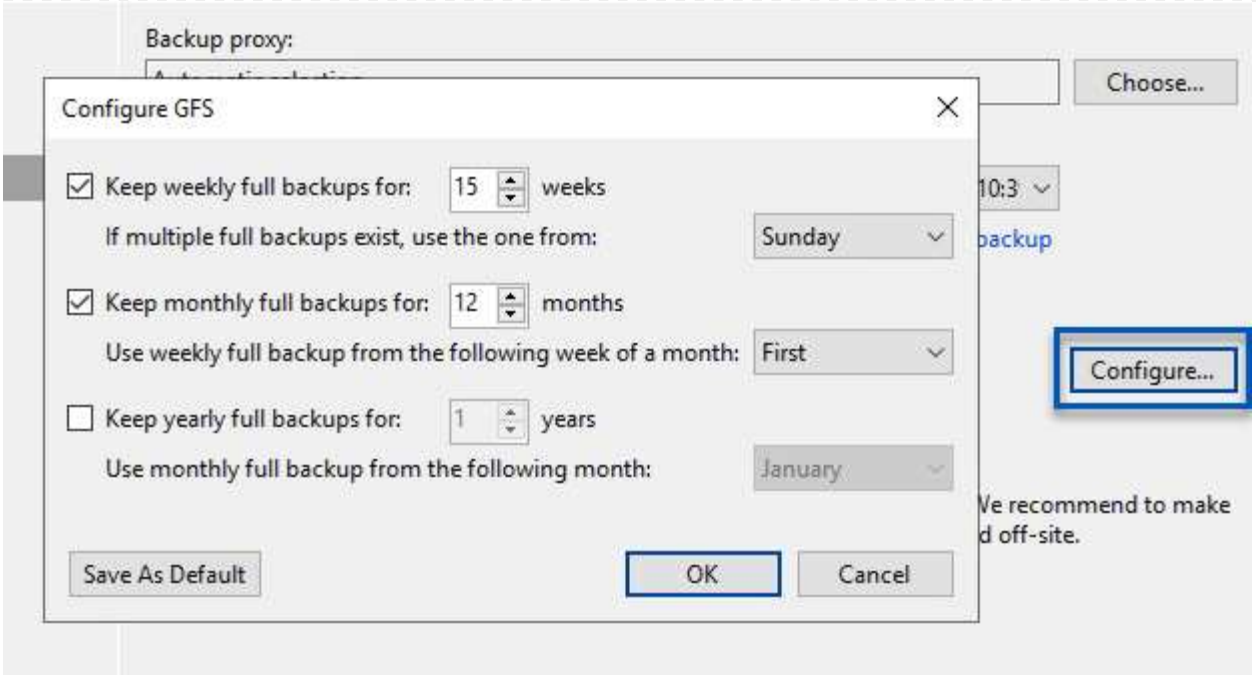
- Serveurs Microsoft Windows SQL Server
- Serveurs de base de données Oracle
- Serveurs de fichiers Windows
- Serveurs de fichiers Linux

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".

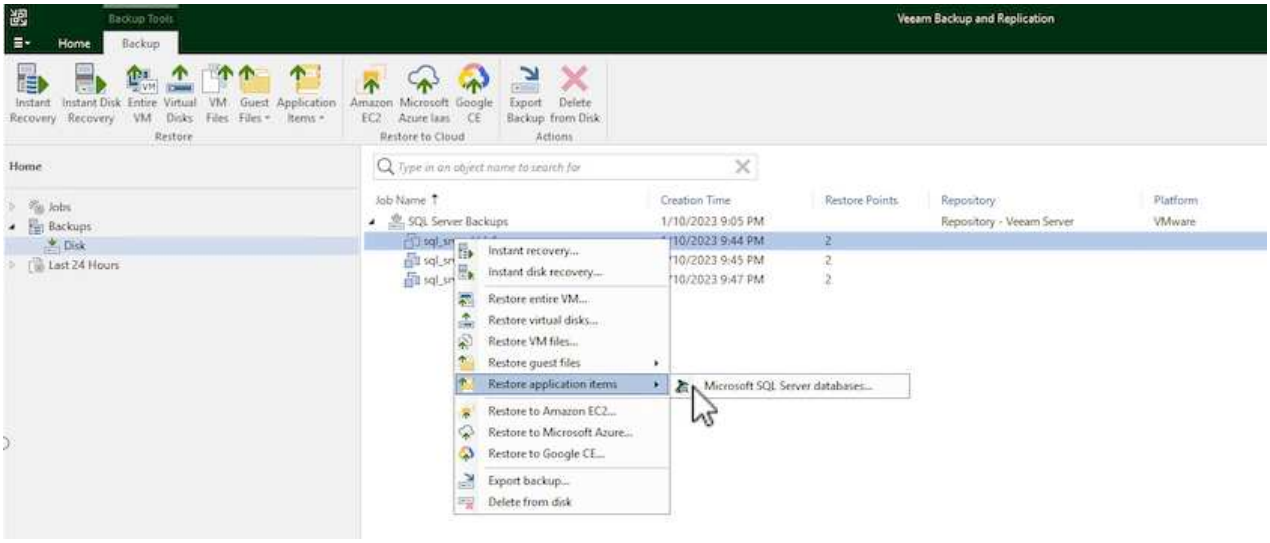
Restaurer les bases de données SQL Server

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 :

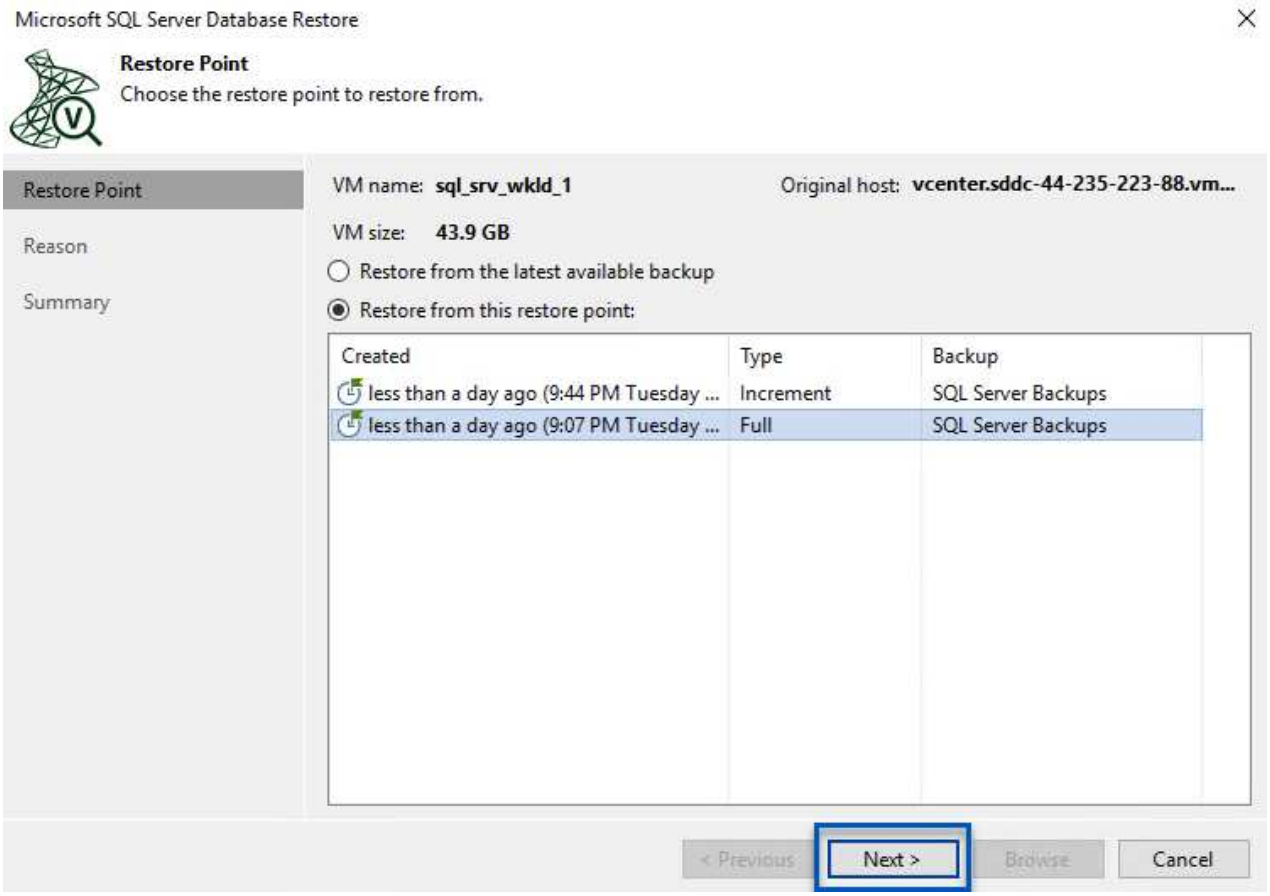
- Veeam Explorer **monte la sauvegarde** contenant la base de données SQL Server à restaurer.
- Le logiciel **publie la base de données** directement à partir des fichiers montés, ce qui la rend accessible en tant que base de données temporaire sur l'instance SQL Server cible.
- Pendant que la base de 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

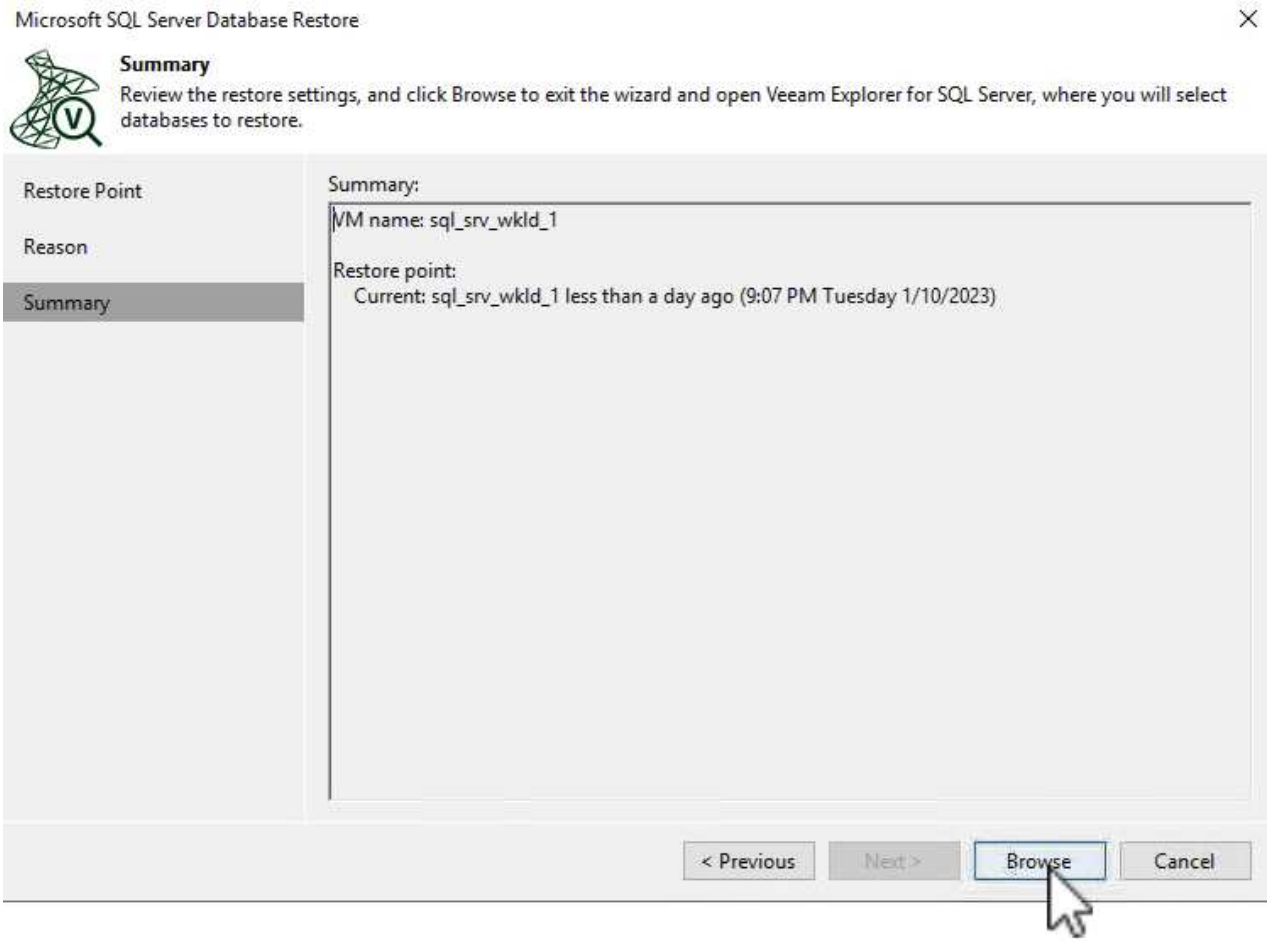
1. Dans la console Veeam Backup and Replication, naviguez jusqu'à la liste des sauvegardes SQL Server, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments d'application**, puis **bases de données Microsoft SQL Server…**.



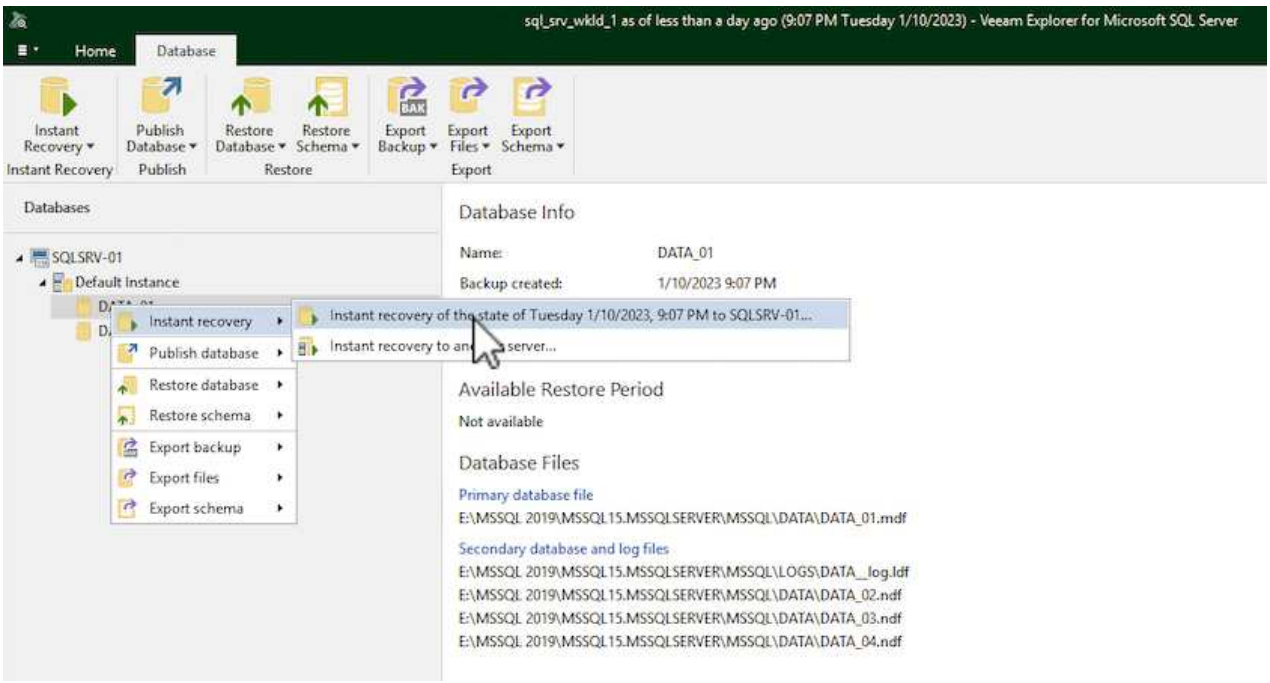
2. Dans l'Assistant de restauration de base de données Microsoft SQL Server, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.



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.

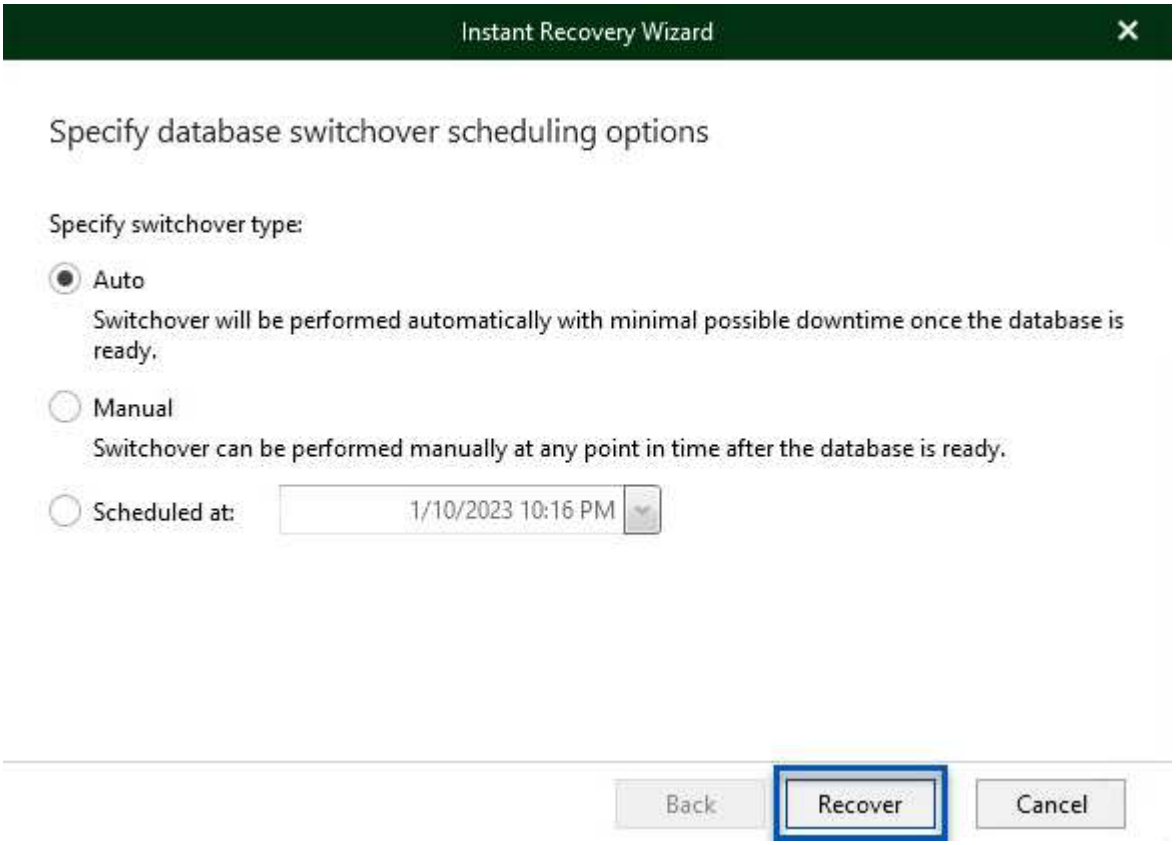


4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez avec le bouton droit de la souris et sélectionnez **Instant Recovery**, puis le point de restauration spécifique vers lequel effectuer la restauration.

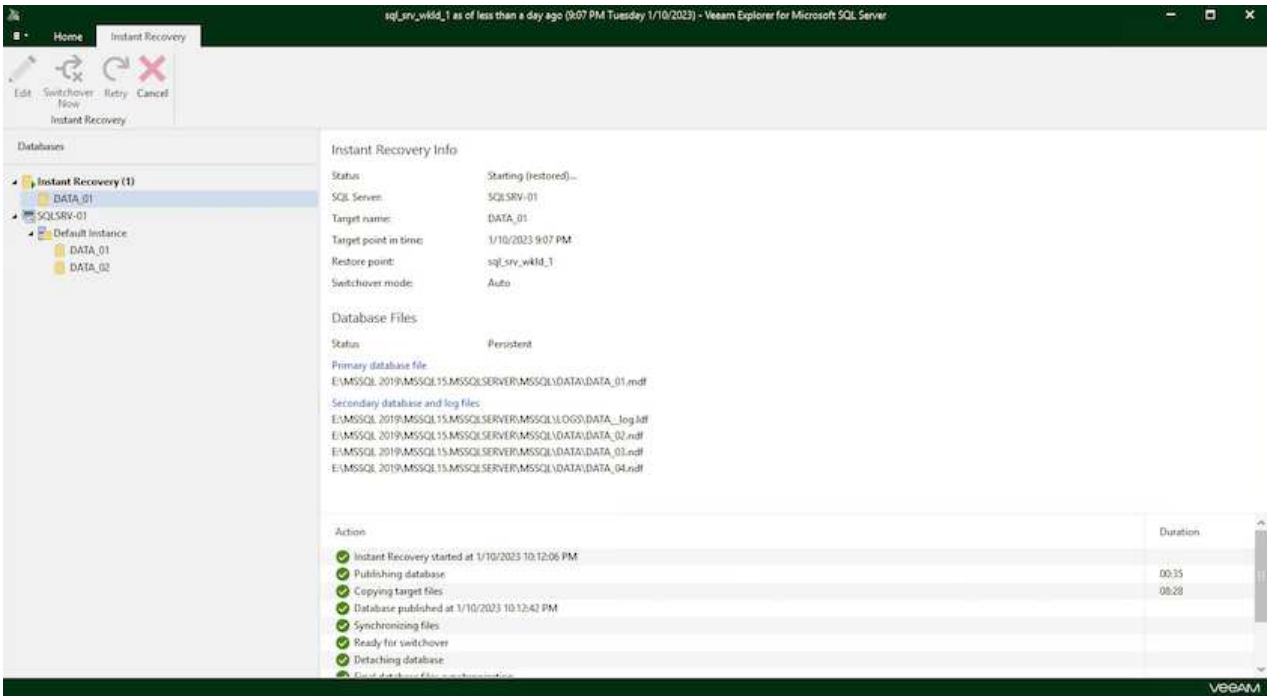


5. Dans l'Assistant de récupération instantanée, spécifiez le type de basculement. Ce processus peut être automatique avec un temps d'arrêt minimal, manuellement ou à un moment donné. Cliquez

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

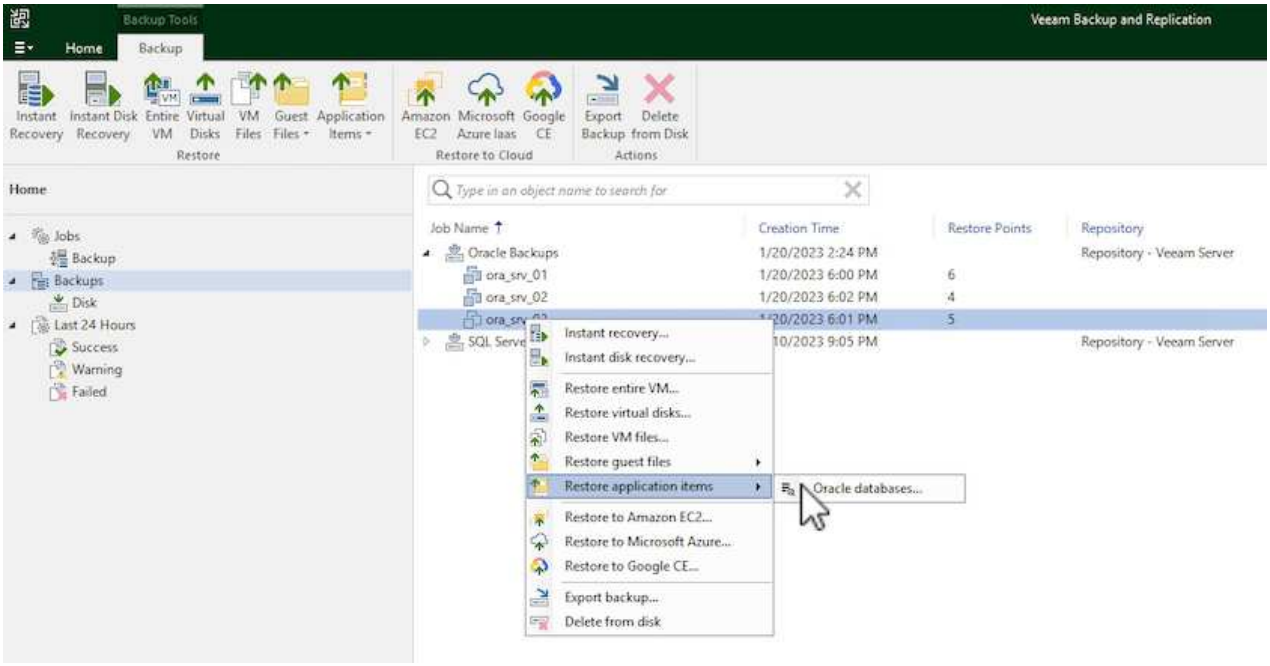
Veeam Explorer for Oracle Database offre la possibilité d'effectuer une restauration standard de base de données Oracle ou une restauration ininterrompue à l'aide d'Instant Recovery. Il prend également en charge les bases de données de publication pour un accès et une restauration rapides des bases de 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".

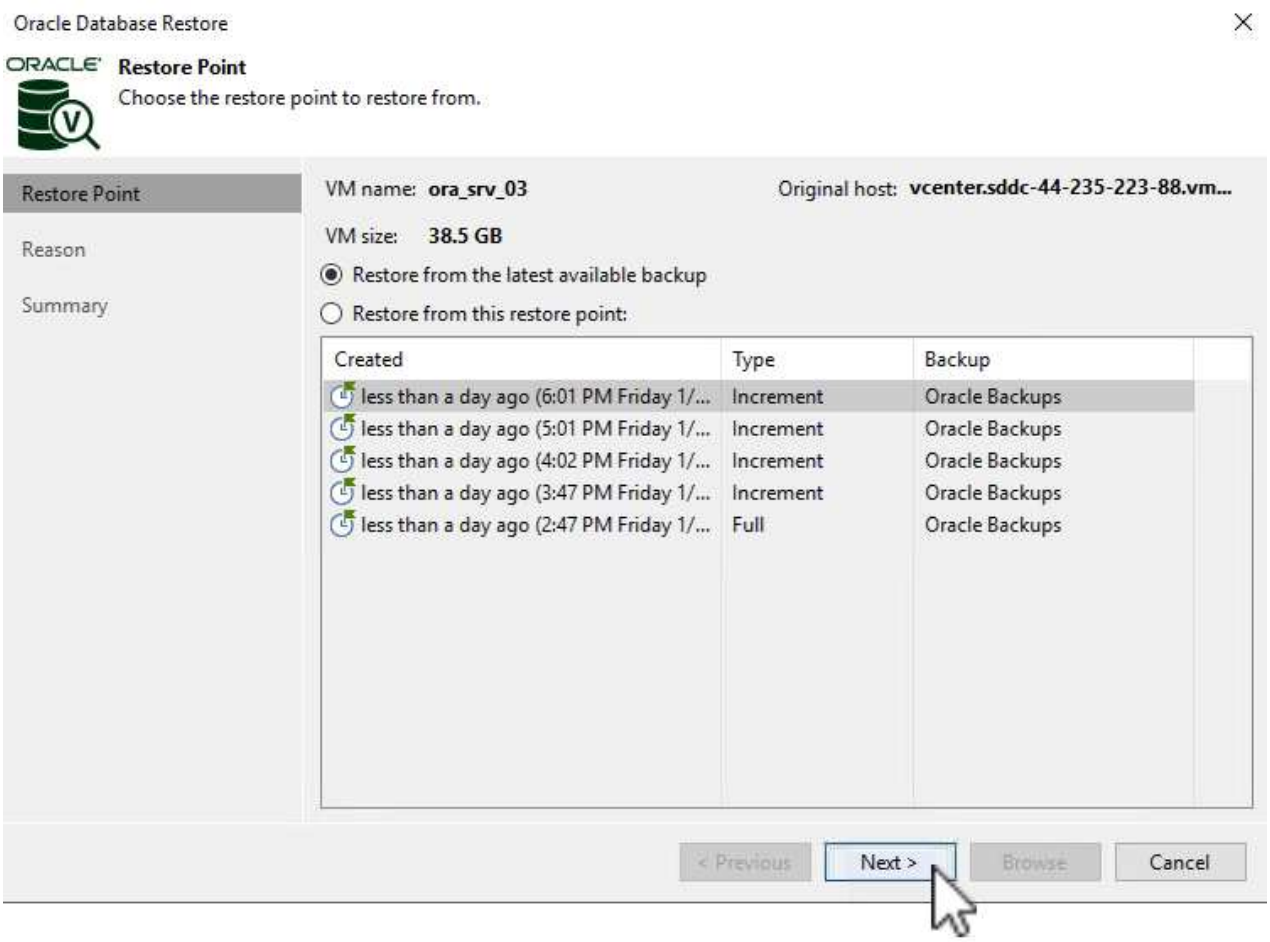
Restaurez la base de données Oracle avec Veeam Explorer

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

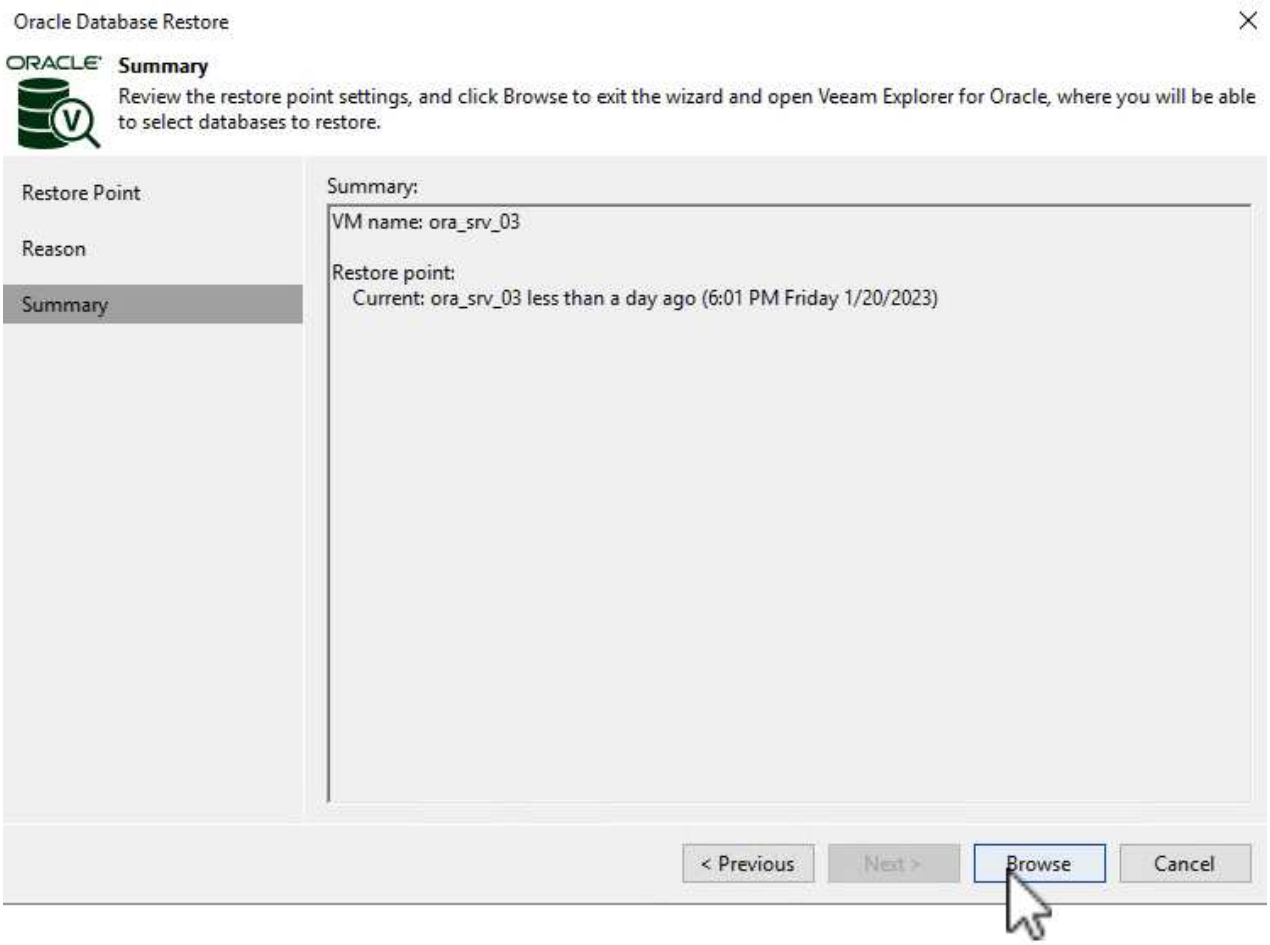
1. Dans la console Veeam Backup and Replication, naviguez jusqu'à la liste des sauvegardes Oracle, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments de l'application**, puis **bases de données Oracle…**.



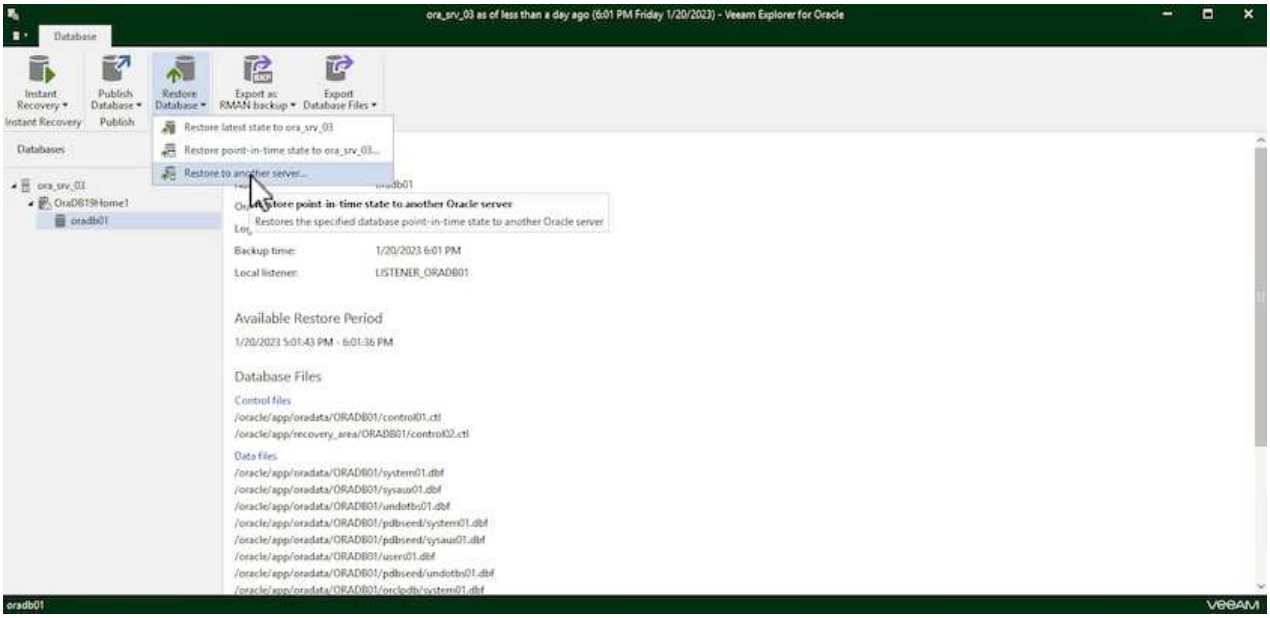
2. Dans l'assistant de restauration de la base de données Oracle, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.



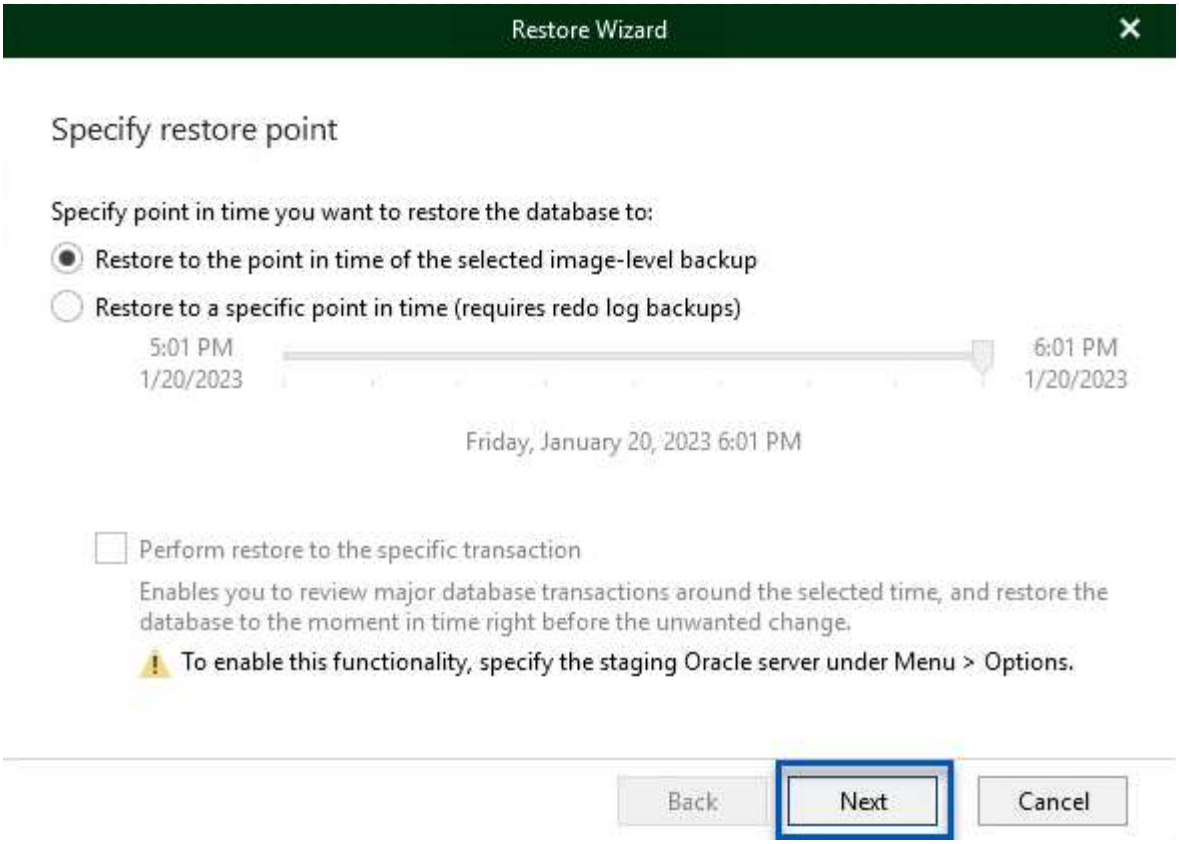
3. Entrez un **motif de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer for Oracle.



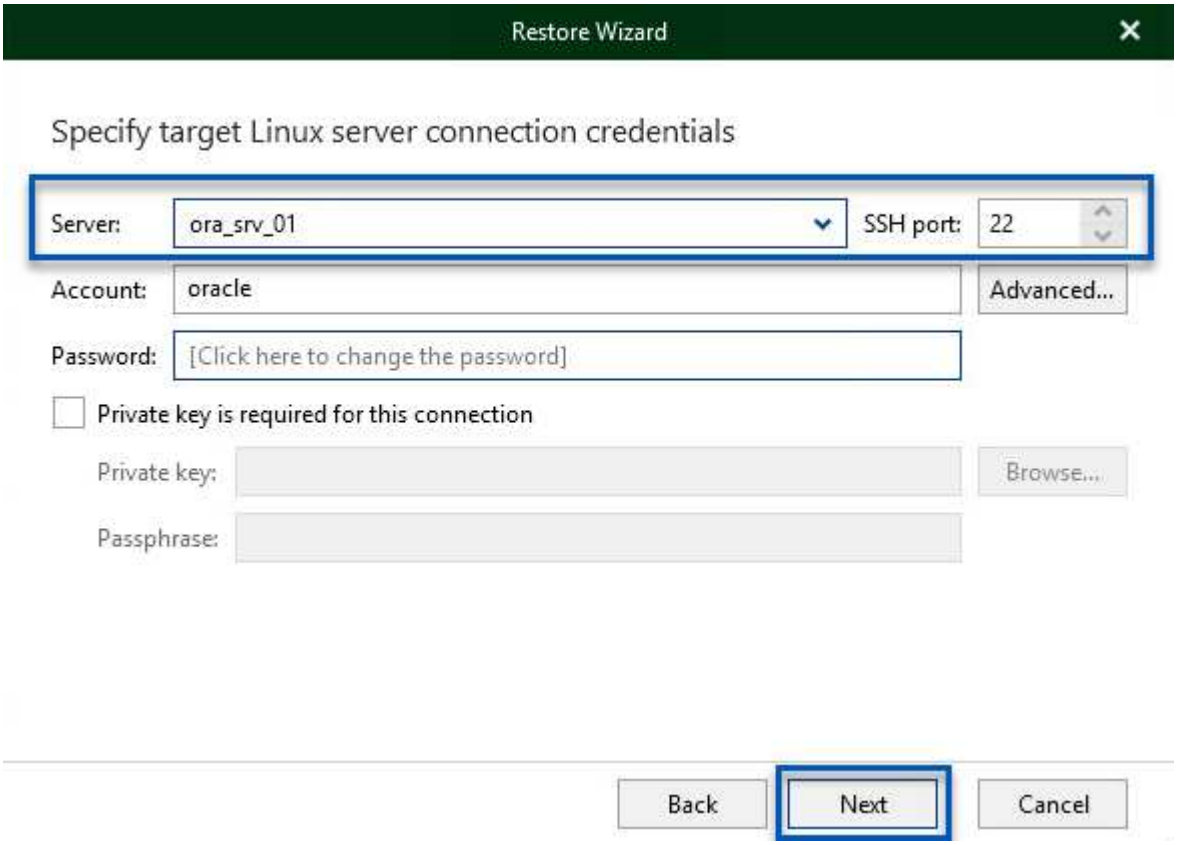
4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez sur la base de données à restaurer, puis dans le menu déroulant **Restaurer la base de données** en haut, sélectionnez **Restaurer sur un autre serveur…**.



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

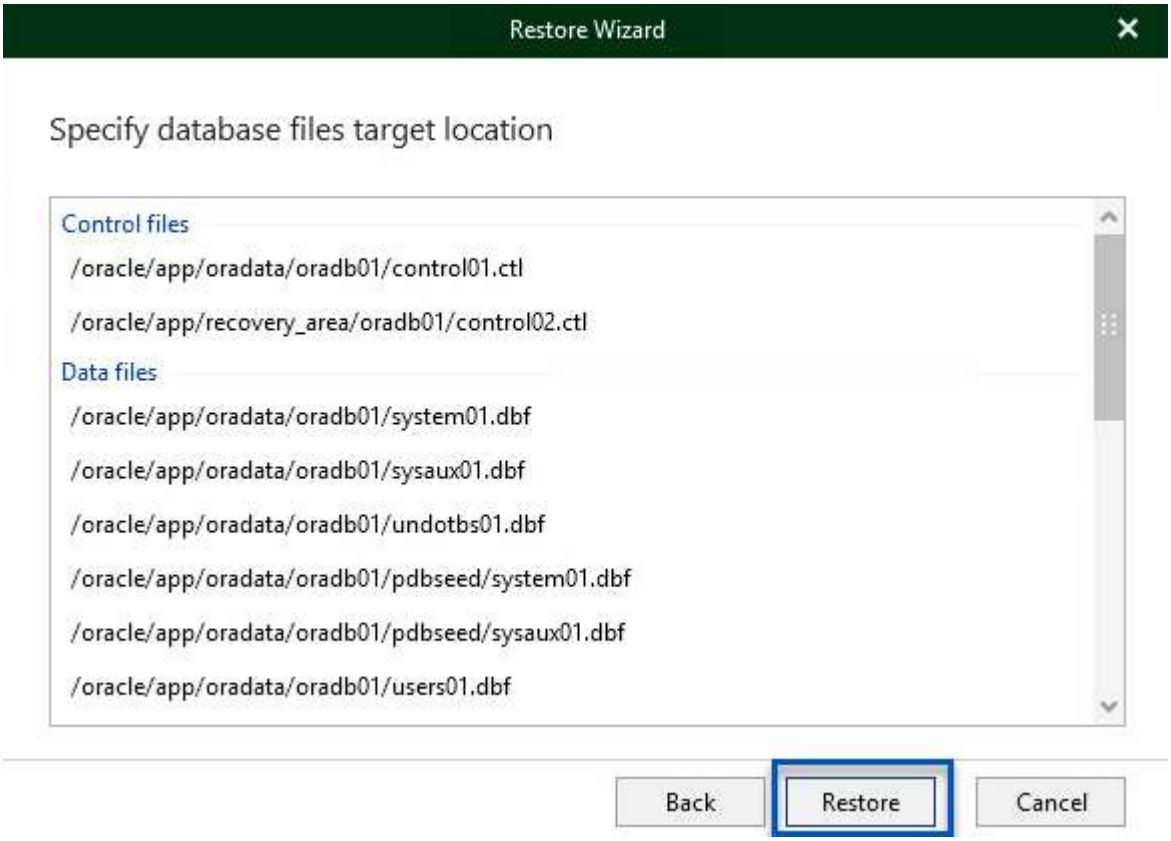


6. Spécifiez le serveur cible vers lequel la base de données sera restaurée et les informations d'identification du compte, puis cliquez sur **Suivant**.



7. Enfin, spécifiez l'emplacement cible des fichiers de base de données et cliquez sur le bouton

Restaurer pour lancer le processus de restauration.

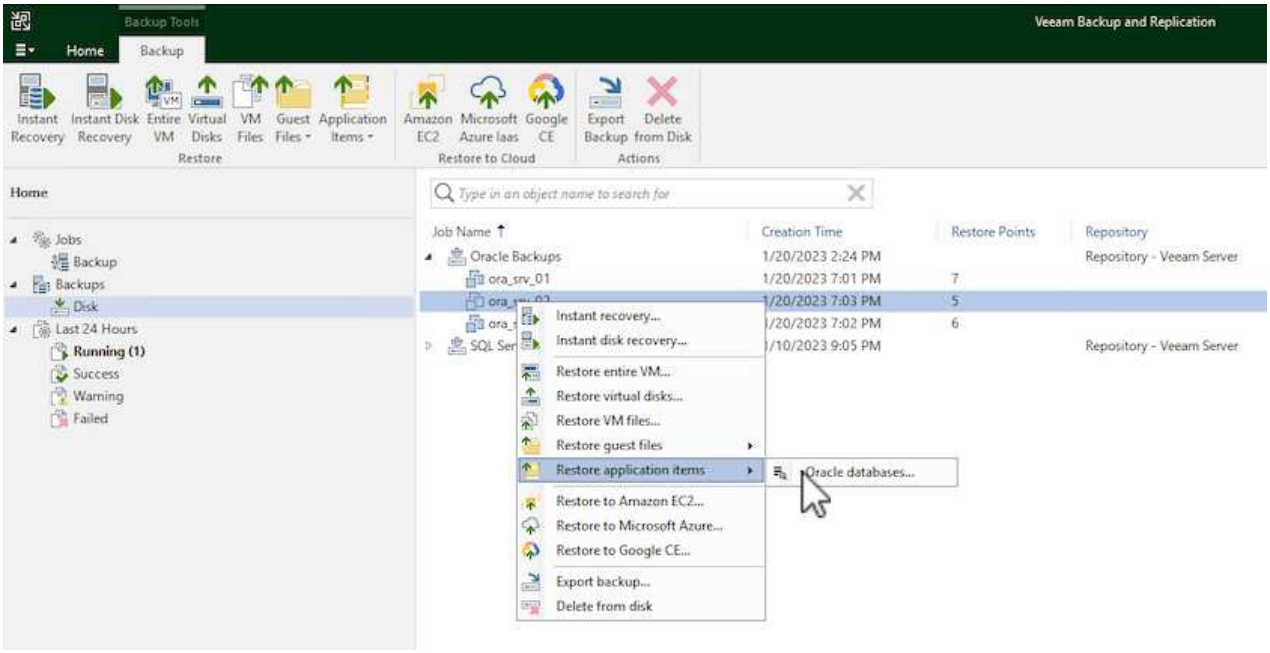


8. Une fois la restauration de la base de données terminée, vérifiez que la base de données Oracle démarre correctement sur le serveur.

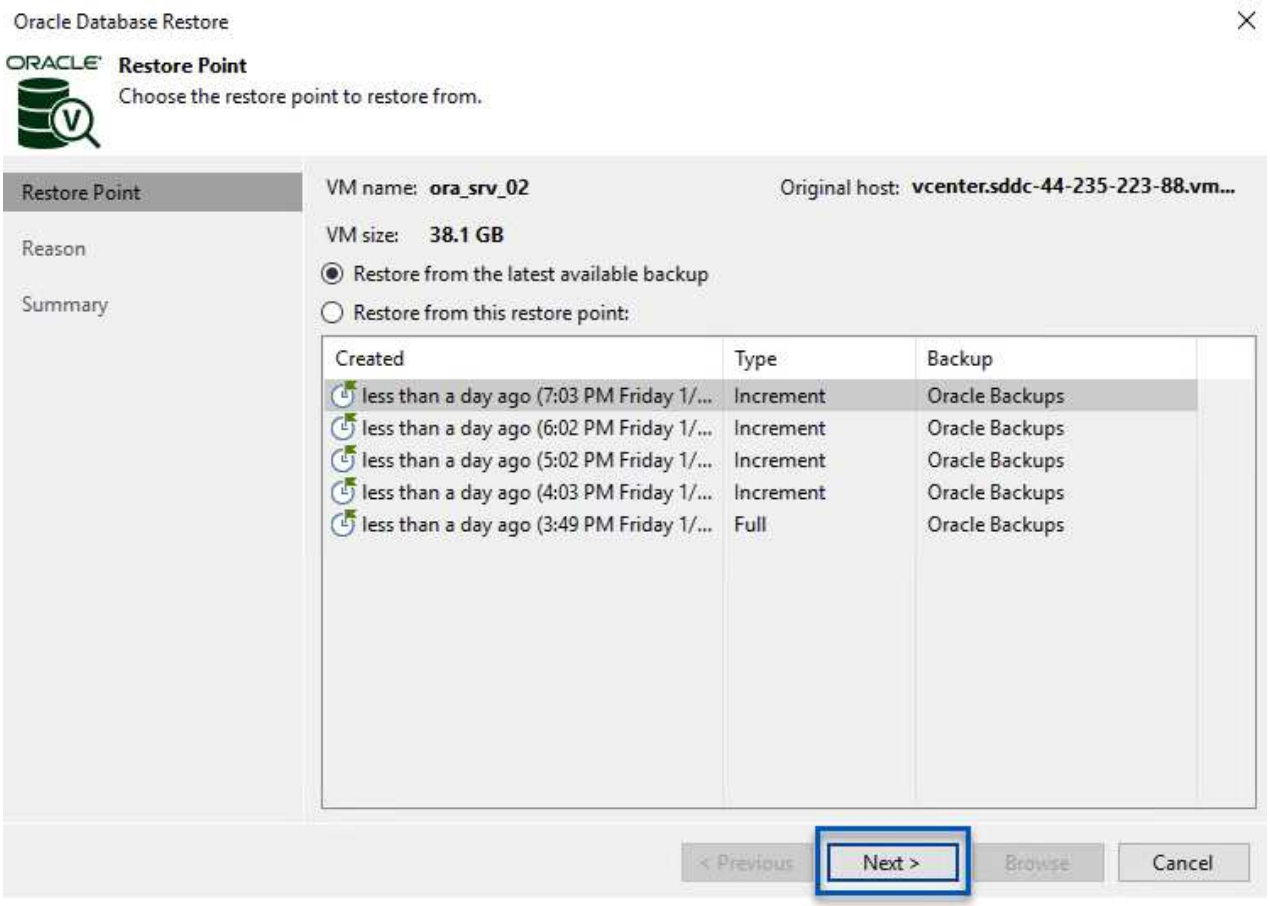
Publier la base de données Oracle sur un autre serveur

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

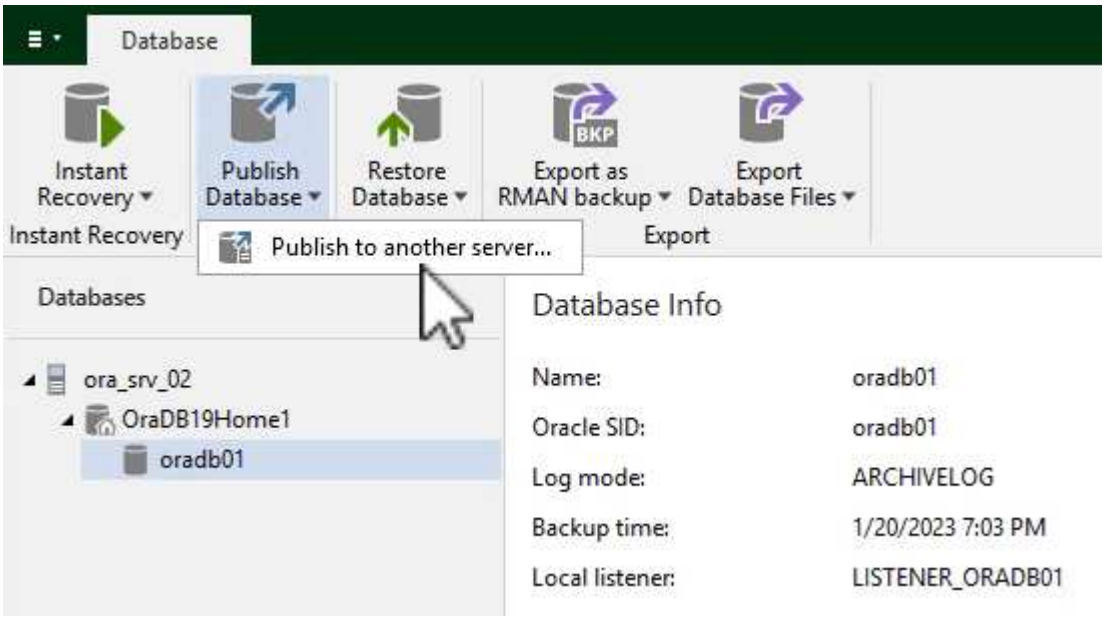
1. Dans la console Veeam Backup and Replication, naviguez jusqu'à la liste des sauvegardes Oracle, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments de l'application**, puis **bases de données Oracle…**.



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

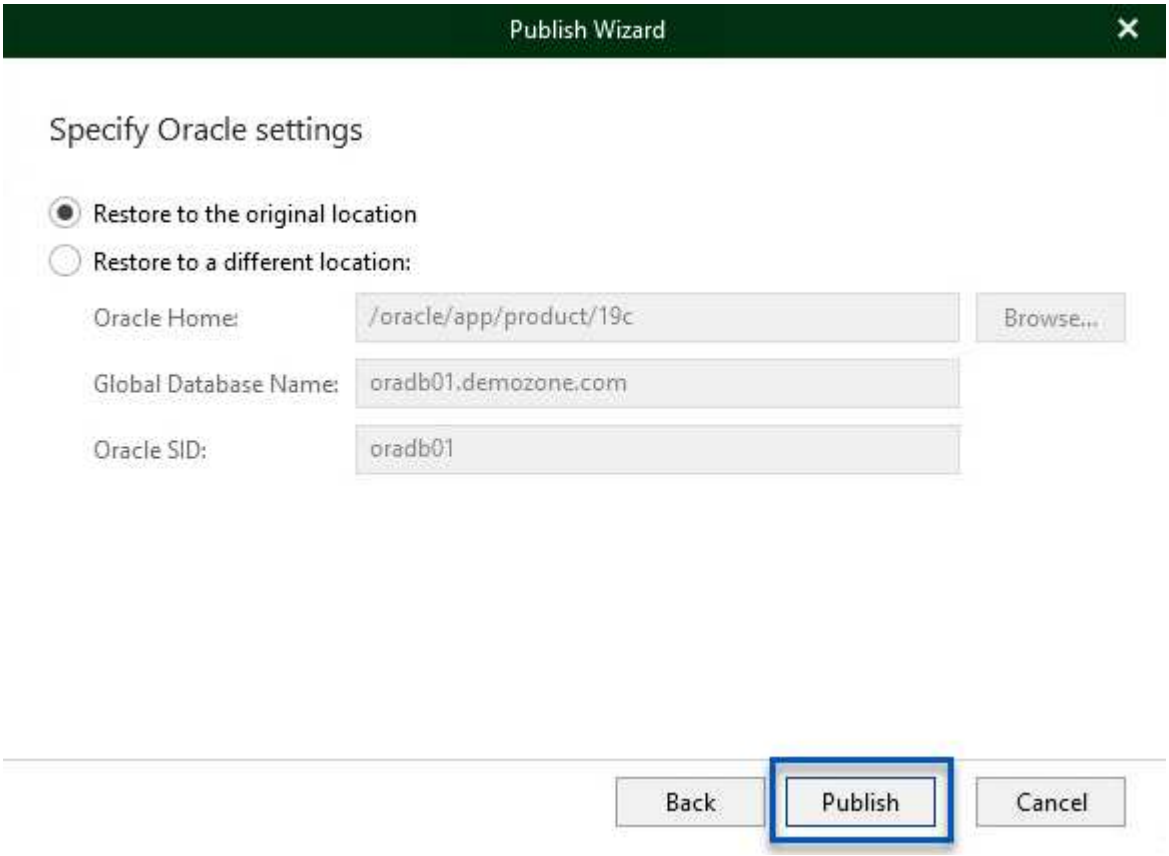


3. Entrez un **motif de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer for Oracle.
4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez sur la base de données à restaurer, puis dans le menu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

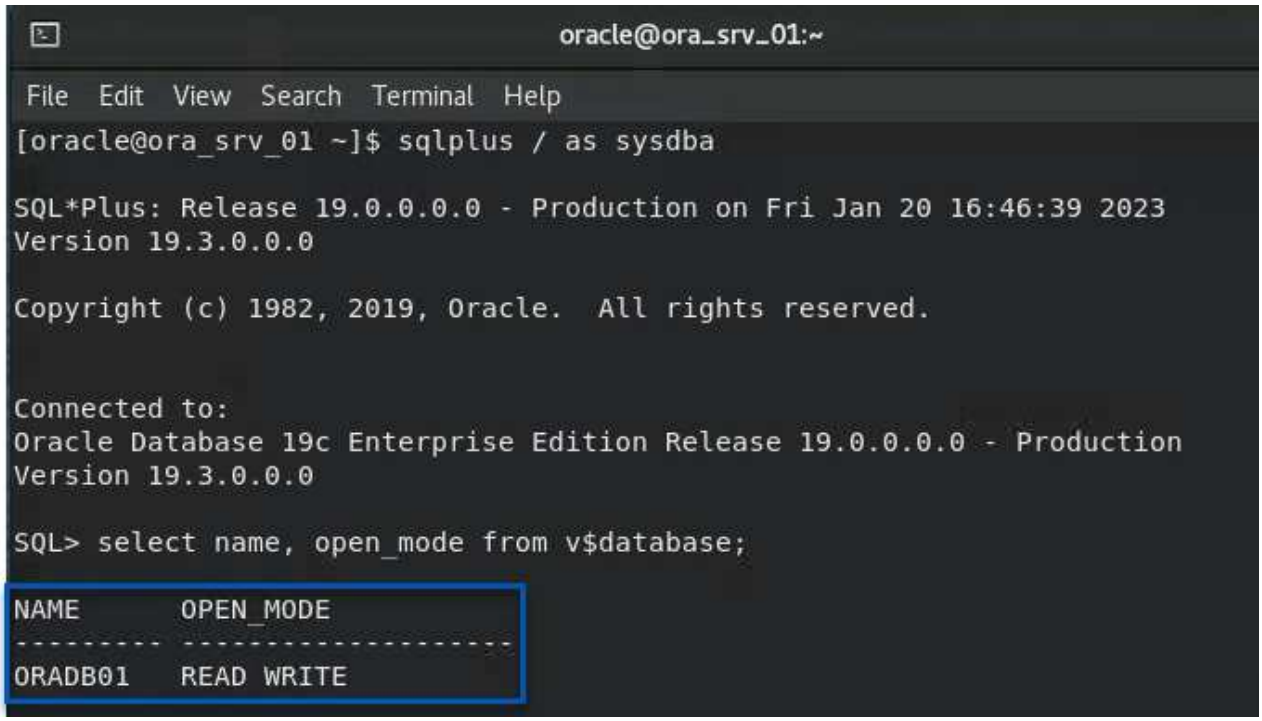
6. Enfin, spécifiez l'emplacement du système de fichiers linux cible et cliquez sur **publier** pour lancer le processus de restauration.



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)

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.

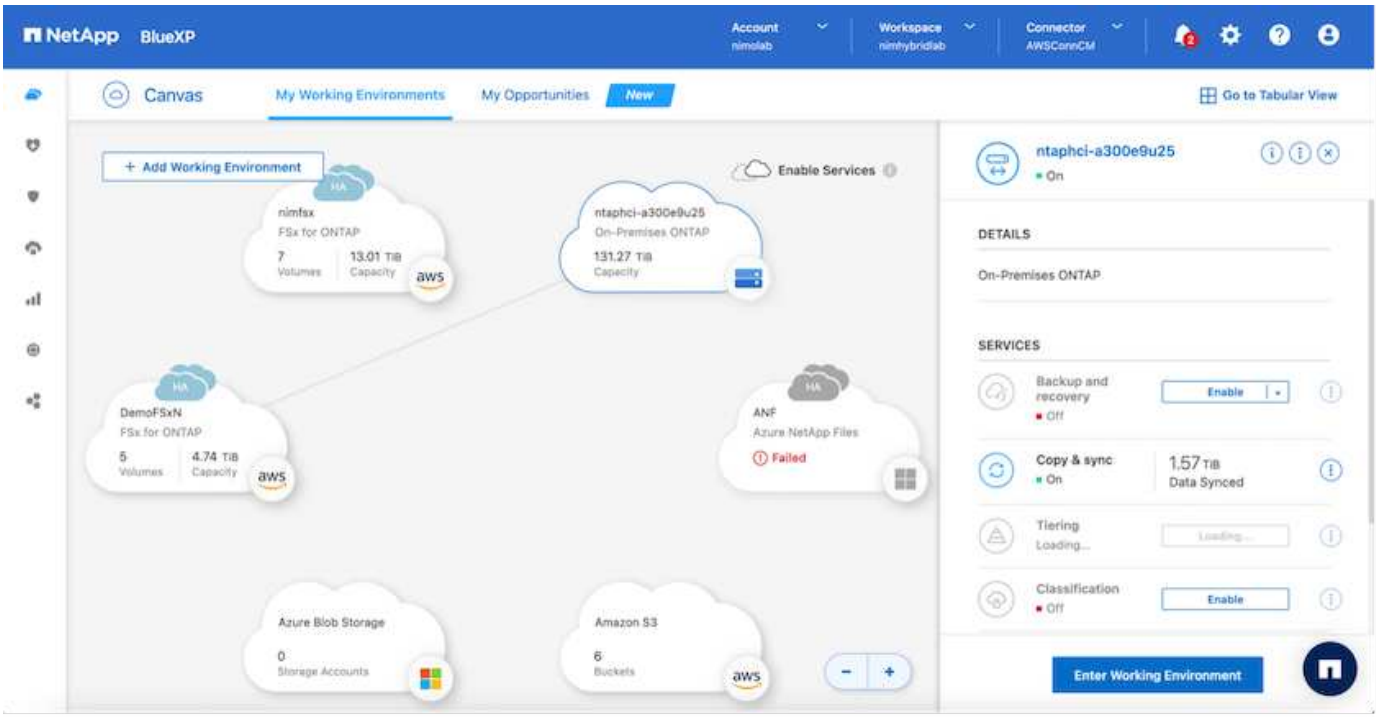
Dans la version initiale, l'analyseur DRO prend en charge un bloc de feux de pilotage existant. La création d'un SDDC à la demande sera disponible dans une prochaine version.

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
```

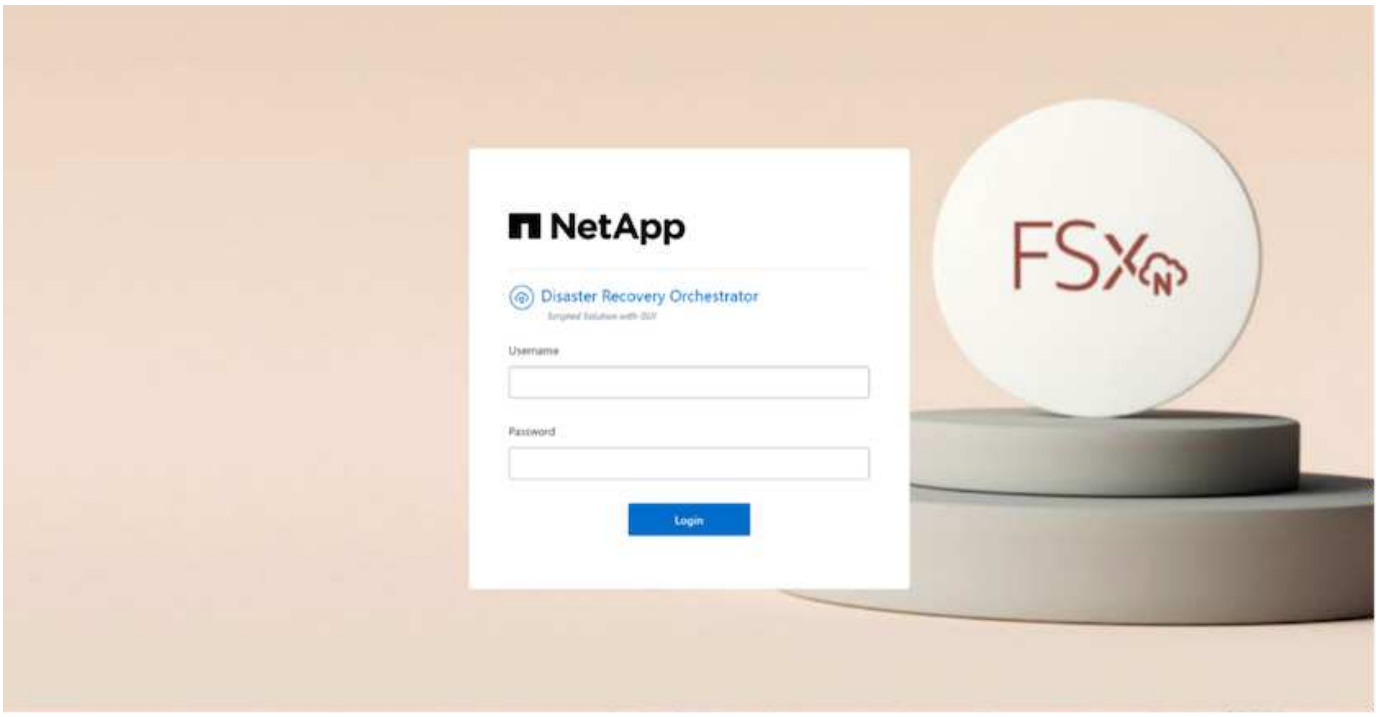
4. Pour accéder à l'interface utilisateur, procédez comme suit :

```
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 ».



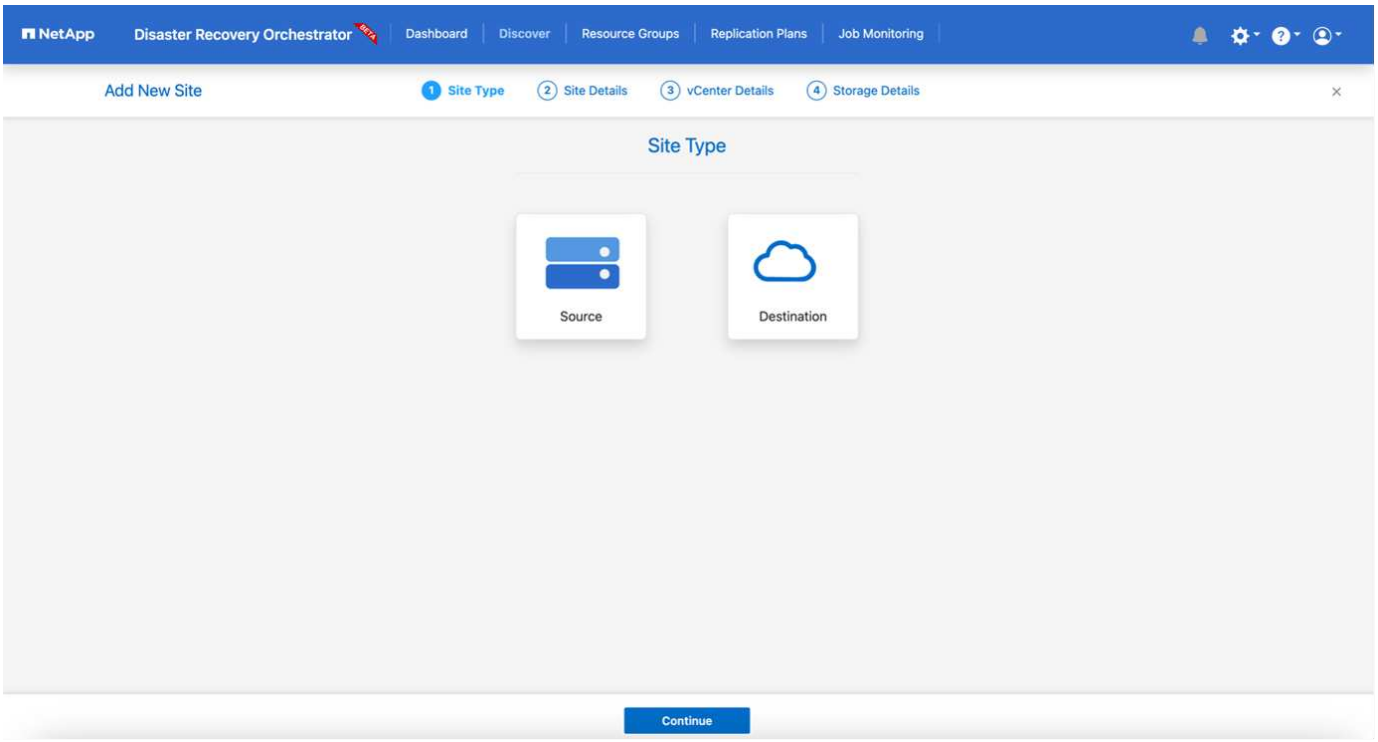
Configuration DRO

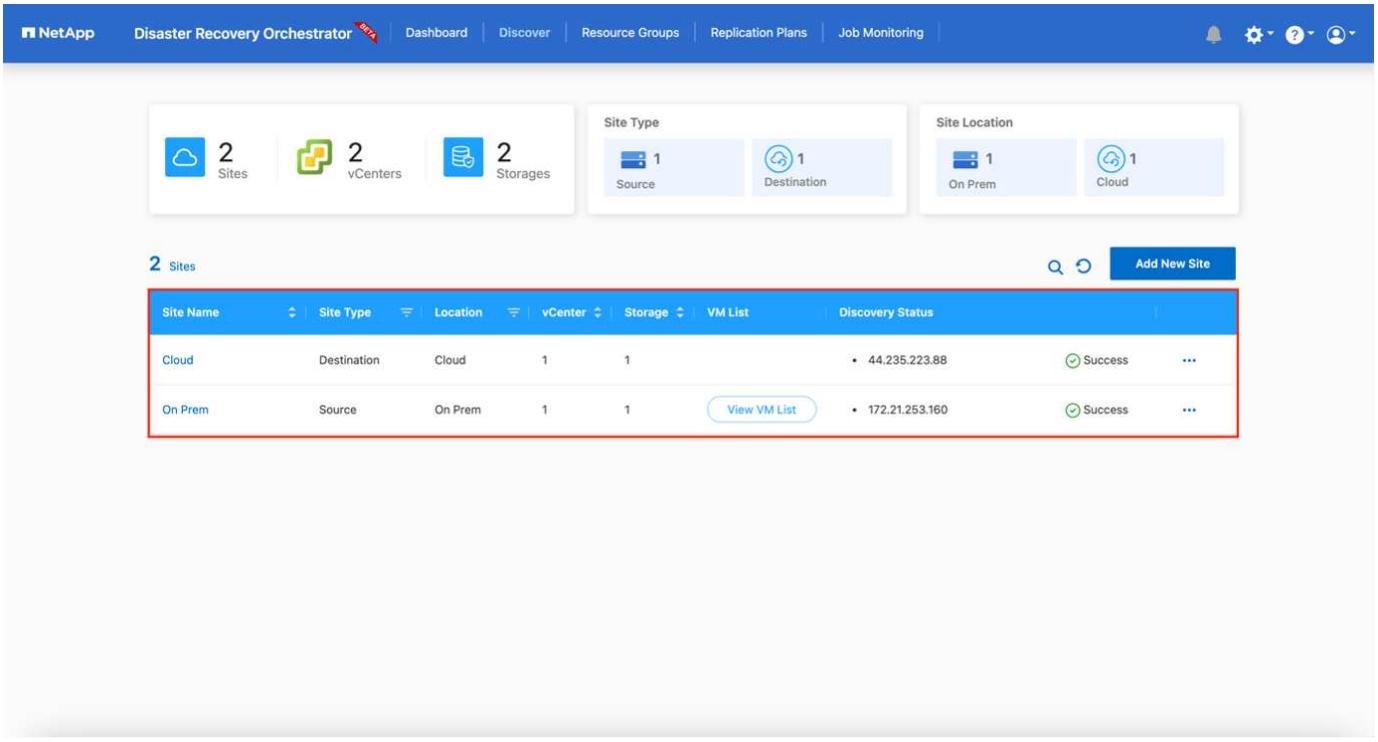
Une fois que FSX pour ONTAP et VMC ont été configurés correctement, vous pouvez commencer à configurer DRO pour automatiser la restauration des charges de travail sur site vers VMC à l'aide des copies SnapMirror en lecture seule sur FSX pour ONTAP.

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.

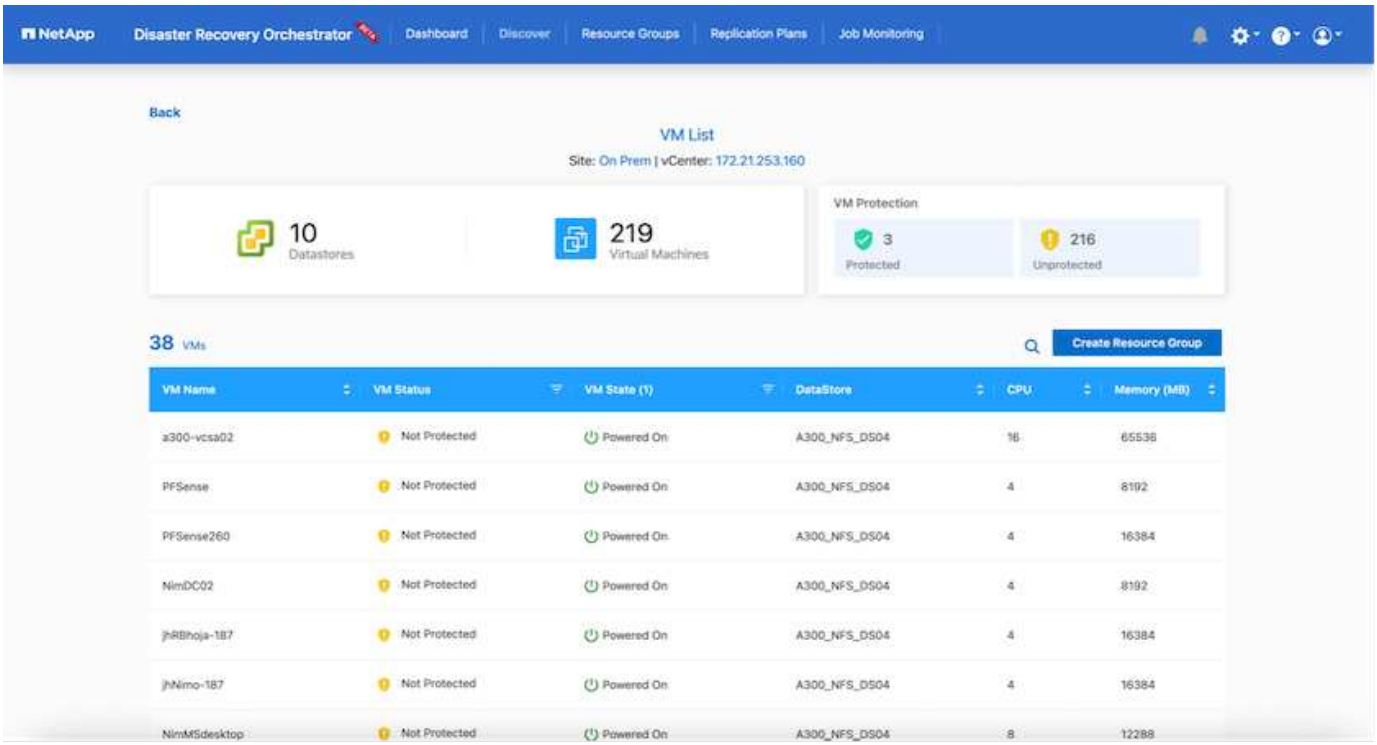
La première étape consiste à découvrir et à ajouter les ressources cloud et sur site (vCenter et du stockage) à DRO. Ouvrez DRO dans un navigateur pris en charge et utilisez le nom d'utilisateur et le mot de passe par défaut (admin/admin) et Ajouter des sites. Vous pouvez également ajouter des sites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

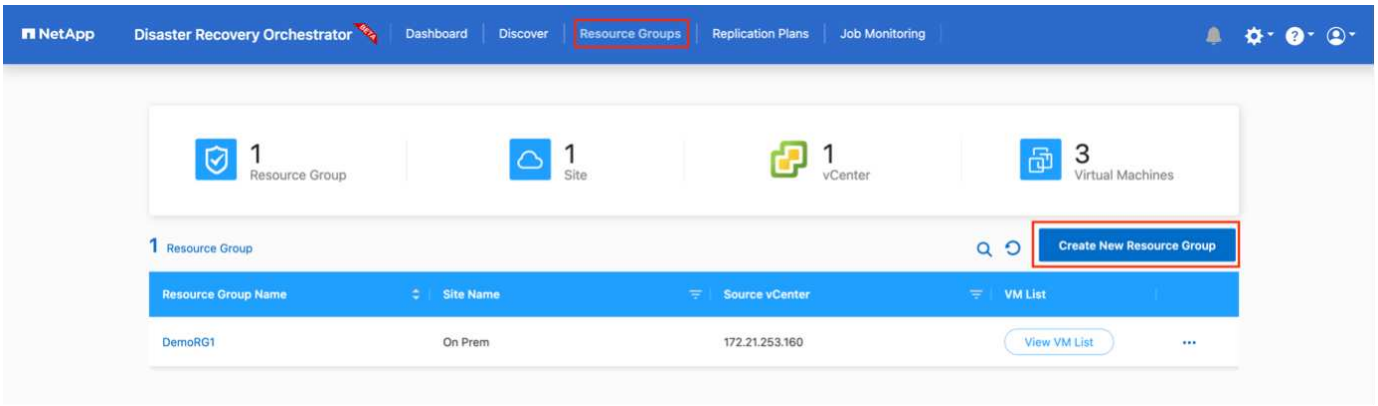
Pour commencer à créer des groupes de ressources, procédez comme suit :

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**.

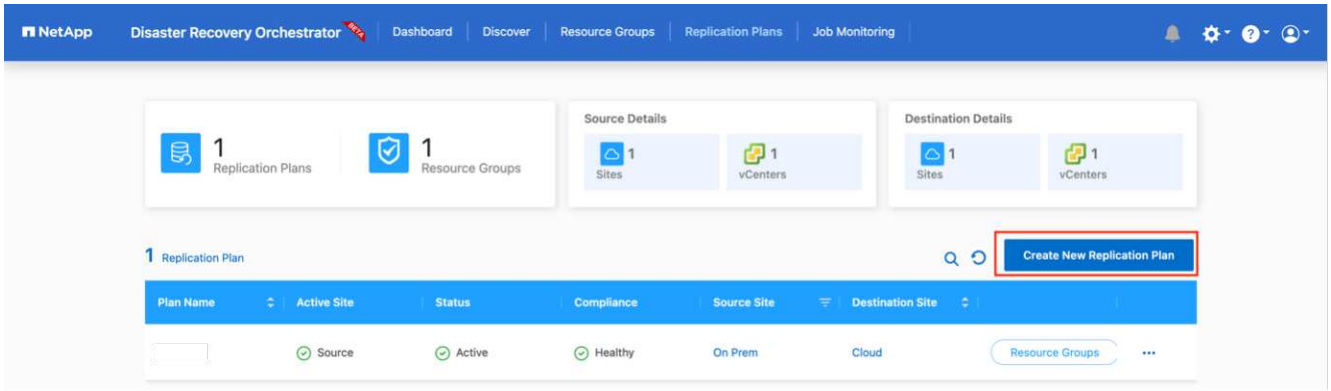


Plans de réplication

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**.

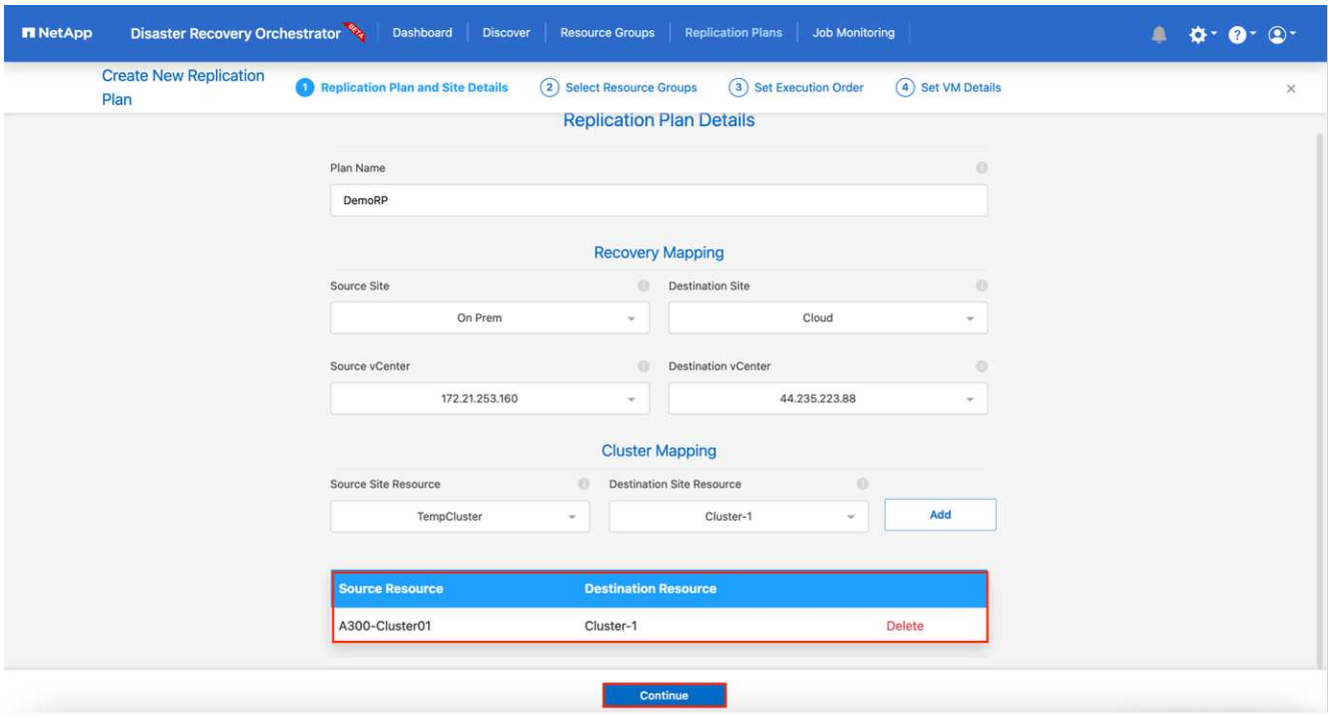
Pour commencer à créer un plan de réplication, procédez comme suit :

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



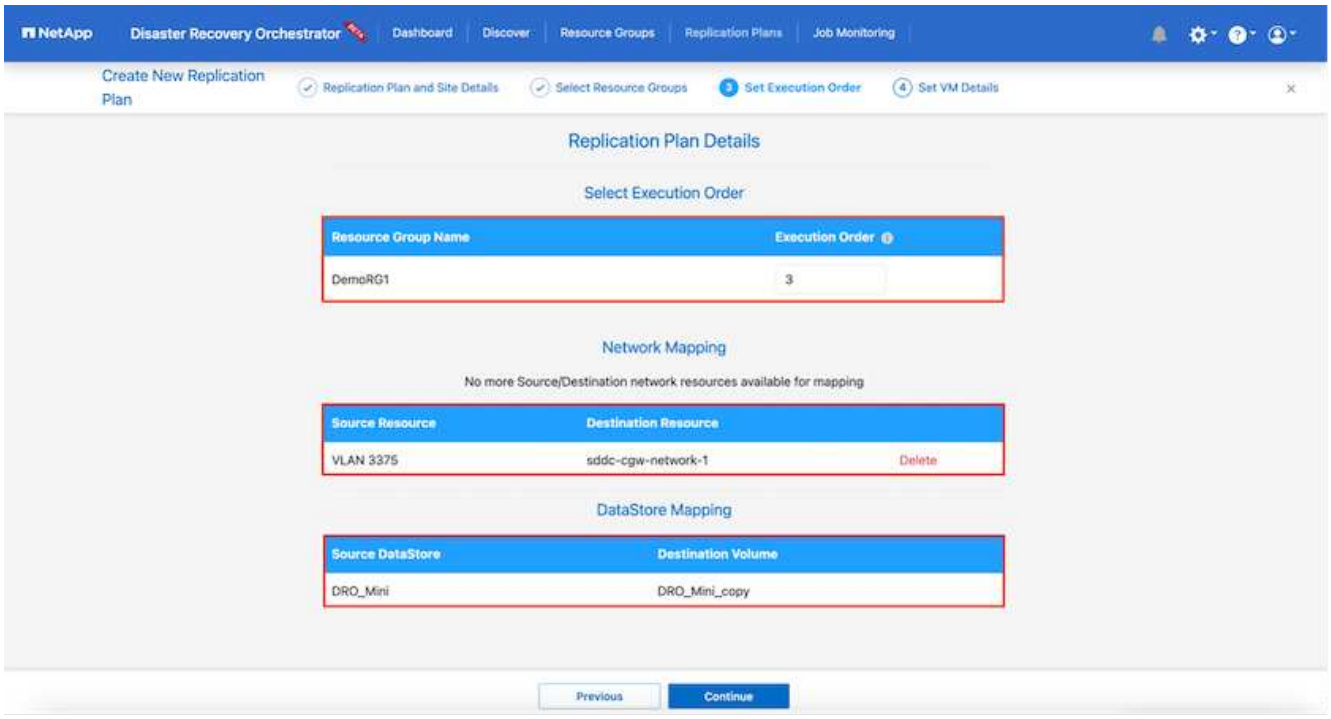
2. Sous **Nouveau plan de réplication**, indiquez un nom pour le plan et ajoutez des mappages de reprise en sélectionnant le site source, le serveur vCenter associé, le site de destination et le serveur vCenter associé.

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

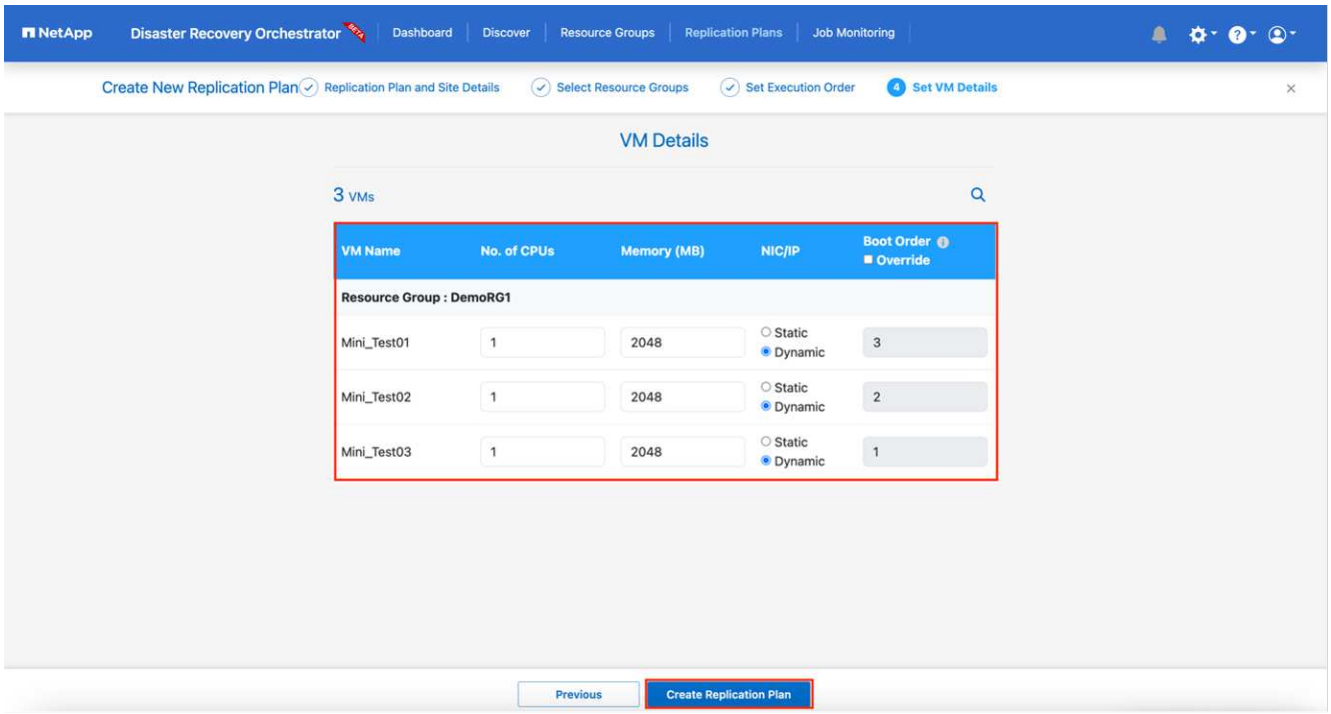


4. Sélectionnez **Détails du groupe de ressources** et cliquez sur **Continuer**.
5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsqu'il existe plusieurs groupes de ressources.
6. Une fois que vous avez terminé, sélectionnez 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.

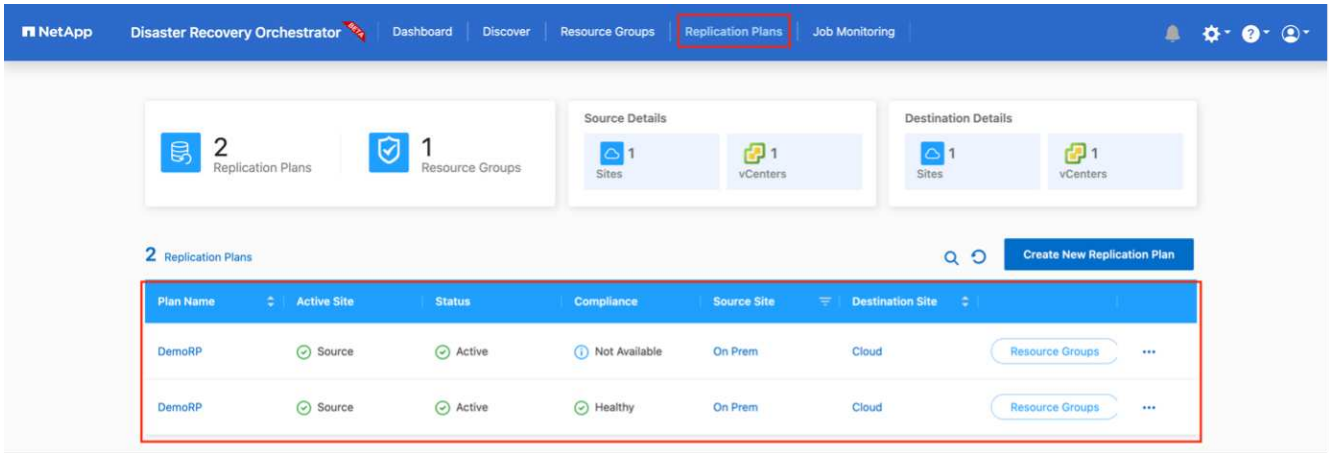
> SnapMirror est au niveau du volume. Par conséquent, tous les VM sont répliqués sur la destination de réplication. Veillez à sélectionner toutes les machines virtuelles faisant partie du datastore. Si elles ne sont pas sélectionnées, seules les machines virtuelles qui font partie du plan de réplication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



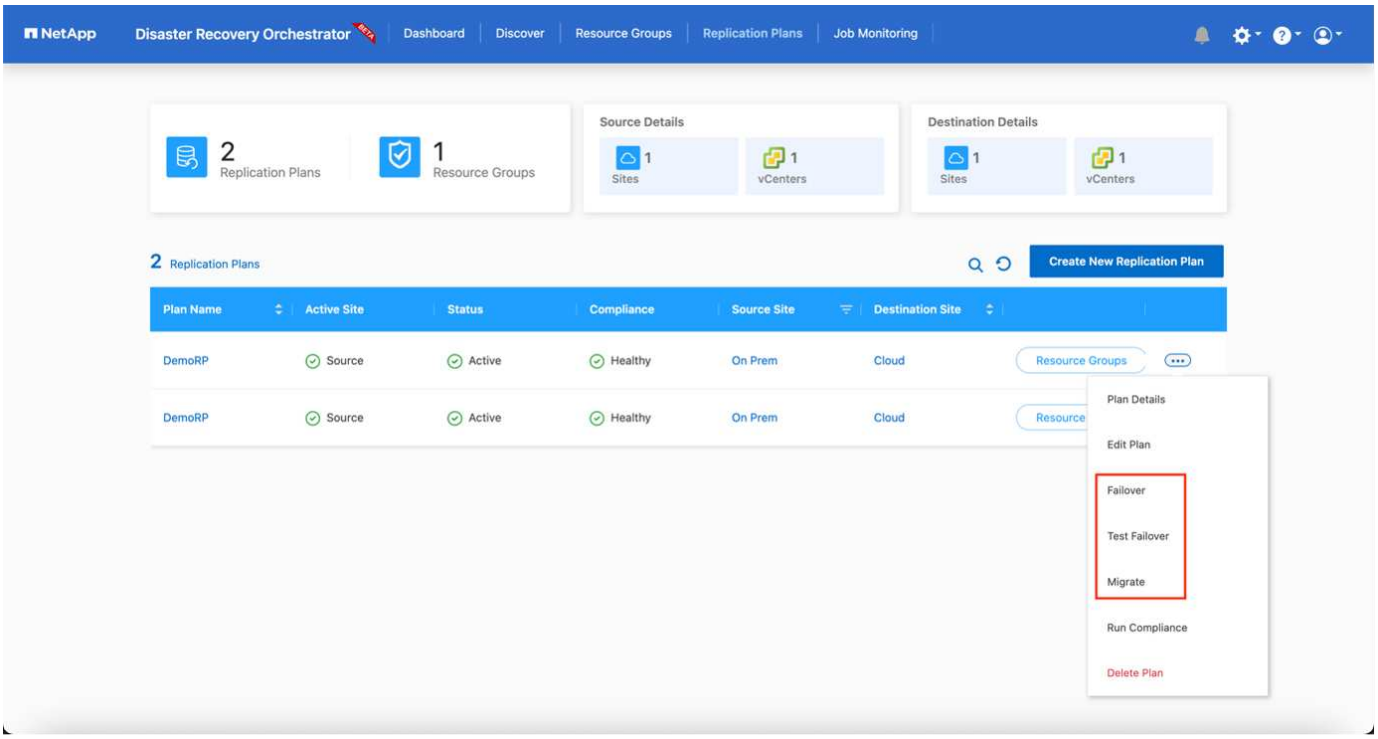
8. Sous les détails de la machine virtuelle, vous pouvez éventuellement redimensionner les paramètres de CPU et de RAM de la machine virtuelle. Cette approche peut être très utile pour restaurer de grands environnements sur des clusters cibles plus petits ou pour effectuer des tests de reprise sur incident 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**.

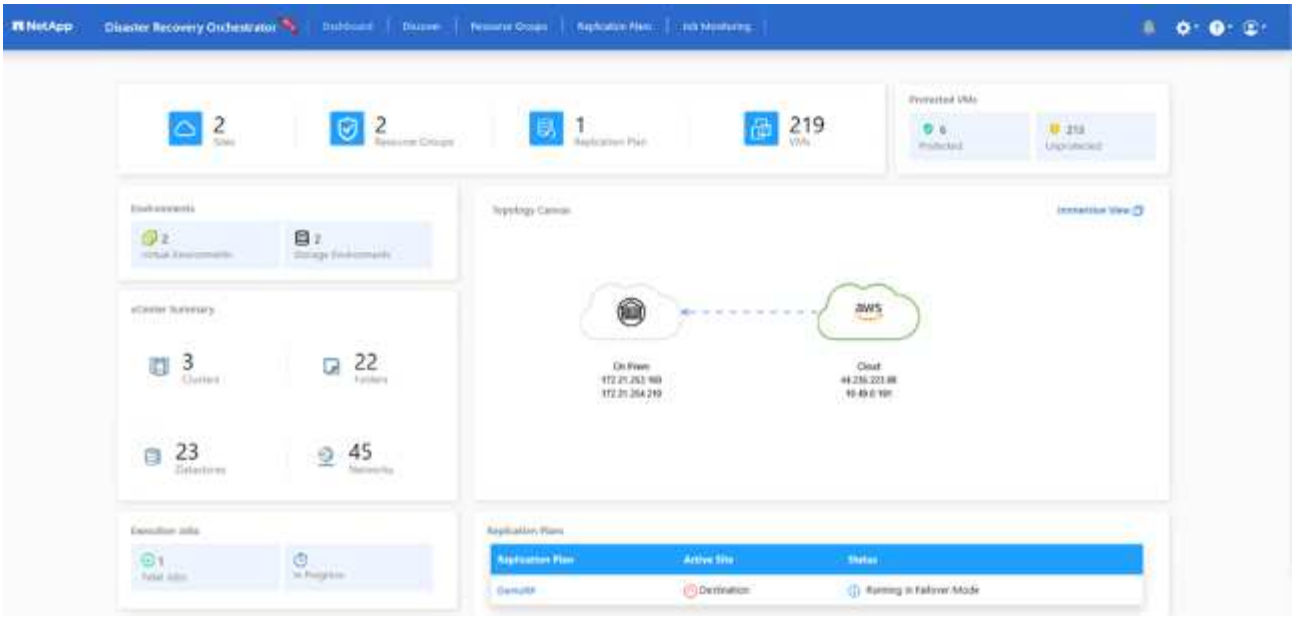


Une fois le plan de réplication créé, l'option de basculement, l'option test-failover ou l'option de migration peuvent être exercées en fonction des exigences. Lors des options de basculement et de test/basculement, la copie Snapshot la plus récente est utilisée ou une copie Snapshot spécifique peut 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**.

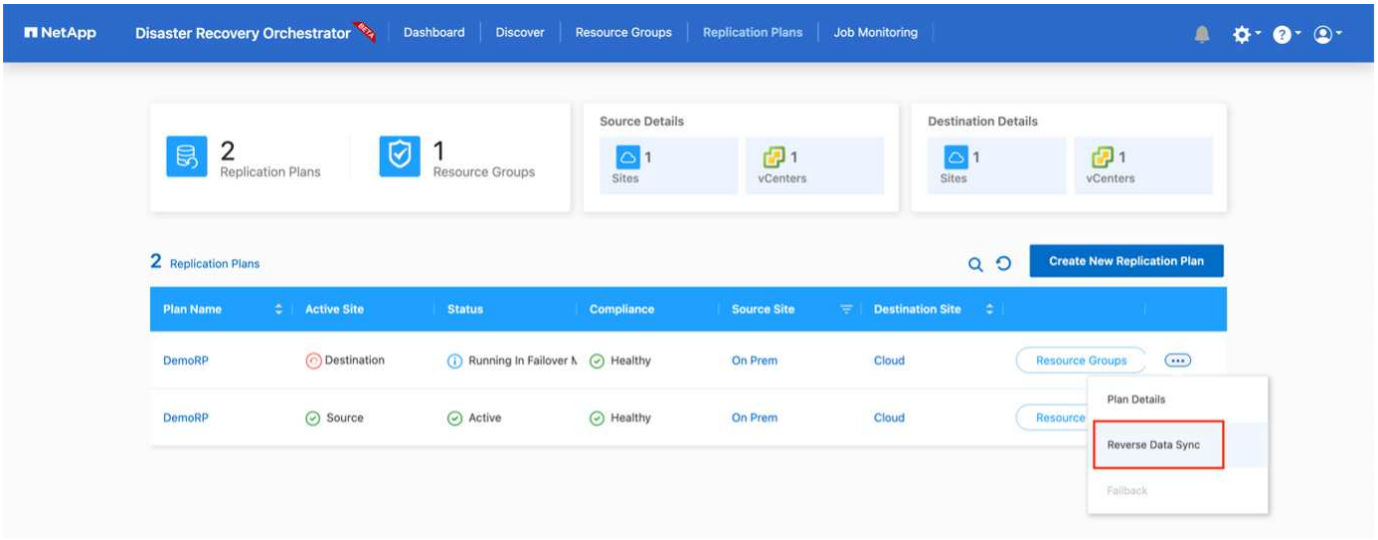


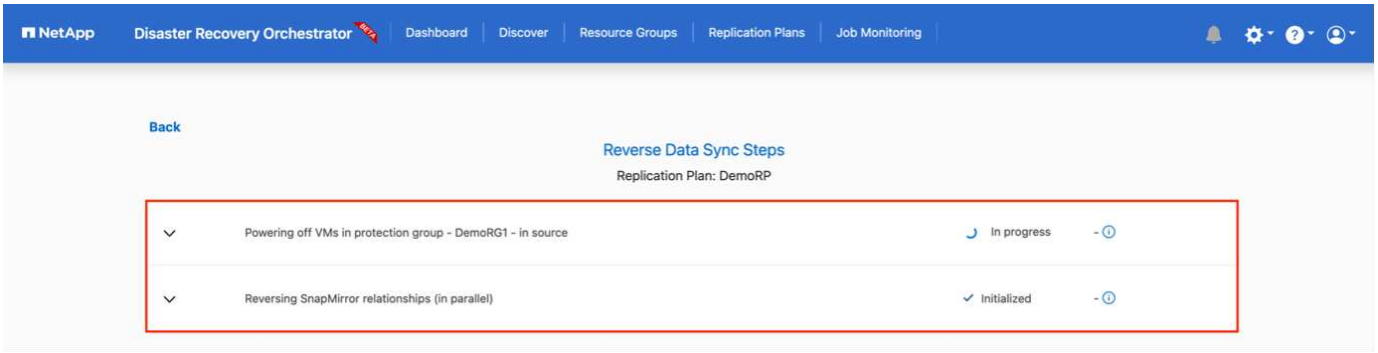
Le plan de réplication peut être surveillé dans le menu des tâches :

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.

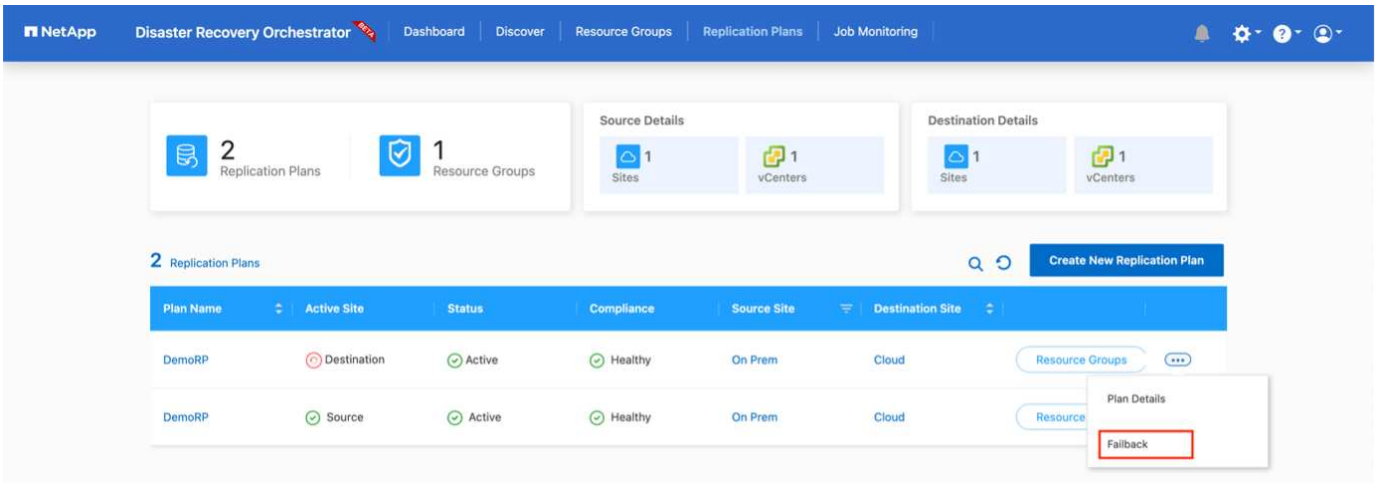


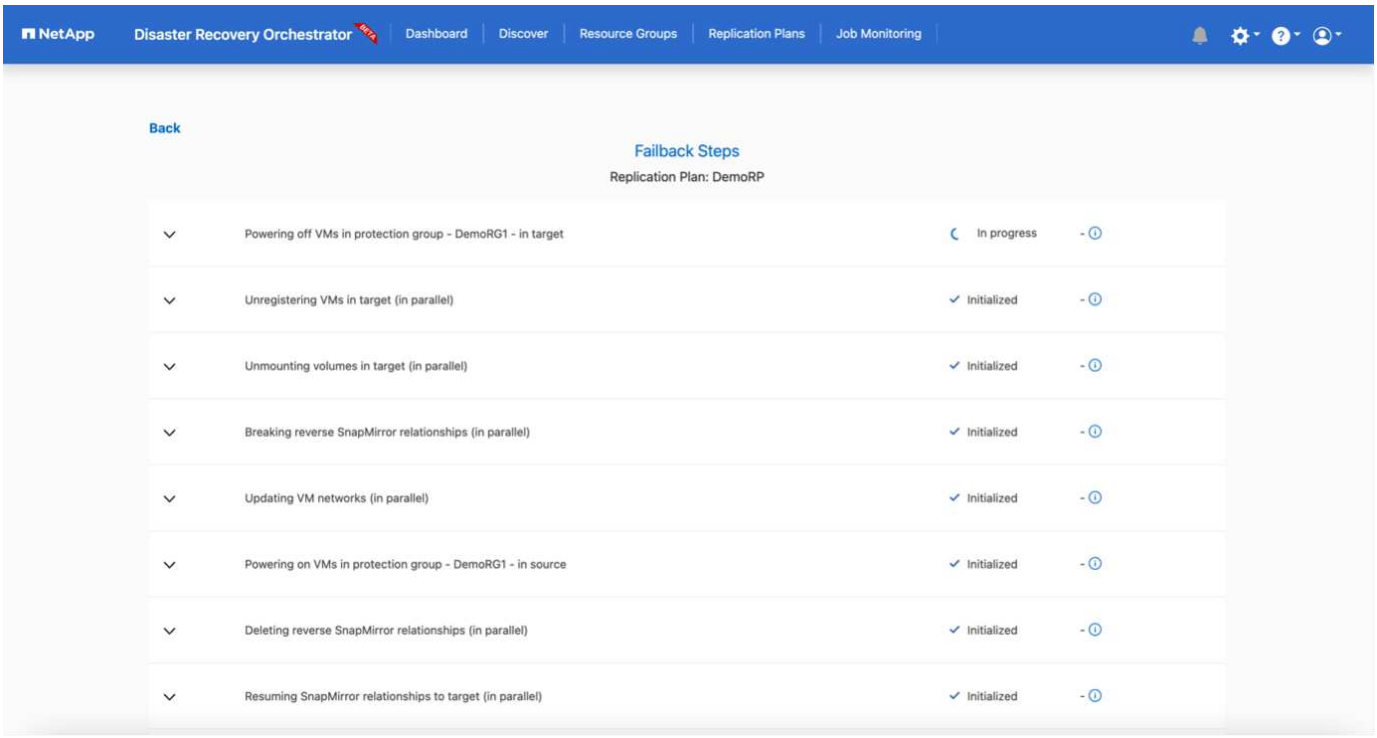
Le retour arrière peut être déclenché au niveau du plan de réplication. Dans le cas d'un basculement test, l'option redescendre peut être utilisée pour annuler les modifications et supprimer la relation FlexClone. La restauration liée au basculement est un processus en deux étapes. Sélectionnez le plan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



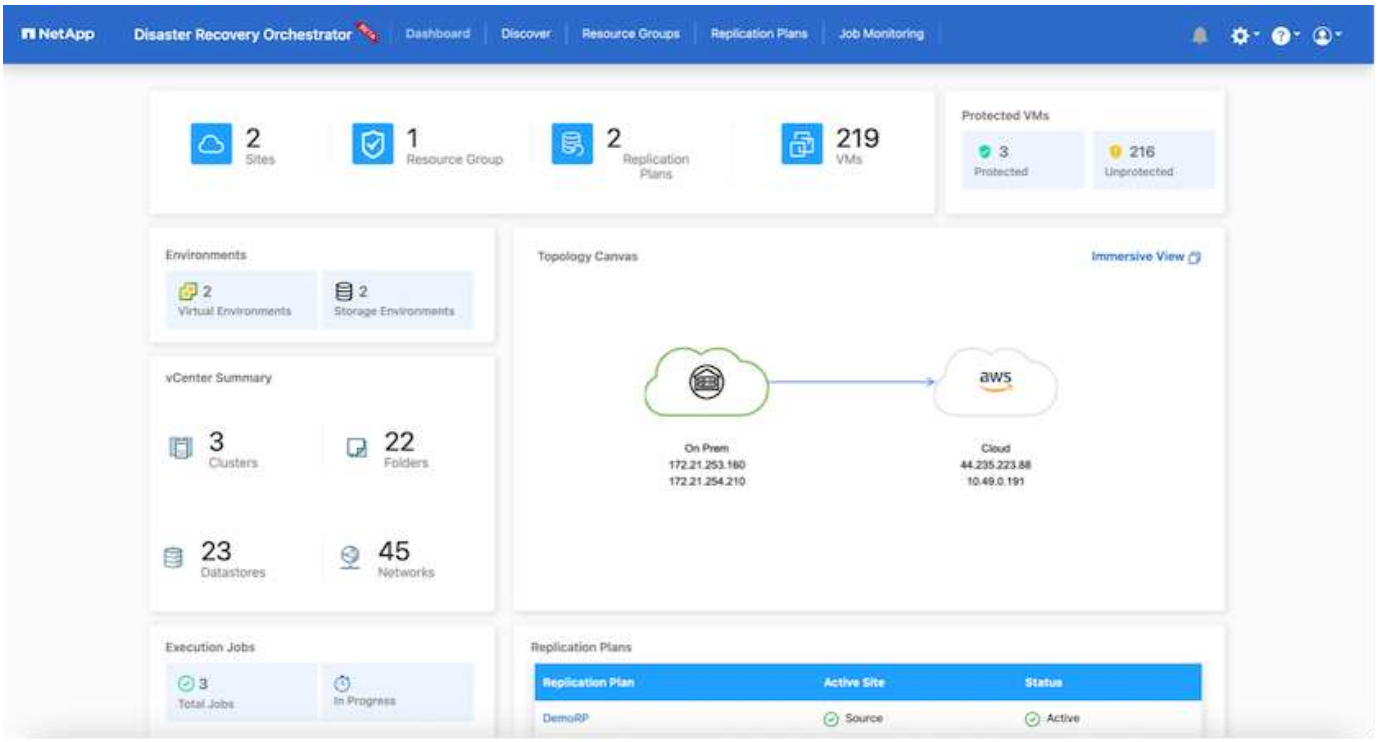


Une fois cette opération terminée, vous pouvez déclencher un retour arrière pour revenir au site de production d'origine.





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.

Auteur: Niyaz Mohamed - NetApp Solutions Engineering

Présentation

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.

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.

[Diagramme du scénario de reprise d'activité avec Veeam Replication et FSX ONTAP pour VMC]

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".

Détails du déploiement

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).

      [dr veeam fsx image2] | *dr-veeam-fsx-image2.png*
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**.

   [dr veeam fsx image3] | *dr-veeam-fsx-image3.png*
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**.

   [dr veeam fsx image4] | *dr-veeam-fsx-image4.png*
6. Dans l'étape suivante, créez le mappage entre le réseau virtuel source et le réseau virtuel de destination, selon vos besoins.

   [dr veeam fsx image5] | *dr-veeam-fsx-image5.png*
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**.

   [dr veeam fsx image6] | *dr-veeam-fsx-image6.png*

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.

    [dr veeam fsx image7] | *dr-veeam-fsx-image7.png*

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.

[dr veeam fsx image8] | *dr-veeam-fsx-image8.png*

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.

   [dr veeam fsx image9] | *dr-veeam-fsx-image9.png*

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.

   [dr veeam fsx image10] | *dr-veeam-fsx-image10.png*

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**.

[dr veeam fsx image11] | *dr-veeam-fsx-image11.png*

[dr veeam fsx image12] | *dr-veeam-fsx-image12.png*

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.

[dr veeam fsx image13] | *dr-veeam-fsx-image13.png*

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

[dr veeam fsx image14] | *dr-veeam-fsx-image14.png*

> 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.

[dr veeam fsx image15] | *dr-veeam-fsx-image15.png*

[dr veeam fsx image16] | *dr-veeam-fsx-image16.png*

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".

[dr veeam fsx image17] | *dr-veeam-fsx-image17.png*

[dr veeam fsx image18] | *dr-veeam-fsx-image18.png*

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

[dr veeam fsx image19] | *dr-veeam-fsx-image19.png*

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

Auteur(s) : Ingénierie de solutions NetApp

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

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.

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.

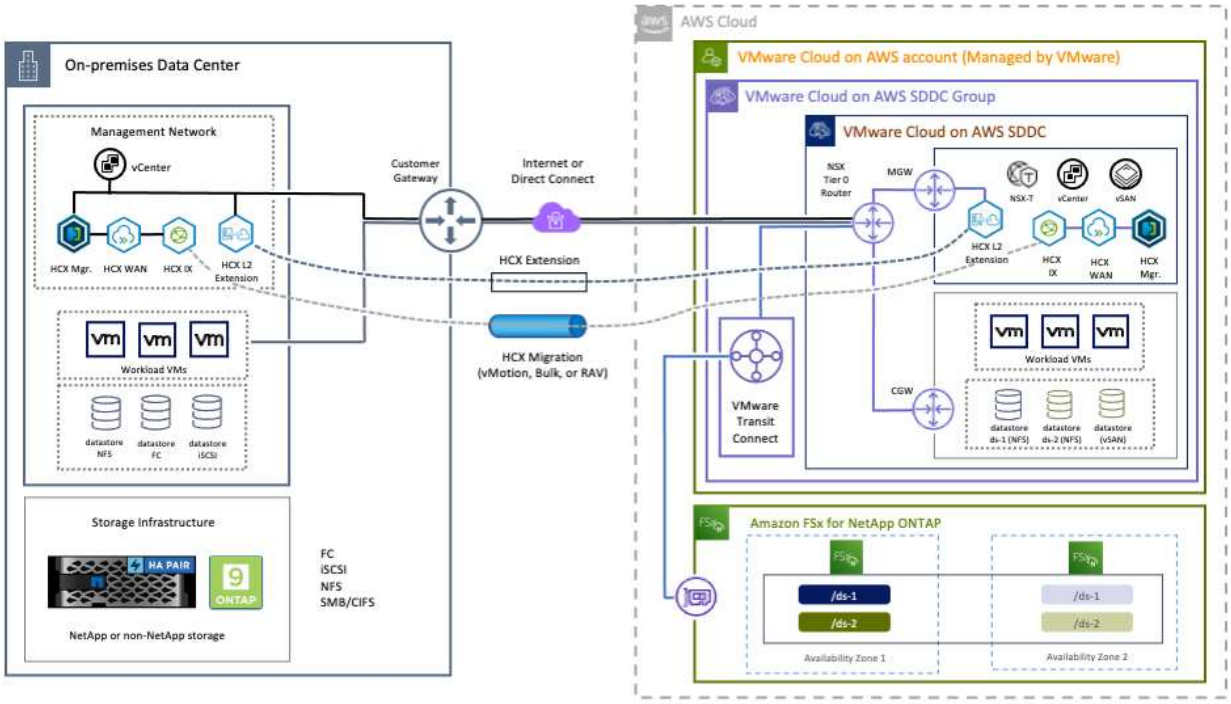
Les étapes d'installation suivantes doivent être effectuées avant de procéder à l'activation et au déploiement du système HCX :

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

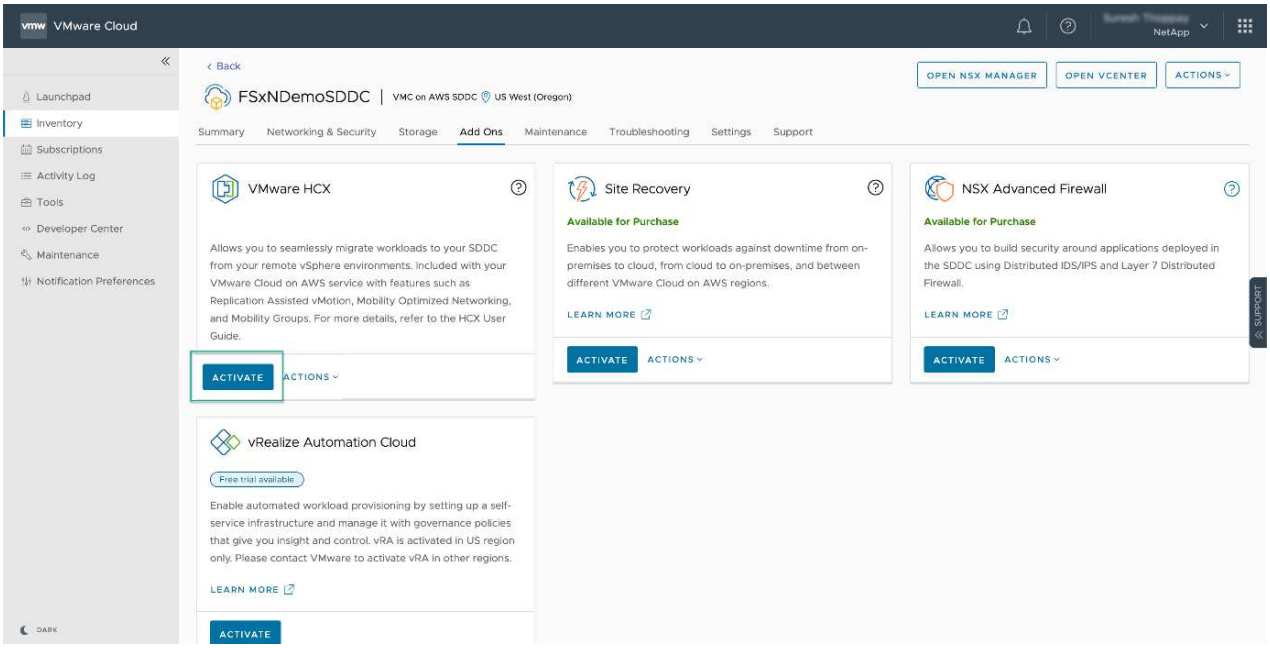
Suivez les étapes du déploiement de cette solution :

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.

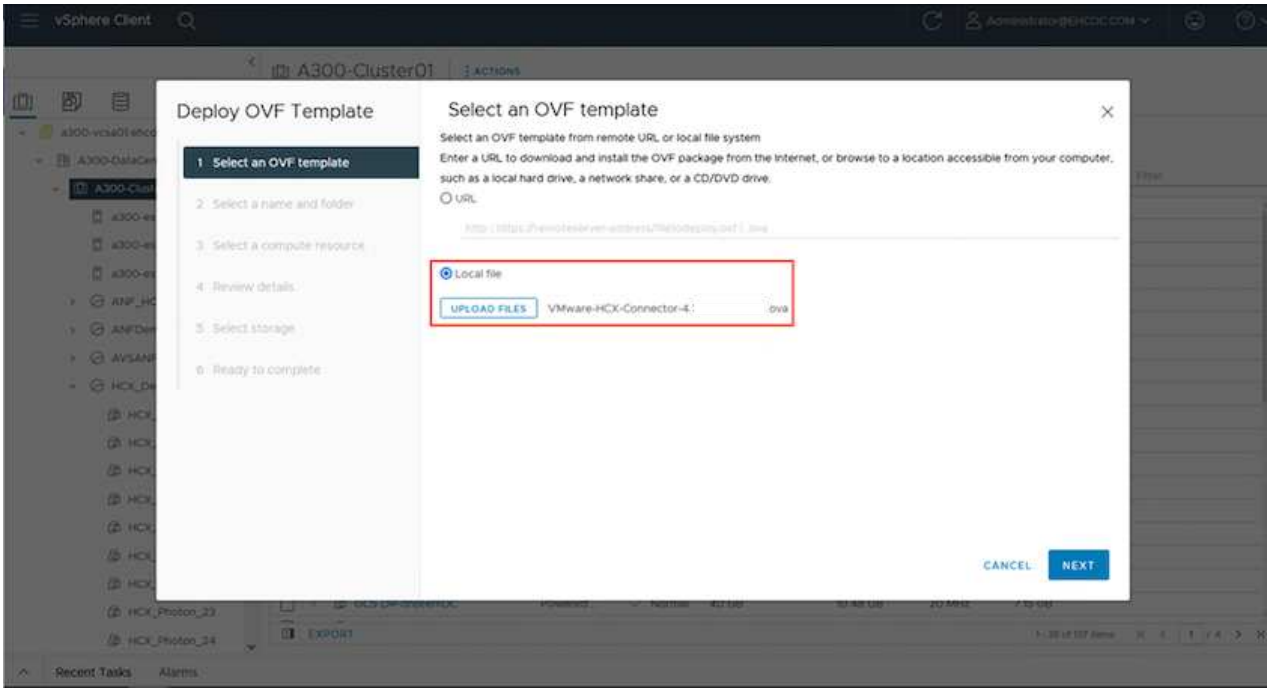


4. Une fois le déploiement terminé, validez le déploiement en vérifiant que HCX Manager et les plug-ins associés sont disponibles dans vCenter Console.
5. Créez les pare-feu de passerelle de gestion appropriés pour ouvrir les ports nécessaires pour accéder à HCX Cloud Manager.HCX Cloud Manager est maintenant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

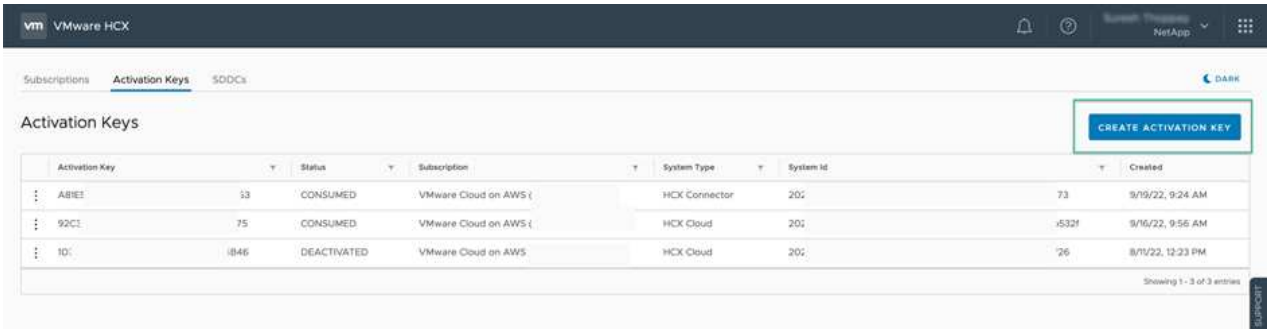


3. Entrez les informations requises dans l'assistant déployer modèle OVF, cliquez sur Suivant, puis sur Terminer pour déployer le connecteur OVA VMware HCX.
4. Mettez l'appliance virtuelle sous tension manuellement.pour obtenir des instructions détaillées, reportez-vous à la section "Guide de l'utilisateur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

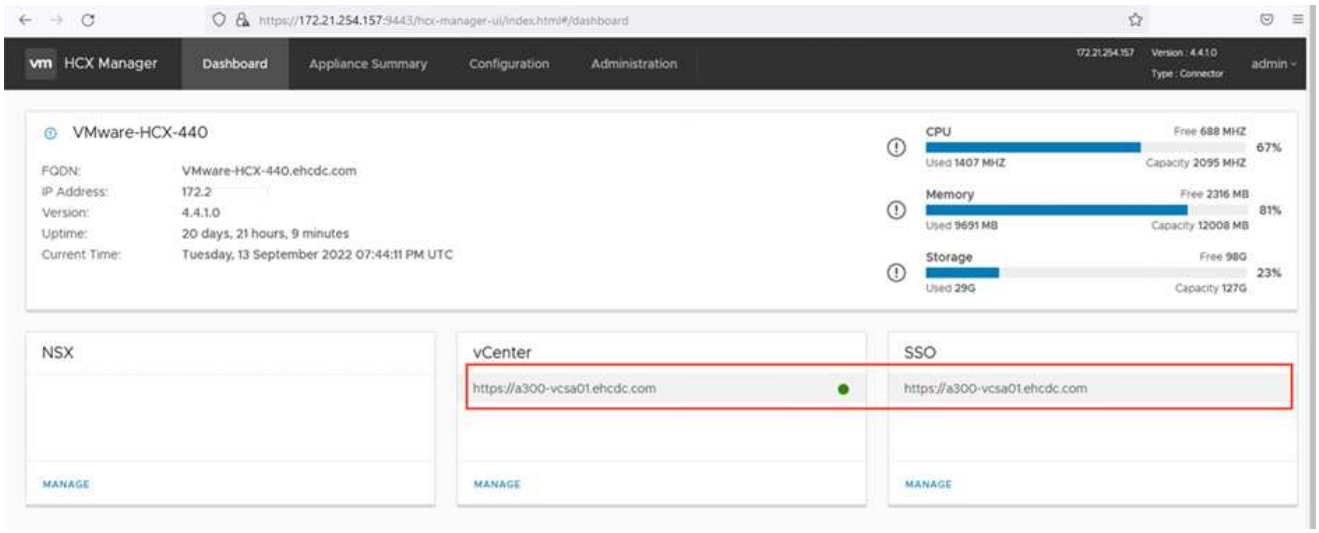
9. Sous configurer SSO/PSC, indiquez le FQDN ou l'adresse IP du contrôleur Platform Services Controller et cliquez sur Continuer.

> 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

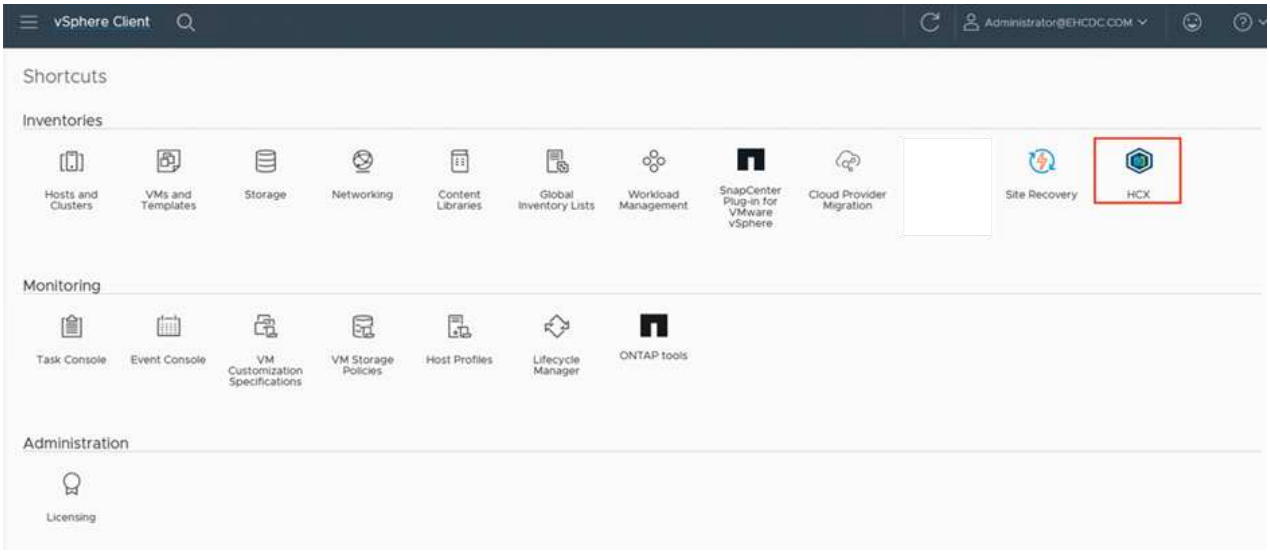
avoir les paramètres de configuration corrects, qui doivent être identiques à la page précédente.

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

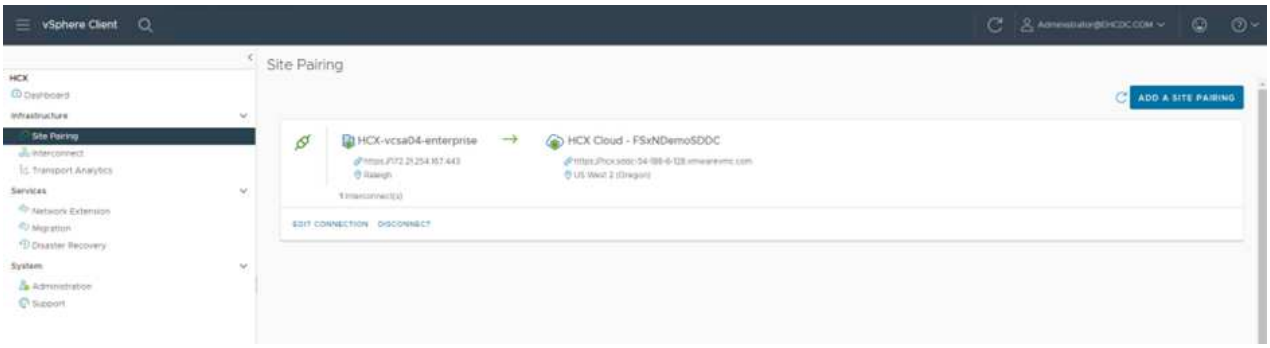


Étape 4 : coupler le connecteur VMware HCX sur site avec VMC HCX Cloud Manager

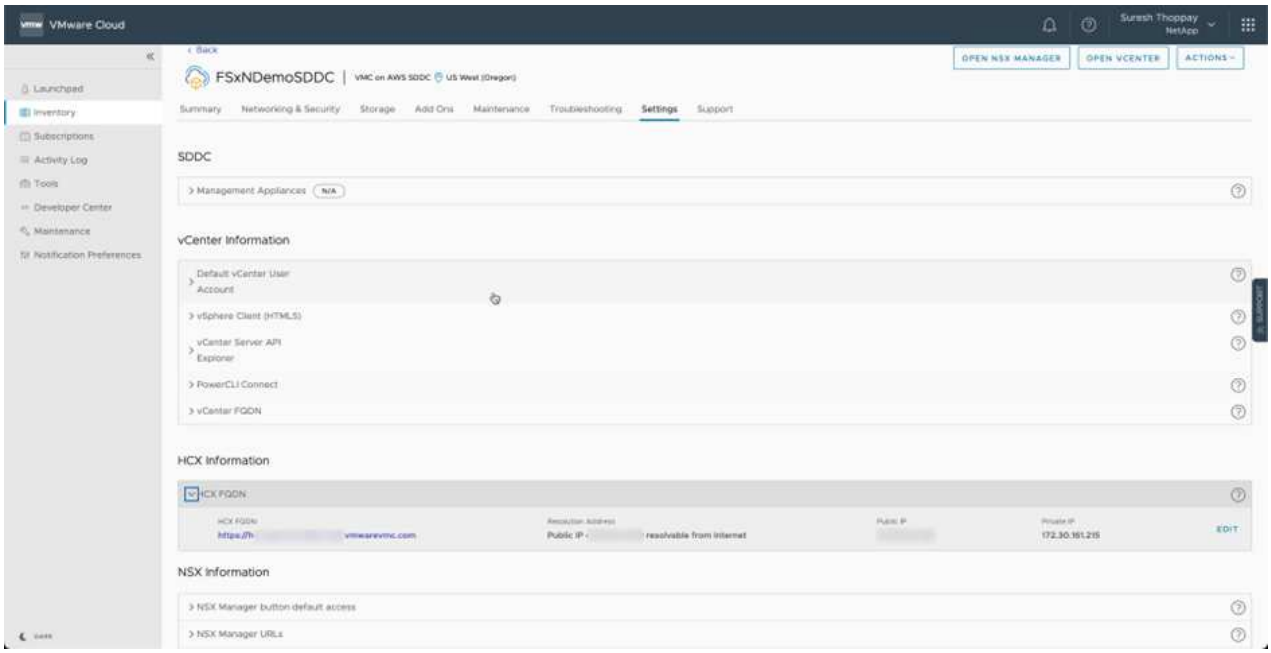
1. Pour créer une paire de sites entre vCenter Server sur site et le SDDC VMC, connectez-vous au serveur vCenter sur site et accédez au plug-in client Web HCX vSphere.

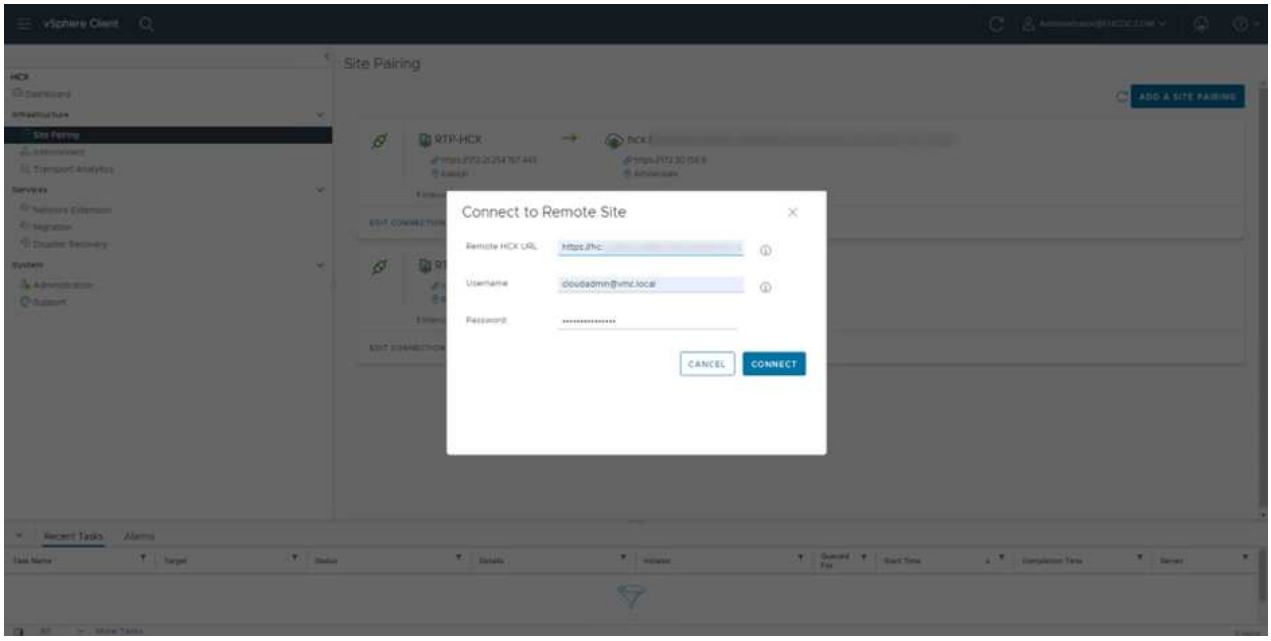


2. Sous Infrastructure, cliquez sur Ajouter un couplage de site. Pour authentifier le site distant, entrez l'URL ou l'adresse IP du VMC HCX Cloud Manager et les informations d'identification du rôle CloudAdmin.



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.

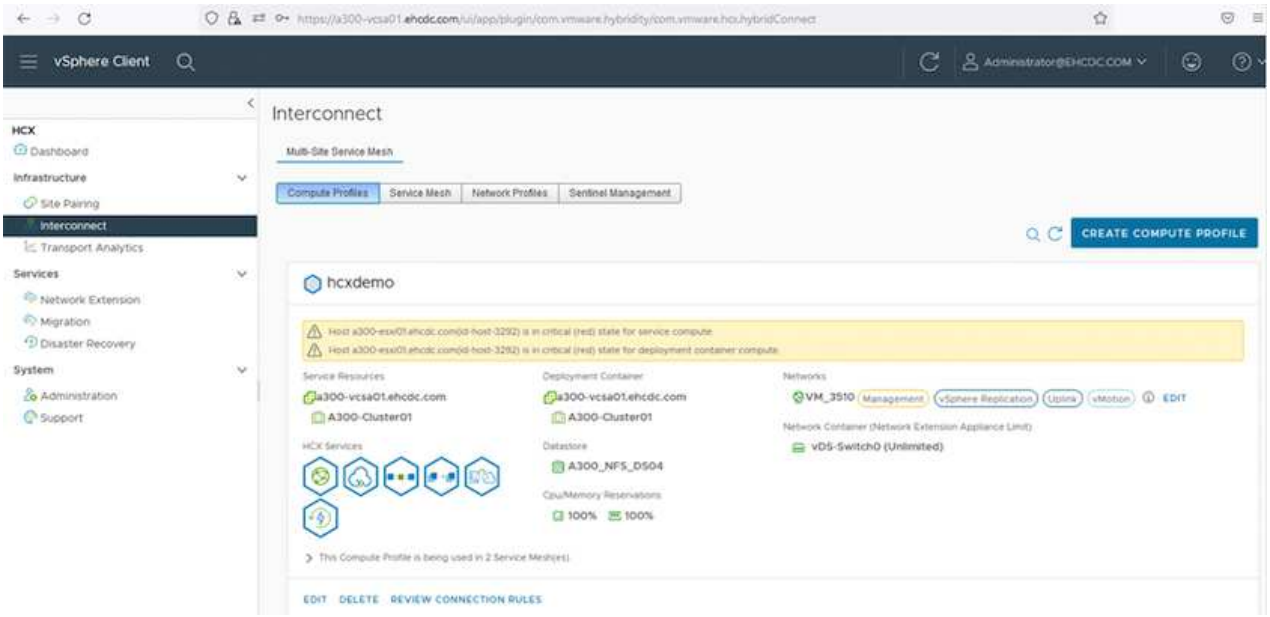
Étape 5 : configurer le profil réseau, le profil de calcul et le maillage de service

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.

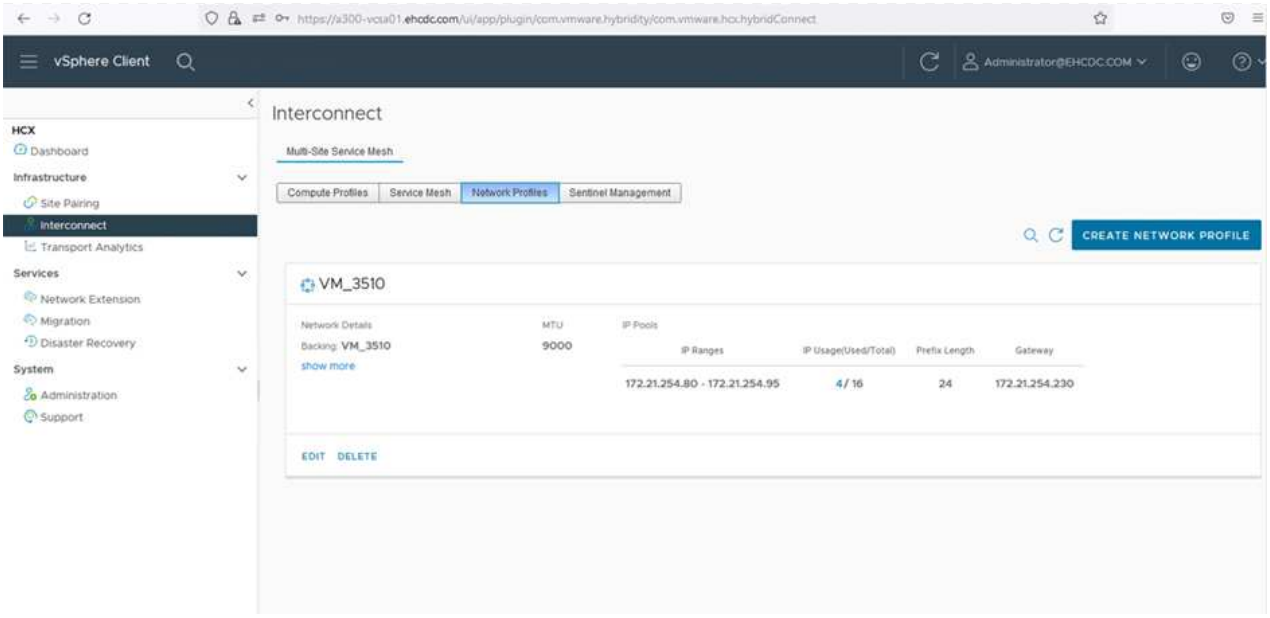
   Les profils de calcul contiennent les paramètres de déploiement de calcul, de stockage et de réseau requis pour déployer une appliance virtuelle d'interconnexion. Ils précisent également quelle partie du data Center VMware sera accessible au service HCX.

   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.

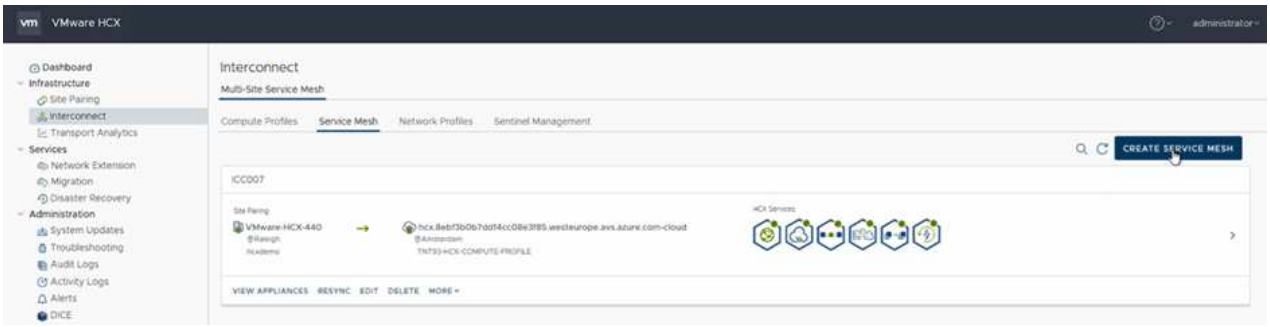


Pour obtenir des instructions détaillées, reportez-vous à la section "Création d'un profil réseau".

