Solutions de cloud public et hybride NetApp

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

Sommaire

Solutions de cloud public et hybride NetApp . . . 1
Nouveautés des solutions de cloud public et hybride NetApp . . . 2
NetApp Hybrid Multicloud avec solutions VMware . . . 3
VMware pour le cloud public . . . 3
Présentation de NetApp Hybrid Multicloud avec VMware . . . 3
Solutions NetApp pour VMware dans les hyperscalers . . . 7
Configurations prises en charge pour NetApp Hybrid Multicloud avec VMware . . . 10
VMware dans la configuration des hyperscalers . . . 10
Stockage NetApp dans les clouds publics . . . 35
Résumé et conclusion : Pourquoi choisir NetApp Hybrid Multicloud avec VMware ? . . . 136
Cas d'utilisation du cloud hybride VMware . . . 138
Cas d'utilisation de NetApp Hybrid Multicloud avec VMware . . . 138
Solutions NetApp pour VMware dans les hyperscalers . . . 139
Solutions NetApp pour Amazon VMware Managed Cloud (VMC) . . . 140
Solutions NetApp pour Azure VMware Solution (AVS) . . . 140
Solutions NetApp pour Google Cloud VMware Engine (GCVE) . . . 141
NetApp pour AWS/VMC . . . 141
Fonctionnalités NetApp pour AWS VMC . . . 141
Protégez les charges de travail sur AWS/VMC . . . 143
Migrer les charges de travail sur AWS/VMC . . . 261
NetApp pour AWS / EVS . . . 276
Monter FSx ONTAP comme banque de données externe pour EVS . . . 276
Protéger le datastore FSx ONTAP pour EVS . . . 300
NetApp pour Azure / AVS . . . 333
Fonctionnalités NetApp pour Azure AVS . . . 334
Protéger les charges de travail sur Azure / AVS . . . 335
Migrer les charges de travail sur Azure/AVS . . . 404
NetApp pour GCP/GCVE . . . 419
Fonctionnalités NetApp pour Google Cloud Platform GCVE . . . 419
Protéger les charges de travail sur GCP/GCVE . . . 420
Migrer les charges de travail sur GCP/GCVE . . . 452
Sécurisez vos données avec Google Cloud NetApp Volumes dans Google Cloud . . . 469
NetApp Disaster Recovery . . . 541
Protection des données 3-2-1 pour VMware avec SnapCenter Plug-in et NetApp Backup and Recovery pour protéger les charges de travail VMware . . . 541
NetApp Disaster Recovery . . . 577
Charges de travail de conteneurs multicloud hybride NetApp avec Red Hat OpenShift . . . 619
Commencer . . . 619
Solutions multicloud hybrides NetApp pour les charges de travail des conteneurs Red Hat OpenShift . . . 619
Propositions de valeur des solutions NetApp Hybrid Multicloud pour les charges de travail Red Hat OpenShift Container . . . 621
Solutions prises en charge par NetApp Hybrid Multicloud pour les charges de travail Red Hat OpenShift Container . . . 622

Versions des différents composants utilisés dans la validation de la solution . . . 626
Intégrations de stockage NetApp prises en charge avec les conteneurs Red Hat OpenShift . . . 627
Documentation supplémentaire . . . 631
Openshift pour sur site . . . 631
Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift sur VMware . . . 631
Déployer et configurer la plateforme Red Hat OpenShift Container sur VMware . . . 632
Protection des données avec Trident Protect . . . 634
Cloud hybride avec composants autogérés . . . 635
Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift dans le cloud hybride . . . 635
Déployer et configurer la plateforme Red Hat OpenShift Container sur AWS . . . 637
Déployer et configurer la plateforme de conteneurs Red Hat OpenShift sur Google Cloud . . . 639
Déployer et configurer la plateforme Red Hat OpenShift Container sur Azure . . . 641
Protection des données avec Trident Protect . . . 644
Cloud hybride avec composants gérés par le fournisseur . . . 644
Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift gérées . . . 645
Déployer et configurer la plateforme Managed Red Hat OpenShift Container sur AWS . . . 645
Déployer et configurer OpenShift Dedicated sur Google Cloud avec Google Cloud NetApp Volumes . . . 648
Protection des données . . . 650
Solutions NetApp Hybrid Multicloud supplémentaires pour les charges de travail Red Hat OpenShift . . . 650
Protégez vos données avec Trident Protect . . . 650
Protection des données pour les applications conteneurisées dans la plateforme OpenShift Container à l'aide de Trident Protect . . . 650
Protégez les machines virtuelles dans Red Hat OpenShift Virtualization à l'aide de Trident Protect . . . 662
Protégez les applications conteneurisées à l'aide d'outils tiers . . . 682
Protection des données pour les applications conteneurisées dans OpenShift Container Platform à l'aide de l'API OpenShift pour la protection des données (OADP) . . . 682
Installation de l'opérateur OpenShift API for Data Protection (OADP) . . . 684
Création d'une sauvegarde à la demande pour les applications dans OpenShift Container Platform . . . 693
Migrer une application d'un cluster à un autre . . . 696
Restaurer une application à partir d'une sauvegarde . . . 700
Suppression des sauvegardes et des restaurations lors de l'utilisation de Velero . . . 707
Regardez des vidéos et des démonstrations sur les solutions multicloud hybrides avec NetApp . . . 709
Regardez des vidéos sur les solutions multicloud hybrides pour Amazon Web Services avec NetApp . . . 709
Stockage connecté aux invités . . . 709
TCO et magasins de données supplémentaires . . . 709
Flux de travail de migration (HCX) . . . 709
Regardez des vidéos sur les solutions multicloud hybrides pour Azure VMware Cloud avec NetApp . . . 709
Magasins de données supplémentaires . . . 709
Reprise après sinistre . . . 709
Flux de travail de migration (HCX) . . . 710
Regardez des vidéos sur les solutions multicloud hybrides pour Red Hat OpenShift avec NetApp . . . 710
Instantanés et restauration . . . 710
Intégration du stockage . . . 710

Basculement et restauration automatique . . . 710
Automatisation des solutions . . . 710
Lisez les blogs sur les solutions cloud des experts NetApp . . . 711
Intégration de VMware avec AWS et Amazon FSx pour ONTAP . . . 711
Solution Azure VMware . . . 711
Moteur VMware de Google Cloud . . . 711
Protection et gestion des données . . . 711
Charges de travail de conteneurs NetApp pour OpenShift . . . 711
VMware Sovereign Cloud . . . 711
Mentions légales . . . 712
Copyright . . . 712
Marques de commerce . . . 712
Brevets . . . 712
Politique de confidentialité . . . 712

Solutions de cloud public et hybride NetApp

Nouveautés des solutions de cloud public et hybride NetApp

Découvrez les nouveautés en matière de solutions de cloud public et hybride.

[[18-august-2025]]
== 18 août 2025

Le site NetApp Solutions est désormais le"Famille de solutions NetApp" , qui comprend les sites suivants :

- "Solutions d'intelligence artificielle NetApp"
- "Solutions de conteneurs NetApp"
- "Solutions de gestion de données NetApp"
- "Solutions de base de données NetApp"
- Solutions de cloud public et hybride NetApp
- "Solutions NetApp pour SAP"
- "Solutions de virtualisation NetApp"

NetApp Hybrid Multicloud avec solutions VMware

VMware pour le cloud public

Présentation de NetApp Hybrid Multicloud avec VMware

La plupart des organisations informatiques adoptent l'approche du cloud hybride en premier. Ces organisations sont en phase de transformation et les clients évaluent leur paysage informatique actuel, puis migrent leurs charges de travail vers le cloud en fonction de l'exercice d'évaluation et de découverte.

Les facteurs qui poussent les clients à migrer vers le cloud peuvent inclure l'élasticité et l'explosion, la sortie du centre de données, la consolidation du centre de données, les scénarios de fin de vie, les fusions, les acquisitions, etc. La raison de cette migration peut varier en fonction de chaque organisation et de ses priorités commerciales respectives. Lors du passage au cloud hybride, le choix du stockage approprié dans le cloud est très important afin de libérer la puissance du déploiement et de l'élasticité du cloud.

Options VMware Cloud dans le cloud public

Cette section décrit comment chacun des fournisseurs de cloud prend en charge une pile VMware Software Defined Data Center (SDDC) et/ou VMware Cloud Foundation (VCF) au sein de leurs offres de cloud public respectives.

Solution Azure VMware

Azure VMware Solution est un service cloud hybride qui permet des SDDC VMware entièrement fonctionnels au sein du cloud public Microsoft Azure. Azure VMware Solution est une solution propriétaire entièrement gérée et prise en charge par Microsoft, vérifiée par VMware s'appuyant sur l'infrastructure Azure. Cela signifie que lorsque Azure VMware Solution est déployé, les clients bénéficient de l'ESXi de VMware pour la virtualisation du calcul, de vSAN pour le stockage hyperconvergé et de NSX pour la mise en réseau et la sécurité, tout en profitant de la présence mondiale de Microsoft Azure, des installations de centre de données de pointe et de la proximité du riche écosystème de services et de solutions Azure natifs.

VMware Cloud sur AWS

VMware Cloud sur AWS apporte le logiciel SDDC de classe entreprise de VMware au cloud AWS avec un accès optimisé aux services AWS natifs. Propulsé par VMware Cloud Foundation, VMware Cloud sur AWS intègre les produits de virtualisation de calcul, de stockage et de réseau de VMware (VMware vSphere, VMware vSAN et VMware NSX) ainsi que la gestion de VMware vCenter Server, optimisée pour fonctionner sur une infrastructure AWS dédiée, élastique et bare-metal.

Moteur VMware de Google Cloud

Google Cloud VMware Engine est une offre IaaS (Infrastructure as a Service) basée sur l'infrastructure évolutive et performante de Google Cloud et la pile VMware Cloud Foundation (VMware vSphere, vCenter, vSAN et NSX-T). Ce service permet une transition rapide vers le cloud, en migrant ou en étendant de manière transparente les charges de travail VMware existantes depuis les environnements sur site vers Google Cloud Platform, sans les coûts, les efforts ni les risques liés à la réarchitecture des applications ou à la refonte des opérations. Il s'agit d'un service vendu et supporté par Google, en étroite collaboration avec VMware.

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

Saviez-vous?

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

- Hôtes VMware ESXi pour la virtualisation du calcul avec une appliance vCenter Server pour la gestion
- Stockage hyperconvergé VMware vSAN intégrant 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 pour la gestion

Configuration de stockage

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

En s'intégrant à NetApp Cloud Volumes, tels qu'Azure Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponible dans les trois principaux hyperscalers) et Google Cloud NetApp Volumes pour Google Cloud, les clients ont désormais la possibilité de mettre à l'échelle leur stockage de manière indépendante et d'ajouter uniquement des nœuds de calcul au cluster SDDC selon les besoins.

Remarques :

- VMware ne recommande pas les configurations de cluster déséquilibrées. Par conséquent, l'extension du stockage implique l'ajout de plus 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 en concurrence directe avec les charges de travail de production.
- Il n'existe aucune option permettant de fournir plusieurs niveaux de performances pour aligner les exigences, les performances et les coûts des applications.
- Il est très facile d'atteindre les limites de capacité de stockage du vSAN construit sur les hôtes du cluster. Utilisez NetApp Cloud Volumes pour mettre à l'échelle le stockage afin d'héberger des ensembles de données actifs ou de hiérarchiser les données les plus froides vers un stockage persistant.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponible dans les trois principaux hyperscalers) et Google Cloud NetApp Volumes pour Google Cloud peuvent être utilisés conjointement avec des machines virtuelles invitées. Cette architecture de stockage hybride se compose d'une banque de données vSAN qui contient les données binaires du système d'exploitation invité et de l'application. Les données d'application sont attachées à la machine virtuelle via un initiateur iSCSI basé sur un invité ou les montages NFS/SMB qui communiquent directement avec Amazon FSx ONTAP, Cloud Volume ONTAP, Azure NetApp Files et Google Cloud NetApp Volumes pour Google Cloud respectivement. Cette configuration vous permet de surmonter facilement les défis liés à la capacité de stockage, car avec vSAN, l'espace libre disponible dépend de l'espace libre et des politiques de stockage utilisées.

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

- La capacité brute totale d'un SDDC à trois nœuds = 31,1 To (environ 10 To pour chaque nœud).
- L'espace libre à maintenir avant l'ajout d'hôtes supplémentaires = 25 % = (0,25 x 31,1 To) = 7,7 To.
- La capacité brute utilisable après déduction de l'espace libre = 23,4 To

- L'espace libre effectif disponible dépend de la politique 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 comme stockage connecté aux invités contribuerait à étendre le stockage et à optimiser le coût total de possession tout en répondant aux exigences de performances et de protection des données.



Le stockage interne était la seule option disponible au moment de la rédaction de ce document.

Points à retenir

- Dans les modèles de stockage hybrides, placez les charges de travail de niveau 1 ou de haute priorité sur la banque de données vSAN pour répondre à toutes les exigences de latence spécifiques, car elles font partie de l'hôte lui-même et se trouvent à proximité. Utilisez des mécanismes intégrés pour toutes les machines virtuelles de charge de travail pour lesquelles les latences transactionnelles sont acceptables.
- Utilisez la technologie NetApp SnapMirror pour répliquer les données de workload du système ONTAP sur site vers Cloud Volumes ONTAP ou Amazon FSx ONTAP afin de faciliter la migration à l'aide de mécanismes au niveau des blocs. Cela ne s'applique pas à Azure NetApp Files ni à Google Cloud NetApp Volumes. Pour migrer des données vers Azure NetApp Files ou Google Cloud NetApp Volumes, utilisez NetApp XCP, NetApp Copy and Sync, rysnc ou robocopy selon le protocole de fichiers utilisé.
- Les tests montrent une latence supplémentaire de 2 à 4 ms lors de l'accès au stockage à partir des SDDC respectifs. Tenez compte de cette latence supplémentaire dans les exigences de l'application lors du mappage du stockage.
- Pour monter le stockage connecté à l'invité pendant le basculement de 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 de registre Microsoft Multipath I/O (MPIO), de pare-feu et de délai d'expiration du disque sont correctement configurés dans la machine virtuelle.



Ceci s'applique uniquement au stockage connecté en tant qu'invité.

Avantages du stockage cloud NetApp

Le stockage cloud NetApp offre les avantages suivants :

- Améliore la densité de calcul et de stockage en mettant à l'échelle le stockage indépendamment du calcul.
- Permet de réduire le nombre d'hôtes, réduisant ainsi le coût total de possession global.
- La défaillance du nœud de calcul n'a pas d'impact sur les performances de stockage.
- La capacité de remodelage du volume et de niveau de service dynamique d' Azure NetApp Files vous permet d'optimiser les coûts en dimensionnant les charges de travail en régime permanent, évitant ainsi le surprovisionnement.
- L'efficacité du stockage, la hiérarchisation du cloud et les capacités de modification du type d'instance de Cloud Volumes ONTAP permettent des moyens optimaux d'ajouter et de mettre à l'échelle le stockage.

- Empêche le surprovisionnement des ressources de stockage, qui ne sont ajoutées qu'en cas de besoin.
- Les copies et clones Snapshot efficaces vous permettent de créer rapidement des copies sans aucun impact sur les performances.
- Aide à lutter contre les attaques de ransomware en utilisant une récupération rapide à partir de copies instantanées.
- Fournit une récupération après sinistre régionale efficace basée sur un transfert de blocs incrémentiel et un niveau de bloc de sauvegarde intégré dans toutes les régions pour de meilleurs RPO et RTO.

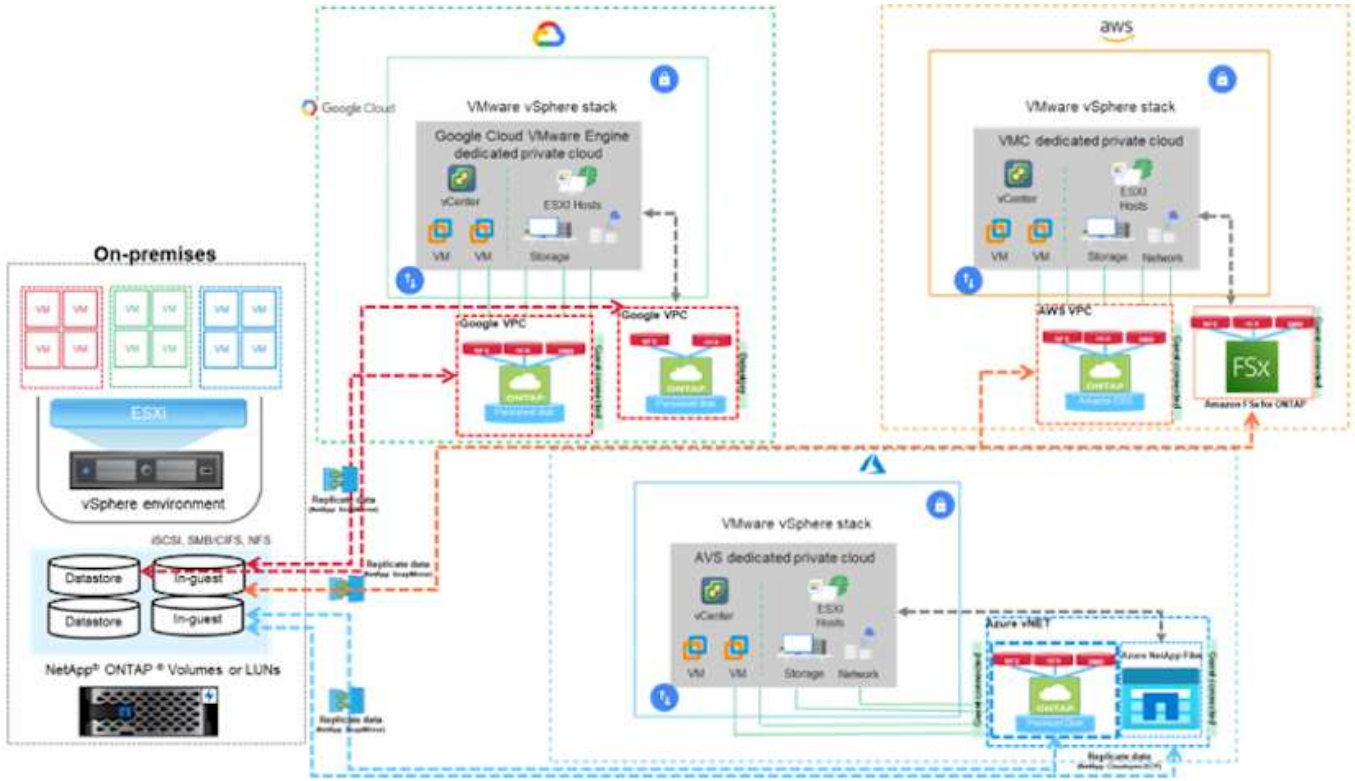
Hypothèses

- La technologie SnapMirror ou d'autres mécanismes de migration de données pertinents sont activés. Il existe de nombreuses options de connectivité, depuis le cloud local jusqu'à n'importe quel cloud hyperscaler. Utilisez le chemin approprié et travaillez avec les équipes réseau concernées.
- Le stockage interne était la seule option disponible au moment de la rédaction de ce document.

Engagez les architectes de solutions NetApp et les architectes cloud hyperscaler respectifs pour la planification et le dimensionnement du stockage et du nombre d'hôtes requis. NetApp recommande d'identifier les exigences de performances de stockage avant d'utiliser le dimensionneur Cloud Volumes ONTAP pour finaliser le type d'instance de stockage ou le niveau de service approprié avec le débit approprié.

Architecture détaillée

D'un point de vue général, cette architecture (illustrée dans la figure ci-dessous) explique comment obtenir une connectivité multicloud hybride et une portabilité des applications sur plusieurs fournisseurs de cloud à l'aide de NetApp Cloud Volumes ONTAP, Google Cloud NetApp Volumes pour Google Cloud et Azure NetApp Files comme option de stockage supplémentaire en invité.



Solutions NetApp pour VMware dans les hyperscalers

Découvrez-en plus sur les fonctionnalités que NetApp apporte aux trois (3) principaux hyperscalers : de NetApp en tant que périphérique de stockage connecté en tant qu'invité ou banque de données NFS supplémentaire à la migration des flux de travail, à l'extension/à l'éclatement vers le cloud, à la sauvegarde/restauration et à la reprise après sinistre.

Choisissez votre cloud et laissez NetApp faire le reste !



Pour voir les capacités d'un hyperscaler spécifique, cliquez sur l'onglet approprié pour cet hyperscaler.

Accédez à la section du contenu souhaité en sélectionnant parmi les options suivantes :

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

VMware dans la configuration des hyperscalers

Comme pour les environnements locaux, la planification d'un environnement de virtualisation basé sur le cloud est essentielle pour un environnement prêt pour la production et la création de machines virtuelles et la migration.

AWS / VMC

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

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

Le processus de configuration peut être décomposé selon les étapes suivantes :

- Déployer et configurer VMware Cloud pour AWS
- Connectez VMware Cloud à FSx ONTAP

Voir le détail"étapes de configuration pour VMC" .

Azure / AVS

Cette section décrit comment configurer et gérer Azure VMware Solution et l'utiliser en combinaison avec les options disponibles pour la connexion au stockage NetApp .

> Le stockage en invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP à Azure VMware Solution.

Le processus de configuration peut être décomposé selon les étapes suivantes :

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

Voir le détail"étapes de configuration pour AVS" .

GCP / GCVE

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

> Le stockage en invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP et Google Cloud NetApp Volumes à GCVE.

Le processus de configuration peut être décomposé selon les étapes suivantes :

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

Voir le détail"étapes de configuration pour GCVE" .

Options de stockage NetApp

Le stockage NetApp peut être utilisé de plusieurs manières, soit en tant qu'invité connecté, soit en tant que banque de données NFS supplémentaire, dans chacun des 3 principaux hyperscalers.

S'il vous plaît visitez"Options de stockage NetApp prises en charge" pour plus d'informations.

AWS / VMC

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

- FSx ONTAP comme stockage connecté invité
- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités

- FSx ONTAP comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour VMC" . Voir le détail"options de banque de données NFS supplémentaires pour VMC" .

Azure / AVS

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

- Azure NetApp Files (ANF) en tant que stockage connecté invité
- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- Azure NetApp Files (ANF) comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour AVS" . Voir le détail"options de banque de données NFS supplémentaires pour AVS" .

GCP / GCVE

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

- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- Google Cloud NetApp Volumes (NetApp Volumes) en tant que stockage connecté invité
- Google Cloud NetApp Volumes (NetApp Volumes) comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour GCVE" . Voir le détail"options de banque de données NFS supplémentaires pour GCVE" .

En savoir plus sur"Prise en charge du magasin de données Google Cloud NetApp Volumes pour Google Cloud VMware Engine (blog NetApp)" ou"Comment utiliser Google Cloud NetApp Volumes comme banques de données pour Google Cloud VMware Engine (blog Google)"

Solutions cloud NetApp / VMware

Avec les solutions cloud NetApp et VMware, de nombreux cas d'utilisation sont simples à déployer dans l'hyperscaler de votre choix. VMware définit les principaux cas d'utilisation de la charge de travail cloud comme suit :

- Protéger (comprend à la fois la reprise après sinistre et la sauvegarde/restauration)
- Émigrer
- Étendre

AWS / VMC

"Parcourez les solutions NetApp pour AWS / VMC"

Azure / AVS

"Parcourez les solutions NetApp pour Azure / AVS"

GCP / GCVE

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

Configurations prises en charge pour NetApp Hybrid Multicloud avec VMware

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

	Invité connecté	Magasin de données NFS supplémentaire
AWS	CVO FSx ONTAP"Détails"	FSx ONTAP"Détails"
Azuré	CVO ANF"Détails"	ANF"Détails"
BPC	CVO NetApp Volumes"Détails"	NetApp Volumes"Détails"

VMware dans la configuration des hyperscalers

Configuration de l'environnement de virtualisation chez le fournisseur de cloud

Les détails sur la façon de configurer l'environnement de virtualisation dans chacun des hyperscalers pris en charge sont traités ici.

AWS / VMC

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

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

Le processus de configuration peut être décomposé selon les étapes suivantes :

- Déployer et configurer VMware Cloud pour AWS
- Connectez VMware Cloud à FSx ONTAP

Voir le détail"étapes de configuration pour VMC" .

Azure / AVS

Cette section décrit comment configurer et gérer Azure VMware Solution et l'utiliser en combinaison avec les options disponibles pour la connexion au stockage NetApp .

Le stockage en invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP à Azure VMware Solution.

Le processus de configuration peut être décomposé selon les étapes suivantes :

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

Voir le détail"étapes de configuration pour AVS" .

GCP / GCVE

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

Le stockage en invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP et Google Cloud NetApp Volumes à GCVE.

Le processus de configuration peut être décomposé selon les étapes suivantes :

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

Voir le détail"étapes de configuration pour GCVE" .

Déployer et configurer l'environnement de virtualisation sur AWS

Comme pour les environnements locaux, la planification de VMware Cloud sur AWS est essentielle pour un environnement prêt pour la production et la création de machines virtuelles et la migration.

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

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

Le processus de configuration peut être décomposé selon les étapes suivantes :

▼ **Déployer et configurer VMware Cloud pour AWS**

"VMware Cloud sur AWS"offre une expérience cloud native pour les charges de travail basées sur VMware dans l'écosystème AWS. Chaque centre de données défini par logiciel VMware (SDDC) s'exécute dans un Amazon Virtual Private Cloud (VPC) et fournit une pile VMware complète (y compris vCenter Server), une mise en réseau définie par logiciel NSX-T, un stockage défini par logiciel 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 combinaison avec Amazon FSx ONTAP et/ou Cloud Volumes ONTAP sur AWS avec stockage invité.

Le stockage en 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 :

▼ **Inscrivez-vous pour un compte AWS**

Inscrivez-vous pour un"Compte Amazon Web Services" .

Vous avez besoin d'un compte AWS pour commencer, en supposant qu'il n'y en ait pas déjà un créé. Nouveau ou existant, vous avez besoin de privilèges administratifs sur le compte pour de nombreuses étapes de cette procédure. Regarde ça"lien" pour plus d'informations sur les informations d'identification AWS.

▼ Inscrivez-vous pour un compte My VMware

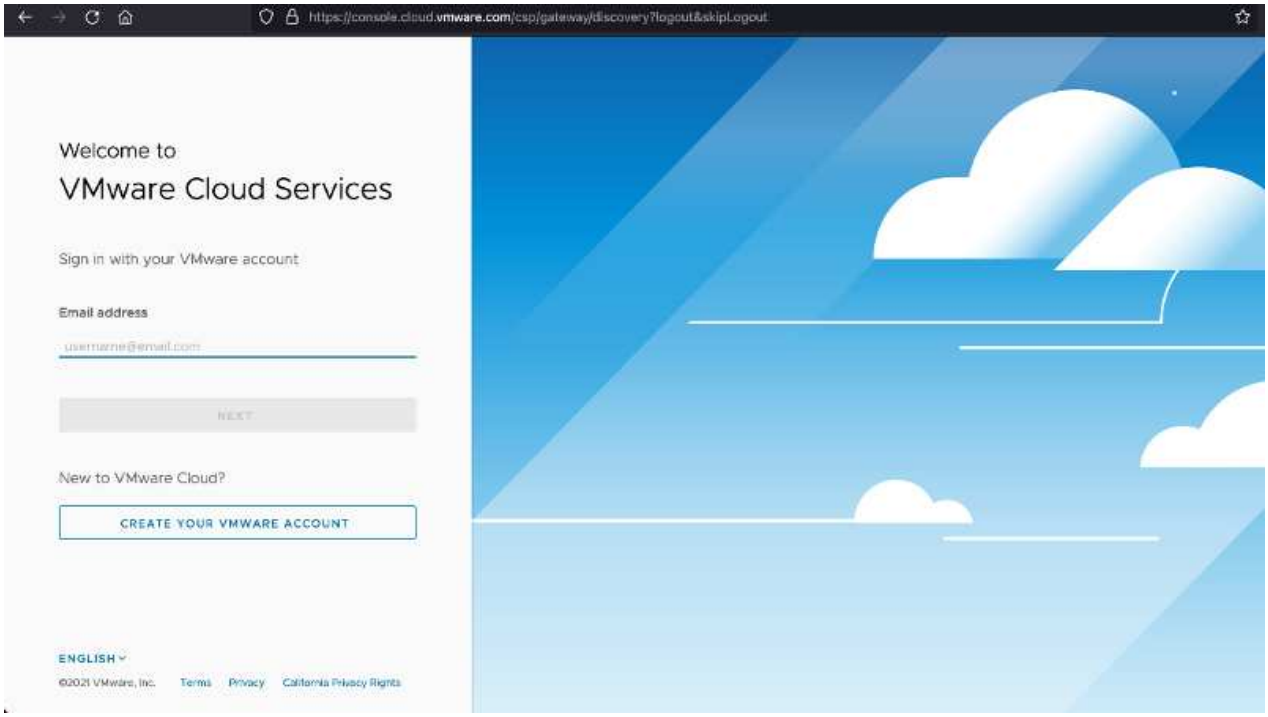
Inscrivez-vous pour un"Mon VMware" compte.

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 vous ne l'avez pas déjà fait, créez un compte VMware"ici" .

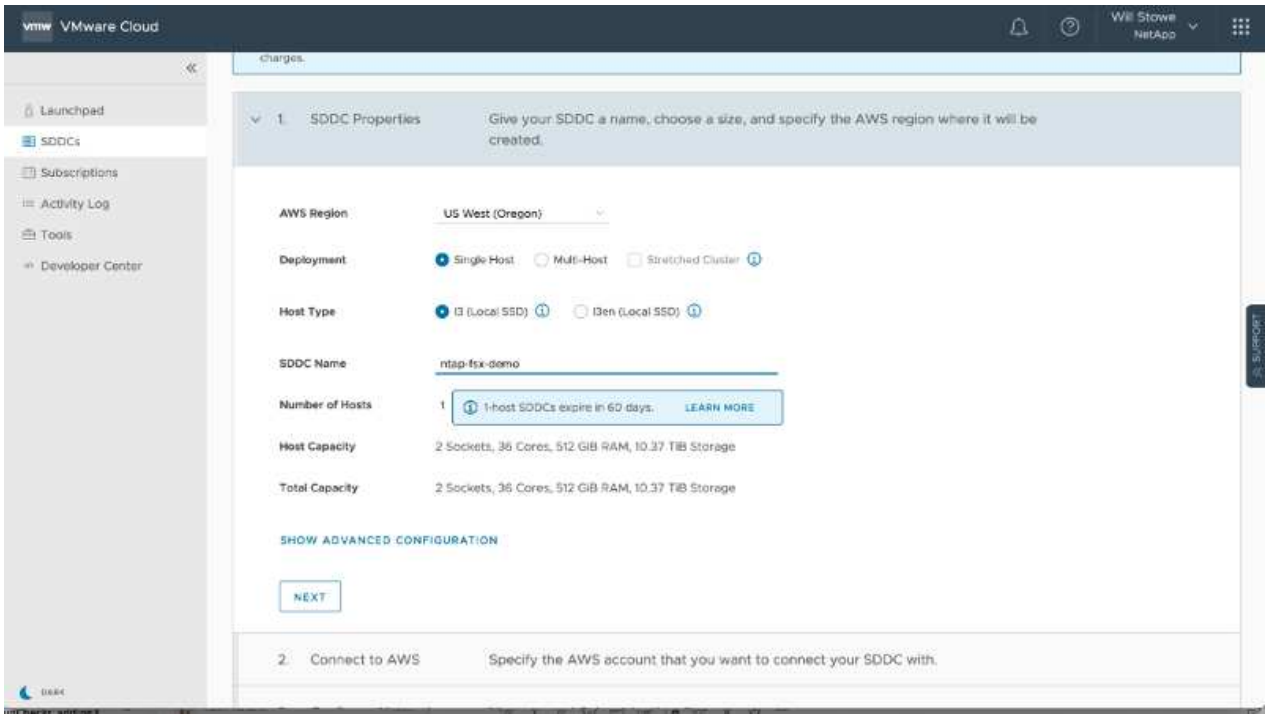
▼ Provisionner un SDDC dans VMware Cloud

Une fois le compte VMware configuré et le dimensionnement approprié effectué, le déploiement d'un centre de données défini par logiciel est la prochaine étape évidente pour utiliser le service VMware Cloud on AWS. Pour créer un SDDC, choisissez une région AWS pour l'héberger, 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 seul hôte ESXi.

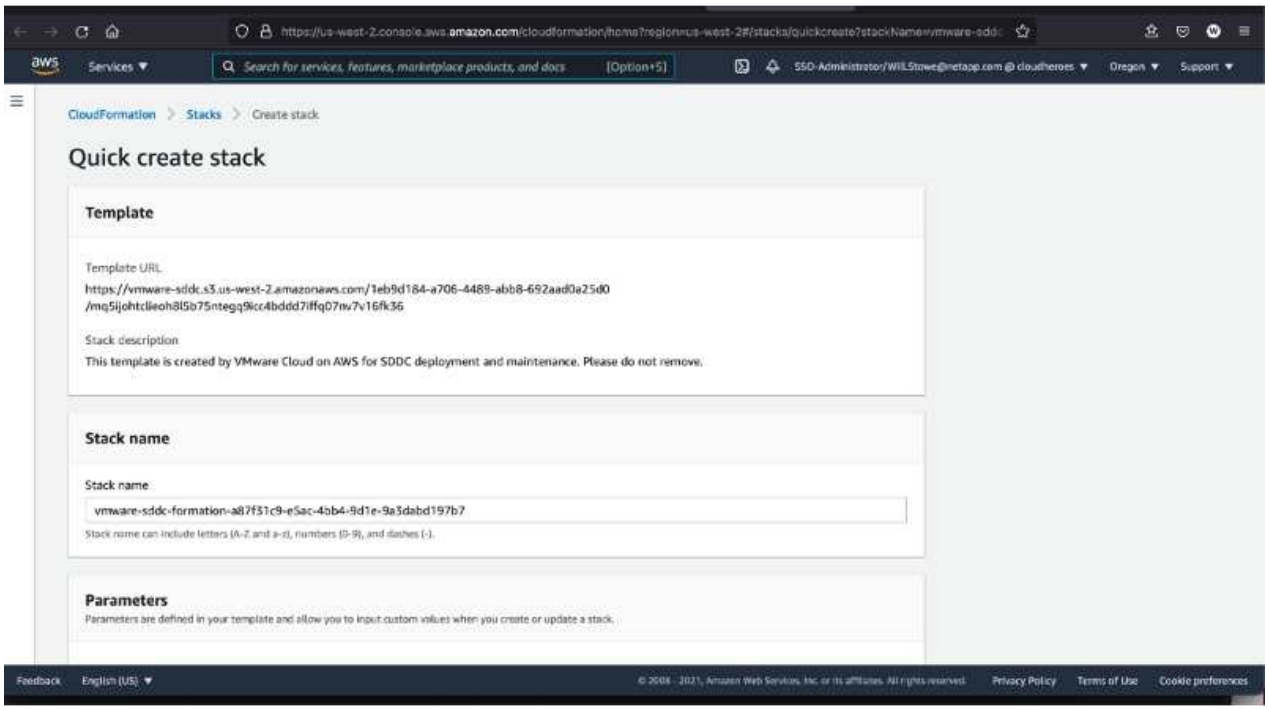
1. Connectez-vous à la console VMware Cloud à l'aide de vos informations d'identification VMware existantes ou nouvellement créées.

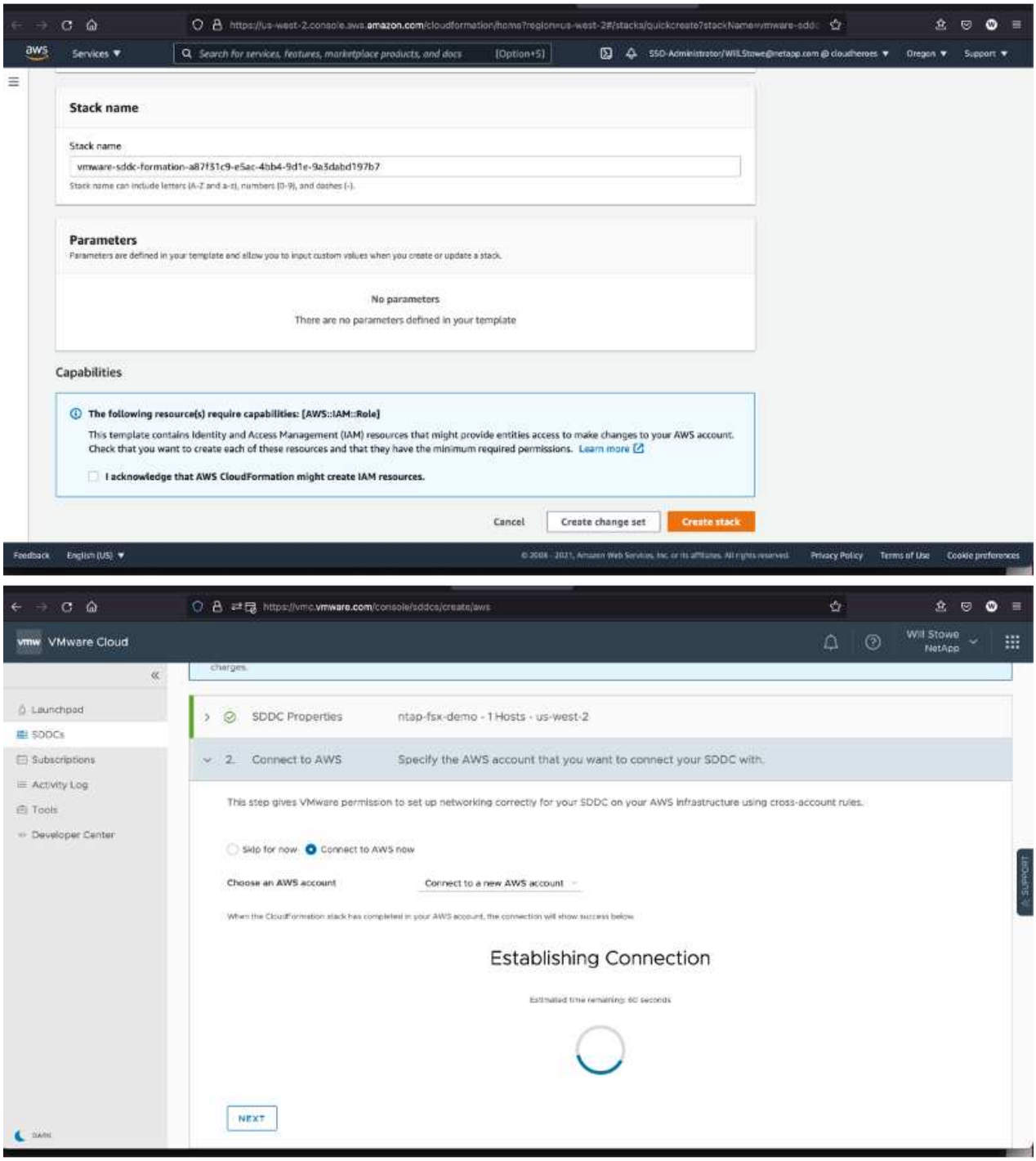


2. Configurez la région AWS, le déploiement, le type d'hôte et le nom du SDDC :

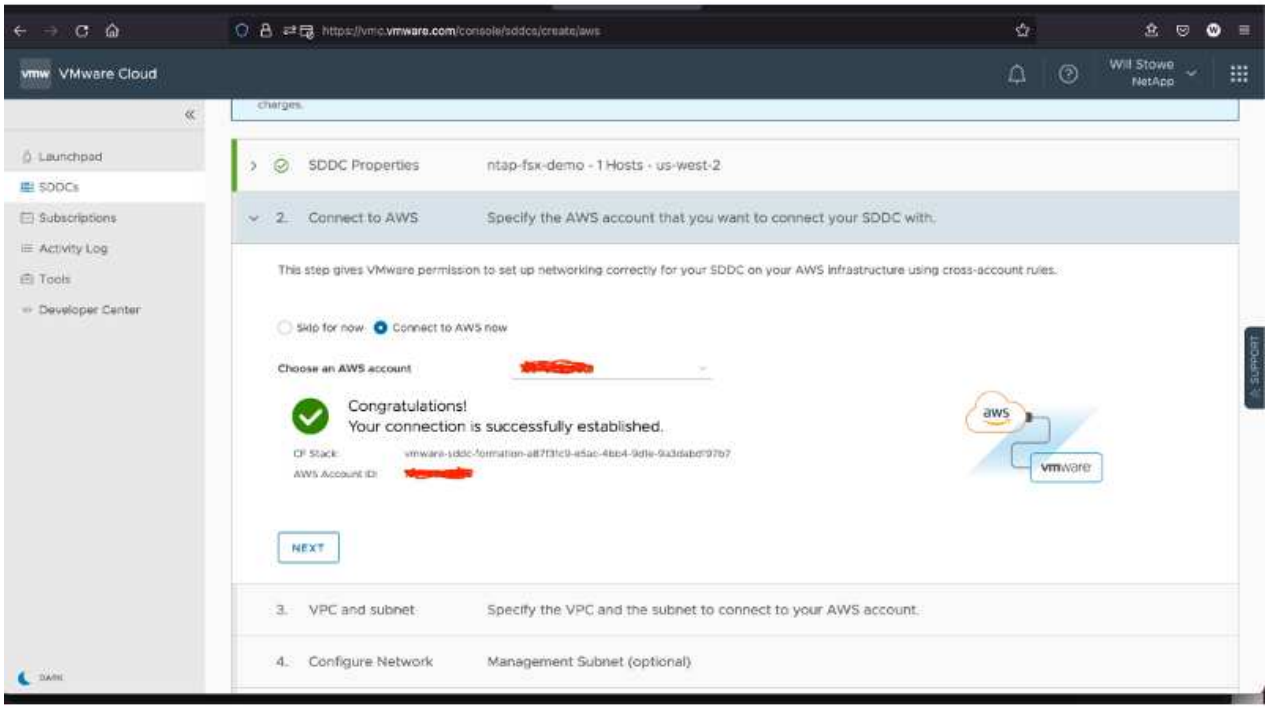


3. Connectez-vous au compte AWS souhaité et exécutez la pile AWS Cloud Formation.



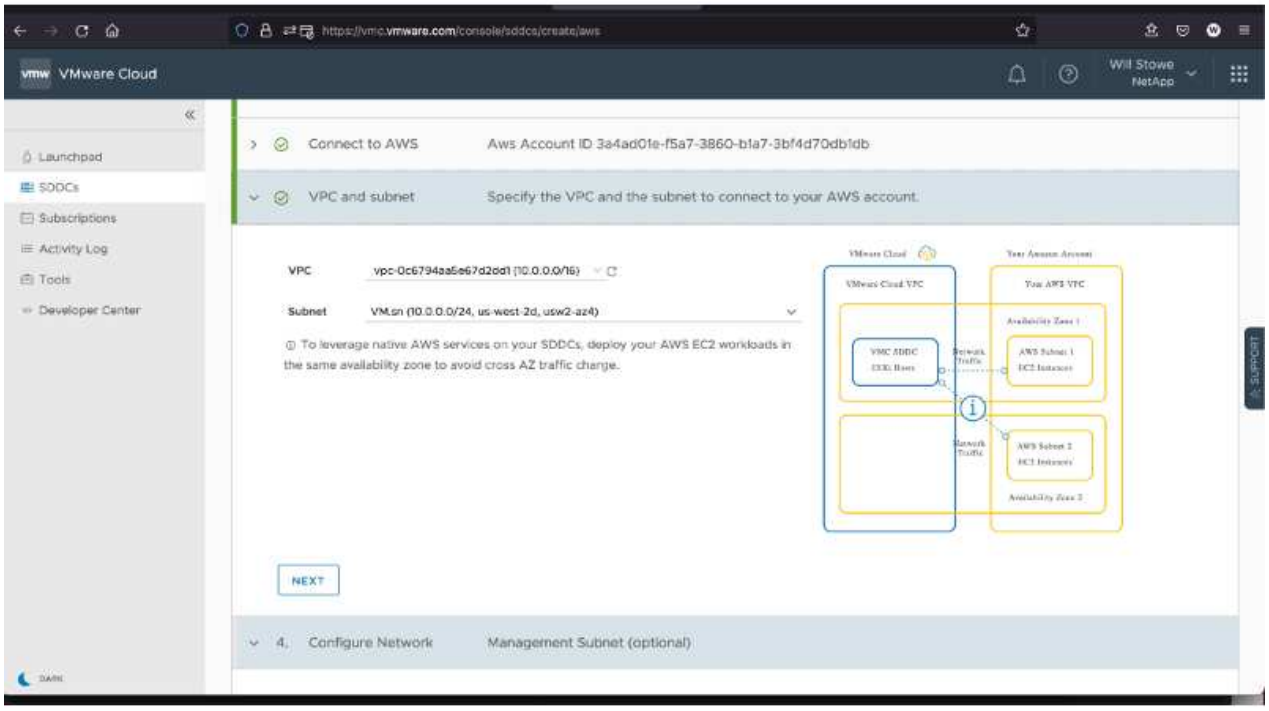

Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
SDDC Properties
ntap-fsx-demo - 1 Hosts - us-west-2
2. Connect to AWS
Specify the AWS account that you want to connect your SDDC with.
This step gives VMware permission to set up networking correctly for your SDDC on your AWS infrastructure using cross-account rules.
Skip for now
Connect to AWS now
Choose an AWS account
Connect to a new AWS account
Establishing Connection
NEXT

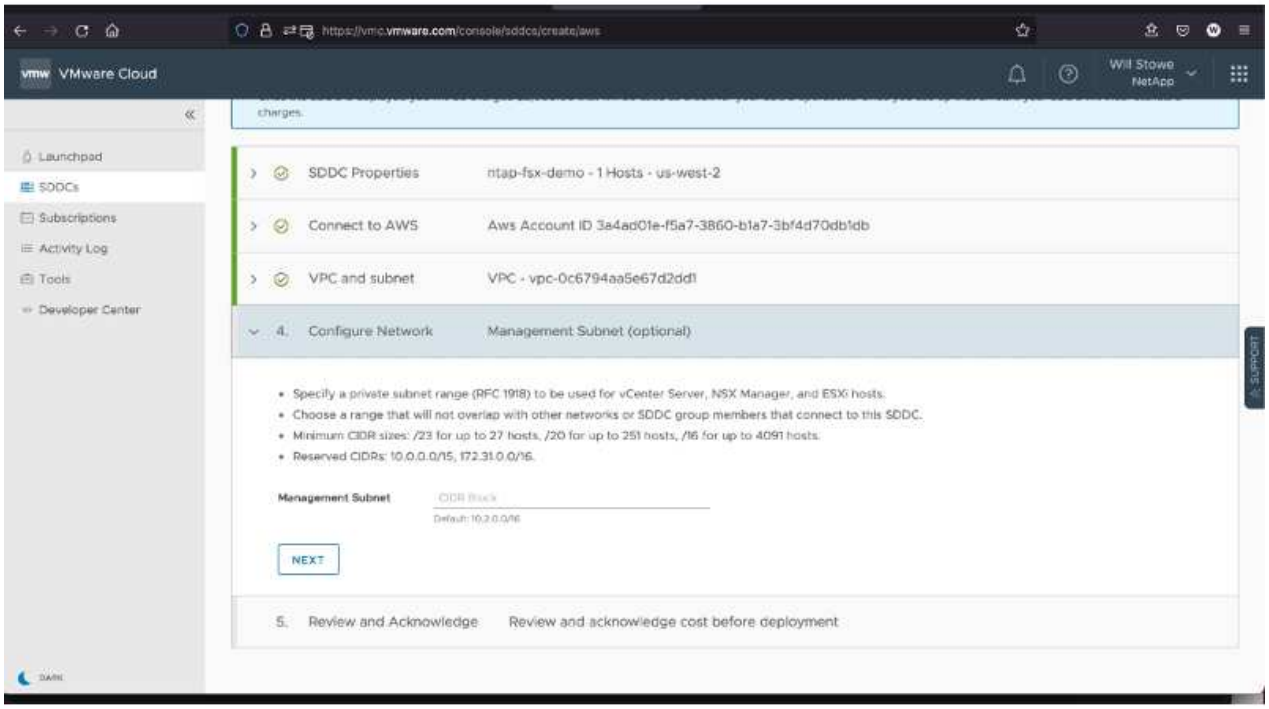


La configuration à hôte unique est utilisée dans cette validation.

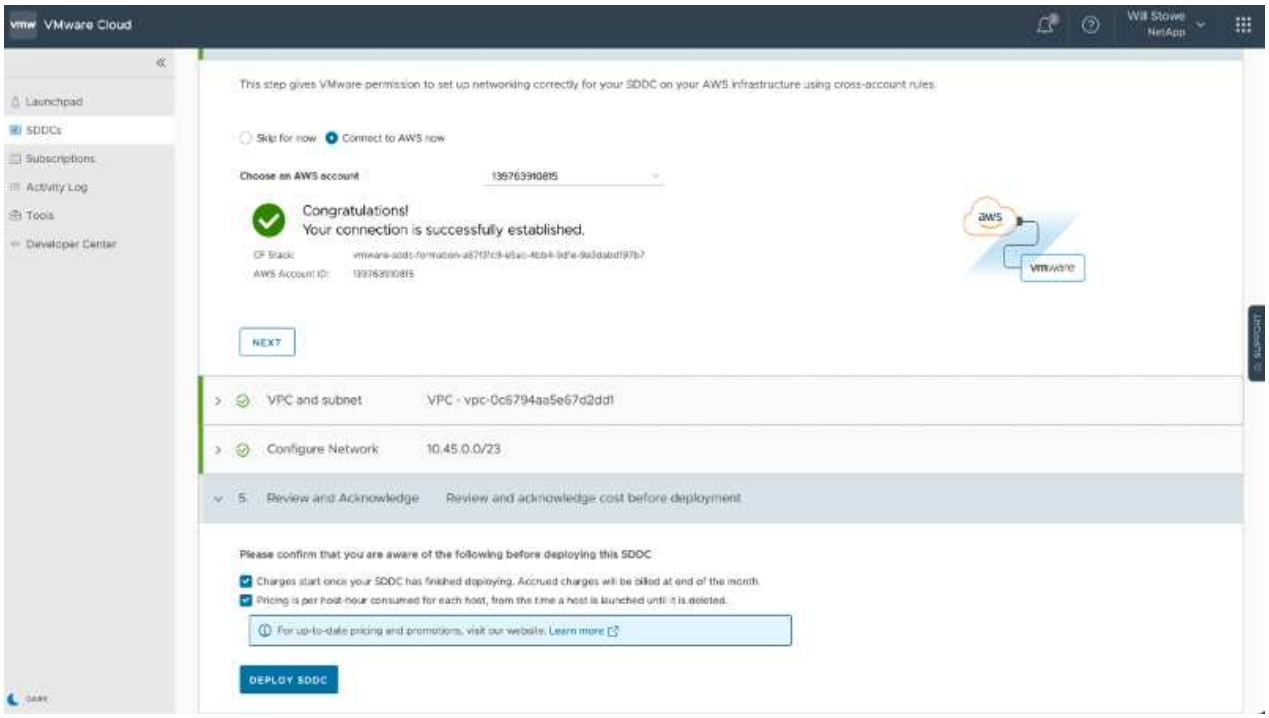
4. Sélectionnez le VPC AWS souhaité pour connecter l'environnement VMC.



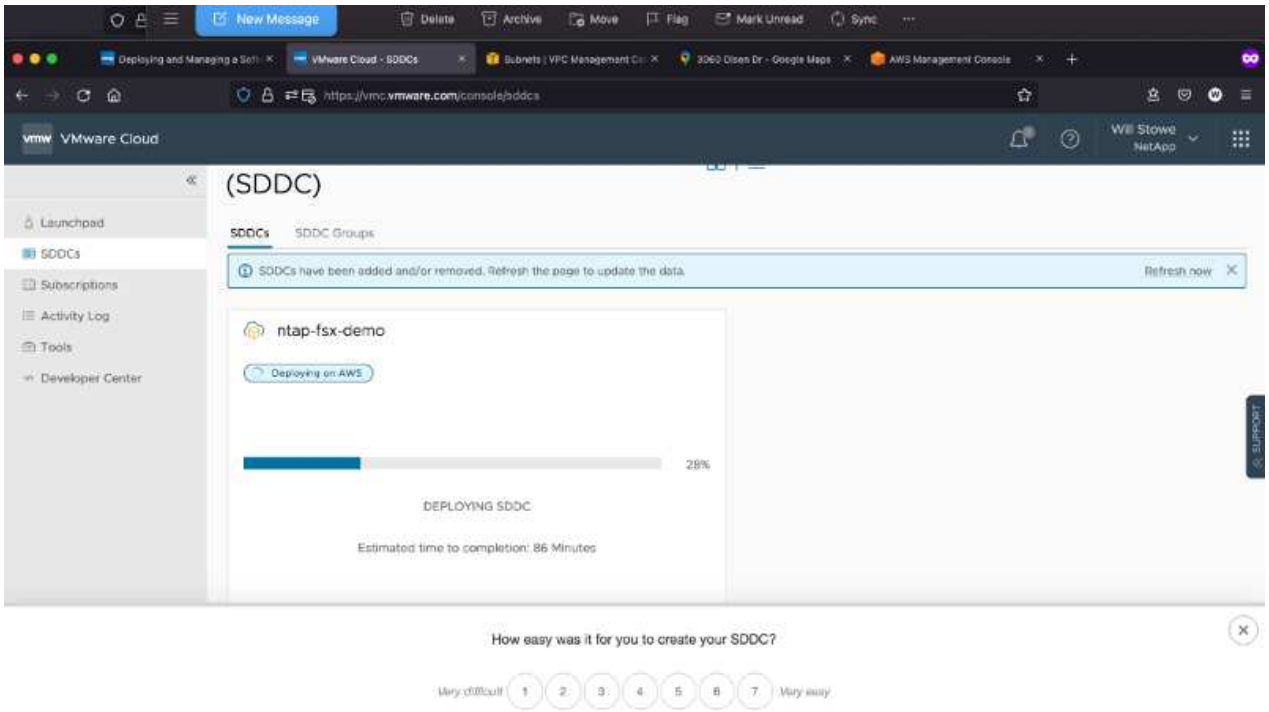
5. Configurez le sous-réseau de gestion VMC ; ce sous-réseau contient des services gérés par VMC tels que vCenter, NSX, etc. Ne choisissez pas un espace d'adressage qui se chevauche avec d'autres réseaux nécessitant une connectivité à l'environnement SDDC. Enfin, suivez les recommandations concernant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



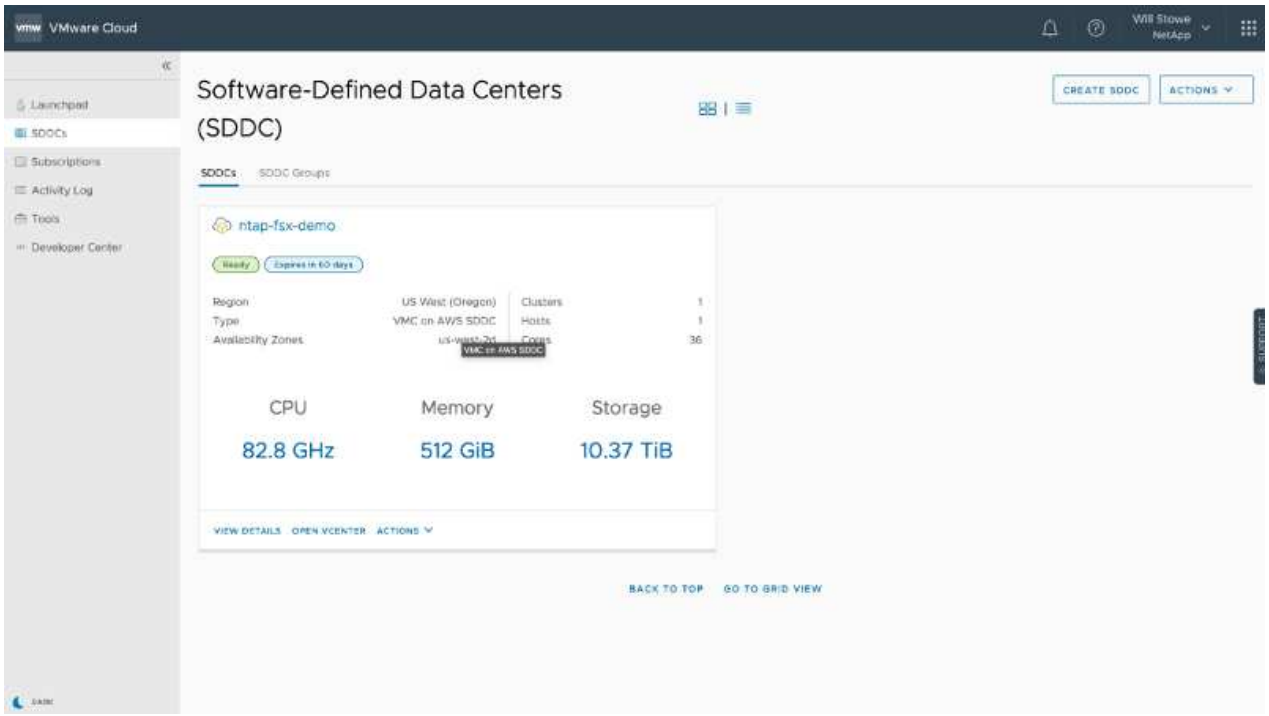
6. Vérifiez et reconnaissez la configuration du SDDC, puis cliquez sur déployer le SDDC.



Le processus de déploiement prend généralement environ deux heures.



7. Une fois terminé, le SDDC est prêt à être utilisé.



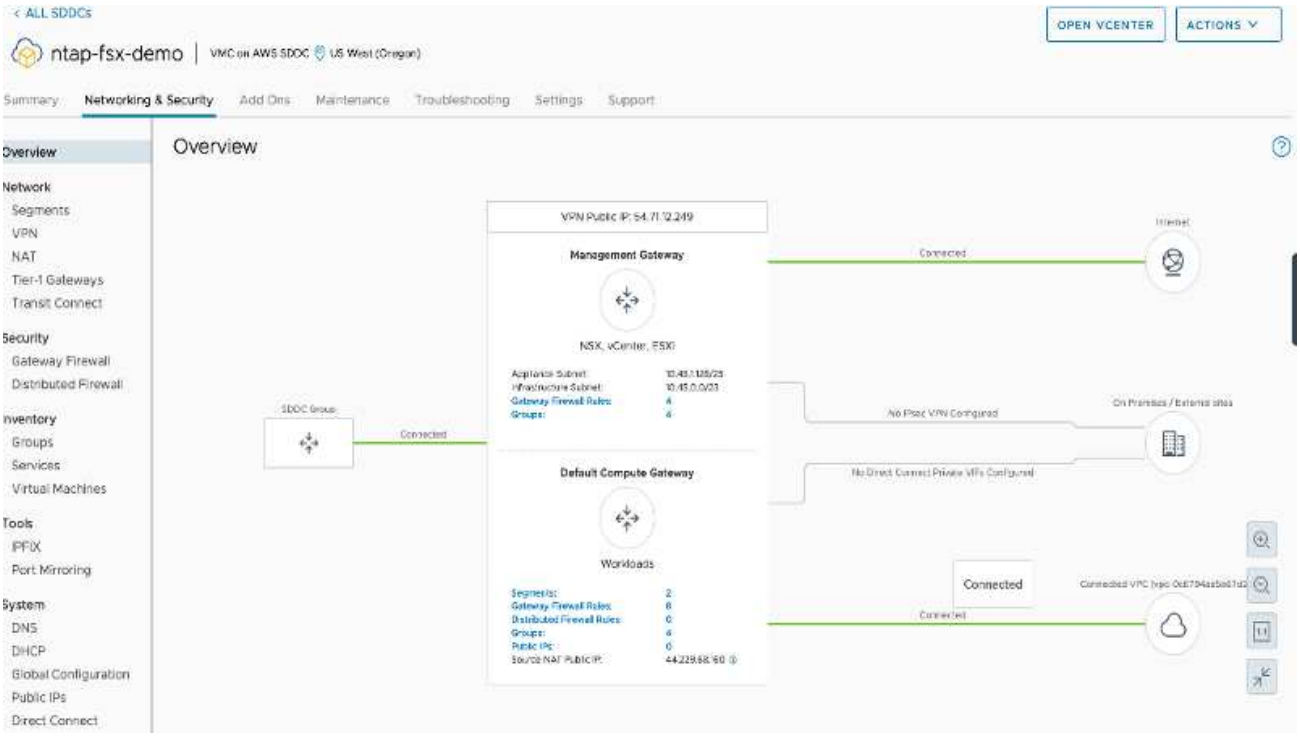
Pour un guide étape par étape sur le déploiement de SDDC, consultez"Déployer un SDDC depuis la console VMC" .

▼ Connectez VMware Cloud à FSx ONTAP

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

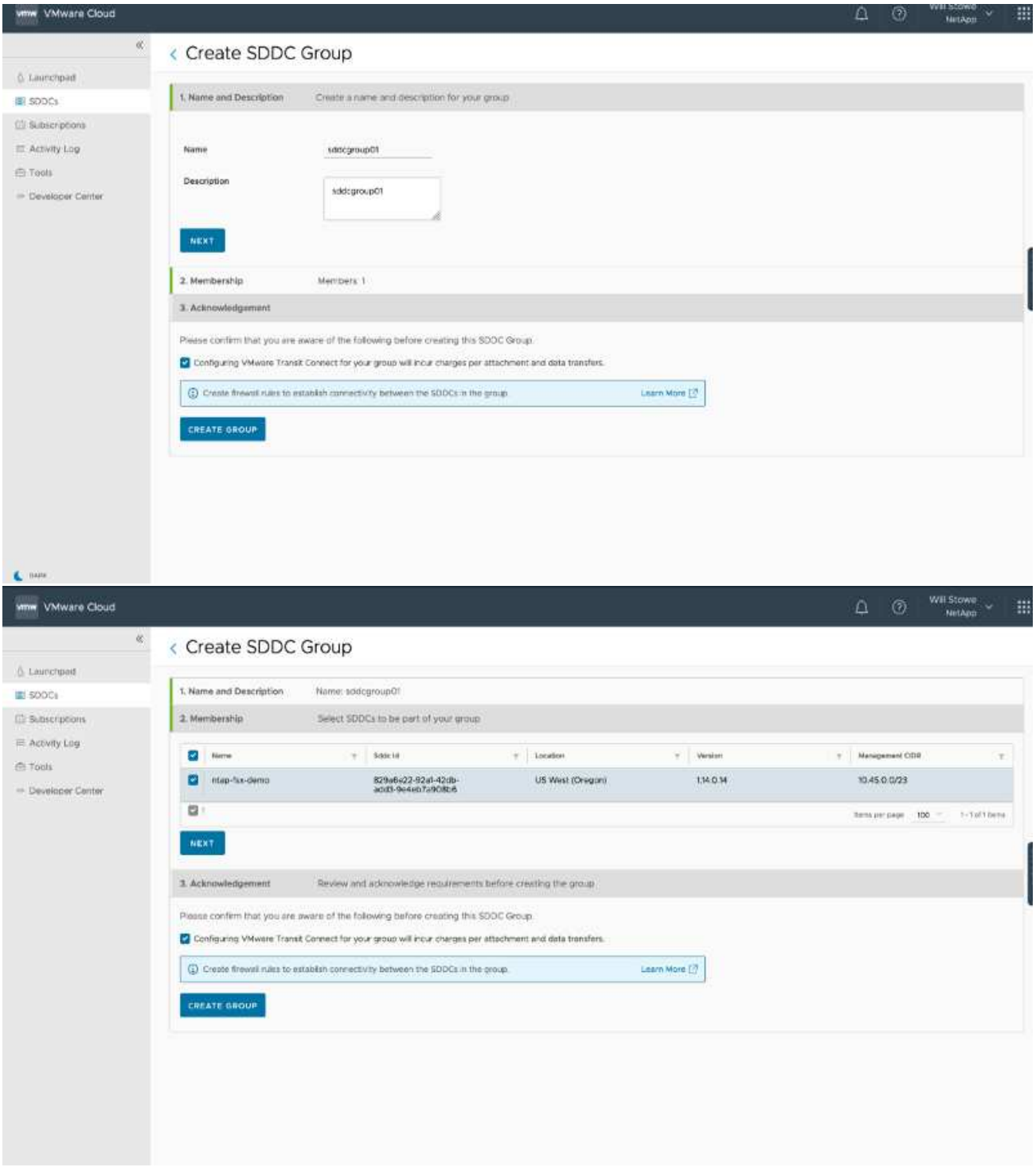
1. Une fois le déploiement de VMware Cloud terminé et connecté à AWS VPC, vous devez déployer Amazon FSx ONTAP dans un nouveau VPC plutôt que dans le VPC connecté d'origine (voir la capture d'écran ci-dessous). FSx (IP flottantes NFS et SMB) n'est pas accessible s'il est déployé dans le VPC

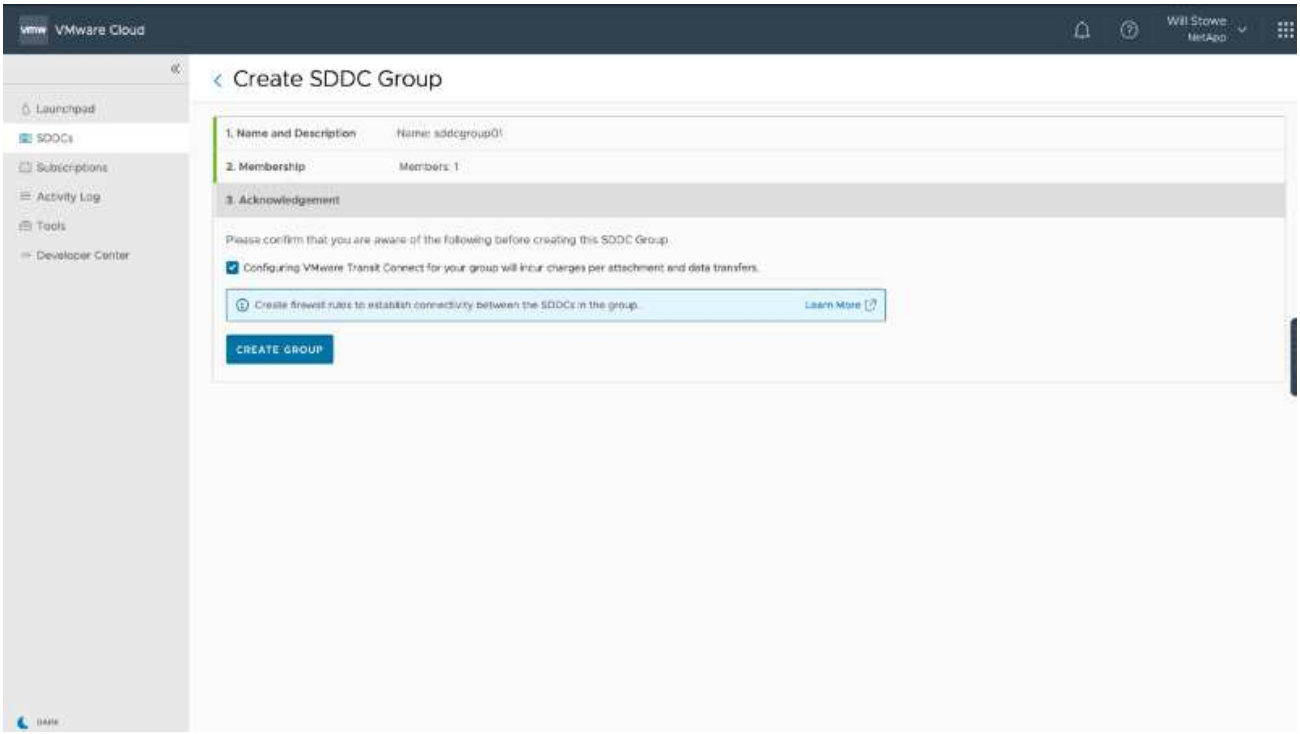
connecté. Gardez à l'esprit que les points de terminaison ISCSI comme Cloud Volumes ONTAP fonctionnent très bien à partir du VPC connecté.



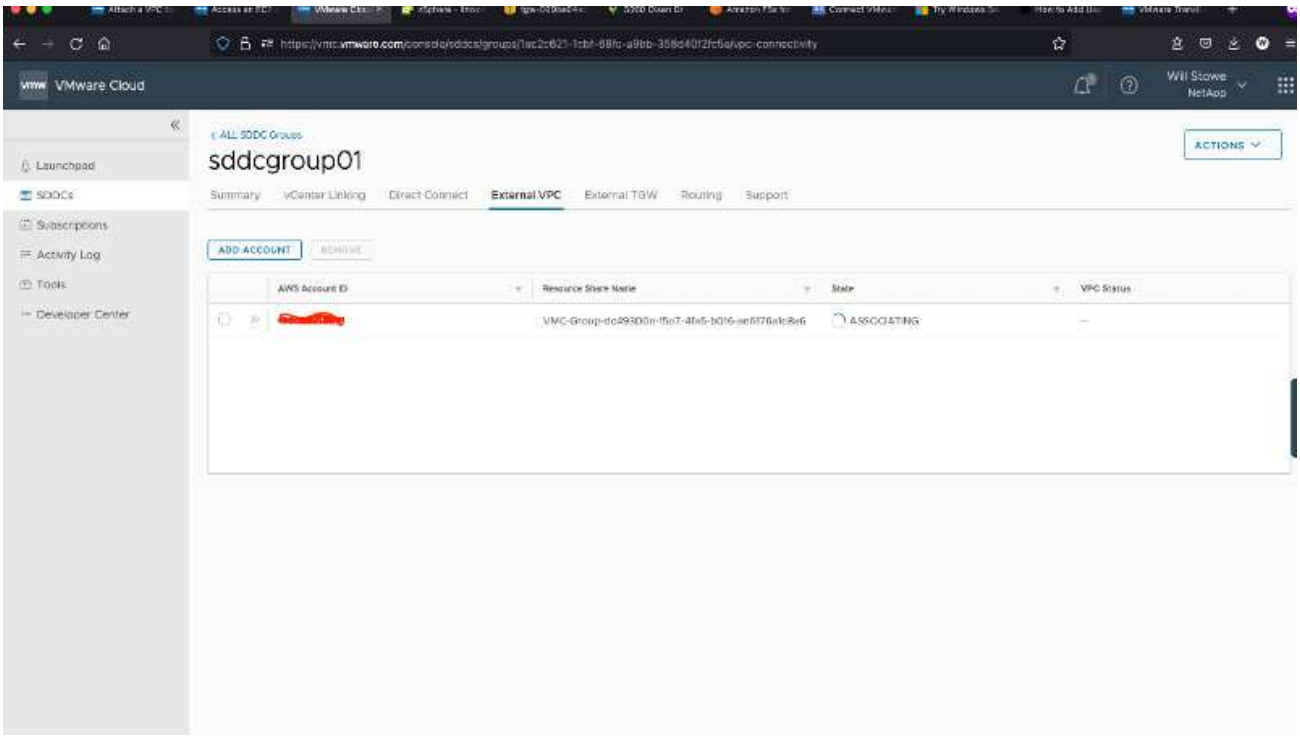
2. Déployez un VPC supplémentaire dans la même région, puis déployez Amazon FSx ONTAP dans le nouveau VPC.

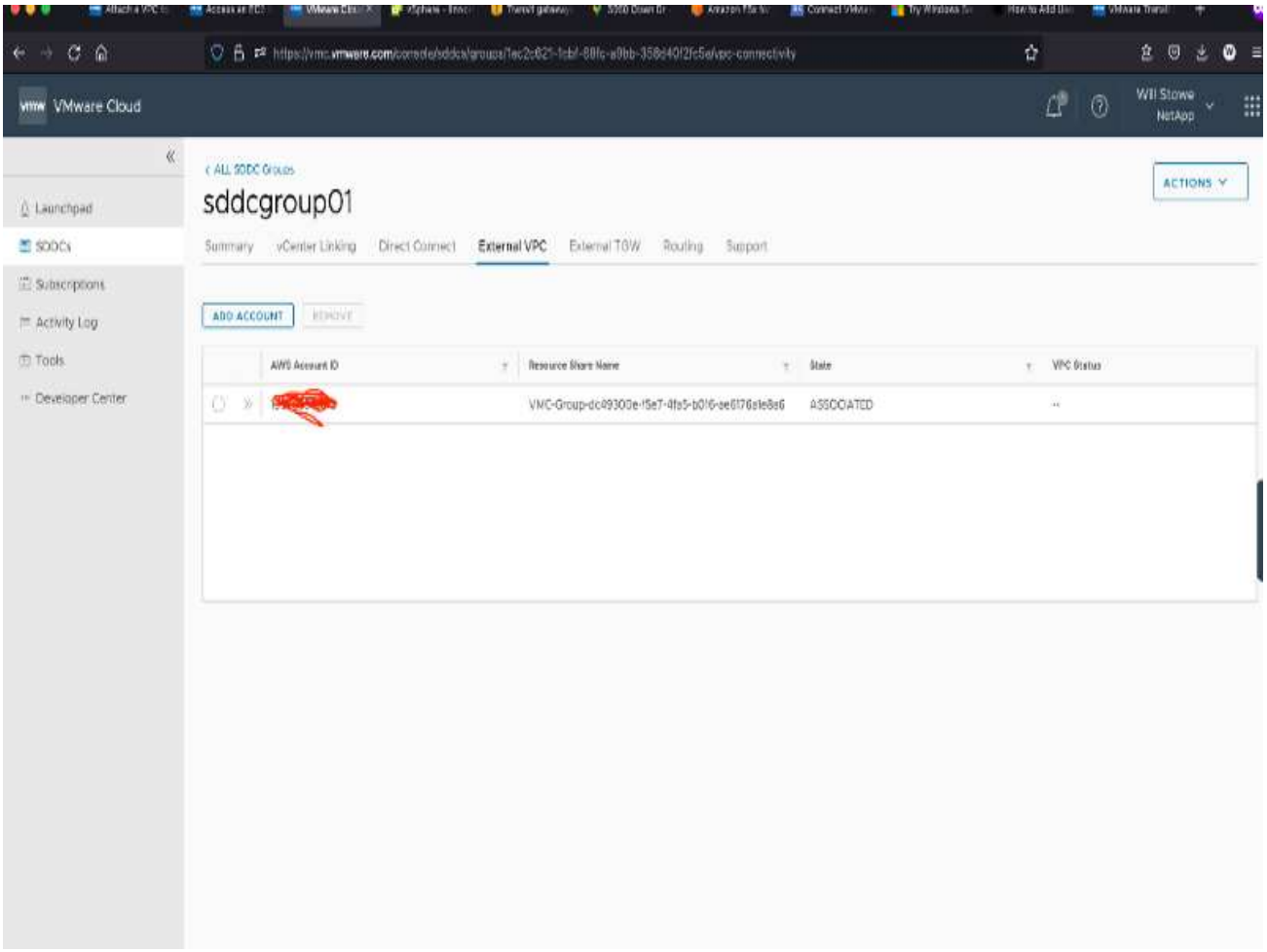
   La configuration d'un groupe SDDC dans la console VMware Cloud active les options de configuration réseau requises pour se connecter au nouveau VPC où FSx est déployé. À l'étape 3, vérifiez que « La configuration de VMware Transit Connect pour votre groupe entraînera des frais par pièce jointe et par transfert de données » est cochée, puis choisissez Créer un groupe. Le 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
829e6e22-92a1-42db-acd3-9e4eb7a90fb6
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

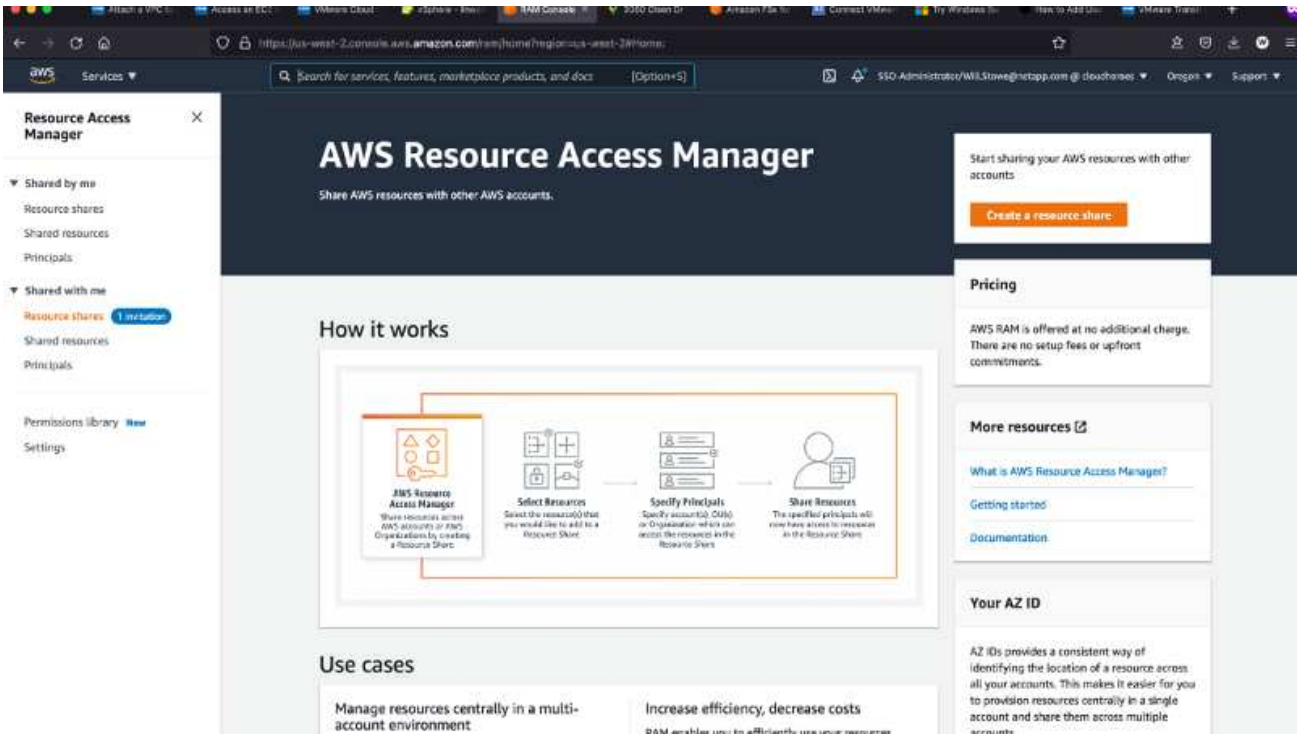


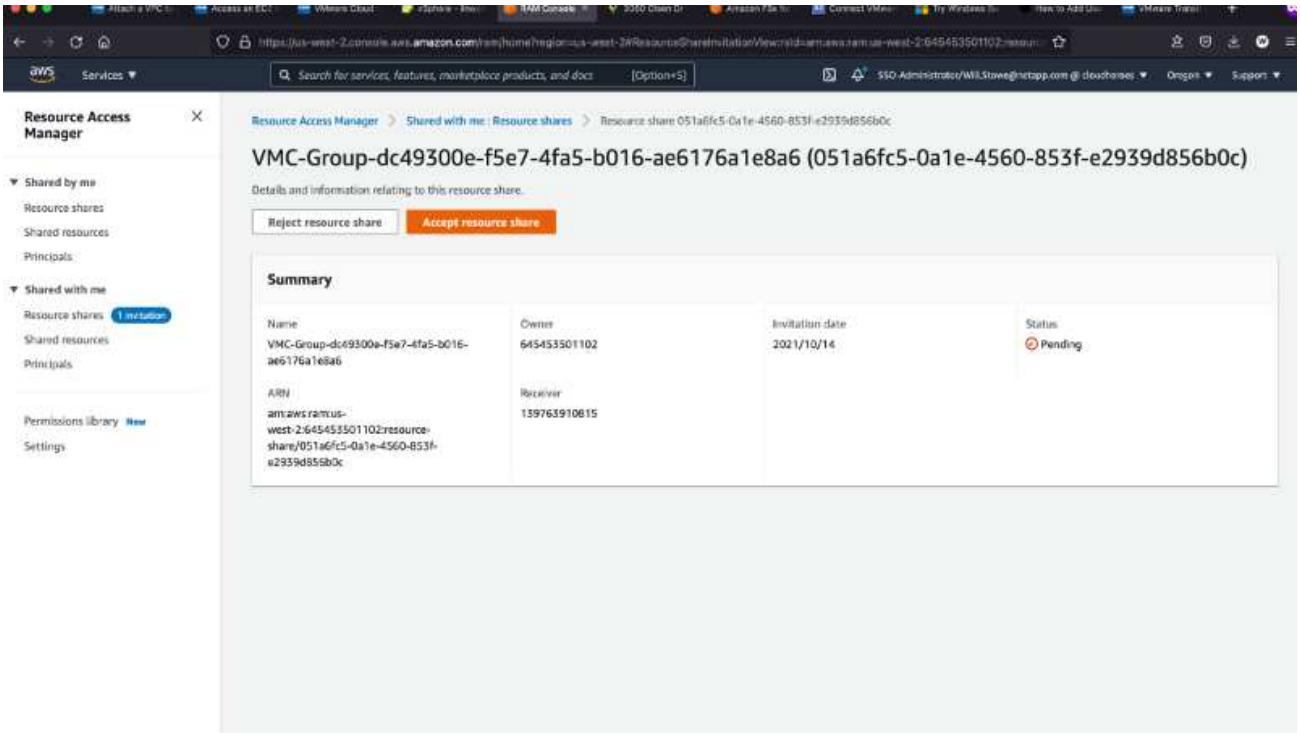
3. Attachez le VPC nouvellement créé au groupe SDDC qui vient d'être créé. Sélectionnez l'onglet VPC externe et suivez les"instructions pour connecter un VPC externe" au groupe. Ce processus peut prendre de 10 à 15 minutes.



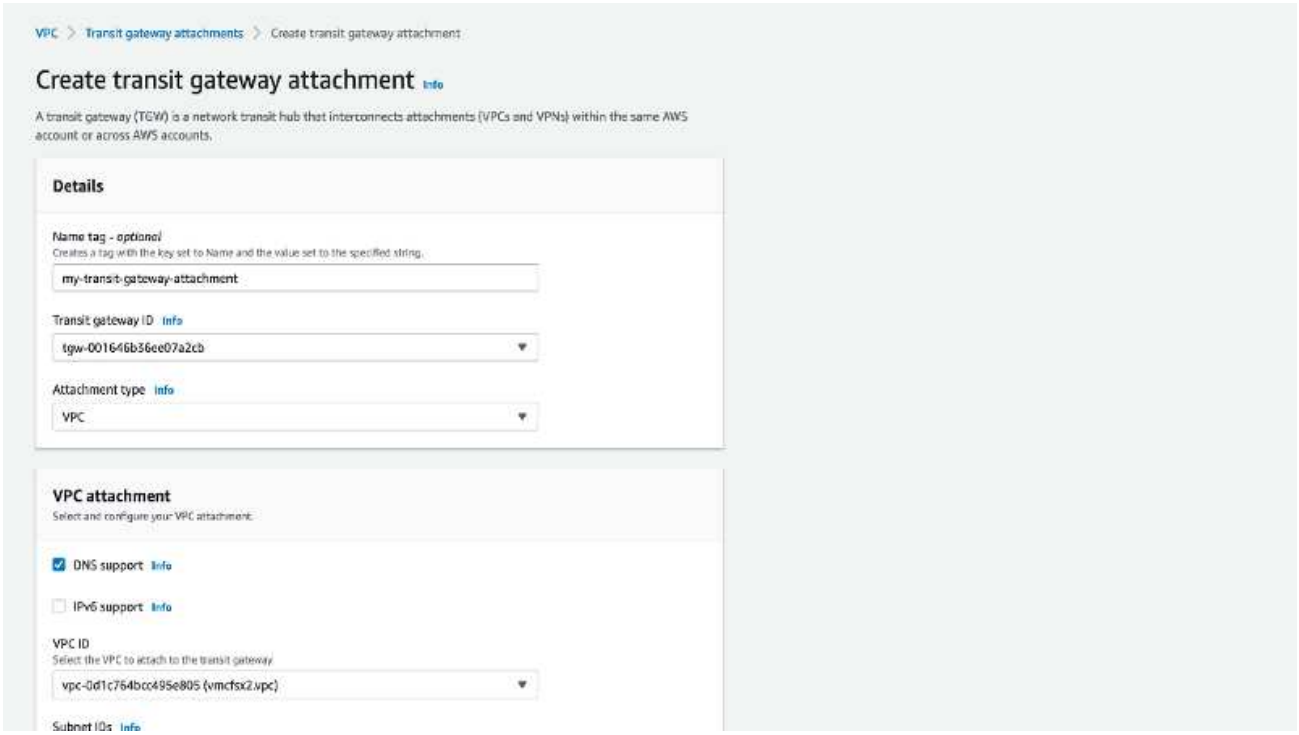


4. Dans le cadre du processus VPC externe, vous êtes invité via la console AWS à accéder à une nouvelle ressource partagée via Resource Access Manager. La ressource partagée est la"Passerelle de transit AWS" géré par VMware Transit Connect.

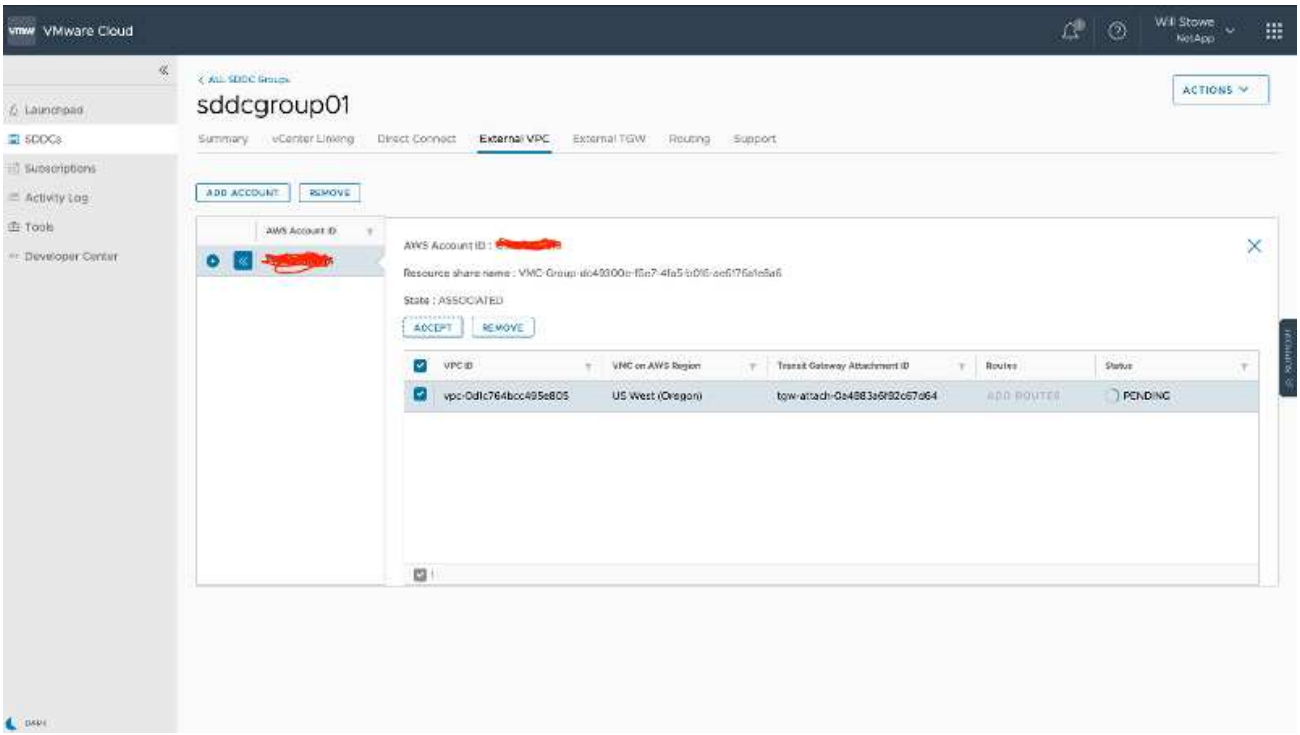




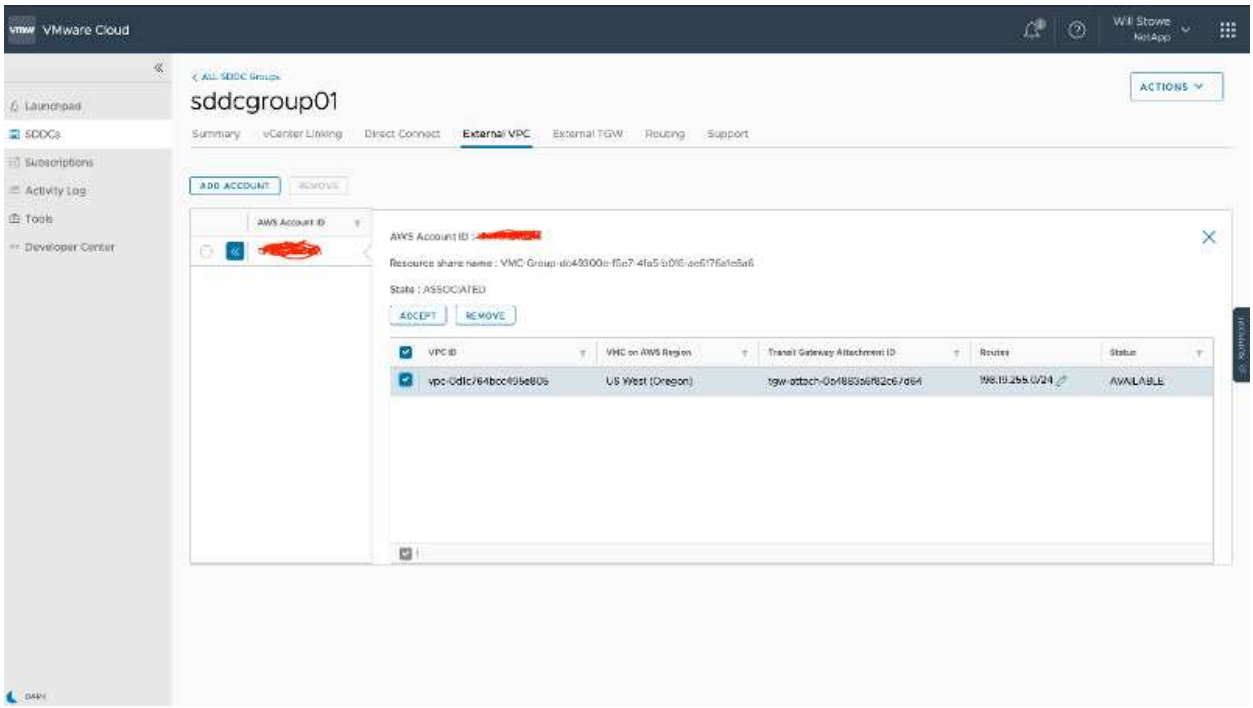
5. Créez la pièce jointe de la passerelle de transit.



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

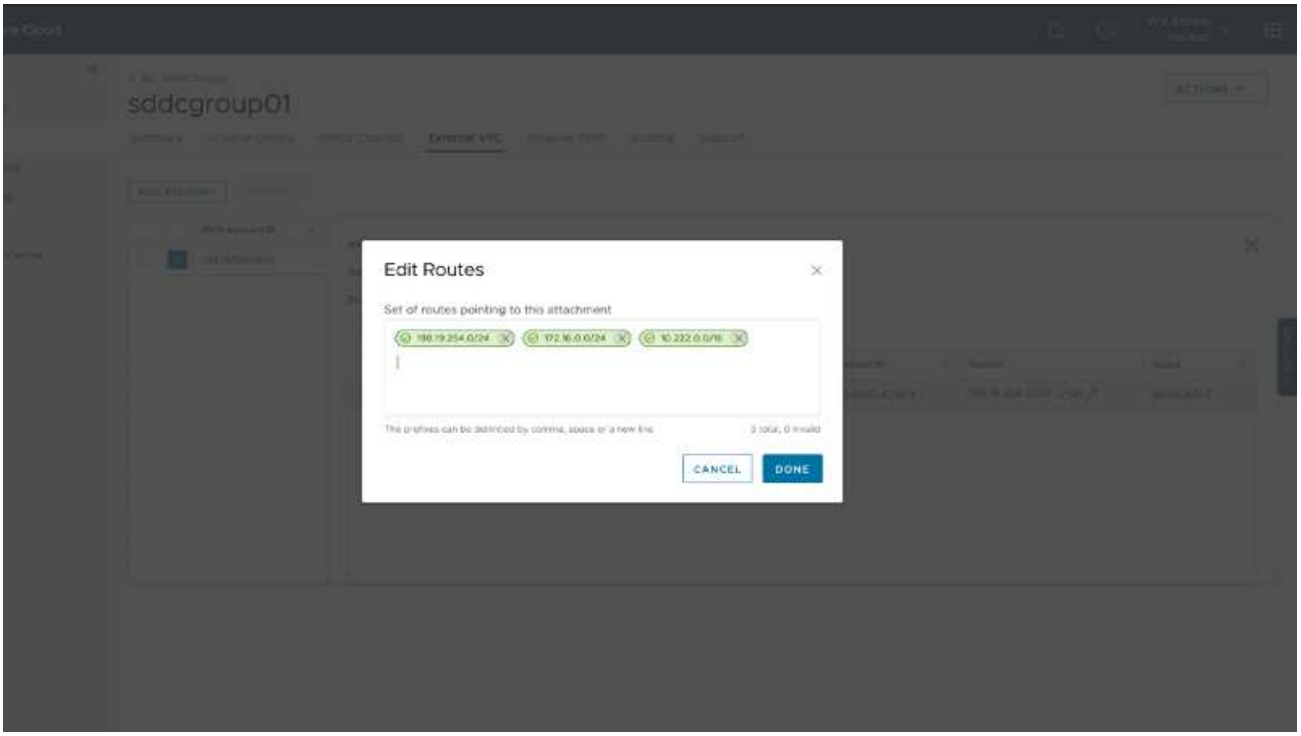


7. Dans l'onglet VPC externe, cliquez sur l'icône de modification dans la colonne Routes et ajoutez les routes requises suivantes :
   - Un itinéraire pour la plage d'adresses IP flottantes pour Amazon FSx ONTAP"adresses IP flottantes" .
   - Un itinéraire pour la plage IP flottante pour Cloud Volumes ONTAP (le cas échéant).
   - Un itinéraire pour l'espace d'adressage VPC externe nouvellement créé.

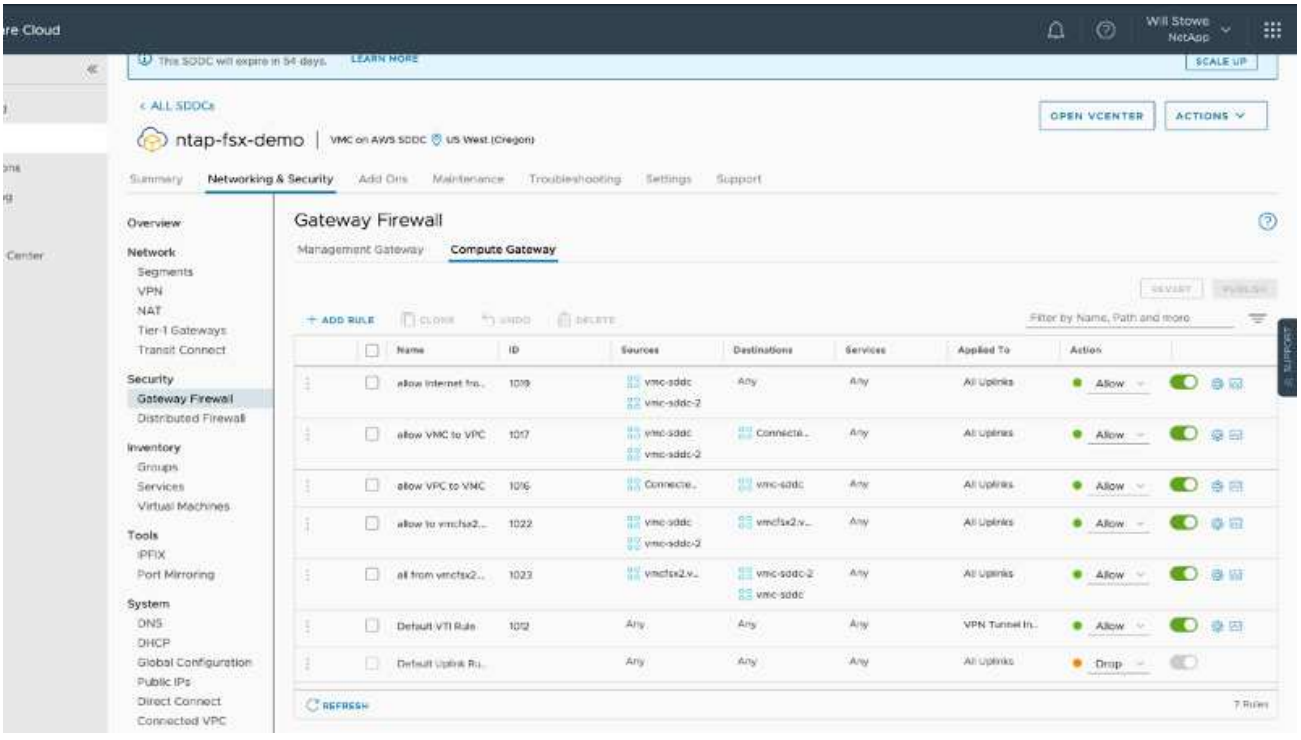


8. Enfin, autorisez le trafic bidirectionnel"règles de pare-feu" pour accéder à FSx/CVO. Suivez ces"étapes détaillées" pour les règles de pare-feu de passerelle de calcul pour la connectivité de charge de travail

SDDC.



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



L'étape suivante consiste à vérifier qu'Amazon 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.

Déployer et configurer l'environnement de virtualisation sur Azure

Comme pour les environnements locaux, la planification de la solution Azure VMware est essentielle pour un environnement prêt pour la production et la création de machines virtuelles et la migration.

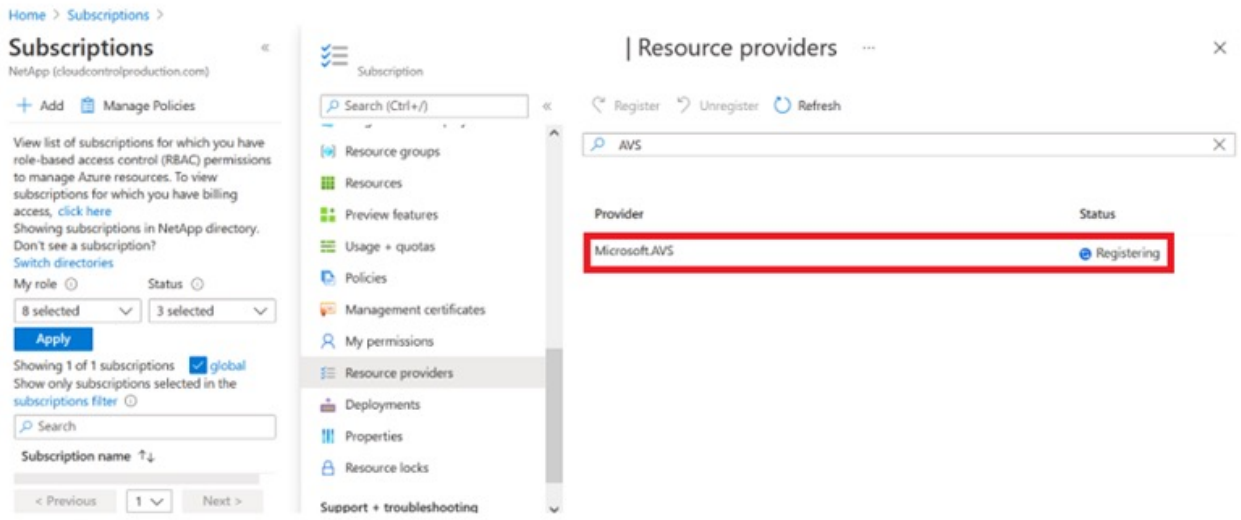
Cette section décrit comment configurer et gérer Azure VMware Solution et l'utiliser en combinaison avec les options disponibles pour la connexion au stockage NetApp .

Le processus de configuration peut être décomposé selon les étapes suivantes :

▼ **Enregistrez le fournisseur de ressources et créez un cloud privé**

Pour utiliser Azure VMware Solution, enregistrez d'abord le fournisseur de ressources dans l'abonnement identifié :

1. Sign in 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, sélectionnez l'abonnement dans la liste des abonnements.
5. Sélectionnez Fournisseurs de ressources et entrez Microsoft.AVS dans la recherche.
6. Si le fournisseur de ressources n'est pas enregistré, sélectionnez S'inscrire.

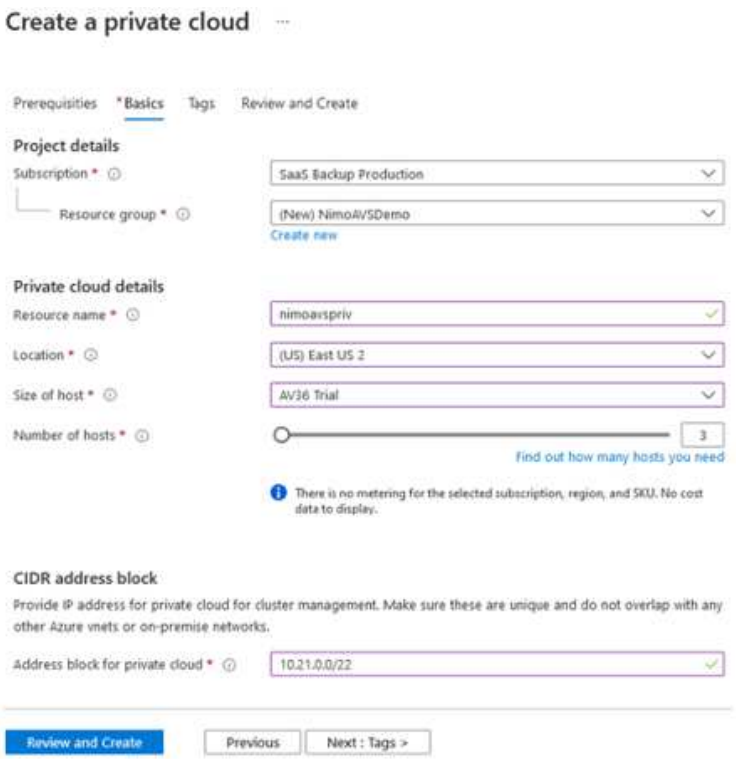




7. Une fois le fournisseur de ressources enregistré, créez un cloud privé Azure VMware Solution à l'aide du portail Azure.
8. Sign in au portail Azure.
9. Sélectionnez Créer une nouvelle ressource.
10. Dans la zone de texte Rechercher sur la place de marché, saisissez Azure VMware Solution et sélectionnez-la dans les résultats.
11. Sur la page Solution Azure VMware, sélectionnez Créer.
12. Dans l'onglet Bases, saisissez les valeurs dans les champs et sélectionnez Réviser + Créer.

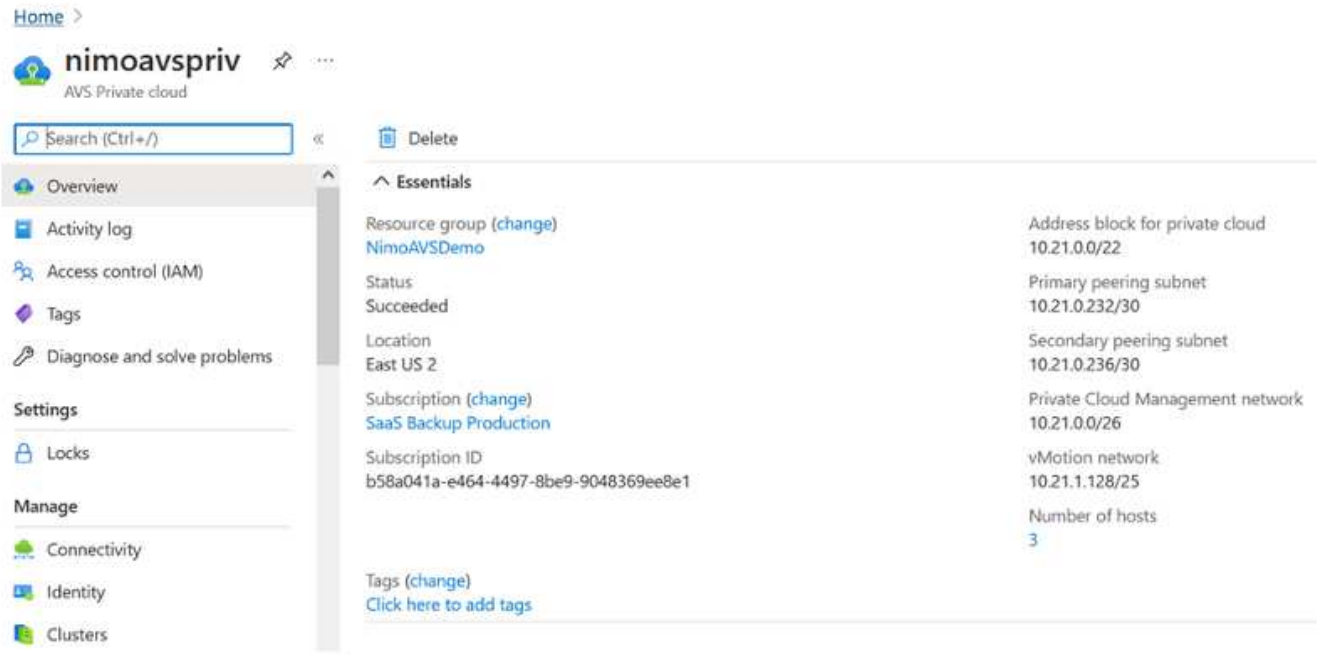
Remarques :

- Pour un démarrage rapide, rassemblez les informations nécessaires lors de 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 ne chevauche pas d'autres réseaux virtuels Azure ou réseaux locaux. Le CIDR représente le réseau de gestion du cloud privé et est 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 d'approvisionnement prend environ 4 à 5 heures. Une fois le processus terminé, vérifiez que le déploiement a réussi en accédant au cloud privé depuis le portail Azure. Un statut Réussi s'affiche lorsque le déploiement est terminé.

Un cloud privé Azure VMware Solution nécessite un réseau virtuel Azure. Étant donné qu'Azure VMware Solution ne prend pas en charge vCenter sur site, des étapes supplémentaires sont nécessaires pour l'intégration à un environnement sur site existant. La configuration d'un circuit ExpressRoute et d'une passerelle réseau virtuelle est également requise. En attendant la fin du provisionnement du cluster, créez un nouveau réseau virtuel ou utilisez-en un existant pour vous connecter à Azure VMware Solution.



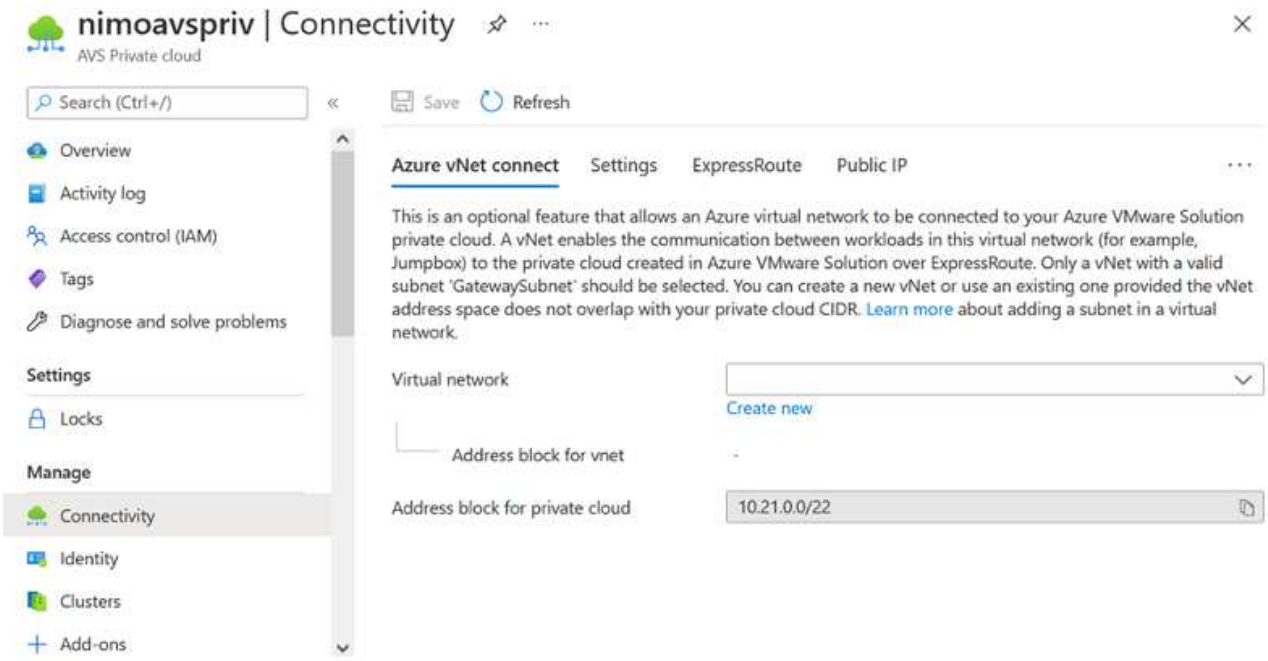
▼ **Connectez-vous à une passerelle de réseau virtuel ExpressRoute nouvelle ou existante**

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 Créer un réseau virtuel :

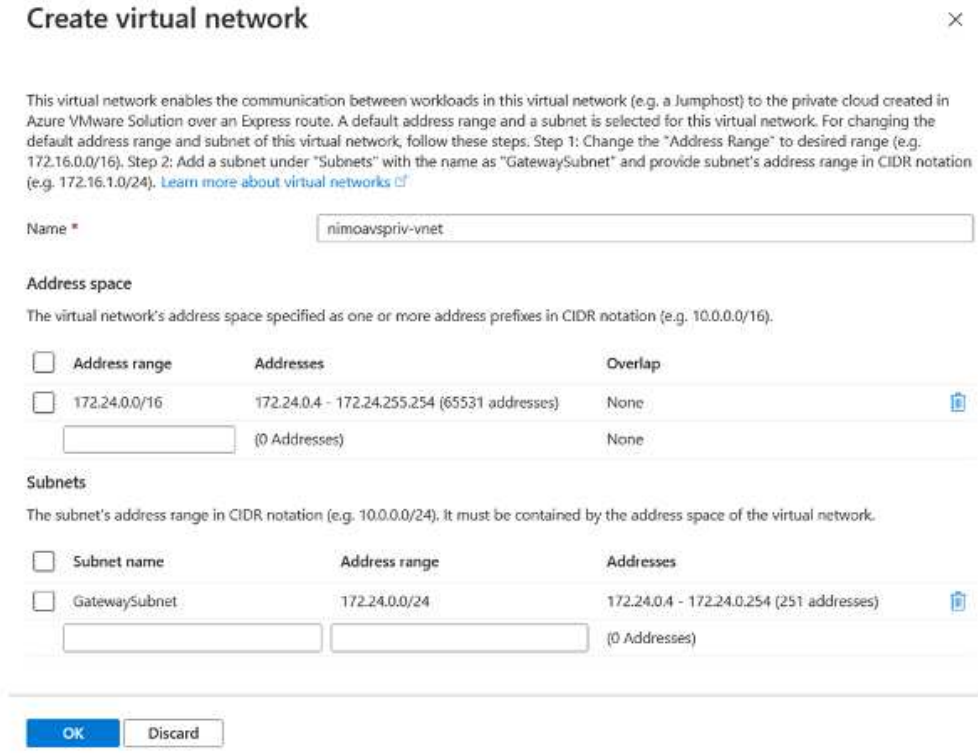
1. Accédez au cloud privé Azure VMware Solution et accédez à Connectivité sous l'option Gérer.
2. Sélectionnez Azure VNet Connect.
3. Pour créer un nouveau réseau virtuel, sélectionnez l'option Créer un nouveau.

   Cette fonctionnalité permet à un réseau virtuel d'être connecté au cloud privé Azure VMware Solution. Le VNet permet la communication entre les charges de travail de ce réseau virtuel en créant automatiquement les composants requis (par exemple, jump box, services partagés tels qu'Azure Azure NetApp Files et Cloud Volume ONTAP) dans le cloud privé créé dans Azure VMware Solution sur ExpressRoute.

   Remarque : l'espace d'adressage du réseau virtuel ne doit pas chevaucher le CIDR du cloud privé.



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



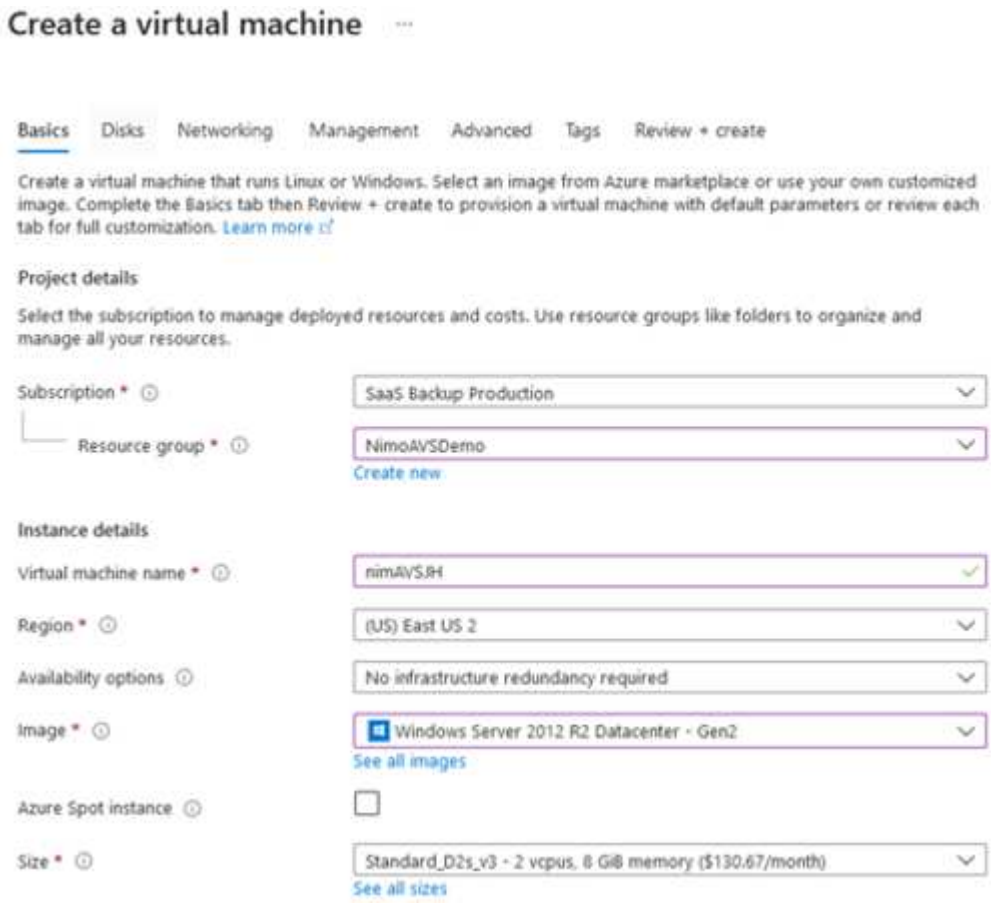
Le réseau virtuel avec la plage d'adresses et le sous-réseau de passerelle fournis est créé dans l'abonnement et le groupe de ressources désignés.

Si vous créez un réseau virtuel manuellement, créez une passerelle de réseau virtuel 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,

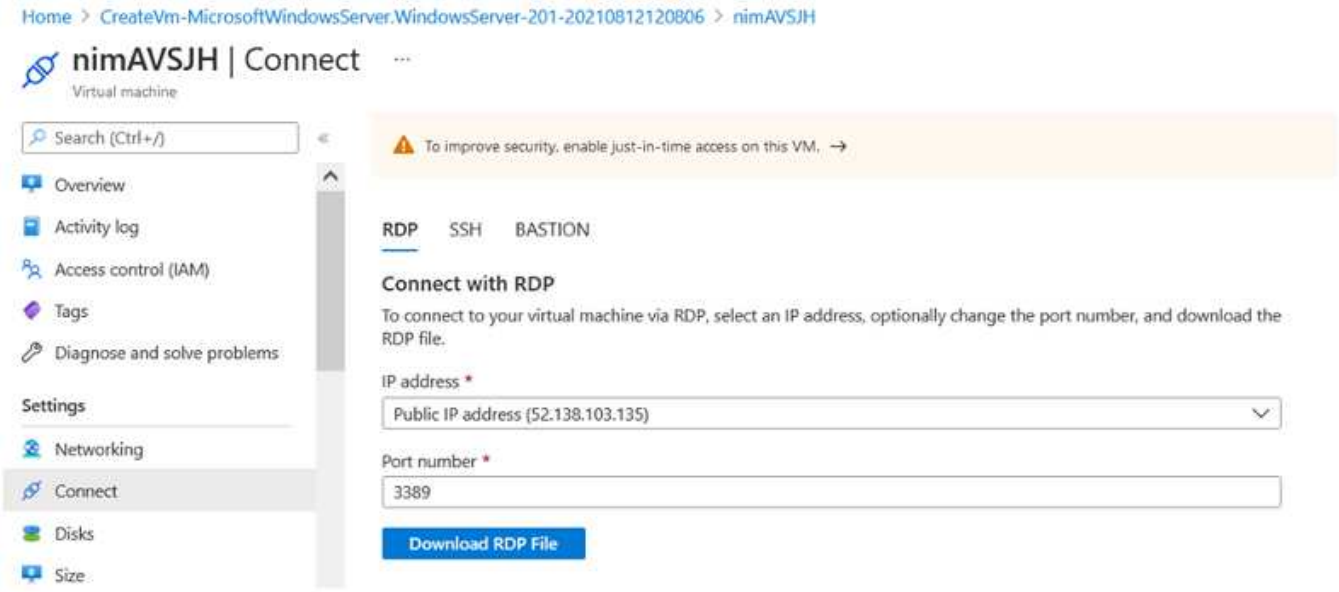
consultez la section "Configurer la mise en réseau de votre cloud privé VMware dans Azure" .

▼ **Valider la connexion réseau et l'accès au cloud privé Azure VMware Solution**

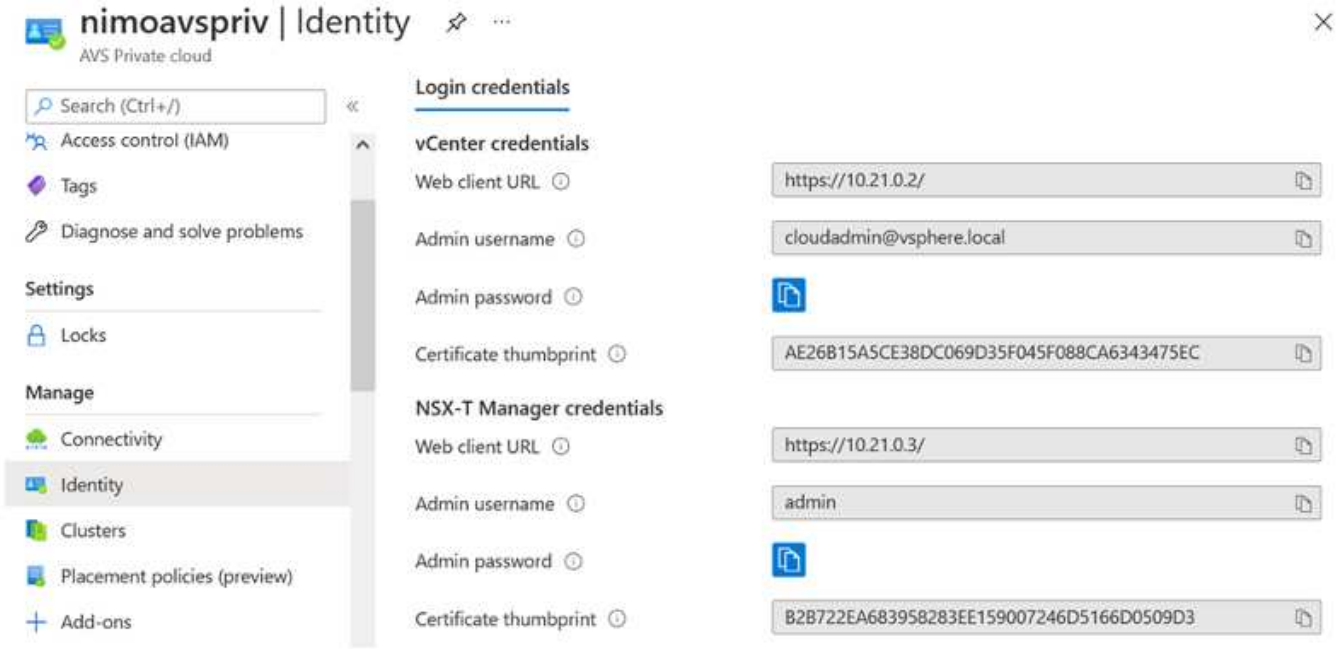
Azure VMware Solution ne vous permet pas de gérer un cloud privé avec VMware vCenter sur site. Au lieu de cela, un hôte de saut est requis pour se connecter à l'instance Azure VMware Solution vCenter. Créez un hôte de saut dans le groupe de ressources désigné et connectez-vous à Azure VMware Solution vCenter. Cet hôte de saut doit être une machine virtuelle Windows sur le même réseau virtuel qui a été créé pour la connectivité et doit fournir un accès à la fois à vCenter et à NSX Manager.



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



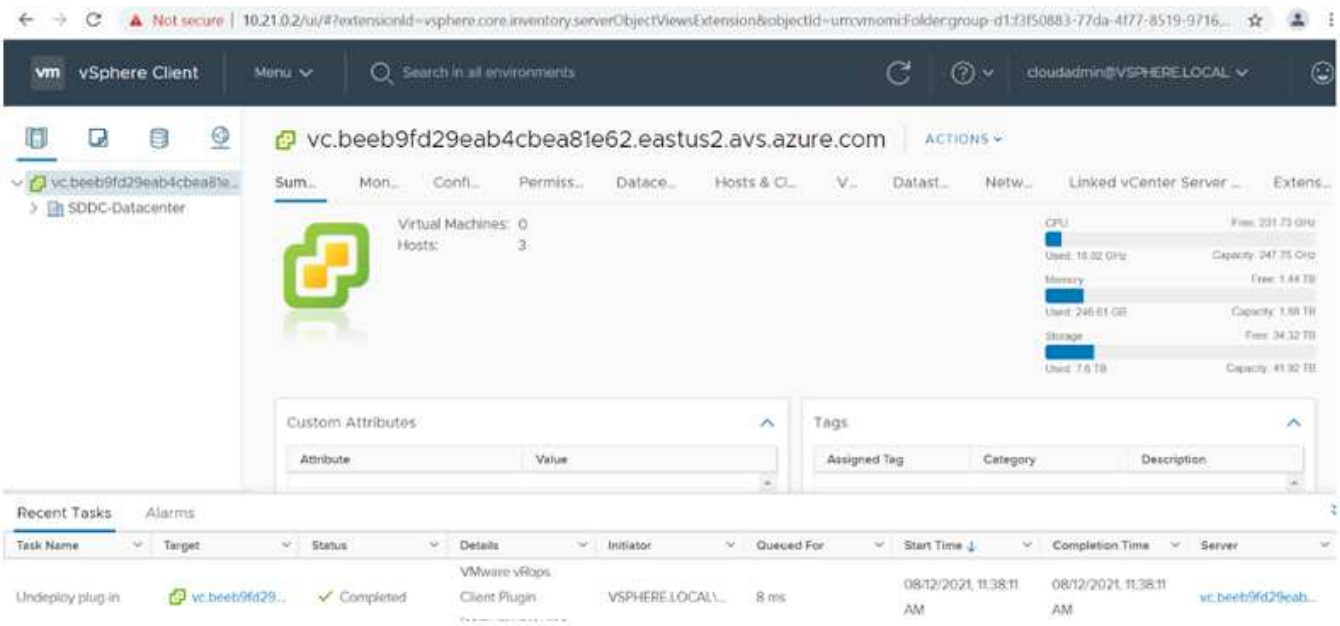
Sign in à vCenter à partir de cette machine virtuelle hôte de saut nouvellement créée à l'aide de l'utilisateur administrateur cloud. Pour accéder aux informations d'identification, accédez au portail Azure et accédez à Identité (sous l'option Gérer dans le cloud privé). Les URL et les informations d'identification utilisateur pour le cloud privé vCenter et NSX-T Manager peuvent être copiées à partir d'ici.



Dans la machine virtuelle Windows, ouvrez un navigateur et accédez à l'URL du client Web vCenter(`"https://10.21.0.2/"`) et utilisez le nom d'utilisateur administrateur comme **cloudadmin@vsphere.local** et collez le mot de passe copié. De même, le gestionnaire NSX-T est également accessible à l'aide de l'URL du client Web(`"https://10.21.0.3/"`) et utilisez le nom d'utilisateur administrateur 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 connecter l'environnement local au cloud privé Azure VMware Solution. Pour plus d'informations, consultez la section "Associez des environnements locaux à Azure VMware Solution" .

Déployer et configurer l'environnement de virtualisation sur Google Cloud Platform (GCP)

Comme sur site, la planification de Google Cloud VMware Engine (GCVE) est essentielle pour un environnement prêt pour la production pour la création de machines virtuelles et la migration.

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

Le processus de configuration peut être décomposé selon les étapes suivantes :

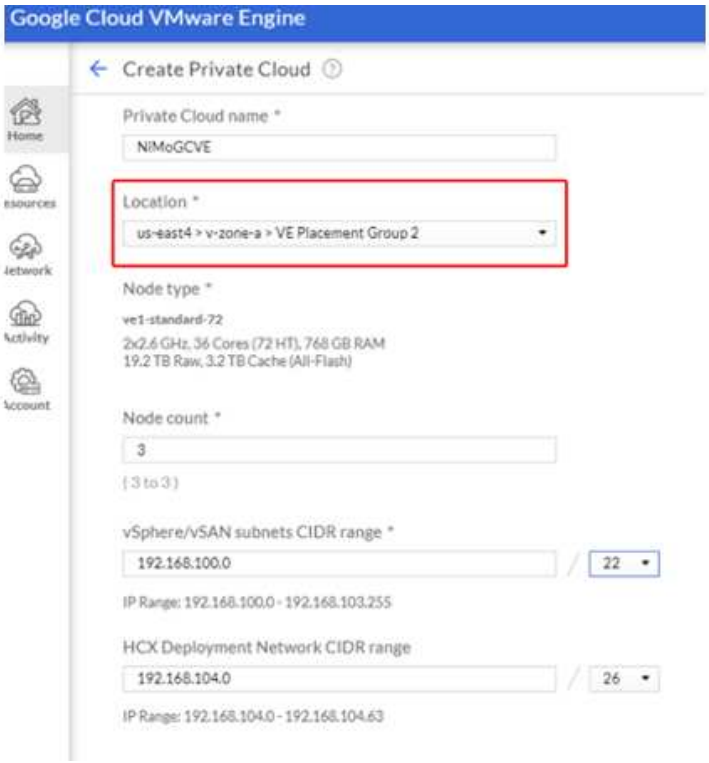
▼ **Déployer et configurer GCVE**

Pour configurer un environnement GCVE sur 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 « Emplacement », assurez-vous de déployer le cloud privé dans la même région/zone où NetApp Volumes/CVO est déployé, pour garantir les meilleures performances et la latence la plus faible.

Prérequis :

- Configurer le rôle IAM d'administrateur du service VMware Engine
- "Activer l'accès à l'API VMWare Engine et le quota de nœuds"
- Assurez-vous que la plage CIDR ne chevauche aucun de vos sous-réseaux locaux ou cloud. La plage CIDR doit être /27 ou supérieure.



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

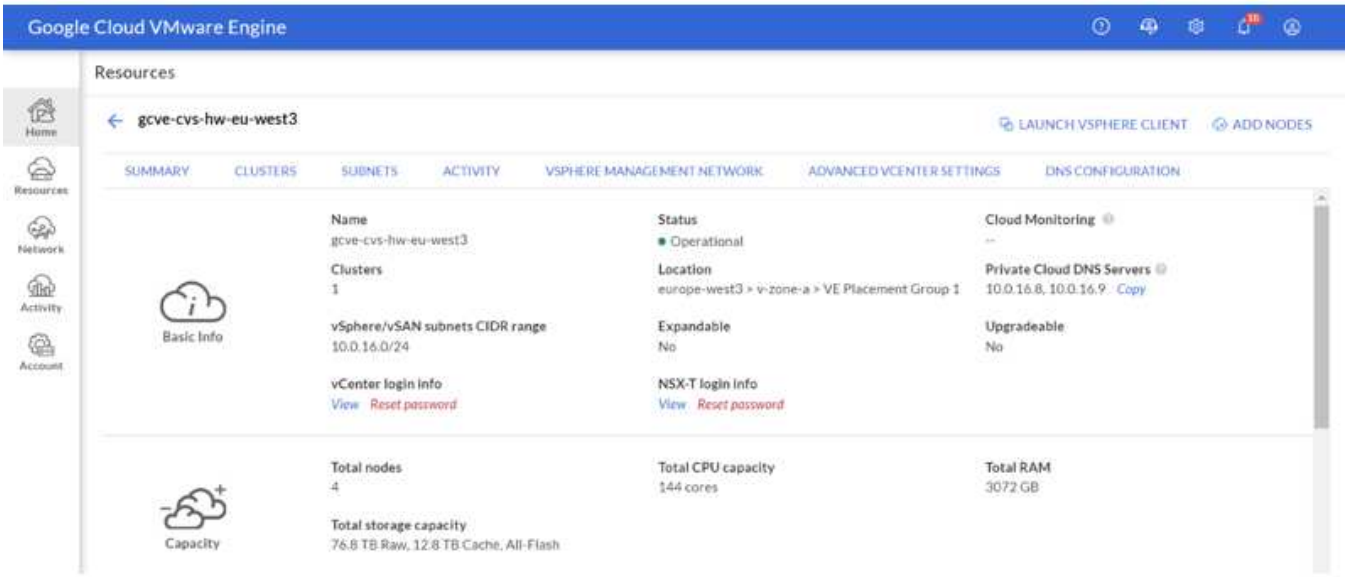
▼ **Activer l'accès privé à GCVE**

Une fois le cloud privé provisionné, configurez l'accès privé au cloud privé pour une connexion de chemin de données à haut débit et à faible latence.

Cela garantira que le réseau VPC sur lequel les instances Cloud Volumes ONTAP s'exécutent peut communiquer avec le cloud privé GCVE. Pour ce faire, suivez les "Documentation GCP". Pour le service Cloud Volume, établissez une connexion entre VMware Engine et Google Cloud NetApp Volumes en effectuant un peering unique entre les projets hôtes du locataire. Pour connaître les étapes détaillées, suivez ce "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

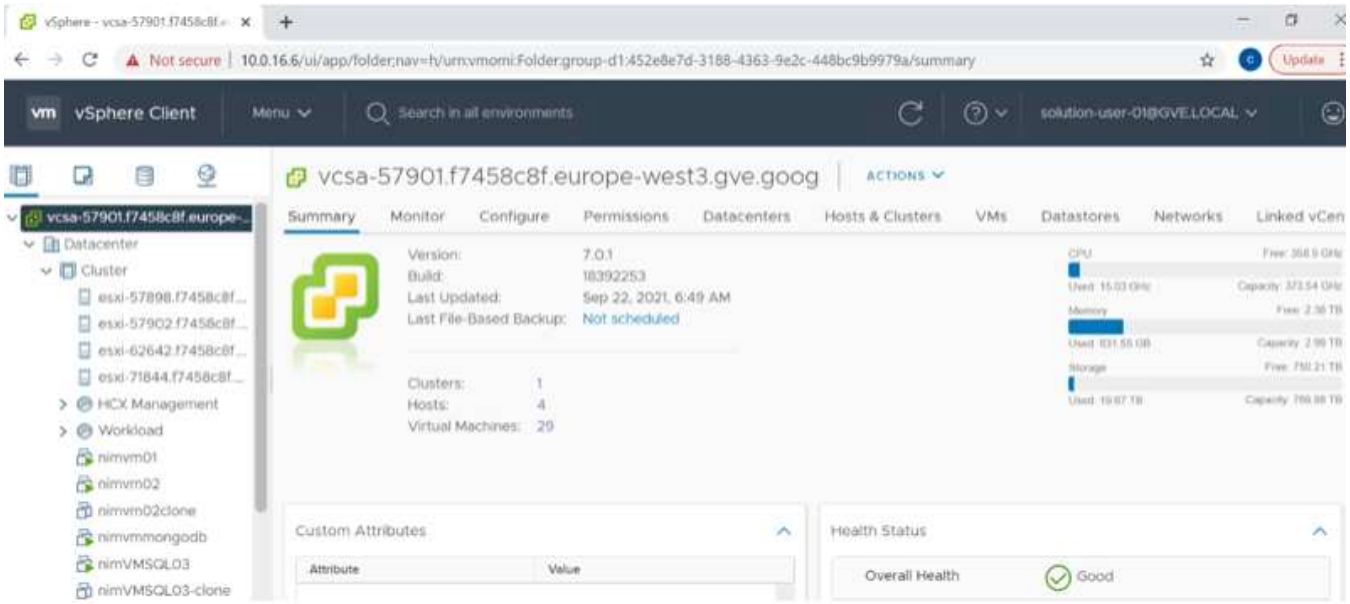
Sign in à vcenter à l'aide de l'utilisateur CloudOwner@gve.local. Pour accéder aux informations d'identification, accédez au portail VMware Engine, accédez à Ressources et sélectionnez le cloud privé approprié. Dans la section Informations de base, cliquez sur le lien Afficher pour obtenir les informations de connexion à vCenter (vCenter Server, HCX Manager) ou les informations de connexion à NSX-T (NSX Manager).



Dans une machine virtuelle Windows, ouvrez un navigateur et accédez à l'URL du client Web vCenter(`"https://10.0.16.6/"`) et utilisez le nom d'utilisateur administrateur comme CloudOwner@gve.local et collez le mot de passe copié. De même, le gestionnaire NSX-T est également accessible via l'URL du client Web(`"https://10.0.16.11/"`) et utilisez le nom d'utilisateur administrateur et collez le mot de passe copié pour créer de nouveaux segments ou modifier les passerelles de niveau existantes.

Pour vous connecter à partir d'un réseau local au cloud privé VMware Engine, utilisez le VPN cloud ou Cloud Interconnect pour une connectivité appropriée et assurez-vous que les ports requis sont ouverts. Pour les étapes détaillées, suivez ceci"lien" .





▼ **Déployer le magasin de données supplémentaire Google Cloud NetApp Volumes sur GCVE**

Référer"Procédure de déploiement d'une banque de données NFS supplémentaire avec des volumes NetApp sur GCVE"

Stockage NetApp dans les clouds publics

Options de stockage NetApp pour les fournisseurs de cloud public

Explorez 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 comme stockage connecté invité
- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- FSx ONTAP comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour VMC" . Voir le détail"options de banque de données NFS supplémentaires pour VMC" .

Azure / AVS

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

- Azure NetApp Files (ANF) en tant que stockage connecté invité
- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- Azure NetApp Files (ANF) comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour AVS" . Voir le détail"options de banque de données NFS supplémentaires pour AVS" .

GCP / GCVE

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

- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- Google Cloud NetApp Volumes (NetApp Volumes) en tant que stockage connecté invité
- Google Cloud NetApp Volumes (NetApp Volumes) comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour GCVE" . Voir le détail"options de banque de données NFS supplémentaires pour GCVE" .

En savoir plus sur"Prise en charge du magasin de données Google Cloud NetApp Volumes pour Google Cloud VMware Engine (blog NetApp)" ou"Comment utiliser Google Cloud NetApp Volumes comme banques de données pour Google Cloud VMware Engine (blog Google)"

Amazon Web Services : options d'utilisation du stockage NetApp

Le stockage NetApp peut être connecté aux services Web Amazon en tant que stockage invité connecté ou stockage supplémentaire.

Amazon FSx for NetApp ONTAP (FSx ONTAP) en tant que banque de données NFS supplémentaire

Amazon FSx ONTAP offre d'excellentes options pour déployer et gérer les charges de travail des applications ainsi que les services de fichiers tout en réduisant le coût total de possession en rendant les exigences de données transparentes pour la couche application. Quel que soit le cas d'utilisation, choisissez VMware Cloud sur AWS avec Amazon FSx ONTAP pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site vers AWS, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise. Il s'agit du même processus et des mêmes procédures familiers utilisés pour connecter le stockage.

Pour plus d'informations, veuillez visiter :

- "FSx ONTAP comme banque de données NFS supplémentaire : présentation"
- "Amazon FSx pour ONTAP comme banque de données supplémentaire"

Amazon FSx for NetApp ONTAP comme stockage connecté en tant qu'invité

Amazon FSx ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités, basé sur le système de fichiers ONTAP populaire de NetApp. FSx ONTAP combine les fonctionnalités, les performances, les capacités et les opérations API familières des systèmes de fichiers NetApp avec l'agilité, l'évolutivité et la simplicité d'un service AWS entièrement géré.

FSx ONTAP fournit un stockage de fichiers partagé riche en fonctionnalités, rapide et flexible, largement accessible à partir d'instances de calcul Linux, Windows et macOS exécutées dans AWS ou sur site. FSx ONTAP offre un stockage SSD (Solid State Drive) hautes performances avec des latences inférieures à la milliseconde. Avec FSx ONTAP, vous pouvez atteindre des niveaux de performances SSD pour votre charge de travail tout en payant pour le stockage SSD pour seulement une petite fraction de vos données.

La gestion de vos données avec FSx ONTAP est plus simple car vous pouvez prendre des instantanés, cloner et répliquer vos fichiers en un clic. De plus, FSx ONTAP hiérarchise automatiquement vos données vers un stockage élastique et moins coûteux, réduisant ainsi le besoin de provisionner ou de gérer la capacité.

FSx ONTAP fournit également un stockage hautement disponible et durable avec des sauvegardes

entièrement gérées et une prise en charge de la reprise après sinistre interrégionale. Pour faciliter la protection et la sécurisation de vos données, FSx ONTAP prend en charge les applications courantes de sécurité des données et d'antivirus.

Pour plus d'informations, veuillez visiter"FSx ONTAP comme stockage connecté aux invités"

Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités

Cloud Volumes ONTAP, ou CVO, est la solution de gestion de données cloud leader du secteur, basée sur le logiciel de stockage ONTAP de NetApp, disponible nativement sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version définie par logiciel d' ONTAP qui consomme du stockage natif dans le cloud, vous permettant d'avoir le même logiciel de stockage dans le cloud et sur site, réduisant ainsi le besoin de recycler votre personnel informatique dans de toutes nouvelles méthodes de gestion de vos données.

CVO offre aux clients la possibilité de déplacer de manière transparente les données de la périphérie vers le centre de données, vers le cloud et vice-versa, en rassemblant votre cloud hybride, le tout géré avec une console de gestion à volet unique, NetApp Cloud Manager.

De par sa conception, CVO offre des performances extrêmes et des capacités avancées de gestion des données pour satisfaire même vos applications les plus exigeantes dans le cloud.

Pour plus d'informations, veuillez visiter"CVO comme stockage connecté aux invités" .

TR-4938 : Monter Amazon FSx ONTAP en tant que banque de données NFS avec VMware Cloud sur AWS

Ce document décrit comment monter Amazon FSx ONTAP en tant que banque de données NFS avec VMware Cloud sur AWS.

Introduction

Toute organisation qui réussit est sur la voie 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 explorer comment migrer, déployer, étendre et assurer la reprise après sinistre des processus de la manière la plus transparente possible. Les clients qui migrent vers le cloud doivent évaluer les cas d'utilisation en termes d'élasticité et d'éclatement, de sortie du centre de données, de consolidation du centre de données, de scénarios de fin de vie, de fusions, d'acquisitions, etc.

Bien que VMware Cloud sur AWS soit l'option préférée de la majorité des clients, car il offre des capacités hybrides uniques au client, les options de stockage natives limitées ont limité son utilité pour les organisations ayant des charges de travail lourdes en stockage. Étant donné que le stockage est directement lié aux hôtes, la seule façon de faire évoluer le stockage est d'ajouter davantage d'hôtes, ce qui peut augmenter les coûts de 35 à 40 % ou plus pour les charges de travail gourmandes en stockage. Ces charges de travail nécessitent un stockage supplémentaire et des performances séparées, et non une puissance supplémentaire, mais cela signifie payer pour des hôtes supplémentaires. C'est ici que le "intégration récente" de FSx ONTAP est pratique pour les charges de travail gourmandes en stockage et en performances avec VMware Cloud sur AWS.

Considérons le scénario suivant : un client a besoin de huit hôtes pour la puissance (vCPU/vMem), mais il a également un besoin substantiel en stockage. D'après leur évaluation, ils ont besoin de 16 hôtes pour répondre aux besoins de stockage. Cela augmente le coût total de possession global car ils doivent acheter toute cette puissance supplémentaire alors qu'ils n'ont réellement besoin que de plus de stockage. Ceci s'applique à tout cas d'utilisation, y compris la migration, la reprise après sinistre, le bursting, le

développement/test, etc.

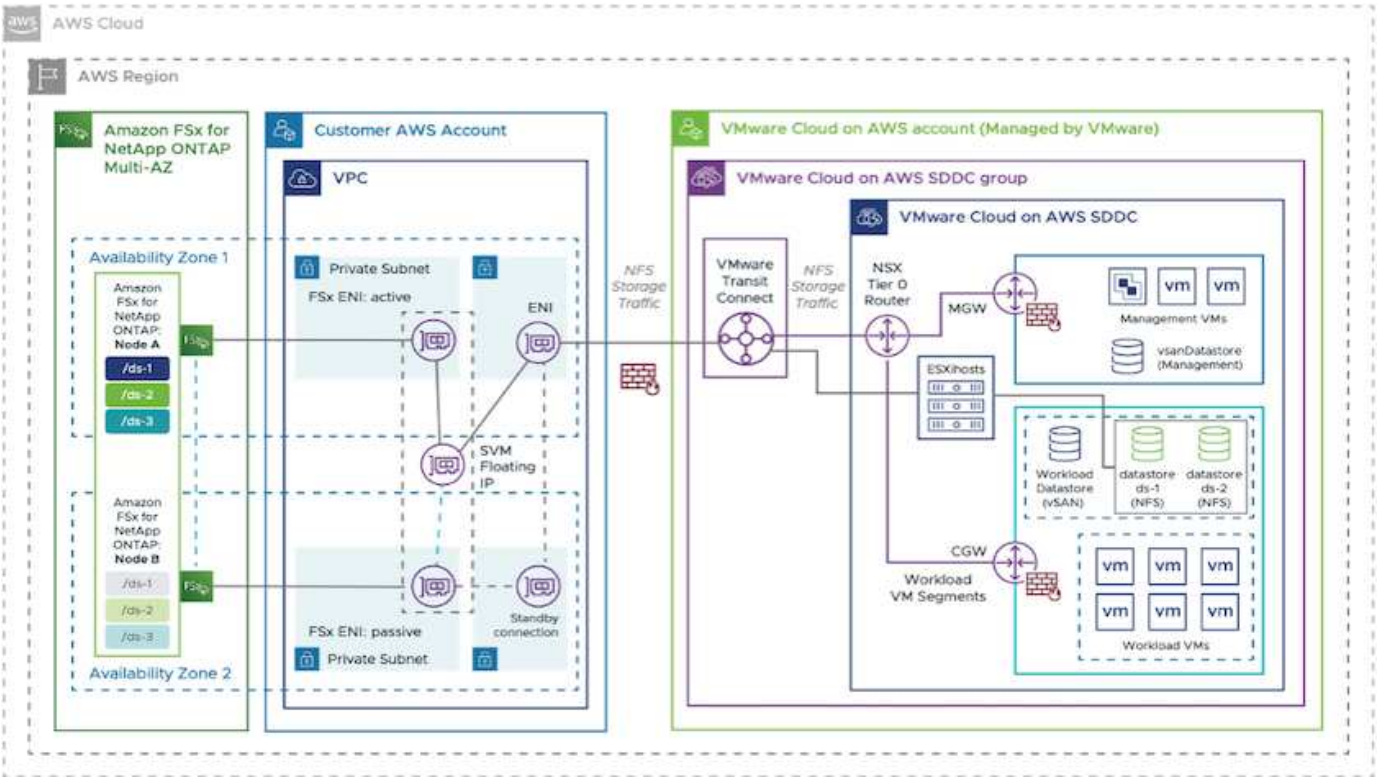
Ce document vous guide à travers les étapes nécessaires pour provisionner et attacher FSx ONTAP en tant que banque de données NFS pour VMware Cloud sur AWS.

Cette solution est également disponible auprès de VMware. Veuillez visiter le"Documentation VMware Cloud sur AWS" pour plus d'informations.

Options de connectivité

VMware Cloud sur AWS prend en charge les déploiements multi-AZ et mono-AZ de FSx ONTAP.

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



Les étapes de déploiement de haut niveau sont les suivantes :

1. Créez Amazon FSx ONTAP dans un nouveau VPC désigné.
2. Créer un groupe SDDC.
3. Créez VMware Transit Connect et une pièce jointe TGW.
4. Configurez le routage (AWS VPC et SDDC) et les groupes de sécurité.
5. Attachez un volume NFS en tant que banque de données au cluster SDDC.

Avant de provisionner et d'attacher FSx ONTAP en tant que banque de données NFS, vous devez d'abord configurer un environnement SDDC VMware on Cloud ou obtenir une mise à niveau d'un SDDC existant vers la version 1.20 ou supérieure. Pour plus d'informations, consultez le "Premiers pas avec VMware Cloud sur

AWS" .

FSx ONTAP n'est actuellement pas pris en charge avec les clusters étendus.

Conclusion

Ce document couvre les étapes nécessaires pour configurer Amazon FSx ONTAP avec VMware Cloud sur AWS. Amazon FSx ONTAP offre d'excellentes options pour déployer et gérer les charges de travail des applications ainsi que les services de fichiers tout en réduisant le coût total de possession en rendant les exigences de données transparentes pour la couche application. Quel que soit le cas d'utilisation, choisissez VMware Cloud sur AWS avec Amazon FSx ONTAP pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site vers AWS, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise. Il s'agit du même processus et des mêmes procédures familiers utilisés pour connecter le stockage. N'oubliez pas que seule la position des données a changé avec les nouveaux noms ; les outils et les processus restent tous les mêmes et Amazon FSx 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 ONTAP VMware Cloud

Création d'un magasin de données NFS supplémentaire dans AWS

Une fois que VMware Cloud est prêt et connecté à AWS VPC, vous devez déployer Amazon FSx ONTAP dans un VPC nouvellement désigné plutôt que dans le VPC par défaut connecté d'origine ou existant.

Pour commencer, déployez un VPC supplémentaire dans la même région et la même zone de disponibilité où réside SDDC, puis déployez Amazon FSx ONTAP dans le nouveau VPC. "Configuration d'un groupe SDDC dans VMware Cloud" la console active les options de configuration réseau requises pour se connecter au VPC nouvellement désigné où FSx ONTAP sera déployé.

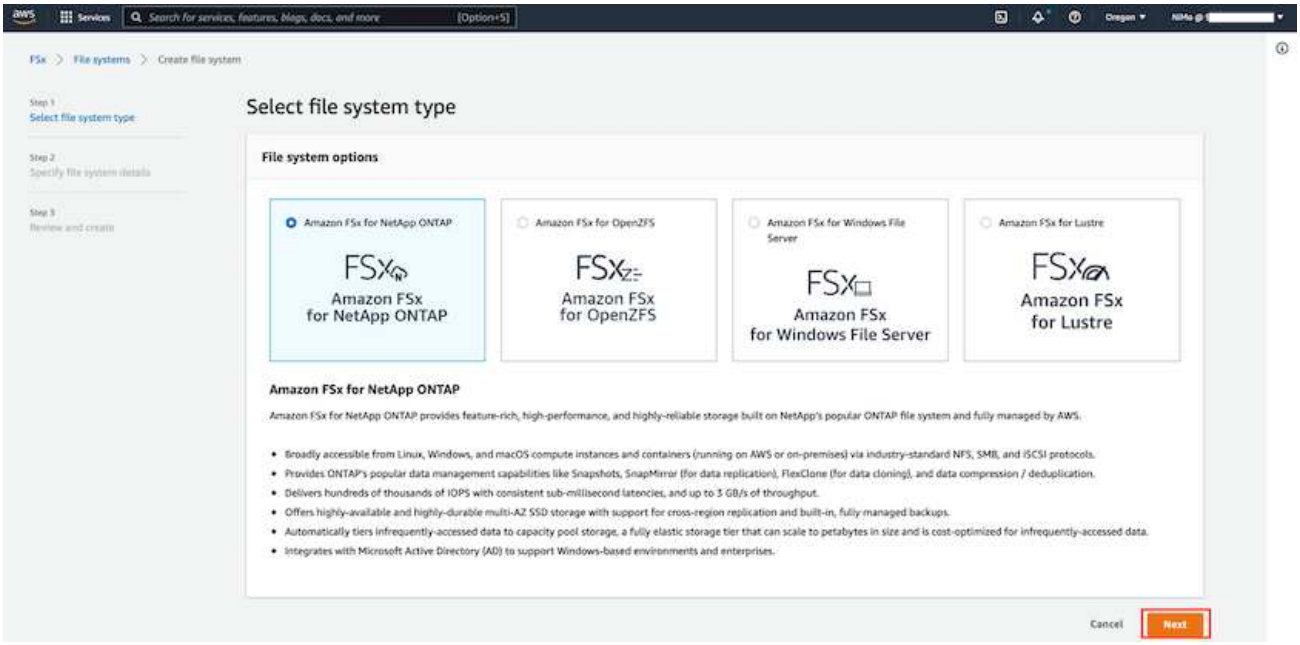
Déployez FSx ONTAP dans la même zone de disponibilité que VMware Cloud sur AWS SDDC.

Vous ne pouvez pas déployer FSx ONTAP dans le VPC connecté. Au lieu de cela, vous devez le déployer dans un nouveau VPC désigné, puis connecter le VPC à une passerelle de transit gérée VMware (vTGW) via des groupes SDDC.

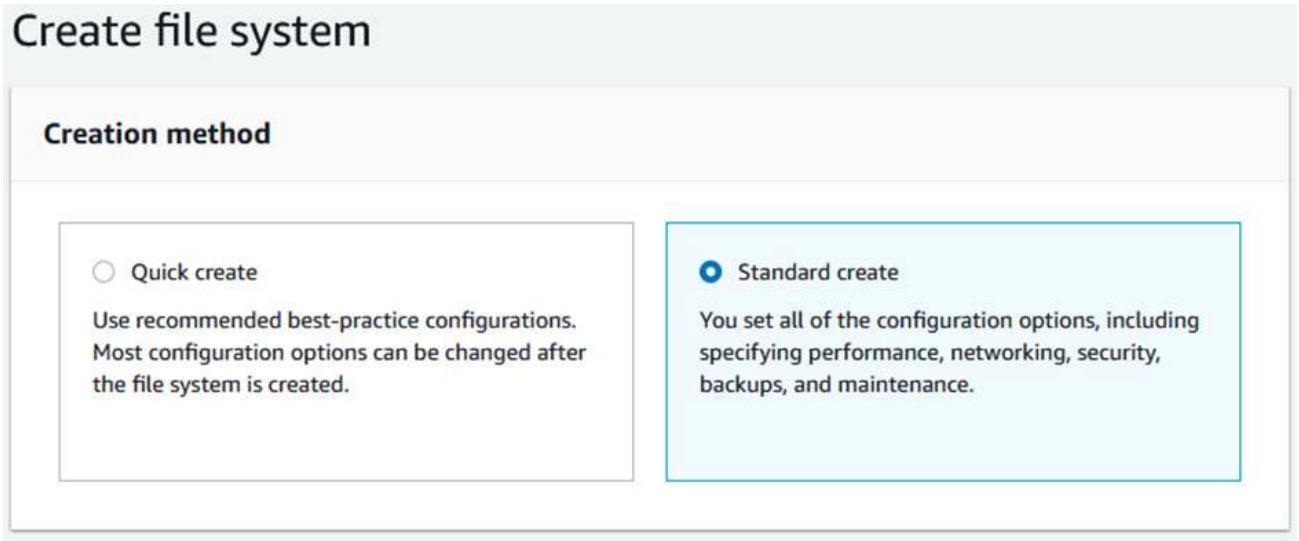
▼ **Étape 1 : créer Amazon FSx ONTAP dans un nouveau VPC désigné**

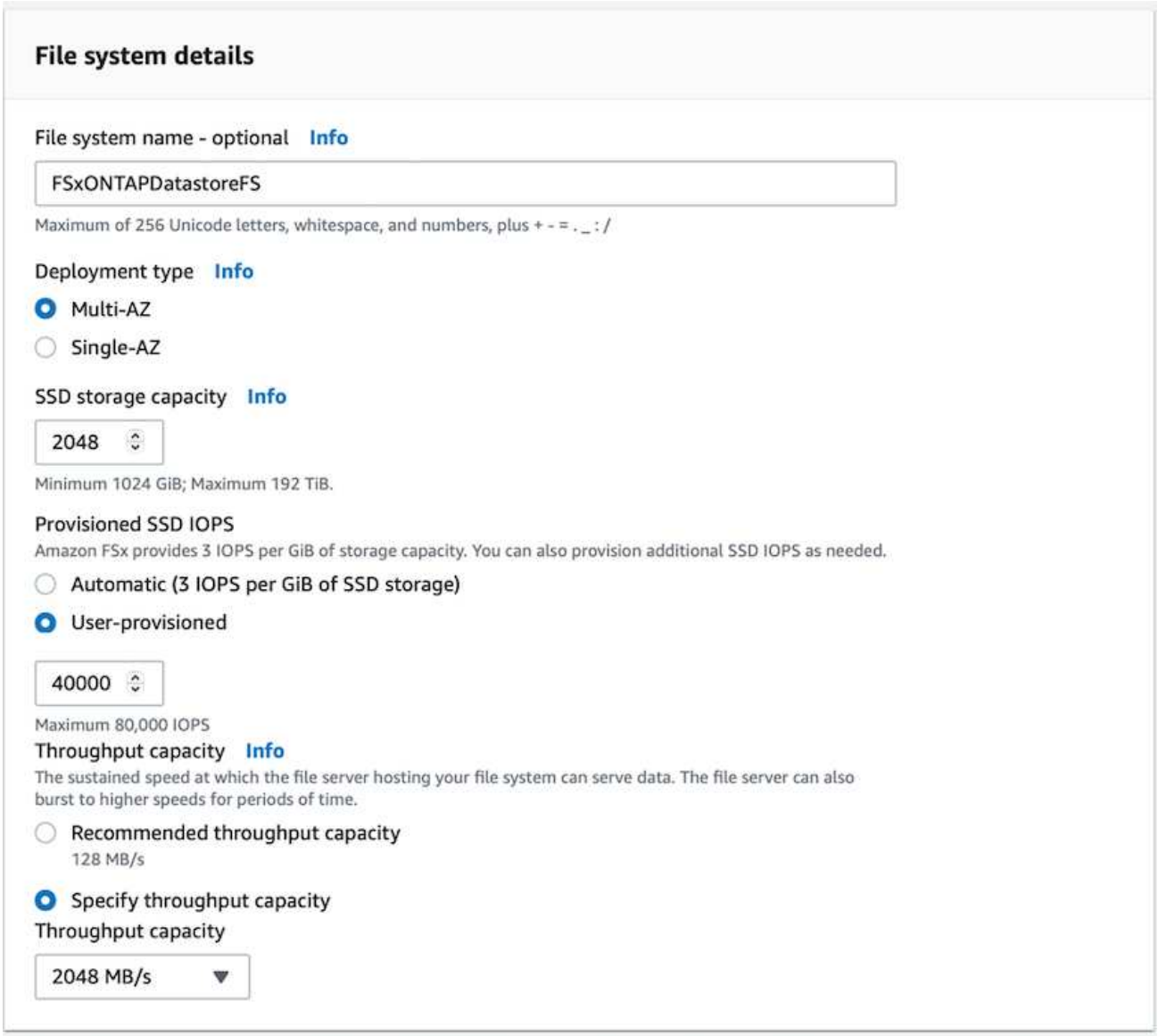
Pour créer et monter le système de fichiers Amazon FSx ONTAP , procédez comme suit :

1. Ouvrez la console Amazon FSx à `https://console.aws.amazon.com/fsx/` et choisissez **Créer un système de fichiers** pour démarrer l'assistant **Création de système de fichiers**.
2. Sur la page Sélectionner le type de système de fichiers, sélectionnez * Amazon FSx ONTAP*, puis cliquez sur **Suivant**. La page **Créer un système de fichiers** apparaît.



3. Pour la méthode de création, choisissez **Création standard**.





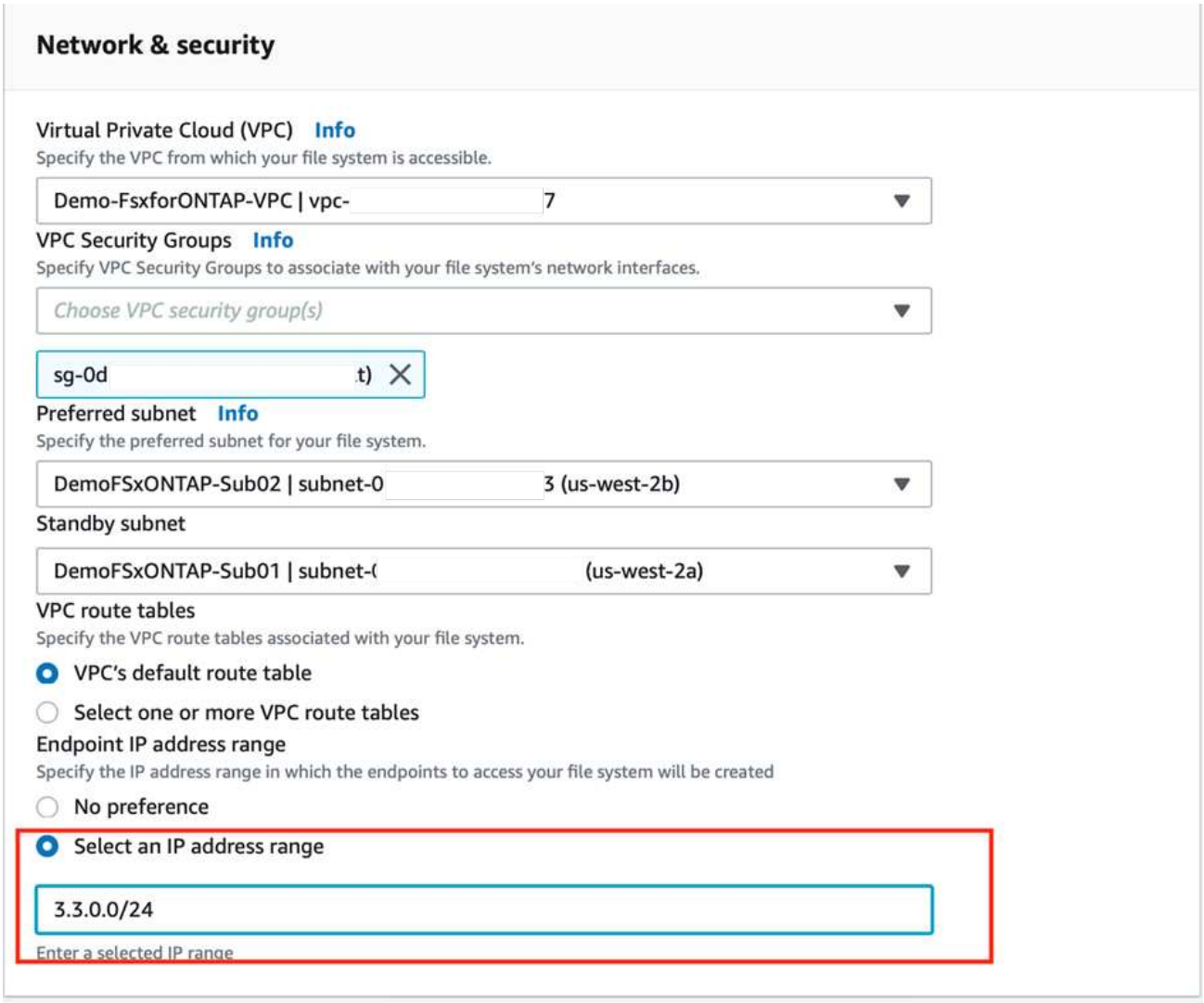
Les tailles des magasins de données varient considérablement d'un client à l'autre. Bien que le nombre recommandé de machines virtuelles par banque de données NFS soit subjectif, de nombreux facteurs déterminent le nombre optimal de machines virtuelles pouvant être placées sur chaque banque de données. Bien que la plupart des administrateurs ne prennent en compte que la capacité, la quantité d'E/S simultanées envoyées aux VMDK est l'un des facteurs les plus importants pour les performances globales. Utilisez les statistiques de performances locales pour dimensionner les volumes de la banque de données en conséquence.

4. Dans la section **Réseau** pour Virtual Private Cloud (VPC), choisissez le VPC approprié et les sous-réseaux préférés ainsi que la table de routage. Dans ce cas, Demo-FSxforONTAP-VPC est sélectionné dans le menu déroulant.

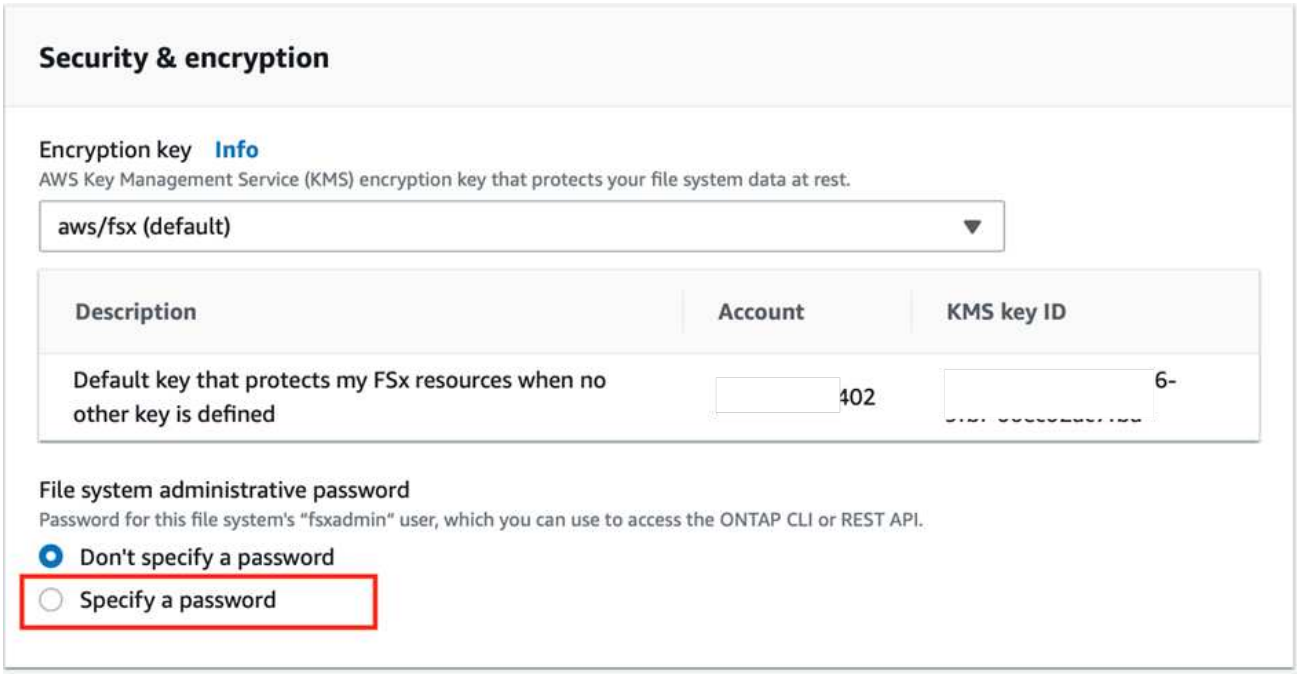
Assurez-vous qu'il s'agit d'un nouveau VPC désigné et non du VPC connecté.

Par défaut, FSx ONTAP utilise 198.19.0.0/16 comme plage d'adresses IP de point de terminaison par défaut pour le système de fichiers. Assurez-vous que la plage d'adresses IP du point de terminaison n'entre pas en conflit avec le VMC sur le SDDC AWS, les

sous-réseaux VPC associés et l'infrastructure sur site. Si vous n'êtes pas sûr, utilisez une plage sans chevauchement et sans conflits.

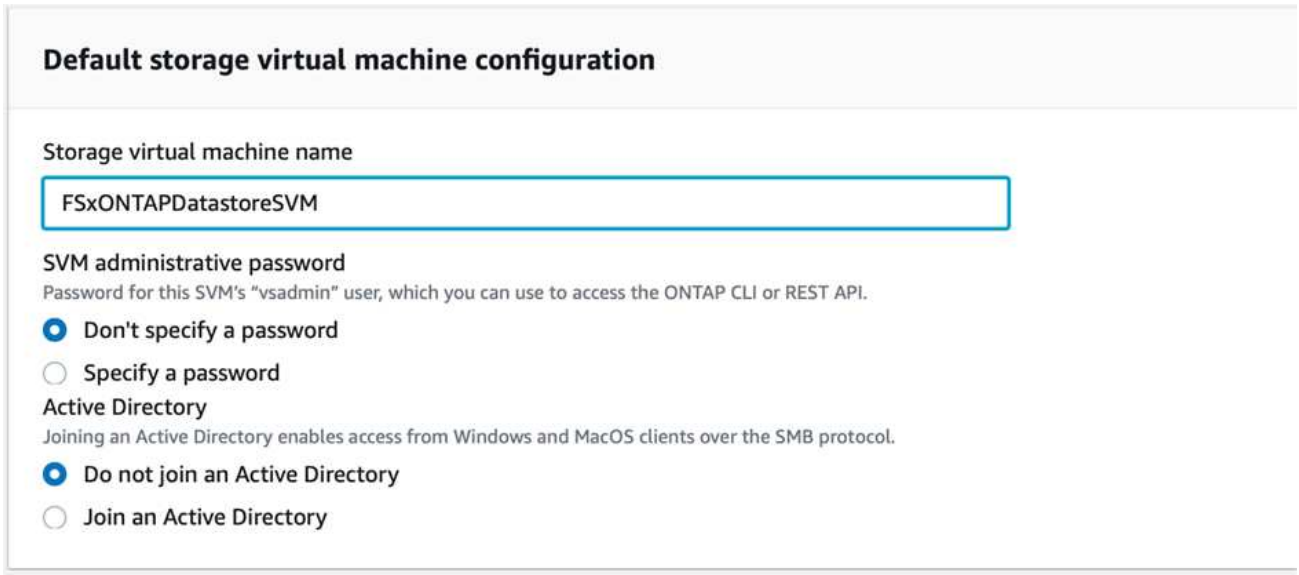


5. Dans la section **Sécurité et chiffrement** pour la clé de chiffrement, choisissez la clé de chiffrement AWS Key Management Service (AWS KMS) qui protège les données du système de fichiers au repos. Pour le **Mot de passe administratif du système de fichiers**, entrez un mot de passe sécurisé pour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



6. Dans la section **Configuration de la machine virtuelle de stockage par défaut**, spécifiez le nom de la SVM.

> À partir de GA, quatre magasins de données NFS sont pris en charge.



7. Dans la section **Configuration du volume par défaut**, spécifiez le nom du volume et la taille requis pour la banque de données et cliquez sur **Suivant**. Il doit s'agir d'un volume NFSv3. Pour **Efficacité du stockage**, choisissez **Activé** pour activer les fonctionnalités d'efficacité du stockage ONTAP (compression, déduplication et compactage). Après la création, utilisez le shell pour modifier les paramètres du volume en utilisant ***volume modify*** comme suit :

Paramètre	Configuration
Garantie de volume (style de garantie d'espace)	Aucun (provisionnement léger) – défini par défaut
réserve_fractionnelle (réserve-fractionnelle)	0% – défini par défaut

Paramètre	Configuration
snap_reserve (pourcentage d'espace d'instantané)	0%
Taille automatique (mode taille automatique)	grandir_rétrécir
Efficacité du stockage	Activé – défini par défaut
Suppression automatique	volume / le plus ancien en premier
Politique de hiérarchisation des volumes	Instantané uniquement – défini par défaut
essayez_en_premier	Auto-croissance
Politique d'instantané	Aucune

Utilisez la commande SSH suivante pour créer et modifier des volumes :

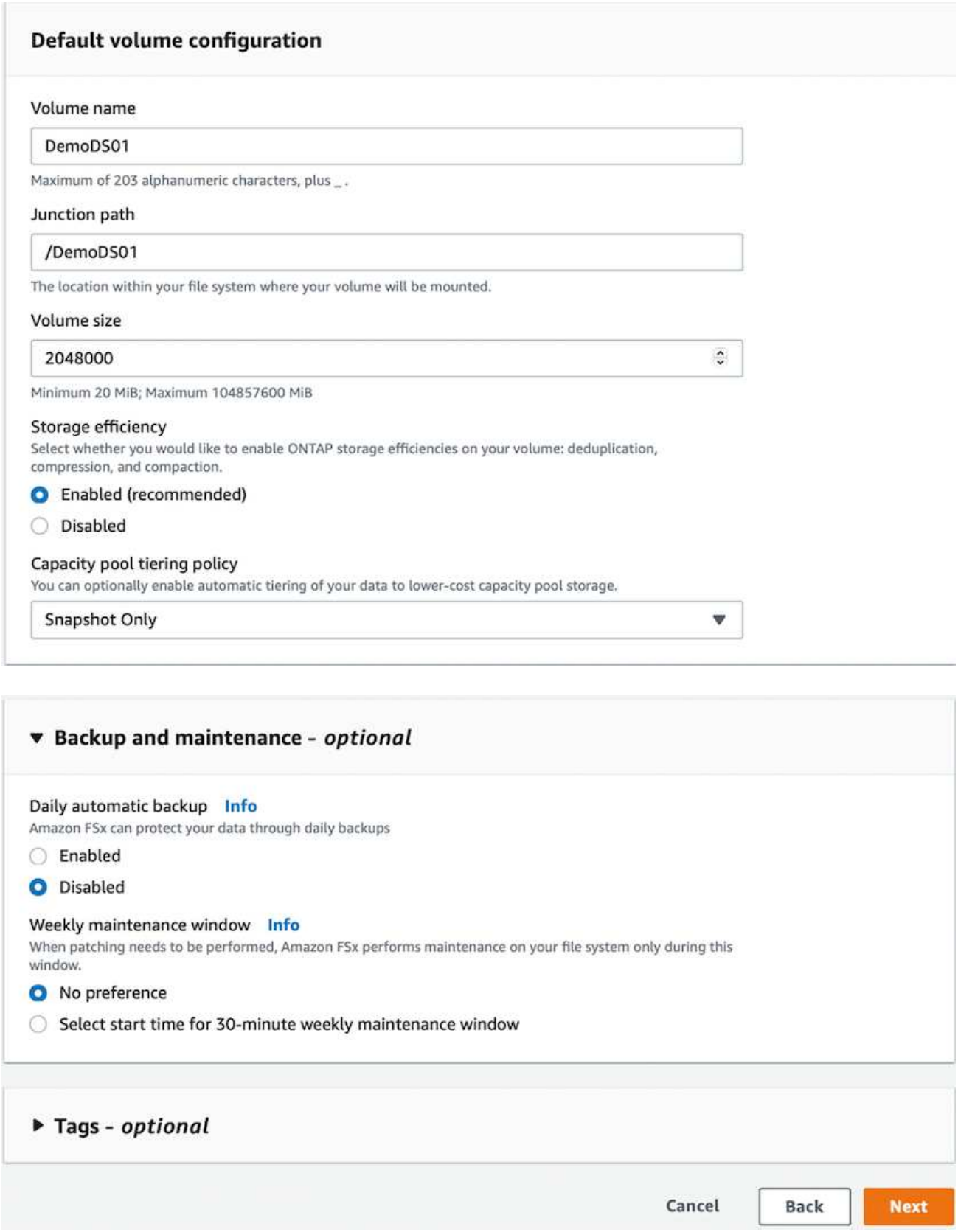
Commande pour créer un nouveau volume de banque de données à partir du shell :

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

Remarque : les volumes créés via le shell prendront quelques minutes pour apparaître dans la console AWS.

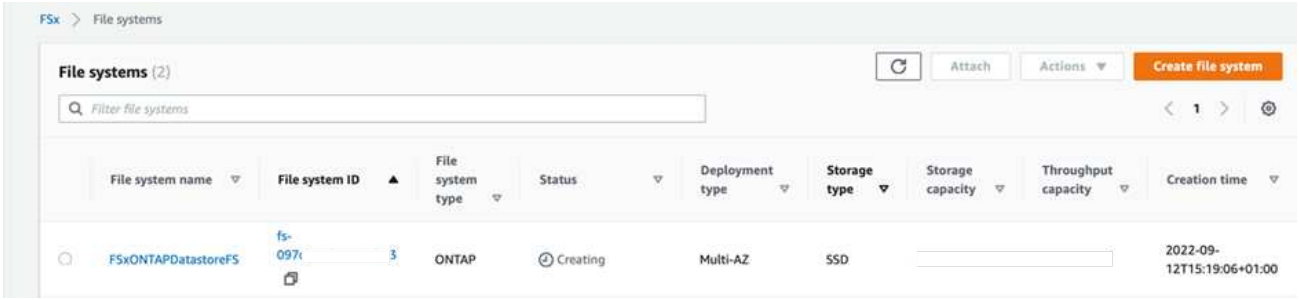
Commande pour modifier les paramètres de volume qui ne sont pas définis par défaut :

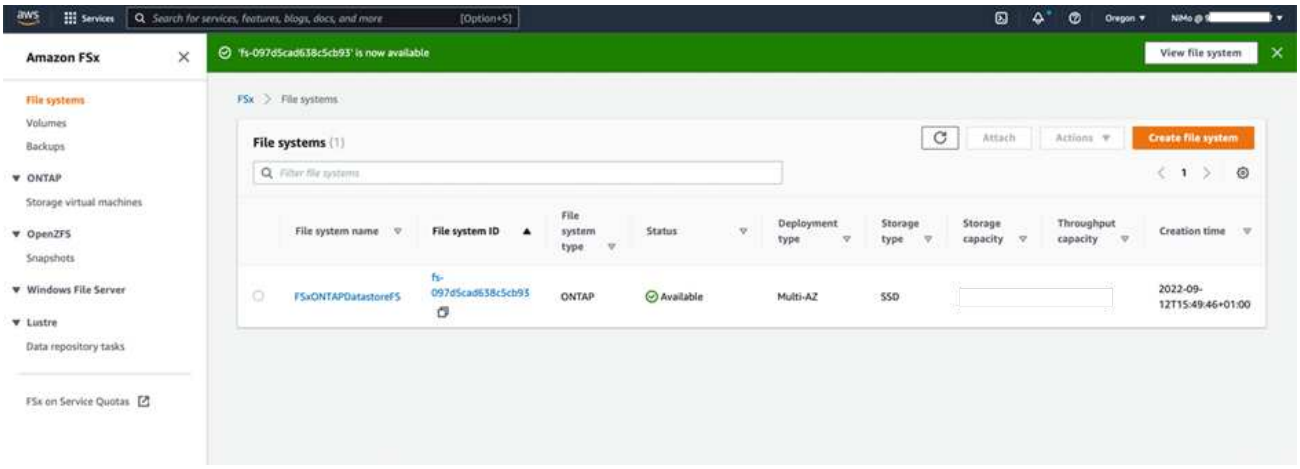
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```



Lors du scénario de migration initial, la stratégie de snapshot par défaut peut entraîner des problèmes de capacité de stockage de données complète. Pour y remédier, modifiez la politique de snapshot en fonction des besoins.

8. Vérifiez la configuration du système de fichiers affichée sur la page **Créer un système de fichiers**.
9. Cliquez sur **Créer un système de fichiers**.





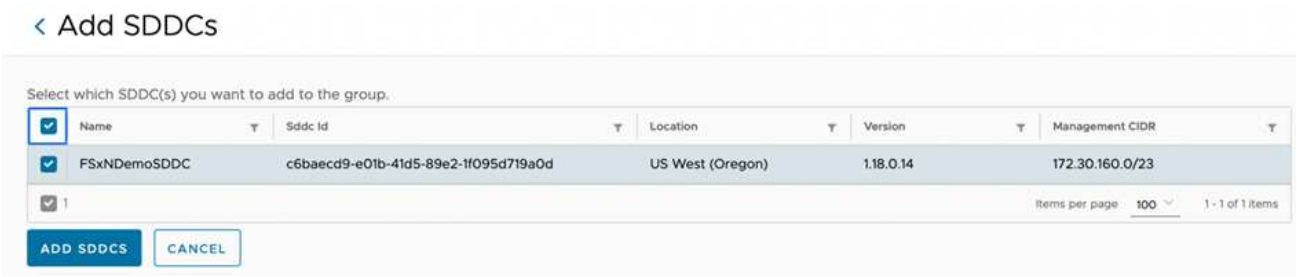
Répétez les étapes précédentes pour créer davantage de machines virtuelles de stockage ou de systèmes de fichiers et les volumes de banque de données en fonction des exigences de capacité et de performances.

Pour en savoir plus sur les performances Amazon FSx ONTAP , consultez "Performances Amazon FSx ONTAP" .

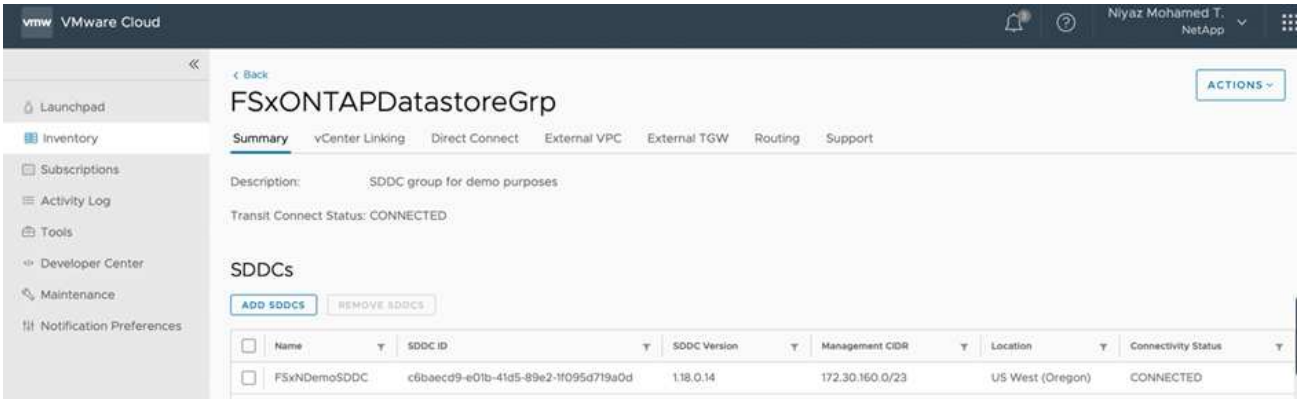
▼ Étape 2 : Créer un groupe SDDC

Une fois les systèmes de fichiers et les SVM créés, utilisez VMware Console pour créer un groupe SDDC et configurer VMware Transit Connect. Pour ce faire, procédez comme suit et n'oubliez pas que vous devez naviguer entre la console VMware Cloud et la console AWS.

1. Connectez-vous à la console VMC à `https://vmc.vmware.com` .
2. Sur la page **Inventaire**, cliquez sur **Groupes SDDC**.
3. Dans l'onglet **Groupes SDDC**, cliquez sur **ACTIONS** et sélectionnez **Créer un groupe SDDC**. À des fins de démonstration, le groupe SDDC est appelé `FSxONTAPDatastoreGrp` .
4. Dans la grille d'adhésion, sélectionnez les SDDC à inclure en tant que membres du groupe.

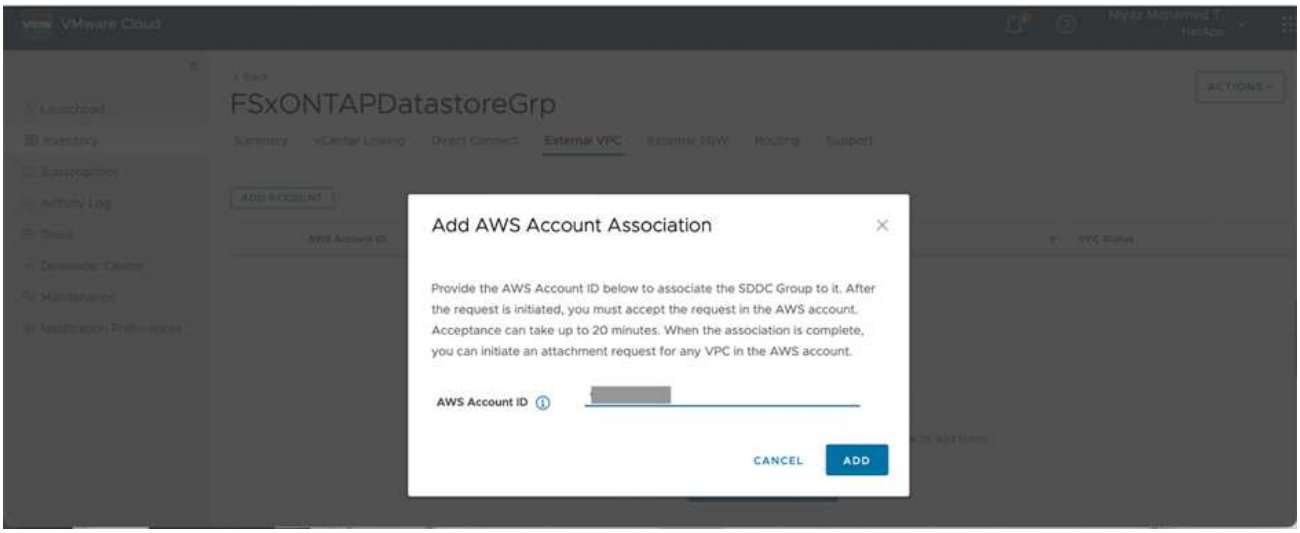


5. Vérifiez que « La configuration de VMware Transit Connect pour votre groupe entraînera des frais par pièce jointe et par transfert de données » est cochée, puis sélectionnez **Créer un groupe**. Le processus peut prendre quelques minutes.

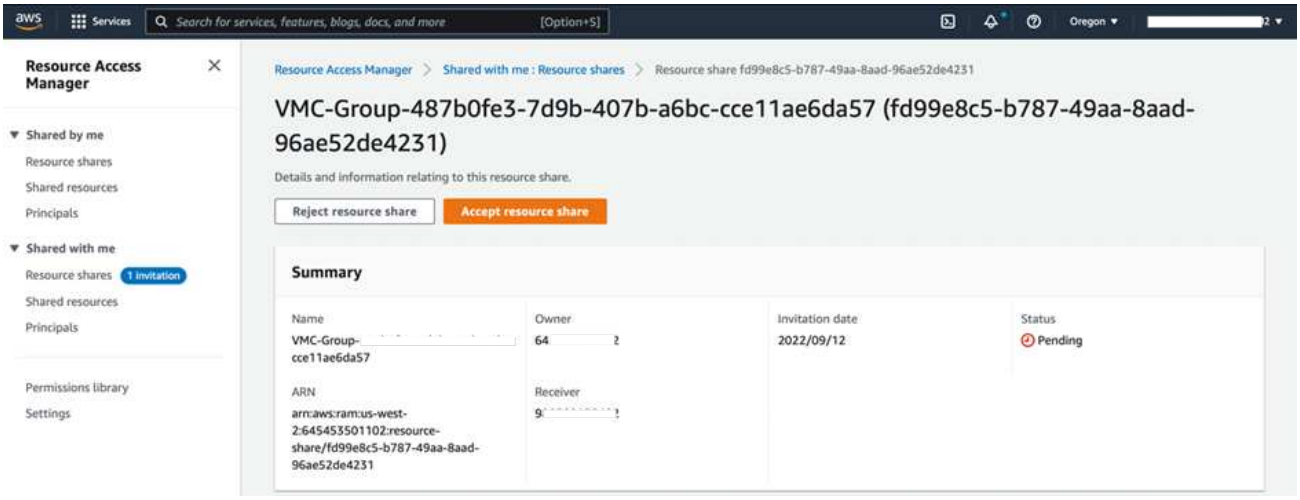


▼ **Étape 3 : Configurer VMware Transit Connect**

1. Attachez le VPC désigné nouvellement créé au groupe SDDC. Sélectionnez l'onglet **VPC externe** et suivez les "instructions pour attacher un VPC externe au groupe" . Ce processus peut prendre 10 à 15 minutes.

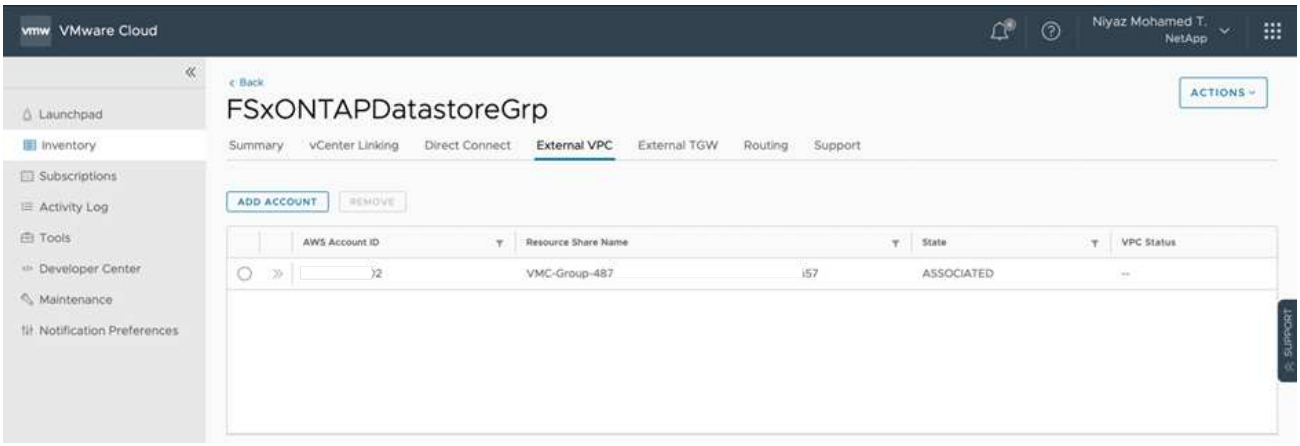


2. Cliquez sur **Ajouter un compte**.
   a. Fournissez le compte AWS qui a été utilisé pour provisionner le système de fichiers FSx ONTAP .
   b. Cliquez sur **Ajouter**.
3. De retour dans la console AWS, connectez-vous au même compte AWS et accédez à la page de service **Resource Access Manager**. Il y a un bouton pour vous permettre d'accepter le partage de ressources.



Dans le cadre du processus VPC externe, vous serez invité via la console AWS à accéder à une nouvelle ressource partagée via le gestionnaire d'accès aux ressources. La ressource partagée est la passerelle AWS Transit gérée par VMware Transit Connect.

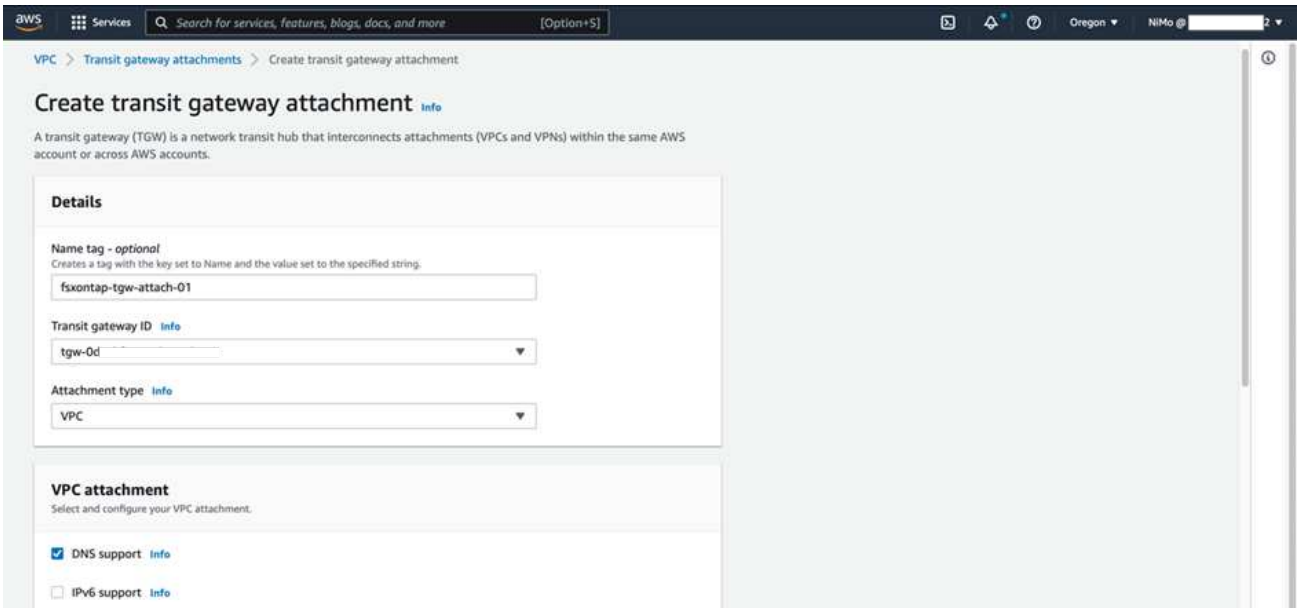
4. Cliquez sur **Accepter le partage de ressources**.



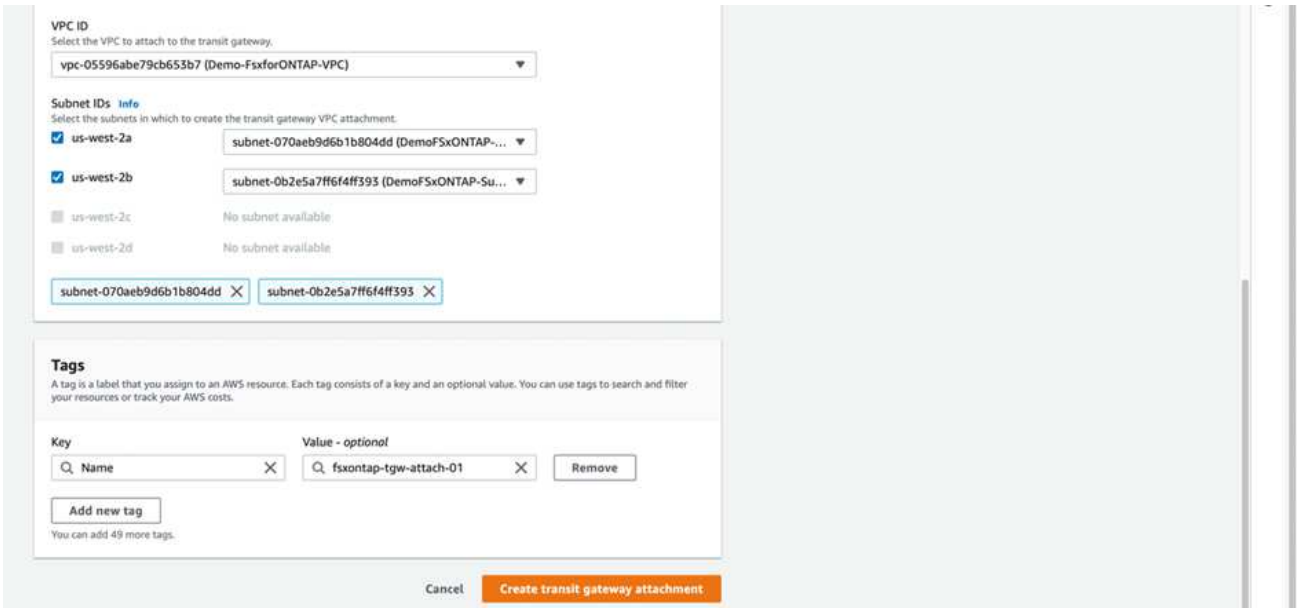
5. De retour dans la console VMC, vous voyez maintenant que le VPC externe est dans un état associé. Cela peut prendre plusieurs minutes pour apparaître.

▼ Étape 4 : Créer une pièce jointe de passerelle de transit

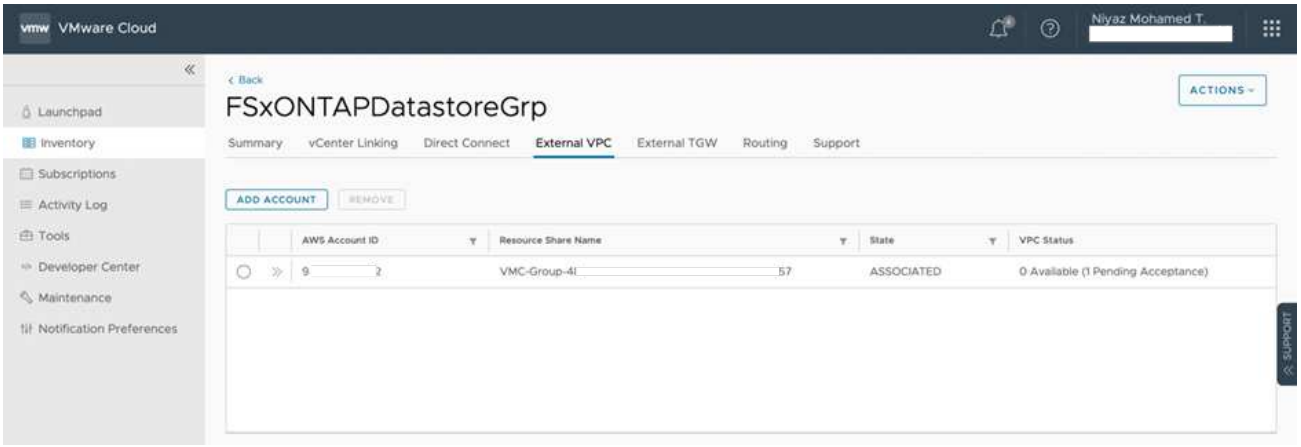
1. Dans la console AWS, accédez à la page du service VPC et accédez au VPC qui a été utilisé pour provisionner le système de fichiers FSx. Ici, vous créez une pièce jointe de passerelle de transit en cliquant sur **Pièce jointe de passerelle de transit** dans le volet de navigation à droite.
2. Sous **Pièce jointe VPC**, assurez-vous que la prise en charge DNS est cochée et sélectionnez le VPC dans lequel FSx ONTAP a été déployé.

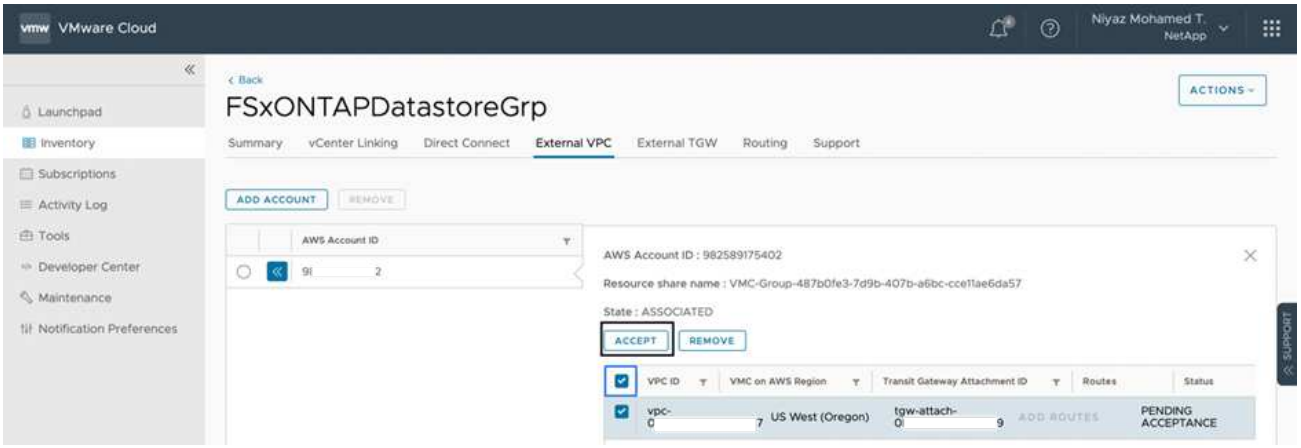


3. Cliquez sur **Créer une pièce jointe de passerelle de transit**.



4. De retour dans la console VMware Cloud, revenez à l'onglet Groupe SDDC > VPC externe. Sélectionnez l'ID de compte AWS utilisé pour FSx, cliquez sur le VPC et cliquez sur **Accepter**.

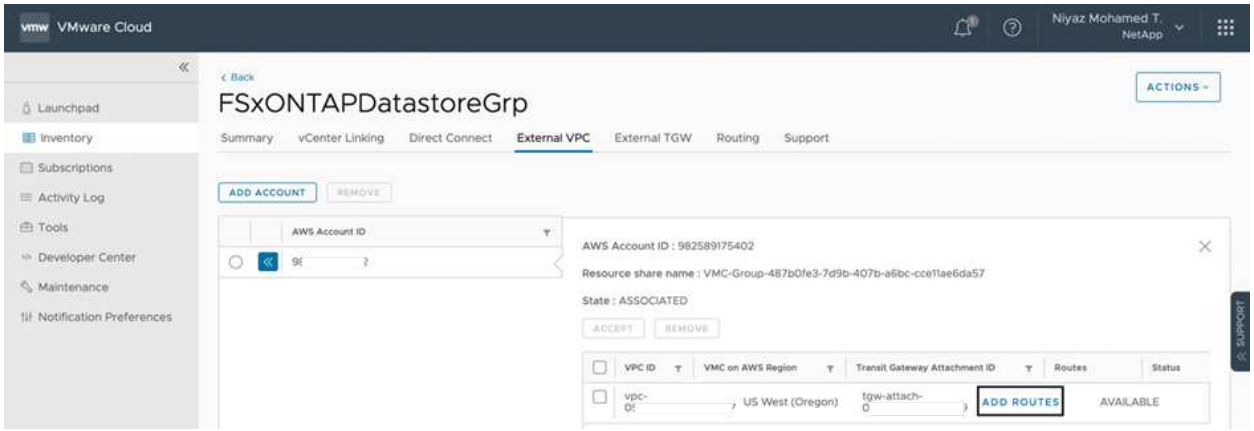


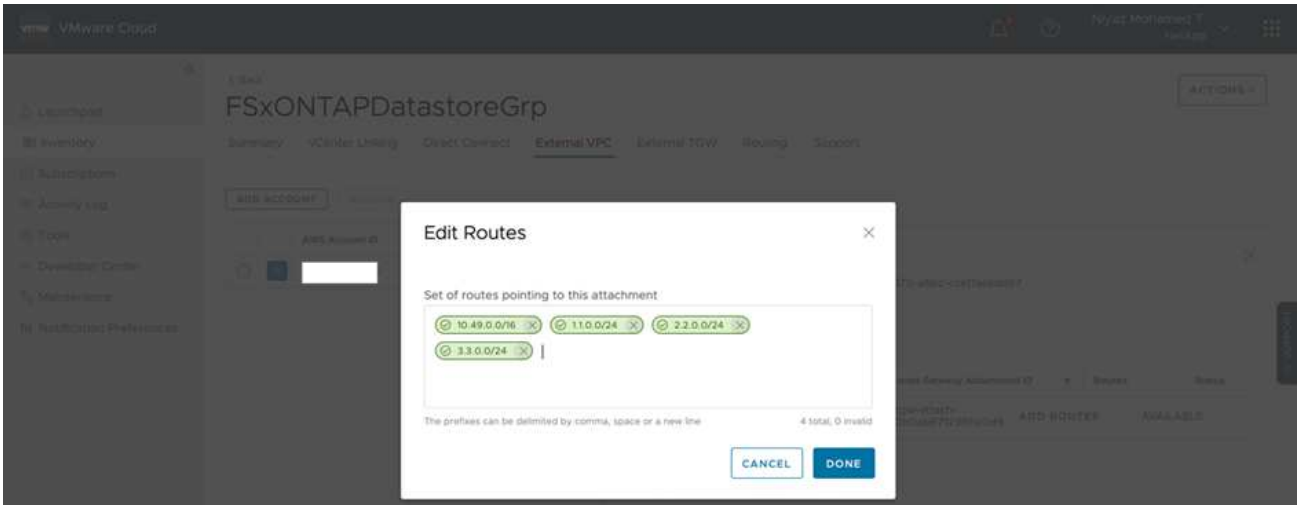


Cette option peut prendre plusieurs minutes à apparaître.

5. Ensuite, dans l'onglet **VPC externe** de la colonne **Routes**, cliquez sur l'option **Ajouter des routes** et ajoutez les routes requises :

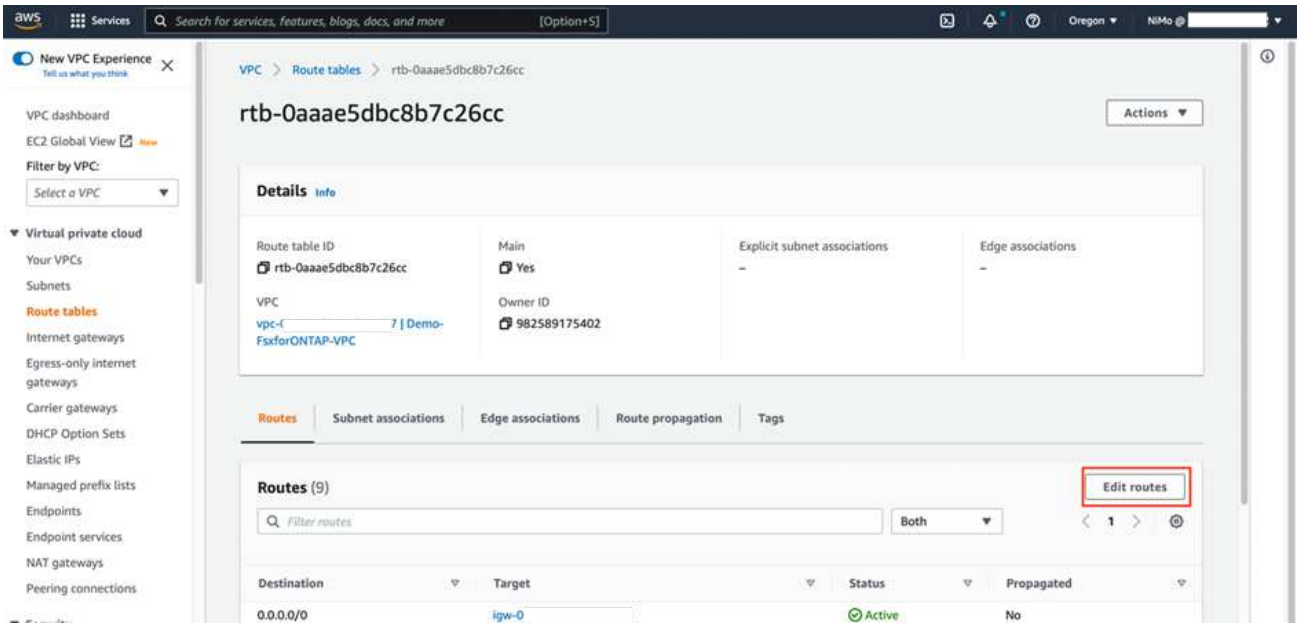
   - Un itinéraire pour la plage d'adresses IP flottantes pour les adresses IP flottantes Amazon FSx ONTAP .
   - Un itinéraire pour l'espace d'adressage VPC externe nouvellement créé.



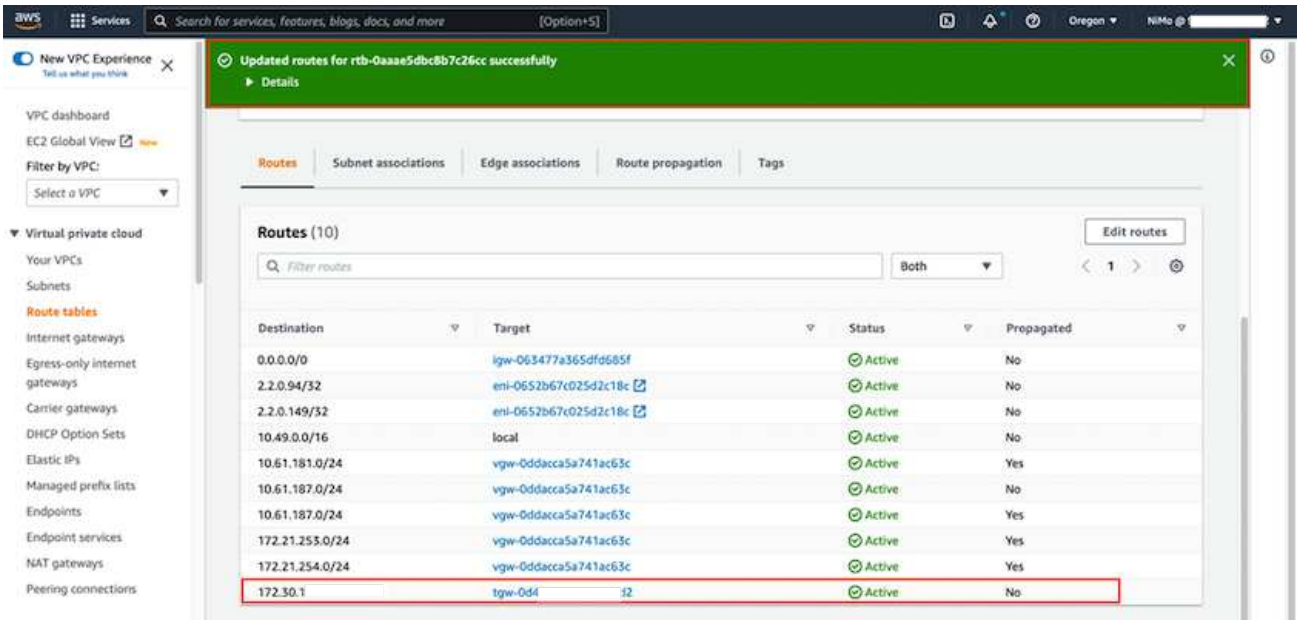


▼ **Étape 5 : Configurer le routage (AWS VPC et SDDC) et les groupes de sécurité**

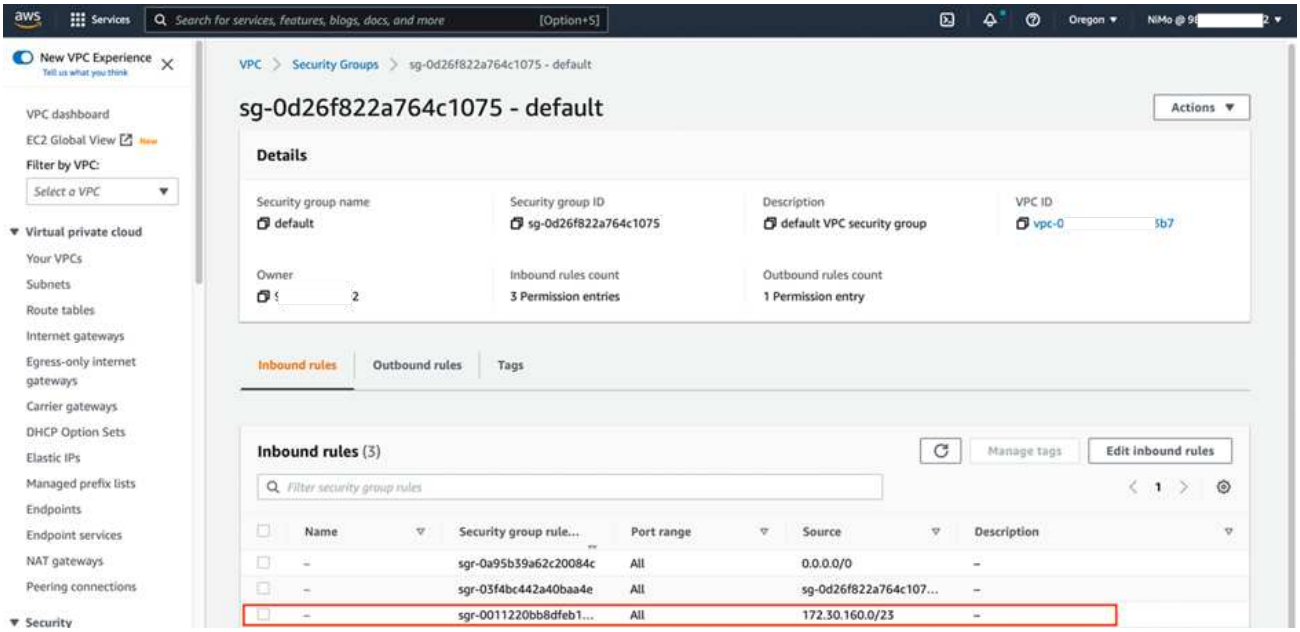
1. Dans la console AWS, créez la route de retour vers le SDDC en localisant le VPC dans la page de service VPC et sélectionnez la table de routage **principale** pour le VPC.
2. Accédez au tableau des itinéraires dans le panneau inférieur et cliquez sur **Modifier les itinéraires**.



3. Dans le panneau **Modifier les itinéraires**, cliquez sur **Ajouter un itinéraire** et saisissez le CIDR de l'infrastructure SDDC en sélectionnant **Passerelle de transit** et l'ID TGW associé. Cliquez sur **Enregistrer les modifications**.



4. L'étape suivante consiste à vérifier que le groupe de sécurité dans le VPC associé est mis à jour avec les règles entrantes correctes pour le CIDR du groupe SDDC.
5. Mettez à jour la règle entrante avec le bloc CIDR de l'infrastructure SDDC.



Vérifiez que la table de routage VPC (où réside FSx ONTAP) est mise à jour pour éviter les problèmes de connectivité.

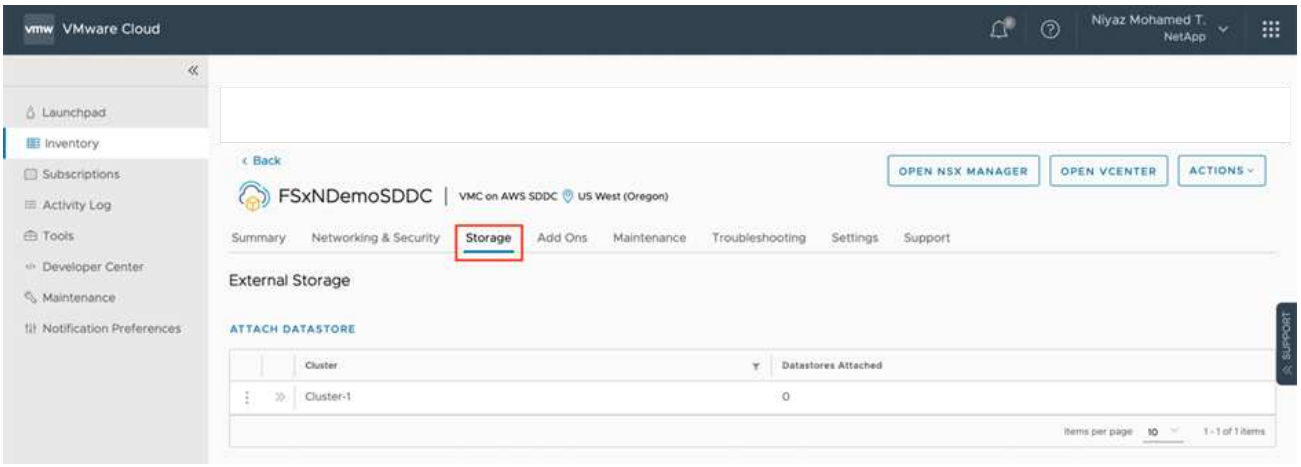
Mettez à jour le groupe de sécurité pour accepter le trafic NFS.

Il s'agit de la dernière étape de la préparation de la connectivité au SDDC approprié. Une fois le système de fichiers configuré, les itinéraires ajoutés et les groupes de sécurité mis à jour, il est temps de monter le ou les magasins de données.

▼ Étape 6 : attacher un volume NFS en tant que banque de données au cluster SDDC

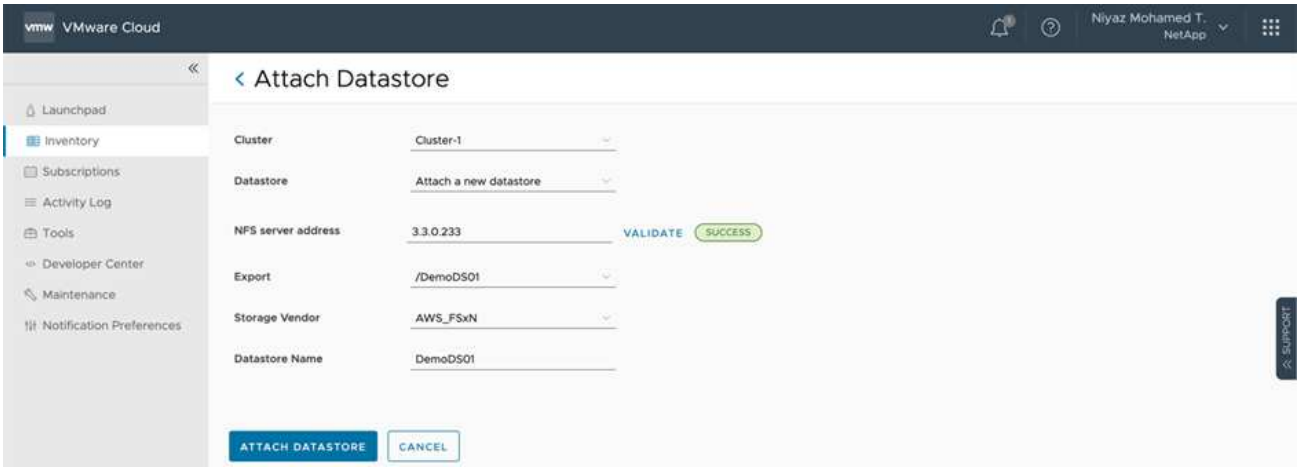
Une fois le système de fichiers provisionné et la connectivité en place, accédez à VMware Cloud Console pour monter la banque de données NFS.

1. Dans la console VMC, ouvrez l'onglet **Stockage** du SDDC.

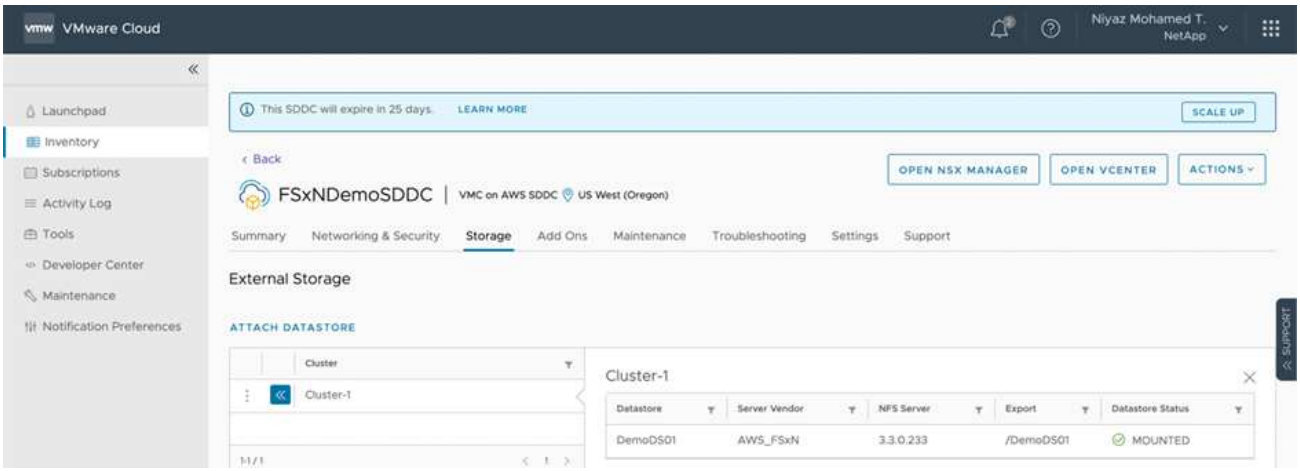


2. Cliquez sur **ATTACH DATASTORE** et remplissez les valeurs requises.

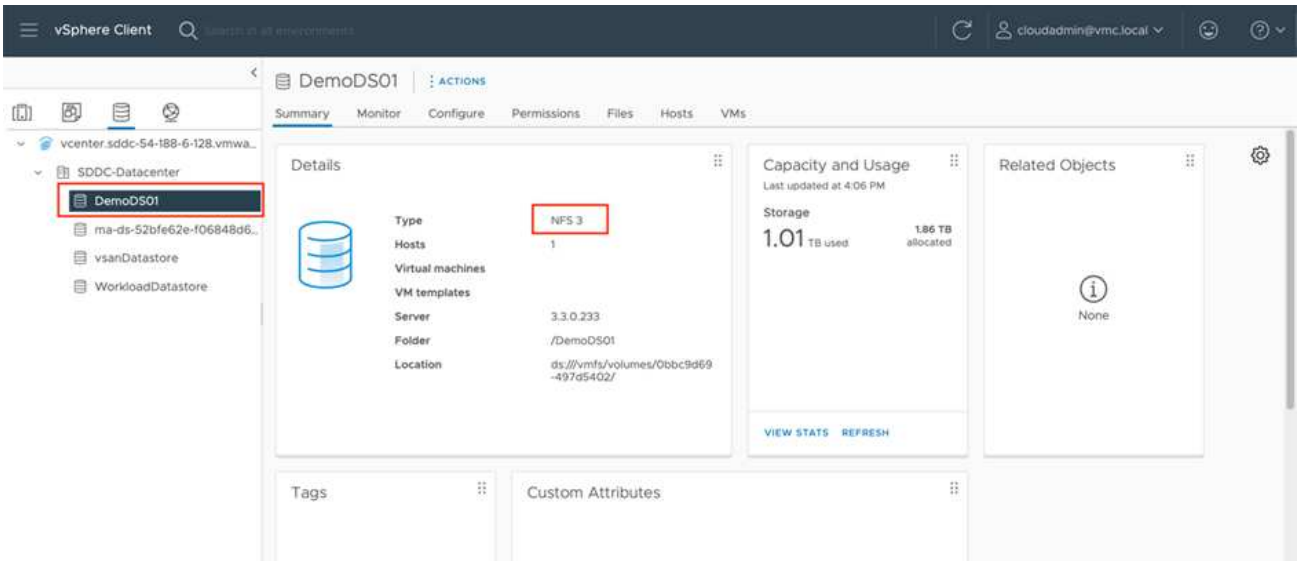
> L'adresse du serveur NFS est l'adresse IP NFS qui se trouve sous l'onglet FSx > Machines virtuelles de stockage > Points de terminaison dans la console AWS.



3. Cliquez sur **ATTACHER LE STOCK DE DONNÉES** pour attacher le magasin de données au cluster.



4. Validez le magasin de données NFS en accédant à vCenter comme indiqué ci-dessous :



Options de stockage invité NetApp connectées pour AWS

AWS prend en charge le stockage NetApp connecté aux invités avec le service FSx natif (FSx ONTAP) ou avec Cloud Volumes ONTAP (CVO).

FSx ONTAP

Amazon FSx ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités, basé sur le système de fichiers ONTAP populaire de NetApp. FSx ONTAP combine les fonctionnalités, les performances, les capacités et les opérations API familières des systèmes de fichiers NetApp avec l'agilité, l'évolutivité et la simplicité d'un service AWS entièrement géré.

FSx ONTAP fournit un stockage de fichiers partagé riche en fonctionnalités, rapide et flexible, largement accessible à partir d'instances de calcul Linux, Windows et macOS exécutées dans AWS ou sur site. FSx ONTAP offre un stockage SSD (Solid State Drive) hautes performances avec des latences inférieures à la milliseconde. Avec FSx ONTAP, vous pouvez atteindre des niveaux de performances SSD pour votre charge de travail tout en payant pour le stockage SSD pour seulement une petite fraction de vos données.

La gestion de vos données avec FSx ONTAP est plus simple car vous pouvez prendre des instantanés, cloner et répliquer vos fichiers en un clic. De plus, FSx ONTAP hiérarchise automatiquement vos données vers un

stockage élastique et moins coûteux, réduisant ainsi le besoin de provisionner ou de gérer la capacité.

FSx ONTAP fournit également un stockage hautement disponible et durable avec des sauvegardes entièrement gérées et une prise en charge de la reprise après sinistre interrégionale. Pour faciliter la protection et la sécurisation de vos données, FSx ONTAP prend en charge les applications courantes de sécurité des données et d'antivirus.

FSx ONTAP comme stockage connecté invité

▼ **Configurer Amazon FSx ONTAP avec VMware Cloud sur AWS**

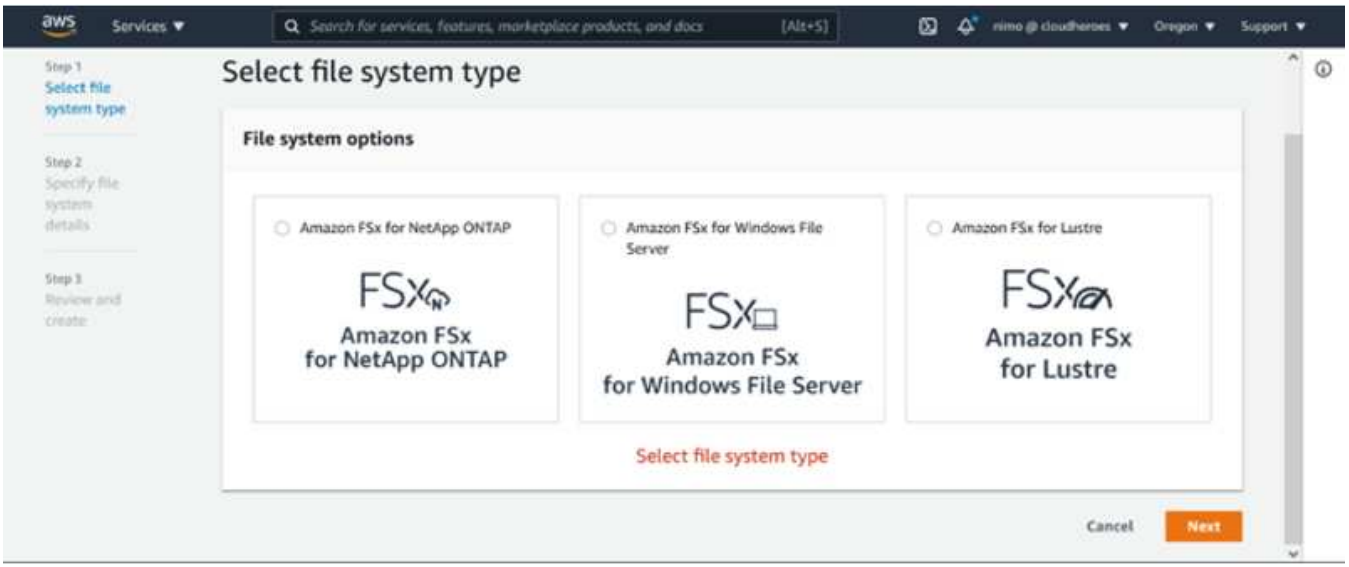
Les partages de fichiers et les LUN Amazon FSx ONTAP peuvent être montés à partir de machines virtuelles créées dans l'environnement VMware SDDC sur VMware Cloud chez AWS. Les volumes peuvent également être montés sur le client Linux et mappés sur le client Windows à l'aide du protocole NFS ou SMB, et les LUN sont accessibles sur les clients Linux ou Windows en tant que périphériques de bloc lorsqu'ils sont montés sur iSCSI. Amazon FSx pour le système de fichiers NetApp ONTAP peut être configuré rapidement en suivant les étapes suivantes.

> ⓘ Amazon FSx ONTAP et VMware Cloud sur AWS doivent se trouver dans la même zone de disponibilité pour obtenir de meilleures performances et éviter les frais de transfert de données entre les zones de disponibilité.

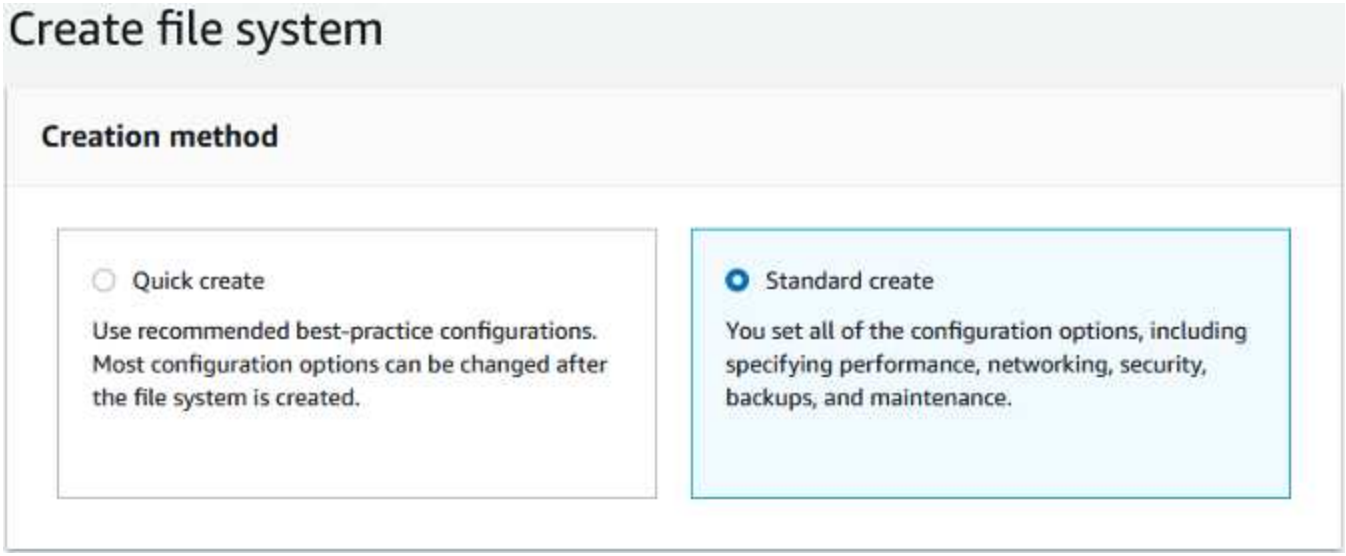
▼ **Créer et monter des volumes Amazon FSx ONTAP**

Pour créer et monter le système de fichiers Amazon FSx ONTAP , procédez comme suit :

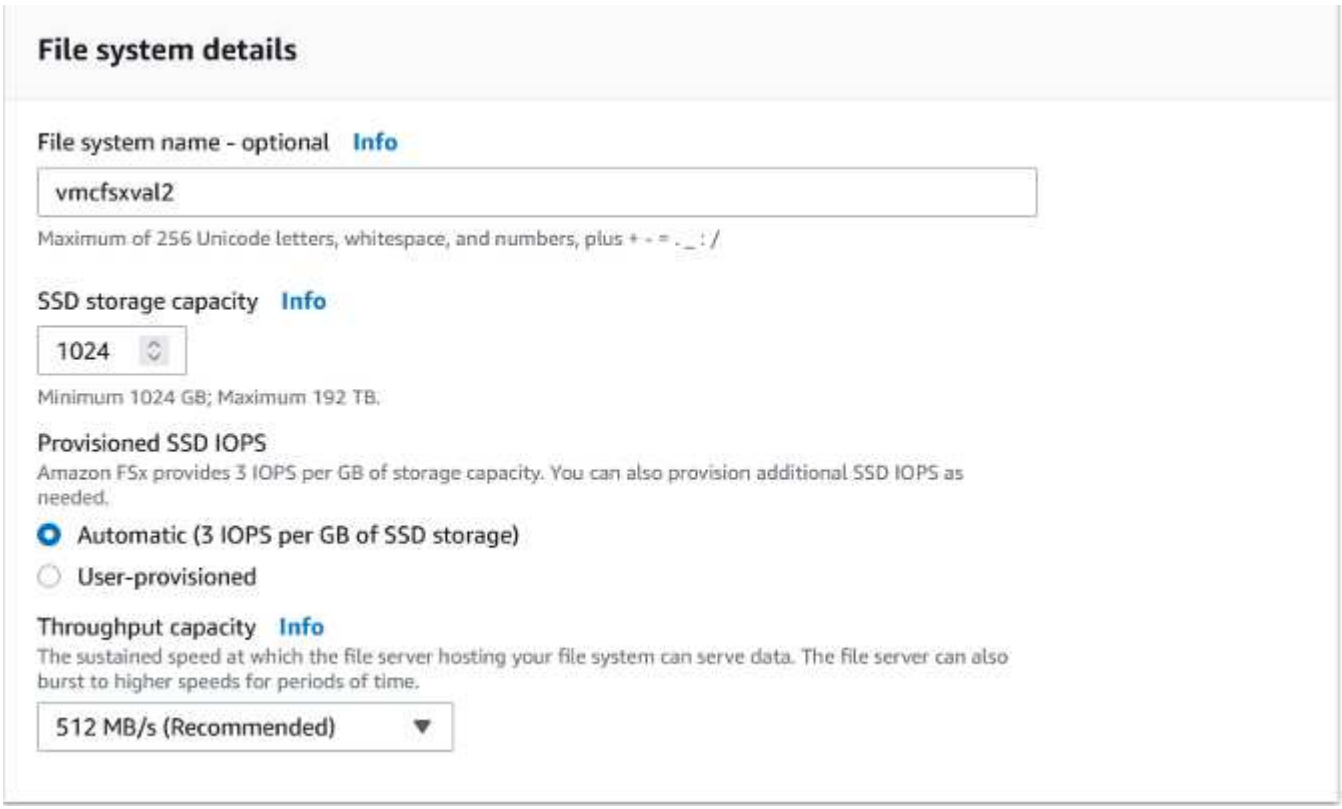
1. Ouvrez le"Console Amazon FSx" et choisissez Créer un système de fichiers pour démarrer l'assistant de création de système de fichiers.
2. Sur la page Sélectionner le type de système de fichiers, choisissez Amazon FSx ONTAP, puis Suivant. La page Créer un système de fichiers s'affiche.



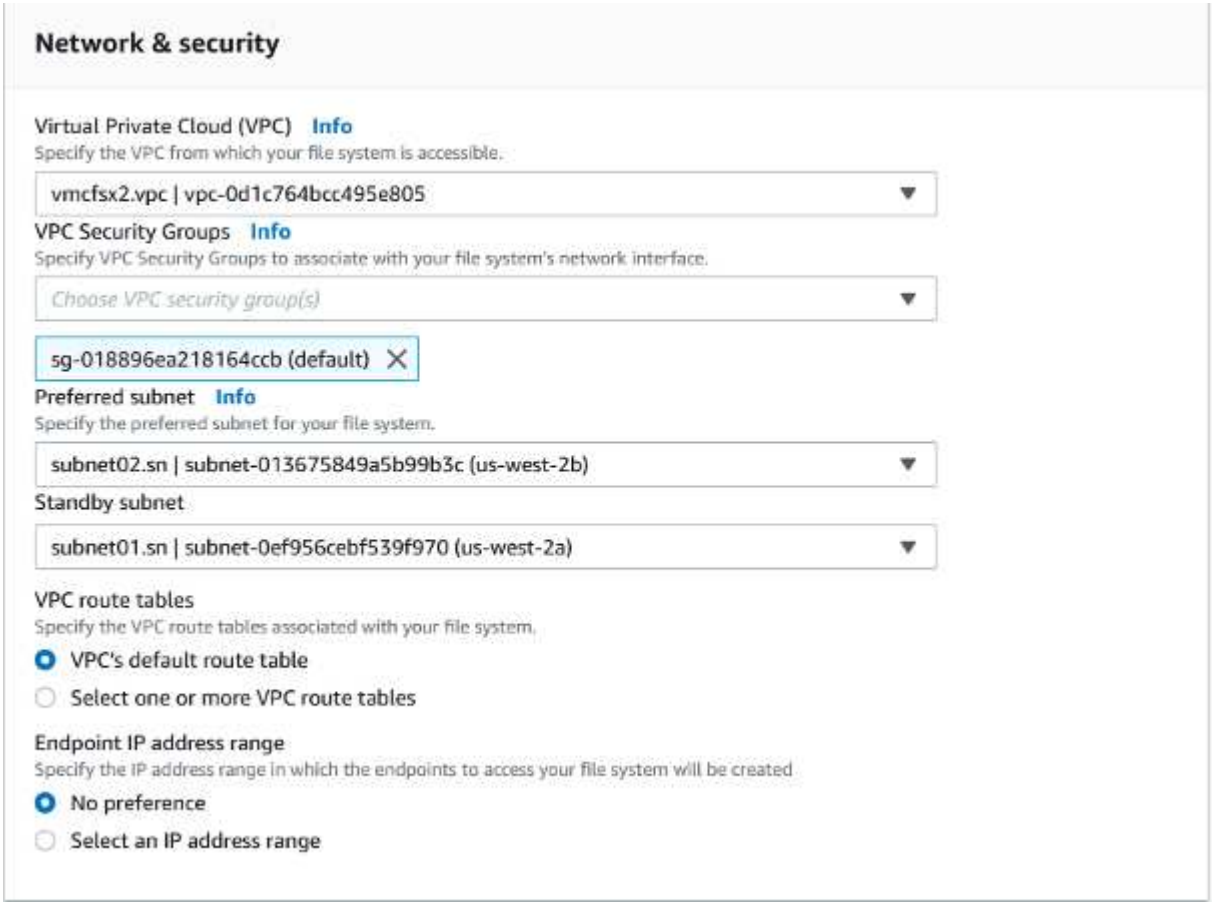
1. Dans la section Mise en réseau, pour Virtual Private Cloud (VPC), choisissez le VPC approprié et les sous-réseaux préférés ainsi que la table de routage. Dans ce cas, vmcfsx2.vpc est sélectionné dans la liste déroulante.



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

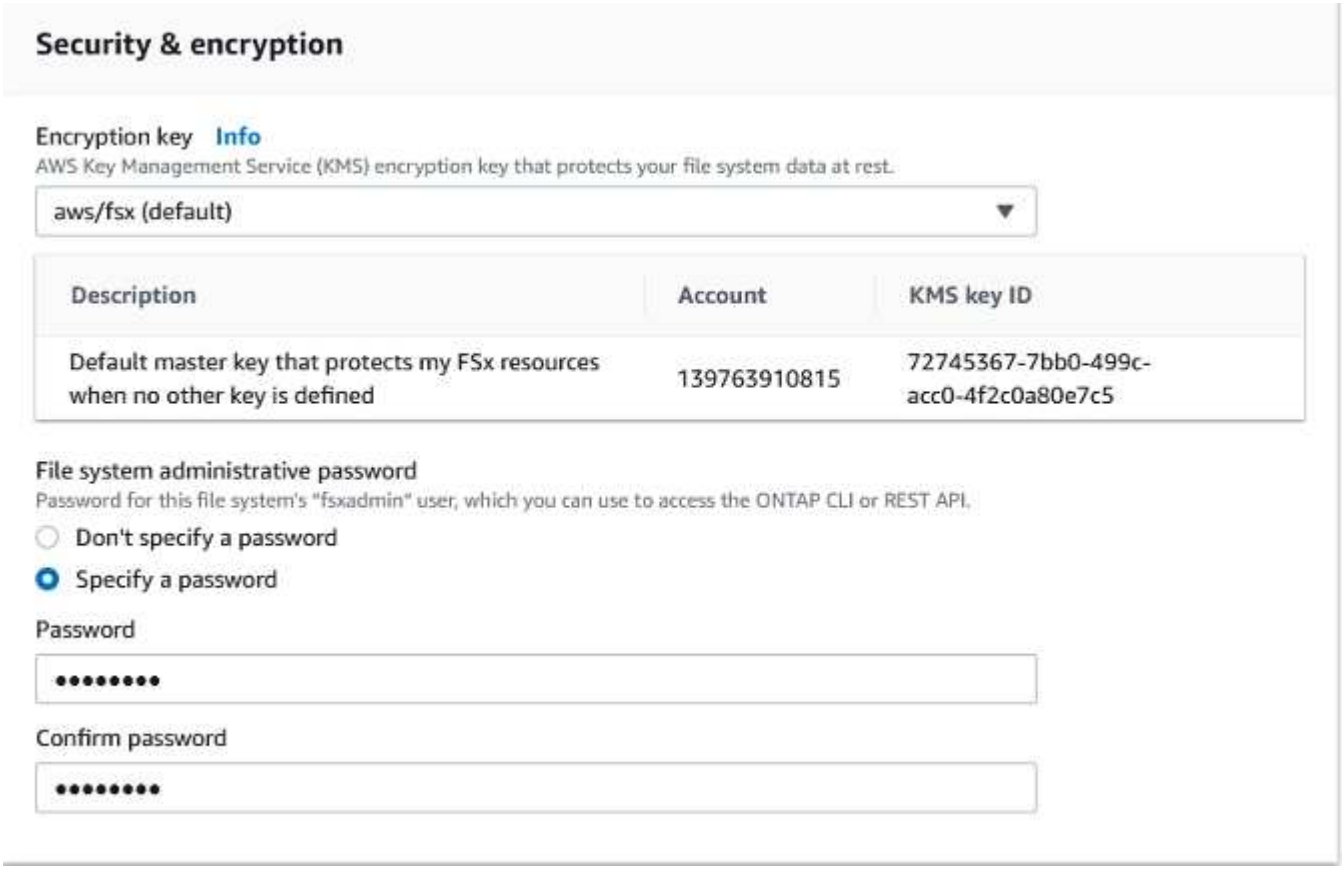


1. Dans la section Mise en réseau, pour Virtual Private Cloud (VPC), choisissez le VPC approprié et les sous-réseaux préférés ainsi que la table de routage. Dans ce cas, vmcfsx2.vpc est sélectionné dans la liste déroulante.

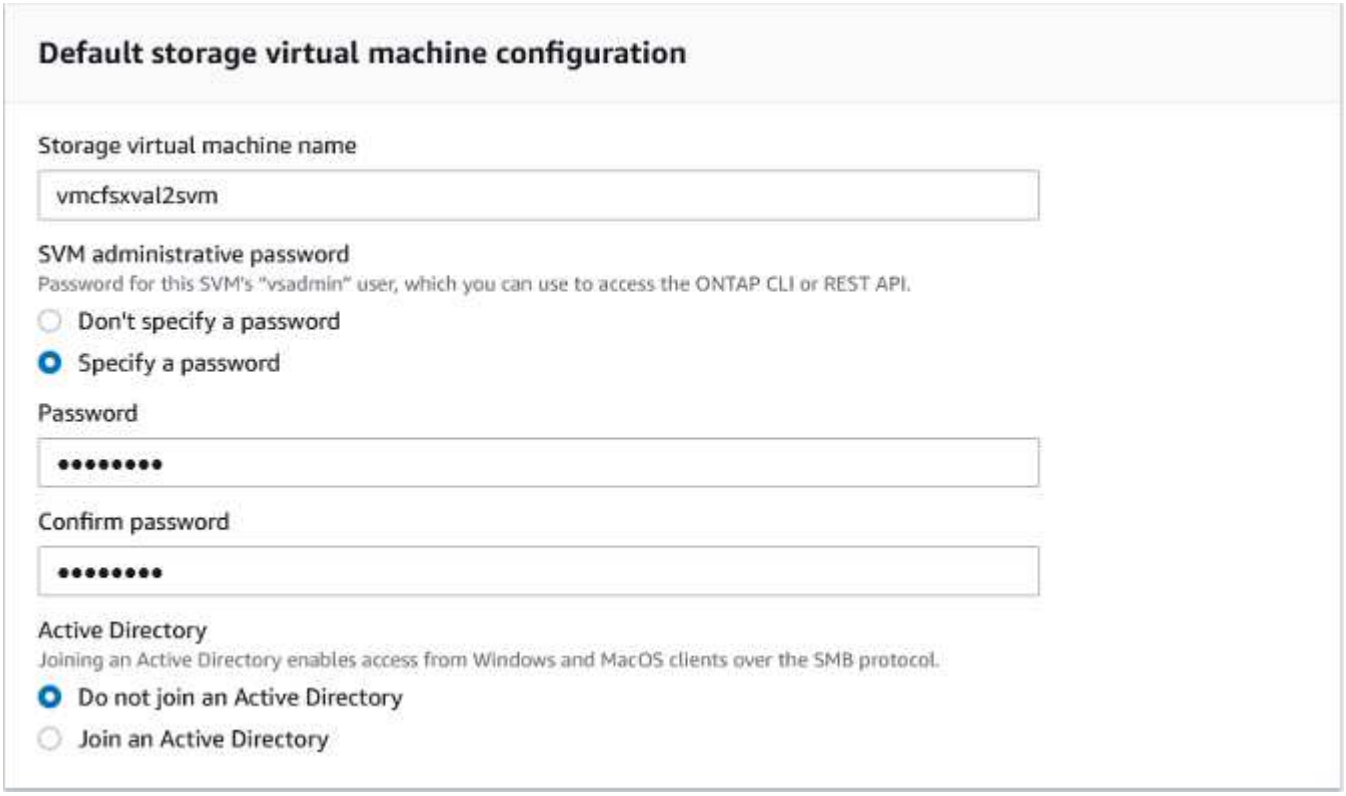


Dans la section Mise en réseau, pour Virtual Private Cloud (VPC), choisissez le VPC approprié et les sous-réseaux préférés ainsi que la table de routage. Dans ce cas, vmcfsx2.vpc est sélectionné dans la liste déroulante.

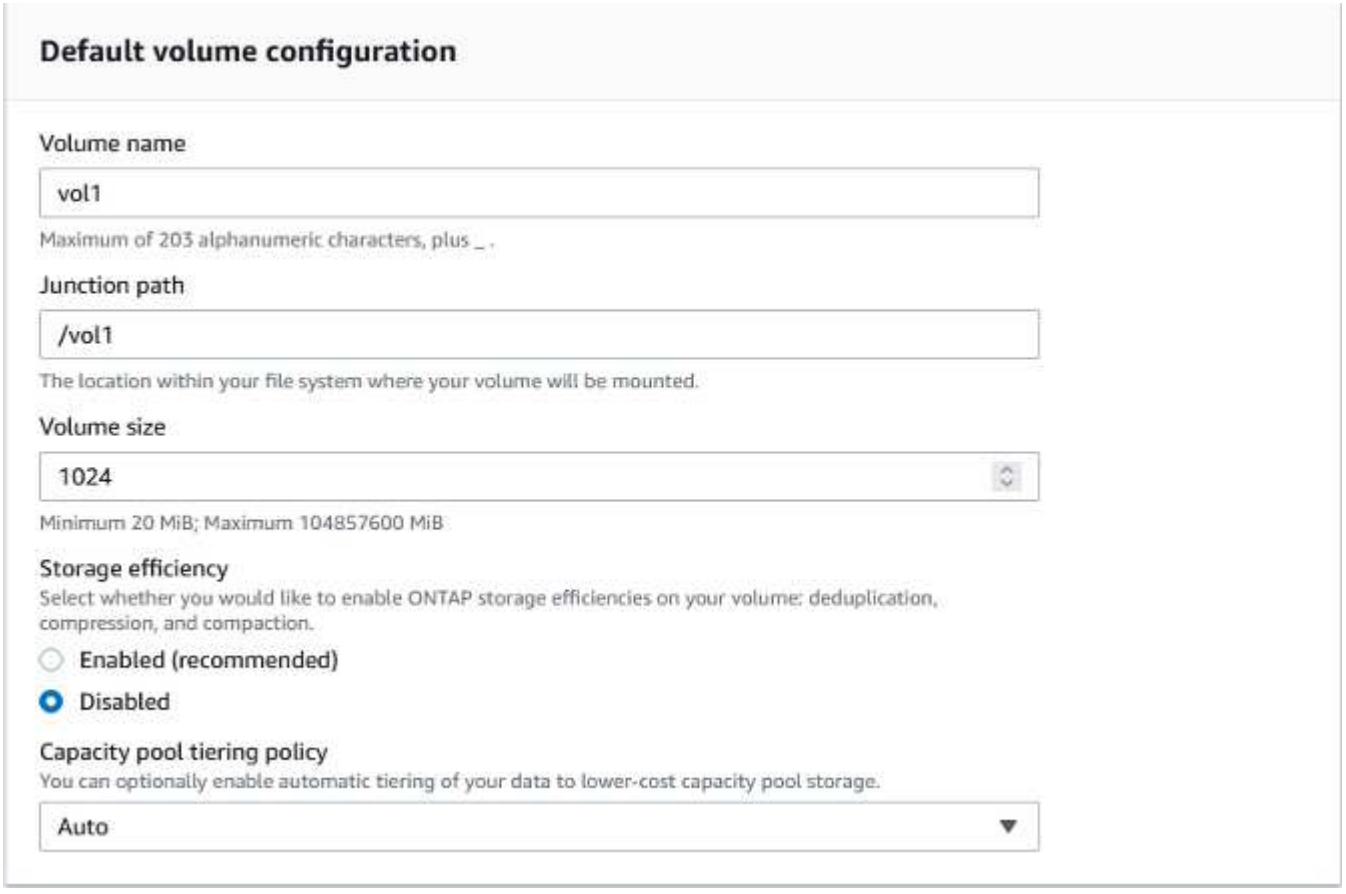
1. Dans la section Sécurité et chiffrement, pour la clé de chiffrement, choisissez la clé de chiffrement AWS Key Management Service (AWS KMS) qui protège les données du système de fichiers au repos. Pour le mot de passe administratif du système de fichiers, entrez un mot de passe sécurisé pour l'utilisateur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



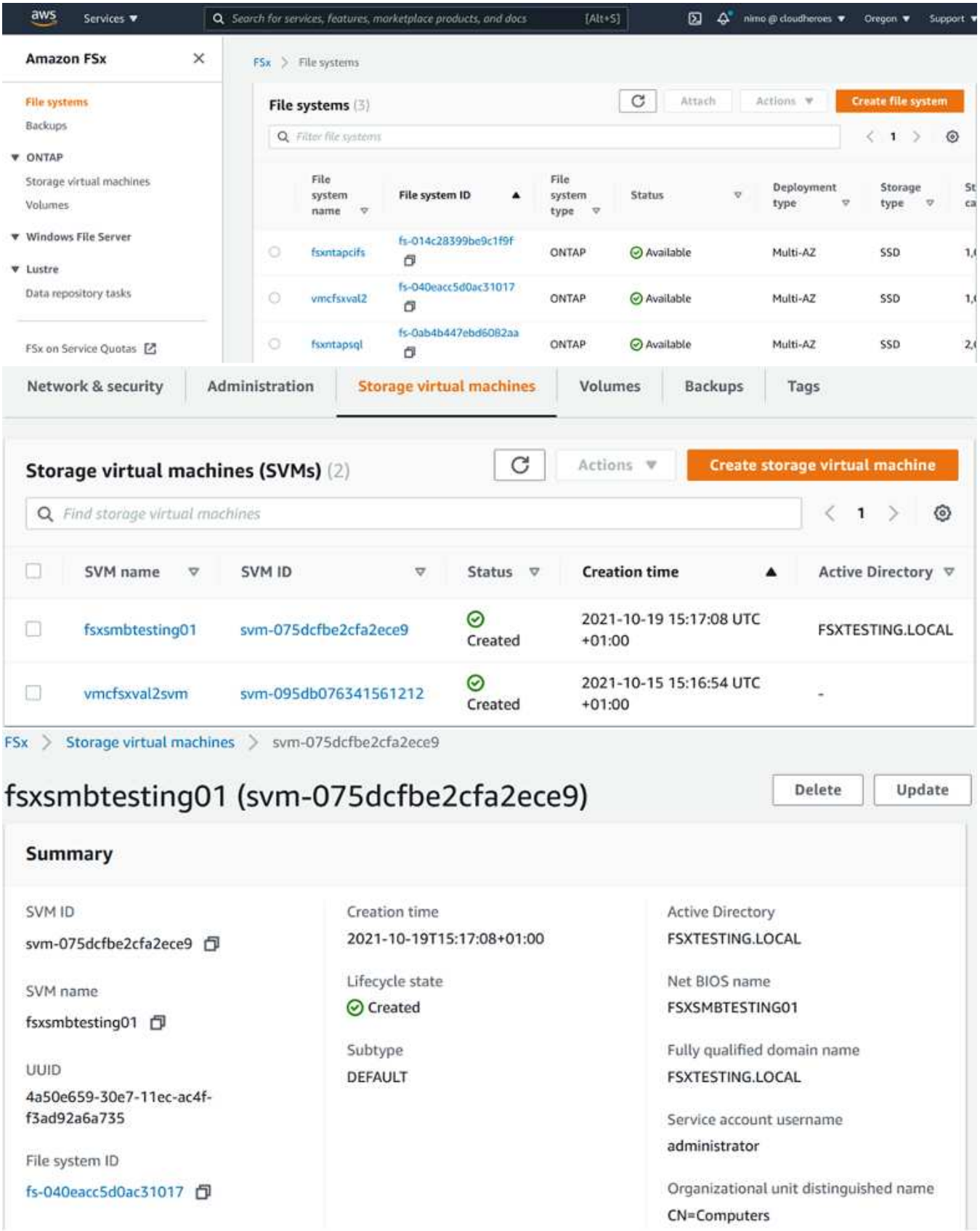
1. Dans la machine virtuelle, spécifiez le mot de passe à utiliser avec vsadmin pour administrer ONTAP à l'aide des API REST ou de la CLI. Si aucun mot de passe n'est spécifié, un utilisateur fsxadmin peut être utilisé pour administrer le SVM. Dans la section Active Directory, assurez-vous de joindre Active Directory au SVM pour provisionner les partages SMB. Dans la section Configuration de la machine virtuelle de stockage 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 compactage) ou Désactivé pour les désactiver.



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

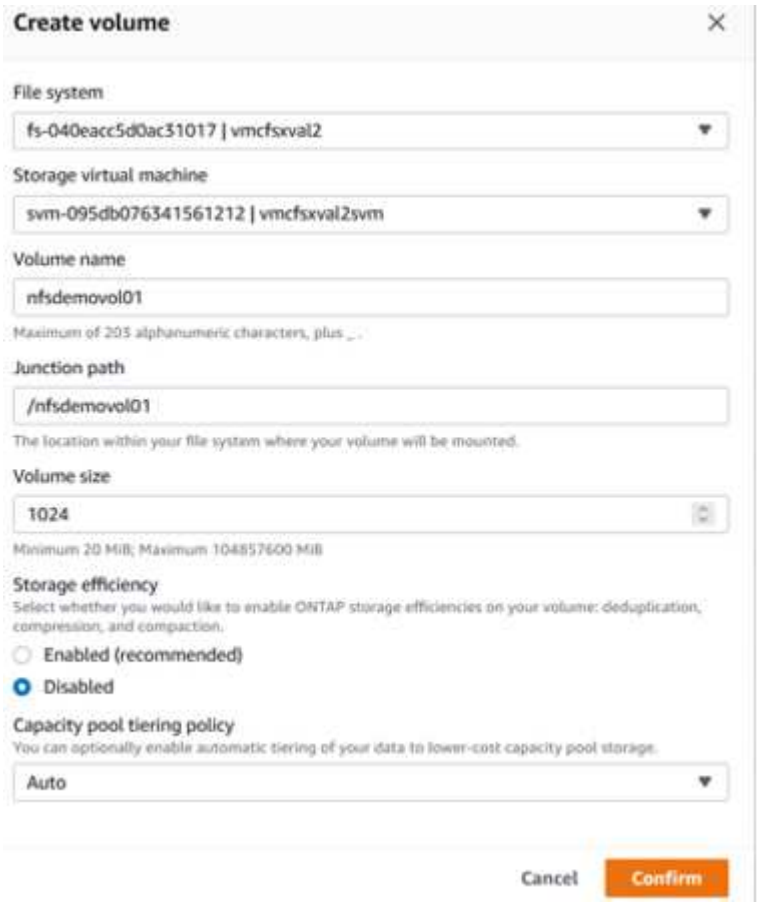


Pour des informations plus détaillées, voir"Premiers pas avec Amazon FSx ONTAP" .

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 qui peut être facilement monté sur des machines virtuelles exécutées sur le cloud VMware sur AWS. nfsdemovol01 est créé comme illustré ci-dessous :



▼ **Monter le volume FSx ONTAP sur un client Linux**

Pour monter le volume FSx ONTAP créé à l'étape précédente à partir des machines virtuelles Linux dans VMC sur AWS SDDC, procédez comme suit :

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. Créez un répertoire pour le point de montage du volume avec la commande suivante :

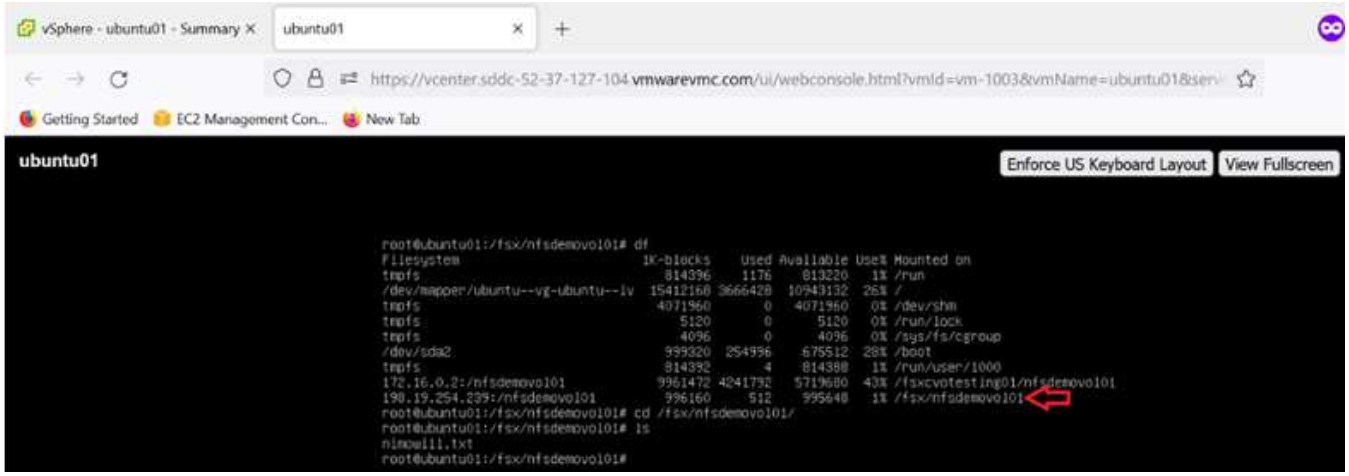
```
$ sudo mkdir /fsx/nfsdemovol01
```

. Montez le volume NFS Amazon FSx 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 exécuté, exécutez la commande df pour valider le montage.



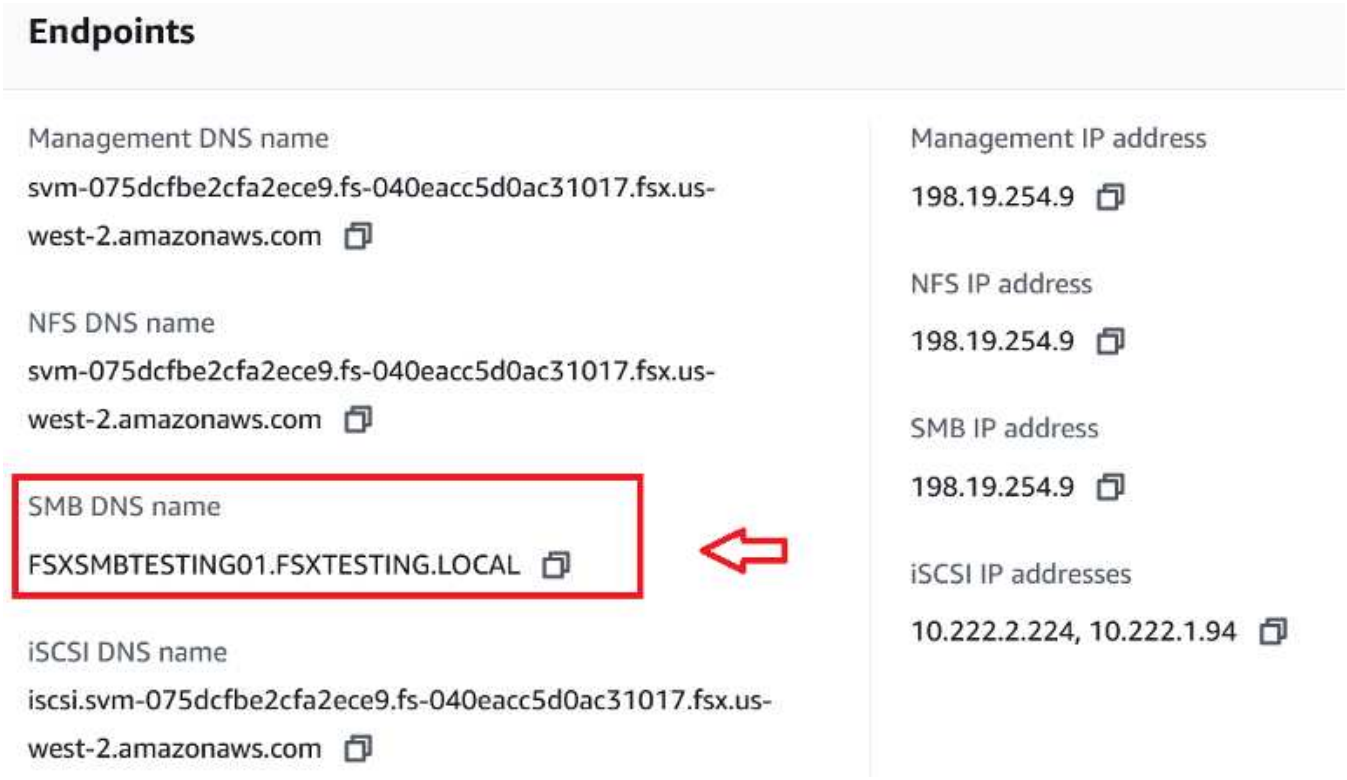
Monter le volume FSx ONTAP sur un client Linux

▼ **Attacher des volumes FSx ONTAP aux clients Microsoft Windows**

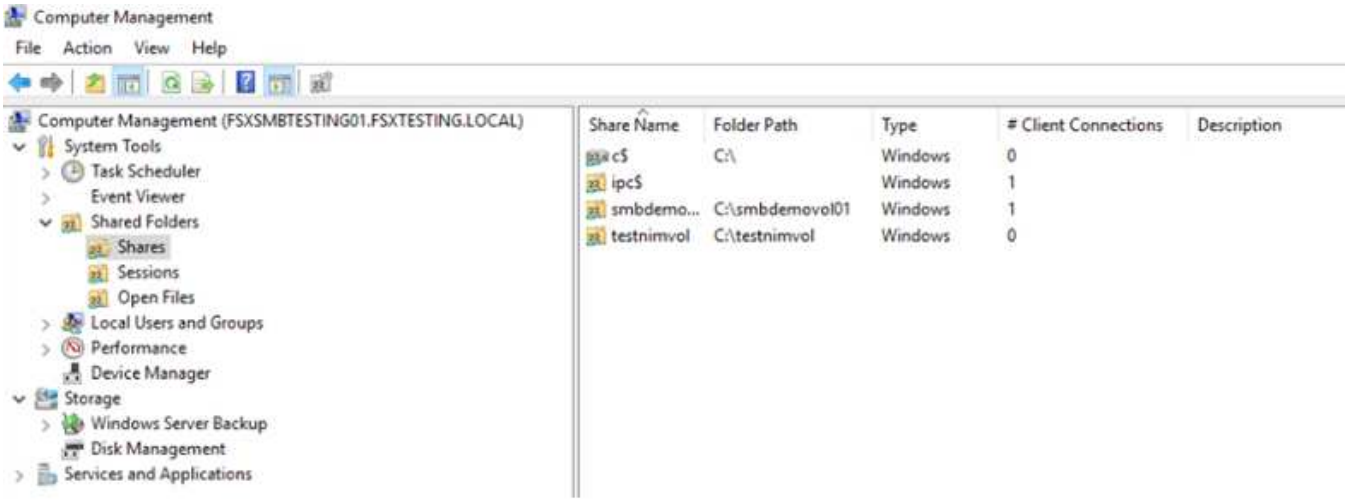
Pour gérer et mapper les partages de fichiers sur un système de fichiers Amazon FSx , l'interface graphique des dossiers partagés doit être utilisée.

1. Ouvrez le menu Démarrer et exécutez fsmgmt.msc à l'aide de Exécuter en tant qu'administrateur. Cela ouvre l'outil d'interface graphique des dossiers partagés.
2. Cliquez sur Action > Toutes les tâches et choisissez Se connecter à un autre ordinateur.
3. Pour un autre ordinateur, entrez le nom DNS de la machine virtuelle de stockage (SVM). Par exemple, FSXSMBTESTING01.FSXTESTING.LOCAL est utilisé dans cet exemple.

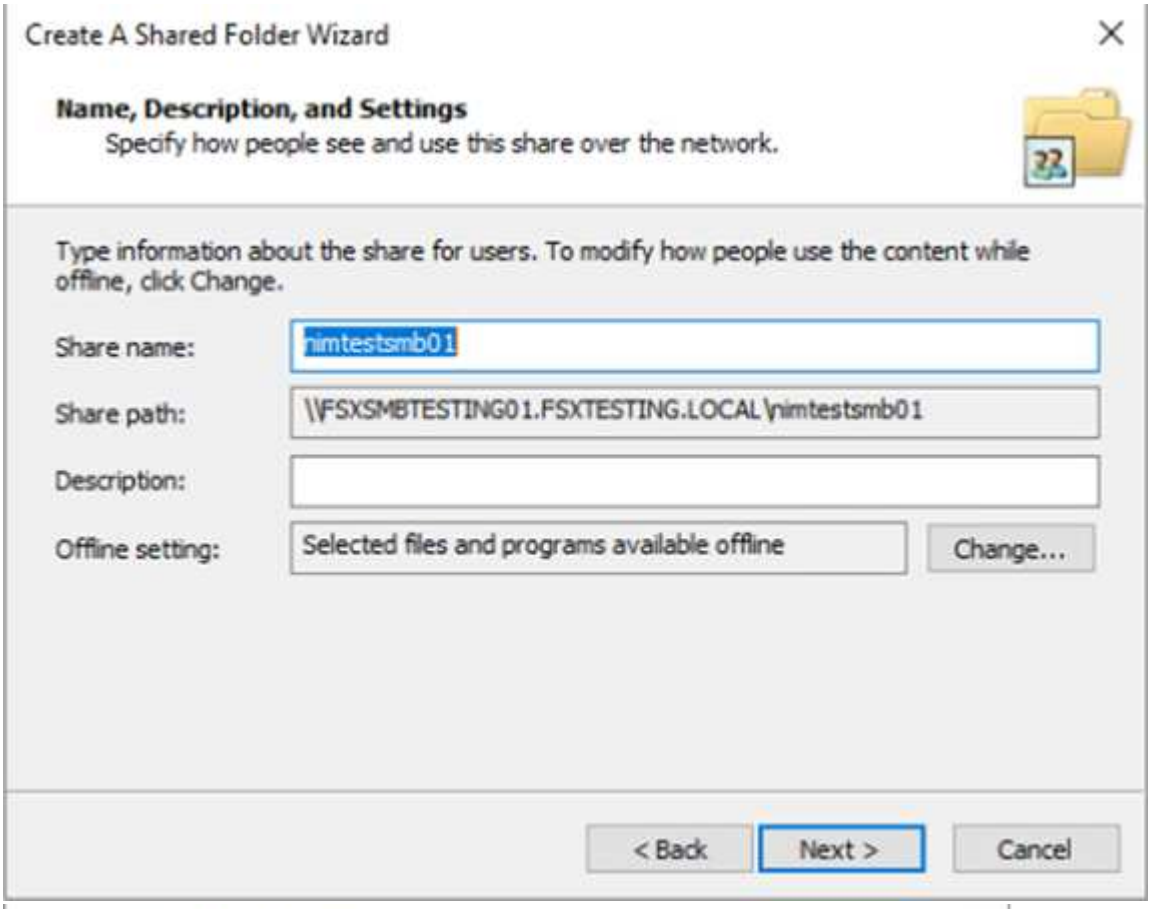
ⓘ Pour trouver le nom DNS du SVM sur la console Amazon FSx , choisissez Machines virtuelles de stockage, choisissez SVM, puis faites défiler jusqu'à Points de terminaison pour trouver le nom DNS SMB. Cliquez sur OK. Le système de fichiers Amazon FSx apparaît dans la liste des dossiers partagés.



1. Dans l'outil Dossiers partagés, choisissez Partages dans le volet de gauche pour voir les partages actifs pour le système de fichiers Amazon FSx .



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

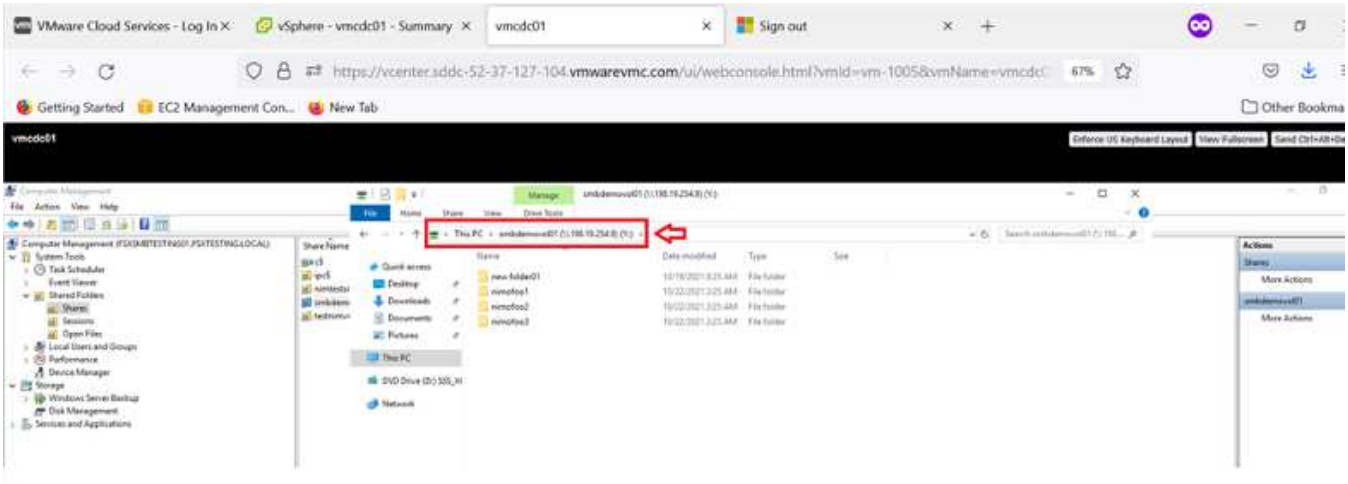




Pour en savoir plus sur la création et la gestion des partages SMB sur un système de fichiers Amazon FSx , consultez"Création de partages SMB" .

1. Une fois la connectivité établie, le partage SMB peut être connecté et utilisé pour les données

d’application. Pour ce faire, copiez le chemin de partage et utilisez l’option Mapper le lecteur réseau pour monter le volume sur la machine virtuelle exécutée sur VMware Cloud sur le SDDC AWS.



▼ **Connecter un LUN FSx ONTAP à un hôte à l’aide d’iSCSI**

Connecter un LUN FSx ONTAP à un hôte à l’aide d’iSCSI

Le trafic iSCSI pour FSx traverse VMware Transit Connect/AWS Transit Gateway via les itinéraires fournis dans la section précédente. Pour configurer un LUN dans Amazon FSx ONTAP, suivez la documentation trouvée"ici" .

Sur les clients Linux, assurez-vous que le démon iSCSI est en cours d’exécution. Une fois les LUN provisionnés, reportez-vous aux instructions détaillées sur la configuration iSCSI avec Ubuntu (à titre d’exemple)"ici" .

Dans cet article, la connexion du LUN iSCSI à un hôte Windows est illustrée :

▼ **Provisionner un LUN dans FSx ONTAP:**

1. Accédez à l’interface de ligne de commande NetApp ONTAP à l’aide du port de gestion du FSx pour le système de fichiers ONTAP .
2. Créez les LUN avec la taille requise comme indiqué par la sortie de dimensionnement.