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

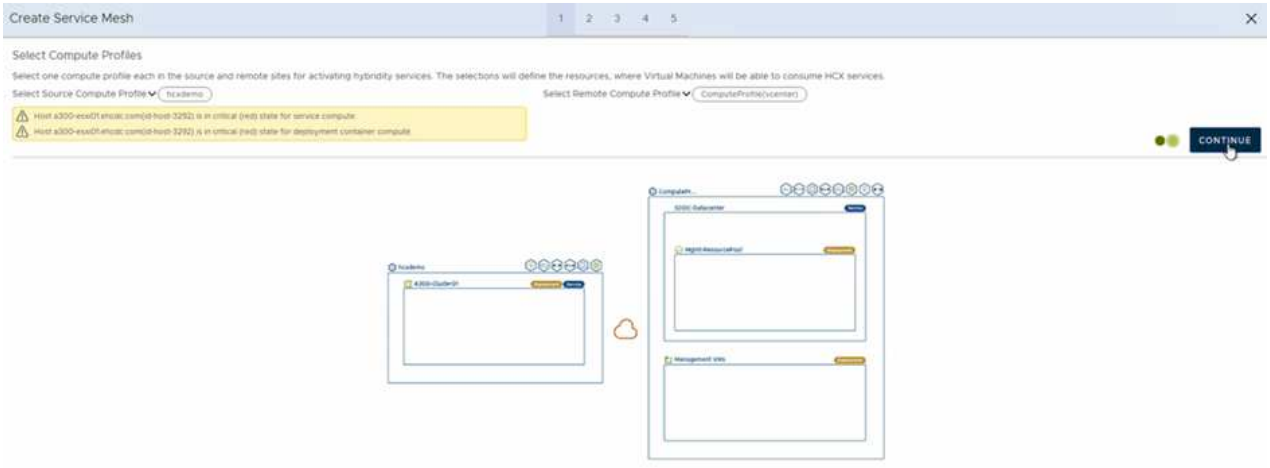
4. Pour créer un maillage de service, sélectionnez l'onglet maillage de service dans l'option interconnexion et sélectionnez sites SDDC locaux et VMC.

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

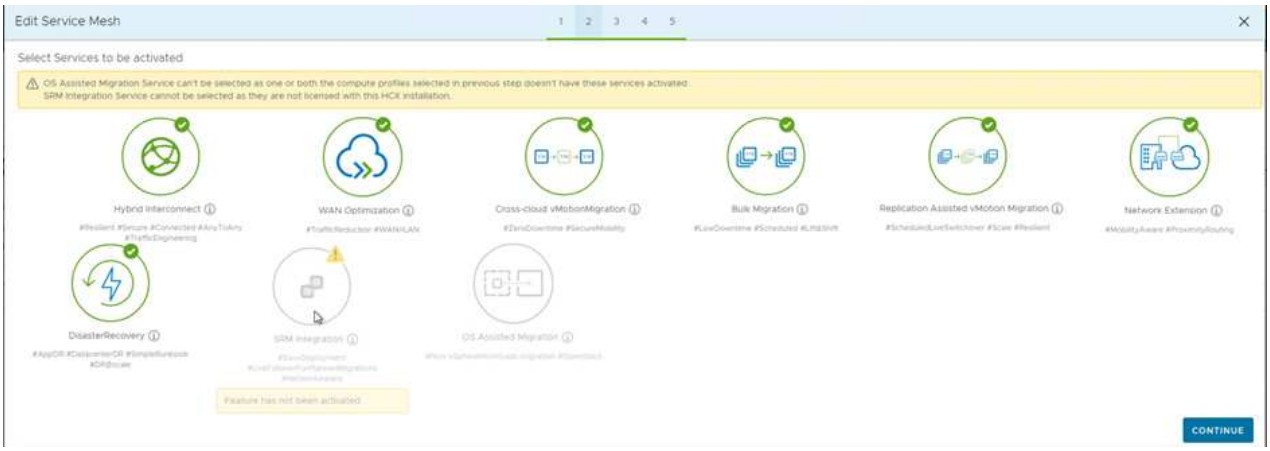


Ce processus implique notamment le déploiement d'appliances HCX qui seront automatiquement configurées sur les sites source et cible, créant ainsi une structure de transport sécurisée.

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

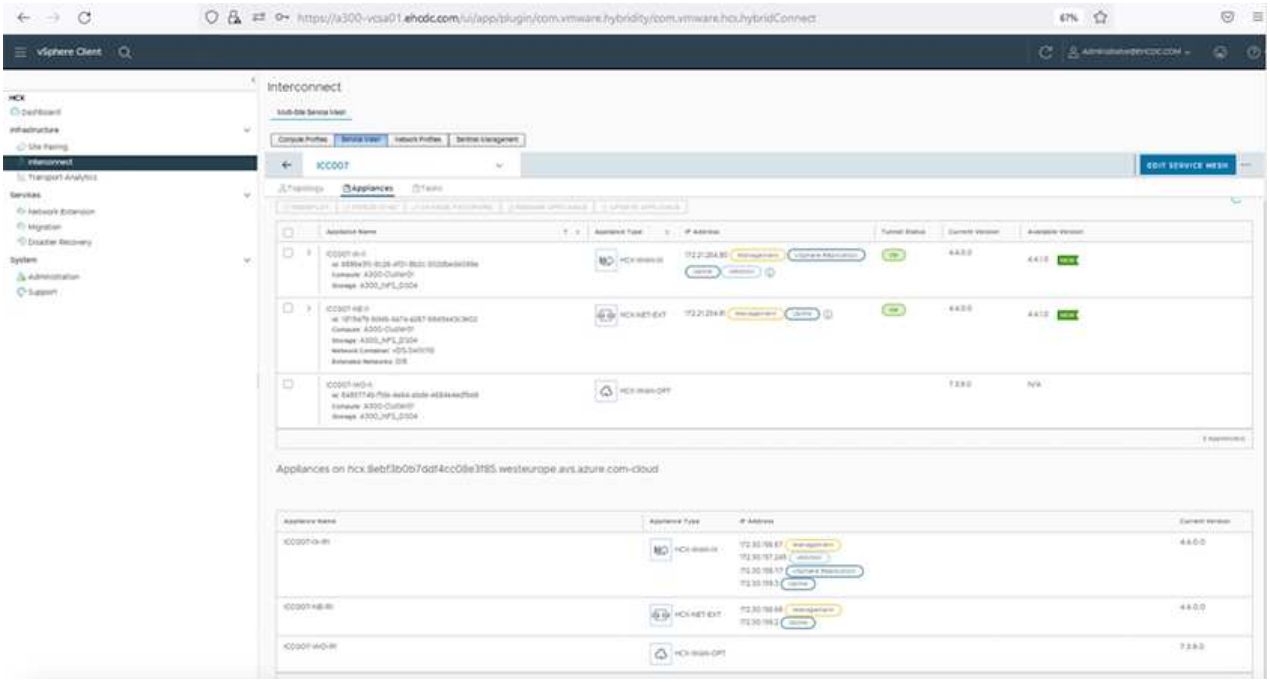


6. Sélectionnez le service à activer et cliquez sur Continuer.



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

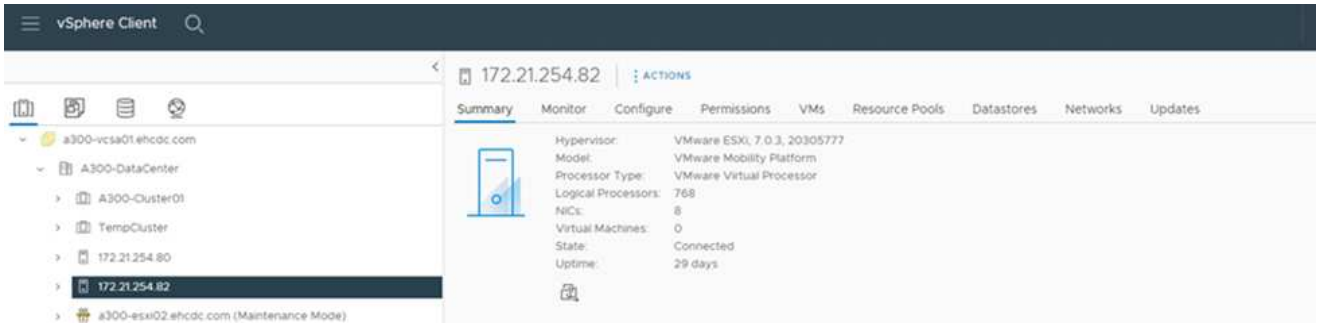
Étape 6 : migration des workloads

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.

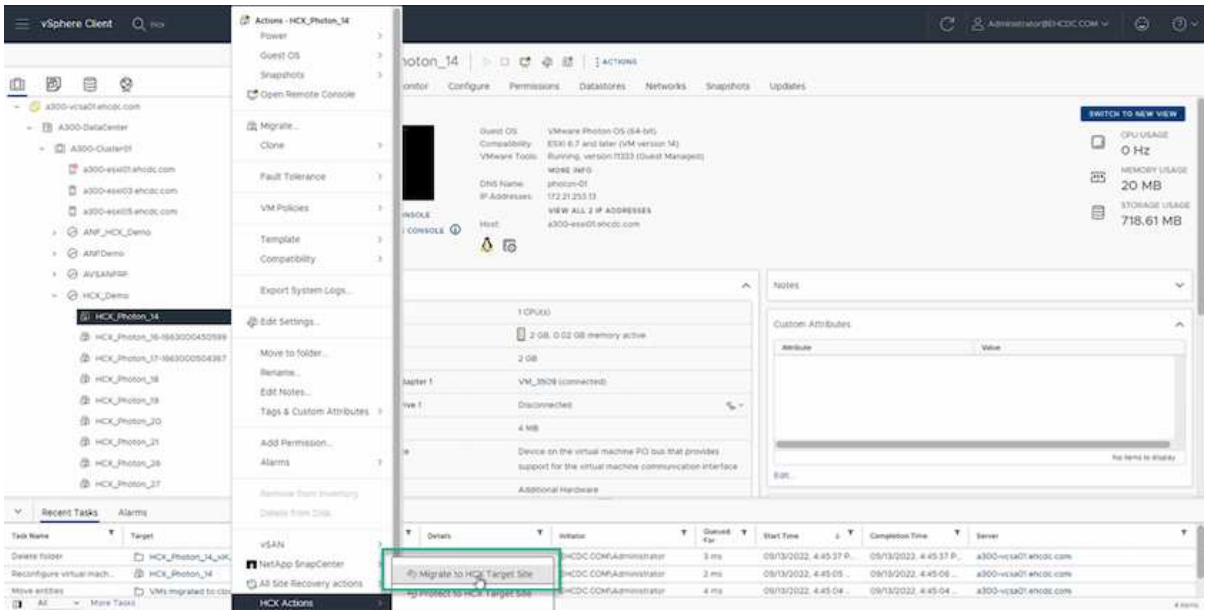


VMware HCX vMotion

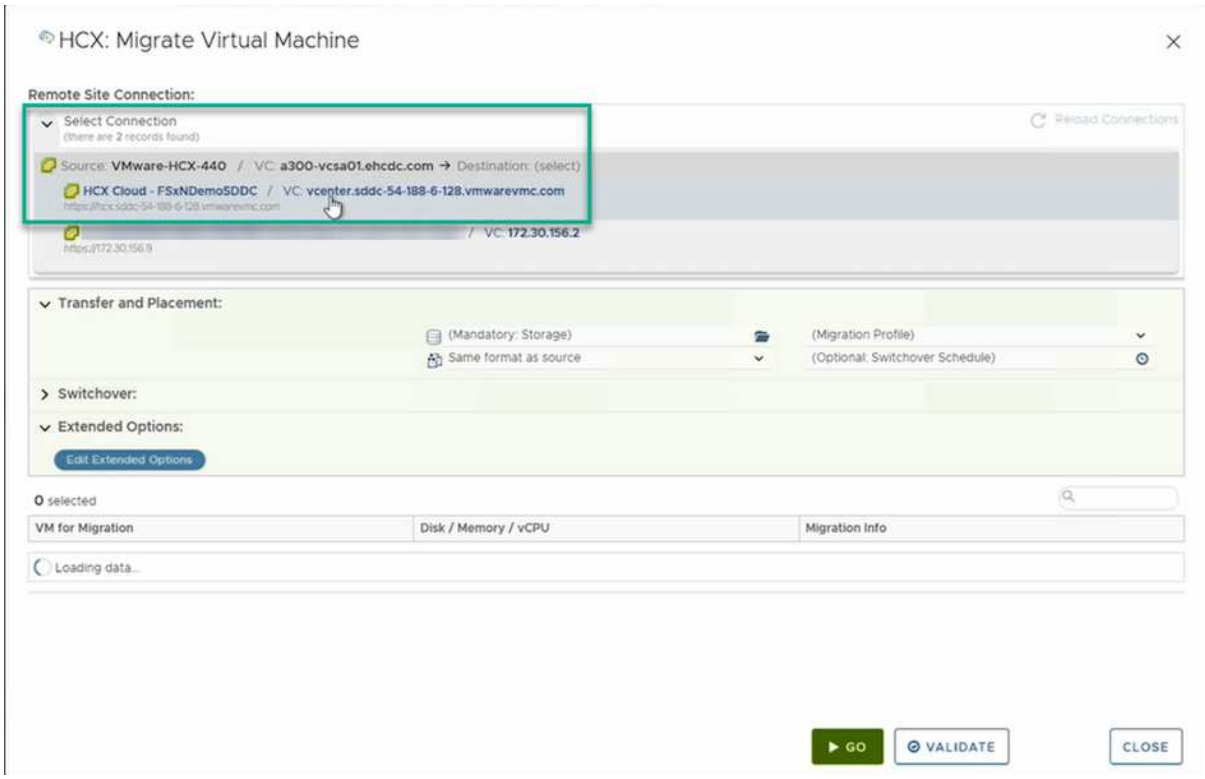
Cette section décrit le mécanisme HCX vMotion. Cette technologie de migration utilise le protocole VMware vMotion pour migrer une machine virtuelle vers un SDDC VMC. L'option de migration vMotion permet de migrer l'état d'une machine virtuelle unique à la fois. Il n'y a pas d'interruption de service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

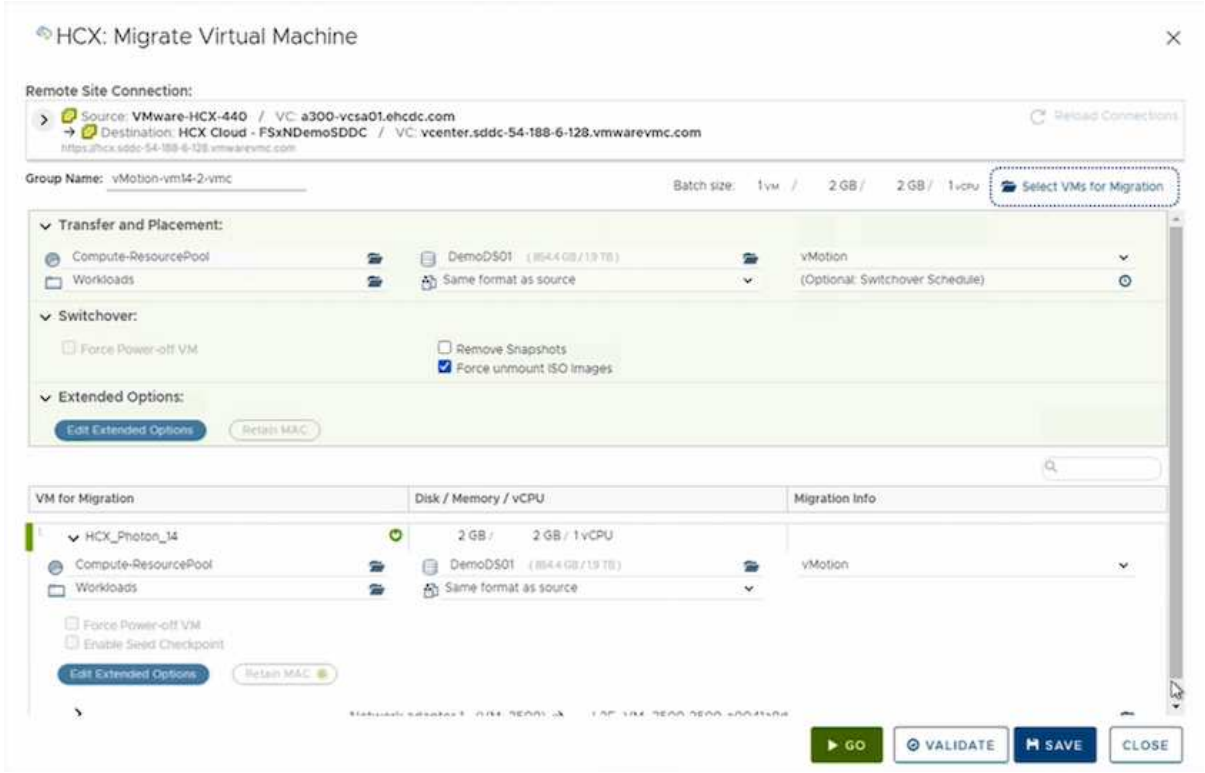
1. Depuis le client vSphere sur site, accédez à Inventory, faites un clic droit sur la machine virtuelle à migrer, puis sélectionnez HCX actions > Migrate to HCX site cible.



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



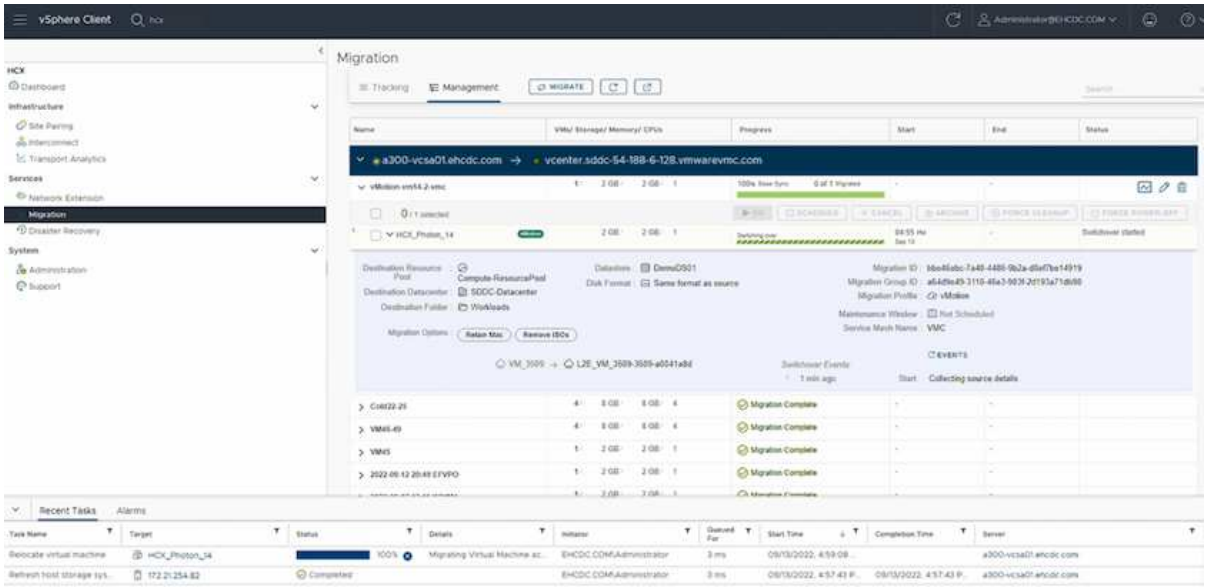
3. Ajoutez un nom de groupe et sous transfert et placement, mettez à jour les champs obligatoires (réseau de cluster, de stockage et de destination), puis cliquez sur Valider.



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".

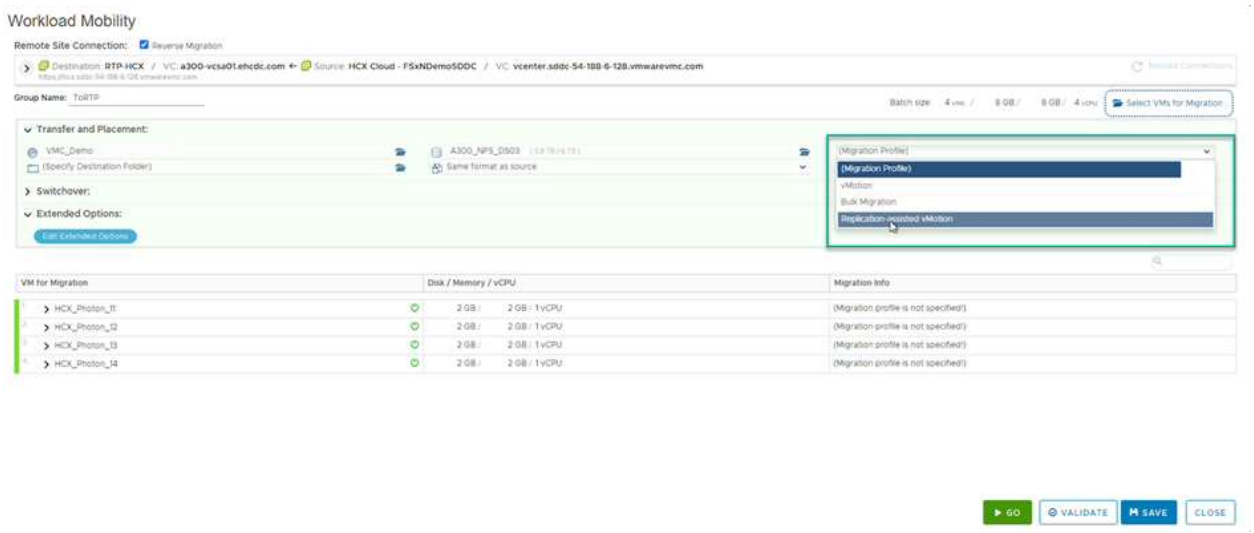
5. Vous pouvez contrôler la progression et l'achèvement de vMotion dans le tableau de bord HCX > migration.



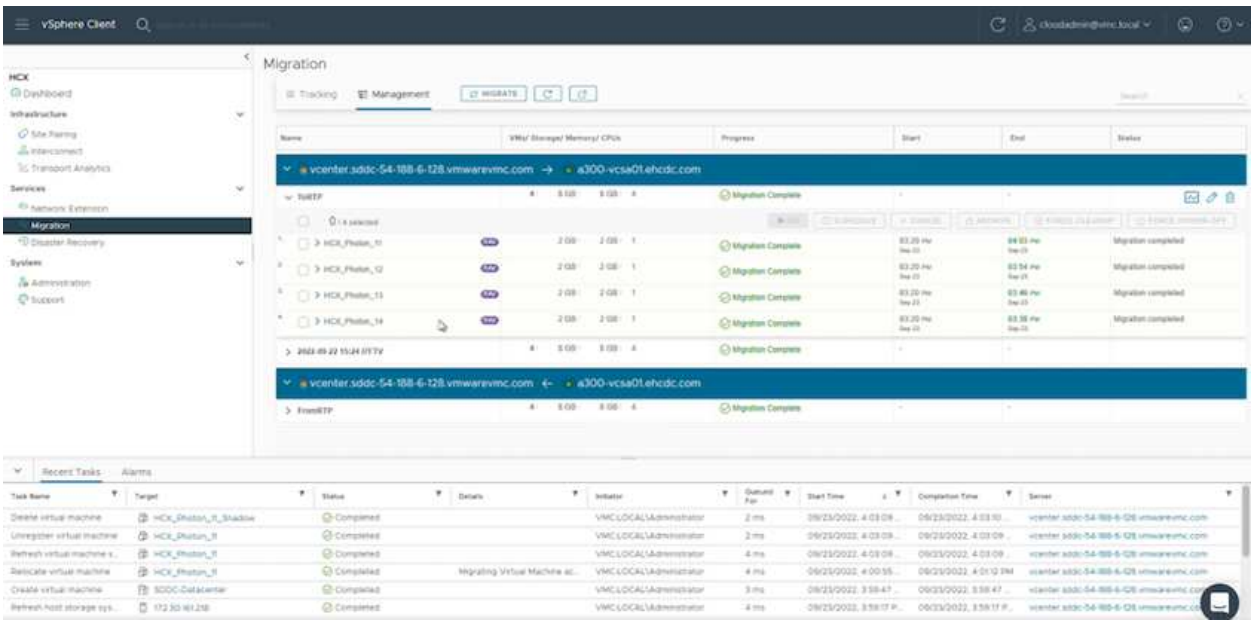
VMware Replication Assisted vMotion

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

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.

Fonctionnalités NetApp pour Azure AVS

Découvrez plus en détail les fonctionnalités que NetApp propose à Azure VMware solution (AVS) : de NetApp en tant que dispositif de stockage connecté à l'invité ou un datastore NFS supplémentaire pour migrer les workflows, étendre/bursting au cloud, sauvegarde/restauration et reprise après incident.

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

- "Configuration d'AVS dans Azure"
- "Options de stockage NetApp pour AVS"
- "Solutions clouds NetApp/VMware"

Configuration d'AVS dans Azure

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 Azure VMware solution et l'utiliser en association avec les options disponibles pour connecter le stockage NetApp.

> Le stockage In-guest est la seule méthode prise en charge de connexion de Cloud Volumes ONTAP à Azure VMware solution.

Le processus de configuration peut être divisé en plusieurs étapes :

- Enregistrez le fournisseur de ressources et créez un cloud privé
- Connectez-vous à une passerelle réseau virtuelle ExpressRoute nouvelle ou existante
- Validation de la connectivité réseau et accès au cloud privé

Afficher les détails "Étapes de configuration de AVS".

Options de stockage NetApp pour AVS

Le stockage NetApp peut être utilisé de plusieurs façons (soit en tant que point de connexion, soit en tant que datastore NFS supplémentaire) dans Azure AVS.

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

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

- Azure NetApp Files (ANF) comme stockage connecté invité
- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- Azure NetApp Files (ANF) comme datastore NFS supplémentaire

Afficher les détails "Option de stockage avec connexion invité pour AVS". Afficher les détails "Options supplémentaires de datastore NFS pour AVS".

Cas d'utilisation de la solution

Avec les solutions cloud de NetApp et VMware, le déploiement dans Azure AVS est très simple. Des cas se sont définis pour chaque domaine cloud défini par VMware :

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

"Découvrez les solutions NetApp pour Azure AVS"

Protection des workloads dans Azure/AVS

Reprise après incident avec ANF et JetStream

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. Grâce à la structure VMware VAIO, les charges de travail VMware sur site peuvent être répliquées vers le stockage Azure Blob et récupérées. Vous bénéficiez ainsi d'une perte de données minimale, voire quasi nulle.

Jetstream DR peut être utilisé pour restaurer de manière transparente les workloads répliqués depuis les sites vers AVS, et plus particulièrement vers Azure NetApp Files. Il permet une reprise d'activité économique en utilisant peu de ressources sur le site de reprise d'activité et un stockage cloud économique. Jetstream DR automatise la restauration vers les datastores ANF via Azure Blob Storage. Jetstream DR restaure les ordinateurs virtuels ou groupes de serveurs virtuels indépendants dans l'infrastructure de site de restauration en fonction du mappage du réseau et assure une restauration instantanée pour la protection par ransomware.

Ce document présente les principes JetStream DR des opérations et de ses principaux composants.

Présentation du déploiement de la solution

1. Installez le logiciel JetStream DR dans le data Center sur site.
   a. Téléchargez le pack logiciel JetStream DR depuis Azure Marketplace (ZIP) et déployez JetStream DR MSA (OVA) dans le cluster désigné.
   b. Configurez le cluster à l'aide du package filtre d'E/S (installez JetStream VIB).
   c. Provisionnez Azure Blob (Azure Storage Account) dans la même région que le cluster AVS pour la reprise après incident.
   d. Déployer des appliances DRVA et attribuer des volumes de journaux de réplication (VMDK à partir d'un datastore existant ou d'un stockage iSCSI partagé).
   e. Créez des domaines protégés (groupes de machines virtuelles associées) et attribuez des DRVAs et Azure Blob Storage/ANF.
   f. Démarrer la protection.
2. Installez le logiciel JetStream DR dans le cloud privé Azure VMware solution.
   a. Utilisez la commande Exécuter pour installer et configurer JetStream DR.
   b. Ajoutez le même conteneur Azure Blob et découvrez les domaines à l'aide de l'option Scan Domains.
   c. Déployer les appareils DRVA requis.
   d. Créez des volumes du journal de réplication à l'aide des datastores VSAN ou ANF disponibles.
   e. Importez des domaines protégés et configurez RocVA (Recovery va) pour utiliser le datastore ANF dans le cadre du placement de VM.
   f. Sélectionnez l'option de basculement appropriée et démarrez la réhydratation continue pour les domaines ou les machines virtuelles RTO proches de zéro.
3. En cas d'incident, déclenchez le basculement vers les datastores Azure NetApp Files sur le site AVS dédié à la reprise après incident.
4. Appelez le rétablissement vers le site protégé après la récupération du site protégé.avant de commencer, assurez-vous que les conditions préalables sont remplies comme indiqué dans le présent document "lien" De plus, exécutez l'outil de test de bande passante (BWT) fourni par JetStream Software pour évaluer les performances potentielles du stockage Azure Blob et de sa bande passante de réplication lorsqu'il est utilisé avec le logiciel JetStream DR. Une fois les conditions requises, y compris la connectivité, mises en place, configurez et abonnez-vous à JetStream DR pour AVS à partir du "Azure Marketplace". Une fois le pack logiciel téléchargé, procédez au processus d'installation décrit ci-dessus.

Lors de la planification et du démarrage de la protection pour un grand nombre de machines virtuelles (par exemple, 100+), utilisez l'outil de planification des capacités (CPT) du kit d'outils JetStream DR Automation. Fournissez une liste des machines virtuelles à protéger avec leurs préférences RTO et de groupes de récupération, puis exécutez CPT.

CPT effectue les fonctions suivantes :

- Combinaison des machines virtuelles dans des domaines de protection selon leur objectif de durée de restauration.
- Définir le nombre optimal de DRVAS et leurs ressources.
- Estimation de la bande passante de réplication requise.

- L’identification des caractéristiques du volume du journal de réplication (capacité, bande passante, etc.)
- Estimation de la capacité de stockage objet requise, etc.

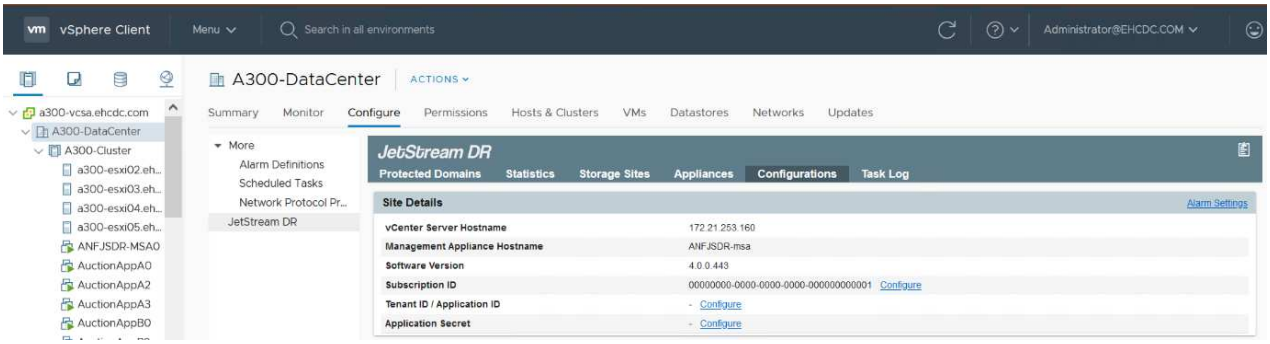
> Le nombre et le contenu des domaines prescrits dépendent de diverses caractéristiques des VM, telles que les IOPS moyennes, la capacité totale, la priorité (qui définit l’ordre de basculement), RTO et autres.

Installer JetStream DR dans le data Center sur site

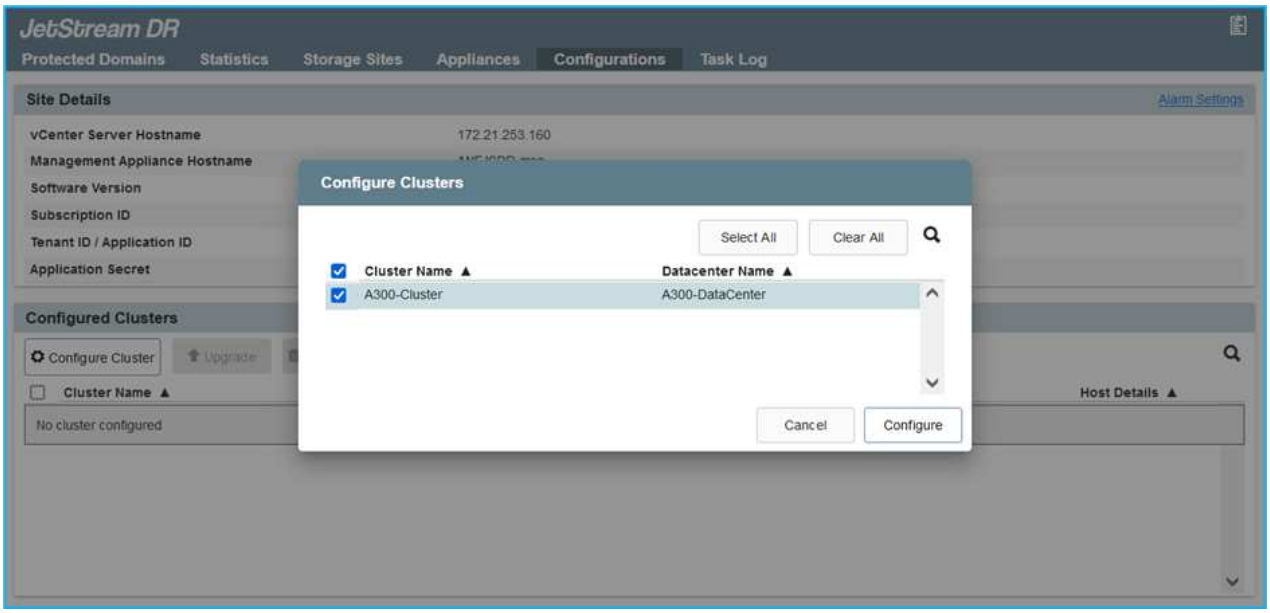
Le logiciel Jetstream DR est constitué de trois composants principaux : le serveur virtuel Jetstream DR Management Server (MSA), le dispositif virtuel DR (DRVA) et les composants hôtes (packages de filtres d’E/S). MSA est utilisé pour installer et configurer des composants hôtes sur le cluster de calcul, puis pour administrer le logiciel JetStream DR. La liste suivante fournit une description générale du processus d’installation :

Comment installer JetStream DR sur site

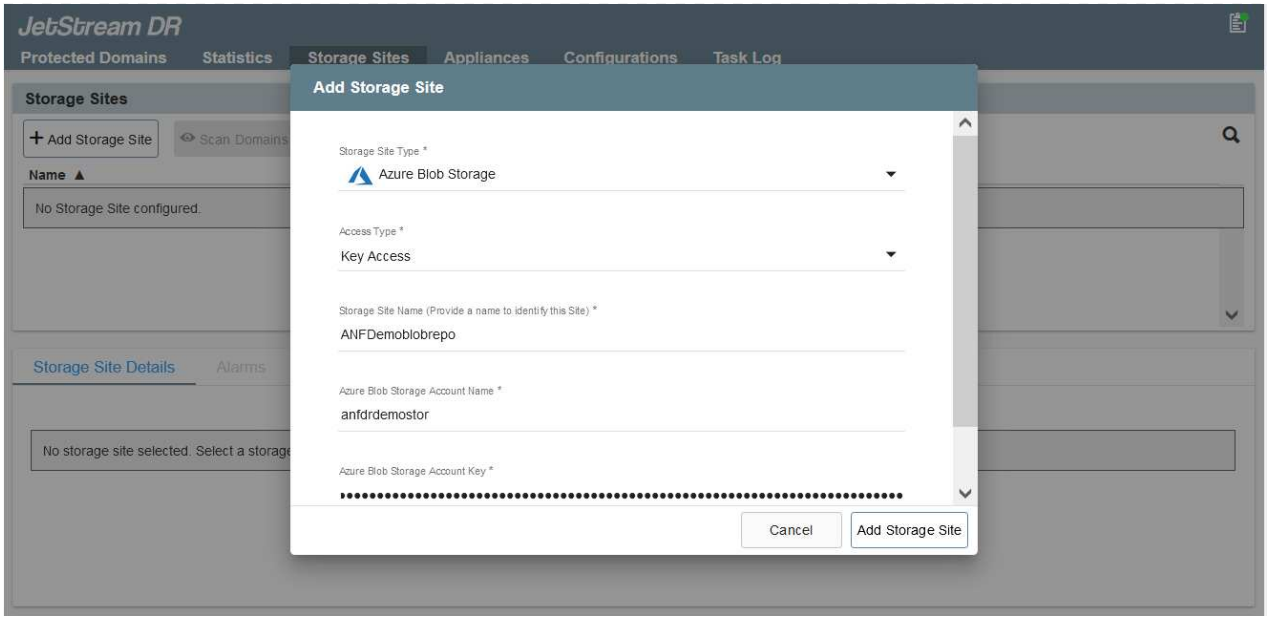
1. Vérifier les prérequis.
2. Exécutez l'outil de planification de la capacité pour obtenir des recommandations en matière de ressources et de configuration (facultatif, mais recommandé pour les essais de validation).
3. Déployez JetStream DR MSA sur un hôte vSphere du cluster désigné.
4. Lancez le MSA à l'aide de son nom DNS dans un navigateur.
5. Enregistrez le serveur vCenter avec MSA.pour effectuer l'installation, procédez comme suit :
6. Après le déploiement de JetStream DR MSA et l'enregistrement du serveur vCenter, accédez au plug-in JetStream DR à l'aide du client Web vSphere. Pour ce faire, accédez à Datacenter > configurer > JetStream DR.



7. Dans l'interface JetStream DR, sélectionnez le cluster approprié.



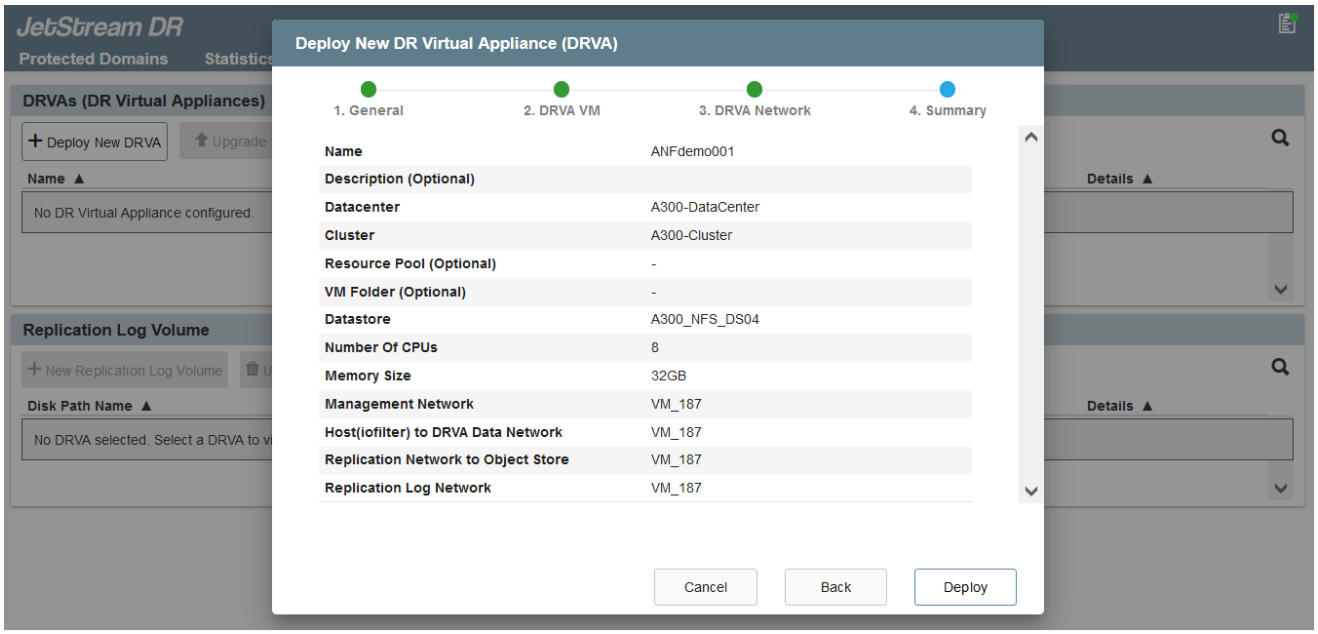
8. Configurez le cluster avec le package de filtre d'E/S.



9. Ajoutez un stockage Azure Blob Storage situé sur le site de reprise.
10. Déployez une appliance DR virtuelle (DRVA) depuis l'onglet Appliances.

> Les DRVAS peuvent être créés automatiquement par CPT, mais pour les tests POC, nous vous recommandons de configurer et d'exécuter manuellement le cycle de reprise après incident (démarrer la protection > basculement > retour arrière).

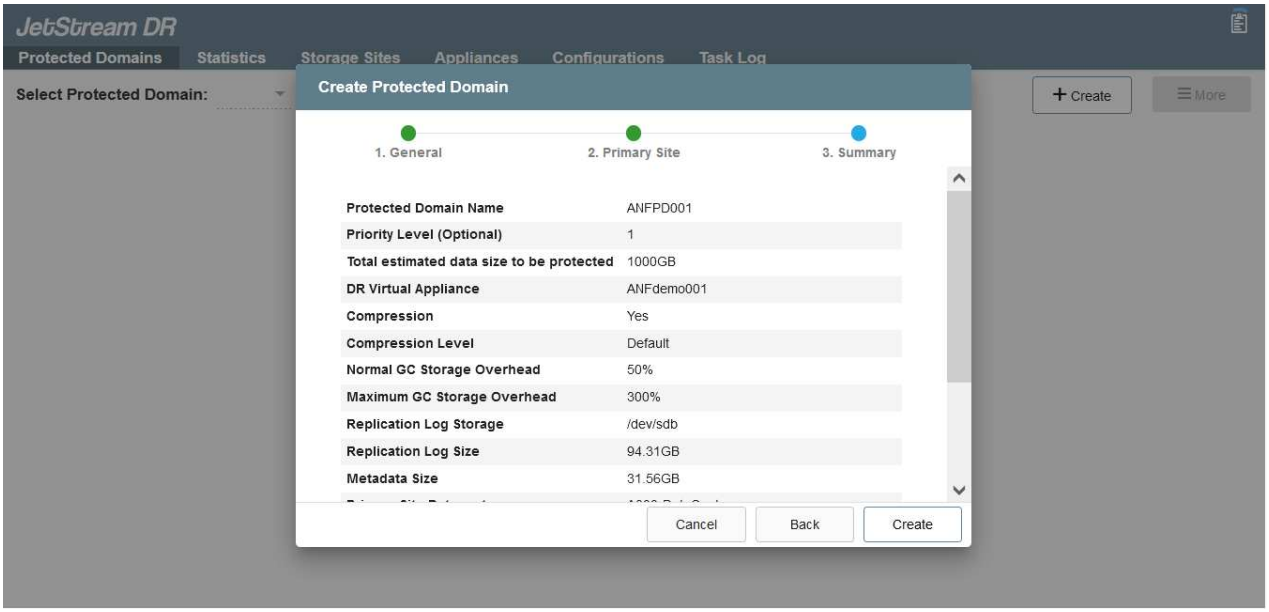
JetStream DRVA est une appliance virtuelle qui facilite les principales fonctions du processus de réplication des données. Un cluster protégé doit contenir au moins un DRVA et, en général, un DRVA est configuré par hôte. Chaque DRVA peut gérer plusieurs domaines protégés.



Dans cet exemple, quatre DRVA ont été créés pour 80 machines virtuelles.

1. Créez des volumes de journal de réplication pour chaque DRVA à l'aide de VMDK provenant des datastores disponibles ou des pools de stockage iSCSI partagés indépendants.

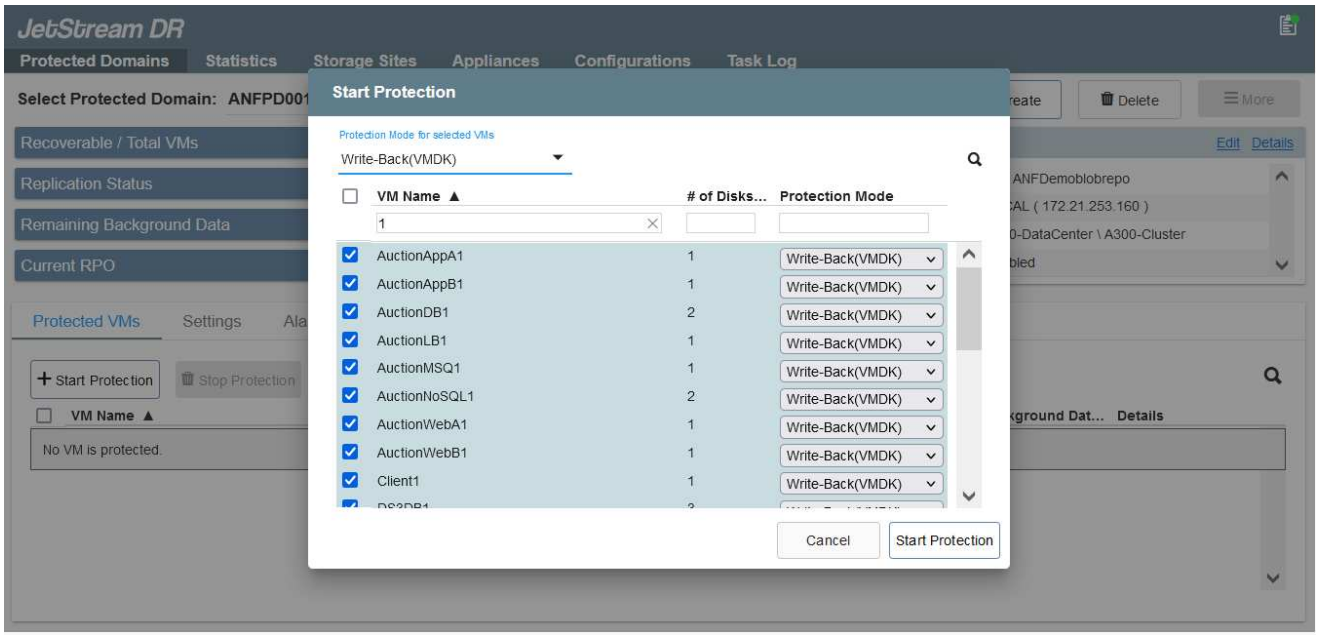
2. À partir de l'onglet domaines protégés, créez le nombre requis de domaines protégés à l'aide des informations concernant le site Azure Blob Storage, l'instance DRVA et le journal de réplication. Un domaine protégé définit un ordinateur virtuel ou un ensemble de serveurs virtuels dans le cluster qui sont protégés ensemble et se voit attribuer un ordre de priorité pour les opérations de basculement/retour arrière.



3. Sélectionnez les machines virtuelles que vous souhaitez protéger et démarrez la protection des machines virtuelles du domaine protégé. La réplication des données commence alors dans le magasin d'objets blob désigné.

Vérifier que le même mode de protection est utilisé pour toutes les VM d'un domaine protégé.

Le mode Write- Back (VMDK) peut offrir de meilleures performances.



Vérifier que les volumes des journaux de réplication sont placés sur un stockage haute performance.

> Les guides d'exécution de basculement peuvent être configurés pour regrouper les VM (appelés groupes de récupération), définir l'ordre de démarrage et modifier les paramètres CPU/mémoire avec les configurations IP.

Installez JetStream DR pour AVS dans un cloud privé Azure VMware solution à l'aide de la commande Exécuter

Il est recommandé de créer à l'avance un cluster Pilot-light à trois nœuds sur le site de récupération (AVS). L'infrastructure du site de reprise peut ainsi être préconfigurée, incluant les éléments suivants :

- Segments de réseau de destination, pare-feu, services comme DHCP et DNS, etc.
- Installation de JetStream DR pour AVS
- La configuration des volumes ANF en tant que datastores, et moreJetStream DR prend en charge le mode RTO quasi-nul pour les domaines stratégiques. Pour ces domaines, le stockage de destination doit être préinstallé. ANF est un type de stockage recommandé dans ce cas.

> La configuration réseau comprenant la création de segments doit être configurée sur le cluster AVS afin de répondre aux exigences sur site.

Selon les exigences des niveaux de service et de l'objectif RTO, il est possible d'utiliser un mode de basculement continu ou standard. Pour un RTO proche de zéro, la réhydratation continue doit être mise sur le site de reprise.

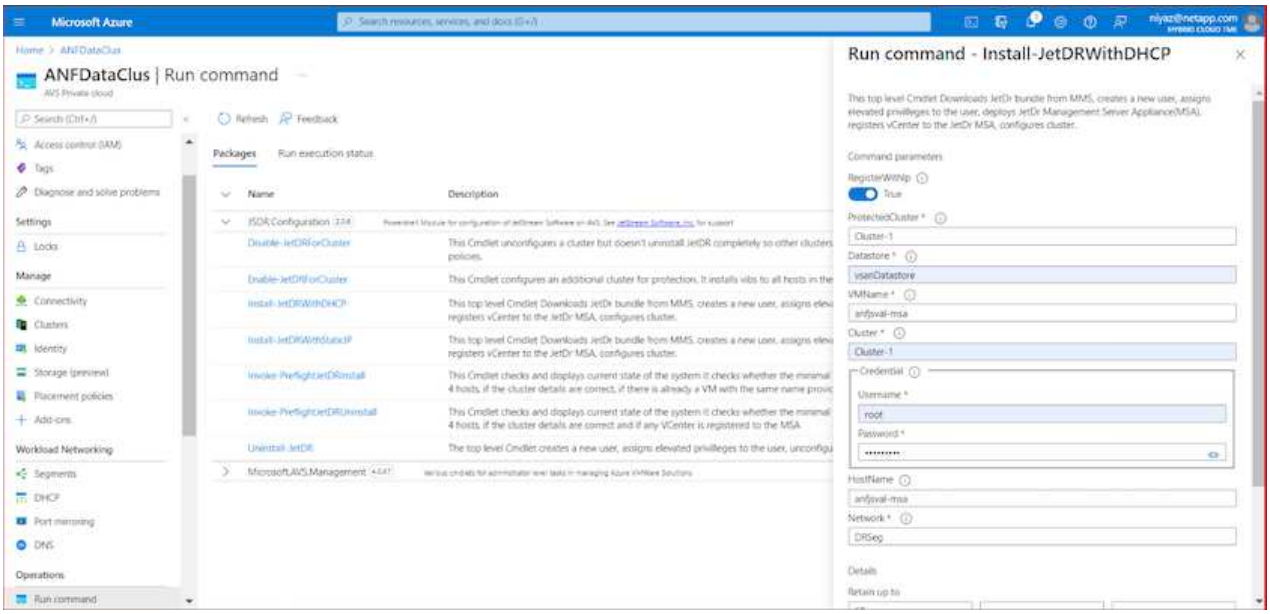
Comment installer JetStream DR pour AVS dans un cloud privé

Pour installer JetStream DR pour AVS sur un cloud privé Azure VMware solution, procédez comme suit :

1. Depuis le portail Azure, accédez à la solution Azure VMware, sélectionnez le cloud privé et sélectionnez Exécuter la commande > packages > JSDR.Configuration.

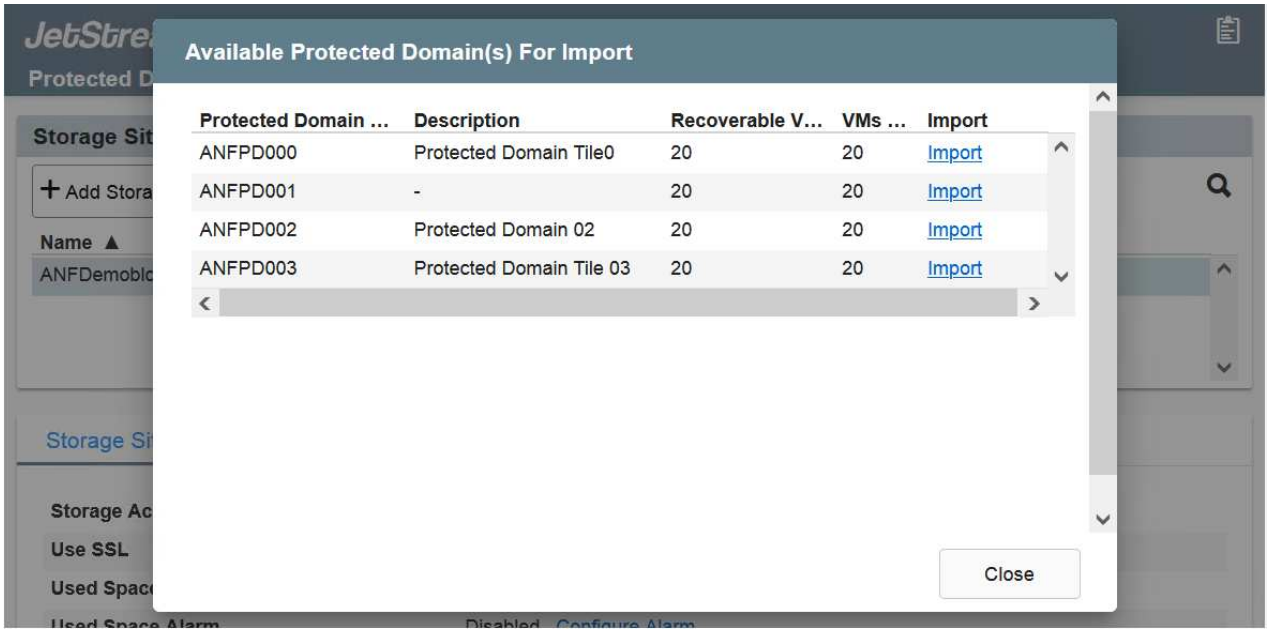
   > L'utilisateur CloudAdmin par défaut dans Azure VMware solution ne dispose pas des privilèges suffisants pour installer JetStream DR pour AVS. Azure VMware solution permet une installation simplifiée et automatisée de JetStream DR en appelant la commande Azure VMware solution Run pour JetStream DR.

   La capture d'écran suivante montre l'installation à l'aide d'une adresse IP DHCP.



2. Une fois l'installation de JetStream DR pour AVS terminée, actualisez le navigateur. Pour accéder à l'interface de reprise après incident JetStream, allez dans SDDC Datacenter > configurer > JetStream DR.

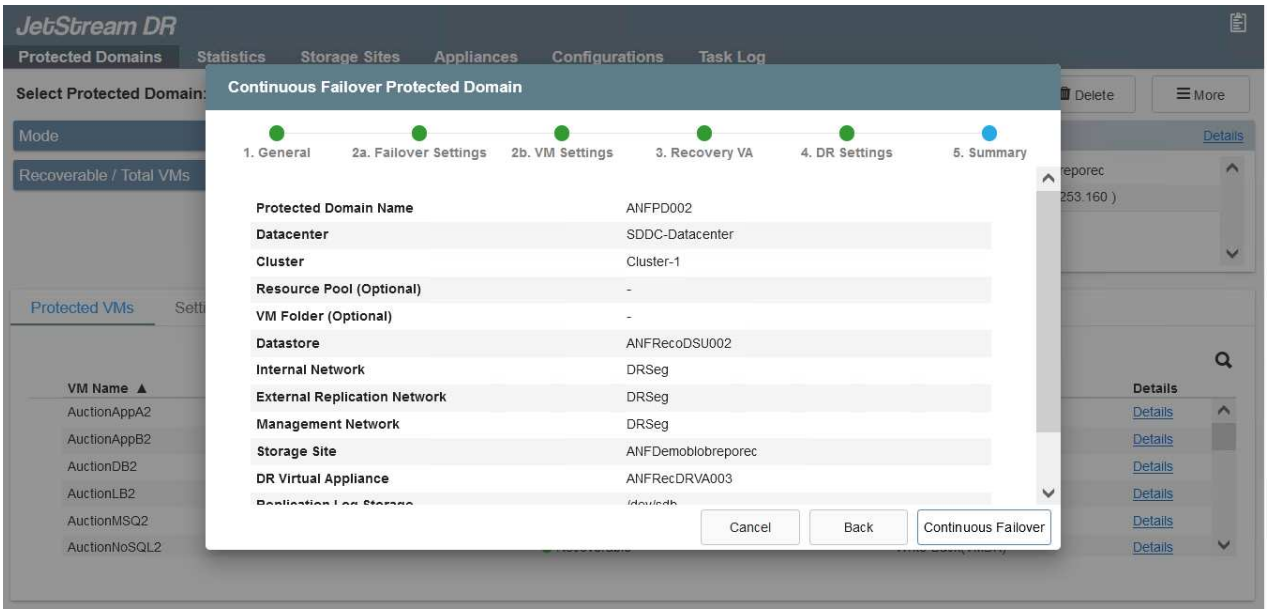
3. À partir de l'interface JetStream DR, ajoutez le compte Azure Blob Storage utilisé pour protéger le cluster sur site en tant que site de stockage, puis exécutez l'option Scan Domains.



4. Une fois les domaines protégés importés, déployez les appareils DRVA. Dans cet exemple, la réhydratation continue est lancée manuellement à partir du site de restauration à l'aide de l'interface utilisateur JetStream DR.

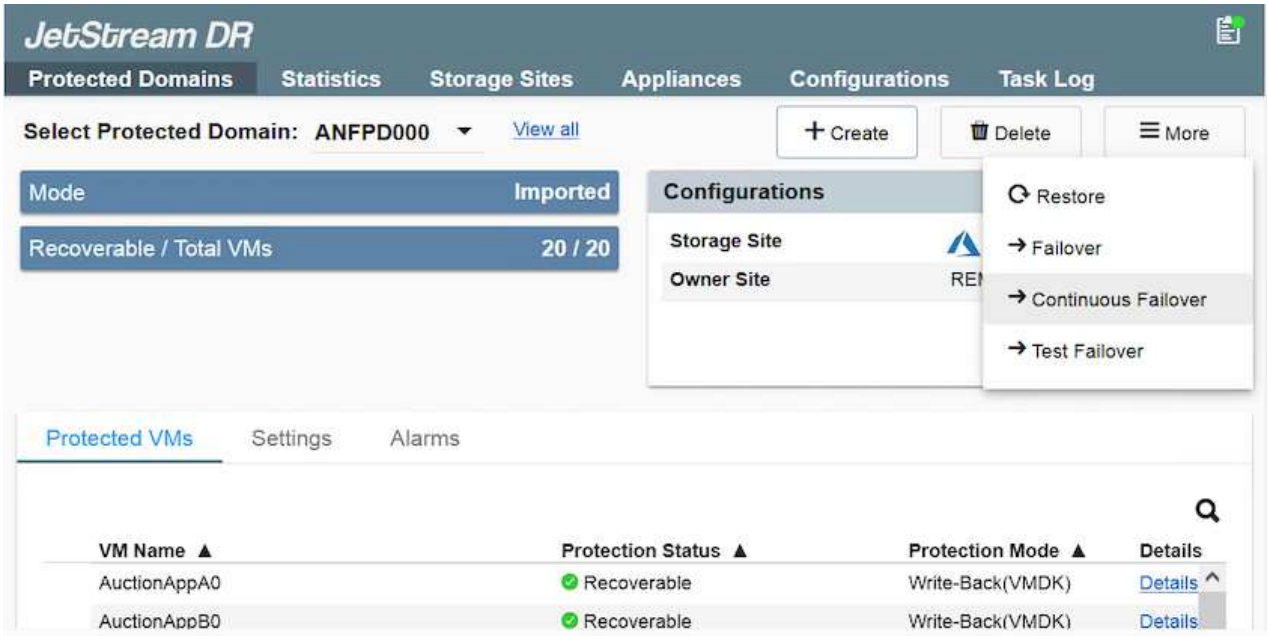
> Ces étapes peuvent également être automatisées à l'aide de plans créés par CPT.

5. Créez des volumes du journal de réplication à l'aide des datastores VSAN ou ANF disponibles.
6. Importez les domaines protégés et configurez le va de restauration de manière à utiliser le datastore ANF pour le positionnement des VM.



> Assurez-vous que DHCP est activé sur le segment sélectionné et qu'un nombre suffisant d'adresses IP est disponible. Des adresses IP dynamiques sont utilisées temporairement pendant la restauration des domaines. Chaque machine virtuelle de restauration (y compris la réhydratation continue) requiert une adresse IP dynamique individuelle. Une fois la récupération terminée, le IP est libéré et peut être réutilisé.

7. Sélectionnez l'option de basculement appropriée (basculement continu ou basculement). Dans cet exemple, la réhydratation continue (basculement continu) est sélectionnée.



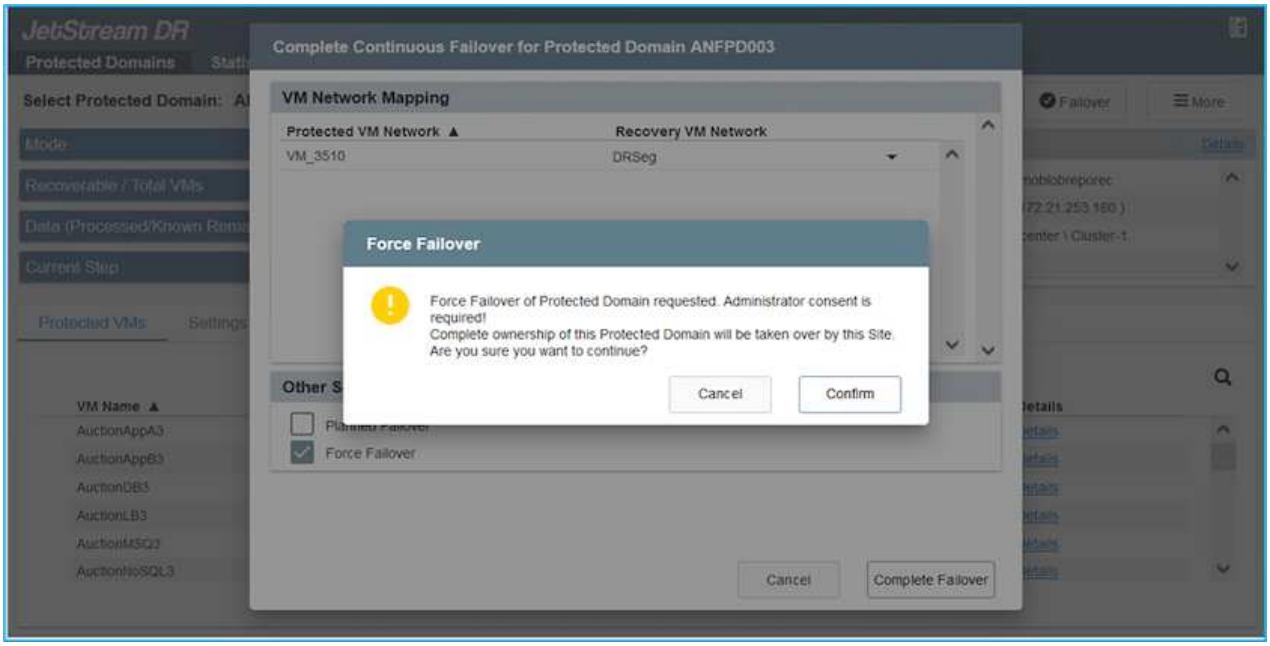
Exécution du basculement/retour arrière

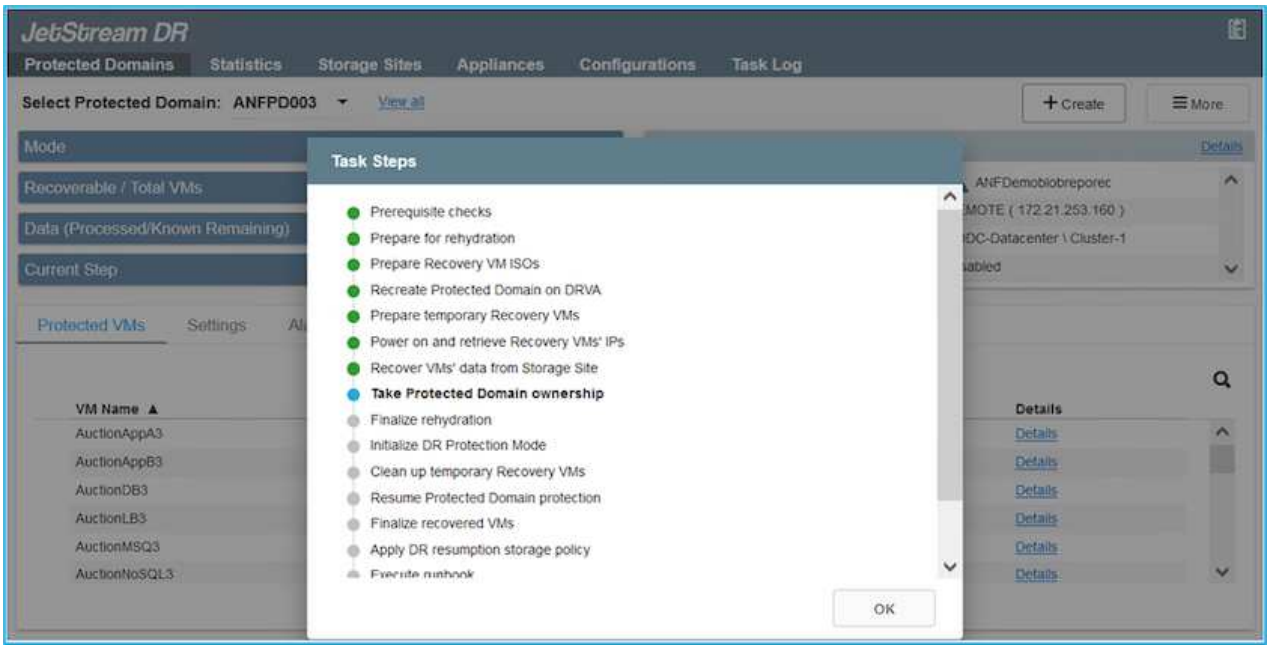
Comment effectuer un basculement/retour arrière

1. Après un incident se produit dans le cluster protégé de l'environnement sur site (défaillance partielle ou complète), déclencher le basculement.

   CPT peut être utilisé pour exécuter le plan de basculement pour restaurer les machines virtuelles à partir d'Azure Blob Storage vers le site de restauration du cluster AVS.

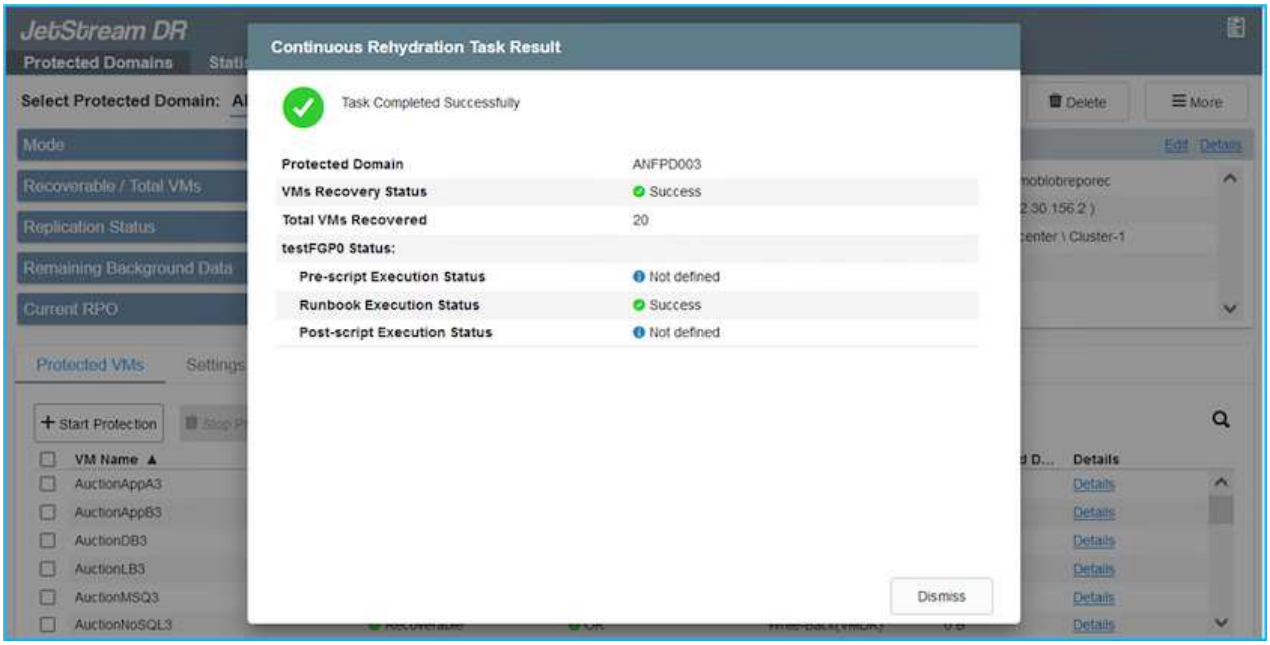
   Après le basculement (pour la réhydratation en continu ou standard) lorsque les machines virtuelles protégées ont été lancées dans AVS, la protection reprend automatiquement et la reprise après incident JetStream continue de répliquer leurs données dans les conteneurs appropriés/originaux dans Azure Blob Storage.





La barre des tâches affiche la progression des activités de basculement.

2. Une fois la tâche terminée, accédez aux machines virtuelles récupérées et l'entreprise continue d'être opérationnelle normalement.

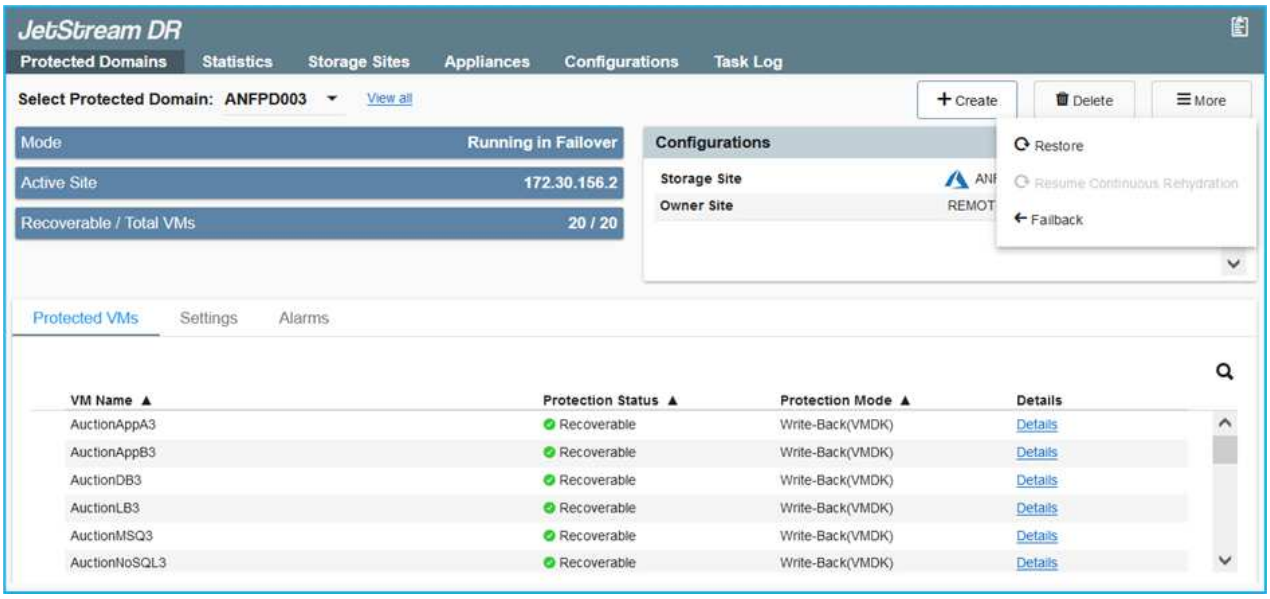


Une fois que le site primaire est à nouveau opérationnel, le retour arrière peut être effectué. La protection des machines virtuelles est reprise et la cohérence des données doit être vérifiée.

3. Restaurer l'environnement sur site. Selon le type d'incident, il peut être nécessaire de restaurer et/ou de vérifier la configuration du cluster protégé. Si nécessaire, il peut être nécessaire de réinstaller le logiciel JetStream DR.

> Remarque : le `recovery_utility_prepare_failback` Le script fourni dans le kit d'automatisation peut être utilisé pour nettoyer le site protégé d'origine de toutes les machines virtuelles obsolètes, des informations de domaine, etc.

4. Accédez à l'environnement sur site restauré, accédez à l'interface utilisateur Jetstream DR et sélectionnez le domaine protégé approprié. Une fois que le site protégé est prêt à être restauré, sélectionnez l'option de retour arrière dans l'interface utilisateur.



Le plan de restauration généré par CPT peut également être utilisé pour initier le retour des VM et de leurs données du magasin d'objets vers l'environnement VMware d'origine.

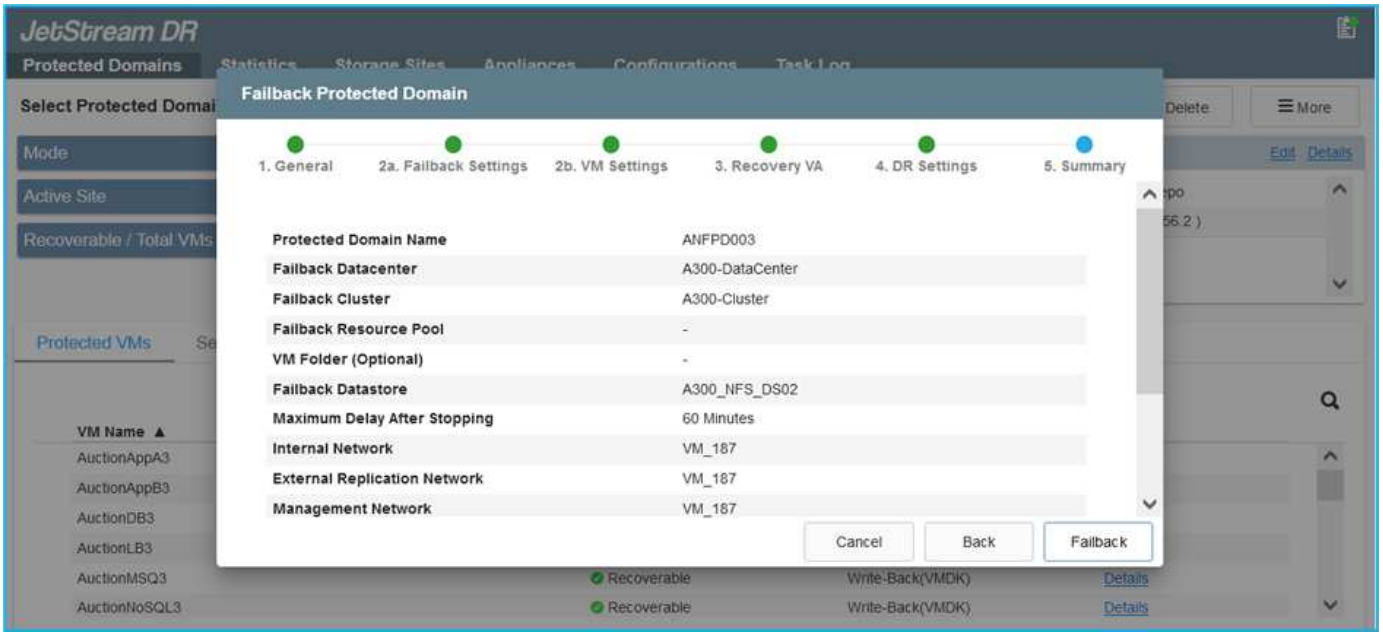
Spécifier le délai maximal après la mise en pause des VM dans le site de reprise et leur redémarrage sur le site protégé. Cette durée comprend l'exécution de la réplication après l'arrêt des machines virtuelles de basculement, la propreté du site de restauration et la recréation des machines virtuelles sur le site protégé. La valeur recommandée par NetApp est de 10 minutes.

Exécuter le processus de retour arrière, puis confirmer la reprise de la protection des machines virtuelles et de la cohérence des données.

Récupération de Rantomeware

Récupérer des données suite à un ransomware peut être une tâche extrêmement fastidieuse. En particulier, il peut être difficile pour les services IT de déterminer le point de retour sûr et, une fois déterminé, de garantir la protection des charges de travail récupérées contre les attaques se reproduisant (contre les programmes malveillants en veille ou à l'aide d'applications vulnérables).

Jetstream DR pour AVS avec les datastores Azure NetApp Files peut résoudre ces problèmes en permettant aux entreprises de récupérer les données à partir de points disponibles dans le temps, de sorte que les charges de travail soient récupérées sur un réseau fonctionnel et isolé si nécessaire. La récupération permet aux applications de fonctionner et de communiquer entre elles sans les exposer au trafic nord- sud, offrant ainsi aux équipes de sécurité un endroit sûr pour effectuer des analyses et autres corrections nécessaires.



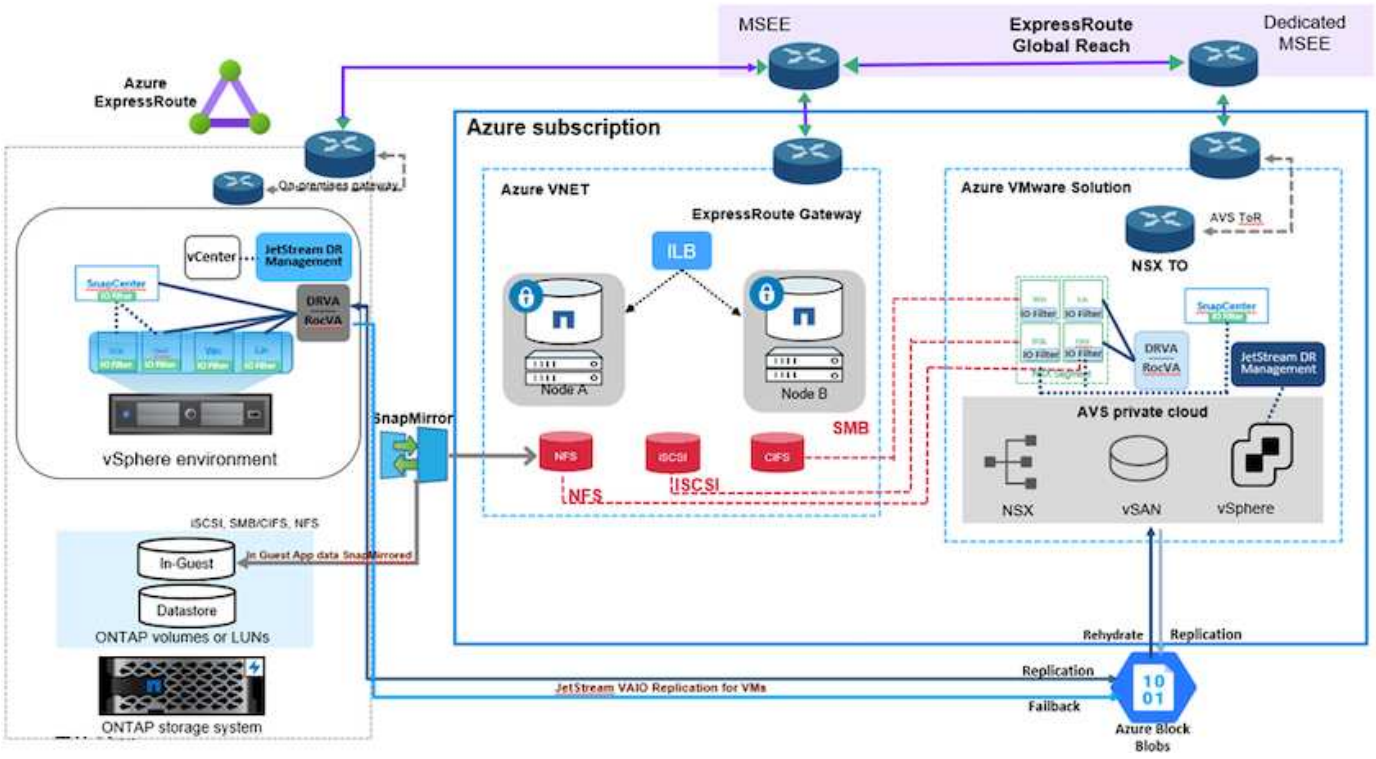
Reprise après incident avec CVO et AVS (stockage connecté à l'invité)

Présentation

Auteurs : Ravi BCB et Niyaz Mohamed, NetApp

La reprise d'activité dans le cloud est une solution résiliente et économique qui protège les charges de travail contre les pannes sur site et la corruption des données, comme les attaques par ransomware. NetApp SnapMirror permet de répliquer les charges de travail VMware sur site utilisant un stockage connecté à l'invité vers NetApp Cloud Volumes ONTAP exécuté dans Azure. Il s'agit aussi des données applicatives, mais qu'en est-il des machines virtuelles elles-mêmes ? La reprise sur incident doit couvrir tous les composants dépendants, notamment les machines virtuelles, les VMDK ou les données d'application. Pour ce faire, SnapMirror et Jetstream peuvent être utilisés pour restaurer de manière transparente les charges de travail répliquées sur site vers Cloud Volumes ONTAP tout en utilisant le stockage VSAN pour les VMDK de VM.

Ce document présente une approche détaillée de la configuration et des performances de la reprise après incident à l'aide de NetApp SnapMirror, JetStream et d'Azure VMware solution (AVS).



Hypothèses

Ce document est axé sur le stockage invité pour les données d'applications (également appelé « invité connecté »), et nous supposons que l'environnement sur site utilise SnapCenter pour assurer des sauvegardes cohérentes au niveau des applications.

> Ce document s'applique à toute solution de sauvegarde et de restauration tierce. En fonction de la solution utilisée dans l'environnement, suivez les bonnes pratiques pour créer des stratégies de sauvegarde conformes aux SLA de l'entreprise.

Pour la connectivité entre l'environnement sur site et le réseau virtuel Azure, utilisez la voie express à portée globale ou un WAN virtuel avec une passerelle VPN. Les segments doivent être créés en fonction de la conception VLAN sur site.

> Plusieurs options de connexion des data centers sur site à Azure restent disponibles. Ainsi, nous ne pouvons pas présenter un workflow spécifique dans ce document. Pour en savoir plus sur la méthode de connectivité, consultez la documentation Azure.

Déploiement de la solution de reprise d'activité

Présentation du déploiement de la solution

1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de Cloud Manager dans l'abonnement et le réseau virtuel appropriés.
    a. Configurer SnapMirror pour les volumes applicatifs concernés.

b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.

3. Installez le logiciel JetStream DR dans le data Center sur site et commencez à protéger les machines virtuelles.
4. Installez le logiciel JetStream DR dans le cloud privé Azure VMware solution.
5. En cas d'incident, interrompre la relation SnapMirror avec Cloud Manager et déclencher le basculement des machines virtuelles vers des datastores Azure NetApp Files ou VSAN sur le site AVS dédié.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
6. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Azure et répliquez les volumes dans CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Azure ("Lien") Et répliquez les volumes souhaités dans Cloud Volumes ONTAP avec les fréquences et les instantanés souhaités.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB
✓	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB
✓	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB

Configurez l’accès aux données des hôtes AVS et CVO

Deux facteurs importants à prendre en compte lors du déploiement d’un SDDC sont la taille du cluster SDDC dans la solution Azure VMware et le délai de conservation d’un SDDC. Ces deux considérations clés à prendre en compte dans une solution de reprise sur incident permettent de réduire les coûts d’exploitation globaux. Le SDDC peut héberger jusqu’à trois hôtes, tout comme un cluster multi-hôtes dans un déploiement à grande échelle.

La décision de déployer un cluster AVS se base principalement sur les exigences en matière de RPO/RTO. Avec la solution Azure VMware, le SDDC peut être provisionné dans le temps en préparation des tests ou d’un incident. Un SDDC déployé juste à temps fait gagner des coûts d’hôtes ESXi lorsque vous ne traitez pas d’incident. Néanmoins, ce type de déploiement affecte le RTO de quelques heures lors du provisionnement du SDDC.

L’option la plus courante consiste à faire fonctionner le SDDC en mode de fonctionnement toujours actif avec un voyant allumé. Cette option réduit l’empreinte de trois hôtes disponibles en continu et accélère les opérations de reprise en fournissant une base en cours d’exécution pour les activités de simulation et les vérifications de conformité, ce qui évite le risque de dérive opérationnelle entre les sites de production et de reprise. Le cluster de lampe témoin peut être rapidement étendu au niveau souhaité si nécessaire pour gérer un événement de reprise après incident réel.

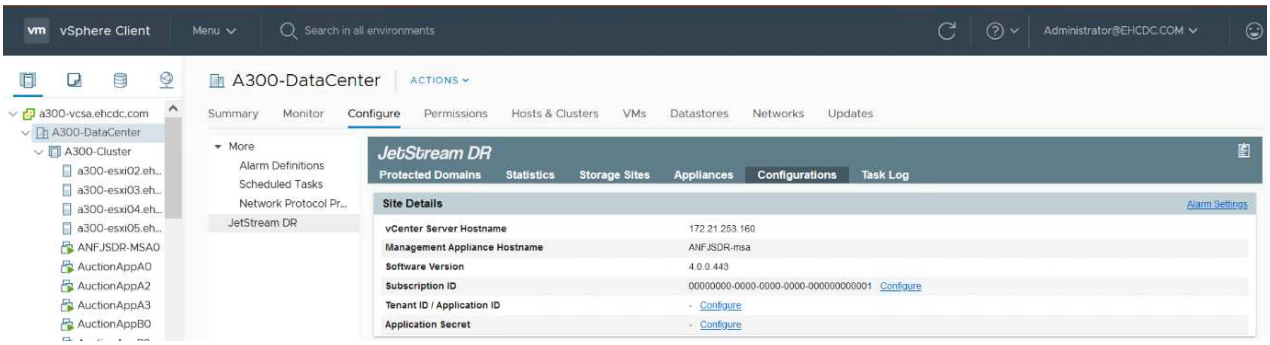
Pour configurer AVS (qu’il s’agit de IT à la demande ou en mode témoin lumineux), voir "Déploiement et configuration de l’environnement de virtualisation sur Azure". Avant cela, vérifiez que les machines virtuelles invitées résidant sur les hôtes AVS peuvent consommer des données depuis Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et AVS ont été correctement configurés, commencez par configurer Jetstream pour automatiser la restauration des charges de travail sur site vers AVS (machines virtuelles avec VMDK des applications et machines virtuelles avec stockage « Guest ») à l’aide du mécanisme VAIO et en exploitant SnapMirror pour les copies de volumes d’applications vers Cloud Volumes ONTAP.

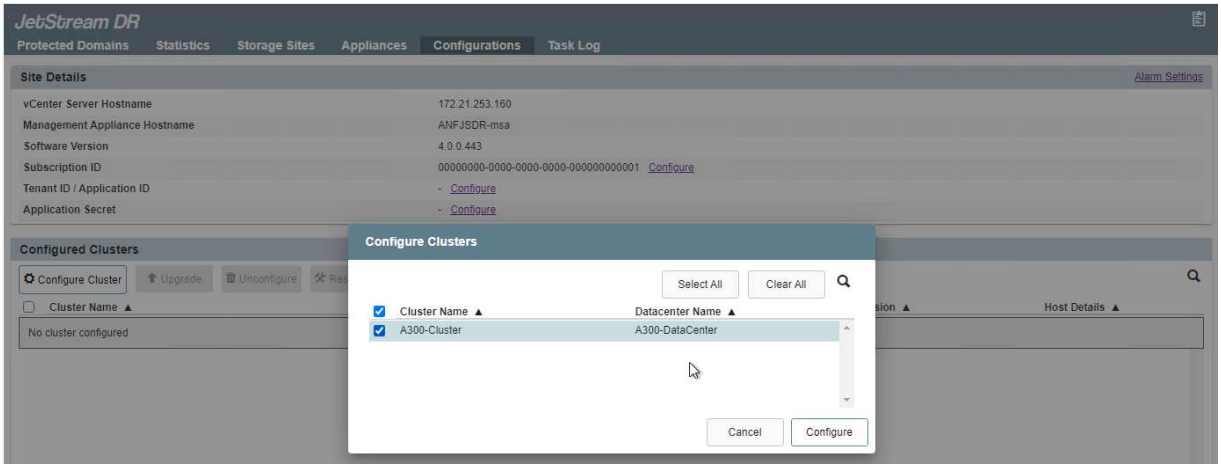
Installer JetStream DR dans le data Center sur site

Le logiciel Jetstream DR est constitué de trois composants principaux : le serveur virtuel JetStream DR Management Server (MSA), le dispositif virtuel DR (DRVA) et les composants hôtes (packages de filtres E/S). MSA est utilisé pour installer et configurer des composants hôtes sur le cluster de calcul, puis pour administrer le logiciel JetStream DR. La procédure d'installation est la suivante :

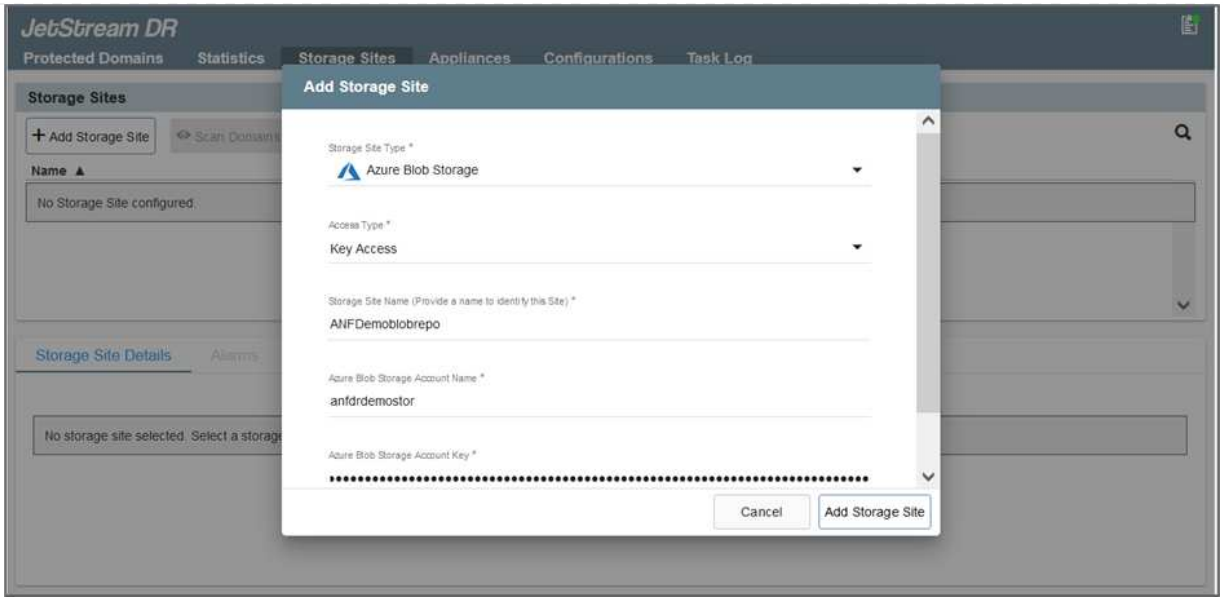
1. Vérifiez les prérequis.
2. Exécutez l'outil de planification de la capacité pour obtenir des recommandations en matière de ressources et de configuration.
3. Déployez JetStream DR MSA sur chaque hôte vSphere du cluster désigné.
4. Lancez le MSA à l'aide de son nom DNS dans un navigateur.
5. Enregistrez le serveur vCenter avec MSA.
6. Après le déploiement de JetStream DR MSA et l'enregistrement du serveur vCenter, accédez au plug-in JetStream DR avec le client Web vSphere. Pour ce faire, accédez à Datacenter > configurer > JetStream DR.



7. À partir de l'interface JetStream DR, effectuez les tâches suivantes :
   a. Configurez le cluster avec le package de filtre d'E/S.

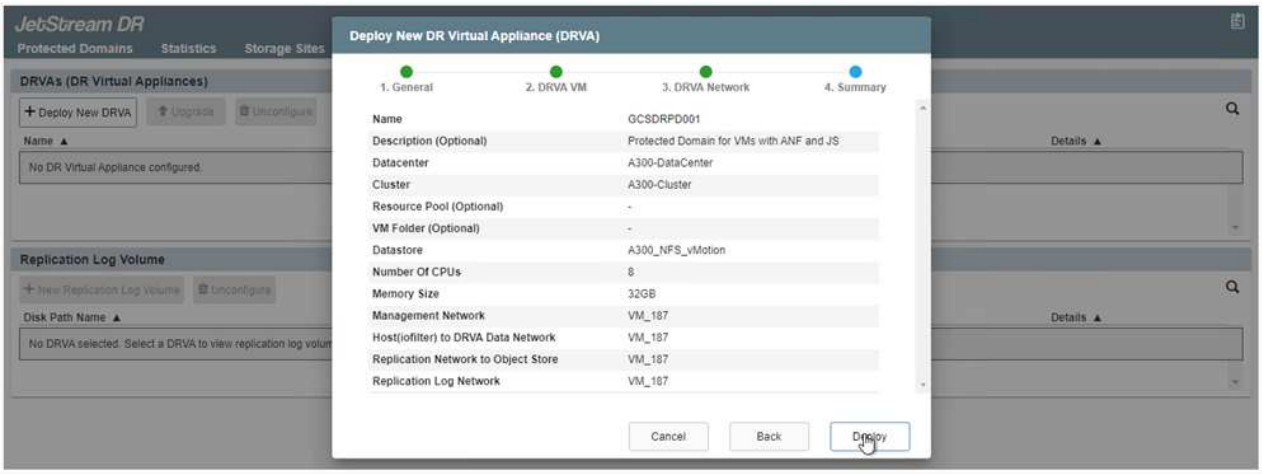


   b. Ajoutez le stockage Azure Blob situé sur le site de reprise.

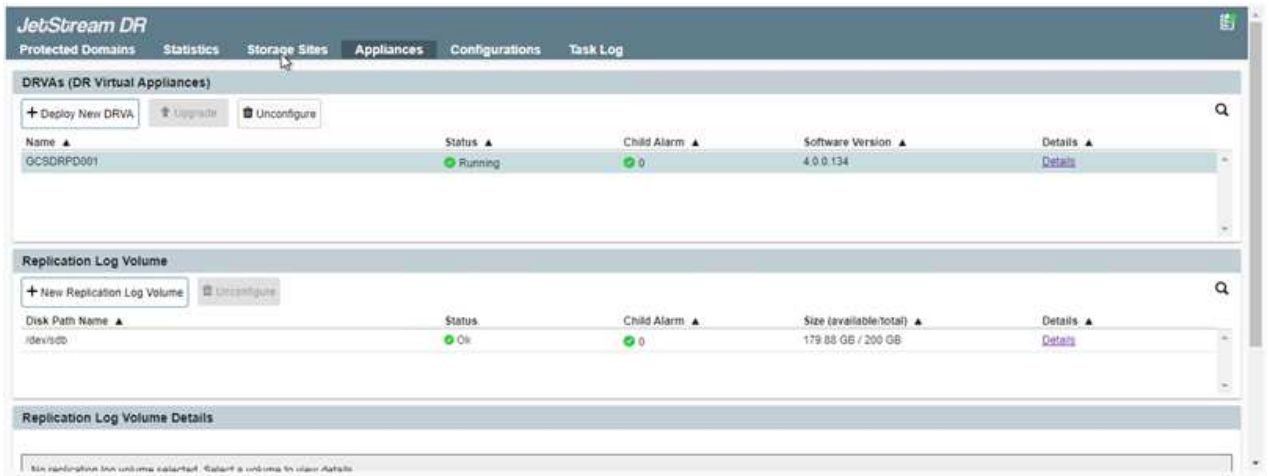


8. Déployez le nombre requis d'appliances virtuelles de reprise sur incident (DR) dans l'onglet appliances.

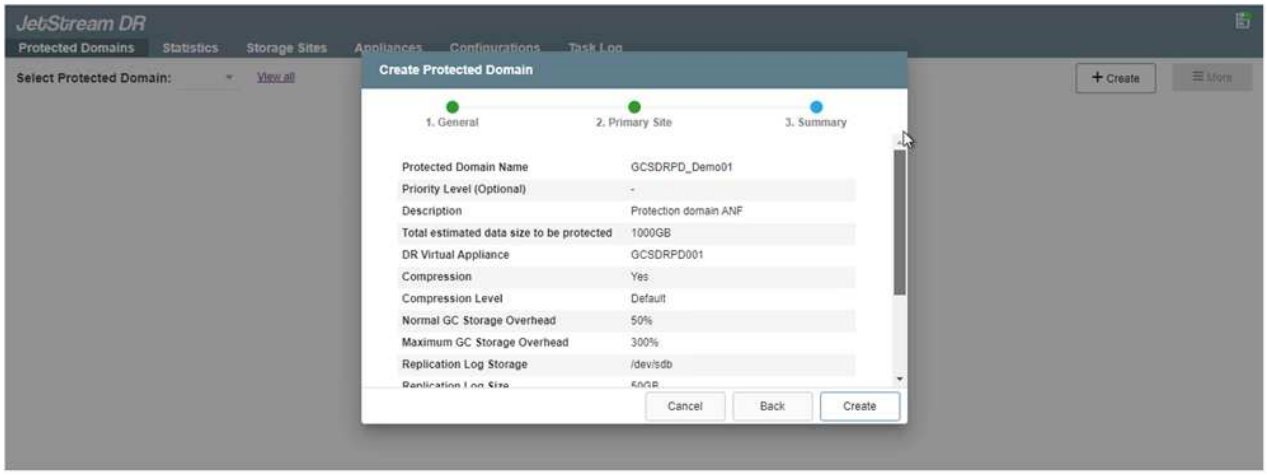
Utiliser l'outil de planification de la capacité pour estimer le nombre d'ACR requis.

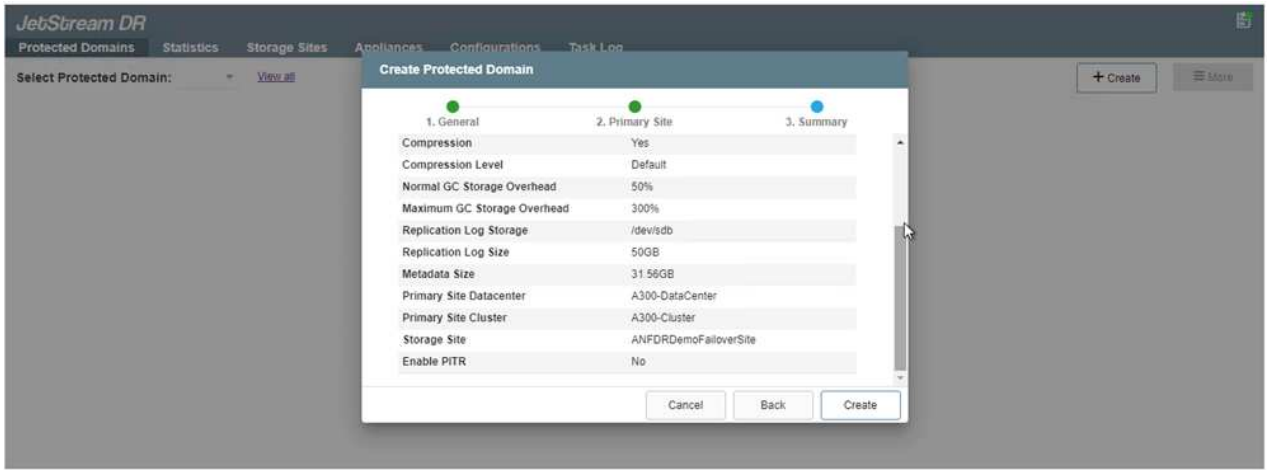


9. Créez des volumes de journal de réplication pour chaque DRVA à l'aide du VMDK provenant des datastores disponibles ou du pool de stockage iSCSI partagé indépendant.



10. À partir de l'onglet domaines protégés, créez le nombre requis de domaines protégés à l'aide des informations concernant le site Azure Blob Storage, l'instance DRVA et le journal de réplication. Un domaine protégé définit un ordinateur virtuel ou un ensemble de VM d'applications spécifiques au sein du cluster, qui sont protégés ensemble et ont un ordre de priorité pour les opérations de basculement/retour arrière.

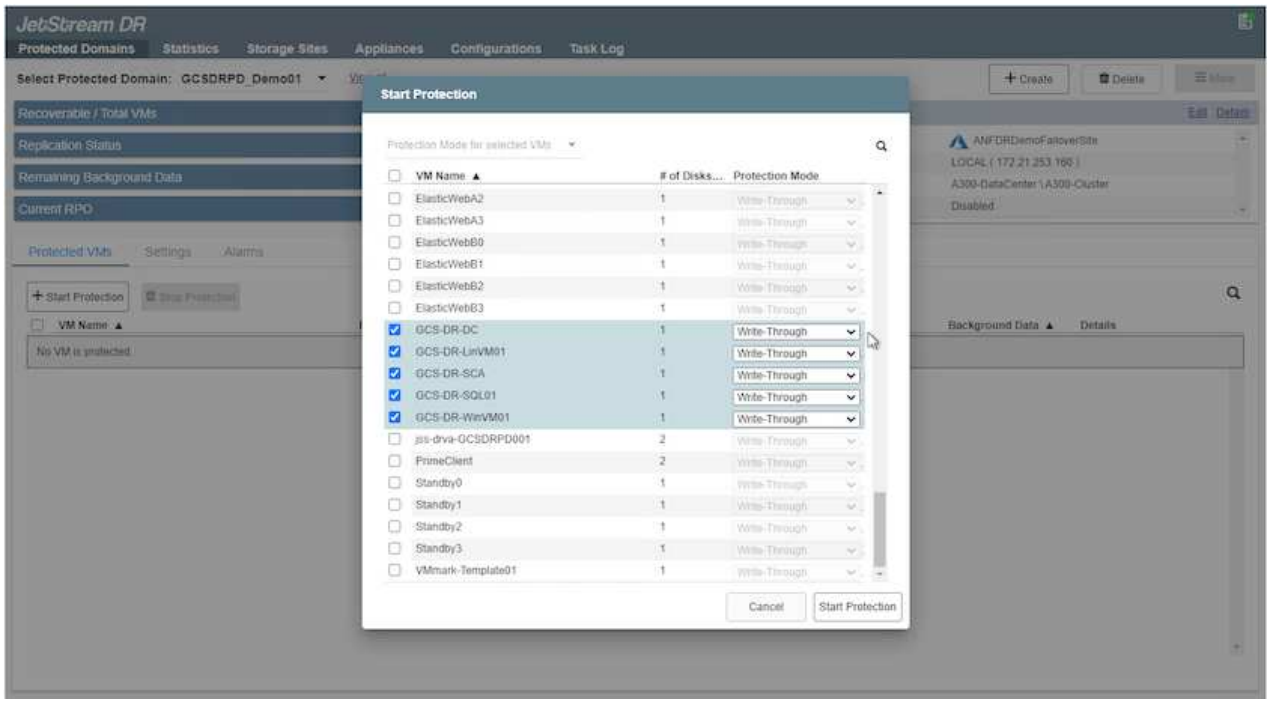




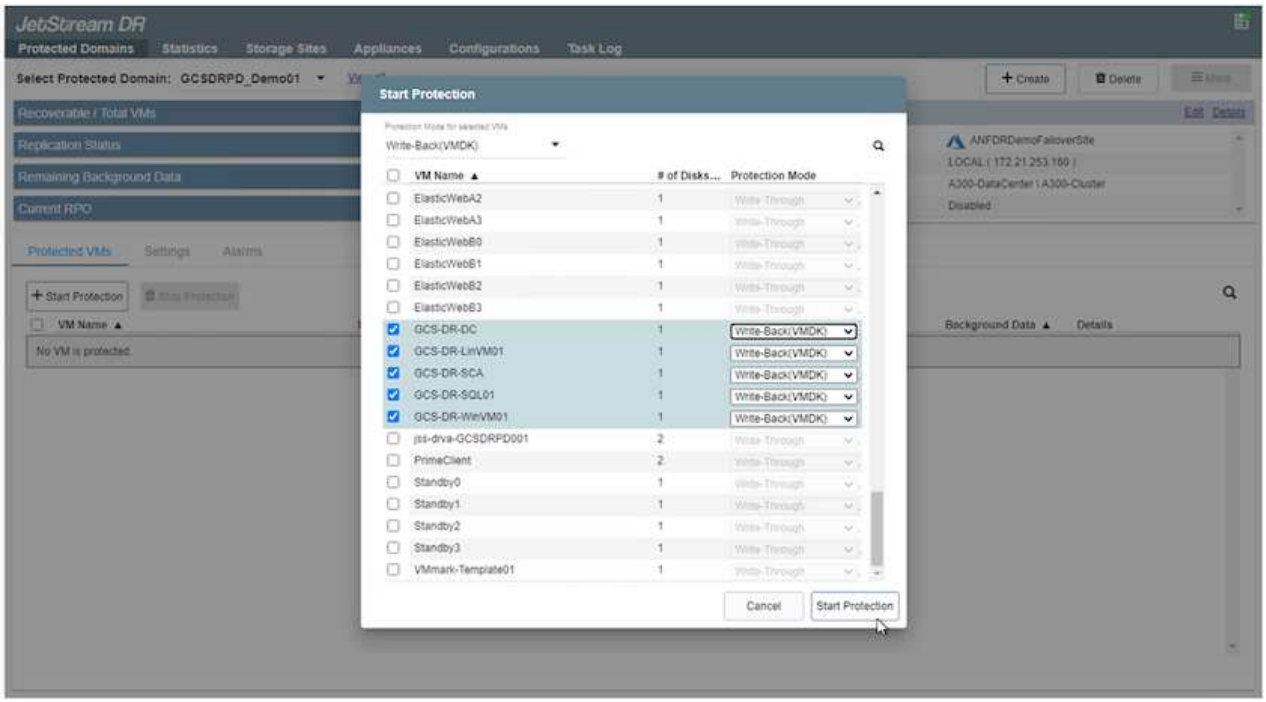
11. Sélectionnez les VM à protéger et regroupez-les dans des groupes d'applications en fonction de la dépendance. Les définitions d'application vous permettent de regrouper des jeux de machines virtuelles en groupes logiques contenant leurs ordres de démarrage, leurs retards de démarrage et les validations d'applications en option qui peuvent être exécutées à la reprise.

Assurez-vous que le même mode de protection est utilisé pour toutes les machines virtuelles d'un domaine protégé.

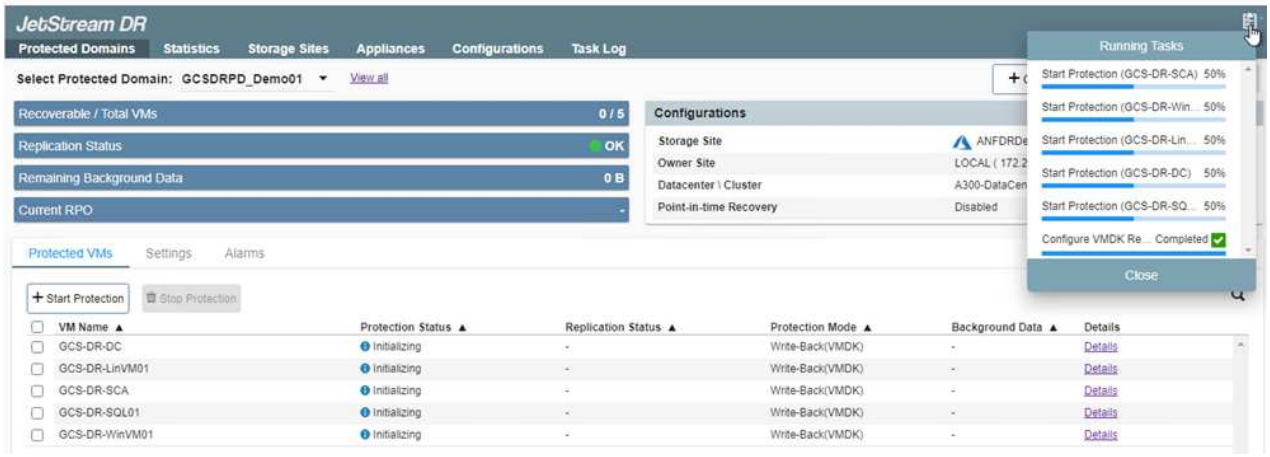
Le mode Write-Back (VMDK) offre de meilleures performances.



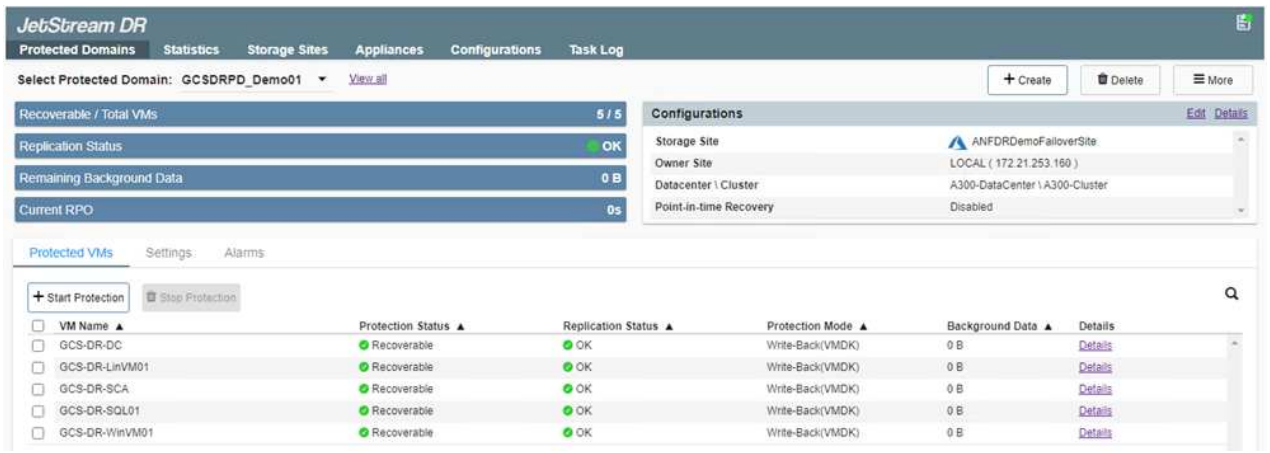
12. Assurez-vous que les volumes des journaux de réplication sont placés sur un stockage haute performance.



13. Une fois que vous avez terminé, cliquez sur Démarrer la protection du domaine protégé. La réplication des données démarre pour les machines virtuelles sélectionnées vers le magasin de objets blob désigné.



14. Une fois la réplication terminée, l'état de protection de la VM est marqué comme récupérable.

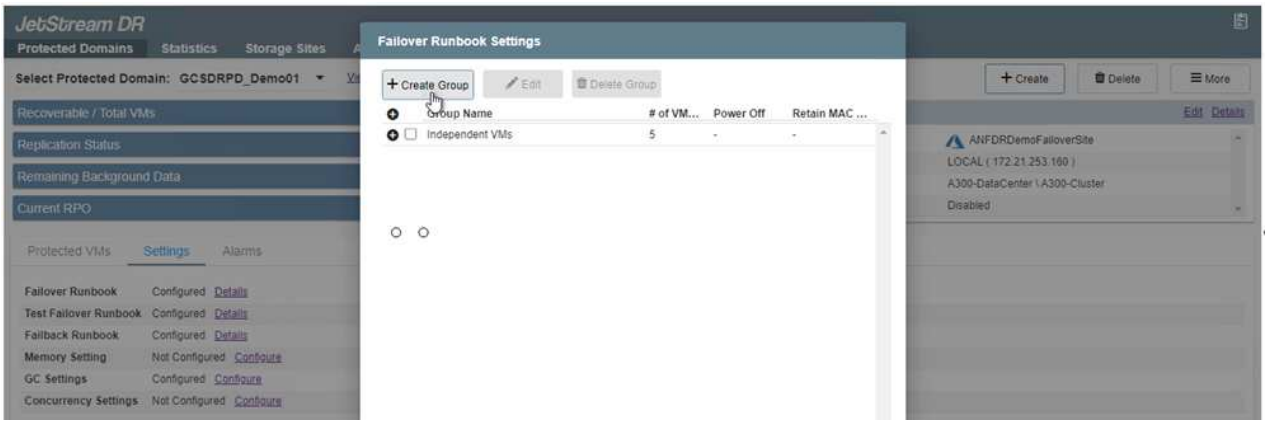


> Les runbooks de basculement peuvent être configurés pour regrouper les VM (appelé groupe de reprise), définir l'ordre de démarrage et modifier les paramètres CPU/mémoire avec les configurations IP.

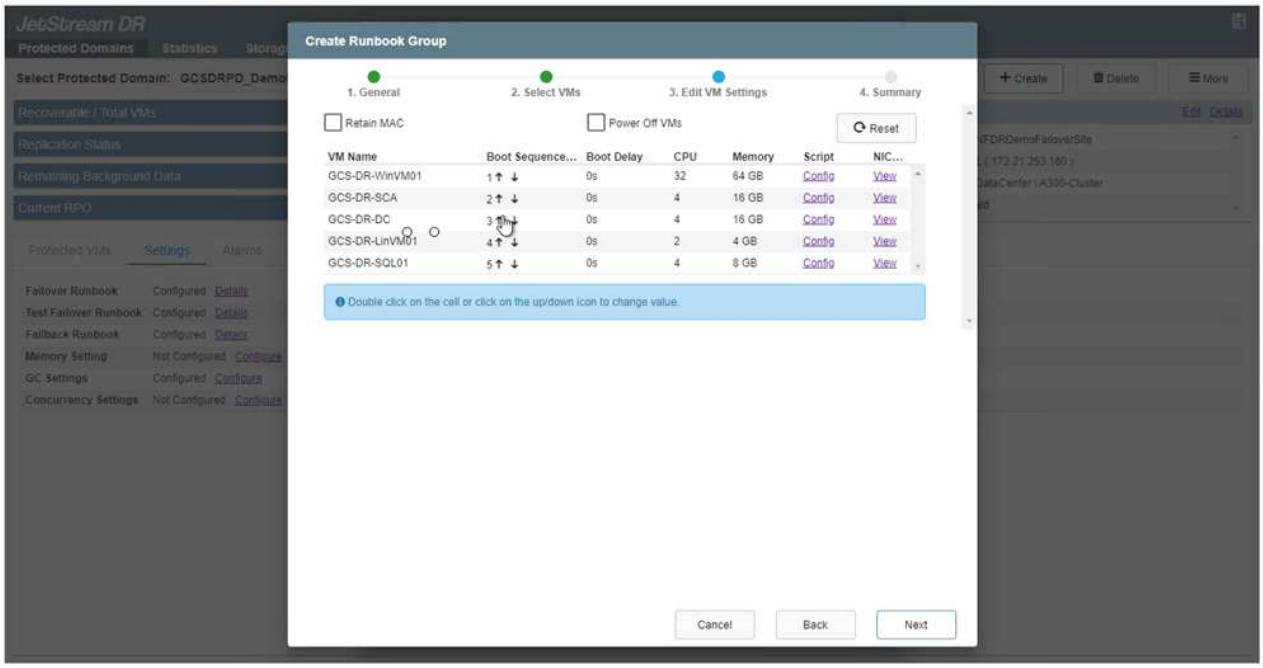
15. Cliquez sur Paramètres, puis sur le lien Runbook Configure pour configurer le groupe Runbook.

16. Cliquez sur le bouton Créer un groupe pour commencer à créer un nouveau groupe de runbook.

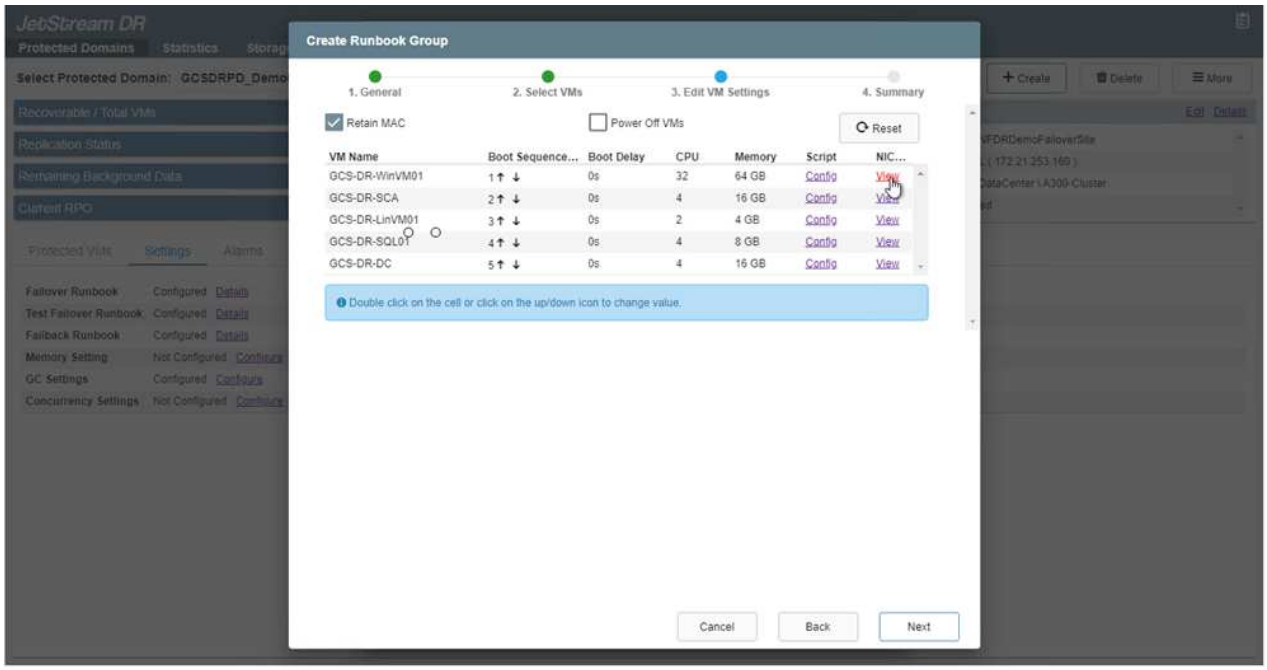
Si nécessaire, dans la partie inférieure de l'écran, appliquez des pré-scripts personnalisés et des post-scripts pour s'exécuter automatiquement avant et après l'opération du groupe Runbook. Assurez-vous que les scripts Runbook résident sur le serveur de gestion.



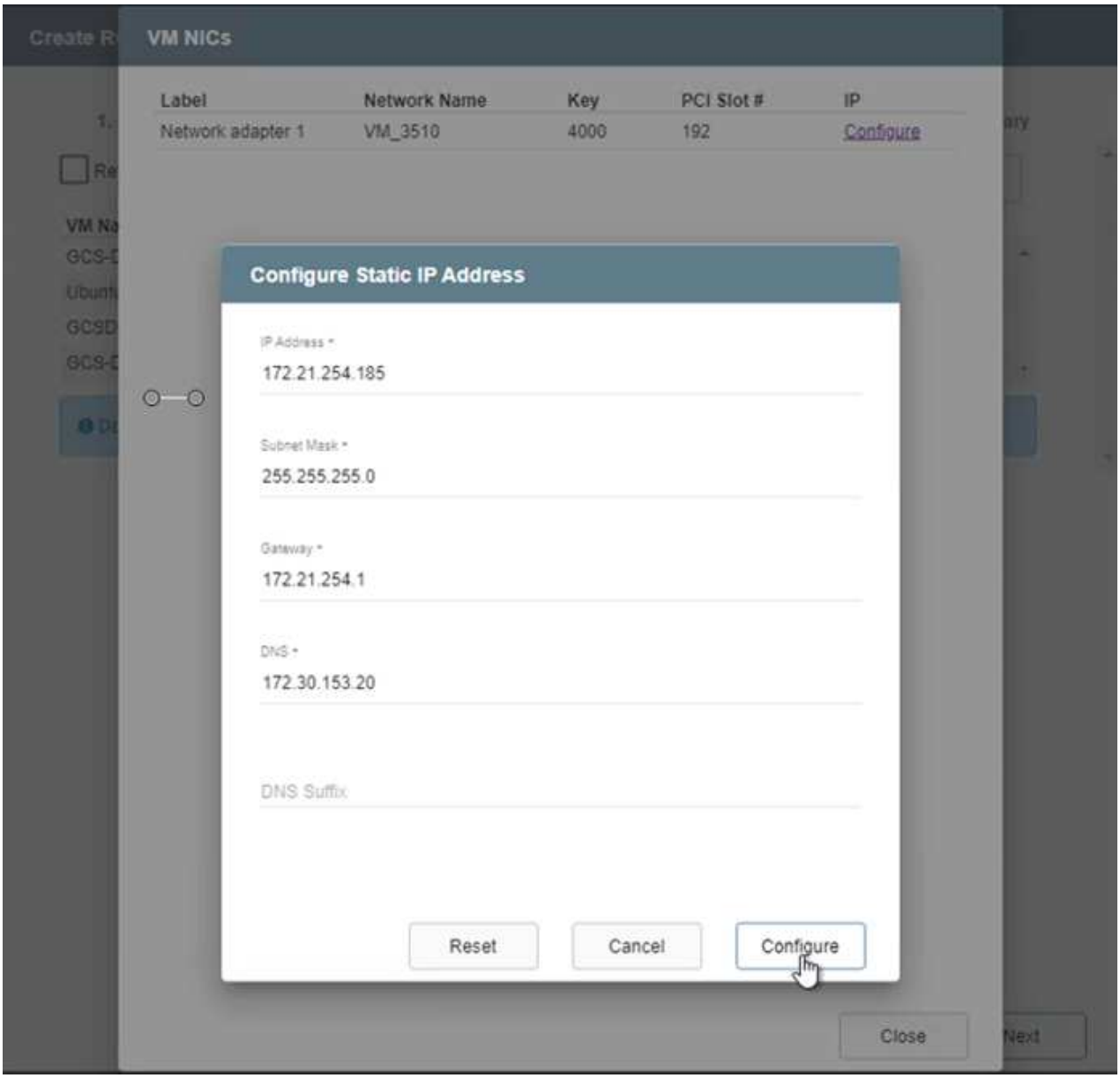
17. Modifiez les paramètres de la machine virtuelle selon vos besoins. Spécifier les paramètres de restauration des VM, y compris la séquence de démarrage, le délai de démarrage (spécifié en secondes), le nombre de CPU et la quantité de mémoire à allouer. Modifier la séquence de démarrage des machines virtuelles en cliquant sur les flèches vers le haut ou vers le bas. Des options sont également fournies pour conserver MAC.

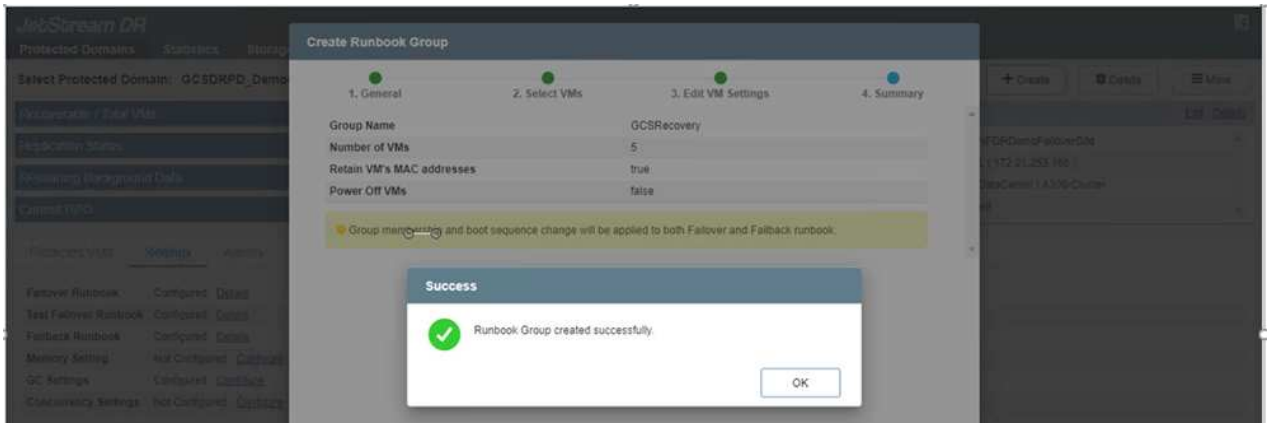


18. Les adresses IP statiques peuvent être configurées manuellement pour les machines virtuelles individuelles du groupe. Cliquez sur le lien vue NIC d'une machine virtuelle pour configurer manuellement ses paramètres d'adresse IP.



19. Cliquez sur le bouton configurer pour enregistrer les paramètres NIC pour les machines virtuelles respectives.





L'état des runbooks de basculement et de retour arrière est désormais répertorié comme configuré. Les groupes de runbooks de basculement et de retour arrière sont créés par paires en utilisant le même groupe initial de machines virtuelles et de paramètres. Si nécessaire, les paramètres d'un groupe de runbook peuvent être personnalisés individuellement en cliquant sur son lien Détails respectifs et en

effectuant des modifications.

Installer JetStream DR pour AVS dans le cloud privé

Il est recommandé de créer à l'avance un cluster Pilot-light à trois nœuds sur le site de récupération (AVS). L'infrastructure du site de reprise peut ainsi être préconfigurée, notamment :

- Segments de réseau de destination, pare-feu, services comme DHCP et DNS, etc
- Installation de JetStream DR pour AVS
- Configuration des volumes ANF comme datastore et plus encore

Jetstream DR prend en charge un mode RTO proche de zéro pour les domaines stratégiques. Pour ces domaines, le stockage de destination doit être préinstallé. ANF est un type de stockage recommandé dans ce cas.

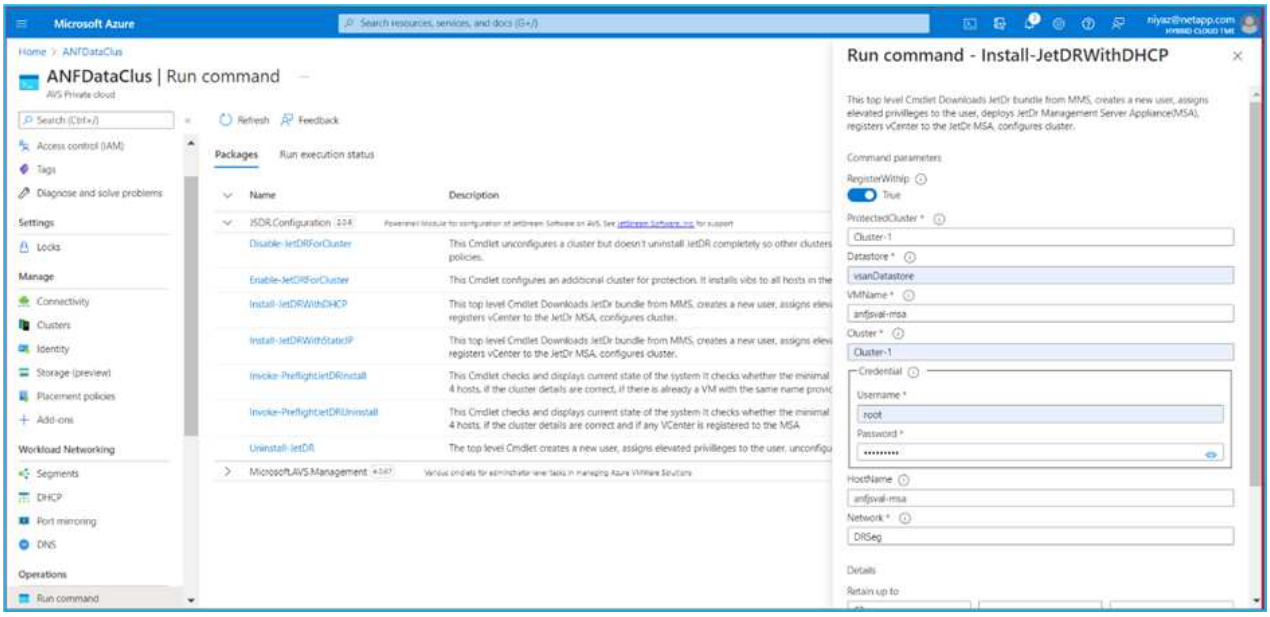
ⓘ La configuration réseau comprenant la création de segments doit être configurée sur le cluster AVS afin de répondre aux exigences sur site.

ⓘ Selon les exigences des contrats de niveau de service et de durée de restauration, vous pouvez utiliser un mode de basculement continu ou standard. Pour un RTO proche de zéro, vous devez commencer la réhydratation continue sur le site de restauration.

1. Pour installer JetStream DR pour AVS sur un cloud privé Azure VMware solution, utilisez la commande Exécuter. Depuis le portail Azure, accédez à la solution VMware Azure, sélectionnez le cloud privé et sélectionnez Exécuter la commande > packages > JSDR.Configuration.

   ⓘ L'utilisateur CloudAdmin par défaut de la solution Azure VMware ne dispose pas des privilèges suffisants pour installer JetStream DR pour AVS. La solution Azure VMware permet une installation simplifiée et automatisée de JetStream DR en appelant la commande Azure VMware solution Run pour JetStream DR.

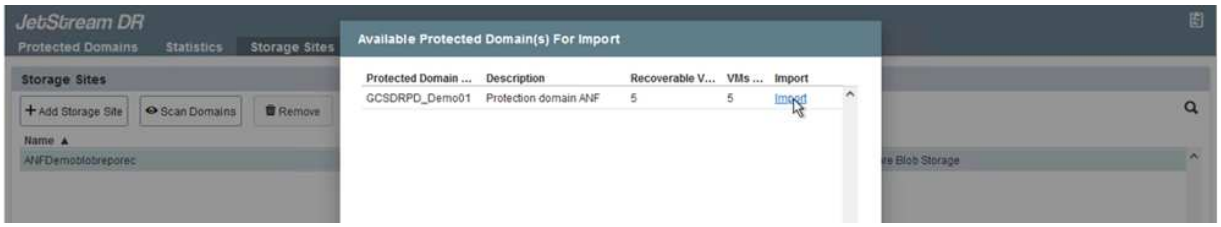
   La capture d'écran suivante montre l'installation à l'aide d'une adresse IP DHCP.



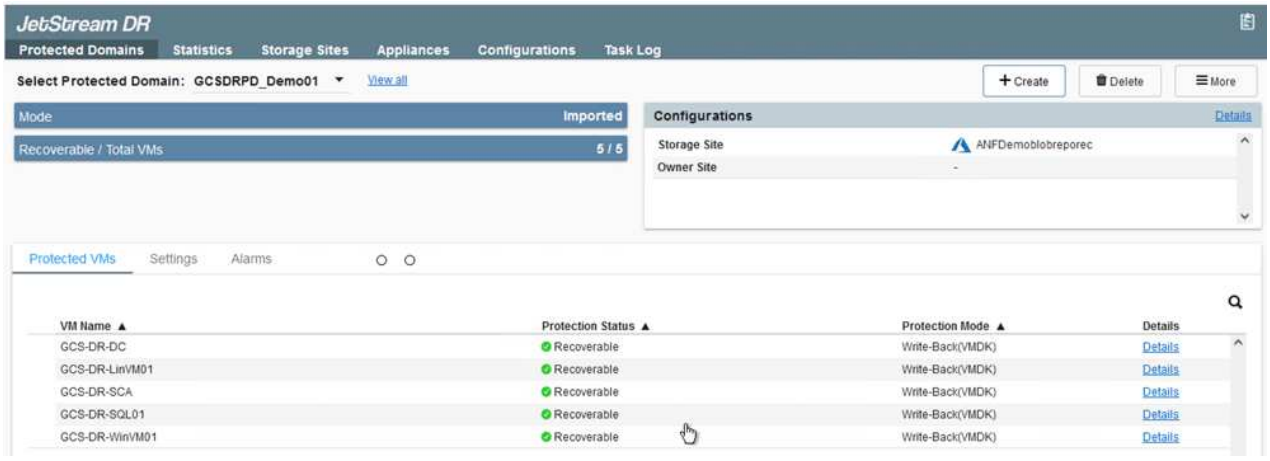
2. Une fois l'installation de JetStream DR pour AVS terminée, actualisez le navigateur. Pour accéder à l'interface de reprise après incident JetStream, allez dans SDDC Datacenter > configurer > JetStream

DR.

3. À partir de l'interface JetStream DR, effectuez les tâches suivantes :
   a. Ajoutez le compte Azure Blob Storage qui a été utilisé pour protéger le cluster sur site en tant que site de stockage, puis exécutez l'option Scan Domains.
   b. Dans la boîte de dialogue qui s'affiche, sélectionnez le domaine protégé à importer, puis cliquez sur son lien Importer.



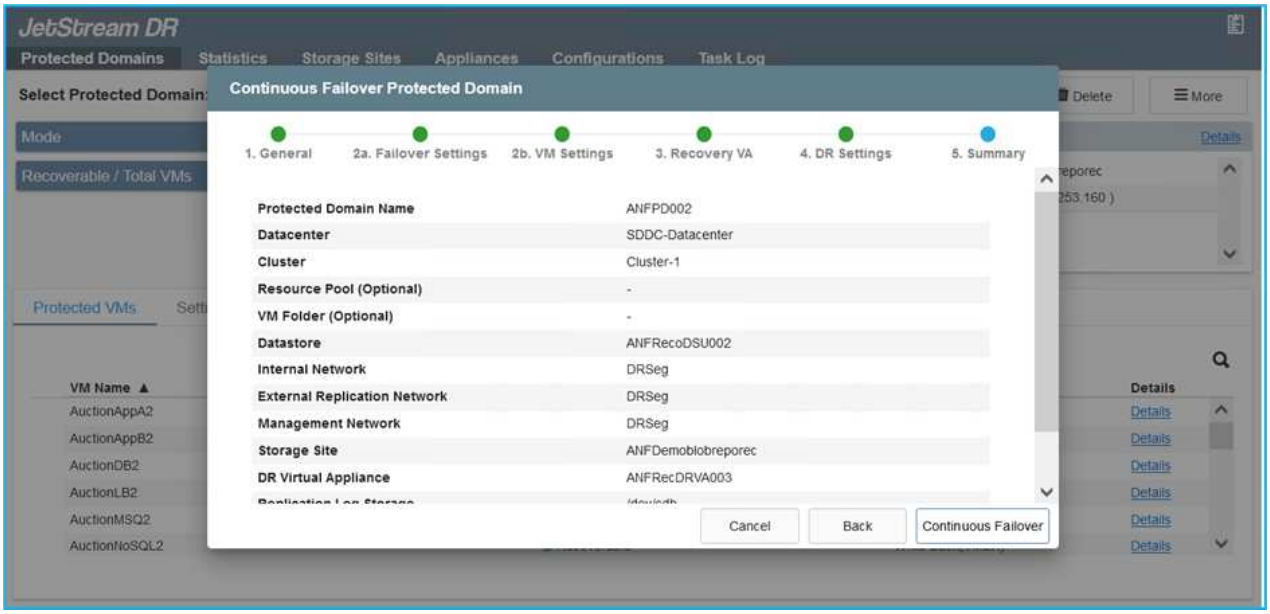
4. Le domaine est importé pour la récupération. Accédez à l'onglet domaines protégés et vérifiez que le domaine prévu a été sélectionné ou choisissez le domaine souhaité dans le menu Sélectionner un domaine protégé. La liste des VM récupérables du domaine protégé s'affiche.



5. Une fois les domaines protégés importés, déployez les appareils DRVA.

Ces étapes peuvent également être automatisées à l'aide de plans créés par CPT.

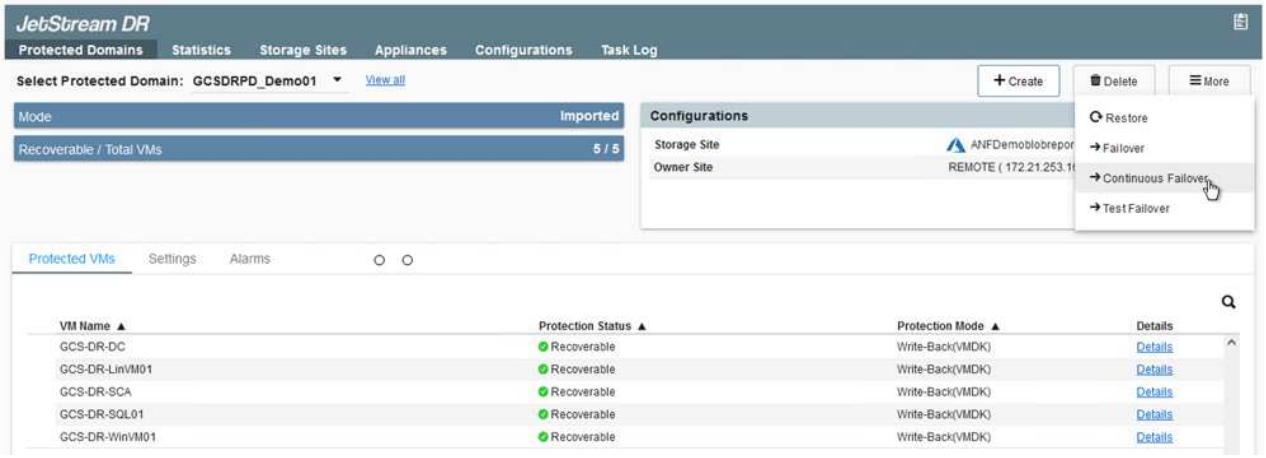
6. Créez des volumes du journal de réplication à l'aide des datastores VSAN ou ANF disponibles.
7. Importez les domaines protégés et configurez le va de restauration de manière à utiliser un datastore ANF pour le positionnement des VM.



Assurez-vous que DHCP est activé sur le segment sélectionné et qu'un nombre suffisant d'adresses IP est disponible. Des adresses IP dynamiques sont utilisées temporairement pendant la restauration des domaines. Chaque machine virtuelle de restauration (y compris la réhydratation continue) requiert une adresse IP dynamique individuelle. Une fois la récupération terminée, le IP est libéré et peut être réutilisé.

8. Sélectionnez l'option de basculement appropriée (basculement continu ou basculement). Dans cet exemple, la réhydratation continue (basculement continu) est sélectionnée.

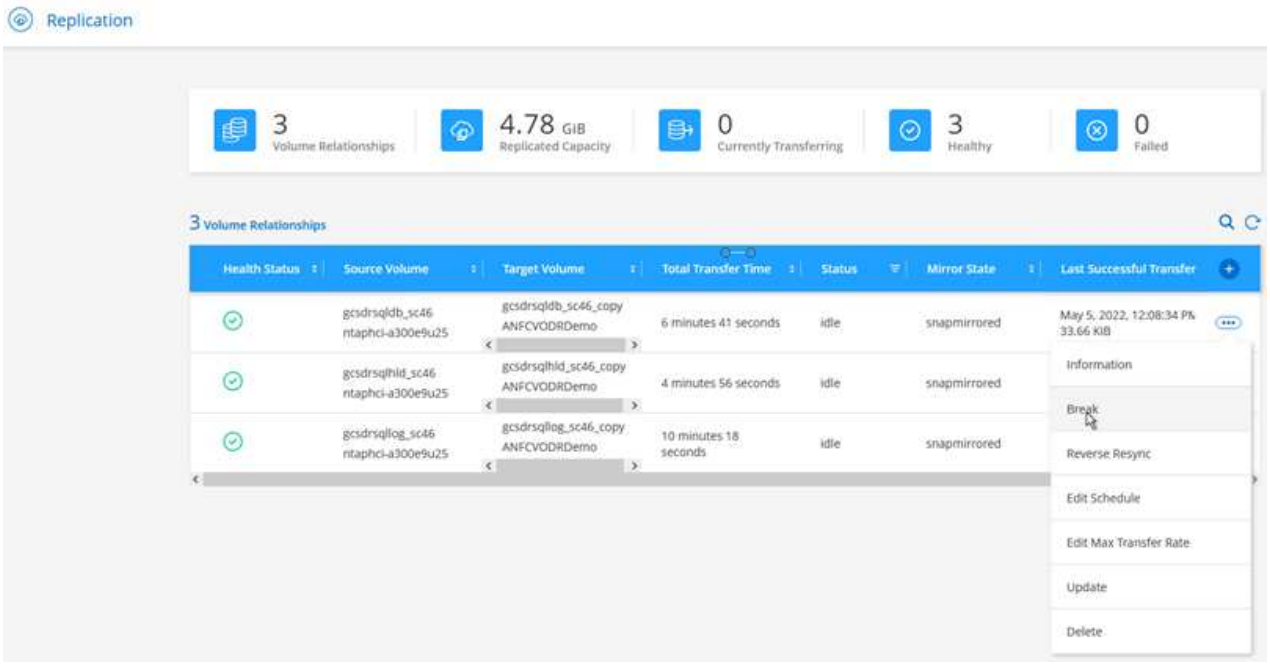
Bien que les modes de basculement et de basculement continu diffèrent lorsque la configuration est effectuée, les deux modes de basculement sont configurés à l'aide des mêmes étapes. Les étapes de basculement sont configurées et effectuées ensemble en cas d'incident. Le basculement continu peut être configuré à tout moment, puis s'exécuter en arrière-plan pendant le fonctionnement normal du système. Après un incident, un basculement continu est effectué pour transférer immédiatement la propriété des machines virtuelles protégées vers le site de reprise (RTO quasi nul).