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

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

1. Créez les groupes i 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 aux 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
```

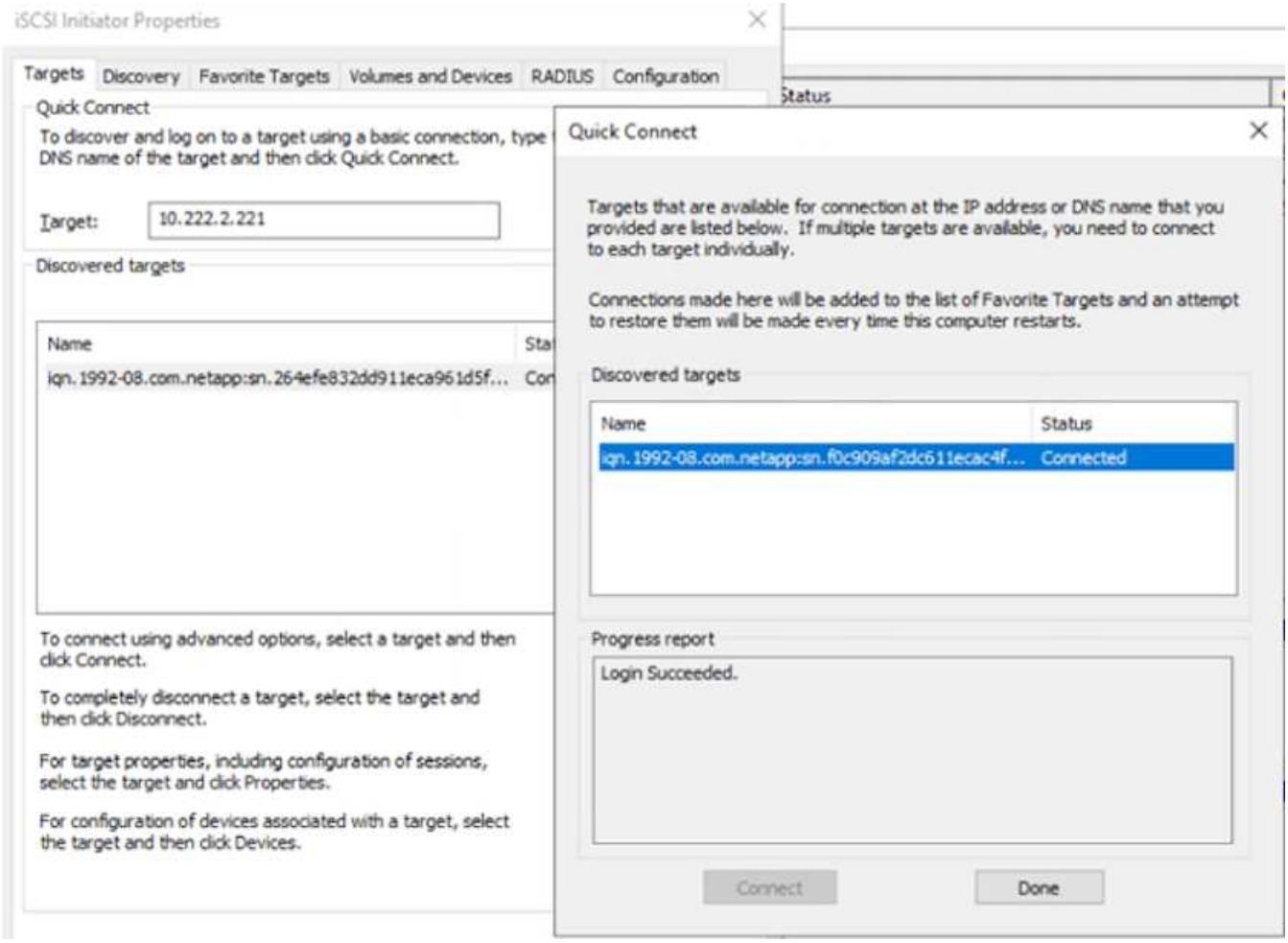
Deux entrées ont été affichées.

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

Pour connecter le nouveau LUN à un hôte Windows résidant sur le cloud VMware sur AWS SDDC, procédez comme suit :

1. RDP vers la machine virtuelle Windows hébergée sur VMware Cloud sur AWS SDDC.
2. Accédez à Gestionnaire de serveur > Tableau de bord > Outils > Initiateur iSCSI pour ouvrir la boîte de dialogue Propriétés de l'initiateur iSCSI.
3. Dans l'onglet Découverte, cliquez sur Découvrir le portail ou Ajouter un portail, puis entrez l'adresse IP du port cible iSCSI.
4. Dans l'onglet Cibles, sélectionnez la cible découverte, puis cliquez sur Connexion ou Connecter.
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.

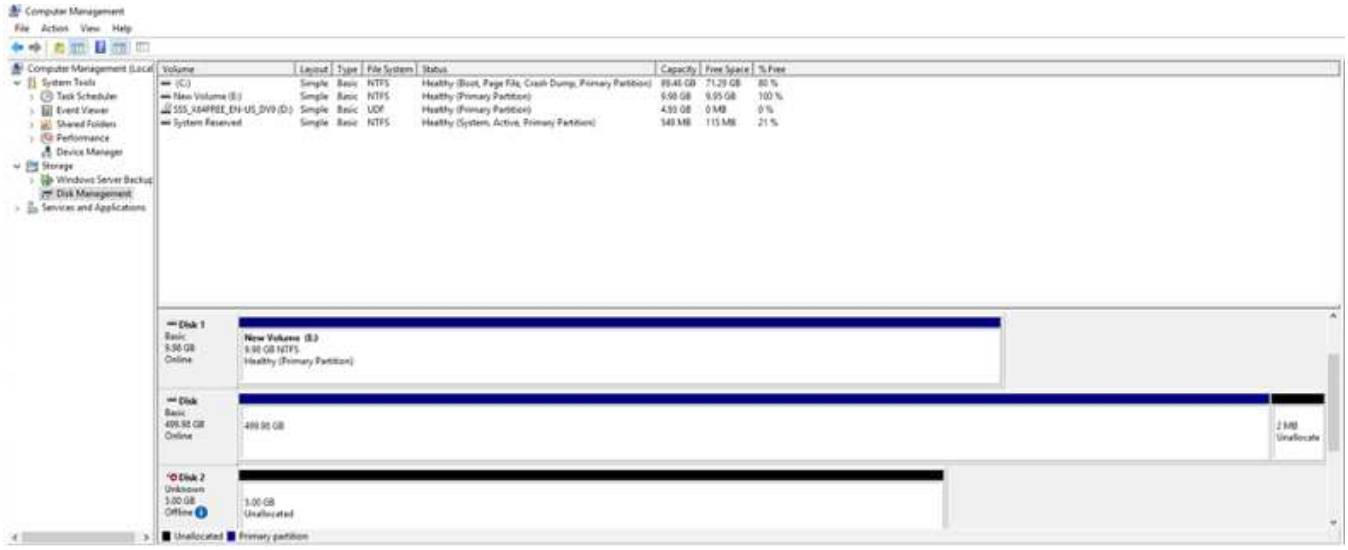
L'hôte Windows doit disposer d'une connexion iSCSI à chaque nœud du cluster. Le DSM natif sélectionne les meilleurs chemins à utiliser.



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

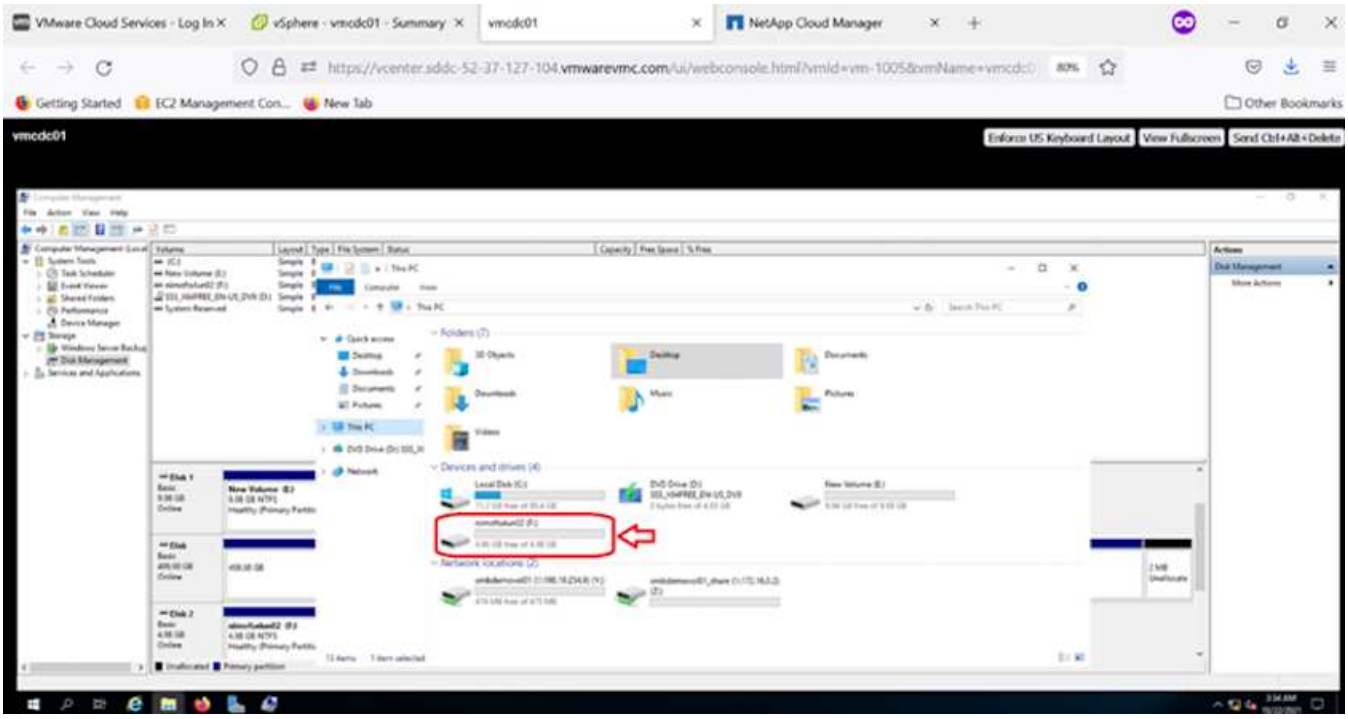
1. Ouvrez l'utilitaire Gestion de l'ordinateur Windows : Démarrer > Outils d'administration > Gestion de l'ordinateur.
2. Développez le nœud Stockage dans l'arborescence de navigation.
3. Cliquez sur Gestion des disques.

4. Cliquez sur Action > Réanalyser les disques.



Lorsqu'un nouveau LUN est accédé pour la première fois par l'hôte Windows, il ne possède aucune partition ni aucun système de fichiers. Initialisez le LUN et, éventuellement, formatez le LUN avec un système de fichiers en procédant comme suit :

1. Démarrez la gestion des disques Windows.
2. Cliquez avec le bouton droit sur le 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 de données cloud leader du secteur, basée sur le logiciel de stockage ONTAP de NetApp, disponible nativement sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s’agit d’une version définie par logiciel d' ONTAP qui consomme du stockage natif dans le cloud, vous permettant d’avoir le même logiciel de stockage dans le cloud et sur site, réduisant ainsi le besoin de recycler votre personnel informatique dans de toutes nouvelles méthodes de gestion de vos données.

CVO offre aux clients la possibilité de déplacer de manière transparente les données de la périphérie vers le centre de données, vers le cloud et vice-versa, en rassemblant votre cloud hybride, le tout géré avec une console de gestion à volet unique, NetApp Cloud Manager.

De par sa conception, CVO offre des performances extrêmes et des capacités avancées de gestion des données pour satisfaire même vos applications les plus exigeantes dans le cloud.

Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités

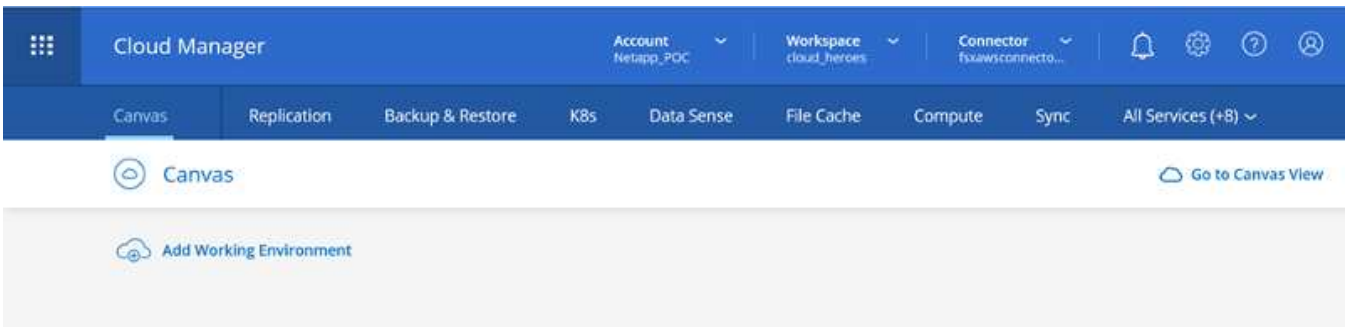
▼ **Déployer une nouvelle instance Cloud Volumes ONTAP dans AWS (faites-le vous-même)**

Les partages et LUN Cloud Volumes ONTAP peuvent être montés à partir de machines virtuelles créées dans l’environnement VMware Cloud on AWS SDDC. Les volumes peuvent également être montés sur des clients AWS VM Linux Windows natifs, et les LUN sont accessibles sur des 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.

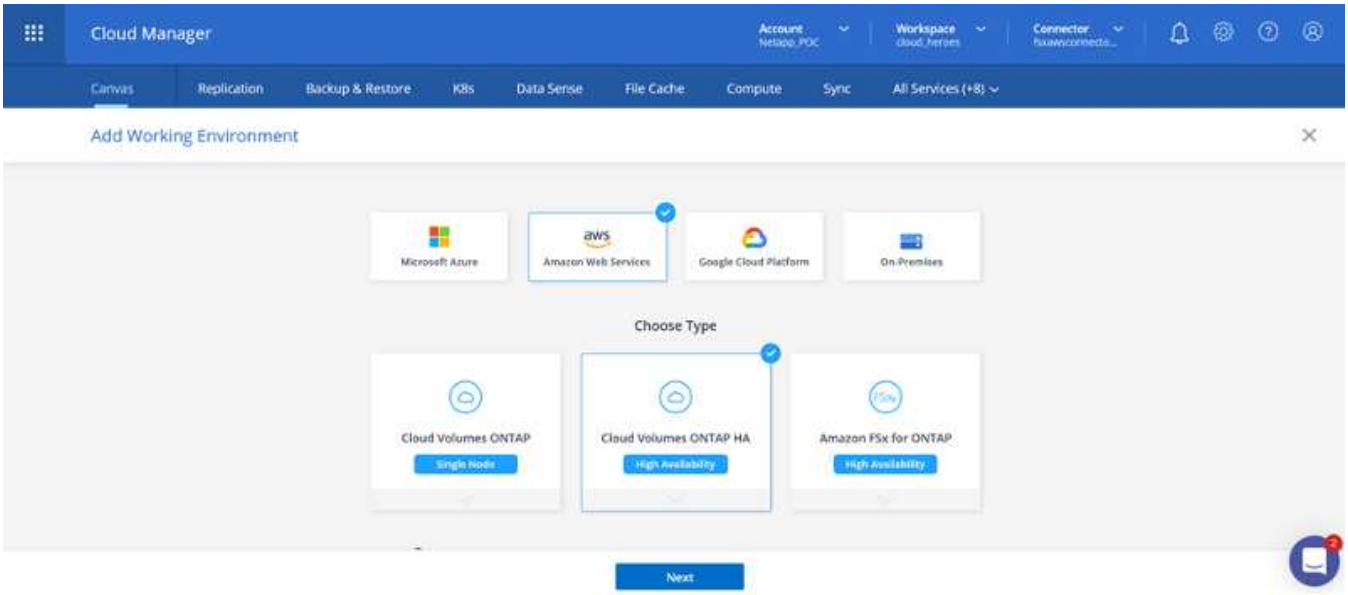
Pour répliquer des volumes d’un environnement local vers le cloud à des fins de reprise après sinistre ou de migration, établissez une connectivité réseau à AWS, soit à l’aide d’un VPN site à site, soit de DirectConnect. La réplication des données sur site vers Cloud Volumes ONTAP n’entre pas dans le cadre de ce document. Pour répliquer des données entre les systèmes locaux et Cloud Volumes ONTAP , consultez"Configuration de la réplication des données entre les systèmes" .

Utilisez le "Dimensionneur Cloud Volumes ONTAP" pour dimensionner avec précision les instances Cloud Volumes ONTAP. Surveillez également les performances sur site afin de les utiliser comme données d’entrée dans l’outil de dimensionnement Cloud Volumes ONTAP.

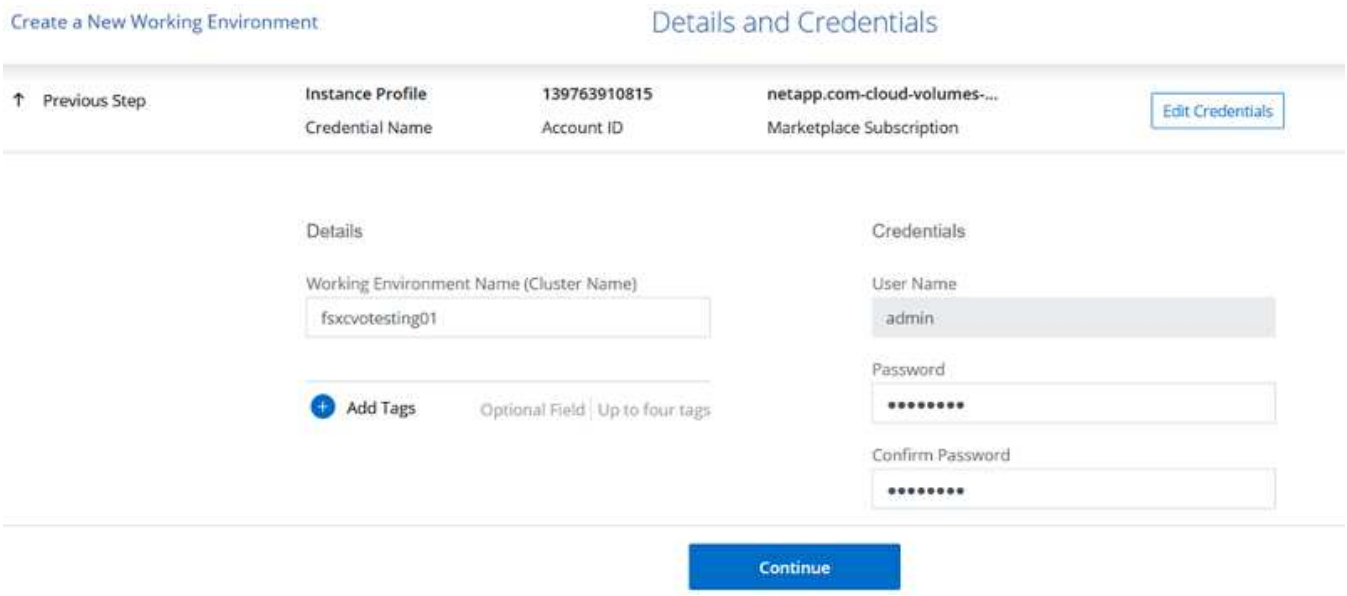
1. Connectez-vous à NetApp Cloud Central ; l’écran Fabric View s’affiche. Localisez l’onglet Cloud Volumes ONTAP et sélectionnez Accéder au Gestionnaire de Cloud. Une fois connecté, l’écran Canvas s’affiche.



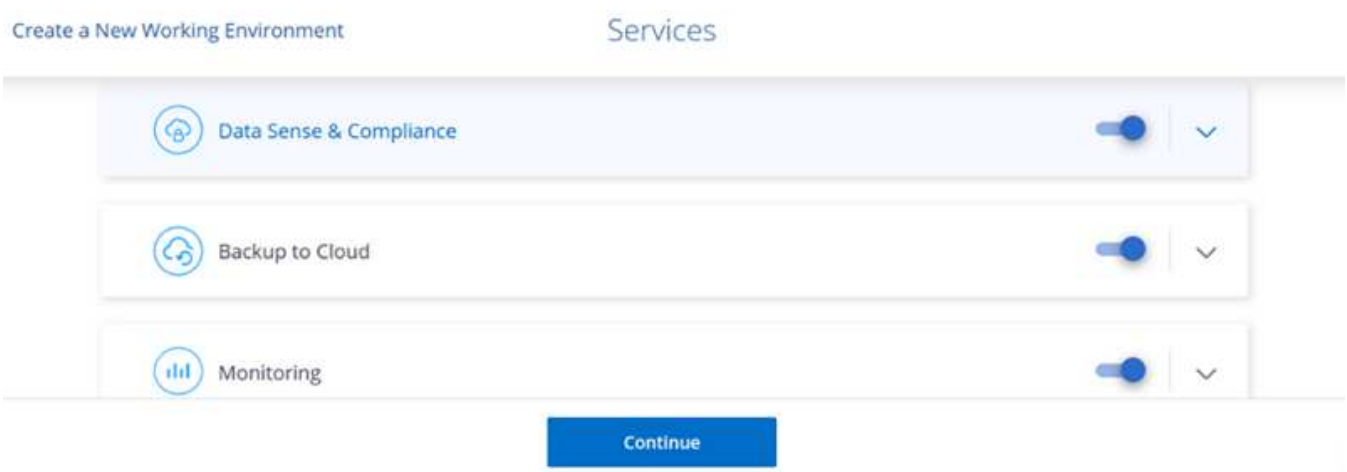
1. Sur la page d’accueil de Cloud Manager, cliquez sur Ajouter un environnement de travail, puis sélectionnez AWS comme cloud et le type de configuration système.



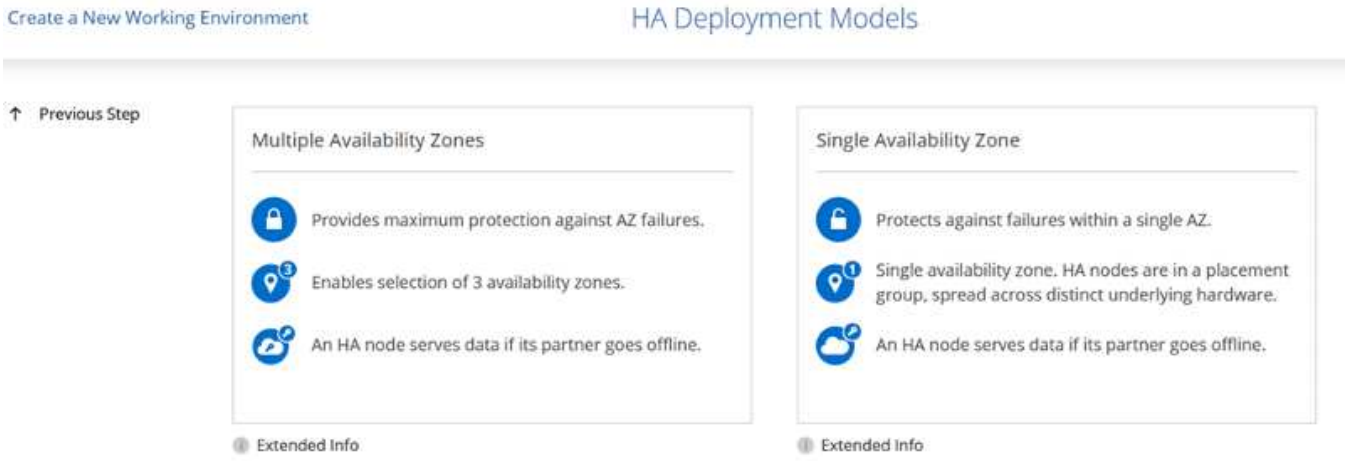
1. Fournissez les détails de l'environnement à créer, y compris le nom de l'environnement et les informations d'identification de l'administrateur. Cliquez sur Continuer.



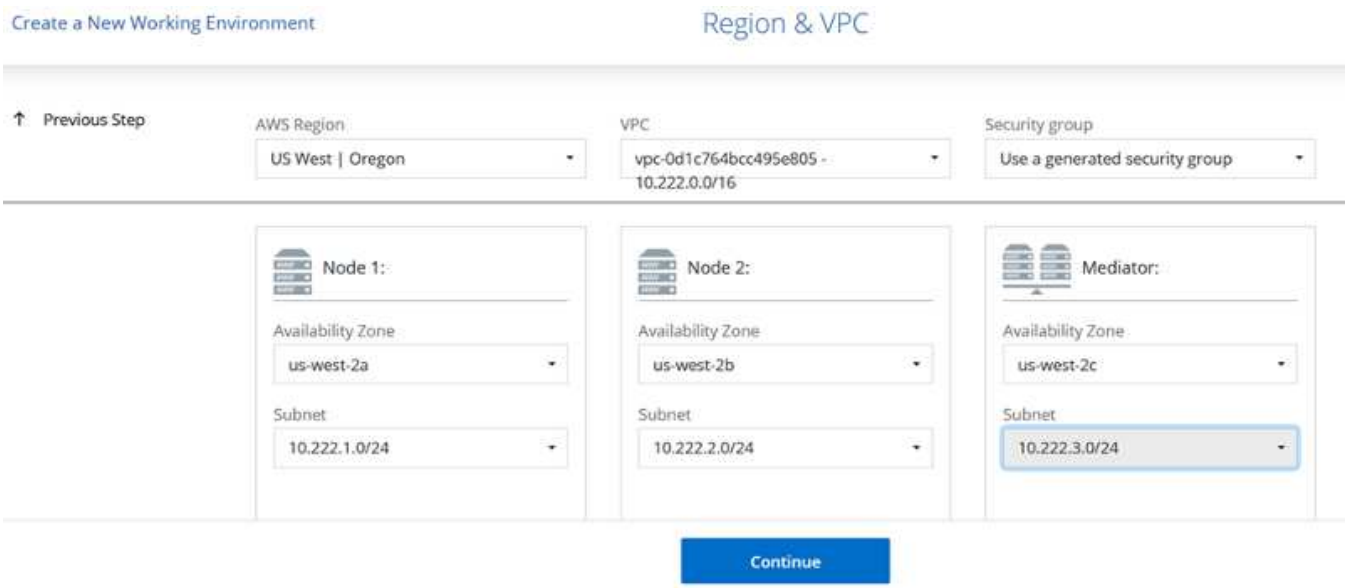
1. Sélectionnez les services complémentaires pour le déploiement de Cloud Volumes ONTAP, notamment NetApp Data Classification, NetApp Backup and Recovery et Data Infrastructure Insights. Cliquez sur Continue.



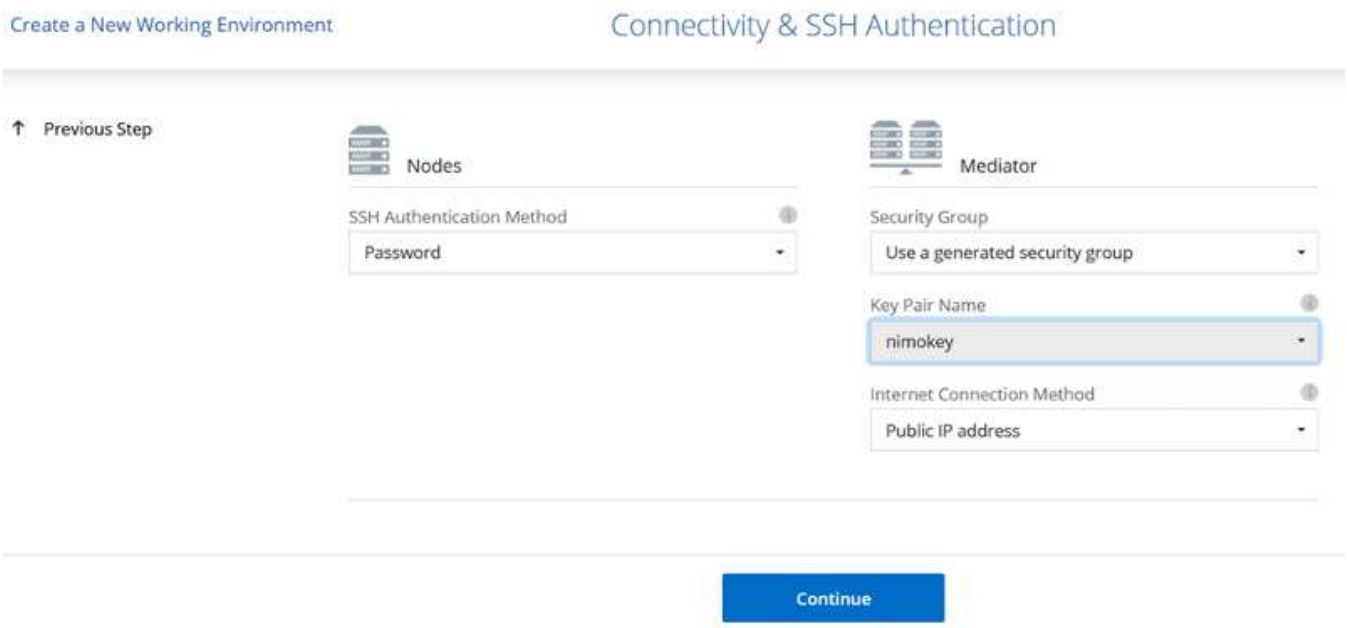
1. Sur la page Modèles de déploiement HA, choisissez la configuration Zones de disponibilité multiples.



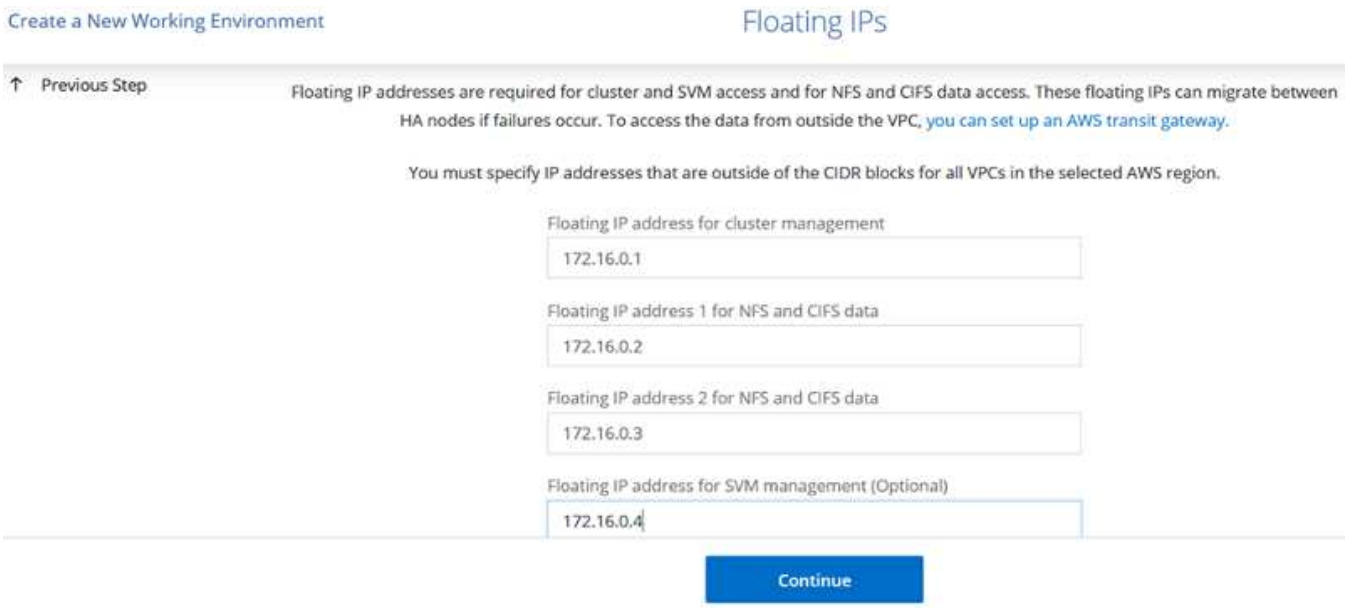
1. Sur la page Région et VPC, saisissez les informations réseau, puis cliquez sur Continuer.



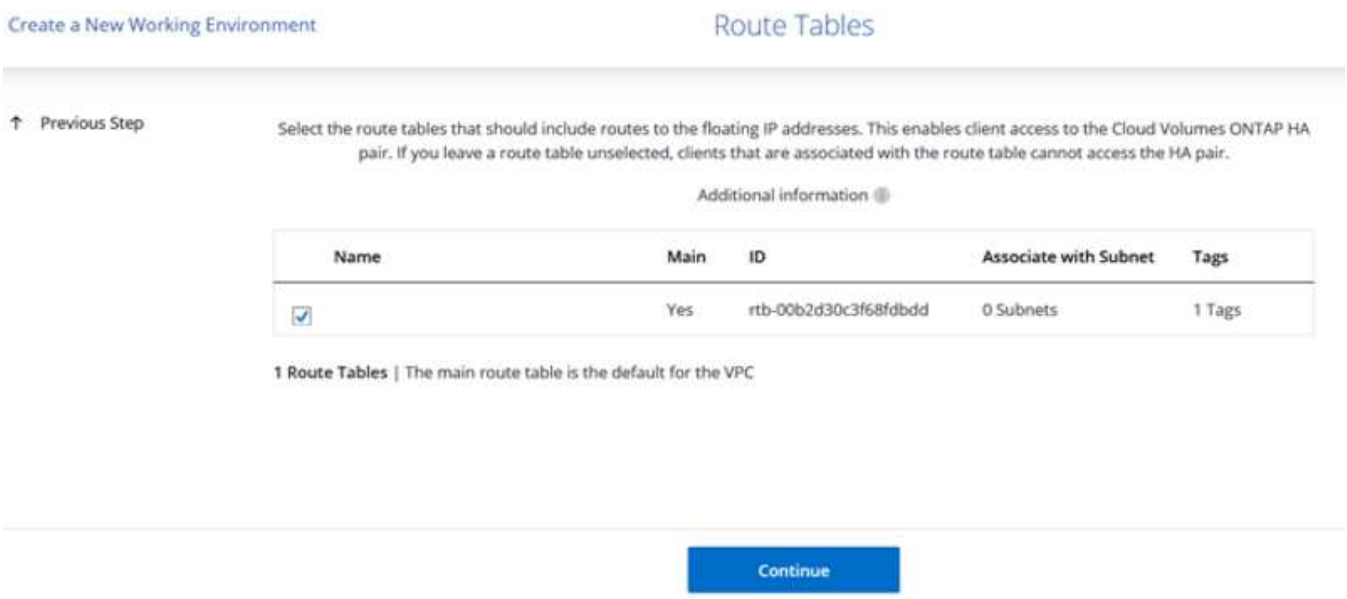
1. Sur la page Connectivité et authentification SSH, choisissez les méthodes de connexion pour la paire HA et le médiateur.



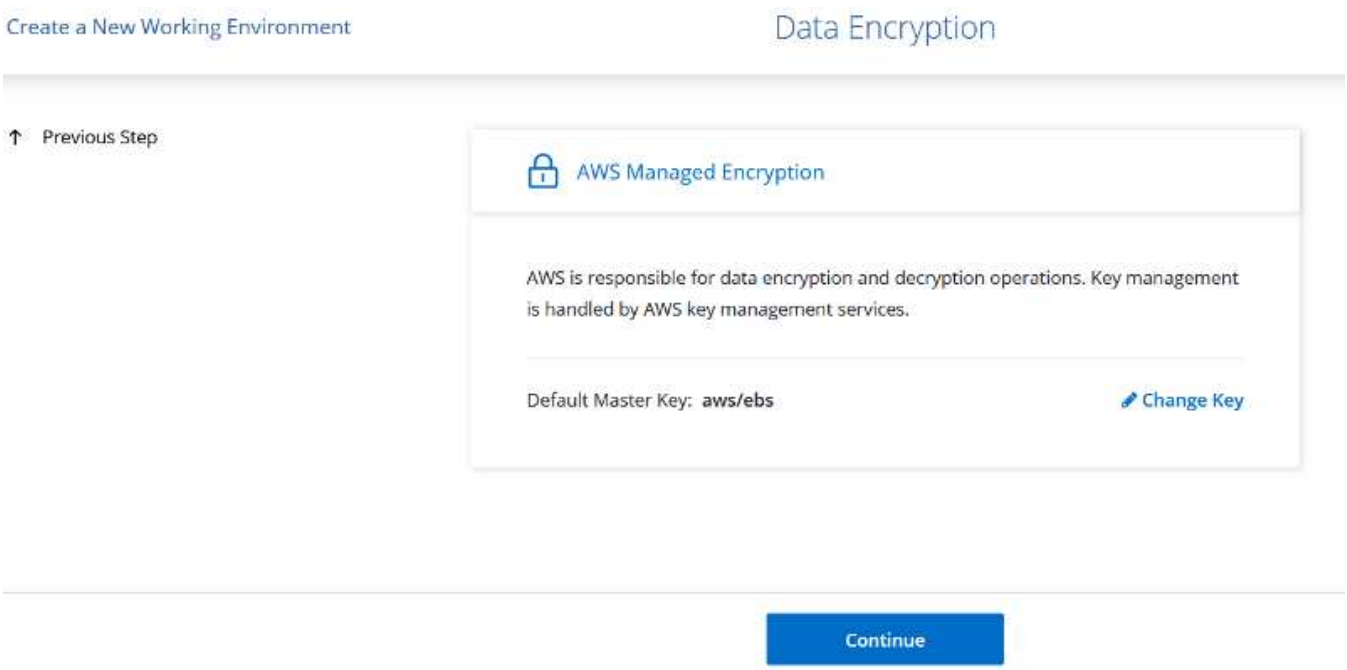
1. Spécifiez les adresses IP flottantes, puis cliquez sur Continuer.



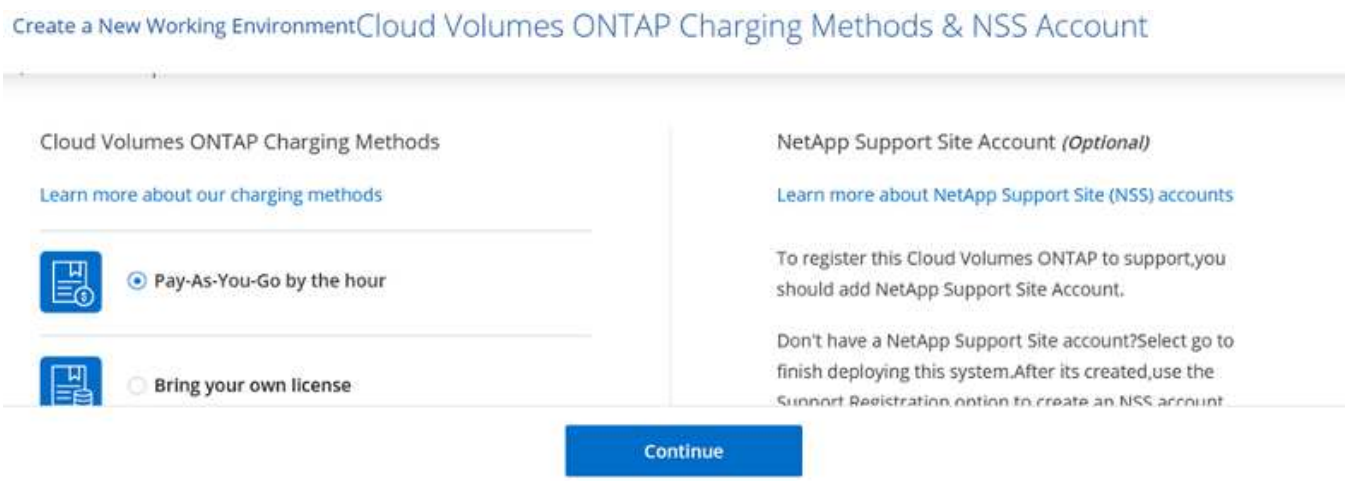
1. Sélectionnez les tables de routage appropriées pour inclure les routes vers les adresses IP flottantes, puis cliquez sur Continuer.



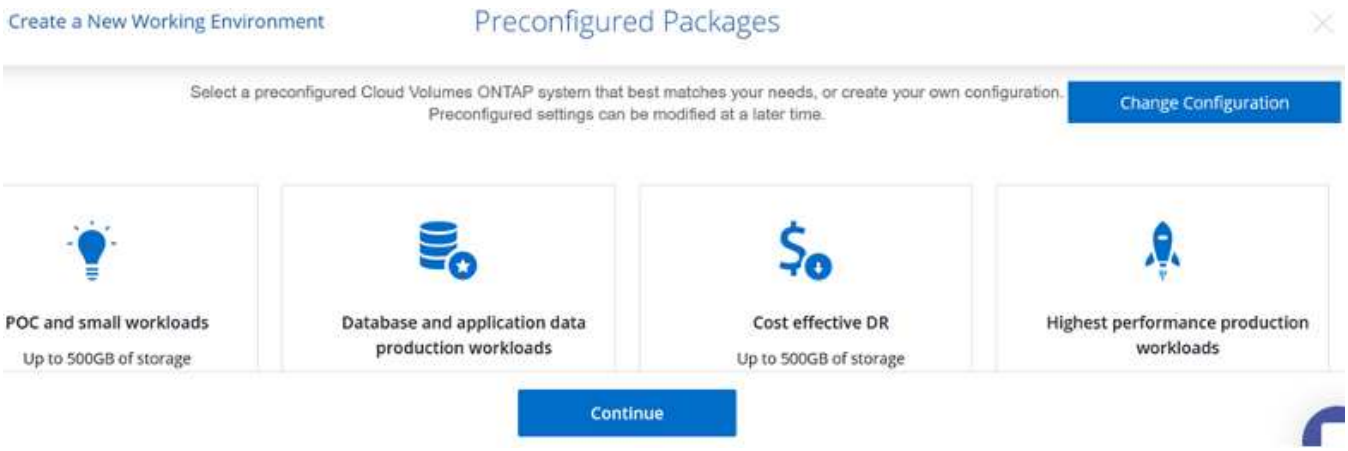
1. Sur la page Chiffrement des données, choisissez le chiffrement géré par AWS.



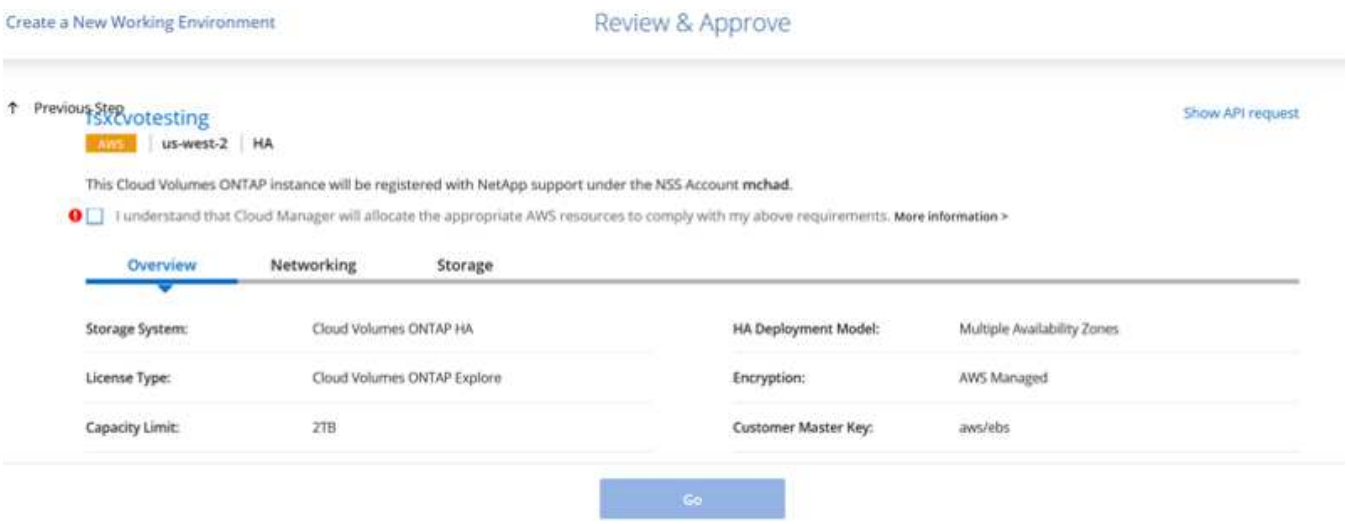
1. Sélectionnez l’option de licence : Pay-As-You-Go ou BYOL pour utiliser une licence existante. Dans cet exemple, l’option Pay-As-You-Go est utilisée.



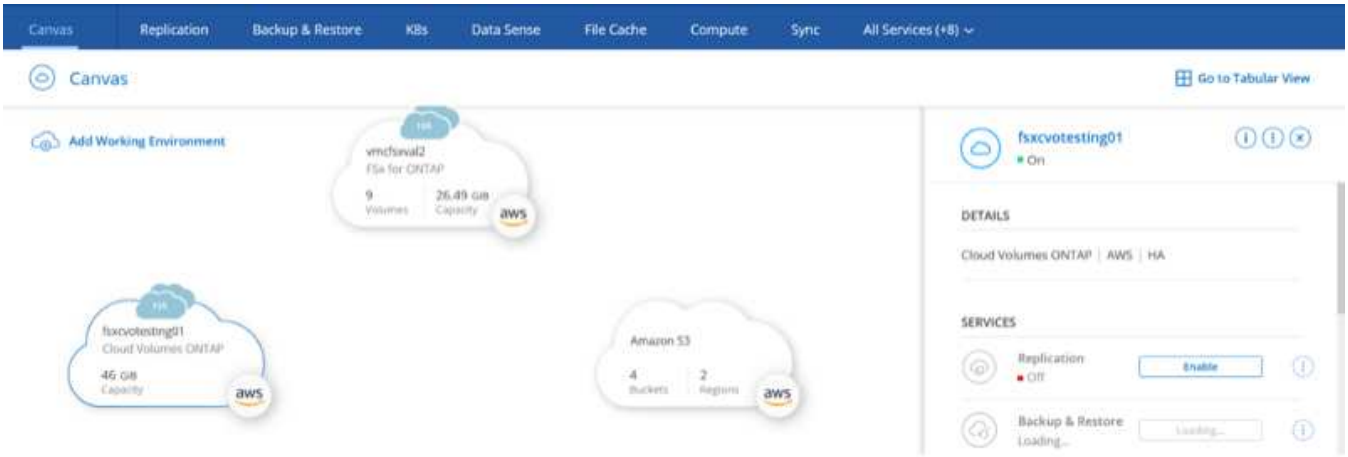
1. Choisissez parmi plusieurs packages préconfigurés disponibles en fonction du type de charge de travail à déployer sur les machines virtuelles exécutées sur le cloud VMware sur AWS SDDC.



1. Sur la page Réviser et approuver, vérifiez et confirmez les sélections. Pour créer l'instance Cloud Volumes ONTAP , cliquez sur Accéder.

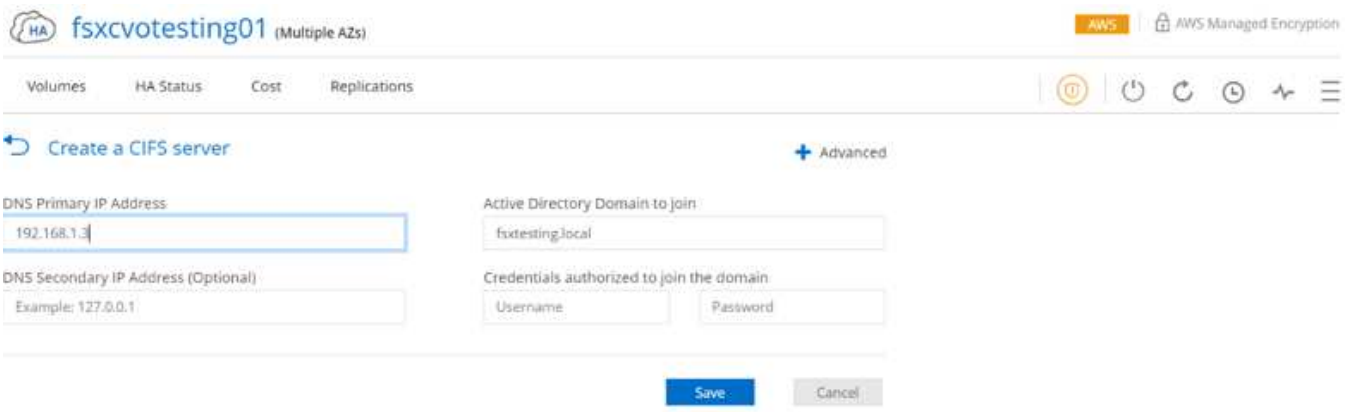


1. Une fois Cloud Volumes ONTAP provisionné, il est répertorié dans les environnements de travail sur la page Canvas.

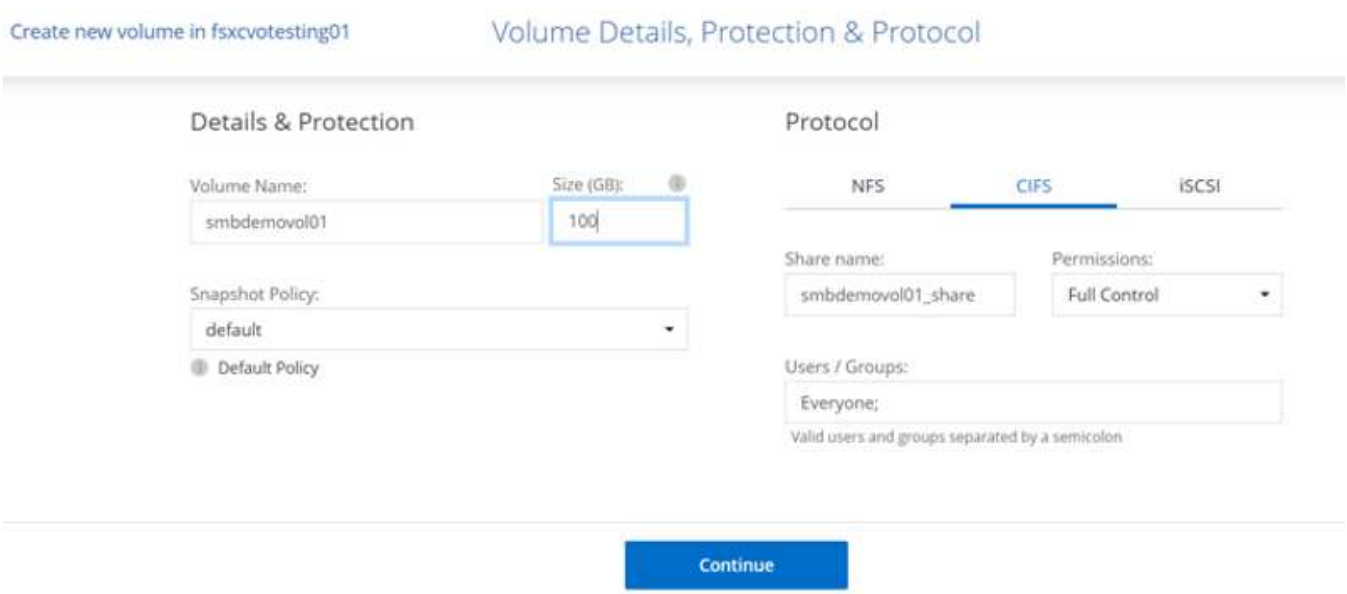


▼ **Configurations supplémentaires pour les volumes SMB**

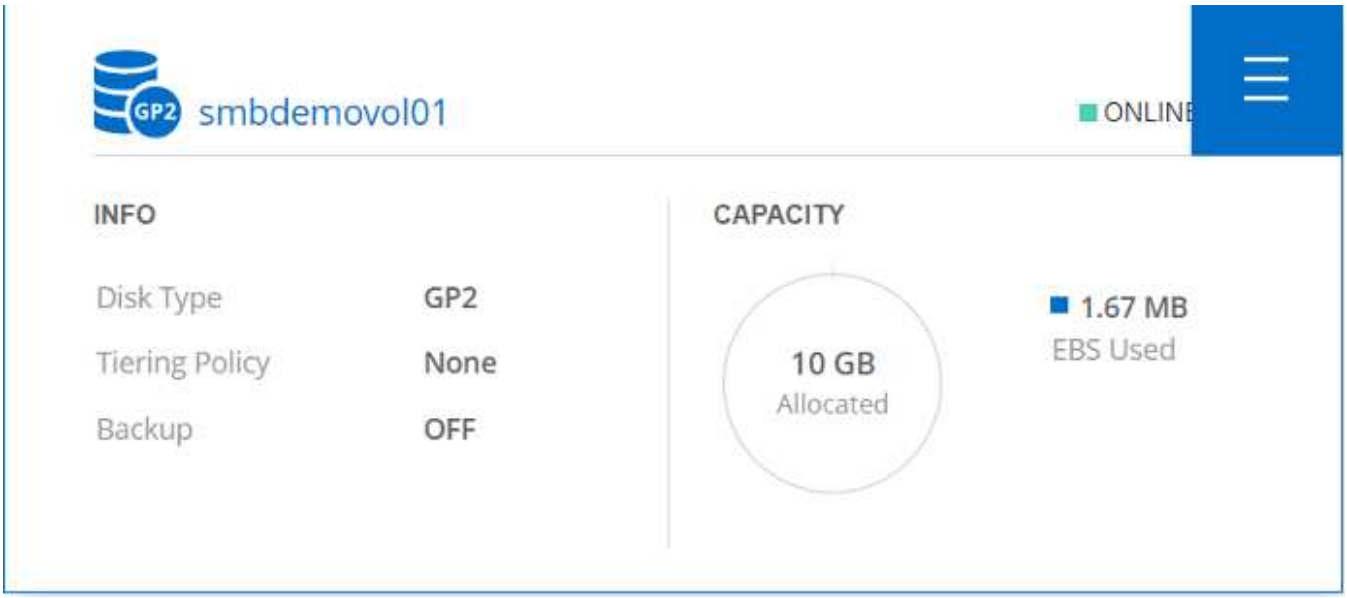
1. Une fois l'environnement de travail prêt, assurez-vous que le serveur CIFS est configuré avec les paramètres de configuration DNS et Active Directory appropriés. Cette étape est requise avant de pouvoir créer le volume SMB.



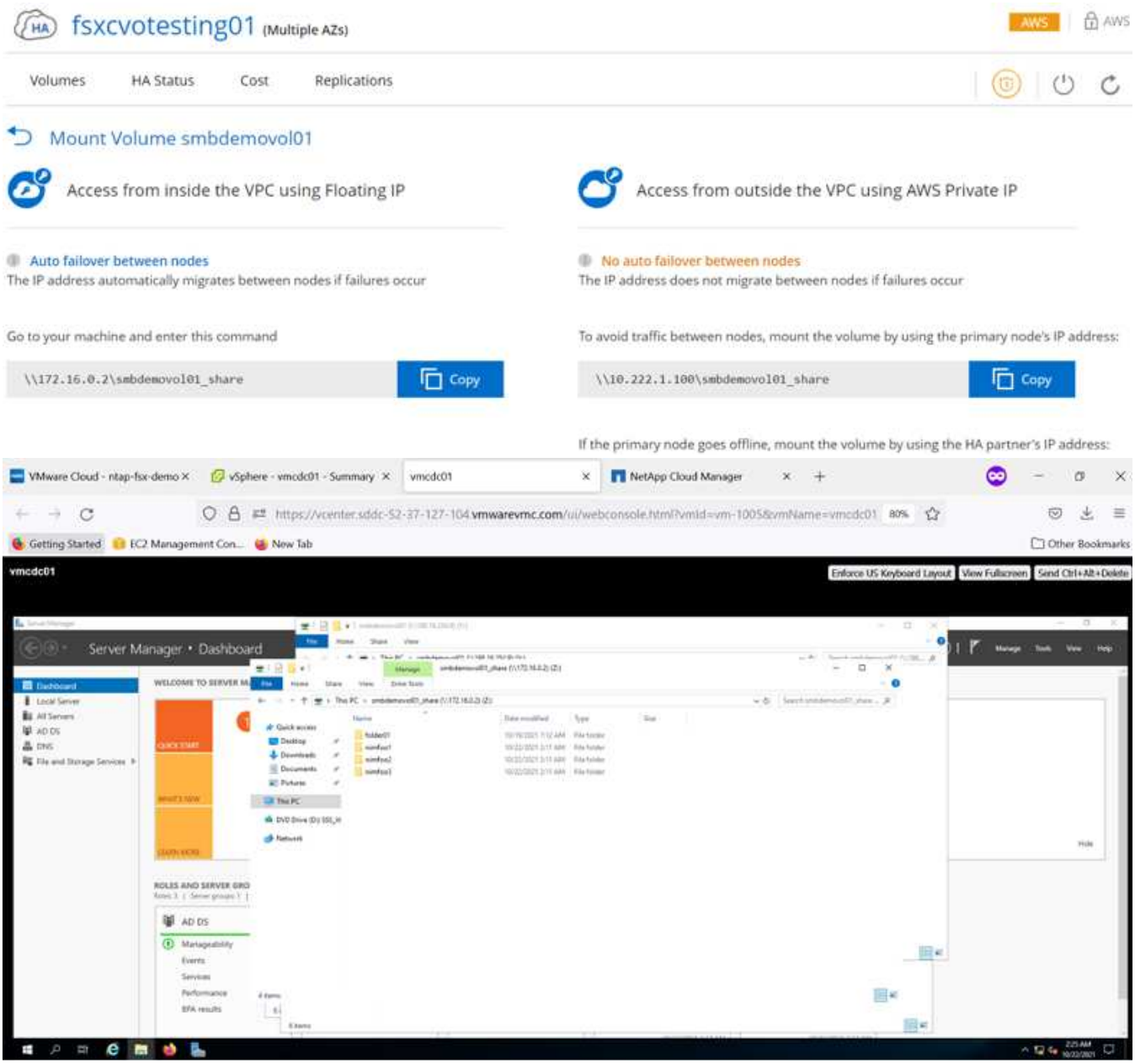
1. Sélectionnez l'instance CVO pour créer le volume et cliquez sur l'option Créer un volume. Choisissez la taille appropriée et le gestionnaire de cloud choisit l'agrégat contenant ou utilise un mécanisme d'allocation avancé pour le placer sur un agrégat spécifique. Pour cette démonstration, SMB est sélectionné comme protocole.



1. Une fois le volume provisionné, il est disponible dans le volet Volumes. Étant donné qu'un partage CIFS est provisionné, vous devez accorder à vos utilisateurs ou groupes l'autorisation d'accéder aux fichiers et dossiers et vérifier que ces utilisateurs peuvent accéder au partage et créer un fichier.



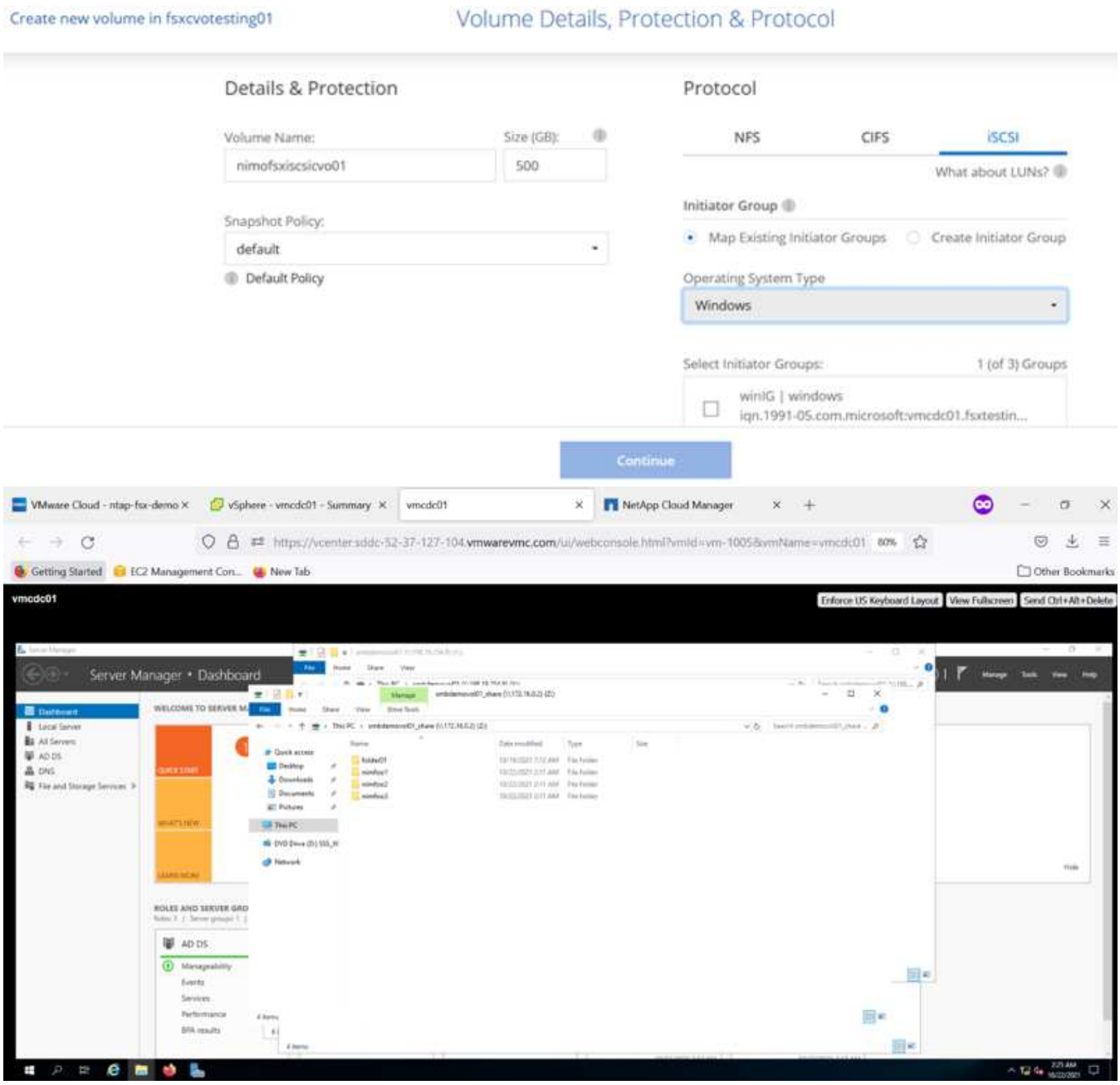
1. Une fois le volume créé, utilisez la commande mount pour vous connecter au partage à partir de la machine virtuelle exécutée sur les hôtes VMware Cloud dans AWS SDDC.
2. Copiez le chemin suivant et utilisez l'option Map Network Drive pour monter le volume sur la machine virtuelle exécutée sur VMware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



▼ **Connecter le LUN à un hôte**

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

1. Sur la page Cloud Manager Canvas, 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.



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

Pour réaliser la même chose pour l'hôte résidant sur le SDDC VMware Cloud sur AWS, procédez comme suit :

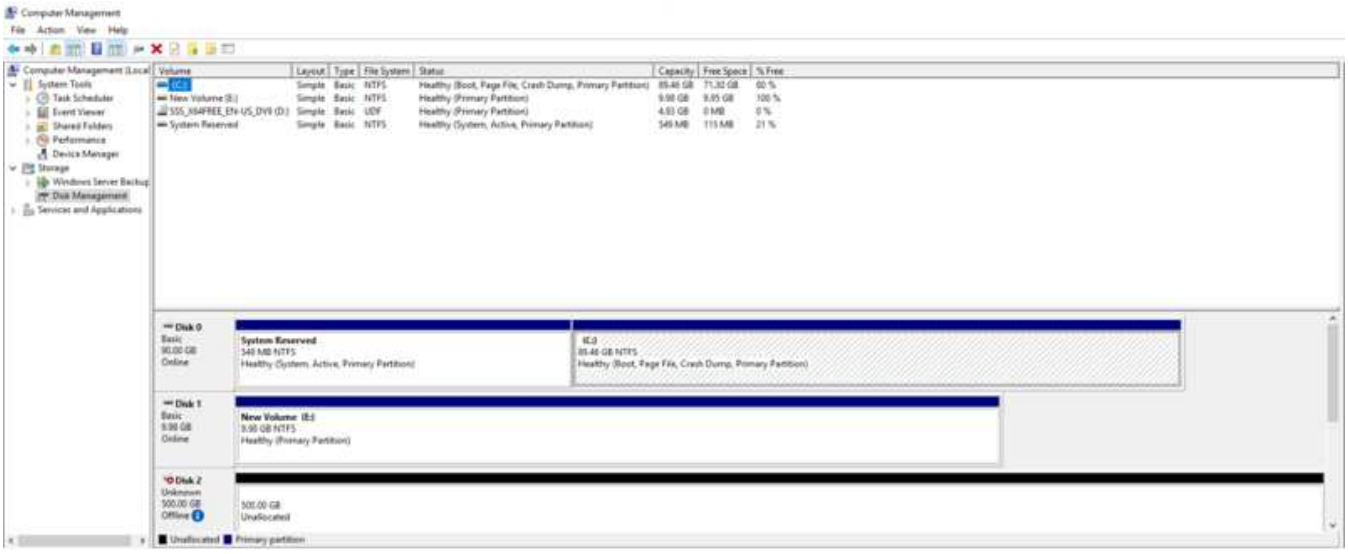
1. RDP vers la VM hébergée sur le cloud VMware sur AWS.
2. Ouvrez la boîte de dialogue Propriétés de l'initiateur iSCSI : Gestionnaire de serveur > Tableau de bord > Outils > Initiateur iSCSI.
3. Dans l'onglet Découverte, cliquez sur Découvrir le portail ou Ajouter un portail, puis entrez l'adresse IP du port cible iSCSI.
4. Dans l'onglet Cibles, sélectionnez la cible découverte, puis cliquez sur Connexion ou Connecter.
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 à utiliser.



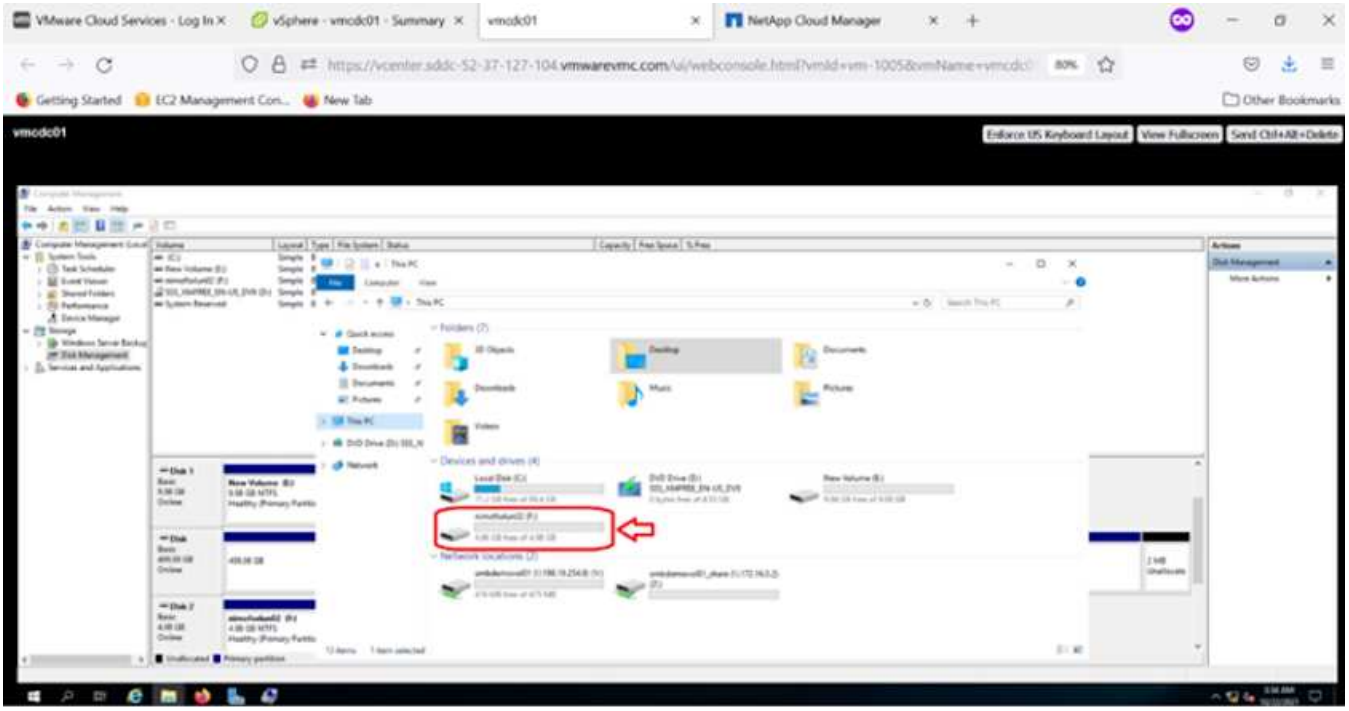
Les LUN du SVM apparaissent comme des disques pour l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclenchez une nouvelle analyse manuelle pour découvrir les disques en procédant comme suit :

1. Ouvrez l'utilitaire 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 > Réanalyser les disques.



Lorsqu'un nouveau LUN est accédé pour la première fois par l'hôte Windows, il ne possède aucune partition ni aucun système de fichiers. Initialisez le LUN ; et éventuellement, formatez le LUN avec un système de fichiers en procédant comme suit :

1. Démarrez la gestion des disques Windows.
2. Cliquez avec le bouton droit sur le 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 provisionnés, reportez-vous aux instructions détaillées sur la configuration iSCSI pour votre distribution Linux. Par exemple, la configuration iSCSI d'Ubuntu peut être trouvée"ici" . Pour vérifier, exécutez lsblk cmd depuis le shell.

▼ **Monter le volume NFS Cloud Volumes ONTAP sur un client Linux**

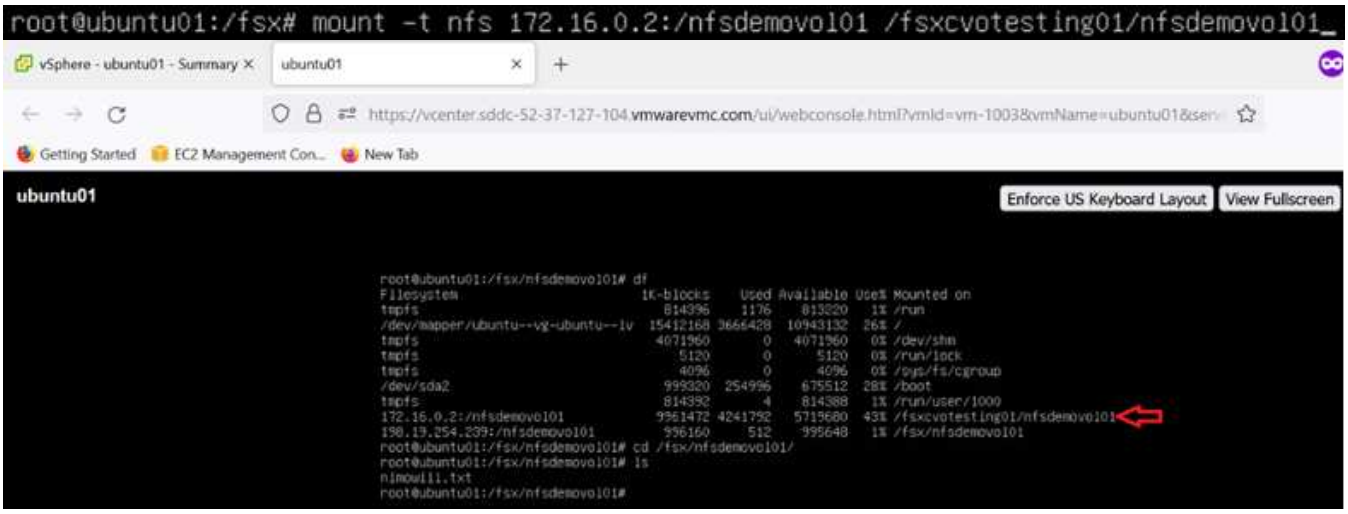
Pour monter le système de fichiers Cloud Volumes ONTAP (DIY) à partir de machines virtuelles dans VMC sur AWS SDDC, procédez comme suit :

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

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

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

```
/fsxcvotesting01/nfsdemovol01
```



Service de virtualisation Azure : options d'utilisation du stockage NetApp

Le stockage NetApp peut être attaché au service Azure VMware en tant que stockage invité connecté ou stockage supplémentaire.

Azure NetApp Files (ANF) comme banque de données NFS supplémentaire

La prise en charge du magasin de données NFS a été introduite avec la version 3 d'ESXi dans les déploiements sur site, ce qui a considérablement étendu les capacités de stockage de vSphere.

L'exécution de vSphere sur NFS est une option largement adoptée pour les déploiements de virtualisation sur site, car elle offre des performances et une stabilité élevées. Si vous disposez d'un stockage en réseau (NAS) important dans un centre de données local, vous devez envisager de déployer une solution Azure VMware SDDC dans Azure avec des magasins de données Azure NetApp File pour surmonter les problèmes de capacité et de performances.

Azure NetApp Files s'appuie sur le logiciel de gestion de données NetApp ONTAP , leader du secteur et hautement disponible. Les services Microsoft Azure sont regroupés en trois catégories : fondamentaux, grand public et spécialisés. Azure NetApp Files appartient à la catégorie spécialisée et s'appuie sur du matériel déjà déployé dans de nombreuses régions. Grâce à la haute disponibilité (HA) intégrée, Azure NetApp Files protège vos données contre la plupart des pannes et vous offre un SLA de pointe de 99,99 %^ de disponibilité.

Pour plus d'informations sur ANF en tant que banque de données NFS supplémentaire, veuillez visiter :

- "ANF comme banque de données NFS supplémentaire : présentation"
- "Option de banque de données NFS supplémentaire dans Azure"

Azure NetApp Files (ANF) en tant que stockage connecté invité

Azure NetApp Files apporte une gestion et un stockage de données de niveau entreprise à Azure afin que vous puissiez gérer vos charges de travail et vos applications en toute simplicité. Migrez vos charges de travail vers le cloud et exécutez-les sans sacrifier les performances.

Azure NetApp Files supprime les obstacles, vous permettant ainsi de déplacer toutes vos applications basées sur des fichiers vers le cloud. Pour la première fois, vous n'avez pas besoin de réarchitecturer vos applications

et vous obtenez un stockage persistant pour vos applications sans complexité.

Étant donné que le service est fourni via le portail Microsoft Azure, les utilisateurs bénéficient d'un service entièrement géré dans le cadre de leur contrat d'entreprise Microsoft. Un support de classe mondiale, géré par Microsoft, vous offre une tranquillité d'esprit totale. Cette solution unique vous permet d'ajouter rapidement et facilement des charges de travail multiprotocoles. Vous pouvez créer et déployer des applications basées sur des fichiers Windows et Linux, même pour les environnements hérités.

Pour plus d'informations, veuillez visiter"ANF comme stockage connecté aux invités" .

Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités

Cloud Volumes ONTAP (CVO) est la solution de gestion de données cloud leader du secteur, basée sur le logiciel de stockage ONTAP de NetApp, disponible nativement sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version définie par logiciel d' ONTAP qui consomme du stockage natif dans le cloud, vous permettant d'avoir le même logiciel de stockage dans le cloud et sur site, réduisant ainsi le besoin de recycler votre personnel informatique dans de toutes nouvelles méthodes de gestion de vos données.

CVO offre aux clients la possibilité de déplacer de manière transparente les données de la périphérie vers le centre de données, vers le cloud et vice-versa, en rassemblant votre cloud hybride, le tout géré avec une console de gestion à volet unique, NetApp Cloud Manager.

De par sa conception, CVO offre des performances extrêmes et des capacités avancées de gestion des données pour satisfaire même vos applications les plus exigeantes dans le cloud.

Pour plus d'informations, veuillez visiter"CVO comme stockage connecté aux invités" .

Présentation des solutions de stockage de données ANF

Toute organisation qui réussit est sur la voie 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, d'éclatement, d'extension et de reprise après sinistre aussi transparents que possible. Les clients qui migrent vers le cloud doivent évaluer les problèmes d'élasticité et d'éclatement, de sortie du centre de données, de consolidation du centre de données, de scénarios de fin de vie, de fusions, d'acquisitions, etc. L'approche adoptée par chaque organisation peut varier en fonction de leurs priorités commerciales respectives. Lors du choix d'opérations basées sur le cloud, la sélection d'un modèle à faible coût avec des performances appropriées et un minimum d'obstacles est un objectif essentiel. Outre le choix de la bonne plateforme, l'orchestration du stockage et des flux de travail est particulièrement importante pour libérer la puissance du déploiement et de l'élasticité du cloud.

Cas d'utilisation

Bien que la solution Azure VMware offre des fonctionnalités hybrides uniques à un client, les options de stockage natives limitées ont limité son utilité pour les organisations avec des charges de travail lourdes en stockage. Étant donné que le stockage est directement lié aux hôtes, la seule façon de faire évoluer le stockage est d'ajouter davantage d'hôtes, ce qui peut augmenter les coûts de 35 à 40 % ou plus pour les charges de travail gourmandes en stockage. Ces charges de travail nécessitent un stockage supplémentaire,

pas une puissance supplémentaire, mais cela signifie payer pour des hôtes supplémentaires.

Considérons le scénario suivant : un client a besoin de six hôtes pour la puissance (vCPU/vMem), mais il a également un besoin substantiel en stockage. Selon leur évaluation, ils ont besoin de 12 hôtes pour répondre aux besoins de stockage. Cela augmente le coût total de possession global car ils doivent acheter toute cette puissance supplémentaire alors qu'ils n'ont réellement besoin que de plus de stockage. Ceci s'applique à tout cas d'utilisation, y compris la migration, la reprise après sinistre, le bursting, le développement/test, etc.

Un autre cas d'utilisation courant d'Azure VMware Solution est la reprise après sinistre (DR). La plupart des organisations ne disposent pas d'une stratégie de reprise après sinistre infaillible ou peuvent avoir du mal à justifier l'exploitation d'un centre de données fantôme uniquement pour la reprise après sinistre. Les administrateurs peuvent explorer des options de reprise après sinistre sans empreinte avec un cluster pilote ou un cluster à la demande. Ils pourraient alors faire évoluer le stockage sans ajouter d'hôtes supplémentaires, ce qui pourrait être une option intéressante.

Ainsi, pour résumer, les cas d'utilisation peuvent être classés de deux manières :

- Mise à l'échelle de la capacité de stockage à l'aide des banques de données ANF
- Utilisation des banques de données ANF comme cible de reprise après sinistre pour un flux de travail de récupération optimisé en termes de coûts à partir de sites locaux ou au sein de régions Azure entre les centres de données définis par logiciel (SDDC). Ce guide fournit des informations sur l'utilisation Azure NetApp Files pour fournir un stockage optimisé pour les banques de données (actuellement en préversion publique) ainsi que des fonctionnalités de protection des données et de reprise après sinistre de premier ordre dans une solution Azure VMware, ce qui vous permet de décharger la capacité de stockage du stockage vSAN.



Contactez les architectes de solutions NetApp ou Microsoft de votre région pour obtenir des informations supplémentaires sur l'utilisation des magasins de données ANF.

Options VMware Cloud dans Azure

Solution Azure VMware

La solution Azure VMware (AVS) est un service cloud hybride qui fournit des SDDC VMware entièrement fonctionnels au sein d'un cloud public Microsoft Azure. AVS est une solution propriétaire entièrement gérée et prise en charge par Microsoft et 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 profitant de la présence mondiale de Microsoft Azure, de ses installations de centre de données de pointe et de sa proximité avec le riche écosystème de services et solutions Azure natifs. Une combinaison d'Azure VMware Solution SDDC et Azure NetApp Files offre les meilleures performances avec une latence réseau minimale.

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

- Hôtes VMware ESXi pour la virtualisation du calcul avec une appliance serveur vCenter pour la gestion.
- Stockage hyperconvergé VMware vSAN intégrant 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 pour la gestion.

Conclusion

Que vous cibliez un cloud entièrement ou un cloud hybride, les fichiers Azure NetApp offrent d'excellentes

options pour déployer et gérer les charges de travail des applications ainsi que les services de fichiers tout en réduisant le coût total de possession en rendant les exigences de données transparentes pour la couche applicative. Quel que soit le cas d'utilisation, choisissez Azure VMware Solution avec Azure NetApp Files pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site et sur plusieurs clouds, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise. Il s'agit du même processus et des mêmes procédures familiers utilisés pour connecter le stockage. N'oubliez pas que c'est simplement la position des données qui a changé avec les nouveaux noms ; les outils et les processus restent tous les mêmes et Azure NetApp Files aide à optimiser le déploiement global.

Plats à emporter

Les points clés de ce document comprennent :

- Vous pouvez désormais utiliser Azure NetApp Files comme banque de données sur AVS SDDC.
- Améliorez les temps de réponse des applications et offrez une plus grande disponibilité pour fournir un accès aux données de charge de travail quand et où cela est nécessaire.
- Simplifiez la complexité globale du stockage vSAN avec des capacités de redimensionnement simples et instantanées.
- Performances garanties pour les charges de travail critiques grâce à des capacités de remodelage dynamique.
- Si Azure VMware Solution Cloud est la destination, Azure NetApp Files est la solution de stockage adaptée pour un déploiement optimisé.

Où trouver des informations supplémentaires

Pour en savoir plus sur les informations décrites dans ce document, reportez-vous aux liens Web suivants :

- Documentation de 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/"

- Attacher des banques de données Azure NetApp Files aux hôtes Azure VMware Solution (version préliminaire)

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

Création d'une banque de données NFS supplémentaire dans Azure

La prise en charge du magasin de données NFS a été introduite avec la version 3 d'ESXi dans les déploiements sur site, ce qui a considérablement étendu les capacités de stockage de vSphere.

L'exécution de vSphere sur NFS est une option largement adoptée pour les déploiements de virtualisation sur site, car elle offre des performances et une stabilité élevées. Si vous disposez d'un stockage en réseau (NAS) important dans un centre de données local, vous devez envisager de déployer une solution Azure VMware SDDC dans Azure avec des magasins de données Azure NetApp File pour surmonter les problèmes de capacité et de performances.

Azure NetApp Files s'appuie sur le logiciel de gestion de données NetApp ONTAP , leader du secteur et hautement disponible. Les services Microsoft Azure sont regroupés en trois catégories : fondamentaux, grand public et spécialisés. Azure NetApp Files appartient à la catégorie spécialisée et s'appuie sur du matériel déjà déployé dans de nombreuses régions. Grâce à la haute disponibilité (HA) intégrée, Azure NetApp Files protège vos données de la plupart des pannes et vous offre un SLA de pointe de "99,99%" disponibilité.

Avant l'introduction de la fonctionnalité de banque de données Azure NetApp Files , les opérations de montée en charge pour les clients prévoyant d'héberger des charges de travail gourmandes en performances et en stockage nécessitaient l'extension du calcul et du stockage.

Gardez à l'esprit les points suivants :

- Les configurations de cluster déséquilibrées ne sont pas recommandées dans un cluster SDDC. Par conséquent, l'extension du stockage signifie l'ajout de plus 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 est en concurrence directe avec les charges de travail de production.
- Il n'existe aucune option permettant de fournir plusieurs niveaux de performances pour aligner les exigences, les performances et les coûts des applications.
- Il est facile d'atteindre les limites de la capacité de stockage pour vSAN construit sur des hôtes de cluster. En intégrant les offres de plate-forme en tant que service (PaaS) natives d'Azure comme Azure NetApp Files en tant que banque de données, les clients ont la possibilité de mettre à l'échelle leur stockage indépendamment et d'ajouter uniquement des nœuds de calcul au cluster SDDC selon les besoins. Cette capacité permet de surmonter les défis mentionnés ci-dessus.

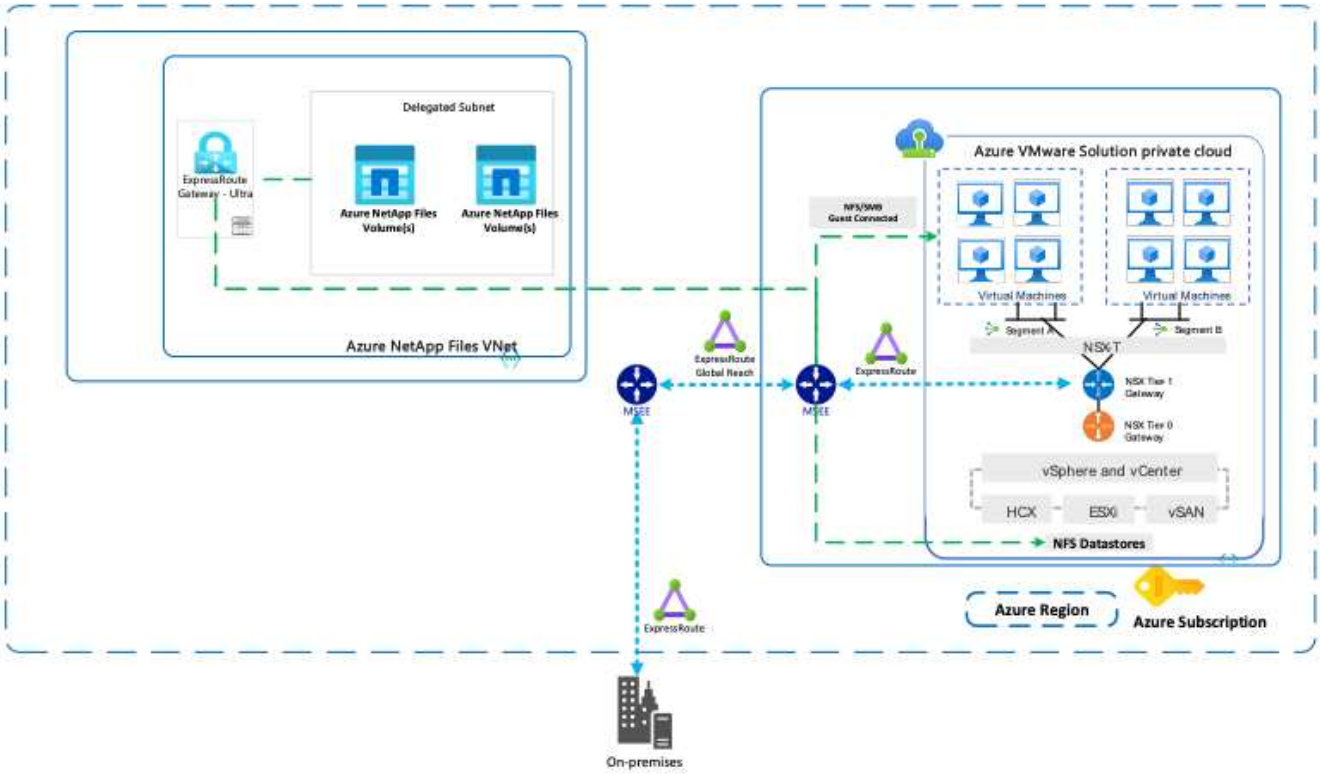
Azure NetApp Files vous permet également de déployer plusieurs banques de données, ce qui permet d'imiter un modèle de déploiement sur site en plaçant des machines virtuelles dans la banque de données appropriée et en attribuant le niveau de service requis pour répondre aux exigences de performances de la charge de travail. Grâce à la capacité unique de prise en charge multiprotocole, le stockage invité est une option supplémentaire pour les charges de travail de base de données telles que SQL et Oracle, tout en utilisant également la capacité de stockage de données NFS supplémentaire pour héberger les VMDK restants. En plus de cela, la capacité de capture instantanée native vous permet d'effectuer des sauvegardes rapides et des restaurations granulaires.



Contactez les architectes de solutions Azure et NetApp pour planifier et dimensionner le stockage et déterminer le nombre d'hôtes requis. NetApp recommande d'identifier les exigences de performances de stockage avant de finaliser la disposition du magasin de données pour les déploiements de test, de POC et de production.

Architecture détaillée

D'un point de vue général, cette architecture décrit comment obtenir une connectivité cloud hybride et une portabilité des applications dans les environnements locaux et Azure. Il décrit également l'utilisation Azure NetApp Files comme banque de données NFS supplémentaire et comme option de stockage en invité pour les machines virtuelles invitées hébergées sur la solution Azure VMware.



Dimensionnement

L'aspect le plus important de la migration ou de la reprise après sinistre est de déterminer la taille appropriée pour l'environnement cible. Il est très important de comprendre combien de nœuds sont nécessaires pour prendre en charge un exercice de transfert et de transfert des locaux vers la solution Azure VMware.

Pour le dimensionnement, utilisez les données historiques de l'environnement local à l'aide de RVTools (préféré) ou d'autres outils tels que Live Optics ou Azure Migrate. RVTools est un outil idéal pour capturer le vCPU, le vMem, le vDisk et toutes les informations requises, y compris les machines virtuelles sous tension ou hors tension, pour caractériser l'environnement cible.

Pour exécuter RVtools, procédez comme suit :

1. Téléchargez et installez RVTools.
2. Exécutez RVTools, entrez les informations requises pour vous connecter à votre serveur vCenter local et appuyez sur Connexion.
3. Exporter l'inventaire vers une feuille de calcul Excel.
4. Modifiez la feuille de calcul et supprimez toutes les machines virtuelles qui ne sont pas des candidats idéaux de l'onglet vInfo. Cette approche fournit une sortie claire sur les exigences de stockage qui peuvent être utilisées pour dimensionner correctement le cluster Azure VMware SDDC avec le nombre d'hôtes requis.

> Les machines virtuelles invitées utilisées avec le stockage invité doivent être calculées séparément ; cependant, Azure NetApp Files peut facilement couvrir la capacité de stockage supplémentaire, maintenant ainsi le coût total de possession global bas.

Déploiement et configuration de la solution Azure VMware

Comme sur site, la planification d'une solution Azure VMware est essentielle pour un environnement prêt pour

la production pour la création de machines virtuelles et la migration.

Cette section décrit comment configurer et gérer AVS pour une utilisation en combinaison avec Azure NetApp Files en tant que banque de données avec stockage invité également.

Le processus de configuration peut être divisé en trois parties :

- Enregistrez le fournisseur de ressources et créez un cloud privé.
- Connectez-vous à une passerelle de réseau virtuel ExpressRoute nouvelle ou existante.
- Validez la connectivité réseau et accédez au cloud privé. Se référer à ceci"lien" pour une présentation étape par étape du processus de provisionnement SDDC de la solution Azure VMware.

Configurer Azure NetApp Files avec Azure VMware Solution

La nouvelle intégration entre Azure NetApp Files vous permet de créer des banques de données NFS via les API/CLI du fournisseur de ressources Azure VMware Solution avec les volumes Azure NetApp Files et de monter les banques de données sur les clusters de votre choix dans un cloud privé. Outre l'hébergement des VMDK de machine virtuelle et d'application, les volumes de fichiers Azure NetApp peuvent également être montés à partir de machines virtuelles créées dans l'environnement Azure VMware Solution SDDC. Les volumes peuvent être montés sur le client Linux et mappés sur un client Windows, car Azure NetApp Files prend en charge les protocoles Server Message Block (SMB) et Network File System (NFS).

> Pour des performances optimales, déployez Azure NetApp Files dans la même zone de disponibilité que le cloud privé. La colocation avec le chemin rapide Express offre les meilleures performances, avec une latence réseau minimale.

Pour attacher un volume Azure NetApp File en tant que banque de données VMware d'un cloud privé Azure VMware Solution, assurez-vous que les conditions préalables suivantes sont remplies.

▼ Prérequis

1. Utilisez az login et validez que l'abonnement est enregistré dans la fonctionnalité CloudSanExperience dans l'espace de noms Microsoft.AVS.

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. S'il n'est pas enregistré, enregistrez-le.

```
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

> L'inscription peut prendre environ 15 minutes.

1. Pour vérifier l'état de l'enregistrement, exécutez la commande suivante.

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. Si l'enregistrement est bloqué dans un état intermédiaire pendant plus de 15 minutes, annulez l'enregistrement puis réenregistrez l'indicateur.

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. Vérifiez que l'abonnement est enregistré auprès de la fonctionnalité AnfDatastoreExperience dans l'espace de noms Microsoft.AVS.

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. Vérifiez que l'extension VMware est installée.

```
az extension show --name vmware
```

1. Si l'extension est déjà installée, vérifiez que la version est 3.0.0. Si une ancienne version est installée, mettez à jour l'extension.

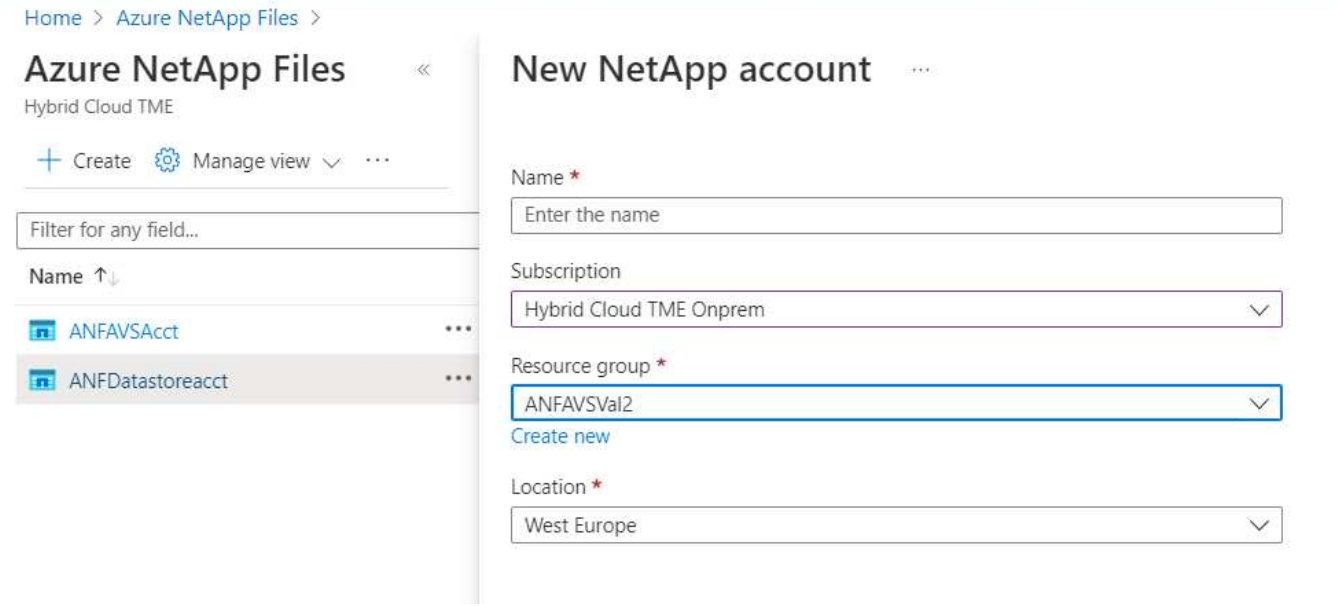
```
az extension update --name vmware
```

1. Si l'extension n'est pas déjà installée, installez-la.

```
az extension add --name vmware
```

▼ Créer et monter des volumes Azure NetApp Files

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 l' `az provider register --namespace Microsoft.NetApp –wait` commande. Après l'inscription, créez un compte NetApp . Se référer à ceci "lien" pour les étapes détaillées.



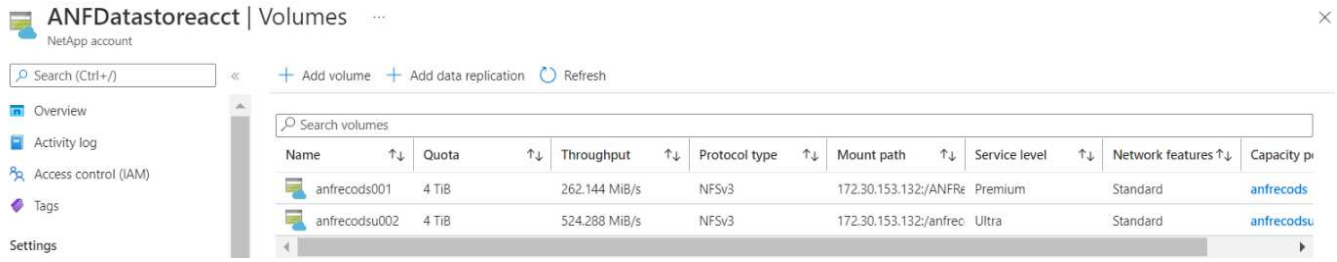
1. Une fois un compte NetApp créé, configurez des pools de capacité avec le niveau de service et la taille requis. Pour des informations détaillées, reportez-vous à ceci "lien" .



Points à retenir

- NFSv3 est pris en charge pour les banques de données sur Azure NetApp Files.
- Utilisez le niveau Premium ou standard pour les charges de travail liées à la capacité et le niveau Ultra pour les charges de travail liées aux performances si nécessaire tout en complétant le stockage vSAN par défaut.

1. Configurez un sous-réseau délégué pour Azure NetApp Files et spécifiez ce sous-réseau lors de la création de volumes. Pour connaître les étapes détaillées de création d'un sous-réseau délégué, reportez-vous à ceci "lien" .
2. Ajoutez un volume NFS pour la banque de données à l'aide de la lame Volumes sous la lame Pools de capacité.



Pour en savoir plus sur les performances des volumes Azure NetApp Files par taille ou par quota, consultez"Considérations sur les performances pour Azure NetApp Files" .

▼ **Ajouter une banque de données Azure NetApp Files au cloud privé**

Le volume Azure NetApp Files peut être attaché à votre cloud privé à l'aide du portail Azure. Suivez ceci"lien de Microsoft" pour une approche étape par étape de l'utilisation du portail Azure pour monter une banque de données de fichiers Azure NetApp .

Pour ajouter une banque de données Azure NetApp Files à un cloud privé, procédez comme suit :

1. Une fois les fonctionnalités requises enregistrées, attachez une banque de données NFS au cluster cloud privé Azure VMware Solution en exécutant la commande appropriée.
2. Créez une banque de données à l'aide d'un volume ANF existant dans le cluster cloud privé Azure VMware Solution.

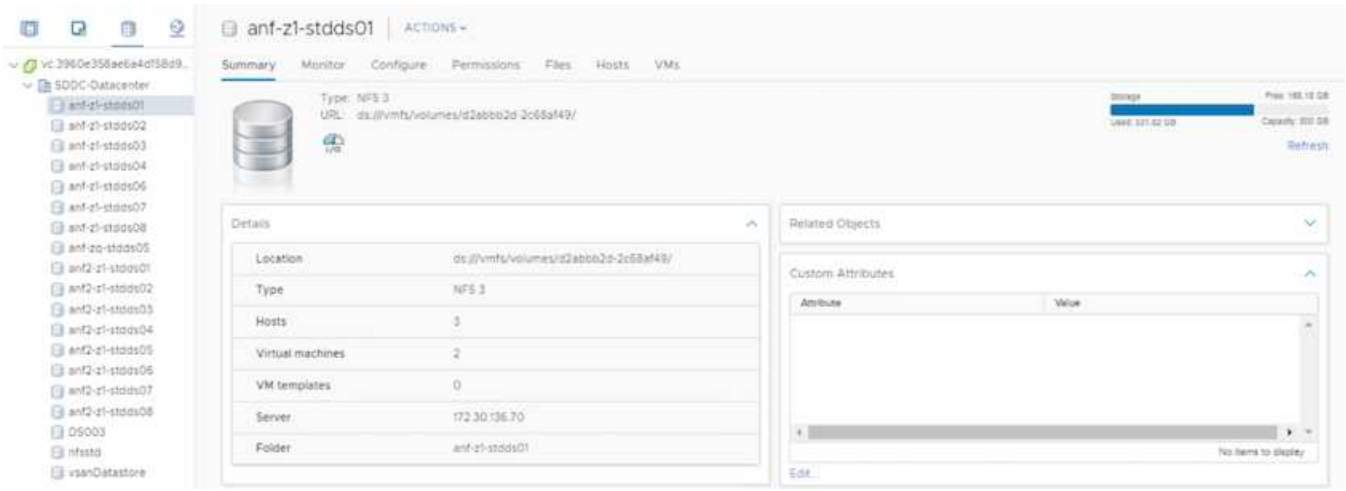
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

. List all the datastores in a private cloud cluster.
```

C:\Users\niyaz>az vmware datastore list --resource-group anfavsval2 --cluster Cluster-1 --private-cloud ANFDataClus [{ "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDS001", "name": "ANFRecoDS001", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001", "resourceGroup": "anfavsval2" }, "provisioningState": "Réussi", "resourceGroup": "anfavsval2", "type":

"Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": /subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp / NetApp/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": "Succeeded", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }]

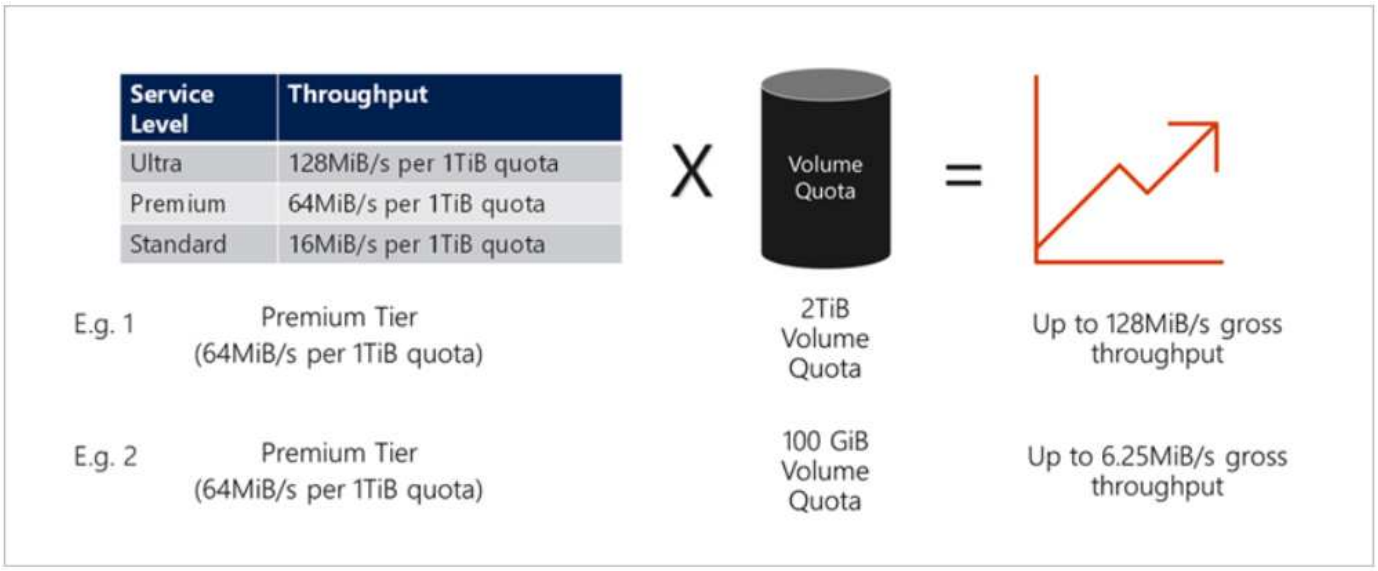
1. Une fois la connectivité nécessaire en place, les volumes sont montés en tant que banque de données.



Dimensionnement et optimisation des performances

Azure NetApp Files prend en charge trois niveaux de service : Standard (16 Mo/s par téraoctet), Premium (64 Mo/s par téraoctet) et Ultra (128 Mo/s par téraoctet). Le provisionnement de la taille de volume appropriée est important pour des performances optimales de la charge de travail de la base de données. Avec Azure NetApp Files, les performances du volume et la limite de débit sont déterminées en fonction des facteurs suivants :

- Le niveau de service du pool de capacité auquel appartient le volume
- Le quota attribué au volume
- Le type de qualité de service (QoS) (automatique ou manuel) du pool de capacité



Pour plus d'informations, consultez la section "Niveaux de service pour Azure NetApp Files" .

Se référer à ceci"lien de Microsoft" pour des critères de performance détaillés qui peuvent être utilisés lors d'un exercice de dimensionnement.

Points à retenir
• Utilisez le niveau Premium ou Standard pour les volumes de banque de données afin d'obtenir une capacité et des performances optimales. Si des performances sont requises, le niveau Ultra peut être utilisé. • Pour les exigences de montage invité, utilisez le niveau Premium ou Ultra et pour les exigences de partage de fichiers pour les machines virtuelles invitées, utilisez les volumes de niveau Standard ou Premium.

Considérations relatives aux performances

Il est important de comprendre qu'avec la version 3 de NFS, il n'existe qu'un seul canal actif pour la connexion entre l'hôte ESXi et une seule cible de stockage. Cela signifie que même s'il peut y avoir des connexions alternatives disponibles pour le basculement, la bande passante d'une seule banque de données et le stockage sous-jacent sont limités à ce qu'une seule connexion peut fournir.

Pour exploiter davantage de bande passante disponible avec les volumes Azure NetApp Files , un hôte ESXi doit disposer de plusieurs connexions aux cibles de stockage. Pour résoudre ce problème, vous pouvez configurer plusieurs banques de données, chaque banque de données utilisant des connexions distinctes entre l'hôte ESXi et le stockage.

Pour une bande passante plus élevée, il est recommandé de créer plusieurs banques de données à l'aide de plusieurs volumes ANF, de créer des VMDK et de répartir les volumes logiques sur les VMDK.

Se référer à ceci"lien de Microsoft" pour des critères de performance détaillés qui peuvent être utilisés lors d'un exercice de dimensionnement.

Points à retenir

- La solution Azure VMware autorise huit banques de données NFS par défaut. Cela peut être augmenté via une demande d'assistance.
- Tirez parti du chemin rapide ER avec Ultra SKU pour une bande passante plus élevée et une latence plus faible. Plus d'informations
- Avec les fonctionnalités réseau « De base » dans les fichiers Azure NetApp , la connectivité d'Azure VMware Solution est liée à la bande passante du circuit ExpressRoute et de la passerelle ExpressRoute.
- Pour les volumes Azure NetApp Files avec des fonctionnalités réseau « Standard », ExpressRoute FastPath est pris en charge. Lorsqu'il est activé, FastPath envoie le trafic réseau directement aux volumes Azure NetApp Files , contournant la passerelle, offrant une bande passante plus élevée et une latence plus faible.

Augmenter la taille du magasin de données

Le remodelage du volume et les changements dynamiques du niveau de service sont totalement transparents pour le SDDC. Dans Azure NetApp Files, ces fonctionnalités offrent des optimisations continues des performances, de la capacité et des coûts. Augmentez la taille des banques de données NFS en redimensionnant le volume à partir du portail Azure ou en utilisant l'interface de ligne de commande. Une fois que vous avez terminé, accédez à vCenter, accédez à l'onglet Banque de données, cliquez avec le bouton droit sur la banque de données appropriée et sélectionnez Actualiser les informations de capacité. Cette approche peut être utilisée pour augmenter la capacité du magasin de données et pour augmenter les performances du magasin de données de manière dynamique sans temps d'arrêt. Ce processus est également totalement transparent pour les applications.

Points à retenir

- La refonte du volume et la capacité de niveau de service dynamique vous permettent d'optimiser les coûts en dimensionnant les charges de travail en régime permanent et ainsi d'éviter le surprovisionnement.
- VAAI n'est pas activé.

Charges de travail

▼ Migration

L'un des cas d'utilisation les plus courants est la migration. Utilisez VMware HCX ou vMotion pour déplacer des machines virtuelles sur site. Vous pouvez également utiliser Rivermeadow pour migrer des machines virtuelles vers des banques de données Azure NetApp Files .

▼ Protection des données

La sauvegarde des machines virtuelles et leur récupération rapide font partie des grands atouts des datastores ANF. Utilisez des copies instantanées pour créer des copies rapides de votre machine virtuelle ou de votre banque de données sans affecter les performances, puis envoyez-les vers le stockage Azure pour une protection des données à plus long terme ou vers une région secondaire à l'aide de la réplication interrégionale à des fins de reprise après sinistre. Cette approche minimise l'espace de stockage et la bande passante du réseau en stockant uniquement les informations modifiées.

Utilisez des copies instantanées Azure NetApp Files pour une protection générale et utilisez des outils d'application pour protéger les données transactionnelles telles que SQL Server ou Oracle résidant sur les machines virtuelles invitées. Ces copies Snapshot sont différentes des snapshots VMware (cohérence) et conviennent à une protection à plus long terme.

Avec les banques de données ANF, l'option Restaurer vers un nouveau volume peut être utilisée pour cloner un volume de banque de données entier, et le volume restauré peut être monté comme une autre banque de données sur des hôtes dans AVS SDDC. Une fois qu'un magasin de données est monté, les machines virtuelles qu'il contient peuvent être enregistrées, reconfigurées et personnalisées comme s'il s'agissait de machines virtuelles clonées individuellement.

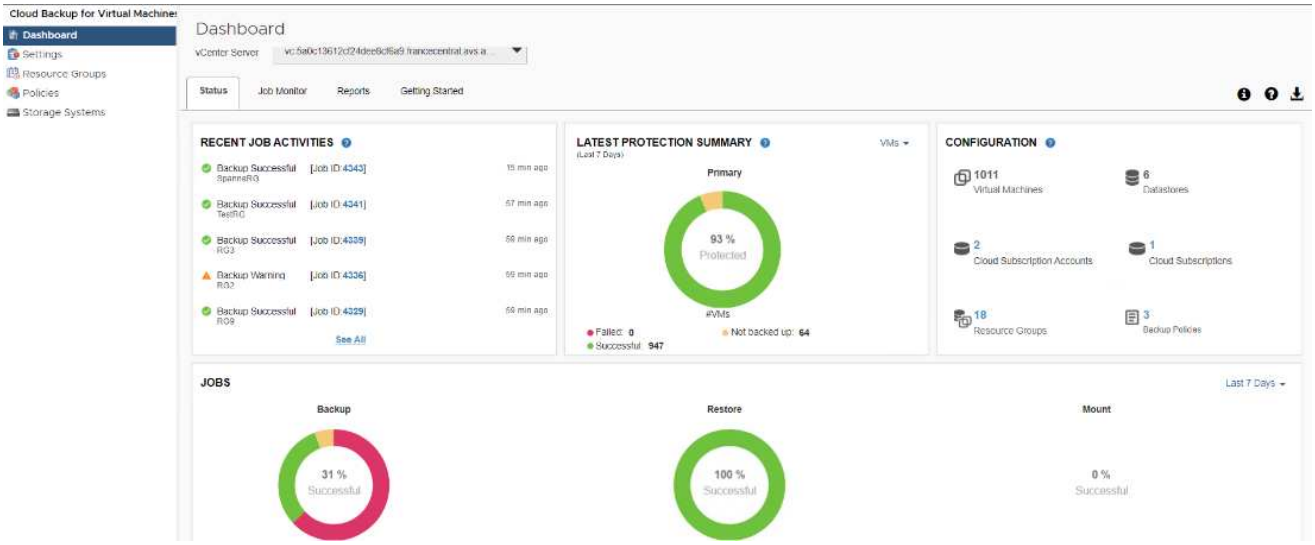
▼ NetApp Backup and Recovery pour machines virtuelles

NetApp Backup and Recovery for Virtual Machines fournit une interface graphique web client vSphere sur vCenter pour protéger les machines virtuelles Azure VMware Solution et les datastores Azure NetApp Files via des règles de sauvegarde. Ces règles peuvent définir la planification, la conservation et d'autres fonctionnalités. La fonctionnalité NetApp Backup and Recovery for Virtual Machine peut être déployée à l'aide de la commande Exécuter.

Les politiques de configuration et de protection peuvent être installées en suivant les étapes suivantes :

1. Installez NetApp Backup and Recovery for Virtual Machine dans le cloud privé Azure VMware Solution à l'aide de la commande Run.
2. Ajoutez les informations d'identification d'abonnement cloud (client et valeur secrète), puis ajoutez un compte d'abonnement cloud (compte NetApp et groupe de ressources associé) qui contient les ressources que vous souhaitez protéger.
3. Créez une ou plusieurs stratégies de sauvegarde qui gèrent la rétention, la fréquence et d'autres paramètres pour les sauvegardes de groupes de ressources.
4. Créez un conteneur pour ajouter une ou plusieurs ressources qui doivent être protégées avec des politiques de sauvegarde.
5. En cas de panne, restaurez l'intégralité de la machine virtuelle ou des VMDK individuels spécifiques au même emplacement.

Avec la technologie Azure NetApp Files Snapshot, les sauvegardes et les restaurations sont très rapides.



▼ Reprise après sinistre avec Azure NetApp Files, JetStream DR et Azure VMware Solution

La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données (par exemple, les

ransomwares). À l'aide de l'infrastructure VMware VAIO, les charges de travail VMware sur site peuvent être répliquées vers le stockage Azure Blob et récupérées, ce qui permet une perte de données minimale ou quasi nulle et un RTO proche de zéro. JetStream DR peut être utilisé pour récupérer de manière transparente les charges de travail répliquées sur site vers AVS et plus particulièrement vers Azure NetApp Files. Il permet une reprise après sinistre rentable en utilisant un minimum de ressources sur le site de reprise après sinistre et un stockage cloud rentable. JetStream DR automatise la récupération vers les banques de données ANF via Azure Blob Storage. JetStream DR récupère des machines virtuelles indépendantes ou des groupes de machines virtuelles associées dans l'infrastructure du site de récupération en fonction du mappage réseau et fournit une récupération ponctuelle pour la protection contre les ransomwares.

"Solution DR avec ANF, JetStream et AVS" .

Options de stockage invité NetApp connectées pour Azure

Azure prend en charge le stockage NetApp connecté aux invités avec le service Azure NetApp Files (ANF) natif ou avec Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure netApp Files apporte une gestion et un stockage de données de niveau entreprise à Azure afin que vous puissiez gérer vos charges de travail et vos applications en toute simplicité. Migrez vos charges de travail vers le cloud et exécutez-les sans sacrifier les performances.

Azure netApp Files supprime les obstacles, vous permettant ainsi de déplacer toutes vos applications basées sur des fichiers vers le cloud. Pour la première fois, vous n'avez pas besoin de réarchitecturer vos applications et vous obtenez un stockage persistant pour vos applications sans complexité.

Étant donné que le service est fourni via le portail Microsoft Azure, les utilisateurs bénéficient d'un service entièrement géré dans le cadre de leur contrat d'entreprise Microsoft. Un support de classe mondiale, géré par Microsoft, vous offre une tranquillité d'esprit totale. Cette solution unique vous permet d'ajouter rapidement et facilement des charges de travail multiprotocoles. Vous pouvez créer et déployer des applications basées sur des fichiers Windows et Linux, même pour les environnements hérités.

Azure NetApp Files (ANF) en tant que stockage connecté invité

▼ **Configurer Azure NetApp Files avec Azure VMware Solution (AVS)**

Les partages Azure NetApp Files peuvent être montés à partir de machines virtuelles 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.

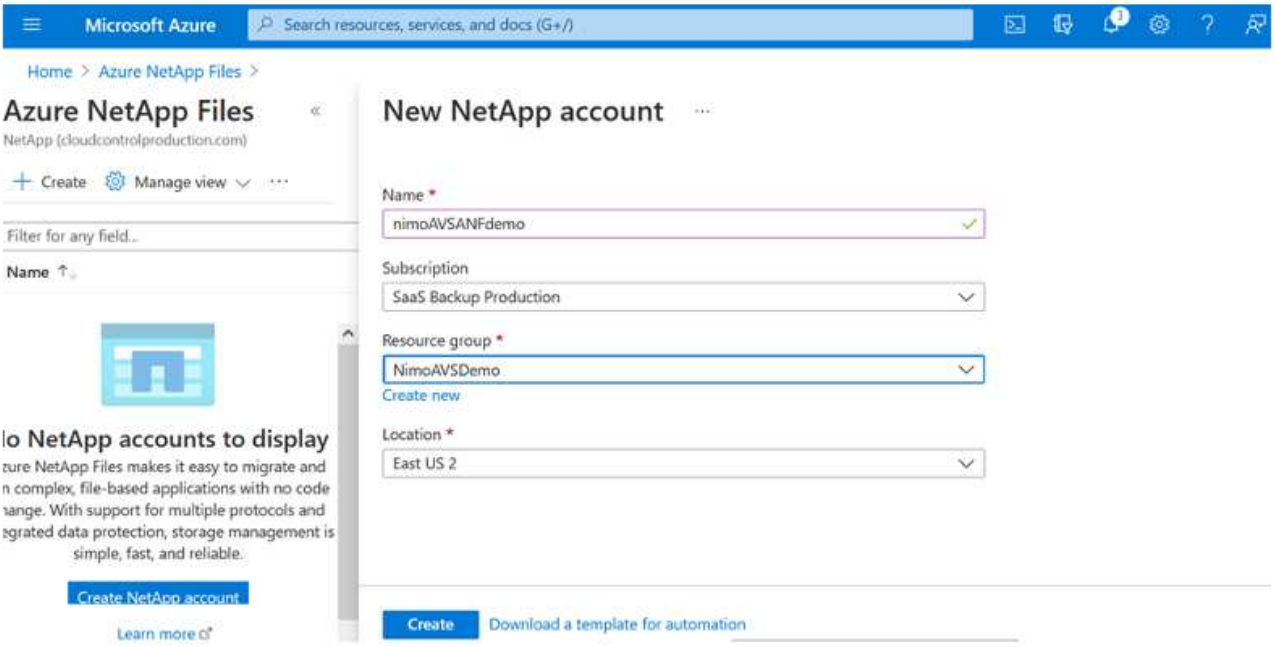
Azure NetApp Files et Azure VMware Solution doivent se trouver dans la même région Azure.

▼ **Créer et monter des volumes Azure NetApp Files**

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

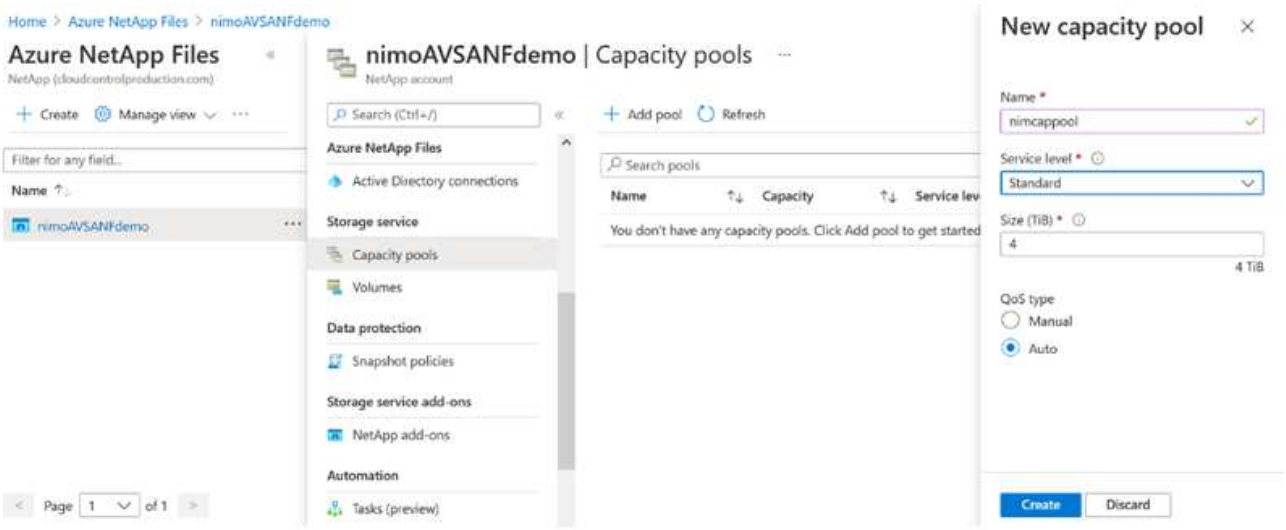
1. Connectez-vous au portail Azure et accédez à Azure NetApp Files. Vérifiez l'accès au service Azure NetApp Files et enregistrez le fournisseur de ressources Azure NetApp Files à l'aide de la commande *az provider register --namespace Microsoft. NetApp –wait*. Une fois l'inscription terminée, créez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

   Pour les étapes détaillées, voir"Partages Azure NetApp Files" . Cette page vous guidera à travers le processus étape par étape.

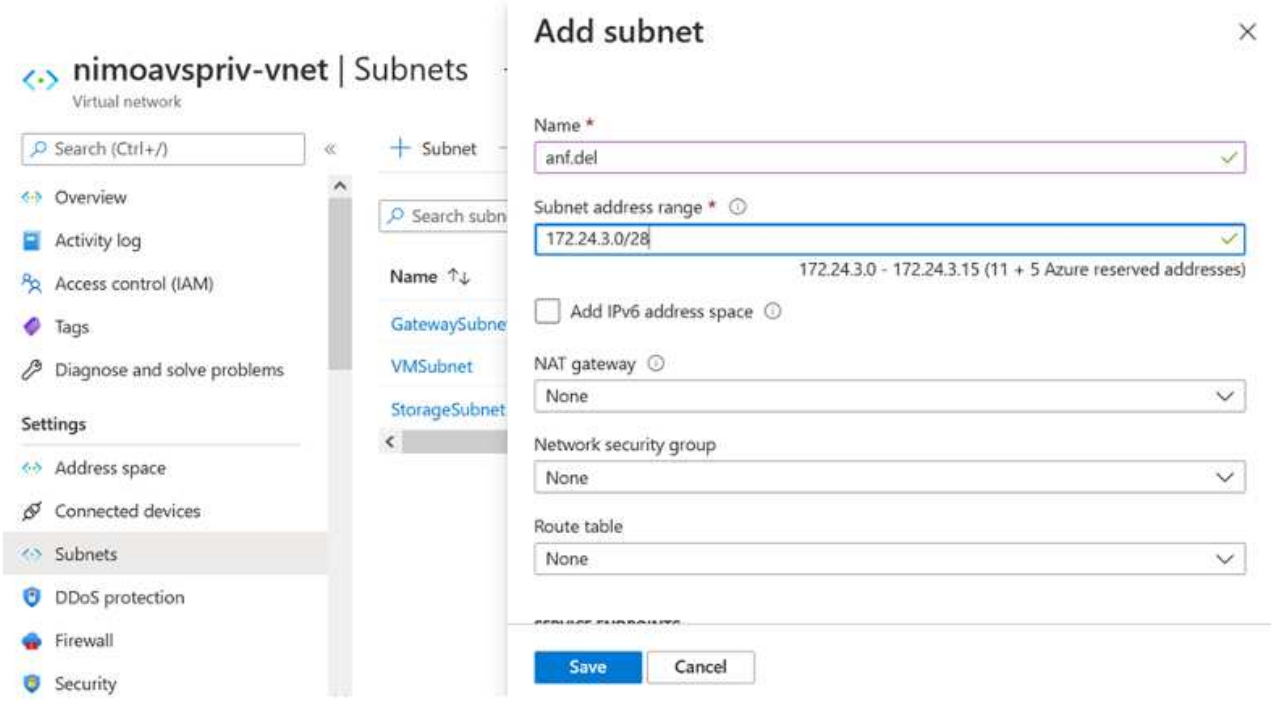


2. Une fois le compte NetApp créé, configurez les pools de capacité avec le niveau de service et la taille requis.

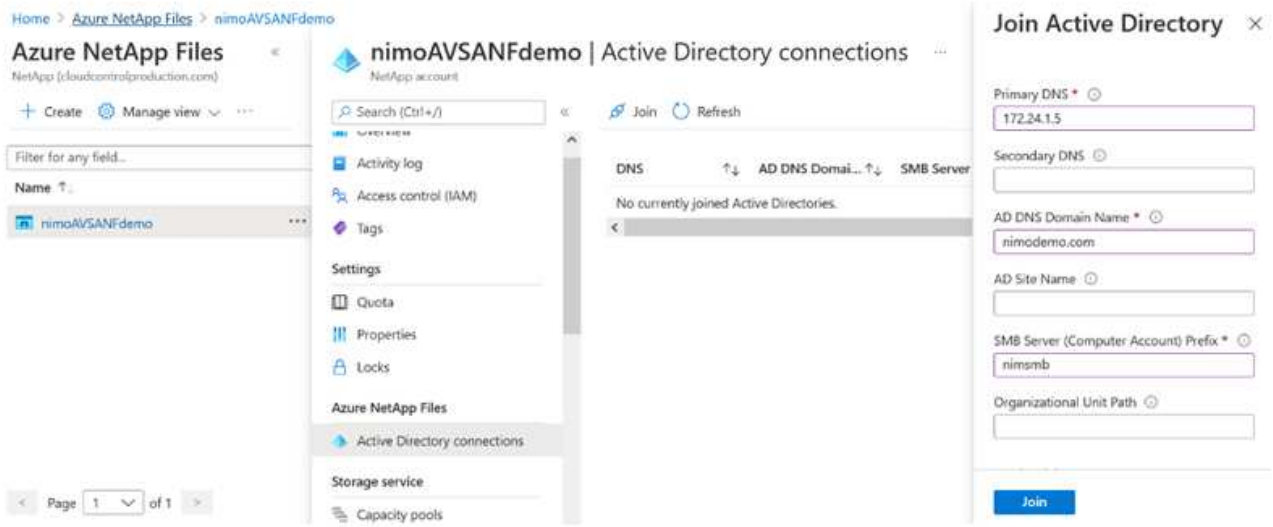
   Pour plus d'informations, consultez la section "Mettre en place un pool de capacité" .



3. Configurez le sous-réseau délégué pour Azure NetApp Files et spécifiez ce sous-réseau lors de la création des volumes. Pour les étapes détaillées de création d'un sous-réseau délégué, voir"Déléguer un sous-réseau à Azure NetApp Files" .

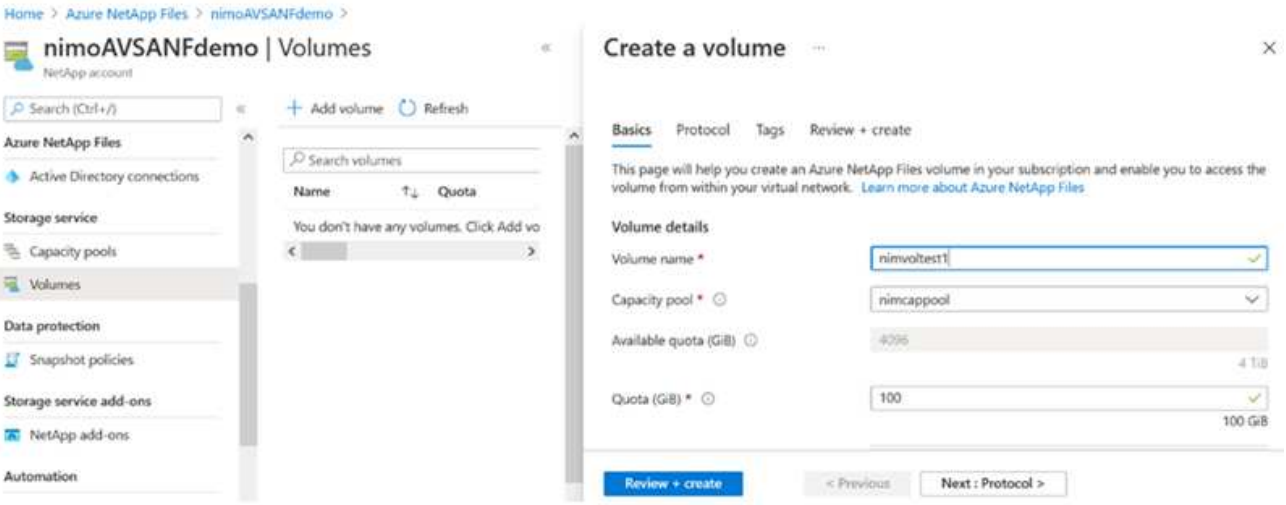


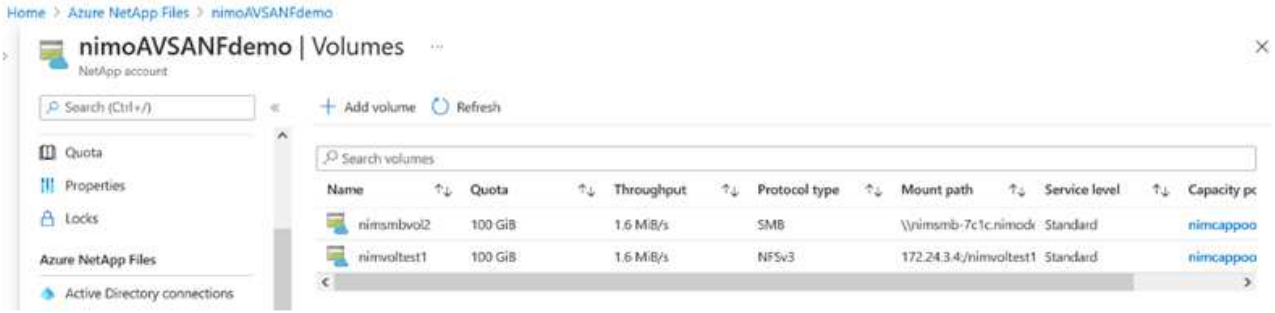
4. Ajoutez un volume SMB à l'aide de la lame Volumes sous la lame Pools de capacité. Assurez-vous que le connecteur Active Directory est configuré avant de créer le volume SMB.



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

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

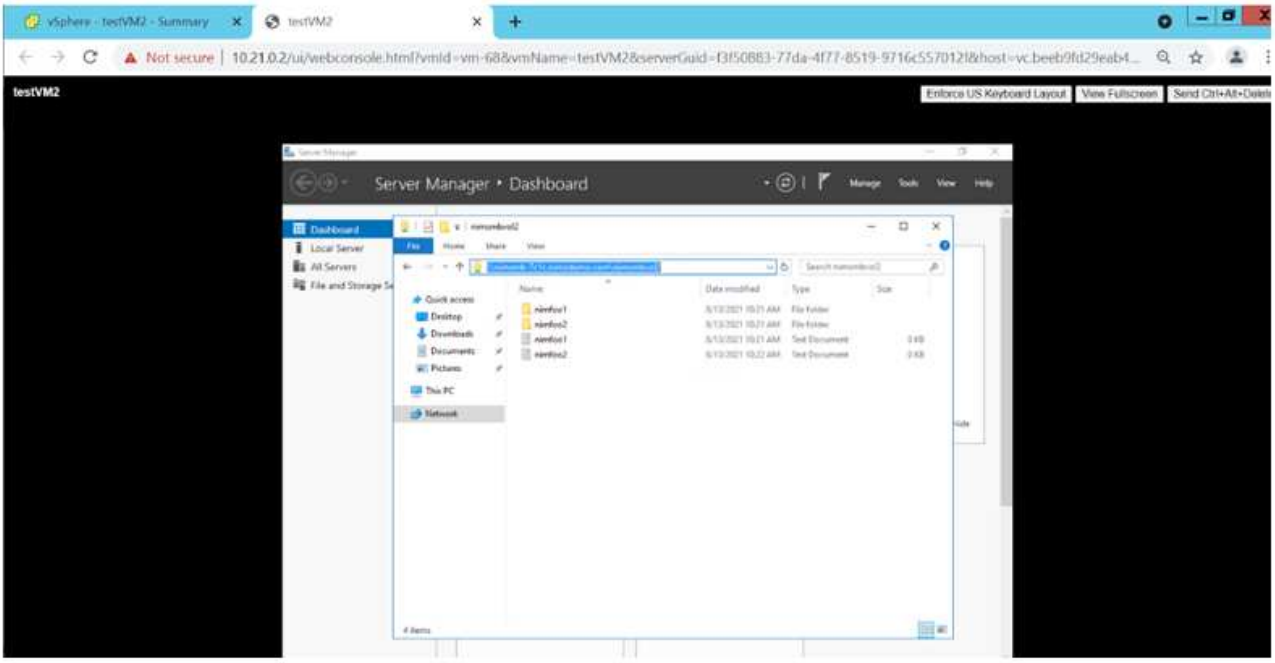


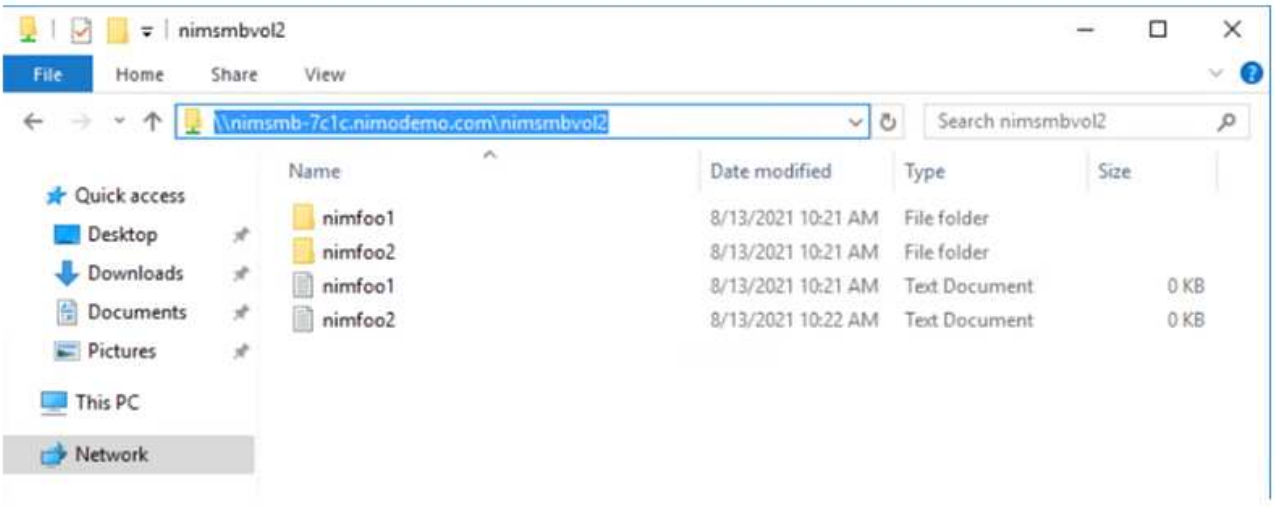


Pour en savoir plus sur les performances des volumes Azure NetApp Files par taille ou par quota, consultez"Considérations sur les performances pour Azure NetApp Files" .

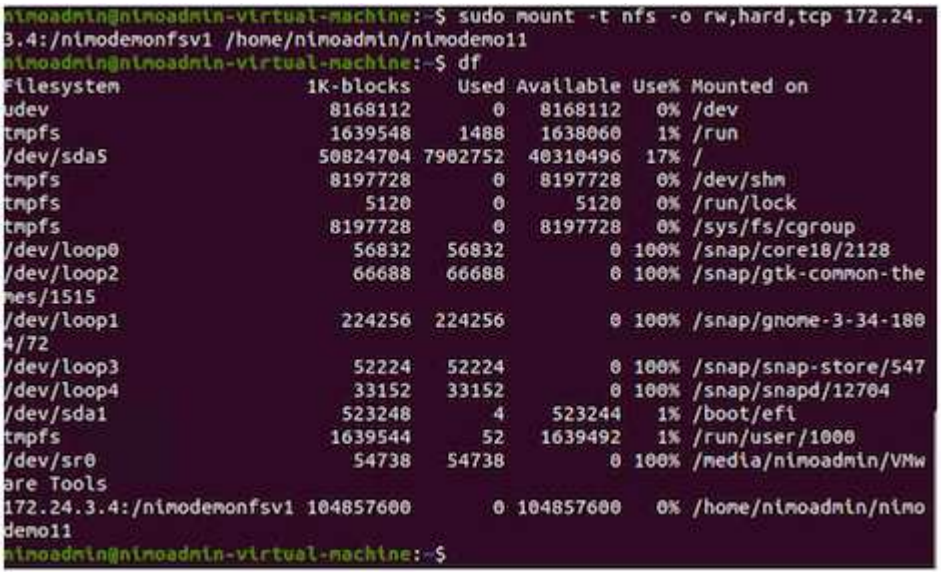
6. Une fois la connectivité établie, le volume peut être monté et utilisé pour les données d'application.

   Pour ce faire, à partir du portail Azure, cliquez sur le panneau Volumes, puis sélectionnez le volume à monter et accédez aux instructions de montage. Copiez le chemin 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 exécutées sur Azure VMware Solution SDDC, utilisez ce même processus. Utilisez la capacité de remodelage du volume ou de niveau de service dynamique pour répondre aux exigences de charge de travail.



Pour plus d'informations, consultez la section "Modifier dynamiquement le niveau de service d'un volume" .

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, ou CVO, est la solution de gestion de données cloud leader du secteur, basée sur le logiciel de stockage ONTAP de NetApp, disponible nativement sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version définie par logiciel d' ONTAP qui consomme du stockage natif dans le cloud, vous permettant d'avoir le même logiciel de stockage dans le cloud et sur site, réduisant ainsi le besoin de recycler votre personnel informatique dans de toutes nouvelles méthodes de gestion de vos données.

CVO offre aux clients la possibilité de déplacer de manière transparente les données de la périphérie vers le centre de données, vers le cloud et vice-versa, en rassemblant votre cloud hybride, le tout géré avec une console de gestion à volet unique, NetApp Cloud Manager.

De par sa conception, CVO offre des performances extrêmes et des capacités avancées de gestion des données pour satisfaire même vos applications les plus exigeantes dans le cloud.

Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités

▼ Déployer de nouveaux Cloud Volumes ONTAP dans Azure

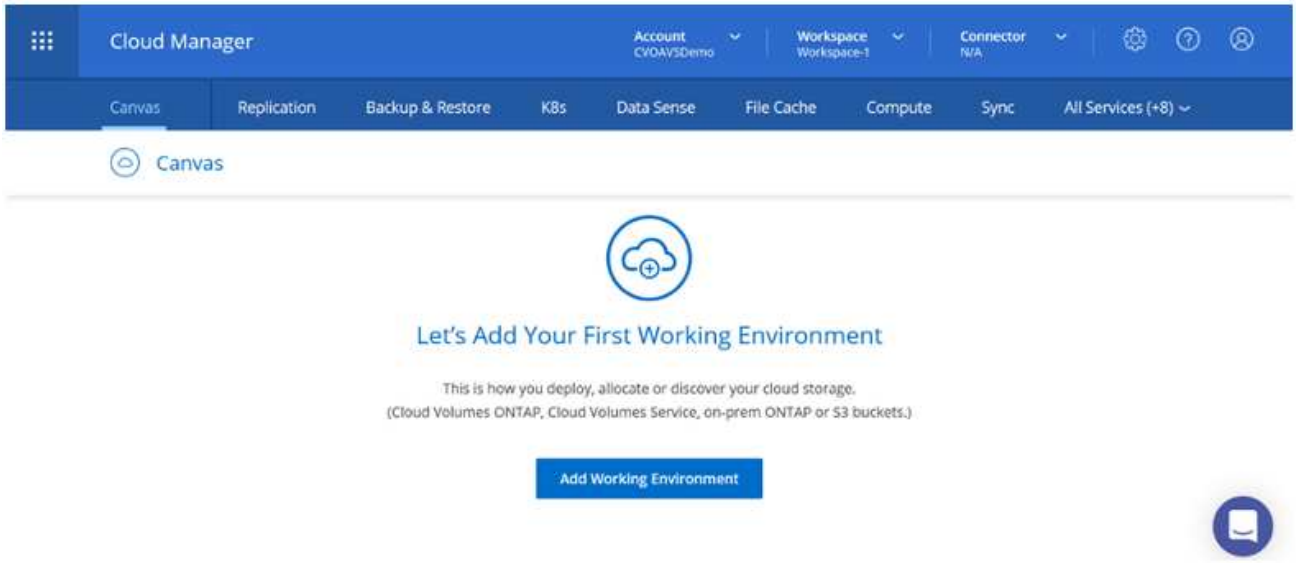
Les partages et LUN Cloud Volumes ONTAP peuvent être montés à partir de machines virtuelles créées dans l'environnement Azure VMware Solution SDDC. Les volumes peuvent également être montés sur le client Linux et sur le client Windows, car Cloud Volumes ONTAP prend en charge les protocoles iSCSI, SMB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

Pour répliquer des volumes d'un environnement local vers le cloud à des fins de reprise après sinistre ou de migration, établissez une connectivité réseau à Azure, soit à l'aide d'un VPN site à site, soit d'ExpressRoute. La réplication des données sur site vers Cloud Volumes ONTAP n'entre pas dans le cadre de ce document. Pour répliquer des données entre les systèmes locaux et Cloud Volumes ONTAP , consultez"Configuration de la réplication des données entre les systèmes" .

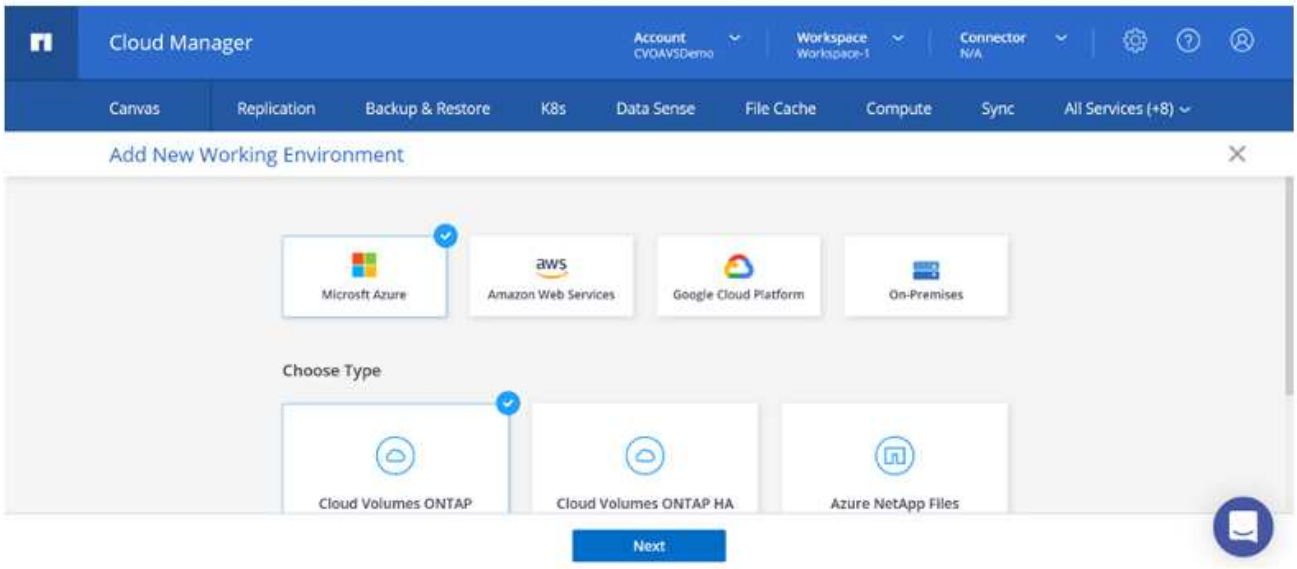
Utilisez "Dimensionneur Cloud Volumes ONTAP" pour dimensionner précisément les instances Cloud Volumes ONTAP. Surveillez également les performances sur site afin de les

utiliser comme données d'entrée dans l'outil de dimensionnement Cloud Volumes ONTAP.

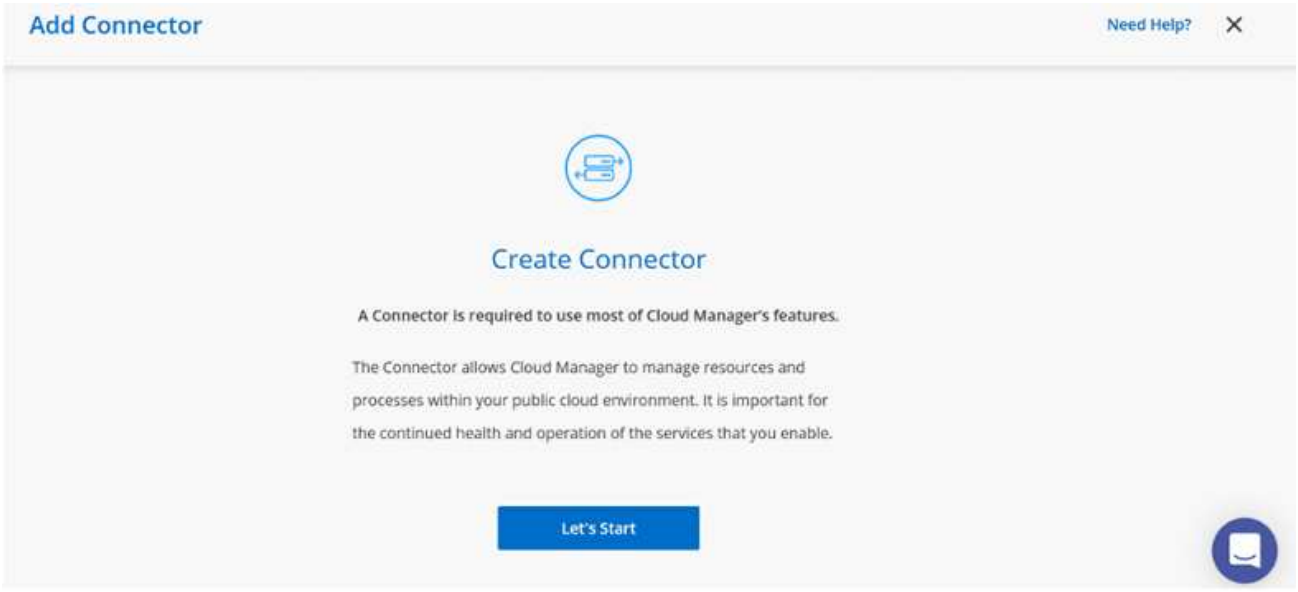
1. Connectez-vous à NetApp Cloud Central : l'écran Fabric View s'affiche. Localisez l'onglet Cloud Volumes ONTAP et sélectionnez Accéder au Gestionnaire de Cloud. Une fois connecté, l'écran Canvas s'affiche.



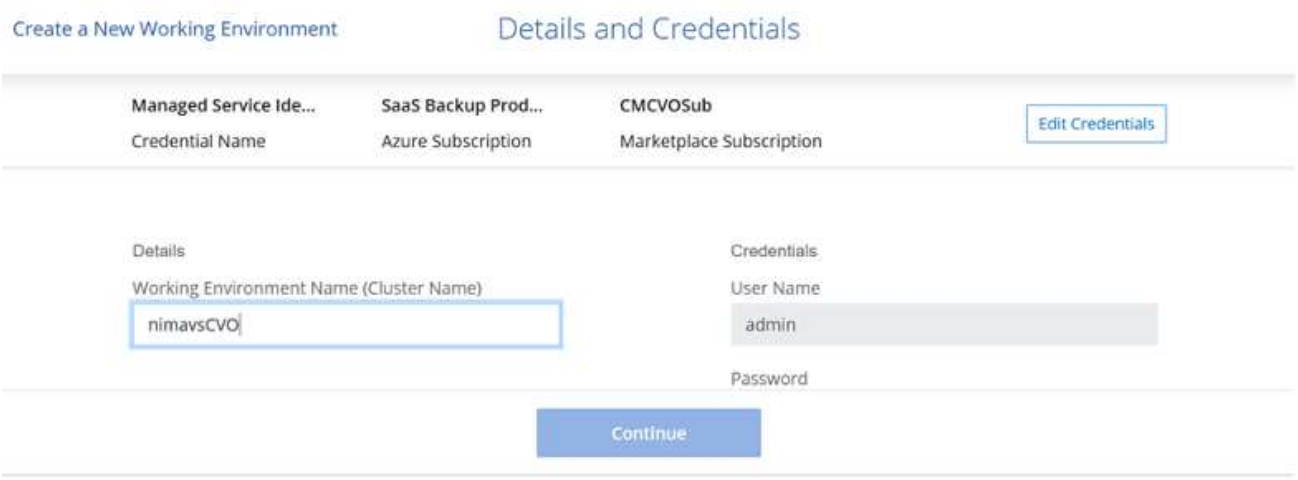
2. Sur la page d'accueil de Cloud Manager, cliquez sur Ajouter un environnement de travail, puis sélectionnez Microsoft Azure comme cloud et le type de configuration système.



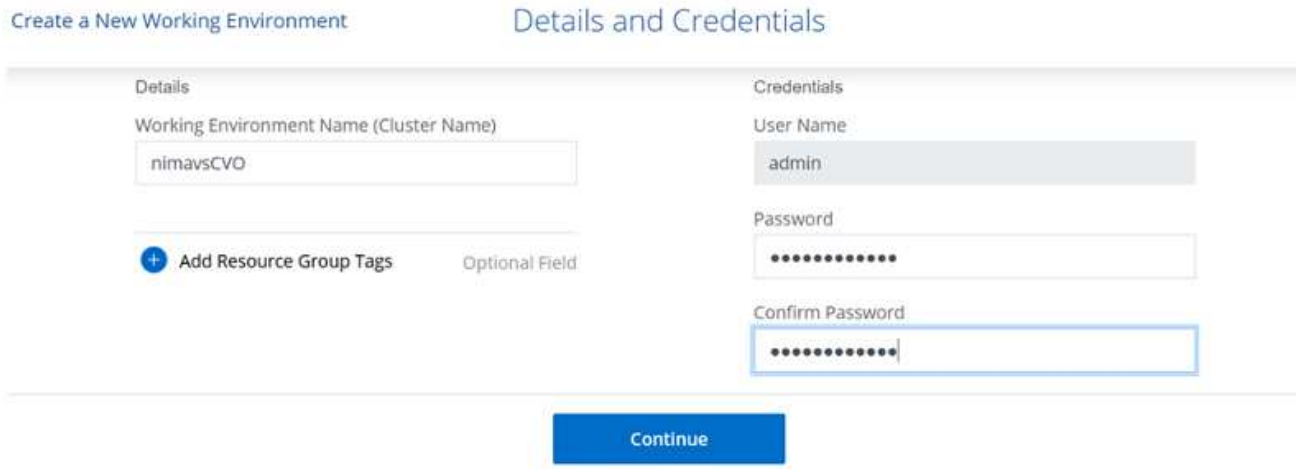
3. Lors de la création du premier environnement de travail Cloud Volumes ONTAP , Cloud Manager vous invite à déployer un connecteur.



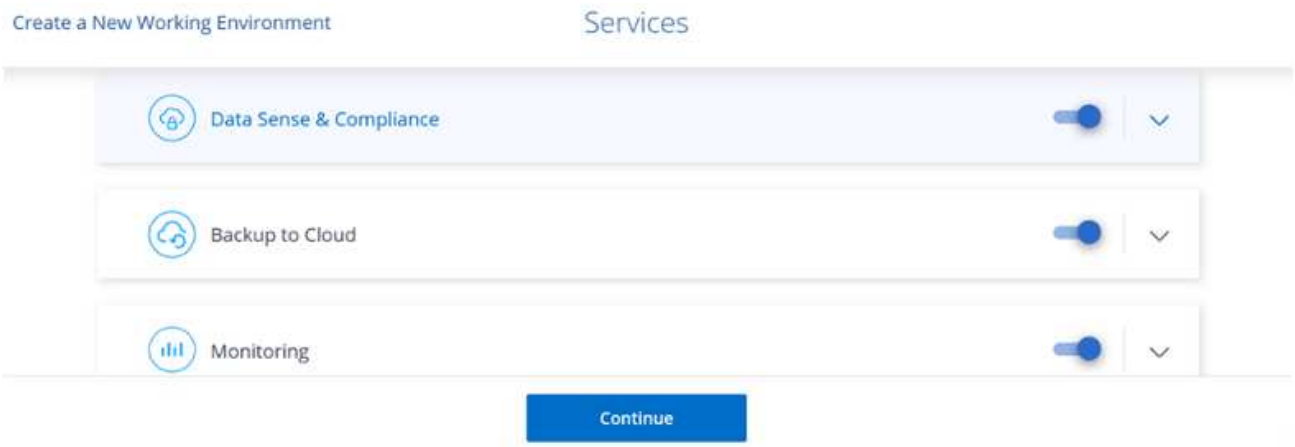
4. Une fois le connecteur créé, mettez à jour les champs Détails et Informations d'identification.



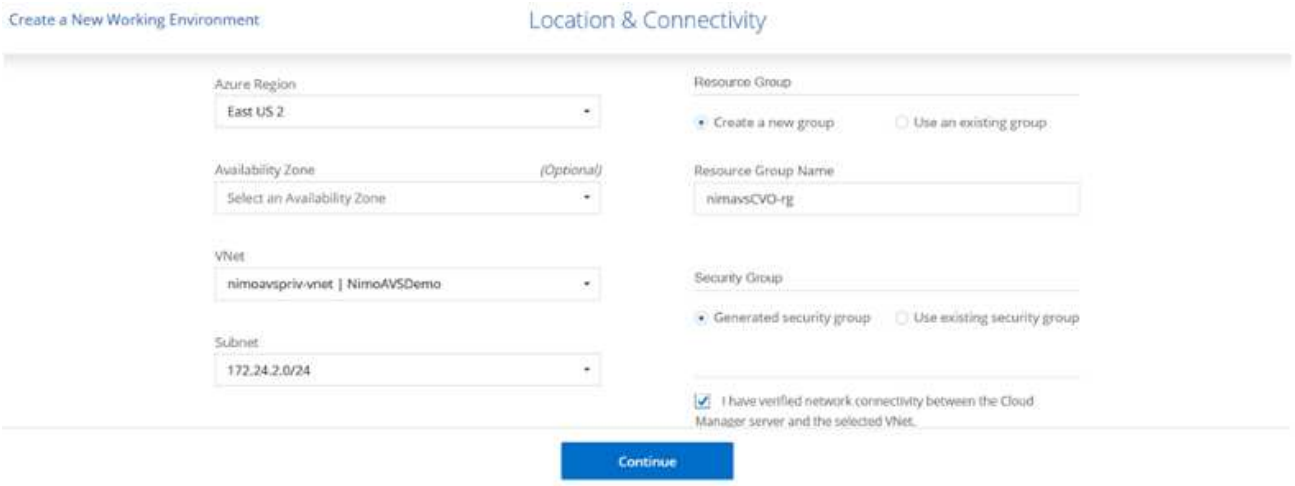
5. Fournissez les détails de l'environnement à créer, y compris le nom de l'environnement et les informations d'identification de l'administrateur. Ajoutez des balises de groupe de ressources pour l'environnement Azure en tant que paramètre facultatif. Une fois que vous avez terminé, cliquez sur Continuer.



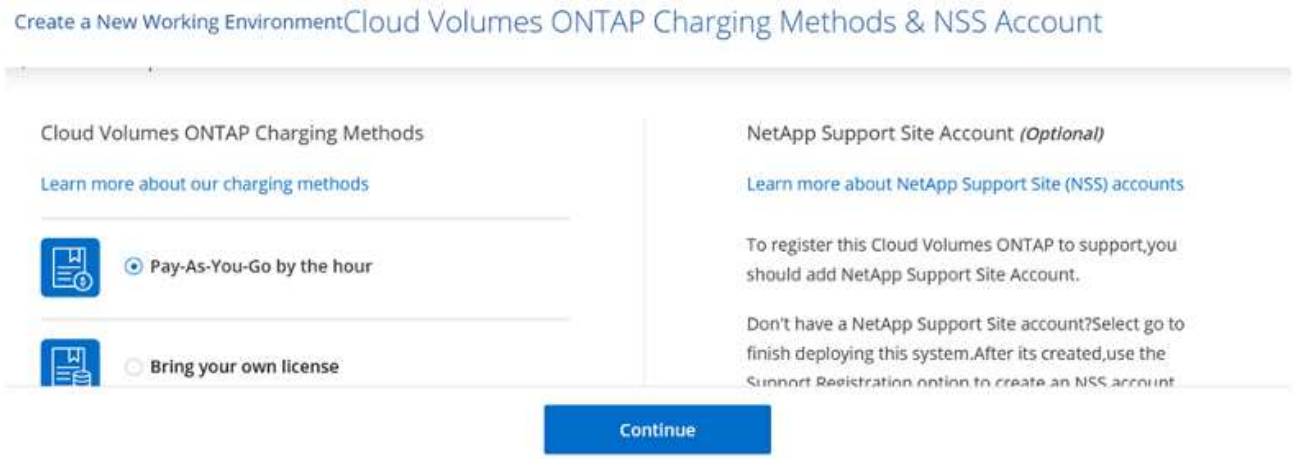
6. Sélectionnez les services complémentaires pour le déploiement de Cloud Volumes ONTAP, notamment NetApp Data Classification, NetApp Backup and Recovery et Data Infrastructure Insights. Sélectionnez les services, puis cliquez sur Continuer.



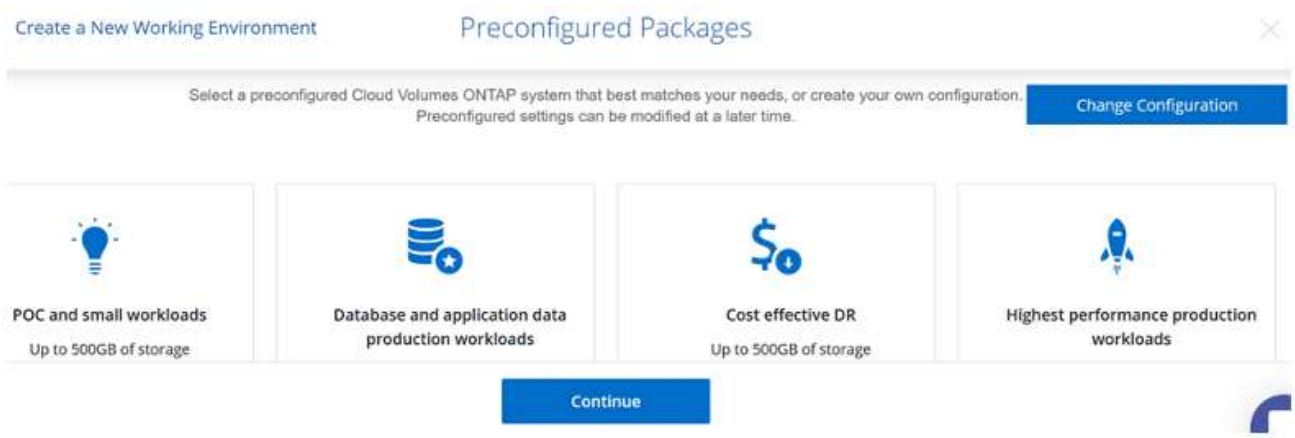
7. Configurez l'emplacement et la connectivité Azure. Sélectionnez la région Azure, le groupe de ressources, le réseau virtuel et le sous-réseau à utiliser.



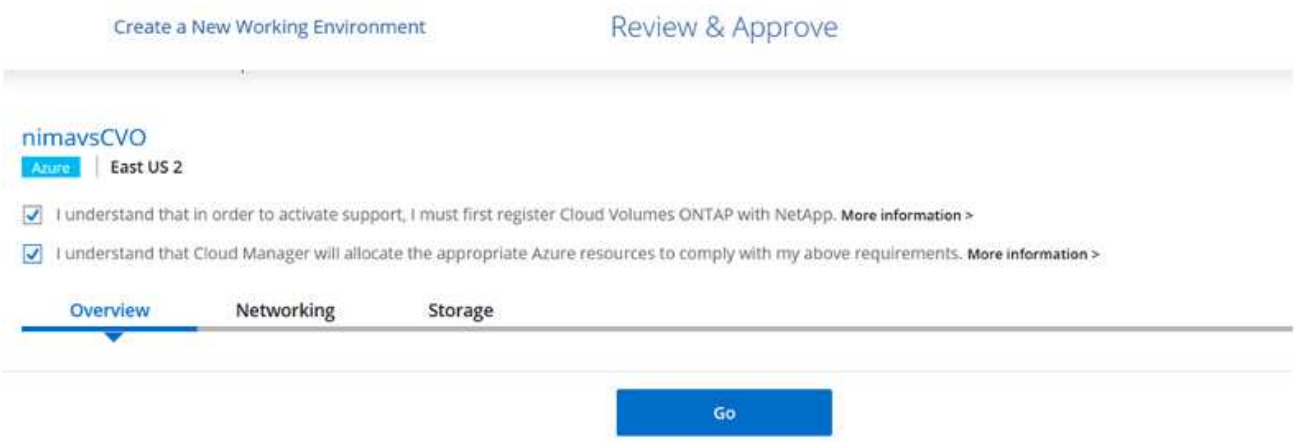
8. Sélectionnez l'option de licence : Pay-As-You-Go ou BYOL pour utiliser la licence existante. Dans cet exemple, l'option Pay-As-You-Go est utilisée.



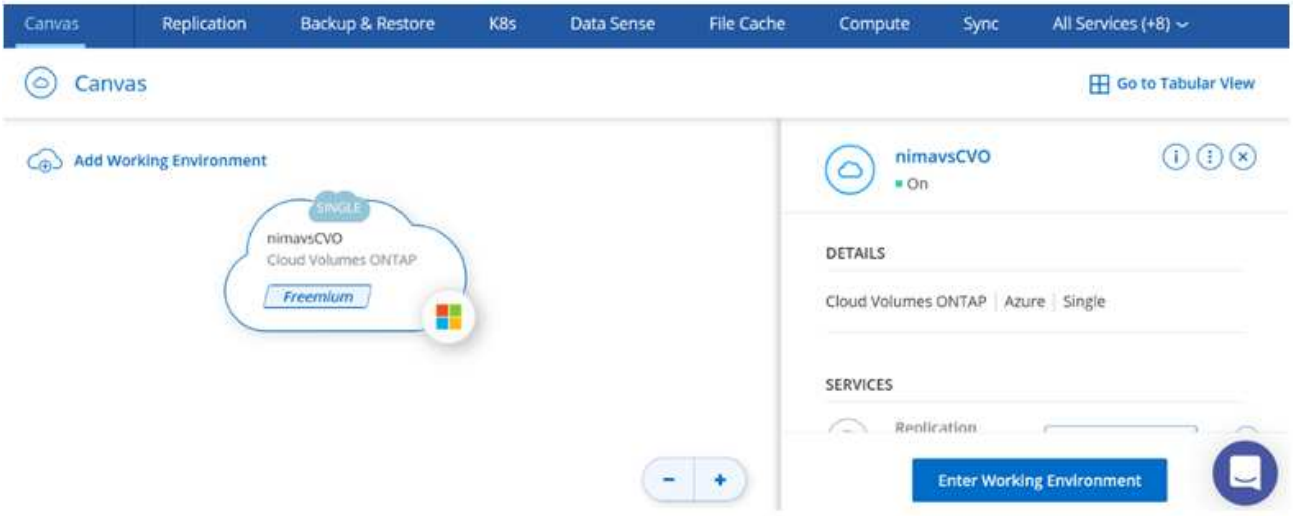
9. Choisissez parmi plusieurs packages préconfigurés disponibles pour les différents types de charges de travail.



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 Accéder.

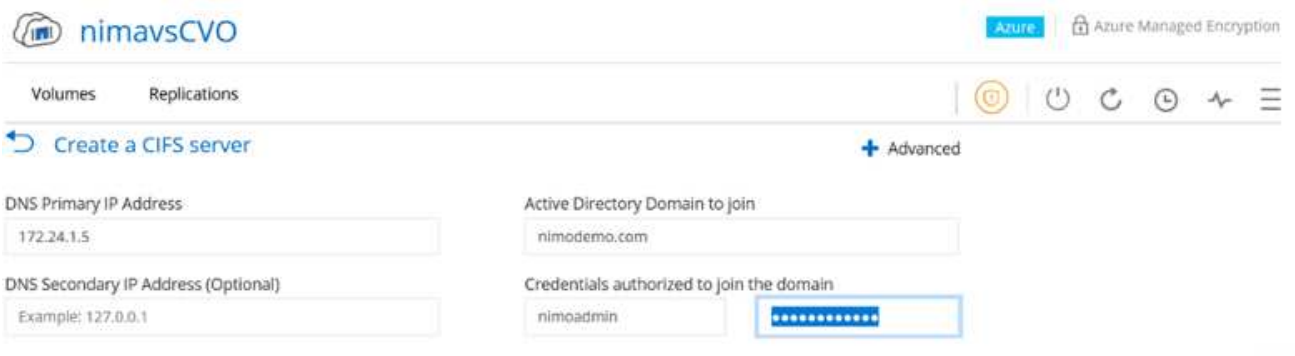


11. Une fois Cloud Volumes ONTAP provisionné, il est répertorié dans les environnements de travail sur la page Canvas.

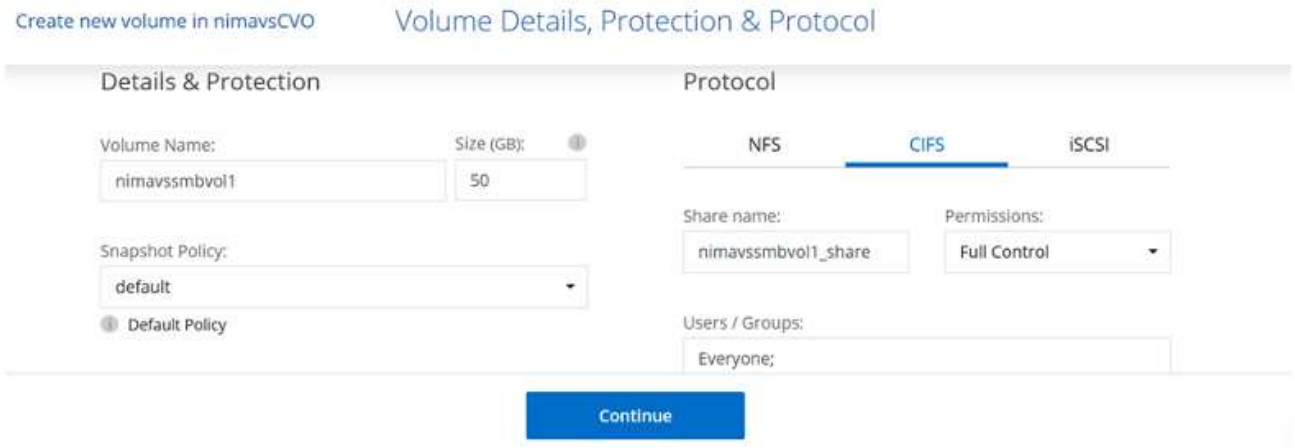


▼ Configurations supplémentaires pour les volumes SMB

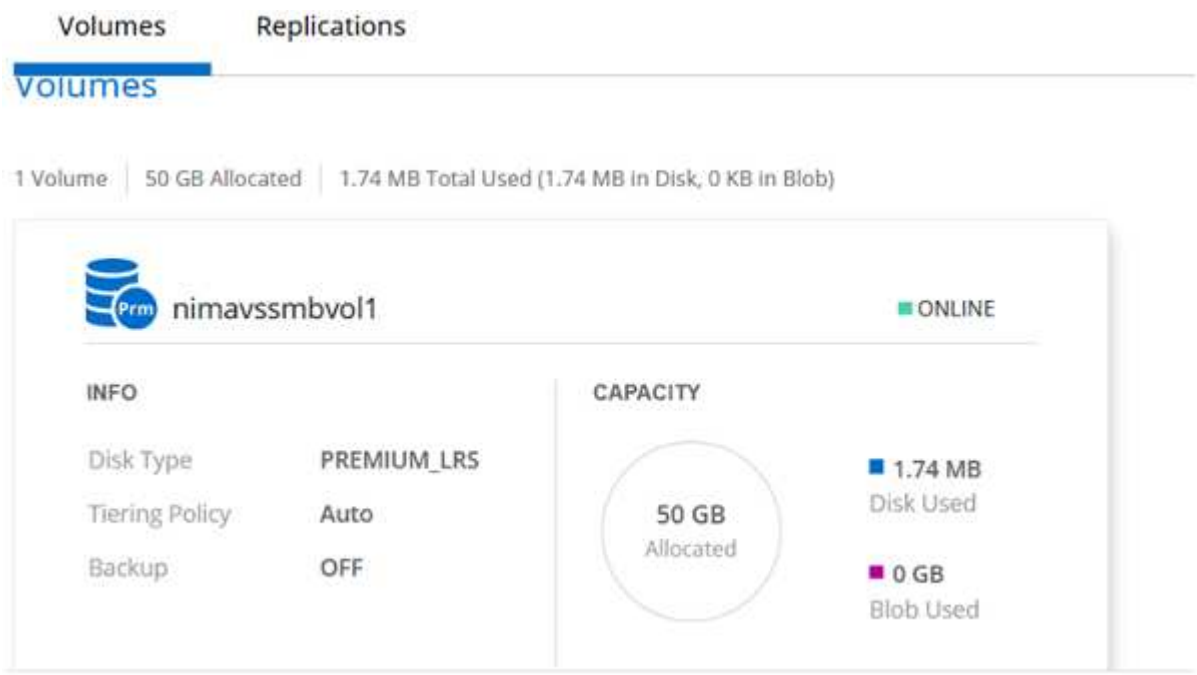
1. Une fois l'environnement de travail prêt, assurez-vous que le serveur CIFS est configuré avec les paramètres de configuration DNS et Active Directory appropriés. Cette étape est requise avant de pouvoir créer le volume SMB.



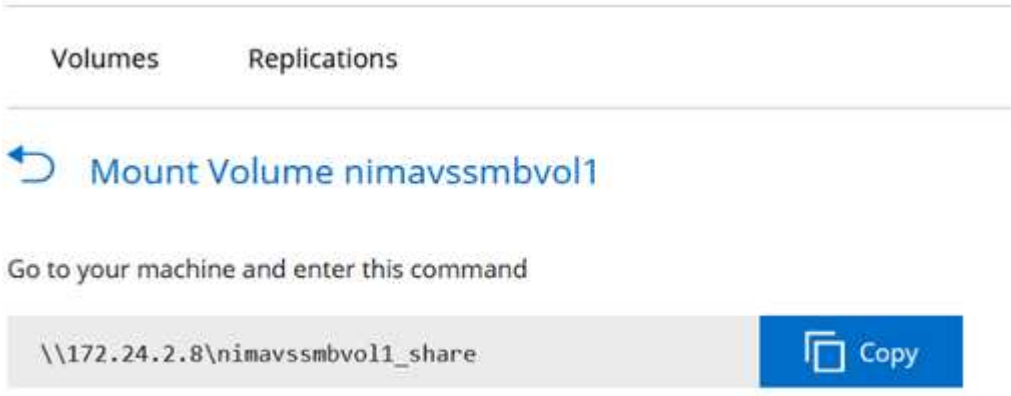
2. La création du volume SMB est un processus simple. Sélectionnez l'instance CVO pour créer le volume et cliquez sur l'option Créer un volume. Choisissez la taille appropriée et le gestionnaire de cloud choisit l'agrégat contenant ou utilise un mécanisme d'allocation avancé pour le placer sur un agrégat spécifique. Pour cette démonstration, SMB est sélectionné comme protocole.

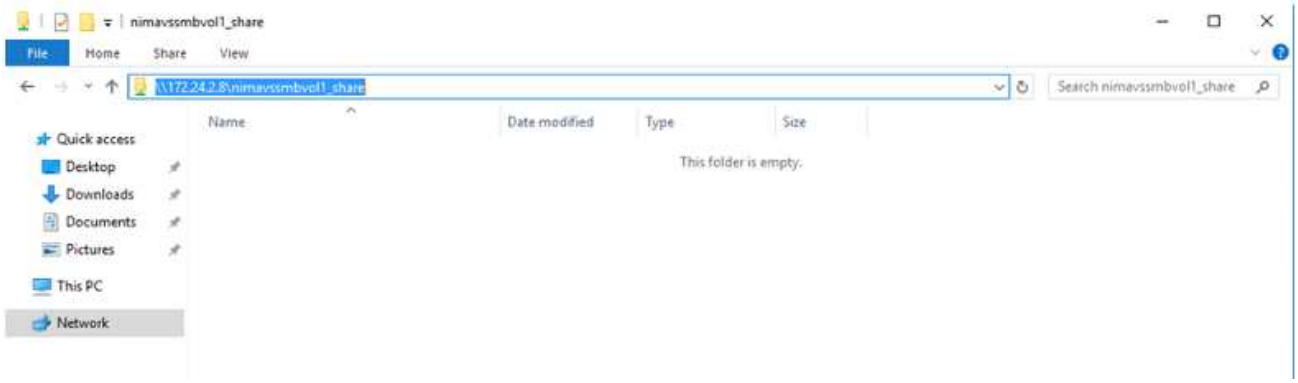


3. Une fois le volume provisionné, il sera disponible dans le volet Volumes. Étant donné qu'un partage CIFS est provisionné, accordez à vos utilisateurs ou groupes l'autorisation d'accéder aux fichiers et dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier. Cette étape n'est pas requise si le volume est répliqué à partir d'un environnement local, car les autorisations de fichiers et de 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.

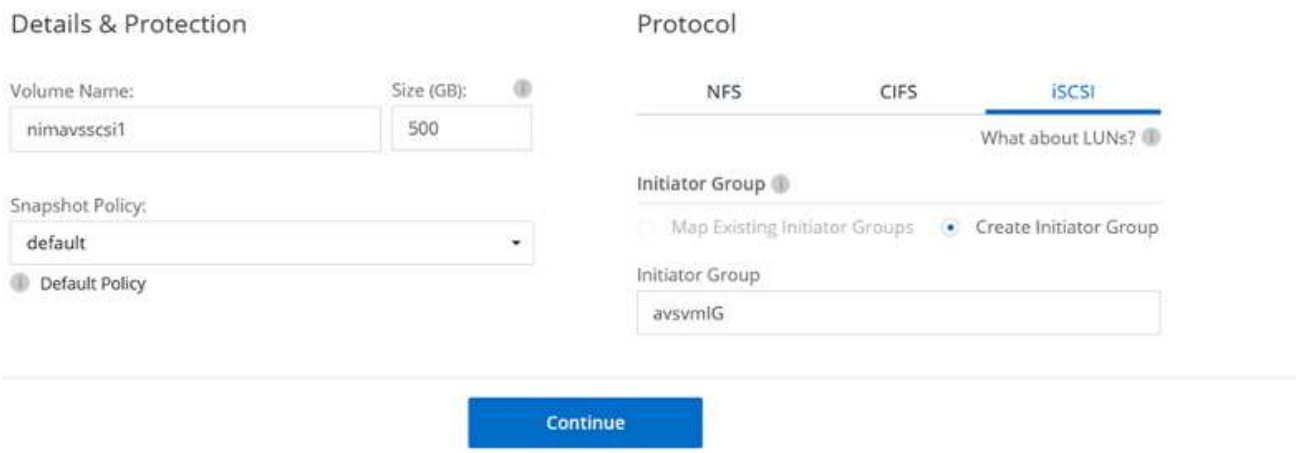




▼ **Connecter le LUN à un hôte**

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

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



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

   Pour réaliser la même chose pour l'hôte résidant sur Azure VMware Solution SDDC :

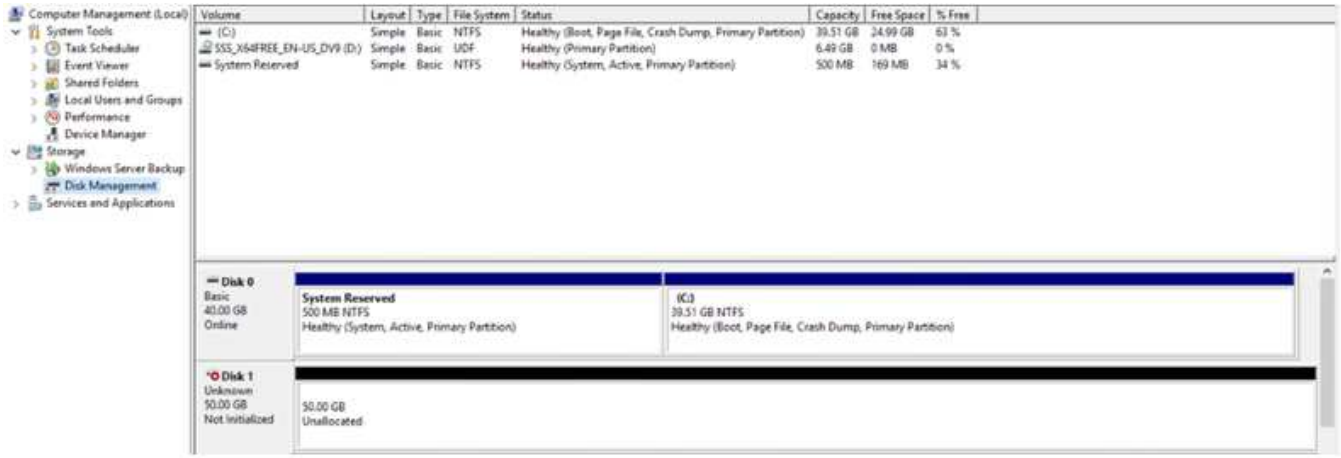
   a. RDP vers la machine virtuelle hébergée sur Azure VMware Solution SDDC.
   b. Ouvrez la boîte de dialogue Propriétés de l'initiateur iSCSI : Gestionnaire de serveur > Tableau de bord > Outils > Initiateur iSCSI.
   c. Dans l'onglet Découverte, cliquez sur Découvrir le portail ou Ajouter un portail, puis entrez l'adresse IP du port cible iSCSI.
   d. Dans l'onglet Cibles, sélectionnez la cible découverte, puis cliquez sur Connexion ou Connecter.
   e. Sélectionnez Activer le multi-chemin, puis sélectionnez Restaurer automatiquement cette connexion au démarrage de l'ordinateur 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 à utiliser.



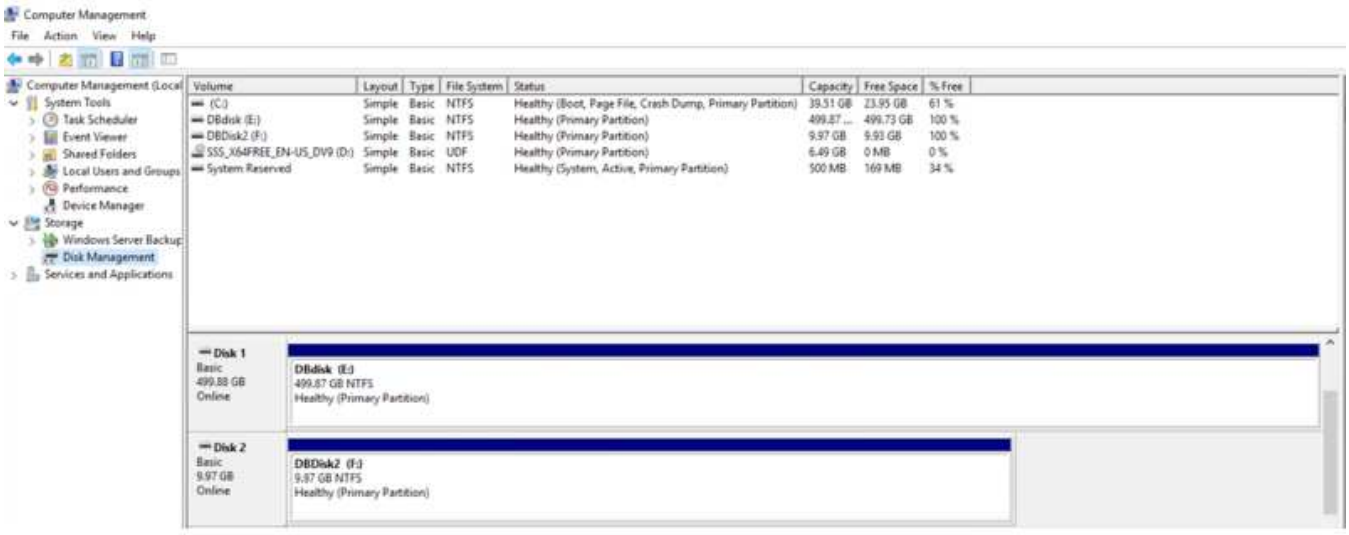
Les LUN sur la machine virtuelle de stockage (SVM) apparaissent comme des disques sur l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclenchez une nouvelle analyse manuelle pour découvrir les disques en procédant comme suit :

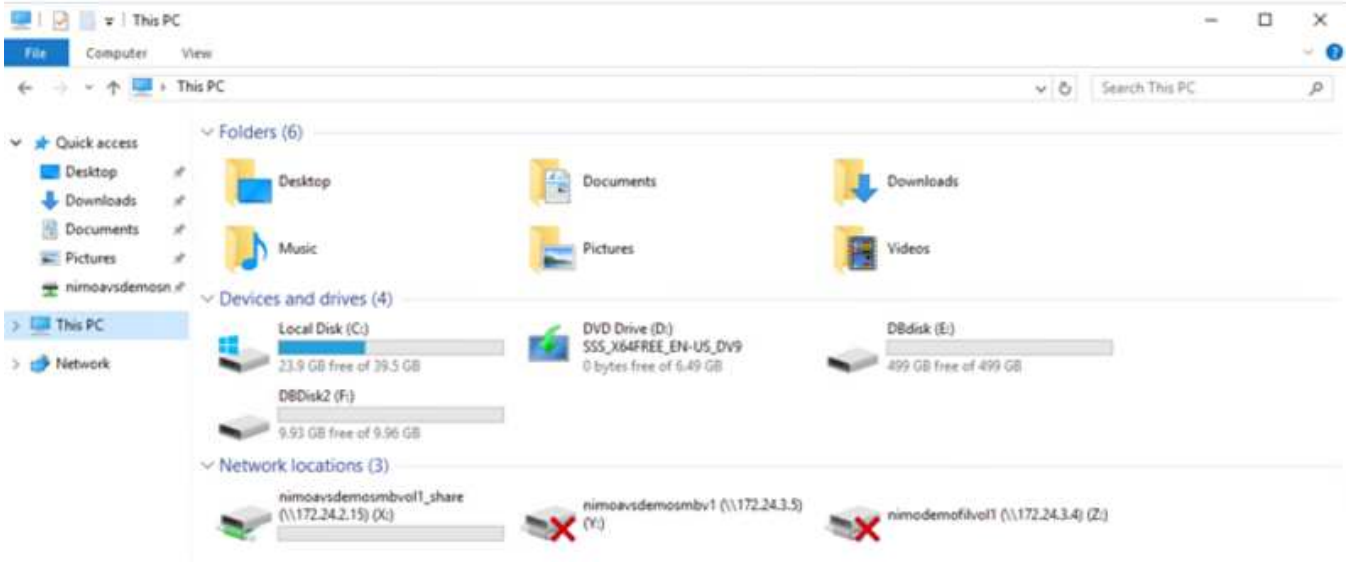
1. Ouvrez l'utilitaire Gestion de l'ordinateur Windows : Démarrer > Outils d'administration > Gestion de l'ordinateur.
2. Développez le nœud Stockage dans l'arborescence de navigation.
3. Cliquez sur Gestion des disques.
4. Cliquez sur Action > Réanalyser les disques.



Lorsqu'un nouveau LUN est accédé pour la première fois par l'hôte Windows, il ne possède aucune partition ni aucun système de fichiers. Initialisez le LUN ; et éventuellement, formatez le LUN avec un système de fichiers en procédant comme suit :

1. Démarrez la gestion des disques Windows.
2. Cliquez avec le bouton droit sur le 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





Google Cloud VMware Engine : options d'utilisation du stockage NetApp

Le stockage NetApp peut être connecté au moteur de virtualisation Google Cloud en tant que stockage invité connecté ou supplémentaire.

Google Cloud NetApp Volumes (NetApp Volumes) comme banque de données NFS supplémentaire

Les clients qui ont besoin d'une capacité de stockage supplémentaire sur leur environnement Google Cloud VMware Engine (GCVE) peuvent utiliser Google Cloud NetApp Volumes pour le monter en tant que banque de données NFS supplémentaire. Le stockage des données sur Google Cloud NetApp Volumes permet aux clients de les répliquer entre les régions pour les protéger des catastrophes.

Pour plus d'informations, veuillez visiter"Google Cloud NetApp Volumes (NetApp Volumes) comme banque de données NFS supplémentaire"

NetApp CVO comme stockage connecté aux invités

Cloud Volumes ONTAP, ou CVO, est la solution de gestion de données cloud leader du secteur, basée sur le logiciel de stockage ONTAP de NetApp, disponible nativement sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version définie par logiciel d' ONTAP qui consomme du stockage natif dans le cloud, vous permettant d'avoir le même logiciel de stockage dans le cloud et sur site, réduisant ainsi le besoin de recycler votre personnel informatique dans de toutes nouvelles méthodes de gestion de vos données.

CVO offre aux clients la possibilité de déplacer de manière transparente les données de la périphérie vers le centre de données, vers le cloud et vice-versa, en rassemblant votre cloud hybride, le tout géré avec une console de gestion à volet unique, NetApp Cloud Manager.

De par sa conception, CVO offre des performances extrêmes et des capacités avancées de gestion des données pour satisfaire même vos applications les plus exigeantes dans le cloud.

Pour plus d'informations, veuillez visiter"NetApp CVO comme stockage connecté aux invités"

Google Cloud NetApp Volumes (NetApp Volumes) comme stockage connecté aux invités

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

Les clouds privés Google Cloud NetApp Volumes et Google Cloud VMware Engine doivent se trouver dans la même région.

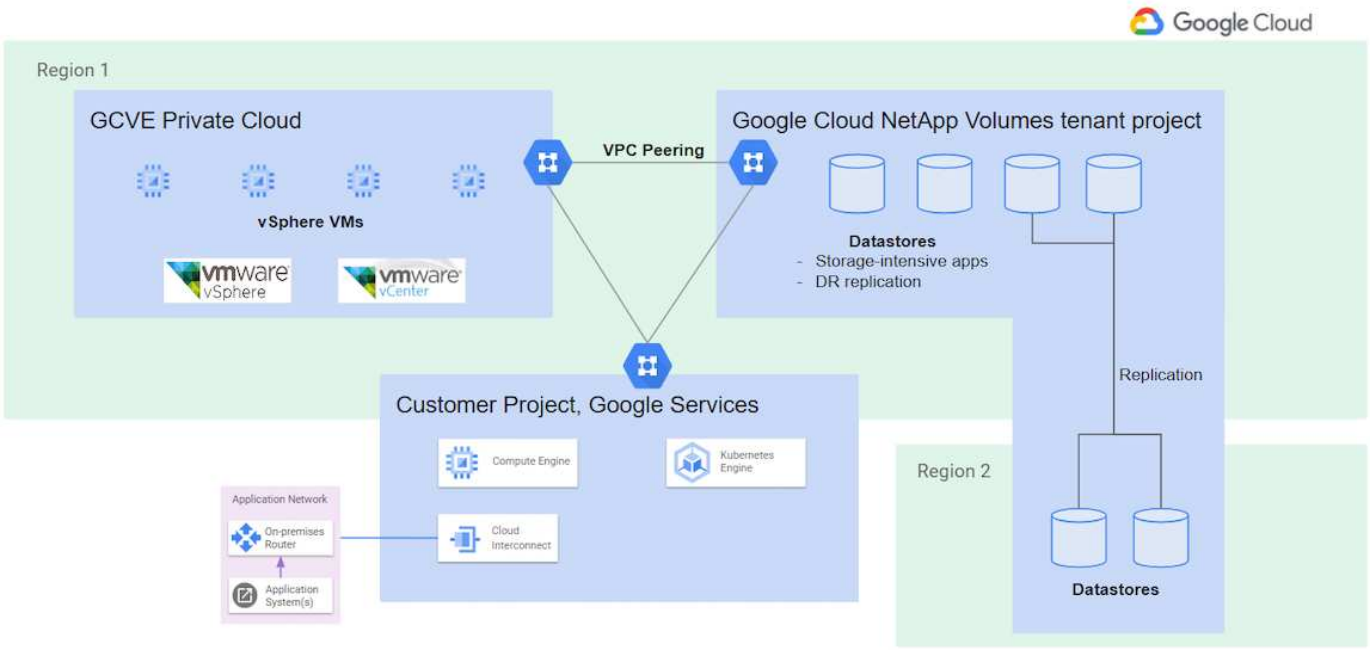
Pour plus d'informations, veuillez visiter"Google Cloud NetApp Volumes (NetApp Volumes) comme stockage connecté aux invités"

Banque de données NFS supplémentaire Google Cloud VMware Engine avec Google Cloud NetApp Volumes

Les clients peuvent étendre la capacité de stockage sur Google Cloud VMware Engine à l'aide d'une banque de données supplémentaire NFS avec Google Cloud NetApp Volumes.

Aperçu

Les clients qui ont besoin d'une capacité de stockage supplémentaire sur leur environnement Google Cloud VMware Engine (GCVE) peuvent utiliser Netapp Cloud Volume Service pour monter une banque de données NFS supplémentaire. Le stockage des données sur Google Cloud NetApp Volumes permet aux clients de les répliquer entre les régions pour les protéger des catastrophes.



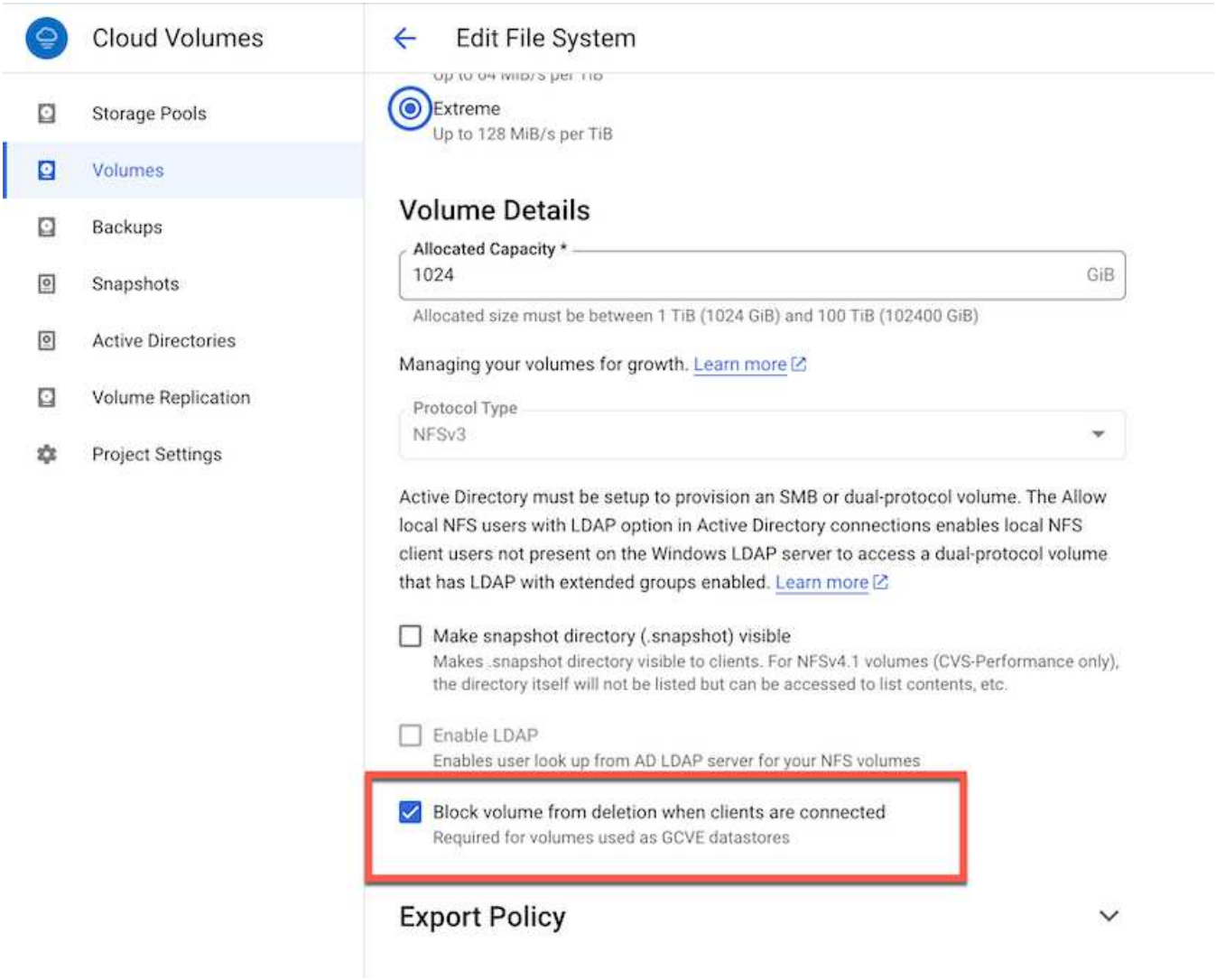
Étapes de déploiement pour monter une banque de données NFS à partir de Google Cloud NetApp Volumes (NetApp Volumes) sur GCVE

▼ **Provisionner les volumes NetApp - Volume de performance**

Le volume Google Cloud NetApp Volumes peut être provisionné par "Utilisation de Google Cloud Console" "Utilisation de l'interface de ligne de commande ou de l'API Google Cloud"

▼ **Marquer ce volume NetApp Volumes 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 indiqué dans la capture d'écran ci-dessous.



Pour plus d'informations, veuillez consulter "Création d'un volume NFS" documentation.

▼ **Assurez-vous que la connexion privée sur GCVE existe pour le VPC locataire NetApp Volumes.**

Pour monter le magasin de données NFS, une connexion privée doit exister entre GCVE et le projet NetApp Volumes. Pour plus d'informations, veuillez vous référer"Comment configurer l'accès aux services privés"

▼ **Monter le magasin de données NFS**

Pour obtenir des instructions sur la façon de monter une banque de données NFS sur GCVE, veuillez vous référer"Comment créer une banque de données NFS avec NetApp Volumes"

Les hôtes vSphere étant gérés par Google, vous n'avez pas accès à l'installation de NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB). Si vous avez besoin d'assistance pour les volumes virtuels (vVol), veuillez nous le faire savoir. Si vous souhaitez utiliser des cadres Jumbo, veuillez vous référer à"Tailles MTU maximales prises en charge sur GCP"

Économies avec Google Cloud NetApp Volumes

Pour en savoir plus sur les économies potentielles que vous pouvez réaliser avec Google Cloud NetApp Volumes pour vos besoins de stockage sur GCVE, veuillez consulter "Calculateur de retour sur investissement NetApp"

Liens de référence

- "Blog Google - Comment utiliser les volumes NetApp comme banques de données pour Google Cloud VMware Engine"
- "Blog NetApp : une meilleure façon de migrer vos applications riches en stockage vers Google Cloud"

Options de stockage NetApp pour GCP

GCP prend en charge le stockage NetApp connecté en tant qu'invité avec Cloud Volumes ONTAP (CVO) ou Google Cloud NetApp Volumes (NetApp Volumes).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, ou CVO, est la solution de gestion de données cloud leader du secteur, basée sur le logiciel de stockage ONTAP de NetApp, disponible nativement sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Il s'agit d'une version définie par logiciel d' ONTAP qui consomme du stockage natif dans le cloud, vous permettant d'avoir le même logiciel de stockage dans le cloud et sur site, réduisant ainsi le besoin de recycler votre personnel informatique dans de toutes nouvelles méthodes de gestion de vos données.

CVO offre aux clients la possibilité de déplacer de manière transparente les données de la périphérie vers le centre de données, vers le cloud et vice-versa, en rassemblant votre cloud hybride, le tout géré avec une console de gestion à volet unique, NetApp Cloud Manager.

De par sa conception, CVO offre des performances extrêmes et des capacités avancées de gestion des données pour satisfaire même vos applications les plus exigeantes dans le cloud.

Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités

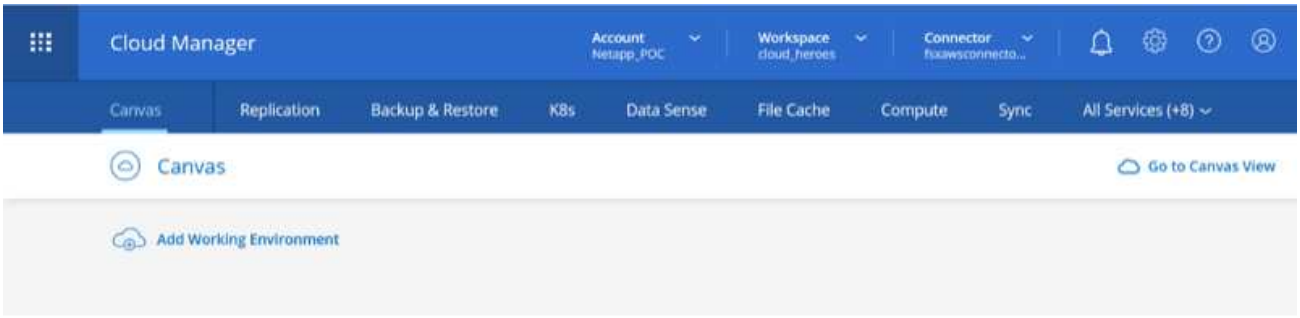
▼ **Déployer Cloud Volumes ONTAP dans Google Cloud (à faire soi-même)**

Les partages et LUN Cloud Volumes ONTAP 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 et sur le client Windows et les LUN sont 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.

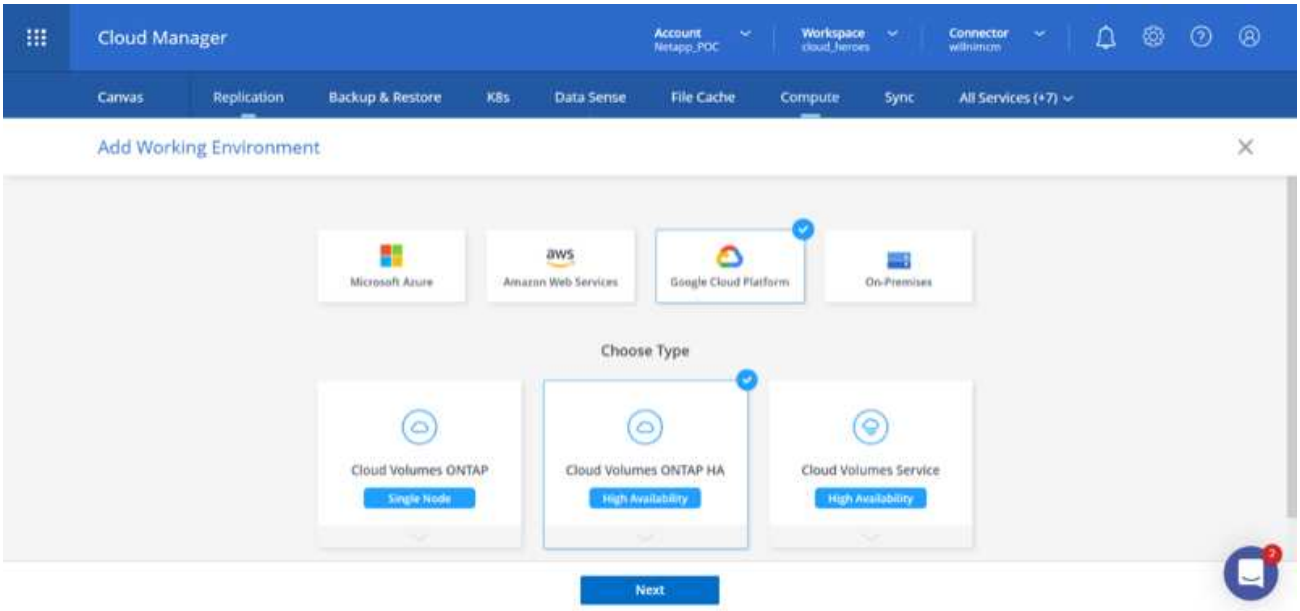
Pour répliquer des volumes d'un environnement local vers le cloud à des fins de reprise après sinistre ou de migration, établissez une connectivité réseau à Google Cloud, soit à l'aide d'un VPN site à site, soit de Cloud Interconnect. La réplication des données sur site vers Cloud Volumes ONTAP n'entre pas dans le cadre de ce document. Pour répliquer des données entre les systèmes locaux et Cloud Volumes ONTAP , consultez"Configuration de la réplication des données entre les systèmes" .

> Utilisez "Dimensionneur Cloud Volumes ONTAP" pour dimensionner précisément les instances Cloud Volumes ONTAP. Surveillez également les performances sur site afin de les utiliser comme données d'entrée dans l'outil de dimensionnement Cloud Volumes ONTAP.

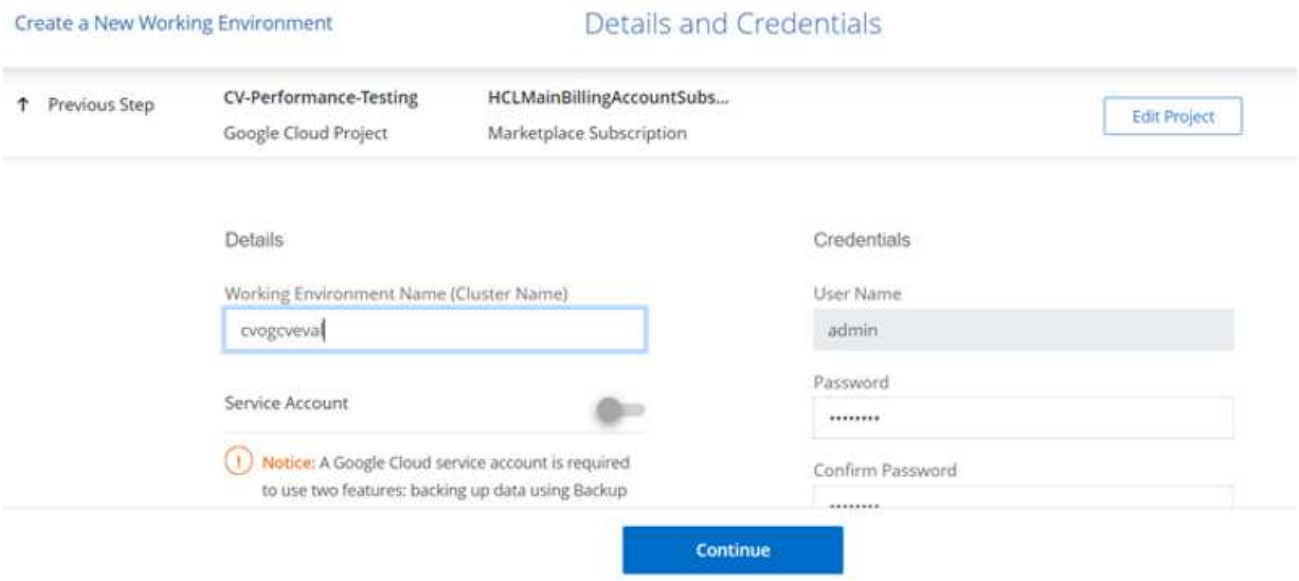
1. Connectez-vous à NetApp Cloud Central : l'écran Fabric View s'affiche. Localisez l'onglet Cloud Volumes ONTAP et sélectionnez Accéder au Gestionnaire de Cloud. Une fois connecté, l'écran Canvas s'affiche.



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



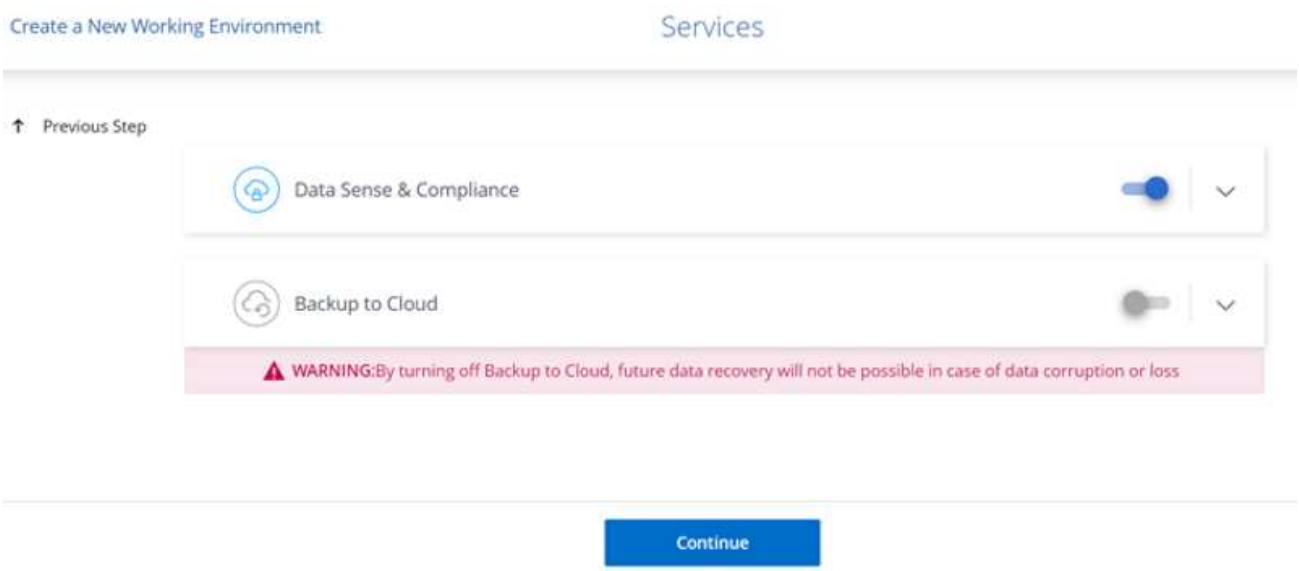
3. Fournissez les détails de l'environnement à créer, y compris le nom de l'environnement et les informations d'identification de l'administrateur. Une fois que vous avez terminé, cliquez sur Continuer.



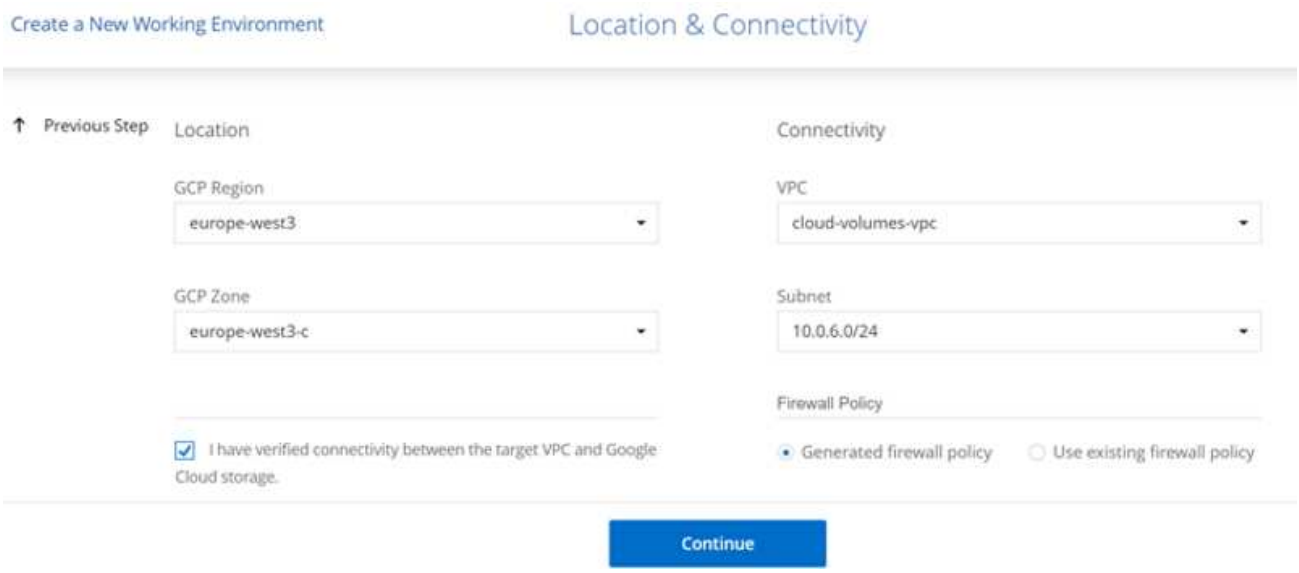
4. Sélectionnez ou désélectionnez les services complémentaires pour le déploiement de Cloud Volumes

ONTAP , notamment Data Sense & Compliance ou Backup to Cloud. Ensuite, cliquez sur Continuer.

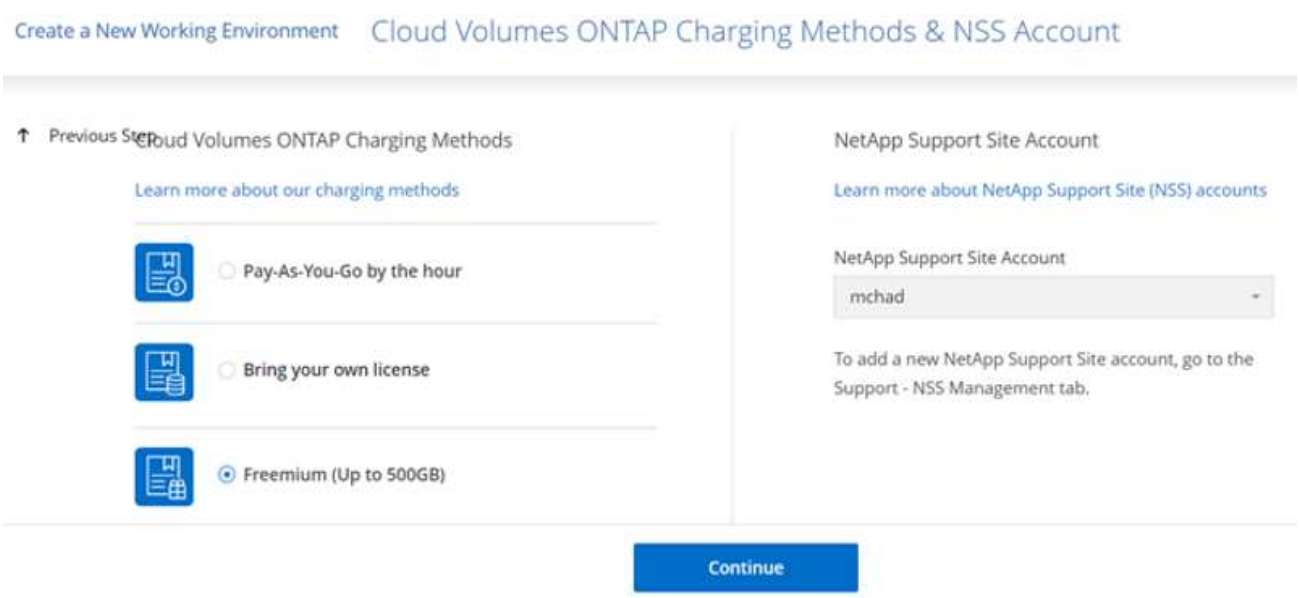
CONSEIL : un message contextuel de vérification s'affichera lors de la désactivation des services complémentaires. Des services complémentaires peuvent être ajoutés/supprimés après le déploiement de CVO, pensez à les désélectionner s'ils ne sont pas nécessaires dès le début pour éviter les coûts.



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

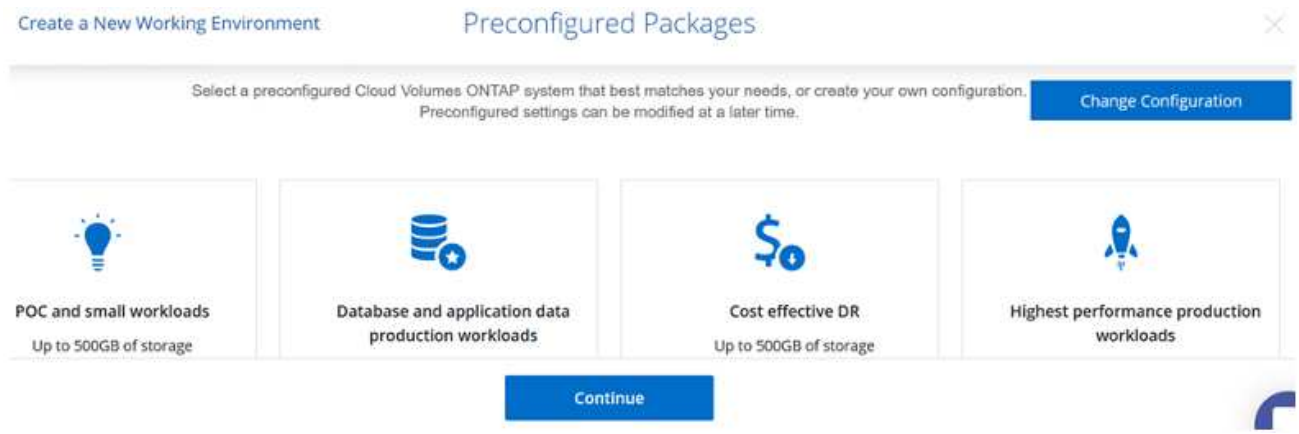


6. Sélectionnez l'option de licence : Pay-As-You-Go ou BYOL pour utiliser la licence existante. Dans cet exemple, l'option Freemium est utilisée. Ensuite, cliquez sur Continuer.

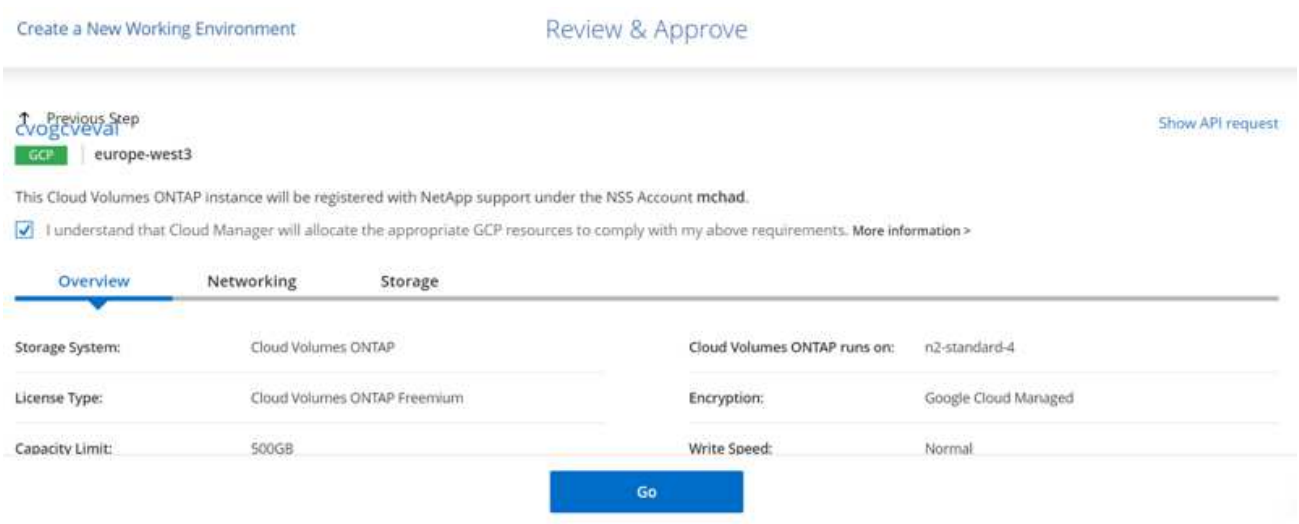


7. Choisissez parmi plusieurs packages préconfigurés disponibles en fonction du type de charge de travail qui sera déployée sur les machines virtuelles exécutées sur le cloud VMware sur AWS SDDC.

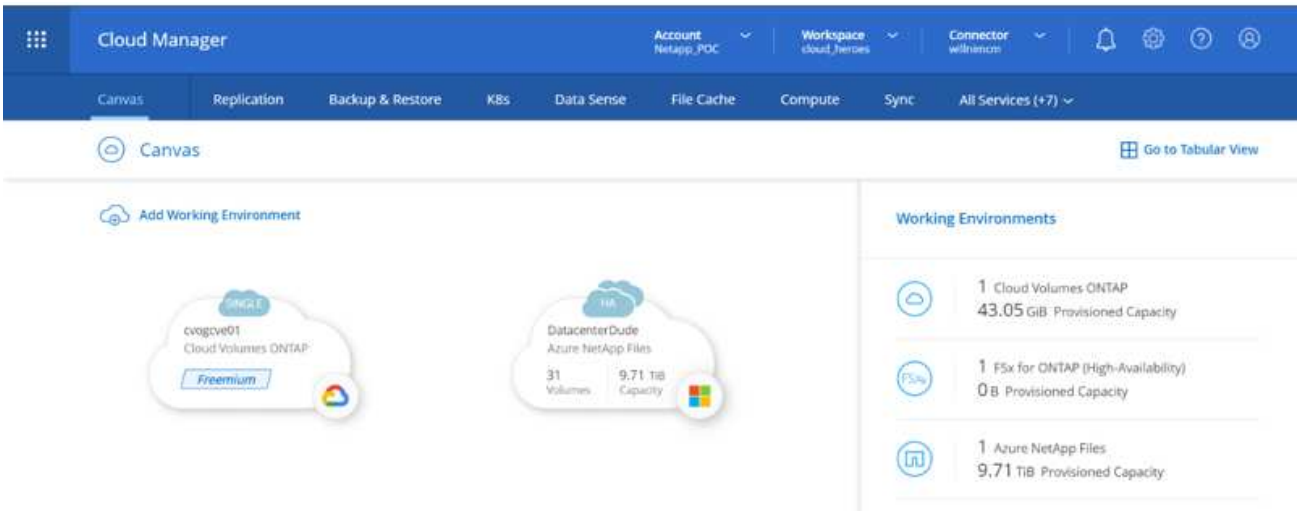
   CONSEIL : passez votre souris sur les tuiles pour plus de détails ou personnalisez les composants CVO et la version ONTAP en cliquant sur Modifier la configuration.



8. Sur la page Réviser et approuver, vérifiez et confirmez les sélections. Pour créer l'instance Cloud Volumes ONTAP , cliquez sur Accéder.



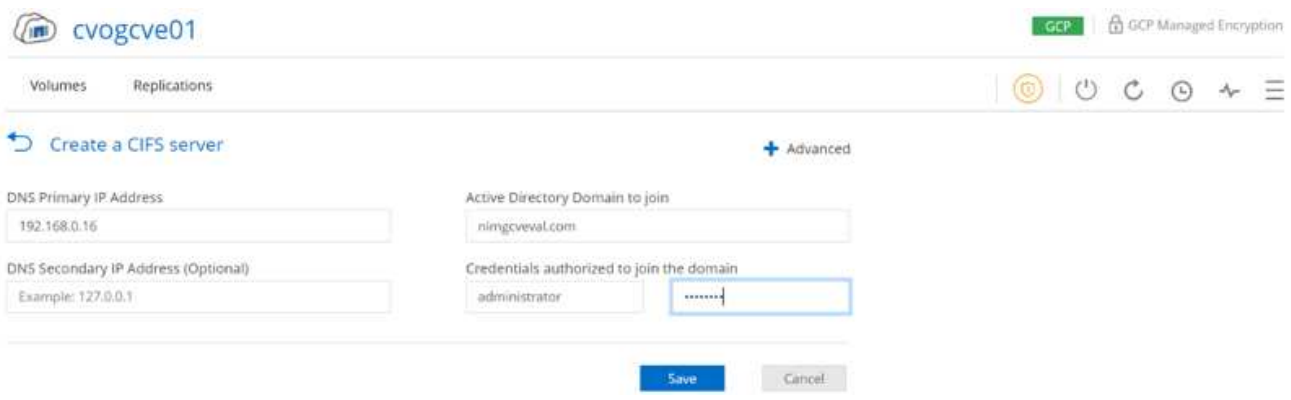
9. Une fois Cloud Volumes ONTAP provisionné, il est répertorié dans les environnements de travail sur la page Canvas.



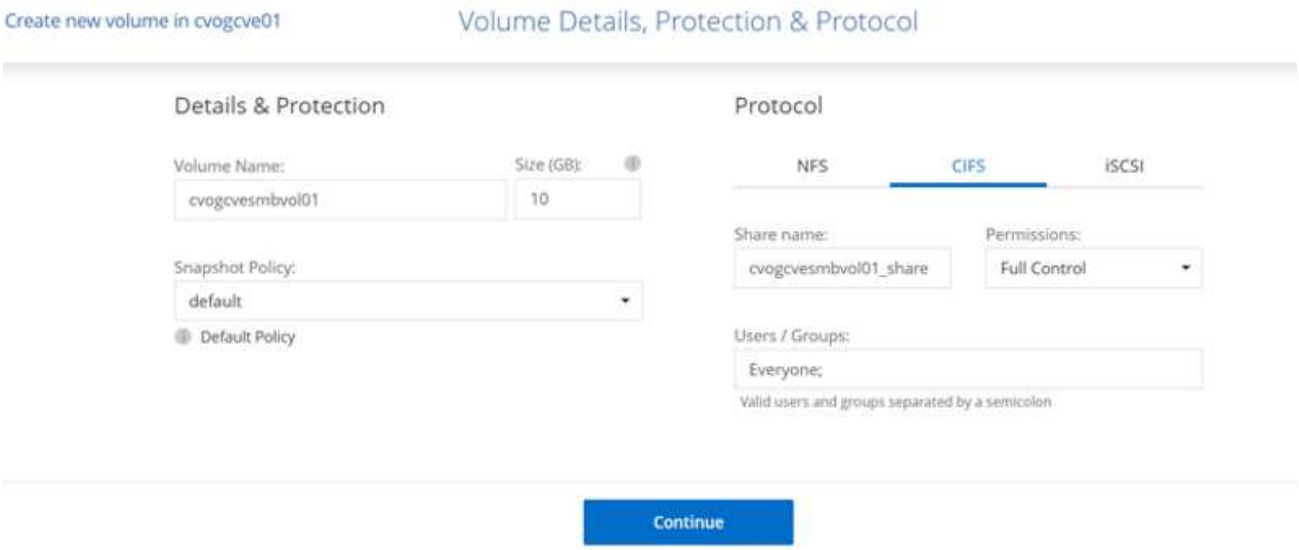
▼ **Configurations supplémentaires pour les volumes SMB**

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 et cliquez sur l'option Créer un volume. Choisissez la taille appropriée et le gestionnaire de cloud choisit l'agrégat contenant ou utilise un mécanisme d'allocation avancé pour le placer sur un agrégat spécifique. Pour cette démonstration, CIFS/SMB est sélectionné comme protocole.



3. Une fois le volume provisionné, il sera disponible dans le volet Volumes. Étant donné qu'un partage CIFS est provisionné, accordez 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 local, car les autorisations de fichiers et de dossiers sont toutes conservées dans le cadre de la réplication SnapMirror .

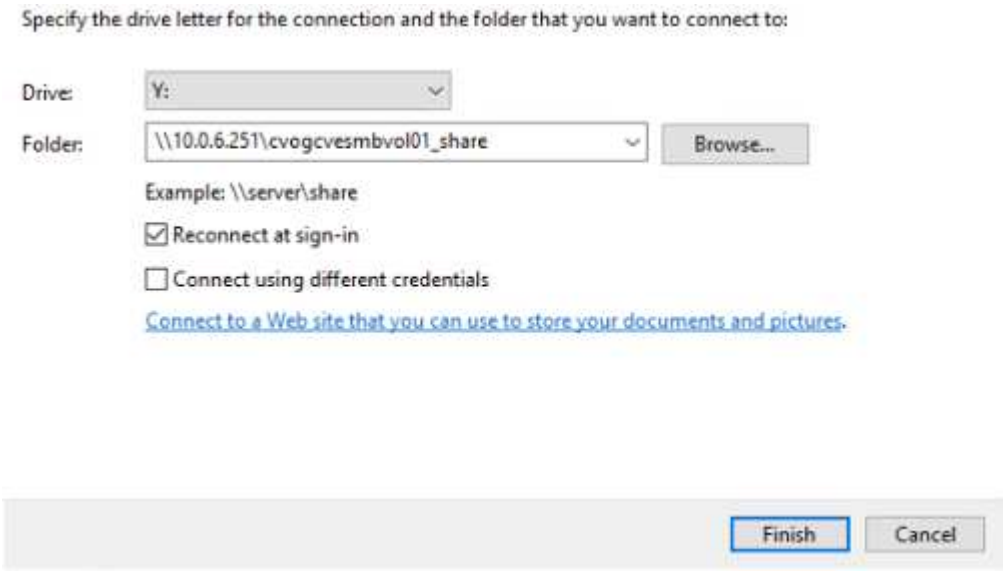
   ASTUCE : Cliquez sur le menu volume (º) pour afficher ses options.



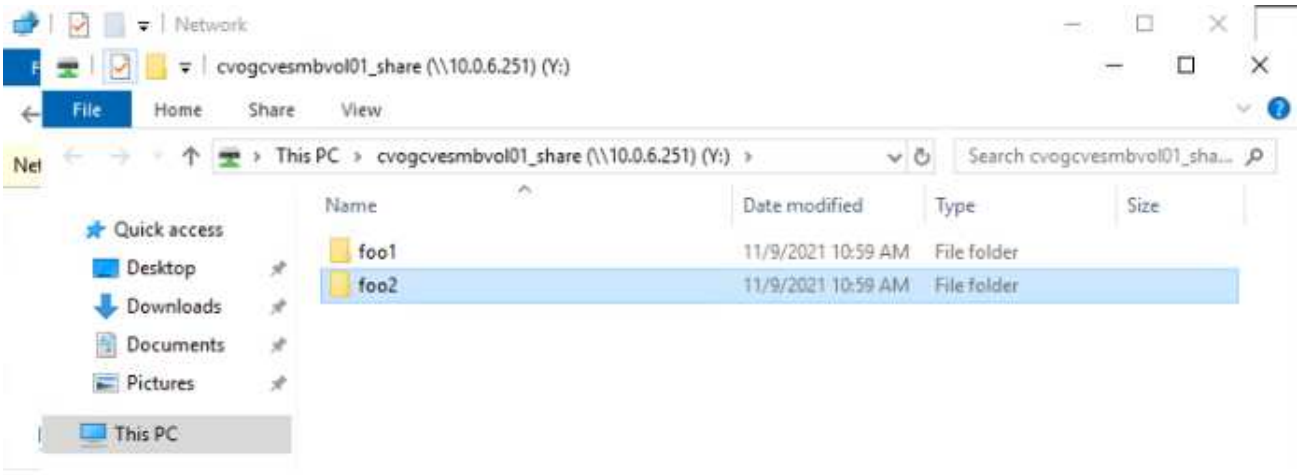
4. Une fois le volume créé, utilisez la commande mount pour afficher les instructions de connexion du volume, puis connectez-vous au partage à partir des machines virtuelles sur Google Cloud VMware Engine.



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.



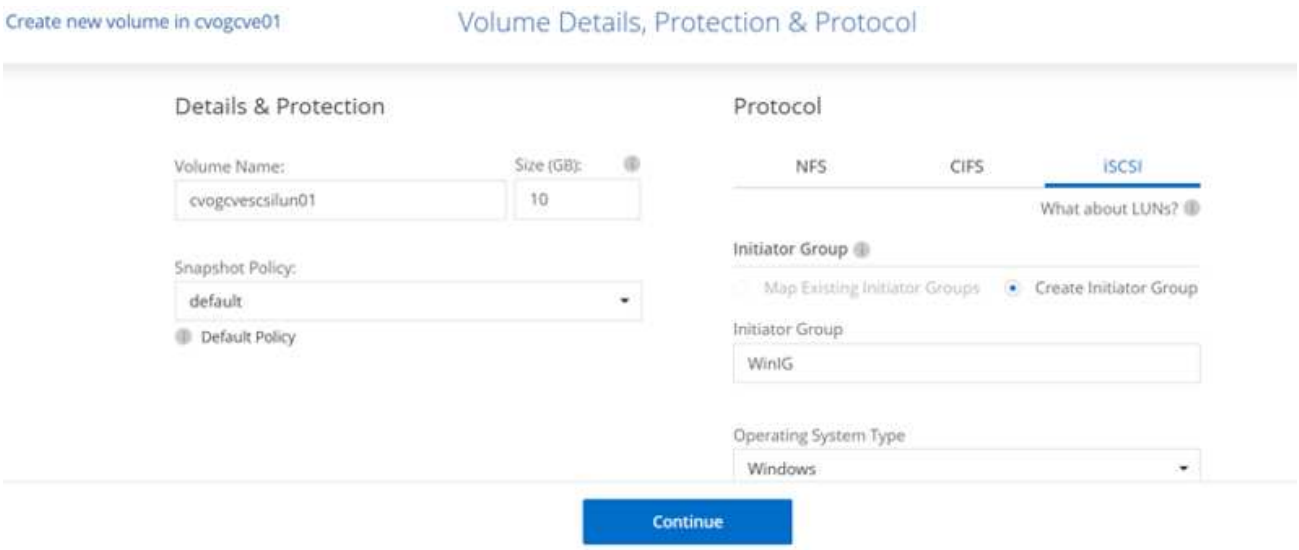
Une fois mappé, il est facilement accessible et les autorisations NTFS peuvent être définies en conséquence.

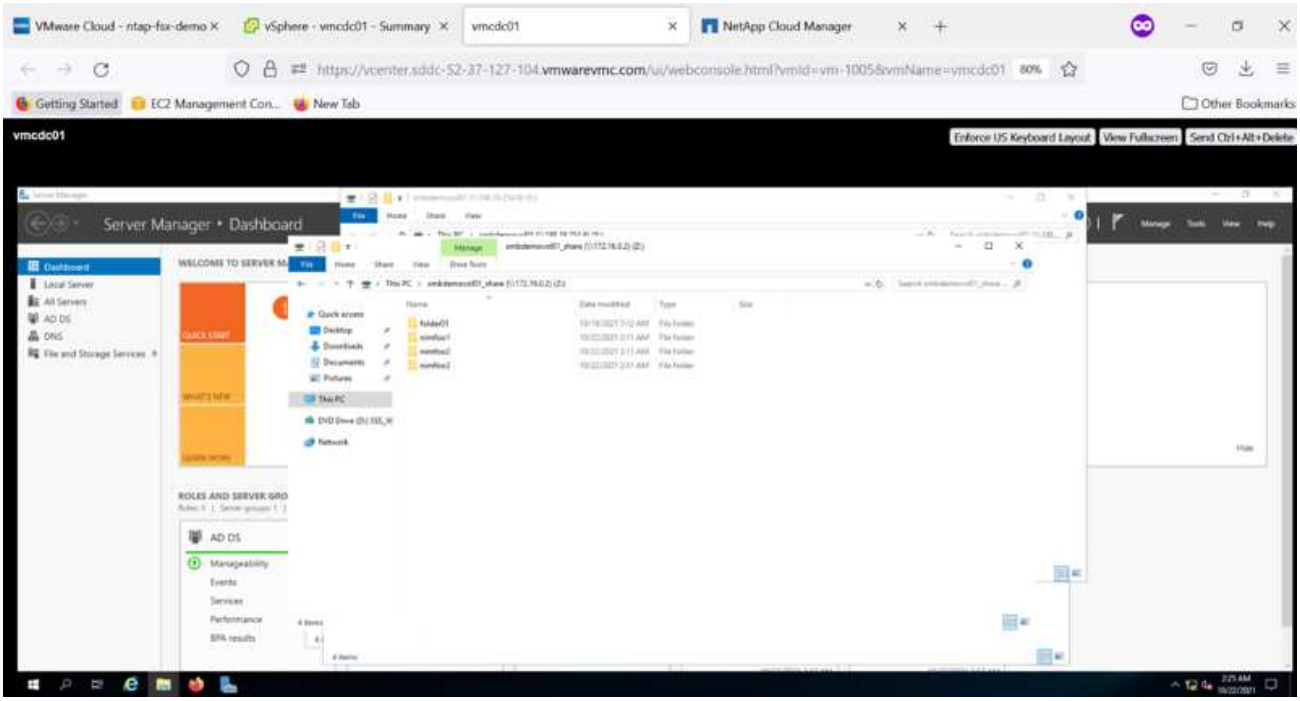


▼ Connecter le LUN sur Cloud Volumes ONTAP à un hôte

Pour connecter les volumes cloud ONTAP LUN à un hôte, procédez comme suit :

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





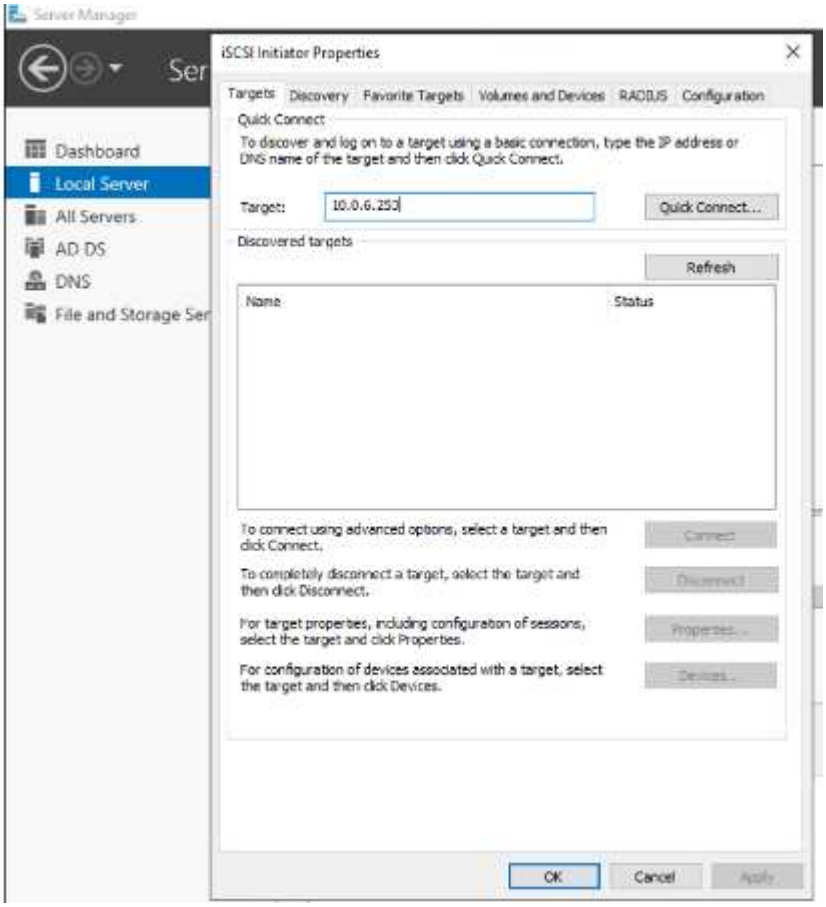
3. Une fois le volume provisionné, sélectionnez le menu Volume (º), puis cliquez sur Cibler iQN. Pour copier le nom qualifié iSCSI (iQN), cliquez sur Copier. Configurez une connexion iSCSI de l'hôte au LUN.

Pour réaliser la même chose pour l'hôte résidant sur Google Cloud VMware Engine :

1. RDP vers la VM 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.

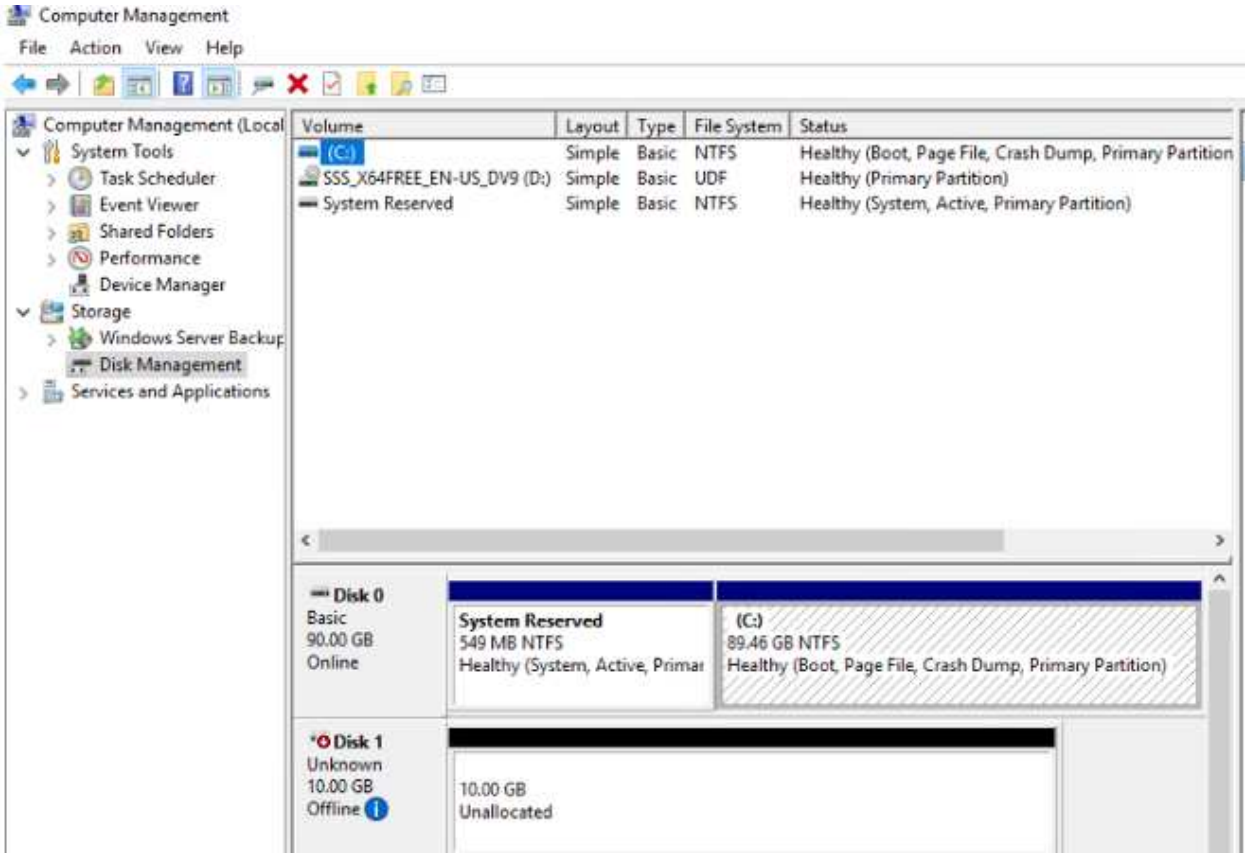
3. Dans l'onglet Découverte, cliquez sur Découvrir le portail ou Ajouter un portail, puis entrez l'adresse IP du port cible iSCSI.
4. Dans l'onglet Cibles, sélectionnez la cible découverte, puis cliquez sur Connexion ou Connecter.
5. Sélectionnez Activer le multi-chemin, puis sélectionnez Restaurer automatiquement 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 à utiliser.



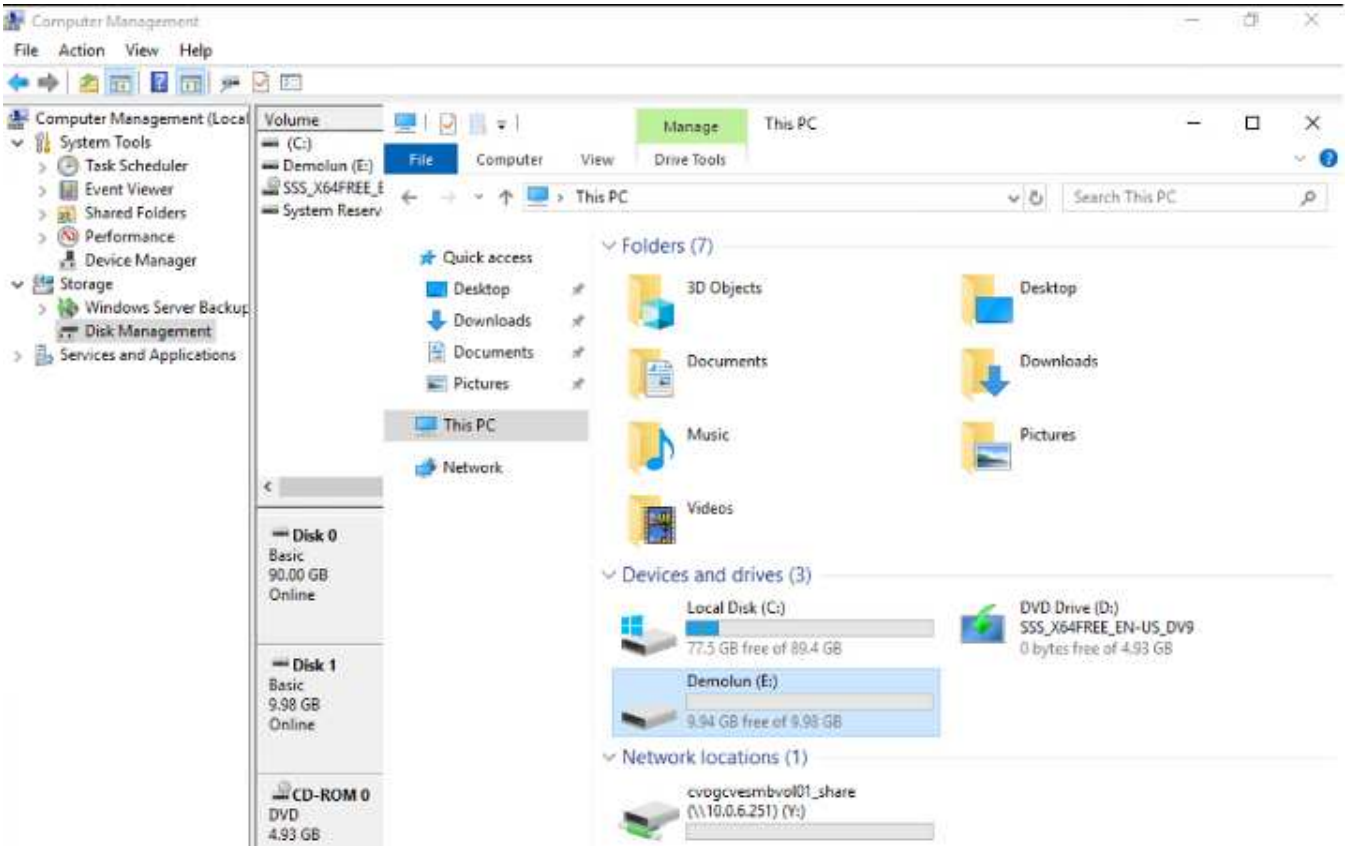
Les LUN sur la machine virtuelle de stockage (SVM) apparaissent comme des disques sur l'hôte Windows. Les nouveaux disques ajoutés ne sont pas automatiquement découverts par l'hôte. Déclenchez une nouvelle analyse manuelle pour découvrir les disques en procédant comme suit :

a. Ouvrez l'utilitaire 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 > Réanalyser les disques.



Lorsqu'un nouveau LUN est accédé pour la première fois par l'hôte Windows, il ne possède aucune partition ni aucun système de fichiers. Initialisez le LUN ; et éventuellement, formatez le LUN avec un système de fichiers en procédant comme suit :

a. Démarrez la gestion des disques Windows.
b. Cliquez avec le bouton droit sur le 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 provisionnés, reportez-vous aux instructions détaillées sur la configuration iSCSI avec Ubuntu comme exemple ici. Pour vérifier, exécutez lsblk cmd depuis le shell.

```
nlyaz@nlmubu01:~$ 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
```

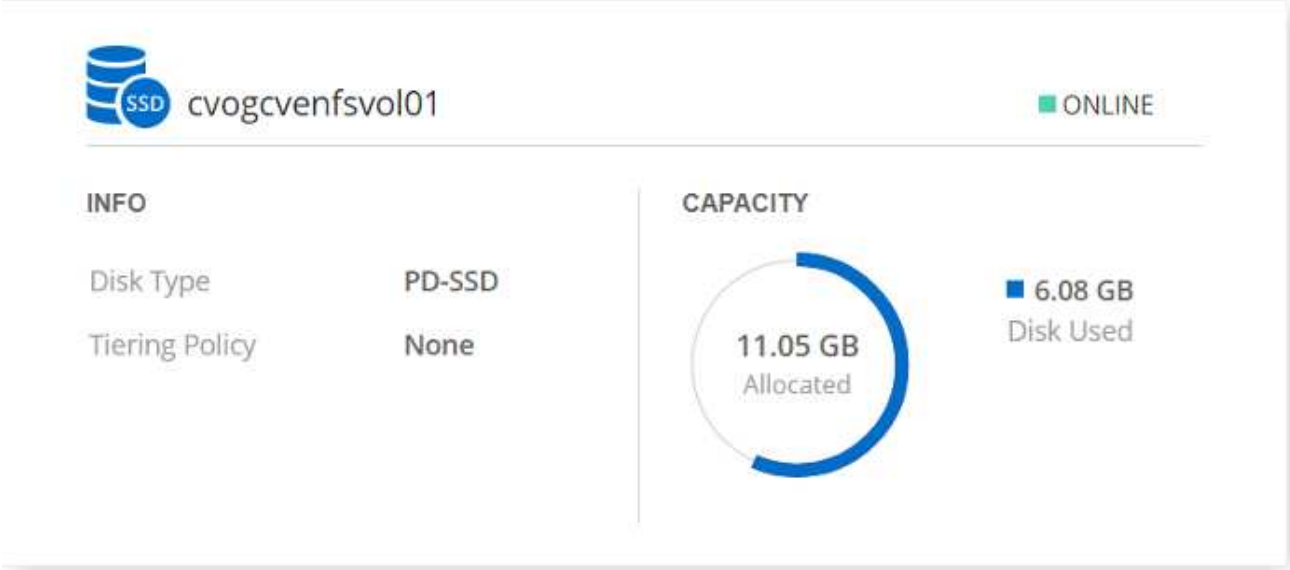
```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           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
```

▼ **Monter le volume NFS Cloud Volumes ONTAP sur un client Linux**

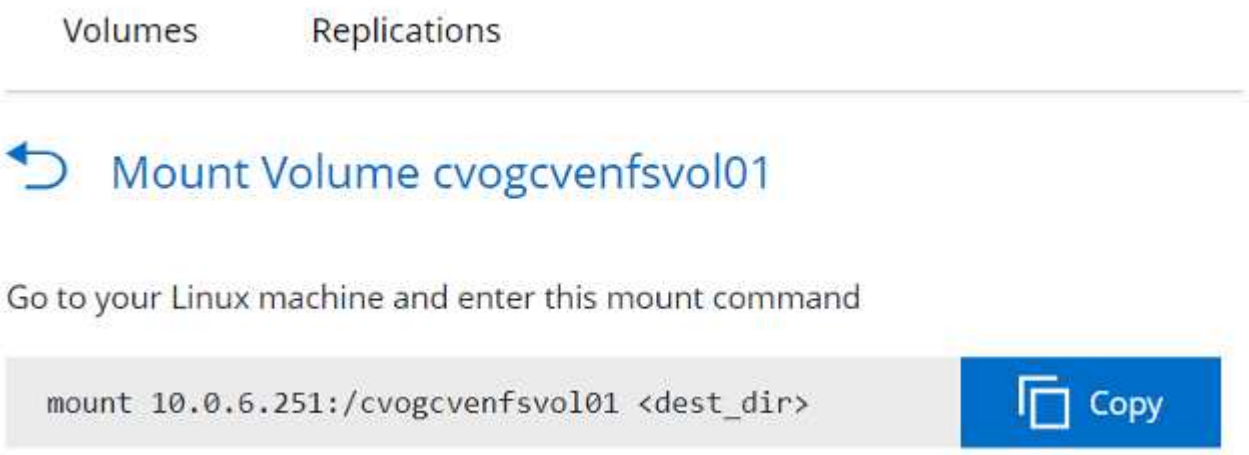
Pour monter le système de fichiers Cloud Volumes ONTAP (DIY) à partir de machines virtuelles dans Google Cloud VMware Engine, suivez les étapes ci-dessous :

Provisionnez le 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 votre souris sur le volume, sélectionnez l'icône de menu (º), puis cliquez sur Monter la commande.



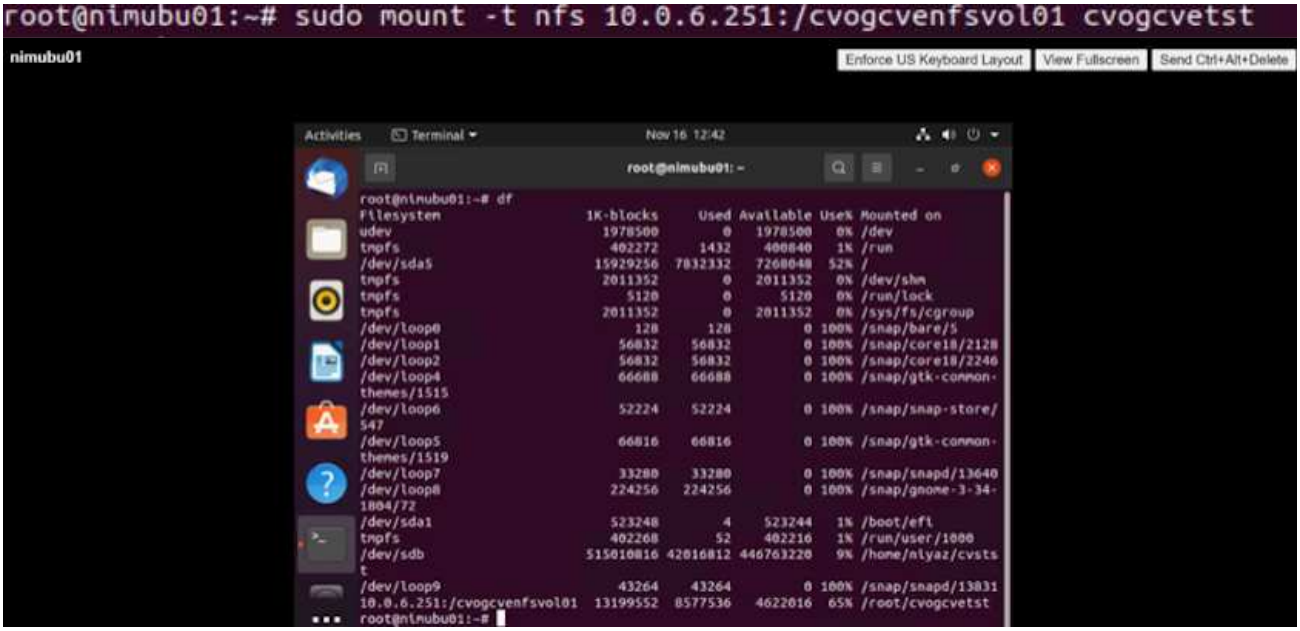
4. Cliquez sur Copier.
5. Connectez-vous à l'instance Linux désignée.
6. Ouvrez un terminal sur l'instance à l'aide d'un shell sécurisé (SSH) et connectez-vous avec les informations d'identification appropriées.
7. Créez un répertoire pour le point de montage du volume avec la commande suivante.

```
$ 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
```



Google Cloud NetApp Volumes (NetApp Volumes)

Google Cloud NetApp Volumes (NetApp Volumes) est un portefeuille complet de services de données permettant de fournir des solutions cloud avancées. NetApp Volumes prend en charge plusieurs protocoles d'accès aux fichiers pour les principaux fournisseurs de cloud (prise en charge NFS et SMB).

D'autres avantages et fonctionnalités incluent : la protection et la restauration des données avec Snapshot ; des fonctionnalités spéciales pour répliquer, synchroniser et migrer les destinations de données sur site ou dans le cloud ; et des performances élevées et constantes au niveau d'un système de stockage flash dédié.

Google Cloud NetApp Volumes (NetApp Volumes) en tant que stockage connecté invité

▼ Configurer les volumes NetApp avec VMware Engine

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

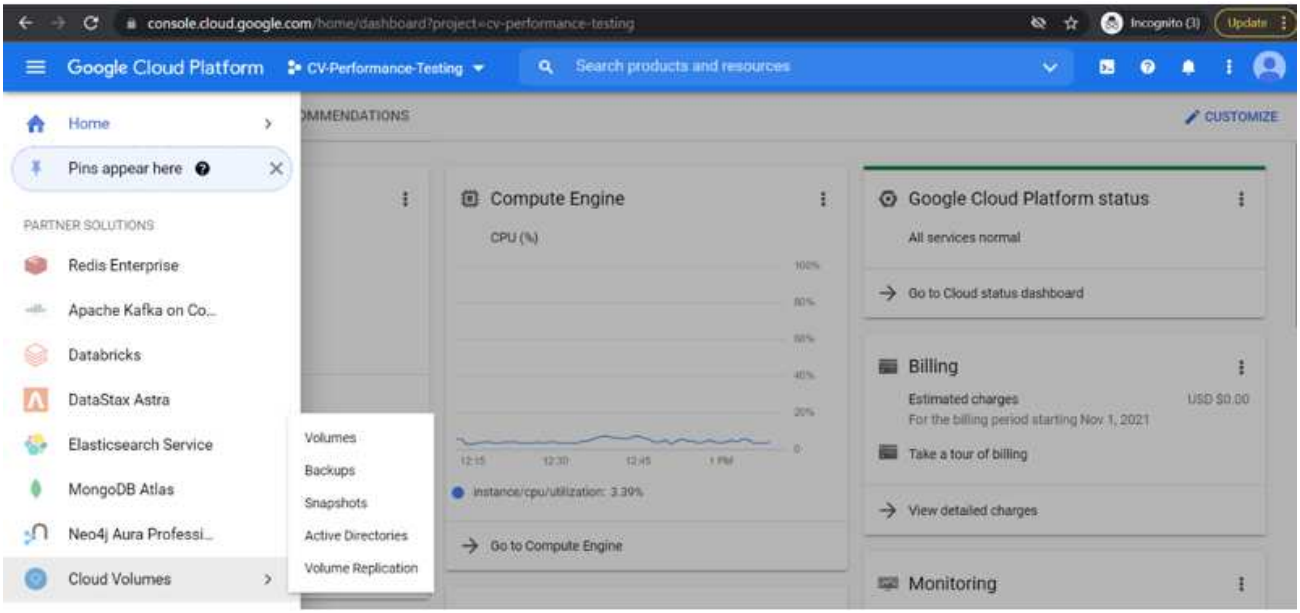
Les clouds privés Google Cloud NetApp Volumes et Google Cloud VMware Engine doivent se trouver dans la même région.

Pour acheter, activer et configurer Google Cloud NetApp Volumes pour Google Cloud à partir de Google Cloud Marketplace, suivez ces instructions détaillées."guide" .

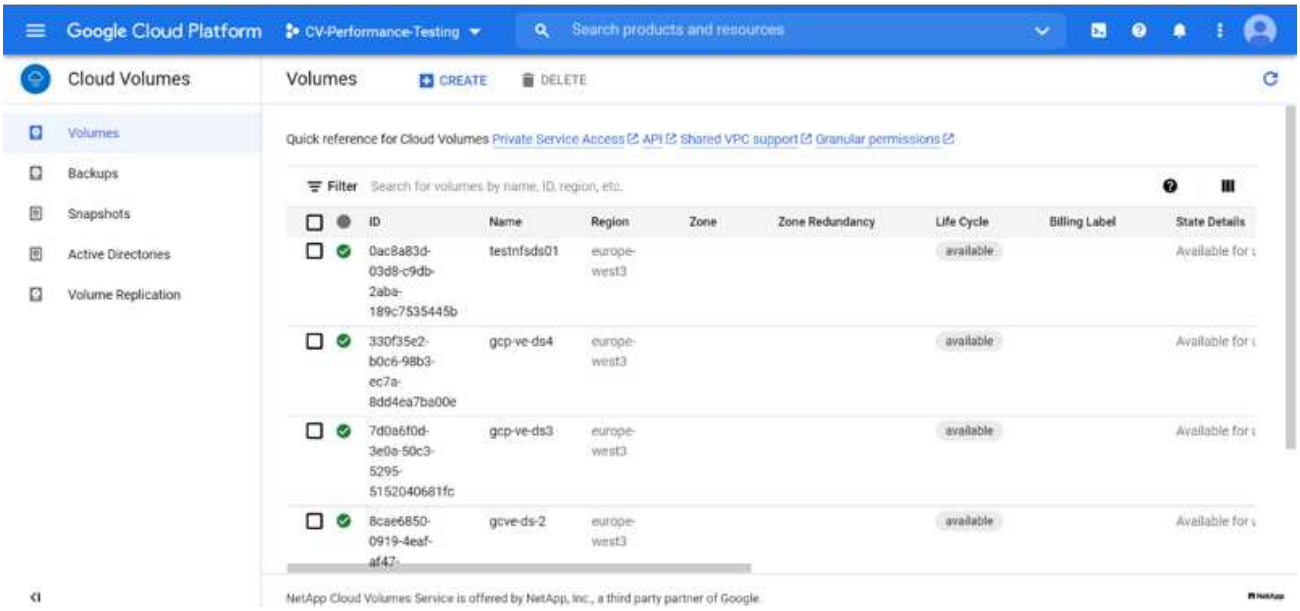
▼ Créer un volume NFS NetApp Volumes vers le cloud privé GCVE

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

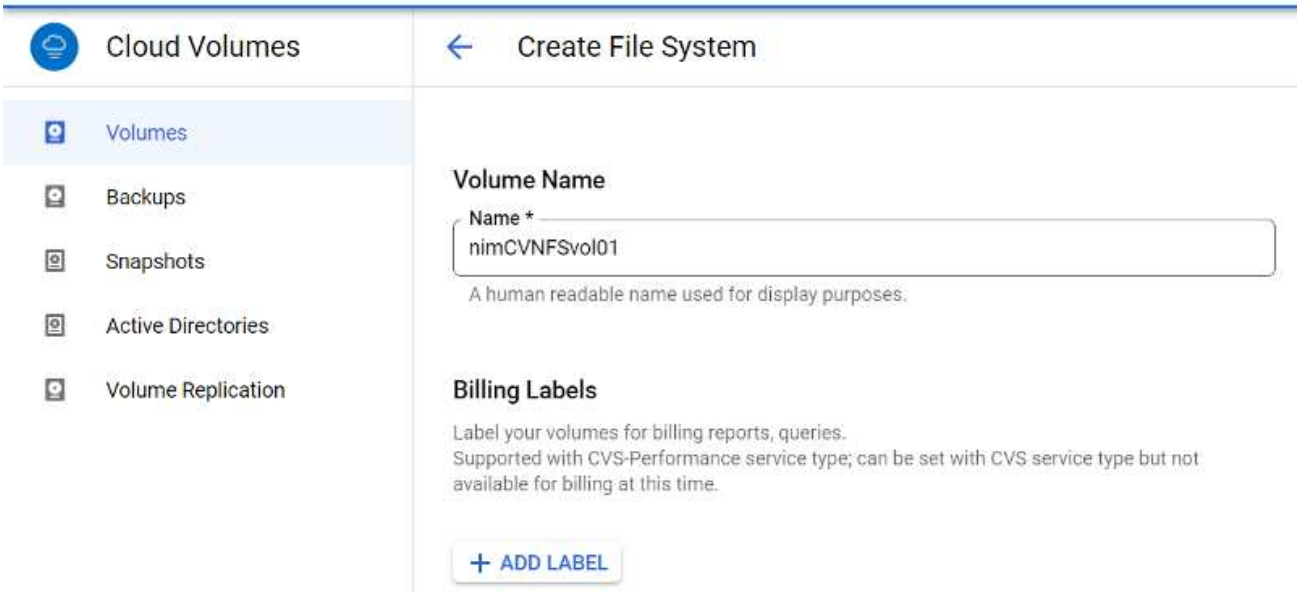
1. Accédez aux volumes Cloud à partir des solutions partenaires dans la console cloud Google.



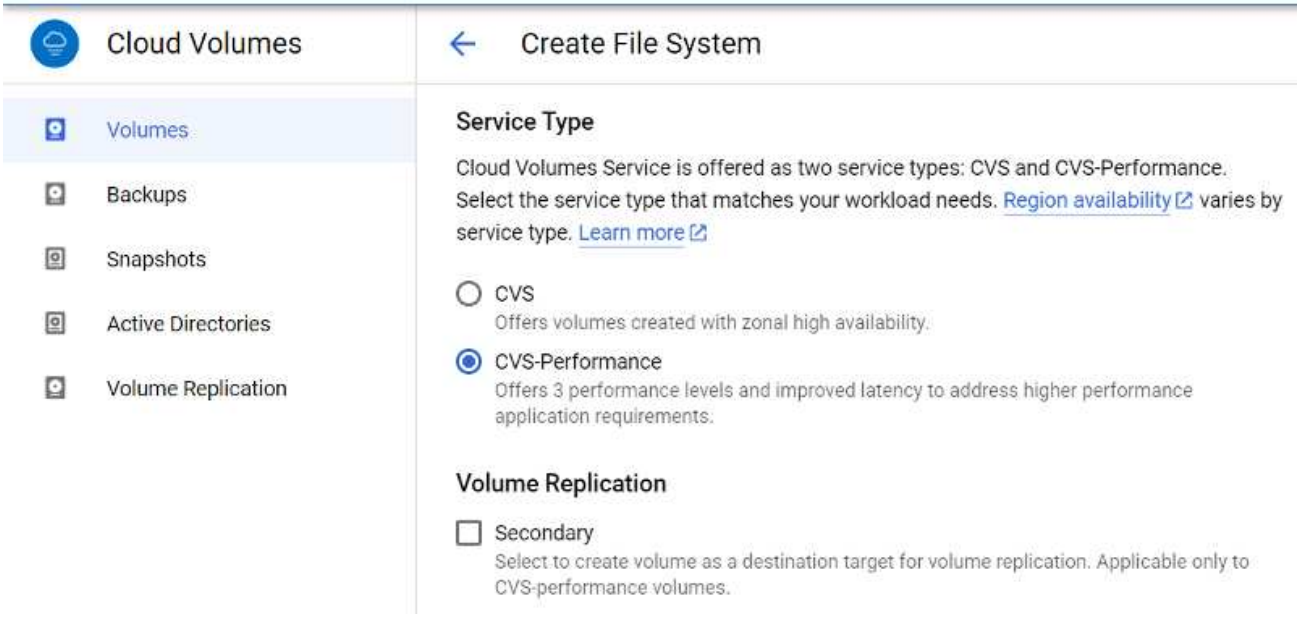
2. Dans la console Cloud Volumes, accédez à la page Volumes et cliquez sur Créer.



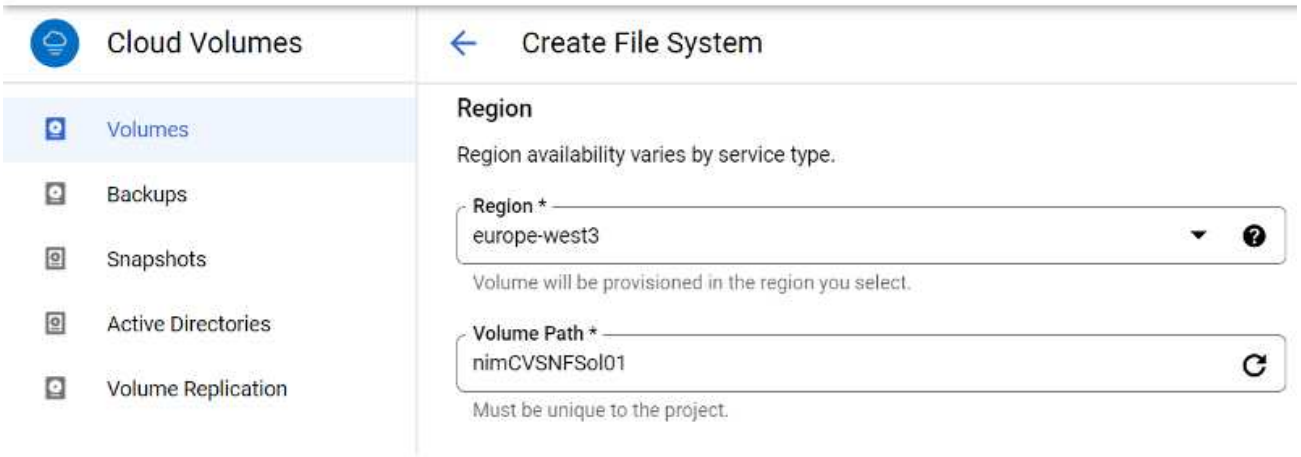
3. Sur la page Créer un système de fichiers, spécifiez le nom du volume et les étiquettes de facturation comme requis pour les mécanismes de rétrofacturation.



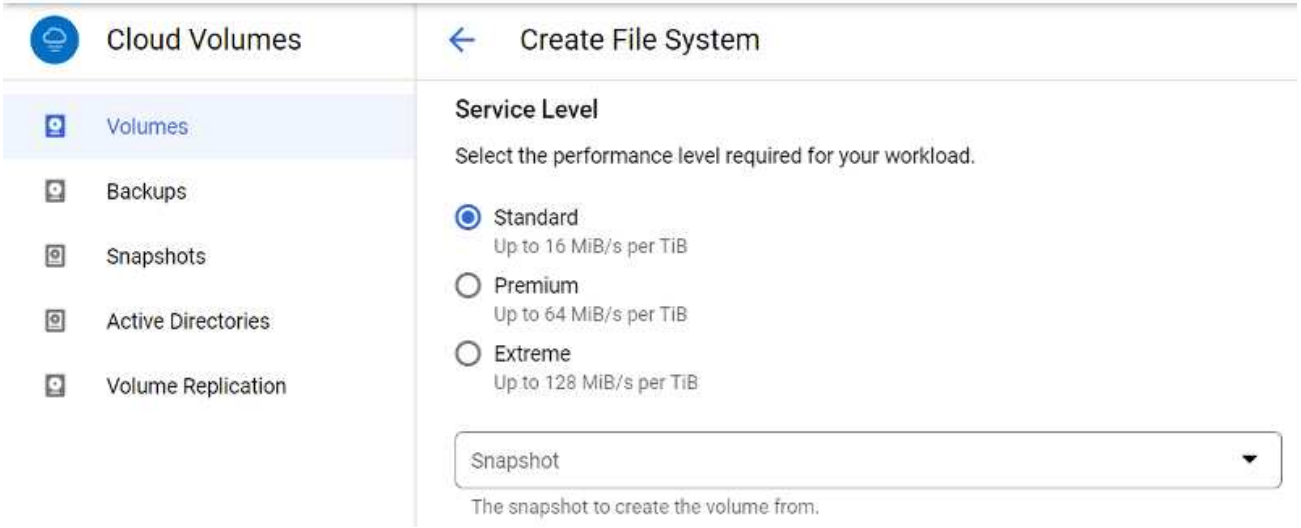
4. Sélectionnez le service approprié. Pour GCVE, choisissez NetApp Volumes-Performance et le niveau de service souhaité pour une latence améliorée et des performances supérieures en fonction des exigences de charge de travail de l'application.



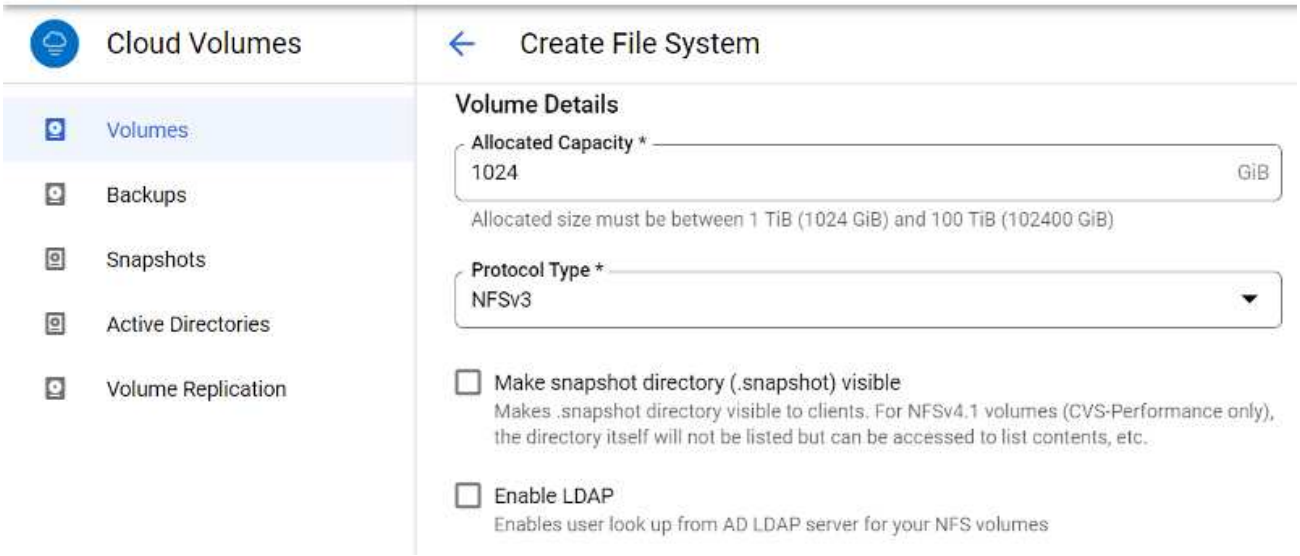
5. Spécifiez la région Google Cloud pour le volume et le chemin du volume (le chemin du volume doit être unique sur tous les volumes cloud du projet)



6. Sélectionnez le niveau de performance du volume.

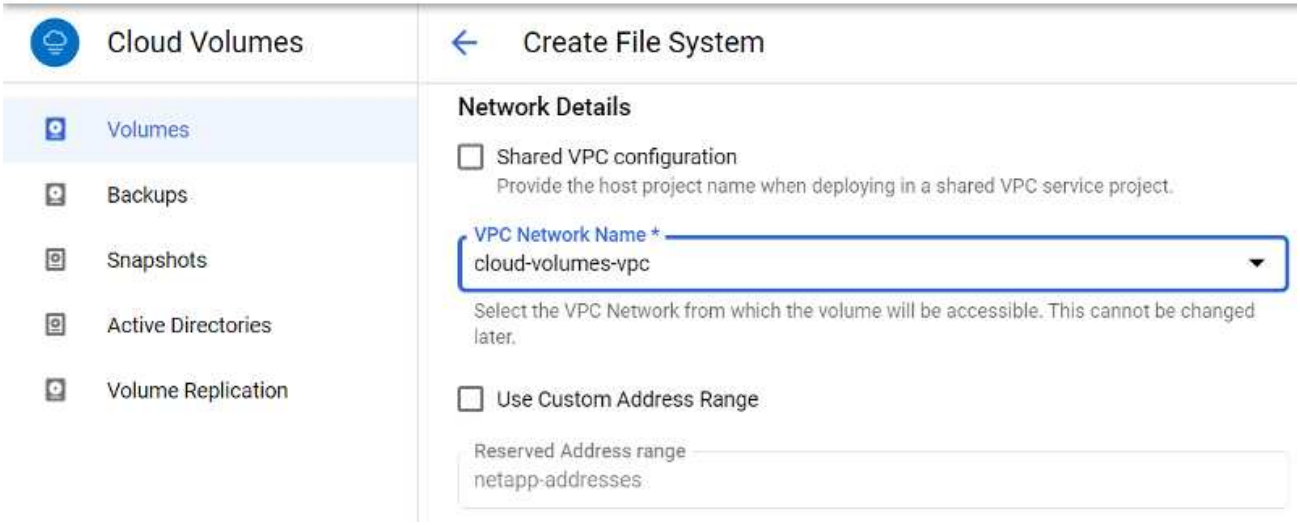


7. Spécifiez la taille du volume et le type de protocole. Dans ce test, NFSv3 est utilisé.



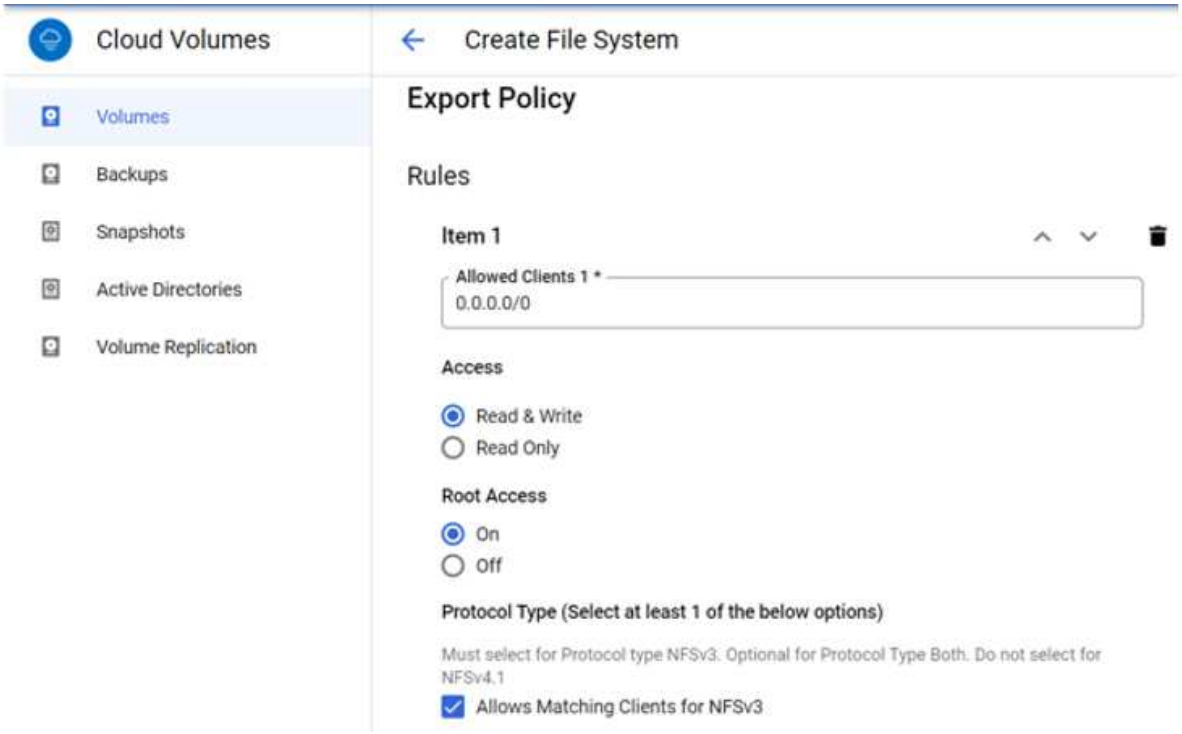
8. Dans cette étape, sélectionnez le réseau VPC à partir duquel le volume sera accessible. Assurez-vous que le peering VPC est en place.

   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 associer votre VPC au producteur Google Cloud NetApp Volumes . Si vous décidez de préparer le peering VPC à l'avance, reportez-vous à ces instructions.



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

   Remarque : l'accès aux volumes NFS ne sera pas possible à moins qu'une politique d'exportation ne soit ajoutée.



10. Cliquez sur Enregistrer pour créer le volume.



▼ **Montage des exportations NFS vers des machines virtuelles exécutées sur VMware Engine**

Avant de préparer le montage du volume NFS, assurez-vous que l'état de peering de la connexion privée est répertorié comme Actif. Une fois que le statut est Actif, utilisez la commande mount.

Pour monter un volume NFS, procédez comme suit :

1. Dans la console Cloud, accédez à Cloud Volumes > Volumes.
2. Accéder à la page Volumes
3. Cliquez sur le volume NFS pour lequel vous souhaitez monter les exportations 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, suivez les étapes ci-dessous :

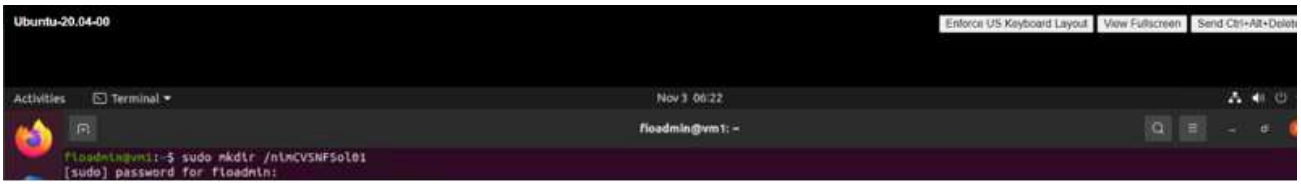
1. Utilisez le client SSH et connectez-vous à la machine virtuelle.
2. Installez le client nfs sur l'instance.
   a. Sur une instance Red Hat Enterprise Linux ou SuSE Linux :

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

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

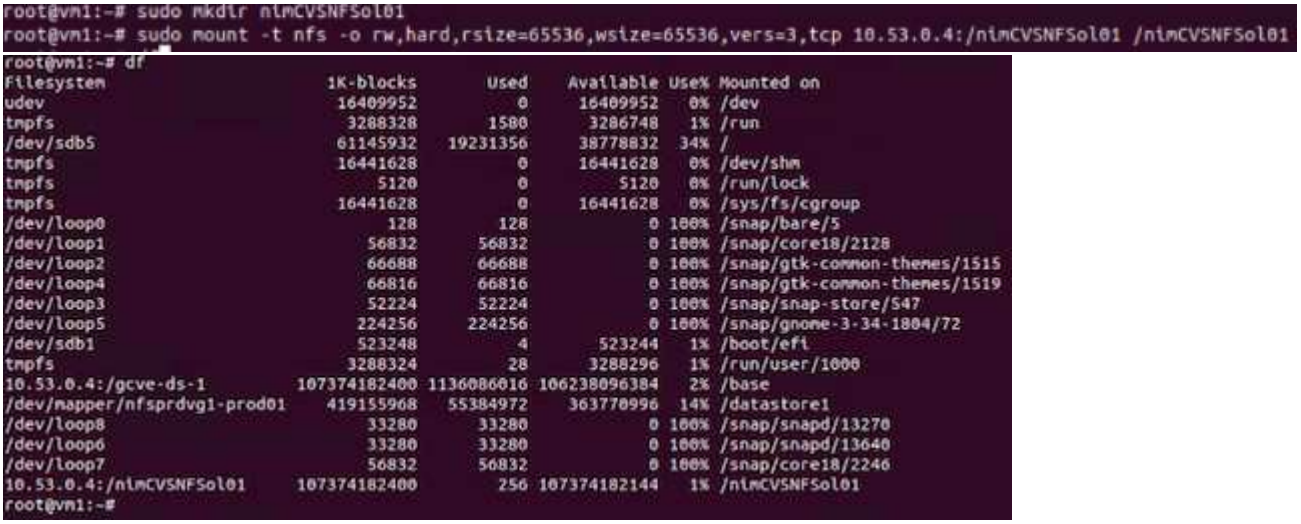
3. Créez un nouveau répertoire sur l'instance, tel que « /nimCVSNFSol01 » :

```
sudo mkdir /nimCVSNFSol01
```



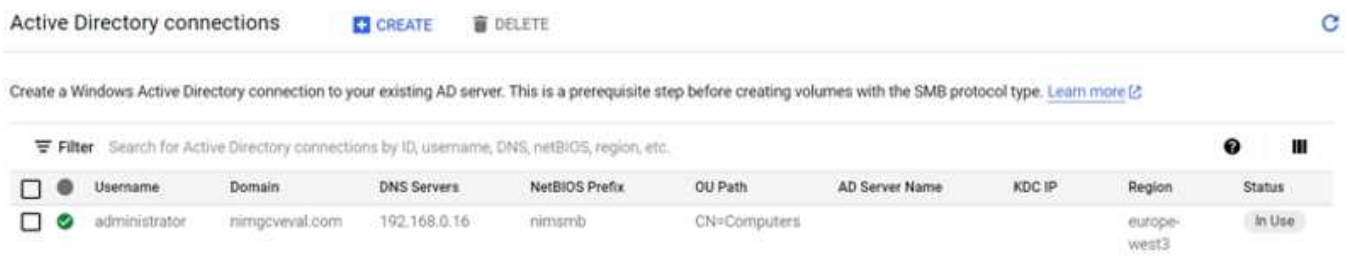
4. Montez le volume à l'aide de la commande appropriée. Un exemple de commande du laboratoire est ci-dessous :

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



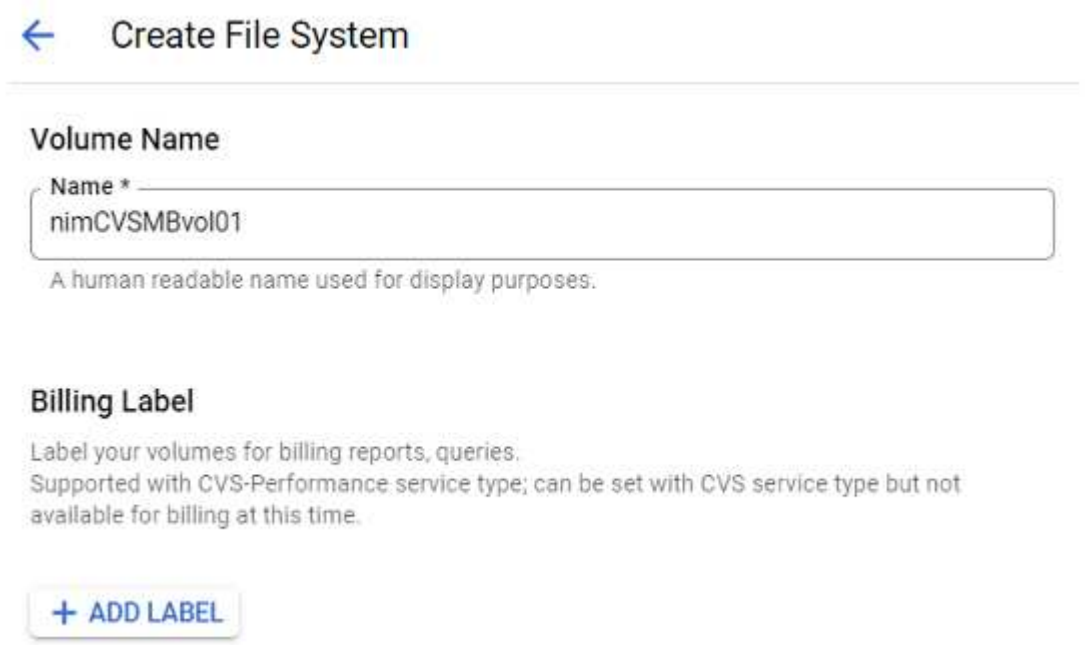
▼ **Création et montage d'un partage SMB sur des machines virtuelles exécutées sur VMware Engine**

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

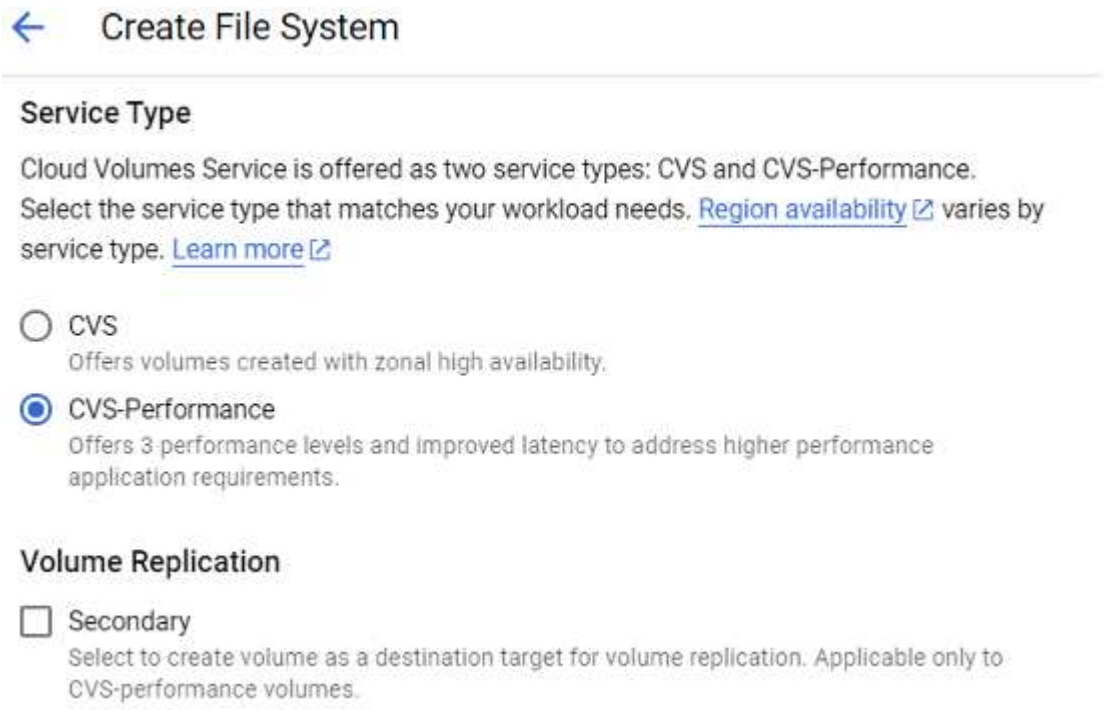


Une fois la connexion AD en place, créez le volume avec le niveau de service souhaité. Les étapes sont similaires à la création d'un volume NFS, sauf que vous sélectionnez le protocole approprié.

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 étiquettes de facturation comme requis pour les mécanismes de rétrofacturation.



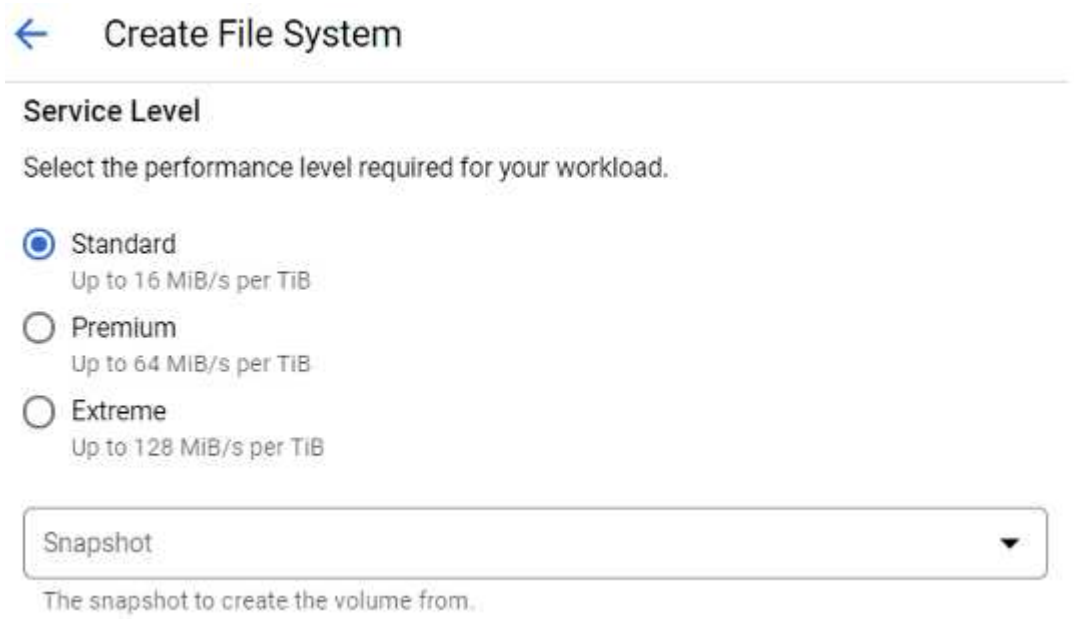
3. Sélectionnez le service approprié. Pour GCVE, choisissez NetApp Volumes-Performance et le niveau de service souhaité pour une latence améliorée et des performances supérieures en fonction des exigences de la charge de travail.



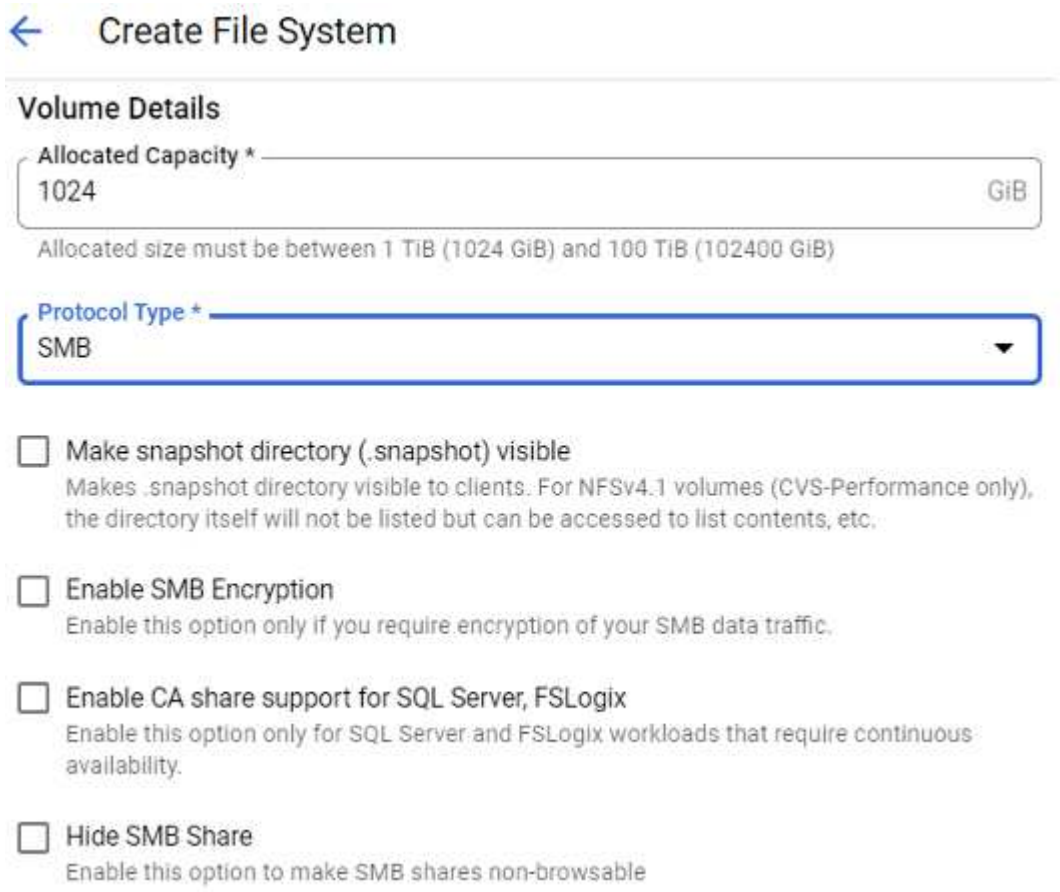
4. Spécifiez la région Google Cloud pour le volume et le chemin du volume (le chemin du volume doit être unique sur tous les volumes cloud du projet)



5. Sélectionnez le niveau de performance du volume.

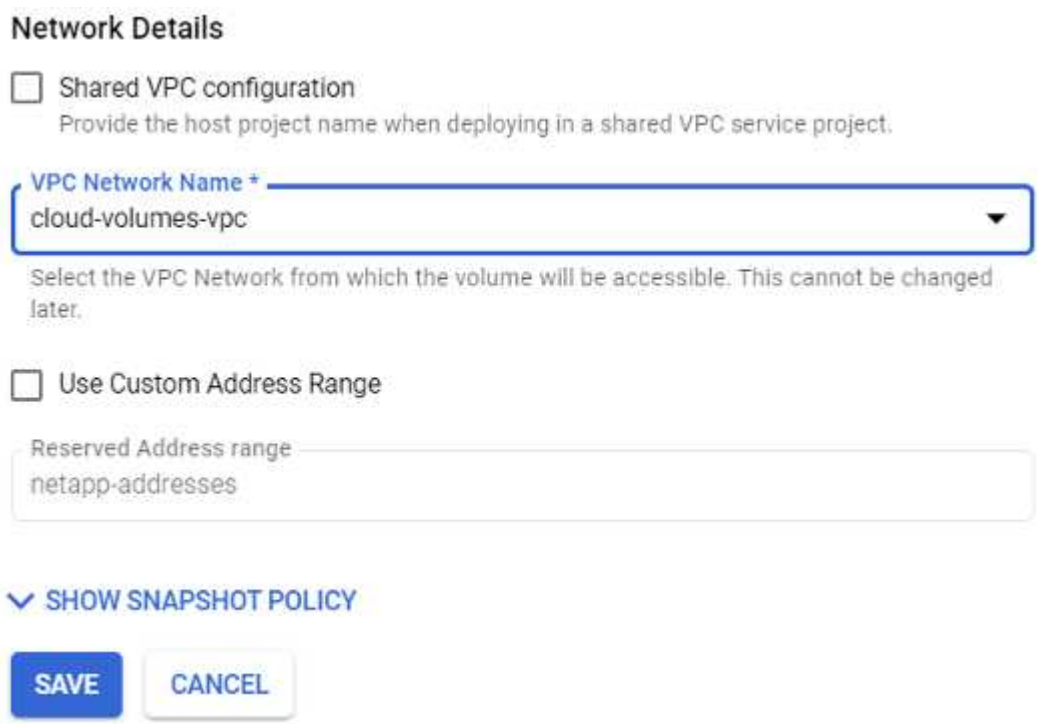


6. Spécifiez la taille du volume et le type de protocole. Dans ce test, SMB est utilisé.



7. Dans 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 encore été effectué, un bouton contextuel s'affichera pour vous guider dans les commandes de peering. Ouvrez une session Cloud Shell et exécutez les commandes appropriées pour établir le peering de votre VPC avec le producteur Google Cloud NetApp Volumes. Si vous souhaitez préparer le peering VPC au préalable, consultez ces "instructions".



8. Cliquez sur Enregistrer pour créer le volume.



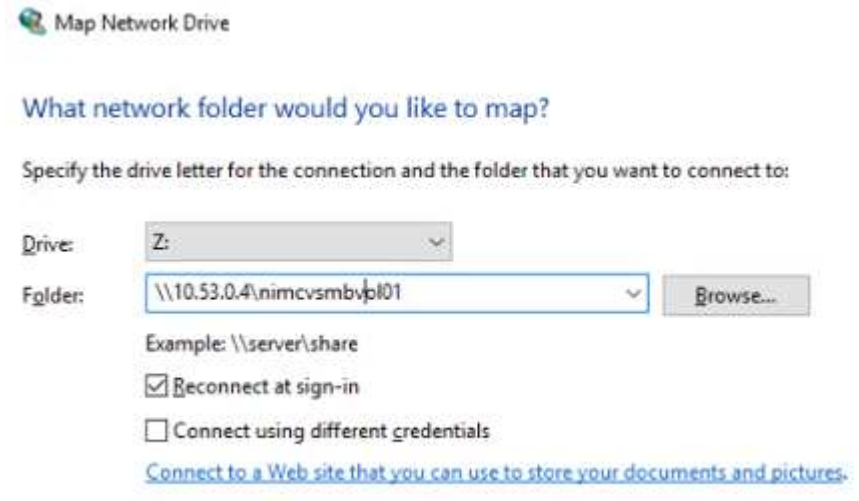
Pour monter le volume SMB, procédez comme suit :

1. Dans la console Cloud, accédez à Cloud Volumes > Volumes.
2. Accéder 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, suivez les étapes ci-dessous :

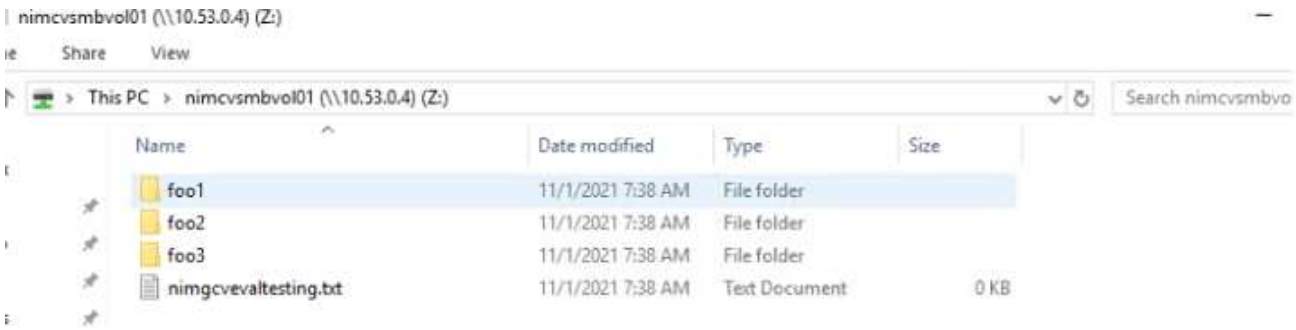
1. Cliquez sur le bouton Démarrer, puis sur Ordinateur.
2. Cliquez sur Connecter un lecteur réseau.
3. Dans la liste des lecteurs, cliquez sur n'importe quelle lettre de lecteur disponible.
4. Dans la zone de dossier, tapez :

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



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

5. Cliquez sur Terminer.



Résumé et conclusion : Pourquoi choisir NetApp Hybrid Multicloud avec VMware ?

NetApp Cloud Volumes ainsi que les solutions VMware pour les principaux hyperscalers offrent un grand potentiel aux organisations qui cherchent à tirer parti du cloud hybride. Le reste de cette section fournit les cas d'utilisation qui montrent que l'intégration de NetApp Cloud Volumes permet de véritables capacités multicloud hybrides.

Cas d'utilisation n°1 : Optimisation du stockage

Lors de l'exécution d'un exercice de dimensionnement à l'aide de la sortie RVtools, il est toujours évident que l'échelle de puissance (vCPU/vMem) est parallèle au stockage. Souvent, les organisations se retrouvent dans une situation où l'espace de stockage requis augmente la taille du cluster bien au-delà de ce qui est nécessaire en termes de puissance.

En intégrant NetApp Cloud Volumes, les organisations peuvent réaliser une solution cloud basée sur vSphere avec une approche de migration simple, sans changement de plate-forme, sans changement d'IP et sans changement d'architecture. De plus, cette optimisation vous permet de faire évoluer l'empreinte de stockage tout en conservant le nombre d'hôtes au minimum requis dans vSphere, mais sans modifier la hiérarchie de stockage, la sécurité ou les fichiers mis à disposition. Cela vous permet d'optimiser le déploiement et de réduire le coût total de possession global de 35 à 45 %. Cette intégration vous permet également de faire

évoluer le stockage du stockage à chaud vers des performances de niveau production en quelques secondes.

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

Les organisations sont soumises à la pression de migrer des applications des centres de données sur site vers le cloud public pour de multiples raisons : une expiration de bail imminente ; une directive financière visant à passer des dépenses d'investissement (capex) aux dépenses opérationnelles (opex) ; ou simplement un mandat descendant visant à tout déplacer vers le cloud.

Lorsque la vitesse est essentielle, seule une approche de migration rationalisée est envisageable, car la refonte et la refactorisation des applications pour s'adapter à la plateforme IaaS particulière du cloud sont lentes et coûteuses, prenant souvent des mois. En combinant NetApp Cloud Volumes avec la réplication SnapMirror à faible consommation de bande passante pour le stockage connecté aux invités (y compris les RDM en conjonction avec des copies Snapshot cohérentes avec les applications et HCX, la migration spécifique au cloud (par exemple Azure Migrate) ou des produits tiers pour la réplication des machines virtuelles), cette transition est encore plus simple que de s'appuyer sur des mécanismes de filtres d'E/S chronophages.

Cas d'utilisation n° 3 : extension du centre de données

Lorsqu'un centre de données atteint ses limites de capacité en raison de pics de demande saisonniers ou simplement d'une croissance organique constante, le passage à VMware hébergé dans le cloud avec NetApp Cloud Volumes est une solution simple. L'utilisation de NetApp Cloud Volumes permet de créer, de répliquer et d'étendre le stockage très facilement en offrant une haute disponibilité dans toutes les zones de disponibilité et des capacités de mise à l'échelle dynamique. L'utilisation de NetApp Cloud Volumes permet de minimiser la capacité du cluster hôte en surmontant le besoin de clusters extensibles.

Cas d'utilisation n° 4 : Reprise après sinistre dans le cloud

Dans une approche traditionnelle, en cas de sinistre, les machines virtuelles répliquées dans le cloud nécessiteraient une conversion vers la propre plateforme d'hyperviseur du cloud avant de pouvoir être restaurées – une tâche qui ne doit pas être gérée en cas de crise.

En utilisant NetApp Cloud Volumes pour le stockage connecté aux invités à l'aide de la réplication SnapCenter et SnapMirror sur site ainsi que des solutions de virtualisation de cloud public, une meilleure approche de reprise après sinistre peut être conçue, permettant aux répliques de machines virtuelles d'être récupérées sur une infrastructure VMware SDDC entièrement cohérente avec des outils de récupération spécifiques au cloud (par exemple, Azure Site Recovery) ou des outils tiers équivalents tels que Veeam. Cette approche vous permet également d'effectuer rapidement des exercices de reprise après sinistre et de récupération après un ransomware. Cela vous permet également de passer à une production complète pour les tests ou en cas de sinistre en ajoutant des hôtes à la demande.

Cas d'utilisation n° 5 : Modernisation des applications

Une fois les applications dans le cloud public, les organisations voudront profiter des centaines de services cloud puissants pour les moderniser et les étendre. Avec l'utilisation de NetApp Cloud Volumes, la modernisation est un processus simple car les données d'application ne sont pas verrouillées dans vSAN et permettent la mobilité des données pour un large éventail de cas d'utilisation, y compris Kubernetes.

Conclusion

Que vous cibliez un cloud entièrement cloud ou hybride, NetApp Cloud Volumes offre d'excellentes options pour déployer et gérer les charges de travail des applications ainsi que les services de fichiers et les protocoles de blocs tout en réduisant le coût total de possession en rendant les exigences de données

transparentes pour la couche applicative.

Quel que soit le cas d'utilisation, choisissez votre cloud/hyperscaler préféré avec NetApp Cloud Volumes pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site et sur plusieurs clouds, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise.

Il s'agit du même processus et des mêmes procédures familiers qui sont utilisés pour connecter le stockage. N'oubliez pas que c'est simplement la position des données qui a changé avec les nouveaux noms ; les outils et les processus restent tous les mêmes et NetApp Cloud Volumes aide à optimiser le déploiement global.

Cas d'utilisation du cloud hybride VMware

Cas d'utilisation de NetApp Hybrid Multicloud avec VMware

Un aperçu des cas d'utilisation importants pour l'organisation informatique lors de la planification de déploiements de cloud hybride ou de cloud first.

Cas d'utilisation populaires

Les cas d'utilisation incluent :

- Reprise après sinistre,
- Hébergement des charges de travail pendant la maintenance du centre de données, * pic rapide dans lequel des ressources supplémentaires sont nécessaires au-delà de ce qui est provisionné dans le centre de données local,
- Extension du site VMware,
- Migration rapide vers le cloud,
- Développement/test, et
- Modernisation des applications exploitant les technologies complémentaires du cloud.

Tout au long de cette documentation, les références de charge de travail cloud seront détaillées à l'aide des cas d'utilisation VMware. Ces cas d'utilisation sont :

- Protéger (comprend à la fois la reprise après sinistre et la sauvegarde/restauration)
- Émigrer
- Étendre

Au cœur du parcours informatique

La plupart des organisations sont en chemin vers la transformation et la 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 moyens de rendre le processus de migration aussi transparent que possible. Cette approche rendrait leurs efforts de modernisation très faciles car les données sont déjà dans le cloud.

La réponse la plus simple à ce scénario est l'offre VMware dans 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 permettant de conserver les actifs, les compétences et les outils sur site existants tout en exécutant des charges de travail de manière native dans le cloud. Cela réduit les risques car il n'y aura

pas d'interruption de service ni de besoin de changement d'IP et offre à l'équipe informatique la possibilité de fonctionner comme elle le fait sur site en utilisant les compétences et les outils existants. Cela peut conduire à des migrations cloud accélérées et à une transition beaucoup plus fluide vers une architecture multicloud hybride.

Comprendre l'importance des options de stockage NFS supplémentaires

Bien que VMware, quel que soit le cloud, offre des capacités hybrides uniques à chaque client, les options de stockage NFS supplémentaires limitées ont limité son utilité pour les organisations ayant des charges de travail lourdes en stockage. Étant donné que le stockage est directement lié aux hôtes, la seule façon de faire évoluer le stockage est d'ajouter davantage d'hôtes, ce qui peut augmenter les coûts de 35 à 40 % ou plus pour les charges de travail gourmandes en stockage. Ces charges de travail nécessitent simplement un stockage supplémentaire, pas une puissance supplémentaire. Mais cela signifie payer pour des hôtes supplémentaires.

Considérons ce scénario :

Un client n'a besoin que de cinq hôtes pour le processeur et la mémoire, mais a de nombreux besoins de stockage et a besoin de 12 hôtes pour répondre aux exigences de stockage. Cette exigence finit par faire pencher la balance financière en obligeant à acheter des chevaux supplémentaires, alors qu'ils n'ont besoin que d'augmenter le stockage.

Lorsque vous planifiez l'adoption et les migrations vers le cloud, il est toujours important d'évaluer la meilleure approche et de suivre le chemin le plus simple qui réduit les investissements totaux. L'approche la plus courante et la plus simple pour toute migration d'application est le réhébergement (également appelé lift and shift) où il n'y a pas de machine virtuelle (VM) ou de conversion de données. L'utilisation de NetApp Cloud Volumes avec le centre de données défini par logiciel VMware (SDDC), tout en complétant vSAN, offre une option de transfert et de transfert facile.

Solutions NetApp pour VMware dans les hyperscalers

Découvrez-en plus sur les solutions que NetApp apporte à l'environnement VMware dans chacun des hyperscalers : de la migration des flux de travail, à l'extension/l'éclatement vers le cloud, à la sauvegarde/restauration et à la reprise après sinistre.

Solutions NetApp pour les environnements VMware

Que vous fonctionniez dans un modèle de cloud hybride ou dans un modèle « cloud first », NetApp propose une grande variété de solutions pour répondre aux cas d'utilisation les plus courants de gestion des charges de travail dans un modèle de cloud ou de cloud hybride.

NetApp propose également des solutions de stockage provisionnées en tant que stockage invité (connecté en tant qu'invité) ou en tant que banque de données NFS supplémentaire dans chacun des hyperscalers. Toutes les solutions sont classées conformément à la classification VMware des charges de travail cloud. Ces classifications comprennent :

- Protéger (comprend à la fois la reprise après sinistre et la sauvegarde/restauration)
- Émigrer
- Étendre

Pour plus de détails sur les solutions disponibles pour chaque hyperscaler, veuillez visiter :

- "Solutions pour AWS / VMC"

- "Solutions pour Azure / AVS"
- "Solutions pour GCP / GCVE"

Solutions NetApp pour Amazon VMware Managed Cloud (VMC)

Découvrez-en plus sur les solutions que NetApp apporte à AWS.

VMware définit les charges de travail cloud dans l'une des trois catégories suivantes :

- Protéger (y compris la reprise après sinistre et la sauvegarde/restauration)
- Émigrer
- Étendre

Parcourez les solutions disponibles dans les sections suivantes.

Protéger

- "Reprise après sinistre avec VMC sur AWS (connecté en tant qu'invité)"
- "Veeam Backup Restore dans VMC avec FSx ONTAP"
- "Reprise après sinistre (DRO) avec FSx ONTAP et VMC"
- "Utilisation de Veeam Replication et de FSx ONTAP pour la reprise après sinistre sur VMware Cloud sur AWS"

Émigrer

- "Migrer les charges de travail vers la banque de données FSx ONTAP à l'aide de VMware HCX"

Étendre

À VENIR!!

Solutions NetApp pour Azure VMware Solution (AVS)

Découvrez-en plus sur les solutions que NetApp apporte à Azure.

VMware définit les charges de travail cloud dans l'une des trois catégories suivantes :

- Protéger (y compris la reprise après sinistre et la sauvegarde/restauration)
- Émigrer
- Étendre

Parcourez les solutions disponibles dans les sections suivantes.

Protéger

- "Reprise après sinistre avec ANF et JetStream (banque de données NFS supplémentaire)"
- "Reprise après sinistre avec ANF et CVO (stockage connecté en invité)"
- "Reprise après sinistre (DRO) avec ANF et AVS"
- "Utilisation de Veeam Replication et du datastore Azure NetApp Files pour la reprise après sinistre

vers Azure VMware Solution"

Émigrer

- "Migrer les charges de travail vers la banque de données Azure NetApp Files à l'aide de VMware HCX"

Étendre

À VENIR!!

Solutions NetApp pour Google Cloud VMware Engine (GCVE)

Découvrez-en plus sur les solutions que NetApp apporte à GCP.

VMware définit les charges de travail cloud dans l'une des trois catégories suivantes :

- Protéger (y compris la reprise après sinistre et la sauvegarde/restauration)
- Émigrer
- Étendre

Parcourez les solutions disponibles dans les sections suivantes.

Protéger

- "Reprise après sinistre des applications avec SnapCenter, Cloud Volumes ONTAP et Veeam Replication"
- "Reprise après sinistre cohérente des applications avec NetApp SnapCenter et réplication Veeam vers les volumes NetApp sur GCVE"

Émigrer

- "Migration de la charge de travail à l'aide de VMware HCX vers la banque de données NFS Google Cloud NetApp Volumes"
- "Réplication de machines virtuelles à l'aide de Veeam vers un magasin de données NFS Google Cloud NetApp Volumes"

Étendre

À VENIR!!

NetApp pour AWS/VMC

Fonctionnalités NetApp pour AWS VMC

Découvrez-en plus sur les fonctionnalités que NetApp apporte à AWS VMware Cloud (VMC) - de NetApp en tant que périphérique de stockage connecté en tant qu'invité ou banque de données NFS supplémentaire à la migration des flux de travail, à l'extension/à l'éclatement vers le cloud, à la sauvegarde/restauration et à la reprise après sinistre.

Accédez à la section du contenu souhaité en sélectionnant parmi les options suivantes :

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

Configuration de VMC dans AWS

Comme pour les environnements locaux, la planification d'un environnement de virtualisation basé sur le cloud est essentielle pour un environnement prêt pour la production et la création de machines virtuelles et la migration.

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



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

Le processus de configuration peut être décomposé selon les étapes suivantes :

- Déployer et configurer VMware Cloud pour AWS
- Connectez VMware Cloud à FSx ONTAP

Voir le détail"étapes de configuration pour VMC" .

Options de stockage NetApp pour VMC

Le stockage NetApp peut être utilisé de plusieurs manières, soit en tant que stockage de données connecté, soit en tant que banque de données NFS supplémentaire, dans AWS VMC.

S'il vous plaît visitez"Options de stockage NetApp prises en charge" pour plus d'informations.

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

- FSx ONTAP comme stockage connecté invité
- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- FSx ONTAP comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour VMC" . Voir le détail"options de banque de données NFS supplémentaires pour VMC" .

Cas d'utilisation de solutions

Avec les solutions cloud NetApp et VMware, de nombreux cas d'utilisation sont simples à déployer dans votre AWS VMC. Des cas d'utilisation sont définis pour chacune des zones de cloud définies par VMware :

- Protéger (comprend à la fois la reprise après sinistre et la sauvegarde/restauration)
- Étendre
- Émigrer

"Parcourez les solutions NetApp pour AWS VMC"

Protégez les charges de travail sur AWS/VMC

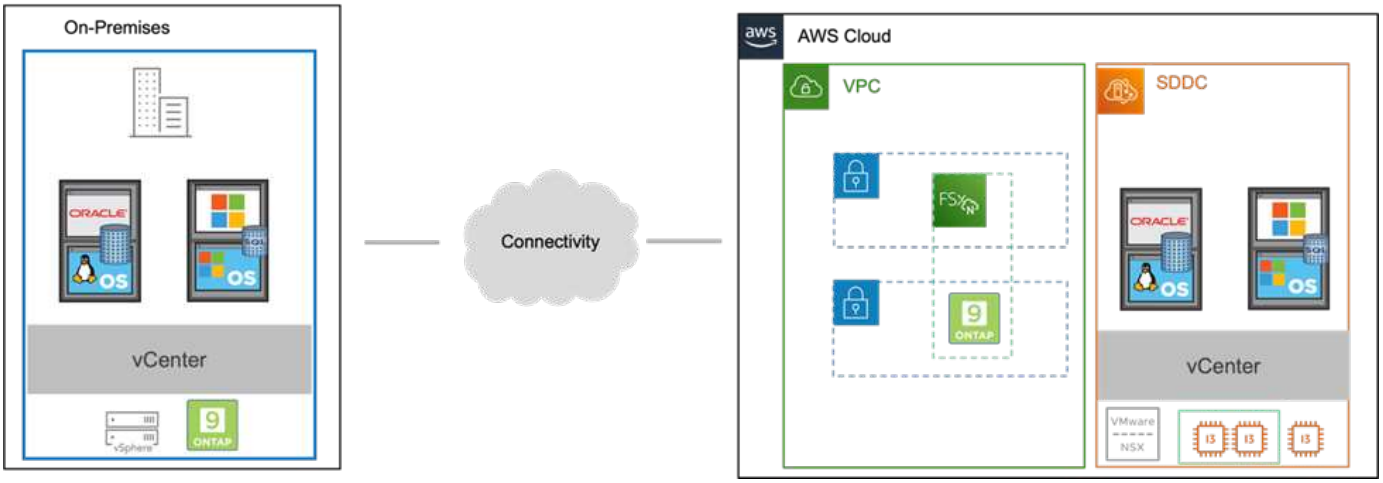
TR-4931 : Reprise après sinistre avec VMware Cloud sur Amazon Web Services et Guest Connect

Un environnement et un plan de reprise après sinistre (DR) éprouvés sont essentiels pour les organisations afin de garantir que les applications critiques pour l'entreprise peuvent être rapidement restaurées en cas de panne majeure. Cette solution se concentre sur la démonstration de cas d'utilisation DR en mettant l'accent sur les technologies VMware et NetApp , à la fois sur site et avec VMware Cloud sur AWS.

Aperçu

NetApp possède une longue histoire d'intégration avec VMware, comme en témoignent les dizaines de milliers de clients qui ont choisi NetApp comme partenaire de stockage pour leur environnement virtualisé. Cette intégration se poursuit avec des options connectées aux invités dans le cloud et des intégrations récentes avec les magasins de données NFS également. Cette solution se concentre sur le cas d'utilisation communément appelé stockage connecté aux invités.

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



Hypothèses, prérequis et aperçu des composants

Avant de déployer cette solution, examinez la présentation des composants, les prérequis requis pour déployer la solution et les hypothèses formulées lors de la documentation de cette solution.

"Exigences, prérequis et planification de la solution DR"

Exécution de la reprise après sinistre avec SnapCenter

Dans cette solution, SnapCenter fournit des instantanés cohérents avec les applications pour les données d'application SQL Server et Oracle. Cette configuration, associée à la technologie SnapMirror , permet une réplication de données à haut débit entre notre cluster AFF sur site et notre cluster FSx ONTAP . De plus, Veeam Backup & Replication fournit des fonctionnalités de sauvegarde et de restauration pour nos machines virtuelles.

Dans cette section, nous couvrons 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 un basculement sur le site secondaire :

Configurer les relations et les calendriers de conservation de SnapMirror

SnapCenter peut mettre à jour les relations SnapMirror au sein du système de stockage principal (primaire > miroir) et vers les systèmes de stockage secondaires (primaire > coffre-fort) à des fins d'archivage et de conservation à long terme. Pour ce faire, vous devez établir et initialiser une relation de réplication de données entre un volume de destination et un volume source à l'aide de SnapMirror.

Les systèmes ONTAP source et de destination doivent se trouver dans des réseaux appairés à l'aide de l'appairage Amazon VPC, d'une passerelle de transit, d'AWS Direct Connect ou d'un VPN AWS.

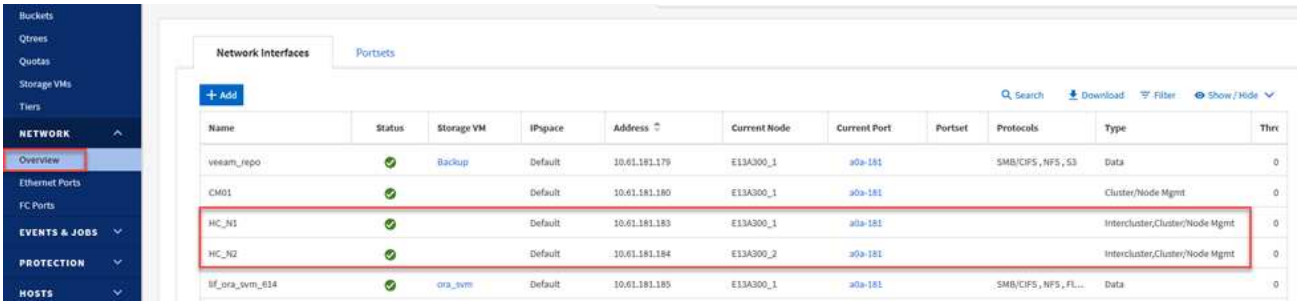
Les étapes suivantes sont requises pour configurer les relations SnapMirror entre un système ONTAP sur site et FSx ONTAP:

ⓘ Se référer à la "FSx 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 à partir du Gestionnaire système ou de l'interface de ligne de commande.

1. Dans ONTAP System Manager, accédez à la page Présentation du réseau et récupérez les adresses IP de type : Intercluster qui sont configurées pour communiquer avec le VPC AWS sur lequel FSx est installé.



2. Pour récupérer les adresses IP intercluster pour FSx, connectez-vous à la CLI 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.
```

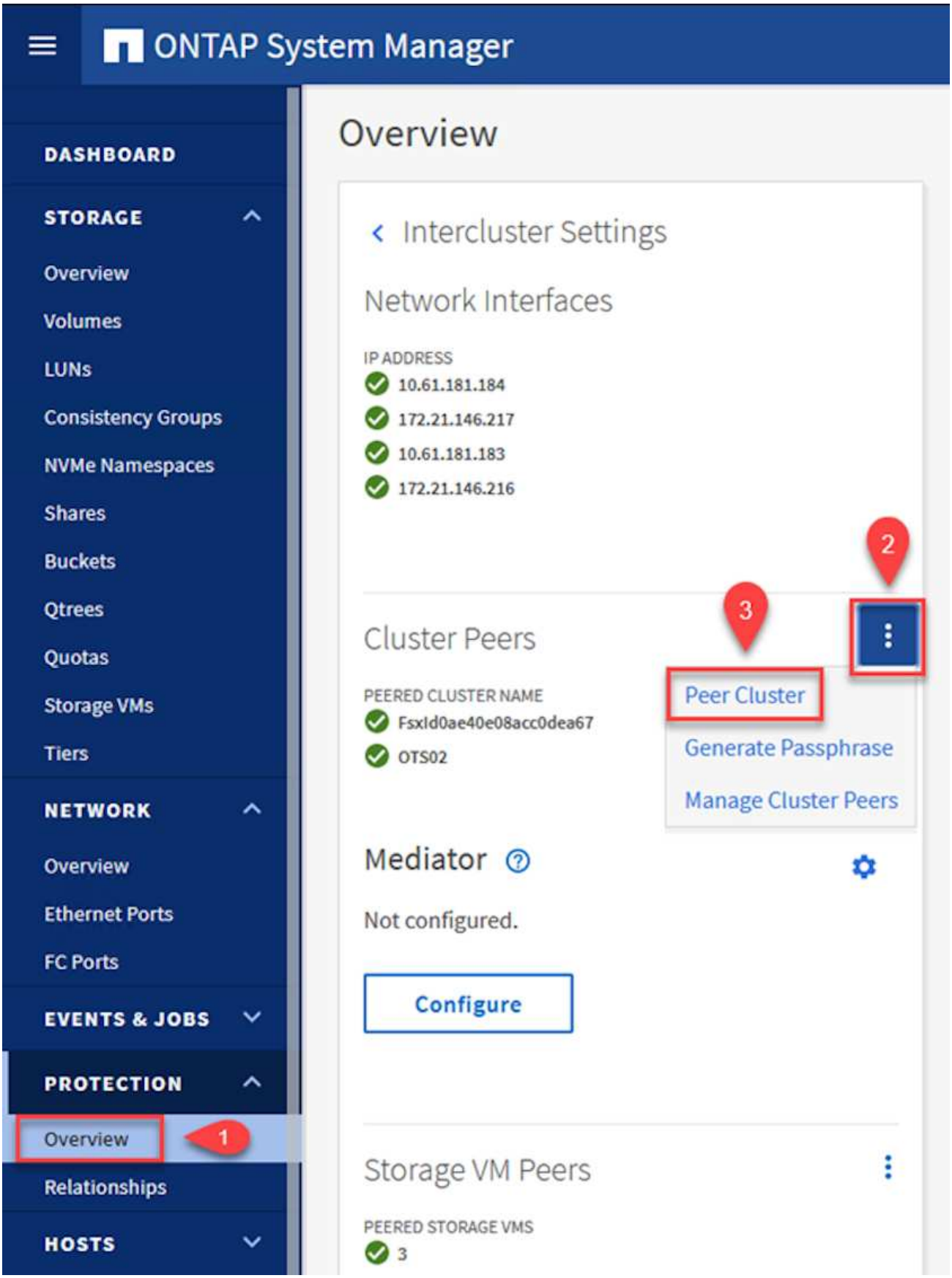
▼ **Établir un peering de cluster entre ONTAP et FSx**

Pour établir un peering de cluster entre les clusters ONTAP , une phrase secrète unique entrée dans le cluster ONTAP initiateur doit être confirmée dans l'autre cluster homologue.

1. Configurer le peering sur le cluster FSx de destination à l'aide de `cluster peer create` commande. Lorsque vous y êtes invité, entrez une phrase secrète unique qui sera 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. Au niveau du cluster source, vous pouvez établir la relation entre homologues du cluster à l'aide d' ONTAP System Manager ou de l'interface de ligne de commande. Depuis ONTAP System Manager, accédez à Protection > Présentation et sélectionnez Cluster homologue.



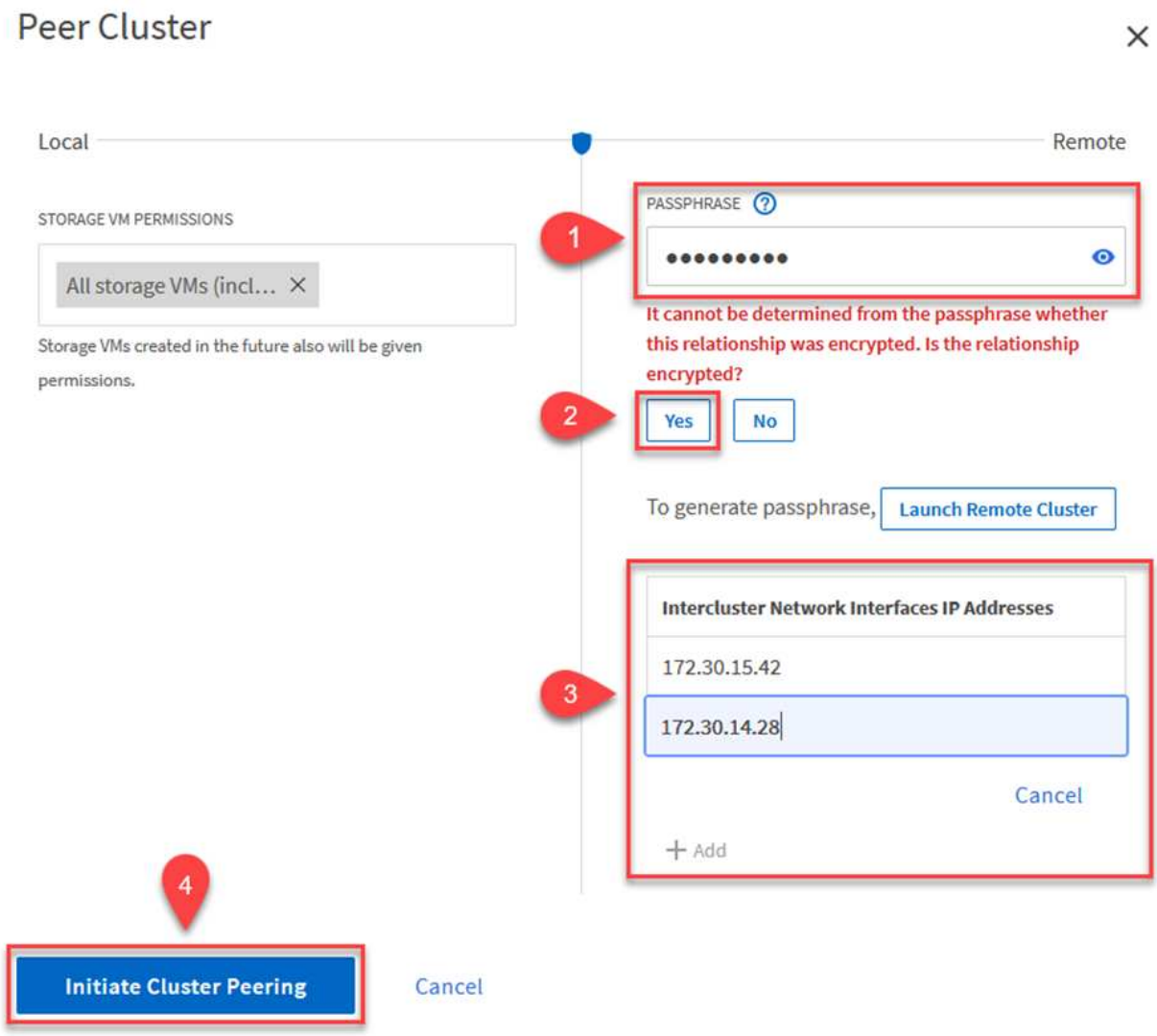
3. Dans la boîte de dialogue Cluster homologue, remplissez les informations requises :
   a. Saisissez la phrase secrète utilisée pour établir la relation de cluster homologue sur le cluster FSx

de destination.

b. Sélectionner `Yes` pour établir une relation cryptée.

c. Saisissez la ou les adresses IP LIF intercluster du cluster FSx de destination.

d. Cliquez sur Initier l'appairage de cluster pour finaliser le processus.



4. Vérifiez l'état de la relation entre les homologues du cluster 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
```

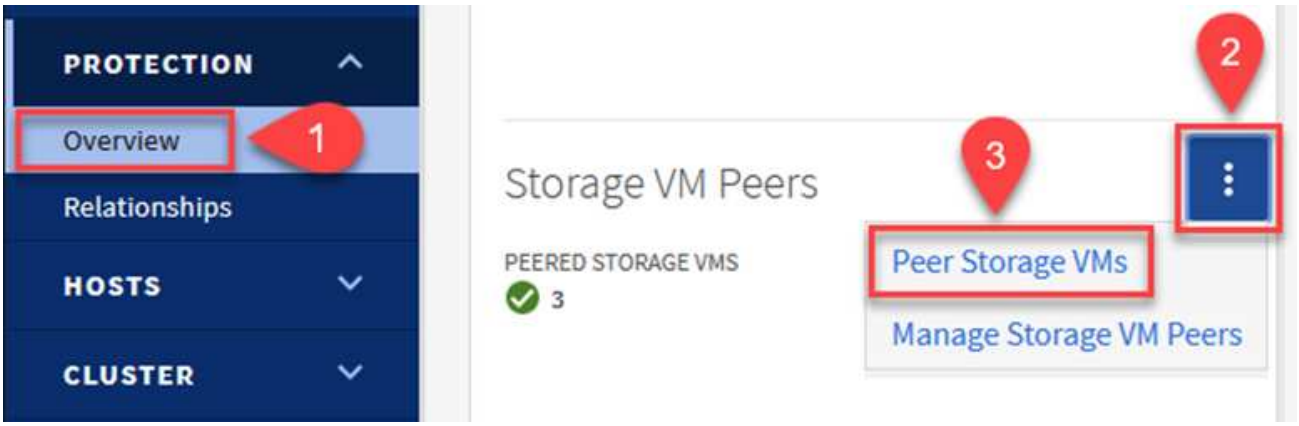
▼ Établir une relation de peering SVM

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

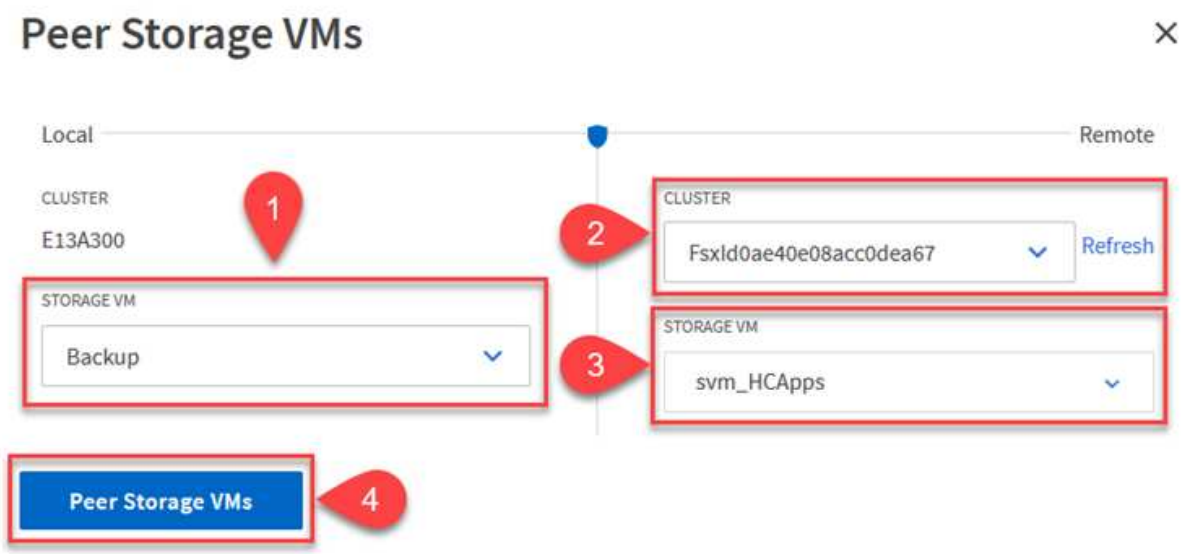
1. À partir du cluster FSx source, utilisez la commande suivante depuis la CLI pour créer la relation homologue SVM :

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

2. À partir du cluster ONTAP source, acceptez la relation de peering avec ONTAP System Manager ou l'interface de ligne de commande.
3. Depuis ONTAP System Manager, accédez à Protection > Présentation et sélectionnez Machines virtuelles de stockage homologues sous Homologues de machines virtuelles de stockage.



4. Dans la boîte de dialogue de la machine virtuelle de stockage homologue, remplissez les champs obligatoires :
   - La machine virtuelle de stockage source
   - Le cluster de destination
   - La machine virtuelle de stockage de destination



5. Cliquez sur « Appairer les machines virtuelles de stockage » pour terminer le processus d'appairage SVM.

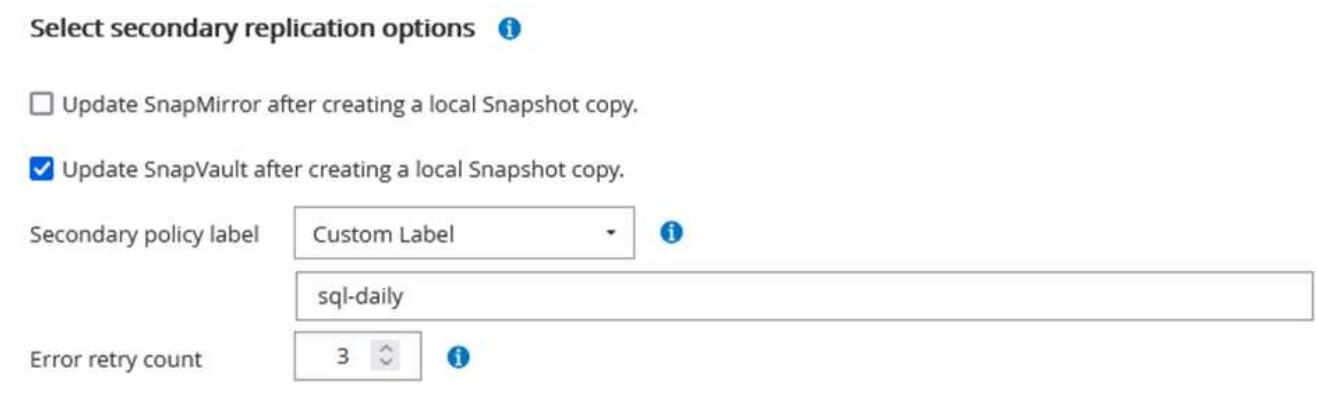
▼ **Créer une politique de conservation des instantanés**

SnapCenter gère les planifications de conservation pour les sauvegardes qui existent sous forme de copies instantanées sur le système de stockage principal. Ceci est établi lors de la création d'une politique dans SnapCenter. SnapCenter ne gère pas les politiques de rétention pour les sauvegardes conservées sur des systèmes de stockage secondaires. Ces politiques sont gérées séparément via une politique SnapMirror créée sur le cluster FSx secondaire et associée aux volumes de destination qui sont dans une relation SnapMirror avec le volume source.

Lors de la création d'une politique SnapCenter , vous avez la possibilité de spécifier une étiquette de politique secondaire qui est ajoutée à l'étiquette SnapMirror de chaque snapshot généré lorsqu'une sauvegarde SnapCenter est effectuée.

ⓘ Sur le stockage secondaire, ces étiquettes correspondent aux règles de stratégie associées au volume de destination afin d'appliquer la conservation des instantanés.

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



Pour plus d'informations sur la création de politiques SnapCenter pour une base de données SQL Server, consultez le "Documentation de SnapCenter" .

Vous devez d'abord créer une stratégie SnapMirror avec des règles qui dictent le nombre de copies d'instantanés à conserver.

1. Créez la politique 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 politique avec des étiquettes SnapMirror qui correspondent aux étiquettes de politique secondaires spécifiées dans les politiques 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 pourrait être ajoutée à une politique :

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

Créez des règles supplémentaires pour chaque étiquette SnapMirror et le nombre d'instantanés à conserver (période de conservation).

▼ **Créer des volumes de destination**

Pour créer un volume de destination sur FSx qui sera le destinataire des copies instantanées de nos volumes sources, exécutez la commande suivante sur FSx ONTAP:

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

▼ **Créer les 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 nouvel instantané généré à partir du volume source et le copie sur le volume de destination.

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

Déployez et configurez le serveur Windows SnapCenter sur site.

▼ **Déployer Windows SnapCenter Server sur site**

Cette solution utilise NetApp SnapCenter pour effectuer des sauvegardes cohérentes avec les applications des bases de données SQL Server et Oracle. Associé à Veeam Backup & Replication pour la sauvegarde des VMDK de machines virtuelles, cela fournit une solution complète de reprise après sinistre pour les centres de données sur site et dans le cloud.

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

Le SnapCenter software peut être obtenu à l'adresse "ce lien" .

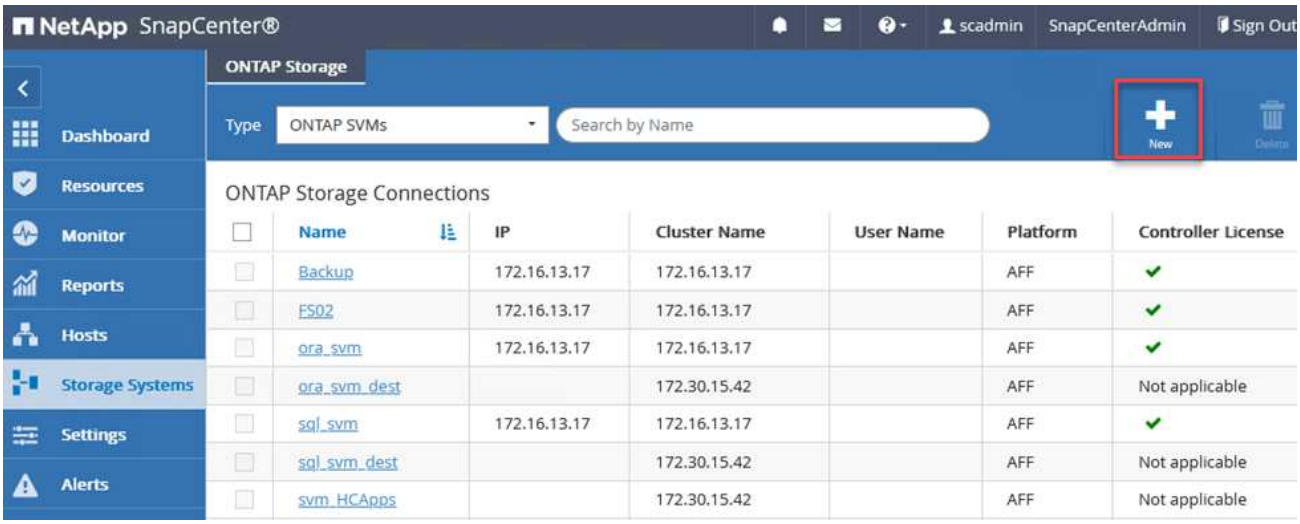
Une fois installé, vous pouvez accéder à la console SnapCenter à partir d'un navigateur Web en utilisant *https://Virtual_Cluster_IP_or_FQDN:8146*.

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

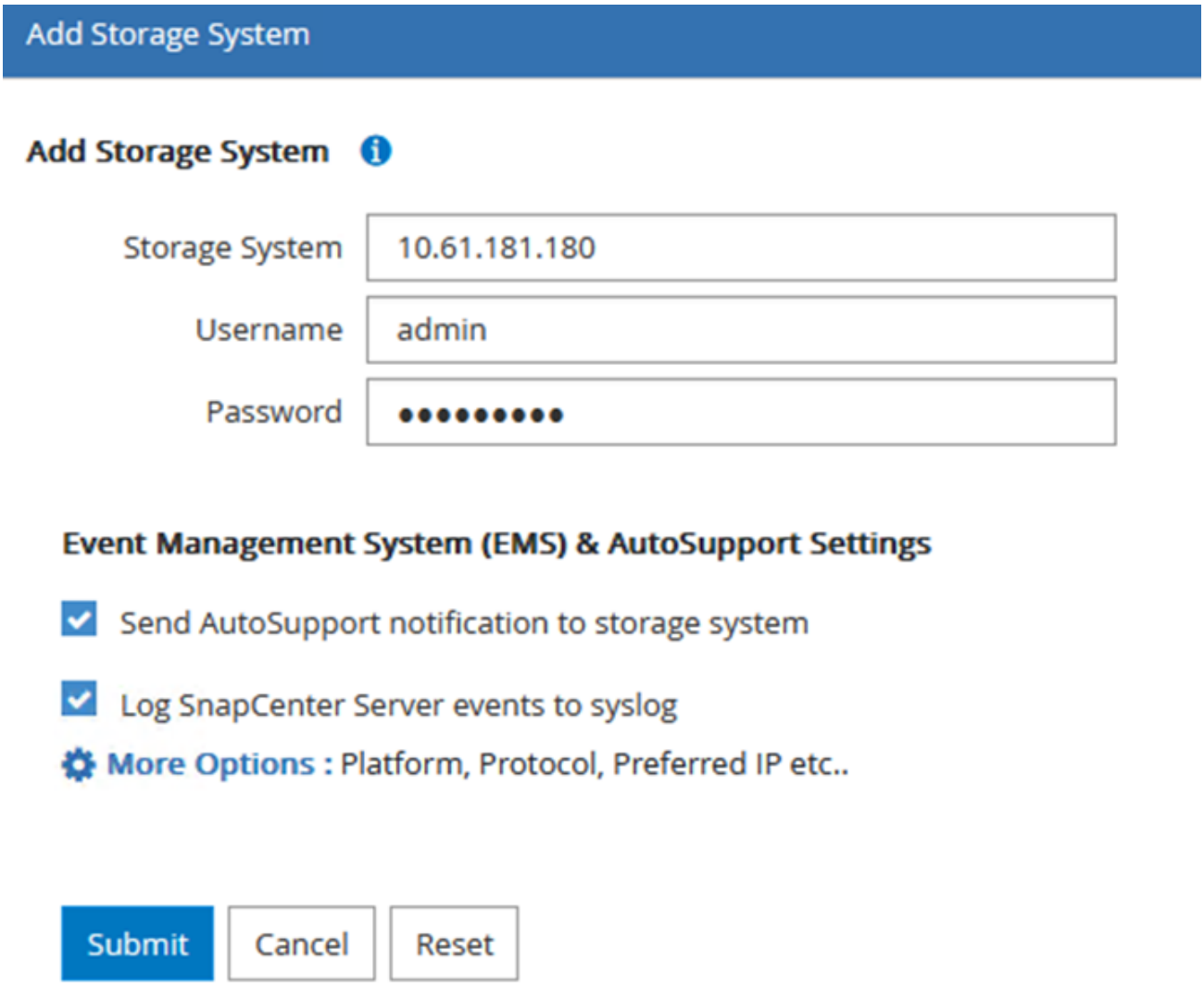
▼ **Ajouter des contrôleurs de stockage à SnapCenter**

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

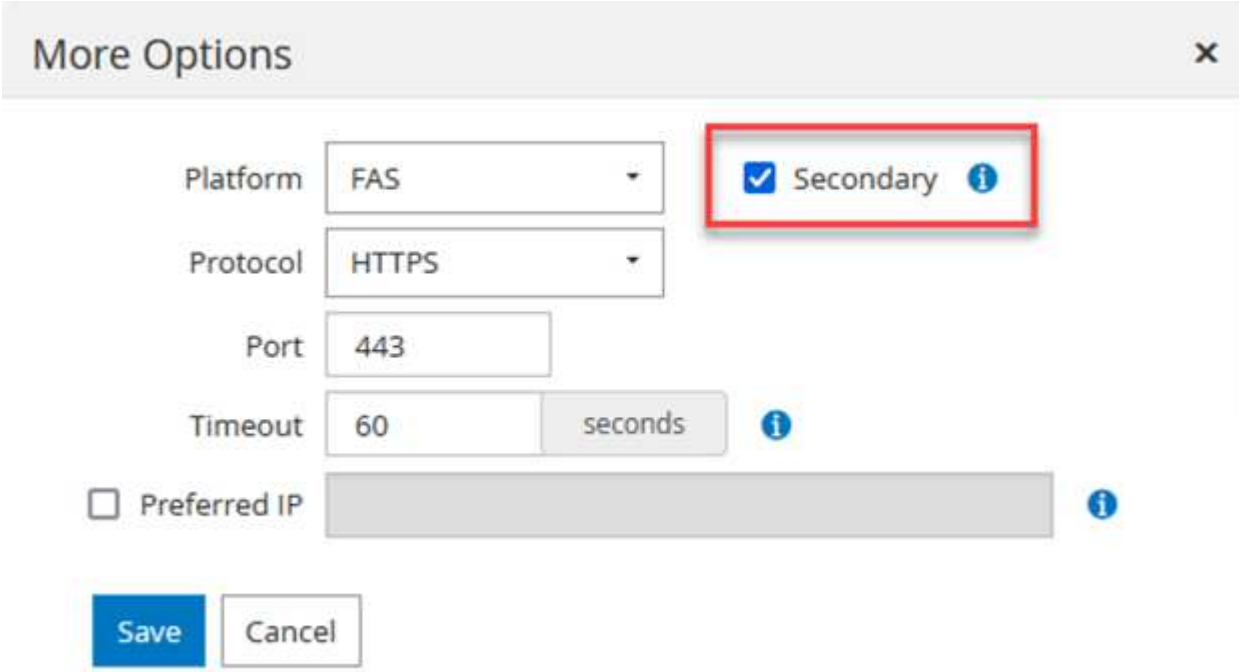
1. Dans le menu de gauche, sélectionnez Systèmes de stockage, puis cliquez sur Nouveau pour commencer le processus d'ajout de vos contrôleurs de stockage à SnapCenter.



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 Soumettre pour commencer la découverte du système de stockage.



3. Répétez ce processus pour ajouter le système FSx ONTAP à SnapCenter. Dans ce cas, sélectionnez Plus d'options en bas de la fenêtre Ajouter un système de stockage et cliquez sur la case à cocher Secondaire pour désigner le système FSx comme système de stockage secondaire mis à jour avec des copies SnapMirror ou nos instantanés de sauvegarde principaux.

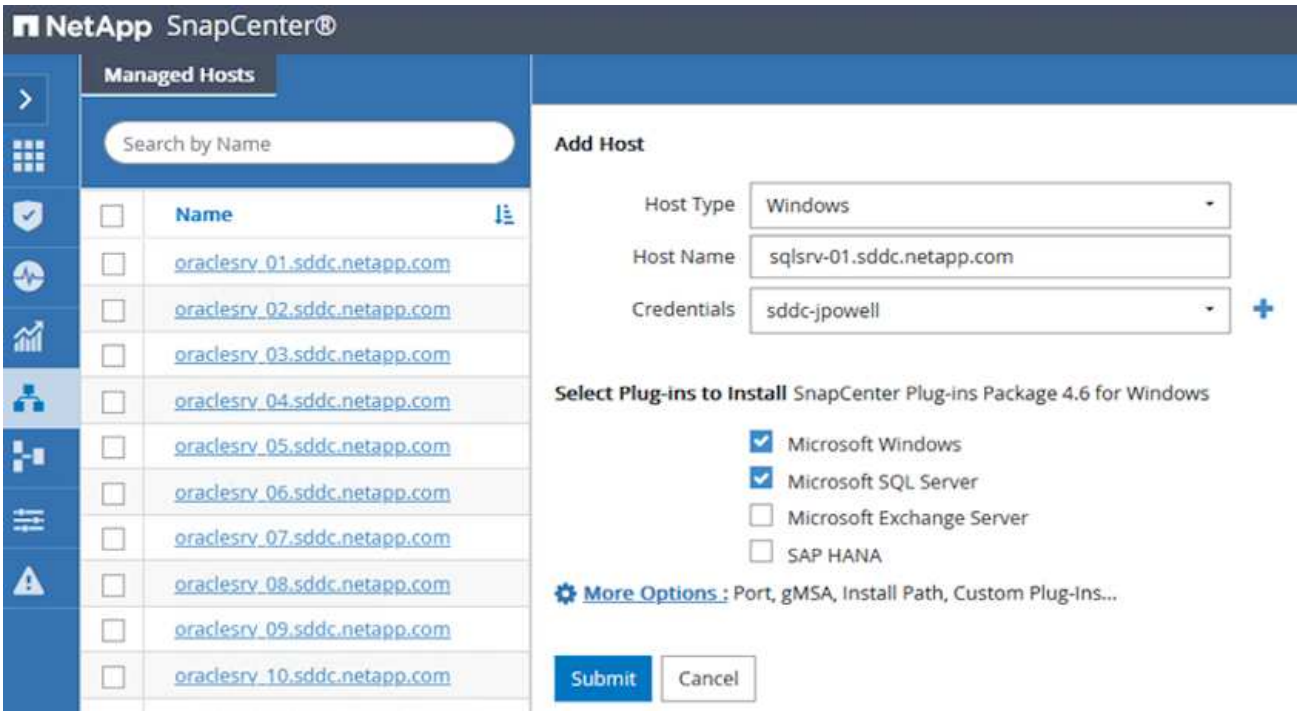


Pour plus d'informations sur l'ajout de systèmes de stockage à SnapCenter, consultez la documentation à l'adresse "ce lien" .

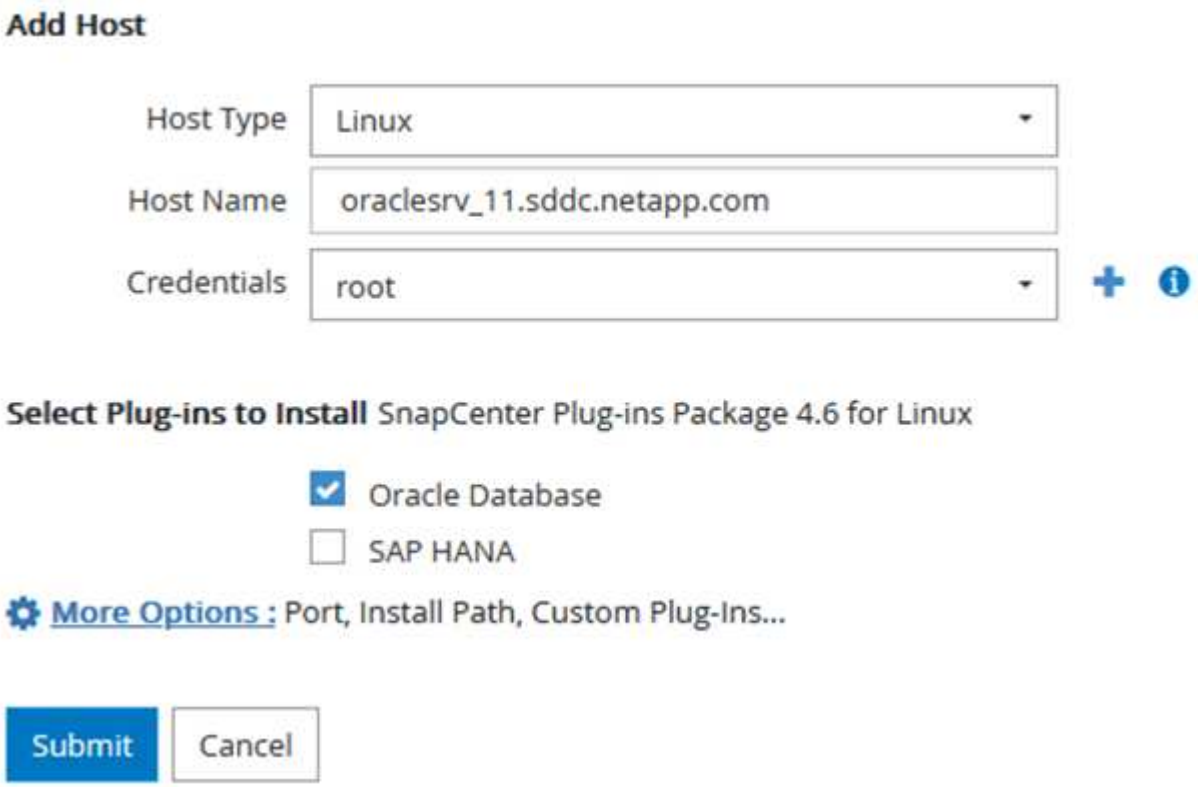
▼ **Ajouter des hôtes à SnapCenter**

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 Hôtes, puis cliquez sur Ajouter pour commencer 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.



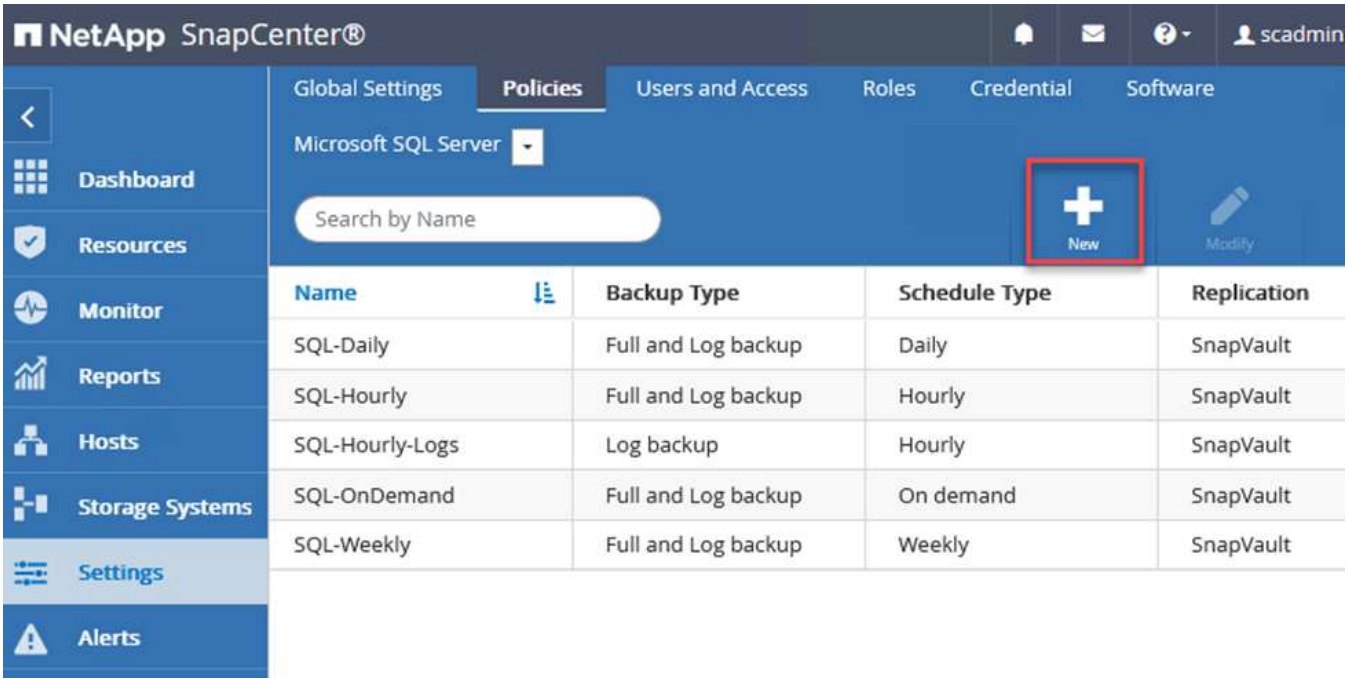
3. Pour Oracle, renseignez les champs obligatoires dans la boîte de dialogue « Ajouter un hôte » et cochez la case correspondant au plug-in Oracle Database. Cliquez ensuite sur « Soumettre » pour lancer le processus de découverte et ajouter l'hôte à SnapCenter.



▼ **Créer des politiques SnapCenter**

Les politiques établissent les règles spécifiques à suivre pour une tâche de sauvegarde. Ils incluent, sans toutefois s'y limiter, la planification de sauvegarde, le type de réplication et la manière dont SnapCenter gère la sauvegarde et la troncature des journaux de transactions.

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



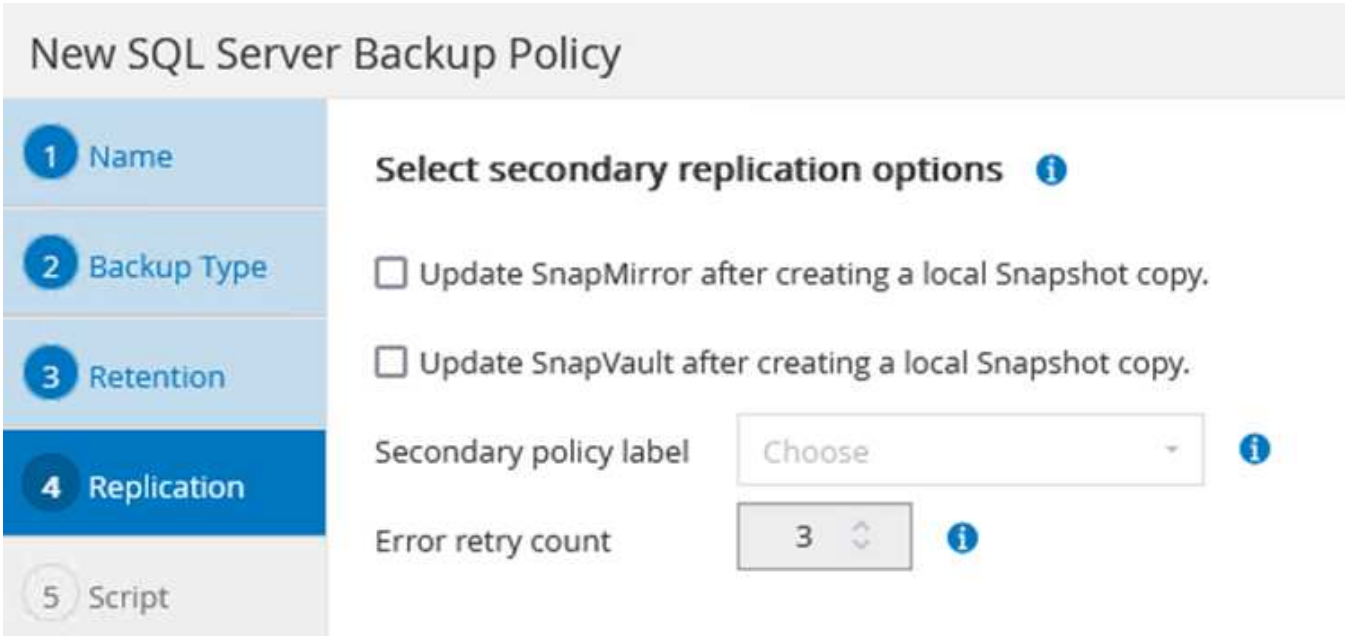
Pour obtenir des informations complètes sur la création de politiques pour les sauvegardes SQL Server, consultez le "Documentation de SnapCenter" .

Pour obtenir des informations complètes sur la création de politiques pour les sauvegardes Oracle, consultez le "Documentation de SnapCenter" .

Remarques :

- Au fur et à mesure que vous progressez dans l'assistant de création de stratégie, portez une attention particulière à la section Réplication. Dans cette section, vous indiquez 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 lorsque cette relation existe entre deux machines virtuelles de stockage résidant sur le même cluster.
- Le paramètre « Mettre à jour SnapVault après la création d'une copie SnapShot locale » est utilisé pour mettre à jour une relation SnapMirror qui existe entre deux clusters distincts et entre un système ONTAP sur site et Cloud Volumes ONTAP ou FSx ONTAP.

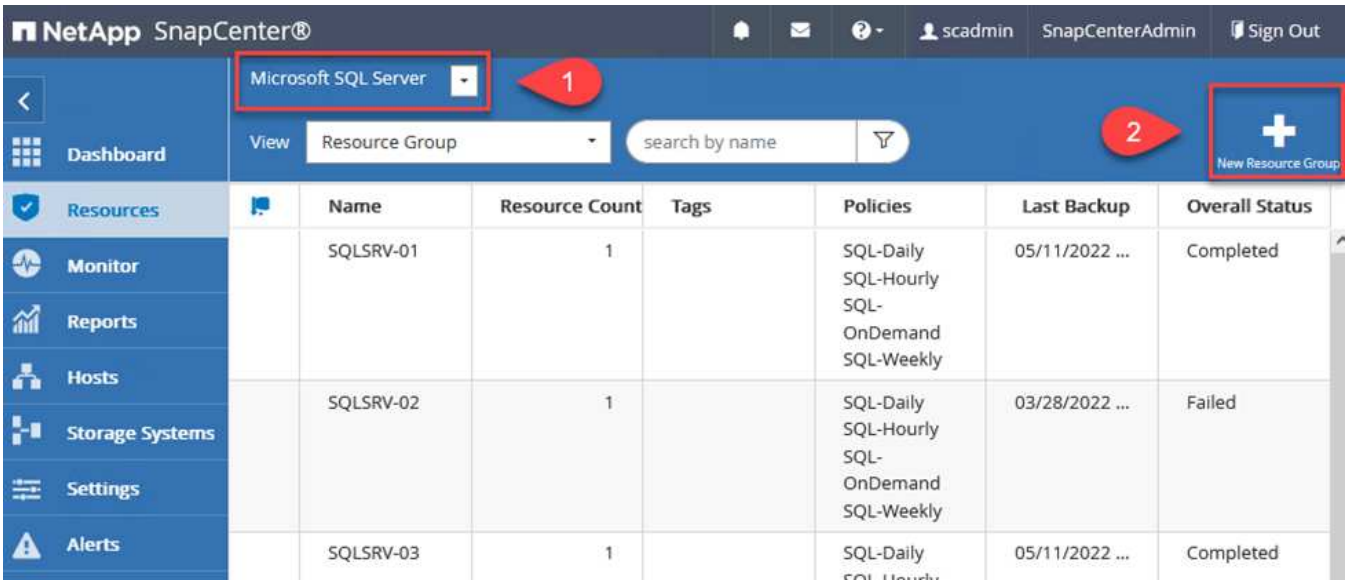
L'image suivante montre les options précédentes et leur apparence dans l'assistant de stratégie de sauvegarde.



▼ **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 politiques suivies pour ces ressources.

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



La documentation SnapCenter couvre les détails étape par étape pour la création de groupes de ressources pour les bases de données SQL Server et Oracle.

Pour sauvegarder les ressources SQL, suivez "ce lien" .

Pour sauvegarder les ressources Oracle, suivez "ce lien" .

Déployer et configurer Veeam Backup Server

Le logiciel Veeam Backup & Replication est utilisé dans la solution pour sauvegarder nos machines virtuelles d'application et archiver une copie des sauvegardes dans un compartiment Amazon S3 à l'aide d'un référentiel de sauvegarde évolutif Veeam (SOBR). Veeam est déployé sur un serveur Windows dans cette solution. Pour des conseils spécifiques sur le déploiement de Veeam, consultez le "Centre d'aide Veeam Documentation technique" .

▼ Configurer le référentiel de sauvegarde évolutif Veeam

Après avoir déployé et obtenu la licence du logiciel, vous pouvez créer un référentiel de sauvegarde évolutif (SOBR) comme stockage cible pour les tâches de sauvegarde. Vous devez également inclure un compartiment S3 comme sauvegarde des données de la machine virtuelle hors site pour la reprise après sinistre.

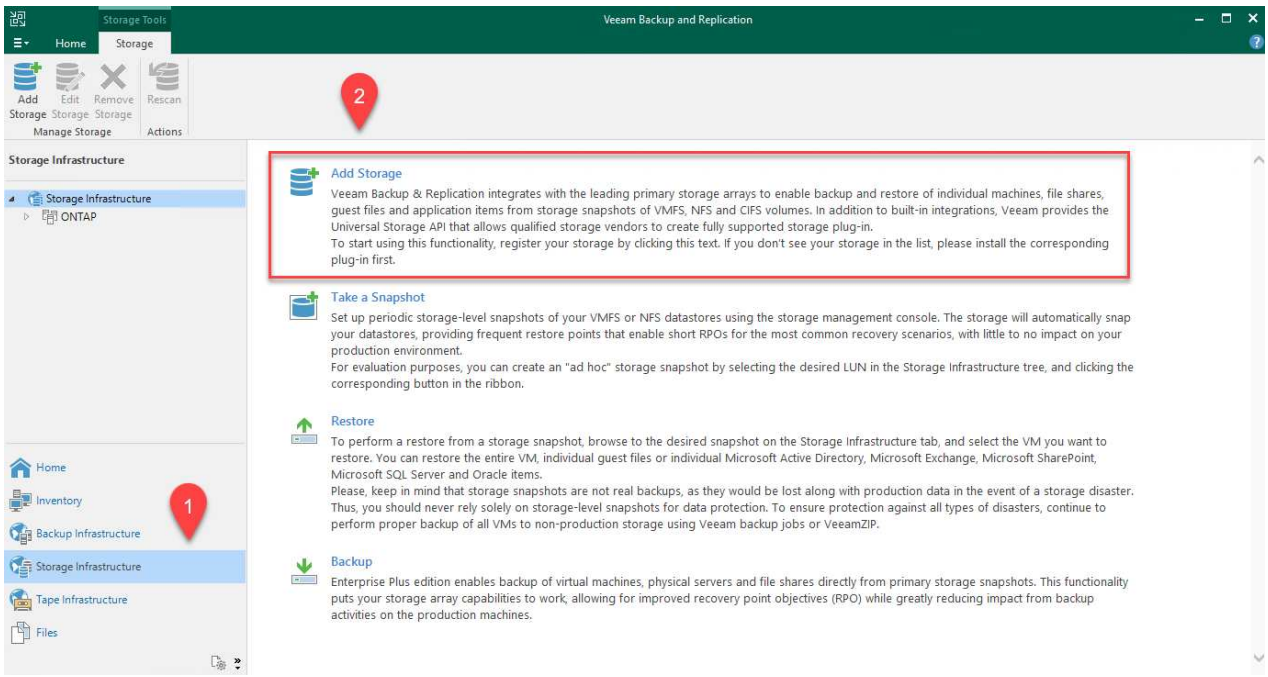
Consultez les prérequis suivants avant de commencer.

1. Créez un partage de fichiers SMB sur votre système ONTAP local comme stockage cible pour les sauvegardes.
2. Créez un bucket Amazon S3 à inclure dans le SOBR. Il s'agit d'un référentiel pour les sauvegardes hors site.

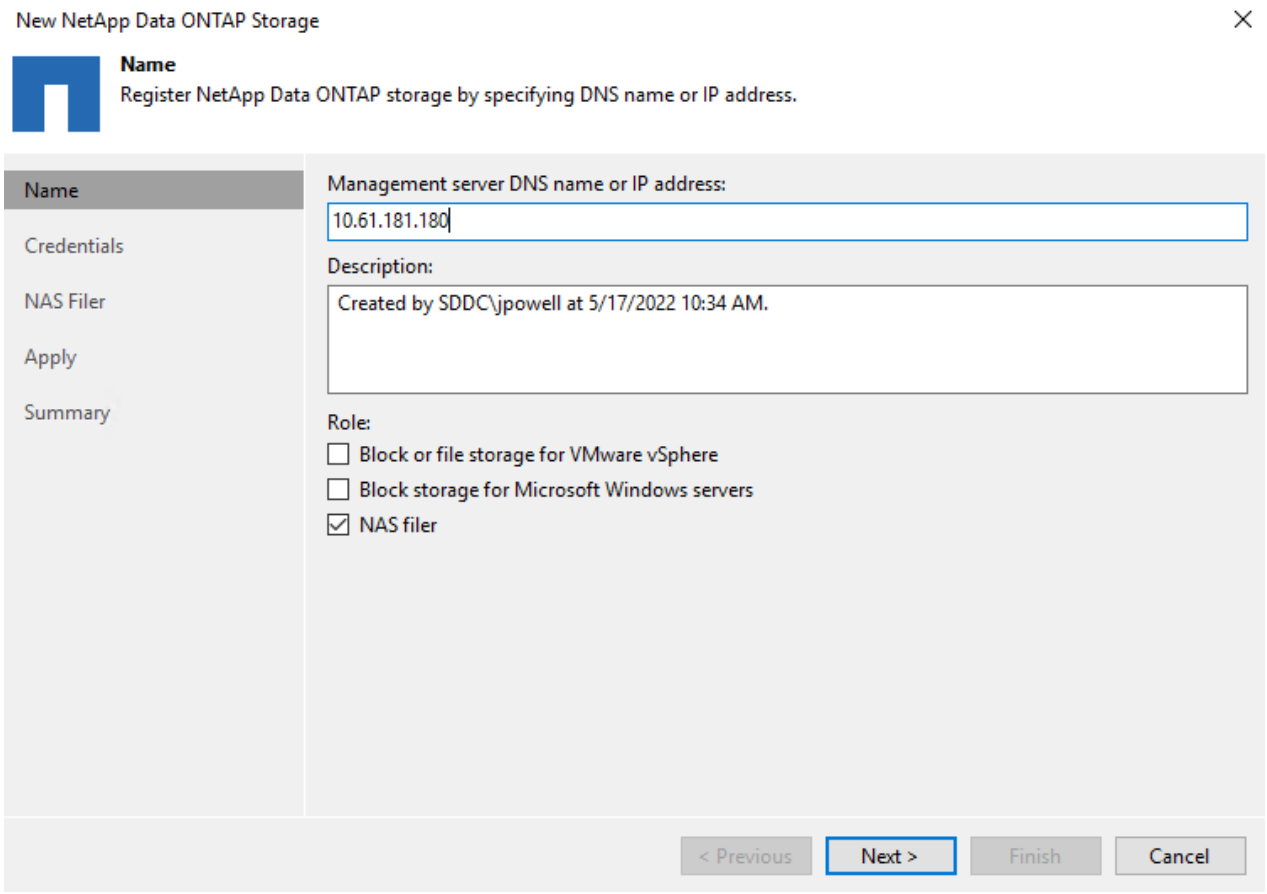
▼ Ajouter le stockage ONTAP à Veeam

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

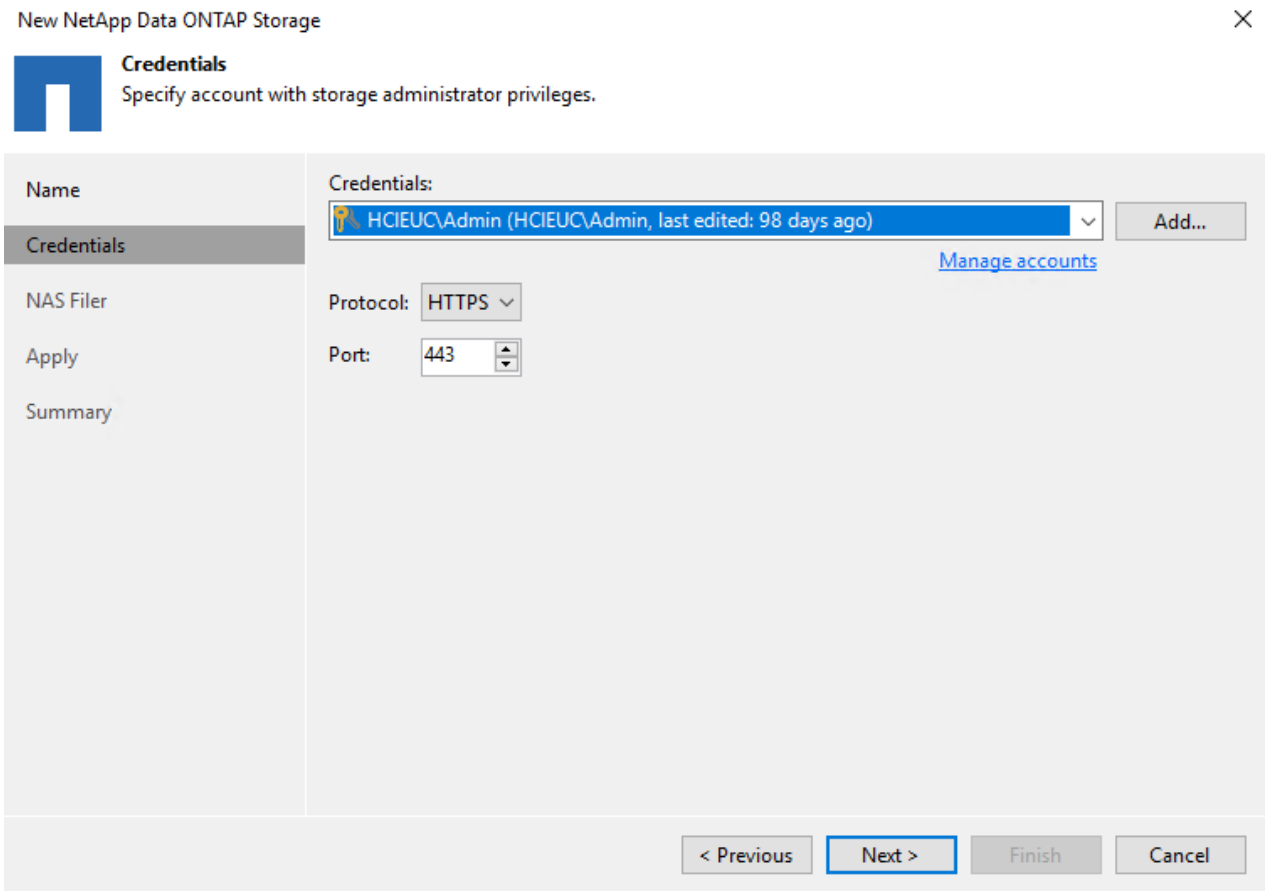
1. Ouvrez la console Veeam et connectez-vous. Accédez à Infrastructure de stockage, puis sélectionnez Ajouter un stockage.



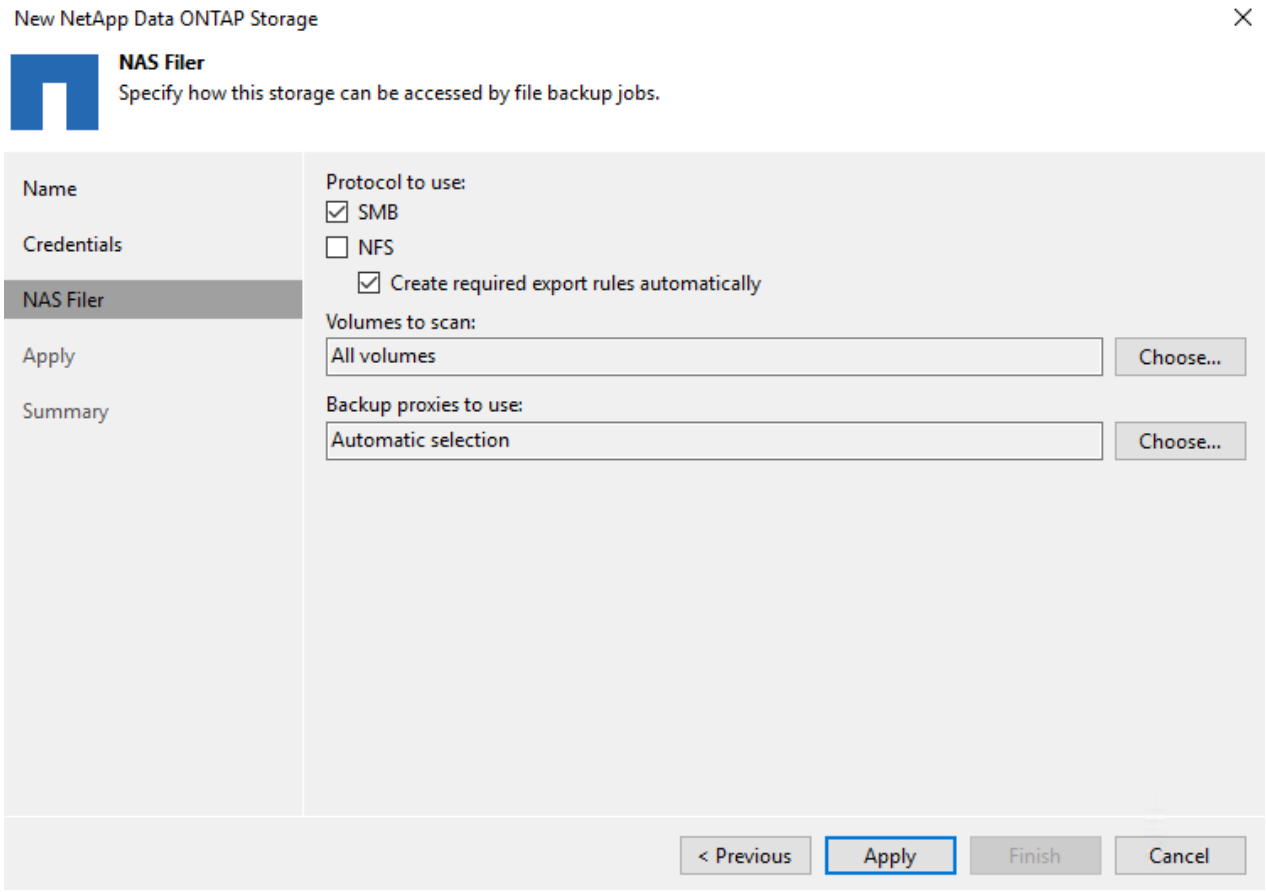
2. Dans l'assistant Ajouter un stockage, sélectionnez NetApp comme fournisseur de stockage, puis sélectionnez Data ONTAP.
3. Saisissez l'adresse IP de gestion et cochez la case NAS Filer. Cliquez sur Suivant.



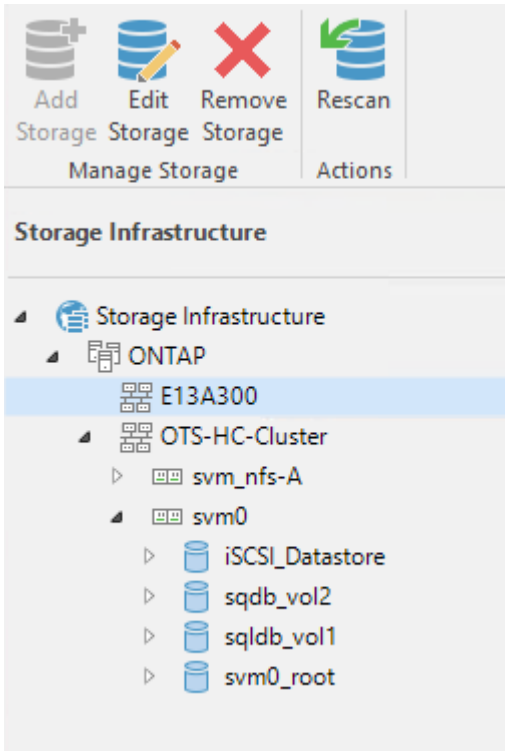
4. Ajoutez vos informations d'identification pour accéder au cluster ONTAP .



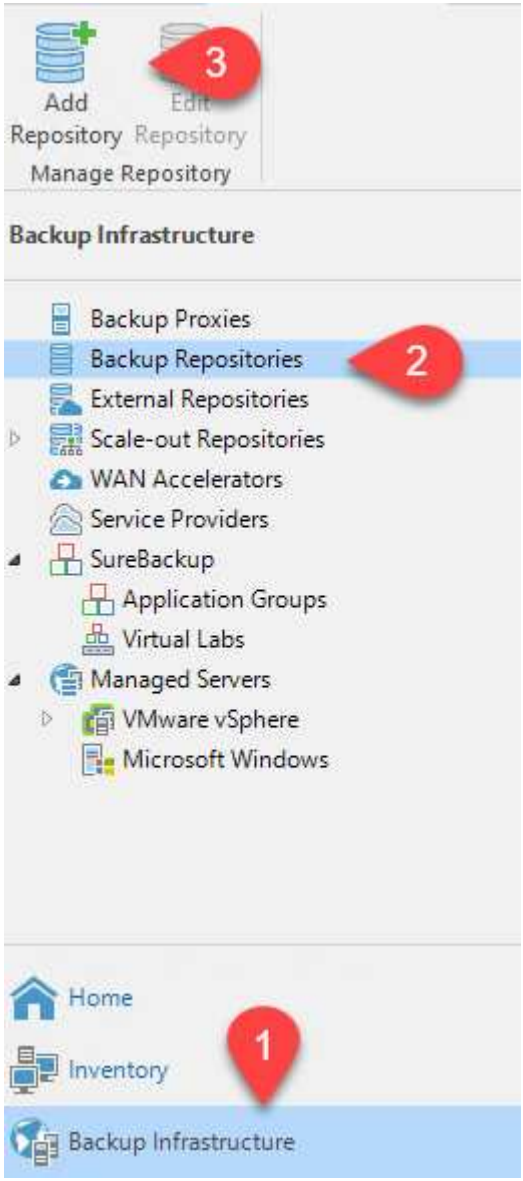
5. Sur la page NAS Filer, choisissez les protocoles souhaités à analyser et sélectionnez Suivant.



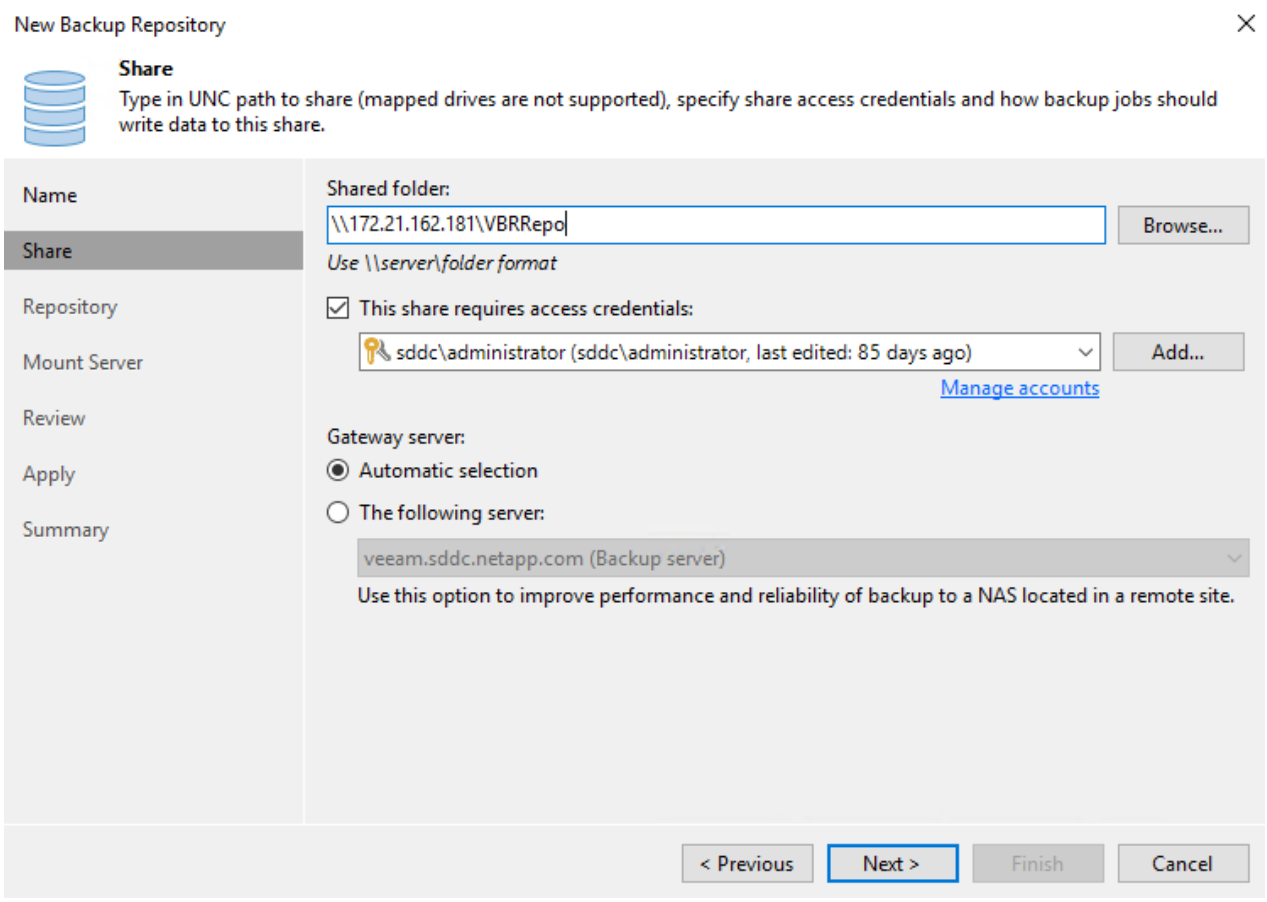
6. Remplissez les pages Appliquer et Résumé de l'assistant et cliquez sur Terminer pour commencer le processus de découverte de stockage. Une fois l'analyse terminée, le cluster ONTAP est ajouté avec les fichiers NAS en tant que ressources disponibles.



7. Créez un référentiel de sauvegarde à l'aide des partages NAS nouvellement découverts. Depuis l'infrastructure de sauvegarde, sélectionnez Référentiels de sauvegarde et cliquez sur l'élément de menu Ajouter un référentiel.



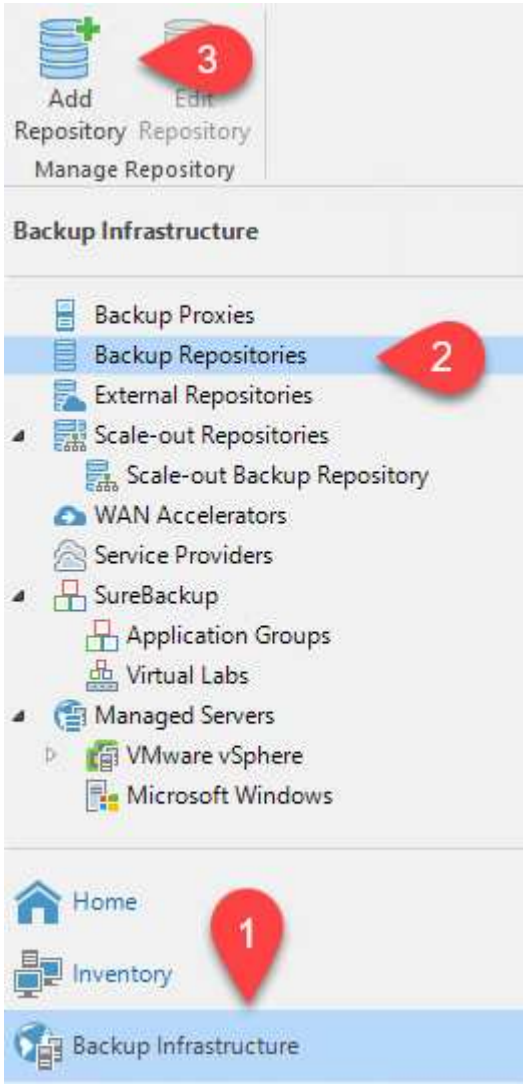
8. Suivez toutes les étapes de l'assistant Nouveau référentiel de sauvegarde pour créer le référentiel. Pour des informations détaillées sur la création de référentiels de sauvegarde Veeam, consultez le "Documentation Veeam" .



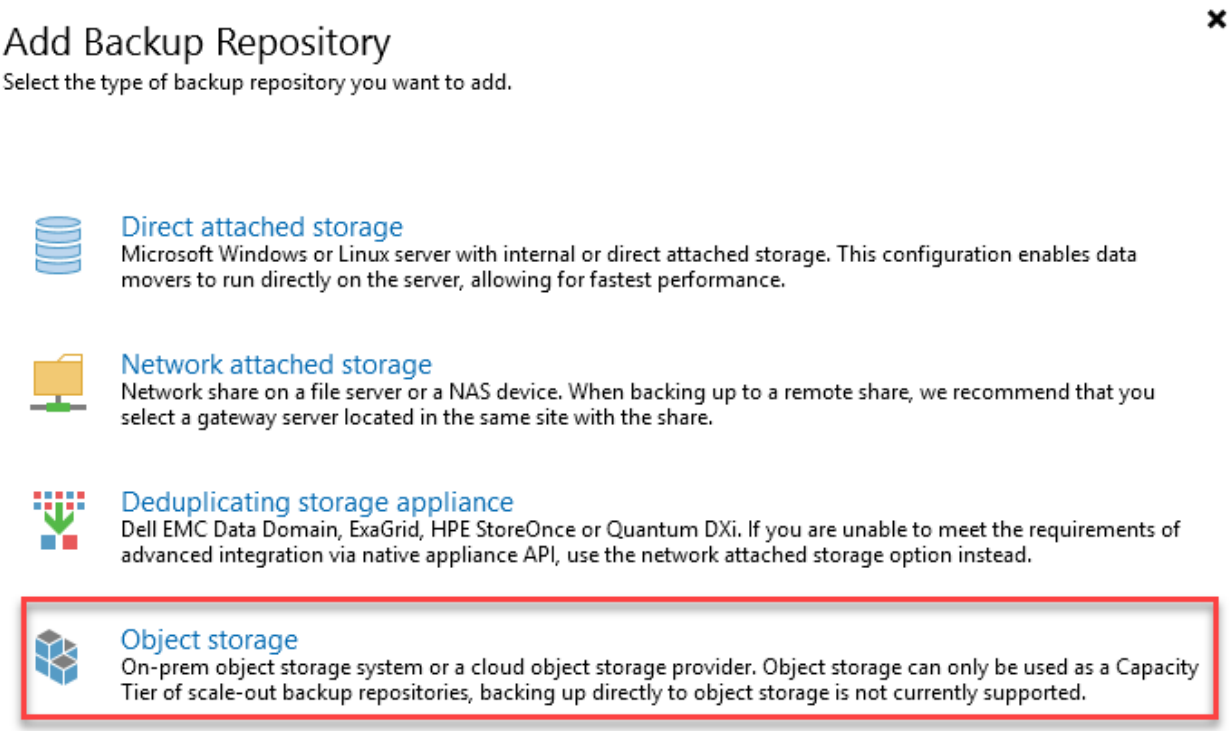
▼ **Ajouter le bucket Amazon S3 comme référentiel de sauvegarde**

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

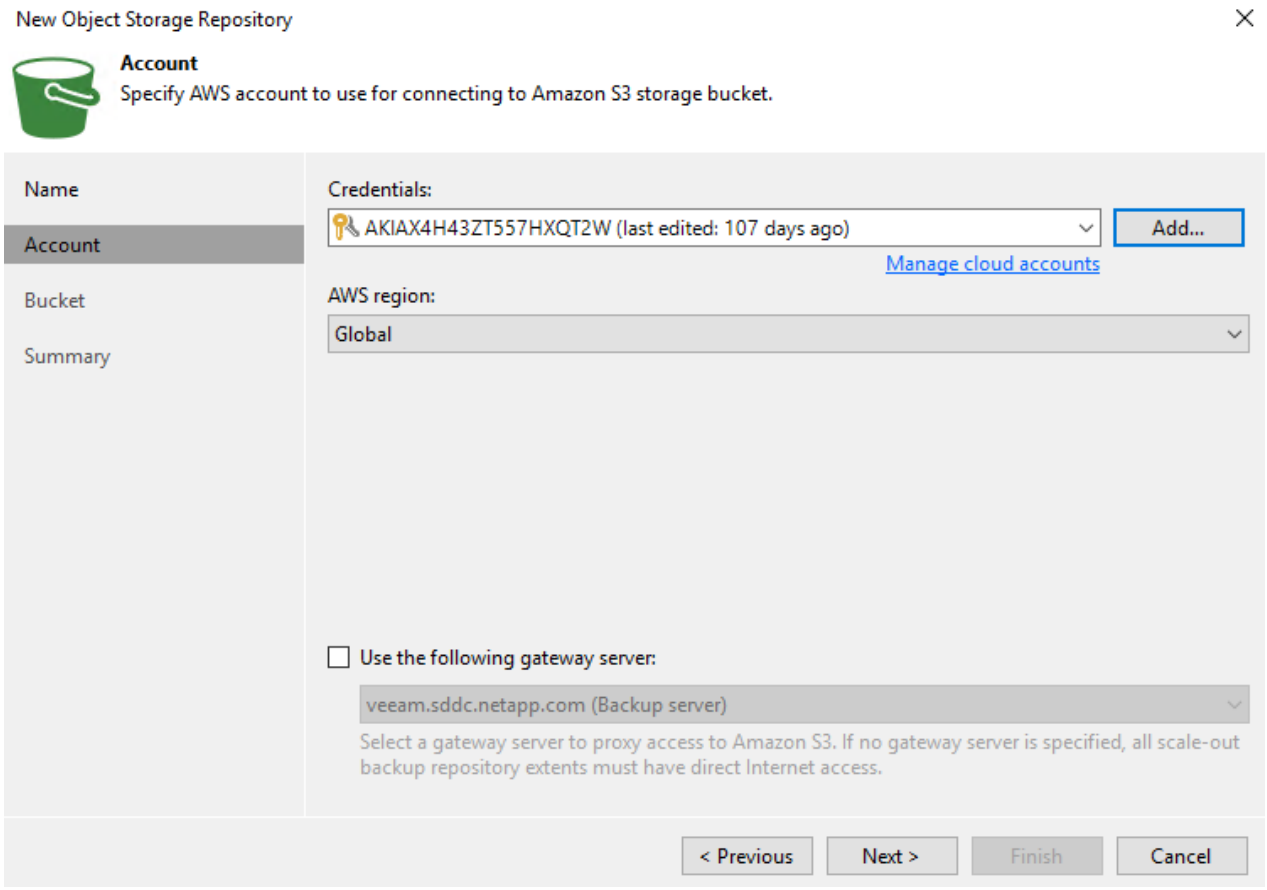
1. Accédez à Infrastructure de sauvegarde > Référentiels de sauvegarde. Cliquez sur Ajouter un référentiel.



2. Dans l'assistant Ajouter un référentiel de sauvegarde, sélectionnez Stockage d'objets, puis Amazon S3. Cela démarre l'assistant Nouveau référentiel de stockage d'objets.



3. Donnez un nom à votre référentiel de stockage d'objets et cliquez sur Suivant.
4. Dans la section suivante, indiquez vos informations d'identification. Vous avez besoin d'une clé d'accès AWS et d'une clé secrète.

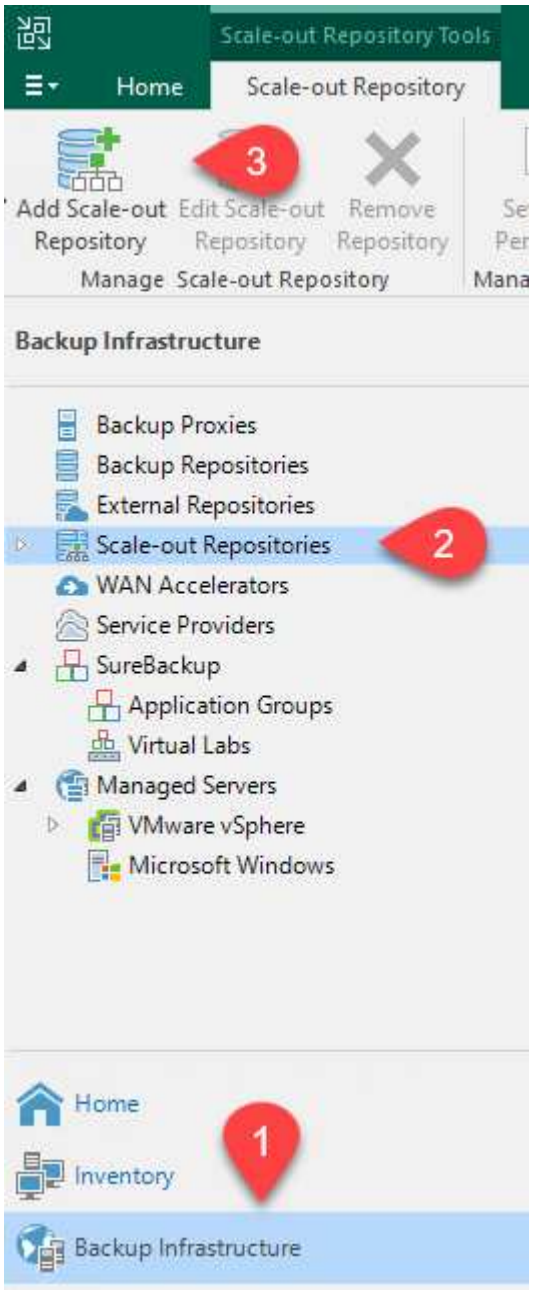


5. Une fois la configuration Amazon chargée, choisissez votre centre de données, votre bucket et votre dossier, puis cliquez sur Appliquer. Enfin, cliquez sur Terminer pour fermer l'assistant.

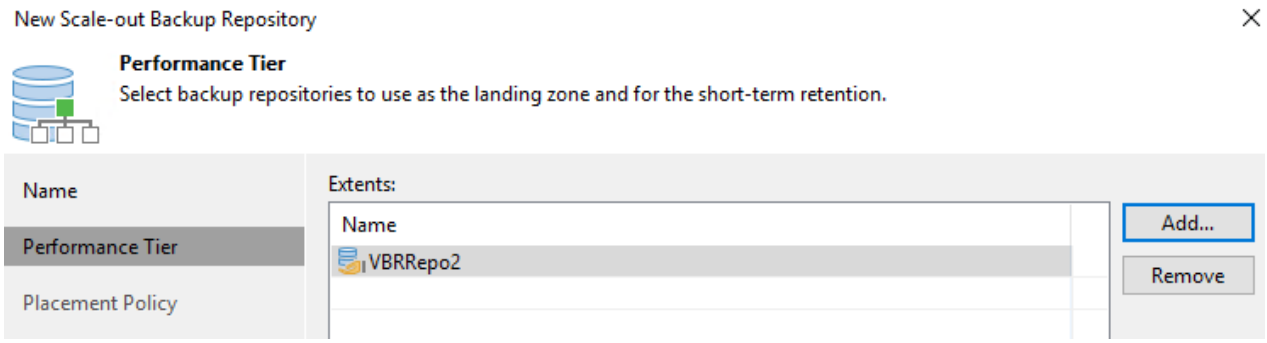
▼ **Créer un référentiel de sauvegarde évolutif**

Maintenant que nous avons ajouté nos référentiels de stockage à Veeam, nous pouvons créer le SOBR pour hiérarchiser automatiquement les copies de sauvegarde vers notre stockage d'objets Amazon S3 hors site pour la reprise après sinistre.

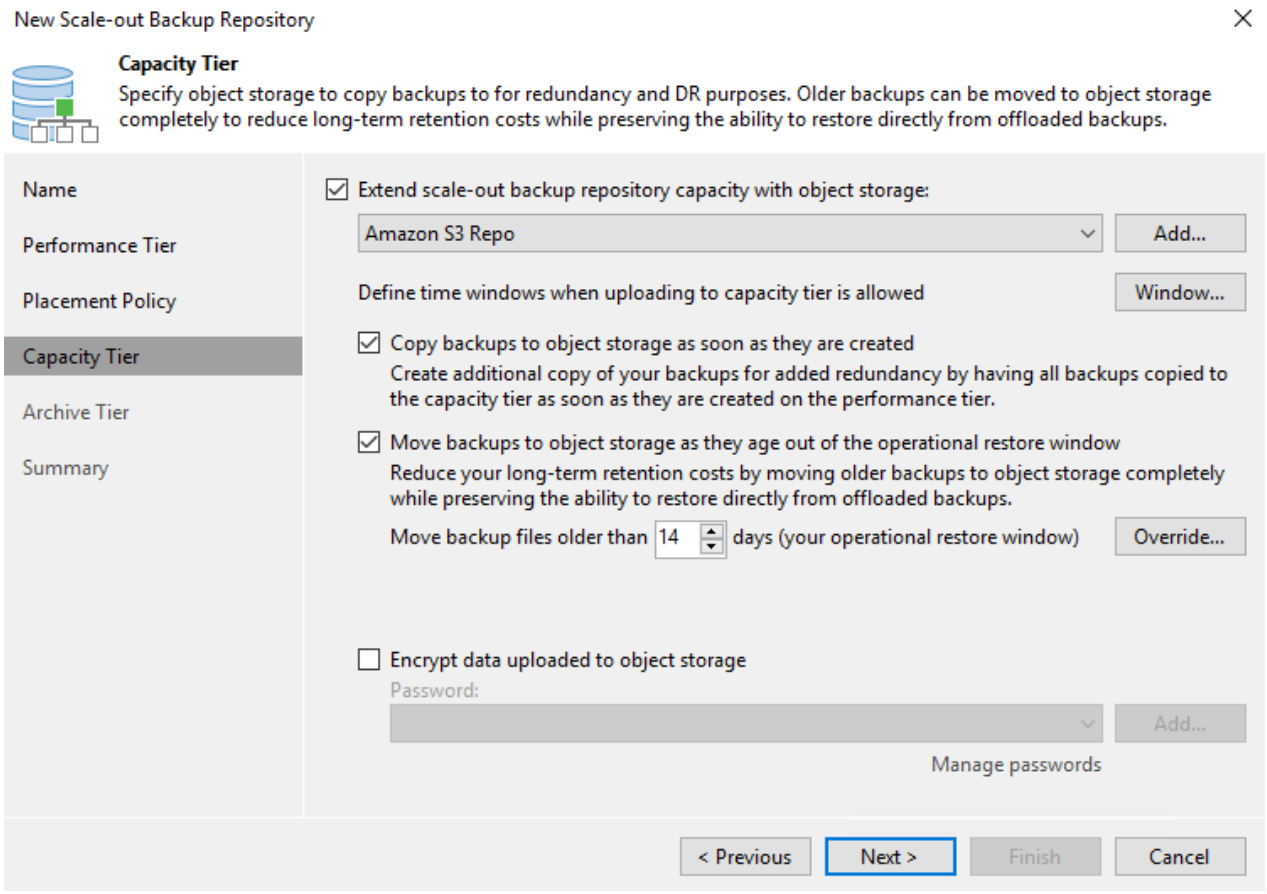
1. Depuis l'infrastructure de sauvegarde, sélectionnez Référentiels évolutifs, puis cliquez sur l'élément de menu Ajouter un référentiel évolutif.



2. Dans le nouveau référentiel de sauvegarde évolutive, indiquez un nom pour le SOBR et cliquez sur Suivant.
3. Pour le niveau de performance, choisissez le référentiel de sauvegarde qui contient le partage SMB résidant sur votre cluster ONTAP local.



4. Pour la politique de placement, choisissez la localité des données ou les performances en fonction de vos besoins. Sélectionnez suivant.
5. Pour le niveau de capacité, nous étendons le SOBR avec le stockage d'objets Amazon S3. À des fins de reprise après sinistre, sélectionnez Copier les sauvegardes vers le stockage d'objets dès leur création pour garantir la livraison rapide de nos sauvegardes secondaires.



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

▼ Créer les tâches de référentiel de sauvegarde évolutive

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

NetApp Backup and Recovery outils et configuration

Pour effectuer un basculement des machines virtuelles d'application et des volumes de base de données vers les services VMware Cloud Volume exécutés dans AWS, vous devez installer et configurer une instance en cours d'exécution de SnapCenter Server et de 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 qu'un retour arrière vers le centre de données sur site soit planifié et exécuté.

▼ **Déployer un serveur Windows SnapCenter secondaire**

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

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

Vous pouvez trouver le SnapCenter software sur "ce lien" .

▼ **Configurer le serveur Windows SnapCenter secondaire**

Pour effectuer une restauration des données d'application mises en miroir sur FSx ONTAP, vous devez d'abord effectuer une restauration complète de la base de données SnapCenter locale. Une fois ce processus terminé, la communication avec les machines virtuelles est rétablie et les sauvegardes d'applications peuvent désormais reprendre en utilisant FSx ONTAP comme stockage principal.

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 à celui du serveur SnapCenter local d'origine.
2. Configurez la mise en réseau pour communiquer avec VMware Cloud et l'instance FSx ONTAP .
3. Terminez la procédure pour restaurer la base de données SnapCenter .
4. Confirmez que SnapCenter est en mode de récupération après sinistre pour vous assurer que FSx est désormais le stockage principal pour les sauvegardes.
5. Confirmez que la communication est rétablie avec les machines virtuelles restaurées.

▼ **Déployer un serveur Veeam Backup & Replication secondaire**

Vous pouvez installer le serveur Veeam Backup & Replication sur un serveur Windows dans VMware Cloud sur AWS ou sur une instance EC2. Pour des conseils de mise en œuvre détaillés, consultez le "Documentation technique du centre d'aide Veeam" .

▼ **Configurer un serveur secondaire Veeam Backup & Replication**

Pour effectuer une restauration de machines virtuelles qui ont été sauvegardées sur le stockage Amazon S3, vous devez installer le serveur Veeam sur un serveur Windows et le configurer pour communiquer avec VMware Cloud, FSx ONTAP et le bucket S3 qui contient le référentiel de sauvegarde d'origine. Il doit également disposer d'un nouveau référentiel de sauvegarde configuré sur FSx ONTAP pour effectuer de nouvelles sauvegardes des machines virtuelles après leur restauration.

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

1. Configurez la mise en réseau pour communiquer avec VMware Cloud, FSx ONTAP et le bucket S3 contenant le référentiel de sauvegarde d'origine.
2. Configurez un partage SMB sur FSx ONTAP pour qu'il devienne un nouveau référentiel de sauvegarde.
3. Montez le bucket S3 d'origine qui a été utilisé dans le cadre du référentiel de sauvegarde évolutif sur site.

4. Après avoir restauré la machine virtuelle, établissez de nouvelles tâches de sauvegarde pour protéger les machines virtuelles SQL et Oracle.

Pour plus d'informations sur la restauration de machines virtuelles à l'aide de Veeam, consultez la section"Restaurer les machines virtuelles d'application avec Veeam Full Restore" .

Sauvegarde de la base de données SnapCenter pour la reprise après sinistre

SnapCenter permet la sauvegarde et la récupération de sa base de données MySQL sous-jacente et de ses données de configuration dans le but de récupérer le serveur SnapCenter en cas de sinistre. Pour notre solution, nous avons récupéré la base de données et la configuration SnapCenter sur une instance AWS EC2 résidant dans notre VPC. Pour plus d'informations sur la reprise après sinistre de SnapCenter, consultez "ce lien" .

▼ **Conditions préalables à la sauvegarde de SnapCenter**

Les conditions préalables suivantes sont requises pour la sauvegarde SnapCenter :

- Un volume et un partage SMB créés sur le système ONTAP local pour localiser la base de données sauvegardée et les fichiers de configuration.
- Une relation SnapMirror entre le système ONTAP sur site et FSx ou CVO dans le compte AWS. Cette relation est utilisée pour transporter 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 machine virtuelle dans le SDDC VMware Cloud.
- SnapCenter installé sur l'instance Windows EC2 ou la machine virtuelle dans VMware Cloud.

▼ **Résumé du processus de sauvegarde et de restauration de SnapCenter**

- Créez un volume sur le système ONTAP local pour héberger la base de données de sauvegarde et les fichiers de configuration.
- Configurez une relation SnapMirror entre le système local et FSx/CVO.
- Montez le partage SMB.
- Récupérez le jeton d'autorisation 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 de la base de données et du fichier de configuration sur le partage SMB.
- Sur FSx, créez un clone du volume ONTAP (copié via SnapMirror à partir du site).
- Montez le partage SMB de FSx vers EC2/VMware Cloud.
- Copiez le répertoire de restauration du partage SMB vers un répertoire local.
- Exécutez le processus de restauration de SQL Server à partir de Swagger.

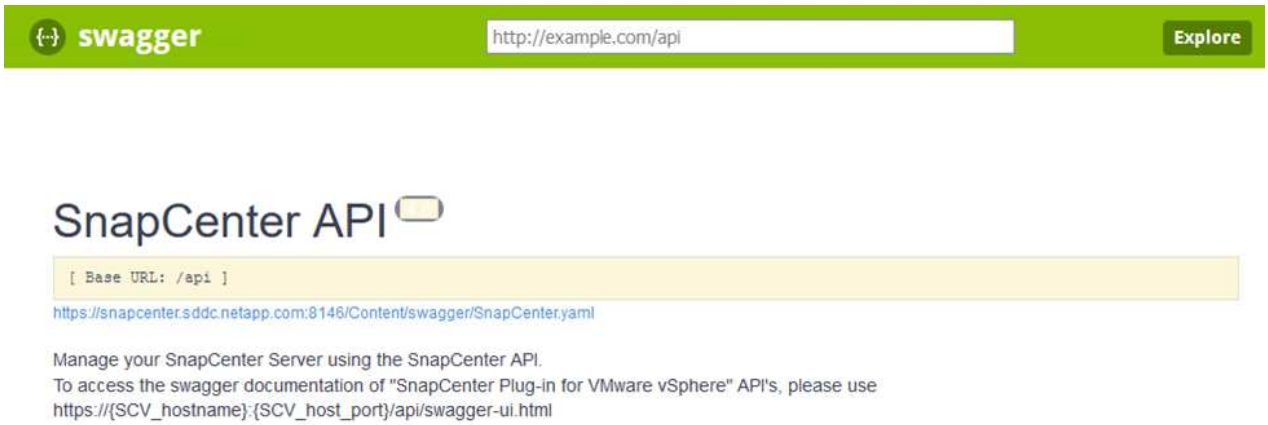
▼ **Sauvegarder la base de données et la configuration de SnapCenter**

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

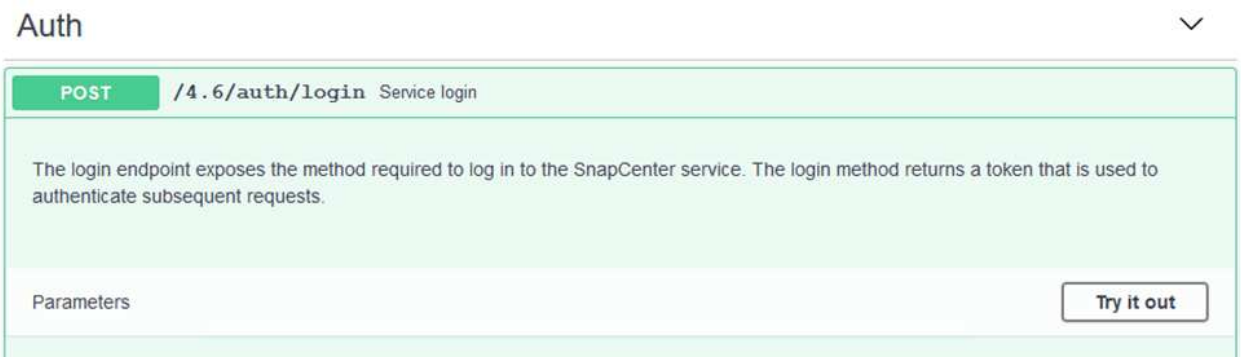
▼ **Connectez-vous à Swagger et obtenez un jeton d'autorisation**

Après avoir accédé à la page Swagger, vous devez récupérer un jeton d'autorisation pour lancer le processus de restauration de la base de données.

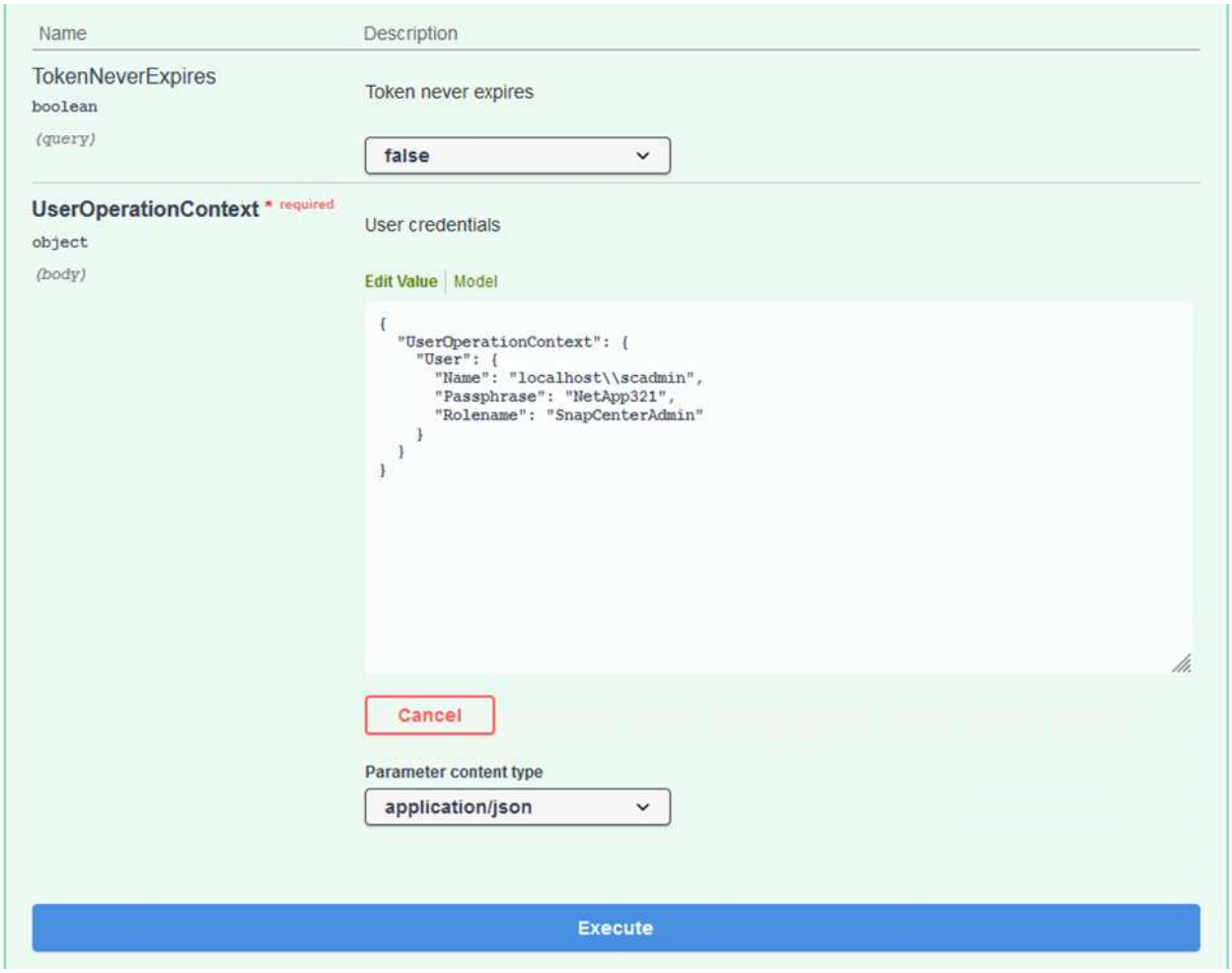
1. Accédez à la page Web de l'API SnapCenter Swagger à l'adresse *https://< IP du serveur SnapCenter >:8146/swagger/*.



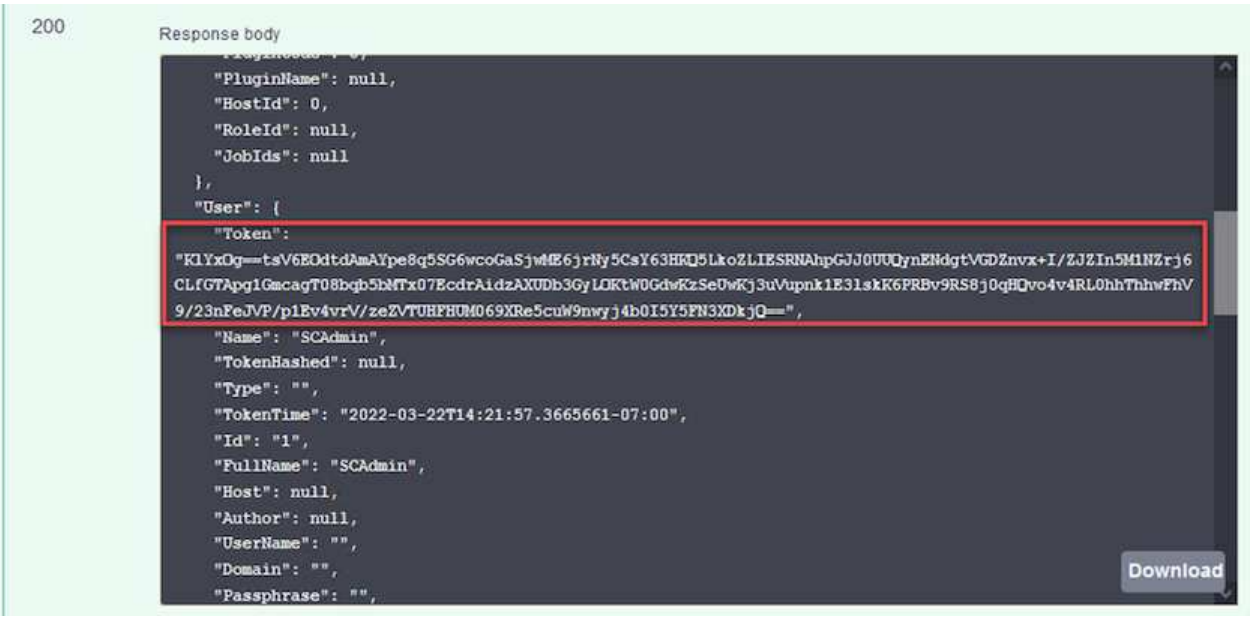
2. Développez la section Authentification et cliquez sur Essayer.



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



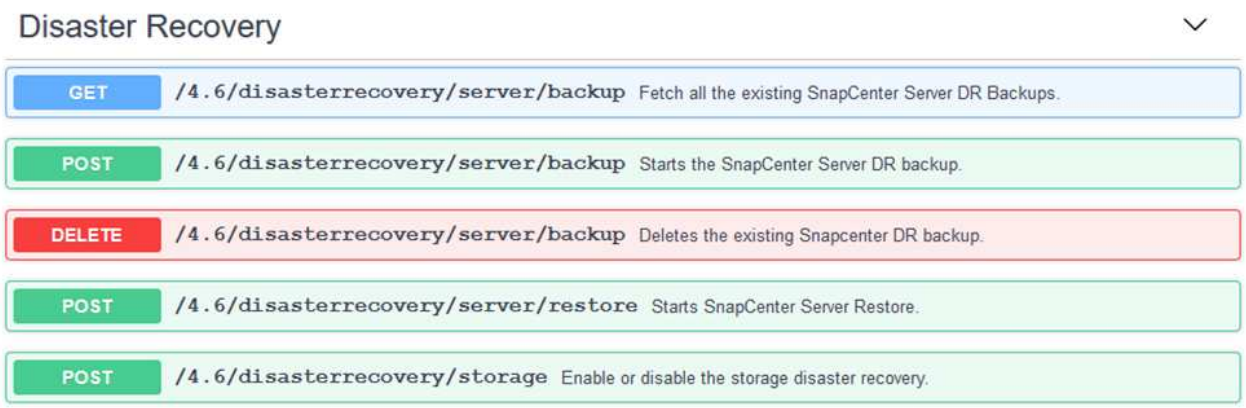
4. Dans le corps de la réponse ci-dessous, vous pouvez voir le jeton. Copiez le texte du jeton pour l'authentification lors de l'exécution du processus de sauvegarde.



▼ **Effectuer une sauvegarde de la base de données SnapCenter**

Accédez ensuite à la zone de récupération après sinistre sur la page Swagger pour commencer le processus de sauvegarde de SnapCenter .

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

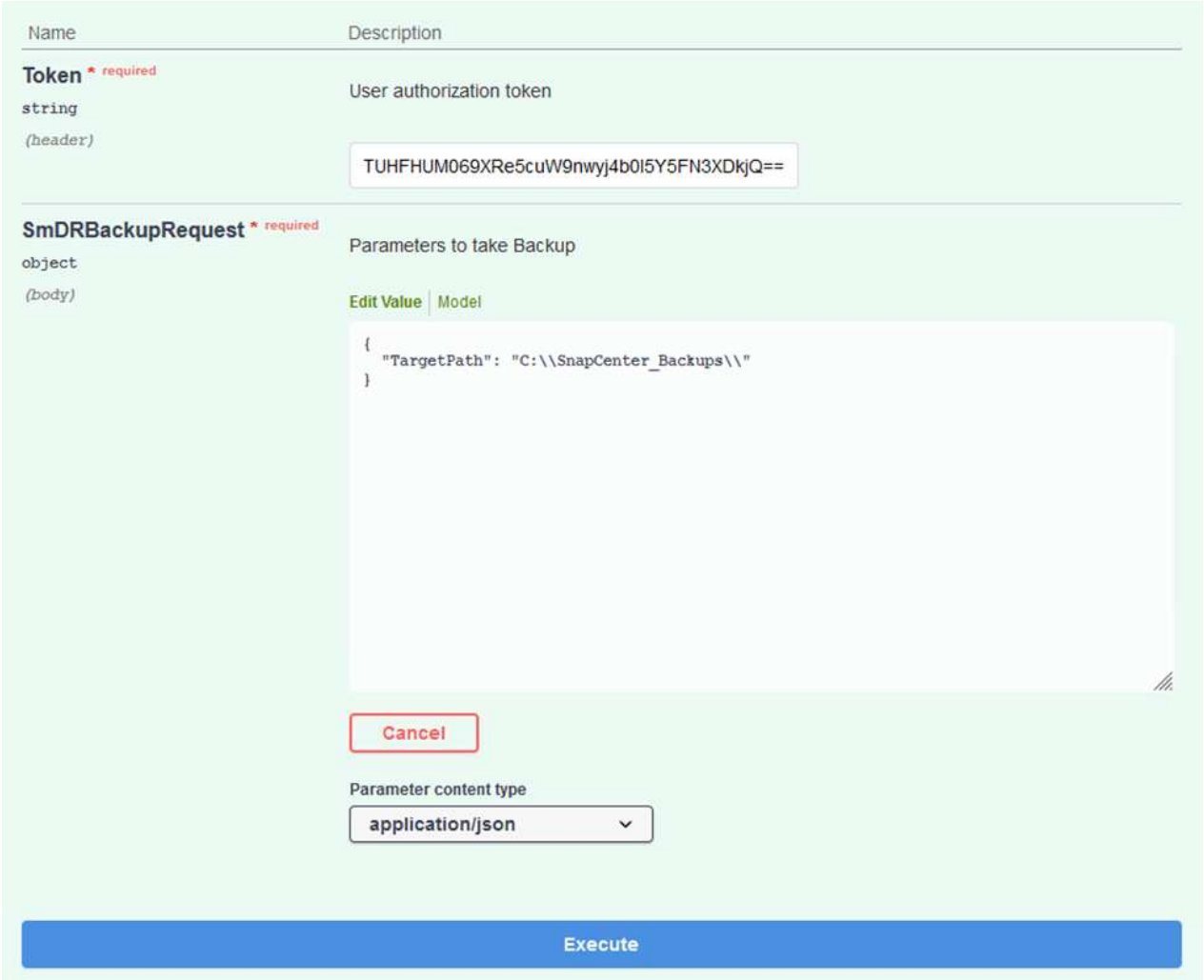


2. Développer le `/4.6/disasterrecovery/server/backup` section et cliquez sur Essayer.



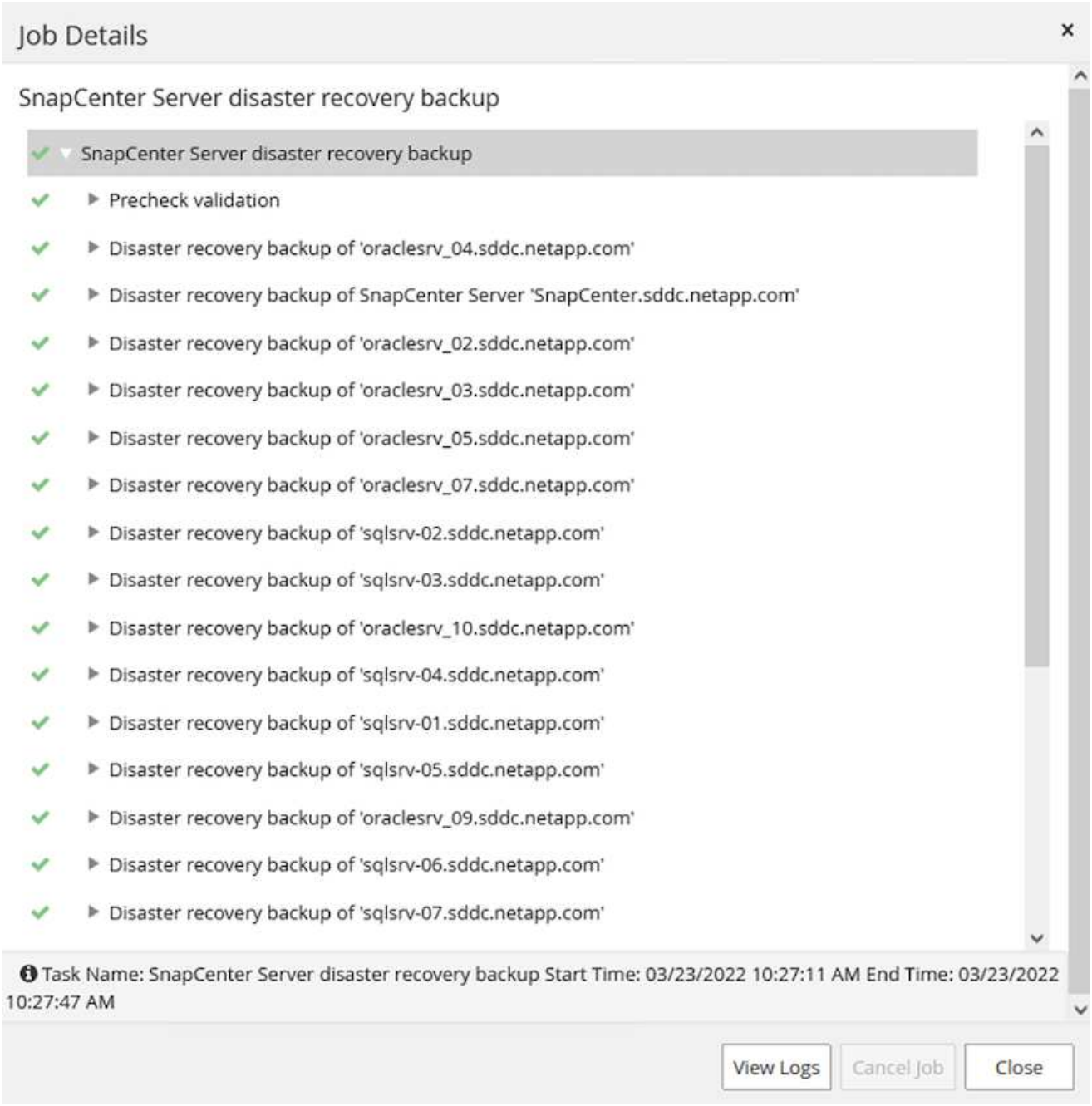
3. Dans la section SmDRBackupRequest, ajoutez le chemin cible local correct et sélectionnez Exécuter pour démarrer la sauvegarde de la base de données et de la configuration SnapCenter .

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



▼ **Surveiller la tâche de sauvegarde depuis SnapCenter**

Connectez-vous à SnapCenter pour consulter les fichiers journaux lors du démarrage du processus de restauration de la base de données. Dans la section Moniteur, vous pouvez afficher les détails de la sauvegarde de récupération après sinistre du serveur SnapCenter .



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

Ensuite, vous devez déplacer la sauvegarde du lecteur local sur le serveur SnapCenter vers le partage CIFS utilisé pour copier les données SnapMirror vers l'emplacement secondaire situé sur l'instance FSx dans AWS. Utilisez xcopy avec des options spécifiques qui conservent les autorisations des fichiers.

Ouvrez une invite de commande en tant qu'administrateur. À partir de 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

▼ Une catastrophe se produit sur le site principal

En cas de sinistre survenant dans le centre de données 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 supposons que les machines virtuelles et notre cluster ONTAP sur site ne sont plus accessibles. De plus, les machines virtuelles SnapCenter et Veeam ne sont plus accessibles et doivent être reconstruites sur notre site secondaire.

Cette section aborde le basculement de notre infrastructure vers le cloud et nous abordons les sujets suivants :

- Restauration de la base de données SnapCenter . Une fois qu'un nouveau serveur SnapCenter a été établi, restaurez la base de données MySQL et les fichiers de configuration et basculez la base de données en mode de récupération après sinistre afin de permettre au stockage FSx secondaire de devenir le périphérique de stockage principal.
- Restaurez les machines virtuelles d'application à l'aide de Veeam Backup & Replication. Connectez le stockage S3 qui contient les sauvegardes de machines virtuelles, importez les sauvegardes et restaurez-les sur VMware Cloud sur AWS.
- Restaurez les données de l'application SQL Server à l'aide de SnapCenter.
- Restaurez les données de l'application Oracle à l'aide de SnapCenter.

▼ Processus de restauration de la base de données SnapCenter

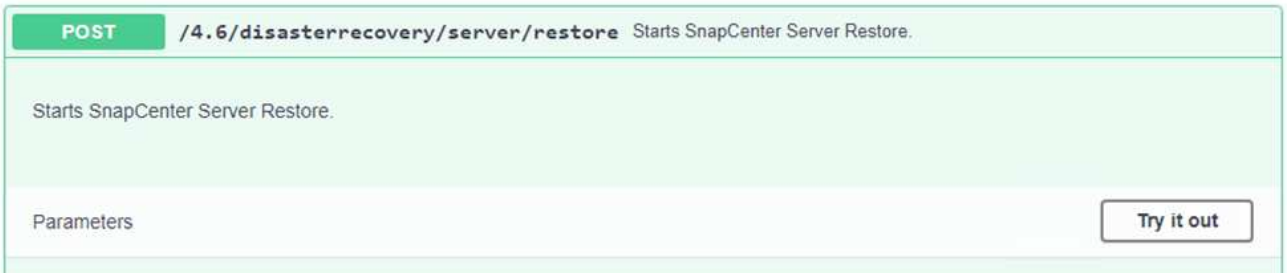
SnapCenter prend en charge les scénarios de reprise après sinistre en permettant la sauvegarde et la restauration de sa base de données MySQL et de ses fichiers de configuration. Cela permet à un administrateur de conserver des sauvegardes régulières de la base de données SnapCenter dans le centre de données local et de restaurer ultérieurement cette base de données dans une base de données SnapCenter secondaire.

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

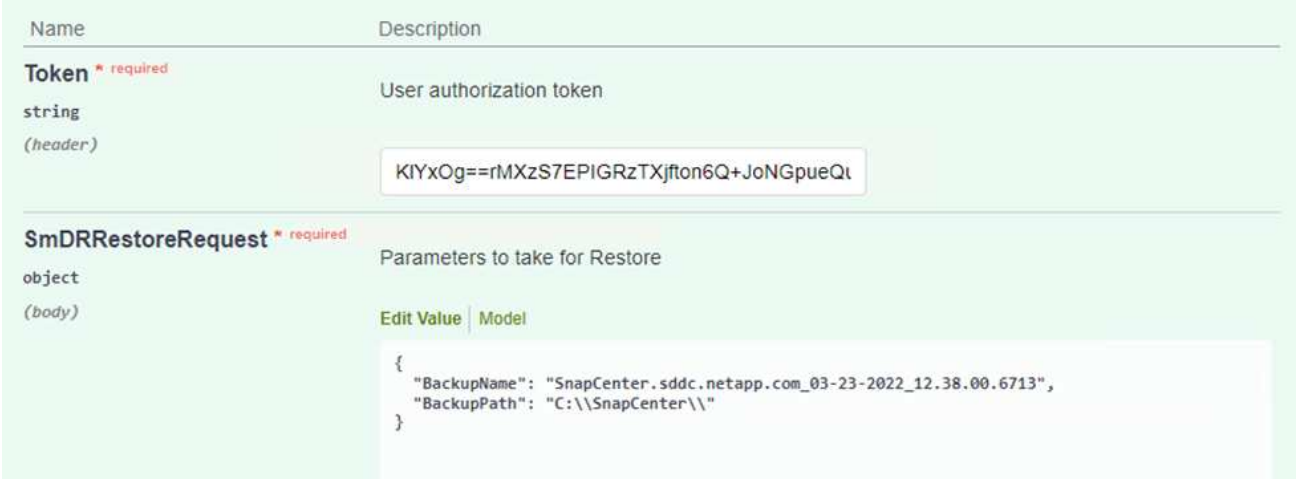
1. Rompre la relation SnapMirror du cluster FSx, ce qui rend le volume en lecture/écriture.
2. Créez un serveur CIFS (si nécessaire) et créez un partage CIFS pointant vers le chemin de jonction du volume cloné.
3. Utilisez xcopy pour copier les fichiers de sauvegarde dans un répertoire local sur le système SnapCenter secondaire.
4. Installez SnapCenter v4.6.
5. Assurez-vous que le serveur SnapCenter possède le même nom de domaine complet que le serveur d'origine. Ceci est nécessaire pour que la restauration de la base de données réussisse.

Pour démarrer le processus de restauration, procédez comme suit :

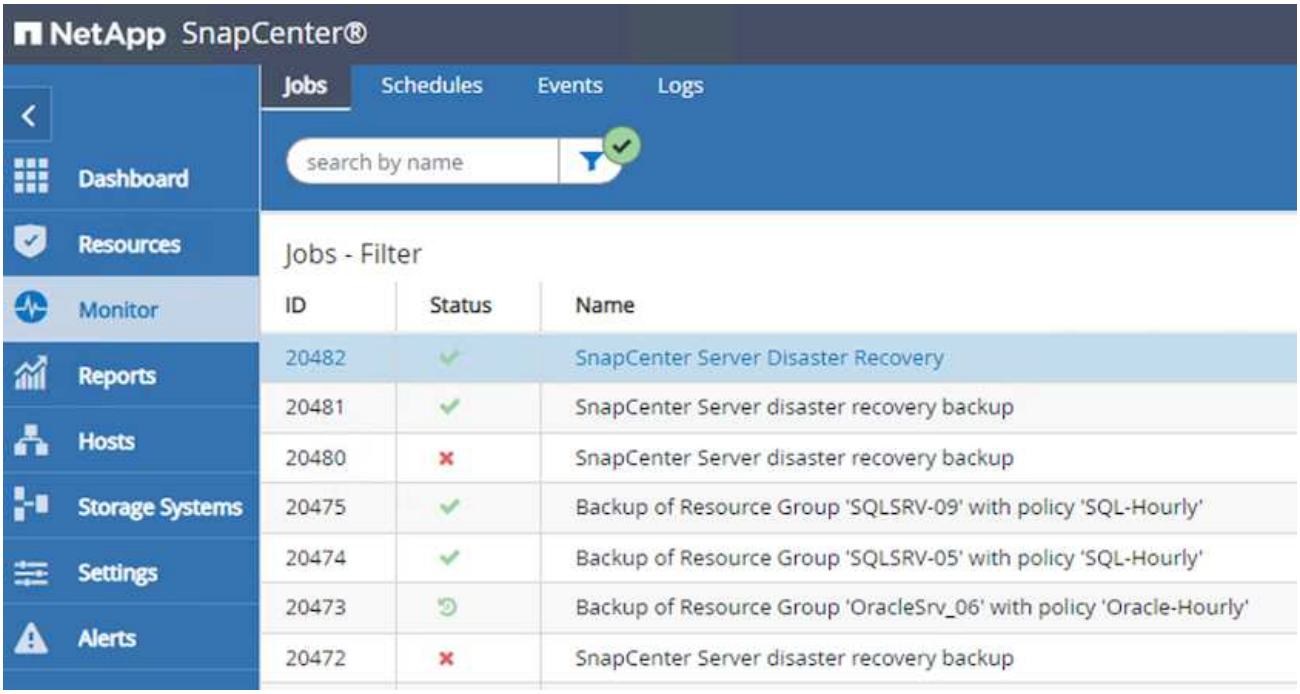
1. Accédez à la page Web de l'API Swagger pour le serveur SnapCenter secondaire et suivez les instructions précédentes pour obtenir un jeton d'autorisation.
2. Accédez à la section Reprise après sinistre de la page Swagger, sélectionnez `/4.6/disasterrecovery/server/restore` , et cliquez sur Essayer.

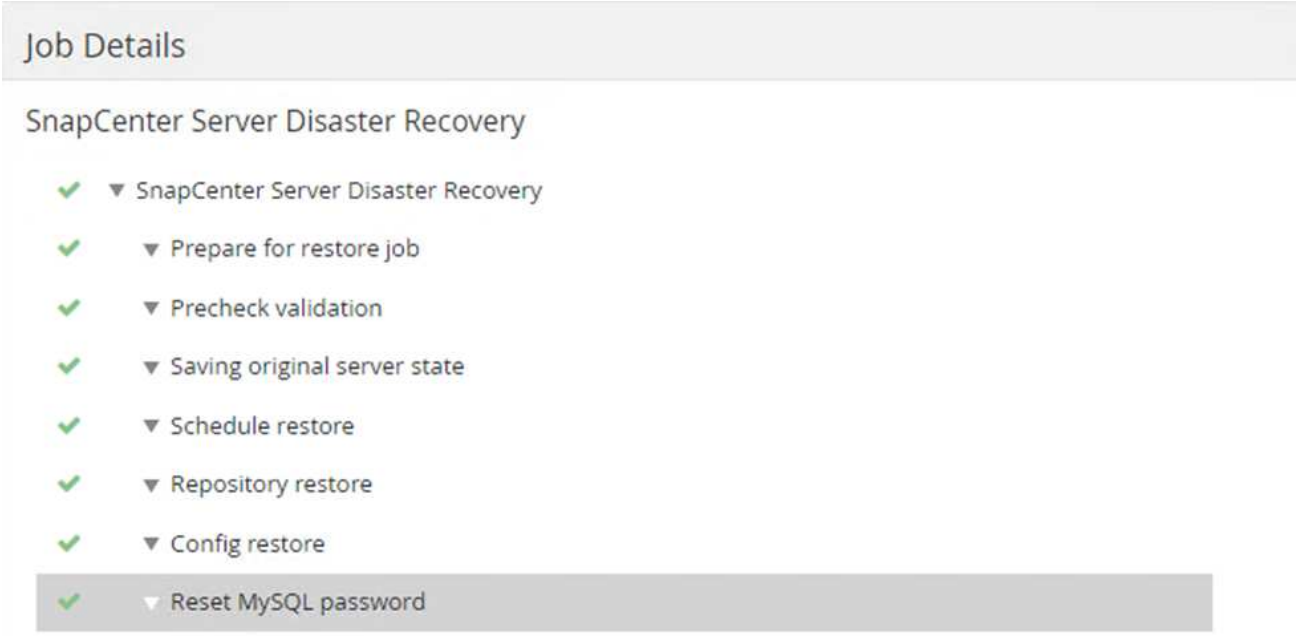


3. Collez votre jeton d'autorisation et, dans la section SmDRResterRequest, collez le nom de la sauvegarde et le répertoire local sur le serveur SnapCenter secondaire.



4. Sélectionnez le bouton Exécuter pour démarrer le processus de restauration.
5. Depuis SnapCenter, accédez à la section Surveiller pour afficher la progression de la tâche de restauration.





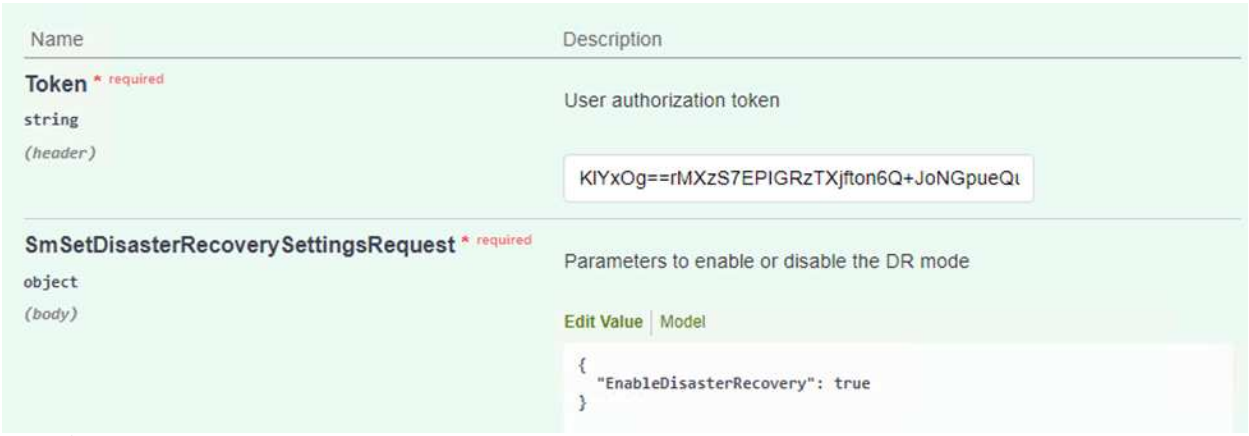
6. Pour activer les restaurations SQL Server à partir du stockage secondaire, vous devez basculer la base de données SnapCenter en mode de récupération après sinistre. Cette opération est effectuée comme une opération distincte et initiée sur la page Web de l'API Swagger.

   a. Accédez à la section Reprise après sinistre et cliquez sur `/4.6/disasterrecovery/storage`.

   b. Collez le jeton d'autorisation de l'utilisateur.

   c. Dans la section SmSetDisasterRecoverySettingsRequest, modifiez `EnableDisasterRecover` à `true`.

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



Voir les commentaires concernant les procédures supplémentaires.

Restaurer les machines virtuelles d'application avec la restauration complète de Veeam

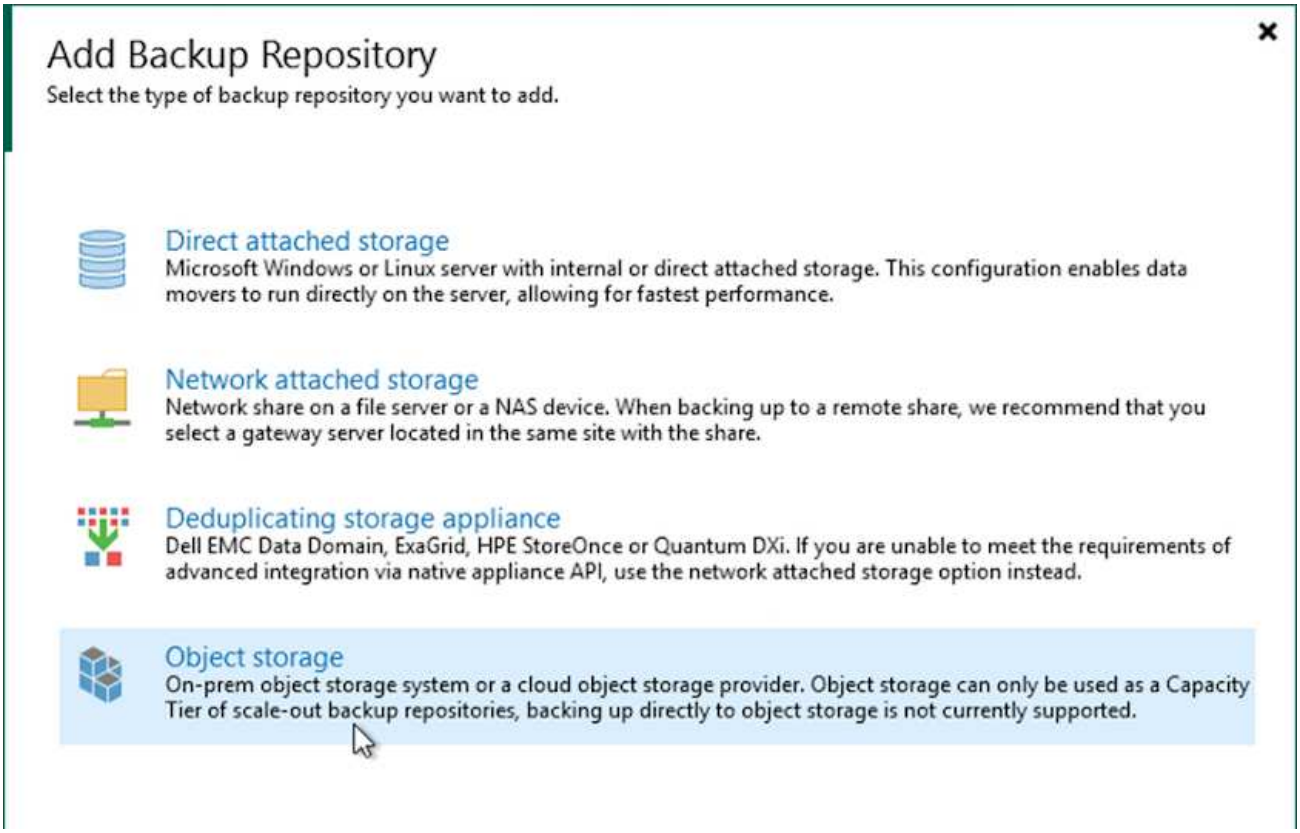
▼ Créer un référentiel de sauvegarde et importer des sauvegardes depuis S3

À partir du serveur Veeam secondaire, importez les sauvegardes du stockage S3 et restaurez les machines virtuelles SQL Server et Oracle sur votre cluster VMware Cloud.

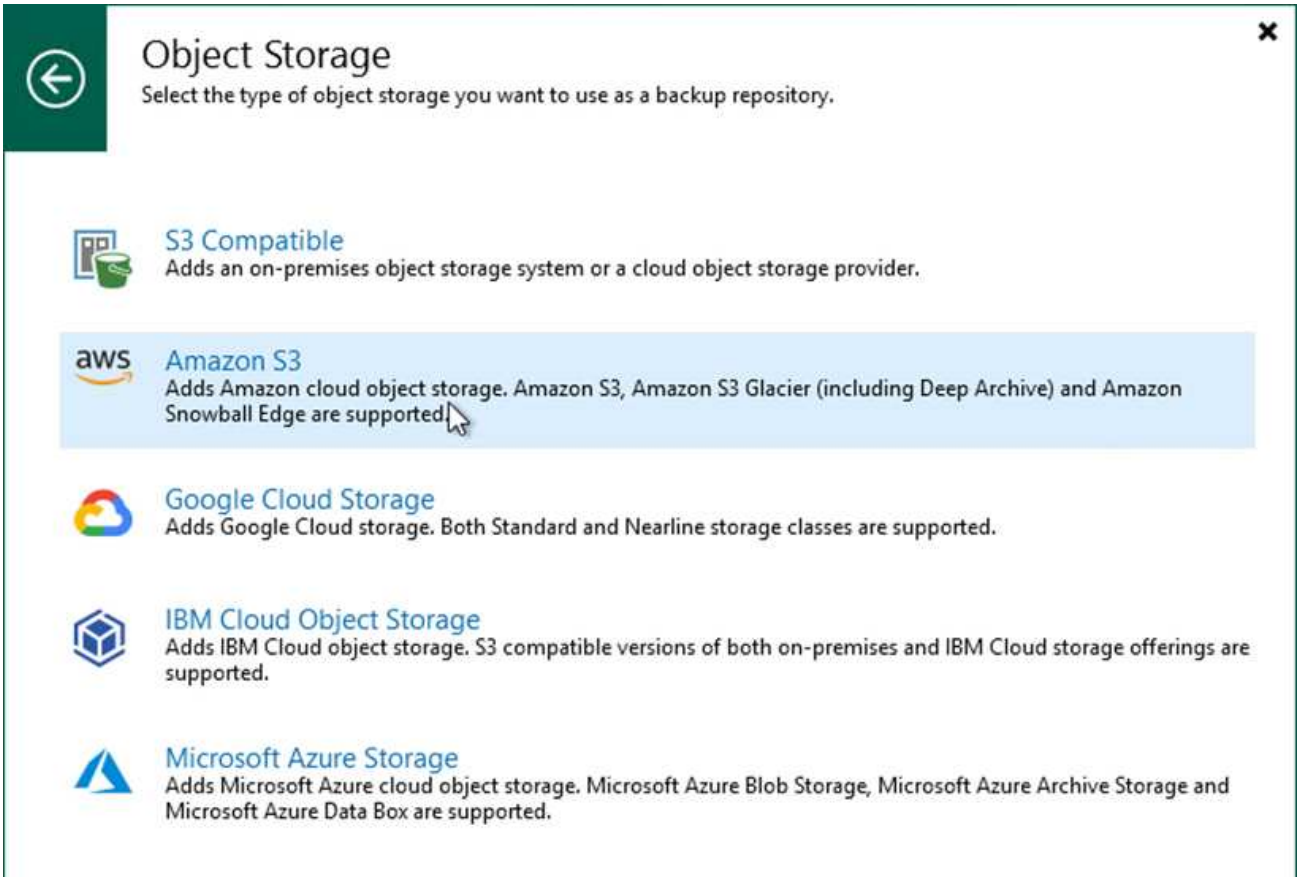
Pour importer les sauvegardes de l'objet S3 qui faisait partie du référentiel de sauvegarde évolutif sur site,

procédez comme suit :

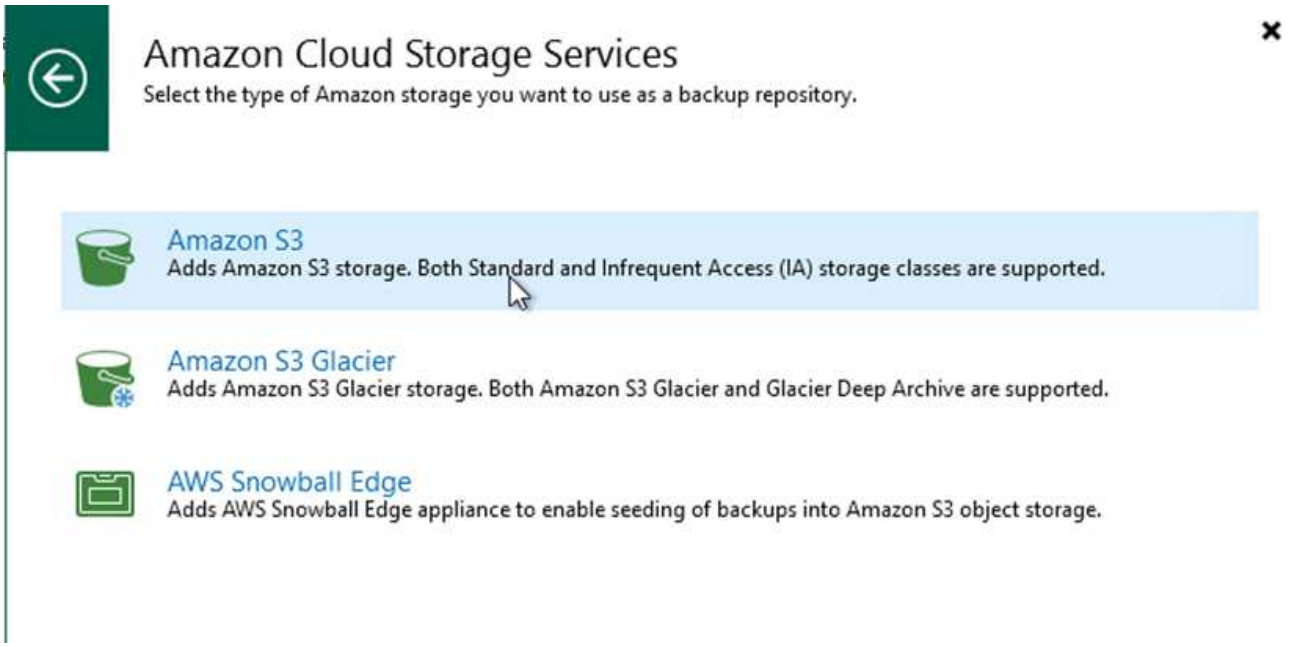
1. Accédez aux référentiels de sauvegarde et cliquez sur Ajouter un référentiel dans le menu supérieur pour lancer l'assistant Ajouter un référentiel de sauvegarde. Sur la première page de l'assistant, sélectionnez Stockage d'objets comme type de référentiel de sauvegarde.



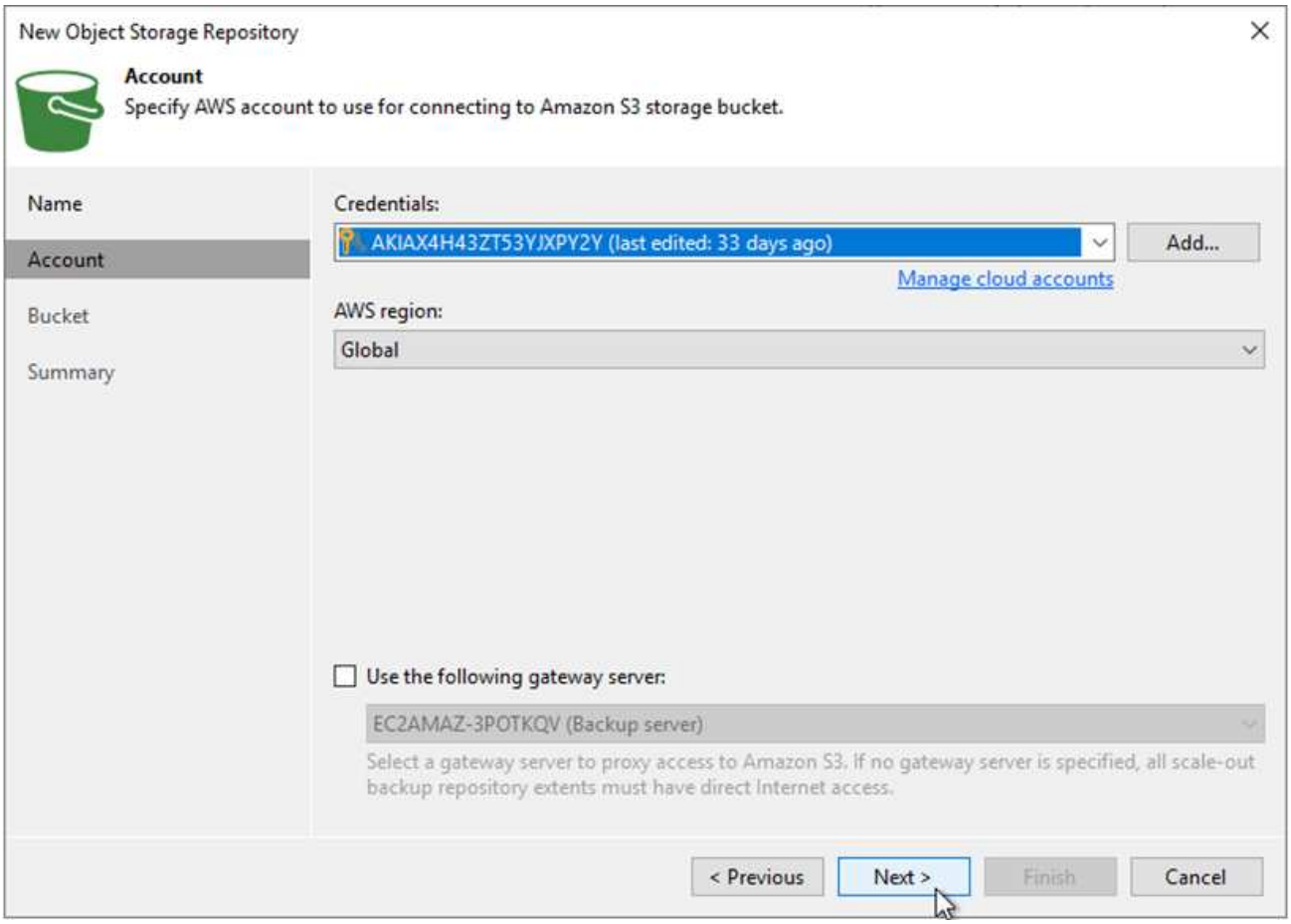
2. Sélectionnez Amazon S3 comme type de stockage d'objets.



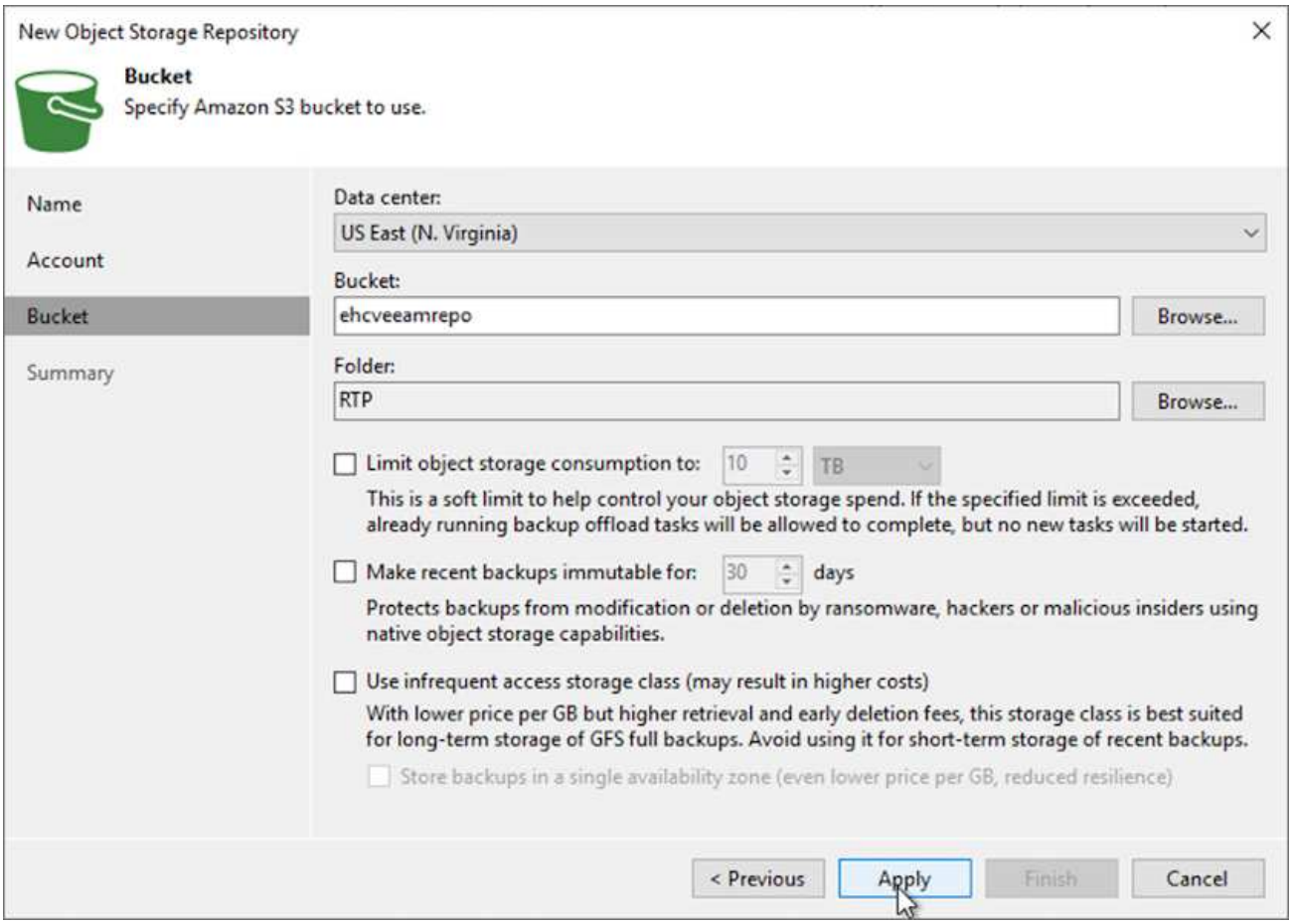
3. Dans la liste des services Amazon Cloud Storage, sélectionnez Amazon S3.



4. Sélectionnez vos informations d'identification pré-saisies dans la liste déroulante ou ajoutez une nouvelle information d'identification pour accéder à la ressource de stockage cloud. Cliquez sur Suivant pour continuer.



5. Sur la page Bucket, entrez le centre de données, le bucket, le dossier et les options souhaitées. Cliquez sur Appliquer.

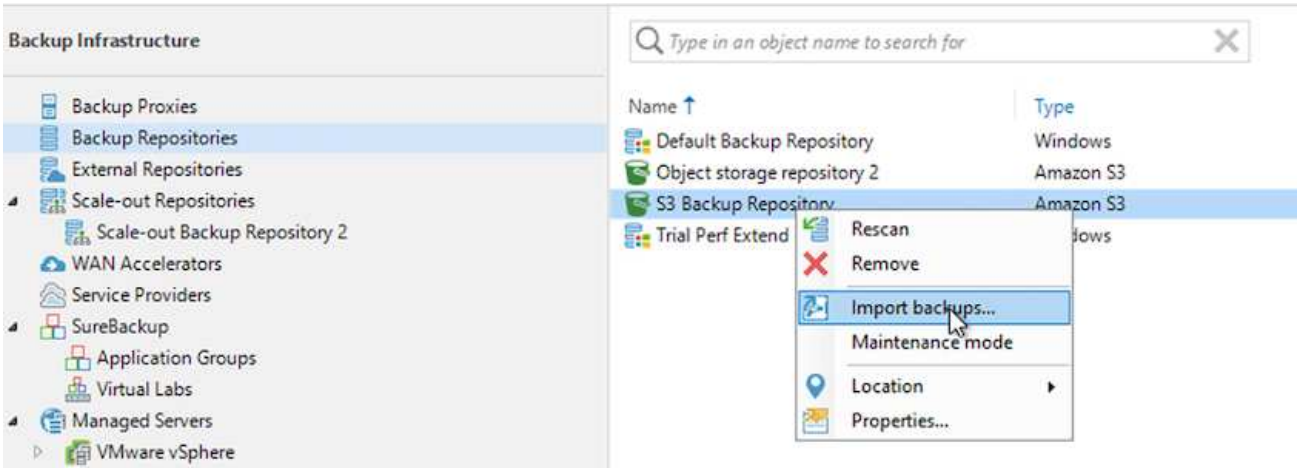


6. Enfin, sélectionnez Terminer pour terminer le processus et ajouter le référentiel.

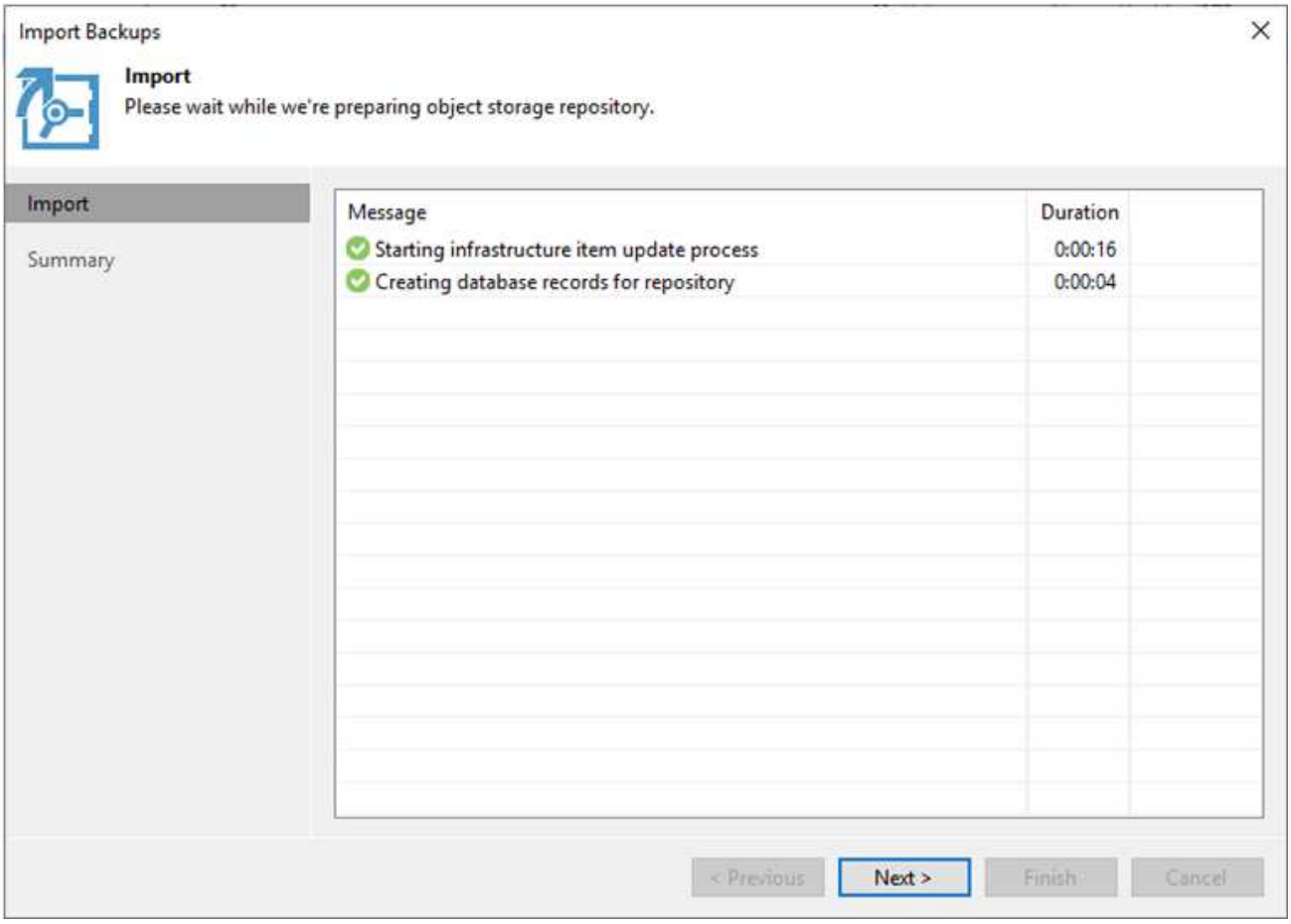
▼ **Importer des sauvegardes à partir du stockage d'objets S3**

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

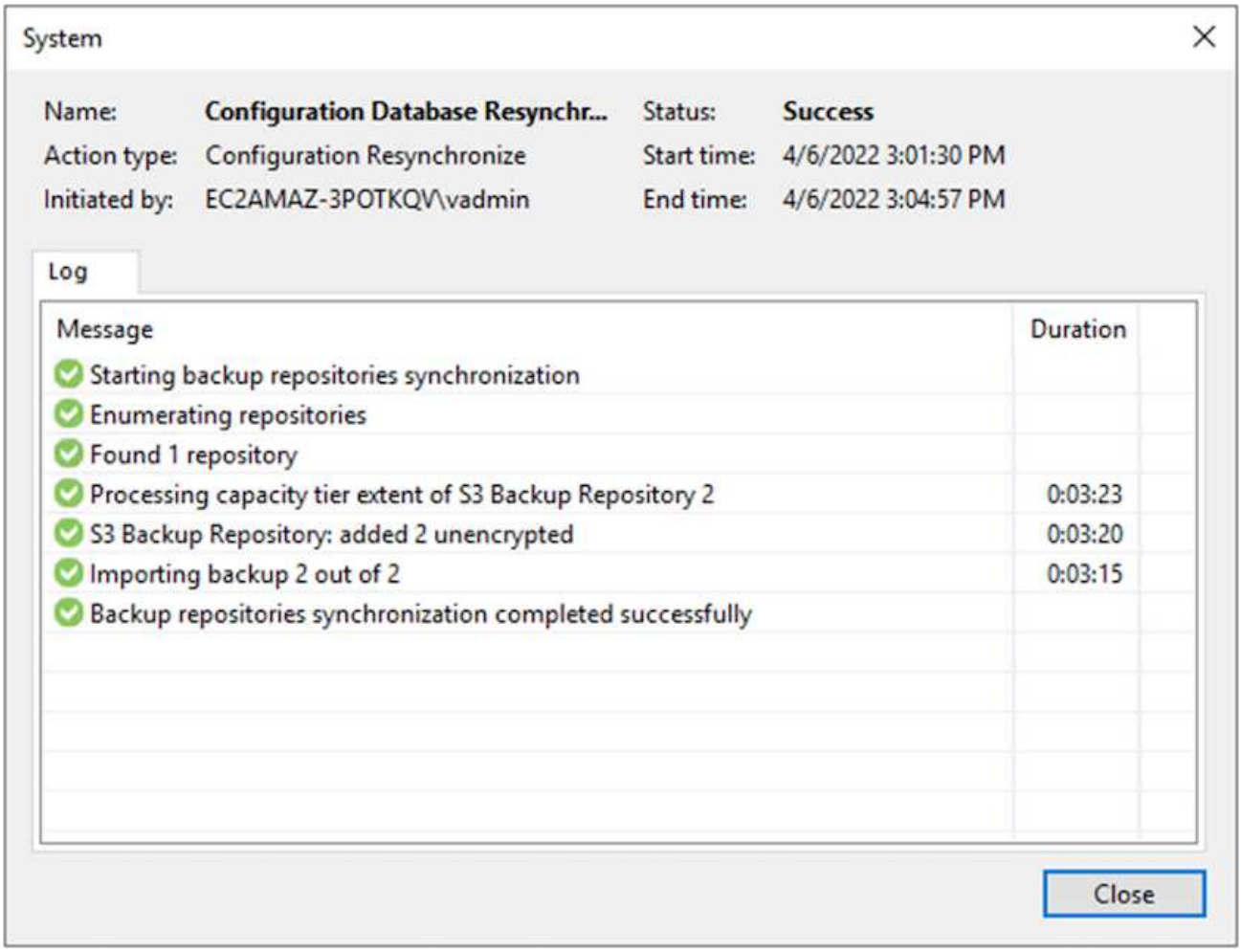
1. Depuis le référentiel de sauvegarde S3, sélectionnez Importer des sauvegardes pour lancer l'assistant Importer des sauvegardes.



2. Une fois les enregistrements de base de données pour l'importation créés, sélectionnez Suivant, puis Terminer dans l'écran récapitulatif pour démarrer le processus d'importation.



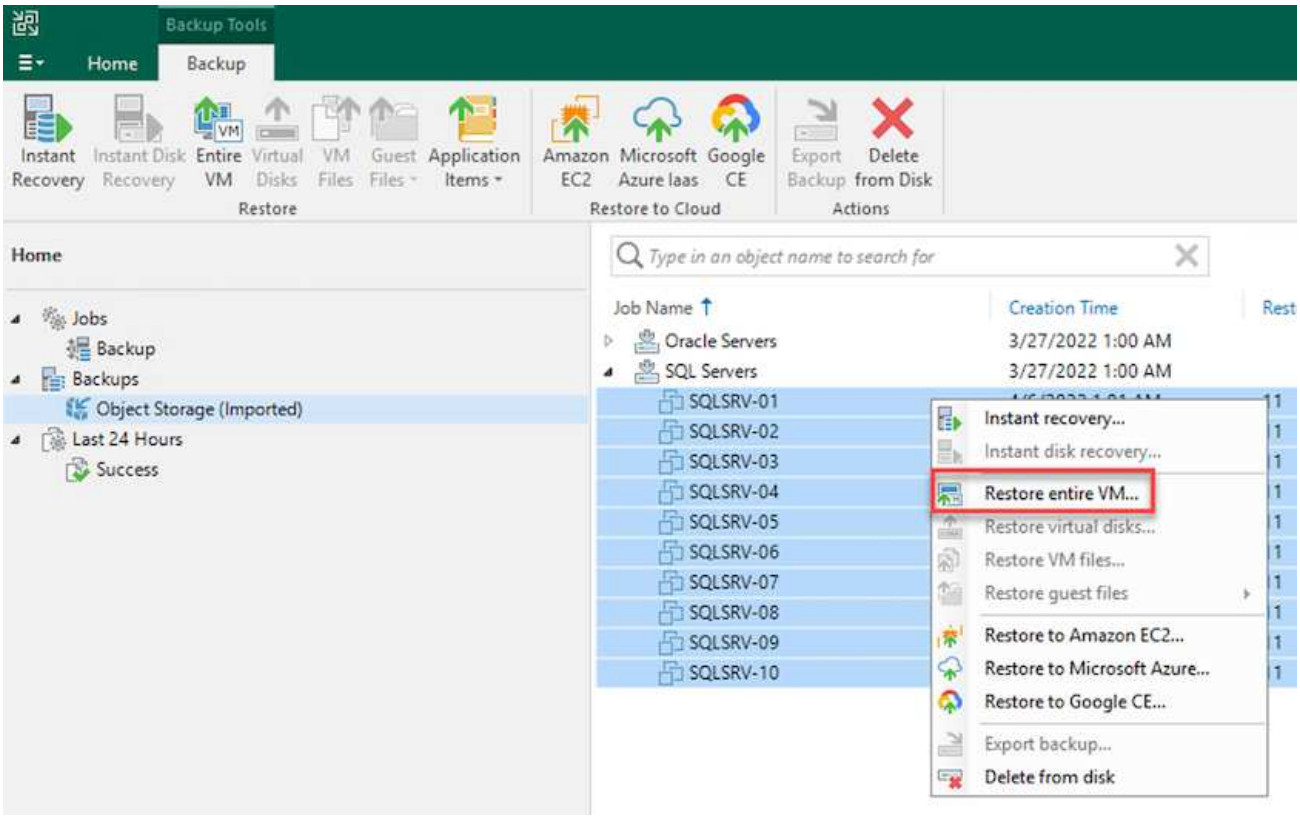
3. Une fois l'importation terminée, vous pouvez restaurer les machines virtuelles dans le cluster VMware Cloud.



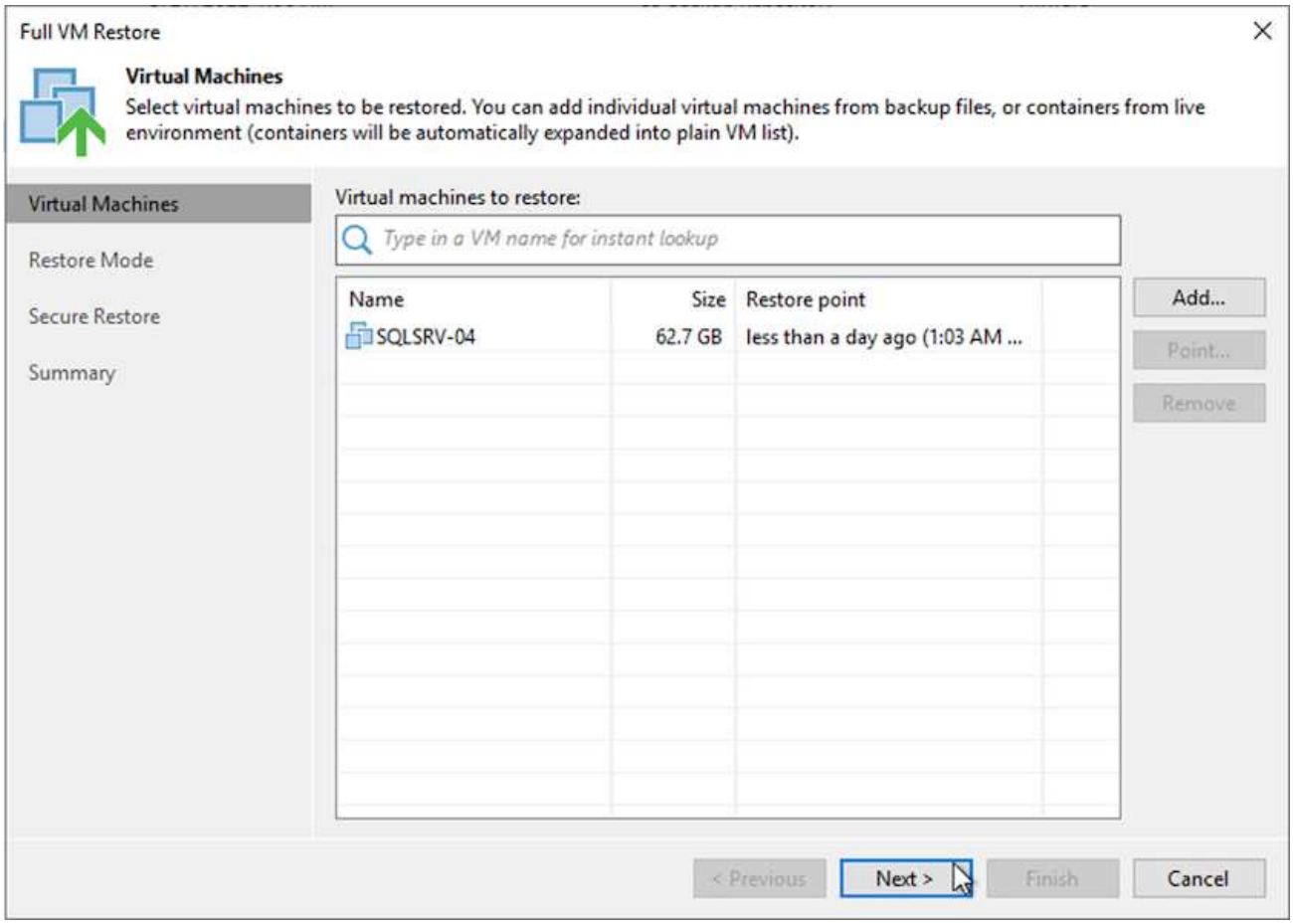
▼ **Restaurer les machines virtuelles d'application avec la restauration complète Veeam vers VMware Cloud**

Pour restaurer les machines virtuelles SQL et Oracle sur le domaine/cluster de charge de travail VMware Cloud on AWS, procédez comme suit.

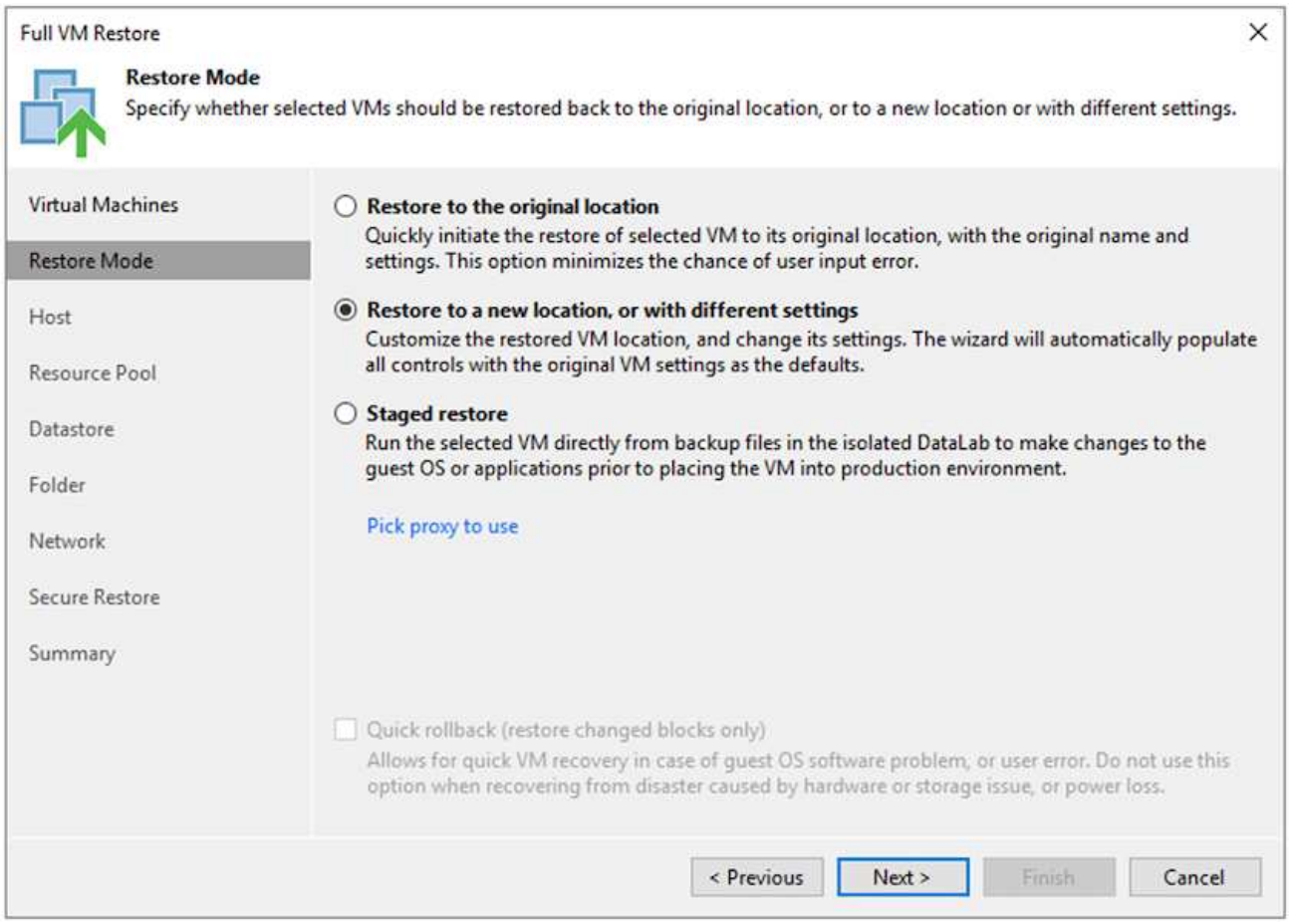
1. Depuis la page d'accueil de Veeam, sélectionnez le stockage d'objets contenant les sauvegardes importées, sélectionnez les machines virtuelles à restaurer, puis cliquez avec le bouton droit de la souris et sélectionnez Restaurer la machine virtuelle entière.



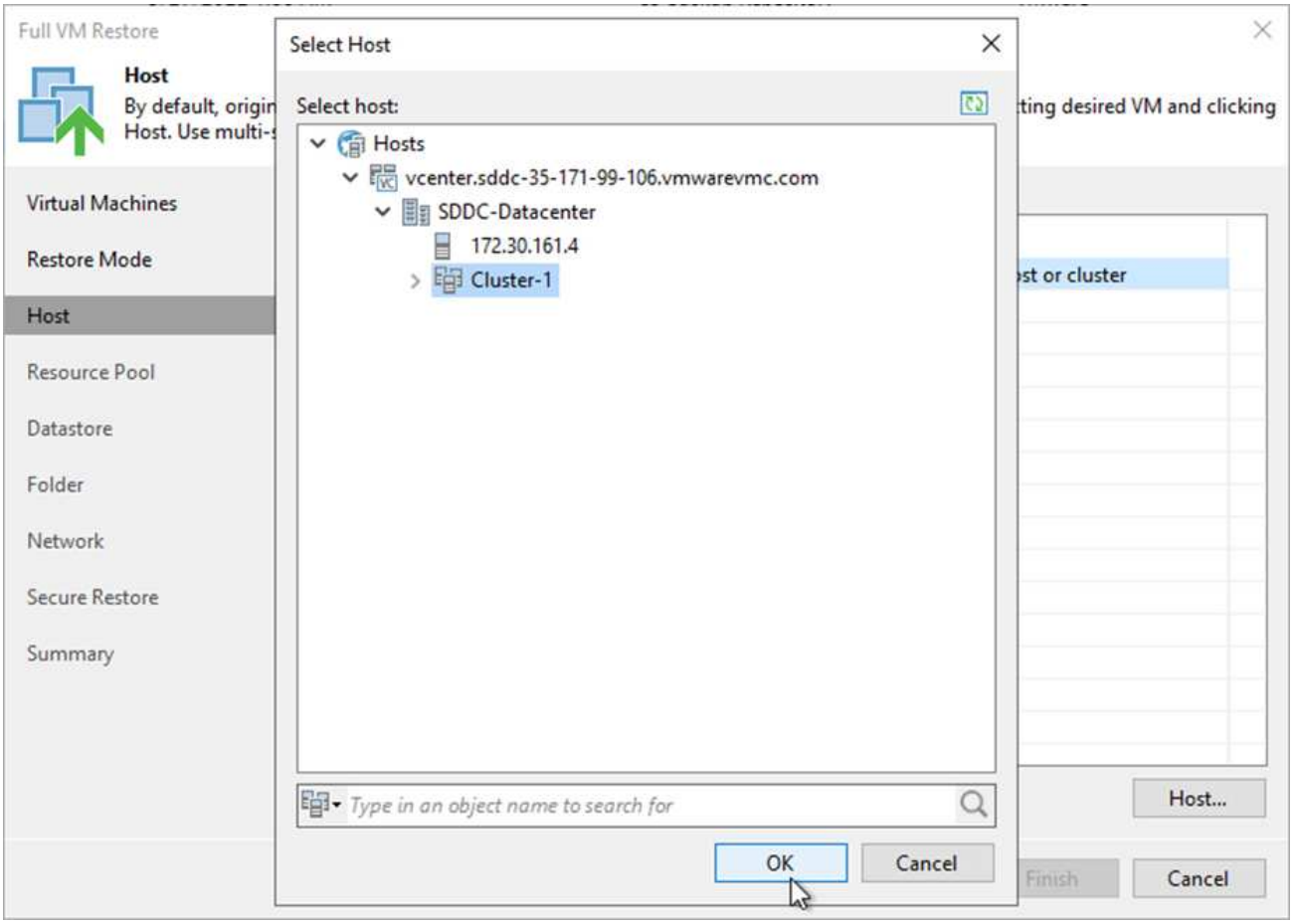
2. Sur la première page de l'assistant de restauration complète de la machine virtuelle, modifiez les machines virtuelles à sauvegarder si vous le souhaitez et sélectionnez Suivant.



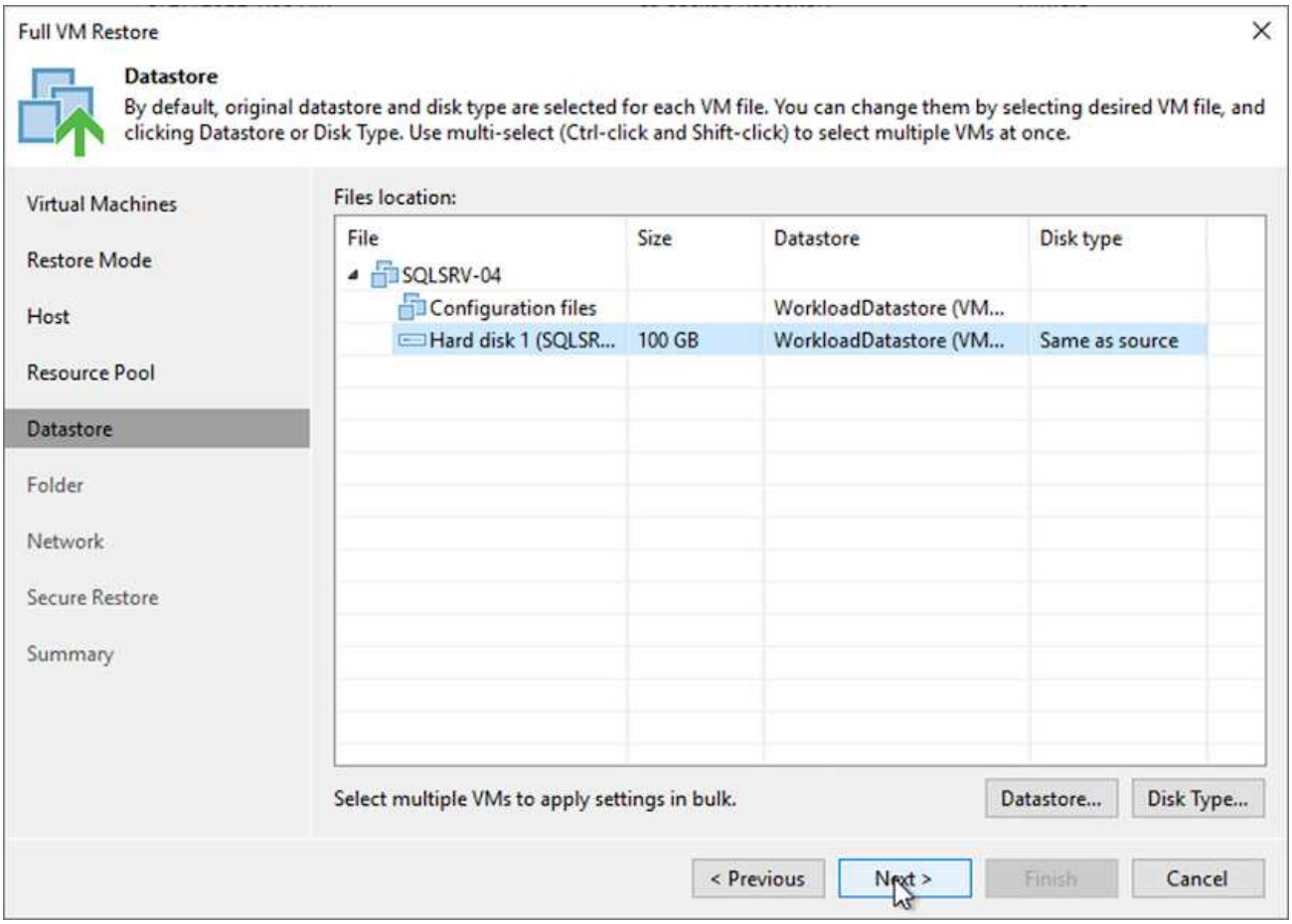
3. Sur la page Mode de restauration, sélectionnez Restaurer vers un nouvel emplacement ou avec des paramètres différents.



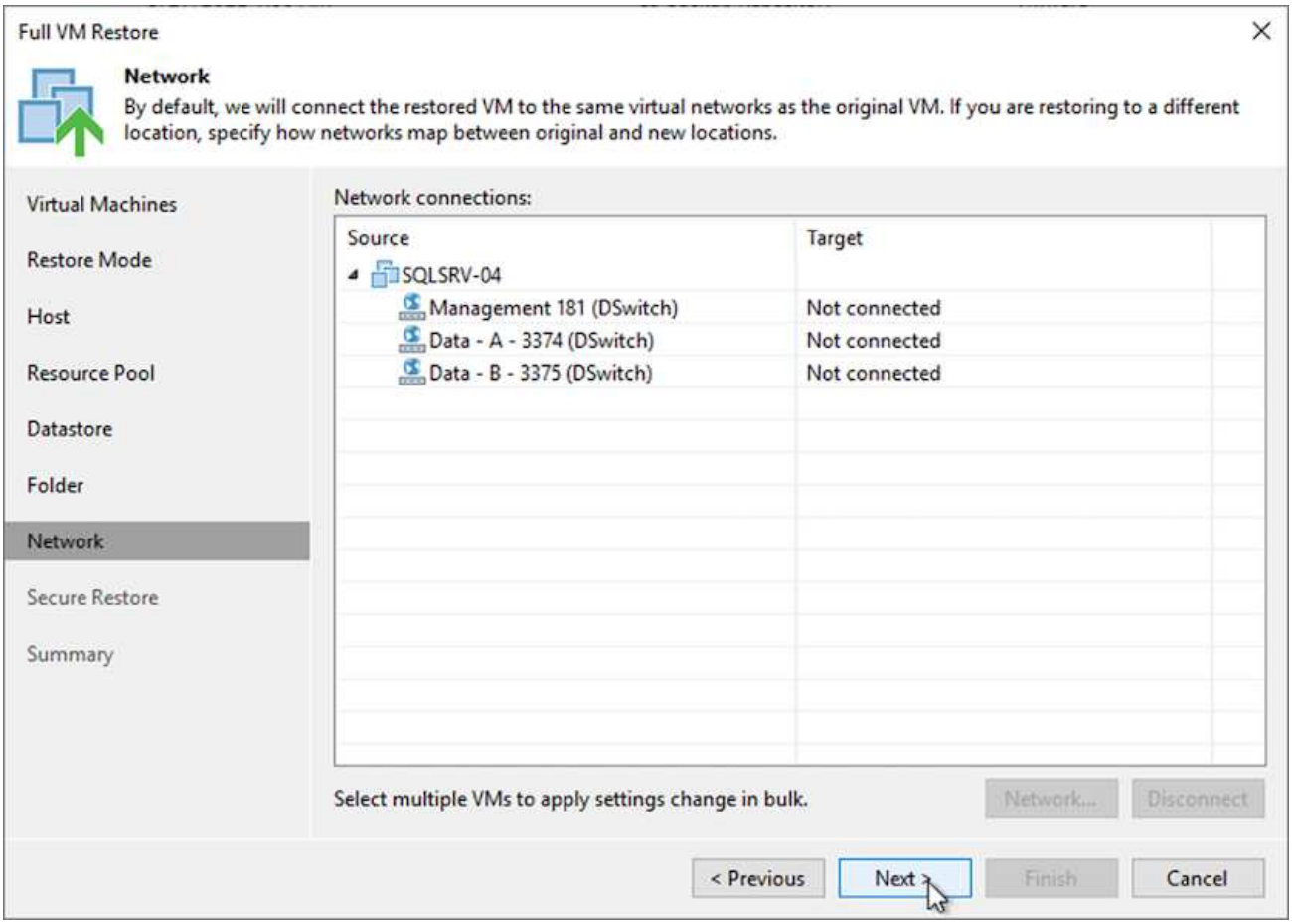
4. Sur la page de l'hôte, sélectionnez l'hôte ou le cluster ESXi cible sur lequel restaurer la machine virtuelle.

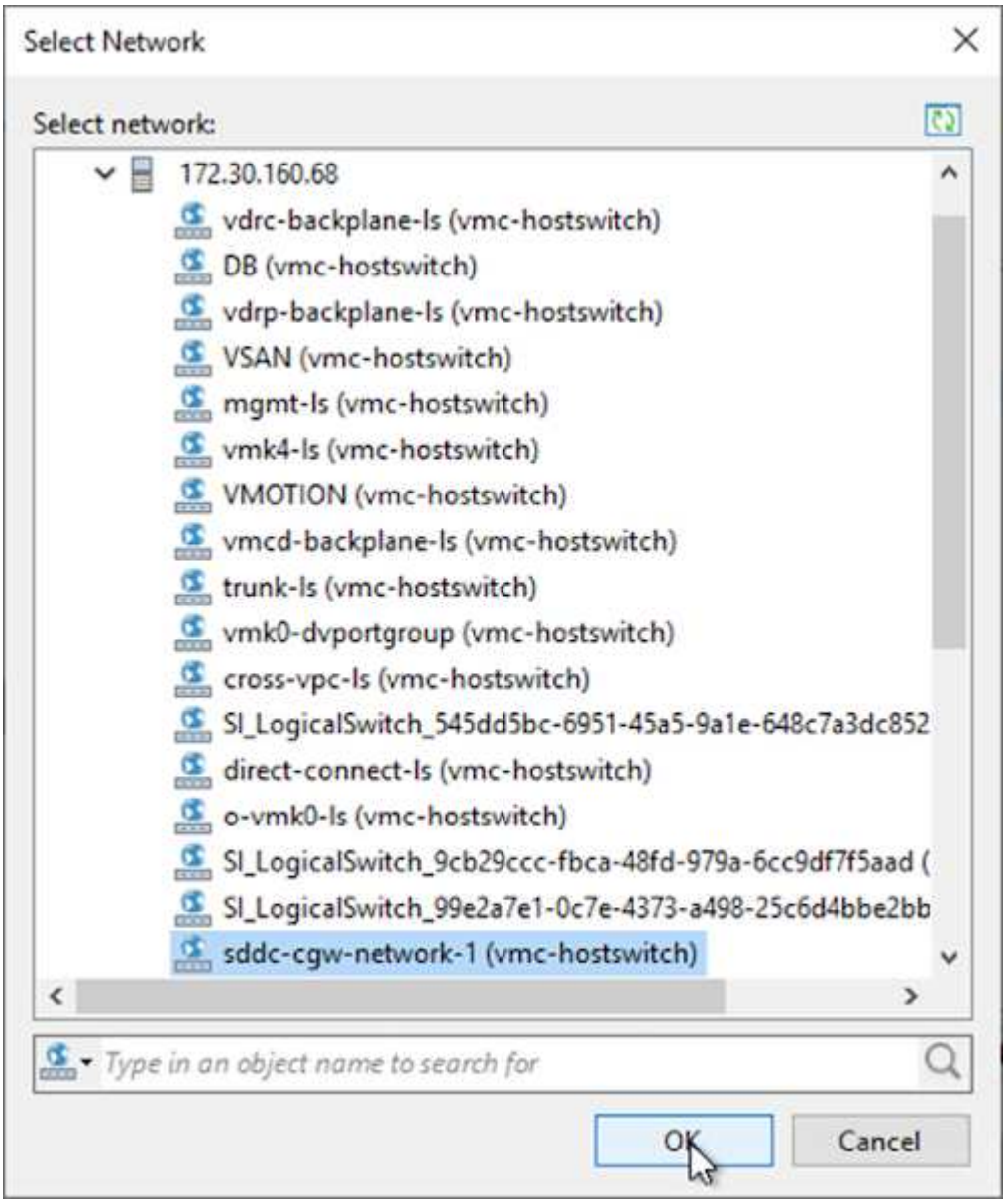


5. Sur la page Magasins de données, sélectionnez l'emplacement du magasin de données cible pour les fichiers de configuration et le disque dur.



6. Sur la page Réseau, mappez les réseaux d'origine de 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 de logiciels malveillants, consultez la page de résumé et cliquez sur Terminer pour démarrer la restauration.

Restaurer les données d'application SQL Server

Le processus suivant fournit des instructions sur la façon de récupérer un serveur SQL dans VMware Cloud Services dans AWS en cas de sinistre rendant le site local inutilisable.

Les conditions préalables suivantes sont supposées être remplies pour pouvoir poursuivre les étapes de récupération :

1. La machine virtuelle Windows Server a été restaurée sur 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"Résumé du processus de sauvegarde et de restauration de SnapCenter ."

▼ VM : configuration post-restauration pour la machine virtuelle SQL Server

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

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

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

> Pour redécouvrir automatiquement les machines virtuelles restaurées dans SnapCenter, le nom de domaine complet doit être identique à celui de la machine virtuelle qui a été initialement ajoutée au SnapCenter sur site.

▼ Configurer le stockage FSx pour la restauration de SQL Server

Pour réaliser le processus de restauration de récupération après sinistre pour une machine virtuelle SQL Server, vous devez rompre la relation SnapMirror existante du cluster FSx et accorder l'accès au volume. Pour ce faire, procédez comme suit.

1. Pour rompre la relation SnapMirror existante pour la base de données SQL Server et les volumes de journaux, exécutez la commande suivante à partir de l'interface de ligne de commande FSx :

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

2. Accordez l'accès au LUN en créant un groupe d'initiateurs contenant l'IQN iSCSI de la machine virtuelle Windows SQL Server :

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

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

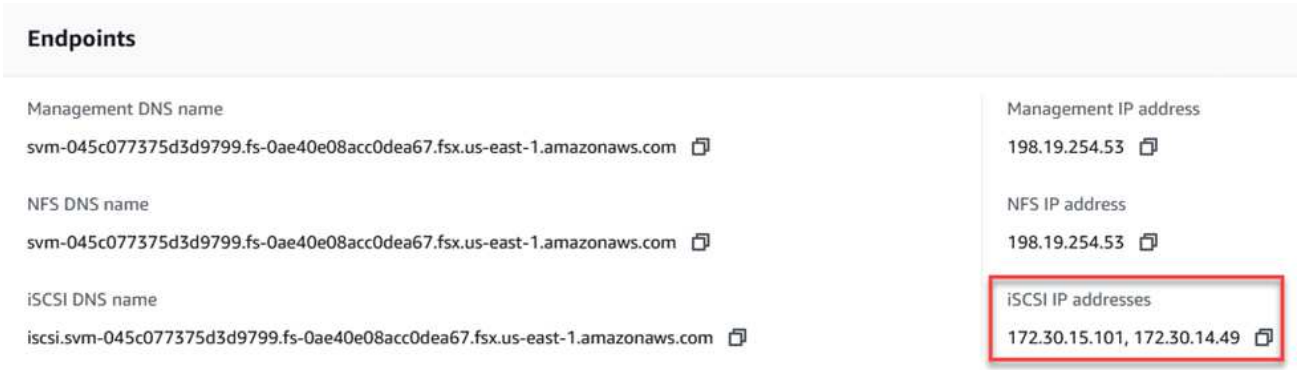
```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

4. Pour trouver le nom du chemin, exécutez la commande `lun show` commande.

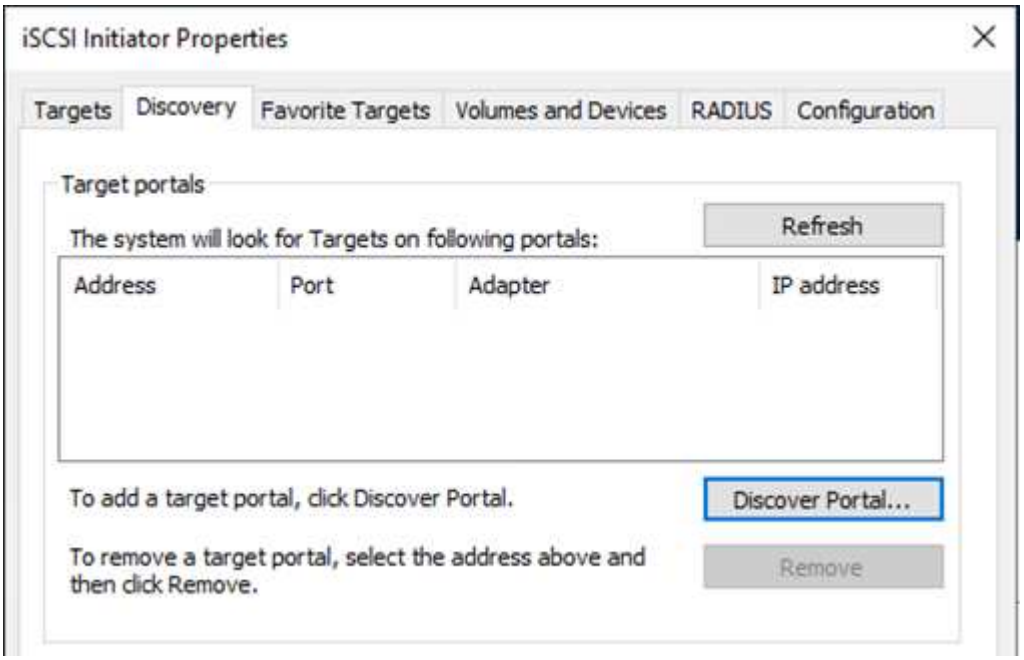
▼ Configurer la machine virtuelle Windows pour l'accès iSCSI et découvrir les systèmes de fichiers

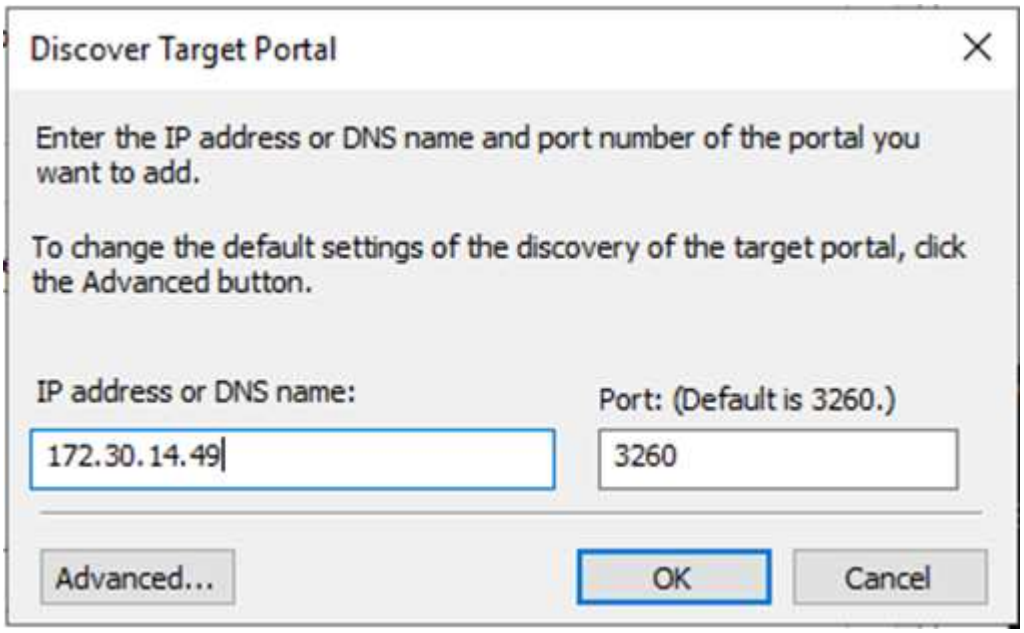
1. À partir de la machine virtuelle SQL Server, configurez votre adaptateur réseau iSCSI pour communiquer sur le groupe de ports VMware qui a été établi avec une connectivité aux interfaces cibles iSCSI sur votre instance FSx.
2. Ouvrez l'utilitaire Propriétés de l'initiateur iSCSI et effacez les anciens paramètres de connectivité dans les onglets Découverte, Cibles favorites et Cibles.

3. Localisez la ou les adresses IP permettant d'accéder à l'interface logique iSCSI sur l'instance/le cluster FSx. Vous pouvez le trouver dans la console AWS sous Amazon FSx > ONTAP > Machines virtuelles de stockage.

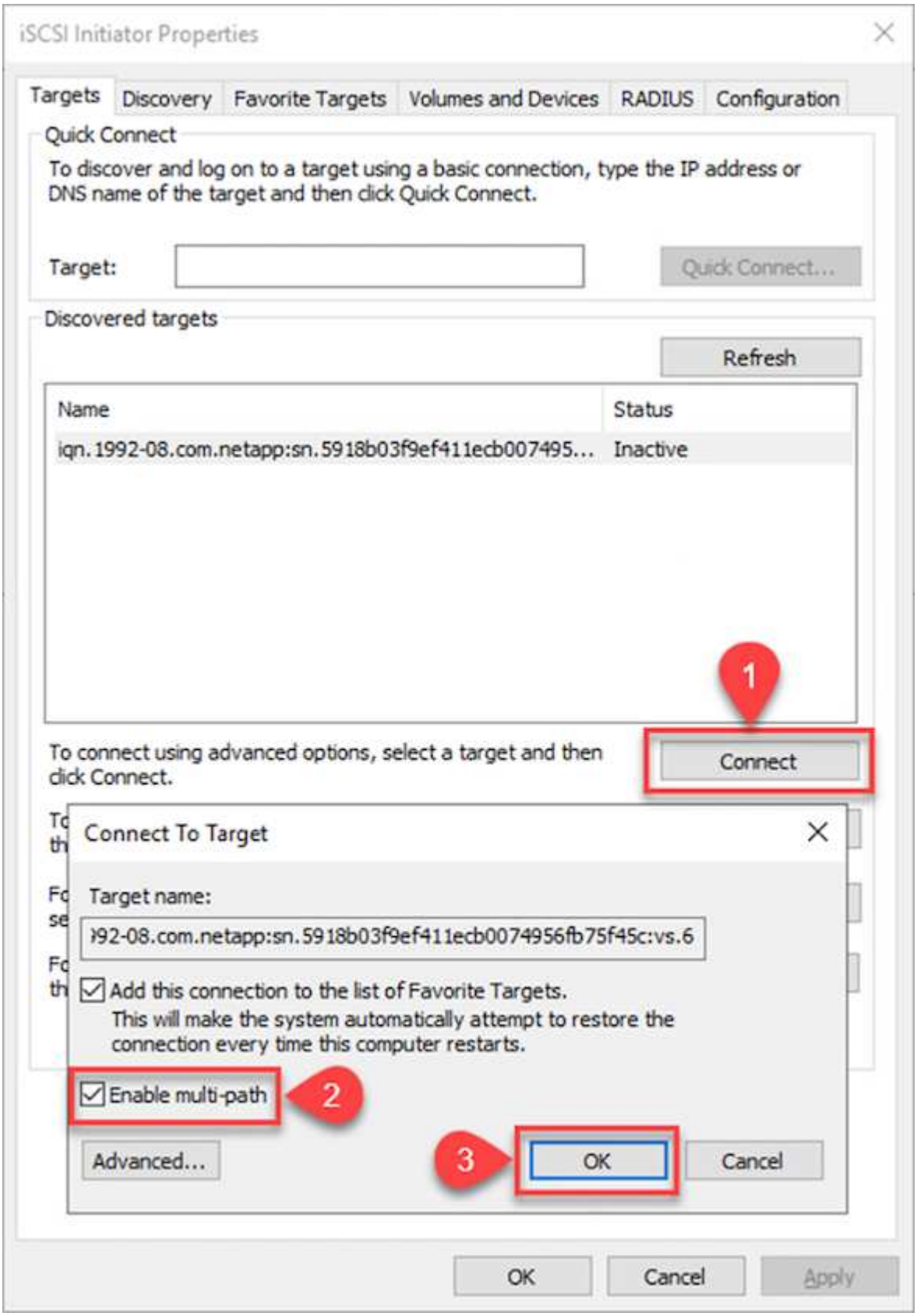


4. Dans l'onglet Découverte, cliquez sur Découvrir le portail et entrez les adresses IP de vos cibles iSCSI FSx.

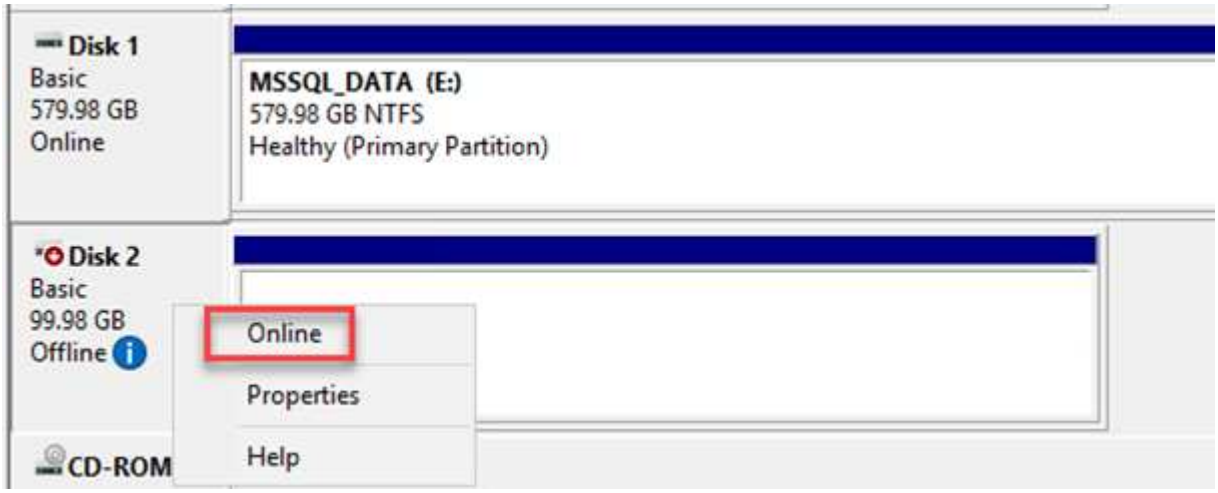




5. Dans l'onglet Cible, cliquez sur Connecter, sélectionnez Activer Multi-Path si cela convient à votre configuration, puis cliquez sur OK pour vous connecter à la cible.

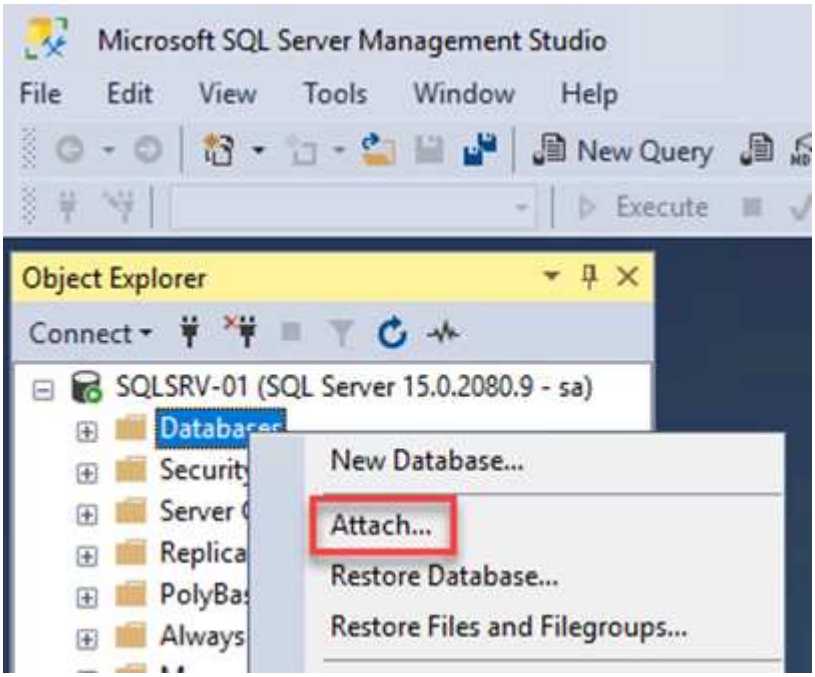


6. Ouvrez l’utilitaire Gestion de l’ordinateur et mettez les disques en ligne. Vérifiez qu’ils conservent les mêmes lettres de lecteur qu’ils détenaient auparavant.

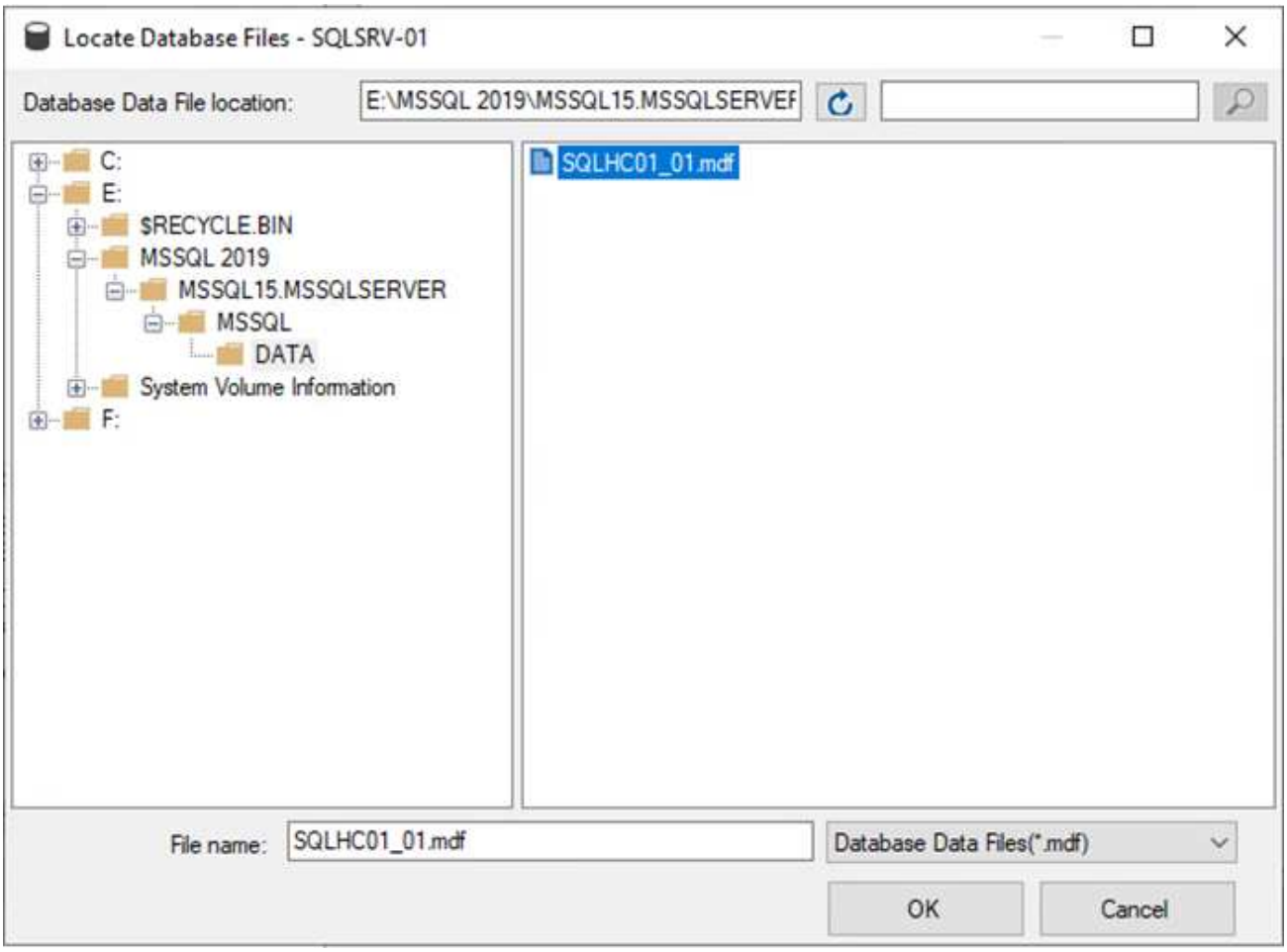


▼ **Attacher les bases de données SQL Server**

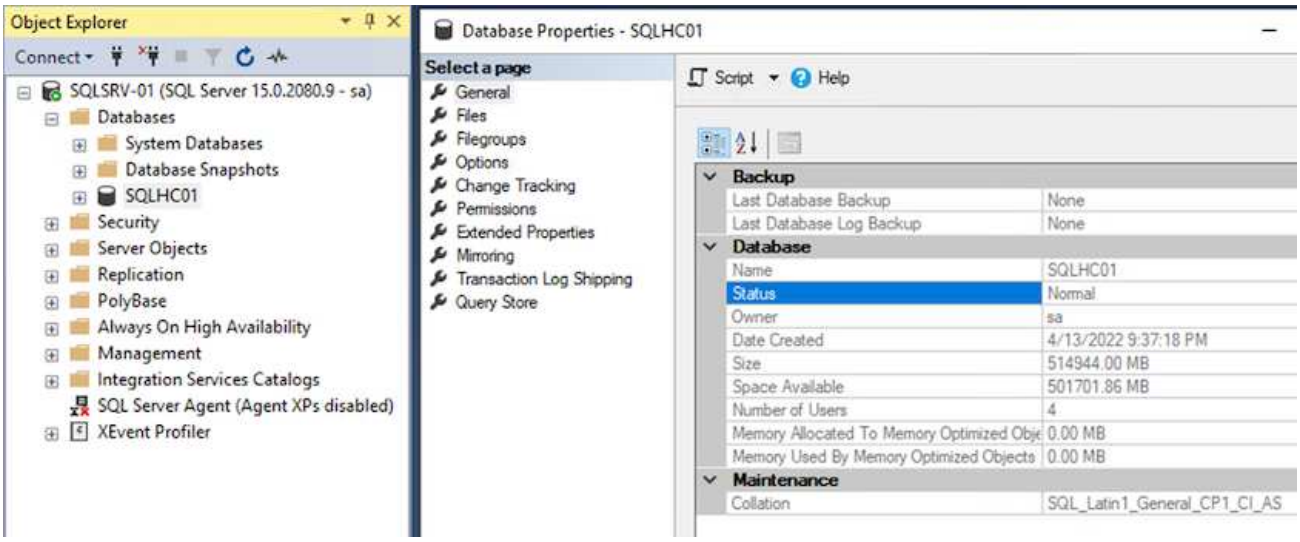
1. À partir de la machine virtuelle SQL Server, ouvrez Microsoft SQL Server Management Studio et sélectionnez Attacher pour démarrer le processus de connexion à la base de données.



2. Cliquez sur Ajouter et accédez au dossier contenant le fichier de base de données principal SQL Server, sélectionnez-le et cliquez sur OK.



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

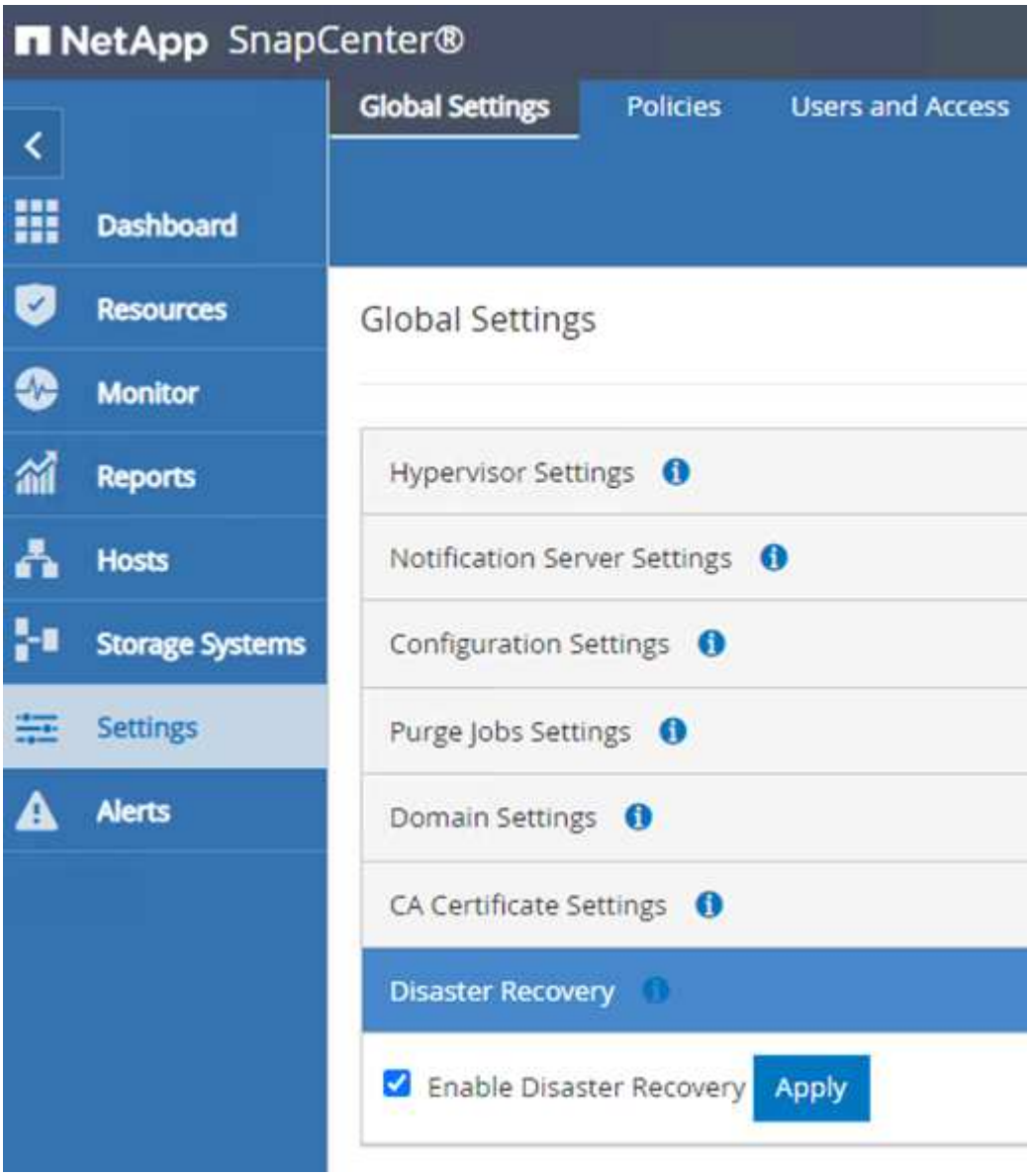


▼ **Confirmer la communication de SnapCenter avec le plug-in SQL Server**

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 prérequis suivants :

- SnapCenter doit être placé en mode de récupération après sinistre. Cela peut être réalisé via l'API Swagger ou dans les paramètres globaux sous Reprise après sinistre.
- Le nom de domaine complet du serveur SQL doit être identique à celui de l'instance qui s'exécutait dans le centre de données local.
- 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 de récupération après sinistre, accédez aux paramètres depuis le client Web SnapCenter . Accédez à l'onglet Paramètres globaux, puis cliquez sur Récupération après sinistre. Assurez-vous que la case à cocher Activer la récupération après sinistre est activée.



Restaurer les données d'application Oracle

Le processus suivant fournit des instructions sur la façon de récupérer les données d'application Oracle dans VMware Cloud Services dans AWS en cas de sinistre rendant le site local inutilisable.

Remplissez les conditions préalables suivantes pour continuer les étapes de récupération :

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

▼ **Configurer FSx pour la restauration Oracle – Rompre la relation SnapMirror**

Pour rendre les volumes de stockage secondaires hébergés sur l'instance FSx ONTAP accessibles aux serveurs Oracle, vous devez d'abord rompre la relation SnapMirror existante.