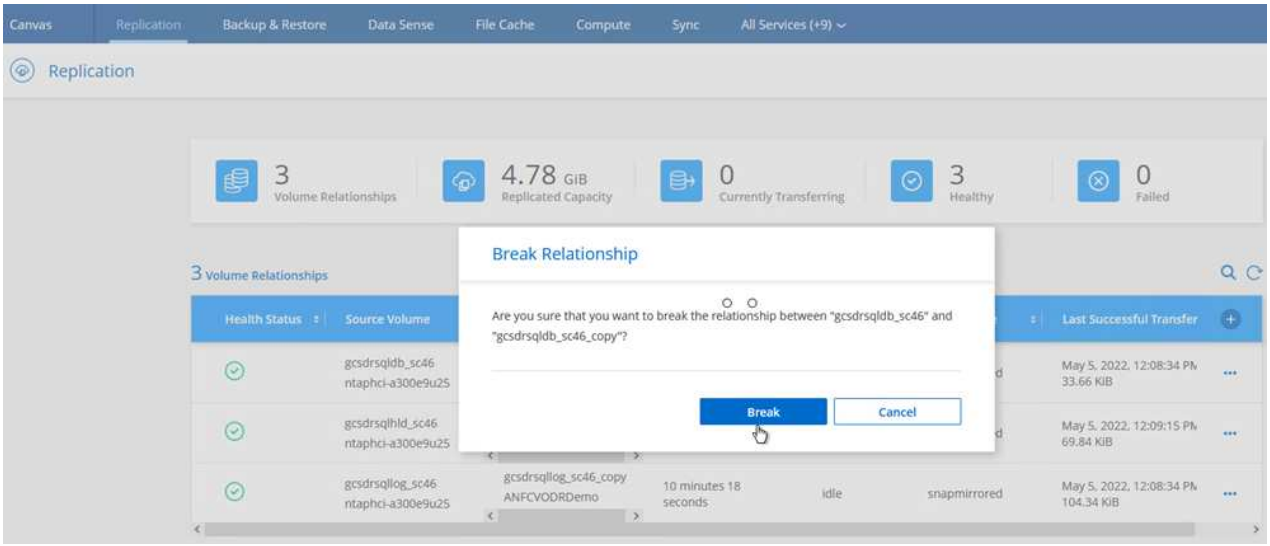


Le processus de basculement continu démarre et sa progression peut être surveillée dans l'interface utilisateur. Un clic sur l'icône bleue dans la section Etape actuelle permet d'afficher une fenêtre contextuelle affichant les détails de l'étape en cours du processus de basculement.

Basculement et rétablissement

1. Après un incident se produit dans le cluster protégé de l'environnement sur site (défaillance partielle ou complète), vous pouvez déclencher le basculement pour les machines virtuelles à l'aide de Jetstream après avoir déclenché la relation SnapMirror pour les volumes d'application respectifs.

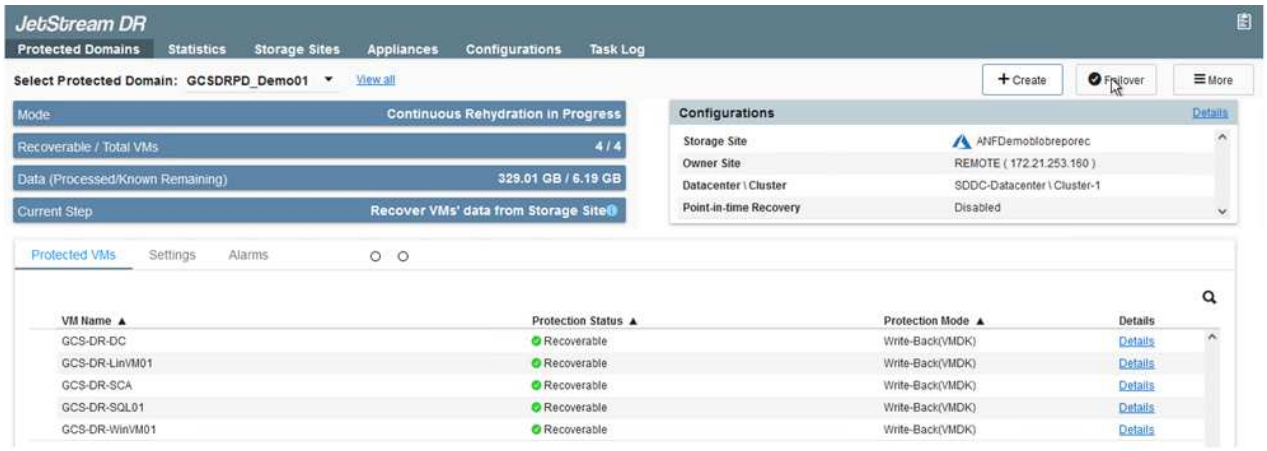


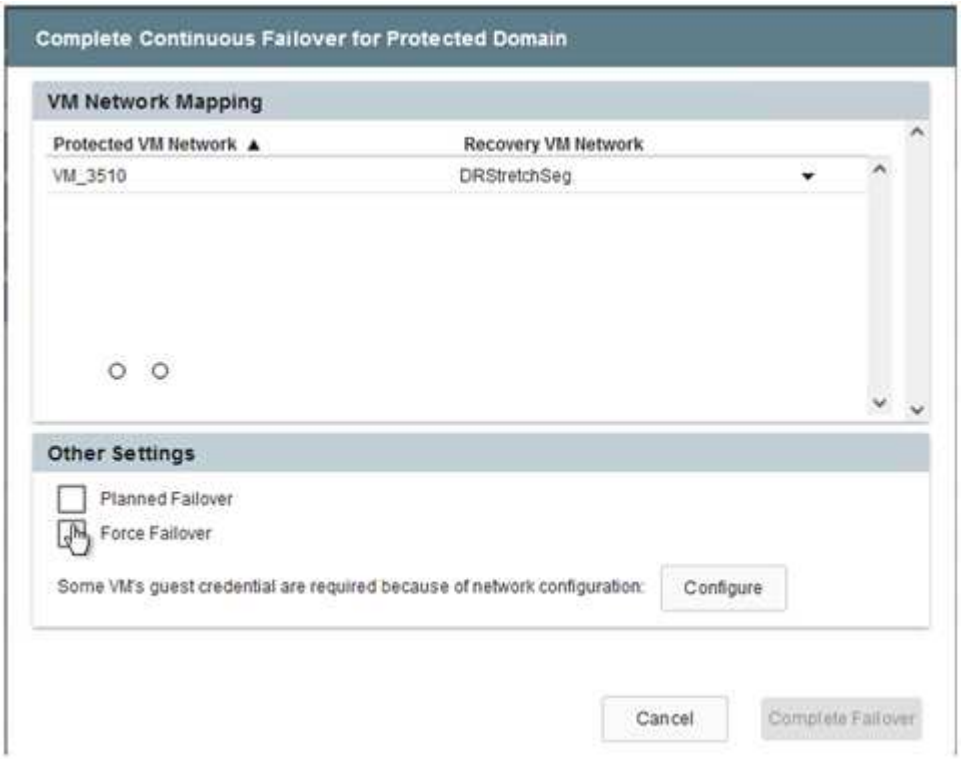


Cette étape peut facilement être automatisée afin de faciliter le processus de reprise.

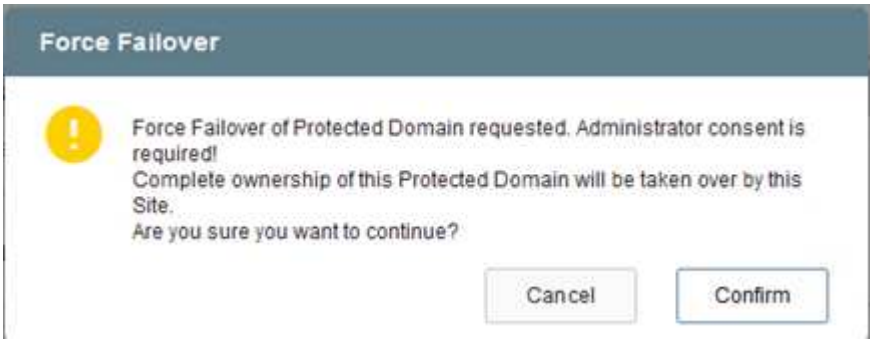
2. Accédez à l'interface utilisateur Jetstream sur AVS SDDC (côté destination) et activez l'option de basculement pour terminer le basculement. La barre des tâches affiche la progression des activités de basculement.

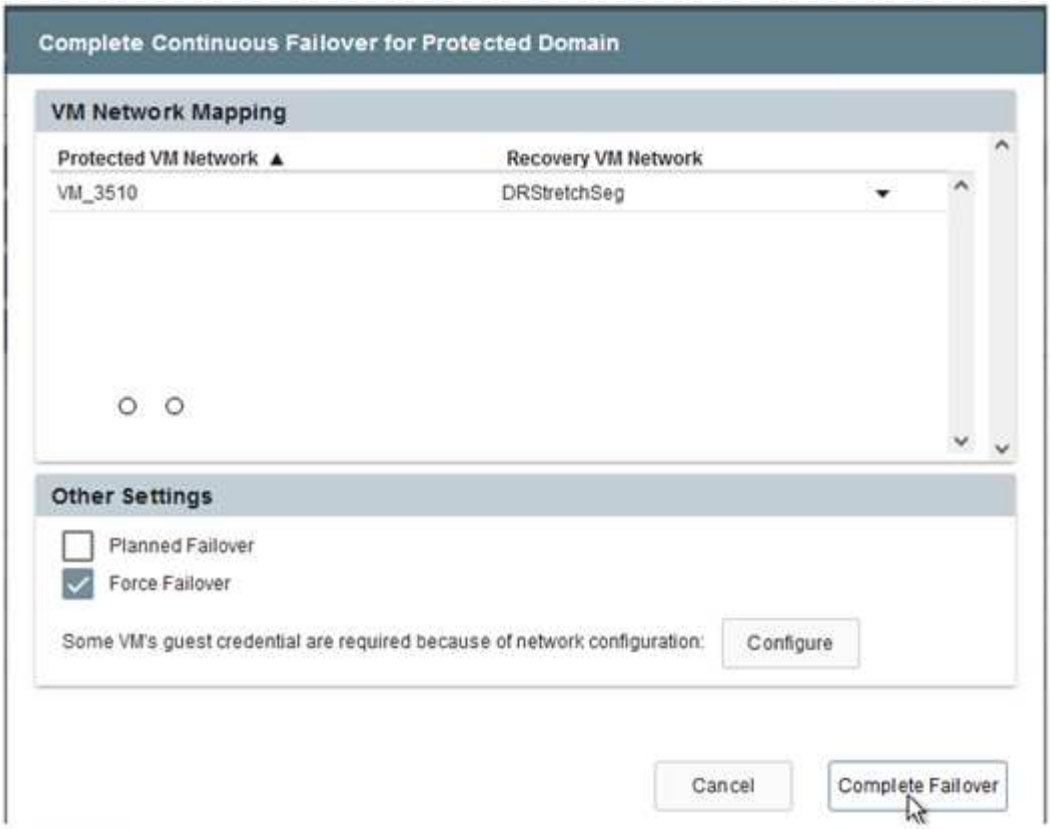
   Dans la boîte de dialogue qui s'affiche lors de la fin du basculement, la tâche de basculement peut être spécifiée comme planifié ou supposée être forcée.





Le basculement forcé suppose que le site principal n'est plus accessible et que la propriété du domaine protégé devrait être directement assumée par le site de reprise.



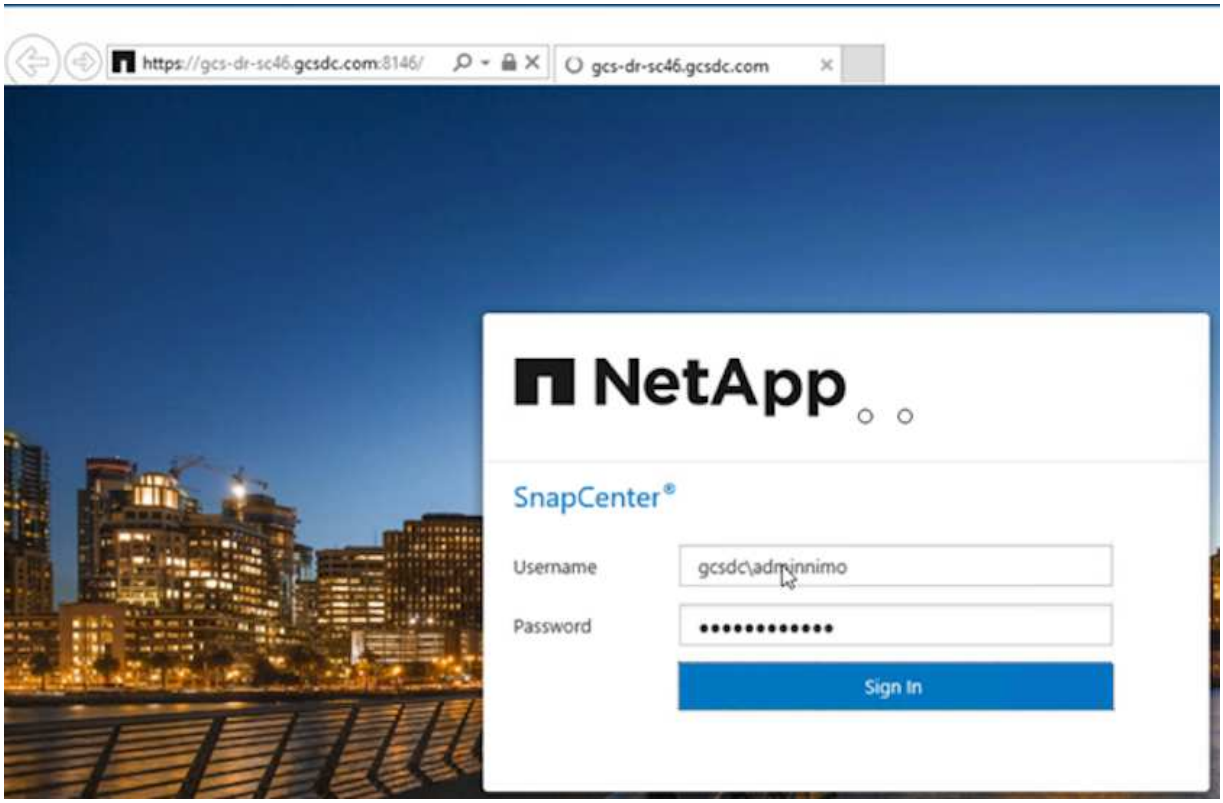


3. Une fois le basculement continu terminé, un message confirmant la fin de la tâche s'affiche. Une fois la tâche terminée, accédez aux VM récupérées pour configurer les sessions ISCSI ou NFS.

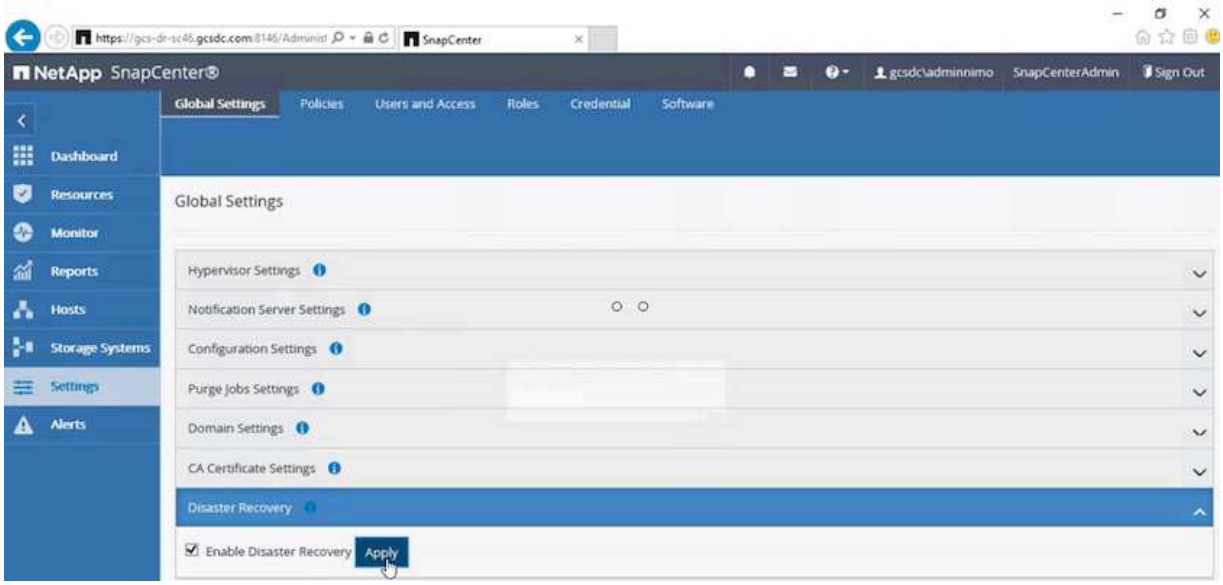
Le mode de basculement passe en mode d'exécution en basculement et l'état de la VM peut être récupérable. Toutes les machines virtuelles du domaine protégé sont à présent exécutées sur le site de reprise, dans l'état spécifié par les paramètres de runbook de basculement.

Pour vérifier la configuration et l'infrastructure de basculement, JetStream DR peut être utilisé en mode test (option Test Failover) afin d'observer la récupération des machines virtuelles et de leurs données à partir du magasin d'objets dans un environnement de restauration de test. Lorsqu'une procédure de basculement est exécutée en mode test, son fonctionnement ressemble à un processus de basculement réel.

4. Une fois les machines virtuelles restaurées, utilisez la reprise après incident du stockage pour le stockage invité. Pour démontrer ce processus, SQL Server est utilisé dans cet exemple.
5. Connectez-vous à la machine virtuelle SnapCenter récupérée sur AVS SDDC et activez le mode DR.
   a. Accédez à l'interface utilisateur SnapCenter à l'aide du navigateur.



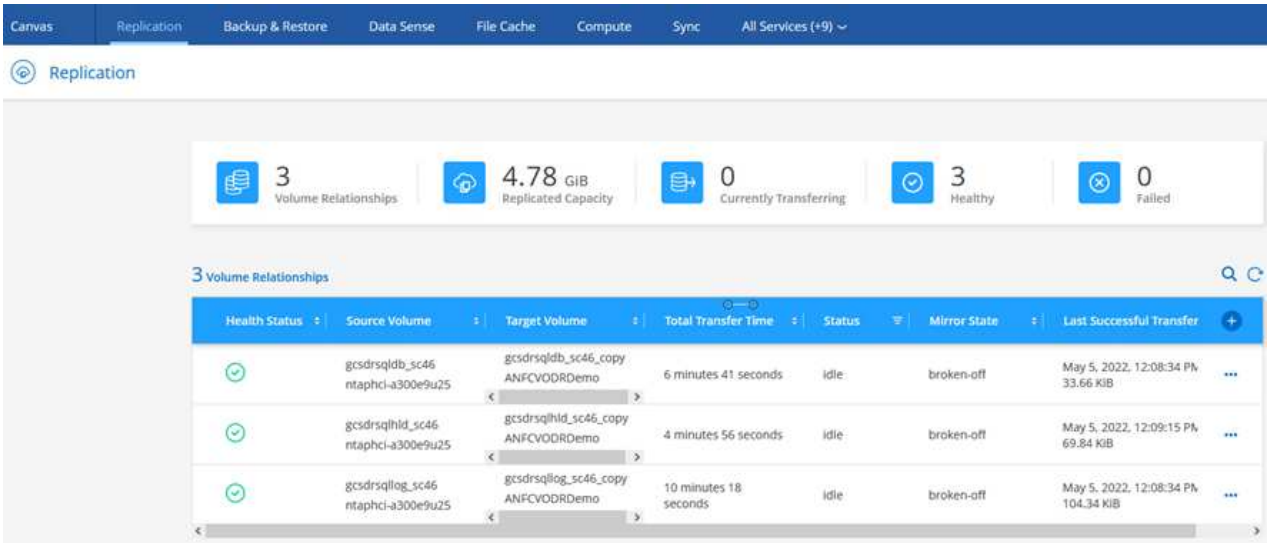
   b. Dans la page Paramètres, accédez à Paramètres > Paramètres globaux > reprise après incident.
   c. Sélectionnez Activer la reprise après incident.
   d. Cliquez sur appliquer.



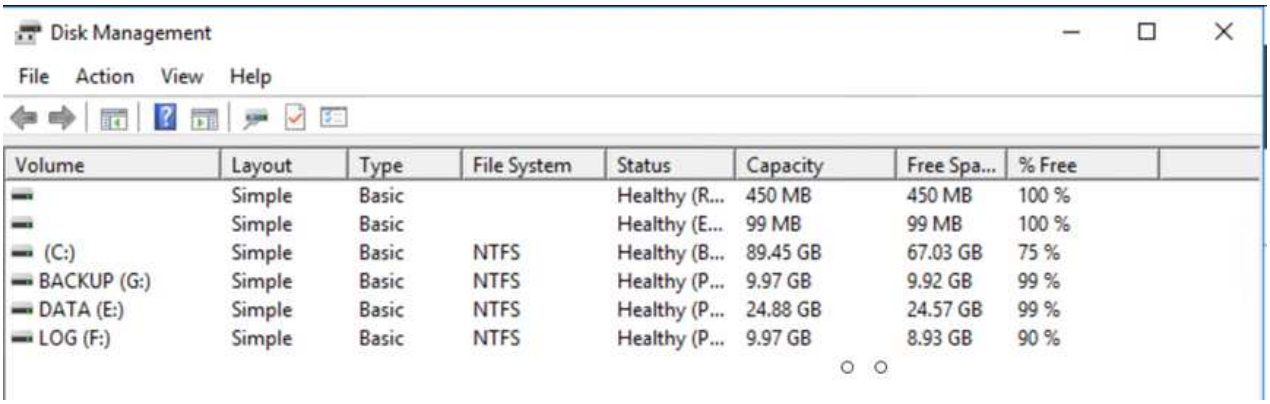
   e. Vérifiez si la tâche DR est activée en cliquant sur Monitor > Jobs.

NetApp SnapCenter 4.6 ou version ultérieure doit être utilisé pour la reprise après incident du stockage. Pour les versions précédentes, des snapshots cohérents avec les applications (répliqués à l'aide de SnapMirror) doivent être utilisés. Il convient également d'exécuter une restauration manuelle si les sauvegardes précédentes doivent être restaurées sur le site de reprise après incident.

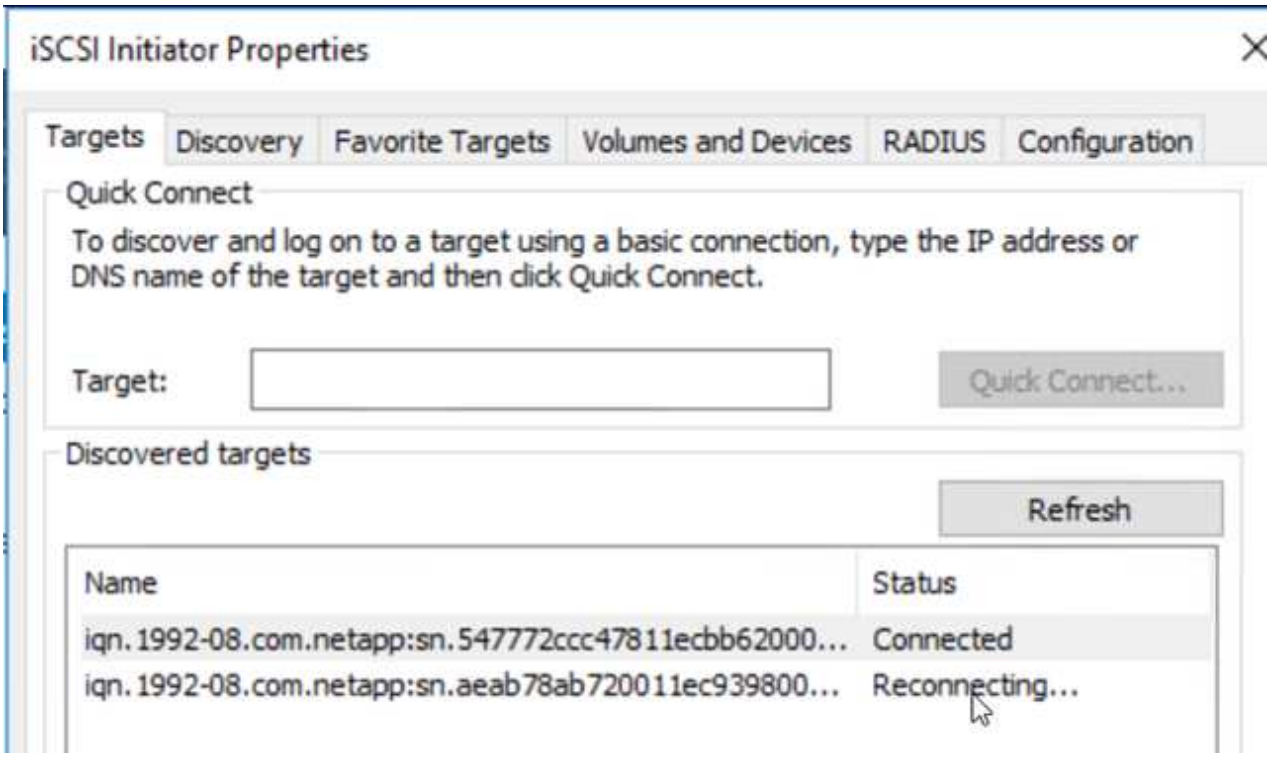
6. S'assurer que la relation SnapMirror est rompue.



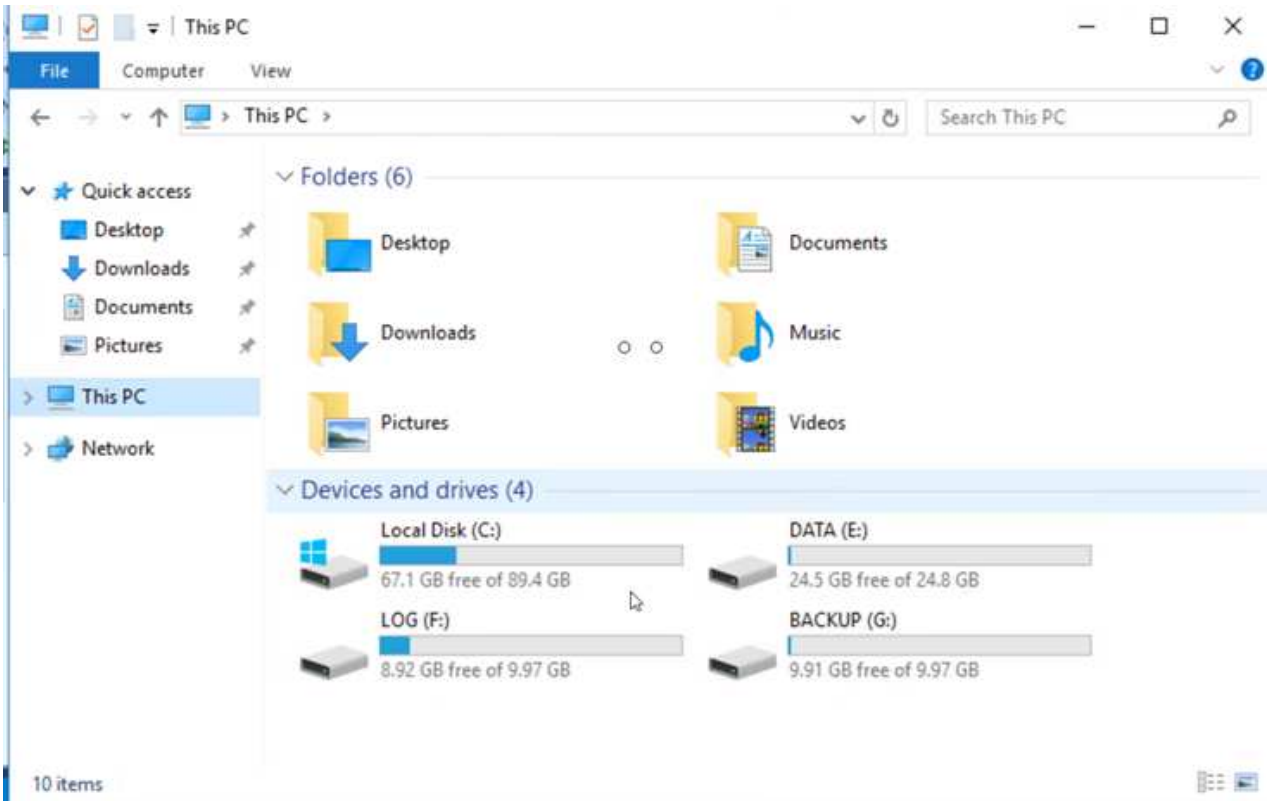
7. Reliez le LUN de Cloud Volumes ONTAP à la machine virtuelle hôte SQL récupérée à l'aide des mêmes lettres de disque.



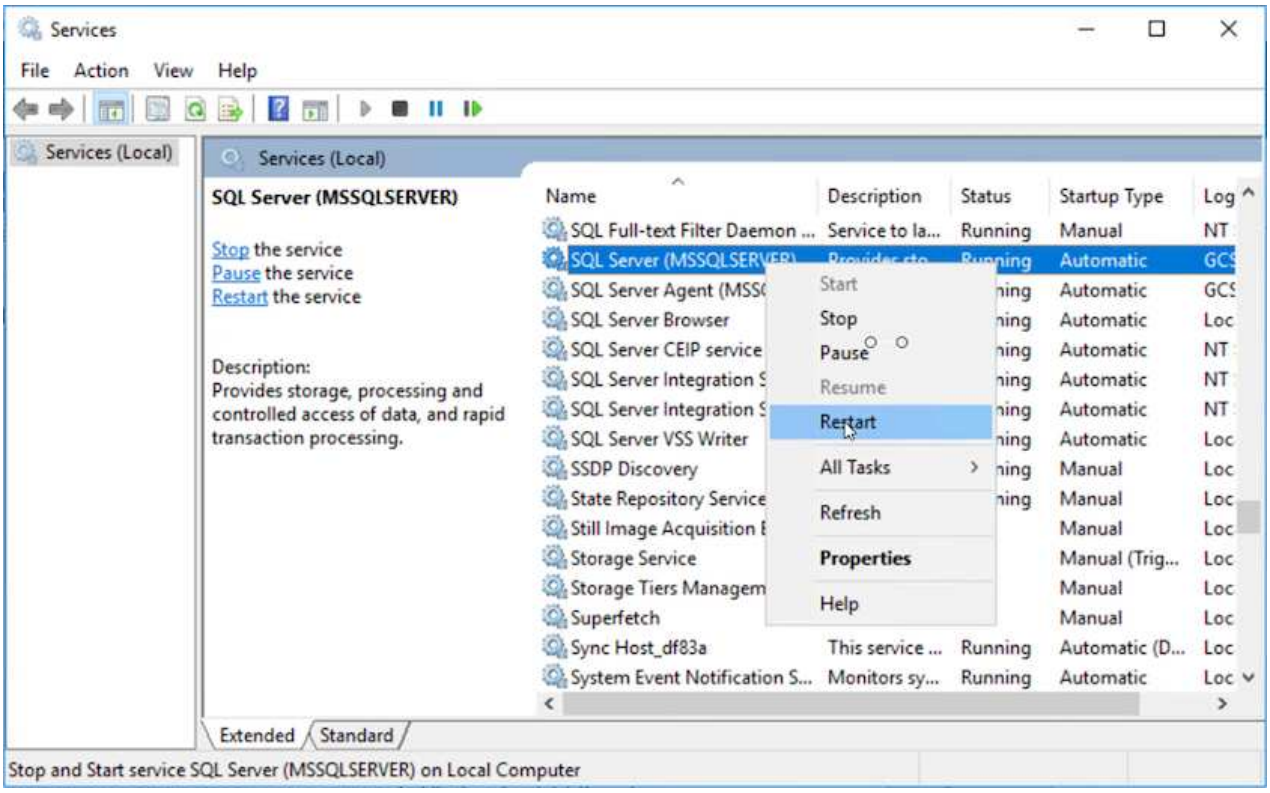
8. Ouvrez l'initiateur iSCSI, effacez la session précédente déconnectée et ajoutez la nouvelle cible avec les chemins d'accès multiples pour les volumes Cloud Volumes ONTAP répliqués.



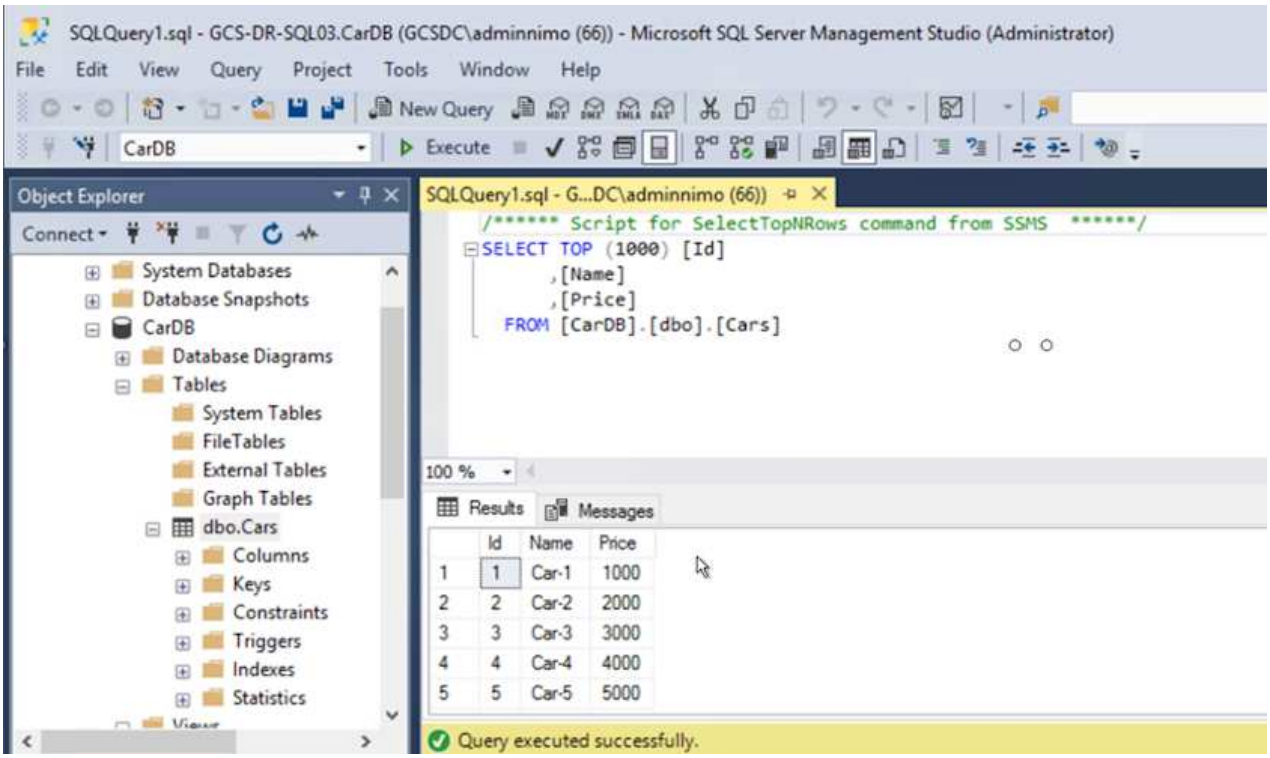
9. Assurez-vous que tous les disques sont connectés à l'aide des mêmes lettres que celles utilisées avant la reprise sur incident.



10. Redémarrez le service serveur MSSQL.



11. Assurez-vous que les ressources SQL sont de nouveau en ligne.



Dans le cas d'un système NFS, reliez les volumes à l'aide de la commande mount et mettez à jour le `/etc/fstab` entrées.

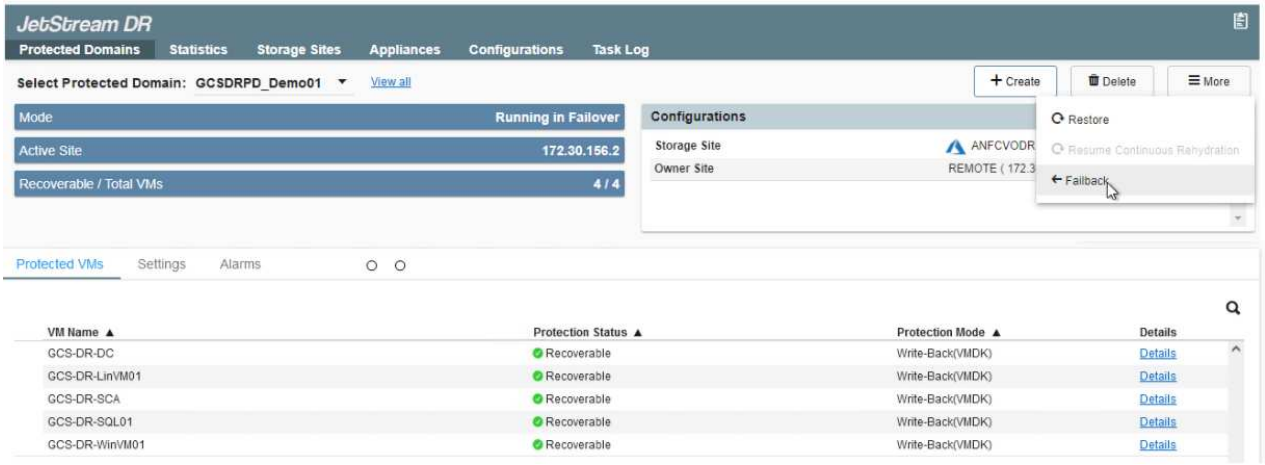
À ce stade, le fonctionnement de l'entreprise peut se faire et son activité se poursuit normalement.

Sur la fin NSX-T, il est possible de créer une passerelle de niveau 1 dédiée distincte pour simuler des scénarios de basculement. Cela permet de s'assurer que toutes les charges de travail peuvent communiquer les unes avec les autres, mais qu'aucun trafic ne peut être acheminé depuis et vers l'environnement, de manière à ce que les tâches de triage, de confinement ou de durcissement puissent être effectuées sans risque de contamination croisée. Cette opération est hors du champ d'application de ce document, mais elle peut être facilement réalisée pour simuler l'isolement.

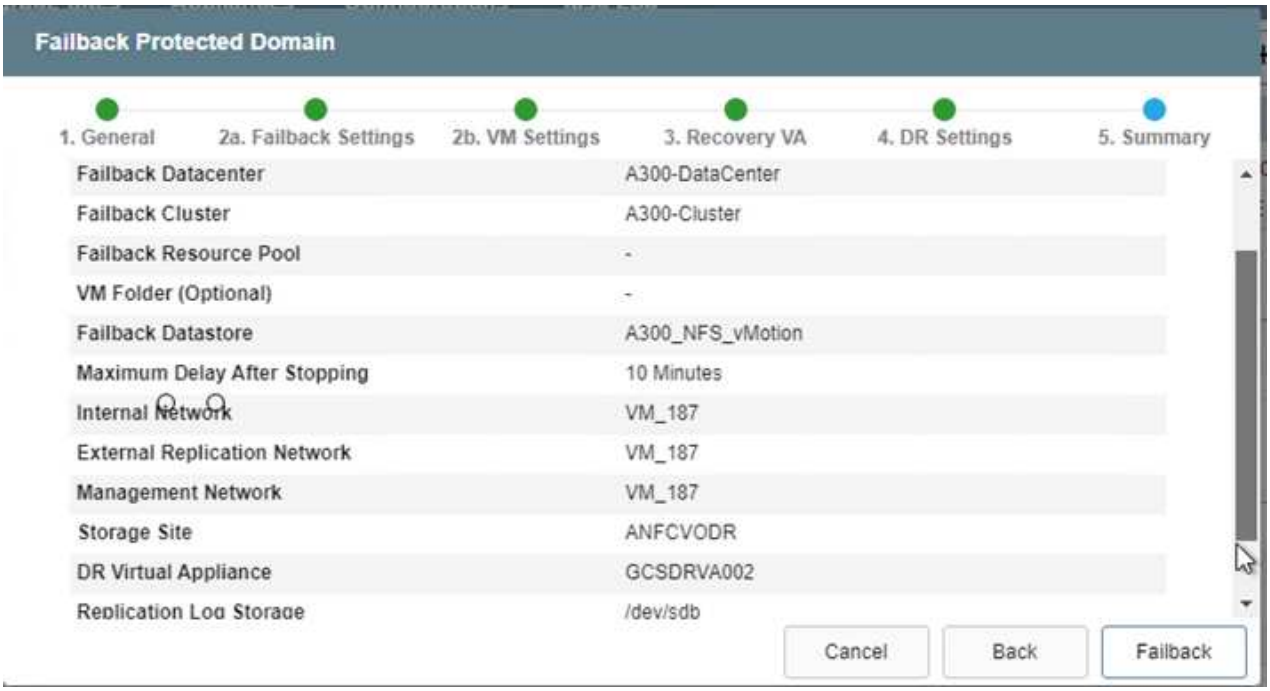
Une fois que le site primaire est de nouveau opérationnel, vous pouvez effectuer le rétablissement. La protection de machine virtuelle est reprise par Jetstream et la relation SnapMirror doit être inversée.

1. Restaurer l'environnement sur site. Selon le type d'incident, il peut être nécessaire de restaurer et/ou de vérifier la configuration du cluster protégé. Si nécessaire, il peut être nécessaire de réinstaller le logiciel JetStream DR.
2. Accédez à l'environnement sur site restauré, accédez à l'interface utilisateur Jetstream DR et sélectionnez le domaine protégé approprié. Une fois que le site protégé est prêt à être restauré, sélectionnez l'option de retour arrière dans l'interface utilisateur.

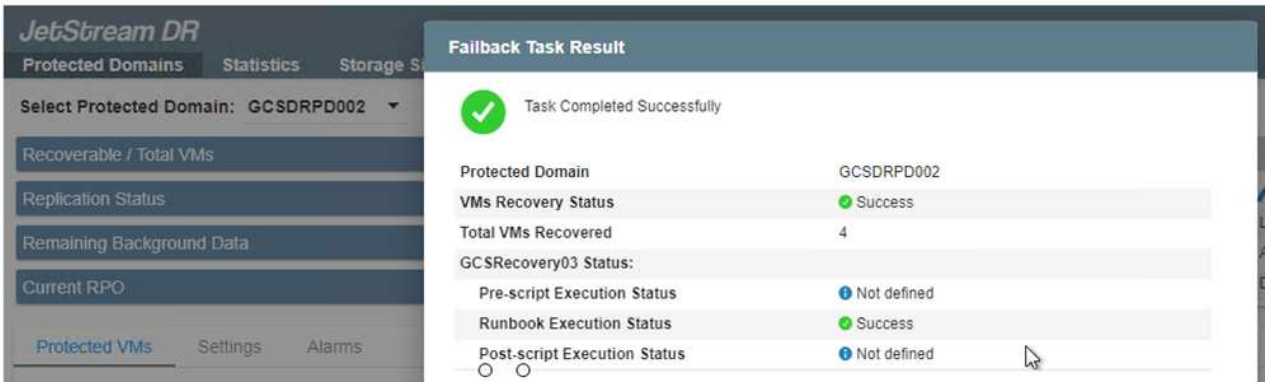
Le plan de restauration généré par CPT peut également être utilisé pour initier le retour des VM et de leurs données du magasin d'objets vers l'environnement VMware d'origine.



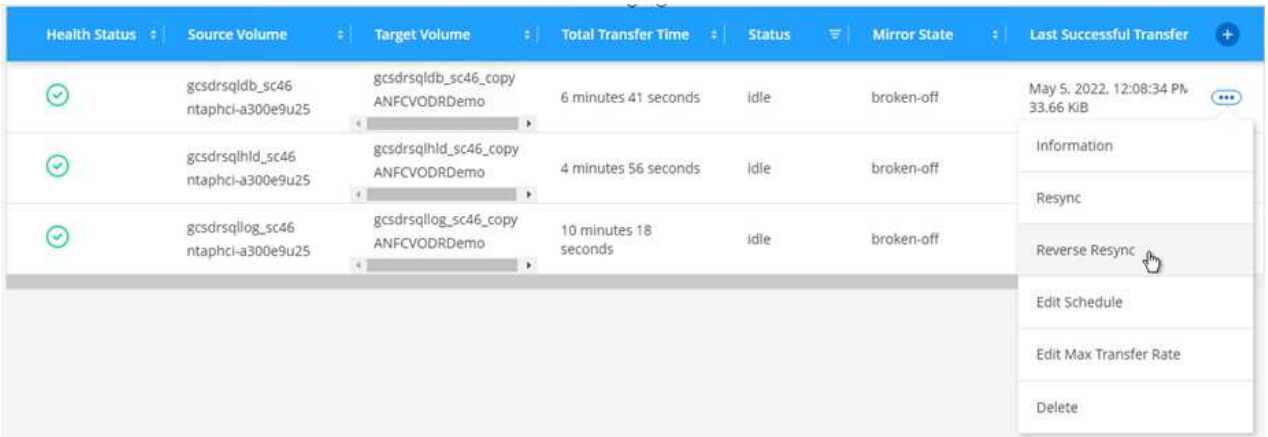
Préciser le délai maximal après la mise en pause des VM dans le site de reprise, puis leur redémarrage sur le site protégé. Le temps nécessaire à l'exécution de ce processus comprend l'achèvement de la réplication après l'arrêt des VM de basculement, le temps nécessaire pour nettoyer le site de reprise et le temps nécessaire pour recréer les VM sur le site protégé. NetApp recommande 10 minutes.

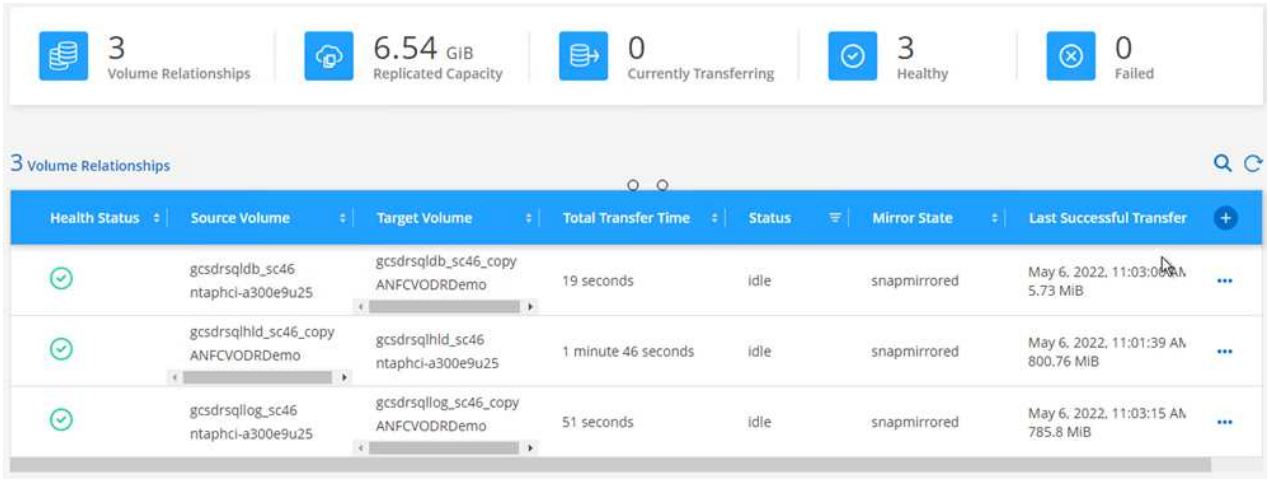


3. Suivre le processus de retour arrière, puis confirmer la reprise de la protection des machines virtuelles et la cohérence des données.

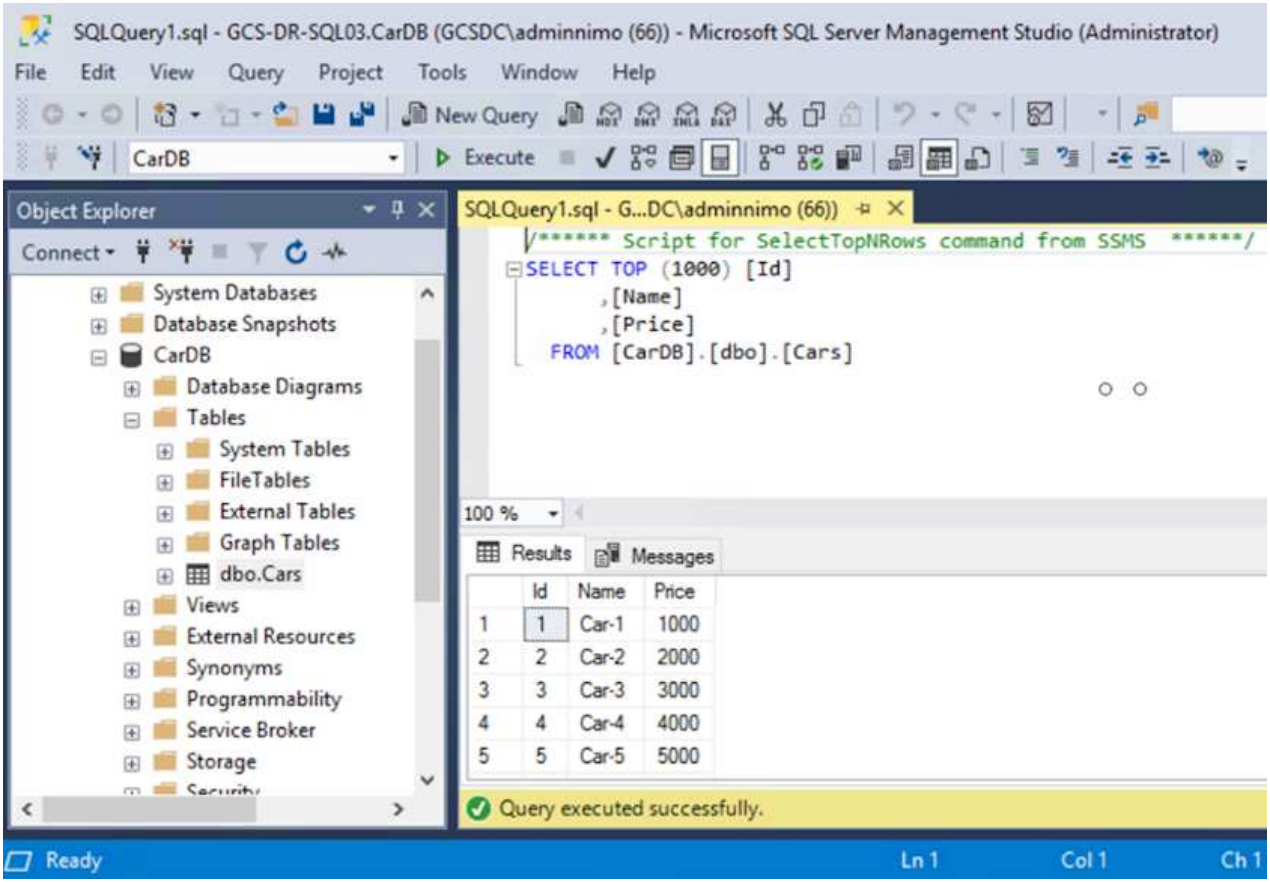


4. Une fois les machines virtuelles restaurées, déconnectez le stockage secondaire de l'hôte et connectez-vous au stockage primaire.





5. Redémarrez le service serveur MSSQL.
6. Vérifiez que les ressources SQL sont de nouveau en ligne.



Pour revenir au stockage primaire, veillez à ce que la direction de la relation reste la même qu'avant le basculement en effectuant une opération de resynchronisation inverse.

Pour conserver les rôles de stockage primaire et secondaire après l'opération de resynchronisation inverse, effectuez à nouveau l'opération de resynchronisation inverse.

Ce processus s'applique à d'autres applications telles qu'Oracle, des versions similaires des bases de données et à toutes les autres applications qui utilisent un système de stockage connecté par l'invité.

Comme toujours, testez les étapes de récupération des charges de travail critiques avant de les porter en production.

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
  - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- L'optimisation du processeur et de la RAM permet de réduire les coûts liés au cloud en permettant la restauration sur des clusters de calcul plus petits.

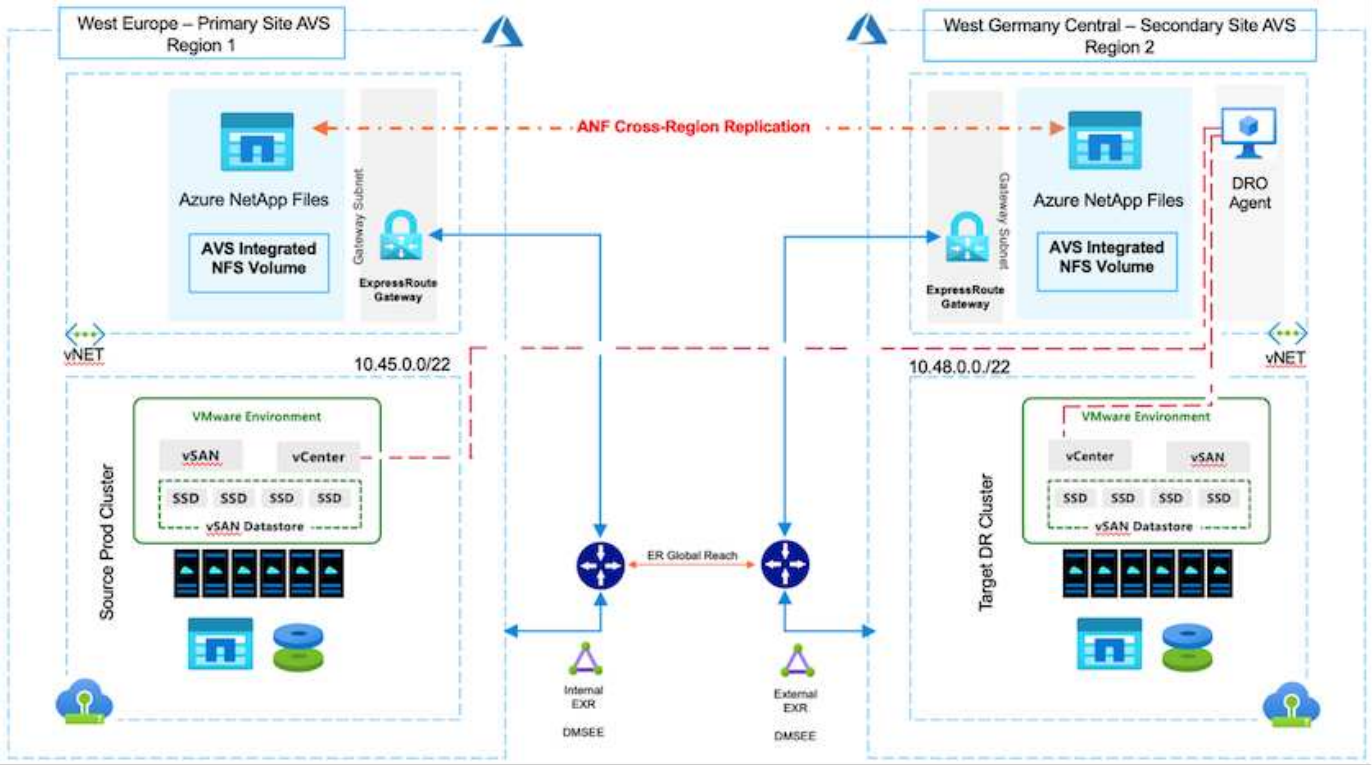
Tr-4955 : reprise d'activité avec Azure NetApp Files (ANF) et solution Azure VMware (AVS)

Auteur(s) : Niyaz Mohamed, ingénierie des solutions NetApp

Présentation

La reprise d'activité avec réplication au niveau des blocs entre les régions dans le cloud est un moyen résilient et économique de protéger les workloads contre les pannes sur site et les corruptions de données (par exemple, les ransomwares). Avec la réplication de volume inter-régions Azure NetApp Files (ANF), les workloads VMware s'exécutant sur un site SDDC Azure VMware solution (AVS) avec des volumes Azure NetApp Files en tant que datastore NFS sur le site AVS principal peuvent être répliqués sur un site AVS secondaire désigné dans la région de restauration cible.

L'orchestrateur de reprise après incident (DRO) (une solution basée sur des scripts avec interface utilisateur) peut être utilisé pour restaurer de manière fluide les workloads répliqués depuis un SDDC AVS. DRO automatise la restauration en rompant le peering de réplication, puis en montant le volume de destination en tant que datastore, via l'enregistrement de machine virtuelle vers AVS, en passant par les mappages du réseau directement sur NSX-T (inclus avec tous les clouds privés AVS).



Conditions préalables et recommandations générales

- Vérifiez que vous avez activé la réplication entre les régions en créant le peering de réplication. Voir "Création d'une réplication de volume pour Azure NetApp Files".
- Vous devez configurer ExpressRoute Global Reach entre les clouds privés de la solution Azure VMware source et cible.
- Vous devez disposer d'une entité de service pouvant accéder aux ressources.
- La topologie suivante est prise en charge : du site AVS principal au site AVS secondaire.
- Configurer le "la réplication" planifiez chaque volume de manière appropriée en fonction des besoins de l'entreprise et du taux de changement des données.

Les topologies en cascade, « Fan-In » et « Fan-Out » ne sont pas prises en charge.

Pour commencer

Déployez la solution Azure VMware

Le "Solution Azure VMware" (AVS) est un service de cloud hybride qui fournit des data centers complets VMware dans un cloud public Microsoft Azure. AVS est une solution première entièrement gérée et prise en charge par Microsoft, puis vérifiée par VMware qui utilise l'infrastructure Azure. Par conséquent, les clients bénéficient de VMware ESXi pour la virtualisation du calcul, de VSAN pour le stockage hyperconvergé et de NSX pour la mise en réseau et la sécurité, tout en exploitant la présence mondiale de Microsoft Azure, les installations de data Center de pointe et la proximité du riche écosystème de services et de solutions Azure natifs. La combinaison d'Azure VMware solution SDDC et d'Azure NetApp Files offre les meilleures performances et une latence réseau minimale.

Pour configurer un cloud privé AVS sur Azure, suivez la procédure décrite dans cette section "lien" Pour la documentation NetApp et dans ce document "lien" Pour la documentation Microsoft. Un environnement de pilote léger configuré avec une configuration minimale peut être utilisé à des fins de reprise sur incident. Cette

configuration ne contient que des composants de base pour prendre en charge les applications stratégiques, et elle peut évoluer horizontalement et générer plus d'hôtes pour prendre la charge en bloc en cas de basculement.

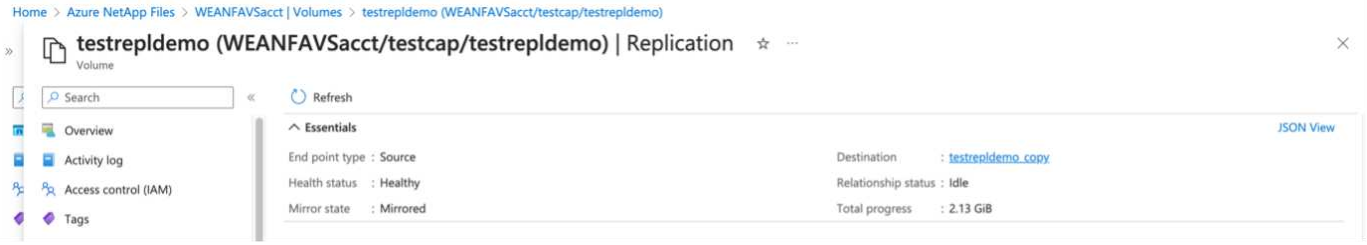
Dans la version initiale, DRO prend en charge un cluster SDDC existant. La création d'un SDDC à la demande sera disponible dans une prochaine version.

Provisionner et configurer Azure NetApp Files

"Azure NetApp Files" service de stockage de fichiers haute performance et mesuré. Suivez les étapes de cette procédure "lien" Pour provisionner et configurer Azure NetApp Files en tant que datastore NFS afin d'optimiser les déploiements de cloud privé AVS.

Créez une réplication de volume pour les volumes de datastore Azure NetApp Files

La première étape consiste à configurer la réplication interrégionale pour les volumes de datastore souhaités du site principal AVS vers le site secondaire AVS avec les fréquences et les rétentions appropriées.



Suivez les étapes de cette procédure "lien" pour configurer la réplication entre les régions en créant le peering de réplication. Le niveau de service du pool de capacité de destination peut correspondre à celui du pool de capacité source. Toutefois, pour ce cas d'utilisation spécifique, vous pouvez sélectionner le niveau de service standard, puis "modifier le niveau de service" En cas d'incident réel ou de simulations de reprise sur incident.

Une relation de réplication entre régions est un prérequis et doit être créée au préalable.

Installation de DRO

Pour commencer avec DRO, utilisez le système d'exploitation Ubuntu sur la machine virtuelle Azure désignée et assurez-vous de respecter les conditions préalables. Installez ensuite le package.

Conditions préalables :

- Principal de service pouvant accéder aux ressources.
- Assurez-vous qu'une connectivité appropriée existe aux instances source et de destination du SDDC et du Azure NetApp Files.
- La résolution DNS doit être en place si vous utilisez des noms DNS. Sinon, utilisez les adresses IP pour vCenter.

Système d'exploitation requis :

- Ubuntu focal 20.04 (LTS)les paquets suivants doivent être installés sur la machine virtuelle de l'agent désignée :
- Docker

- Docker- compose
- JqModifier `docker.sock` à cette nouvelle autorisation : `sudo chmod 666 /var/run/docker.sock`.

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

Les étapes sont les suivantes :

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

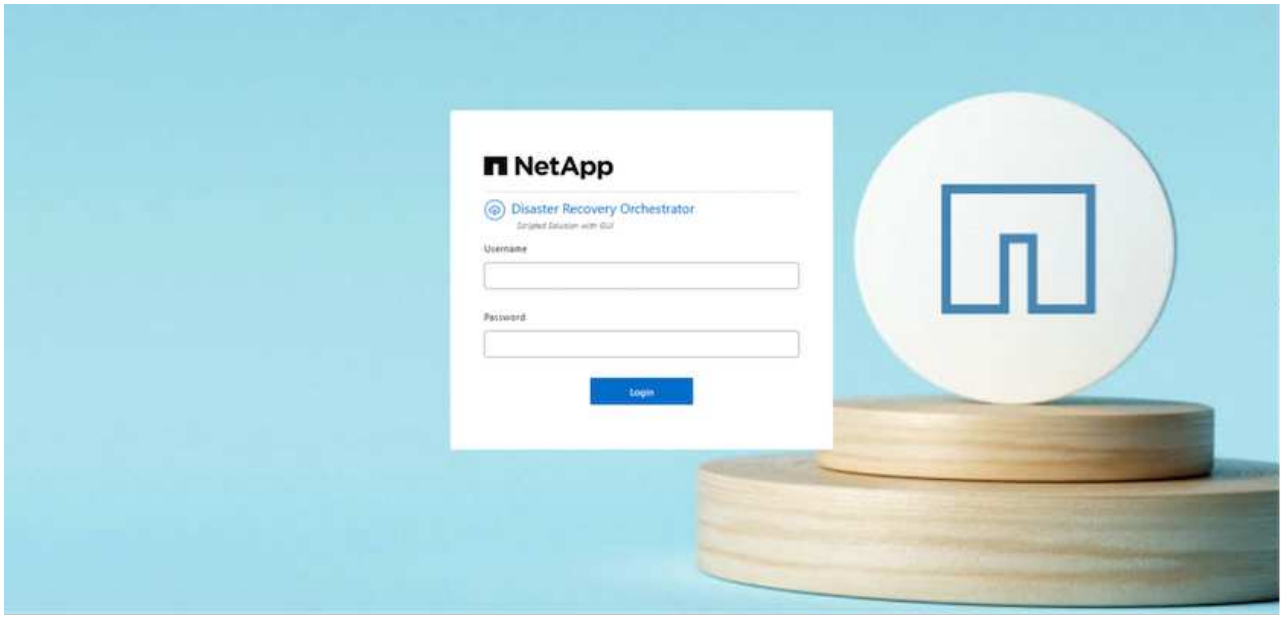
```
git clone https://github.com/NetApp/DRO-Azure.git
```

L'agent doit être installé dans la région du site AVS secondaire ou dans la région du site AVS principal dans une zone de disponibilité autre que le SDDC.

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

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Accédez à l'interface utilisateur à l'aide des informations d'identification suivantes :
   - Nom d'utilisateur : `admin`
   - Mot de passe : `admin`



Configuration DRO

Une fois que Azure NetApp Files et AVS ont été correctement configurés, vous pouvez commencer à

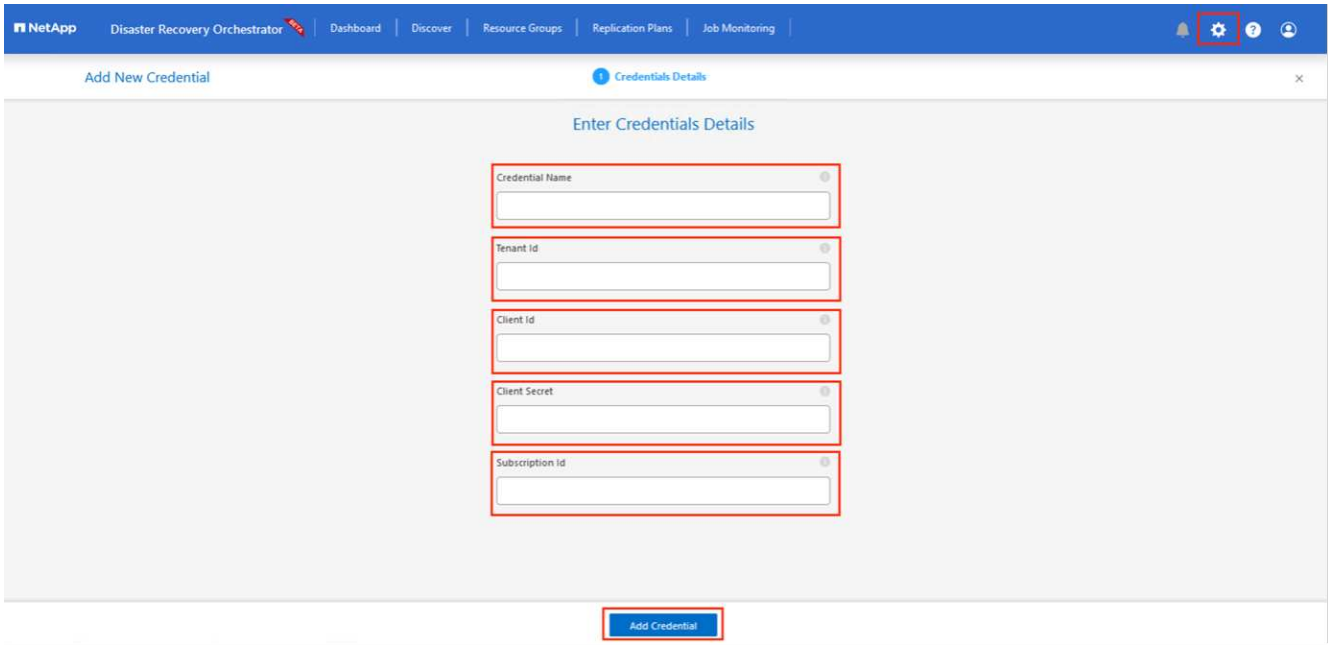
configurer DRO afin d'automatiser la restauration des workloads du site AVS principal vers le site AVS secondaire. NetApp recommande de déployer l'agent DRO sur le site AVS secondaire et de configurer la connexion de passerelle ExpressRoute de sorte que l'agent DRO puisse communiquer via le réseau avec les composants AVS et Azure NetApp Files appropriés.

La première étape consiste à ajouter des informations d'identification. DRO nécessite l'autorisation de découvrir Azure NetApp Files et la solution Azure VMware. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une application Azure Active Directory (AD) et en obtenant les identifiants Azure dont DRO a besoin. Vous devez lier l'entité de service à votre abonnement Azure et lui attribuer un rôle personnalisé disposant des autorisations requises appropriées. Lorsque vous ajoutez des environnements source et de destination, vous êtes invité à sélectionner les informations d'identification associées à l'entité de service. Vous devez ajouter ces informations d'identification à DRO avant de cliquer sur Ajouter un nouveau site.

Pour effectuer cette opération, procédez comme suit :

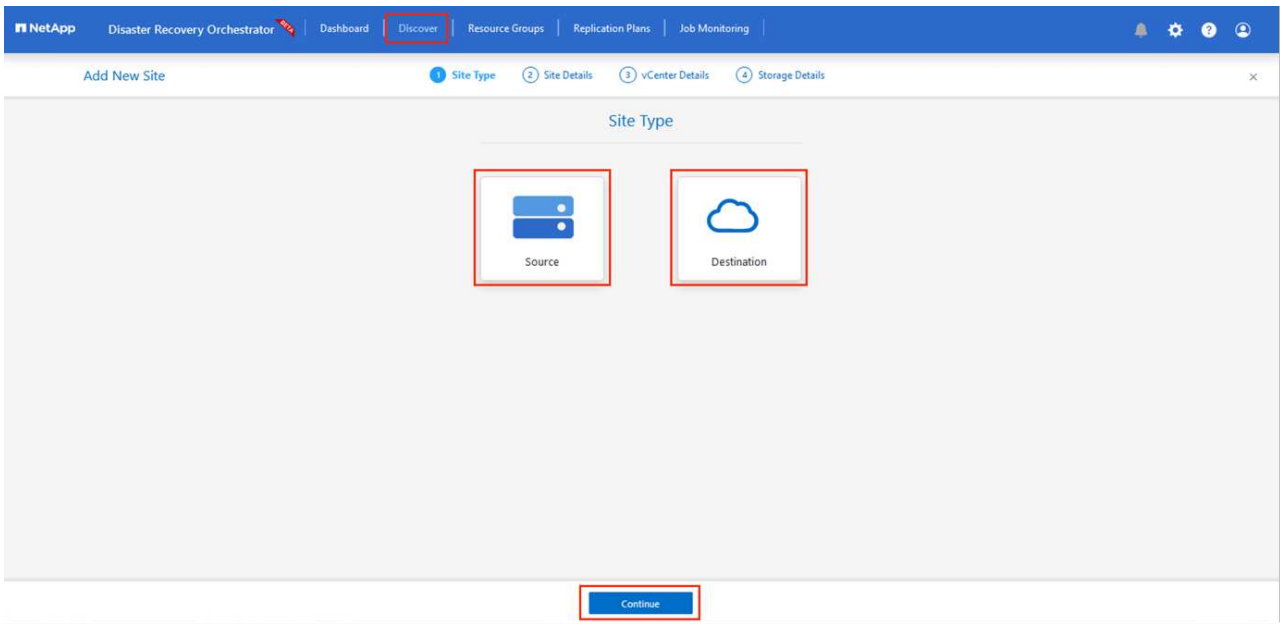
1. Ouvrez DRO dans un navigateur pris en charge et utilisez le nom d'utilisateur et le mot de passe par défaut (`admin`/`admin`). Le mot de passe peut être réinitialisé après la première connexion à l'aide de l'option Modifier le mot de passe.
2. Dans le coin supérieur droit de la console DRO, cliquez sur l'icône **Settings** et sélectionnez **Credentials**.
3. Cliquez sur Ajouter une nouvelle information d'identification et suivez les étapes de l'assistant.
4. Pour définir les informations d'identification, entrez les informations relatives au principal du service Azure Active Directory qui accorde les autorisations requises :
   - Nom d'identification
   - ID locataire
   - ID client
   - Secret client
   - ID d'abonnement

     Vous devez avoir capturé ces informations lorsque vous avez créé l'application AD.
5. Confirmez les détails des nouvelles informations d'identification et cliquez sur Ajouter une information d'identification.



Après avoir ajouté les identifiants, il est temps de découvrir et d'ajouter les sites AVS principaux et secondaires (à la fois vCenter et le compte de stockage Azure NetApp Files) à DRO. Pour ajouter le site source et le site de destination, procédez comme suit :

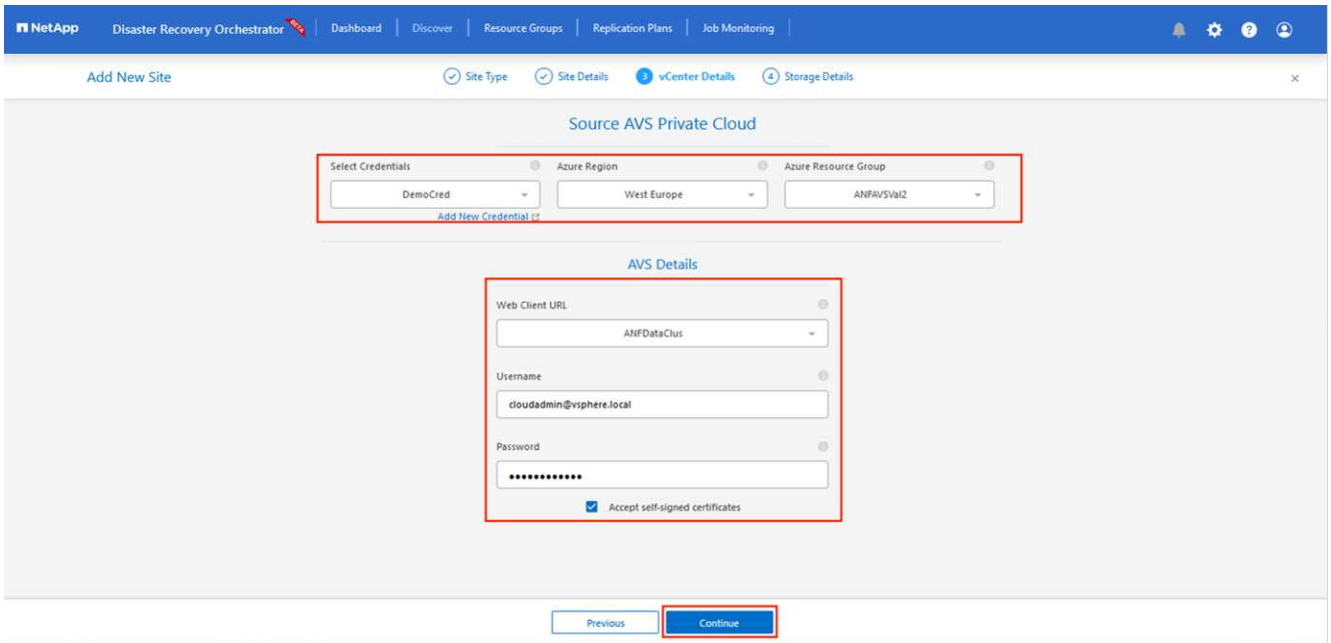
6. Accédez à l'onglet **Discover**.
7. Cliquez sur **Ajouter un nouveau site**.
8. Ajoutez le site AVS principal suivant (désigné comme **Source** dans la console).
   - VCenter SDDC
   - Compte de stockage Azure NetApp Files
9. Ajoutez le site AVS secondaire suivant (désigné comme **destination** dans la console).
   - VCenter SDDC
   - Compte de stockage Azure NetApp Files



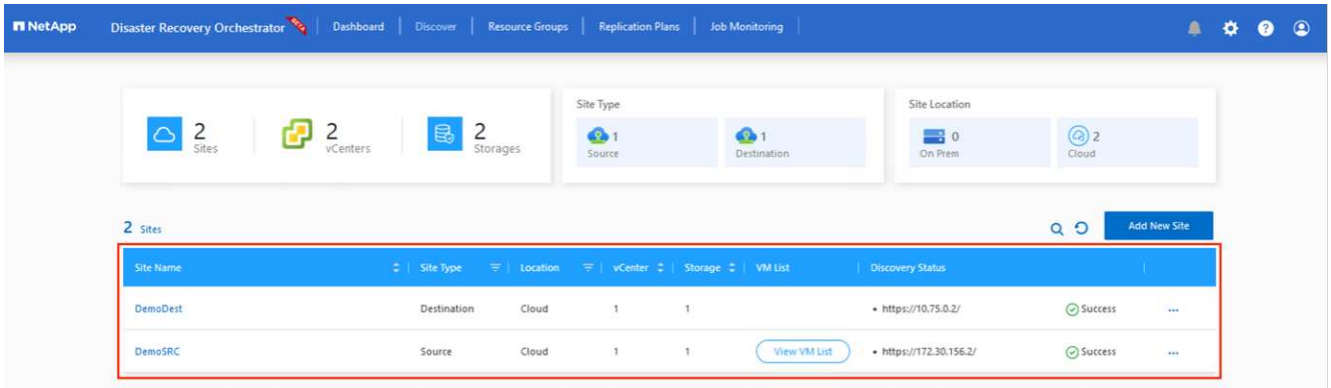
10. Ajoutez les détails du site en cliquant sur **Source**, en saisissant un nom de site convivial, puis sélectionnez le connecteur. Cliquez ensuite sur **Continuer**.

   À des fins de démonstration, l'ajout d'un site source est abordé dans ce document.

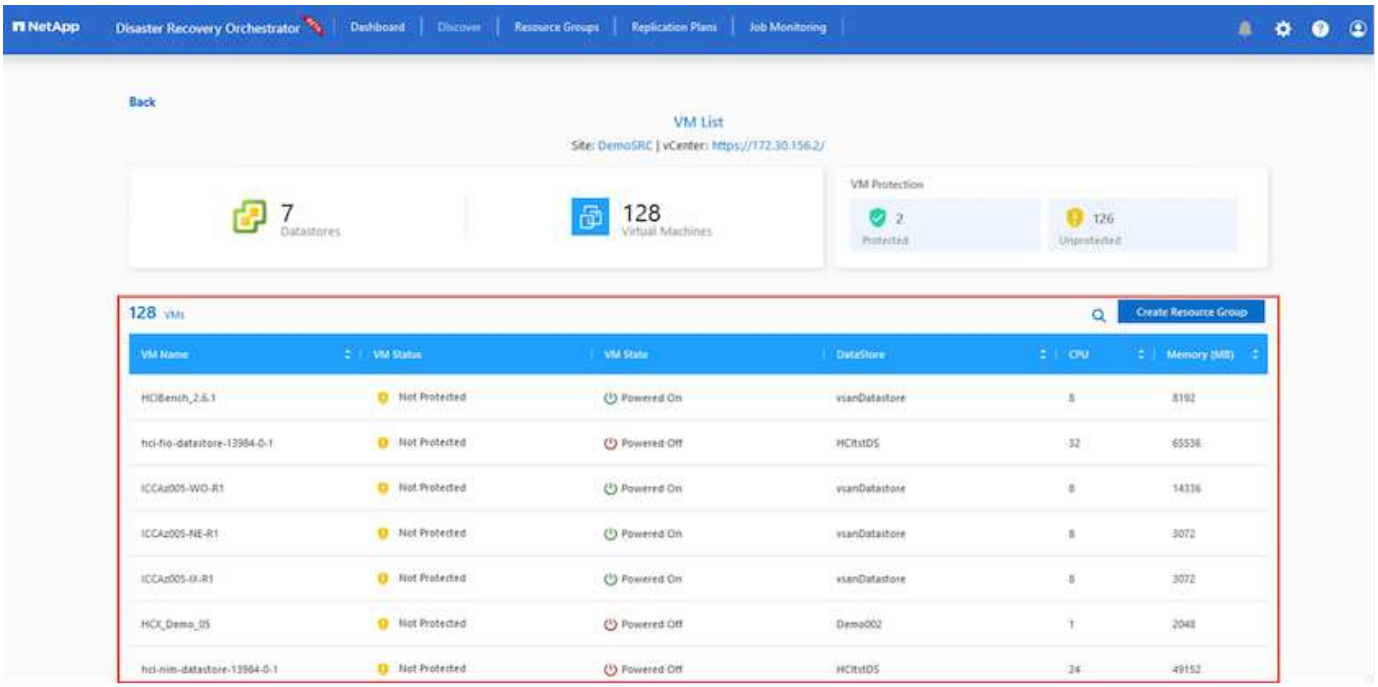
11. Mettez à jour les détails de vCenter. Pour ce faire, sélectionnez les informations d'identification, la région Azure et le groupe de ressources dans le menu déroulant du SDDC AVS principal.
12. DRO répertorie tous les SDDC disponibles dans la région. Sélectionnez l'URL de cloud privé désignée dans la liste déroulante.
13. Entrez le `cloudadmin@vsphere.local` informations d'identification de l'utilisateur. Vous pouvez y accéder depuis le portail Azure. Suivez les étapes mentionnées dans ce document "lien". Une fois terminé, cliquez sur **Continuer**.



14. Sélectionnez le groupe de ressources Azure et le compte NetApp dans les détails du stockage source (ANF).
15. Cliquez sur **Créer un site**.



Une fois ajouté, DRO effectue une détection automatique et affiche les VM qui ont des répliques inter-régions correspondantes du site source au site de destination. DRO détecte automatiquement les réseaux et les segments utilisés par les machines virtuelles et les remplit.



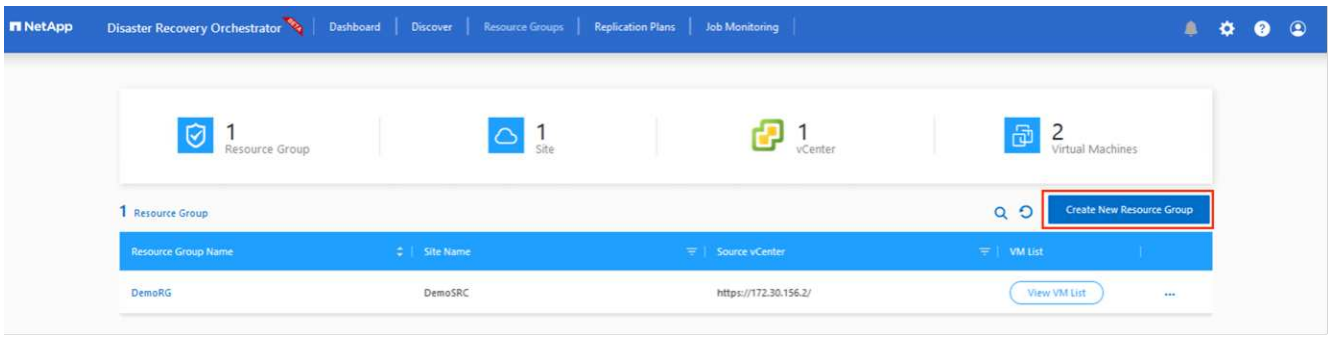
L’étape suivante consiste à regrouper les VM requises dans leurs groupes fonctionnels en tant que groupes de ressources.

Regroupements de ressources

Une fois les plates-formes ajoutées, regroupez les VM que vous souhaitez restaurer en 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, cliquez sur l’élément de menu **Créer un nouveau groupe de ressources**.

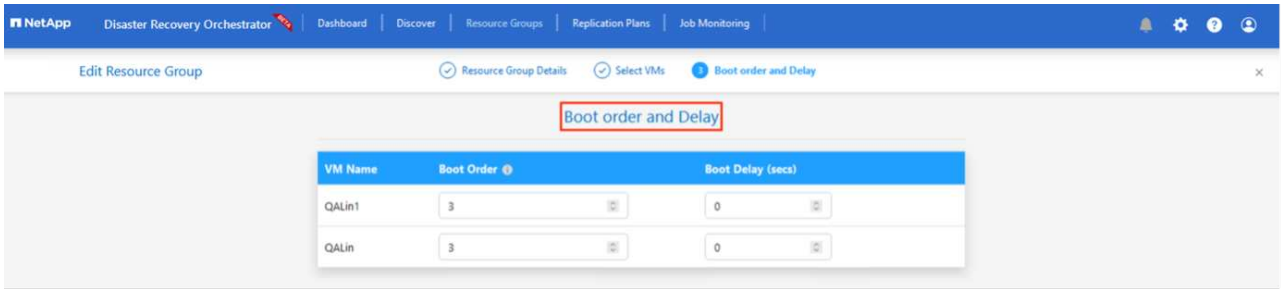
1. Accédez à **Resource Grou*ps et cliquez sur *Create New Resource Group**.



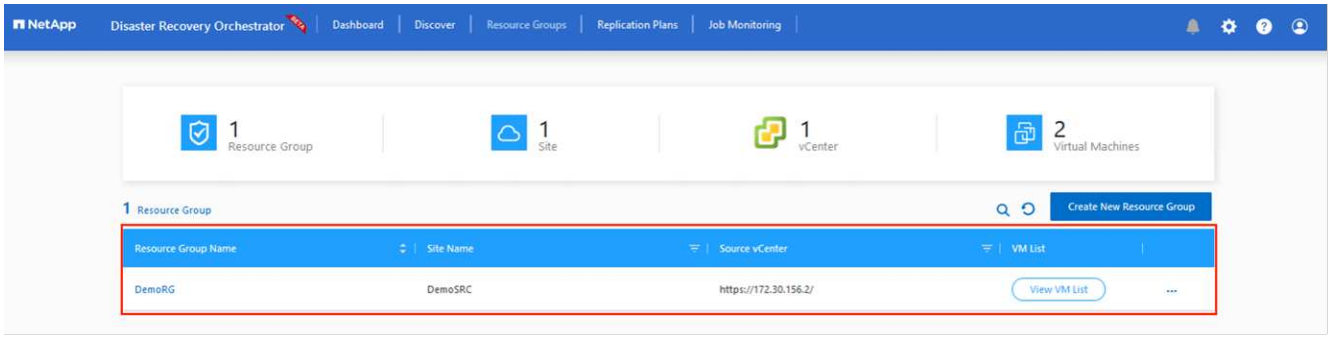
2. Sous Nouveau groupe de ressources, sélectionnez le site source dans la liste déroulante et cliquez sur **Créer**.
3. Fournissez les détails du groupe de ressources et cliquez sur **Continuer**.
4. Sélectionnez les machines virtuelles appropriées à l’aide de l’option de recherche.
5. Sélectionnez **Boot Order** et **Boot Delay** (sec) pour toutes les machines virtuelles sélectionnées. Définissez l’ordre de la séquence de mise sous tension en sélectionnant chaque machine virtuelle et en

définissant sa priorité. La valeur par défaut pour toutes les machines virtuelles est 3. Les options sont les suivantes :

- Première machine virtuelle à mettre sous tension
- Valeur par défaut
- Dernière machine virtuelle à mettre sous tension



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

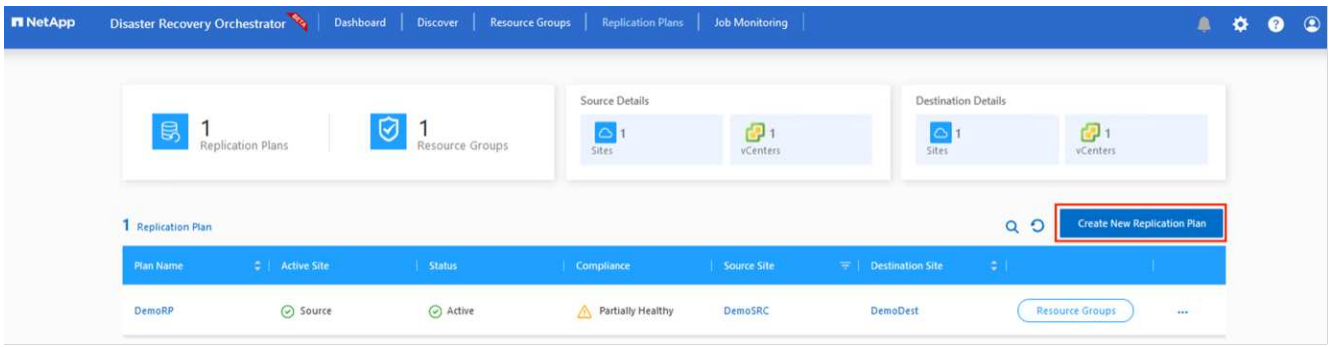


Plans de réplication

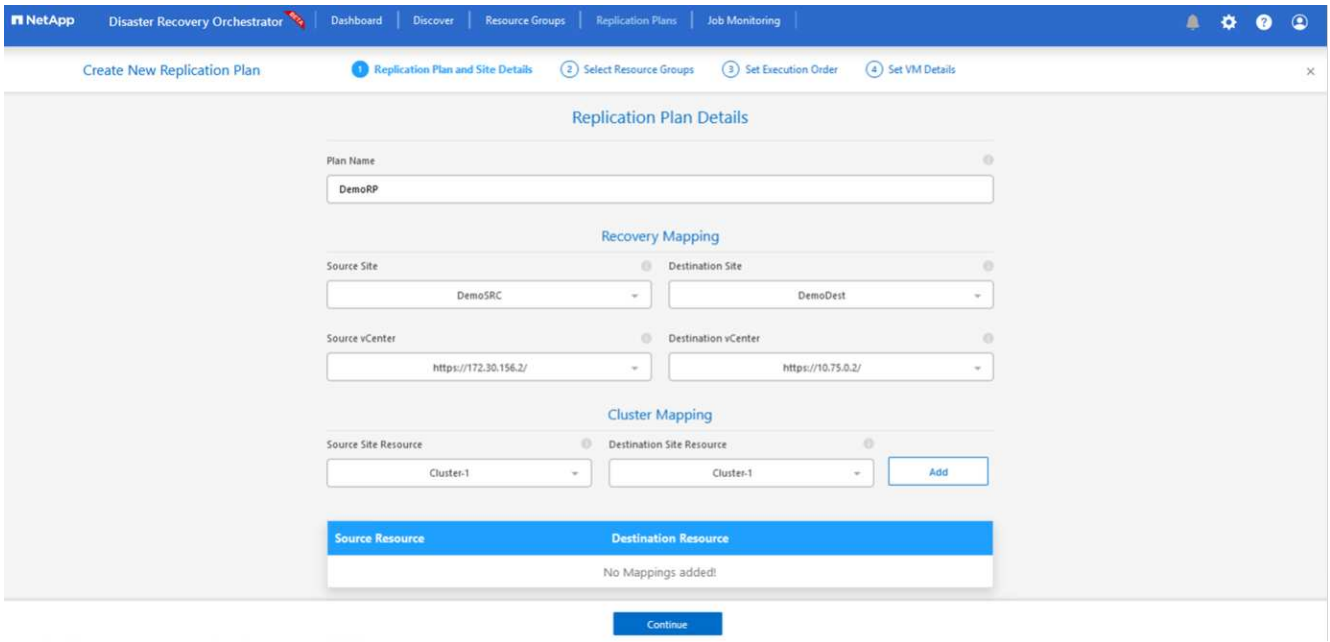
En cas d'incident, vous devez disposer d'un plan de restauration des applications. Sélectionnez les plateformes vCenter source et cible dans la liste déroulante, choisissez les groupes de ressources à inclure dans ce plan, ainsi que le regroupement des méthodes de restauration et de mise sous tension des applications (par exemple, contrôleurs de domaine, niveau 1, niveau 2, etc.). Les plans sont souvent appelés plans. Pour définir le plan de reprise, accédez à l'onglet Replication Plan, puis cliquez sur **Nouveau plan de réplication**.

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

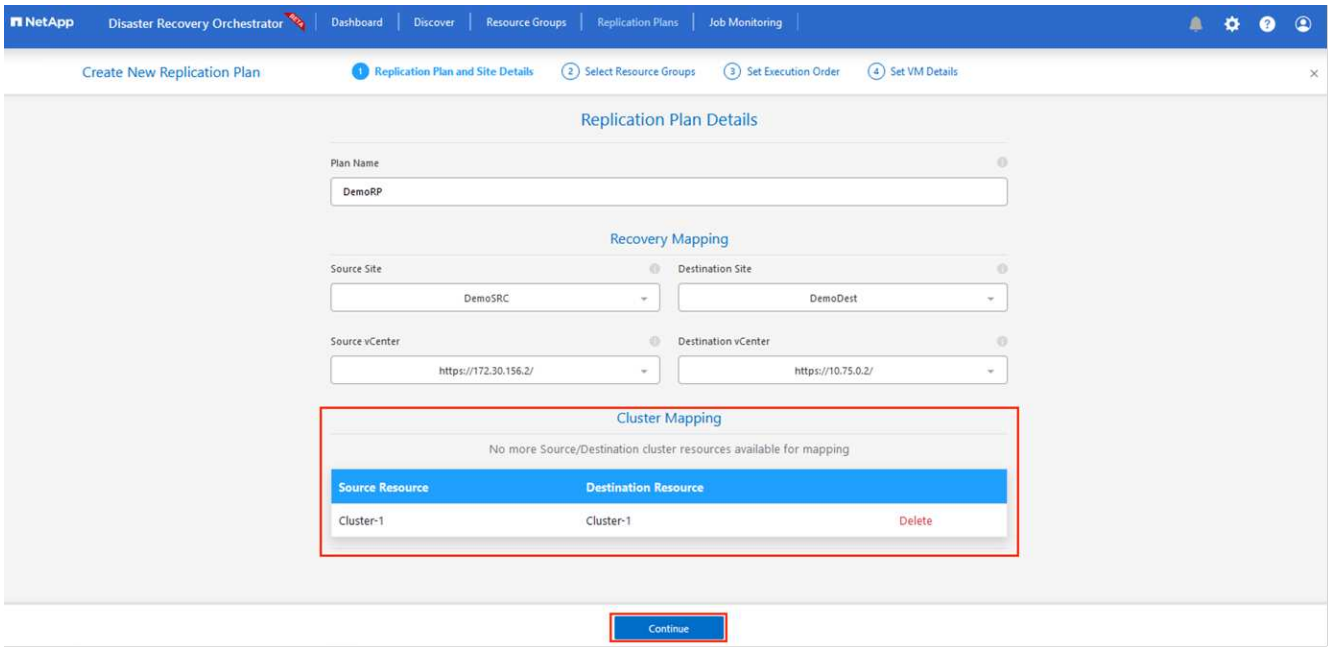
1. Naviguez jusqu'à **plans de réplication** et cliquez sur **Créer un nouveau plan de réplication**.



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

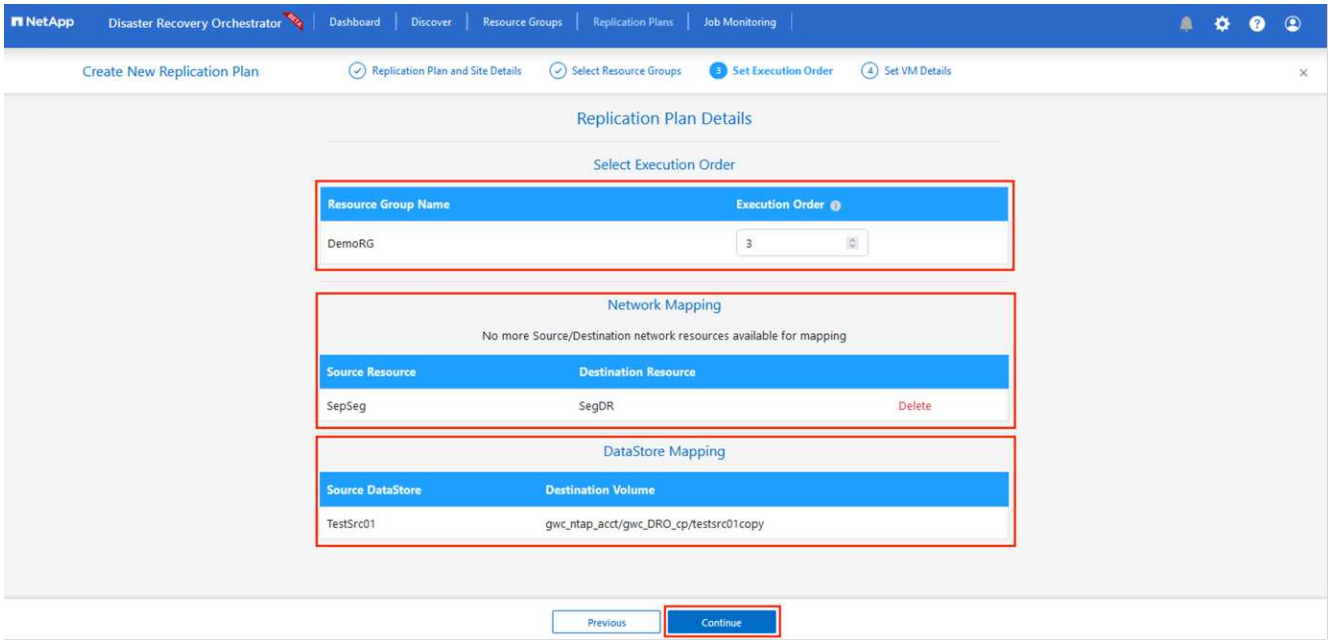


3. Une fois le mappage de récupération terminé, sélectionnez **Cluster Mapping**.

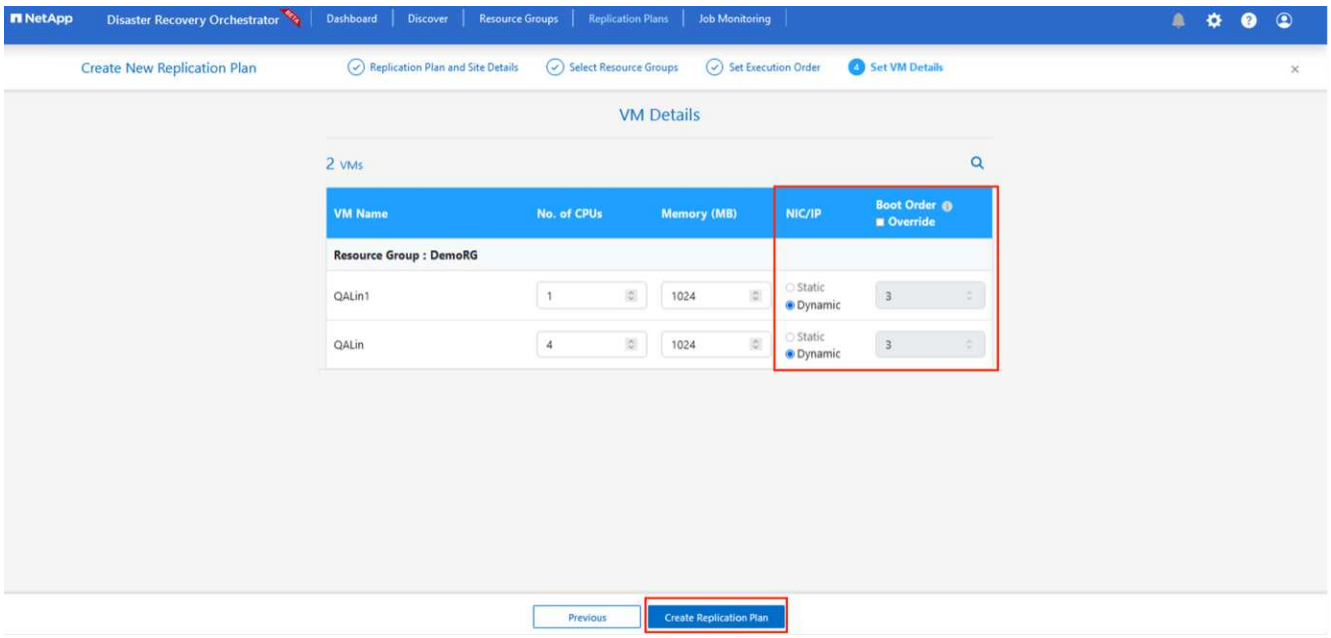


4. Sélectionnez **Détails du groupe de ressources** et cliquez sur **Continuer**.
5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsqu'il existe plusieurs groupes de ressources.
6. Une fois l'opération terminée, définissez le mappage réseau sur le segment approprié. Les segments doivent déjà être provisionnés sur le cluster AVS secondaire et, pour mapper les VM vers ceux-ci, sélectionnez le segment approprié.
7. Les mappages de datastores sont sélectionnés automatiquement en fonction de la sélection de machines virtuelles.

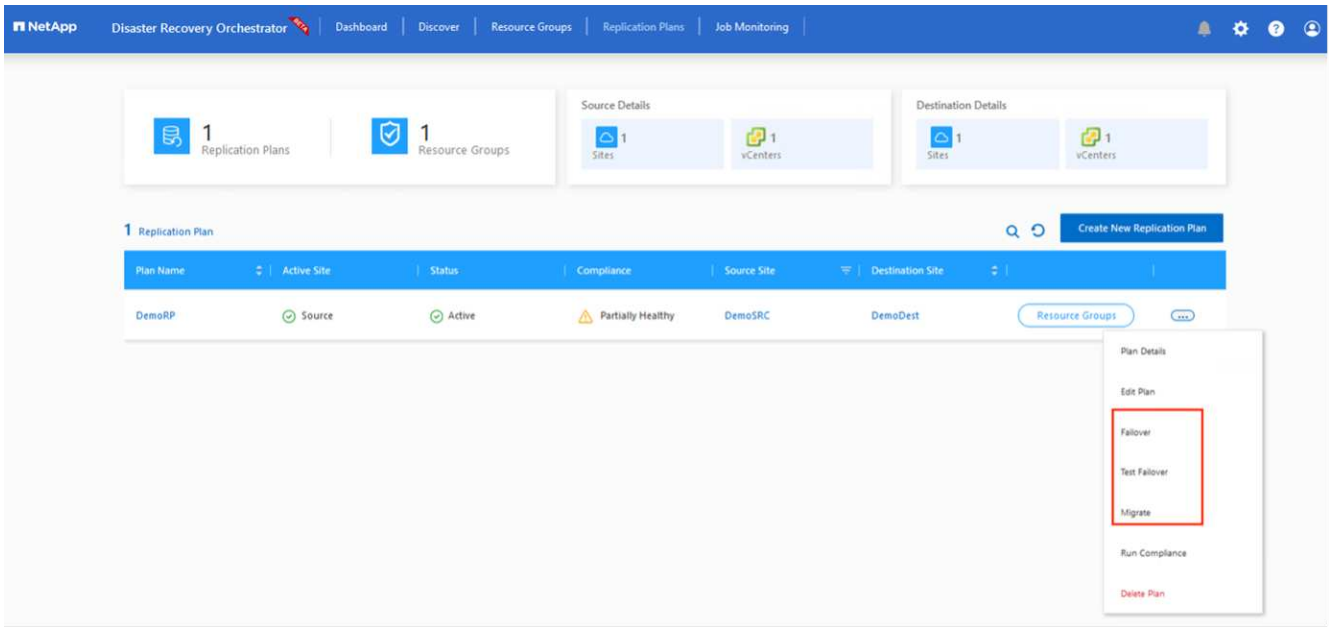
La réplication interrégionale (CRR) se situe au niveau du volume. Par conséquent, toutes les VM résidant sur le volume respectif sont répliquées vers la destination CRR. Assurez-vous de sélectionner toutes les machines virtuelles qui font partie du datastore, car seules les machines virtuelles qui font partie du plan de réplication sont traitées.



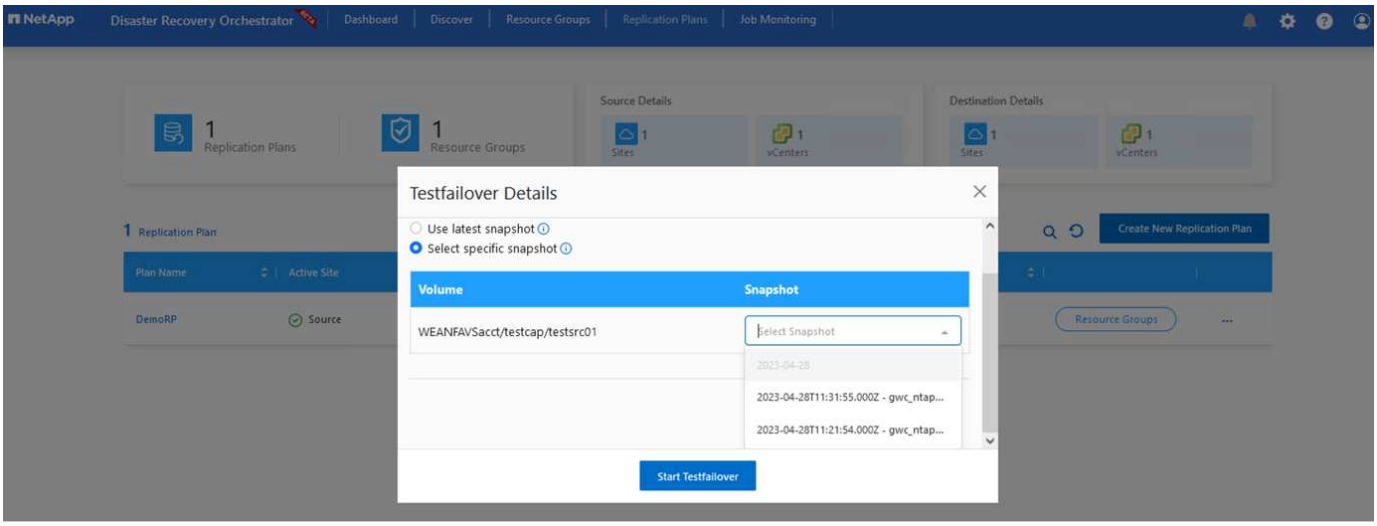
8. Sous VM details, vous pouvez éventuellement redimensionner les paramètres CPU et RAM des VM. Cela peut s'avérer très utile lorsque vous récupérez de grands environnements sur des clusters cibles plus petits ou lorsque vous effectuez des tests de reprise après incident sans avoir à provisionner une infrastructure VMware physique individuelle. Modifiez également l'ordre de démarrage et le délai de démarrage (s) pour toutes les machines virtuelles sélectionnées dans les groupes de ressources. Il existe une option supplémentaire pour modifier l'ordre de démarrage si des modifications sont requises par rapport à ce que vous avez sélectionné lors de la sélection de l'ordre de démarrage ressource-groupe. Par défaut, l'ordre de démarrage sélectionné lors de la sélection de groupe de ressources est utilisé, mais toutes les modifications peuvent être effectuées à ce stade.



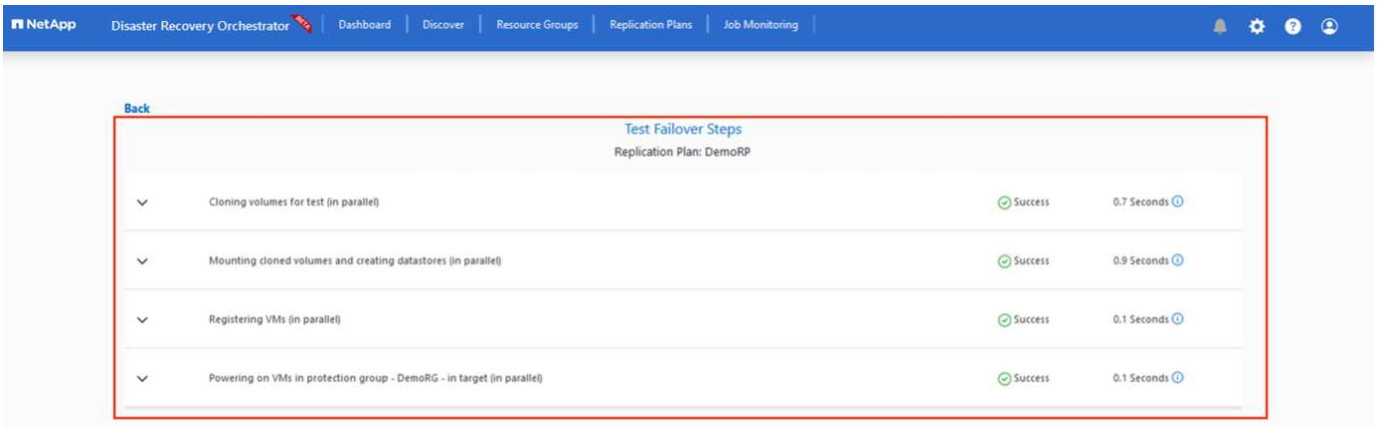
9. Cliquez sur **Créer un plan de réplication**.une fois le plan de réplication créé, vous pouvez utiliser les options de basculement, de basculement ou de migration selon vos besoins.



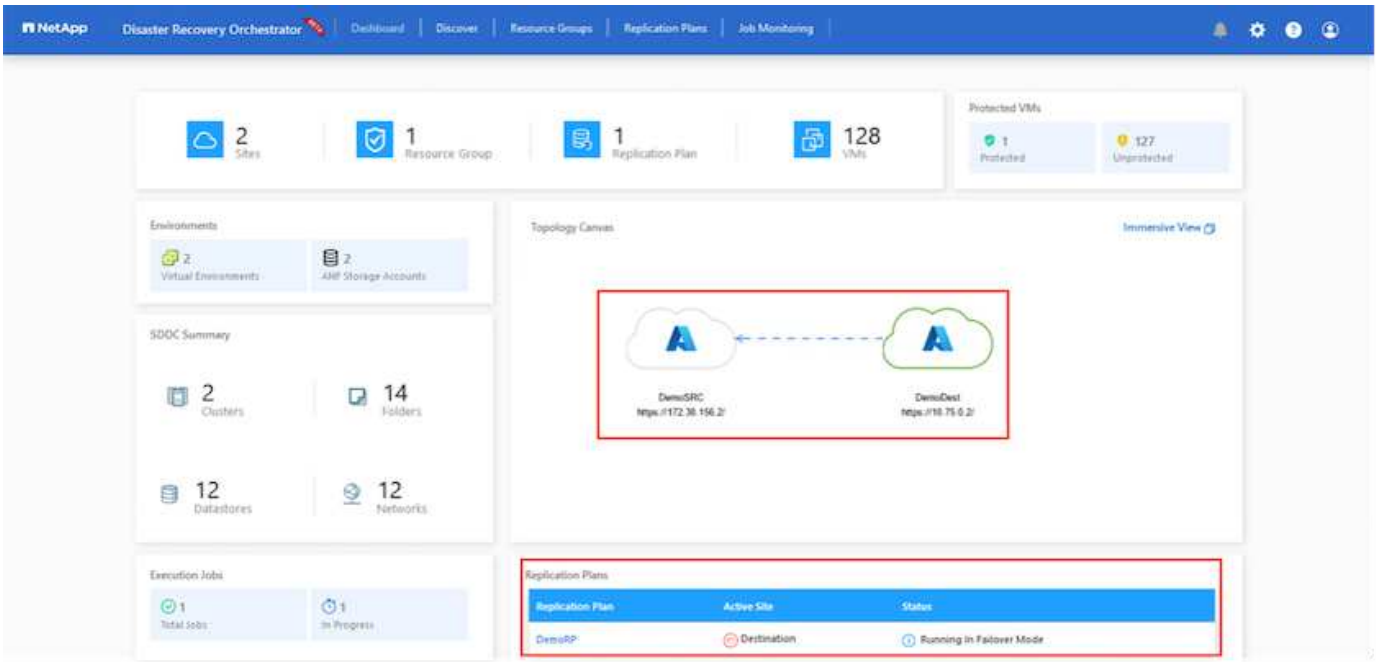
Au cours des options de basculement et de test, le snapshot le plus récent est utilisé ou un snapshot spécifique peut être sélectionné à partir d'un snapshot instantané. L'option instantanée peut être très avantageuse si vous êtes confronté à une situation de corruption, comme les ransomwares, où les réplicas les plus récents sont déjà compromis ou chiffrés. DRO affiche tous les points temporels disponibles.



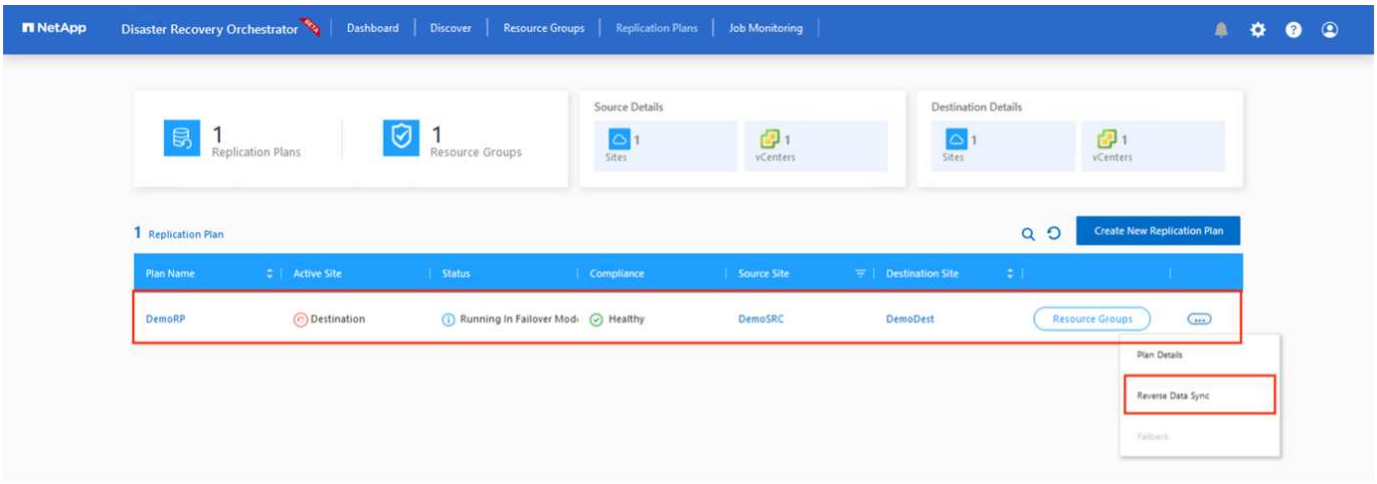
Pour déclencher le basculement ou tester le basculement avec la configuration spécifiée dans le plan de réplication, vous pouvez cliquer sur **basculement** ou **Test basculement**. Vous pouvez contrôler le plan de réplication dans le menu des tâches.



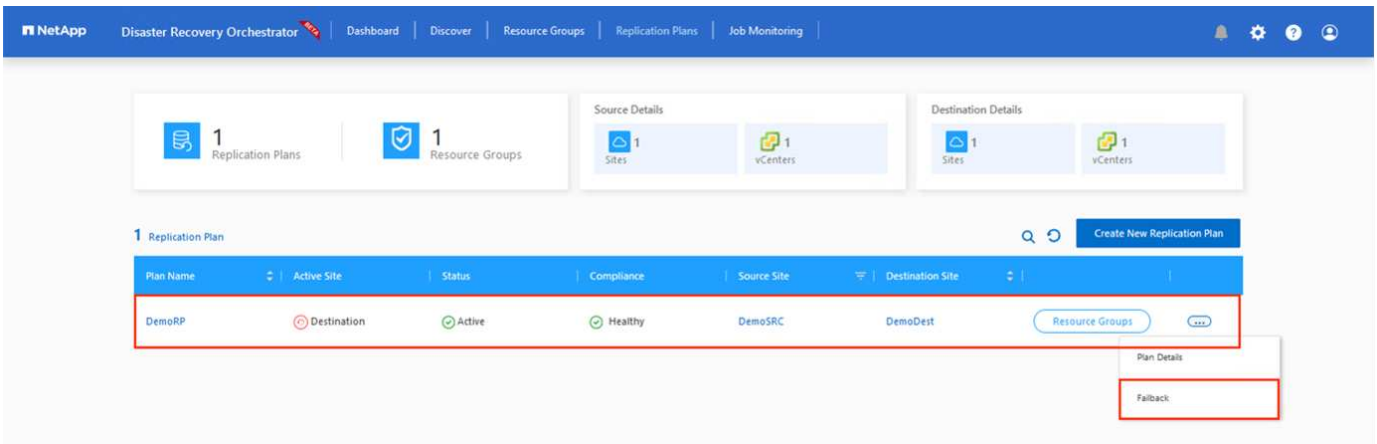
Une fois le basculement déclenché, les éléments récupérés sont visibles sur le site secondaire AVS SDDC vCenter (VM, réseaux et datastores). Par défaut, les machines virtuelles sont restaurées dans le dossier Workload.

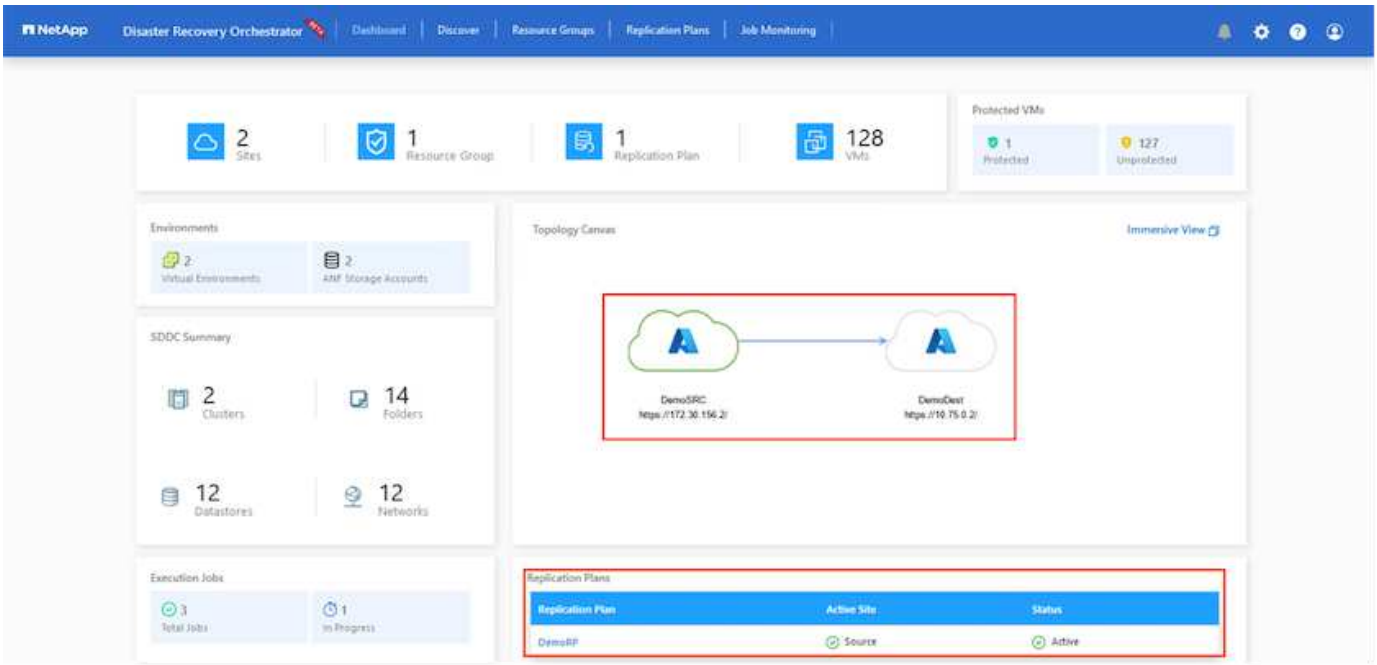


La restauration peut être déclenchée au niveau du plan de réplication. En cas de basculement de test, l'option de démontage peut être utilisée pour annuler les modifications et supprimer le nouveau volume créé. Les retours arrière liés au basculement sont un processus en deux étapes. Sélectionnez le plan de réplication et sélectionnez **Inverser la synchronisation des données**.



Une fois cette étape terminée, déclenchez la restauration pour revenir au site AVS principal.





Depuis le portail Azure, nous constatons que l'état de la réplication a été rompu pour les volumes appropriés mappés au SDDC AVS du site secondaire en tant que volumes de lecture/écriture. Pendant le basculement de test, DRO ne mappe pas le volume de destination ou de réplica. Elle crée un nouveau volume du snapshot de

réplication interrégionale requis et expose le volume en tant que datastore, ce qui consomme de la capacité physique supplémentaire du pool de capacité et garantit que le volume source n'est pas modifié. Les tâches de réplication peuvent notamment se poursuivre pendant les tests de reprise d'activité ou les workflows de hiérarchisation. De plus, ce processus permet de s'assurer que la restauration peut être nettoyée sans risque de destruction de la réplique si des erreurs se produisent ou si des données corrompues sont récupérées.

Restauration par ransomware

Récupérer des données suite à un ransomware peut être une tâche extrêmement fastidieuse. Plus précisément, il peut être difficile pour les services IT de déterminer le point de retour sûr et, une fois déterminé, comment s'assurer que les charges de travail restaurées sont protégées contre les attaques qui se produisent (par exemple, suite à un malware en sommeil ou à des applications vulnérables).

La DRO répond à ces préoccupations en permettant aux entreprises de récupérer leurs données à partir d'un point de disponibilité dans le temps. Les charges de travail sont ensuite restaurées sur des réseaux fonctionnels mais isolés, de sorte que les applications puissent fonctionner et communiquer les unes avec les autres, sans toutefois être exposées au trafic nord-sud. Ce processus permet aux équipes de sécurité d'effectuer des analyses et d'identifier tout malware caché ou endormi.

Conclusion

La solution de reprise d'activité Azure NetApp Files et Azure VMware offre les avantages suivants :

- Exploitez la réplication interrégionale Azure NetApp Files efficace et résiliente.
- Restaurez vos données à un point dans le temps grâce à la conservation des copies Snapshot.
- Automatisez entièrement toutes les étapes requises pour restaurer des centaines, voire des milliers de machines virtuelles à partir des étapes de validation du stockage, du calcul, du réseau et des applications.
- La restauration des charges de travail repose sur le processus de « création de nouveaux volumes à partir des snapshots les plus récents », qui ne manipule pas le volume répliqué.
- Évitez tout risque de corruption des données sur les volumes ou les snapshots.
- Évitez les interruptions de réplication lors des workflows de test de reprise après incident.
- Exploitez les données de reprise d'activité et les ressources de calcul cloud pour les workflows en dehors de la reprise d'activité, tels que le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de correction.
- L'optimisation des processeurs et de la RAM peut contribuer à réduire les coûts du cloud en permettant la restauration vers des clusters de calcul plus petits.

Où trouver des informations complémentaires

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

- Création d'une réplication de volume pour Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Réplication entre les régions de volumes Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Solution Azure VMware"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Déploiement et configuration de l'environnement de virtualisation sur Azure

  "Configurez AVS sur Azure"

- Déploiement et configuration de la solution Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Utilisation de la réplication Veeam et du datastore Azure NetApp Files pour la reprise après incident vers la solution Azure VMware

Auteur: Niyaz Mohamed - NetApp Solutions Engineering

Présentation

Les datastores Azure NetApp Files (ANF) dissocient le stockage du calcul et libèrent la flexibilité requise pour que les entreprises puissent migrer leurs workloads vers le cloud. Elle fournit aux clients une infrastructure de stockage haute performance flexible capable d'évoluer indépendamment des ressources de calcul. Le datastore Azure NetApp Files simplifie et optimise le déploiement en parallèle d'Azure VMware solution (AVS) en tant que site de reprise d'activité pour les environnements VMware sur site.

Les datastores NFS basés sur volumes Azure NetApp Files (ANF) peuvent être utilisés pour répliquer les données depuis un environnement sur site à l'aide d'une solution tierce validée qui offre une fonctionnalité de réplication de machine virtuelle. En ajoutant des datastores Azure NetApp Files, il permettra un déploiement plus économique que la création d'un SDDC avec une solution Azure VMware avec un nombre considérable d'hôtes ESXi pour prendre en charge le stockage. Cette approche est appelée « groupe de témoins lumineux ». Un cluster pilote léger est une configuration hôte AVS minimale (3 nœuds AVS) avec la capacité de datastore Azure NetApp Files.

L'objectif est de maintenir une infrastructure à faible coût avec tous les composants de base pour gérer un basculement. Un cluster pilote peut évoluer horizontalement et provisionner davantage d'hôtes AVS en cas de basculement. Par ailleurs, une fois le basculement terminé et les opérations normales restaurées, le cluster de pilotage peut revenir en mode d'opérations à faible coût.

Objectifs du présent document

Cet article décrit l'utilisation du datastore Azure NetApp Files avec Veeam Backup et la réplication pour configurer la reprise d'activité pour les machines virtuelles VMware sur site vers (AVS) à l'aide des fonctionnalités du logiciel de réplication de VM Veeam.

Veeam Backup & Replication est une application de sauvegarde et de réplication destinée aux environnements virtuels. Lors de la réplication de machines virtuelles, Veeam Backup & Replication est répliqué à partir de sur AVS, le logiciel crée une copie exacte des machines virtuelles au format natif VMware vSphere sur le cluster SDDC AVS cible. Avec Veeam Backup & Replication, la copie reste synchronisée avec la machine virtuelle d'origine. La réplication offre le meilleur objectif de délai de restauration (RTO), car une copie montée d'une machine virtuelle sur le site de reprise est prête à démarrer.

Ce mécanisme de réplication permet de s'assurer que les workloads peuvent démarrer rapidement dans un SDDC AVS en cas d'incident. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. Il filtre également les blocs de données dupliqués, les blocs de données nuls, les fichiers swap et les « fichiers exclus du système d'exploitation invité des

machines virtuelles ». Le logiciel compresse également le trafic de réplica. Pour éviter que les tâches de réplication ne consomment la totalité de la bande passante réseau, les accélérateurs WAN et les règles de restriction réseau peuvent être utilisés.

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 sur 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. 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. "Déploiement d'une solution Azure VMware (AVS)" cloud privé et "Reliez des datastores Azure NetApp Files" Aux hôtes de la solution Azure VMware.

   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. Configurez la tâche 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.

Conditions préalables pour la réplication de VM Veeam vers les datastores AVS et ANF

1. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée à la source ainsi qu'aux clusters SDDC AVS cibles.
2. Le serveur de sauvegarde doit pouvoir résoudre les noms abrégés et se connecter aux vCenters source et cible.
3. Le datastore Azure NetApp Files cible doit disposer d'un espace libre suffisant pour stocker des VMDK de VM répliquées.

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

Détails du déploiement

Étape 1 : réplication des machines virtuelles

Veeam Backup & Replication exploite les fonctionnalités Snapshot de VMware vSphere/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 et les métadonnées. 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. Cliquez avec le bouton droit de la souris sur le nœud Jobs et sélectionnez Replication Job > Virtual machine.
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 Azure a une bande passante limitée.
     *Cochez la case Remapping réseau (pour les sites SDDC AVS avec différents réseaux) si les segments du SDDC solution Azure VMware ne correspondent pas à ceux des réseaux de sites sur site.
   - Si le schéma d'adressage IP du site de production sur site diffère du schéma du site AVS cible, cochez la case Replica re-IP (pour les sites DR avec un schéma d'adressage IP différent).

     []
4. Sélectionnez les machines virtuelles à répliquer sur le datastore Azure NetApp Files attaché à un SDDC de solution Azure VMware à l'étape **Virtual** machines*. 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 facilement placé dans les datastores Azure NetApp Files afin que les machines virtuelles puissent être restaurées, et le cluster peut être étendu pour répondre aux besoins en processeur/en Mo. 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 la solution Azure VMware 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/hôte AVS 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 **replicas** 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 d'accueil. Cliquez avec le bouton droit de la souris sur le nœud répliques et sélectionnez plans de basculement > Plan de basculement > VMware vSphere.

   []

2. Indiquez ensuite un nom et une description du 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 lors du basculement.

Pour démarrer le plan de basculement, cliquez simplement sur l'onglet **plans de basculement** et cliquez avec le bouton droit de la souris sur votre 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 des répliques de machine virtuelle passe de Ready à Failover et les machines virtuelles démarrent sur le cluster/hôte SDDC Azure VMware solution (AVS) de destination.

[]

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 Annuler le retour arrière 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

Grâce à la fonctionnalité de datastore Azure NetApp Files, Veeam ou tout outil tiers validé fournit une solution de reprise d'activité économique en exploitant les clusters Pilot light au lieu de créer un cluster volumineux uniquement pour prendre en charge les réplicas de VM. Cela constitue un moyen efficace de gérer un plan de reprise d'activité personnalisé et de réutiliser les produits de sauvegarde en interne pour la reprise d'activité,

permettant ainsi la reprise d'activité dans le cloud en fermant les data centers de reprise d'activité sur site. Il est possible de basculer en cliquant sur un bouton en cas d'incident ou de basculer automatiquement en cas d'incident.

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=2855e0d5-97e7-430f-944a-b061015e9278

Migration de workloads sur Azure/AVS

Tr-4940 : migrer des charges de travail vers un datastore Azure NetApp Files à l'aide de VMware HCX - Guide de démarrage rapide

Auteur(s) : Ingénierie de solutions NetApp

Présentation : migration de machines virtuelles avec VMware HCX, datastores Azure NetApp Files et solution Azure VMware

L'une des utilisations les plus courantes pour la solution Azure VMware et le datastore Azure NetApp Files est la migration des charges de travail VMware. VMware HCX est une option privilégiée qui fournit plusieurs mécanismes de migration pour déplacer des machines virtuelles sur site et leurs données vers les datastores Azure NetApp Files.

VMware HCX est principalement une plateforme de migration conçue pour simplifier la migration des applications, le rééquilibrage des charges de travail et même la continuité de l'activité dans les clouds. Il est inclus dans le cloud privé Azure VMware solution et offre de nombreuses façons de migrer les workloads et peut être utilisé pour les opérations de reprise d'activité.

Ce document fournit des instructions détaillées pour le provisionnement du datastore Azure NetApp Files, puis le téléchargement, le déploiement et la configuration de VMware HCX, notamment tous ses composants principaux sur site et côté solution VMware Azure, notamment l'interconnexion, l'extension réseau et l'optimisation WAN pour activer divers mécanismes de migration de VM.

VMware HCX fonctionne avec n'importe quel type de datastore lorsque la migration se trouve au niveau des VM. Ce document s'applique donc aux clients NetApp et aux clients non NetApp qui prévoient de déployer Azure NetApp Files avec Azure VMware, pour un déploiement cloud VMware rentable.

Étapes générales

Cette liste fournit les étapes générales nécessaires pour installer et configurer HCX Cloud Manager côté cloud Azure et installer HCX Connector sur site :

1. Installez HCX via le portail Azure.
2. Téléchargez et déployez le programme d'installation HCX Connector Open Virtualization Appliance (OVA) dans VMware vCenter Server sur site.
3. Activez HCX à l'aide de la clé de licence.
4. Couplez le connecteur VMware HCX sur site avec Azure VMware solution HCX Cloud Manager.
5. Configurez le profil réseau, le profil de calcul et le maillage de service.
6. (Facultatif) effectuez l'extension réseau pour éviter toute nouvelle IP pendant les migrations.
7. Validez l'état du système et assurez-vous que la migration est possible.
8. Migrer les workloads de VM.

Prérequis

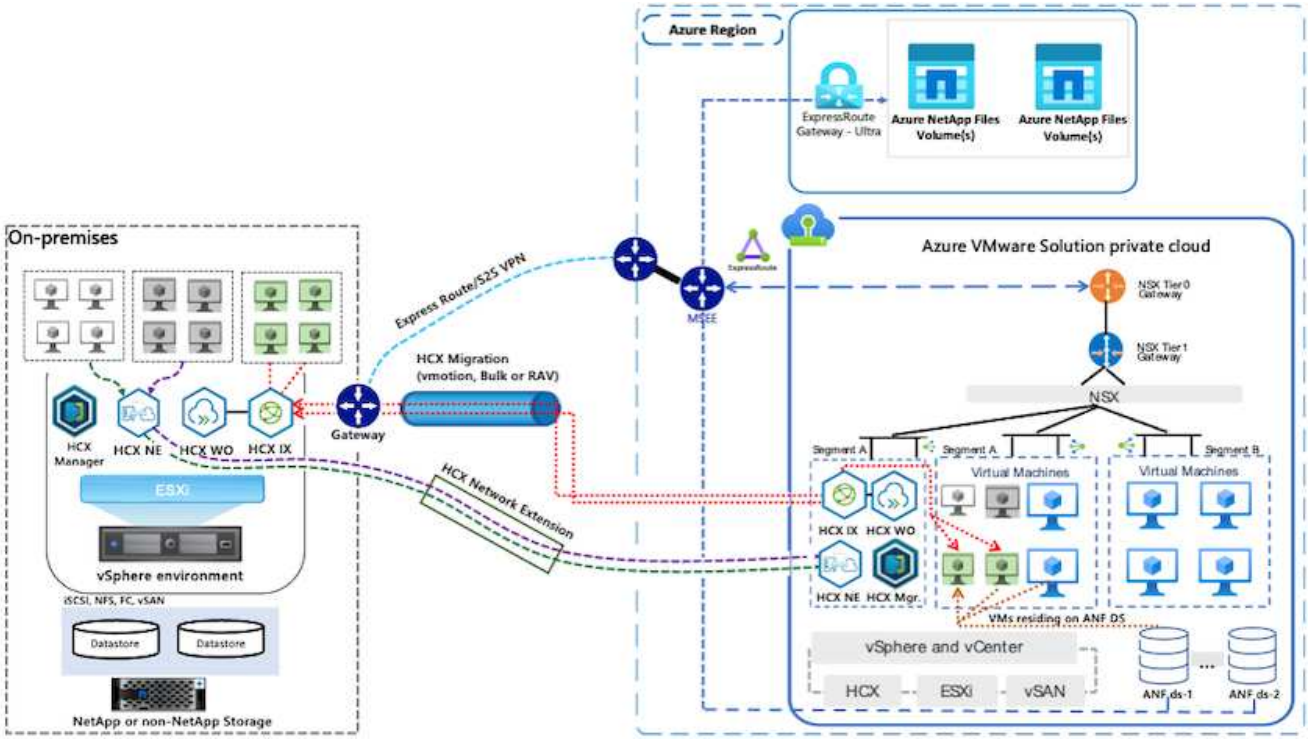
Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, reportez-vous à ce document "lien". Une fois les prérequis, y compris la connectivité, mis en place, configurez et activez HCX en générant la clé de licence à partir du portail de solutions Azure VMware. Une fois le programme d'installation OVA téléchargé, procédez au processus d'installation comme décrit ci-dessous.

> HCX Advanced est l'option par défaut et VMware HCX Enterprise Edition est également disponible via un ticket d'assistance et pris en charge sans frais supplémentaires.

- Utilisez un SDDC (Software-Defined Data Center) ou créez un cloud privé avec la solution Azure VMware "Lien NetApp" ou ceci "Lien Microsoft".
- La migration des VM et des données associées depuis le data Center sur site compatible VMware vSphere nécessite une connectivité réseau du data Center vers l'environnement SDDC. Avant de migrer des workloads, "Configurez une connexion VPN site à site ou une connexion à portée globale express" entre l'environnement sur site et le cloud privé respectif.
- Le chemin du réseau depuis l'environnement VMware vCenter Server sur site vers le cloud privé Azure VMware solution doit prendre en charge la migration des machines virtuelles à l'aide de vMotion.
- 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. Dans le cloud privé, le routage sur le réseau vMotion est configuré par défaut.
- Le volume NFS Azure NetApp Files doit être monté en tant que datastore dans Azure VMware solution. Suivez les étapes décrites dans ce document "lien" Connexion de datastores Azure NetApp Files aux hôtes Azure VMware Solutions

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, permettant une connectivité sur site à la solution Azure VMware.



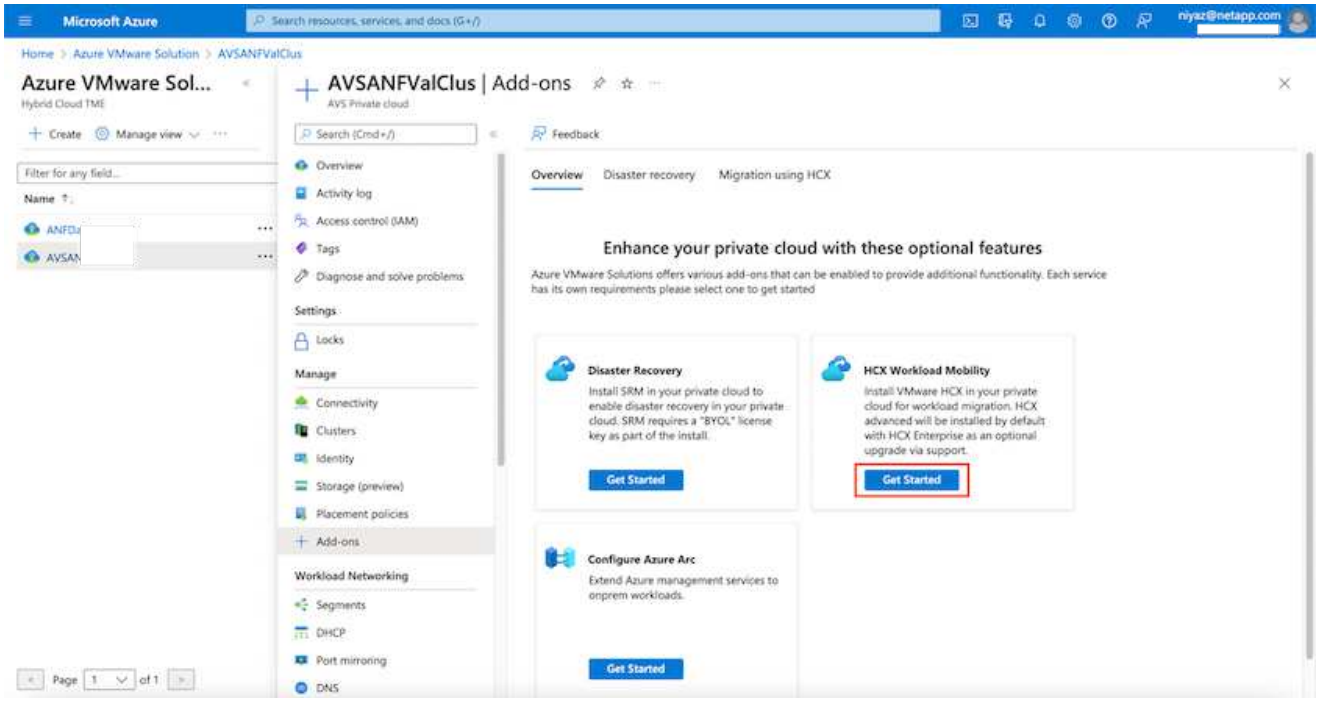
Déploiement de la solution

Suivez les étapes du déploiement de cette solution :

Étape 1 : installez HCX via Azure Portal à l'aide de l'option Add-ons

Pour effectuer l'installation, procédez comme suit :

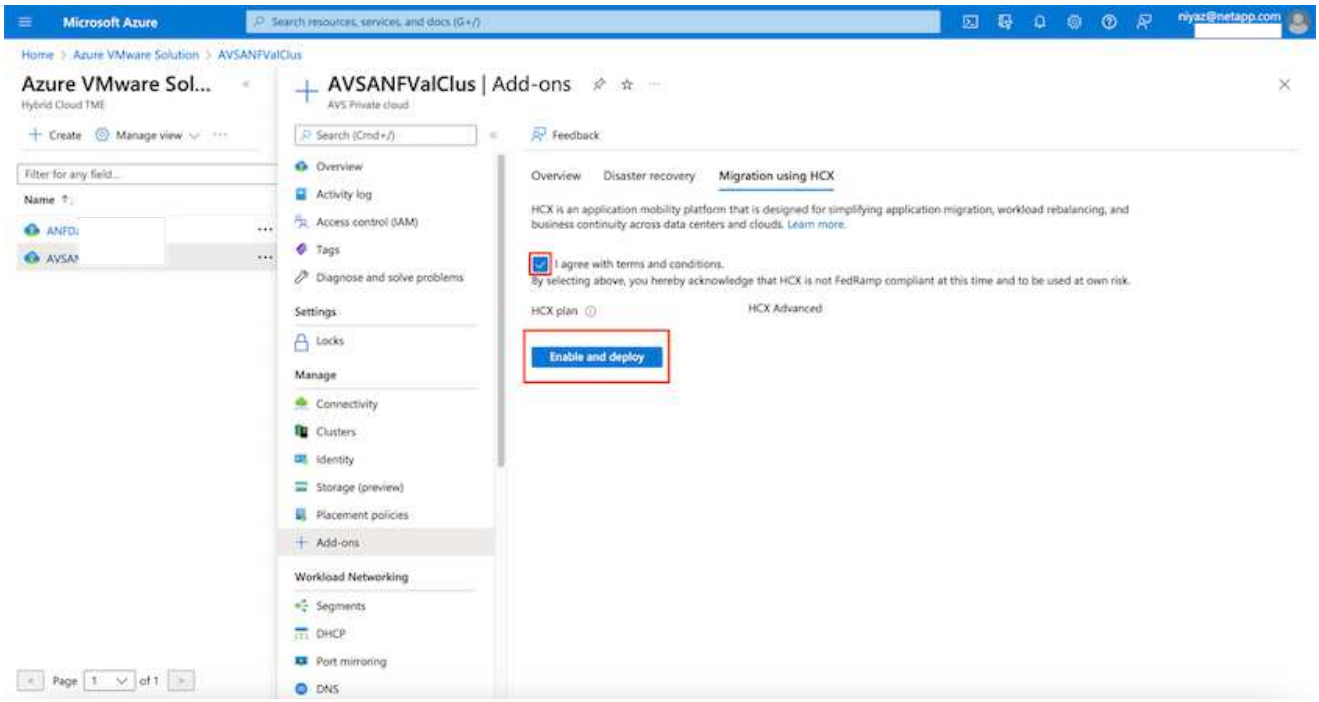
1. Connectez-vous au portail Azure et accédez au cloud privé Azure VMware solution.
2. Sélectionnez le cloud privé approprié et accédez à des modules complémentaires. Pour ce faire, accédez à **Manage > Add-ons**.
3. Dans la section mobilité de la charge de travail HCX, cliquez sur **Get Started**.



1. Sélectionnez l'option **J'accepte les termes et conditions** et cliquez sur **Activer et déployer**.

> Le déploiement par défaut est HCX Advanced. Ouvrez une demande d'assistance pour activer l'édition Enterprise.

> Le déploiement prend environ 25 à 30 minutes.


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDu
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

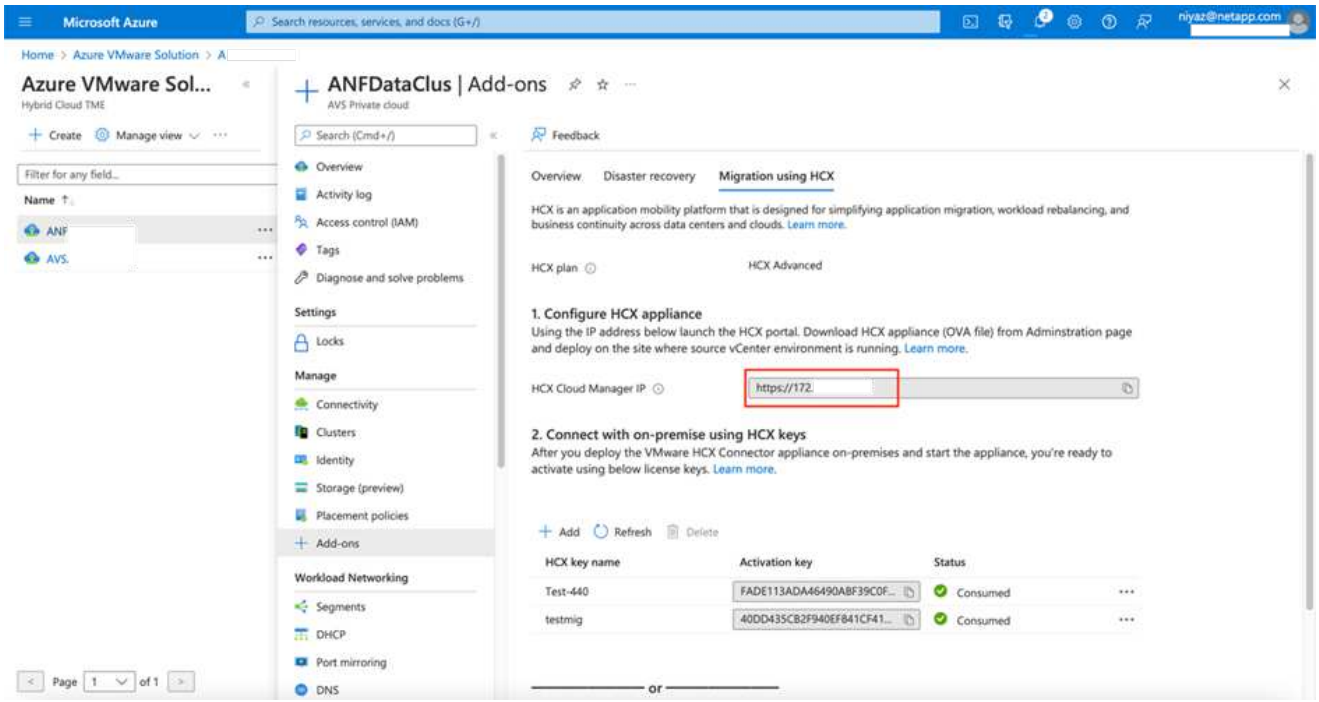
Étape 2 : déployer le fichier OVA du programme d'installation dans le serveur vCenter sur site

Pour que le connecteur sur site puisse se connecter à HCX Manager dans Azure VMware solution, assurez-vous que les ports pare-feu appropriés sont ouverts dans l'environnement sur site.

Pour télécharger et installer HCX Connector dans le serveur vCenter sur site, procédez comme suit :

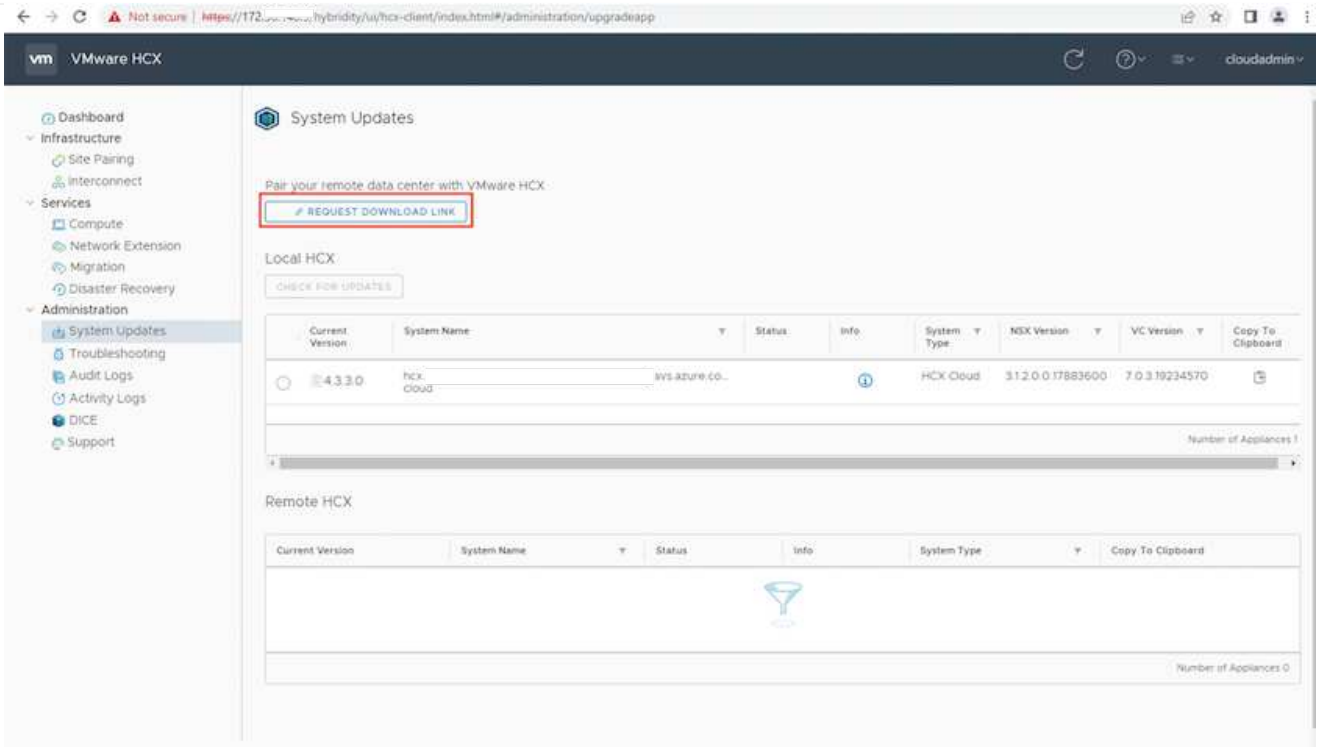
1. Depuis le portail Azure, accédez à la solution VMware Azure, sélectionnez le cloud privé, puis sélectionnez **Manage > Add-ons > migration** à l'aide de HCX et copiez le portail HCX Cloud Manager pour télécharger le fichier OVA.

Utilisez les informations d'identification par défaut de l'utilisateur CloudAdmin pour accéder au portail HCX.

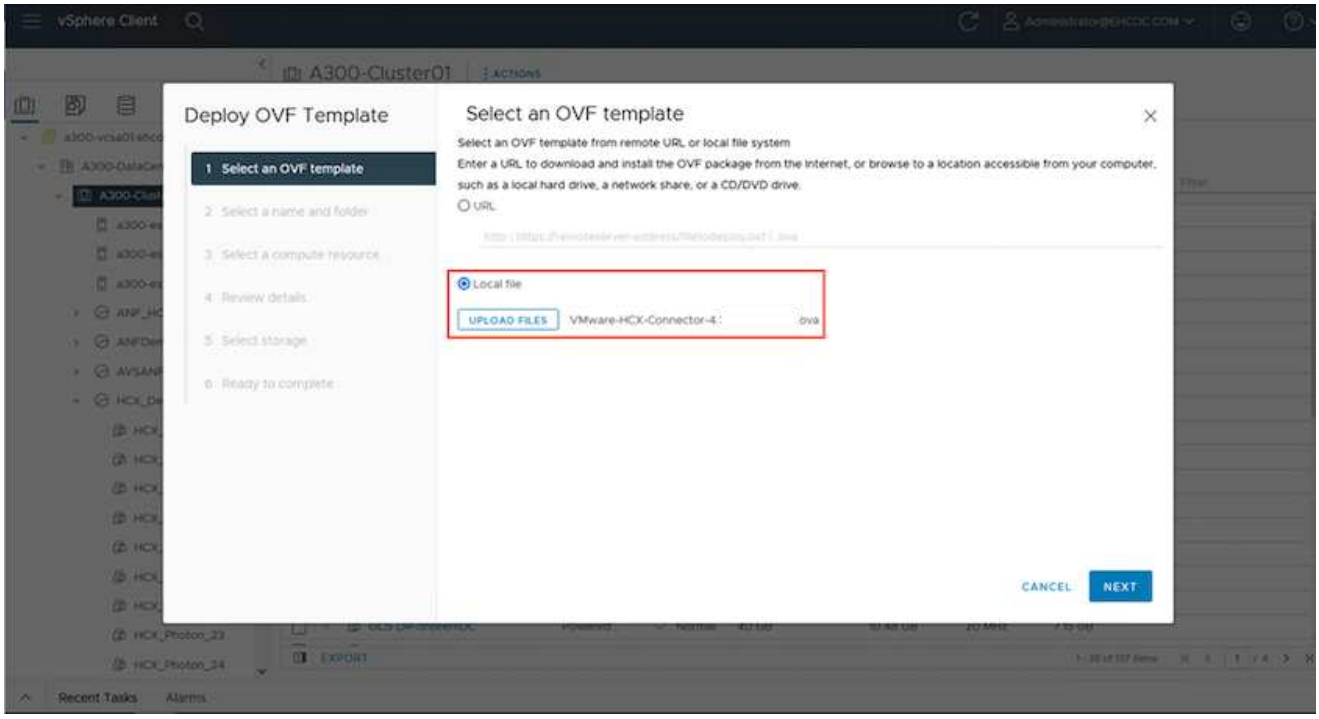


1. Une fois que vous avez accédé au portail HCX avec cloudadmin@vsphere.lockubl à l'aide de la commande jumpost, accédez à **Administration > mises à jour du système** et cliquez sur **demander un lien de téléchargement**.

Téléchargez ou copiez le lien vers le fichier OVA et collez-le dans un navigateur pour lancer le processus de téléchargement du fichier OVA VMware HCX Connector à déployer sur le serveur vCenter sur site.



1. Une fois le fichier OVA téléchargé, déployez-le dans l'environnement VMware vSphere sur site à l'aide de l'option **Deploy OVF Template**.



1. Entrez toutes les informations requises pour le déploiement OVA, cliquez sur **Next**, puis sur **Finish** pour déployer le connecteur OVA VMware HCX.

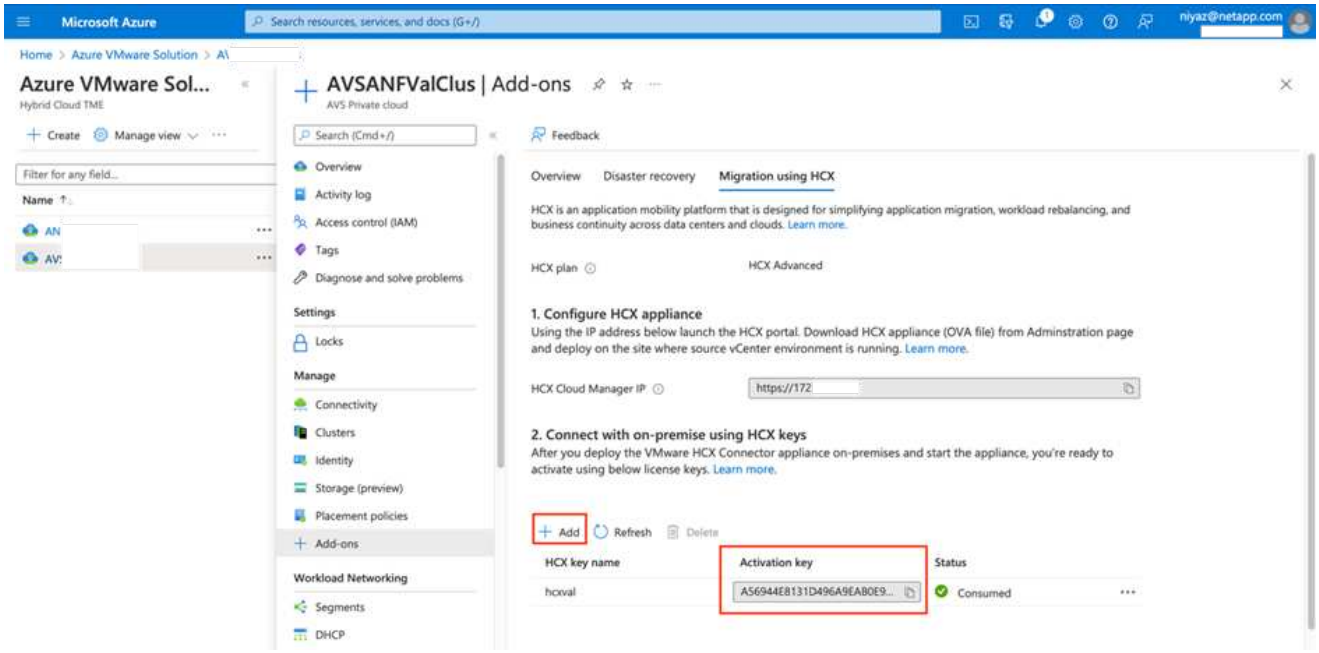
Mettez l'appliance virtuelle sous tension manuellement.

Pour des instructions détaillées, reportez-vous à la "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 du portail Azure VMware solution et activez-la dans VMware HCX Manager.

1. Depuis le portail Azure, accédez à la solution VMware Azure, sélectionnez le cloud privé et sélectionnez **gérer > modules complémentaires > migration à l'aide de HCX**.
2. Sous **connexion avec sur site à l'aide des clés HCX**, cliquez **Ajouter** et copiez la clé d'activation.



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

1. Connectez-vous au gestionnaire VMware HCX sur site à l'adresse "https://hcxmanagerIP:9443" utilisation des informations d'identification administrateur.

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

1. Dans la licence, entrez la clé copiée à partir de l'étape 3 et cliquez sur **Activer**.

> Le connecteur HCX sur site doit disposer d'un accès Internet.

1. Sous **Datacenter Location**, indiquez l'emplacement le plus proche pour l'installation sur site de VMware HCX Manager. Cliquez sur **Continuer**.
2. Sous **Nom du système**, mettez à jour le nom et cliquez sur **Continuer**.
3. Cliquez sur **Oui, Continuer**.
4. Sous **Connect Your vCenter**, indiquez le nom de domaine complet (FQDN) ou l'adresse IP de vCenter Server et les informations d'identification appropriées, puis cliquez sur **Continuer**.

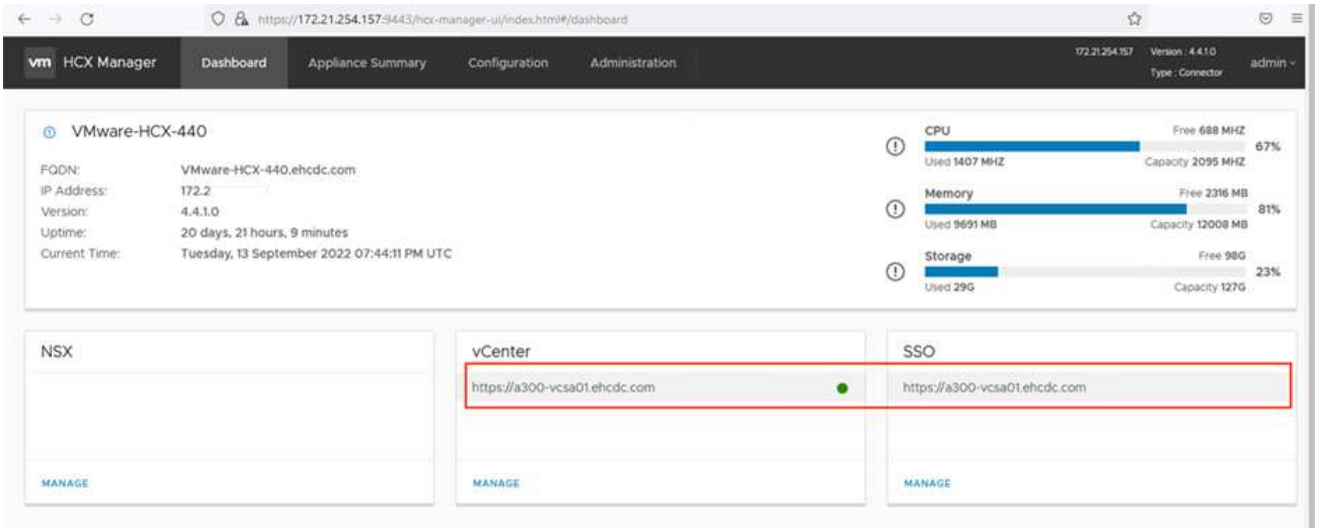
> Utilisez le FQDN pour éviter les problèmes de connectivité ultérieurement.

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

Entrez le FQDN ou l'adresse IP de VMware vCenter Server.

1. Vérifiez que les informations saisies sont correctes et cliquez sur **redémarrer**.
2. Après le redémarrage des services, vCenter Server s'affiche en vert sur la page qui s'affiche. VCenter Server et SSO doivent avoir les paramètres de configuration appropriés, qui doivent être identiques à la page précédente.

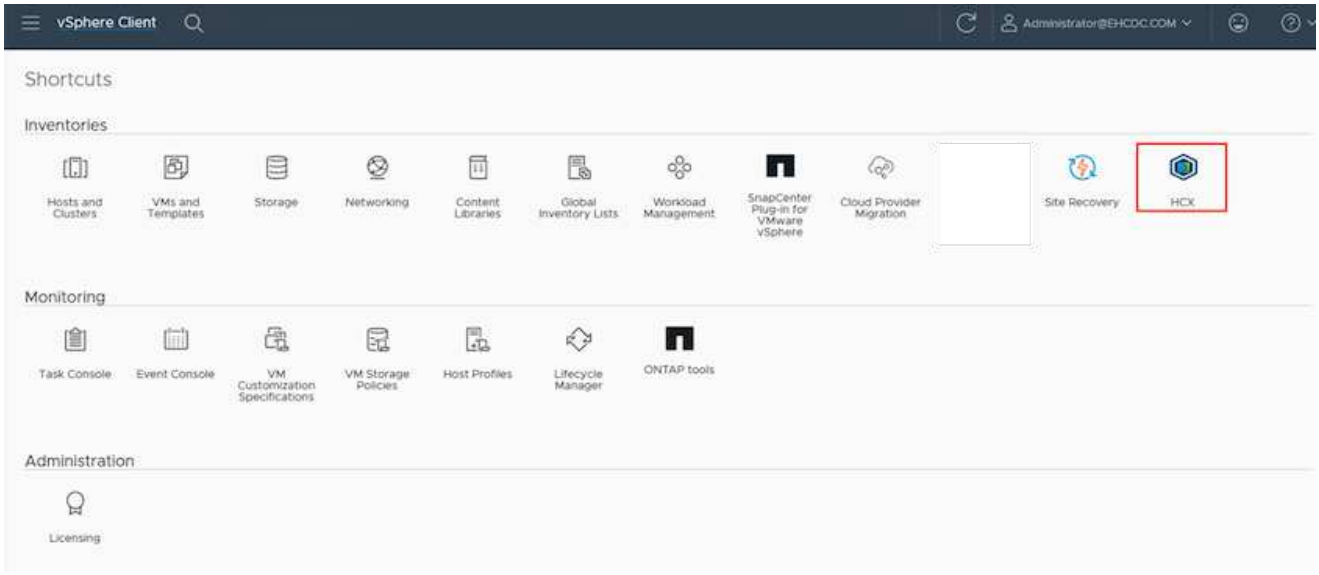
Ce processus dure environ 10 à 20 minutes et le plug-in doit être ajouté à vCenter Server.



Étape 4 : connecteur VMware HCX sur site avec Azure VMware solution HCX Cloud Manager

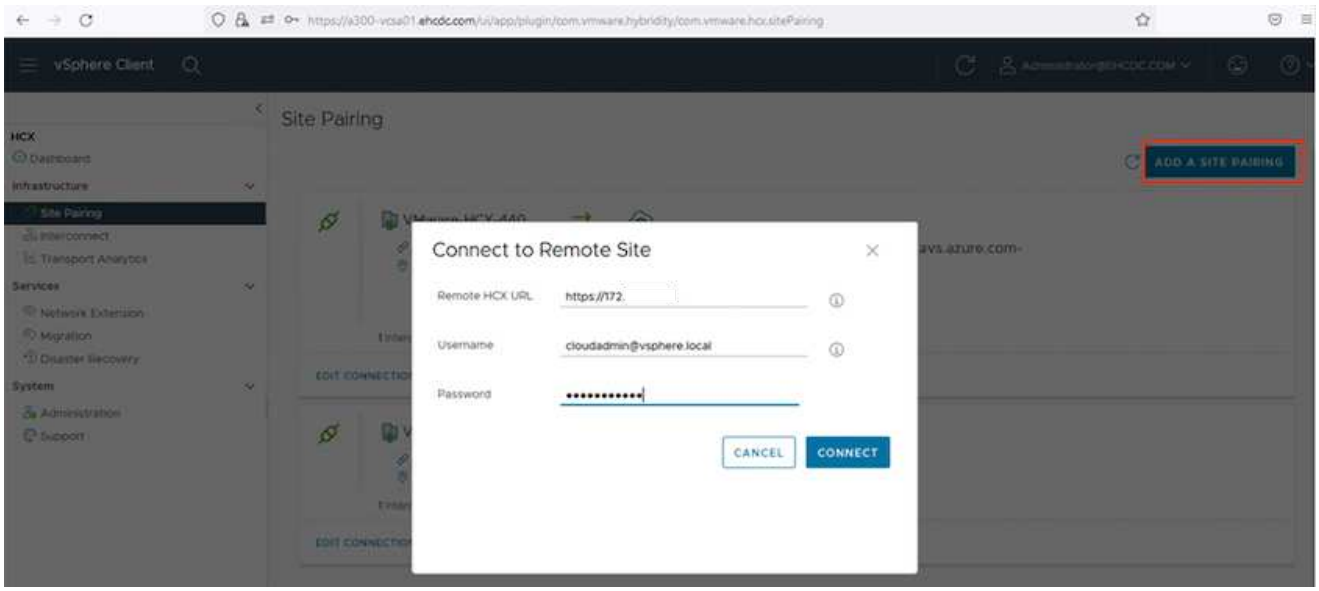
Une fois que HCX Connector est installé à la fois sur site et dans Azure VMware solution, configurez le connecteur VMware HCX sur site pour le cloud privé Azure VMware solution en ajoutant le couplage. Pour configurer le couplage du site, procédez comme suit :

1. Pour créer une paire de sites entre l'environnement vCenter sur site et Azure VMware solution SDDC, connectez-vous au serveur vCenter sur site et accédez au nouveau plug-in client Web HCX vSphere.



1. Sous Infrastructure, cliquez sur **Ajouter un couplage de site**.

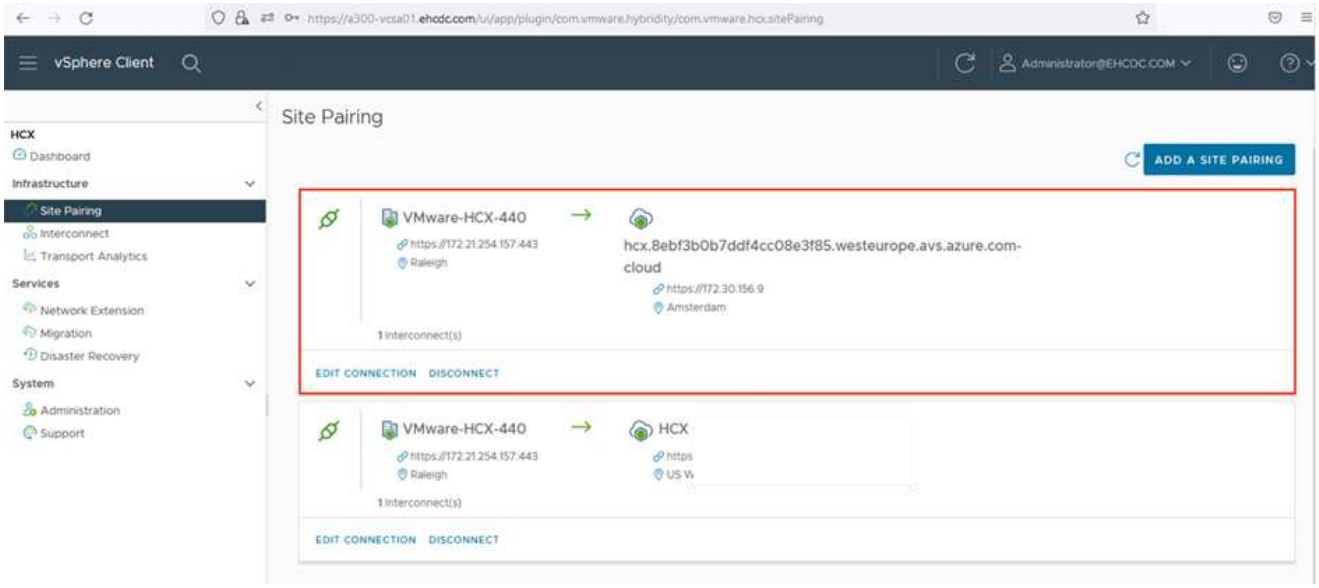
Entrez l'URL ou l'adresse IP d'Azure VMware solution HCX Cloud Manager et les identifiants du rôle CloudAdmin pour accéder au cloud privé.



1. Cliquez sur **connexion**.

Le connecteur VMware HCX doit pouvoir acheminer vers l'IP HCX Cloud Manager via le port 443.

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

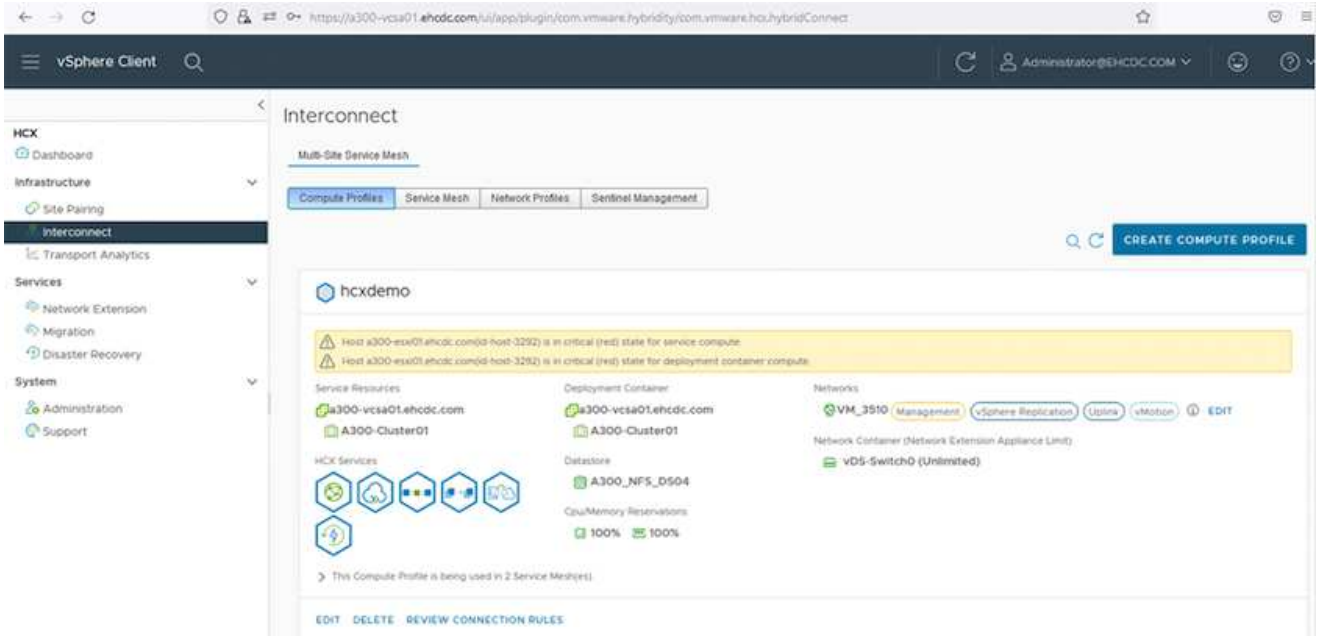


Étape 5 : configurer le profil réseau, le profil de calcul et le maillage de service

Le dispositif d'interconnexion VMware HCX offre des fonctionnalités de réplication et de migration basée sur vMotion via Internet et des connexions privées vers le site cible. L'interconnexion offre le cryptage, l'ingénierie du trafic et la mobilité des machines virtuelles. Pour créer une appliance de service d'interconnexion, procédez comme suit :

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

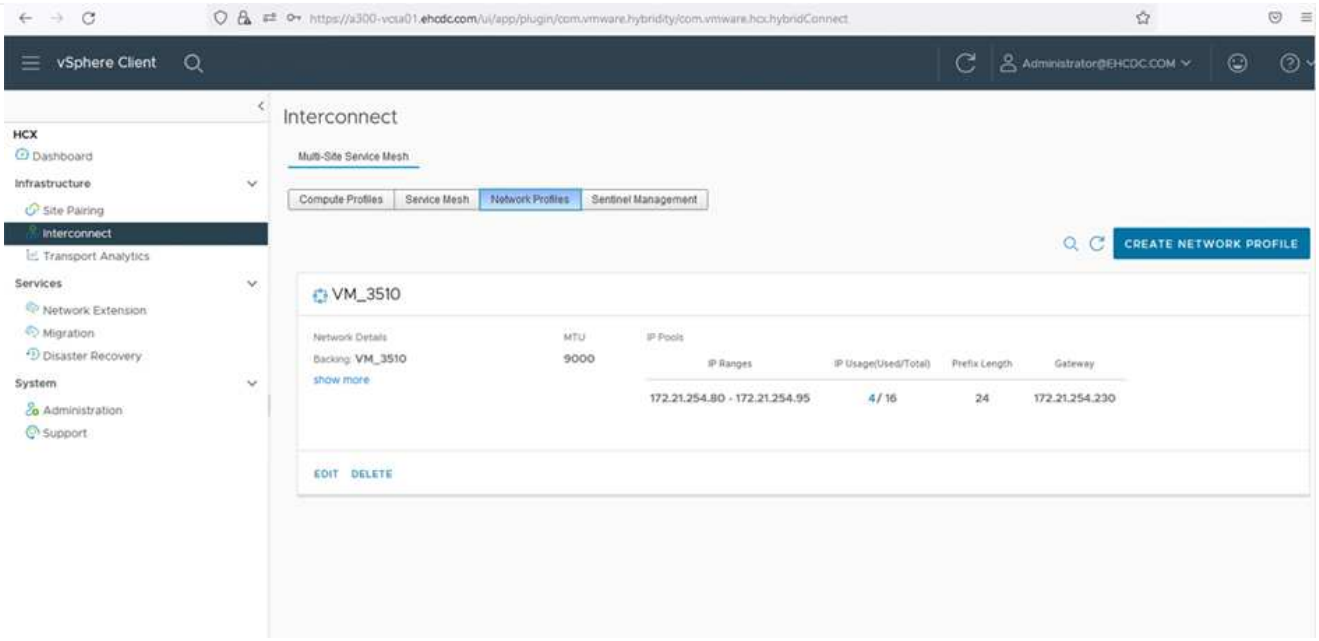
Les profils de calcul définissent les paramètres de déploiement, y compris les appliances déployées et la partie du data Center VMware accessible au service HCX.



1. Une fois le profil de calcul créé, créez les profils réseau en sélectionnant **maillage de service multisite > profils réseau > Créer profil réseau**.

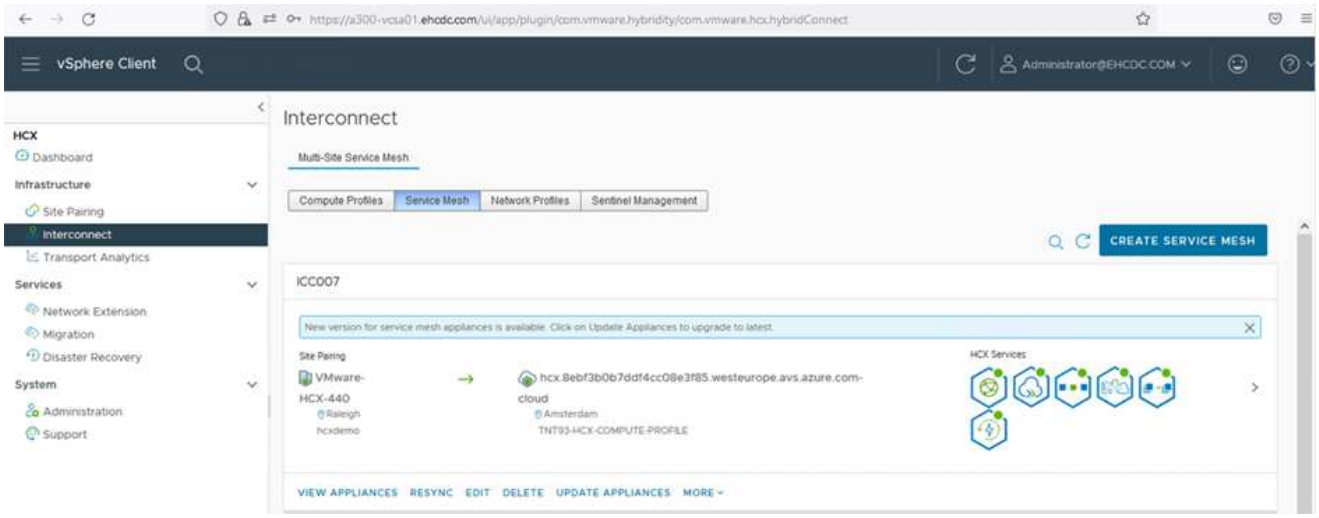
Le profil réseau définit une plage d'adresses IP et de réseaux utilisés par HCX pour ses appliances virtuelles.

Cette étape nécessite au moins deux adresses IP. Ces adresses IP sont attribuées depuis le réseau de gestion aux dispositifs d'interconnexion.

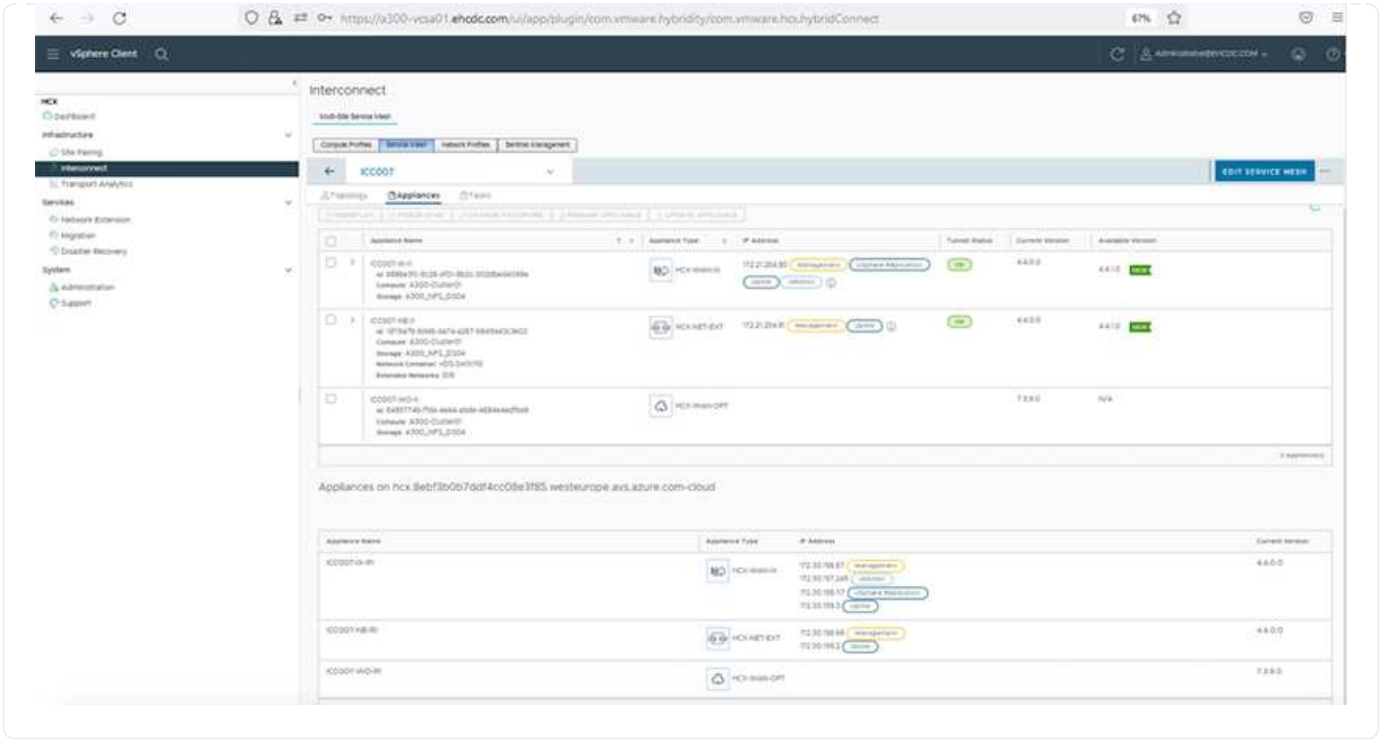


1. A ce stade, les profils de calcul et de réseau ont été créés avec succès.
2. Créez le maillage de service en sélectionnant l'onglet **maillage de service** dans l'option **Interconnexion** et sélectionnez les sites SDDC sur site et Azure.
3. Le maillage de service spécifie une paire de profils réseau et de calcul locale et distante.

Dans le cadre de ce processus, les appliances HCX sont déployées et configurées automatiquement sur les sites source et cible afin de créer une structure de transport sécurisée.



1. Il s'agit de la dernière étape de la configuration. Le déploiement devrait s'effectuer en 30 minutes environ. Une fois le maillage de service configuré, l'environnement est prêt avec les tunnels IPsec créés pour migrer les VM de charge de travail.


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

Étape 6 : migrer les workloads

Les charges de travail peuvent être migrées dans un sens bidirectionnel entre les SDDC sur site et Azure à l'aide de différentes technologies de migration VMware HCX. Les machines virtuelles peuvent être déplacées vers et depuis des entités activées par VMware HCX à l'aide de plusieurs 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 l'édition Enterprise de HCX) et la migration assistée par système d'exploitation HCX (disponible avec l'édition Enterprise de HCX).

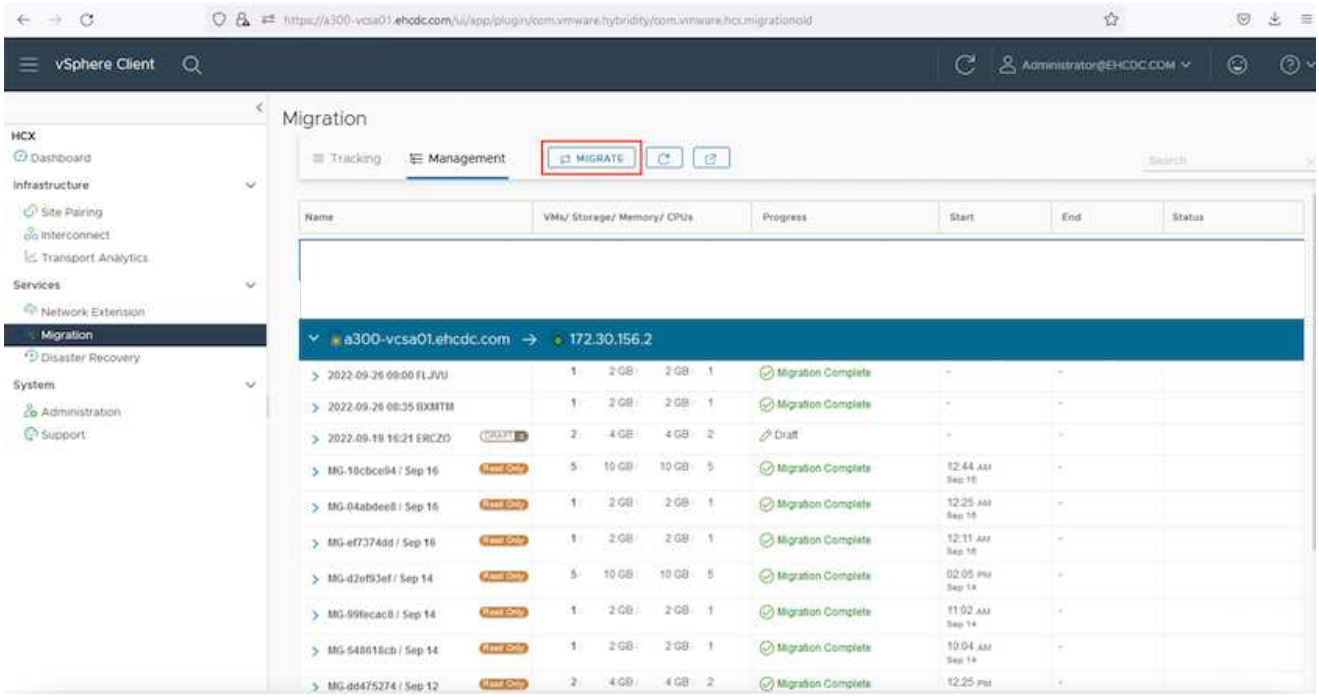
Pour en savoir plus sur les différents mécanismes de migration HCX, voir "Types de migration VMware HCX".

Migration groupée

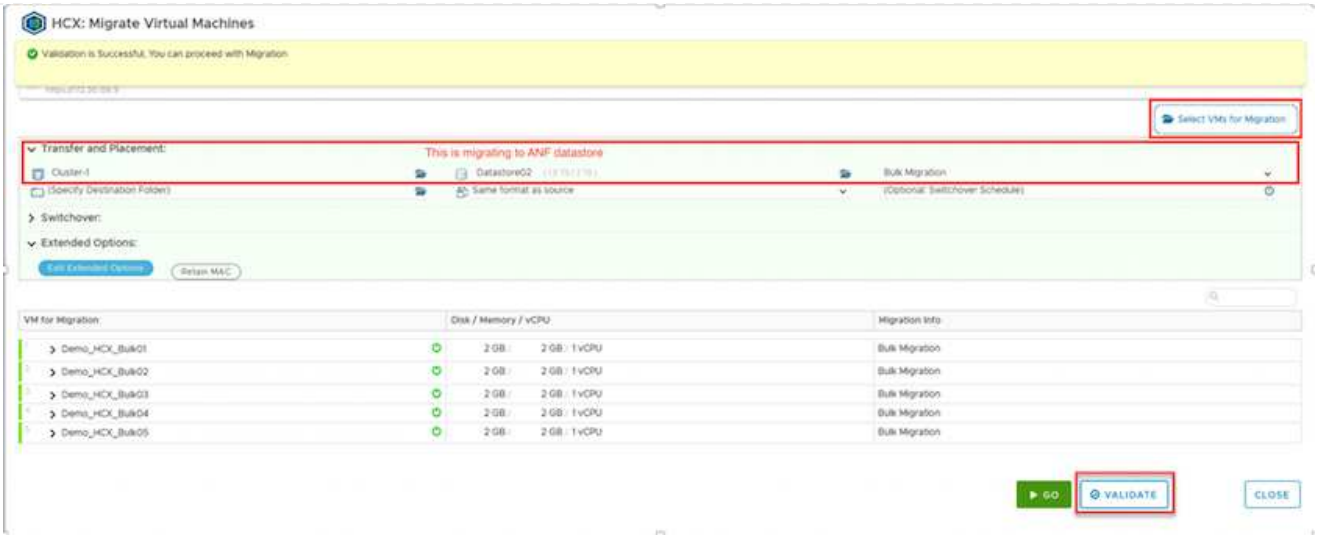
Cette section détaille le mécanisme de migration en bloc. Lors d'une migration en bloc, la fonctionnalité de migration en bloc de HCX utilise la réplication vSphere pour migrer des fichiers de disque tout en recréant la machine virtuelle sur l'instance vSphere HCX de destination.

Pour démarrer une migration de serveurs virtuels en bloc, procédez comme suit :

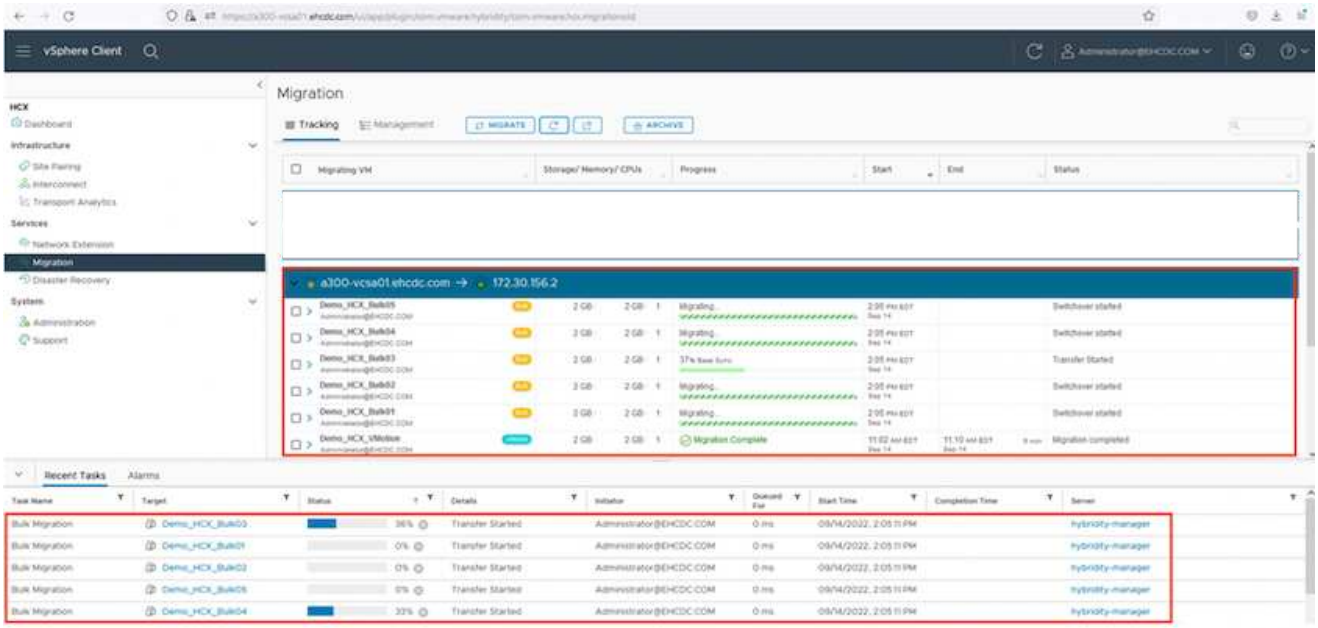
1. Accédez à l'onglet **migration** sous **Services > migration**.



1. Sous **Remote site Connection**, sélectionnez la connexion du site distant et sélectionnez la source et la destination. Dans cet exemple, le terminal Microsoft Azure VMware solution SDDC HCX est la destination.
2. Cliquez sur **Sélectionner les VM pour migration**. Fournit une liste de toutes les machines virtuelles sur site. Sélectionnez les machines virtuelles en fonction de l'expression correspondance:valeur et cliquez sur **Ajouter**.
3. Dans la section **transfert et placement**, mettez à jour les champs obligatoires (**Cluster**, **Storage**, **destination** et **Network**), y compris le profil de migration, puis cliquez sur **Validate**.

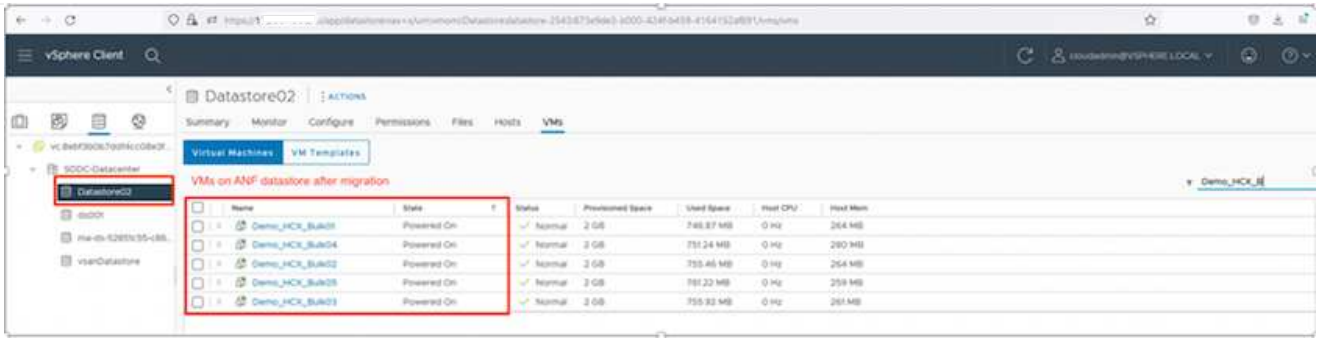


1. Une fois les vérifications de validation terminées, cliquez sur **Go** pour lancer la migration.



Au cours de cette migration, un disque réservé est créé dans le datastore Azure NetApp Files spécifié dans le vCenter cible afin de permettre la réplication des données du disque de la machine virtuelle source vers les disques de l'espace réservé. Le mode HBR est déclenché pour une synchronisation complète vers la cible. Une fois la ligne de base terminée, une synchronisation incrémentielle est effectuée en fonction du cycle de l'objectif de point de récupération (RPO). Une fois la synchronisation complète/incrémentielle terminée, le basculement est déclenché automatiquement, sauf si un planning spécifique est défini.

1. Une fois la migration terminée, validez la même opération en accédant au SDDC vCenter de destination.

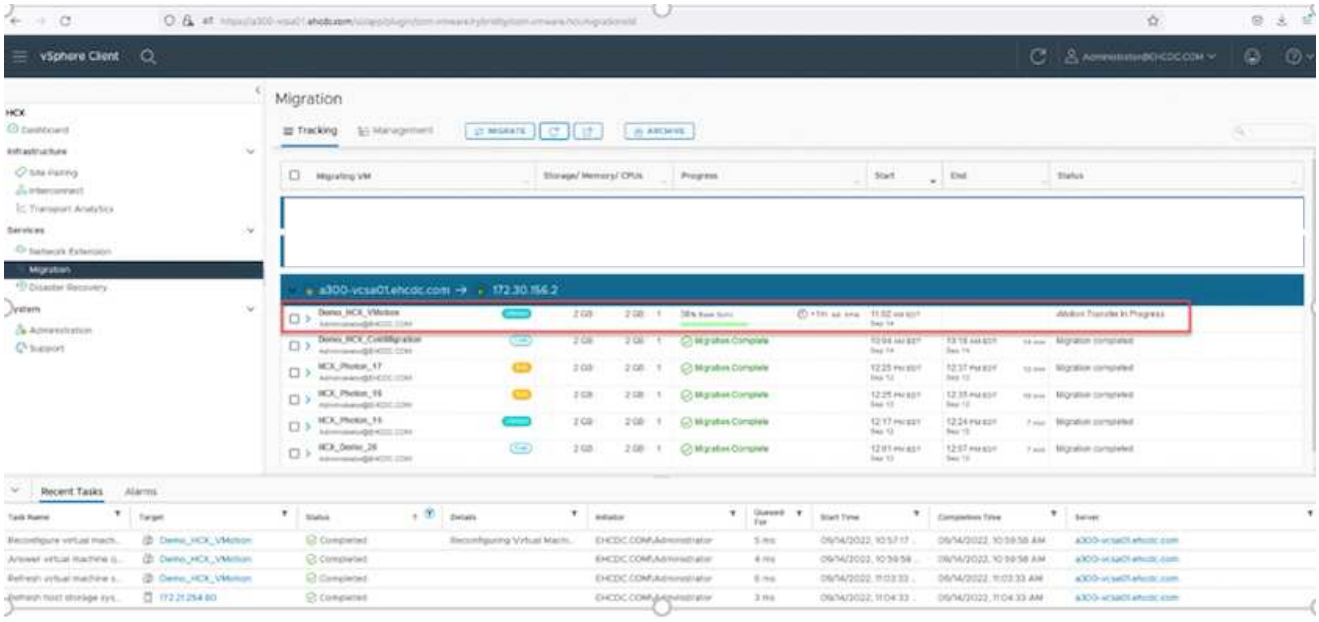


Pour plus d'informations sur les différentes options de migration et sur la façon de migrer des workloads du site vers la solution VMware Azure via HCX, consultez "Guide de l'utilisateur VMware HCX".

Pour en savoir plus sur ce processus, n'hésitez pas à regarder la vidéo suivante :

Migration des workloads à l'aide de HCX

Voici une capture d'écran de l'option HCX vMotion.



Pour en savoir plus sur ce processus, n'hésitez pas à regarder la vidéo suivante :

HCX vMotion

Assurez-vous que suffisamment de bande passante est disponible pour gérer la migration.

L'espace du datastore ANF cible doit être suffisant pour gérer la migration.

Conclusion

Que vous ciblez les clouds ou les clouds hybrides et les données qui résident sur un système de stockage de tout type ou fournisseur sur site, Azure NetApp Files et HCX offrent d'excellentes options pour déployer et migrer les charges de travail applicatives tout en réduisant le coût total de possession en rendant les données

requises de manière transparente dans la couche applicative. Quelle que soit l'utilisation, optez pour Azure VMware solution et Azure NetApp Files afin de bénéficier rapidement des avantages du cloud, d'une infrastructure cohérente et des opérations sur site et dans plusieurs clouds, de la portabilité bidirectionnelle des charges de travail, et de la capacité et des performances élevées. Il s'agit du même processus et procédures que celui utilisé pour connecter le stockage et migrer les machines virtuelles à l'aide de VMware vSphere Replication, VMware vMotion ou même de la copie de fichiers réseau (NFC).

Messages clés

Les points clés de ce document sont les suivants :

- Vous pouvez désormais utiliser Azure NetApp Files comme datastore dans Azure VMware solution SDDC.
- Vous pouvez migrer facilement les données depuis un environnement sur site vers un datastore Azure NetApp Files.
- Vous pouvez aisément étendre et réduire le datastore Azure NetApp Files afin 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 sur la solution Azure VMware

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Documentation Azure NetApp Files

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

- 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 ANF

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

- Vérifier la disponibilité de AVS et ANF "ici".
- Vérifier la disponibilité du datastore NFS supplémentaire ANF "ici".

Fonctionnalités NetApp pour Google Cloud Platform GCVE

Découvrez les fonctionnalités qu'NetApp apporte à Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) : de NetApp en tant que périphérique de stockage connecté par l'invité ou datastore NFS supplémentaire en tant que migration des workflows, extension/bursting dans le cloud, sauvegarde/restauration et reprise après incident.

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

- "Configuration de GCVE dans GCP"
- "Options de stockage NetApp pour GCVE"
- "Solutions clouds NetApp/VMware"

Configuration de GCVE dans GCP

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 GCVE et l'utiliser en association avec les options disponibles pour la connexion du stockage NetApp.

> Le stockage « en invité » est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP et Cloud volumes Services à GCVE.

Le processus de configuration peut être divisé en plusieurs étapes :

- Déployer et configurer GCVE
- Activez l'accès privé à GCVE

Afficher les détails "Étapes de configuration pour GCVE".

Options de stockage NetApp pour GCVE

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

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

Google Cloud prend en charge le stockage NetApp dans les configurations suivantes :

- Cloud Volumes ONTAP (CVO) comme stockage connecté à l'invité
- Cloud Volumes Service (CVS) comme stockage connecté invité
- Cloud Volumes Service (CVS) comme datastore NFS supplémentaire

Afficher les détails "Options de stockage de connexion invité pour GCVE".

En savoir plus sur "Prise en charge du datastore NetApp Cloud Volumes Service pour Google Cloud VMware Engine (blog NetApp)" ou "Comment utiliser NetApp CVS en tant que datastores pour Google Cloud VMware Engine (blog Google)"

Cas d'utilisation de la solution

Avec les solutions cloud de NetApp et VMware, le déploiement dans Azure AVS est très simple. Des cas se sont définis pour chaque domaine cloud défini par VMware :

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

"Découvrez les solutions NetApp pour Google Cloud GCVE"

Protection des charges de travail sur GCP/GCVE

Reprise d'activité cohérente avec les applications avec NetApp SnapCenter et Veeam Replication

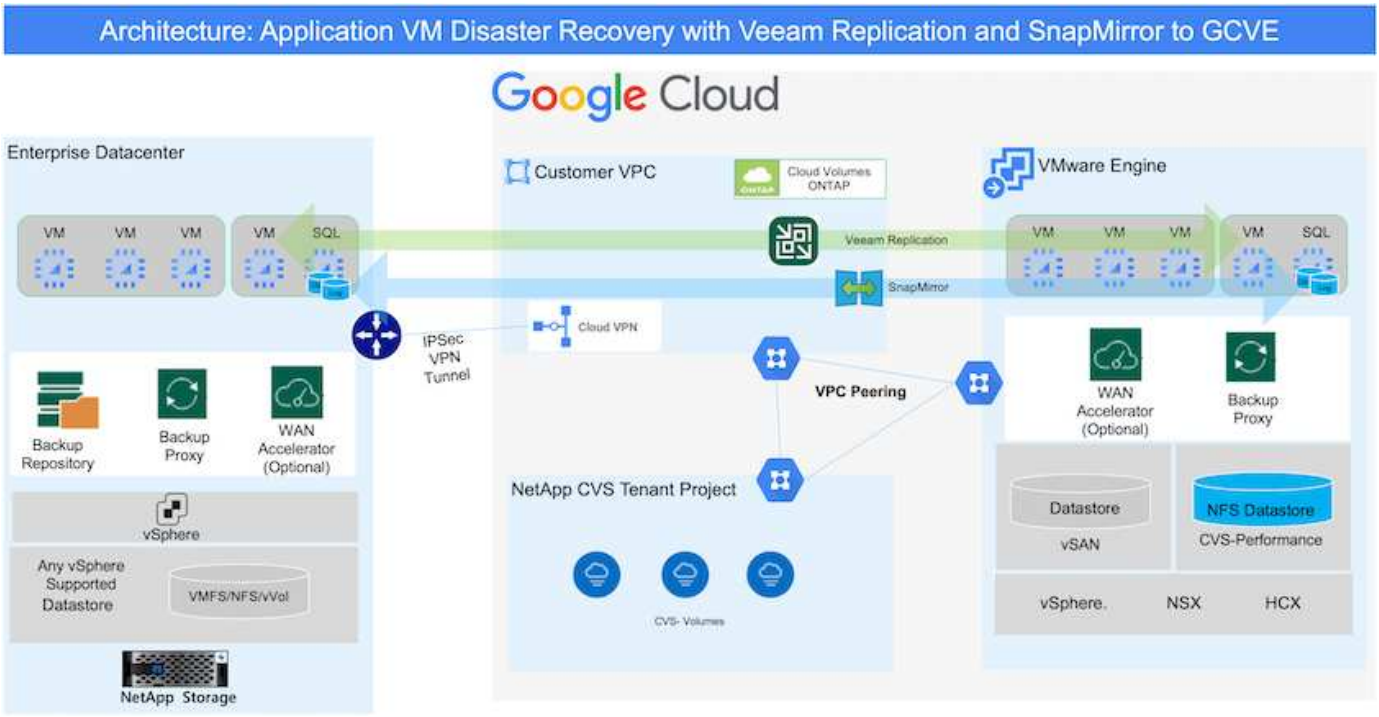
Auteurs : Suresh Thoppay, NetApp

Présentation

De nombreux clients recherchent une solution de reprise après incident efficace pour leurs machines virtuelles d'application hébergées sur VMware vSphere. La plupart d'entre eux utilisent leur solution de sauvegarde existante pour effectuer une restauration pendant les diaster.
La plupart du temps, cette solution augmente le RTO et ne répond pas à leurs attentes. Pour réduire les objectifs RPO et RTO, la réplication de machine virtuelle Veeam peut être utilisée même sur site vers GCVE dans la mesure où la connectivité réseau et l'environnement ne disposent pas des autorisations appropriées.
REMARQUE : Veeam VM Replication ne protège pas les dispositifs de stockage connectés invités d'une machine virtuelle, tels que les montages iSCSI ou NFS au sein de la machine virtuelle invitée. Ils doivent les protéger séparément.

Pour assurer une réplication cohérente avec les applications pour SQL VM et réduire l'objectif de durée de restauration, nous avons utilisé SnapCenter pour orchestrer les opérations snapmirror des volumes de bases de données et de journaux SQL.

Ce document propose une approche détaillée de la configuration et de l'exécution d'une reprise d'activité à l'aide de NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document est axé sur le stockage invité pour les données d'applications (également appelé « invité connecté »), et nous supposons que l'environnement sur site utilise SnapCenter pour assurer des sauvegardes cohérentes au niveau des applications.

Ce document s'applique à toute solution de sauvegarde et de restauration tierce. En fonction de la solution utilisée dans l'environnement, suivez les bonnes pratiques pour créer des stratégies de sauvegarde conformes aux SLA de l'entreprise.

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que une interconnexion dédiée ou un VPN cloud. Les segments doivent être créés en fonction de la conception VLAN sur site.

Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document. Consultez la documentation Google Cloud pour connaître la méthode de connectivité appropriée, du site vers Google.

Déploiement de la solution de reprise d'activité

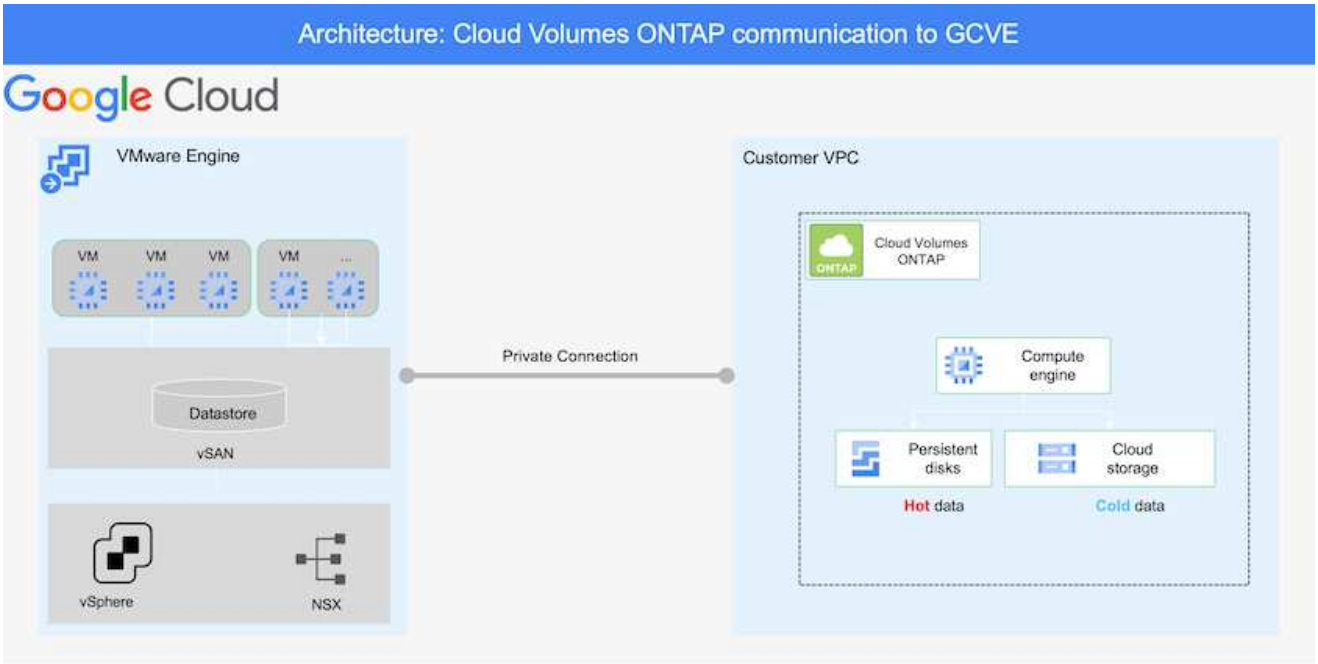
Présentation du déploiement de la solution

1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de BlueXP avec l'abonnement et le réseau virtuel appropriés.
   a. Configurer SnapMirror pour les volumes applicatifs concernés.
   b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer des machines virtuelles sur l'instance Google Cloud VMware Engine.
4. En cas d'incident, rompez la relation SnapMirror avec BlueXP et déclenchez le basculement des serveurs virtuels avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
   b. Permet de mettre les applications en ligne.
5. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Google Cloud et répliquez les volumes dans CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Google Cloud ("cvo") Et répliquez les volumes souhaités dans Cloud Volumes ONTAP avec les fréquences et les instantanés souhaités.



Pour obtenir des exemples d'instructions détaillées sur la configuration de SnapCenter et la réplication des données, reportez-vous à la section "Configurez la réplication avec SnapCenter"

Révision de la protection de SQL VM avec SnapCenter

Configurez l'accès aux données des hôtes GCVE et CVO

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution GCVE et le temps de maintenance du SDDC. Ces deux considérations clés à prendre en compte dans une solution de reprise sur incident permettent de réduire les coûts d'exploitation globaux. Le SDDC peut héberger jusqu'à trois hôtes, tout comme un cluster multi-hôtes dans un déploiement à grande échelle.

Le datastore NetApp Cloud Volume Service pour NFS et le journal et les bases de données Cloud Volumes ONTAP pour SQL peuvent être déployés sur n'importe quel VPC et GCVE doivent disposer d'une connexion privée à ce VPC pour monter le datastore NFS et se connecter aux LUN iSCSI par un VM.

Pour configurer GCVE SDDC, voir "Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)". Avant cela, vérifiez que les VM invités résidant sur les hôtes GCVE peuvent consommer des données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et GCVE ont été correctement configurés, commencez à configurer Veeam pour automatiser la restauration des workloads sur site vers GCVE (machines virtuelles avec VMDK d'application et VM avec stockage « Guest ») en utilisant la fonctionnalité de réplication Veeam et en utilisant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

Installer les composants Veeam

Selon le scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde à déployer. Pour ce cas d'utilisation, nul besoin de déployer un magasin d'objets pour Veeam et le référentiel scale-out non plus requis.
"Se référer à la documentation Veeam pour la procédure d'installation"
Pour plus d'informations, reportez-vous à la section "Migration avec Veeam Replication"

Configuration de la réplication de machine virtuelle avec Veeam

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere" À l'étape traitement invité de l'assistant, sélectionnez Désactiver le traitement de l'application, car nous utilisons SnapCenter pour la sauvegarde et la restauration intégrant la cohérence applicative.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Le basculement de la machine virtuelle Microsoft SQL Server

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
  - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- Veeam Replication permet de modifier les adresses IP des VM sur le site de reprise après incident.

Reprise après incident des applications avec SnapCenter, Cloud Volumes ONTAP et Veeam Replication

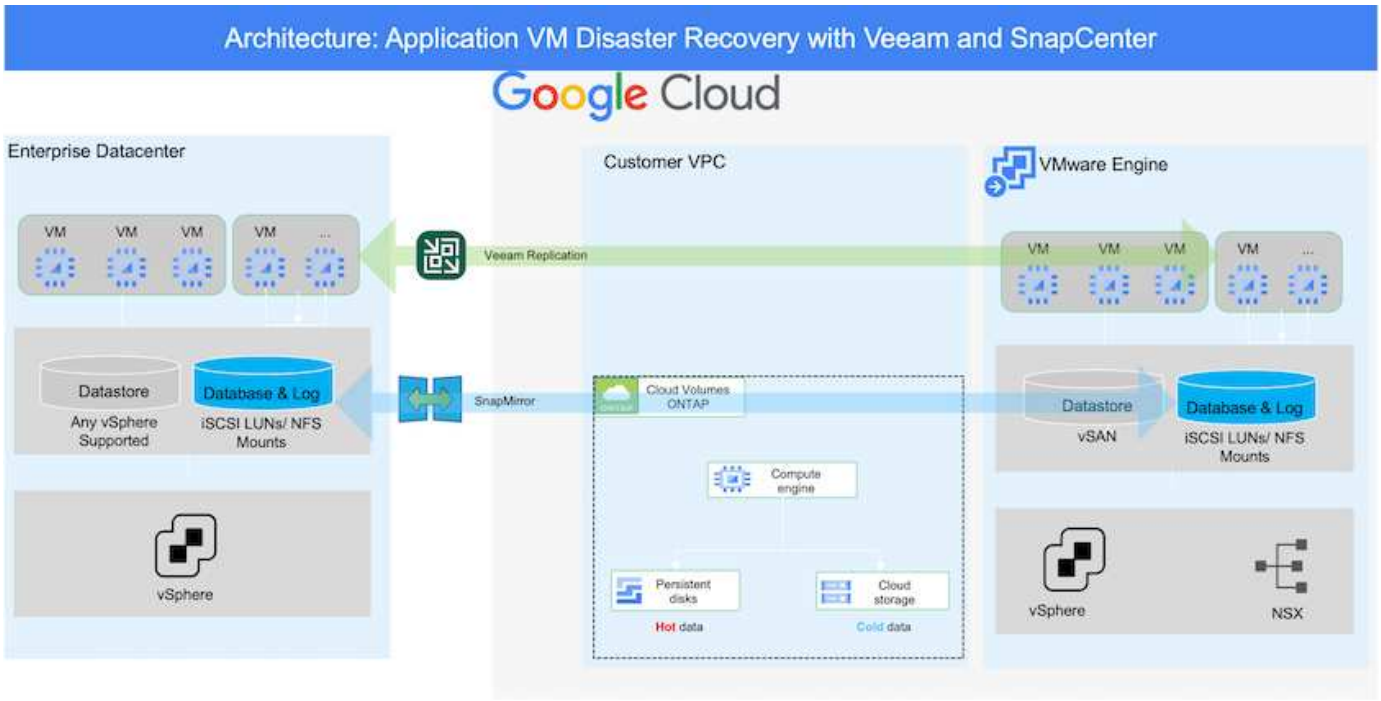
Auteurs : Suresh Thoppay, NetApp

Présentation

La reprise d'activité dans le cloud est une solution résiliente et économique qui protège les charges de travail contre les pannes sur site et la corruption des données, comme les attaques par ransomware. NetApp SnapMirror permet de répliquer les charges de travail VMware sur site utilisant un stockage connecté à l'invité vers NetApp Cloud Volumes ONTAP exécuté dans Google Cloud. Il s'agit aussi des données applicatives,

mais qu'en est-il des machines virtuelles elles-mêmes ? La reprise sur incident doit couvrir tous les composants dépendants, notamment les machines virtuelles, les VMDK ou les données d'application. Pour ce faire, SnapMirror et Veeam peuvent être utilisés pour restaurer de manière transparente les workloads répliqués depuis des sites sur Cloud Volumes ONTAP et en utilisant le stockage VSAN pour les VMDK de VM.

Ce document propose une approche détaillée de la configuration et de l'exécution d'une reprise d'activité à l'aide de NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document est axé sur le stockage invité pour les données d'applications (également appelé « invité connecté »), et nous supposons que l'environnement sur site utilise SnapCenter pour assurer des sauvegardes cohérentes au niveau des applications.

> Ce document s'applique à toute solution de sauvegarde et de restauration tierce. En fonction de la solution utilisée dans l'environnement, suivez les bonnes pratiques pour créer des stratégies de sauvegarde conformes aux SLA de l'entreprise.

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que une interconnexion dédiée ou un VPN cloud. Les segments doivent être créés en fonction de la conception VLAN sur site.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document. Consultez la documentation Google Cloud pour connaître la méthode de connectivité appropriée, du site vers Google.

Déploiement de la solution de reprise d'activité

Présentation du déploiement de la solution

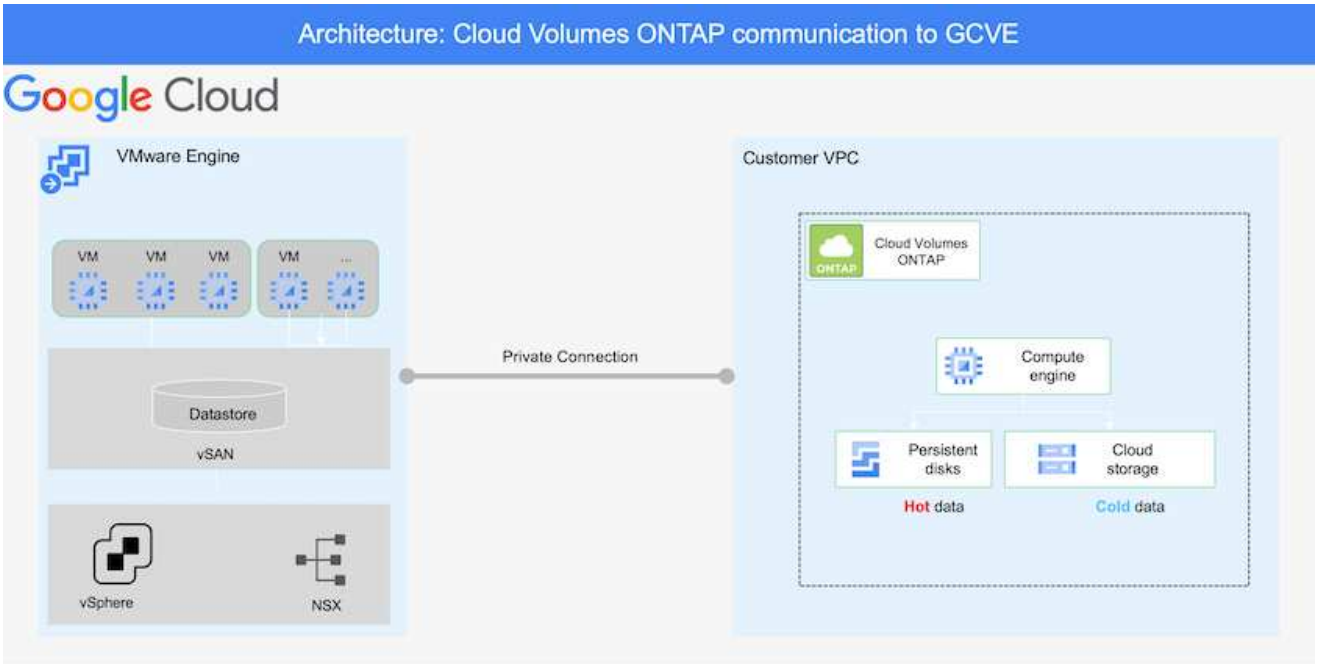
1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.

2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de Cloud Manager dans l'abonnement et le réseau virtuel appropriés.
   a. Configurer SnapMirror pour les volumes applicatifs concernés.
   b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer des machines virtuelles sur l'instance Google Cloud VMware Engine.
4. En cas d'incident, interrompre la relation SnapMirror avec Cloud Manager et déclencher le basculement des machines virtuelles avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
   b. Permet de mettre les applications en ligne.
5. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Google Cloud et répliquez les volumes dans CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Google Cloud ("cvo") Et répliquez les volumes souhaités dans Cloud Volumes ONTAP avec les fréquences et les instantanés souhaités.



Pour obtenir des exemples d'instructions détaillées sur la configuration de SnapCenter et la réplication des données, reportez-vous à la section "Configurez la réplication avec SnapCenter"

Configurez la réplication avec SnapCenter

Configurez l'accès aux données des hôtes GCVE et CVO

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution GCVE et le temps de maintenance du SDDC. Ces deux considérations clés à prendre en compte dans une solution de reprise sur incident permettent de réduire les coûts d'exploitation globaux. Le SDDC peut héberger jusqu'à trois hôtes, tout comme un cluster multi-hôtes dans un déploiement à grande échelle.

Cloud Volumes ONTAP peut être déployé sur n'importe quel VPC et GCVE doit disposer d'une connexion privée à ce VPC pour que la VM se connecte aux LUN iSCSI.

Pour configurer GCVE SDDC, voir "Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)". Avant cela, vérifiez que les VM invités résidant sur les hôtes GCVE peuvent consommer des données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et GCVE ont été correctement configurés, commencez à configurer Veeam pour automatiser la restauration des workloads sur site vers GCVE (machines virtuelles avec VMDK d'application et VM avec stockage « Guest ») en utilisant la fonctionnalité de réplication Veeam et en utilisant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

Installer les composants Veeam

Selon le scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde à déployer. Pour ce cas d'utilisation, nul besoin de déployer un magasin d'objets pour Veeam et le référentiel scale-out non plus requis.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Se référer à la documentation Veeam pour la procédure d'installation"]

Configuration de la réplication de machine virtuelle avec Veeam

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere" À l'étape traitement invité de l'assistant, sélectionnez Désactiver le traitement de l'application, car nous utilisons SnapCenter pour la sauvegarde et la restauration intégrant la cohérence applicative.

Configuration de la tâche de réplication de VM vSphere

Le basculement de la machine virtuelle Microsoft SQL Server

Le basculement de la machine virtuelle Microsoft SQL Server

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.

    - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
    - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
    - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- Veeam Replication permet de modifier les adresses IP des VM sur le site de reprise après incident.

Migration de workloads sur GCP/GCVE

Migrez vos workloads vers un datastore NetApp Cloud Volume Service sur Google Cloud VMware Engine avec VMware HCX - Guide de démarrage rapide

Auteur(s) : Ingénierie de solutions NetApp

Présentation : migration de machines virtuelles avec VMware HCX, datastores NetApp Cloud Volume Service et Google Cloud VMware Engine (GCVE)

L'une des utilisations les plus courantes pour le magasin de données Google Cloud VMware Engine et Cloud Volume Service est la migration des charges de travail VMware. VMware HCX est une option privilégiée qui propose plusieurs mécanismes de migration pour transférer des machines virtuelles sur site et leurs données vers des datastores NFS Cloud Volume Service.

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

Ce document fournit des instructions détaillées pour le provisionnement du datastore Cloud Volume Service, suivi du téléchargement, du déploiement et de la configuration de VMware HCX, y compris tous ses composants principaux sur site et Google Cloud VMware Engine, y compris l'interconnexion, l'extension réseau et l'optimisation WAN pour activer divers mécanismes de migration de machines virtuelles.

VMware HCX fonctionne avec n'importe quel type de datastore lorsque la migration se trouve au niveau des VM. Ce document s'applique donc aux clients NetApp et aux clients non NetApp qui prévoient de déployer Cloud Volume Service avec Google Cloud VMware Engine pour un déploiement cloud VMware économique.

Étapes générales

Cette liste fournit les étapes générales nécessaires pour coupler et migrer les machines virtuelles vers HCX Cloud Manager sur le côté Google Cloud VMware Engine depuis HCX Connector sur site :

1. Préparez HCX à partir du portail Google VMware Engine.
2. Téléchargez et déployez le programme d'installation HCX Connector Open Virtualization Appliance (OVA) dans VMware vCenter Server sur site.
3. Activez HCX à l'aide de la clé de licence.
4. Couplez le connecteur VMware HCX sur site avec Google Cloud VMware Engine HCX Cloud Manager.
5. Configurez le profil réseau, le profil de calcul et le maillage de service.
6. (Facultatif) effectuez l'extension réseau pour éviter toute nouvelle IP pendant les migrations.
7. Validez l'état du système et assurez-vous que la migration est possible.
8. Migrer les workloads de VM.

Prérequis

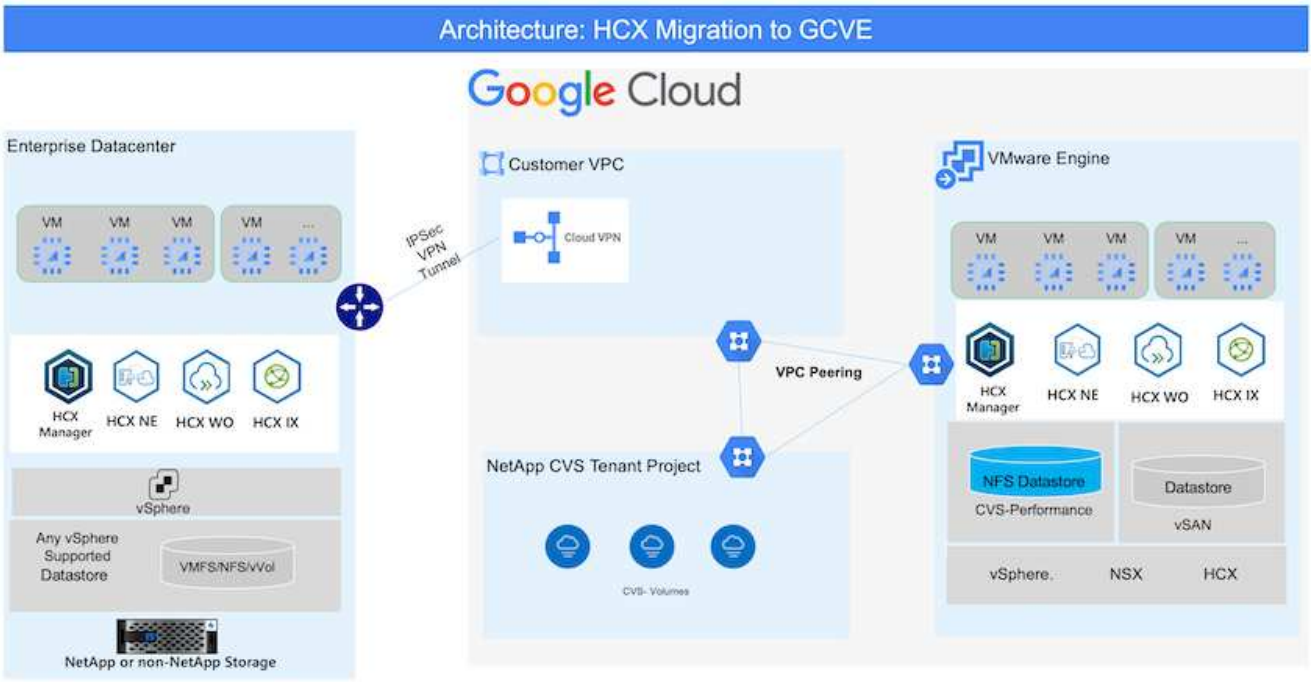
Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, reportez-vous à ce document "lien". Une fois les prérequis, y compris la connectivité, téléchargez la clé de licence HCX sur le portail Google Cloud VMware Engine. Une fois le programme d'installation OVA téléchargé, procédez au processus d'installation comme décrit ci-dessous.

HCX Advanced est l'option par défaut et VMware HCX Enterprise Edition est également disponible via un ticket d'assistance et pris en charge sans frais supplémentaires. Reportez-vous à "ce lien"

- L'utilisation d'un Software-Defined Data Center (SDDC) Google Cloud VMware Engine ou la création d'un cloud privé à l'aide de ce protocole "Lien NetApp" ou ceci "Lien Google".
- La migration des VM et des données associées depuis le data Center sur site compatible VMware vSphere nécessite une connectivité réseau du data Center vers l'environnement SDDC. Avant de migrer des workloads, "Configurez une connexion au cloud VPN ou à l'interconnexion du cloud" entre l'environnement sur site et le cloud privé respectif.
- Le chemin du réseau depuis l'environnement VMware vCenter Server sur site vers le cloud privé Google Cloud VMware Engine doit prendre en charge la migration des machines virtuelles à l'aide de vMotion.
- 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.
- Le volume NFS Cloud Volume Service doit être monté en tant que datastore dans Google Cloud VMware Engine. Suivez les étapes décrites dans ce document "lien" Ajout de datastores Cloud Volume Service à des hôtes Google Cloud VMware Engines.

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 cloud, qui autorise la connectivité sur site à Google Cloud VPC.



Pour plus d'informations sur le schéma HCX, reportez-vous à "Lien VMware"

Déploiement de la solution

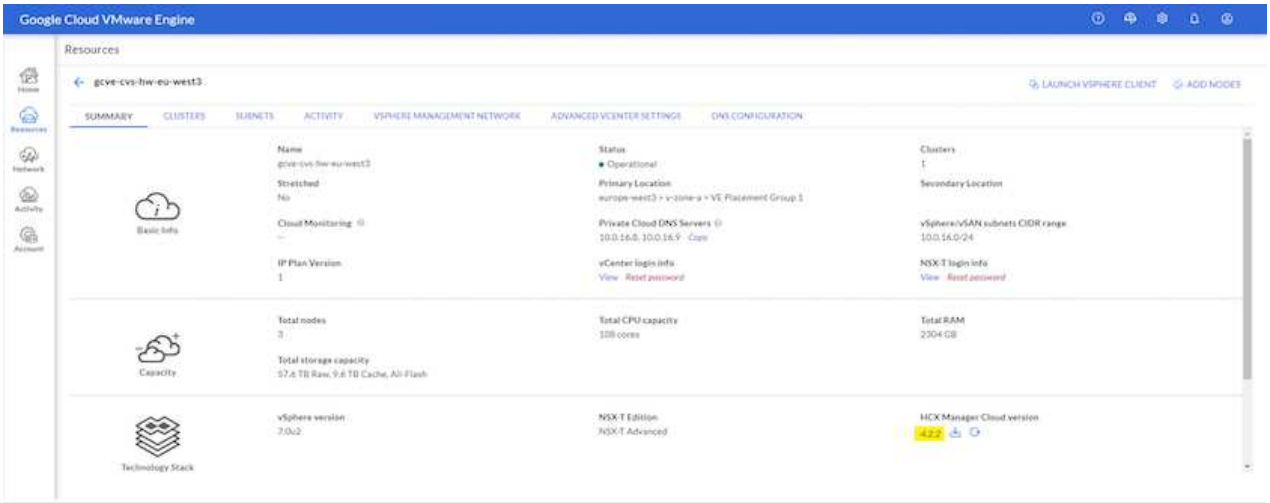
Suivez les étapes du déploiement de cette solution :

Étape 1 : préparer HCX via le portail Google VMware Engine

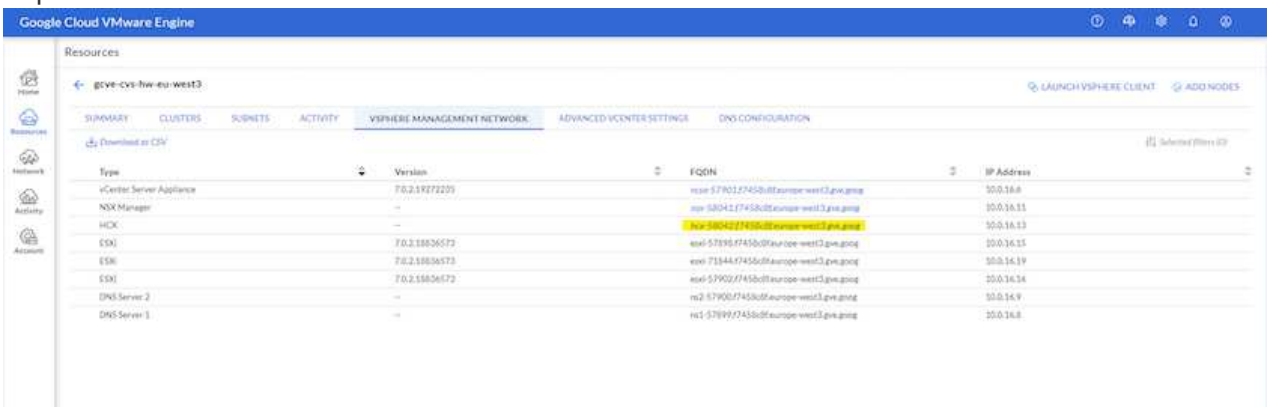
LE composant HCX Cloud Manager est automatiquement installé lorsque vous provisionnez le cloud privé avec VMware Engine. Pour préparer le couplage du site, procédez comme suit :

1. Connectez-vous au portail Google VMware Engine Portal et connectez-vous au HCX Cloud Manager.

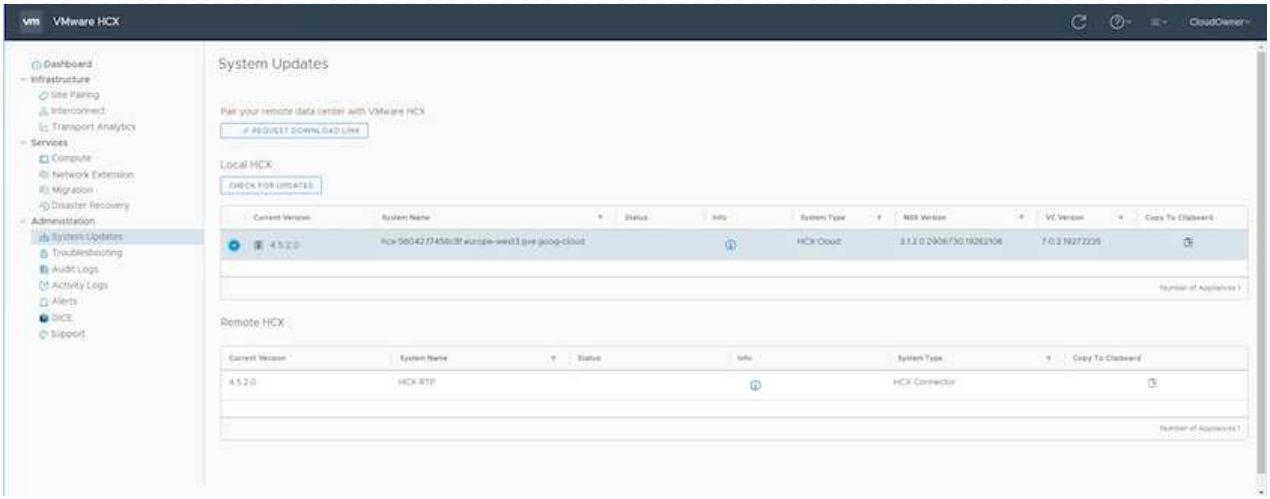
   Vous pouvez vous connecter à la console HCX en cliquant sur le lien de la version HCX



   Ou cliquez sur le FQDN HCX sous l'onglet réseau de gestion vSphere.



2. Dans HCX Cloud Manager, accédez à **Administration > mises à jour du système**.
3. Cliquez sur **Request download link** et téléchargez le fichier OVA.



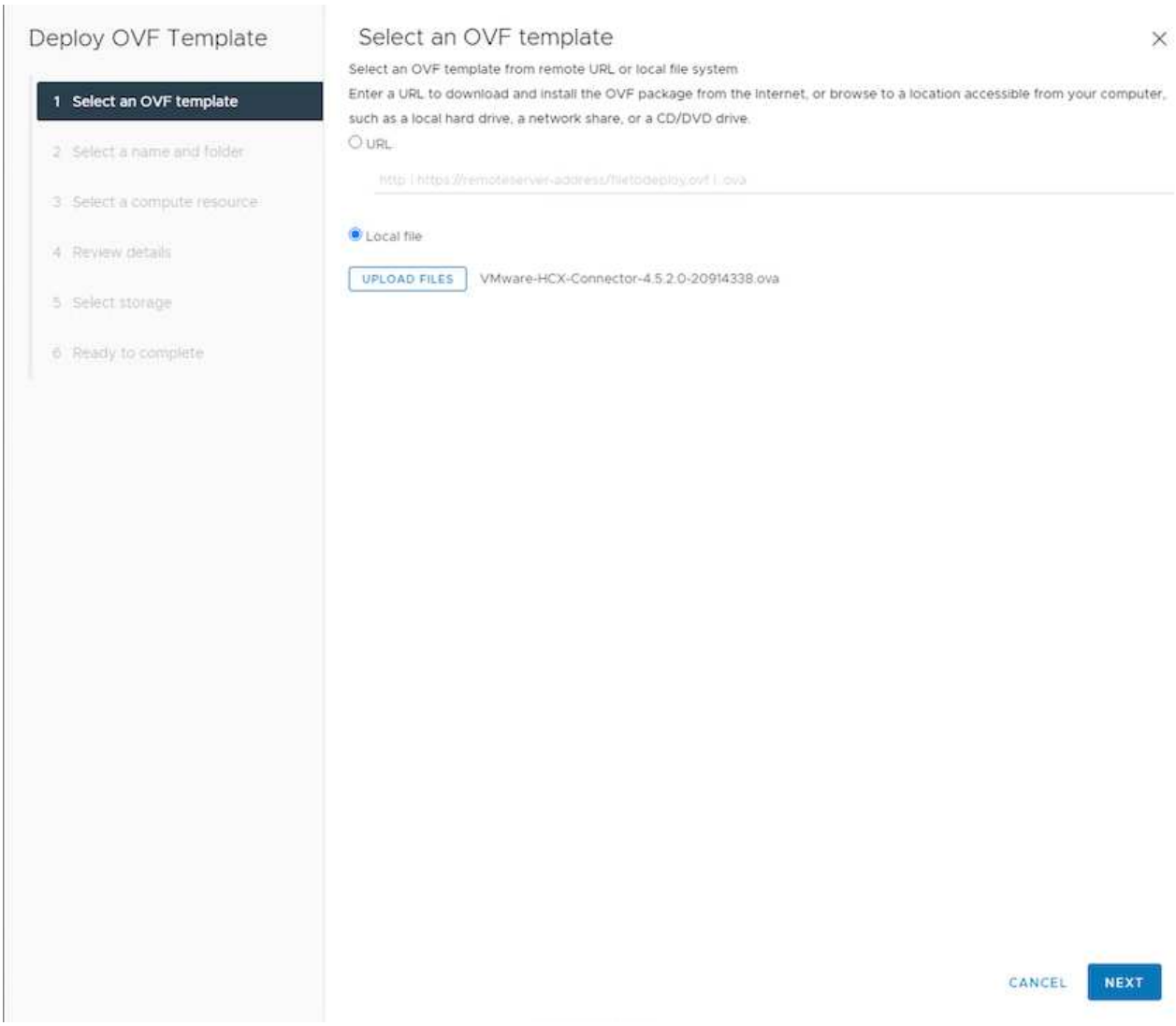
4. Mettez à jour HCX Cloud Manager vers la dernière version disponible depuis l'interface utilisateur HCX Cloud Manager.

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

Pour que le connecteur sur site puisse se connecter au HCX Manager dans Google Cloud VMware Engine, assurez-vous que les ports pare-feu appropriés sont ouverts dans l'environnement sur site.

Pour télécharger et installer HCX Connector dans le serveur vCenter sur site, procédez comme suit :

1. Téléchargez les ova depuis la console HCX sur Google Cloud VMware Engine, comme indiqué à l'étape précédente.
2. Une fois le fichier OVA téléchargé, déployez-le dans l'environnement VMware vSphere sur site à l'aide de l'option **Deploy OVF Template**.



3. Entrez toutes les informations requises pour le déploiement OVA, cliquez sur **Next**, puis sur **Finish** pour déployer le connecteur OVA VMware HCX.

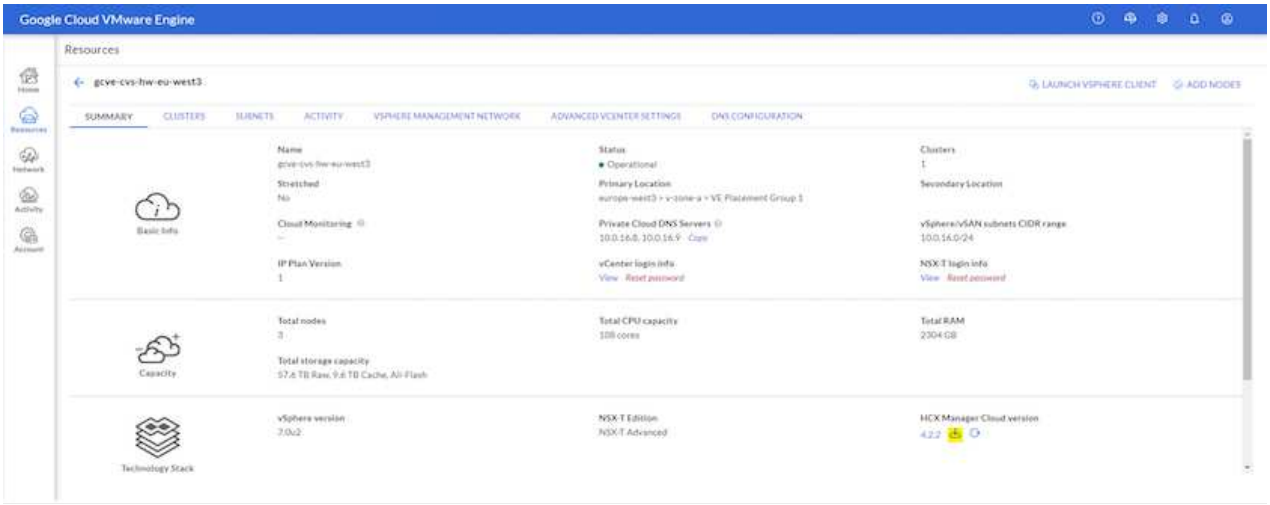
> Mettez l'appliance virtuelle sous tension manuellement.

Pour des instructions détaillées, reportez-vous à la "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 du portail Google Cloud VMware Engine et activez-la dans VMware HCX Manager.

1. Sur le portail VMware Engine, cliquez sur Ressources, sélectionnez le cloud privé et **cliquez sur l'icône de téléchargement sous HCX Manager Cloud version**
   .



   Ouvrez le fichier téléchargé et copiez la chaîne de clé de licence.

2. Connectez-vous au gestionnaire VMware HCX sur site à l'adresse "https://hcxmanagerIP:9443" utilisation des informations d'identification administrateur.

   Utilisez l'hcxmangerIP et le mot de passe définis lors du déploiement du système OVA.

3. Dans la licence, entrez la clé copiée à partir de l'étape 3 et cliquez sur **Activer**.

   Le connecteur HCX sur site doit disposer d'un accès Internet.

4. Sous **Datacenter Location**, indiquez l'emplacement le plus proche pour l'installation sur site de VMware HCX Manager. Cliquez sur **Continuer**.
5. Sous **Nom du système**, mettez à jour le nom et cliquez sur **Continuer**.
6. Cliquez sur **Oui, Continuer**.
7. Sous **Connect Your vCenter**, indiquez le nom de domaine complet (FQDN) ou l'adresse IP de vCenter Server et les informations d'identification appropriées, puis cliquez sur **Continuer**.

   Utilisez le FQDN pour éviter les problèmes de connectivité ultérieurement.

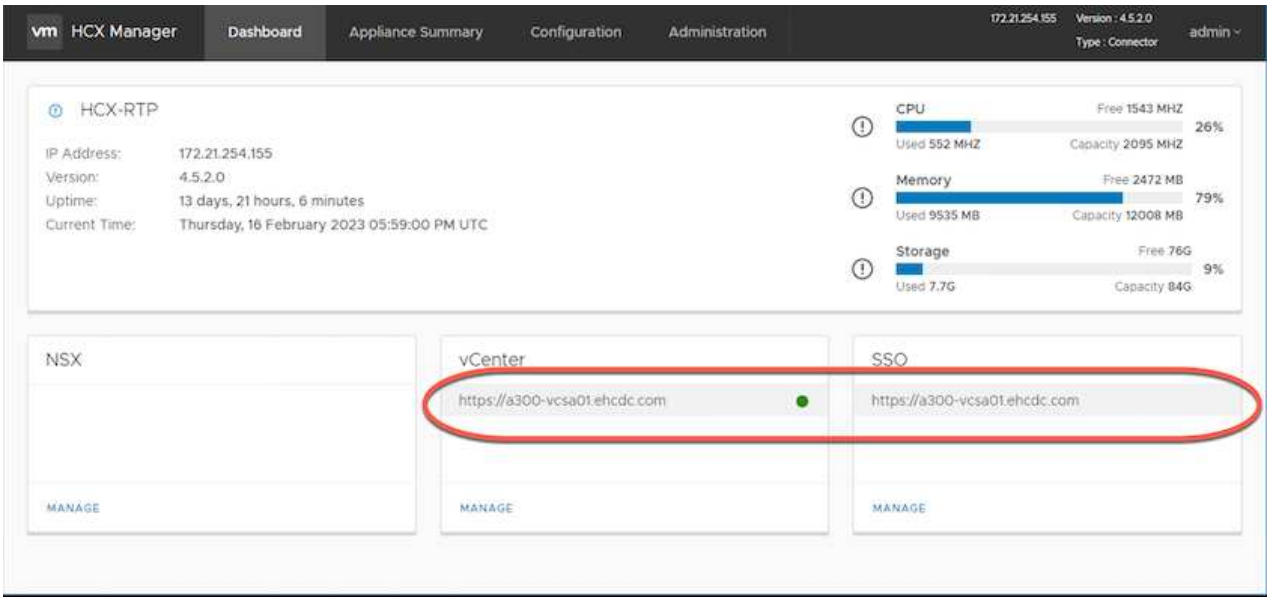
8. Sous **configurer SSO/PSC**, indiquez le FQDN ou l'adresse IP du contrôleur des services de plate-forme (PSC) et cliquez sur **Continuer**.

   Pour Embedded PSC, entrez le nom de domaine complet ou l'adresse IP du serveur VMware vCenter.

9. Vérifiez que les informations saisies sont correctes et cliquez sur **redémarrer**.

10. Après le redémarrage des services, vCenter Server s'affiche en vert sur la page qui s'affiche. VCenter Server et SSO doivent avoir les paramètres de configuration appropriés, qui doivent être identiques à la page précédente.

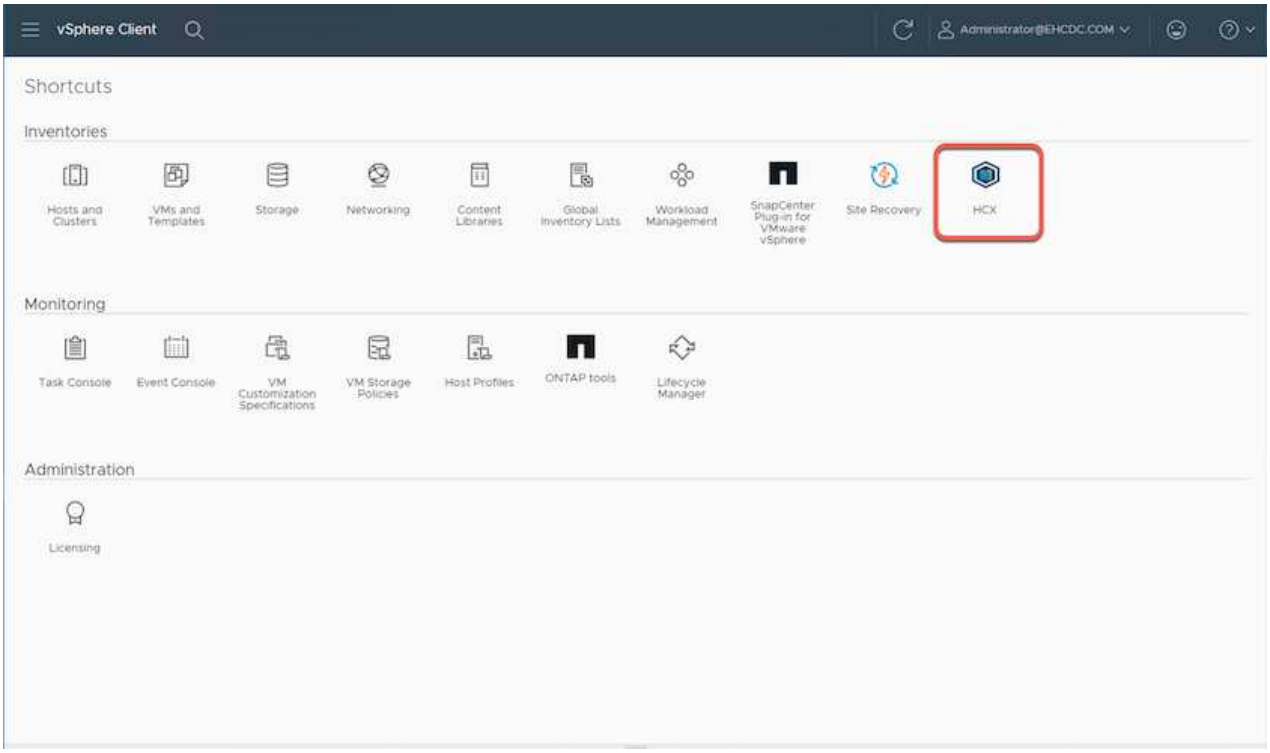
> Ce processus dure environ 10 à 20 minutes et le plug-in doit être ajouté à vCenter Server.



Étape 4 : connecteur VMware HCX sur site avec Google Cloud VMware Engine HCX Cloud Manager

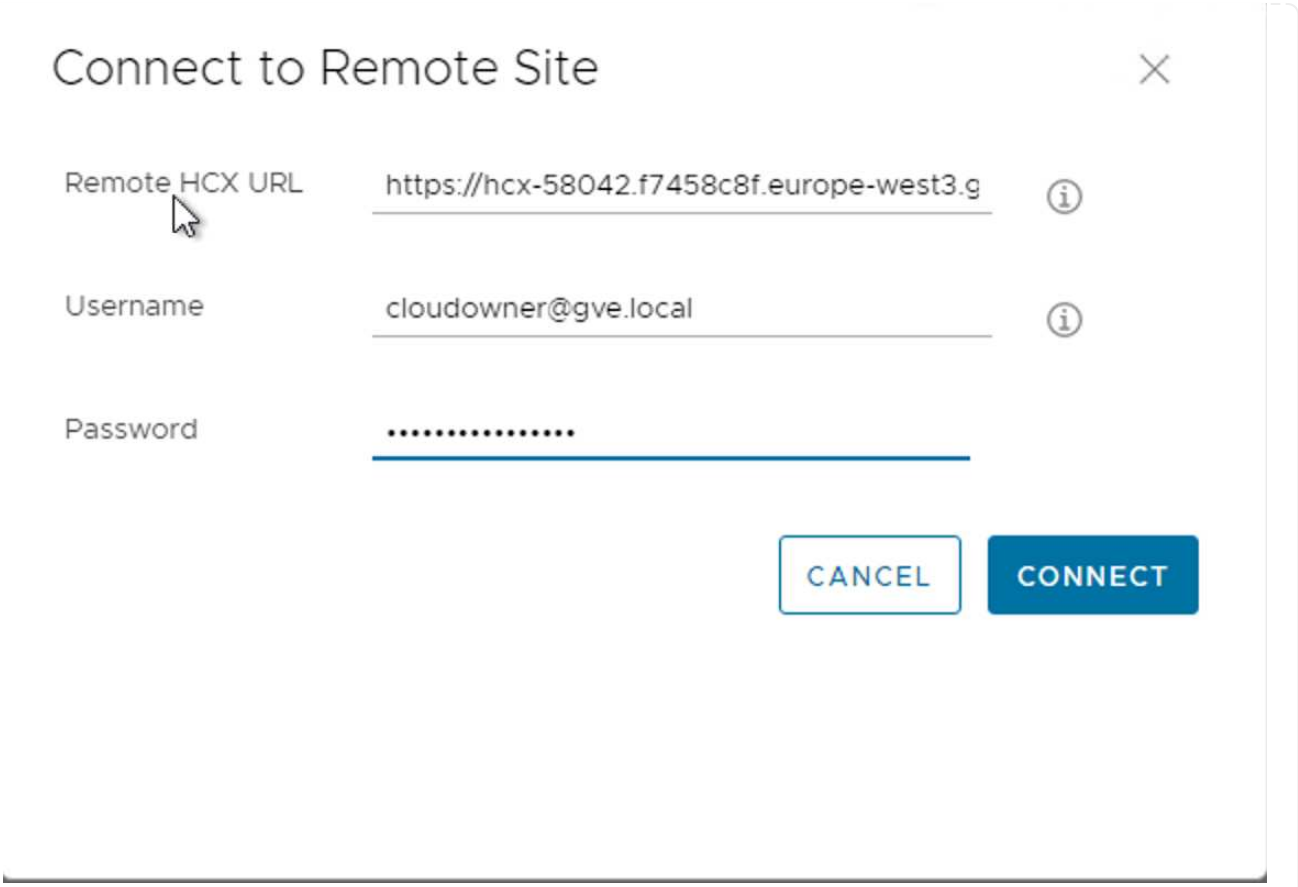
Une fois que HCX Connector est déployé et configuré sur site vCenter, établissez une connexion à Cloud Manager en ajoutant le couplage. Pour configurer le couplage du site, procédez comme suit :

1. Pour créer une paire de sites entre l'environnement vCenter sur site et Google Cloud VMware Engine SDDC, connectez-vous au serveur vCenter sur site et accédez au nouveau plug-in client Web HCX vSphere.



2. Sous Infrastructure, cliquez sur **Ajouter un couplage de site**.

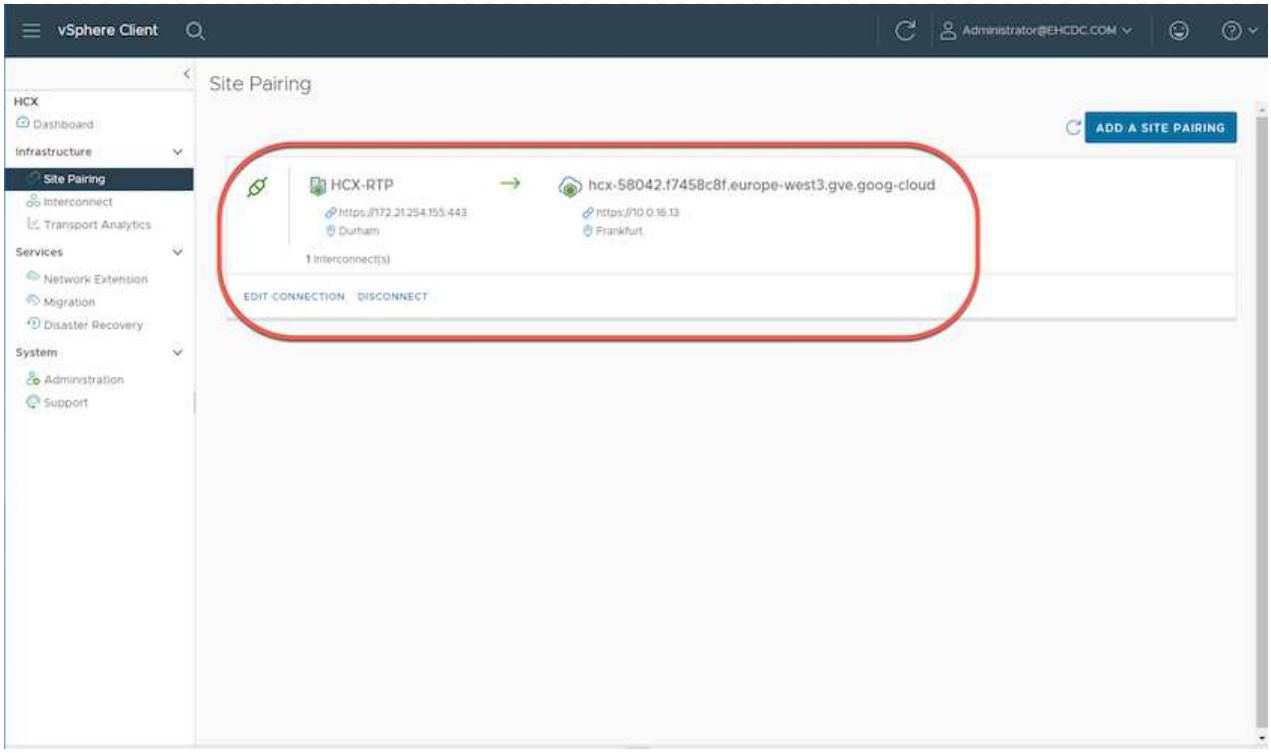
Entrez l'URL ou l'adresse IP Google Cloud VMware Engine HCX Cloud Manager et les identifiants de l'utilisateur disposant des privilèges de rôle propriétaire cloud pour accéder au cloud privé.



3. Cliquez sur **connexion**.

> Le connecteur VMware HCX doit pouvoir acheminer vers 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.

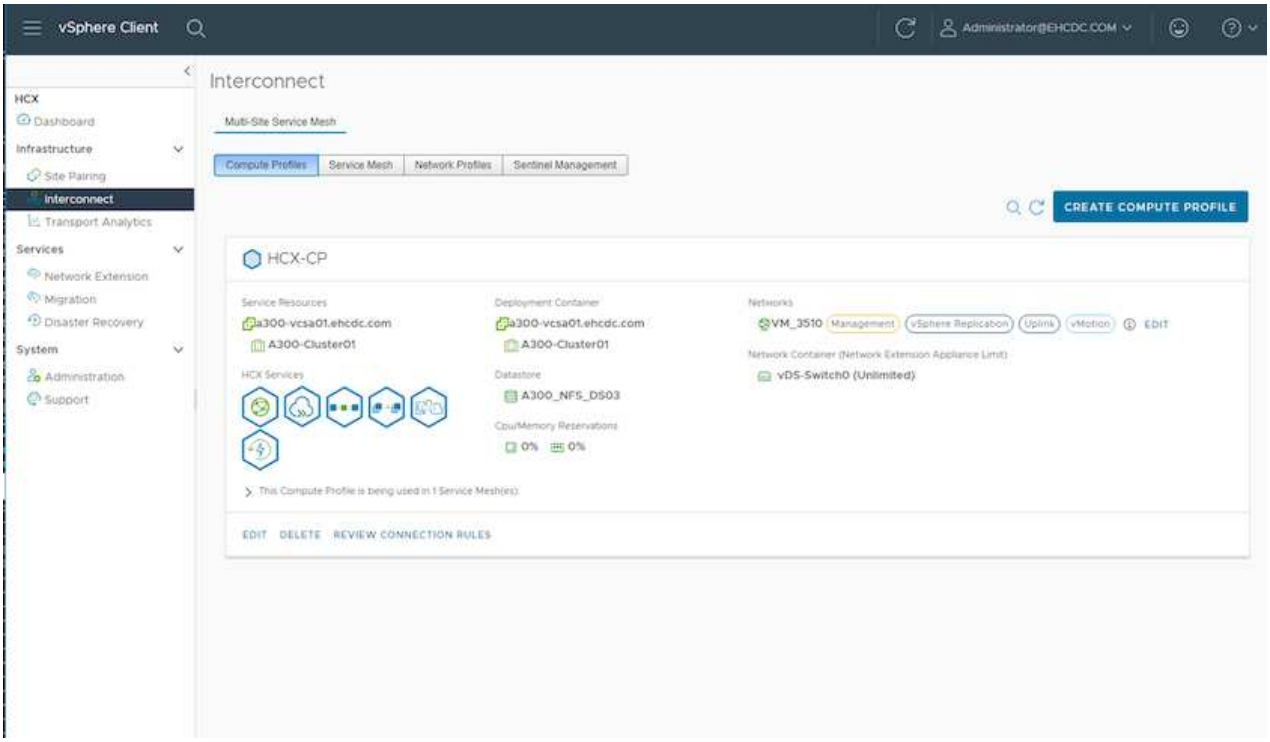

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

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

Le dispositif d'interconnexion VMware HCX offre des fonctionnalités de réplication et de migration basée sur vMotion via Internet et des connexions privées vers le site cible. L'interconnexion offre le cryptage, l'ingénierie du trafic et la mobilité des machines virtuelles. Pour créer une appliance de service d'interconnexion, procédez comme suit :

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

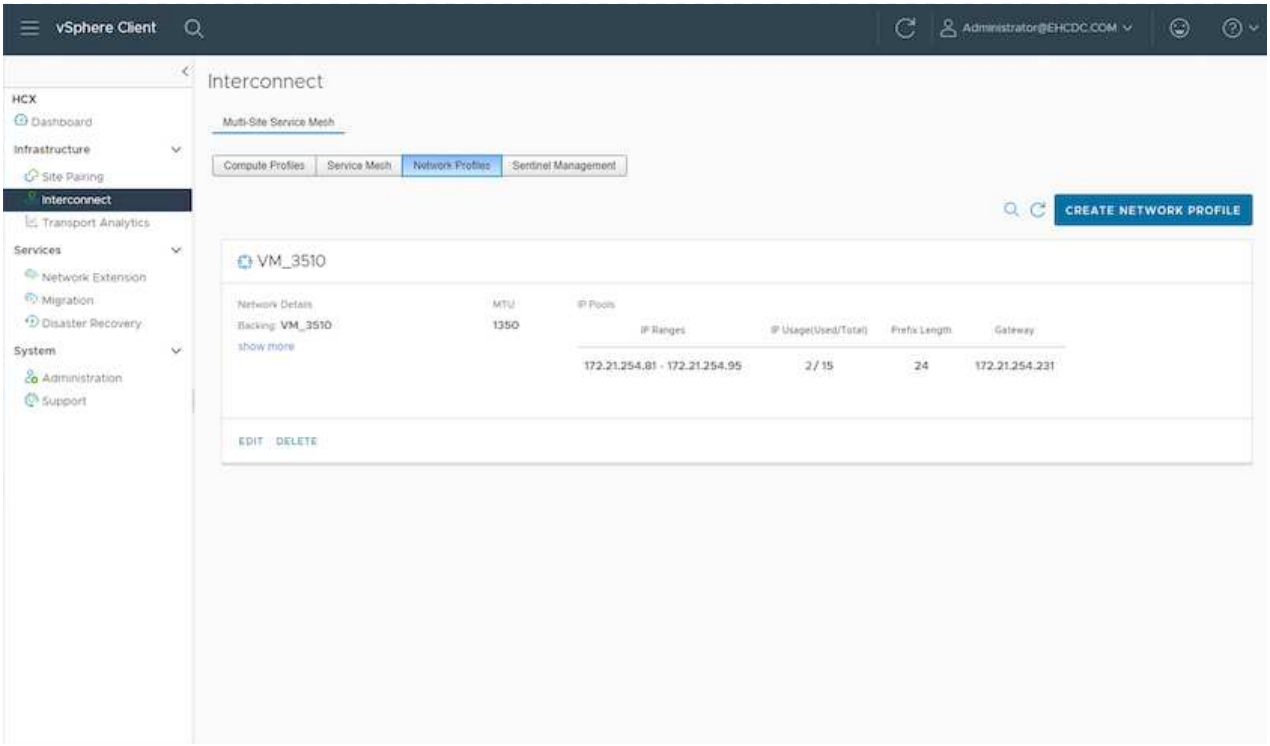
   Les profils de calcul définissent les paramètres de déploiement, y compris les appliances déployées et la partie du data Center VMware accessible au service HCX.



2. Une fois le profil de calcul créé, créez les profils réseau en sélectionnant **maillage de service multisite > profils réseau > Créer profil réseau**.

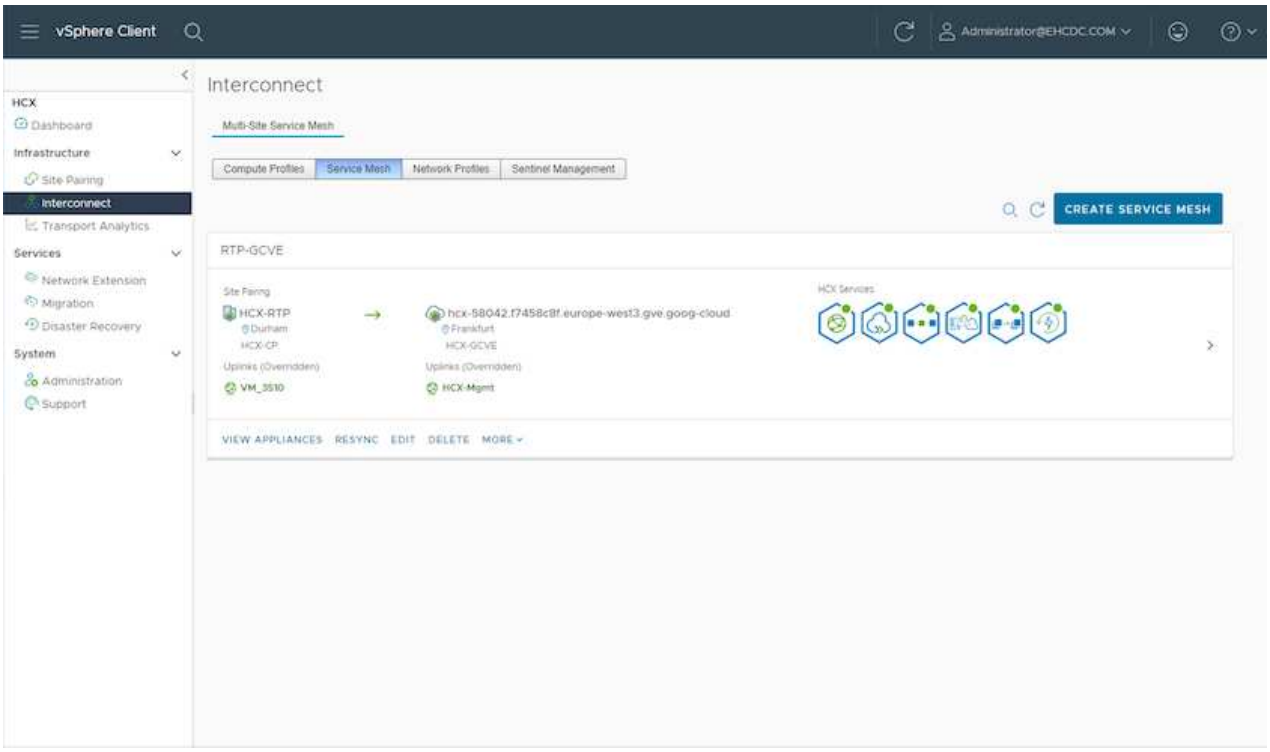
   Le profil réseau définit une plage d'adresses IP et de réseaux utilisés par HCX pour ses appliances virtuelles.

   Cette étape nécessite au moins deux adresses IP. Ces adresses IP sont attribuées depuis le réseau de gestion aux dispositifs d'interconnexion.

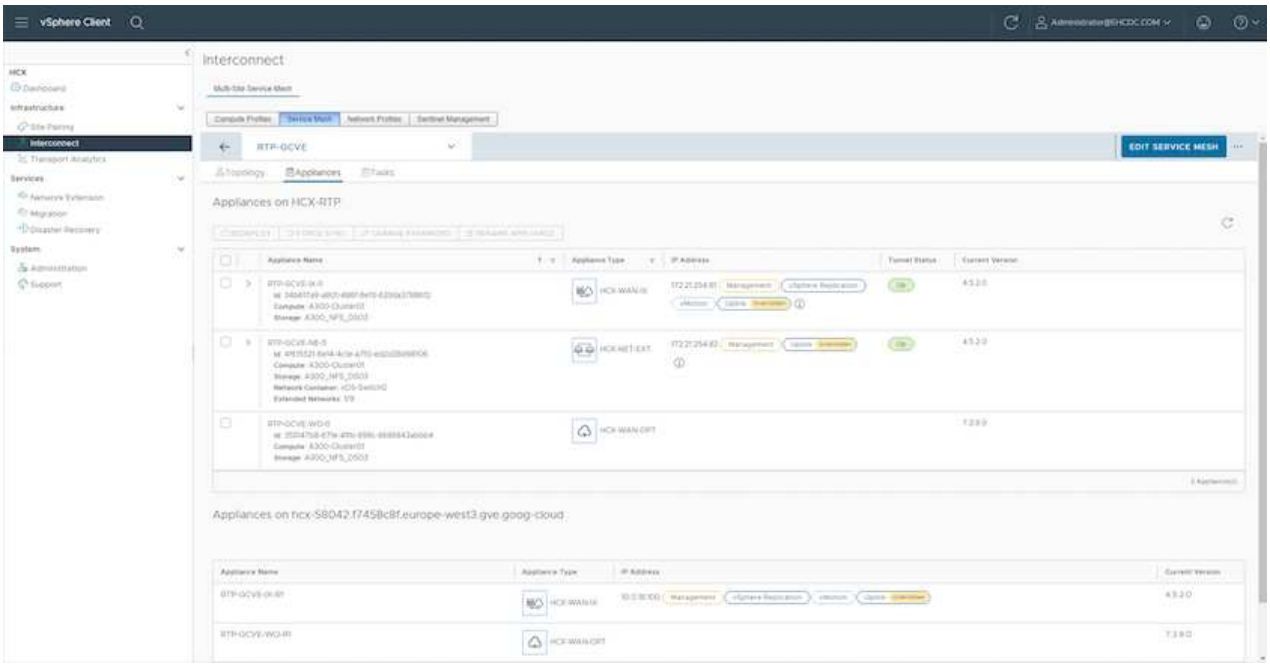


3. A ce stade, les profils de calcul et de réseau ont été créés avec succès.
4. Créez le maillage de service en sélectionnant l'onglet **maillage de service** dans l'option **Interconnexion** et sélectionnez les sites SDDC sur site et GCVE.
5. Le maillage de service spécifie une paire de profils réseau et de calcul locale et distante.

Dans le cadre de ce processus, les appliances HCX sont déployées et configurées automatiquement sur les sites source et cible afin de créer une structure de transport sécurisée.



6. Il s’agit de la dernière étape de la configuration. Le déploiement devrait s’effectuer en 30 minutes environ. Une fois le maillage de service configuré, l’environnement est prêt avec les tunnels IPsec créés pour migrer les VM de charge de travail.



Étape 6 : migrer les workloads

Les charges de travail peuvent être migrées de façon bidirectionnelle entre les SDDC sur site et GCVE à l'aide de diverses technologies de migration HCX de VMware. Les machines virtuelles peuvent être déplacées vers et depuis des entités activées par VMware HCX à l'aide de plusieurs 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 l'édition Enterprise de HCX) et la migration assistée par système d'exploitation HCX (disponible avec l'édition Enterprise de HCX).

Pour en savoir plus sur les différents mécanismes de migration HCX, voir "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).

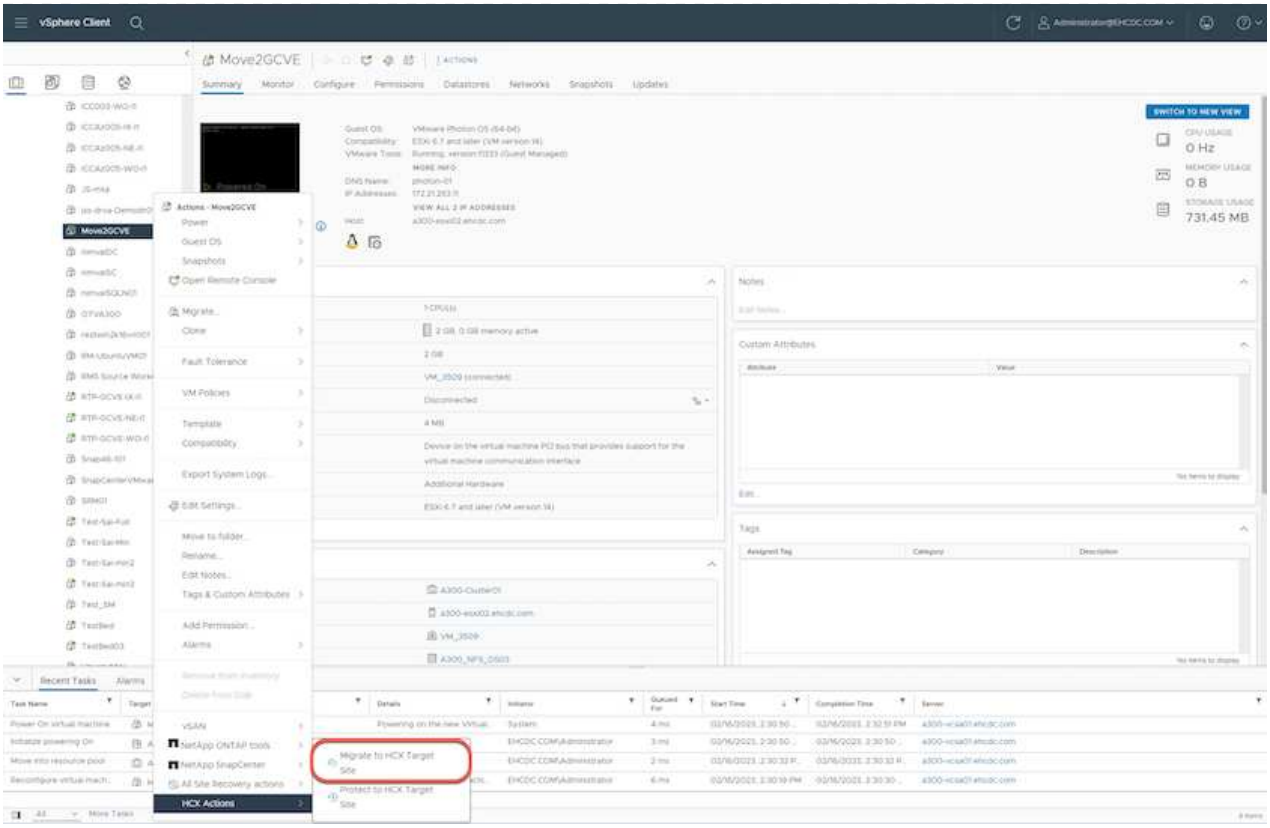
> ⓘ L'appliance HCX-IX ajoute le service Mobility Agent en tant qu'objet hôte dans vCenter Server. Les ressources processeur, mémoire, stockage et réseau affichées sur cet objet ne représentent pas la consommation réelle sur l'hyperviseur physique hébergeant l'appliance IX.

HCX vMotion

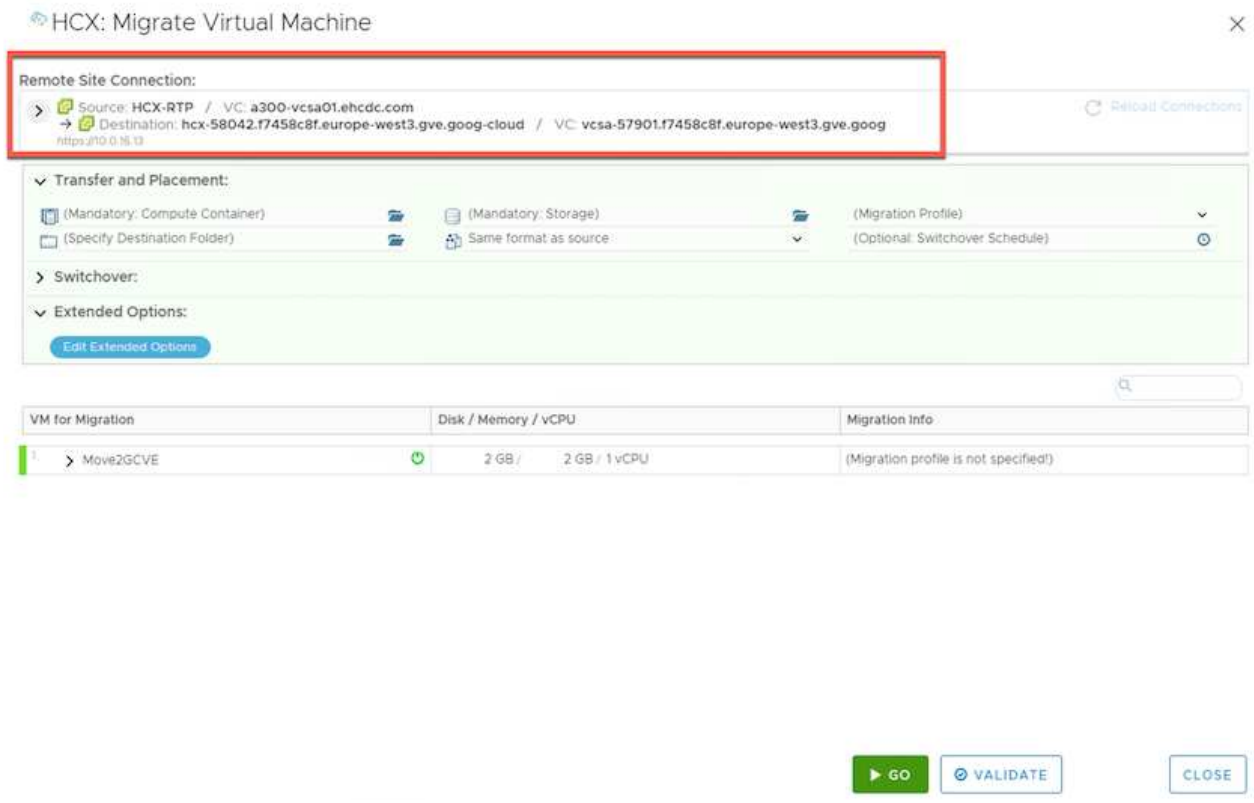
Cette section décrit le mécanisme HCX vMotion. Cette technologie de migration utilise le protocole VMware vMotion pour migrer un VM vers GCVE. L'option de migration vMotion permet de migrer l'état d'une machine virtuelle unique à la fois. Il n'y a pas d'interruption de service pendant cette méthode de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

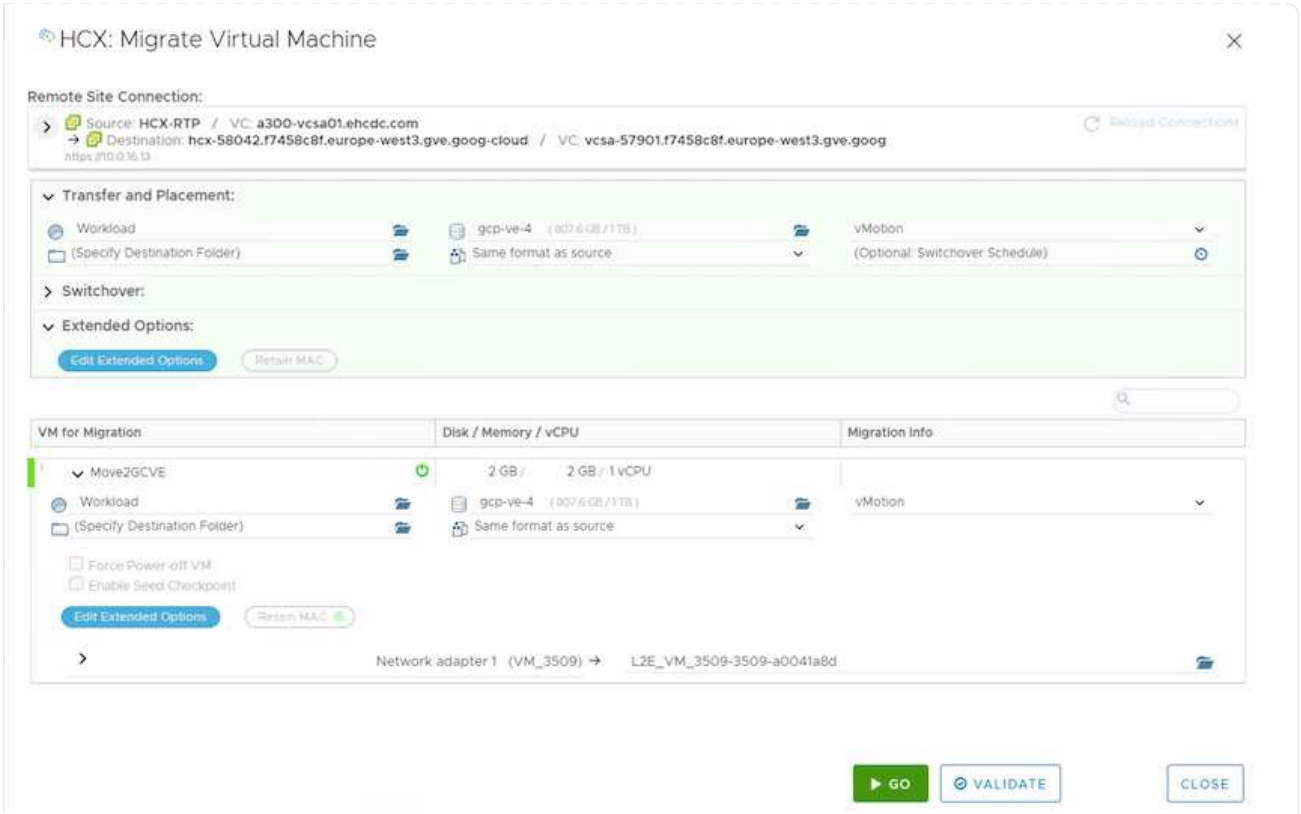
1. Depuis le client vSphere sur site, accédez à Inventory, faites un clic droit sur la machine virtuelle à migrer, puis sélectionnez HCX actions > Migrate to HCX site cible.



2. Dans l’assistant de migration d’ordinateur virtuel, sélectionnez connexion de site distant (GCVE cible).



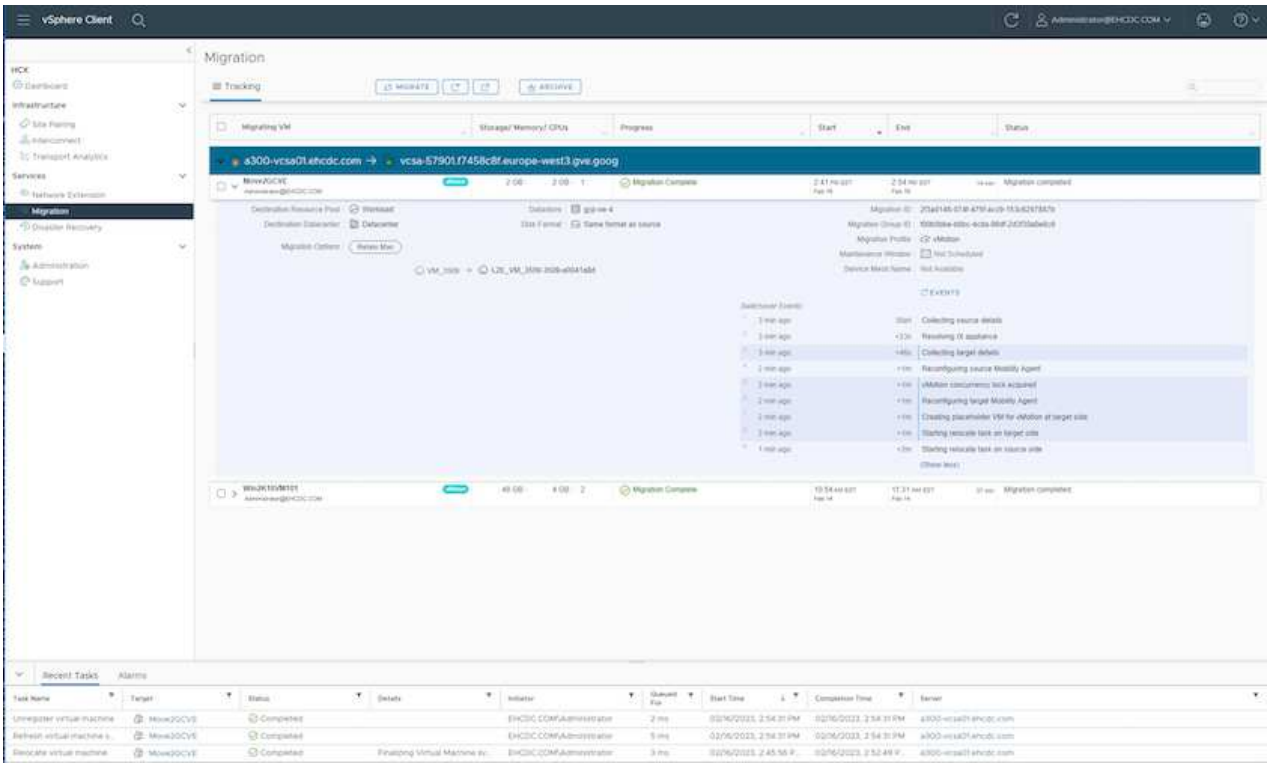
3. Mettez à jour les champs obligatoires (Cluster, Storage et destination Network), puis cliquez sur Validate.



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.



L'espace requis pour le datastore NFS CVS cible doit être suffisant pour gérer la migration.

Conclusion

Que vous ciblez les clouds ou les clouds hybrides et les données qui résident sur un stockage sur site de tout type ou fournisseur, Cloud Volume Service et HCX offrent d'excellentes options pour déployer et migrer les charges de travail applicatives tout en réduisant le coût total de possession en rendant les besoins en données transparents vers la couche applicative. Quelles que soient les utilisations, choisissez Google Cloud VMware Engine et Cloud Volume Service 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 élevées. Il s'agit du même processus et procédures que celui utilisé pour connecter le stockage et migrer les machines virtuelles à l'aide de VMware vSphere Replication, VMware vMotion ou même de la copie de fichiers réseau (NFC).

Messages clés

Les points clés de ce document sont les suivants :

- Il est désormais possible d'utiliser Cloud Volume Service comme datastore sur Google Cloud VMware Engine SDDC.
- Vous pouvez facilement migrer les données depuis des installations sur site vers le datastore Cloud Volume Service.
- Vous pouvez facilement étendre et réduire le datastore Cloud Volume Service pour répondre aux exigences de capacité et de performances lors de l'activité de migration.

Vidéos de référence de Google et VMware

De Google

- "Déployer le connecteur HCX avec GCVE"
- "Configurez le maillage HCX avec GCVE"
- "Migrer VM avec HCX vers GCVE"

À l'aide de VMware

- "Déploiement DU connecteur HCX pour GCVE"
- "Configuration SERVICEMESH HCX pour GCVE"
- "Migration de la charge DE travail HCX vers GCVE"

Où trouver des informations complémentaires

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

- Documentation Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentation du service Cloud volumes

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- Guide de l'utilisateur VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

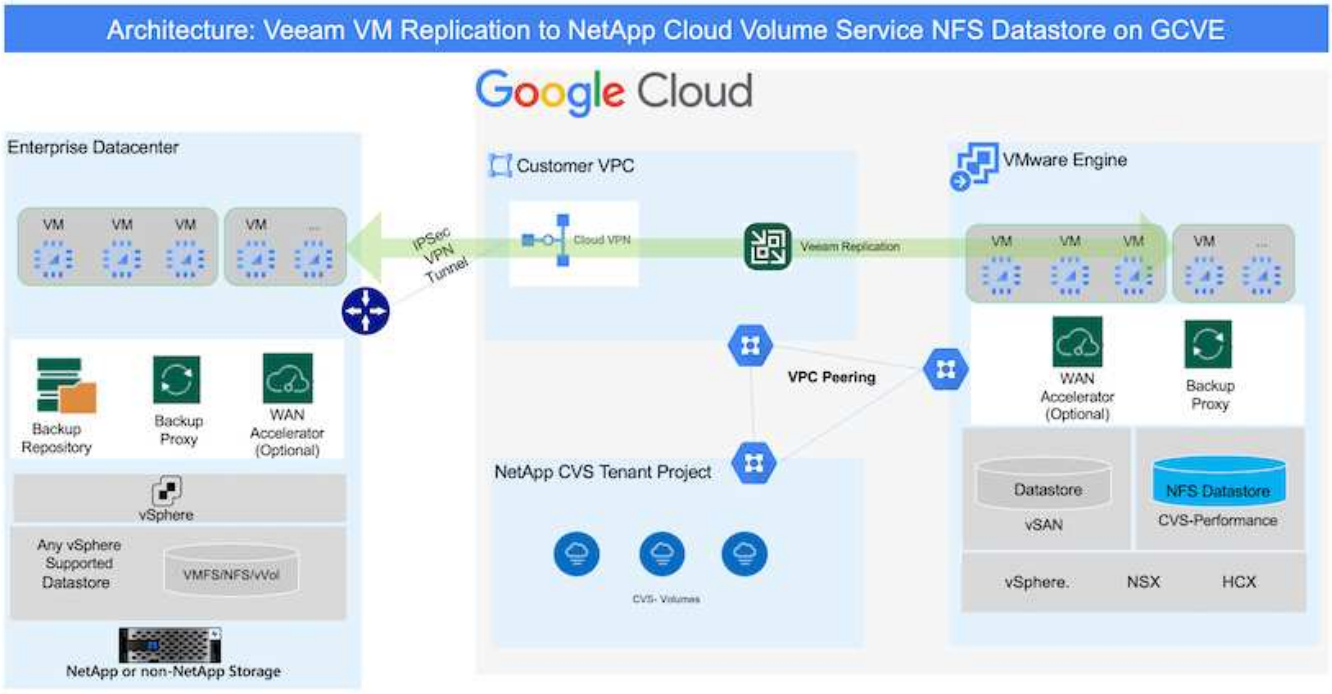
Migration de machines virtuelles vers un datastore NFS NetApp Cloud Volume Service sur Google Cloud VMware Engine utilisant la fonctionnalité de réplication de Veeam

Présentation

Auteurs : Suresh Thoppay, NetApp

Les charges de travail de machines virtuelles exécutées sur VMware vSphere peuvent être migrées vers Google Cloud VMware Engine (GCVE) à l'aide de la fonctionnalité de réplication Veeam.