1. Après vous être connecté à l'interface de ligne de commande 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::>
```

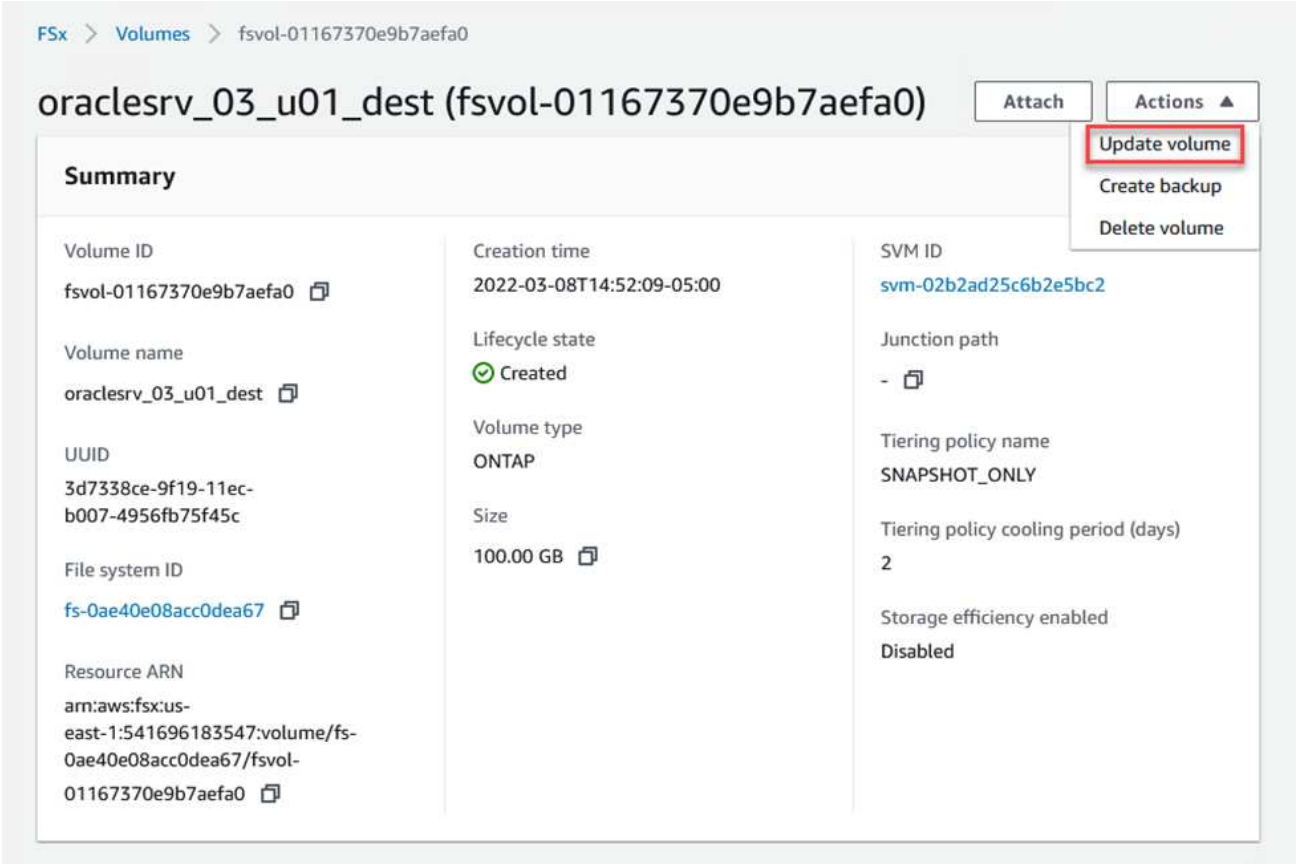
2. Exécutez la commande suivante pour rompre les relations SnapMirror existantes.

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

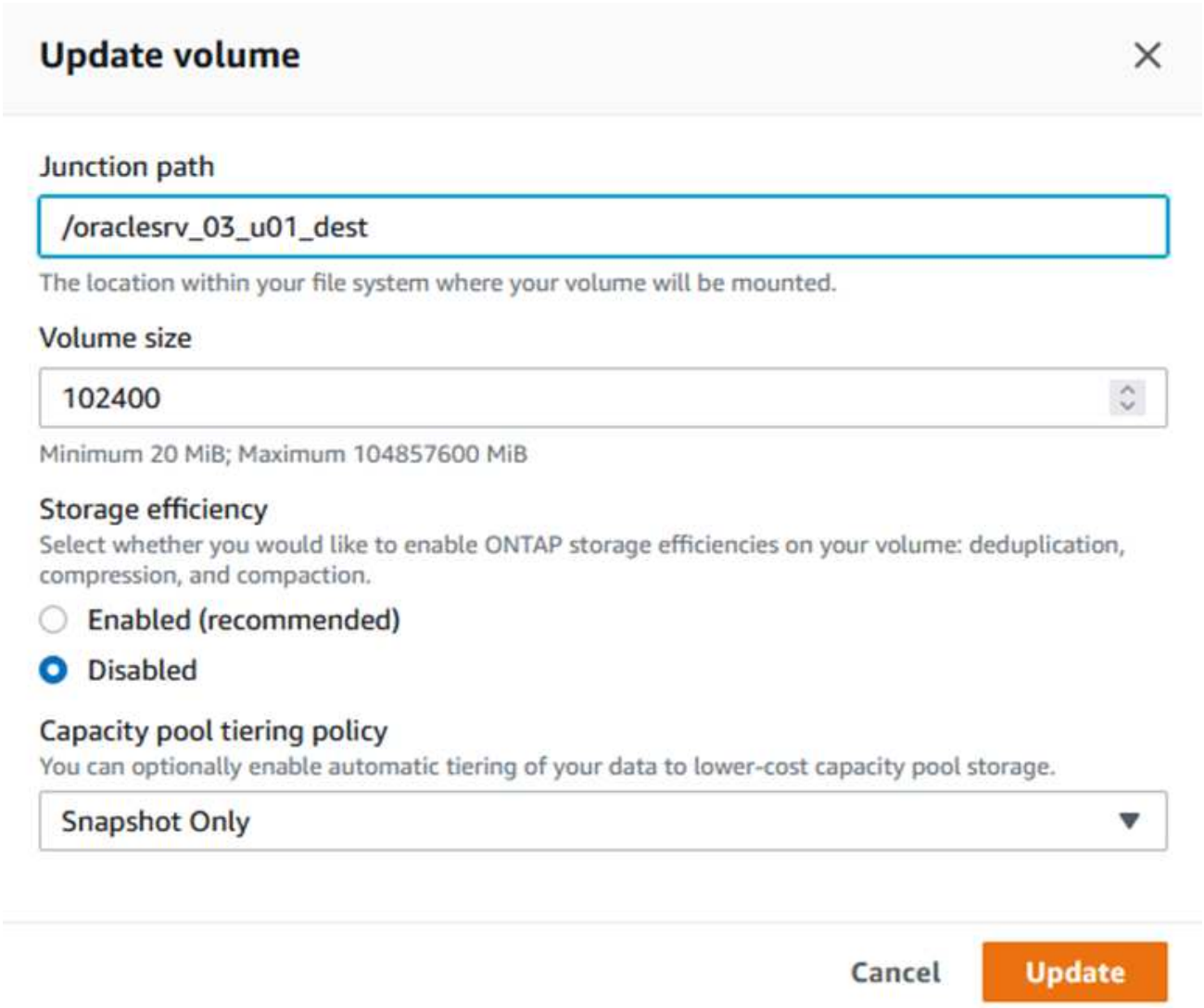
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

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. Mettre à jour le chemin de jonction dans le client Web Amazon FSx :



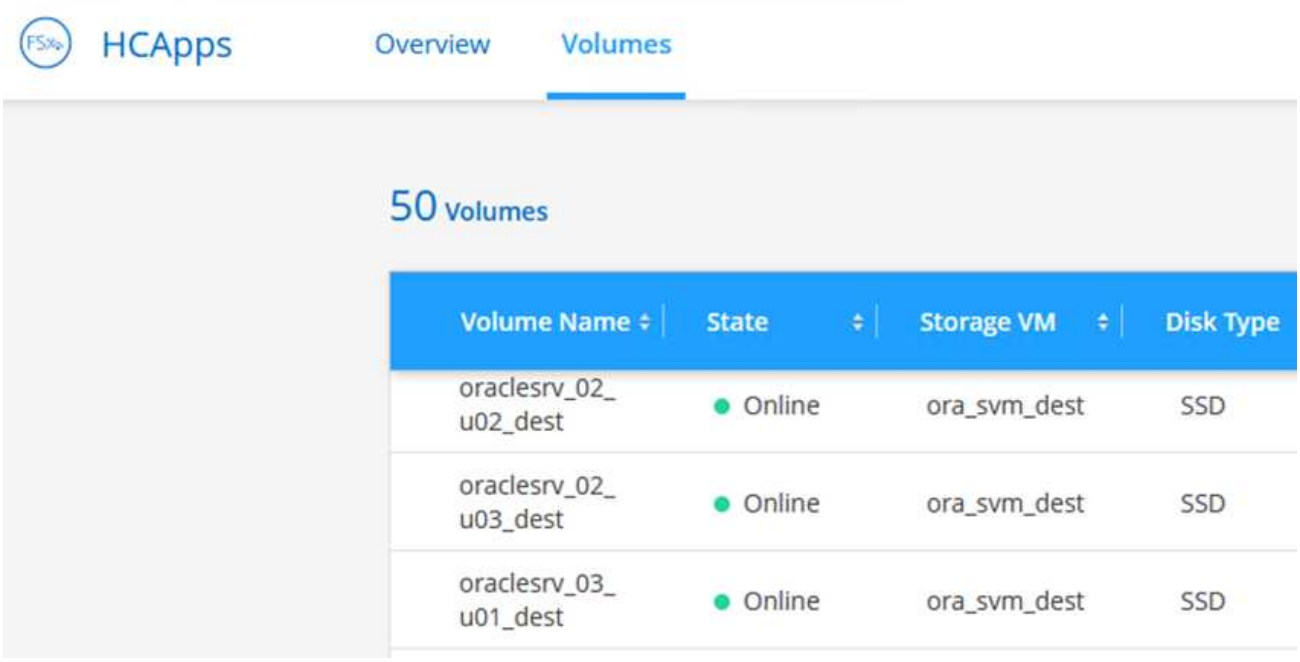
4. Ajoutez le nom du chemin de jonction et cliquez sur Mettre à jour. Spécifiez ce chemin de jonction lors du montage du volume NFS à partir du serveur Oracle.



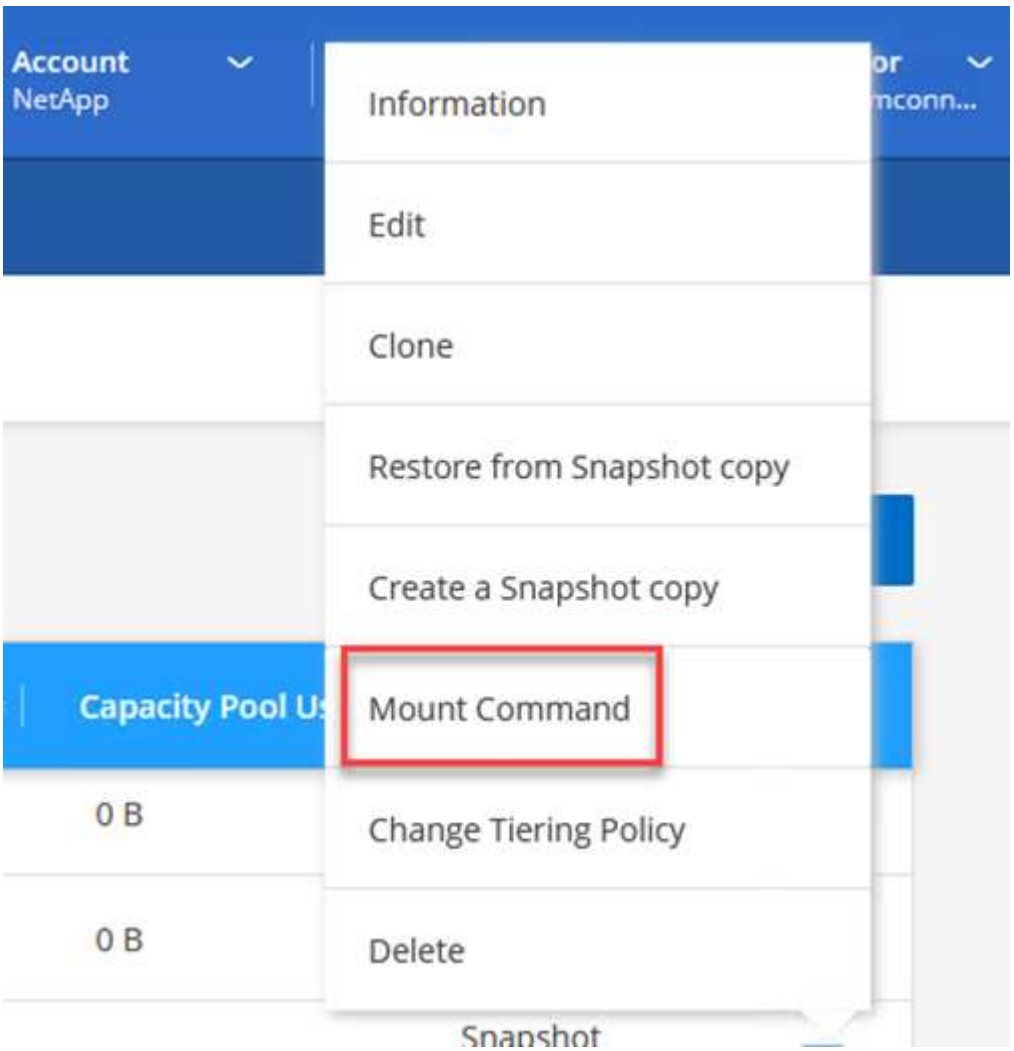
▼ **Monter des volumes NFS sur Oracle Server**

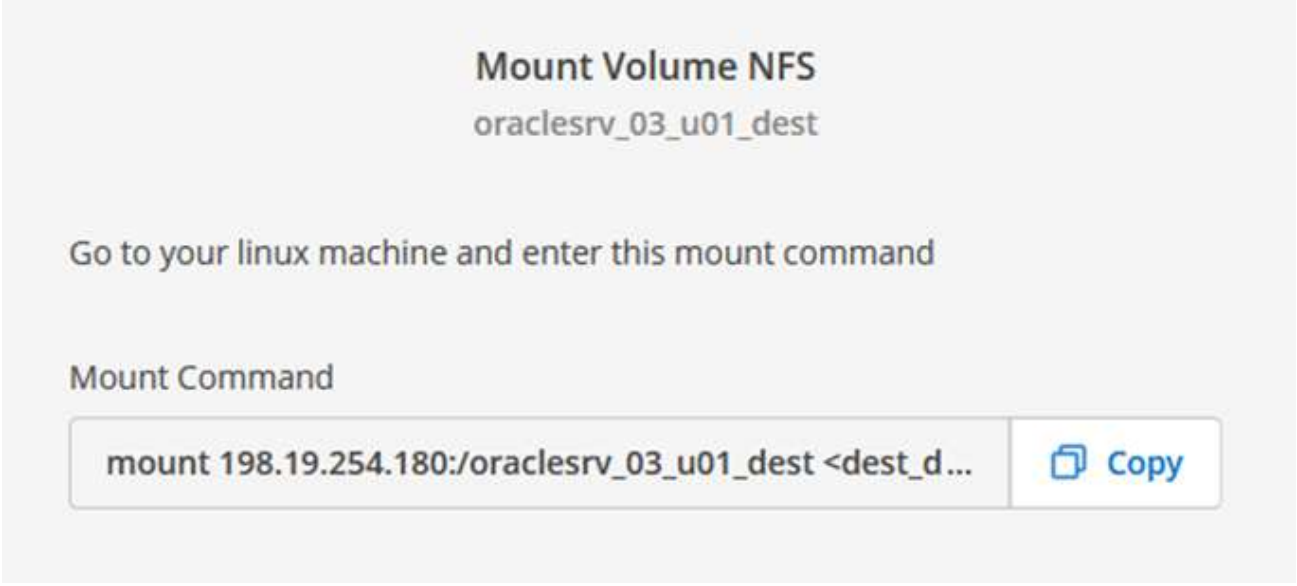
Dans Cloud Manager, vous pouvez obtenir la commande mount avec l'adresse IP NFS LIF correcte pour monter les volumes NFS qui contiennent les fichiers et les journaux de base de données Oracle.

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



2. Dans le menu d'action, sélectionnez Commande de montage pour afficher et copier la commande de montage 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. Depuis le 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 pour inclure les commandes de montage.

5. Redémarrez le serveur Oracle. Les bases de données Oracle devraient démarrer normalement et être disponibles à l'utilisation.

Retour arrière

Une fois le processus de basculement décrit dans cette solution terminé avec succès, SnapCenter et Veeam reprennent leurs fonctions de sauvegarde exécutées dans AWS, et FSx ONTAP est désormais désigné comme stockage principal sans relations SnapMirror existantes avec le centre de données local d'origine. Une fois le fonctionnement normal repris sur site, vous pouvez utiliser un processus identique à celui décrit dans cette documentation pour mettre en miroir les données sur le système de stockage ONTAP sur site.

Comme indiqué dans cette documentation, vous pouvez configurer SnapCenter pour mettre en miroir les volumes de données d'application de FSx ONTAP vers un système de stockage ONTAP résidant sur site. De même, vous pouvez configurer Veeam pour répliquer des copies de sauvegarde sur Amazon S3 à l'aide d'un référentiel de sauvegarde évolutif afin que ces sauvegardes soient accessibles à un serveur de sauvegarde Veeam résidant dans le centre de données sur site.

La restauration automatique n'entre pas dans le cadre de cette documentation, mais elle diffère peu du processus détaillé décrit ici.

Conclusion

Le cas d'utilisation présenté dans cette documentation se concentre sur les technologies de reprise après sinistre éprouvées qui mettent en évidence l'intégration entre NetApp et VMware. Les systèmes de stockage NetApp ONTAP fournissent des technologies de mise en miroir de données éprouvées qui permettent aux organisations de concevoir des solutions de reprise après sinistre qui couvrent les technologies sur site et ONTAP résidant chez les principaux fournisseurs de cloud.

FSx ONTAP sur AWS est l'une de ces solutions 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 bien connue qui s'intègre bien aux systèmes de stockage NetApp ONTAP et peut fournir un basculement vers le stockage natif vSphere.

Cette solution présentait une solution de reprise après sinistre utilisant le stockage de connexion invité à partir d'un système ONTAP hébergeant des données d'application SQL Server et Oracle. SnapCenter avec SnapMirror fournit une solution facile à gérer pour protéger les volumes d'application sur les systèmes ONTAP et les répliquer vers FSx ou CVO résidant dans le cloud. SnapCenter est une solution compatible DR permettant de basculer toutes les données d'application vers VMware Cloud sur AWS.

Veeam Backup & Restore dans VMware Cloud, avec Amazon FSx ONTAP

Veeam Backup & Replication est une solution efficace et fiable pour la protection des données dans VMware Cloud. Cette solution démontre la configuration et l'installation appropriées pour l'utilisation de Veeam Backup and Replication pour sauvegarder et restaurer les machines virtuelles d'application résidant sur les banques de données FSx ONTAP NFS dans VMware Cloud.

Aperçu

VMware Cloud (dans AWS) prend en charge l'utilisation de banques de données NFS comme stockage supplémentaire, et FSx ONTAP est une solution sécurisée pour les clients qui ont besoin de stocker de grandes quantités de données pour leurs applications cloud qui peuvent évoluer indépendamment du nombre d'hôtes ESXi dans le cluster SDDC. Ce service de stockage AWS intégré offre un stockage hautement efficace avec toutes les fonctionnalités traditionnelles de NetApp ONTAP .

Cas d'utilisation

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde et restauration de machines virtuelles Windows et Linux hébergées dans VMC en utilisant FSx ONTAP comme référentiel de sauvegarde.
- Sauvegarde et restauration des données d'application Microsoft SQL Server à l'aide de FSx ONTAP comme référentiel de sauvegarde.
- Sauvegarde et restauration des données d'application Oracle à l'aide de FSx ONTAP comme référentiel de sauvegarde.

Banques de données NFS utilisant Amazon FSx ONTAP

Toutes les machines virtuelles de cette solution résident sur des banques de données NFS supplémentaires FSx ONTAP . L'utilisation de FSx ONTAP comme banque de données NFS supplémentaire présente plusieurs avantages. Par exemple, il vous permet de :

- Créez un système de fichiers évolutif et hautement disponible dans le cloud sans avoir besoin d'une

configuration et d'une gestion complexes.

- Intégrez-vous à votre environnement VMware existant, vous permettant d'utiliser des outils et des processus familiers pour gérer vos ressources cloud.
- Bénéficiez des fonctionnalités avancées de gestion des données fournies par ONTAP, telles que les instantanés et la réplication, pour protéger vos données et garantir leur disponibilité.

▼ **Présentation du déploiement de la solution**

Cette liste fournit les étapes de haut niveau nécessaires pour configurer Veeam Backup & Replication, exécuter des tâches de sauvegarde et de restauration à l'aide de FSx ONTAP comme 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 ONTAP à utiliser comme référentiel de sauvegarde iSCSI pour Veeam Backup & Replication.
2. Déployez Veeam Proxy pour distribuer les charges de travail de sauvegarde et monter des référentiels de sauvegarde iSCSI hébergés sur FSx ONTAP.
3. Configurez les tâches de sauvegarde Veeam pour sauvegarder les machines virtuelles SQL Server, Oracle, Linux et Windows.
4. Restaurez les machines virtuelles SQL Server et les bases de données individuelles.
5. Restaurez les machines virtuelles Oracle et les bases de données individuelles.

▼ **Prérequis**

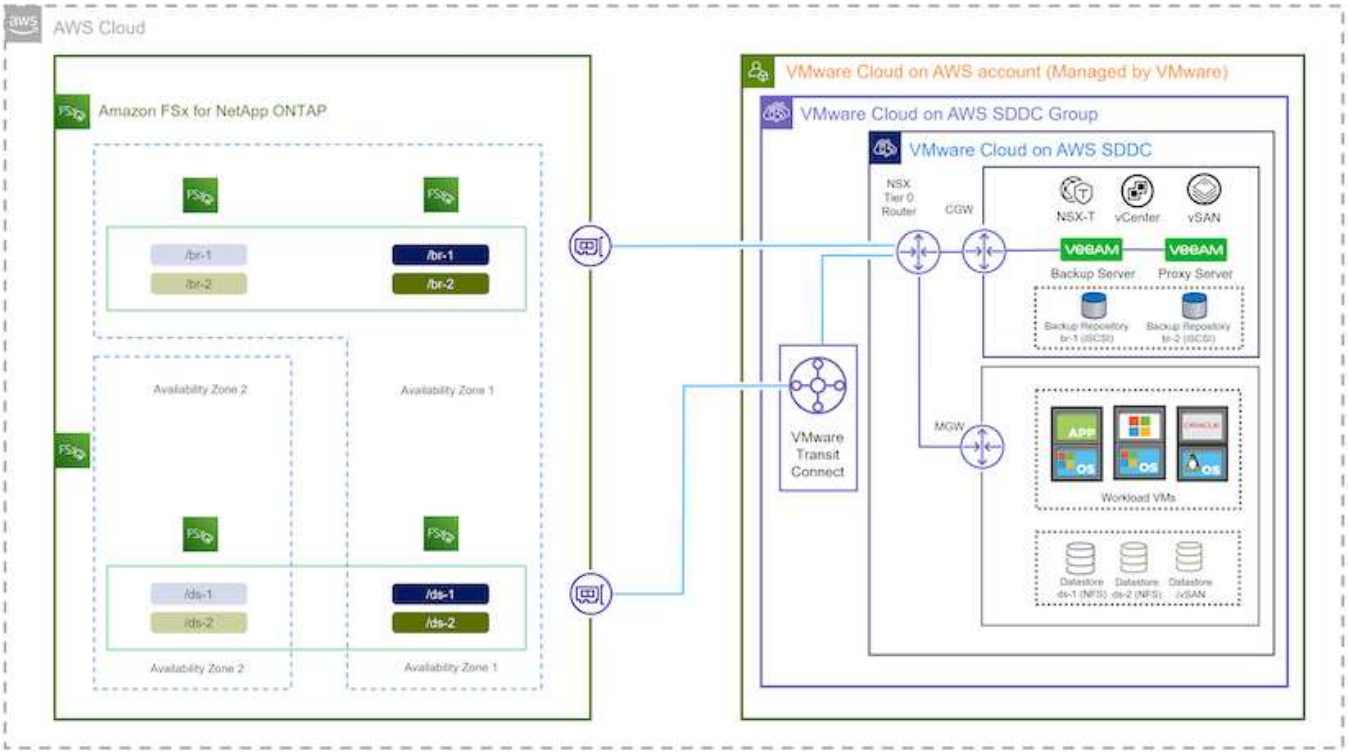
L'objectif de cette solution est de démontrer la protection des données des machines virtuelles exécutées dans VMware Cloud et situées sur des magasins de données NFS hébergés par FSx ONTAP. Cette solution suppose que les composants suivants sont configurés et prêts à l'emploi :

1. Système de fichiers FSx ONTAP avec un ou plusieurs magasins de données NFS connectés à VMware Cloud.
2. Machine virtuelle Microsoft Windows Server avec logiciel Veeam Backup & Replication installé.
    - Le serveur vCenter a été découvert par le serveur Veeam Backup & Replication à l'aide de son adresse IP ou de son nom de domaine complet.
3. Machine virtuelle Microsoft Windows Server à installer 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 des banques de données NFS FSx ONTAP . Pour cette solution, nous avions deux bases de données SQL sur deux VMDK distincts.
    - Remarque : en tant que meilleure pratique, les fichiers de base de données et les fichiers journaux de transactions sont placés sur des lecteurs séparés, car cela améliore les performances et la fiabilité. Cela est en partie dû au fait que les journaux de transactions sont écrits de manière séquentielle, tandis que les fichiers de base de données sont écrits de manière aléatoire.
5. Machines virtuelles Oracle Database avec VMDK et données d'application résidant sur des banques de données NFS FSx ONTAP .
6. Machines virtuelles de serveur de fichiers Linux et Windows avec VMDK résidant sur des banques de données NFS FSx ONTAP .
7. Veeam nécessite 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 une liste complète des exigences du port réseau, reportez-vous à la section Ports du "Guide de l'utilisateur de Veeam Backup

and Replication pour VMware vSphere" .

Architecture de haut niveau

Les tests/validations de cette solution ont été réalisés dans un laboratoire qui peut ou non correspondre à l'environnement de déploiement final. Pour plus d'informations, veuillez vous référer aux sections suivantes.



▼ **Composants matériels/logiciels**

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

- Machines virtuelles Microsoft Windows situées sur un magasin de données NFS FSx ONTAP
- Machines virtuelles Linux (CentOS) situées sur un magasin de données NFS FSx ONTAP
- Machines virtuelles Microsoft SQL Server situées sur une banque de données NFS FSx ONTAP
  - Deux bases de données hébergées sur des VMDK distincts
- Machines virtuelles Oracle situées sur un magasin de données NFS FSx ONTAP

Déploiement de la solution

Dans cette solution, nous fournissons des instructions détaillées pour le déploiement et la validation d'une solution utilisant le logiciel Veeam Backup and Replication pour effectuer la sauvegarde et la restauration des machines virtuelles de serveur de fichiers SQL Server, Oracle et Windows et Linux dans un SDDC VMware Cloud sur AWS. Les machines virtuelles de cette solution résident sur une banque de données NFS supplémentaire hébergée par FSx ONTAP. De plus, un système de fichiers FSx ONTAP distinct est utilisé pour héberger les volumes iSCSI qui seront utilisés pour les référentiels de sauvegarde Veeam.

Nous passerons en revue la création du système de fichiers FSx ONTAP , le montage de volumes iSCSI à utiliser comme référentiels de sauvegarde, la création et l'exécution de tâches de sauvegarde et la réalisation

de restaurations de machines virtuelles et de bases de données.

Pour des informations détaillées sur FSx ONTAP, reportez-vous au "Guide de l'utilisateur de FSx ONTAP" .

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

Pour connaître les considérations et les limitations lors de l'utilisation de Veeam Backup and Replication avec VMware Cloud sur AWS, reportez-vous à "Prise en charge de VMware Cloud sur AWS et VMware Cloud sur Dell EMC. Considérations et limites" .

Déployer le serveur proxy Veeam

Un serveur proxy Veeam est un composant du logiciel Veeam Backup & Replication qui agit comme 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 prendre en compte le nombre de tâches simultanées et le mode de transport ou le type d'accès au stockage souhaité.

Pour dimensionner le nombre de serveurs proxy et connaître leurs exigences système, reportez-vous à la "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 de la machine virtuelle à partir 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 banques de données NFS en utilisant l'accès direct au stockage.

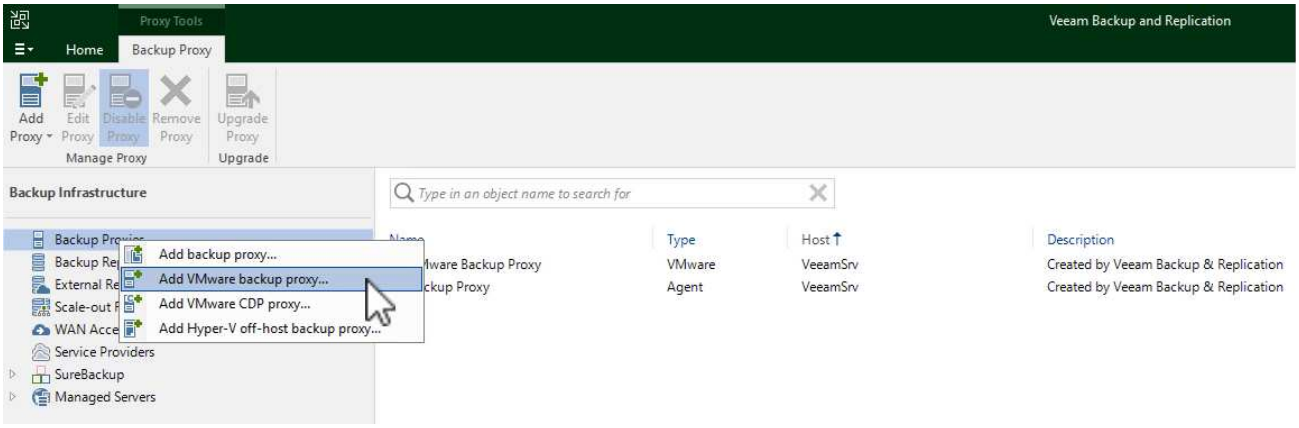
Pour plus d'informations sur les modes de transport, reportez-vous au "Guide de l'utilisateur de Veeam Backup and Replication pour VMware vSphere" .

Dans l'étape suivante, nous couvrons le déploiement du serveur proxy Veeam sur une machine virtuelle Windows dans le SDDC VMware Cloud.

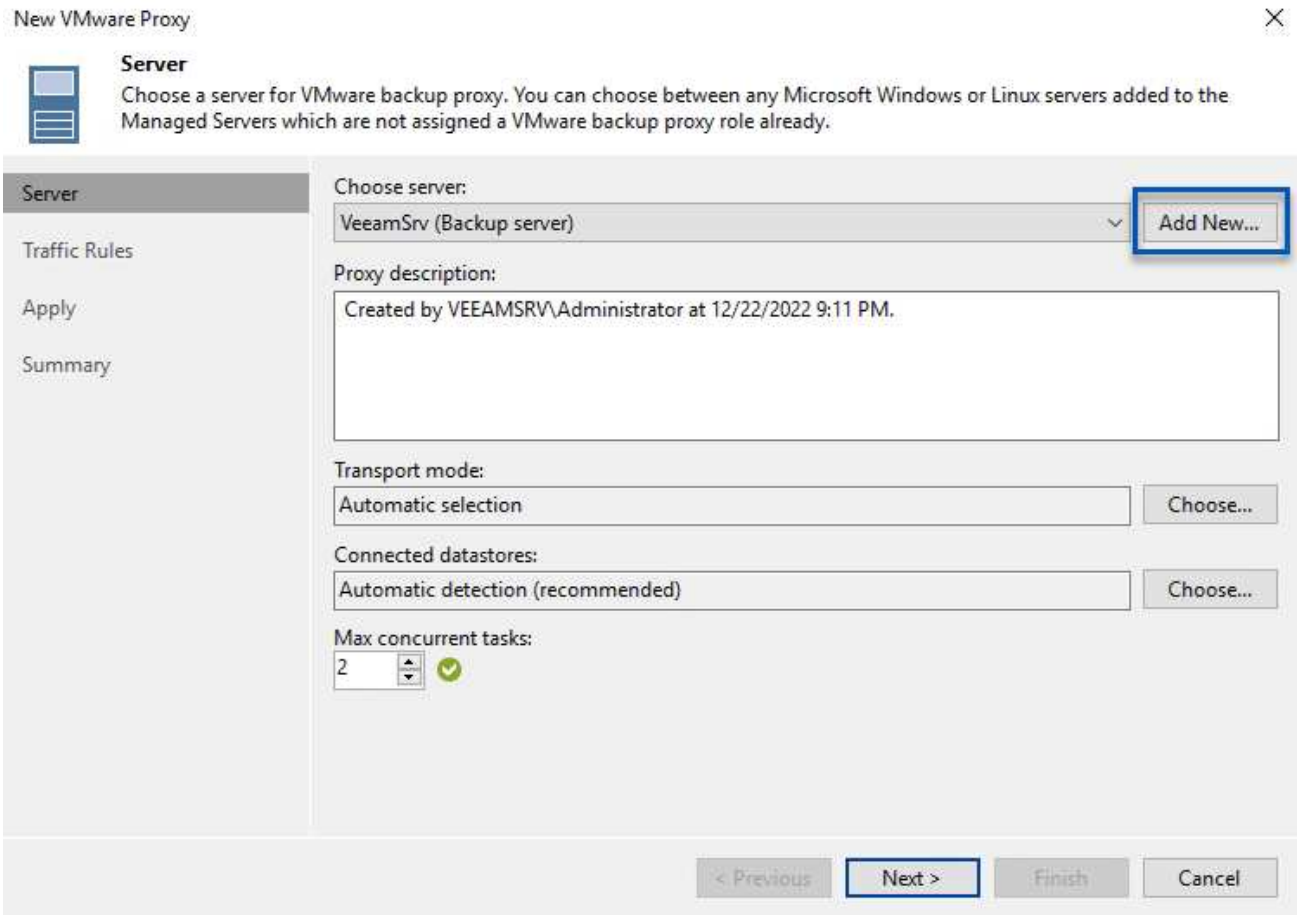
▼ **Déployer Veeam Proxy pour distribuer les charges de travail de sauvegarde**

Dans cette étape, le proxy Veeam est déployé sur une machine virtuelle Windows existante. Cela permet de distribuer les tâches de sauvegarde entre le serveur de sauvegarde Veeam principal et le proxy Veeam.

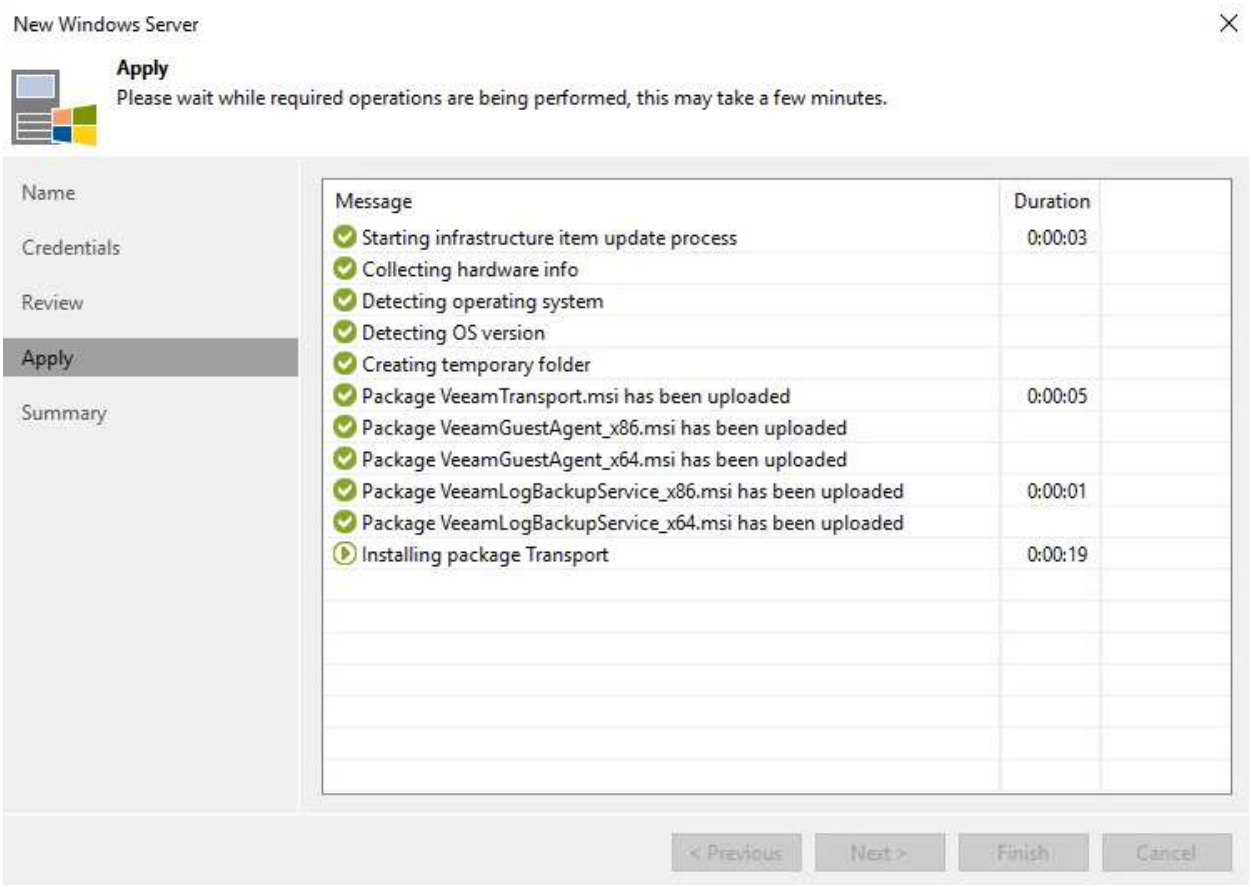
1. Sur le serveur Veeam Backup and Replication, ouvrez la console d'administration et sélectionnez **Infrastructure de sauvegarde** dans le menu inférieur gauche.
2. Faites un clic droit sur **Proxys de sauvegarde** et cliquez sur **Ajouter un proxy de sauvegarde VMware…** pour ouvrir l'assistant.



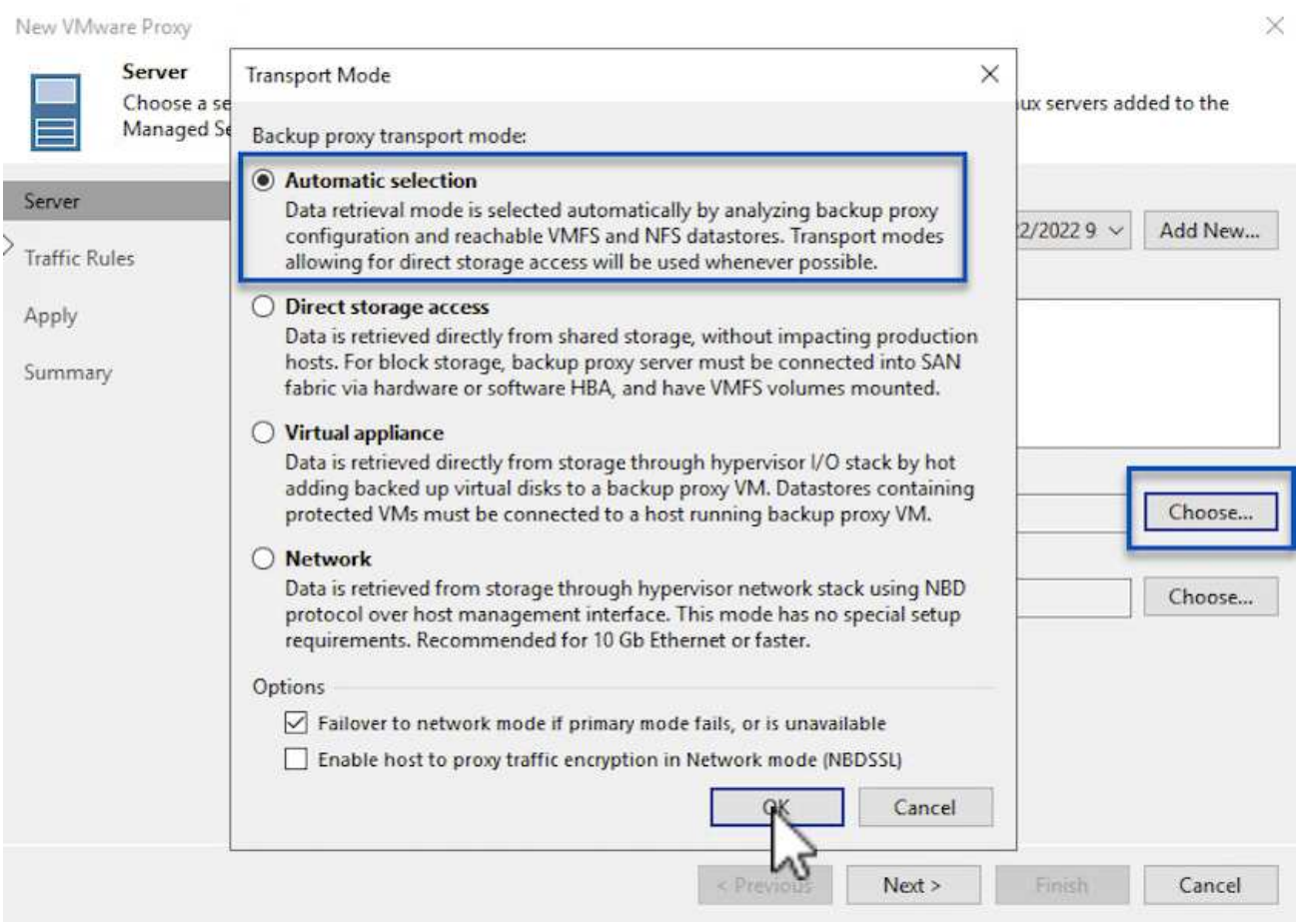
3. Dans l'assistant **Ajouter un proxy VMware**, cliquez sur le bouton **Ajouter un nouveau…** pour ajouter un nouveau serveur proxy.



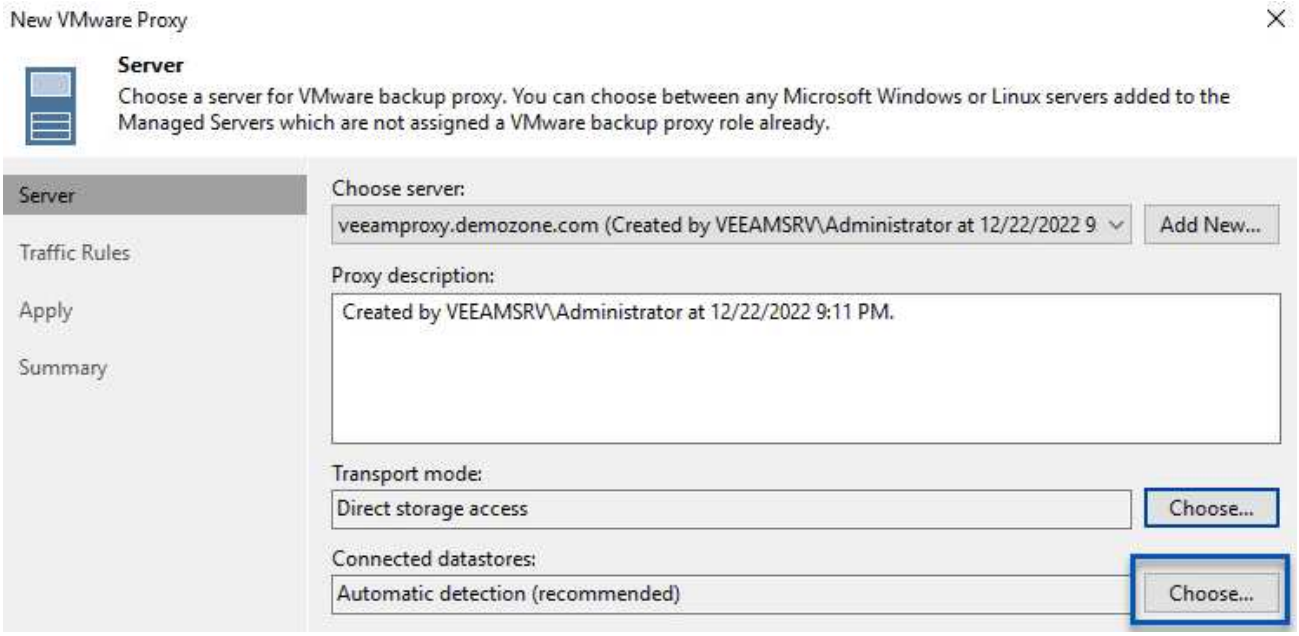
4. Sélectionnez pour ajouter Microsoft Windows et suivez les invites pour ajouter le serveur :
   - Remplissez le nom DNS ou l'adresse IP
   - Sélectionnez un compte à utiliser pour les informations d'identification sur le nouveau système ou ajoutez de nouvelles informations d'identification
   - Vérifiez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

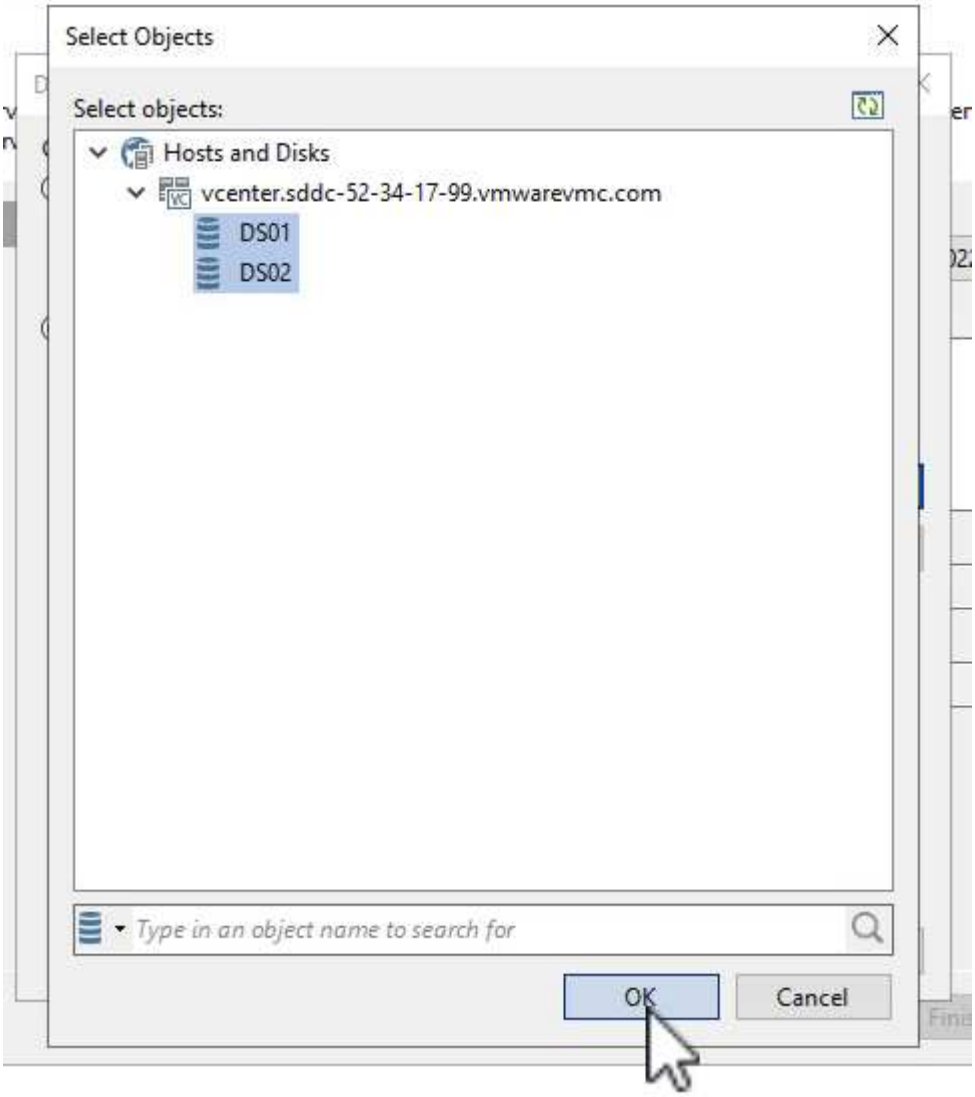


5. De retour dans l'assistant **Nouveau proxy VMware**, choisissez un mode de transport. Dans notre cas, nous avons choisi **Sélection automatique**.

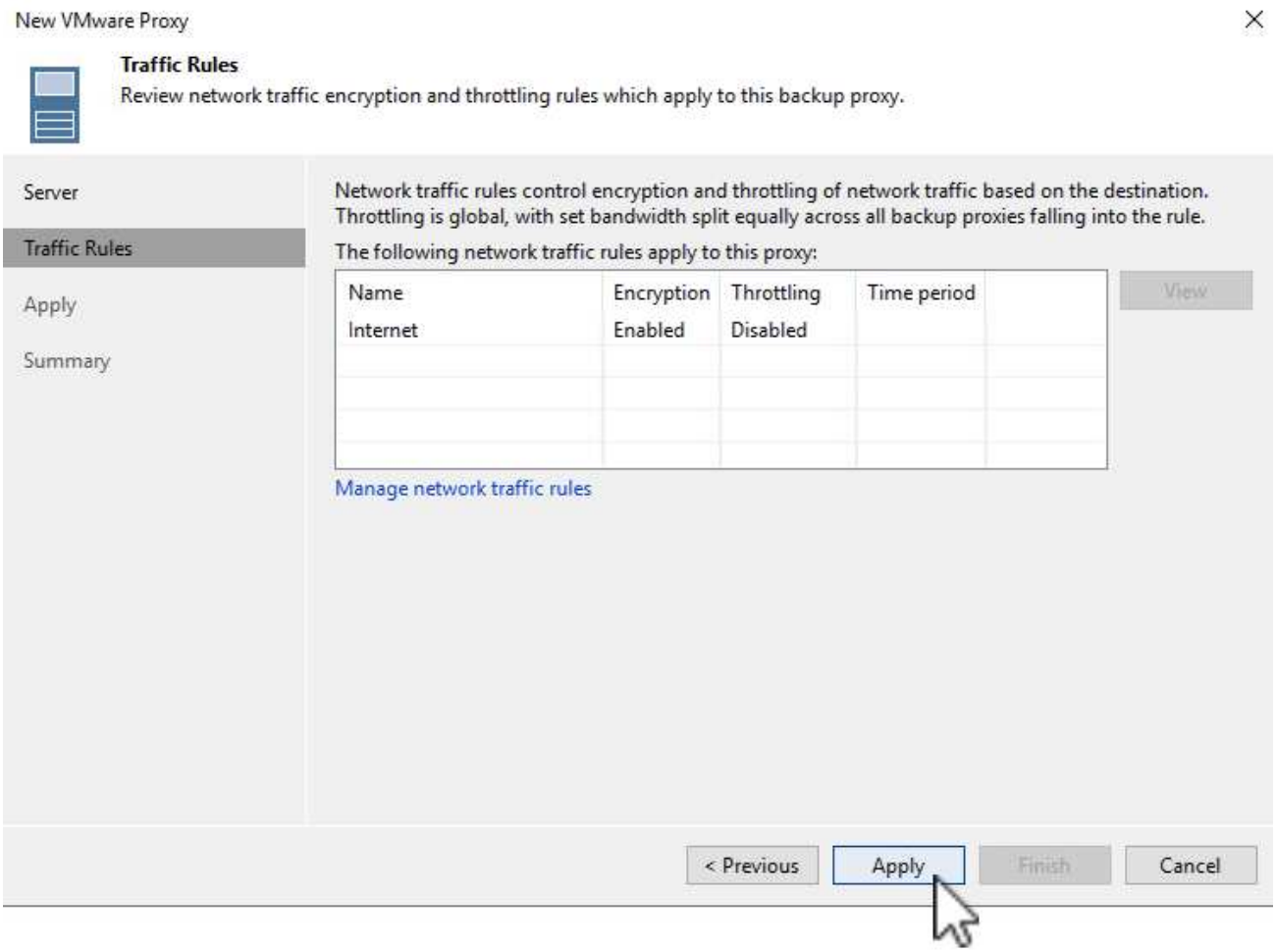


6. Sélectionnez les banques de données connectées auxquelles vous souhaitez que le proxy VMware ait un accès direct.





7. Configurez et appliquez toutes les règles de trafic réseau spécifiques souhaitées, telles que le chiffrement ou la limitation. Une fois terminé, cliquez sur le bouton **Appliquer** pour terminer le déploiement.



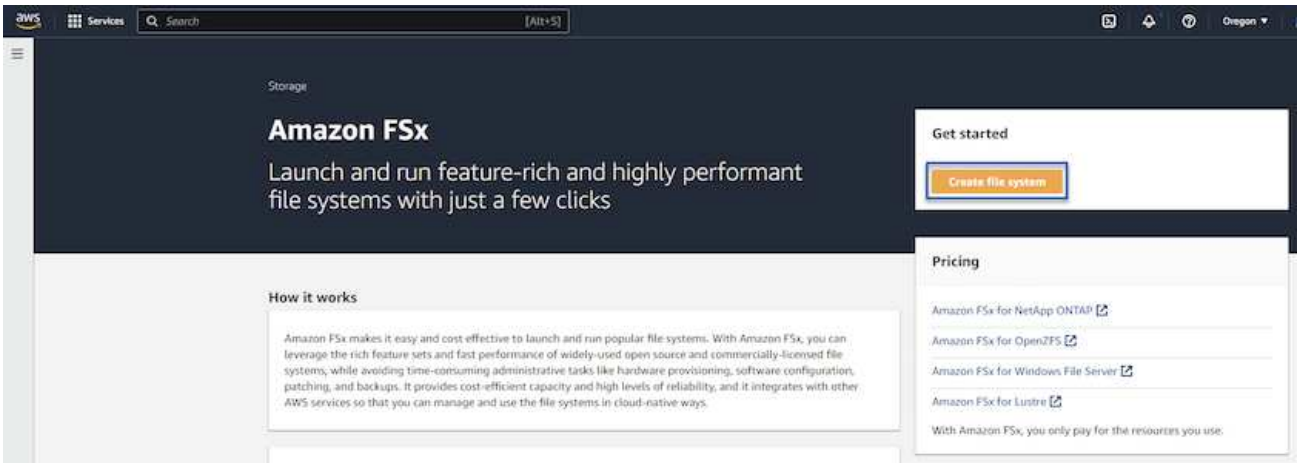
Configurer le stockage et les référentiels de sauvegarde

Le serveur principal Veeam Backup et le serveur proxy Veeam ont accès à un référentiel de sauvegarde sous la forme d'un stockage connecté directement. Dans cette section, nous abordons la création d'un système de fichiers FSx ONTAP , le montage de LUN iSCSI sur les serveurs Veeam et la création de référentiels de sauvegarde.

▼ Créer un système de fichiers FSx ONTAP

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

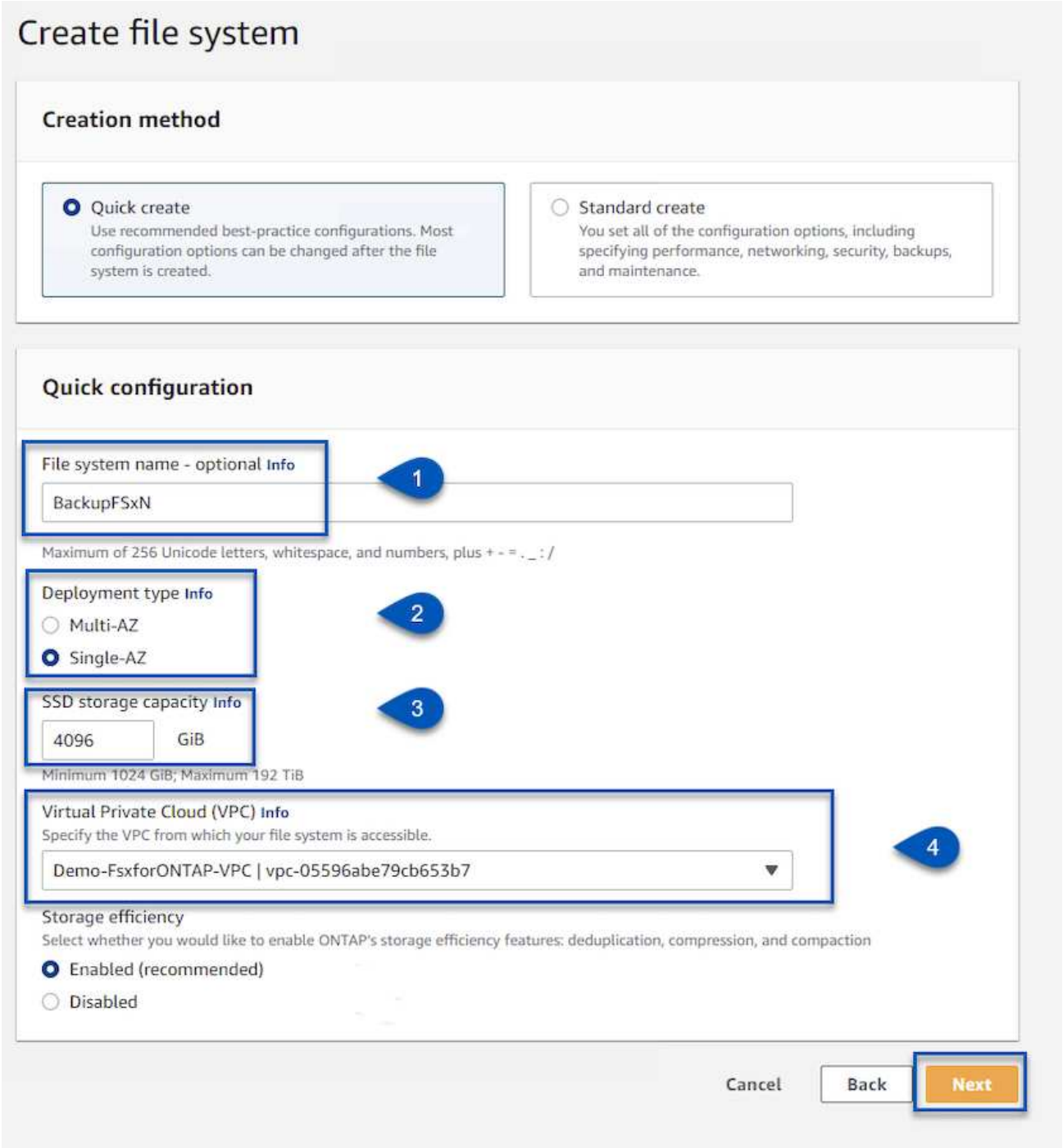
1. Dans la console AWS, accédez à FSx, puis **Créer un système de fichiers**



2. Sélectionnez * Amazon FSx 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 résidera le cluster FSx ONTAP . Il doit s'agir d'un VPC configuré pour communiquer avec le réseau de 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 commencer le processus de création du système de fichiers.

▼ **Configurer et monter des LUN iSCSI**

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

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

ⓘ Pour plus d'informations sur l'utilisation de FSx ONTAP, consultez le "Guide de l'utilisateur de

FSx ONTAP" .

1. À partir de la CLI NetApp ONTAP, créez 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 à l'aide des 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. Accordez l'accès aux LUN en créant un groupe d'initiateurs contenant l'IQN iSCSI des serveurs de sauvegarde et proxy Veeam :

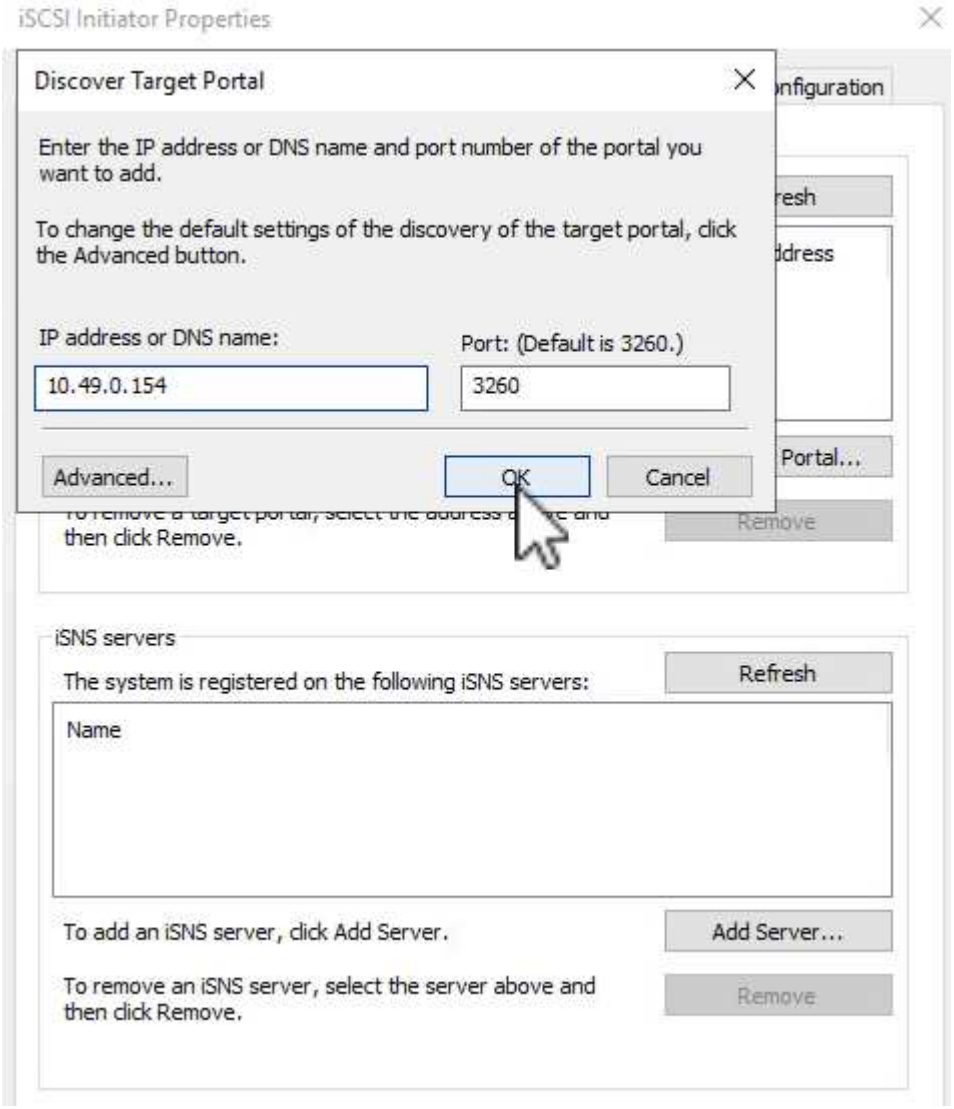
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

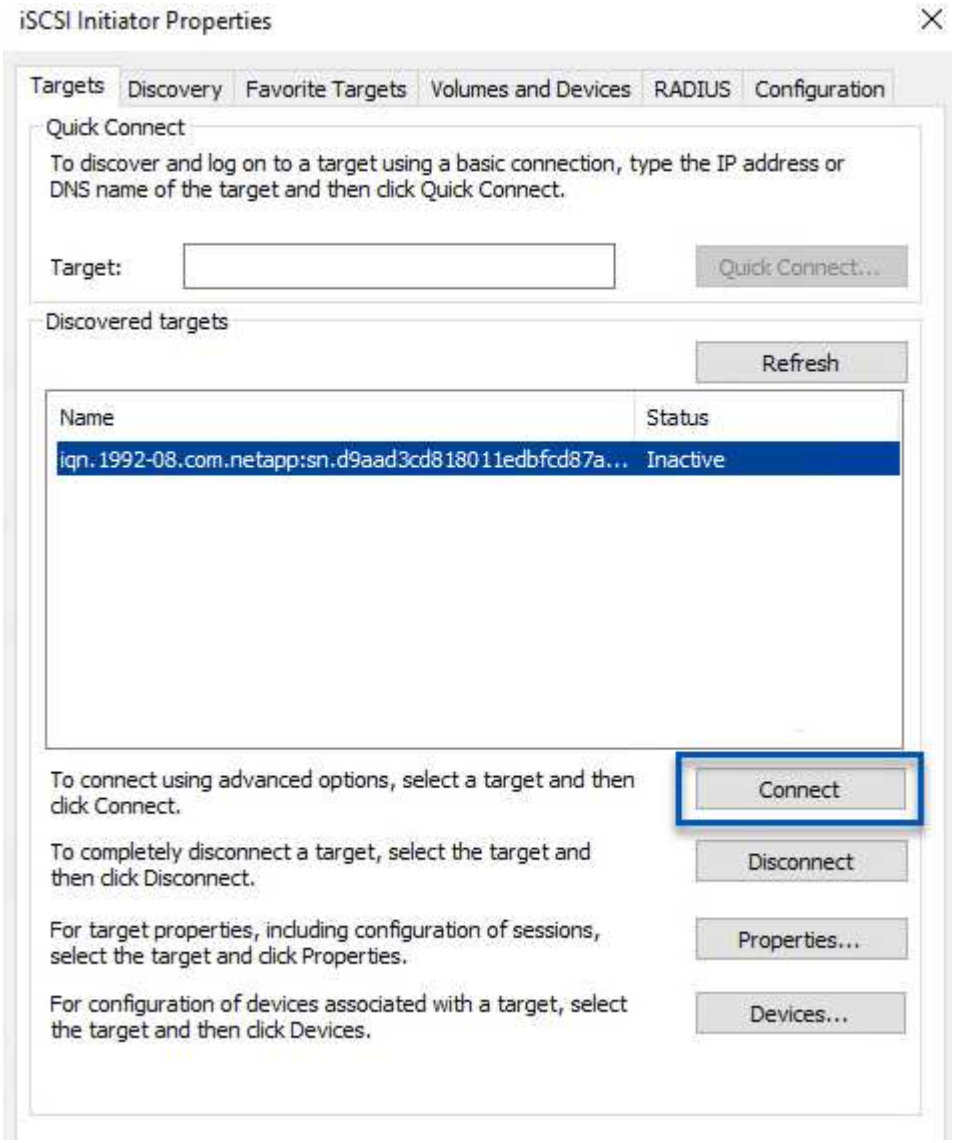
4. Enfin, mappez les LUN au groupe initiateur que vous venez de créer :

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

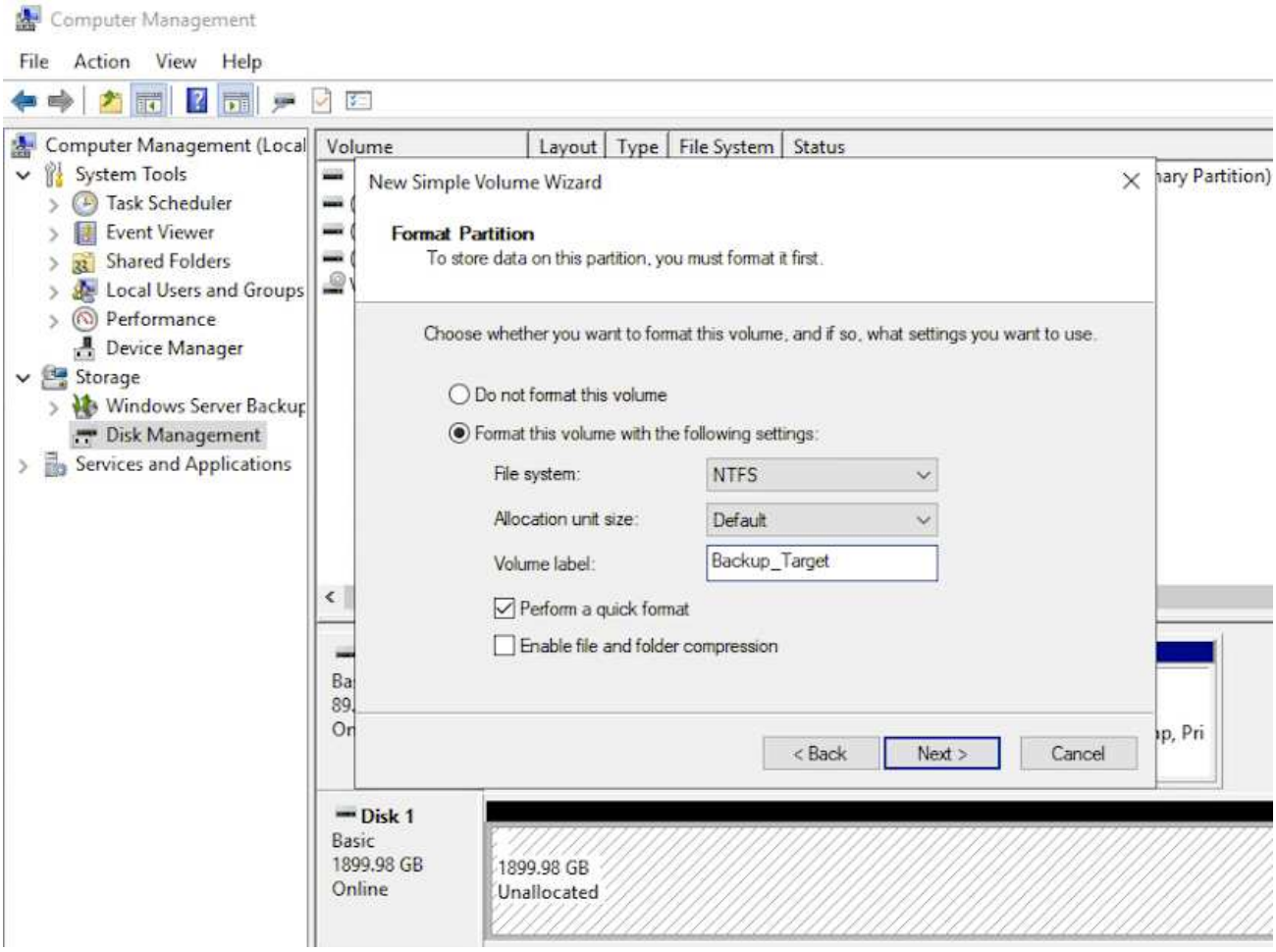
5. Pour monter les LUN iSCSI, connectez-vous au serveur Veeam Backup & Replication et ouvrez les propriétés de l'initiateur iSCSI. Accédez à l'onglet **Découvrir** et saisissez l'adresse IP cible iSCSI.



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



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

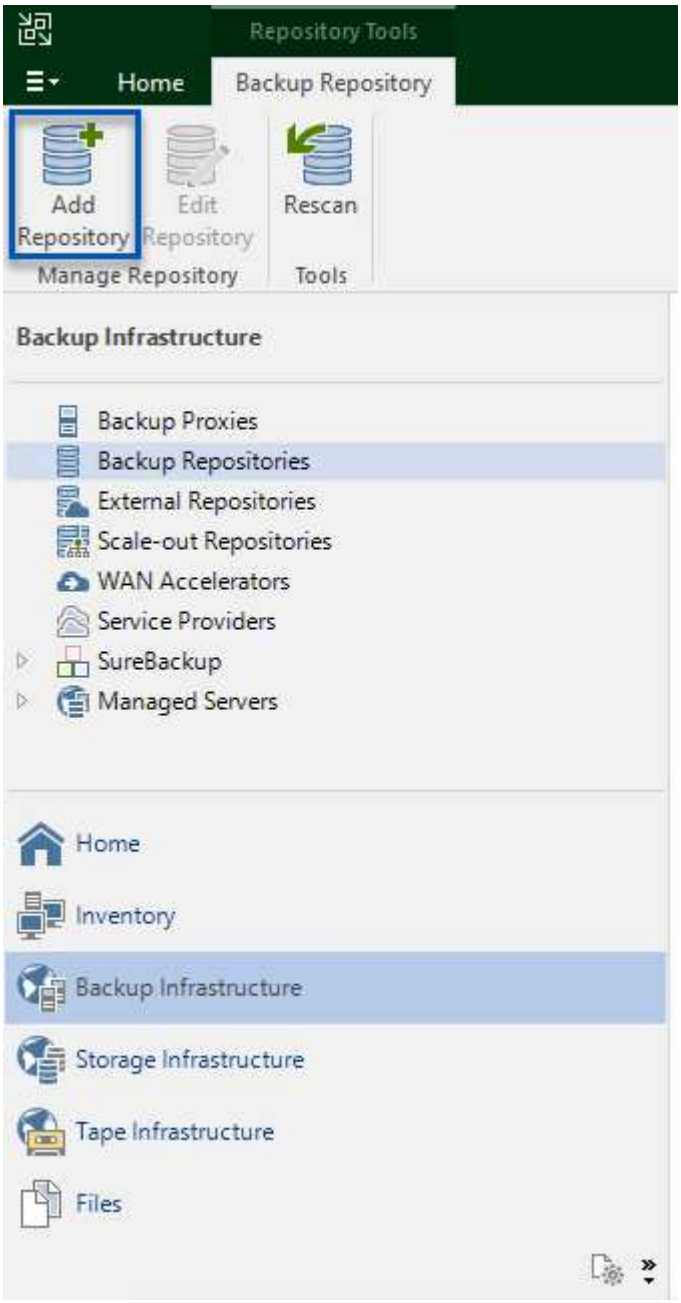


8. Répétez ces étapes pour monter les volumes iSCSI sur le serveur proxy Veeam.

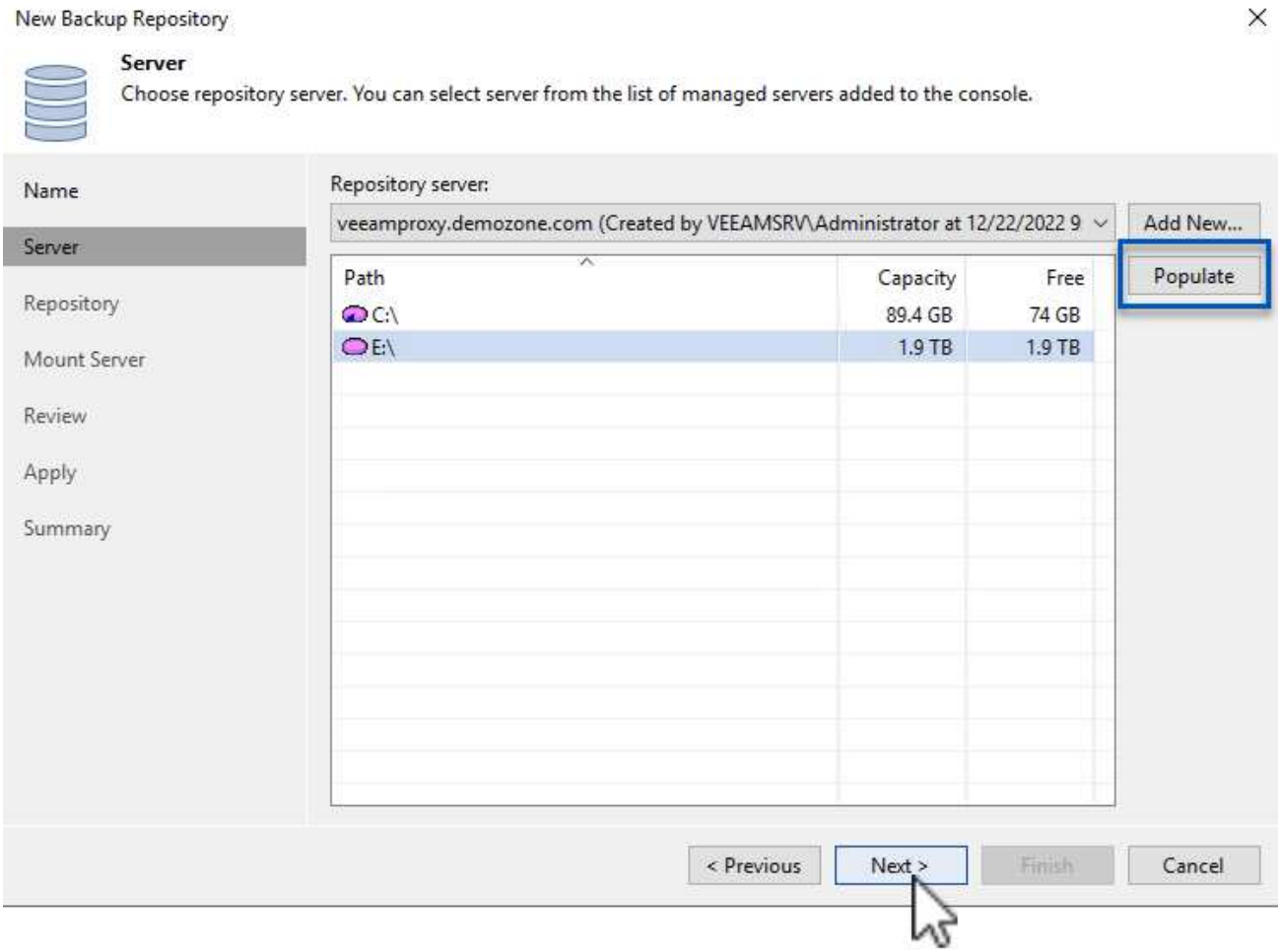
▼ **Créer des référentiels de sauvegarde Veeam**

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.

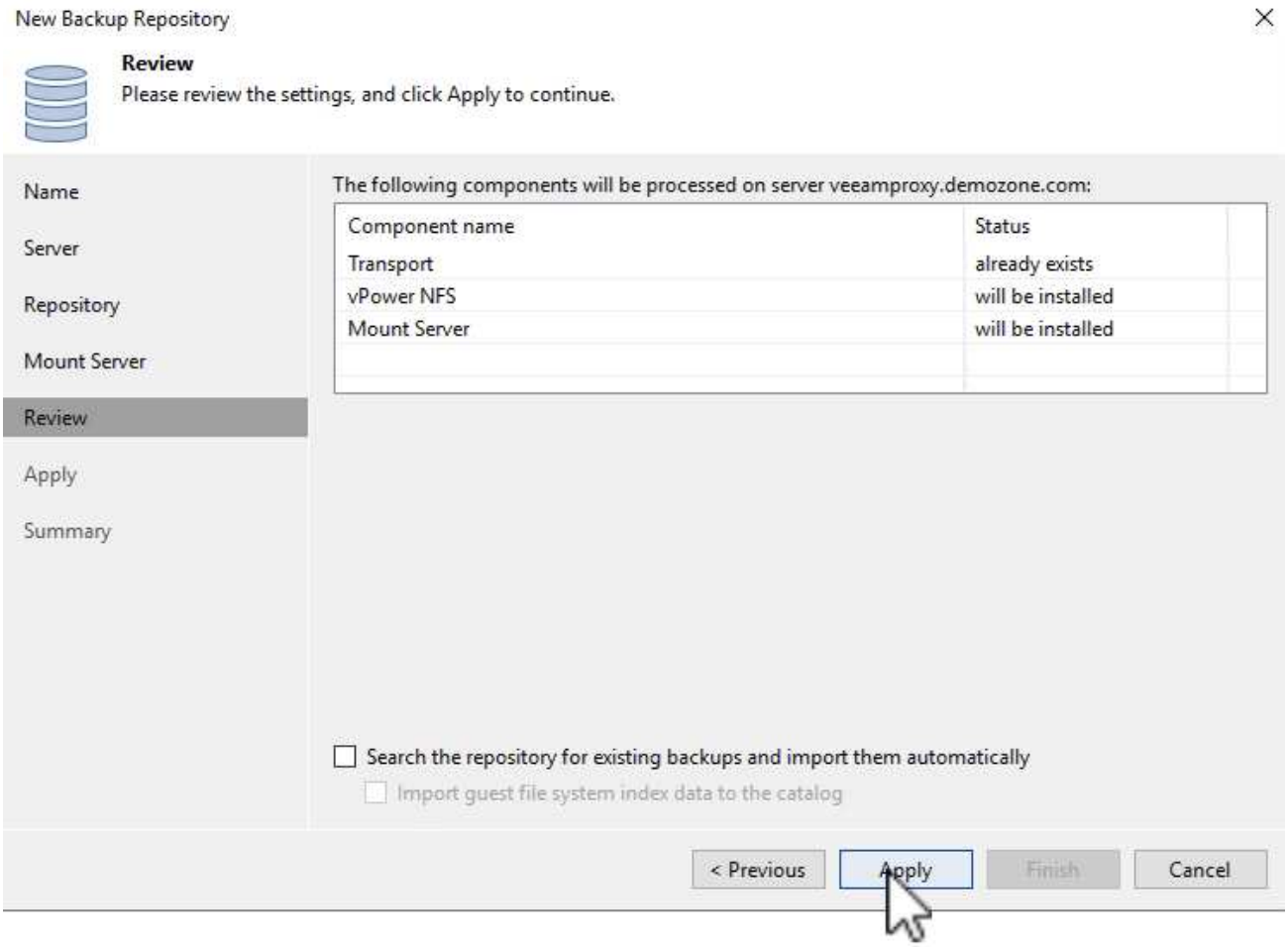
1. Dans la console Veeam Backup and Replication, cliquez sur **Infrastructure de sauvegarde** en bas à gauche, puis sélectionnez **Ajouter un référentiel**



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 **Remplir** pour choisir le volume NTFS qui sera utilisé.



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



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

Configurer les tâches de sauvegarde Veeam

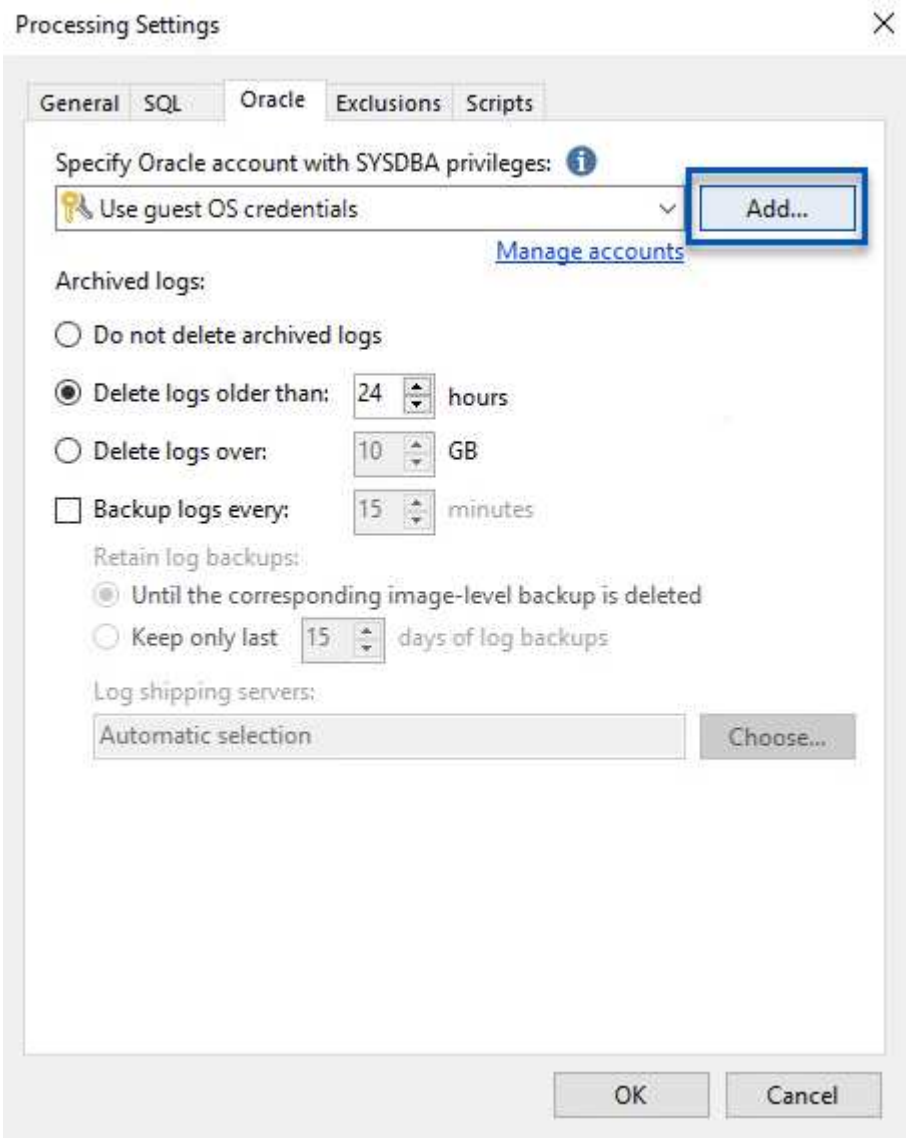
Les tâches de sauvegarde doivent être créées à l'aide des référentiels de sauvegarde de la section précédente. La création de tâches de sauvegarde fait partie intégrante du répertoire de tout administrateur de stockage et nous ne couvrons pas toutes les étapes ici. Pour des informations plus complètes 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 :

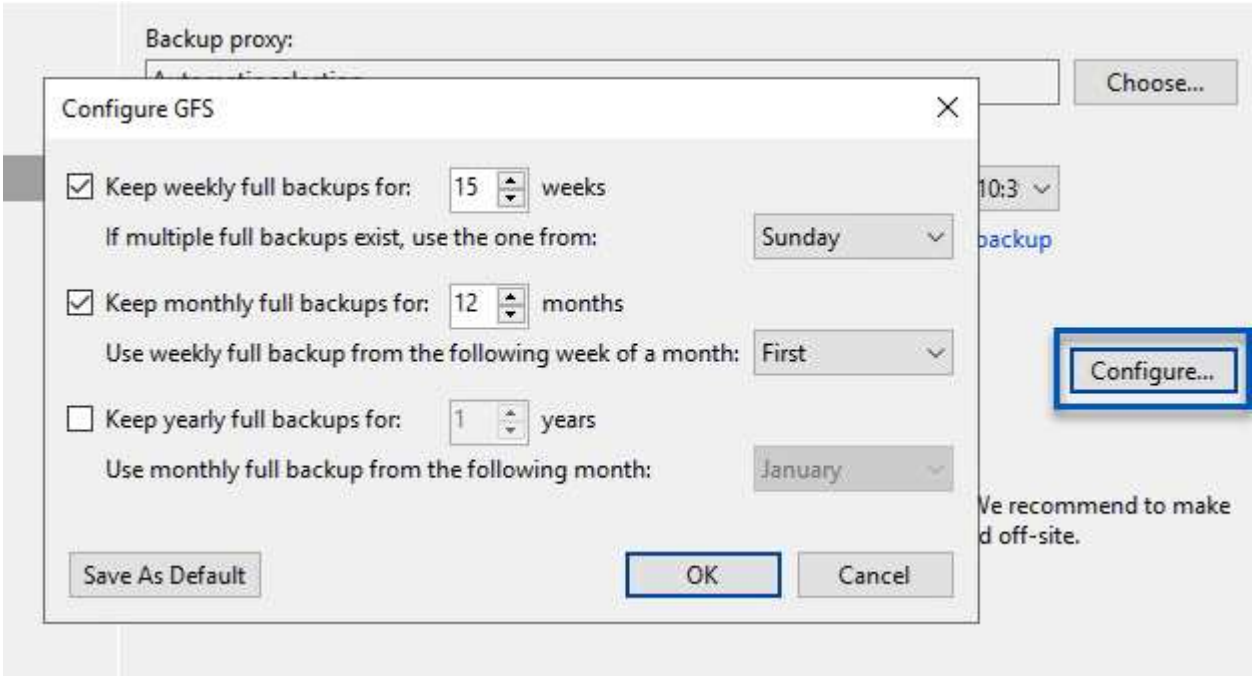
- Serveurs Microsoft Windows SQL
- Serveurs de bases de données Oracle
- Serveurs de fichiers Windows
- Serveurs de fichiers Linux

▼ Considérations générales lors de la configuration des tâches de sauvegarde Veeam

1. Activez le traitement sensible aux applications pour créer des sauvegardes cohérentes et effectuer le traitement du journal des transactions.
2. Après avoir activé le traitement prenant en charge 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 politique de conservation de 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 politique.



Restaurer les machines virtuelles d'application avec la restauration complète de Veeam

L'exécution d'une restauration complète avec Veeam est la première étape de la restauration d'une application. Nous avons validé que les restaurations complètes de nos machines virtuelles étaient sous tension et que tous les services fonctionnaient normalement.

La restauration des serveurs fait partie intégrante du répertoire de tout administrateur de stockage et nous ne couvrons pas toutes les étapes ici. Pour des informations plus complètes sur l'exécution de restaurations complètes dans Veeam, consultez le "Documentation technique du centre d'aide Veeam" .

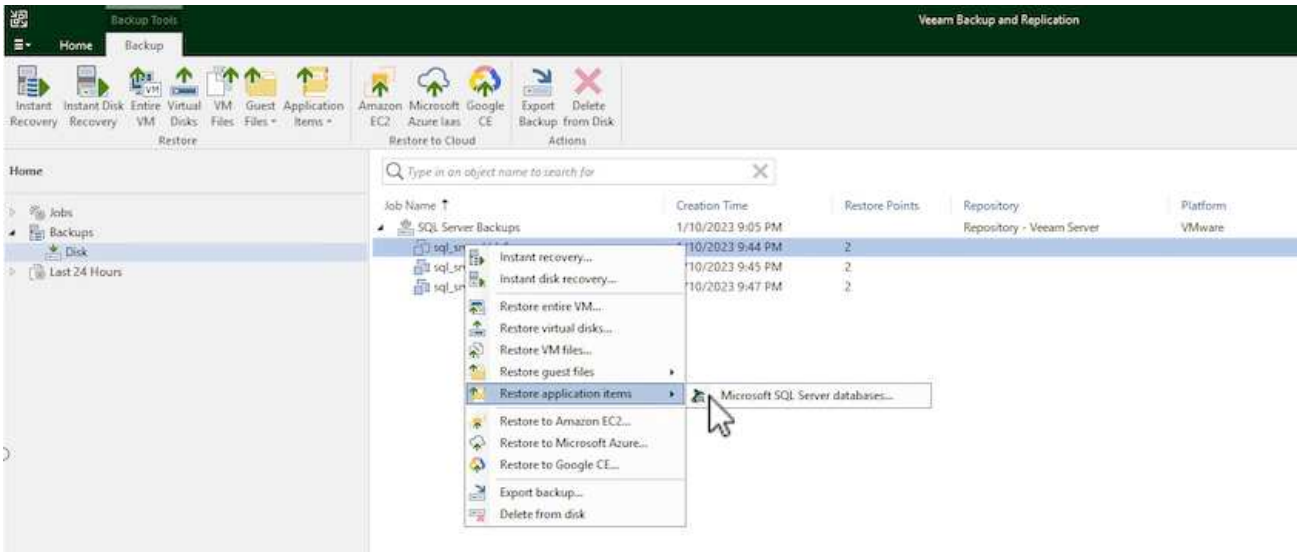
Restaurer les bases de données SQL Server

Veeam Backup & Replication propose plusieurs options pour restaurer les bases de données SQL Server. Pour cette validation, nous avons utilisé Veeam Explorer pour SQL Server avec récupération instantanée 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 une restauration complète de la base de données. Ce processus de récupération rapide minimise les temps d'arrêt et garantit la continuité des activités. Voici comment cela fonctionne :

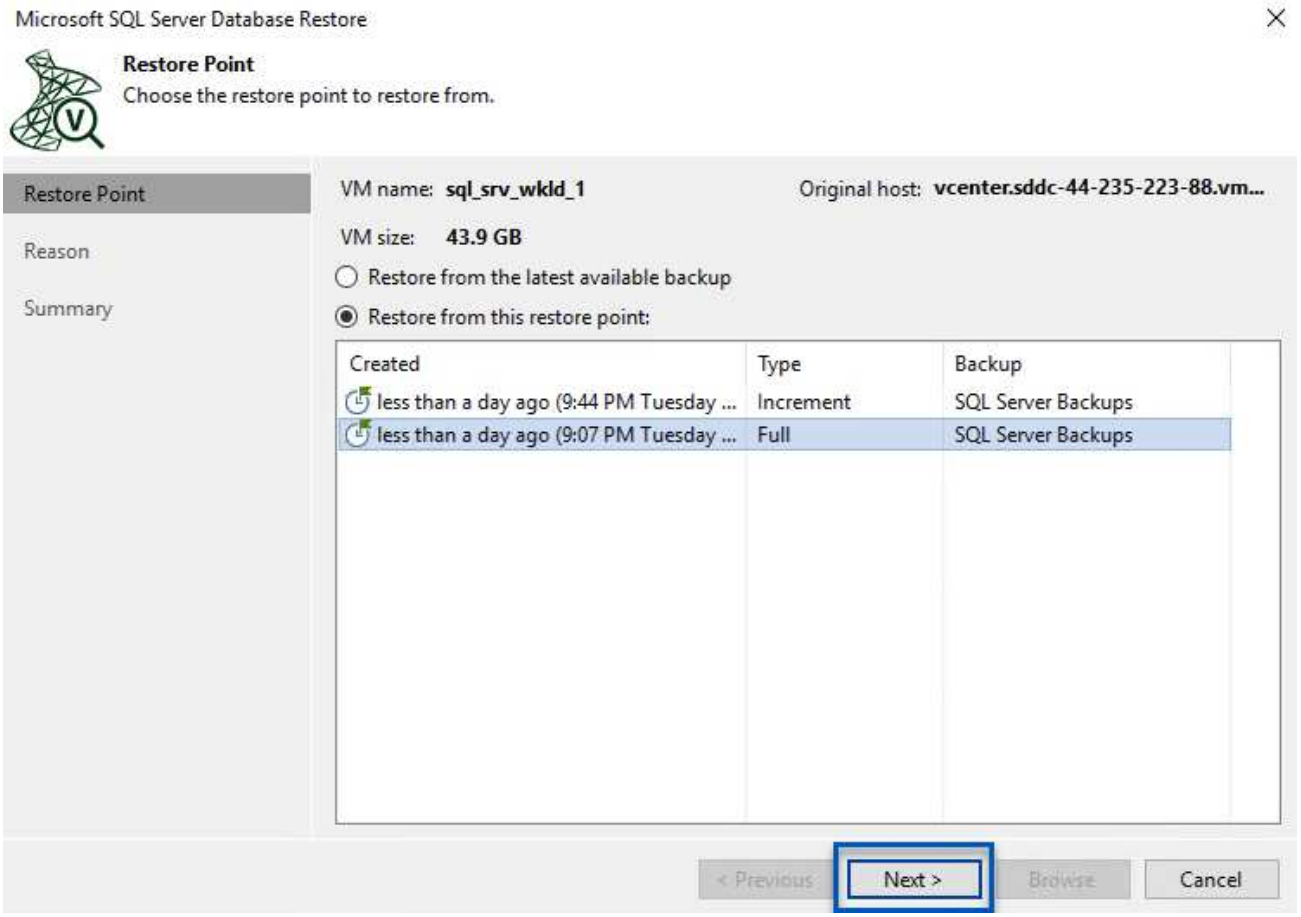
- Veeam Explorer **monte la sauvegarde** contenant la base de données SQL Server à restaurer.
- Le logiciel **publie la base de données** directement à partir des fichiers montés, la rendant accessible en tant que base de données temporaire sur l'instance SQL Server cible.
- Pendant que la base de données temporaire est utilisée, Veeam Explorer **redirige les requêtes des utilisateurs** vers cette base de données, garantissant ainsi que les utilisateurs peuvent continuer à accéder aux données et à travailler avec elles.
- 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 de la base de données d'origine.
- Une fois la restauration complète de la base de données terminée, Veeam Explorer **rétablit les requêtes utilisateur vers la base de données d'origine** et supprime la base de données temporaire.

▼ Restaurer la base de données SQL Server avec Veeam Explorer Instant Recovery

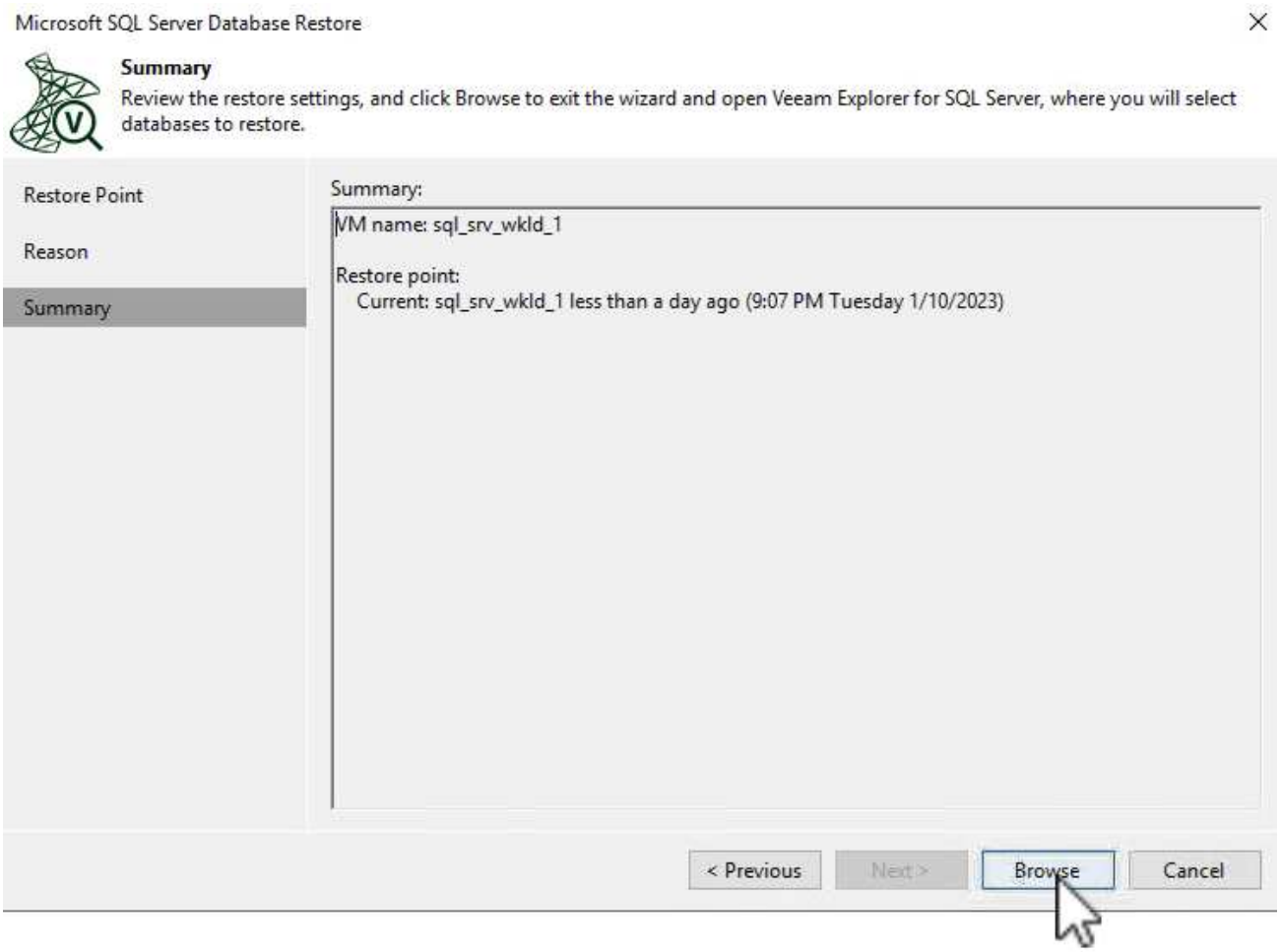
1. Dans la console Veeam Backup and Replication, accédez à la liste des sauvegardes SQL Server, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments d'application**, puis **Bases de données Microsoft SQL Server…**.



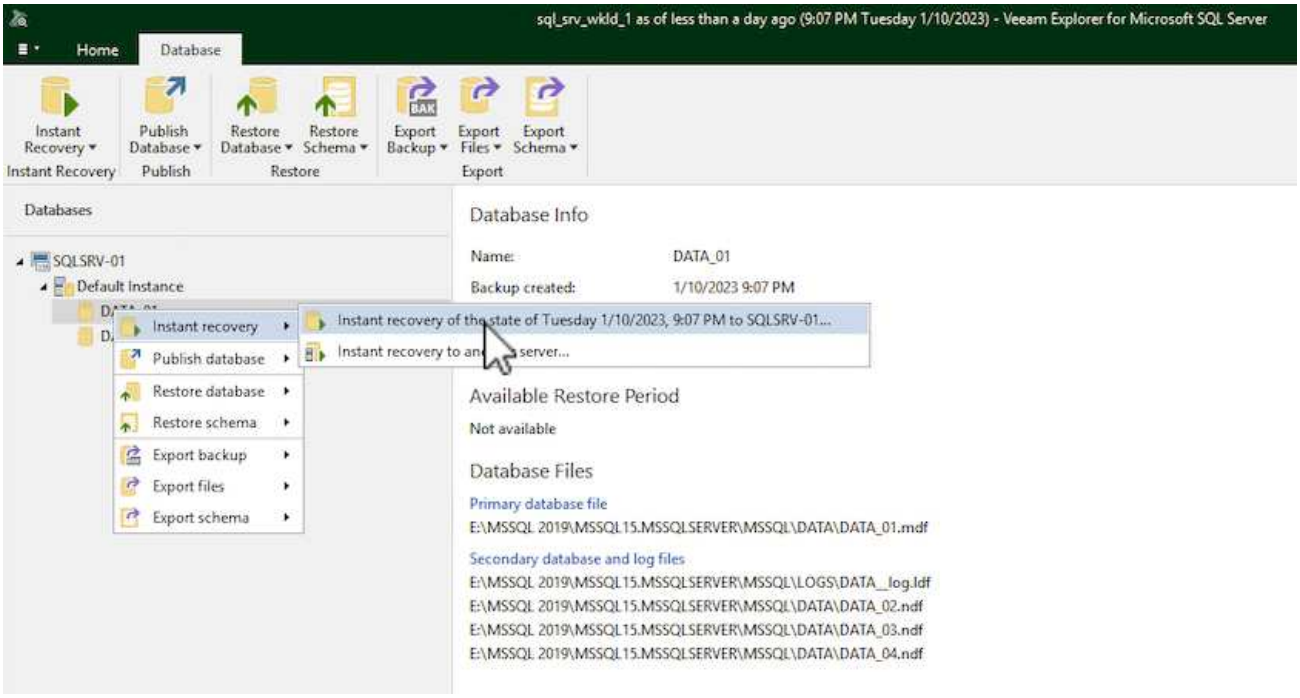
2. Dans l'assistant de restauration de base de données Microsoft SQL Server, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.



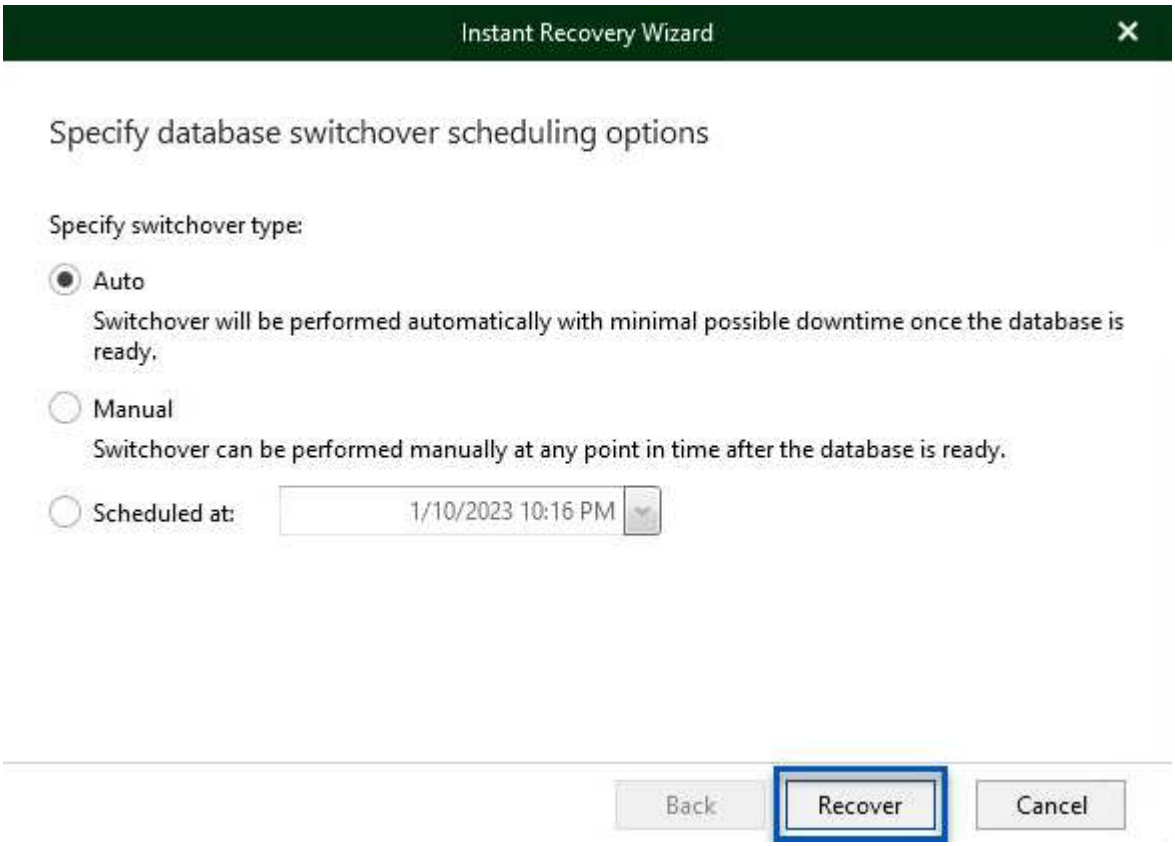
3. Saisissez une **Raison de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer pour Microsoft SQL Server.



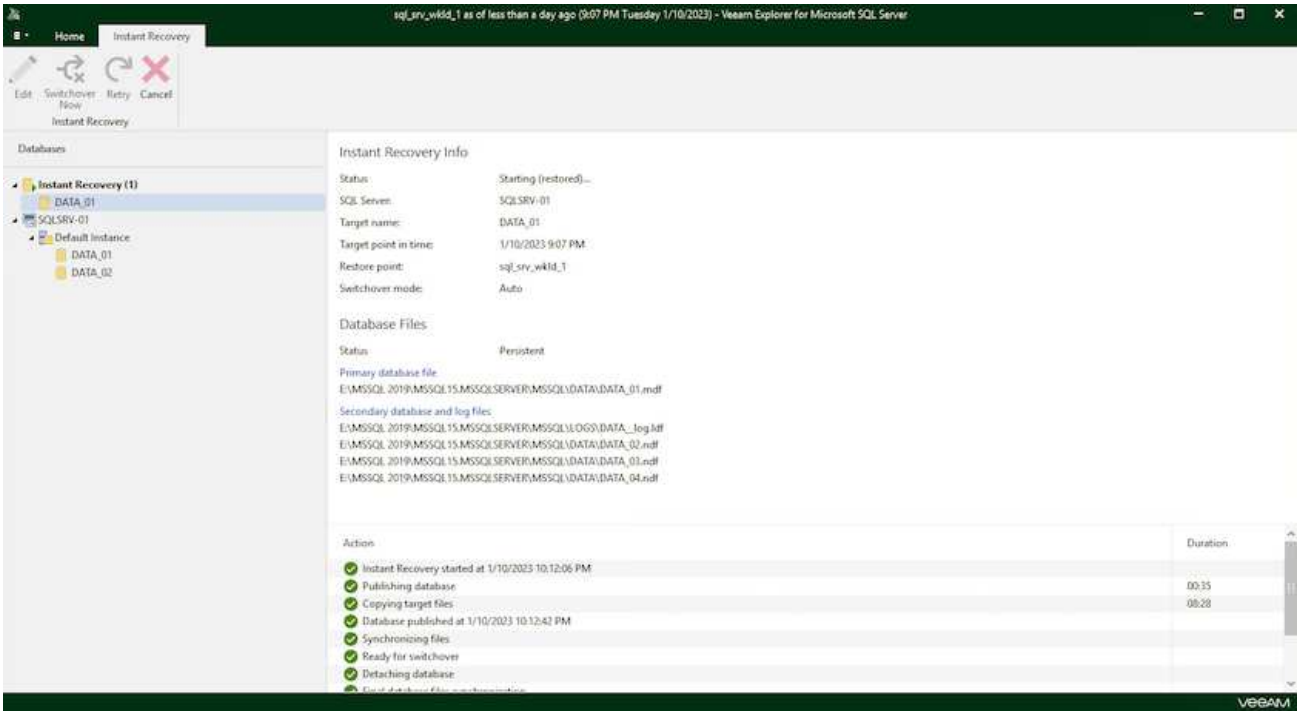
4. Dans Veeam Explorer, développez la liste des instances de base de données, faites un clic droit et sélectionnez **Récupération instantanée**, puis le point de restauration spécifique vers lequel effectuer la récupération.



5. Dans l'assistant de récupération instantanée, spécifiez le type de basculement. Cela peut être fait automatiquement avec un temps d'arrêt minimal, manuellement ou à une heure spécifiée. Cliquez ensuite sur le bouton **Récupérer** pour lancer le processus de restauration.



6. Le processus de récupération peut être surveillé à partir de Veeam Explorer.



Pour des informations plus détaillées sur l'exécution des opérations de restauration SQL Server avec Veeam

Explorer, reportez-vous à la section Microsoft SQL Server dans le "Guide de l'utilisateur de Veeam Explorers" .

Restaurer les bases de données Oracle avec Veeam Explorer

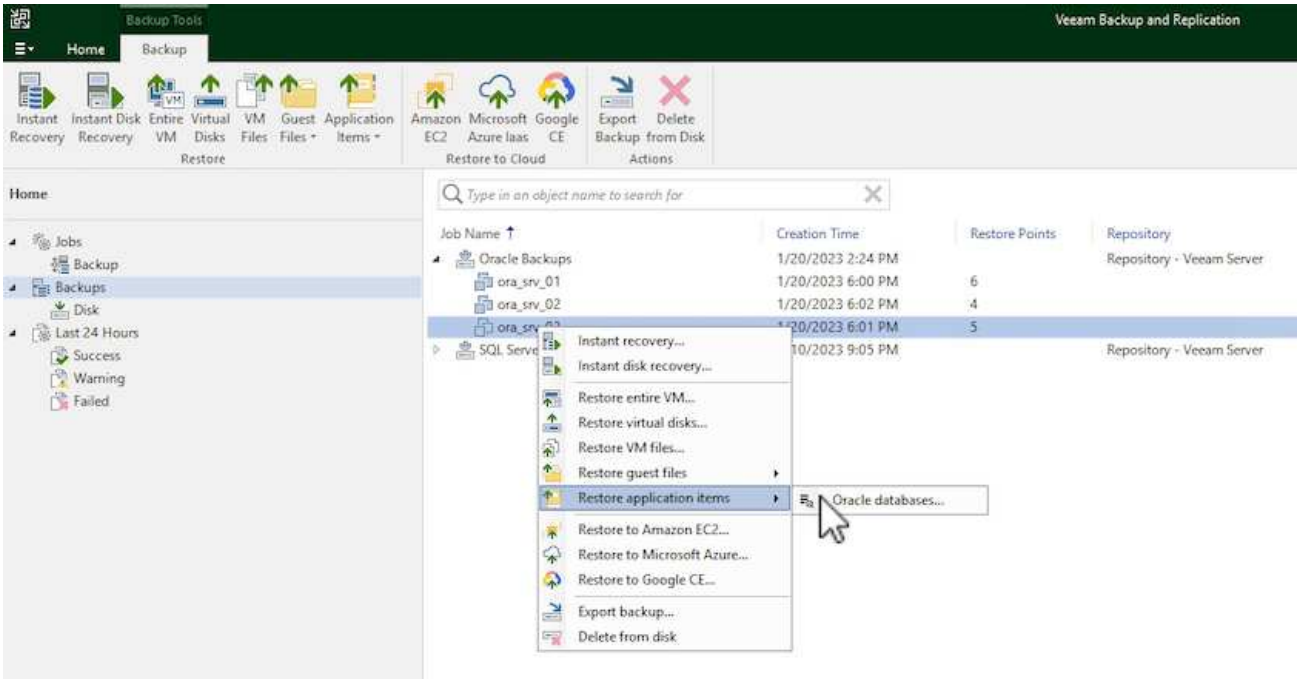
Veeam Explorer pour la base de données Oracle offre la possibilité d'effectuer une restauration de base de données Oracle standard ou une restauration ininterrompue à l'aide de la récupération instantanée. Il prend également en charge la publication de bases de données pour un accès rapide, la récupération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

Pour des informations plus détaillées sur l'exécution des opérations de restauration de base de données Oracle avec Veeam Explorer, reportez-vous à la section Oracle du "Guide de l'utilisateur de Veeam Explorers" .

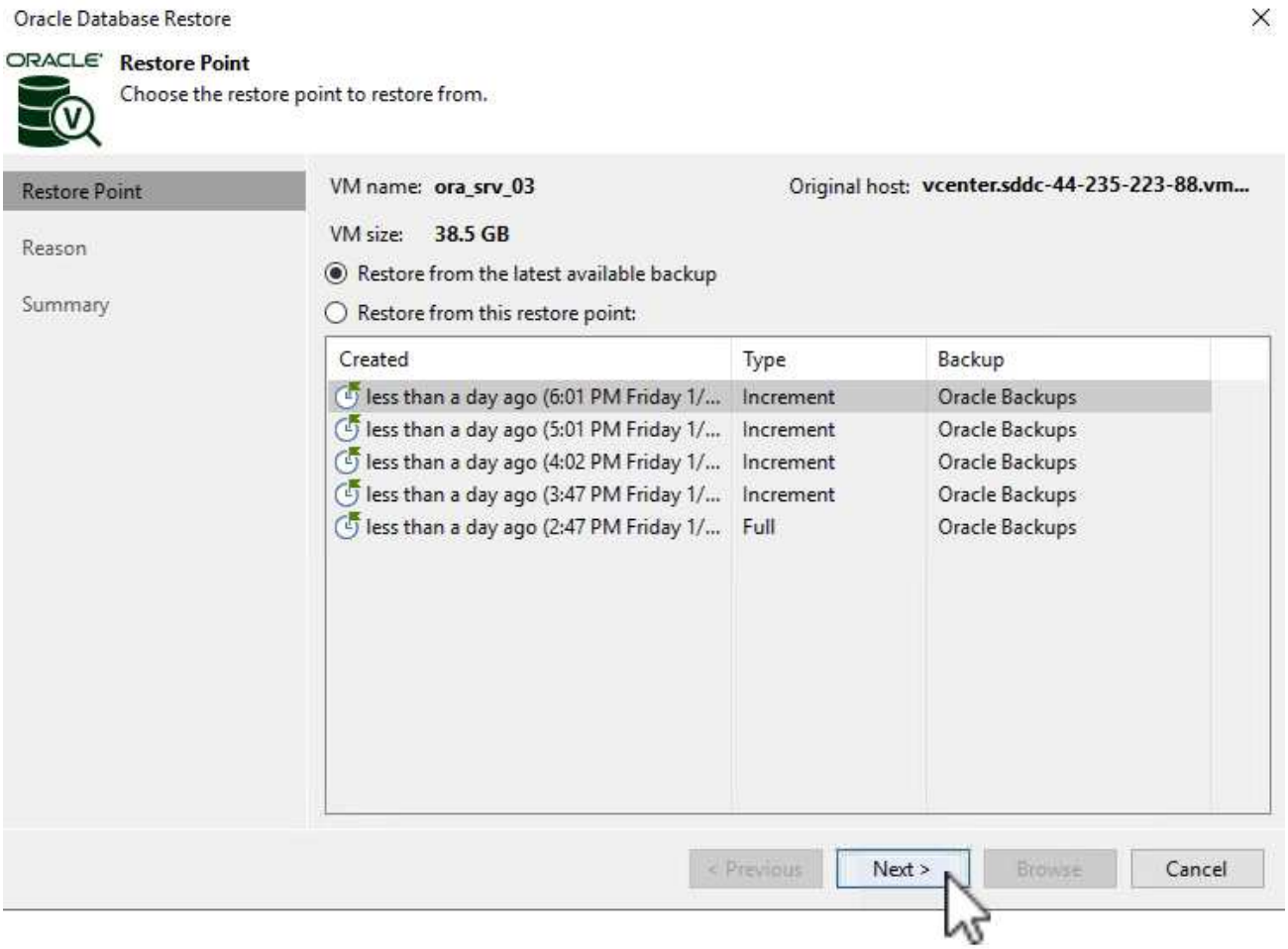
▼ **Restaurer la base de données Oracle avec Veeam Explorer**

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

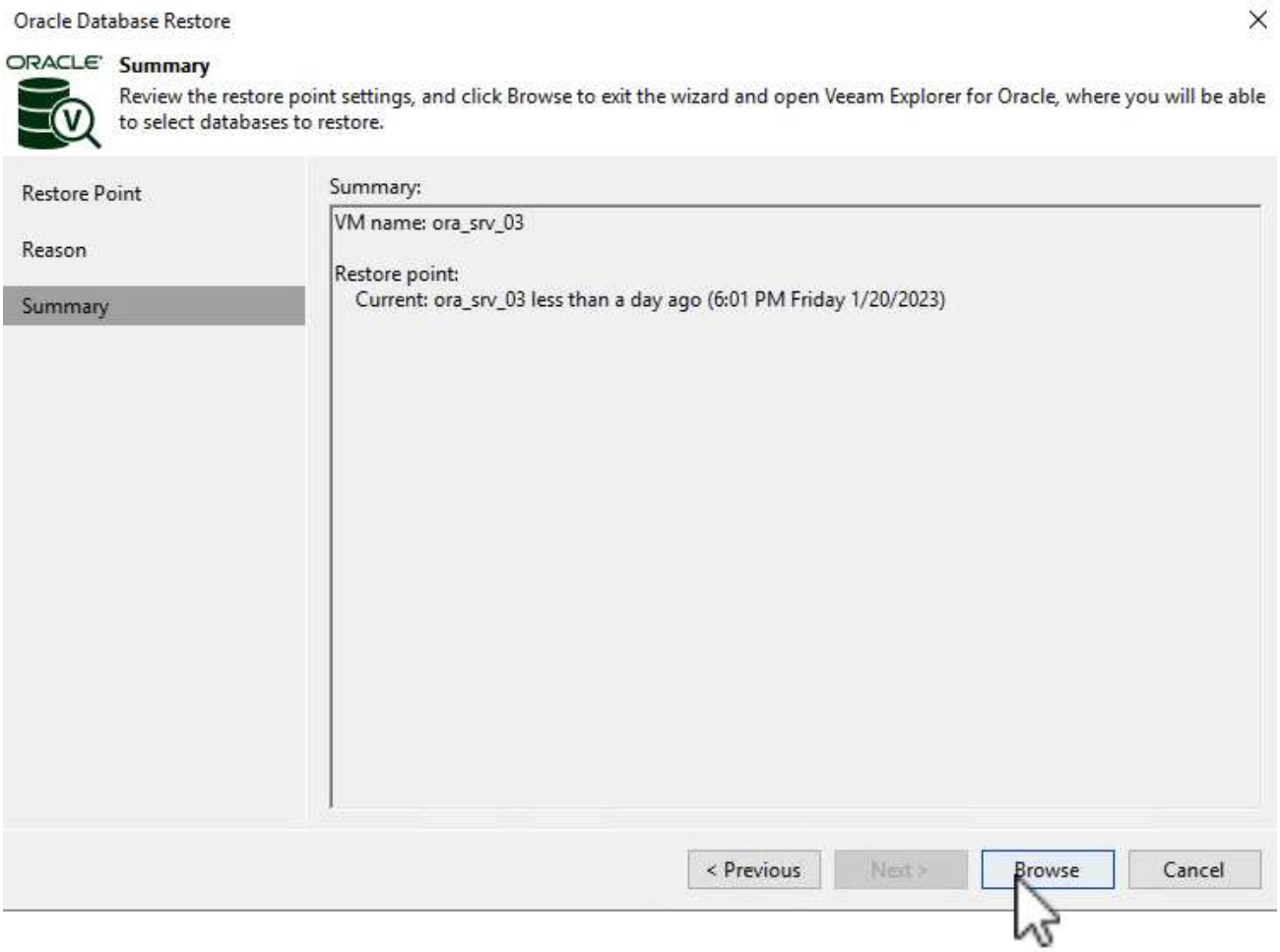
1. Dans la console Veeam Backup and Replication, accédez à la liste des sauvegardes Oracle, cliquez avec le bouton droit sur un serveur et sélectionnez **Restaurer les éléments d'application**, puis **Bases de données Oracle…**.



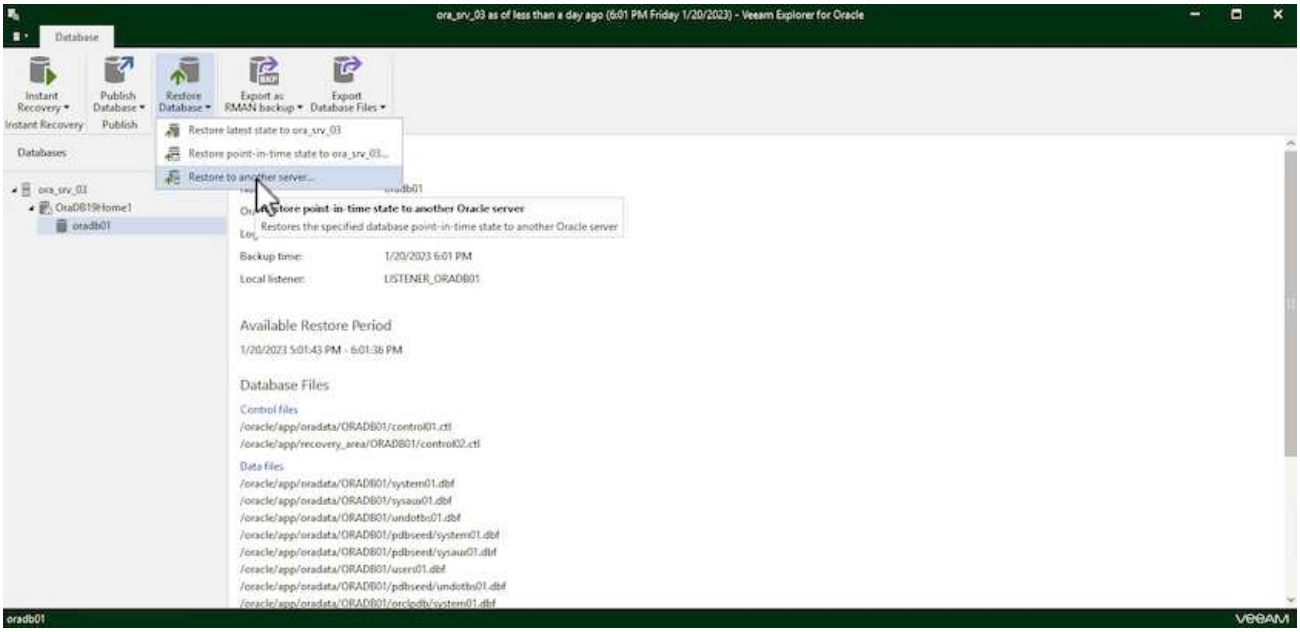
2. Dans l'assistant de restauration de base de données Oracle, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.



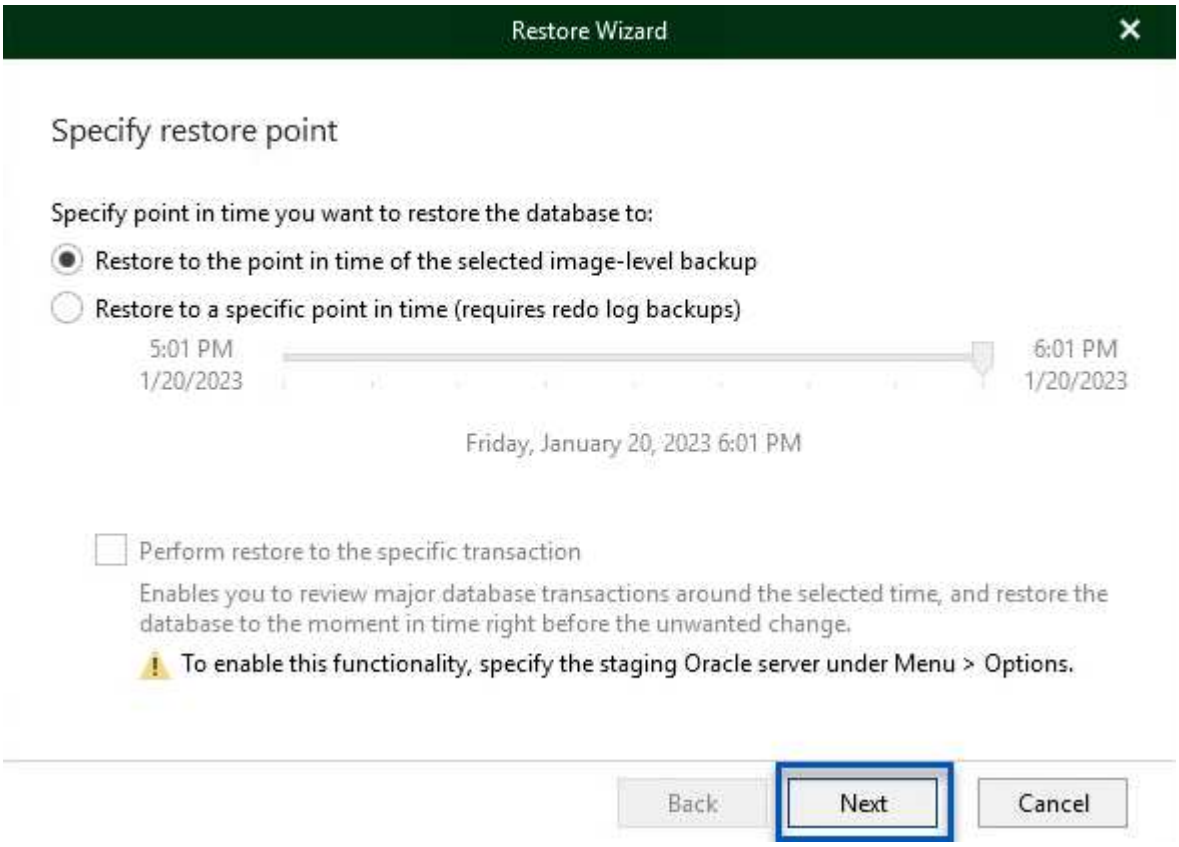
3. Saisissez une **raison de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer pour Oracle.



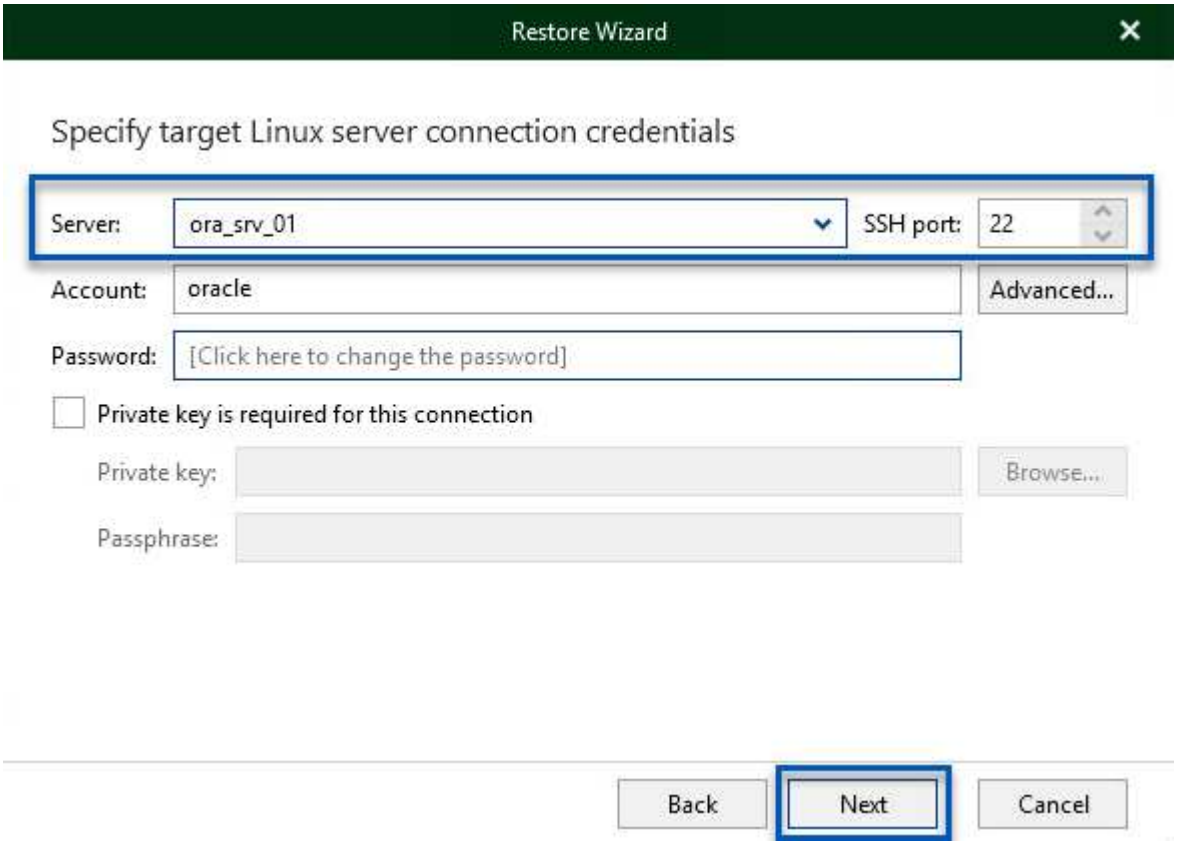
4. Dans Veeam Explorer, développez la liste des instances de base de données, cliquez sur la base de données à restaurer, puis dans le menu déroulant **Restaurer la base de données** en haut, sélectionnez **Restaurer sur un autre serveur…**.



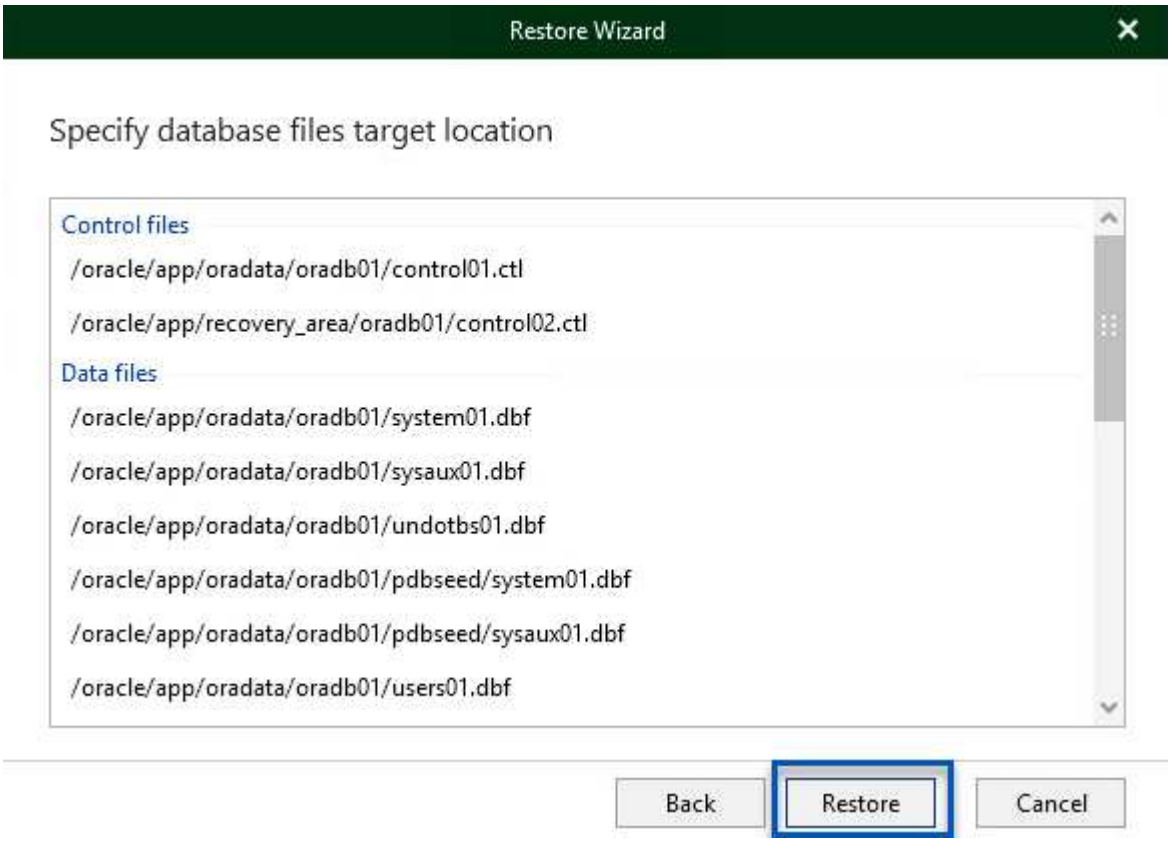
5. Dans l'assistant de restauration, spécifiez le point de restauration à partir duquel effectuer la restauration et cliquez sur **Suivant**.



6. Spécifiez le serveur cible sur lequel la base de données sera restaurée ainsi que 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 démarrer le processus de restauration.

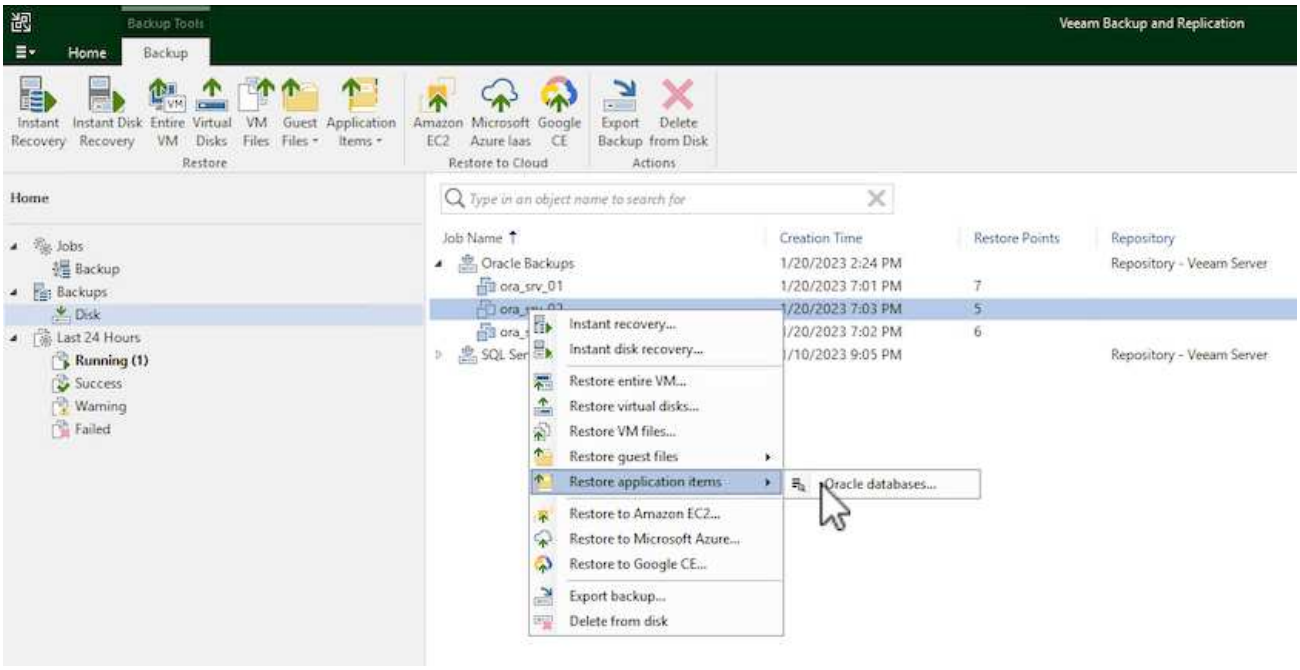


8. Une fois la récupération de la base de données terminée, vérifiez que la base de données Oracle démarre correctement sur le serveur.

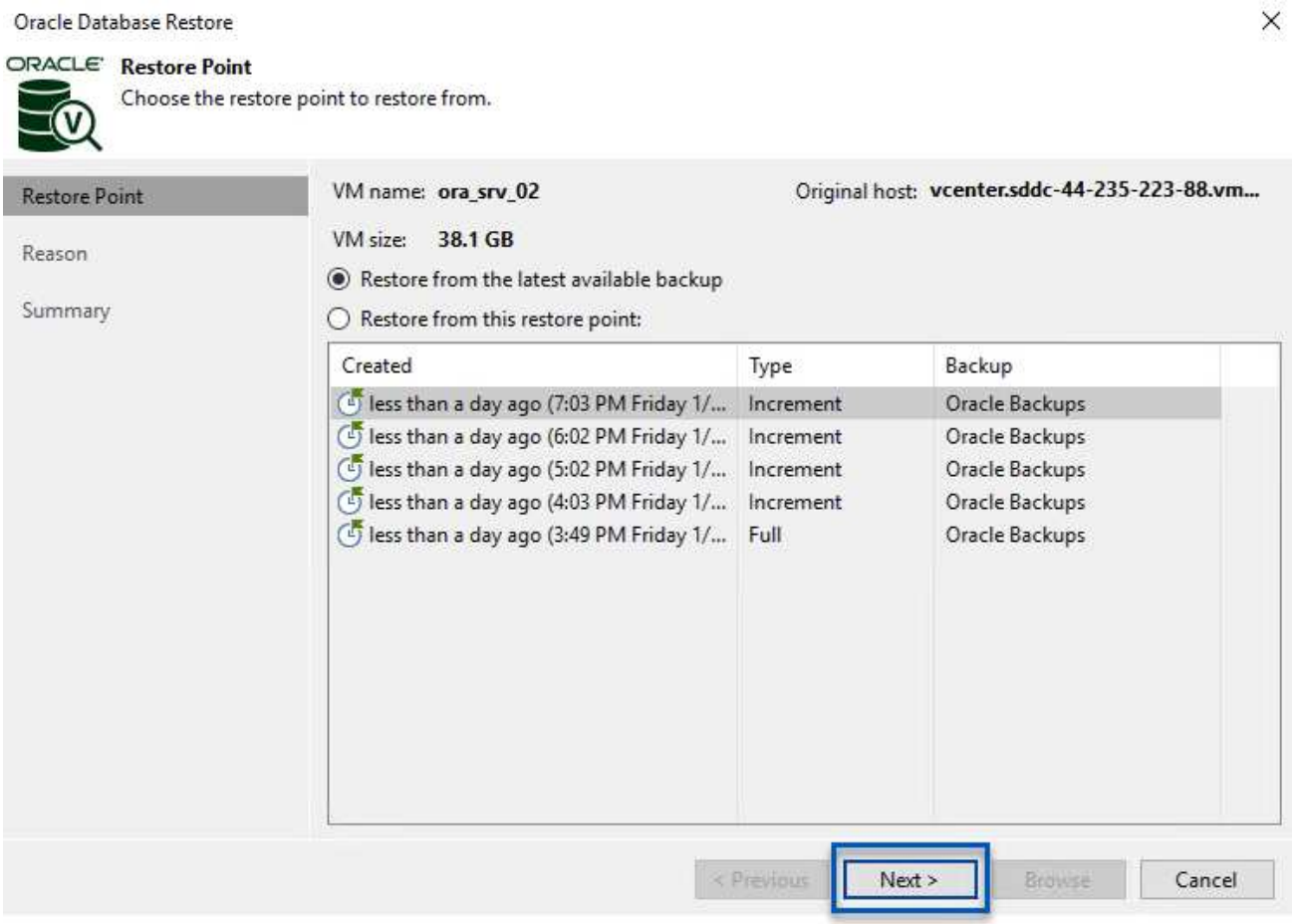
▼ **Publier la base de données Oracle sur un autre serveur**

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

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

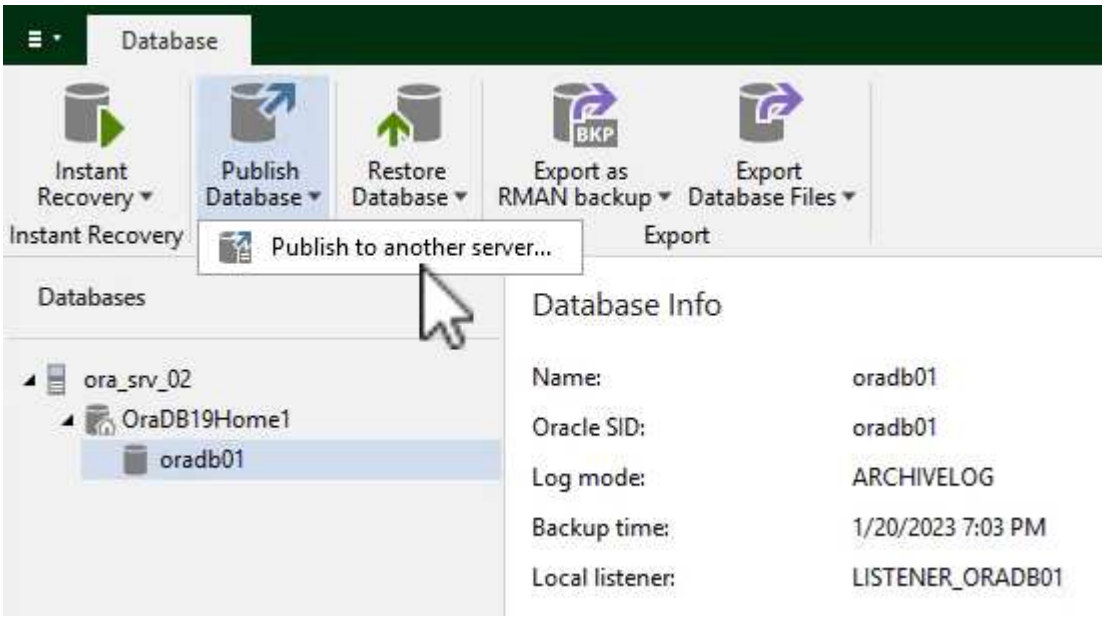


2. Dans l'assistant de restauration de base de données Oracle, sélectionnez un point de restauration dans la liste et cliquez sur **Suivant**.

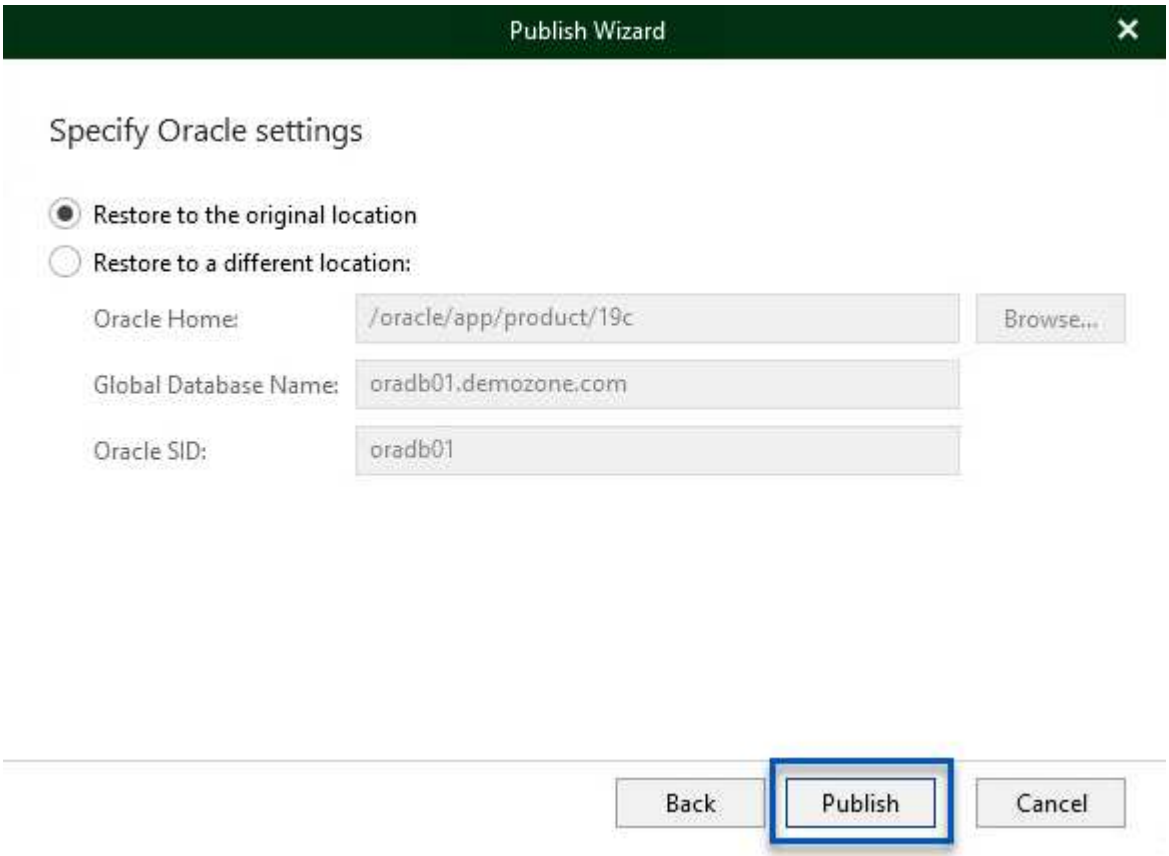


3. Saisissez une **raison de restauration** si vous le souhaitez, puis, sur la page Résumé, cliquez sur le bouton **Parcourir** pour lancer Veeam Explorer pour Oracle.

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…**.



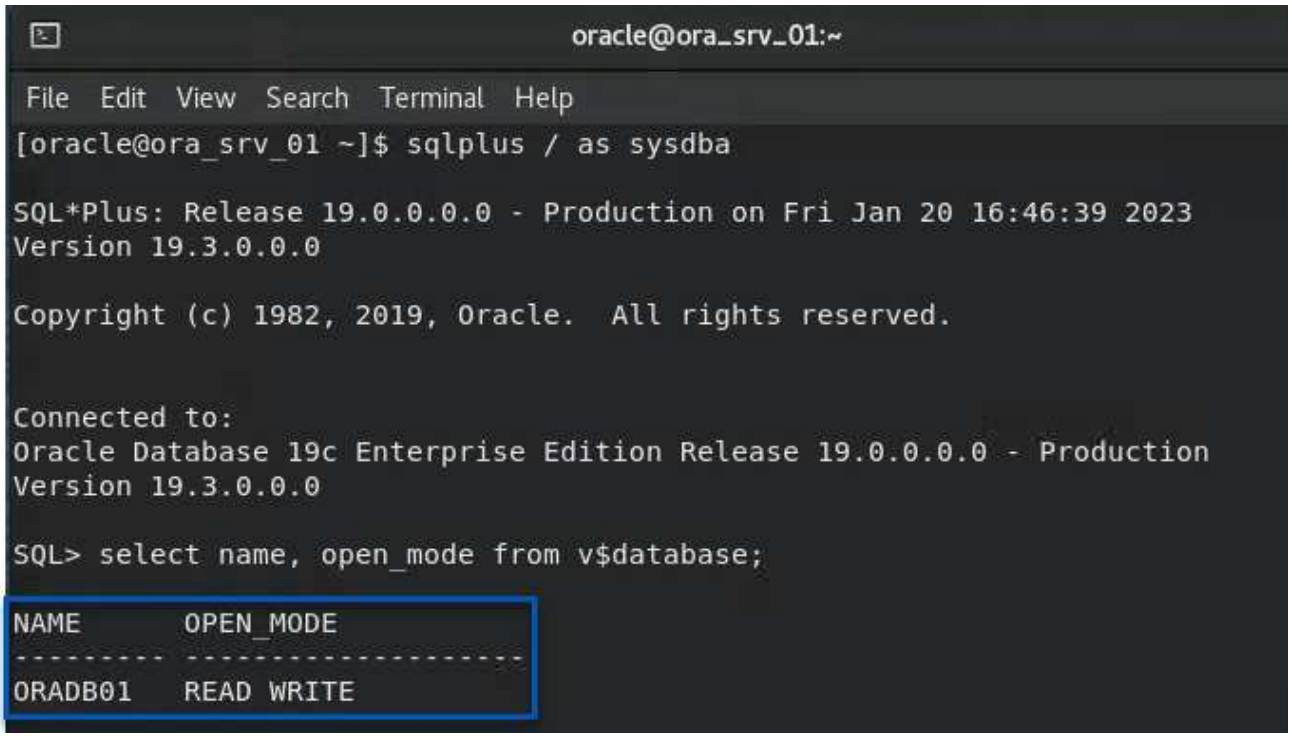
5. Dans l'assistant de publication, spécifiez le point de restauration à partir duquel publier la base de données et cliquez sur **Suivant**.
6. Enfin, spécifiez l'emplacement du système de fichiers Linux cible et cliquez sur **Publier** pour commencer le processus de restauration.



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 plate-forme puissante permettant d'exécuter des applications critiques pour l'entreprise et de stocker des données sensibles. Une solution de protection des données sécurisée est essentielle pour les entreprises qui s'appuient sur VMware Cloud pour garantir la continuité des activités et se protéger contre les cybermenaces et la perte de données. En choisissant une solution de protection des données fiable et robuste, les entreprises peuvent être sûres que leurs données critiques sont sûres et sécurisées, quoi qu'il arrive.

Le cas d'utilisation présenté dans cette documentation se concentre sur les technologies de protection des données éprouvées qui mettent en évidence l'intégration entre NetApp, VMware et Veeam. FSx ONTAP est pris en charge en tant que banques de données NFS supplémentaires pour VMware Cloud dans AWS et est utilisé pour toutes les données de machines virtuelles et d'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 en conjonction avec les volumes cibles de sauvegarde iSCSI, hébergés sur FSx ONTAP, pour 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, reportez-vous aux informations complémentaires suivantes.

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

TR-4955 : Reprise après sinistre avec FSx ONTAP et VMC (AWS VMware Cloud)

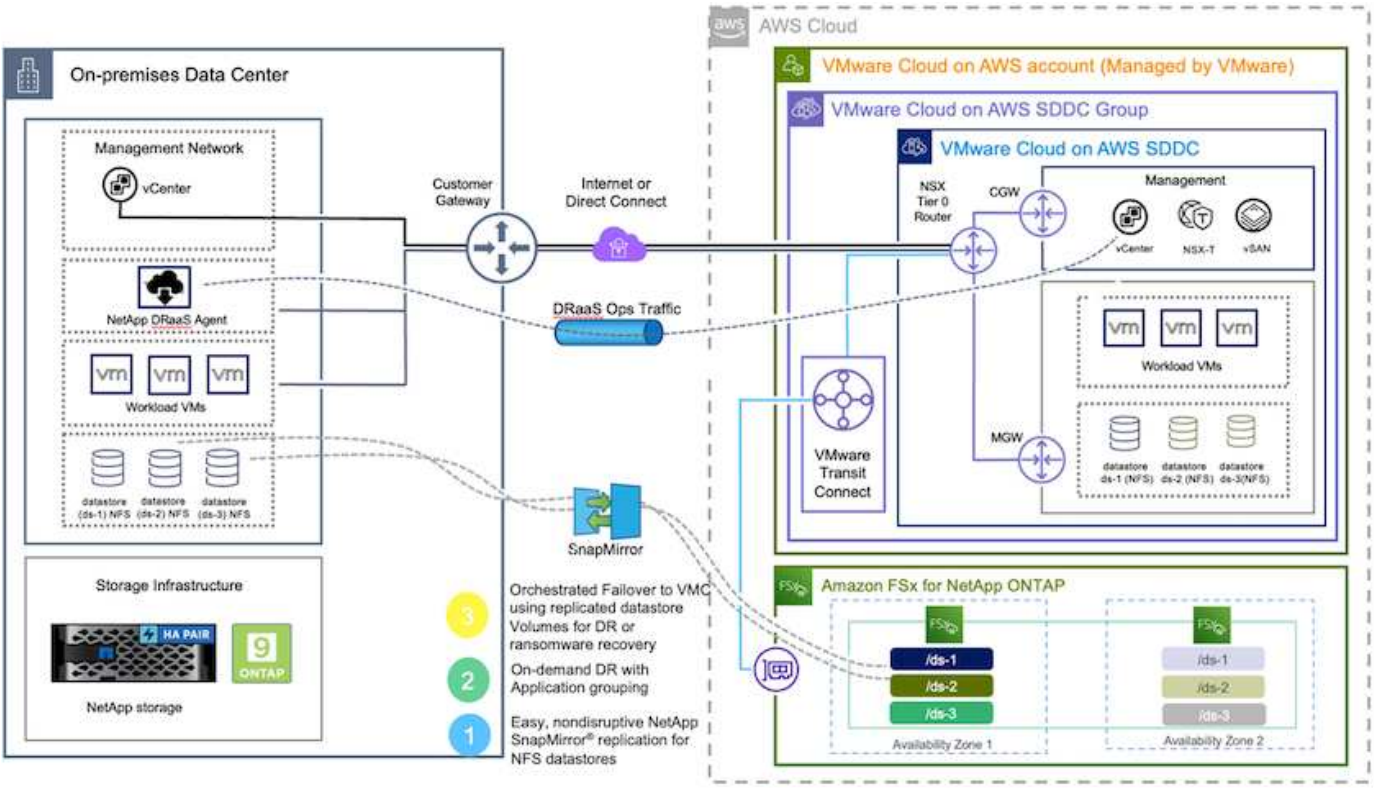
Disaster Recovery Orchestrator (DRO ; une solution scriptée avec interface utilisateur) peut être utilisé pour récupérer de manière transparente les charges de travail répliquées sur site vers FSx ONTAP. DRO automatise la récupération depuis SnapMirror , via l'enregistrement des VM sur VMC, jusqu'aux mappages réseau directement sur NSX-T. Cette fonctionnalité est incluse dans tous les environnements VMC.

Niyaz Mohamed, NetApp

Aperçu

La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données (par exemple, les ransomwares). Avec la technologie NetApp SnapMirror , les charges de travail VMware sur site peuvent être répliquées vers FSx ONTAP exécuté dans AWS.

Disaster Recovery Orchestrator (DRO ; une solution scriptée avec interface utilisateur) peut être utilisé pour récupérer de manière transparente les charges de travail répliquées sur site vers FSx ONTAP. DRO automatise la récupération depuis SnapMirror , via l'enregistrement des VM sur VMC, jusqu'aux mappages réseau directement sur NSX-T. Cette fonctionnalité est incluse dans tous les environnements VMC.



Déployer et configurer VMware Cloud sur AWS

"VMware Cloud sur AWS"offre une expérience cloud native pour les charges de travail basées sur VMware dans l'écosystème AWS. Chaque centre de données défini par logiciel VMware (SDDC) s'exécute dans un Amazon Virtual Private Cloud (VPC) et fournit une pile VMware complète (y compris vCenter Server), une mise en réseau définie par logiciel NSX-T, un stockage défini par logiciel 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, suivez les étapes ci-dessous."lien" . Un groupe de veilleuses peut également être utilisé à des fins de DR.

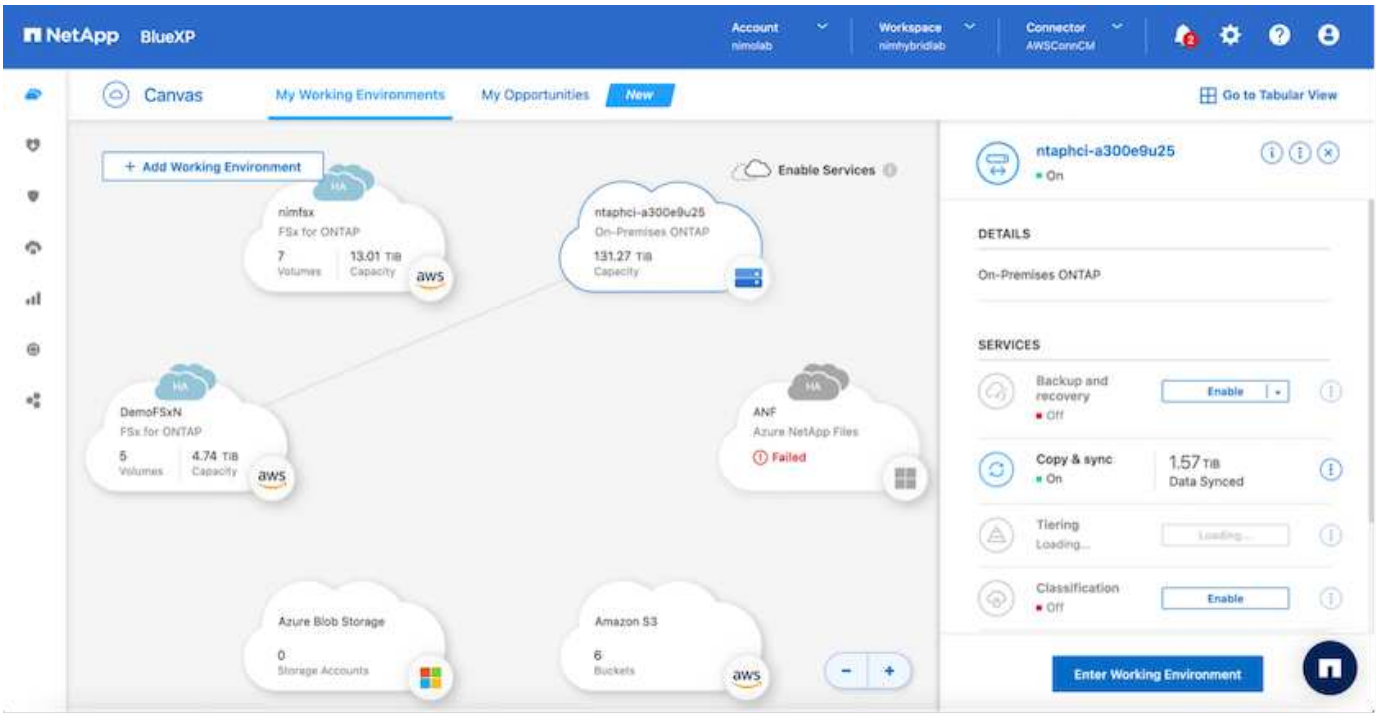
Dans la version initiale, DRO prend en charge un cluster de veilleuses existant. La création de SDDC à la demande sera disponible dans une prochaine version.

Provisionner et configurer FSx ONTAP

Amazon FSx ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités, basé sur le système de fichiers populaire NetApp ONTAP . Suivez les étapes à ce sujet"lien" pour provisionner et configurer FSx ONTAP.

Déployer et configurer SnapMirror sur FSx ONTAP

L'étape suivante consiste à utiliser NetApp Console pour découvrir l'instance FSx ONTAP provisionnée sur AWS et répliquer les volumes de datastore souhaités depuis un environnement sur site vers FSx ONTAP avec la fréquence appropriée et la durée de conservation appropriée des copies Snapshot de NetApp :



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

Une relation SnapMirror est une condition préalable et 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 de répondre aux conditions préalables. Ensuite, installez le package.

Prérequis

- Assurez-vous que la connectivité aux systèmes vCenter et de stockage source et de destination existe.
- La résolution DNS doit être en place si vous utilisez des noms DNS. Sinon, vous devez utiliser des adresses IP pour le vCenter et les systèmes de stockage.
- Créez un utilisateur avec des autorisations root. Vous pouvez également utiliser sudo avec une instance EC2.

Exigences OS

- Ubuntu 20.04 (LTS) avec un minimum de 2 Go et 4 vCPU
- Les packages suivants doivent être installés sur la machine virtuelle de l'agent désigné :
  - Docker
  - Docker-compose
  - Jq

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

Le `deploy.sh` le script exécute tous les prérequis requis.

Installer le paquet

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 entrez 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
```