Ce document présente une approche détaillée de la configuration et de la migration de serveurs virtuels qui utilise NetApp Cloud Volume Service, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Dans ce document, vous devez disposer d'un VPN Google Cloud, d'une interconnexion de cloud ou d'une autre option de mise en réseau pour établir une connectivité réseau entre les serveurs vSphere existants et Google Cloud VMware Engine.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document.
> Reportez-vous à la "Documentation Google Cloud" Pour la méthode de connectivité appropriée du stockage sur site vers Google.

Déploiement de la solution de migration

Présentation du déploiement de la solution

1. Assurez-vous que le datastore NFS du service NetApp Cloud Volume est monté sur GCVE vCenter.
2. Assurez-vous que Veeam Backup Recovery est déployé dans l'environnement VMware vSphere existant
3. Créez une tâche de réplication pour lancer la réplication des machines virtuelles vers une instance Google Cloud VMware Engine.
4. Effectuer le basculement de la tâche de réplication Veeam.
5. Effectuez un basculement permanent sur Veeam.

Détails du déploiement

Assurez-vous que le datastore NFS du service NetApp Cloud Volume est monté sur GCVE vCenter

Connectez-vous à GCVE vCenter et assurez-vous que le datastore NFS disposant d'un espace suffisant est disponible.
Si ce n'est pas le cas, veuillez vous reporter à "Montez NetApp CVS en tant que datastore NFS sur GCVE"

Assurez-vous que Veeam Backup Recovery est déployé dans l'environnement VMware vSphere existant

Veuillez vous reporter à "Composants de réplication Veeam" documentation d'installation des composants requis.

Créez une tâche de réplication pour lancer la réplication des machines virtuelles vers une instance Google Cloud VMware Engine.

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere"
Voici une vidéo expliquant comment
"Configurer la tâche de réplication".

> La machine virtuelle de réplica peut avoir une adresse IP différente de la machine virtuelle source et peut également être connectée à différents groupes de ports. Pour plus de détails, consultez la vidéo ci-dessus.

Effectuer le basculement de la tâche de réplication Veeam

Pour migrer des machines virtuelles, effectuez "Effectuer un basculement"

Effectuez un basculement permanent sur Veeam.

Pour traiter GCVE comme votre nouvel environnement source, exécutez "Basculement permanent"

Avantages de cette solution

- L'infrastructure de sauvegarde Veeam existante peut être utilisée pour la migration.
- Veeam Replication permet de modifier les adresses IP de VM sur le site cible.
- Possibilité de remmapper les données existantes répliquées en dehors de Veeam (comme les données répliquées de BlueXP)
- A la capacité de spécifier différents groupes de ports réseau sur le site cible.
- Peut spécifier l'ordre de mise sous tension des machines virtuelles.
- Utilise le suivi des blocs de modifications VMware pour réduire la quantité de données à envoyer sur le réseau WAN.
- Possibilité d'exécuter des scripts pré et post pour la réplication.
- Possibilité d'exécuter des scripts pré et post pour les snapshots.

Disponibilité de région – datastore NFS supplémentaire pour Google Cloud Platform (GCP)

Un datastore NFS supplémentaire pour GCVE est pris en charge avec le service NetApp Cloud Volume.

> Seuls les volumes CVS-Performance peuvent être utilisés pour les datastores GCVE NFS. Pour connaître l'emplacement disponible, reportez-vous à la section "Carte de région globale"

Google Cloud VMware Engine est disponible aux emplacements suivants

Pour minimiser la latence, le volume NetApp CVS et GCVE dans lesquels vous avez l'intention de monter le volume doivent se trouver dans la même zone de disponibilité.
Collaborez avec les architectes de solutions Google et NetApp pour optimiser la disponibilité et le TCO.

Présentation de la sécurité - NetApp Cloud Volumes Service (CVS) dans Google Cloud

Tr-4918 : présentation de la sécurité - NetApp Cloud Volumes Service dans Google Cloud

Oliver Krause, Justin Parisi, NetApp

Étendue du document

La sécurité, notamment dans le cloud où l'infrastructure ne contrôle pas les administrateurs du stockage, est primordiale pour faire confiance aux données des offres de services des fournisseurs cloud. Ce document présente les offres de sécurité de NetApp "Cloud Volumes Service fournit dans Google Cloud".

Public visé

Le public visé par ce document comprend, mais sans s'y limiter, les rôles suivants :

- Fournisseurs de cloud
- Administrateurs du stockage
- Les architectes du stockage
- Ressources sur site
- Décideurs de l'entreprise

Pour toute question sur le contenu de ce rapport technique, consultez la section "« Contactez-nous. »"

Abréviation	Définition
CVS-SW	Cloud Volumes Service, CVS de type de service
CVS-Performance	Cloud volumes Service, CVS-Performance type de service
PSA	

Comment sécuriser vos données avec Cloud Volumes Service dans Google Cloud

Avec Cloud Volumes Service dans Google Cloud, vous pouvez sécuriser vos données de manière native,

Architecture et modèle de colocation sécurisés

Cloud Volumes Service procure une architecture sécurisée dans Google Cloud en segmentant la gestion des services (plan de contrôle) et l'accès aux données (plan de contrôle) entre différents terminaux de sorte qu'ils ne puissent en aucun cas affecter l'autre (voir la section) "« Architecture Cloud Volumes Service »"). Il utilise Google "accès aux services privés" (PSA) pour fournir le service. Cette structure distingue le producteur de services fourni et exploité par NetApp, et le consommateur de services, qui est un cloud privé virtuel (VPC) dans un projet client, en hébergeant les clients souhaitant accéder aux partages de fichiers Cloud Volumes Service.

Dans cette architecture, les locataires (voir la section "« Modèle de colocation »") Sont définis comme des projets Google Cloud complètement isolés les uns des autres, sauf s'ils sont explicitement connectés par l'utilisateur. Les locataires autorisent une isolation complète des volumes de données, des services de noms externes et des autres éléments essentiels de la solution par rapport à d'autres locataires via la plateforme de volumes Cloud Volumes Service. Comme la plateforme Cloud Volumes Service est connectée via le peering

VPC, cette isolation s'applique également à celle-ci. Vous pouvez activer le partage de volumes Cloud Volumes Service entre plusieurs projets à l'aide d'un VPC partagé (voir la section) ""VPC partagés""). Vous pouvez appliquer des contrôles d'accès aux partages SMB et aux exportations NFS pour limiter les personnes ou les données qui peuvent afficher ou modifier les jeux de données.

Forte gestion des identités pour le plan de contrôle

Dans le plan de contrôle où se déroule la configuration Cloud Volumes Service, la gestion des identités est gérée à l'aide de "Gestion des accès aux identités". IAM est un service standard qui vous permet de contrôler l'authentification (connexions) et l'autorisation (autorisations) des instances de projet Google Cloud. Toutes les configurations sont effectuées avec des API Cloud Volumes Service sur un transport HTTPS sécurisé via le cryptage TLS 1.2, et l'authentification est effectuée à l'aide de jetons JWT pour une sécurité accrue. L'interface utilisateur de la console Google pour Cloud Volumes Service convertit les entrées utilisateur en appels de l'API Cloud Volumes Service.

Renforcement de la sécurité - limitation des surfaces d'attaque

Une partie de la sécurité efficace limite le nombre de surfaces d'attaque disponibles dans un service. Les surfaces d'attaque peuvent inclure divers éléments, notamment les données au repos, les transferts à la volée, les connexions et les jeux de données eux-mêmes.

Un service géré supprime certaines des surfaces d'attaque par nature dans sa conception. Gestion de l'infrastructure, comme décrit dans la section ""Fonctionnement de l'entretien"," est gérée par une équipe dédiée et automatisée afin de réduire le nombre d'interventions humaines liées aux configurations, ce qui permet de réduire le nombre d'erreurs intentionnelles et non intentionnelles. La mise en réseau est clôturée de sorte que seuls les services nécessaires peuvent accéder les uns aux autres. Le chiffrement est intégré au stockage des données et seul le plan de données nécessite une attention particulière de la part des administrateurs Cloud Volumes Service. En masquant la majeure partie de la gestion derrière une interface API, la sécurité est obtenue en limitant les surfaces d'attaque.

Modèle « zéro confiance »

Historiquement, la philosophie de sécurité INFORMATIQUE a été de faire confiance mais de vérifier, et se manifeste comme s'appuyant uniquement sur des mécanismes externes (tels que des pare-feu et des systèmes de détection d'intrusion) pour atténuer les menaces. Cependant, les attaques et les violations ont évolué pour contourner la vérification dans les environnements par le biais du phishing, de l'ingénierie sociale, des menaces internes et d'autres méthodes qui permettent de vérifier l'entrée en réseau et de causer des ravages.

La confiance zéro est devenue une nouvelle méthodologie de sécurité, avec le mantra actuel comme « n'avoir confiance en rien tout en vérifiant tout ». Par conséquent, aucun accès n'est autorisé par défaut. Ce mantra est appliqué de diverses façons, notamment les pare-feu standard et les systèmes de détection des intrusions (IDS), ainsi que les méthodes suivantes :

- Méthodes d'authentification fortes (telles que les jetons Kerberos ou JWT chiffrés AES)
- Sources d'identités solides uniques (telles que Windows Active Directory, LDAP (Lightweight Directory Access Protocol) et Google IAM)
- Segmentation réseau et colocation sécurisée (seuls les locataires sont autorisés à accéder par défaut)
- Contrôles d'accès granulaires avec les règles d'accès les moins privilégiées
- Petites listes exclusives d'administrateurs dédiés et fiables avec audit numérique et pistes papier

L'exécution de Cloud Volumes Service dans Google Cloud adhère au modèle « zéro confiance » en mettant en œuvre la politique « confiance en rien et vérification de tout ».

Le cryptage

Chiffrement des données au repos (voir la section "« Chiffrement des données au repos »") En utilisant le chiffrement XTS-AES-256 avec NetApp Volume Encryption (NVE) et en transit avec ""Chiffrement SMB"" Ou NFS Kerberos 5p pris en charge. REST aisément accessible en sachant que les transferts de réplication entre régions sont protégés par le chiffrement TLS 1.2 (voir la section "« Réplication inter-région »"). En outre, Google Networking fournit également des communications cryptées (voir la section ""Chiffrement des données en transit"") pour une couche supplémentaire de protection contre les attaques. Pour plus d'informations sur le chiffrement de transport, reportez-vous à la section "« Réseau Google Cloud »".

Protection des données et sauvegardes

La sécurité ne se limite pas à la prévention des attaques. Il s'agit également de la manière dont nous parvenons à nous remettre des attaques si elles se produisent ou quand elles se produisent. Cette stratégie inclut la protection des données et les sauvegardes. Cloud Volumes Service propose des méthodes de réplication vers d'autres régions en cas de panne (voir la section) "« Réplication inter-région »") ou si un dataset est affecté par une attaque par ransomware. Il peut également effectuer des sauvegardes asynchrones de données vers des emplacements situés en dehors de l'instance Cloud Volumes Service à l'aide de "Sauvegarde Cloud Volumes Service". Grâce aux sauvegardes régulières, la réduction des événements de sécurité peut prendre moins de temps et faire des économies et des problèmes d'administration.

Atténuation rapide des ransomwares grâce aux copies Snapshot leaders du secteur

Outre la protection des données et les sauvegardes, Cloud Volumes Service prend en charge les copies Snapshot immuables (voir la section "« Copies Snapshot immuables »") de volumes qui permettent la restauration suite à des attaques par ransomware (voir la section ""Fonctionnement de l'entretien"") en quelques secondes après la découverte du problème et avec une interruption minimale. Le temps et les effets de la restauration dépendent du calendrier Snapshot. Toutefois, vous pouvez créer des copies Snapshot qui permettent de définir des données modifiées d'une heure ou moins dans le cadre d'attaques par ransomware. Les copies Snapshot ont un impact négligeable sur les performances et l'utilisation de la capacité. Elles constituent une approche à faible risque et à haut rendement pour la protection de vos datasets.

Considérations de sécurité et surfaces d'attaque

Pour comprendre comment sécuriser vos données, il faut d'abord identifier les risques et les surfaces d'attaque potentielles.

Ces mesures comprennent (sans s'y limiter) les éléments suivants :

- Administration et connexions
- Au repos
- Données en cours de vol
- Réseau et pare-feu
- Attaques par ransomware, logiciel malveillant et virus

Comprendre les surfaces d'attaque peut vous aider à mieux sécuriser vos environnements. Cloud Volumes Service dans Google Cloud prend déjà en compte bon nombre de ces sujets et implémente la fonctionnalité de sécurité par défaut, sans aucune interaction administrative.

Assurer des connexions sécurisées

Lors de la sécurisation des composants d'infrastructure critiques, il est impératif de s'assurer que seuls les utilisateurs approuvés peuvent se connecter et gérer vos environnements. Si de mauvais acteurs violent vos informations d'identification administratives, ils ont les clés du château et peuvent faire tout ce qu'ils veulent : changer de configuration, supprimer des volumes et des sauvegardes, créer des backdoors ou désactiver les planifications de snapshots.

Cloud Volumes Service pour Google Cloud protège contre les connexions administratives non autorisées grâce à l'obfuscation du stockage à la demande. Cloud Volumes Service est entièrement géré par le fournisseur cloud, sans qu'il soit possible de se connecter en externe. Toutes les opérations d'installation et de configuration sont entièrement automatisées. De ce fait, un administrateur humain n'a jamais à interagir avec les systèmes, sauf dans de rares circonstances.

Si vous devez vous connecter, Cloud Volumes Service dans Google Cloud sécurise vos connexions en maintenant une liste très courte d'administrateurs de confiance qui ont accès aux systèmes. Ce contrôle d'accès contribue à réduire le nombre de mauvais acteurs potentiels avec accès. De plus, la mise en réseau Google Cloud masque les systèmes derrière des couches de sécurité réseau et expose uniquement ce qui est nécessaire pour le monde extérieur. Pour plus d'informations sur Google Cloud, l'architecture Cloud Volumes Service, consultez la section "« Architecture Cloud Volumes Service »."

Mises à niveau et administration du cluster

Deux domaines présentant des risques de sécurité potentiels incluent l'administration du cluster (que se passe-t-il si un acteur défectueux a accès administrateur) et les mises à niveau (que se passe-t-il si une image logicielle est compromise).

L'administration du stockage

Le stockage fourni à la demande élimine le risque supplémentaire d'exposition des administrateurs en les supprimant pour l'accès aux utilisateurs finaux en dehors du data Center cloud. En effet, la seule configuration effectuée concerne le plan d'accès aux données par les clients. Chaque locataire gère ses propres volumes, et aucun locataire ne peut accéder à d'autres instances Cloud Volumes Service. Le service est géré par l'automatisation, avec une très petite liste d'administrateurs de confiance qui ont accès aux systèmes via les processus décrits dans la section ""Fonctionnement de l'entretien.""

Le type de service CVS-Performance offre une réplication entre régions en tant que possibilité de protéger les données vers une autre région en cas de défaillance d'une région. Dans ce cas, Cloud Volumes Service peut basculer vers une région non affectée pour maintenir l'accès aux données.

Mises à niveau du service

Les mises à jour permettent de protéger les systèmes vulnérables. Chaque mise à jour fournit des améliorations de sécurité et des correctifs de bogues qui réduisent les surfaces d'attaque. Les mises à jour logicielles sont téléchargées à partir de référentiels centralisés et sont validées avant que les mises à jour ne soient autorisées à vérifier que les images officielles sont utilisées et que les mises à niveau ne sont pas compromises par les acteurs défectueux.

Avec Cloud Volumes Service, les mises à jour sont gérées par les équipes des fournisseurs cloud, ce qui élimine les risques pour les équipes d'administration. Les experts maîtrisent la configuration et les mises à niveau de manière automatisée et entièrement testée. Les mises à niveau ne entraînent pas de perturbation et Cloud Volumes Service effectue les mises à jour les plus récentes pour des résultats globaux optimaux.

Pour plus d'informations sur l'équipe d'administration qui effectue ces mises à niveau de service, reportez-vous à la section ""Fonctionnement de l'entretien.""

Sécurisation des données au repos

Le chiffrement des données au repos est important pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque. Les données au repos Cloud Volumes Service sont protégées au moyen du chiffrement logiciel.

- Les clés générées par Google sont utilisées pour CVS-SW.
- Pour CVS-Performance, les clés par volume sont stockées dans un gestionnaire de clés intégré dans Cloud Volumes Service, qui utilise NetApp ONTAP CryptoMod pour générer des clés de cryptage AES-256. CryptoMod figure dans la liste des modules validés CCVP FIPS 140-2. Voir "Certificat no FIPS 140-2-4144".

Depuis novembre 2021, CVS-Performance a mis à disposition une fonctionnalité de chiffrement géré par le client (CMEK). Cette fonctionnalité vous permet de chiffrer les clés par volume avec des clés principales par projet et par région hébergées dans Google Key Management Service (KMS). LES KILOMÈTRES vous permettent d'associer des gestionnaires de clés externes.

Pour plus d'informations sur la configuration de KMS pour CVS-Performance, "Consultez la documentation Cloud Volumes Service".

Pour plus d'informations sur l'architecture, voir la section "« Architecture Cloud Volumes Service »."

Sécurisation des données à la volée

En plus de sécuriser les données au repos, vous devez également être à même de sécuriser les données lorsqu'elles sont en transit entre l'instance Cloud Volumes Service et un client ou une cible de réplication. Cloud Volumes Service permet le chiffrement des données à la volée sur les protocoles NAS à l'aide de méthodes de chiffrement, telles que le chiffrement SMB via Kerberos, la signature/chiffrement des paquets et NFS Kerberos 5p pour le chiffrement complet des transferts de données.

La réplication des volumes Cloud Volumes Service utilise le protocole TLS 1.2, qui tire parti des méthodes de chiffrement AES-GCM.

La plupart des protocoles en vol non sécurisés tels que telnet, NDMP, etc. Sont désactivés par défaut. Toutefois, le DNS n'est pas chiffré par Cloud Volumes Service (pas de prise en charge de DNS sec) et doit être chiffré en utilisant le cryptage réseau externe lorsque cela est possible. Voir la section ""Chiffrement des données en transit"" pour en savoir plus sur la sécurisation des données à la volée.

Pour plus d'informations sur le cryptage du protocole NAS, reportez-vous à la section "« Protocoles NAS »."

Utilisateurs et groupes pour les autorisations NAS

Une partie de la sécurisation de vos données dans le cloud implique une authentification adéquate des utilisateurs et des groupes, où les utilisateurs accédant aux données sont vérifiés en tant qu'utilisateurs réels dans l'environnement et où les groupes contiennent des utilisateurs valides. Ces utilisateurs et groupes offrent un accès initial au partage et à l'exportation, ainsi qu'une validation des autorisations pour les fichiers et dossiers du système de stockage.

Cloud Volumes Service utilise l'authentification standard d'utilisateur et de groupe Windows basée sur Active Directory pour les partages SMB et les autorisations de style Windows. Le service peut également tirer parti de fournisseurs d'identités UNIX tels que le LDAP pour les utilisateurs et groupes UNIX pour les exportations NFS, la validation des ID NFSv4, l'authentification Kerberos et les ACL NFSv4.

Actuellement, seul Active Directory LDAP est pris en charge avec la fonctionnalité Cloud Volumes Service pour LDAP.

La détection, la prévention et la réduction des ransomwares, des malwares et des virus

Les ransomwares, les malwares et les virus sont une menace persistante pour les administrateurs, et la détection, la prévention et la réduction de ces menaces sont toujours une priorité absolue pour les entreprises. En cas d'attaque par ransomware d'un jeu de données stratégique, vous pouvez coûter plusieurs millions de dollars. Il est donc préférable de faire ce que vous pouvez minimiser ce risque.

Bien que Cloud Volumes Service n'inclut actuellement pas de mesures de détection ou de prévention natives, telles que la protection antivirus ou "détection automatique des ransomwares", Il existe des moyens de récupérer rapidement après un événement ransomware en activant des planifications Snapshot régulières. Les copies Snapshot sont immuables et les pointeurs en lecture seule vers les blocs modifiés dans le système de fichiers sont quasi instantanés, ont un impact minimal sur les performances et utilisent uniquement de l'espace lorsque les données sont modifiées ou supprimées. Vous pouvez définir des calendriers pour les copies Snapshot en fonction de l'objectif de point de récupération (RPO)/objectif de durée de restauration (RTO) souhaité. Vous pouvez également conserver jusqu'à 1,024 copies Snapshot par volume.

La prise en charge des snapshots est incluse sans frais supplémentaires (en plus des frais de stockage de données pour les blocs/données modifiés conservés par les copies Snapshot) avec Cloud Volumes Service et, en cas d'attaque par ransomware, elle peut être utilisée pour restaurer la copie Snapshot avant l'attaque. Les restaurations Snapshot ne prennent que quelques secondes et vous permettent ensuite de rétablir le service des données normal. Pour plus d'informations, voir "Solution NetApp pour ransomware".

Pour empêcher les ransomwares d'affecter votre activité, vous devez adopter une approche à plusieurs couches :

- Protection des terminaux
- Protection contre les menaces externes grâce à des pare-feu réseau
- Détection des anomalies de données
- Plusieurs sauvegardes (sur site et hors site) de jeux de données stratégiques
- Tests réguliers de restauration des sauvegardes
- Copies Snapshot NetApp immuables en lecture seule
- Authentification multifacteur pour les infrastructures stratégiques
- Audits de sécurité des connexions système

Cette liste est loin d'être exhaustive, mais elle constitue un bon plan à suivre pour gérer le potentiel d'attaques par ransomware. Cloud Volumes Service dans Google Cloud fournit plusieurs façons de vous protéger contre les événements par ransomware et de réduire leurs effets.

Copies Snapshot immuables

Cloud Volumes Service fournit de manière native des copies Snapshot immuables en lecture seule, qui sont mises en œuvre dans un calendrier personnalisable pour une restauration instantanée rapide en cas de suppression de données ou si un volume entier a été victime d'une attaque par ransomware. Les restaurations Snapshot vers les précédentes copies Snapshot sont rapides et limitent la perte de données en fonction de la période de conservation de vos planifications Snapshot et des objectifs RTO/RPO. L'impact de la technologie Snapshot sur les performances est négligeable.

Étant donné que les copies Snapshot dans Cloud Volumes Service sont en lecture seule, elles ne peuvent pas

être infectées par un ransomware à moins que ces dernières aient proliféré dans le dataset inaperçu et que les copies Snapshot ont été prises en compte par les données infectées par un ransomware. C'est pourquoi vous devez également envisager la détection par ransomware basée sur les anomalies de données. Cloud Volumes Service n'offre pas actuellement de fonction de détection native, mais vous pouvez utiliser un logiciel de surveillance externe.

Les sauvegardes et les restaurations

Cloud Volumes Service fournit des fonctionnalités standard de sauvegarde client NAS (sauvegardes sur NFS ou SMB).

- CVS-Performance offre une réplication de volume entre régions vers d'autres volumes CVS-Performance. Pour plus d'informations, voir "réplication de volume" Dans la documentation Cloud Volumes Service.
- CVS-SW offre des fonctionnalités de sauvegarde/restauration de volume natives des services. Pour plus d'informations, voir "la sauvegarde dans le cloud" Dans la documentation Cloud Volumes Service.

La réplication de volume fournit une copie exacte du volume source pour un basculement rapide en cas d'incident, y compris en cas d'attaque par ransomware.

Réplication entre les régions

CVS-Performance vous permet de répliquer en toute sécurité des volumes entre les régions Google Cloud pour la protection des données et les archives à l'aide du chiffrement TLS1.2 AES 256 GCM sur un réseau de service back-end contrôlé par NetApp à l'aide d'interfaces spécifiques utilisées pour la réplication sur le réseau Google. Un volume primaire (source) contient les données de production actives et effectue une réplication vers un volume secondaire (destination) afin de fournir une réplique exacte du jeu de données primaire.

La réplication initiale transfère tous les blocs, mais les mises à jour ne transmettent que les blocs modifiés dans un volume primaire. Par exemple, si une base de données de 1 To résidant sur un volume primaire est répliquée sur le volume secondaire, alors 1 To d'espace est transféré sur la réplication initiale. Si cette base de données a quelques centaines de lignes (hypothetiquement, quelques Mo) qui changent entre l'initialisation et la mise à jour suivante, seuls les blocs avec les lignes modifiées sont répliqués sur le secondaire (quelques Mo). Cela permet de s'assurer que les temps de transfert restent faibles et de limiter les coûts de réplication.

Toutes les autorisations des fichiers et dossiers sont répliquées sur le volume secondaire, mais les autorisations d'accès au partage (telles que les export-policies et les règles ou les partages SMB et les ACL de partage) doivent être gérées de manière indépendante. Dans le cas d'un basculement de site, le site de destination doit utiliser les mêmes services de nom et les mêmes connexions de domaine Active Directory pour assurer un traitement cohérent des identités et autorisations des utilisateurs et des groupes. En cas d'incident, il est possible d'utiliser un volume secondaire comme cible de basculement afin de briser la relation de réplication, qui convertit le volume secondaire en lecture/écriture.

Les répliques de volumes sont en lecture seule, ce qui permet d'obtenir une copie inaltérable des données hors site pour une restauration rapide des données lorsqu'un virus a infecté des données ou où un ransomware a chiffré le jeu de données principal. Les données en lecture seule ne sont pas cryptées, mais, en cas de volume primaire affecté et de réplication, les blocs infectés sont également répliqués. Vous pouvez utiliser des copies Snapshot plus anciennes et non affectées pour effectuer une restauration, mais les SLA peuvent tomber dans la plage des RTO/RPO promis en fonction de la rapidité de détection d'une attaque.

De plus, vous pouvez empêcher les actions administratives malveillantes, telles que les suppressions de volumes, les suppressions de snapshots ou les modifications de planifications de snapshots, dans le cadre de la gestion de la réplication multi-région (CRR) dans Google Cloud. Pour ce faire, des rôles personnalisés séparent les administrateurs de volumes, qui peuvent supprimer des volumes source sans interrompre les miroirs et ne peuvent donc pas supprimer des volumes de destination des administrateurs CRR, qui ne

peuvent pas effectuer d'opérations de volume. Voir "Considérations de sécurité" Dans la documentation Cloud Volumes Service pour les autorisations autorisées par chaque groupe d'administrateurs.

Sauvegarde Cloud Volumes Service

Bien que Cloud Volumes Service assure une durabilité élevée des données, les événements externes peuvent entraîner des pertes de données. En cas d'incident de sécurité tel qu'un virus ou un ransomware, les sauvegardes et les restaurations sont essentielles pour la reprise de l'accès aux données en temps opportun. Un administrateur peut accidentellement supprimer un volume Cloud Volumes Service. Ou il suffit aux utilisateurs de conserver les versions de sauvegarde de leurs données pendant plusieurs mois et de conserver l'espace supplémentaire de copie Snapshot dans le volume peut représenter un défi de coût. Même si les copies Snapshot doivent être le moyen le plus conseillé de conserver les versions de sauvegarde pendant les dernières semaines pour restaurer les données perdues, elles se trouvent à l'intérieur du volume et sont perdues en cas de perte du volume.

Pour toutes ces raisons, NetApp Cloud Volumes Service propose des services de sauvegarde par l'intermédiaire de "Sauvegarde Cloud Volumes Service".

La sauvegarde Cloud Volumes Service génère une copie du volume sur Google Cloud Storage (GCS). Il sauvegarde uniquement les données réelles stockées au sein du volume, et non l'espace libre. Cela fonctionne comme une opération incrémentielle à l'infini. Cela signifie qu'il transfère le contenu du volume une fois et depuis là, il continue de sauvegarder les données modifiées uniquement. Comparé aux concepts de sauvegarde classiques à plusieurs sauvegardes complètes, elle permet d'économiser une grande quantité de stockage de sauvegarde, ce qui réduit les coûts. Le prix mensuel de l'espace de sauvegarde est inférieur à celui d'un volume. C'est l'endroit idéal pour conserver les versions de sauvegarde plus longtemps.

Les utilisateurs peuvent utiliser une sauvegarde Cloud Volumes Service pour restaurer toute version de sauvegarde sur un volume identique ou différent dans la même région. Si le volume source est supprimé, les données de sauvegarde sont conservées et doivent être gérées indépendamment (par exemple, supprimées).

Cloud Volumes Service Backup est intégré à Cloud Volumes Service en option. Les utilisateurs peuvent décider des volumes à protéger en activant la sauvegarde Cloud Volumes Service sur la base de chaque volume. Voir la "Documentation de sauvegarde Cloud Volumes Service" pour plus d'informations sur les sauvegardes, le "nombre maximal de versions de sauvegarde prises en charge", planification, et "tarifs".

Toutes les données de sauvegarde d'un projet sont stockées dans un compartiment GCS, géré par le service et non visible par l'utilisateur. Chaque projet utilise un compartiment différent. Actuellement, les compartiments se trouvent dans la même région que les volumes Cloud Volumes Service, mais davantage d'options sont présentées. Consultez la documentation pour connaître l'état le plus récent.

Le transport des données d'un compartiment Cloud Volumes Service vers GCS utilise des réseaux Google internes et externes avec HTTPS et TLS1.2. Les données sont chiffrées au repos à l'aide de clés gérées par Google.

Pour gérer la sauvegarde Cloud Volumes Service (création, suppression et restauration de sauvegardes), un utilisateur doit disposer du "roles/netappdevolumes.admin" rôle.

Architecture

Présentation

L'architecture et la sécurité font partie des processus de confiance aux solutions cloud. Cette section décrit différents aspects de l'architecture Cloud Volumes Service de Google qui contribuent à réduire les risques de sécurisation des données et indique les domaines

dans lesquels des étapes de configuration supplémentaires peuvent être nécessaires pour obtenir le déploiement le plus sécurisé.

L'architecture générale d'Cloud Volumes Service peut être décomposée en deux composants principaux : le plan de contrôle et le plan de données.

Plan de contrôle

Le plan de contrôle d'Cloud Volumes Service est l'infrastructure back-end gérée par les administrateurs Cloud Volumes Service et le logiciel d'automatisation natif de NetApp. Ce plan est totalement transparent pour les utilisateurs finaux. Il inclut des fonctionnalités de mise en réseau, du matériel de stockage, des mises à jour logicielles, etc. Pour que les solutions hébergées dans le cloud telles que Cloud Volumes Service puissent apporter de la valeur ajoutée.

Plan de données

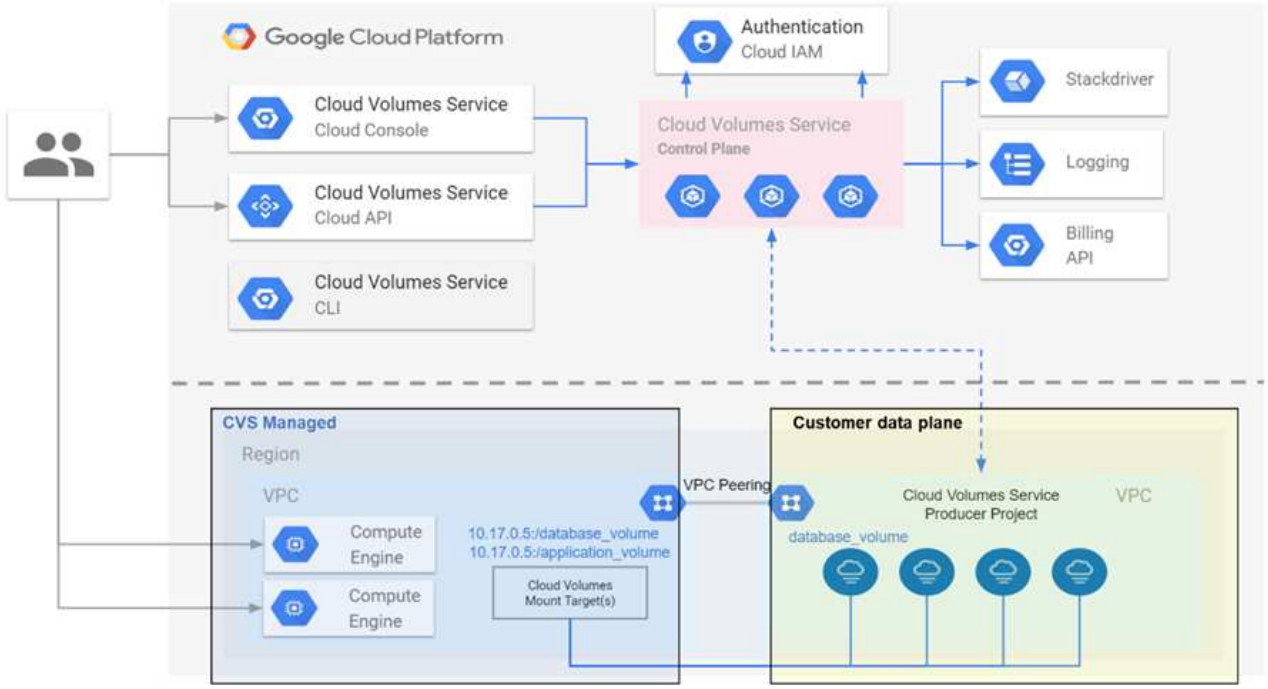
Le plan de données de Cloud Volumes Service inclut les volumes de données réels et la configuration Cloud Volumes Service globale (contrôle d'accès, authentification Kerberos, etc.). Le plan de données est entièrement sous le contrôle des utilisateurs finaux et des consommateurs de la plateforme Cloud Volumes Service.

La façon dont chaque plan est sécurisé et géré est différente. Ces différences sont en commençant par la présentation de l'architecture Cloud Volumes Service.

Architecture Cloud Volumes Service

De la même manière que d'autres services Google Cloud natifs, tels que CloudSQL, Google Cloud VMware Engine (GCVE) et filestore, utilise Cloud Volumes Service "Google PSA" pour fournir le service. Dans PSA, les services sont intégrés à un projet de producteur de services, qui utilise "Peering de réseau VPC" pour se connecter au consommateur de services. Le producteur de service est fourni et exploité par NetApp, et le consommateur du service est un VPC dans un projet client qui héberge les clients souhaitant accéder aux partages de fichiers Cloud Volumes Service.

La figure suivante, référencée à partir du "section architecture" De la documentation Cloud Volumes Service, affiche une vue générale.



La partie au-dessus de la ligne pointillée montre le plan de contrôle du service, qui contrôle le cycle de vie du volume. La partie sous la ligne pointillée montre le plan de données. La zone bleue gauche représente le VPC (Service Consumer) de l'utilisateur, la zone bleue droite est le producteur de services fourni par NetApp. Les deux sont connectés via le peering VPC.

Modèle de location

Dans Cloud Volumes Service, chaque projet est considéré comme un locataire unique. Cela signifie que la manipulation des volumes et des copies Snapshot, etc., est effectuée sur la base de chaque projet. En d'autres termes, tous les volumes sont détenus par le projet dans lequel ils ont été créés, et seul ce projet peut gérer et accéder aux données qui leur sont propres par défaut. Cette vue est considérée comme le plan de contrôle du service.

VPC partagés

Dans la vue du plan de données, Cloud Volumes Service peut se connecter à un VPC partagé. Vous pouvez créer des volumes dans le projet d'hébergement ou dans l'un des projets de service connectés au VPC partagé. Tous les projets (hôte ou service) connectés à ce VPC partagé peuvent atteindre les volumes au niveau de la couche réseau (TCP/IP). Étant donné que tous les clients disposant d'une connectivité réseau sur le VPC partagé peuvent accéder aux données via les protocoles NAS, vous devez utiliser le contrôle d'accès sur chacun des volumes (listes de contrôle d'accès (ACL) d'utilisateur/de groupe, ainsi que les noms d'hôte/adresses IP pour les exportations NFS) pour contrôler qui peut accéder aux données.

Vous pouvez connecter Cloud Volumes Service à cinq VPC maximum par projet client. Sur le plan de contrôle, le projet vous permet de gérer tous les volumes créés, quel que soit le VPC auquel ils sont connectés. Sur le plan de données, les VPC sont isolés les uns des autres et chaque volume ne peut être connecté qu'à un VPC.

L'accès aux volumes individuels est contrôlé par des mécanismes de contrôle d'accès spécifiques à un protocole (NFS/SMB).

En d'autres termes, sur la couche réseau, tous les projets connectés au VPC partagé peuvent voir le volume,

tandis que, du point de vue de la gestion, le plan de contrôle ne permet au projet propriétaire de voir le volume que.

Contrôles du service VPC

Les contrôles du service VPC établissent un périmètre de contrôle d'accès autour des services Google Cloud reliés à Internet et accessibles dans le monde entier. Ces services permettent le contrôle d'accès par le biais d'identités utilisateur, mais ne peuvent pas limiter les demandes d'emplacement réseau. Les contrôles de service VPC comblent ce fossé en introduisant des capacités permettant de limiter l'accès aux réseaux définis.

Le plan de données Cloud Volumes Service n'est pas connecté à Internet externe mais à des VPC privés avec des limites de réseau bien définies (périmètres). Sur ce réseau, chaque volume utilise un contrôle d'accès spécifique au protocole. Toute connectivité réseau externe est créée de manière explicite par les administrateurs de projet Google Cloud. Le plan de contrôle, cependant, n'offre pas les mêmes protections que le plan de données et peut être accessible par n'importe qui à partir de n'importe où avec des informations d'identification valides ("Jetons JWT").

En bref, le plan de données Cloud Volumes Service offre la possibilité de contrôler l'accès au réseau sans devoir prendre en charge les contrôles de service VPC et n'utilise pas explicitement les contrôles de service VPC.

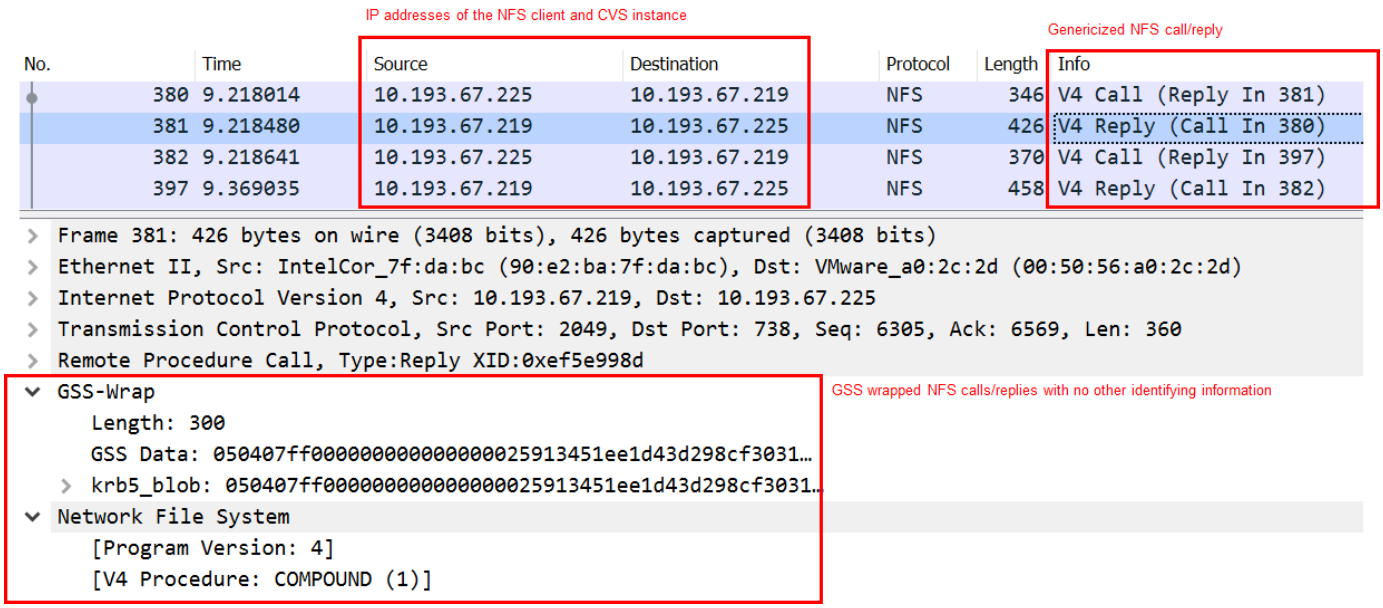
Considérations relatives à la détection et à la détection des paquets

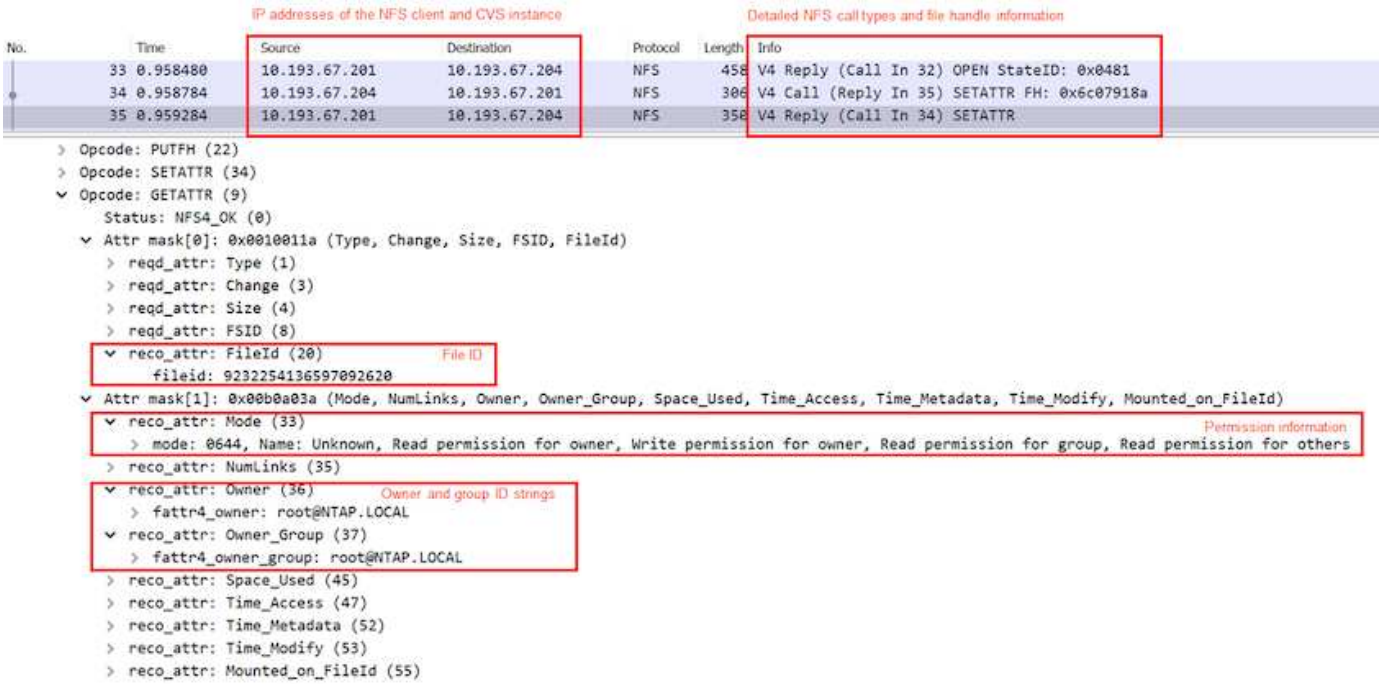
Les captures de paquets peuvent être utiles pour résoudre des problèmes réseau ou d'autres problèmes (autorisations NAS, connectivité LDAP, etc.), mais peuvent également être utilisées de manière malveillante pour obtenir des informations sur les adresses IP réseau, les adresses MAC, les noms d'utilisateurs et de groupes, ainsi que le niveau de sécurité utilisé sur les noeuds finaux. En raison de la configuration de la mise en réseau Google Cloud, des VPC et des règles de pare-feu, l'accès non autorisé aux paquets réseau devrait être difficile à obtenir sans identifiants de connexion utilisateur ou "Jetons JWT" dans les instances cloud. Les captures de paquets ne sont possibles que sur les terminaux (tels que les machines virtuelles) et uniquement sur les terminaux internes au VPC, à moins qu'un VPC partagé et/ou un tunnel/IP de réseau externe ne soit utilisé pour permettre explicitement le trafic externe vers les terminaux. Il n'y a pas de moyen de sniff trafic en dehors des clients.

Lorsque des VPC partagés sont utilisés, le chiffrement à la volée avec NFS Kerberos et/ou "Chiffrement SMB" peut masquer une grande partie des informations tirées de traces. Cependant, un certain trafic est encore envoyé en texte clair, par exemple "DNS" et "Requêtes LDAP". La figure suivante montre une capture de paquet à partir d'une requête LDAP en texte clair provenant de Cloud Volumes Service et les informations d'identification potentielles qui sont exposées. Les requêtes LDAP dans Cloud Volumes Service ne prennent actuellement pas en charge le cryptage ou LDAP sur SSL. CVS-Performance prend en charge la signature LDAP, si Active Directory en fait la demande. CVS-SW ne prend pas en charge la signature LDAP.

UnixUserPassword est interrogé par LDAP et n'est pas envoyé en texte clair, mais plutôt dans un hash salé. Par défaut, Windows LDAP ne renseigne pas les champs unixUserPassword. Ce champ est uniquement obligatoire si vous devez utiliser Windows LDAP pour les connexions interactives via LDAP aux clients. Cloud Volumes Service ne prend pas en charge les connexions LDAP interactives vers les instances.

La figure suivante montre une capture de paquets d'une conversation Kerberos NFS à côté d'une capture de NFS sur AUTH_SYS. Notez que les informations disponibles dans une trace diffèrent entre les deux et que l'activation du cryptage à la volée offre une sécurité globale accrue pour le trafic NAS.





Interfaces réseau des VM

Une astuce peut tenter d'ajouter une nouvelle carte d'interface réseau (NIC) à une machine virtuelle dans "mode promiscueux" (Mise en miroir des ports) ou activez le mode promiscuous sur une carte réseau existante afin de sniiser tout le trafic. Dans Google Cloud, l'ajout d'une nouvelle carte réseau nécessite l'arrêt complet d'une machine virtuelle, ce qui génère des alertes, ce qui rend les pirates informatiques inaperçus.

De plus, les cartes réseau ne peuvent pas être configurées en mode promiscuous et déclencheront des alertes dans Google Cloud.

Architecture du plan de contrôle

Toutes les actions de gestion vers Cloud Volumes Service sont effectuées par l'intermédiaire d'une API. La gestion Cloud Volumes Service intégrée à la console GCP Cloud utilise également l'API Cloud Volumes Service.

Gestion des identités et des accès

Gestion des identités et des accès ("IAM") Est un service standard qui vous permet de contrôler l'authentification (connexions) et l'autorisation (autorisations) des instances de projet Google Cloud. Google IAM fournit une piste d'audit complète des autorisations et des suppressions. Actuellement, Cloud Volumes Service ne fournit pas d'audit du plan de contrôle.

Présentation de l'autorisation/autorisation

IAM propose des autorisations granulaires intégrées pour Cloud Volumes Service. Vous pouvez trouver un "liste complète des autorisations granulaires ici".

IAM propose également deux rôles prédéfinis appelés `netappcloudvolumes.admin` et `netappcloudvolumes.viewer`. Ces rôles peuvent être attribués à des utilisateurs ou à des comptes de service spécifiques.

Attribuez les rôles et les autorisations appropriés pour permettre aux utilisateurs IAM de gérer Cloud Volumes

Service.

Voici quelques exemples d'utilisation d'autorisations granulaires :

- Créez un rôle personnalisé avec uniquement les autorisations obtenir/liste/créer/mettre à jour pour que les utilisateurs ne puissent pas supprimer de volumes.
- Utilisez un rôle personnalisé avec uniquement `snapshot.*` Autorisations permettant de créer un compte de service utilisé pour créer une intégration Snapshot cohérente avec les applications.
- Définissez un rôle personnalisé à déléguer `volumereplication.*` pour des utilisateurs spécifiques.

Comptes de service

Pour passer des appels API Cloud Volumes Service par le biais de scripts ou "Terraform", vous devez créer un compte de service avec `roles/netappcloudvolumes.admin` rôle. Vous pouvez utiliser ce compte de service pour générer les jetons JWT requis pour authentifier les requêtes API Cloud Volumes Service de deux manières différentes :

- Générez une clé JSON et utilisez les API Google pour dériver un jeton JWT. C'est l'approche la plus simple, mais elle implique une gestion manuelle des secrets (clé JSON).
- Utiliser "Emprunt d'identité du compte de service" avec `roles/iam.serviceAccountTokenCreator`. Le code (script, Terraform, etc.) s'exécute avec "Informations d'identification par défaut de l'application" et emprunt de l'identité du compte de service pour obtenir ses autorisations. Cette approche reflète les bonnes pratiques de sécurité de Google.

Voir "Création de votre compte de service et de votre clé privée" Dans la documentation Google Cloud pour plus d'informations.

API Cloud Volumes Service

L'API Cloud Volumes Service utilise une API REST en utilisant HTTPS (TLSv1.2) comme transport réseau sous-jacent. Vous trouverez la définition d'API la plus récente "ici" Et des informations sur l'utilisation de l'API à l'adresse "API Cloud volumes dans la documentation Google Cloud".

Le terminal API est exploité et sécurisé par NetApp à l'aide de la fonctionnalité HTTPS standard (TLSv1.2).

Jetons JWT

L'authentification à l'API est effectuée avec des jetons de support JWT ("RFC-7519"). Les jetons JWT valides doivent être obtenus via l'authentification Google Cloud IAM. Pour ce faire, il faut récupérer un jeton depuis IAM en fournissant une clé JSON de compte de service.

Consignation des audits

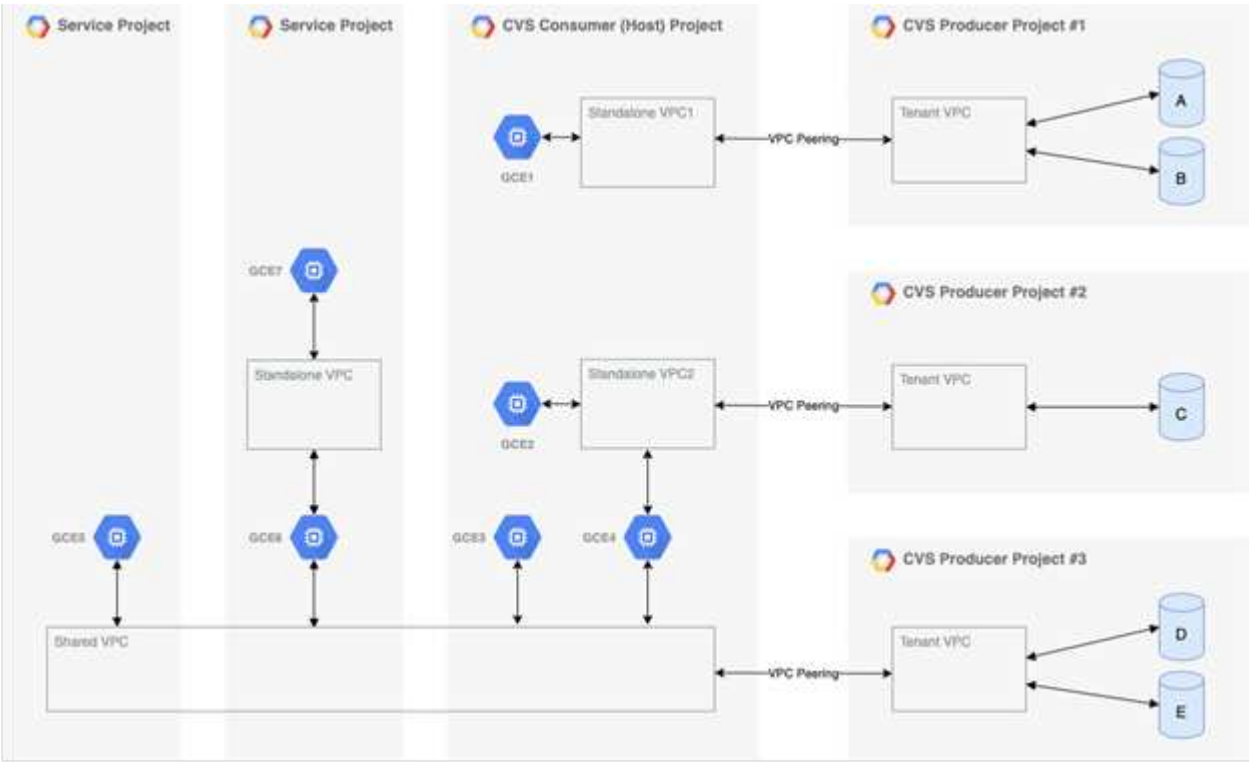
Aucun journal d'audit du plan de contrôle accessible par l'utilisateur n'est actuellement disponible.

Architecture de plan de données

Cloud Volumes Service pour Google Cloud s'appuie sur Google Cloud "accès aux services privés" structure. Dans ce cadre, les utilisateurs peuvent se connecter à Cloud Volumes Service. Cette structure utilise des services de mise en réseau et des constructions de peering de VPC comme d'autres services Google Cloud, qui assurent une isolation complète entre les locataires.

Pour obtenir une présentation de l'architecture de Cloud Volumes Service pour Google Cloud, rendez-vous sur "Architecture pour Cloud Volumes Service".

Les VPC utilisateur (autonomes ou partagés) sont associés à des VPC au sein de projets de locataires gérés Cloud Volumes Service, qui hébergent les volumes.



La figure précédente montre un projet (projet CVS de milieu de gamme) avec trois réseaux VPC connectés à Cloud Volumes Service et plusieurs VM de moteur de calcul (GCE1-7) partageant des volumes :

- VPC1 permet à GCE1 d'accéder aux volumes A et B.
- Le VPC2 permet aux GCE2 et GCE4 d'accéder au volume C.
- Le troisième réseau VPC est un VPC partagé, partagé avec deux projets de service. Il permet aux GCE3, GCE4, GCE5 et GCE6 d'accéder aux volumes D et E. Les réseaux VPC partagés ne sont pris en charge que pour les volumes du type de service CVS-Performance.

Le GCE7 ne peut accéder à aucun volume.

Les données peuvent être chiffrées à la fois en transit (par le chiffrement Kerberos et/ou SMB) et au repos dans Cloud Volumes Service.

Chiffrement des données en transit

Les données en transit peuvent être chiffrées au niveau de la couche de protocole NAS et le réseau Google Cloud lui-même est chiffré, comme décrit dans les sections suivantes.

Réseau Google Cloud

Google Cloud chiffre le trafic au niveau du réseau comme décrit à la section "Chiffrement en transit" Dans la

documentation Google. Comme indiqué dans la section « architecture de services Cloud volumes », Cloud Volumes Service est fourni à partir d'un projet de production PSA contrôlé par NetApp.

Dans le cas de CVS-SW, le locataire exécute les machines virtuelles Google pour fournir le service. Le trafic entre les VM utilisateur et les machines virtuelles Cloud Volumes Service est automatiquement chiffré par Google.

Bien que le chemin d'accès aux données de CVS-Performance ne soit pas intégralement chiffré sur la couche réseau, NetApp et Google utilisent une combinaison "De cryptage IEEE 802.1AE (MACSec)", "encapsulation" (Chiffrement des données) et des réseaux physiquement restreints pour protéger les données en transit entre le type de service Cloud Volumes Service CVS-Performance et Google Cloud.

Protocoles NAS

Les protocoles NAS NFS et SMB fournissent un chiffrement de transport en option au niveau de la couche de protocoles.

Chiffrement SMB

"Chiffrement SMB" Offre un cryptage de bout en bout des données SMB et protège les données contre les occurrences de réseaux non fiables. Vous pouvez activer le cryptage à la fois pour la connexion de données client/serveur (uniquement disponible pour les clients compatibles SMB3.x) et pour l'authentification du contrôleur serveur/domaine.

Lorsque le cryptage SMB est activé, les clients qui ne prennent pas en charge le cryptage ne peuvent pas accéder au partage.

Cloud Volumes Service prend en charge le chiffrement de sécurité RC4-HMAC, AES-128-CTS-HMAC-SHA1 et AES-256-CTS-HMAC-SHA1 pour le cryptage SMB. SMB négocie le type de cryptage le plus élevé pris en charge par le serveur.

Kerberos NFSv4.1

Pour NFSv4.1, CVS-Performance propose l'authentification Kerberos, comme décrit dans "RFC7530". Vous pouvez activer Kerberos par volume.

Le type de chiffrement le plus puissant actuellement disponible pour Kerberos est AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service prend en charge AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 et DES pour NFS. Il prend également en charge ARCFOUR-HMAC (RC4) pour le trafic CIFS/SMB, mais pas pour NFS.

Kerberos propose trois niveaux de sécurité différents pour les montages NFS qui offrent des options de sécurité Kerberos.

Selon RedHat "Options de montage courantes" documentation :

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

En règle générale, plus le niveau de sécurité Kerberos est important, plus les performances sont faibles, car le client et le serveur passent du temps à chiffrer et déchiffrer les opérations NFS pour chaque paquet envoyé. De nombreux clients et serveurs NFS prennent en charge le transfert AES-ni vers les processeurs pour une meilleure expérience globale. Cependant, l'impact sur les performances de Kerberos 5p (chiffrement complet de bout en bout) est considérablement plus important que l'impact de Kerberos 5 (authentification utilisateur).

Le tableau ci-dessous présente les différences par rapport à chaque niveau pour la sécurité et les performances.

Niveau de sécurité	Sécurité	Performance
NFSv3 : sys	• Moins sécurisé ; texte brut avec ID utilisateur numérique/ID de groupe • Possibilité d'afficher les UID, GID, adresses IP client, chemins d'exportation, noms de fichiers, autorisations dans les captures de paquets	• Idéal pour la plupart des cas
NFSv4.x — sys	• Plus sûr que NFSv3 (ID client, correspondance de chaîne de nom/chaîne de domaine) mais texte brut • Possibilité d'afficher les UID, GID, adresses IP des clients, chaînes de noms, ID de domaine, chemins d'exportation, noms de fichiers, autorisations dans les captures de paquets	• Adapté aux charges de travail séquentielles (VM, bases de données, fichiers volumineux) • Erreurs avec un nombre élevé de fichiers/métadonnées élevées (30 à 50 % en moins)

Niveau de sécurité	Sécurité	Performance
NFS - krb5	• Le chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS — enveloppe l'UID/GID des utilisateurs/groupes dans les appels RPC dans l'encapsuleur GSS • L'utilisateur qui demande l'accès au montage a besoin d'un ticket Kerberos valide (via nom d'utilisateur/mot de passe ou par échange manuel de clés) ; le ticket expire après une période spécifiée et l'utilisateur doit de nouveau s'authentifier pour l'accès • Aucun chiffrement pour les opérations NFS ou les protocoles annexes tels que mount/portmapper/nlm (peut voir les chemins d'exportation, les adresses IP, les pointeurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets)	• Le meilleur dans la plupart des cas pour Kerberos ; pire que AUTH_SYS

Niveau de sécurité	Sécurité	Performance
NFS - krb5i	• Le chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS — enveloppe l'UID/GID des utilisateurs/groupes dans les appels RPC dans l'encapsuleur GSS • L'utilisateur qui demande l'accès au montage doit disposer d'un ticket Kerberos valide (via nom d'utilisateur/mot de passe ou échange manuel par onglet) ; le ticket expire après une période spécifiée et l'utilisateur doit de nouveau s'authentifier pour l'accès • Aucun chiffrement pour les opérations NFS ou les protocoles annexes tels que mount/portmapper/nlm (peut voir les chemins d'exportation, les adresses IP, les pointeurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets) • La somme de contrôle GSS Kerberos est ajoutée à chaque paquet pour garantir que rien n'intercepte les paquets. Si les checksums correspondent, la conversation est autorisée.	• Supérieur à krb5p parce que la charge NFS n'est pas chiffrée. Seule la surcharge supplémentaire par rapport à krb5 est la somme de contrôle d'intégrité. Les performances de krb5i ne seront pas beaucoup plus mauvais que krb5, mais il y aura une certaine dégradation.

Niveau de sécurité	Sécurité	Performance
NFS – krb5p	• Le chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS — enveloppe l'UID/GID des utilisateurs/groupes dans les appels RPC dans l'encapsuleur GSS • L'utilisateur qui demande l'accès au montage doit disposer d'un ticket Kerberos valide (via nom d'utilisateur/mot de passe ou échange manuel de clavier) ; le ticket expire après la période spécifiée et l'utilisateur doit de nouveau s'authentifier pour l'accès • Tous les payload de paquets NFS sont cryptés avec l'encapsuleur GSS (ne peut pas voir les descripteurs de fichier, les autorisations, les noms de fichier, atime/mtime dans les captures de paquets). • Inclut le contrôle d'intégrité. • Le type d'opération NFS est visible (FSINFO, ACCESS, GETATTR, etc.). • Les protocoles auxiliaires (montage, portmap, nlm, etc.) ne sont pas cryptés (voir chemins d'exportation, adresses IP)	• Performances les plus faibles des niveaux de sécurité ; la krb5p doit chiffrer/décrypter plus. • Performances supérieures à celles du krb5p avec NFSv4.x pour les workloads avec un nombre élevé de fichiers.

Dans Cloud Volumes Service, un serveur Active Directory configuré est utilisé comme serveur Kerberos et serveur LDAP (pour rechercher les identités d'utilisateur à partir d'un schéma compatible RFC2307). Aucun autre serveur Kerberos ou LDAP n'est pris en charge. NetApp vous recommande vivement d'utiliser le protocole LDAP pour la gestion des identités dans Cloud Volumes Service. Pour plus d'informations sur l'affichage de Kerberos sur NFS dans les captures de paquets, reportez-vous à la section ""Considérations sur la capture et la détection des paquets.""

Chiffrement des données au repos

Tous les volumes Cloud Volumes Service sont chiffrés au repos à l'aide du chiffrement AES-256, qui signifie que toutes les données utilisateur écrites sur le support sont chiffrées et ne peuvent être déchiffrées qu'à l'aide d'une clé par volume.

- Pour CVS-SW, des clés générées par Google sont utilisées.
- Pour CVS-Performance, les clés par volume sont stockées dans un gestionnaire de clés intégré dans

Cloud Volumes Service.

Depuis novembre 2021, un aperçu des fonctionnalités de clés de chiffrement gérées par les clients (CMEK) a été disponible. Vous pouvez ainsi chiffrer les clés par volume avec une clé principale par projet et par région hébergée dans "Google Key Management Service (KMS)." LES KILOMÈTRES vous permettent d'associer des gestionnaires de clés externes.

Pour plus d'informations sur la configuration de KMS pour CVS-Performance, reportez-vous à la section "La configuration des clés de chiffrement gérées par le client".

Pare-feu

Cloud Volumes Service expose plusieurs ports TCP pour servir les partages NFS et SMB :

- "Ports requis pour l'accès NFS"
- "Ports requis pour l'accès SMB"

En outre, SMB, NFS avec LDAP, y compris Kerberos, et des configurations à double protocole requièrent l'accès à un domaine Windows Active Directory. Les connexions Active Directory doivent être de "configuré" par région. Les contrôleurs de domaine (DC) Active Directory sont identifiés à l'aide de "Découverte de data Center basée sur DNS" Utilisation des serveurs DNS spécifiés. Tous les DCS renvoyés sont utilisés. La liste des DCS admissibles peut être limitée en spécifiant un site Active Directory.

Cloud Volumes Service atteint son niveau avec les adresses IP de la plage CIDR allouée à l' `gcloud compute address` commande pendant "Intégration de la Cloud Volumes Service". Vous pouvez utiliser ce CIDR comme adresses source pour configurer les pare-feu entrants sur vos contrôleurs de domaine Active Directory.

Les contrôleurs de domaine Active Directory doivent "Exposer les ports aux rapports CIDR Cloud Volumes Service comme indiqué ici".

Protocoles NAS

Présentation des protocoles NAS

Les protocoles NAS incluent NFS (v3 et v4.1) et SMB/CIFS (2.x et 3.x). Ces protocoles sont la façon dont CVS permet un accès partagé aux données entre plusieurs clients NAS. Par ailleurs, Cloud Volumes Service permet d'accéder simultanément aux clients NFS et SMB/CIFS (double protocole) tout en respectant l'ensemble des paramètres d'identité et d'autorisation sur les fichiers et les dossiers des partages NAS. Pour préserver un niveau maximal de sécurité des transferts de données, Cloud Volumes Service prend en charge le chiffrement de protocole à la volée avec le chiffrement SMB et NFS Kerberos 5p.

Le double protocole est disponible avec CVS-Performance uniquement.

Notions de base sur les protocoles NAS

Les protocoles NAS permettent à plusieurs clients sur un réseau d'accéder aux mêmes données sur un système de stockage, notamment Cloud Volumes Service sur GCP. NFS

et SMB sont les protocoles NAS définis et fonctionnent sur une base client/serveur où Cloud Volumes Service fait office de serveur. Les clients envoient des demandes d'accès, de lecture et d'écriture au serveur, et le serveur est responsable de la coordination des mécanismes de verrouillage des fichiers, du stockage des autorisations et du traitement des demandes d'identité et d'authentification.

Par exemple, le processus général suivant est suivi si un client NAS souhaite créer un nouveau fichier dans un dossier.

1. Le client demande au serveur des informations sur le répertoire (autorisations, propriétaire, groupe, ID de fichier, espace disponible, et ainsi de suite) ; le serveur répond avec les informations si le client et l'utilisateur demandeur disposent des autorisations nécessaires sur le dossier parent.
2. Si les autorisations du répertoire autorisent l'accès, le client demande alors au serveur si le nom de fichier en cours de création existe déjà dans le système de fichiers. Si le nom de fichier est déjà utilisé, la création échoue. Si le nom de fichier n'existe pas, le serveur indique au client qu'il peut continuer.
3. Le client envoie un appel au serveur pour créer le fichier avec le descripteur de répertoire et le nom du fichier et définit l'accès et les heures modifiées. Le serveur émet un ID de fichier unique pour s'assurer qu'aucun autre fichier n'est créé avec le même ID de fichier.
4. Le client envoie un appel pour vérifier les attributs du fichier avant l'opération D'ÉCRITURE. Si les autorisations le permettent, le client écrit le nouveau fichier. Si le verrouillage est utilisé par le protocole/l'application, le client demande au serveur un verrouillage pour empêcher les autres clients d'accéder au fichier lorsqu'il est verrouillé afin d'éviter la corruption des données.

NFS

NFS est un protocole de système de fichiers distribué qui est une norme IETF ouverte définie dans la norme RFC (Request for Comments) qui permet à quiconque d'implémenter le protocole.

Les volumes de Cloud Volumes Service sont partagés avec les clients NFS en exportant un chemin accessible à un client ou à un ensemble de clients. Les autorisations de monter ces exportations sont définies par des règles et des règles d'exportation, qui peuvent être configurées par les administrateurs Cloud Volumes Service.

L'implémentation NFS de NetApp est considérée comme une norme Gold pour le protocole et elle est utilisée dans d'innombrables environnements NAS d'entreprise. Les sections suivantes présentent le protocole NFS ainsi que les fonctionnalités de sécurité spécifiques disponibles dans Cloud Volumes Service et leur mise en œuvre.

Utilisateurs et groupes UNIX locaux par défaut

Cloud Volumes Service contient plusieurs utilisateurs et groupes UNIX par défaut pour diverses fonctionnalités de base. Ces utilisateurs et ces groupes ne peuvent actuellement pas être modifiés ou supprimés. Actuellement, les nouveaux utilisateurs et groupes locaux ne peuvent pas être ajoutés à Cloud Volumes Service. Les utilisateurs et groupes UNIX hors des utilisateurs et des groupes par défaut doivent être fournis par un service de noms LDAP externe.

Le tableau suivant indique les utilisateurs et groupes par défaut et leurs ID numériques correspondants. NetApp recommande de ne pas créer de nouveaux utilisateurs ou groupes dans LDAP ou sur les clients locaux qui utilisent à nouveau ces ID numériques.

Utilisateurs par défaut : ID numériques	Groupes par défaut : ID numériques
• racine : 0 • pcuser:65534 • personne:65535	• racine : 0 • démon:1 • pcuser:65534 • personne:65535

Lors de l'utilisation de NFSv4.1, l'utilisateur root peut s'afficher comme personne lors de l'exécution des commandes de liste de répertoires sur les clients NFS. Ceci est dû à la configuration du mappage de domaine d'ID du client. Voir la section appelée NFSv4.1 et personne utilisateur/groupe pour plus de détails sur ce problème et sur la façon de le résoudre.

L'utilisateur root

Sous Linux, le compte racine a accès à toutes les commandes, fichiers et dossiers d'un système de fichiers Linux. En raison de la puissance de ce compte, les bonnes pratiques en matière de sécurité exigent souvent que l'utilisateur root soit désactivé ou restreint d'une façon ou d'une autre. Dans les exportations NFS, la puissance dont dispose un utilisateur root sur les fichiers et les dossiers peut être contrôlée dans Cloud Volumes Service au moyen de règles et de stratégies d'exportation et d'un concept appelé « squash racine ».

Le scaling racine garantit que l'utilisateur root accédant à un montage NFS est écrasé à l'utilisateur numérique anonyme 65534 (voir la section «L'utilisateur anonyme") et n'est actuellement disponible que lors de l'utilisation de CVS-Performance en sélectionnant Désactivé pour l'accès racine lors de la création de règles d'export. Si l'utilisateur root est écrasé par l'utilisateur anonyme, il n'a plus accès à exécuter CHown ou "commandes setuid/setgid (le bit collant)" Sur les fichiers ou dossiers du montage NFS, et les fichiers ou dossiers créés par l'utilisateur root affichent l'UID d'anon comme propriétaire/groupe. En outre, les ACL NFSv4 ne peuvent pas être modifiés par l'utilisateur root. Cependant, l'utilisateur root a toujours accès aux fichiers chmod et supprimés pour lesquels il n'a pas d'autorisations explicites. Si vous souhaitez limiter l'accès aux autorisations de fichier et de dossier d'un utilisateur root, envisagez d'utiliser un volume avec des listes de contrôle d'accès NTFS, créant un utilisateur Windows nommé `root`, et application des autorisations souhaitées aux fichiers ou dossiers.

L'utilisateur anonyme

L'ID utilisateur anonyme (anon) spécifie un ID utilisateur UNIX ou un nom d'utilisateur qui est mappé aux requêtes client qui arrivent sans identifiants NFS valides. Cela peut inclure l'utilisateur racine lorsque le squaing racine est utilisé. L'utilisateur d'anon dans Cloud Volumes Service est 65534.

Cet UID est normalement associé au nom d'utilisateur `nobody` ou `nfsnobody` Dans les environnements Linux. Cloud Volumes Service utilise également 65534 comme pcuser UNIX local (voir la section «Utilisateurs et groupes UNIX locaux par défaut"), qui est également l'utilisateur de secours par défaut pour les mappages de noms Windows à UNIX lorsqu'aucun utilisateur UNIX correspondant valide n'est trouvé dans LDAP.

En raison des différences entre les noms d'utilisateur Linux et Cloud Volumes Service pour UID 65534, la chaîne de nom des utilisateurs mappés sur 65534 risque de ne pas correspondre lors de l'utilisation de NFSv4.1. Vous pouvez donc voir `nobody` en tant qu'utilisateur sur certains fichiers et dossiers. Voir la section «NFSv4.1 et personne utilisateur/groupe" pour plus d'informations sur ce problème et sur la façon de le résoudre.

Contrôle d'accès/exportations

L'accès initial aux exportations/partages pour les montages NFS est contrôlé par le biais de règles d'export policy basées sur les hôtes, figurant dans une export policy. Une adresse IP hôte, un nom d'hôte, un sous-réseau, un groupe réseau ou un domaine sont définis pour permettre l'accès au montage du partage NFS et le niveau d'accès autorisé à l'hôte. Les options de configuration des règles d'export-policy dépendent du niveau Cloud Volumes Service.

Pour CVS-SW, les options suivantes sont disponibles pour la configuration des export-policy :

- **Correspondance client.** liste d'adresses IP séparées par des virgules, liste de noms d'hôte séparés par des virgules, sous-réseaux, groupes réseau, noms de domaine.
- **Règles d'accès RO/RW.** sélectionnez lecture/écriture ou lecture seule pour contrôler le niveau d'accès à l'exportation.CVS-Performance fournit les options suivantes :
- **Correspondance client.** liste d'adresses IP séparées par des virgules, liste de noms d'hôte séparés par des virgules, sous-réseaux, groupes réseau, noms de domaine.
- **Règles d'accès RO/RW.** sélectionnez lecture/écriture ou lecture seulement pour contrôler le niveau d'accès à l'exportation.
- **Accès racine (activé/désactivé).** configure le squash racine (voir la section «L'utilisateur root« pour plus de détails).
- **Type de protocole.** cette option limite l'accès au montage NFS à une version de protocole spécifique. Lorsque vous spécifiez à la fois NFS v3 et NFS v4.1 pour le volume, laissez les deux vides ou cochez les deux cases.
- **Niveau de sécurité Kerberos (lorsque l'option Activer Kerberos est sélectionnée).** fournit les options de krb5, krb5i et/ou krb5p pour l'accès en lecture seule ou en lecture/écriture.

Changer la propriété (chown) et le groupe de changement (chgrp)

NFS sur Cloud Volumes Service ne permet à l'utilisateur root d'exécuter chown/chgrp que sur des fichiers et des dossiers. Les autres utilisateurs voient un `Operation not permitted` erreur : même sur les fichiers qu'ils possèdent. Si vous utilisez du squash racine (comme décrit dans la section «L'utilisateur root"), la racine est écrasée à un utilisateur non root et ne peut pas accéder à chown et chgrp. Il n'existe actuellement aucune solution de contournement dans Cloud Volumes Service pour permettre aux chown et aux chgrp de non-root utilisateurs. Si des modifications de propriété sont requises, envisagez d'utiliser des volumes à double protocole et définissez le style de sécurité sur NTFS pour contrôler les autorisations du côté Windows.

Gestion des autorisations

Cloud Volumes Service prend en charge les deux bits de mode (par exemple 644, 777, etc. Pour rwx) et les ACL NFSv4.1 pour contrôler les autorisations sur les clients NFS pour les volumes qui utilisent le style de sécurité UNIX. La gestion des autorisations standard est utilisée pour ces clients (tels que chmod, chown ou nfs4_setfacl) et avec n'importe quel client Linux qui les prend en charge.

En outre, lorsque des volumes à double protocole sont définis sur NTFS, les clients NFS peuvent tirer parti du mappage de noms Cloud Volumes Service aux utilisateurs Windows, qui sont ensuite utilisés pour résoudre les autorisations NTFS. Pour ce faire, une connexion LDAP à Cloud Volumes Service doit fournir des traductions d'ID numérique vers nom d'utilisateur car Cloud Volumes Service nécessite un nom d'utilisateur UNIX valide pour être correctement mappé à un nom d'utilisateur Windows.

Fournissant des listes de contrôle d'accès granulaires pour NFSv3

Les autorisations bits du mode couvrent uniquement le propriétaire, le groupe et tous les autres éléments de la

sémantique, ce qui signifie qu'aucun contrôle granulaire des accès utilisateur n'est mis en place pour les données NFSv3 de base. Cloud Volumes Service ne prend pas en charge les listes de contrôle d'accès POSIX, ni les attributs étendus (tels que chattr). Les listes de contrôle d'accès granulaires ne sont donc possibles que dans les scénarios suivants avec NFSv3 :

- Volumes de style de sécurité NTFS (serveur CIFS requis) avec des mappages utilisateur UNIX vers Windows valides.
- NFS v4.1 a été appliqué à l'aide d'un client admin montage NFSv4.1 pour appliquer les ACL.

Ces deux méthodes nécessitent une connexion LDAP pour la gestion des identités UNIX et des informations utilisateur et groupe UNIX valides (voir la section "« LDAP »") Et ne sont disponibles qu'avec des instances CVS-Performance. Pour utiliser des volumes de style de sécurité NTFS avec le protocole NFS, vous devez utiliser le protocole double (SMB et NFS v3) ou le double protocole (SMB et NFS v4.1), même si aucune connexion SMB n'est établie. Pour utiliser les listes de contrôle d'accès NFSv4.1 avec montages NFSv3, vous devez sélectionner `Both (NFSv3/NFSv4.1)` comme type de protocole.

Les bits standard en mode UNIX ne fournissent pas le même niveau de granularité dans les autorisations que les ACL NTFS ou NFSv4.x fournissent. Le tableau suivant compare la granularité des autorisations entre les bits en mode NFS v3 et les ACL NFSv4.1. Pour plus d'informations sur les listes de contrôle d'accès NFSv4.1, voir "Nfs4_acl - listes de contrôle d'accès NFSv4".

Bits de mode NFSv3	Listes de contrôle d'accès NFSv4.1
• Définir l'ID utilisateur lors de l'exécution • Définir l'ID du groupe lors de l'exécution • Enregistrer le texte échangé (non défini dans POSIX) • Autorisation de lecture du propriétaire • Autorisation d'écriture pour le propriétaire • Exécutez l'autorisation de propriétaire sur un fichier ou recherchez (recherchez) l'autorisation de propriétaire dans le répertoire • Autorisation de lecture pour le groupe • Autorisation d'écriture pour le groupe • Exécutez l'autorisation de groupe sur un fichier ou recherchez (recherchez) l'autorisation de groupe dans le répertoire • Autorisation de lecture pour les autres utilisateurs • Autorisation d'écriture pour les autres • Exécutez l'autorisation pour les autres utilisateurs d'un fichier ou recherchez (recherchez) l'autorisation pour d'autres personnes dans le répertoire	Types d'entrée de contrôle d'accès (ACE) (Allow/Deny/Audit) * indicateurs d'héritage * Directory-Hériter * fichier-Hériter * no-Propagate-Hériter * hériter-only Autorisations * lecture-données (fichiers) / répertoire-liste (répertoires) * écriture-données (fichiers) / création-fichier (répertoires) * ajout-données (fichiers) / création-sous-répertoire (répertoires) * exécution (fichiers) / changement-répertoire (répertoires) * suppression * suppression-enfant * lecture-attributs * écriture-attributs * liste de contrôle d'accès * lecture-écriture * liste de contrôle d'accès *

Enfin, l'appartenance au groupe NFS (dans NFSv3 et NFSV4.x) est limitée à un maximum par défaut de 16 pour AUTH_SYS selon les limites de paquets RPC. NFS Kerberos fournit jusqu'à 32 groupes et les ACL NFSv4 suppriment la limite par le biais de listes de contrôle d'accès granulaires des utilisateurs et des groupes (jusqu'à 1024 entrées par ACE).

En outre, Cloud Volumes Service offre une prise en charge étendue des groupes pour étendre le nombre maximal de groupes pris en charge jusqu'à 32. Pour ce faire, une connexion LDAP à un serveur LDAP qui contient des identités d'utilisateur et de groupe UNIX valides est nécessaire. Pour plus d'informations sur cette configuration, reportez-vous à la section "Création et gestion des volumes NFS" Dans la documentation Google.

ID d'utilisateur et de groupe NFSv3

Les ID utilisateur et groupe NFSv3 sont répartis sur le fil sous forme d'ID numériques plutôt que de noms. Cloud Volumes Service ne résout pas le nom d'utilisateur de ces ID numériques avec NFSv3, avec des volumes de style de sécurité UNIX utilisant des bits de mode uniquement. Lorsque des listes de contrôle d'accès NFSv4.1 sont présentes, une recherche d'ID numérique et/ou une recherche de chaîne de nom est nécessaire pour résoudre correctement la liste de contrôle d'accès, même en cas d'utilisation de NFS v3. Avec les volumes de style de sécurité NTFS, Cloud Volumes Service doit résoudre un ID numérique à un utilisateur UNIX valide, puis le mapper à un utilisateur Windows valide pour négocier les droits d'accès.

Limitations de sécurité des ID d'utilisateur et de groupe NFSv3

Avec NFSv3, le client et le serveur n'ont jamais à confirmer que l'utilisateur qui tente de lire ou d'écrire avec un ID numérique est un utilisateur valide ; il est simplement implicitement approuvé. Cela ouvre le système de fichiers jusqu'à des failles potentielles simplement en usurper n'importe quel ID numérique. Pour éviter les trous de sécurité de ce type, il existe quelques options pour Cloud Volumes Service.

- L'implémentation de Kerberos pour NFS oblige les utilisateurs à s'authentifier avec un nom d'utilisateur et un mot de passe ou un fichier keytab afin d'obtenir un ticket Kerberos pour autoriser l'accès à un montage. Kerberos est disponible avec des instances CVS-Performance et uniquement avec NFSv4.1.
- En limitant la liste des hôtes des règles d'export policy, les clients NFSv3 disposent d'un accès au volume Cloud Volumes Service.
- L'utilisation de volumes à double protocole et l'application de listes de contrôle d'accès NTFS au volume oblige les clients NFSv3 à résoudre des ID numériques à des noms d'utilisateur UNIX valides afin de s'authentifier correctement pour accéder aux montages. Pour cela, il est nécessaire d'activer LDAP et de configurer les identités d'utilisateur et de groupe UNIX.
- L'affaissement de l'utilisateur root limite les dommages qu'un utilisateur root peut faire sur un montage NFS, mais ne élimine pas complètement les risques. Pour plus d'informations, reportez-vous à la section «L'utilisateur root. »

En fin de compte, la sécurité NFS est limitée à la version de protocole que vous utilisez. NFS v3, bien que plus performant que NFSv4.1, n'offre pas le même niveau de sécurité.

NFSv4.1

NFSv4.1 offre une sécurité et une fiabilité supérieures par rapport à NFS v3, pour les raisons suivantes :

- Verrouillage intégré grâce à un mécanisme de location
- Sessions avec état
- Toutes les fonctionnalités NFS sur un seul port (2049)
- TCP uniquement
- Mappage du domaine d'ID
- Intégration Kerberos (NFSv3 peut utiliser Kerberos, mais uniquement pour NFS, pas pour les protocoles auxiliaires tels que NLM)

Dépendances NFSv4.1

En raison des fonctions de sécurité ajoutées dans NFSv4.1, certaines dépendances externes étaient impliquées dans l'utilisation de NFSv3 (semblable au mode d'utilisation requis par SMB, comme Active Directory).

Listes de contrôle d'accès NFSv4.1

Cloud Volumes Service prend en charge les listes de contrôle d'accès NFSv4.x, qui offrent des avantages distincts par rapport aux autorisations de style POSIX standard, notamment :

- Contrôle granulaire de l'accès des utilisateurs aux fichiers et aux répertoires
- Sécurité NFS renforcée
- Interopérabilité améliorée avec CIFS/SMB
- Suppression de la limitation NFS de 16 groupes par utilisateur avec sécurité AUTH_SYS
- Les ACL contournent le besoin en résolution d'ID de groupe (GID), qui supprime efficacement les ACL limitésNFS sont contrôlées par les clients NFS, et non par Cloud Volumes Service. Pour utiliser les listes de contrôle d'accès NFS NFSv4.1, assurez-vous que la version logicielle de votre client les prend en charge et que les utilitaires NFS appropriés sont installés.

Compatibilité entre les listes de contrôle d'accès NFSv4.1 et les clients SMB

Les ACL NFSv4 ne sont pas plus les ACL de niveau fichier (ACL NTFS) de Windows, mais possèdent une fonctionnalité similaire. Cependant, dans les environnements NAS multiprotocoles, si vous disposez de listes de contrôle d'accès NFSv4.1 et que vous utilisez un accès double protocole (NFS et SMB sur les mêmes datasets), les clients qui utilisent SMB2.0 et versions ultérieures ne pourront pas afficher ni gérer les listes de contrôle d'accès à partir des onglets de sécurité Windows.

Fonctionnement des listes de contrôle d'accès NFSv4.1

Pour référence, les termes suivants sont définis :

- **Liste de contrôle d'accès (ACL).** liste des entrées d'autorisations.
- **Entrée de contrôle d'accès (ACE).** Entrée d'autorisation dans la liste.

Lorsqu'un client définit une liste de contrôle d'accès NFSv4.1 sur un fichier lors d'une opération SETATTR, Cloud Volumes Service définit cette liste de contrôle d'accès sur l'objet en remplaçant toute liste de contrôle d'accès existante. S'il n'y a pas de liste de contrôle d'accès sur un fichier, les autorisations de mode sur ce fichier sont calculées à partir DE OWNER@, GROUP@ et EVERYONE@. S'il existe des SUID/SGID/bits COLLANTS sur le fichier, ils ne sont pas affectés.

Lorsqu'un client obtient une liste de contrôle d'accès NFS (ACL) NFSv4.1 sur un fichier au cours d'une opération GETATTR, Cloud Volumes Service lit la liste de contrôle d'accès NFS (ACL) associée à l'objet, construit une liste d'ACE et renvoie la liste au client. Si le fichier possède une liste de contrôle d'accès NT ou des bits de mode, une liste de contrôle d'accès est construite à partir de bits de mode et renvoyée au client.

L'accès est refusé si une ACE DE REFUS est présente dans la liste de contrôle d'accès ; l'accès est accordé si une ACE D'AUTORISATION existe. Toutefois, l'accès est également refusé si aucun des ACE n'est présent dans l'ACL.

Un descripteur de sécurité se compose d'une liste de contrôle d'accès (SACL) et d'une liste de contrôle d'accès discrétionnaire (DACL). Lorsque NFSv4.1 interagit avec CIFS/SMB, le DACL est mappé à NFSv4 et CIFS. La DACL se compose des ACCE AUTORISER et REFUSER.

Si un niveau de base `chmod` Est exécuté sur un fichier ou un dossier avec les ACL NFSv4.1 définies, les listes de contrôle d'accès utilisateur et groupe existantes sont conservées, mais le PROPRIÉTAIRE par défaut@, GROUPE@, EVERYONE@ ACL sont modifiés.

Un client utilisant des listes de contrôle d'accès NFSv4.1 peut définir et afficher des listes de contrôle d'accès pour les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire comportant une liste de contrôle d'accès, cet objet hérite de tous les ACE de la liste de contrôle d'accès qui ont été marqués avec le nom approprié "indicateurs d'héritage".

Si un fichier ou un répertoire possède une liste de contrôle d'accès NFSv4.1, cette liste de contrôle d'accès est utilisée pour contrôler l'accès, quel que soit le protocole utilisé pour accéder au fichier ou au répertoire.

Les fichiers et les répertoires héritent des ACE des listes de contrôle d'accès NFSv4 sur les répertoires parents (éventuellement avec les modifications appropriées) tant que les ACE ont été balisés avec les indicateurs d'héritage corrects.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une requête NFSv4, la liste de contrôle d'accès du fichier ou répertoire résultant dépend du fait que la demande de création de fichier inclut une liste de contrôle d'accès ou uniquement les autorisations d'accès aux fichiers UNIX standard. La liste de contrôle d'accès dépend également de la présence ou non d'une liste de contrôle d'accès dans le répertoire parent.

- Si la requête inclut une liste de contrôle d'accès, cette liste de contrôle d'accès est utilisée.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent ne dispose pas d'ACL, le mode fichier client est utilisé pour définir les autorisations d'accès aux fichiers UNIX standard.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent dispose d'une liste de contrôle d'accès non héritable, une liste de contrôle d'accès par défaut basée sur les bits de mode transmis à la requête est définie sur le nouvel objet.
- Si la demande comprend uniquement des autorisations d'accès aux fichiers UNIX standard mais que le répertoire parent possède une ACL, les ACE de l'ACL du répertoire parent sont hérités par le nouveau fichier ou répertoire tant que les ACE ont été balisés avec les indicateurs d'héritage appropriés.

Autorisations ACE

Les autorisations de listes de contrôle d'accès NFSv4.1 utilisent une série de valeurs de lettres majuscules et minuscules (par exemple `rxtncy`) pour contrôler l'accès. Pour plus d'informations sur ces valeurs de lettre, reportez-vous à la section "COMMENT : utiliser NFSv4 ACL".

Comportement ACL NFSv4.1 avec umask et héritage ACL

"Les ACL NFSv4 permettent d'offrir l'héritage ACL". L'héritage ACL signifie que les fichiers ou les dossiers créés sous des objets avec des listes de contrôle d'accès NFSv4.1 peuvent hériter des listes de contrôle d'accès basées sur la configuration du "Indicateur d'héritage ACL".

"Umask" permet de contrôler le niveau d'autorisation auquel les fichiers et dossiers sont créés dans un répertoire sans interaction avec l'administrateur. Par défaut, Cloud Volumes Service permet à umask de remplacer les listes de contrôle d'accès héritées, ce qui est le comportement attendu selon "RFC 5661".

Formatage ACL

Les ACL NFSv4.1 ont un formatage spécifique. L'exemple suivant est un ensemble ACE sur un fichier :

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

L'exemple précédent suit les directives de format ACL de :

```
type:flags:principal:permissions
```

Un type de `A` signifie « autoriser ». Les indicateurs hériter ne sont pas définis dans ce cas, car le principal n'est pas un groupe et n'inclut pas l'héritage. De plus, comme l'ACE n'est pas une entrée D'AUDIT, il n'est pas nécessaire de définir les indicateurs d'audit. Pour plus d'informations sur les listes de contrôle d'accès NFSv4.1, voir "http://linux.die.net/man/5/nfs4_acl".

Si la liste de contrôle d'accès NFSv4.1 n'est pas définie correctement (ou si une chaîne de nom ne peut pas être résolue par le client et le serveur), la liste de contrôle d'accès peut ne pas se comporter comme prévu, ou si la modification de la liste de contrôle d'accès échoue à s'appliquer et générer une erreur.

Les exemples d'erreurs sont les suivants :

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

REFUS explicite

Les autorisations NFSv4.1 peuvent inclure des attributs DE REFUS explicites pour LE PROPRIÉTAIRE, LE GROUPE et TOUT LE MONDE. En effet, les listes de contrôle d'accès NFSv4.1 étant des listes de contrôle d'accès par défaut, ce qui signifie que si une liste de contrôle d'accès n'est pas explicitement accordée par une ACE, elle est alors refusée. Les attributs DE REFUS explicite remplacent les ACE D'ACCÈS, explicites ou non.

LES ACE DE REFUS sont définis avec une balise d'attribut de `D`.

Dans l'exemple ci-dessous, GROUP@ est autorisé à toutes les autorisations de lecture et d'exécution, mais a refusé tout accès en écriture.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DANS la mesure du possible, LES ACE DE REFUS doivent être évités parce qu'ils peuvent être confus et compliqués ; AUTORISER les listes de contrôle d'accès qui ne sont pas explicitement définies sont refusées implicitement. Lorsque LES ACE DE REFUS sont définis, les utilisateurs peuvent se voir refuser l'accès lorsqu'ils s'attendent à bénéficier de l'accès.

L'ensemble précédent d'ACE est équivalent à 755 bits de mode, ce qui signifie :

- Le propriétaire a tous les droits.
- Les groupes ont lecture seule.
- D'autres ont lecture seule.

Cependant, même si les autorisations sont ajustées à l'équivalent 775, l'accès peut être refusé en raison du REFUS explicite défini sur TOUT LE MONDE.

Dépendances de mappage de domaine ID NFSv4.1

NFSv4.1 s'appuie sur la logique de mappage de domaine d'ID en tant que couche de sécurité pour garantir qu'un utilisateur qui tente d'accéder à un montage NFSv4.1 est en effet celui qu'il prétend être. Dans ce cas, le nom d'utilisateur et le nom de groupe provenant du client NFSv4.1 ajoute une chaîne de nom et l'envoie à l'instance Cloud Volumes Service. Si cette combinaison nom d'utilisateur/groupe et chaîne ID ne correspond pas, alors l'utilisateur et/ou le groupe est écrasé par défaut, aucun utilisateur spécifié dans le `/etc/idmapd.conf` fichier sur le client.

Cette chaîne d'ID est une exigence pour le respect correct des autorisations, en particulier lorsque des ACL NFSv4.1 et/ou Kerberos sont utilisés. Par conséquent, des dépendances au niveau du serveur de service de noms, telles que les serveurs LDAP, sont nécessaires pour assurer la cohérence entre les clients et Cloud Volumes Service afin de permettre une résolution appropriée de l'identité des noms d'utilisateur et de groupe.

Cloud Volumes Service utilise une valeur de nom de domaine d'ID par défaut statique de `defaultv4iddomain.com`. Les clients NFS utilisent par défaut le nom de domaine DNS pour ses paramètres de nom de domaine ID, mais vous pouvez régler manuellement le nom de domaine ID dans `/etc/idmapd.conf`.

Si le protocole LDAP est activé dans Cloud Volumes Service, Cloud Volumes Service automatise le domaine d'ID NFS pour modifier ce qui est configuré pour le domaine de recherche dans DNS et les clients n'ont pas besoin d'être modifiés à moins qu'ils n'utilisent des noms de recherche de domaine DNS différents.

Lorsque Cloud Volumes Service peut résoudre un nom d'utilisateur ou un nom de groupe dans les fichiers locaux ou LDAP, la chaîne de domaine est utilisée et les ID de domaine ne sont pas identiques. Si Cloud Volumes Service ne parvient pas à trouver un nom d'utilisateur ou un nom de groupe dans les fichiers locaux ou LDAP, la valeur d'ID numérique est utilisée et le client NFS résout correctement le nom (ceci est similaire au comportement NFSv3).

Sans modifier le domaine d'ID NFSv4.1 du client pour correspondre à l'utilisation du volume Cloud Volumes Service, le comportement suivant s'affiche :

- Les utilisateurs et groupes UNIX avec des entrées locales dans Cloud Volumes Service (comme root, comme défini dans les utilisateurs et groupes UNIX locaux) sont écrasés sur la valeur personne.
- Les utilisateurs et groupes UNIX dont les entrées sont dans LDAP (si Cloud Volumes Service est configuré pour utiliser LDAP) ne s'acclaent à personne si les domaines DNS sont différents entre les clients NFS et Cloud Volumes Service.
- Les utilisateurs et groupes UNIX sans entrées locales ou LDAP utilisent la valeur d'ID numérique et résolvez le nom spécifié sur le client NFS. Si aucun nom n'existe sur le client, seul l'ID numérique est affiché.

Voici les résultats du scénario précédent :

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Lorsque les domaines d'ID client et serveur correspondent, voici l'apparence de la même liste de fichiers :

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Pour plus d'informations sur ce problème et sur la façon de le résoudre, reportez-vous à la section «NFSv4.1 et personne utilisateur/groupe. »

Les dépendances Kerberos

Si vous prévoyez d'utiliser Kerberos avec NFS, vous devez disposer des éléments suivants en Cloud Volumes Service :

- Domaine Active Directory pour les services du centre de distribution Kerberos (KDC)
- Domaine Active Directory avec des attributs utilisateur et groupe renseignés avec des informations UNIX pour la fonctionnalité LDAP (le protocole Kerberos NFS dans Cloud Volumes Service requiert un mappage utilisateur SPN vers UNIX pour assurer le bon fonctionnement du système).
- LDAP activée sur l'instance Cloud Volumes Service
- Domaine Active Directory pour les services DNS

NFSv4.1 et personne utilisateur/groupe

L'un des problèmes les plus courants rencontrés avec une configuration NFSv4.1 est lorsqu'un fichier ou un dossier est affiché dans une liste à l'aide de `ls` appartenant au `user:group` combinaison de `nobody:nobody`.

Par exemple :

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

Et l'ID numérique est `99`.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

Dans certains cas, le fichier peut indiquer le propriétaire correct, mais `nobody` en tant que groupe.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Qui n'est personne?

Le `nobody` L'utilisateur dans NFSv4.1 est différent de `nfsnobody` utilisateur. Vous pouvez afficher la manière dont un client NFS voit chaque utilisateur en exécutant le `id` commande :

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Avec NFSv4.1, le `nobody` l'utilisateur est l'utilisateur par défaut défini par le `idmapd.conf` et peut être défini comme n'importe quel utilisateur que vous voulez utiliser.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Pourquoi cela se produit-il ?

Étant donné que la sécurité par mappage de chaînes de noms est un principe clé des opérations NFSv4.1, le comportement par défaut lorsqu'une chaîne de noms ne correspond pas correctement est de court-courser cet utilisateur à un utilisateur qui n'aura normalement pas accès aux fichiers et dossiers appartenant aux utilisateurs et aux groupes.

Lorsque vous voyez `nobody` Pour l'utilisateur et/ou le groupe dans les listes de fichiers, cela signifie généralement que quelque chose dans NFSv4.1 est mal configuré. La sensibilité de la casse peut être ici en jeu.

Par exemple, si utilisateur1@CVSDEMO.LOmabL (uid 1234, gid 1234) accède à une exportation, alors Cloud Volumes Service doit pouvoir trouver utilisateur1@CVSDEMO.LOMOL (uid 1234, gid 1234). Si l'utilisateur dans Cloud Volumes Service est USER1@CVSDEMO.LOmabmacop, il ne correspond pas (majuscules UTILISATEUR1 contre minuscules utilisateur1). Dans de nombreux cas, vous pouvez voir ce qui suit dans le fichier de messages sur le client :

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Le client et le serveur doivent tous deux convenir qu'un utilisateur est effectivement celui qu'il prétend être. Vous devez donc vérifier les éléments suivants pour vous assurer que l'utilisateur que le client voit dispose des mêmes informations que l'utilisateur que celui que Cloud Volumes Service voit.

- **Domaine ID NFSv4.x.** client : `idmapd.conf` Fichier ; utilisations de Cloud Volumes Service `defaultv4iddomain.com` et ne peut pas être modifié manuellement. En cas d'utilisation de LDAP avec NFSv4.1, Cloud Volumes Service modifie le domaine d'ID en fonction de ce que le domaine de recherche DNS utilise, ce qui est le même que le domaine AD.
- **Nom d'utilisateur et ID numériques.** Ceci détermine l'endroit où le client recherche des noms d'utilisateur et utilise la configuration du commutateur de service de nom—client: `nsswitch.conf` Et/ou fichiers de passwd et de groupe locaux ; Cloud Volumes Service n'autorise pas les modifications à ceci mais ajoute automatiquement LDAP à la configuration lorsqu'elle est activée.
- **Nom de groupe et ID numériques.** cette option détermine où le client recherche des noms de groupe et utilise la configuration du commutateur de service de nom—client : `nsswitch.conf` Et/ou fichiers de passwd et de groupe locaux ; Cloud Volumes Service n'autorise pas les modifications à ceci mais ajoute automatiquement LDAP à la configuration lorsqu'elle est activée.

Dans presque tous les cas, si vous voyez `nobody` Dans les listes d'utilisateurs et de groupes des clients, le problème est la traduction de l'ID de domaine de nom d'utilisateur ou de groupe entre Cloud Volumes Service et le client NFS. Pour éviter ce scénario, utilisez LDAP pour résoudre les informations d'utilisateur et de groupe entre les clients et Cloud Volumes Service.

Affichage des chaînes d'ID de nom pour NFSv4.1 sur les clients

Si vous utilisez NFSv4.1, un mappage de chaîne de nom a lieu lors des opérations NFS, comme décrit précédemment.

En plus de l'utilisation `/var/log/messages` Pour trouver un problème avec les ID NFSv4, vous pouvez utiliser le "nfsidmap -l" Commande sur le client NFS pour afficher les noms d'utilisateur qui sont correctement mappés au domaine NFSv4.

Par exemple, ceci est la sortie de la commande après un utilisateur qui peut être trouvé par le client et que Cloud Volumes Service accède à un montage NFSv4.x :

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Lorsqu'un utilisateur qui ne se mappe pas correctement dans le domaine ID NFSv4.1 (dans ce cas, `netapp-user`) essaie d'accéder au même montage et touche un fichier, ils sont affectés `nobody:nobody`, comme

prévu.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

Le `nfsidmap -l` la sortie affiche l'utilisateur `pcuser` à l'écran, mais pas `netapp-user`; il s'agit de l'utilisateur anonyme dans notre règle d'export-policy (`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

PME

"PME" Est un protocole de partage de fichiers réseau développé par Microsoft qui fournit une authentification utilisateur/groupe centralisée, des autorisations, un verrouillage et un partage de fichiers à plusieurs clients SMB sur un réseau Ethernet. Les fichiers et les dossiers sont présentés aux clients par le biais de partages, qui peuvent être configurés avec diverses propriétés de partage et offre un contrôle d'accès par le biais d'autorisations de niveau partage. SMB peut être présenté à n'importe quel client prenant en charge le protocole, y compris les clients Windows, Apple et Linux.

Cloud Volumes Service prend en charge les versions SMB 2.1 et 3.x du protocole.

Contrôle d'accès/partages SMB

- Lorsqu'un nom d'utilisateur Windows demande l'accès au volume Cloud Volumes Service, Cloud Volumes Service recherche un nom d'utilisateur UNIX en utilisant les méthodes configurées par les administrateurs Cloud Volumes Service.

- Si un fournisseur d'identités UNIX externe (LDAP) est configuré et que les noms d'utilisateur Windows/UNIX sont identiques, les noms d'utilisateur Windows mappent les noms d'utilisateur 1:1 vers UNIX sans configuration supplémentaire. Lorsque LDAP est activée, Active Directory est utilisé pour héberger ces attributs UNIX pour les objets utilisateur et groupe.
- Si les noms Windows et UNIX ne correspondent pas de la même manière, LDAP doit être configurée pour permettre à Cloud Volumes Service d'utiliser la configuration du mappage de noms LDAP (voir la section ""Utilisation du protocole LDAP pour le mappage de noms asymétrique"").
- Si LDAP n'est pas utilisé, les utilisateurs Windows SMB mappent un utilisateur UNIX local par défaut nommé `pcuser` À Cloud Volumes Service. Cela signifie que les fichiers écrits dans Windows par les utilisateurs qui font correspondre à `pcuser` Afficher la propriété UNIX sous `pcuser` Dans des environnements NAS multiprotocoles. `pcuser` voici le `nobody` Utilisateur dans les environnements Linux (UID 65534).

Dans les déploiements avec SMB uniquement, le `pcuser` Le mappage a toujours lieu, mais cela n'a aucune importance, car la propriété des utilisateurs et des groupes Windows est correctement affichée et l'accès NFS au volume SMB uniquement n'est pas autorisé. De plus, les volumes SMB uniquement ne prennent pas en charge la conversion en volumes NFS ou à double protocole après leur création.

Windows utilise Kerberos pour l'authentification par nom d'utilisateur avec les contrôleurs de domaine Active Directory, qui nécessitent un échange nom d'utilisateur/mot de passe avec les DCS AD, qui est externe à l'instance Cloud Volumes Service. L'authentification Kerberos est utilisée lors de l'utilisation de `\\SERVERNAME` Le chemin UNC est utilisé par les clients SMB et le suivant est vrai :

- L'entrée DNS A/AAAA existe pour NOM_SERVEUR
- Un code SPN valide pour l'accès SMB/CIFS existe pour NOM DE SERVEUR

Lorsqu'un volume SMB Cloud Volumes Service est créé, le nom du compte machine est créé comme défini dans la section "« Comment Cloud Volumes Service s'affiche dans Active Directory. »" Ce nom de compte machine devient également le chemin d'accès au partage SMB car Cloud Volumes Service utilise le DNS dynamique (DDNS) pour créer les entrées A/AAAA et PTR nécessaires dans le DNS et les entrées SPN nécessaires sur le principal du compte machine.

> Pour que les entrées PTR soient créées, la zone de recherche inversée de l'adresse IP de l'instance Cloud Volumes Service doit exister sur le serveur DNS.

Par exemple, ce volume Cloud Volumes Service utilise le chemin de partage UNC suivant : `\\cvs-east-433d.cvsdemo.local`.

Dans Active Directory, il s'agit des entrées SPN générées par le service Cloud volumes :

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Il s'agit du résultat de recherche DNS avant/arrière :

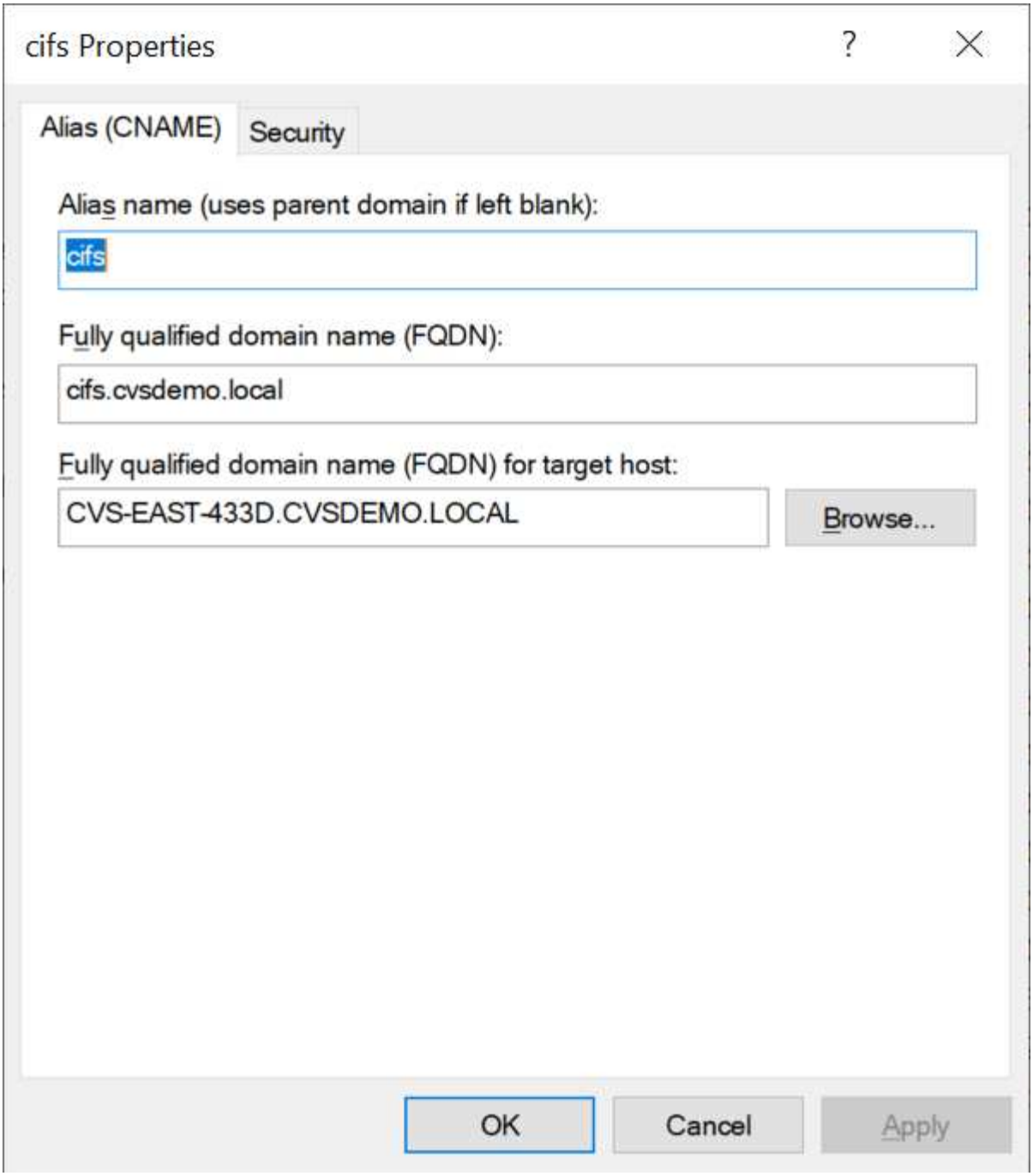
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Par ailleurs, un contrôle d'accès plus important peut être appliqué en activant/exigeant un chiffrement SMB pour les partages SMB dans Cloud Volumes Service. Si le chiffrement SMB n'est pas pris en charge par l'un des noeuds finaux, l'accès n'est pas autorisé.

Utilisation des alias de nom SMB

Dans certains cas, les utilisateurs finaux ne pourront pas connaître le nom du compte de la machine utilisé pour Cloud Volumes Service et ce, sans problèmes de sécurité. Dans d'autres cas, vous souhaiterez peut-être fournir aux utilisateurs un chemin d'accès plus simple. Dans ces cas, vous pouvez créer des alias SMB.

Si vous souhaitez créer des alias pour le chemin du partage SMB, vous pouvez exploiter ce qu'on appelle un enregistrement CNAME dans DNS. Par exemple, si vous souhaitez utiliser le nom `\\CIFS` pour accéder aux partages au lieu de `\\cvs-east- 433d.cvsdemo.local`, Mais vous souhaitez toujours utiliser l'authentification Kerberos, un CNAME dans DNS qui pointe vers l'enregistrement A/AAAA existant et un SPN supplémentaire ajouté au compte de machine existant fournit l'accès Kerberos.



Il s'agit du résultat de la recherche de transfert DNS après l'ajout d'un CNAME :

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Il s'agit de la requête SPN qui s'affiche après l'ajout de nouveaux SPN :

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Dans une capture de paquets, nous pouvons voir la demande de configuration de session en utilisant le SPN associé au CNAME.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
    name-type: kRB5-NT-SRV-INST (2)
    sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
enc-part
    etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Dialectes d'authentification SMB

Cloud Volumes Service prend en charge les éléments suivants "dialectes" Pour l'authentification SMB :

- LM
- NTLM
- NTLMv2
- Kerberos

L'authentification Kerberos pour l'accès au partage SMB est le niveau d'authentification le plus sécurisé que vous pouvez utiliser. Avec le cryptage AES et SMB activé, le niveau de sécurité est encore amélioré.

Cloud Volumes Service prend également en charge la rétrocompatibilité pour l'authentification LM et NTLM. Lorsque Kerberos est mal configuré (par exemple lors de la création d'alias SMB), l'accès au partage revient à des méthodes d'authentification plus faibles (telles que NTLMv2). Comme ces mécanismes sont moins sécurisés, ils sont désactivés dans certains environnements Active Directory. Si les méthodes d'authentification les plus faibles sont désactivées et que Kerberos n'est pas configuré correctement, l'accès au partage échoue car il n'existe pas de méthode d'authentification valide pour revenir à.

Pour plus d'informations sur la configuration/l'affichage des niveaux d'authentification pris en charge dans Active Directory, reportez-vous à la section "Sécurité du réseau : niveau d'authentification de LAN Manager".

Modèles d'autorisation

Autorisations NTFS/File

Les autorisations NTFS sont les autorisations appliquées aux fichiers et dossiers dans les systèmes de fichiers qui adhèrent à la logique NTFS. Vous pouvez appliquer des autorisations NTFS dans `Basic` ou `Advanced` et peut être défini sur `Allow` ou `Deny` pour le contrôle d'accès.

Les autorisations de base incluent les éléments suivants :

- Contrôle total
- Modifier
- Lecture et exécution
- Lecture
- Écriture

Lorsque vous définissez les autorisations d'un utilisateur ou d'un groupe, appelées ACE, elles résident dans une liste de contrôle d'accès. Les autorisations NTFS utilisent les mêmes principes de base en lecture/écriture/exécution que les bits du mode UNIX, mais elles peuvent également s'étendre à des contrôles d'accès plus granulaires et étendus (également appelés autorisations spéciales), tels que prendre propriété, Créer des dossiers/ajouter des données, écrire des attributs, etc.

Les bits standard du mode UNIX ne fournissent pas le même niveau de granularité que les autorisations NTFS (par exemple, la possibilité de définir des autorisations pour des objets individuels utilisateur et groupe dans une ACL ou la définition d'attributs étendus). Cependant, les listes de contrôle d'accès NFSv4.1 offrent les mêmes fonctionnalités que les listes de contrôle d'accès NTFS.

Les autorisations NTFS sont plus spécifiques que les autorisations de partage et peuvent être utilisées conjointement avec les autorisations de partage. Avec les structures d'autorisation NTFS, la plus restrictive s'applique. Ainsi, les refus explicites d'un utilisateur ou d'un groupe remplacent même le contrôle total lors de la définition des droits d'accès.

Les autorisations NTFS sont contrôlées à partir de clients SMB Windows.

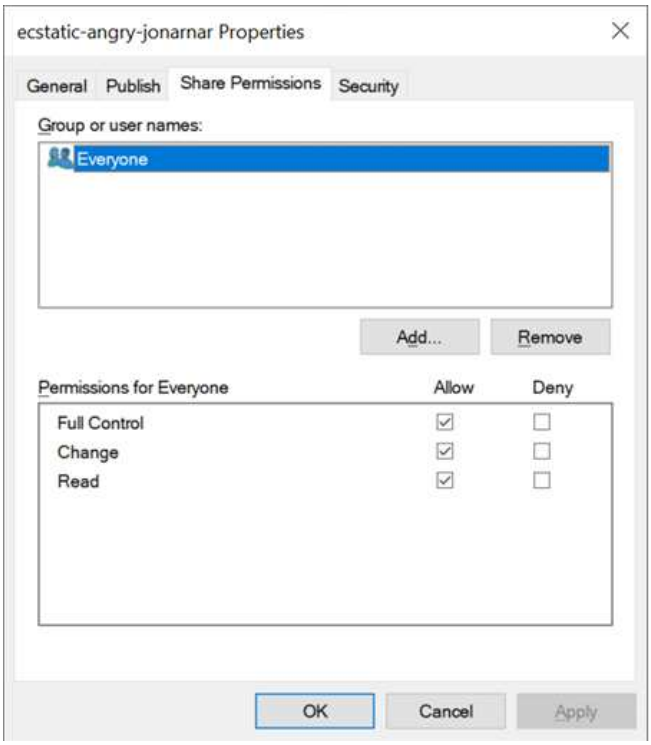
Partager les autorisations

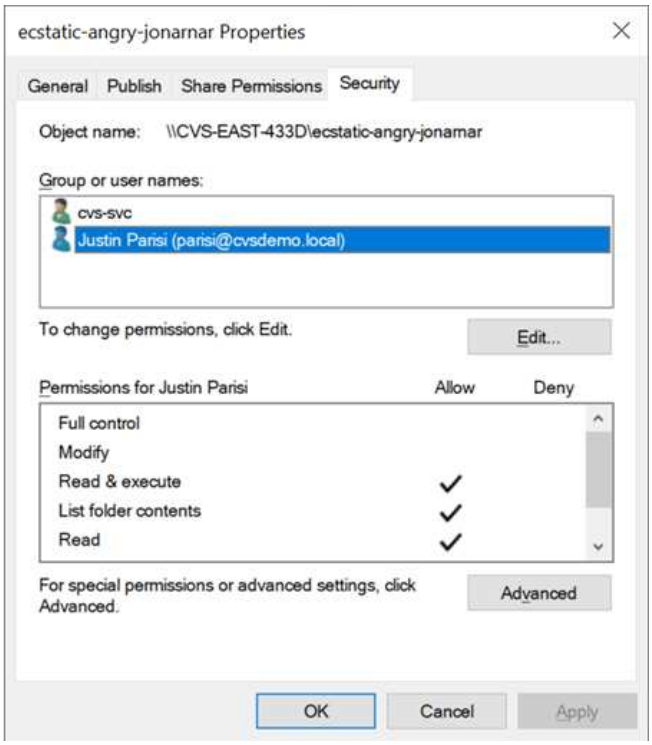
Les autorisations de partage sont plus générales que les autorisations NTFS (lecture/modification/contrôle total uniquement) et contrôlez l'entrée initiale dans un partage SMB, à l'instar des règles de règles d'export NFS.

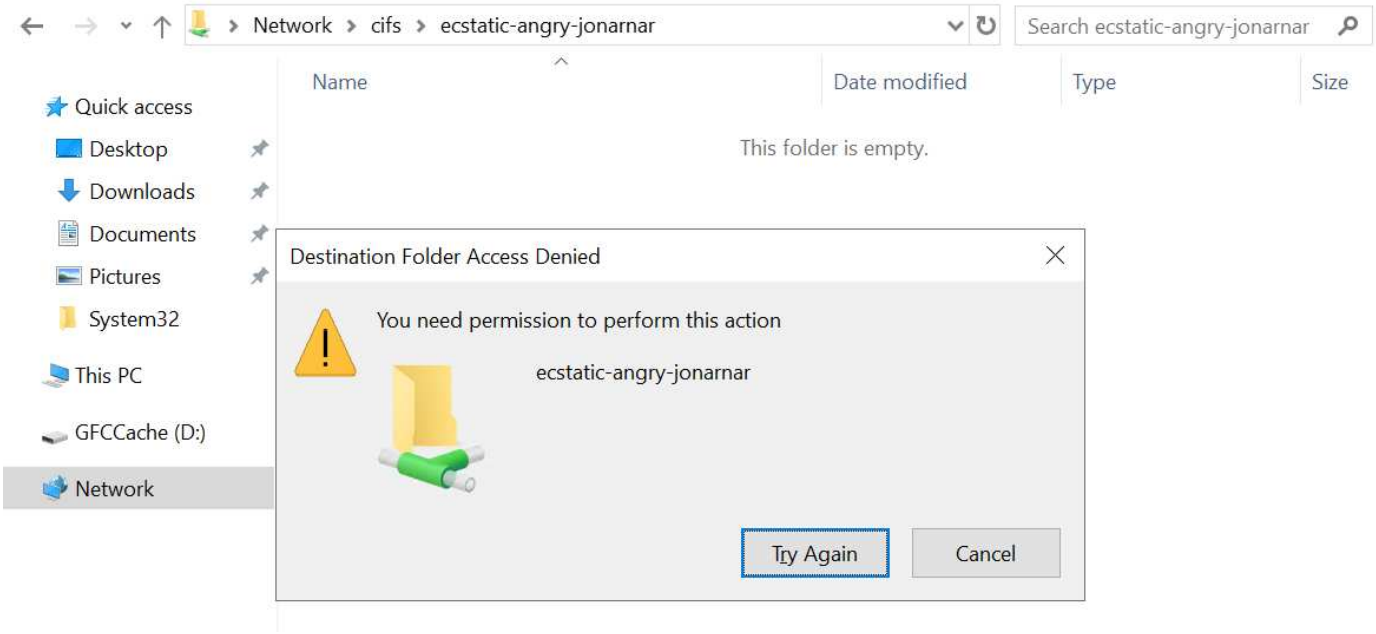
Bien que les règles d'export NFS contrôlent l'accès via des informations basées sur l'hôte telles que des adresses IP ou des noms d'hôte, les autorisations de partage SMB peuvent contrôler l'accès à l'aide d'ACE d'utilisateur et de groupe dans une liste de contrôle d'accès de partage. Vous pouvez définir des listes de contrôle d'accès de partage depuis le client Windows ou depuis l'interface utilisateur de gestion Cloud Volumes Service.

Par défaut, les listes de contrôle d'accès de partage et les listes de contrôle d'accès de volume initiales incluent tous les utilisateurs ayant un contrôle total. Les listes de contrôle d'accès du fichier doivent être modifiées, mais les autorisations de partage sont surdéfinies par les autorisations de fichier sur les objets du partage.

Par exemple, si un utilisateur n'est autorisé que l'accès en lecture à la liste de contrôle d'accès de fichier de volume Cloud Volumes Service, il est refusé d'accéder à la création de fichiers et de dossiers, même si la liste de contrôle d'accès du partage est définie sur tous les utilisateurs bénéficiant d'un contrôle total, comme indiqué dans la figure suivante.







Pour obtenir les meilleurs résultats en matière de sécurité, procédez comme suit :

- Supprimez tout le monde des listes de contrôle d'accès de partage et de fichiers et définissez plutôt l'accès de partage pour les utilisateurs ou les groupes.
- Pour faciliter la gestion des utilisateurs individuels, vous pouvez utiliser des groupes pour le contrôle d'accès, et pour accélérer la suppression et l'ajout d'utilisateurs pour partager ces listes via la gestion de groupes.
- Autorisez un accès plus général et moins restrictif au partage aux ACE depuis les autorisations de partage et verrouillez l'accès aux utilisateurs et aux groupes avec des autorisations de fichier pour un contrôle d'accès plus granulaire.
- Évitez l'utilisation générale des listes de contrôle d'accès de refus explicites, car elles remplacent les listes

de contrôle d'accès d'autorisation. Limiter l'utilisation des listes de contrôle d'accès de refus explicites pour les utilisateurs ou les groupes qui doivent être restreints rapidement d'un accès à un système de fichiers.

- Assurez-vous d'accorder votre attention au "Héritage ACL" paramètres lors de la modification des autorisations ; la définition de l'indicateur d'héritage au niveau supérieur d'un répertoire ou d'un volume avec un nombre élevé de fichiers signifie que chaque fichier sous ce répertoire ou volume possède des autorisations héritées ajoutées à celui-ci, ce qui peut créer un comportement indésirable tel qu'un accès/un refus involontaire et une longue perte de modification des autorisations au fur et à mesure que chaque fichier est ajusté.

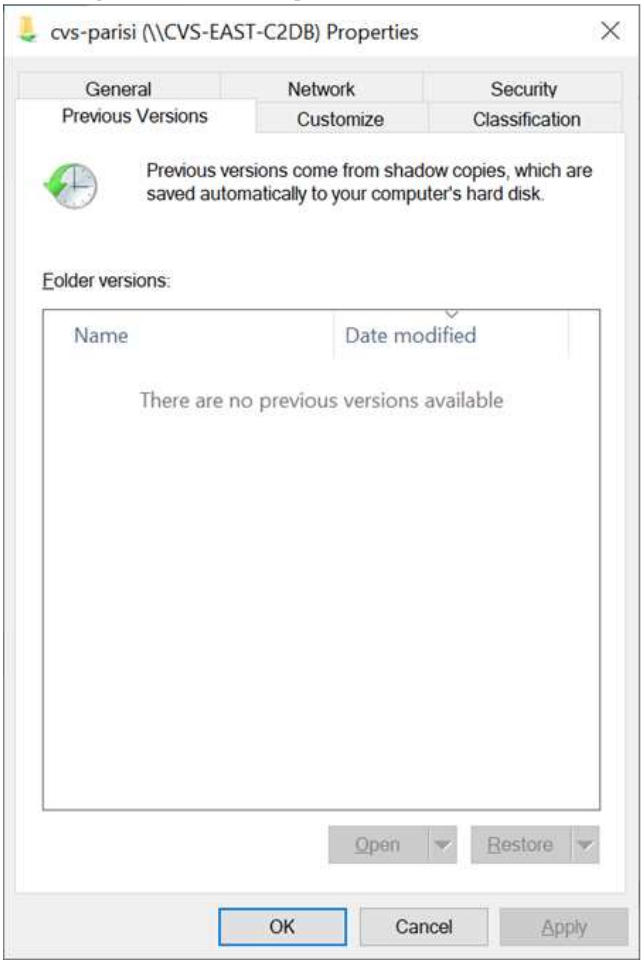
Fonctionnalités de sécurité de partage SMB

Lorsque vous créez un volume avec accès SMB dans Cloud Volumes Service pour la première fois, vous disposez d'une série d'options pour sécuriser ce volume.

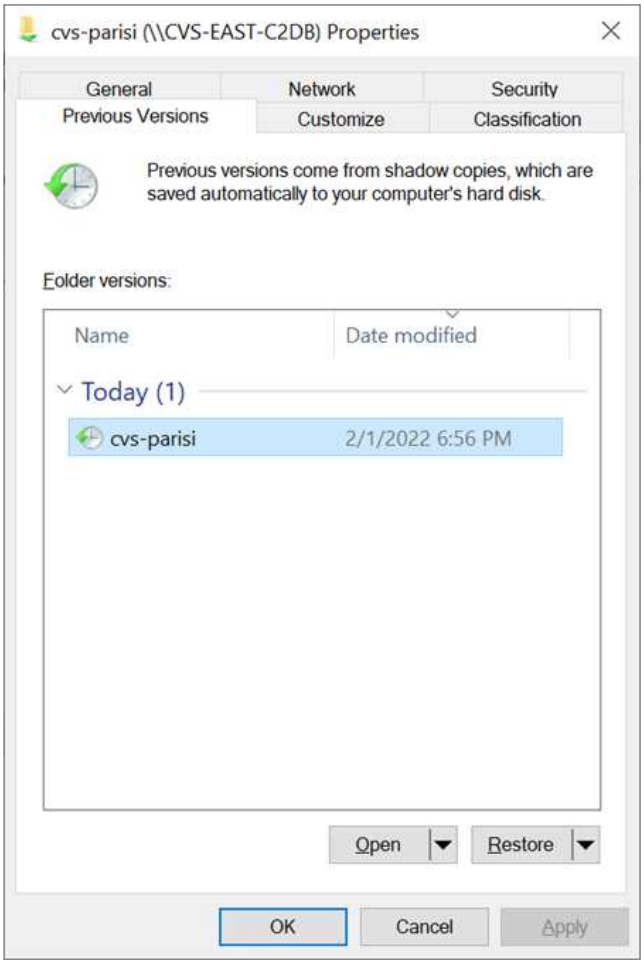
Les options suivantes dépendent du niveau Cloud Volumes Service (performances ou logiciels) et sont proposées :

- **Rendre le répertoire snapshot visible (disponible pour CVS-Performance et CVS-SW).** cette option permet de contrôler si les clients SMB peuvent accéder au répertoire snapshot dans un partage SMB (`\\server\share\~snapshot` Et/ou l'onglet versions précédentes). Le paramètre par défaut n'est pas coché, ce qui signifie que le volume par défaut est masqué et interdit l'accès au `~snapshot` Et aucune copie Snapshot n'apparaît dans l'onglet versions précédentes du volume.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Le masquage des copies Snapshot à partir des utilisateurs finaux peut être souhaité pour des raisons de

sécurité, de performances (masquage de ces dossiers à partir d'analyses antivirus) ou de préférence. Les snapshots Cloud Volumes Service sont en lecture seule. Par conséquent, même si ces snapshots sont visibles, les utilisateurs finaux ne peuvent pas supprimer ou modifier les fichiers dans le répertoire Snapshot. Autorisations liées aux fichiers ou dossiers au moment de la copie Snapshot. Si les autorisations d'un fichier ou d'un dossier changent entre les copies Snapshot, les modifications s'appliquent également aux fichiers ou dossiers du répertoire Snapshot. Les utilisateurs et les groupes peuvent accéder à ces fichiers ou dossiers en fonction des autorisations. Lorsque des suppressions ou des modifications de fichiers dans le répertoire Snapshot ne sont pas possibles, il est possible de copier des fichiers ou des dossiers à partir du répertoire Snapshot.

- **Activer le chiffrement SMB (disponible pour CVS-Performance et CVS-SW).** le chiffrement SMB est désactivé par défaut sur le partage SMB (non vérifié). La case active le chiffrement SMB, ce qui signifie que le trafic entre le client SMB et le serveur est crypté à la volée avec les niveaux de cryptage les plus élevés pris en charge négociés. Cloud Volumes Service prend en charge le chiffrement AES-256 pour SMB. L'activation du cryptage SMB a des retombées sur les performances de vos clients SMB, c'est-à-dire dans une plage de 10 à 20 %. NetApp encourage fortement les tests à vérifier si les performances sont acceptables.
- **Masquer le partage SMB (disponible pour CVS-Performance et CVS-SW).** définir cette option masque le chemin du partage SMB à partir de la navigation normale. Cela signifie que les clients qui ne connaissent pas le chemin du partage ne peuvent pas voir les partages lorsqu'ils accèdent au chemin UNC par défaut (par exemple `\\CVS-SMB`). Lorsque la case est cochée, seuls les clients qui connaissent explicitement le chemin du partage SMB ou qui ont le chemin du partage défini par un objet de stratégie de groupe peuvent y accéder (sécurité via obfuscation).
- **Activer l'énumération basée sur l'accès (ABE) (CVS-SW uniquement).** Ceci est similaire à masquer le partage SMB, sauf que les partages ou fichiers sont masqués uniquement des utilisateurs ou des groupes qui n'ont pas les autorisations d'accéder aux objets. Par exemple, si utilisateur Windows `joe` N'est pas autorisé au moins l'accès en lecture via les autorisations, puis l'utilisateur Windows `joe` Impossible de voir le partage SMB ou les fichiers. Cette option est désactivée par défaut et vous pouvez l'activer en cochant la case. Pour en savoir plus sur ABE, consultez l'article de la base de connaissances NetApp "Comment fonctionne l'énumération basée sur l'accès (ABE) ?"
- **Activer le support de partage disponible en continu (CA) (CVS-Performance uniquement).** "Partages SMB disponibles en permanence" Offrir un moyen de réduire les interruptions des applications lors des basculements en répliquant les États de verrouillage sur les nœuds du système back-end Cloud Volumes Service. Il ne s'agit pas d'une fonctionnalité de sécurité, mais elle offre une meilleure résilience globale. Actuellement, seules les applications SQL Server et FSLogix sont prises en charge pour cette fonctionnalité.

Partages masqués par défaut

Lorsqu'un serveur SMB est créé dans Cloud Volumes Service, il y a "partages administratifs masqués" (Avec la convention de nommage $) créées en plus du partage SMB du volume de données. Il s'agit notamment de C$ (accès à l'espace de noms) et IPC$ (partage de canaux nommés pour la communication entre les programmes, tels que les appels de procédure distante (RPC) utilisés pour l'accès à la console MMC (Microsoft Management Console)).

Le partage IPC$ ne contient pas de listes de contrôle d'accès partagées et ne peut pas être modifié – il est strictement utilisé pour les appels RPC et "Windows interdit l'accès anonyme à ces partages par défaut".

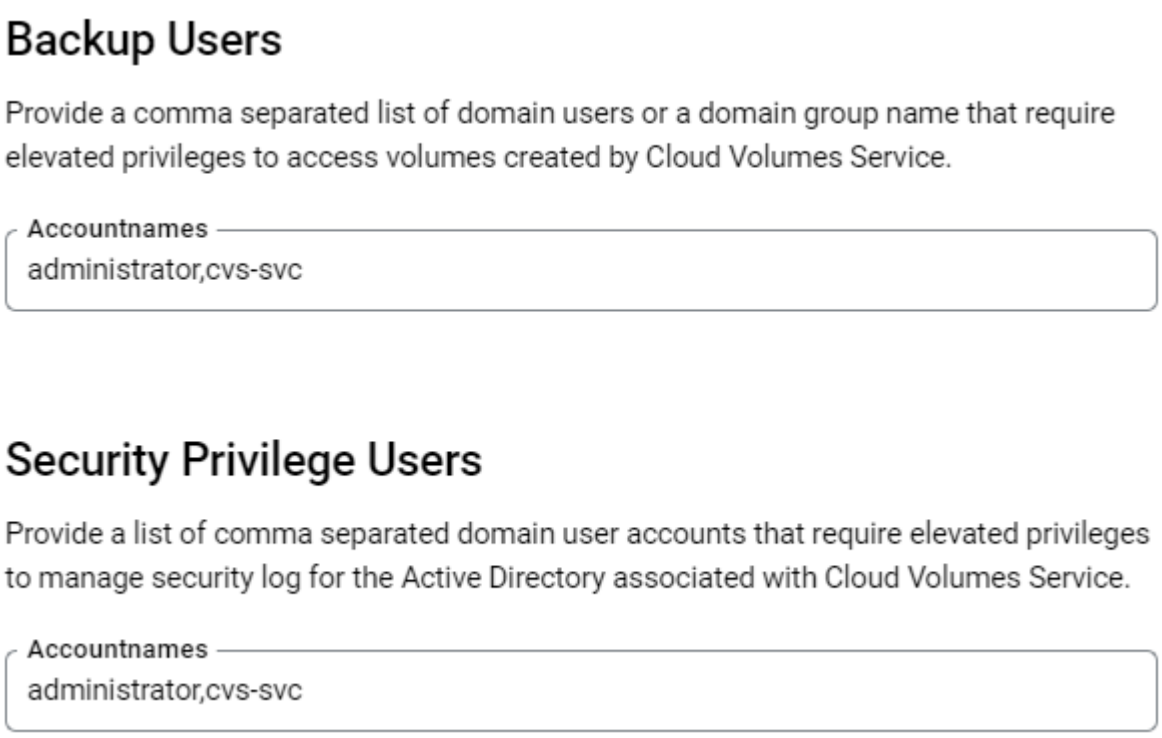
Le partage C$ permet l'accès par défaut à BUILTIN/Administrators, mais l'automatisation Cloud Volumes Service supprime la liste de contrôle d'accès de partage et n'autorise l'accès à personne car l'accès au partage C$ permet la visibilité de tous les volumes montés dans les systèmes de fichiers Cloud Volumes Service. Par conséquent, tente de naviguer vers `\\SERVER\C$` echec.

Comptes avec droits d'administrateur/de sauvegarde local/BUILTIN

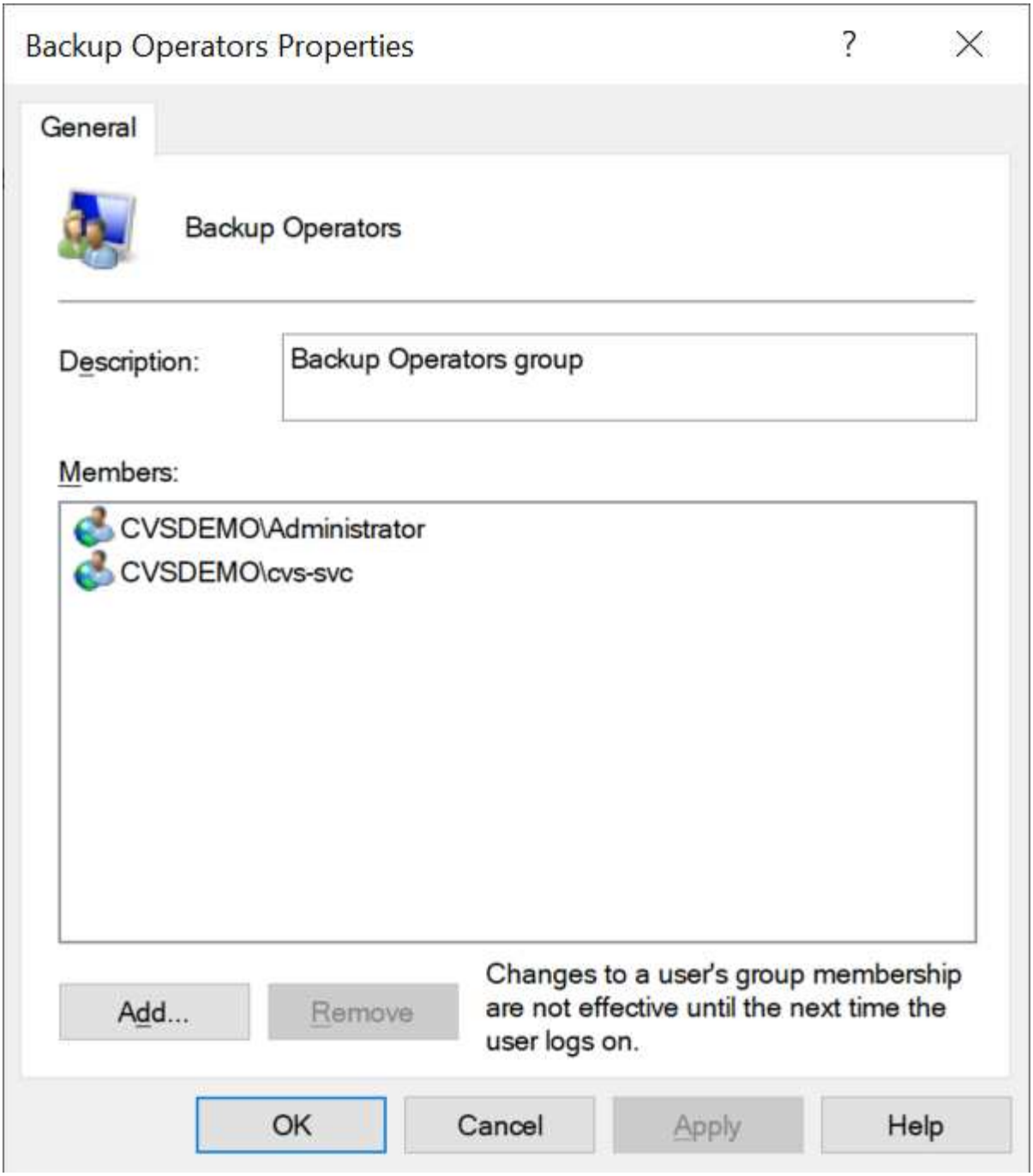
Les serveurs Cloud Volumes Service SMB conservent des fonctionnalités similaires aux serveurs Windows SMB classiques, dans la mesure où des groupes locaux (tels que BUILTIN\Administrators) appliquent des droits d'accès à certains utilisateurs et groupes de domaine.

Lorsque vous spécifiez un utilisateur à ajouter aux utilisateurs de sauvegarde, l'utilisateur est ajouté au groupe BULILTIN\opérateurs de sauvegarde de l'instance Cloud Volumes Service qui utilise cette connexion Active Directory, qui obtient ensuite le "SeBackupPrivilege et SeRestorePrivilege".

Lorsque vous ajoutez un utilisateur à des utilisateurs de privilèges de sécurité, l'utilisateur reçoit le privilège de sécurité, ce qui est utile dans certains cas d'utilisation d'application, tels que "SQL Server sur des partages SMB".



Vous pouvez afficher les membres du groupe local Cloud Volumes Service par l'intermédiaire de la console MMC avec les privilèges appropriés. La figure suivante montre les utilisateurs qui ont été ajoutés à l'aide de la console Cloud Volumes Service.

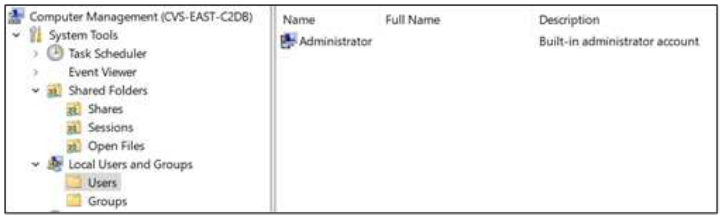


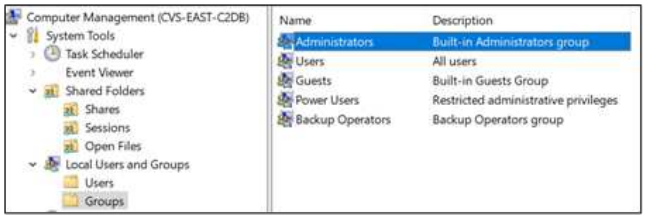
Le tableau suivant présente la liste des groupes par défaut BUILTIN et les utilisateurs/groupes ajoutés par défaut.

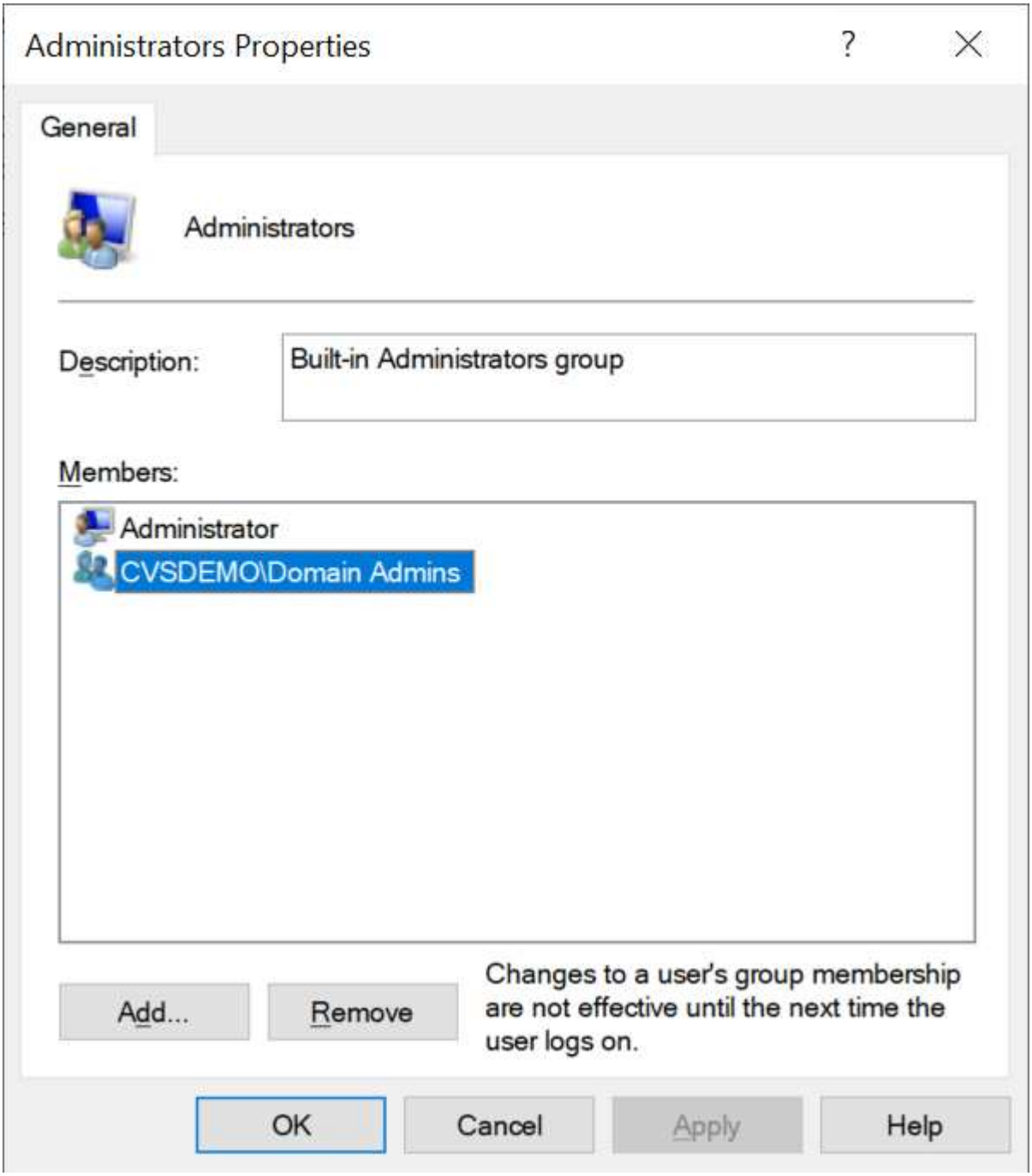
Groupe local/BUILTIN	Membres par défaut
INTÉGRÉ\administrateurs*	Administrateurs DE DOMAINE
INTÉGRÉ\opérateurs de sauvegarde*	Aucune
INTÉGRÉ\clients	Invités DOMAINE/domaine
UTILISATEURS INTENSIFS ET INTÉGRÉS	Aucune
Utilisateurs DE DOMAINE/INTÉGRÉ	Utilisateurs DU DOMAINE

*Appartenance au groupe contrôlée dans la configuration de connexion Cloud Volumes Service Active Directory.