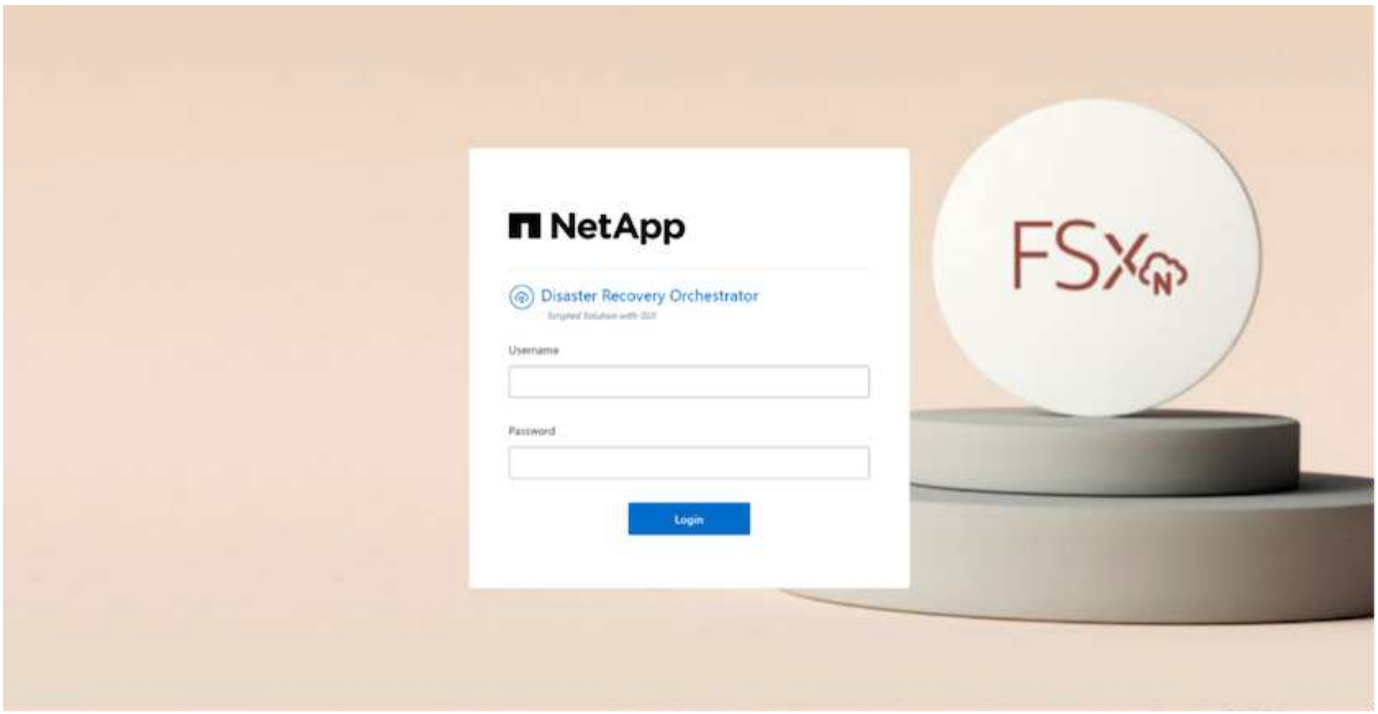
4. Accédez à l'interface utilisateur en utilisant :

```
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

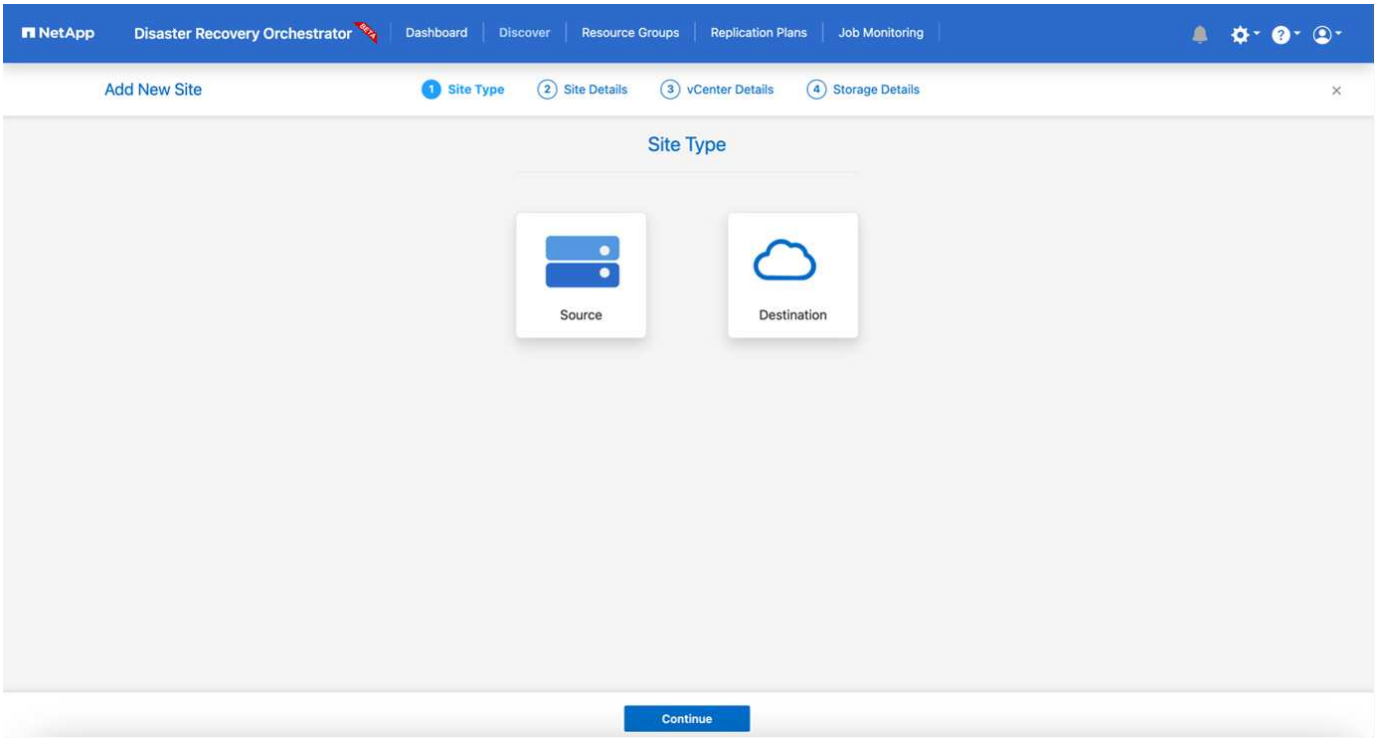
Une fois FSx ONTAP et VMC correctement configurés, vous pouvez commencer à configurer DRO pour automatiser la récupération des charges de travail locales sur VMC en utilisant les copies SnapMirror en lecture seule sur FSx ONTAP.

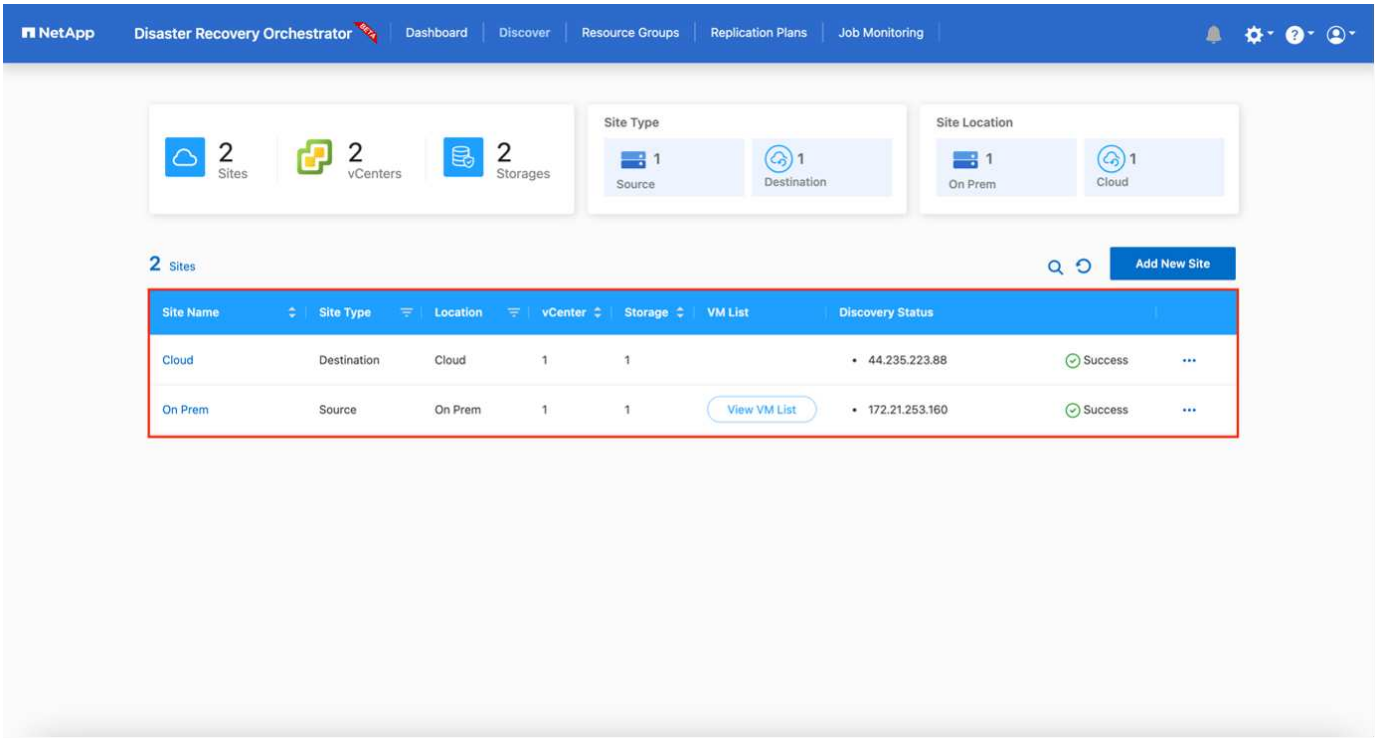
NetApp recommande de déployer l'agent DRO dans AWS et également sur le même VPC où FSx ONTAP est déployé (il peut également être connecté en mode homologue), afin que l'agent DRO puisse communiquer via le réseau avec vos composants sur site ainsi qu'avec les ressources FSx ONTAP et VMC.

La première étape consiste à découvrir et à ajouter les ressources sur site et dans le cloud (vCenter et 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 ajoutez des sites. Les sites peuvent également être ajoutés à l'aide de l'option Découvrir. Ajoutez les plateformes suivantes :

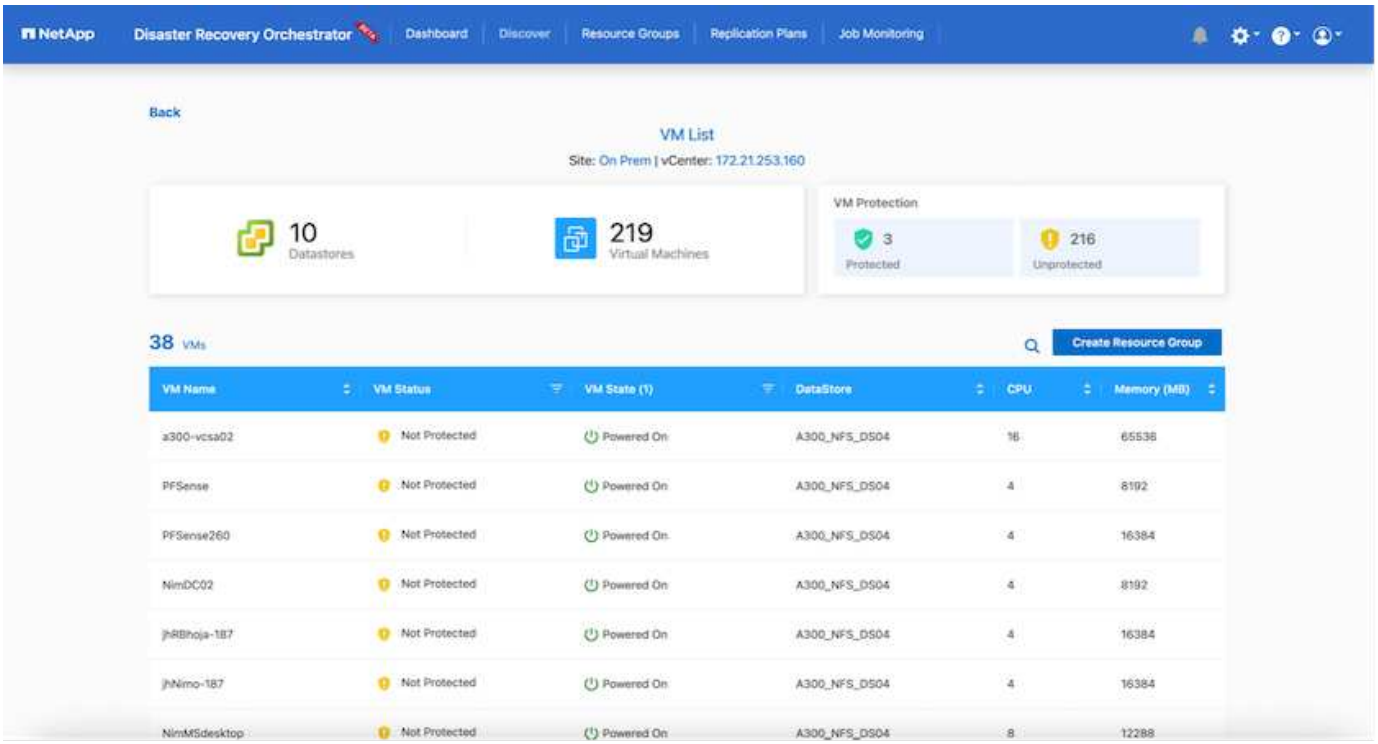
- Sur site
  - vCenter sur site
  - Système de stockage ONTAP

- Nuage
  - VMC vCenter
  - FSx ONTAP





Une fois ajouté, DRO effectue une découverte automatique et affiche les machines virtuelles qui ont des répliques SnapMirror correspondantes du stockage source vers FSx ONTAP. DRO détecte automatiquement les réseaux et les groupes de ports utilisés par les machines virtuelles et les remplit.



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

Groupements de ressources

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

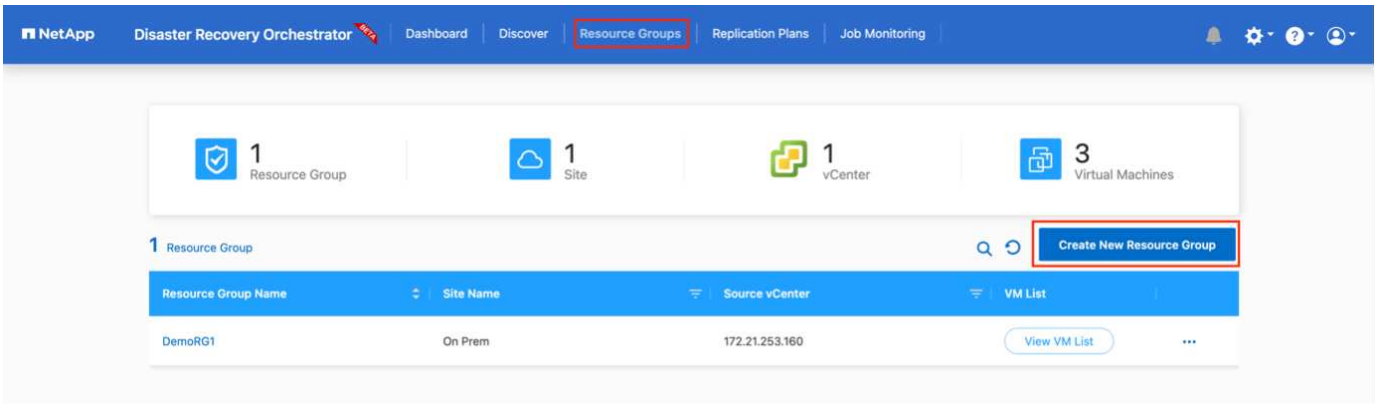
Pour commencer à créer des groupes de ressources, procédez comme suit :

1. Accédez à **Groupes de ressources** et 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 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 l'ordre de démarrage et le délai de démarrage (en secondes) pour les machines virtuelles sélectionnées. Définissez l'ordre de la séquence de mise sous tension en sélectionnant chaque machine virtuelle et en définissant sa priorité. Trois est la valeur par défaut pour toutes les machines virtuelles.

   Les options sont les suivantes :

   1 – La première machine virtuelle à s'allumer 3 – Par défaut 5 – La dernière machine virtuelle à s'allumer

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

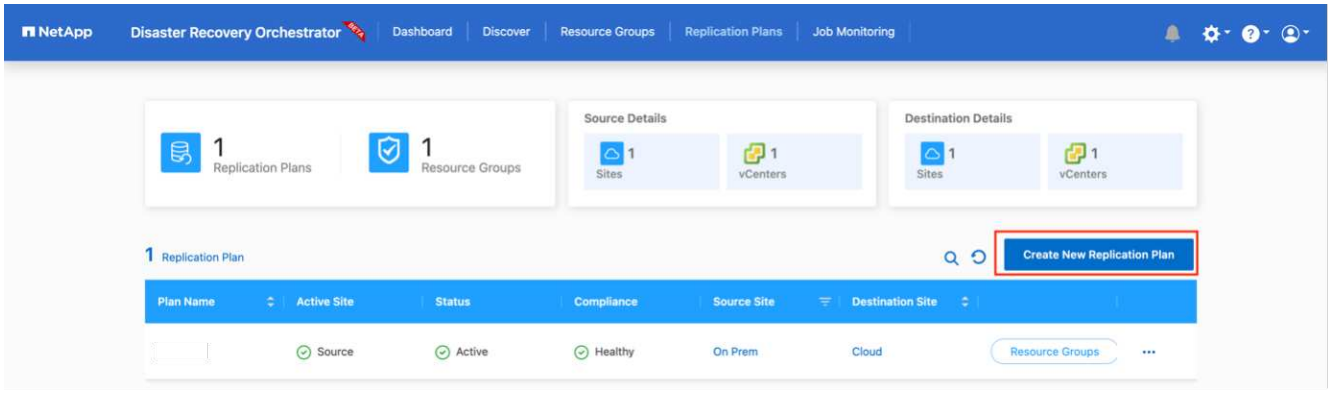


Plans de réplication

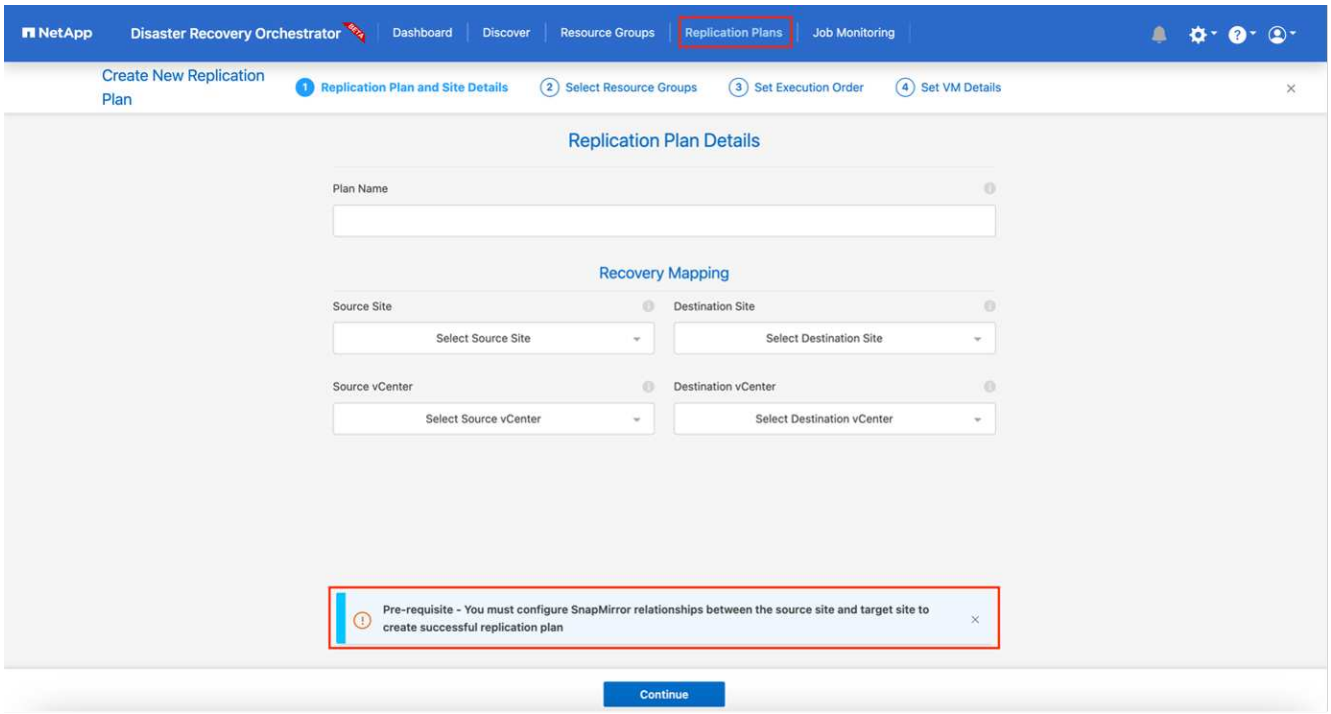
Vous avez besoin d'un plan pour récupérer les applications en cas de sinistre. Sélectionnez les plates-formes vCenter source et de destination dans la liste déroulante et choisissez les groupes de ressources à inclure dans ce plan, ainsi que le regroupement de la manière dont les applications doivent être restaurées et mises sous tension (par exemple, les contrôleurs de domaine, puis le niveau 1, puis le niveau 2, etc.). Ces plans sont parfois également appelés plans directeurs. Pour définir le plan de récupération, 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 :

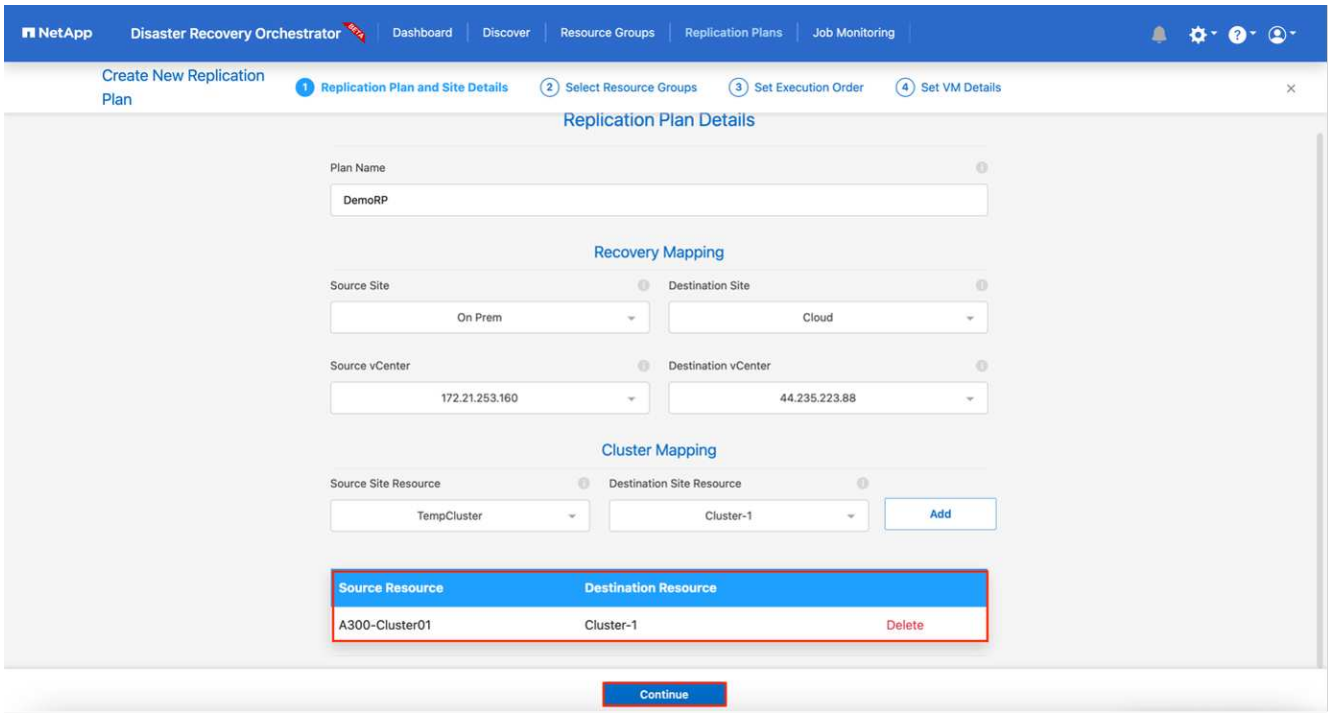
1. Accédez à **Plans de réplication** et cliquez sur **Créer un nouveau plan de réplication**.



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

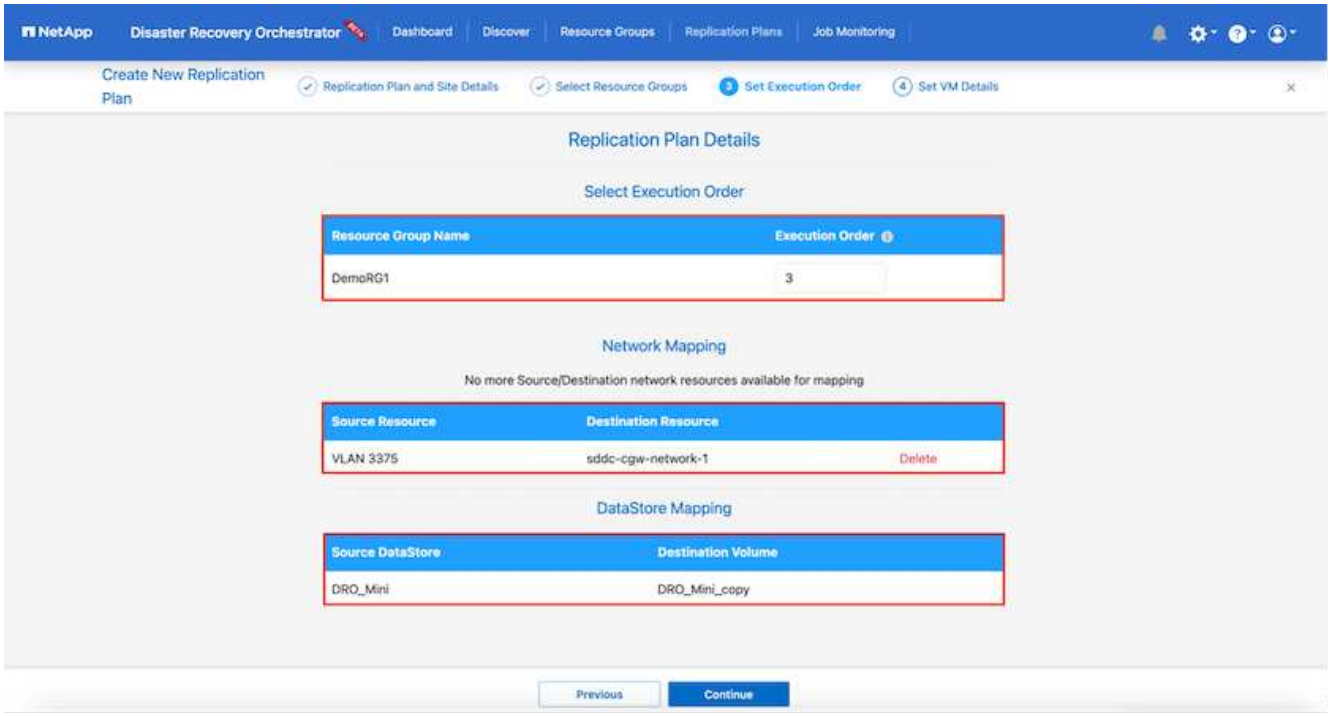


3. Une fois le mappage de récupération terminé, sélectionnez le mappage de cluster.

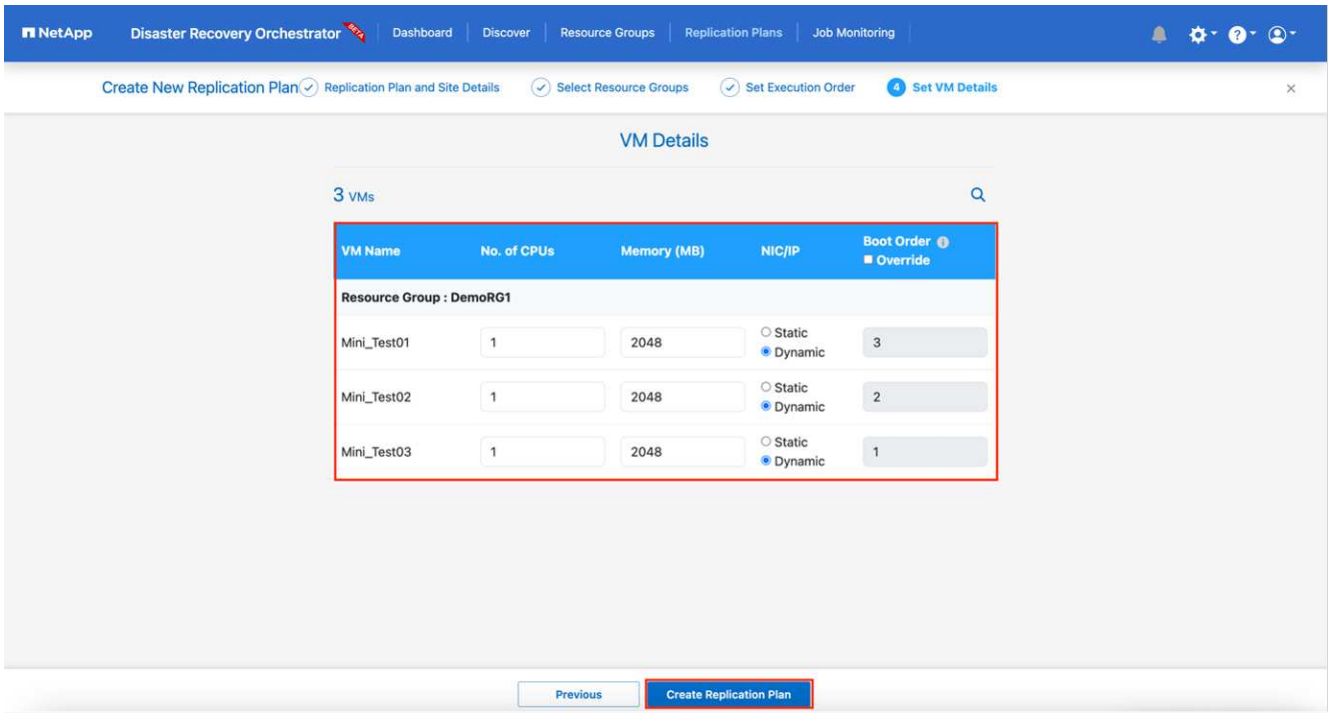


4. Sélectionnez **Détails du groupe de ressources** et cliquez sur **Continuer**.
5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsque plusieurs groupes de ressources existent.
6. Une fois que vous avez terminé, sélectionnez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

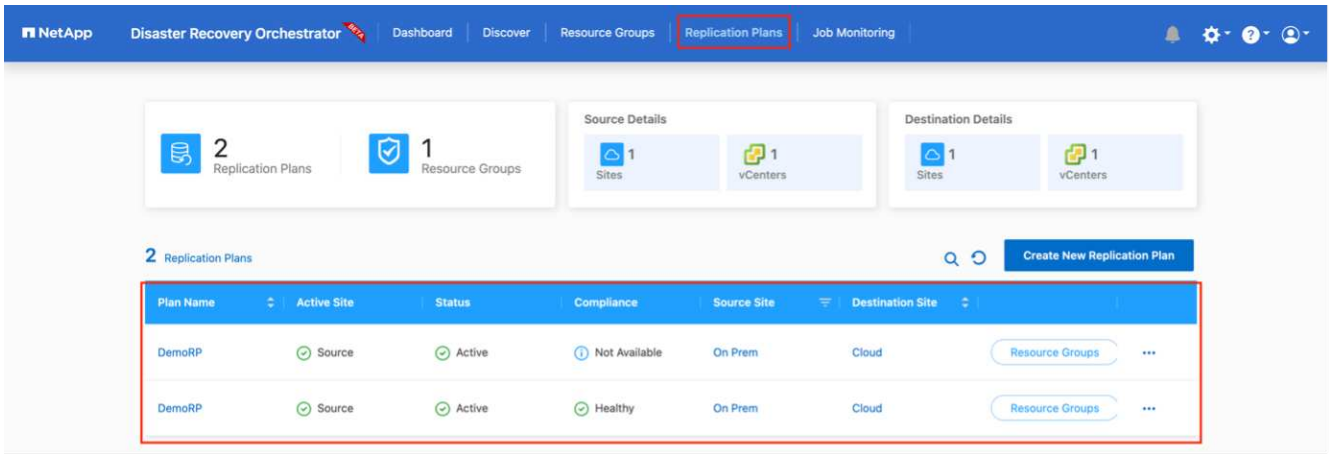
SnapMirror est au niveau du volume. Par conséquent, toutes les machines virtuelles sont répliquées vers la destination de réplication. Assurez-vous de sélectionner toutes les machines virtuelles qui font partie du magasin de données. Si elles ne sont pas sélectionnées, seules les machines virtuelles faisant partie du plan de réplication sont traitées.



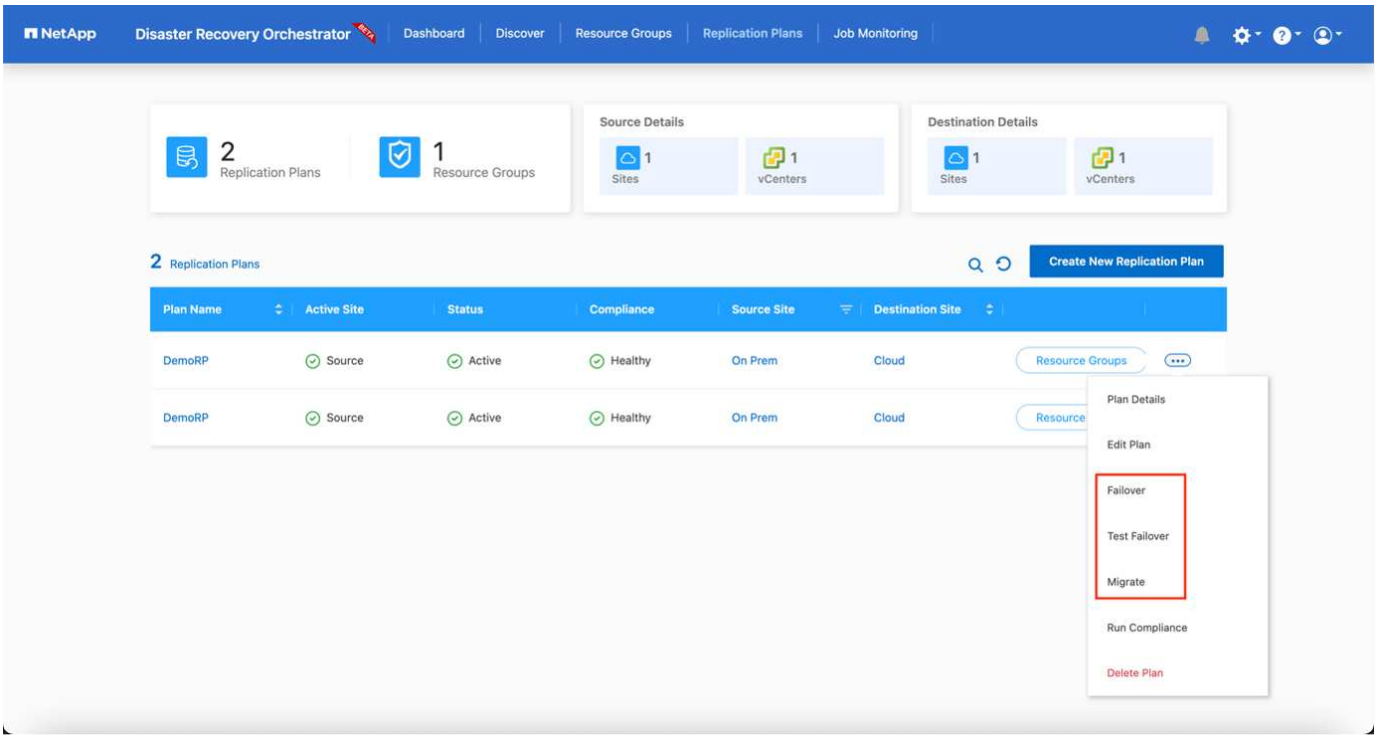
8. Sous les détails de la machine virtuelle, vous pouvez éventuellement redimensionner les paramètres CPU et RAM de la machine virtuelle ; cela peut être très utile lors de la récupération de grands environnements vers des clusters cibles plus petits ou pour effectuer des tests DR sans avoir à provisionner une infrastructure VMware physique individuelle. Vous pouvez également modifier l'ordre de démarrage et le délai de démarrage (en secondes) 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 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, toutes les modifications peuvent être effectuées à ce stade.

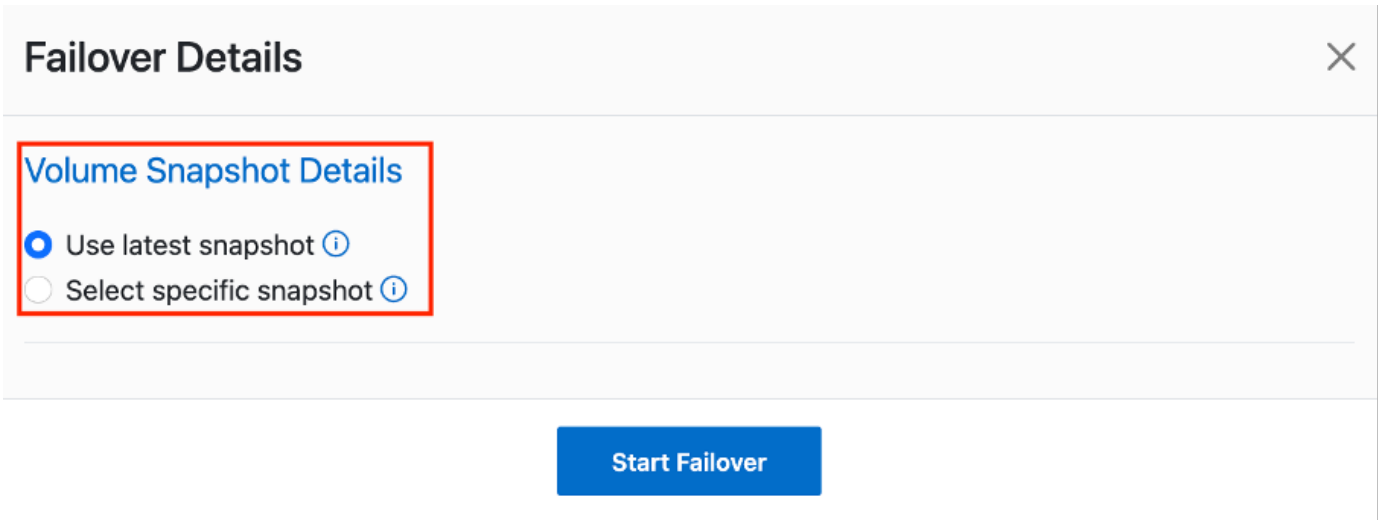


9. Cliquez sur **Créer un plan de réplication**.

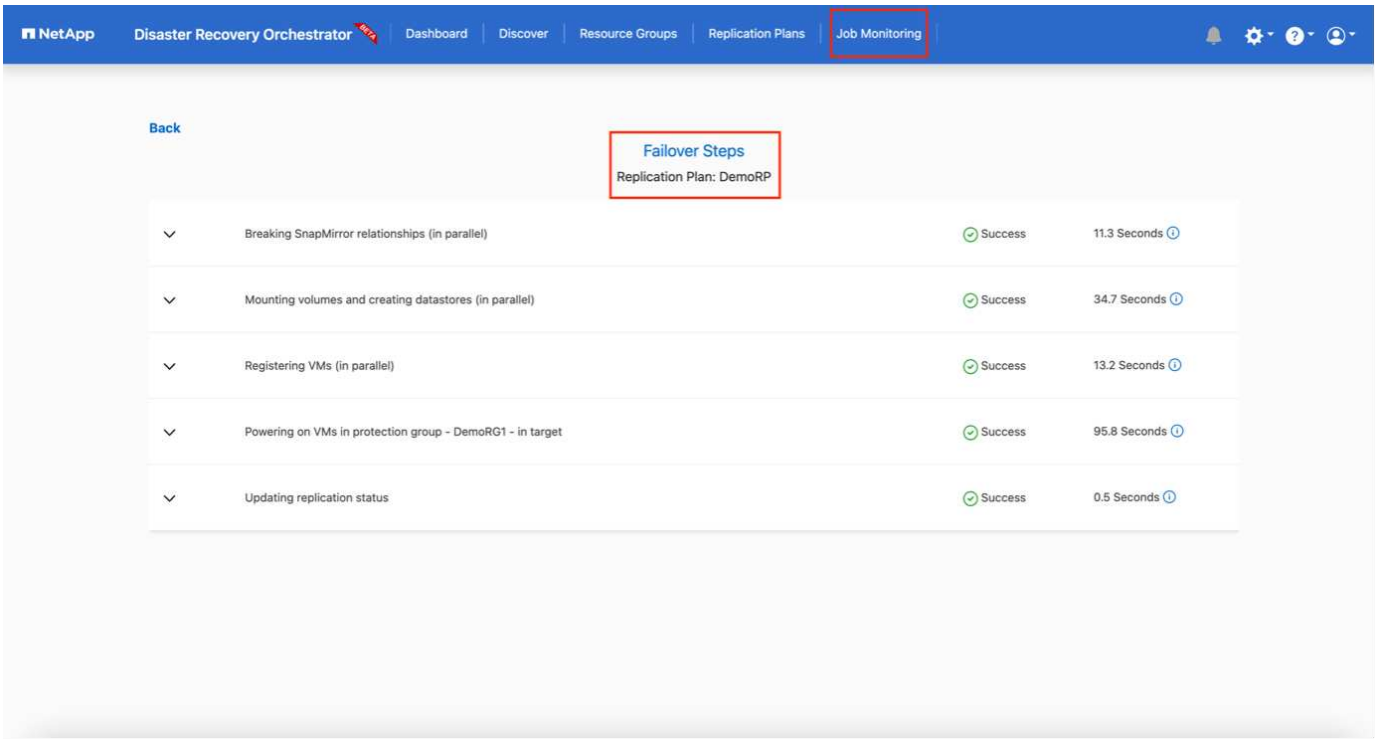


Une fois le plan de réplication créé, l'option de basculement, l'option de basculement de test ou l'option de migration peuvent être exercées en fonction des besoins. Pendant les options de basculement et de test de basculement, la copie Snapshot SnapMirror la plus récente est utilisée, ou une copie Snapshot spécifique peut être sélectionnée à partir d'une copie Snapshot à un instant T (conformément à la politique de conservation de SnapMirror). L'option ponctuelle peut être très utile si vous êtes confronté à un événement de corruption comme un ransomware, où les répliques les plus récentes sont déjà compromises ou cryptées. DRO affiche tous les points disponibles dans le temps. Pour déclencher un basculement ou un test de basculement avec la configuration spécifiée dans le plan de réplication, vous pouvez cliquer sur **Basculement** ou **Tester le basculement**.

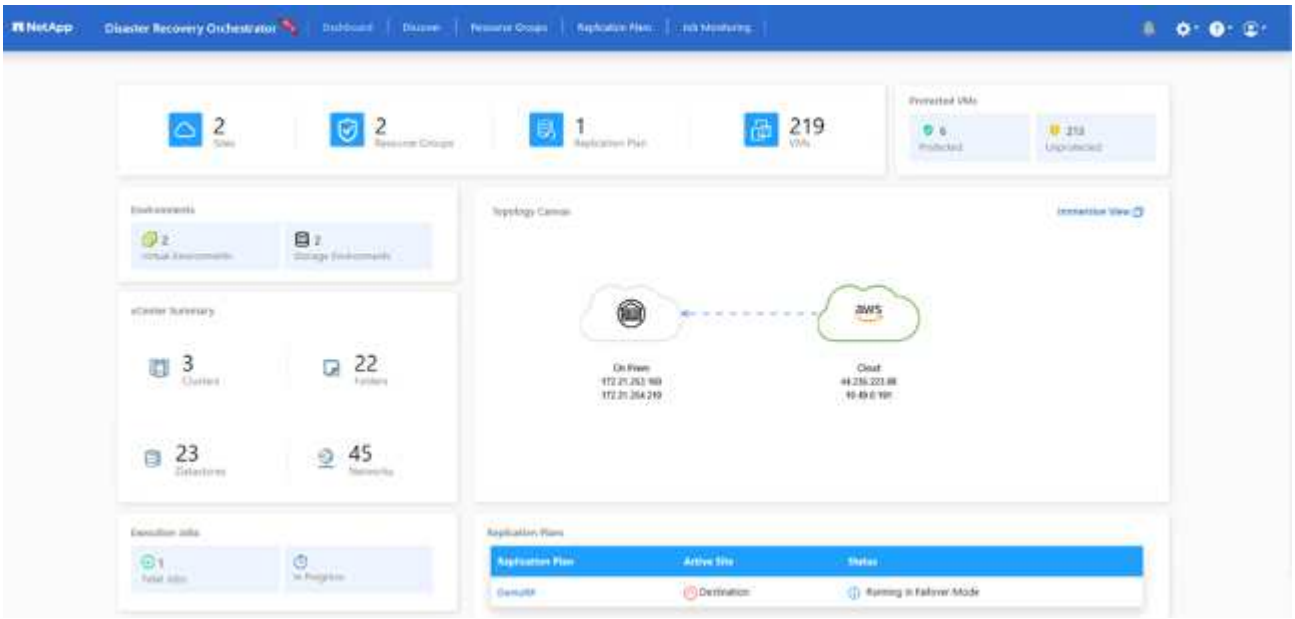




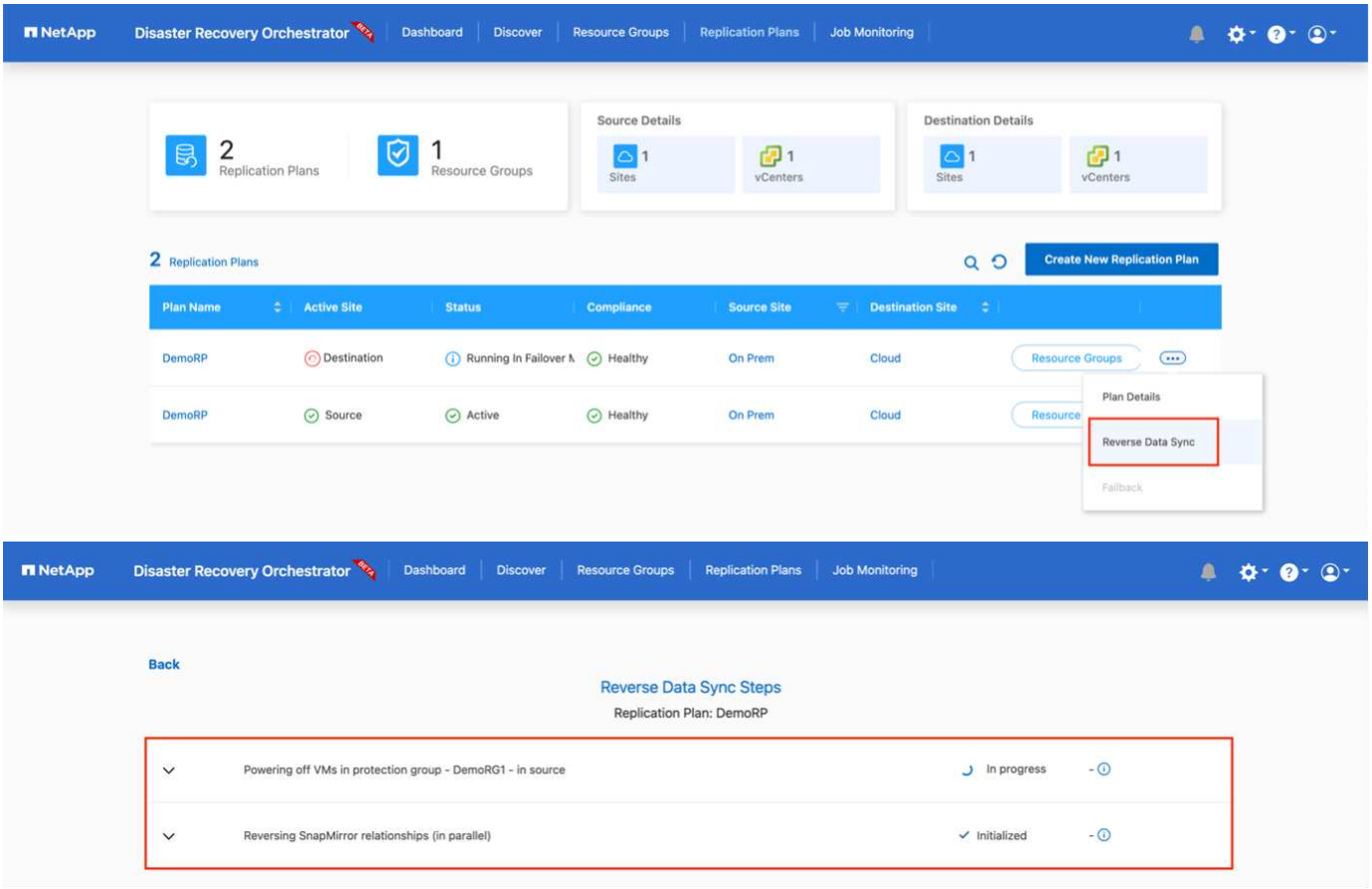
Le plan de réplication peut être surveillé dans le menu des tâches :



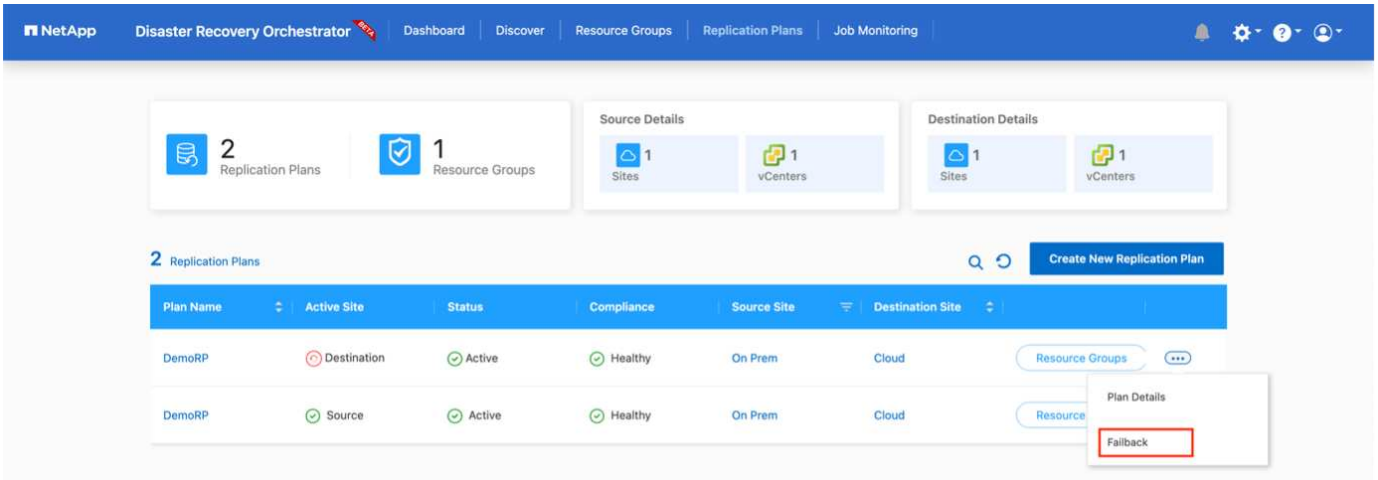
Une fois le basculement déclenché, les éléments récupérés peuvent être vus dans le vCenter VMC (machines virtuelles, réseaux, banques de données). Par défaut, les machines virtuelles sont récupérées dans le dossier Workload.

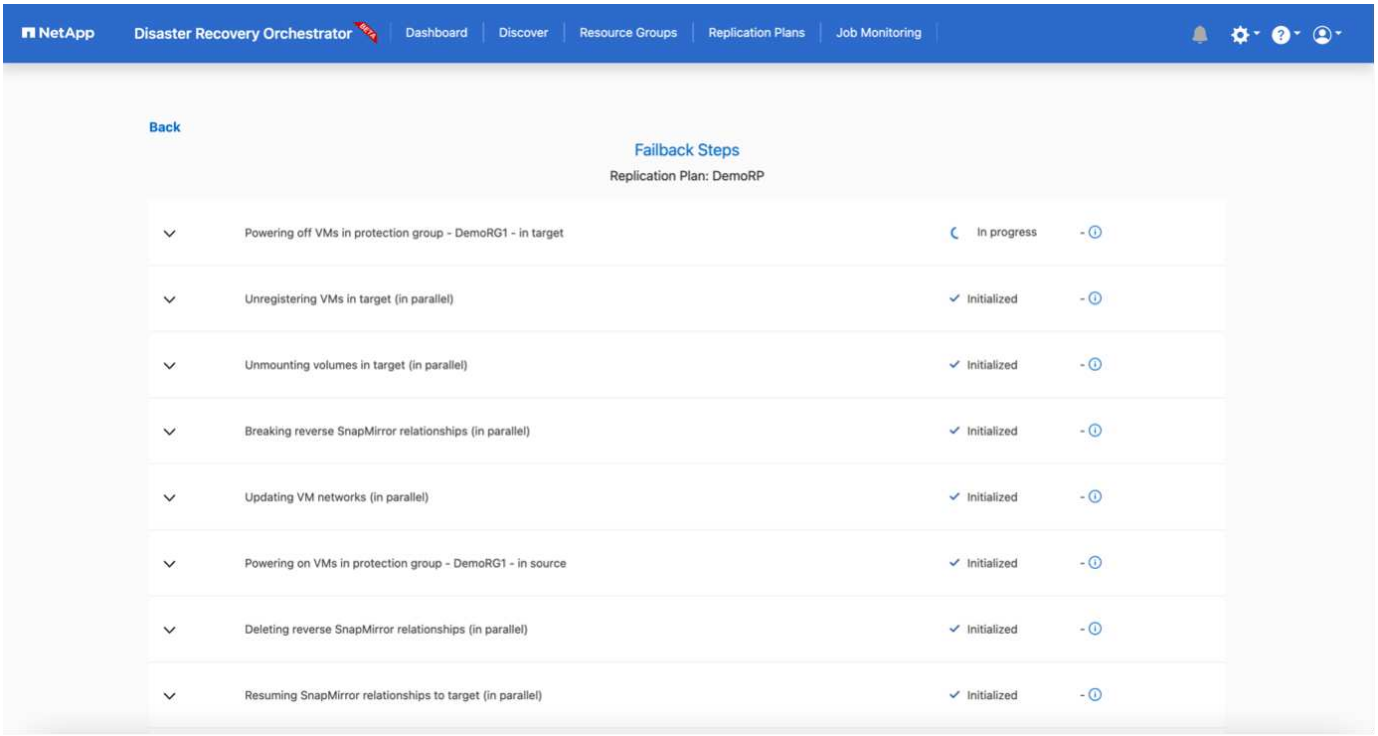


La restauration peut être déclenchée au niveau du plan de réplication. Pour un basculement de test, l'option de suppression peut être utilisée pour annuler les modifications et supprimer la relation FlexClone . La restauration automatique liée au basculement est un processus en deux étapes. Sélectionnez le plan de réplication et sélectionnez **Synchronisation des données inversées**.

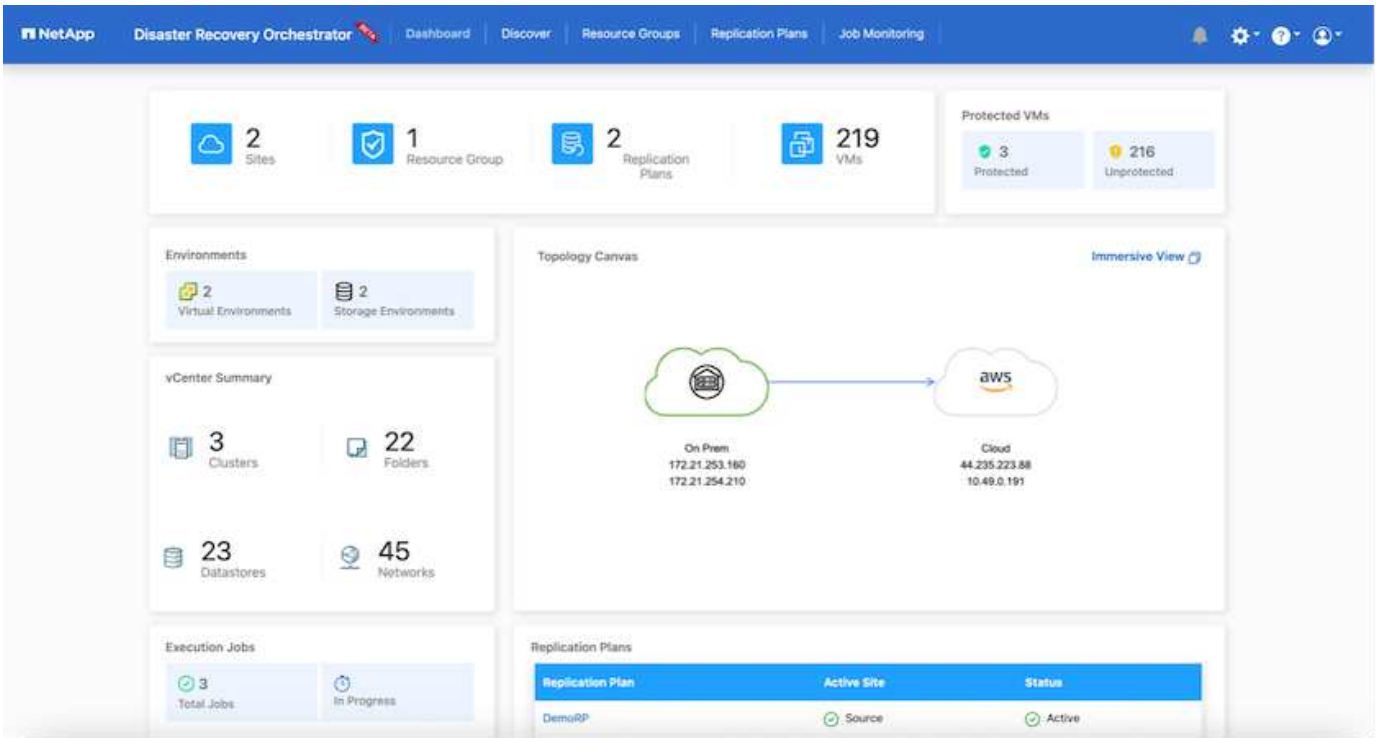


Une fois terminé, vous pouvez déclencher la restauration automatique pour revenir au site de production d'origine.





Depuis NetApp Console, nous pouvons constater que l'état de la réplication a été interrompu pour les volumes appropriés (ceux mappés à VMC en tant que volumes en lecture-écriture). Pendant le basculement de test, DRO ne mappe pas le volume de destination ou le volume répliqué. À la place, il crée une copie FlexClone® de l'instance SnapMirror (ou Snapshot) requise et expose l'instance FlexClone®, ce qui ne consomme pas de capacité physique supplémentaire pour FSx ONTAP. Ce processus garantit que le volume n'est pas modifié et que les tâches de réplication peuvent continuer même pendant les tests de reprise d'activité ou les flux de travail de triage. De plus, ce processus garantit que, si des erreurs se produisent ou si des données corrompues sont récupérées, la récupération peut être nettoyée sans risque de destruction de la réplique.



Récupération après un ransomware

Se remettre d'un ransomware peut être une tâche ardue. Plus précisément, il peut être difficile pour les organisations informatiques d'identifier précisément le point de retour sûr et, une fois celui-ci déterminé, de protéger les charges de travail récupérées contre les attaques récurrentes provenant, par exemple, de logiciels malveillants dormants ou d'applications vulnérables.

DRO répond à ces préoccupations en vous permettant de récupérer votre système à partir de n'importe quel moment disponible. Vous pouvez également récupérer des charges de travail sur des réseaux fonctionnels et pourtant isolés afin que les applications puissent fonctionner et communiquer entre elles dans un emplacement où elles ne sont pas exposées au trafic nord-sud. Cela offre à votre équipe de sécurité un endroit sûr pour effectuer des analyses médico-légales et s'assurer qu'il n'y a pas de malware caché ou dormant.

Avantages

- Utilisation de la réplication SnapMirror efficace et résiliente.
- Récupération à n'importe quel moment disponible avec conservation de copie instantanée.
- Automatisation complète de toutes les étapes requises pour récupérer des centaines à des milliers de machines virtuelles à partir des étapes de stockage, de calcul, de réseau et de validation des applications.
- Récupération de la charge de travail avec la technologie ONTAP FlexClone à l'aide d'une méthode qui ne modifie pas le volume répliqué.
  - Évite le risque de corruption des données pour les volumes ou les copies Snapshot.
  - Évite les interruptions de réplication pendant les flux de travail de test DR.
  - Utilisation potentielle des données DR avec des ressources de cloud computing pour des flux de travail au-delà de la DR tels que DevTest, les tests de sécurité, les tests de correctifs ou de mise à niveau et les tests de correction.
- Optimisation du processeur et de la RAM pour aider à réduire les coûts du cloud en permettant la récupération vers des clusters de calcul plus petits.

Utilisation de Veeam Replication et de FSx ONTAP pour la reprise après sinistre sur VMware Cloud sur AWS

L'intégration d' Amazon FSx ONTAP avec VMware Cloud sur AWS est un magasin de données NFS externe géré par AWS basé sur le système de fichiers ONTAP de NetApp qui peut être attaché à un cluster dans le SDDC. Il fournit aux clients une infrastructure de stockage virtualisée flexible et hautes performances qui s'adapte indépendamment des ressources de calcul.

Aperçu

Pour les clients souhaitant utiliser VMware Cloud sur AWS SDDC comme cible de reprise après sinistre, les banques de données FSx ONTAP peuvent être utilisées pour répliquer des données à partir de sites locaux à l'aide de n'importe quelle solution tierce validée offrant une capacité de réplication de machines virtuelles. En ajoutant la banque de données FSx ONTAP , cela permettra un déploiement optimisé en termes de coûts par rapport à la création d'un cloud VMware sur AWS SDDC avec une énorme quantité d'hôtes ESXi juste pour accueillir le stockage.

Cette approche permet également aux clients d'utiliser un cluster de voyants dans VMC avec les banques de données FSx ONTAP pour héberger les répliques de machines virtuelles. Le même processus peut également être étendu en tant qu'option de migration vers VMware Cloud sur AWS en basculant de manière élégante le

plan de réplication.

Énoncé du problème

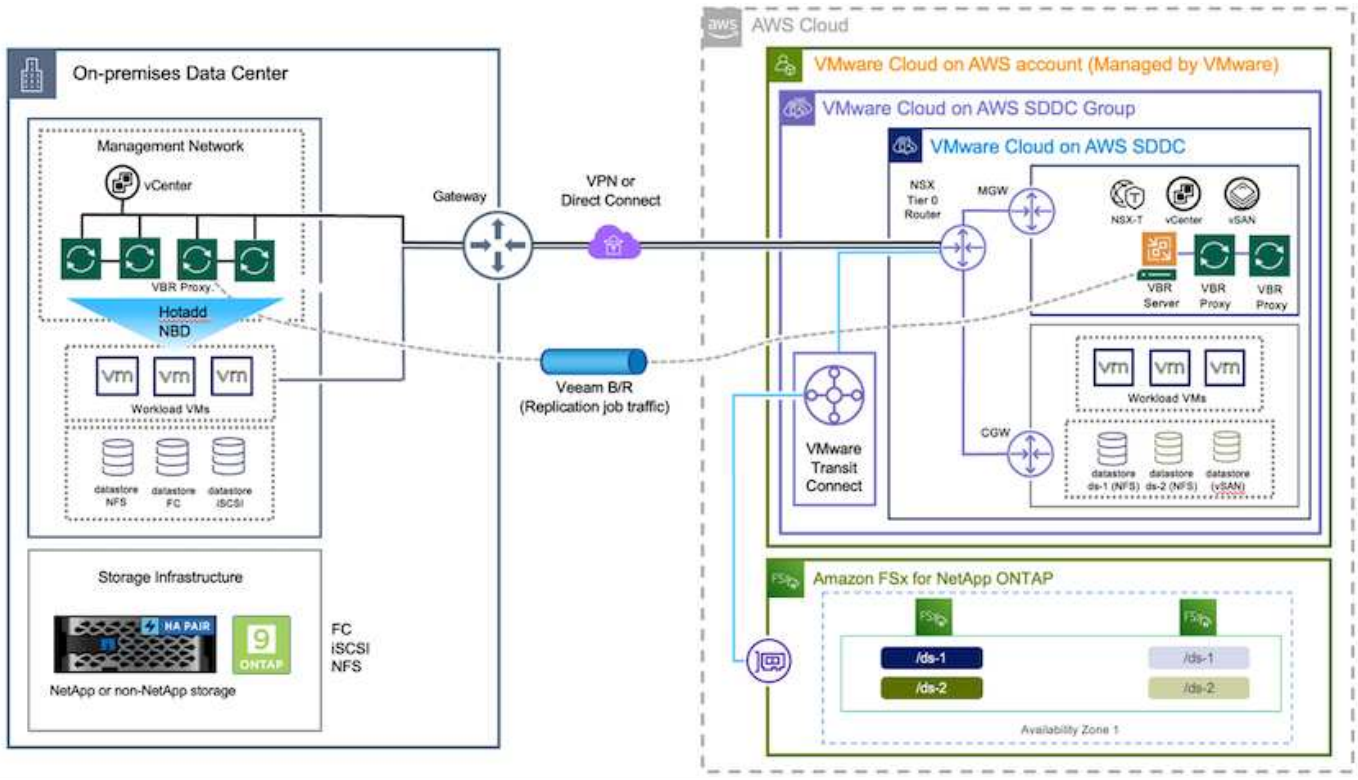
Ce document décrit comment utiliser la banque de données FSx ONTAP et Veeam Backup et la réplication pour configurer la reprise après sinistre des machines virtuelles VMware sur site vers VMware Cloud sur AWS à l'aide de la fonctionnalité de réplication de machines virtuelles.

Veeam Backup & Replication permet la réplication sur site et à distance pour la reprise après sinistre (DR). Lorsque des machines virtuelles sont répliquées, Veeam Backup & Replication crée une copie exacte des machines virtuelles au format VMware vSphere natif sur le cluster SDDC VMware Cloud on AWS cible et maintient la copie synchronisée avec la machine virtuelle d'origine.

La réplication fournit les meilleures valeurs d'objectif de temps de récupération (RTO) car il existe une copie d'une machine virtuelle dans l'état prêt à démarrer. Ce mécanisme de réplication garantit que les charges de travail peuvent démarrer rapidement dans VMware Cloud sur AWS SDDC en cas de sinistre. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. En outre, il filtre également les blocs de données en double, les blocs de données nuls, les fichiers d'échange et les fichiers du système d'exploitation invité de la machine virtuelle exclus, et compresse le trafic de réplication.

Pour éviter que les tâches de réplication ne consomment toute la bande passante du réseau, des accélérateurs WAN et des règles de limitation du réseau peuvent être mis en place. Le processus de réplication dans Veeam Backup & Replication est piloté par tâches, ce qui signifie que la réplication est effectuée en configurant des tâches de réplication. En cas de sinistre, le basculement peut être déclenché pour récupérer les machines virtuelles en basculant vers leur copie de réplication.

Lorsqu'un basculement est effectué, une machine virtuelle répliquée reprend le rôle de la machine virtuelle d'origine. Le basculement peut être effectué vers le dernier état d'une réplique ou vers l'un de ses points de restauration connus. Cela permet la récupération des ransomwares ou des tests isolés selon les besoins. Dans Veeam Backup & Replication, le basculement et la restauration sont des étapes intermédiaires temporaires qui doivent être finalisées ultérieurement. Veeam Backup & Replication offre plusieurs options pour gérer différents scénarios de reprise après sinistre.



Déploiement de la solution

Étapes de haut niveau

1. Le logiciel Veeam Backup and Replication s'exécute dans un environnement sur site avec une connectivité réseau appropriée.
2. Pour configurer VMware Cloud on AWS, consultez l'article VMware Cloud Tech Zone "Guide de déploiement de l'intégration de VMware Cloud sur AWS avec Amazon FSx ONTAP" pour déployer et configurer VMware Cloud on AWS SDDC et FSx ONTAP en tant que datastore NFS. (Un environnement pilot-light configuré avec une configuration minimale peut être utilisé à des fins de reprise après sinistre. Les VM basculeront vers ce cluster en cas d'incident, et des nœuds supplémentaires peuvent être ajoutés).
3. Configurez des tâches de réplication pour créer des répliques de machines virtuelles à l'aide de Veeam Backup and Replication.
4. Créez un plan de basculement et effectuez le basculement.
5. Revenez aux machines virtuelles de production une fois l'événement de catastrophe terminé et le site principal opérationnel.

Prérequis pour la réplication de machines virtuelles Veeam vers les datastores VMC et FSx ONTAP

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

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

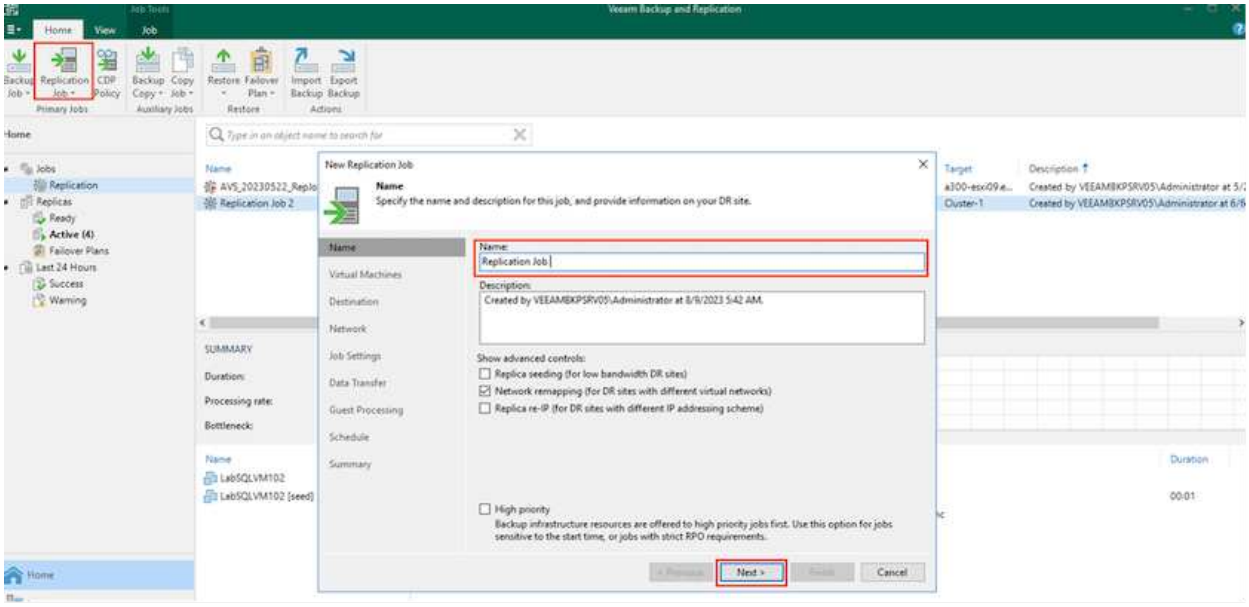
Détails du déploiement

▼ Étape 1 : Répliquer les machines virtuelles

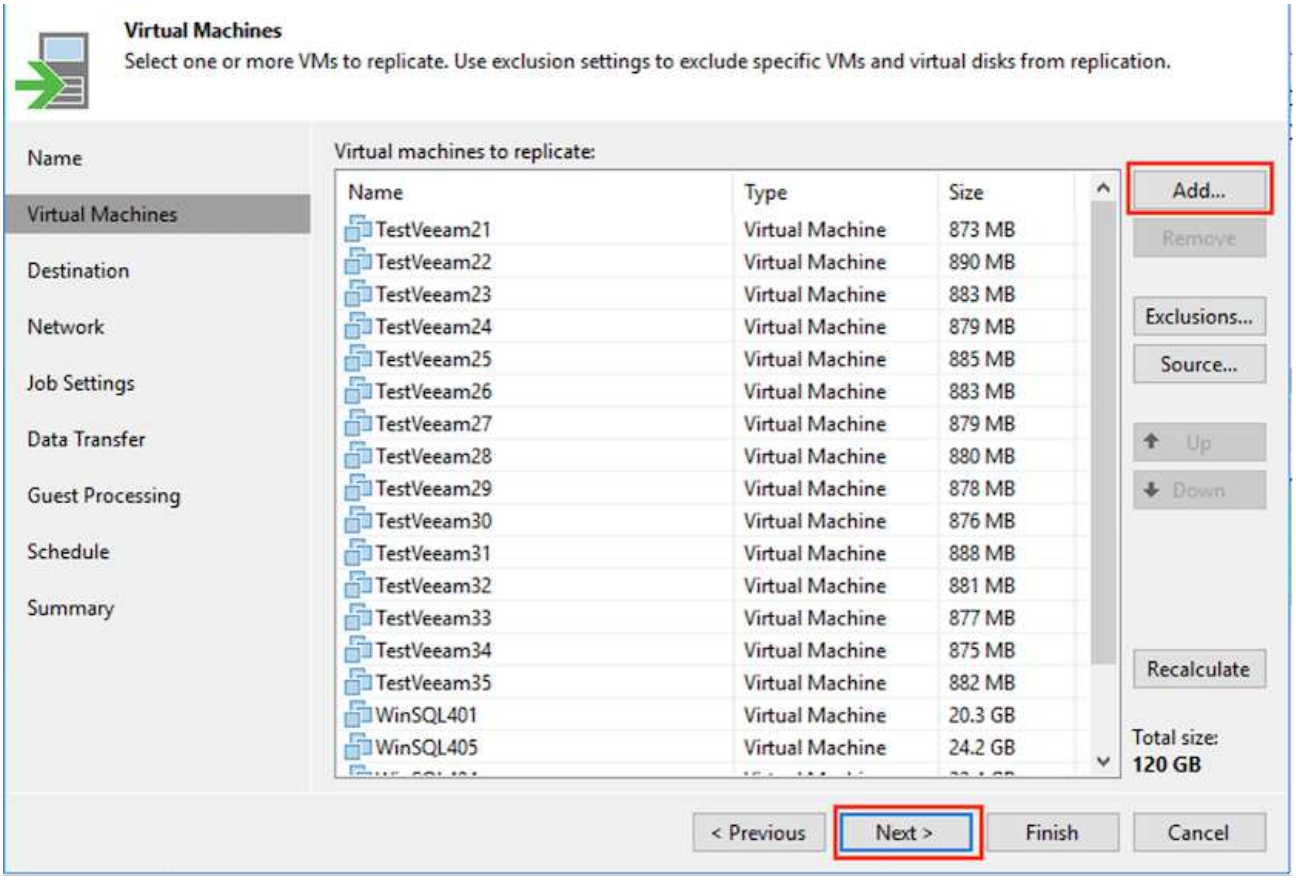
Veeam Backup & Replication exploite les fonctionnalités de snapshot de VMware vSphere et pendant la réplication, Veeam Backup & Replication demande à VMware vSphere de créer un snapshot de VM. L'instantané de machine virtuelle est la copie ponctuelle d'une machine virtuelle qui inclut les disques virtuels, 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, suivez les étapes ci-dessous :

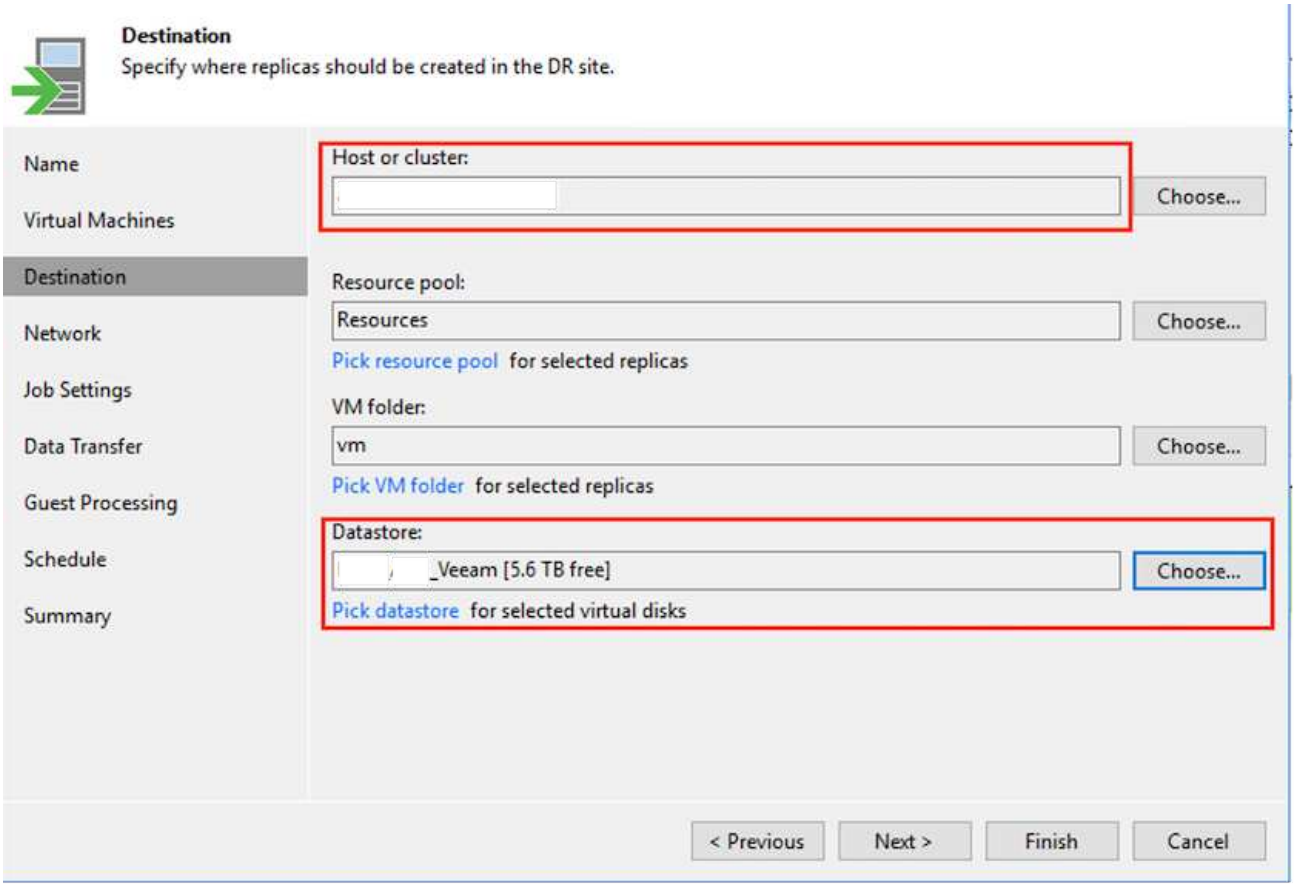
1. Ouvrez la console Veeam Backup & Replication.
2. Dans la vue Accueil, sélectionnez Tâche de réplication > Machine virtuelle > VMware vSphere.
3. Spécifiez un nom de tâche et sélectionnez la case à cocher de contrôle avancé appropriée. Cliquez sur Suivant.
   - Cochez la case Amorçage de réplication si la connectivité entre le système local et AWS a une bande passante restreinte.
   - Cochez la case Remappage réseau (pour les sites AWS VMC avec des réseaux différents) si les segments sur VMware Cloud sur AWS SDDC ne correspondent pas à ceux des réseaux de sites locaux.
   - Si le schéma d'adressage IP du site de production sur site diffère du schéma du site AWS VMC, cochez la case Réplication de l'adresse IP (pour les sites DR avec un schéma d'adressage IP différent).



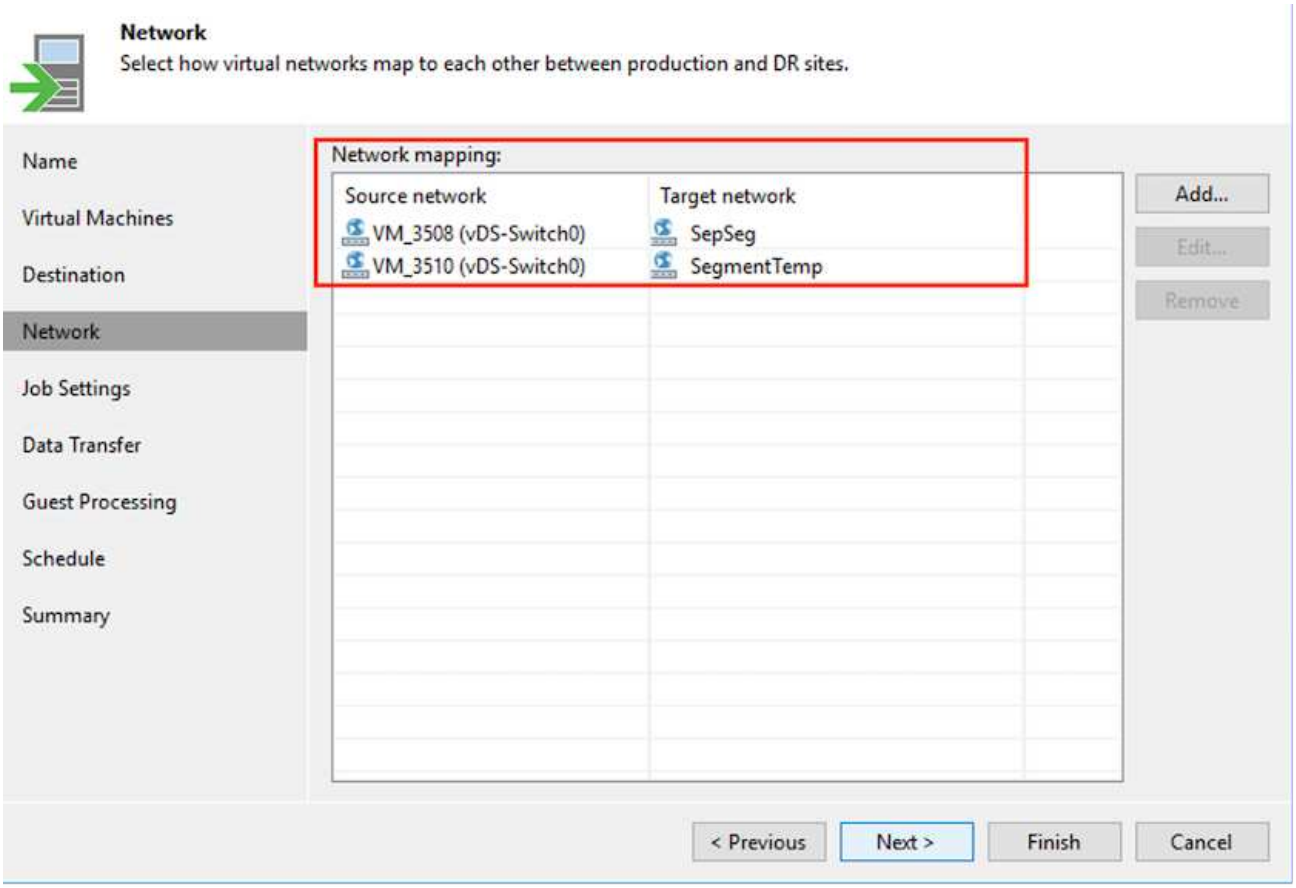
4. Sélectionnez les machines virtuelles qui doivent être répliquées vers la banque de données FSx ONTAP connectée à VMware Cloud sur AWS SDDC à l'étape **Machines virtuelles**. Les machines virtuelles peuvent être placées sur vSAN pour remplir la capacité de stockage de données vSAN disponible. Dans un groupe de veilleuses, la capacité utilisable d'un groupe à 3 nœuds sera limitée. Le reste des données peut être répliqué vers les banques de données FSx ONTAP . Cliquez sur **Ajouter**, puis dans la fenêtre **Ajouter un objet**, sélectionnez les machines virtuelles ou les conteneurs de machines virtuelles nécessaires et cliquez sur **Ajouter**. Cliquez sur **Suivant**.



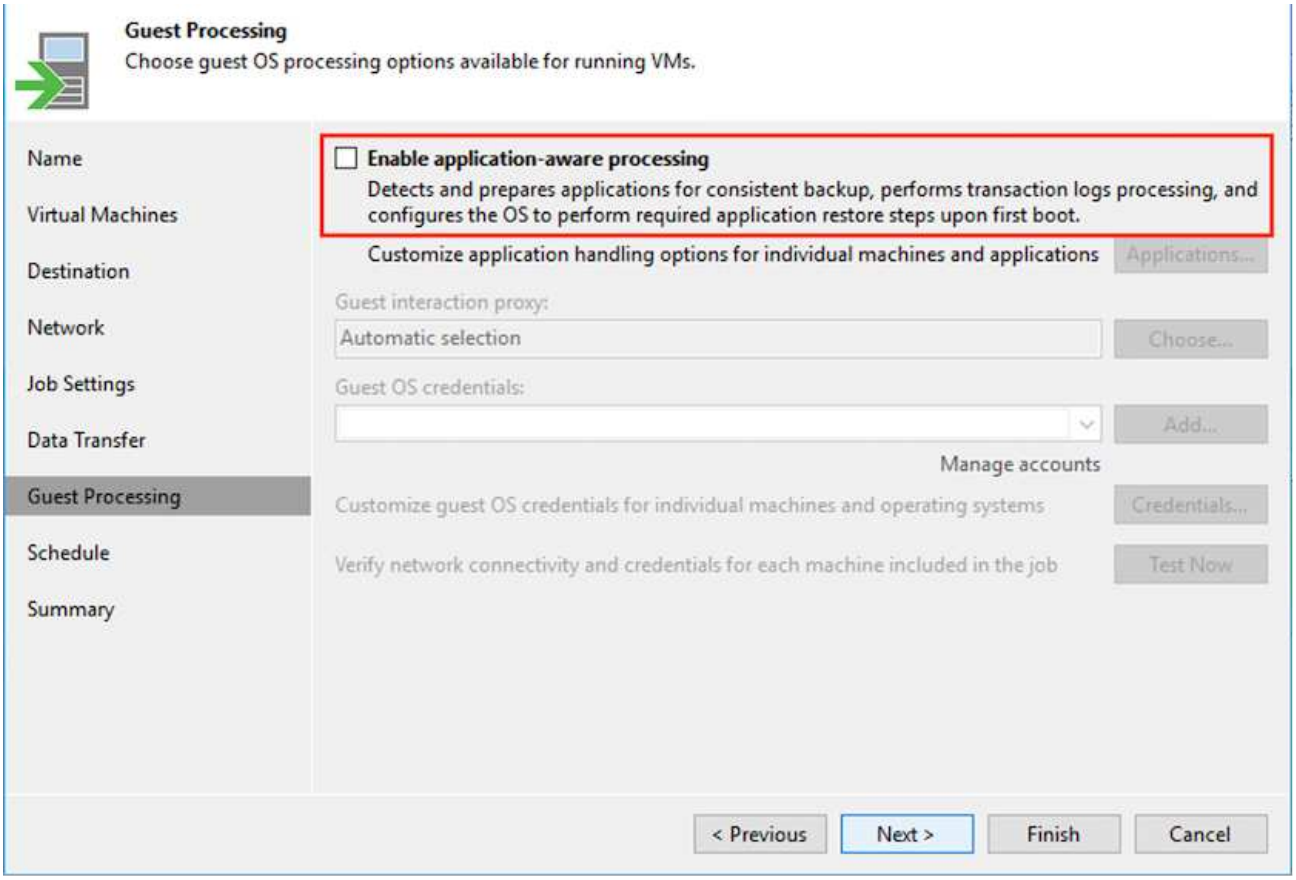
5. Après cela, sélectionnez la destination en tant que cluster/hôte VMware Cloud sur AWS SDDC et le pool de ressources, le dossier de machine virtuelle et la banque de données FSx ONTAP appropriés pour les répliques de machine virtuelle. Cliquez ensuite sur **Suivant**.



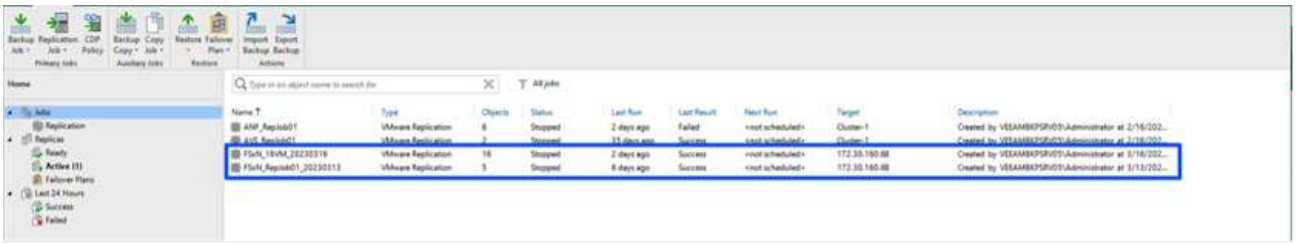
6. À l'étape suivante, créez le mappage entre le réseau virtuel source et le réseau virtuel de destination selon vos besoins.



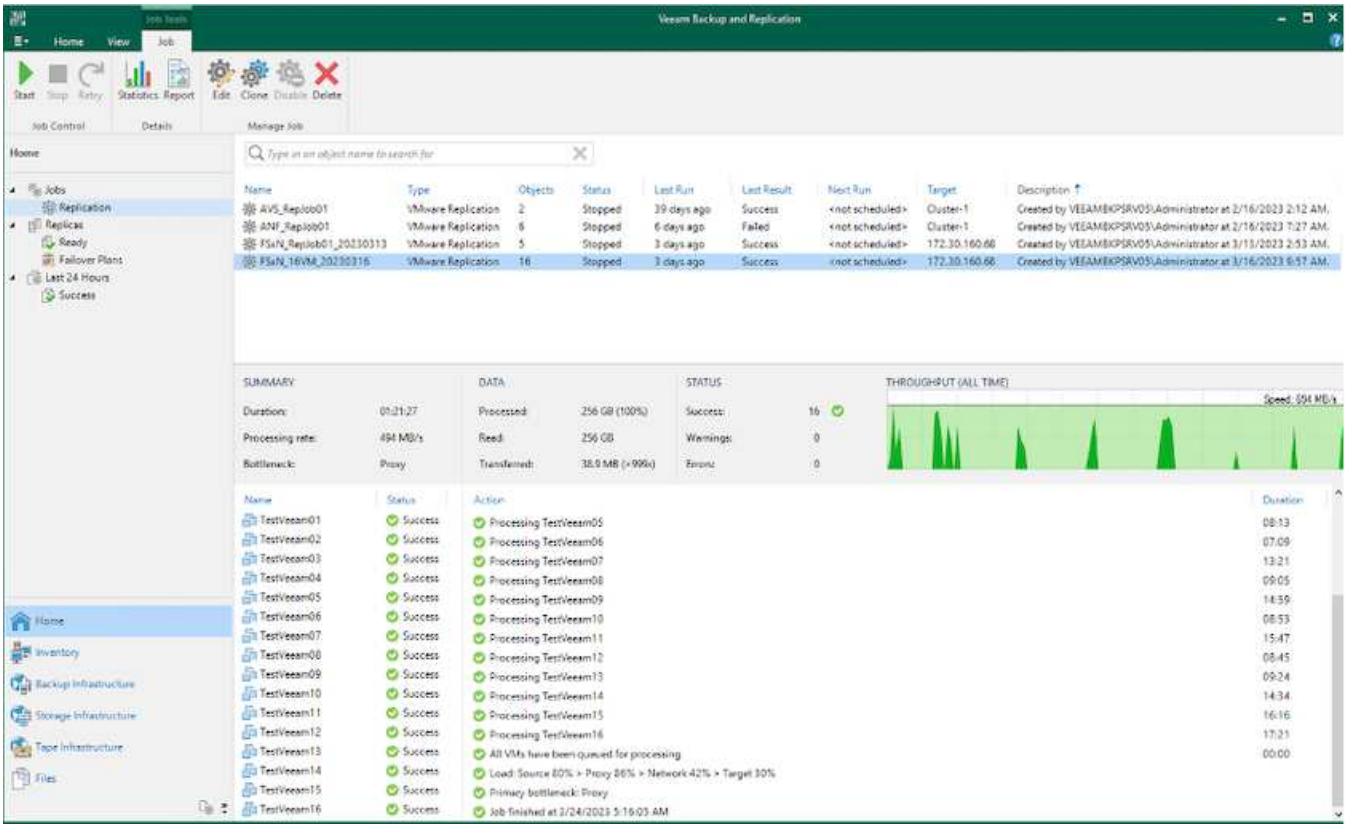
7. À l'étape **Paramètres de tâche**, spécifiez le référentiel de sauvegarde qui stockera les métadonnées des répliques de machines virtuelles, la politique de rétention, etc.
8. Mettez à jour les serveurs proxy **Source** et **Cible** dans l'étape **Transfert de données** et laissez la sélection **Automatique** (par défaut) et gardez l'option **Direct** sélectionnée et cliquez sur **Suivant**.
9. À l'étape **Traitement des invités**, sélectionnez l'option **Activer le traitement sensible aux applications** selon vos besoins. Cliquez sur **Suivant**.



10. Choisissez la planification de réplication pour exécuter le travail de réplication régulièrement.
11. À l'étape **Résumé** de l'assistant, vérifiez les détails de la tâche 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 laissez la case décochée. Cliquez ensuite sur **Terminer** pour fermer l'assistant.



Une fois le travail de réplication démarré, les machines virtuelles avec le suffixe spécifié seront renseignées sur le cluster/hôte VMC SDDC de destination.



Pour plus d'informations sur la réplication Veeam, reportez-vous à"Comment fonctionne la réplication" .

▼ Étape 2 : Créer un plan de basculement

Une fois la réplication ou l'amorçage initial terminé, créez le plan de basculement. Le plan de basculement permet d'effectuer le basculement des machines virtuelles dépendantes une par une ou en tant que groupe automatiquement. Le plan de basculement est le plan directeur de l'ordre dans lequel les machines virtuelles sont traitées, y compris les délais de démarrage. Le plan de basculement permet également de garantir que les machines virtuelles dépendantes critiques sont déjà en cours d'exécution.

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

> ⓘ Le plan de basculement ne peut être ajouté qu'une fois la réplication initiale terminée et les répliques de machines virtuelles à l'état Prêt.

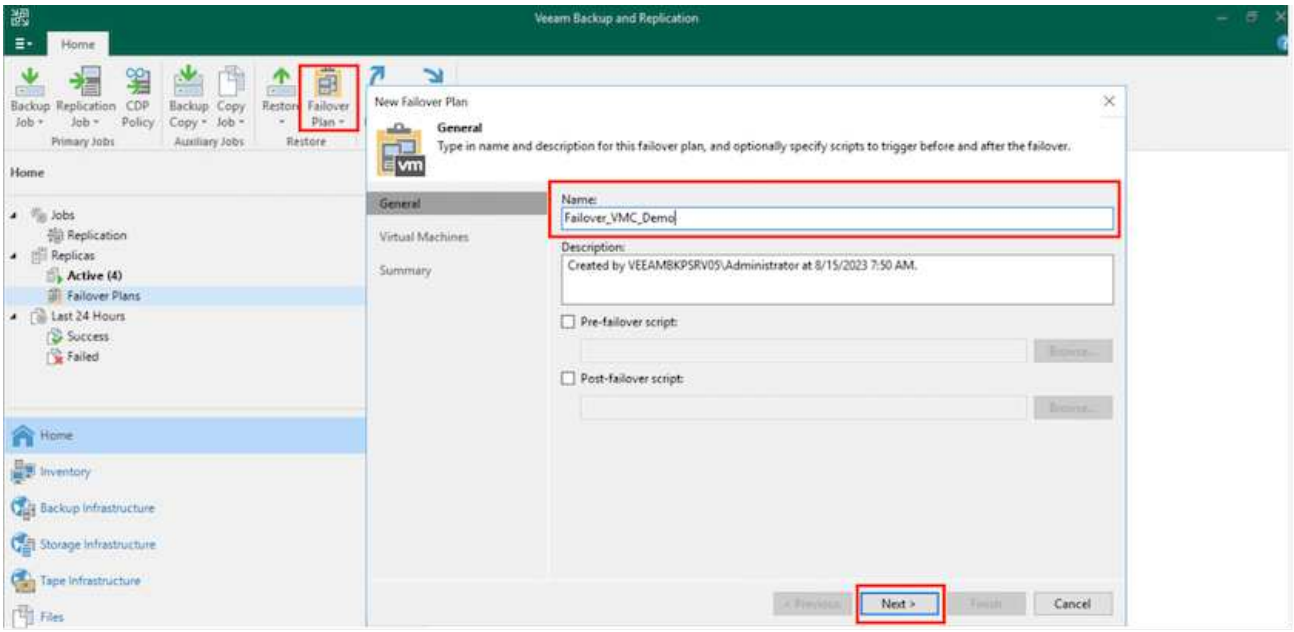
> ⓘ Le nombre maximal de machines virtuelles pouvant être démarrées simultanément lors de l'exécution d'un plan de basculement est de 10.

> ⓘ Pendant le processus de basculement, les machines virtuelles sources ne seront pas mises hors tension.

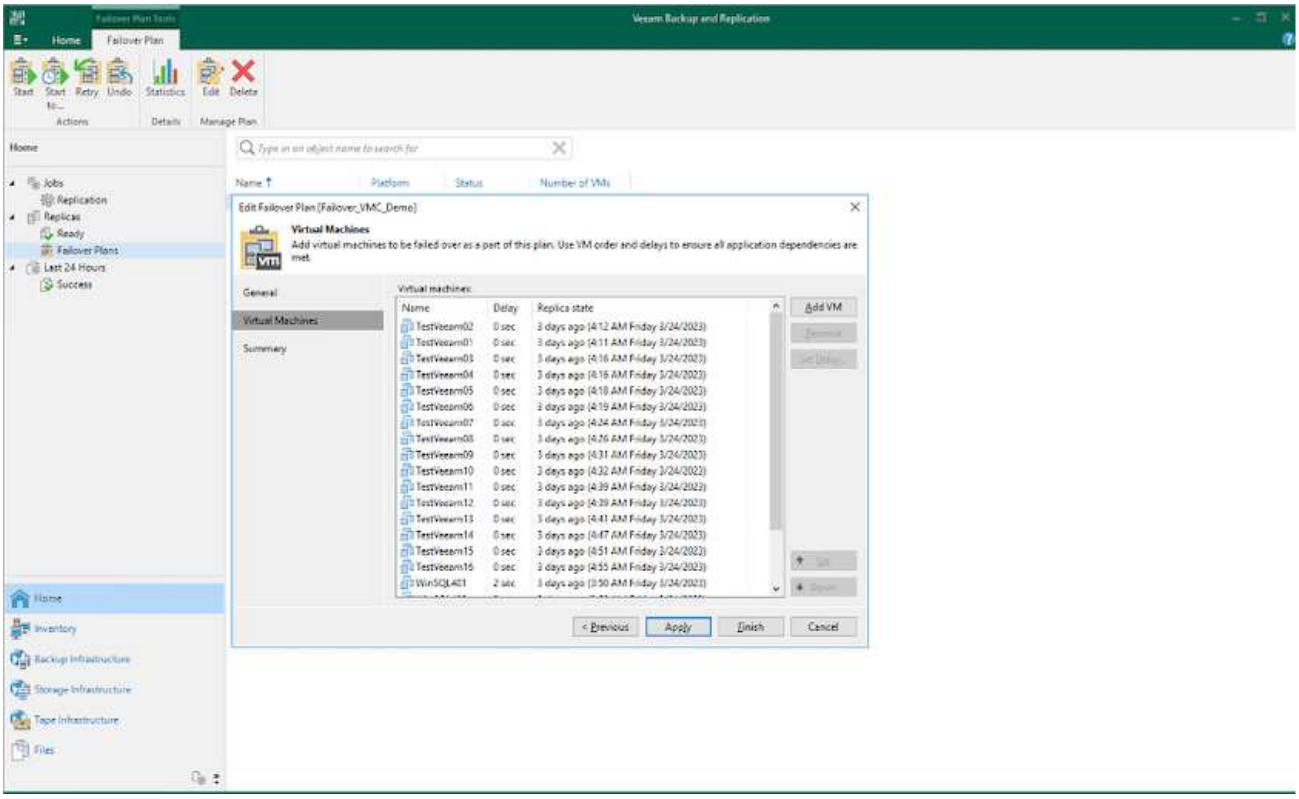
Pour créer le **Plan de basculement**, procédez comme suit :

1. Dans la vue Accueil, sélectionnez **Plan de basculement > VMware vSphere**.
2. Ensuite, donnez un nom et une description au plan. Un script de pré et post-basculement peut être

ajouté selon les besoins. 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 des machines virtuelles et les délais de démarrage pour répondre aux dépendances de l'application.



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

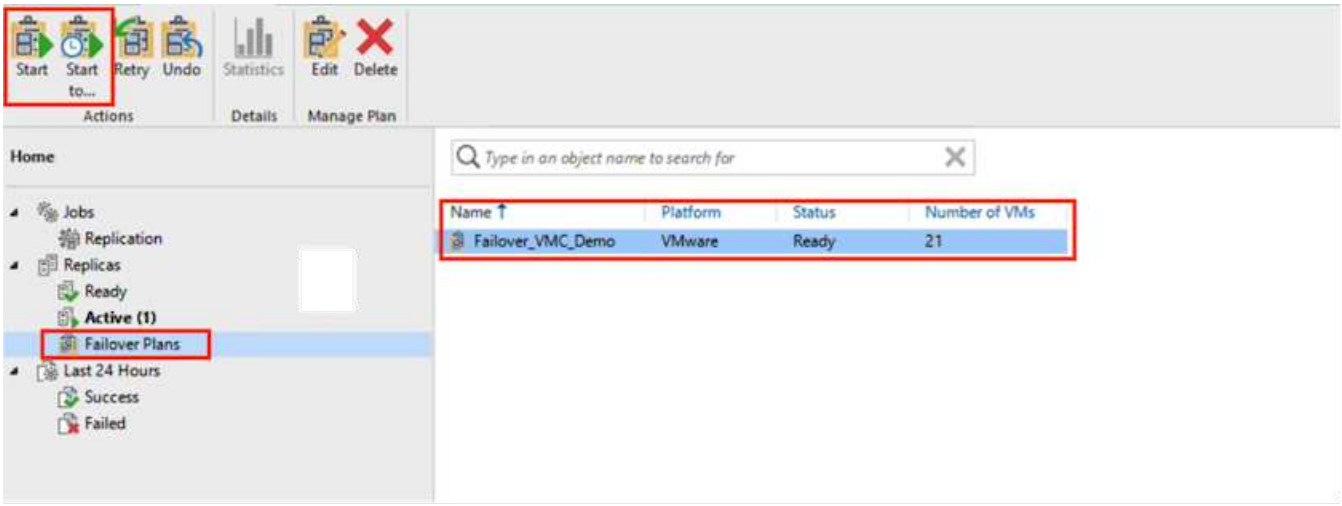
▼ **Étape 3 : Exécuter le plan de basculement**

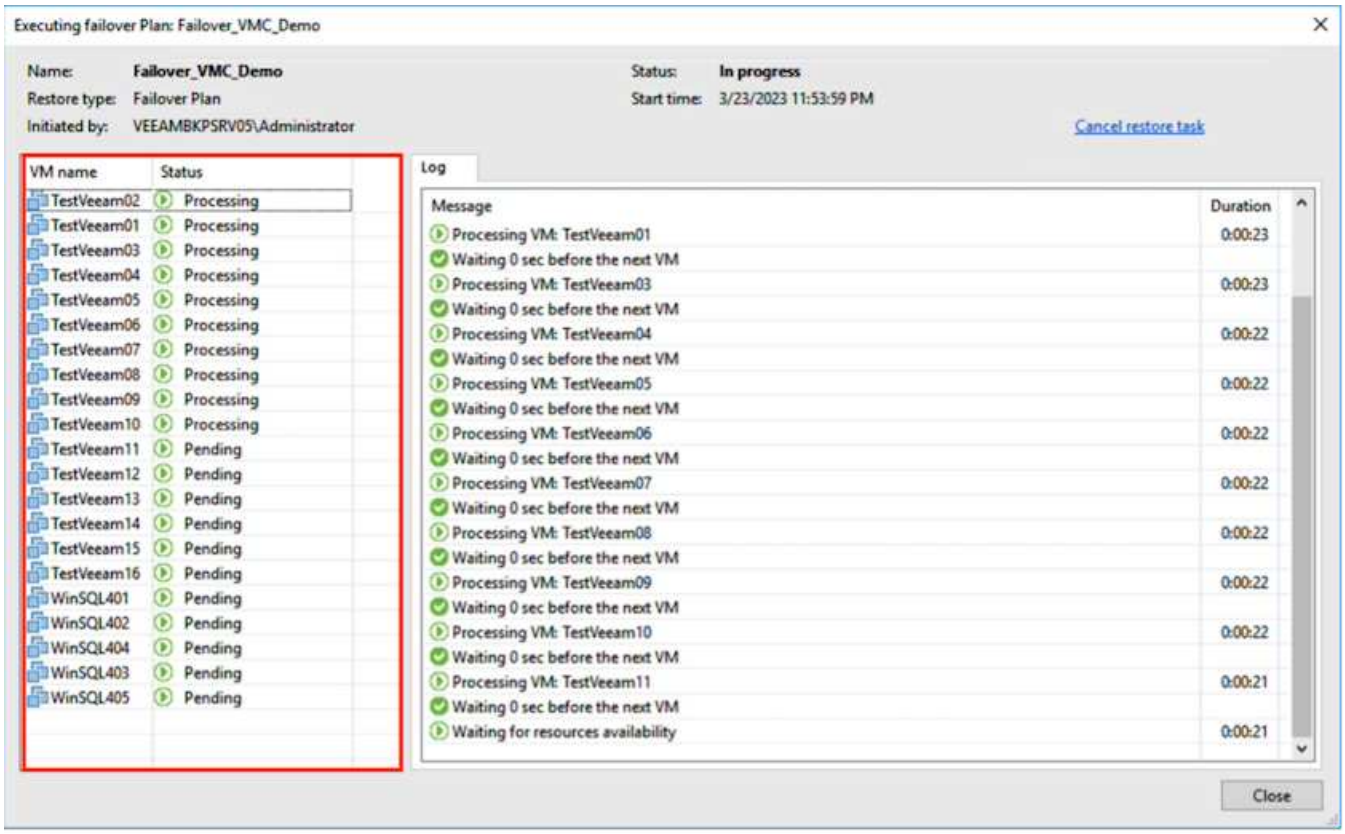
Lors du basculement, la machine virtuelle source du site de production est basculée vers sa réplique sur le

site de reprise après sinistre. Dans le cadre du processus de basculement, Veeam Backup & Replication restaure la réplique de la machine virtuelle au point de restauration requis et déplace toutes les activités d'E/S de la machine virtuelle source vers sa réplique. Les répliques peuvent être utilisées non seulement en cas de catastrophe, mais également pour simuler des exercices de reprise après sinistre. 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.

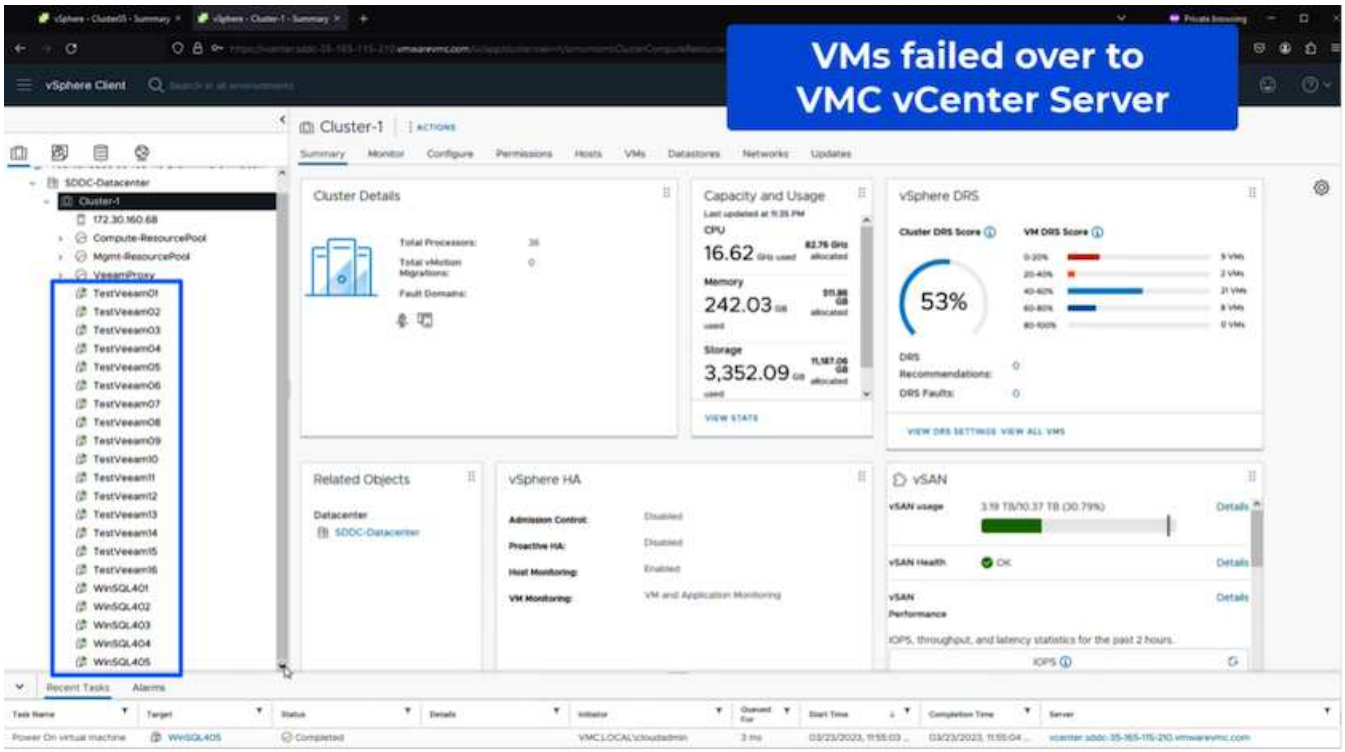
Assurez-vous que la segmentation du réseau est en place pour éviter les conflits IP lors des exercices de reprise après sinistre.

Pour démarrer le plan de basculement, cliquez simplement sur l'onglet **Plans de basculement** et faites un clic droit sur le plan de basculement. Sélectionnez **Démarrer**. Cela basculera en utilisant les derniers points de restauration des répliques de VM. Pour basculer vers des points de restauration spécifiques de répliques de machines virtuelles, sélectionnez **Démarrer vers**.

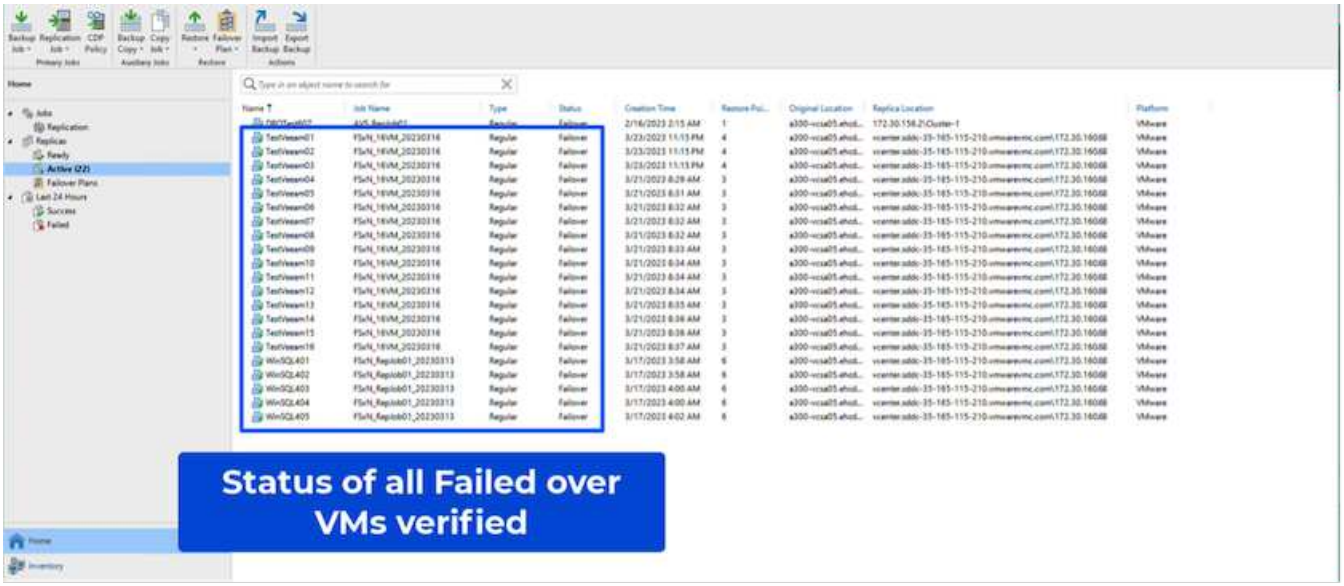




L'état de la réplique de machine virtuelle passe de Prêt à Basculement et les machines virtuelles démarrent sur le cluster/hôte VMware Cloud on AWS SDDC de destination.



Une fois le basculement terminé, le statut des machines virtuelles passera à « Basculement ».



Veeam Backup & Replication arrête toutes les activités de réplication pour la machine virtuelle source jusqu'à ce que sa réplique soit ramenée à l'état Prêt.

Pour des informations détaillées sur les plans de basculement, reportez-vous à"Plans de basculement" .

▼ **Étape 4 : Retour au site de production**

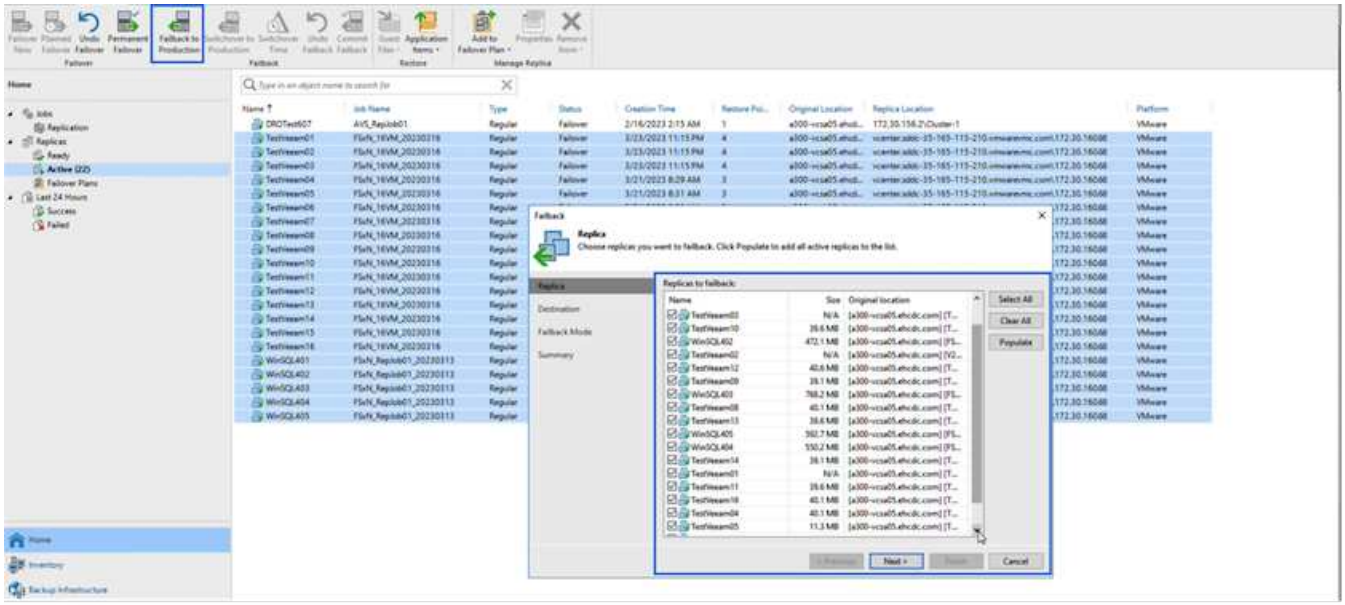
Lorsque le plan de basculement est en cours d'exécution, il est considéré comme une étape intermédiaire et doit être finalisé en fonction des besoins. Les options incluent les suivantes :

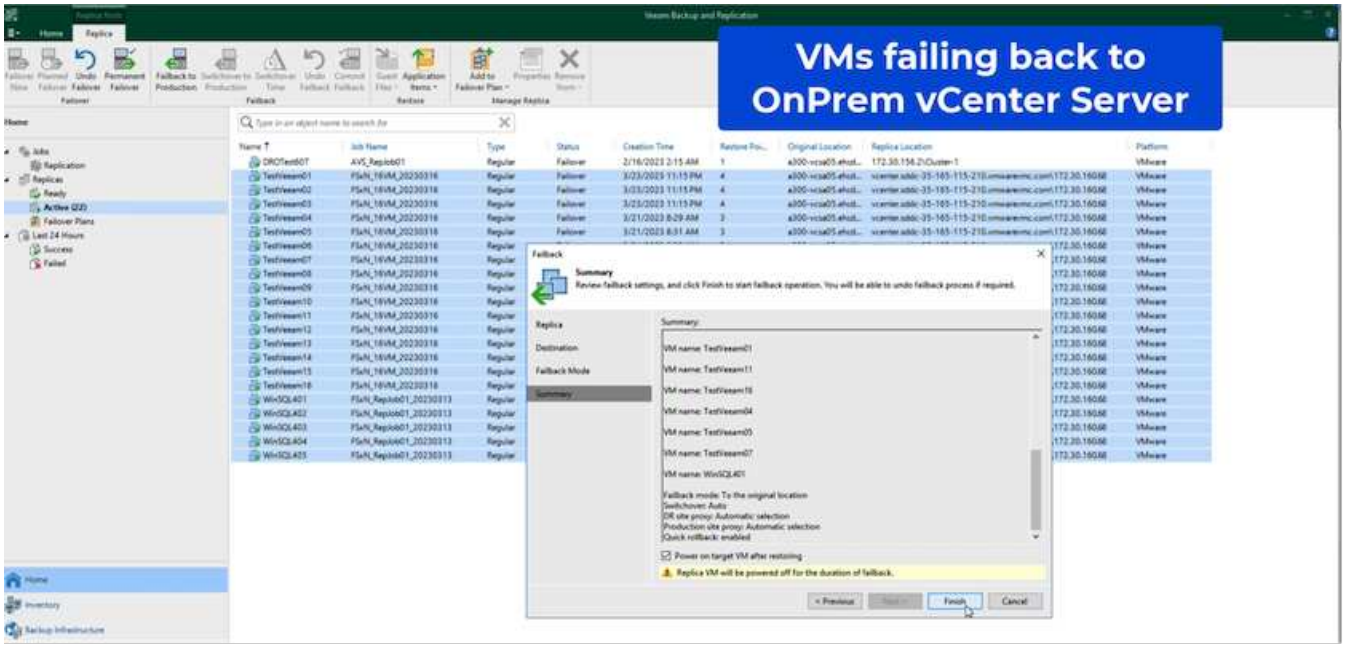
- **Retour à la production** - revenez à la machine virtuelle d'origine et transférez toutes les modifications qui ont eu lieu pendant l'exécution de la réplique de la machine virtuelle vers la machine virtuelle d'origine.

Lorsque vous effectuez une restauration automatique, les modifications sont uniquement transférées mais non publiées. Choisissez **Commit failback** (une fois que la VM d'origine est confirmée comme fonctionnant comme prévu) ou **Annuler la restauration automatique** pour revenir à la réplique de la VM si la VM d'origine ne fonctionne pas comme prévu.

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

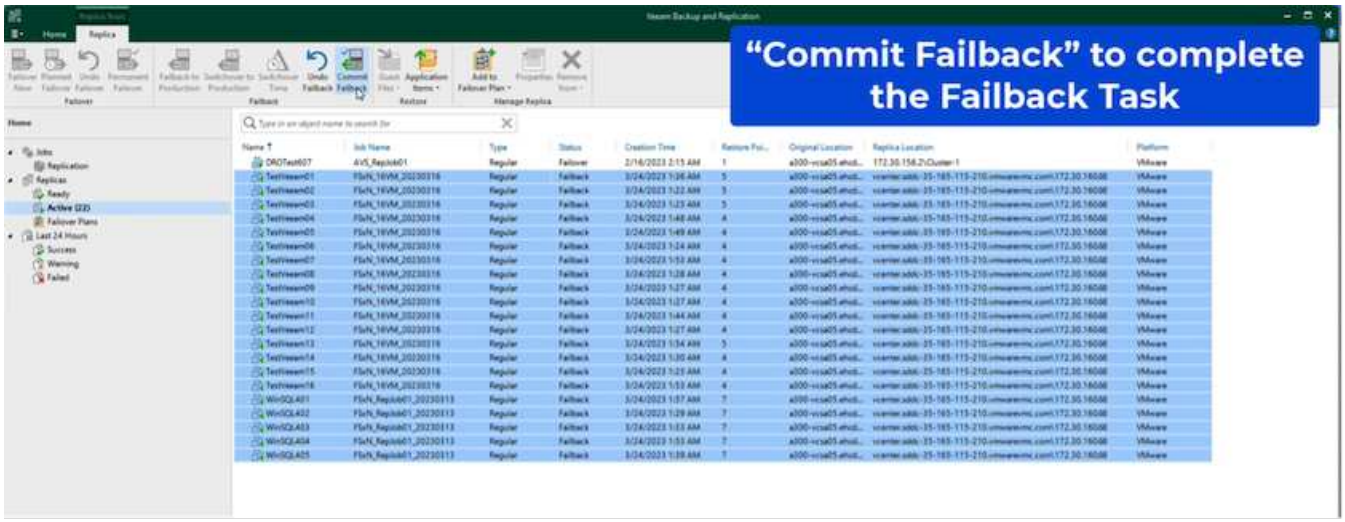
Dans cette démo, le retour à la production a été choisi. La restauration vers la machine virtuelle d'origine a été sélectionnée lors de l'étape Destination de l'assistant et la case à cocher « Mettre sous tension la machine virtuelle après la restauration » a été activée.

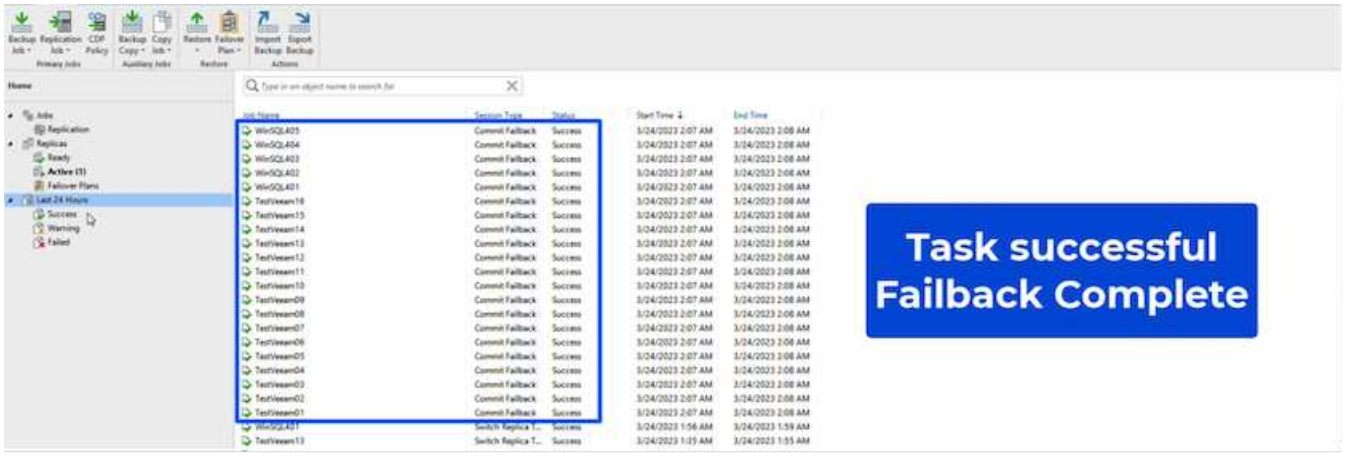




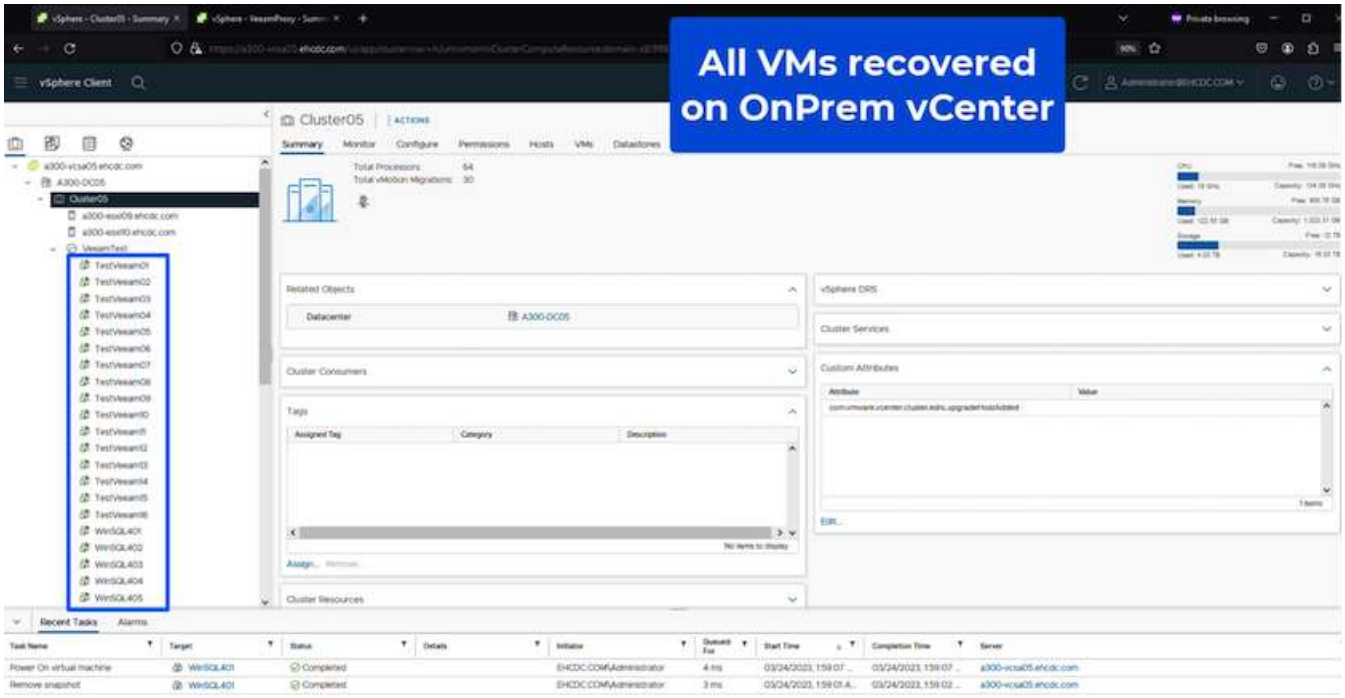
La validation de la restauration est l'un des moyens de finaliser l'opération de restauration. Lorsque la restauration est validée, elle confirme que les modifications envoyées à la machine virtuelle qui est restaurée (la machine virtuelle de production) fonctionnent comme prévu. Après l'opération de validation, Veeam Backup & Replication reprend les activités de réplication pour la machine virtuelle de production.

Pour des informations détaillées sur le processus de restauration automatique, reportez-vous à la documentation Veeam."Basculement et restauration pour la réplication" .





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



Conclusion

La capacité de stockage de données FSx ONTAP permet à Veeam ou à tout outil tiers validé de fournir une solution DR à faible coût à l'aide d'un cluster Pilot Light et sans avoir à créer un grand nombre d'hôtes dans le cluster juste pour héberger la copie de réplique de la machine virtuelle. Cela fournit une solution puissante pour gérer un plan de reprise après sinistre personnalisé et sur mesure et permet également de réutiliser les produits de sauvegarde existants en interne pour répondre aux besoins de reprise après sinistre, permettant ainsi une reprise après sinistre basée sur le cloud en quittant les centres de données DR sur site. Le basculement peut être effectué sous forme de basculement planifié ou de basculement en un clic en cas de sinistre et une décision est prise pour activer le site DR.

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

Migrer les charges de travail sur AWS/VMC

TR 4942 : Migration des charges de travail vers la banque de données FSx ONTAP à l'aide de VMware HCX

Un cas d'utilisation courant de VMware Cloud (VMC) sur Amazon Web Services (AWS), avec son magasin de données NFS supplémentaire sur Amazon FSx ONTAP, est la migration des charges de travail VMware. VMware HCX est une option privilégiée et fournit diverses méthodes de migration pour déplacer des machines virtuelles (VM) sur site et leurs données, exécutées sur n'importe quel magasin de données pris en charge par VMware, vers des magasins de données VMC, qui incluent des magasins de données NFS supplémentaires sur FSx ONTAP.

Présentation : Migration de machines virtuelles avec VMware HCX, banques de données supplémentaires FSx ONTAP et VMware Cloud

VMware HCX est principalement une plate-forme de mobilité conçue pour simplifier la migration des charges de travail, le rééquilibrage des charges de travail et la continuité des activités 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 sinistre (DR).

Ce document fournit des instructions étape par étape pour le déploiement et la configuration de VMware HCX, y compris tous ses principaux composants, sur site et côté centre de données cloud, ce qui permet divers mécanismes de migration de machines virtuelles.

Pour plus d'informations, voir "Guide de l'utilisateur de VMware HCX" et "Liste de contrôle d'installation B - HCX avec un environnement de destination SDDC VMware Cloud sur AWS" .

▼ **Étapes de haut niveau**

Cette liste fournit les étapes de haut niveau pour installer et configurer VMware HCX :

1. Activez HCX pour le centre de données défini par logiciel (SDDC) VMC via VMware Cloud Services Console.
2. Téléchargez et déployez le programme d'installation OVA du connecteur HCX sur le serveur vCenter local.
3. Activez HCX avec une clé de licence.
4. Associez le connecteur VMware HCX sur site à VMC HCX Cloud Manager.

5. Configurez le profil réseau, le profil de calcul et le maillage de services.
6. (Facultatif) Effectuez une extension de réseau pour étendre le réseau et éviter la ré-IP.
7. Validez l'état de l'appliance et assurez-vous que la migration est possible.
8. Migrer les charges de travail de la machine virtuelle.

▼ Prérequis

Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, consultez la section "Préparation de l'installation" . Une fois les conditions préalables 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 HCX activé, le plug-in vCenter est déployé et est accessible à l'aide de la console vCenter pour la gestion.

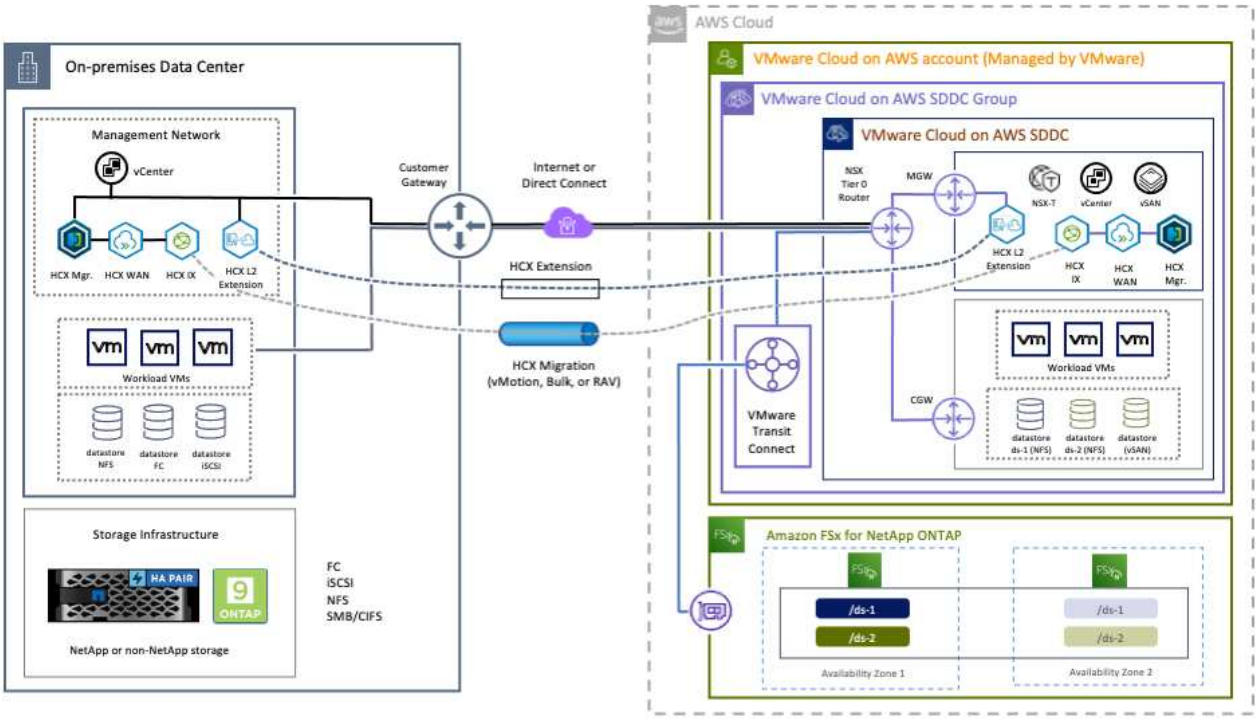
Les étapes d'installation suivantes doivent être effectuées avant de procéder à l'activation et au déploiement de HCX :

1. Utilisez un SDDC VMC existant ou créez un nouveau SDDC en suivant ceci"Lien NetApp" ou ceci "Lien VMware" .
2. Le chemin réseau de l'environnement vCenter local vers le SDDC VMC doit prendre en charge la migration des machines virtuelles à l'aide de vMotion.
3. Assurez-vous que les informations requises "règles et ports du pare-feu" sont autorisés pour le trafic vMotion entre le vCenter Server local et le vCenter SDDC.
4. Le volume NFS FSx ONTAP doit être monté en tant que banque de données supplémentaire dans le SDDC VMC. Pour attacher les banques de données NFS au cluster approprié, suivez les étapes décrites dans ce"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 via un VPN site à site à AWS VPC, ce qui a permis la connectivité sur site à AWS et au SDDC cloud VMware via une passerelle de transit externe. Le trafic de migration HCX et d'extension de réseau circule sur Internet entre le SDDC de destination cloud VMware et sur site. Cette architecture peut être modifiée pour utiliser des interfaces virtuelles privées Direct Connect.

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



Déploiement de la solution

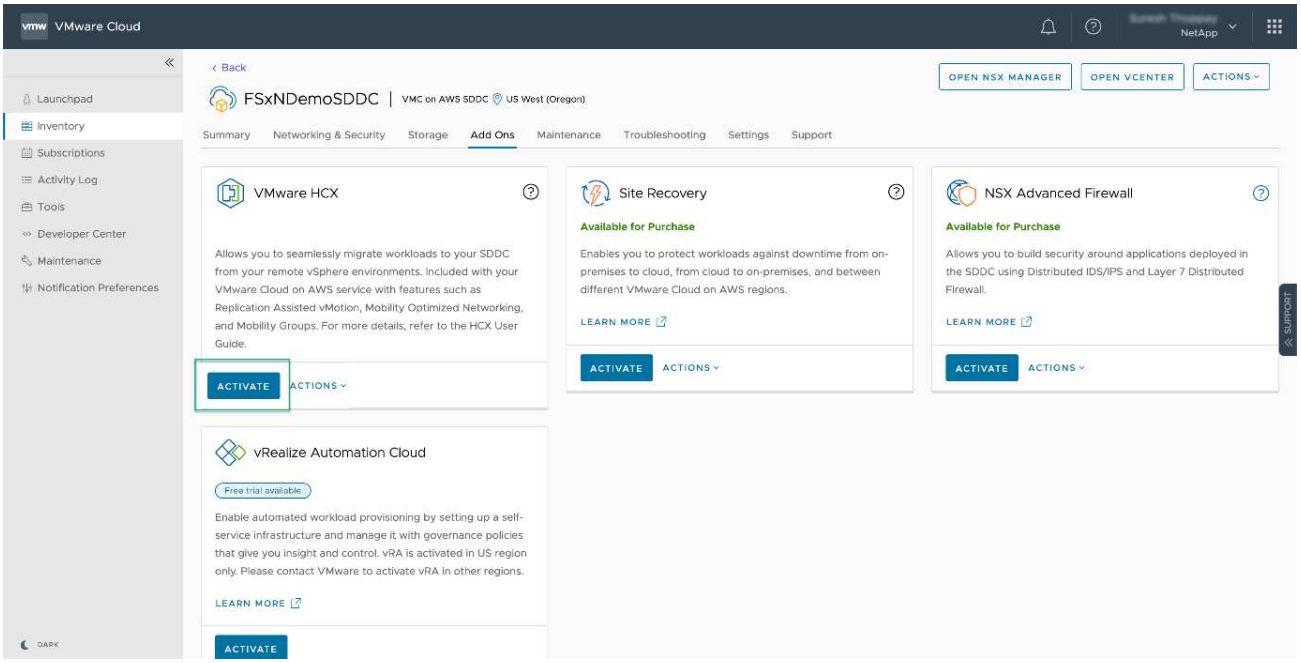
Suivez la série d'étapes pour terminer le déploiement de cette solution :

▼ **Étape 1 : Activez HCX via VMC SDDC à l'aide de l'option Modules complémentaires**

Pour effectuer l'installation, procédez comme suit :

1. Connectez-vous à la console VMC à l'adresse "vmc.vmware.com" et accéder à l'inventaire.
2. Pour sélectionner le SDDC approprié et accéder aux modules complémentaires, cliquez sur Afficher les détails sur le SDDC et sélectionnez l'onglet Modules complémentaires.
3. Cliquez sur Activer pour VMware HCX.

Cette étape prend jusqu'à 25 minutes.

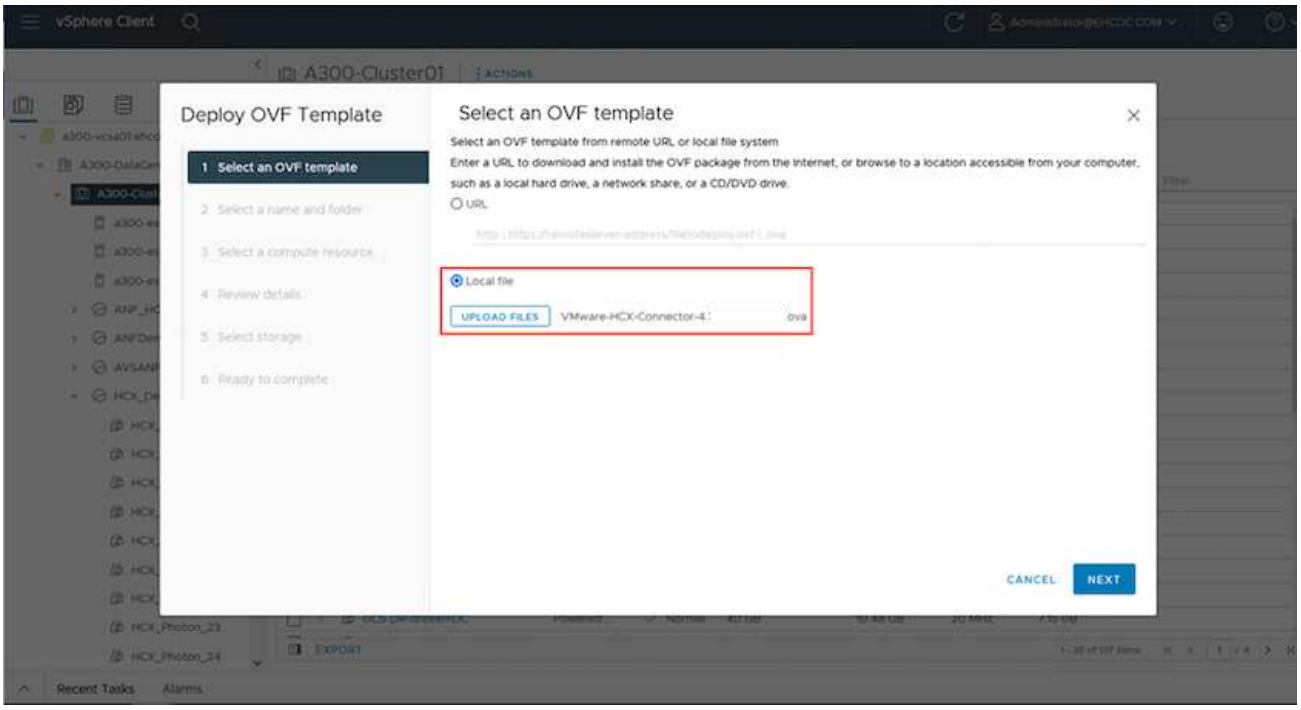


4. Une fois le déploiement terminé, validez le déploiement en confirmant que HCX Manager et ses plug-ins associés sont disponibles dans la console vCenter.
5. Créez les pare-feu de passerelle de gestion appropriés pour ouvrir les ports nécessaires à l'accès à HCX Cloud Manager. HCX Cloud Manager est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

▼ Étape 2 : Déployer le programme d'installation OVA sur le serveur vCenter local

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

1. Depuis la console VMC, accédez au tableau de bord HCX, accédez 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. Une fois le connecteur HCX téléchargé, déployez l'OVA sur le serveur vCenter local. Cliquez avec le bouton droit sur vSphere Cluster et sélectionnez l'option Déployer le modèle OVF.

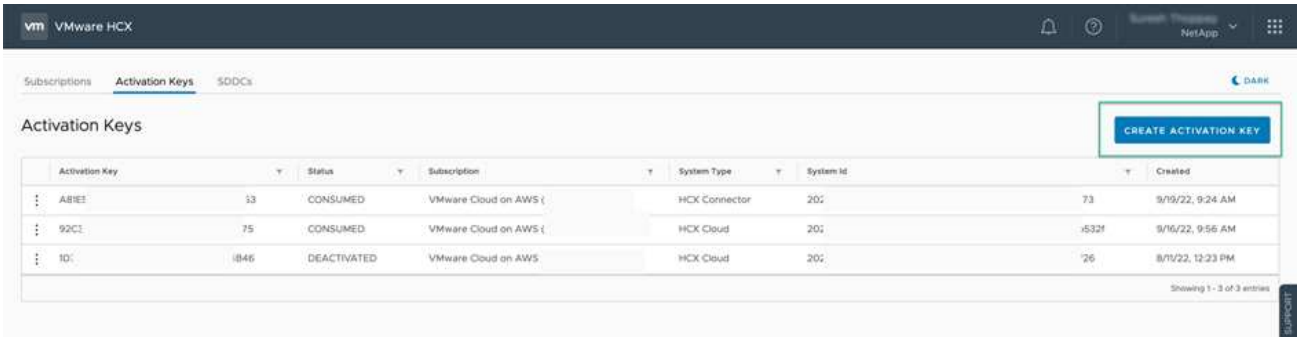


3. Saisissez les informations requises dans l'assistant Déployer le modèle OVF, cliquez sur Suivant, puis sur Terminer pour déployer le connecteur VMware HCX OVA.
4. Allumez l'appliance virtuelle manuellement. Pour obtenir des instructions étape par étape, accédez à "Guide de l'utilisateur de VMware HCX" .

▼ **Étape 3 : Activer HCX Connector avec la clé de licence**

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

1. Depuis la console VMware Cloud, accédez à Inventaire, sélectionnez le SDDC et cliquez sur Afficher les détails. Dans l'onglet Modules complémentaires, 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. Copiez 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 l'adresse `"https://hcxconnectorIP:9443"` en utilisant les informations d'identification de l'administrateur.

Utilisez le mot de passe défini lors du déploiement OVA.

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

Le connecteur HCX sur site doit disposer d'un accès Internet pour que l'activation se termine avec succès.

5. Sous Emplacement du centre de données, indiquez l'emplacement souhaité pour l'installation de VMware HCX Manager sur site. 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) et les informations d'identification du serveur vCenter, puis cliquez sur Continuer.

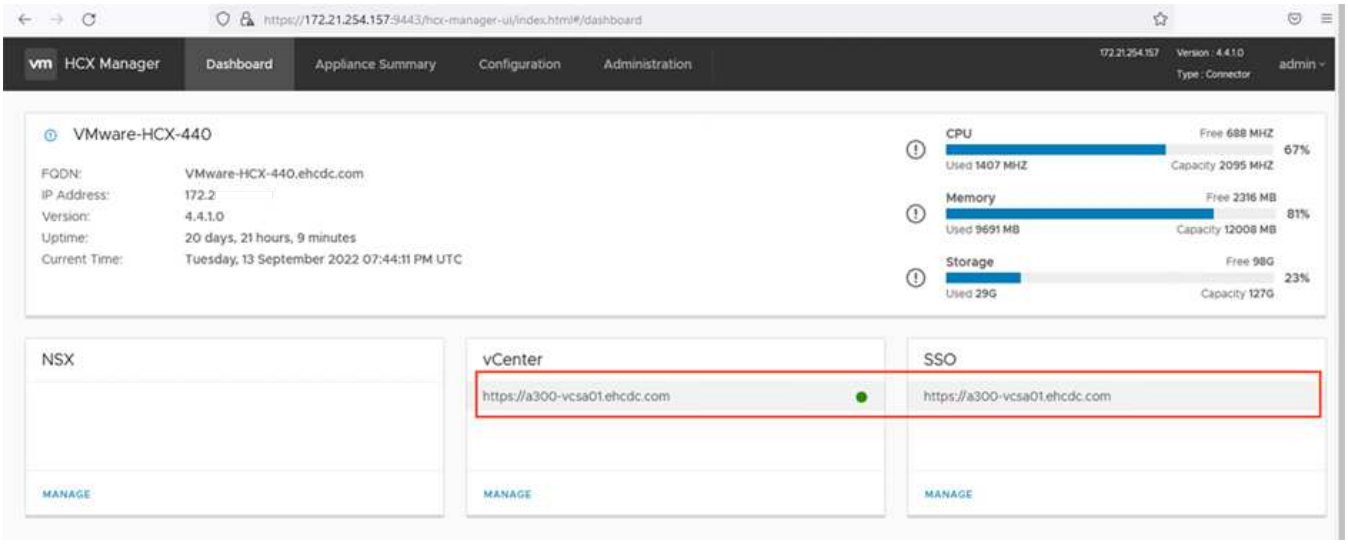
Utilisez le FQDN pour éviter les problèmes de communication ultérieurs.

9. Sous Configurer SSO/PSC, indiquez le nom de domaine complet ou l'adresse IP du Platform Services Controller et cliquez sur Continuer.

Saisissez l'adresse IP ou le nom de domaine complet du serveur vCenter.

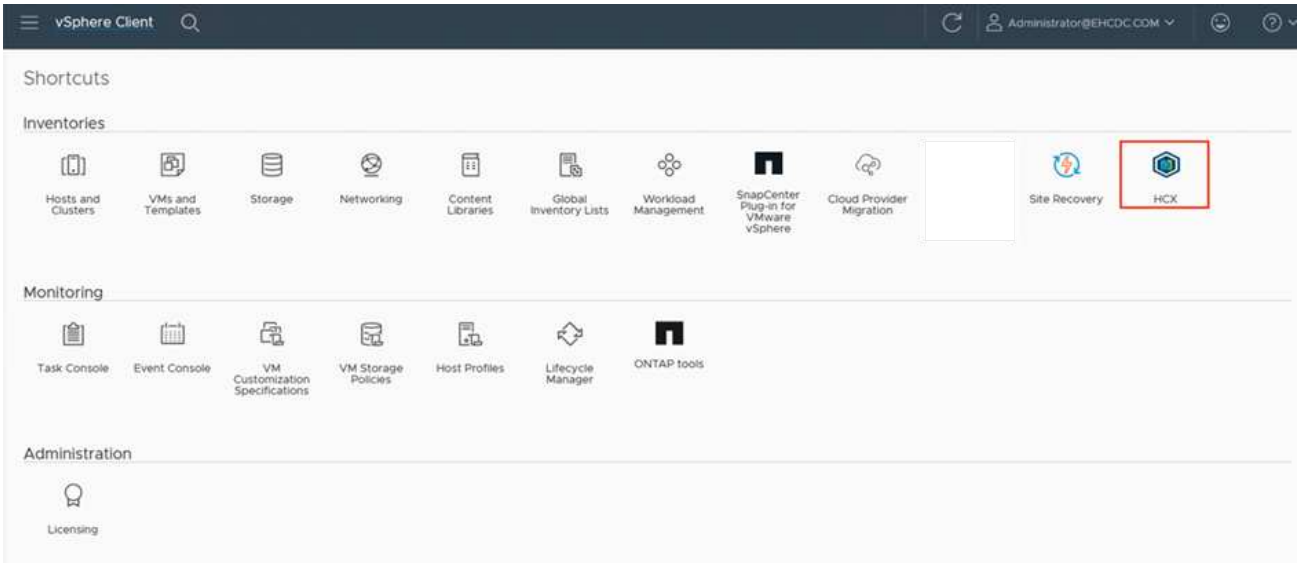
10. Vérifiez que les informations sont correctement saisies et cliquez sur Redémarrer.
11. Une fois terminé, le serveur vCenter s'affiche en vert. Le serveur vCenter et SSO doivent tous deux disposer des paramètres de configuration corrects, qui doivent être identiques à ceux de la page précédente.

Ce processus devrait prendre environ 10 à 20 minutes pour que le plug-in soit ajouté au serveur vCenter.

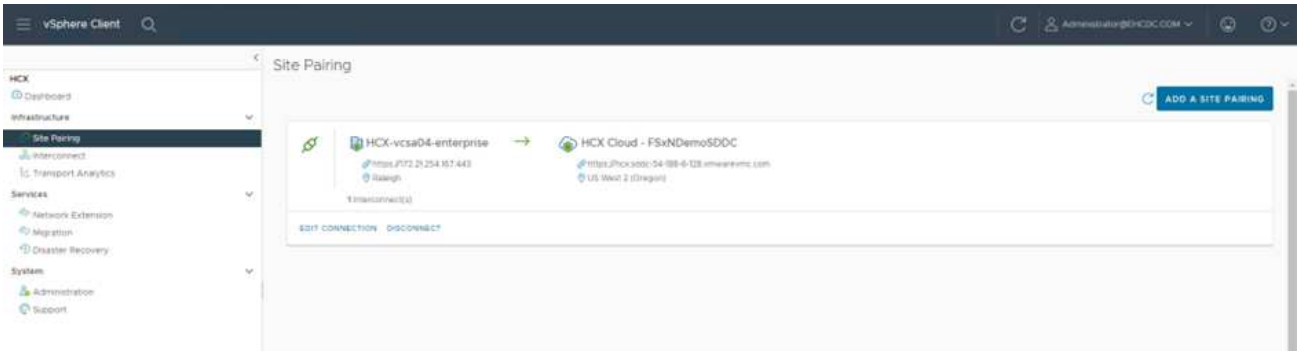


▼ Étape 4 : Associez le connecteur VMware HCX sur site à VMC HCX Cloud Manager

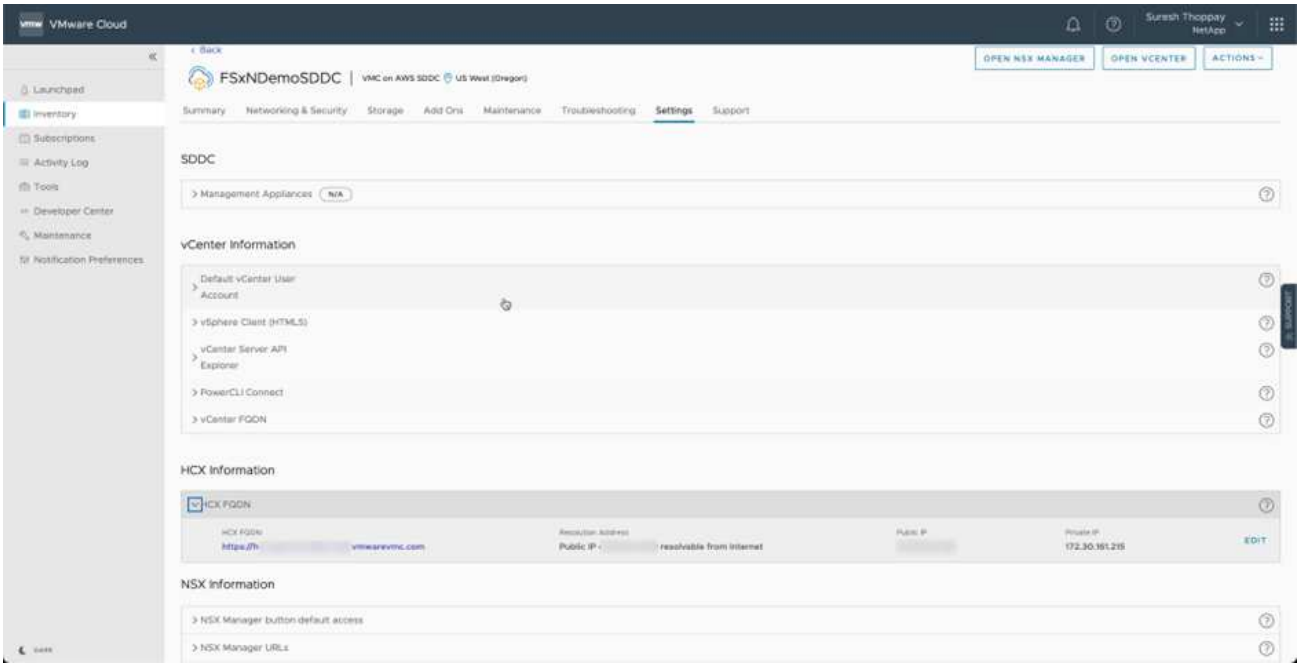
1. Pour créer une paire de sites entre le serveur vCenter local et le SDDC VMC, connectez-vous au serveur vCenter local et accédez au plug-in HCX vSphere Web Client.

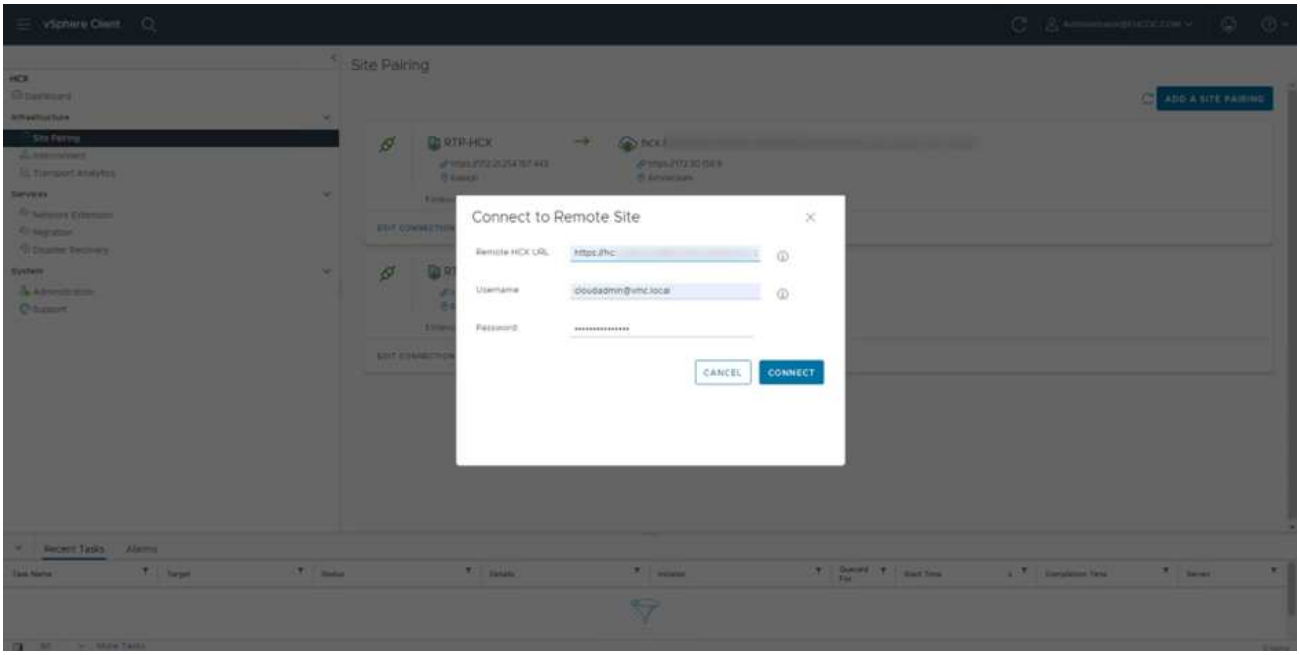


2. Sous Infrastructure, cliquez sur Ajouter un appariement de sites. Pour authentifier le site distant, saisissez l'URL ou l'adresse IP de VMC HCX Cloud Manager et les informations d'identification du rôle CloudAdmin.



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





3. Pour lancer l'appairage du site, cliquez sur Connecter.

> VMware HCX Connector doit pouvoir communiquer avec l'adresse IP de HCX Cloud Manager via le port 443.

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

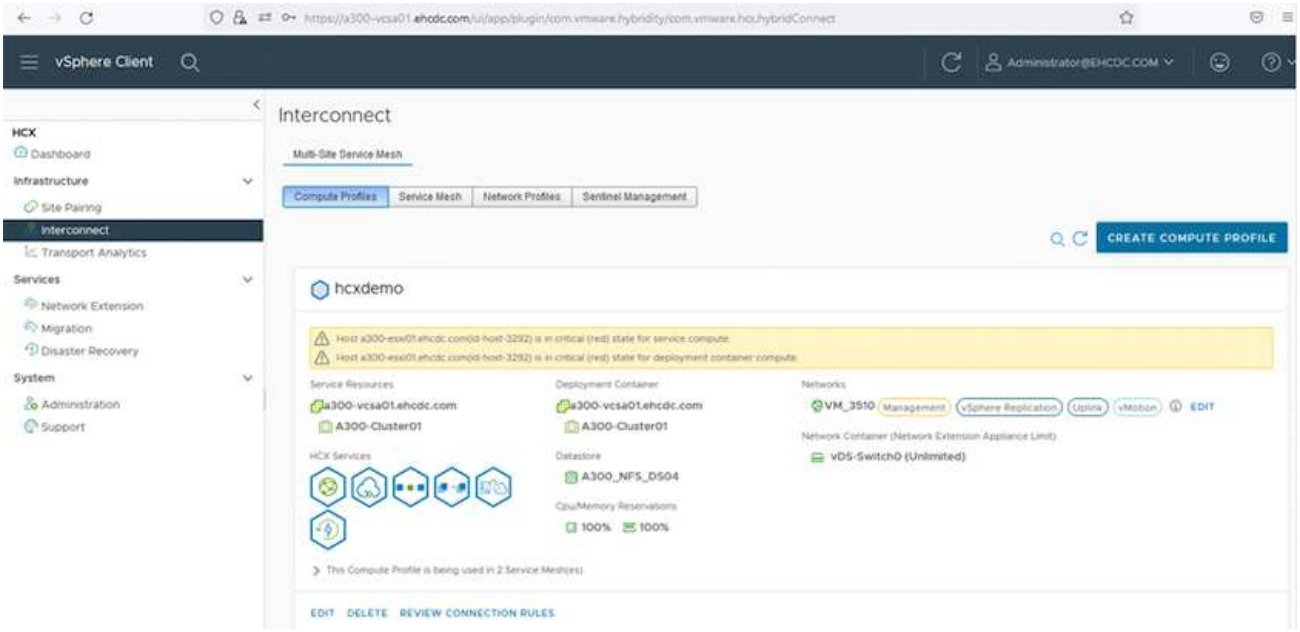
▼ **Étape 5 : Configurer le profil réseau, le profil de calcul et le maillage de services**

L'appliance VMware HCX Interconnect (HCX-IX) fournit des fonctionnalités de tunnel sécurisé sur Internet et des connexions privées au site cible qui permettent la réplication et les fonctionnalités basées sur vMotion. L'interconnexion fournit le cryptage, l'ingénierie du trafic et un SD-WAN. Pour créer l'appliance d'interconnexion HCI-IX, procédez comme suit :

1. Sous Infrastructure, sélectionnez Interconnexion > Maillage de services multisites > Profils de calcul > Créer un profil de calcul.

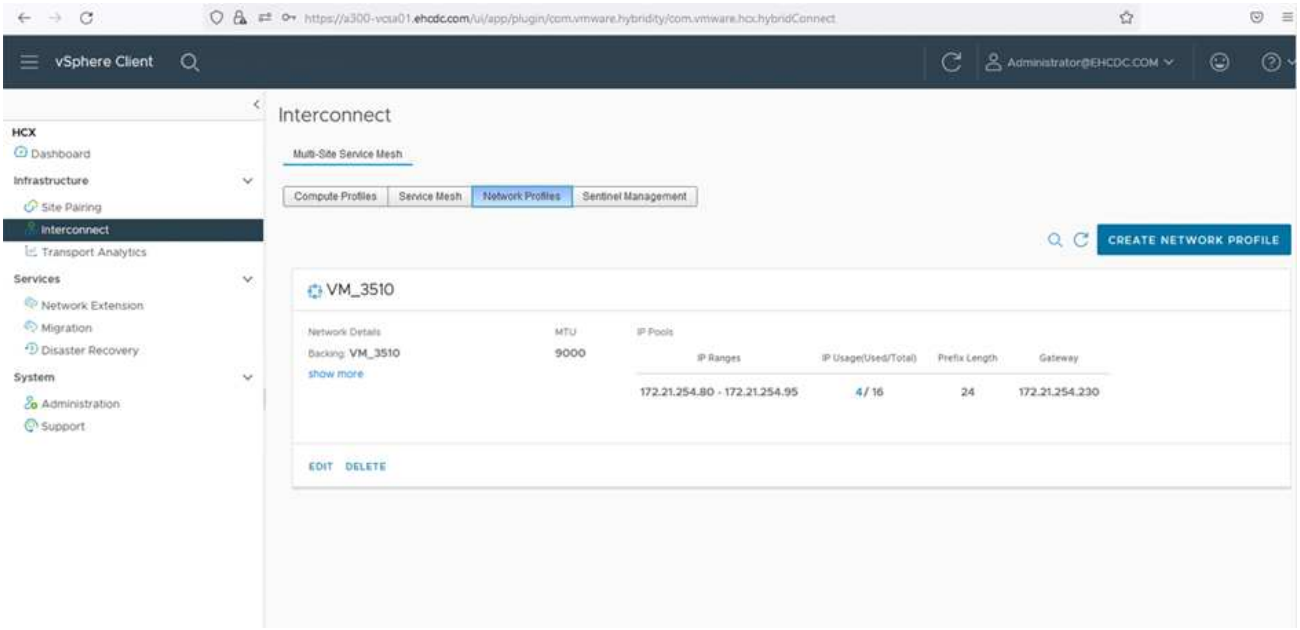
> Les profils de calcul contiennent les paramètres de calcul, de stockage et de déploiement réseau requis pour déployer une appliance virtuelle d'interconnexion. Ils précisent également quelle partie du centre de données VMware sera accessible au service HCX.

Pour des instructions détaillées, voir "Création d'un profil de calcul" .



2. Une fois le profil de calcul créé, créez le profil réseau en sélectionnant Multi-Site Service Mesh > 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 nécessitera deux adresses IP ou plus. Ces adresses IP seront attribuées à partir du réseau de gestion aux appliances virtuelles.



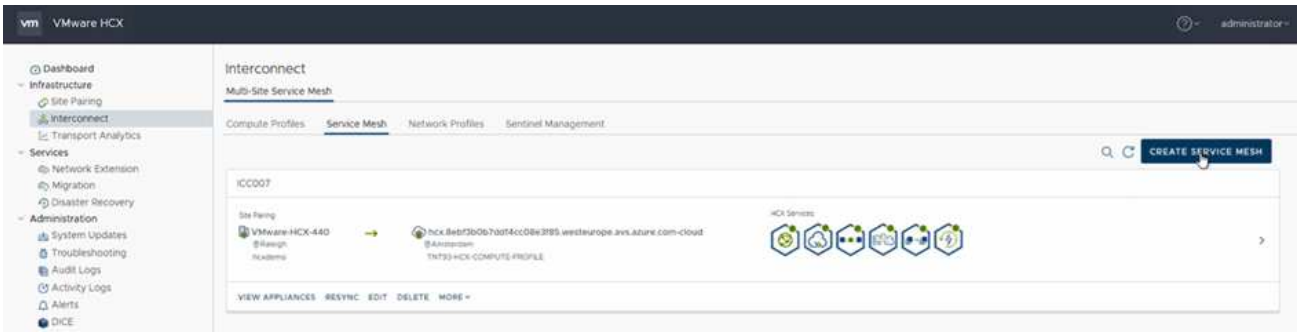
Pour des instructions détaillées, voir "Création d'un profil réseau" .

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

4. Pour créer un maillage de services, sélectionnez l'onglet Maillage de services dans l'option

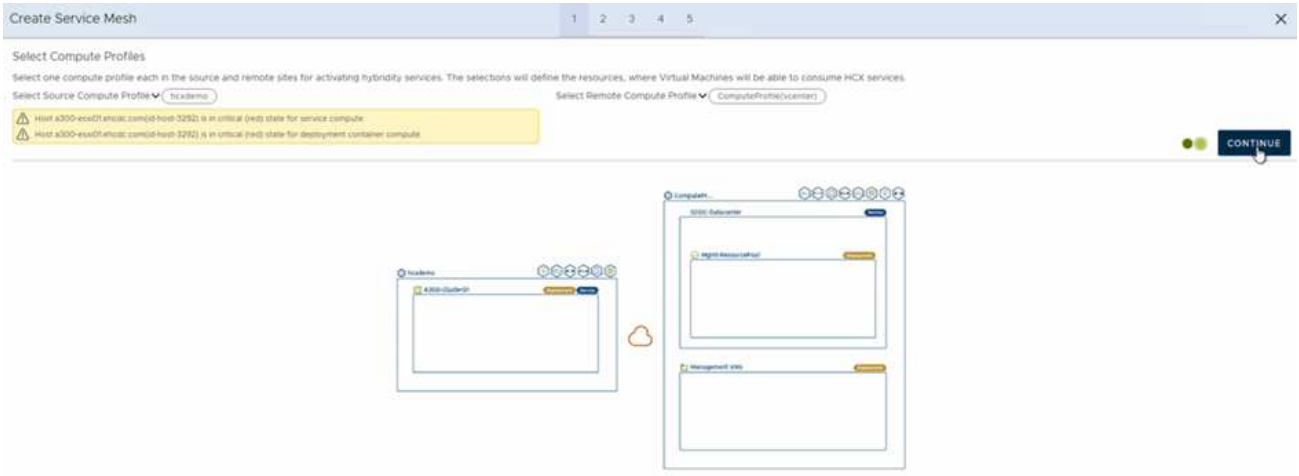
Interconnexion et sélectionnez les sites SDDC locaux et VMC.

Le maillage de services établit une paire de profils de calcul et de réseau locaux et distants.

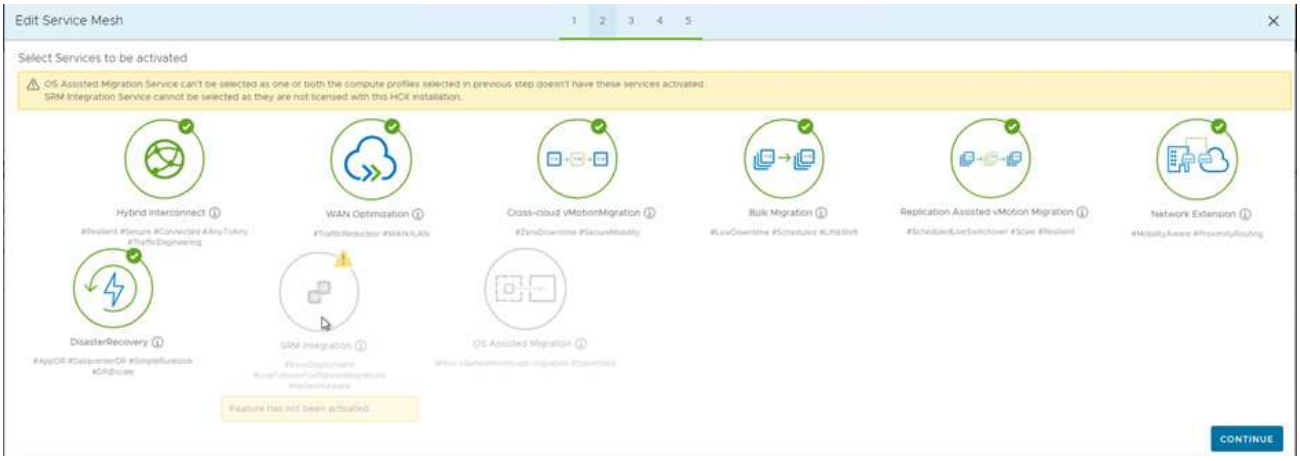


Une partie de ce processus implique le déploiement d'appliances HCX qui seront automatiquement configurées sur les sites source et cible, créant ainsi une structure de transport sécurisée.

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

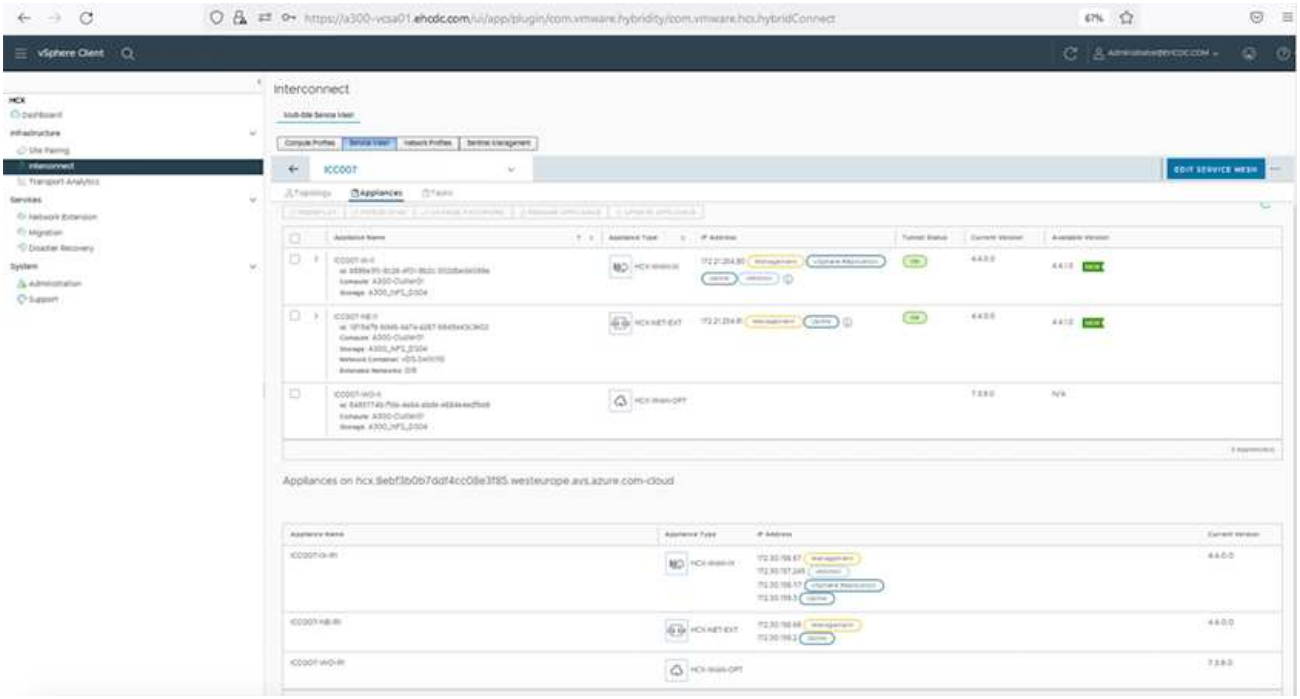


6. Sélectionnez le service à activer et cliquez sur Continuer.



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

7. Créez un nom pour le maillage de services et cliquez sur Terminer pour commencer le processus de création. Le déploiement devrait prendre environ 30 minutes. Une fois le maillage de services configuré, l'infrastructure virtuelle et le réseau nécessaires à la migration des machines virtuelles de charge de travail ont été créés.



▼ **Étape 6 : Migration des charges de travail**

HCX fournit des services de migration bidirectionnelle entre deux ou plusieurs environnements distincts tels que les SDDC sur site et VMC. Les charges de travail des applications peuvent être migrées vers et depuis les sites activés par HCX à l'aide de diverses technologies de migration telles que la migration en masse HCX, HCX vMotion, la migration à froid HCX, HCX Replication Assisted vMotion (disponible avec l'édition HCX Enterprise) et la migration assistée par le 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 de processeur, de mémoire, de stockage et de réseau affichées sur cet objet ne représentent pas la consommation réelle sur l'hyperviseur physique hébergeant l'appliance IX.

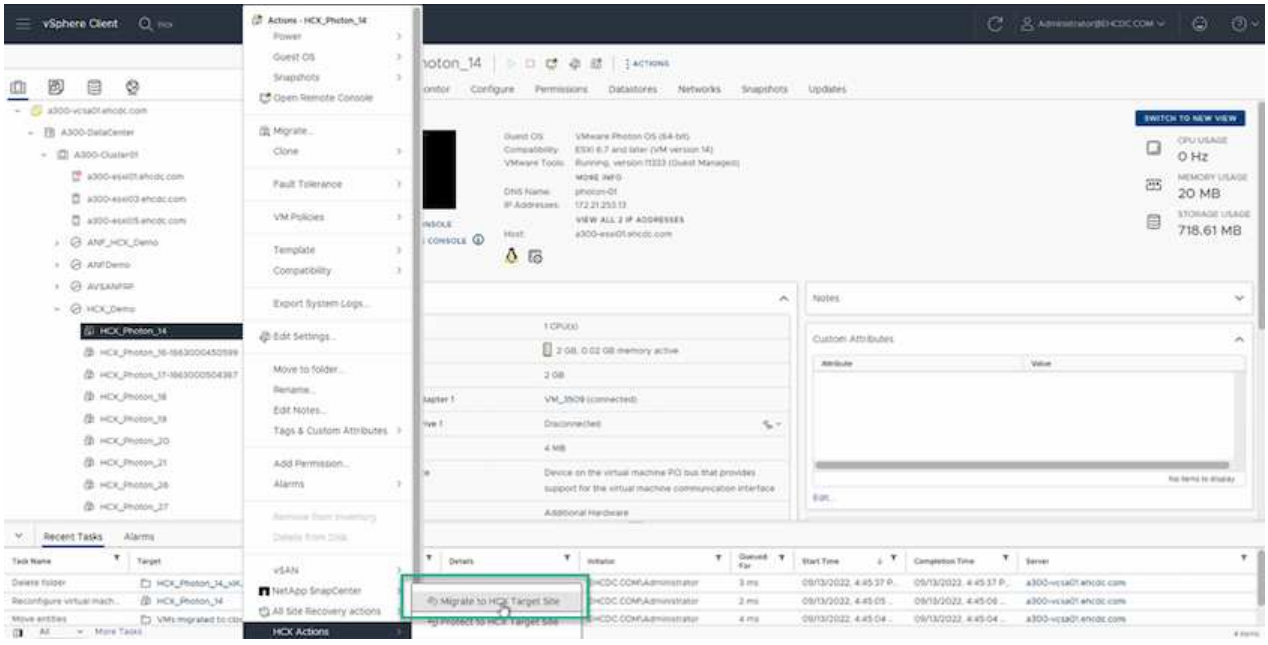


▼ VMware HCX vMotion

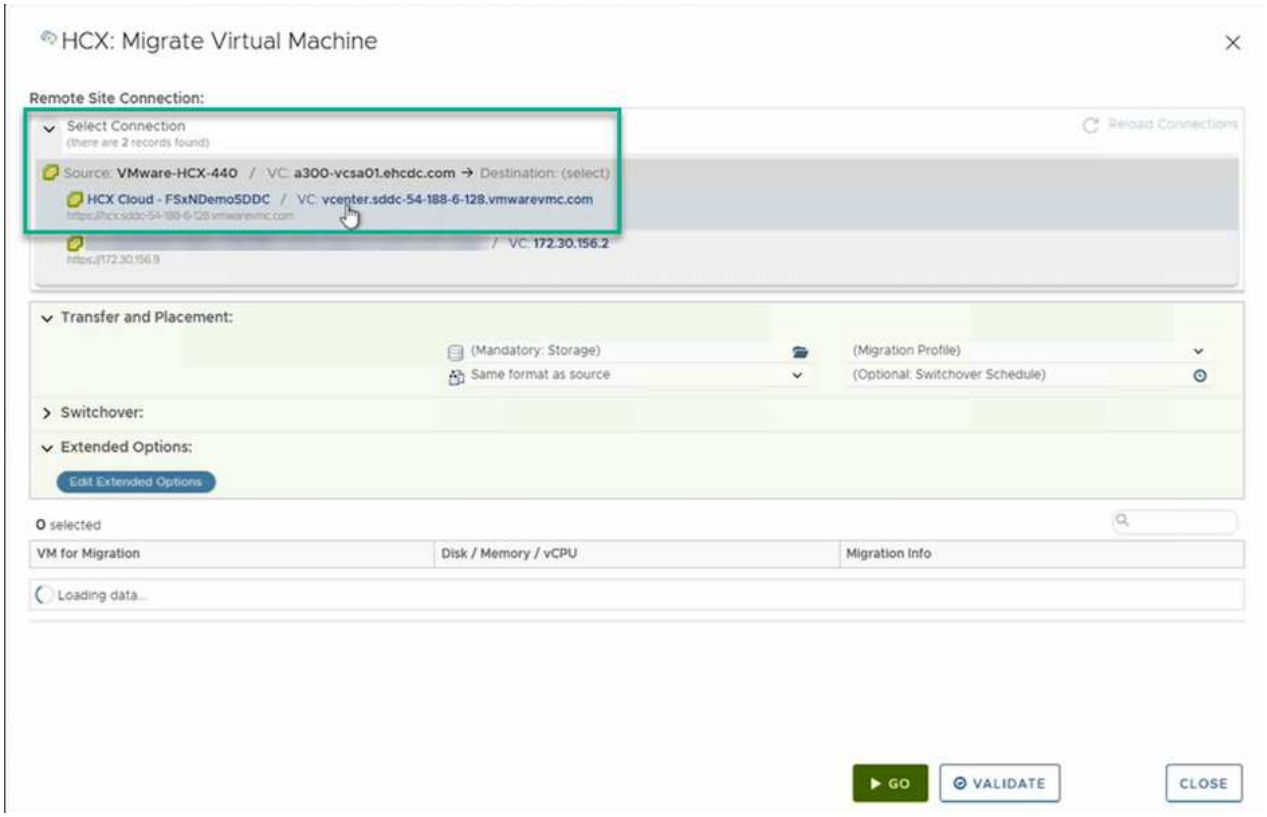
Cette section décrit le mécanisme HCX vMotion. Cette technologie de migration utilise le protocole VMware vMotion pour migrer une machine virtuelle vers VMC SDDC. L'option de migration vMotion est utilisée pour migrer l'état de la machine virtuelle d'une seule machine virtuelle à la fois. Il n'y a aucune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

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

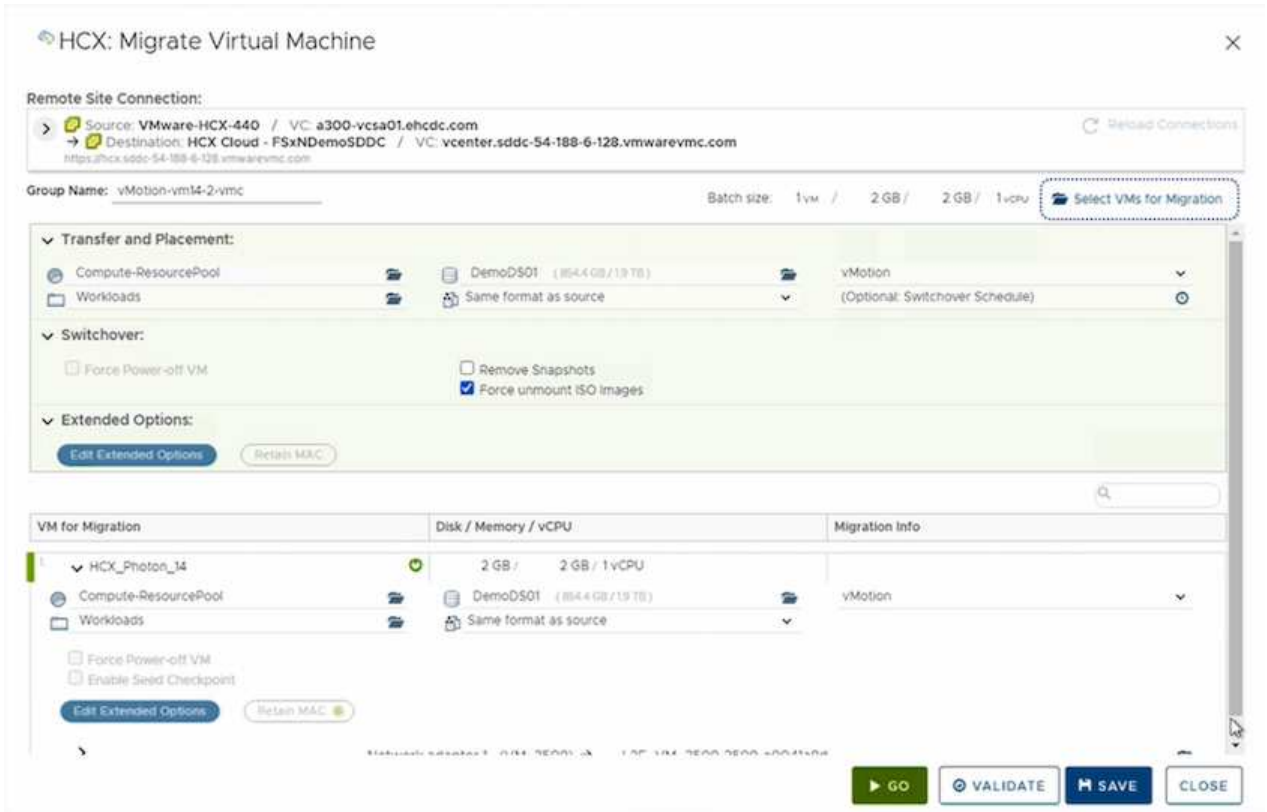
1. À partir du client vSphere sur site, accédez à Inventaire, cliquez avec le bouton droit sur la machine virtuelle à migrer et sélectionnez Actions HCX > Migrer vers le site cible HCX.



2. Dans l'assistant Migrer la machine virtuelle, sélectionnez la connexion au site distant (SDDC VMC cible).



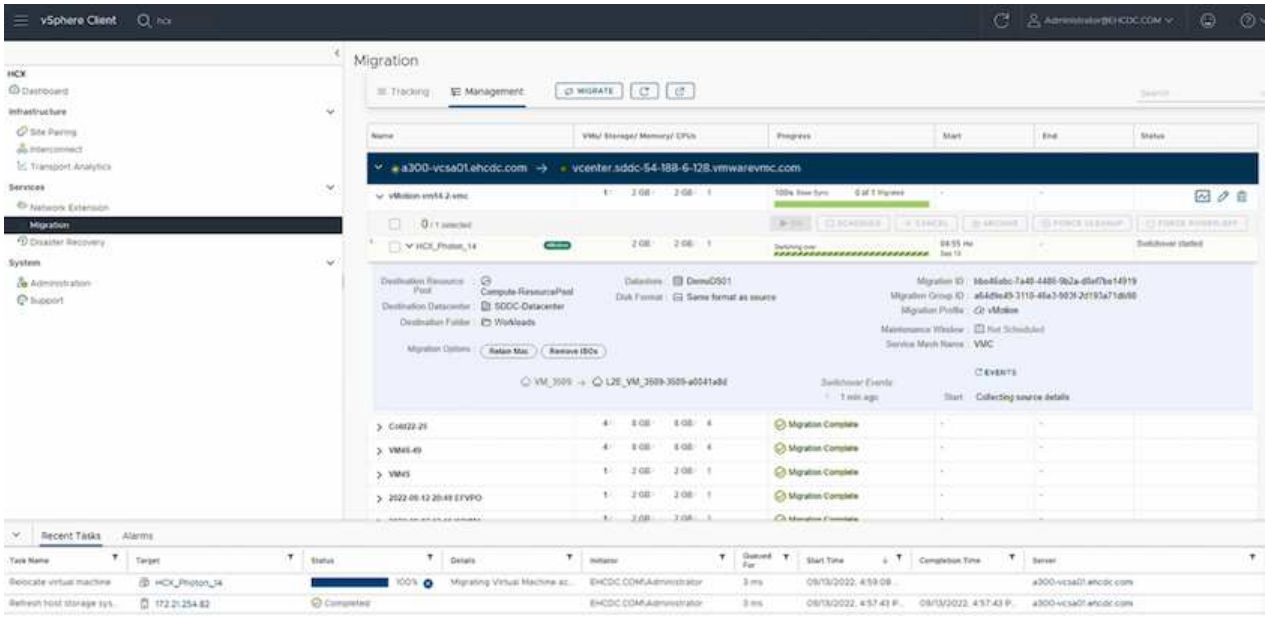
3. Ajoutez un nom de groupe et sous Transfert et placement, mettez à jour les champs obligatoires (Cluster, Stockage et Réseau de destination), cliquez sur Valider.



4. Une fois les vérifications de validation terminées, cliquez sur Aller 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 limitations de HCX vMotion, consultez "Comprendre VMware HCX vMotion et la migration à froid" .

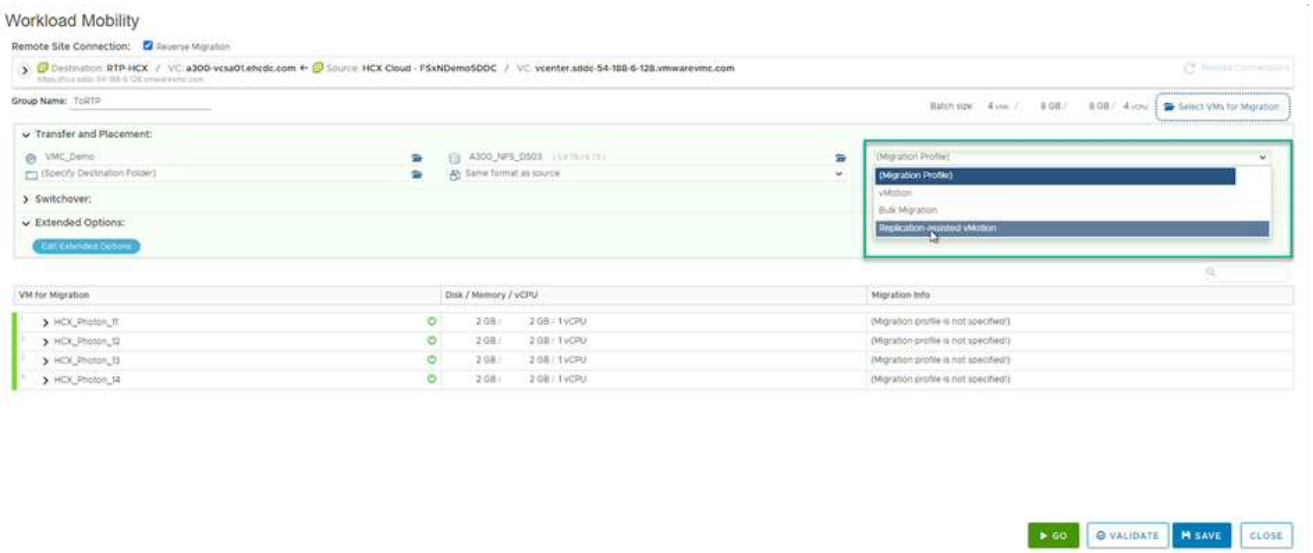
5. Vous pouvez surveiller la progression et l'achèvement du vMotion à partir du tableau de bord HCX > Migration.



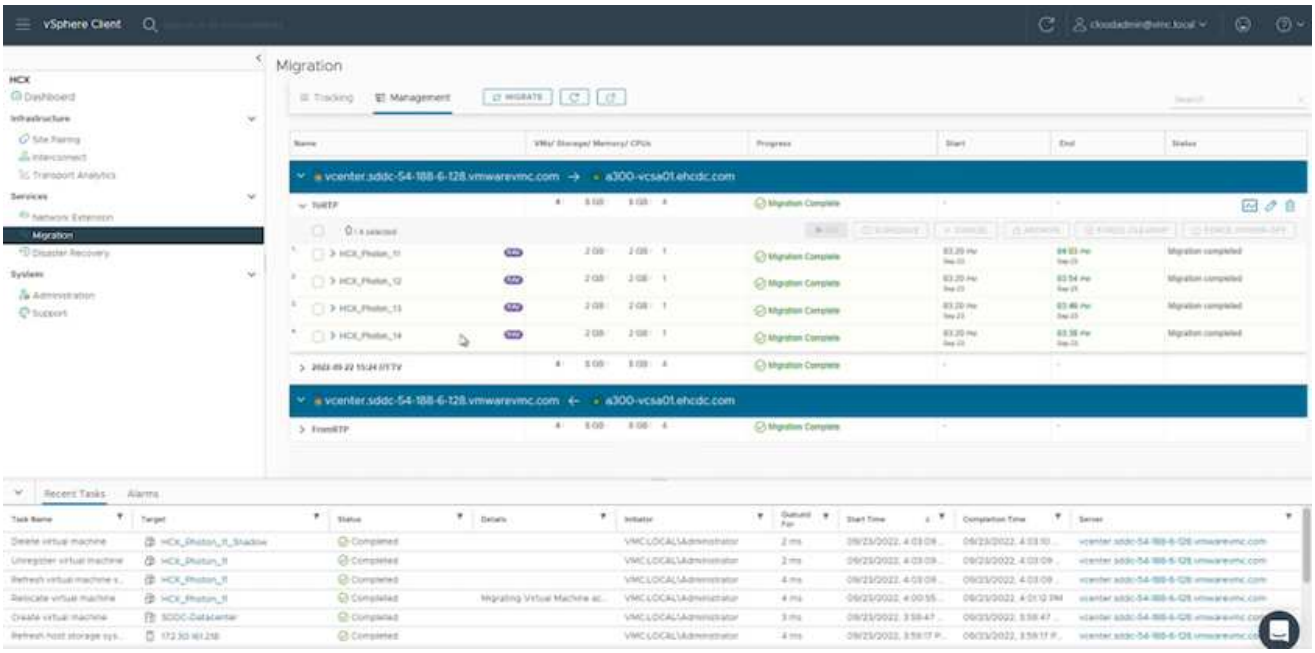
▼ **Réplication assistée par VMware vMotion**

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

La capture d'écran suivante montre le profil de migration en tant que Replication Assisted vMotion.



La durée de la réplication peut être plus longue par rapport au vMotion d'un petit nombre de machines virtuelles. Avec RAV, synchronisez uniquement les deltas et incluez le contenu de la mémoire. Voici une capture d'écran de l'état de la migration : elle montre que l'heure de début de la migration est la même et que 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 les charges de travail des locaux vers VMware Cloud sur AWS à l'aide de HCX, consultez le "Guide de l'utilisateur de VMware HCX" .

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

La banque de données VMC FSx ONTAP cible doit disposer de suffisamment d'espace pour prendre en charge la migration.

Conclusion

Que vous cibliez un cloud entièrement ou un cloud hybride et des données résidant sur n'importe quel type/fournisseur de stockage sur site, Amazon FSx ONTAP ainsi que HCX offrent d'excellentes options pour déployer et migrer les charges de travail tout en réduisant le coût total de possession en rendant les exigences de données transparentes pour la couche applicative. Quel que soit le cas d'utilisation, choisissez VMC avec la banque de données FSx ONTAP pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site et sur plusieurs clouds, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise. Il s'agit du même processus et des mêmes procédures familiers utilisés 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.

Plats à emporter

Les points clés de ce document comprennent :

- Vous pouvez désormais utiliser Amazon FSx ONTAP comme banque de données avec VMC SDDC.
- Vous pouvez facilement migrer des données depuis n'importe quel centre de données local vers VMC exécuté avec la banque de données FSx ONTAP

- Vous pouvez facilement développer et réduire la banque de données FSx ONTAP pour répondre aux exigences de capacité et de performances pendant l'activité de migration.

Où trouver des informations supplémentaires

Pour en savoir plus sur les informations décrites dans ce document, reportez-vous aux liens Web suivants :

- Documentation VMware Cloud

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

- Documentation Amazon FSx ONTAP

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

  Guide de l'utilisateur de VMware HCX

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

NetApp pour AWS / EVS

Monter FSx ONTAP comme banque de données externe pour EVS

Comment monter Amazon FSx for NetApp ONTAP en tant que banque de données externe pour Amazon Elastic VMware Service

Ce document présente les étapes détaillées pour créer un système de fichiers FSx pour ONTAP et le joindre pour l'utiliser comme banque de données Internet Small Computer System Interface (iSCSI) ou Network File System (NFS) à utiliser avec Amazon EVS.

Introduction

Les organisations disposant d'investissements VMware sur site existants et recherchant des moyens efficaces et rentables pour moderniser leurs déploiements en migrant, en explosant, en étendant ou en protégeant (sauvegarde, reprise après sinistre) des copies sur AWS ont été confrontées à plusieurs défis. Avec la sortie d'Amazon Elastic VMware Service (Amazon EVS), il existe désormais un service AWS natif qui permet d'exécuter VMware Cloud Foundation (VCF) directement dans un Amazon Virtual Private Cloud (VPC).

Amazon EVS permet d'étendre les déploiements VCF existants vers AWS, de s'intégrer à AWS pour étendre les performances pendant les pics d'utilisation et d'exécuter entièrement les charges de travail VCF sur AWS pour faciliter les modernisations, les sorties de centres de données, les consolidations et d'autres cas d'utilisation.

Bien qu'Amazon EVS offre de solides avantages, l'architecture hyperconvergée par défaut associe le calcul et le stockage, empêchant ainsi une mise à l'échelle indépendante de l'un ou de l'autre en fonction des besoins de l'entreprise. Dans le monde actuel centré sur les données, les besoins en stockage de nombreuses organisations sont supérieurs à ceux en matière de calcul. Cependant, avec l'architecture hyperconvergée de VMware, les ressources de stockage sont couplées aux ressources de calcul. Cela signifie que la mise à l'échelle du stockage ne peut être effectuée qu'en ajoutant des hôtes de calcul qui ne seront jamais utilisés. C'est une situation qui peut augmenter considérablement les coûts, en particulier dans les charges de travail nécessitant beaucoup de stockage.

Pour résoudre ce problème, AWS et NetApp proposent Amazon FSx for NetApp ONTAP (FSx pour ONTAP)

comme service de stockage externe pour Amazon EVS. FSx for ONTAP est un service de stockage natif AWS qui offre les fonctionnalités de hautes performances, de résilience des données et de rentabilité du logiciel NetApp ONTAP . En utilisant FSx pour ONTAP comme stockage externe, les utilisateurs d'Amazon EVS peuvent faire évoluer les ressources de calcul et de stockage de manière indépendante, permettant ainsi un coût total de possession (TCO) optimal.

Aperçu

Ce document présente les étapes détaillées pour créer un système de fichiers FSx pour ONTAP et le joindre pour l'utiliser comme banque de données Internet Small Computer System Interface (iSCSI) ou Network File System (NFS) à utiliser avec Amazon EVS.

Objectif de ce guide

Ce guide fournit des instructions sur la configuration d'une banque de données FSx pour ONTAP pour Amazon EVS, ainsi que les meilleures pratiques, les exigences de prise en charge, les considérations de dimensionnement et d'autres informations pour vous aider à planifier, concevoir et mettre en œuvre l'intégration.

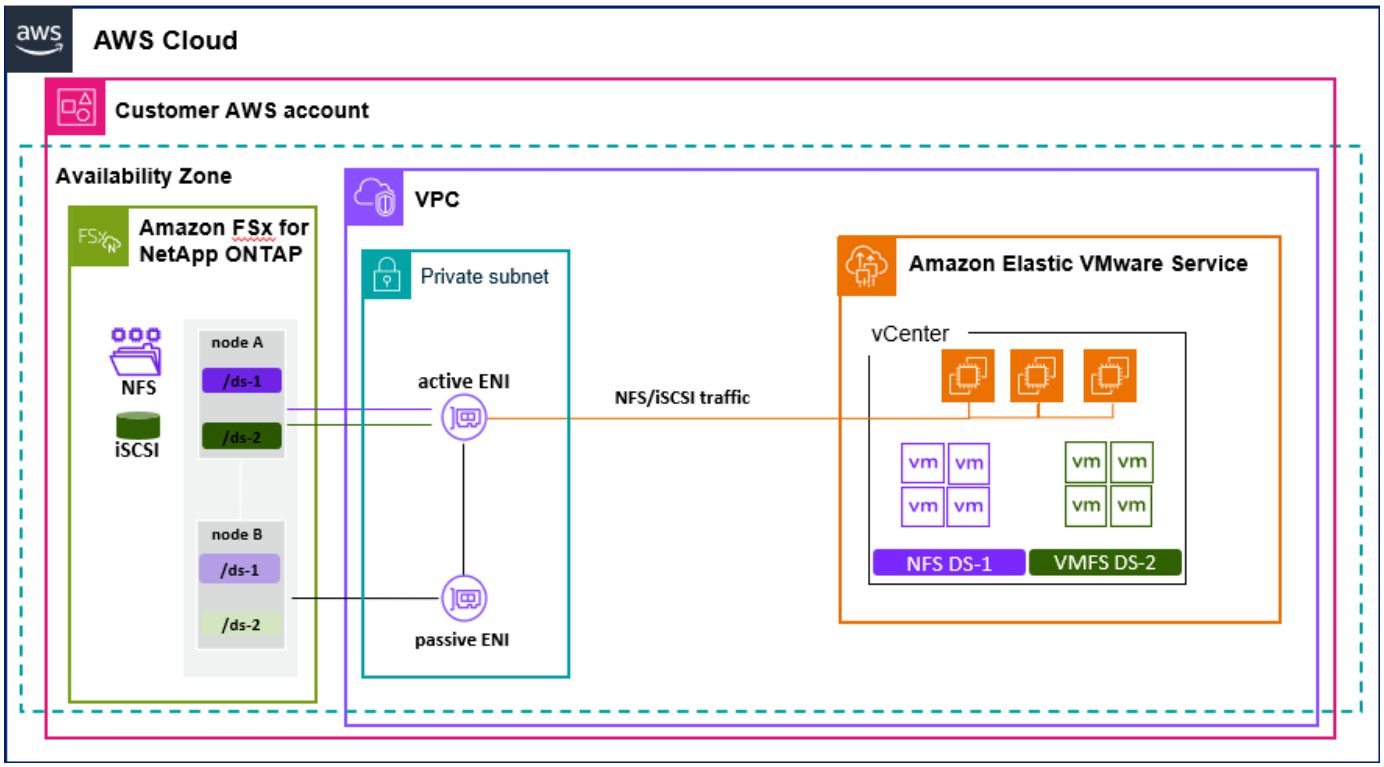
Public

Ce didacticiel est destiné aux architectes et administrateurs Cloud familiarisés avec VMware vSphere, Amazon EVS, la console AWS et FSx pour ONTAP.

Architecture de haut niveau

Dans cette section, nous donnerons un aperçu de l'architecture de la solution permettant d'utiliser FSx pour ONTAP comme banque de données pour Amazon EVS.

Ci-dessous, vous pouvez voir une vue d'ensemble de l'architecture du magasin de données FSx for ONTAP avec un environnement Amazon EVS au sein d'un AWS VPC.



Procédure de déploiement pour l'utilisation de FSx pour ONTAP comme banque de données NFS

Cette section présente les étapes à suivre pour déployer FSx pour ONTAP en tant que banque de données NFS. Les étapes de déploiement d'une banque de données iSCSI sont détaillées dans la section suivante.

Étapes de déploiement de haut niveau

Le déploiement du système de fichiers FSx for ONTAP pour l'utiliser comme banque de données NFS pour Amazon EVS et l'établissement de la connectivité entre les deux services comprendront les étapes suivantes :

- Configuration d'un système de fichiers FSx pour ONTAP dans le même VPC où se trouve l'environnement Amazon EVS VCF.
- Validation des groupes de sécurité et de la table de routage.
- Attachement d'un volume de stockage FSx pour ONTAP à utiliser comme banque de données NFS pour Amazon EVS.

Prérequis

Les conditions préalables suivantes doivent être réunies avant de commencer le processus de configuration d'un FSx pour ONTAP en tant que banque de données NFS pour Amazon EVS :

- Un environnement de virtualisation Amazon EVS. Pour plus d'informations sur la façon de procéder, consultez la documentation sur"Guide de démarrage avec Amazon EVS" .
- Créez une zone de disponibilité unique (AZ) FSx pour ONTAP avec une capacité de stockage SSD appropriée, des IOPS provisionnés et un débit.
- Pour des performances optimales, placez le système de fichiers FSx for ONTAP dans le même VPC que l'instance Amazon EVS. Notez que le peering VPC est également pris en charge dans le cas où FSx pour ONTAP est déployé dans un autre VPC.
- En fonction des exigences de performances, sélectionnez les IOPS et le débit appropriés nécessaires pour un système de fichiers Single-AZ FSx pour ONTAP . Voir"détails des spécifications de performances pour FSx pour ONTAP" pour comprendre le débit et les IOPS fournis par chaque option disponible.



Pour ce guide, nous déploierons le système de fichiers FSx pour ONTAP dans le même sous-réseau que le sous-réseau d'accès au service.

Une fois l'environnement de virtualisation Amazon EVS déployé dans le VPC, vous pouvez procéder à la configuration du système de fichiers Single-AZ FSx pour ONTAP qui sera utilisé comme banque de données NFS.



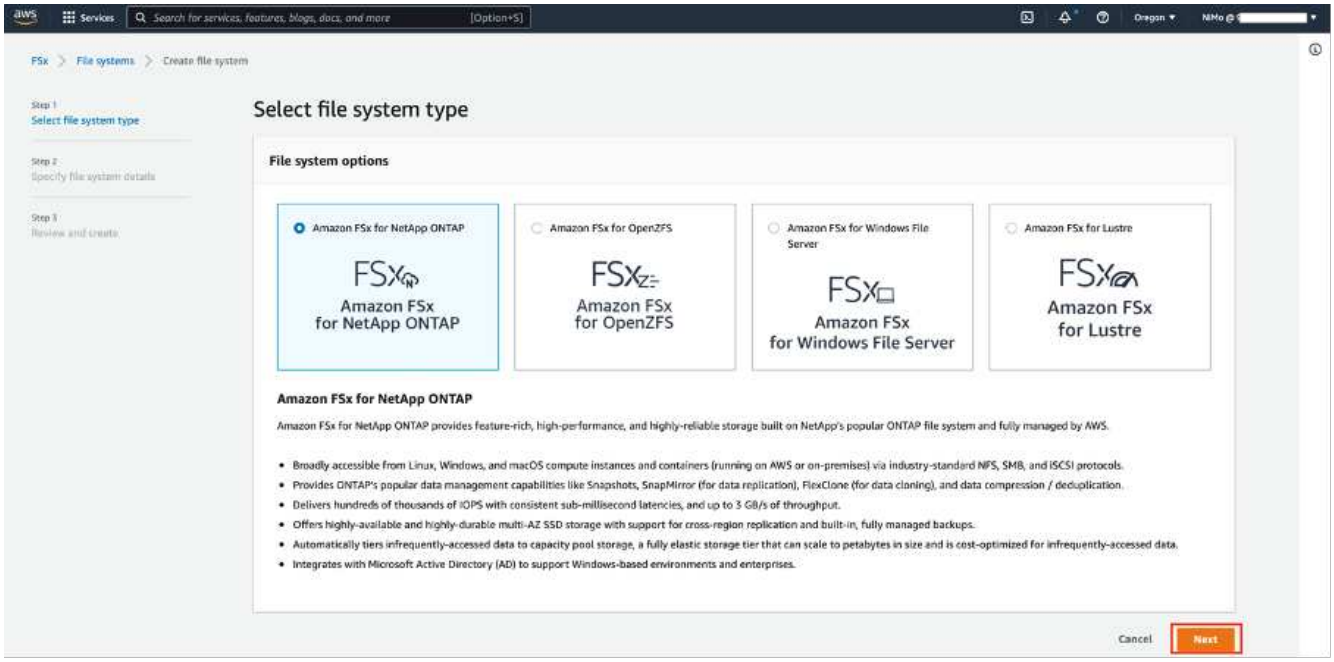
Votre système de fichiers FSx for ONTAP doit être déployé dans la même zone de disponibilité que le SDDC Amazon EVS.

Créer un système de fichiers FSx pour ONTAP

Les étapes suivantes vous montreront comment provisionner et monter un système de fichiers FSx pour ONTAP :

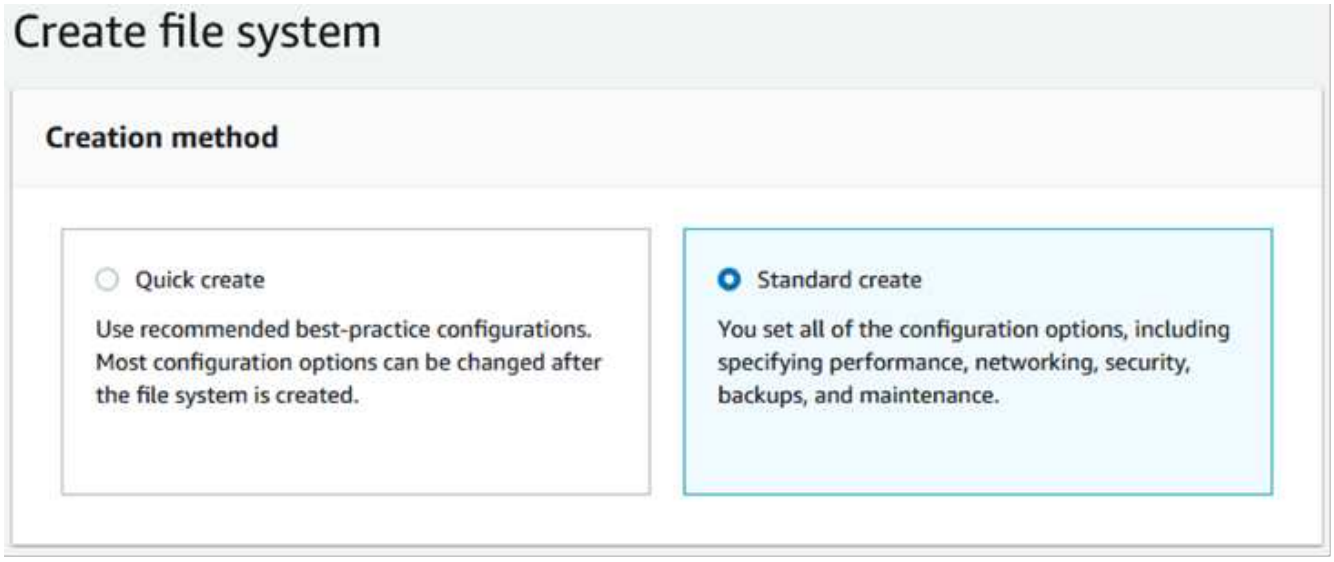
1. Accédez à la console Amazon FSx à l'adresse `https://console.aws.amazon.com/fsx/` en utilisant votre navigateur Internet et connectez-vous avec vos identifiants.

2. Dans la console, sélectionnez Créer un système de fichiers. Cela lancera l'assistant de configuration pour créer un système de fichiers FSx pour ONTAP .
3. Tout d'abord, sélectionnez le type de système de fichiers. Parmi les options de système de fichiers disponibles, sélectionnez «Amazon FSx for NetApp ONTAP» et continuez en cliquant sur le bouton « Suivant ».

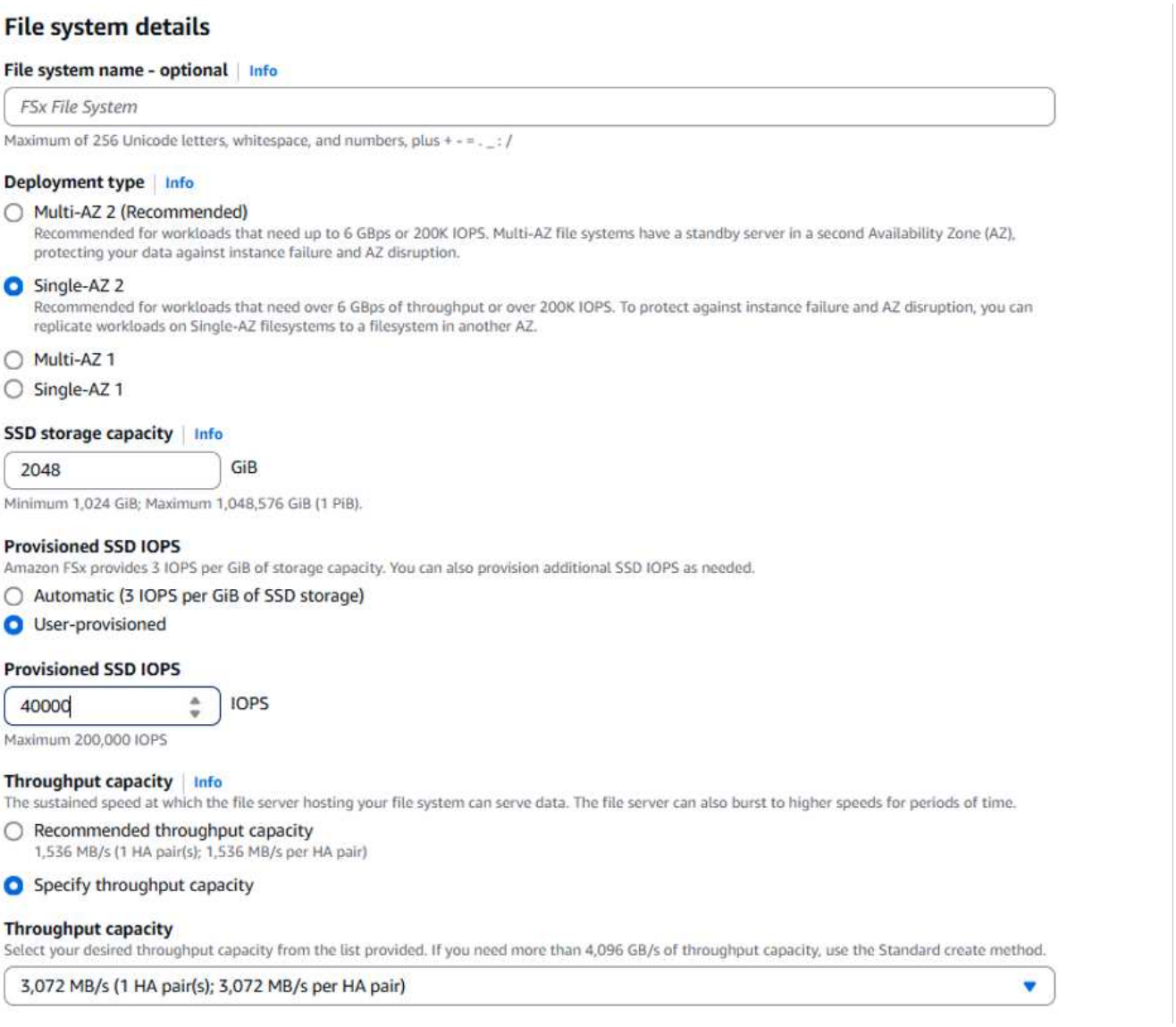


4. Vous aurez le choix entre les options de création rapide et de création standard. La création rapide propose des configurations prédéfinies et la création standard vous permet de définir vos propres configurations.

   Sélectionnez l'option « Création standard ».

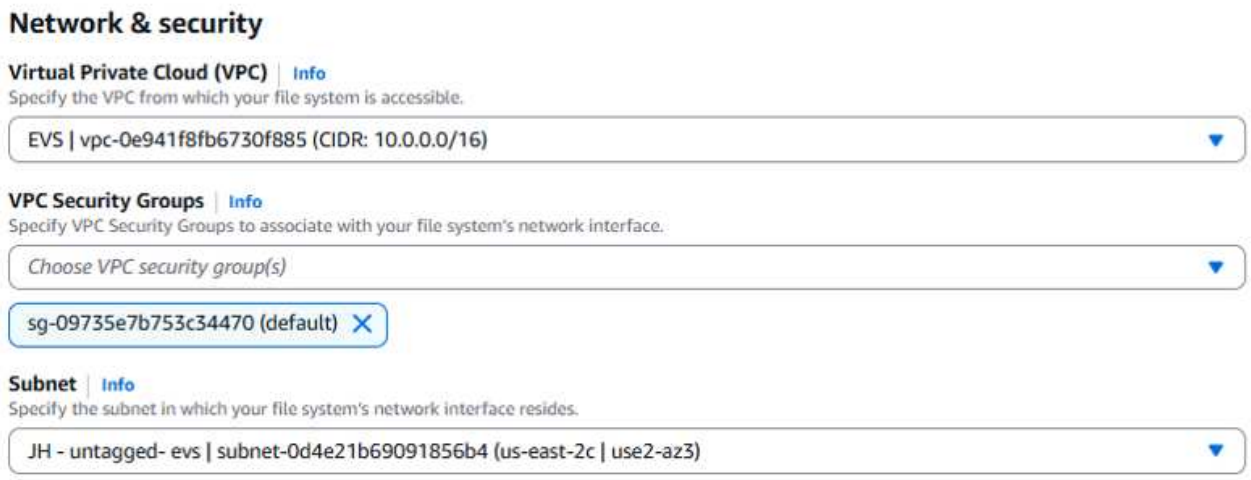


   Vous serez maintenant dans l'assistant de configuration de création de système de fichiers standard. Dans la page des détails du système de fichiers, choisissez et saisissez les mêmes informations que celles indiquées dans l'image ci-dessous :



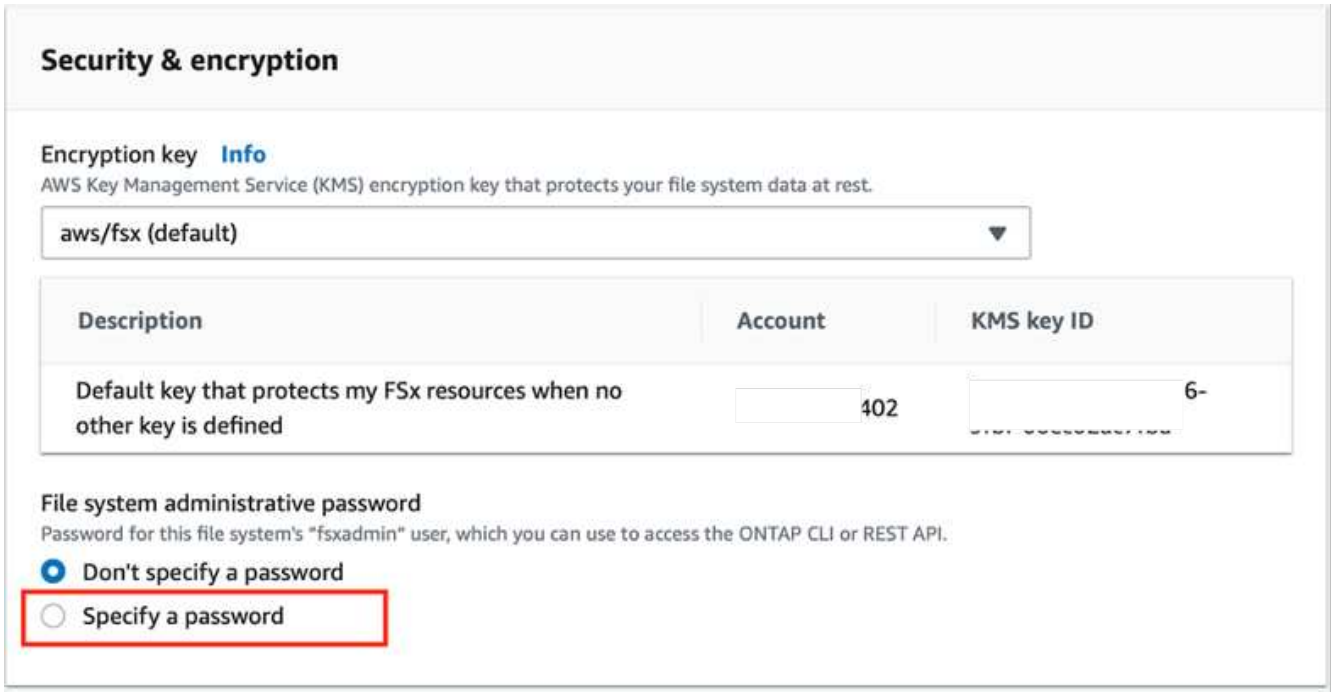
5. Faites défiler vers le bas jusqu'à ce que vous trouviez une section intitulée « Réseau et sécurité ». Dans cette section, vous définirez les détails du sous-réseau et du VPC. Pour les besoins de ce guide, nous avons sélectionné « EVS-VPC » dans le menu déroulant et sélectionné le sous-réseau d'accès au service (VLAN non balisé) comme sous-réseau pour l'environnement virtuel EVS.

> Le sous-réseau peut être n'importe quel sous-réseau privé non balisé dans le VPC. Il peut également se trouver dans un autre VPC/sous-réseau connecté via VPC Peering, à condition qu'un routage approprié ait été configuré.

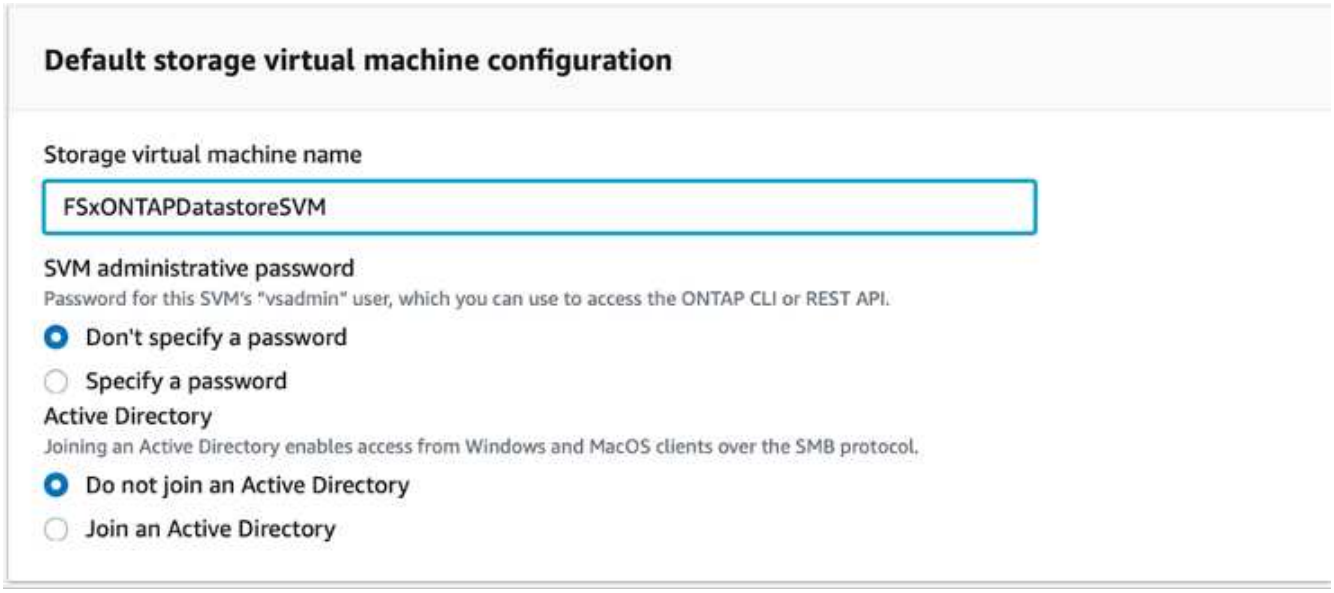


6. En faisant défiler vers le bas, vous trouverez la section « Sécurité et cryptage ». Ici, sélectionnez la clé de cryptage dans le menu déroulant. Ces clés sont fournies par AWS Key Management Service (AWS KMS) et protégeront les données au repos dans votre système de fichiers FSx for ONTAP .

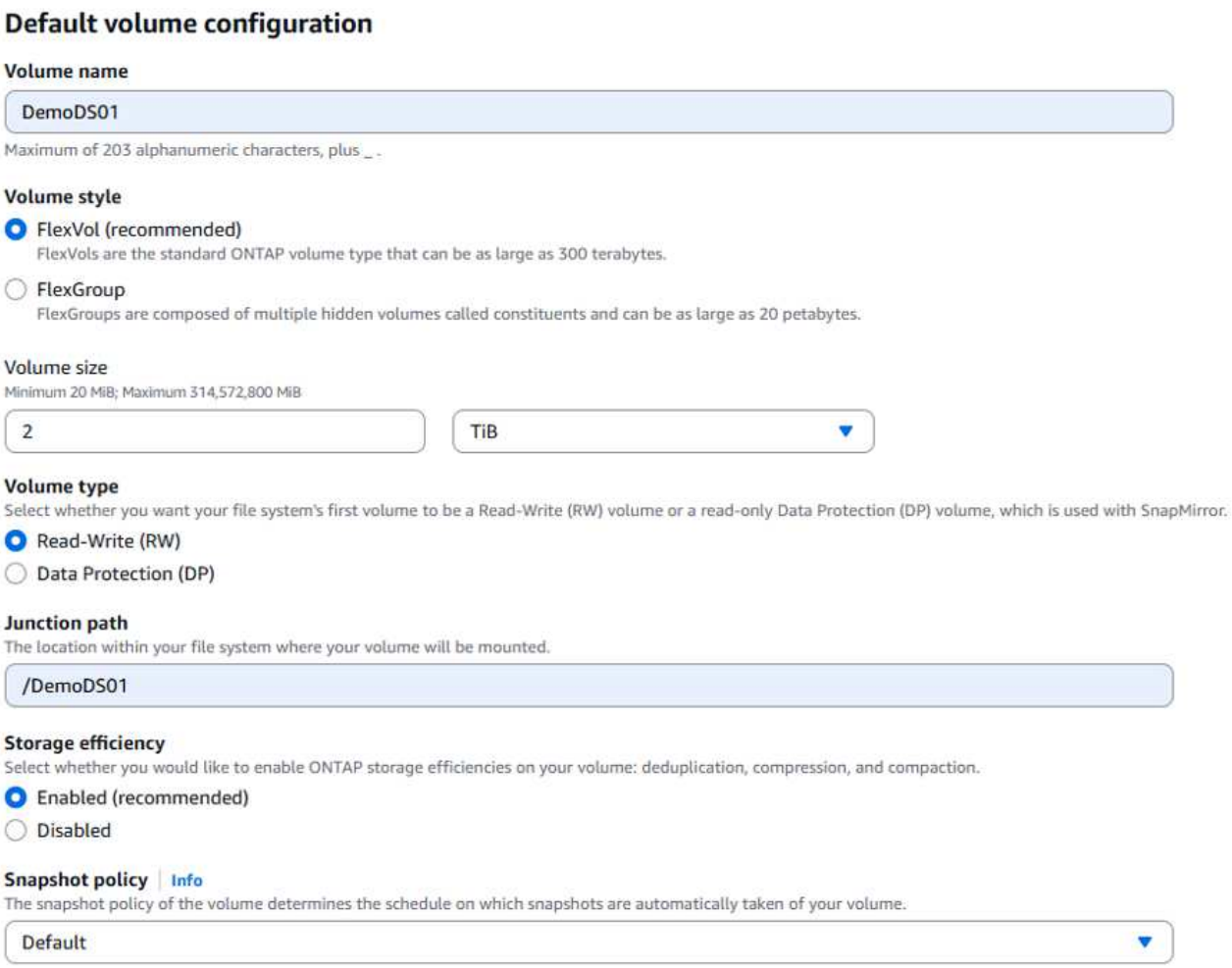
   Ensuite, dans le paramètre « Mot de passe d'administration du système de fichiers », spécifiez un mot de passe unique pour l'utilisateur fsxadmin qui administrera le système de fichiers.



7. Ensuite, vous ferez défiler la page jusqu'à une section intitulée « Configuration par défaut de la machine virtuelle de stockage ». Ici, vous devrez fournir un nom pour la machine virtuelle de stockage (SVM).

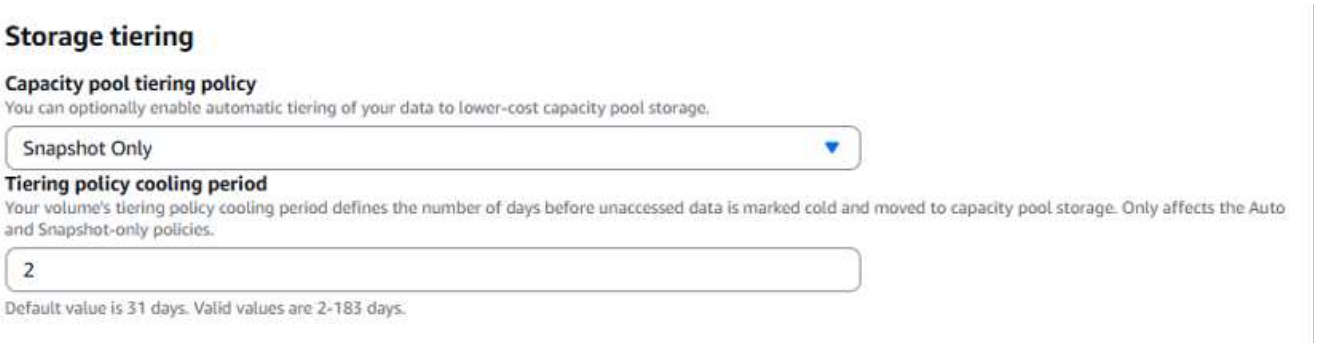


8. Ensuite, faites défiler jusqu'à la section intitulée « Configuration du volume par défaut ». Ici, vous fournirez un nom pour le volume et définirez la taille du volume. Le protocole de volume doit être NFS v3 (activé par défaut). Cliquez sur l'option pour activer les fonctionnalités d'efficacité du stockage (compression, déduplication et compactage) afin de réduire votre utilisation globale du stockage et vos coûts.



9. Pour l'option de hiérarchisation du stockage, sélectionnez « Instantané uniquement » dans le menu

déroulant et définissez une période de refroidissement de la politique de hiérarchisation. La valeur par défaut est de 31 jours, mais pour cet exemple, nous définissons une période de refroidissement de deux jours.

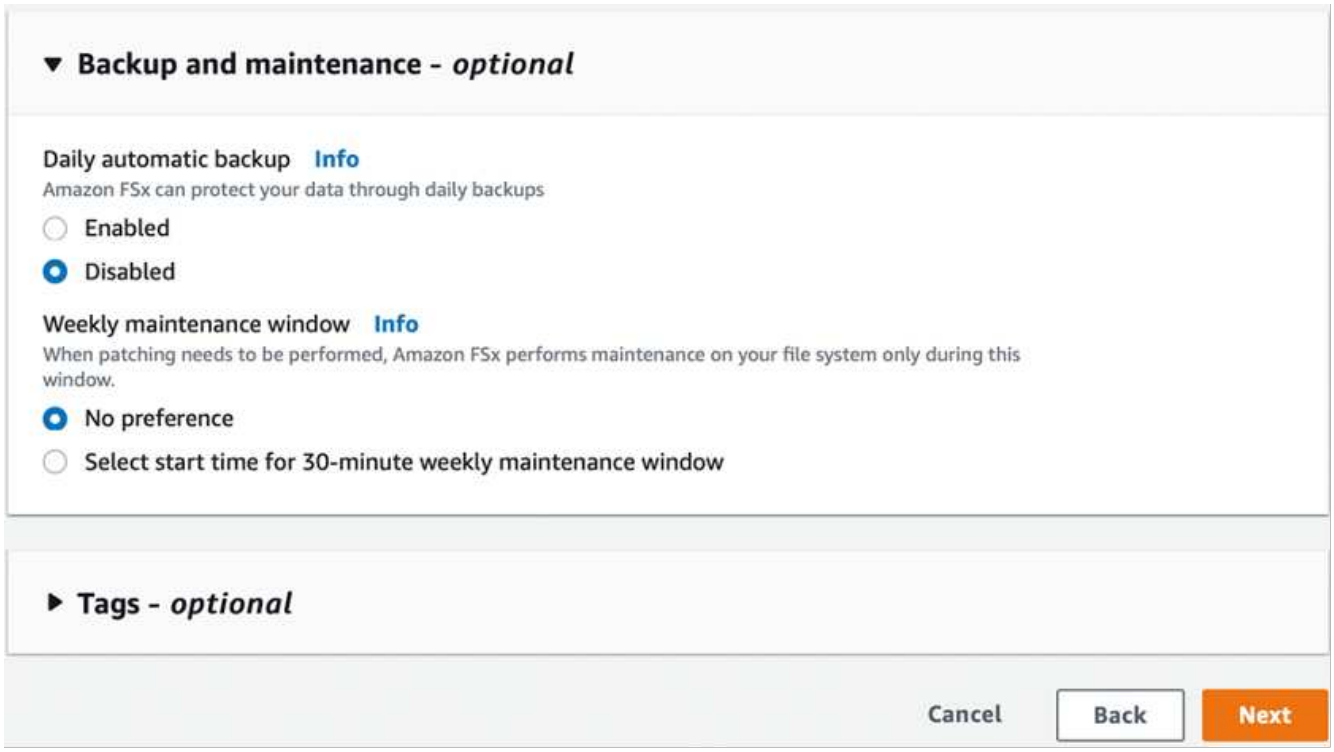


10. Une fois le volume créé, modifiez les paramètres suivants à l'aide de l'interface de ligne de commande ONTAP (ONTAP CLI) :

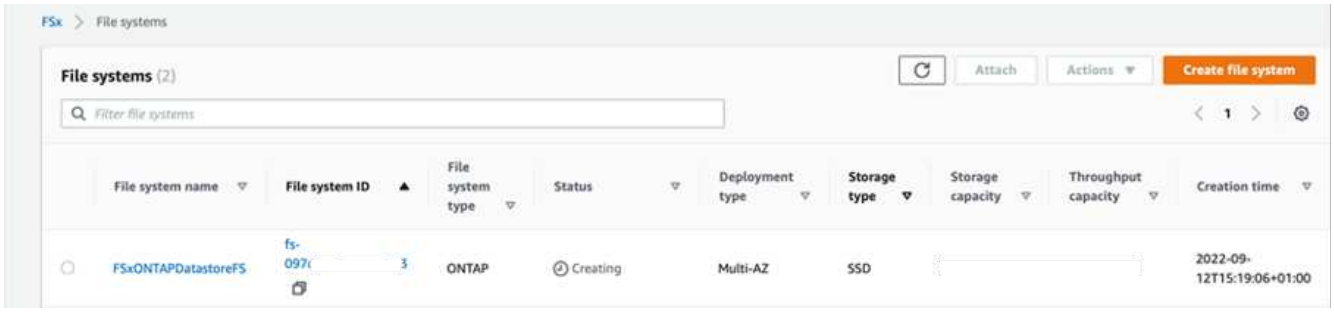
Paramètre	Configuration
Garantie de volume	Aucun (provisionnement léger)
réserve fractionnaire	0%
snap_reserve	0%
Dimensionnement automatique	grandir_rétrécir
Efficacité du stockage	Activé
Politique de hiérarchisation des volumes	Instantané uniquement
Mise à jour de l'heure d'accès (-atime-update)	FAUX
Lecture anticipée minimale (-min-readahead)	FAUX
Politique d'instantané	Aucune

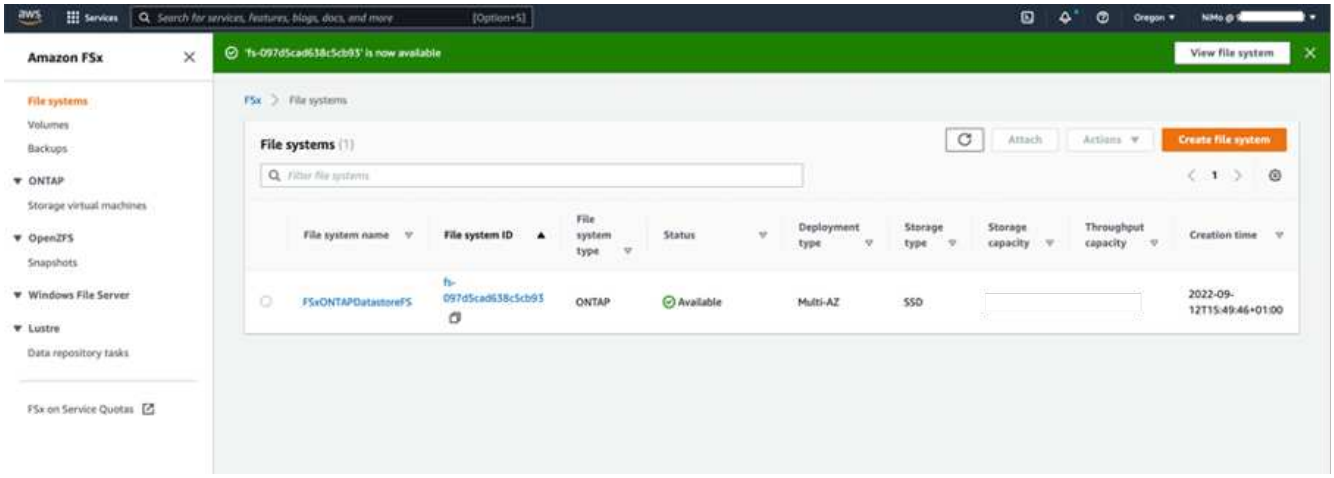
11. Dans l'étape facultative « Sauvegarde et maintenance », désactivez les sauvegardes automatiques quotidiennes et sélectionnez « Aucune préférence » pour la fenêtre de maintenance hebdomadaire.

    Cliquez sur « Suivant » lorsque vous avez terminé.



12. Vous allez maintenant avoir accès à un aperçu de l'ensemble de la configuration du système de fichiers que vous avez configurée en suivant les étapes précédentes. Vérifiez que tous les paramètres sont corrects, puis cliquez sur le bouton « Créer un système de fichiers » pour terminer la configuration.





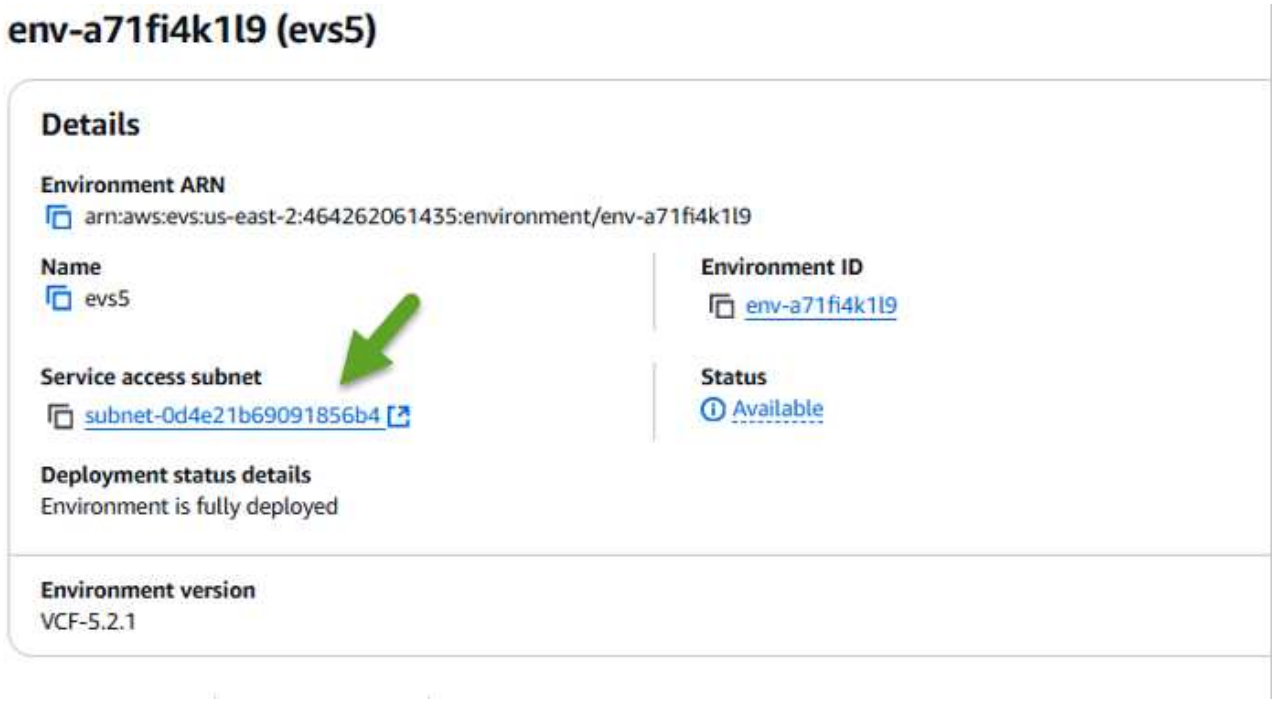
Pour créer des systèmes de fichiers FSx supplémentaires pour ONTAP , vous pouvez suivre les étapes détaillées ci-dessus, en ajustant les valeurs qui affectent les performances et la capacité du disque selon vos besoins. Pour en savoir plus sur les options de performances

de FSx for ONTAP, consultez"cette page de documentation" .

Validation du routage et des groupes de sécurité de l'environnement VPC et de virtualisation

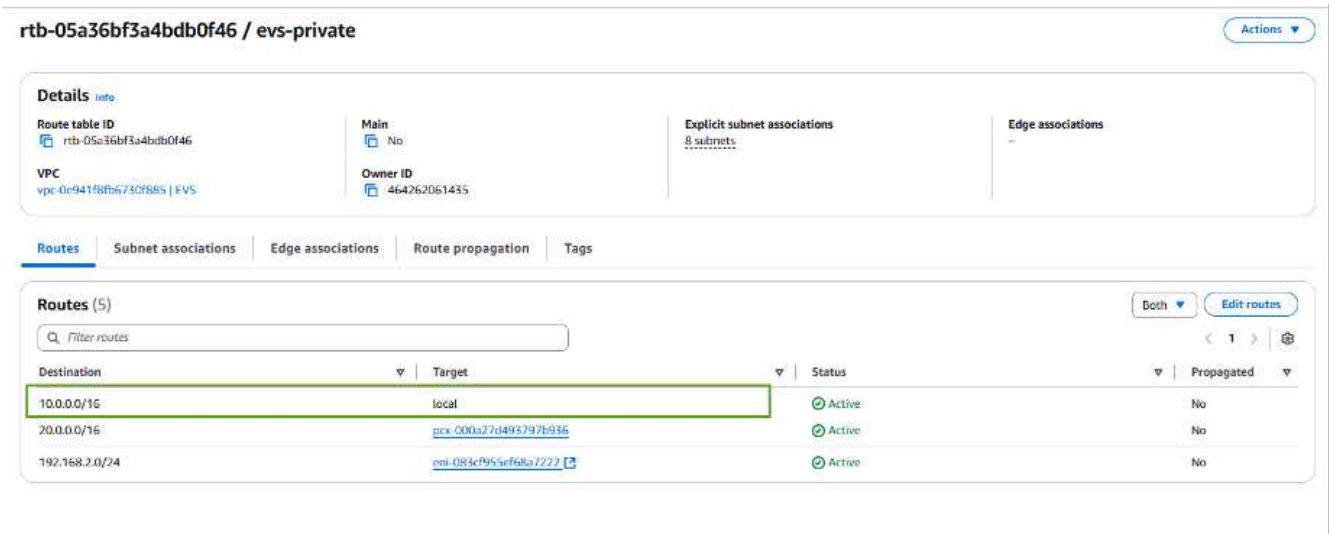
La validation des groupes de routage et de sécurité VPC et SDDC est importante pour garantir que l'environnement de virtualisation Amazon EVS et les composants du système de fichiers FSx for ONTAP peuvent fonctionner correctement ensemble.

1. Accédez à Elastic VMware Service > Environnements de virtualisation > [votre environnement Amazon EVS] et sélectionnez le sous-réseau d'accès au service, comme indiqué par la flèche verte ci-dessous :



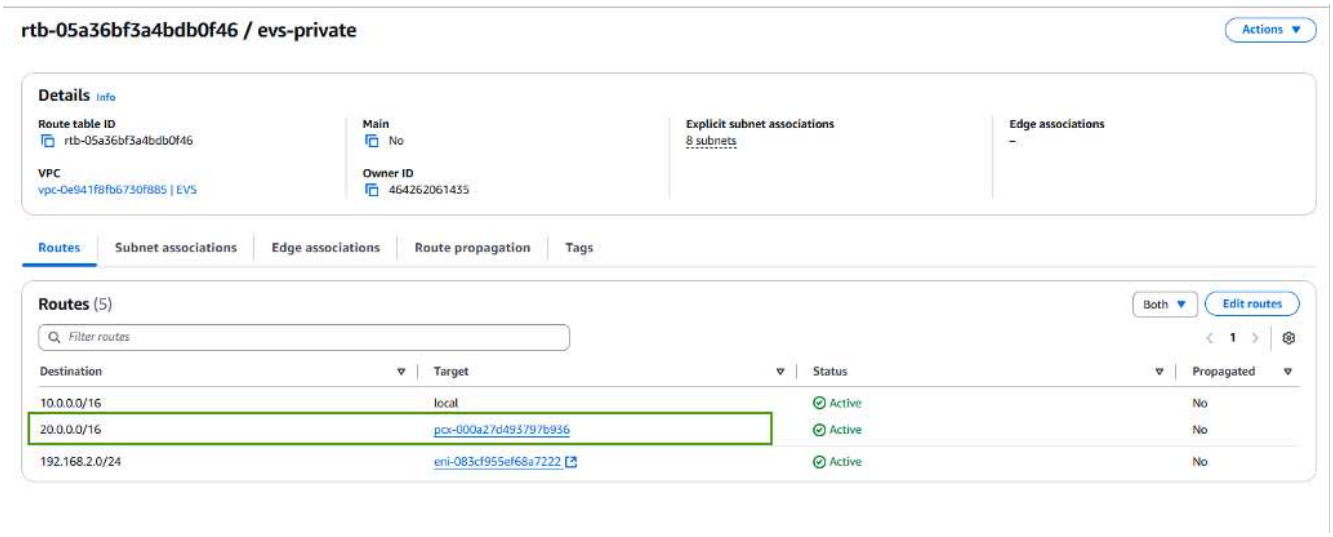
2. Cela ouvrira le panneau de sous-réseau. Recherchez le tableau Routes sur ce panneau et cliquez dessus.

   Dans cet exemple, le système de fichiers FSxN ONTAP se trouve dans le même VPC que l'environnement Amazon EVS VCF, les routes par défaut sont donc suffisantes.



   Si le système de fichiers FSx pour ONTAP se trouve dans un VPC différent, vérifiez que les routes vers ce

VPC ont été ajoutées. Dans cet exemple, des itinéraires pour le peering VPC vers le VPC où réside le système FSx pour ONTAP ont été ajoutés.

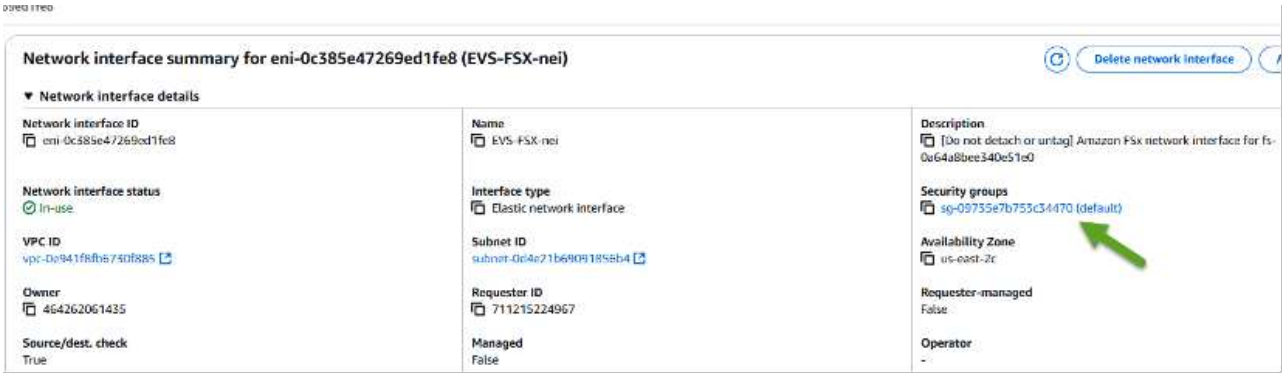


3. Ensuite, vous devrez vérifier que le groupe de sécurité connecté au système de fichiers FSx pour ONTAP (c'est-à-dire celui connecté à l'interface réseau élastique (ENI)) autorise l'accès aux ports NFS.

   Pour une liste complète des ports de protocole NFS et iSCSI, reportez-vous au lien : https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]Documentation sur le contrôle d'accès au système de fichiers avec Amazon VPC].

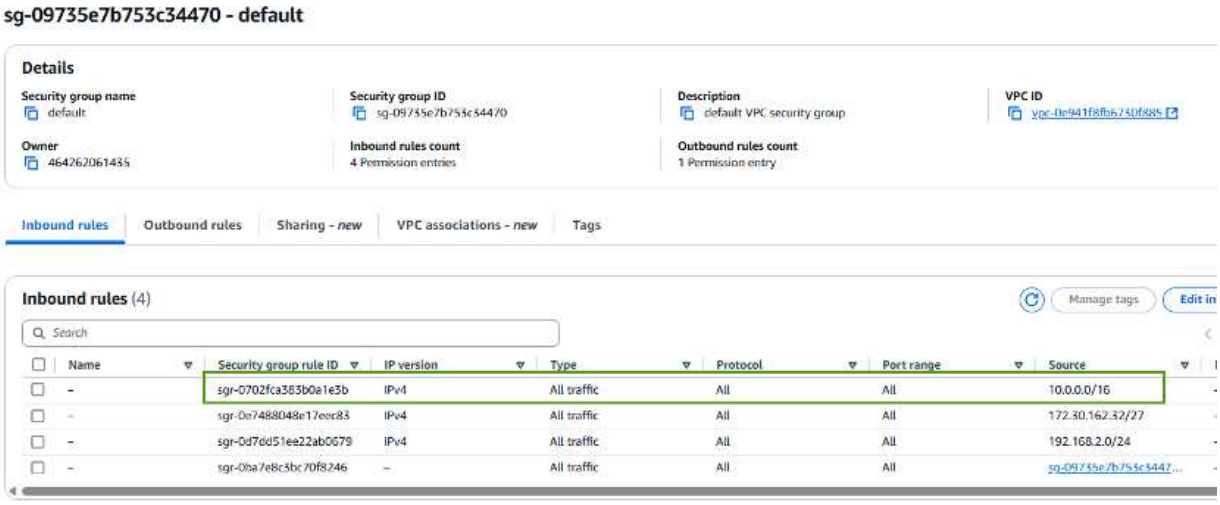
   Pour vérifier que votre système de fichiers FSx for ONTAP est associé au groupe de sécurité :

   a. Dans la console AWS, accédez à FSx > Systèmes de fichiers > [votre système de fichiers FSx pour ONTAP].
   b. Dans l'onglet Réseau et sécurité, cliquez sur ENI.
   c. Recherchez le groupe de sécurité répertorié sous les détails de l'interface réseau. associé à l'ENI (indiqué par la flèche verte dans l'image ci-dessous).



   d. Valider les ports. Dans cet exemple présenté dans l'écran suivant, tout le trafic est autorisé. Cependant, vous pouvez les limiter aux ports NFS uniquement. Voici la liste des ports :
      - Port 111 TCP : Portmapper, utilisé pour négocier les ports utilisés dans les requêtes NFS.
      - Port 635 TCP : Mountd, qui sert à recevoir les demandes de montage entrantes.
      - Port 2049 TCP : NFS, qui gère le trafic NFS.

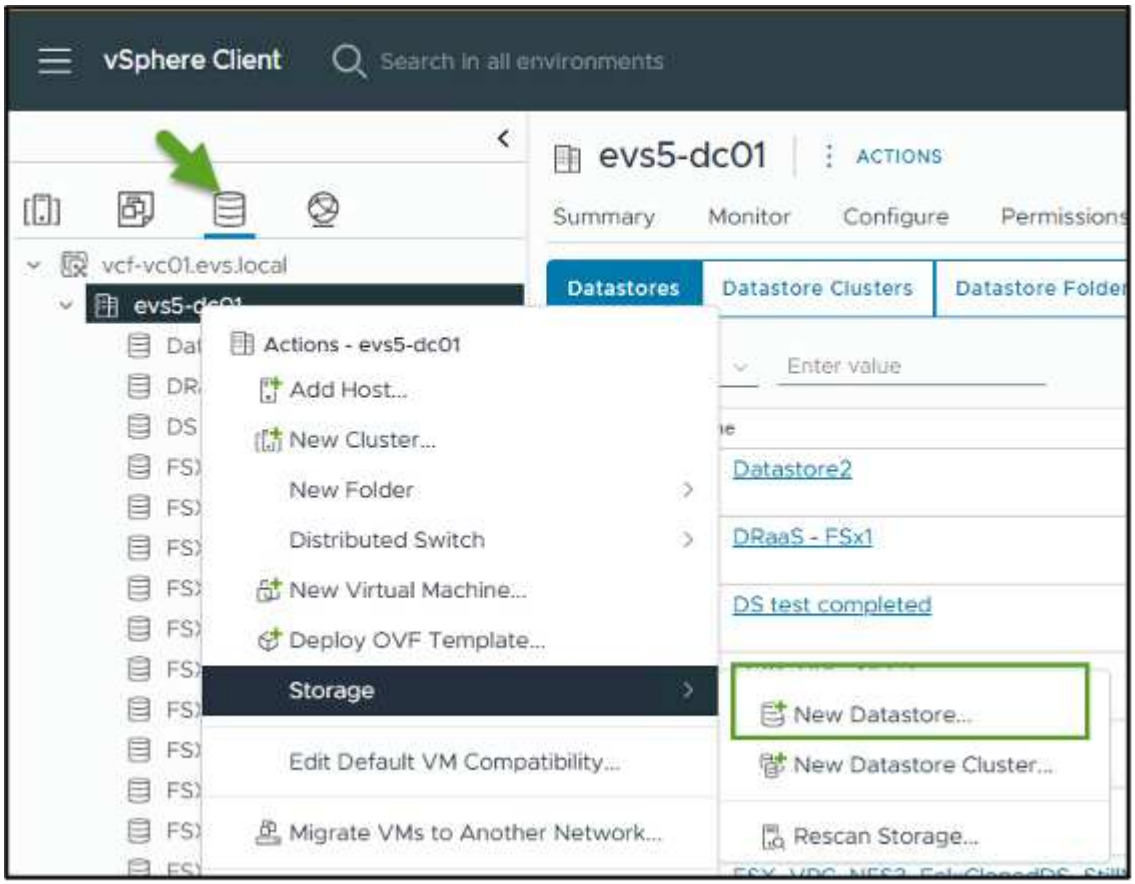
- Port 4045 TCP : Network Lock Manager (NLM), qui gère les demandes de verrouillage.
- Port 4046 TCP : Network Status Monitor (NSM), qui envoie des notifications aux clients NFS lorsque le serveur redémarre pour la gestion du verrouillage.



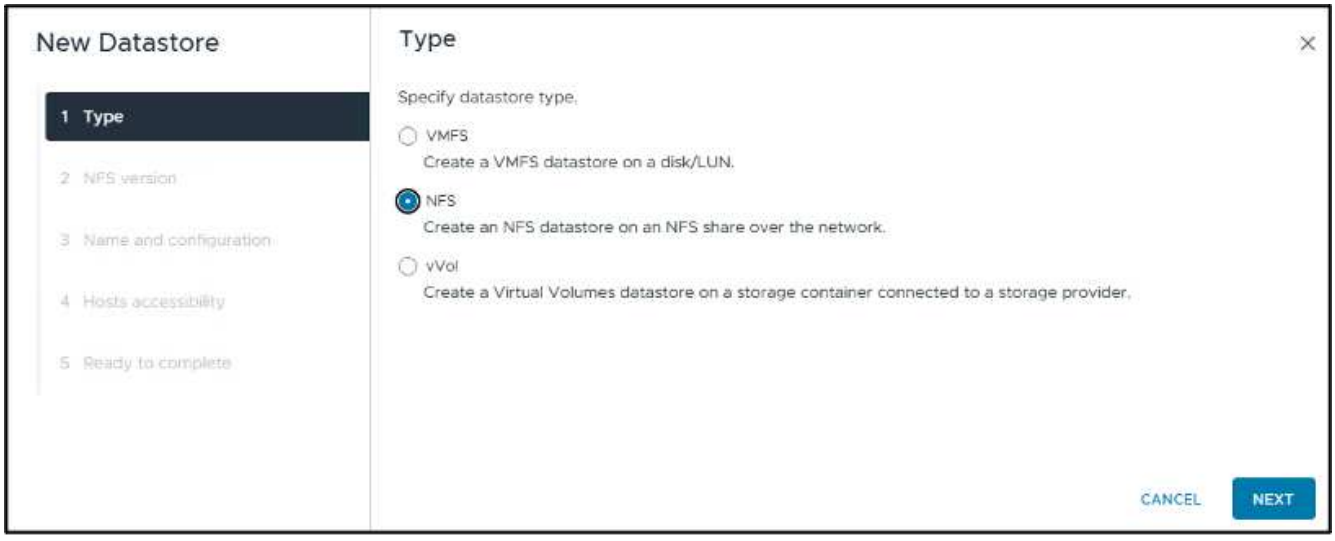
Attacher un volume NFS FSx pour ONTAP à Amazon EVS pour l'utiliser comme banque de données

Maintenant que votre système de fichiers FSx for ONTAP a été provisionné et que tous les paramètres de connectivité appropriés ont été validés, il est temps de connecter un volume de stockage FSx for ONTAP à Amazon EVS. Les étapes suivantes montrent comment accéder à vCenter et monter le volume FSx for ONTAP en tant que banque de données NFS :

1. Dans le client vSphere, accédez à l'onglet « Datastore ». Recherchez le centre de données et accédez à Stockage > Nouveau magasin de données, comme indiqué ci-dessous :

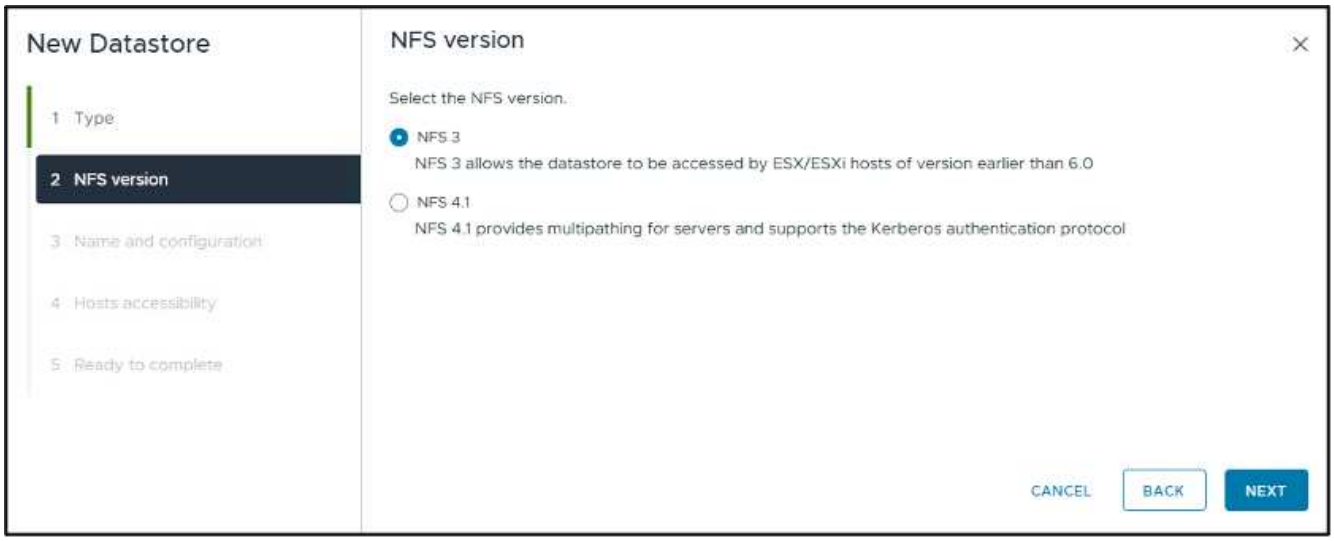


2. Vous serez maintenant dans l'assistant Nouveau magasin de données. À l'étape « Type », vous choisirez un type de banque de données. Sélectionnez « NFS » et cliquez sur « SUIVANT » pour continuer.



3. À l'étape « Version NFS », vous sélectionnerez une version NFS.

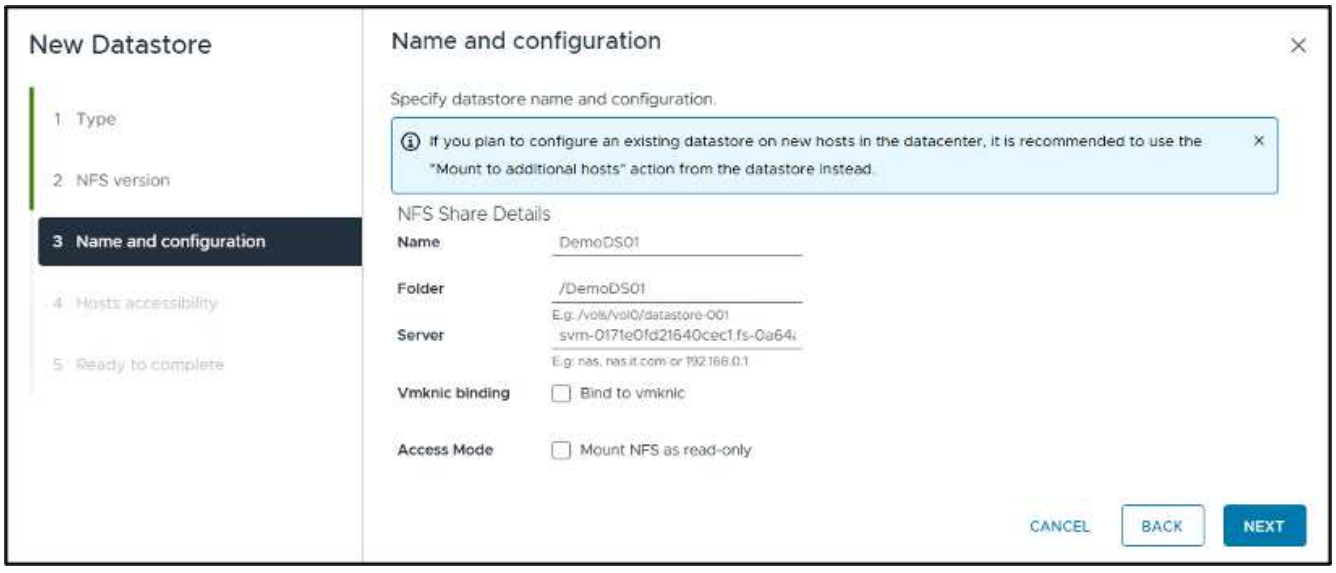
   Pour les besoins de cet exemple, nous choisirons « NFS 3 » mais notez que NFS v4.1 peut également être utilisé.



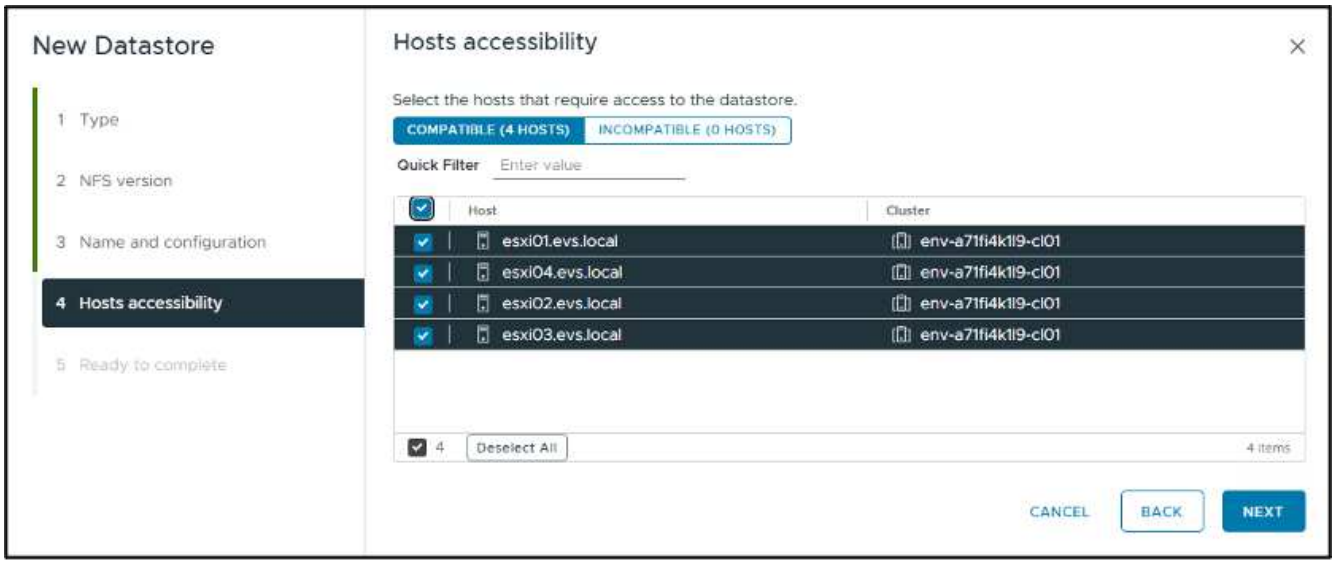
4. Dans l'étape « Nom et configuration », vous :

   a. Nommez le magasin de données.
   b. Nommez le dossier. Utilisez le chemin de jonction vers votre volume NFS.
   c. Nommez le serveur. Utilisez soit le nom DNS NFS de votre SVM, soit l'adresse IP du NFS.

   Cliquez sur « SUIVANT » pour continuer.



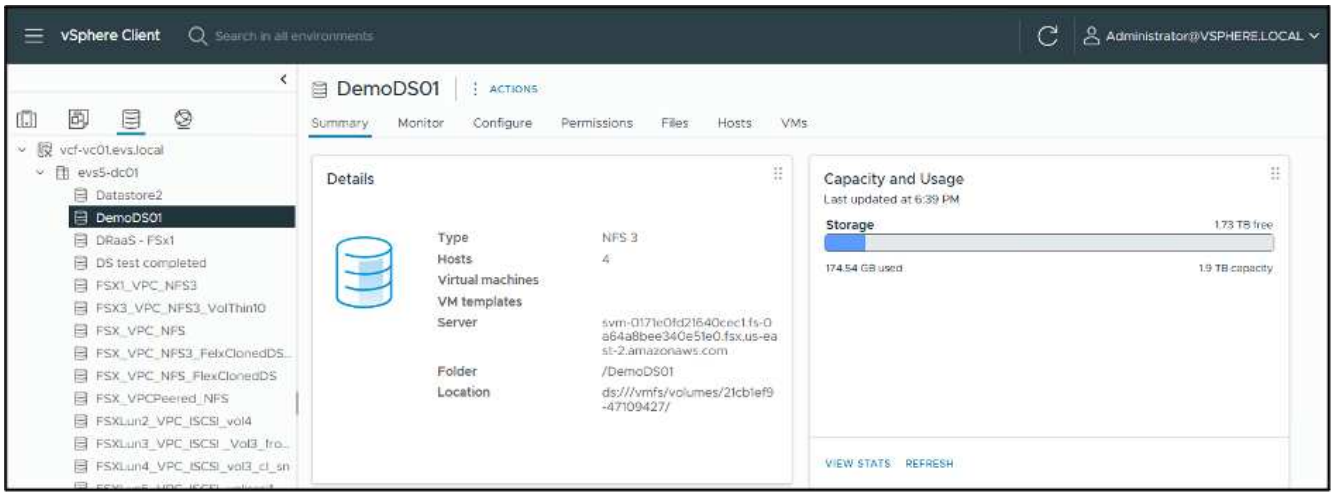
5. À l'étape « Accessibilité de l'hôte », sélectionnez tous les hôtes qui nécessitent un accès au magasin de données, puis cliquez sur « SUIVANT » pour continuer.



6. À l'étape « Prêt à terminer », vérifiez les données et cliquez sur « TERMINER » pour terminer la configuration.



7. Validez que la banque de données NFS a été connectée en accédant à vCenter, comme indiqué ci-dessous :



Procédure de déploiement pour l'utilisation de FSx pour ONTAP comme banque de données iSCSI

Cette section couvre les étapes de configuration d'une banque de données iSCSI à l'aide de FSx pour ONTAP.

Prérequis

Avant de provisionner et d'attacher FSx pour ONTAP en tant que banque de données iSCSI, vous devez d'abord déployer un environnement de virtualisation Amazon EVS. Pour plus d'informations, consultez la documentation sur le guide de démarrage rapide avec Amazon EVS. Cette section suppose également que vous avez déployé un système de fichiers FSx pour ONTAP . Veuillez consulter la section Approche détaillée ci-dessus pour connaître les étapes appropriées.

Étapes de déploiement de haut niveau

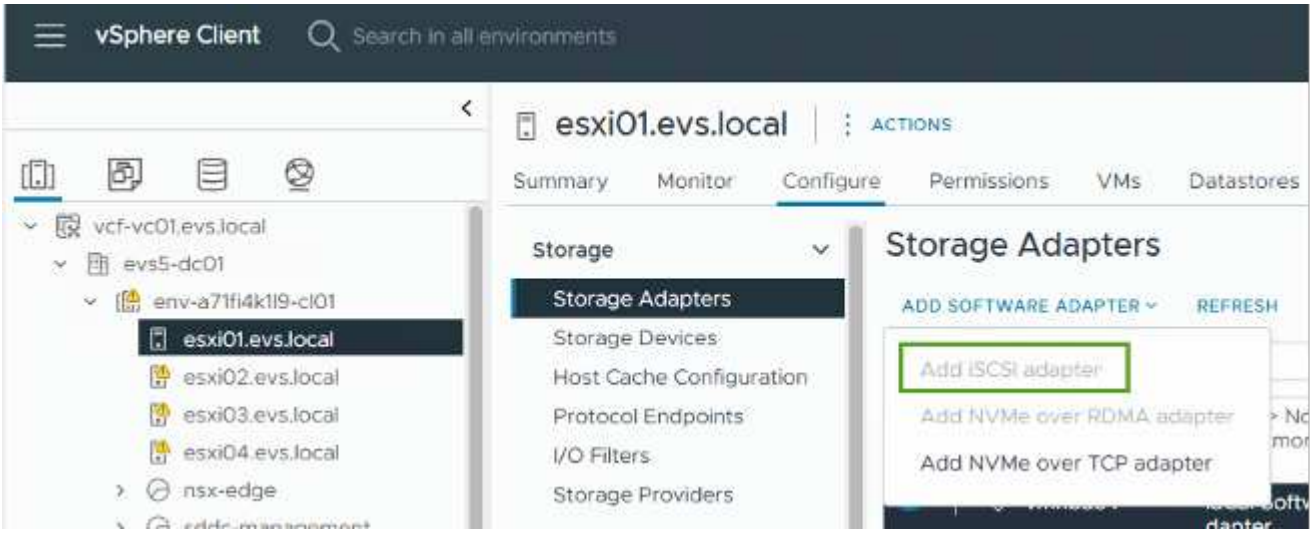
Le déploiement du système de fichiers FSx for ONTAP pour l'utiliser comme banque de données iSCSI pour Amazon EVS et l'établissement de la connectivité entre les deux services comprendront les étapes suivantes :

- Configuration d'un adaptateur réseau iSCSI pour chaque hôte ESXi.
- Création et configuration du système de fichiers FSx pour ONTAP , volume, LUN, etc.
- Connexion des hôtes ESXi au serveur de système de fichiers FSx for ONTAP .
- Création d'un système de fichiers de machine virtuelle de banque de données iSCSI (VMFS).

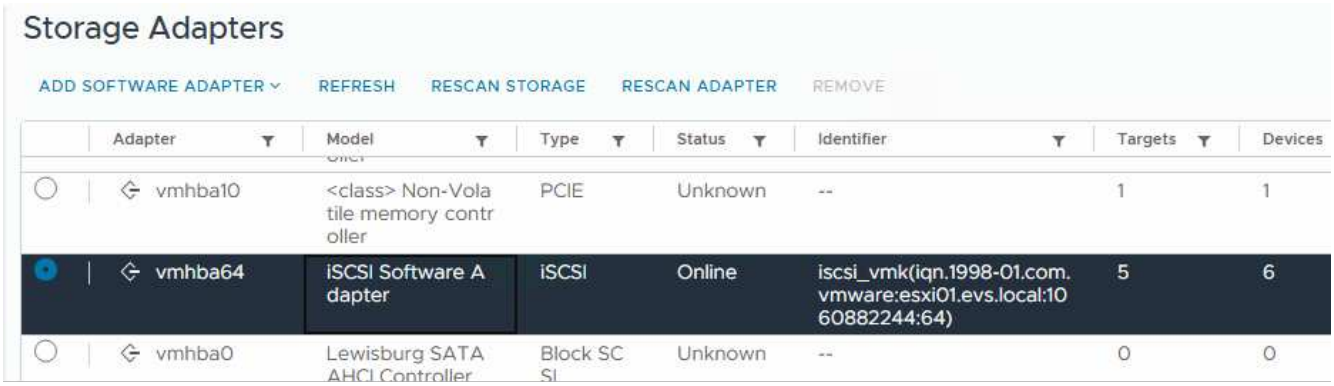
Ajouter un adaptateur réseau iSCSI

Les étapes suivantes doivent être effectuées sur chaque hôte ESXi de votre environnement.

1. Entrez le client vSphere et sélectionnez l'hôte ESXi. Sous l'onglet Configurer, choisissez « Ajouter un adaptateur logiciel », puis sélectionnez « Ajouter un adaptateur iSCSI » dans le menu déroulant, comme indiqué ici :

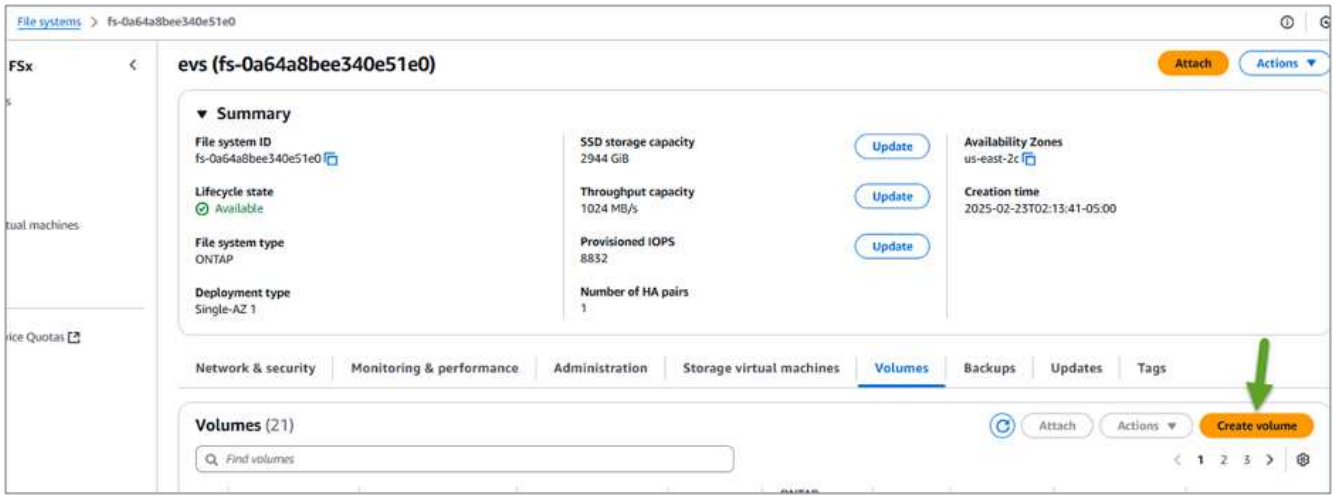


2. Une fois l'installation terminée, vous serez sur l'écran Adaptateurs de stockage. Sélectionnez « Réanalyser l'adaptateur » dans la barre de menu. Enregistrez l'IQN de l'adaptateur iSCSI : iqn.xxxx. Cette valeur sera utilisée ultérieurement dans l'étape de mappage LUN.



Créer un volume FSx pour ONTAP

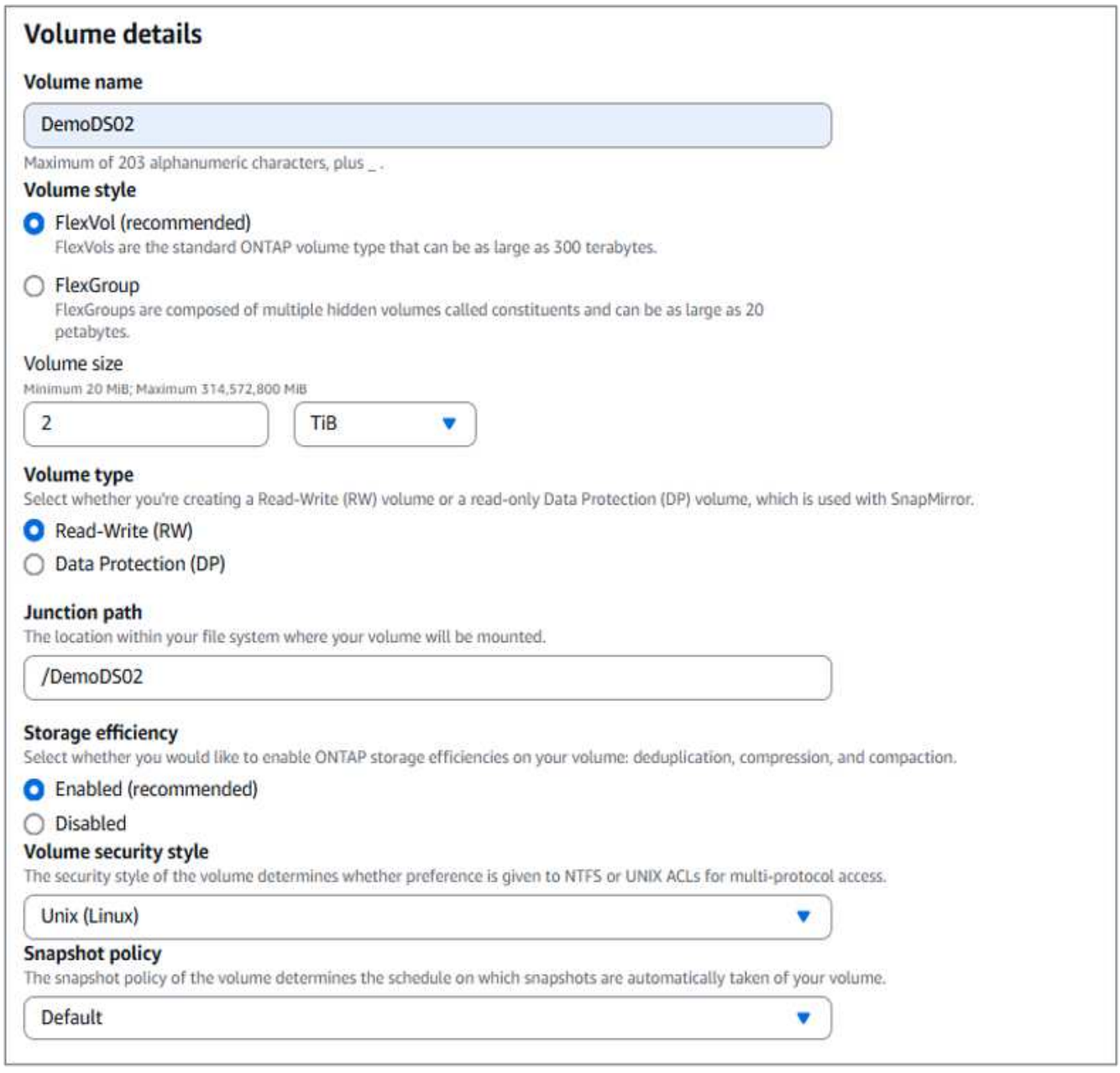
1. Accédez à la console AWS et accédez à la page de votre système de fichiers FSx for ONTAP et cliquez sur « Créer un volume ».



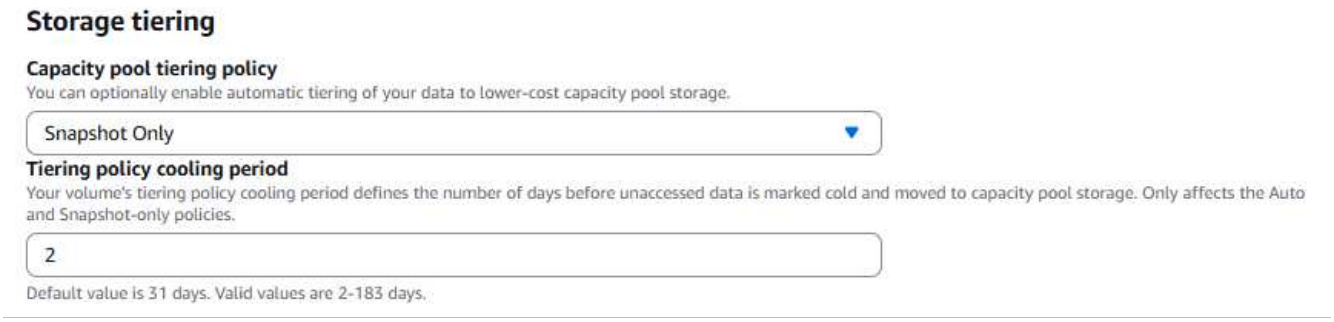
2. Sélectionnez le SVM sur lequel vous souhaitez créer le volume.



3. Sur la page « Détails du volume », saisissez les détails comme indiqué dans la capture d'écran ci-dessous. Lorsque vous avez terminé, cliquez sur « Créer » pour configurer le volume. Choisissez « Activé » pour activer les fonctionnalités d'efficacité du stockage ONTAP (compression, déduplication et compactage).



4. Pour l'option de hiérarchisation du stockage, sélectionnez « Instantané uniquement » dans le menu déroulant et définissez une période de refroidissement de la politique de hiérarchisation. La valeur par défaut est de 31 jours, mais pour cet exemple, nous définissons une période de refroidissement de deux jours.



5. Une fois le volume créé, utilisez l'interface de ligne de commande ONTAP pour définir les valeurs suivantes :

Paramètre	Configuration
Garantie de volume	Aucun (provisionnement léger)
réserve fractionnaire	0%
snap_reserve	0%
Dimensionnement automatique	grandir_rétrécir
Efficacité du stockage	Activé
Politique de hiérarchisation des volumes	Instantané uniquement
Mise à jour de l'heure d'accès (-atime-update)	FAUX
Lecture anticipée minimale (-min-readahead)	FAUX
Politique d'instantané	Aucune
Réservation d'espace LUN	Désactivées
Allocation d'espace LUN	Activé

Créer un LUN, un igroup et mapper le LUN

Dans cette section, nous montrons comment créer le LUN qui apparaîtra comme un disque dans vSphere. Nous montrerons également comment créer un groupe d'initiateurs (igroup), qui est la liste des initiateurs qui ont accès au LUN. Le groupe i permettra l'accès au LUN à partir des hôtes vSphere ESXi. Enfin, nous montrerons comment mapper l'igroup au LUN.

1. Pour accéder à l'interface de ligne de commande ONTAP , établissez une session SSH sur le port de gestion du système de fichiers FSx for ONTAP ou SVM en exécutant la commande suivante :

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. Créez le LUN. Assurez-vous de définir l'allocation d'espace et la réservation d'espace comme activées. La taille doit être jusqu'à 90 % de la taille du volume :

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. Créez le groupe i et ajoutez l'IQN de tous les hôtes ESXi au sein du cluster.

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. Mappez le LUN avec le code suivant :

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. Vérifiez le mappage LUN et vérifiez que l'état a été modifié en « mappé ». Il s'agit d'une double vérification nécessaire pour s'assurer que le LUN est dans un état mappé :

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

Obtenir les informations de configuration iSCSI à partir du SVM

1. Exécutez iSCSI show et enregistrez le nom de la cible. Cela sera utilisé dans la découverte vSphere des disques FSx pour ONTAP (Remarque : ce nom de cible est unique à votre SVM) :

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. Enregistrez les adresses IP iSCSI :

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

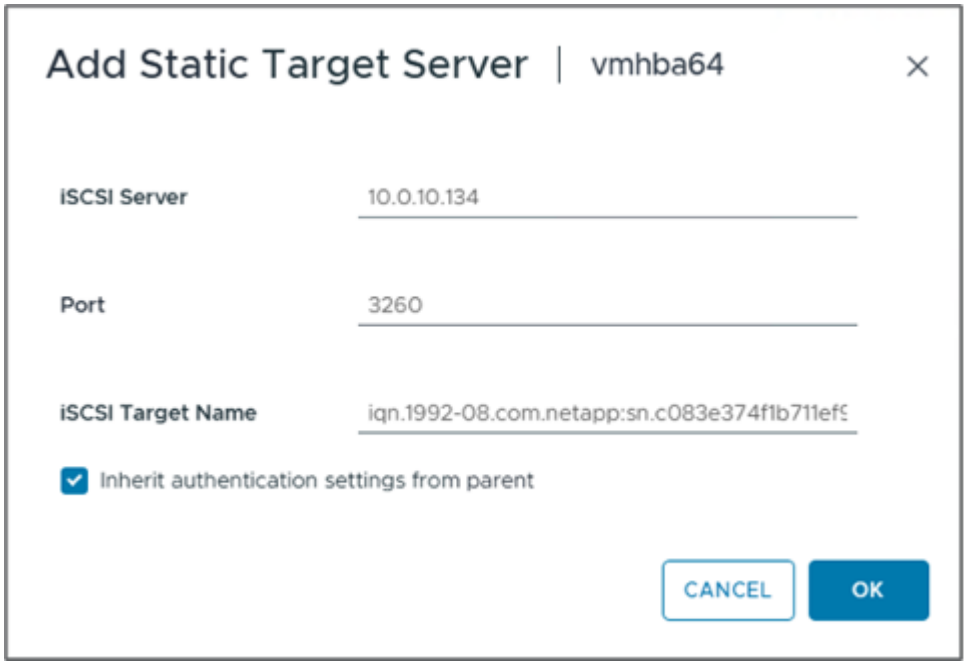
Découvrez le serveur iSCSI FSx pour ONTAP

Maintenant que nous avons mappé le LUN, nous pouvons découvrir le serveur iSCSI FSx pour ONTAP pour le SVM. Notez que pour chaque hôte ESXi existant dans votre SDDC, vous devrez répéter les étapes répertoriées ici.

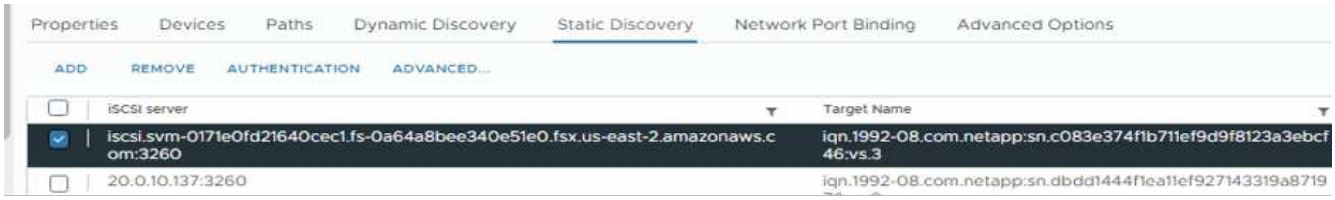
1. Tout d'abord, assurez-vous que le groupe de sécurité lié au système de fichiers FSx for ONTAP (c'est-à-dire celui connecté à l'ENI) autorise les ports iSCSI.

   Pour une liste complète des ports du protocole iSCSI et comment les appliquer, reportez-vous à"Contrôle d'accès au système de fichiers avec Amazon VPC" .

2. Dans le client vSphere, accédez à Hôte ESXi > Adaptateurs de stockage > Découverte statique et cliquez sur « Ajouter ».
3. Saisissez l'adresse IP du serveur iSCSI ci-dessus (le port est 3260). Le nom de la cible iSCSI est l'IQN de la commande iSCSI show. Cliquez sur « OK » pour continuer.



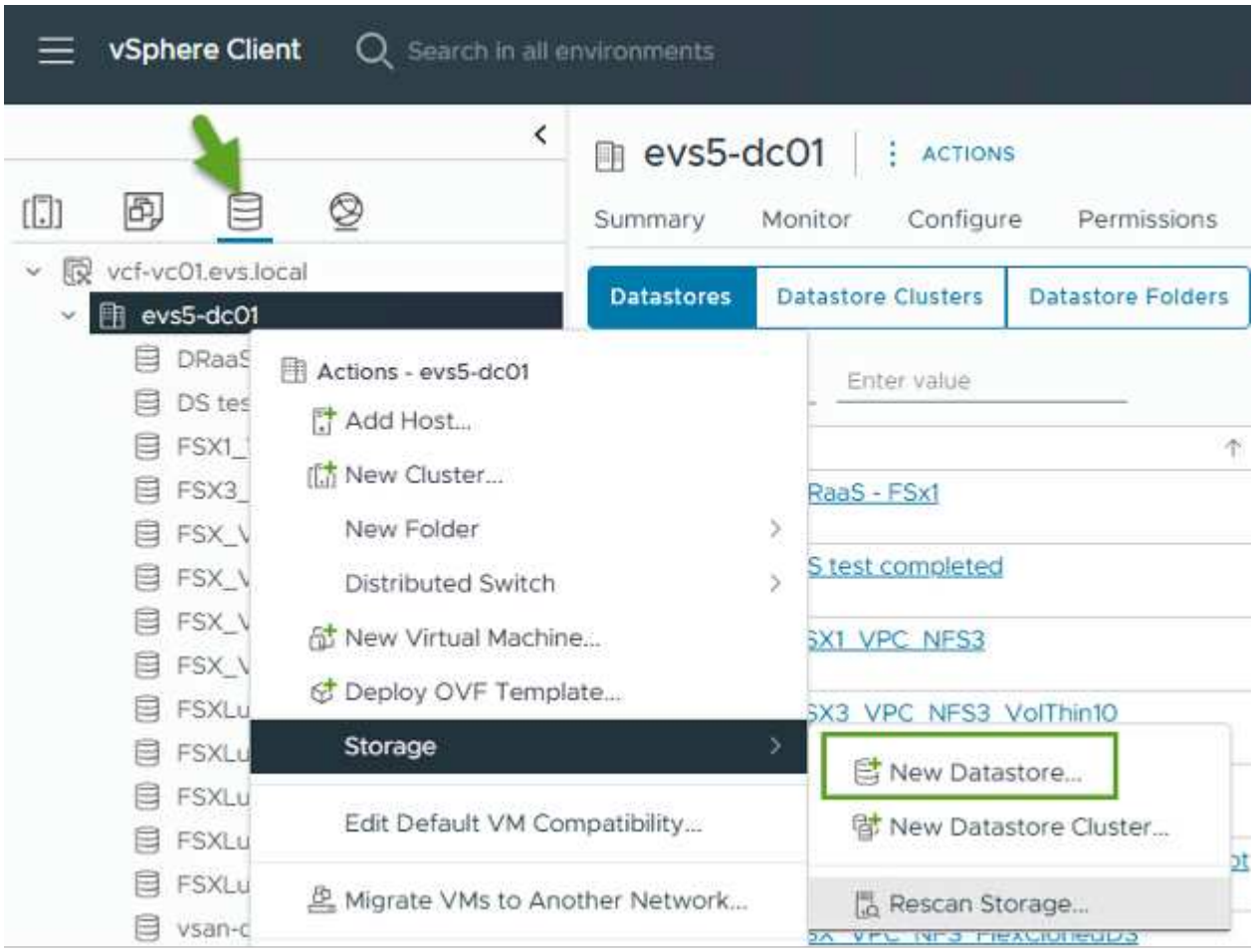
4. L'assistant se fermera et vous serez sur l'écran Découverte statique du magasin de données. Dans le tableau de cette page, vous pourrez vérifier que la cible a été découverte.



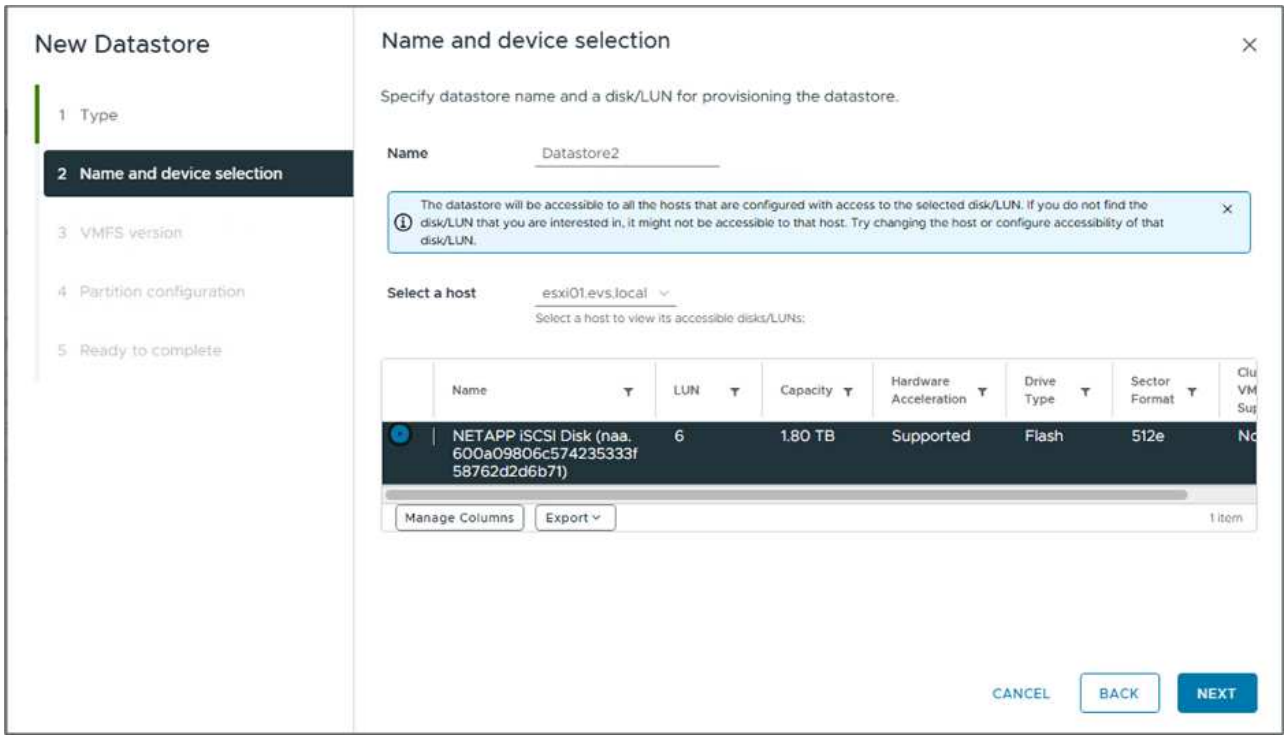
Créer une banque de données iSCSI

Maintenant que nous avons découvert le serveur iSCSI, nous pouvons créer une banque de données iSCSI.

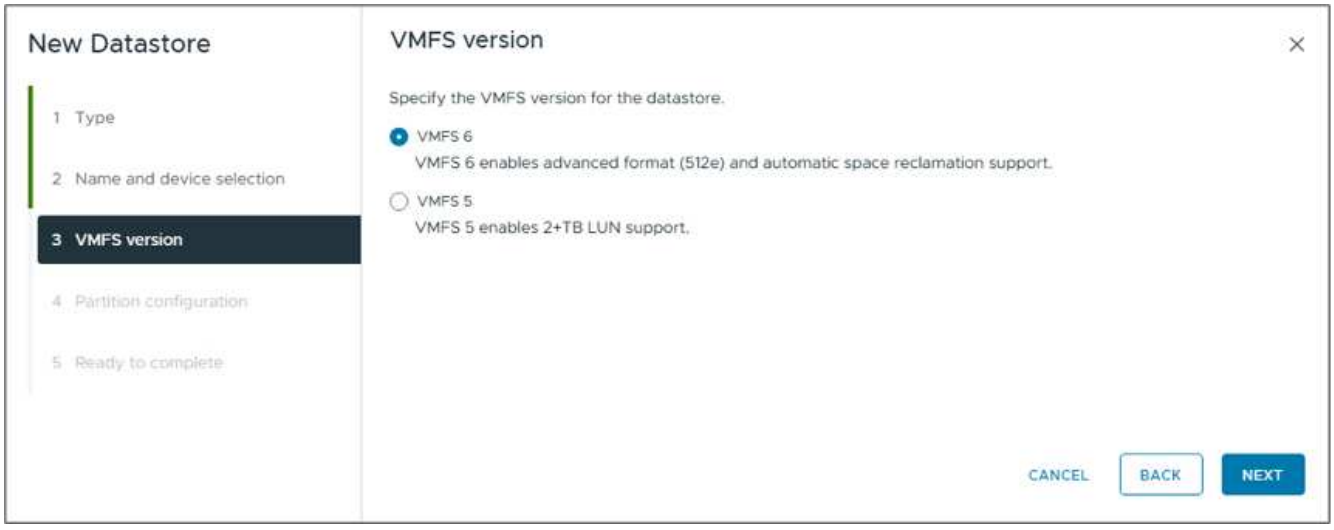
1. Dans le client vSphere, accédez à l'onglet Banque de données, sélectionnez le SDDC sur lequel vous souhaitez déployer la banque de données. Faites un clic droit et sélectionnez l'icône Stockage (indiquée par la flèche verte dans la capture d'écran ci-dessous), puis sélectionnez « Nouveau magasin de données » dans le menu déroulant :



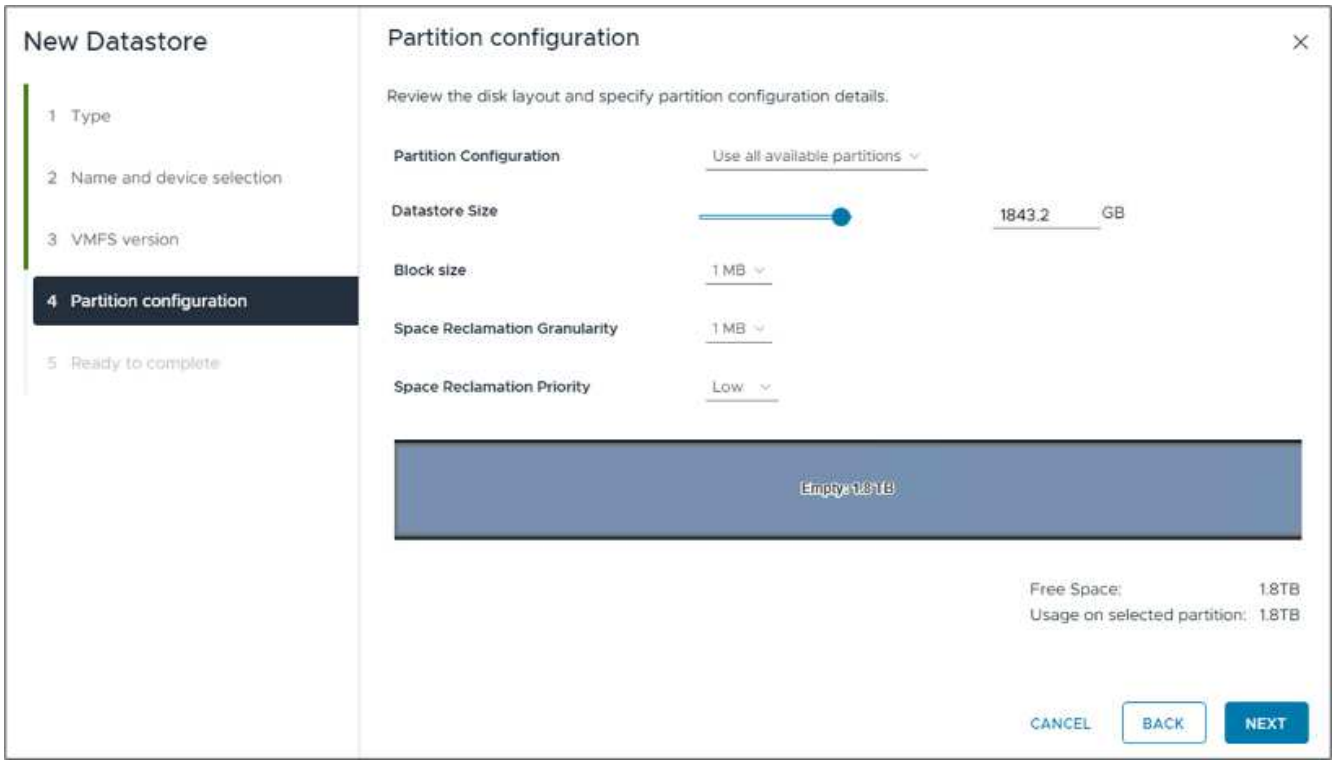
2. Vous serez maintenant dans l'assistant Nouveau magasin de données. Dans l'étape « Type », sélectionnez l'option VMFS.
3. À l'étape « Sélection du nom et de l'appareil » :
   a. Donnez un nom à votre banque de données.
   b. Sélectionnez l'hôte ESXi auquel vous souhaitez vous connecter au magasin de données.
   c. Sélectionnez le disque découvert (LUN) et cliquez sur « Suivant ».



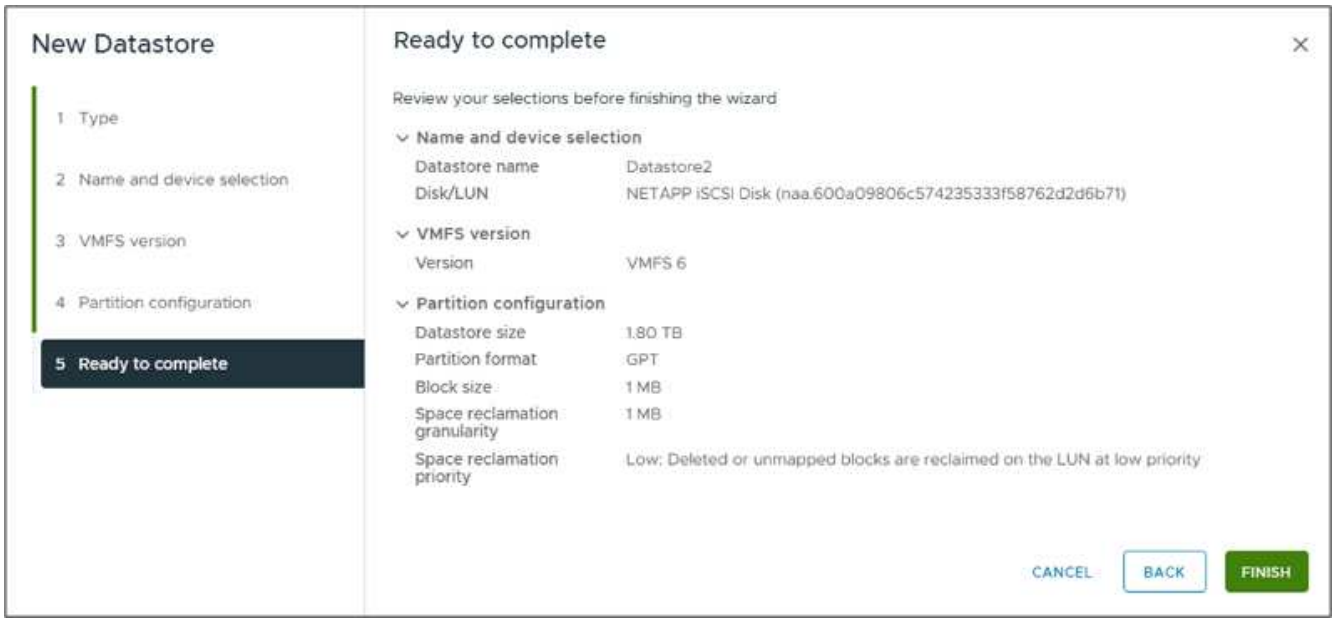
4. À l'étape « Version VMFS », sélectionnez « VMFS 6 ».



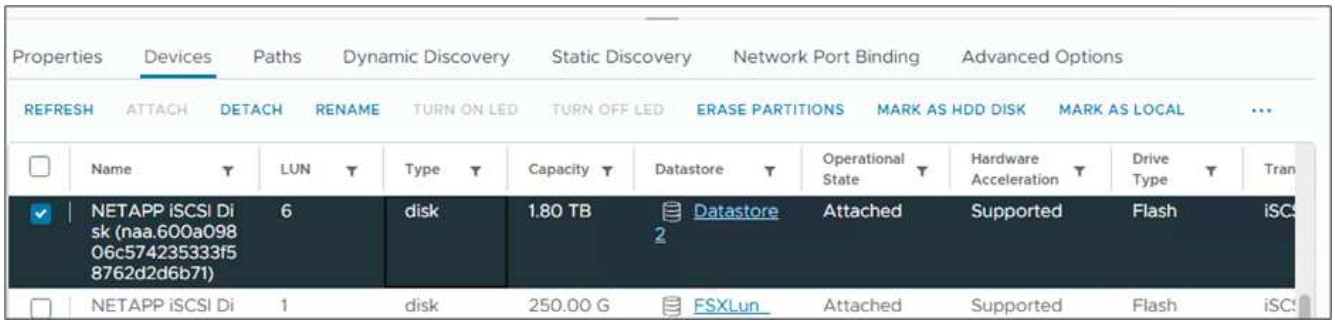
5. À l'étape « Configuration de la partition », laissez les paramètres par défaut tels quels, y compris l'option « Utiliser toutes les partitions disponibles ». Cliquez sur « Suivant » pour continuer.



6. À l'étape « Prêt à terminer », assurez-vous que les paramètres sont corrects. Lorsque vous avez terminé, cliquez sur « TERMINER » pour terminer la configuration.



7. Revenez à la page Périphériques et vérifiez que le magasin de données a été connecté.



Conclusion

Ce document fournit des instructions sur la façon de configurer FSx pour ONTAP en tant que stockage externe pour Amazon EVS pour une utilisation avec les protocoles NFS et iSCSI.

L'utilisation de FSx pour ONTAP comme stockage externe pour Amazon EVS offre des valeurs opérationnelles et commerciales claires. Il offre une meilleure résilience des données, une meilleure protection, une meilleure réplication et une meilleure rentabilité grâce à la technologie ONTAP , et maintient le coût total de possession optimisé grâce au découplage de l'architecture hyperconvergée VMware. Avec FSx pour ONTAP, les utilisateurs d'Amazon EVS peuvent faire évoluer le stockage sans ajouter de ressources de calcul et sans augmenter les coûts. Cela ouvre tout le potentiel d'élasticité et d'évolutivité présenté par le cloud AWS.

Pour en savoir plus, lisez l'annonce des nouveautés d'Amazon :"Amazon EVS s'intègre désormais à FSx pour ONTAP" , et le blog NetApp :"Amazon EVS annonce la prise en charge de FSx pour ONTAP" .

Protéger le datastore FSx ONTAP pour EVS

Comment protéger les datastores Amazon FSx for NetApp ONTAP avec Amazon Elastic VMware Service à l'aide du NetApp SnapCenter Plug-in for VMware

Ce guide présentera une approche de déploiement simple pour protéger les datastores FSx for ONTAP Network File System (NFS) et iSCSI Amazon EVS et les machines virtuelles associées à l'aide de la solution de sauvegarde et de restauration NetApp SnapCenter® Plug-in for VMware vSphere (SCV) pour machines virtuelles.

Introduction

Les datastores supplémentaires basés sur Amazon FSx for NetApp ONTAP (FSx for ONTAP) pour Amazon Elastic VMware Service (Amazon EVS) offrent une excellente solution pour exécuter à la fois des charges de travail exigeantes en termes de performances — telles que l'utilisation de nConnect, l'appairage Amazon Virtual Private Cloud (Amazon VPC) et l'utilisation de plusieurs connexions réseau par montage de datastore — et des charges de travail gourmandes en stockage.

Cette fonctionnalité permet aux clients de s'affranchir des limitations du stockage local fourni par un réseau de stockage virtuel (vSAN), de faire évoluer le stockage indépendamment des ressources de calcul et de réduire le coût de possession total. Au-delà des avantages en termes de coût de possession total (TCO), FSx for ONTAP offre Amazon EVS avec des fonctionnalités de niveau entreprise familières aux clients d'ONTAP sur site, contribuant ainsi à optimiser et à simplifier les déploiements. L'utilisation de FSx for ONTAP donne accès aux technologies NetApp® Snapshot™, SnapMirror® et SnapVault® qui prennent en charge les opérations de sauvegarde et de restauration des machines virtuelles (VM), des datastores et des disques de machines virtuelles (VMDK). La protection basée sur les snapshots constitue une fonctionnalité clé.

Aperçu

À mesure que les entreprises développent et consolident leurs environnements, la protection des charges de travail et du stockage sous-jacent devient primordiale. SCV peut être utilisé pour sauvegarder les datastores et les machines virtuelles directement depuis le client Amazon EVS vSphere.

Objectif de ce guide

Ce guide fournit des instructions sur la façon de protéger un datastore FSx for ONTAP pour Amazon EVS à l'aide de SCV. Des exemples de scénarios de protection et de restauration de machines virtuelles et de bases de données sont également fournis.

Public

Ce didacticiel est destiné aux architectes et administrateurs Cloud familiarisés avec VMware vSphere, Amazon EVS, la console AWS et FSx pour ONTAP.

Étapes générales du déploiement et de la configuration

Vous trouverez ci-dessous les étapes principales pour déployer et configurer SCV afin de protéger vos VMs et datastores sur Amazon EVS :

1. Téléchargez l'Open Virtual Appliance (OVA) SCV.
2. Connectez-vous avec les identifiants du client vSphere à Amazon EVS.
3. Déployez un modèle Open Virtualization Format (OVF) pour démarrer l'assistant de déploiement VMware.
4. Pour accéder au plug-in, sélectionnez SnapCenter Plug-in for VMware dans le menu.
5. Ajouter du stockage.
6. Créer des règles de sauvegarde.
7. Créer des groupes de ressources.
8. Groupes de ressources de sauvegarde.
9. Restaurez l'intégralité de la machine virtuelle ou un disque virtuel particulier ou des fichiers invités.

Procédure d'installation du plug-in SnapCenter pour VMware

Cette section décrit les étapes de configuration du SnapCenter Plug-in pour VMware.

Prérequis

Les prérequis suivants sont nécessaires avant de commencer :

1. Pour enregistrer le serveur vCenter lors du déploiement de l'OVA, spécifiez le nom de domaine complet (FQDN) ou l'adresse IP du vCenter.
2. Pour les identifiants vCenter, utilisez un compte disposant des privilèges minimaux requis
3. Ouvrez les ports du pare-feu pour l'accès au serveur vCenter.
4. Mettez à jour le groupe de sécurité du VPC Amazon où FSx for ONTAP est en cours d'exécution pour permettre à SCV d'accéder à FSx for ONTAP.

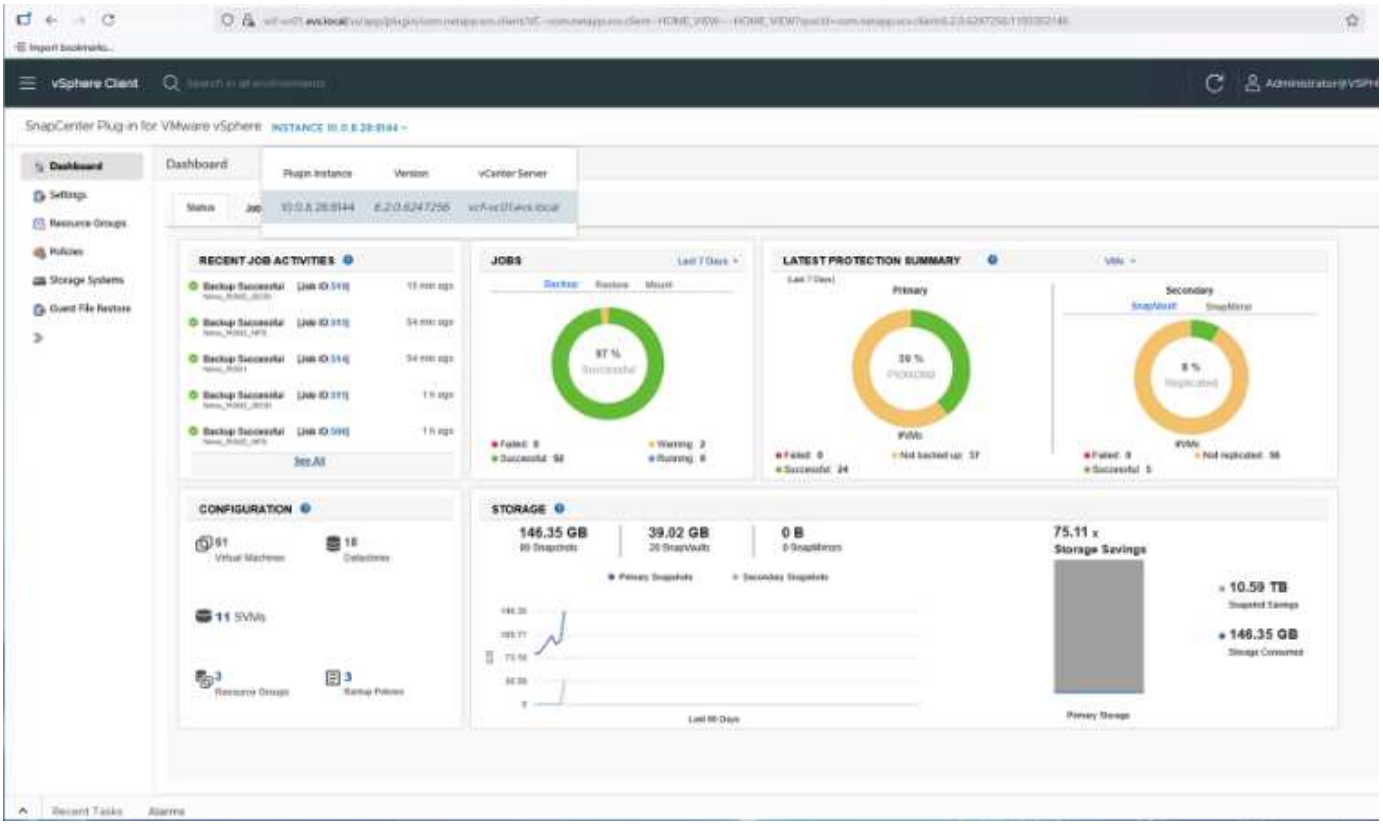
SCV est disponible gratuitement.

Configuration du SnapCenter Plug-in pour VMware

Pour protéger les machines virtuelles et les banques de données NFS/iSCSI qui les hébergent, SCV doit être déployé. Il s'agit d'une simple importation OVF.

Les étapes de déploiement sont les suivantes :

1. Téléchargez l'OVA depuis "Site de support NetApp".
2. Connectez-vous à Amazon EVS vCenter.
3. Dans vCenter, cliquez avec le bouton droit sur n'importe quel objet d'inventaire tel qu'un centre de données, un dossier, un cluster ou un hôte et sélectionnez « Déployer le modèle OVF ».
4. Sélectionnez les paramètres appropriés, y compris le stockage, segmentez et personnalisez le modèle pour mettre à jour le vCenter et ses informations d'identification, créer des identifiants SCV et les détails IP. Une fois la vérification effectuée, sélectionnez « Terminer ».
5. Attendez que les tâches d'importation et de déploiement OVF soient terminées.
6. Une fois le SCV déployé avec succès, il sera enregistré dans vCenter.
7. Pour accéder au plug-in, accédez à la barre latérale gauche de la page du client web vCenter, puis sélectionnez « SnapCenter Plug-in for VMware ».



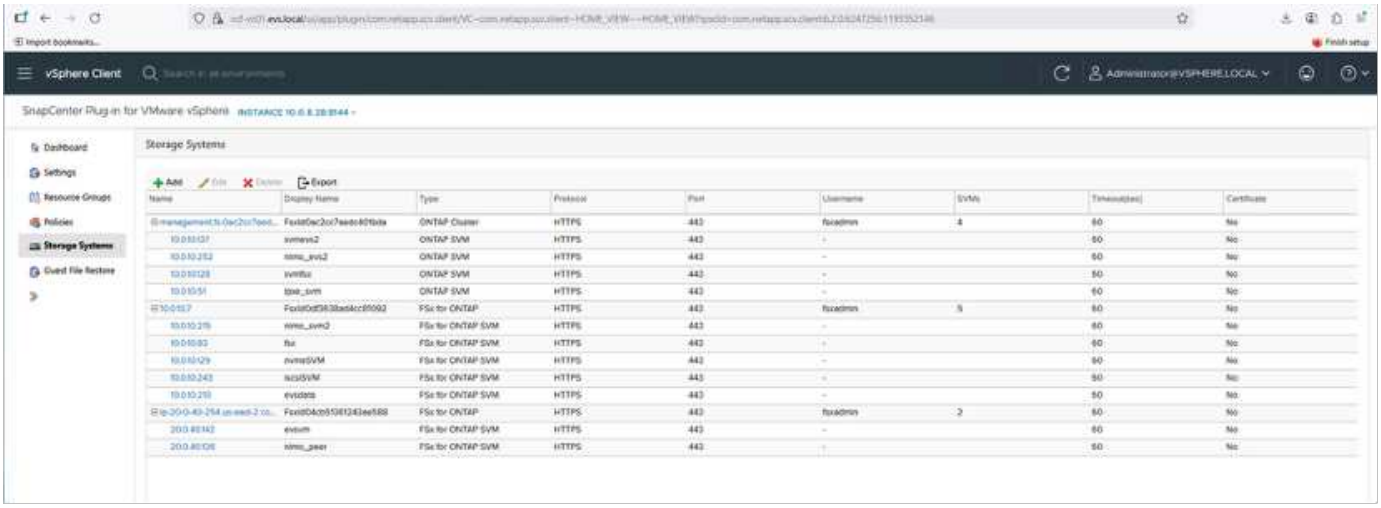
Procédure de configuration du SnapCenter Plug-in pour VMware

Cette section décrit les étapes de configuration du SnapCenter Plug-in pour VMware. Les sections suivantes détaillent comment ajouter du stockage, créer des règles de sauvegarde et créer des groupes de ressources.

Ajout du système de stockage

L'étape suivante pour protéger les charges de travail avec SVC consiste à ajouter le "système de stockage". L'ajout de stockage permet à SCV de détecter et de gérer les opérations de sauvegarde et de restauration au sein de vCenter. Incluez le point de terminaison de gestion FSx for NetApp ONTAP ou l'adresse IP du point de terminaison d'administration de la machine virtuelle de stockage (SVM) comme système de stockage pour activer la sauvegarde et la restauration des machines virtuelles.

1. Dans le menu de navigation de gauche de l'EVS vCenter, sélectionnez « SnapCenter Plug-in for VMware ».
2. Sélectionnez « Storage System ».
3. Sélectionnez « Ajouter » pour ajouter les détails FSx for ONTAP.
4. Utilisez la méthode « Credentials as the Authentication » et saisissez FSxadmin comme nom d'utilisateur et mot de passe. Sélectionnez ensuite « Add » pour enregistrer les paramètres.



Tous les SVM sont automatiquement ajoutés lorsque le système de fichiers est ajouté.

Si la version de SCV est 6.2, allez sur "la page d'assistance SCV" et téléchargez la version SCV 6.2P1.

Créer une règle de sauvegarde

Une stratégie de sauvegarde robuste doit définir des facteurs clés tels que la planification des sauvegardes, les données à sauvegarder et la durée de conservation des sauvegardes. Des copies instantanées peuvent être planifiées toutes les heures ou tous les jours afin de protéger l'ensemble des datastores. La planification des sauvegardes de cette manière sécurise non seulement les datastores, mais prend également en charge les opérations de sauvegarde et de restauration des VMs et des VMDK contenus dans ces datastores.

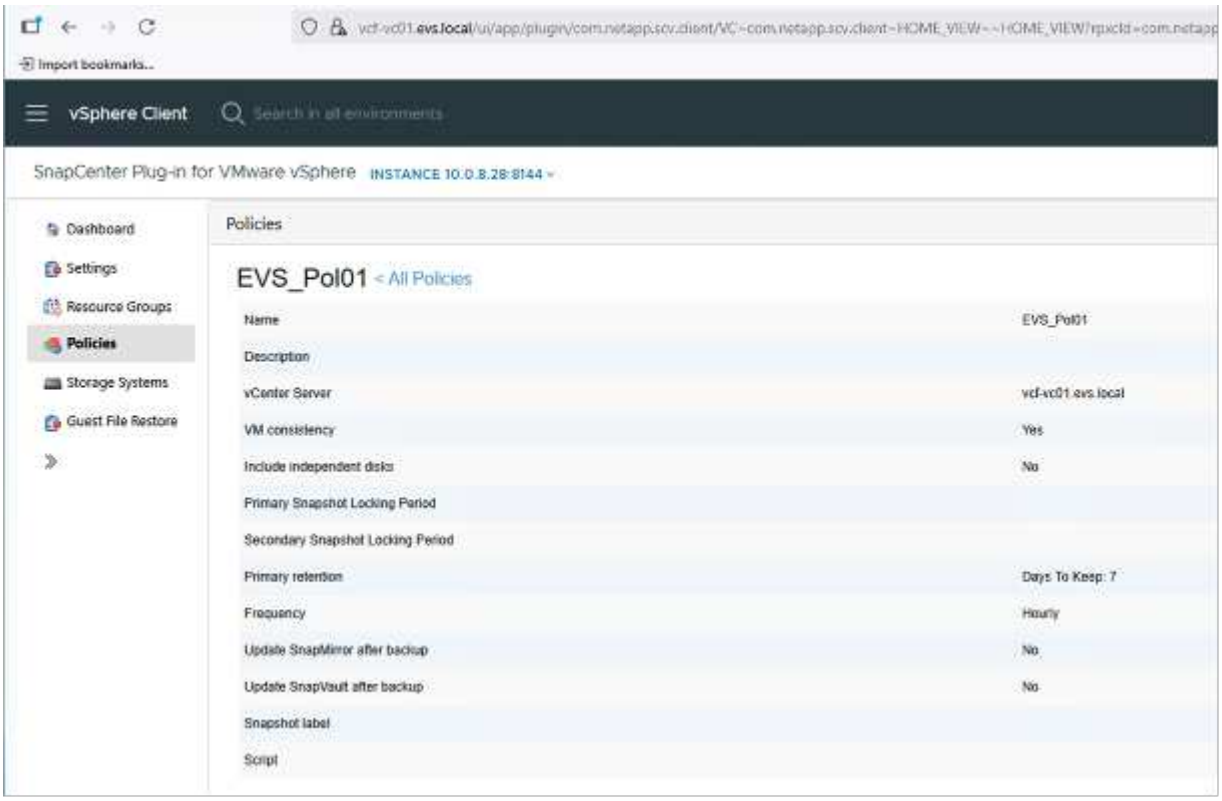
Avant de lancer les sauvegardes des machines virtuelles et des banques de données, créez "règles de sauvegarde" et un groupe de ressources. La règle de sauvegarde spécifie des paramètres tels que la planification des sauvegardes et les paramètres de conservation.

Voici les étapes à suivre pour créer une règle de sauvegarde :

1. Accédez au menu de navigation situé à gauche dans SCV et sélectionnez « Policies ».
2. Sur la page Policies, sélectionnez « Create » pour démarrer l'assistant.
3. Sur la page « New Backup Policy », saisissez un nom pour la politique.

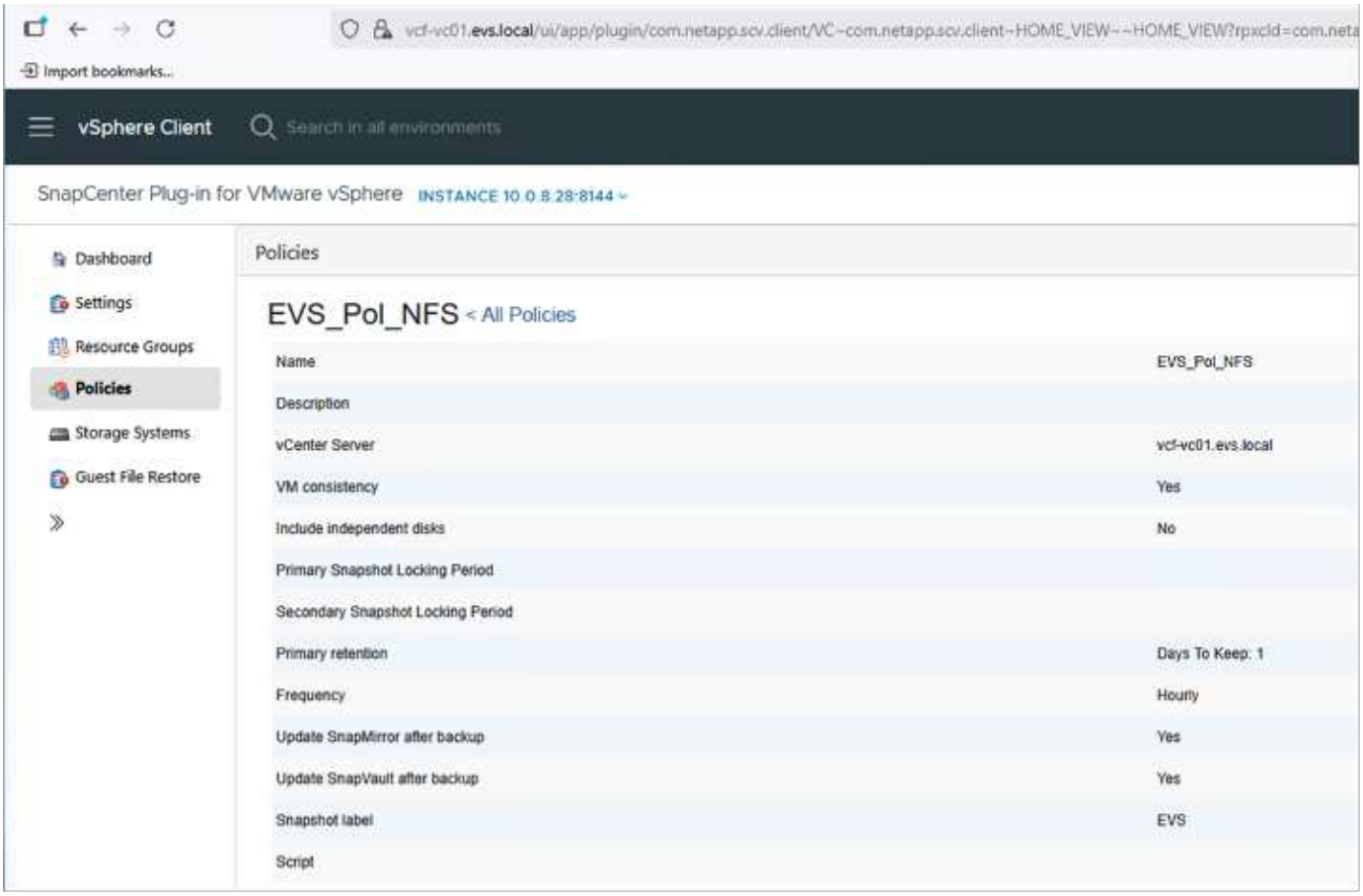
4. Spécifiez la période de conservation, la fréquence de sauvegarde et les paramètres de réplication.
5. Cochez la case "Locking Period" pour activer le verrouillage des instantanés. Vous pouvez sélectionner les périodes de verrouillage des instantanés principale et secondaire en jours/mois/années.

Quelle que soit la valeur de conservation définie dans la politique SnapMirror, la copie secondaire du Snapshot reste intacte jusqu'à l'expiration de la période de verrouillage du snapshot secondaire spécifiée.



Pour activer les sauvegardes cohérentes avec les machines virtuelles, VMware tools doit être installé et en cours d'exécution. Lorsque la case de cohérence des machines virtuelles est cochée, les machines virtuelles sont d'abord mises en veille, puis VMware effectue une capture instantanée cohérente des machines virtuelles (à l'exclusion de la mémoire), puis SCV effectue son opération de sauvegarde, et enfin les opérations sur les machines virtuelles reprennent.

Pour répliquer les copies Snapshot vers un système de fichiers miroir ou de coffre, les relations doivent être configurées au préalable.



Une fois la règle de sauvegarde créée, l'étape suivante consiste à créer le groupe de ressources qui définira les datastores NFS ou iSCSI appropriés et les machines virtuelles devant être sauvegardées.

Créer un groupe de ressources

Un groupe de ressources sert de conteneur pour les machines virtuelles et les banques de données nécessitant une protection. Les ressources peuvent être ajoutées ou supprimées d'un groupe de ressources à tout moment, offrant ainsi une flexibilité dans la gestion des configurations de sauvegarde.

Vous pouvez créer un "groupe de ressources" en suivant les étapes suivantes :

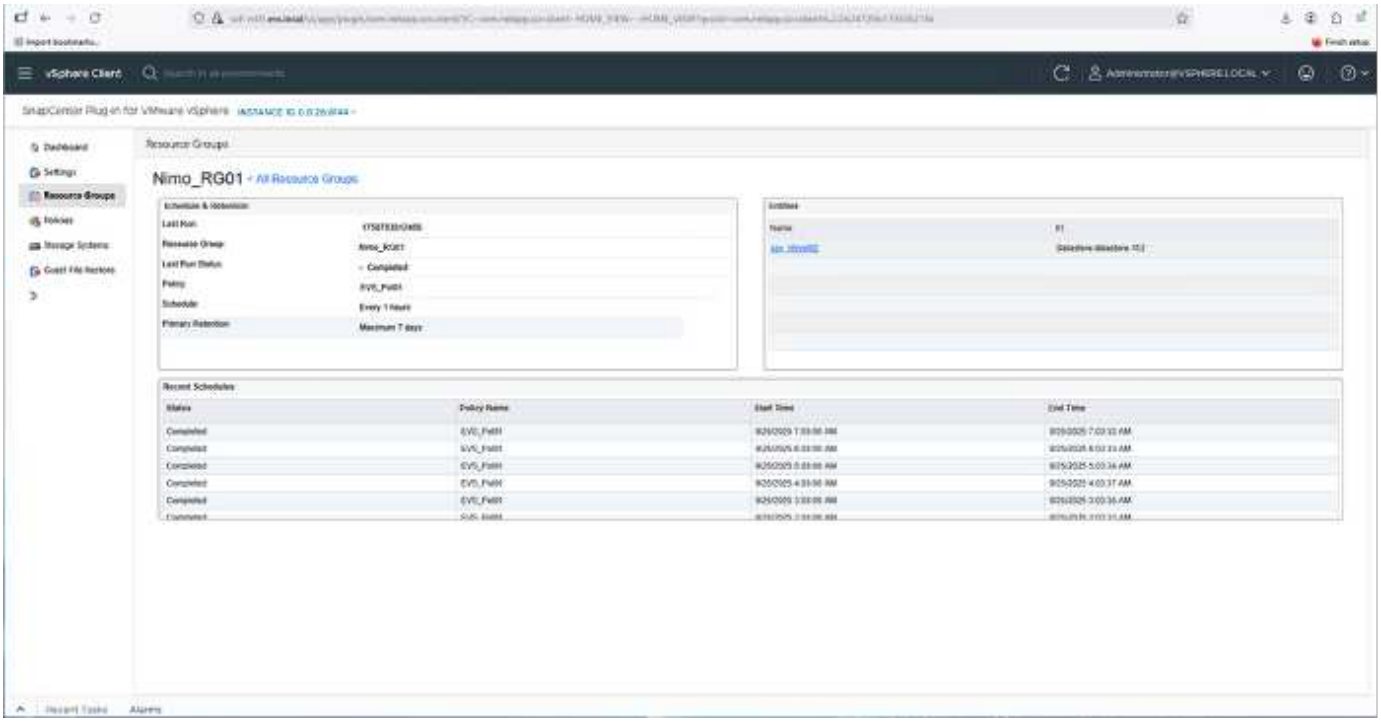
1. Accédez au volet de navigation de gauche dans SCV et sélectionnez "Resource Groups".
2. Sur la page Groupes de ressources, sélectionnez « Créer » pour démarrer l'assistant de création de groupe de ressources.

> Une autre option pour créer des groupes de ressources consiste à sélectionner une VM ou un datastore individuel et à créer un groupe de ressources qui ne contient que cette ressource.

3. Sur la page « Ressources », sélectionnez la portée (VMs ou datastores) et le centre de données.
4. Sur la page « Spanning disks », sélectionnez l'option « Virtual Machines with multiple VMDKs across multiple datastores ».
5. Ensuite, associez une règles de sauvegarde. Sélectionnez une règles de sauvegarde existante ou créez-en une nouvelle.
6. Sur la page « Planifications », configurez la planification des sauvegardes pour chaque règles de

sauvegarde sélectionnée.

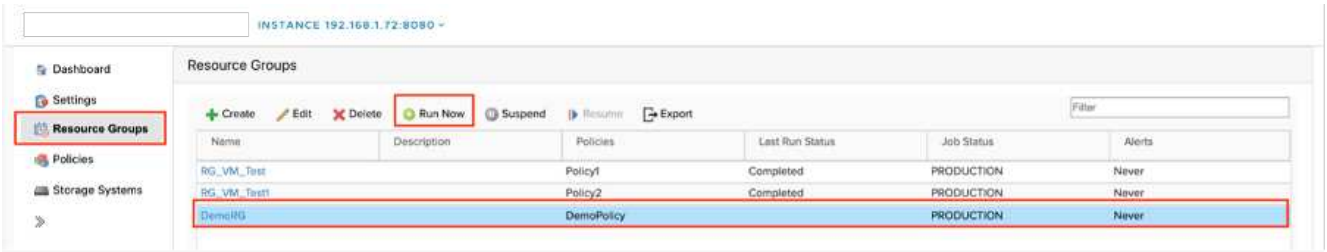
7. Une fois vos sélections effectuées, sélectionnez « Finish ». Cela créera un nouveau groupe de ressources et l'ajoutera à la liste des groupes de ressources.



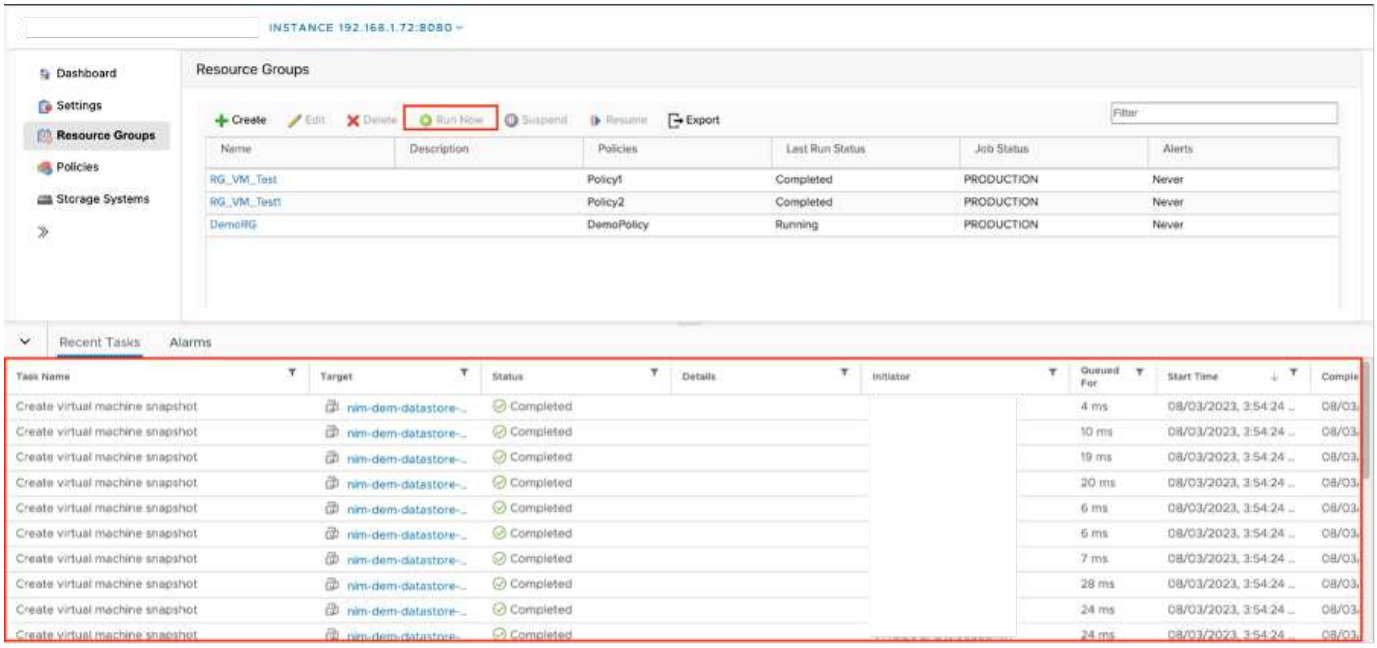
Sauvegarde des groupes de ressources

Les opérations de sauvegarde sont exécutées sur toutes les ressources définies au sein d'un groupe de ressources. Si un groupe de ressources a une règle de sauvegarde attachée et une planification configurée, les sauvegardes s'effectuent automatiquement selon la planification.

1. Dans le menu de navigation de gauche de la page du client web vCenter, sélectionnez « SnapCenter Plug-in for VMware », puis « Resource Groups ».
2. Sur la page Groupes de ressources, trouvez le groupe de ressources désigné et sélectionnez « Exécuter maintenant » pour démarrer la sauvegarde manuelle.



3. Si le groupe de ressources comporte plusieurs règles de sauvegarde configurées, sélectionnez la règle de sauvegarde pour l'opération de sauvegarde dans la boîte de dialogue « Backup Now ».
4. Sélectionnez "OK" pour lancer la sauvegarde.

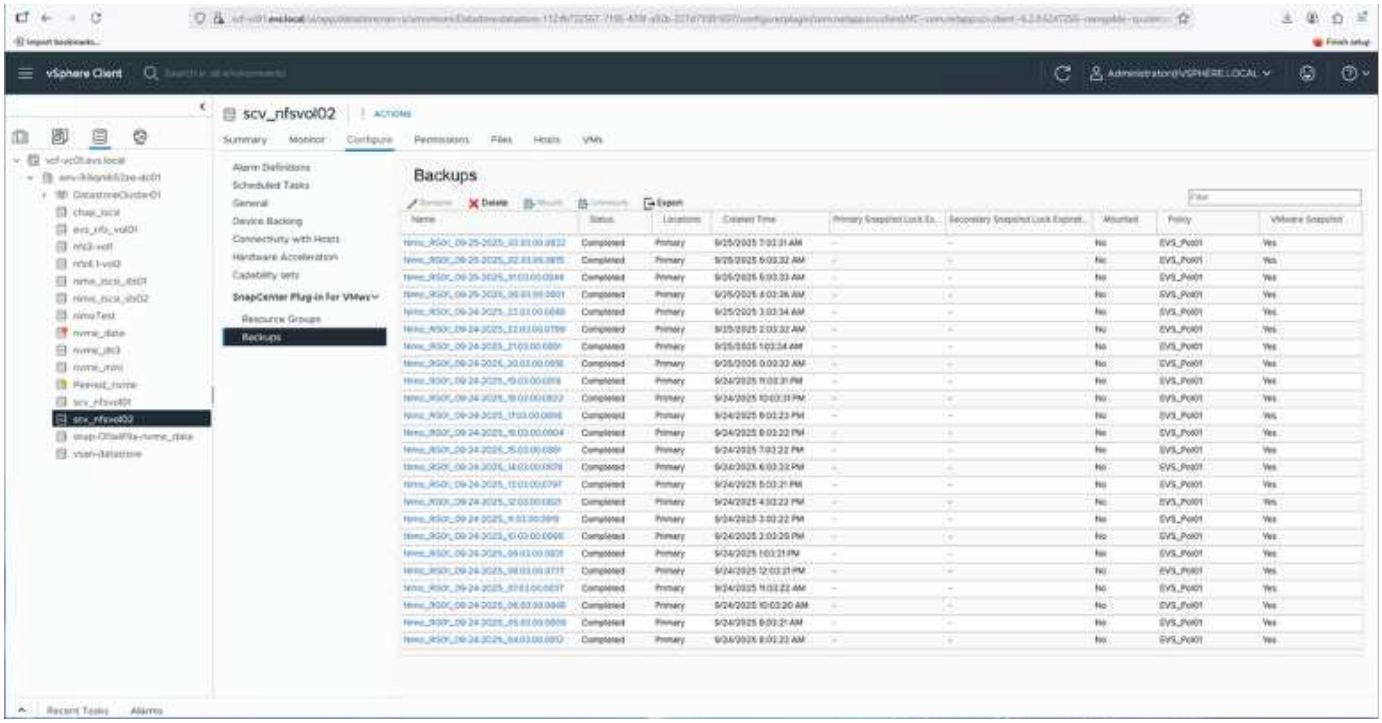


Surveillez l'avancement de l'opération en sélectionnant « Recent Tasks » en bas de la fenêtre ou, pour plus de détails, en sélectionnant « Job Monitor » sur le tableau de bord.

Le processus de création de règles de sauvegarde, de configuration des groupes de ressources et d'exécution des opérations de sauvegarde est cohérent pour différents protocoles de stockage, notamment NFS et iSCSI.

Les sauvegardes sont effectuées selon le calendrier défini dans la règle.

Une fois la sauvegarde terminée, elle peut être consultée au niveau du datastore ou pour des machines virtuelles individuelles en sélectionnant « SnapCenter Plug-in for VMware vSphere » dans la liste déroulante, puis en choisissant « Restaurer ».



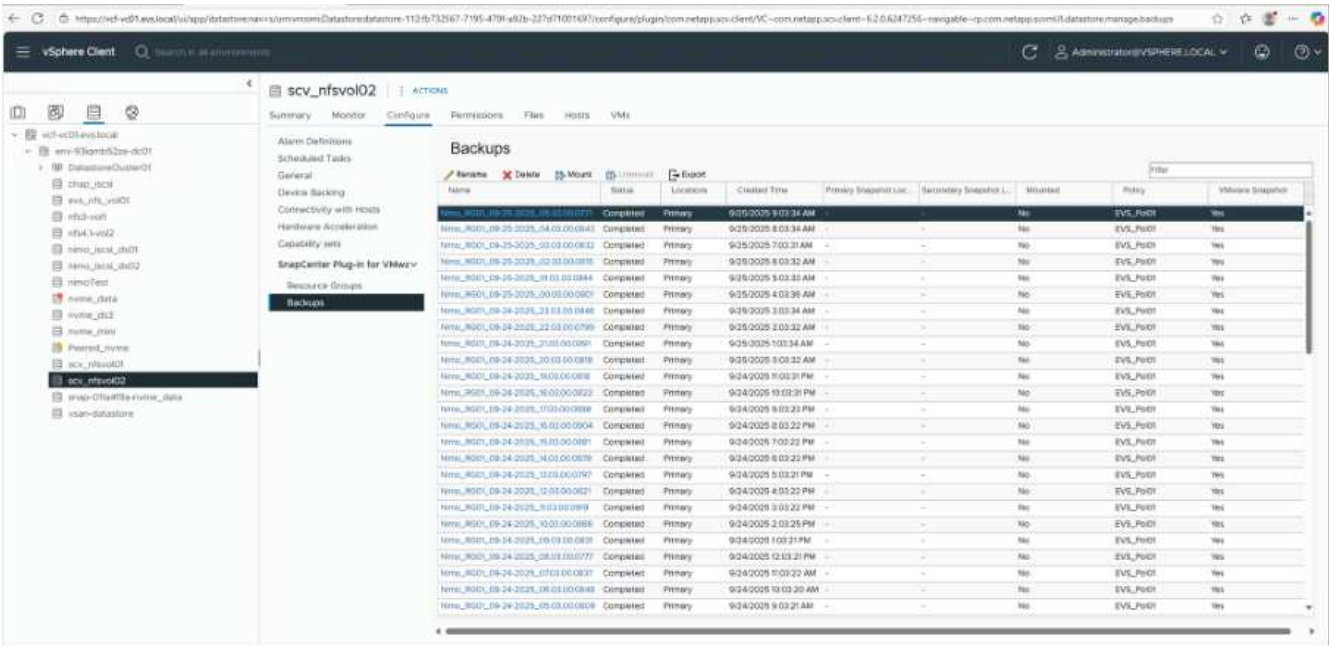
Procédure de restauration des machines virtuelles protégées par le SnapCenter Plug-in pour VMware

Cette section décrit les étapes de restauration des machines virtuelles à partir de sauvegardes. SCV peut être utilisé pour restaurer des machines virtuelles au sein de vCenter, permettant de les récupérer sur le datastore d'origine de l'hôte ESXi d'origine (en écrasant le contenu existant), de restaurer des machines virtuelles supprimées ou renommées à partir d'une copie de sauvegarde, sur un autre datastore de l'hôte ESXi d'origine, sur le datastore d'origine d'un autre hôte ESXi géré par le même vCenter, ou sur un autre datastore d'un autre hôte ESXi au sein du même environnement vCenter.

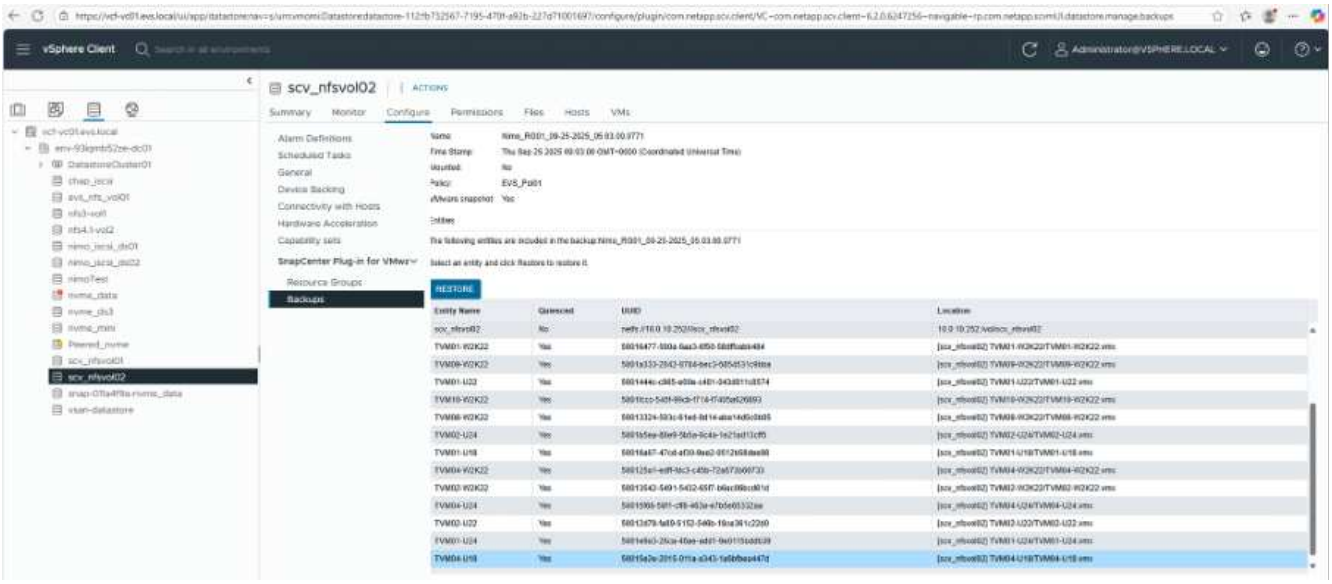
Étapes pour effectuer l'opération de restauration

Pour effectuer l'opération de restauration, suivez ces étapes :

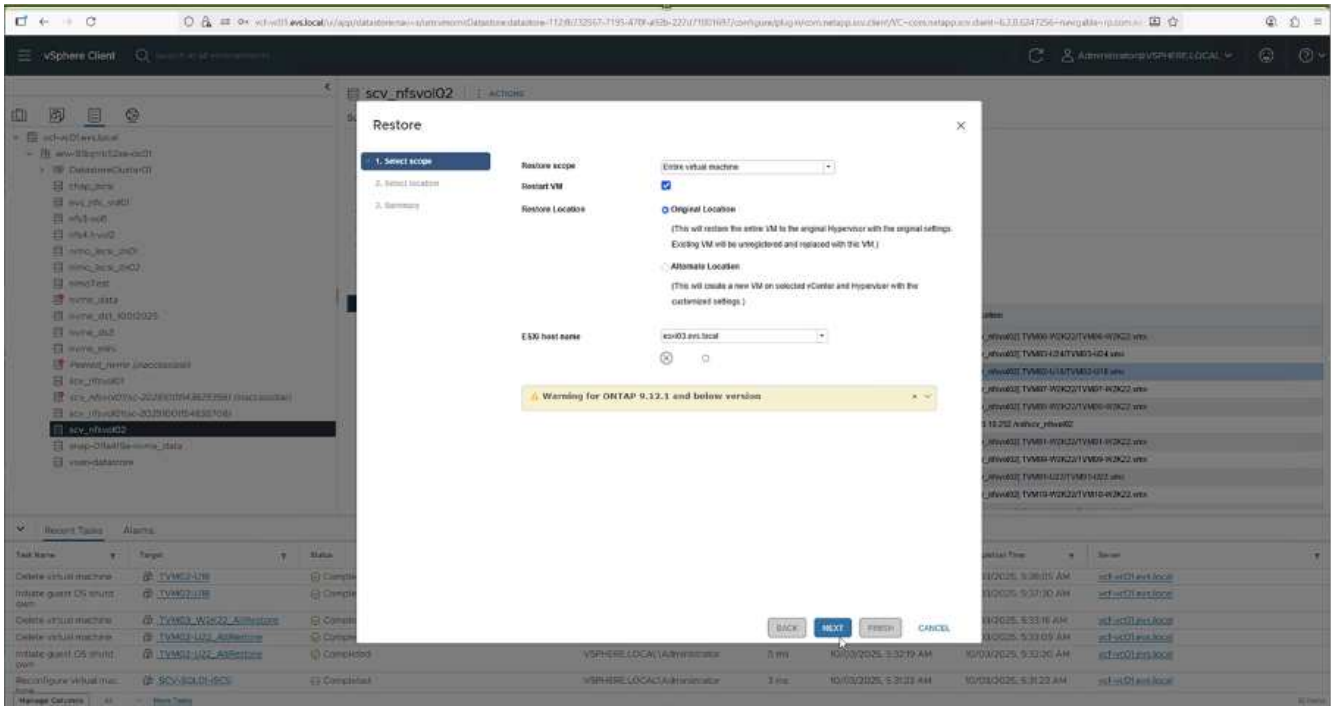
1. Dans l'interface graphique du client web EVS vSphere, accédez à « Inventory > Datastores » et sélectionnez le datastore souhaité. Ensuite, naviguez jusqu'à « Configure > Backups » dans la section « SnapCenter Plug-in for VMware vSphere ».



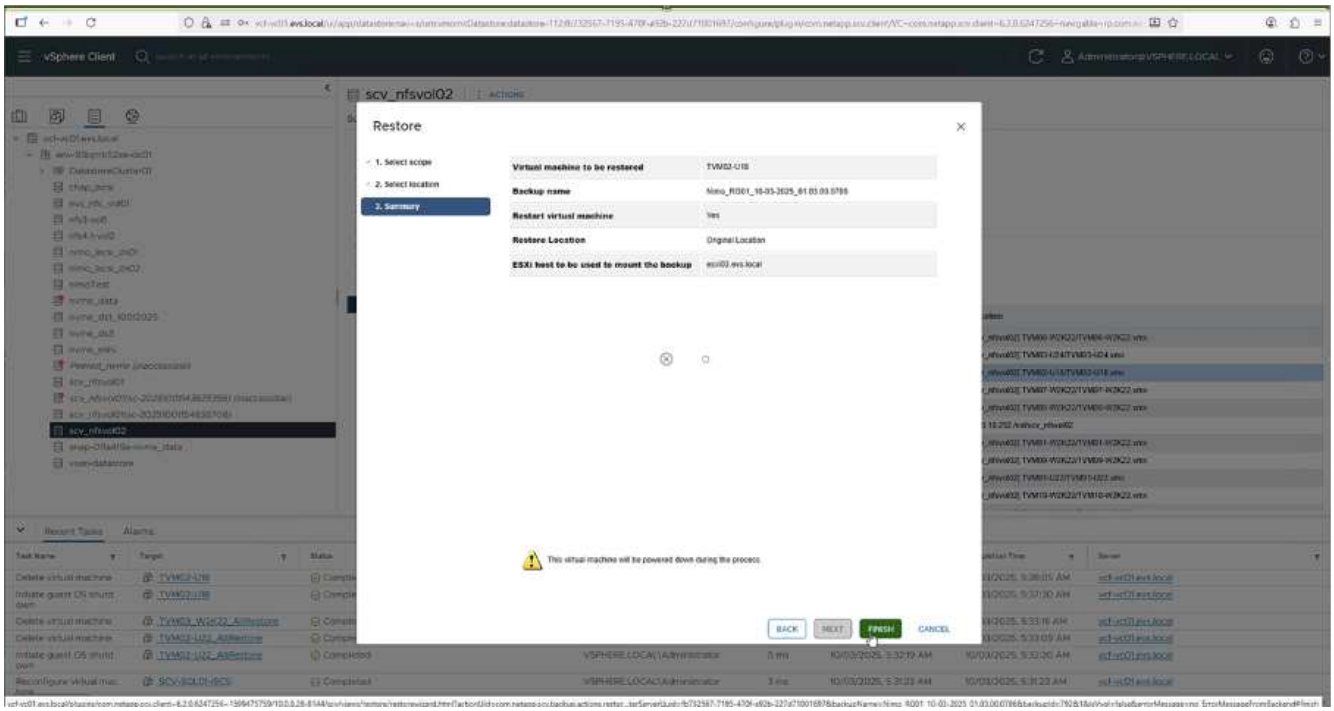
2. Double-cliquez sur une sauvegarde pour afficher toutes les machines virtuelles incluses dans cette sauvegarde. Trouvez la machine virtuelle à restaurer dans la liste et sélectionnez "Restaurer".



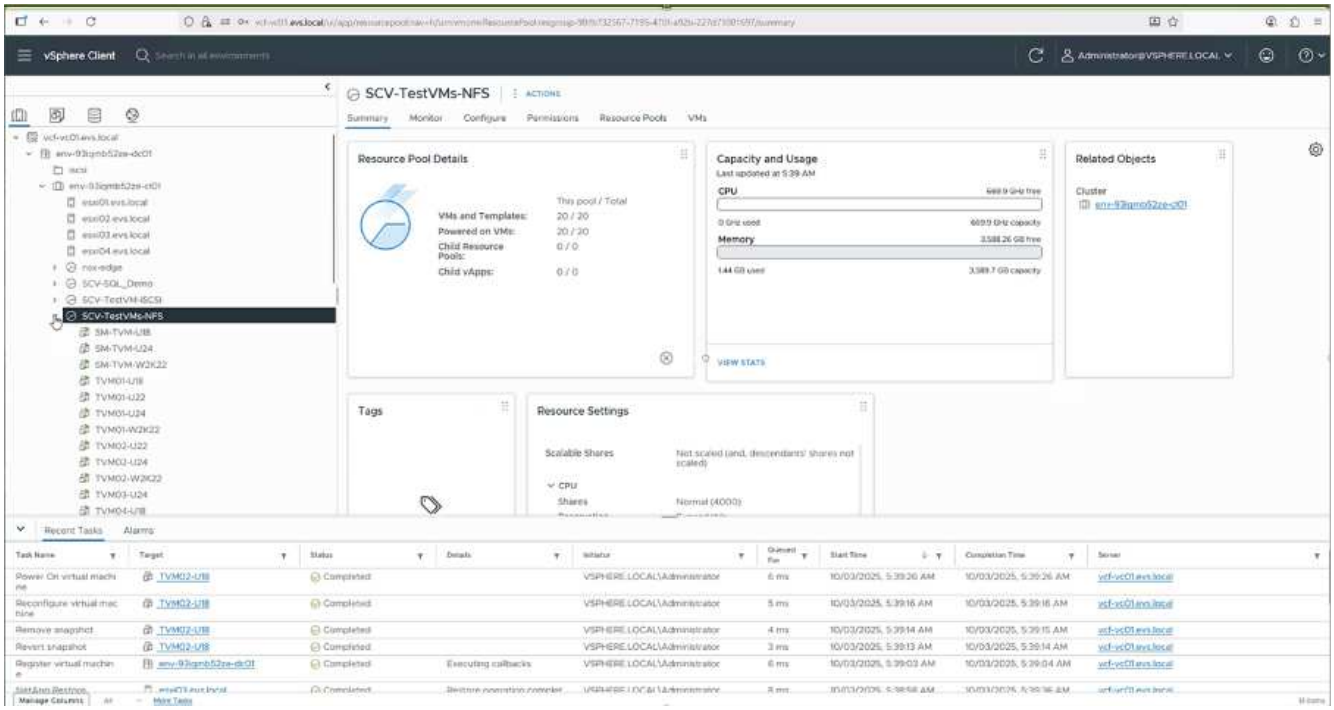
3. Sur la page « Select Scope page », sélectionnez « Entire Virtual Machine » dans le champ « Restore scope », puis sélectionnez « Restore location » et saisissez les informations ESXi de destination où la sauvegarde doit être montée.
4. Activez la case à cocher « Restart VM » si la VM doit être mise sous tension après l'opération de restauration.
5. Sur la page "Sélectionner un emplacement", choisissez un emplacement principal.



6. Consultez la page « Summary », puis sélectionnez « Finish ».



7. Surveillez l’avancement de l’opération en sélectionnant "Tâches récentes" en bas de l’écran.



Bien que les machines virtuelles soient restaurées, elles ne sont pas automatiquement réintégrées à leurs groupes de ressources d’origine. Si vous souhaitez protéger ces machines virtuelles, ajoutez-les manuellement aux groupes de ressources appropriés.

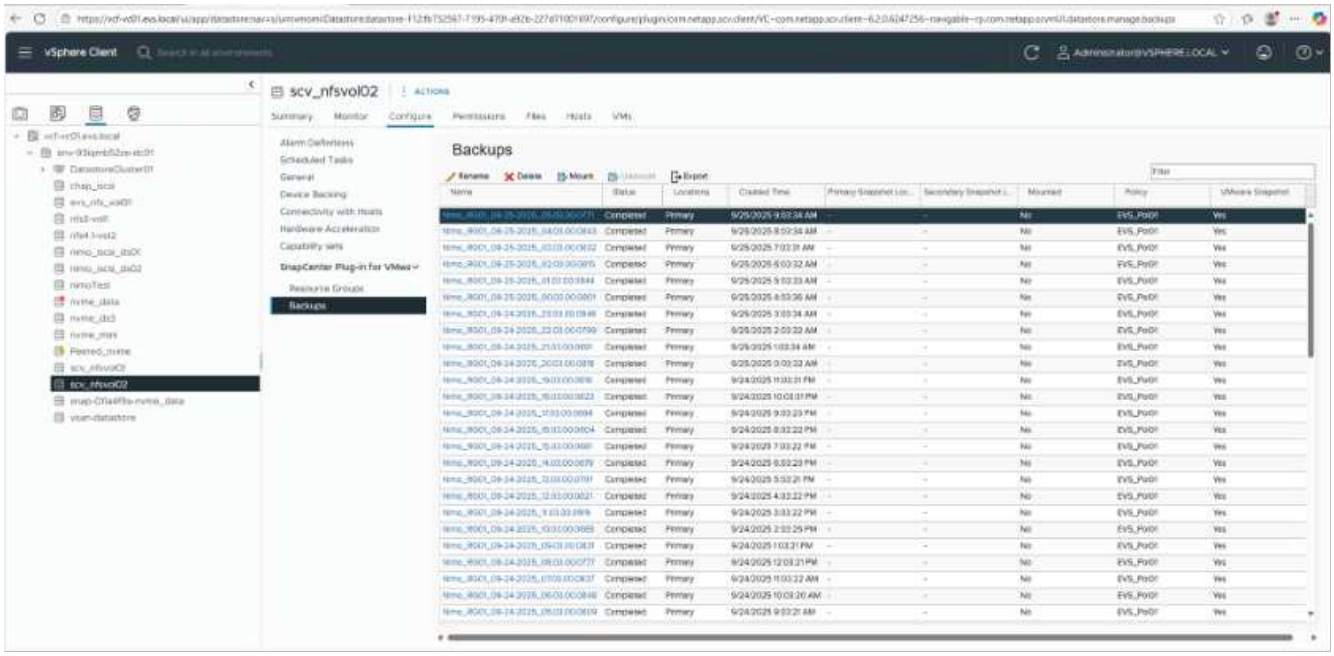
L’opération de restauration peut également être déclenchée au niveau de chaque machine virtuelle.

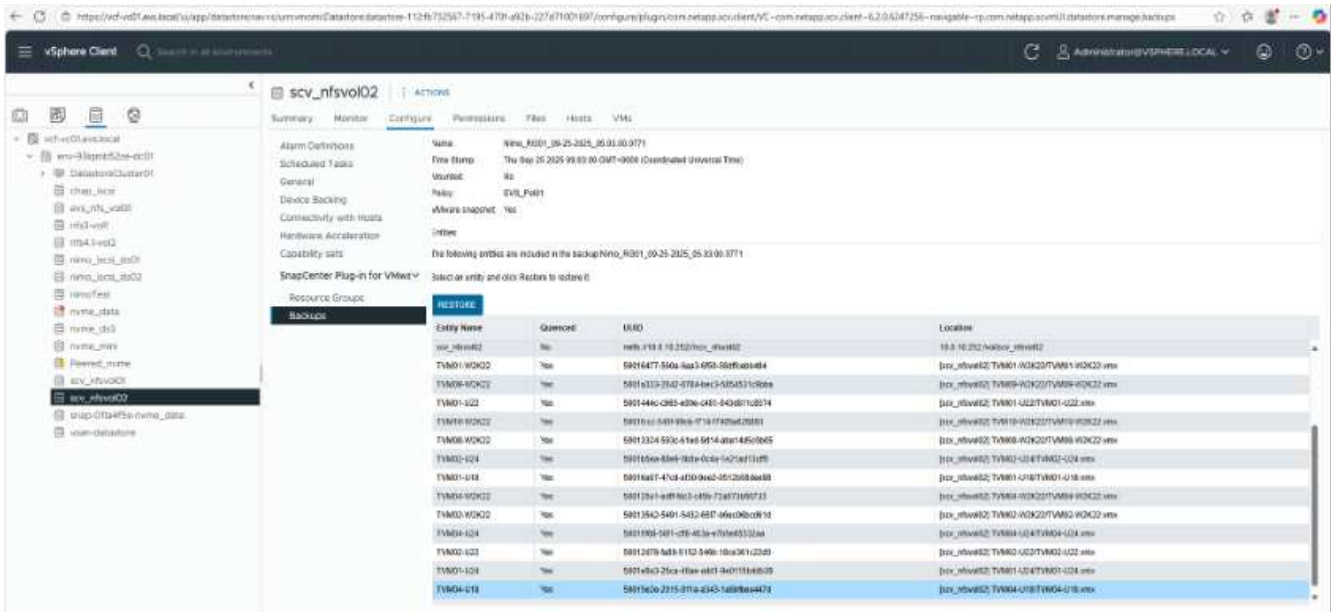
Étapes pour restaurer une machine virtuelle supprimée

Restaurer une machine virtuelle supprimée est un processus simple avec SCV.

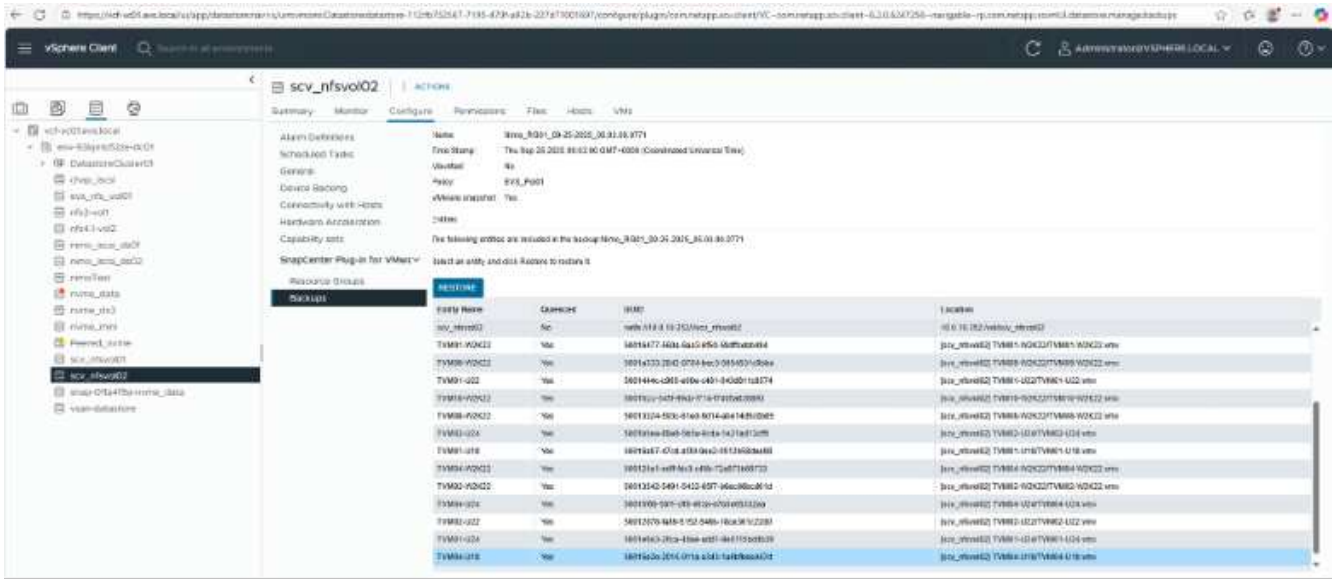
L'opération de restauration d'une machine virtuelle supprimée peut être effectuée au niveau du datastore.

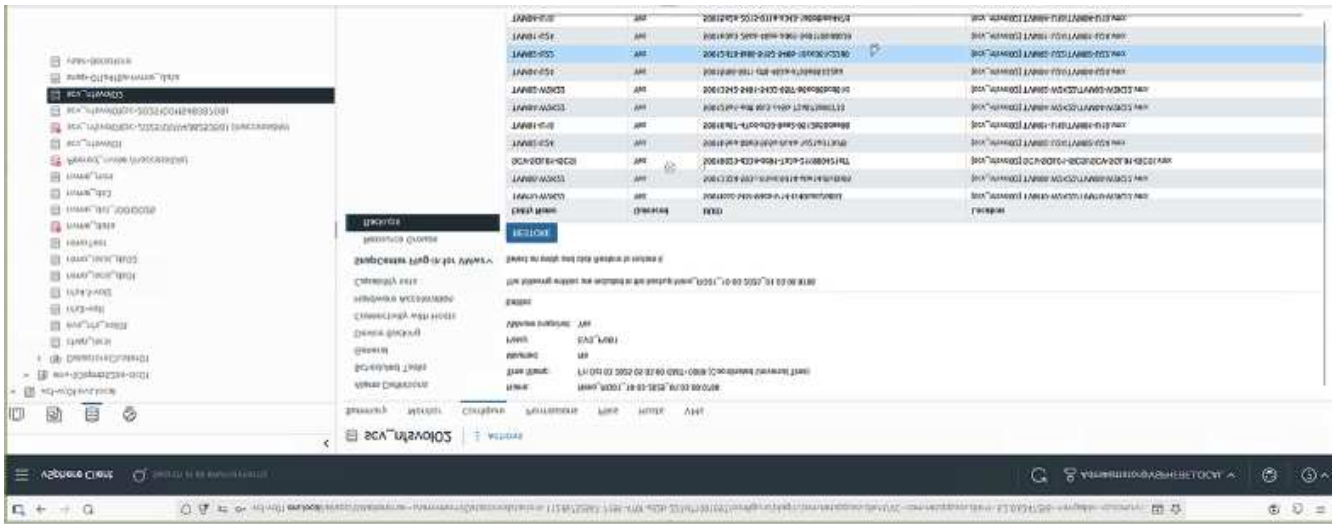
1. Accédez à la banque de données concernée > Configurer > Sauvegardes. Là, sélectionnez la machine virtuelle supprimée et sélectionnez « Restaurer ».

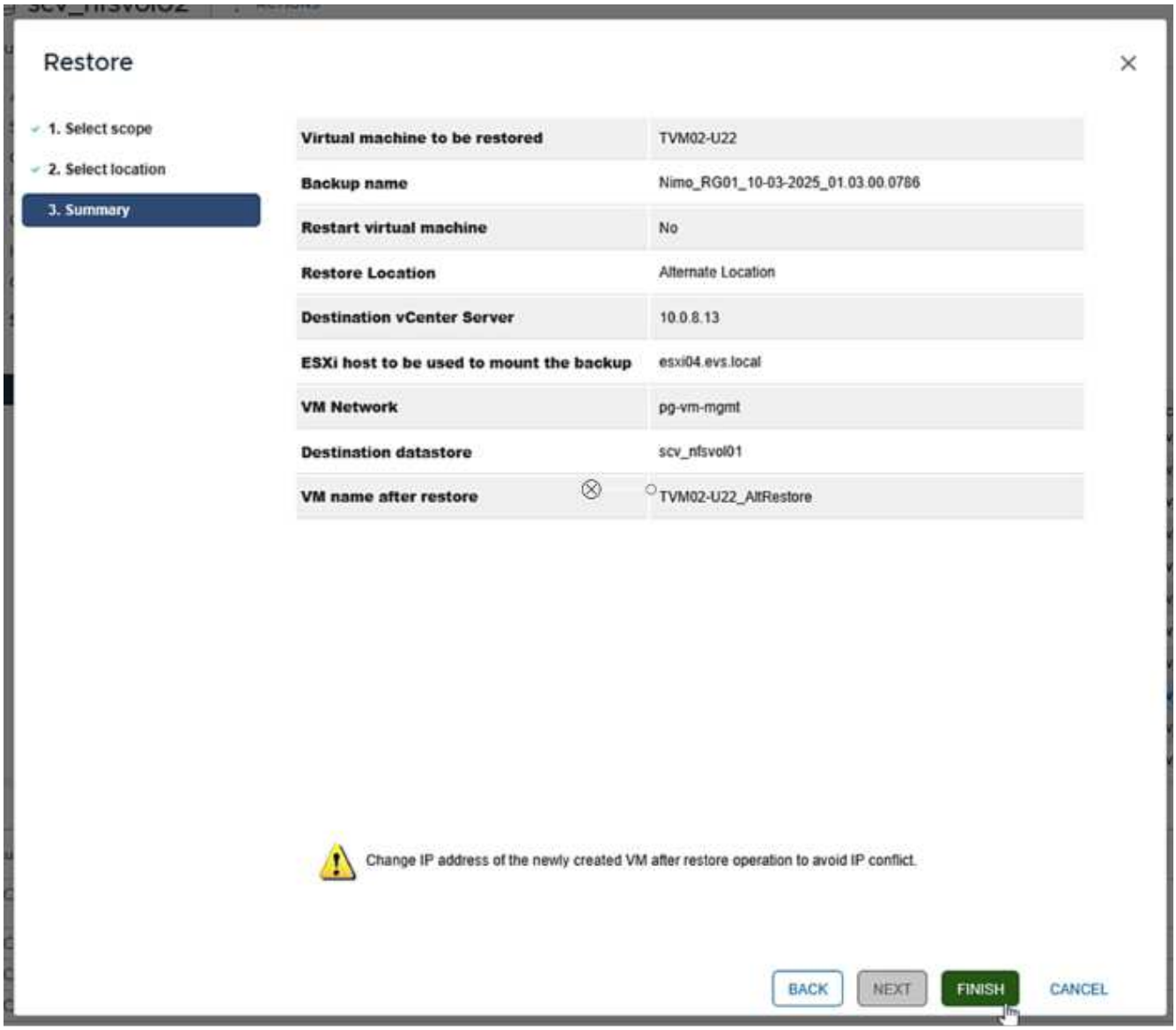


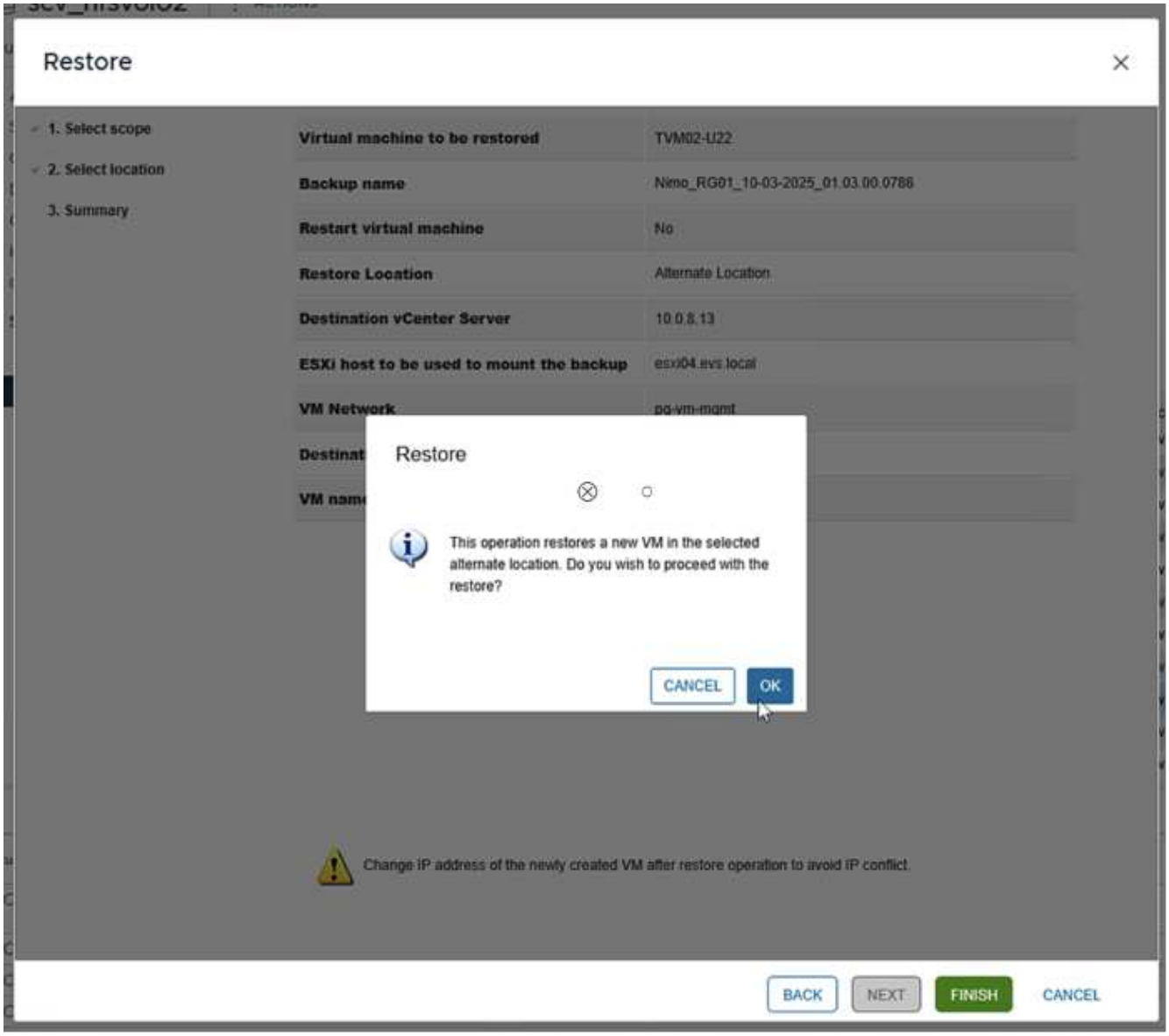


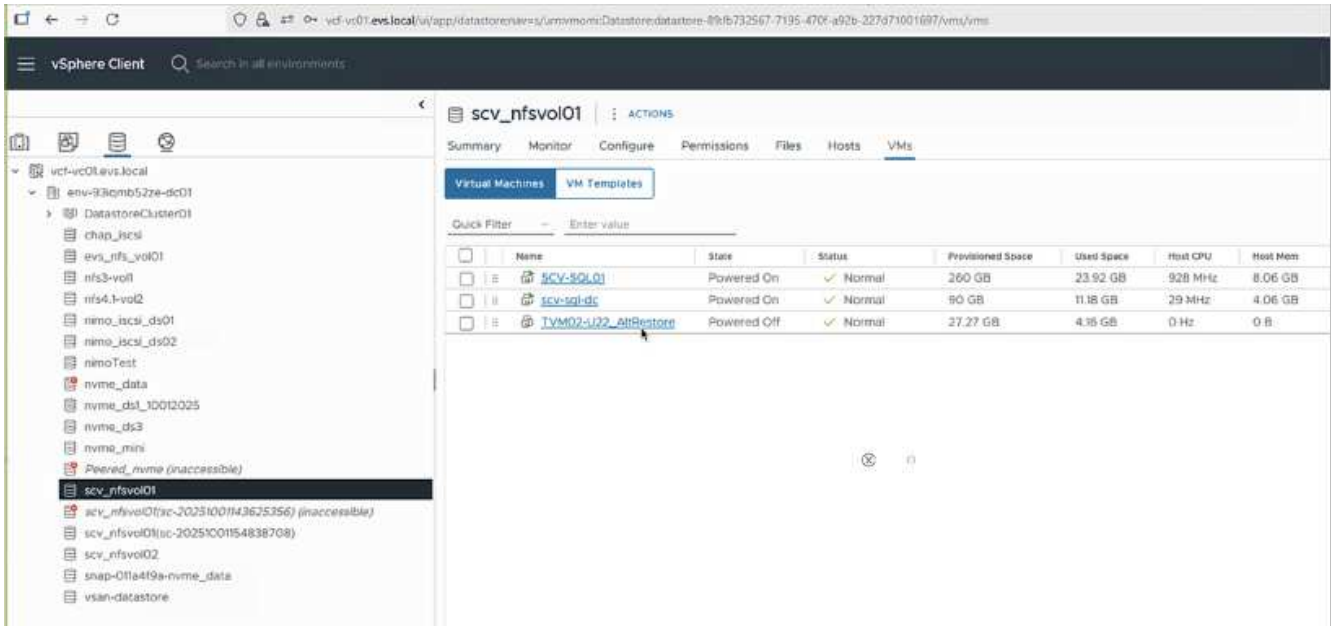
2. La séquence de captures d'écran qui suit illustre la restauration d'une machine virtuelle sur un autre hôte ESXi et un autre datastore.


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE




Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

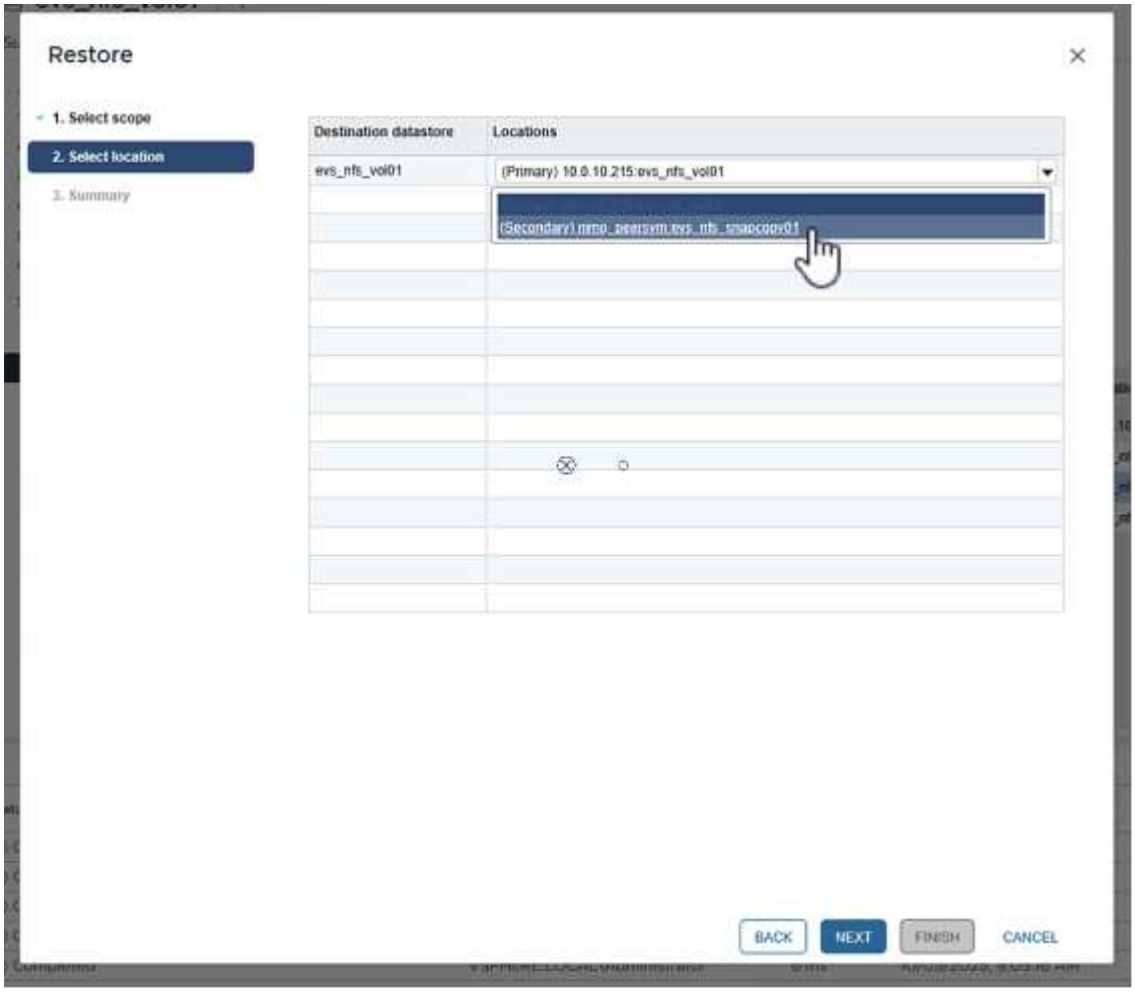

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

Le datastore de destination doit disposer d'un espace libre suffisant et le vCenter spécifié dans le champ « Restore to Alternate Location » doit être résolvable par DNS.

Pour une meilleure efficacité de restauration dans les environnements NFS, activez l'API vStorage pour l'intégration de baies VMware (VAAI).

Les restaurations peuvent également être effectuées à partir de sites secondaires, tels qu'une SnapMirror destination.



+

Procédure de restauration des fichiers et dossiers invités protégés par le SnapCenter Plug-in pour VMware

La section suivante explique comment restaurer les fichiers et dossiers invités à partir de VMDK.

SnapCenter prend en charge la restauration des fichiers et des dossiers à partir de VMDK uniquement lorsque le système d'exploitation invité est Windows.

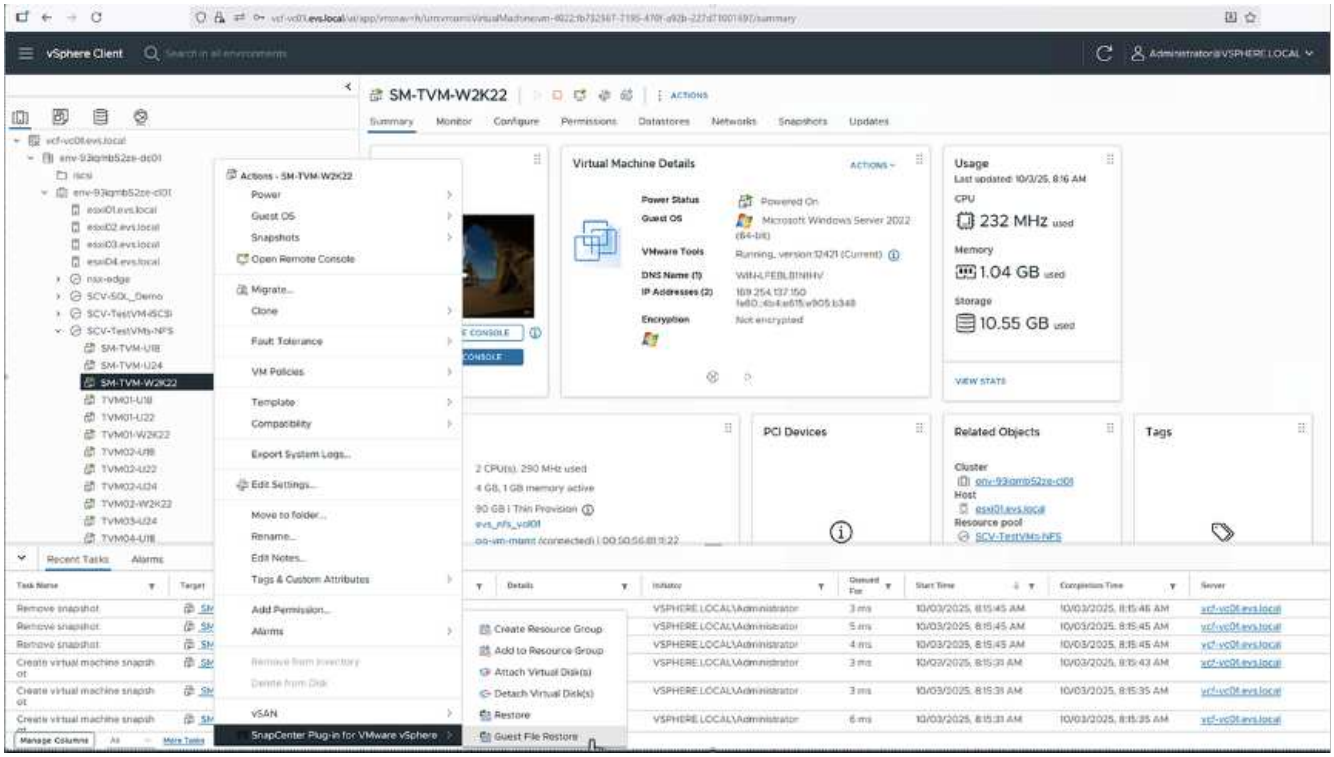
Considérations relatives à la restauration des fichiers et dossiers invités avec SCV :

- Les outils VMware doivent être en cours d'exécution sur la VM.

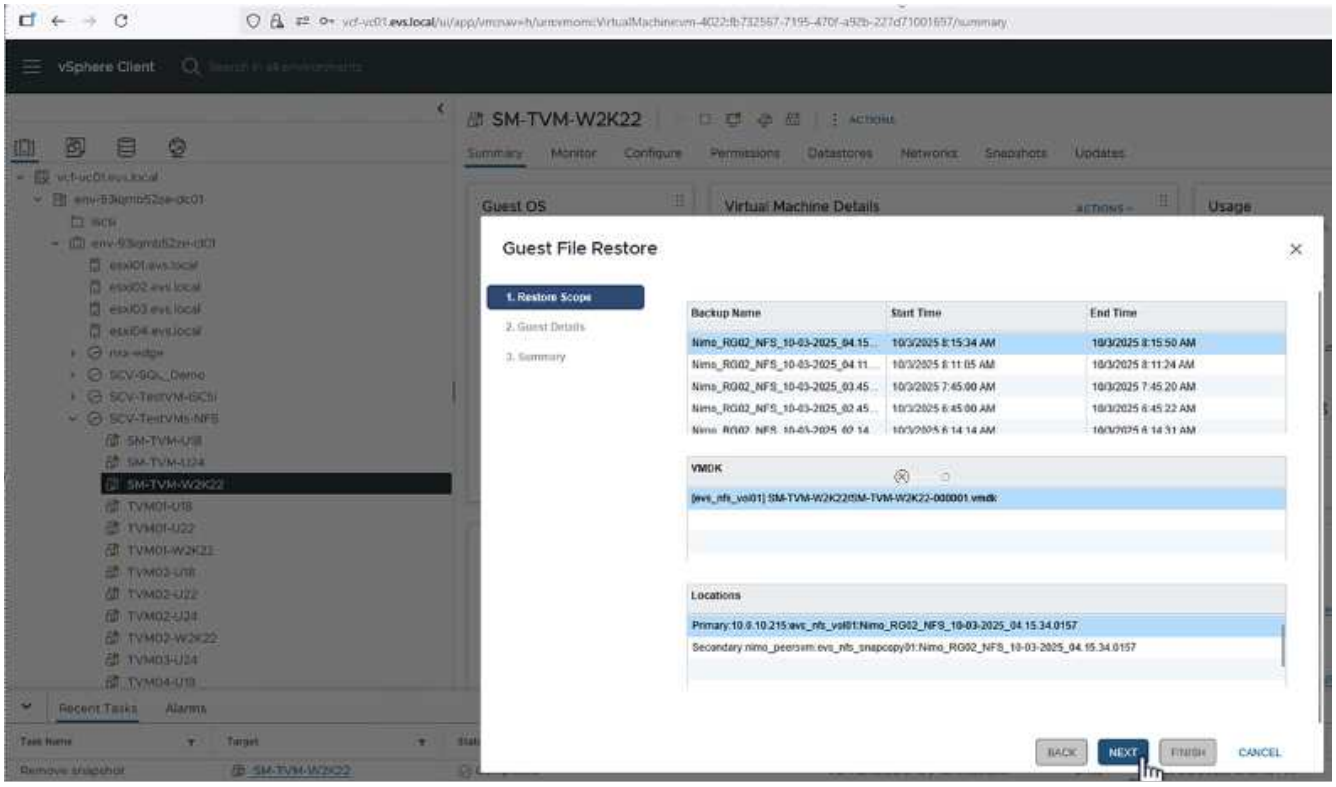
- Le fichier VMDK joint est accessible pendant 24 heures par défaut.
- Une seule opération de restauration ou d'attachement peut être effectuée sur une machine virtuelle à la fois.
- Les fichiers système, cachés et chiffrés peuvent être restaurés ; cependant, leurs attributs d'origine ne seront pas préservés.
- Évitez de restaurer des fichiers chiffrés dans des dossiers chiffrés ou d'écraser des fichiers système.

Étapes pour la restauration des fichiers et dossiers invités :

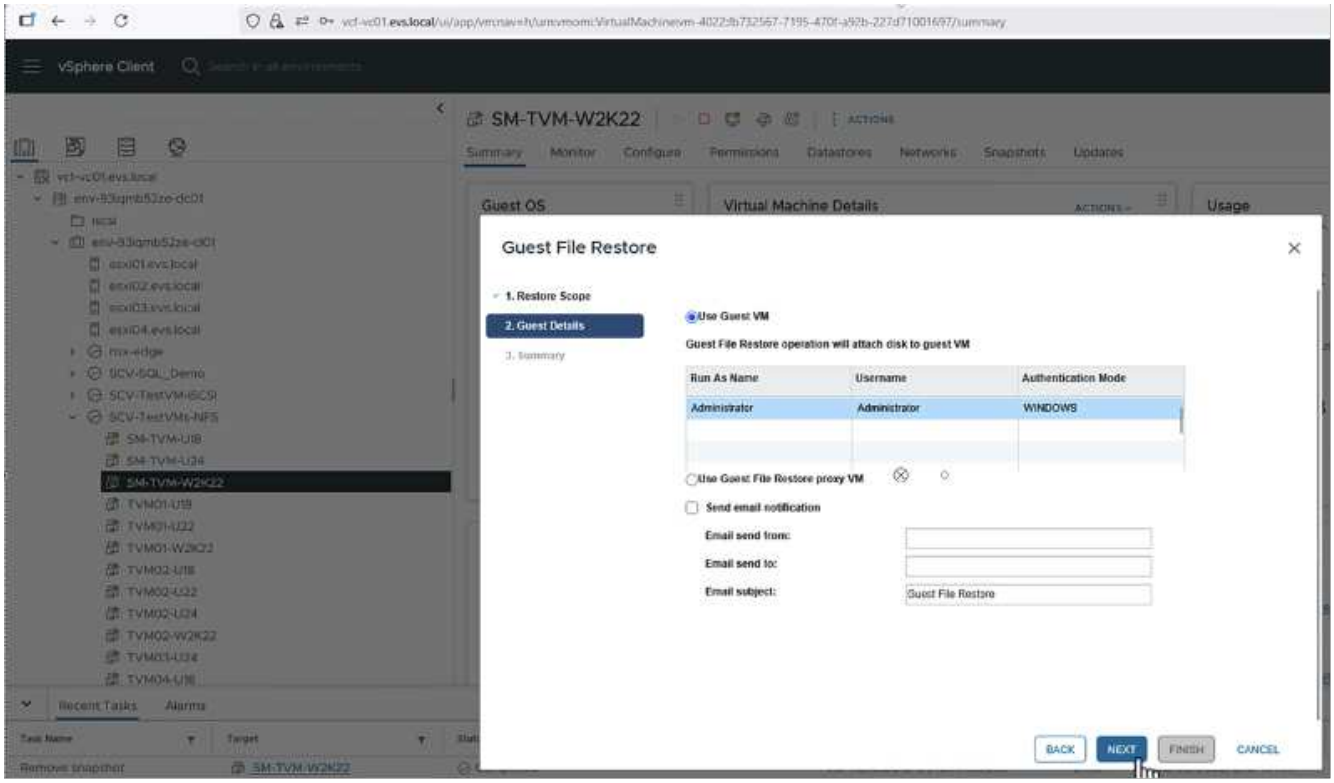
1. Cliquez avec le bouton droit sur la machine virtuelle cible et sélectionnez « NetApp SnapCenter > Restauration des fichiers invités ».



2. Choisissez la sauvegarde contenant le VMDK requis. Spécifiez le VMDK et son emplacement (primaire ou secondaire).



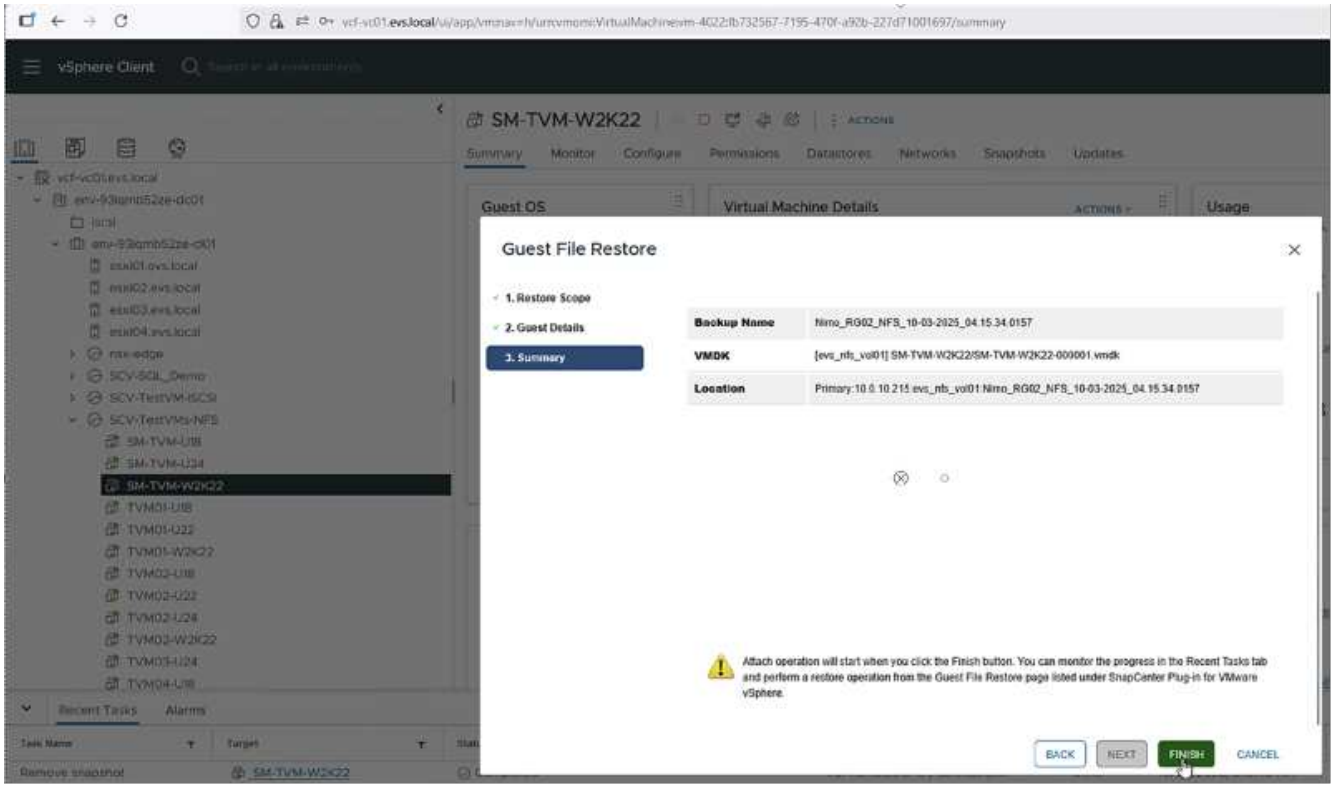
3. Choisissez « Disk Attachment Method ».

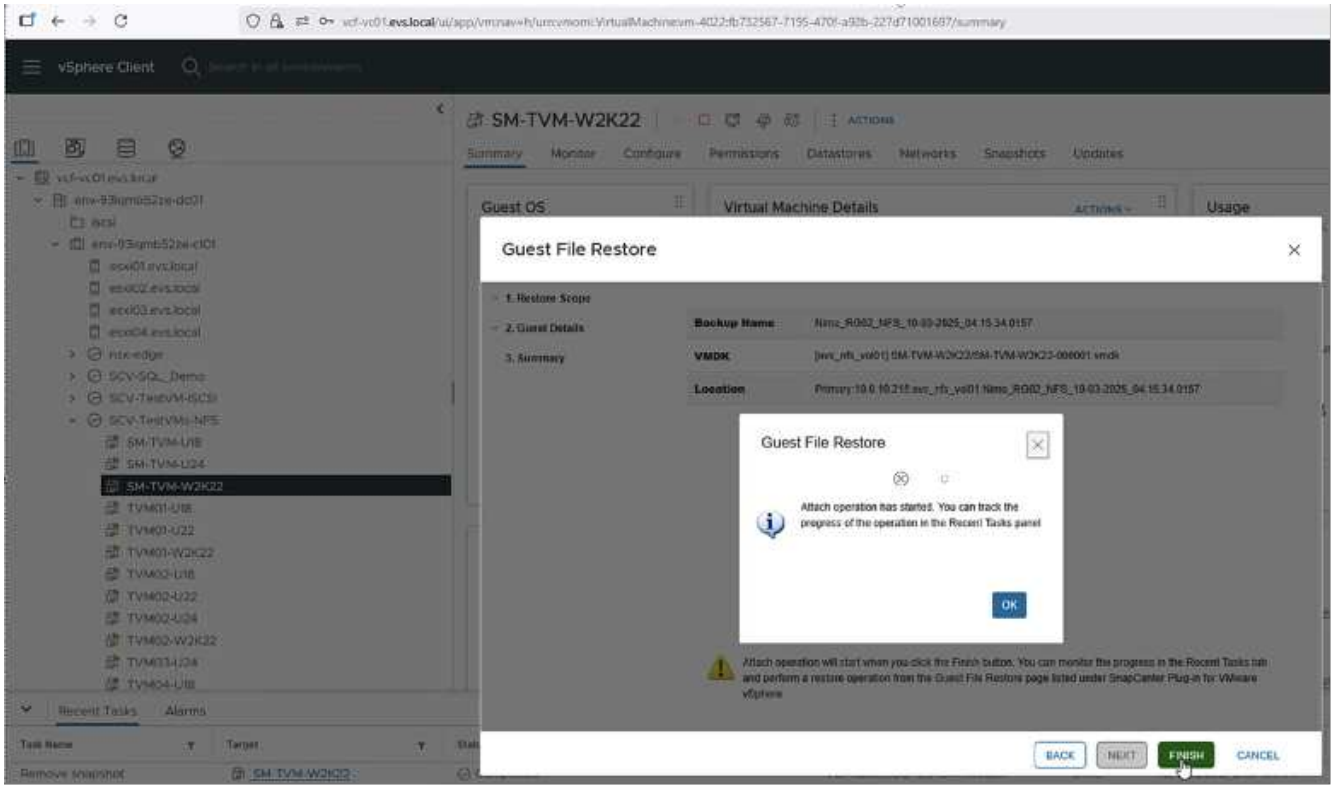


- Option de machine virtuelle invitée : Attachez le disque à la machine virtuelle d'origine (nécessite des informations d'identification préconfigurées). C'est l'option utilisée dans cette démonstration.
- Option Proxy VM : Attachez le disque à une Proxy VM désignée (doit être configurée au préalable).

4. Veuillez patienter jusqu'à la fin de l'opération de rattachement avant de parcourir et de restaurer les

fichiers. Une fois l'opération terminée, SnapCenter crée automatiquement une session de restauration de fichiers invité.





5. Accédez au VMDK dans la session de restauration de fichiers invités, sélectionnez les fichiers ou dossiers requis et restaurez-les à l'emplacement spécifié.

Procédures de protection pour les bases de données exécutées sur des VMDK VMware avec SnapCenter pour SQL (SCSQL)

La section suivante explique comment protéger les bases de données exécutées sur des VMDK VMware avec SnapCenter pour SQL (SCSQL).

Configuration de SCSQL

La configuration requise pour utiliser SCSQL afin de protéger les bases de données sur les VMDK est la suivante :

1. "Installer et configurer" Serveur SnapCenter.
2. Connectez-vous à SnapCenter.
3. Configurez l'environnement SnapCenter :
   - "Ajouter ou affecter" Connexions du système de stockage.
   - "Créer" informations d'identification.
4. Pour les bases de données Microsoft SQL Server sur les VMDK VMware :
   - "Déployer SCV" (déjà abordé dans la section configuration).
   - Enregistrez le plug-in avec SnapCenter.
5. Ajouter "Hôtes SQL server et installation des plug-ins" :
   - "Configurer les plug-ins SQL".
   - "Configurez le plan de protection et les horaires pour la base de données et les journaux".

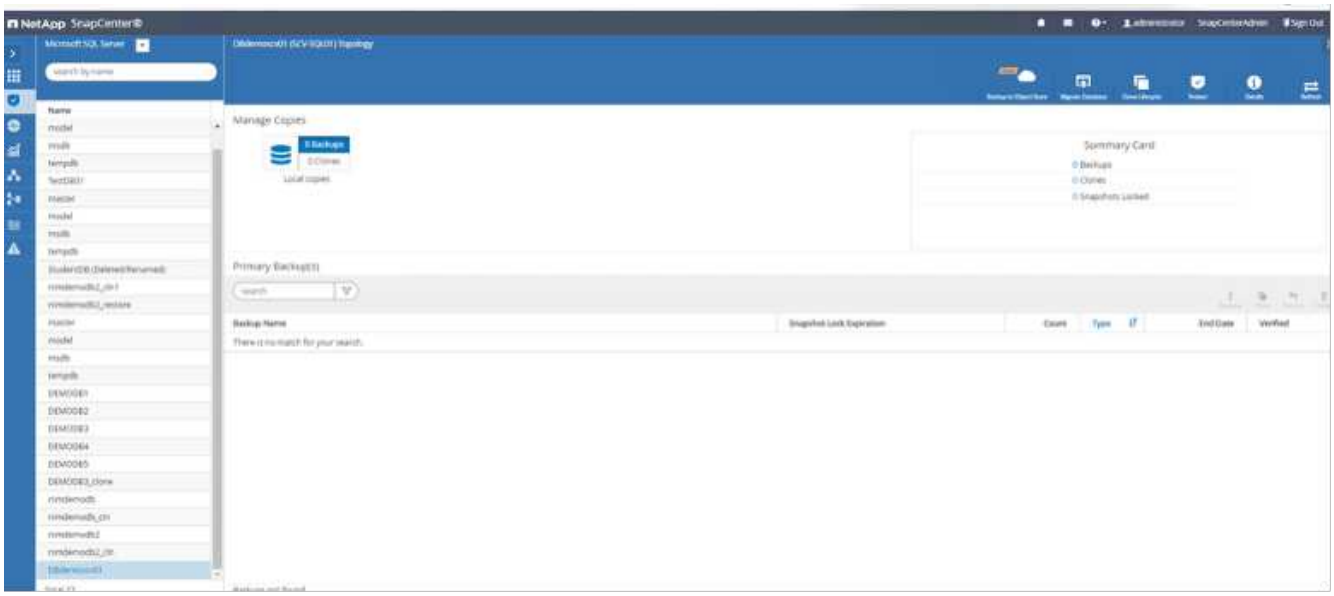


Mise en place d'une règle de sauvegarde

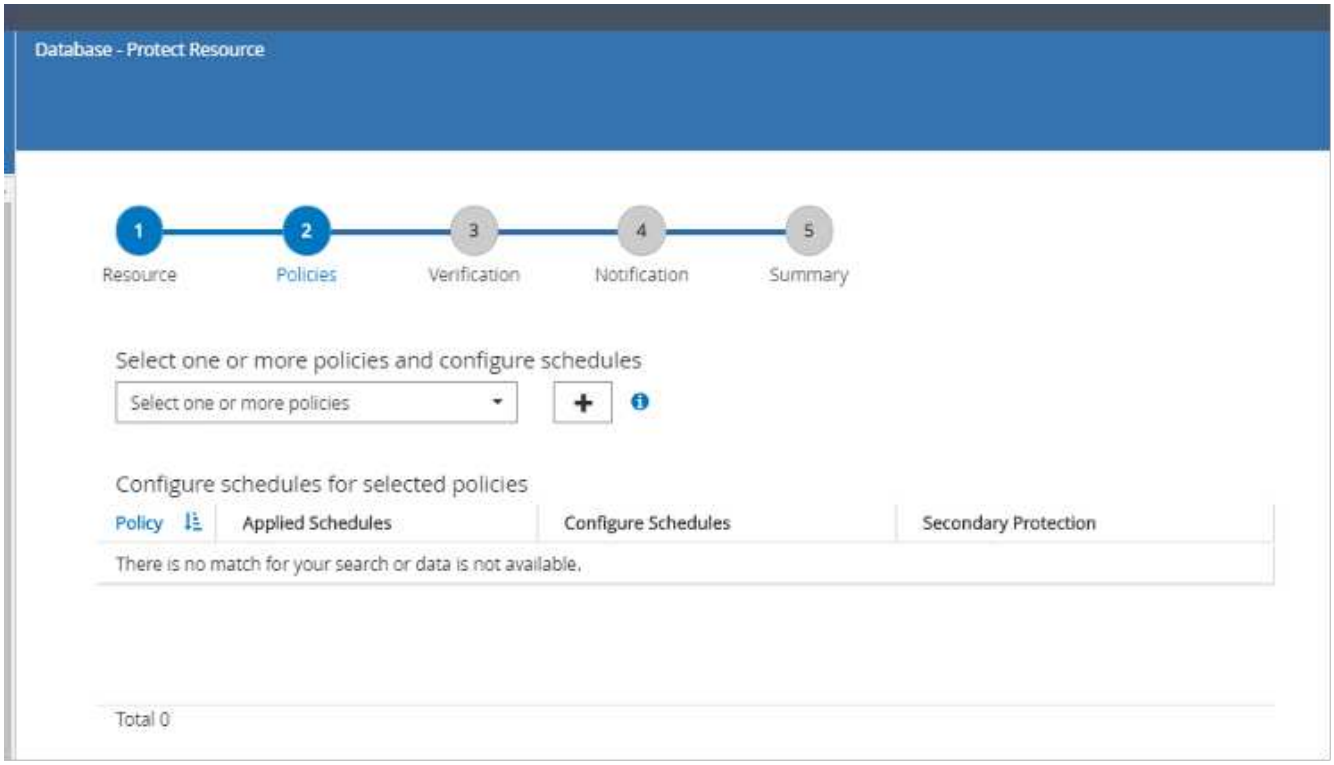
Les étapes suivantes vous montreront comment configurer une règle de sauvegarde.

1. Sélectionnez la base de données dans l'onglet Ressources et sélectionnez "Protéger" dans le coin supérieur droit.

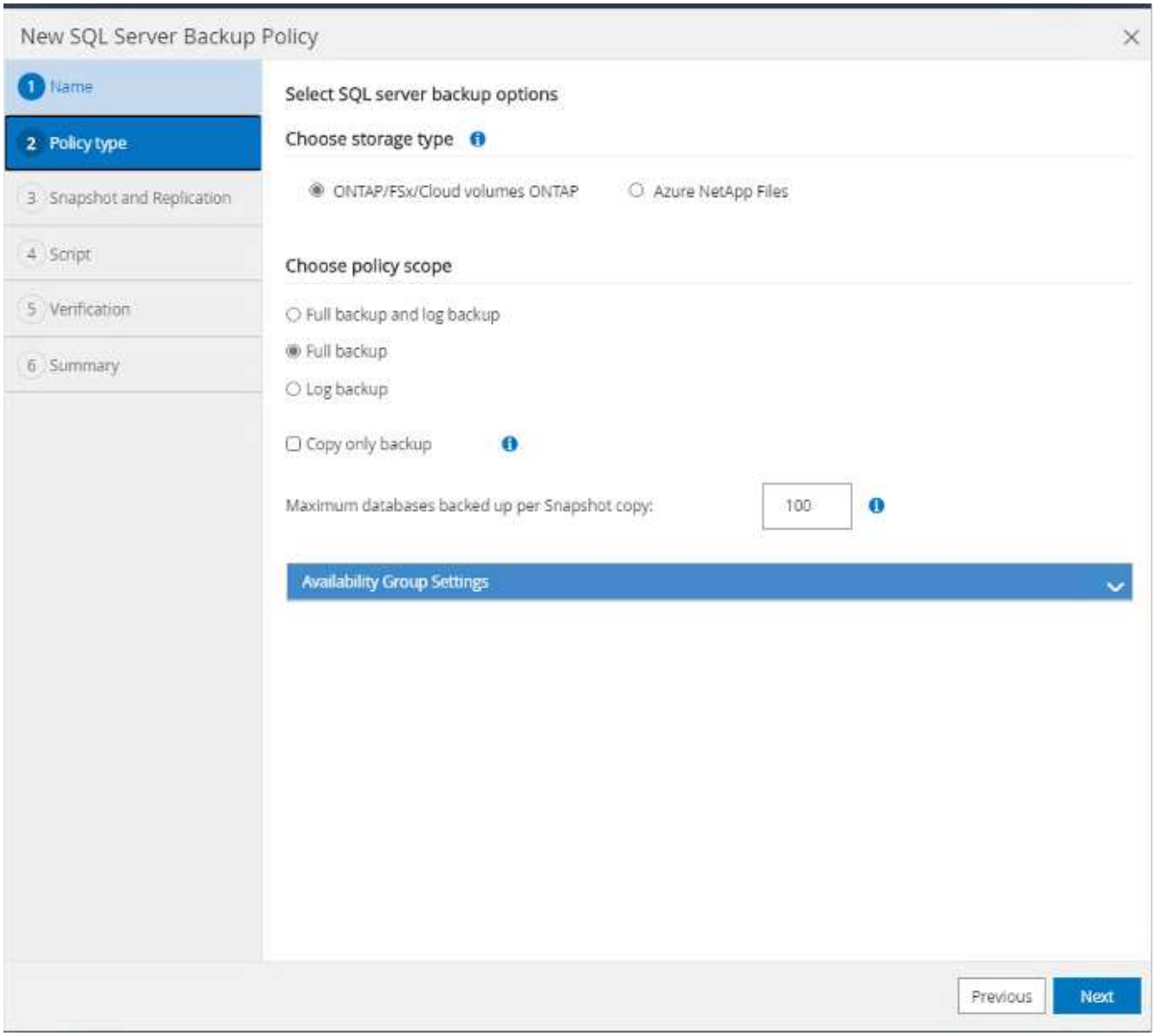
> Les validations sont effectuées sur une base de données SQL Server exécutée sur la machine virtuelle invitée.



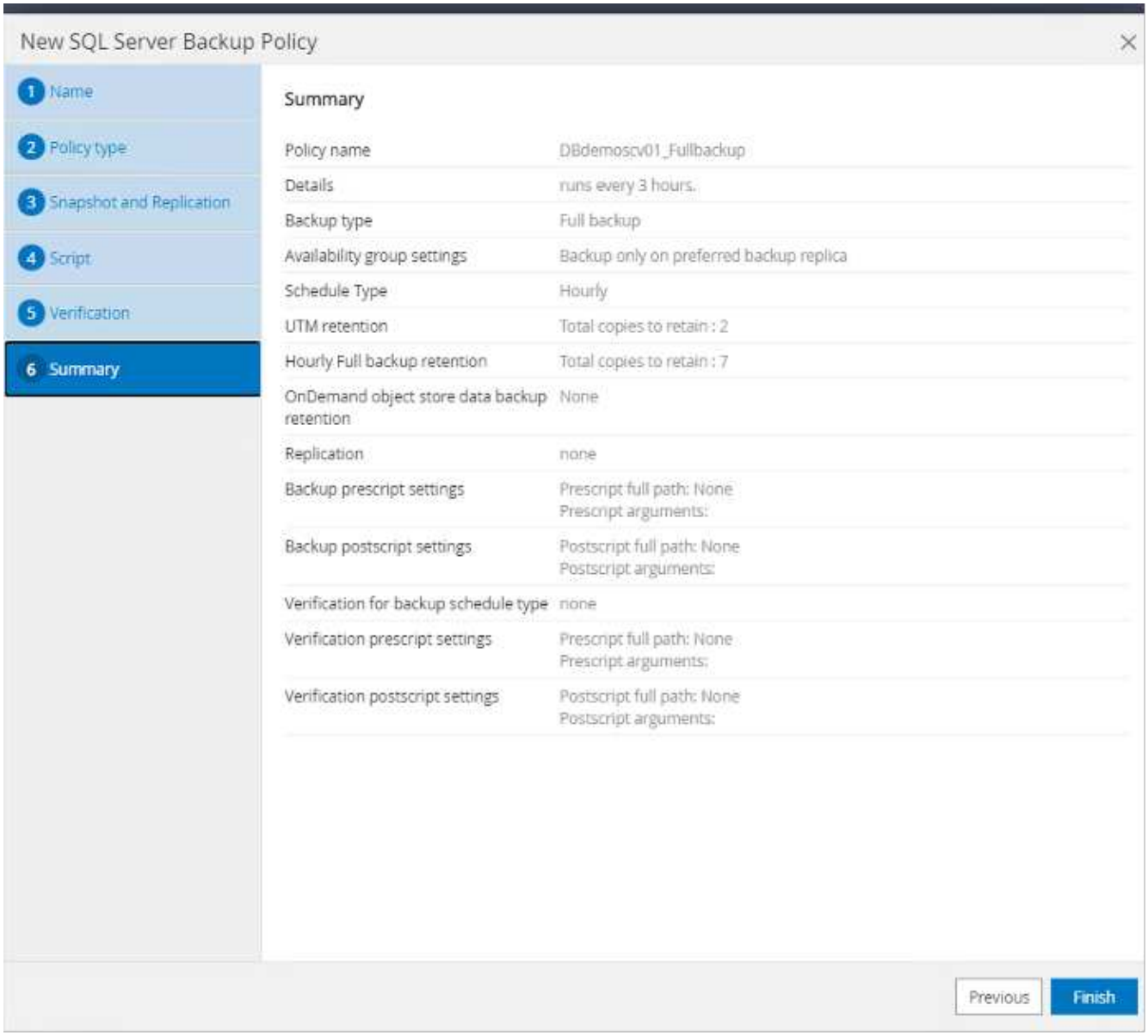
2. Cliquez sur l'icône du signe plus pour configurer une règle de sauvegarde SQL Server.



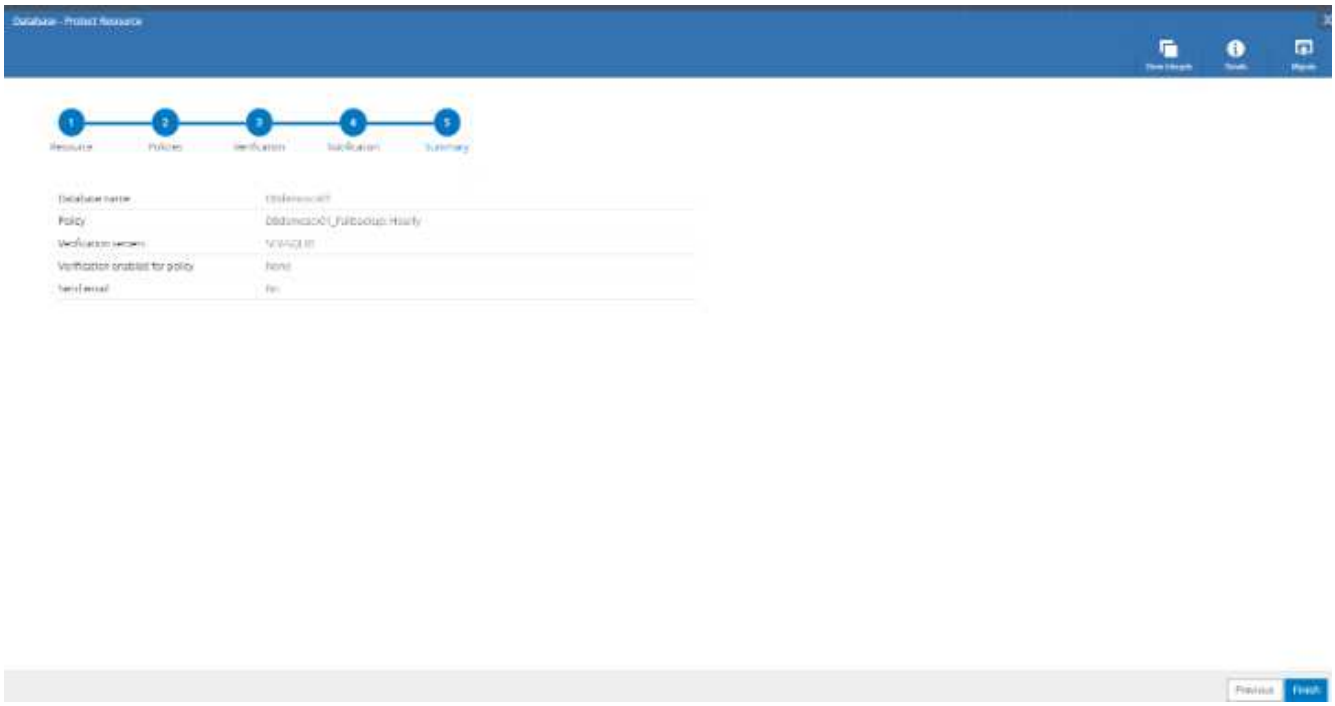
3. Dans cette démonstration, l'option « Sauvegarde complète » est sélectionnée. Sélectionnez « Suivant » pour continuer.



4. Sur la page Résumé, sélectionnez "Terminer".



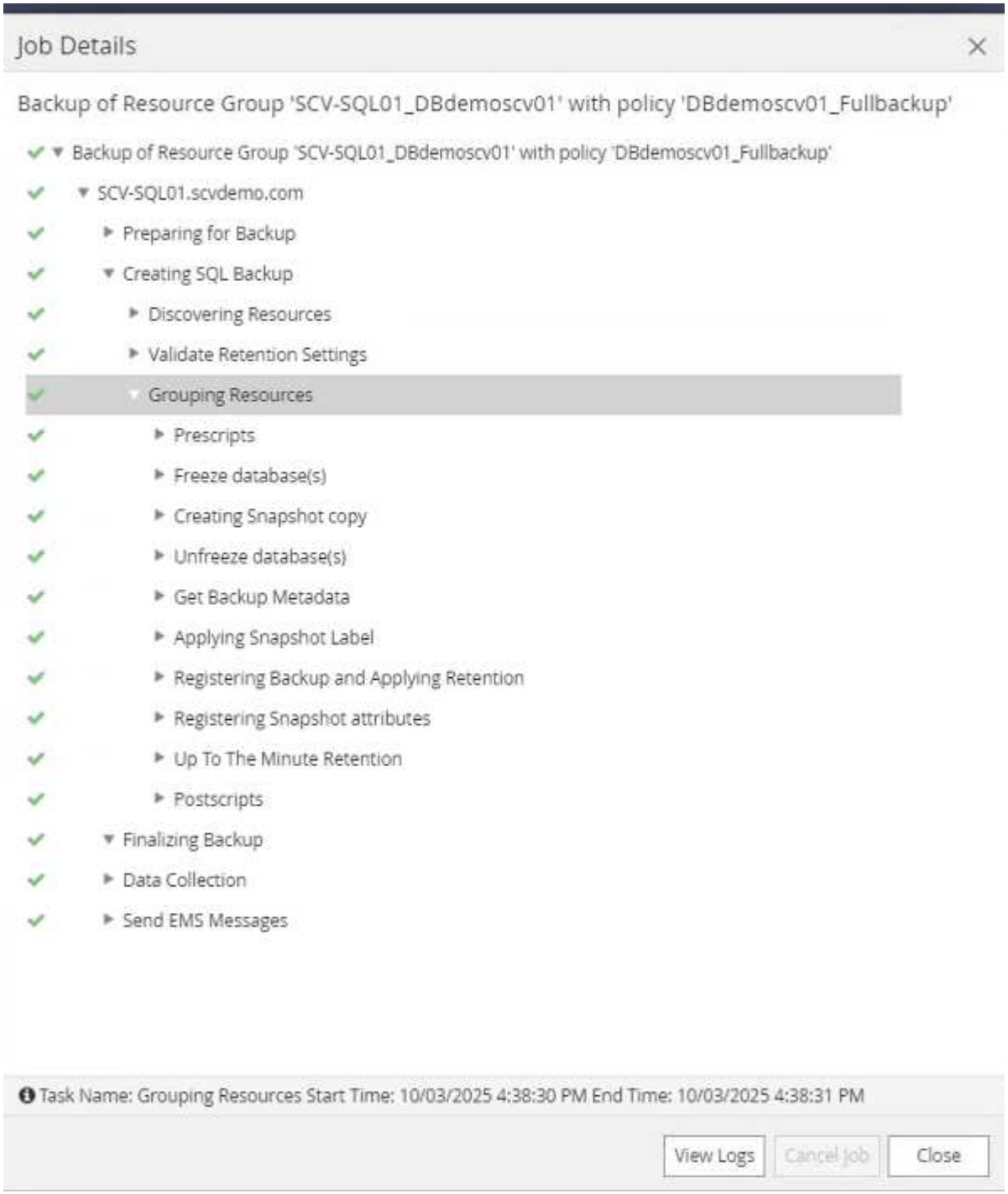
5. Passez à « Finish ».



Surveillance d’une sauvegarde

Une fois que vous avez défini une règles de sauvegarde, vous pouvez surveiller vos opérations de sauvegarde au fur et à mesure qu’elles ont lieu. Vous pouvez le faire soit en cliquant sur Backup now pour déclencher une opération de sauvegarde à la demande, soit en attendant que votre règles de sauvegarde planifiée s’exécute.

1. Surveillez la progression du travail à l’aide de « Monitor > Jobs ».
2. Sélectionnez la tâche de sauvegarde, puis cliquez sur "Détails" pour afficher les détails de la tâche comme ci-dessous.

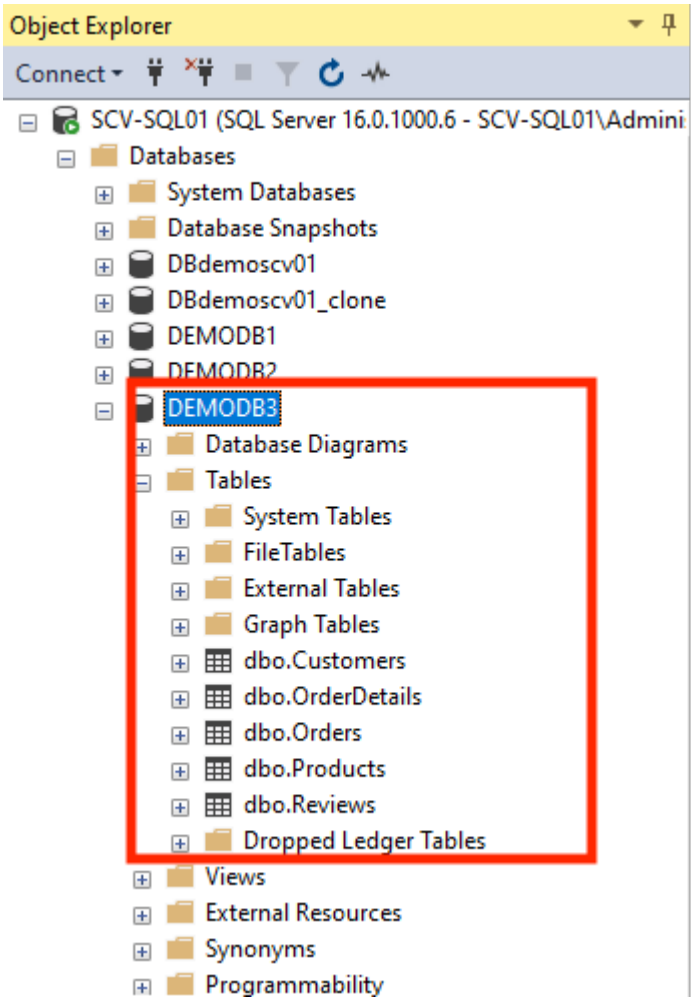


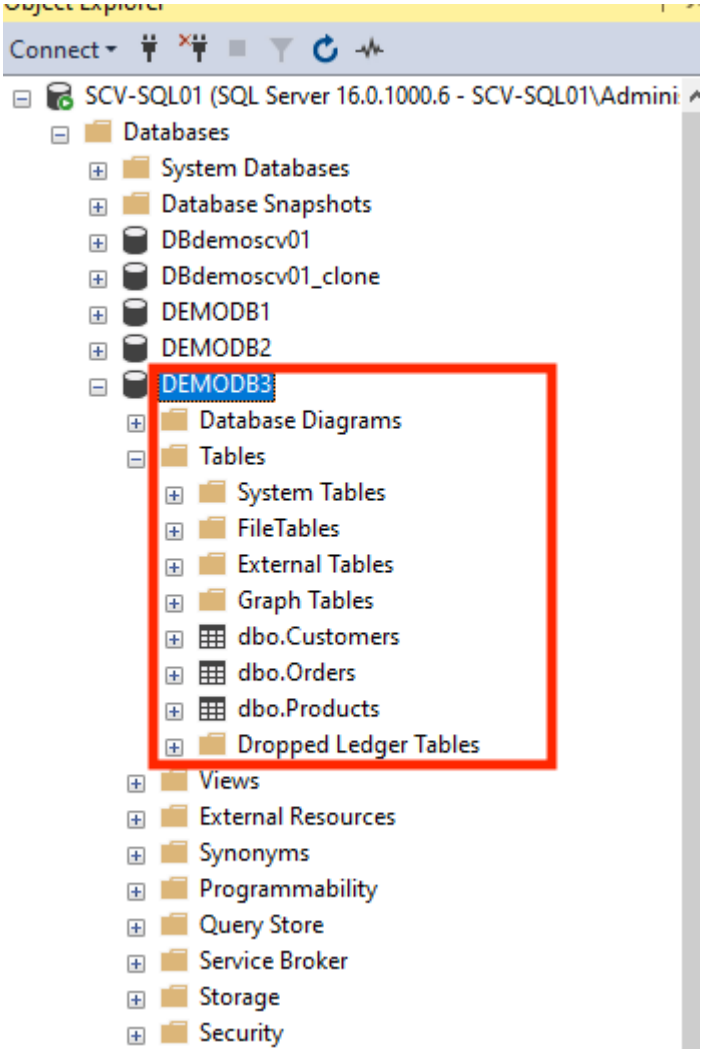
Restauration des bases de données résidant sur les VMDKs

La base de données sur le VMDK peut être restaurée à un point spécifique dans le temps.

Nous pouvons simuler l'importance de ceci en supprimant certaines tables de votre base de données, qui seront ensuite corrigées par une restauration à un instant précis.

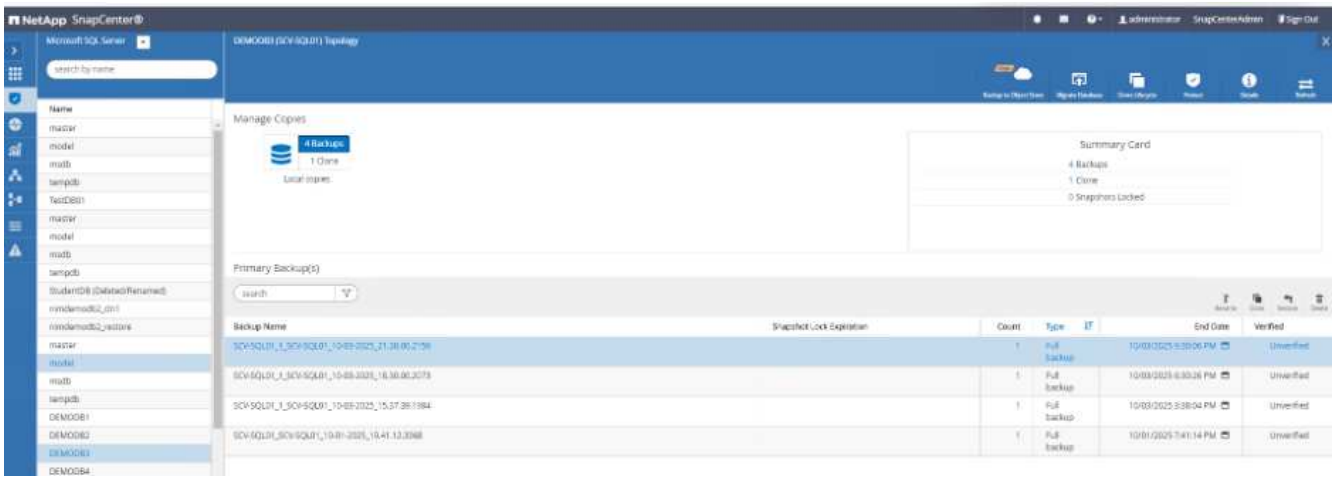
Vous pouvez constater ci-dessous que plusieurs tables de notre base de données affichées dans la première capture d'écran ont été supprimées dans la seconde capture d'écran :


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

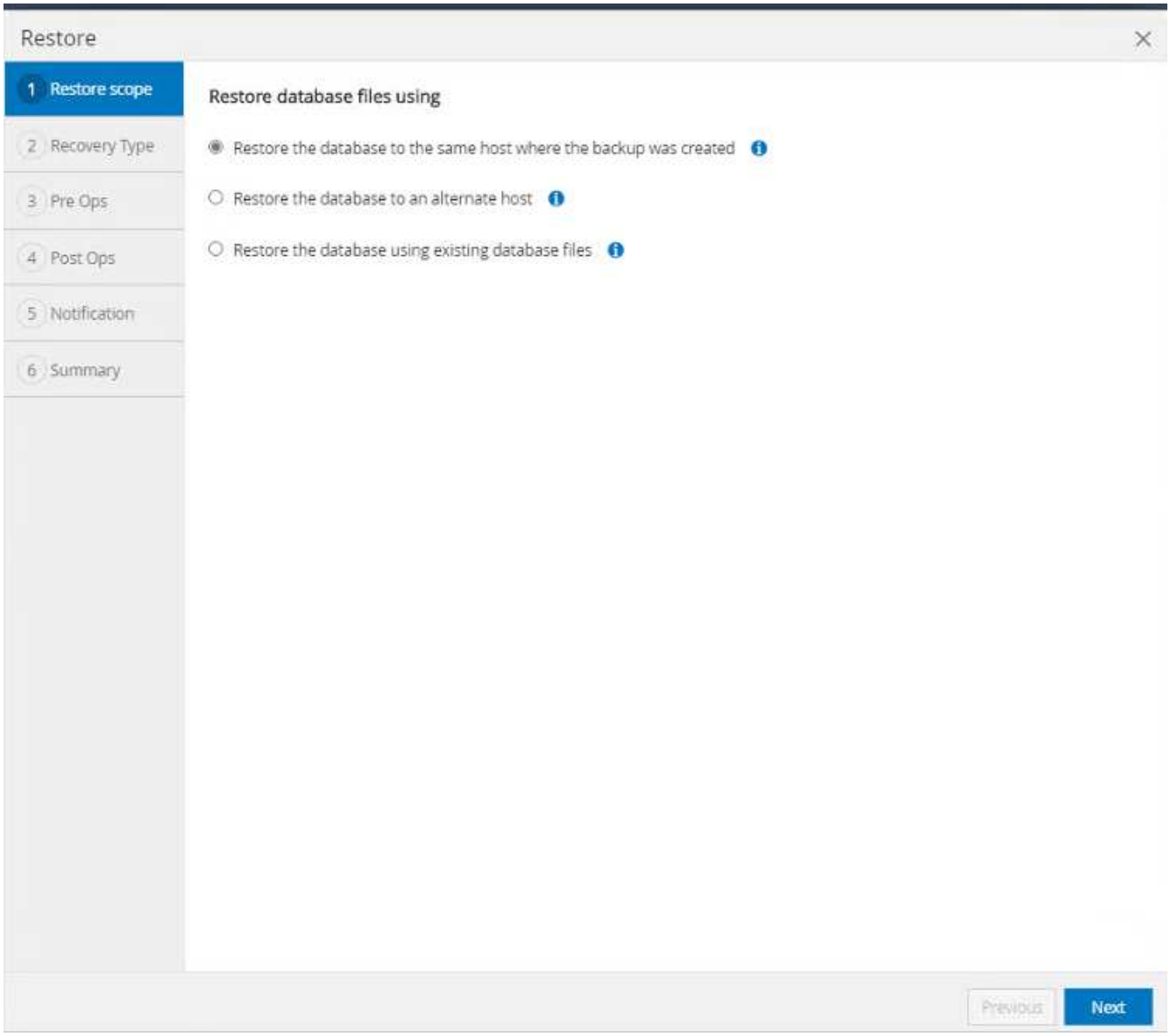


Les étapes suivantes montrent comment effectuer une restauration pour récupérer les tables supprimées :

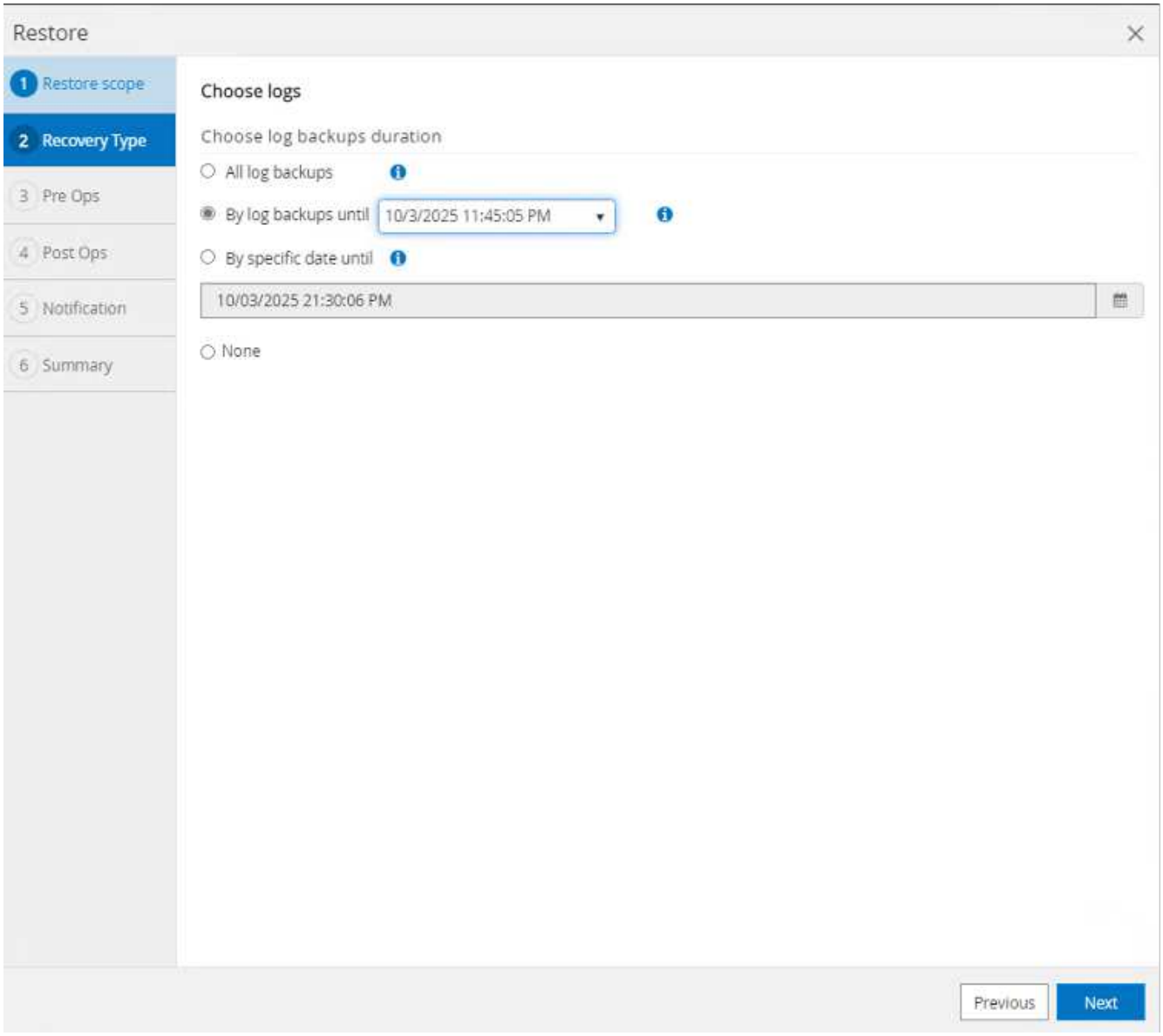
1. Sélectionnez la base de données dans le groupe de ressources.



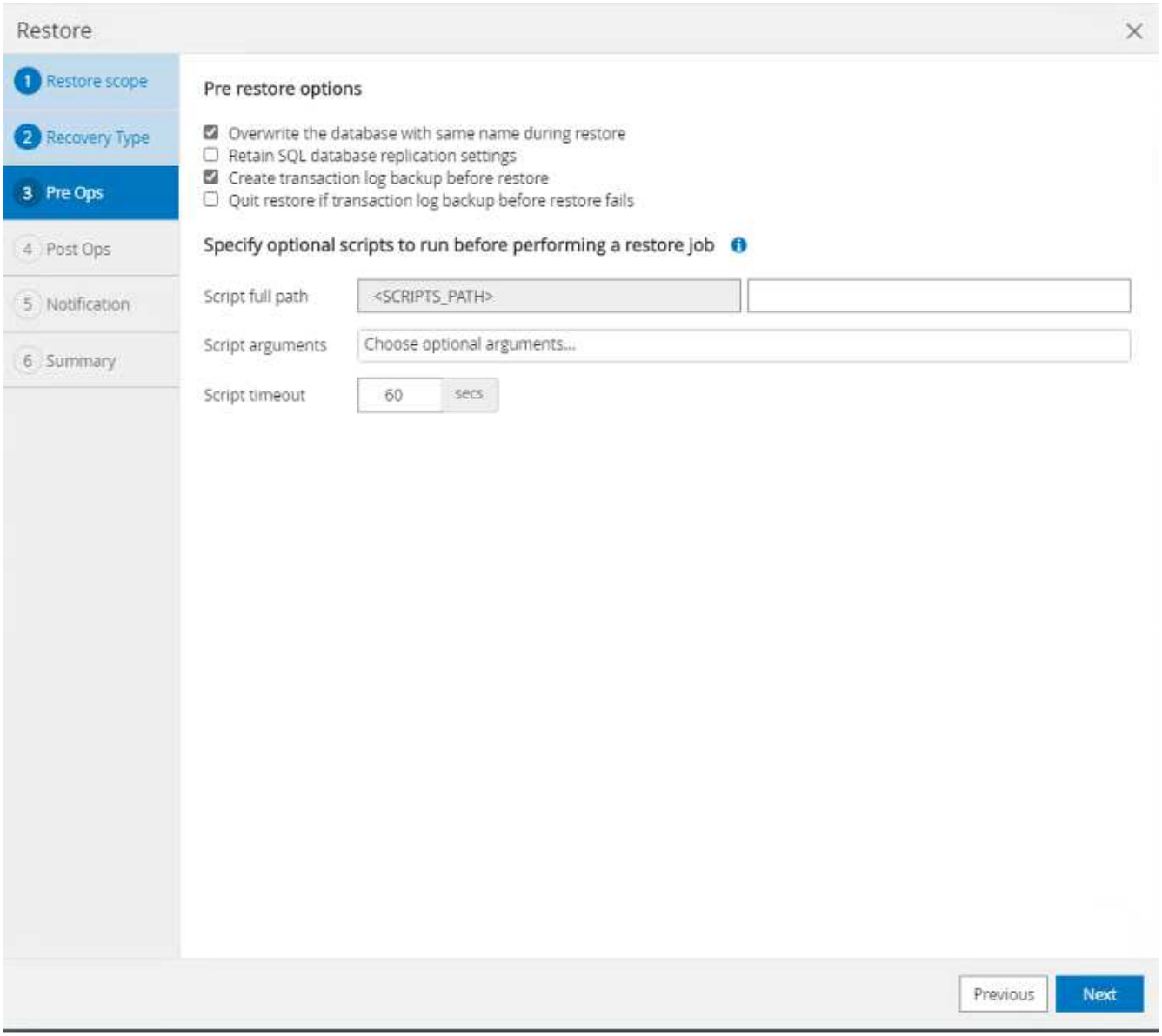
2. Sur la page Restaurer, sélectionnez l'option "Restaurer la base de données sur le même hôte où la sauvegarde a été créée".



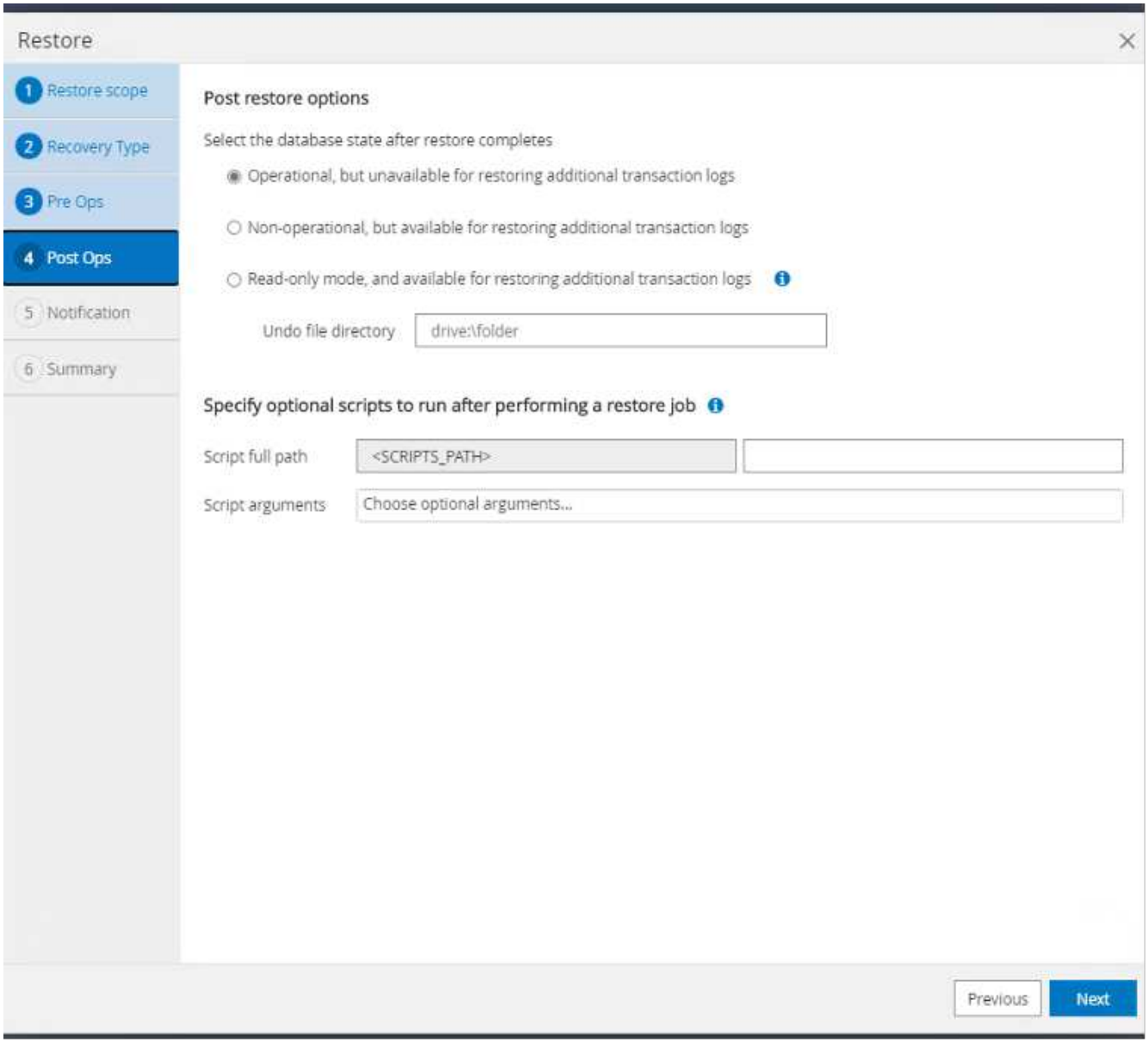
3. Sélectionnez l’option pour utiliser une sauvegarde du journal jusqu’à un point dans le temps.



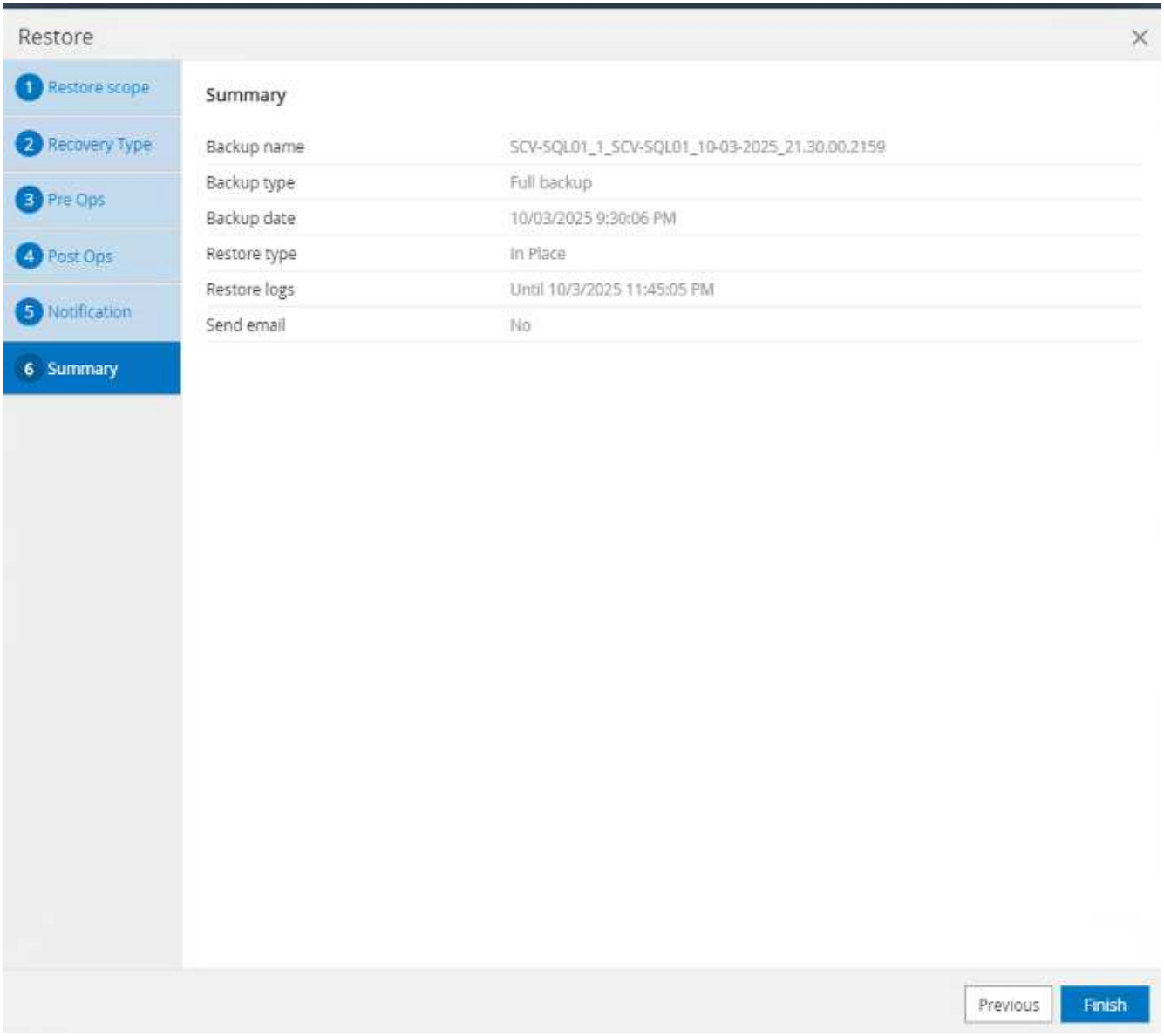
4. Sélectionnez « Overwrite database with same name during restore, Create transaction log backup before restore », puis sélectionnez « Next ».



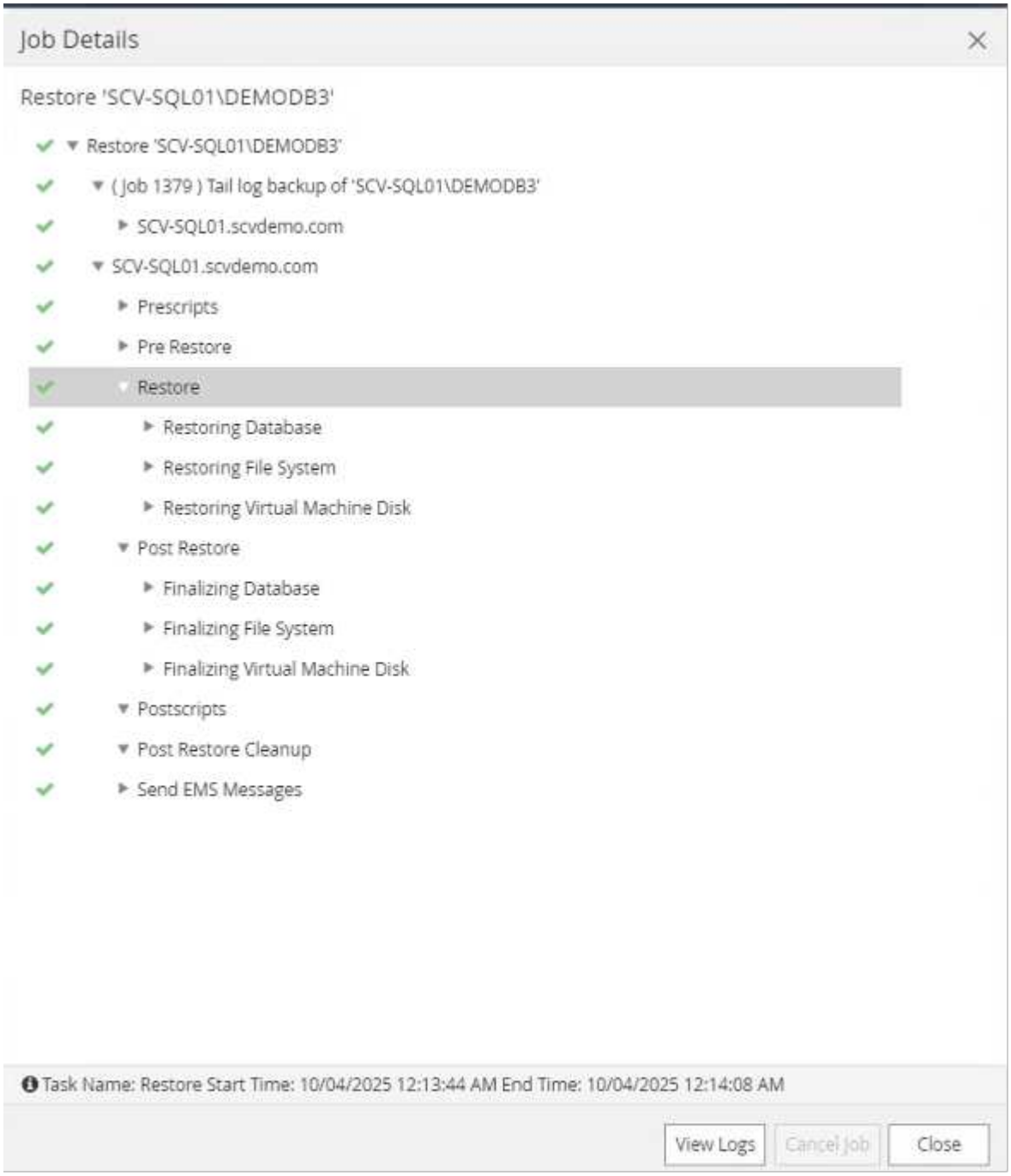
5. Sélectionnez l'état post-restauration que vous souhaitez que la base de données adopte dans les options de la liste, puis sélectionnez « Suivant ».



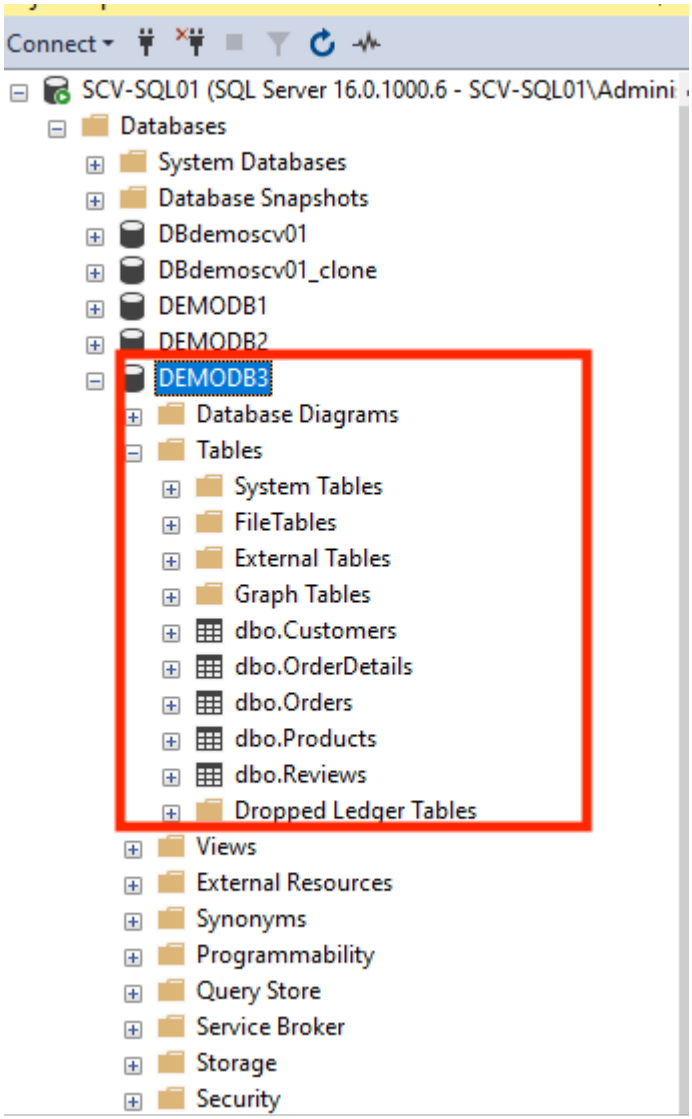
6. Sur la page récapitulative, sélectionnez "Terminer".



7. Surveillez le job jusqu'à son achèvement.



8. Vérifiez que les tables supprimées ont bien été restaurées.



Conclusion

Dans ce document, nous avons fourni des instructions détaillées étape par étape sur le déploiement, la configuration et l'utilisation de SCV et "SnapCenter Plug-in for SQL Server (SCSQL)" tout en utilisant FSx for ONTAP comme datastore supplémentaire avec les clusters Amazon EVS.

Conclusion

En résumé, lors de l'utilisation de FSx for ONTAP pour optimiser le TCO d'un déploiement Amazon EVS, SCV offre une méthode simple et efficace pour sauvegarder les machines virtuelles. Il peut sauvegarder et restaurer les machines virtuelles de manière transparente et rapide puisqu'il s'appuie sur des copies Snapshot, qui ne prennent littéralement que quelques secondes à s'exécuter.

"Essayez le plug-in SnapCenter pour VMware dès maintenant gratuitement".

NetApp pour Azure / AVS

Fonctionnalités NetApp pour Azure AVS

Découvrez-en plus sur les fonctionnalités que NetApp apporte à la solution Azure VMware (AVS) : de NetApp en tant que périphérique de stockage connecté en tant qu'invité ou banque de données NFS supplémentaire à la migration des flux de travail, à l'extension/à l'éclatement vers le cloud, à la sauvegarde/restauration et à la reprise après sinistre.

Accédez à la section du contenu souhaité en sélectionnant parmi les options suivantes :

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

Configuration d'AVS dans Azure

Comme pour les environnements locaux, la planification d'un environnement de virtualisation basé sur le cloud est essentielle pour un environnement prêt pour la production et la création de machines virtuelles et la migration.

Cette section décrit comment configurer et gérer Azure VMware Solution et l'utiliser en combinaison avec les options disponibles pour la connexion au stockage NetApp .

> Le stockage en invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP à Azure VMware Solution.

Le processus de configuration peut être décomposé selon les étapes suivantes :

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

Voir le détail"étapes de configuration pour AVS" .

Options de stockage NetApp pour AVS

Le stockage NetApp peut être utilisé de plusieurs manières, soit en tant que stockage de données connecté, soit en tant que banque de données NFS supplémentaire, dans Azure AVS.

S'il vous plaît visitez"Options de stockage NetApp prises en charge" pour plus d'informations.

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

- Azure NetApp Files (ANF) en tant que stockage connecté invité
- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- Azure NetApp Files (ANF) comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour AVS" . Voir le détail"options de banque de données NFS supplémentaires pour AVS" .

Cas d'utilisation de solutions

Avec les solutions cloud NetApp et VMware, de nombreux cas d'utilisation sont simples à déployer dans Azure AVS. Ces cas sont définis pour chacune des zones cloud définies par VMware :

- Protéger (comprend à la fois la reprise après sinistre et la sauvegarde/restauration)
- Étendre
- Émigrer

"Parcourez les solutions NetApp pour Azure AVS"

Protéger les charges de travail sur Azure / AVS

Reprise après sinistre avec ANF et JetStream

La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données (par exemple, les ransomwares). À l'aide de l'infrastructure VMware VAIO, les charges de travail VMware sur site peuvent être répliquées vers le stockage Azure Blob et récupérées, ce qui permet une perte de données minimale ou quasi nulle et un RTO proche de zéro.

JetStream DR peut être utilisé pour récupérer de manière transparente les charges de travail répliquées sur site vers AVS et plus particulièrement vers Azure NetApp Files. Il permet une reprise après sinistre rentable en utilisant un minimum de ressources sur le site de reprise après sinistre et un stockage cloud rentable. JetStream DR automatise la récupération vers les banques de données ANF via Azure Blob Storage. JetStream DR récupère des machines virtuelles indépendantes ou des groupes de machines virtuelles associées dans l'infrastructure du site de récupération en fonction du mappage réseau et fournit une récupération ponctuelle pour la protection contre les ransomwares.

Ce document fournit une compréhension des principes de fonctionnement de JetStream DR et de ses principaux composants.

▼ Présentation du déploiement de la solution

1. Installez le logiciel JetStream DR dans le centre de données sur site.
    a. Téléchargez le pack logiciel JetStream DR depuis Azure Marketplace (ZIP) et déployez le JetStream DR MSA (OVA) dans le cluster désigné.
    b. Configurez le cluster avec le package de filtre d'E/S (installez JetStream VIB).
    c. Provisionnez Azure Blob (compte de stockage Azure) dans la même région que le cluster DR AVS.
    d. Déployez des appliances DRVA et attribuez des volumes de journaux de réplication (VMDK à partir d'une banque de données existante ou d'un stockage iSCSI partagé).
    e. Créez des domaines protégés (groupes de machines virtuelles associées) et attribuez des DRVA 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 Analyser les domaines.

c. Déployez les appliances DRVA requises.

d. Créez des volumes de journaux de réplication à l'aide des banques de données vSAN ou ANF disponibles.

e. Importez des domaines protégés et configurez RocVA (VA de récupération) pour utiliser la banque de données ANF pour les placements de machines virtuelles.

f. Sélectionnez l'option de basculement appropriée et démarrez la réhydratation continue pour les domaines ou machines virtuelles RTO proches de zéro.

3. Lors d'un événement de catastrophe, déclenchez le basculement vers les banques de données Azure NetApp Files dans le site de reprise après sinistre AVS désigné.
4. Appelez la restauration automatique du site protégé une fois que le site protégé a été récupéré. Avant de commencer, assurez-vous que les conditions préalables sont remplies comme indiqué dans ce "lien" et exécutez également l'outil de test de bande passante (BWT) fourni par JetStream Software pour évaluer les performances potentielles du stockage Azure Blob et sa bande passante de réplication lorsqu'il est utilisé avec le logiciel JetStream DR. Une fois les prérequis, y compris la connectivité, en place, configurez et abonnez-vous à JetStream DR pour AVS à partir du "Place de marché Azure" . Une fois le logiciel téléchargé, procédez au processus d'installation décrit ci-dessus.

Lors de la planification et du démarrage de la protection d'un grand nombre de machines virtuelles (par exemple, plus de 100), utilisez l'outil de planification de capacité (CPT) de la boîte à outils d'automatisation DR JetStream. Fournissez une liste des machines virtuelles à protéger avec leurs préférences de RTO et de groupe de récupération, puis exécutez CPT.

Le CPT remplit les fonctions suivantes :

- Combinaison de machines virtuelles dans des domaines de protection en fonction de leur RTO.
- Définir le nombre optimal de DRVA et leurs ressources.
- Estimation de la bande passante de réplication requise.
- Identification des caractéristiques du volume du journal de réplication (capacité, bande passante, etc.).
- Estimation de la capacité de stockage d'objets requise, et plus encore.



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

Installer JetStream DR dans un centre de données sur site

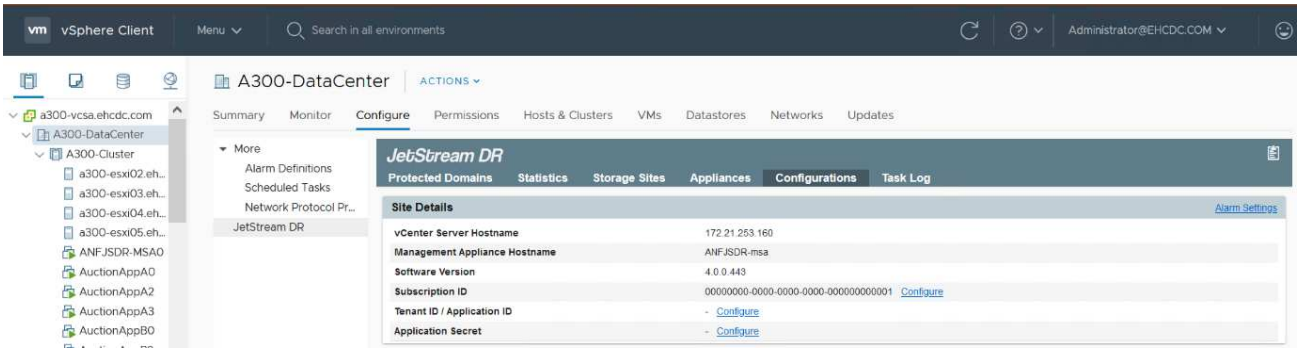
Le logiciel JetStream DR se compose de trois composants principaux : JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) et les composants hôtes (packages de filtres d'E/S). MSA est utilisé pour installer et configurer les composants hôtes sur le cluster de calcul, puis pour administrer le logiciel JetStream DR. La liste suivante fournit une description de haut niveau du processus d'installation :

▼ Comment installer JetStream DR sur site

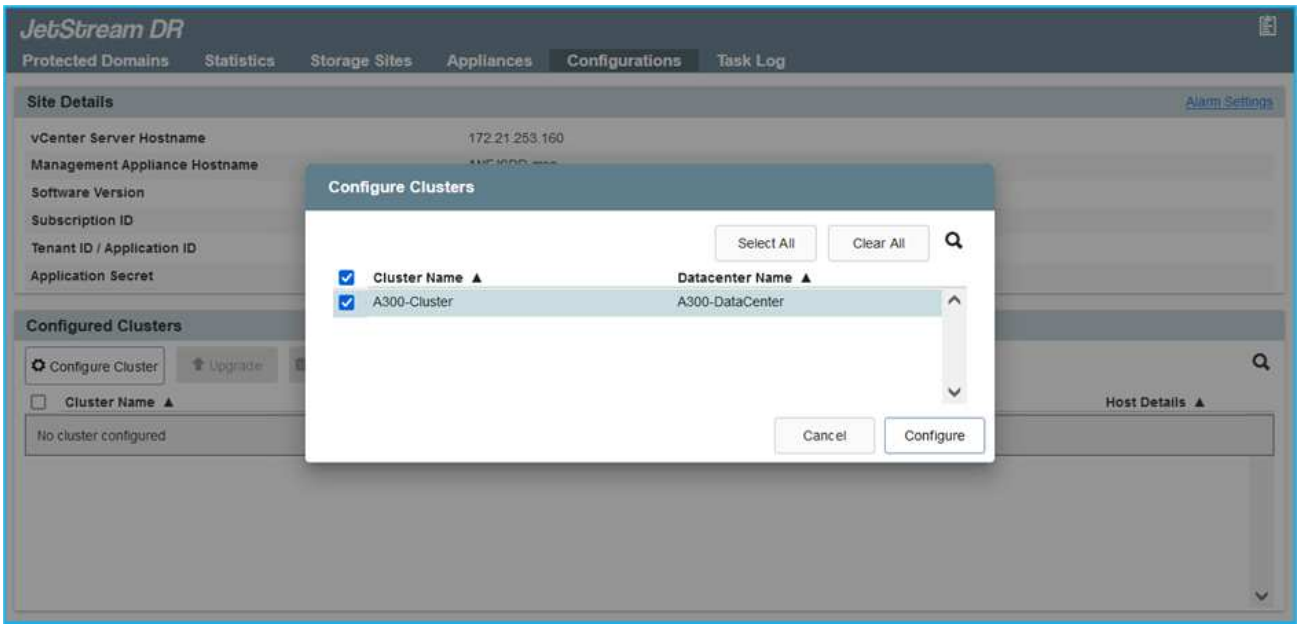
1. Vérifiez les prérequis.
2. Exécutez l'outil de planification de la capacité pour obtenir des recommandations en matière de ressources et de configuration (facultatif mais recommandé pour les essais de validation de principe).
3. Déployez le JetStream DR MSA sur un hôte vSphere dans le cluster désigné.
4. Lancez le MSA en utilisant son nom DNS dans un navigateur.
5. Enregistrez le serveur vCenter auprès du MSA. Pour effectuer l'installation, suivez les étapes détaillées

suivantes :

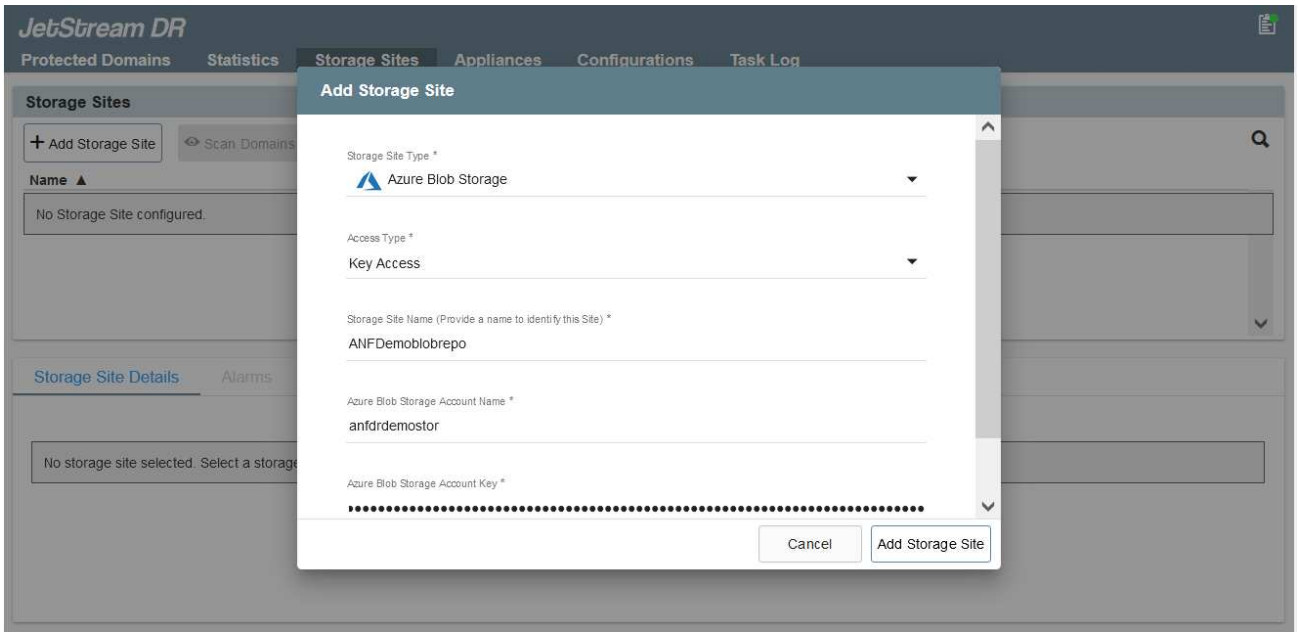
6. Une fois JetStream DR MSA déployé et vCenter Server enregistré, accédez au plug-in JetStream DR à l'aide de vSphere Web Client. Cela peut être fait en accédant à Datacenter > Configurer > JetStream DR.



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



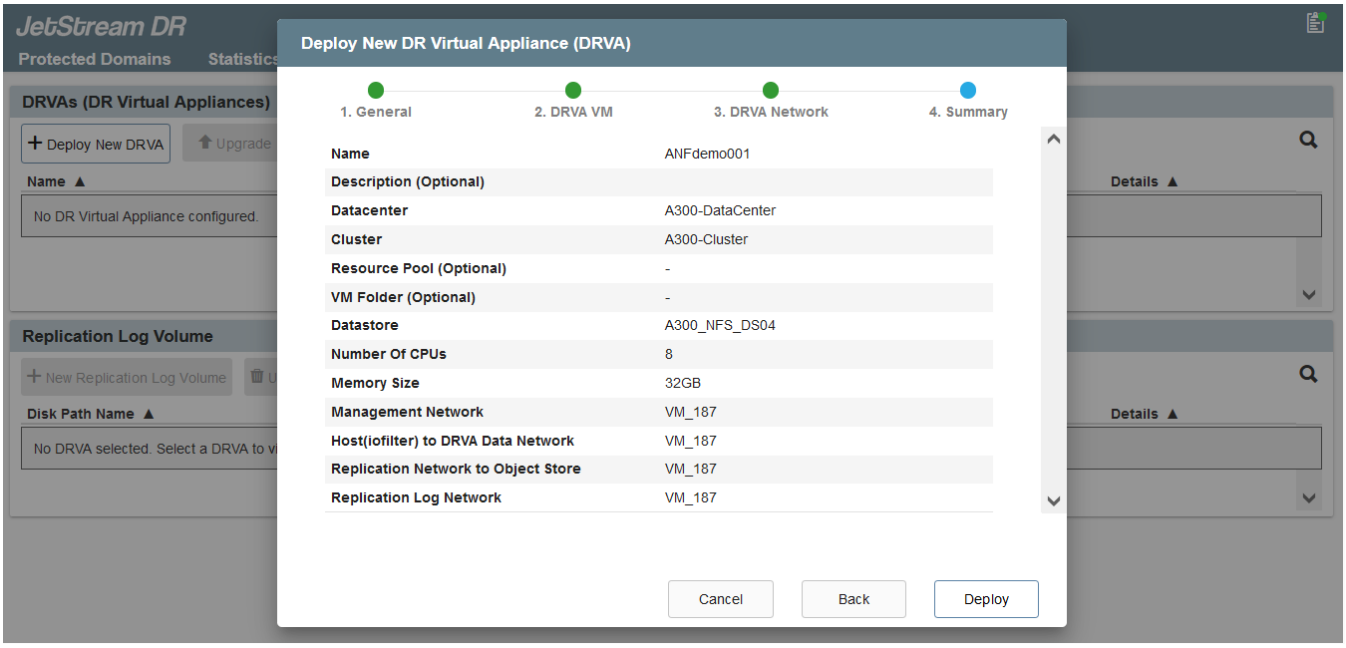
8. Configurez le cluster avec le package de filtre d'E/S.



9. Ajoutez Azure Blob Storage situé sur le site de récupération.
10. Déployez une appliance virtuelle DR (DRVA) à partir de l'onglet Appliances.

> Les DRVA peuvent être créés automatiquement par CPT, mais pour les essais POC, nous recommandons de configurer et d'exécuter le cycle DR manuellement (démarrer la protection > basculement > restauration).

Le JetStream DRVA est un appareil virtuel qui facilite les fonctions clés du processus de réplication des données. Un cluster protégé doit contenir au moins un DRVA, et généralement un DRVA est configuré par hôte. Chaque DRVA peut gérer plusieurs domaines protégés.

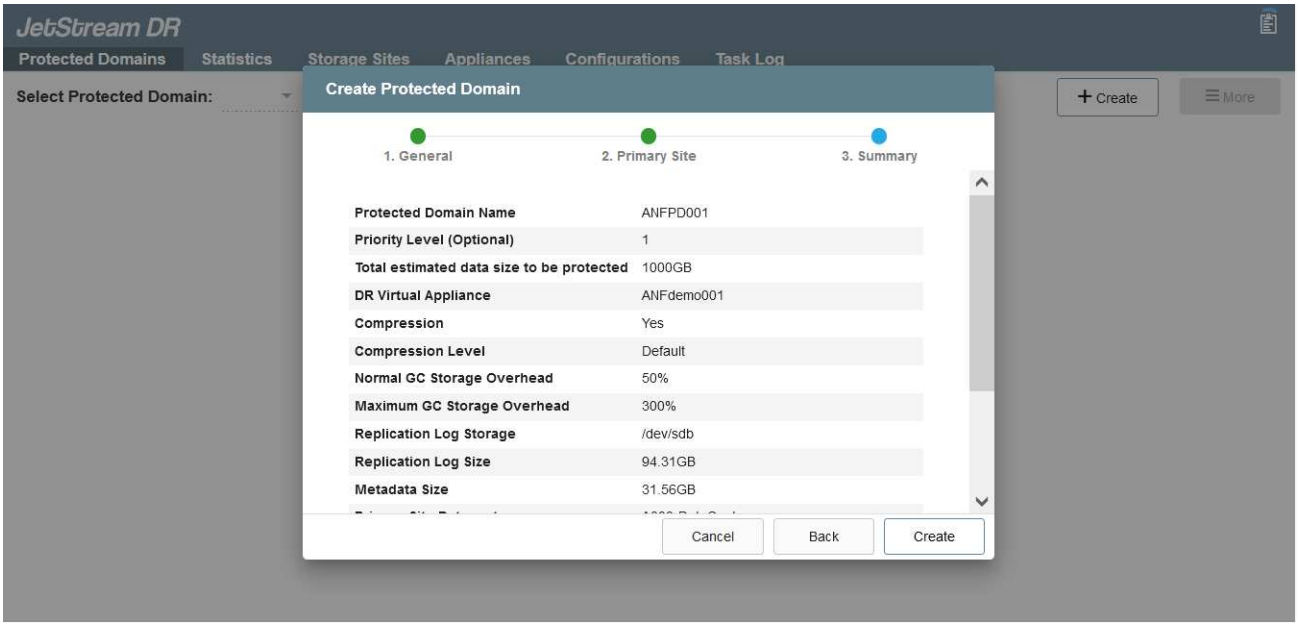


Dans cet exemple, quatre DRVA ont été créés pour 80 machines virtuelles.

1. Créez des volumes de journaux de réplication pour chaque DRVA à l'aide de VMDK à partir des

banques de données disponibles ou des pools de stockage iSCSI partagés indépendants.

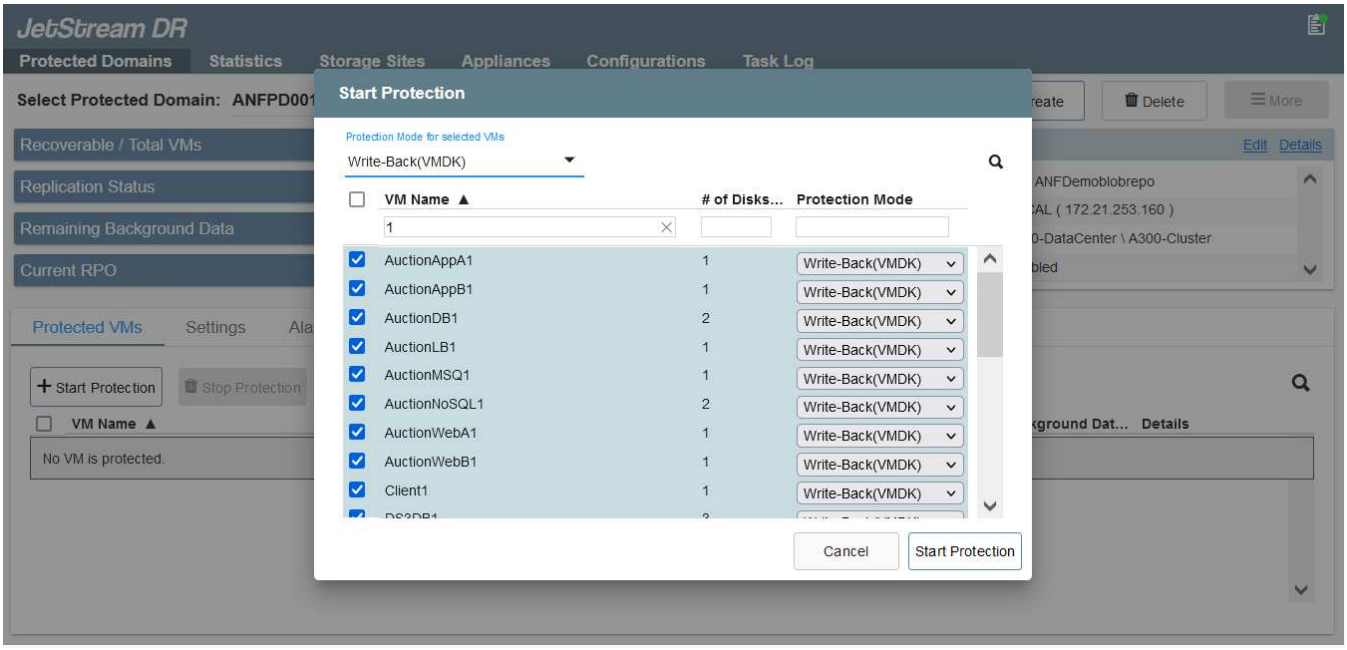
2. À partir de l'onglet Domaines protégés, créez le nombre requis de domaines protégés à l'aide des informations sur le site Azure Blob Storage, l'instance DRVA et le journal de réplication. Un domaine protégé définit une machine virtuelle spécifique ou un ensemble de machines virtuelles au sein du cluster qui sont protégées ensemble et auxquelles est attribué un ordre de priorité pour les opérations de basculement/restauration.



3. Sélectionnez les machines virtuelles que vous souhaitez protéger et démarrez la protection des machines virtuelles du domaine protégé. Cela démarre la réplication des données vers le magasin d'objets Blob désigné.

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

Le mode Write-Back (VMDK) peut offrir des performances supérieures.



Vérifiez que les volumes de journaux de réplication sont placés sur un stockage hautes performances.

Les livres d'exécution de basculement peuvent être configurés pour regrouper les machines virtuelles (appelées groupe de récupération), définir la séquence d'ordre de démarrage et modifier les paramètres CPU/mémoire ainsi que les configurations IP.

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

Une bonne pratique pour un site de récupération (AVS) consiste à créer à l'avance un cluster de voyants lumineux à trois nœuds. Cela permet de préconfigurer l'infrastructure du site de récupération, y compris les éléments suivants :

- Segments de réseau de destination, pare-feu, services tels que DHCP et DNS, etc.
- Installation de JetStream DR pour AVS
- Configuration des volumes ANF en tant que banques de données, et plus encoreJetStream DR prend en charge le mode RTO proche de zéro pour les domaines critiques. Pour ces domaines, le stockage de destination doit être préinstallé. L'ANF est un type de stockage recommandé dans ce cas.

La configuration du réseau, y compris la création de segments, doit être configurée sur le cluster AVS pour correspondre aux exigences locales.

En fonction des exigences SLA et RTO, un basculement continu ou un mode de basculement régulier (standard) peut être utilisé. Pour un RTO proche de zéro, une réhydratation continue doit être démarrée au site de récupération.

▼ **Comment installer JetStream DR pour AVS dans un cloud privé**

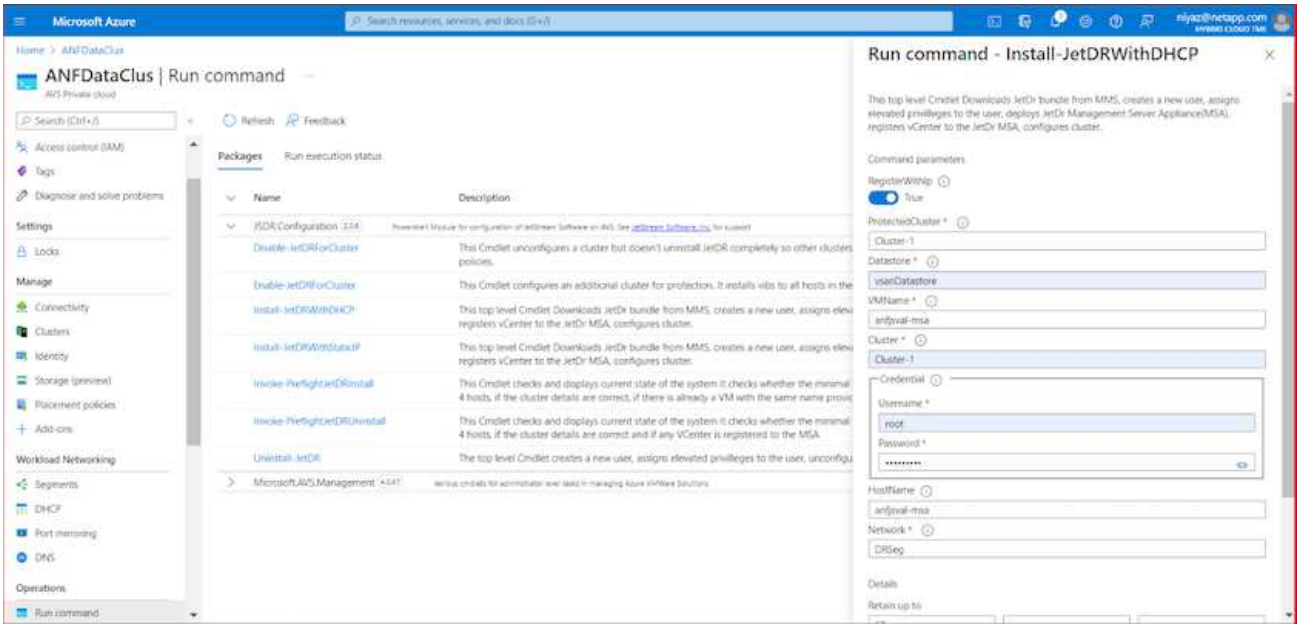
Pour installer JetStream DR pour AVS sur un cloud privé Azure VMware Solution, procédez comme suit :

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

L'utilisateur CloudAdmin par défaut dans Azure VMware Solution ne dispose pas de

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.

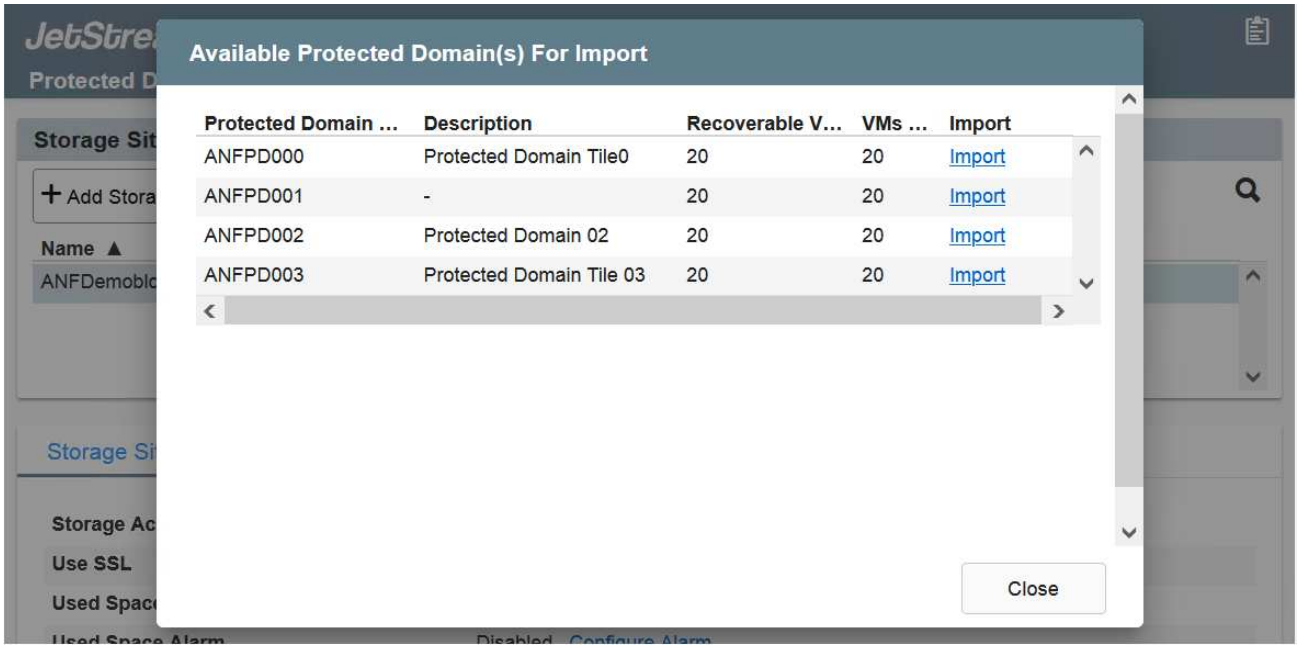
La capture d'écran suivante montre l'installation à l'aide d'une adresse IP basée sur DHCP.



2. Une fois l'installation de JetStream DR pour AVS terminée, actualisez le navigateur. Pour accéder à l'interface utilisateur de JetStream DR, accédez à SDDC Datacenter > Configurer > JetStream DR.



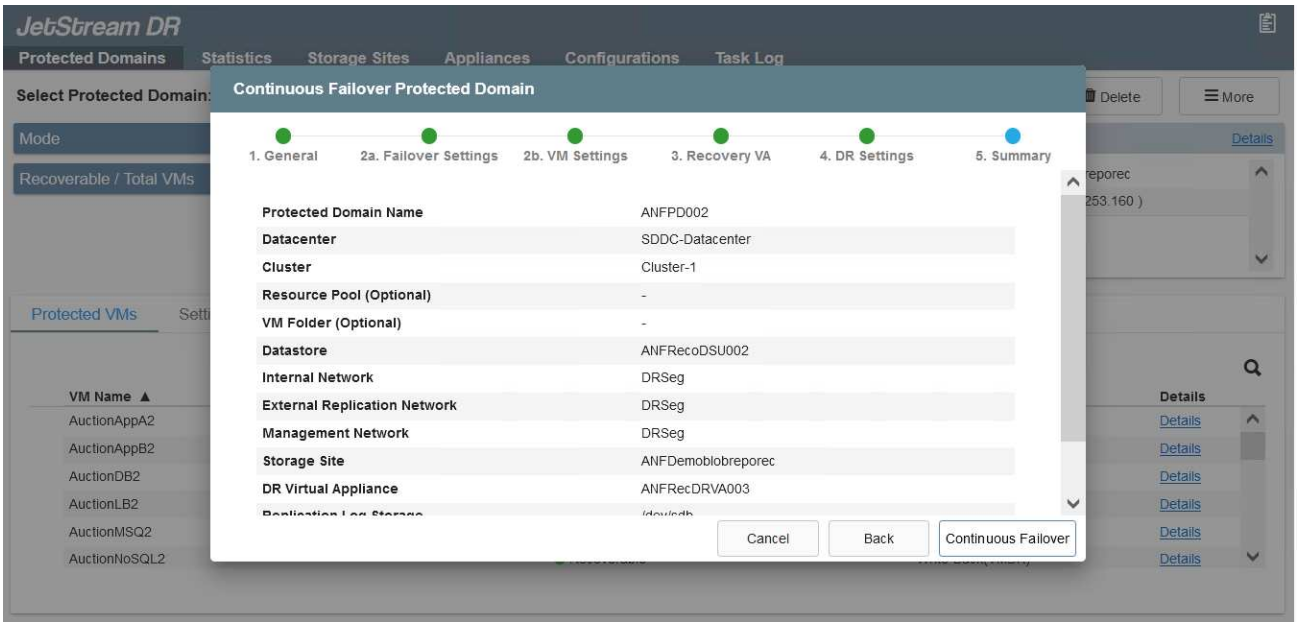
3. À partir de l'interface JetStream DR, ajoutez le compte Azure Blob Storage qui a été utilisé pour protéger le cluster local en tant que site de stockage, puis exécutez l'option Analyser les domaines.



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

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

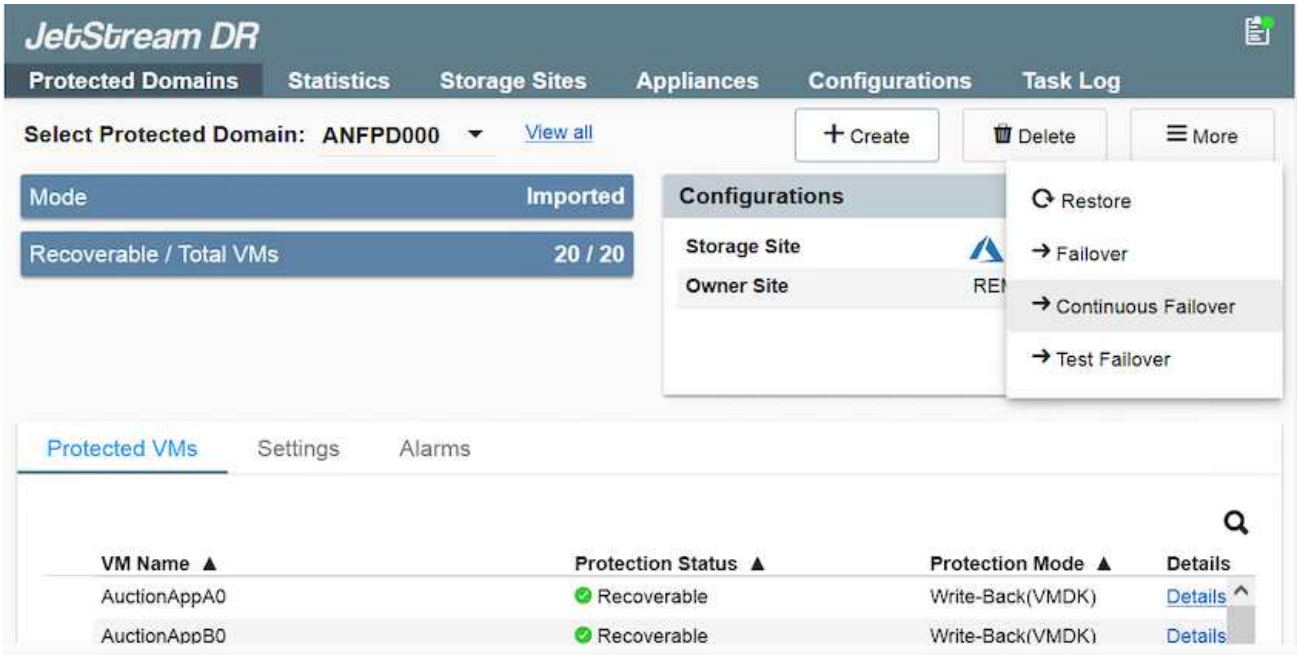
5. Créez des volumes de journaux de réplication à l'aide des banques de données vSAN ou ANF disponibles.
6. Importez les domaines protégés et configurez Recovery VA pour utiliser la banque de données ANF pour les placements de machines virtuelles.



> Assurez-vous que DHCP est activé sur le segment sélectionné et que suffisamment d'adresses IP sont disponibles. Les adresses IP dynamiques sont utilisées temporairement pendant la récupération des domaines. Chaque VM en cours de

récupération (y compris la réhydratation continue) nécessite une IP dynamique individuelle. Une fois la récupération terminée, l'IP est libérée et peut être réutilisée.

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



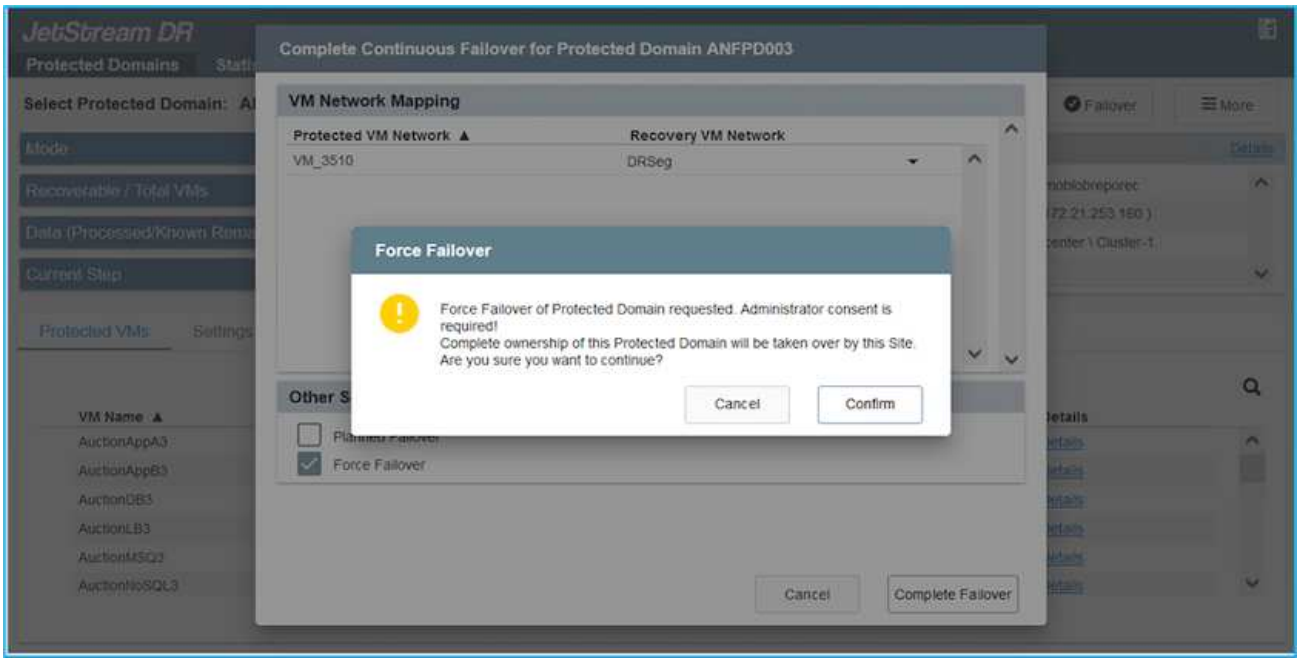
Exécution d'un basculement/retour arrière

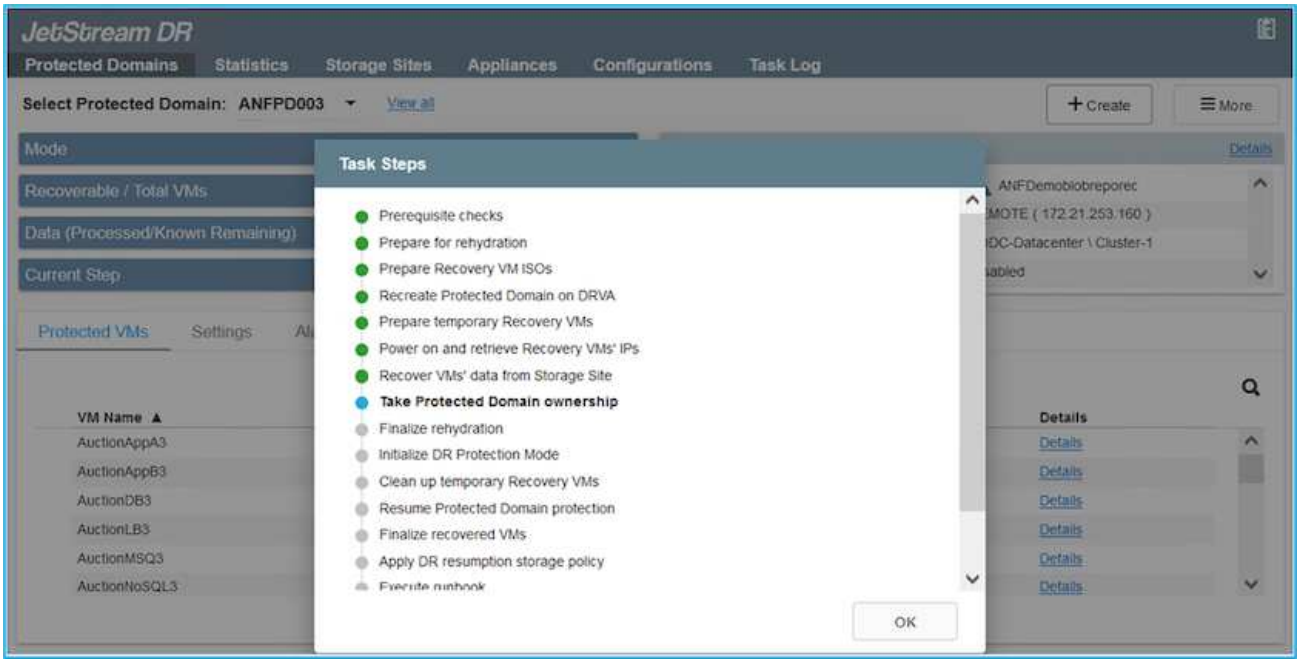
▼ Comment effectuer un basculement / retour arrière

1. Après qu'un sinistre se produit dans le cluster protégé de l'environnement local (panne partielle ou totale), déclenchez le basculement.

CPT peut être utilisé pour exécuter le plan de basculement afin de récupérer les machines virtuelles d'Azure Blob Storage vers le site de récupération du cluster AVS.

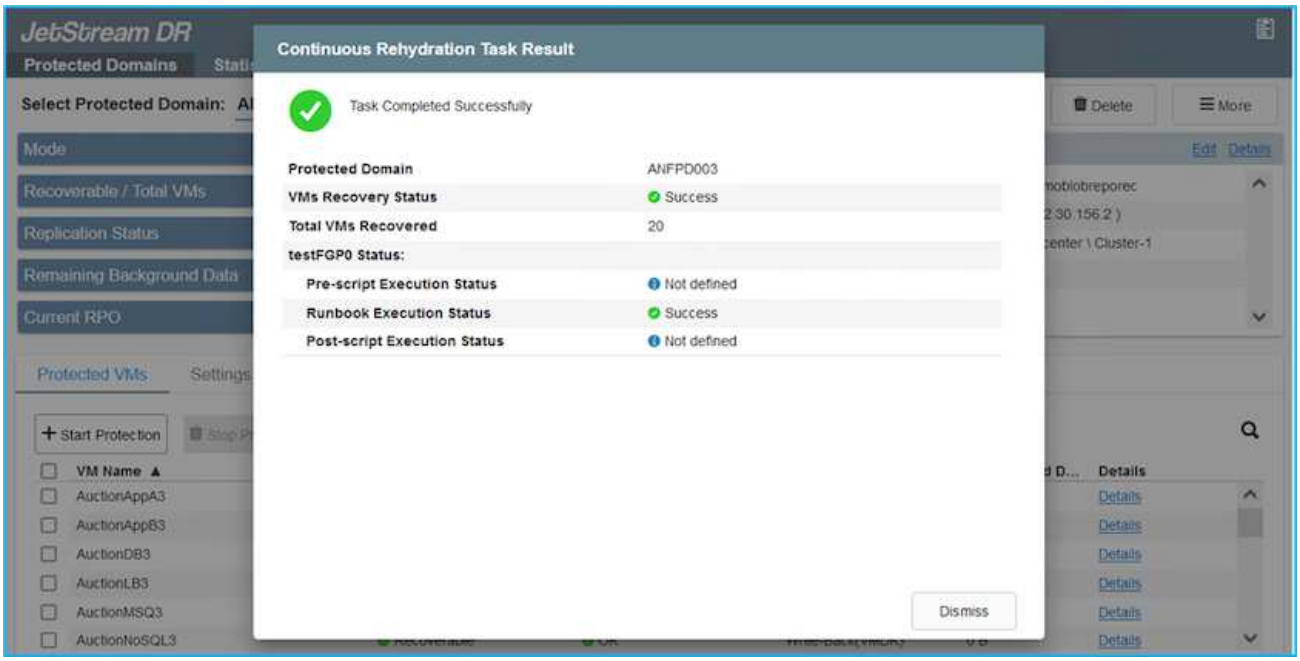
Après le basculement (pour une réhydratation continue ou standard), lorsque les machines virtuelles protégées ont été démarrées dans AVS, la protection reprend automatiquement et JetStream DR continue de répliquer leurs données dans les conteneurs appropriés/d'origine dans Azure Blob Storage.





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

2. Une fois la tâche terminée, accédez aux machines virtuelles récupérées et l'activité continue normalement.

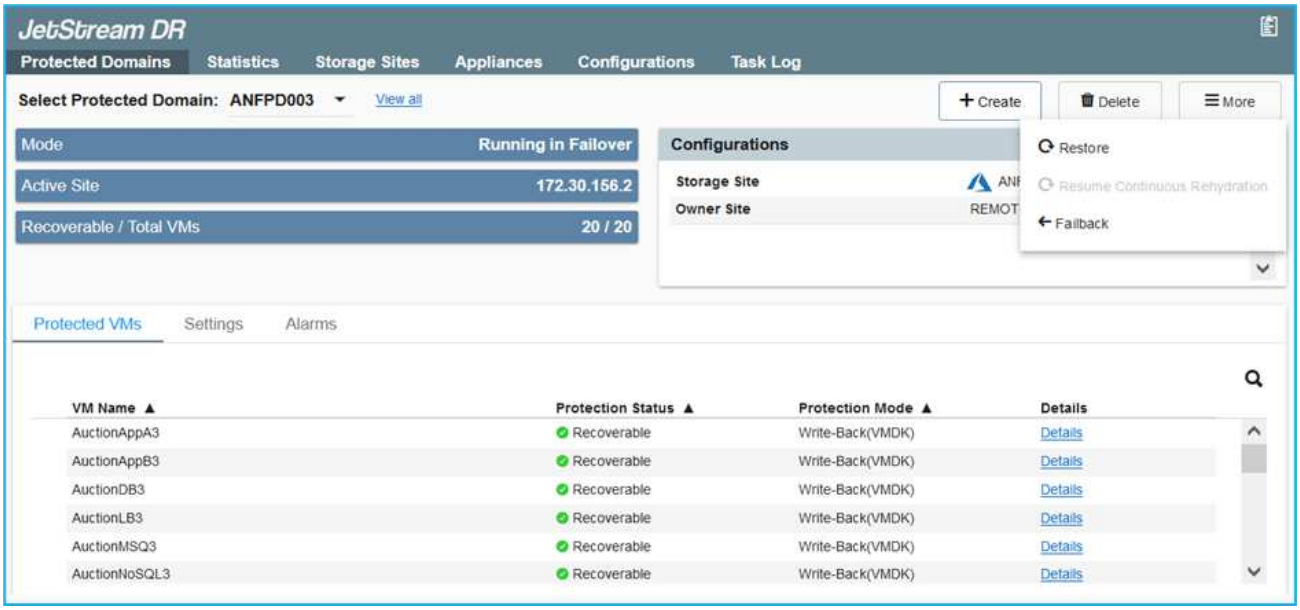


Une fois le site principal à nouveau opérationnel, une restauration peut être effectuée. La protection de la machine virtuelle est reprise et la cohérence des données doit être vérifiée.

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

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

4. Accédez à l'environnement local restauré, accédez à l'interface utilisateur Jetstream DR et sélectionnez le domaine protégé approprié. Une fois que le site protégé est prêt pour la restauration, sélectionnez l'option Restauration dans l'interface utilisateur.



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

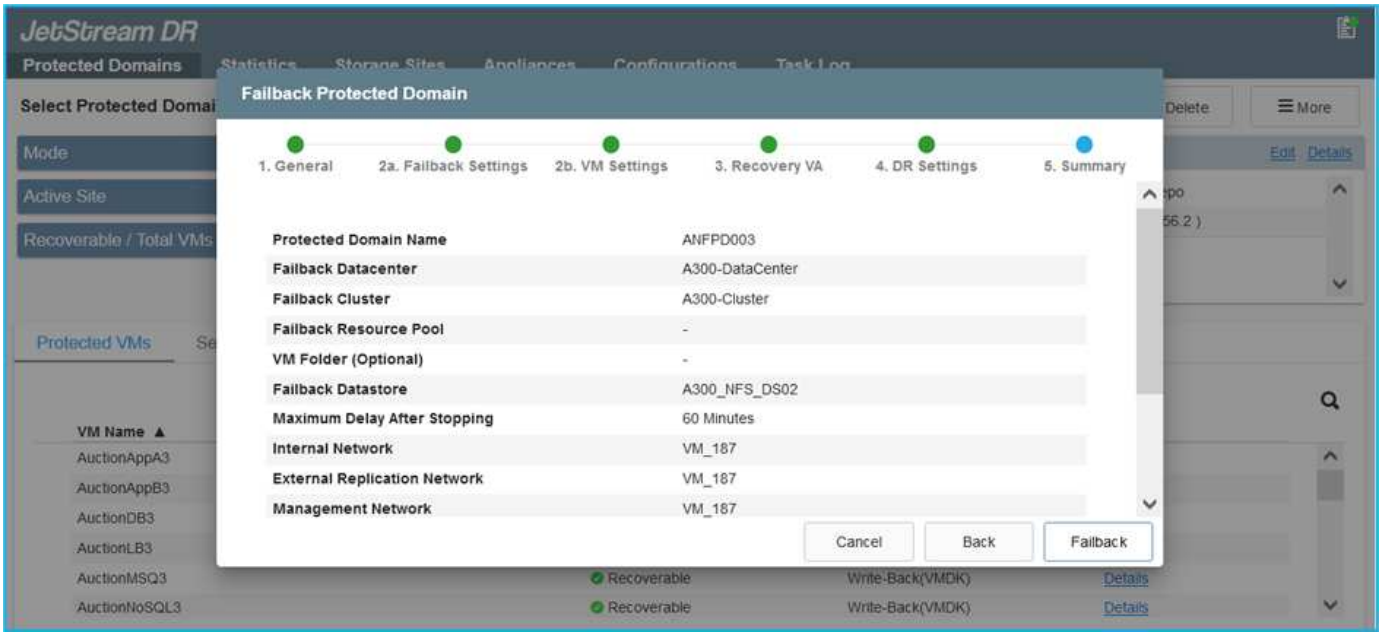
Spécifiez le délai maximal après la mise en pause des machines virtuelles sur le site de récupération et le redémarrage sur le site protégé. Ce temps comprend la fin de la réplication après l'arrêt des machines virtuelles de basculement, le temps de nettoyage du site de récupération et le temps de recréation des machines virtuelles dans le site protégé. La valeur recommandée par NetApp est de 10 minutes.

Terminez le processus de restauration automatique, puis confirmez la reprise de la protection de la machine virtuelle et de la cohérence des données.

Récupération de ransomware

Se remettre d'un ransomware peut être une tâche ardue. Plus précisément, il peut être difficile pour les organisations informatiques de déterminer le point de retour sûr et, une fois déterminé, comment garantir que les charges de travail récupérées sont protégées contre les attaques récurrentes (provenant de logiciels malveillants dormants ou d'applications vulnérables).

JetStream DR pour AVS, associé aux banques de données Azure NetApp Files, peut répondre à ces préoccupations en permettant aux organisations de récupérer 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 médico-légales et d'autres mesures correctives nécessaires.



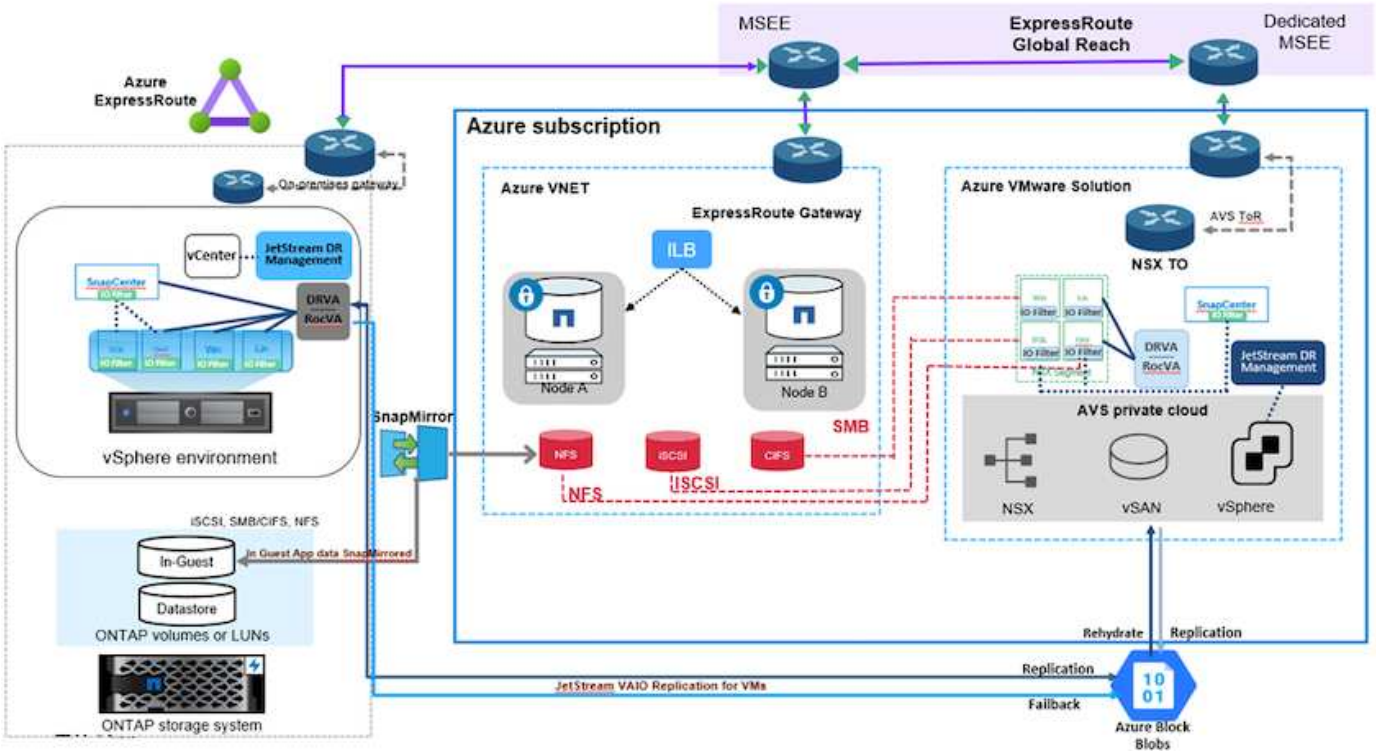
Reprise après sinistre avec CVO et AVS (stockage connecté en tant qu'invité)

La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données tels que les ransomwares. Avec NetApp SnapMirror, les charges de travail VMware sur site qui utilisent un stockage connecté en tant qu'invité peuvent être répliquées vers

NetApp Cloud Volumes ONTAP exécuté dans Azure.

Aperçu

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
Ce document fournit une approche étape par étape pour la configuration et
l'exécution de la reprise après sinistre qui utilise NetApp SnapMirror,
JetStream et Azure VMware Solution (AVS).
```



Hypothèses

Ce document se concentre sur le stockage en invité pour les données d'application (également appelé invité connecté), et nous supposons que l'environnement sur site utilise SnapCenter pour les sauvegardes cohérentes avec les applications.

> Ce document s'applique à toute solution de sauvegarde ou de récupération tierce. En fonction de la solution utilisée dans l'environnement, suivez les meilleures pratiques pour créer des politiques de sauvegarde qui respectent les SLA organisationnels.

Pour la connectivité entre l'environnement local et le réseau virtuel Azure, utilisez la route express globale ou un WAN virtuel avec une passerelle VPN. Les segments doivent être créés en fonction de la conception du

VLAN sur site.

> Il existe plusieurs options pour connecter les centres de données locaux à Azure, ce qui nous empêche de décrire un flux de travail spécifique dans ce document. Reportez-vous à la documentation Azure pour connaître la méthode de connectivité locale vers Azure appropriée.

Déploiement de la solution DR

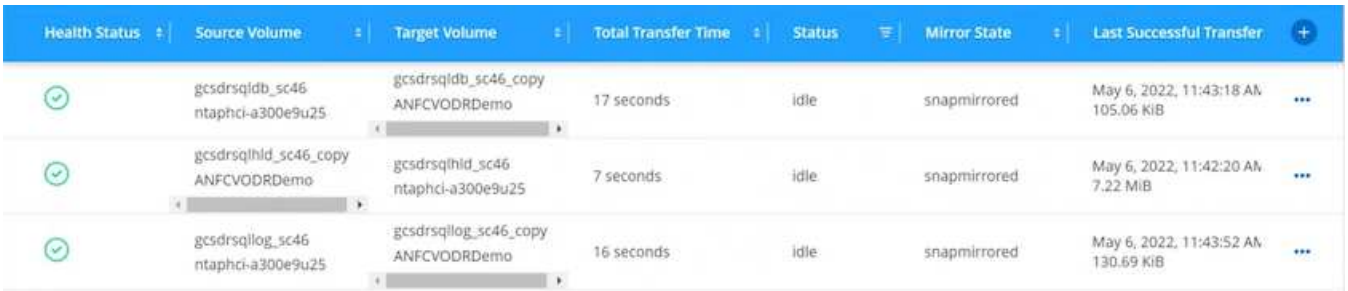
Présentation du déploiement de la solution

1. Assurez-vous que les données d'application sont sauvegardées à l'aide de SnapCenter avec les exigences RPO nécessaires.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance correcte à l'aide du gestionnaire Cloud dans l'abonnement et le réseau virtuel appropriés.
   a. Configurez SnapMirror pour les volumes d'application concernés.
   b. Mettez à jour les stratégies de sauvegarde dans SnapCenter pour déclencher les mises à jour de SnapMirror après les tâches planifiées.
3. Installez le logiciel JetStream DR dans le centre de données sur site et démarrez la protection des machines virtuelles.
4. Installez le logiciel JetStream DR dans le cloud privé Azure VMware Solution.
5. Lors d'un événement de catastrophe, interrompez la relation SnapMirror à l'aide de Cloud Manager et déclenchez le basculement des machines virtuelles vers Azure NetApp Files ou vers les banques de données vSAN dans le site de reprise après sinistre AVS désigné.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'application.
6. Appelez la restauration automatique du site protégé en resynchronisant SnapMirror en sens inverse une fois le site principal récupéré.

Détails du déploiement

▼ Configurer CVO sur Azure et répliquer les volumes vers CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Azure ("Lien") et répliquez les volumes souhaités vers Cloud Volumes ONTAP avec les fréquences et les rétentions de snapshots souhaitées.



▼ Configurer les hôtes AVS et l'accès aux données CVO

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution Azure VMware et la durée pendant laquelle le SDDC doit être maintenu en service. Ces deux considérations clés pour une solution de reprise après sinistre contribuent à réduire les coûts opérationnels globaux. Le SDDC peut être aussi petit que trois hôtes, jusqu'à un cluster multi-hôtes dans un déploiement à grande échelle.

La décision de déployer un cluster AVS est principalement basée sur les exigences RPO/RTO. Avec la solution Azure VMware, le SDDC peut être provisionné juste à temps en prévision d'un test ou d'un événement catastrophique réel. Un SDDC déployé juste à temps permet d'économiser sur les coûts d'hébergement ESXi lorsque vous n'êtes pas confronté à une catastrophe. Cependant, cette forme de déploiement affecte le RTO de quelques heures pendant que le SDDC est en cours de provisionnement.

L'option déployée la plus courante consiste à faire fonctionner le SDDC en mode de fonctionnement permanent et en mode veilleuse. Cette option offre une petite empreinte de trois hôtes toujours disponibles et accélère également les opérations de récupération en fournissant une base de référence pour les activités de simulation et les contrôles de conformité, évitant ainsi le risque de dérive opérationnelle entre les sites de production et de reprise après sinistre. Le groupe de veilleuses peut être rapidement mis à l'échelle jusqu'au niveau souhaité lorsque cela est nécessaire pour gérer un événement DR réel.

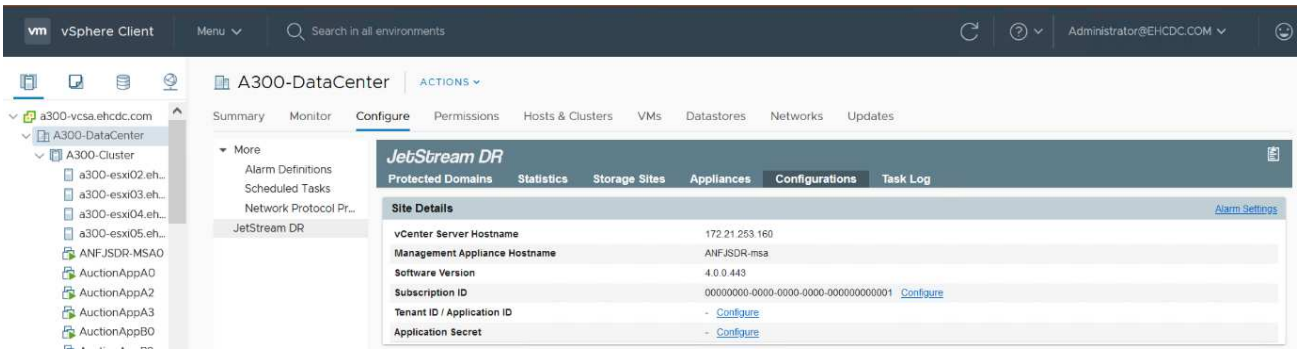
Pour configurer AVS SDDC (que ce soit à la demande ou en mode veilleuse), voir"Déployer et configurer l'environnement de virtualisation sur Azure" . Comme condition préalable, vérifiez que les machines virtuelles invitées résidant sur les hôtes AVS sont en mesure de consommer les données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois Cloud Volumes ONTAP et AVS correctement configurés, commencez à configurer Jetstream pour automatiser la récupération des charges de travail sur site vers AVS (machines virtuelles avec VMDK d'application et machines virtuelles avec stockage en invité) en utilisant le mécanisme VAIO et en exploitant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

▼ Installer JetStream DR dans un centre de données sur site

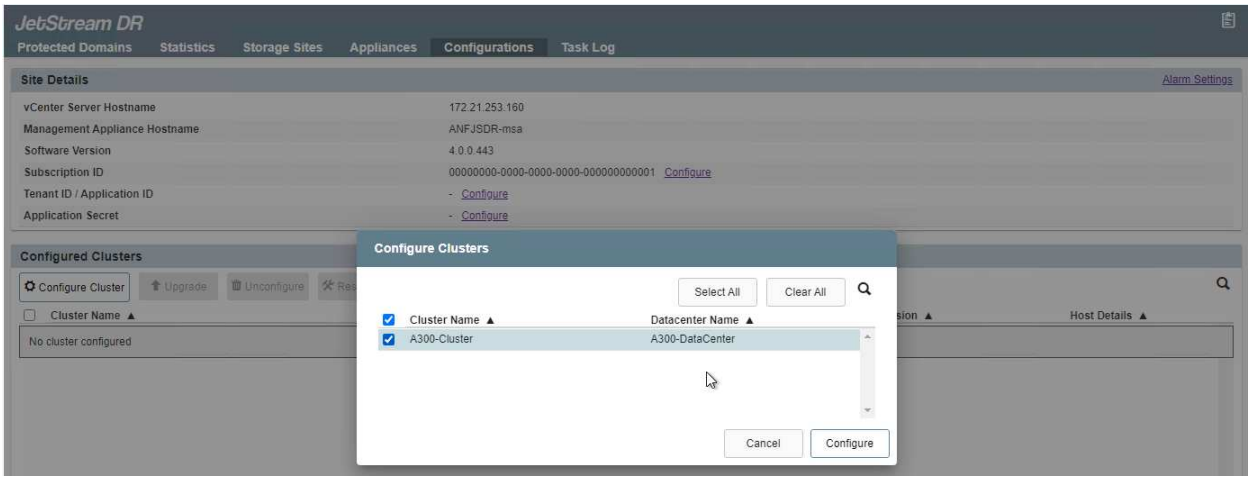
Le logiciel JetStream DR se compose de trois composants principaux : le JetStream DR Management Server Virtual Appliance (MSA), le DR Virtual Appliance (DRVA) et les composants hôtes (packages de filtres d'E/S). Le MSA est utilisé pour installer et configurer les composants hôtes sur le cluster de calcul, puis pour administrer le logiciel JetStream DR. Le processus d'installation est le suivant :

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 le JetStream DR MSA sur chaque hôte vSphere du cluster désigné.
4. Lancez le MSA en utilisant son nom DNS dans un navigateur.
5. Enregistrez le serveur vCenter auprès du MSA.
6. Une fois JetStream DR MSA déployé et vCenter Server enregistré, accédez au plug-in JetStream DR avec vSphere Web Client. Cela peut être fait en accédant à Centre de données > Configurer > JetStream DR.

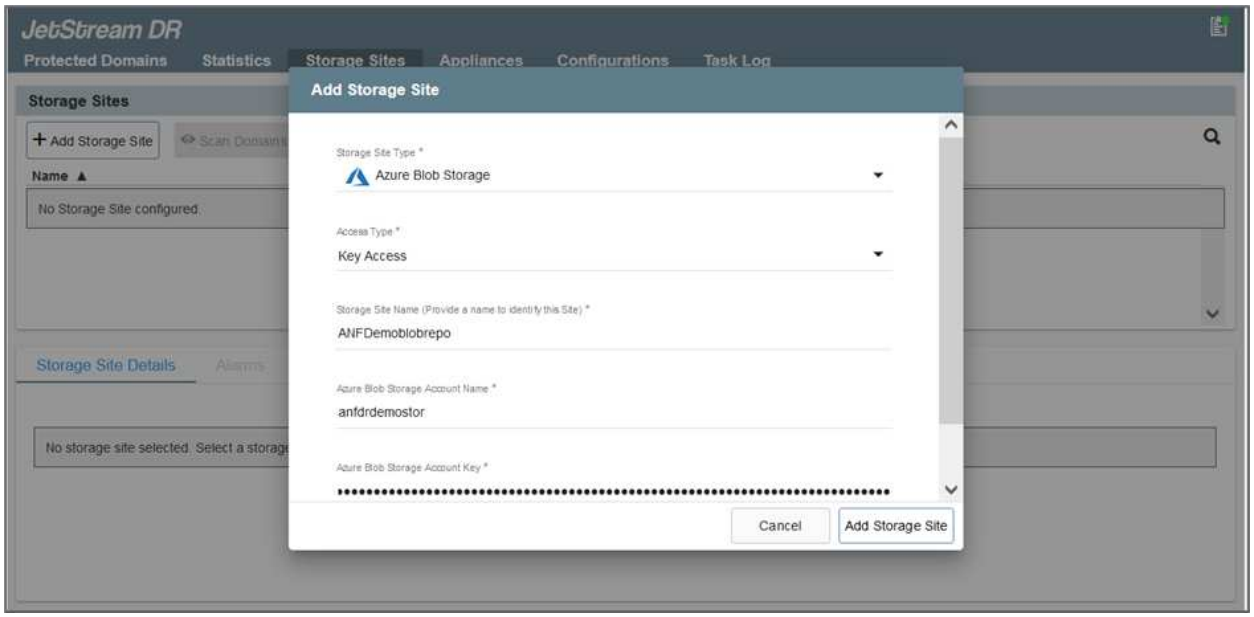


7. Depuis l'interface JetStream DR, effectuez les tâches suivantes :

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



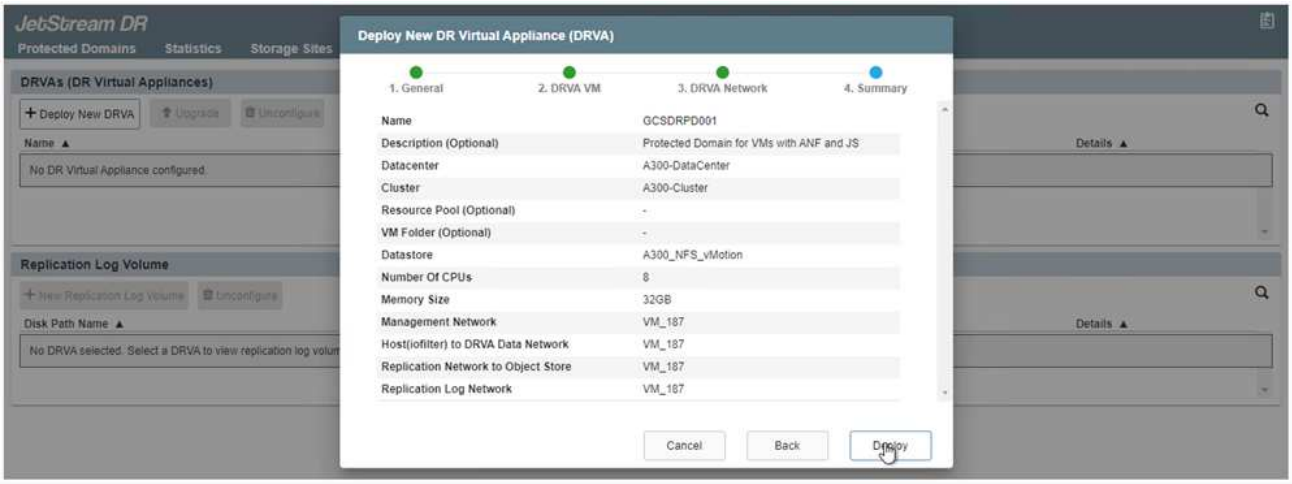
b. Ajoutez le stockage Azure Blob situé sur le site de récupération.



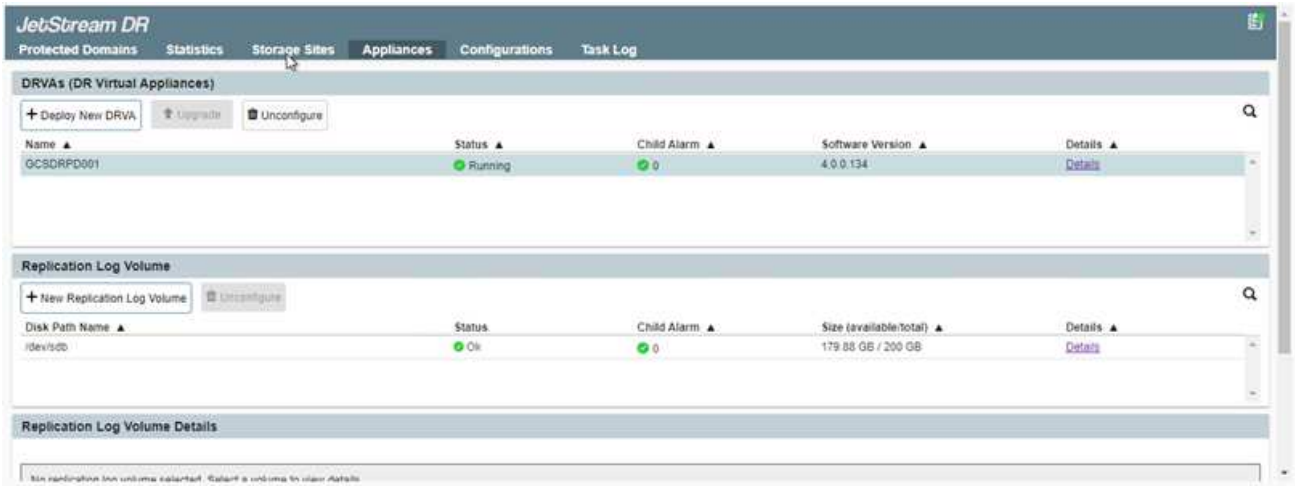
8. Déployez le nombre requis d'appliances virtuelles DR (DRVA) à partir de l'onglet Appliances.

Utilisez l'outil de planification de la capacité pour estimer le nombre de DRVA requis.

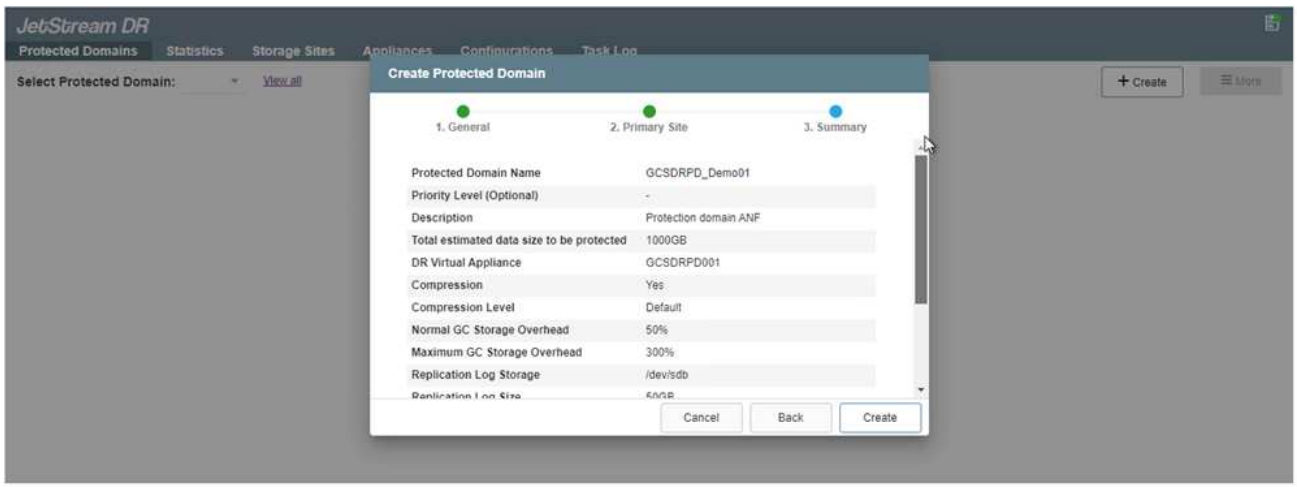


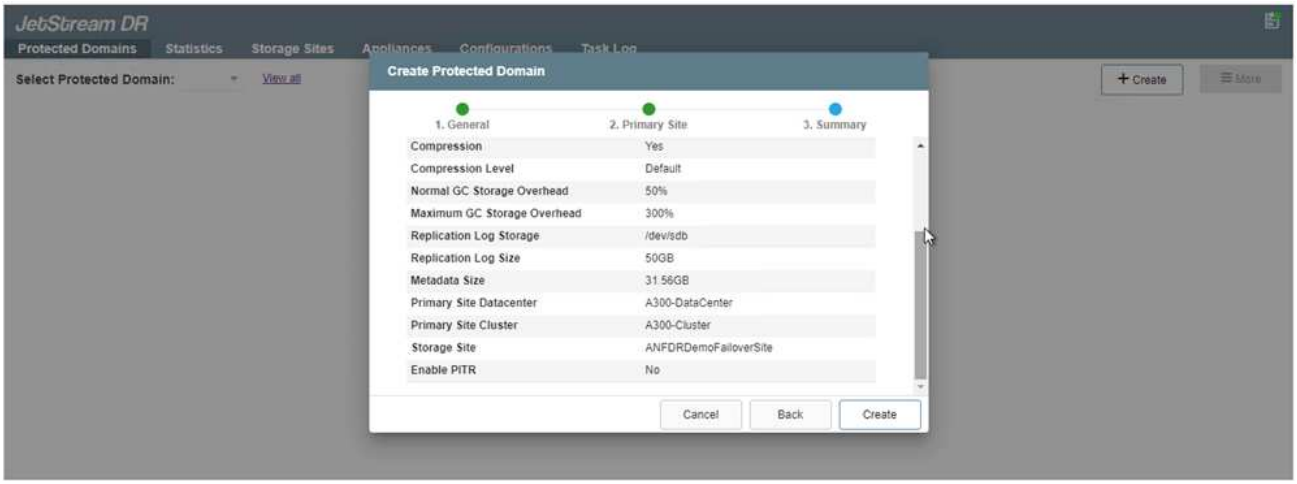


9. Créez des volumes de journaux de réplication pour chaque DRVA à l'aide du VMDK à partir des banques de données disponibles ou du pool de stockage iSCSI partagé indépendant.



10. À partir de l'onglet Domaines protégés, créez le nombre requis de domaines protégés à l'aide des informations sur le site Azure Blob Storage, l'instance DRVA et le journal de réplication. Un domaine protégé définit une machine virtuelle spécifique ou un ensemble de machines virtuelles d'application au sein du cluster qui sont protégées ensemble et auxquelles est attribué un ordre de priorité pour les opérations de basculement/restauration.

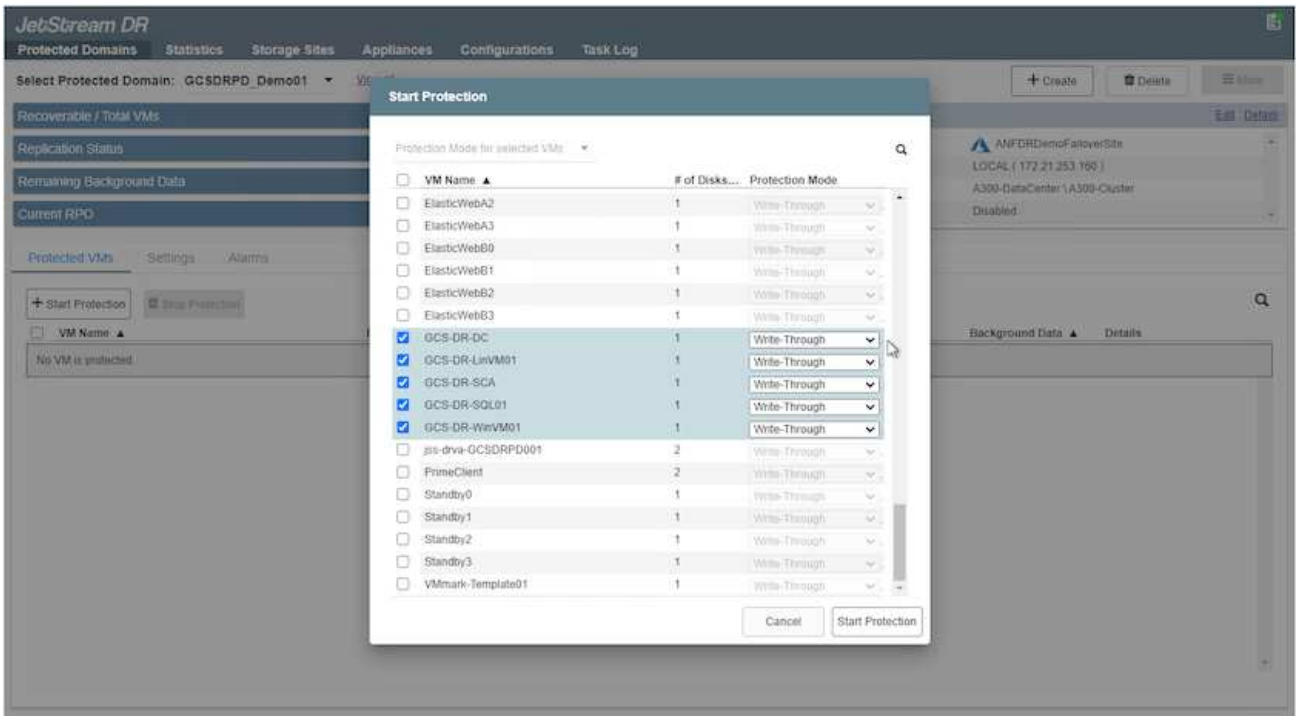




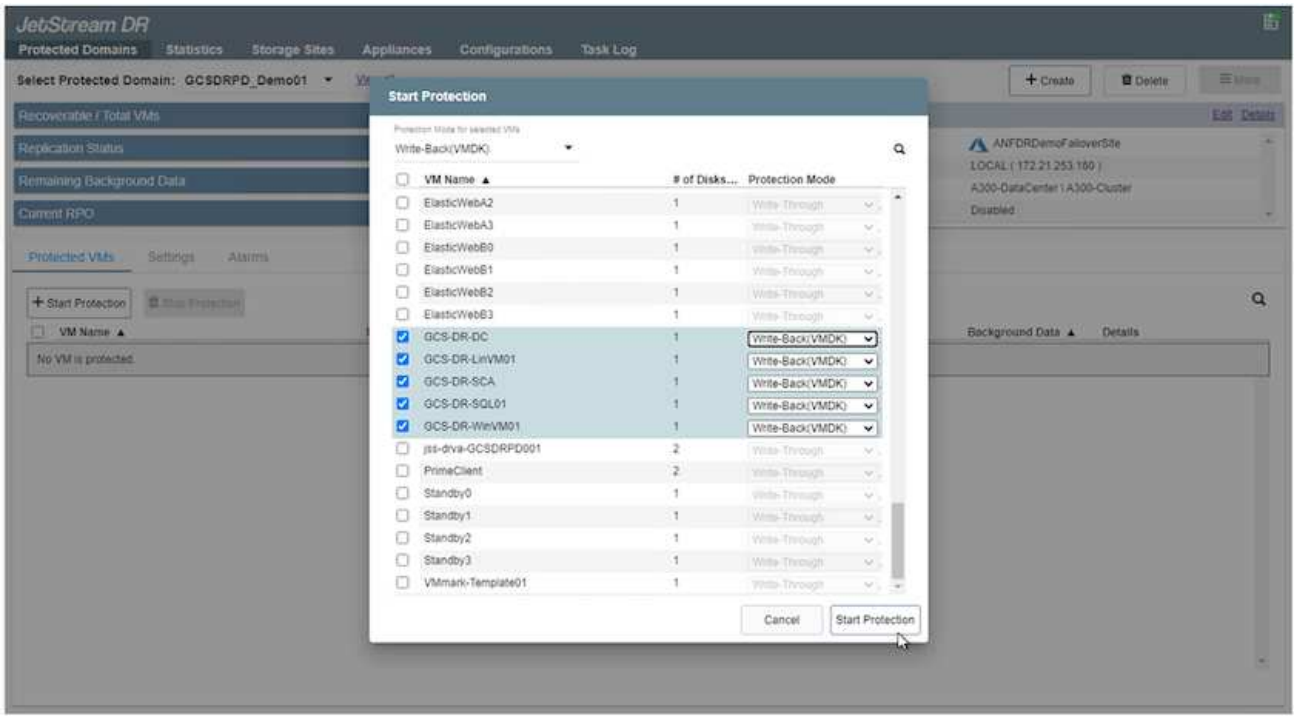
11. Sélectionnez les machines virtuelles à protéger et regroupez-les en groupes d'applications en fonction de la dépendance. Les définitions d'application vous permettent de regrouper des ensembles de machines virtuelles en groupes logiques contenant leurs ordres de démarrage, leurs délais de démarrage et leurs validations d'application facultatives qui peuvent être exécutées lors de la récupération.

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

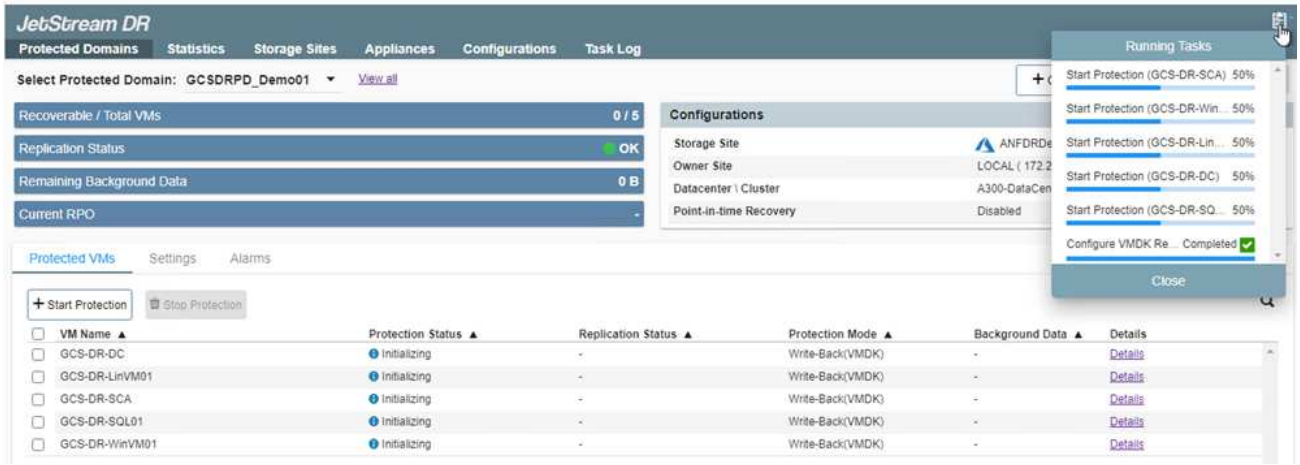
Le mode Write-Back (VMDK) offre des performances supérieures.



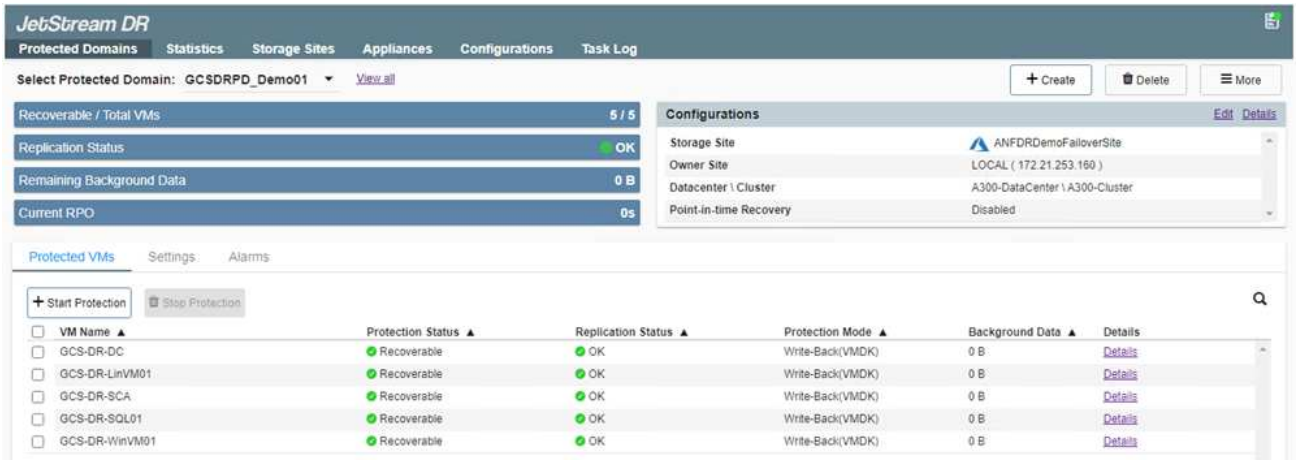
12. Assurez-vous que les volumes de journaux de réplication sont placés sur un stockage hautes performances.



13. Une fois que vous avez terminé, cliquez sur Démarrer la protection pour le domaine protégé. Cela démarre la réplication des données pour les machines virtuelles sélectionnées vers le magasin d'objets Blob désigné.



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



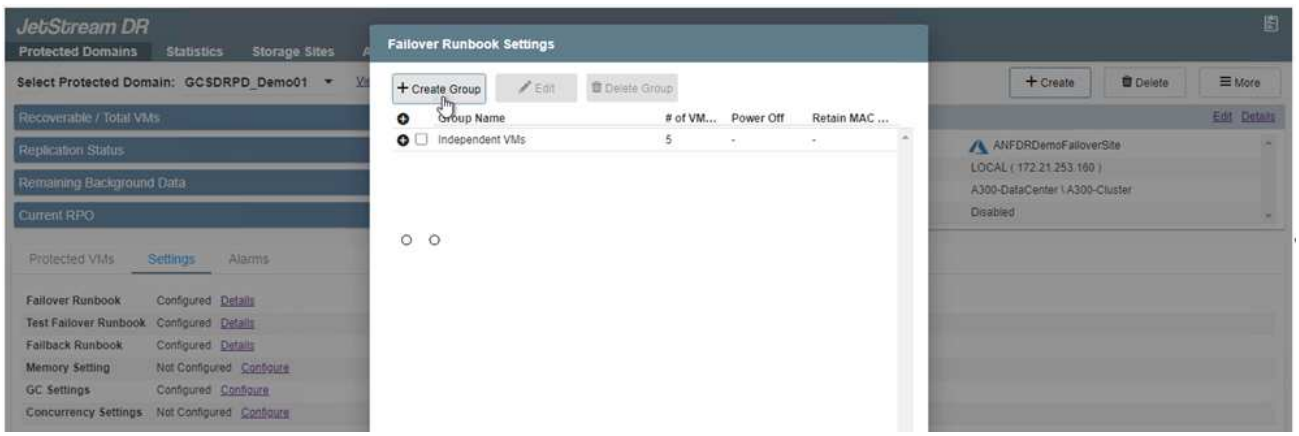
Les runbooks de basculement peuvent être configurés pour regrouper les machines virtuelles (appelées groupe de récupération), définir la séquence d'ordre de démarrage et modifier les paramètres CPU/mémoire ainsi que les configurations IP.

15. Cliquez sur Paramètres, puis sur le lien Configurer du runbook pour configurer le groupe de runbooks.

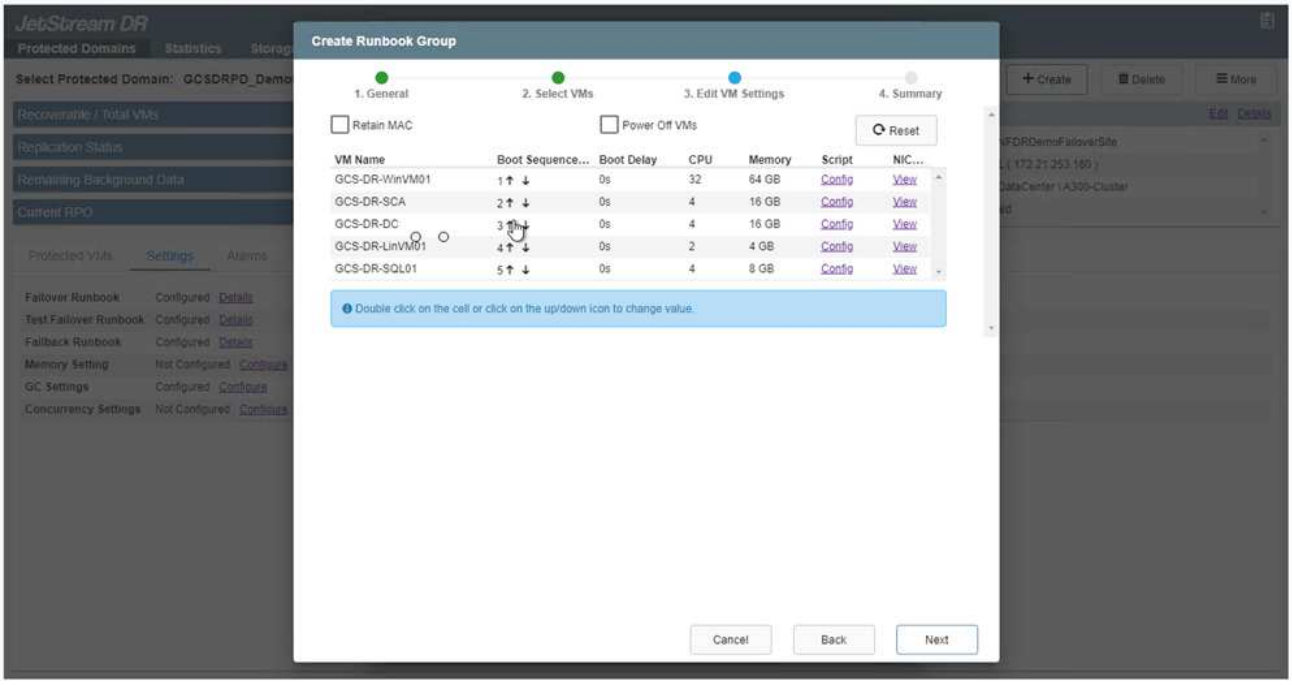


16. Cliquez sur le bouton Créer un groupe pour commencer à créer un nouveau groupe de cahiers d'exécution.

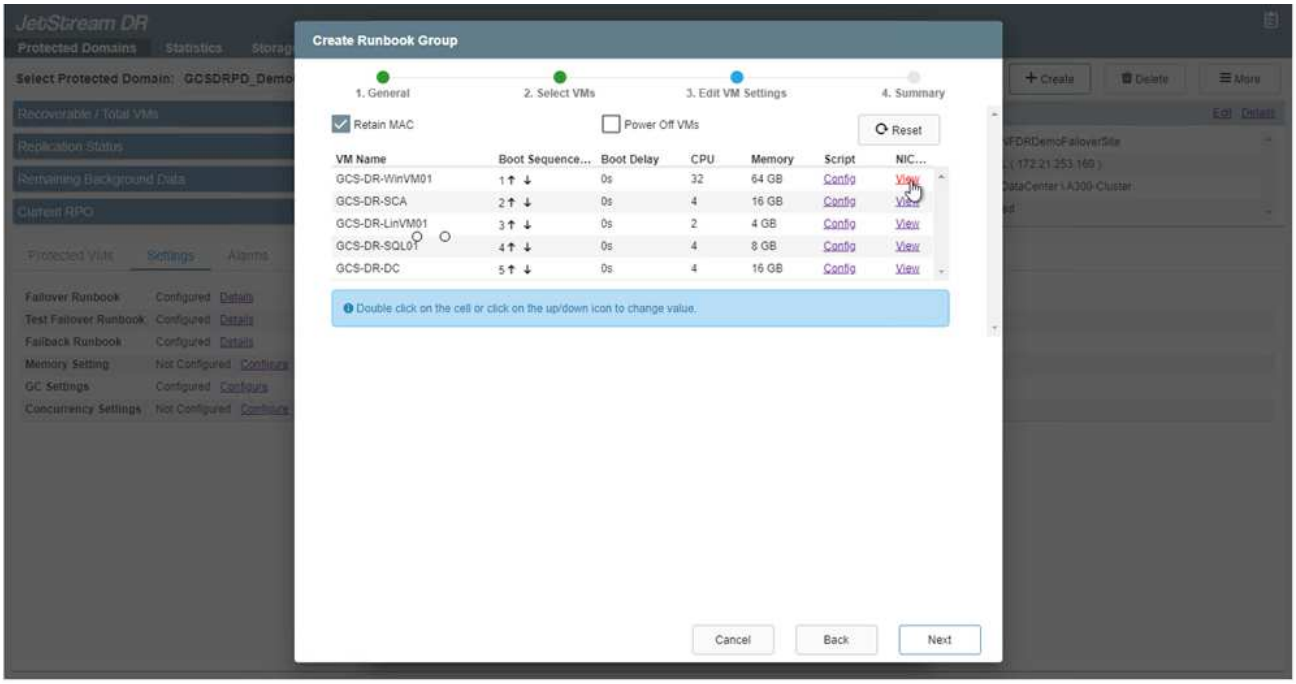
Si nécessaire, dans la partie inférieure de l'écran, appliquez des pré-scripts et des post-scripts personnalisés à exécuter automatiquement avant et après l'opération du groupe de runbooks. Assurez-vous que les scripts Runbook résident sur le serveur de gestion.



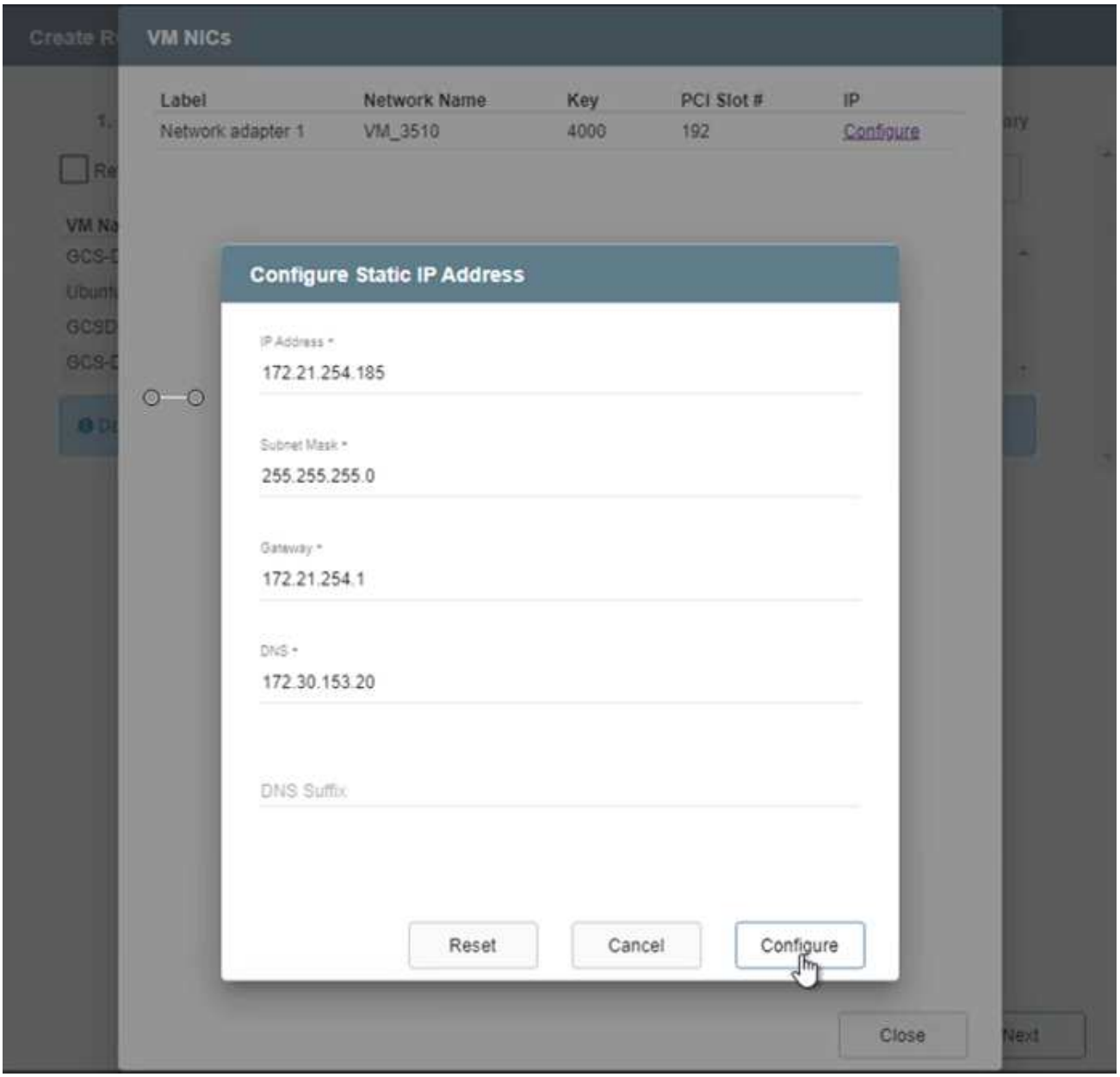
17. Modifiez les paramètres de la machine virtuelle selon vos besoins. Spécifiez les paramètres de récupération des machines virtuelles, notamment la séquence de démarrage, le délai de démarrage (spécifié en secondes), le nombre de processeurs et la quantité de mémoire à allouer. Modifiez la séquence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

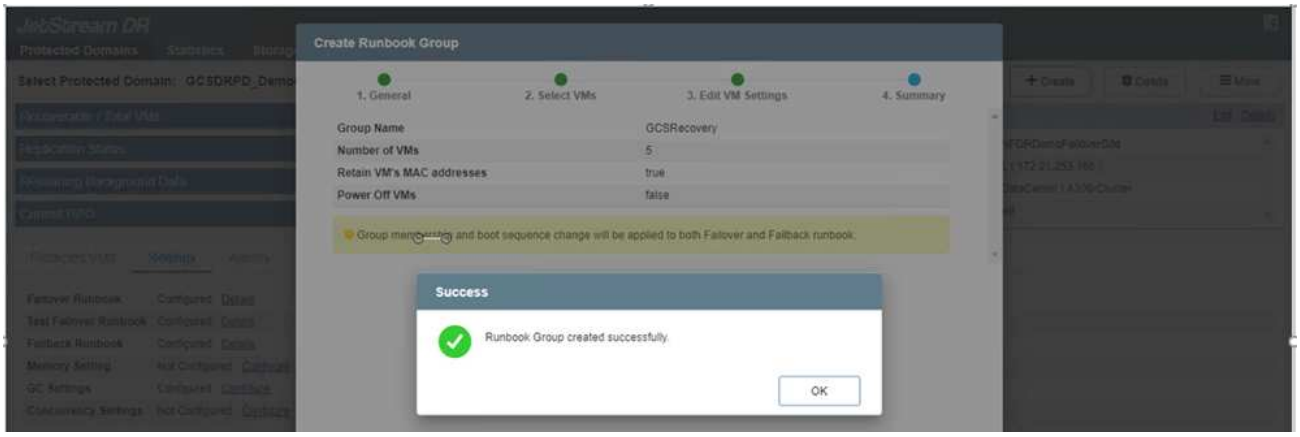


18. Les adresses IP statiques peuvent être configurées manuellement pour les machines virtuelles individuelles du groupe. Cliquez sur le lien Affichage NIC d'une machine virtuelle pour configurer manuellement ses paramètres d'adresse IP.



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





L’état des runbooks de basculement et de restauration est désormais répertorié comme Configuré. Les groupes de runbooks de basculement et de restauration sont créés par paires à l’aide du même groupe initial de machines virtuelles et de paramètres. Si nécessaire, les paramètres de n’importe quel groupe de runbook peuvent être personnalisés individuellement en cliquant sur son lien Détails respectif et en

apportant des modifications.

▼ Installer JetStream DR pour AVS dans un cloud privé

Une bonne pratique pour un site de récupération (AVS) consiste à créer à l'avance un cluster de voyants lumineux à trois nœuds. Cela permet de préconfigurer l'infrastructure du site de récupération, y compris les éléments suivants :

- Segments de réseau de destination, pare-feu, services tels que DHCP et DNS, etc.
- Installation de JetStream DR pour AVS
- Configuration des volumes ANF en tant que banques de données et plus

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

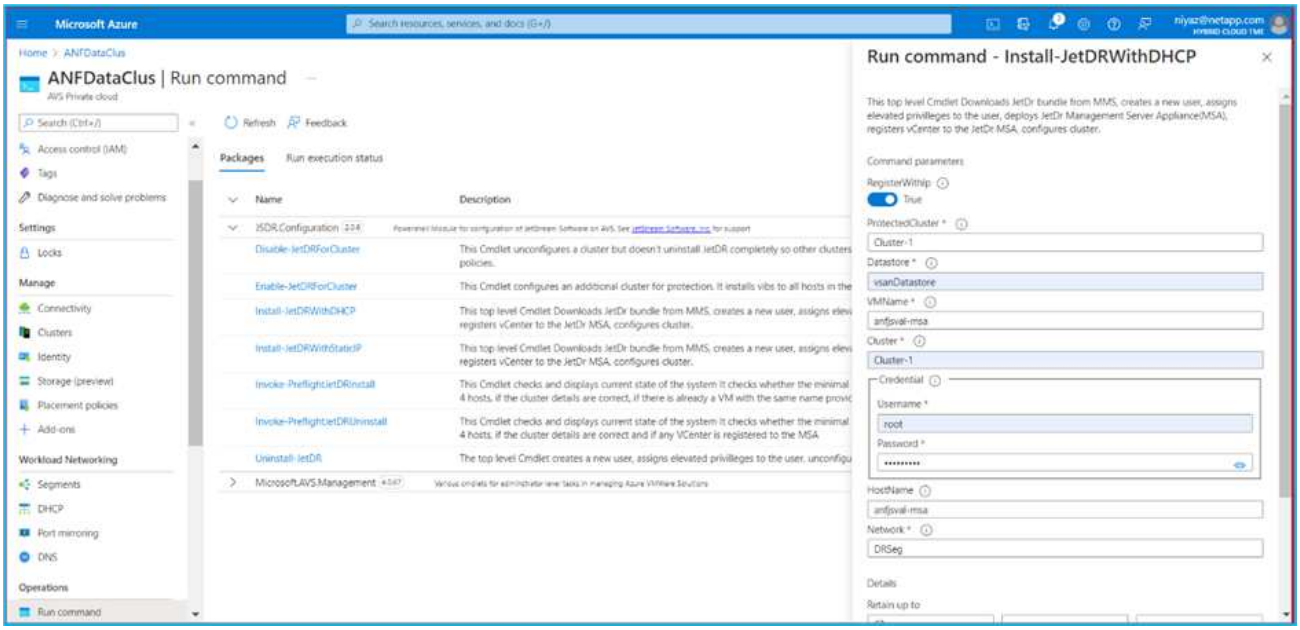
> ⓘ La configuration du réseau, y compris la création de segments, doit être configurée sur le cluster AVS pour correspondre aux exigences locales.

> ⓘ En fonction des exigences SLA et RTO, vous pouvez utiliser le mode de basculement continu ou le mode de basculement standard. Pour un RTO proche de zéro, vous devez commencer la réhydratation continue au site de récupération.

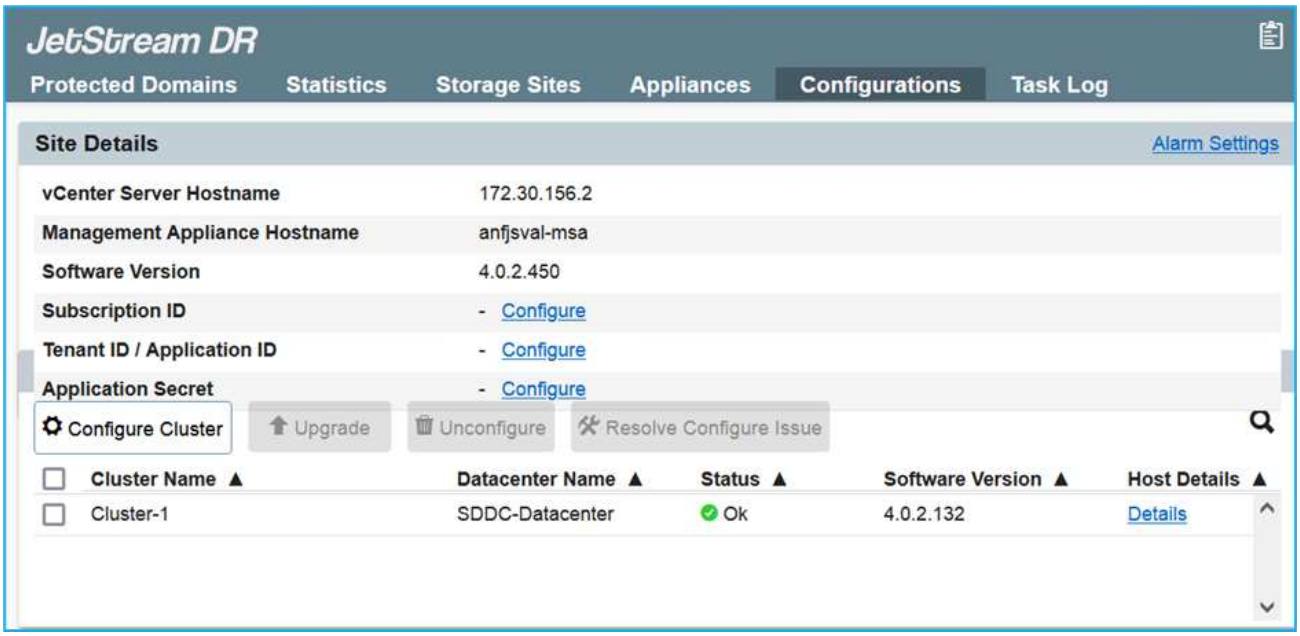
1. Pour installer JetStream DR pour AVS sur un cloud privé Azure VMware Solution, utilisez la commande Exécuter. Depuis le portail Azure, accédez à la solution Azure VMware, sélectionnez le cloud privé, puis sélectionnez Exécuter la commande > Packages > JSDR.Configuration.

   > ⓘ L'utilisateur CloudAdmin par défaut de la solution Azure VMware ne dispose pas de 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.

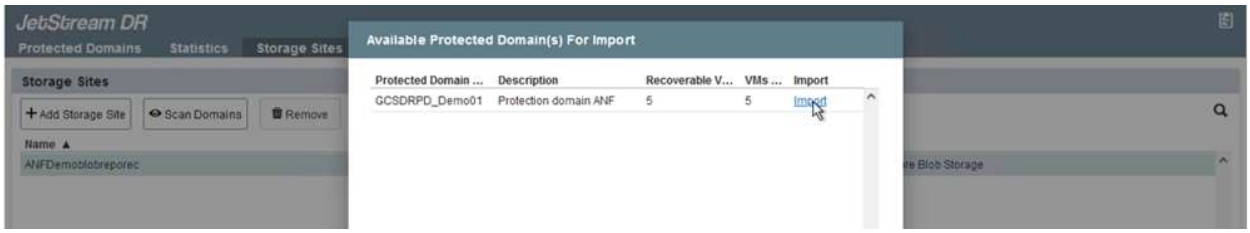
   La capture d'écran suivante montre l'installation à l'aide d'une adresse IP basée sur DHCP.



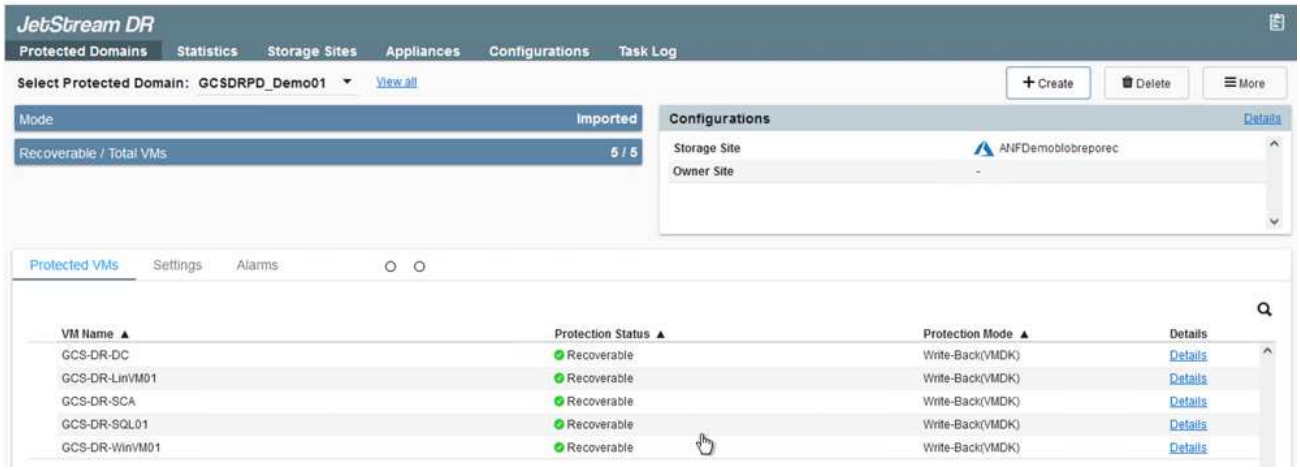
2. Une fois l'installation de JetStream DR pour AVS terminée, actualisez le navigateur. Pour accéder à l'interface utilisateur de JetStream DR, accédez à SDDC Datacenter > Configurer > JetStream DR.



3. Depuis l'interface JetStream DR, effectuez les tâches suivantes :
   a. Ajoutez le compte de stockage d'objets blob Azure qui a été utilisé pour protéger le cluster local en tant que site de stockage, puis exécutez l'option Analyser les domaines.
   b. Dans la fenêtre de dialogue contextuelle qui s'affiche, sélectionnez le domaine protégé à importer, puis cliquez sur son lien Importer.



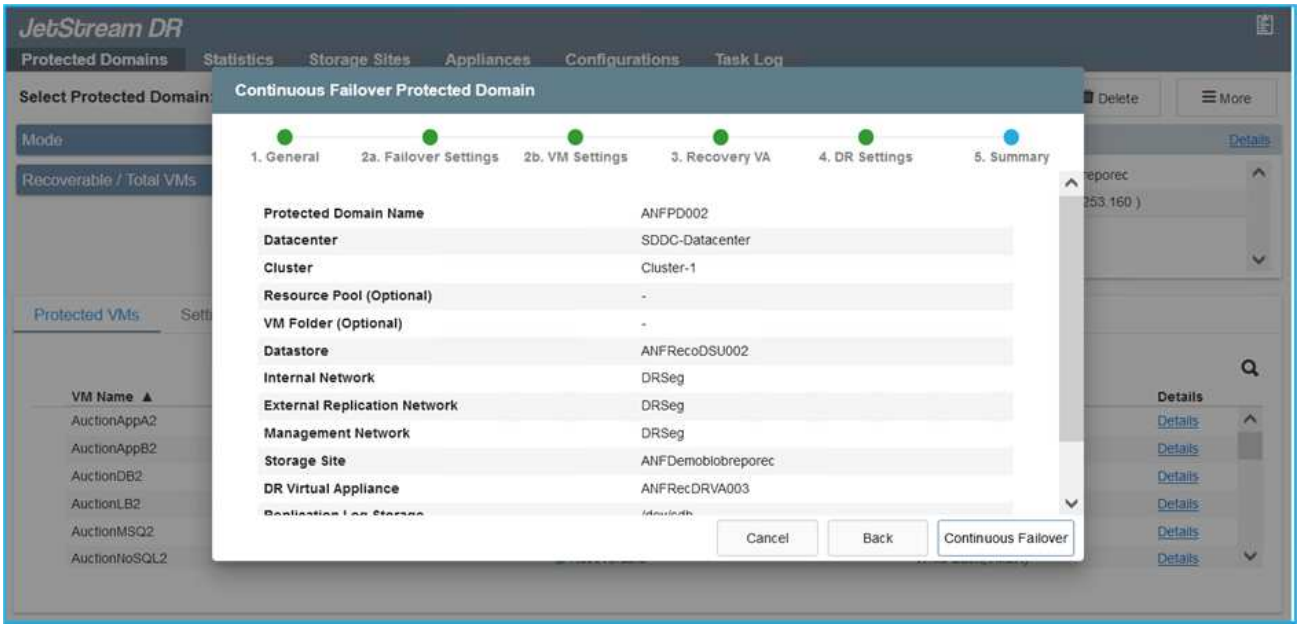
4. Le domaine est importé pour récupération. Accédez à l'onglet Domaines protégés et vérifiez que le domaine souhaité a été sélectionné ou choisissez celui souhaité dans le menu Sélectionner un domaine protégé. Une liste des machines virtuelles récupérables dans le domaine protégé s'affiche.



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

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

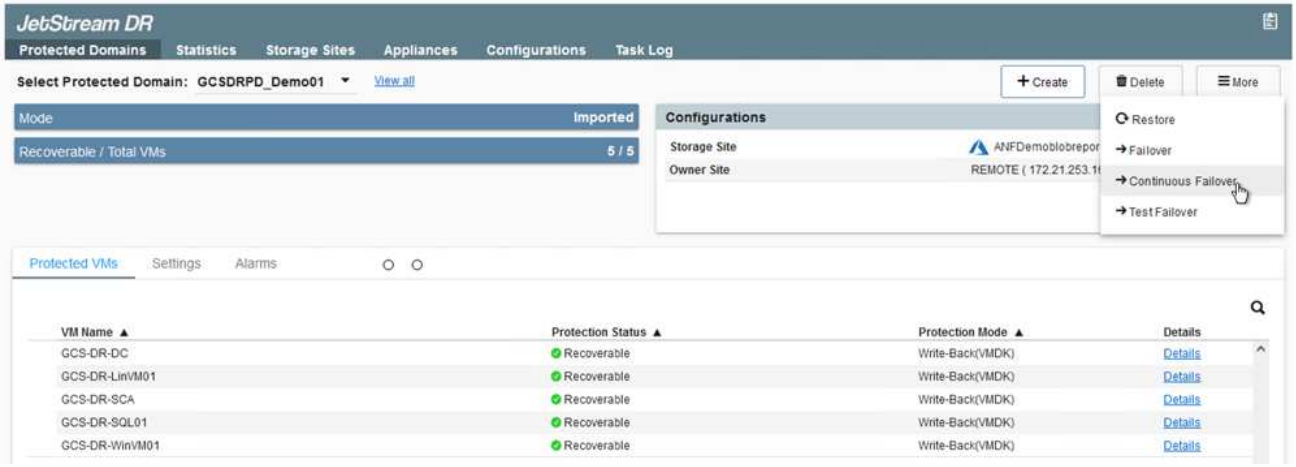
6. Créez des volumes de journaux de réplication à l'aide des banques de données vSAN ou ANF disponibles.
7. Importez les domaines protégés et configurez l'AV de récupération pour utiliser une banque de données ANF pour les placements de machines virtuelles.



Assurez-vous que DHCP est activé sur le segment sélectionné et que suffisamment d'adresses IP sont disponibles. Les adresses IP dynamiques sont utilisées temporairement pendant la récupération des domaines. Chaque VM en cours de récupération (y compris la réhydratation continue) nécessite une IP dynamique individuelle. Une fois la récupération terminée, l'IP est libérée et peut être réutilisée.

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

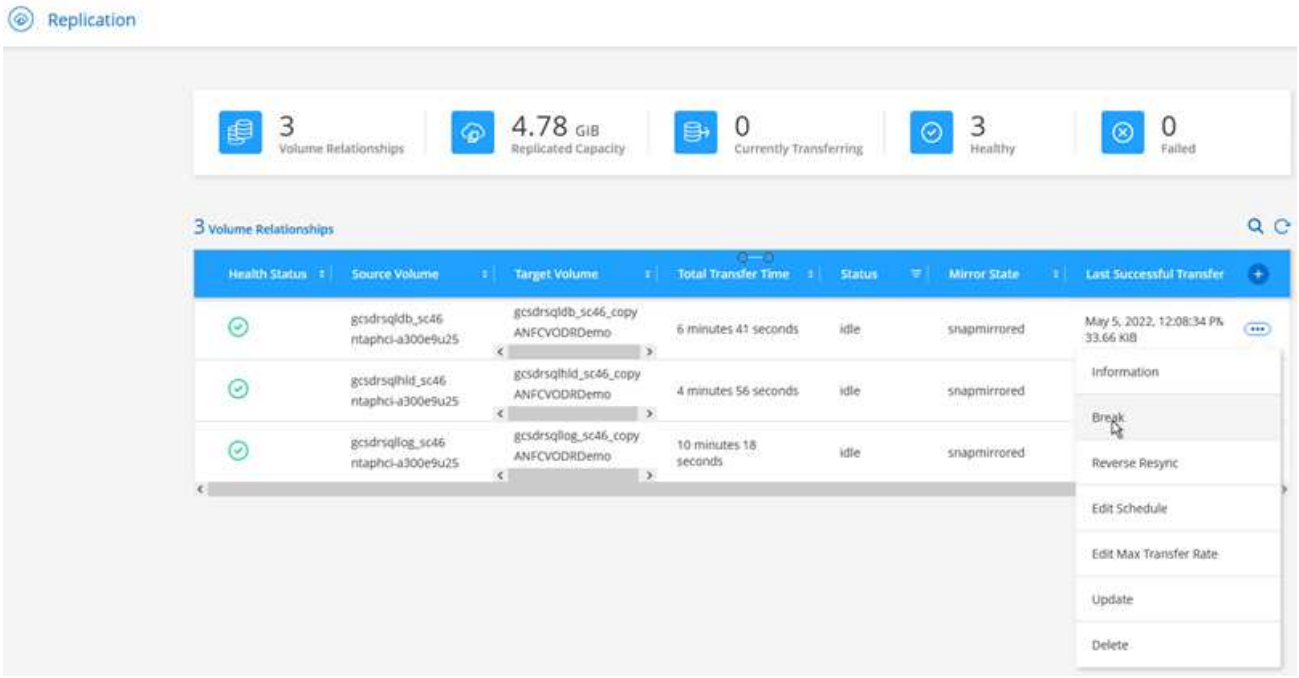
Bien que les modes de basculement continu et de basculement diffèrent selon le moment où la configuration est effectuée, les deux modes de basculement sont configurés à l'aide des mêmes étapes. Les étapes de basculement sont configurées et exécutées ensemble en réponse à un événement catastrophique. Le basculement continu peut être configuré à tout moment, puis autorisé à s'exécuter en arrière-plan pendant le fonctionnement normal du système. Après un événement catastrophique, un basculement continu est effectué pour transférer immédiatement la propriété des machines virtuelles protégées vers le site de récupération (RTO proche de zéro).

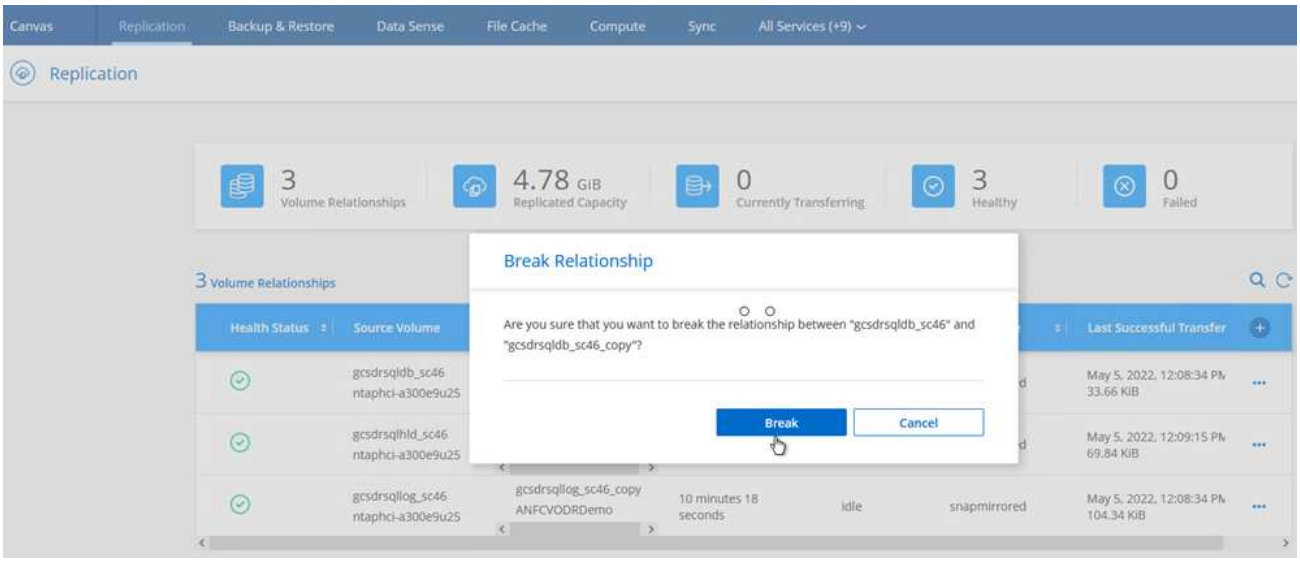


Le processus de basculement continu commence et sa progression peut être surveillée à partir de l'interface utilisateur. Cliquer sur l'icône bleue dans la section Étape actuelle affiche une fenêtre contextuelle affichant les détails de l'étape actuelle du processus de basculement.

▼ **Basculement et restauration automatique**

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

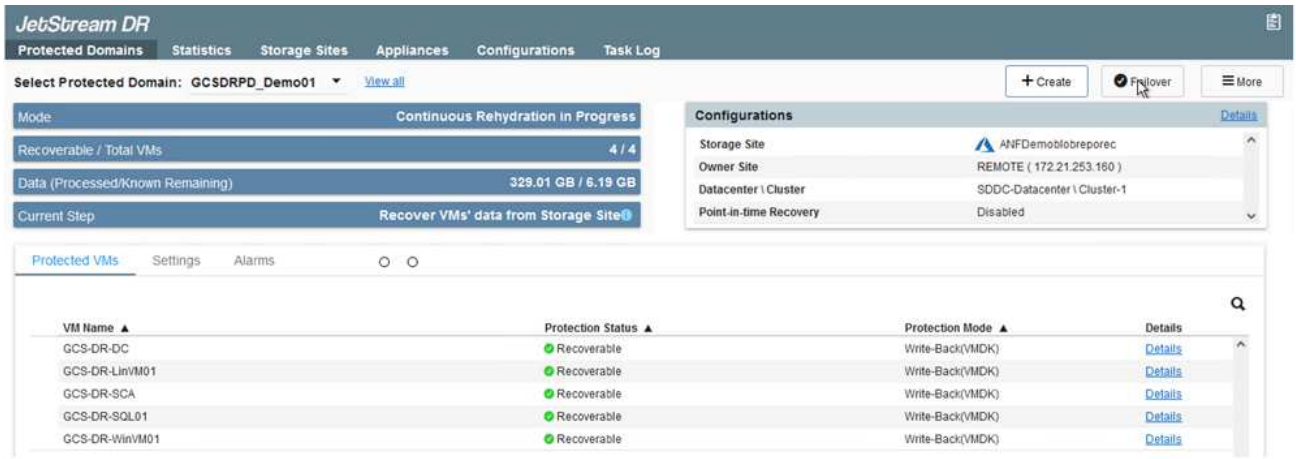


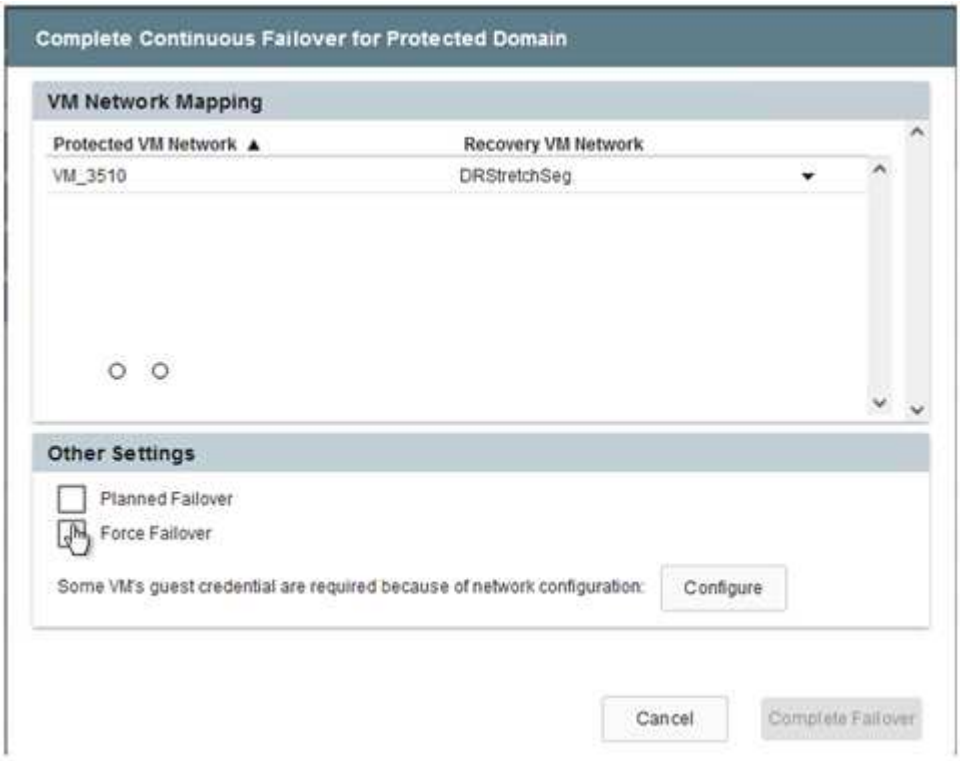


Cette étape peut facilement être automatisée pour faciliter le processus de récupération.

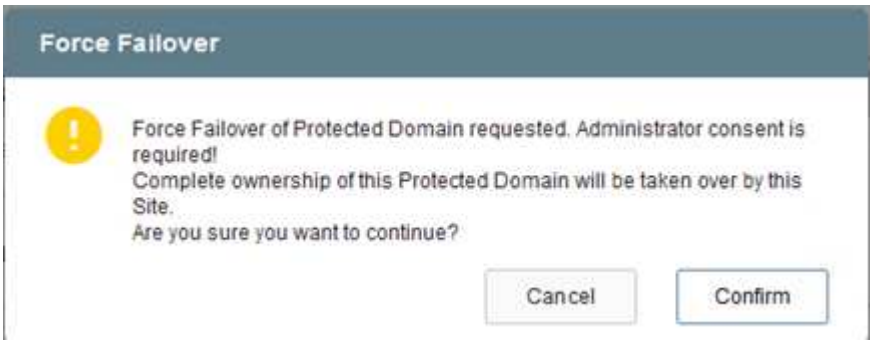
2. Accédez à l'interface utilisateur Jetstream sur AVS SDDC (côté destination) et déclenchez l'option de basculement pour terminer le basculement. La barre des tâches affiche la progression des activités de basculement.

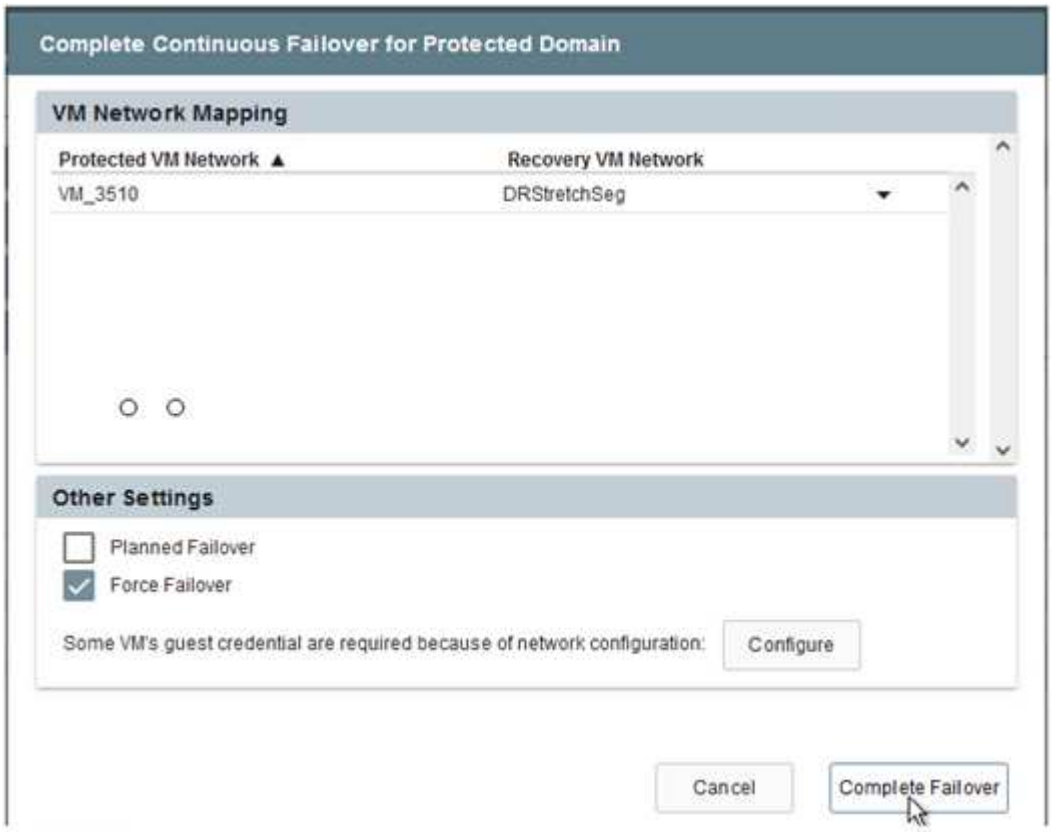
   Dans la fenêtre de dialogue qui s'affiche une fois le basculement terminé, la tâche de basculement peut être spécifiée comme planifiée ou supposée forcée.





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





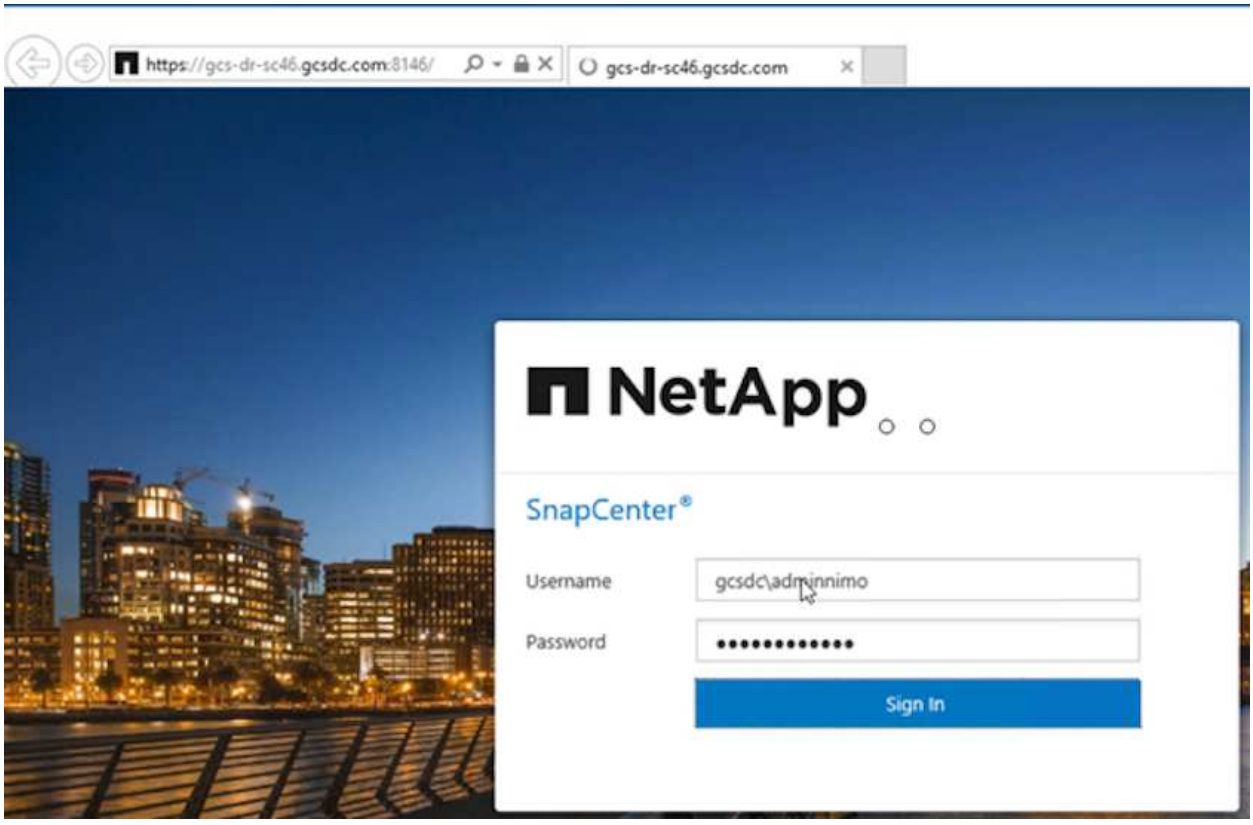
3. Une fois le basculement continu terminé, un message s'affiche confirmant la fin de la tâche. Une fois la tâche terminée, accédez aux machines virtuelles récupérées pour configurer les sessions ISCSI ou NFS.

Le mode de basculement passe à Exécution en mode de basculement et l'état de la machine virtuelle est Récupérable. Toutes les machines virtuelles du domaine protégé s'exécutent désormais sur le site de récupération dans l'état spécifié par les paramètres du runbook de basculement.

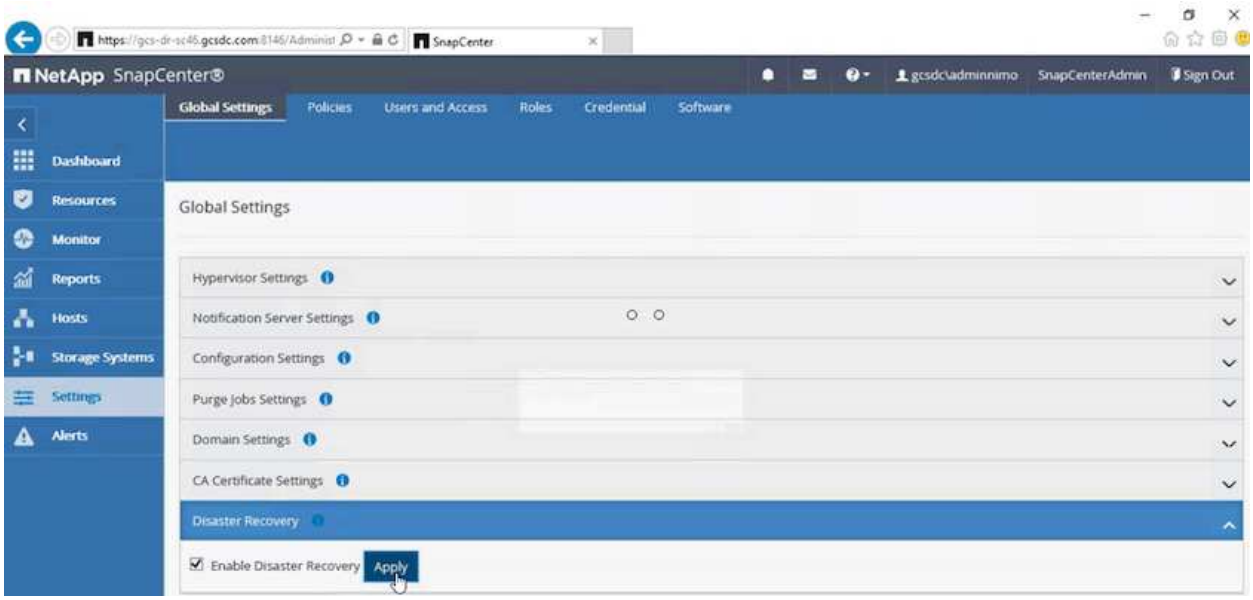
Pour vérifier la configuration et l'infrastructure de basculement, JetStream DR peut être utilisé en mode test (option Test Failover) pour observer la récupération des machines virtuelles et de leurs données depuis le magasin d'objets vers un environnement de récupération de test. Lorsqu'une procédure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



4. Une fois les machines virtuelles récupérées, utilisez la récupération après sinistre du stockage pour le stockage en invité. Pour illustrer ce processus, le serveur SQL 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 de SnapCenter à l'aide du navigateurN.



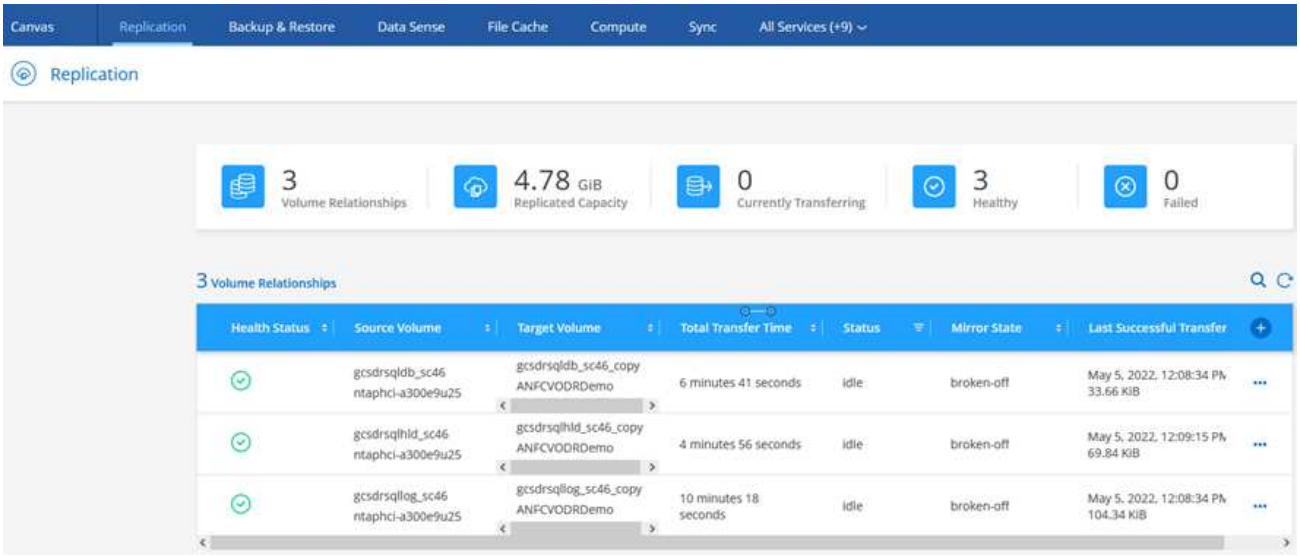
   b. Dans la page Paramètres, accédez à Paramètres > Paramètres globaux > Reprise après sinistre.
   c. Sélectionnez Activer la récupération après sinistre.
   d. Cliquez sur Appliquer.



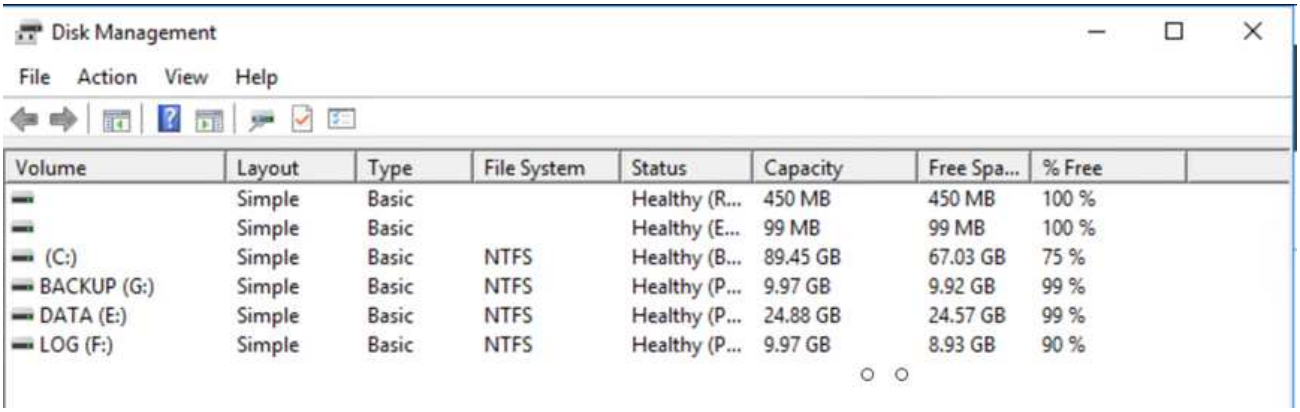
e. Vérifiez si la tâche DR est activée en cliquant sur Surveiller > Tâches.

> NetApp SnapCenter 4.6 ou version ultérieure doit être utilisé pour la récupération après sinistre du stockage. Pour les versions précédentes, des snapshots cohérents avec l'application (répliqués à l'aide de SnapMirror) doivent être utilisés et une récupération manuelle doit être exécutée au cas où des sauvegardes précédentes doivent être récupérées sur le site de reprise après sinistre.

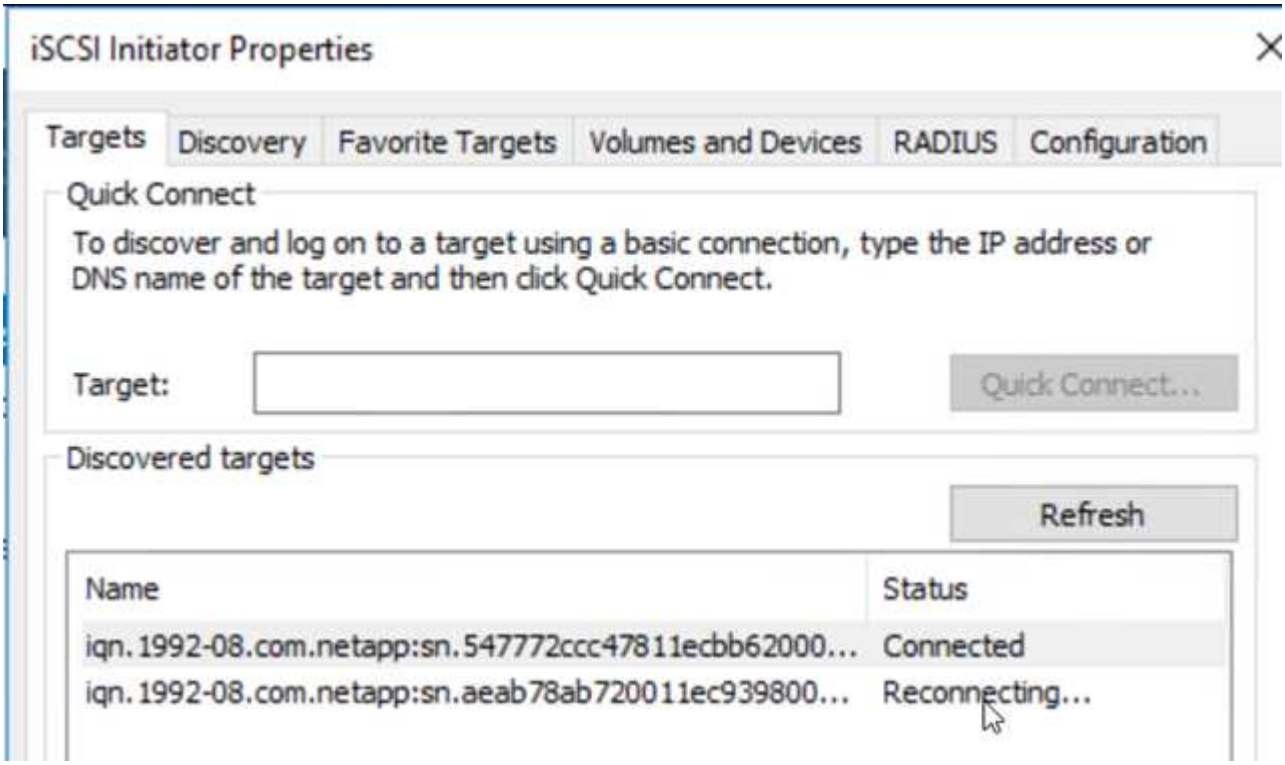
6. Assurez-vous que la relation SnapMirror est rompue.



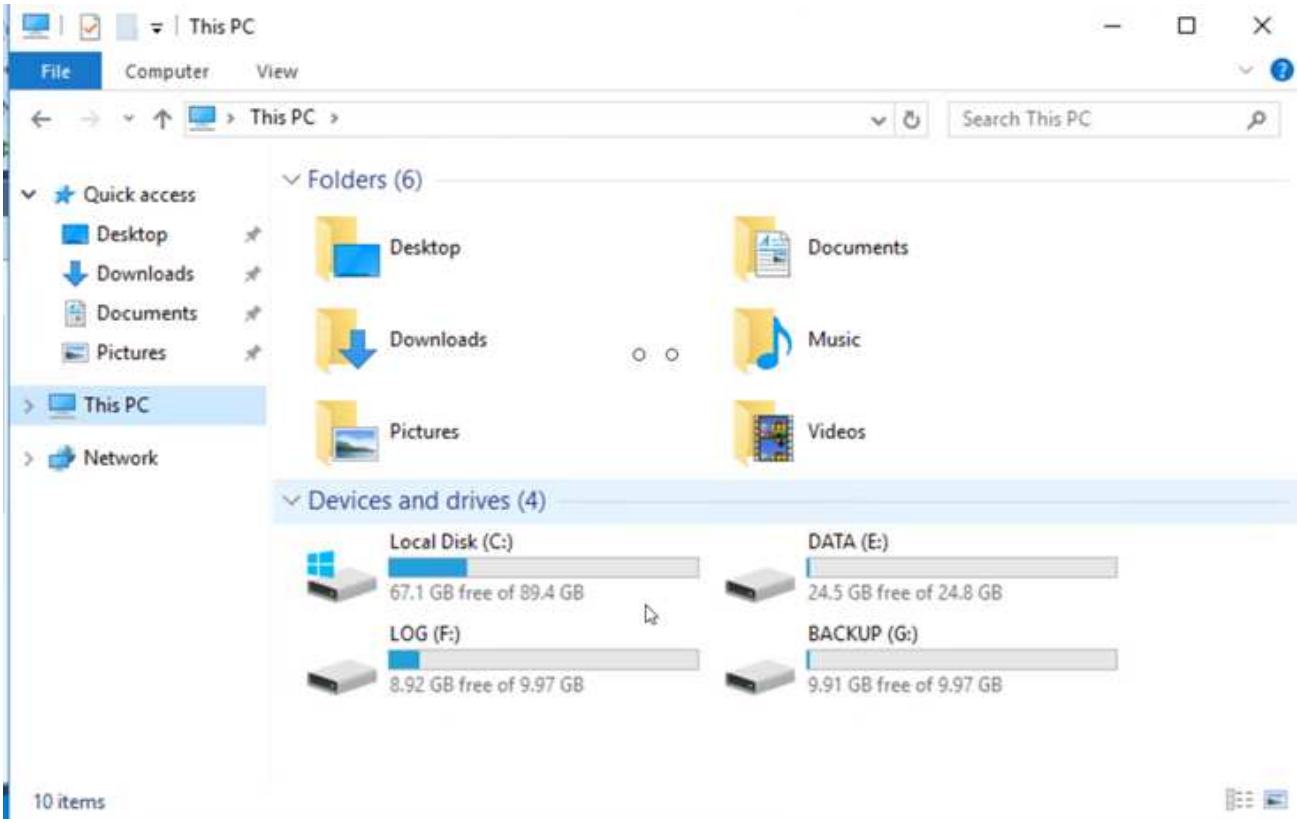
7. Attachez le LUN de Cloud Volumes ONTAP à la machine virtuelle invitée SQL récupérée avec les mêmes lettres de lecteur.



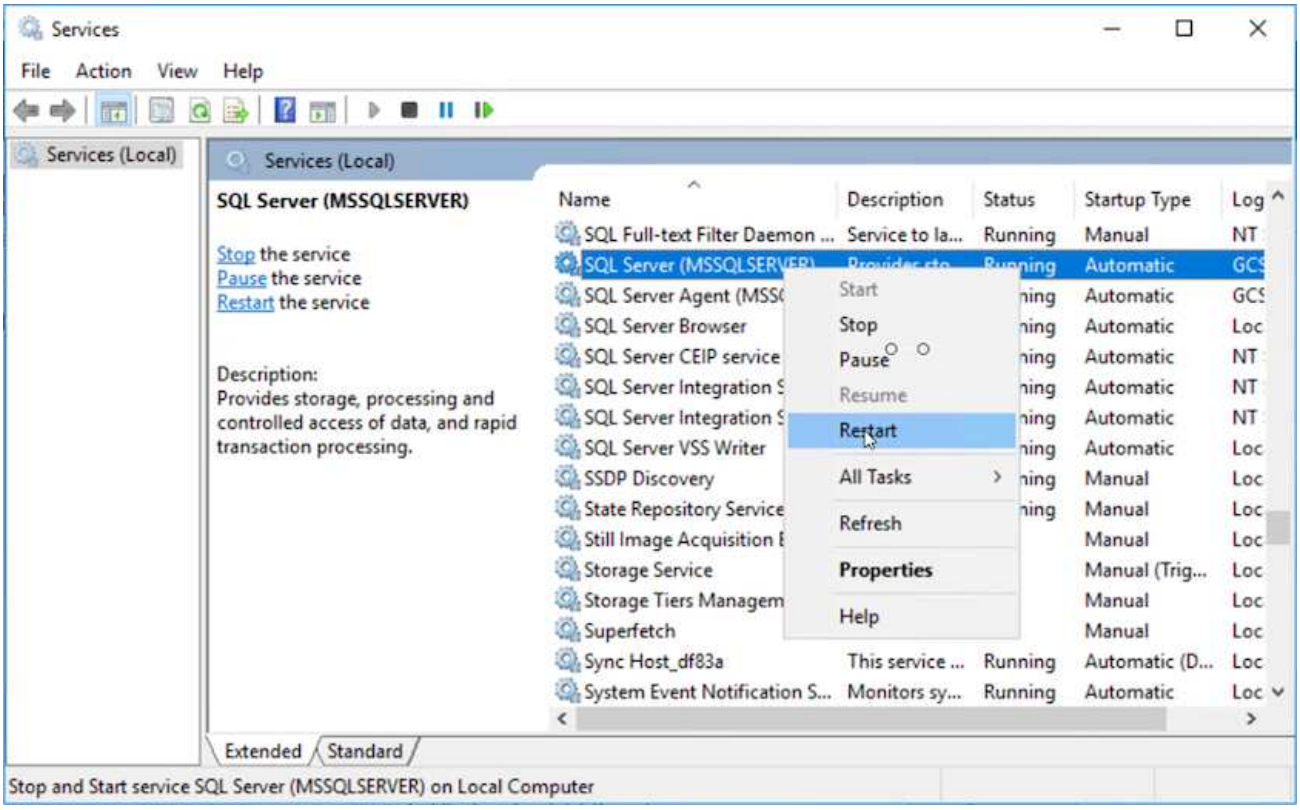
8. Ouvrez l'initiateur iSCSI, effacez la session déconnectée précédente et ajoutez la nouvelle cible avec le multipath pour les volumes Cloud Volumes ONTAP répliqués.



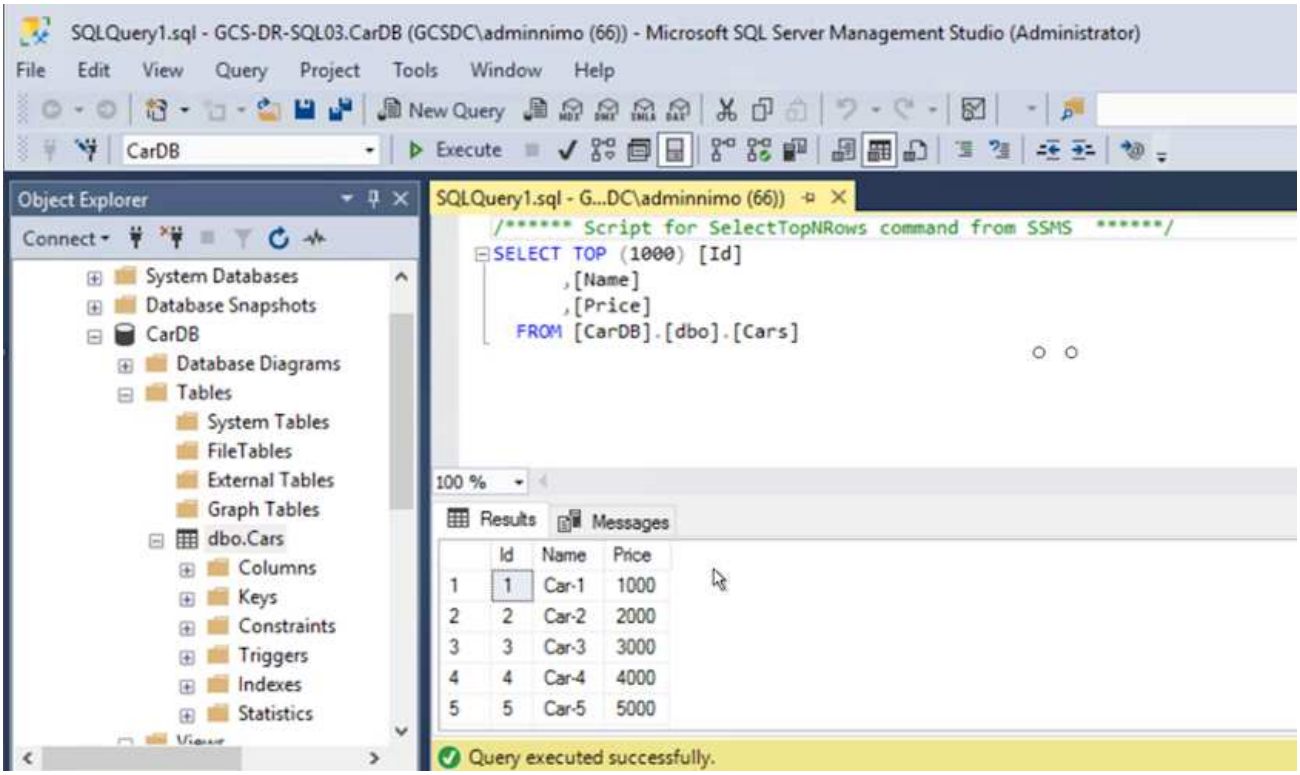
9. Assurez-vous que tous les disques sont connectés à l'aide des mêmes lettres de lecteur que celles utilisées avant DR.



10. Redémarrez le service serveur MSSQL.



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



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

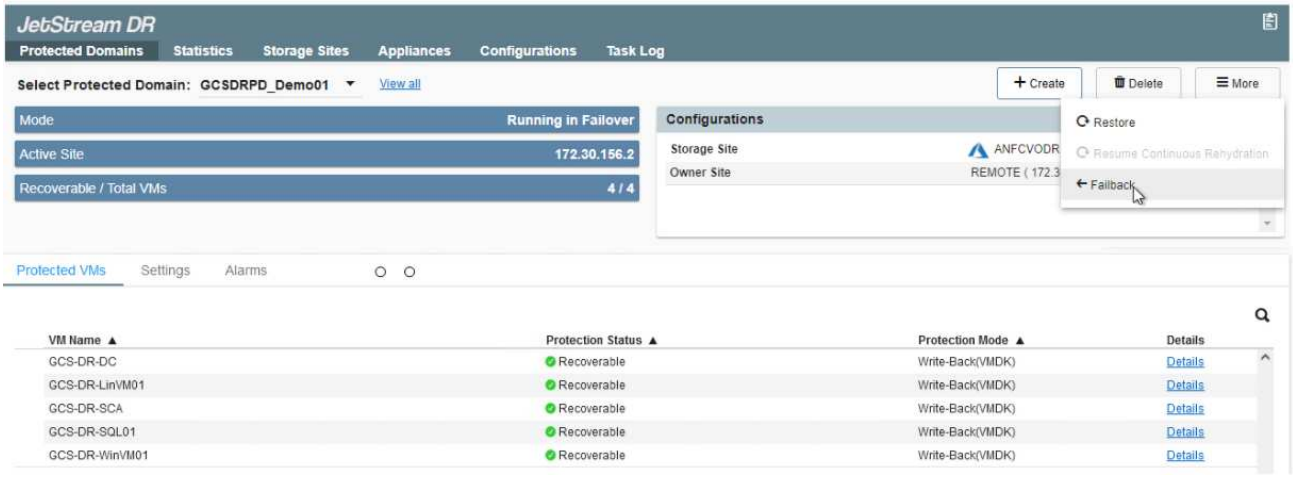
À ce stade, les opérations peuvent être exécutées et les affaires continuent normalement.

Du côté NSX-T, une passerelle de niveau 1 dédiée distincte peut être créée pour simuler des scénarios de basculement. Cela garantit que toutes les charges de travail peuvent communiquer entre elles, mais qu'aucun trafic ne peut entrer ou sortir de l'environnement, de sorte que toutes les tâches de triage, de confinement ou de renforcement peuvent être effectuées sans risque de contamination croisée. Cette opération n'entre pas dans le cadre de ce document, mais elle peut être facilement réalisée pour simuler l'isolement.

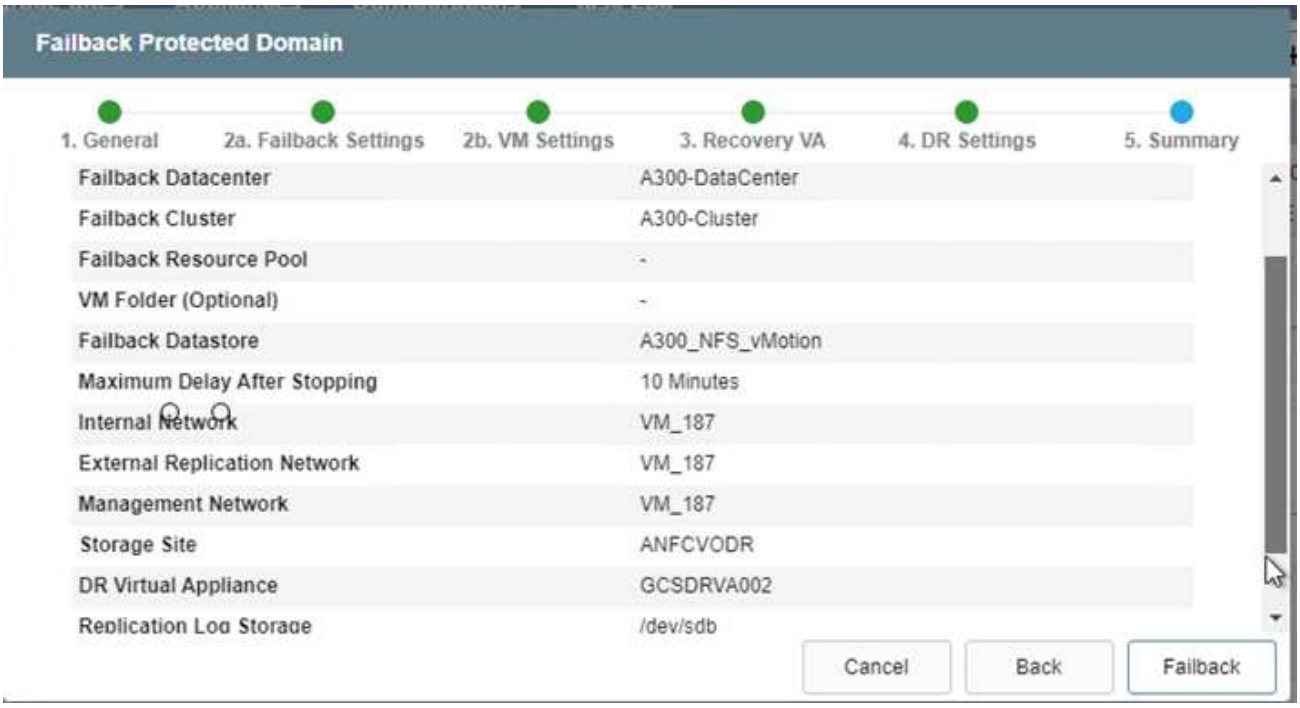
Une fois le site principal à nouveau opérationnel, vous pouvez effectuer une restauration automatique. La protection de la machine virtuelle est reprise par Jetstream et la relation SnapMirror doit être inversée.

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

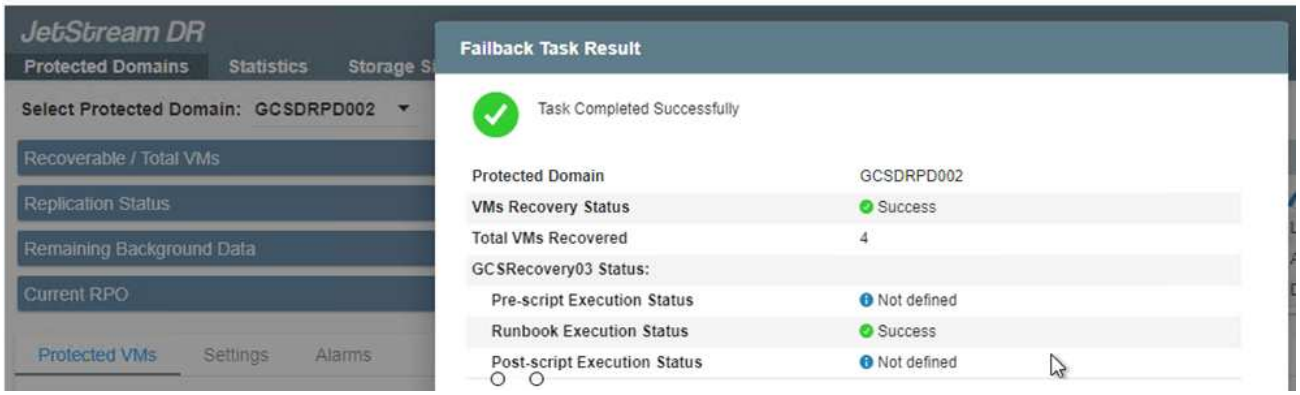
Le plan de restauration automatique généré par CPT peut également être utilisé pour initier le retour des machines virtuelles et de leurs données du magasin d'objets vers l'environnement VMware d'origine.



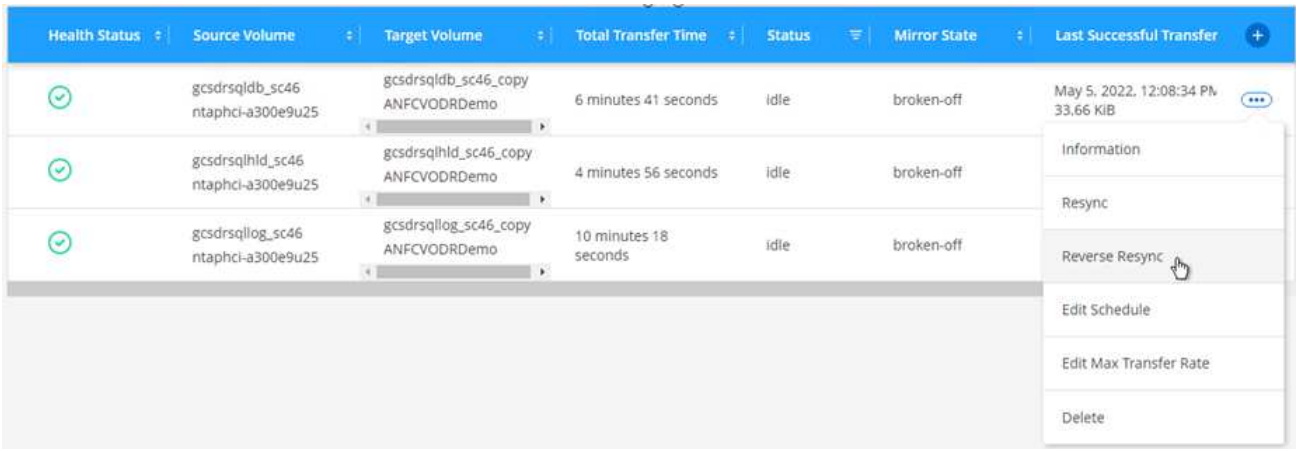
Spécifiez le délai maximal après la mise en pause des machines virtuelles sur le site de récupération et leur redémarrage sur le site protégé. Le temps nécessaire pour terminer ce processus comprend l'achèvement de la réplication après l'arrêt des machines virtuelles de basculement, le temps nécessaire pour nettoyer le site de récupération et le temps nécessaire pour recréer les machines virtuelles dans le site protégé. NetApp recommande 10 minutes.

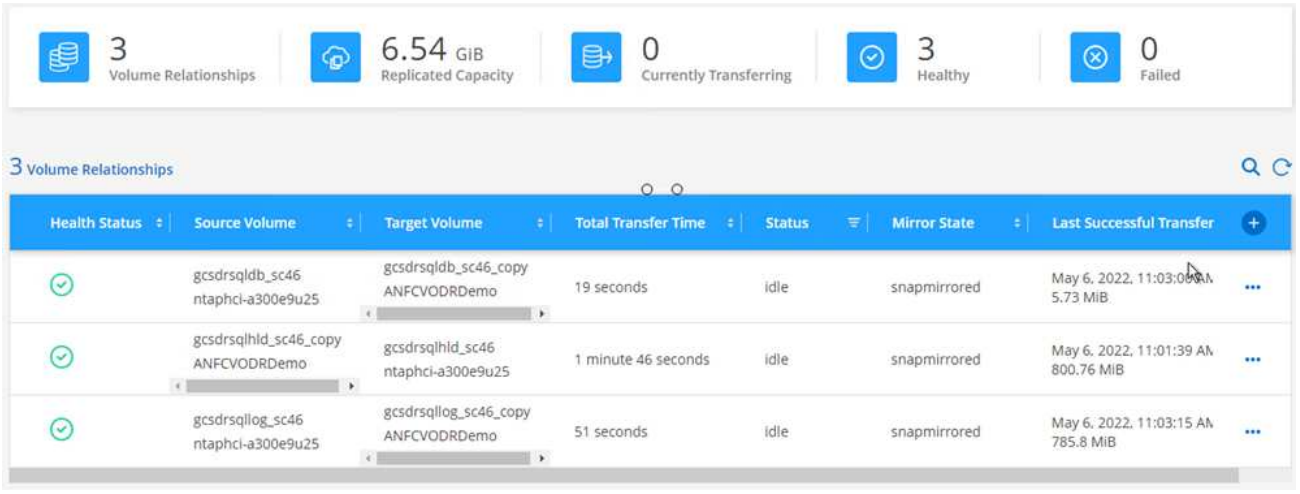


3. Terminez le processus de restauration automatique, puis confirmez la reprise de la protection de la machine virtuelle et de la cohérence des données.

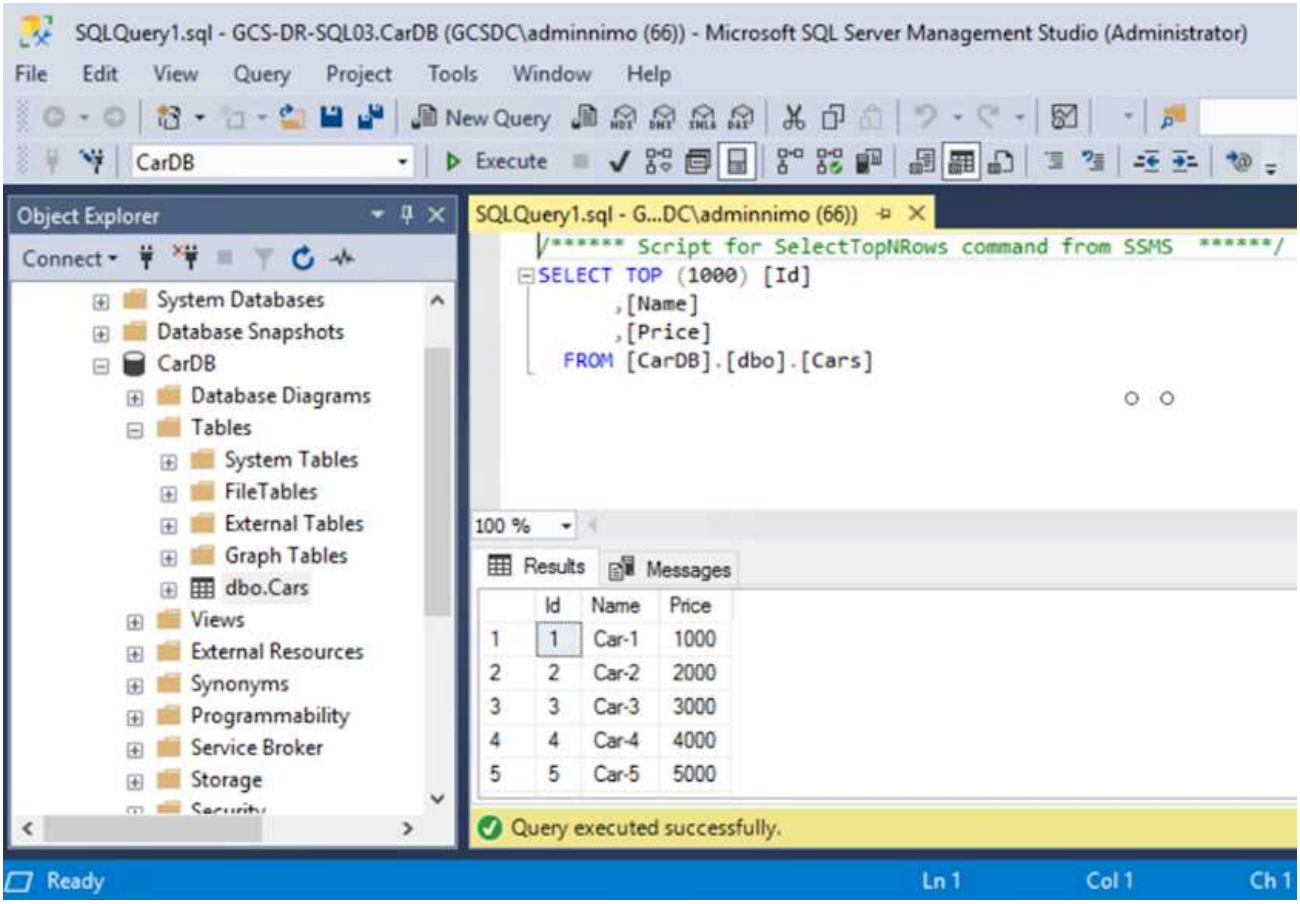


4. Une fois les machines virtuelles récupérées, déconnectez le stockage secondaire de l'hôte et connectez-vous au stockage principal.





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



Pour revenir au stockage principal, assurez-vous 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 principal et secondaire après l'opération de resynchronisation inverse, effectuez à nouveau l'opération de resynchronisation inverse.

Ce processus est applicable à d'autres applications comme Oracle, à des versions de bases de données similaires et à toute autre application utilisant un stockage connecté en tant qu'invité.

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

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Récupère à n'importe quel point disponible dans le temps avec la conservation des instantanés ONTAP .
- L'automatisation complète est disponible pour toutes les étapes requises pour récupérer des centaines à des milliers de machines virtuelles, depuis les étapes de stockage, de calcul, de réseau et de validation des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela évite le risque de corruption des données pour les volumes et les instantanés.
  - Évite les interruptions de réplication pendant les flux de travail de test DR.
  - Exploite les données DR pour les flux de travail au-delà de DR, 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 du processeur et de la RAM peut contribuer à réduire les coûts du cloud en permettant la récupération vers des clusters de calcul plus petits.

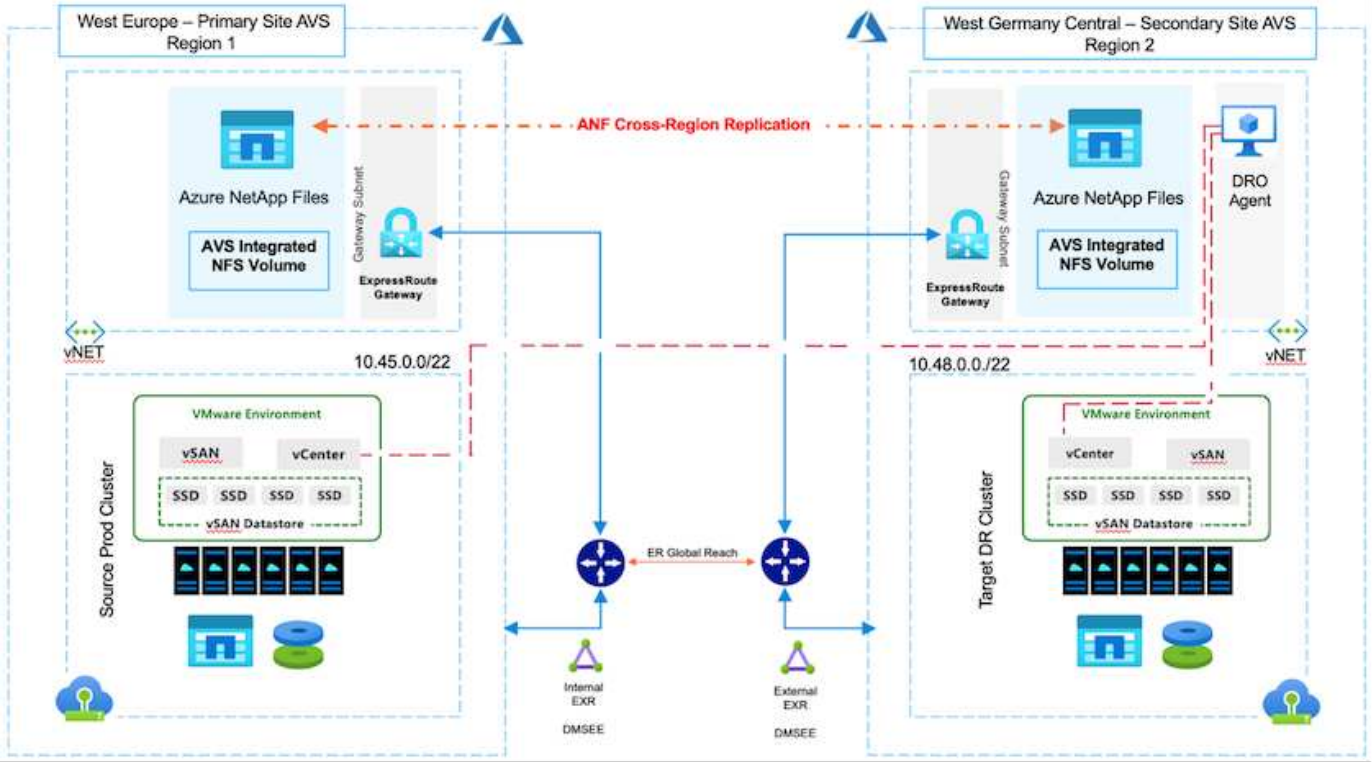
TR-4955 : Reprise après sinistre avec Azure NetApp Files (ANF) et Azure VMware Solution (AVS)

La reprise après sinistre utilisant la réplication au niveau des blocs entre les régions du cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données (par exemple, les ransomwares).

Aperçu

Avec la réplication de volume interrégionale Azure NetApp Files (ANF), les charges de travail VMware exécutées sur un site SDDC Azure VMware Solution (AVS) utilisant des volumes Azure NetApp Files comme banque de données NFS sur le site AVS principal peuvent être répliquées vers un site AVS secondaire désigné dans la région de récupération cible.

Disaster Recovery Orchestrator (DRO) (une solution scriptée avec une interface utilisateur) peut être utilisé pour récupérer de manière transparente les charges de travail répliquées d'un SDDC AVS vers un autre. DRO automatise la récupération en interrompant le peering de réplication, puis en montant le volume de destination en tant que banque de données, via l'enregistrement de la machine virtuelle sur AVS, vers des mappages réseau directement sur NSX-T (inclus avec tous les clouds privés AVS).



Prérequis et recommandations générales

- Vérifiez que vous avez activé la réplication interrégionale en créant un peering de réplication. Voir "Créer une réplication de volume pour Azure NetApp Files" .
- Vous devez configurer ExpressRoute Global Reach entre les clouds privés Azure VMware Solution source

et cible.

- Vous devez disposer d'un principal de service pouvant accéder aux ressources.
- La topologie suivante est prise en charge : site AVS principal vers site AVS secondaire.
- Configurer le "réplication" planifier chaque volume de manière appropriée en fonction des besoins de l'entreprise et du taux de modification des données.

Les topologies en cascade et en éventail ne sont pas prises en charge.

Commencer

Déployer la solution Azure VMware

Le "Solution Azure VMware" (AVS) est un service cloud hybride qui fournit des SDDC VMware entièrement fonctionnels au sein d'un cloud public Microsoft Azure. AVS est une solution propriétaire entièrement gérée et prise en charge par Microsoft et 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 profitant de la présence mondiale de Microsoft Azure, des installations de centre de données de pointe et de la proximité du riche écosystème de services et de solutions Azure natifs. Une combinaison d'Azure VMware Solution SDDC et Azure NetApp Files offre les meilleures performances avec une latence réseau minimale.

Pour configurer un cloud privé AVS sur Azure, suivez les étapes décrites dans cet article."lien" pour la documentation NetApp et dans ce "lien" pour la documentation Microsoft. Un environnement de veilleuse configuré avec une configuration minimale peut être utilisé à des fins de reprise après sinistre. Cette configuration contient uniquement les composants principaux pour prendre en charge les applications critiques et peut évoluer et générer davantage d'hôtes pour prendre en charge la majeure partie de la charge en cas de basculement.

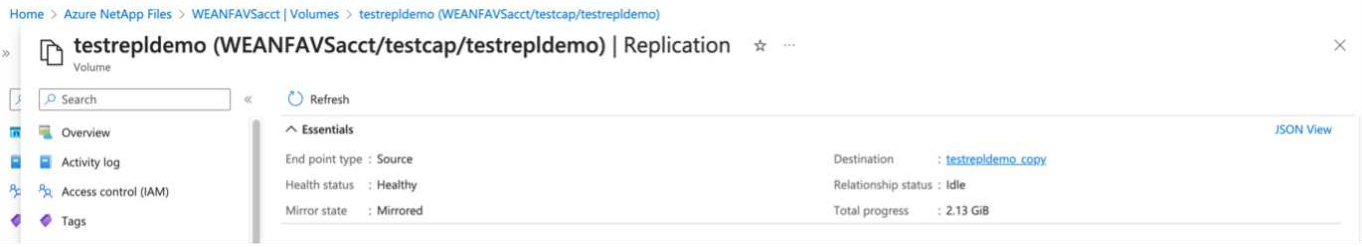
Dans la version initiale, DRO prend en charge un cluster AVS SDDC existant. La création de SDDC à la demande sera disponible dans une prochaine version.

Provisionner et configurer Azure NetApp Files

"Azure NetApp Files"est un service de stockage de fichiers à hautes performances, de niveau entreprise et mesuré. Suivez les étapes de cette "lien" pour provisionner et configurer Azure NetApp Files en tant que banque de données NFS afin d'optimiser les déploiements de cloud privé AVS.

Créer une réplication de volume pour les volumes de banque de données alimentés par Azure NetApp Files

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



Suivez les étapes de cette "lien" pour configurer la réplication inter-régionale en créant un peering de

réplication. Le niveau de service du pool de capacité de destination peut correspondre à celui du pool de capacité source. Cependant, pour ce cas d'utilisation spécifique, vous pouvez sélectionner le niveau de service standard, puis "modifier le niveau de service" en cas de catastrophe réelle ou de simulations DR.

> Une relation de réplication inter-régionale est une condition préalable 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 remplir les conditions préalables. Ensuite, installez le package.

Prérequis :

- Principal de service pouvant accéder aux ressources.
- Assurez-vous qu'une connectivité appropriée existe avec les instances SDDC source et de destination et Azure NetApp Files .
- La résolution DNS doit être en place si vous utilisez des noms DNS. Sinon, utilisez les adresses IP pour vCenter.

Configuration requise pour le système d'exploitation :

- Ubuntu Focal 20.04 (LTS)Les packages suivants doivent être installés sur la machine virtuelle de l'agent désigné :
- Docker
- Docker-compose
- JqChange `docker.sock` à cette nouvelle permission : `sudo chmod 666 /var/run/docker.sock` .

> Le `deploy.sh` le script exécute tous les prérequis requis.

Les étapes sont les suivantes :

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

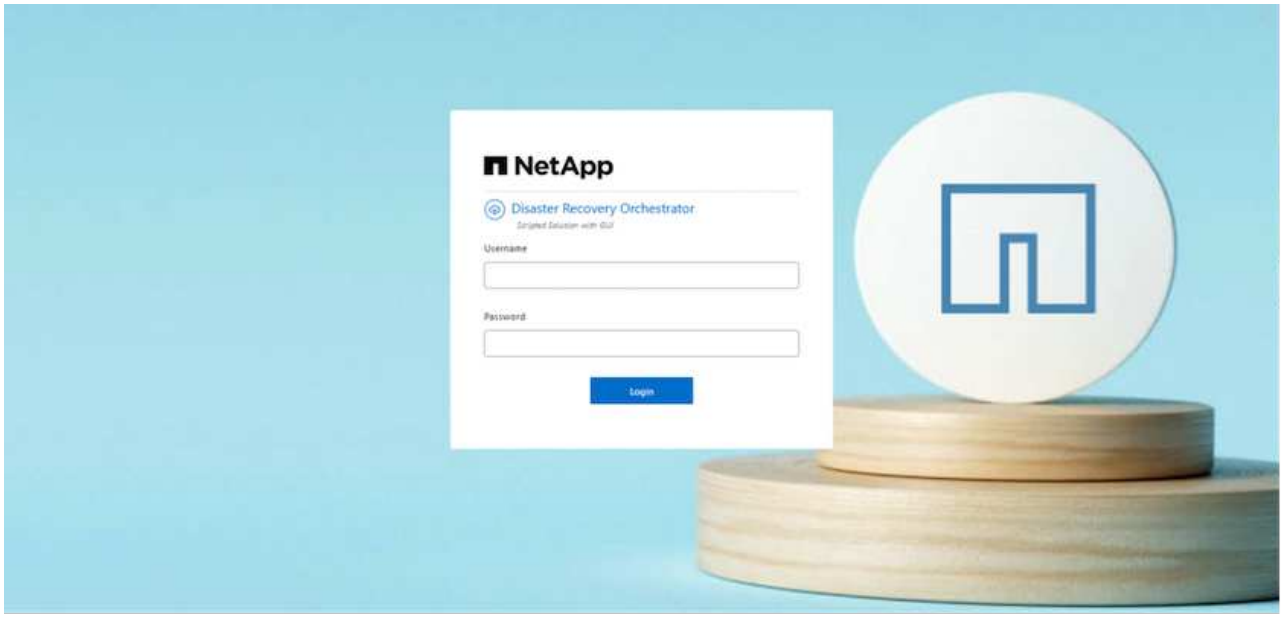
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> 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 distincte de celle du 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 Azure NetApp Files et AVS correctement configurés, vous pouvez commencer à configurer DRO pour automatiser la récupération des charges de travail 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 afin 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 une autorisation pour 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 informations d'identification Azure dont DRO a besoin. Vous devez lier le principal du service à votre abonnement Azure et lui attribuer un rôle personnalisé disposant des autorisations requises. Lorsque vous ajoutez des environnements source et de destination, vous êtes invité à sélectionner les informations d'identification associées au principal du service. Vous devez ajouter ces informations d'identification à DRO avant de pouvoir cliquer sur Ajouter un nouveau site.

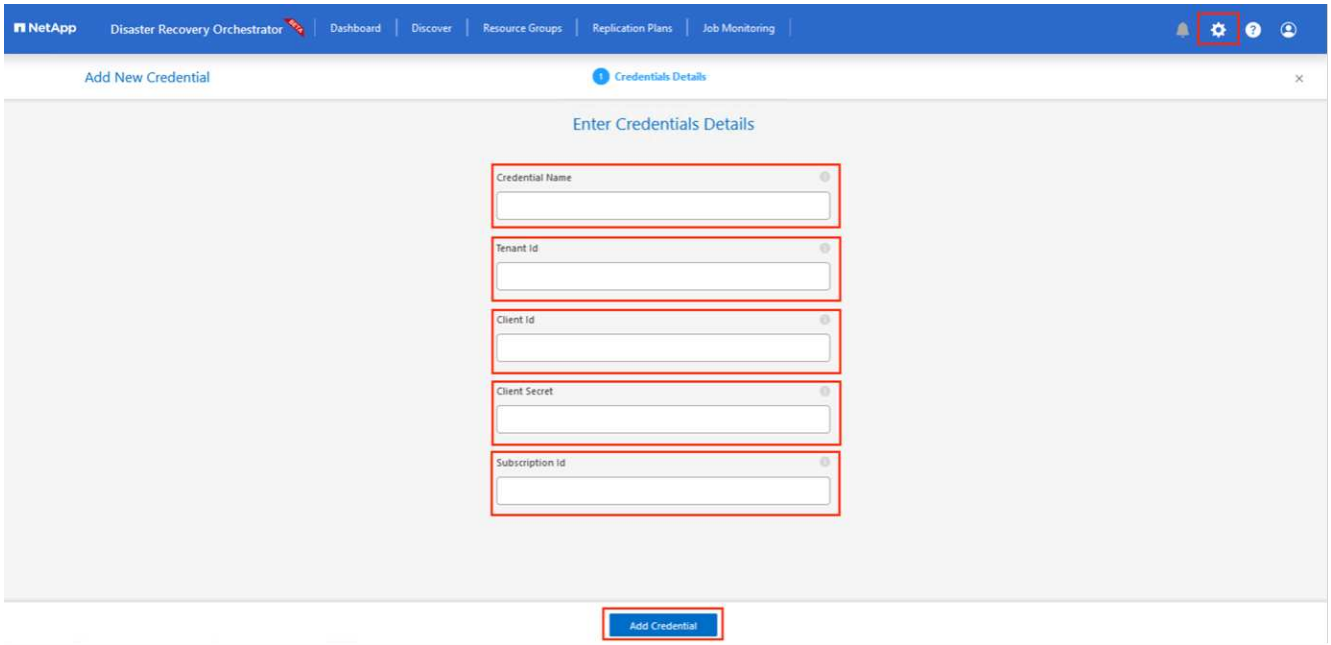
Pour effectuer cette opération, procédez comme suit :

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 **Paramètres** et sélectionnez **Informations d'identification**.
3. Cliquez sur Ajouter de nouvelles informations d'identification et suivez les étapes de l'assistant.
4. Pour définir les informations d'identification, entrez les informations sur le principal du service Azure Active Directory qui accorde les autorisations requises :
   - Nom d'identification

- ID du locataire
- ID client
- Secret client
- ID d'abonnement

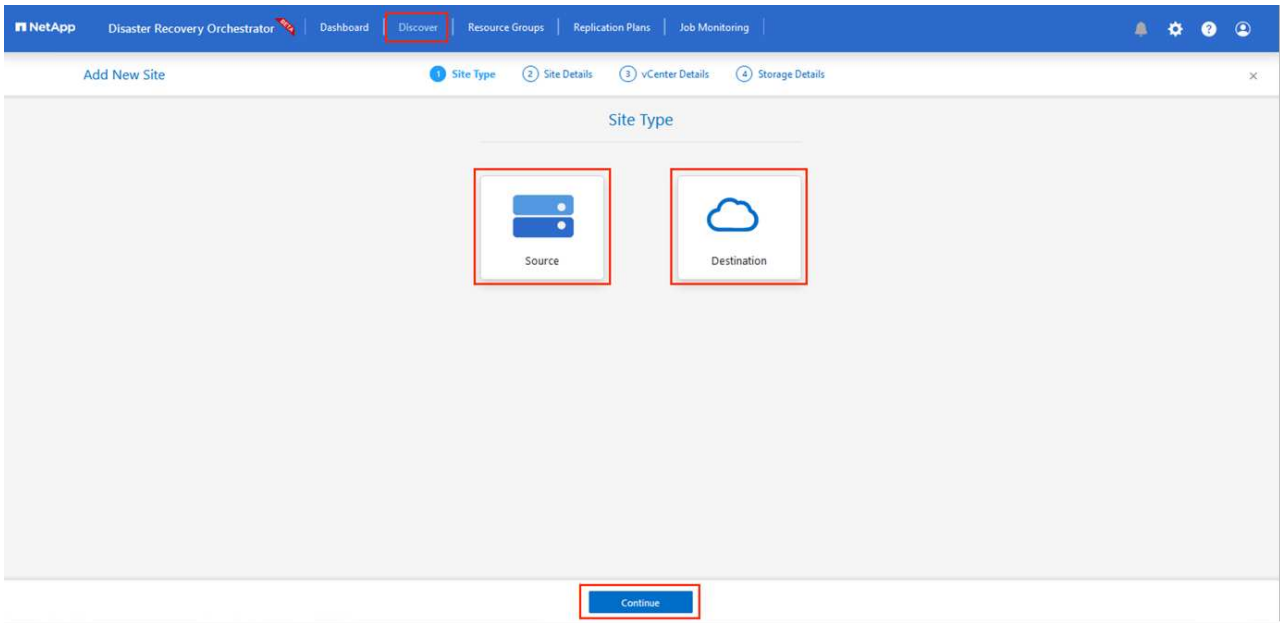
  Vous auriez dû capturer ces informations lorsque vous avez créé l'application AD.

5. Confirmez les détails des nouvelles informations d'identification et cliquez sur Ajouter des informations d'identification.



Après avoir ajouté les informations d'identification, il est temps de découvrir et d'ajouter les sites AVS principal et secondaire (vCenter et le compte de stockage des fichiers Azure NetApp) à DRO. Pour ajouter le site source et le site de destination, procédez comme suit :

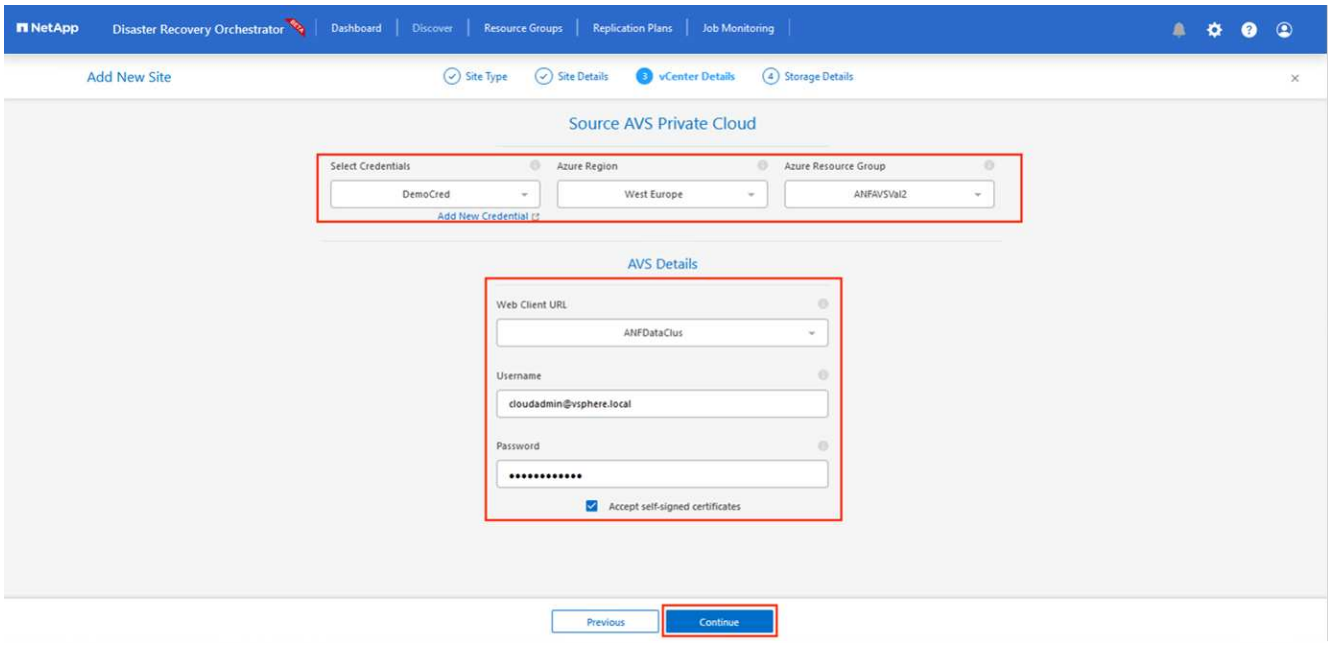
6. Accédez à l'onglet **Découvrir**.
7. Cliquez sur **Ajouter un nouveau site**.
8. Ajoutez le site AVS principal suivant (désigné comme **Source** dans la console).
   - SDDC vCenter
   - Compte de stockage Azure NetApp Files
9. Ajoutez le site AVS secondaire suivant (désigné comme **Destination** dans la console).
   - SDDC vCenter
   - Compte de stockage Azure NetApp Files



10. Ajoutez les détails du site en cliquant sur **Source**, en saisissant un nom de site convivial et en sélectionnant le connecteur. Cliquez ensuite sur **Continuer**.

> À des fins de démonstration, l'ajout d'un site source est abordé dans ce document.

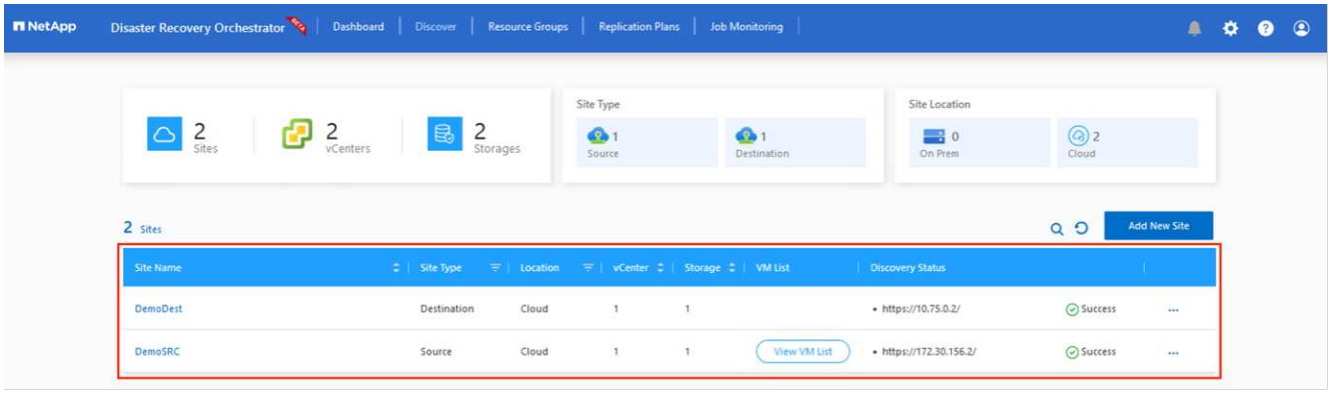
11. Mettre à jour les détails de vCenter. Pour ce faire, sélectionnez les informations d'identification, la région Azure et le groupe de ressources dans la liste déroulante du SDDC AVS principal.
12. DRO répertorie tous les SDDC disponibles dans la région. Sélectionnez l'URL du cloud privé désigné dans 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 "lien" . Une fois terminé, cliquez sur **Continuer**.



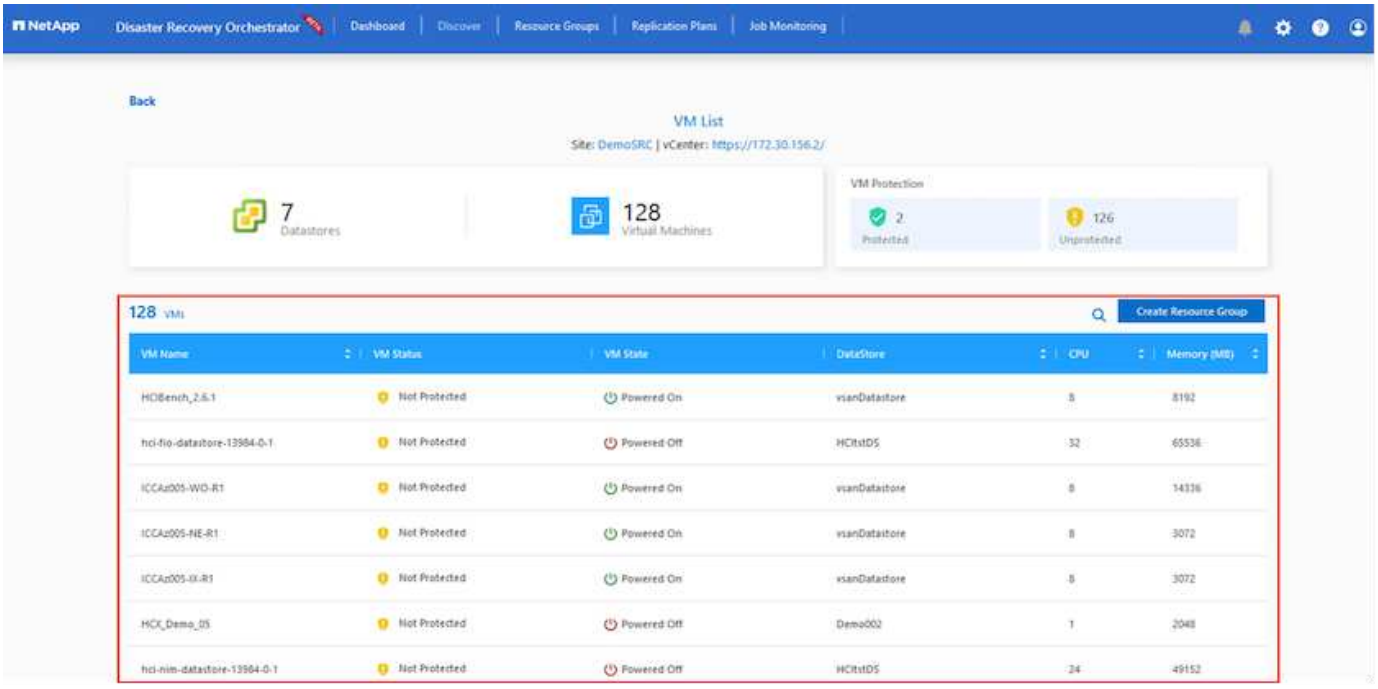
14. Sélectionnez les détails du stockage source (ANF) en sélectionnant le groupe de ressources Azure et le

compte NetApp .

15. Cliquez sur **Créer un site**.



Une fois ajouté, DRO effectue une découverte automatique et affiche les machines virtuelles qui ont des répliques interrégionales correspondantes du site source au site de destination. DRO détecte automatiquement les réseaux et les segments utilisés par les machines virtuelles et les remplit.



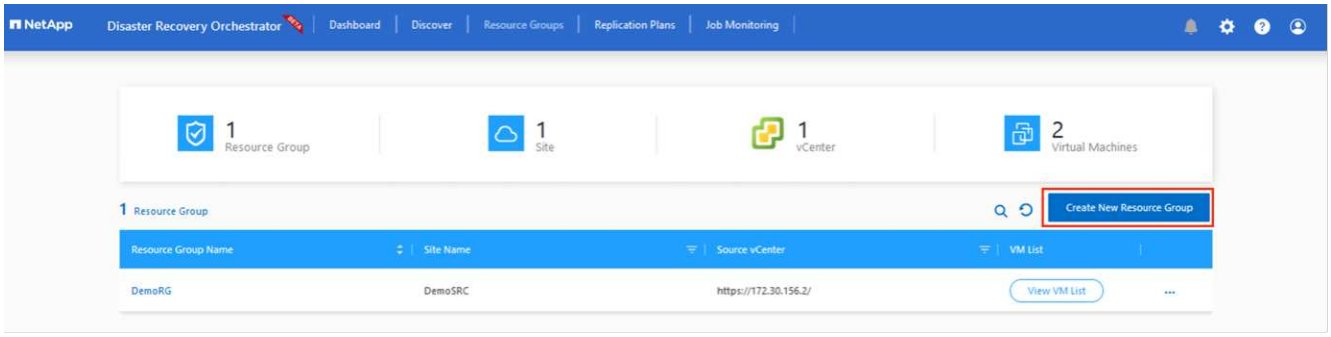
L’étape suivante consiste à regrouper les machines virtuelles requises dans leurs groupes fonctionnels en tant que groupes de ressources.

Groupements de ressources

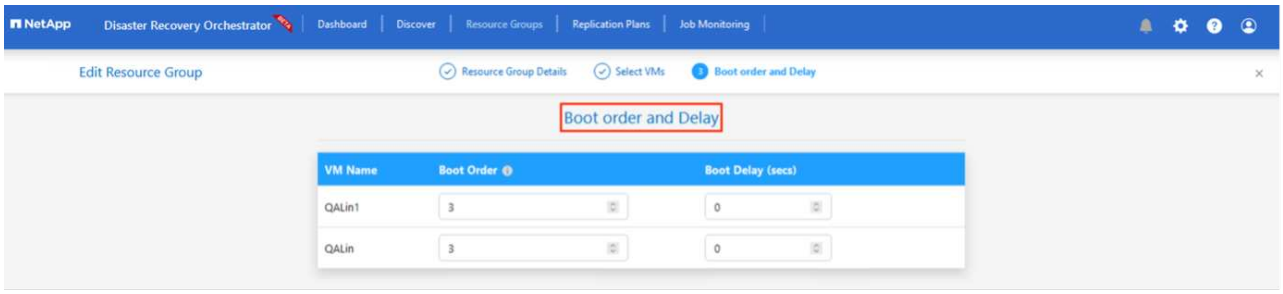
Une fois les plates-formes ajoutées, regroupez les machines virtuelles que vous souhaitez récupérer dans des groupes de ressources. Les groupes de ressources DRO vous permettent de regrouper un ensemble de machines virtuelles dépendantes en groupes logiques contenant leurs ordres de démarrage, leurs délais de démarrage et leurs validations d’application 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**.

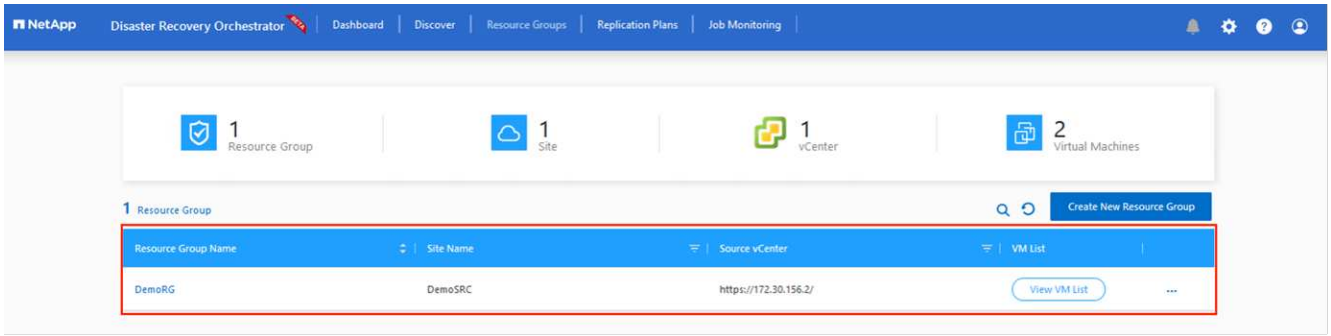
1. Accédez aux **Groupes de ressources** et cliquez sur **Créer un nouveau groupe de ressources**.



2. Sous Nouveau groupe de ressources, sélectionnez le site source dans la liste déroulante et cliquez sur **Créer**.
3. Fournissez 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 l'**Ordre de démarrage** et le **Délai de démarrage** (en secondes) 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 :
   - La première machine virtuelle à s'allumer
   - Défaut
   - La dernière machine virtuelle à s'allumer



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



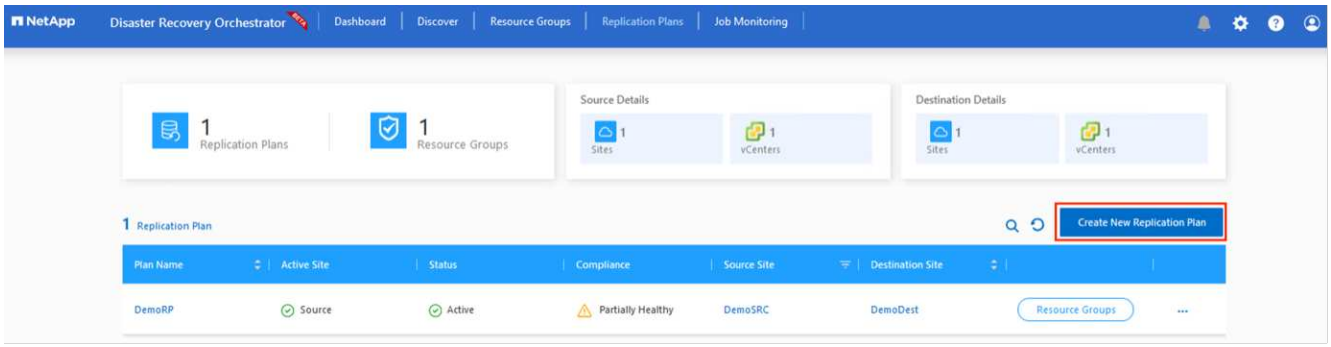
Plans de réplication

Vous devez disposer d'un plan pour récupérer les applications en cas de sinistre. Sélectionnez les plates-formes vCenter source et de destination dans la liste déroulante, choisissez les groupes de ressources à inclure dans ce plan et incluez également le regroupement de la manière dont les applications doivent être

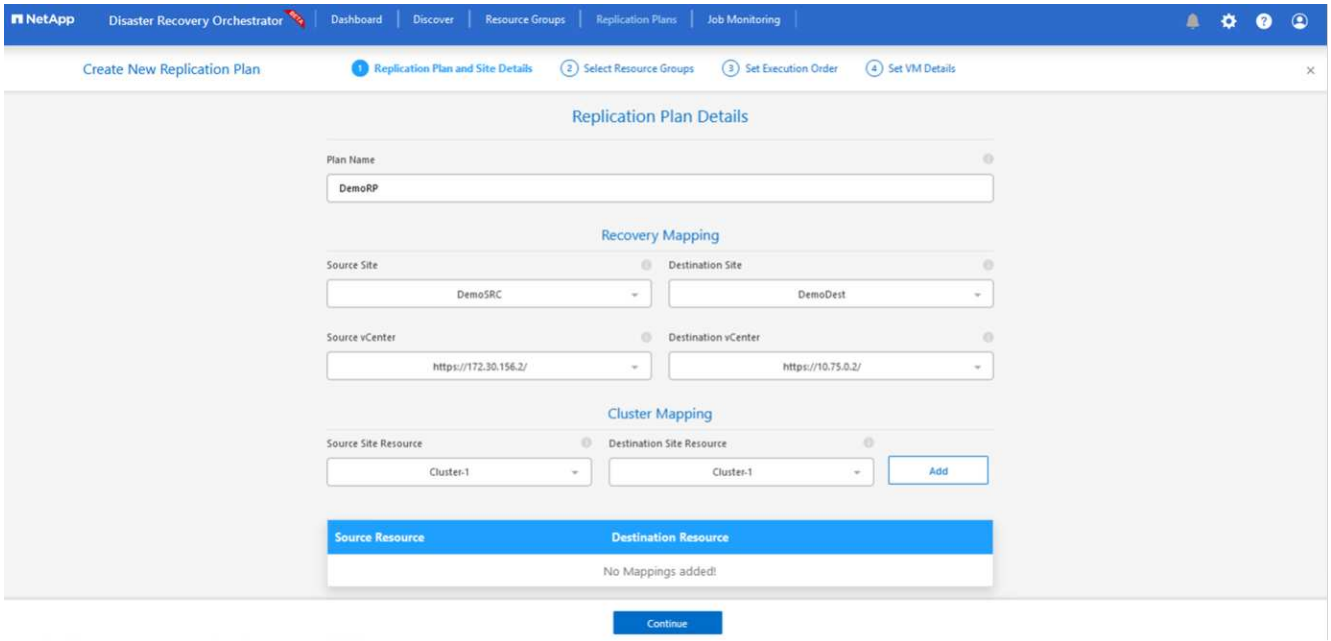
restaurées et mises sous tension (par exemple, contrôleurs de domaine, niveau 1, niveau 2, etc.). Les plans sont souvent également appelés schémas directeurs. Pour définir le plan de récupération, accédez à l'onglet Plan de réplication et cliquez sur **Nouveau plan de réplication**.

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

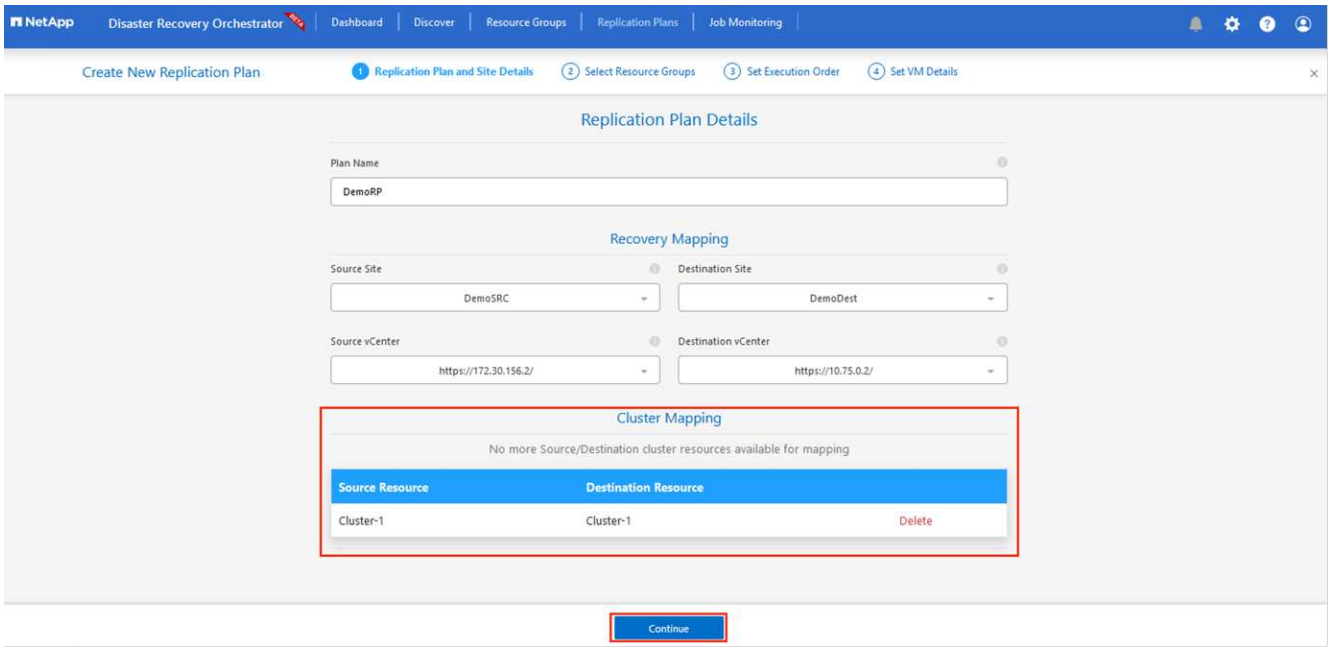
1. Accédez à **Plans de réplication** et cliquez sur **Créer un nouveau plan de réplication**.



2. Dans 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.

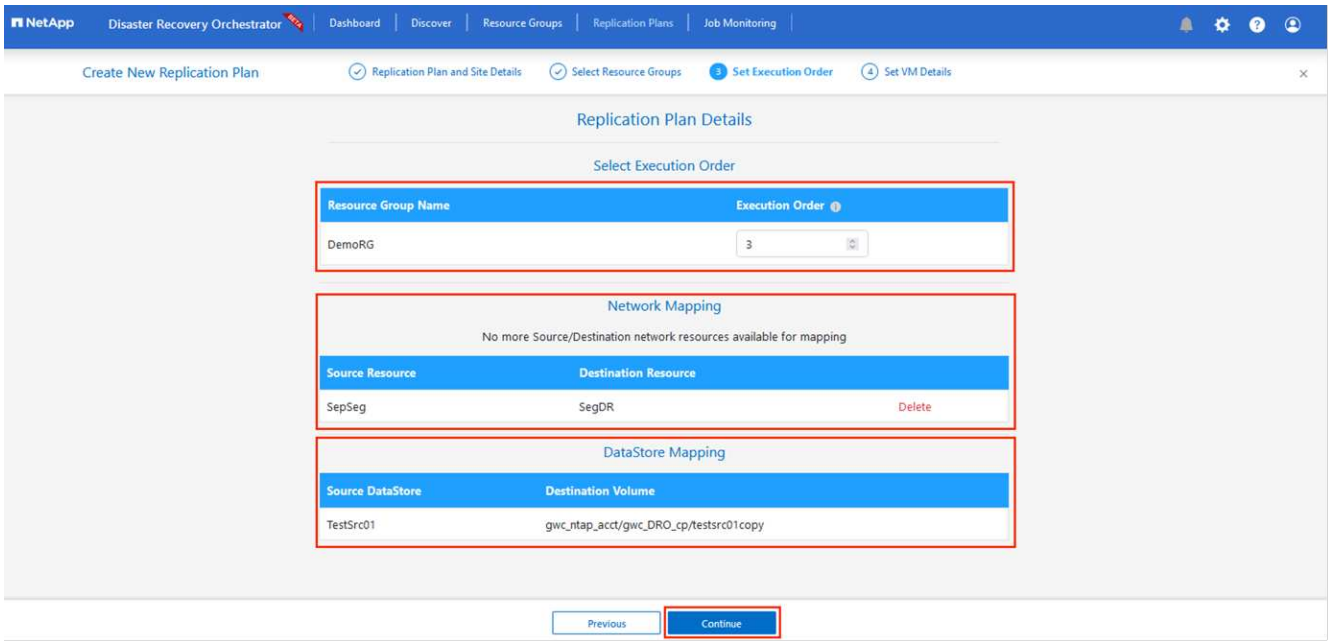


3. Une fois le mappage de récupération terminé, sélectionnez le **Mappage de cluster**.

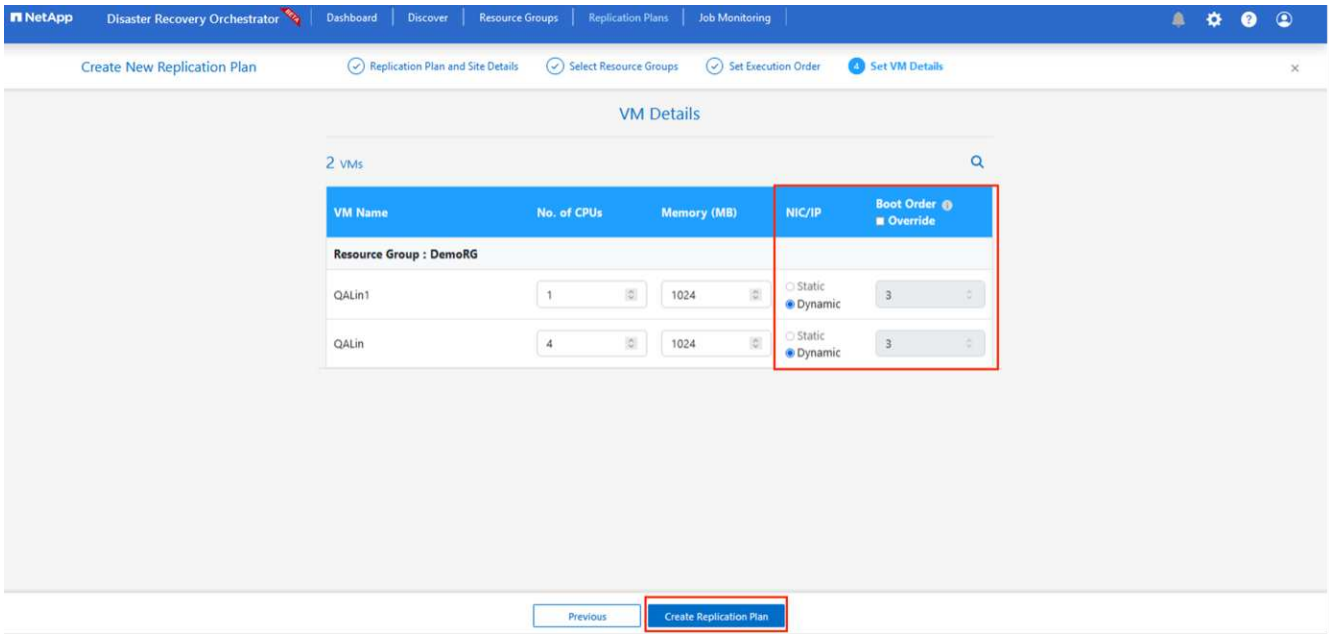


4. Sélectionnez **Détails du groupe de ressources** et cliquez sur **Continuer**.
5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsque plusieurs groupes de ressources existent.
6. Une fois terminé, définissez le mappage réseau sur le segment approprié. Les segments doivent déjà être provisionnés sur le cluster AVS secondaire et, pour mapper les machines virtuelles à ceux-ci, sélectionnez le segment approprié.
7. Les mappages de magasins de données sont automatiquement sélectionnés en fonction de la sélection des machines virtuelles.

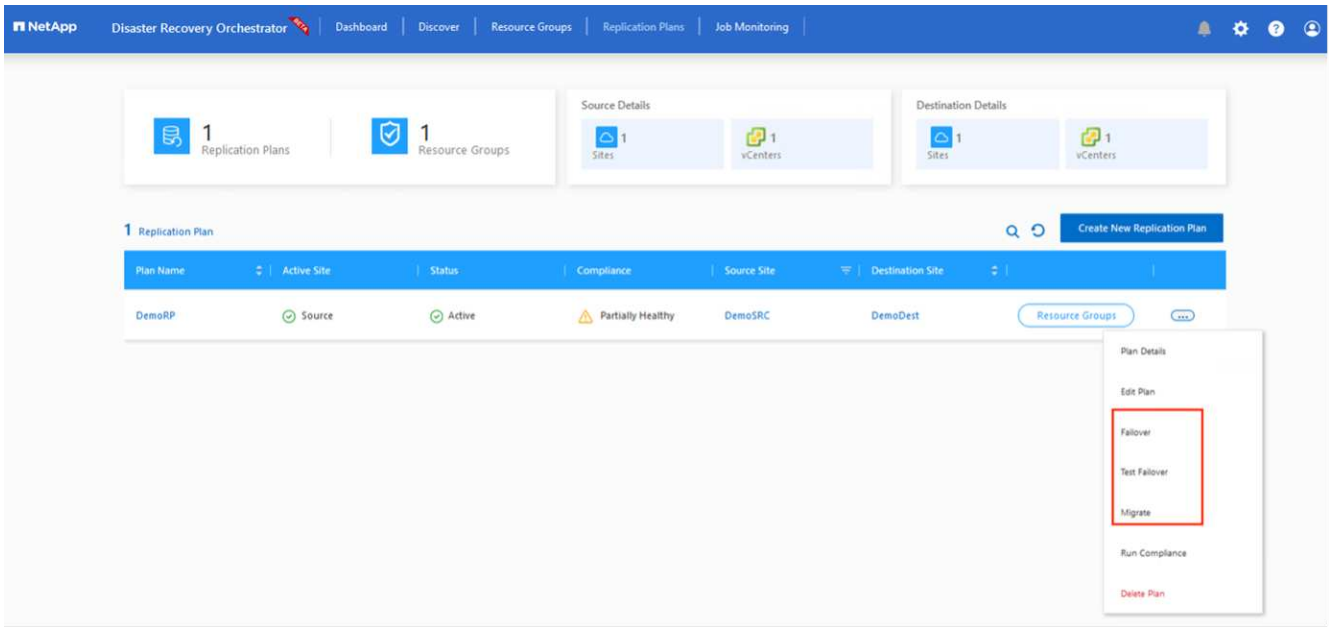
> ⓘ La réplication interrégionale (CRR) se fait au niveau du volume. Par conséquent, toutes les machines virtuelles résidant sur le volume respectif sont répliquées vers la destination CRR. Assurez-vous de sélectionner toutes les machines virtuelles qui font partie du magasin de données, car seules les machines virtuelles qui font partie du plan de réplication sont traitées.



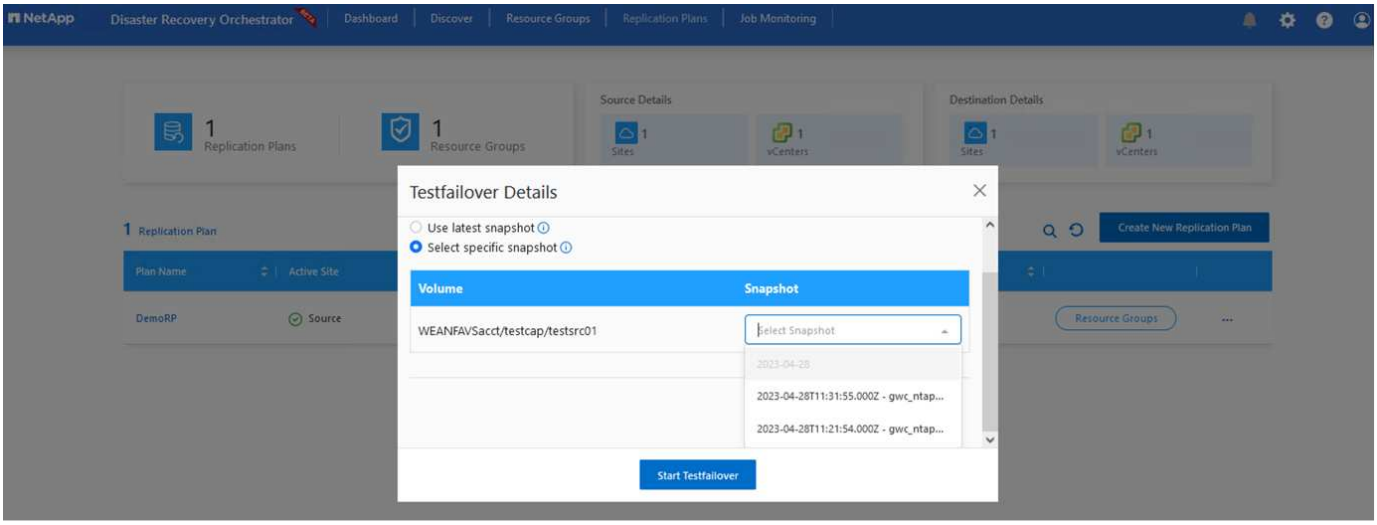
8. Sous les détails de la machine virtuelle, vous pouvez éventuellement redimensionner les paramètres CPU et RAM des machines virtuelles. Cela peut être très utile lorsque vous récupérez de grands environnements vers des clusters cibles plus petits ou lorsque vous effectuez des tests DR sans avoir à provisionner une infrastructure VMware physique individuelle. Modifiez également l'ordre de démarrage et le délai de démarrage (en secondes) 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 nécessaires par rapport à ce que vous avez sélectionné 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, mais toutes les modifications peuvent être effectuées à ce stade.



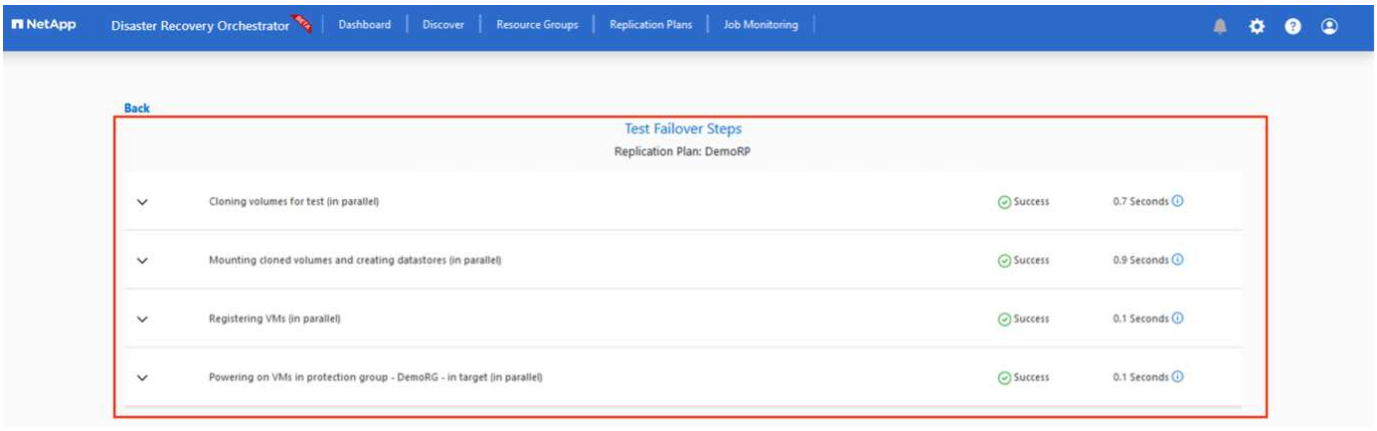
9. Cliquez sur **Créer un plan de réplication**. Une fois le plan de réplication créé, vous pouvez exercer les options de basculement, de test de basculement ou de migration en fonction de vos besoins.



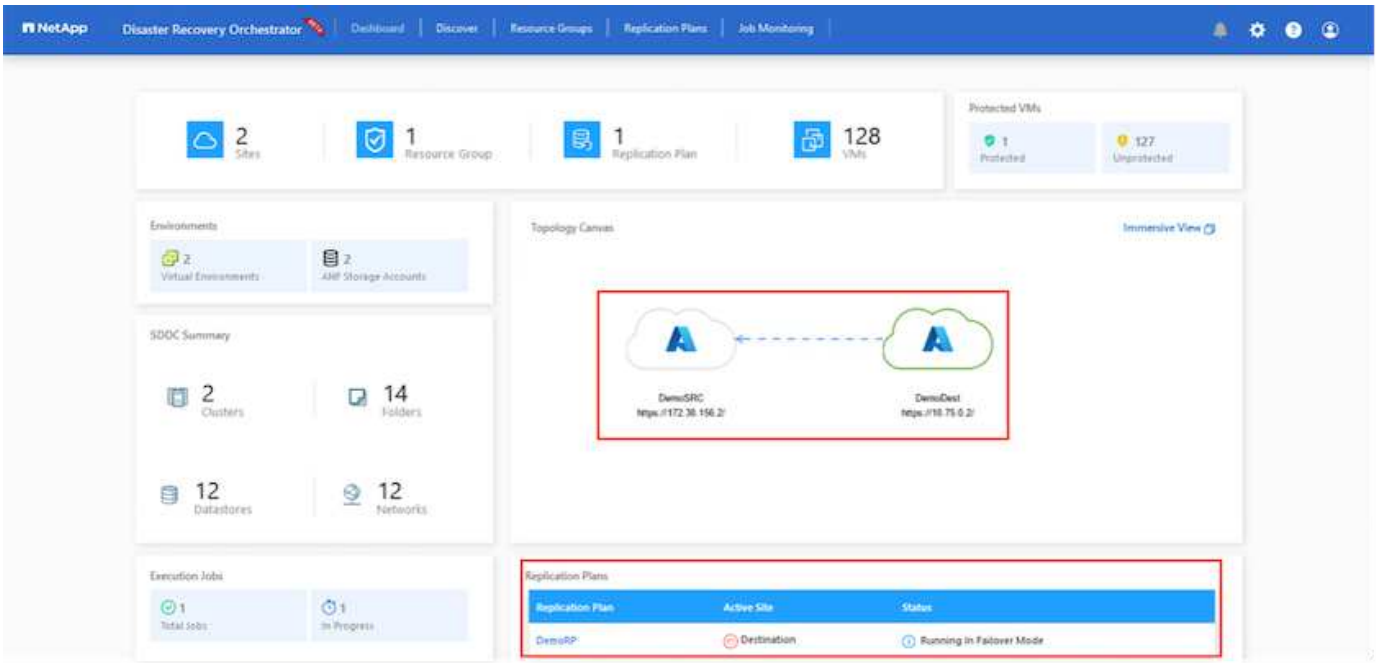
Lors des options de basculement et de test de basculement, l'instantané le plus récent est utilisé ou un instantané spécifique peut être sélectionné à partir d'un instantané ponctuel. L'option ponctuelle peut être très bénéfique si vous êtes confronté à un événement de corruption comme un ransomware, où les répliques les plus récentes sont déjà compromises ou cryptées. DRO affiche tous les points de temps disponibles.



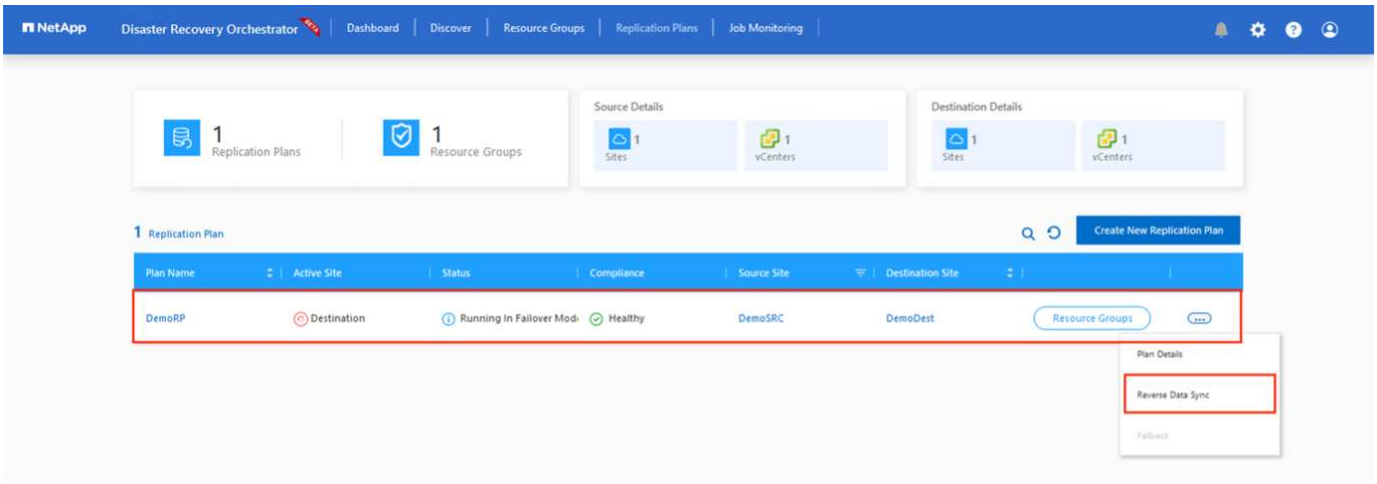
Pour déclencher un basculement ou un test de basculement avec la configuration spécifiée dans le plan de réplication, vous pouvez cliquer sur **Basculement** ou **Tester le basculement**. Vous pouvez surveiller le plan de réplication dans le menu des tâches.



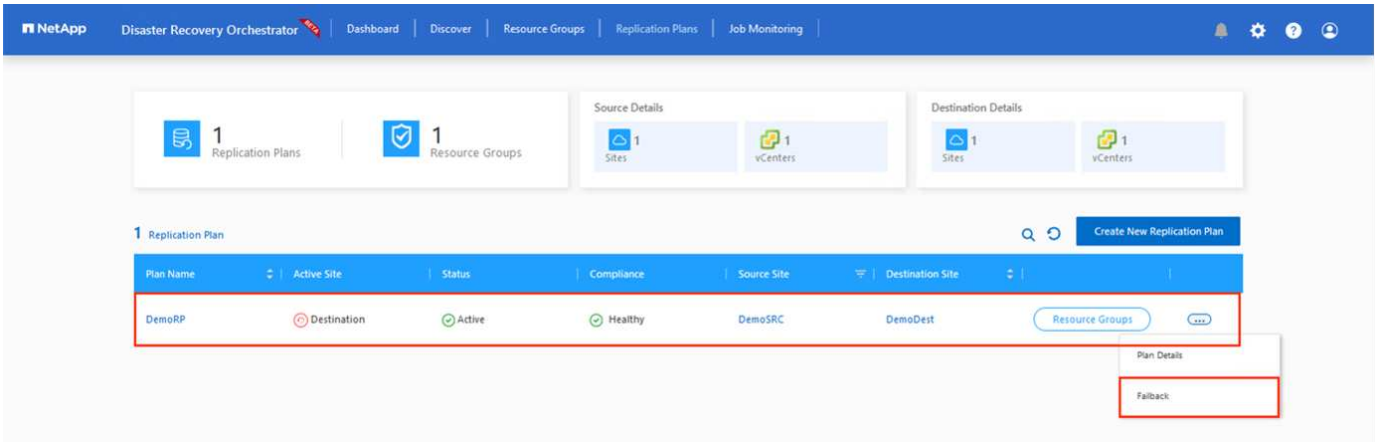
Une fois le basculement déclenché, les éléments récupérés peuvent être vus dans le site secondaire AVS SDDC vCenter (machines virtuelles, réseaux et banques de données). Par défaut, les machines virtuelles sont récupérées dans le dossier Workload.

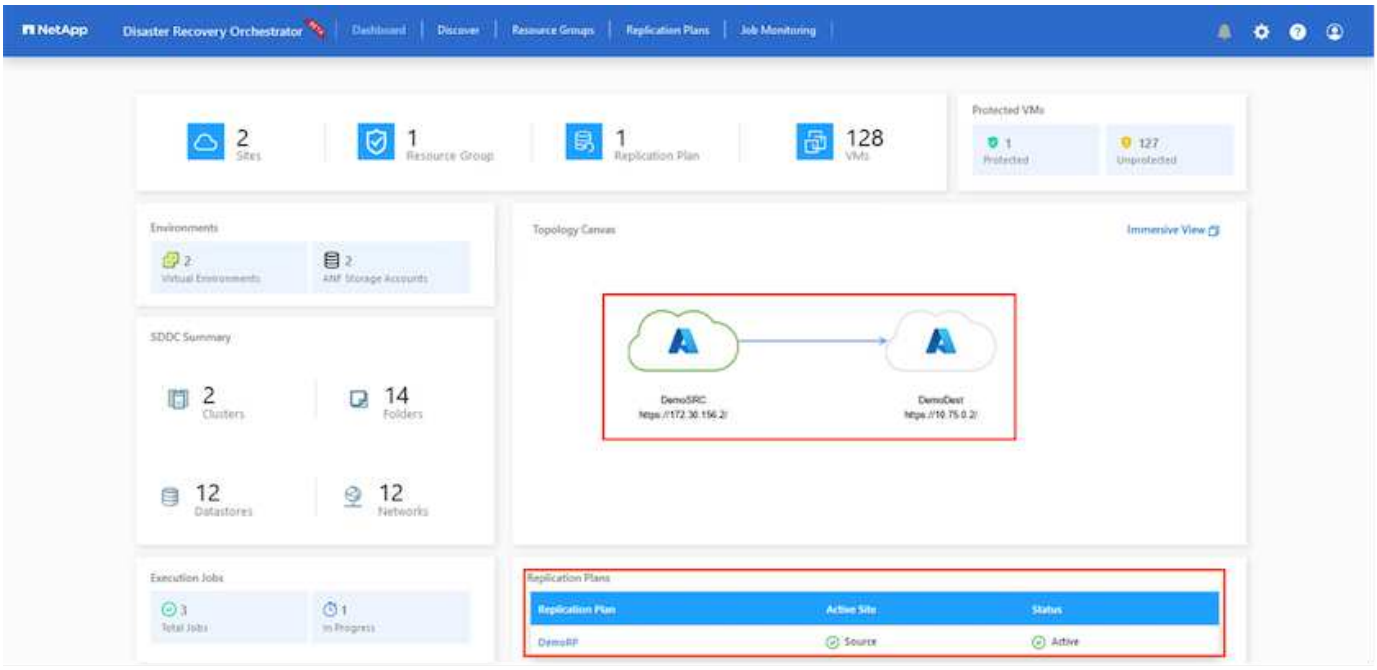


La restauration peut être déclenchée au niveau du plan de réplication. En cas de basculement de test, l'option de suppression peut être utilisée pour annuler les modifications et supprimer le volume nouvellement créé. Les retours en arrière liés au basculement sont un processus en deux étapes. Sélectionnez le plan de réplication et sélectionnez **Synchronisation des données inversées**.



Une fois cette étape terminée, déclenchez la restauration automatique pour revenir au site AVS principal.





À partir du portail Azure, nous pouvons voir que l'intégrité de la réplication a été interrompue pour les volumes appropriés qui ont été mappés au site secondaire AVS SDDC en tant que volumes de lecture/écriture. Lors du basculement de test, DRO ne mappe pas le volume de destination ou de réplication. Au lieu de cela, il crée un

nouveau volume de l'instantané de réplication interrégional requis et expose le volume en tant que banque de données, ce qui consomme une capacité physique supplémentaire du pool de capacité et garantit que le volume source n'est pas modifié. En particulier, les tâches de réplication peuvent se poursuivre pendant les tests DR ou les flux de travail de triage. De plus, ce processus garantit que la récupération peut être nettoyée sans risque de destruction de la réplique en cas d'erreurs ou de récupération de données corrompues.

Récupération après un ransomware

Se remettre d'un ransomware peut être une tâche ardue. Plus précisément, il peut être difficile pour les organisations informatiques d'identifier précisément le point de retour sûr et, une fois celui-ci déterminé, de garantir que les charges de travail récupérées sont protégées contre les attaques récurrentes (par exemple, contre des logiciels malveillants dormants ou via des applications vulnérables).

DRO répond à ces préoccupations en permettant aux organisations de récupérer à partir de n'importe quel moment disponible. Les charges de travail sont ensuite récupérées sur des réseaux fonctionnels et pourtant isolés, de sorte que les applications peuvent fonctionner et communiquer entre elles mais ne sont exposées à aucun trafic nord-sud. Ce processus offre aux équipes de sécurité un endroit sûr pour effectuer des analyses médico-légales et identifier tout logiciel malveillant caché ou dormant.

Conclusion

La solution de reprise après sinistre Azure NetApp Files et Azure VMware vous offre les avantages suivants :

- Tirez parti d'une réplication interrégionale Azure NetApp Files efficace et résiliente.
- Récupérez à n'importe quel moment disponible avec la conservation des instantanés.
- Automatisez entièrement toutes les étapes requises pour récupérer des centaines à des milliers de machines virtuelles à partir des étapes de stockage, de calcul, de réseau et de validation des applications.
- La récupération de la charge de travail exploite le processus « Créer de nouveaux volumes à partir des instantanés les plus récents », qui ne manipule pas le volume répliqué.
- Évitez tout risque de corruption de données sur les volumes ou les snapshots.
- Évitez les interruptions de réplication pendant les flux de travail de test DR.
- Exploitez les données DR et les ressources de calcul cloud pour les flux de travail au-delà de la DR, 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 du processeur et de la RAM peut contribuer à réduire les coûts du cloud en permettant la récupération vers des clusters de calcul plus petits.

Où trouver des informations supplémentaires

Pour en savoir plus sur les informations décrites dans ce document, consultez les documents et/ou sites Web suivants :

- Créer une réplication de volume pour Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Réplication interrégionale des 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"

- Déployer et configurer l'environnement de virtualisation sur Azure

  "Configurer AVS sur Azure"

- Déployer et configurer la solution Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Utilisation de Veeam Replication et du datastore Azure NetApp Files pour la reprise après sinistre vers Azure VMware Solution

Les magasins de données Azure NetApp Files (ANF) dissocient le stockage du calcul et libèrent la flexibilité nécessaire à toute organisation pour transférer ses charges de travail vers le cloud. Il fournit aux clients une infrastructure de stockage flexible et hautes performances qui s'adapte indépendamment des ressources de calcul. Le magasin de données Azure NetApp Files simplifie et optimise le déploiement aux côtés d'Azure VMware Solution (AVS) en tant que site de reprise après sinistre pour les environnements VMWare sur site.

Aperçu

Les magasins de données NFS basés sur des volumes Azure NetApp Files (ANF) peuvent être utilisés pour répliquer des données à partir de sites locaux à l'aide de n'importe quelle solution tierce validée offrant une capacité de réplication de machines virtuelles. En ajoutant des magasins de données Azure NetApp Files , cela permettra un déploiement optimisé en termes de coûts par rapport à la création d'un SDDC Azure VMware Solution avec une énorme quantité d'hôtes ESXi pour accueillir le stockage. Cette approche est appelée « Pilot Light Cluster ». Un cluster de voyants lumineux est une configuration d'hôte AVS minimale (3 nœuds AVS) avec une capacité de banque de données Azure NetApp Files .

L'objectif est de maintenir une infrastructure à faible coût avec tous les composants essentiels pour gérer un basculement. Un cluster de voyants lumineux peut évoluer et provisionner davantage d'hôtes AVS en cas de basculement. Et une fois le basculement terminé et les opérations normales rétablies, le groupe de voyants lumineux peut revenir à un mode de fonctionnement à faible coût.

Objectifs du présent document

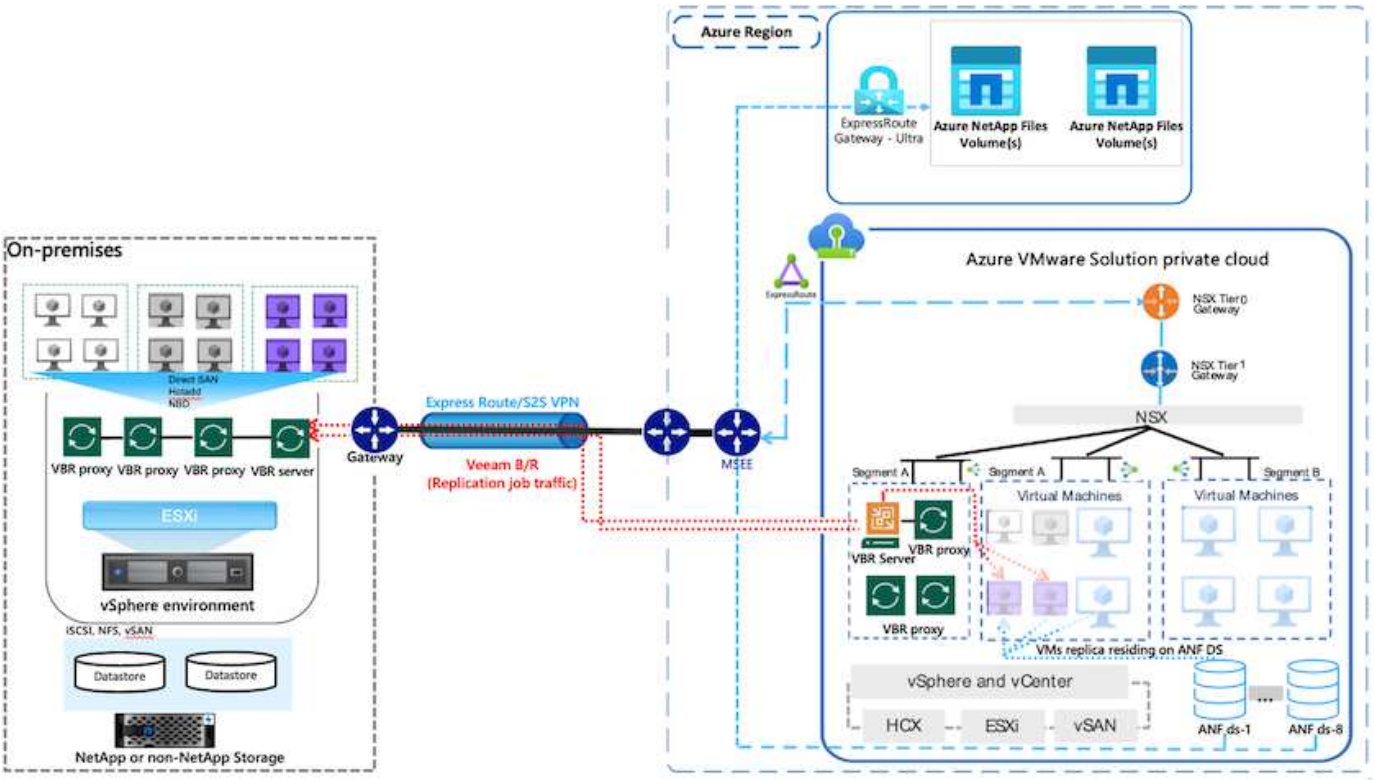
Cet article décrit comment utiliser la banque de données Azure NetApp Files avec Veeam Backup et la réplication pour configurer la reprise après sinistre des machines virtuelles VMware locales (AVS) à l'aide de la fonctionnalité du logiciel de réplication de machines virtuelles Veeam.

Veeam Backup & Replication est une application de sauvegarde et de réplication pour les environnements virtuels. Lorsque les machines virtuelles sont répliquées, Veeam Backup & Replication est répliqué à partir d'AVS, le logiciel créera une copie exacte des machines virtuelles au format VMware vSphere natif sur le cluster SDDC AVS cible. Veeam Backup & Replication gardera la copie synchronisée avec la machine virtuelle d'origine. La réplication fournit le meilleur objectif de temps de récupération (RTO) car il existe une copie montée d'une machine virtuelle sur le site DR dans un état prêt à démarrer.

Ce mécanisme de réplication garantit que les charges de travail peuvent démarrer rapidement dans un SDDC AVS en cas de sinistre. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. De plus, il filtre également les blocs de données en

double, les blocs de données nuls, les fichiers d'échange et les « fichiers du système d'exploitation invité de la machine virtuelle exclus ». Le logiciel compressera également le trafic de réplique. Pour éviter que les tâches de réplication ne consomment toute la bande passante du réseau, des accélérateurs WAN et des règles de limitation du réseau peuvent être utilisés.

Le processus de réplication dans Veeam Backup & Replication est piloté par tâches, ce qui signifie que la réplication est effectuée en configurant des tâches de réplication. En cas de sinistre, le basculement peut être déclenché pour récupérer les machines virtuelles en basculant vers leur copie de réplication. Lorsqu'un basculement est effectué, une machine virtuelle répliquée reprend le rôle de la machine virtuelle d'origine. Le basculement peut être effectué vers le dernier état d'une réplique ou vers l'un de ses points de restauration connus. Cela permet la récupération des ransomwares ou des tests isolés selon les besoins. Veeam Backup & Replication offre plusieurs options pour gérer différents scénarios de reprise après sinistre.



Déploiement de la solution

Étapes de haut niveau

1. Le logiciel Veeam Backup and Replication s'exécute dans un environnement sur site avec une connectivité réseau appropriée.
2. "Déployer la solution Azure VMware (AVS)"cloud privé et"attacher des banques de données Azure NetApp Files" aux hôtes Azure VMware Solution.

   Un environnement de veilleuse configuré avec une configuration minimale peut être utilisé à des fins de reprise après sinistre. Les machines virtuelles basculeront vers ce cluster en cas d'incident et des nœuds supplémentaires pourront être ajoutés).

3. Configurez une tâche de réplication pour créer des répliques de machines virtuelles à l'aide de Veeam Backup and Replication.
4. Créez un plan de basculement et effectuez le basculement.

5. Revenez aux machines virtuelles de production une fois l'événement de catastrophe terminé et le site principal opérationnel.

Prérequis pour la réplication de machines virtuelles Veeam vers les datastores AVS et ANF

1. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée aux clusters AVS SDDC source et cible.
2. Le serveur de sauvegarde doit être capable de résoudre les noms courts et de se connecter aux vCenters source et cible.
3. La banque de données Azure NetApp Files cible doit disposer de suffisamment d'espace libre pour stocker les VMDK des machines virtuelles répliquées.

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

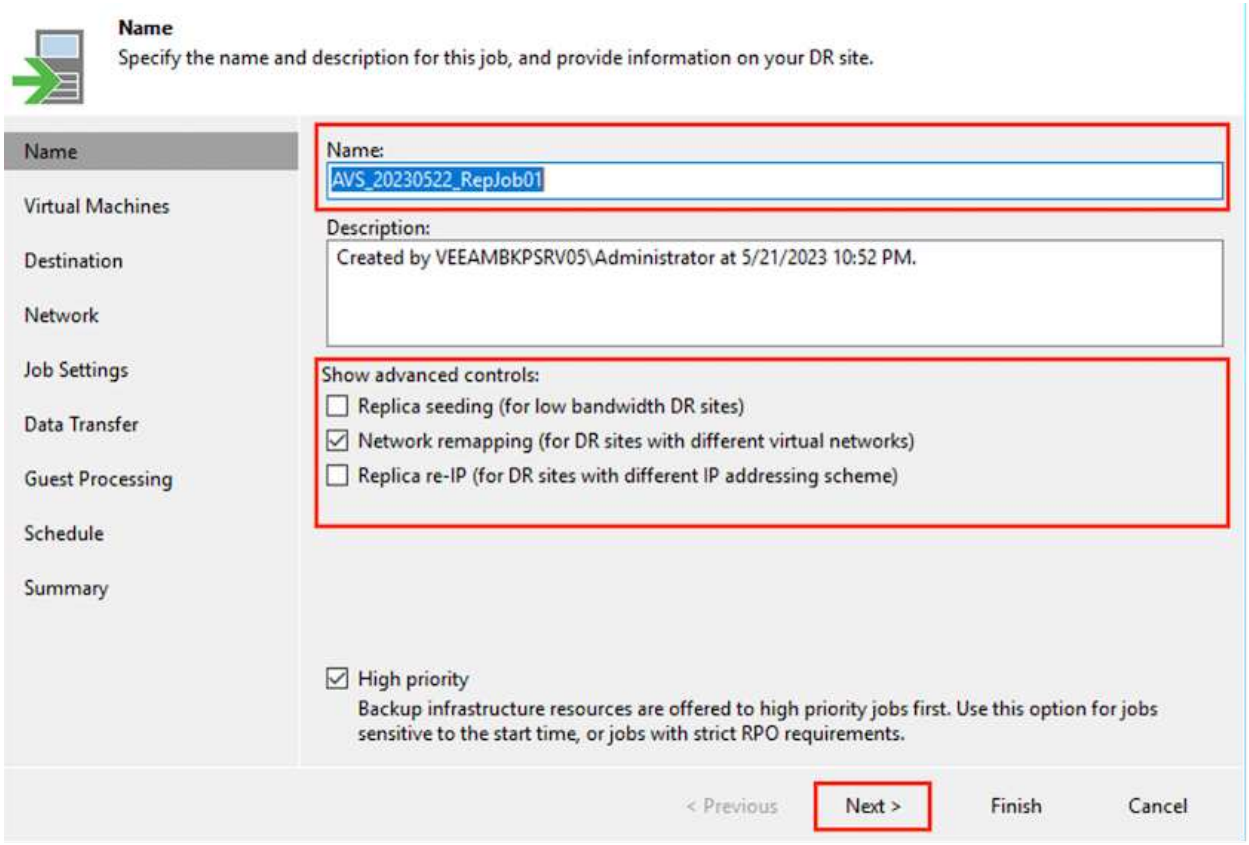
Détails du déploiement

▼ Étape 1 : Répliquer les machines virtuelles

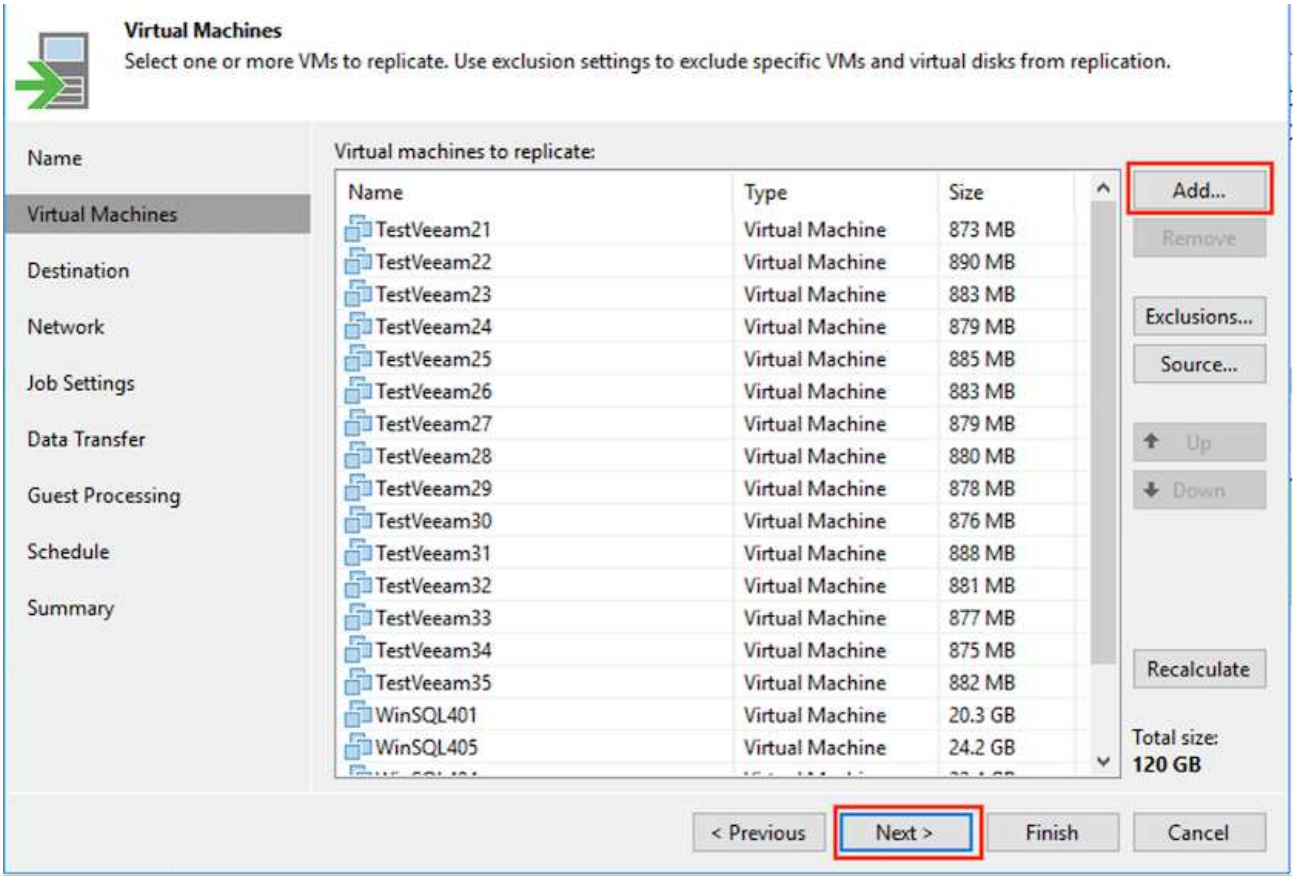
Veeam Backup & Replication exploite les fonctionnalités de snapshot de VMware vSphere. Pendant la réplication, Veeam Backup & Replication demande à VMware vSphere de créer un snapshot de VM. L'instantané de machine virtuelle est la copie ponctuelle d'une machine virtuelle qui inclut les disques virtuels, 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, suivez les étapes ci-dessous :

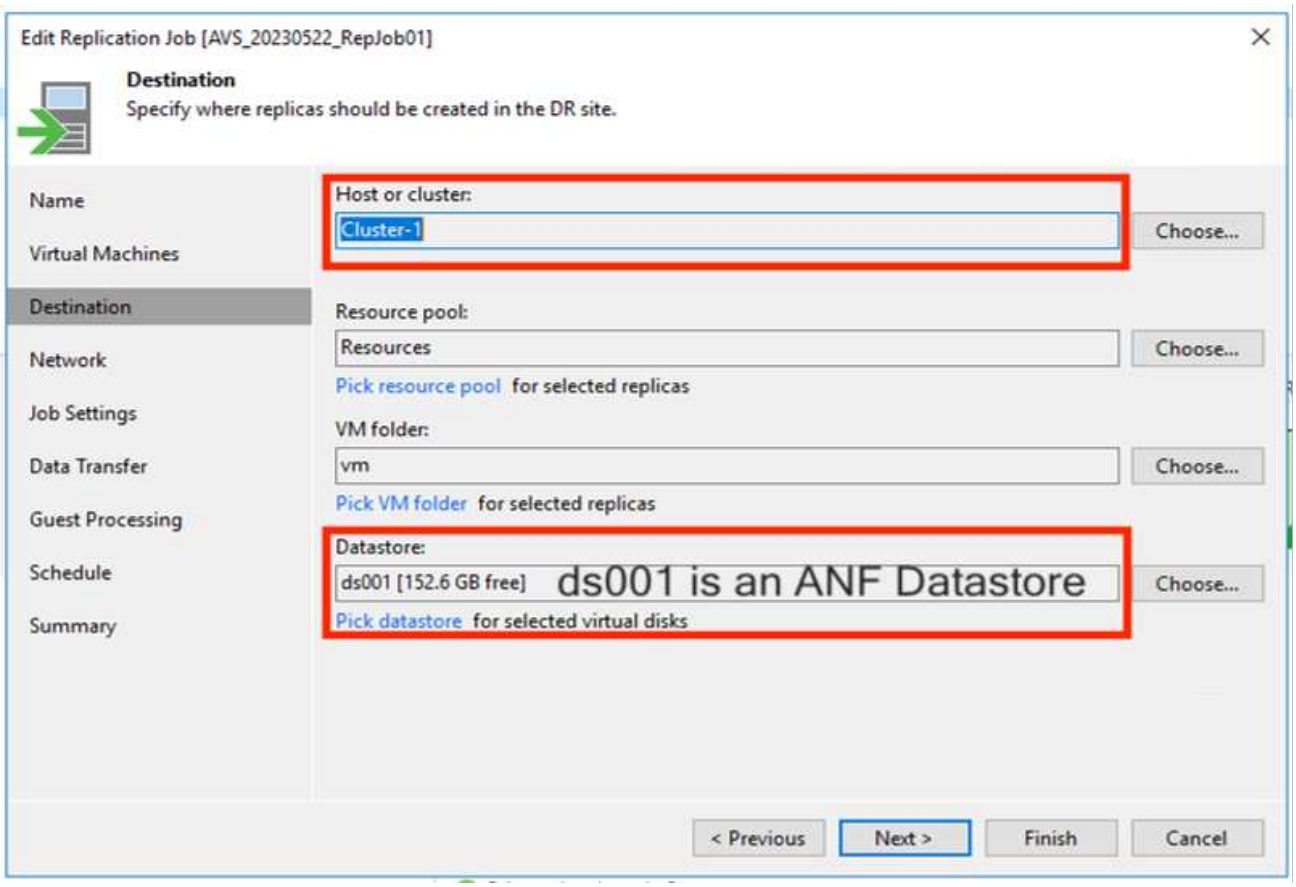
1. Ouvrez la console Veeam Backup & Replication.
2. Sur la vue Accueil. Cliquez avec le bouton droit sur le nœud des tâches et sélectionnez Tâche de réplication > Machine virtuelle.
3. Spécifiez un nom de tâche et sélectionnez la case à cocher de contrôle avancé appropriée. Cliquez sur Suivant.
    - Cochez la case Amorçage de réplica si la connectivité entre le site local et Azure a une bande passante restreinte. *Sélectionnez la case à cocher Remappage réseau (pour les sites AVS SDDC avec des réseaux différents) si les segments sur Azure VMware Solution SDDC ne correspondent pas à ceux des réseaux de sites locaux.
    - Si le schéma d'adressage IP du site de production sur site diffère du schéma du site AVS cible, cochez la case Réplication de l'adresse IP (pour les sites DR avec un schéma d'adressage IP différent).



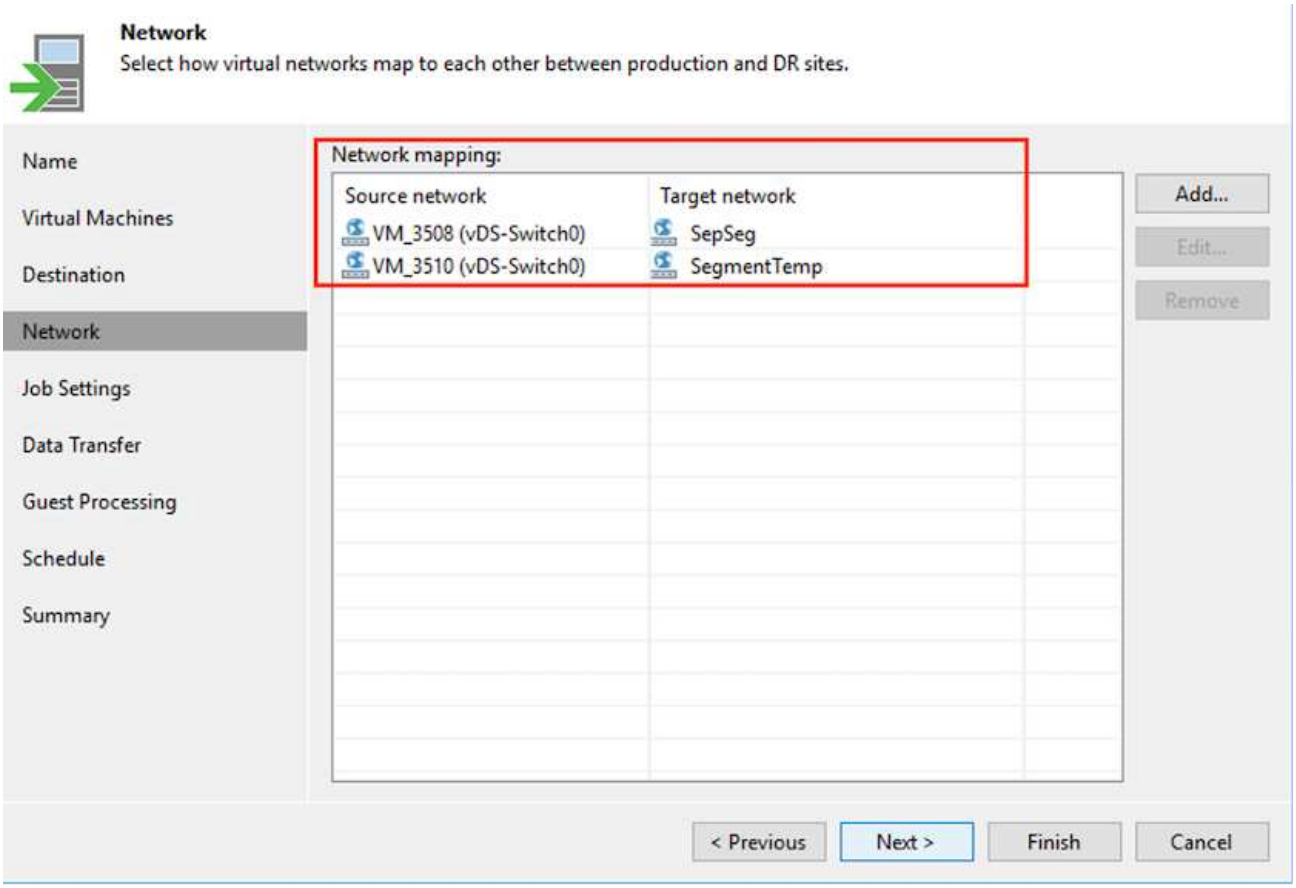
4. Sélectionnez les machines virtuelles à répliquer vers une banque de données Azure NetApp Files attachée à un SDDC Azure VMware Solution à l'étape **Machines** virtuelles*. Les machines virtuelles peuvent être placées sur vSAN pour remplir la capacité de stockage de données vSAN disponible. Dans un groupe de veilleuses, la capacité utilisable d'un groupe à 3 nœuds sera limitée. Le reste des données peut être facilement placé sur des magasins de données Azure NetApp Files afin que les machines virtuelles puissent être récupérées et que le cluster puisse être étendu pour répondre aux exigences CPU/mémoire. Cliquez sur **Ajouter**, puis dans la fenêtre **Ajouter un objet**, sélectionnez les machines virtuelles ou les conteneurs de machines virtuelles nécessaires et cliquez sur **Ajouter**. Cliquez sur **Suivant**.



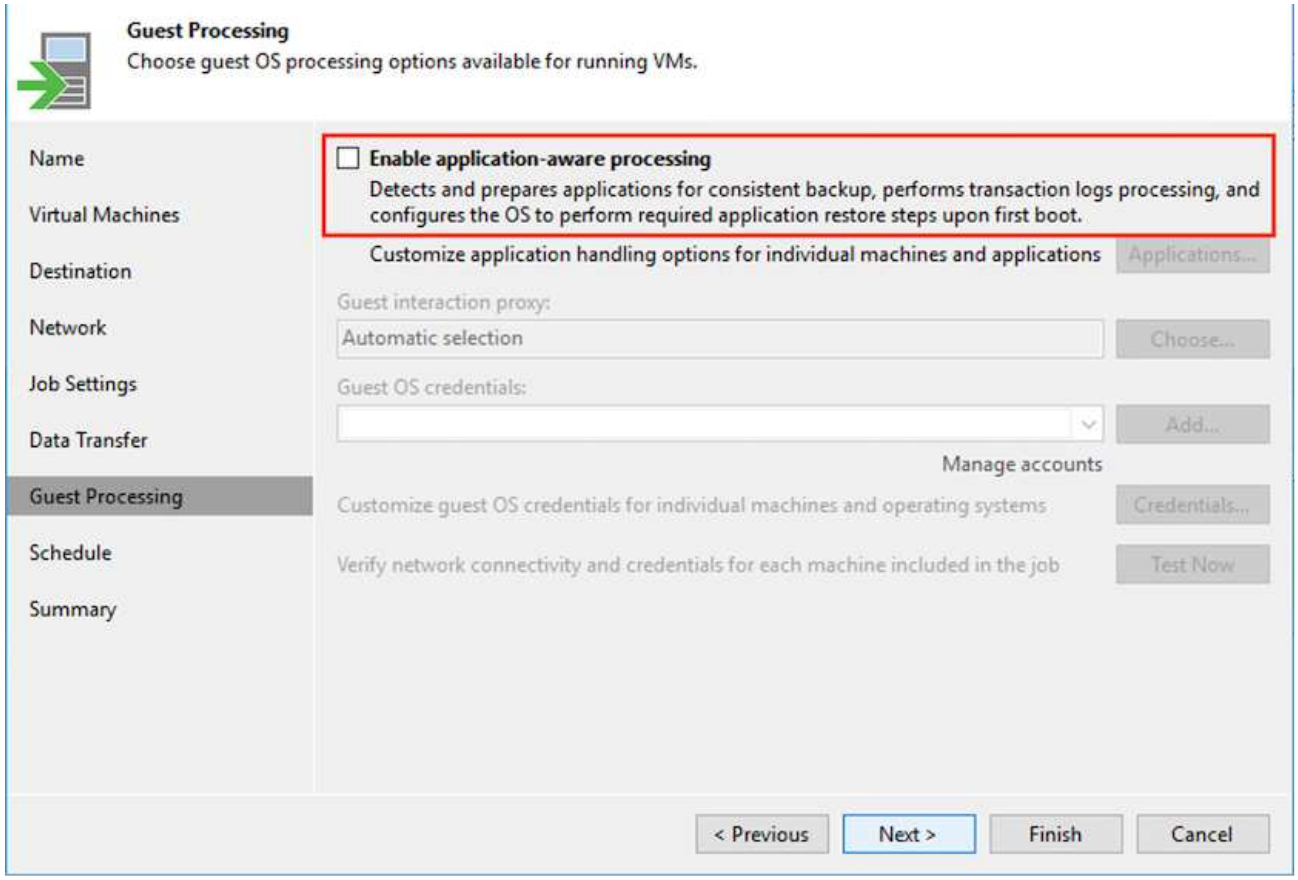
5. Après cela, sélectionnez la destination en tant que cluster/hôte Azure VMware Solution SDDC et le pool de ressources, le dossier de machine virtuelle et la banque de données FSx ONTAP appropriés pour les réplicas de machine virtuelle. Cliquez ensuite sur **Suivant**.



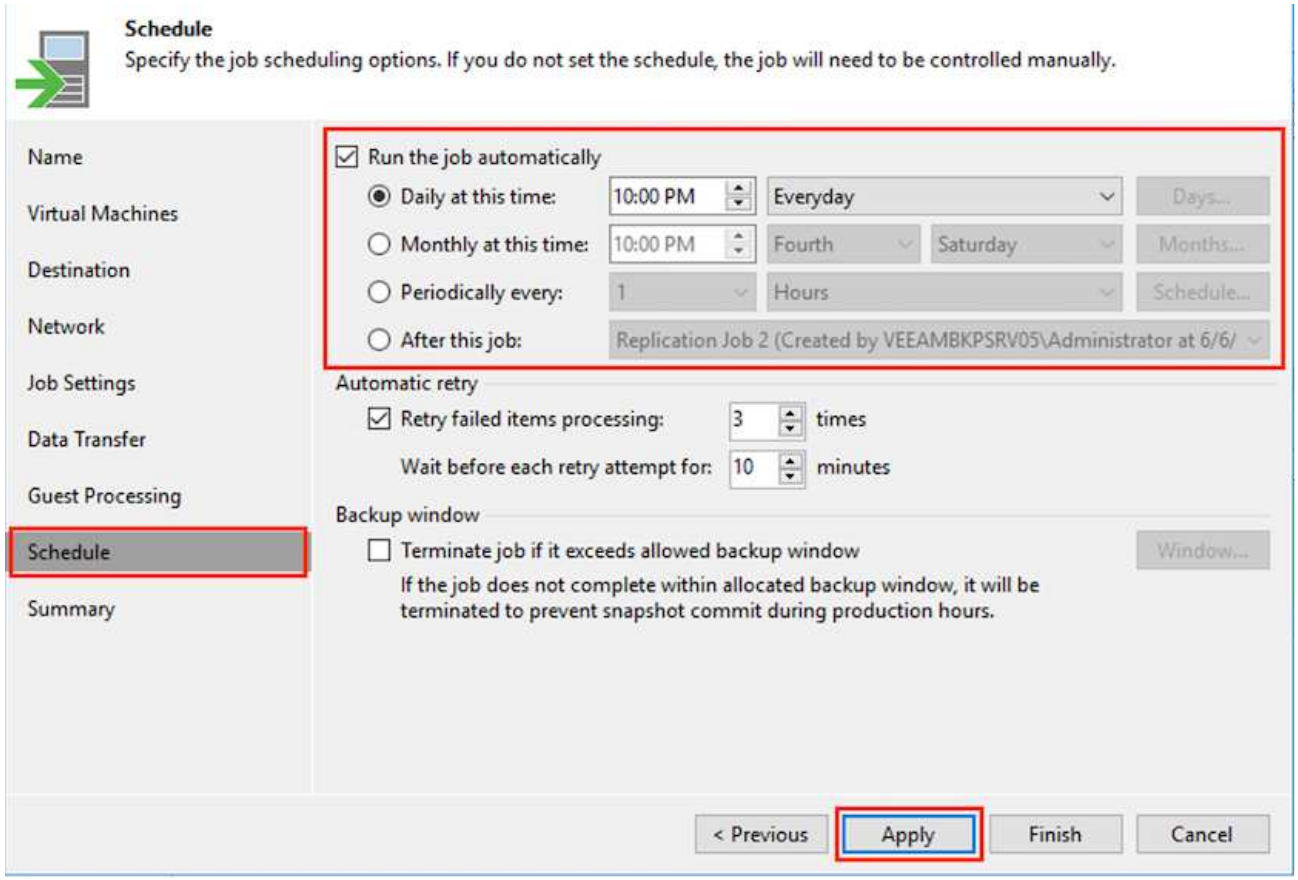
6. À l'étape suivante, créez le mappage entre le réseau virtuel source et le réseau virtuel de destination selon vos besoins.



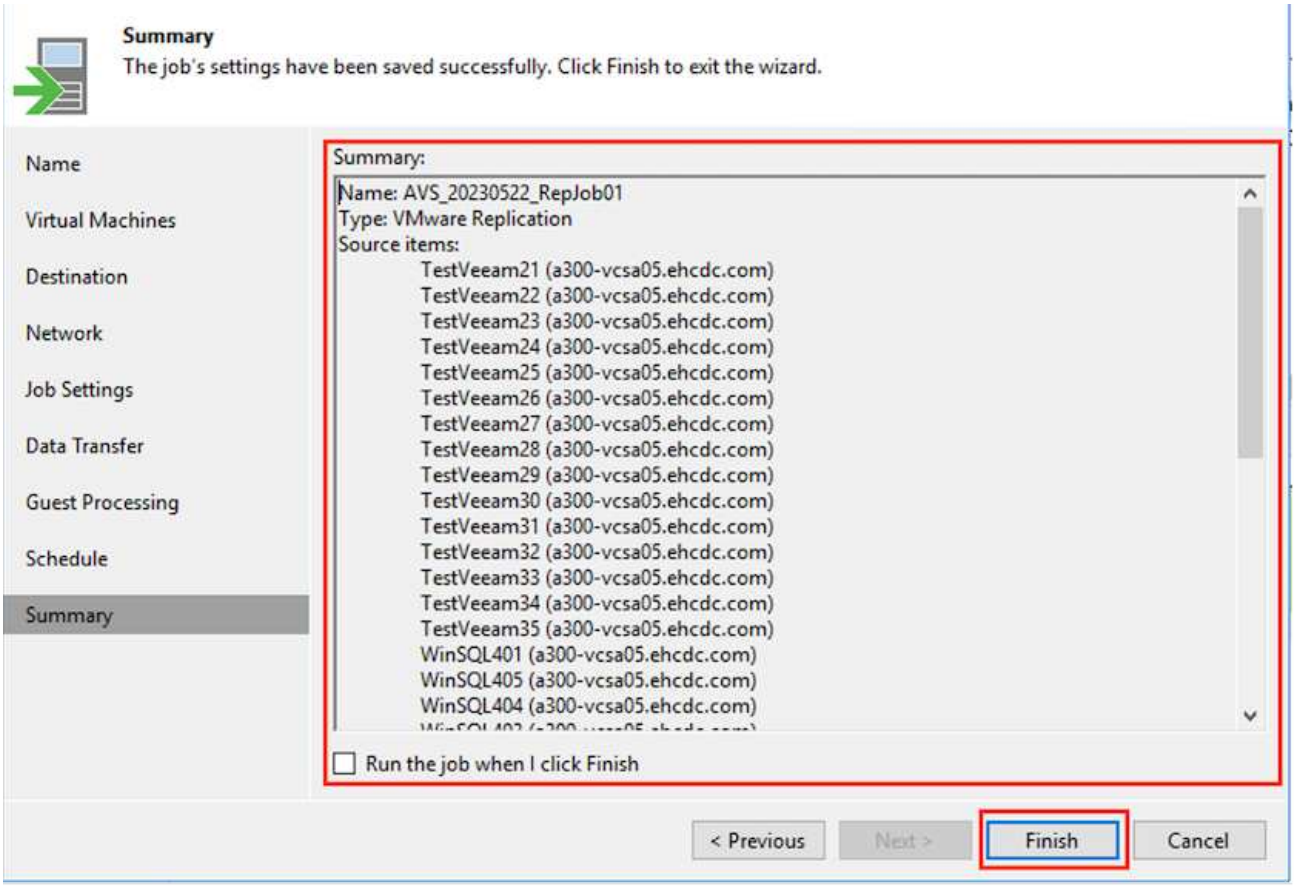
7. À l'étape **Paramètres de tâche**, spécifiez le référentiel de sauvegarde qui stockera les métadonnées des répliques de machines virtuelles, la politique de rétention, etc.
8. Mettez à jour les serveurs proxy **Source** et **Cible** dans l'étape **Transfert de données** et laissez la sélection **Automatique** (par défaut) et gardez l'option **Direct** sélectionnée et cliquez sur **Suivant**.
9. À l'étape **Traitement des invités**, sélectionnez l'option **Activer le traitement sensible aux applications** selon vos besoins. Cliquez sur **Suivant**.



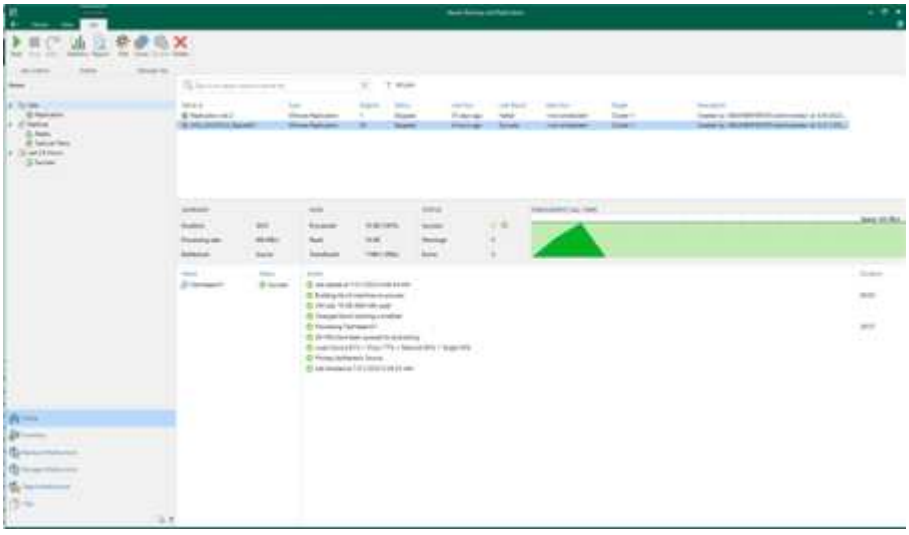
10. Choisissez la planification de réplication pour exécuter le travail de réplication régulièrement.



11. À l'étape **Résumé** de l'assistant, vérifiez les détails de la tâche 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 laissez la case décochée. Cliquez ensuite sur **Terminer** pour fermer l'assistant.



Une fois le travail de réplication démarré, les machines virtuelles avec le suffixe spécifié seront renseignées sur le cluster/hôte AVS SDDC de destination.



Pour plus d'informations sur la réplication Veeam, reportez-vous à"Comment fonctionne la réplication"

▼ Étape 2 : Créer un plan de basculement

Une fois la réplication ou l'amorçage initial terminé, créez le plan de basculement. Le plan de basculement

permet d'effectuer le basculement des machines virtuelles dépendantes une par une ou en tant que groupe automatiquement. Le plan de basculement est le plan directeur de l'ordre dans lequel les machines virtuelles sont traitées, y compris les délais de démarrage. Le plan de basculement permet également de garantir que les machines virtuelles dépendantes critiques sont déjà en cours d'exécution.

Pour créer le plan, accédez à la nouvelle sous-section appelée **Répliques** et sélectionnez **Plan de basculement**. Choisissez les machines virtuelles appropriées. Veeam Backup & Replication recherchera les points de restauration les plus proches de ce point dans le temps et les utilisera pour démarrer les répliques de machines virtuelles.

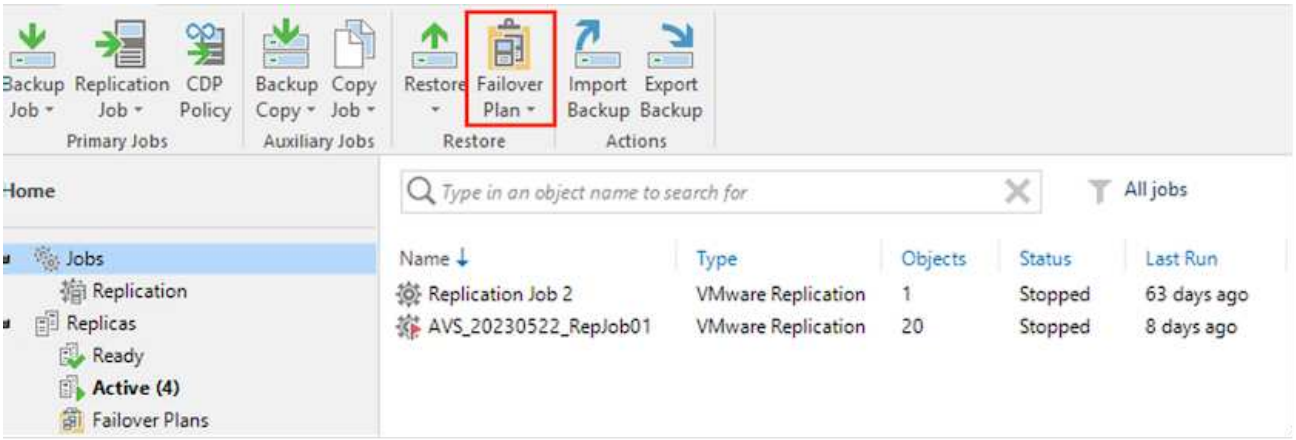
ⓘ Le plan de basculement ne peut être ajouté qu'une fois la réplication initiale terminée et les répliques de machines virtuelles à l'état Prêt.

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

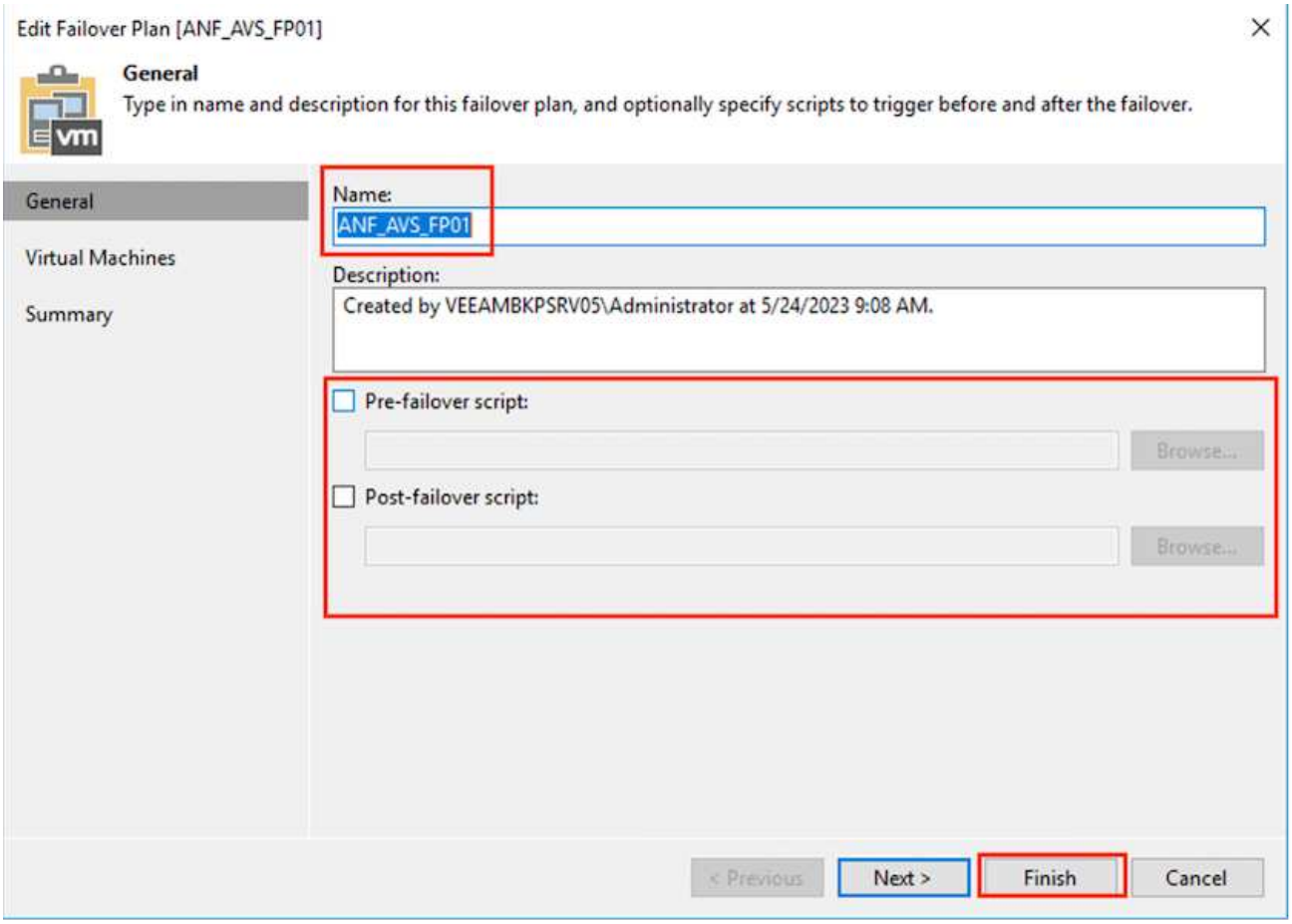
ⓘ Pendant le processus de basculement, les machines virtuelles sources ne seront pas mises hors tension

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

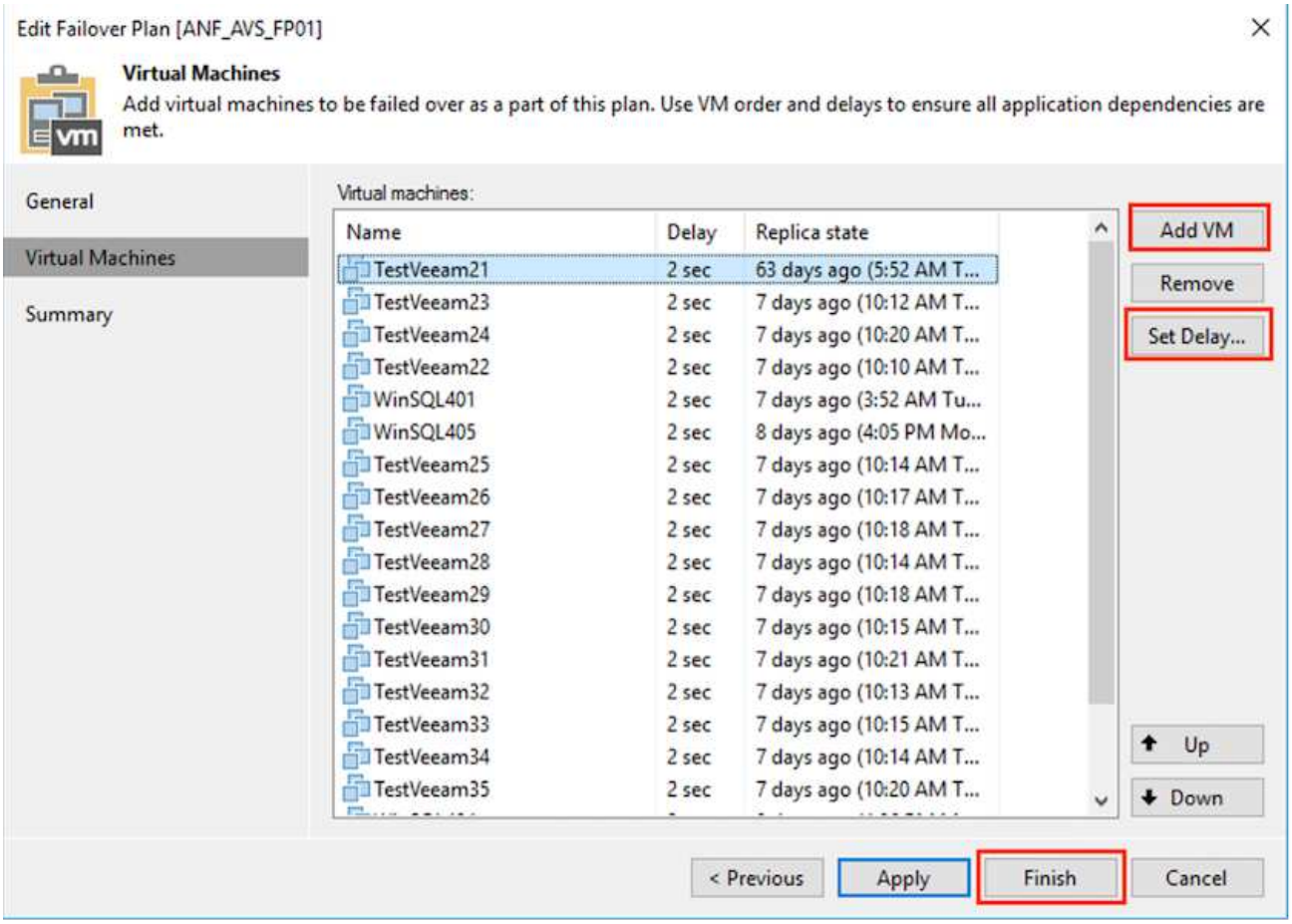
1. Sur la vue Accueil. Cliquez avec le bouton droit sur le nœud Répliques et sélectionnez Plans de basculement > Plan de basculement > VMware vSphere.



2. Donnez ensuite un nom et une description au plan. Un script de pré et post-basculement peut être ajouté selon les besoins. 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 des machines virtuelles et les délais de démarrage pour répondre aux dépendances de l'application.



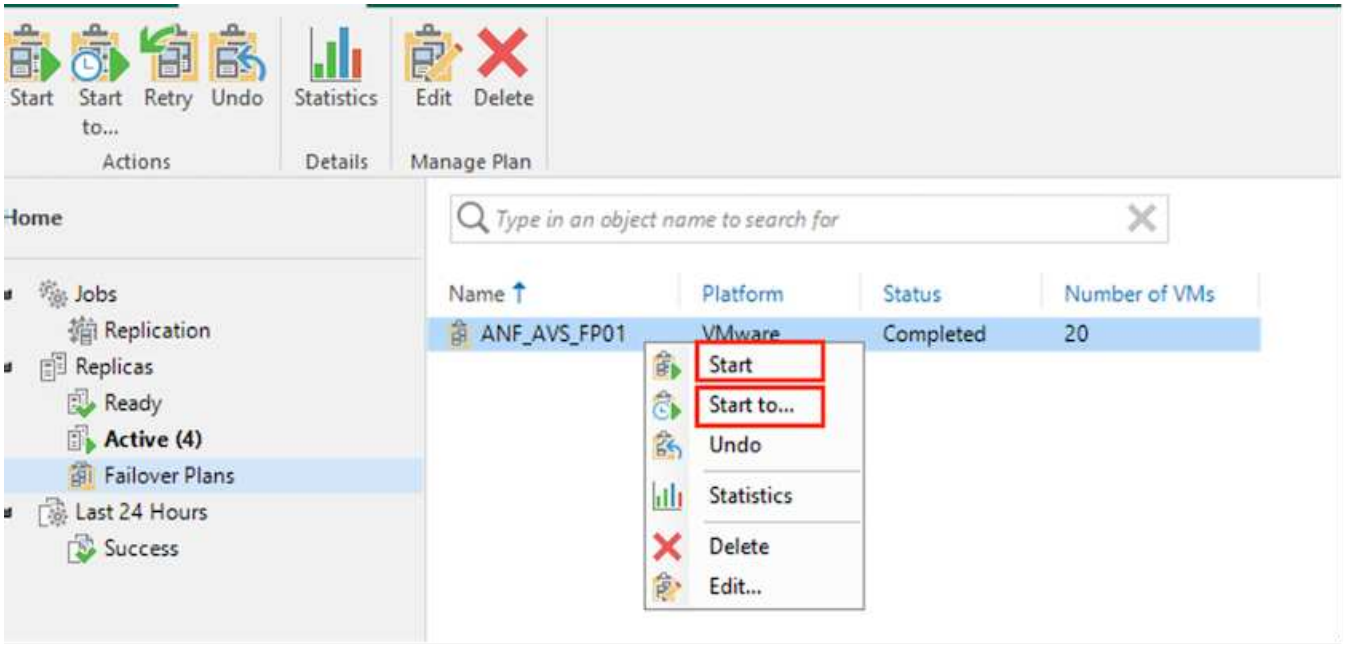
Pour plus d'informations sur la création de tâches de réplication, reportez-vous à"Création de tâches de réplication" .

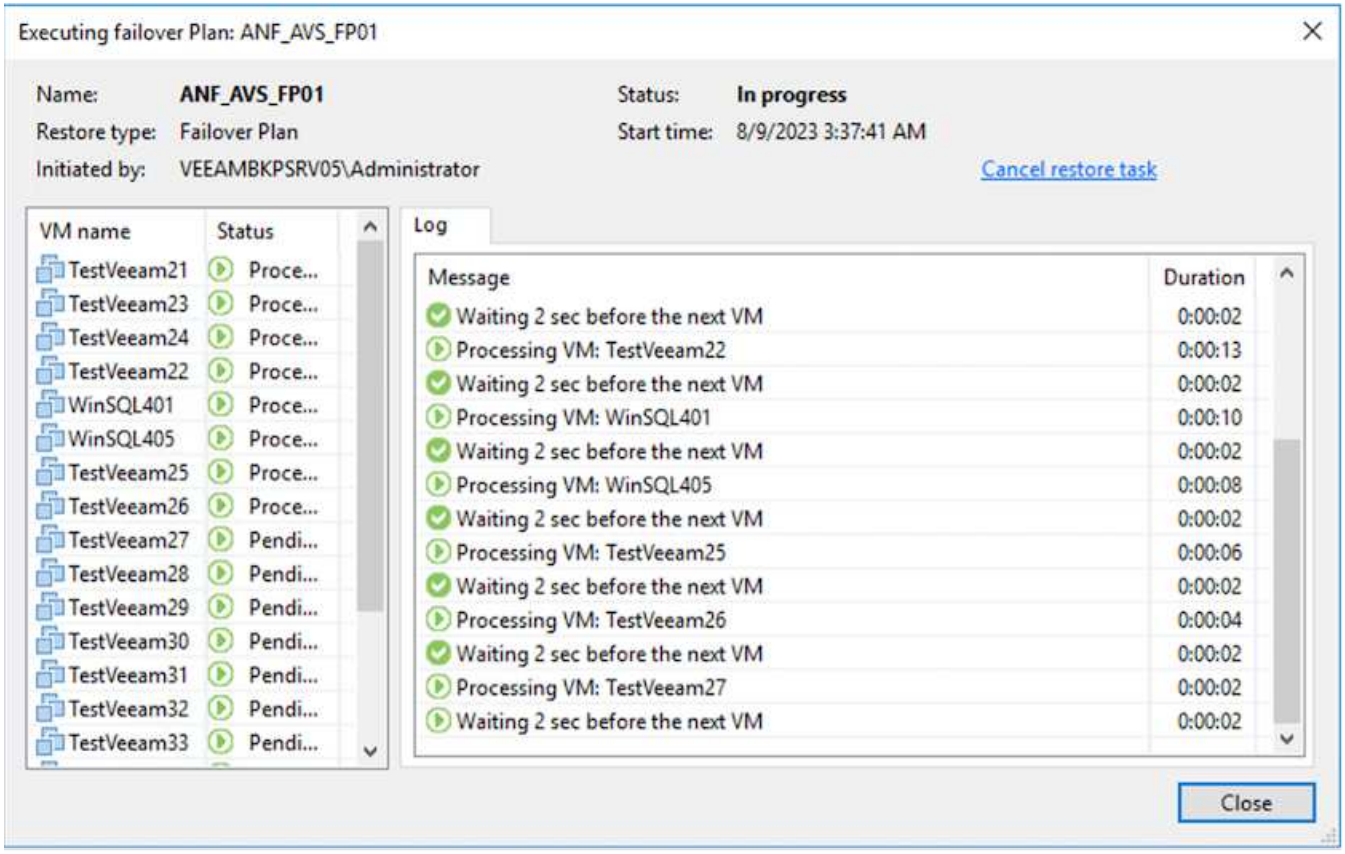
▼ Étape 3 : Exécuter le plan de basculement

Lors du basculement, la machine virtuelle source du site de production est basculée vers sa réplique sur le site de reprise après sinistre. Dans le cadre du processus de basculement, Veeam Backup & Replication restaure la réplique de la machine virtuelle au point de restauration requis et déplace toutes les activités d'E/S de la machine virtuelle source vers sa réplique. Les répliques peuvent être utilisées non seulement en cas de catastrophe, mais également pour simuler des exercices de reprise après sinistre. 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.

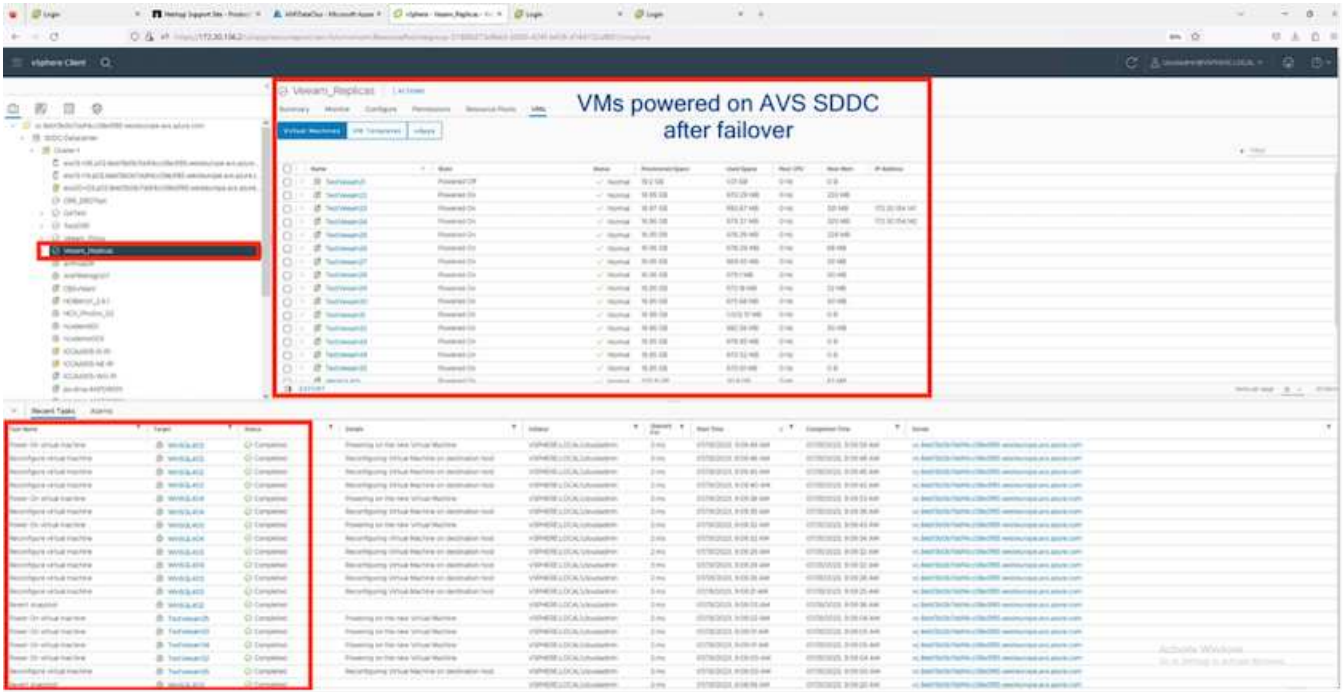
ⓘ Assurez-vous que la segmentation du réseau est en place pour éviter les conflits IP lors du basculement.

Pour démarrer le plan de basculement, cliquez simplement sur l'onglet **Plans de basculement** et faites un clic droit sur votre plan de basculement. Sélectionnez ***Démarrer**. Cela basculera en utilisant les derniers points de restauration des répliques de VM. Pour basculer vers des points de restauration spécifiques de répliques de machines virtuelles, sélectionnez **Démarrer vers**.