Vous pouvez afficher des utilisateurs et des groupes locaux (et des membres de groupe) dans la fenêtre MMC, mais vous ne pouvez pas ajouter ou supprimer des objets ou modifier les appartenances de groupe à partir de cette console. Par défaut, seul le groupe administrateurs de domaine et l'administrateur sont ajoutés au groupe BULILTIN\Administrators dans Cloud Volumes Service. Actuellement, vous ne pouvez pas le modifier.







Accès MMC/gestion de l'ordinateur

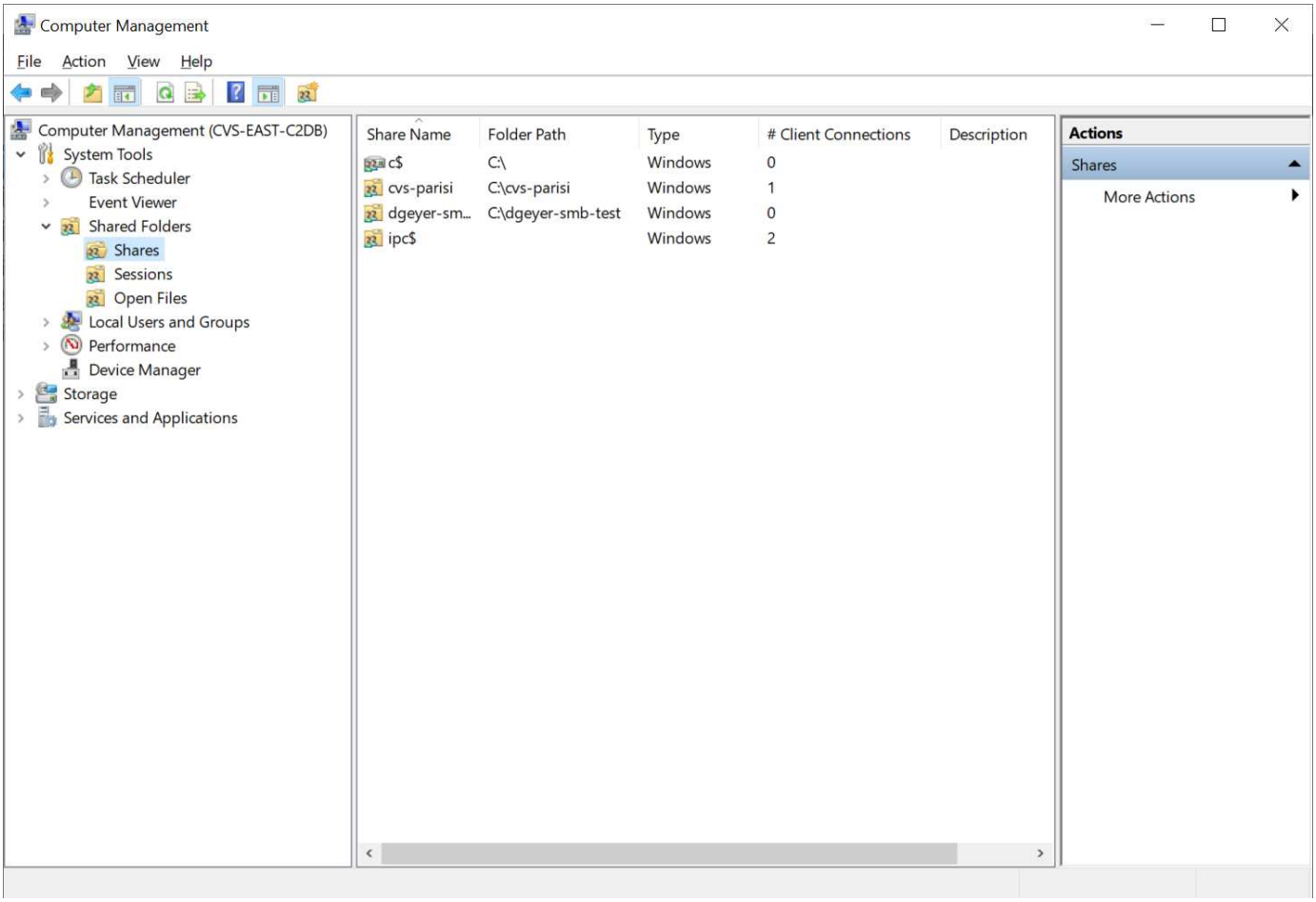
L'accès SMB dans Cloud Volumes Service fournit une connexion à la console MMC Computer Management, qui vous permet d'afficher les partages, de gérer les listes de contrôle d'accès de partage, d'afficher/gérer les sessions SMB et les fichiers ouverts.

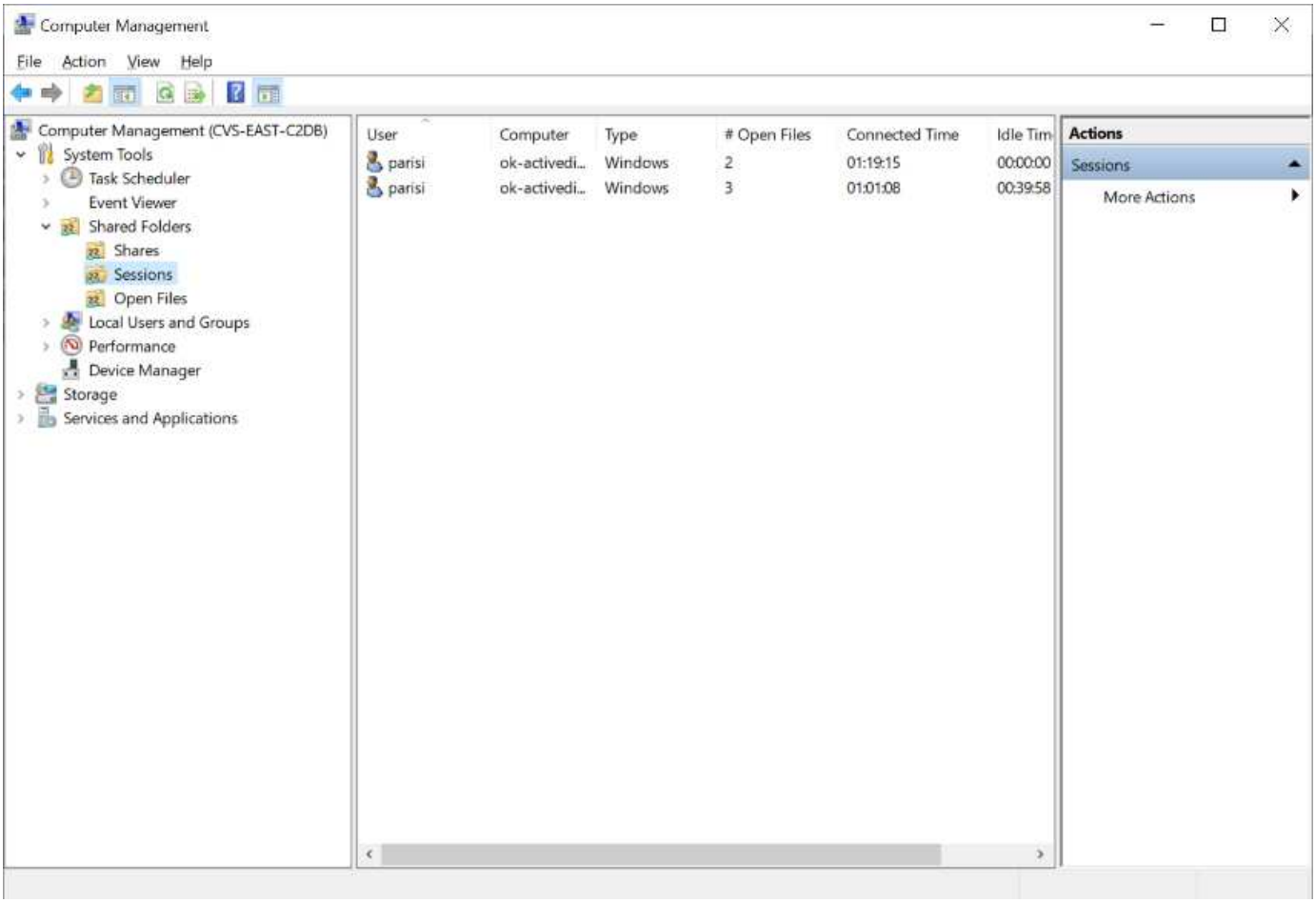
Pour utiliser la console MMC pour afficher les partages et sessions SMB dans Cloud Volumes Service, l'utilisateur connecté doit actuellement être un administrateur de domaine. Les autres utilisateurs sont autorisés à accéder à l'affichage ou à la gestion du serveur SMB à partir de MMC et reçoivent une boîte de dialogue vous n'avez pas d'autorisations lors de la tentative d'affichage de partages ou de sessions sur l'instance SMB de Cloud Volumes Service.

Pour vous connecter au serveur SMB, ouvrez gestion de l'ordinateur, cliquez avec le bouton droit de la souris sur gestion de l'ordinateur, puis sélectionnez connexion à un autre ordinateur. La boîte de dialogue Sélectionner un ordinateur s'ouvre, dans laquelle vous pouvez saisir le nom du serveur SMB (dans les informations sur le volume Cloud Volumes Service).

Lorsque vous affichez des partages SMB avec les autorisations appropriées, tous les partages disponibles de l'instance Cloud Volumes Service partageant la connexion Active Directory s'affichent. Pour contrôler ce comportement, définissez l'option Masquer les partages SMB sur l'instance de volume Cloud Volumes Service.

N'oubliez pas qu'une seule connexion Active Directory est autorisée par région.





Le tableau suivant présente la liste des fonctionnalités prises en charge/non prises en charge pour la console MMC.

Fonctions prises en charge	Fonctions non prises en charge
• Afficher les partages • Afficher les sessions SMB actives • Afficher les fichiers ouverts • Affichez les utilisateurs et groupes locaux • Afficher les membres du groupe local • Énumérer la liste des sessions, des fichiers et des connexions d'arborescence dans le système • Fermez les fichiers ouverts dans le système • Fermer les sessions ouvertes • Création/gestion de partages	• Création de nouveaux utilisateurs/groupes locaux • Gestion/affichage des utilisateurs/groupes locaux existants • Affichez les journaux d'événements ou de performances • La gestion du stockage • Gestion des services et des applications

Informations sur la sécurité du serveur SMB

Le serveur SMB de Cloud Volumes Service utilise un ensemble d'options qui définissent les stratégies de sécurité des connexions SMB, notamment l'inclinaison de l'horloge Kerberos, l'ancienneté des tickets, le cryptage, etc.

Le tableau suivant contient la liste de ces options, leur rôle et les configurations par défaut, si elles peuvent être modifiées avec Cloud Volumes Service. Certaines options ne s'appliquent pas à Cloud Volumes Service.

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Hauteur maximale de l'horloge Kerberos (minutes)	Décalage de temps maximal entre les contrôleurs Cloud Volumes Service et de domaine. Si l'écart de temps dépasse 5 minutes, l'authentification Kerberos échoue. Cette valeur est définie sur la valeur par défaut d'Active Directory.	5	Non
Durée de vie d'un ticket Kerberos (en heures)	Durée maximale pendant laquelle un ticket Kerberos reste valide avant d'exiger un renouvellement. Si aucun renouvellement n'a lieu avant les 10 heures, vous devez obtenir un nouveau billet. Cloud Volumes Service effectue automatiquement ces renouvellements. 10 heures est la valeur par défaut d'Active Directory.	10	Non
Renouvellement maximal de ticket Kerberos (jours)	Nombre maximum de jours pendant lesquels un ticket Kerberos peut être renouvelé avant qu'une nouvelle demande d'autorisation ne soit nécessaire. Cloud Volumes Service renouvelle automatiquement les billets pour les connexions des PME. Sept jours est la valeur par défaut d'Active Directory.	7	Non
Expiration du délai de connexion KDC Kerberos (secondes)	Nombre de secondes avant qu'une connexion KDC ne se soit interrompue.	3	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Signature requise pour le trafic SMB entrant	Paramètre pour exiger la signature pour le trafic SMB. Si la valeur est true, les clients qui ne prennent pas en charge la connexion échouent.	Faux	
Exiger la complexité du mot de passe pour les comptes d'utilisateur locaux	Utilisé pour les mots de passe des utilisateurs SMB locaux. Cloud Volumes Service ne prend pas en charge la création d'utilisateur local, donc cette option ne s'applique pas à Cloud Volumes Service.	Vrai	Non
Utilisez START_tls pour les connexions LDAP Active Directory	Utilisé pour activer les connexions TLS de démarrage pour Active Directory LDAP. Cloud Volumes Service ne prend pas encore en charge la mise en œuvre de cette fonctionnalité.	Faux	Non
Est compatible avec le chiffrement AES-128 et AES-256 pour Kerberos	Cette option permet de contrôler si le chiffrement AES est utilisé pour les connexions Active Directory et est contrôlé à l'aide de l'option Activer le chiffrement AES pour l'authentification Active Directory lors de la création/modification de la connexion Active Directory.	Faux	Oui.
Niveau de compatibilité LM	Niveau de dialectes d'authentification pris en charge pour les connexions Active Directory. Voir la section «Dialectes d'authentification SMB" pour plus d'informations.	ntlmv2-krb	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Cryptage SMB requis pour le trafic CIFS entrant	Chiffrement SMB requis pour tous les partages. Cette fonction n'est pas utilisée par Cloud Volumes Service ; définissez plutôt le chiffrement par volume (voir la section «Fonctionnalités de sécurité de partage SMB").	Faux	Non
Sécurité de la session client	Définit la signature et/ou le chiffrement pour la communication LDAP. Ce paramètre n'est pas actuellement défini dans Cloud Volumes Service mais peut être nécessaire dans les prochaines versions pour traiter . La résolution des problèmes d'authentification LDAP dus au correctif Windows est traitée dans la section ""Liaison de canal LDAP."".	Aucune	Non
SMB2 activé pour les connexions CC	Utilise SMB2 pour les connexions CC. Activé par défaut.	Système par défaut	Non
Poursuite des recommandations LDAP	Lors de l'utilisation de plusieurs serveurs LDAP, la recherche de références permet au client de se référer à d'autres serveurs LDAP de la liste lorsqu'une entrée est introuvable dans le premier serveur. Cette opération n'est actuellement pas prise en charge par Cloud Volumes Service.	Faux	Non
Utilisez LDAPS pour les connexions Active Directory sécurisées	Permet l'utilisation de LDAP sur SSL. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Le cryptage est requis pour la connexion CC	Nécessite un chiffrement pour des connexions CC réussies. Désactivé par défaut dans Cloud Volumes Service.	Faux	Non

Double protocole/multiprotocole

Cloud Volumes Service permet de partager les mêmes datasets avec les clients SMB et NFS tout en maintenant les autorisations d'accès adéquates ("double protocole"). Pour ce faire, le mappage d'identités entre les protocoles et un serveur LDAP back-end centralisé permettent de fournir les identités UNIX à Cloud Volumes Service. Vous pouvez utiliser Windows Active Directory pour fournir à la fois aux utilisateurs Windows et UNIX la facilité d'utilisation.

Contrôle d'accès

- **Partage des contrôles d'accès.** déterminer quels clients et/ou utilisateurs et groupes peuvent accéder à un partage NAS. Dans le cas de NFS, les export-policy et les règles contrôlent l'accès client aux exports. Les exportations NFS sont gérées à partir de l'instance Cloud Volumes Service. SMB utilise les partages CIFS/SMB et les listes de contrôle d'accès de partage pour fournir un contrôle plus granulaire au niveau de l'utilisateur et du groupe. Vous ne pouvez configurer des listes de contrôle d'accès au niveau du partage que depuis des clients SMB en utilisant "MMC/gestion de l'ordinateur" Avec un compte disposant de droits d'administrateur sur l'instance Cloud Volumes Service (voir la section "« Comptes avec droits d'administrateur/de sauvegarde local/BUILTIN. »").
- **Contrôles d'accès aux fichiers.** les autorisations de contrôle au niveau d'un fichier ou d'un dossier sont toujours gérées à partir du client NAS. Les clients NFS peuvent utiliser les bits de mode classiques (rwx) ou les listes de contrôle d'accès NFSv4. Les clients SMB exploitent les autorisations NTFS.

Le contrôle d'accès pour les volumes qui fournissent des données à la fois aux protocoles NFS et SMB dépend du protocole utilisé. Pour plus d'informations sur les autorisations avec double protocole, reportez-vous à la section «Modèle d'autorisation. »

Mappage d'utilisateurs

Lorsqu'un client accède à un volume, Cloud Volumes Service tente de mapper l'utilisateur entrant vers un utilisateur valide dans la direction opposée. Cela est nécessaire pour que l'accès soit déterminé dans l'ensemble des protocoles et pour s'assurer que l'utilisateur qui demande l'accès est bien celui qu'il prétend être.

Par exemple, si un utilisateur Windows nommé `joe` Tente d'accéder à un volume avec des autorisations UNIX via SMB, puis Cloud Volumes Service effectue une recherche pour trouver un utilisateur UNIX correspondant nommé `joe`. Le cas échéant, les fichiers qui sont écrits dans un partage SMB en tant qu'utilisateur Windows `joe` S'affiche en tant qu'utilisateur UNIX `joe` À partir de clients NFS.

Sinon, si un utilisateur UNIX nommé `joe` Tente d'accéder à un volume Cloud Volumes Service avec des autorisations Windows, puis l'utilisateur UNIX doit pouvoir mapper un utilisateur Windows valide. Dans le cas contraire, l'accès au volume est refusé.

Actuellement, seul Active Directory est pris en charge pour la gestion externe des identités UNIX avec LDAP. Pour plus d'informations sur la configuration de l'accès à ce service, reportez-vous à la section "Création d'une connexion AD".

Modèle d'autorisation

Lors de l'utilisation de configurations à double protocole, Cloud Volumes Service utilise des styles de sécurité pour les volumes afin de déterminer le type de liste de contrôle d'accès. Ces styles de sécurité sont définis en fonction du protocole NAS spécifié, ou dans le cas d'un double protocole, en fait l'option choisie au moment de la création du volume Cloud Volumes Service.

- Si vous utilisez uniquement NFS, les volumes Cloud Volumes Service utilisent des autorisations UNIX.
- Si vous utilisez uniquement SMB, les volumes Cloud Volumes Service utilisent des autorisations NTFS.

Si vous créez un volume à double protocole, vous pouvez choisir le style ACL lors de la création du volume. Cette décision doit être prise en fonction de la gestion des autorisations souhaitée. Si vos utilisateurs gèrent les autorisations des clients Windows/SMB, sélectionnez NTFS. Si vos utilisateurs préfèrent utiliser des clients NFS et chmod/chown, utilisez des styles de sécurité UNIX.

Considérations relatives à la création de connexions Active Directory

Cloud Volumes Service permet de connecter votre instance Cloud Volumes Service à un serveur Active Directory externe pour la gestion des identités tant pour les utilisateurs SMB que UNIX. La création d'une connexion Active Directory est nécessaire pour utiliser SMB dans Cloud Volumes Service.

La configuration offre plusieurs options qui nécessitent d'être prises en compte pour la sécurité. Le serveur Active Directory externe peut être une instance sur site ou un cloud natif. Si vous utilisez un serveur Active Directory sur site, n'exposez pas le domaine au réseau externe (par exemple avec une DMZ ou une adresse IP externe). Au lieu de cela, utilisez des tunnels privés sécurisés ou des VPN, des fiducies forestières à sens unique ou des connexions réseau dédiées aux réseaux sur site avec "Accès privé à Google". Consultez la documentation Google Cloud pour plus d'informations sur "Bonnes pratiques avec Active Directory dans Google Cloud".

> CVS-SW nécessite que les serveurs Active Directory soient situés dans la même région. Si une connexion CC est tentée dans CVS-SW vers une autre région, la tentative échoue. Lorsque vous utilisez CVS-SW, veillez à créer des sites Active Directory incluant les DCS Active Directory, puis spécifiez des sites dans Cloud Volumes Service pour éviter les tentatives de connexion CC entre régions.

Informations d'identification Active Directory

Lorsque SMB ou LDAP pour NFS est activé, Cloud Volumes Service interagit avec les contrôleurs Active Directory pour créer un objet de compte de machine à utiliser pour l'authentification. Ce n'est pas différent de la façon dont un client SMB Windows rejoint un domaine et nécessite les mêmes droits d'accès aux unités organisationnelles (UO) dans Active Directory.

Dans de nombreux cas, les groupes de sécurité n'autorisent pas l'utilisation d'un compte administrateur Windows sur des serveurs externes tels que Cloud Volumes Service. Dans certains cas, l'utilisateur de l'administrateur Windows est entièrement désactivé en tant que meilleure pratique de sécurité.

Autorisations nécessaires pour créer des comptes de machine SMB

Pour ajouter des objets machine Cloud Volumes Service à un Active Directory, un compte qui possède des droits d'administration sur le domaine ou a "autorisations déléguées pour créer et modifier des objets de compte machine" À une UO spécifiée est nécessaire. Pour ce faire, vous pouvez créer une tâche personnalisée avec l'assistant délégation de contrôle d'Active Directory qui fournit un accès utilisateur à la création/suppression d'objets d'ordinateur avec les autorisations d'accès suivantes :

- Lecture/écriture
- Créer/Supprimer tous les objets enfants
- Lire/écrire toutes les propriétés
- Modifier/Réinitialiser le mot de passe

Cette opération ajoute automatiquement une liste de contrôle d'accès de sécurité pour l'utilisateur défini à l'UO dans Active Directory et réduit l'accès à l'environnement Active Directory. Après la délégation d'un utilisateur, ce nom d'utilisateur et ce mot de passe peuvent être fournis en tant qu'informations d'identification Active Directory dans cette fenêtre.

> Le nom d'utilisateur et le mot de passe transmis au domaine Active Directory exploitent le chiffrement Kerberos lors de la requête et de la création d'objet de compte machine pour une sécurité supplémentaire.

Détails de la connexion à Active Directory

Le "Détails de connexion Active Directory" Indiquez les champs permettant aux administrateurs de fournir des informations spécifiques sur le schéma Active Directory pour le placement de compte machine, par exemple :

- **Type de connexion Active Directory.** utilisé pour spécifier si la connexion Active Directory dans une région est utilisée pour les volumes de type de service Cloud Volumes Service ou CVS-Performance. Si ce paramètre n'est pas défini correctement sur une connexion existante, il est possible qu'il ne fonctionne pas correctement lorsqu'il est utilisé ou modifié.
- **Domaine.** le nom de domaine Active Directory.
- **Site.** limite les serveurs Active Directory à un site spécifique pour la sécurité et les performances "considérations". Ceci est nécessaire lorsque plusieurs serveurs Active Directory s'étendent sur des régions car Cloud Volumes Service ne prend pas en charge actuellement l'autorisation d'autoriser les requêtes d'authentification Active Directory à des serveurs Active Directory dans une région différente de celle de l'instance Cloud Volumes Service. (Par exemple, le contrôleur de domaine Active Directory se trouve dans une région qui ne prend en charge que CVS-Performance mais vous voulez un partage SMB dans une instance CVS-SW.)
- **Serveurs DNS.** serveurs DNS à utiliser dans les recherches de noms.
- **Nom NetBIOS (facultatif).** si vous le souhaitez, le nom NetBIOS du serveur. Ce qui est utilisé lorsque de nouveaux comptes machine sont créés à l'aide de la connexion Active Directory. Par exemple, si le nom NetBIOS est défini sur CVS-EAST, les noms des comptes machine seront CVS-EAST-{1234}. Voir la section "Comment Cloud Volumes Service s'affiche dans Active Directory" pour en savoir plus.
- **Unité organisationnelle (UO).** l'UO spécifique pour créer le compte d'ordinateur. Ceci est utile si vous déléguez le contrôle à un utilisateur pour les comptes machine à une unité d'organisation spécifique.
- **Cryptage AES.** vous pouvez également cocher ou décocher la case Activer le cryptage AES pour l'authentification AD. L'activation du cryptage AES pour l'authentification Active Directory offre une sécurité supplémentaire pour la communication entre Cloud Volumes Service et Active Directory au cours des recherches utilisateur et de groupe. Avant d'activer cette option, vérifiez auprès de votre administrateur de

domaine que les contrôleurs de domaine Active Directory prennent en charge l'authentification AES.

> Par défaut, la plupart des serveurs Windows ne désactivent pas les chiffrements plus faibles (tels QUE DES ou RC4-HMAC), mais si vous choisissez de désactiver les chiffrements plus faibles, confirmez que la connexion Cloud Volumes Service Active Directory a été configurée pour activer AES. Dans le cas contraire, des échecs d'authentification se produisent. L'activation du cryptage AES ne désactive pas les chiffrements plus faibles mais ajoute au contraire la prise en charge du chiffrement AES au compte de la machine Cloud Volumes Service SMB.

Détails du domaine Kerberos

Cette option ne s'applique pas aux serveurs SMB. Elles sont plutôt utilisées lors de la configuration de Kerberos par NFS pour le système Cloud Volumes Service. Lorsque ces informations sont renseignées, le domaine Kerberos NFS est configuré (similaire à un fichier krb5.conf sous Linux) et utilisé lorsque NFS Kerberos est spécifié dans la création du volume Cloud Volumes Service, car la connexion Active Directory fait office de centre de distribution Kerberos NFS (KDC).

> Actuellement, les KDC non Windows ne sont pas pris en charge pour une utilisation avec Cloud Volumes Service.

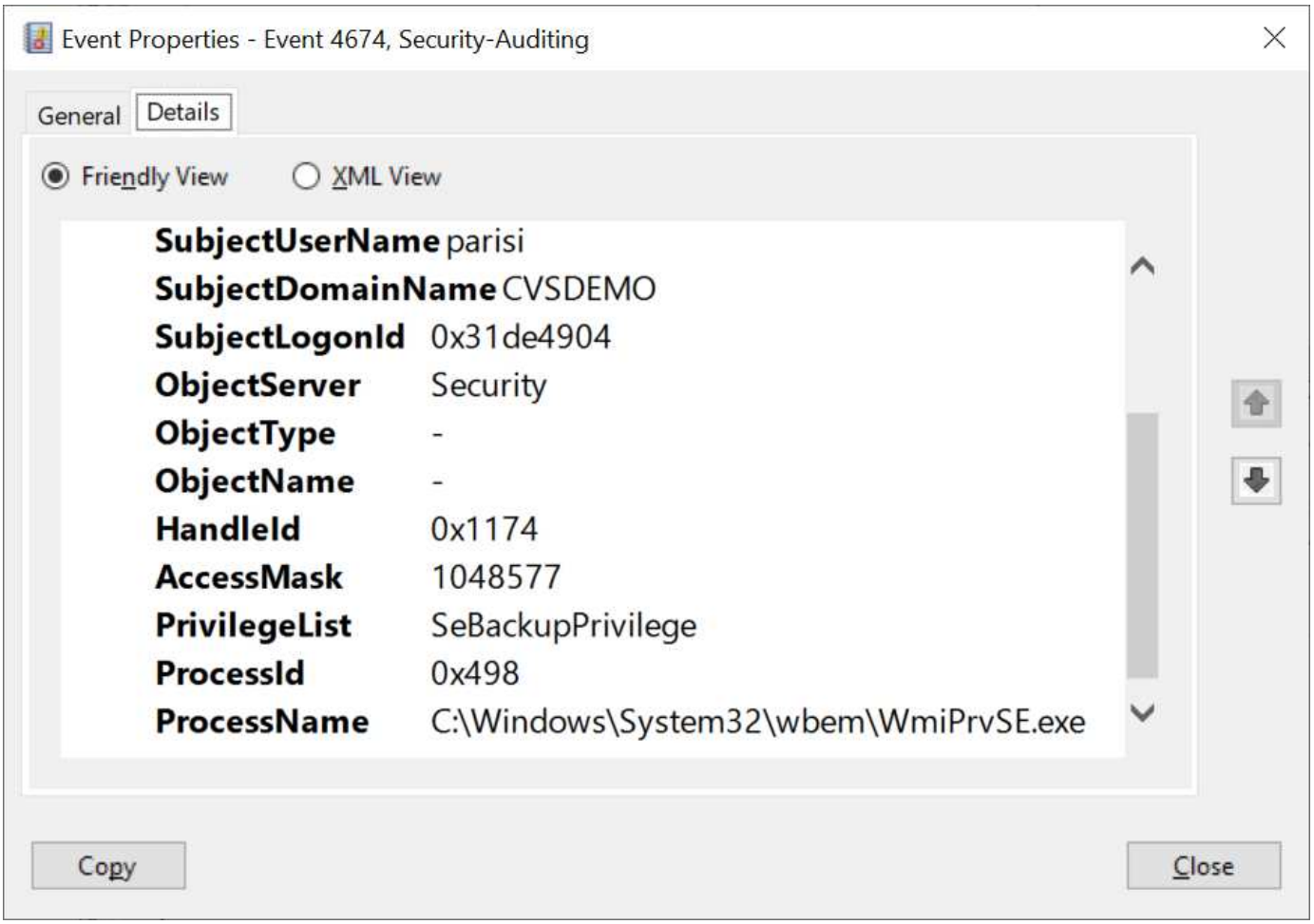
Région

Une région vous permet de spécifier l'emplacement où réside la connexion Active Directory. Cette région doit être la même région que le volume Cloud Volumes Service.

- **Utilisateurs NFS locaux avec LDAP.** dans cette section, il existe également une option permettant aux utilisateurs NFS locaux avec LDAP. Cette option doit être désélectionnée si vous souhaitez étendre votre prise en charge d'appartenance à un groupe d'utilisateurs UNIX au-delà de la limite de 16 groupes de NFS (groupes étendus). Cependant, l'utilisation de groupes étendus nécessite un serveur LDAP configuré pour les identités UNIX. Si vous ne disposez pas d'un serveur LDAP, laissez cette option non sélectionnée. Si vous disposez d'un serveur LDAP et souhaitez également utiliser des utilisateurs UNIX locaux (comme root), sélectionnez cette option.

Utilisateurs de la sauvegarde

Cette option vous permet de spécifier les utilisateurs Windows disposant d'autorisations de sauvegarde sur le volume Cloud Volumes Service. Les privilèges de sauvegarde (SeBackupPrivilege) sont nécessaires pour que certaines applications puissent sauvegarder et restaurer correctement les données dans des volumes NAS. Cet utilisateur dispose d'un haut niveau d'accès aux données du volume. Vous devez donc tenir compte de cet aspect "activation de l'audit de cet accès utilisateur". Une fois activée, les événements d'audit s'affichent dans Event Viewer > Windows Logs > Security.



Utilisateurs disposant des privilèges de sécurité

Cette option vous permet de spécifier les utilisateurs Windows disposant d'autorisations de modification de sécurité pour le volume Cloud Volumes Service. Des privilèges de sécurité (SeSecurityPrivilege) sont nécessaires pour certaines applications ("Tels que SQL Server") pour définir correctement les autorisations lors de l'installation. Ce privilège est nécessaire pour gérer le journal de sécurité. Bien que ce privilège ne soit pas aussi puissant que SeBackupPrivilege, NetApp recommande "audit de l'accès des utilisateurs" avec ce niveau de privilège, le cas échéant.

Pour plus d'informations, voir "Privilèges spéciaux attribués à la nouvelle connexion".

Comment Cloud Volumes Service s'affiche dans Active Directory

Cloud Volumes Service apparaît dans Active Directory comme un objet de compte machine normal. Les conventions de nom sont les suivantes.

- CIFS/SMB et NFS Kerberos créent des objets de compte de machine distincts.
- Le protocole NFS avec LDAP activé crée un compte machine dans Active Directory pour les liaisons LDAP Kerberos.
- Les volumes à double protocole avec LDAP partagent le compte de machine CIFS/SMB pour LDAP et SMB.
- Les comptes de machine CIFS/SMB utilisent une convention de dénomination de NOM-1234 (identifiant aléatoire à quatre chiffres avec tiret ajouté à <10 caractères name) pour le compte de machine. Vous pouvez définir LE NOM à l'aide du paramètre Nom NetBIOS de la connexion Active Directory (voir la

section «Détails de la connexion à Active Directory”).

- NFS Kerberos utilise NFS-NAME-1234 comme convention de nommage (15 caractères au maximum). Si plus de 15 caractères sont utilisés, le nom est NFS-TRONQUÉ-NAME-1234.
- Les instances CVS-Performance uniquement avec LDAP activées créent un compte de machine SMB pour la liaison au serveur LDAP avec la même convention de nommage que les instances CIFS/SMB.
- Lorsqu’un compte de machine SMB est créé, les partages admin masqués par défaut (voir la section "« Partages masqués par défaut »") Sont également créés (c$, admin$, ipc$), mais ces partages n’ont pas de listes de contrôle d’accès attribuées et sont inaccessibles.
- Les objets de compte machine sont placés par défaut dans CN=Computers, mais un vous pouvez spécifier une autre UO si nécessaire. Voir la section «Autorisations nécessaires pour créer des comptes de machine SMB” Pour plus d’informations sur les droits d’accès nécessaires pour ajouter/supprimer des objets de compte machine pour Cloud Volumes Service.

Lorsque Cloud Volumes Service ajoute le compte de machine SMB à Active Directory, les champs suivants sont renseignés :

- cn (avec le nom de serveur SMB spécifié)
- DnsHostName (avec SMBserver.domain.com)
- MSDS-SupportedEncryptionTypes (autorise LES_CBC_MD5, RC4_HMAC_MD5 si le chiffrement AES n’est pas activé ; si le chiffrement AES est activé, DES_CBC_MD5, RC4_HMAC_MD5, AES128_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1 est autorisé pour l’échange avec le compte SMB_96)
- Nom (avec le nom du serveur SMB)
- SAMAccountName (avec SMBserver$)
- ServicePrincipalName (avec hôte/smbserver.domain.com et SPN hôte/smbserver pour Kerberos)

Si vous souhaitez désactiver les types de cryptage Kerberos les plus faibles (type d’enc) sur le compte de la machine, vous pouvez modifier la valeur MSDS-SupportedEncryptionTypes sur le compte de la machine à l’une des valeurs du tableau suivant pour n’autoriser que AES.

MSDS-SupportedEncryptionTypes valeur	Type d’encan activé
2	DES_CBC_MD5
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96 UNIQUEMENT
16	AES256_CTS_HMAC_SHA1_96 UNIQUEMENT
24	AES128_CTS_HMAC_SHA1_96 ET AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 ET AES256_CTS_HMAC_SHA1_96

Pour activer le cryptage AES pour les comptes de machine SMB, cliquez sur Activer le cryptage AES pour l’authentification AD lors de la création de la connexion Active Directory.

Pour activer le chiffrement AES pour NFS Kerberos, "Consultez la documentation Cloud Volumes Service".

Autres dépendances des services d'infrastructure NAS (KDC, LDAP et DNS)

Lorsque vous utilisez Cloud Volumes Service pour les partages NAS, certaines dépendances externes peuvent être requises pour assurer le bon fonctionnement des partages. Ces dépendances sont en jeu dans des circonstances spécifiques. Le tableau suivant présente différentes options de configuration et le cas échéant, quelles dépendances sont nécessaires.

Configuration	Dépendances requises
NFSv3 uniquement	Aucune
Kerberos NFSv3 uniquement	Windows Active Directory : * KDC * DNS * LDAP
NFSv4.1 uniquement	Configuration du mappage d'ID client (/etc/idmap.conf)
NFSv4.1 Kerberos uniquement	• Configuration du mappage d'ID client (/etc/idmap.conf) • Windows Active Directory : LDAP KDC DNS
PME uniquement	Active Directory : * KDC * DNS
NAS multiprotocole (NFS et SMB)	• Configuration du mappage des ID client (NFSv4.1 uniquement ; /etc/idmap.conf) • Windows Active Directory : LDAP KDC DNS

La rotation/mot de passe de l'onglet clé Kerberos est réinitialisée pour les objets du compte machine

Avec les comptes machine SMB, Cloud Volumes Service planifie régulièrement les réinitialisations de mots de passe pour le compte machine SMB. Ces réinitialisations de mot de passe se produisent à l'aide du chiffrement Kerberos et fonctionnent sur une programmation de tous les 4 dimanches à une heure aléatoire comprise entre 23 H et 1 H. Ces réinitialisations de mot de passe modifient les versions de clé Kerberos, font pivoter les onglets enregistrés sur le système Cloud Volumes Service et permettent de maintenir un niveau de sécurité supérieur pour les serveurs SMB exécutés dans Cloud Volumes Service. Les mots de passe du compte machine sont randomisés et ne sont pas connus des administrateurs.

Pour les comptes de machine Kerberos NFS, les réinitialisations de mot de passe n'ont lieu que lorsqu'un nouveau keytab est créé/échangé avec le KDC. Actuellement, il n'est pas possible de le faire dans Cloud Volumes Service.

Ports réseau à utiliser avec LDAP et Kerberos

Lorsque vous utilisez LDAP et Kerberos, vous devez déterminer les ports réseau utilisés par ces services. La liste complète des ports utilisés par Cloud Volumes Service se trouve dans le "Documentation Cloud Volumes Service sur les considérations de sécurité".

LDAP

Cloud Volumes Service agit comme un client LDAP et utilise des requêtes de recherche LDAP standard pour les recherches utilisateur et de groupe pour les identités UNIX. LDAP est nécessaire si vous avez l'intention d'utiliser des utilisateurs et des groupes en dehors des utilisateurs standard par défaut fournis par Cloud Volumes Service. LDAP est également nécessaire si vous prévoyez d'utiliser NFS Kerberos avec des

principes utilisateur (tels que user1@domain.com). Actuellement, seul LDAP utilisant Microsoft Active Directory est pris en charge.

Pour utiliser Active Directory en tant que serveur LDAP UNIX, vous devez renseigner les attributs UNIX nécessaires pour les utilisateurs et groupes que vous souhaitez utiliser pour les identités UNIX. Cloud Volumes Service utilise un modèle de schéma LDAP par défaut qui interroge les attributs sur la base "RFC-2307-bis". Par conséquent, le tableau suivant montre les attributs Active Directory minimum requis pour remplir pour les utilisateurs et les groupes et pour quels attributs sont utilisés.

Pour plus d'informations sur la définition des attributs LDAP dans Active Directory, reportez-vous à la section "Gestion de l'accès double protocole."

Attribut	Ce qu'il fait
uid*	Spécifie le nom d'utilisateur UNIX
Numéro uidNumber*	Spécifie l'ID numérique de l'utilisateur UNIX
Numéro gidNumber*	Spécifie l'ID numérique du groupe principal de l'utilisateur UNIX
Objectclass*	Spécifie le type d'objet utilisé ; Cloud Volumes Service nécessite que "user" soit inclus dans la liste des classes d'objets (inclus dans la plupart des déploiements Active Directory par défaut).
nom	Informations générales sur le compte (nom réel, numéro de téléphone, etc., également connu sous le nom de gecos)
Mot de passe unixUserPassword	Inutile de le définir ; non utilisé dans les recherches d'identité UNIX pour l'authentification NAS. Cette option place la valeur unixUserPassword configurée dans le texte en texte clair.
UnixHomeDirectory	Définit le chemin d'accès aux répertoires locaux UNIX lorsqu'un utilisateur s'authentifie auprès de LDAP à partir d'un client Linux. Définissez cette option si vous souhaitez utiliser la fonctionnalité de répertoire local LDAP pour UNIX.
LoginShell	Définit le chemin d'accès au shell bash/de profil pour les clients Linux lorsqu'un utilisateur s'authentifie auprès de LDAP.

*L'attribut Denotes est requis pour une fonctionnalité correcte avec Cloud Volumes Service. Les autres attributs sont uniquement destinés à un usage côté client.

Attribut	Ce qu'il fait
cn*	Spécifie le nom du groupe UNIX. Lors de l'utilisation d'Active Directory pour LDAP, ce paramètre est défini lors de la création de l'objet, mais il peut être modifié ultérieurement. Ce nom ne peut pas être identique à celui des autres objets. Par exemple, si votre utilisateur UNIX nommé user1 appartient à un groupe nommé user1 sur votre client Linux, Windows n'autorise pas deux objets avec le même attribut cn. Pour contourner ce problème, renommez l'utilisateur Windows en un nom unique (tel que user1-UNIX) ; LDAP dans Cloud Volumes Service utilise l'attribut uid pour les noms d'utilisateur UNIX.
Numéro gidNumber*	Spécifie l'ID numérique du groupe UNIX.
Objectclass*	Indique le type d'objet utilisé ; Cloud Volumes Service nécessite que le groupe soit inclus dans la liste des classes d'objets (cet attribut est inclus par défaut dans la plupart des déploiements Active Directory).
MemberUid	Indique quels utilisateurs UNIX sont membres du groupe UNIX. Avec Active Directory LDAP dans Cloud Volumes Service, ce champ n'est pas nécessaire. Le schéma LDAP Cloud Volumes Service utilise le champ membre pour les appartenances de groupe.
Membre*	Requis pour les membres de groupe/groupes UNIX secondaires. Ce champ est rempli en ajoutant des utilisateurs Windows aux groupes Windows. Cependant, si les attributs UNIX des groupes Windows ne sont pas renseignés, ils ne sont pas inclus dans les listes d'appartenance aux groupes de l'utilisateur UNIX. Tous les groupes devant être disponibles dans NFS doivent remplir les attributs de groupe UNIX requis répertoriés dans ce tableau.

*L'attribut Denotes est requis pour une fonctionnalité correcte avec Cloud Volumes Service. Les autres attributs sont uniquement destinés à un usage côté client.

Informations de liaison LDAP

Pour interroger les utilisateurs dans LDAP, Cloud Volumes Service doit se lier (connexion) au service LDAP. Cette connexion possède des autorisations en lecture seule et est utilisée pour interroger les attributs LDAP UNIX pour les recherches de répertoire. Actuellement, les liaisons LDAP ne sont possibles qu'à l'aide d'un compte de machine SMB.

Vous pouvez uniquement activer LDAP pour `CVS-Performance` Instances et s'utilisent pour les volumes NFS v3, NFS v4.1 ou double protocole. Une connexion Active Directory doit être établie dans la même région que le volume Cloud Volumes Service pour le déploiement réussi du volume LDAP.

Lorsque LDAP est activée, les opérations suivantes se produisent dans des scénarios spécifiques.

- Si seul NFSv3 ou NFSv4.1 est utilisé pour le projet Cloud Volumes Service, un nouveau compte machine est créé dans le contrôleur de domaine Active Directory et le client LDAP dans Cloud Volumes Service se

lie à Active Directory à l'aide des informations d'identification du compte machine. Aucun partage SMB n'est créé pour le volume NFS et les partages administratifs masqués par défaut (voir la section "« Partages masqués par défaut »") Ont supprimé les ACL de partage.

- Si des volumes à double protocole sont utilisés pour le projet Cloud Volumes Service, seul le compte de machine unique créé pour l'accès SMB est utilisé pour lier le client LDAP de Cloud Volumes Service à Active Directory. Aucun compte machine supplémentaire n'est créé.
- Si des volumes SMB dédiés sont créés séparément (avant ou après l'activation des volumes NFS avec LDAP), le compte machine pour les liaisons LDAP est partagé avec le compte de machine SMB.
- Si NFS Kerberos est également activé, deux comptes machine sont créés : un pour les partages SMB et/ou des liaisons LDAP et un pour l'authentification Kerberos NFS.

Requêtes LDAP

Bien que les liaisons LDAP soient cryptées, les requêtes LDAP sont transmises sur le réseau en texte clair à l'aide du port LDAP commun 389. Ce port connu ne peut actuellement pas être modifié dans Cloud Volumes Service. Par conséquent, une personne ayant accès au sniffing de paquets dans le réseau peut voir les noms d'utilisateur et de groupe, les ID numériques et les appartenances de groupe.

Cependant, les machines virtuelles Google Cloud ne peuvent pas sniff le trafic unicast d'autres machines virtuelles. Seules les machines virtuelles participant activement au trafic LDAP (c'est-à-dire en mesure de lier) peuvent voir le trafic à partir du serveur LDAP. Pour plus d'informations sur le sniffing de paquets dans Cloud Volumes Service, reportez-vous à la section ""Considérations sur la capture et la détection des paquets.""

Paramètres par défaut de configuration du client LDAP

Lorsque LDAP est activée dans une instance Cloud Volumes Service, une configuration client LDAP est créée par défaut avec des détails de configuration spécifiques. Dans certains cas, les options ne s'appliquent pas à Cloud Volumes Service (non prises en charge) ou ne peuvent pas être configurées.

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Liste des serveurs LDAP	Définit les noms de serveur LDAP ou les adresses IP à utiliser pour les requêtes. Ceci n'est pas utilisé pour Cloud Volumes Service. À la place, Active Directory Domain est utilisé pour définir les serveurs LDAP.	Non défini	Non
Domaine Active Directory	Définit le domaine Active Directory à utiliser pour les requêtes LDAP. Cloud Volumes Service utilise les enregistrements SRV pour LDAP dans DNS pour trouver des serveurs LDAP dans le domaine.	Définissez le domaine Active Directory spécifié dans la connexion Active Directory.	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Serveurs Active Directory préférés	Définit les serveurs Active Directory préférés à utiliser pour LDAP. Non pris en charge par Cloud Volumes Service. Utilisez plutôt les sites Active Directory pour contrôler la sélection du serveur LDAP.	Non défini.	Non
Lier à l'aide des informations d'identification du serveur SMB	Se lie à LDAP à l'aide du compte de machine SMB. Actuellement, la seule méthode de liaison LDAP prise en charge dans Cloud Volumes Service.	Vrai	Non
Modèle de schéma	Modèle de schéma utilisé pour les requêtes LDAP.	MS-AD-BIS	Non
Port du serveur LDAP	Numéro de port utilisé pour les requêtes LDAP. Cloud Volumes Service utilise actuellement uniquement le port LDAP standard 389. Le port LDAPS/636 n'est pas pris en charge actuellement.	389	Non
LDAPS est activé	Contrôle si LDAP sur SSL (Secure Sockets Layer) est utilisé pour les requêtes et les liaisons. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non
Délai d'expiration de la requête (secondes)	Délai d'attente pour les requêtes. Si les requêtes prennent plus de temps que la valeur spécifiée, les requêtes échouent.	3	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Niveau d'authentification de liaison minimum	Niveau de liaison minimum pris en charge. Étant donné que Cloud Volumes Service utilise des comptes machine pour les liaisons LDAP et qu'Active Directory ne prend pas en charge les liaisons anonymes par défaut, cette option n'est pas en jeu pour la sécurité.	Anonyme	Non
Lier DN	Nom d'utilisateur/nom distinctif (DN) utilisé pour les liaisons lorsque la liaison simple est utilisée. Cloud Volumes Service utilise des comptes machine pour les liaisons LDAP et ne prend actuellement pas en charge l'authentification BIND simple.	Non défini	Non
DN de base	Le DN de base utilisé pour les recherches LDAP.	Le domaine Windows utilisé pour la connexion Active Directory, au format DN (c.c.=domaine, c.c.=local).	Non
Étendue de la recherche de base	Domaine de recherche pour les recherches de DN de base. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service prend uniquement en charge les recherches dans les sous-arborescences.	Sous-arbre	Non
Nom unique de l'utilisateur	Définit le DN où l'utilisateur recherche les requêtes LDAP. Actuellement non pris en charge pour Cloud Volumes Service, toutes les recherches d'utilisateur commencent par le NA de base.	Non défini	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Étendue de la recherche utilisateur	Domaine de recherche pour les recherches de DN utilisateur. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service ne prend pas en charge la définition de l'étendue de la recherche utilisateur.	Sous-arbre	Non
DN du groupe	Définit le DN où le groupe recherche les requêtes LDAP. Actuellement non pris en charge pour Cloud Volumes Service, toutes les recherches de groupe commencent par le NA de base.	Non défini	Non
Étendue de la recherche de groupe	Domaine de recherche pour les recherches de DN de groupe. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service ne prend pas en charge la définition de l'étendue de la recherche de groupe.	Sous-arbre	Non
DN du groupe réseau	Définit le DN où le groupe réseau recherche les requêtes LDAP. Actuellement non pris en charge pour Cloud Volumes Service, toutes les recherches de groupe réseau commencent par le DN de base.	Non défini	Non
Domaine de recherche de groupe réseau	Domaine de recherche pour les recherches de DN de groupe réseau. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service ne prend pas en charge la définition de l'étendue de recherche du groupe réseau.	Sous-arbre	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Utilisez START_tls sur LDAP	Utilise Start TLS pour les connexions LDAP basées sur des certificats via le port 389. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non
Activez la recherche netgroup-by-host	Active les recherches de groupe réseau par nom d'hôte plutôt que d'étendre les groupes réseau pour répertorier tous les membres. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non
DN netgroup-by-host	Définit le DN où les recherches de netgroup-par-hôte commencent pour les requêtes LDAP. Netgroup-by-host n'est actuellement pas pris en charge pour Cloud Volumes Service.	Non défini	Non
Étendue de recherche netgroup-by-host	Étendue de recherche pour les recherches de DN netgroup-par-hôte. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Netgroup-by-host n'est actuellement pas pris en charge pour Cloud Volumes Service.	Sous-arbre	Non
Sécurité de session client	Définit le niveau de sécurité de session utilisé par LDAP (signe, sceau ou aucun). La signature LDAP est prise en charge par CVS-Performance, sur demande d'Active Directory. CVS-SW ne prend pas en charge la signature LDAP. Pour les deux types d'entretien, le scellage n'est actuellement pas pris en charge.	Aucune	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Renvoi LDAP à la recherche	Lors de l'utilisation de plusieurs serveurs LDAP, la recherche de références permet au client de se référer à d'autres serveurs LDAP de la liste lorsqu'une entrée est introuvable dans le premier serveur. Cette opération n'est actuellement pas prise en charge par Cloud Volumes Service.	Faux	Non
Filtre d'appartenance au groupe	Fournit un filtre de recherche LDAP personnalisé à utiliser lors de la recherche d'appartenance à un groupe à partir d'un serveur LDAP. Non pris en charge actuellement avec Cloud Volumes Service.	Non défini	Non

Utilisation de LDAP pour le mappage de noms asymétrique

Par défaut, Cloud Volumes Service mappe les utilisateurs Windows et les utilisateurs UNIX avec des noms d'utilisateur identiques, dans le même sens, sans configuration spéciale. Tant que Cloud Volumes Service peut trouver un utilisateur UNIX valide (avec LDAP), un mappage de nom 1:1 se produit. Par exemple, si utilisateur Windows `johnsmith` Est utilisé, alors, si Cloud Volumes Service peut trouver un utilisateur UNIX nommé `johnsmith` Dans LDAP, le mappage de noms réussit pour cet utilisateur, tous les fichiers/dossiers créés par `johnsmith` Affiche la propriété correcte de l'utilisateur et toutes les listes de contrôle d'accès qui affectent `johnsmith` Sont honorés quel que soit le protocole NAS utilisé. Il s'agit d'un mappage de nom symétrique.

Le mappage de nom asymétrique est utilisé lorsque l'identité utilisateur Windows et l'identité utilisateur UNIX ne correspondent pas. Par exemple, si utilisateur Windows `johnsmith` Possède une identité UNIX de `jsmith`, Cloud Volumes Service a besoin d'une façon d'être racontée sur la variation. Cloud Volumes Service ne prenant actuellement pas en charge la création de règles de mappage de noms statiques, LDAP doit être utilisé pour rechercher l'identité des utilisateurs pour les identités Windows et UNIX afin d'assurer la propriété correcte des fichiers et dossiers et des autorisations attendues.

Par défaut, Cloud Volumes Service inclut `LDAP` Dans le commutateur ns-switch de l'instance de la base de données de mappage de noms, afin de fournir une fonctionnalité de mappage de noms en utilisant LDAP pour les noms asymétriques, il vous suffit de modifier certains attributs utilisateur/groupe pour refléter ce que recherche Cloud Volumes Service.

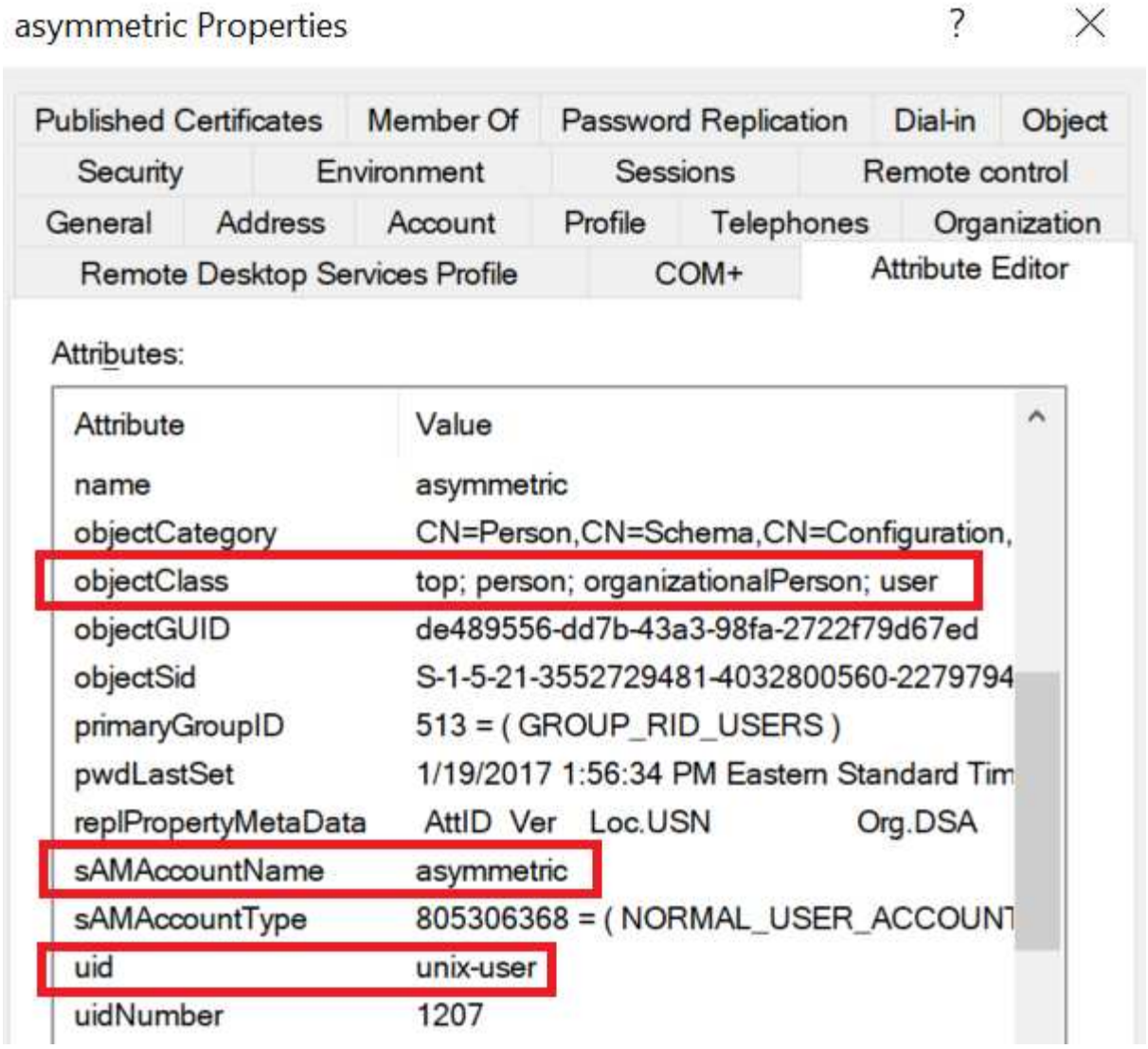
Le tableau suivant indique quels attributs doivent être renseignés dans LDAP pour la fonctionnalité de mappage de noms asymétriques. Dans la plupart des cas, Active Directory est déjà configuré pour le faire.

Attribut Cloud Volumes Service	Ce qu'il fait	Valeur utilisée par Cloud Volumes Service pour le mappage de noms
ObjectClass de Windows à UNIX	Spécifie le type d'objet utilisé. (C'est-à-dire utilisateur, groupe, posixAccount, etc.)	Doit inclure l'utilisateur (peut contenir plusieurs autres valeurs, si nécessaire).
Attribut Windows à UNIX	Qui définit le nom d'utilisateur Windows lors de sa création. Cloud Volumes Service utilise cette fonction pour les recherches Windows vers UNIX.	Aucune modification n'est nécessaire ici ; sAMAccountName est identique au nom de connexion Windows.
UID	Définit le nom d'utilisateur UNIX.	Nom d'utilisateur UNIX souhaité.

Cloud Volumes Service n'utilise actuellement pas de préfixes de domaine dans les recherches LDAP, de sorte que plusieurs environnements LDAP de domaine ne fonctionnent pas correctement avec les recherches de carte de noms LDAP.

L'exemple suivant montre un utilisateur portant le nom Windows `asymmetric`, Le nom UNIX `unix-user`, Et le comportement suivant lors de l'écriture de fichiers à partir de SMB et NFS.

La figure suivante montre l'apparence des attributs LDAP à partir du serveur Windows.



À partir d'un client NFS, vous pouvez interroger le nom UNIX mais pas le nom Windows :

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Lorsqu'un fichier est écrit à partir de NFS en tant que `unix-user`, Le résultat suivant est celui du client NFS :

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

À partir d'un client Windows, vous pouvez voir que le propriétaire du fichier est défini sur l'utilisateur Windows approprié :

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Inversement, les fichiers créés par l'utilisateur Windows `asymmetric` À partir d'un client SMB, montrer le propriétaire UNIX approprié, comme indiqué dans le texte suivant.

SMB :

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS :

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Liaison de canal LDAP

En raison d'une vulnérabilité avec les contrôleurs de domaine Windows Active Directory, "Avis de sécurité de Microsoft ADV190023" Modifie la façon dont le DCS autorise les liaisons LDAP.

L'impact pour Cloud Volumes Service est le même que pour tous les clients LDAP. Cloud Volumes Service ne prend actuellement pas en charge la liaison de canaux. Étant donné que Cloud Volumes Service prend en charge la signature LDAP par défaut via la négociation, la liaison du canal LDAP ne doit pas poser problème. Si vous rencontrez des problèmes de liaison avec LDAP alors que la liaison des canaux est activée, suivez les étapes de correction décrites dans ADV190023 pour permettre aux liaisons LDAP à partir de Cloud Volumes Service de réussir.

DNS

Active Directory et Kerberos ont tous deux des dépendances sur DNS pour la résolution du nom d'hôte à IP/IP vers le nom d'hôte. Le DNS requiert l'ouverture du port 53. Cloud Volumes Service n'apporte aucune modification aux enregistrements DNS et ne prend actuellement en charge l'utilisation de "DNS dynamique" sur les interfaces réseau.

Vous pouvez configurer Active Directory DNS pour limiter les serveurs qui peuvent mettre à jour les enregistrements DNS. Pour plus d'informations, voir "Un DNS Windows sécurisé".

Notez que les ressources d'un projet Google utilisent par défaut Google Cloud DNS, qui n'est pas connecté à Active Directory DNS. Les clients utilisant le DNS du cloud ne peuvent pas résoudre les chemins UNC renvoyés par Cloud Volumes Service. Les clients Windows joints au domaine Active Directory sont configurés

pour utiliser Active Directory DNS et peuvent résoudre de tels chemins UNC.

Pour joindre un client à Active Directory, vous devez configurer sa configuration DNS pour utiliser Active Directory DNS. Vous pouvez également configurer Cloud DNS pour transférer les demandes vers Active Directory DNS. Voir "Pourquoi mon client ne parvient-il pas à résoudre le nom NetBIOS du SMB ?"pour en savoir plus.

Cloud Volumes Service ne prend pas actuellement en charge les requêtes DNSSEC et DNS sont exécutées en texte clair.

Audit de l'accès aux fichiers

Actuellement non pris en charge par Cloud Volumes Service.

Protection antivirus

Vous devez effectuer une analyse antivirus dans Cloud Volumes Service au niveau du client vers un partage NAS. Il n'existe actuellement pas d'intégration antivirus native avec Cloud Volumes Service.

Opération d'entretien

L'équipe Cloud Volumes Service gère les services de back-end dans Google Cloud et exploite plusieurs stratégies pour sécuriser la plateforme et empêcher les accès non autorisés.

Chaque client bénéficie de son propre sous-réseau unique, qui dispose d'un accès clôturé par défaut par rapport à d'autres clients. Par ailleurs, chaque locataire de Cloud Volumes Service dispose de son propre espace de noms et VLAN pour assurer l'isolation totale des données. Après l'authentification d'un utilisateur, le moteur de fourniture de services (SDE) peut uniquement lire les données de configuration spécifiques à ce locataire.

Sécurité physique

Une fois la préapprobation adéquate obtenue, seuls les ingénieurs sur site et les ingénieurs de support de terrain (FSE) certifiés NetApp ont accès à la cage et aux racks pour les travaux physiques. La gestion du réseau et du stockage n'est pas autorisée. Seules ces ressources sur site sont en mesure d'effectuer les tâches de maintenance du matériel.

Pour les ingénieurs sur site, un ticket est émis pour l'énoncé des travaux (SOW) qui inclut l'ID de rack et l'emplacement du périphérique (RU). Toutes les autres informations sont incluses dans le ticket. Pour les FSE NetApp, un ticket de visite sur site doit être levé avec la COLOCATION. Le ticket inclut également les détails, la date et l'heure du visiteur à des fins d'audit. Le cahier des charges du FSE est communiqué à NetApp en interne.

Équipe chargée des opérations

L'équipe des opérations de Cloud Volumes Service se compose de l'ingénierie de production et d'un ingénieur de fiabilité de site (SRE) pour les services de volume cloud, ainsi que des ingénieurs de support sur site de NetApp et des partenaires pour le matériel. Tous les membres de l'équipe des opérations sont accrédités pour travailler dans Google Cloud et des dossiers de travail détaillés sont conservés pour chaque billet émis. De plus, un processus rigoureux de contrôle et d'approbation du changement est en place pour s'assurer que chaque décision est examinée de façon appropriée.

L'équipe SRE gère le plan de contrôle et la manière dont les données sont acheminées depuis les demandes

d'interface utilisateur vers le matériel et les logiciels back-end dans Cloud Volumes Service. L'équipe SRE gère également les ressources système, telles que les volumes et les volumes d'inode maximaux. Les SRES ne sont pas autorisés à interagir avec les données clients ou à y accéder. SRES assure également la coordination des autorisations de renvoi de matériel (RMA), telles que les demandes de remplacement de nouveau disque ou de mémoire pour le matériel interne.

Obligations du client

Les clients de Cloud Volumes Service gèrent Active Directory et la gestion des rôles utilisateur de leur entreprise, ainsi que les opérations de volume et de données. Les clients peuvent disposer de rôles administratifs et déléguer des autorisations à d'autres utilisateurs au sein du même projet Google Cloud à l'aide des deux rôles prédéfinis de NetApp et Google Cloud (Administrateur et Viewer).

L'administrateur peut homologue à Cloud Volumes Service tout VPC dans le projet du client, que le client détermine approprié. Il est de la responsabilité du client de gérer l'accès à son abonnement à Google Cloud Marketplace et de gérer les VPC qui ont accès au plan de données.

Protection de SRE malveillante

Une préoccupation pouvant survenir est la façon dont Cloud Volumes Service protège-t-elle contre les scénarios dans lesquels il existe un SRE malveillant ou lorsque les informations d'identification des SRE ont été compromises ?

L'accès à l'environnement de production n'est possible qu'avec un nombre limité de SRE particuliers. Les privilèges administratifs sont en outre limités à une poignée d'administrateurs expérimentés. Toutes les actions réalisées par toute personne dans l'environnement de production Cloud Volumes Service sont consignées et toute anomalie affectant une activité de base ou suspecte est détectée par notre plateforme de veille centralisée des informations de sécurité et des événements (SIEM) pour les menaces. Ainsi, les actions malveillantes peuvent être suivies et atténuées avant que le back-end Cloud Volumes Service ne soit trop endommagé.

Cycle de vie du volume

Cloud Volumes Service gère uniquement les objets au sein du service, pas les données au sein des volumes. Seuls les clients qui accèdent aux volumes peuvent gérer les données, les listes de contrôle d'accès, les propriétaires de fichiers, etc. Les données de ces volumes sont chiffrées au repos et l'accès est limité aux locataires de l'instance Cloud Volumes Service.

Le cycle de vie des volumes pour Cloud Volumes Service est create-update-delete. Les volumes conservent des copies Snapshot de volumes jusqu'à leur suppression et seuls les administrateurs Cloud Volumes Service validés peuvent supprimer des volumes dans Cloud Volumes Service. Lorsqu'un administrateur demande la suppression d'un volume, une étape supplémentaire de la saisie du nom du volume est requise pour vérifier la suppression. Un volume est supprimé et ne peut plus être restauré.

Dans les cas où un contrat Cloud Volumes Service a été résilié, NetApp marque la suppression des volumes au bout d'une période donnée. Avant l'expiration de cette période, vous pouvez récupérer des volumes à la demande du client.

Certifications

Cloud volumes Services pour Google Cloud est actuellement certifié conforme aux normes ISO/IEC 27001:2013 et ISO/IEC 27018:2019. Le service a aussi récemment reçu son rapport d'attestation de type I de la SOC2. Pour plus d'informations sur l'engagement de NetApp en matière de sécurité et de confidentialité des données, consultez la page "Conformité : sécurité et confidentialité des données".

LE RGPD

Notre engagement en matière de confidentialité et de conformité avec le RGPD est disponible dans un certain nombre de nos "contrats clients", comme notre "Addenda relatif au traitement des données client", qui inclut le "Clauses contractuelles standard" Fourni par la Commission européenne. Nous prenons également ces engagements dans notre politique de confidentialité, soutenue par les valeurs fondamentales énoncées dans notre Code de conduite d'entreprise.

Informations complémentaires et coordonnées

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

- Documentation Google Cloud pour Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Service privé Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentation des produits NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Programme de module de validation cryptographique : NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- Solution NetApp pour ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- Tr-4616 : NFS Kerberos dans ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Contactez-nous

Dites-nous comment nous pourrions améliorer ce rapport technique.

Contactez-nous à l'adresse : doccomments@netapp.com. Incluez LE RAPPORT TECHNIQUE 4918 dans la ligne d'objet.

Sauvegarde et restauration BlueXP

Sauvegarde et restauration BlueXP pour les VM

3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration BlueXP pour les VM

Auteur : Josh Powell - Ingénierie de solutions NetApp

Présentation

La stratégie de sauvegarde 3-2-1 est une méthode de protection des données reconnue par le secteur et offre une approche complète pour la sauvegarde des données précieuses. Cette stratégie est fiable et garantit que même en cas de sinistre inattendu, une copie des données sera toujours disponible.

La stratégie comprend trois règles fondamentales :

1. Conservez au moins trois copies de vos données. Ainsi, même en cas de perte ou de corruption d'une copie, vous avez toujours au moins deux copies restantes à remettre en marche.
2. Stockez deux copies de sauvegarde sur différents supports ou périphériques de stockage. La diversification des supports de stockage permet d'offrir une protection contre les défaillances spécifiques aux périphériques ou aux supports. Si un périphérique est endommagé ou si un type de support échoue, l'autre copie de sauvegarde n'est pas affectée.
3. Enfin, assurez-vous qu'au moins une copie de sauvegarde est hors site. Le stockage hors site sert de protection contre les incidents localisés tels que des incendies ou des inondations qui pourraient rendre les copies sur site inutilisables.

Ce document présente une solution de sauvegarde 3-2-1 avec le plug-in SnapCenter pour VMware vSphere (SCV) pour créer des sauvegardes primaires et secondaires de nos machines virtuelles sur site, et BlueXP pour la sauvegarde et la restauration des machines virtuelles afin de sauvegarder une copie de nos données dans le stockage cloud ou dans StorageGRID.

Cas d'utilisation

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde et restauration de machines virtuelles et de datastores sur site à l'aide du plug-in SnapCenter pour VMware vSphere.
- Sauvegarde et restauration de machines virtuelles et de datastores sur site, hébergés sur des clusters ONTAP, et sauvegarde sur un stockage objet à l'aide de la sauvegarde et de la restauration BlueXP pour les machines virtuelles.

Stockage des données NetApp ONTAP

ONTAP est la solution de stockage de pointe de NetApp qui offre un stockage unifié, quel que soit le protocole utilisé : SAN ou NAS. Grâce à la stratégie de sauvegarde 3-2-1, les données sur site sont protégées sur plusieurs types de supports, et NetApp propose des plateformes allant du Flash haut débit aux supports moins coûteux.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
			
Hybrid flash storage	**Capacity all-flash storage**	**Performance all-flash storage**	**All-flash SAN storage**
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

Pour en savoir plus sur la plateforme matérielle NetApp, consultez la page "Stockage des données NetApp".

Plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter pour VMware vSphere est une offre de protection des données étroitement intégrée à VMware vSphere qui facilite la gestion des sauvegardes et des restaurations des machines virtuelles. Dans le cadre de cette solution, SnapMirror offre une méthode rapide et fiable pour créer une seconde copie de sauvegarde immuable des données du serveur virtuel sur un cluster de stockage ONTAP secondaire. Une fois cette architecture en place, les opérations de restauration des machines virtuelles peuvent facilement être lancées à partir des emplacements de sauvegarde principaux ou secondaires.

SCV est déployé en tant qu'appliance virtuelle linux à l'aide d'un fichier OVA. Le plug-in utilise désormais un plug-in distant
architecture. Le plug-in distant s'exécute en dehors du serveur vCenter et est hébergé sur l'appliance virtuelle SCV.

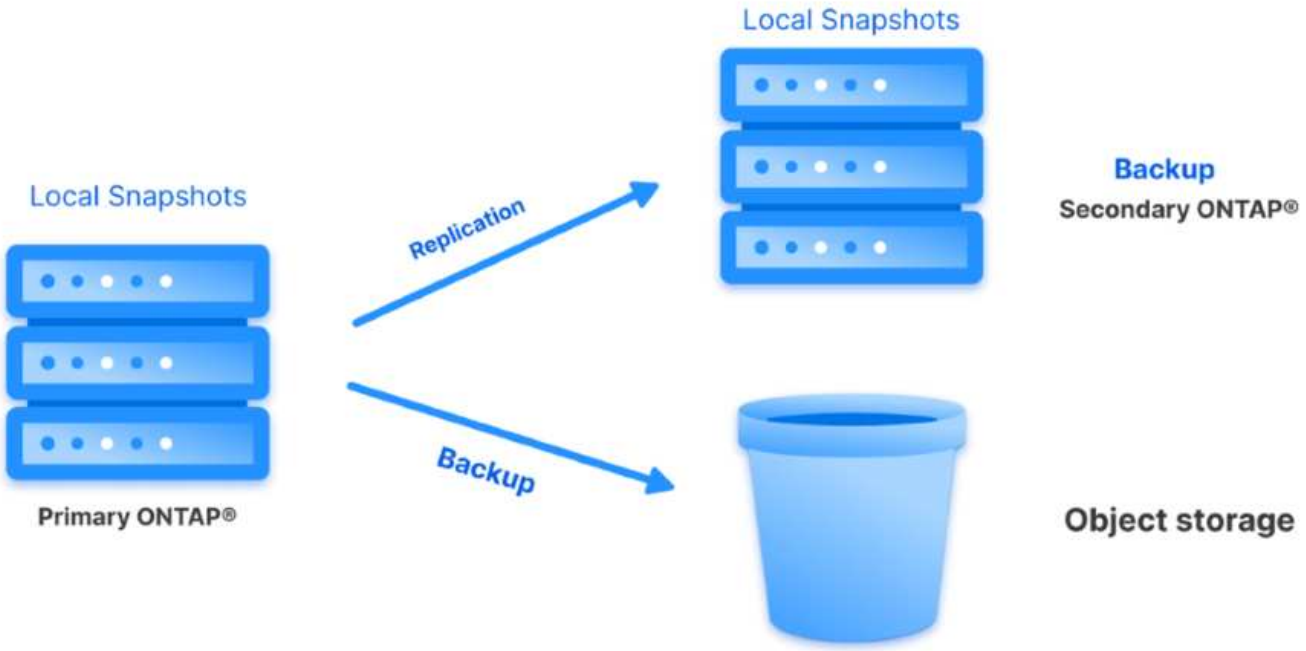
Pour plus d'informations sur le distributeur auxiliaire, se reporter à "Documentation du plug-in SnapCenter pour VMware vSphere".

Sauvegarde et restauration BlueXP pour les machines virtuelles

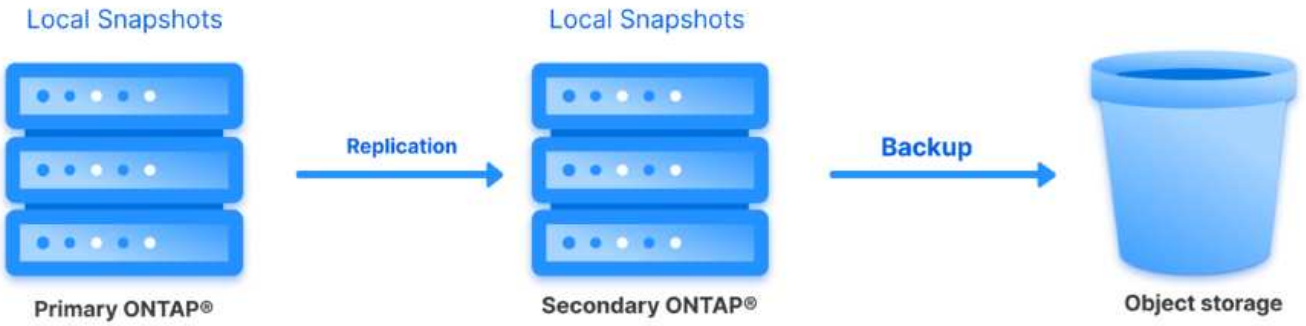
BlueXP Backup and Recovery est un outil cloud de gestion des données qui offre un plan de contrôle unique pour un large éventail d'opérations de sauvegarde et de restauration dans les environnements sur site et cloud. Une fonctionnalité de la suite de sauvegarde et de restauration NetApp BlueXP s'intègre avec le plug-in SnapCenter pour VMware vSphere (sur site) pour étendre une copie des données au stockage objet dans le cloud. Cela établit une troisième copie des données hors site, qui provient des sauvegardes de stockage primaire ou secondaire. Avec la sauvegarde et la restauration BlueXP, il est facile de définir des règles de stockage qui transfèrent des copies de vos données à partir de l'un de ces deux emplacements sur site.

En choisissant entre les sauvegardes primaires et secondaires comme source dans BlueXP Backup and Recovery, vous implémentation de l'une des deux topologies suivantes :

Topologie « Fan-Out » – lorsqu'une sauvegarde est lancée par le plug-in SnapCenter pour VMware vSphere, un snapshot local est immédiatement pris. SCV lance ensuite une opération SnapMirror qui réplique l'instantané le plus récent sur le cluster ONTAP secondaire. Dans BlueXP Backup and Recovery, une règle spécifie le cluster ONTAP principal comme source d'une copie Snapshot des données à transférer vers le stockage objet dans le fournisseur cloud de votre choix.



Topologie en cascade – la création de copies de données primaires et secondaires à l'aide de SCV est identique à la topologie de sortie mentionnée ci-dessus. Cependant, cette fois-ci, une règle est créée dans BlueXP Backup and Recovery en spécifiant que la sauvegarde vers le stockage objet va provenir du cluster ONTAP secondaire.



La sauvegarde et la restauration BlueXP permettent de créer des copies de sauvegarde des copies ONTAP sur site vers AWS Glacier, Azure Blob et le stockage d'archives GCP.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

En outre, vous pouvez utiliser NetApp StorageGRID comme cible de sauvegarde du stockage objet. Pour plus d'informations sur StorageGRID, reportez-vous au "Page d'accueil StorageGRID".

Présentation du déploiement de la solution

Cette liste répertorie les étapes générales nécessaires à la configuration de cette solution et à l'exécution des opérations de sauvegarde et de restauration à partir des sauvegardes et restaurations SCV et BlueXP :

1. Configurez la relation SnapMirror entre les clusters ONTAP à utiliser pour les copies de données primaires et secondaires.
2. Configuration du plug-in SnapCenter pour VMware vSphere
   a. Ajouter des systèmes de stockage
   b. Création de règles de sauvegarde
   c. Créer des groupes de ressources
   d. Exécutez d'abord les tâches de sauvegarde
3. Configurer la sauvegarde et la restauration BlueXP pour les machines virtuelles
   a. Ajouter un environnement de travail
   b. Découvrez les appliances SCV et vCenter
   c. Création de règles de sauvegarde
   d. Activer les sauvegardes
4. Restaurer les machines virtuelles à partir du stockage primaire et secondaire à l'aide de SCV.
5. Restaurez les machines virtuelles à partir du stockage objet à l'aide de la sauvegarde et de la restauration BlueXP.

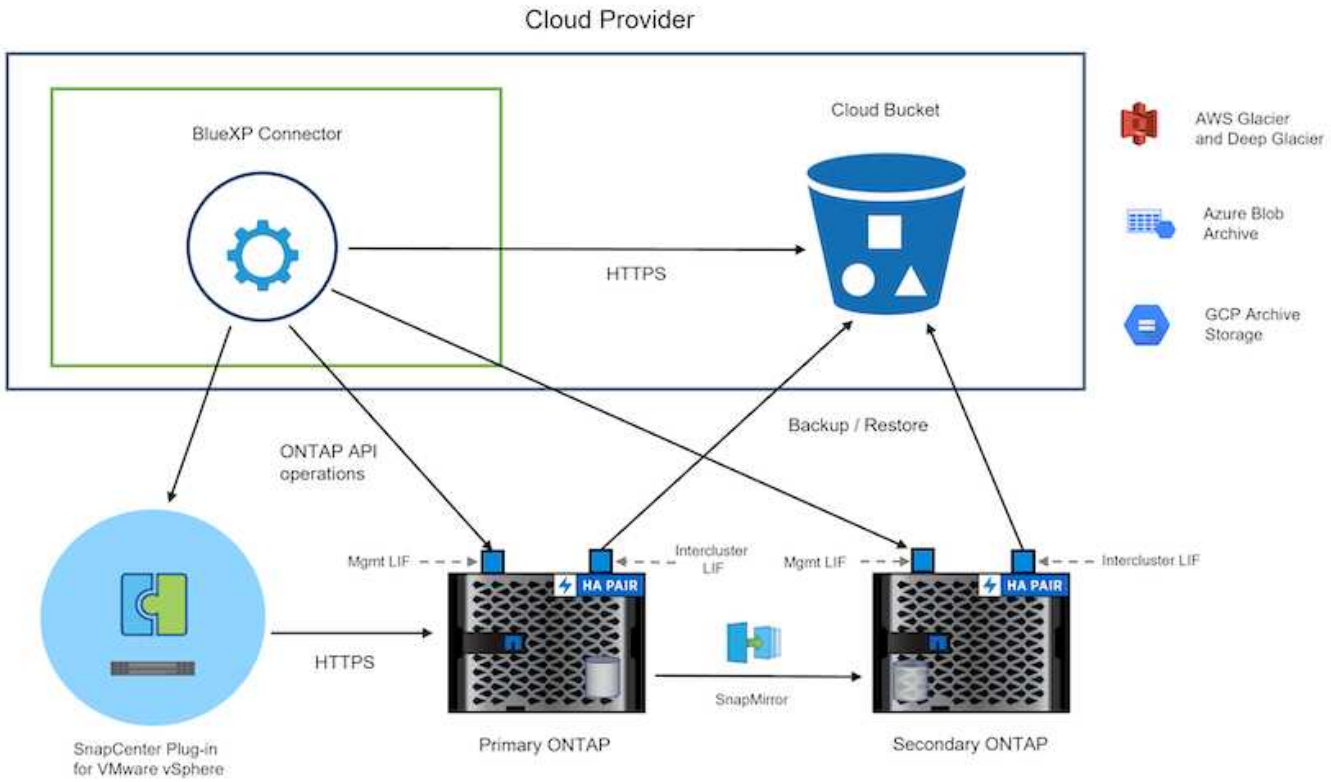
Prérequis

L'objectif de cette solution est de démontrer la protection des données des serveurs virtuels s'exécutant dans VMware vSphere et situés sur des datastores NFS hébergés par NetApp ONTAP. Cette solution suppose que les composants suivants sont configurés et prêts à l'emploi :

1. Cluster de stockage ONTAP avec datastores NFS ou VMFS connectés à VMware vSphere. Les datastores NFS et VMFS sont pris en charge. Des datastores NFS ont été utilisés pour cette solution.
2. Cluster de stockage ONTAP secondaire avec relations SnapMirror établies pour les volumes utilisés pour les datastores NFS.
3. BlueXP Connector installé pour le fournisseur cloud utilisé pour les sauvegardes de stockage objet.
4. Les machines virtuelles à sauvegarder se trouvent sur des datastores NFS résidant sur le cluster de stockage ONTAP principal.
5. Connectivité réseau entre le connecteur BlueXP et les interfaces de gestion des clusters de stockage ONTAP sur site.
6. Connectivité réseau entre le connecteur BlueXP et la machine virtuelle de l'appliance SCV sur site, et entre le connecteur BlueXP et vCenter.
7. Connectivité réseau entre les LIFs intercluster ONTAP sur site et le service de stockage objet.
8. DNS configuré pour la gestion des SVM sur les clusters de stockage ONTAP principal et secondaire. Pour plus d'informations, reportez-vous à la section "Configurez le DNS pour la résolution du nom d'hôte".

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.



Déploiement de la solution

Dans cette solution, nous fournissons des instructions détaillées pour le déploiement et la validation d'une solution qui utilise le plug-in SnapCenter pour VMware vSphere, ainsi que la sauvegarde et la restauration BlueXP, pour effectuer la sauvegarde et la restauration de machines virtuelles Windows et Linux dans un cluster VMware vSphere situé dans un data Center sur site. Les machines virtuelles de cette configuration sont stockées dans des datastores NFS hébergés par un cluster de stockage ONTAP A300. En outre, un cluster de stockage ONTAP A300 distinct sert de destination secondaire pour les volumes répliqués à l'aide de SnapMirror. En outre, le stockage objet hébergé sur Amazon Web Services et Azure Blob ont été utilisés comme cibles pour la troisième copie des données.

Nous allons poursuivre la création de relations SnapMirror pour les copies secondaires de nos sauvegardes gérées par SCV et la configuration des tâches de sauvegarde dans les sauvegardes et les restaurations de SCV et BlueXP.

Pour plus d'informations sur le plug-in SnapCenter pour VMware vSphere, reportez-vous au "Documentation du plug-in SnapCenter pour VMware vSphere".

Pour plus d'informations sur la sauvegarde et la restauration BlueXP, reportez-vous au "Documentation sur la sauvegarde et la restauration BlueXP".

Établissement de relations SnapMirror entre clusters ONTAP

Le plug-in SnapCenter pour VMware vSphere utilise la technologie ONTAP SnapMirror pour gérer le transport des copies SnapMirror et/ou SnapVault secondaires vers un cluster ONTAP secondaire.

Les règles de sauvegarde des distributeurs sélectifs ont la possibilité d'utiliser les relations SnapMirror ou SnapVault. La principale différence est que lorsque vous utilisez l'option SnapMirror, le planning de conservation configuré pour les sauvegardes dans la règle sera le même sur les sites principal et secondaire. SnapVault est conçu pour l'archivage et si cette option permet d'établir une planification de conservation distincte avec la relation SnapMirror pour les copies Snapshot sur le cluster de stockage ONTAP secondaire.

La configuration des relations SnapMirror peut être effectuée dans BlueXP où de nombreuses étapes sont automatisées ou via System Manager et l'interface de ligne de commande ONTAP. Toutes ces méthodes sont présentées ci-dessous.

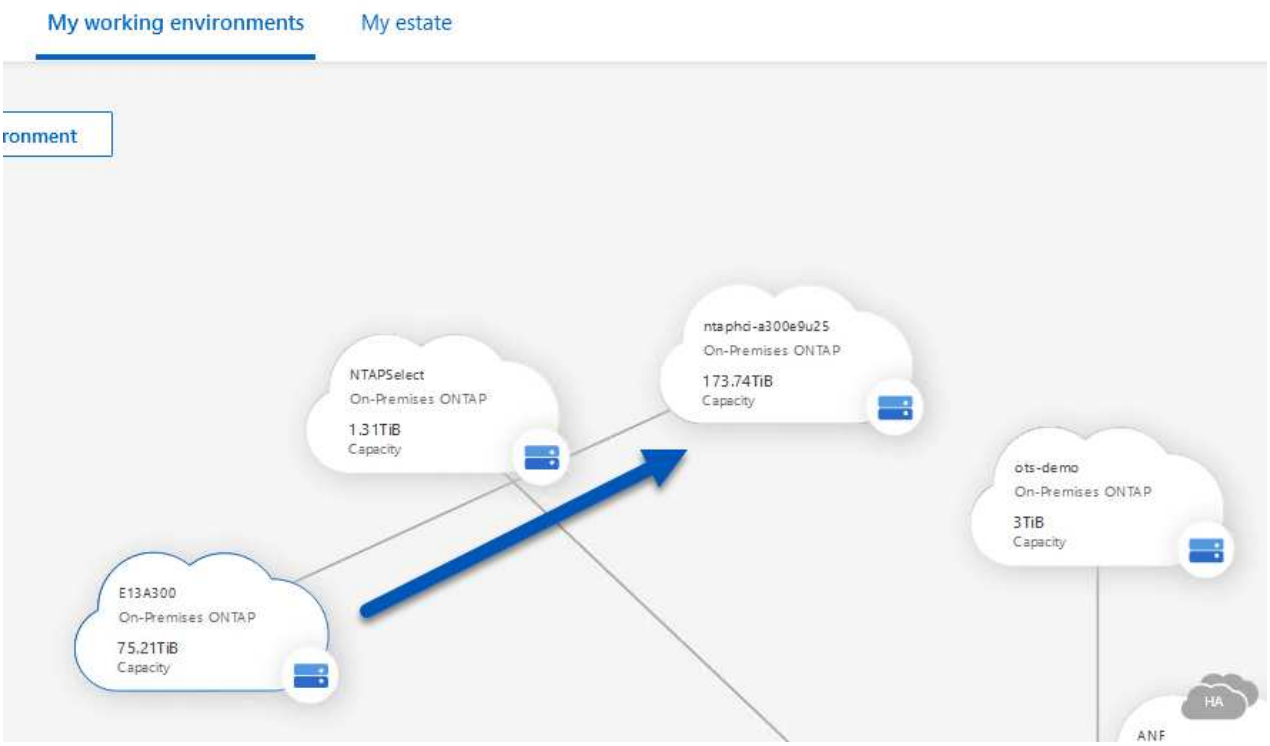
Établissez des relations SnapMirror avec BlueXP

Les étapes suivantes doivent être effectuées à partir de la console Web BlueXP :

Configuration de la réplication pour les systèmes de stockage ONTAP principaux et secondaires

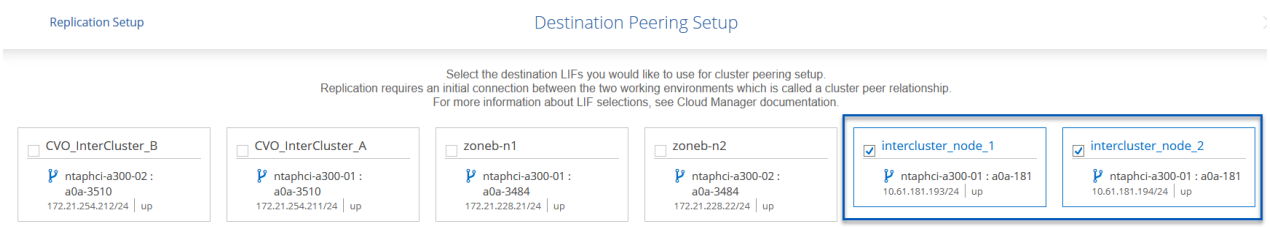
Commencez par vous connecter à la console Web BlueXP et naviguer jusqu'au Canvas.

1. Glissez-déposez le système de stockage ONTAP source (principal) sur le système de stockage ONTAP de destination (secondaire).

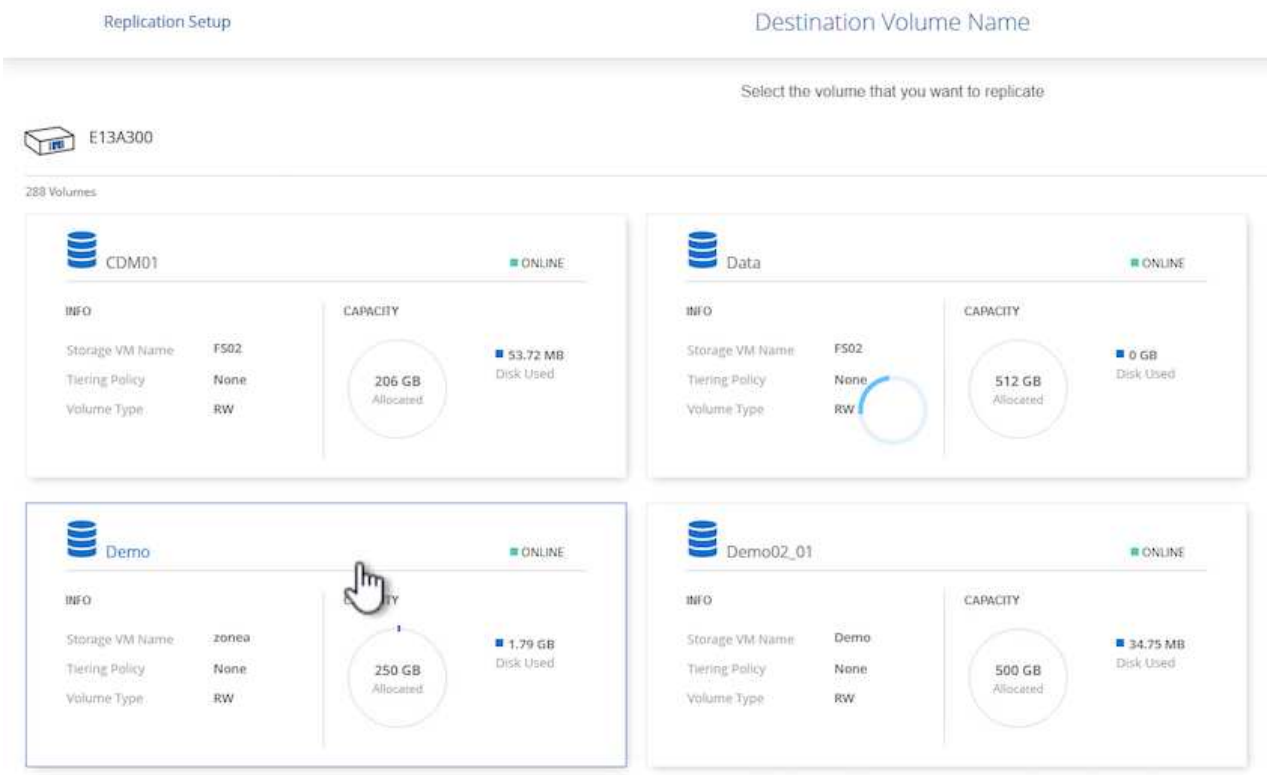


2. Dans le menu qui s'affiche, sélectionnez **Replication**.

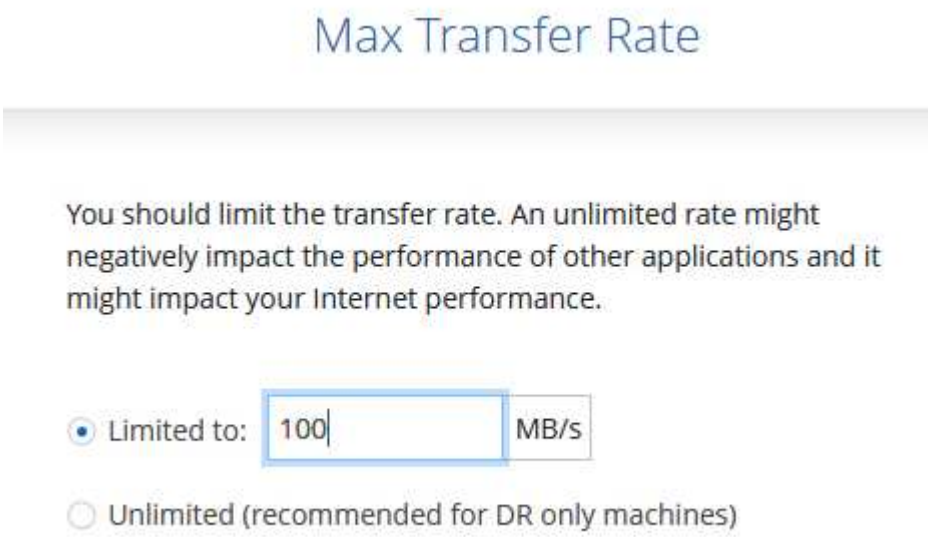
3. Sur la page **destination peering Setup**, sélectionnez les LIFs intercluster de destination à utiliser pour la connexion entre systèmes de stockage.



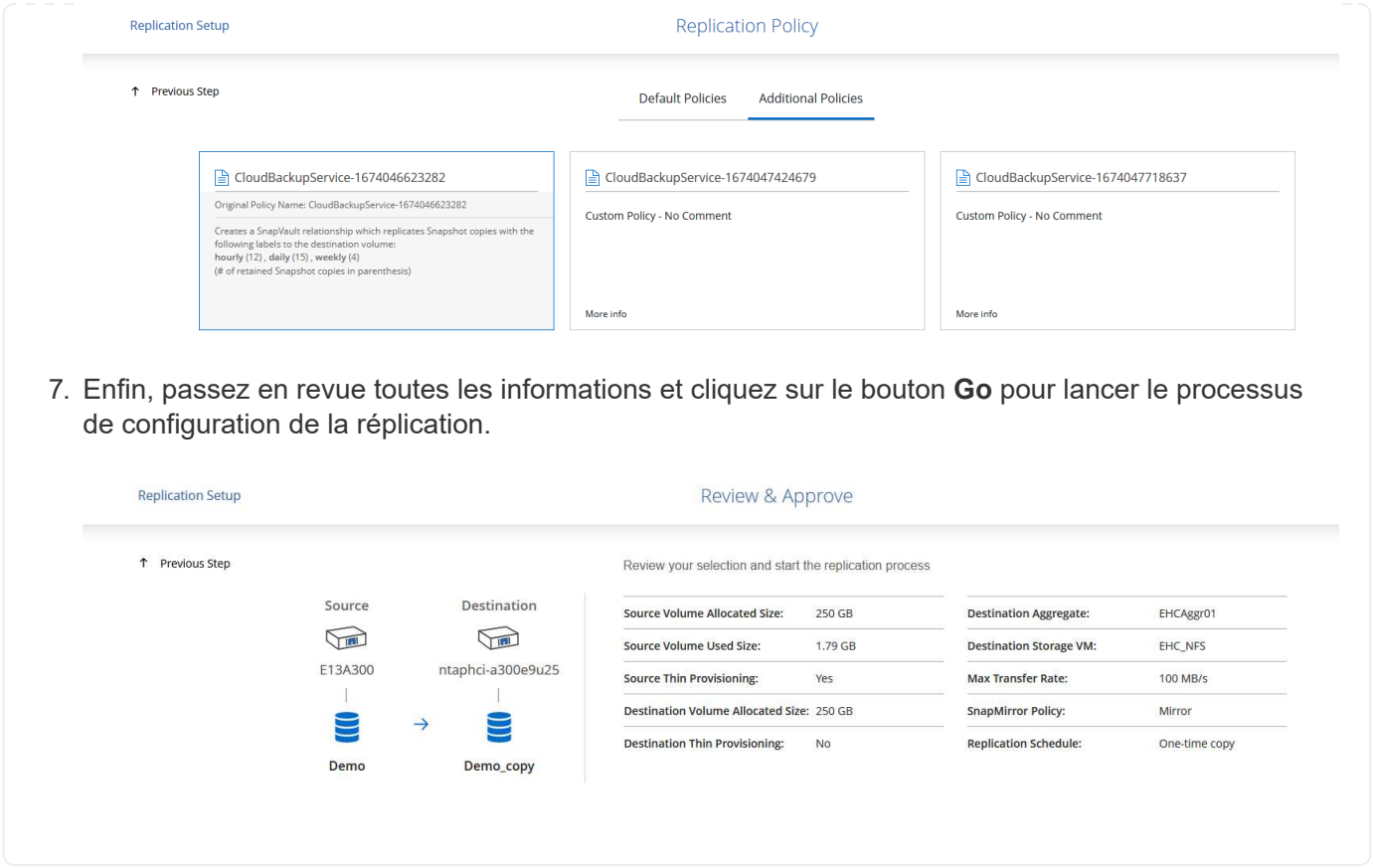
4. Sur la page **destination Volume Name**, sélectionner d'abord le volume source, puis remplir le nom du volume de destination et sélectionner le SVM et l'agrégat de destination. Cliquez sur **Suivant** pour continuer.



5. Choisissez le taux de transfert maximal pour la réplication.



6. Choisissez la règle qui déterminera le calendrier de conservation des sauvegardes secondaires. Cette stratégie peut être créée au préalable (voir le processus manuel ci-dessous dans l'étape **Créer une stratégie de rétention d'instantanés**) ou peut être modifiée après le fait si vous le souhaitez.



7. Enfin, passez en revue toutes les informations et cliquez sur le bouton **Go** pour lancer le processus de configuration de la réplication.

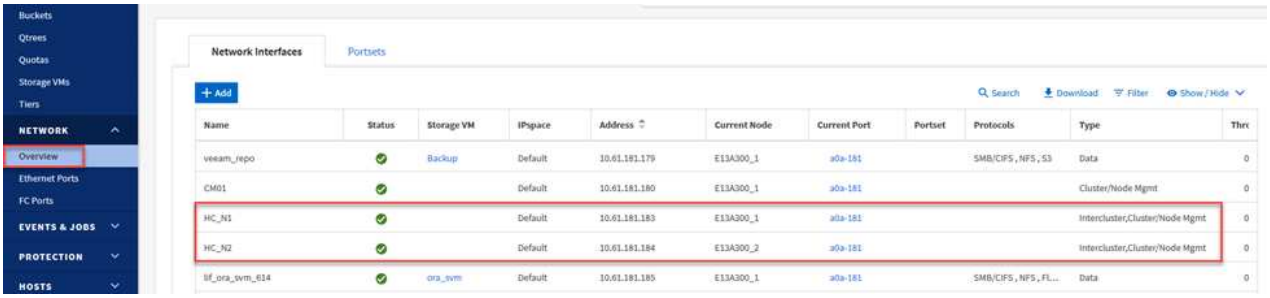
Établissez des relations SnapMirror avec System Manager et l'interface de ligne de commandes de ONTAP

Toutes les étapes requises pour établir des relations SnapMirror peuvent être effectuées à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP. La section suivante fournit des informations détaillées sur les deux méthodes :

Enregistrer les interfaces logiques intercluster source et destination

Pour les clusters ONTAP source et destination, vous pouvez récupérer les informations relatives aux LIF intercluster à partir de System Manager ou de 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 à l'aide de l'interface de ligne de commandes, exécutez la commande suivante :

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

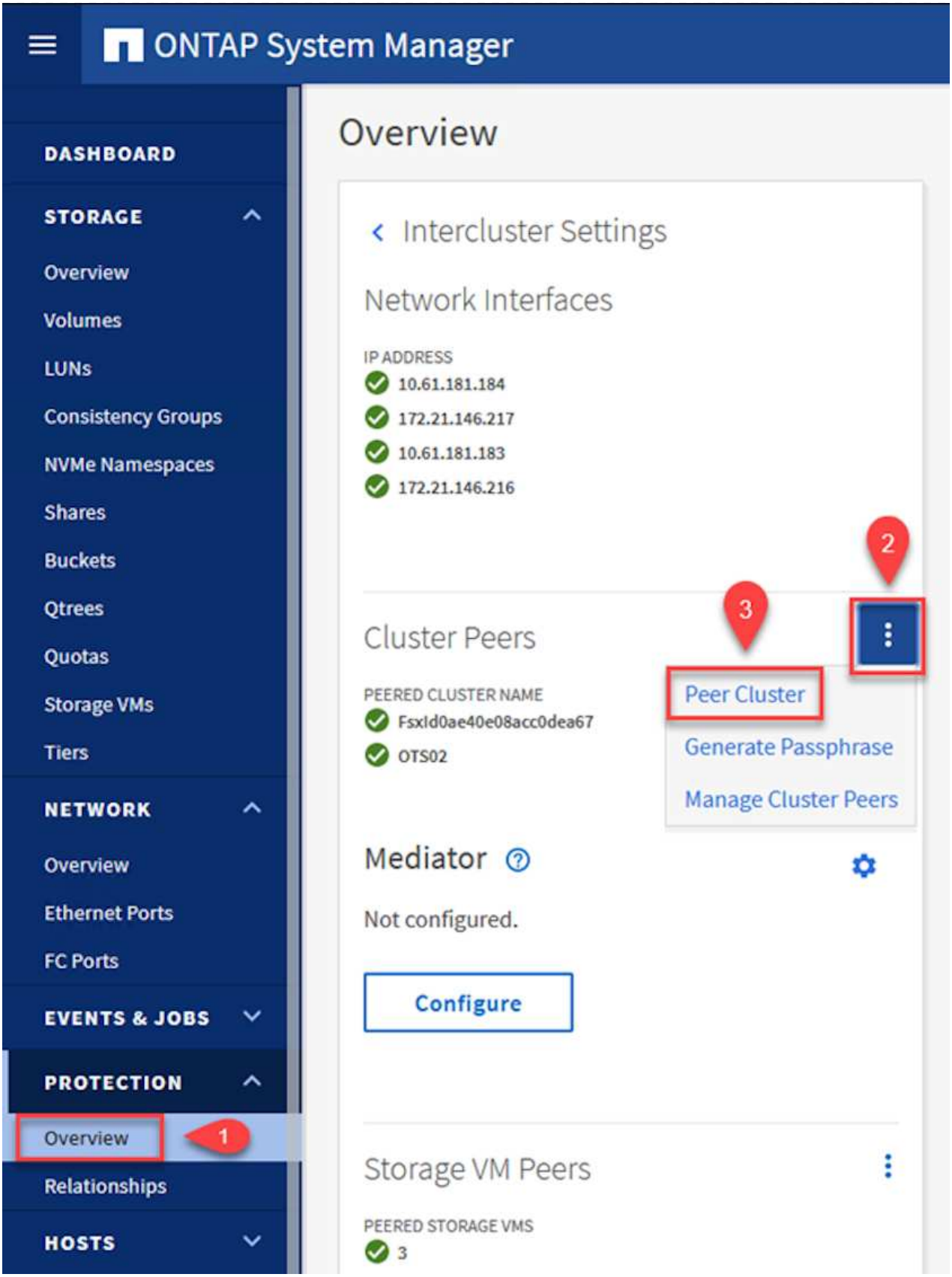
Établissement du peering de cluster entre clusters ONTAP

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 ONTAP de destination à l'aide du `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.

```
ONTAP-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.

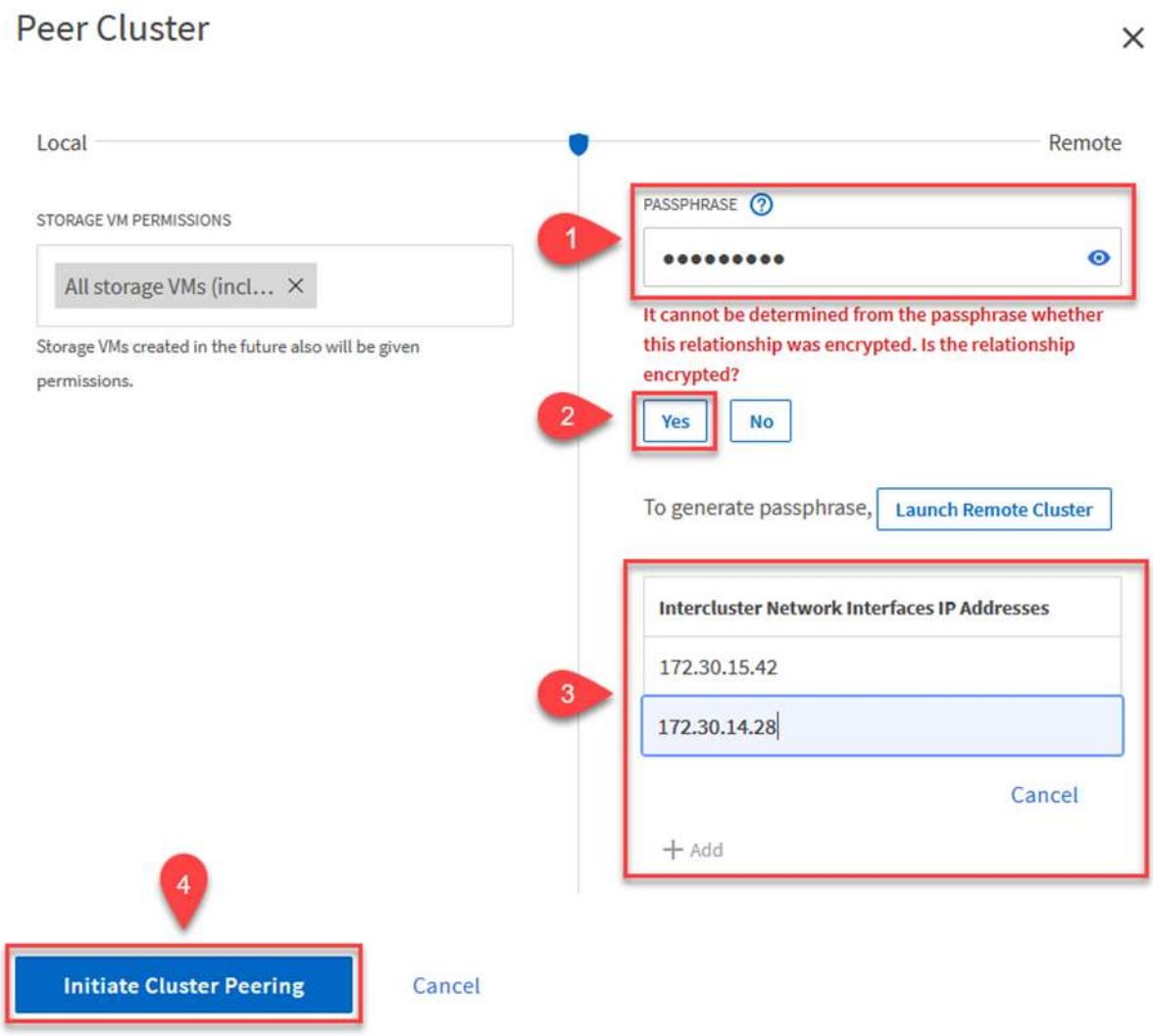


3. Dans la boîte de dialogue Peer Cluster, saisissez les informations requises :
   a. Entrez la phrase secrète utilisée pour établir la relation entre clusters sur le cluster ONTAP de destination.

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

c. Entrer les adresses IP du LIF intercluster du cluster ONTAP destination.

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



4. Vérifiez l'état de la relation entre clusters depuis le cluster ONTAP de destination à l'aide de la commande suivante :

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

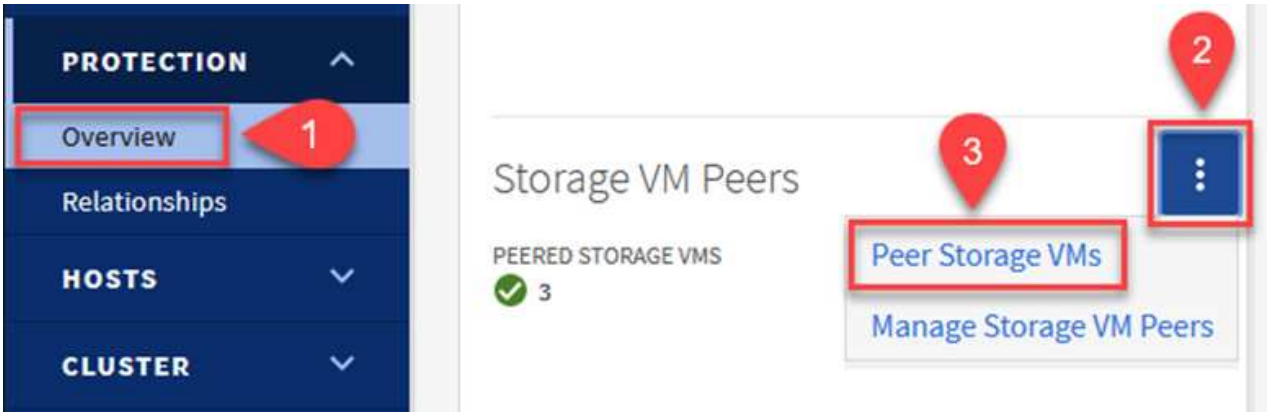
Établir une relation de peering de SVM

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.

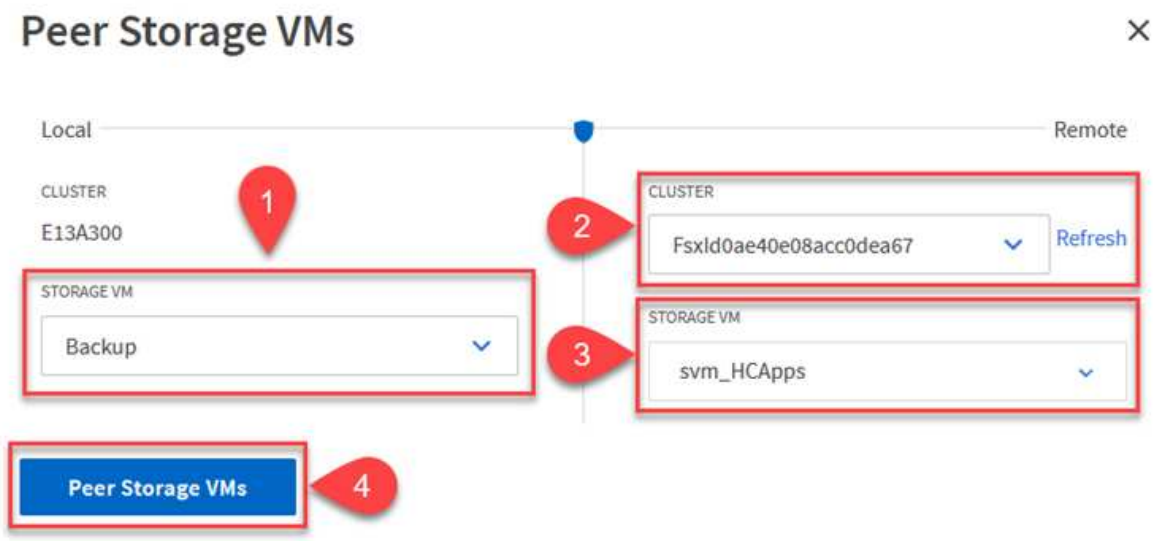
1. Depuis le cluster ONTAP de destination, utiliser la commande suivante depuis l'interface de ligne de commandes pour créer la relation SVM peer :

```
ONTAP-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.

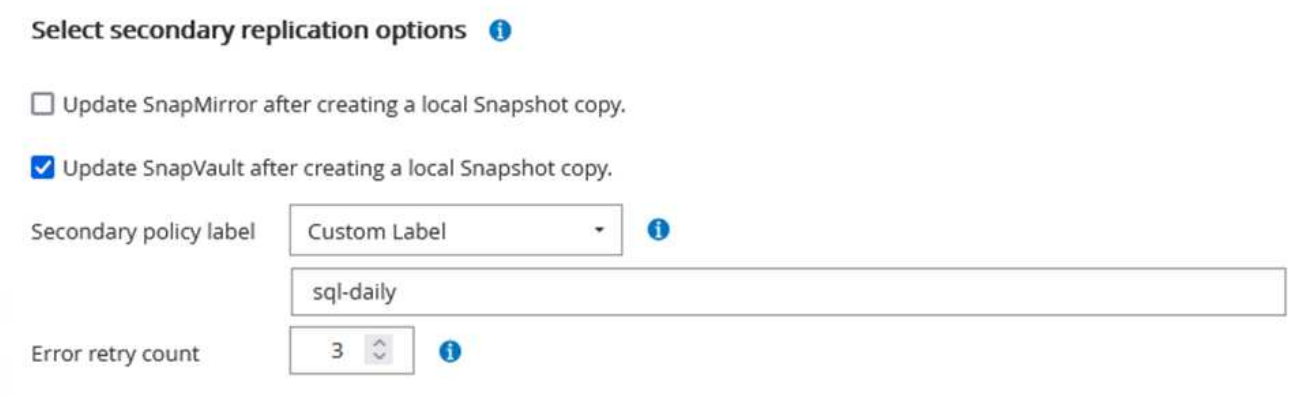
Création d'une règle de conservation des snapshots

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

```
ONTAP-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.

```
ONTAP-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 :

```
ONTAP-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 sur ONTAP un volume de destination qui sera destinataire des copies Snapshot de nos volumes source, exécutez la commande suivante sur le cluster ONTAP de destination :