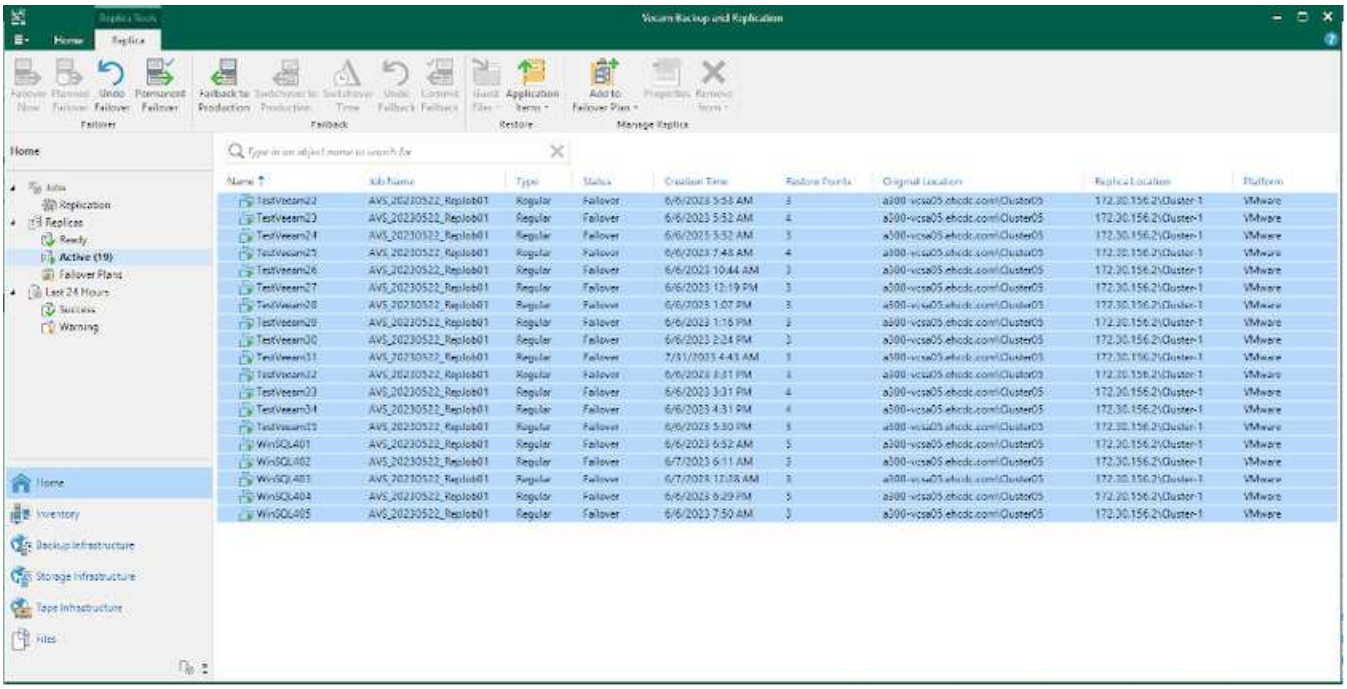




L'état de la réplique de machine virtuelle passe de Prêt à Basculement et les machines virtuelles démarrent sur le cluster/hôte SDDC Azure VMware Solution (AVS) de destination.



Une fois le basculement terminé, le statut des machines virtuelles passera à « Basculement ».



Veeam Backup & Replication arrête toutes les activités de réplication pour la machine virtuelle source jusqu'à ce que sa réplique soit ramenée à l'état Prêt.

Pour des informations détaillées sur les plans de basculement, reportez-vous à"Plans de basculement" .

▼ **Étape 4 : Retour au site de production**

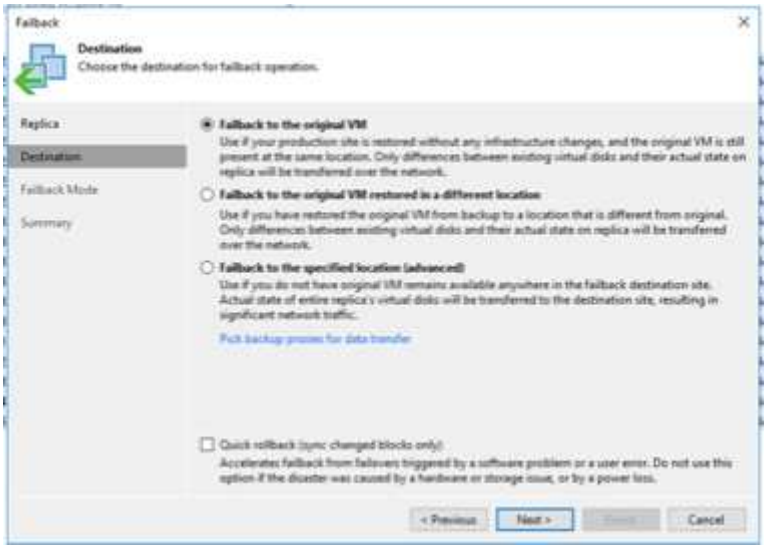
Lorsque le plan de basculement est en cours d'exécution, il est considéré comme une étape intermédiaire et doit être finalisé en fonction des besoins. Les options incluent les suivantes :

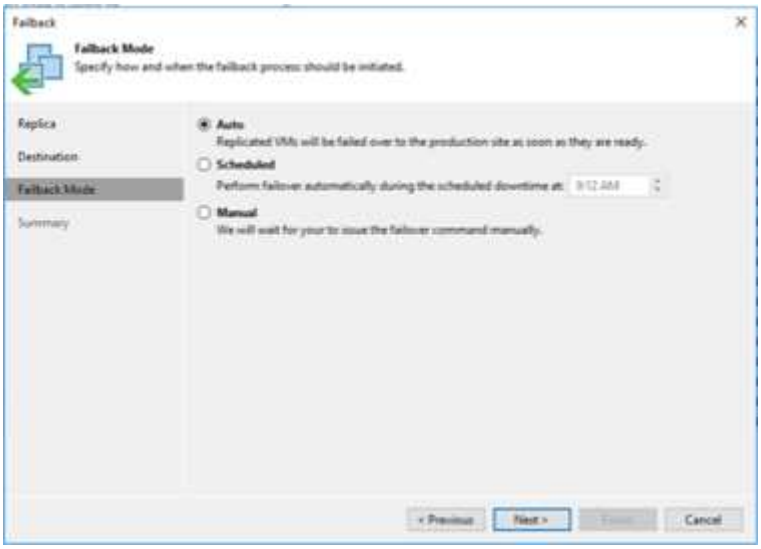
- **Retour à la production** - revenez à la machine virtuelle d'origine et transférez toutes les modifications qui ont eu lieu pendant l'exécution de la réplique de la machine virtuelle vers la machine virtuelle d'origine.

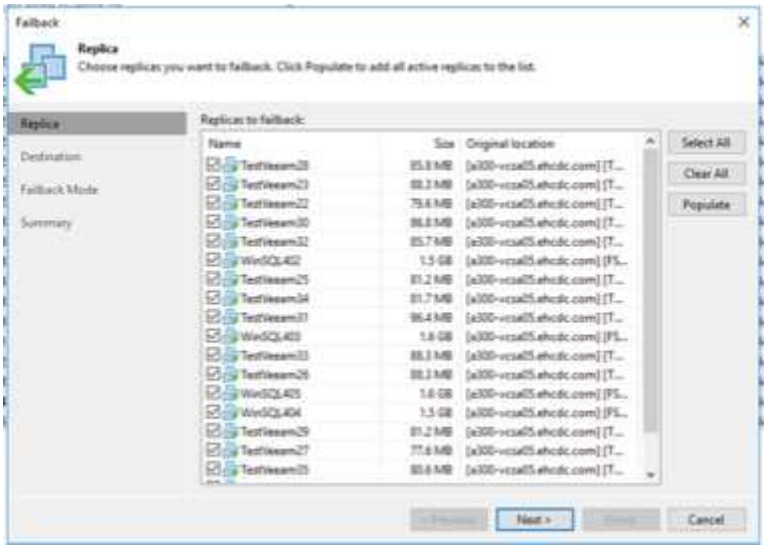
> Lorsque vous effectuez une restauration automatique, les modifications sont uniquement transférées mais non publiées. Choisissez **Commit failback** (une fois que la machine virtuelle d'origine est confirmée comme fonctionnant comme prévu) ou Annuler la restauration pour revenir à la réplique de la machine virtuelle si la machine virtuelle d'origine ne fonctionne pas comme prévu.

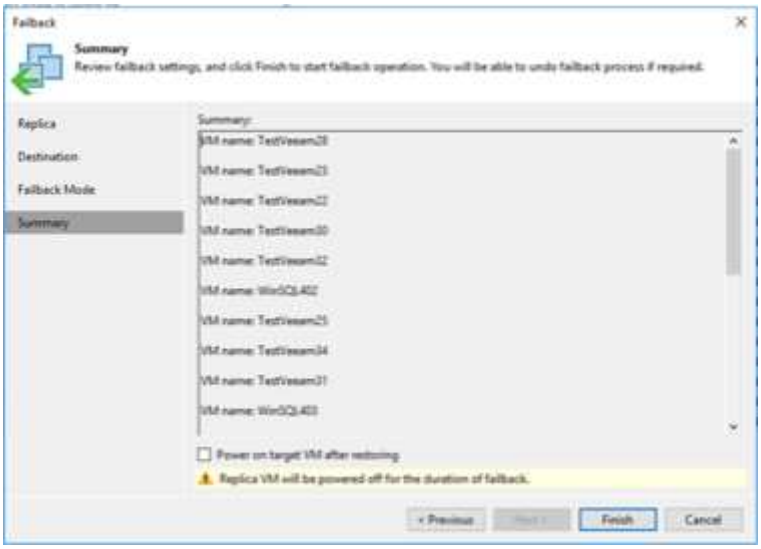
- **Annuler le basculement** - revenez à la machine virtuelle d'origine et annulez toutes les modifications apportées à la réplique de la machine virtuelle pendant son exécution.
- **Basculement permanent** - basculez définitivement de la machine virtuelle d'origine vers une réplique de machine virtuelle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

Dans cette démo, le retour à la production a été choisi. La restauration vers la machine virtuelle d'origine a été sélectionnée lors de l'étape Destination de l'assistant et la case à cocher « Mettre sous tension la machine virtuelle après la restauration » a été activée.



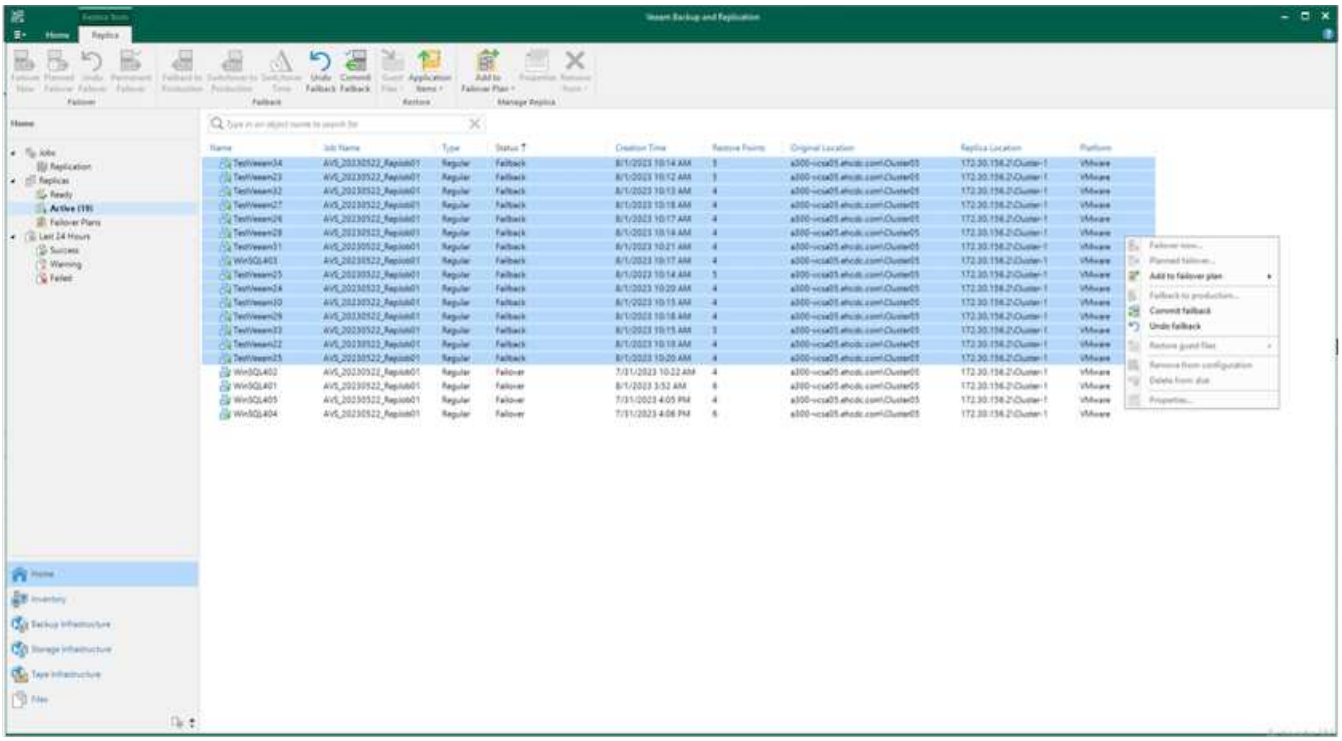




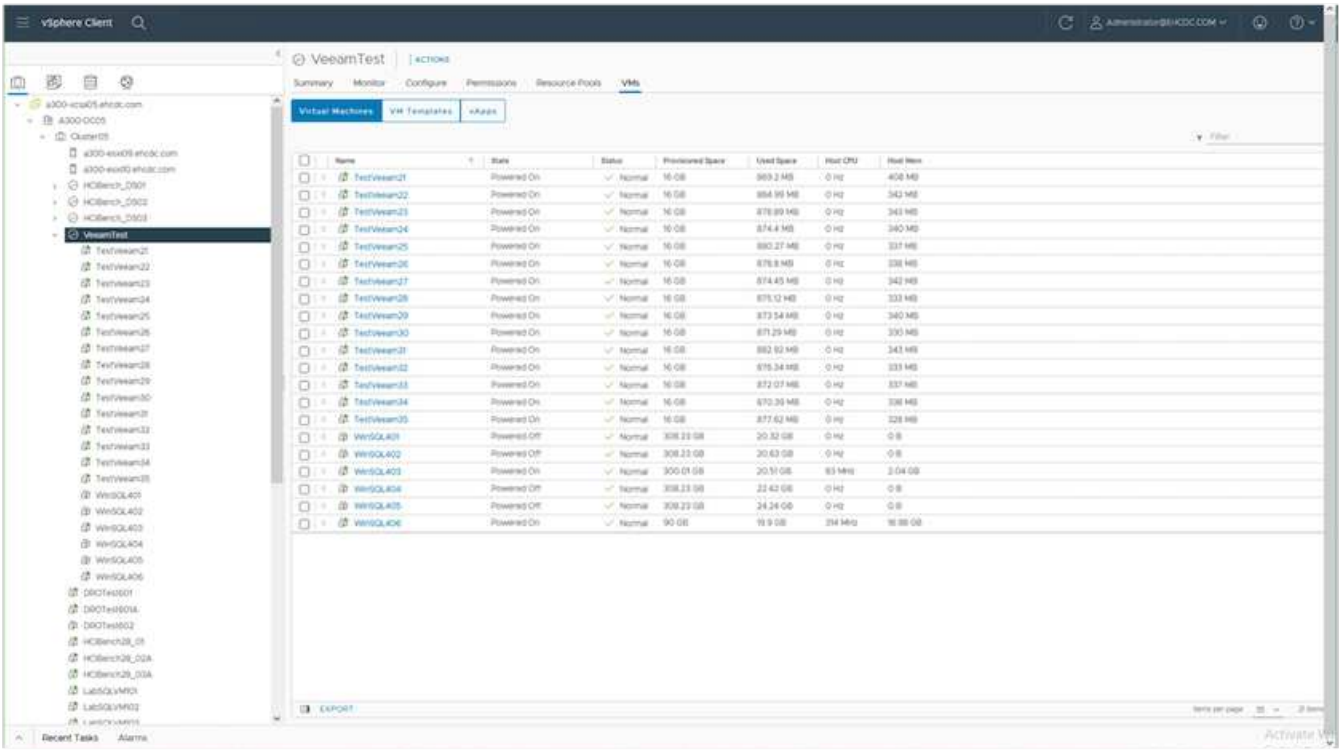


La validation de la restauration est l'un des moyens de finaliser l'opération de restauration. Lorsque la restauration est validée, elle confirme que les modifications envoyées à la machine virtuelle qui est restaurée (la machine virtuelle de production) fonctionnent comme prévu. Après l'opération de validation, Veeam Backup & Replication reprend les activités de réplication pour la machine virtuelle de production.

Pour des informations détaillées sur le processus de restauration automatique, reportez-vous à la documentation Veeam."Basculement et restauration pour la réplication" .



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



Conclusion

La capacité de stockage de données Azure NetApp Files permet à Veeam ou à tout outil tiers validé de fournir une solution DR à faible coût en exploitant les clusters Pilot Light au lieu de mettre en place un grand cluster uniquement pour héberger les répliques de machines virtuelles. Cela offre un moyen efficace de gérer un plan de reprise après sinistre personnalisé et sur mesure et de réutiliser les produits de sauvegarde existants en

interne pour la reprise après sinistre, permettant une reprise après sinistre basée sur le cloud en quittant les centres de données de reprise après sinistre sur site. Il est possible de basculer en cliquant sur un bouton en cas de sinistre ou de basculer automatiquement si un sinistre survient.

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

Migrer les charges de travail sur Azure/AVS

TR-4940 : Migrer des charges de travail vers une banque de données Azure NetApp Files à l'aide de VMware HCX - Guide de démarrage rapide

L'un des cas d'utilisation les plus courants de la solution Azure VMware et du magasin de données Azure NetApp Files est la migration des charges de travail VMware. VMware HCX est une option privilégiée et fournit divers mécanismes de migration pour déplacer des machines virtuelles (VM) sur site et leurs données vers des banques de données Azure NetApp Files .

Présentation : Migration de machines virtuelles avec VMware HCX, banques de données Azure NetApp Files et solution Azure VMware

VMware HCX est principalement une plate-forme de migration conçue pour simplifier la migration des applications, le rééquilibrage de la charge de travail et même la continuité des activités dans les clouds. Il est inclus dans le cadre d'Azure VMware Solution Private Cloud et offre de nombreuses façons de migrer les charges de travail et peut être utilisé pour les opérations de reprise après sinistre (DR).

Ce document fournit des instructions étape par étape pour le provisionnement du magasin de données Azure NetApp Files, suivi du téléchargement, du déploiement et de la configuration de VMware HCX, y compris tous ses principaux composants sur site et côté Azure VMware Solution, 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 banque de données car la migration s'effectue au niveau de la machine virtuelle. Par conséquent, ce document s'applique aux clients NetApp existants et aux clients non NetApp qui prévoient de déployer Azure NetApp Files avec Azure VMware Solution pour un déploiement cloud VMware rentable.

▼ **Étapes de haut niveau**

Cette liste fournit les étapes de haut niveau 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 de HCX Connector Open Virtualization Appliance (OVA) sur le serveur VMware vCenter local.
3. Activez HCX avec la clé de licence.
4. Associez le connecteur VMware HCX sur site à Azure VMware Solution HCX Cloud Manager.
5. Configurez le profil réseau, le profil de calcul et le maillage de services.
6. (Facultatif) Effectuez une extension du réseau pour éviter la ré-IP pendant les migrations.
7. Validez l'état de l'appliance et assurez-vous que la migration est possible.

8. Migrer les charges de travail de la machine virtuelle.

▼ **Prérequis**

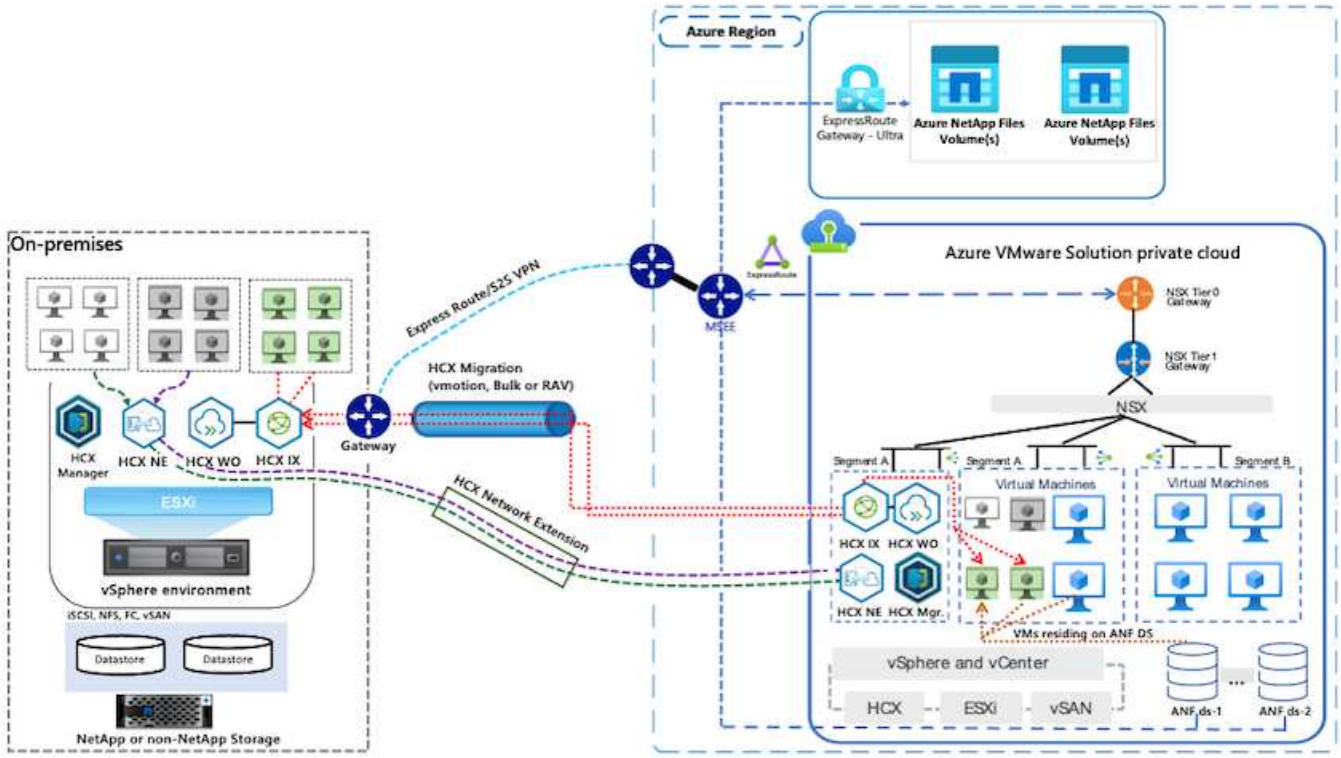
Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, voir ceci "lien" . Une fois les conditions préalables, y compris la connectivité, en place, configurez et activez HCX en générant la clé de licence à partir du portail Azure VMware Solution. 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 centre de données défini par logiciel (SDDC) de solution Azure VMware existant ou créez un cloud privé en l'utilisant"Lien NetApp" ou ceci "Lien Microsoft" .
- La migration des machines virtuelles et des données associées à partir du centre de données local compatible VMware vSphere nécessite une connectivité réseau du centre de données vers l'environnement SDDC. Avant de migrer les charges de travail, "configurer une connexion VPN site à site ou une connexion Express Route Global Reach" entre l'environnement sur site et le cloud privé respectif.
- Le chemin réseau de l'environnement VMware vCenter Server local vers le cloud privé Azure VMware Solution doit prendre en charge la migration des machines virtuelles à l'aide de vMotion.
- Assurez-vous que les informations requises "règles et ports du pare-feu" sont autorisés pour le trafic vMotion entre le vCenter Server sur site et le vCenter SDDC. Sur 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 banque de données dans Azure VMware Solution. Suivez les étapes détaillées dans ce "lien" pour attacher des banques de données Azure NetApp Files aux hôtes Azure VMware Solutions.

▼ **Architecture de haut niveau**

À des fins de test, l'environnement de laboratoire local utilisé pour cette validation a été connecté via un VPN site à site, qui permet la connectivité sur site à Azure VMware Solution.



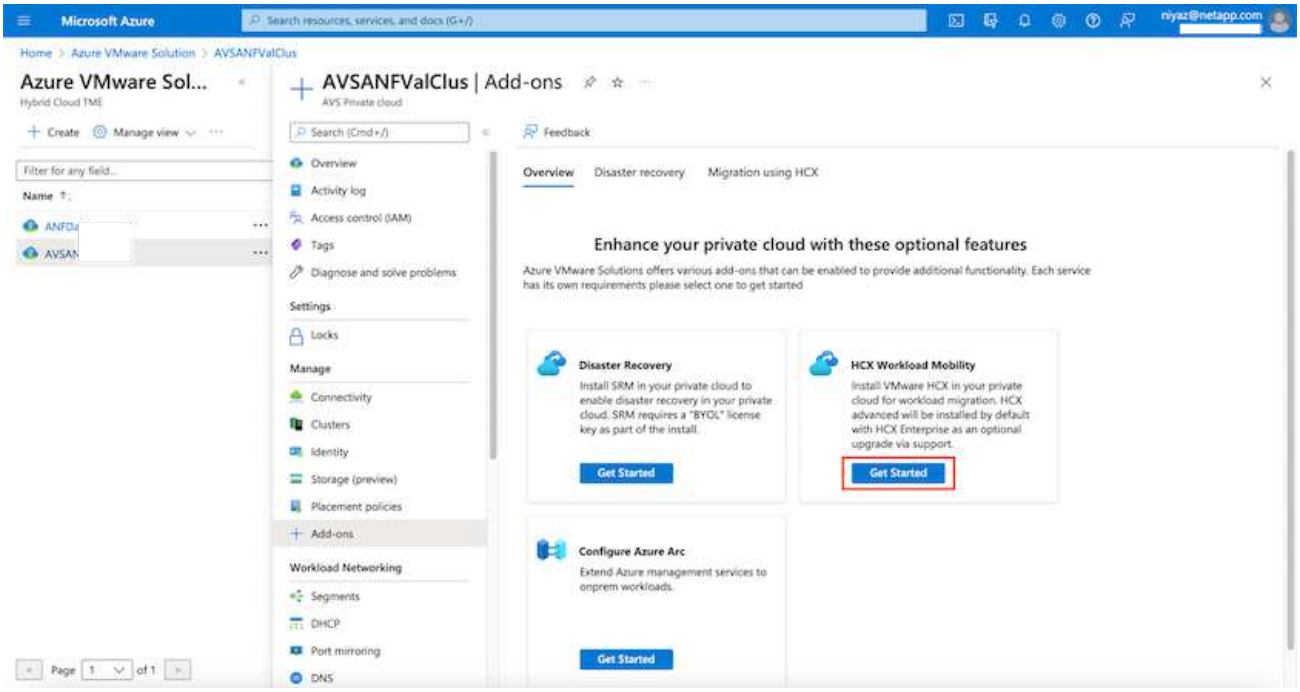
Déploiement de la solution

Suivez la série d'étapes pour terminer le déploiement de cette solution :

▼ **Étape 1 : Installez HCX via le portail Azure à l'aide de l'option Modules complémentaires**

Pour effectuer l'installation, procédez comme suit :

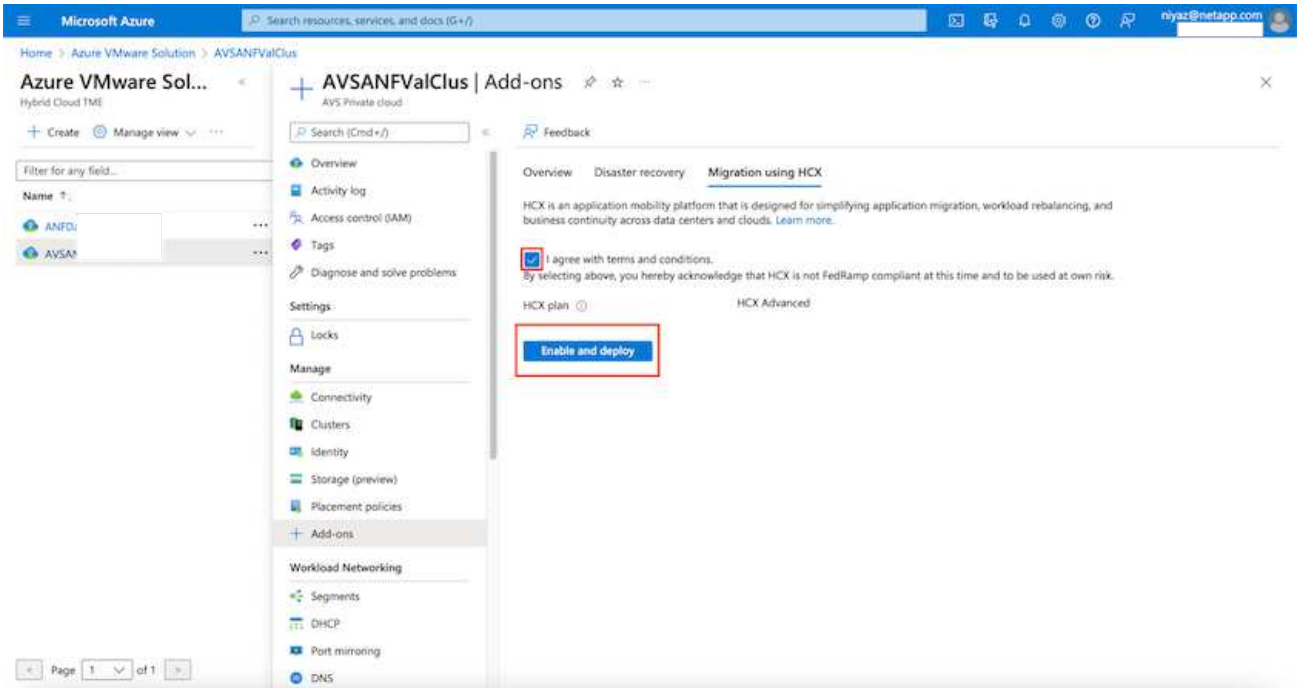
1. Connectez-vous au portail Azure et accédez au cloud privé Azure VMware Solution.
2. Sélectionnez le cloud privé approprié et accédez aux modules complémentaires. Cela peut être fait en naviguant vers **Gérer > Modules complémentaires**.
3. Dans la section Mobilité de la charge de travail HCX, cliquez sur **Commencer**.



4. Sélectionnez l'option **J'accepte les conditions générales** 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.



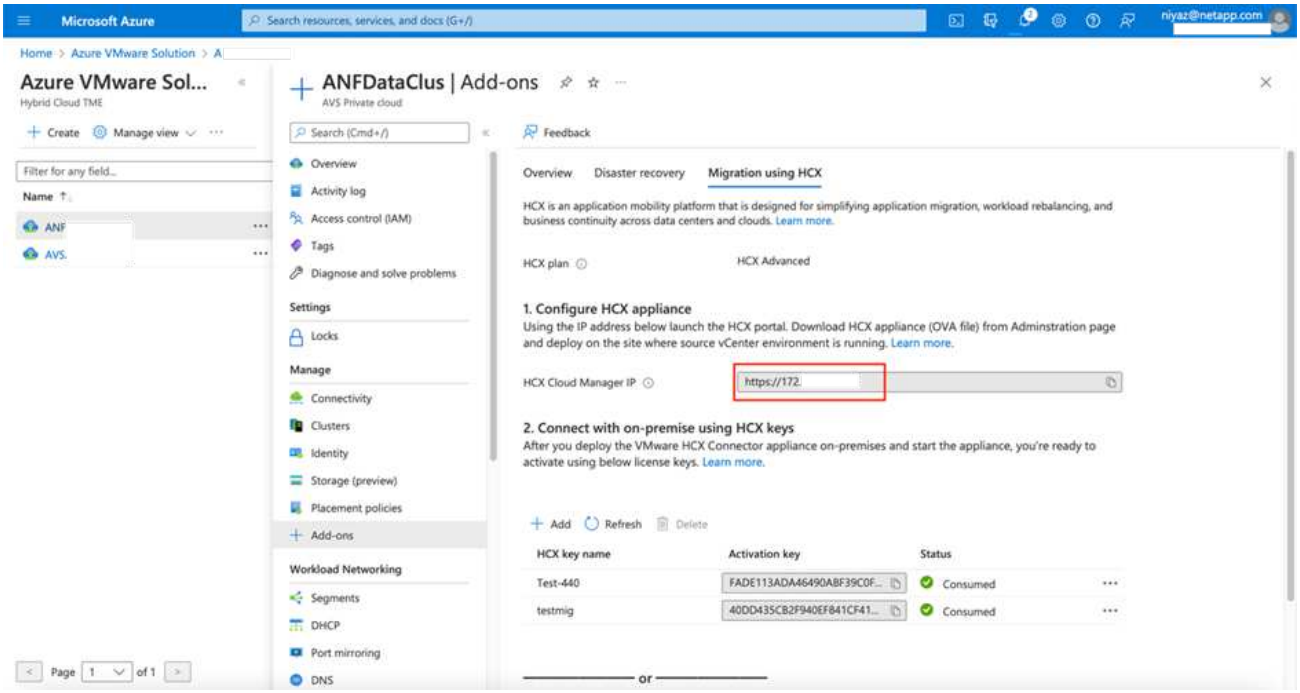
▼ **Étape 2 : Déployer le programme d'installation OVA sur le serveur vCenter local**

Pour que le connecteur sur site se connecte au gestionnaire HCX dans Azure VMware Solution, assurez-vous que les ports de pare-feu appropriés sont ouverts dans l'environnement sur site.

Pour télécharger et installer HCX Connector sur le serveur vCenter local, procédez comme suit :

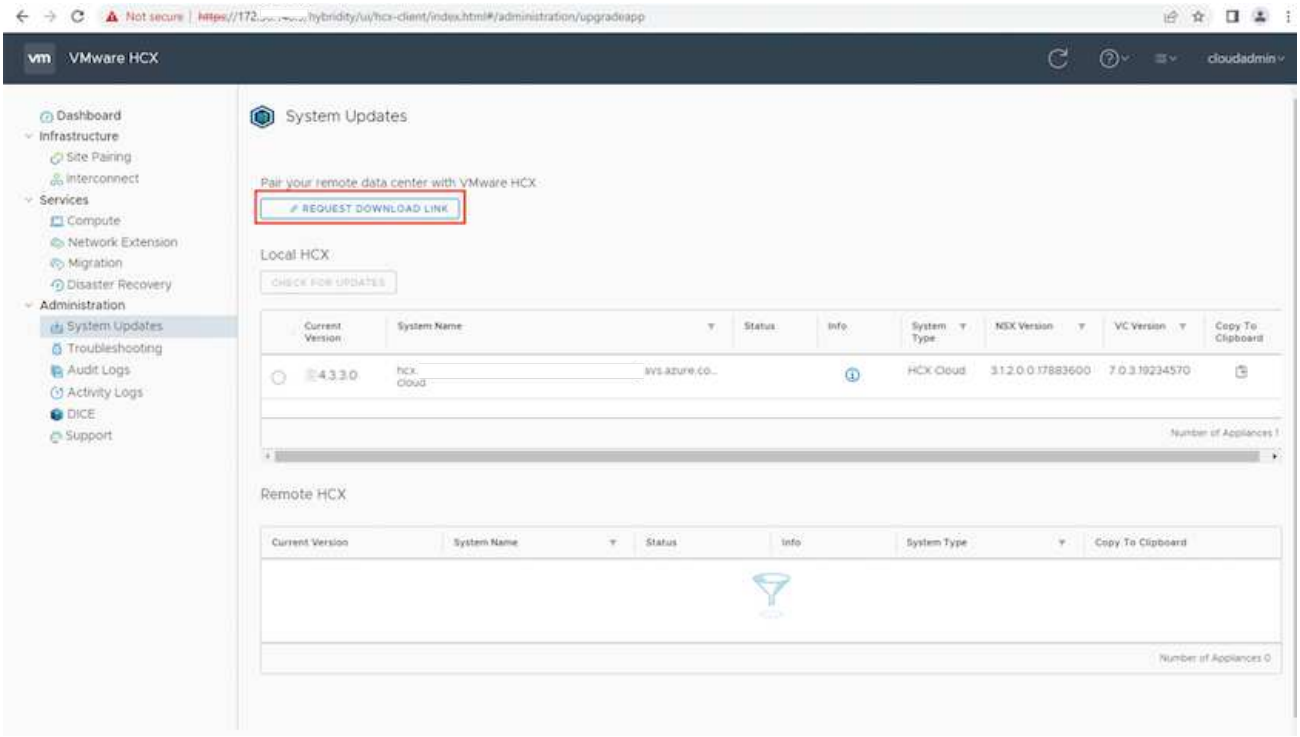
1. Depuis le portail Azure, accédez à la solution Azure VMware, sélectionnez le cloud privé, puis sélectionnez **Gérer > Modules complémentaires > Migration** à l'aide de HCX et copiez le portail HCX Cloud Manager pour télécharger le fichier OVA.

   Utilisez les informations d'identification de l'utilisateur CloudAdmin par défaut pour accéder au portail HCX.

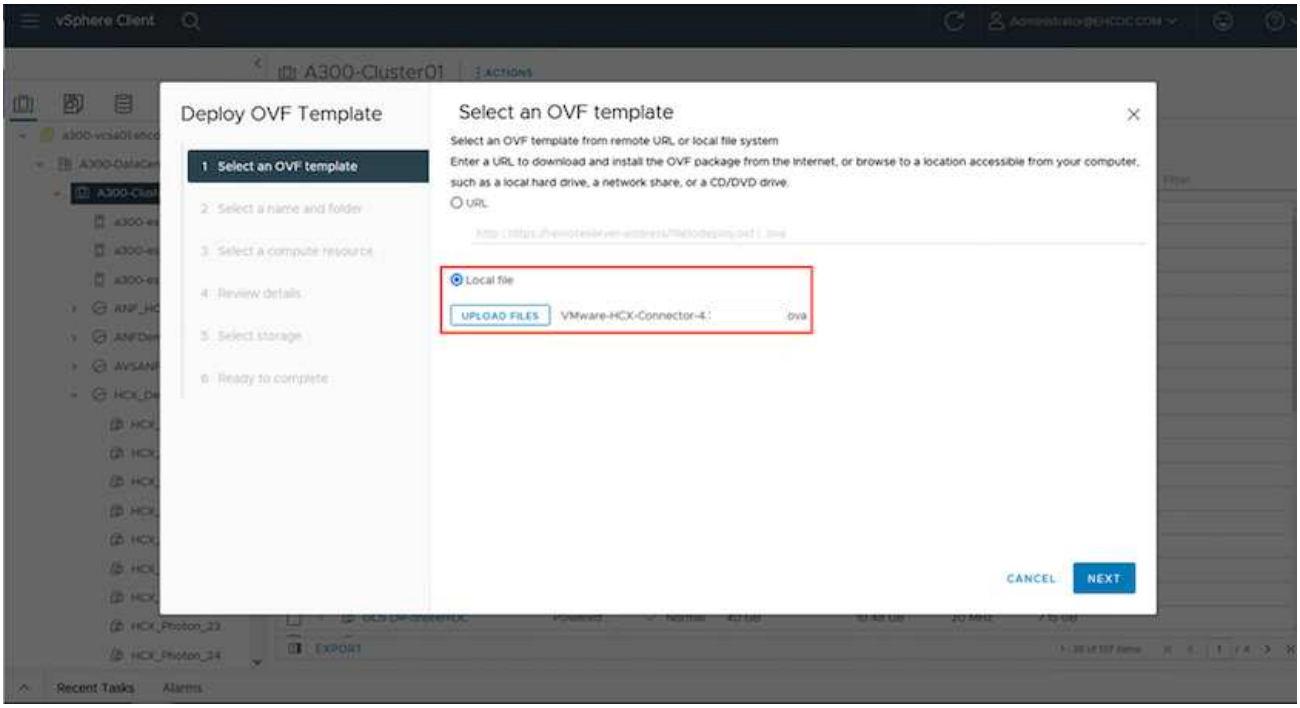


2. Après avoir accédé au portail HCX avec cloudadmin@vsphere.local à l'aide de jumphost, accédez à **Administration > Mises à jour système** et cliquez sur **Demander un lien de téléchargement**.

   Téléchargez ou copiez le lien vers l'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 local.



3. Une fois l'OVA téléchargé, déployez-le sur l'environnement VMware vSphere local à l'aide de l'option **Déployer le modèle OVF**.



4. Saisissez toutes les informations requises pour le déploiement OVA, cliquez sur **Suivant**, puis sur **Terminer** pour déployer le connecteur VMware HCX OVA.

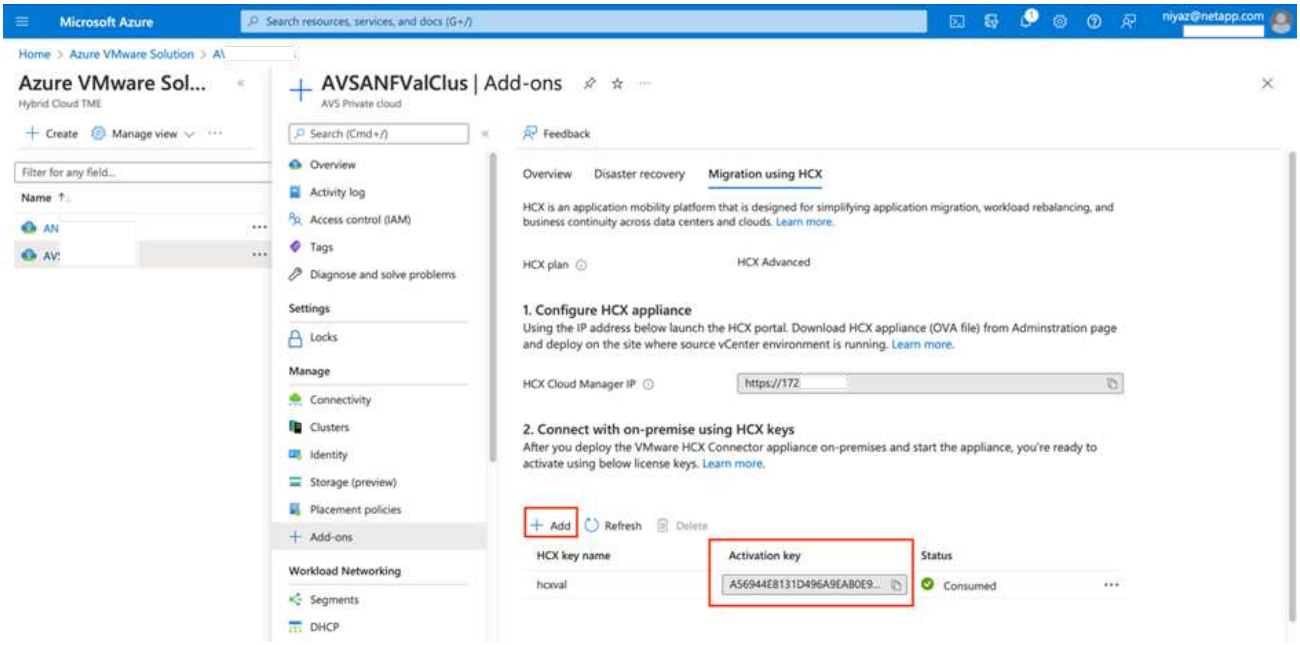
> Mettez sous tension l'appliance virtuelle manuellement.

Pour des instructions étape par étape, consultez le "Guide de l'utilisateur de VMware HCX" .

▼ Étape 3 : Activer HCX Connector avec la clé de licence

Après avoir déployé VMware HCX Connector OVA sur site et démarré l'appliance, procédez comme suit pour activer HCX Connector. 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 Azure VMware, sélectionnez le cloud privé, puis sélectionnez **Gérer > Modules complémentaires > Migration à l'aide de HCX**.
2. Sous **Se connecter sur site à l'aide des clés HCX**, cliquez sur **Ajouter** et copiez la clé d'activation.



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

3. Connectez-vous au gestionnaire VMware HCX sur site à l'adresse `"https://hcxmanagerIP:9443"` en utilisant les informations d'identification de l'administrateur.

> ⓘ Utilisez le mot de passe défini lors du déploiement OVA.

4. Dans la licence, entrez la clé copiée à l'étape 3 et cliquez sur **Activer**.

> ⓘ Le connecteur HCX sur site doit avoir accès à Internet.

5. Sous **Emplacement du centre de données**, indiquez l'emplacement le plus proche pour l'installation de VMware HCX Manager sur site. Cliquez sur **Continuer**.
6. Sous **Nom du système**, mettez à jour le nom et cliquez sur **Continuer**.
7. Cliquez sur **Oui, continuer**.
8. Sous **Connectez votre 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**.

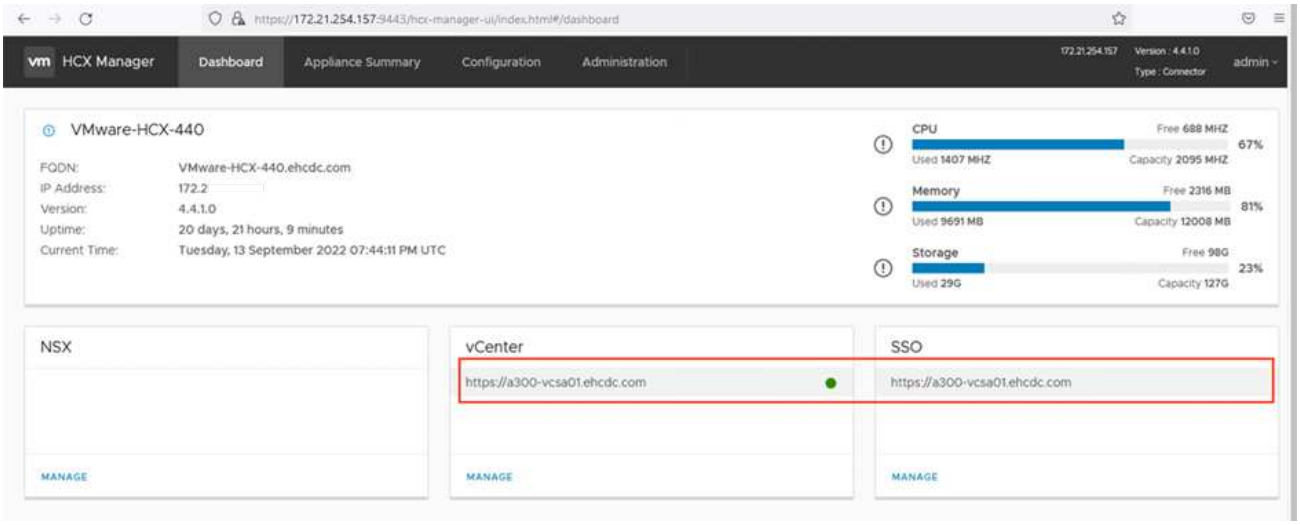
> ⓘ Utilisez le FQDN pour éviter les problèmes de connectivité ultérieurs.

9. Sous **Configurer SSO/PSC**, indiquez le nom de domaine complet ou l'adresse IP du Platform Services Controller et cliquez sur **Continuer**.

Saisissez le nom de domaine complet ou l'adresse IP du serveur VMware vCenter.

10. Vérifiez que les informations saisies sont correctes et cliquez sur **Redémarrer**.
11. Après le redémarrage des services, vCenter Server s'affiche en vert sur la page qui s'affiche. vCenter Server et SSO doivent tous deux disposer des paramètres de configuration appropriés, qui doivent être identiques à ceux de la page précédente.

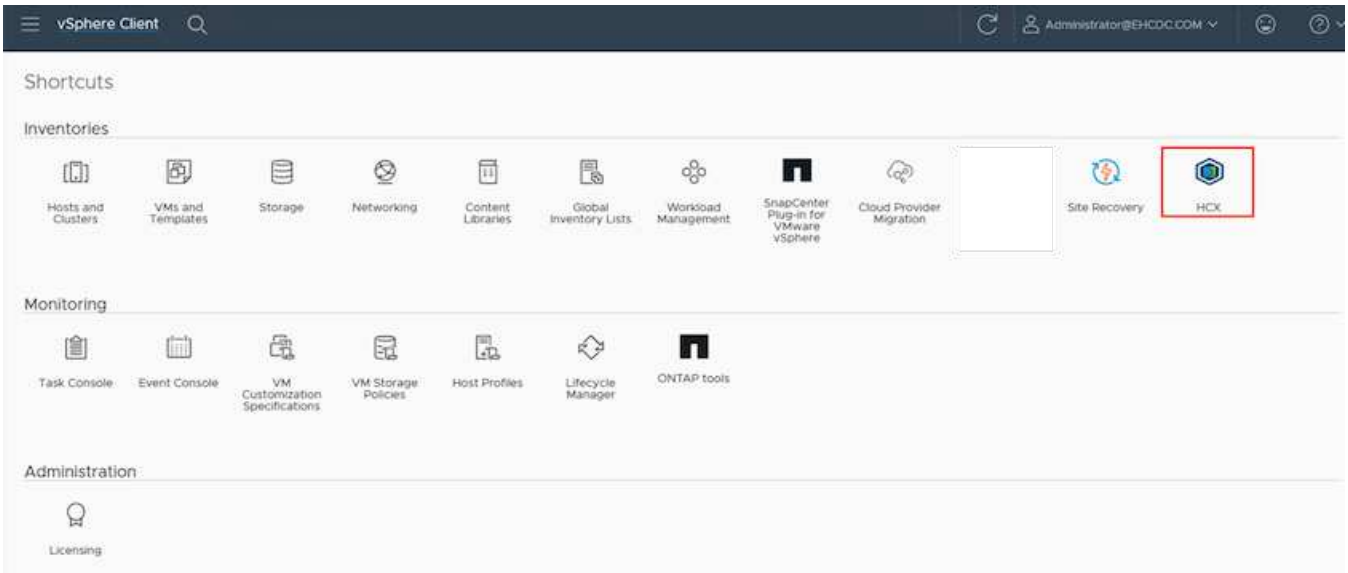
Ce processus devrait prendre environ 10 à 20 minutes pour que le plug-in soit ajouté au serveur vCenter.



▼ **Étape 4 : Associez le connecteur VMware HCX sur site à Azure VMware Solution HCX Cloud Manager**

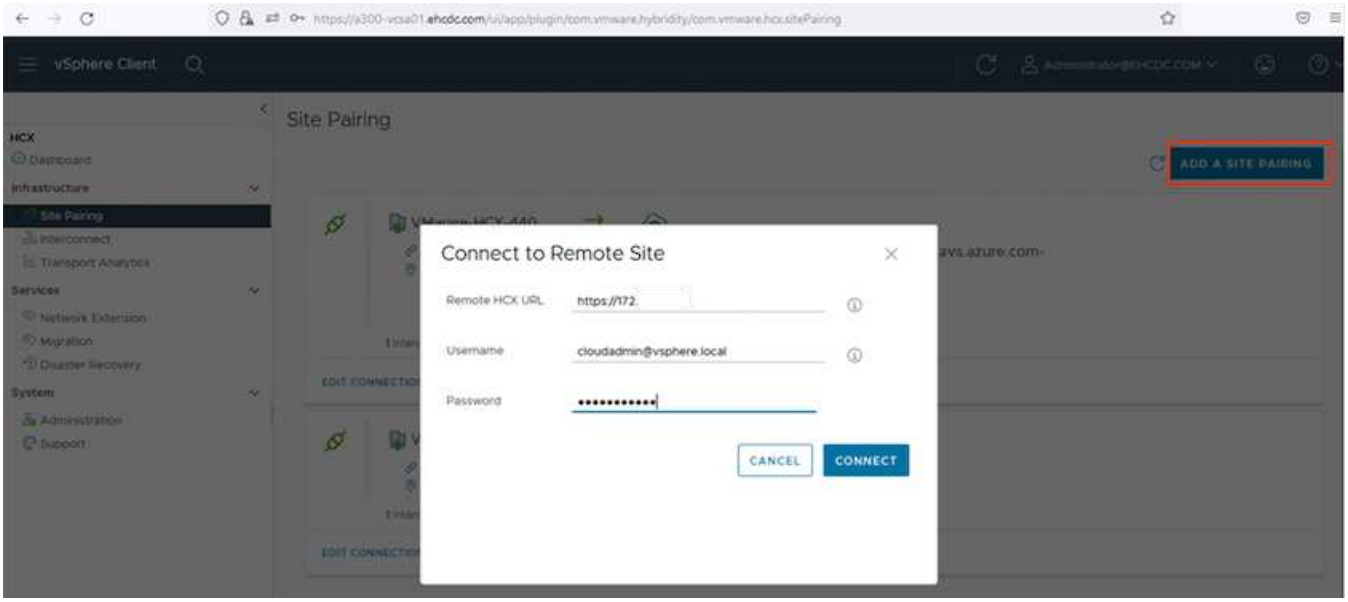
Une fois HCX Connector installé sur site et dans Azure VMware Solution, configurez le connecteur VMware HCX sur site pour le cloud privé Azure VMware Solution en ajoutant le couplage. Pour configurer le couplage de sites, procédez comme suit :

1. Pour créer une paire de sites entre l'environnement vCenter local et Azure VMware Solution SDDC, connectez-vous au serveur vCenter local et accédez au nouveau plug-in HCX vSphere Web Client.



1. Sous Infrastructure, cliquez sur **Ajouter un appariement de sites**.

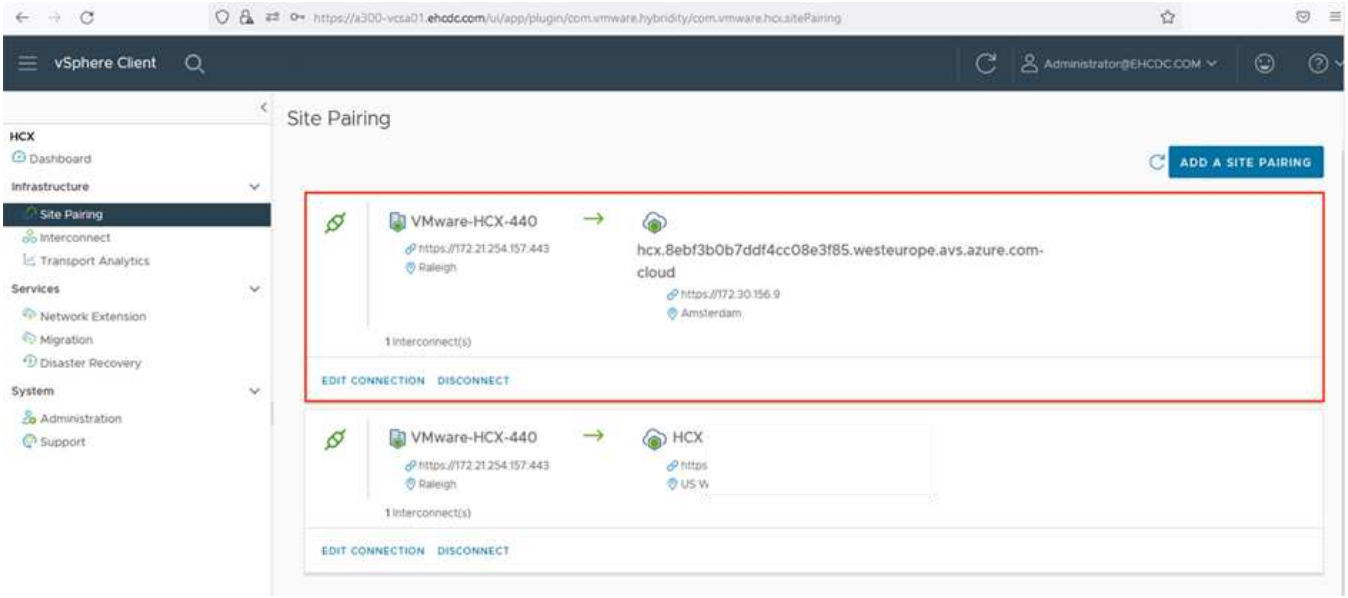
Saisissez l'URL ou l'adresse IP d'Azure VMware Solution HCX Cloud Manager et les informations d'identification du rôle CloudAdmin pour accéder au cloud privé.



1. Cliquez sur **Connecter**.

VMware HCX Connector doit pouvoir acheminer vers l'adresse IP de HCX Cloud Manager via le port 443.

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



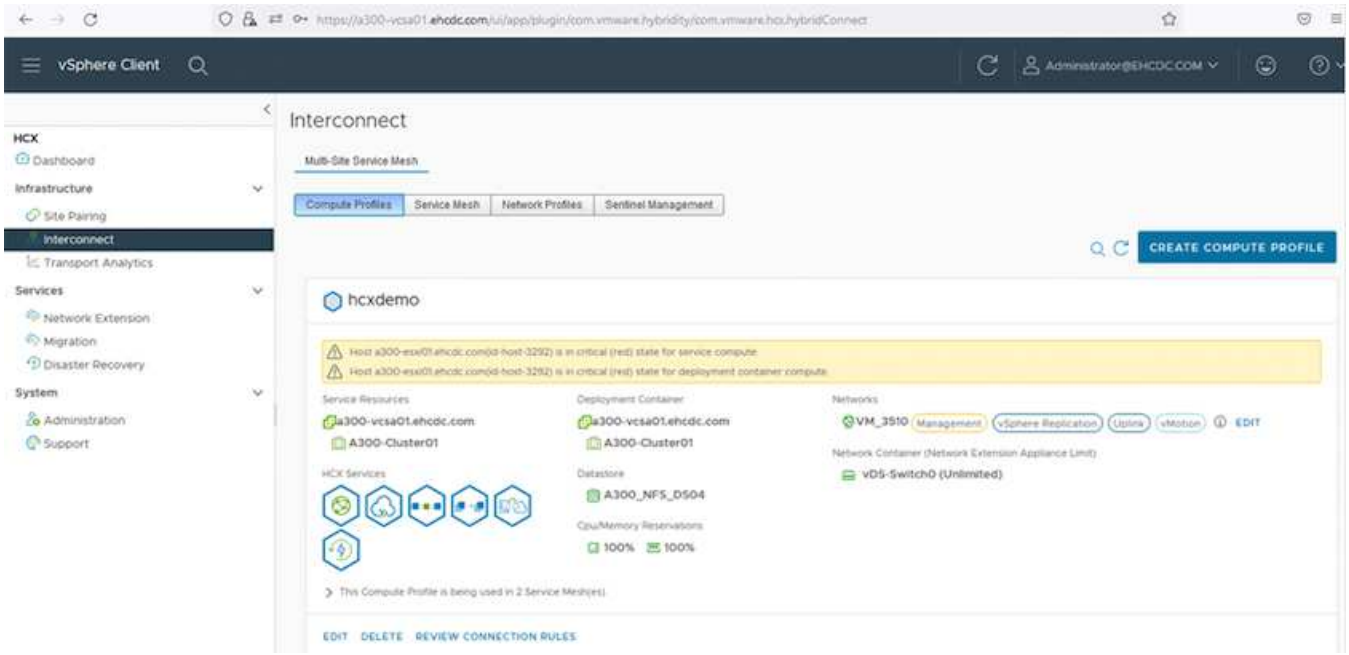
▼ Étape 5 : Configurer le profil réseau, le profil de calcul et le maillage de services

L'appliance de service VMware HCX Interconnect fournit des fonctionnalités de réplication et de migration basées sur vMotion via Internet et des connexions privées vers le site cible. L'interconnexion fournit le

cryptage, l'ingénierie du trafic et la mobilité des machines virtuelles. Pour créer un dispositif de service d'interconnexion, procédez comme suit :

1. Sous Infrastructure, sélectionnez **Interconnexion > Maillage de services multisites > Profils de calcul > Créer un profil de calcul**.

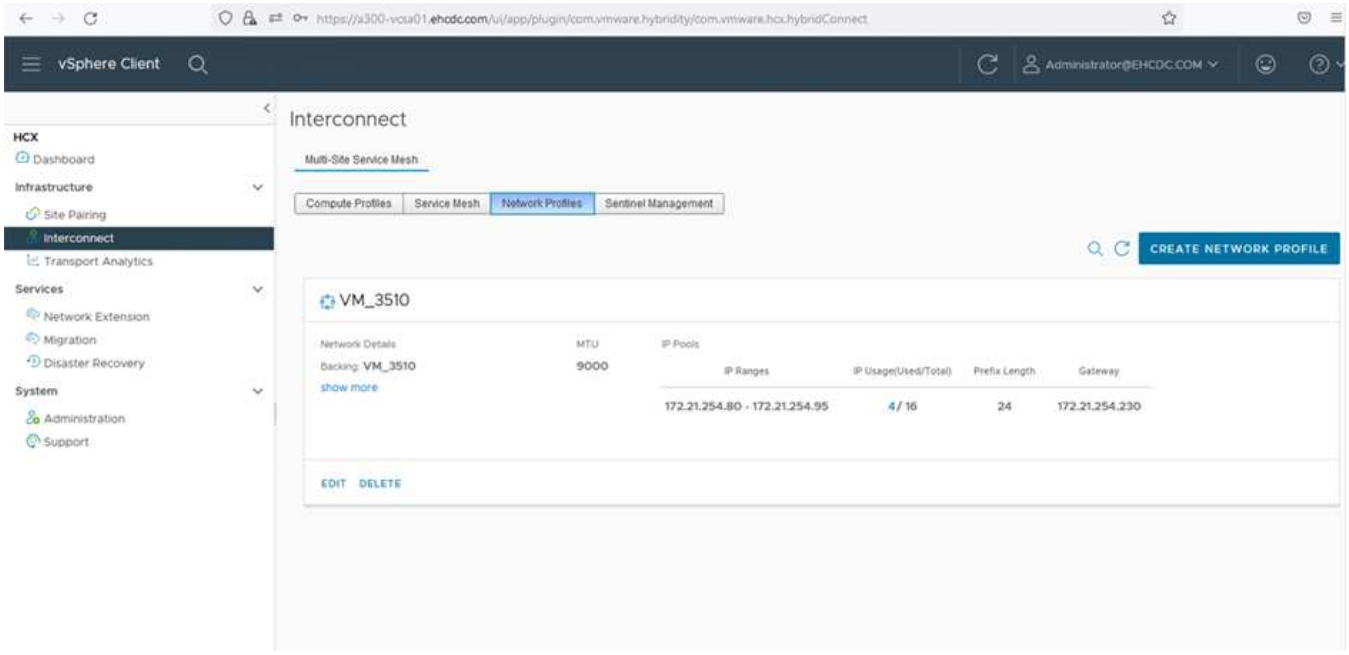
Les profils de calcul définissent les paramètres de déploiement, y compris les appliances déployées et la partie du centre de données VMware accessible au service HCX.



1. Une fois le profil de calcul créé, créez les profils réseau en sélectionnant **Multi-Site Service Mesh > Profils réseau > Créer un profil réseau**.

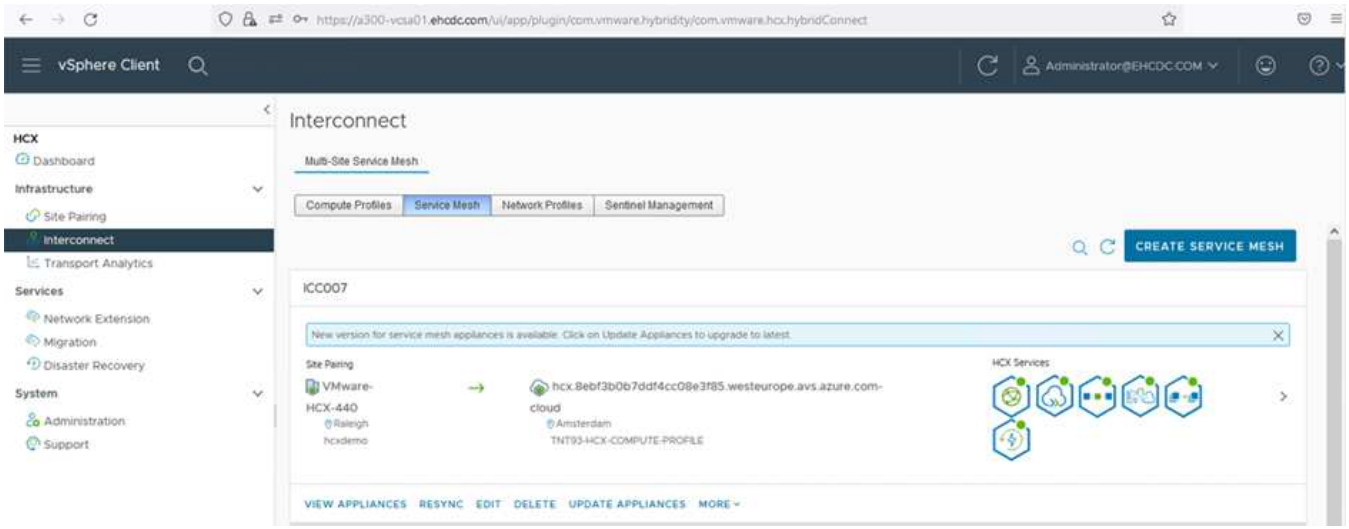
Le profil réseau définit une plage d'adresses IP et de réseaux utilisés par HCX pour ses appliances virtuelles.

Cette étape nécessite deux adresses IP ou plus. Ces adresses IP sont attribuées par le réseau de gestion aux appareils d'interconnexion.

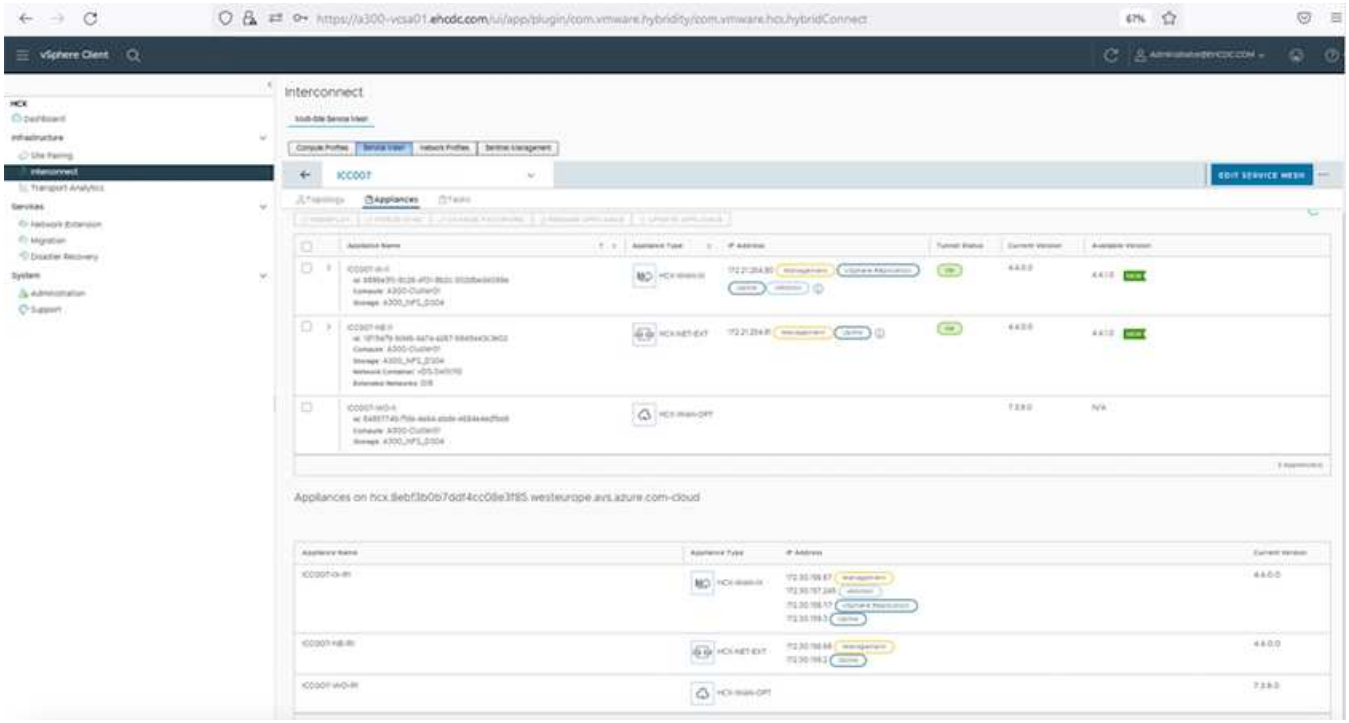


1. À ce stade, les profils de calcul et de réseau ont été créés avec succès.
2. Créez le Service Mesh en sélectionnant l'onglet **Service Mesh** dans l'option **Interconnexion** et sélectionnez les sites SDDC locaux et Azure.
3. Le Service Mesh spécifie une paire de profils de calcul et de réseau locaux et distants.

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. C'est l'étape finale de la configuration. Cela devrait prendre près de 30 minutes pour terminer le déploiement. Une fois le maillage de services configuré, l'environnement est prêt avec les tunnels IPsec créés avec succès pour migrer les machines virtuelles de charge de travail.



▼ **Étape 6 : Migrer les charges de travail**

Les charges de travail peuvent être migrées de manière bidirectionnelle entre les SDDC locaux et Azure à l'aide de diverses 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 masse HCX, HCX vMotion, la migration à froid HCX, HCX Replication Assisted vMotion (disponible avec l'édition HCX Enterprise) et la migration assistée par le système d'exploitation HCX (disponible avec l'édition HCX Enterprise).

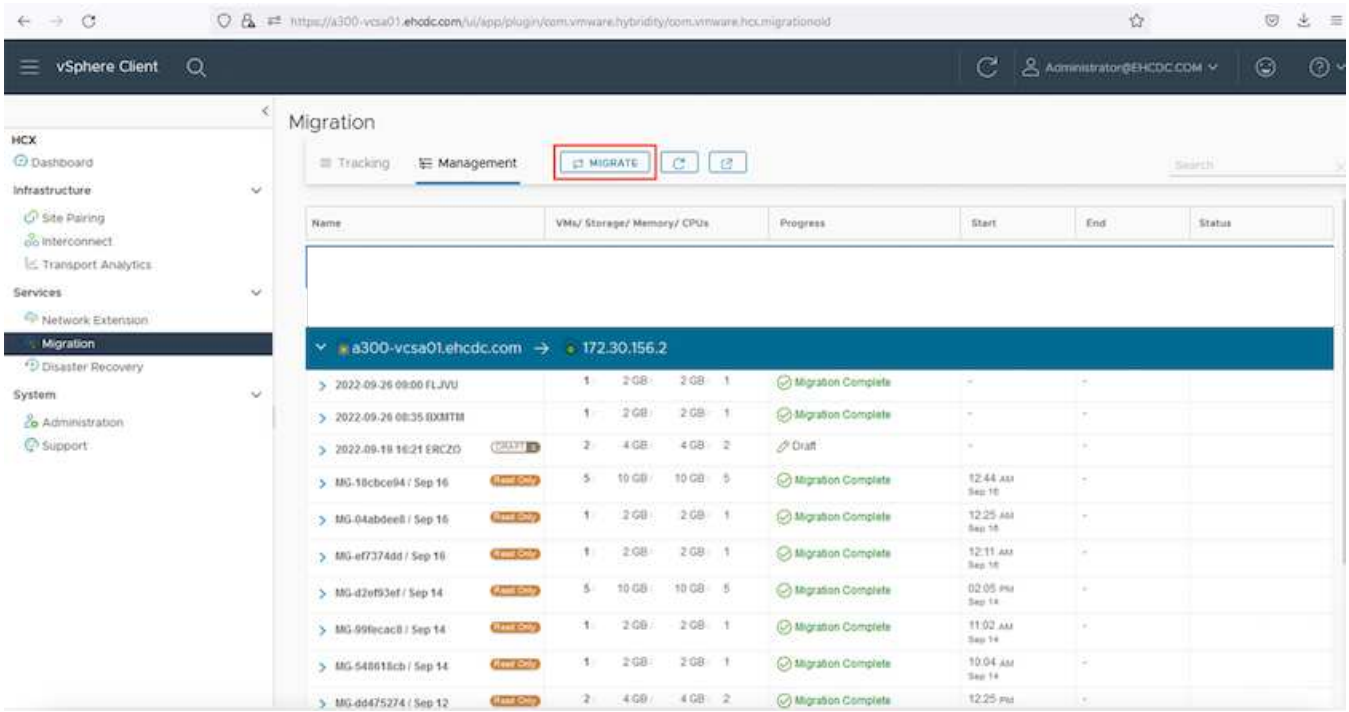
Pour en savoir plus sur les différents mécanismes de migration HCX, consultez "Types de migration VMware HCX" .

Migration en masse

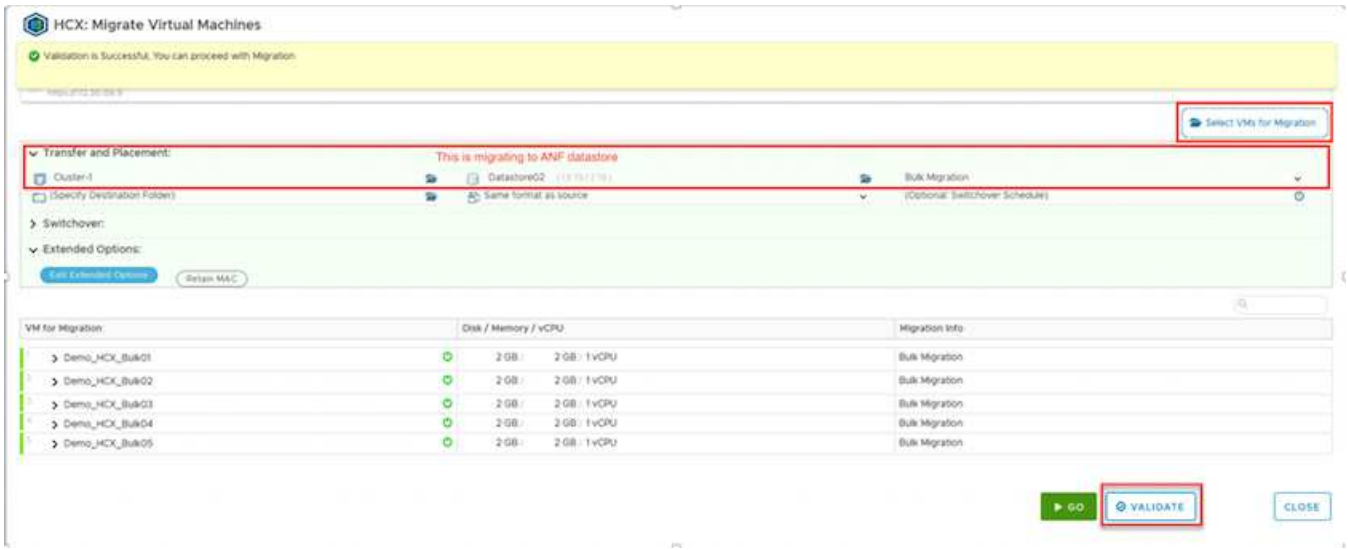
Cette section détaille le mécanisme de migration en masse. Lors d'une migration en masse, la capacité de migration en masse de HCX utilise vSphere Replication pour migrer les fichiers de disque tout en recréant la machine virtuelle sur l'instance vSphere HCX de destination.

Pour lancer des migrations de machines virtuelles en masse, procédez comme suit :

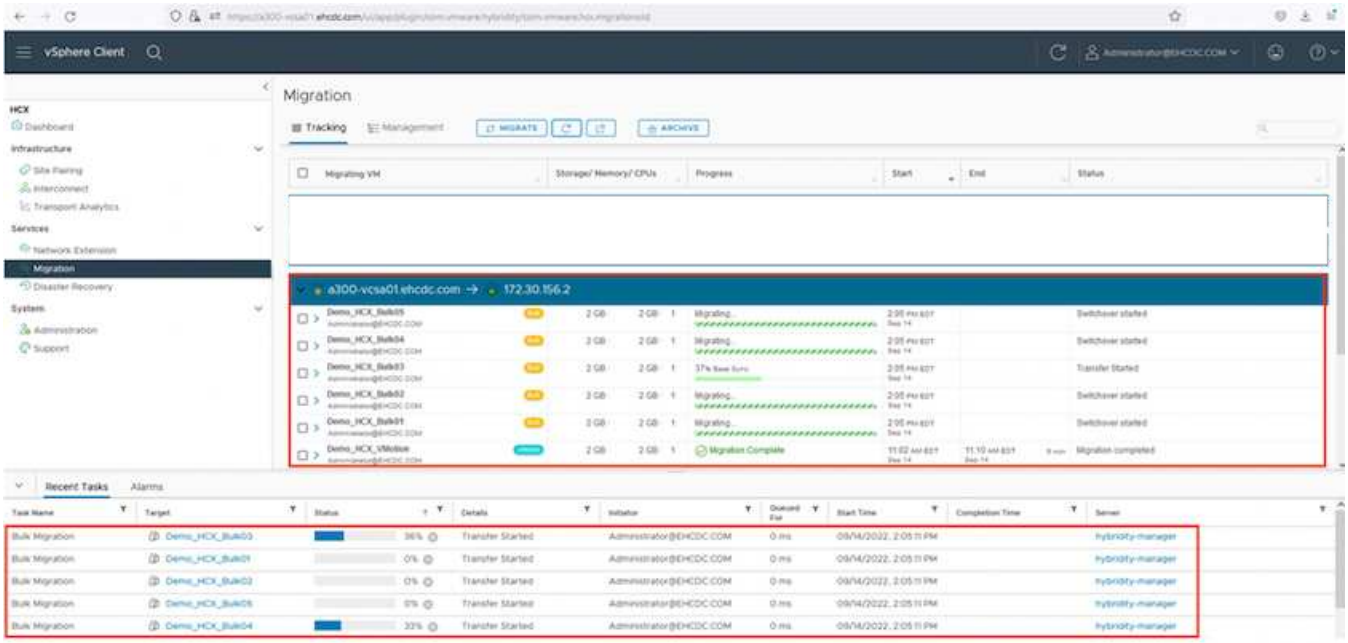
1. Accédez à l'onglet **Migrer** sous **Services > Migration**.



1. Sous **Connexion au site distant**, sélectionnez la connexion au site distant et sélectionnez la source et la destination. Dans cet exemple, la destination est le point de terminaison Azure VMware Solution SDDC HCX.
2. Cliquez sur **Sélectionner les machines virtuelles pour la migration**. Cela fournit une liste de toutes les machines virtuelles sur site. Sélectionnez les machines virtuelles en fonction de l'expression match:value et cliquez sur **Ajouter**.
3. Dans la section **Transfert et placement**, mettez à jour les champs obligatoires (**Cluster**, **Stockage**, **Destination** et **Réseau**), y compris le profil de migration, puis cliquez sur **Valider**.

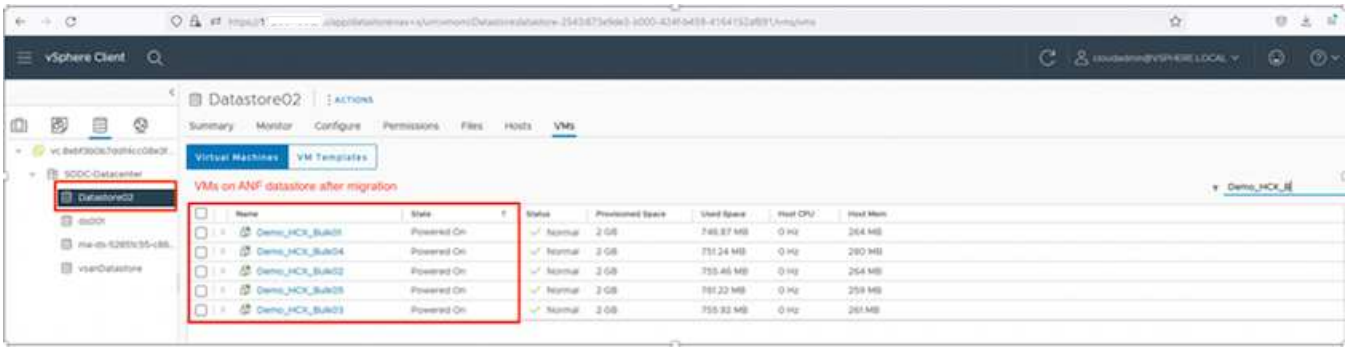


1. Une fois les vérifications de validation terminées, cliquez sur **Go** pour lancer la migration.



Au cours de cette migration, un disque d'espace réservé est créé sur la banque de données Azure NetApp Files spécifiée dans le vCenter cible pour permettre la réplication des données du disque de la machine virtuelle source sur les disques d'espace réservé. HBR est déclenché pour une synchronisation complète avec la cible, et une fois la ligne de base terminée, une synchronisation incrémentielle est effectuée en fonction du cycle d'objectif de point de récupération (RPO). Une fois la synchronisation complète/incrémentielle terminée, le basculement est déclenché automatiquement, sauf si une planification spécifique est définie.

1. Une fois la migration terminée, validez-la en accédant au SDDC vCenter de destination.

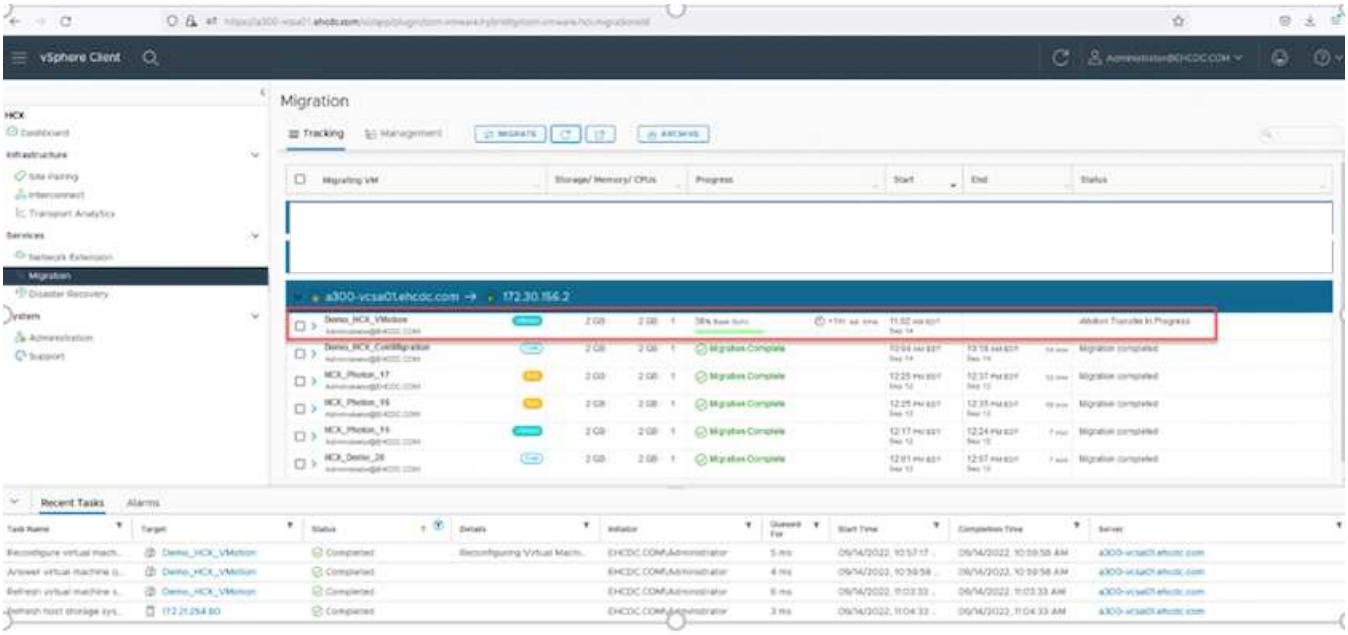


Pour obtenir des informations supplémentaires et détaillées sur les différentes options de migration et sur la manière de migrer les charges de travail des locaux vers Azure VMware Solution à l'aide de HCX, consultez "Considérations relatives à la migration vers VMware HCX" .

Pour en savoir plus sur ce processus, n'hésitez pas à regarder la vidéo suivante :

Migration de la charge de travail 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 qu'une bande passante suffisante est disponible pour gérer la migration.

Le magasin de données ANF cible doit disposer de suffisamment d'espace pour gérer la migration.

Conclusion

Que vous cibliez un cloud entièrement ou un cloud hybride et que vos données résident sur n'importe quel type/fournisseur de stockage sur site, Azure NetApp Files et HCX offrent d'excellentes options pour déployer et migrer les charges de travail des applications tout en réduisant le coût total de possession en rendant les exigences de données transparentes pour la couche applicative. Quel que soit le cas d'utilisation, choisissez Azure VMware Solution avec Azure NetApp Files pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site et sur plusieurs clouds, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise. Il s'agit du même processus et des mêmes procédures familiers utilisés 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).

Plats à emporter

Les points clés de ce document comprennent :

- Vous pouvez désormais utiliser Azure NetApp Files comme banque de données sur Azure VMware Solution SDDC.
- Vous pouvez facilement migrer des données depuis un emplacement local vers une banque de données Azure NetApp Files .
- Vous pouvez facilement développer et réduire la banque de données Azure NetApp Files pour répondre aux exigences de capacité et de performances pendant l'activité de migration.

Où trouver des informations supplémentaires

Pour en savoir plus sur les informations décrites dans ce document, reportez-vous aux liens Web suivants :

- Documentation de 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/"

- Considérations relatives à la migration vers VMware HCX

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

NetApp pour GCP/GCVE

Fonctionnalités NetApp pour Google Cloud Platform GCVE

Découvrez-en plus sur les fonctionnalités que NetApp apporte à Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) - de NetApp en tant que périphérique de stockage connecté invité ou banque de données NFS supplémentaire à la migration des flux de travail, à l'extension/à l'éclatement vers le cloud, à la sauvegarde/restauration et à la reprise après sinistre.

Accédez à la section du contenu souhaité en sélectionnant parmi les options suivantes :

- "Configuration de GCVE dans GCP"
- "Options de stockage NetApp pour GCVE"
- "Solutions cloud NetApp / VMware"

Configuration de GCVE dans GCP

Comme pour les environnements locaux, la planification d'un environnement de virtualisation basé sur le cloud est essentielle pour un environnement prêt pour la production et la création de machines virtuelles et la migration.

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

> Le stockage en invité est la seule méthode prise en charge pour connecter Cloud Volumes ONTAP et Google Cloud NetApp Volumes à GCVE.

Le processus de configuration peut être décomposé selon les étapes suivantes :

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

Voir le détail"étapes de configuration pour GCVE" .

Options de stockage NetApp pour GCVE

Le stockage NetApp peut être utilisé de plusieurs manières, soit en tant que stockage de données connecté, soit en tant que banque de données NFS supplémentaire, dans GCP GCVE.

S'il vous plaît visitez"Options de stockage NetApp prises en charge" pour plus d'informations.

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

- Cloud Volumes ONTAP (CVO) en tant que stockage connecté aux invités
- Google Cloud NetApp Volumes (NetApp Volumes) en tant que stockage connecté invité
- Google Cloud NetApp Volumes (NetApp Volumes) comme banque de données NFS supplémentaire

Voir le détail"options de stockage de connexion invité pour GCVE" . Voir le détail"options de banque de données NFS supplémentaires pour GCVE" .

En savoir plus sur"Prise en charge du magasin de données Google Cloud NetApp Volumes pour Google Cloud VMware Engine (blog NetApp)" ou"Comment utiliser Google Cloud NetApp Volumes comme banques de données pour Google Cloud VMware Engine (blog Google)"

Cas d'utilisation de solutions

Avec les solutions cloud NetApp et VMware, de nombreux cas d'utilisation sont simples à déployer dans Azure AVS. Ces cas sont définis pour chacune des zones cloud définies par VMware :

- Protéger (comprend à la fois la reprise après sinistre et la sauvegarde/restauration)
- Étendre
- Émigrer

"Parcourez les solutions NetApp pour Google Cloud GCVE"

Protéger les charges de travail sur GCP/GCVE

Reprise après sinistre cohérente des applications avec NetApp SnapCenter et Veeam Replication

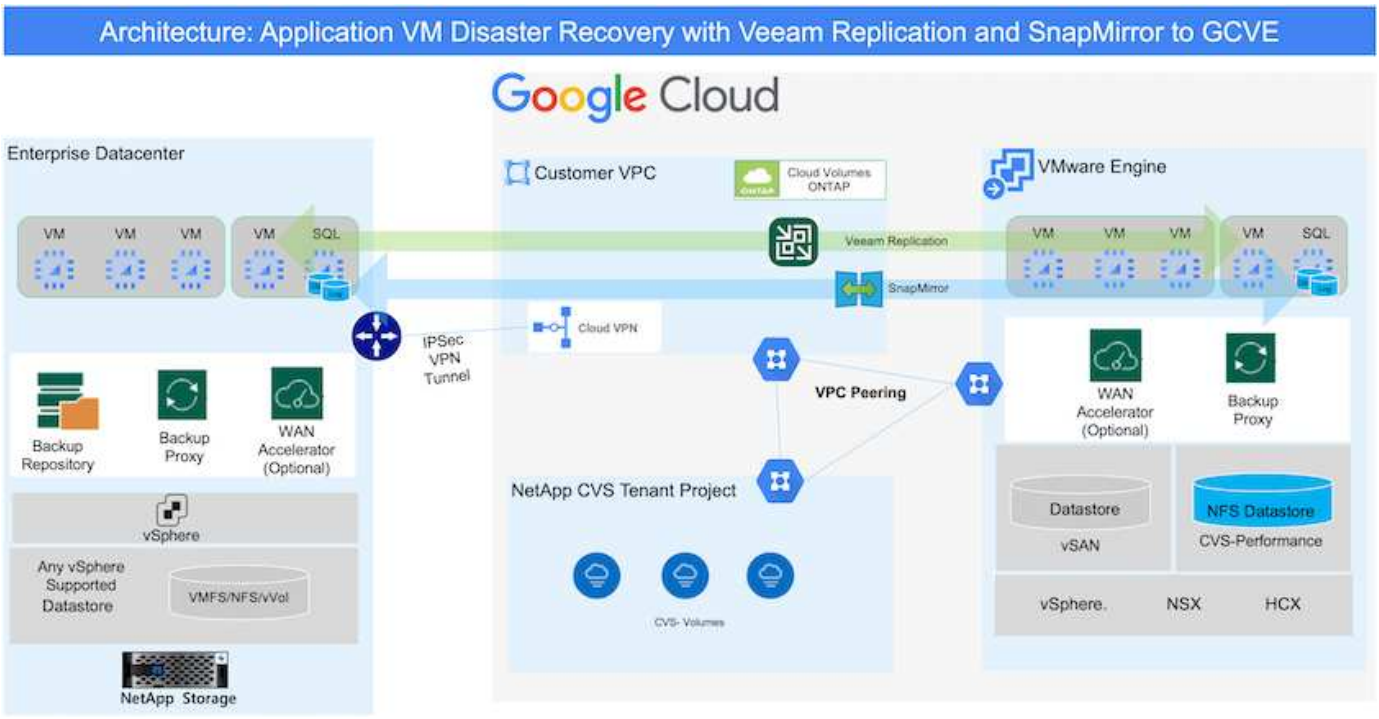
La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données tels que les ransomwares. Avec NetApp SnapMirror, les charges de travail VMware sur site qui utilisent un stockage connecté en tant qu'invité peuvent être répliquées vers NetApp Cloud Volumes ONTAP exécuté dans Google Cloud.

Aperçu

De nombreux clients recherchent une solution de reprise après sinistre efficace pour leurs machines virtuelles d'application hébergées sur VMware vSphere. Beaucoup d'entre eux utilisent leur solution de sauvegarde existante pour effectuer une récupération en cas de catastrophe. Souvent, cette solution augmente le RTO et ne répond pas à leurs attentes. Pour réduire le RPO et le RTO, la réplication de VM Veeam peut être utilisée même sur site vers GCVE tant que la connectivité réseau et l'environnement avec les autorisations appropriées sont disponibles. REMARQUE : Veeam VM Replication ne protège pas les périphériques de stockage connectés aux invités de la machine virtuelle, tels que les montages iSCSI ou NFS à l'intérieur de la machine virtuelle invitée. Il faut les protéger séparément.

Pour une réplication cohérente des applications pour SQL VM et pour réduire le RTO, nous avons utilisé SnapCenter pour orchestrer les opérations snapmirror des volumes de base de données et de journaux SQL.

Ce document fournit une approche étape par étape pour la configuration et l'exécution de la reprise après sinistre qui utilise NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document se concentre sur le stockage en invité pour les données d'application (également appelé invité connecté), et nous supposons que l'environnement sur site utilise SnapCenter pour les sauvegardes cohérentes avec les applications.

> ⓘ Ce document s'applique à toute solution de sauvegarde ou de récupération tierce. En fonction de la solution utilisée dans l'environnement, suivez les meilleures pratiques pour créer des politiques de sauvegarde qui respectent les SLA organisationnels.

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que l'interconnexion dédiée ou le VPN Cloud. Les segments doivent être créés en fonction de la conception du VLAN sur site.

> ⓘ Il existe plusieurs options pour connecter les centres de données sur site à Google Cloud, ce qui nous empêche de décrire un flux de travail spécifique dans ce document. Consultez la documentation de Google Cloud pour connaître la méthode de connectivité locale à Google appropriée.

Déploiement de la solution DR

Présentation du déploiement de la solution

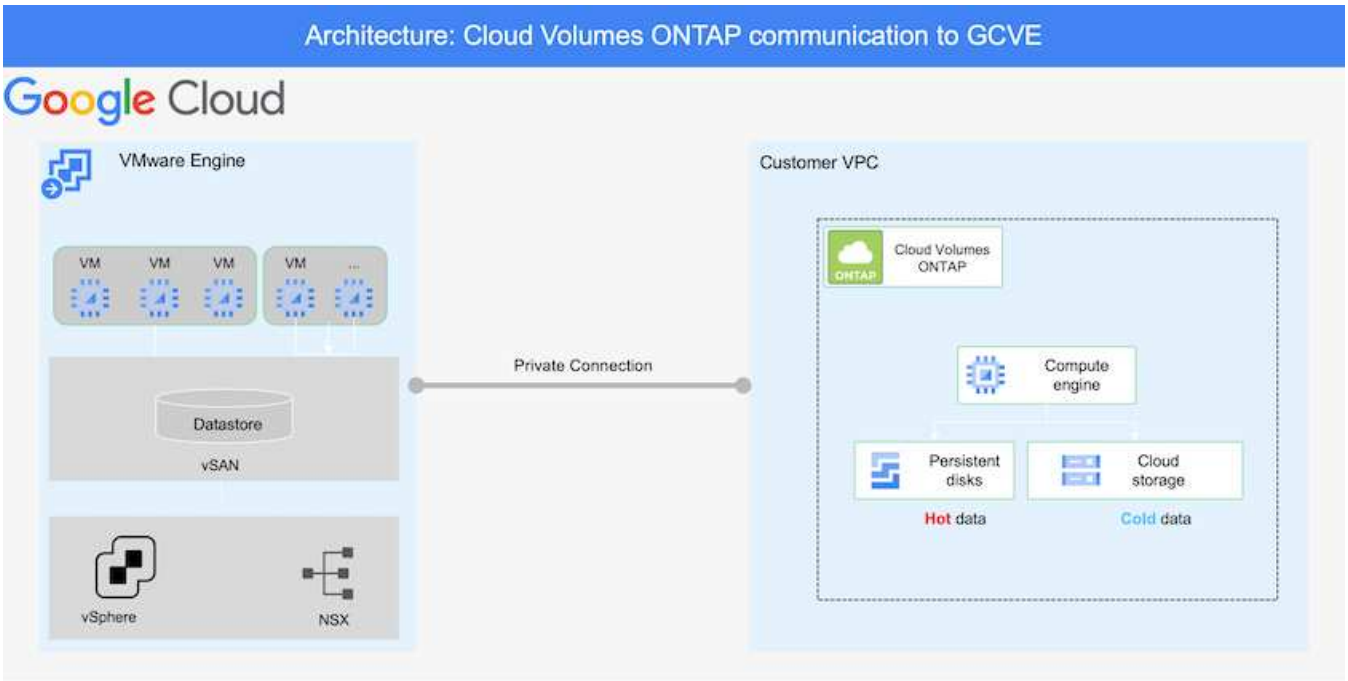
1. Assurez-vous que les données d'application sont sauvegardées à l'aide de SnapCenter avec les exigences RPO nécessaires.

2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de NetApp Console dans l'abonnement et le réseau virtuel appropriés.
   a. Configurez SnapMirror pour les volumes d'application concernés.
   b. Mettez à jour les stratégies de sauvegarde dans SnapCenter pour déclencher les mises à jour de SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer les machines virtuelles sur l'instance Google Cloud VMware Engine.
4. En cas de sinistre, interrompez la relation SnapMirror à l'aide de NetApp Console et déclenchez le basculement des machines virtuelles avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'application.
   b. Déposez vos candidatures en ligne.
5. Appelez la restauration automatique du site protégé en resynchronisant SnapMirror en sens inverse une fois le site principal récupéré.

Détails du déploiement

▼ **Configurer CVO sur Google Cloud et répliquer les volumes vers CVO**

La première étape consiste à configurer Cloud Volumes ONTAP sur Google Cloud ("cvo") et répliquez les volumes souhaités vers Cloud Volumes ONTAP avec les fréquences et les rétentions de snapshots souhaitées.



Pour obtenir des exemples d'instructions étape par étape sur la configuration de SnapCenter et la réplication des données, reportez-vous à"Configurer la réplication avec SnapCenter"

Examen de la protection des machines virtuelles SQL avec SnapCenter

▼ **Configurer les hôtes GCVE et l'accès aux données CVO**

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution GCVE et la durée pendant laquelle le SDDC doit être maintenu en service. Ces deux considérations clés pour une solution de reprise après sinistre contribuent à réduire les coûts opérationnels

globaux. Le SDDC peut être aussi petit que trois hôtes, jusqu'à un cluster multi-hôtes dans un déploiement à grande échelle.

Les Google Cloud NetApp Volumes pour les bases de données NFS Datastore et Cloud Volumes ONTAP pour SQL et les journaux peuvent être déployés sur n'importe quel VPC et GCVE doit disposer d'une connexion privée à ce VPC pour monter le datastore NFS et permettre à la machine virtuelle de se connecter aux LUN iSCSI.

Pour configurer GCVE SDDC, voir"Déployer et configurer l'environnement de virtualisation sur Google Cloud Platform (GCP)" . Comme condition préalable, vérifiez que les machines virtuelles invitées résidant sur les hôtes GCVE sont en mesure de consommer les données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois Cloud Volumes ONTAP et GCVE correctement configurés, commencez à configurer Veeam pour automatiser la récupération des charges de travail sur site vers GCVE (machines virtuelles avec VMDK d'application et machines virtuelles avec stockage en invité) en utilisant la fonctionnalité de réplication Veeam et en exploitant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

▼ **Installer les composants Veeam**

En fonction du scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde doivent être déployés. Pour ce cas d'utilisation, il n'est pas nécessaire de déployer un magasin d'objets pour Veeam et le référentiel Scale-out n'est pas non plus requis. "Reportez-vous à la documentation Veeam pour la procédure d'installation" Pour plus d'informations, veuillez consulter"Migration avec Veeam Replication"

▼ **Configurer la réplication de VM avec Veeam**

Le vCenter sur site et le vCenter GCVE doivent tous deux être enregistrés auprès de Veeam. "Configurer la tâche de réplication de machine virtuelle vSphere" À l'étape Traitement des invités de l'assistant, sélectionnez Désactiver le traitement des applications, car nous utiliserons SnapCenter pour la sauvegarde et la récupération prenant en charge les applications.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **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.
- Récupère à n'importe quel point disponible dans le temps avec la conservation des instantanés ONTAP .
- L'automatisation complète est disponible pour toutes les étapes requises pour récupérer des centaines à des milliers de machines virtuelles, depuis les étapes de stockage, de calcul, de réseau et de validation des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela évite le risque de corruption des données pour les volumes et les instantanés.
  - Évite les interruptions de réplication pendant les flux de travail de test DR.
  - Exploite les données DR pour les flux de travail au-delà de DR, tels que le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau et les tests de correction.
- Veeam Replication permet de modifier les adresses IP des machines virtuelles sur le site de reprise après

sinistre.

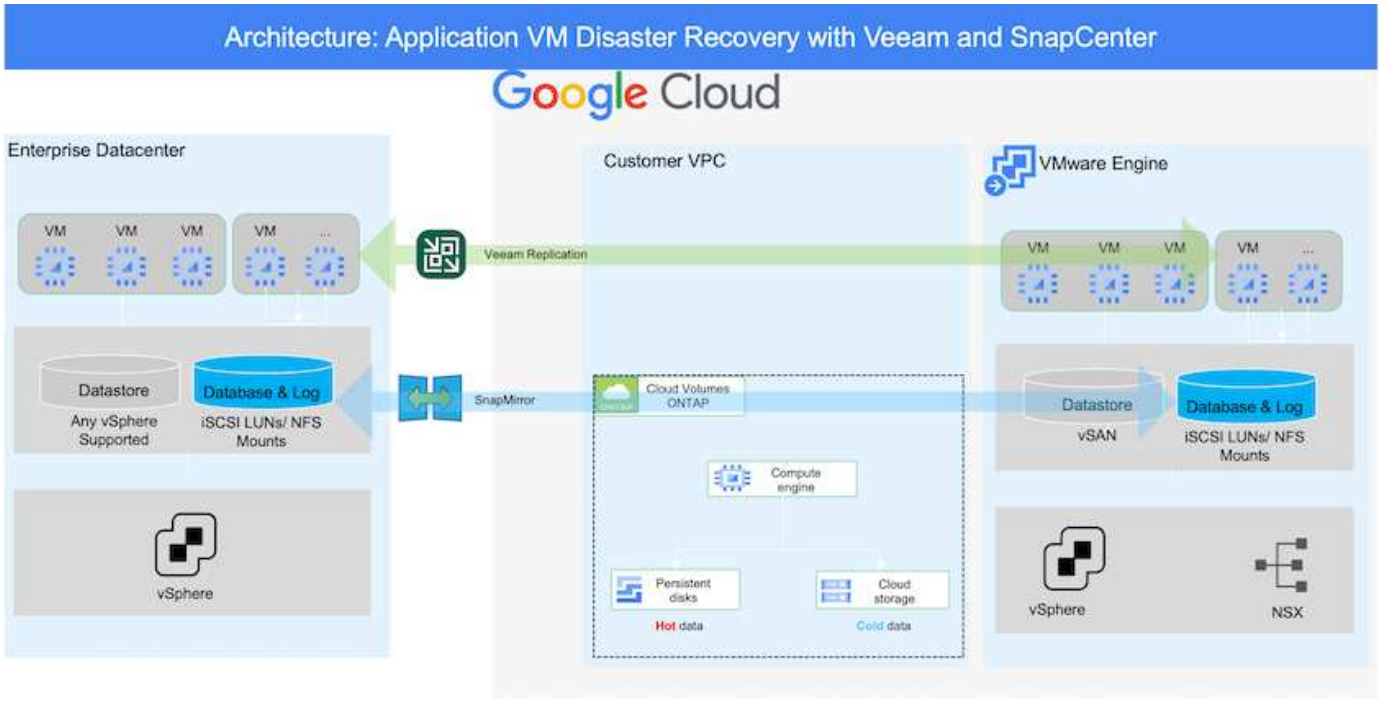
Reprise après sinistre des applications avec SnapCenter, Cloud Volumes ONTAP et Veeam Replication

La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données tels que les ransomwares. Avec NetApp SnapMirror, les charges de travail VMware sur site qui utilisent un stockage connecté en tant qu'invité peuvent être répliquées vers NetApp Cloud Volumes ONTAP exécuté dans Google Cloud.

Aperçu

Cela couvre les données d'application ; cependant, qu'en est-il des machines virtuelles elles-mêmes ? La reprise après sinistre doit couvrir tous les composants dépendants, y compris les machines virtuelles, les VMDK, les données d'application, etc. Pour ce faire, SnapMirror et Veeam peuvent être utilisés pour récupérer de manière transparente les charges de travail répliquées sur site vers Cloud Volumes ONTAP tout en utilisant le stockage vSAN pour les VMDK.

Ce document fournit une approche étape par étape pour la configuration et l'exécution de la reprise après sinistre qui utilise NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document se concentre sur le stockage en invité pour les données d'application (également appelé invité connecté), et nous supposons que l'environnement sur site utilise SnapCenter pour les sauvegardes cohérentes avec les applications.

> Ce document s'applique à toute solution de sauvegarde ou de récupération tierce. En fonction de la solution utilisée dans l'environnement, suivez les meilleures pratiques pour créer des politiques de sauvegarde qui respectent les SLA organisationnels.

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de

connectivité telles que l'interconnexion dédiée ou le VPN Cloud. Les segments doivent être créés en fonction de la conception du VLAN sur site.

> Il existe plusieurs options pour connecter les centres de données sur site à Google Cloud, ce qui nous empêche de décrire un flux de travail spécifique dans ce document. Consultez la documentation de Google Cloud pour connaître la méthode de connectivité locale à Google appropriée.

Déploiement de la solution DR

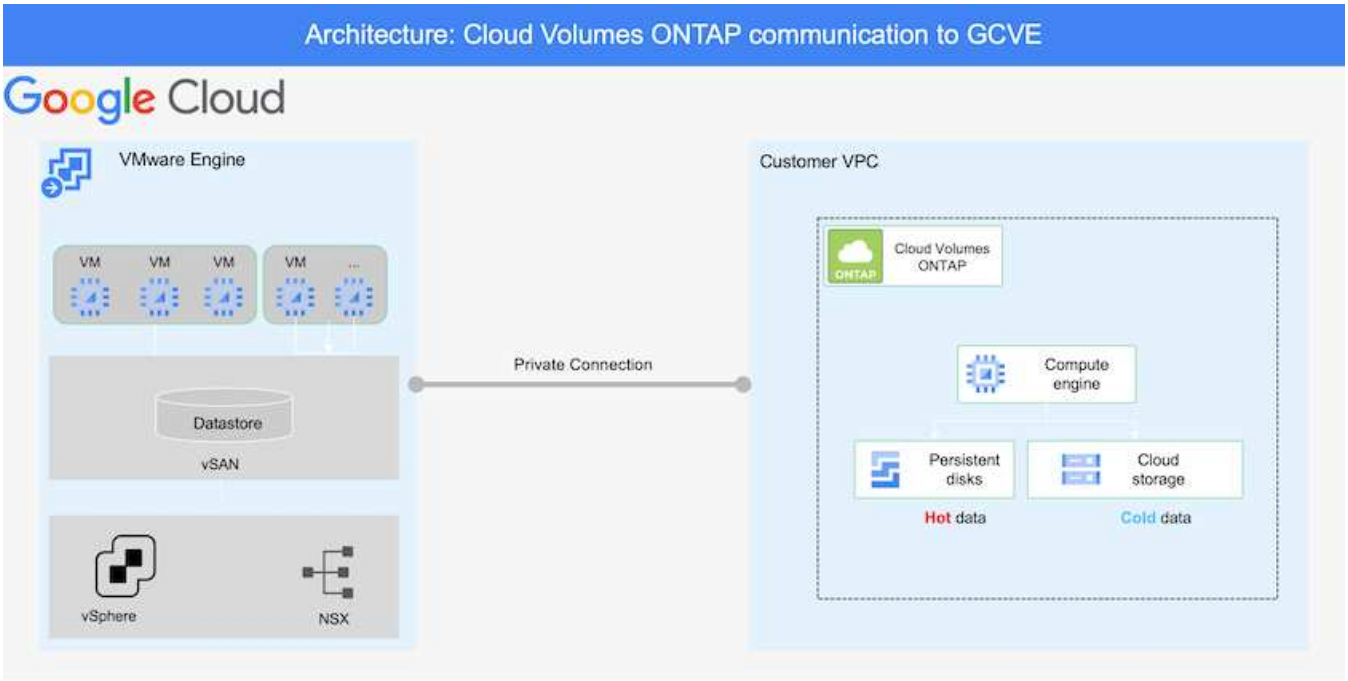
Présentation du déploiement de la solution

1. Assurez-vous que les données d'application sont sauvegardées à l'aide de SnapCenter avec les exigences RPO nécessaires.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance correcte à l'aide du gestionnaire Cloud dans l'abonnement et le réseau virtuel appropriés.
   a. Configurez SnapMirror pour les volumes d'application concernés.
   b. Mettez à jour les stratégies de sauvegarde dans SnapCenter pour déclencher les mises à jour de SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer les machines virtuelles sur l'instance Google Cloud VMware Engine.
4. Lors d'un événement catastrophique, interrompez la relation SnapMirror à l'aide de Cloud Manager et déclenchez le basculement des machines virtuelles avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'application.
   b. Déposez vos candidatures en ligne.
5. Appelez la restauration automatique du site protégé en resynchronisant SnapMirror en sens inverse une fois le site principal récupéré.

Détails du déploiement

▼ Configurer CVO sur Google Cloud et répliquer les volumes vers CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Google Cloud ("cvo") et répliquez les volumes souhaités vers Cloud Volumes ONTAP avec les fréquences et les rétentions de snapshots souhaitées.



Pour obtenir des exemples d'instructions étape par étape sur la configuration de SnapCenter et la réplication des données, reportez-vous à"Configurer la réplication avec SnapCenter"

Configurer la réplication avec SnapCenter

▼ **Configurer les hôtes GCVE et l'accès aux données CVO**

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution GCVE et la durée pendant laquelle le SDDC doit être maintenu en service. Ces deux considérations clés pour une solution de reprise après sinistre contribuent à réduire les coûts opérationnels globaux. Le SDDC peut être aussi petit que trois hôtes, jusqu'à 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 machine virtuelle se connecte aux LUN iSCSI.

Pour configurer GCVE SDDC, voir"Déployer et configurer l'environnement de virtualisation sur Google Cloud Platform (GCP)" . Comme condition préalable, vérifiez que les machines virtuelles invitées résidant sur les hôtes GCVE sont en mesure de consommer les données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois Cloud Volumes ONTAP et GCVE correctement configurés, commencez à configurer Veeam pour automatiser la récupération des charges de travail sur site vers GCVE (machines virtuelles avec VMDK d'application et machines virtuelles avec stockage en invité) en utilisant la fonctionnalité de réplication Veeam et en exploitant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

▼ **Installer les composants Veeam**

En fonction du scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde doivent être déployés. Pour ce cas d'utilisation, il n'est pas nécessaire de déployer un magasin d'objets pour Veeam et le référentiel Scale-out n'est pas non plus requis.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Reportez-vous à la documentation Veeam pour la procédure d'installation"]

▼ **Configurer la réplication de VM avec Veeam**

Le vCenter sur site et le vCenter GCVE doivent tous deux être enregistrés auprès de Veeam. "Configurer la tâche de réplication de machine virtuelle vSphere" À l'étape Traitement des invités de l'assistant, sélectionnez Désactiver le traitement des applications, car nous utiliserons SnapCenter pour la sauvegarde et la récupération prenant en charge les applications.

Configurer la tâche de réplication de machine virtuelle vSphere

▼ **Basculement de la machine virtuelle Microsoft SQL Server**

Basculement de la machine virtuelle Microsoft SQL Server

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Récupère à n'importe quel point disponible dans le temps avec la conservation des instantanés ONTAP .
- L'automatisation complète est disponible pour toutes les étapes requises pour récupérer des centaines à des milliers de machines virtuelles, depuis les étapes de stockage, de calcul, de réseau et de validation des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela évite le risque de corruption des données pour les volumes et les instantanés.
  - Évite les interruptions de réplication pendant les flux de travail de test DR.
  - Exploite les données DR pour les flux de travail au-delà de DR, tels que le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau et les tests de correction.
- Veeam Replication permet de modifier les adresses IP des machines virtuelles sur le site de reprise après sinistre.

Utilisation de Veeam Replication et du datastore Google Cloud NetApp Volumes pour la reprise après sinistre sur Google Cloud VMware Engine

Un plan complet de reprise après sinistre est essentiel pour les entreprises en temps de crise. De nombreuses organisations utilisent le cloud computing pour leurs opérations quotidiennes et leur reprise après sinistre. Cette approche proactive peut réduire ou éliminer les perturbations commerciales coûteuses.

Cet article décrit comment utiliser Veeam Backup & Replication pour configurer la reprise après sinistre des machines virtuelles VMware sur site vers Google Cloud VMware Engine (GCVE) avec Google Cloud NetApp Volumes (NetApp Volumes).

Aperçu

Google Cloud NetApp Volumes est un service de stockage de Google et NetApp disponible pour Google Cloud. Le service NetApp Volumes fournit un stockage NFS/SMB hautes performances. Le stockage NFS NetApp Volumes certifié VMware peut être utilisé comme banque de données externe pour les hôtes ESXi dans GCVE. Les utilisateurs doivent établir une connexion peering entre leur cloud privé GCVE et leur projet NetApp Volumes. Il n'y a pas de frais de réseau résultant de l'accès au stockage dans une région. Les utilisateurs peuvent créer des volumes NetApp Volumes dans la console Google Cloud et activer la protection contre la suppression avant de monter des volumes en tant que banques de données sur leurs hôtes ESXi.

Les magasins de données NFS basés sur NetApp Volumes peuvent être utilisés pour répliquer des données à partir de sites locaux à l'aide de n'importe quelle solution tierce validée offrant une capacité de réplication de machines virtuelles. En ajoutant des magasins de données NetApp Volumes, il permet un déploiement

optimisé en termes de coûts au lieu de créer un SDDC basé sur Google Cloud VMware Engine (GCVE) avec un grand nombre d'hôtes ESXi pour accueillir le stockage. Cette approche est appelée « Pilot Light Cluster ». Un cluster de voyants lumineux est une configuration d'hôte GCVE minimale (3 hôtes GCVE ESXi) avec une capacité de stockage de données NetApp Volumes pour permettre une mise à l'échelle indépendante afin de répondre aux exigences de capacité.

L'objectif est de maintenir une infrastructure rentable avec uniquement les composants de base pour gérer un basculement. Un cluster de voyants lumineux peut s'étendre et ajouter davantage d'hôtes GCVE en cas de basculement. Une fois le basculement résolu et les opérations normales reprises, le groupe de voyants lumineux peut réduire son échelle, revenant à un mode opérationnel à faible coût.

Objectifs du présent document

Cet article décrit comment utiliser une banque de données Google Cloud NetApp Volumes avec Veeam Backup & Replication pour configurer la reprise après sinistre des machines virtuelles VMware sur site vers GCVE à l'aide de la fonctionnalité du logiciel de réplication de machines virtuelles Veeam.

Veeam Backup & Replication est une application de sauvegarde et de réplication pour les environnements virtuels. Lorsque des machines virtuelles sont répliquées, Veeam Backup & Replication crée une copie exacte des machines virtuelles au format VMware vSphere natif sur le cluster SDDC GCVE cible. Veeam Backup & Replication gardera la copie synchronisée avec la VM d'origine. La réplication fournit le meilleur objectif de temps de récupération (RTO) car il existe une copie montée d'une machine virtuelle sur le site DR dans un état prêt à démarrer.

Ce mécanisme de réplication garantit que les charges de travail peuvent démarrer rapidement dans GCVE en cas de catastrophe. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. De plus, il filtre également les blocs de données en double, les blocs de données nuls, les fichiers d'échange et les « fichiers du système d'exploitation invité de la machine virtuelle exclus ». Le logiciel compressera également le trafic de réplique. Pour éviter que les tâches de réplication ne consomment toute la bande passante du réseau, des accélérateurs WAN et des règles de limitation du réseau peuvent être utilisés.

Le processus de réplication dans Veeam Backup & Replication est piloté par tâches, ce qui signifie que la réplication est effectuée en configurant des tâches de réplication. En cas de sinistre, le basculement peut être déclenché pour récupérer les machines virtuelles en basculant vers leur copie de réplication. Lorsqu'un basculement est effectué, une machine virtuelle répliquée reprend le rôle de la machine virtuelle d'origine. Le basculement peut être effectué vers le dernier état d'une réplique ou vers l'un de ses points de restauration connus comme étant corrects. Cela permet la récupération des ransomwares ou des tests isolés selon les besoins. Veeam Backup & Replication offre plusieurs options pour gérer différents scénarios de reprise après sinistre.

Présentation de la solution

Cette solution couvre les étapes de haut niveau suivantes :

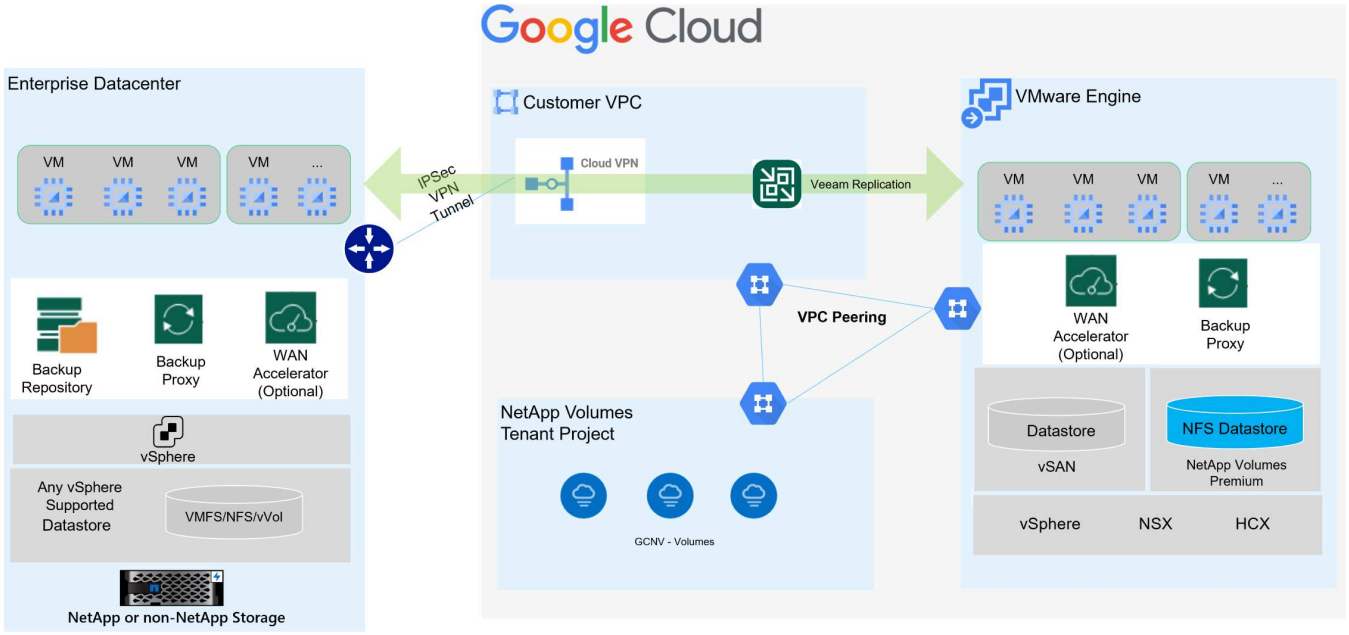
1. Créer un volume NFS à l'aide de Google Cloud NetApp Volumes
2. Suivez le processus GCP pour créer une banque de données GCVE à partir du volume NFS NetApp Volumes.
3. Configurez une tâche de réplication pour créer des répliques de machines virtuelles à l'aide de Veeam Backup & Replication.
4. Créez un plan de basculement et effectuez le basculement.
5. Revenez aux machines virtuelles de production une fois l'événement de catastrophe terminé et le site principal opérationnel.

Lors de la création d'un volume dans NetApp Volumes, pour une utilisation en tant que banque de données GCVE, seul NFS v3 est pris en charge.

Pour plus d'informations sur l'utilisation des volumes NFS NetApp Volumes comme banques de données pour GCVE, consultez "Utilisation du volume NFS comme banque de données vSphere hébergée par Google Cloud NetApp Volumes" .

Architecture

Le schéma suivant montre l'architecture de la solution présentée dans cette documentation. Une bonne pratique recommandée consiste à disposer d'un serveur Veeam Backup & Replication situé à la fois sur le site local et dans le SDDC GCVE. La sauvegarde et la restauration sont effectuées et gérées par le serveur Veeam sur site, et la réplication est gérée par le serveur Veeam dans le SDDC GCVE. Cette architecture offre la plus haute disponibilité en cas de panne dans le centre de données principal.



Prérequis pour la réplication Veeam vers les datastores GCVE et NetApp Volumes

Cette solution nécessite les composants et configurations suivants :

1. NetApp Volumes dispose d'un pool de stockage disponible avec une capacité libre suffisante pour accueillir le volume NFS à créer.
2. Le logiciel Veeam Backup and Replication s'exécute dans un environnement sur site avec une connectivité réseau appropriée.
3. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée aux clusters SDDC GCVE source et cible.
4. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée aux machines virtuelles du serveur proxy Veeam sur les clusters GCVE source et cible.
5. Le serveur de sauvegarde doit être capable de résoudre les noms courts et de se connecter aux vCenters source et cible.

Les utilisateurs doivent établir une connexion de peering entre leur cloud privé GCVE et leur projet NetApp Volumes à l'aide des pages de peering de réseau VPC ou de connexions privées dans l'interface utilisateur de

la console VMware Engine Cloud.

> Veeam requiert un compte utilisateur de solution GCVE disposant de privilèges élevés pour ajouter le serveur GCVE vCenter à l'inventaire Veeam Backup and Replication. Pour plus d'informations, consultez la documentation Google Cloud Platform (GCP), "Élévation des privilèges de VMware Engine".

Pour plus d'informations, reportez-vous à "Considérations et limites" dans la documentation Veeam Backup & Replication.

Étapes de déploiement

Les sections suivantes décrivent les étapes de déploiement pour créer et monter une banque de données NFS à l'aide de Google Cloud NetApp Volumes et utiliser Veeam Backup and Replication pour implémenter une solution de reprise après sinistre complète entre un centre de données sur site et Google Cloud VMware Engine.

Créer un volume NFS et une banque de données NetApp Volumes pour GCVE

Se référer à "Utilisation du volume NFS comme banque de données vSphere hébergée par Google Cloud NetApp Volumes" pour un aperçu de la façon d'utiliser Google Cloud NetApp Volumes comme banque de données pour GCVE.

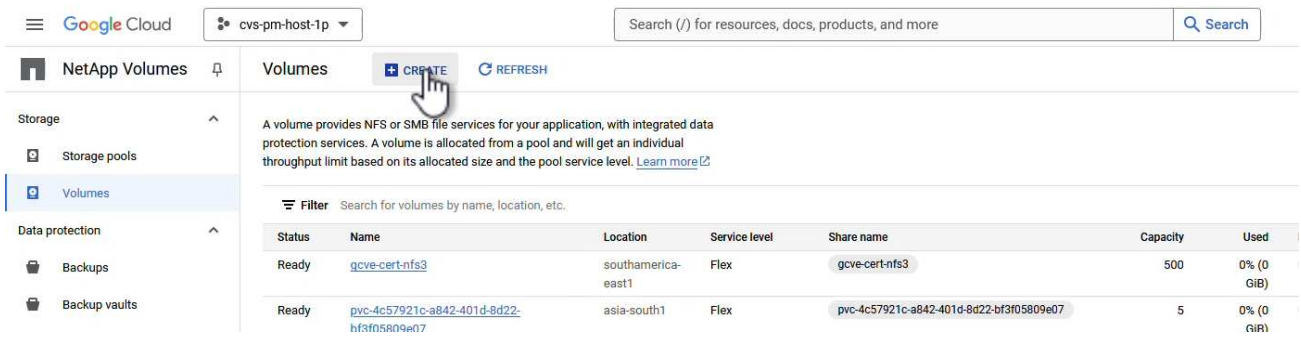
Suivez les étapes suivantes pour créer et utiliser une banque de données NFS pour GCVE à l'aide de NetApp Volumes :

▼ **Créer un volume NFS NetApp Volumes**

Google Cloud NetApp Volumes est accessible depuis la console Google Cloud Platform (GCP).

Se référer à "Créer un volume" dans la documentation Google Cloud NetApp Volumes pour obtenir des informations détaillées sur cette étape.

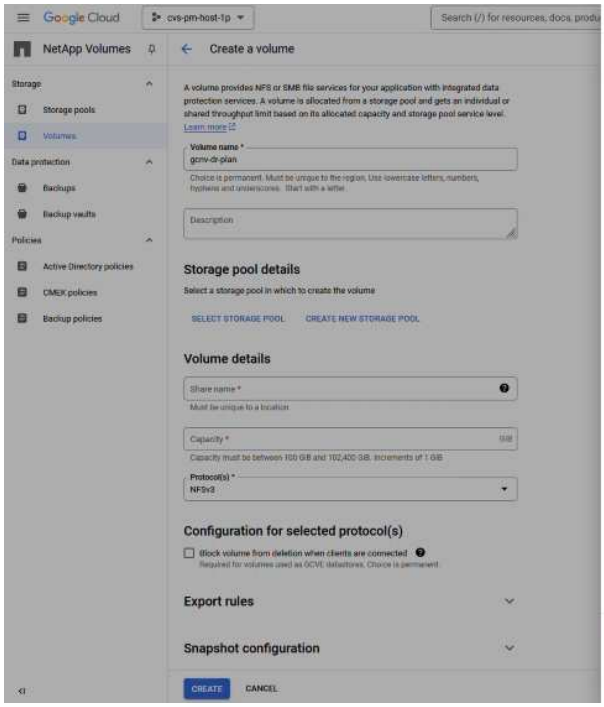
1. Dans un navigateur Web, accédez à https://console.cloud.google.com/ et connectez-vous à votre console GCP. Recherchez * NetApp Volumes* pour commencer.
2. Dans l'interface de gestion * NetApp Volumes*, cliquez sur **Créer** pour commencer à créer un volume NFS.

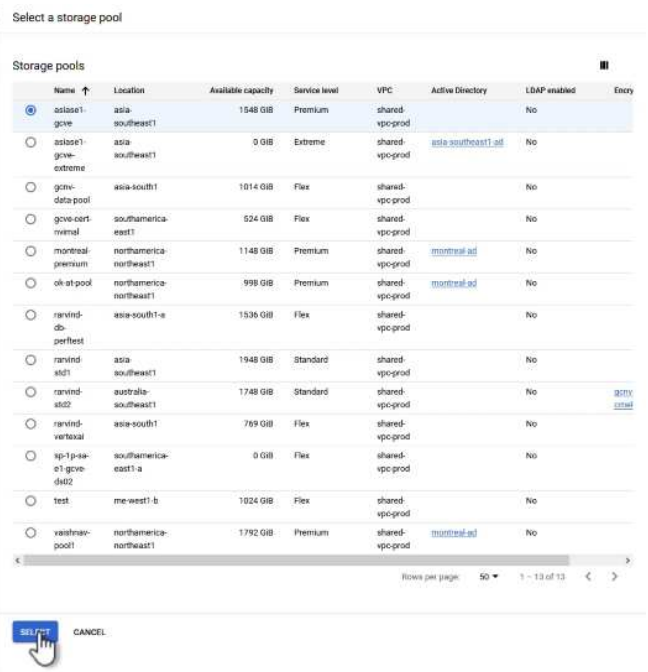


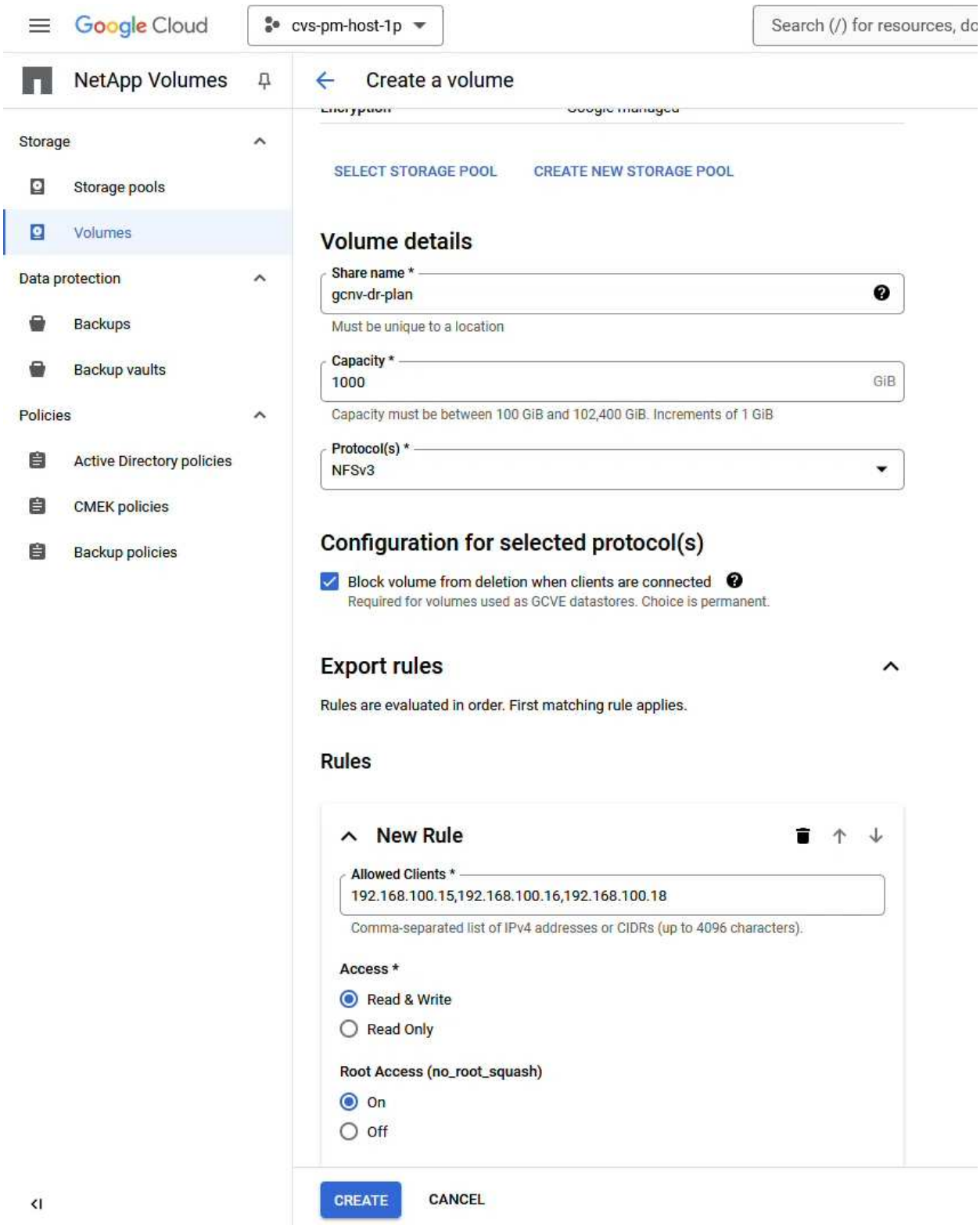
3. Dans l'assistant **Créer un volume**, remplissez toutes les informations requises :
   - Un nom pour le volume.
   - Le pool de stockage sur lequel créer le volume.

- Un nom de partage utilisé lors du montage du volume NFS.
- La capacité du volume en Gio.
- Le protocole de stockage à utiliser.
- Cochez la case pour **Bloquer la suppression du volume lorsque les clients sont connectés** (requis par GCVE lors du montage en tant que banque de données).
- Les règles d'exportation pour accéder au volume. Il s'agit des adresses IP des adaptateurs ESXi sur le réseau NFS.
- Une planification d'instantanés utilisée pour protéger le volume à l'aide d'instantanés locaux.
- Vous pouvez également choisir de sauvegarder le volume et/ou de créer des étiquettes pour le volume.

Lors de la création d'un volume dans NetApp Volumes, pour une utilisation en tant que banque de données GCVE, seul NFS v3 est pris en charge.

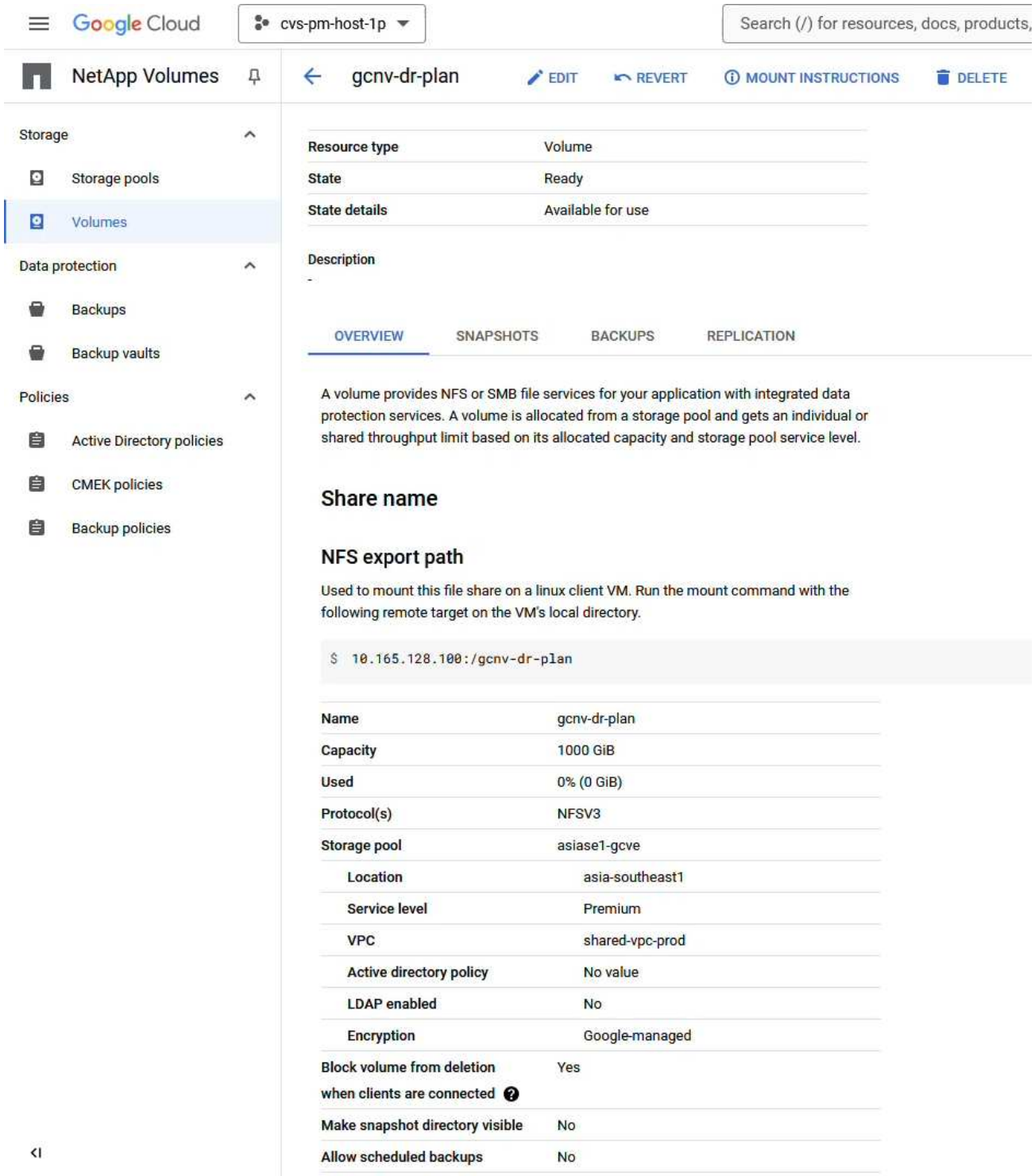






Cliquez sur **Créer** pour terminer la création du volume.

4. Une fois le volume créé, le chemin d'exportation NFS requis pour monter le volume peut être affiché à partir de la page des propriétés du volume.



▼ **Monter le magasin de données NFS dans GCVE**

Au moment de la rédaction de cet article, le processus de montage d'une banque de données dans GCVE nécessite l'ouverture d'un ticket de support GCP pour que le volume soit monté en tant que banque de données NFS.

Se référer à "Utilisation du volume NFS comme banque de données vSphere hébergée par Google Cloud NetApp Volumes" pour plus d'informations.

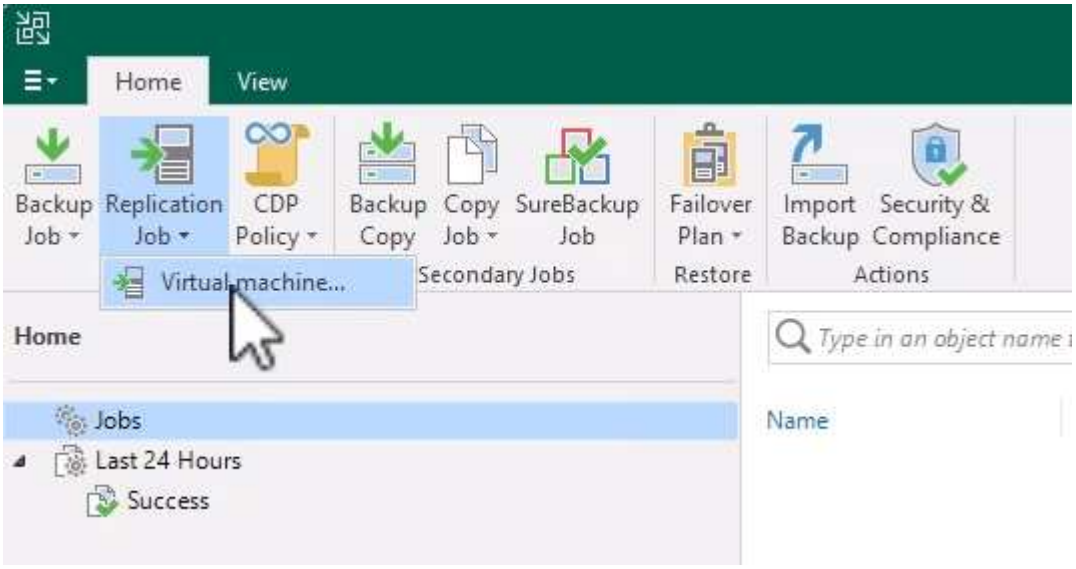
Répliquer les machines virtuelles vers GCVE et exécuter le plan de basculement et la restauration

▼ Répliquer des machines virtuelles vers une banque de données NFS dans GCVE

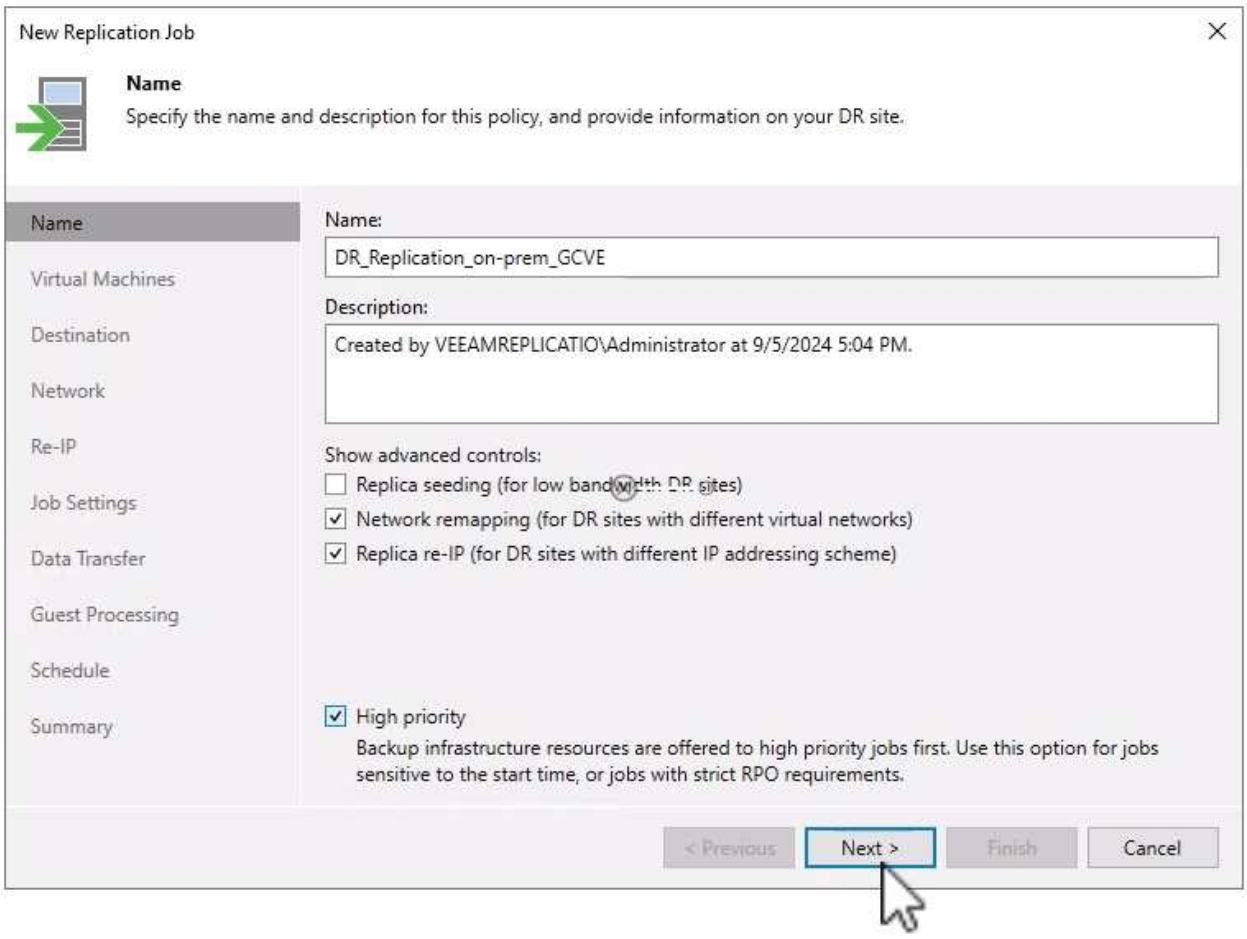
Veeam Backup & Replication exploite les fonctionnalités de snapshot de VMware vSphere pendant la réplication. Veeam Backup & Replication demande à VMware vSphere de créer un snapshot de VM. L'instantané de machine virtuelle est la copie ponctuelle d'une machine virtuelle qui inclut les disques virtuels, 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 la console Veeam Backup & Replication.
2. Dans l'onglet **Accueil**, cliquez sur **Tâche de réplication > Machine virtuelle…**

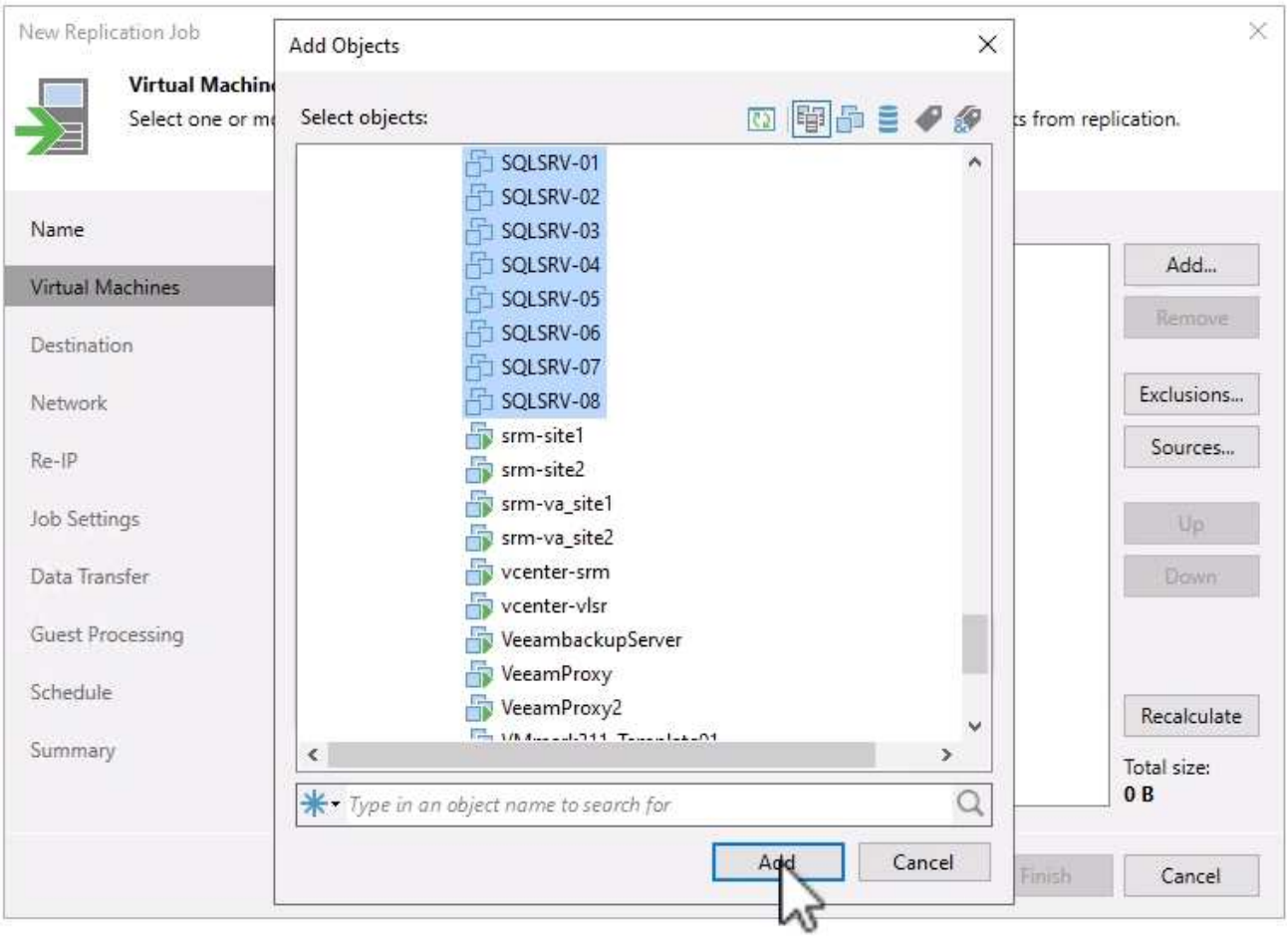


3. Sur la page **Nom** de l'assistant **Nouveau travail de réplication**, spécifiez un nom de travail et sélectionnez les cases à cocher de contrôle avancé appropriées.
   - Cochez la case Amorçage de réplication si la connectivité entre le site local et GCP a une bande passante restreinte.
   - Cochez la case Remappage réseau (pour les sites GCVE SDDC avec des réseaux différents) si les segments du GCVE SDDC ne correspondent pas à ceux des réseaux du site local.
   - Cochez la case Réplication IP (pour les sites DR avec un schéma d'adressage IP différent) si le schéma d'adressage IP du site de production sur site diffère du schéma du site GCVE cible.

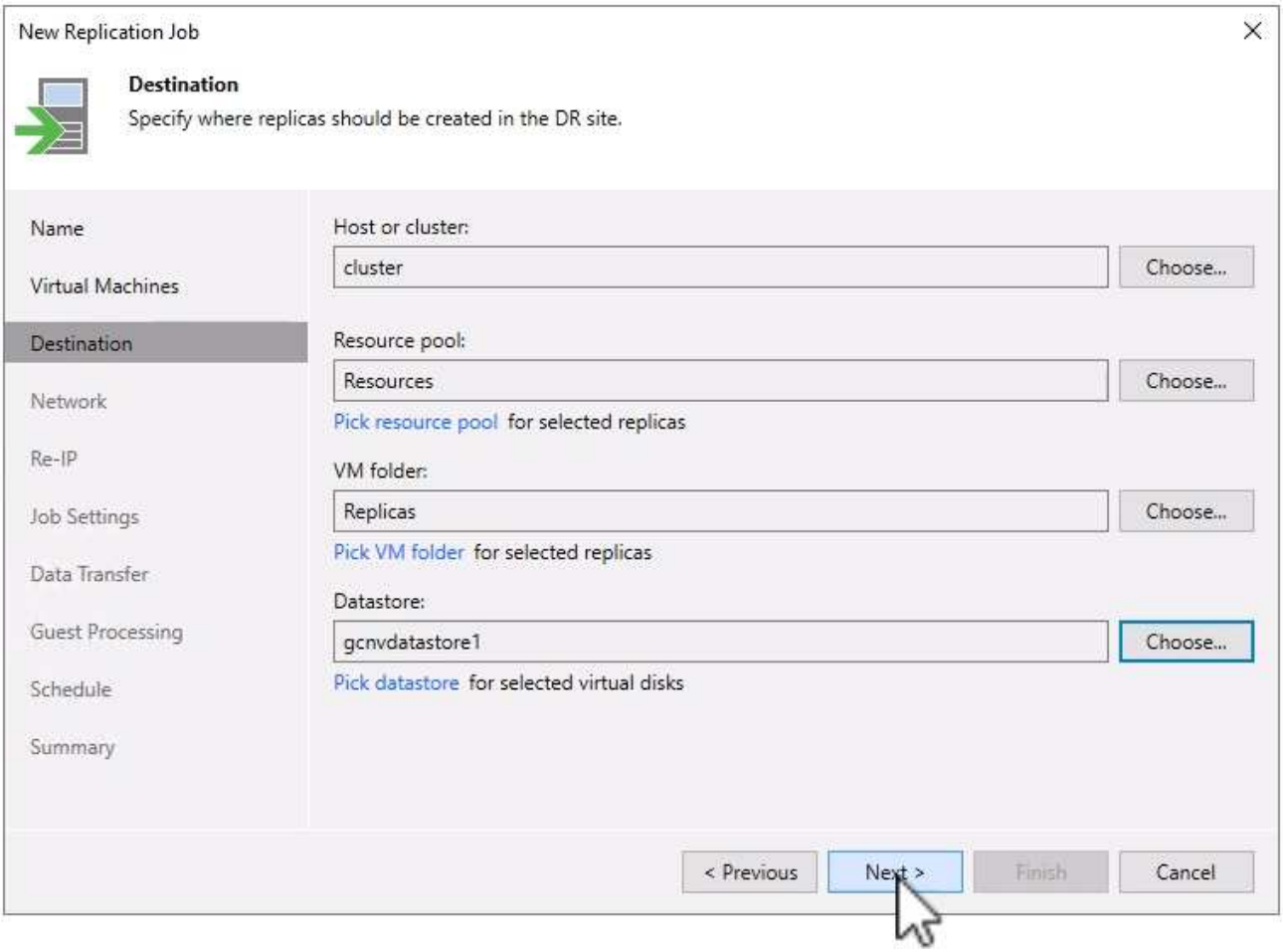


4. Sur la page **Machines virtuelles**, sélectionnez les machines virtuelles à répliquer vers la banque de données NetApp Volumes attachée à un SDDC GCVE. Cliquez sur **Ajouter**, puis dans la fenêtre **Ajouter un objet**, sélectionnez les machines virtuelles ou les conteneurs de machines virtuelles nécessaires et cliquez sur **Ajouter**. Cliquez sur **Suivant**.

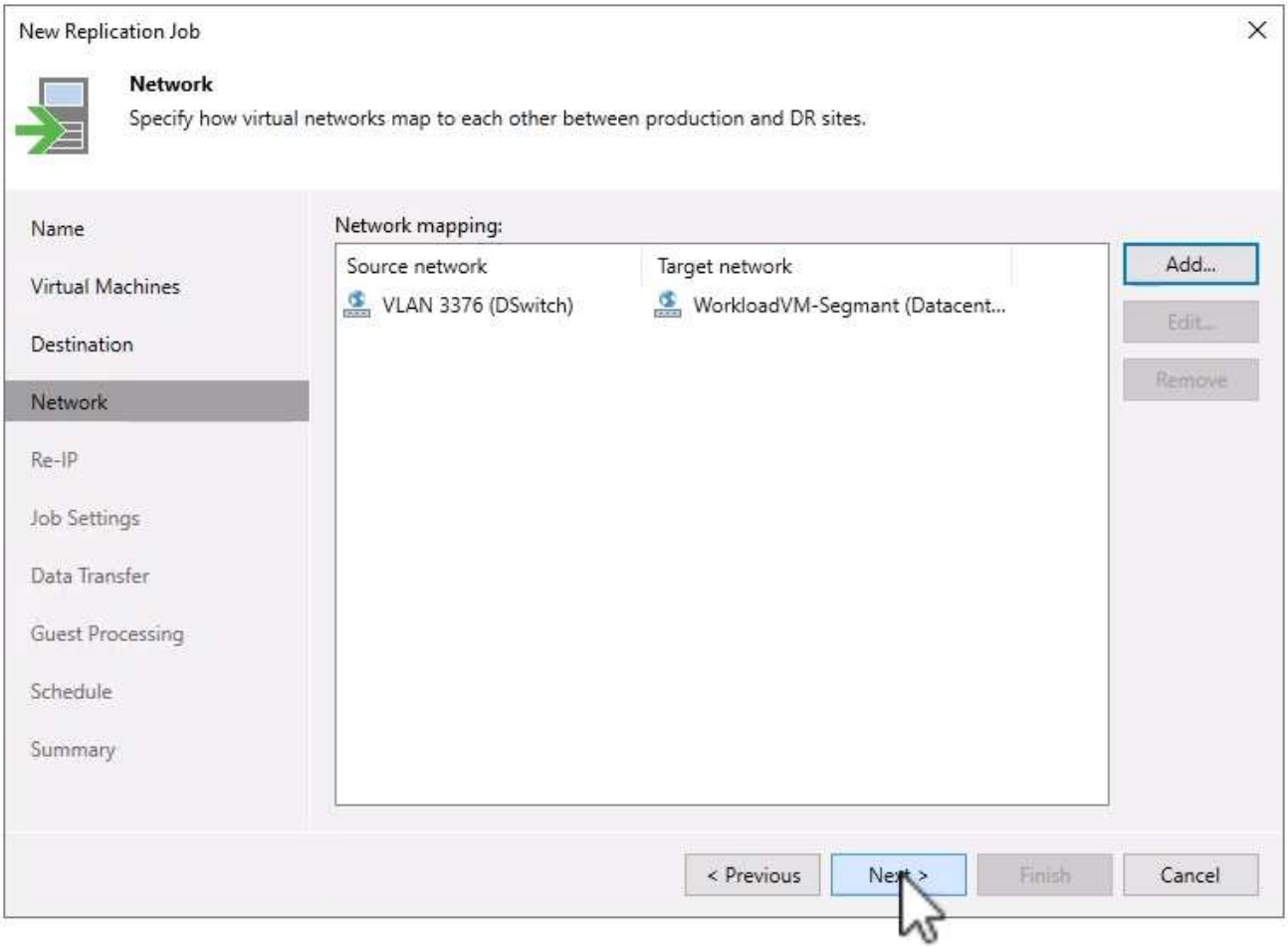
Les machines virtuelles peuvent être placées sur vSAN pour remplir la capacité de stockage de données vSAN disponible. Dans un cluster pilote, la capacité utilisable d'un cluster vSAN à 3 nœuds sera limitée. Le reste des données peut être facilement placé sur les magasins de données Google Cloud NetApp Volumes afin que les machines virtuelles puissent être récupérées et que le cluster puisse être étendu ultérieurement pour répondre aux exigences CPU/mémoire.



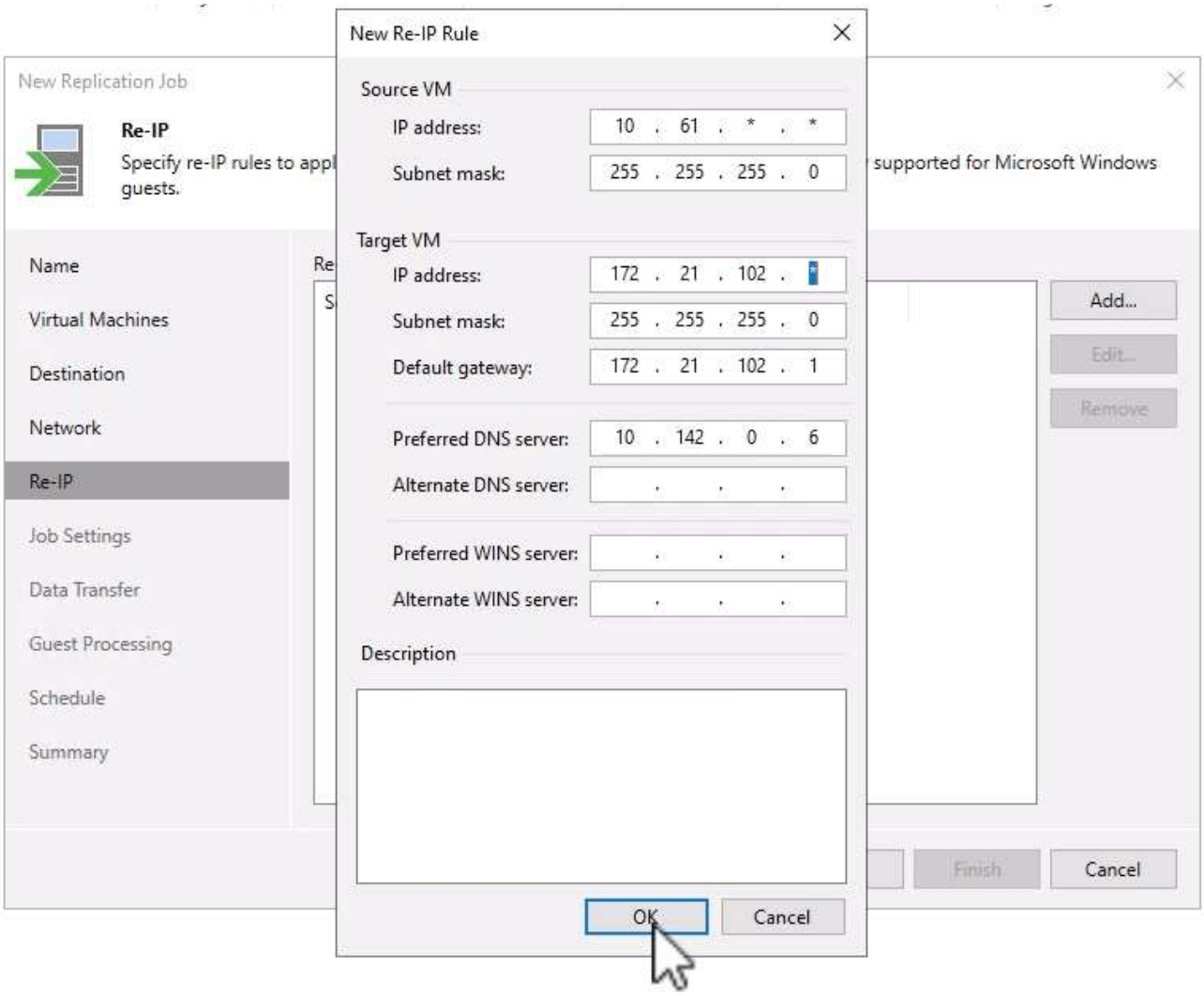
5. Sur la page **Destination**, sélectionnez la destination comme cluster/hôtes GCVE SDDC et le pool de ressources, le dossier de machine virtuelle et la banque de données NetApp Volumes appropriés pour les répliques de machine virtuelle. Cliquez sur **Suivant** pour continuer.



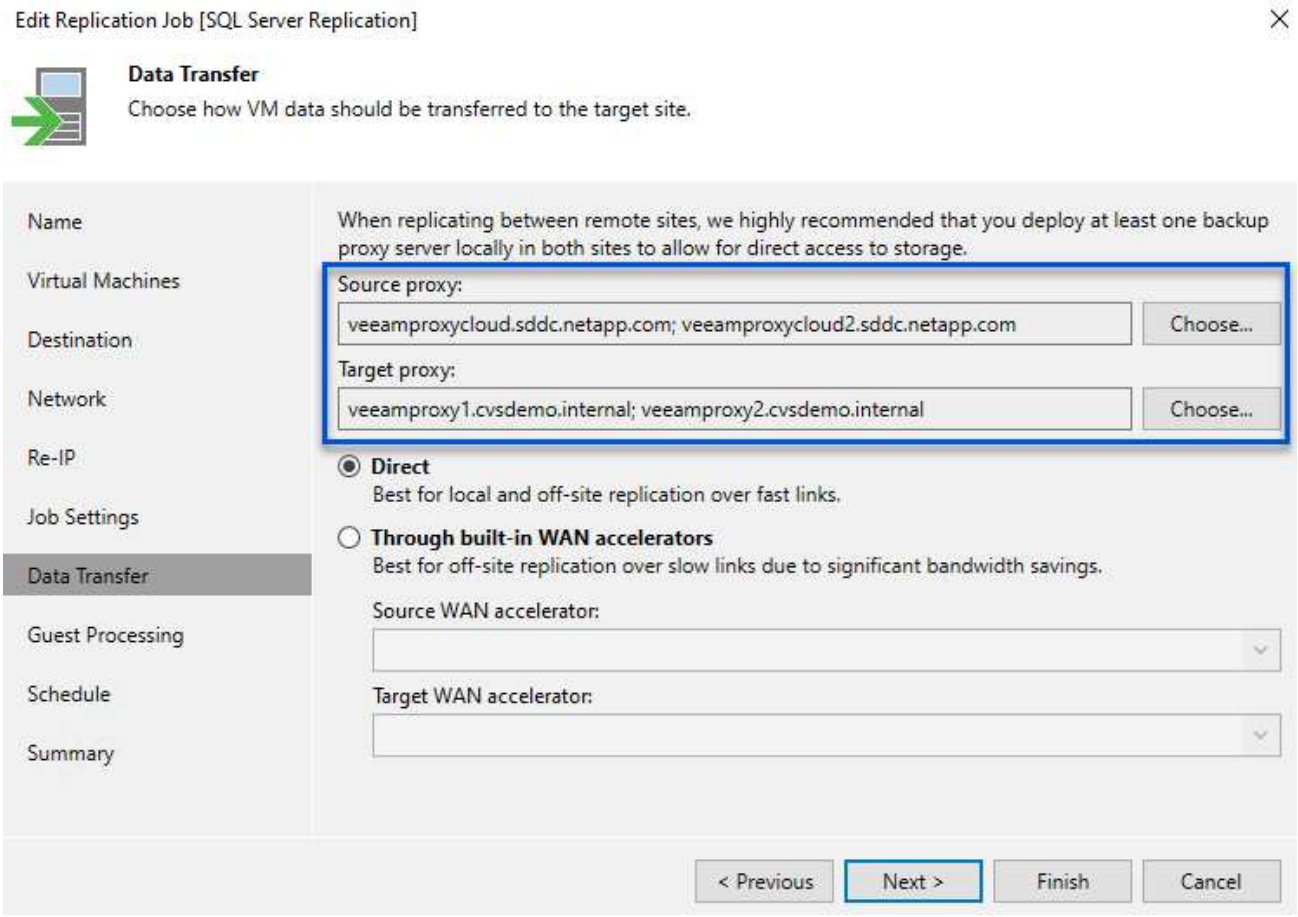
6. Sur la page **Réseau**, créez le mappage entre les réseaux virtuels source et cible selon vos besoins. Cliquez sur **Suivant** pour continuer.



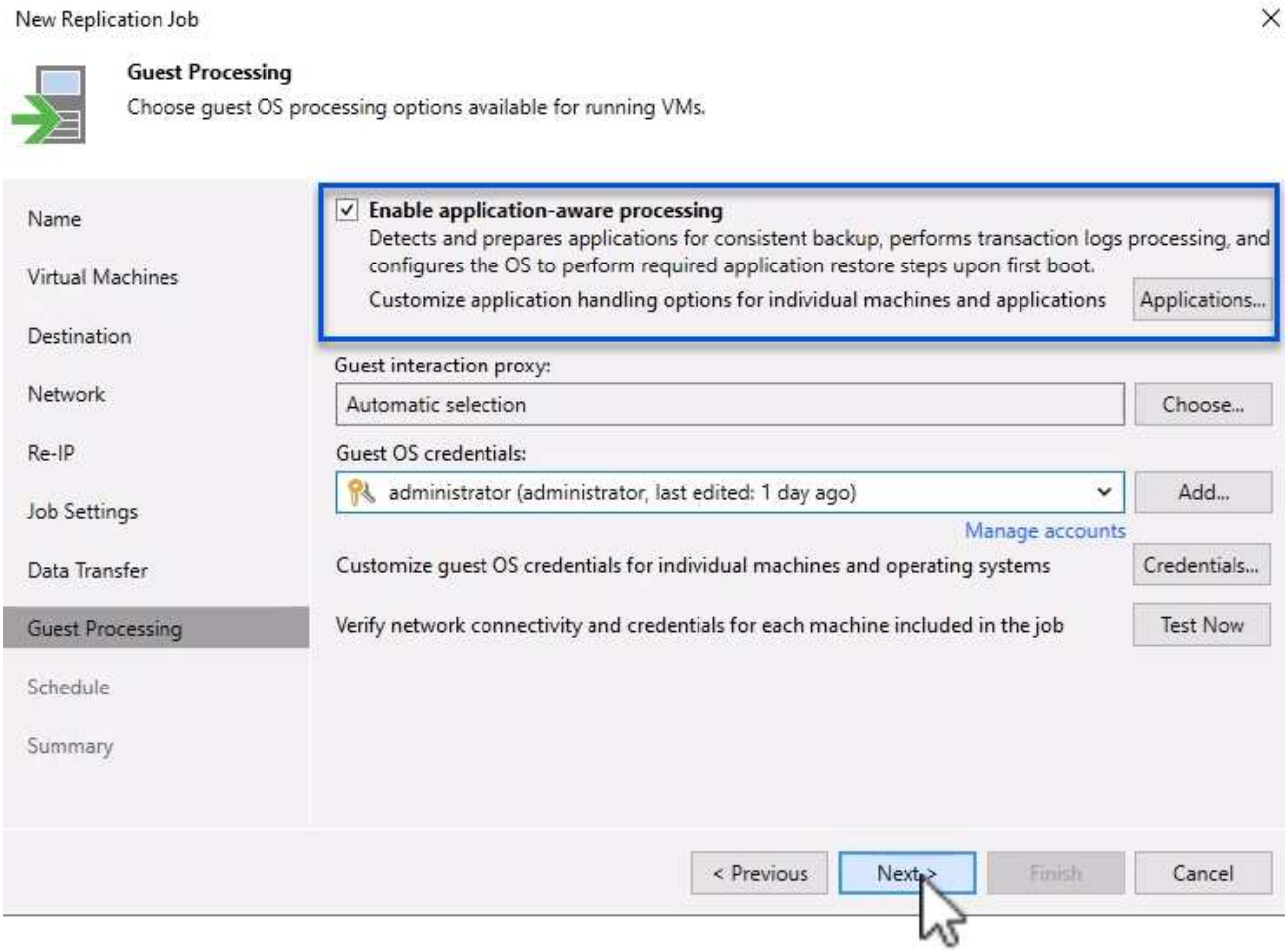
7. Sur la page **Re-IP**, cliquez sur le bouton **Ajouter…** pour ajouter une nouvelle règle de ré-IP. Remplissez les plages d'adresses IP des machines virtuelles source et cible pour spécifier la mise en réseau qui sera appliquée aux machines virtuelles source en cas de basculement. Utilisez des astérisques pour spécifier qu'une plage d'adresses est indiquée pour cet octet. Cliquez sur **Suivant** pour continuer.



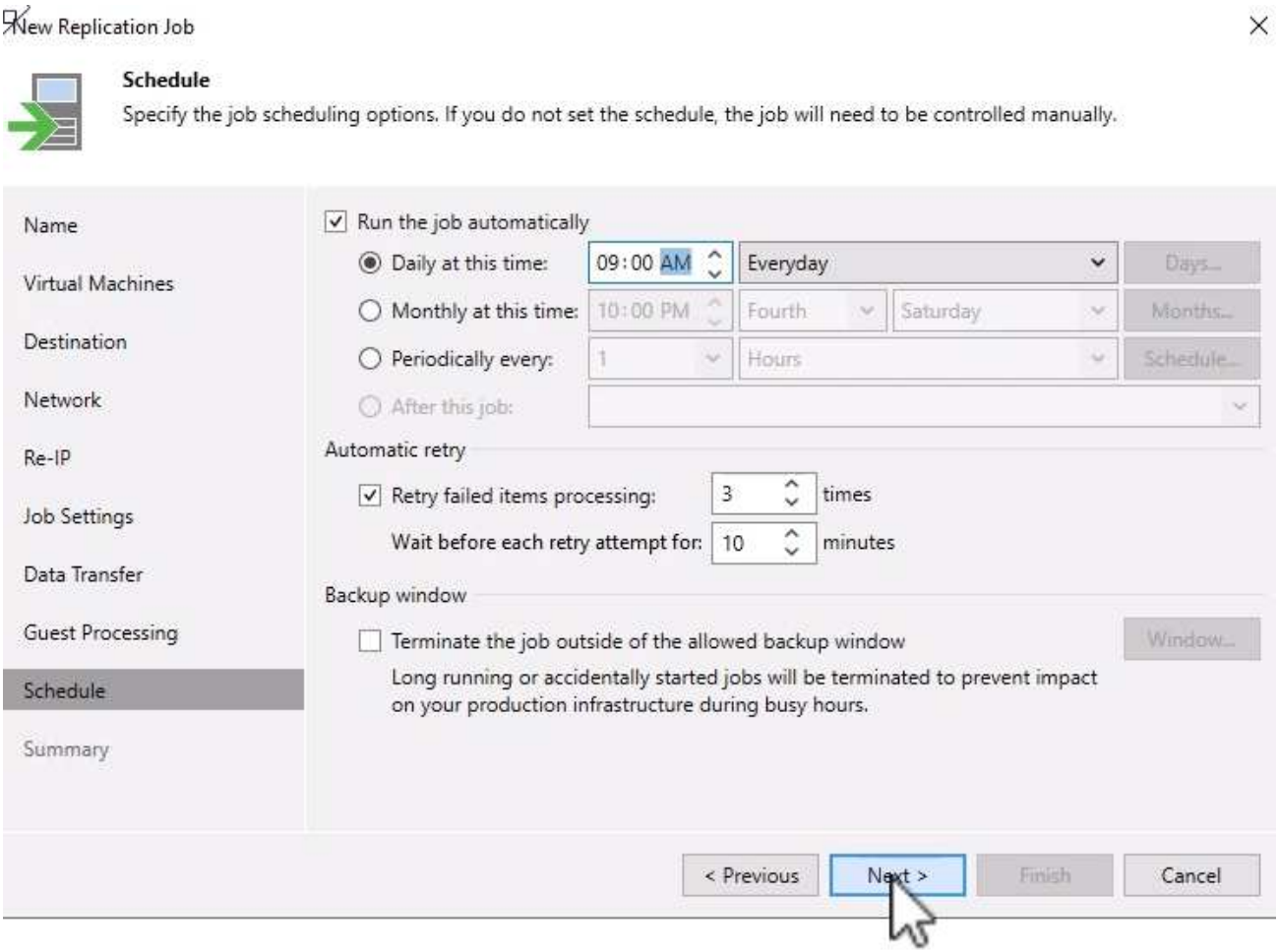
8. Sur la page **Paramètres de tâche**, spécifiez le référentiel de sauvegarde qui stockera les métadonnées des répliques de machines virtuelles, la politique de rétention et sélectionnez le bouton en bas pour **Avancé…** pour des paramètres de tâche supplémentaires. Cliquez sur **Suivant** pour continuer.
9. Dans le **Transfert de données**, sélectionnez les serveurs proxy qui résident sur les sites source et cible, et conservez l'option Direct sélectionnée. Les accélérateurs WAN peuvent également être sélectionnés ici, s'ils sont configurés. Cliquez sur **Suivant** pour continuer.



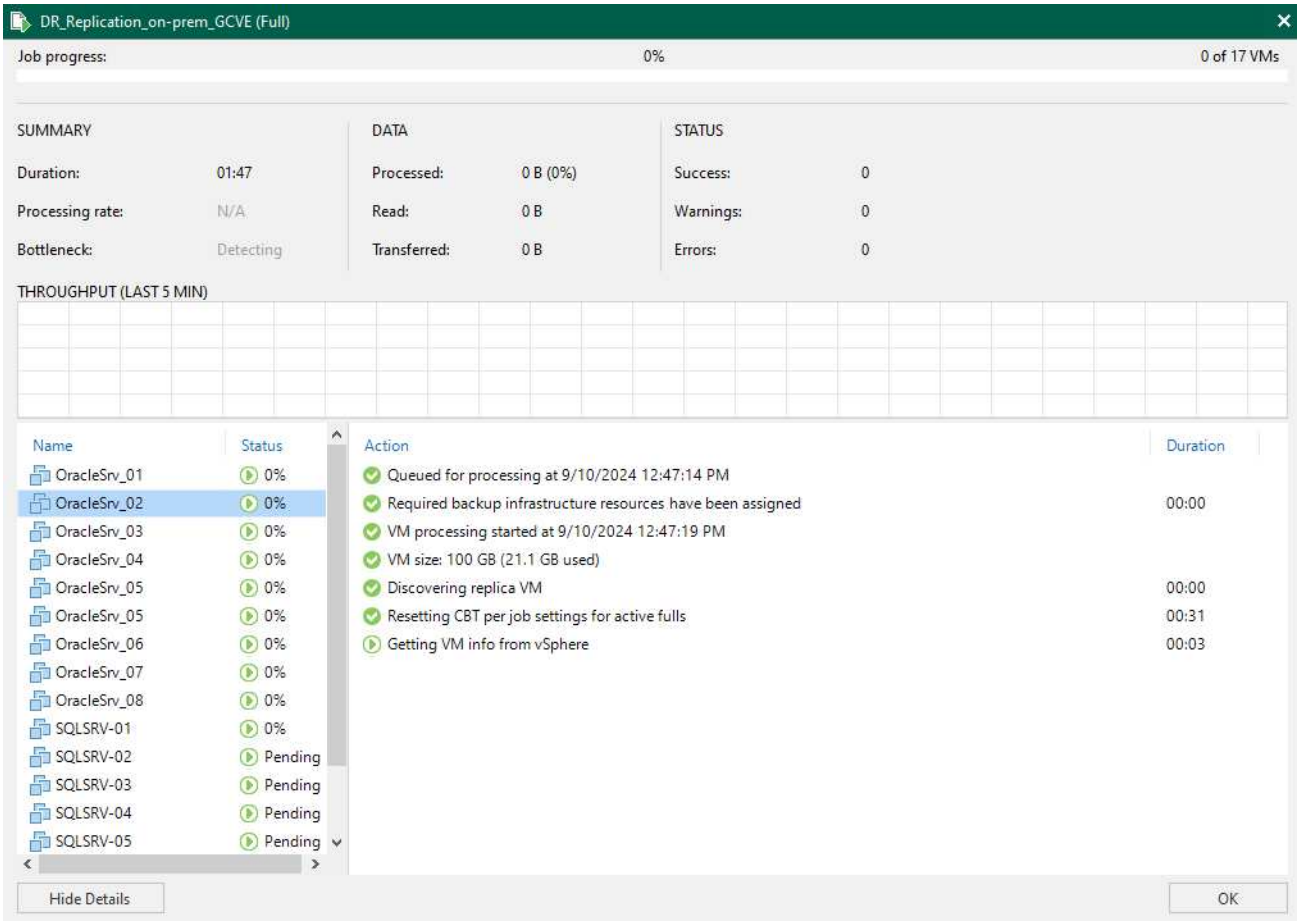
10. Sur la page **Traitement invité**, cochez la case **Activer le traitement sensible aux applications** si nécessaire et sélectionnez les **Informations d'identification du système d'exploitation invité**. Cliquez sur **Suivant** pour continuer.



11. Sur la page **Planification**, définissez les heures et la fréquence auxquelles le travail de réplication sera exécuté. Cliquez sur **Suivant** pour continuer.



12. Enfin, vérifiez les paramètres du travail sur la page **Résumé**. Cochez la case **Exécuter le travail lorsque je clique sur Terminer**, puis cliquez sur **Terminer** pour terminer la création du travail de réplication.
13. Une fois exécuté, le travail de réplication peut être visualisé dans la fenêtre d'état du travail.



Pour plus d'informations sur la réplication Veeam, reportez-vous à"Comment fonctionne la réplication"

▼ **Créer un plan de basculement**

Une fois la réplication ou l'amorçage initial terminé, créez le plan de basculement. Le plan de basculement permet d'effectuer le basculement des machines virtuelles dépendantes une par une ou en tant que groupe automatiquement. Le plan de basculement est le plan directeur de l'ordre dans lequel les machines virtuelles sont traitées, y compris les délais de démarrage. Le plan de basculement permet également de garantir que les machines virtuelles dépendantes critiques sont déjà en cours d'exécution.

Après avoir terminé la réplication ou l'amorçage initial, créez un plan de basculement. Ce plan sert de modèle stratégique pour orchestrer le basculement des machines virtuelles dépendantes, individuellement ou en groupe. Il définit l'ordre de traitement des machines virtuelles, intègre les délais de démarrage nécessaires et garantit que les machines virtuelles dépendantes critiques sont opérationnelles avant les autres. En mettant en œuvre un plan de basculement bien structuré, les organisations peuvent rationaliser leur processus de reprise après sinistre, en minimisant les temps d'arrêt et en maintenant l'intégrité des systèmes interdépendants lors d'un événement de basculement.

Lors de la création du plan, Veeam Backup & Replication identifie et utilise automatiquement les points de restauration les plus récents pour lancer les répliques de VM.

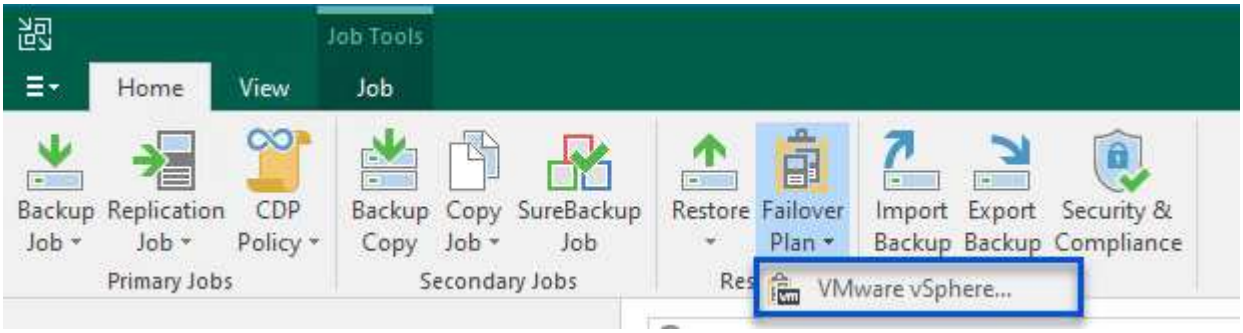
ⓘ Le plan de basculement ne peut être créé qu'une fois la réplication initiale terminée et les répliques de machines virtuelles à l'état Prêt.

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

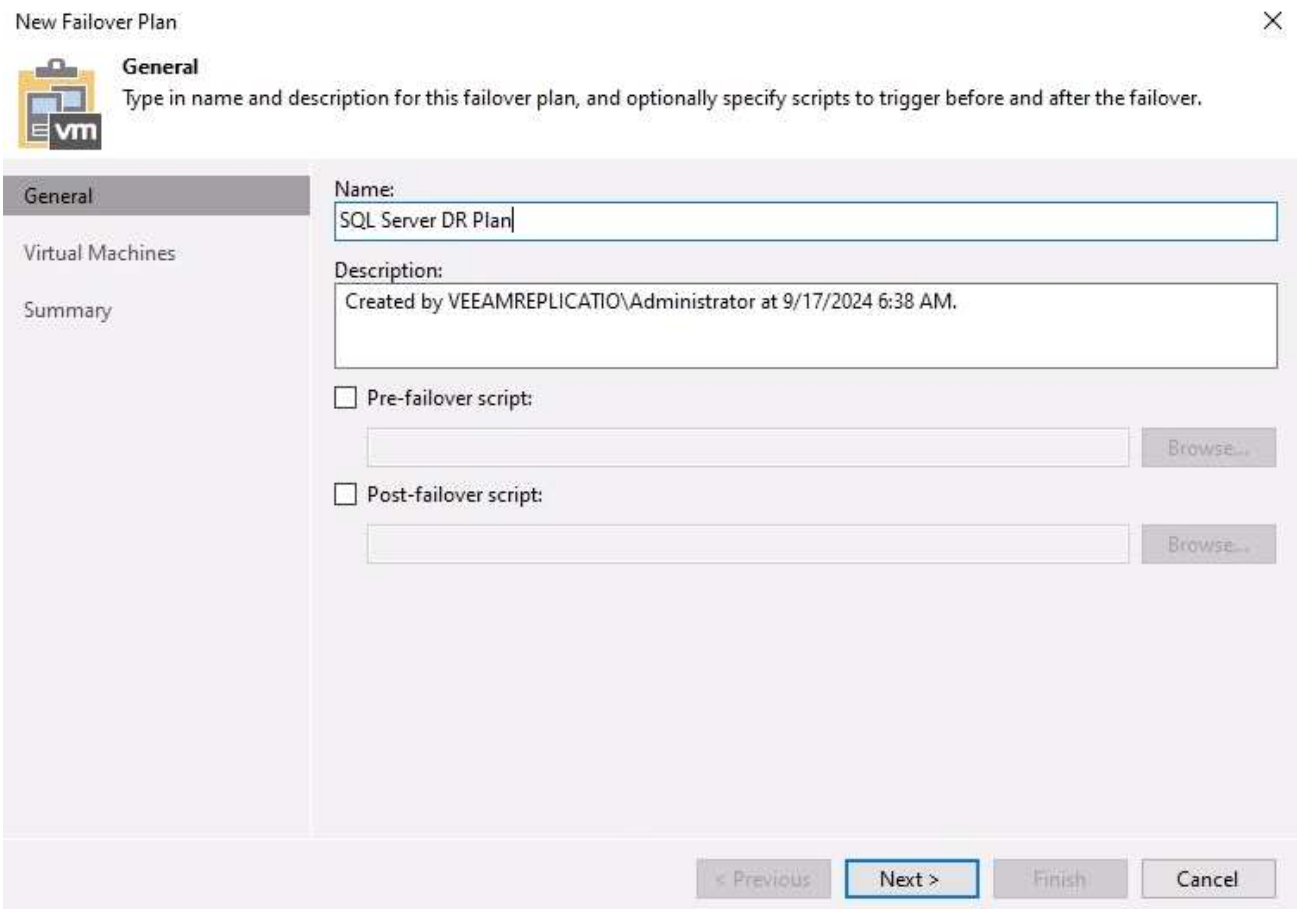
Pendant le processus de basculement, les machines virtuelles sources ne seront pas mises hors tension.

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

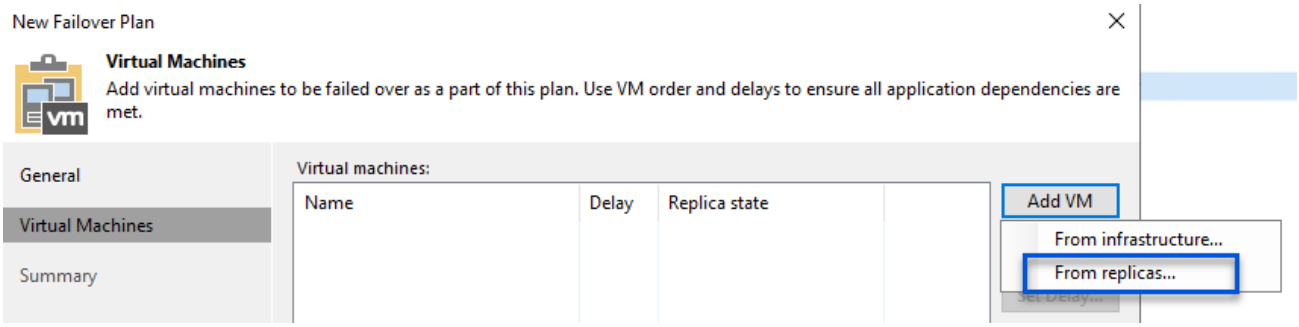
1. Dans la vue **Accueil**, cliquez sur le bouton **Plan de basculement** dans la section **Restaurer**. Dans la liste déroulante, sélectionnez **VMware vSphere…**

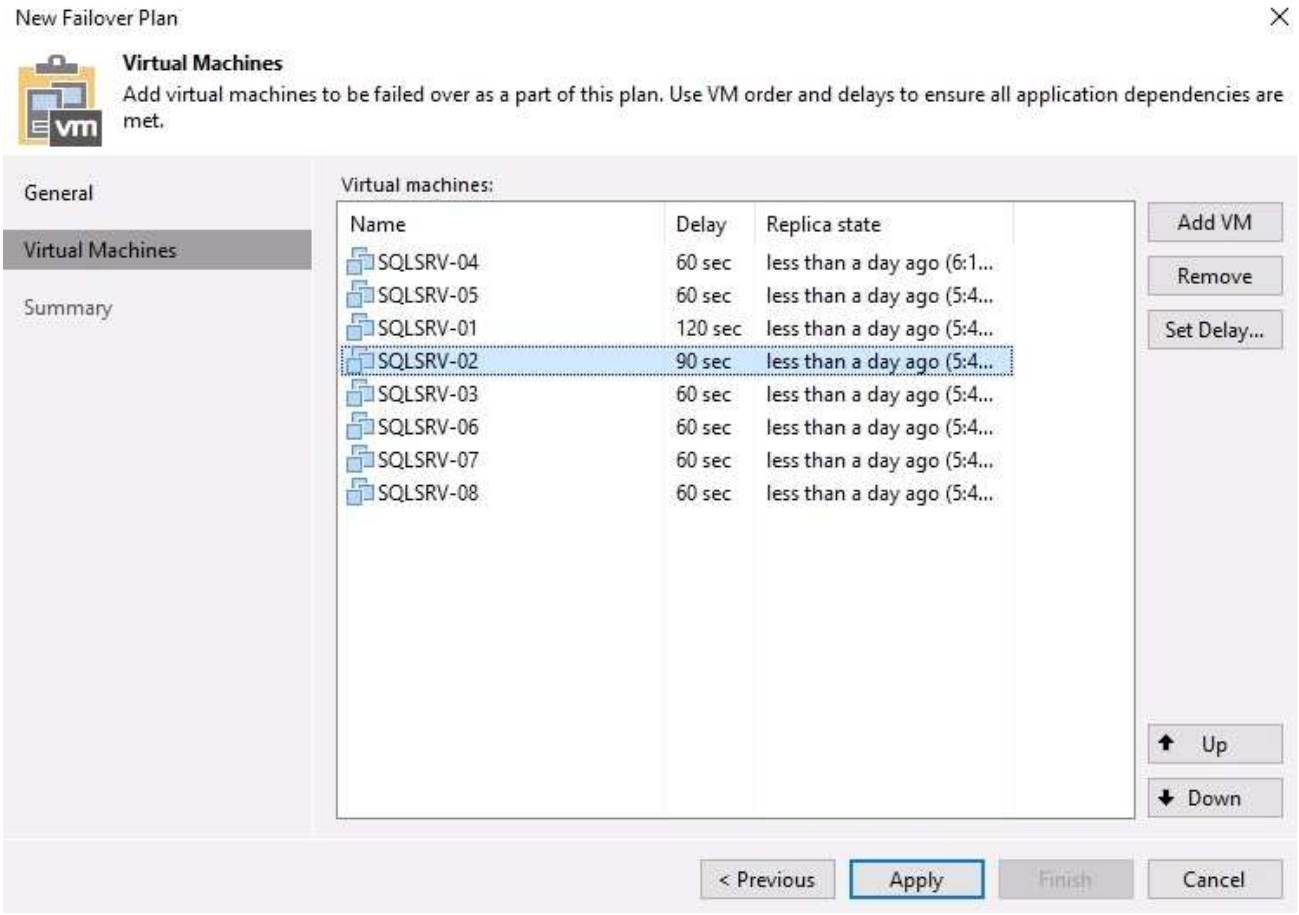


2. Sur la page **Général** de l'assistant **Nouveau plan de basculement**, indiquez un nom et une description pour le plan. Des scripts de pré et post-basculement peuvent être ajoutés selon les besoins. Par exemple, exécutez un script pour arrêter les machines virtuelles avant de démarrer les machines virtuelles répliquées.



3. Sur la page **Machines virtuelles**, cliquez sur le bouton **Ajouter une VM** et sélectionnez **À partir de répliques…**. Choisissez les machines virtuelles qui feront partie du plan de basculement, puis modifiez l'ordre de démarrage des machines virtuelles et les délais de démarrage requis pour répondre aux dépendances de l'application.





Cliquez sur **Appliquer** pour continuer.

4. Enfin, vérifiez tous les paramètres du plan de basculement et cliquez sur **Terminer** pour créer le plan de basculement.

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

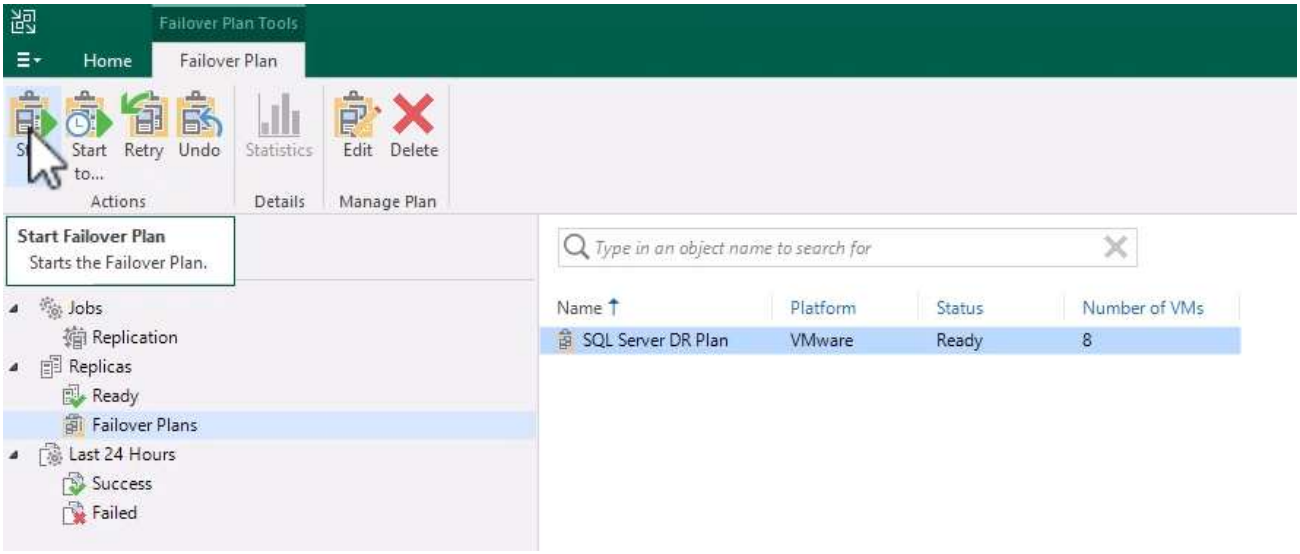
▼ Exécuter le plan de basculement

Lors du basculement, la machine virtuelle source du site de production bascule vers sa réplique sur le site de reprise après sinistre. Dans le cadre du processus, Veeam Backup & Replication restaure la réplique de la machine virtuelle au point de restauration requis et transfère toutes les activités d'E/S de la machine virtuelle source vers sa réplique. Les répliques servent non seulement à faire face à des catastrophes réelles, mais également à simuler des exercices de DR. Dans la simulation de basculement, la machine virtuelle source continue de fonctionner. Une fois les tests nécessaires terminés, le basculement peut être annulé, ramenant les opérations à la normale.

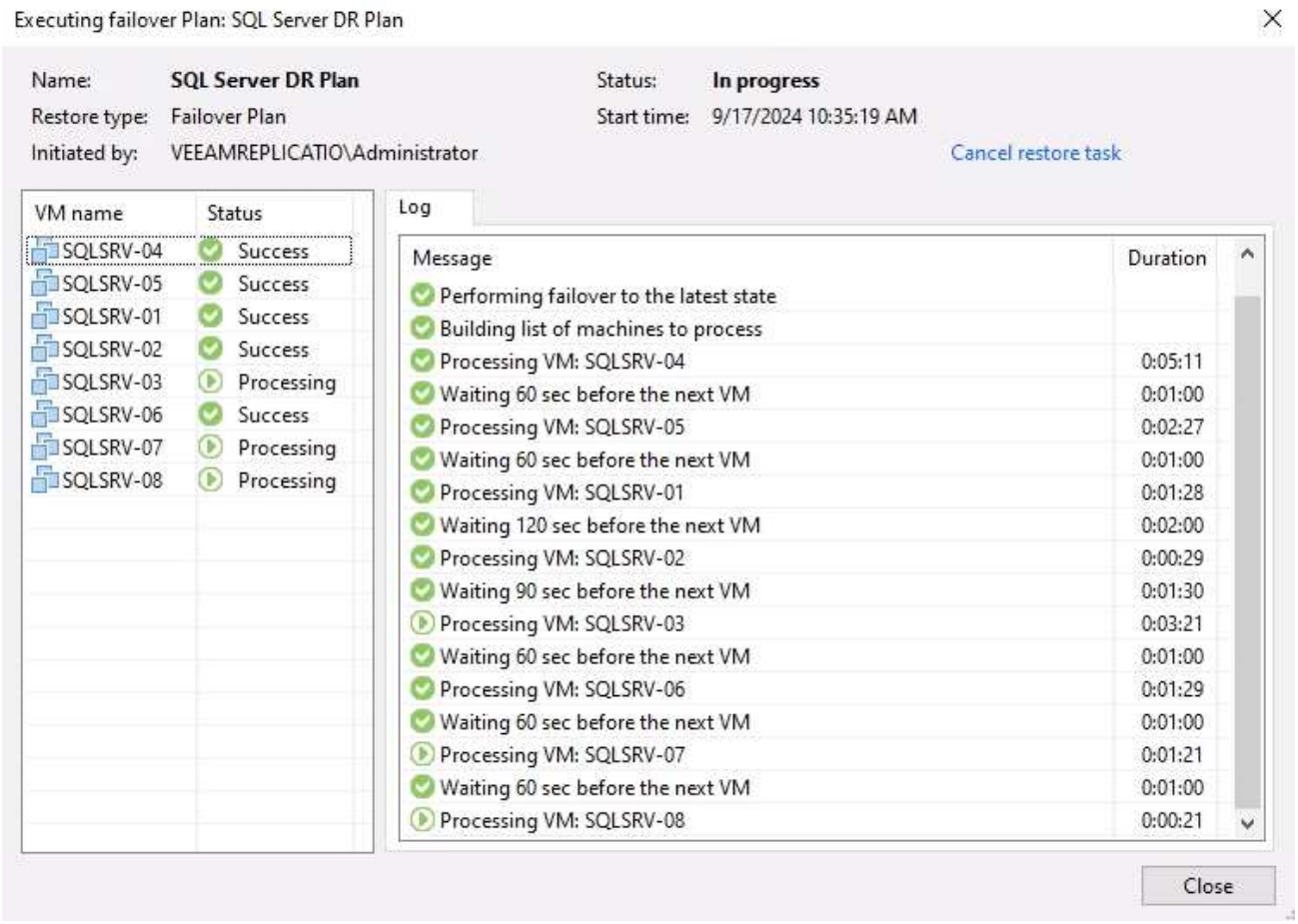
Assurez-vous que la segmentation du réseau est en place pour éviter les conflits IP lors du basculement.

Suivez les étapes suivantes pour démarrer le plan de basculement :

1. Pour commencer, dans la vue **Accueil**, cliquez sur **Répliques > Plans de basculement** dans le menu de gauche, puis sur le bouton **Démarrer**. Alternativement, le bouton **Démarrer vers…** peut être utilisé pour basculer vers un point de restauration antérieur.



2. Surveillez la progression du basculement dans la fenêtre **Exécution du plan de basculement**.



Veeam Backup & Replication arrête toutes les activités de réplication pour la machine virtuelle source jusqu'à ce que sa réplique soit ramenée à l'état Prêt.

Pour des informations détaillées sur les plans de basculement, reportez-vous à"Plans de basculement" .

▼ **Retour au site de production**

La réalisation d'un basculement est considérée comme une étape intermédiaire et doit être finalisée en fonction des besoins. Les options incluent les suivantes :

- **Retour à la production** - Revenez à la machine virtuelle d'origine et synchronisez toutes les modifications apportées pendant la période active de la réplique avec la machine virtuelle source.

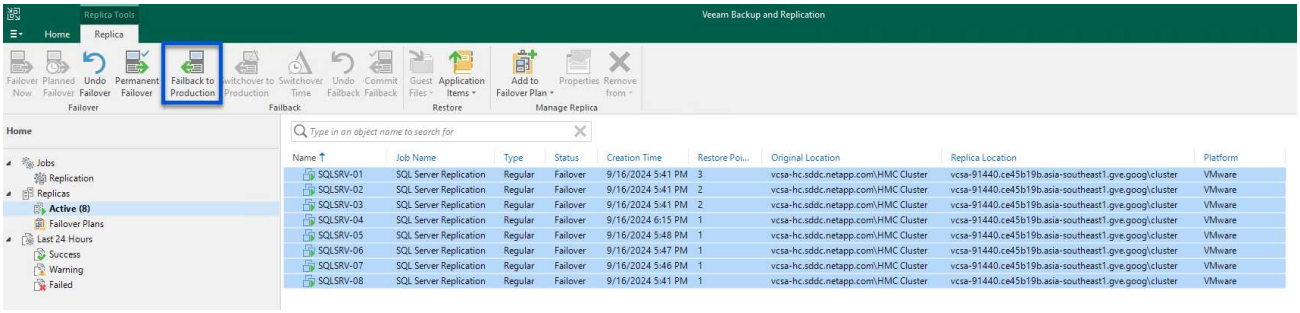
Lors de la restauration automatique, les modifications sont transférées mais pas immédiatement appliquées. Sélectionnez **Commit failback** une fois que la fonctionnalité de la machine virtuelle d'origine est vérifiée. Vous pouvez également choisir **Annuler la restauration automatique** pour revenir à la réplique de la machine virtuelle si la machine virtuelle d'origine présente un comportement inattendu.

- **Annuler le basculement** - Revenir à la machine virtuelle d'origine, en supprimant toutes les modifications apportées à la réplique de la machine virtuelle pendant sa période de fonctionnement.
- **Basculement permanent** - Basculez définitivement de la machine virtuelle d'origine vers sa réplique, en établissant la réplique comme nouvelle machine virtuelle principale pour les opérations en cours.

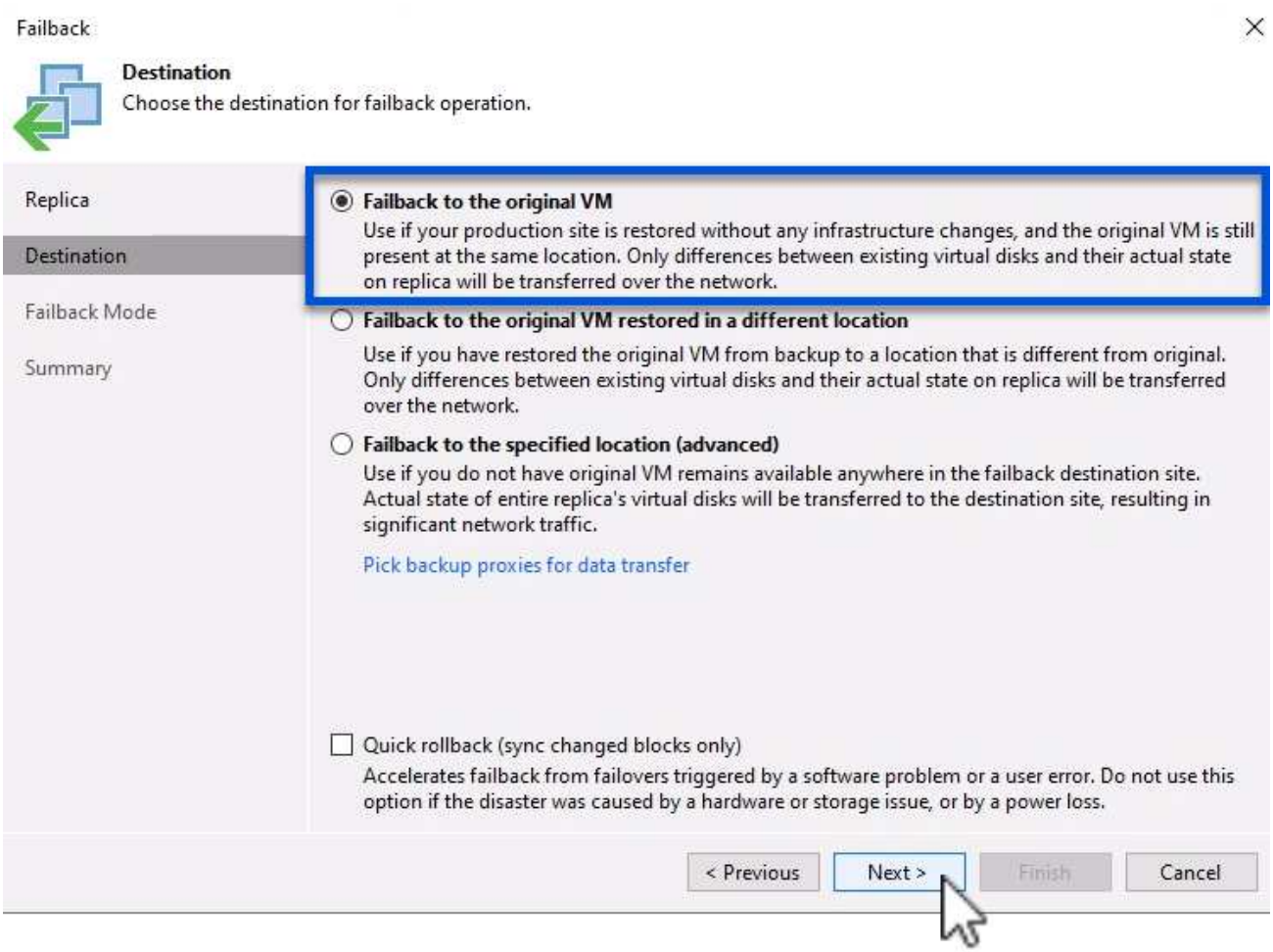
Dans ce scénario, l'option « Retour à la production » a été sélectionnée.

Suivez les étapes suivantes pour effectuer une restauration automatique vers le site de production :

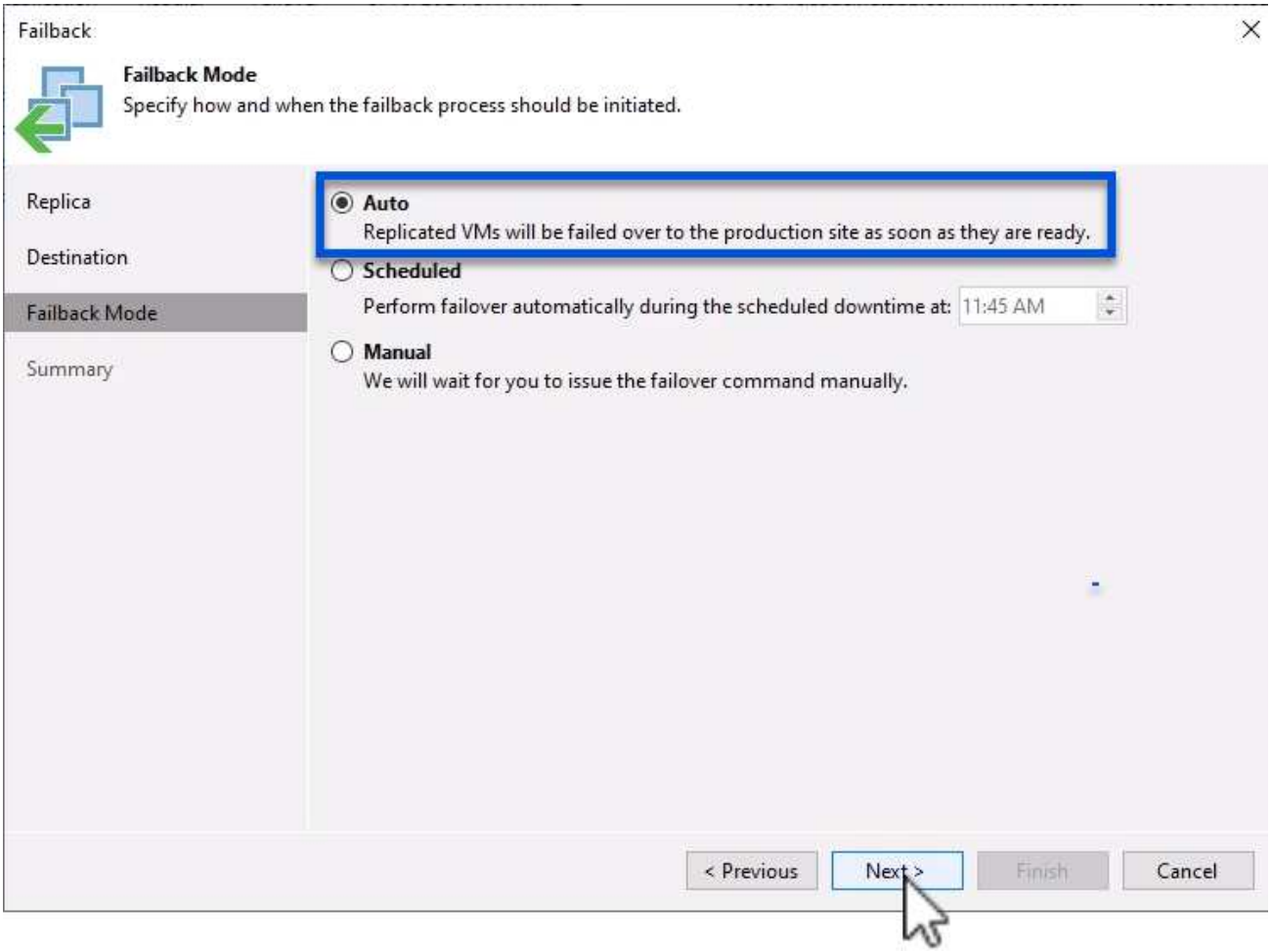
1. Depuis la vue **Accueil**, cliquez sur **Répliques > Actif** dans le menu de gauche. Sélectionnez les machines virtuelles à inclure et cliquez sur le bouton **Retour en production** dans le menu supérieur.



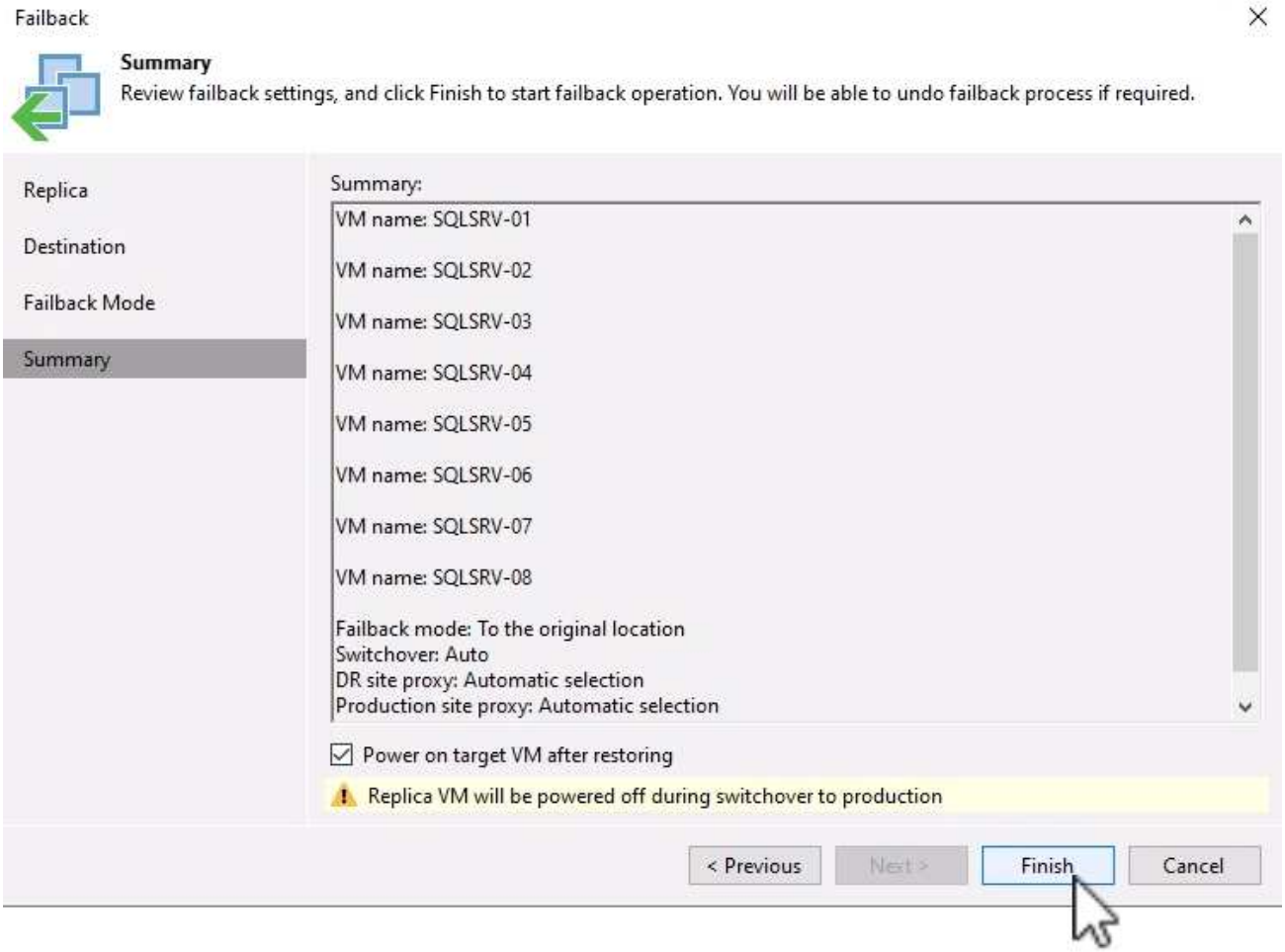
2. Sur la page **Réplique** de l'assistant **Retour en arrière**, sélectionnez les répliques à inclure dans la tâche de retour en arrière.
3. Sur la page **Destination**, sélectionnez **Retour à la VM d'origine** et cliquez sur **Suivant** pour continuer.



4. Sur la page **Mode de restauration automatique**, sélectionnez **Auto** pour démarrer la restauration automatique dès que possible.

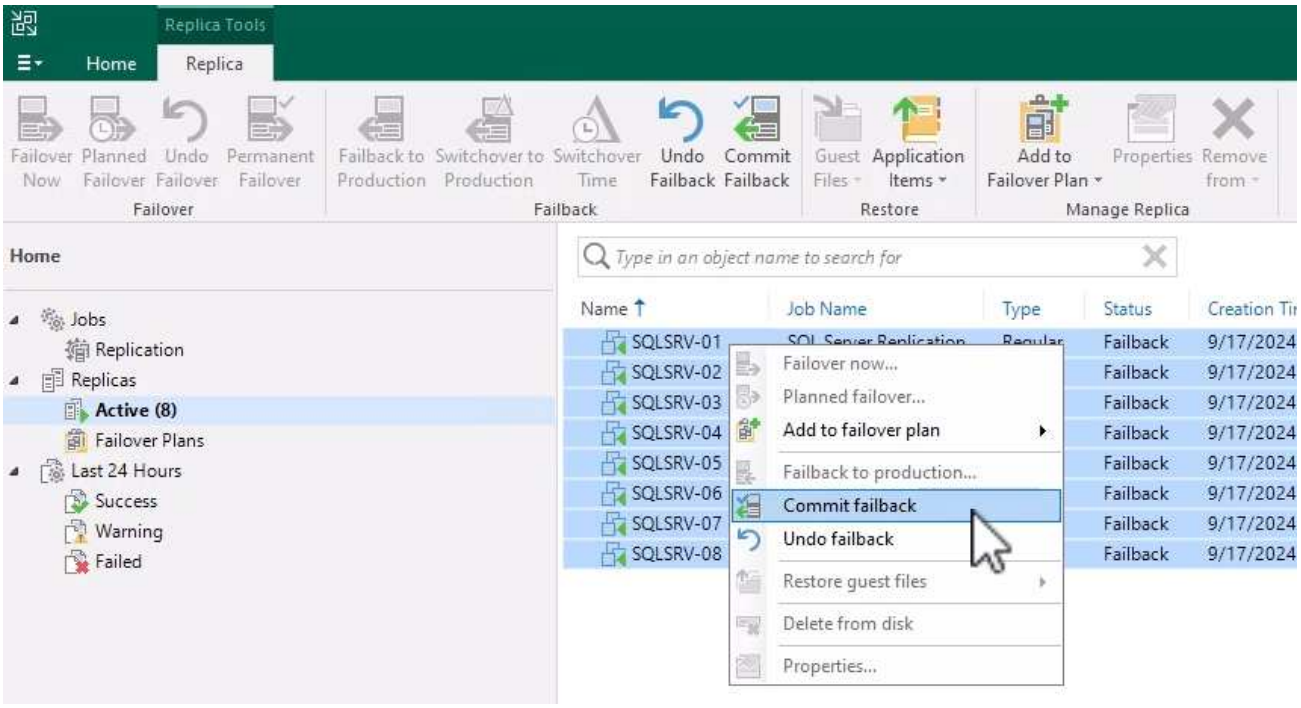


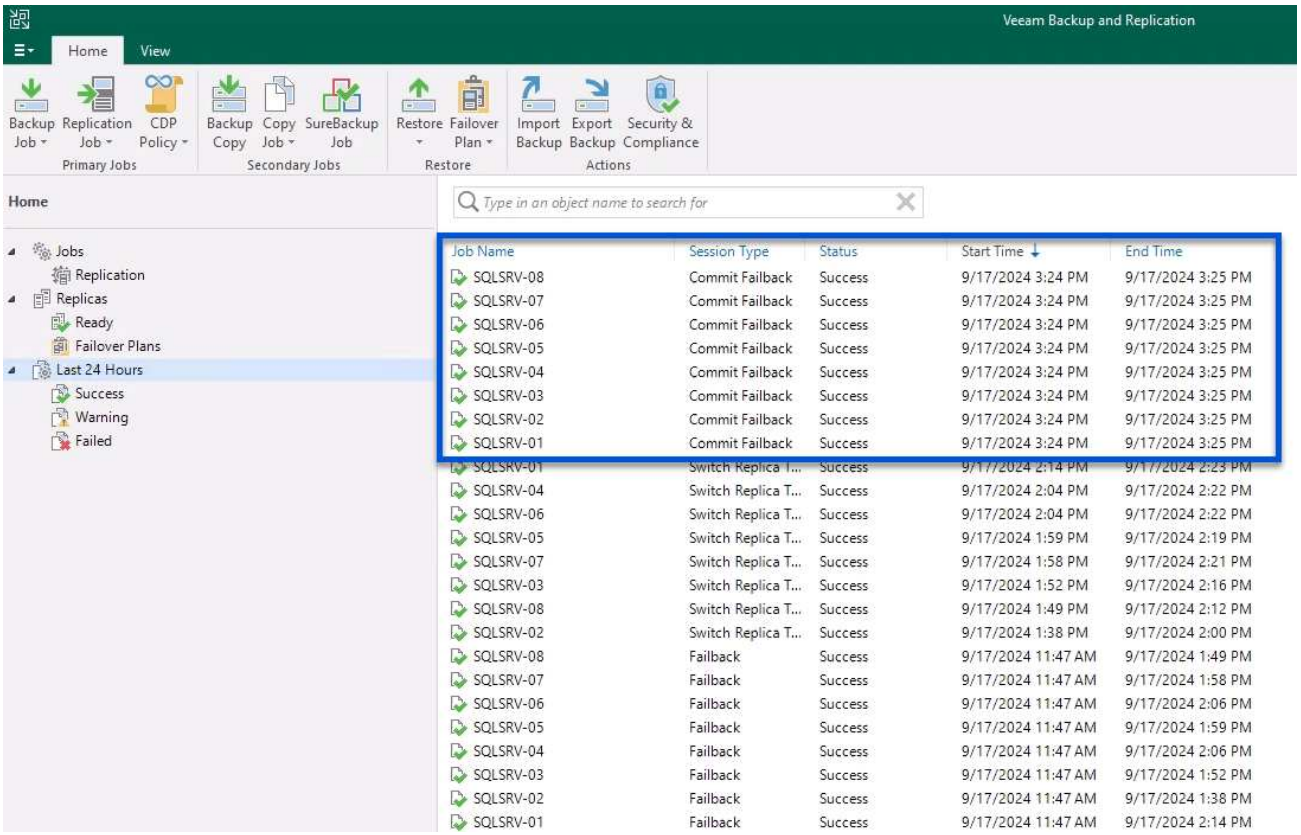
5. Sur la page **Résumé**, choisissez si vous souhaitez **Mettre sous tension la machine virtuelle cible après la restauration**, puis cliquez sur Terminer pour démarrer la tâche de restauration automatique.



La validation de restauration finalise l'opération de restauration, confirmant l'intégration réussie des modifications apportées à la machine virtuelle de production. Lors de la validation, Veeam Backup & Replication reprend les activités de réplication normales pour la machine virtuelle de production restaurée. Cela modifie l'état de la réplique restaurée de *Failback* à *Ready*.

1. Pour valider la restauration, accédez à **Répliques > Actif**, sélectionnez les machines virtuelles à valider, faites un clic droit et sélectionnez **Valider la restauration**.





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

Pour des informations détaillées sur le processus de restauration automatique, reportez-vous à la documentation Veeam."Basculement et restauration pour la réplication" .

Conclusion

La fonctionnalité de banque de données Google Cloud NetApp Volumes permet à Veeam et à d'autres outils tiers validés de fournir des solutions de reprise après sinistre (DR) rentables. En utilisant des clusters Pilot Light au lieu de grands clusters dédiés aux répliques de machines virtuelles, les organisations peuvent réduire considérablement leurs dépenses. Cette approche permet des stratégies de reprise après sinistre sur mesure qui exploitent les solutions de sauvegarde internes existantes pour la reprise après sinistre basée sur le cloud, éliminant ainsi le besoin de centres de données sur site supplémentaires. En cas de sinistre, le basculement peut être lancé en un seul clic ou configuré pour se produire automatiquement, garantissant ainsi la continuité des activités avec un temps d'arrêt minimal.

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=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

Migrer les charges de travail sur GCP/GCVE

Migrer des charges de travail vers la banque de données Google Cloud NetApp Volumes sur Google Cloud VMware Engine à l'aide de VMware HCX - Guide de démarrage rapide

L'un des cas d'utilisation les plus courants du 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 et fournit divers mécanismes de migration pour déplacer des machines virtuelles (VM) sur site et leurs données vers des banques de données NFS Cloud Volume Service.

Présentation : Migration de machines virtuelles avec VMware HCX, les magasins de données Google Cloud NetApp Volumes et Google Cloud VMware Engine (GCVE)

VMware HCX est principalement une plate-forme de migration conçue pour simplifier la migration des applications, le rééquilibrage de la charge de travail et même la continuité des activités dans les clouds. Il est inclus dans le cadre de Google Cloud VMware Engine Private Cloud et offre de nombreuses façons de migrer les charges de travail et peut être utilisé pour les opérations de reprise après sinistre (DR).

Ce document fournit des instructions étape par étape pour le provisionnement de la banque de données Cloud Volume Service, suivies du téléchargement, du déploiement et de la configuration de VMware HCX, y compris tous ses principaux composants sur site et du côté de 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 banque de données car la migration s'effectue au niveau de la machine virtuelle. Par conséquent, ce document s'applique aux clients NetApp existants et aux clients non NetApp qui prévoient de déployer Cloud Volume Service avec Google Cloud VMware Engine pour un déploiement cloud VMware rentable.

▼ **Étapes de haut niveau**

Cette liste fournit les étapes de haut niveau nécessaires pour coupler et migrer les machines virtuelles vers HCX Cloud Manager côté Google Cloud VMware Engine à partir du connecteur HCX sur site :

1. Préparez HCX via le portail Google VMware Engine.
2. Téléchargez et déployez le programme d'installation de HCX Connector Open Virtualization Appliance (OVA) sur le serveur VMware vCenter local.

3. Activez HCX avec la clé de licence.
4. Associez le connecteur VMware HCX sur site à Google Cloud VMware Engine HCX Cloud Manager.
5. Configurez le profil réseau, le profil de calcul et le maillage de services.
6. (Facultatif) Effectuez une extension du réseau pour éviter la ré-IP pendant les migrations.
7. Validez l'état de l'appliance et assurez-vous que la migration est possible.
8. Migrer les charges de travail de la machine virtuelle.

▼ Prérequis

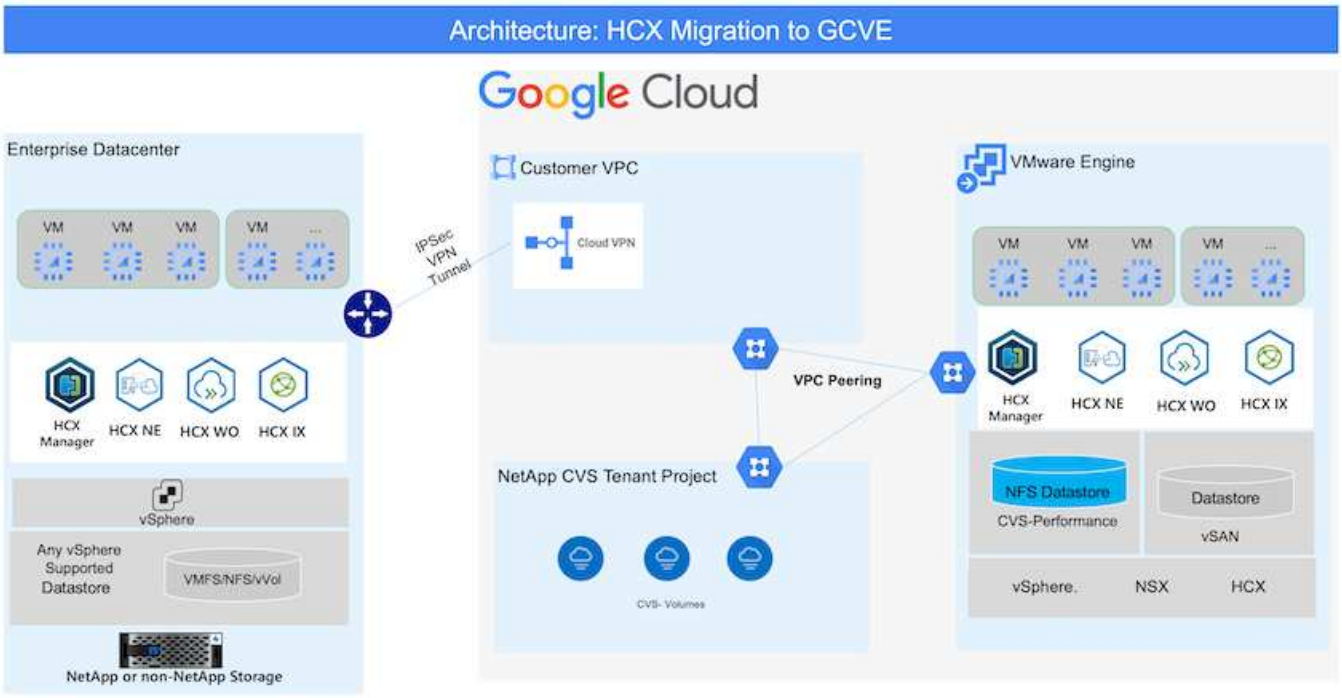
Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, voir ceci "lien" . Une fois les conditions préalables, y compris la connectivité, en place, téléchargez la clé de licence HCX à partir du portail Google Cloud VMware Engine. Une fois le programme 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. Référer "ce lien"

- Utilisez un centre de données défini par logiciel (SDDC) Google Cloud VMware Engine existant ou créez un cloud privé en l'utilisant."Lien NetApp" ou ceci "Lien Google" .
- La migration des machines virtuelles et des données associées à partir du centre de données local compatible VMware vSphere nécessite une connectivité réseau du centre de données vers l'environnement SDDC. Avant de migrer les charges de travail, "configurer une connexion Cloud VPN ou Cloud Interconnect" entre l'environnement sur site et le cloud privé respectif.
- Le chemin réseau de l'environnement VMware vCenter Server local 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 les informations requises "règles et ports du pare-feu" sont autorisés pour le trafic vMotion entre le vCenter Server local et le vCenter SDDC.
- Le volume NFS Cloud Volume Service doit être monté en tant que banque de données dans Google Cloud VMware Engine. Suivez les étapes détaillées dans ce "lien" pour attacher des magasins de données Cloud Volume Service aux hôtes Google Cloud VMware Engines.

▼ Architecture de haut niveau

À des fins de test, l'environnement de laboratoire local utilisé pour cette validation a été connecté via un VPN Cloud, qui permet la connectivité sur site à Google Cloud VPC.



Pour plus de détails sur l'utilisation de VMware HCX avec Google, veuillez consulter "Lien VMware"

Déploiement de la solution

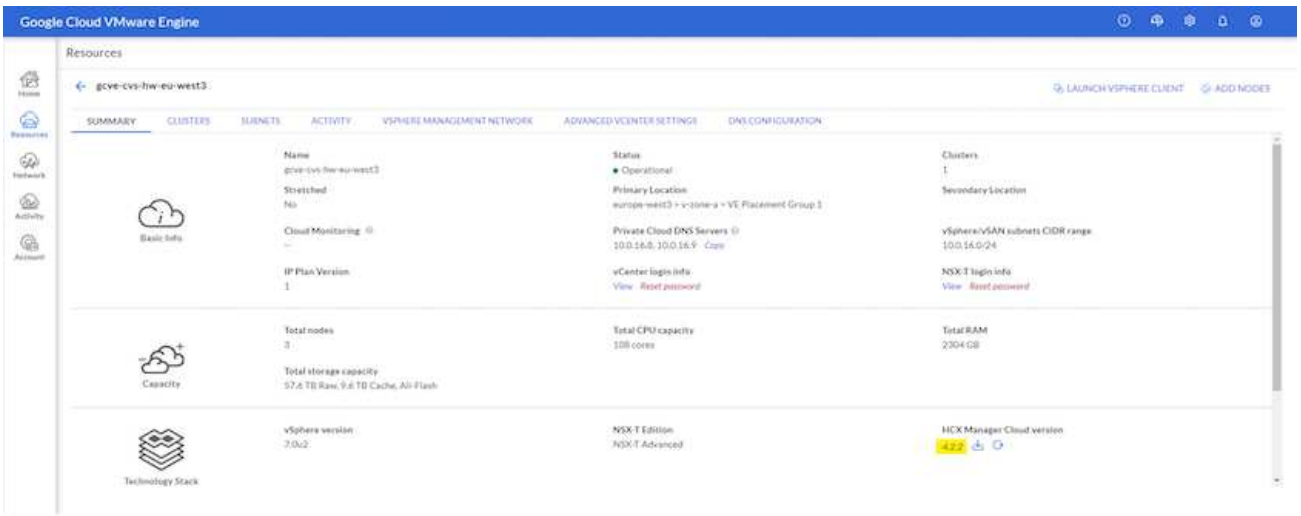
Suivez la série d'étapes pour terminer le déploiement de cette solution :

▼ **Étape 1 : Préparez HCX via le portail Google VMware Engine**

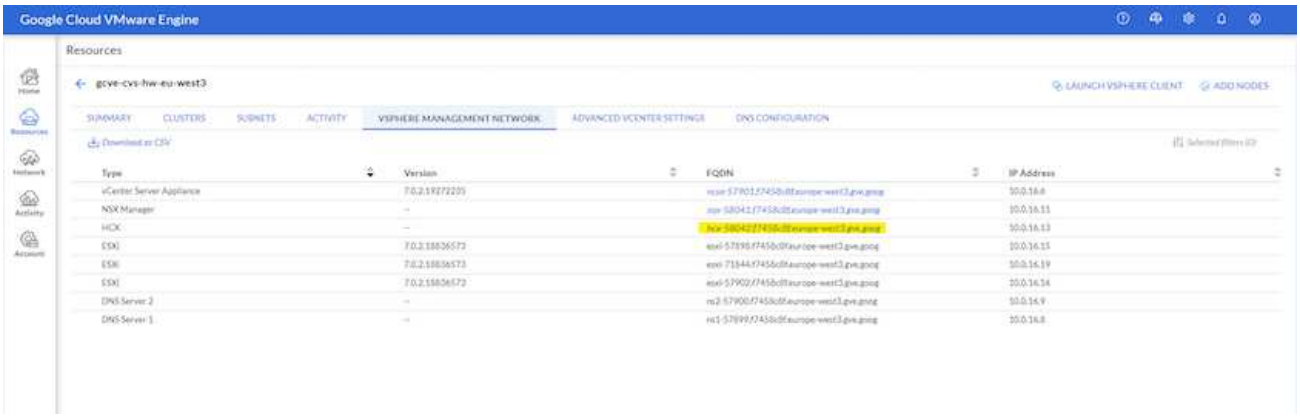
Le composant HCX Cloud Manager est automatiquement installé lorsque vous provisionnez un cloud privé avec VMware Engine. Pour préparer l'appariement de sites, procédez comme suit :

1. Connectez-vous au portail Google VMware Engine et connectez-vous à HCX Cloud Manager.

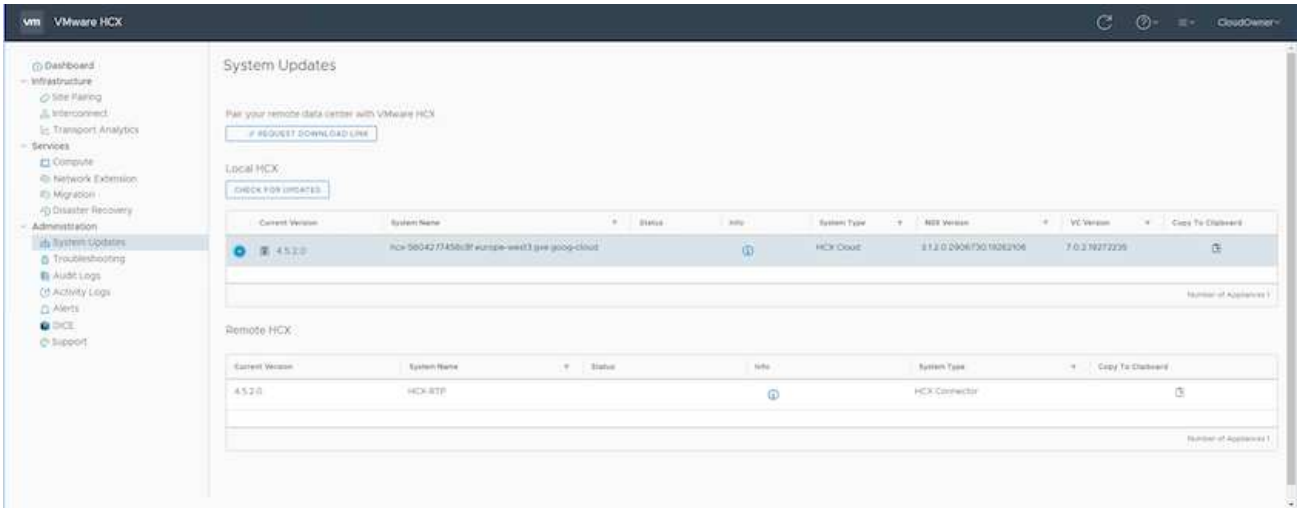
   Vous pouvez vous connecter à la console HCX en cliquant sur le lien de la version HCX



   ou en cliquant sur HCX FQDN sous l'onglet Réseau de gestion vSphere.



2. Dans HCX Cloud Manager, accédez à **Administration > Mises à jour système**.
3. Cliquez sur **Demander un lien de téléchargement** et téléchargez le fichier OVA.



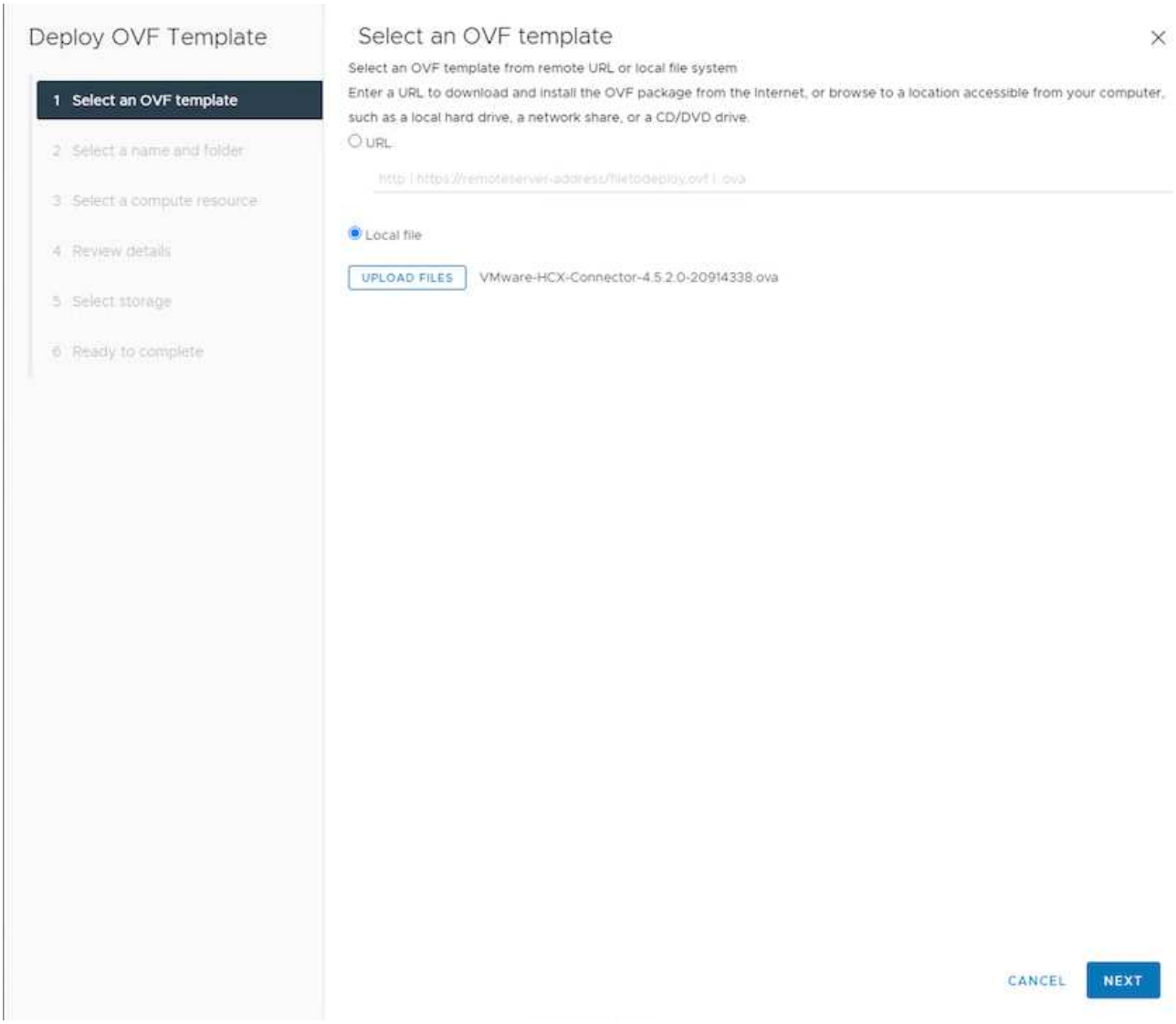
4. Mettez à jour HCX Cloud Manager vers la dernière version disponible à partir de l'interface utilisateur de HCX Cloud Manager.

▼ **Étape 2 : Déployer le programme d'installation OVA sur le serveur vCenter local**

Pour que le connecteur sur site se connecte au gestionnaire HCX dans Google Cloud VMware Engine, assurez-vous que les ports de pare-feu appropriés sont ouverts dans l'environnement sur site.

Pour télécharger et installer HCX Connector sur le serveur vCenter local, 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 l'OVA téléchargé, déployez-le sur l'environnement VMware vSphere local à l'aide de l'option **Déployer le modèle OVF**.



3. Saisissez toutes les informations requises pour le déploiement OVA, cliquez sur **Suivant**, puis sur **Terminer** pour déployer le connecteur VMware HCX OVA.

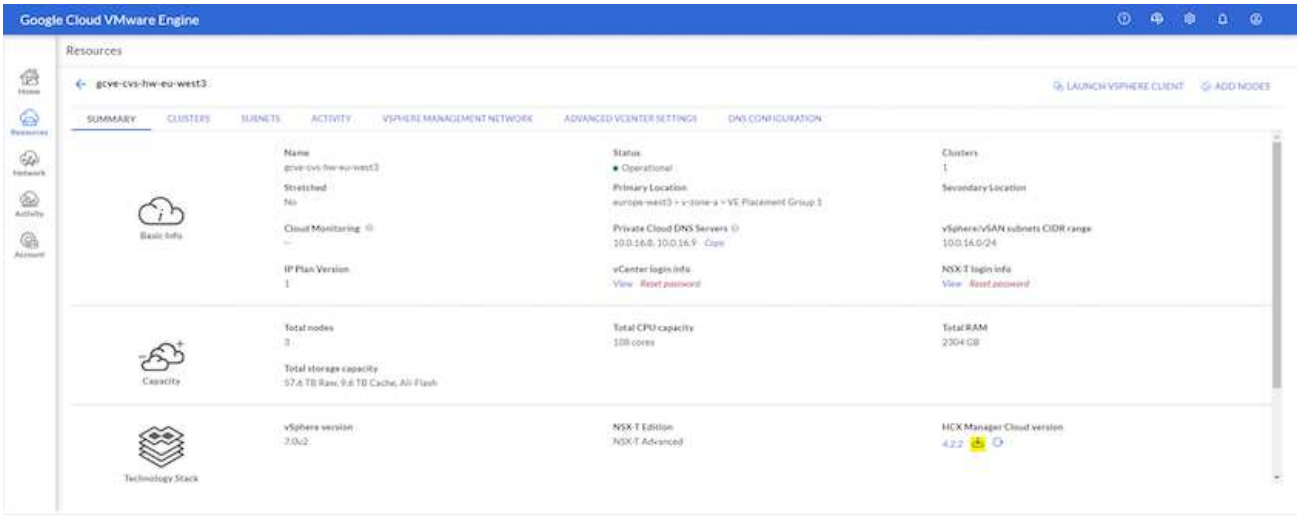
   Mettez sous tension l'appliance virtuelle manuellement.

Pour des instructions étape par étape, consultez le "Documentation Google HCX" .

▼ **Étape 3 : Activer HCX Connector avec la clé de licence**

Après avoir déployé VMware HCX Connector OVA sur site et démarré l'appliance, procédez comme suit pour activer HCX Connector. Générez la clé de licence à partir du portail Google Cloud VMware Engine et activez-la dans VMware HCX Manager.

1. Depuis 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"` en utilisant les informations d'identification de l'administrateur.

   Utilisez l'adresse IP et le mot de passe hcxmanager définis lors du déploiement OVA.

3. Dans la licence, entrez la clé copiée à l'étape 3 et cliquez sur **Activer**.

   Le connecteur HCX sur site doit avoir accès à Internet.

4. Sous **Emplacement du centre de données**, indiquez l'emplacement le plus proche pour l'installation de VMware HCX Manager sur site. Cliquez sur **Continuer**.
5. Sous **Nom du système**, mettez à jour le nom et cliquez sur **Continuer**.
6. Cliquez sur **Oui, continuer**.
7. Sous **Connectez votre 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**.

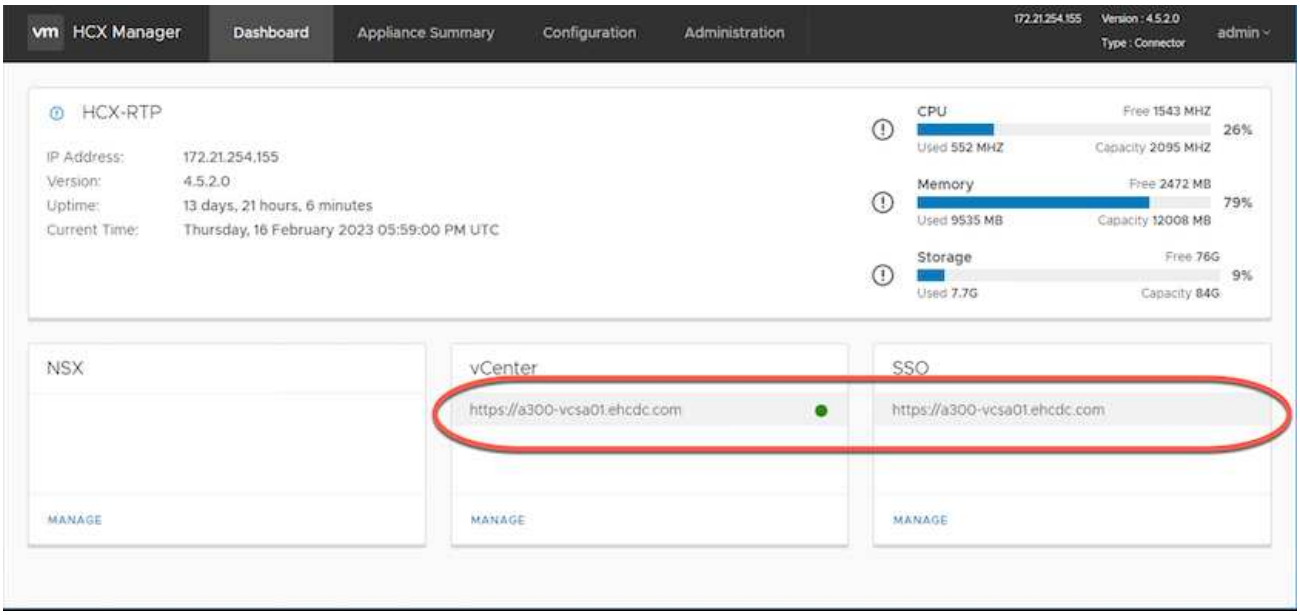
   Utilisez le FQDN pour éviter les problèmes de connectivité ultérieurs.

8. Sous **Configurer SSO/PSC**, indiquez le nom de domaine complet ou l'adresse IP du Platform Services Controller (PSC) et cliquez sur **Continuer**.

   Pour PSC intégré, saisissez le nom de domaine complet ou l'adresse IP de VMware vCenter Server.

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 tous deux disposer des paramètres de configuration appropriés, qui doivent être identiques à ceux de la page précédente.

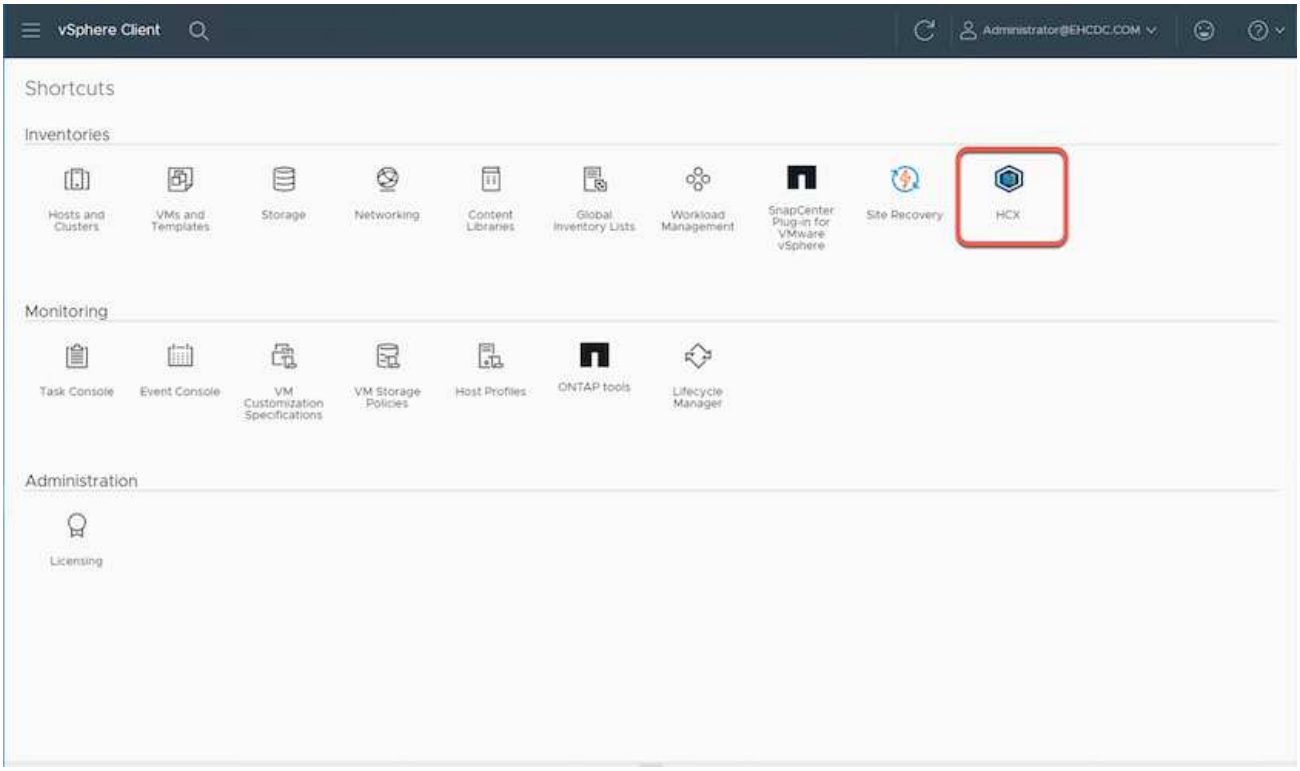
    Ce processus devrait prendre environ 10 à 20 minutes pour que le plug-in soit ajouté au serveur vCenter.



▼ Étape 4 : Associez le connecteur VMware HCX sur site à Google Cloud VMware Engine HCX Cloud Manager

Une fois HCX Connector déployé et configuré sur vCenter local, établissez une connexion à Cloud Manager en ajoutant le couplage. Pour configurer l'appairage des sites, procédez comme suit :

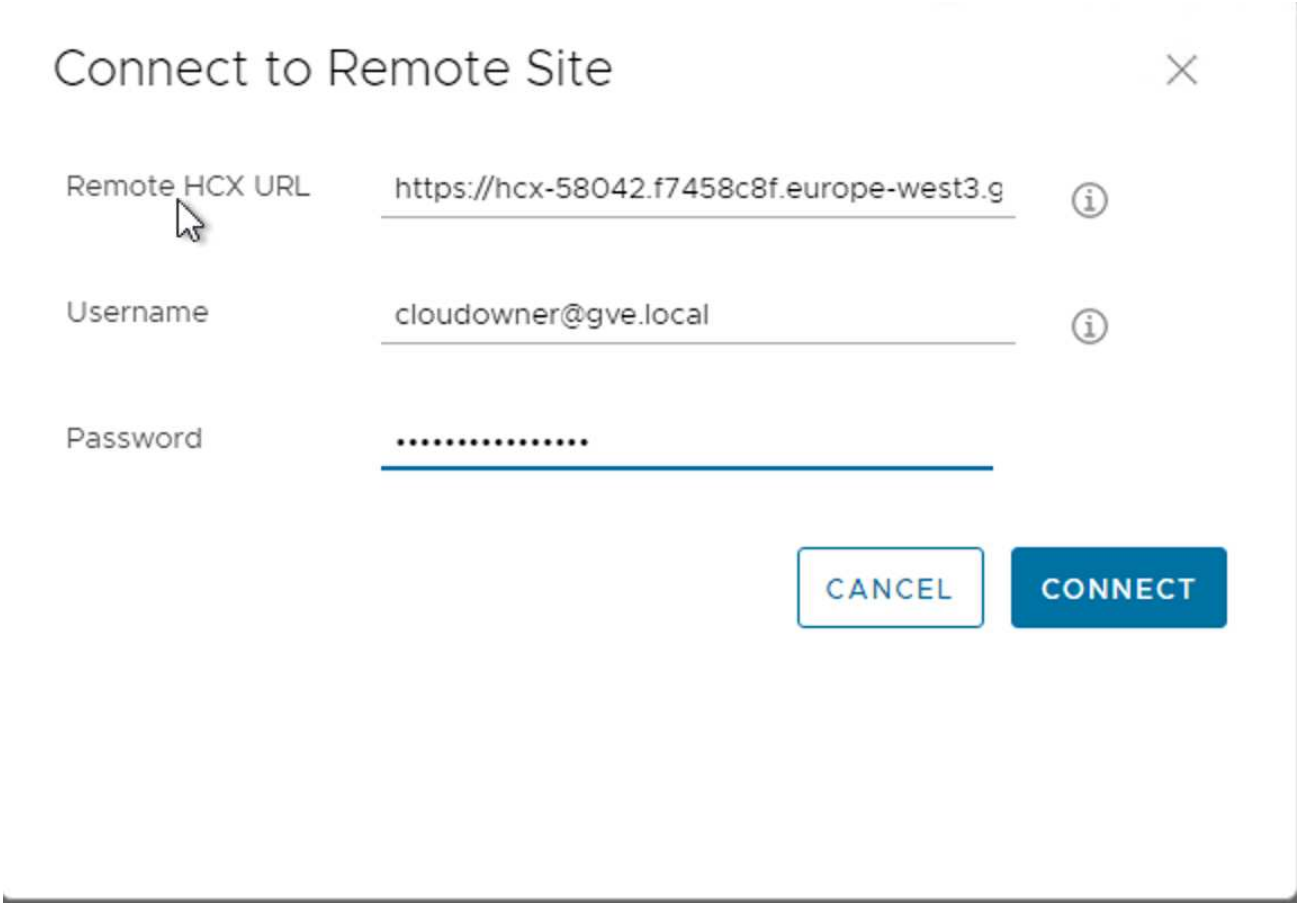
1. Pour créer une paire de sites entre l'environnement vCenter sur site et Google Cloud VMware Engine SDDC, connectez-vous au serveur vCenter sur site et accédez au nouveau plug-in HCX vSphere Web Client.



2. Sous Infrastructure, cliquez sur **Ajouter un appariement de sites**.

Saisissez l'URL ou l'adresse IP de Google Cloud VMware Engine HCX Cloud Manager et

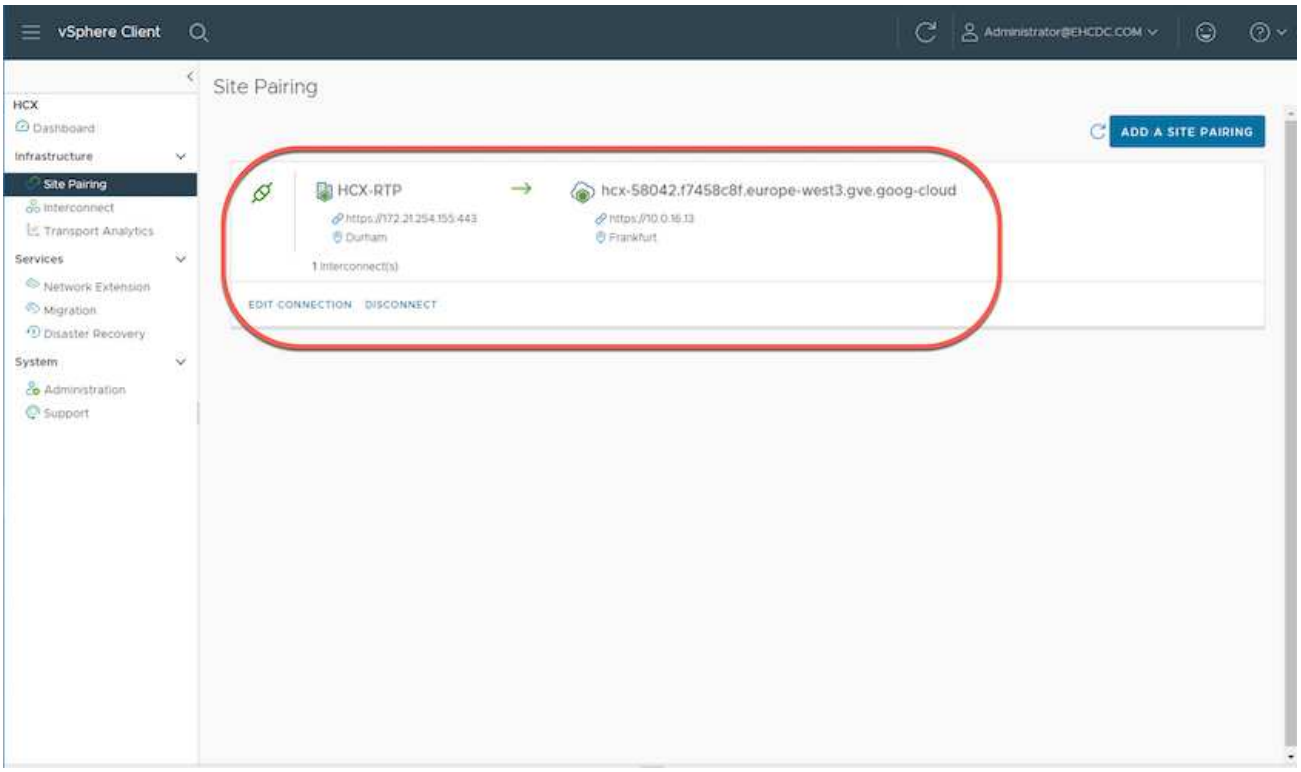
les informations d'identification de l'utilisateur disposant des privilèges Cloud-Owner-Role pour accéder au cloud privé.



3. Cliquez sur **Connecter**.

VMware HCX Connector doit pouvoir acheminer vers l'adresse IP de HCX Cloud Manager via le port 443.

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

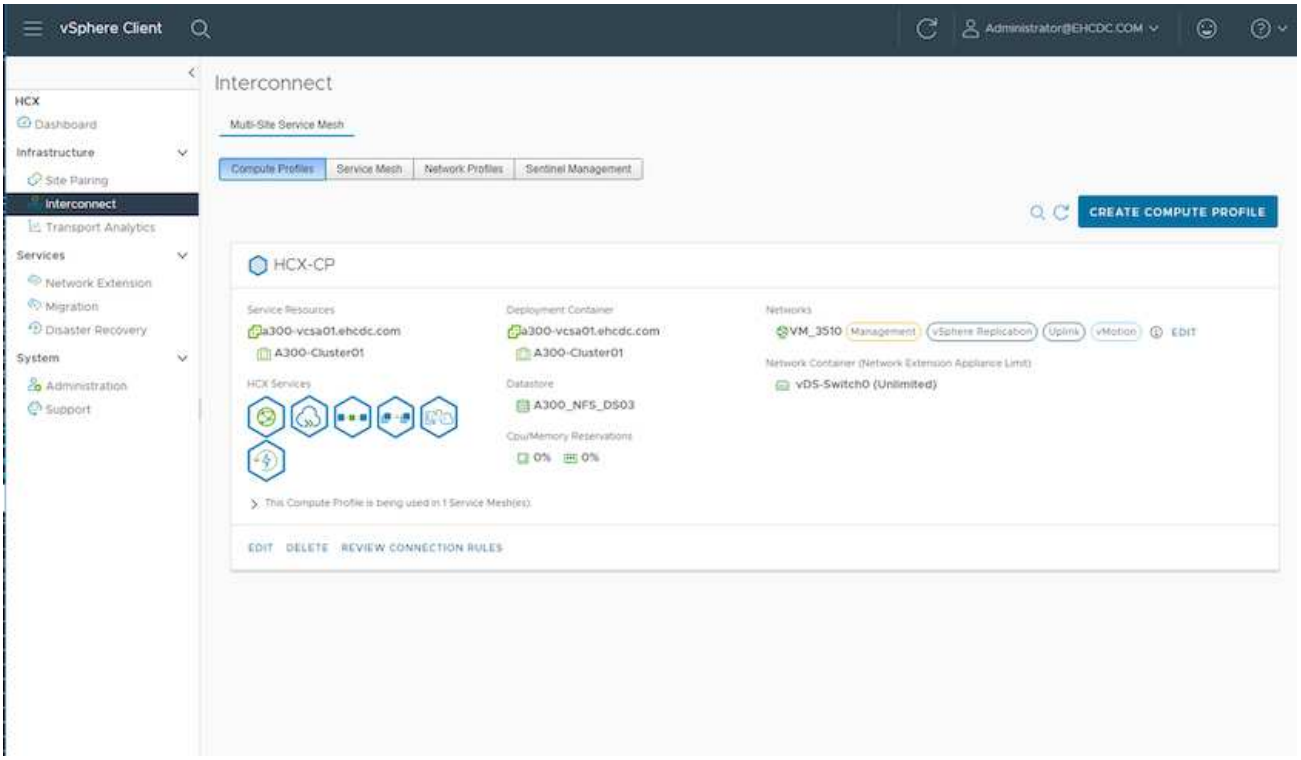


▼ **Étape 5 : Configurer le profil réseau, le profil de calcul et le maillage de services**

L'appliance de service VMware HCX Interconnect fournit des fonctionnalités de réplication et de migration basées sur vMotion via Internet et des connexions privées vers le site cible. L'interconnexion fournit le cryptage, l'ingénierie du trafic et la mobilité des machines virtuelles. Pour créer un dispositif de service d'interconnexion, procédez comme suit :

1. Sous Infrastructure, sélectionnez **Interconnexion > Maillage de services multisites > Profils de calcul > Créer un profil de calcul**.

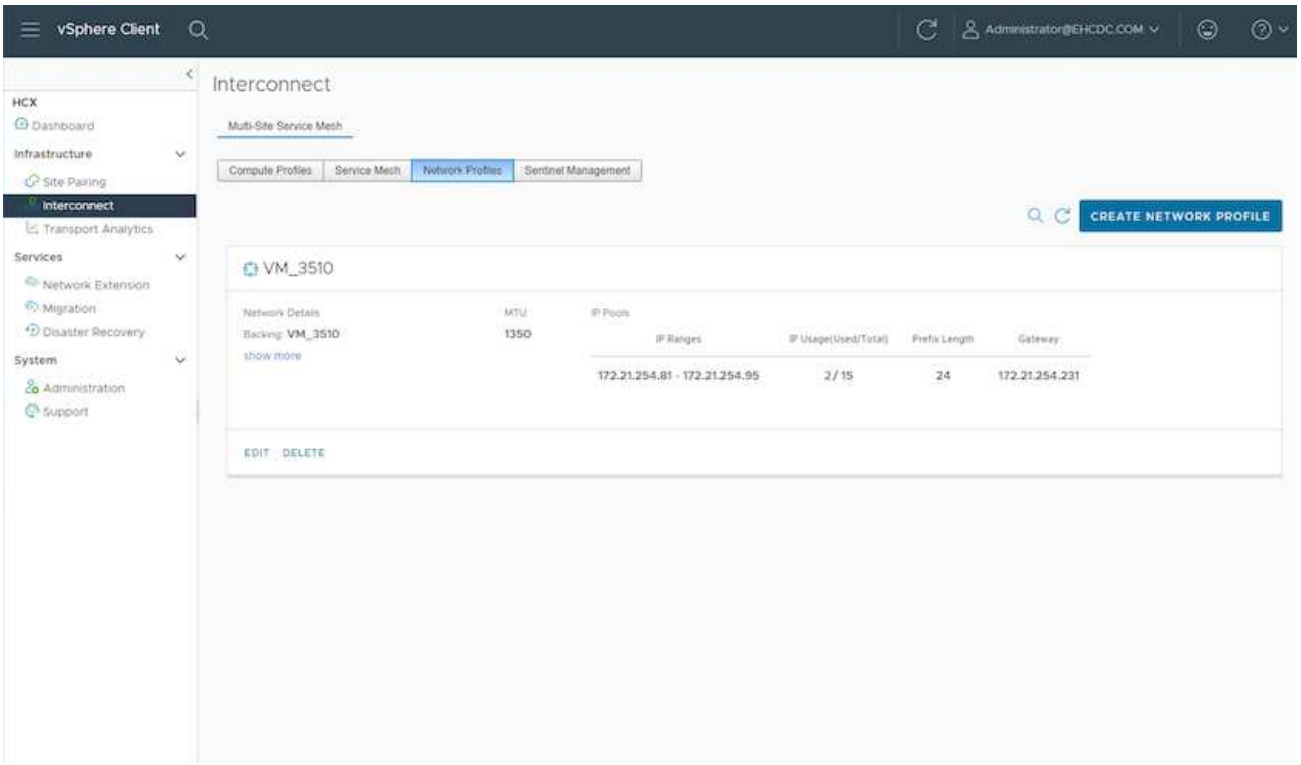
Les profils de calcul définissent les paramètres de déploiement, y compris les appliances déployées et la partie du centre de données VMware accessible au service HCX.



2. Une fois le profil de calcul créé, créez les profils réseau en sélectionnant **Multi-Site Service Mesh > Profils réseau > Créer un profil réseau**.

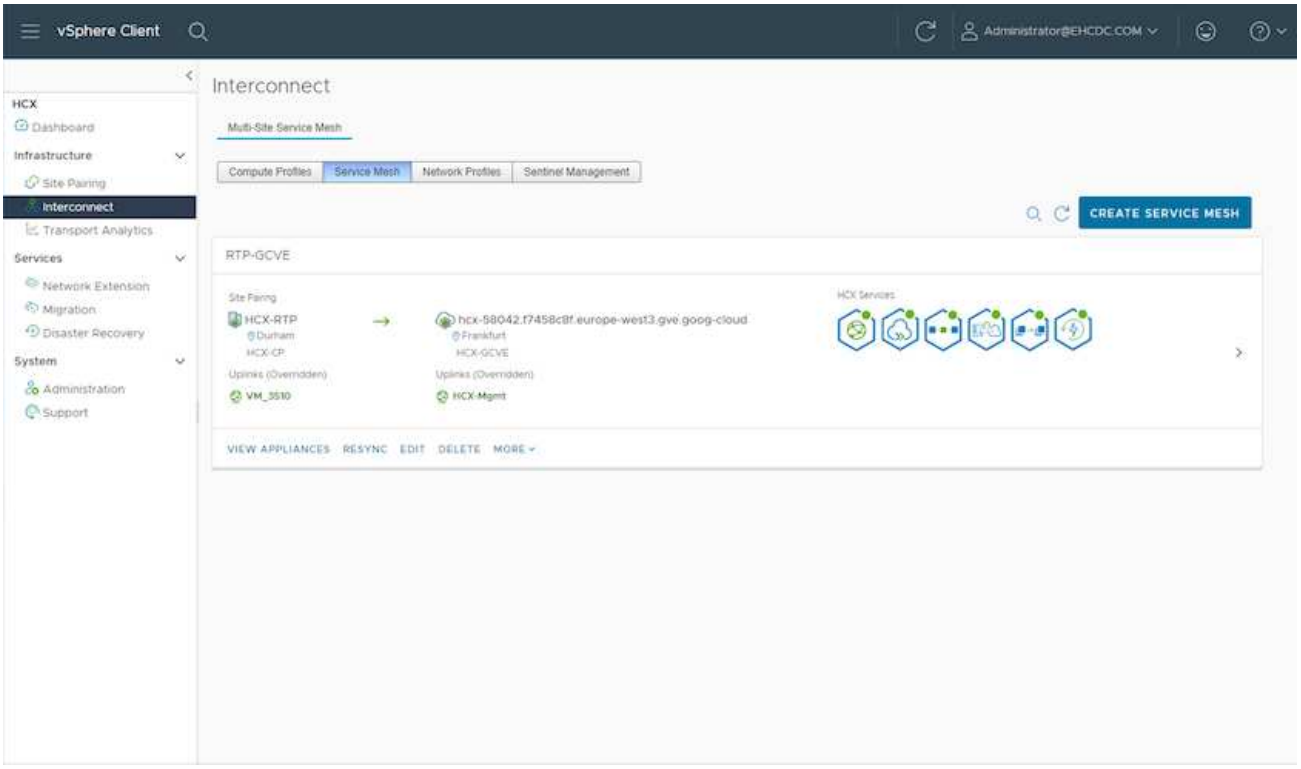
   Le profil réseau définit une plage d'adresses IP et de réseaux utilisés par HCX pour ses appliances virtuelles.

   > Cette étape nécessite deux adresses IP ou plus. Ces adresses IP sont attribuées par le réseau de gestion aux appareils d'interconnexion.

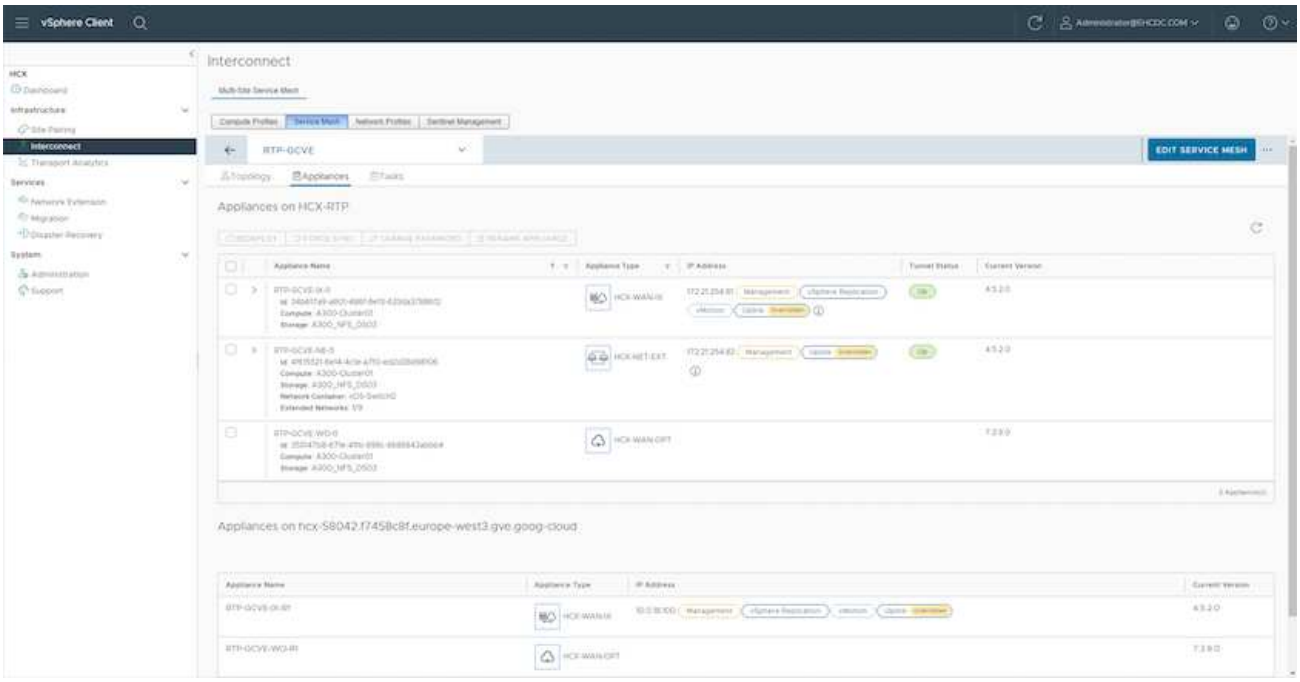


3. À ce stade, les profils de calcul et de réseau ont été créés avec succès.
4. Créez le Service Mesh en sélectionnant l'onglet **Service Mesh** dans l'option **Interconnexion** et sélectionnez les sites SDDC sur site et GCVE.
5. Le Service Mesh spécifie une paire de profils de calcul et de réseau locaux et distants.

> 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. C'est l'étape finale de la configuration. Cela devrait prendre près de 30 minutes pour terminer le déploiement. Une fois le maillage de services configuré, l'environnement est prêt avec les tunnels IPsec créés avec succès pour migrer les machines virtuelles de charge de travail.



▼ **Étape 6 : Migrer les charges de travail**

Les charges de travail peuvent être migrées de manière bidirectionnelle entre les SDDC locaux et GCVE à l'aide de diverses 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 masse HCX, HCX vMotion, la migration à froid HCX, HCX Replication Assisted vMotion (disponible avec l'édition HCX Enterprise) et la migration assistée par le système d'exploitation HCX (disponible avec l'édition HCX Enterprise).

Pour en savoir plus sur les différents mécanismes de migration HCX, consultez "Migration de machines virtuelles VMware à l'aide de la documentation VMware HCX" .

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

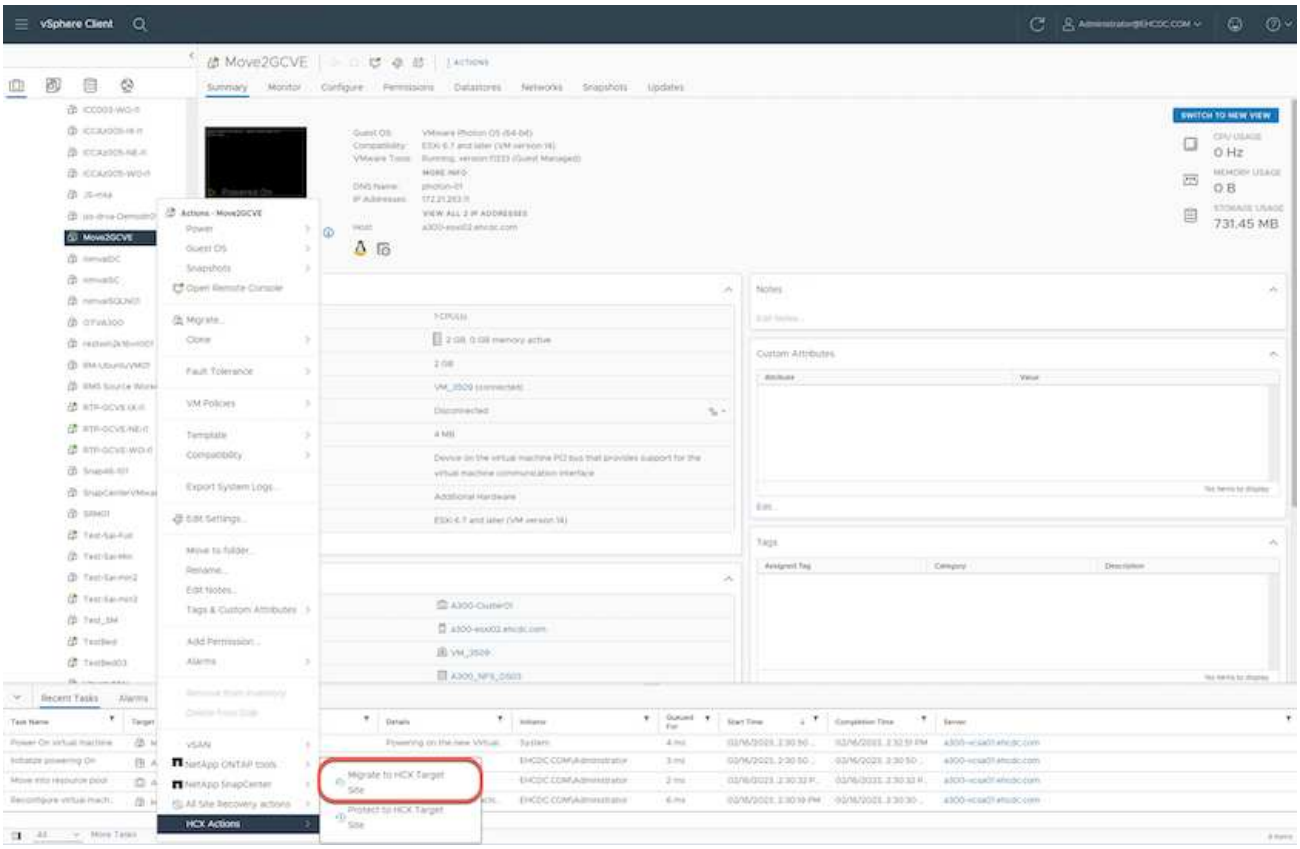
> ⓘ L'appliance HCX-IX ajoute le service Mobility Agent en tant qu'objet hôte dans vCenter Server. Les ressources de processeur, de mémoire, de stockage et de réseau affichées sur cet objet ne représentent pas la consommation réelle sur l'hyperviseur physique hébergeant l'appliance IX.

HCX vMotion

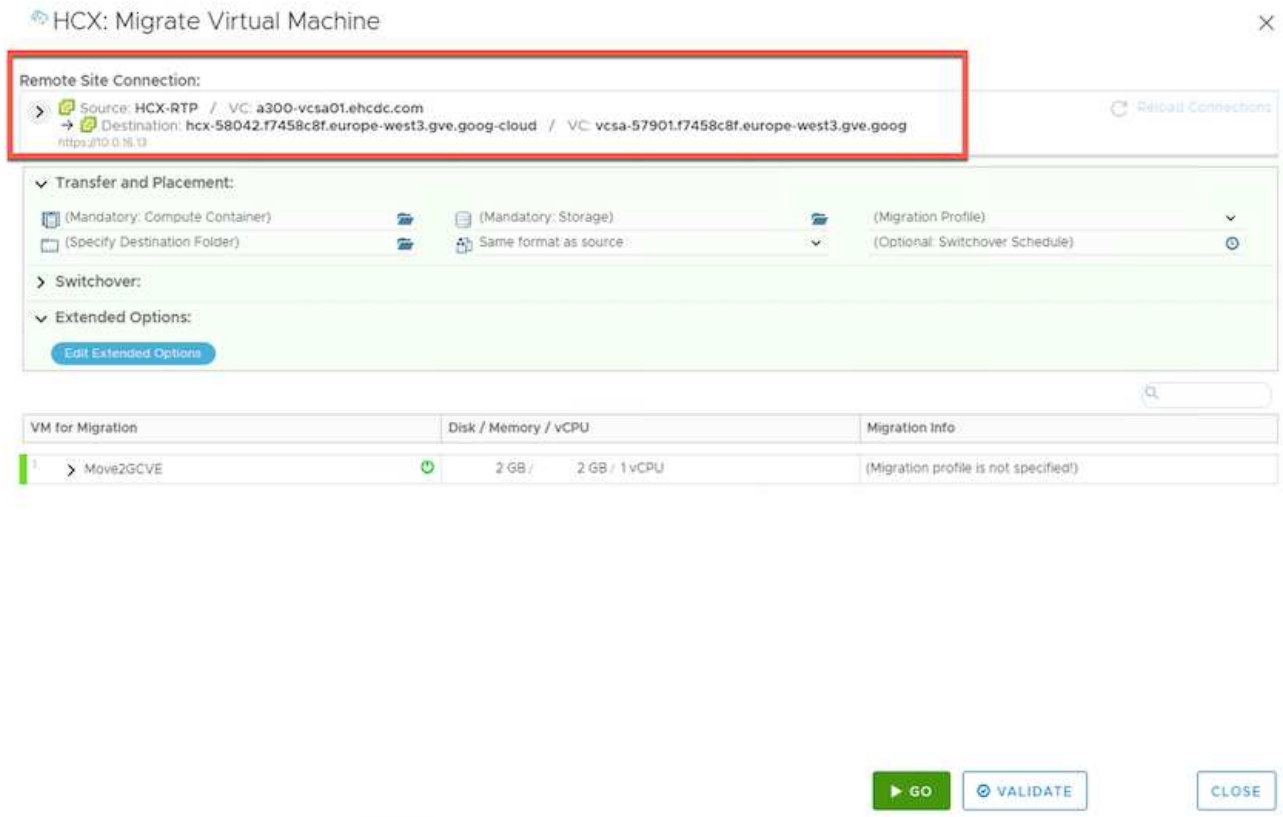
Cette section décrit le mécanisme HCX vMotion. Cette technologie de migration utilise le protocole VMware vMotion pour migrer une machine virtuelle vers GCVE. L'option de migration vMotion est utilisée pour migrer l'état de la machine virtuelle d'une seule machine virtuelle à la fois. Il n'y a aucune interruption de service pendant cette méthode de migration.

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

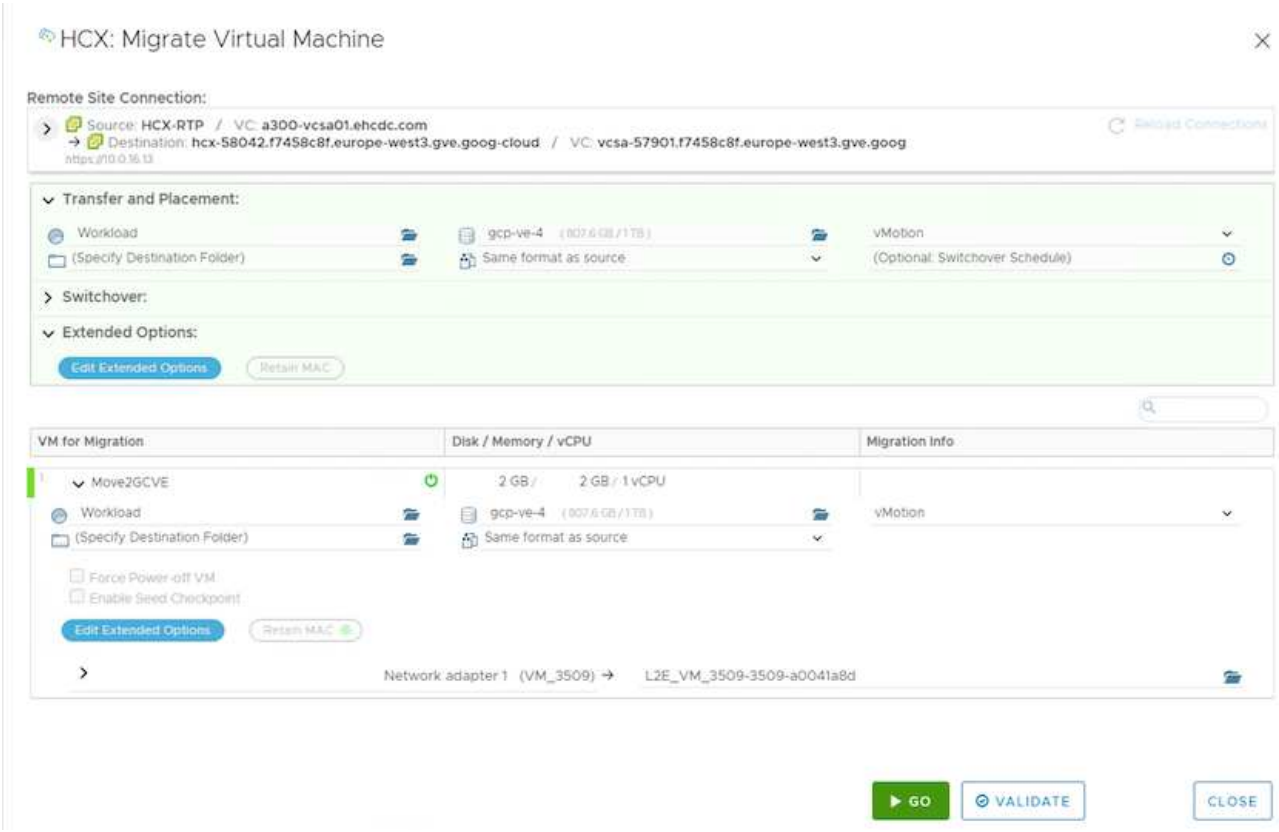
1. À partir du client vSphere sur site, accédez à Inventaire, cliquez avec le bouton droit sur la machine virtuelle à migrer et sélectionnez Actions HCX > Migrer vers le site cible HCX.



2. Dans l'assistant Migrer la machine virtuelle, sélectionnez la connexion au site distant (cible GCVE).



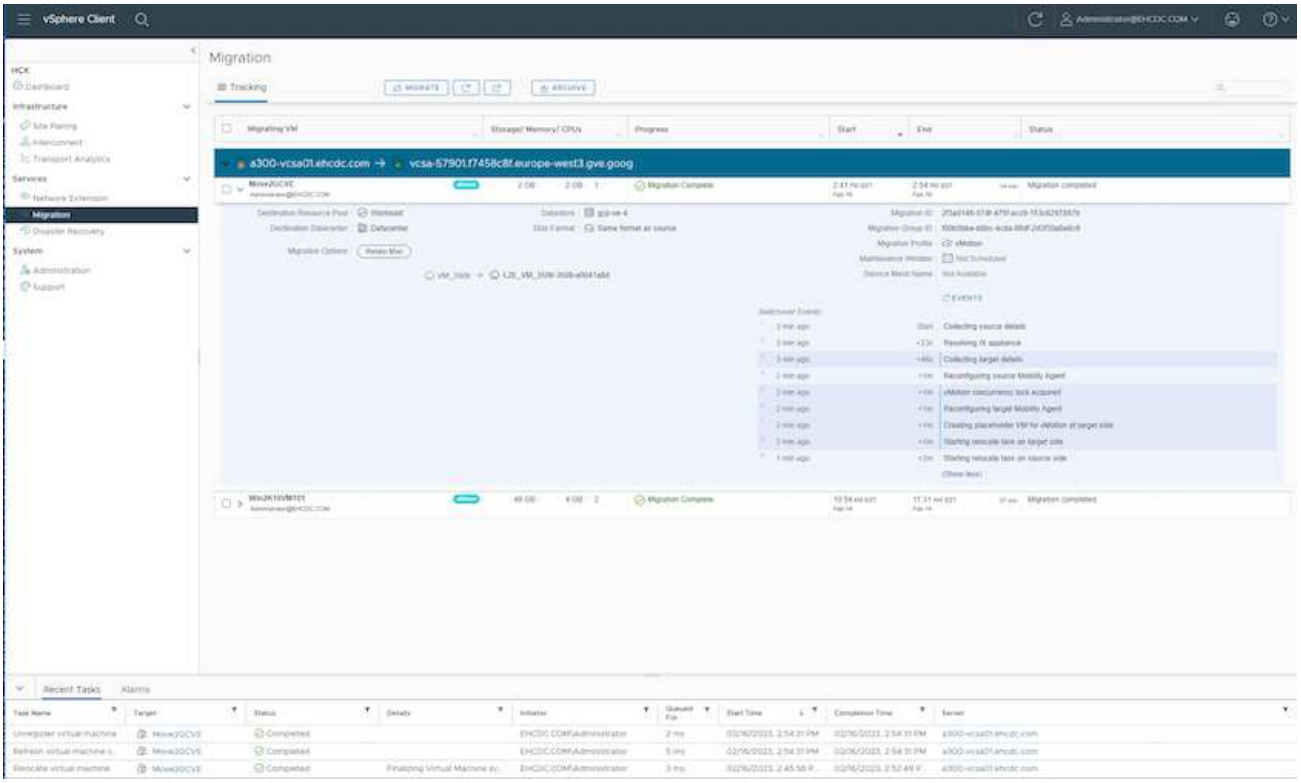
3. Mettez à jour les champs obligatoires (Cluster, Stockage et Réseau de destination), cliquez sur Valider.



4. Une fois les vérifications de validation terminées, cliquez sur Aller 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 limitations de HCX vMotion, consultez "Comprendre VMware HCX vMotion et la migration à froid" .

5. Vous pouvez surveiller la progression et l'achèvement du vMotion à partir du tableau de bord HCX > Migration.



Le magasin de données NFS cible Google Cloud NetApp Volumes (NetApp Volumes) doit disposer de suffisamment d'espace pour gérer la migration.

Conclusion

Que vous cibliez un cloud entièrement ou un cloud hybride et que vos données résident sur n'importe quel type/fournisseur de stockage sur site, Cloud Volume Service et HCX offrent d'excellentes options pour déployer et migrer les charges de travail des applications tout en réduisant le coût total de possession en rendant les exigences de données transparentes pour la couche applicative. Quel que soit le cas d'utilisation, choisissez Google Cloud VMware Engine avec Cloud Volume Service pour une réalisation rapide des avantages du cloud, une infrastructure et des opérations cohérentes sur site et sur plusieurs clouds, une portabilité bidirectionnelle des charges de travail et une capacité et des performances de niveau entreprise. Il s'agit du même processus et des mêmes procédures familiers utilisés 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).

Plats à emporter

Les points clés de ce document comprennent :

- Vous pouvez désormais utiliser Cloud Volume Service comme banque de données sur Google Cloud VMware Engine SDDC.
- Vous pouvez facilement migrer des données depuis un emplacement local vers une banque de données Cloud Volume Service.
- Vous pouvez facilement développer et réduire la banque de données Cloud Volume Service pour répondre aux exigences de capacité et de performances pendant l'activité de migration.