```
ONTAP-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 le cluster ONTAP de destination :

```
ONTAP-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.

Pour créer un volume, exécutez la commande suivante sur le cluster ONTAP de destination :

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

Configuration du plug-in SnapCenter pour VMware vSphere

Une fois installé, le plug-in SnapCenter pour VMware vSphere est accessible à partir de l'interface de gestion de l'appliance vCenter Server. SCV gère les sauvegardes des datastores NFS montés sur les hôtes ESXi et contenant les machines virtuelles Windows et Linux.

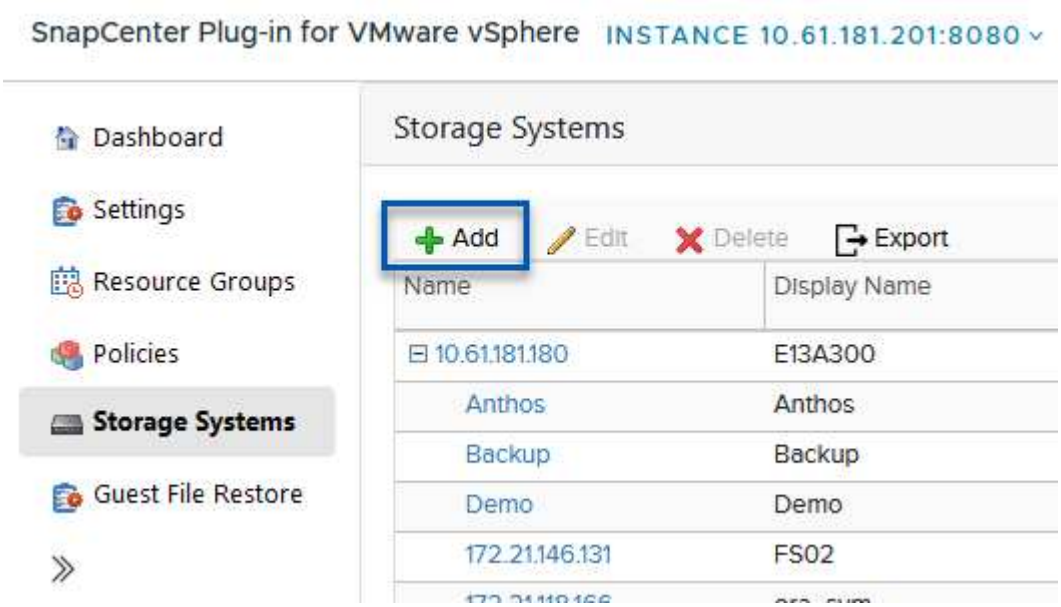
Vérifiez le "Flux de travail de protection des données" Section de la documentation SCV pour plus d'informations sur les étapes de configuration des sauvegardes.

Pour configurer les sauvegardes de vos machines virtuelles et de vos datastores, les étapes suivantes doivent être effectuées à partir de l'interface du plug-in.

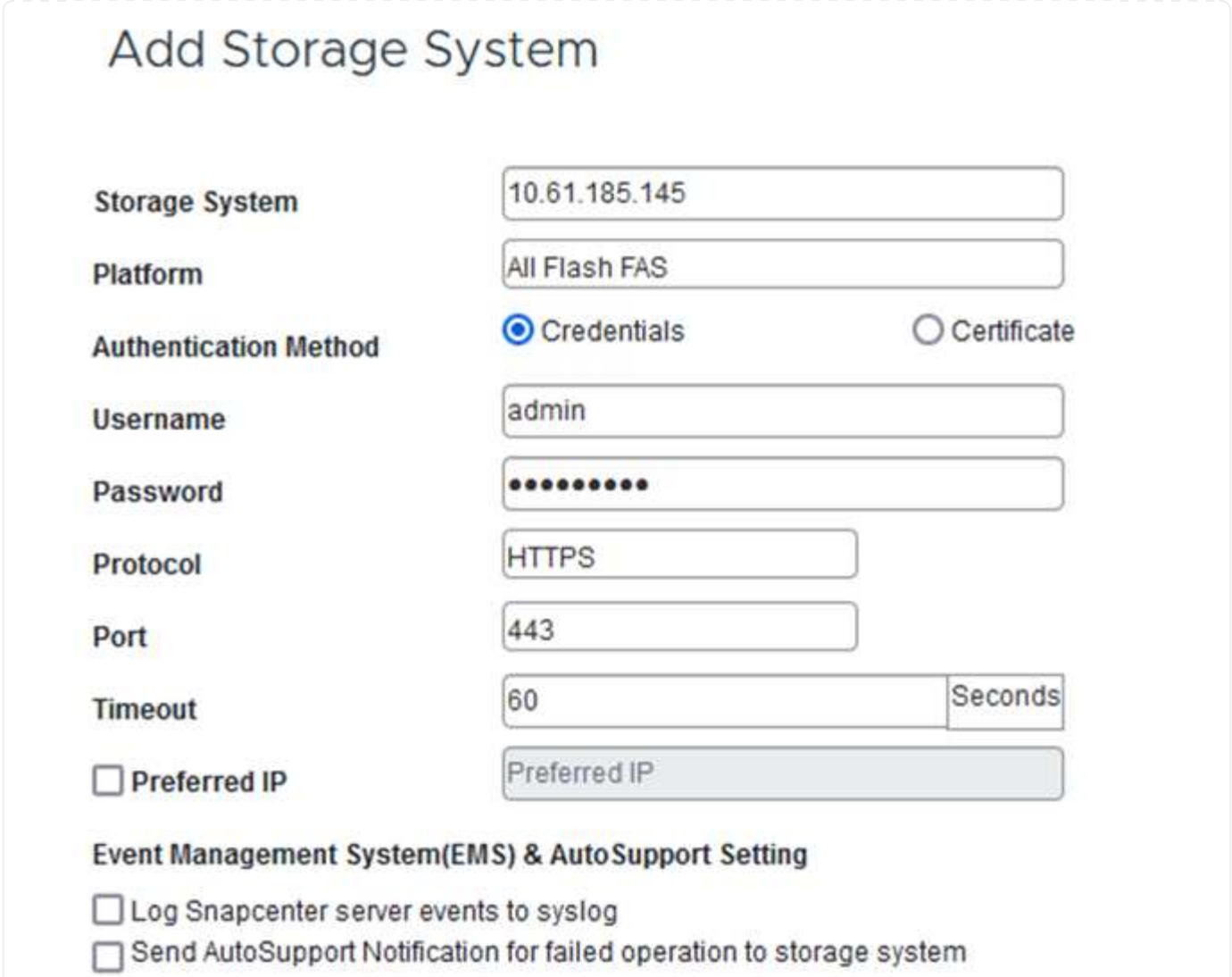
Découvrez les systèmes de stockage ONTAP

Découvrez les clusters de stockage ONTAP à utiliser pour les sauvegardes primaires et secondaires.

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **systèmes de stockage** dans le menu de gauche et cliquez sur le bouton **Ajouter**.



2. Renseignez les informations d'identification et le type de plate-forme du système de stockage ONTAP principal et cliquez sur **Ajouter**.



3. Répétez cette procédure pour le système de stockage ONTAP secondaire.

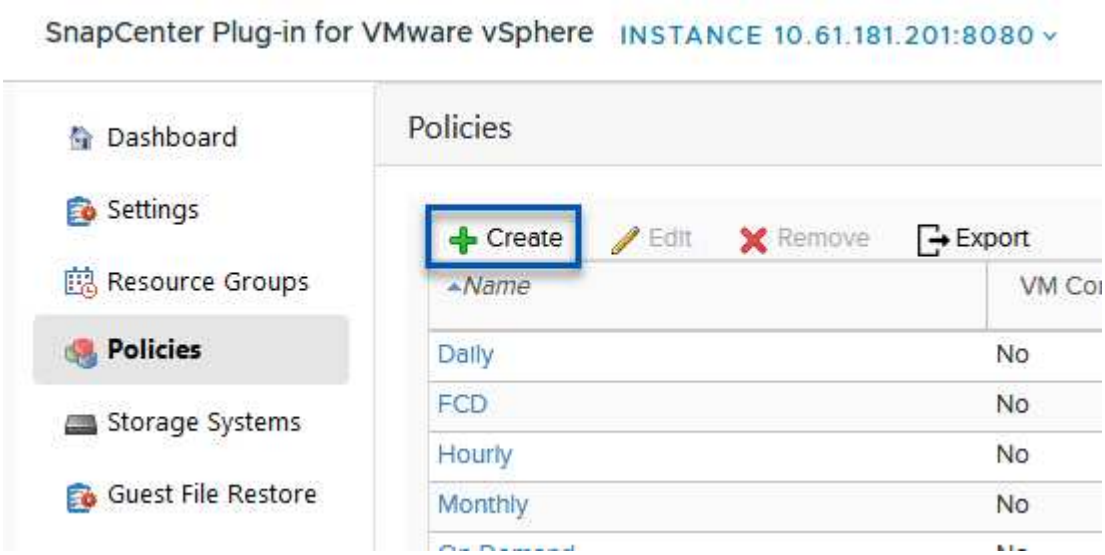
Créer des politiques de sauvegarde SCV

Les règles spécifient la période de rétention, la fréquence et les options de réplication pour les sauvegardes gérées par SCV.

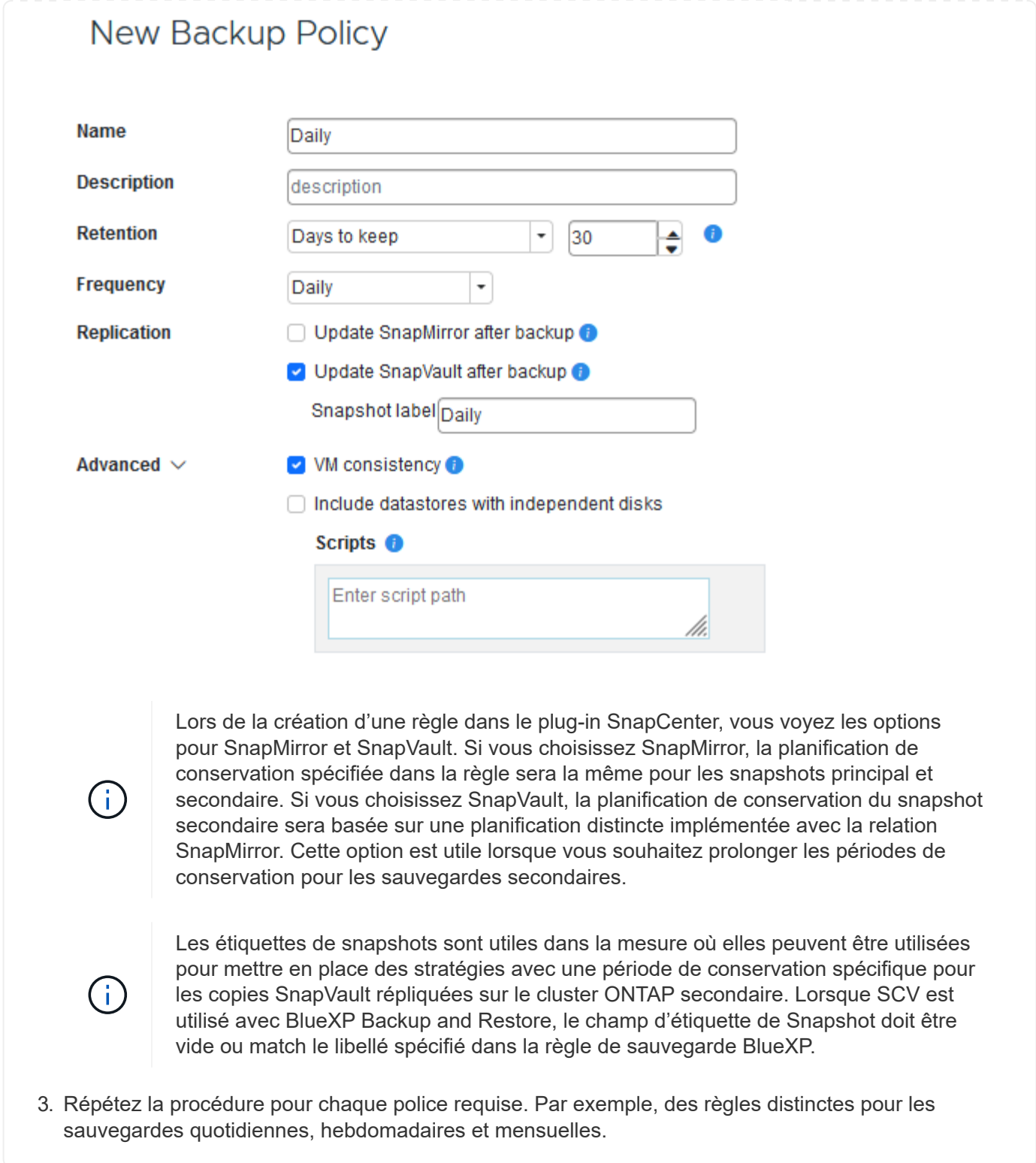
Vérifiez le "Créez des règles de sauvegarde pour les VM et les datastores" pour plus d'informations, reportez-vous à la section de la documentation.

Pour créer des stratégies de sauvegarde, procédez comme suit :

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **Policies** dans le menu de gauche et cliquez sur le bouton **Create**.



2. Spécifiez un nom pour la règle, la période de conservation, les options de fréquence et de réplication, ainsi que le libellé de l'instantané.



Lors de la création d'une règle dans le plug-in SnapCenter, vous voyez les options pour SnapMirror et SnapVault. Si vous choisissez SnapMirror, la planification de conservation spécifiée dans la règle sera la même pour les snapshots principal et secondaire. Si vous choisissez SnapVault, la planification de conservation du snapshot secondaire sera basée sur une planification distincte implémentée avec la relation SnapMirror. Cette option est utile lorsque vous souhaitez prolonger les périodes de conservation pour les sauvegardes secondaires.

Les étiquettes de snapshots sont utiles dans la mesure où elles peuvent être utilisées pour mettre en place des stratégies avec une période de conservation spécifique pour les copies SnapVault répliquées sur le cluster ONTAP secondaire. Lorsque SCV est utilisé avec BlueXP Backup and Restore, le champ d'étiquette de Snapshot doit être vide ou match le libellé spécifié dans la règle de sauvegarde BlueXP.

3. Répétez la procédure pour chaque police requise. Par exemple, des règles distinctes pour les sauvegardes quotidiennes, hebdomadaires et mensuelles.

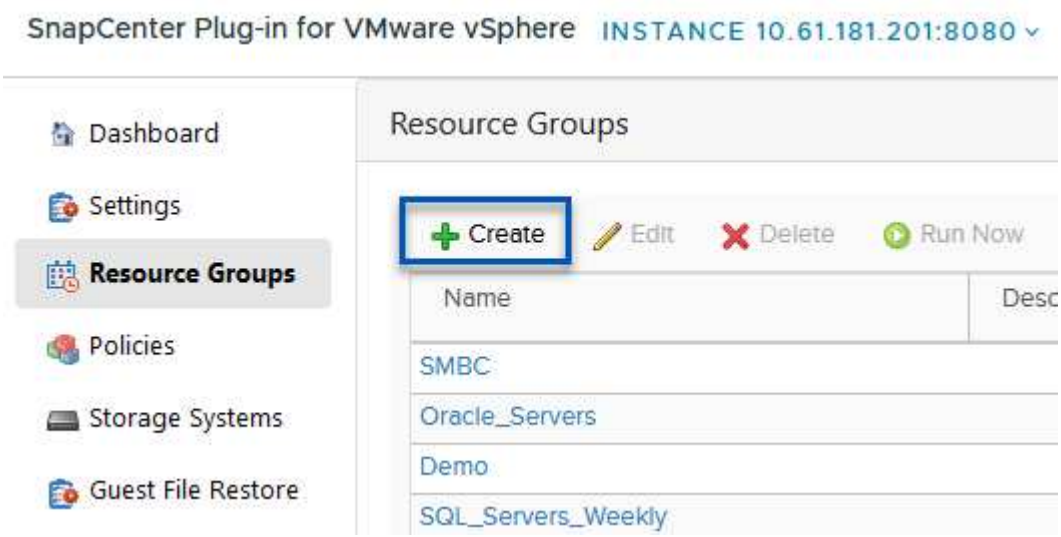
Créer des groupes de ressources

Les groupes de ressources contiennent les datastores et les machines virtuelles à inclure dans une tâche de sauvegarde, ainsi que la stratégie et le planning de sauvegarde associés.

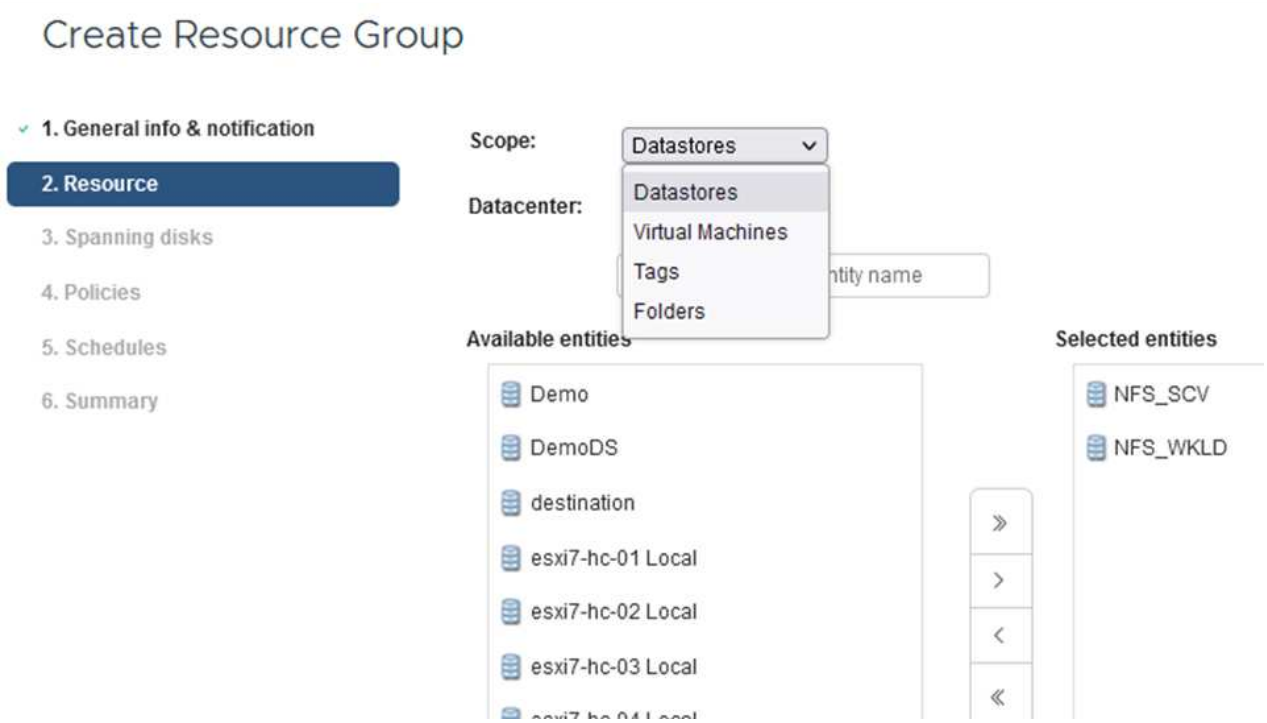
Vérifiez le "Créer des groupes de ressources" pour plus d'informations, reportez-vous à la section de la documentation.

Pour créer des groupes de ressources, procédez comme suit.

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **Resource Groups** dans le menu de gauche et cliquez sur le bouton **Create**.

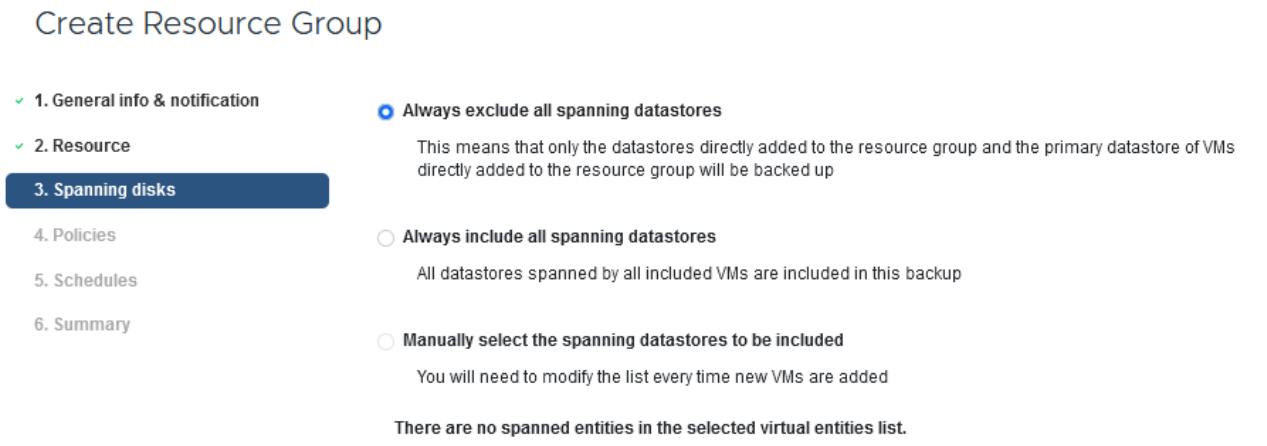


2. Dans l'assistant Créer un groupe de ressources, entrez un nom et une description pour le groupe, ainsi que les informations requises pour recevoir les notifications. Cliquez sur **Suivant**
3. Sur la page suivante, sélectionnez les datastores et les machines virtuelles à inclure dans la tâche de sauvegarde, puis cliquez sur **Suivant**.



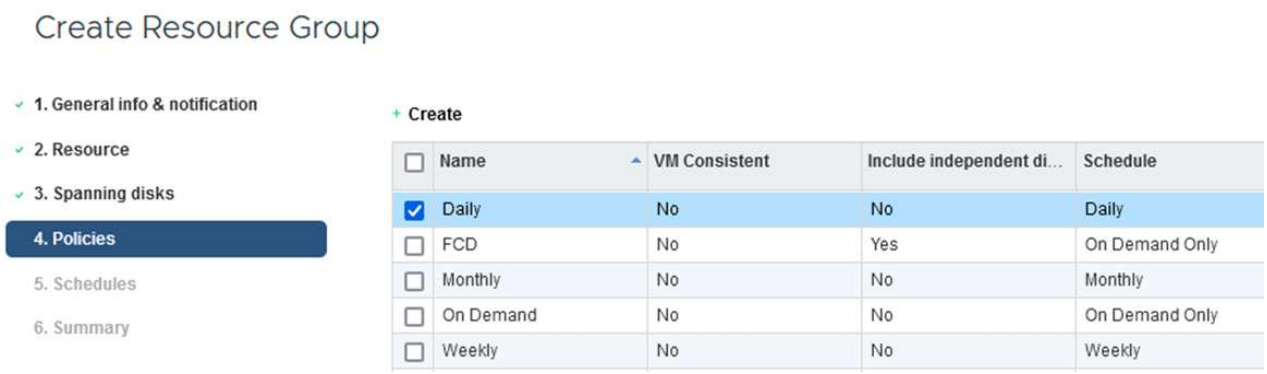
Vous avez la possibilité de sélectionner des VM spécifiques ou des datastores entiers. Quelle que soit l'option choisie, la totalité du volume (et du datastore) est sauvegardée, car la sauvegarde résulte de la création d'un snapshot du volume sous-jacent. Dans la plupart des cas, il est plus facile de choisir l'intégralité du datastore. Toutefois, si vous souhaitez limiter la liste des machines virtuelles disponibles lors de la restauration, vous ne pouvez choisir qu'un sous-ensemble de machines virtuelles à sauvegarder.

4. Choisissez des options de répartition des datastores pour les machines virtuelles avec VMDK qui résident sur plusieurs datastores, puis cliquez sur **Next**.



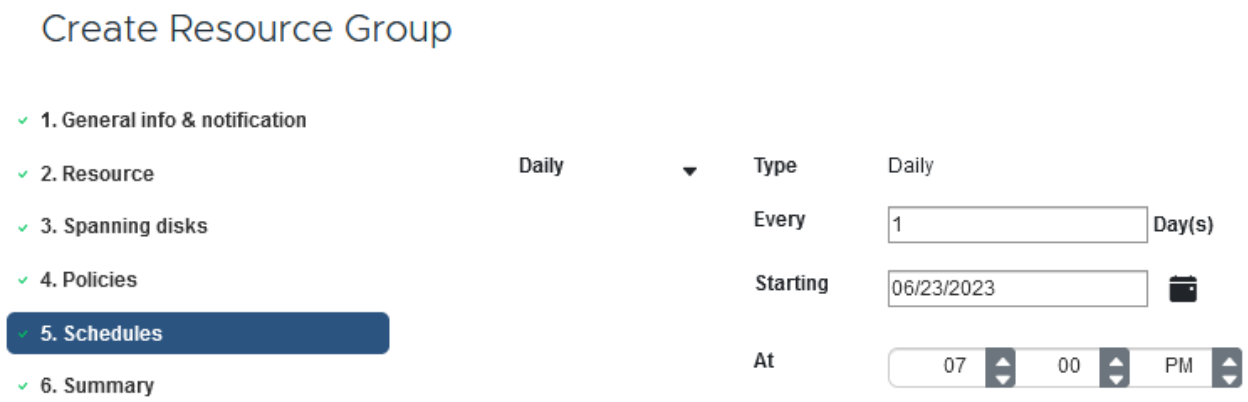
La sauvegarde et la restauration BlueXP ne prennent pas actuellement en charge la sauvegarde des machines virtuelles avec des VMDK qui s'étendent sur plusieurs datastores.

5. Sur la page suivante, sélectionnez les stratégies qui seront associées au groupe de ressources et cliquez sur **Suivant**.



Lors de la sauvegarde des snapshots gérés par SCV dans le stockage objet à l'aide de la sauvegarde et de la restauration BlueXP, chaque groupe de ressources ne peut être associé qu'à une seule règle.

6. Sélectionnez une planification qui déterminera à quelle heure les sauvegardes seront exécutées. Cliquez sur **Suivant**.

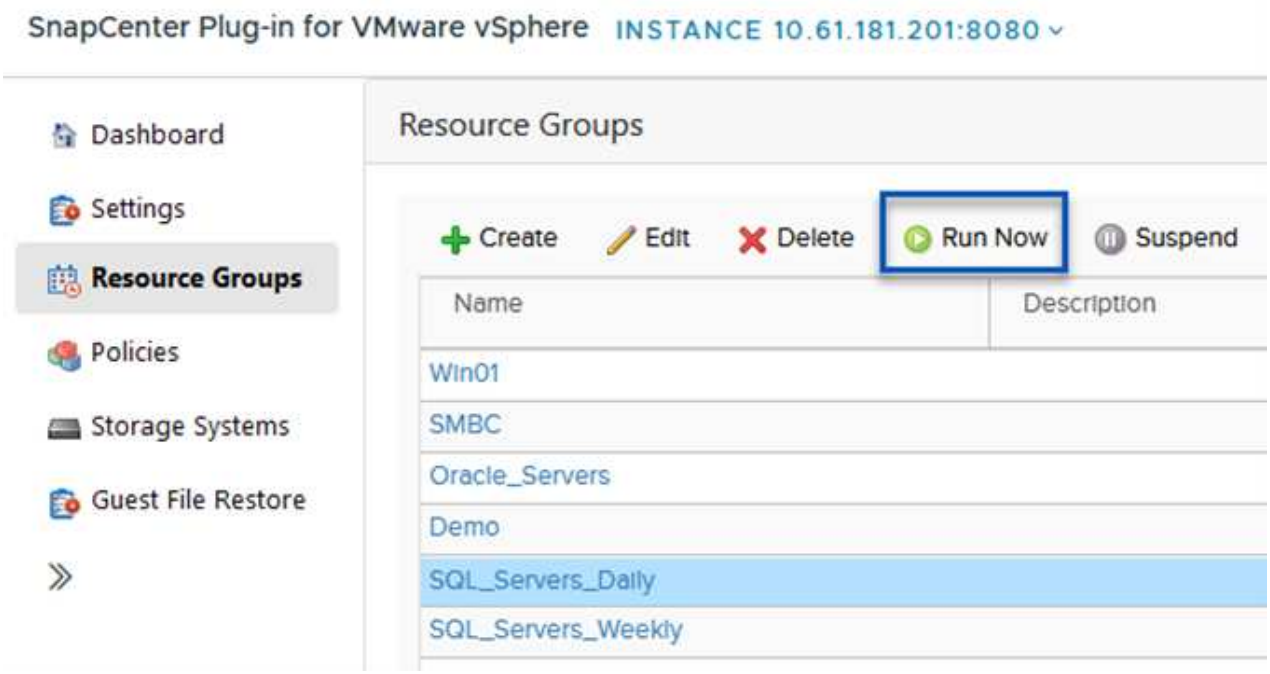


7. Enfin, passez en revue la page de résumé, puis sur **Terminer** pour terminer la création du groupe de ressources.

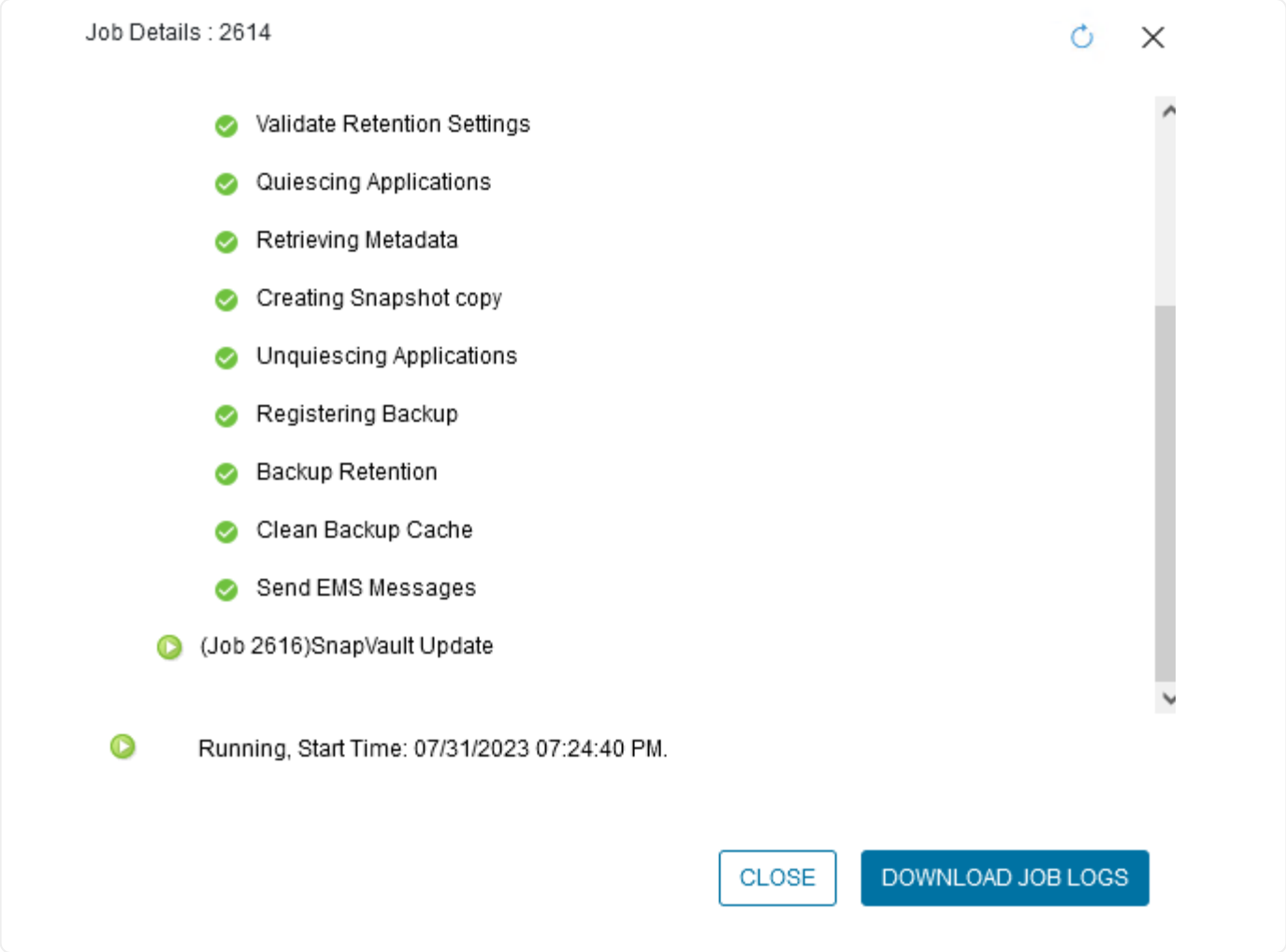
Exécutez une tâche de sauvegarde

Dans cette dernière étape, exécutez une tâche de sauvegarde et surveillez sa progression. Au moins une tâche de sauvegarde doit être effectuée avec succès dans SCV pour que les ressources puissent être découvertes à partir de la sauvegarde et de la restauration BlueXP.

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **Resource Groups** dans le menu de gauche.
2. Pour lancer une tâche de sauvegarde, sélectionnez le groupe de ressources souhaité et cliquez sur le bouton **Exécuter maintenant**.



3. Pour surveiller la tâche de sauvegarde, accédez à **Dashboard** dans le menu de gauche. Sous **activités récentes**, cliquez sur le numéro d'ID du travail pour surveiller la progression du travail.



Configurez les sauvegardes vers le stockage objet dans la sauvegarde et la restauration BlueXP

Pour que BlueXP puisse gérer efficacement l'infrastructure de données, il faut au préalable installer un connecteur. Le connecteur exécute les actions impliquées dans la découverte des ressources et la gestion des opérations de données.

Pour plus d'informations sur le connecteur BlueXP, reportez-vous à la section "En savoir plus sur les connecteurs" Dans la documentation BlueXP.

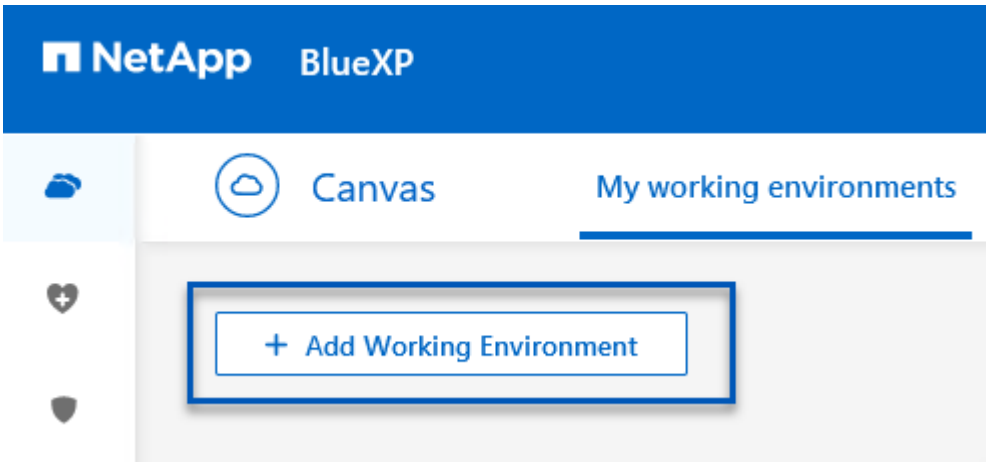
Une fois le connecteur installé pour le fournisseur de cloud utilisé, une représentation graphique du stockage objet est visible dans la zone de dessin.

Pour configurer la sauvegarde et la restauration BlueXP pour les données de sauvegarde gérées par SCV sur site, effectuez les opérations suivantes :

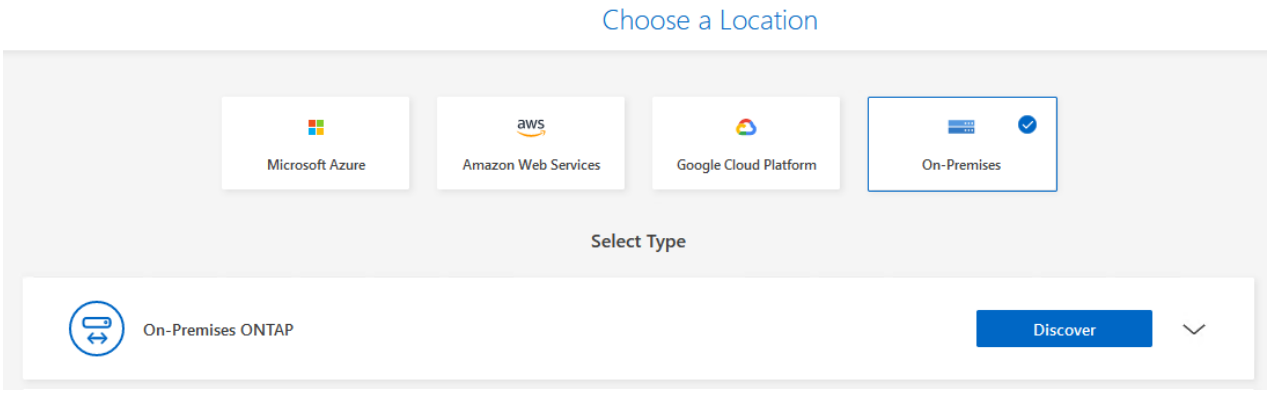
Ajoutez des environnements de travail au canevas

La première étape consiste à ajouter les systèmes de stockage ONTAP sur site à BlueXP

1. Dans la zone de travail, sélectionnez **Ajouter un environnement de travail** pour commencer.



2. Sélectionnez **sur place** dans les emplacements de votre choix, puis cliquez sur le bouton **découvrir**.



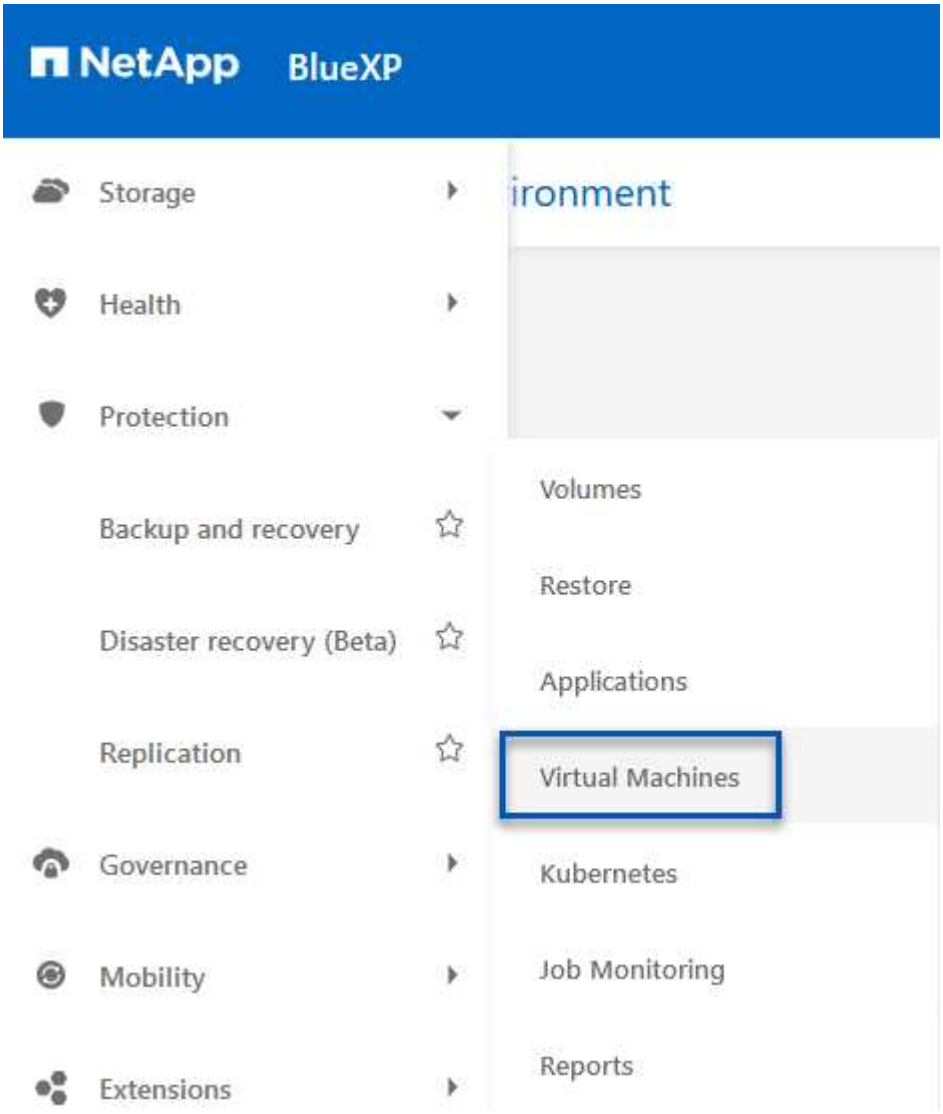
3. Renseignez les informations d'identification du système de stockage ONTAP et cliquez sur le bouton **découvrir** pour ajouter l'environnement de travail.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

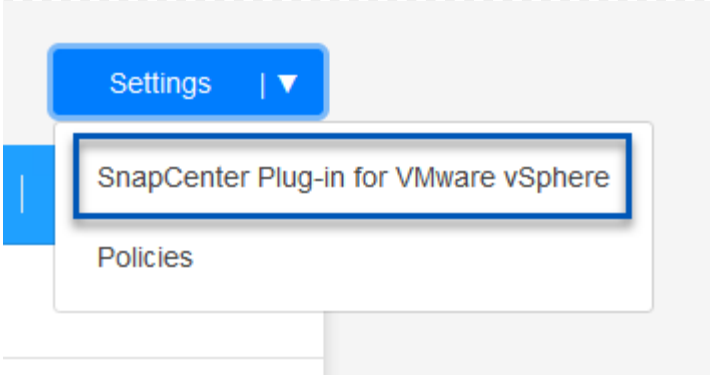
Découvrez l'appliance SCV sur site et vCenter

Pour découvrir les ressources des datastores sur site et des machines virtuelles, ajoutez des informations pour le courtier de données SCV et des informations d'identification pour l'appliance de gestion vCenter.

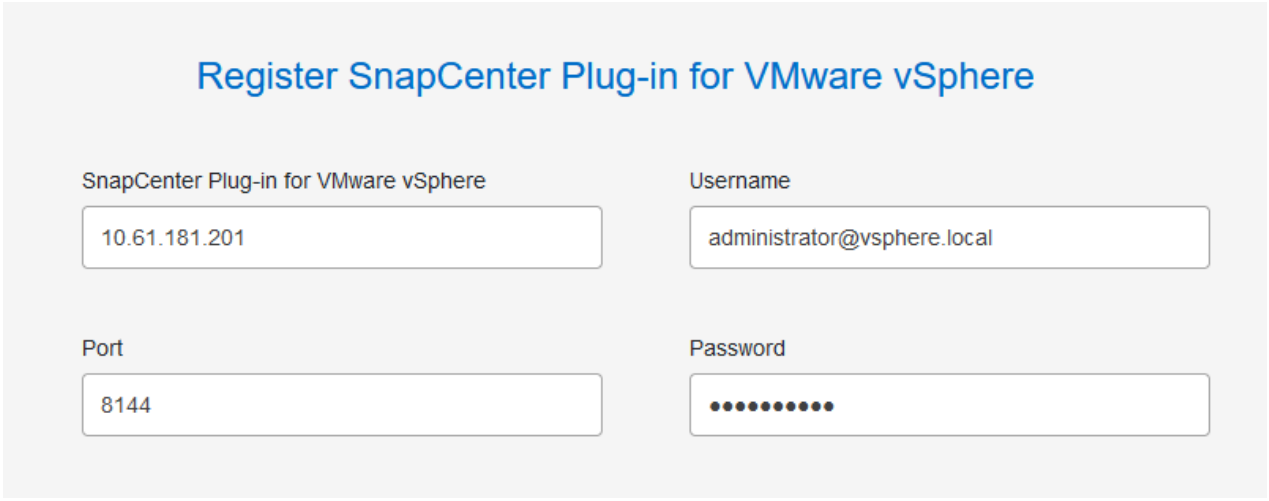
1. Dans le menu de gauche de BlueXP, sélectionnez **protection > sauvegarde et restauration > machines virtuelles**



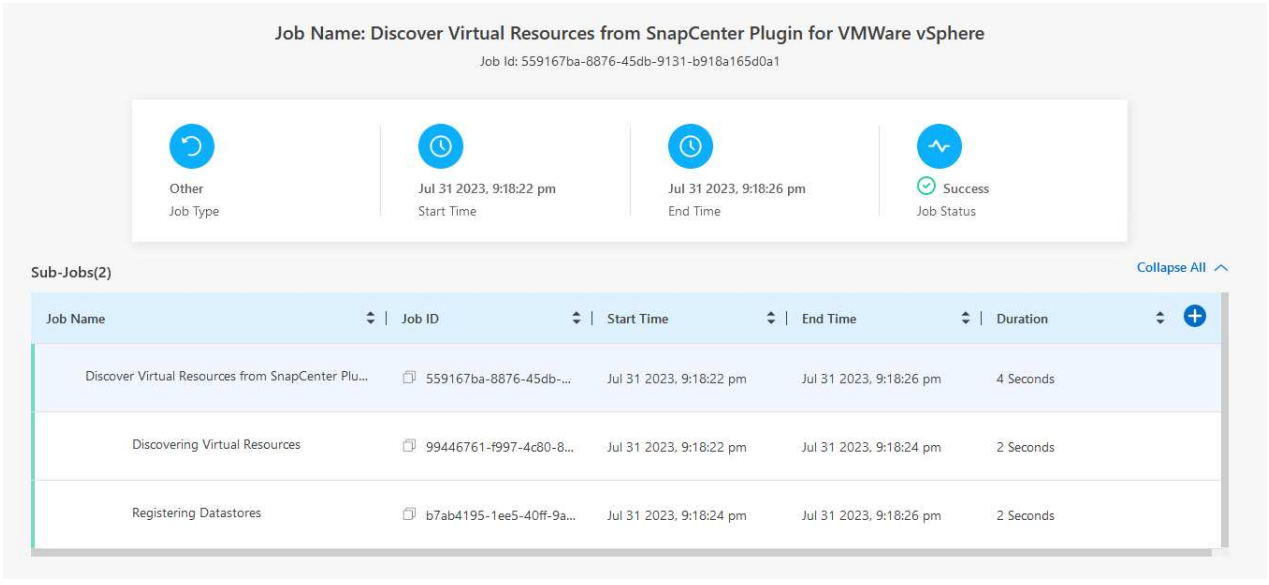
2. Dans l'écran principal des machines virtuelles, accédez au menu déroulant **Paramètres** et sélectionnez **Plug-in SnapCenter pour VMware vSphere**.



3. Cliquez sur le bouton **Enregistrer**, puis entrez l'adresse IP et le numéro de port de l'appliance de plug-in SnapCenter, ainsi que le nom d'utilisateur et le mot de passe de l'appliance de gestion vCenter. Cliquez sur le bouton **Register** pour commencer le processus de découverte.



4. La progression des travaux peut être contrôlée à partir de l'onglet surveillance des travaux.



5. Une fois la découverte terminée, vous pourrez afficher les datastores et les machines virtuelles sur tous les dispositifs SCV découverts.

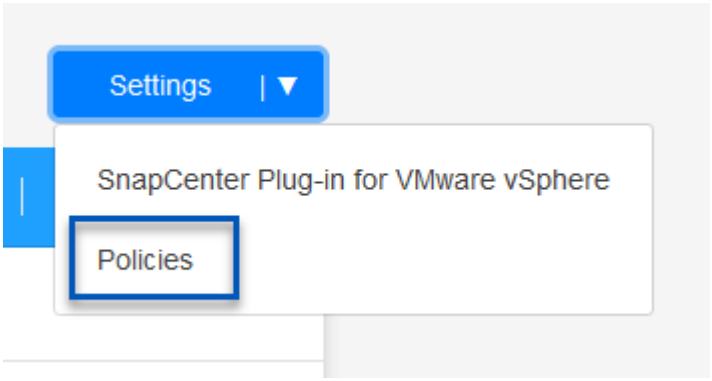
   Image ::bxp-scv-Hybrid-23.png[Afficher les ressources disponibles]

Créez des règles de sauvegarde BlueXP

Dans le cadre de la sauvegarde et de la restauration BlueXP pour les machines virtuelles, créez des règles pour spécifier la période de conservation, la source de sauvegarde et la règle d'archivage.

Pour plus d'informations sur la création de règles, reportez-vous à la section "Créer une stratégie pour sauvegarder les datastores".

1. Sur la page principale de BlueXP Backup and Recovery for Virtual machines, accédez au menu déroulant **Settings** et sélectionnez **Policies**.



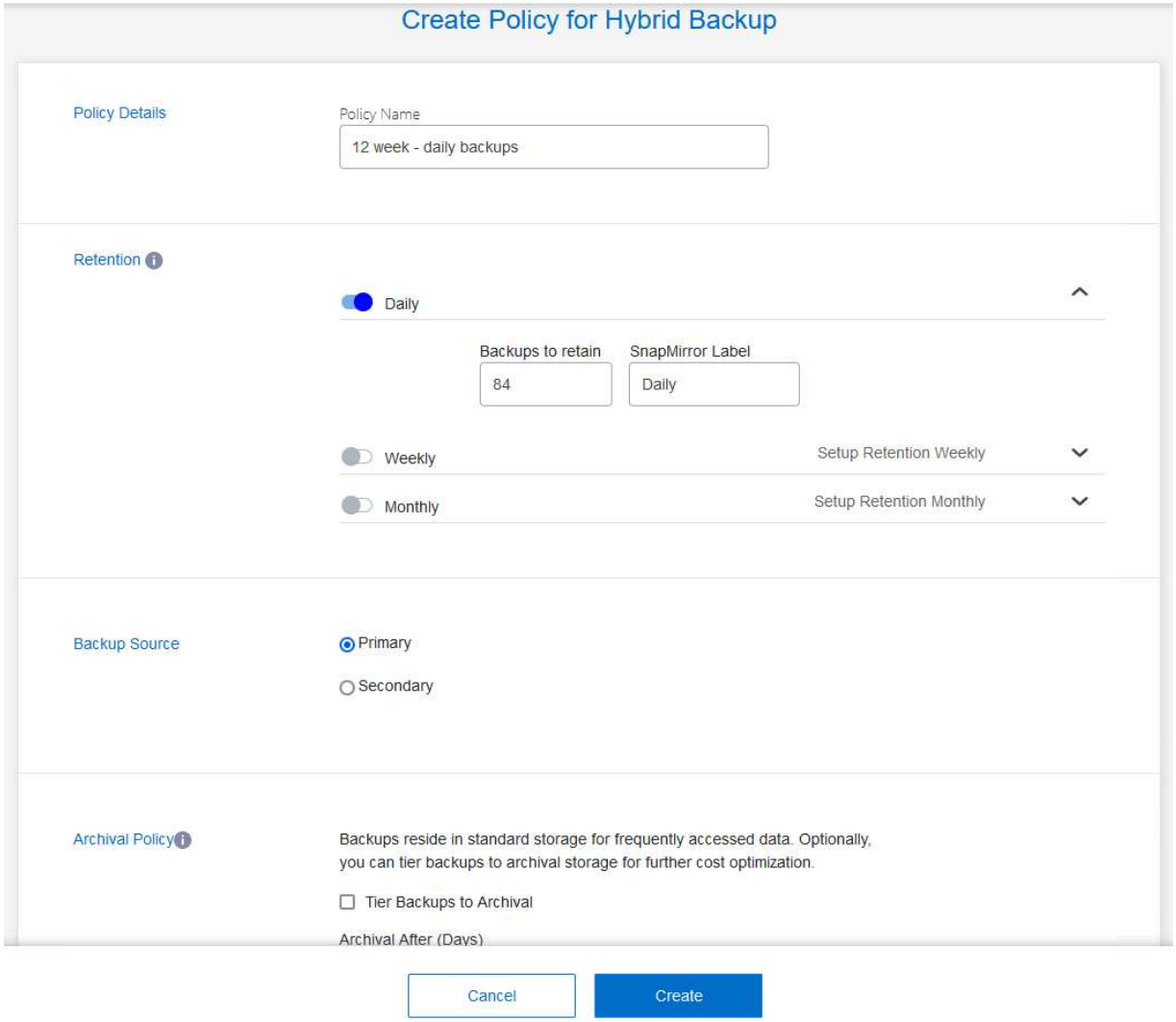
2. Cliquez sur **Create Policy** pour accéder à la fenêtre **Create Policy for Hybrid Backup**.

   a. Ajoutez un nom à la règle

   b. Sélectionnez la période de conservation souhaitée

   c. Indiquez si les sauvegardes seront effectuées à partir du système de stockage ONTAP sur site principal ou secondaire

   d. Vous pouvez également spécifier après quelle période les sauvegardes seront hiérarchisées vers le stockage d'archivage pour réaliser des économies supplémentaires.



Le libellé SnapMirror saisi ici permet également d'identifier les sauvegardes à appliquer à la règle. Le nom de l'étiquette doit correspondre au nom de l'étiquette dans la politique de distributeur sélectif sur site correspondante.

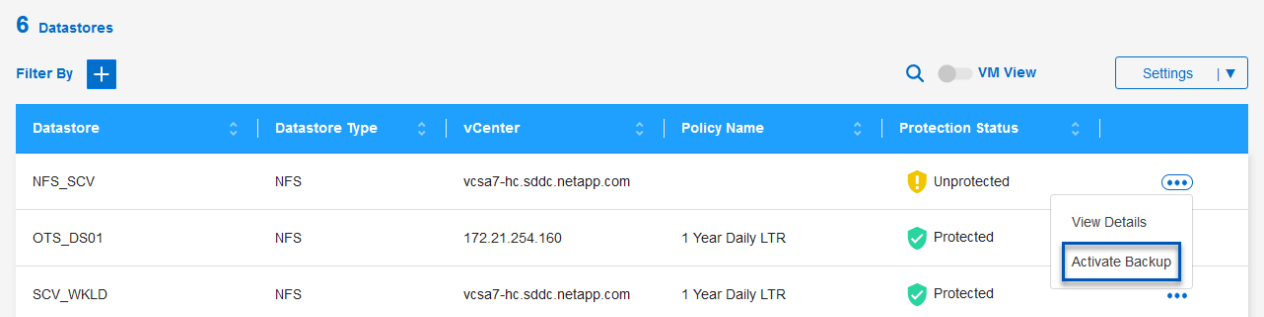
3. Cliquez sur **Créer** pour terminer la création de la police.

Sauvegarde des datastores vers Amazon Web Services

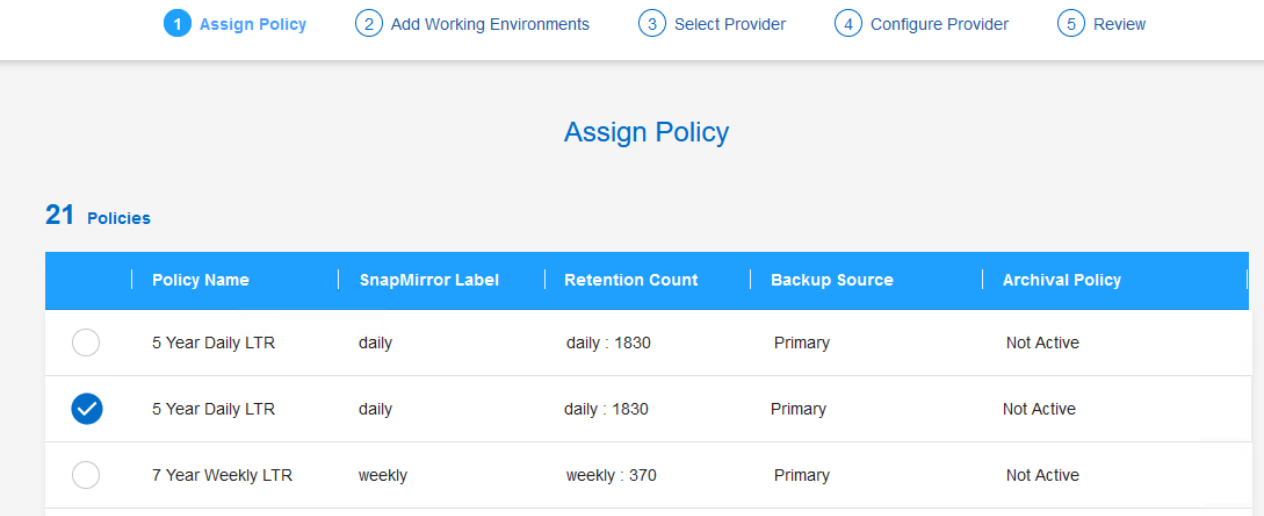
L'étape finale consiste à activer la protection des données pour les datastores et les machines virtuelles individuels. Les étapes suivantes expliquent comment activer les sauvegardes dans AWS.

Pour plus d'informations, reportez-vous à la section "Sauvegarde des datastores dans Amazon Web Services".

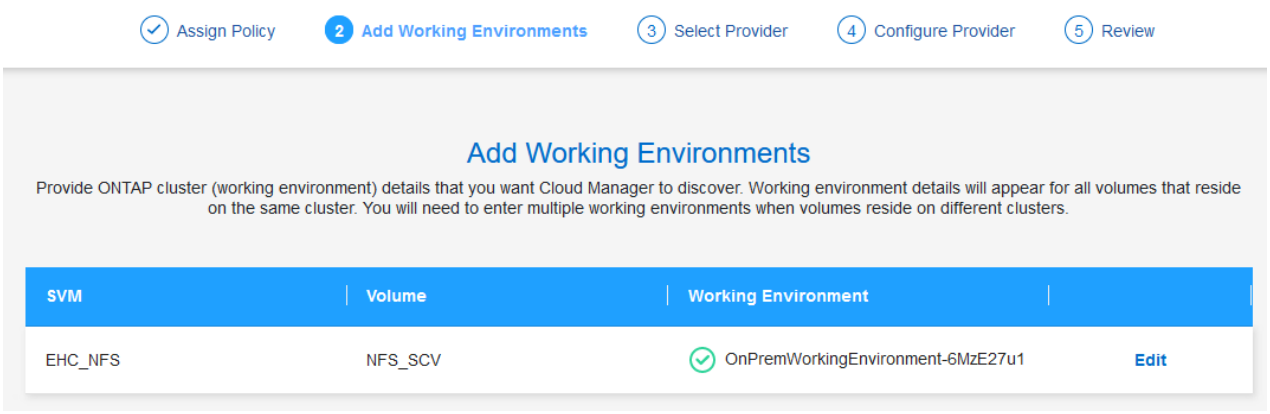
1. Sur la page principale sauvegarde et restauration BlueXP pour les machines virtuelles, accédez à la liste déroulante des paramètres du datastore à sauvegarder et sélectionnez **Activer la sauvegarde**.



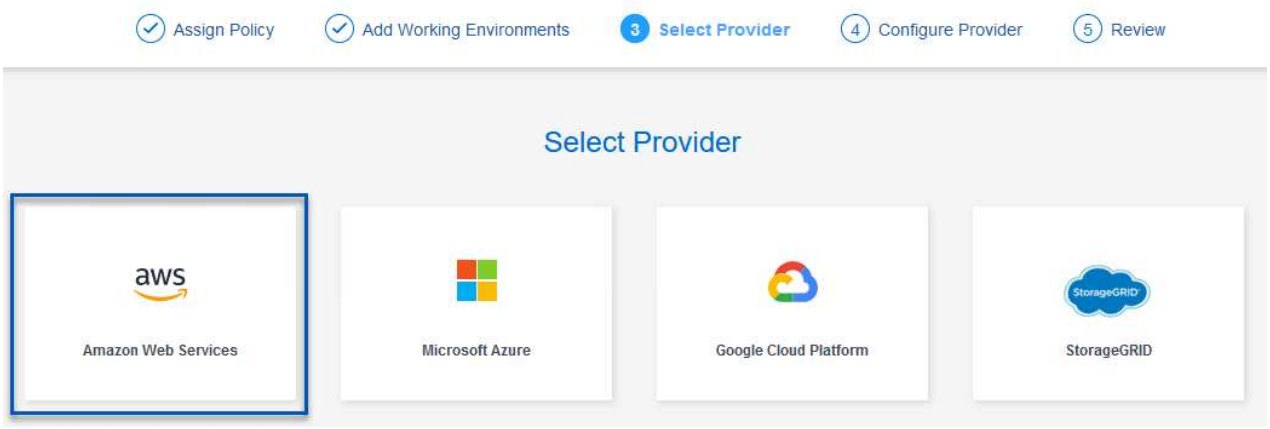
2. Attribuez la stratégie à utiliser pour l'opération de protection des données et cliquez sur **Suivant**.



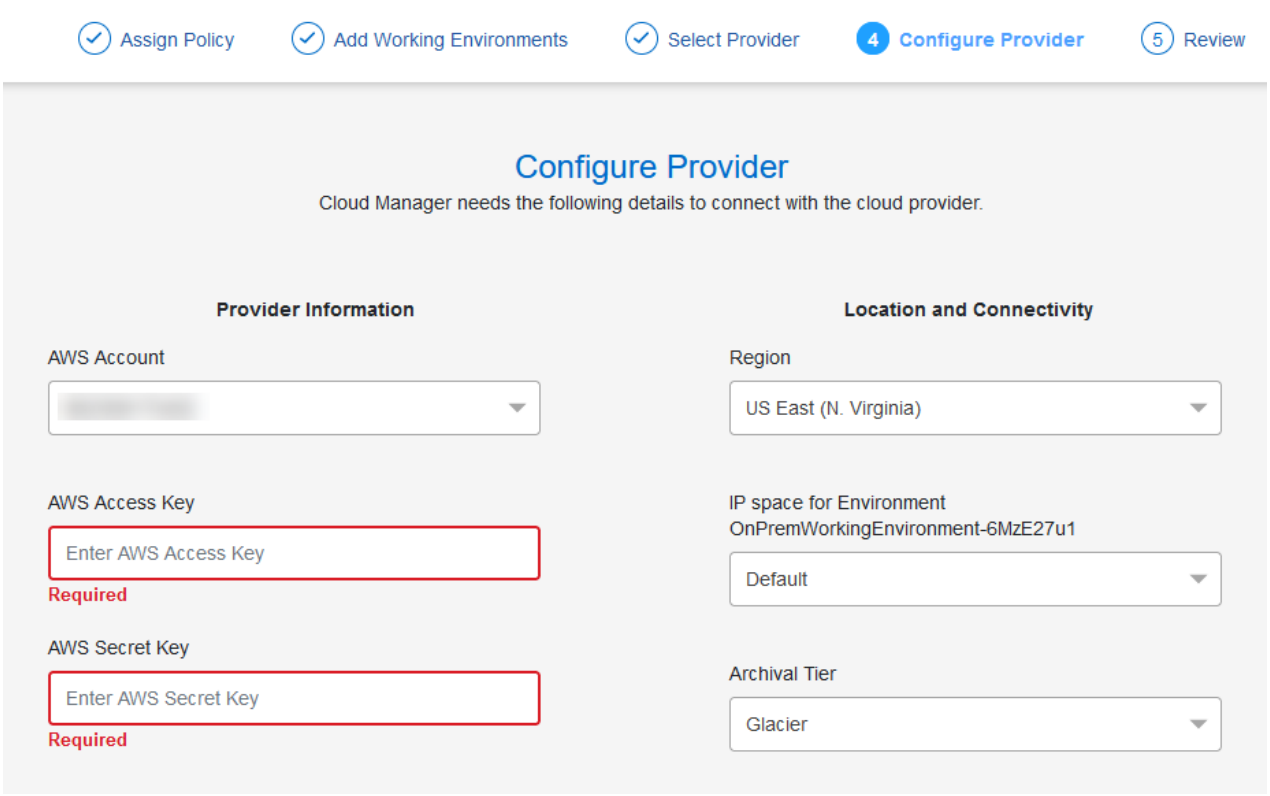
3. Sur la page **Ajouter des environnements de travail**, le datastore et l'environnement de travail avec une coche doivent apparaître si l'environnement de travail a été découvert précédemment. Si l'environnement de travail n'a pas été découvert précédemment, vous pouvez l'ajouter ici. Cliquez sur **Suivant** pour continuer.



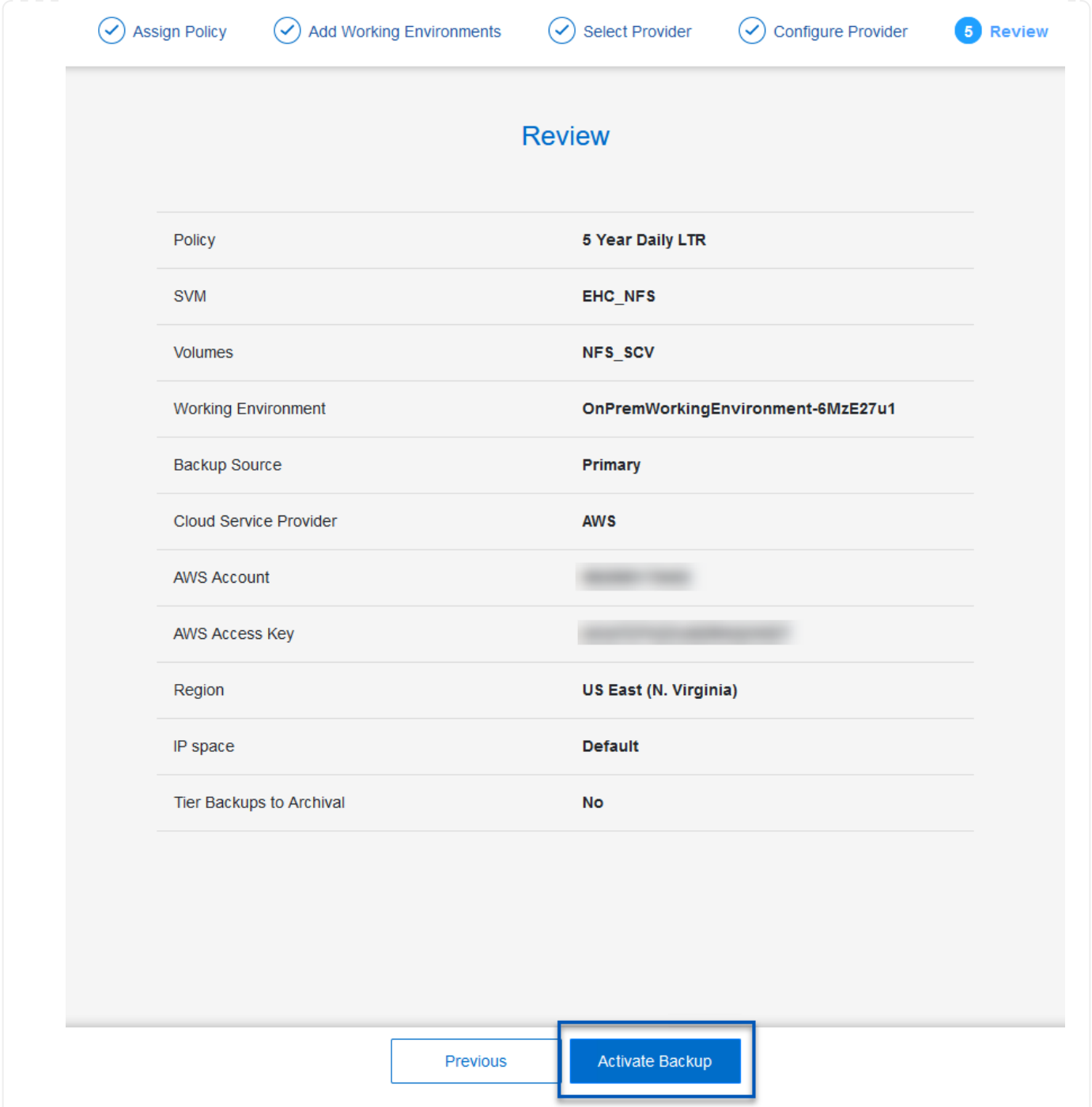
4. Sur la page **Select Provider**, cliquez sur AWS, puis sur le bouton **Next** pour continuer.



5. Remplissez les informations d'identification spécifiques au fournisseur pour AWS, notamment la clé d'accès AWS et la clé secrète, la région et le Tier d'archivage à utiliser. Vous pouvez également sélectionner l'espace IP ONTAP du système de stockage ONTAP sur site. Cliquez sur **Suivant**.



6. Enfin, passez en revue les détails de la tâche de sauvegarde et cliquez sur le bouton **Activer la sauvegarde** pour lancer la protection des données du datastore.



À ce stade, le transfert de données peut ne pas commencer immédiatement. La sauvegarde et la restauration BlueXP analysent afin de détecter tout snapshot exceptionnel toutes les heures, puis les transfère vers le stockage objet.

Restauration de machines virtuelles en cas de perte de données

Assurer la sauvegarde de vos données n'est qu'un aspect de la protection complète des données. Il est tout aussi important de pouvoir restaurer rapidement vos données en tout lieu en cas de perte de données ou d'attaque par ransomware. Cette fonctionnalité est essentielle pour assurer la transparence des opérations et atteindre les objectifs de point de récupération.

NetApp propose une stratégie 3-2-1 extrêmement flexible qui offre un contrôle personnalisé des calendriers de conservation dans les emplacements de stockage principal, secondaire et objet. Cette stratégie offre la flexibilité nécessaire pour adapter les approches de protection des données aux besoins spécifiques.

Cette section présente le processus de restauration des données du plug-in SnapCenter pour VMware vSphere ainsi que la sauvegarde et la restauration BlueXP pour les machines virtuelles.

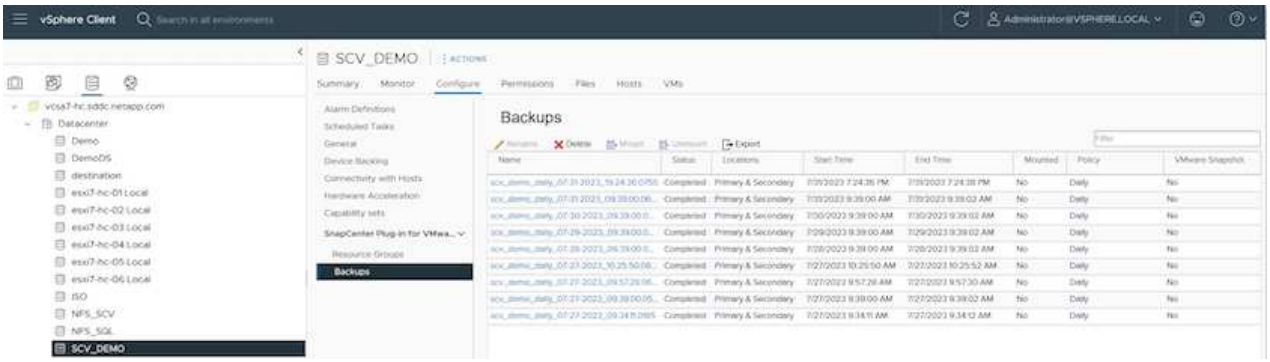
Restauration de machines virtuelles à partir du plug-in SnapCenter pour VMware vSphere

Pour cette solution, les machines virtuelles ont été restaurées dans leur emplacement d'origine et dans d'autres emplacements. Tous les aspects des capacités de restauration des données de SCV ne seront pas abordés dans cette solution. Pour plus d'informations sur tout ce que le distributeur auxiliaire doit offrir, voir "Restauration de machines virtuelles à partir des sauvegardes" dans la documentation du produit.

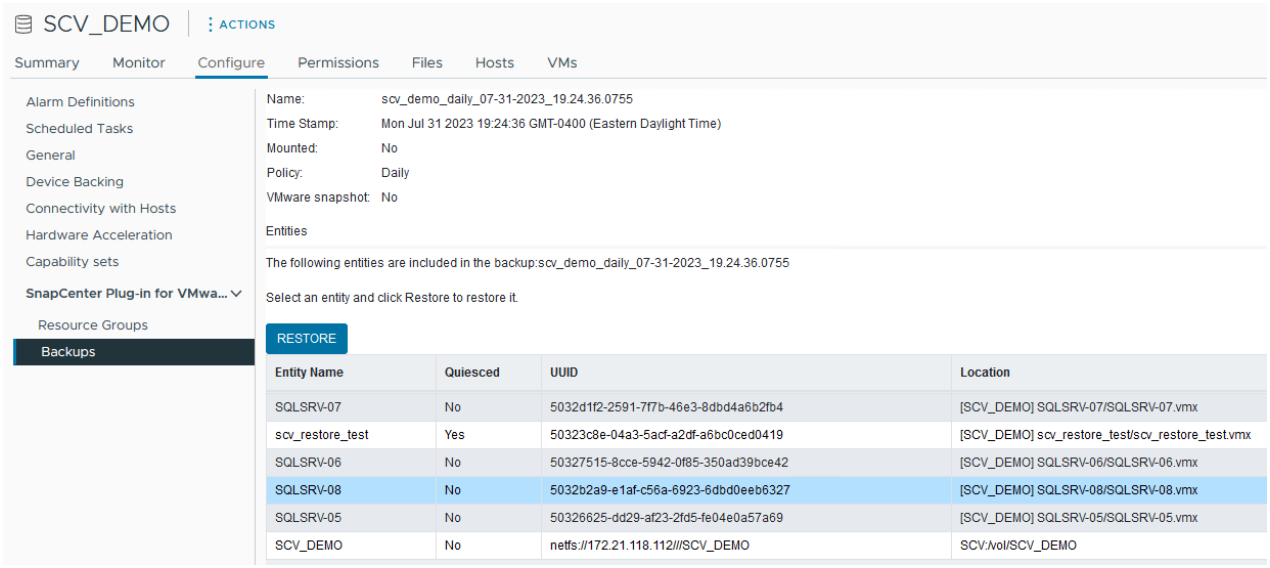
Restaurer les machines virtuelles à partir du distributeur sélectif

Procédez comme suit pour restaurer une machine virtuelle à partir du stockage principal ou secondaire.

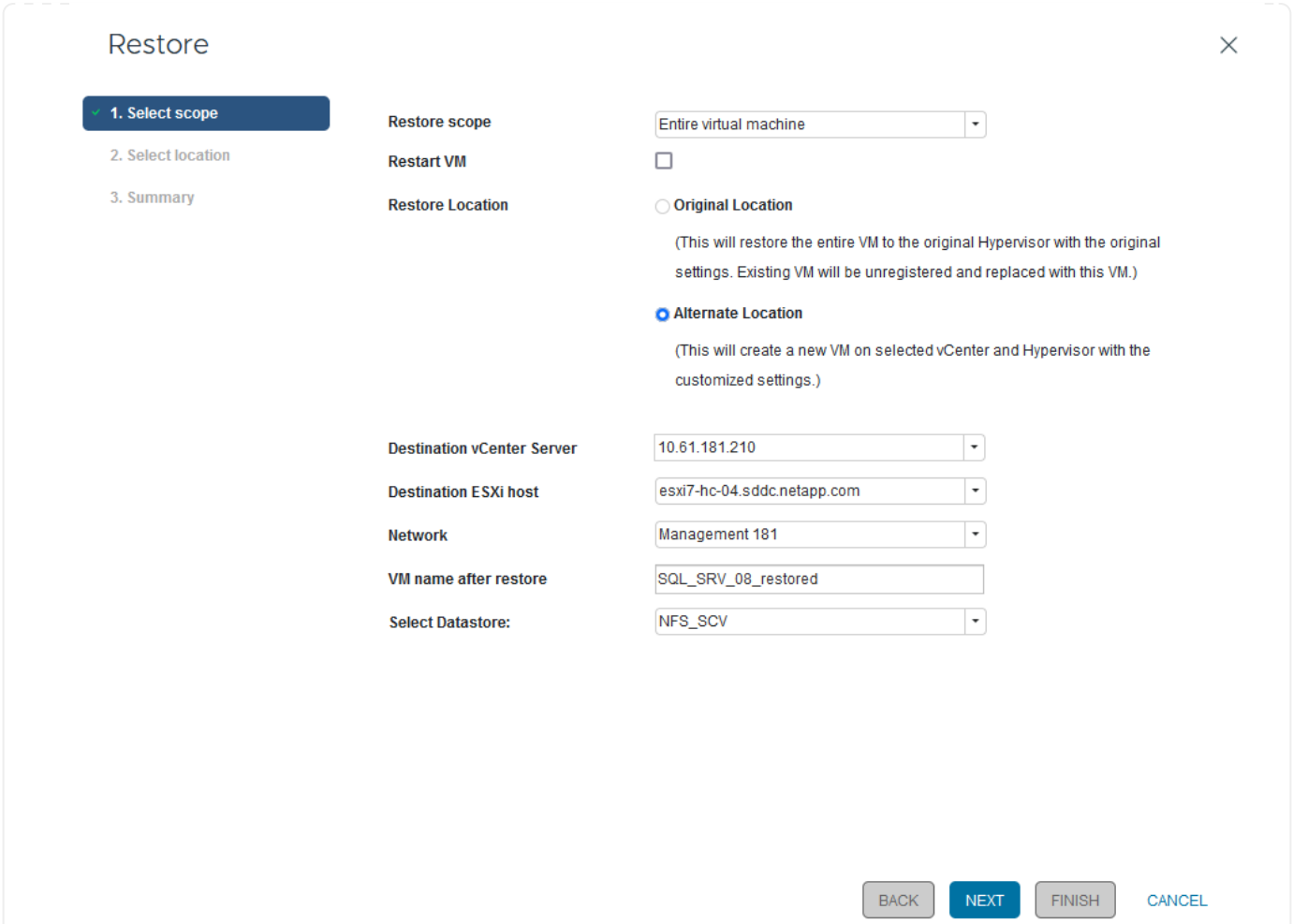
1. Dans le client vCenter, accédez à **Inventory > Storage** et cliquez sur le datastore contenant les machines virtuelles que vous souhaitez restaurer.
2. Dans l'onglet **configurer**, cliquez sur **sauvegardes** pour accéder à la liste des sauvegardes disponibles.



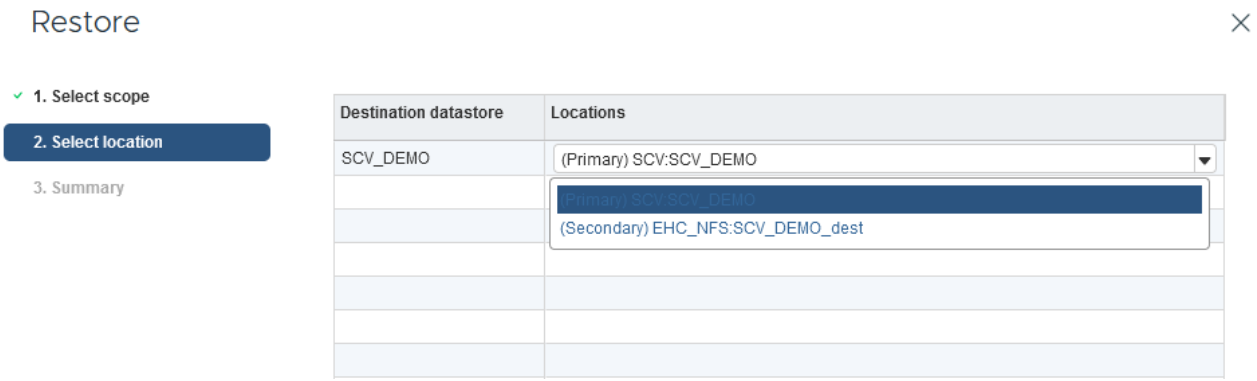
3. Cliquez sur une sauvegarde pour accéder à la liste des machines virtuelles, puis sélectionnez une machine virtuelle à restaurer. Cliquez sur **Restaurer**.



4. Dans l'assistant de restauration, sélectionnez pour restaurer la machine virtuelle entière ou un VMDK spécifique. Sélectionnez cette option pour installer dans l'emplacement d'origine ou dans un autre emplacement, indiquez le nom de la machine virtuelle après la restauration et le datastore de destination. Cliquez sur **Suivant**.



5. Choisissez de sauvegarder vos données depuis l'emplacement de stockage principal ou secondaire.



6. Enfin, consultez un résumé de la procédure de sauvegarde et cliquez sur Terminer pour lancer le processus de restauration.

Restauration des machines virtuelles à partir de la sauvegarde et de la restauration BlueXP pour les machines virtuelles

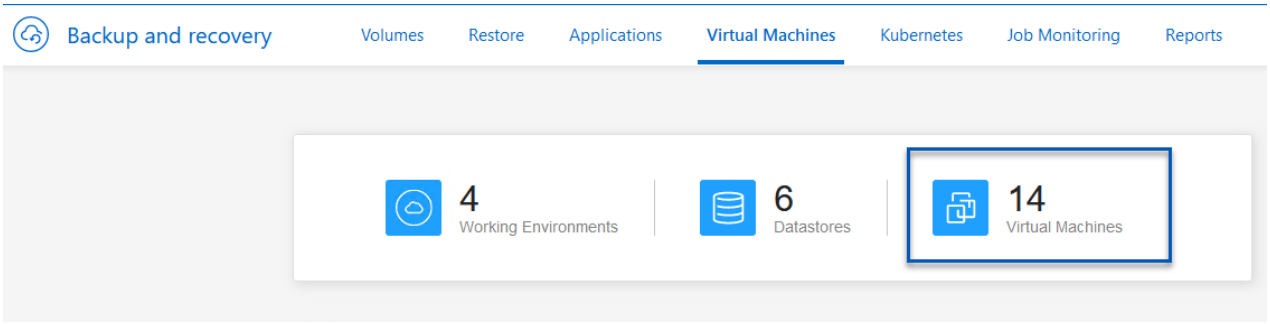
La sauvegarde et la restauration BlueXP pour les machines virtuelles permettent de restaurer les machines virtuelles à leur emplacement d'origine. Les fonctions de restauration sont accessibles via la console Web BlueXP.

Pour plus d’informations, reportez-vous à la section "Restaurez des données de machines virtuelles à partir du cloud".

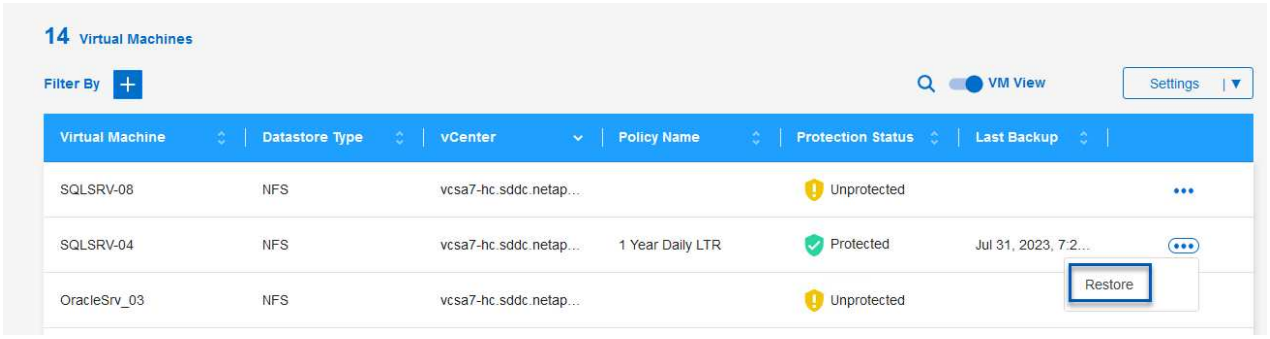
Restaurez les machines virtuelles à partir de la sauvegarde et de la restauration BlueXP

Pour restaurer une machine virtuelle à partir de la sauvegarde et de la restauration BlueXP, procédez comme suit.

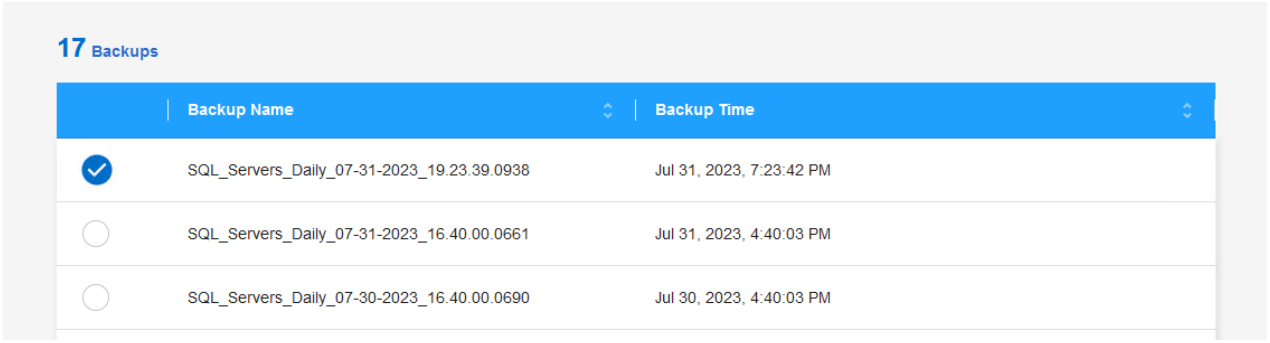
1. Accédez à **protection > sauvegarde et restauration > machines virtuelles** et cliquez sur machines virtuelles pour afficher la liste des machines virtuelles à restaurer.



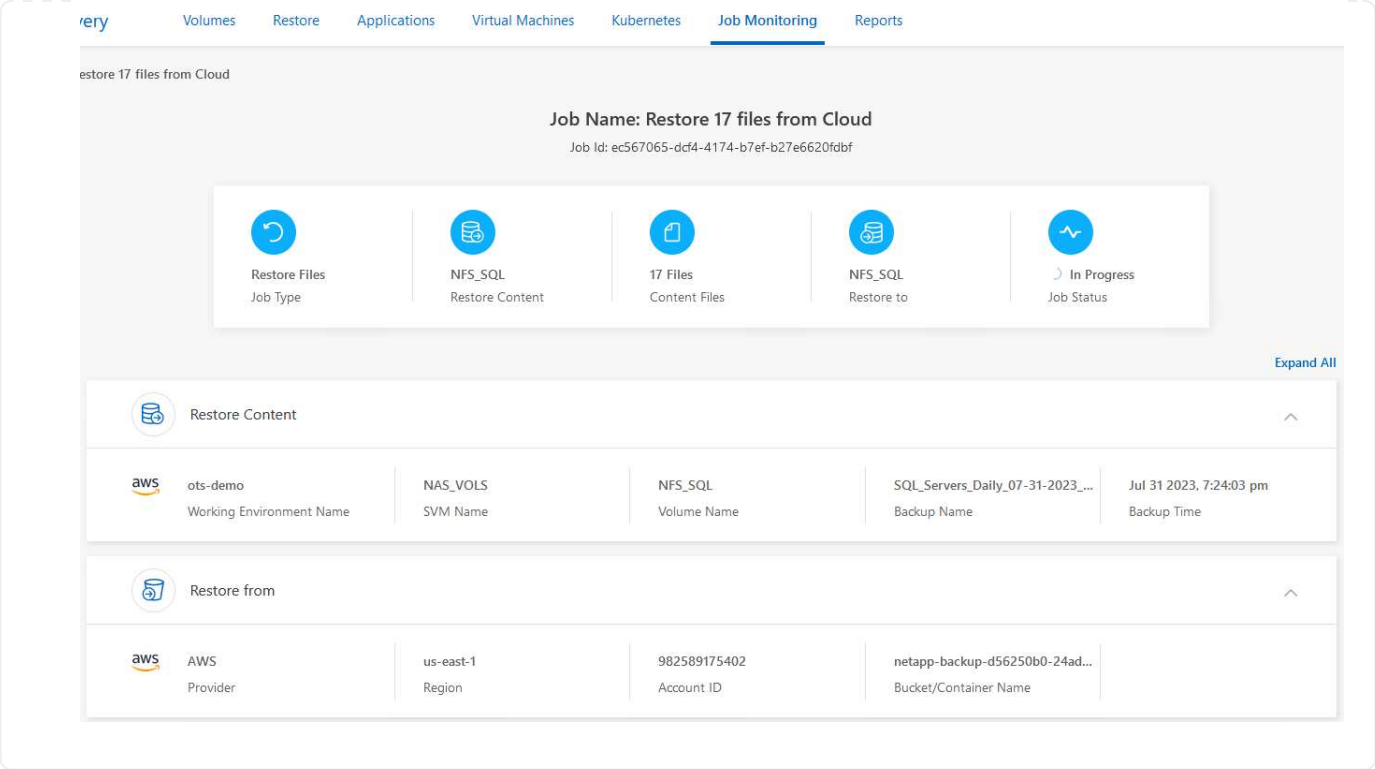
2. Accédez au menu déroulant des paramètres de la machine virtuelle à restaurer et sélectionnez



3. Sélectionnez la sauvegarde à partir de laquelle effectuer la restauration et cliquez sur **Suivant**.



4. Consultez un résumé de la procédure de sauvegarde et cliquez sur **Restore** pour lancer le processus de restauration.
5. Surveillez la progression du travail de restauration à partir de l'onglet **Job Monitoring**.



Conclusion

La stratégie de sauvegarde 3-2-1, implémentée avec le plug-in SnapCenter pour VMware vSphere et la sauvegarde et restauration BlueXP pour les machines virtuelles, offre une solution de protection des données robuste, fiable et économique. Cette stratégie assure non seulement la redondance et l'accessibilité des données, mais également la flexibilité de restauration des données en tout lieu et à partir des systèmes de stockage ONTAP sur site et du stockage objet basé dans le cloud.

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 les principaux fournisseurs de cloud. Le plug-in SnapCenter pour VMware vSphere permet une intégration transparente à VMware vSphere, ce qui permet une gestion efficace et centralisée des opérations de protection des données. Cette intégration rationalise les processus de sauvegarde et de restauration des machines virtuelles, facilitant ainsi la planification, la surveillance et les opérations de restauration flexibles au sein de l'écosystème VMware. La sauvegarde et la restauration BlueXP pour les machines virtuelles fournissent une (1) solution en 3-2-1, grâce à des sauvegardes sécurisées et à air Gap des données des machines virtuelles vers un stockage objet basé sur le cloud. L'interface intuitive et le flux de travail logique offrent une plate-forme sécurisée pour l'archivage à long terme des données critiques.

Informations supplémentaires

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

- "Documentation du plug-in SnapCenter pour VMware vSphere"
- "Documentation BlueXP"

Cloud souverain VMware

Ressources VMware pour le cloud souverain

NetApp et cloud souverain VMware

Présentation de VMware Sovereign Cloud

Pour de nombreuses entités qui traitent et conservent des données hautement sensibles, telles que les administrations nationales et gouvernementales, et les secteurs où les réglementations sont très strictes, comme la finance et la santé, le concept de souveraineté fait son apparition. Les gouvernements nationaux cherchent également à étendre leurs capacités économiques numériques et à réduire la dépendance envers les entreprises multinationales pour leurs services cloud.

Initiative VMware Sovereign Cloud

VMware définit un cloud souverain comme un cloud qui :

- Protège et valorise les données stratégiques (par exemple, les données nationales, les données d'entreprise et les données personnelles) pour les entreprises du secteur public et privé
- Une capacité nationale pour l'économie numérique
- Sécurisation des données grâce à des contrôles de sécurité vérifiés
- Garantit la conformité aux lois sur la confidentialité des données
- Améliore le contrôle des données en garantissant à la fois la résidence et la souveraineté des données tout en assurant un contrôle juridictionnel total

Partenariat avec un fournisseur de services clouds souverains VMware de confiance

Pour assurer leur réussite, les entreprises doivent collaborer avec des partenaires en qui ils ont confiance et qui sont capables d'héberger des plateformes cloud souveraines authentiques et autonomes. Les fournisseurs cloud VMware reconnus dans le cadre de l'initiative Sovereign Cloud de VMware s'engagent à concevoir et à exploiter des solutions cloud basées sur des architectures Software-defined modernes, qui incarnent les principes clés et les meilleures pratiques décrits dans le cadre du cloud souverain de VMware.

- **Souveraineté des données et contrôle juridictionnel** – toutes les données résident et sont soumises au contrôle et à l'autorité exclusifs de l'État-nation où ces données ont été recueillies. Les opérations sont entièrement gérées dans la juridiction
- **Accès et intégrité des données** – l'infrastructure cloud est résiliente et disponible dans au moins deux centres de données de la juridiction avec des options de connectivité privée et sécurisée.
- **Sécurité et conformité des données** – les contrôles du système de gestion de la sécurité de l'information sont certifiés par rapport à une norme mondiale (ou régionale) reconnue par l'industrie et vérifiés régulièrement.
- **Indépendance et mobilité des données** – prise en charge des architectures d'applications modernes pour empêcher la dépendance vis-à-vis d'un fournisseur de cloud et permettre la portabilité et l'indépendance des applications

Pour plus d'informations sur VMware, consultez le site :

- "Présentation de VMware Sovereign Cloud"
- "Qu'est-ce que le cloud souverain de VMware ?"

- "Voici la nouvelle initiative VMware Sovereign Cloud"
- "Livre blanc technique sur le cloud souverain de VMware"

Netpp avec VMware Sovereign Cloud : utilisations

NetApp prend en charge les concepts de cloud souverain VMware grâce à l'intégration de plusieurs technologies NetApp.

Utilisez le(s) lien(s) suivant(s) pour en savoir plus sur les intégrations technologiques NetApp avec VMware Sovereign Cloud :

- "NetApp StorageGRID en tant qu'extension de magasin d'objets"

NetApp StorageGRID en tant qu'extension de magasin d'objets

NetApp a collaboré avec VMware pour intégrer NetApp StorageGRID dans VMware Cloud Director afin de prendre en charge le cloud souverain VMware. Ce plug-in à VMware Cloud Director permet aux fournisseurs de services d'utiliser StorageGRID en tant qu'offre de stockage objet (quel que soit le cas d'utilisation) et de gérer StorageGRID à l'aide de la même solution mutualisée VMware (VMware Cloud Director) que celle utilisée par les fournisseurs de services pour gérer d'autres parties de leur catalogue.

Les partenaires qui proposent des clouds souverains VMware peuvent choisir NetApp StorageGRID pour les aider à gérer et à gérer des environnements cloud avec des données non structurées. Sa compatibilité universelle dans sa prise en charge native des API standard telles qu'Amazon S3 contribue à assurer une interopérabilité fluide dans divers environnements cloud, ainsi que des innovations uniques telles que la gestion automatisée du cycle de vie permettent d'assurer une sauvegarde, un stockage et une conservation à long terme plus économiques des données non structurées des clients.

L'intégration souveraine de NetApp avec Cloud Director permet aux clients de bénéficier des avantages suivants :

- Vous avez la garantie que les données sensibles, y compris les métadonnées, restent sous contrôle souverain tout en empêchant l'accès d'autorités étrangères susceptibles de violer les lois sur la confidentialité des données.
- Sécurité et conformité accrues qui protègent les applications et les données contre les vecteurs d'attaque en constante évolution tout en assurant la conformité continue avec une infrastructure locale de confiance. infrastructures, structures intégrées et experts locaux.
- Une infrastructure pérenne capable de réagir rapidement à l'évolution des réglementations en matière de confidentialité des données, des menaces de sécurité et de la géopolitique.
- La capacité à exploiter tout le potentiel des données avec le partage et l'analyse sécurisés des données pour stimuler l'innovation sans violer les lois sur la confidentialité. L'intégrité des données est protégée pour une information précise.

Pour en savoir plus sur l'intégration de StorageGRID, consultez les documents suivants :

- "Annonce NetApp"

Le multicloud hybride NetApp avec les workloads de conteneurs Red Hat OpenShift

Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

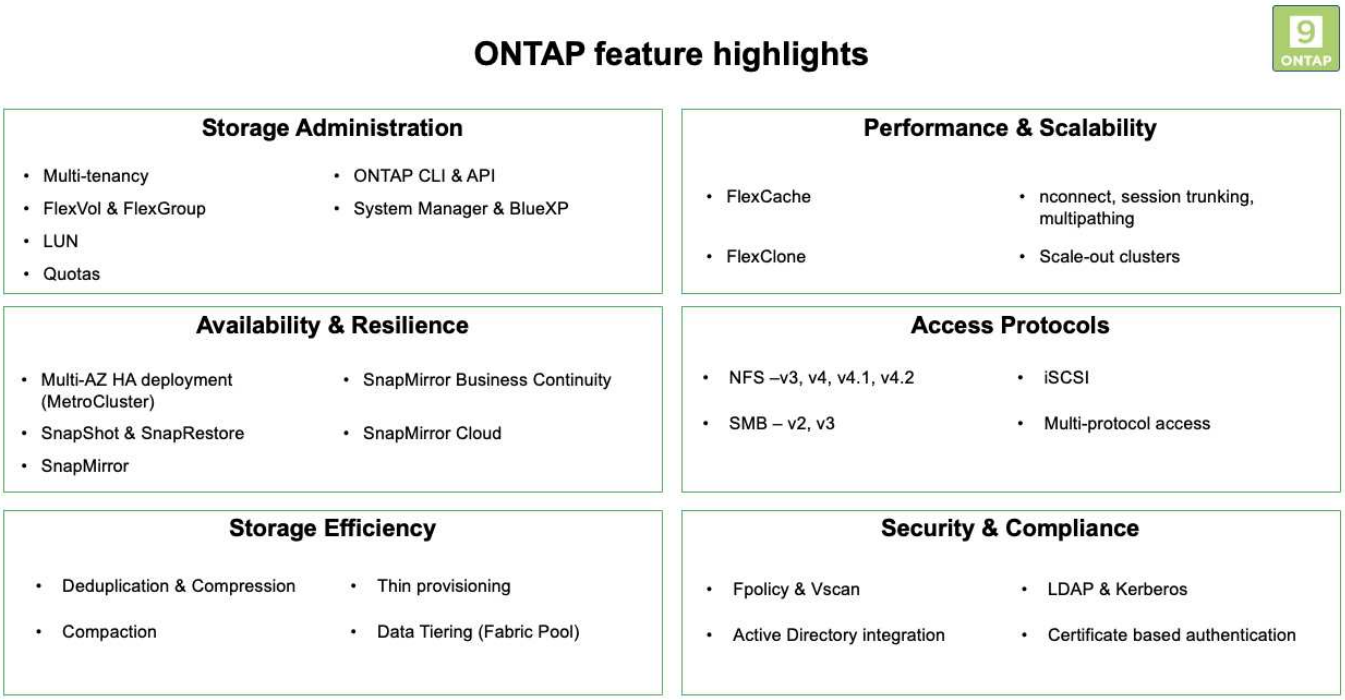
Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers

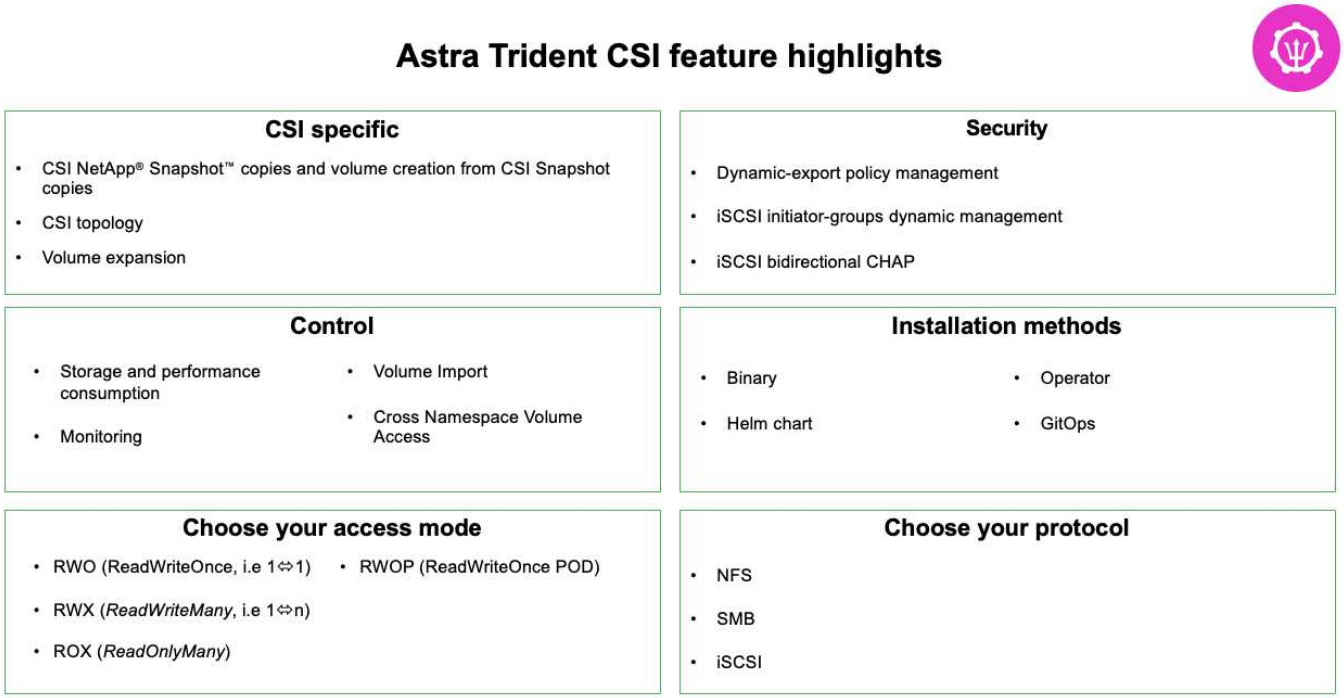


NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un

seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de

conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Propositions de valeur des solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

La plupart des clients ne se contentent pas de créer des environnements Kubernetes sans infrastructure existante. Il s'agit peut-être d'un service INFORMATIQUE traditionnel qui exécute la plupart de ses applications d'entreprise sur des machines virtuelles (dans de grands environnements VMware, par exemple). Ils commencent ensuite à créer de petits environnements basés sur des conteneurs pour répondre aux besoins de leurs équipes de développement d'applications modernes. Ces initiatives commencent généralement à petite échelle et commencent à devenir plus omniprésentes lorsque les équipes apprennent ces nouvelles technologies et compétences, et commencent à reconnaître les nombreux avantages de leur adoption. La bonne nouvelle pour les clients est que NetApp répond aux besoins des deux environnements. Cet ensemble de solutions pour le multicloud hybride avec Red Hat OpenShift permettra aux clients NetApp d'adopter des technologies et des services cloud modernes sans avoir à remanier l'ensemble de leur infrastructure et de leur organisation. Que les applications et les données des clients soient hébergées sur site, dans le cloud, sur des machines virtuelles ou sur des conteneurs, NetApp offre des fonctionnalités cohérentes de gestion, de protection, de sécurité et de portabilité des données. Avec ces nouvelles solutions, la valeur ajoutée qu'offre NetApp dans les environnements de data Center sur site pendant des décennies sera disponible à l'échelle de l'entreprise à tous les niveaux, sans nécessiter d'investissements importants pour changer d'outil, acquérir de nouvelles compétences ou constituer de nouvelles équipes. NetApp est bien placé pour aider les clients à relever ces défis métier, quelle que soit l'étape de leur transition vers le cloud.

NetApp Hybrid Multi-Cloud avec Red Hat OpenShift :

- Fournit aux clients des conceptions et des pratiques validées qui démontrent la meilleure façon de gérer, protéger, sécuriser et migrer leurs données et applications lors de l'utilisation de Red Hat OpenShift avec les solutions de stockage NetApp.
- Présenter les meilleures pratiques pour les clients exécutant Red Hat OpenShift avec le stockage NetApp dans des environnements VMware, une infrastructure bare Metal ou une combinaison des deux.
- Présentez les stratégies et les options des environnements sur site et cloud, ainsi que des environnements hybrides dans lesquels les deux sont utilisés.

Solutions prises en charge de multicloud hybride NetApp pour les workloads de conteneurs Red Hat OpenShift

La solution teste et valide la migration et la protection centralisée des données avec OpenShift Container Platform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP et NetApp Astra Control Center (ACC).

Pour cette solution, les scénarios suivants sont testés et validés par NetApp. La solution est divisée en plusieurs scénarios selon les caractéristiques suivantes :

- sur site
- le cloud
  - Clusters OpenShift autogérés et stockage NetApp autogéré
  - Clusters OpenShift gérés par le fournisseur et stockage NetApp géré par le fournisseur

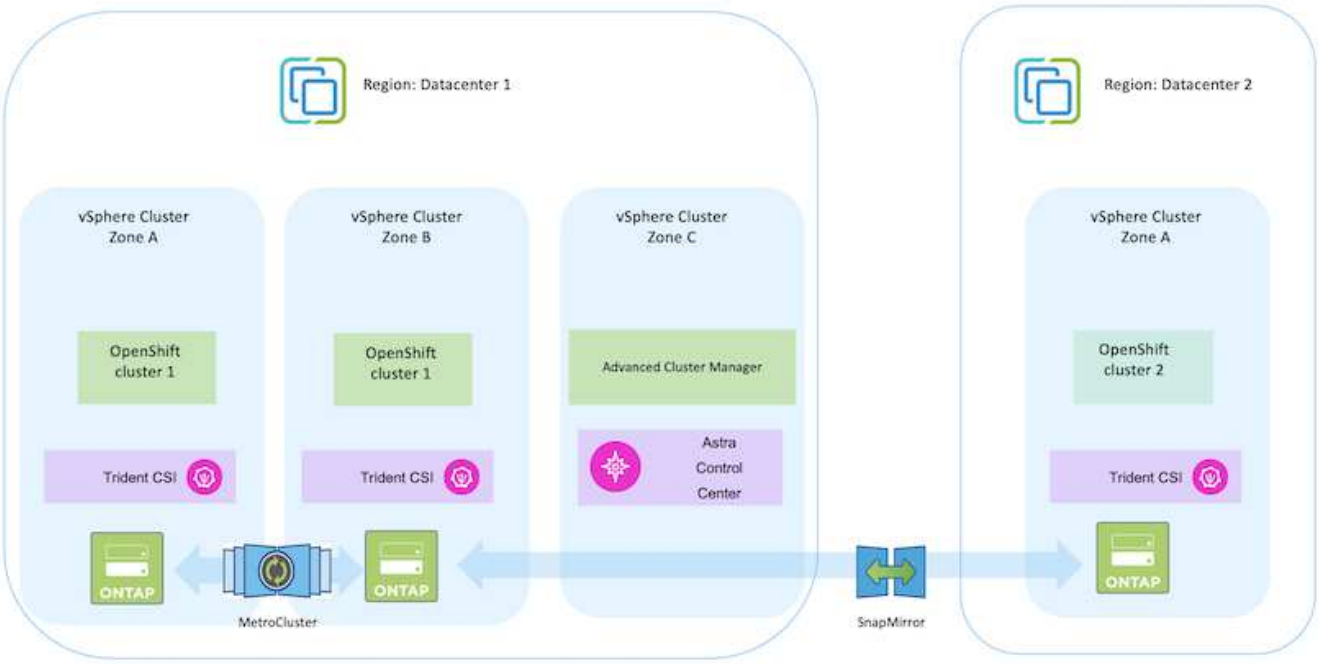
Nous élaborerons à l'avenir des solutions et des cas d'utilisation supplémentaires.

Scénario 1 : protection et migration des données au sein d'un environnement sur site avec ACC

Sur site : clusters OpenShift autogérés et stockage NetApp autogéré

- Avec ACC, créez des copies Snapshot, des sauvegardes et des restaurations pour protéger les données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.

Scénario 1

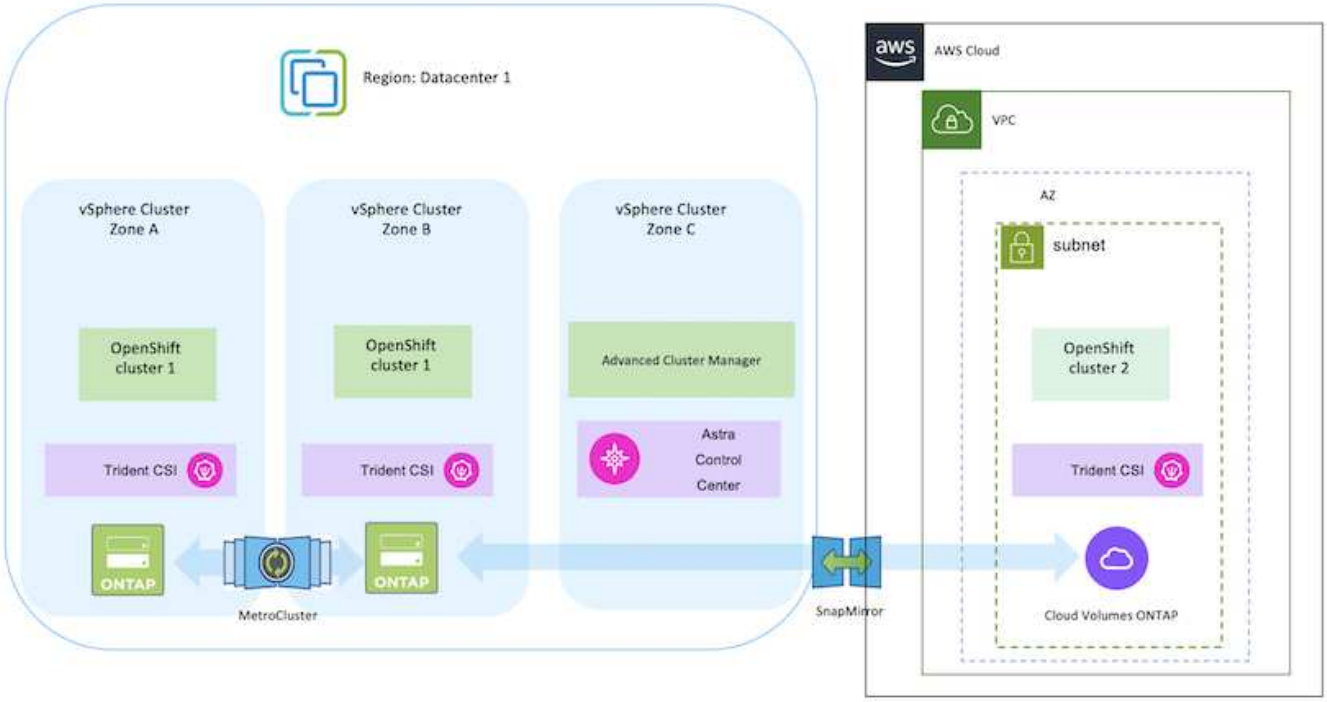


Scénario 2 : protection des données et migration d'un environnement sur site vers un environnement AWS à l'aide d'ACC

Sur site : cluster OpenShift autogéré et stockage autogéré AWS Cloud : cluster OpenShift autogéré et stockage autogéré

- Avec ACC, effectuez des sauvegardes et des restaurations pour protéger vos données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.

Scénario 2

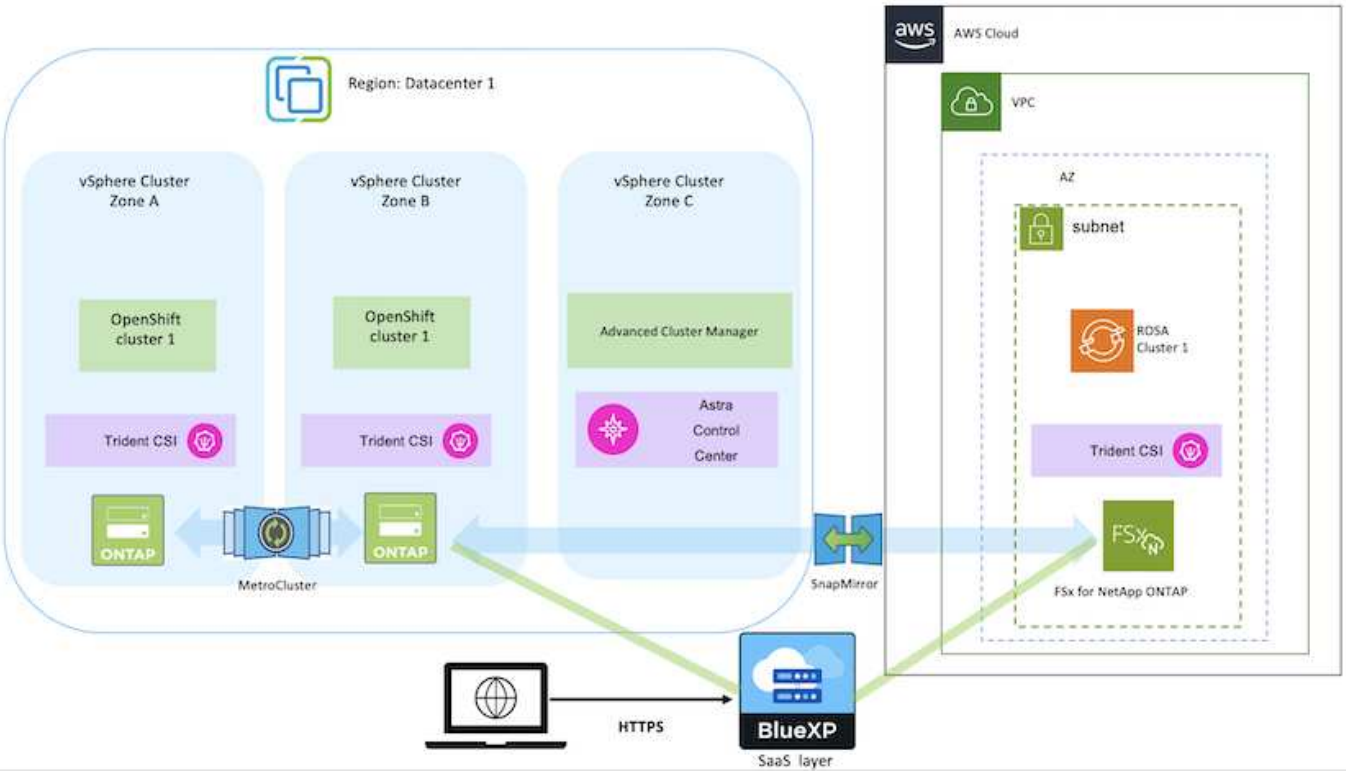


Scénario 3 : protection des données et migration d'un environnement sur site vers un environnement AWS

Sur site : cluster OpenShift autogéré et stockage autogéré AWS Cloud : cluster OpenShift géré par le fournisseur (ROSA) et stockage géré par le fournisseur (FSxN)

- Avec BlueXP, répliquez des volumes persistants (FSxN).
- À l'aide d'OpenShift GitOps, recréez les métadonnées de l'application.

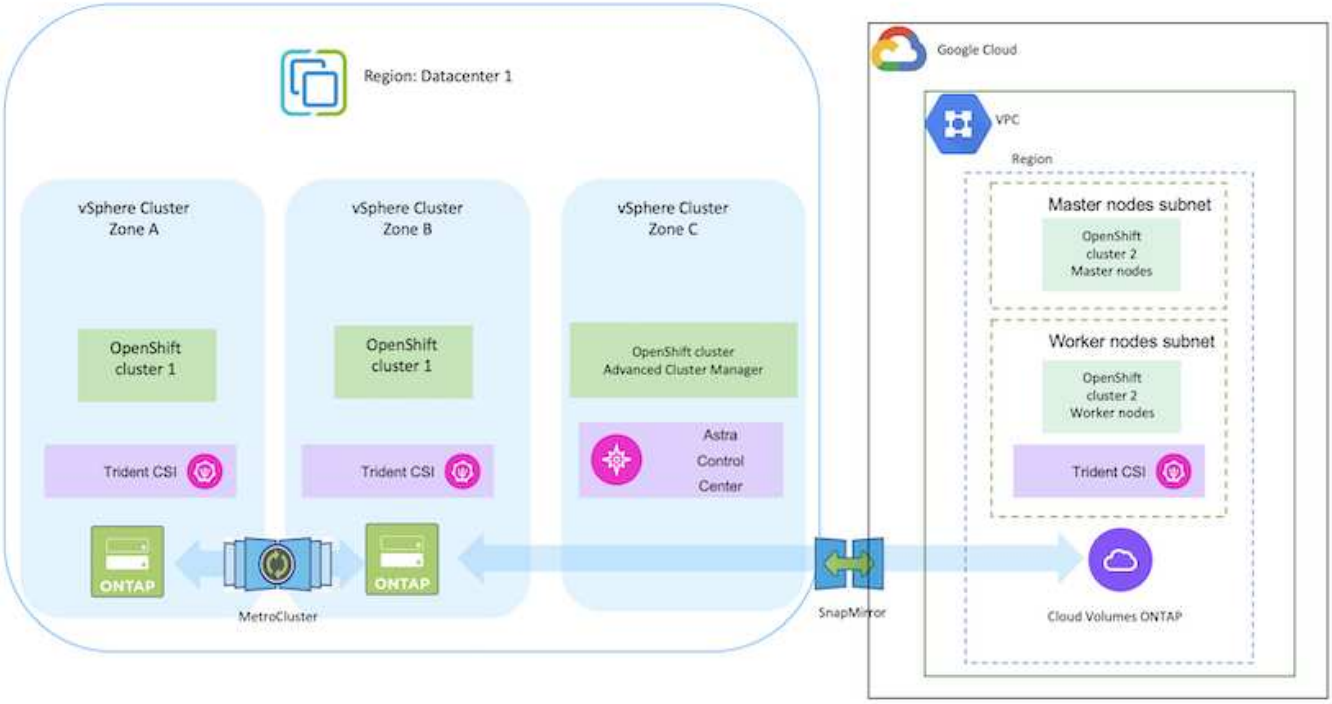
Scénario 3



Scénario 4 : protection des données et migration d'un environnement sur site vers un environnement GCP à l'aide d'ACC

Sur site : cluster OpenShift autogéré et stockage autogéré
Google Cloud : cluster OpenShift autogéré et stockage autogéré

- Avec ACC, effectuez des sauvegardes et des restaurations pour protéger vos données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.

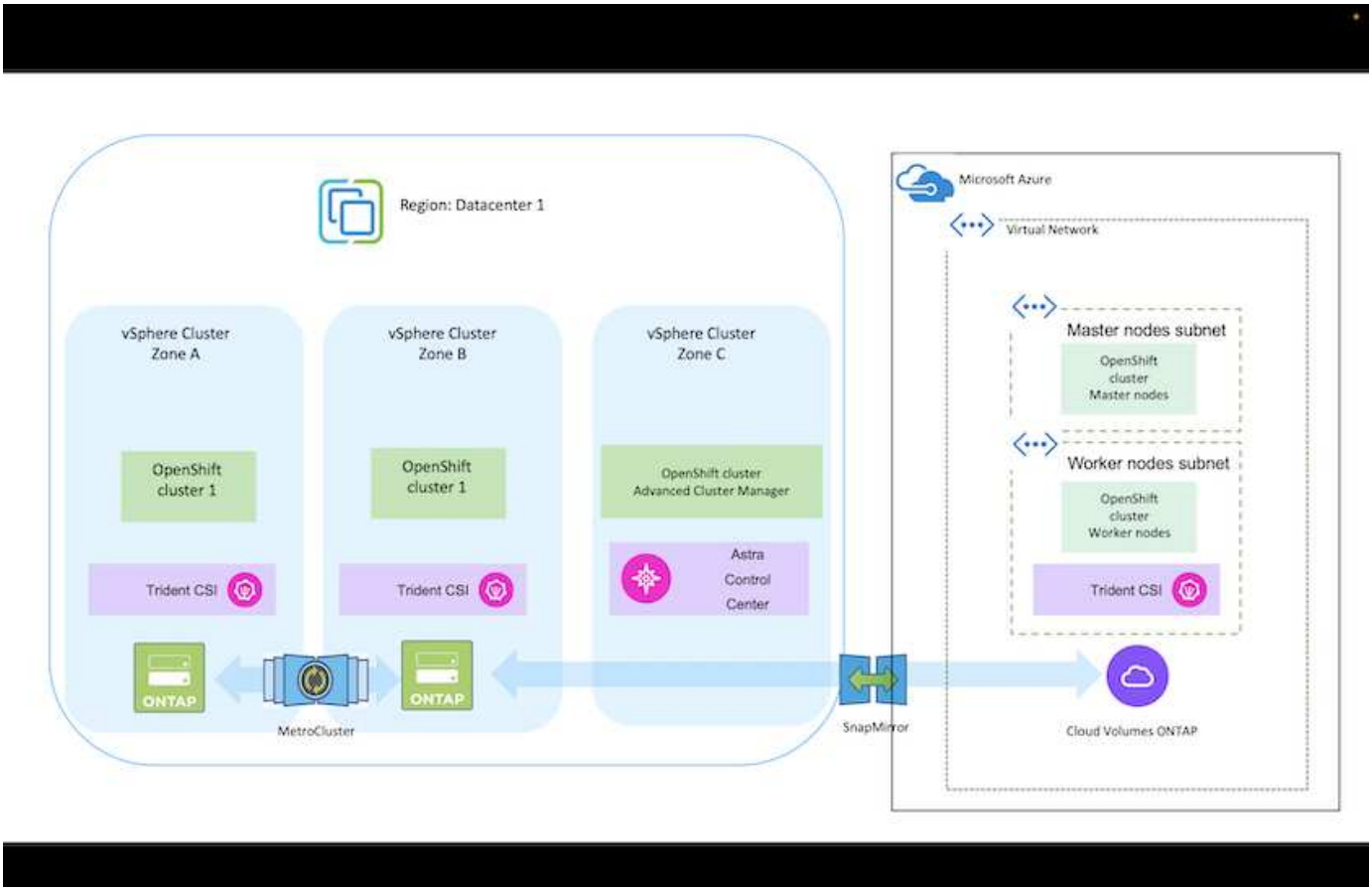


Pour connaître les points à prendre en compte lors de l'utilisation de ONTAP dans une configuration MetroCluster, reportez-vous à la section "ici".

Scénario 5 : protection des données et migration d'un environnement sur site vers un environnement Azure à l'aide d'ACC

Sur site : cluster OpenShift autogéré et stockage autogéré
Azure Cloud : cluster OpenShift autogéré et stockage autogéré

- Avec ACC, effectuez des sauvegardes et des restaurations pour protéger vos données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.



Pour connaître les points à prendre en compte lors de l'utilisation de ONTAP dans une configuration MetroCluster, reportez-vous à la section "ici".

Versions des différents composants utilisés dans la validation de la solution

La solution teste et valide la migration et la protection centralisée des données avec OpenShift Container Platform, OpenShift Advanced Cluster Manager, NetApp ONTAP et NetApp Astra Control Center.

Les scénarios 1, 2 et 3 de la solution ont été validés à l'aide des versions indiquées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Cluster Hub	OpenShift 4.11.34
Clusters source et de destination	OpenShift 4.12.9 sur site et dans AWS
NetApp Astra Trident	Serveur et client Trident 23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1

AWS FSX pour NetApp ONTAP	AZ unique

Le scénario 4 de la solution a été validé à l'aide des versions indiquées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Cluster Hub	OpenShift 4.13.13
Clusters source et de destination	OpenShift 4.13.12 Sur site et dans Google Cloud
NetApp Astra Trident	Serveur et client Trident 23.07.0
NetApp Astra Control Center	ACC 23.07.0-25
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Disponibilité unique, nœud unique, 9.14.0

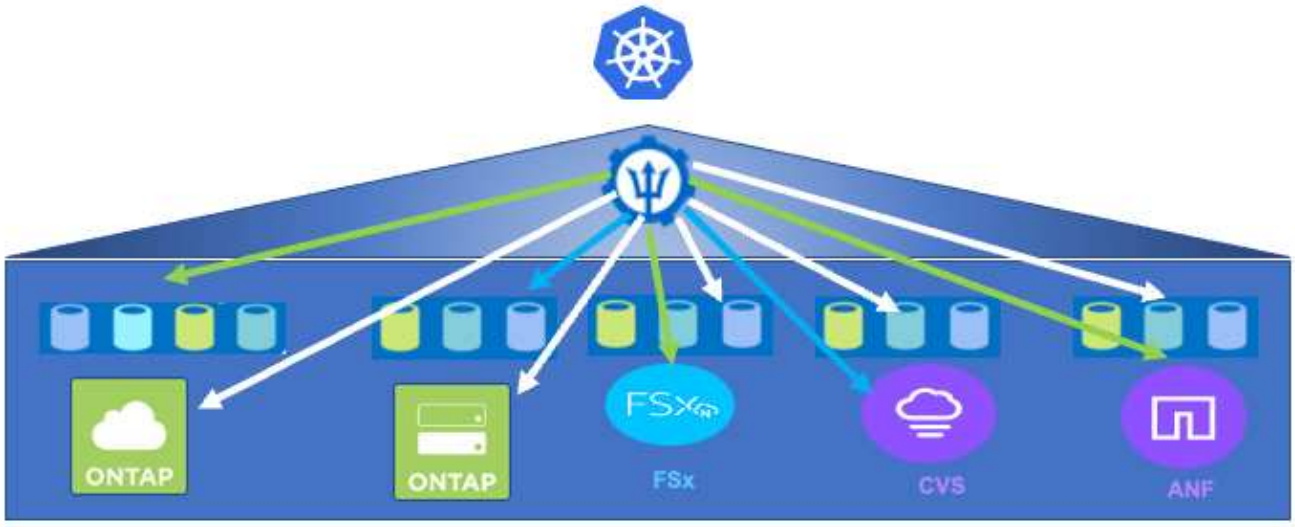
Le scénario 5 de la solution a été validé à l'aide des versions indiquées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Clusters source et de destination	OpenShift 4.13.25 Sur site et dans Azure
NetApp Astra Trident	Serveur et client Trident et Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23.10
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Disponibilité unique, nœud unique, 9.14.0

Intégrations NetApp Storage prises en charge avec les conteneurs Red Hat Open Shift

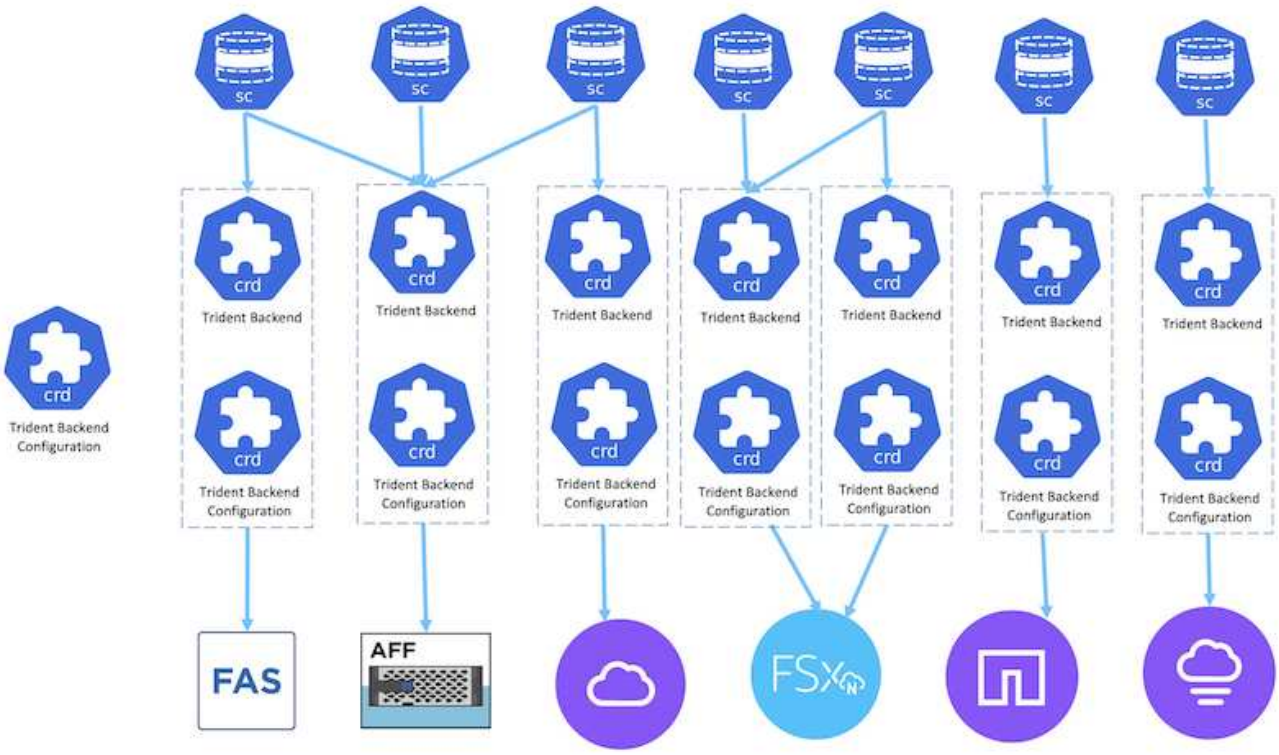
Que les conteneurs Red Hat Open Shift s'exécutent sur VMware ou dans les hyperscalers, NetApp Astra Trident peut être utilisé comme mécanisme de provisionnement CSI pour les différents types de stockage NetApp back-end pris en charge.

Le schéma suivant décrit les différents systèmes de stockage NetApp back-end pouvant être intégrés avec des clusters OpenShift à l'aide de NetApp Astra Trident.

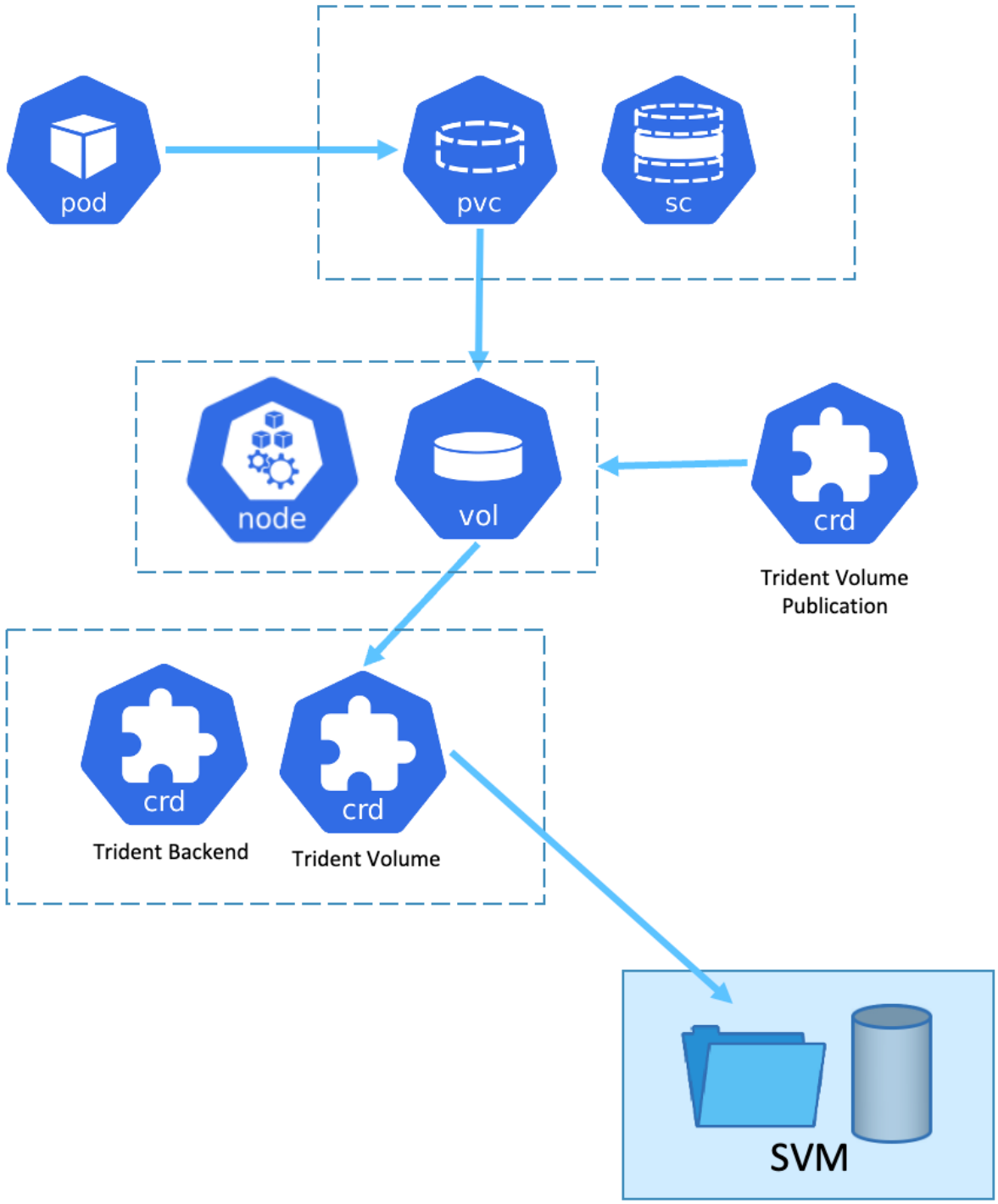


La SVM (Storage Virtual machine) de ONTAP assure une colocation sécurisée. Un cluster OpenShift peut se connecter à un seul SVM ou à plusieurs SVM, voire à plusieurs clusters ONTAP. Storage Class filtre le stockage back-end en fonction de paramètres ou de libellés. Les administrateurs du stockage définissent les paramètres de connexion au système de stockage à l'aide de la configuration back-end trident. Une fois la connexion établie, il crée le back-end trident et renseigne les informations que la classe de stockage peut filtrer.

La relation entre le storageclass et le backend est présentée ci-dessous.



Le propriétaire de l'application demande un volume persistant en utilisant la classe de stockage. La classe de stockage filtre le stockage back-end. La relation entre le pod et le système de stockage back-end est présentée ci-dessous.



Options Container Storage interface (CSI)

Sur les environnements vSphere, les clients peuvent choisir le pilote VMware CSI et/ou Astra Trident CSI pour s'intégrer à ONTAP. Avec VMware CSI, les volumes persistants sont utilisés en tant que disques SCSI locaux, tandis qu'avec Trident, ils sont utilisés avec le réseau. Étant donné que VMware CSI ne prend pas en charge les modes d'accès RWX avec ONTAP, les applications doivent utiliser Trident CSI si le mode RWX est requis. Pour les déploiements basés sur FC, VMware CSI est privilégié et SnapMirror Business Continuity (SMBC) offre une haute disponibilité au niveau de la zone.

Prise en charge de VMware CSI

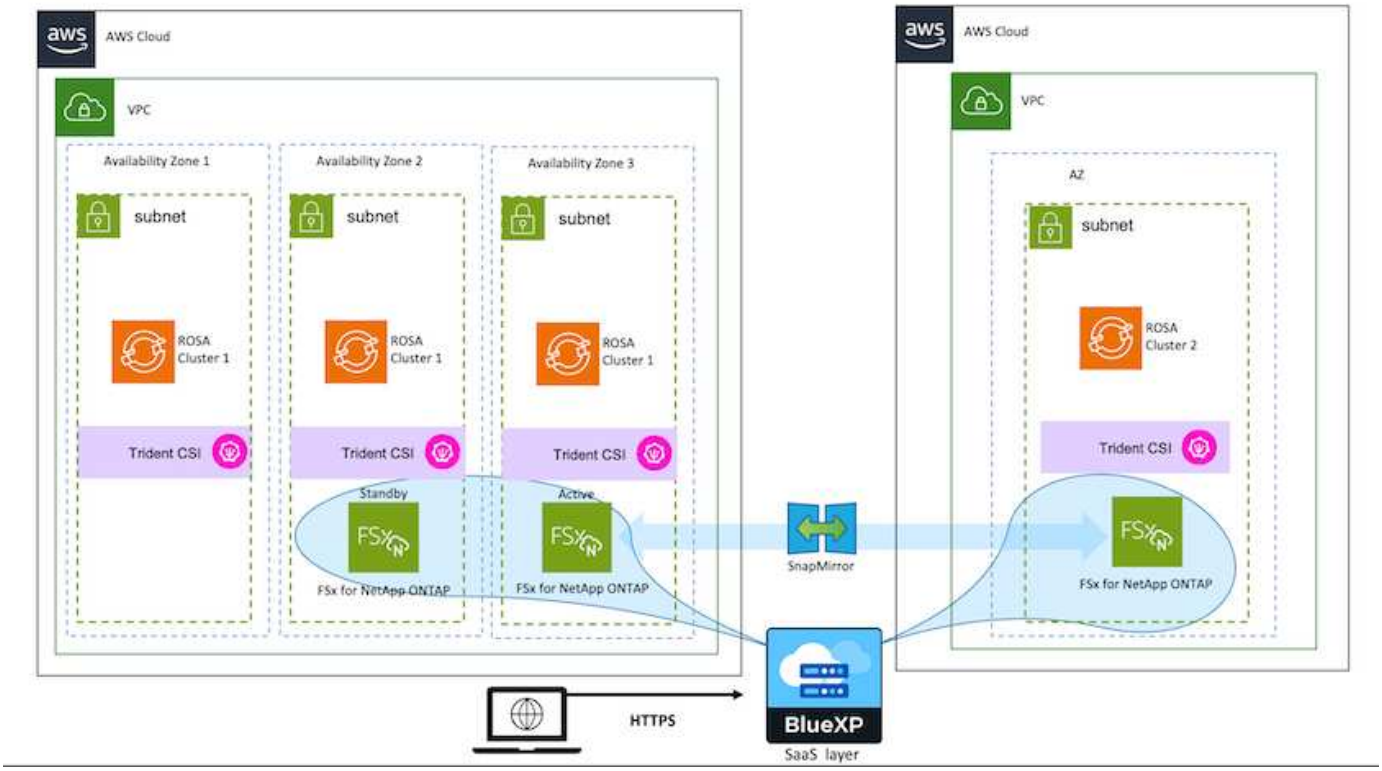
- Datastores basés sur des blocs principaux (FC, FCoE, iSCSI, NVMeoF)
- Datastores basés sur des fichiers principaux (NFS v3, v4)
- Datastores vVol (bloc et fichier)

Trident dispose des pilotes suivants pour prendre en charge ONTAP

- san ontap (volume dédié)
- ontap-san-economy (volume partagé)
- ontap-nas (volume dédié)
- ontap-nas-economy (volume partagé)
- ontap-nas-flexgroup (volume dédié à grande échelle)

Pour VMware CSI et Astra Trident CSI, ONTAP prend en charge nconnect, l'agrégation de sessions, kerberos, etc. Pour NFS et les chemins d'accès multiples, l'authentification chap, etc. Pour les protocoles en mode bloc.

Dans AWS, FSX pour NetApp ONTAP (FSxN) peut être déployé dans une zone de disponibilité unique (AZ) ou dans plusieurs zones de disponibilité. Pour les workloads de production qui nécessitent une haute disponibilité, plusieurs zones de disponibilité offrent une tolérance aux pannes de niveau zonal et un meilleur cache de lecture NVMe qu'une zone de disponibilité unique. Pour plus d'informations, consultez "Conseils sur les performances d'AWS".
Pour réduire les coûts sur le site de reprise après incident, un seul serveur AZ FSX ONTAP peut être utilisé.



Pour connaître le nombre de SVM pris en charge par FSX ONTAP, reportez-vous à la section "Gestion de la machine virtuelle de stockage FSX ONTAP"

Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

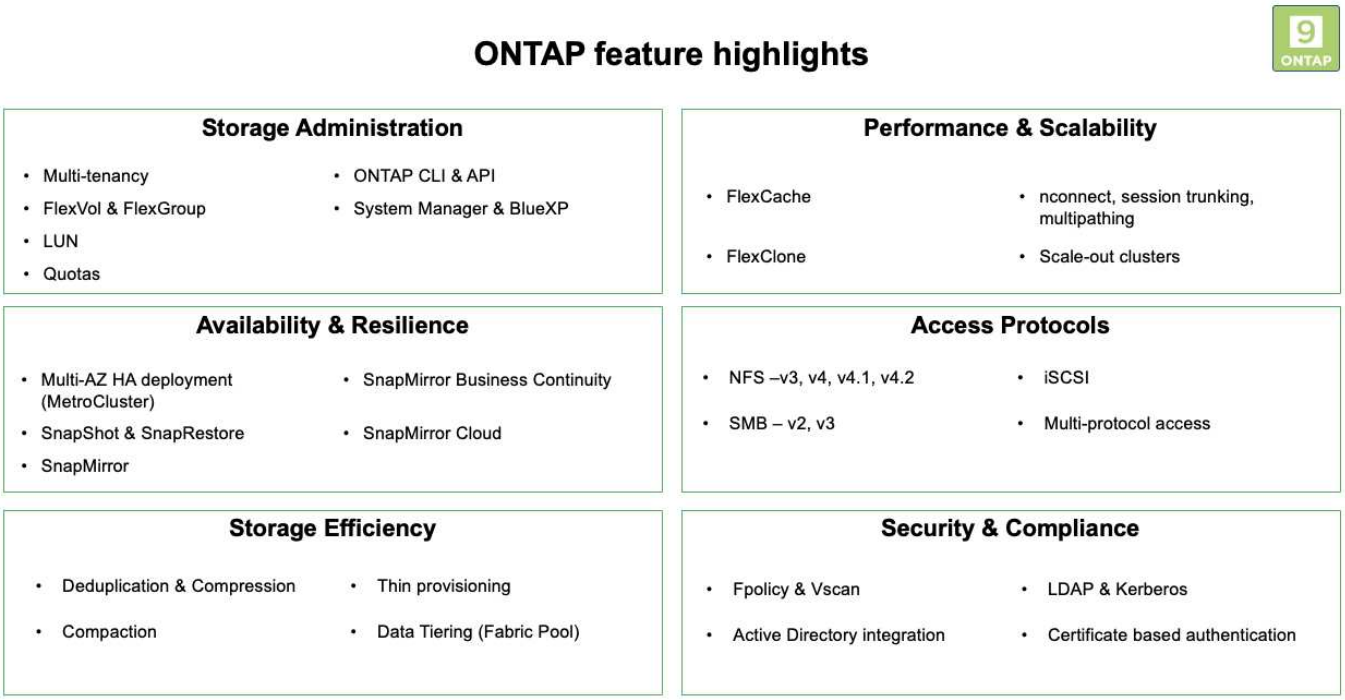
Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers

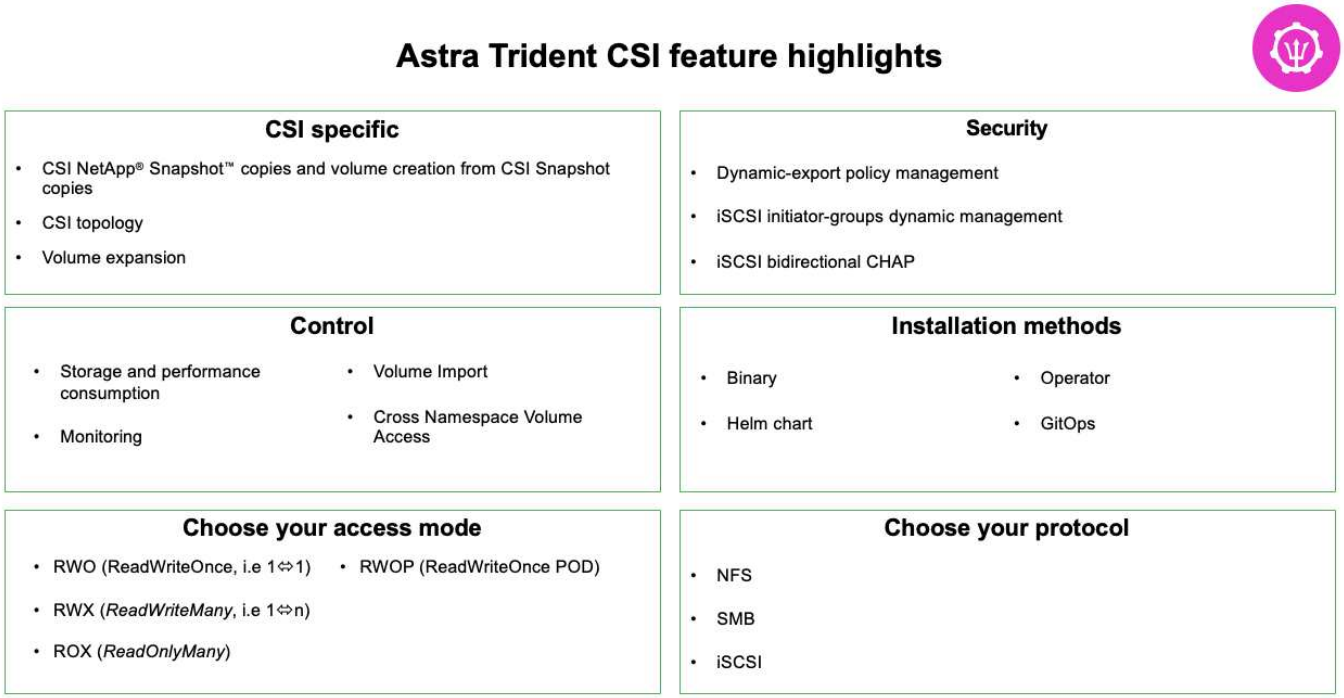


NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un

seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de

conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Solution NetApp avec les workloads de plateforme de conteneurs Red Hat OpenShift sur VMware

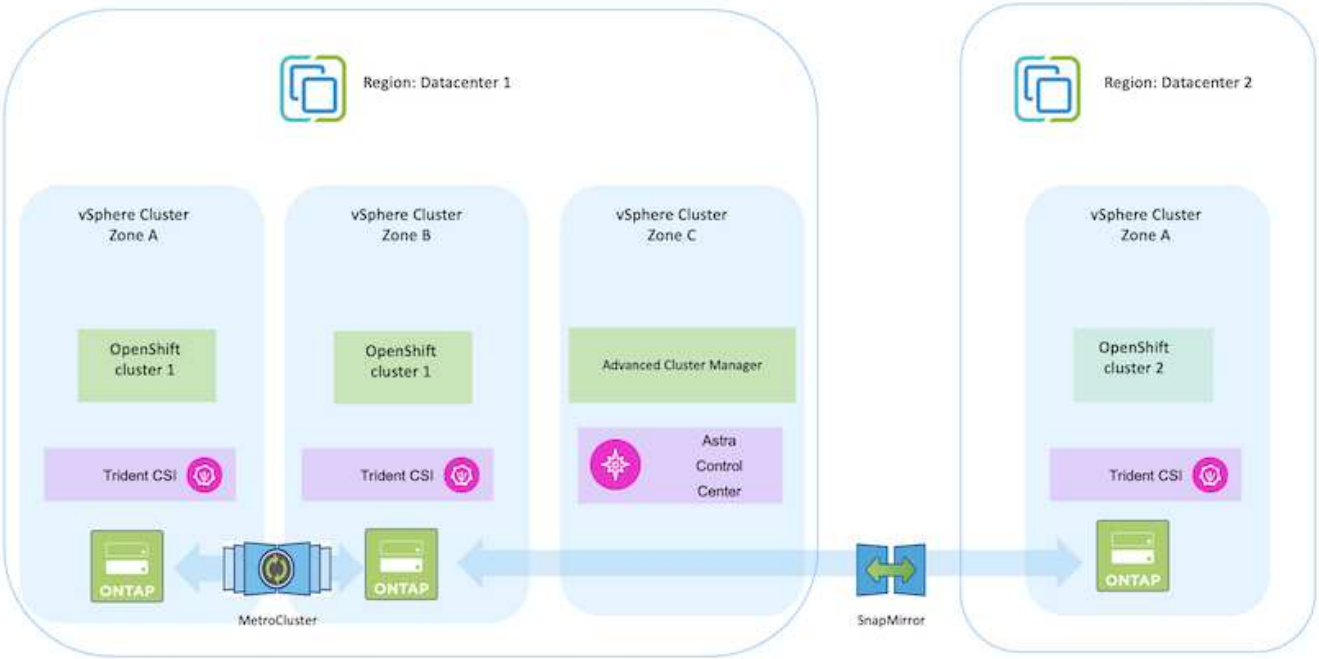
Si les clients ont besoin d'exécuter leurs applications conteneurisées modernes dans leur infrastructure dans leurs data centers privés, ils peuvent le faire. Ils doivent planifier et déployer Red Hat OpenShift Container Platform (OCP) pour que l'environnement de production soit prêt pour le déploiement de leurs workloads de conteneurs. Leurs clusters OCP peuvent être déployés sur VMware ou sur bare Metal.

Le stockage ONTAP de NetApp assure la protection, la fiabilité et la flexibilité des données pour les déploiements de conteneurs. ASTRA Trident sert de mécanisme de provisionnement de stockage dynamique pour consommer le stockage ONTAP persistant pour les applications avec état des clients. ASTRA Control Center peut être utilisé pour orchestrer les nombreuses exigences de gestion des données des applications avec état, telles que la protection des données, la migration et la continuité de l'activité.

Avec VMware vSphere, les outils NetApp ONTAP fournissent un plug-in vCenter qui peut être utilisé pour provisionner les datastores. Appliquez les balises et utilisez-les avec OpenShift pour stocker la configuration et les données des nœuds. Le stockage basé sur NVMe offre une latence faible et des performances élevées.

Cette solution fournit des informations détaillées sur la protection des données et la migration des workloads de conteneurs à l'aide d'Astra Control Center. Pour cette solution, les workloads de conteneurs sont déployés sur les clusters Red Hat OpenShift sur vSphere au sein de l'environnement sur site. REMARQUE : nous fournirons prochainement une solution pour les workloads de conteneurs sur des clusters OpenShift sur du serveur bare Metal.

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift à l'aide d'Astra Control Center

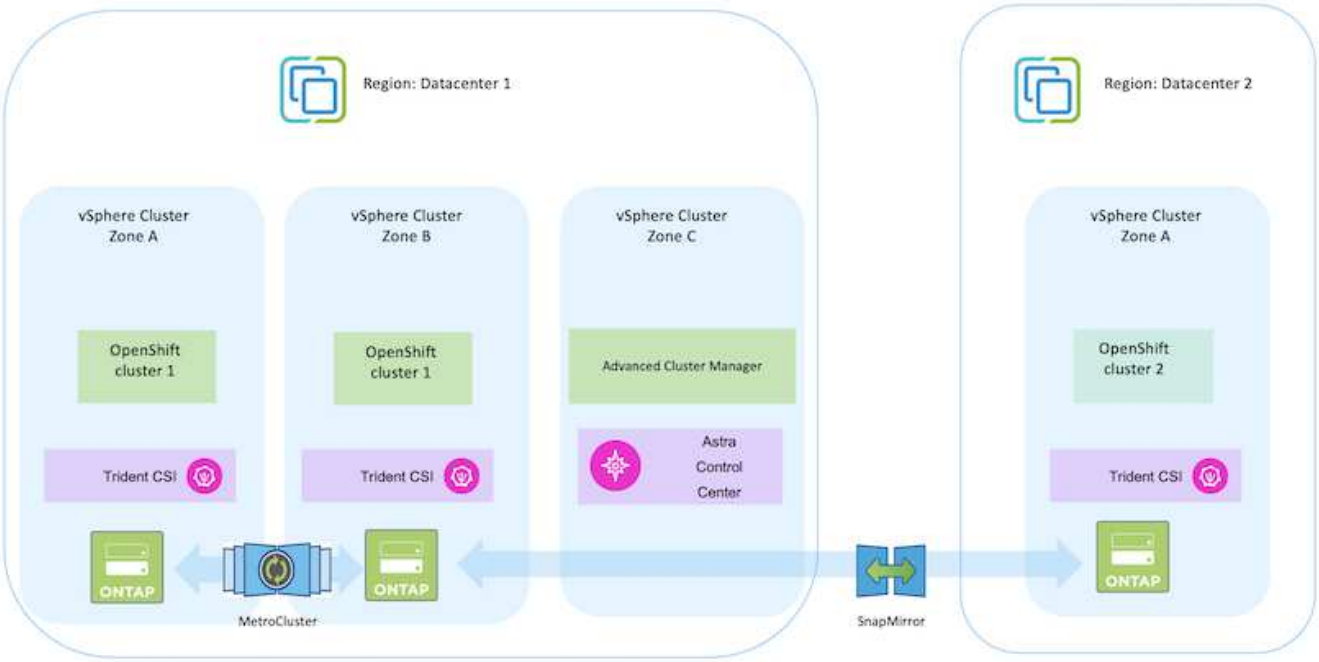


Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur VMware

Cette section décrit un workflow général expliquant comment configurer et gérer des clusters OpenShift et gérer des applications avec état sur ces clusters. Il présente l'utilisation des baies de stockage NetApp ONTAP à l'aide d'Astra Trident pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

Il existe plusieurs façons de déployer les clusters de la plateforme de conteneurs Red Hat OpenShift. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Voici un diagramme illustrant les clusters déployés sur VMware dans un data Center.



Le processus de configuration peut être divisé en plusieurs étapes :

Déployez et configurez une machine virtuelle CentOS

- Elle est déployée dans l'environnement VMware vSphere.
- Cette VM sert à déployer certains composants, tels que NetApp Astra Trident et NetApp Astra Control Center, pour la solution.
- Un utilisateur root est configuré sur cette VM lors de l'installation.

Déploiement et configuration d'un cluster OpenShift Container Platform sur VMware vSphere (Hub Cluster)

Reportez-vous aux instructions du "Déploiement assisté" Méthode de déploiement d'un cluster OCP.

Souvenez-vous des éléments suivants : - Créez une clé publique et privée ssh à fournir au programme d'installation. Ces clés seront utilisées pour se connecter aux nœuds maître et worker si nécessaire. - Téléchargez le programme d'installation à partir de l'installateur assisté. Ce programme permet de démarrer les machines virtuelles que vous créez dans l'environnement VMware vSphere pour les nœuds maître et worker. - Les machines virtuelles doivent avoir la configuration minimale requise pour le processeur, la mémoire et le disque dur. (Reportez-vous aux commandes vm create sur "c'est ça" Pour les nœuds maître et worker qui fournissent ces informations) - l'UUID de disque doit être activé sur toutes les machines virtuelles. - Créer un minimum de 3 nœuds pour le maître et 3 nœuds pour le travailleur. - Une fois qu'ils sont découverts par le programme d'installation, activez le bouton bascule d'intégration de VMware vSphere.

Installez Advanced Cluster Management sur le cluster Hub

Ceci est installé à l'aide de l'opérateur de gestion avancée des clusters sur le cluster Hub. Reportez-vous aux instructions "ici".

Installez un registre Red Hat Quay interne sur le cluster Hub.

- Un registre interne est requis pour transmettre l'image Astra. Un registre interne Quay est installé à l'aide de l'opérateur dans le cluster Hub.
- Reportez-vous aux instructions "ici"

Installer deux clusters OCP supplémentaires (source et destination)

- Les clusters supplémentaires peuvent être déployés à l'aide de l'ACM sur le cluster Hub.
- Reportez-vous aux instructions "ici".

Configuration du stockage NetApp ONTAP

- Installez un cluster ONTAP connecté aux VM OCP dans un environnement VMware.
- Créer un SVM.
- Configurer la lif de données NAS pour accéder au stockage en SVM

Installez NetApp Trident sur les clusters OCP

- Installez NetApp Trident sur les trois clusters : concentrateur, source et destination
- Reportez-vous aux instructions "ici".
- Créez un système back-end de stockage pour ontap-nas .
- Créez une classe de stockage pour ontap-nas.
- Reportez-vous aux instructions "ici".

Installez NetApp Astra Control Center

- NetApp Astra Control Center est installé à l'aide d'Astra Operator sur le cluster Hub.
- Reportez-vous aux instructions "ici".

Points à retenir : * Téléchargez l'image NetApp Astra Control Center sur le site du support. * Poussez l'image dans un registre interne. * Reportez-vous aux instructions ici.

Déployer une application sur un cluster source

Déployez une application à l'aide d'OpenShift GitOps. (par ex. Postgres, fantôme)

Ajoutez les clusters source et cible dans Astra Control Center.

Une fois que vous avez ajouté un cluster au système de gestion Astra Control, vous pouvez installer des applications sur le cluster (à l'extérieur d'Astra Control), puis accéder à la page applications dans Astra Control pour définir les applications et leurs ressources. Reportez-vous à la section "Commencez à gérer les applications d'Astra Control Center".

L'étape suivante consiste à utiliser Astra Control Center pour la protection des données et la migration des données du cluster source vers le cluster destination.

Protection des données avec Astra

Cette page présente les options de protection des données pour les applications basées sur des conteneurs Red Hat OpenShift qui s'exécutent sur VMware vSphere à l'aide d'Astra Control Center (ACC).

Au fur et à mesure que les utilisateurs s'engagent dans la modernisation de leurs applications avec Red Hat OpenShift, une stratégie de protection des données doit être mise en place pour les protéger contre toute suppression accidentelle ou toute autre erreur humaine. Souvent, une stratégie de protection est également nécessaire à des fins réglementaires ou de conformité afin de protéger leurs données contre les données d'un grand nombre.

Les exigences en matière de protection des données varient entre le retour à une copie instantanée et le basculement automatique vers un autre domaine de panne sans intervention humaine. De nombreux clients choisissent ONTAP comme plateforme de stockage préférée pour leurs applications Kubernetes en raison de ses nombreuses fonctionnalités, telles que la colocation, le multiprotocole, les performances et les capacités élevées, la réplication et la mise en cache pour les sites multisites, la sécurité et la flexibilité.

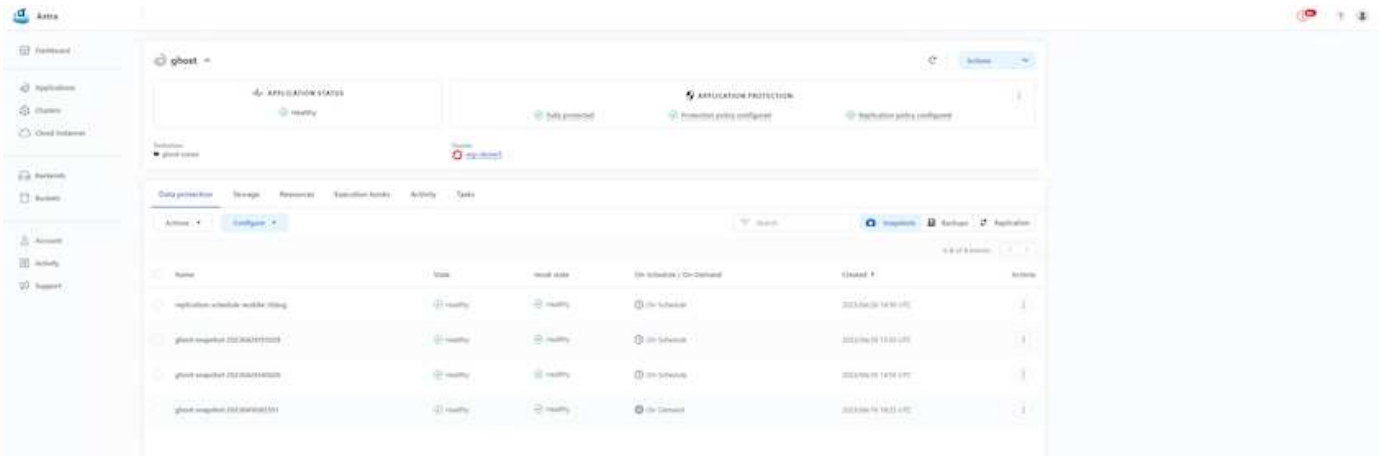
La protection des données dans ONTAP peut être obtenue en utilisant ad hoc ou contrôlé par des règles - **instantané** - **sauvegarde et restauration**

Les copies Snapshot et les sauvegardes protègent les types de données suivants : - **les métadonnées de l'application qui représentent l'état de l'application** - **tout volume de données persistantes associé à l'application** - **tout artefact de ressource appartenant à l'application**

Instantané avec ACC

Une copie instantanée des données peut être capturée à l'aide de Snapshot avec ACC. La règle de protection définit le nombre de copies Snapshot à conserver. L'option horaire minimum disponible est horaire. Les copies Snapshot manuelles à la demande peuvent être effectuées à tout moment et à intervalles plus courts que les copies Snapshot planifiées. Les copies Snapshot sont stockées sur le même volume provisionné que l'application.

Configuration de l'instantané avec ACC

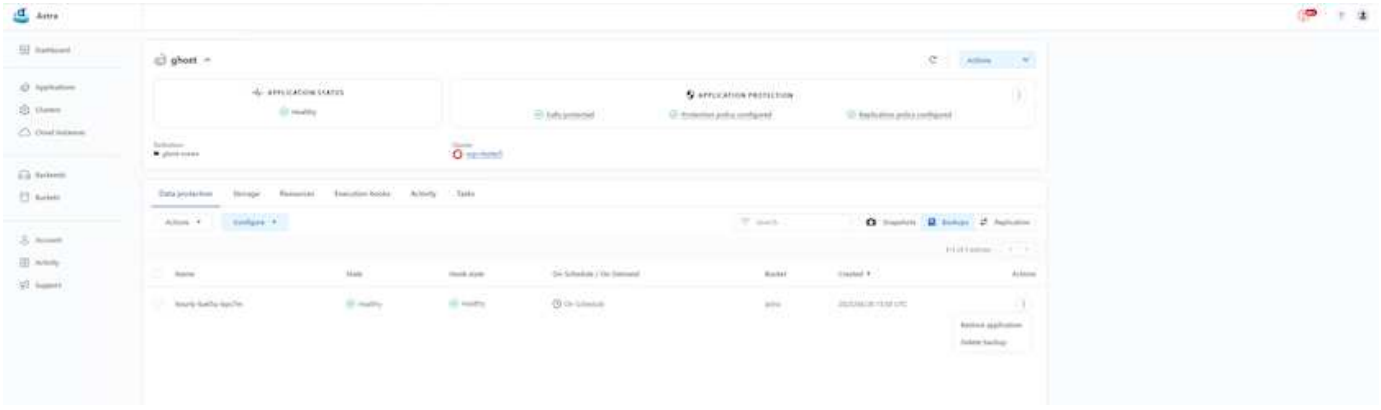


Sauvegarde et restauration avec ACC

Une sauvegarde est basée sur une copie Snapshot. ACC peut effectuer des copies Snapshot à l'aide de CSI et effectuer des sauvegardes à l'aide de la copie Snapshot instantanée. La sauvegarde est stockée dans un magasin d'objets externe (tout système s3 compatible avec ONTAP S3 à un emplacement différent). La règle de protection peut être configurée pour les sauvegardes planifiées et le nombre de versions de sauvegarde à conserver. L'objectif de point de récupération minimal est d'une heure.

Restauration d'une application à partir d'une sauvegarde à l'aide d'ACC

ACC restaure l'application à partir du compartiment S3 où sont stockées les sauvegardes.



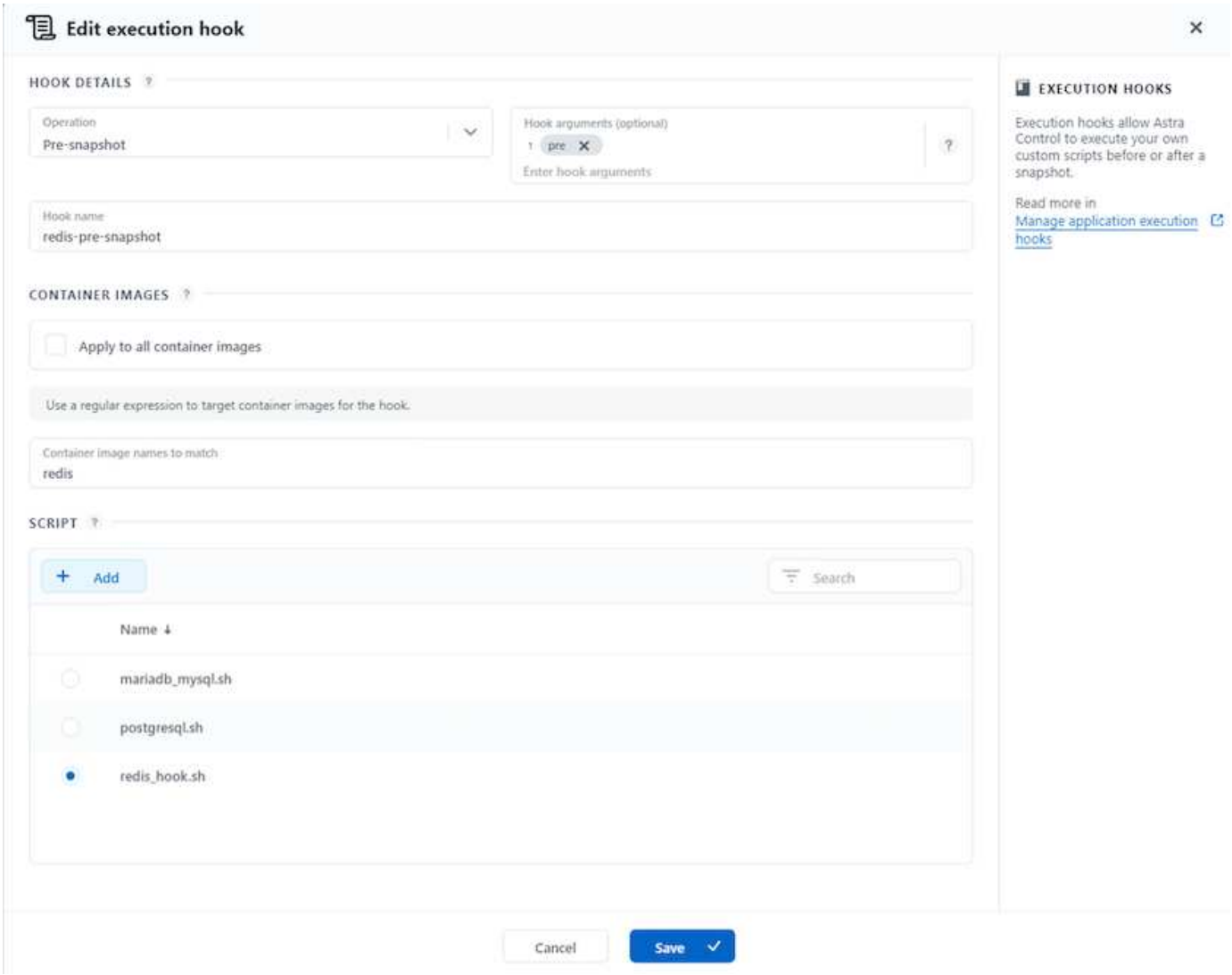
Crochets d'exécution spécifiques à l'application

En outre, vous pouvez configurer des crochets d'exécution pour qu'ils s'exécutent en conjonction avec une opération de protection des données d'une application gérée. Même si les fonctionnalités de protection des données au niveau des baies de stockage sont disponibles, il est souvent nécessaire de suivre des étapes supplémentaires pour rendre les sauvegardes et les restaurations cohérentes avec les applications. Les étapes supplémentaires spécifiques à l'application peuvent être : - avant ou après la création d'une copie Snapshot. - avant ou après la création d'une sauvegarde. - Après restauration à partir d'une copie Snapshot ou d'une sauvegarde.

ASTRA Control peut exécuter ces étapes spécifiques à l'application codées comme des scripts personnalisés appelés crochets d'exécution.

"Projet GitHub NetApp Verda" fournit des crochets d'exécution pour les applications cloud les plus courantes afin de simplifier, renforcer et orchestrer la protection des applications. N'hésitez pas à contribuer à ce projet si vous avez suffisamment d'informations pour une application qui ne se trouve pas dans le référentiel.

Exemple de crochet d'exécution pour pré-instantané d'une application redis.



Réplication avec ACC

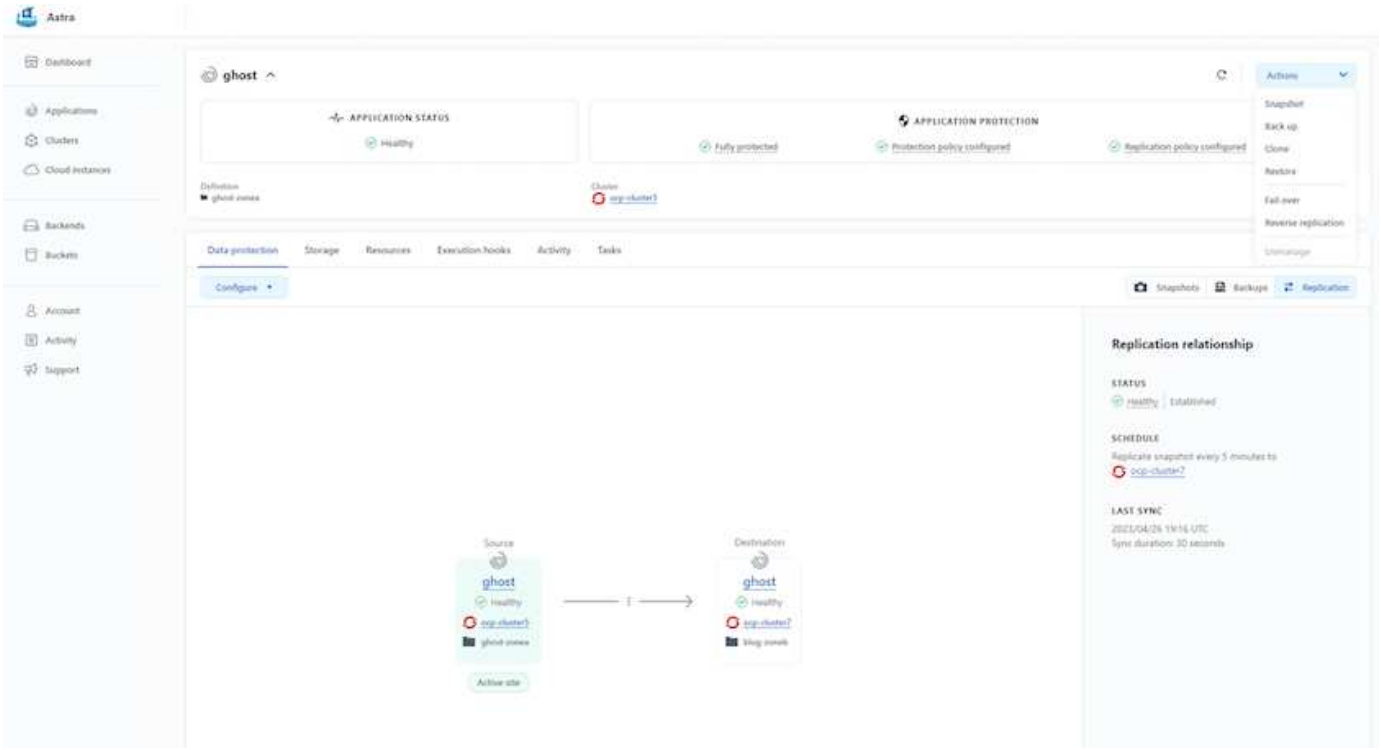
Pour la protection régionale ou pour une solution à faible RPO et RTO, une application peut être répliquée vers une autre instance Kubernetes s'exécutant sur un autre site, de préférence dans une autre région. ACC utilise

ONTAP Async SnapMirror avec RPO à partir de 5 minutes. La réplication s'effectue par réplication dans ONTAP, puis un basculement crée les ressources Kubernetes dans le cluster de destination.

Notez que la réplication est différente de la sauvegarde et de la restauration où la sauvegarde est envoyée vers S3 et la restauration depuis S3. Pour plus d'informations sur les différences entre les deux types de protection des données, consultez le lien : here.

Reportez-vous à "ici" Pour obtenir les instructions d'installation de SnapMirror.

SnapMirror avec ACC



les pilotes de stockage san-economy et nas-economy ne prennent pas en charge la fonction de réplication. Reportez-vous à "ici" pour plus d'informations.

Vidéo de démonstration :

"Vidéo de démonstration de la reprise d'activité avec Astra Control Center"

Protection des données avec Astra Control Center

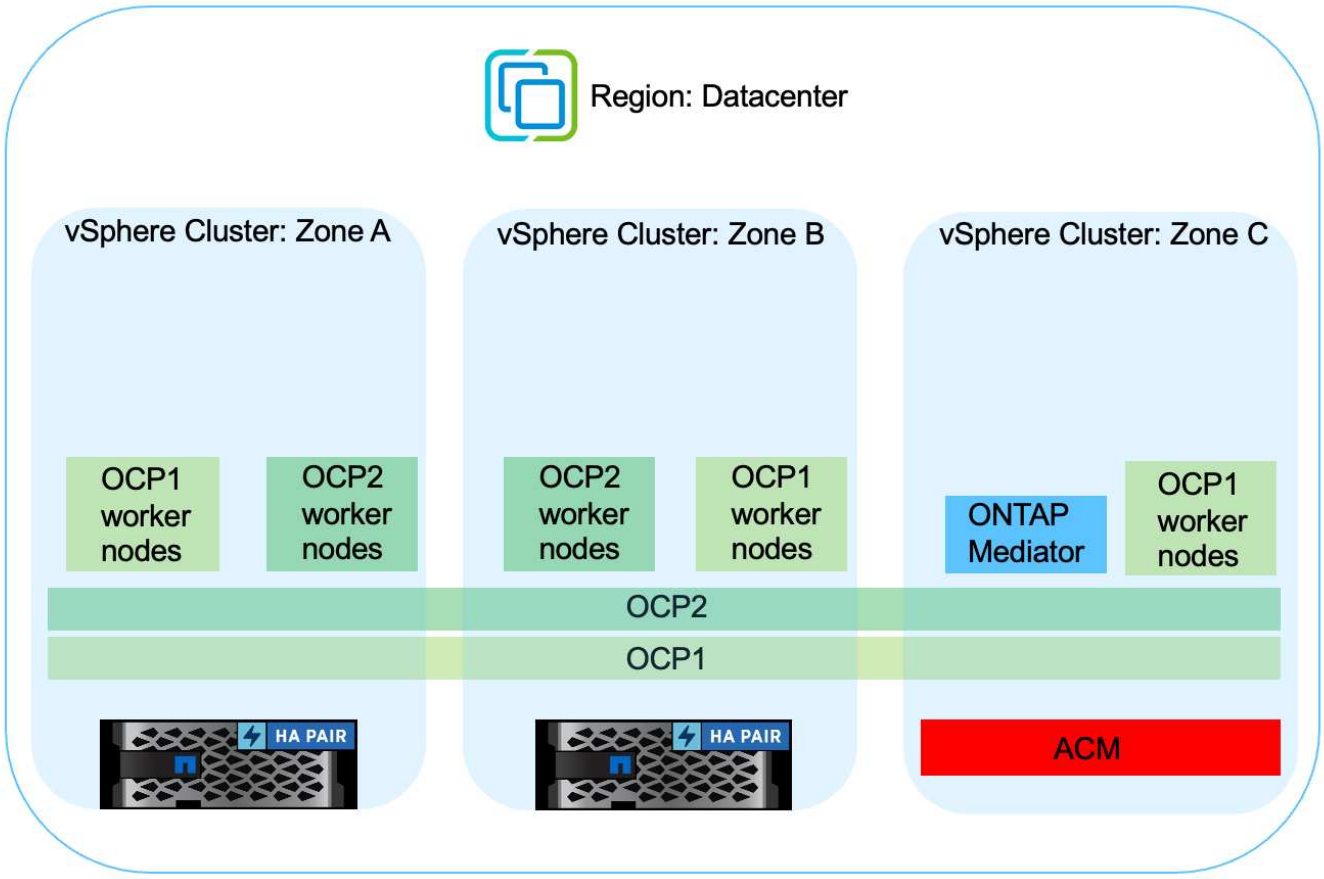
Continuité de l'activité avec MetroCluster

La plupart de notre plate-forme matérielle pour ONTAP dispose de fonctionnalités de haute disponibilité pour se protéger contre les pannes de systèmes, ce qui évite d'avoir à effectuer des opérations de récupération à plat. Mais pour éviter les risques d'incendie ou de tout autre incident et pour poursuivre l'activité avec un RPO nul et un RTO faible, on utilise souvent une solution MetroCluster.

Les clients qui disposent actuellement d'un système ONTAP peuvent s'étendre à MetroCluster en ajoutant des systèmes ONTAP pris en charge dans les limites de distance pour fournir une reprise après incident au niveau de la zone. ASTRA Trident, le CSI (interface de stockage de conteneurs) prend en charge NetApp ONTAP, y compris la configuration MetroCluster, ainsi que d'autres options comme Cloud Volumes ONTAP, Azure

NetApp Files, AWS FSX pour NetApp ONTAP, etc ASTRA Trident inclut cinq options de pilotes de stockage pour ONTAP et tous sont pris en charge pour la configuration MetroCluster. Reportez-vous à "ici" Pour en savoir plus sur les pilotes de stockage ONTAP pris en charge par Astra Trident.

La solution MetroCluster nécessite une extension réseau de couche 2 ou une capacité d'accès à la même adresse réseau à partir des deux domaines de défaillance. Une fois la configuration MetroCluster en place, la solution est transparente pour les propriétaires d'applications, puisque tous les volumes du svm MetroCluster sont protégés et profitent des avantages de SyncMirror (RPO nul).



Pour la configuration back-end Trident (TBC), ne spécifiez pas la dataLIF et le SVM lors de l'utilisation de la configuration MetroCluster. Spécifier l'IP de gestion du SVM pour la LIF managementLIF et utiliser les identifiants de rôle vsadmin

Des informations détaillées sur les fonctionnalités de protection des données d'Astra Control Center sont disponibles "ici"

Migration des données à l'aide d'Astra Control Center

Cette page présente les options de migration des données pour les workloads de conteneurs sur des clusters Red Hat OpenShift avec Astra Control Center (ACC).

Les applications Kubernetes doivent souvent être déplacées d'un environnement à un autre. Pour migrer une application et ses données persistantes, il est possible d'utiliser NetApp ACC.

Migration des données entre différents environnements Kubernetes

ACC prend en charge plusieurs versions de Kubernetes, notamment Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Kubernetes en amont, etc Pour plus d'informations, reportez-vous à la section "ici".

Pour migrer une application d'un cluster à un autre, vous pouvez utiliser l'une des fonctions suivantes d'ACC :

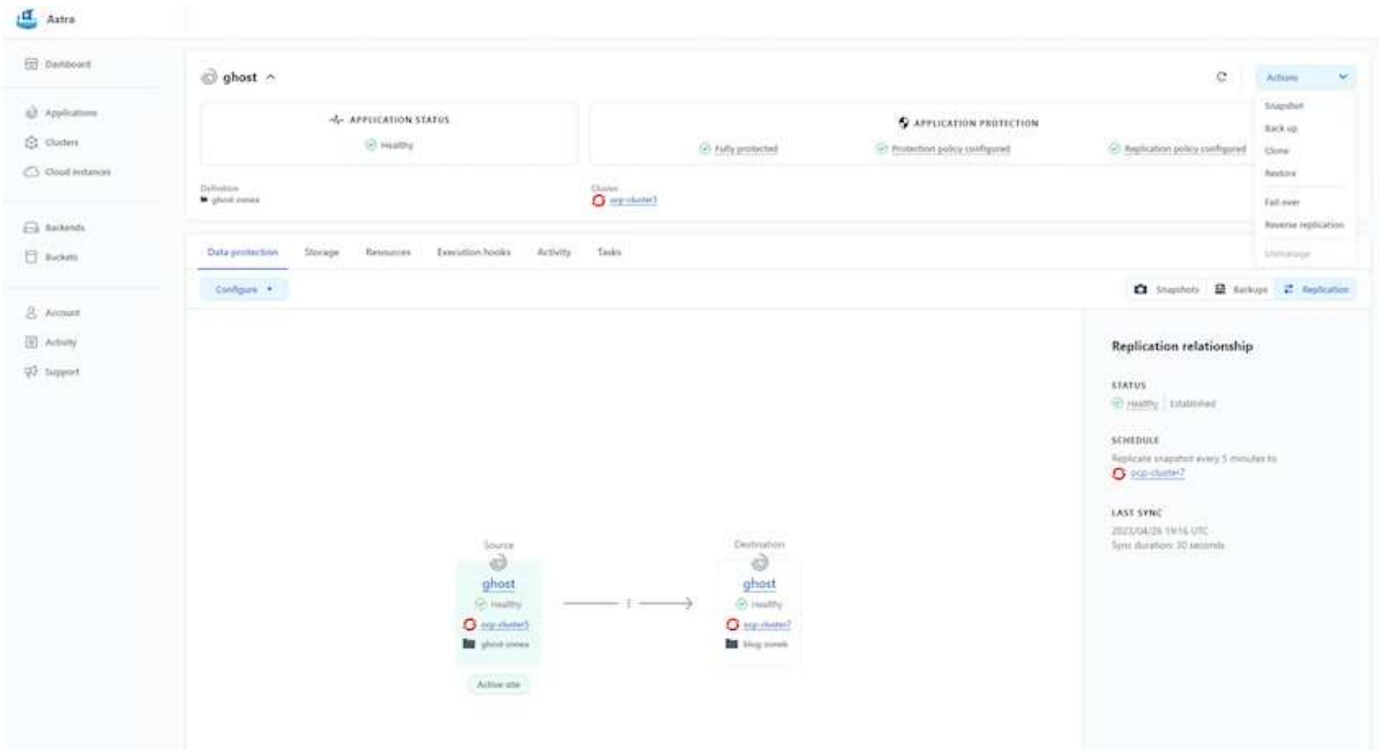
- **réplication**
- **sauvegarde et restauration**
- **clone**

Reportez-vous à la "section sur la protection des données" pour les options **réplication et sauvegarde et restauration**.

Reportez-vous à "ici" pour plus de détails sur **clonage**.

> La fonctionnalité de réplication Astra n'est prise en charge qu'avec le plug-in Trident Container Storage interface (CSI). Cependant, la réplication n'est pas prise en charge par les pilotes NAS-Economy et san-Economy.

Réplication des données à l'aide d'ACC



Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

Présentation

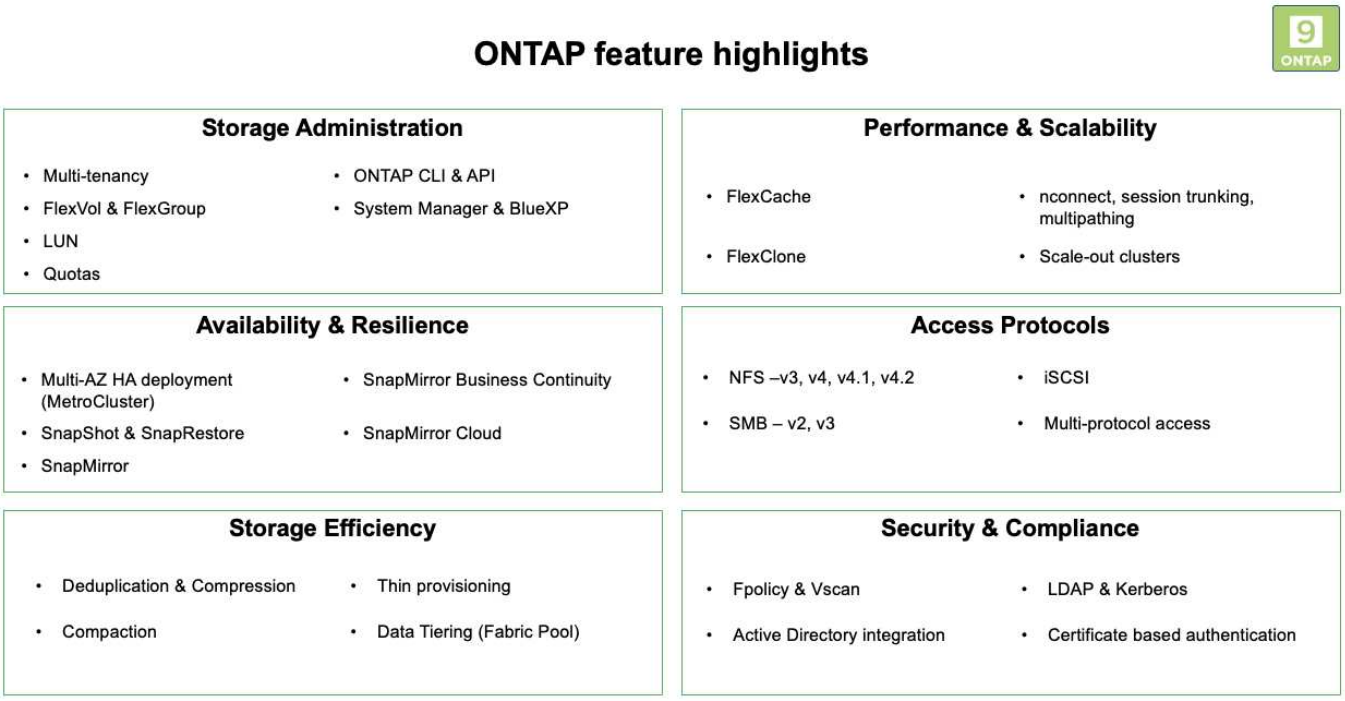
NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées

sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers

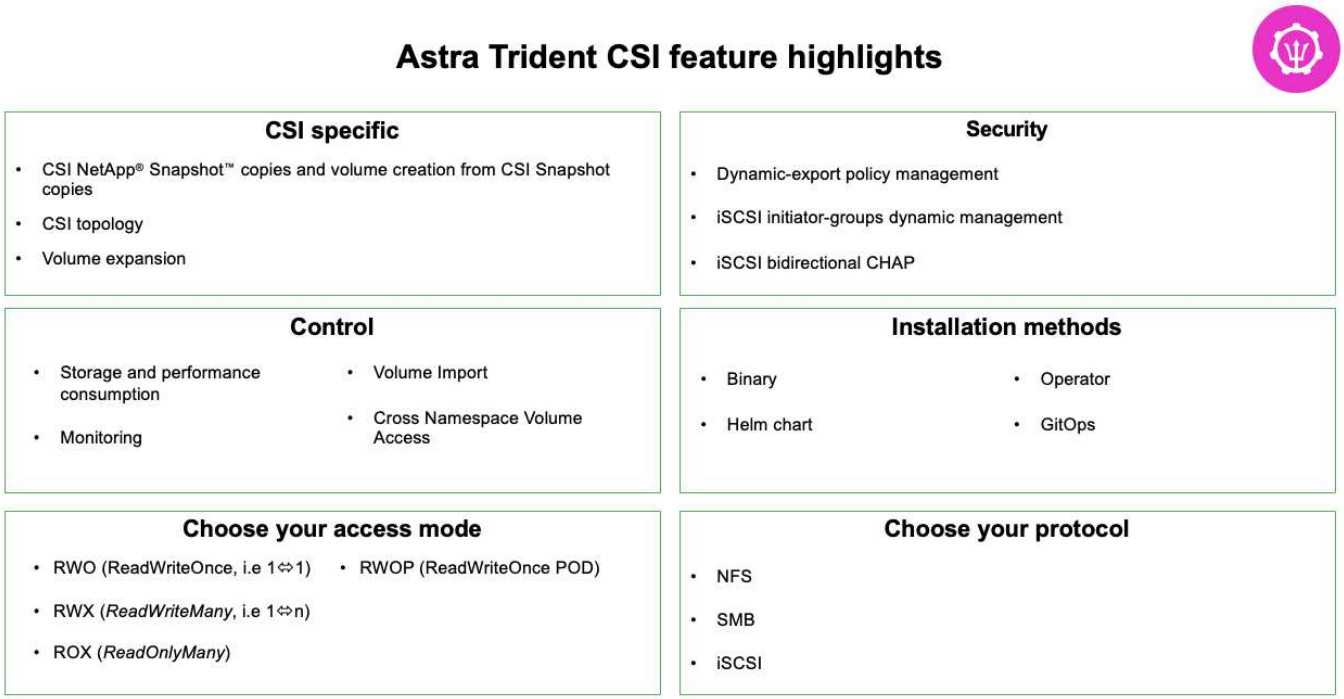


NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées

ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Solution NetApp avec les workloads de plateforme de conteneurs Red Hat OpenShift dans le cloud hybride

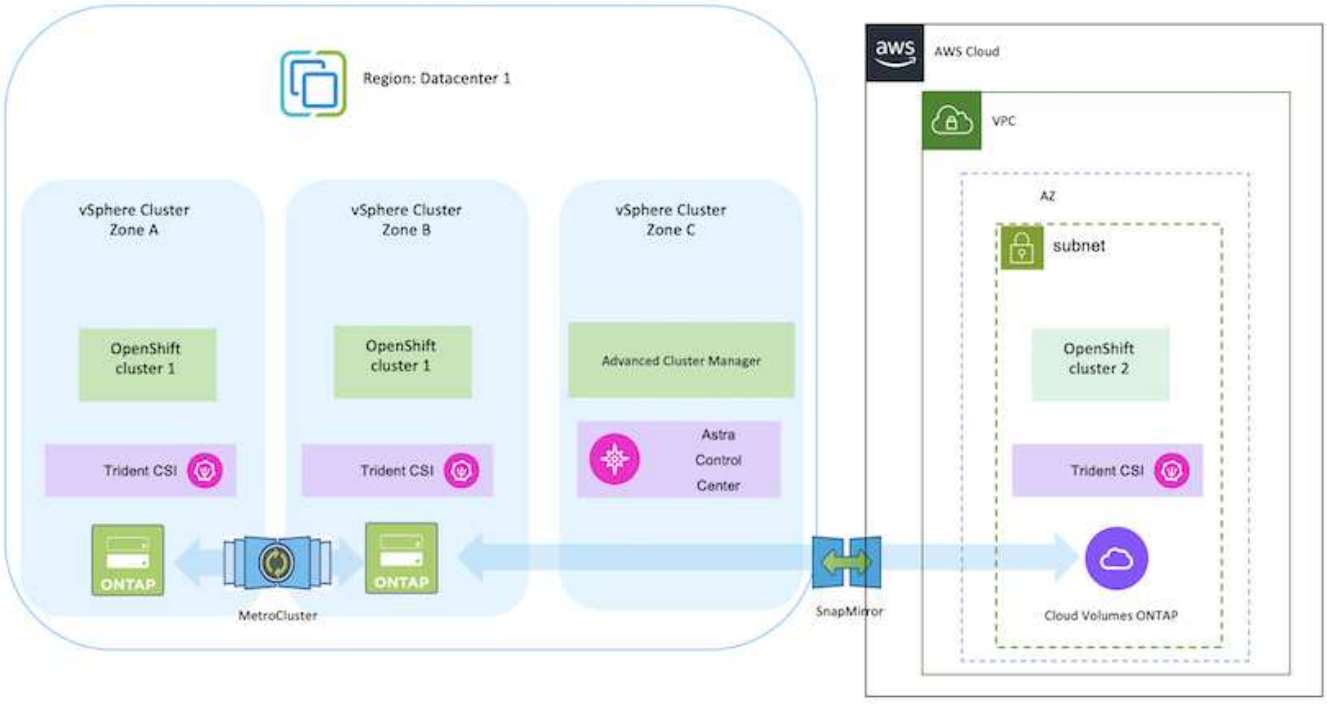
Les clients peuvent se trouver à un point de leur parcours de modernisation lorsqu'ils sont prêts à déplacer des workloads spécifiques ou tous les workloads de leurs data

centers vers le cloud. Ils peuvent choisir d'utiliser des conteneurs OpenShift autogérés et du stockage NetApp autogéré dans le cloud pour diverses raisons. Ils doivent planifier et déployer Red Hat OpenShift Container Platform (OCP) dans le cloud pour que l'environnement soit prêt à la production et puisse migrer les workloads de conteneurs depuis leurs data centers. Leurs clusters OCP peuvent être déployés sur VMware ou bare Metal dans leurs data centers, ainsi que sur AWS, Azure ou Google Cloud dans l'environnement cloud.

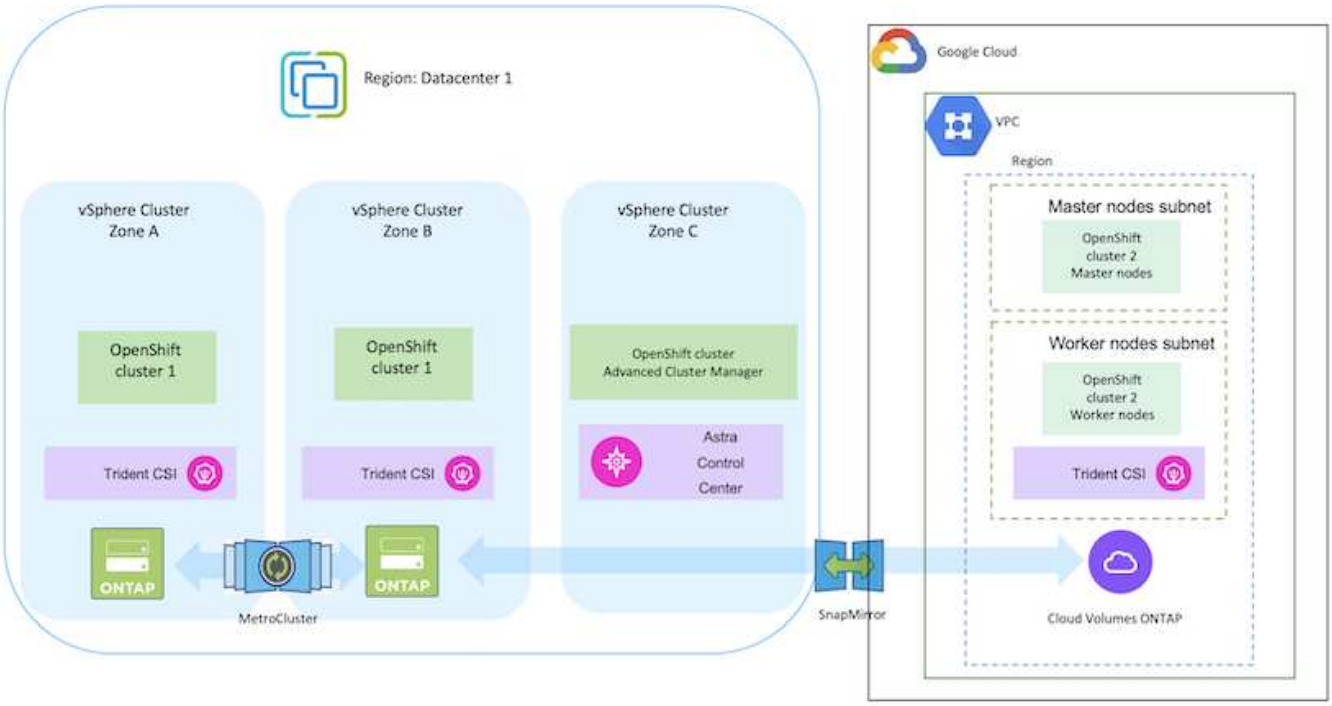
Le stockage NetApp Cloud Volumes ONTAP assure la protection, la fiabilité et la flexibilité des données pour les déploiements de conteneurs dans AWS, Azure et dans Google Cloud. ASTRA Trident sert de mécanisme de provisionnement de stockage dynamique pour consommer le stockage Cloud Volumes ONTAP persistant pour les applications avec état des clients. ASTRA Control Center peut être utilisé pour orchestrer les nombreuses exigences de gestion des données des applications avec état, telles que la protection des données, la migration et la continuité de l'activité.

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift dans un cloud hybride via Astra Control Center

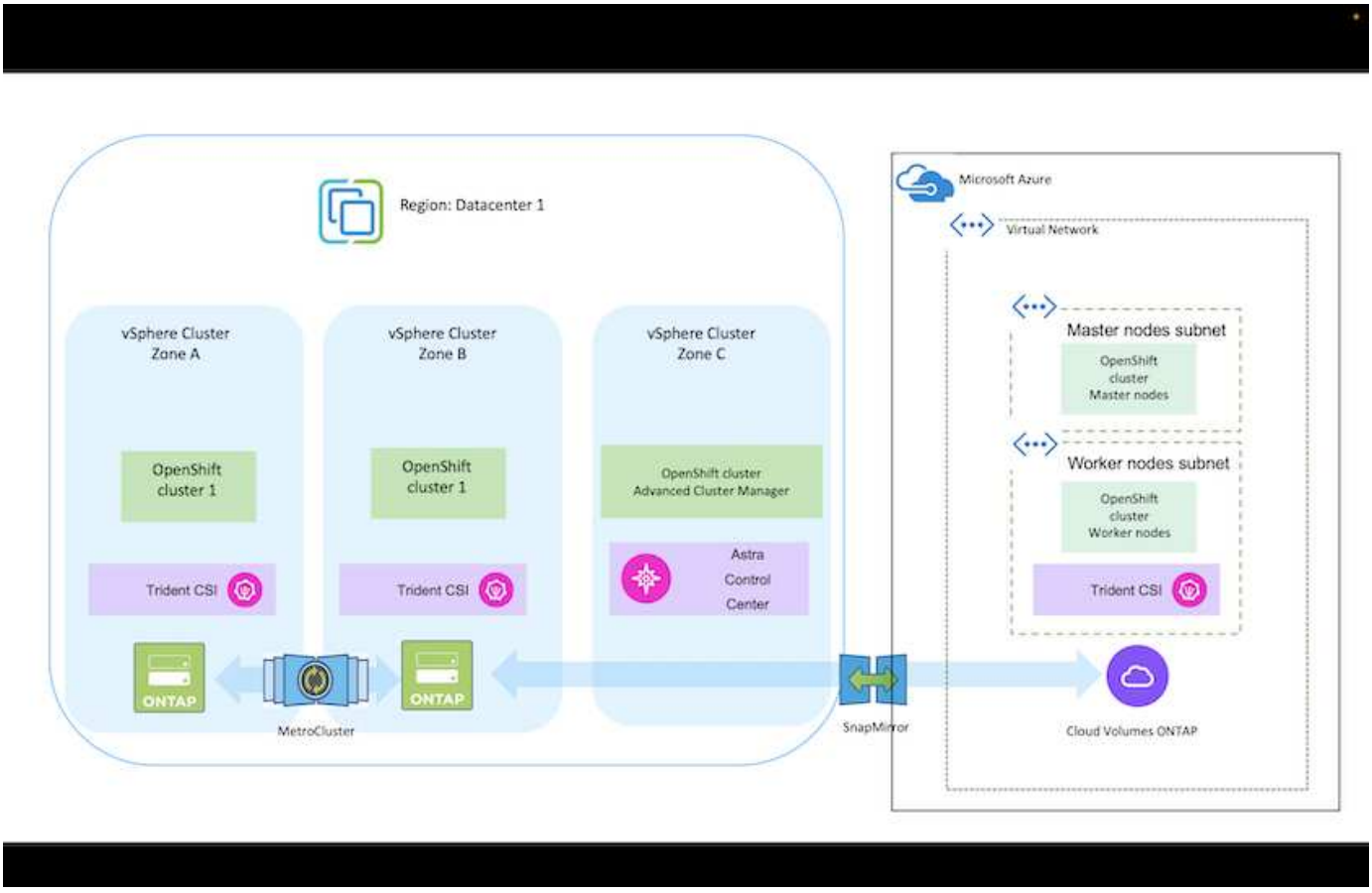
Sur site et AWS



Sur site et Google Cloud



Sur site et dans le cloud Azure



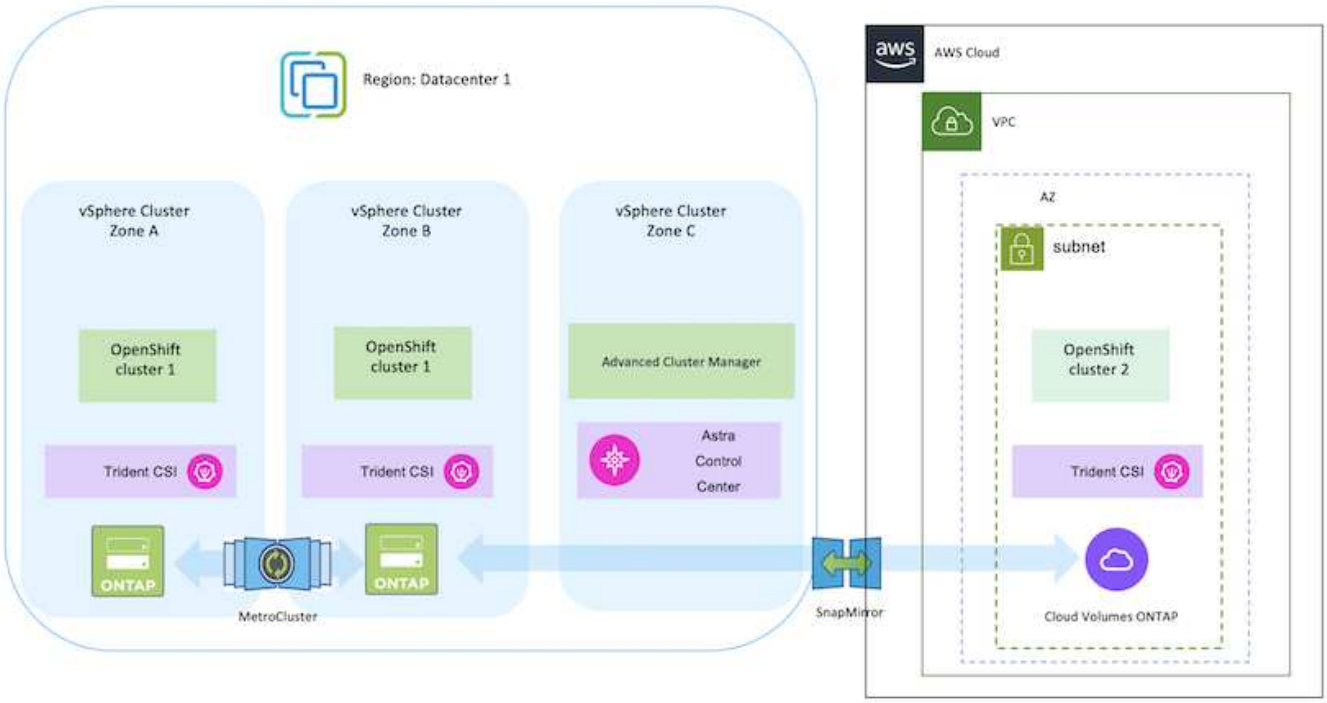
Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur AWS

Cette section décrit un workflow général expliquant comment configurer et gérer des

clusters OpenShift dans AWS et comment déployer des applications avec état sur ces clusters. Il présente l'utilisation du stockage NetApp Cloud Volumes ONTAP à l'aide d'Astra Trident pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

Il existe plusieurs façons de déployer les clusters Red Hat OpenShift Container Platform sur AWS. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Voici un diagramme illustrant les clusters déployés sur AWS et connectés au data Center à l'aide d'un VPN.



Le processus de configuration peut être divisé en plusieurs étapes :

Installez un cluster OCP sur AWS à partir de Advanced Cluster Management.

- Créez un VPC avec une connexion VPN de site à site (à l'aide de pfsense) pour vous connecter au réseau sur site.
- Le réseau sur site dispose d'une connectivité Internet.
- Créez 3 sous-réseaux privés dans 3 zones de disponibilité différentes.
- Créez une zone hébergée privée route 53 et un résolveur DNS pour le VPC.

Créez OpenShift Cluster sur AWS à partir de l'assistant ACM (Advanced Cluster Management). Reportez-vous aux instructions "ici".

Vous pouvez également créer le cluster dans AWS à partir de la console OpenShift Hybrid Cloud. Reportez-vous à "ici" pour obtenir des instructions.

Lors de la création du cluster à l'aide de l'ACM, vous avez la possibilité de personnaliser l'installation en modifiant le fichier yaml après avoir rempli les détails dans la vue de formulaire. Une fois le cluster créé, vous pouvez vous connecter en ssh aux nœuds du cluster à des fins de dépannage ou à des fins de configuration manuelle supplémentaire. Utilisez la clé ssh que vous avez fournie lors de l'installation et le nom d'utilisateur core pour vous connecter.

Déployez Cloud Volumes ONTAP dans AWS à l'aide de BlueXP.

- Installez le connecteur dans un environnement VMware sur site. Reportez-vous aux instructions "ici".
- Déployez une instance CVO dans AWS à l'aide de Connector. Reportez-vous aux instructions "ici".

Le connecteur peut également être installé dans l'environnement cloud. Reportez-vous à "ici" pour plus d'informations.

Installer Astra Trident dans le cluster OCP

- Déployez l'opérateur Trident à l'aide d'Helm. Reportez-vous aux instructions "ici"
- Créez un back-end et une classe de stockage. Reportez-vous aux instructions "ici".

Ajoutez le cluster OCP sur AWS à Astra Control Center.

Ajoutez le cluster OCP dans AWS à Astra Control Center.

Utilisation de la fonctionnalité de topologie CSI de Trident pour les architectures multi-zones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de frayer les nœuds des clusters basés sur les zones. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones. Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Reportez-vous à "ici" pour plus d'informations.

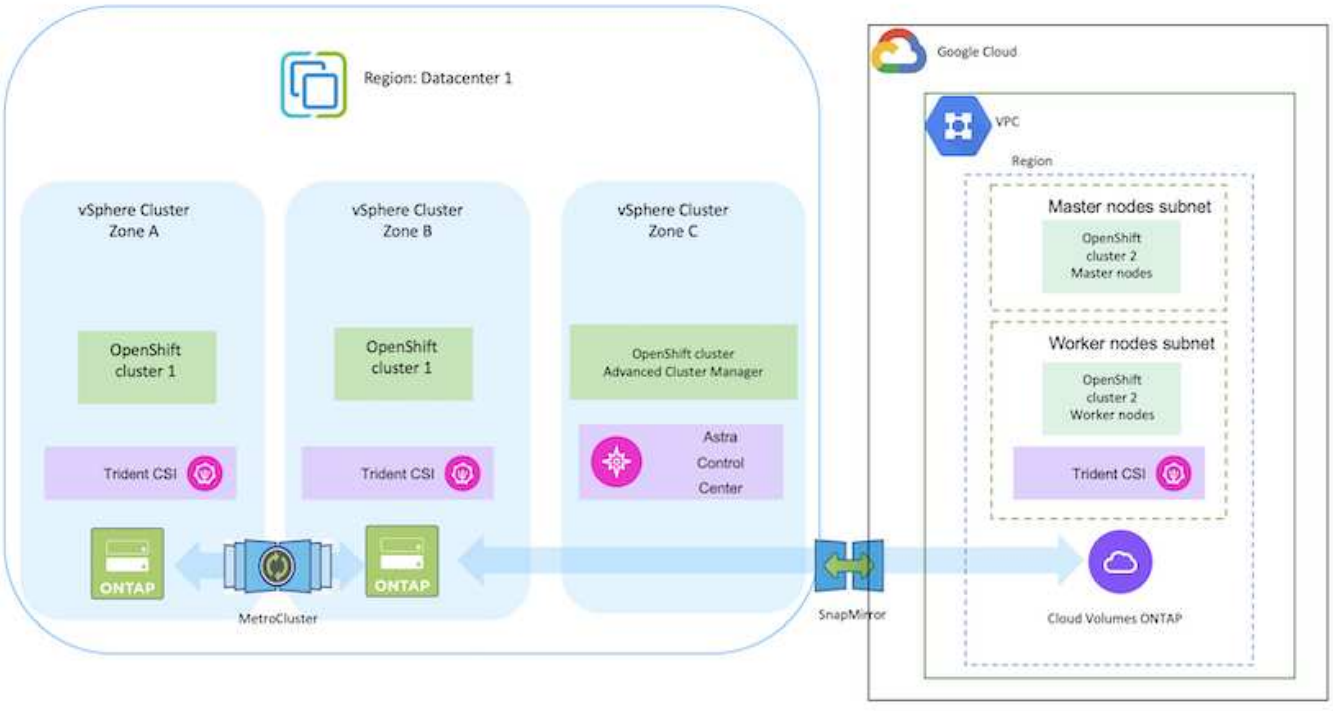
Kubernetes prend en charge deux modes de liaison de volume : - lorsque ***VolumeBindingMode*** **est défini sur** ***immédiat*** (par défaut), Astra Trident crée le volume sans sensibilisation à la topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod qui en fait la demande. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour une PVC est retardée jusqu'à ce qu'un pod qui utilise la PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie. Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (back-end compatible avec la topologie). Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge. (Classes de stockage orientées topologie) "ici" pour plus d'informations.

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur GCP

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur GCP

Cette section décrit un workflow de haut niveau expliquant comment configurer et gérer des clusters OpenShift dans GCP et déployer des applications avec état sur ces clusters. Il présente l'utilisation du stockage NetApp Cloud Volumes ONTAP à l'aide d'Astra Trident pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

La présente figure présente les clusters déployés sur GCP et connectés au data Center à l'aide d'un VPN.



Il existe plusieurs façons de déployer les clusters de plateforme de conteneurs Red Hat OpenShift dans GCP. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Le processus de configuration peut être divisé en plusieurs étapes :

Installez un cluster OCP sur GCP à partir de l'interface de ligne de commande.

- Assurez-vous que vous avez rempli toutes les conditions préalables indiquées "ici".
- Pour la connectivité VPN entre l'infrastructure sur site et GCP, une machine virtuelle pfsense a été créée et configurée. Pour obtenir des instructions, reportez-vous à la section "ici".
  - L'adresse de la passerelle distante dans pfsense ne peut être configurée qu'après avoir créé une passerelle VPN dans Google Cloud Platform.
  - Les adresses IP de réseau distant pour la phase 2 ne peuvent être configurées qu'après l'exécution du programme d'installation du cluster OpenShift et la création des composants d'infrastructure pour le cluster.
  - Le VPN dans Google Cloud ne peut être configuré qu'une fois que les composants de l'infrastructure du cluster ont été créés par le programme d'installation.
- Installez maintenant le cluster OpenShift sur GCP.
  - Obtenez le programme d'installation et le code Pull et déployez le cluster en suivant les étapes fournies dans la documentation "ici".
  - L'installation crée un réseau VPC dans Google Cloud Platform. Il crée également une zone privée dans Cloud DNS et ajoute Des enregistrements.
    - Utilisez l'adresse de bloc CIDR du réseau VPC pour configurer pfsense et établir la connexion VPN. Assurez-vous que les pare-feu sont correctement configurés.
    - Ajoutez des enregistrements dans le DNS de l'environnement sur site en utilisant l'adresse IP dans les enregistrements A du DNS Google Cloud.
  - L'installation du cluster est terminée et fournira un fichier kubeconfig ainsi qu'un nom d'utilisateur et un mot de passe pour vous connecter à la console du cluster.

Déployez Cloud Volumes ONTAP dans GCP à l'aide de BlueXP.

- Installez un connecteur dans Google Cloud. Reportez-vous aux instructions "ici".
- Déployez une instance CVO dans Google Cloud à l'aide de Connector. Reportez-vous aux instructions ici. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Installez Astra Trident dans le cluster OCP dans GCP

- Comme illustré, il existe de nombreuses méthodes de déploiement d'Astra Trident "ici".
- Pour ce projet, Astra Trident a été installé en déployant l'opérateur Astra Trident manuellement en utilisant les instructions "ici".
- Créez le back-end et des classes de stockage. Reportez-vous aux instructions "ici".

Ajoutez le cluster OCP sur GCP à Astra Control Center.

- Créez un fichier KubeConfig distinct avec un rôle de cluster qui contient les autorisations minimales nécessaires à la gestion d'un cluster par Astra Control. Les instructions sont disponibles "ici".
- Ajoutez le cluster à Astra Control Center en suivant les instructions "ici"

Utilisation de la fonctionnalité de topologie CSI de Trident pour les architectures multi-zones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de frayer les nœuds des clusters basés sur les zones. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones. Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Reportez-vous à "ici" pour plus d'informations.

> Kubernetes prend en charge deux modes de liaison de volume : - lorsque ***VolumeBindingMode*** **est défini sur** ***immédiat*** (par défaut), Astra Trident crée le volume sans sensibilisation à la topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod qui en fait la demande. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour une PVC est retardée jusqu'à ce qu'un pod qui utilise la PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie. Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (back-end compatible avec la topologie). Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge. (Classes de stockage orientées topologie) "ici" pour plus d'informations.

vidéo de démonstration

Installation d'OpenShift Cluster sur Google Cloud Platform

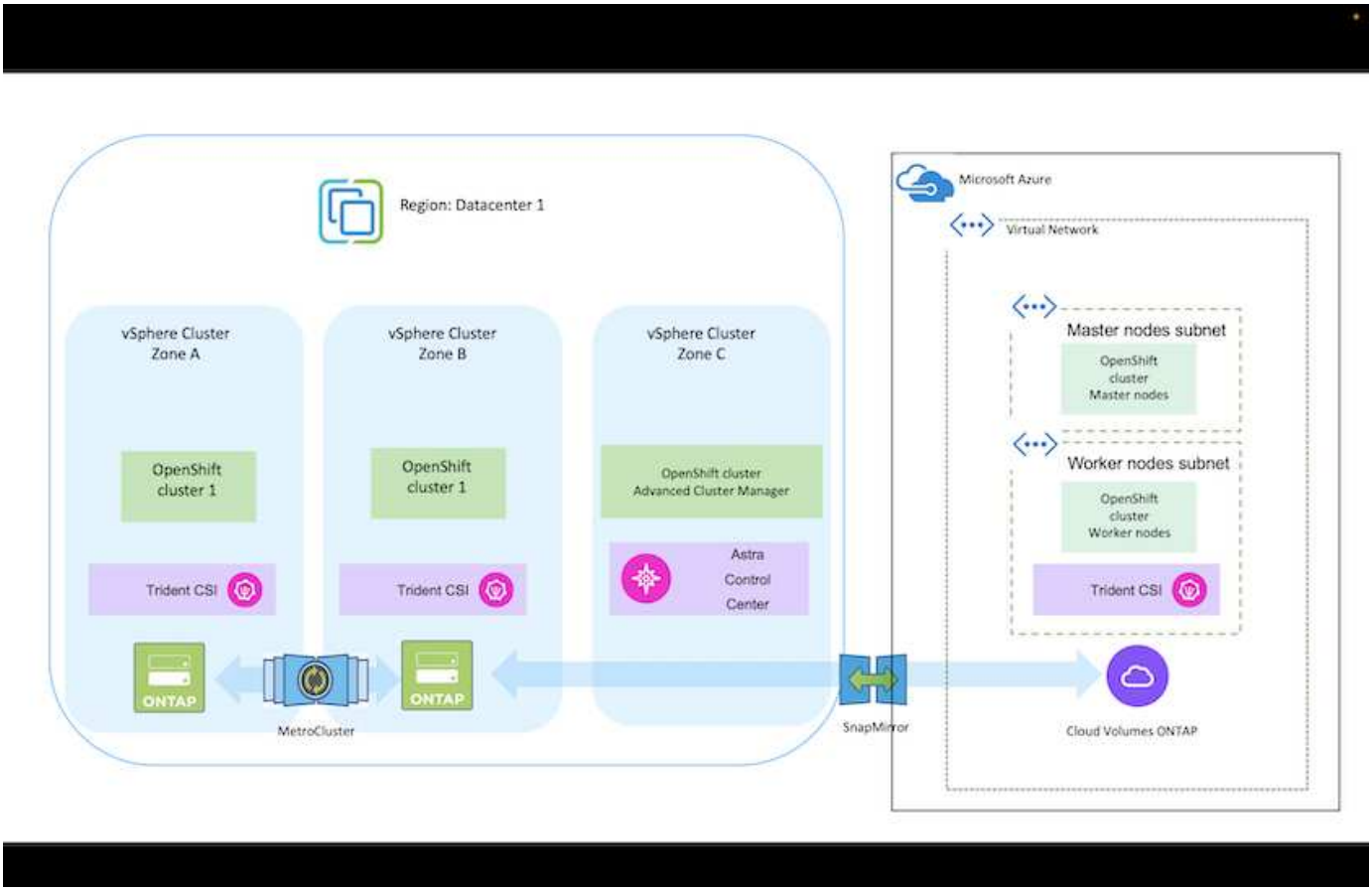
Importation de clusters OpenShift dans Astra Control Center

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur Azure

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur Azure

Cette section décrit un workflow général expliquant comment configurer et gérer des clusters OpenShift dans Azure et comment déployer des applications avec état sur ces clusters. Il présente l'utilisation du stockage NetApp Cloud Volumes ONTAP à l'aide d'Astra Trident/Astra Control Provisioner pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

Voici un diagramme illustrant les clusters déployés sur Azure et connectés au data Center à l'aide d'un VPN.



Il existe plusieurs façons de déployer les clusters de plateforme de conteneurs Red Hat OpenShift dans Azure. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Le processus de configuration peut être divisé en plusieurs étapes :

Installez un cluster OCP sur Azure à partir de l'interface de ligne de commande.

- Assurez-vous que vous avez rempli toutes les conditions préalables indiquées "ici".
- Créez un VPN, des sous-réseaux et des groupes de sécurité réseau, ainsi qu'une zone DNS privée. Créez une passerelle VPN et une connexion VPN de site à site.
- Pour la connectivité VPN entre les installations sur site et Azure, une machine virtuelle pfsense a été créée et configurée. Pour obtenir des instructions, reportez-vous à la section "ici".
- Obtenez le programme d'installation et le code Pull et déployez le cluster en suivant les étapes fournies dans la documentation "ici".
- L'installation du cluster est terminée et fournira un fichier kubeconfig ainsi qu'un nom d'utilisateur et un mot de passe pour vous connecter à la console du cluster.

Un exemple de fichier install-config.yaml est fourni ci-dessous.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
```

```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

Déployez Cloud Volumes ONTAP dans Azure à l'aide de BlueXP.

- Installez un connecteur dans Azure. Reportez-vous aux instructions "ici".
- Déployez une instance CVO dans Azure à l'aide de Connector. Reportez-vous au lien d'instructions :https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [ici].

Installez Astra Control Provisioner dans le cluster OCP dans Azure

- Pour ce projet, Astra Control Provisioner (ACP) a été installé sur tous les clusters (cluster sur site, cluster sur site où Astra Control Center est déployé et le cluster dans Azure). En savoir plus sur Astra Control Provisioner "ici".
- Créez le back-end et des classes de stockage. Reportez-vous aux instructions "ici".

Ajoutez le cluster OCP sur Azure à Astra Control Center.

- Créez un fichier KubeConfig distinct avec un rôle de cluster qui contient les autorisations minimales nécessaires à la gestion d'un cluster par Astra Control. Les instructions sont disponibles "ici".
- Ajoutez le cluster à Astra Control Center en suivant les instructions "ici"

Utilisation de la fonctionnalité de topologie CSI de Trident pour les architectures multi-zones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de frayer les nœuds des clusters basés sur les zones. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones. Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Reportez-vous à "ici" pour plus d'informations.

> Kubernetes prend en charge deux modes de liaison de volume : - lorsque ***VolumeBindingMode*** **est défini sur** ***immédiat*** (par défaut), Astra Trident crée le volume sans sensibilisation à la topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod qui en fait la demande. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour une PVC est retardée jusqu'à ce qu'un pod qui utilise la PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie. Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (back-end compatible avec la topologie). Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge. (Classes de stockage orientées topologie) "ici" pour plus d'informations.

vidéo de démonstration

Utilisation d'Astra Control pour le basculement et le retour arrière des applications

Protection des données avec Astra Control Center

Cette page présente les options de protection des données pour les applications basées sur des conteneurs Red Hat OpenShift s'exécutant sur VMware vSphere ou dans le cloud via Astra Control Center (ACC).

Au fur et à mesure que les utilisateurs s'engagent dans la modernisation de leurs applications avec Red Hat OpenShift, une stratégie de protection des données doit être mise en place pour les protéger contre toute suppression accidentelle ou toute autre erreur humaine. Souvent, une stratégie de protection est également nécessaire à des fins réglementaires ou de conformité afin de protéger leurs données contre les données d'un grand nombre.

Les exigences en matière de protection des données varient entre le retour à une copie instantanée et le basculement automatique vers un autre domaine de panne sans intervention humaine. De nombreux clients choisissent ONTAP comme plateforme de stockage préférée pour leurs applications Kubernetes en raison de ses nombreuses fonctionnalités, telles que la colocation, le multiprotocole, les performances et les capacités élevées, la réplication et la mise en cache pour les sites multisites, la sécurité et la flexibilité.

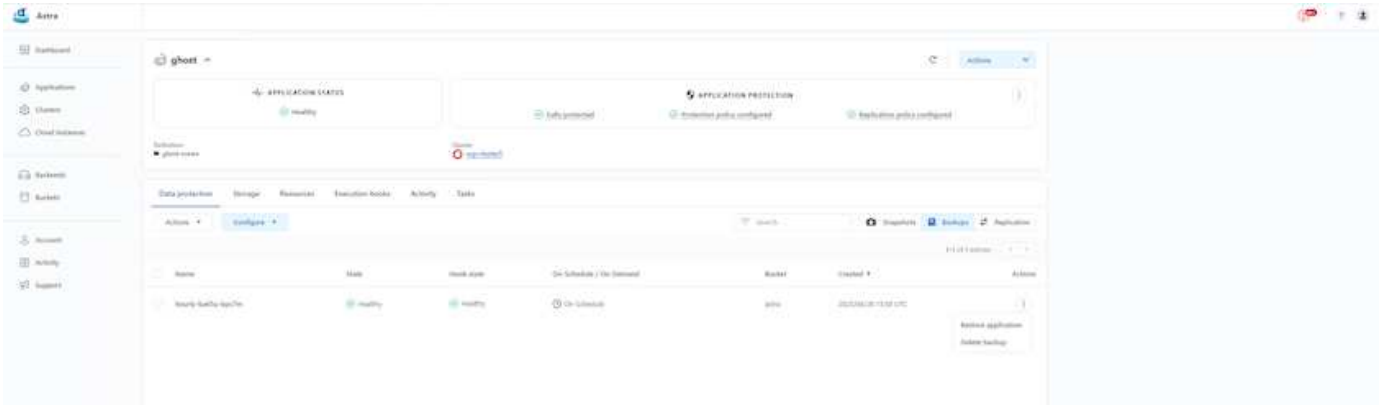
Les clients peuvent disposer d'un environnement cloud pour étendre leur data Center, afin de bénéficier des

avantages du cloud et de disposer d'un positionnement idéal pour déplacer leurs charges de travail à un moment ultérieur. Pour ces clients, la sauvegarde de leurs applications OpenShift et de leurs données dans l'environnement cloud devient un choix inévitable. Ils peuvent ensuite restaurer les applications et les données associées sur un cluster OpenShift dans le cloud ou dans leur data Center.

Sauvegarde et restauration avec ACC

Les propriétaires d'applications peuvent consulter et mettre à jour les applications découvertes par ACC. ACC peut effectuer des copies Snapshot à l'aide de CSI et effectuer des sauvegardes à l'aide de la copie Snapshot instantanée. La destination de la sauvegarde peut être un magasin d'objets dans l'environnement cloud. La règle de protection peut être configurée pour les sauvegardes planifiées et le nombre de versions de sauvegarde à conserver. L'objectif de point de récupération minimal est d'une heure.

Restauration d'une application à partir d'une sauvegarde à l'aide d'ACC

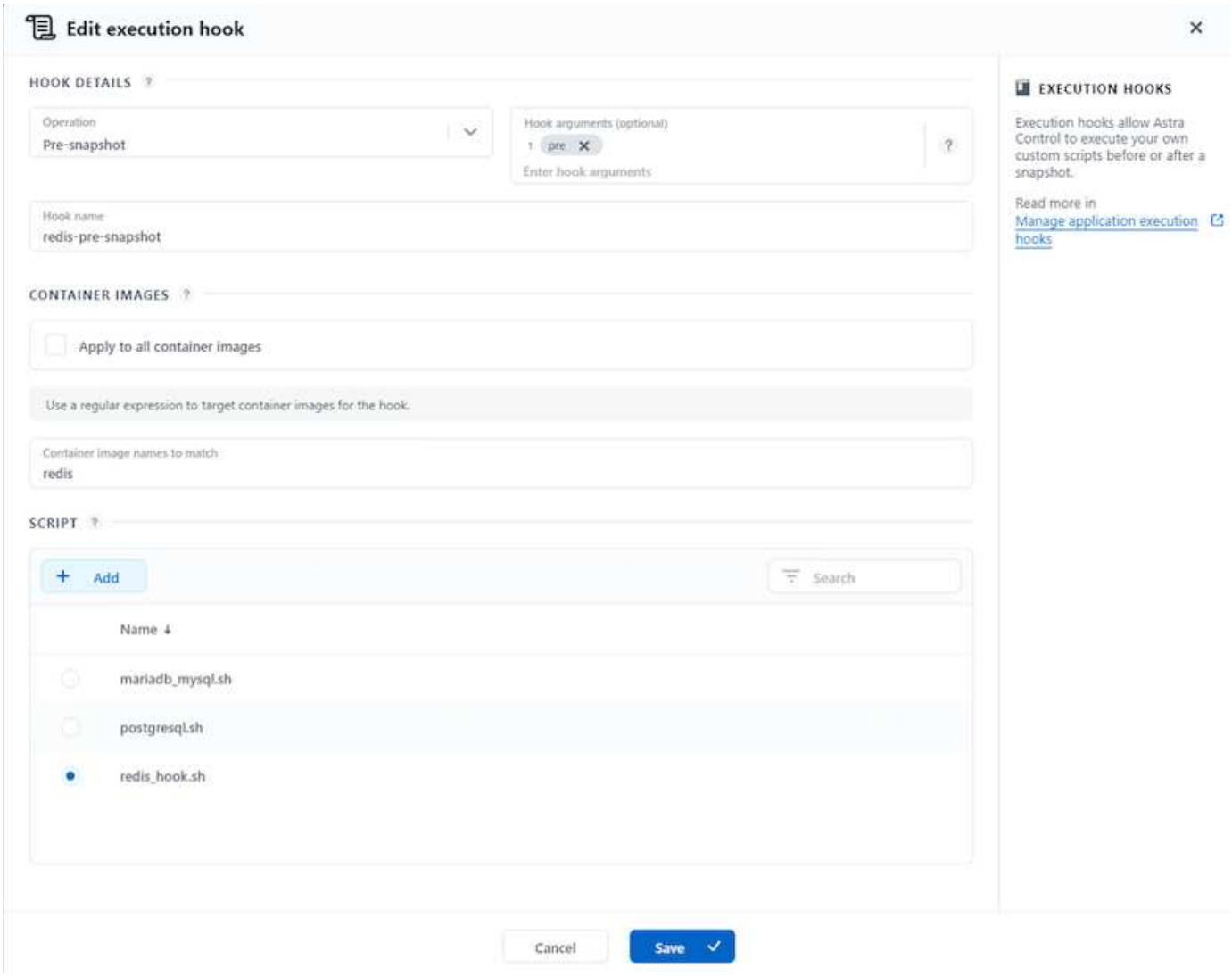


Crochets d'exécution spécifiques à l'application

Même si les fonctionnalités de protection des données au niveau des baies de stockage sont disponibles, des étapes supplémentaires sont souvent nécessaires pour assurer la cohérence des sauvegardes et des restaurations au niveau des applications. Les étapes supplémentaires spécifiques à l'application peuvent être : - avant ou après la création d'une copie Snapshot. - avant ou après la création d'une sauvegarde. - Après restauration à partir d'une copie Snapshot ou d'une sauvegarde. ASTRA Control peut exécuter ces étapes spécifiques à l'application codées comme des scripts personnalisés appelés crochets d'exécution.

NetApp "Projet open source Verda" fournit des crochets d'exécution pour les applications cloud les plus courantes afin de simplifier, renforcer et orchestrer la protection des applications. N'hésitez pas à contribuer à ce projet si vous avez suffisamment d'informations pour une application qui ne se trouve pas dans le référentiel.

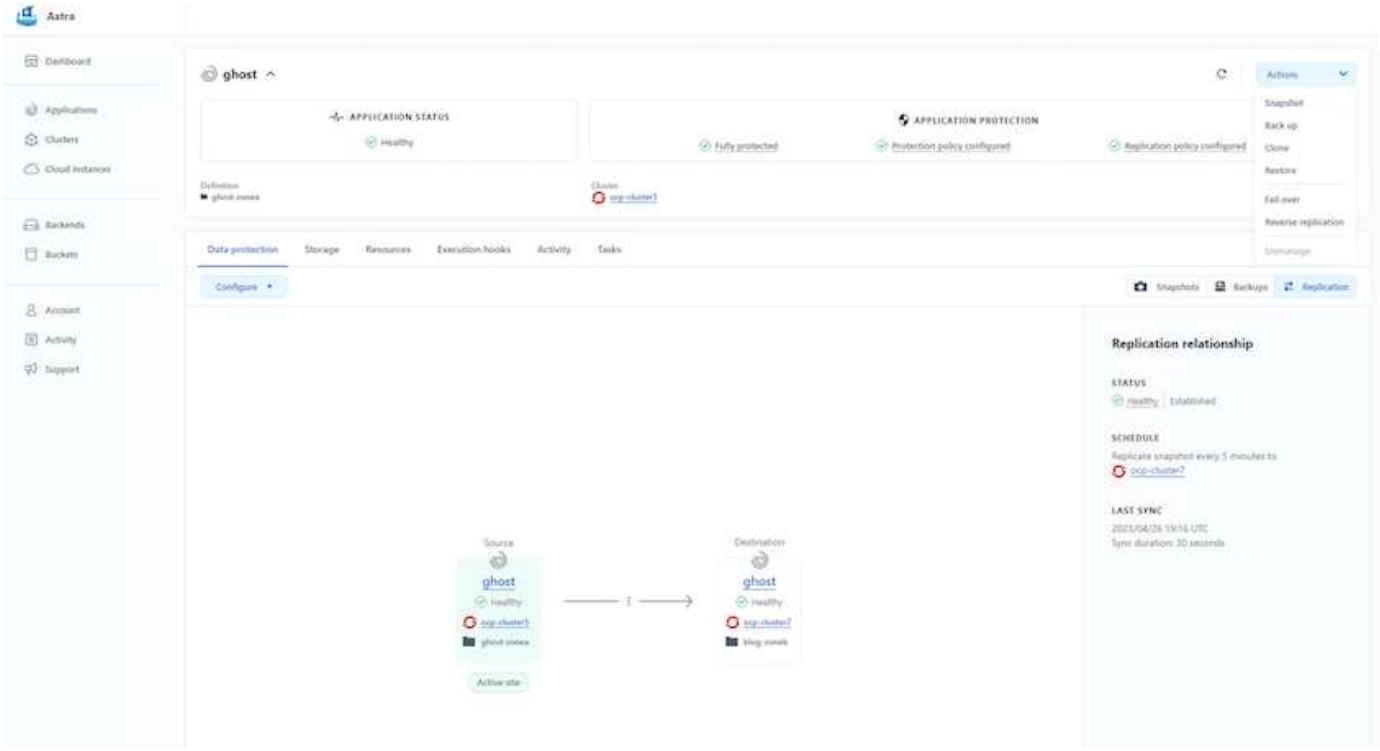
Exemple de crochet d'exécution pour pré-instantané d'une application redis.



Réplication avec ACC

Pour la protection régionale ou pour une solution à faible RPO et RTO, une application peut être répliquée vers une autre instance Kubernetes s'exécutant sur un autre site, de préférence dans une autre région. ACC utilise ONTAP Async SnapMirror avec RPO à partir de 5 minutes. Reportez-vous à "ici" Pour obtenir les instructions d'installation de SnapMirror.

SnapMirror avec ACC



les pilotes de stockage san-economy et nas-economy ne prennent pas en charge la fonction de réplication. Reportez-vous à "ici" pour plus d'informations.

Vidéo de démonstration :

"Vidéo de démonstration de la reprise d'activité avec Astra Control Center"

Protection des données avec Astra Control Center

Des informations détaillées sur les fonctionnalités de protection des données d'Astra Control Center sont disponibles "ici"

Reprise après incident (basculement et retour arrière avec réplication) avec ACC

Utilisation d'Astra Control pour le basculement et le retour arrière des applications

Migration des données à l'aide d'Astra Control Center

Cette page présente les options de migration des données pour les workloads de conteneurs sur des clusters Red Hat OpenShift avec Astra Control Center (ACC). Plus précisément, les clients peuvent utiliser ACC pour : déplacer des workloads sélectionnés ou tous les workloads de leurs data centers sur site vers le cloud ; cloner leurs applications vers le cloud à des fins de test ou passer du data Center au cloud

Migration des données

Pour migrer une application d'un environnement à un autre, vous pouvez utiliser l'une des fonctions suivantes d'ACC :

- **réplication**

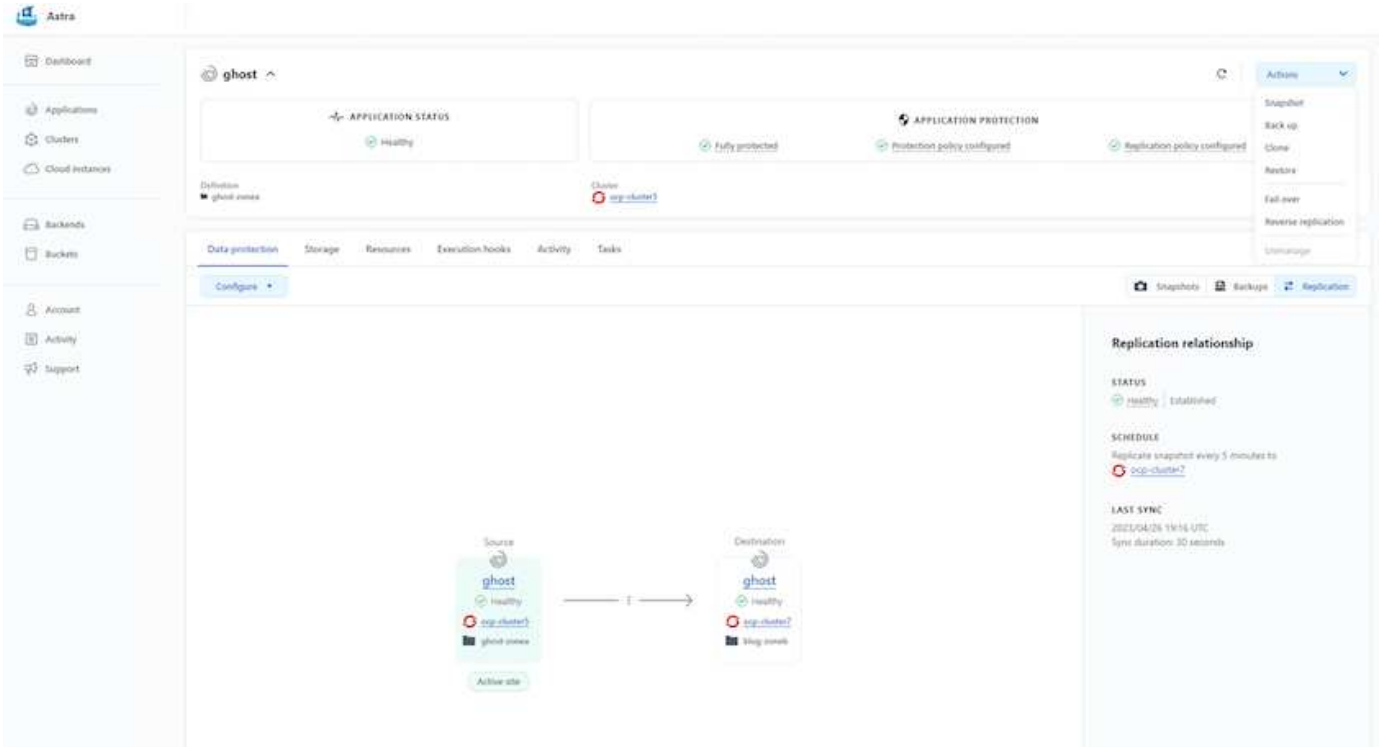
- **sauvegarde et restauration**
- **clone**

Reportez-vous à la "section sur la protection des données" pour les options **réplication et sauvegarde et restauration**.

Reportez-vous à "ici" pour plus de détails sur **clonage**.

> La fonctionnalité de réplication Astra n'est prise en charge qu'avec le plug-in Trident Container Storage interface (CSI). Cependant, la réplication n'est pas prise en charge par les pilotes NAS-Economy et san-Economy.

Réplication des données à l'aide d'ACC



Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

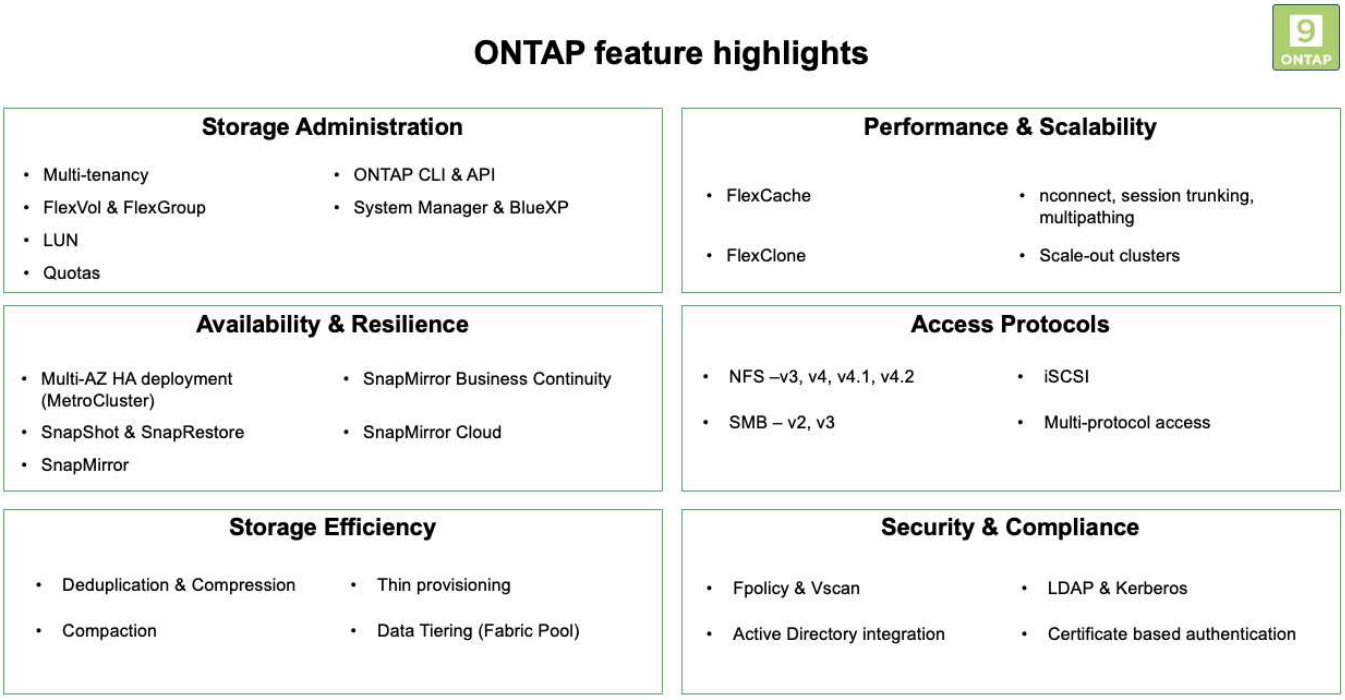
Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

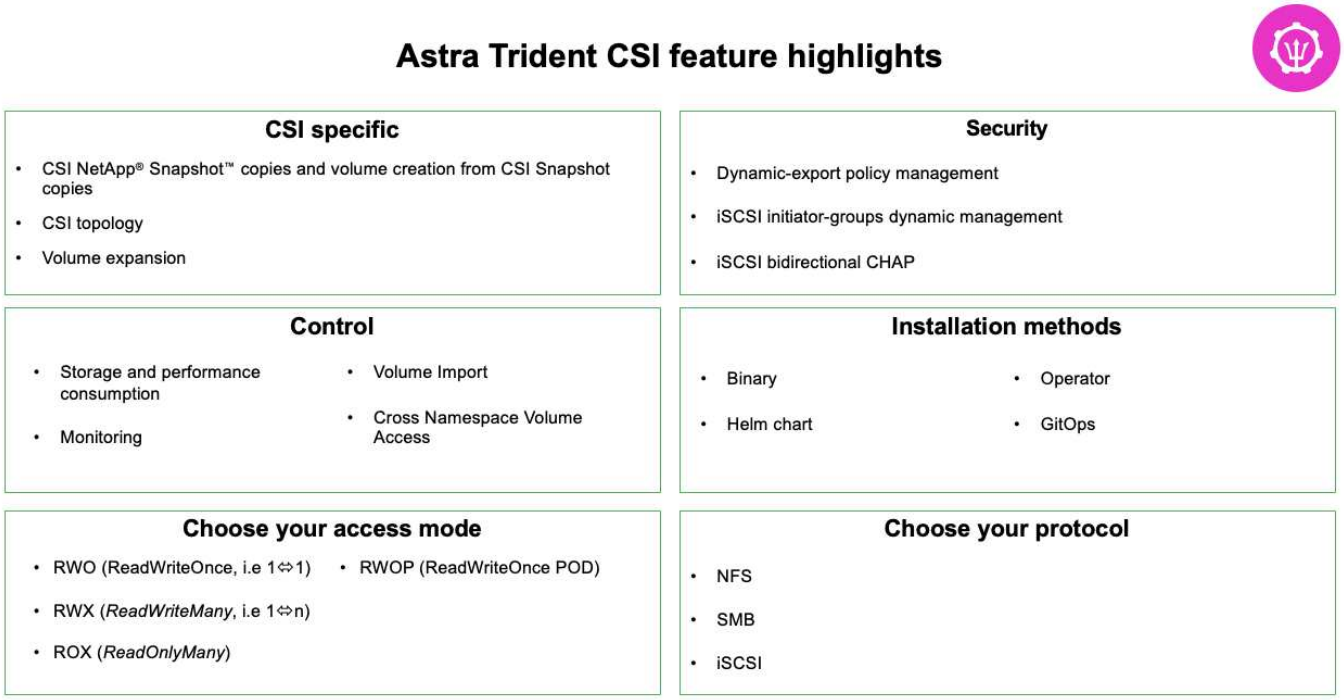
- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers



NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Solution NetApp avec les workloads gérés de la plateforme de conteneurs Red Hat OpenShift sur AWS

Solution NetApp avec les workloads gérés de la plateforme de conteneurs Red Hat OpenShift sur AWS

Les clients peuvent être « nés dans le cloud » ou se trouver à un point de leur parcours de modernisation lorsqu'ils sont prêts à déplacer des workloads spécifiques ou tous les

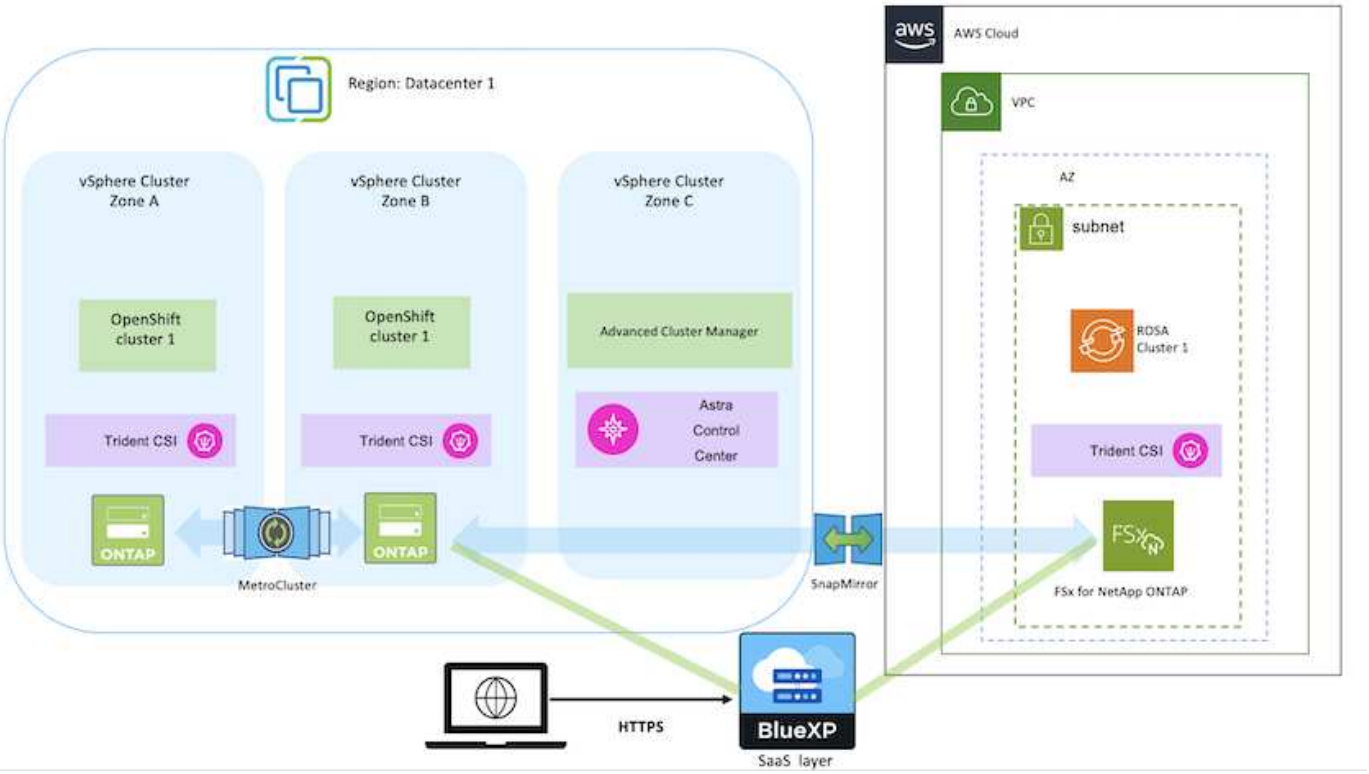
workloads de leurs data centers vers le cloud. Ils peuvent choisir d'utiliser des conteneurs OpenShift gérés par un fournisseur et du stockage NetApp géré par un fournisseur dans le cloud pour exécuter leurs workloads. Ils doivent planifier et déployer les clusters de conteneurs Red Hat OpenShift (ROSA) gérés dans le cloud pour assurer la réussite de leur environnement de production pour leurs workloads de conteneurs. Dans le cloud AWS, ils peuvent également déployer FSX pour NetApp ONTAP pour répondre aux besoins en stockage.

FSX pour NetApp ONTAP assure la protection, la fiabilité et la flexibilité des données pour les déploiements de conteneurs dans AWS. ASTRA Trident sert de mécanisme de provisionnement de stockage dynamique pour consommer le stockage FSxN persistant pour les applications avec état des clients.

COMME ROSA peut être déployée en mode HA avec des nœuds de plan de contrôle répartis sur plusieurs zones de disponibilité, FSX ONTAP peut également être provisionné avec l'option multi-AZ qui assure la haute disponibilité et la protection contre les défaillances AZ.

> L'accès à un système de fichiers Amazon FSX à partir de la zone de disponibilité préférée (AZ) du système de fichiers ne comporte aucun frais de transfert de données. Pour plus d'informations sur les prix, reportez-vous à la section "ici".

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift

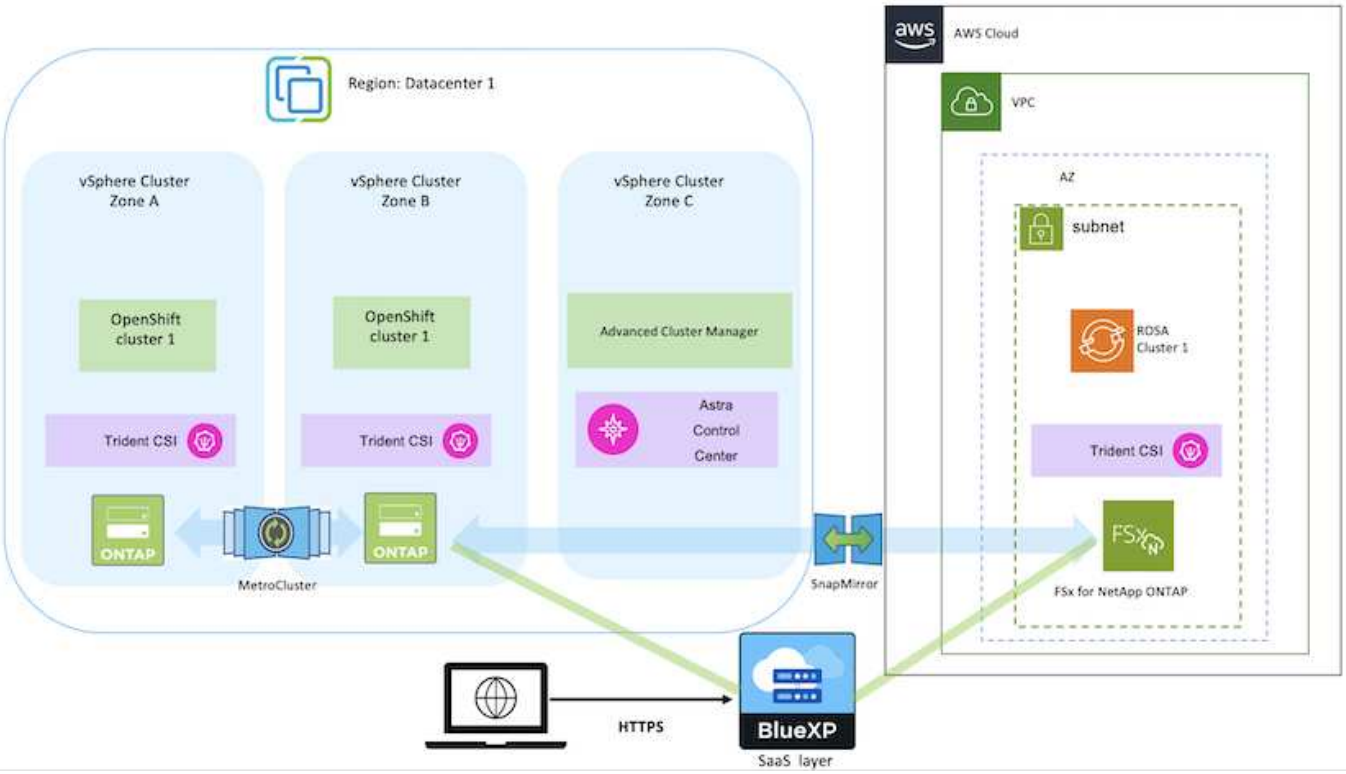


Déployez et configurez la plateforme de conteneurs Red Hat OpenShift gérée sur AWS

Cette section décrit un workflow général de configuration des clusters Red Hat OpenShift gérés sur AWS(ROSA). Il présente l'utilisation de FSX for NetApp ONTAP (FSxN) géré en tant que back-end de stockage par Astra Trident pour fournir des volumes persistants. Vous trouverez des informations détaillées sur le déploiement de FSxN sur AWS à l'aide

de BlueXP. Vous y trouverez également des informations détaillées sur l'utilisation de BlueXP et d'OpenShift GitOps (Argo CD) pour exécuter les activités de protection et de migration des données pour les applications avec état sur les clusters ROSA.

Voici un diagramme illustrant les clusters ROSA déployés sur AWS et utilisant FSxN comme stockage back-end.



Cette solution a été vérifiée en utilisant deux clusters ROSA dans deux VPC dans AWS. Chaque cluster ROSA a été intégré à FSxN à l'aide d'Astra Trident. IL existe plusieurs façons de déployer les clusters ROSA et FSxN dans AWS. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Le processus de configuration peut être divisé en plusieurs étapes :

Installer les clusters ROSA

- Créez deux VPC et configurez la connectivité de peering VPC entre les VPC.
- Reportez-vous à "ici" Pour obtenir des instructions sur l'installation des clusters ROSA.

Installez FSxN

- Installez FSxN sur les VPC de BlueXP. Reportez-vous à "ici" Pour créer un compte BlueXP et démarrer. Reportez-vous à "ici" Pour l'installation de FSxN. Reportez-vous à "ici" Pour créer un connecteur dans AWS pour gérer le FSxN.
- Déploiement de FSxN à l'aide d'AWS Reportez-vous à "ici" Déploiement via la console AWS

Installation de Trident sur les clusters ROSA (à l'aide du graphique Helm)

- Utilisez le tableau Helm pour installer Trident sur les clusters ROSA. url du graphique Helm : https://netapp.github.io/trident-helm-chart

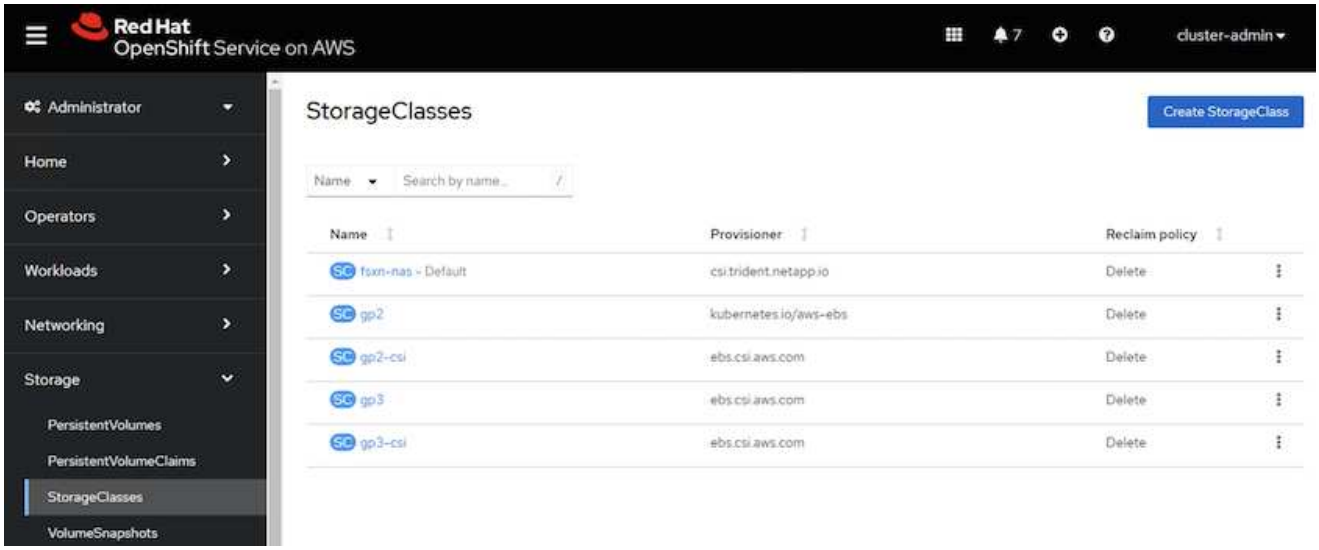
Intégration de FSxN avec Astra Trident pour les clusters ROSA

OpenShift GitOps peut être utilisé pour déployer Astra Trident CSI sur tous les clusters gérés lors de leur enregistrement sur ArgoCD à l'aide d'ApplicationSet.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Création de classes de stockage et de back-end à l'aide de Trident (pour FSxN)

- Reportez-vous à "ici" pour plus d'informations sur la création de systèmes back-end et de classes de stockage.
- Créez la classe de stockage créée pour FsxN avec Trident CSI par défaut depuis la console OpenShift. Voir la capture d'écran ci-dessous :



Déployer une application à l'aide d'OpenShift GitOps (Argo CD)

- Installez l'opérateur OpenShift GitOps sur le cluster. Reportez-vous aux instructions "ici".
- Configurez une nouvelle instance Argo CD pour le cluster. Reportez-vous aux instructions "ici".

Ouvrez la console du CD Argo et déployez une application. Par exemple, vous pouvez déployer une application Jenkins à l'aide du CD Argo avec Helm Chart. Lors de la création de l'application, les détails suivants ont été fournis : projet : cluster par défaut : https://kubernetes.default.svcEspace de noms : Jenkins l'url du graphique Helm : https://charts.bitnami.com/bitnami

Paramètres Helm : global.storageClass : fsxn-nas

Protection des données

Cette page présente les options de protection des données pour les clusters Red Hat OpenShift sur AWS (ROSA) gérés à l'aide d'Astra Control Service. ASTRA Control Service (ACS) est une interface utilisateur graphique simple d'utilisation qui vous permet d'ajouter des clusters, de définir des applications qui s'exécutent sur eux et d'effectuer des activités de gestion des données intégrant la cohérence applicative. Les fonctions ACS sont également accessibles via une API qui permet l'automatisation des flux de travail.

NetApp Astra Trident est le moteur d'Astra Control (ACS ou ACC). ASTRA Trident intègre plusieurs types de clusters Kubernetes tels que Red Hat OpenShift, EKS, AKS, SUSE Rancher, Anthos, etc. avec plusieurs versions de stockage NetApp ONTAP telles que FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files et Amazon FSX pour NetApp ONTAP.

Cette section fournit des détails sur les options de protection des données suivantes à l'aide d'ACS :

- Vidéo montrant la sauvegarde et la restauration d'une application ROSA s'exécutant dans une région et la restauration dans une autre région.
- Vidéo présentant Snapshot et la restauration d'une application ROSA.
- Détails détaillés de l'installation d'un cluster ROSA, Amazon FSX pour NetApp ONTAP, à l'aide d'NetApp Astra Trident pour l'intégration au back-end de stockage, installation d'une application postgresql sur un cluster ROSA, utilisation d'ACS pour créer un snapshot de l'application et restaurer son application.
- Un blog montrant les détails pas à pas de la création et de la restauration à partir d'un snapshot pour une application mysql sur un cluster ROSA avec FSX pour ONTAP à l'aide d'ACS.

Sauvegarde/Restauration à partir de la sauvegarde

La vidéo suivante montre la sauvegarde d'une application ROSA s'exécutant dans une région et la restauration dans une autre région.

FSX NetApp ONTAP pour Red Hat OpenShift Service sur AWS

Snapshot/Restaurer à partir d'un snapshot

La vidéo suivante montre la prise d'un instantané d'une application ROSA et la restauration à partir de l'instantané après.

Snapshot/Restore pour les applications sur les clusters Red Hat OpenShift Service sur AWS (ROSA) avec le stockage Amazon FSX pour NetApp ONTAP

Blog

- "Utilisation d'Astra Control Service pour la gestion des données des applications sur des clusters ROSA avec le stockage Amazon FSX"

Détails détaillés étape par étape pour créer un snapshot et le restaurer à partir de celui-ci

Configuration des prérequis

- "Compte AWS"
- "Compte Red Hat OpenShift"
- Utilisateur IAM avec "autorisations appropriées" Pour créer et accéder au cluster ROSA
- "CLI AWS"
- "CLI ROSA"
- "Interface de ligne de commande OpenShift"(oc)
- VPC avec sous-réseaux et passerelles et routes appropriées
- "ROSA Cluster installée" Dans le VPC
- "Amazon FSX pour NetApp ONTAP" Créées dans le même VPC
- Accès au cluster ROSA depuis "OpenShift Hybrid Cloud Console"

Étapes suivantes

1. Créer un utilisateur admin et se connecter au cluster

2. Créez un fichier kubeconfig pour le cluster.
3. Installer Astra Trident sur le cluster.
4. Créez une configuration back-end, une classe de stockage et une classe Snapshot à l'aide du mécanisme de provisionnement Trident CSI.
5. Déployer une application postgresql sur le cluster.
6. Créez une base de données et ajoutez un enregistrement.
7. Ajoutez le cluster dans ACS.
8. Définissez l'application dans ACS.
9. Créez un instantané à l'aide d'ACS.
10. Supprimez la base de données dans l'application postgresql.
11. Restauration à partir d'un snapshot à l'aide d'ACS.
12. Vérifiez que votre application a été restaurée à partir de l'instantané.

1. Créer un utilisateur admin et se connecter au cluster

Accédez au cluster ROSA en créant un utilisateur admin avec la commande suivante : (vous devez créer un utilisateur admin uniquement si vous n'en avez pas créé un au moment de l'installation)

```
rosa create admin --cluster=<cluster-name>
```

La commande fournit une sortie qui ressemble à ce qui suit. Connectez-vous au cluster à l'aide de `oc login` commande fournie dans la sortie.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

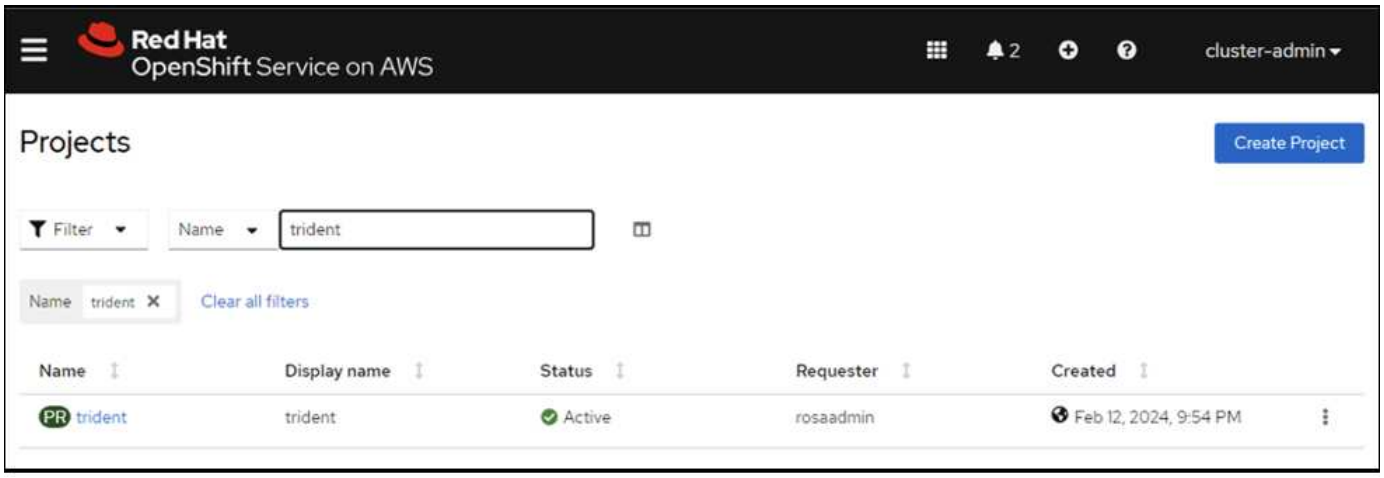
Vous pouvez également vous connecter au cluster à l'aide d'un jeton. Si vous avez déjà créé un administrateur au moment de la création du cluster, vous pouvez vous connecter au cluster depuis la console Red Hat OpenShift Hybrid Cloud à l'aide des informations d'identification de l'administrateur. Ensuite, en cliquant sur le coin supérieur droit où il affiche le nom de l'utilisateur connecté, vous pouvez obtenir le `oc login` commande (jeton de connexion) pour la ligne de commande.

2. Créez un fichier kubeconfig pour le cluster

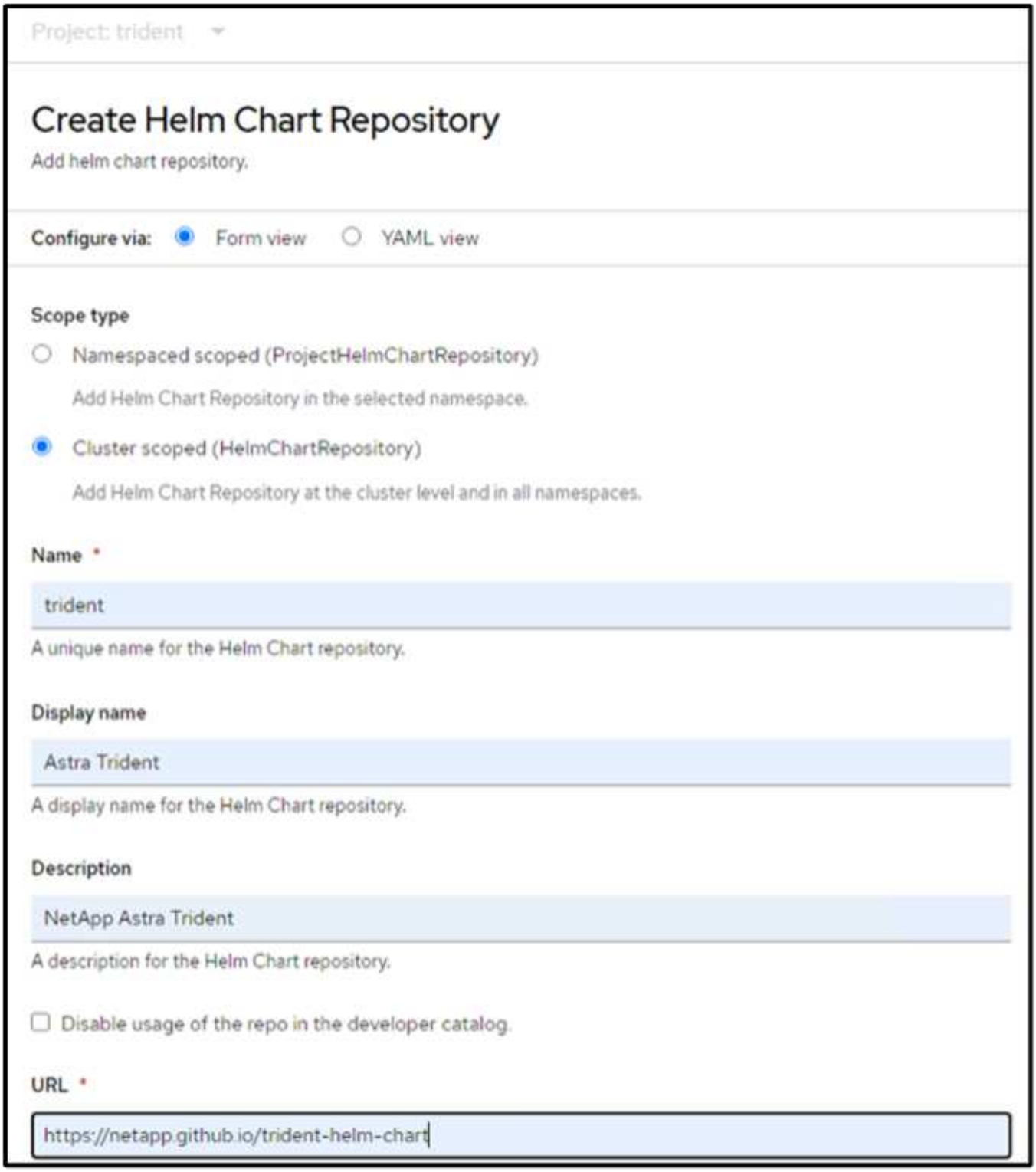
Suivre les procédures "ici" Pour créer un fichier kubeconfig pour le cluster ROSA. Ce fichier kubeconfig sera utilisé plus tard lorsque vous ajoutez le cluster dans ACS.

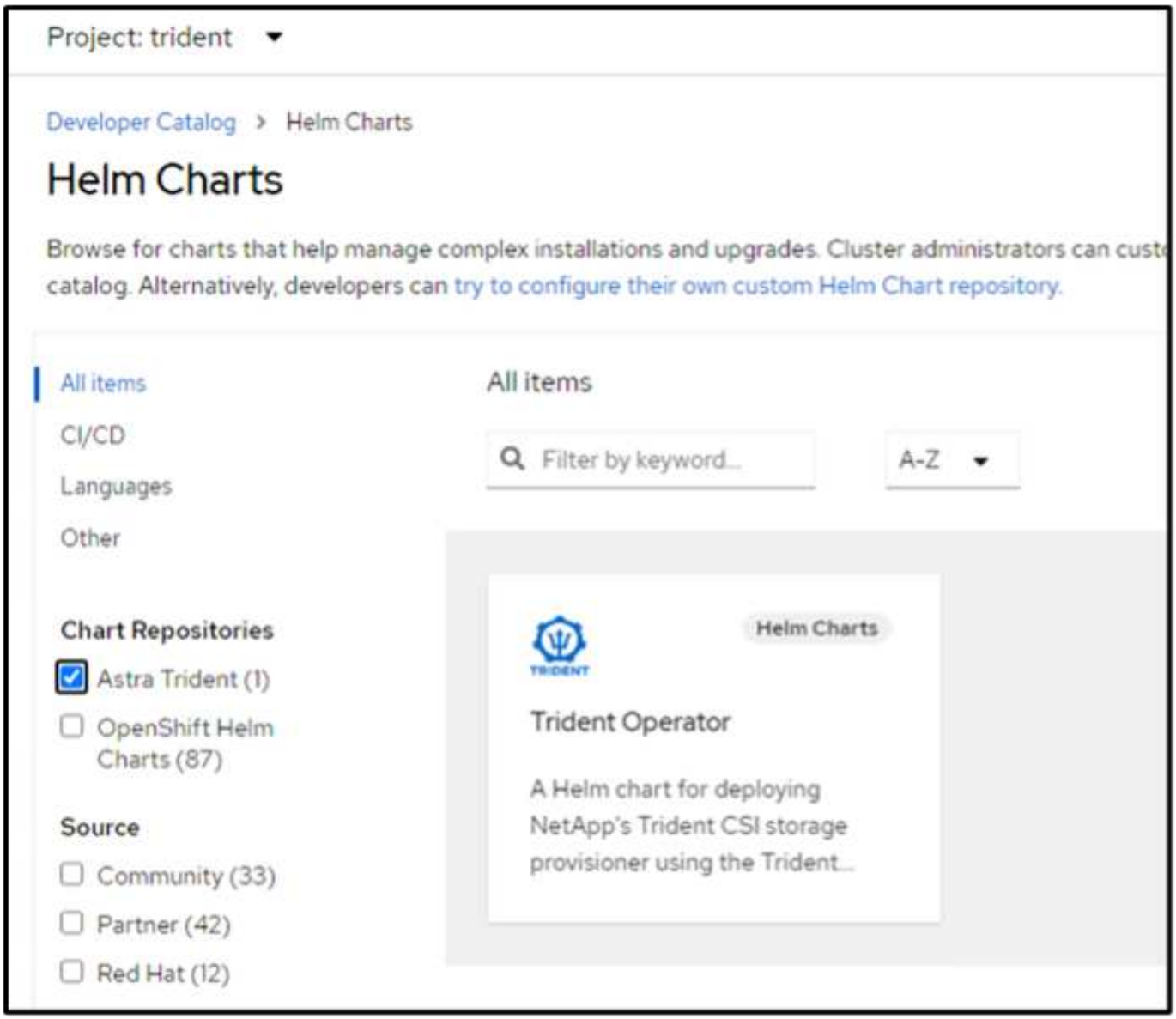
3. Installer Astra Trident sur le cluster

Installer Astra Trident (dernière version) sur le cluster ROSA. Pour ce faire, vous pouvez suivre l'une des procédures données "ici". Pour installer Trident à l'aide de Helm à partir de la console du cluster, commencez par créer un projet appelé Trident.

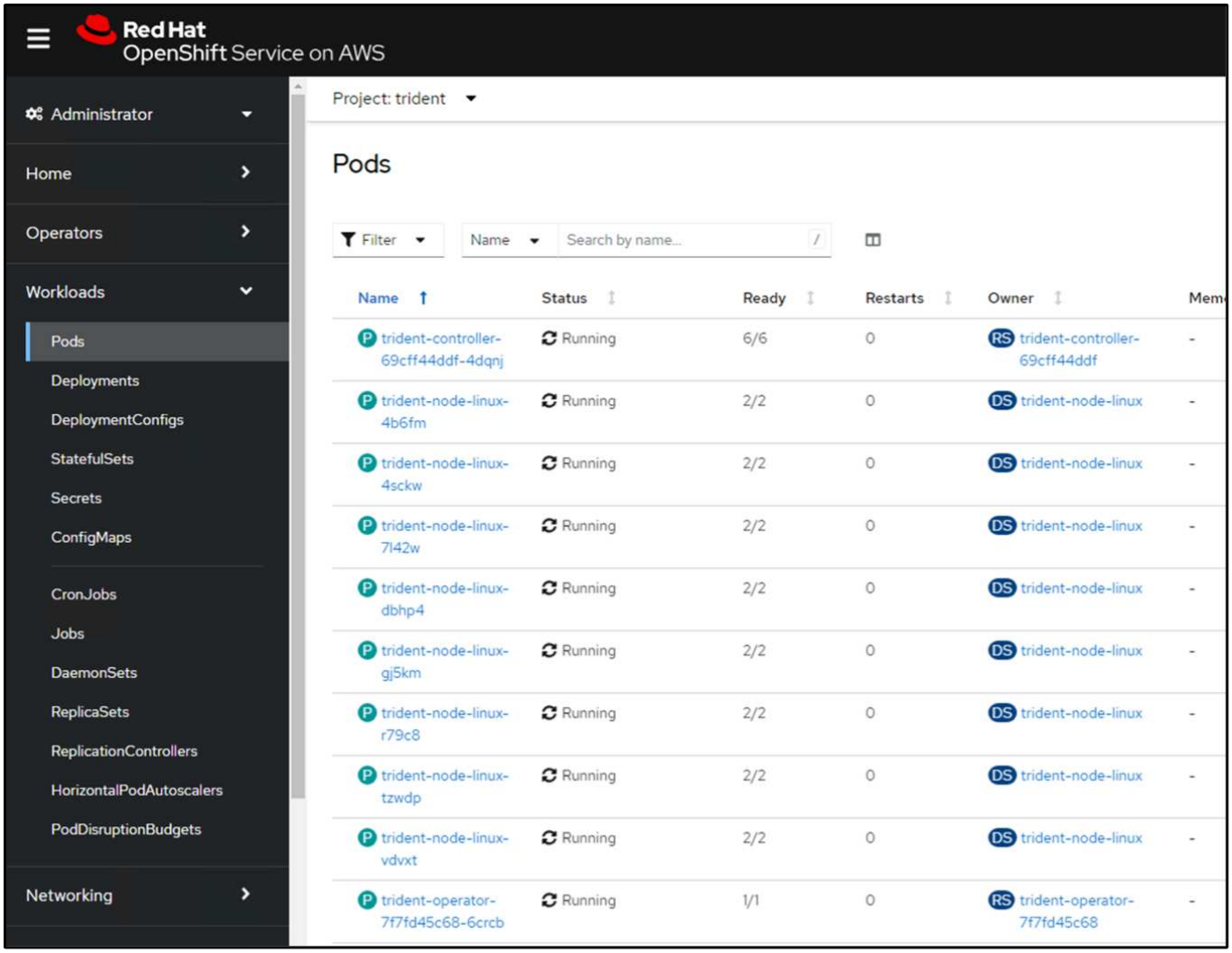


Ensuite, dans la vue Développeur, créez un référentiel de graphiques Helm. Pour le champ URL, utilisez `'https://netapp.github.io/trident-helm-chart'`. Créez ensuite une version de Helm pour l'opérateur Trident.


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



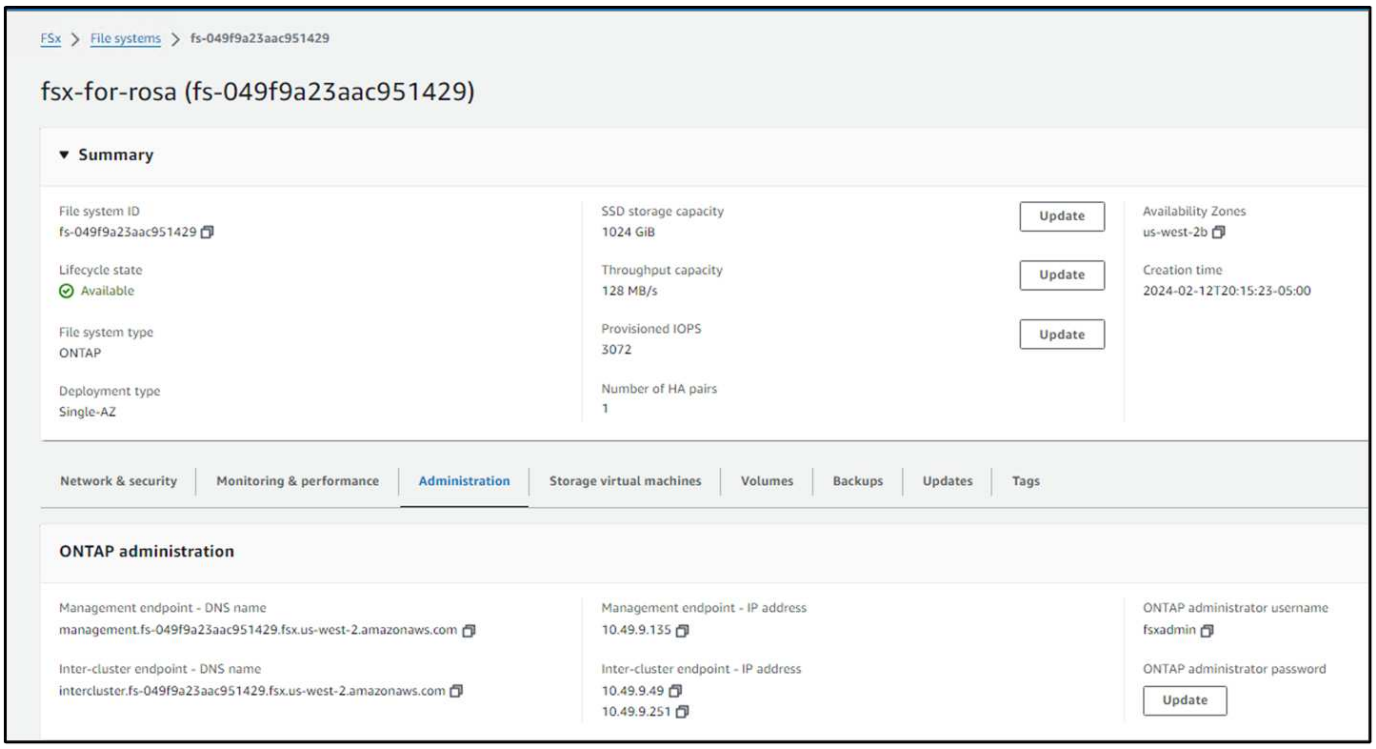
Vérifiez que tous les pods trident sont en cours d'exécution en revenant à la vue de l'administrateur de la console et en sélectionnant les pods dans le projet trident.



4. Créez une configuration backend, de classe de stockage et de classe de snapshots à l'aide du mécanisme de provisionnement Trident CSI

Utilisez les fichiers yaml illustrés ci-dessous pour créer un objet back-end trident, un objet classe de stockage et l'objet Volumesnapshot. Assurez-vous de fournir les informations d'identification de votre système de fichiers Amazon FSX for NetApp ONTAP que vous avez créé, la LIF de gestion et le nom de vServer de votre système de fichiers dans la configuration yaml pour le back-end. Pour obtenir ces informations, accédez à la console AWS pour Amazon FSX et sélectionnez le système de fichiers, accédez à l'onglet Administration. Cliquez également sur mettre à jour pour définir le mot de passe du `fsxadmin` utilisateur.

Vous pouvez utiliser la ligne de commande pour créer les objets ou les créer avec les fichiers yaml à partir de la console de cloud hybride.



Configuration back-end Trident

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Classe de stockage

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

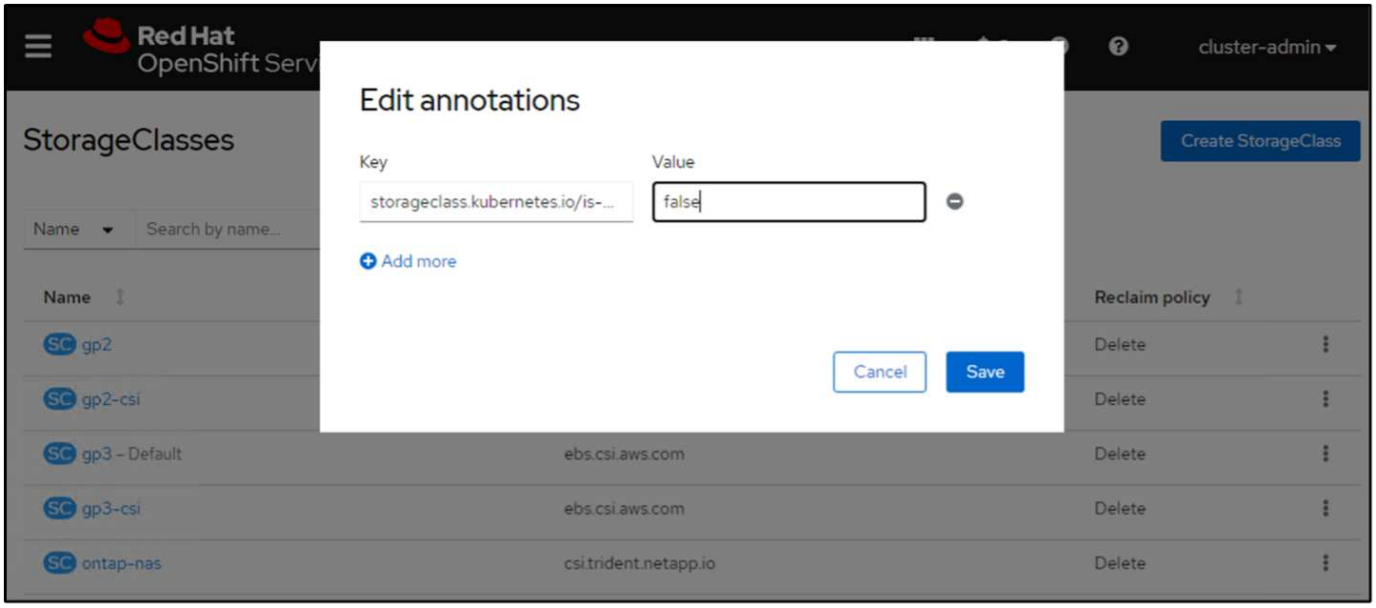
classe d'instantanés

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Vérifiez que le backend, la classe de stockage et les objets trident-snapshotclass sont créés à l'aide des commandes indiquées ci-dessous.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

Vous devez à présent modifier de façon importante : définir ontap-nas comme classe de stockage par défaut au lieu de gp3 de sorte que l'application postgresql que vous déployez ultérieurement puisse utiliser la classe de stockage par défaut. Dans la console OpenShift de votre cluster, sous stockage, sélectionnez classes de stockage. Editez l'annotation de la classe par défaut actuelle à false et ajoutez l'annotation storageclass.kubernetes.io/is-default-class set à true pour la classe de stockage ontap-nas.



5. Déployer une application postgresql sur le cluster

Vous pouvez déployer l'application à partir de la ligne de commande comme suit :

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Si vous ne voyez pas les modules d'application s'exécuter, une erreur peut survenir en raison de contraintes de contexte de sécurité.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql      ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl   ClusterIP   None            <none>        5432/TCP   12m

NAME                              READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Corrigez l'erreur en modifiant le `runAsUser` et `fsGroup` champs dans `statefuleset.apps/postgresql` objet avec l'uid qui se trouve dans la sortie du `oc get project` comme indiqué ci-dessous.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

L'application postgresql doit être en cours d'exécution et utiliser des volumes persistants pris en charge par le stockage Amazon FSX pour NetApp ONTAP.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

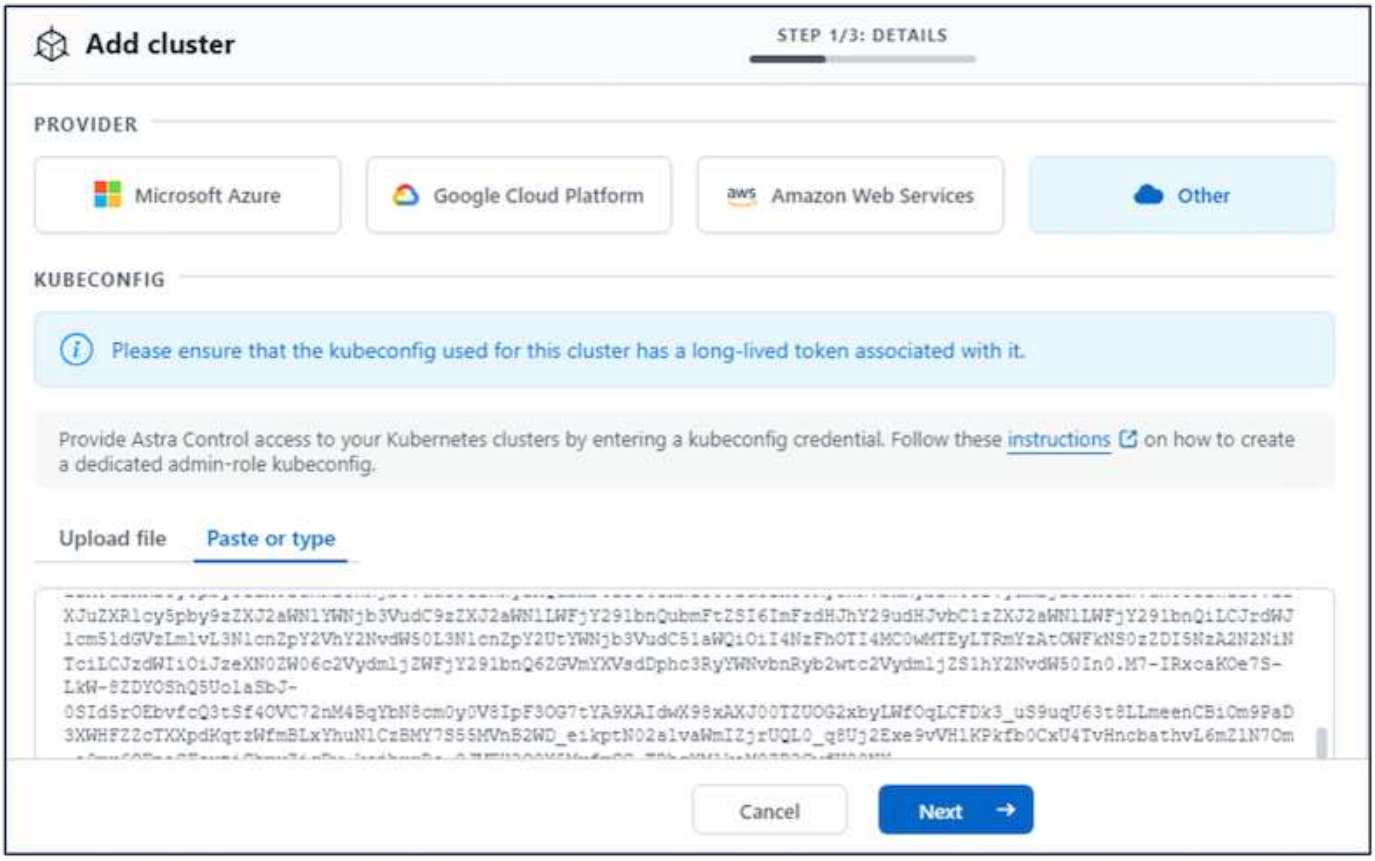
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME               STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0  Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. Créer une base de données et ajouter un enregistrement

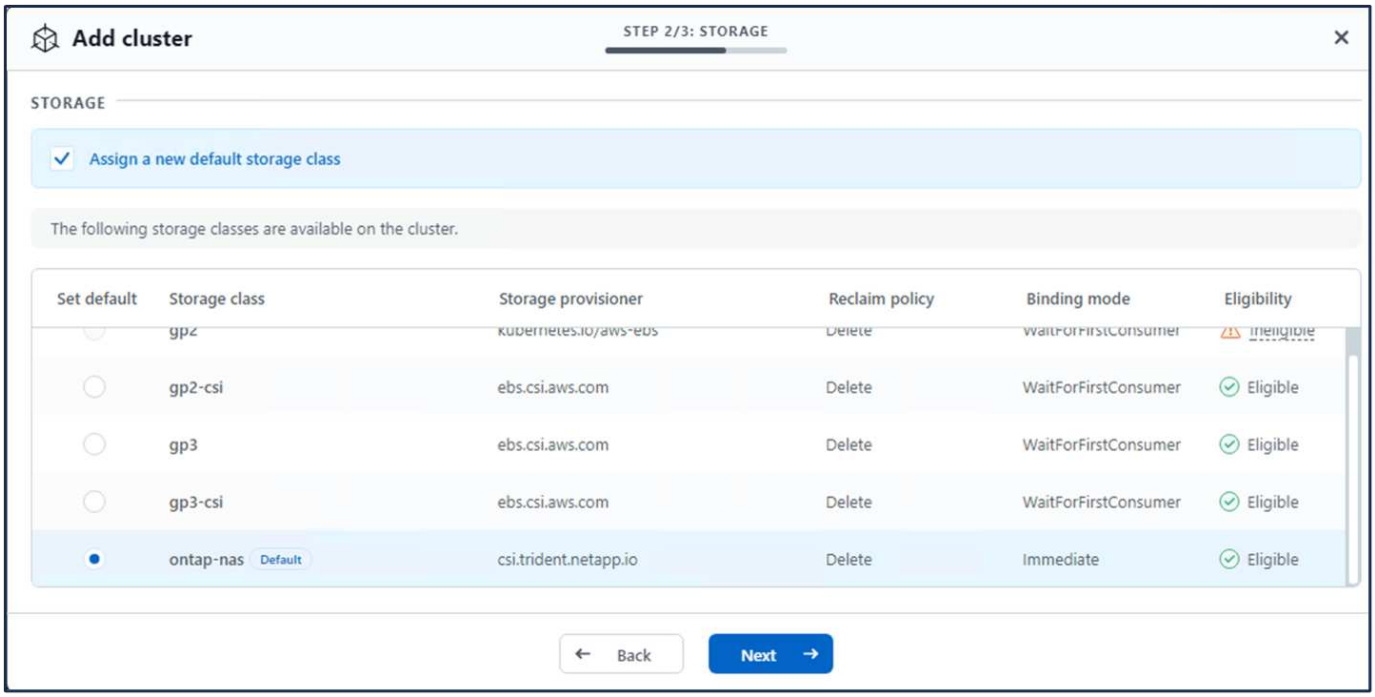
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. Ajouter le cluster dans ACS

Connectez-vous à ACS. Sélectionnez cluster et cliquez sur Ajouter. Sélectionnez autre et téléchargez ou collez le fichier kubecconfig.



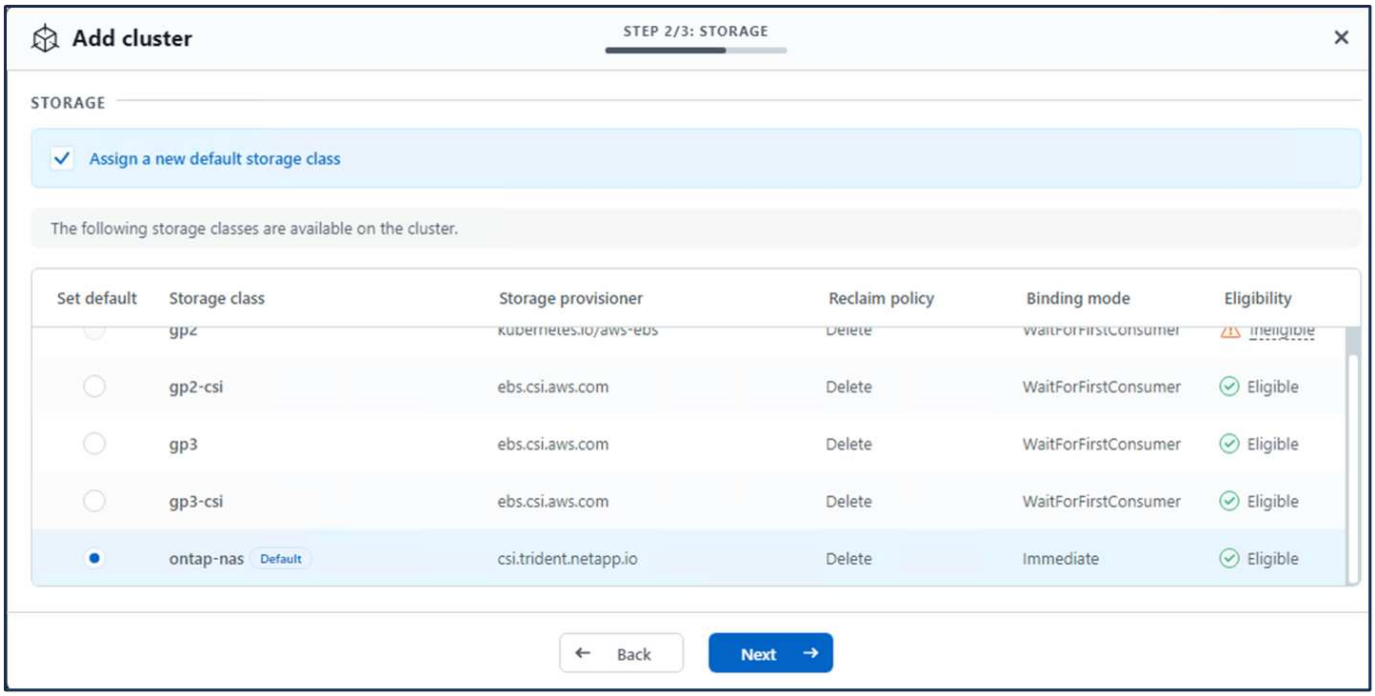
Cliquez sur **Suivant** et sélectionnez ontap-nas comme classe de stockage par défaut pour ACS. Cliquez sur **Suivant**, consultez les détails et **Ajouter** le cluster.



8. Définir l'application dans ACS

Définissez l'application postgresql dans ACS. Sur la page d'accueil, sélectionnez **applications**, **définir** et entrez les détails appropriés. Cliquez sur **Suivant** à plusieurs reprises, passez en revue les détails et cliquez

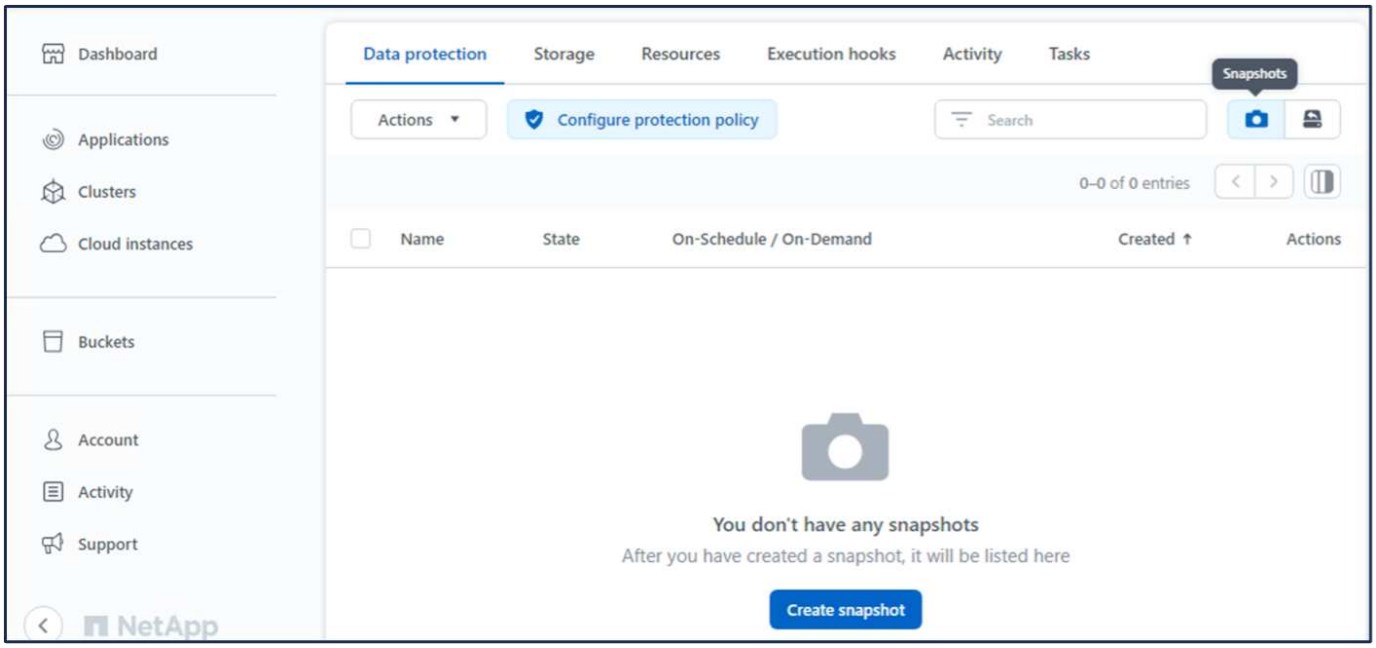
sur **définir**. L'application est ajoutée à ACS.

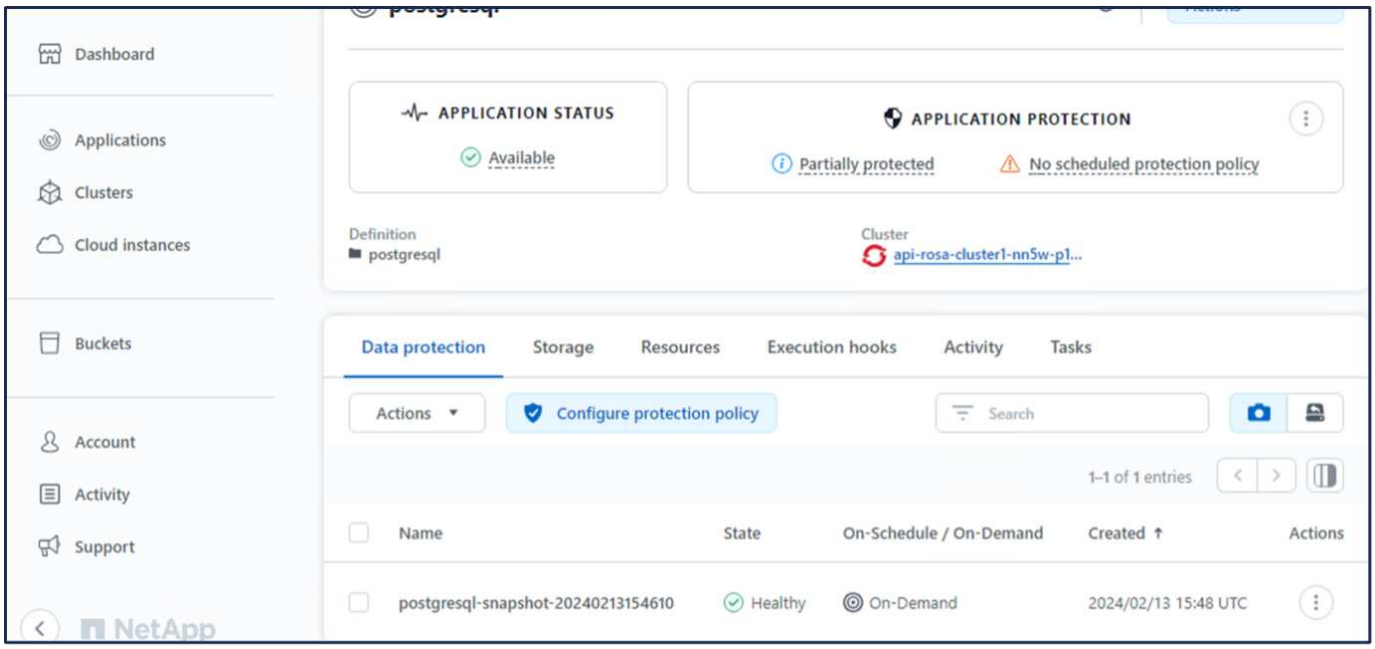


9. Créez un instantané à l'aide d'ACS

Il existe de nombreuses façons de créer un instantané dans ACS. Vous pouvez sélectionner l'application et créer un instantané à partir de la page qui affiche les détails de l'application. Vous pouvez cliquer sur Create snapshot pour créer un snapshot à la demande ou configurer une règle de protection.

Créez un instantané à la demande en cliquant simplement sur **Créer un instantané**, en fournissant un nom, en examinant les détails et en cliquant sur **instantané**. L'état de l'instantané passe à sain une fois l'opération terminée.





10. Supprimez la base de données dans l'application postgresql

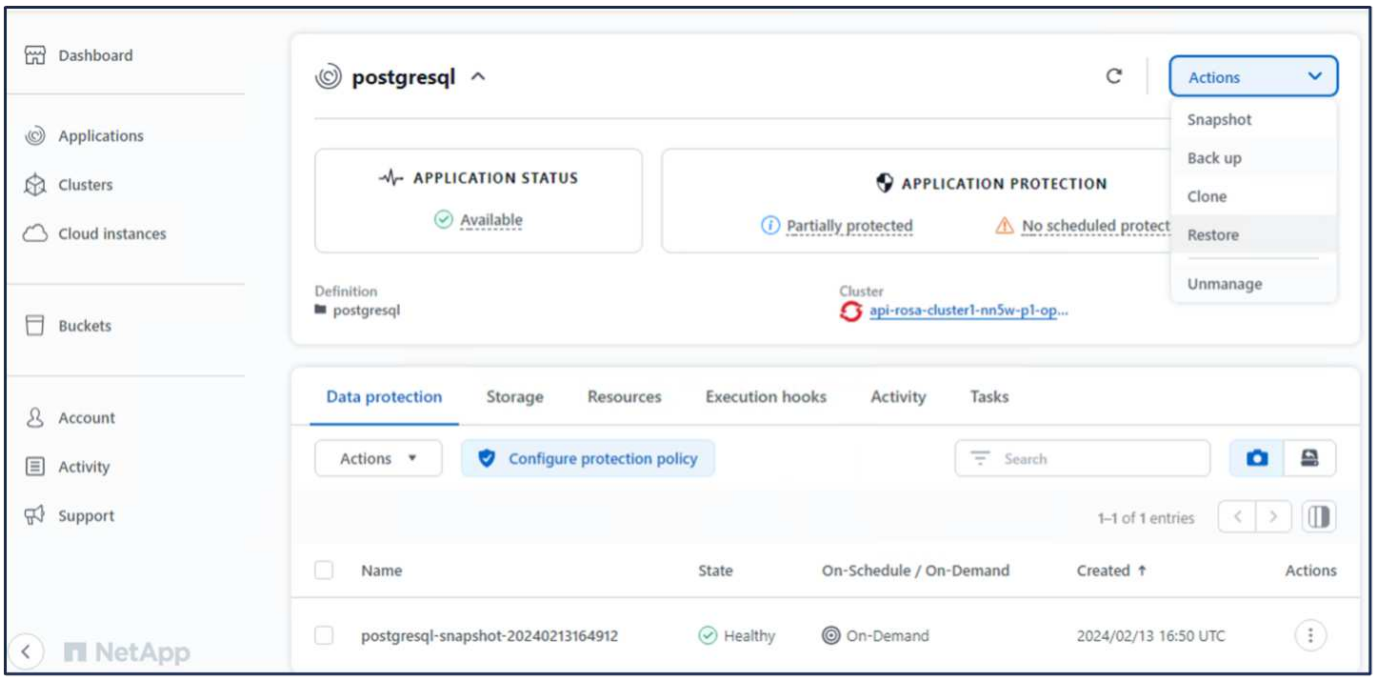
Reconnectez-vous à postgresql, répertoriez les bases de données disponibles, supprimez celle que vous avez créée précédemment et répertoriez à nouveau pour vous assurer que la base de données a été supprimée.

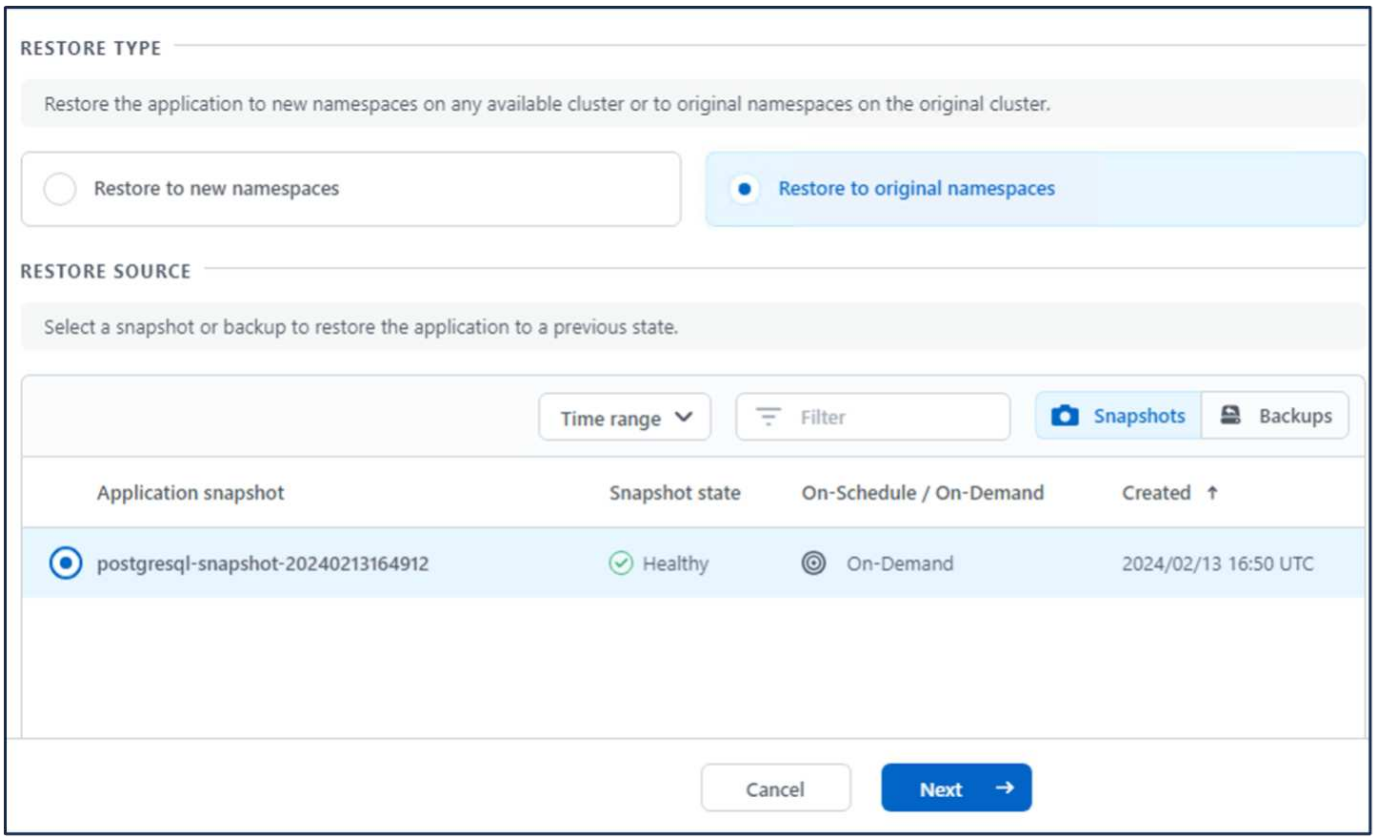
```
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

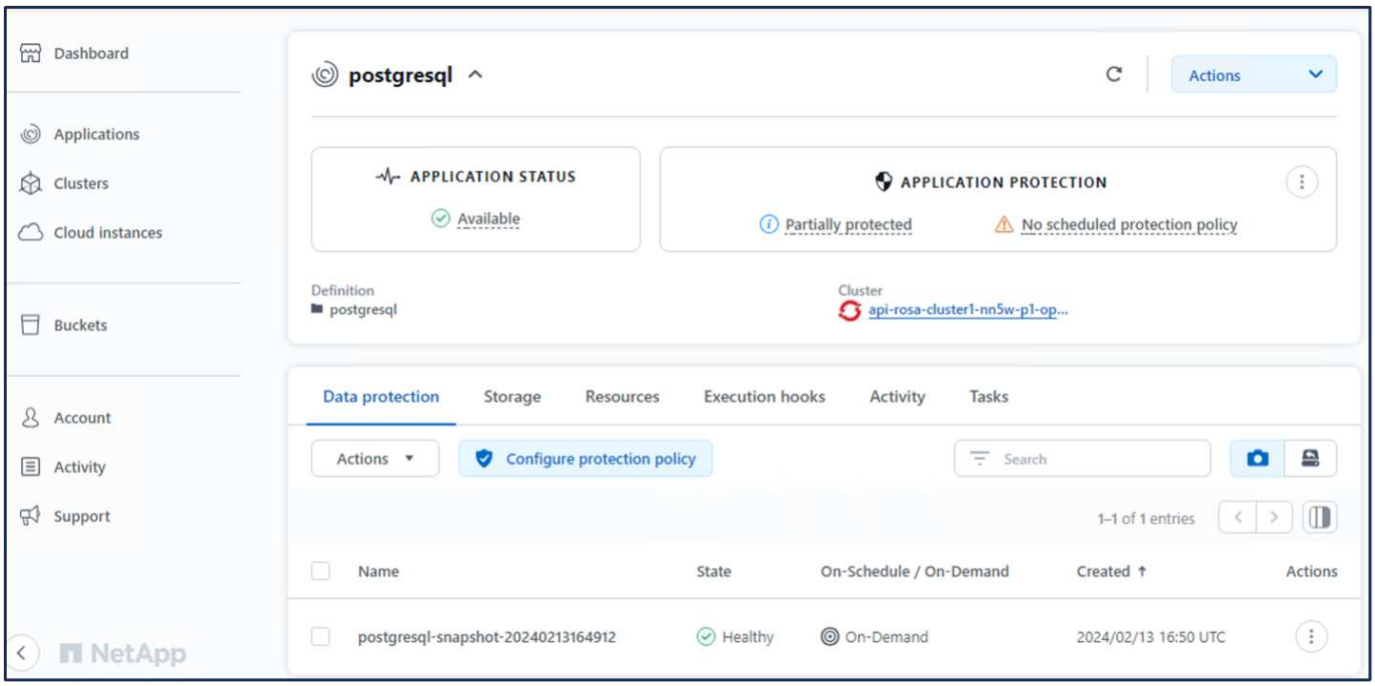
11. Restauration à partir d'un instantané à l'aide d'ACS

Pour restaurer l'application à partir d'un instantané, accédez à la page d'accueil de l'interface utilisateur ACS,

sélectionnez l'application et sélectionnez Restaurer. Vous devez choisir un snapshot ou une sauvegarde à partir de laquelle effectuer la restauration. (En général, plusieurs d'entre elles sont créées en fonction d'une règle que vous avez configurée). Faites les choix appropriés dans les deux écrans suivants, puis cliquez sur **Restaurer**. L'état de l'application passe de la restauration à disponible après sa restauration à partir de l'instantané.







12. Vérifiez que votre application a été restaurée à partir de l'instantané

Connectez-vous au client postgresql et vous devriez maintenant voir la table et l'enregistrement dans la table que vous aviez précédemment. C'est tout. En cliquant simplement sur un bouton, votre application a été restaurée à un état antérieur. C'est à ce niveau de simplicité que nous proposons à nos clients avec Astra Control.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
          List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


Migration des données

Cette page présente les options de migration des données pour les workloads de conteneurs dans des clusters Red Hat OpenShift gérés à l'aide de FSX pour NetApp ONTAP pour le stockage persistant.

Migration des données

Les services Red Hat OpenShift sur AWS et FSX pour NetApp ONTAP (FSxN) font partie de leur portefeuille de services par AWS. FSxN est disponible avec les options Single AZ ou Multi-AZ. L'option Multi-Az assure la protection des données contre les défaillances de zone de disponibilité. FSxN peut être intégré à Astra Trident pour fournir un stockage persistant aux applications sur les clusters ROSA.

Intégration de FSxN avec Trident à l'aide de Helm Chart

Intégration de clusters ROSA avec Amazon FSX for ONTAP

La migration des applications de conteneurs implique :

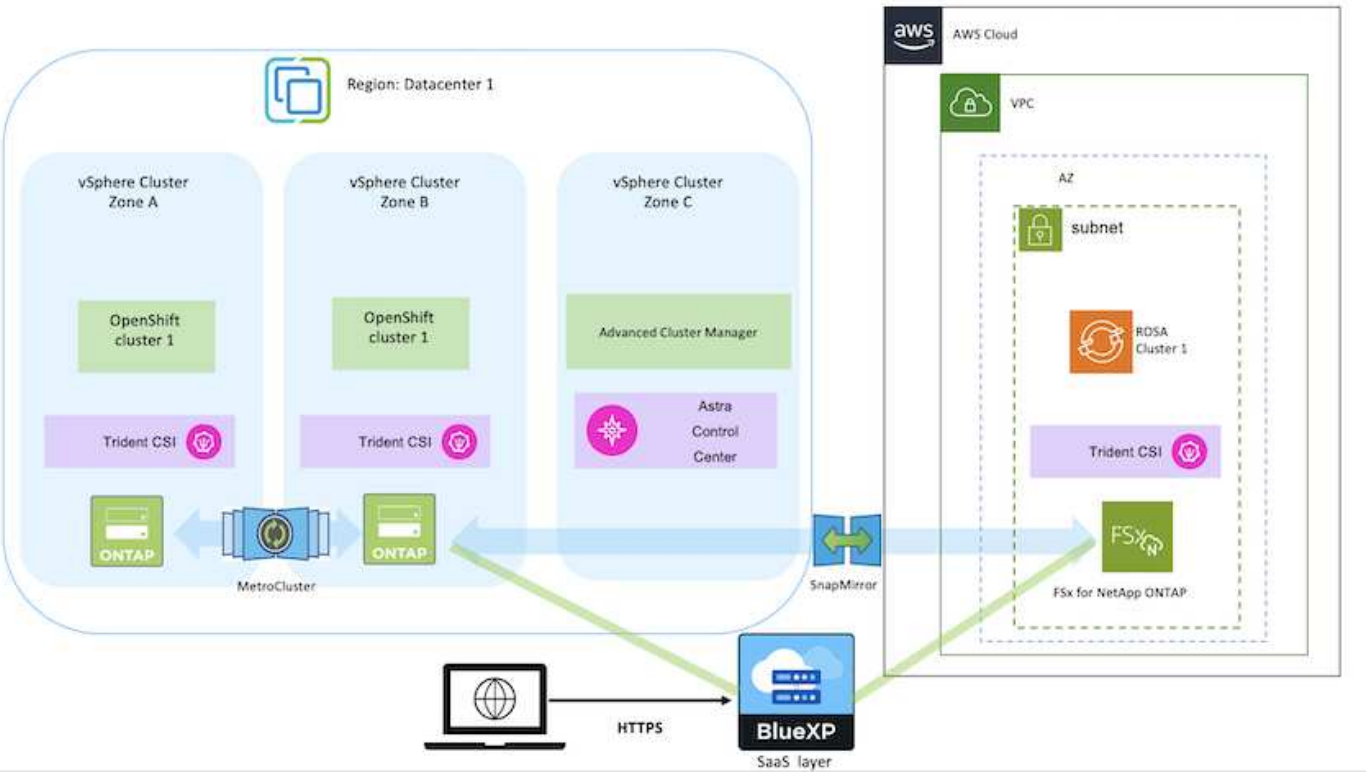
- Volumes persistants : cette opération peut être effectuée à l'aide de BlueXP. Une autre option consiste à utiliser Astra Control Center pour gérer les migrations d'applications de conteneurs d'un environnement sur site vers le cloud. L'automatisation peut être utilisée dans le même but.
- Métadonnées des applications : cette opération peut être réalisée à l'aide d'OpenShift GitOps (Argo CD).

Basculement et retour arrière des applications sur un cluster ROSA à l'aide de FSxN pour le stockage persistant

La vidéo suivante présente des scénarios de basculement et de retour arrière d'applications à l'aide de BlueXP et d'Argo CD.

Basculement et retour arrière des applications sur le cluster ROSA

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift



Informations sur le copyright

Informations sur les marques commerciales