Vidéos de Google et VMware pour référence

▼ **De Google**

- "Déployer le connecteur HCX avec GCVE"
- "Configurer HCX ServiceMesh avec GCVE"
- "Migrer une machine virtuelle avec HCX vers GCVE"

▼ **De VMware**

- "Déploiement du connecteur HCX pour GCVE"
- "Configuration de HCX ServiceMesh pour GCVE"
- "Migration de la charge de travail HCX vers GCVE"

Où trouver des informations supplémentaires

Pour en savoir plus sur les informations décrites dans ce document, reportez-vous aux liens Web suivants :

- Documentation de Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentation de Cloud Volume Service

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Guide de l'utilisateur de VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

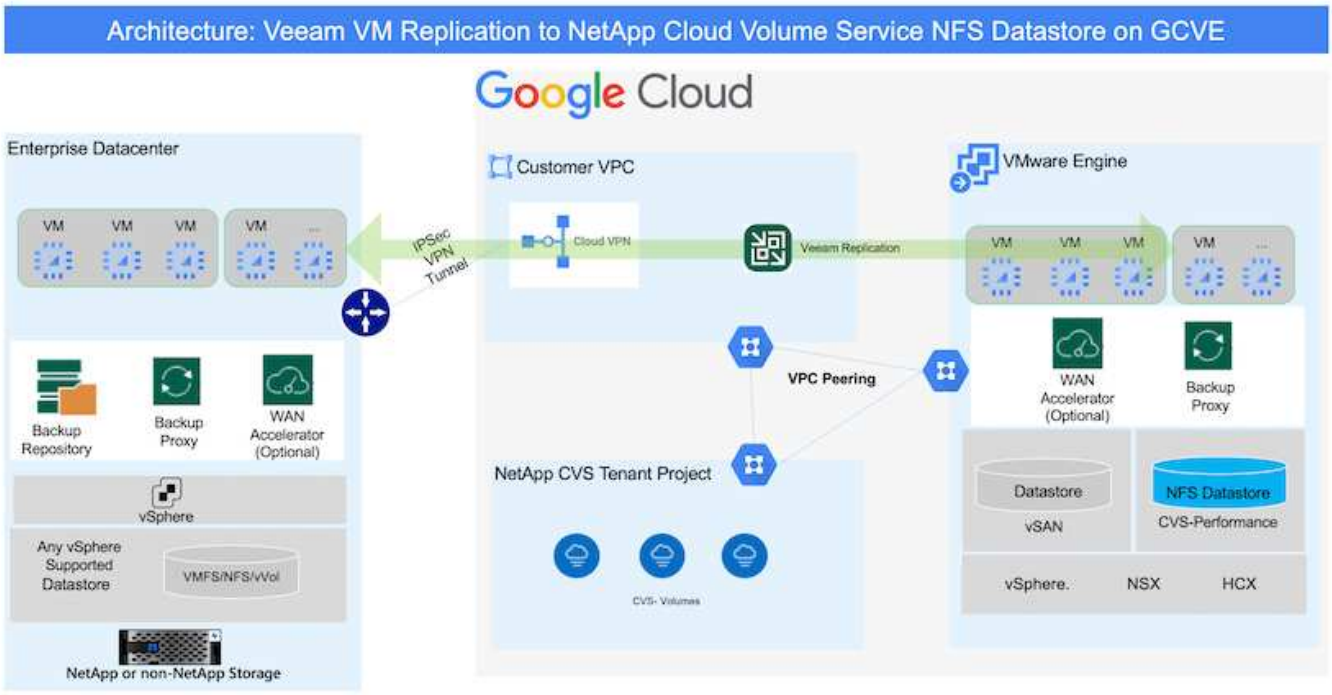
Migration de machines virtuelles vers Google Cloud NetApp Volumes NFS Datastore sur Google Cloud VMware Engine à l'aide de la fonctionnalité de réplication Veeam

Les clients qui utilisent actuellement Veeam pour leurs besoins de protection des données continuent d'utiliser cette solution pour migrer les charges de travail vers GCVE et profiter des avantages des magasins de données NFS Google Cloud NetApp Volumes .

Aperçu

Les charges de travail VM exécutées sur VMware vSphere peuvent être migrées vers Google Cloud VMware Engine (GCVE) à l'aide de la fonctionnalité de réplication Veeam.

Ce document fournit une approche étape par étape pour configurer et effectuer une migration de machine virtuelle qui utilise Google Cloud NetApp Volumes, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document suppose que vous disposez de Google Cloud VPN, de Cloud Interconnect ou d'une autre option de mise en réseau pour établir une connectivité réseau entre les serveurs vSphere existants et Google Cloud VMware Engine.

> Il existe plusieurs options pour connecter les centres de données sur site à Google Cloud, ce qui nous empêche de décrire un flux de travail spécifique dans ce document. Se référer à la"Documentation Google Cloud" pour la méthode de connectivité appropriée entre les locaux et Google.

Déploiement de la solution de migration

Présentation du déploiement de la solution

1. Assurez-vous que le magasin de données NFS de Google Cloud NetApp Volumes est monté sur GCVE vCenter.
2. Assurez-vous que Veeam Backup Recovery est déployé sur l'environnement VMware vSphere existant
3. Créez une tâche de réplication pour démarrer la réplication des machines virtuelles vers l'instance Google Cloud VMware Engine.
4. Effectuer le basculement de la tâche de réplication Veeam.
5. Effectuer un basculement permanent sur Veeam.

Détails du déploiement

Assurez-vous que la banque de données NFS de Google Cloud NetApp Volumes est montée sur GCVE vCenter

Connectez-vous à GCVE vCenter et assurez-vous qu'une banque de données NFS avec suffisamment d'espace est disponible. Si ce n'est pas le cas, veuillez vous référer"Monter les volumes NetApp en tant que

banque de données NFS sur GCVE"

Assurez-vous que Veeam Backup Recovery est déployé sur l'environnement VMware vSphere existant

Veuillez vous référer"Composants de réplication Veeam" documentation pour installer les composants requis.

Créez une tâche de réplication pour démarrer la réplication des machines virtuelles vers l'instance Google Cloud VMware Engine.

Le vCenter sur site et le vCenter GCVE doivent tous deux être enregistrés auprès de Veeam. "Configurer la tâche de réplication de machine virtuelle vSphere" Voici une vidéo expliquant comment faire"Configurer la tâche de réplication" .

> La machine virtuelle répliquée peut avoir une adresse IP différente de la machine virtuelle source et peut également être connectée à un groupe de ports différent. Pour plus de détails, regardez la vidéo ci-dessus.

Effectuer le basculement du travail de réplication Veeam

Pour migrer des machines virtuelles, effectuez"Effectuer un basculement"

Effectuer un basculement permanent sur Veeam.

Pour traiter GCVE comme votre nouvel environnement source, effectuez"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 des machines virtuelles sur le site cible.
- Permet de remapper les données existantes répliquées en dehors de Veeam (comme les données répliquées du système NetApp)
- A la capacité de spécifier différents groupes de ports réseau sur le site cible.
- Peut spécifier l'ordre des machines virtuelles à mettre sous tension.
- Utilise VMware Change Block Tracking pour minimiser la quantité de données à envoyer sur le WAN.
- Capacité à exécuter des scripts pré et post pour la réplication.
- Capacité à exécuter des scripts pré et post pour les instantanés.

Sécurisez vos données avec Google Cloud NetApp Volumes dans Google Cloud

TR-4918 : Présentation de la sécurité – Google Cloud NetApp Volumes dans Google Cloud

Oliver Krause, Justin Parisi, NetApp

La sécurité, notamment dans le cloud où l'infrastructure échappe au contrôle des administrateurs du stockage, est primordiale pour vous permettre de confier vos données aux offres de services proposées par les fournisseurs de cloud. Ce document présente un aperçu des offres de sécurité qui "Google Cloud NetApp Volumes est fourni dans Google Cloud".

Public visé

Le public visé par ce document comprend, sans s'y limiter, les rôles suivants :

- Fournisseurs de cloud
- Administrateurs de stockage
- Architectes de stockage
- Ressources sur le terrain
- Les décideurs d'entreprise

Si vous avez des questions sur le contenu de ce rapport technique, consultez la section"Contactez-nous."

Abréviation	Définition
NetApp Volumes-SW	Google Cloud NetApp Volumes, type de service NetApp Volumes
NetApp Volumes-Performances	Service Cloud Volume, type de service NetApp Volumes-Performances
PSA	

Comment Google Cloud NetApp Volumes dans Google Cloud sécurise vos données

Google Cloud NetApp Volumes dans Google Cloud offre une multitude de moyens pour sécuriser nativement vos données.

Architecture sécurisée et modèle de location

Google Cloud NetApp Volumes fournit une architecture sécurisée dans Google Cloud en segmentant la gestion des services (plan de contrôle) et l'accès aux données (plan de données) sur différents points de terminaison afin qu'aucun des deux ne puisse avoir d'impact sur l'autre (voir la section"Architecture de Google Cloud NetApp Volumes"). Il utilise Google "accès aux services privés" (PSA) cadre pour fournir le service. Ce cadre fait la distinction entre 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, hébergeant les clients qui souhaitent accéder aux partages de fichiers Google Cloud NetApp Volumes .

Dans cette architecture, les locataires (voir la section"Modèle de location") sont définis comme des projets Google Cloud qui sont complètement isolés les uns des autres, sauf s'ils sont explicitement connectés par l'utilisateur. Les locataires permettent une isolation complète des volumes de données, des services de noms externes et d'autres éléments essentiels de la solution des autres locataires à l'aide de la plate-forme de volumes Google Cloud NetApp Volumes . Étant donné que la plate-forme Google Cloud NetApp Volumes est connectée via le peering VPC, cette isolation s'applique également à elle. Vous pouvez activer le partage des volumes Google Cloud NetApp Volumes entre plusieurs projets en utilisant un VPC partagé (voir la section"VPC partagés"). Vous pouvez appliquer des contrôles d'accès aux partages SMB et aux exportations NFS pour limiter qui ou quoi peut afficher ou modifier les ensembles de données.

Gestion des identités renforcée pour le plan de contrôle

Dans le plan de contrôle où la configuration de Google Cloud NetApp Volumes a lieu, la gestion des identités est gérée à l'aide de "Gestion des accès aux identités (IAM)" . IAM est un service standard qui vous permet de contrôler l'authentification (connexions) et l'autorisation (autorisations) des instances de projet Google Cloud. Toute la configuration est effectuée avec les API Google Cloud NetApp Volumes via un transport HTTPS sécurisé utilisant le cryptage TLS 1.2, et l'authentification est effectuée à l'aide de jetons JWT pour plus de

sécurité. L'interface utilisateur de la console Google pour Google Cloud NetApp Volumes traduit les entrées utilisateur en appels d'API Google Cloud NetApp Volumes .

Renforcement de la sécurité - Limitation des surfaces d'attaque

Une partie de la sécurité efficace consiste à limiter le nombre de surfaces d'attaque disponibles dans un service. Les surfaces d'attaque peuvent inclure une variété d'éléments, notamment les données au repos, les transferts en cours, les connexions et les ensembles de données eux-mêmes.

Un service géré supprime certaines des surfaces d'attaque inhérentes à sa conception. Gestion des infrastructures, telle que décrite dans la section"Opération de service," est géré par une équipe dédiée et est automatisé pour réduire le nombre de fois qu'un humain touche réellement les configurations, ce qui contribue à réduire le nombre d'erreurs intentionnelles et non intentionnelles. Le réseau est clôturé 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 l'attention des administrateurs de Google Cloud NetApp Volumes en matière de sécurité. En cachant la majeure partie de la gestion derrière une interface API, la sécurité est obtenue en limitant les surfaces d'attaque.

Modèle Zero Trust

Historiquement, la philosophie de la sécurité informatique a consisté à faire confiance mais à vérifier, et s'est manifestée en s'appuyant uniquement sur des mécanismes externes (tels que les pare-feu et les 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 fournissent la vérification pour entrer dans les réseaux et faire des ravages.

Zero Trust est devenu une nouvelle méthodologie en matière de sécurité, le mantra actuel étant « ne faire confiance à rien tout en vérifiant tout ». Par conséquent, rien n'est autorisé à accéder par défaut. Ce mantra est appliqué de diverses manières, notamment par des pare-feu standard et des systèmes de détection d'intrusion (IDS), ainsi qu'avec les méthodes suivantes :

- Méthodes d'authentification fortes (telles que les jetons Kerberos ou JWT cryptés AES)
- Sources uniques et solides d'identités (telles que Windows Active Directory, Lightweight Directory Access Protocol (LDAP) et Google IAM)
- Segmentation du réseau et multi-location sécurisée (seuls les locataires sont autorisés à accéder par défaut)
- Contrôles d'accès granulaires avec politiques d'accès au moindre privilège
- Petites listes exclusives d'administrateurs dévoués et de confiance avec audit numérique et pistes papier

Google Cloud NetApp Volumes exécuté dans Google Cloud adhère au modèle Zero Trust en mettant en œuvre la position « ne faire confiance à rien, tout vérifier ».

Cryptage

Chiffrer les données au repos (voir la section"Cryptage des données au repos") en utilisant des chiffrements XTS-AES-256 avec NetApp Volume Encryption (NVE) et en vol avec"cryptage SMB" ou prise en charge NFS Kerberos 5p. Soyez rassuré en sachant que les transferts de réplication interrégionale sont protégés par le cryptage TLS 1.2 (voir le lien de section : gcp-gcnv-security-considerations.html#Détection, prévention et atténuation des ransomwares, malwares et virus#cross-region-replication["Réplication interrégionale"]). De plus, le réseau Google fournit également des communications cryptées (voir la section"Cryptage des données en transit") pour une couche de protection supplémentaire contre les attaques. Pour plus d'informations sur le cryptage des transports, consultez 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 nous remettons des attaques si elles se produisent. Cette stratégie comprend la protection des données et les sauvegardes. Google Cloud NetApp Volumes fournit des méthodes de réplication vers d'autres régions en cas de panne (voir la section"Réplication interrégionale") ou si un ensemble de données est affecté par une attaque de ransomware. Il peut également effectuer des sauvegardes asynchrones de données vers des emplacements extérieurs à l'instance Google Cloud NetApp Volumes en utilisant"Sauvegarde des Google Cloud NetApp Volumes" . Avec des sauvegardes régulières, l'atténuation des événements de sécurité peut prendre moins de temps et permettre aux administrateurs d'économiser de l'argent et de l'angoisse.

Atténuation rapide des ransomwares avec des copies Snapshot de pointe

Outre la protection des données et les sauvegardes, Google Cloud NetApp Volumes prend en charge les copies Snapshot immuables (voir la section"Copies instantanées immuables") de volumes permettant la récupération après des attaques de ransomware (voir la section"Opération de service") dans les secondes qui suivent la découverte du problème et avec une perturbation minimale. Le temps de récupération et les effets dépendent de la planification des instantanés, mais vous pouvez créer des copies d'instantanés qui fournissent des deltas d'une heure seulement dans les attaques de ransomware. Les copies instantanées ont un effet négligeable sur les performances et l'utilisation de la capacité et constituent une approche à faible risque et à haut rendement pour protéger vos ensembles de données.

Considérations de sécurité et surfaces d'attaque

La première étape pour comprendre comment sécuriser vos données consiste à identifier les risques et les surfaces d'attaque potentielles.

Il s'agit notamment (mais sans s'y limiter) des éléments suivants :

- Administration et connexions
- Données au repos
- Données en vol
- Réseau et pare-feu
- Ransomwares, logiciels malveillants et virus

Comprendre les surfaces d'attaque peut vous aider à mieux sécuriser vos environnements. Google Cloud NetApp Volumes dans Google Cloud prend déjà en compte bon nombre de ces sujets et implémente des fonctionnalités de sécurité par défaut, sans aucune interaction administrative.

Assurer des connexions sécurisées

Lors de la sécurisation de vos composants d'infrastructure critiques, il est impératif de vous assurer que seuls les utilisateurs approuvés peuvent se connecter et gérer vos environnements. Si des acteurs malveillants enfreignent vos informations d'identification administratives, ils disposent alors des clés du château et peuvent faire tout ce qu'ils veulent : modifier les configurations, supprimer des volumes et des sauvegardes, créer des portes dérobées ou désactiver les planifications de snapshots.

Google Cloud NetApp Volumes pour Google Cloud offre une protection contre les connexions administratives non autorisées grâce à l'obscurcissement du stockage en tant que service (StaaS). Google Cloud NetApp Volumes est entièrement géré par le fournisseur de cloud sans possibilité de connexion externe. Toutes les opérations d'installation et de configuration sont entièrement automatisées, de sorte qu'un administrateur humain n'a jamais besoin d'interagir avec les systèmes, sauf dans de très rares circonstances.

Si une connexion est requise, Google Cloud NetApp Volumes dans Google Cloud sécurise les connexions en conservant une très courte liste d'administrateurs de confiance ayant accès aux systèmes. Ce contrôle d'accès permet de réduire le nombre d'acteurs potentiellement malveillants disposant d'un accès. De plus, le réseau Google Cloud cache les systèmes derrière des couches de sécurité réseau et expose uniquement ce qui est nécessaire au monde extérieur. Pour plus d'informations sur l'architecture Google Cloud, Google Cloud NetApp Volumes , consultez la section"Architecture des Google Cloud NetApp Volumes ."

Administration et mises à niveau des clusters

Deux domaines présentant des risques de sécurité potentiels incluent l'administration des clusters (que se passe-t-il si un acteur malveillant a un accès administrateur) et les mises à niveau (que se passe-t-il si une image logicielle est compromise).

Protection de l'administration du stockage

Le stockage fourni en tant que service supprime le risque supplémentaire d'exposition des administrateurs en supprimant cet accès aux utilisateurs finaux en dehors du centre de données cloud. Au lieu de cela, 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 Google Cloud NetApp Volumes . Le service est géré par automatisation, avec une très petite liste d'administrateurs de confiance ayant accès aux systèmes via les processus abordés dans la section"Opération de service."

Le type de service NetApp Volumes-Performance offre une réplication interrégionale en option pour fournir une protection des données à une région différente en cas de défaillance d'une région. Dans ces cas, les Google Cloud NetApp Volumes peuvent être basculés vers la région non affectée pour maintenir l'accès aux données.

Mises à niveau de service

Les mises à jour aident à protéger les systèmes vulnérables. Chaque mise à jour fournit des améliorations de sécurité et des corrections de bogues qui minimisent 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 pour vérifier que les images officielles sont utilisées et que les mises à niveau ne sont pas compromises par de mauvais acteurs.

Avec Google Cloud NetApp Volumes, les mises à jour sont gérées par les équipes du fournisseur de cloud, ce qui élimine l'exposition aux risques pour les équipes d'administrateurs en fournissant des experts bien familiarisés avec la configuration et les mises à niveau qui ont automatisé et entièrement testé le processus. Les mises à niveau ne sont pas perturbatrices et Google Cloud NetApp Volumes conserve les dernières mises à jour pour de meilleurs résultats globaux.

Pour plus d'informations sur l'équipe d'administrateurs qui effectue ces mises à niveau de service, consultez la section"Opération de service."

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 réutilisation d'un disque. Les données dans Google Cloud NetApp Volumes sont protégées au repos à l'aide d'un cryptage logiciel.

- Les clés générées par Google sont utilisées pour NetApp Volumes-SW.
- Pour NetApp Volumes-Performance, les clés par volume sont stockées dans un gestionnaire de clés intégré à Google Cloud NetApp Volumes, qui utilise NetApp ONTAP CryptoMod pour générer des clés de chiffrement AES-256. CryptoMod est répertorié sur la liste des modules validés CMVP FIPS 140-2. Voir "Certificat FIPS 140-2 n° 4144" .

À partir de novembre 2021, la fonctionnalité d'aperçu du chiffrement géré par le client (CMEK) a été rendue disponible pour NetApp Volumes-Performance. Cette fonctionnalité vous permet de crypter les clés par volume avec des clés principales par projet et par région hébergées dans Google Key Management Service (KMS). KMS vous permet de joindre des gestionnaires de clés externes.

Pour plus de détails sur la façon de configurer KMS pour NetApp Volumes-Performance, "voir la documentation de Google Cloud NetApp Volumes".

Pour plus d'informations sur l'architecture, consultez la section"Architecture des Google Cloud NetApp Volumes ."

Sécurisation des données en vol

Outre la sécurisation des données au repos, vous devez également être en mesure de sécuriser les données lorsqu'elles sont en transit entre l'instance Google Cloud NetApp Volumes et un client ou une cible de réplication. Google Cloud NetApp Volumes fournit un chiffrement des données en vol sur les protocoles NAS en utilisant des méthodes de chiffrement telles que le chiffrement SMB à l'aide de Kerberos, la signature/le scellement des paquets et NFS Kerberos 5p pour le chiffrement de bout en bout des transferts de données.

La réplication des volumes Google Cloud NetApp Volumes utilise 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. Cependant, le DNS n'est pas chiffré par Google Cloud NetApp Volumes (pas de prise en charge DNS Sec) et doit être chiffré à l'aide d'un chiffrement réseau externe lorsque cela est possible. Voir la section"Cryptage des données en transit" pour plus d'informations sur la sécurisation des données en vol.

Pour plus d'informations sur le cryptage du protocole NAS, consultez 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 appropriée des utilisateurs et des groupes, où les utilisateurs accédant aux données sont vérifiés en tant qu'utilisateurs réels dans l'environnement et les groupes contiennent des utilisateurs valides. Ces utilisateurs et groupes fournissent un accès initial au partage et à l'exportation, ainsi qu'une validation des autorisations pour les fichiers et les dossiers du système de stockage.

Google Cloud NetApp Volumes utilise l'authentification utilisateur et groupe Windows standard basée sur Active Directory pour les partages SMB et les autorisations de type Windows. Le service peut également exploiter les fournisseurs d'identité UNIX tels que LDAP pour les utilisateurs et les groupes UNIX pour les exportations NFS, la validation d'ID NFSv4, l'authentification Kerberos et les ACL NFSv4.

Actuellement, seul Active Directory LDAP est pris en charge avec la fonctionnalité Google Cloud NetApp Volumes pour LDAP.

Détection, prévention et atténuation des ransomwares, des logiciels malveillants et des virus

Les ransomwares, les logiciels malveillants et les virus constituent une menace persistante pour les administrateurs, et la détection, la prévention et l'atténuation de ces menaces sont toujours une priorité pour les entreprises. Un seul événement de ransomware sur un ensemble de données critiques peut potentiellement coûter des millions de dollars, il est donc avantageux de faire ce que vous pouvez pour minimiser le risque.

Bien que Google Cloud NetApp Volumes n'intègre actuellement pas de mesures natives de détection ou de prévention, telles qu'une protection antivirus ou "détection automatique des ransomwares", il existe des

moyens de récupérer rapidement après une attaque par ransomware en activant des planifications Snapshot régulières. Les copies Snapshot sont des pointeurs immuables en lecture seule vers les blocs modifiés du système de fichiers, sont quasi instantanées, ont un impact minimal sur les performances et n'occupent de l'espace que lorsque des données sont modifiées ou supprimées. Vous pouvez définir des planifications pour les copies Snapshot afin qu'elles correspondent à votre objectif de point de récupération (RPO)/objectif de temps de récupération (RTO) acceptable souhaité et conserver jusqu'à 1 024 copies Snapshot par volume.

La prise en charge des snapshots est incluse sans frais supplémentaires (au-delà des frais de stockage de données pour les blocs/données modifiés conservés par les copies Snapshot) avec Google Cloud NetApp Volumes et, en cas d'attaque par ransomware, peut être utilisée pour revenir à une copie Snapshot avant que l'attaque ne se produise. Les restaurations instantanées ne prennent que quelques secondes et vous pouvez ensuite reprendre la diffusion des données normalement. Pour plus d'informations, consultez la section "La solution NetApp contre les ransomwares" .

Pour empêcher les ransomwares d'affecter votre entreprise, il faut adopter une approche multicouche qui comprend un ou plusieurs des éléments suivants :

- Protection des terminaux
- Protection contre les menaces externes grâce aux pare-feu réseau
- Détection d'anomalies de données
- Sauvegardes multiples (sur site et hors site) des ensembles de données critiques
- Tests de restauration réguliers des sauvegardes
- Copies immuables de NetApp Snapshot en lecture seule
- Authentification multifactorielle pour les infrastructures critiques
- Audits de sécurité des connexions au système

Cette liste est loin d'être exhaustive, mais constitue un bon modèle à suivre pour faire face au potentiel d'attaques de ransomware. Google Cloud NetApp Volumes dans Google Cloud propose plusieurs moyens de se protéger contre les événements de ransomware et de réduire leurs effets.

Copies instantanées immuables

Google Cloud NetApp Volumes fournit nativement des copies Snapshot immuables en lecture seule qui sont prises selon un calendrier personnalisable pour une récupération rapide à un instant T en cas de suppression de données ou si un volume entier a été victime d'une attaque de ransomware. Les restaurations d'instantanés vers des copies d'instantanés précédentes sont rapides et minimisent la perte de données en fonction de la période de conservation de vos planifications d'instantanés et de votre RTO/RPO. L'effet sur les performances avec la technologie Snapshot est négligeable.

Étant donné que les copies Snapshot dans Google Cloud NetApp Volumes sont en lecture seule, elles ne peuvent pas être infectées par un ransomware, sauf si ce dernier a proliféré dans l'ensemble de données sans que personne ne le remarque et que des copies Snapshot ont été prises des données infectées par le ransomware. C'est pourquoi vous devez également envisager la détection des ransomwares en fonction des anomalies de données. Google Cloud NetApp Volumes ne fournit actuellement pas de détection native, mais vous pouvez utiliser un logiciel de surveillance externe.

Sauvegardes et restaurations

Google Cloud NetApp Volumes fournit des fonctionnalités de sauvegarde client NAS standard (telles que des sauvegardes via NFS ou SMB).

- NetApp Volumes-Performance offre une réplication de volumes entre régions vers d'autres volumes NetApp Volumes-Performance. Pour plus d'informations, consultez "réplication de volume" la documentation Google Cloud NetApp Volumes.
- NetApp Volumes-SW offre des fonctionnalités natives de sauvegarde/restauration des volumes. Pour plus d'informations, consultez "sauvegarde dans le cloud" dans la documentation Google Cloud NetApp Volumes.

La réplication de volume fournit une copie exacte du volume source pour un basculement rapide en cas de sinistre, y compris en cas d'événements de ransomware.

Réplication interrégionale

NetApp Volumes-Performance vous permet de répliquer en toute sécurité des volumes dans les régions Google Cloud pour la protection des données et les cas d'utilisation d'archivage en utilisant le cryptage TLS1.2 AES 256 GCM sur un réseau de services back-end contrôlé par NetApp à l'aide d'interfaces spécifiques utilisées pour la réplication exécutée sur le réseau de Google. Un volume principal (source) contient les données de production actives et est répliqué sur un volume secondaire (destination) pour fournir une réplique exacte de l'ensemble de données principal.

La réplication initiale transfère tous les blocs, mais les mises à jour transmettent uniquement les blocs modifiés dans un volume principal. Par exemple, si une base de données de 1 To résidant sur un volume principal est répliquée sur le volume secondaire, 1 To d'espace est transféré lors de la réplication initiale. Si cette base de données comporte quelques centaines de lignes (hypothétiquement, quelques Mo) qui changent entre l'initialisation et la mise à jour suivante, seuls les blocs avec les lignes modifiées sont répliqués sur la base secondaire (quelques Mo). Cela permet de garantir que les temps de transfert restent faibles et de maintenir les frais de réplication à un niveau bas.

Toutes les autorisations sur les fichiers et les dossiers sont répliquées sur le volume secondaire, mais les autorisations d'accès aux partages (telles que les politiques et règles d'exportation ou les partages SMB et les listes de contrôle d'accès aux partages) doivent être gérées séparément. En cas de basculement de site, le site de destination doit exploiter les mêmes services de noms et connexions de domaine Active Directory pour assurer une gestion cohérente des identités et des autorisations des utilisateurs et des groupes. Vous pouvez utiliser un volume secondaire comme cible de basculement en cas de sinistre en rompant la relation de réplication, ce qui convertit le volume secondaire en lecture-écriture.

Les répliques de volume sont en lecture seule, ce qui fournit une copie immuable des données hors site pour une récupération rapide des données dans les cas où un virus a infecté les données ou un ransomware a chiffré l'ensemble de données principal. Les données en lecture seule ne seront pas chiffrées, mais si le volume principal est affecté et que la réplication se produit, les blocs infectés se répliquent également. Vous pouvez utiliser des copies Snapshot plus anciennes et non affectées pour récupérer, mais les SLA peuvent sortir de la portée du RTO/RPO promis en fonction de la rapidité avec laquelle une attaque est détectée.

De plus, vous pouvez empêcher les actions administratives malveillantes, telles que les suppressions de volumes, les suppressions de Snapshot ou les modifications de planification des Snapshot, grâce à la gestion de la réplication interrégionale (CRR) dans Google Cloud. Pour ce faire, vous devez créer des rôles personnalisés qui distinguent les administrateurs de volumes, qui peuvent supprimer les volumes sources mais pas rompre les miroirs et ne peuvent donc pas supprimer les volumes de destination, des administrateurs CRR, qui ne peuvent effectuer aucune opération sur les volumes. Consultez "Considérations de sécurité" la documentation Google Cloud NetApp Volumes pour connaître les autorisations accordées à chaque groupe d'administrateurs.

Sauvegarde des Google Cloud NetApp Volumes

Bien que Google Cloud NetApp Volumes offre une durabilité élevée des données, des événements externes

peuvent entraîner une perte de données. En cas d'événement de sécurité tel qu'un virus ou un ransomware, les sauvegardes et les restaurations deviennent essentielles pour reprendre l'accès aux données en temps opportun. Un administrateur peut supprimer accidentellement un volume Google Cloud NetApp Volumes . Ou bien les utilisateurs souhaitent simplement conserver des versions de sauvegarde de leurs données pendant plusieurs mois et conserver l'espace de copie Snapshot supplémentaire à l'intérieur du volume devient un défi financier. Bien que les copies instantanées doivent être le moyen privilégié pour conserver les versions de sauvegarde des dernières semaines afin de restaurer les données perdues, elles se trouvent à l'intérieur du volume et sont perdues si le volume disparaît.

Pour toutes ces raisons, Google Cloud NetApp Volumes propose des services de sauvegarde via "Sauvegarde des Google Cloud NetApp Volumes".

La sauvegarde Google Cloud NetApp Volumes génère une copie du volume sur Google Cloud Storage (GCS). Il sauvegarde uniquement les données réelles stockées dans le volume, pas l'espace libre. Il fonctionne de manière incrémentielle, ce qui signifie qu'il transfère le contenu du volume une fois et qu'à partir de là, il continue de sauvegarder uniquement les données modifiées. Par rapport aux concepts de sauvegarde classiques avec plusieurs sauvegardes complètes, il permet d'économiser de grandes quantités de stockage de sauvegarde, réduisant ainsi les coûts. Étant donné que le prix mensuel de l'espace de sauvegarde est inférieur à celui d'un volume, c'est un endroit idéal pour conserver les versions de sauvegarde plus longtemps.

Les utilisateurs peuvent utiliser une sauvegarde Google Cloud NetApp Volumes pour restaurer n'importe quelle version de sauvegarde sur le même volume ou sur un volume différent dans la même région. Si le volume source est supprimé, les données de sauvegarde sont conservées et doivent être gérées (par exemple, supprimées) de manière indépendante.

La sauvegarde de Google Cloud NetApp Volumes est intégrée à Google Cloud NetApp Volumes en tant qu'option. Les utilisateurs peuvent choisir les volumes à protéger en activant la sauvegarde de Google Cloud NetApp Volumes pour chaque volume. Consultez la "Documentation sur la sauvegarde de Google Cloud NetApp Volumes" pour obtenir des informations sur les sauvegardes, la "nombre maximal de versions de sauvegarde prises en charge", la planification et "prix".

Toutes les données de sauvegarde d'un projet sont stockées dans un bucket GCS, qui est géré par le service et non visible par l'utilisateur. Chaque projet utilise un bucket différent. Actuellement, les buckets se trouvent dans la même région que les volumes Google Cloud NetApp Volumes , mais d'autres options sont en cours de discussion. Consultez la documentation pour connaître l'état le plus récent.

Le transport de données d'un bucket Google Cloud NetApp Volumes vers GCS utilise les réseaux Google internes au service avec HTTPS et TLS1.2. Les données sont chiffrées au repos avec des clés gérées par Google.

Pour gérer les sauvegardes de Google Cloud NetApp Volumes (création, suppression et restauration des sauvegardes), un utilisateur doit disposer du "roles/netapp.admin" rôle.

Aperçu

Faire confiance à une solution cloud implique notamment de comprendre son architecture et la manière dont elle est sécurisée. Cette section présente différents aspects de l'architecture Google Cloud NetApp Volumes dans Google pour aider à atténuer les préoccupations potentielles concernant la manière dont les données sont sécurisées, ainsi que pour souligner les domaines dans lesquels des étapes de configuration supplémentaires peuvent être nécessaires pour obtenir le déploiement le plus sécurisé.

L’architecture générale de Google Cloud NetApp Volumes peut être divisée en deux composants principaux : le plan de contrôle et le plan de données.

Plan de contrôle

Le plan de contrôle dans Google Cloud NetApp Volumes est l’infrastructure back-end gérée par les administrateurs Google Cloud NetApp Volumes et le logiciel d’automatisation natif NetApp . Ce plan est totalement transparent pour les utilisateurs finaux et inclut la mise en réseau, le matériel de stockage, les mises à jour logicielles, etc. pour aider à apporter de la valeur à une solution résidente dans le cloud telle que Google Cloud NetApp Volumes.

Plan de données

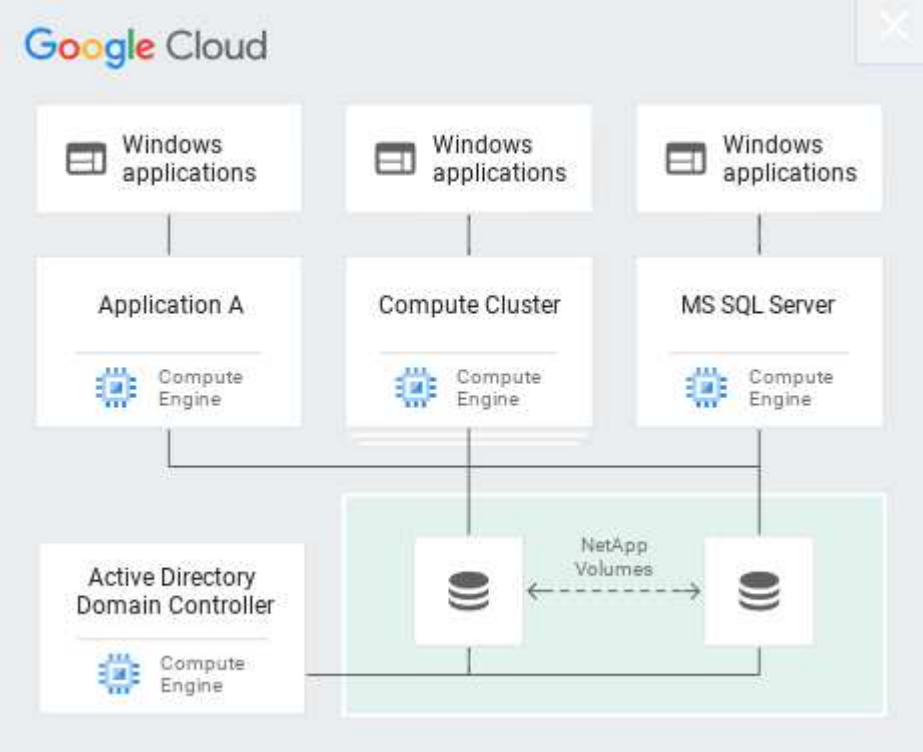
Le plan de données dans Google Cloud NetApp Volumes inclut les volumes de données réels et la configuration globale de Google Cloud NetApp Volumes (comme le contrôle d’accès, l’authentification Kerberos, etc.). Le plan de données est entièrement sous le contrôle des utilisateurs finaux et des consommateurs de la plateforme Google Cloud NetApp Volumes .

Il existe des différences distinctes dans la manière dont chaque avion est sécurisé et géré. Les sections suivantes couvrent ces différences, en commençant par une présentation de l’architecture Google Cloud NetApp Volumes .

Architecture de Google Cloud NetApp Volumes

De manière similaire à d’autres services natifs de Google Cloud tels que CloudSQL, Google Cloud VMware Engine (GCVE) et FileStore, Google Cloud NetApp Volumes utilise "Message d’intérêt public de Google" pour fournir le service. Dans PSA, les services sont construits dans un projet de producteur de services, qui utilise "Appairage de réseau VPC" pour se connecter au consommateur de services. Le producteur de services est fourni et exploité par NetApp, et le consommateur de services est un VPC dans un projet client, hébergeant les clients qui souhaitent accéder aux partages de fichiers Google Cloud NetApp Volumes .

La figure suivante, référencée dans le "Documentation Google Cloud NetApp Volumes", présente une vue d’ensemble.



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 située sous la ligne pointillée montre le plan de données. La case bleue de gauche représente le VPC utilisateur (consommateur de services), la case bleue de droite représente le producteur de services fourni par NetApp. Les deux sont connectés via le peering VPC.

Modèle de location

Dans Google Cloud NetApp Volumes, les projets individuels sont considérés comme des locataires uniques. Cela signifie que la manipulation des volumes, des copies Snapshot, etc. sont effectuées projet par projet. En d'autres termes, tous les volumes appartiennent au projet dans lequel ils ont été créés et seul ce projet peut gérer et accéder aux données qu'ils contiennent par défaut. Ceci est considéré comme la vue du plan de contrôle du service.

VPC partagés

Sur la vue du plan de données, Google Cloud NetApp Volumes 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 potentiellement accéder aux données via les protocoles NAS, le contrôle d'accès sur le volume individuel (tel que les listes de contrôle d'accès utilisateur/groupe (ACL) et les noms d'hôte/adresses IP pour les exportations NFS) doit être utilisé pour contrôler qui peut accéder aux données.

Vous pouvez connecter Google Cloud NetApp Volumes à un maximum de cinq VPC 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 seul VPC.

L'accès aux volumes individuels est contrôlé par des mécanismes de contrôle d'accès spécifiques au 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 côté de la gestion, le plan de contrôle permet uniquement au projet propriétaire de voir le volume.

Contrôles de service VPC

Les contrôles de service VPC établissent un périmètre de contrôle d'accès autour des services Google Cloud connectés à Internet et accessibles dans le monde entier. Ces services fournissent un contrôle d'accès via les identités des utilisateurs, mais ne peuvent pas restreindre l'emplacement réseau d'où proviennent les demandes. Les contrôles de service VPC comblent cette lacune en introduisant des fonctionnalités permettant de restreindre l'accès à des réseaux définis.

Le plan de données Google Cloud NetApp Volumes n'est pas connecté à Internet externe mais à des VPC privés avec des limites de réseau bien définies (périmètres). Au sein de ce réseau, chaque volume utilise un contrôle d'accès spécifique au protocole. Toute connectivité réseau externe est explicitement créée 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 consulté par n'importe qui, de n'importe où, avec des informations d'identification valides ("Jetons JWT").

En bref, le plan de données Google Cloud NetApp Volumes offre la possibilité de contrôler l'accès au réseau, sans nécessiter de prise en charge des contrôles de service VPC et n'utilise pas explicitement les contrôles de service VPC.

Considérations relatives au reniflage et au traçage des paquets

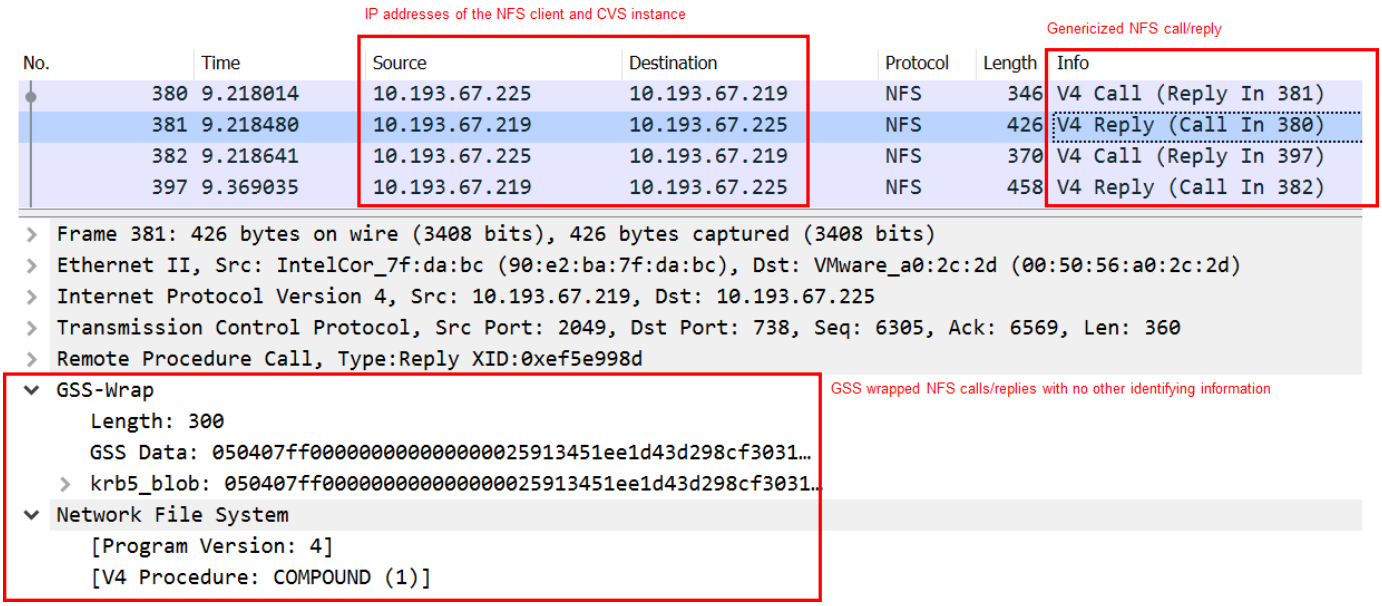
Les captures de paquets peuvent être utiles pour résoudre les problèmes de réseau ou d'autres problèmes (tels que les autorisations NAS, la connectivité LDAP, etc.), mais peuvent également être utilisées de manière malveillante pour obtenir des informations sur les adresses IP du réseau, les adresses MAC, les noms d'utilisateur et de groupe, et le niveau de sécurité utilisé sur les points de terminaison. En raison de la façon dont les règles de réseau, de VPC et de pare-feu de Google Cloud sont configurées, l'accès indésirable aux paquets réseau devrait être difficile à obtenir sans les informations de connexion de l'utilisateur ou"Jetons JWT" dans les instances cloud. Les captures de paquets ne sont possibles que sur les points de terminaison (tels que les machines virtuelles (VM)) et uniquement possibles sur les points de terminaison internes au VPC, sauf si un VPC partagé et/ou un tunnel réseau externe/un transfert IP sont utilisés pour autoriser explicitement le trafic externe vers les points de terminaison. Il n'existe aucun moyen de détecter le trafic en dehors des clients.

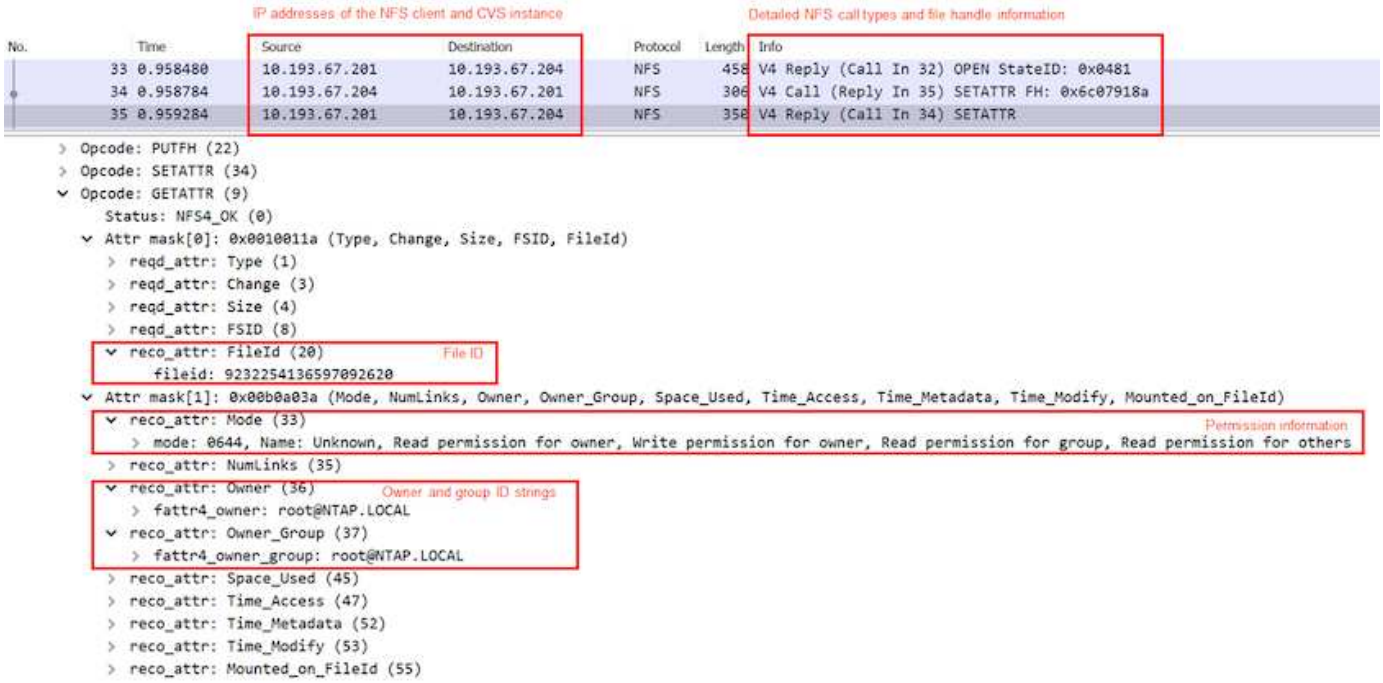
Lorsque des VPC partagés sont utilisés, un chiffrement en vol avec NFS Kerberos et/ou"cryptage SMB" peut masquer une grande partie des informations glanées à partir des traces. Cependant, une partie du trafic est toujours envoyée en texte clair, comme"DNS" et"Requêtes LDAP" . La figure suivante montre une capture de paquet à partir d'une requête LDAP en texte brut provenant de Google Cloud NetApp Volumes et les informations d'identification potentielles exposées. Les requêtes LDAP dans Google Cloud NetApp Volumes ne prennent actuellement pas en charge le chiffrement ou LDAP sur SSL. NetApp Volumes-Performance prend en charge la signature LDAP, si demandé par Active Directory. NetApp Volumes-SW ne prend pas en charge la signature LDAP.



unixUserPassword est interrogé par LDAP et n'est pas envoyé en texte brut mais plutôt dans un hachage salé. Par défaut, Windows LDAP ne renseigne pas les champs unixUserPassword. Ce champ n'est obligatoire que si vous devez utiliser Windows LDAP pour les connexions interactives via LDAP aux clients. Google Cloud NetApp Volumes ne prend pas en charge les connexions LDAP interactives aux instances.

La figure suivante montre une capture de paquet à partir d'une conversation NFS Kerberos à côté d'une capture de NFS sur AUTH_SYS. Notez comment les informations disponibles dans une trace diffèrent entre les deux et comment l'activation du chiffrement en vol offre une meilleure sécurité globale pour le trafic NAS.





Interfaces réseau VM

Une astuce que les attaquants pourraient tenter est d'ajouter une nouvelle carte d'interface réseau (NIC) à une machine virtuelle. "mode promiscuité" (mise en miroir des ports) ou activer le mode promiscuité sur une carte réseau existante afin de renifler tout le trafic. Dans Google Cloud, l'ajout d'une nouvelle carte réseau nécessite l'arrêt complet d'une machine virtuelle, ce qui crée des alertes, de sorte que les attaquants ne peuvent pas le faire sans se faire remarquer.

De plus, les cartes réseau ne peuvent pas du tout être configurées en mode promiscuité et déclencheront des alertes dans Google Cloud.

Architecture du plan de contrôle

Toutes les actions de gestion sur Google Cloud NetApp Volumes sont effectuées via l'API. La gestion des Google Cloud NetApp Volumes intégrée à la console GCP Cloud utilise également l'API Google Cloud NetApp Volumes .

Gestion des identités et des accès

Gestion des identités et des accès("JE SUIS") 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 d'autorisations. Actuellement, Google Cloud NetApp Volumes ne fournit pas d'audit du plan de contrôle.

Aperçu des autorisations/permissions

IAM offre des autorisations intégrées et granulaires pour Google Cloud NetApp Volumes. Vous pouvez en 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 des rôles et des autorisations appropriés pour permettre aux utilisateurs IAM de gérer les Google Cloud NetApp Volumes.

Voici quelques exemples d'utilisation d'autorisations granulaires :

- Créez un rôle personnalisé avec uniquement les autorisations d'obtention/répertoire/création/mise à jour afin que les utilisateurs ne puissent pas supprimer de volumes.
- Utiliser un rôle personnalisé avec uniquement `snapshot.*` autorisations pour créer un compte de service utilisé pour créer une intégration Snapshot cohérente avec l'application.
- Créez un rôle personnalisé à déléguer `volumereplication.*` à des utilisateurs spécifiques.

Comptes de service

Pour effectuer des appels d'API Google Cloud NetApp Volumes via des scripts ou "Terraform" , vous devez créer un compte de service avec le `roles/netappcloudvolumes.admin` rôle. Vous pouvez utiliser ce compte de service pour générer les jetons JWT requis pour authentifier les requêtes API Google Cloud NetApp Volumes de deux manières différentes :

- Générez une clé JSON et utilisez les API Google pour en dériver un jeton JWT. Il s'agit de l'approche la plus simple, mais elle implique une gestion manuelle des secrets (la clé JSON).
- Utiliser "Usurpation d'identité de compte de service" avec `roles/iam.serviceAccountTokenCreator` . Le code (script, Terraform, etc.) s'exécute avec "Informations d'identification par défaut de l'application" et usurpe l'identité du compte de service pour obtenir ses autorisations. Cette approche reflète les meilleures pratiques de sécurité de Google.

Consultez "Création de votre compte de service et de votre clé privée" dans la documentation Google cloud pour plus d'informations.

API Google Cloud NetApp Volumes

L'API de Google Cloud NetApp Volumes utilise une API basée sur REST en utilisant HTTPS (TLSv1.2) comme transport réseau sous-jacent. Vous trouverez la définition la plus récente de l'API et des informations sur son utilisation à l'adresse "API Cloud Volumes dans la documentation Google Cloud".

Le point de terminaison de l'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 porteurs JWT("RFC-7519"). Les jetons JWT valides doivent être obtenus à l'aide de l'authentification Google Cloud IAM. Cela doit être fait en récupérant un jeton auprès d'IAM en fournissant une clé JSON de compte de service.

Journalisation d'audit

Actuellement, aucun journal d'audit du plan de contrôle accessible aux utilisateurs n'est disponible.

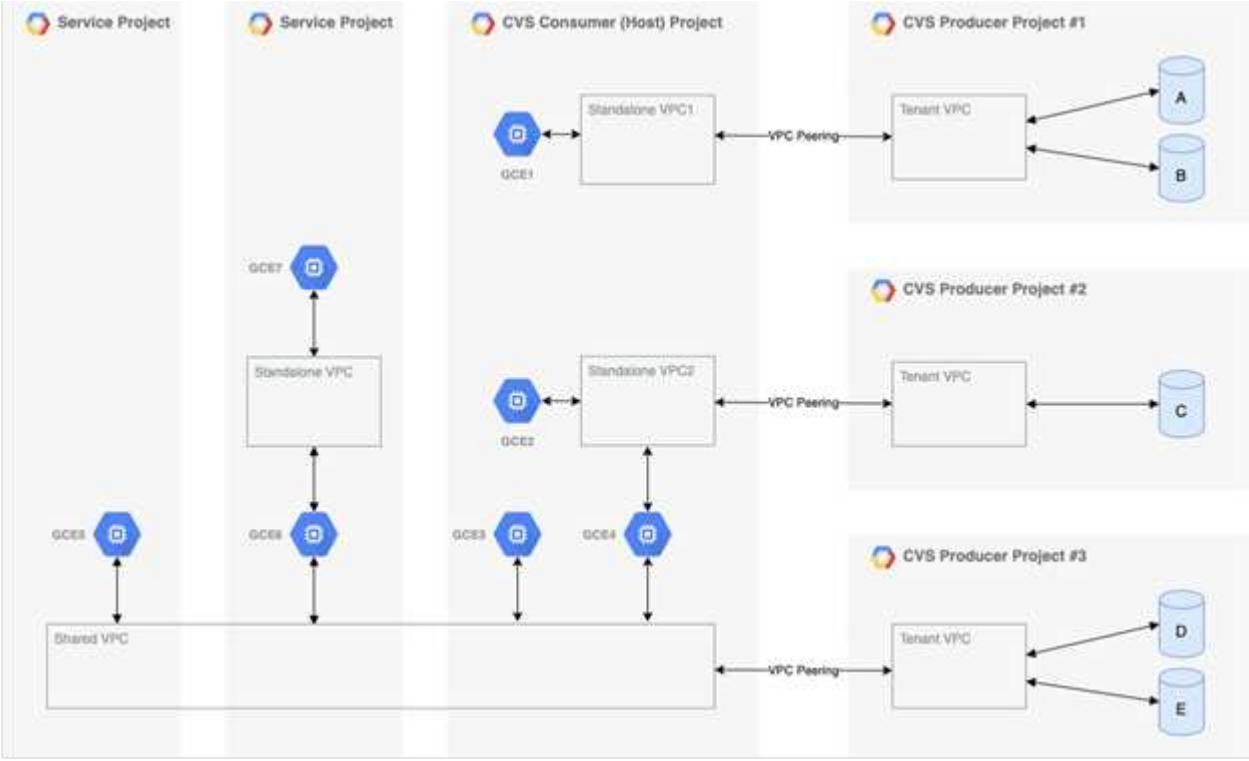
Architecture du plan de données

Google Cloud NetApp Volumes pour Google Cloud exploite Google Cloud "accès aux services privés" cadre. Dans ce cadre, les utilisateurs peuvent se connecter aux Google Cloud NetApp Volumes. Ce framework utilise des structures de réseau de services et de

peering VPC comme d'autres services Google Cloud, garantissant une isolation complète entre les locataires.

Pour une vue d'ensemble de l'architecture de Google Cloud NetApp Volumes for Google Cloud, voir "Architecture pour Google Cloud NetApp Volumes".

Les VPC utilisateur (autonomes ou partagés) sont associés à des VPC au sein de projets locataires gérés par Google Cloud NetApp Volumes , qui hébergent les volumes.



La figure précédente montre un projet (le projet consommateur NetApp Volumes au milieu) avec trois réseaux VPC connectés à Google Cloud NetApp Volumes et plusieurs machines virtuelles Compute Engine (GCE1-7) partageant des volumes :

- VPC1 permet à GCE1 d'accéder aux volumes A et B.
- VPC2 permet à GCE2 et GCE4 d'accéder au volume C.
- Le troisième réseau VPC est un VPC partagé, partagé avec deux projets de service. Il permet à 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 de type de service NetApp Volumes-Performance.

GCE7 ne peut accéder à aucun volume.

Les données peuvent être chiffrées à la fois en transit (à l'aide du chiffrement Kerberos et/ou SMB) et au repos dans Google Cloud NetApp Volumes.

Cryptage 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 crypte le trafic au niveau du réseau comme décrit dans "Cryptage en transit" dans la documentation Google. Comme mentionné dans la section « Architecture de Google Cloud NetApp Volumes », Google Cloud NetApp Volumes est fourni à partir d'un projet producteur PSA contrôlé par NetApp.

Dans le cas de NetApp Volumes-SW, le locataire producteur exécute des machines virtuelles Google pour fournir le service. Le trafic entre les machines virtuelles utilisateur et les machines virtuelles Google Cloud NetApp Volumes est automatiquement chiffré par Google.

Bien que le chemin de données pour NetApp Volumes-Performance ne soit pas entièrement chiffré sur la couche réseau, NetApp et Google utilisent une combinaison "du 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 Google Cloud NetApp Volumes NetApp Volumes et Google Cloud.

Protocoles NAS

Les protocoles NAS NFS et SMB fournissent un cryptage de transport facultatif au niveau de la couche de protocole.

cryptage SMB

"cryptage SMB"fournit un cryptage de bout en bout des données SMB et protège les données contre les écoutes clandestines sur des réseaux non fiables. Vous pouvez activer le chiffrement pour la connexion de données client/serveur (disponible uniquement pour les clients compatibles SMB3.x) et pour l'authentification du serveur/contrôleur de domaine.

Lorsque le chiffrement SMB est activé, les clients qui ne prennent pas en charge le chiffrement ne peuvent pas accéder au partage.

Google Cloud NetApp Volumes prend en charge les chiffrements de sécurité RC4-HMAC, AES-128-CTS-HMAC-SHA1 et AES-256-CTS-HMAC-SHA1 pour le chiffrement SMB. SMB négocie le type de cryptage le plus élevé pris en charge par le serveur.

NFSv4.1 Kerberos

Pour NFSv4.1, NetApp Volumes-Performance propose l'authentification Kerberos comme décrit dans "RFC7530" Vous pouvez activer Kerberos volume par volume.

Le type de cryptage le plus puissant actuellement disponible pour Kerberos est AES-256-CTS-HMAC-SHA1. Google Cloud NetApp Volumes 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 fournit trois niveaux de sécurité différents pour les montages NFS qui offrent des choix quant au niveau 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 doit intervenir, plus les performances sont mauvaises, 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 déchargement AES-NI vers les processeurs pour une meilleure expérience globale, mais l'impact sur les performances de Kerberos 5p (chiffrement de bout en bout complet) est nettement supérieur à l'impact de Kerberos 5 (authentification utilisateur).

Le tableau suivant montre les différences entre ce que chaque niveau fait en matière de sécurité et de performances.

Niveau de sécurité	Sécurité	Performances
NFSv3—sys	• Le moins sécurisé ; texte brut avec identifiants d'utilisateur/de groupe numériques • Capable d'afficher l'UID, le GID, les adresses IP des clients, les chemins d'exportation, les noms de fichiers et les autorisations dans les captures de paquets	• Idéal pour la plupart des cas
NFSv4.x—sys	• Plus sécurisé que NFSv3 (identifiants client, correspondance chaîne de nom/chaîne de domaine) mais toujours en texte brut • Capable d'afficher l'UID, le GID, les adresses IP des clients, les chaînes de noms, les ID de domaine, les chemins d'exportation, les noms de fichiers et les autorisations dans les captures de paquets	• Idéal pour les charges de travail séquentielles (telles que les machines virtuelles, les bases de données, les fichiers volumineux) • Mauvais avec un nombre élevé de fichiers/métadonnées élevées (30 à 50 % pire)

Niveau de sécurité	Sécurité	Performances
NFS—krb5	• Chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS : encapsule l'UID/GID des utilisateurs/groupes dans les appels RPC dans le wrapper GSS • L'utilisateur demandant l'accès au montage a besoin d'un ticket Kerberos valide (soit via un nom d'utilisateur/mot de passe, soit via un échange manuel de clés) ; le ticket expire après une période de temps spécifiée et l'utilisateur doit se réauthentifier pour accéder • Aucun cryptage pour les opérations NFS ou les protocoles auxiliaires tels que mount/portmapper/nlm (peut voir les chemins d'exportation, les adresses IP, les descripteurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets)	• Meilleur dans la plupart des cas pour Kerberos ; pire que AUTH_SYS

Niveau de sécurité	Sécurité	Performances
NFS—krb5i	• Chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS : encapsule l'UID/GID des utilisateurs/groupes dans les appels RPC dans le wrapper GSS • L'utilisateur demandant l'accès au montage a besoin d'un ticket Kerberos valide (soit via un nom d'utilisateur/mot de passe, soit via un échange manuel de clés) ; le ticket expire après une période de temps spécifiée et l'utilisateur doit se réauthentifier pour accéder • Aucun cryptage pour les opérations NFS ou les protocoles auxiliaires tels que mount/portmapper/nlm (peut voir les chemins d'exportation, les adresses IP, les descripteurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets) • La somme de contrôle Kerberos GSS est ajoutée à chaque paquet pour garantir que rien n'intercepte les paquets. Si les sommes de contrôle correspondent, la conversation est autorisée.	• Mieux que krb5p car la charge utile NFS n'est pas chiffrée ; la seule surcharge supplémentaire par rapport à krb5 est la somme de contrôle d'intégrité. Les performances de krb5i ne seront pas bien pires que celles de krb5 mais connaîtront une certaine dégradation.

Niveau de sécurité	Sécurité	Performances
NFS – krb5p	• Chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS : encapsule l'UID/GID des utilisateurs/groupes dans les appels RPC dans le wrapper GSS • L'utilisateur demandant l'accès au montage a besoin d'un ticket Kerberos valide (via un nom d'utilisateur/mot de passe ou un échange manuel de keytab) ; le ticket expire après la période spécifiée et l'utilisateur doit se réauthentifier pour accéder • Toutes les charges utiles des paquets NFS sont chiffrées avec le wrapper GSS (impossible de voir les descripteurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets). • Inclut un contrôle d'intégrité. • Le type d'opération NFS est visible (FSINFO, ACCESS, GETATTR, etc.). • Les protocoles auxiliaires (mount, portmap, nlm, etc.) ne sont pas chiffrés - (peuvent voir les chemins d'exportation, les adresses IP)	• Pire performance des niveaux de sécurité ; krb5p doit crypter/décrypter davantage. • Meilleures performances que krb5p avec NFSv4.x pour les charges de travail à nombre de fichiers élevé.

Dans Google Cloud NetApp Volumes, un serveur Active Directory configuré est utilisé comme serveur Kerberos et serveur LDAP (pour rechercher les identités des utilisateurs à partir d'un schéma compatible RFC2307). Aucun autre serveur Kerberos ou LDAP n'est pris en charge. NetApp vous recommande vivement d'utiliser LDAP pour la gestion des identités dans Google Cloud NetApp Volumes. Pour plus d'informations sur la façon dont NFS Kerberos est affiché dans les captures de paquets, consultez la section "Packet sniffing/trace considerations."

Cryptage des données au repos

Tous les volumes de Google Cloud NetApp Volumes sont chiffrés au repos à l'aide du chiffrement AES-256, ce qui signifie que toutes les données utilisateur écrites sur le support sont chiffrées et ne peuvent être déchiffrées qu'avec une clé par volume.

- Pour NetApp Volumes-SW, les clés générées par Google sont utilisées.
- Pour NetApp Volumes-Performance, les clés par volume sont stockées dans un gestionnaire de clés

intégré à Google Cloud NetApp Volumes.

À partir de novembre 2021, la fonctionnalité d'aperçu des clés de chiffrement gérées par le client (CMEK) a été rendue disponible. Cela vous permet de crypter les clés par volume avec une clé principale par projet et par région hébergée dans "Service de gestion des clés Google (KMS)." KMS vous permet de joindre des gestionnaires de clés externes.

Pour plus d'informations sur la configuration de KMS pour NetApp Volumes-Performance, consultez "Configuration des clés de chiffrement gérées par le client".

Pare-feu

Google Cloud NetApp Volumes expose plusieurs ports TCP pour servir les partages NFS et SMB :

- "Ports requis pour l'accès NFS"
- "Ports requis pour l'accès SMB"

De plus, les configurations SMB, NFS avec LDAP, y compris Kerberos, et à double protocole nécessitent un accès à un domaine Windows Active Directory. Les connexions Active Directory doivent être "configuré" établies par région. Les contrôleurs de domaine Active Directory (DC) sont identifiés en utilisant "Découverte de DC basée sur DNS" les serveurs DNS spécifiés. Tous les DC renvoyés sont utilisés. La liste des DC éligibles peut être limitée en spécifiant un site Active Directory.

Google Cloud NetApp Volumes utilise des adresses IP de la plage CIDR allouée avec la `gcloud compute address` commande lorsque "intégration de Google Cloud NetApp Volumes". Vous pouvez utiliser cette plage CIDR comme adresses source pour configurer les pare-feu entrants de vos contrôleurs de domaine Active Directory.

Les contrôleurs de domaine Active Directory doivent "exposer les ports aux CIDR Google Cloud NetApp Volumes comme mentionné ici".

Présentation des protocoles NAS

Les protocoles NAS incluent NFS (v3 et v4.1) et SMB/CIFS (2.x et 3.x). Ces protocoles permettent à NetApp Volumes de permettre un accès partagé aux données sur plusieurs clients NAS. De plus, Google Cloud NetApp Volumes peut fournir un accès simultané aux clients NFS et SMB/CIFS (double protocole) tout en respectant tous les paramètres d'identité et d'autorisation sur les fichiers et dossiers des partages NAS. Pour maintenir la sécurité de transfert de données la plus élevée possible, Google Cloud NetApp Volumes prend en charge le chiffrement de protocole en vol à l'aide du chiffrement SMB et de NFS Kerberos 5p.

Le double protocole est disponible uniquement avec NetApp Volumes-Performance.

Notions de base sur les protocoles NAS

Les protocoles NAS sont des moyens permettant à plusieurs clients d'un réseau d'accéder aux mêmes données sur un système de stockage, tel que Google Cloud NetApp Volumes sur GCP. NFS et SMB sont les protocoles NAS définis et fonctionnent

sur une base client/serveur où Google Cloud NetApp Volumes agit comme 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 de la gestion 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, etc.) ; le serveur répond avec les informations si le client et l'utilisateur demandeurs disposent des autorisations nécessaires sur le dossier parent.
2. Si les autorisations sur le 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 du fichier est déjà utilisé, la création échoue. Si le nom du fichier n'existe pas, le serveur informe le client qu'il peut continuer.
3. Le client émet un appel au serveur pour créer le fichier avec le handle du répertoire et le nom du fichier et définit les heures d'accès et de modification. Le serveur attribue un ID de fichier unique au fichier pour garantir 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 WRITE. Si les autorisations le permettent, le client écrit alors le nouveau fichier. Si le verrouillage est utilisé par le protocole/l'application, le client demande au serveur un verrou pour empêcher d'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 demande de commentaires (RFC) qui permet à quiconque de mettre en œuvre le protocole.

Les volumes dans Google Cloud NetApp Volumes sont partagés entre les clients NFS en exportant un chemin accessible à un client ou à un ensemble de clients. Les autorisations pour monter ces exportations sont définies par des politiques et des règles d'exportation, qui sont configurables par les administrateurs de Google Cloud NetApp Volumes .

L'implémentation NetApp NFS est considérée comme une référence absolue pour le protocole et est utilisée dans d'innombrables environnements NAS d'entreprise. Les sections suivantes couvrent NFS et les fonctionnalités de sécurité spécifiques disponibles dans Google Cloud NetApp Volumes et la manière dont elles sont implémentées.

Utilisateurs et groupes UNIX locaux par défaut

Google Cloud NetApp Volumes contient plusieurs utilisateurs et groupes UNIX par défaut pour diverses fonctionnalités de base. Ces utilisateurs et groupes ne peuvent actuellement pas être modifiés ou supprimés. Les nouveaux utilisateurs et groupes locaux ne peuvent actuellement pas être ajoutés à Google Cloud NetApp Volumes. Les utilisateurs et groupes UNIX en dehors des utilisateurs et groupes par défaut doivent être fournis par un service de noms LDAP externe.

Le tableau suivant présente les utilisateurs et les groupes par défaut ainsi que leurs identifiants numériques correspondants. NetApp recommande de ne pas créer de nouveaux utilisateurs ou groupes dans LDAP ou sur les clients locaux qui réutilisent ces ID numériques.

Utilisateurs par défaut : identifiants numériques	Groupes par défaut : identifiants 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 de commandes de liste de répertoires sur les clients NFS. Cela est dû à la configuration du mappage du domaine d'ID du client. Voir la section intituléeNFSv4.1 et l'utilisateur/groupe nobody pour plus de détails sur ce problème et comment le résoudre.

L'utilisateur root

Sous Linux, le compte root a accès à toutes les commandes, fichiers et dossiers d'un système de fichiers basé sur Linux. En raison de la puissance de ce compte, les meilleures pratiques de sécurité nécessitent souvent que l'utilisateur root soit désactivé ou restreint d'une manière ou d'une autre. Dans les exportations NFS, le pouvoir dont dispose un utilisateur root sur les fichiers et les dossiers peut être contrôlé dans Google Cloud NetApp Volumes via des stratégies et des règles d'exportation et un concept appelé root squash.

L'écrasement de la racine garantit que l'utilisateur root accédant à un montage NFS est écrasé vers l'utilisateur numérique anonyme 65534 (voir la section «L'utilisateur anonyme ") et n'est actuellement disponible que lors de l'utilisation de NetApp Volumes-Performance en sélectionnant Désactivé pour l'accès root lors de la création de la règle de stratégie d'exportation. Si l'utilisateur root est écrasé vers l'utilisateur anonyme, il n'a plus accès pour exécuter chown ou "commandes setuid/setgid (la partie collante)" sur les fichiers ou dossiers dans le montage NFS, et les fichiers ou dossiers créés par l'utilisateur root affichent l'UID anonyme comme propriétaire/groupe. De plus, les ACL NFSv4 ne peuvent pas être modifiées par l'utilisateur root. Cependant, l'utilisateur root a toujours accès à chmod et aux fichiers supprimés pour lesquels il ne dispose pas d'autorisations explicites. Si vous souhaitez limiter l'accès aux autorisations de fichiers et de dossiers d'un utilisateur root, envisagez d'utiliser un volume avec des ACL NTFS, en créant un utilisateur Windows nommé `root` , et en appliquant les autorisations souhaitées aux fichiers ou dossiers.

L'utilisateur anonyme

L'ID utilisateur anonyme (anon) spécifie un ID utilisateur ou un nom d'utilisateur UNIX qui est mappé aux demandes client qui arrivent sans informations d'identification NFS valides. Cela peut inclure l'utilisateur root lorsque l'écrasement root est utilisé. L'utilisateur anonyme dans Google Cloud NetApp Volumes est 65534.

Cet UID est normalement associé au nom d'utilisateur `nobody` ou `nfsnobody` dans les environnements Linux. Google Cloud NetApp Volumes utilise également 65534 comme utilisateur UNIX local` pcuser` (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 vers UNIX lorsqu'aucun utilisateur UNIX correspondant valide ne peut être trouvé dans LDAP.

En raison des différences entre les noms d'utilisateur sur Linux et Google Cloud NetApp Volumes pour l'UID 65534, la chaîne de nom des utilisateurs mappés à 65534 peut ne pas correspondre lors de l'utilisation de NFSv4.1. En conséquence, vous pourriez voir `nobody` en tant qu'utilisateur sur certains fichiers et dossiers. Voir la section "NFSv4.1 et l'utilisateur/groupe nobody " pour plus d'informations sur ce problème et comment le résoudre.

Contrôle d'accès/exportations

L'accès initial à l'exportation/au partage pour les montages NFS est contrôlé par des règles de politique d'exportation basées sur l'hôte contenues dans une politique d'exportation. Une adresse IP d'hôte, un nom d'hôte, un sous-réseau, un groupe réseau ou un domaine est défini pour permettre l'accès au montage du partage NFS et le niveau d'accès autorisé à l'hôte. Les options de configuration des règles de stratégie d'exportation dépendent du niveau de Google Cloud NetApp Volumes .

Pour NetApp Volumes-SW, les options suivantes sont disponibles pour la configuration de la stratégie d'exportation :

- **Correspondance client.** Liste d'adresses IP séparées par des virgules, liste de noms d'hôtes, de sous-réseaux, de groupes de réseaux, de noms de domaine séparés par des virgules.
- **Règles d'accès RO/RW.** Sélectionnez lecture/écriture ou lecture seule pour contrôler le niveau d'accès à l'exportation. NetApp Volumes-Performance propose les options suivantes :
- **Correspondance client.** Liste d'adresses IP séparées par des virgules, liste de noms d'hôtes, de sous-réseaux, de groupes de réseaux, de noms de domaine séparés par des virgules.
- **Règles d'accès RO/RW.** Sélectionnez lecture/écriture ou lecture seule pour contrôler le niveau d'accès à l'exportation.
- **Accès root (activé/désactivé).** Configure le squash racine (voir la section «L'utilisateur root " pour plus de détails).
- **Type de protocole.** Cela limite l'accès au montage NFS à une version de protocole spécifique. Lorsque vous spécifiez à la fois NFSv3 et NFSv4.1 pour le volume, laissez les deux cases vides ou cochez les deux cases.
- **Niveau de sécurité Kerberos (lorsque l'option Activer Kerberos est sélectionnée).** Fournit les options krb5, krb5i et/ou krb5p pour un accès en lecture seule ou en lecture-écriture.

Changer de propriétaire (chown) et changer de groupe (chgrp)

NFS sur Google Cloud NetApp Volumes permet uniquement à l'utilisateur root d'exécuter chown/chgrp sur des fichiers et des dossiers. Les autres utilisateurs voient un `Operation not permitted` erreur, même sur les fichiers qui leur appartiennent. Si vous utilisez des racines de courge (comme indiqué dans la section «L'utilisateur root "), la racine est écrasée sur un utilisateur non root et n'est pas autorisée à accéder à chown et chgrp. Il n'existe actuellement aucune solution de contournement dans Google Cloud NetApp Volumes pour autoriser chown et chgrp pour les utilisateurs non root. Si des modifications de propriété sont nécessaires, 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

Google Cloud NetApp Volumes prend en charge les bits de mode (tels que 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 derniers (comme chmod, chown ou nfs4_setfacl) et fonctionne avec tout client Linux qui les prend en charge.

De plus, lors de l'utilisation de volumes à double protocole définis sur NTFS, les clients NFS peuvent exploiter le mappage de noms de Google Cloud NetApp Volumes vers les utilisateurs Windows, qui sont ensuite utilisés pour résoudre les autorisations NTFS. Cela nécessite une connexion LDAP à Google Cloud NetApp Volumes pour fournir des traductions d'ID numérique en nom d'utilisateur, car Google Cloud NetApp Volumes nécessite un nom d'utilisateur UNIX valide pour être correctement mappé à un nom d'utilisateur Windows.

Fournir des ACL granulaires pour NFSv3

Les autorisations de bits de mode couvrent uniquement le propriétaire, le groupe et tous les autres dans la sémantique, ce qui signifie qu'il n'existe aucun contrôle d'accès utilisateur granulaire en place pour NFSv3 de base. Google Cloud NetApp Volumes ne prend pas en charge les ACL POSIX, ni les attributs étendus (tels que chattr), donc les ACL granulaires ne sont possibles que dans les scénarios suivants avec NFSv3 :

- Volumes de style de sécurité NTFS (serveur CIFS requis) avec mappages utilisateur UNIX vers Windows valides.
- Les ACL NFSv4.1 sont appliquées à l'aide d'un client administrateur montant NFSv4.1 pour appliquer les ACL.

Les deux méthodes nécessitent une connexion LDAP pour la gestion des identités UNIX et des informations d'utilisateur et de groupe UNIX valides renseignées (voir la section"LDAP") et ne sont disponibles qu'avec les instances NetApp Volumes-Performance. Pour utiliser des volumes de style de sécurité NTFS avec NFS, vous devez utiliser un double protocole (SMB et NFSv3) ou un double protocole (SMB et NFSv4.1), même si aucune connexion SMB n'est établie. Pour utiliser les ACL NFSv4.1 avec les montages NFSv3, vous devez sélectionner `Both (NFSv3/NFSv4.1)` comme type de protocole.

Les bits de mode UNIX standard ne fournissent pas le même niveau de granularité dans les autorisations que les ACL NTFS ou NFSv4.x. Le tableau suivant compare la granularité des autorisations entre les bits du mode NFSv3 et les ACL NFSv4.1. Pour plus d'informations sur les ACL NFSv4.1, consultez "nfs4_acl - Listes de contrôle d'accès NFSv4" .

Bits du mode NFSv3	Listes de contrôle d'accès NFSv4.1
• Définir l'ID utilisateur lors de l'exécution • Définir l'ID de groupe lors de l'exécution • Enregistrer le texte échangé (non défini dans POSIX) • Autorisation de lecture pour le propriétaire • Autorisation d'écriture pour le propriétaire • Exécuter l'autorisation pour le propriétaire sur un fichier ; ou rechercher l'autorisation pour le propriétaire dans le répertoire • Autorisation de lecture pour le groupe • Autorisation d'écriture pour le groupe • Exécuter l'autorisation pour le groupe sur un fichier ; ou rechercher l'autorisation pour le groupe dans le répertoire • Autorisation de lecture pour les autres • Autorisation d'écriture pour les autres • Exécuter l'autorisation pour d'autres sur un fichier ; ou rechercher l'autorisation pour d'autres dans le répertoire	Types d'entrée de contrôle d'accès (ACE) (Autoriser/Refuser/Audit) * Indicateurs d'héritage * héritage de répertoire * héritage de fichier * héritage sans propagation * héritage uniquement Autorisations * read-data (fichiers) / list-directory (répertoires) * write-data (fichiers) / create-file (répertoires) * append-data (fichiers) / create-subdirectory (répertoires) * execute (fichiers) / change-directory (répertoires) * delete * delete-child * read-attributes * write-attributes * read-named-attributes * write-named-attributes * read-ACL * write-ACL * write-owner * Synchronize

Enfin, l'appartenance au groupe NFS (dans NFSv3 et NFSV4.x) est limitée à un maximum par défaut de 16 pour AUTH_SYS conformément aux limites des paquets RPC. NFS Kerberos fournit jusqu'à 32 groupes et les ACL NFSv4 suppriment la limitation au moyen d'ACL utilisateur et groupe granulaires (jusqu'à 1024 entrées

par ACE).

De plus, Google Cloud NetApp Volumes prend en charge un nombre étendu de groupes, jusqu'à 32. Cela nécessite une connexion LDAP à un serveur LDAP contenant des identités d'utilisateurs et de groupes UNIX valides. Pour plus d'informations sur cette configuration, consultez "Création et gestion des volumes NFS" dans la documentation Google.

ID utilisateur et groupe NFSv3

Les identifiants d'utilisateur et de groupe NFSv3 sont transmis sous forme d'identifiants numériques plutôt que de noms. Google Cloud NetApp Volumes ne résout pas le nom d'utilisateur pour ces ID numériques avec NFSv3, les volumes de style de sécurité UNIX utilisant uniquement des bits de mode. Lorsque des ACL NFSv4.1 sont présentes, une recherche d'ID numérique et/ou une recherche de chaîne de nom est nécessaire pour résoudre correctement l'ACL, même lors de l'utilisation de NFSv3. Avec les volumes de style de sécurité NTFS, Google Cloud NetApp Volumes doit résoudre un ID numérique en un utilisateur UNIX valide, puis mapper à un utilisateur Windows valide pour négocier les droits d'accès.

Limitations de sécurité des identifiants d'utilisateur et de groupe NFSv3

Avec NFSv3, le client et le serveur n'ont jamais besoin de confirmer que l'utilisateur qui tente une lecture ou une écriture avec un ID numérique est un utilisateur valide ; il est simplement implicitement approuvé. Cela ouvre le système de fichiers à des violations potentielles simplement en usurpant un identifiant numérique. Pour éviter des failles de sécurité comme celle-ci, plusieurs options sont disponibles pour Google Cloud NetApp Volumes.

- 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 pour obtenir un ticket Kerberos permettant l'accès à un montage. Kerberos est disponible avec les instances NetApp Volumes-Performance et uniquement avec NFSv4.1.
- La limitation de la liste des hôtes dans vos règles de stratégie d'exportation limite les clients NFSv3 ayant accès au volume Google Cloud NetApp Volumes .
- L'utilisation de volumes à double protocole et l'application d'ACL NTFS au volume obligent les clients NFSv3 à résoudre les ID numériques en noms d'utilisateur UNIX valides pour s'authentifier correctement afin d'accéder aux montages. Cela nécessite l'activation de LDAP et la configuration des identités d'utilisateur et de groupe UNIX.
- L'écrasement de l'utilisateur root limite les dommages qu'un utilisateur root peut causer à un montage NFS, mais ne supprime pas complètement le risque. Pour plus d'informations, consultez la section «L'utilisateur root ."

En fin de compte, la sécurité NFS est limitée à ce que propose la version du protocole que vous utilisez. NFSv3, bien que plus performant en général que NFSv4.1, n'offre pas le même niveau de sécurité.

NFSv4.1

NFSv4.1 offre une sécurité et une fiabilité supérieures à NFSv3, pour les raisons suivantes :

- Verrouillage intégré grâce à un mécanisme basé sur le bail
- Sessions avec état
- Toutes les fonctionnalités NFS sur un seul port (2049)
- TCP uniquement
- Mappage de domaine d'identification
- Intégration Kerberos (NFSv3 peut utiliser Kerberos, mais uniquement pour NFS, pas pour les protocoles

auxiliaires tels que NLM)

Dépendances NFSv4.1

En raison des fonctionnalités de sécurité supplémentaires de NFSv4.1, certaines dépendances externes sont impliquées et n'étaient pas nécessaires pour utiliser NFSv3 (de la même manière que SMB nécessite des dépendances telles qu'Active Directory).

Listes de contrôle d'accès NFSv4.1

Google Cloud NetApp Volumes prend en charge les ACL NFSv4.x, qui offrent des avantages distincts par rapport aux autorisations de style POSIX normales, tels que les suivants :

- Contrôle granulaire de l'accès des utilisateurs aux fichiers et répertoires
- Meilleure sécurité NFS
- Interopérabilité améliorée avec CIFS/SMB
- Suppression de la limitation NFS de 16 groupes par utilisateur avec la sécurité AUTH_SYS
- Les ACL contournent le besoin de résolution d'ID de groupe (GID), ce qui supprime efficacement la limite GID. Les ACL NFSv4.1 sont contrôlées à partir des clients NFS, et non à partir de Google Cloud NetApp Volumes. Pour utiliser les ACL NFSv4.1, assurez-vous que la version du logiciel de votre client les prend en charge et que les utilitaires NFS appropriés sont installés.

Compatibilité entre les ACL NFSv4.1 et les clients SMB

Les ACL NFSv4 sont différentes des ACL au niveau des fichiers Windows (ACL NTFS) mais possèdent des fonctionnalités similaires. Cependant, dans les environnements NAS multiprotocoles, si des ACL NFSv4.1 sont présentes et que vous utilisez un accès à double protocole (NFS et SMB sur les mêmes ensembles de données), les clients utilisant SMB2.0 et versions ultérieures ne pourront pas afficher ou gérer les ACL à partir des onglets de sécurité Windows.

Comment fonctionnent les ACL NFSv4.1

Pour référence, les termes suivants sont définis :

- **Liste de contrôle d'accès (ACL).** Une liste d'entrées d'autorisations.
- **Entrée de contrôle d'accès (ACE).** Une entrée d'autorisation dans la liste.

Lorsqu'un client définit une ACL NFSv4.1 sur un fichier lors d'une opération SETATTR, Google Cloud NetApp Volumes définit cette ACL sur l'objet, remplaçant toute ACL existante. S'il n'y a pas d'ACL sur un fichier, les autorisations de mode sur le fichier sont calculées à partir de OWNER@, GROUP@ et EVERYONE@. S'il existe des bits SUID/SGID/STICKY sur le fichier, ils ne sont pas affectés.

Lorsqu'un client obtient une ACL NFSv4.1 sur un fichier au cours d'une opération GETATTR, Google Cloud NetApp Volumes lit l'ACL NFSv4.1 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 est renvoyée au client.

L'accès est refusé si un DENY ACE est présent dans l'ACL ; l'accès est accordé si un ALLOW ACE existe. Cependant, l'accès est également refusé si aucun des ACE n'est présent dans l'ACL.

Un descripteur de sécurité se compose d'une ACL de sécurité (SACL) et d'une ACL discrétionnaire (DACL). Lorsque NFSv4.1 interagit avec CIFS/SMB, la DACL est mappée un à un avec NFSv4 et CIFS. La DACL se

compose des ACE ALLOW et DENY.

Si une base `chmod` est exécuté sur un fichier ou un dossier avec des ACL NFSv4.1 définies, les ACL d'utilisateur et de groupe existantes sont conservées, mais les ACL par défaut OWNER@, GROUP@, EVERYONE@ sont modifiées.

Un client utilisant les ACL NFSv4.1 peut définir et afficher les ACL pour les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire qui possède une ACL, cet objet hérite de toutes les ACE de l'ACL qui ont été marquées avec l' "drapeaux d'héritage" .

Si un fichier ou un répertoire possède une ACL NFSv4.1, cette ACL 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 ACL NFSv4 sur les répertoires parents (éventuellement avec les modifications appropriées) à condition que les ACE aient été marqués avec les indicateurs d'héritage corrects.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une demande NFSv4, l'ACL sur le fichier ou le répertoire résultant dépend du fait que la demande de création de fichier inclut une ACL ou uniquement des autorisations d'accès aux fichiers UNIX standard. L'ACL dépend également du fait que le répertoire parent possède ou non une ACL.

- Si la demande inclut une ACL, cette ACL est utilisée.
- Si la demande 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 demande inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent possède une ACL non héritable, une ACL par défaut basée sur les bits de mode transmis dans la demande est définie sur le nouvel objet.
- Si la demande inclut uniquement les 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 à condition que les ACE aient été marqués avec les indicateurs d'héritage appropriés.

Autorisations ACE

Les autorisations ACL NFSv4.1 utilisent une série de valeurs de lettres majuscules et minuscules (telles que `rxtncy`) pour contrôler l'accès. Pour plus d'informations sur ces valeurs de lettres, voir "COMMENT FAIRE : Utiliser l'ACL NFSv4" .

Comportement de l'ACL NFSv4.1 avec umask et héritage ACL

"Les ACL NFSv4 offrent la possibilité d'offrir l'héritage ACL" . L'héritage ACL signifie que les fichiers ou dossiers créés sous des objets avec des ACL NFSv4.1 définies peuvent hériter des ACL en fonction de la configuration du "Drapeau d'héritage ACL" .

"Umask"est utilisé pour contrôler le niveau d'autorisation auquel les fichiers et les dossiers sont créés dans un répertoire sans interaction de l'administrateur. Par défaut, Google Cloud NetApp Volumes permet à umask de remplacer les ACL héritées, ce qui est un comportement attendu selon "RFC 5661" .

Formatage ACL

Les ACL NFSv4.1 ont un formatage spécifique. L'exemple suivant est un ACE défini 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 « permettre ». Les indicateurs d'héritage 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 AUDIT, il n'est pas nécessaire de définir les indicateurs d'audit. Pour plus d'informations sur les ACL NFSv4.1, consultez "http://linux.die.net/man/5/nfs4_acl" .

Si l'ACL NFSv4.1 n'est pas définie correctement (ou si une chaîne de nom ne peut pas être résolue par le client et le serveur), l'ACL peut ne pas se comporter comme prévu ou la modification de l'ACL peut ne pas s'appliquer et générer une erreur.

Les exemples d'erreurs incluent :

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

REFUS explicite

Les autorisations NFSv4.1 peuvent inclure des attributs DENY explicites pour OWNER, GROUP et EVERYONE. C'est parce que les ACL NFSv4.1 sont refusées par défaut, ce qui signifie que si une ACL n'est pas explicitement accordée par une ACE, elle est refusée. Les attributs DENY explicites remplacent tous les ACE d'ACCÈS, explicites ou non.

Les ACE DENY sont définis avec une balise d'attribut de `D` .

Dans l'exemple ci-dessous, GROUP@ dispose de toutes les autorisations de lecture et d'exécution, mais se voit refuser 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
```

Les ACE DENY doivent être évités autant que possible car ils peuvent être déroutants et compliqués ; les ACL ALLOW qui ne sont pas explicitement définies sont implicitement refusées. Lorsque les ACE DENY sont définis, l'accès peut être refusé aux utilisateurs alors qu'ils s'attendent à ce qu'il leur soit accordé.

L'ensemble d'ACE précédent équivaut à 755 en bits de mode, ce qui signifie :

- Le propriétaire a tous les droits.
- Les groupes sont en lecture seule.
- D'autres ont seulement lu.

Cependant, même si les autorisations sont ajustées à l'équivalent 775, l'accès peut être refusé en raison du DENY explicite défini sur TOUT LE MONDE.

Dépendances de mappage de domaine d'identification NFSv4.1

NFSv4.1 exploite la logique de mappage de domaine d'ID comme couche de sécurité pour aider à vérifier qu'un utilisateur tentant d'accéder à un montage NFSv4.1 est bien celui qu'il prétend être. Dans ces cas, le nom d'utilisateur et le nom de groupe provenant du client NFSv4.1 ajoutent une chaîne de nom et l'envoient à l'instance Google Cloud NetApp Volumes . Si cette combinaison de nom d'utilisateur/nom de groupe et de chaîne d'identification ne correspond pas, l'utilisateur et/ou le groupe est alors écrasé par l'utilisateur nobody par défaut spécifié dans le `/etc/idmapd.conf` fichier sur le client.

Cette chaîne d'identification est une exigence pour le respect des autorisations, en particulier lorsque les ACL NFSv4.1 et/ou Kerberos sont utilisés. Par conséquent, les dépendances du serveur de service de noms, telles que les serveurs LDAP, sont nécessaires pour garantir la cohérence entre les clients et les Google Cloud NetApp Volumes pour une résolution appropriée de l'identité des noms d'utilisateur et de groupe.

Google Cloud NetApp Volumes utilise une valeur de nom de domaine d'ID statique par défaut de `defaultv4iddomain.com` . Les clients NFS utilisent par défaut le nom de domaine DNS pour leurs paramètres de nom de domaine d'ID, mais vous pouvez ajuster manuellement le nom de domaine d'ID dans `/etc/idmapd.conf` .

Si LDAP est activé dans Google Cloud NetApp Volumes, Google Cloud NetApp Volumes automatise le domaine d'ID NFS pour le modifier en fonction de ce qui est configuré pour le domaine de recherche dans DNS et les clients n'auront pas besoin d'être modifiés, sauf s'ils utilisent des noms de recherche de domaine DNS différents.

Lorsque Google Cloud NetApp Volumes peut résoudre un nom d'utilisateur ou un nom de groupe dans des fichiers locaux ou LDAP, la chaîne de domaine est utilisée et les ID de domaine non correspondants sont écrasés sur personne. Si Google Cloud NetApp Volumes 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 qu'il corresponde à celui utilisé par le volume Google Cloud NetApp Volumes , vous voyez le comportement suivant :

- Les utilisateurs et groupes UNIX avec des entrées locales dans Google Cloud NetApp Volumes (tels que root, tel que défini dans les utilisateurs et groupes UNIX locaux) sont écrasés sur la valeur nobody.
- Les utilisateurs et groupes UNIX avec des entrées dans LDAP (si Google Cloud NetApp Volumes est configuré pour utiliser LDAP) sont écrasés par personne si les domaines DNS sont différents entre les clients NFS et Google Cloud NetApp Volumes.
- Les utilisateurs et groupes UNIX sans entrées locales ou entrées LDAP utilisent la valeur d'ID numérique et se résolvent en nom spécifié sur le client NFS. Si aucun nom n'existe sur le client, seul l'ID numérique est affiché.

Ce qui suit montre 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 à quoi ressemble 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 comment le résoudre, consultez la section «NFSv4.1 et l'utilisateur/groupe nobody ."

Dépendances Kerberos

Si vous prévoyez d'utiliser Kerberos avec NFS, vous devez disposer des éléments suivants avec Google Cloud NetApp Volumes:

- Domaine Active Directory pour les services du centre de distribution Kerberos (KDC)
- Domaine Active Directory avec attributs utilisateur et groupe renseignés avec des informations UNIX pour la fonctionnalité LDAP (NFS Kerberos dans Google Cloud NetApp Volumes nécessite un mappage utilisateur SPN vers UNIX pour une fonctionnalité appropriée.)
- LDAP activé sur l'instance Google Cloud NetApp Volumes
- Domaine Active Directory pour les services DNS

NFSv4.1 et l'utilisateur/groupe nobody

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` comme étant la propriété de `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 bon propriétaire, 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 du `nfsnobody` utilisateur. Vous pouvez voir comment 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` fichier et peut être défini comme n'importe quel utilisateur que vous souhaitez utiliser.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Pourquoi cela arrive-t-il ?

Étant donné que la sécurité via le 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 transférer cet utilisateur vers un utilisateur qui n'aura normalement aucun accès aux fichiers et dossiers appartenant aux utilisateurs et aux groupes.

Quand tu vois `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 à la casse peut entrer en jeu ici.

Par exemple, si user1@CVSDEMO.LOCAL (uid 1234, gid 1234) accède à une exportation, Google Cloud NetApp Volumes doit pouvoir trouver user1@CVSDEMO.LOCAL (uid 1234, gid 1234). Si l'utilisateur dans Google Cloud NetApp Volumes est USER1@CVSDEMO.LOCAL, il ne correspondra pas (USER1 majuscule contre user1 minuscule). 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 bien 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 Google Cloud NetApp Volumes voit.

- **Domaine d'identification NFSv4.x.** Client: `idmapd.conf` fichier ; Google Cloud NetApp Volumes utilise `defaultv4iddomain.com` et ne peut pas être modifié manuellement. Si vous utilisez LDAP avec NFSv4.1, Google Cloud NetApp Volumes modifie le domaine d'ID en fonction de celui utilisé par le domaine de recherche DNS, qui est le même que le domaine AD.
- **Nom d'utilisateur et identifiants numériques.** Cela détermine où le client recherche les noms d'utilisateur et exploite la configuration du commutateur de service de noms : client : `nsswitch.conf` et/ou les fichiers de mot de passe et de groupe locaux ; Google Cloud NetApp Volumes n'autorise pas de modifications à ce sujet, mais ajoute automatiquement LDAP à la configuration lorsqu'il est activé.
- **Nom du groupe et identifiants numériques.** Cela détermine où le client recherche les noms de groupe et exploite la configuration du commutateur de service de noms : client : `nsswitch.conf` et/ou les fichiers de mot de passe et de groupe locaux ; Google Cloud NetApp Volumes n'autorise pas de modifications à ce sujet, mais ajoute automatiquement LDAP à la configuration lorsqu'il est activé.

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 du nom d'utilisateur ou de groupe entre Google Cloud NetApp Volumes et le client NFS. Pour éviter ce scénario, utilisez LDAP pour résoudre les informations utilisateur et groupe entre les clients et Google Cloud NetApp Volumes.

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 pendant les opérations NFS, comme décrit précédemment.

En plus d'utiliser `/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 correctement mappés au domaine NFSv4.

Par exemple, voici la sortie de la commande après qu'un utilisateur qui peut être trouvé par le client et Google Cloud NetApp Volumes 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 ne se mappe pas correctement dans le domaine d'ID NFSv4.1 (dans ce cas, `netapp-user`) essaie d'accéder au même montage et touche un fichier, ils sont attribués `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 montre à l'utilisateur `pcuser` dans l'affichage mais pas `netapp-user` ; il s'agit de l'utilisateur anonyme dans notre règle de politique d'exportation(`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 centralisée des utilisateurs/groupes, des autorisations, le verrouillage et le partage de fichiers à plusieurs clients SMB sur un réseau Ethernet. Les fichiers et les dossiers sont présentés aux clients sous forme de partages, qui peuvent être configurés avec diverses propriétés de partage et offrent un contrôle d'accès via des autorisations au niveau du partage. SMB peut être présenté à tout client prenant en charge le protocole, y compris les clients Windows, Apple et Linux.

Google Cloud NetApp Volumes 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 Google Cloud NetApp Volumes , Google Cloud NetApp Volumes recherche un nom d'utilisateur UNIX à l'aide des méthodes configurées par les administrateurs Google Cloud NetApp Volumes .
- Si un fournisseur d'identité UNIX externe (LDAP) est configuré et que les noms d'utilisateur Windows/UNIX sont identiques, les noms d'utilisateur Windows seront mappés 1:1 aux noms d'utilisateur UNIX sans aucune configuration supplémentaire nécessaire. Lorsque LDAP est activé, Active Directory est utilisé pour héberger ces attributs UNIX pour les objets utilisateur et groupe.

- Si les noms Windows et les noms UNIX ne correspondent pas de manière identique, LDAP doit être configuré pour permettre à Google Cloud NetApp Volumes d'utiliser la configuration de mappage de noms LDAP (voir la section"Utilisation de LDAP pour le mappage de noms asymétriques").
- Si LDAP n'est pas utilisé, les utilisateurs Windows SMB sont mappés à un utilisateur UNIX local par défaut nommé `pcuser` dans Google Cloud NetApp Volumes. Cela signifie que les fichiers écrits dans Windows par les utilisateurs correspondent au `pcuser` afficher la propriété UNIX comme `pcuser` dans les environnements NAS multiprotocoles. `pcuser` voici effectivement le `nobody` utilisateur dans les environnements Linux (UID 65534).

Dans les déploiements avec SMB uniquement, le `pcuser` le mappage se produit toujours, mais cela n'aura pas d'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 du nom d'utilisateur avec les contrôleurs de domaine Active Directory, ce qui nécessite un échange de nom d'utilisateur/mot de passe avec les contrôleurs de domaine AD, qui est externe à l'instance Google Cloud NetApp Volumes . L'authentification Kerberos est utilisée lorsque le `\\SERVERNAME` Le chemin UNC est utilisé par les clients SMB et ce qui suit est vrai :

- Une entrée DNS A/AAAA existe pour SERVERNAME
- Un SPN valide pour l'accès SMB/CIFS existe pour SERVERNAME

Lorsqu'un volume SMB Google Cloud NetApp Volumes est créé, le nom du compte machine est créé comme défini dans la section"Comment Google Cloud NetApp Volumes s'affiche dans Active Directory." Ce nom de compte machine devient également le chemin d'accès au partage SMB, car Google Cloud NetApp Volumes exploite Dynamic DNS (DDNS) pour créer les entrées A/AAAA et PTR nécessaires dans DNS et les entrées SPN nécessaires sur le principal du compte machine.

Pour que les entrées PTR soient créées, la zone de recherche inversée pour l'adresse IP de l'instance Google Cloud NetApp Volumes doit exister sur le serveur DNS.

Par exemple, ce volume Google Cloud NetApp Volumes utilise le chemin de partage UNC suivant : `\\cvs-east- 433d.cvsdemo.local` .

Dans Active Directory, voici les entrées SPN générées par Google Cloud NetApp 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
```

Voici le résultat de la recherche DNS directe/inverse :

```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-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
```

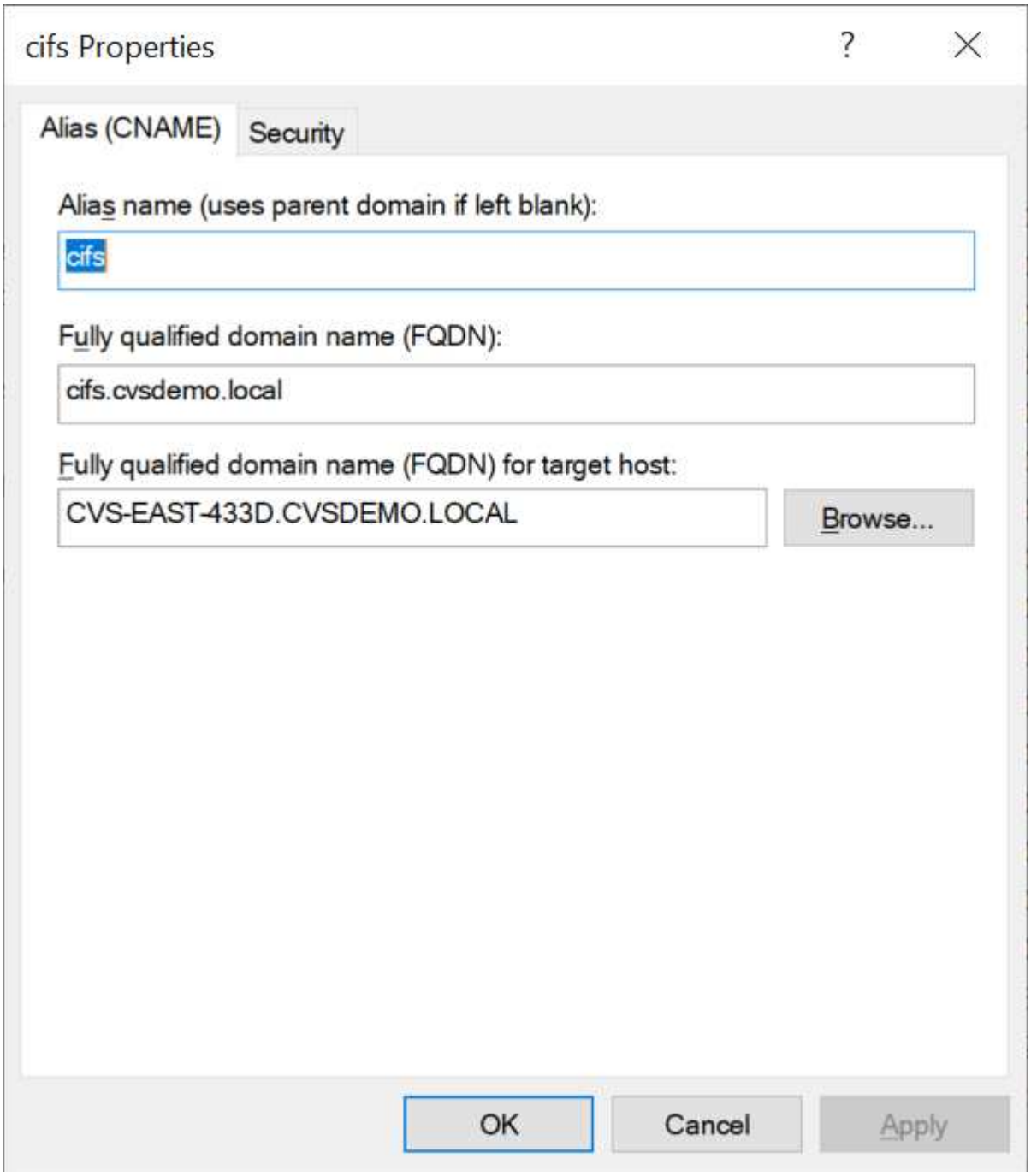
```
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

En option, un contrôle d'accès plus strict peut être appliqué en activant/exigeant le chiffrement SMB pour les partages SMB dans Google Cloud NetApp Volumes. Si le chiffrement SMB n'est pas pris en charge par l'un des points de terminaison, l'accès n'est pas autorisé.

Utilisation des alias de noms SMB

Dans certains cas, il peut s'agir d'un problème de sécurité pour les utilisateurs finaux de connaître le nom du compte machine utilisé pour Google Cloud NetApp Volumes. Dans d'autres cas, vous souhaiterez peut-être simplement fournir un chemin d'accès plus simple à vos utilisateurs finaux. Dans ces cas, vous pouvez créer des alias SMB.

Si vous souhaitez créer des alias pour le chemin de partage SMB, vous pouvez exploiter ce que l'on appelle un enregistrement CNAME dans DNS. Par exemple, si vous souhaitez utiliser le nom `\\CIFS` pour accéder aux actions 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.



Voici le résultat de la recherche DNS directe 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:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Voici la requête SPN résultante 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 paquet, nous pouvons voir la demande de configuration de session à l'aide du SPN lié 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

Google Cloud NetApp Volumes 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 puissiez utiliser. Avec le cryptage AES et SMB activé, le niveau de sécurité est encore augmenté.

Google Cloud NetApp Volumes prend également en charge la compatibilité descendante 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). Étant donné que ces mécanismes sont moins sécurisés, ils sont désactivés dans certains environnements Active Directory. Si les méthodes d'authentification plus faibles sont désactivées et que Kerberos n'est pas configuré correctement, l'accès au partage échoue car il n'existe aucune méthode d'authentification valide vers laquelle se rabattre.

Pour plus d'informations sur la configuration/l'affichage de vos niveaux d'authentification pris en charge dans Active Directory, consultez "Sécurité du réseau : niveau d'authentification du gestionnaire LAN" .

Modèles d'autorisation

Autorisations NTFS/Fichiers

Les autorisations NTFS sont les autorisations appliquées aux fichiers et dossiers dans les systèmes de fichiers adhérant à la logique NTFS. Vous pouvez appliquer des autorisations NTFS dans `Basic` ou `Advanced` et peut être réglé sur `Allow` ou `Deny` pour le contrôle d'accès.

Les autorisations de base incluent les éléments suivants :

- Contrôle total
- Modifier
- Lire et exécuter
- Lire
- Écrire

Lorsque vous définissez des autorisations pour un utilisateur ou un groupe, appelé ACE, elles résident dans une ACL. Les autorisations NTFS utilisent les mêmes bases de 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 la prise de possession, la création de dossiers/l'ajout de données, l'écriture d'attributs, etc.

Les bits du mode UNIX standard ne fournissent pas le même niveau de granularité que les autorisations NTFS (comme la possibilité de définir des autorisations pour des objets utilisateur et groupe individuels dans une ACL ou de définir des attributs étendus). Cependant, les ACL NFSv4.1 fournissent les mêmes fonctionnalités que les ACL 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 à un utilisateur ou à un groupe remplacent même le contrôle total lors de la définition des droits d'accès.

Les autorisations NTFS sont contrôlées à partir des clients Windows SMB.

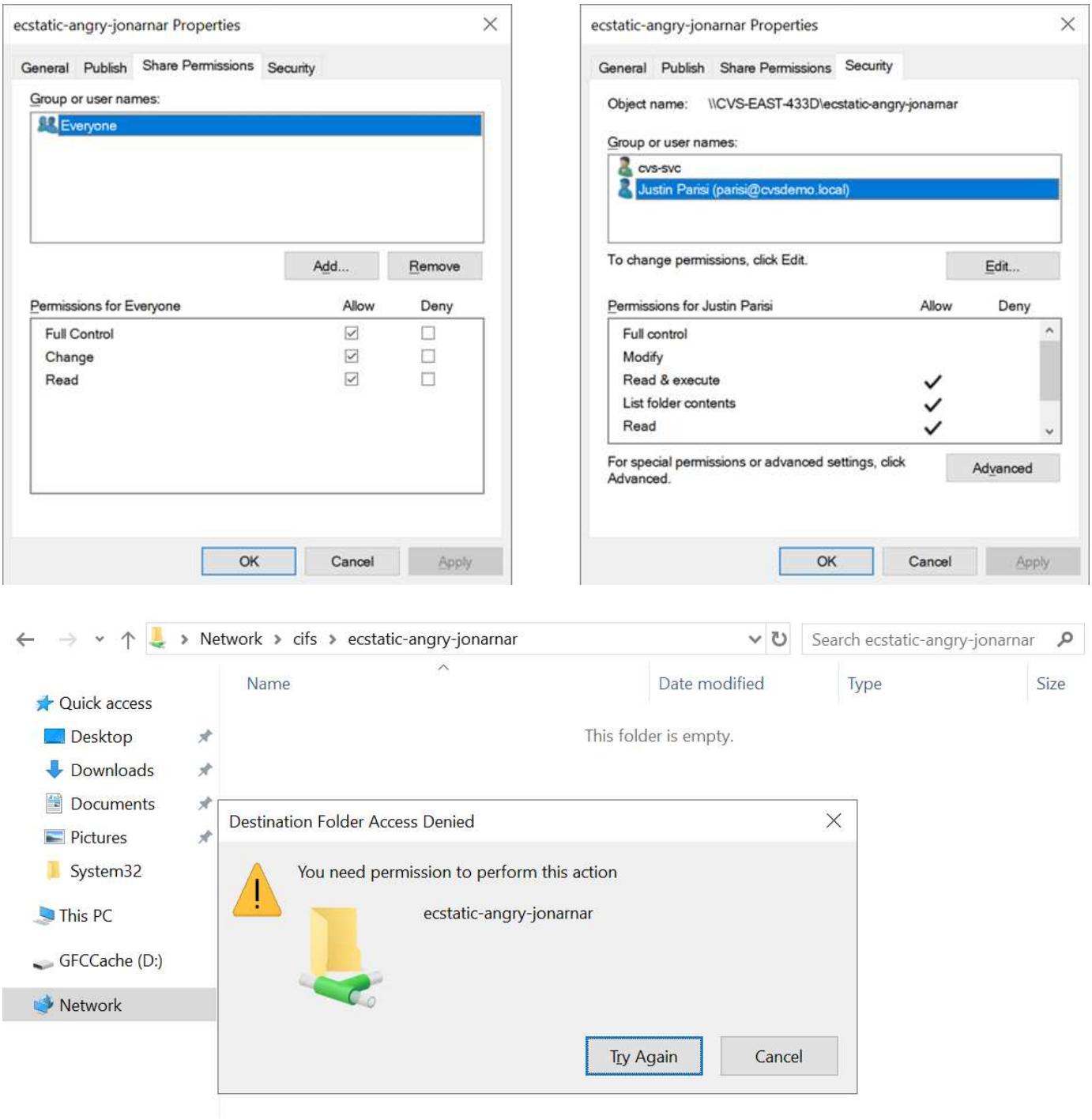
Autorisations de partage

Les autorisations de partage sont plus générales que les autorisations NTFS (lecture/modification/contrôle total uniquement) et contrôlent l'entrée initiale dans un partage SMB, de la même manière que fonctionnent les règles de stratégie d'exportation NFS.

Bien que les règles de stratégie d'exportation NFS contrôlent l'accès via des informations basées sur l'hôte telles que les adresses IP ou les noms d'hôte, les autorisations de partage SMB peuvent contrôler l'accès à l'aide des 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 à partir du client Windows ou de l'interface utilisateur de gestion de Google Cloud NetApp Volumes .

Par défaut, les listes de contrôle d'accès de partage et les listes de contrôle d'accès de volume initiales incluent Tout le monde avec un contrôle total. Les ACL des fichiers doivent être modifiées, mais les autorisations de partage sont remplacées par les autorisations de fichier sur les objets du partage.

Par exemple, si un utilisateur est uniquement autorisé à accéder en lecture à l'ACL du fichier de volume Google Cloud NetApp Volumes , l'accès à la création de fichiers et de dossiers lui est refusé, même si l'ACL de partage est définie sur Tout le monde avec un contrôle total, comme illustré dans la figure suivante.



Pour de meilleurs résultats en matière de sécurité, procédez comme suit :

- Supprimez tout le monde des listes de contrôle d'accès aux fichiers et aux partages et définissez plutôt l'accès au partage pour les utilisateurs ou les groupes.
- Utilisez des groupes pour le contrôle d'accès au lieu d'utilisateurs individuels pour faciliter la gestion et accélérer la suppression/l'ajout d'utilisateurs afin de partager les ACL via la gestion de groupe.
- Autorisez un accès de partage moins restrictif et plus général aux ACE sur 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 ACL de refus explicites, car elles remplacent les ACL d'autorisation. Limitez l'utilisation des listes de contrôle d'accès de refus explicites pour les utilisateurs ou les groupes qui doivent

être rapidement restreints dans leur accès à un système de fichiers.

- Assurez-vous de faire attention à la "Héritage ACL" paramètres lors de la modification des autorisations ; définir 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 a des autorisations héritées qui lui sont ajoutées, ce qui peut créer un comportement indésirable tel qu'un accès/refus involontaire et une longue période de modification des autorisations à mesure que chaque fichier est ajusté.

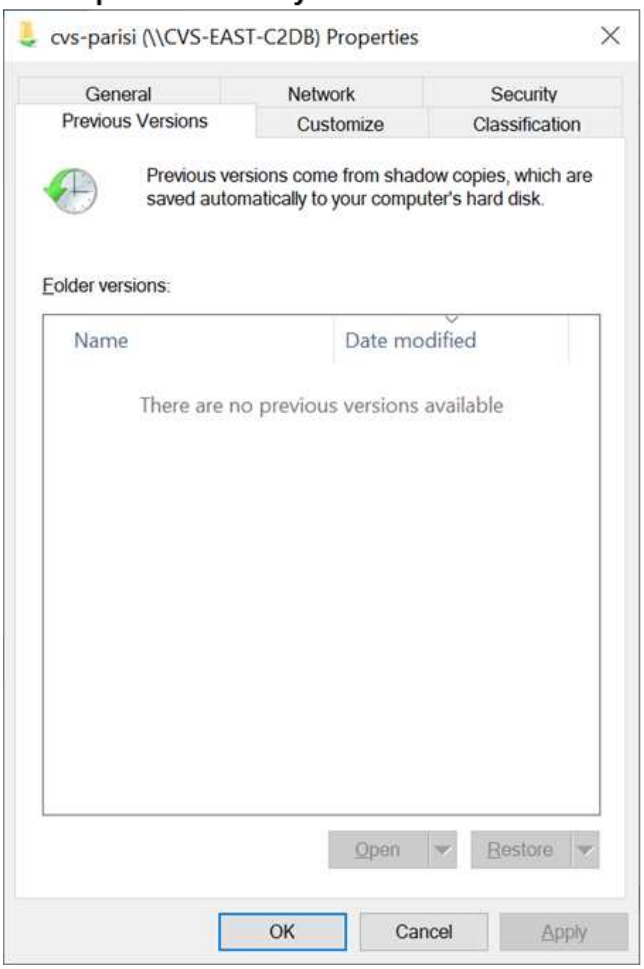
Fonctionnalités de sécurité du partage SMB

Lorsque vous créez pour la première fois un volume avec accès SMB dans Google Cloud NetApp Volumes, une série de choix vous sont proposés pour sécuriser ce volume.

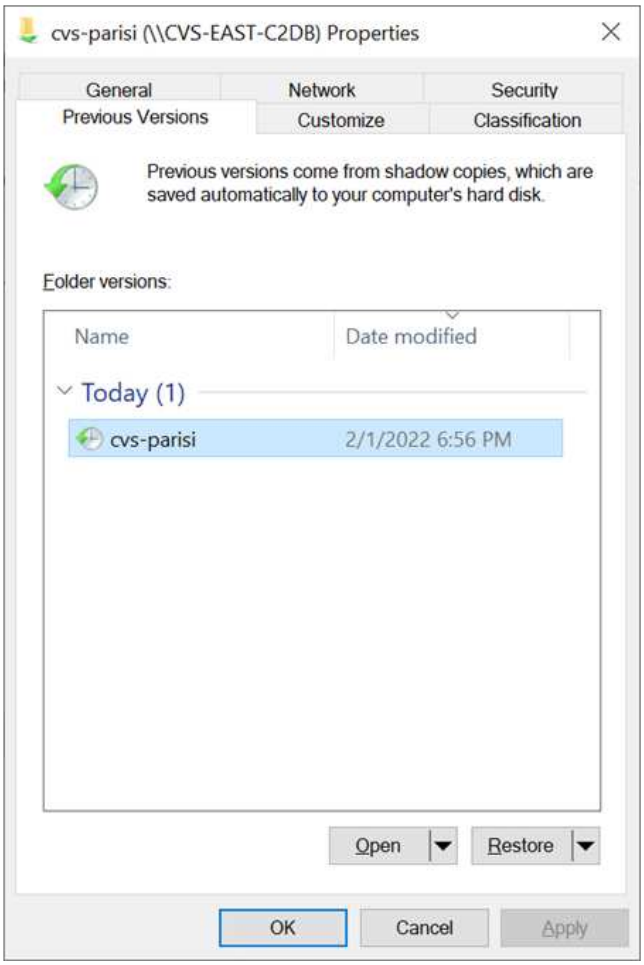
Certains de ces choix dépendent du niveau de Google Cloud NetApp Volumes (Performances ou Logiciel) et les choix incluent :

- **Rendre le répertoire des instantanés visible (disponible pour NetApp Volumes-Performance et NetApp Volumes-SW).** Cette option contrôle si les clients SMB peuvent ou non accéder au répertoire Snapshot dans un partage SMB(`\\server\share\~snapshot` et/ou onglet Versions précédentes). Le paramètre par défaut est Non coché, ce qui signifie que le volume est masqué par défaut et interdit l'accès au `~snapshot` répertoire et aucune copie instantanée n'apparaît dans l'onglet Versions précédentes pour le volume.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Masquer les copies Snapshot aux utilisateurs finaux peut être souhaité pour des raisons de sécurité, de performances (masquer ces dossiers des analyses AV) ou par préférence. Les instantanés Google Cloud

NetApp Volumes sont en lecture seule. Ainsi, même si ces instantanés sont visibles, les utilisateurs finaux ne peuvent pas supprimer ou modifier les fichiers du répertoire Instantanés. Les autorisations de fichiers sur les fichiers ou dossiers au moment où la copie instantanée a été prise s'appliquent. 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. Bien que les suppressions ou modifications de fichiers dans le répertoire Snapshot ne soient pas possibles, il est possible de copier des fichiers ou des dossiers hors du répertoire Snapshot.

- **Activer le chiffrement SMB (disponible pour NetApp Volumes-Performance et NetApp Volumes-SW).** Le cryptage SMB est désactivé sur le partage SMB par défaut (non coché). Cocher la case active le cryptage SMB, ce qui signifie que le trafic entre le client SMB et le serveur est crypté en vol avec les niveaux de cryptage les plus élevés pris en charge négociés. Google Cloud NetApp Volumes prend en charge le chiffrement jusqu'à AES-256 pour SMB. L'activation du chiffrement SMB entraîne une baisse des performances qui peut être perceptible ou non par vos clients SMB, de l'ordre de 10 à 20 %. NetApp encourage fortement les tests pour voir si cette baisse de performance est acceptable.
- **Masquer le partage SMB (disponible pour NetApp Volumes-Performance et NetApp Volumes-SW).** La définition de cette option masque le chemin de partage SMB de la navigation normale. Cela signifie que les clients qui ne connaissent pas le chemin de partage ne peuvent pas voir les partages lorsqu'ils accèdent au chemin UNC par défaut (tel que `\\NetApp Volumes-SMB`). Lorsque la case à cocher est sélectionnée, seuls les clients qui connaissent explicitement le chemin de partage SMB ou dont le chemin de partage est défini par un objet de stratégie de groupe peuvent y accéder (sécurité par obscurcissement).
- **Activer l'énumération basée sur l'accès (ABE) (NetApp Volumes-SW uniquement).** Cela est similaire au masquage du partage SMB, sauf que les partages ou les fichiers sont uniquement masqués aux utilisateurs ou aux groupes qui n'ont pas les autorisations d'accéder aux objets. Par exemple, si l'utilisateur Windows `joe` n'est pas autorisé au moins l'accès en lecture via les autorisations, puis l'utilisateur Windows `joe` je ne peux pas voir le partage SMB ou les fichiers du tout. Cette option est désactivée par défaut et vous pouvez l'activer en cochant la case. Pour plus d'informations sur ABE, consultez l'article de la base de connaissances NetApp "Comment fonctionne l'énumération basée sur l'accès (ABE) ?"
- **Activer la prise en charge du partage disponible en continu (CA) (NetApp Volumes-Performance uniquement).** "Partages PME disponibles en continu" fournir un moyen de minimiser les interruptions d'application lors des événements de basculement en répliquant les états de verrouillage sur les nœuds du système backend Google Cloud NetApp Volumes . 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 cachés par défaut

Lorsqu'un serveur SMB est créé dans Google Cloud NetApp Volumes, il existe "partages administratifs cachés" (en utilisant la convention de nommage $) qui sont créés en plus du partage SMB du volume de données. Il s'agit notamment de C$ (accès à l'espace de noms) et d'IPC$ (partage de canaux nommés pour la communication entre les programmes, tels que les appels de procédure à distance (RPC) utilisés pour l'accès à la console de gestion Microsoft (MMC)).

Le partage IPC$ ne contient aucune ACL de partage et ne peut pas être modifié. Il est strictement utilisé pour les appels RPC et "Windows interdit par défaut l'accès anonyme à ces partages" .

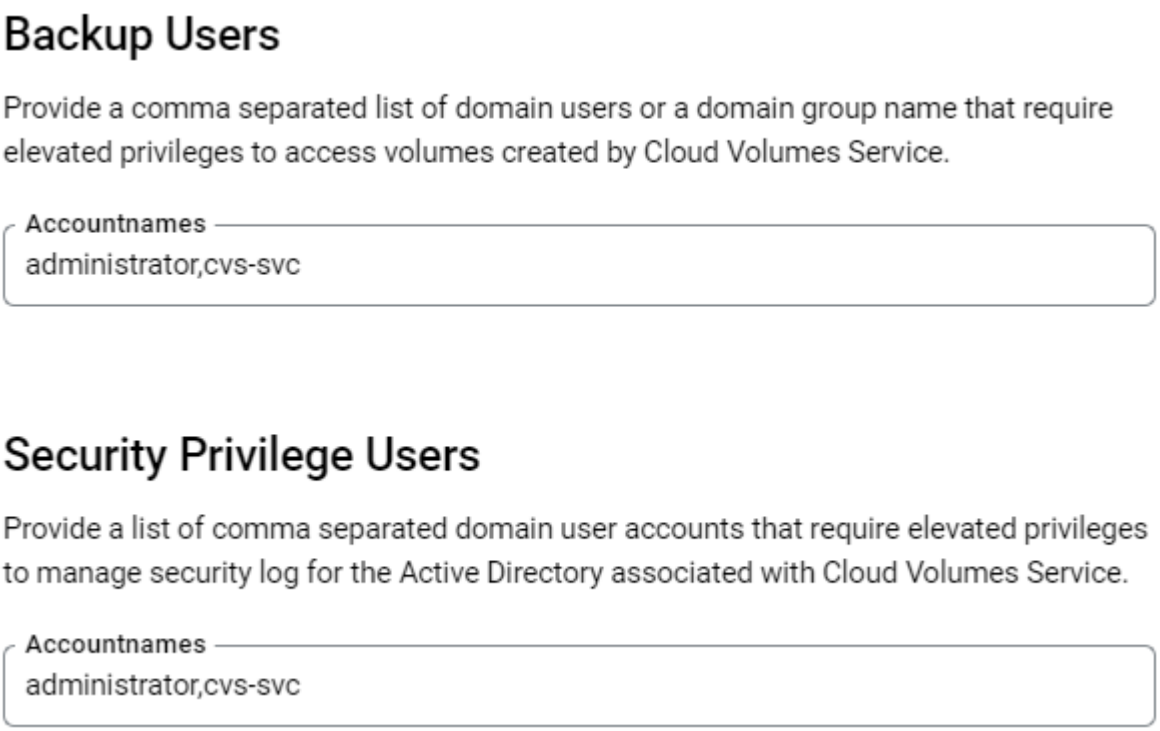
Le partage C$ permet l'accès BUILTIN/Administrateurs par défaut, mais l'automatisation de Google Cloud NetApp Volumes supprime l'ACL de partage et n'autorise l'accès à personne, car l'accès au partage C$ permet une visibilité sur tous les volumes montés dans les systèmes de fichiers Google Cloud NetApp Volumes . En conséquence, les tentatives de navigation vers `\\SERVER\C$` échouer.

Comptes avec droits d'administrateur/de sauvegarde locaux/INTÉGRÉS

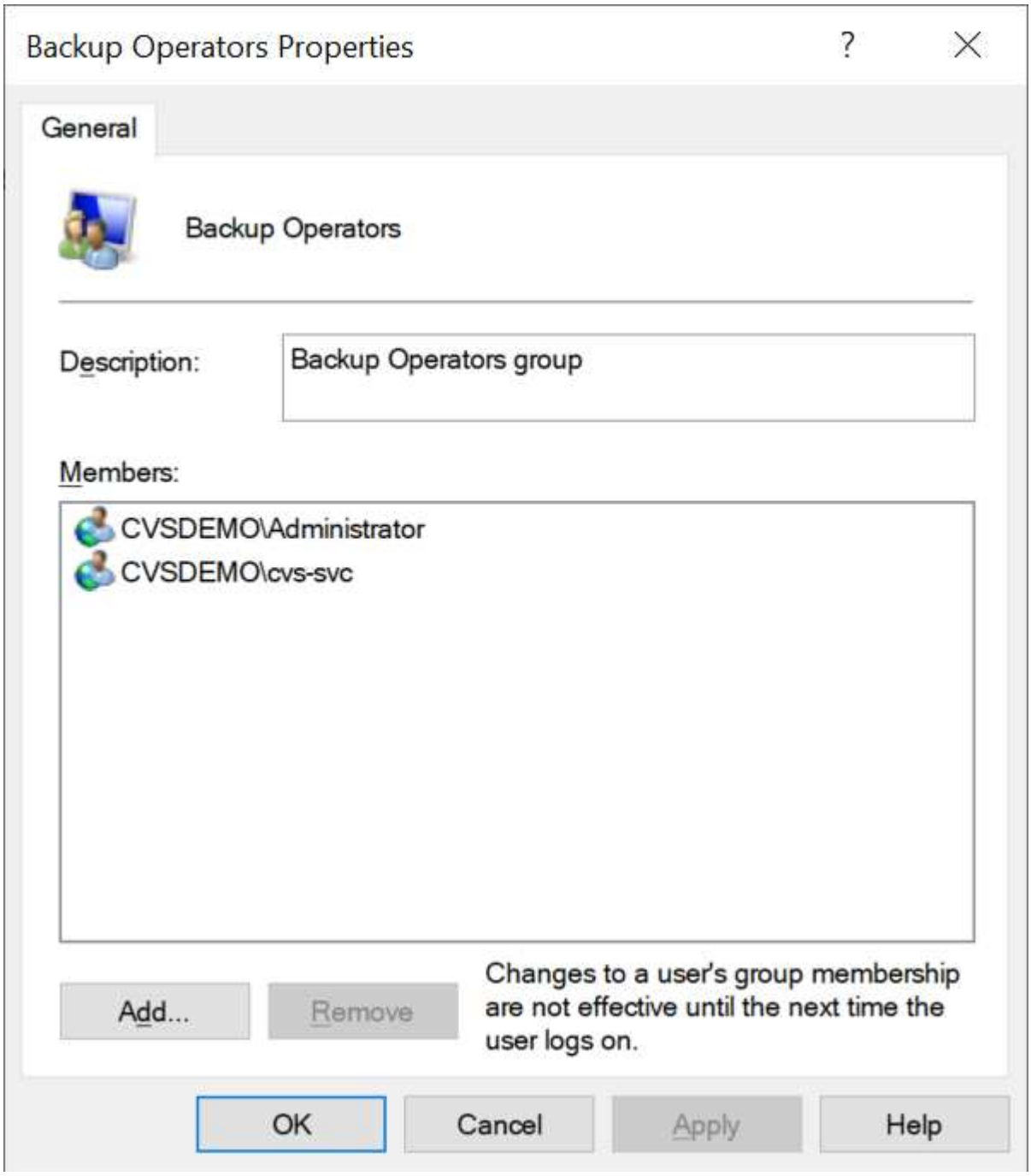
Les serveurs SMB Google Cloud NetApp Volumes conservent des fonctionnalités similaires aux serveurs SMB Windows classiques dans la mesure où il existe des groupes locaux (tels que BUILTIN\Administrators) qui appliquent des droits d'accès pour sélectionner des utilisateurs et des groupes de domaine.

Lorsque vous spécifiez un utilisateur à ajouter aux utilisateurs de sauvegarde, l'utilisateur est ajouté au groupe BUILTIN\Backup Operators dans l'instance Google Cloud NetApp Volumes qui utilise cette connexion Active Directory, qui obtient ensuite le "SeBackupPrivilege et SeRestorePrivilege" .

Lorsque vous ajoutez un utilisateur aux utilisateurs avec privilèges de sécurité, l'utilisateur reçoit le SeSecurityPrivilege, ce qui est utile dans certains cas d'utilisation d'application, tels que "SQL Server sur les partages SMB" .



Vous pouvez afficher les appartenances aux groupes locaux Google Cloud NetApp Volumes via la console MMC avec les privilèges appropriés. La figure suivante montre les utilisateurs qui ont été ajoutés à l'aide de la console Google Cloud NetApp Volumes .

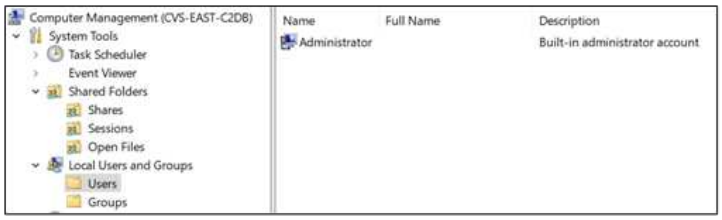


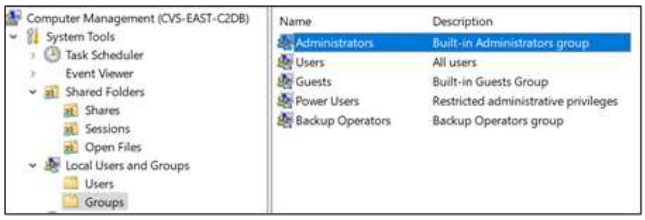
Le tableau suivant montre la liste des groupes BUILTIN par défaut et les utilisateurs/groupes ajoutés par défaut.

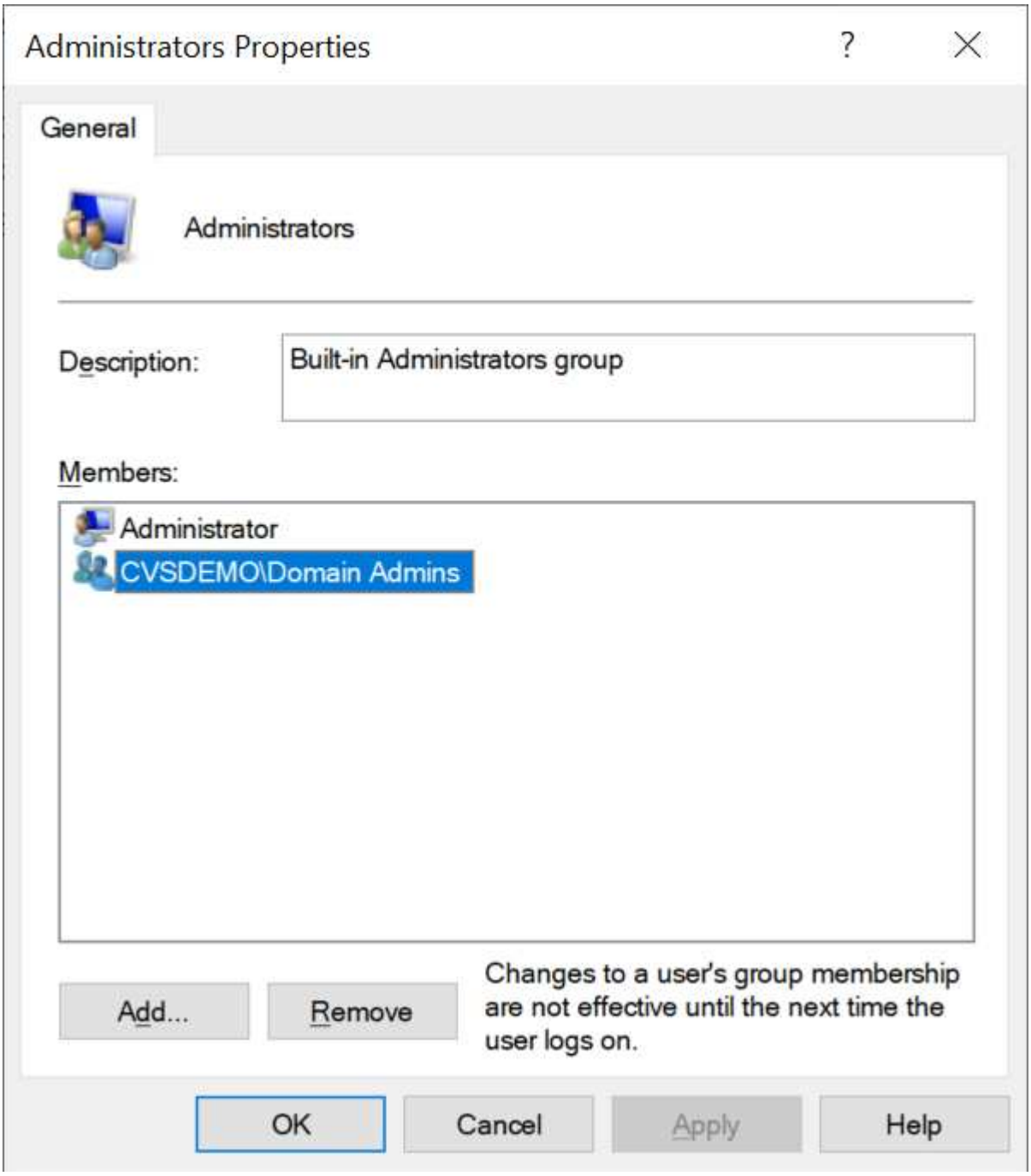
Groupe local/BUILTIN	Membres par défaut
BUILTIN\Administrateurs*	DOMAINE\Administrateurs de domaine
Opérateurs de sauvegarde BUILTIN*	Aucune
BUILTIN\Invités	DOMAINE\Invités du domaine
Utilisateurs expérimentés intégrés	Aucune
Utilisateurs du domaine BUILTIN\Domain	DOMAINE\Utilisateurs du domaine

*L’appartenance au groupe est contrôlée dans la configuration de connexion Active Directory de Google Cloud NetApp Volumes .

Vous pouvez afficher les utilisateurs et les groupes locaux (et les membres du groupe) dans la fenêtre MMC, mais vous ne pouvez pas ajouter ou supprimer des objets ni modifier les appartenances aux groupes à partir de cette console. Par défaut, seuls le groupe Administrateurs de domaine et l’administrateur sont ajoutés au groupe BUILTIN\Administrators dans Google Cloud NetApp Volumes. Actuellement, vous ne pouvez pas modifier cela.







Accès MMC/Gestion de l'ordinateur

L'accès SMB dans Google Cloud NetApp Volumes fournit une connectivité à la console MMC de gestion de l'ordinateur, qui vous permet d'afficher les partages, de gérer les listes de contrôle d'accès (ACL) de partage et d'afficher/gérer les sessions SMB et d'ouvrir des fichiers.

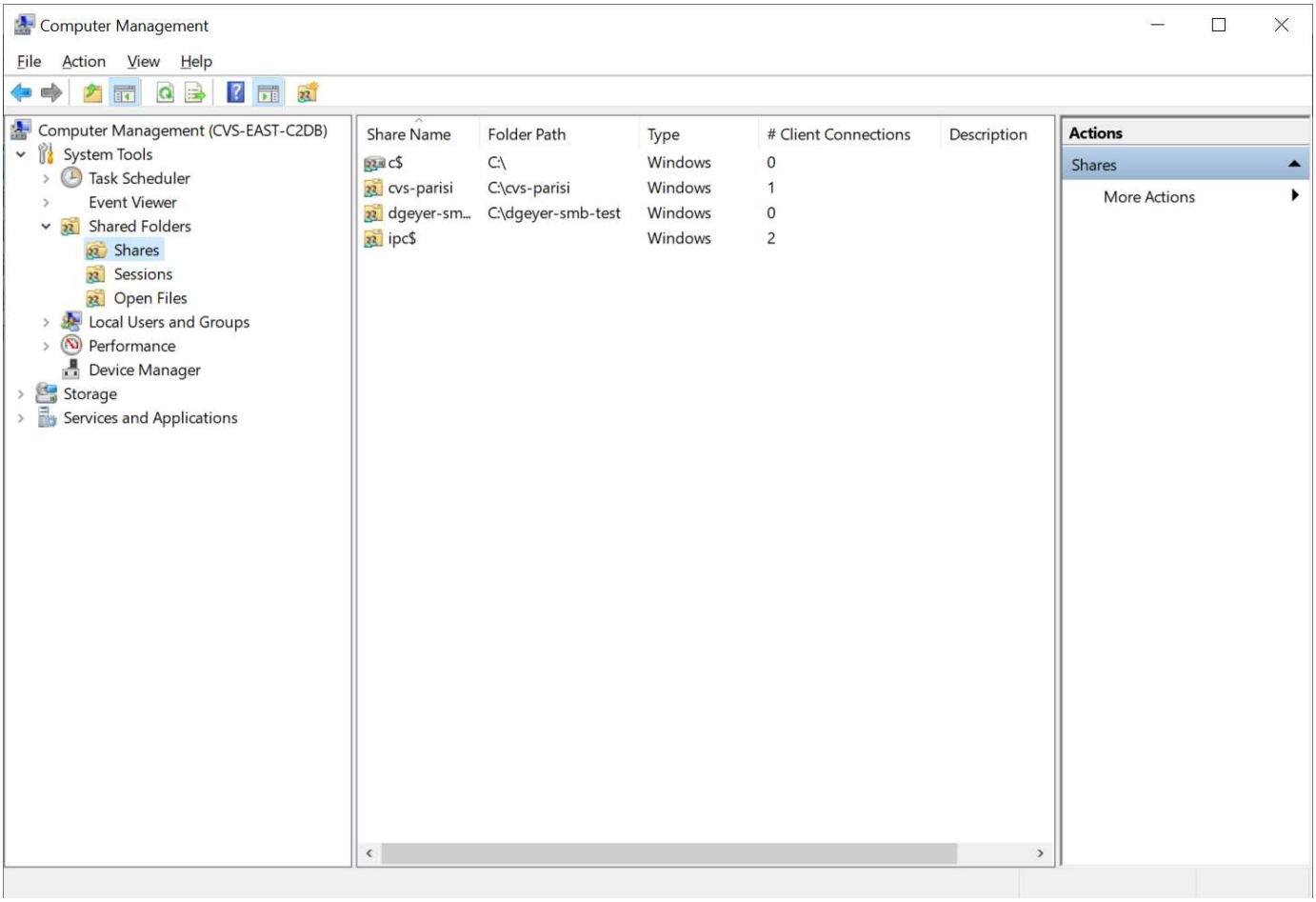
Pour utiliser la console MMC afin d'afficher les partages et sessions SMB dans Google Cloud NetApp Volumes, l'utilisateur actuellement connecté doit être un administrateur de domaine. D'autres utilisateurs sont autorisés à accéder à l'affichage ou à la gestion du serveur SMB à partir de MMC et reçoivent une boîte de dialogue Vous n'avez pas d'autorisations lorsqu'ils tentent d'afficher des partages ou des sessions sur l'instance SMB de Google Cloud NetApp Volumes .

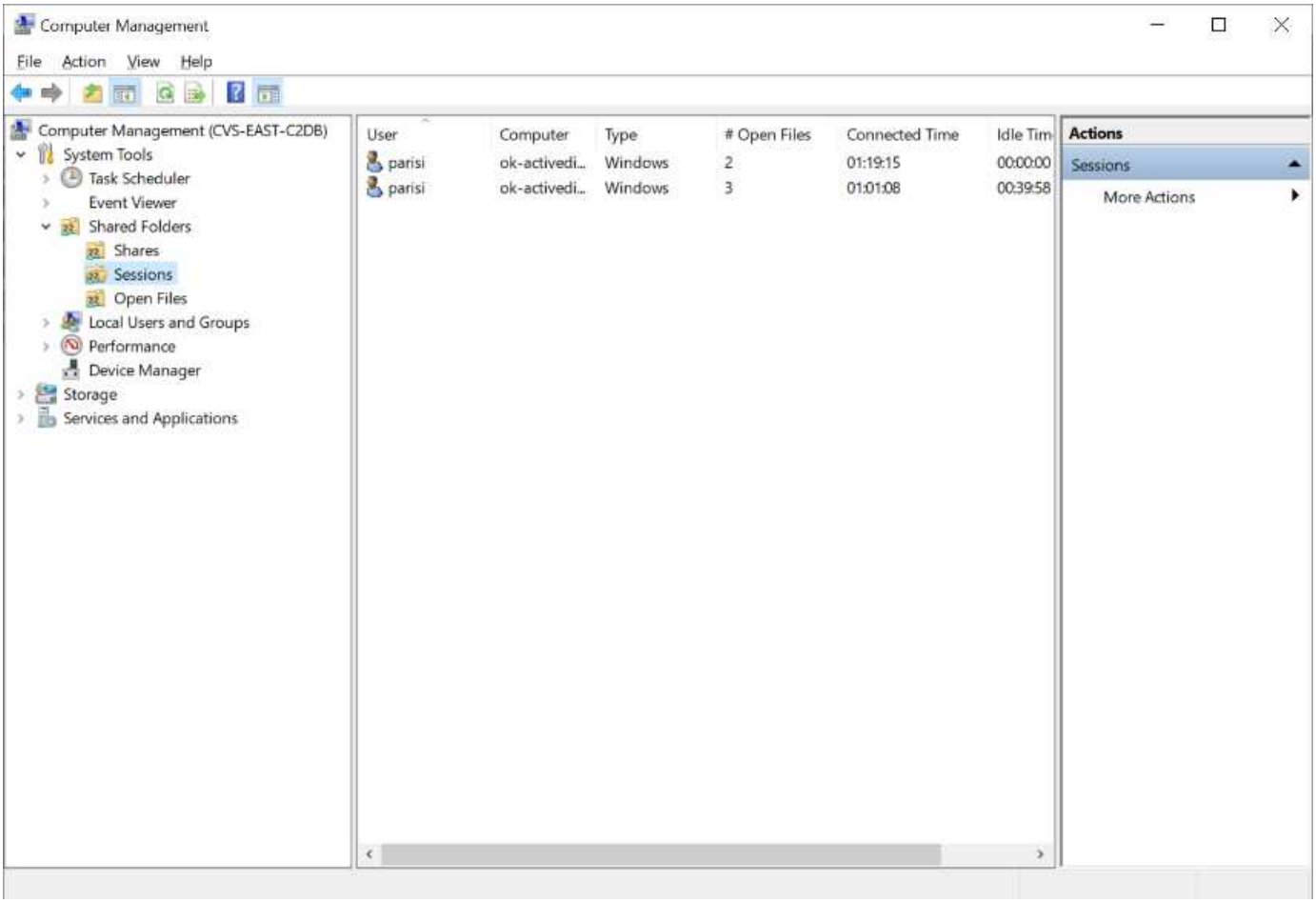
Pour vous connecter au serveur SMB, ouvrez Gestion de l'ordinateur, cliquez avec le bouton droit sur Gestion de l'ordinateur, puis sélectionnez Se connecter à un autre ordinateur. Cela ouvre la boîte de dialogue

Sélectionner un ordinateur dans laquelle vous pouvez saisir le nom du serveur SMB (trouvé dans les informations de volume Google Cloud NetApp Volumes).

Lorsque vous affichez les partages SMB avec les autorisations appropriées, vous voyez tous les partages disponibles dans l'instance Google Cloud NetApp Volumes qui partagent la connexion Active Directory. Pour contrôler ce comportement, définissez l'option Masquer les partages SMB sur l'instance de volume Google Cloud NetApp Volumes .

N'oubliez pas qu'une seule connexion Active Directory est autorisée par région.





Le tableau suivant présente une liste des fonctionnalités prises en charge/non prises en charge pour la MMC.

Fonctions prises en charge	Fonctions non prises en charge
• Voir les actions • Afficher les sessions SMB actives • Afficher les fichiers ouverts • Afficher les utilisateurs et les groupes locaux • Afficher les adhésions aux groupes locaux • Énumérer la liste des sessions, des fichiers et des connexions arborescentes dans le système • Fermer les fichiers ouverts dans le système • Clôture des séances ouvertes • Créer/gérer des partages	• Création de nouveaux utilisateurs/groupes locaux • Gestion/affichage des utilisateurs/groupes locaux existants • Afficher les événements ou les journaux de performances • Gestion du stockage • Gestion des services et des applications

Informations sur la sécurité du serveur SMB

Le serveur SMB dans Google Cloud NetApp Volumes utilise une série d'options qui définissent les politiques de sécurité pour les connexions SMB, notamment le décalage d'horloge Kerberos, l'âge du ticket, le chiffrement, etc.

Le tableau suivant contient une liste de ces options, leur fonction, les configurations par défaut et si elles

peuvent être modifiées avec Google Cloud NetApp Volumes. Certaines options ne s'appliquent pas à Google Cloud NetApp Volumes.

Option de sécurité	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
Décalage maximal de l'horloge Kerberos (minutes)	Décalage horaire maximal entre les Google Cloud NetApp Volumes et les contrôleurs de domaine. Si le décalage horaire dépasse 5 minutes, l'authentification Kerberos échoue. Ceci est défini sur la valeur par défaut d'Active Directory.	5	Non
Durée de vie du ticket Kerberos (heures)	Durée maximale pendant laquelle un ticket Kerberos reste valide avant de nécessiter un renouvellement. Si aucun renouvellement n'intervient avant les 10 heures, vous devez obtenir un nouveau billet. Google Cloud NetApp Volumes effectue ces renouvellements automatiquement. 10 heures est la valeur par défaut d'Active Directory.	10	Non
Renouvellement maximal des tickets Kerberos (jours)	Nombre maximal de jours pendant lesquels un ticket Kerberos peut être renouvelé avant qu'une nouvelle demande d'autorisation ne soit nécessaire. Google Cloud NetApp Volumes renouvelle automatiquement les tickets pour les connexions SMB. Sept jours est la valeur par défaut d'Active Directory.	7	Non
Délai d'expiration de la connexion Kerberos KDC (sec)	Le nombre de secondes avant l'expiration d'une connexion KDC.	3	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
Exiger une signature pour le trafic SMB entrant	Paramètre pour exiger la signature pour le trafic SMB. Si défini sur vrai, les clients qui ne prennent pas en charge la signature échouent à la connectivité.	FAUX	
Exiger une complexité de mot de passe pour les comptes d'utilisateurs locaux	Utilisé pour les mots de passe des utilisateurs SMB locaux. Google Cloud NetApp Volumes ne prend pas en charge la création d'utilisateurs locaux. Cette option ne s'applique donc pas à Google Cloud NetApp Volumes.	Vrai	Non
Utiliser start_tls pour les connexions LDAP Active Directory	Utilisé pour activer le démarrage des connexions TLS pour Active Directory LDAP. Google Cloud NetApp Volumes ne prend actuellement pas en charge cette activation.	FAUX	Non
Le chiffrement AES-128 et AES-256 pour Kerberos est-il activé ?	Cela contrôle si le cryptage AES est utilisé pour les connexions Active Directory et est contrôlé avec l'option Activer le cryptage AES pour l'authentification Active Directory lors de la création/modification de la connexion Active Directory.	FAUX	Oui
Niveau de compatibilité LM	Niveau des 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	Peut-on changer ?
Exiger le cryptage SMB pour le trafic CIFS entrant	Nécessite un cryptage SMB pour tous les partages. Ceci n'est pas utilisé par Google Cloud NetApp Volumes; à la place, définissez le chiffrement sur une base par volume (voir la section «Fonctionnalités de sécurité du partage SMB ").	FAUX	Non
Sécurité des sessions client	Définit la signature et/ou le scellement pour la communication LDAP. Cette option n'est pas actuellement définie dans Google Cloud NetApp Volumes, mais elle pourrait être nécessaire dans les versions futures pour résoudre ce problème. La correction des problèmes d'authentification LDAP dus au correctif Windows est abordée 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
Recherche de référence LDAP	Lors de l'utilisation de plusieurs serveurs LDAP, la recherche de référence permet au client de faire référence à d'autres serveurs LDAP de la liste lorsqu'une entrée n'est pas trouvée dans le premier serveur. Ceci n'est actuellement pas pris en charge par Google Cloud NetApp Volumes.	FAUX	Non
Utiliser LDAPS pour des connexions Active Directory sécurisées	Permet l'utilisation de LDAP sur SSL. Actuellement non pris en charge par Google Cloud NetApp Volumes.	FAUX	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
Le cryptage est requis pour la connexion DC	Nécessite un cryptage pour des connexions DC réussies. Désactivé par défaut dans Google Cloud NetApp Volumes.	FAUX	Non

Double protocole/multiprotocole

Google Cloud NetApp Volumes permet de partager les mêmes ensembles de données avec les clients SMB et NFS tout en conservant les autorisations d'accès appropriées ("double protocole"). Cela se fait en coordonnant le mappage des identités entre les protocoles et en utilisant un serveur LDAP backend centralisé pour fournir les identités UNIX à Google Cloud NetApp Volumes. Vous pouvez utiliser Windows Active Directory pour fournir à la fois des utilisateurs Windows et UNIX afin de faciliter l'utilisation.

Contrôle d'accès

- **Partager les contrôles d'accès.** Déterminez quels clients et/ou utilisateurs et groupes peuvent accéder à un partage NAS. Pour NFS, les politiques et règles d'exportation contrôlent l'accès des clients aux exportations. Les exportations NFS sont gérées à partir de l'instance Google Cloud NetApp Volumes . SMB utilise des partages CIFS/SMB et des listes de contrôle d'accès (ACL) pour fournir un contrôle plus précis au niveau de l'utilisateur et du groupe. Vous pouvez uniquement configurer les ACL au niveau du partage à partir de clients SMB en utilisant https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Computer Management^] avec un compte disposant de droits d'administrateur sur l'instance Google Cloud NetApp Volumes (voir la section "Comptes avec droits d'administrateur/de sauvegarde locaux/BUILTIN.").
- **Contrôles d'accès aux fichiers.** Contrôlez les autorisations au niveau d'un fichier ou d'un dossier et elles sont toujours gérées à partir du client NAS. Les clients NFS peuvent utiliser des bits de mode traditionnels (rwx) ou des ACL NFSv4. Les clients SMB exploitent les autorisations NTFS.

Le contrôle d'accès pour les volumes qui servent des données à la fois à NFS et à SMB dépend du protocole utilisé. Pour plus d'informations sur les autorisations avec double protocole, consultez la section «Modèle d'autorisation ."

Cartographie des utilisateurs

Lorsqu'un client accède à un volume, Google Cloud NetApp Volumes tente de mapper l'utilisateur entrant à un utilisateur valide dans la direction opposée. Cela est nécessaire pour que l'accès approprié soit déterminé à travers les protocoles et pour garantir que l'utilisateur demandant 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 Google Cloud NetApp Volumes effectue une recherche pour trouver un utilisateur UNIX correspondant nommé `joe` . S'il en existe un, alors les fichiers écrits sur un partage SMB en tant qu'utilisateur Windows `joe` apparaît comme utilisateur UNIX `joe` des clients NFS.

Alternativement, si un utilisateur UNIX nommé `joe` tente d'accéder à un volume Google Cloud NetApp Volumes avec des autorisations Windows, l'utilisateur UNIX doit alors pouvoir se mapper à 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 des identités UNIX externes avec LDAP.

Pour plus d'informations sur la configuration de l'accès à ce service, consultez "Création d'une connexion AD".

Modèle d'autorisation

Lors de l'utilisation de configurations à double protocole, Google Cloud NetApp Volumes utilise des styles de sécurité pour les volumes afin de déterminer le type d'ACL. Ces styles de sécurité sont définis en fonction du protocole NAS spécifié ou, dans le cas d'un protocole double, d'un choix effectué au moment de la création du volume Google Cloud NetApp Volumes .

- Si vous utilisez uniquement NFS, les volumes Google Cloud NetApp Volumes utilisent les autorisations UNIX.
- Si vous utilisez uniquement SMB, les volumes Google Cloud NetApp Volumes utilisent les 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 à partir des clients Windows/SMB, sélectionnez NTFS. Si vos utilisateurs préfèrent utiliser des clients NFS et chmod/chown, utilisez les styles de sécurité UNIX.

Considérations relatives à la création de connexions Active Directory

Google Cloud NetApp Volumes offre la possibilité de connecter votre instance Google Cloud NetApp Volumes à un serveur Active Directory externe pour la gestion des identités pour les utilisateurs SMB et UNIX. La création d'une connexion Active Directory est requise pour utiliser SMB dans Google Cloud NetApp Volumes.

La configuration de ce système offre plusieurs options qui nécessitent une certaine réflexion en matière de sécurité. Le serveur Active Directory externe peut être une instance locale ou native du cloud. Si vous utilisez un serveur Active Directory local, n'exposez pas le domaine au réseau externe (par exemple avec une DMZ ou une adresse IP externe). Utilisez plutôt des tunnels privés sécurisés ou des VPN, des approbations de forêt unidirectionnelles ou des connexions réseau dédiées aux réseaux locaux avec "Accès privé à Google" . Consultez la documentation de Google Cloud pour plus d'informations sur "bonnes pratiques d'utilisation d'Active Directory dans Google Cloud" .

> NetApp Volumes-SW nécessite que les serveurs Active Directory soient situés dans la même région. Si une connexion DC est tentée dans NetApp Volumes-SW vers une autre région, la tentative échoue. Lorsque vous utilisez NetApp Volumes-SW, assurez-vous de créer des sites Active Directory qui incluent les contrôleurs de domaine Active Directory, puis spécifiez des sites dans Google Cloud NetApp Volumes pour éviter les tentatives de connexion entre régions DC.

Informations d'identification Active Directory

Lorsque SMB ou LDAP pour NFS est activé, Google Cloud NetApp Volumes interagit avec les contrôleurs Active Directory pour créer un objet de compte de machine à utiliser pour l'authentification. Cela ne diffère pas de la manière dont un client Windows SMB rejoint un domaine et nécessite les mêmes droits d'accès aux unités d'organisation (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 Google Cloud NetApp Volumes. Dans certains cas, l'utilisateur 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 Google Cloud NetApp Volumes à un Active Directory, un compte disposant de droits d'administration sur le domaine ou "autorisations déléguées pour créer et modifier des objets de compte machine" à une unité d'organisation spécifiée est requise. Vous pouvez le faire avec l'assistant de délégation de contrôle dans Active Directory en créant une tâche personnalisée qui fournit à un utilisateur l'accès à la création/suppression d'objets informatiques avec les autorisations d'accès suivantes fournies :

- 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'unité d'organisation dans Active Directory et minimise l'accès à l'environnement Active Directory. Une fois qu'un utilisateur a été délégué, ce nom d'utilisateur et ce mot de passe peuvent être fournis comme informations d'identification Active Directory dans cette fenêtre.

> Le nom d'utilisateur et le mot de passe transmis au domaine Active Directory utilisent le chiffrement Kerberos lors de la requête et de la création de l'objet de compte machine pour plus de sécurité.

Détails de connexion Active Directory

Le "Détails de connexion Active Directory" guide fournit des instructions aux administrateurs pour fournir des informations spécifiques sur le schéma Active Directory pour le placement des comptes machines, telles que les suivantes :

- **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 Google Cloud NetApp Volumes ou NetApp Volumes-Performance. Si cette option est mal définie sur une connexion existante, elle risque de ne pas fonctionner correctement lors de son utilisation ou de sa modification.
- **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 plusieurs régions car Google Cloud NetApp Volumes ne prend actuellement pas en charge l'autorisation des demandes d'authentification Active Directory vers les serveurs Active Directory dans une région différente de celle de l'instance Google Cloud NetApp Volumes. (Par exemple, le contrôleur de domaine Active Directory se trouve dans une région que seul NetApp Volumes-Performance prend en charge, mais vous voulez un partage SMB dans une instance NetApp Volumes-SW.)
- **Serveurs DNS.** Serveurs DNS à utiliser dans les recherches de noms.
- **Nom NetBIOS (facultatif).** Si vous le souhaitez, le nom NetBIOS du serveur. C'est ce qui est utilisé lorsque de nouveaux comptes de machine sont créés à l'aide de la connexion Active Directory. Par exemple, si le nom NetBIOS est défini sur NetApp Volumes-EAST, les noms de compte de machine seront NetApp Volumes-EAST-{1234}. Voir la section"Comment Google Cloud NetApp Volumes apparaît dans Active Directory" pour plus d'informations.
- **Unité organisationnelle (UO).** L'unité d'organisation spécifique pour créer le compte d'ordinateur. Ceci est utile si vous déléguez le contrôle à un utilisateur pour des comptes de machine vers une unité d'organisation spécifique.
- **Cryptage AES.** Vous pouvez également cocher ou décocher la case Activer le chiffrement AES pour

l'authentification AD. L'activation du chiffrement AES pour l'authentification Active Directory offre une sécurité supplémentaire pour la communication entre Google Cloud NetApp Volumes et Active Directory lors des recherches d'utilisateurs et de groupes. 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, vérifiez que la connexion Active Directory de Google Cloud NetApp Volumes a été configurée pour activer AES. Dans le cas contraire, des échecs d'authentification se produisent. L'activation du chiffrement AES ne désactive pas les chiffrements plus faibles, mais ajoute plutôt la prise en charge des chiffrements AES au compte de machine SMB Google Cloud NetApp Volumes .

Détails du domaine Kerberos

Cette option ne s'applique pas aux serveurs SMB. Il est plutôt utilisé lors de la configuration de NFS Kerberos pour le système Google Cloud NetApp Volumes . Lorsque ces détails sont renseignés, le domaine NFS Kerberos est configuré (similaire à un fichier krb5.conf sous Linux) et est utilisé lorsque NFS Kerberos est spécifié lors de la création du volume Google Cloud NetApp Volumes , car la connexion Active Directory agit comme le centre de distribution NFS Kerberos (KDC).

> Les KDC non Windows ne sont actuellement pas pris en charge pour une utilisation avec Google Cloud NetApp Volumes.

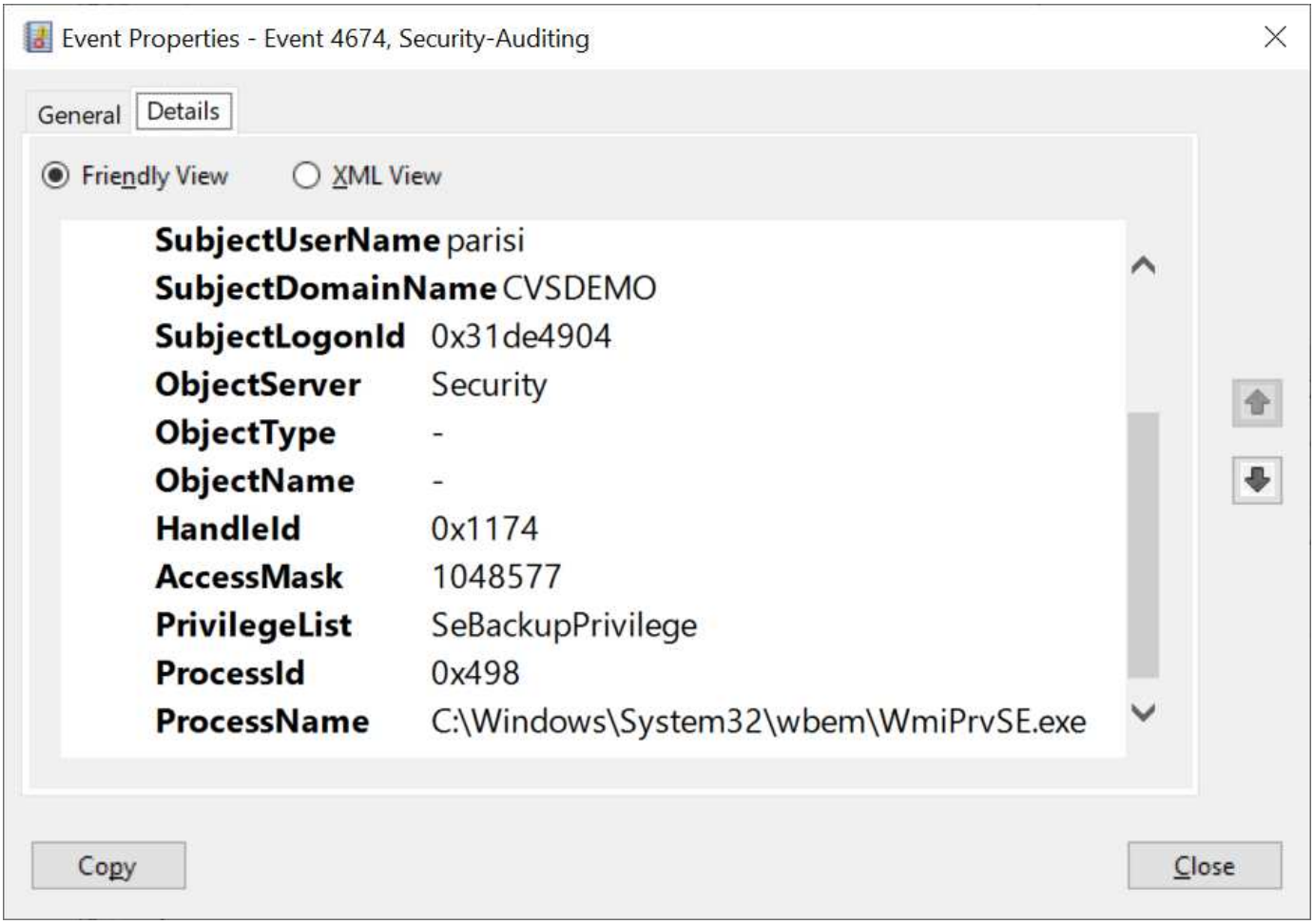
Région

Une région vous permet de spécifier l'emplacement où réside la connexion Active Directory. Cette région doit être la même région que le volume Google Cloud NetApp Volumes .

- **Utilisateurs NFS locaux avec LDAP.** Dans cette section, il existe également une option pour autoriser les utilisateurs NFS locaux avec LDAP. Cette option doit être laissée non sélectionnée si vous souhaitez étendre la prise en charge de votre appartenance à un groupe d'utilisateurs UNIX au-delà de la limitation de 16 groupes de NFS (groupes étendus). Cependant, l'utilisation de groupes étendus nécessite un serveur LDAP configuré pour les identités UNIX. Si vous n'avez pas de serveur LDAP, laissez cette option non sélectionnée. Si vous disposez d'un serveur LDAP et que vous souhaitez également utiliser des utilisateurs UNIX locaux (tels que root), sélectionnez cette option.

Utilisateurs de sauvegarde

Cette option vous permet de spécifier les utilisateurs Windows disposant d'autorisations de sauvegarde sur le volume Google Cloud NetApp Volumes . Les privilèges de sauvegarde (SeBackupPrivilege) sont nécessaires à certaines applications pour sauvegarder et restaurer correctement les données dans les volumes NAS. Cet utilisateur dispose d'un niveau d'accès élevé aux données du volume, vous devez donc prendre en compte "activer l'audit de cet accès utilisateur" . Une fois activé, les événements d'audit s'affichent dans Observateur d'événements > Journaux Windows > Sécurité.



Utilisateurs bénéficiant de privilèges de sécurité

Cette option vous permet de spécifier les utilisateurs Windows disposant d'autorisations de modification de sécurité sur le volume Google Cloud NetApp Volumes . Les privilèges de sécurité (SeSecurityPrivilege) sont nécessaires pour certaines applications("comme 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 des accès utilisateurs" avec ce niveau de privilège si nécessaire.

Pour plus d'informations, consultez la section "Privilèges spéciaux attribués à la nouvelle connexion" .

Comment Google Cloud NetApp Volumes apparaît dans Active Directory

Google Cloud NetApp Volumes apparaît dans Active Directory comme un objet de compte de machine normal. Les conventions de nommage sont les suivantes.

- CIFS/SMB et NFS Kerberos créent des objets de compte de machine distincts.
- NFS avec LDAP activé crée un compte de machine dans Active Directory pour les liaisons LDAP Kerberos.
- Les volumes à double protocole avec LDAP partagent le compte machine CIFS/SMB pour LDAP et SMB.
- Les comptes de machine CIFS/SMB utilisent une convention de dénomination NAME-1234 (ID aléatoire à quatre chiffres avec un trait d'union ajouté à un nom <10 caractères) pour le compte de machine. Vous pouvez définir NAME par le paramètre de nom NetBIOS sur la connexion Active Directory (voir la section «Détails de connexion Active Directory ").

- NFS Kerberos utilise NFS-NAME-1234 comme convention de nommage (jusqu'à 15 caractères). Si plus de 15 caractères sont utilisés, le nom est NFS-TRUNCATED-NAME-1234.
- Les instances NetApp Volumes-Performance NFS uniquement avec LDAP activé créent un compte de machine SMB pour la liaison au serveur LDAP avec la même convention de dénomination que les instances CIFS/SMB.
- Lorsqu'un compte de machine SMB est créé, les partages d'administration masqués par défaut (voir la section"Partages cachés par défaut") sont également créés (c$, admin$, ipc$), mais ces partages n'ont pas d'ACL attribuées et sont inaccessibles.
- Les objets de compte machine sont placés dans CN=Computers par défaut, mais vous pouvez spécifier une autre unité d'organisation 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 de machine pour Google Cloud NetApp Volumes.

Lorsque Google Cloud NetApp Volumes ajoute le compte de machine SMB à Active Directory, les champs suivants sont renseignés :

- cn (avec le nom du serveur SMB spécifié)
- dNSHostName (avec SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (autorise DES_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_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 sont autorisés pour l'échange de tickets Kerberos avec le compte machine pour SMB)
- nom (avec le nom du serveur SMB)
- sAMAccountName (avec SMBserver$)
- servicePrincipalName (avec host/smbserver.domain.com et host/smbserver SPN pour Kerberos)

Si vous souhaitez désactiver les types de chiffrement Kerberos plus faibles (enctype) sur le compte de machine, vous pouvez modifier la valeur msDS-SupportedEncryptionTypes sur le compte de machine sur l'une des valeurs du tableau suivant pour autoriser AES uniquement.

Valeur msDS-SupportedEncryptionTypes	Enctype 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 chiffrement AES pour les comptes de machine SMB, cliquez sur Activer le chiffrement AES pour l'authentification AD lors de la création de la connexion Active Directory.

Pour activer le chiffrement AES pour NFS Kerberos, "voir la documentation de Google Cloud NetApp Volumes".

Autres dépendances des services d'infrastructure NAS (KDC, LDAP et DNS)

Lors de l'utilisation de Google Cloud NetApp Volumes pour les partages NAS, des dépendances externes peuvent être requises pour un fonctionnement correct. Ces dépendances entrent en jeu dans des circonstances spécifiques. Le tableau suivant présente différentes options de configuration et les dépendances requises, le cas échéant.

Configuration	Dépendances requises
NFSv3 uniquement	Aucune
NFSv3 Kerberos 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 : KDC DNS LDAP
PME uniquement	Active Directory : * KDC * DNS
NAS multiprotocole (NFS et SMB)	• Configuration du mappage d'ID client (NFSv4.1 uniquement ; /etc/idmap.conf) • Windows Active Directory : KDC DNS LDAP

Rotation des clés Kerberos/réinitialisations de mots de passe pour les objets de compte machine

Avec les comptes de machine SMB, Google Cloud NetApp Volumes planifie des réinitialisations de mot de passe périodiques pour le compte de machine SMB. Ces réinitialisations de mot de passe se produisent à l'aide du cryptage Kerberos et fonctionnent selon un calendrier tous les quatrièmes dimanches à une heure aléatoire entre 23h et 1h du matin. Ces réinitialisations de mot de passe modifient les versions de clé Kerberos, font pivoter les keytabs stockés sur le système Google Cloud NetApp Volumes et contribuent à maintenir un niveau de sécurité plus élevé pour les serveurs SMB exécutés dans Google Cloud NetApp Volumes. Les mots de passe des comptes machines sont aléatoires et ne sont pas connus des administrateurs.

Pour les comptes de machine NFS Kerberos, les réinitialisations de mot de passe ont lieu uniquement lorsqu'un nouveau keytab est créé/échangé avec le KDC. Actuellement, cela n'est pas possible dans Google Cloud NetApp Volumes.

Ports réseau à utiliser avec LDAP et Kerberos

Lorsque vous utilisez LDAP et Kerberos, vous devez identifier les ports réseau utilisés par ces services. Vous trouverez la liste complète des ports utilisés par Google Cloud NetApp Volumes dans la documentation "Documentation de Google Cloud NetApp Volumes sur les considérations de sécurité".

LDAP

Google Cloud NetApp Volumes agit comme un client LDAP et utilise des requêtes de recherche LDAP standard pour les recherches d'utilisateurs et de groupes pour les identités UNIX. LDAP est nécessaire si vous avez l'intention d'utiliser des utilisateurs et des groupes en dehors des utilisateurs par défaut standard fournis par Google Cloud NetApp Volumes. LDAP est également nécessaire si vous prévoyez d'utiliser NFS Kerberos avec des principaux utilisateurs (tels que user1@domain.com). Actuellement, seul LDAP utilisant Microsoft

Active Directory est pris en charge.

Pour utiliser Active Directory comme serveur LDAP UNIX, vous devez renseigner les attributs UNIX nécessaires sur les utilisateurs et les groupes que vous souhaitez utiliser pour les identités UNIX. Google Cloud NetApp Volumes utilise un modèle de schéma LDAP par défaut qui interroge les attributs en fonction de "RFC-2307-bis" . Par conséquent, le tableau suivant indique les attributs Active Directory minimaux nécessaires à renseigner pour les utilisateurs et les groupes et à quoi sert chaque attribut.

Pour plus d'informations sur la configuration des attributs LDAP dans Active Directory, consultez "Gestion de l'accès double protocole."

Attribut	Ce qu'il fait
uid*	Spécifie le nom d'utilisateur UNIX
uidNumber*	Spécifie l'ID numérique de l'utilisateur UNIX
gidNumber*	Spécifie l'ID numérique du groupe principal de l'utilisateur UNIX
classe d'objet*	Spécifie le type d'objet utilisé ; Google Cloud NetApp Volumes nécessite que « utilisateur » soit inclus dans la liste des classes d'objets (est inclus dans la plupart des déploiements Active Directory par défaut).
nom	Informations générales sur le compte (nom réel, numéro de téléphone, etc., également appelés gecos)
mot de passe utilisateur unix	Il n'est pas nécessaire de définir ceci ; non utilisé dans les recherches d'identité UNIX pour l'authentification NAS. Ce paramètre place la valeur unixUserPassword configurée en texte brut.
unixHomeDirectory	Définit le chemin d'accès aux répertoires personnels UNIX lorsqu'un utilisateur s'authentifie auprès de LDAP à partir d'un client Linux. Définissez cette option si vous souhaitez utiliser LDAP pour la fonctionnalité de répertoire personnel UNIX.
connexionShell	Définit le chemin vers le shell bash/profile pour les clients Linux lorsqu'un utilisateur s'authentifie auprès de LDAP.

*Indique que l'attribut est requis pour un fonctionnement correct avec Google Cloud NetApp Volumes. Les attributs restants sont réservés à une utilisation côté client.

Attribut	Ce qu'il fait
cn*	Spécifie le nom du groupe UNIX. Lorsque vous utilisez Active Directory pour LDAP, cette option est définie lors de la création initiale de l'objet, mais elle peut être modifiée ultérieurement. Ce nom ne peut pas être le même que celui d'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 avec un nom unique (tel que user1-UNIX) ; LDAP dans Google Cloud NetApp Volumes utilise l'attribut uid pour les noms d'utilisateur UNIX.
gidNumber*	Spécifie l'ID numérique du groupe UNIX.
classe d'objet*	Spécifie le type d'objet utilisé ; Google Cloud NetApp Volumes nécessite que le groupe soit inclus dans la liste des classes d'objets (cet attribut est inclus dans la plupart des déploiements Active Directory par défaut).
memberUid	Spécifie quels utilisateurs UNIX sont membres du groupe UNIX. Avec Active Directory LDAP dans Google Cloud NetApp Volumes, ce champ n'est pas nécessaire. Le schéma LDAP de Google Cloud NetApp Volumes utilise le champ Membre pour les appartenances aux groupes.
Membre*	Obligatoire pour les appartenances aux groupes/groupes UNIX secondaires. Ce champ est renseigné en ajoutant des utilisateurs Windows aux groupes Windows. Toutefois, si les groupes Windows n'ont pas d'attributs UNIX 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.

*Indique que l'attribut est requis pour un fonctionnement correct avec Google Cloud NetApp Volumes. Les attributs restants sont réservés à une utilisation côté client.

Informations de liaison LDAP

Pour interroger les utilisateurs dans LDAP, Google Cloud NetApp Volumes doit se lier (se connecter) au service LDAP. Cette connexion dispose d'autorisations en lecture seule et est utilisée pour interroger les attributs LDAP UNIX pour les recherches d'annuaire. Actuellement, les liaisons LDAP ne sont possibles qu'en utilisant un compte machine SMB.

Vous ne pouvez activer LDAP que pour `NetApp Volumes-Performance` instances et utilisez-le pour les volumes NFSv3, NFSv4.1 ou à double protocole. Une connexion Active Directory doit être établie dans la même région que le volume Google Cloud NetApp Volumes pour un déploiement réussi du volume compatible LDAP.

Lorsque LDAP est activé, les événements suivants se produisent dans des scénarios spécifiques.

- Si seul NFSv3 ou NFSv4.1 est utilisé pour le projet Google Cloud NetApp Volumes , un nouveau compte de machine est créé dans le contrôleur de domaine Active Directory et le client LDAP dans Google Cloud NetApp Volumes se lie à Active Directory à l'aide des informations d'identification du compte de machine. Aucun partage SMB n'est créé pour le volume NFS et les partages administratifs masqués par défaut (voir la section"Partages cachés par défaut") ont supprimé les ACL de partage.
- Si des volumes à double protocole sont utilisés pour le projet Google Cloud NetApp Volumes , seul le compte de machine unique créé pour l'accès SMB est utilisé pour lier le client LDAP dans Google Cloud NetApp Volumes 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 de machine pour les liaisons LDAP est partagé avec le compte de machine SMB.
- Si NFS Kerberos est également activé, deux comptes de machine sont créés : un pour les partages SMB et/ou les liaisons LDAP et un pour l'authentification NFS Kerberos.

Requêtes LDAP

Bien que les liaisons LDAP soient chiffrées, les requêtes LDAP sont transmises sur le réseau en texte clair à l'aide du port LDAP commun 389. Ce port bien connu ne peut actuellement pas être modifié dans Google Cloud NetApp Volumes. Par conséquent, une personne ayant accès au reniflage de paquets sur le réseau peut voir les noms d'utilisateur et de groupe, les identifiants numériques et les appartenances aux groupes.

Cependant, les machines virtuelles Google Cloud ne peuvent pas détecter le trafic monodiffusion d'autres machines virtuelles. Seules les machines virtuelles participant activement au trafic LDAP (c'est-à-dire capables de se lier) peuvent voir le trafic provenant du serveur LDAP. Pour plus d'informations sur le reniflage de paquets dans Google Cloud NetApp Volumes, consultez la section"Considérations relatives au reniflage/tracage des paquets."

Paramètres de configuration par défaut du client LDAP

Lorsque LDAP est activé dans une instance Google Cloud NetApp Volumes , une configuration client LDAP est créée avec des détails de configuration spécifiques par défaut. Dans certains cas, les options ne s'appliquent pas aux Google Cloud NetApp Volumes (non pris en charge) ou ne sont pas configurables.

Option client LDAP	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
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 les Google Cloud NetApp Volumes. Au lieu de cela, le domaine Active Directory est utilisé pour définir les serveurs LDAP.	Non défini	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
Domaine Active Directory	Définit le domaine Active Directory à utiliser pour les requêtes LDAP. Google Cloud NetApp Volumes exploite les enregistrements SRV pour LDAP dans DNS pour rechercher les serveurs LDAP dans le domaine.	Définissez le domaine Active Directory spécifié dans la connexion Active Directory.	Non
Serveurs Active Directory préférés	Définit les serveurs Active Directory préférés à utiliser pour LDAP. Non pris en charge par Google Cloud NetApp Volumes. 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 en utilisant le compte machine SMB. Actuellement, la seule méthode de liaison LDAP prise en charge dans Google Cloud NetApp Volumes.	Vrai	Non
Modèle de schéma	Le modèle de schéma utilisé pour les requêtes LDAP.	MS-AD-BIS	Non
Port du serveur LDAP	Le numéro de port utilisé pour les requêtes LDAP. Google Cloud NetApp Volumes utilise actuellement uniquement le port LDAP standard 389. LDAPS/port 636 n'est actuellement pas pris en charge.	389	Non
LDAPS est-il activé ?	Contrôle si LDAP sur Secure Sockets Layer (SSL) est utilisé pour les requêtes et les liaisons. Actuellement non pris en charge par Google Cloud NetApp Volumes.	FAUX	Non
Délai d'expiration de la requête (sec)	Délai d'expiration 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	Peut-on changer ?
Niveau d'authentification de liaison minimum	Le niveau de liaison minimum pris en charge. Étant donné que Google Cloud NetApp Volumes utilise des comptes d'ordinateur pour les liaisons LDAP et qu'Active Directory ne prend pas en charge les liaisons anonymes par défaut, cette option n'entre pas en jeu pour la sécurité.	Anonyme	Non
Lier DN	Le nom d'utilisateur/nom distinctif (DN) utilisé pour les liaisons lorsque la liaison simple est utilisée. Google Cloud NetApp Volumes utilise des comptes de machine pour les liaisons LDAP et ne prend actuellement pas en charge l'authentification par liaison simple.	Non défini	Non
Base DN	Le DN de base utilisé pour les recherches LDAP.	Le domaine Windows utilisé pour la connexion Active Directory, au format DN (c'est-à-dire DC=domaine, DC=local).	Non
Portée de la recherche de base	La portée de recherche pour les recherches DN de base. Les valeurs peuvent inclure la base, un niveau ou un sous-arbre. Google Cloud NetApp Volumes prend uniquement en charge les recherches de sous-arborescence.	Sous-arbre	Non
DN de l'utilisateur	Définit le DN où les recherches des utilisateurs commencent pour les requêtes LDAP. Actuellement non pris en charge pour Google Cloud NetApp Volumes, toutes les recherches d'utilisateurs commencent donc au DN de base.	Non défini	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
Portée de la recherche utilisateur	La portée de recherche pour les recherches DN d'utilisateur. Les valeurs peuvent inclure la base, un niveau ou un sous-arbre. Google Cloud NetApp Volumes ne prend pas en charge la définition de l'étendue de la recherche utilisateur.	Sous-arbre	Non
Groupe DN	Définit le DN où les recherches de groupe commencent pour les requêtes LDAP. Actuellement non pris en charge pour Google Cloud NetApp Volumes, toutes les recherches de groupe commencent donc au DN de base.	Non défini	Non
Portée de la recherche de groupe	La portée de recherche pour les recherches de groupe DN. Les valeurs peuvent inclure la base, un niveau ou un sous-arbre. Google Cloud NetApp Volumes ne prend pas en charge la définition de l'étendue de recherche de groupe.	Sous-arbre	Non
DN du groupe réseau	Définit le DN où les recherches de groupe réseau commencent pour les requêtes LDAP. Actuellement non pris en charge pour Google Cloud NetApp Volumes, toutes les recherches de groupes réseau commencent donc au DN de base.	Non défini	Non
Portée de recherche du groupe réseau	La portée de recherche pour les recherches de DN de groupe réseau. Les valeurs peuvent inclure la base, un niveau ou un sous-arbre. Google Cloud NetApp Volumes 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	Peut-on changer ?
Utiliser start_tls sur LDAP	Exploite Start TLS pour les connexions LDAP basées sur des certificats sur le port 389. Actuellement non pris en charge par Google Cloud NetApp Volumes.	FAUX	Non
Activer la recherche de groupe réseau par hôte	Permet les recherches de groupes réseau par nom d'hôte plutôt que d'étendre les groupes réseau pour répertorier tous les membres. Actuellement non pris en charge par Google Cloud NetApp Volumes.	FAUX	Non
DN du groupe réseau par hôte	Définit le DN où les recherches netgroup-by-host commencent pour les requêtes LDAP. Netgroup-by-host n'est actuellement pas pris en charge pour Google Cloud NetApp Volumes.	Non défini	Non
Portée de recherche Netgroup par hôte	La portée de recherche pour les recherches DN par groupe réseau par hôte. Les valeurs peuvent inclure la base, un niveau ou un sous-arbre. Netgroup-by-host n'est actuellement pas pris en charge pour Google Cloud NetApp Volumes.	Sous-arbre	Non
Sécurité des sessions client	Définit le niveau de sécurité de session utilisé par LDAP (signature, sceau ou aucun). La signature LDAP est prise en charge par NetApp Volumes-Performance, si elle est demandée par Active Directory. NetApp Volumes-SW ne prend pas en charge la signature LDAP. Pour les deux types de services, le scellement n'est actuellement pas pris en charge.	Aucune	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Peut-on changer ?
Recherche de référence LDAP	Lors de l'utilisation de plusieurs serveurs LDAP, la recherche de référence permet au client de faire référence à d'autres serveurs LDAP de la liste lorsqu'une entrée n'est pas trouvée dans le premier serveur. Ceci n'est actuellement pas pris en charge par Google Cloud NetApp Volumes.	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 Google Cloud NetApp Volumes.	Non défini	Non

Utilisation de LDAP pour le mappage de noms asymétriques

Par défaut, Google Cloud NetApp Volumes mappe les utilisateurs Windows et UNIX avec des noms d'utilisateur identiques de manière bidirectionnelle sans configuration spéciale. Tant que Google Cloud NetApp Volumes peut trouver un utilisateur UNIX valide (avec LDAP), le mappage de noms 1:1 se produit. Par exemple, si l'utilisateur Windows `johnsmith` est utilisé, alors, si Google Cloud NetApp Volumes peut trouver un utilisateur UNIX nommé `johnsmith` dans LDAP, le mappage de noms réussit pour cet utilisateur, tous les fichiers/dossiers créés par `johnsmith` afficher la propriété correcte de l'utilisateur et toutes les ACL affectant `johnsmith` sont honorés quel que soit le protocole NAS utilisé. C'est ce qu'on appelle le mappage de noms symétrique.

Le mappage de noms asymétrique se produit lorsque l'identité de l'utilisateur Windows et de l'utilisateur UNIX ne correspondent pas. Par exemple, si l'utilisateur Windows `johnsmith` a une identité UNIX de `jsmith` Google Cloud NetApp Volumes a besoin d'un moyen d'être informé de la variation. Étant donné que Google Cloud NetApp Volumes ne prend 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 de garantir la propriété appropriée des fichiers et des dossiers et les autorisations attendues.

Par défaut, Google Cloud NetApp Volumes inclut `LDAP` dans le commutateur ns de l'instance pour 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 des attributs utilisateur/groupe pour refléter ce que recherche Google Cloud NetApp Volumes .

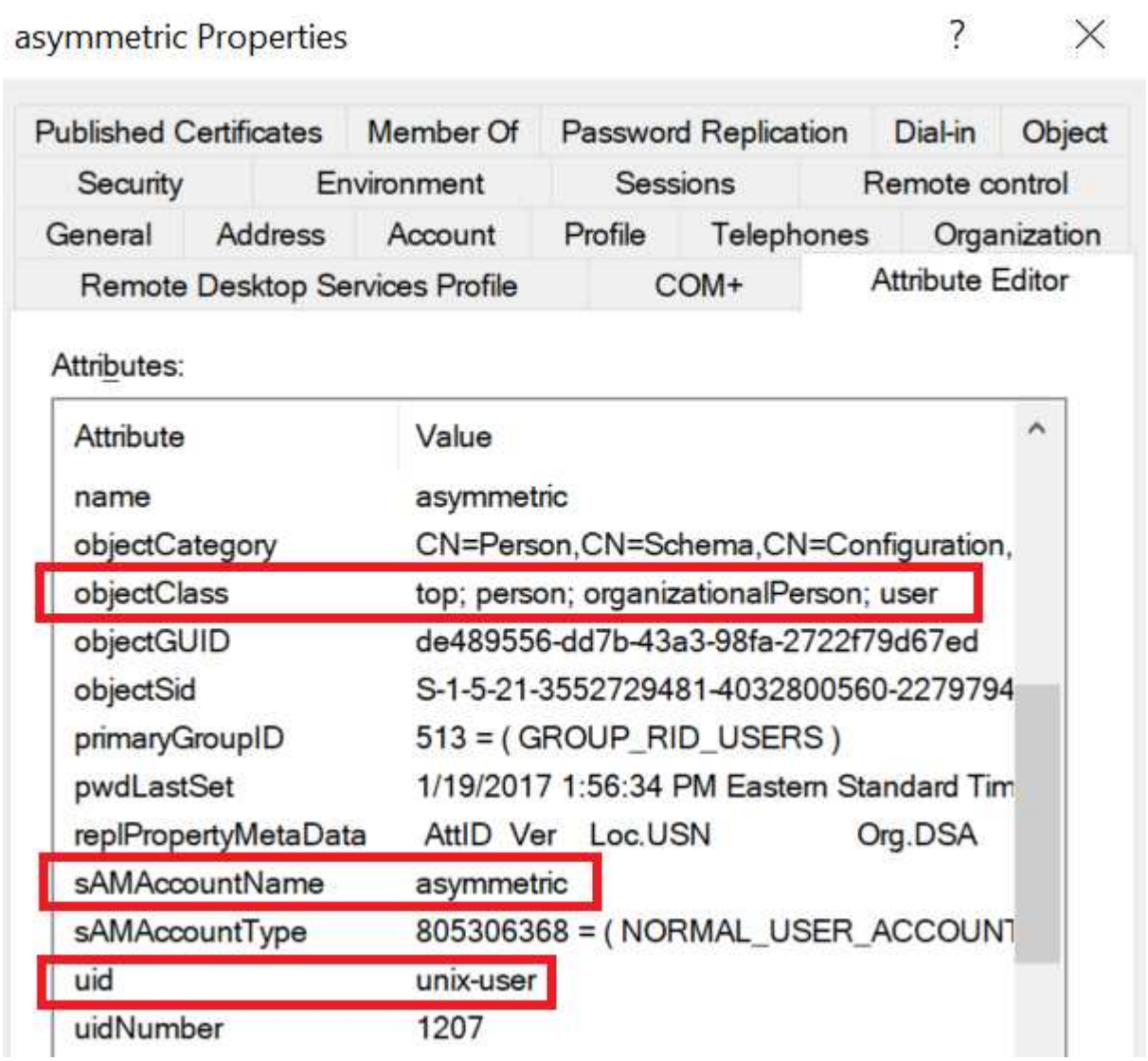
Le tableau suivant indique les attributs qui doivent être renseignés dans LDAP pour la fonctionnalité de mappage de noms asymétriques. Dans la plupart des cas, Active Directory est déjà configuré pour faire cela.

Attribut Google Cloud NetApp Volumes	Ce qu'il fait	Valeur utilisée par Google Cloud NetApp Volumes pour le mappage de noms
Classe d'objets Windows vers 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 vous le souhaitez).
Attribut Windows vers UNIX	qui définit le nom d'utilisateur Windows lors de la création. Google Cloud NetApp Volumes l'utilise pour les recherches Windows vers UNIX.	Aucune modification n'est nécessaire ici ; sAMAccountName est le même que le nom de connexion Windows.
UID	Définit le nom d'utilisateur UNIX.	Nom d'utilisateur UNIX souhaité.

Google Cloud NetApp Volumes n'utilise actuellement pas de préfixes de domaine dans les recherches LDAP. Par conséquent, les environnements LDAP à domaines multiples ne fonctionnent pas correctement avec les recherches de mappage de noms LDAP.

L'exemple suivant montre un utilisateur avec le nom Windows `asymmetric` , le nom UNIX `unix-user` , et le comportement qu'il suit lors de l'écriture de fichiers à partir de SMB et de NFS.

La figure suivante montre à quoi ressemblent les 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` , voici le résultat 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
```

À l'inverse, les fichiers créés par l'utilisateur Windows `asymmetric` à partir d'un client SMB, affichez le propriétaire UNIX approprié, comme indiqué dans le texte suivant.

PME :

```
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 des contrôleurs de domaine Windows Active Directory, "Avis de sécurité Microsoft ADV190023" modifie la manière dont les contrôleurs de domaine autorisent les liaisons LDAP.

L'impact pour Google Cloud NetApp Volumes est le même que pour n'importe quel client LDAP. Google Cloud NetApp Volumes ne prend actuellement pas en charge la liaison de canaux. Étant donné que Google Cloud NetApp Volumes prend en charge la signature LDAP par défaut via la négociation, la liaison de canal LDAP ne devrait pas poser de problème. Si vous rencontrez des problèmes de liaison à LDAP avec la liaison de canal activée, suivez les étapes de correction décrites dans ADV190023 pour permettre aux liaisons LDAP à partir de Google Cloud NetApp Volumes de réussir.

DNS

Active Directory et Kerberos ont tous deux des dépendances sur DNS pour la résolution du nom d'hôte vers l'IP/IP vers le nom d'hôte. DNS nécessite que le port 53 soit ouvert. Google Cloud NetApp Volumes n'apporte aucune modification aux enregistrements DNS et ne prend actuellement pas en charge l'utilisation de "DNS dynamique" sur les interfaces réseau.

Vous pouvez configurer le DNS Active Directory pour restreindre les serveurs pouvant mettre à jour les enregistrements DNS. Pour plus d'informations, consultez la section "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 Cloud DNS ne peuvent pas résoudre les chemins UNC renvoyés par Google Cloud NetApp Volumes. Les clients Windows joints au domaine Active Directory sont configurés pour

utiliser le DNS Active Directory et peuvent résoudre ces chemins UNC.

Pour joindre un client à Active Directory, vous devez configurer son DNS afin qu'il utilise les serveurs DNS d'Active Directory. Vous pouvez également configurer Cloud DNS pour rediriger les requêtes vers les serveurs DNS d'Active Directory. Consultez "Pourquoi mon client ne peut-il pas résoudre le nom NetBIOS SMB ?"pour plus d'informations.

Google Cloud NetApp Volumes ne prend actuellement pas en charge DNSSEC et les requêtes DNS sont effectuées en texte brut.

Audit d'accès aux fichiers

Actuellement non pris en charge pour Google Cloud NetApp Volumes.

Protection antivirus

Vous devez effectuer une analyse antivirus dans Google Cloud NetApp Volumes sur le client vers un partage NAS. Il n'existe actuellement aucune intégration antivirus native avec Google Cloud NetApp Volumes.

Opération de service

L'équipe Google Cloud NetApp Volumes gère les services back-end dans Google Cloud et utilise plusieurs stratégies pour sécuriser la plateforme et empêcher tout accès indésirable.

Chaque client obtient son propre sous-réseau unique dont l'accès est isolé des autres clients par défaut, et chaque locataire de Google Cloud NetApp Volumes obtient son propre espace de noms et son propre VLAN pour une isolation totale des données. Une fois qu'un utilisateur est authentifié, le moteur de distribution de services (SDE) peut uniquement lire les données de configuration spécifiques à ce locataire.

Sécurité physique

Avec une approbation préalable appropriée, seuls les ingénieurs sur site et les ingénieurs de support sur le terrain (FSE) portant le badge NetApp ont accès à la cage et aux racks pour le travail physique. Le stockage et la gestion du réseau ne sont pas autorisés. Seules ces ressources sur site sont en mesure d'effectuer des tâches de maintenance matérielle.

Pour les ingénieurs sur site, un ticket est émis pour l'énoncé des travaux (SOW) qui comprend l'ID du rack et l'emplacement du périphérique (RU) et tous les autres détails sont inclus dans le ticket. Pour les FSE NetApp , un ticket de visite du site doit être émis auprès du COLO et le ticket inclut les détails du visiteur, la date et l'heure à des fins d'audit. Le SOW du FSE est communiqué en interne à NetApp.

Équipe des opérations

L'équipe d'exploitation de Google Cloud NetApp Volumes se compose d'ingénieurs de production et d'un ingénieur de fiabilité du site (SRE) pour Google Cloud NetApp Volumes et d'ingénieurs et partenaires de support sur le terrain NetApp pour le matériel. Tous les membres de l'équipe d'exploitation sont accrédités pour travailler dans Google Cloud et des enregistrements détaillés du travail sont conservés pour chaque ticket soulevé. De plus, un processus rigoureux de contrôle et d'approbation des changements est en place pour garantir que chaque décision est examinée de manière appropriée.

L'équipe SRE gère le plan de contrôle et la manière dont les données sont acheminées des requêtes d'interface utilisateur vers le matériel et les logiciels back-end dans Google Cloud NetApp Volumes. L'équipe SRE gère également les ressources système, telles que les volumes et les maximums d'inodes. Les SRE ne

sont pas autorisés à interagir avec les données clients ni à y avoir accès. Les SRE assurent également la coordination avec les autorisations de retour de matériel (RMA), telles que les demandes de remplacement de nouveaux disques ou de mémoire pour le matériel principal.

Responsabilités du client

Les clients de Google Cloud NetApp Volumes gèrent l'Active Directory et la gestion des rôles utilisateur de leur organisation, ainsi que les opérations de volume et de données. Les clients peuvent avoir des rôles administratifs et déléguer des autorisations à d'autres utilisateurs finaux au sein du même projet Google Cloud à l'aide des deux rôles prédéfinis fournis par NetApp et Google Cloud (Administrateur et Spectateur).

L'administrateur peut connecter n'importe quel VPC du projet client aux Google Cloud NetApp Volumes que le client juge appropriés. Il est de la responsabilité du client de gérer l'accès à son abonnement Google Cloud Marketplace et de gérer les VPC qui ont accès au plan de données.

Protection SRE malveillante

Une préoccupation qui pourrait survenir est de savoir comment Google Cloud NetApp Volumes protège contre les scénarios dans lesquels il existe un SRE malveillant ou lorsque les informations d'identification SRE ont été compromises ?

L'accès à l'environnement de production est réservé à un nombre limité de personnes SRE. Les privilèges administratifs sont en outre limités à une poignée d'administrateurs expérimentés. Toutes les actions effectuées par quiconque dans l'environnement de production Google Cloud NetApp Volumes sont enregistrées et toute anomalie par rapport à la ligne de base ou activité suspecte est détectée par notre plateforme de renseignement sur les menaces de gestion des informations et des événements de sécurité (SIEM). Par conséquent, les actions malveillantes peuvent être suivies et atténuées avant que trop de dommages ne soient causés au backend de Google Cloud NetApp Volumes .

Cycle de vie du volume

Google Cloud NetApp Volumes gère uniquement les objets au sein du service, et non les données au sein des volumes. Seuls les clients accédant aux volumes peuvent gérer les données, les ACL, les propriétaires de fichiers, etc. Les données de ces volumes sont chiffrées au repos et l'accès est limité aux locataires de l'instance Google Cloud NetApp Volumes .

Le cycle de vie du volume pour Google Cloud NetApp Volumes est le suivant : création-mise à jour-suppression. Les volumes conservent des copies instantanées des volumes jusqu'à ce que les volumes soient supprimés, et seuls les administrateurs Google Cloud NetApp Volumes validés peuvent supprimer des volumes dans Google Cloud NetApp Volumes. Lorsqu'une suppression de volume est demandée par un administrateur, une étape supplémentaire de saisie du nom du volume est requise pour vérifier la suppression. Une fois un volume supprimé, le volume disparaît et ne peut pas être récupéré.

Dans les cas où un contrat Google Cloud NetApp Volumes est résilié, NetApp marque les volumes pour suppression après une période de temps spécifique. Avant l'expiration de ce délai, vous pouvez récupérer les volumes à la demande du client.

Certifications

Google Cloud NetApp Volumes pour Google Cloud est actuellement certifié selon les normes ISO/IEC 27001:2013 et ISO/IEC 27018:2019. Le service a également récemment reçu son rapport d'attestation SOC2 Type I. Pour plus d'informations sur l'engagement de NetApp en matière de sécurité et de confidentialité des données, consultez "Conformité : sécurité et confidentialité des données" .

RGPD

Nos engagements en matière de confidentialité et de conformité au GDPR sont disponibles dans plusieurs de nos "contrats clients", comme notre "Addendum relatif au Data Processing clients", qui inclut les "Clauses contractuelles types" fournies par la Commission européenne. Nous prenons également ces engagements dans notre Privacy Policy, appuyée par les valeurs fondamentales énoncées dans notre Code of Conduct.

Informations complémentaires et coordonnées

Pour en savoir plus sur les informations décrites dans ce document, consultez les documents et/ou sites Web suivants :

- Documentation Google Cloud pour Google Cloud NetApp Volumes

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Accès au service privé de Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentation produit 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"

- La solution NetApp contre les ransomwares

  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 pouvons améliorer ce rapport technique.

Contactez-nous à doccomments@netapp.com. Inclure le RAPPORT TECHNIQUE 4918 dans la ligne d’objet.

NetApp Disaster Recovery

Protection des données 3-2-1 pour VMware avec SnapCenter Plug-in et NetApp Backup and Recovery pour protéger les charges de travail VMware

La stratégie de sauvegarde 3-2-1 est une méthode de protection des données acceptée par l’industrie, offrant une approche complète pour la sauvegarde des données précieuses. Cette stratégie est fiable et garantit que même en cas de catastrophe inattendue, une copie des données sera toujours disponible.

Aperçu

La stratégie comprend trois règles fondamentales :

1. Conservez au moins trois copies de vos données. Cela garantit que même si une copie est perdue ou corrompue, vous disposez toujours d'au moins deux copies restantes sur lesquelles vous pouvez compter.
2. Stockez deux copies de sauvegarde sur des supports ou périphériques de stockage différents. La diversification des supports de stockage permet de se protéger contre les pannes spécifiques à l'appareil ou au support. Si un appareil est endommagé ou qu'un type de support tombe en panne, l'autre copie de sauvegarde reste inchangée.
3. Enfin, assurez-vous qu'au moins une copie de sauvegarde est hors site. Le stockage hors site sert de mesure de sécurité contre les catastrophes localisées telles que les incendies ou les inondations qui pourraient rendre les copies sur site inutilisables.

Ce document de solution décrit une solution de sauvegarde 3-2-1 utilisant SnapCenter Plug-in for VMware vSphere (SCV) pour créer des sauvegardes primaires et secondaires de nos machines virtuelles sur site et NetApp Backup and Recovery for virtual machines pour sauvegarder une copie de nos données sur stockage cloud ou StorageGRID.

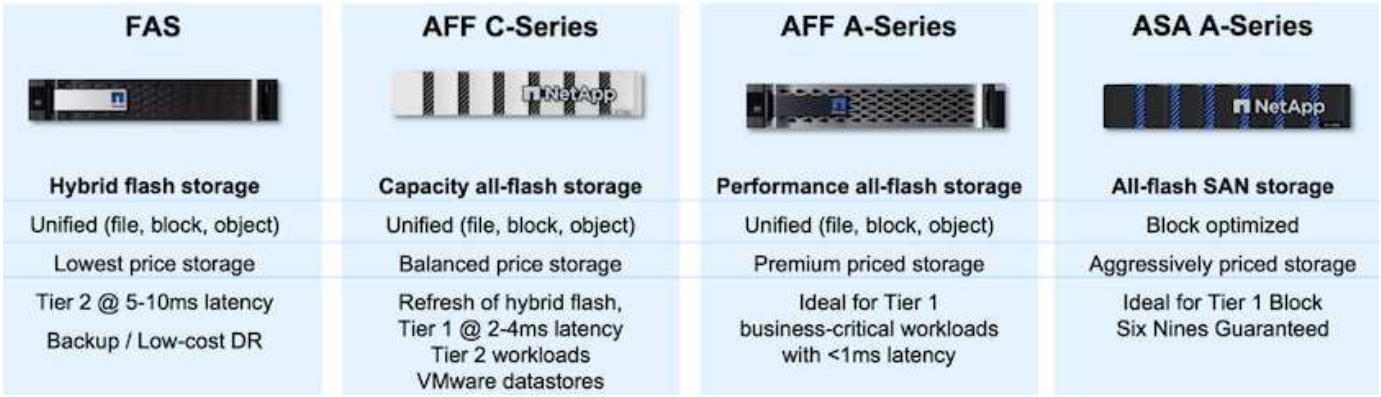
Cas d'utilisation

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde et restauration de machines virtuelles et de banques de données sur site à l'aide du SnapCenter Plug-in for VMware vSphere.
- Sauvegarde et restauration des machines virtuelles et des datastores sur site, hébergés sur des clusters ONTAP et sauvegardés dans un stockage objet à l'aide de NetApp Backup and Recovery for virtual machines.

Stockage de données NetApp ONTAP

ONTAP est la solution de stockage leader du secteur de NetApp qui offre un stockage unifié, que vous y accédiez via des protocoles SAN ou NAS. La stratégie de sauvegarde 3-2-1 garantit que les données sur site sont protégées sur plusieurs types de supports et NetApp propose des plates-formes allant du flash haute vitesse aux supports à moindre coût.



Pour plus d'informations sur toutes les plateformes matérielles de NetApp, consultez "Stockage de données NetApp" .

SnapCenter Plug-in for VMware vSphere

Le plugin SnapCenter pour VMware vSphere est une offre de protection des données étroitement intégrée à VMware vSphere et permet une gestion facile des sauvegardes et des restaurations pour les machines virtuelles. Dans le cadre de cette solution, SnapMirror fournit une méthode rapide et fiable pour créer une deuxième copie de sauvegarde immuable des données de la machine virtuelle sur un cluster de stockage ONTAP secondaire. Avec cette architecture en place, les opérations de restauration de 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 une architecture de plug-in distant. Le plug-in distant s'exécute en dehors du serveur vCenter et est hébergé sur l'appliance virtuelle SCV.

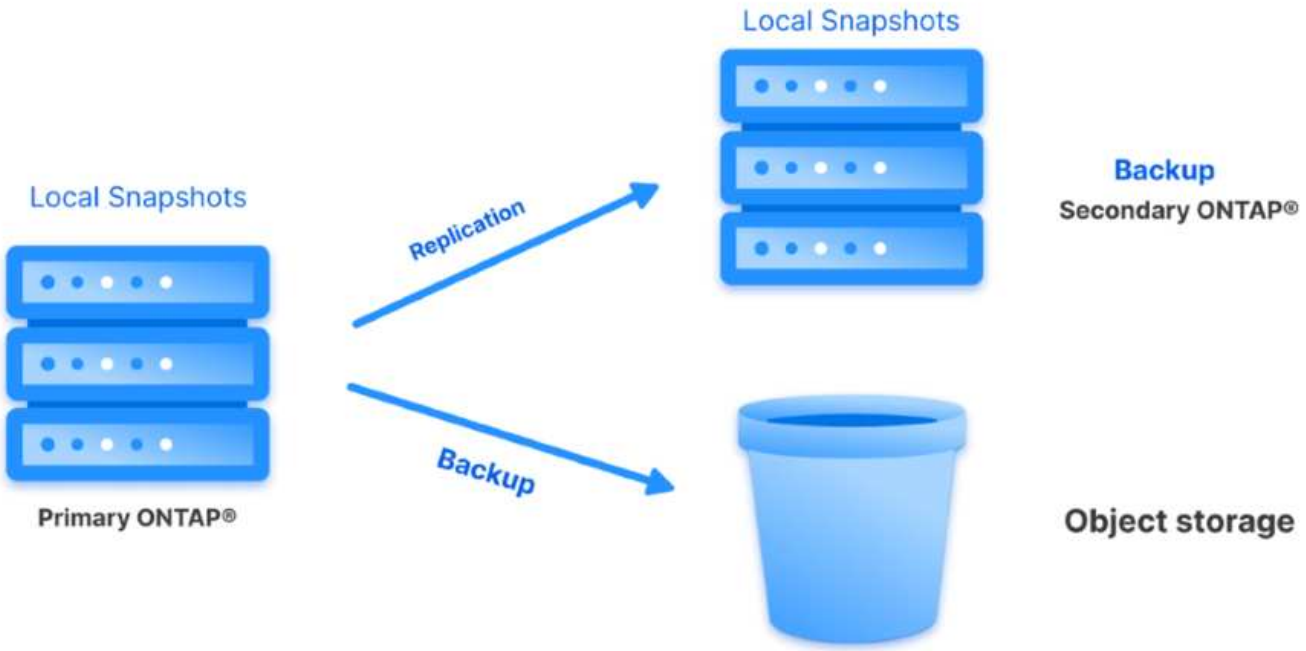
Pour des informations détaillées sur SCV, reportez-vous à "Documentation du SnapCenter Plug-in for VMware vSphere" .

NetApp Backup and Recovery pour protéger les charges de travail VMware

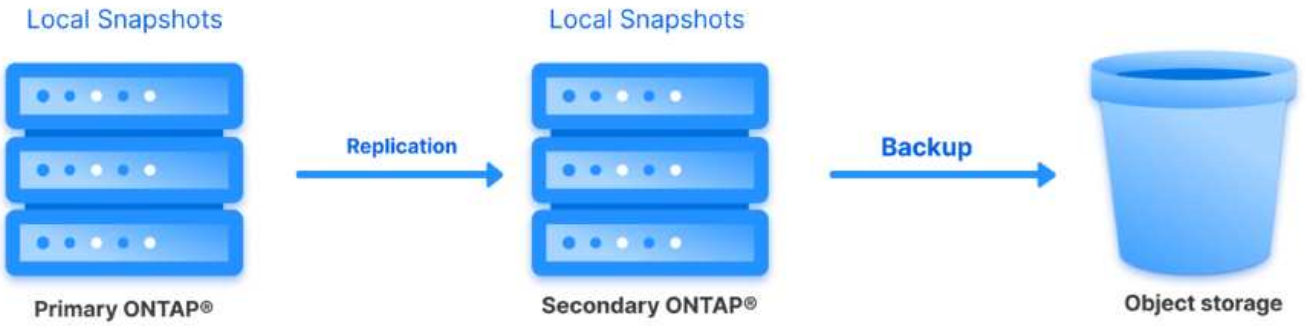
NetApp Backup and Recovery est un outil basé sur le cloud pour la gestion des données qui fournit un plan de contrôle unique pour un large éventail d'opérations de sauvegarde et de restauration dans les environnements sur site et cloud. La suite NetApp Backup and Recovery pour VM comprend une fonctionnalité qui s'intègre au SnapCenter Plugin for VMware vSphere (sur site) afin d'étendre une copie des données vers le stockage objet dans le cloud. Cela établit une troisième copie des données hors site, issue des sauvegardes du stockage primaire ou secondaire. NetApp Backup and Recovery pour VM facilite la configuration de règles de stockage qui transfèrent des copies de vos données depuis l'un ou l'autre de ces deux emplacements sur site.

Le choix entre la sauvegarde principale et la sauvegarde secondaire comme source dans NetApp Backup and Recovery entraînera la mise en œuvre de l'une des deux topologies suivantes :

Topologie en éventail – Lorsqu'une sauvegarde est lancée par le SnapCenter Plug-in for VMware vSphere, un snapshot local est immédiatement créé. SCV lance ensuite une opération SnapMirror qui réplique le snapshot le plus récent vers le cluster ONTAP secondaire. Dans NetApp Backup and Recovery, une règle spécifie le cluster ONTAP principal comme source d'une copie Snapshot des données à transférer vers le stockage objet du fournisseur de cloud de votre choix.



Topologie en cascade – La création des copies de données primaires et secondaires à l'aide de SCV est identique à la topologie en éventail mentionnée précédemment. Toutefois, cette fois-ci, une règle est créée dans NetApp Backup and Recovery, spécifiant que la sauvegarde vers le stockage objet proviendra du cluster ONTAP secondaire.



NetApp Backup and Recovery peut créer des copies de sauvegarde de snapshots ONTAP sur site vers AWS Glacier, Azure Blob et le stockage GCP Archive.



AWS Glacier and Deep Glacier



Azure Blob Archive



GCP Archive Storage

De plus, vous pouvez utiliser NetApp StorageGRID comme cible de sauvegarde du stockage d'objets. Pour en savoir plus sur StorageGRID , reportez-vous au "Page de destination de StorageGRID" .

▼ **Présentation du déploiement de la solution**

Cette liste présente les étapes principales nécessaires à la configuration de cette solution et à l'exécution des opérations de sauvegarde et de restauration à partir de SCV et NetApp Console:

1. Configurez la relation SnapMirror entre les clusters ONTAP à utiliser pour les copies de données principales et secondaires.
2. Configurer le plug-in SnapCenter pour VMware vSphere.
   a. Ajouter des systèmes de stockage
   b. Créer des politiques de sauvegarde
   c. Créer des groupes de ressources
   d. Exécuter les premières tâches de sauvegarde
3. Configurer NetApp Backup and Recovery pour les machines virtuelles
   a. Ajouter un environnement de travail
   b. Découvrez les appliances SCV et vCenter
   c. Créer des politiques de sauvegarde
   d. Activer les sauvegardes
4. Restaurez les machines virtuelles à partir du stockage principal et secondaire à l'aide de SCV.
5. Restaurez les machines virtuelles à partir du stockage d'objets à l'aide de NetApp Console.

▼ **Prérequis**

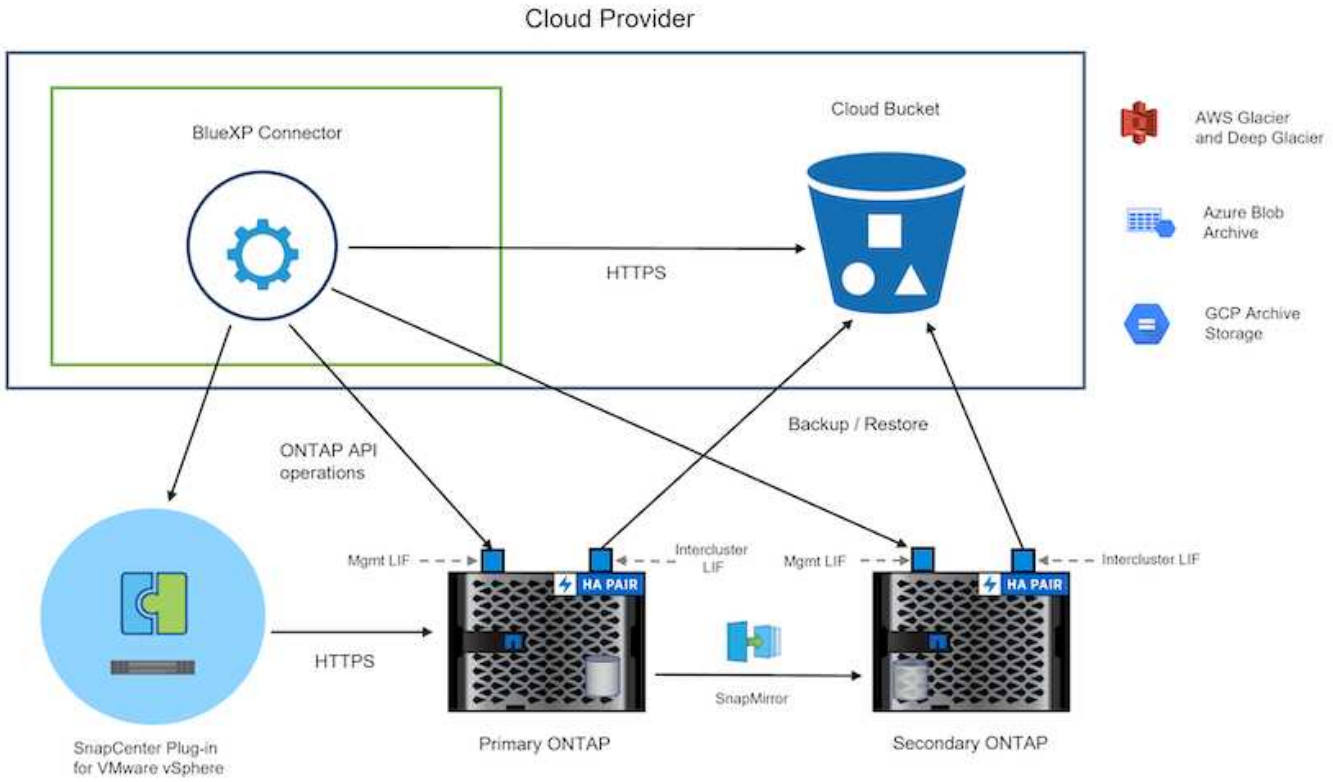
L'objectif de cette solution est de démontrer la protection des données des machines virtuelles exécutées dans VMware vSphere et situées sur des magasins de données NFS hébergés par NetApp ONTAP. Cette solution suppose que les composants suivants sont configurés et prêts à l'emploi :

1. Cluster de stockage ONTAP avec banques de données NFS ou VMFS connectées à VMware vSphere. Les banques de données NFS et VMFS sont prises en charge. Des magasins de données NFS ont été utilisés pour cette solution.
2. Cluster de stockage ONTAP secondaire avec relations SnapMirror établies pour les volumes utilisés pour les banques de données NFS.
3. Agent Console installé pour le fournisseur de cloud utilisé pour les sauvegardes du stockage objet.

4. Les machines virtuelles à sauvegarder se trouvent sur des banques de données NFS résidant sur le cluster de stockage ONTAP principal.
5. Connectivité réseau entre le Console agent et les interfaces de gestion du cluster de stockage ONTAP sur site.
6. Connectivité réseau entre l'agent Console et la VM de l'appliance SCV sur site, et entre l'agent Console et vCenter.
7. Connectivité réseau entre les LIF intercluster ONTAP sur site et le service de stockage d'objets.
8. DNS configuré pour la gestion SVM sur les clusters de stockage ONTAP principaux et secondaires. Pour plus d'informations, reportez-vous à "Configurer DNS pour la résolution du nom d'hôte" .

Architecture de haut niveau

Les tests/validations de cette solution ont été réalisés dans un laboratoire qui peut ou non correspondre à l'environnement de déploiement final.



Déploiement de la solution

Dans cette solution, nous fournissons des instructions détaillées pour déployer et valider une solution qui utilise SnapCenter Plug-in for VMware vSphere, ainsi que Backup and Recovery, afin d'effectuer la sauvegarde et la restauration de machines virtuelles Windows et Linux au sein d'un cluster VMware vSphere situé dans un centre de données sur site. Les machines virtuelles de cette configuration sont stockées sur des datastores NFS hébergés par un cluster de stockage ONTAP A300. De plus, 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 a été utilisé comme cible pour une troisième copie des données.

Nous allons aborder la création de relations SnapMirror pour les copies secondaires de nos sauvegardes gérées par SCV et la configuration des tâches de sauvegarde dans SCV et NetApp Console.

Pour des informations détaillées sur le SnapCenter Plug-in for VMware vSphere, reportez-vous au "Documentation du SnapCenter Plug-in for VMware vSphere" .

Pour des informations détaillées sur Backup and Recovery, reportez-vous au "Documentation Backup and Recovery".

Établir des relations SnapMirror entre les clusters ONTAP

Le SnapCenter Plug-in for VMware vSphere utilise la technologie ONTAP SnapMirror pour gérer le transport des copies SnapMirror et/ou SnapVault secondaires vers un cluster ONTAP secondaire.

Les politiques de sauvegarde SCV ont la possibilité d'utiliser les relations SnapMirror ou SnapVault . La principale différence est que lorsque vous utilisez l'option SnapMirror , la planification de conservation configurée pour les sauvegardes dans la politique sera la même aux emplacements principal et secondaire. SnapVault est conçu pour l'archivage et lorsque vous utilisez cette option, un calendrier de conservation distinct peut être établi avec la relation SnapMirror pour les copies de snapshots sur le cluster de stockage ONTAP secondaire.

La configuration des relations SnapMirror peut être effectuée dans NetApp Console, où de nombreuses étapes sont automatisées, ou à l'aide de System Manager et de l'ONTAP CLI. Toutes ces méthodes sont décrites ci-dessous.

Établir des relations SnapMirror avec NetApp Console

Les étapes suivantes doivent être effectuées à partir de la NetApp Console :

▼ **Configuration de la réplication pour les systèmes de stockage ONTAP primaires et secondaires**

Commencez par vous connecter à la NetApp Console, puis accédez à Systèmes.

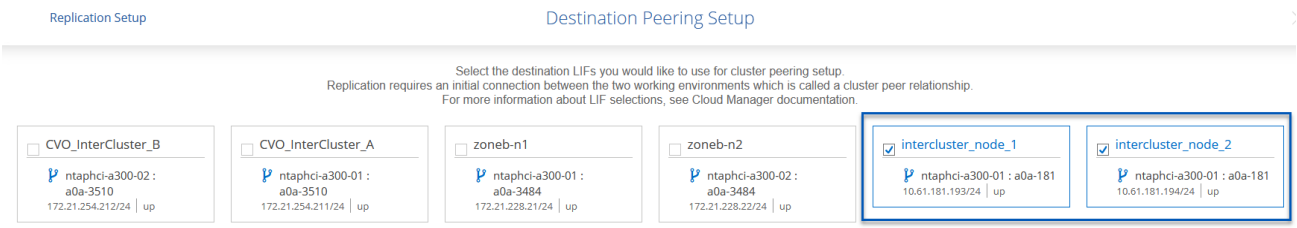
1. Faites glisser et déposez le système de stockage ONTAP source (principal) sur le système de stockage ONTAP de destination (secondaire).



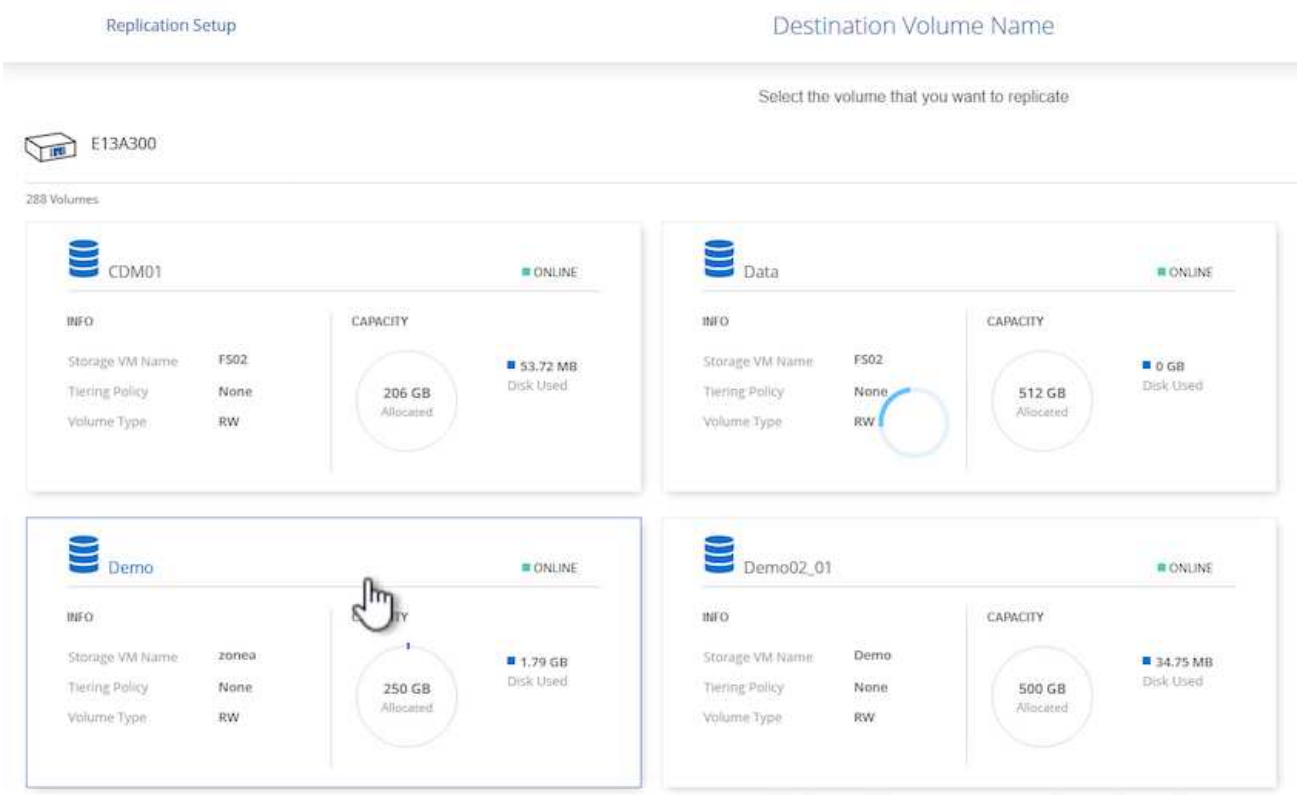
2. Dans le menu qui apparaît, sélectionnez **Réplication**.



3. Sur la page **Configuration du peering de destination**, sélectionnez les LIF intercluster de destination à utiliser pour la connexion entre les systèmes de stockage.

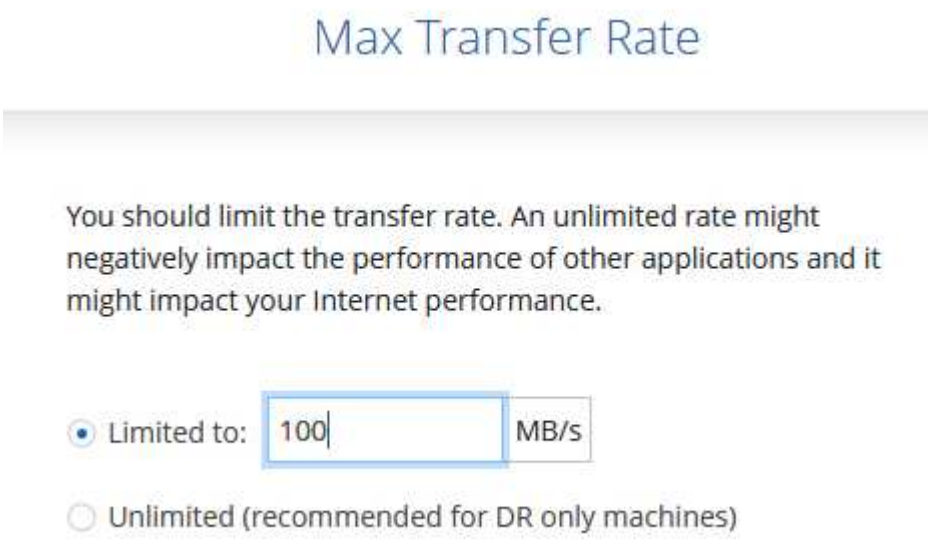


4. Sur la page **Nom du volume de destination**, sélectionnez d'abord le volume source, puis renseignez le nom du volume de destination et sélectionnez le SVM de destination et l'agrégat. Cliquez sur **Suivant** pour continuer.

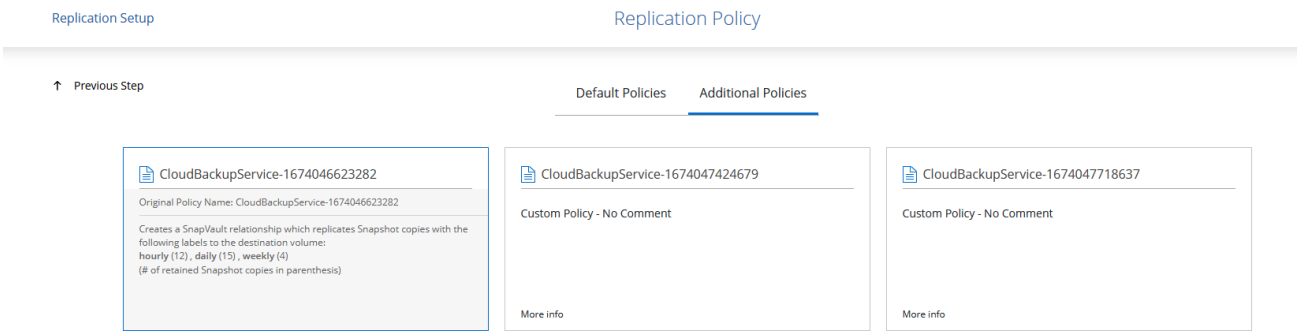




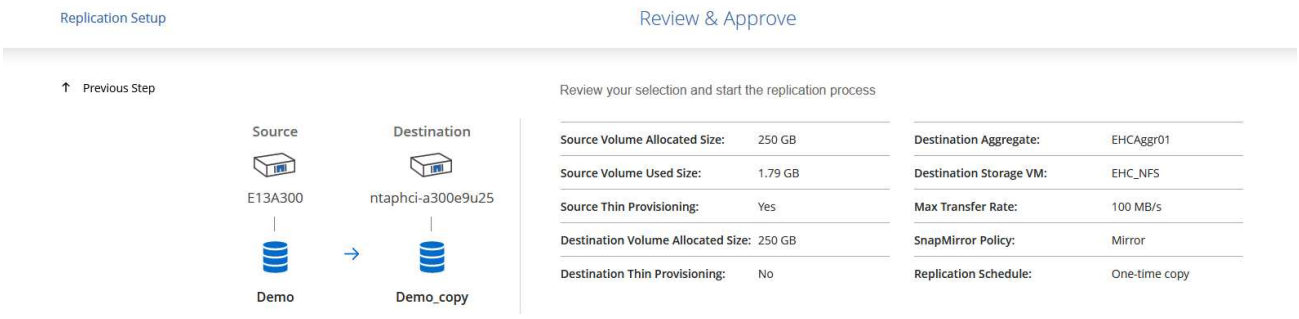
5. Choisissez le taux de transfert maximal auquel la réplication doit se produire.



6. Choisissez la politique qui déterminera le calendrier de conservation des sauvegardes secondaires. Cette politique peut être créée au préalable (voir le processus manuel ci-dessous dans l'étape **Créer une politique de conservation des instantanés**) ou peut être modifiée après coup si vous le souhaitez.



7. Enfin, vérifiez toutes les informations et cliquez sur le bouton **Go** pour démarrer le processus de configuration de la réplication.



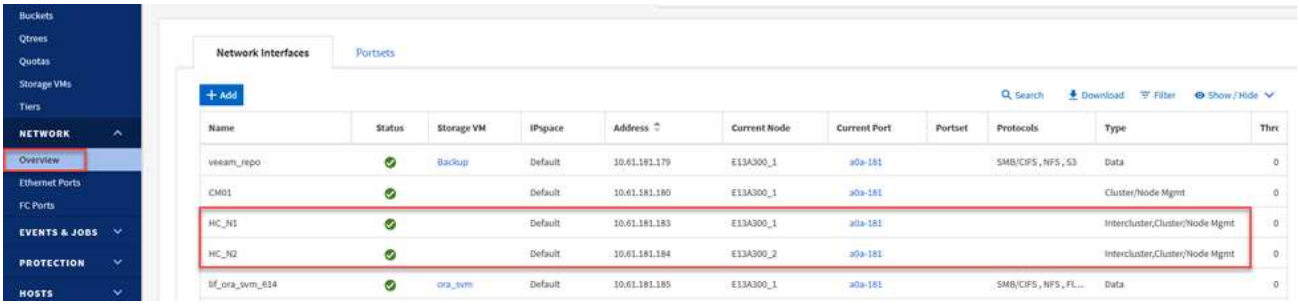
Établir des relations SnapMirror avec System Manager et ONTAP CLI

Toutes les étapes requises pour établir des relations SnapMirror peuvent être réalisées avec System Manager ou l'interface de ligne de commande 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 de destination, vous pouvez récupérer les informations LIF inter-cluster à partir du Gestionnaire système ou de l'interface de ligne de commande.

1. Dans ONTAP System Manager, accédez à la page Présentation du réseau et récupérez les adresses IP de type : Intercluster qui sont configurées pour communiquer avec le VPC AWS sur lequel FSx est installé.



2. Pour récupérer les adresses IP intercluster à l'aide de la CLI, exécutez la commande suivante :

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

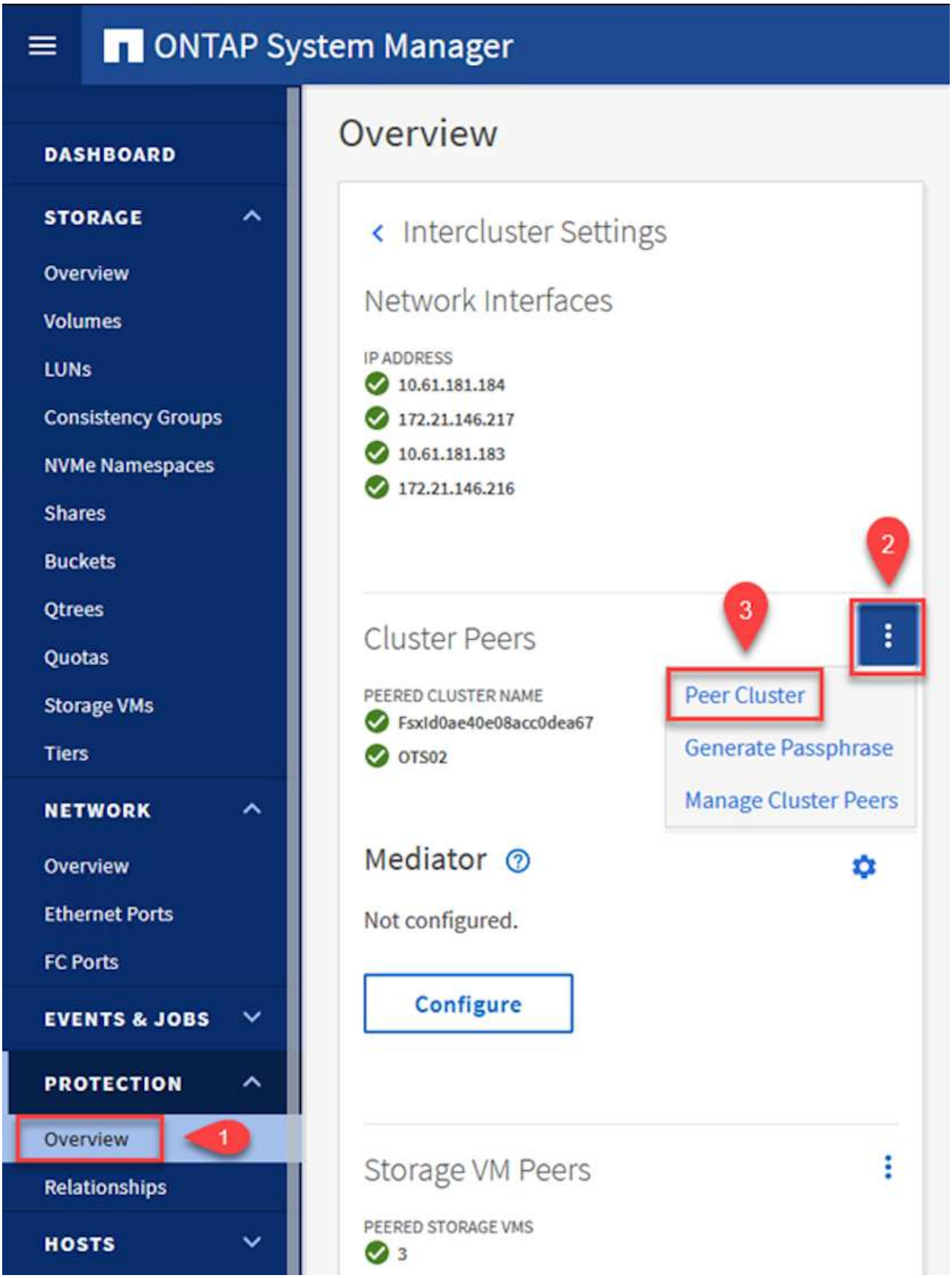
▼ **Établir un peering de cluster entre les clusters ONTAP**

Pour établir un peering de cluster entre les clusters ONTAP , une phrase secrète unique entrée dans le cluster ONTAP initiateur doit être confirmée dans l'autre cluster homologue.

1. Configurer le peering sur le cluster ONTAP de destination à l'aide de `cluster peer create` commande. Lorsque vous y êtes invité, entrez une phrase secrète unique qui sera 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. Au niveau du cluster source, vous pouvez établir la relation entre homologues du cluster à l'aide d' ONTAP System Manager ou de l'interface de ligne de commande. Depuis ONTAP System Manager, accédez à Protection > Présentation et sélectionnez Cluster homologue.



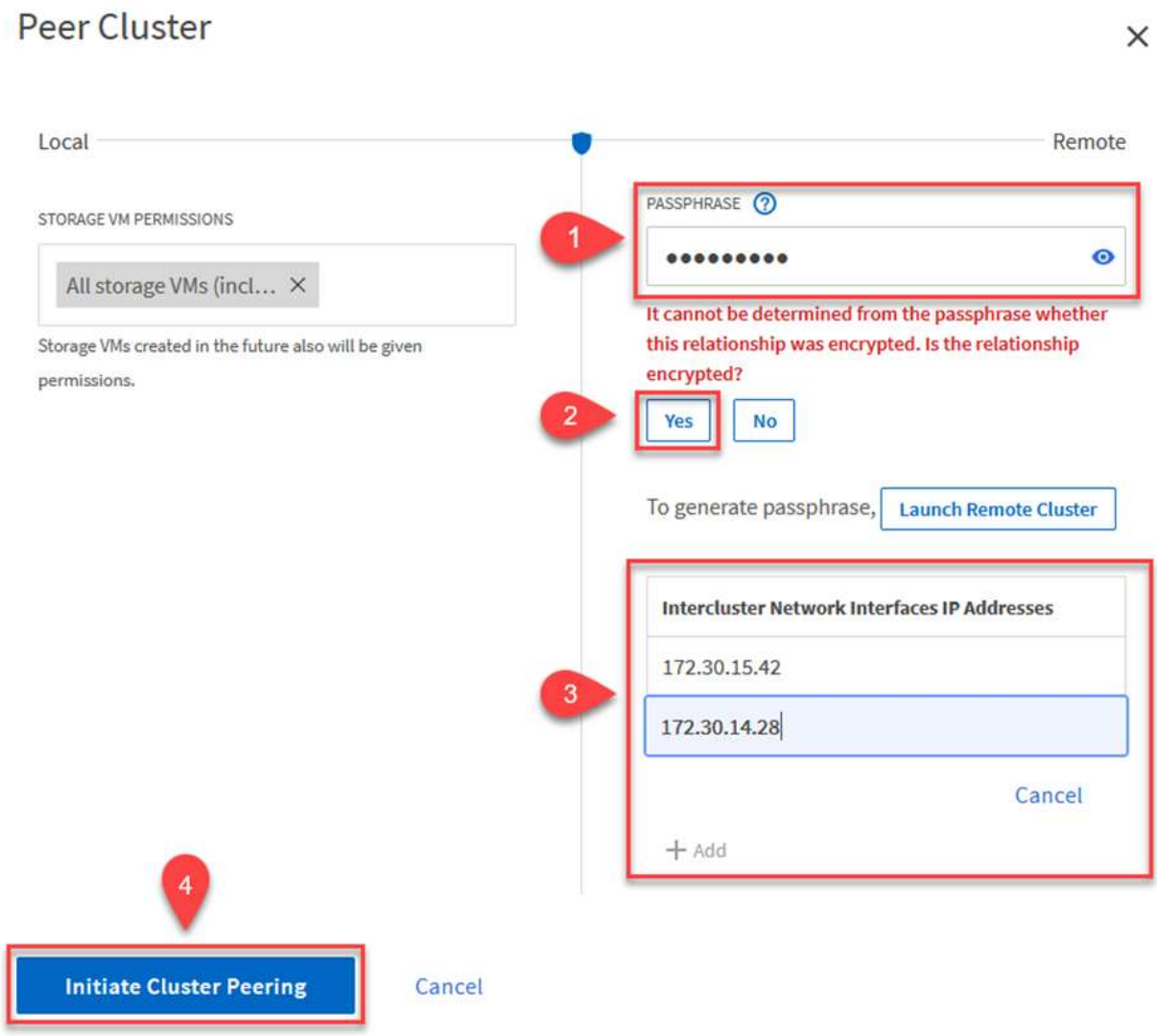
3. Dans la boîte de dialogue Cluster homologue, remplissez les informations requises :
   a. Saisissez la phrase secrète utilisée pour établir la relation de cluster homologue sur le cluster

ONTAP de destination.

b. Sélectionner `Yes` pour établir une relation cryptée.

c. Saisissez la ou les adresses IP LIF intercluster du cluster ONTAP de destination.

d. Cliquez sur Initier l'appairage de cluster pour finaliser le processus.



4. Vérifiez l'état de la relation entre les homologues du cluster à partir du cluster ONTAP de destination avec la commande suivante :

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

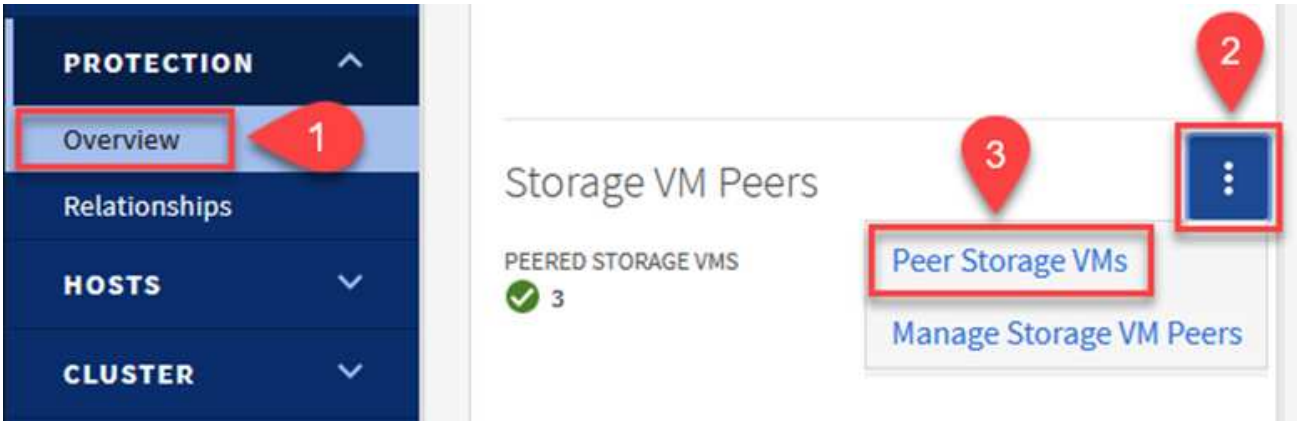
▼ **Établir une relation de peering SVM**

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

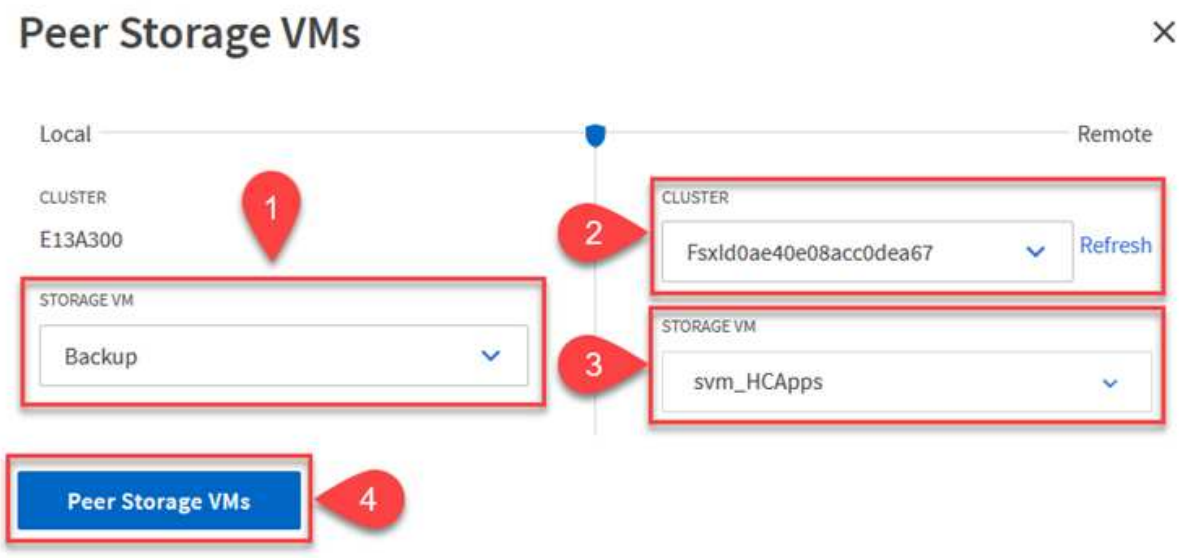
1. À partir du cluster ONTAP de destination, utilisez la commande suivante depuis l'interface de ligne de commande pour créer la relation homologue SVM :

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

2. À partir du cluster ONTAP source, acceptez la relation de peering avec ONTAP System Manager ou l'interface de ligne de commande.
3. Depuis ONTAP System Manager, accédez à Protection > Présentation et sélectionnez Machines virtuelles de stockage homologues sous Homologues de machines virtuelles de stockage.



4. Dans la boîte de dialogue de la machine virtuelle de stockage homologue, remplissez les champs obligatoires :
   - La machine virtuelle de stockage source
   - Le cluster de destination
   - La machine virtuelle de stockage de destination



5. Cliquez sur « Appairer les machines virtuelles de stockage » pour terminer le processus d'appairage SVM.

▼ Créer une politique de conservation des instantanés

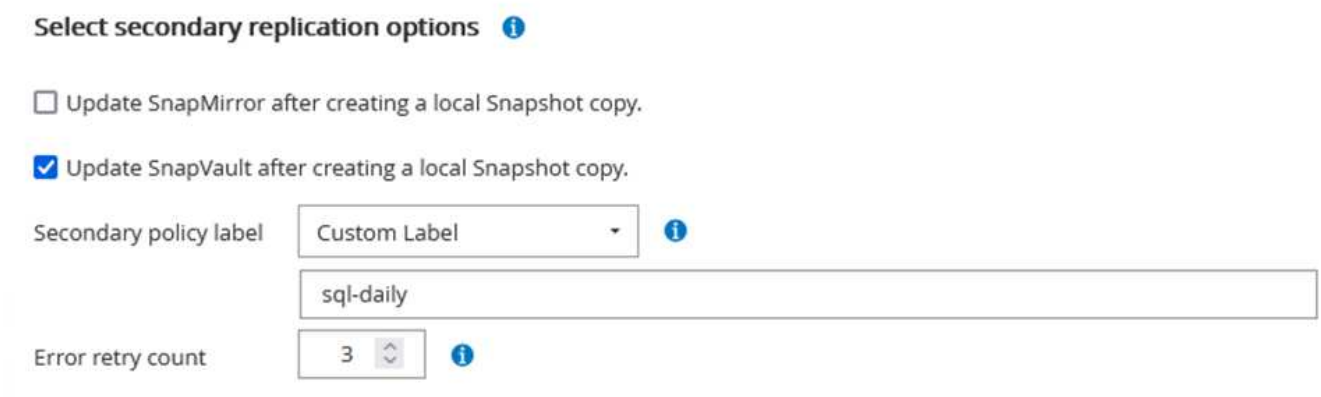
SnapCenter gère les planifications de conservation pour les sauvegardes qui existent sous forme de copies

instantanées sur le système de stockage principal. Ceci est établi lors de la création d'une politique dans SnapCenter. SnapCenter ne gère pas les politiques de rétention pour les sauvegardes conservées sur des systèmes de stockage secondaires. Ces politiques sont gérées séparément via une politique SnapMirror créée sur le cluster FSx secondaire et associée aux volumes de destination qui sont dans une relation SnapMirror avec le volume source.

Lors de la création d'une politique SnapCenter , vous avez la possibilité de spécifier une étiquette de politique secondaire qui est ajoutée à l'étiquette SnapMirror de chaque snapshot généré lorsqu'une sauvegarde SnapCenter est effectuée.

Sur le stockage secondaire, ces étiquettes correspondent aux règles de stratégie associées au volume de destination afin d'appliquer la conservation des instantanés.

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



Pour plus d'informations sur la création de politiques SnapCenter pour une base de données SQL Server, consultez le "Documentation de SnapCenter" .

Vous devez d'abord créer une stratégie SnapMirror avec des règles qui dictent le nombre de copies d'instantanés à conserver.

1. Créez la politique 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 politique avec des étiquettes SnapMirror qui correspondent aux étiquettes de politique secondaires spécifiées dans les politiques 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 pourrait être ajoutée à une politique :

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

Créez des règles supplémentaires pour chaque étiquette SnapMirror et le nombre d'instantanés à conserver (période de conservation).

▼ **Créer des volumes de destination**

Pour créer un volume de destination sur ONTAP qui sera le destinataire des copies instantanées de nos volumes sources, exécutez la commande suivante sur le cluster ONTAP de destination :

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

▼ **Créer les 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 nouvel instantané généré à partir du volume source et le copie sur 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
```

Configurer le SnapCenter Plug-in for VMware vSphere

Une fois installé, le SnapCenter Plug-in for VMware vSphere est accessible à partir de l'interface de gestion de vCenter Server Appliance. SCV gérera les sauvegardes des banques de données NFS montées sur les hôtes ESXi et qui contiennent les machines virtuelles Windows et Linux.

Passez en revue le "Flux de travail de protection des données" section de la documentation SCV pour plus d'informations sur les étapes impliquées dans la configuration des sauvegardes.

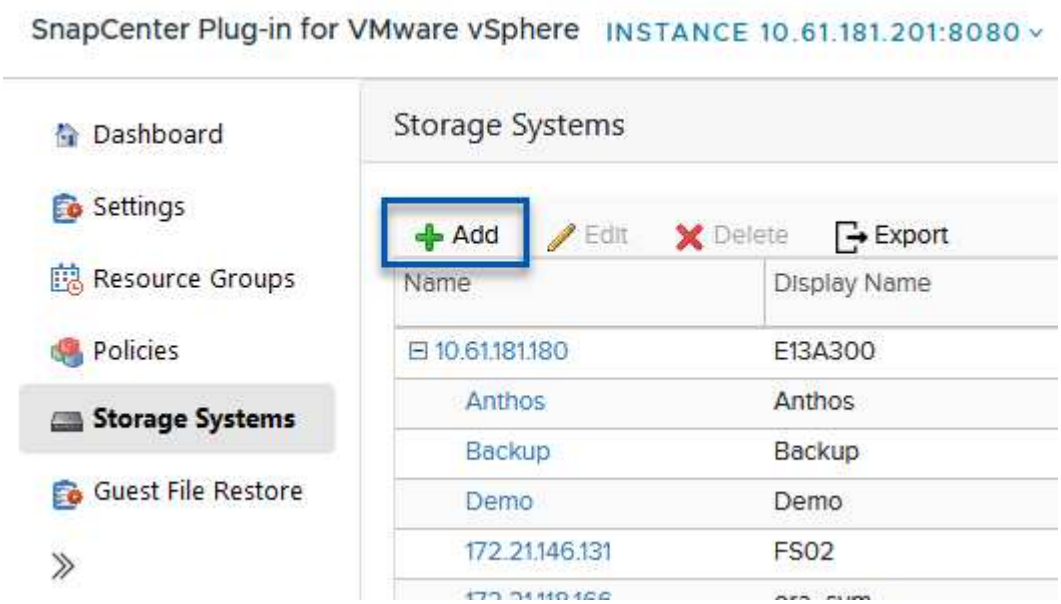
Pour configurer les sauvegardes de vos machines virtuelles et de vos banques de données, les étapes suivantes doivent être effectuées à partir de l'interface du plug-in.

▼ **Systèmes de stockage Discovery ONTAP**

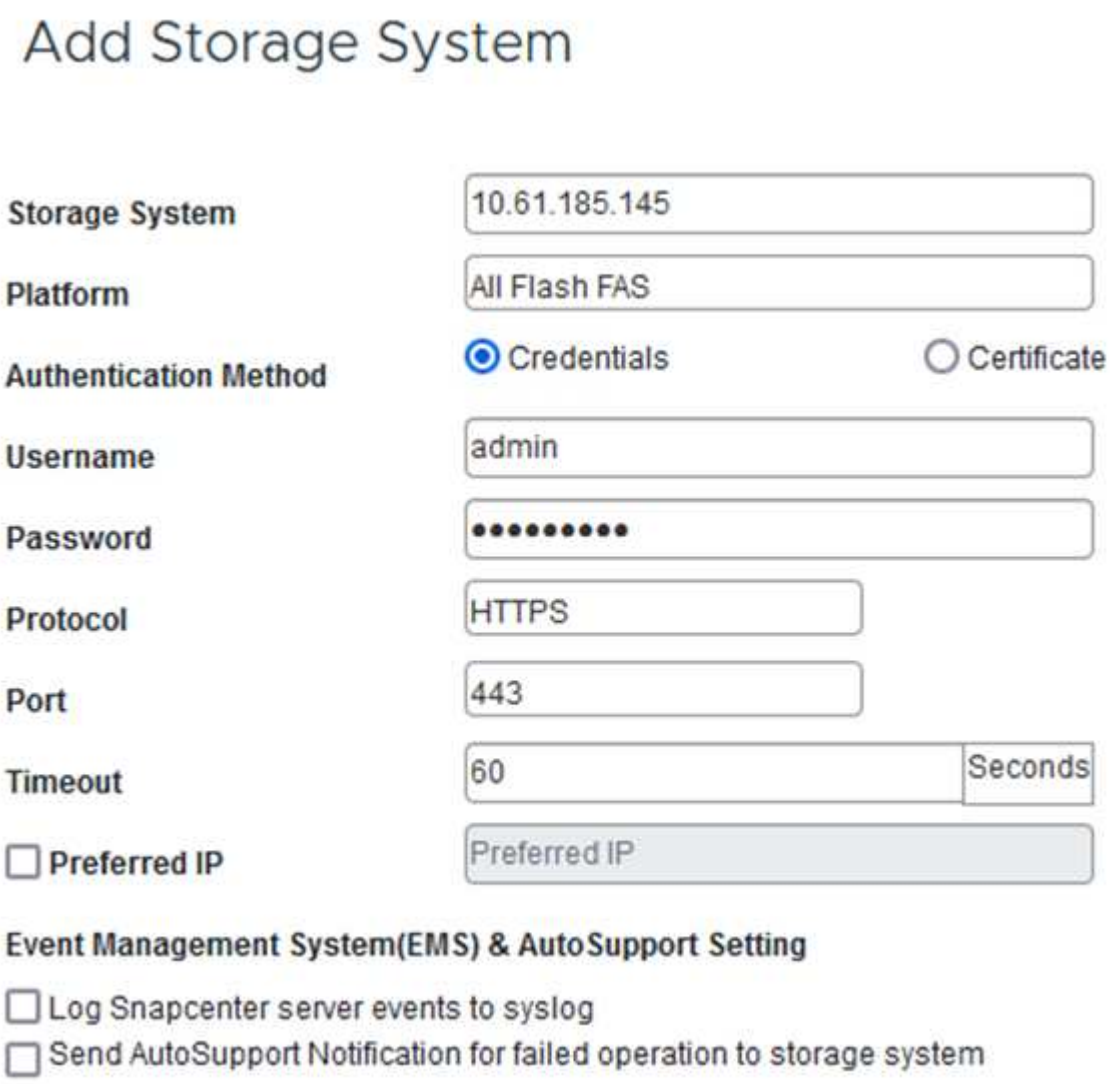
Découvrez les clusters de stockage ONTAP à utiliser pour les sauvegardes principales et secondaires.

1. Dans le SnapCenter Plug-in for VMware vSphere, accédez à **Systèmes de stockage** dans le menu de

gauche et cliquez sur le bouton **Ajouter**.



2. Remplissez les informations d'identification et le type de plate-forme pour le système de stockage ONTAP principal et cliquez sur **Ajouter**.



3. Répétez cette procédure pour le système de stockage ONTAP secondaire.

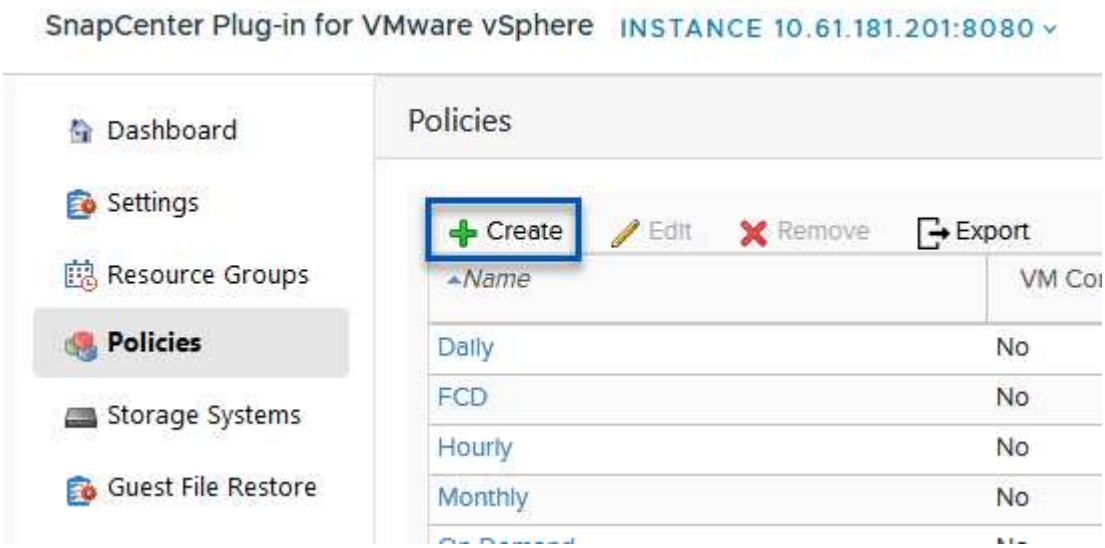
▼ **Créer des politiques de sauvegarde SCV**

Les politiques spécifient la période de conservation, la fréquence et les options de réplication pour les sauvegardes gérées par SCV.

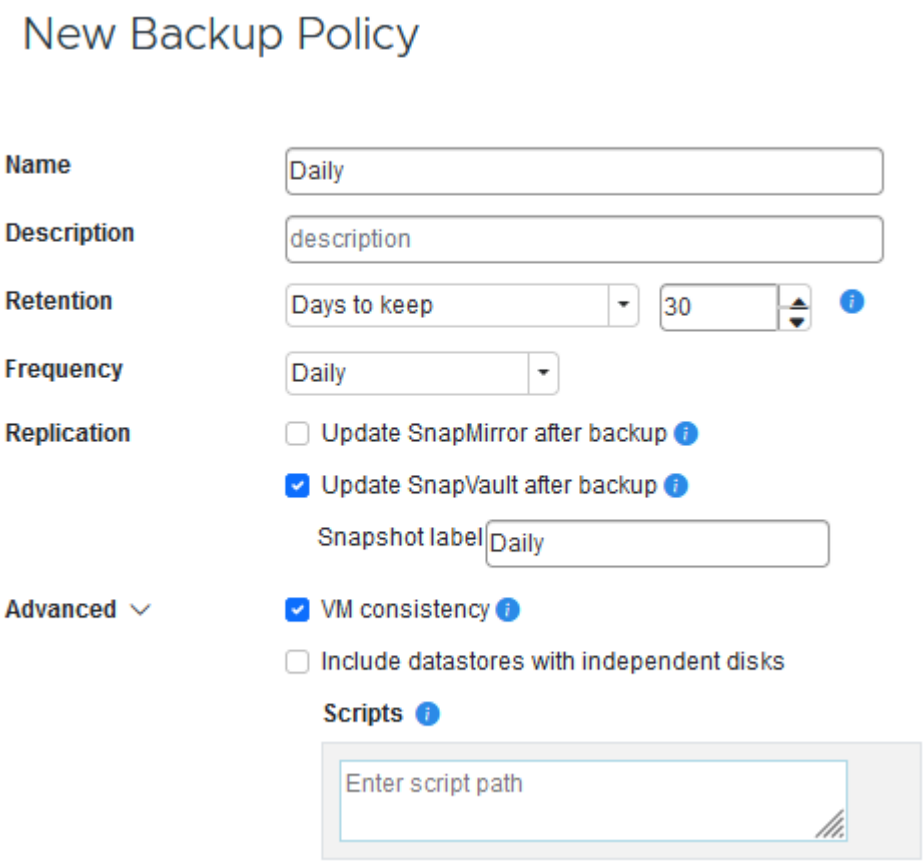
Passez en revue le "Créer des politiques de sauvegarde pour les machines virtuelles et les banques de données" section de la documentation pour plus d'informations.

Pour créer des politiques de sauvegarde, procédez comme suit :

1. Dans le SnapCenter Plug-in for VMware vSphere, accédez à **Politiques** dans le menu de gauche et cliquez sur le bouton **Créer**.



2. Spécifiez un nom pour la politique, la période de conservation, la fréquence et les options de réplication, ainsi que l'étiquette de l'instantané.



Lors de la création d'une politique dans le plug-in SnapCenter , vous verrez des options pour SnapMirror et SnapVault. Si vous choisissez SnapMirror, le calendrier de conservation spécifié dans la stratégie sera le même pour les snapshots principaux et secondaires. Si vous choisissez SnapVault, la planification de conservation du snapshot secondaire sera basée sur une planification distincte implémentée avec la relation SnapMirror . Ceci est utile lorsque vous souhaitez des périodes de conservation plus

longues pour les sauvegardes secondaires.

Les étiquettes Snapshot sont utiles, car elles peuvent être utilisées pour appliquer des règles avec une période de conservation spécifique aux copies SnapVault répliquées vers le cluster ONTAP secondaire. Lorsque SCV est utilisé avec NetApp Data Services, le champ d'étiquette Snapshot doit être vide ou correspondre à l'étiquette spécifiée dans la règle de sauvegarde.

3. Répétez la procédure pour chaque politique requise. Par exemple, des politiques distinctes pour les sauvegardes quotidiennes, hebdomadaires et mensuelles.

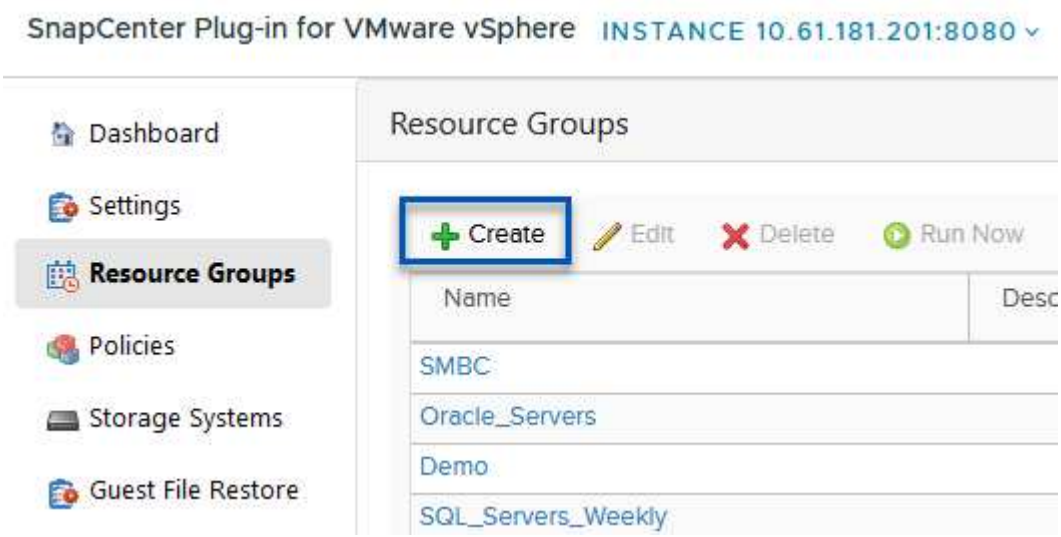
▼ **Créer des groupes de ressources**

Les groupes de ressources contiennent les banques de données et les machines virtuelles à inclure dans une tâche de sauvegarde, ainsi que la politique et la planification de sauvegarde associées.

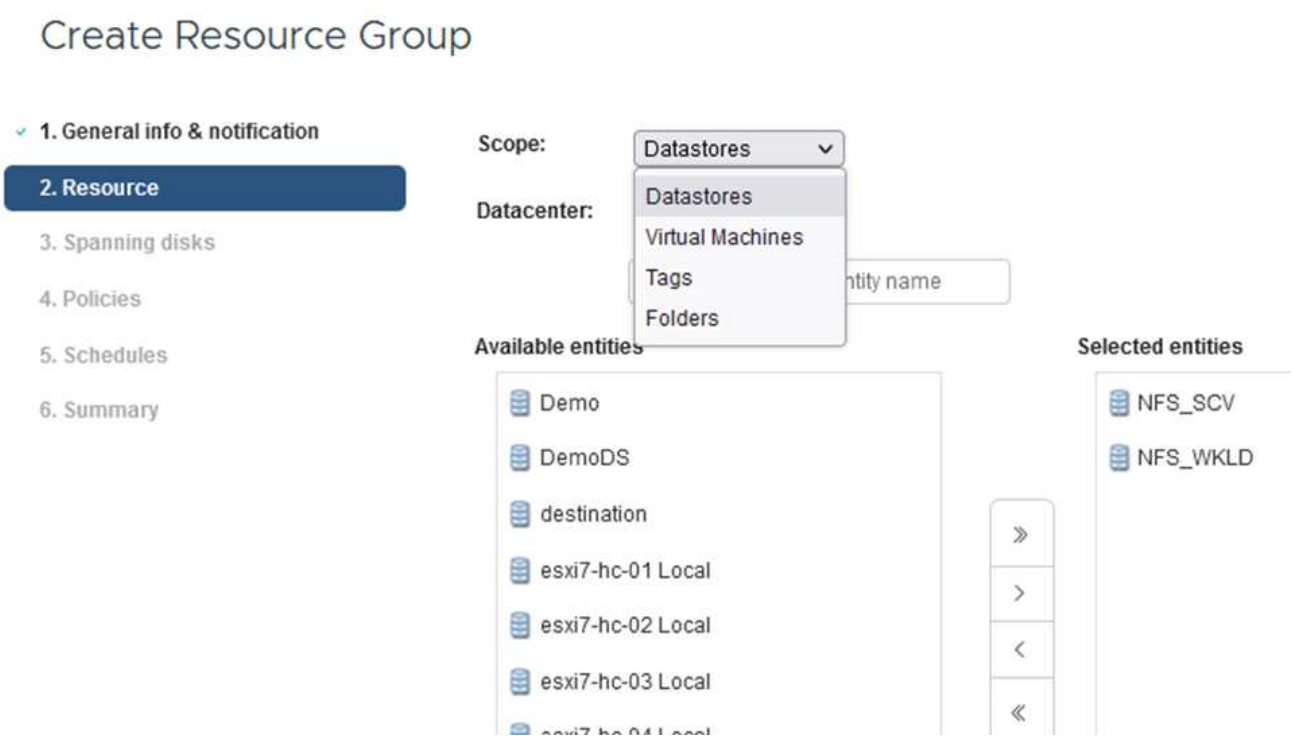
Passez en revue le "Créer des groupes de ressources" section de la documentation pour plus d'informations.

Pour créer des groupes de ressources, procédez comme suit.

1. Dans le SnapCenter Plug-in for VMware vSphere, accédez à **Groupes de ressources** dans le menu de gauche et cliquez sur le bouton **Créer**.

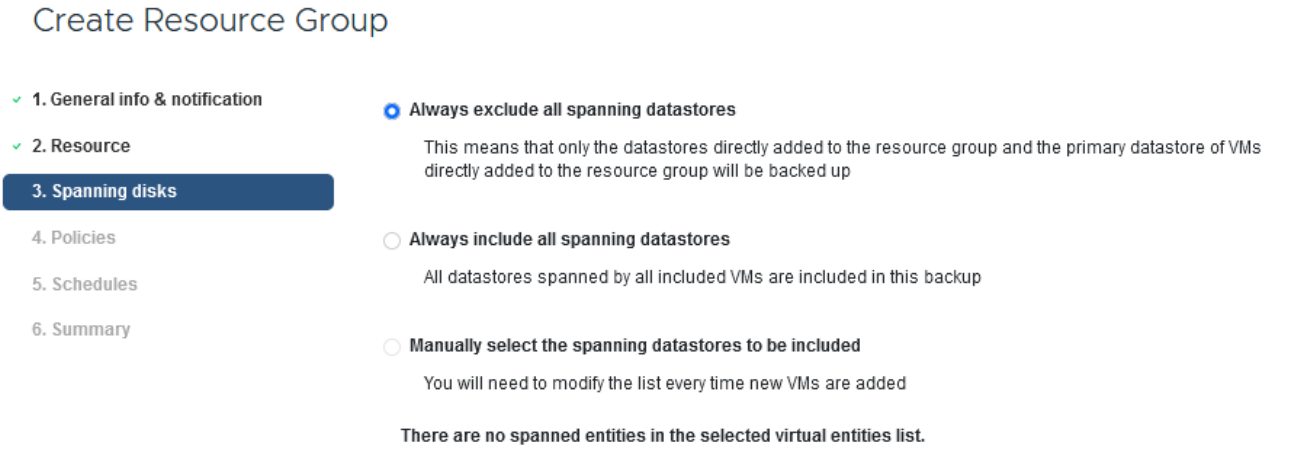


2. Dans l'assistant Créer un groupe de ressources, entrez un nom et une description pour le groupe, ainsi que les informations requises pour recevoir des notifications. Cliquez sur **Suivant**
3. Sur la page suivante, sélectionnez les banques de données et les machines virtuelles que vous souhaitez inclure dans la tâche de sauvegarde, puis cliquez sur **Suivant**.



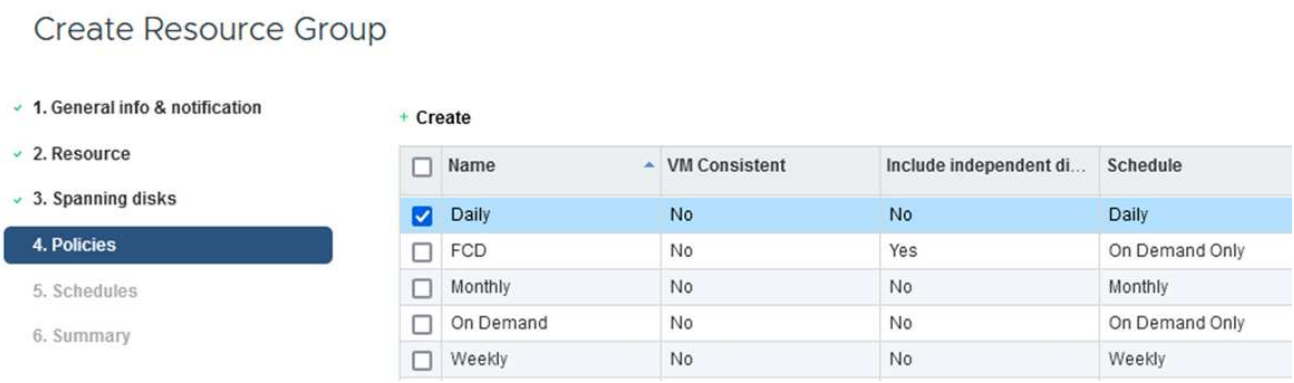
Vous avez la possibilité de sélectionner des machines virtuelles spécifiques ou des banques de données entières. Quel que soit votre choix, l'intégralité du volume (et du magasin de données) est sauvegardée puisque la sauvegarde est le résultat de la prise d'un instantané du volume sous-jacent. Dans la plupart des cas, il est plus simple de choisir l'ensemble du magasin de données. Cependant, si vous souhaitez limiter la liste des machines virtuelles disponibles lors de la restauration, vous pouvez choisir uniquement un sous-ensemble de machines virtuelles pour la sauvegarde.

4. Choisissez les options de répartition des banques de données pour les machines virtuelles avec des VMDK résidant sur plusieurs banques de données, puis cliquez sur **Suivant**.



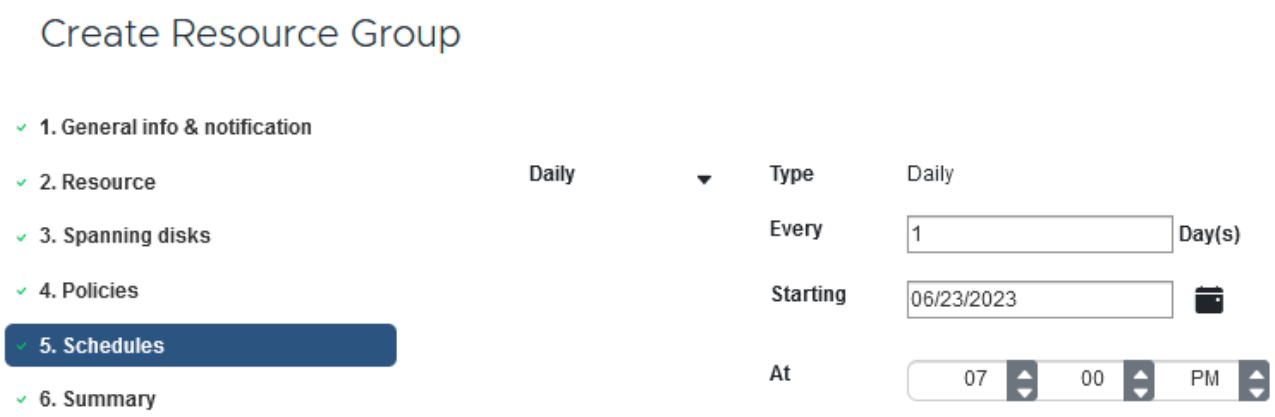
La sauvegarde et la restauration pour protéger les charges de travail VMware ne prennent actuellement pas en charge la sauvegarde des machines virtuelles avec des VMDK répartis sur plusieurs datastores.

5. Sur la page suivante, sélectionnez les politiques qui seront associées au groupe de ressources et cliquez sur **Suivant**.



Lors de la sauvegarde de snapshots gérés par SCV sur un stockage d'objets à l'aide de Backup and Recovery, chaque groupe de ressources ne peut être associé qu'à une seule stratégie.

6. Sélectionnez une planification qui déterminera à quelles heures les sauvegardes seront exécutées. Cliquez sur **Suivant**.

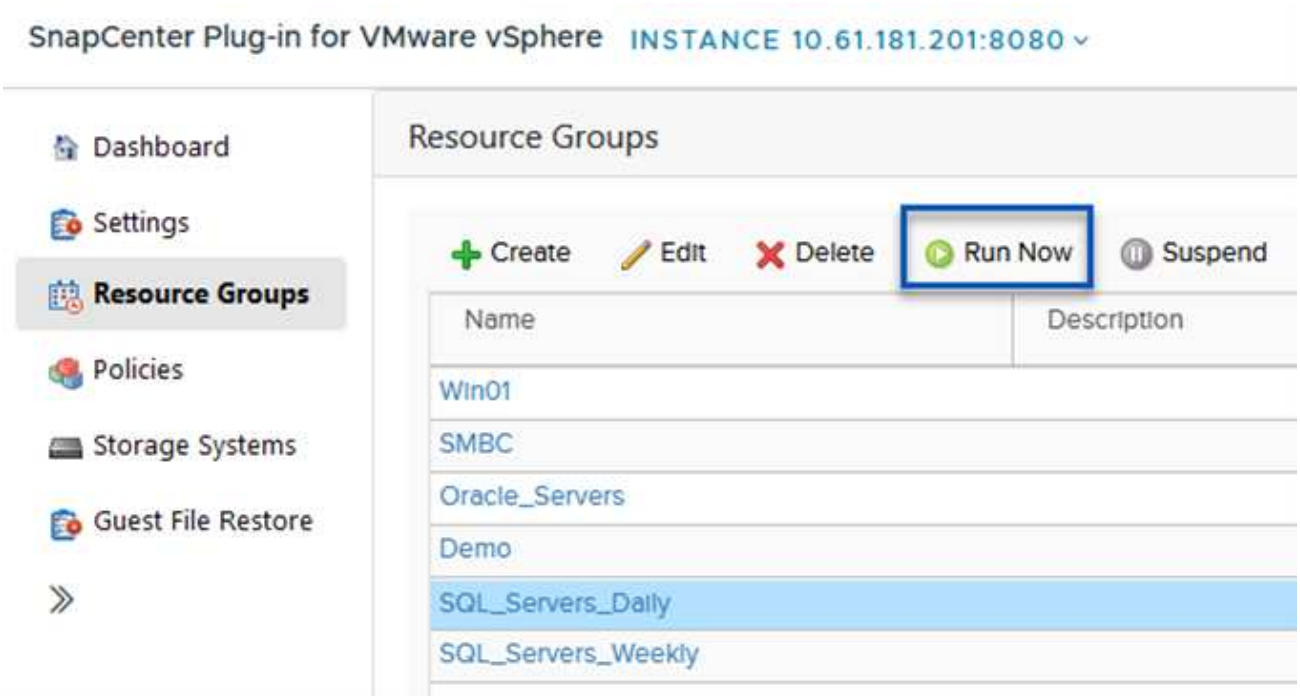


7. Enfin, consultez la page de résumé, puis cliquez sur **Terminer** pour terminer la création du groupe de ressources.

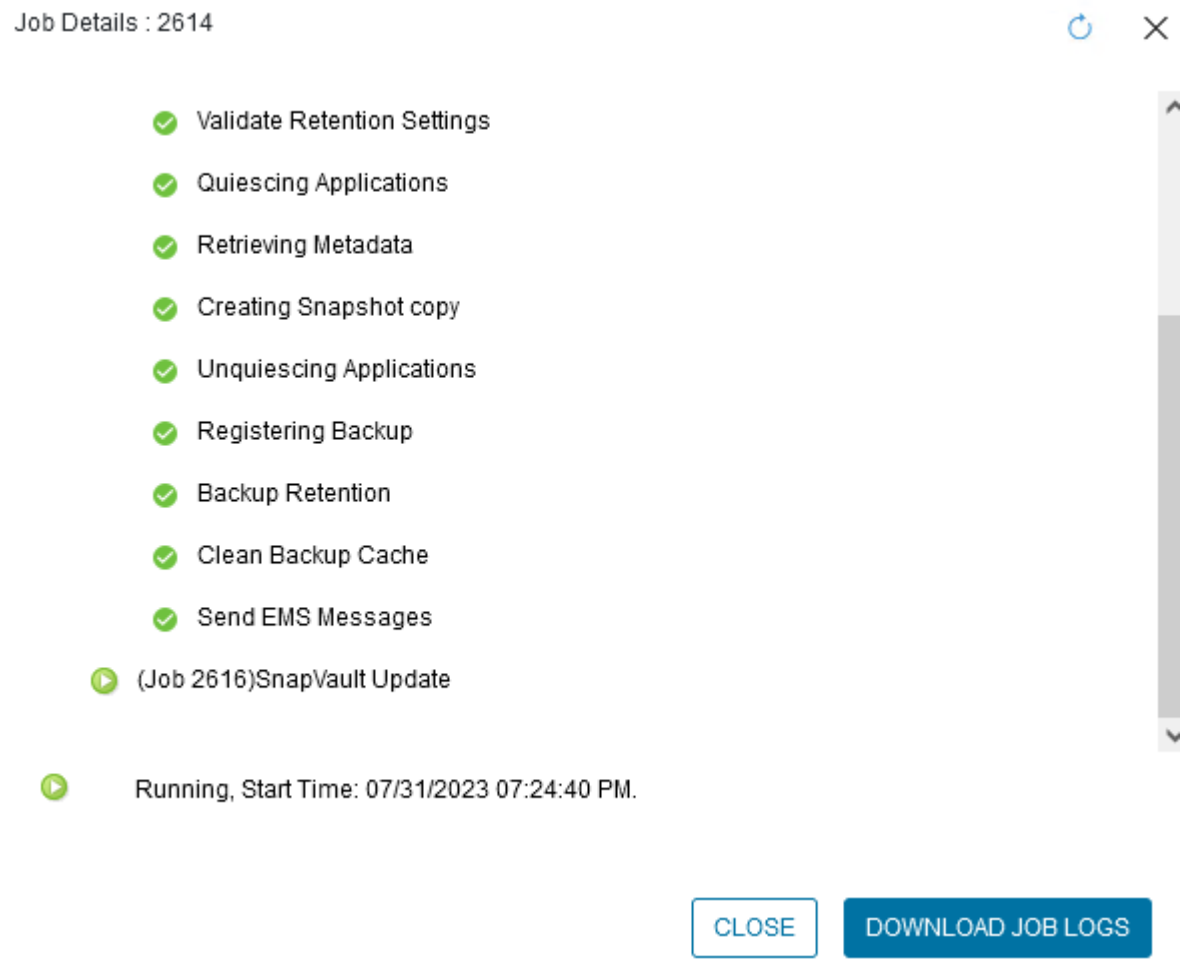
▼ Exécuter une tâche de sauvegarde

Dans cette dernière étape, exécutez une tâche de sauvegarde et suivez sa progression. Au moins une tâche de sauvegarde doit être menée à bien dans SCV avant que les ressources puissent être détectées depuis NetApp Console.

1. Dans le SnapCenter Plug-in for VMware vSphere, accédez à **Groupes de ressources** 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 **Tableau de bord** dans le menu de gauche. Sous **Activités de travail récentes**, cliquez sur le numéro d'identification du travail pour suivre la progression du travail.



Configurer les sauvegardes vers le stockage objet dans NetApp Console

Pour que NetApp Console puisse gérer efficacement l'infrastructure de données, l'installation préalable d'un agent Console est nécessaire. L'agent Console exécute les actions liées à la découverte des ressources et à la gestion des opérations de données.

Pour plus d'informations sur l'agent Console, consultez "Découvrez les agents Console" la documentation de NetApp Console.

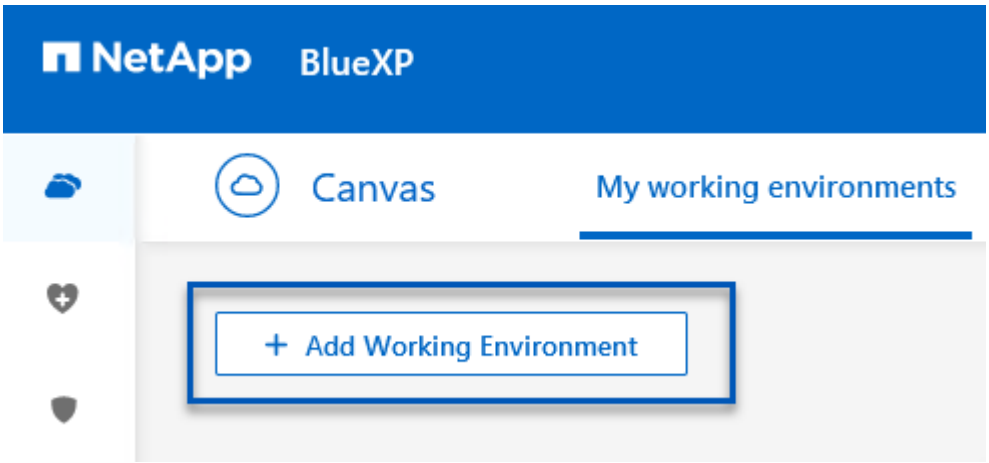
Une fois l'agent installé pour le fournisseur de cloud utilisé, une représentation graphique du stockage d'objets sera visible depuis Systems.

Pour configurer Backup and Recovery afin de sauvegarder les données gérées par SCV sur site, procédez comme suit :

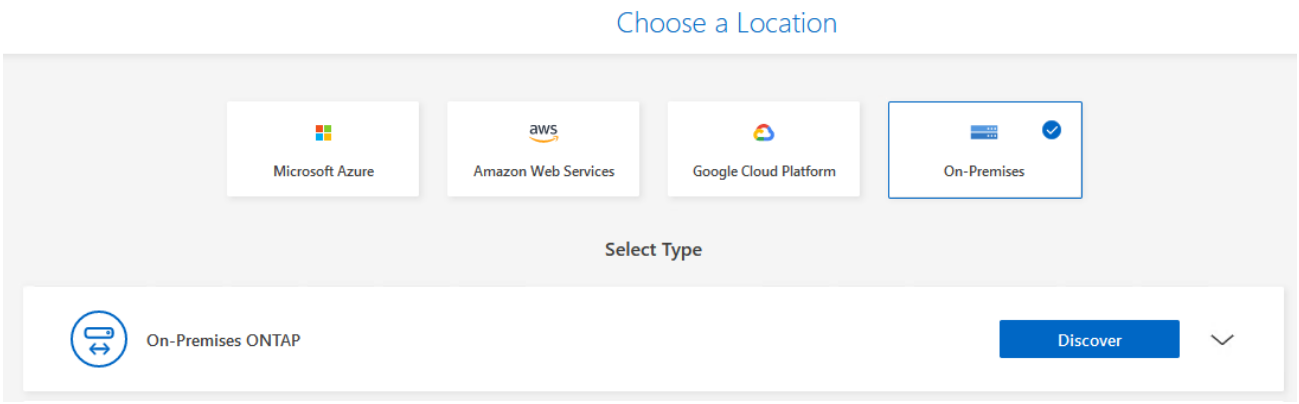
▼ **Ajouter le système de stockage ONTAP aux systèmes**

La première étape consiste à ajouter les systèmes de stockage ONTAP sur site à NetApp Console.

1. Dans la section Systèmes, cliquez sur **+ Ajouter** pour commencer.



2. Sélectionnez **Sur site** parmi le choix d'emplacements, puis cliquez sur le bouton **Découvrir**.



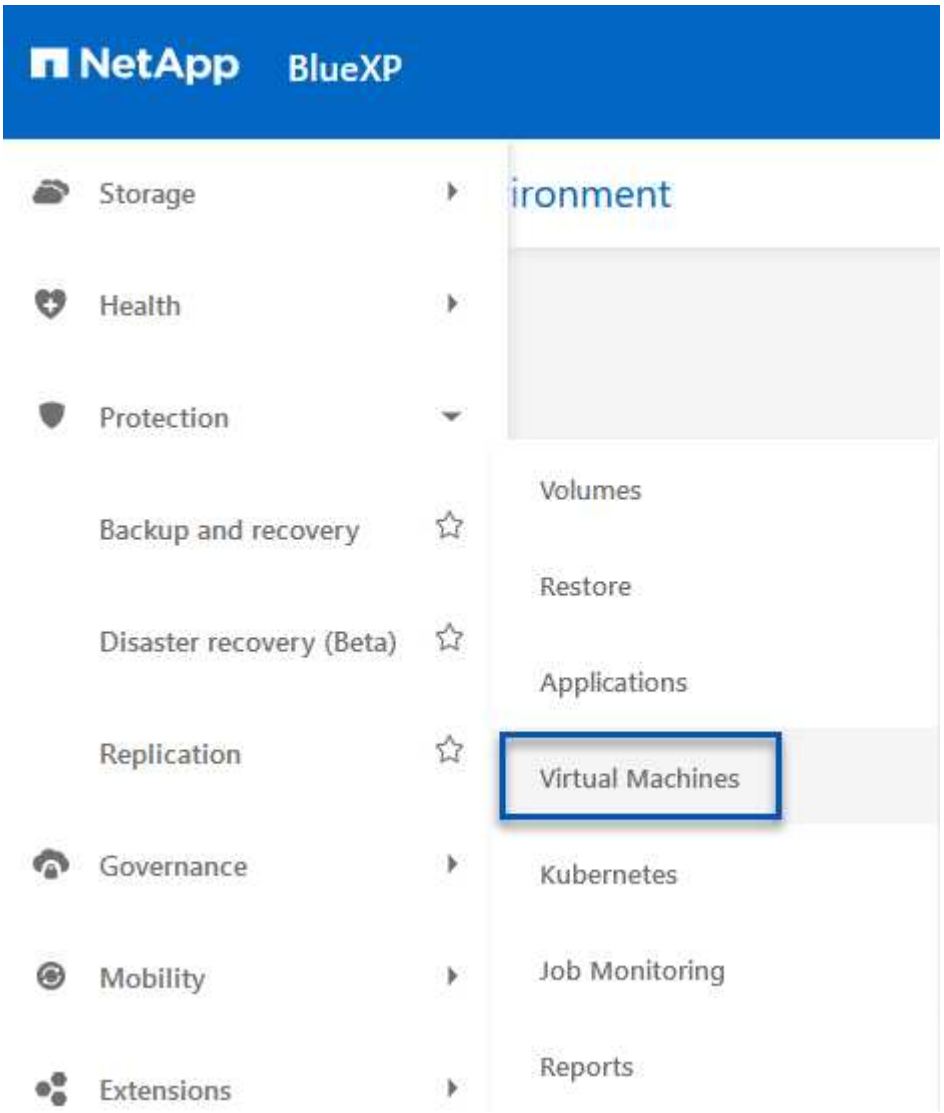
3. Remplissez les informations d'identification du système de stockage ONTAP et cliquez sur le bouton **Découvrir** pour ajouter l'environnement de travail.



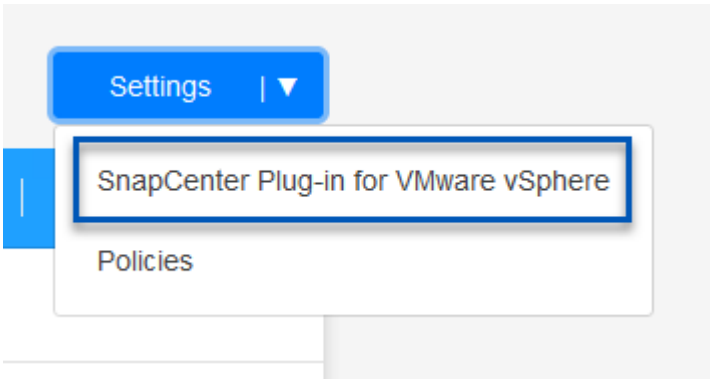
▼ **Découvrez l'appliance SCV sur site et vCenter**

Pour découvrir les ressources de la banque de données locale et de la machine virtuelle, ajoutez des informations pour le courtier de données SCV et les informations d'identification pour l'appliance de gestion vCenter.

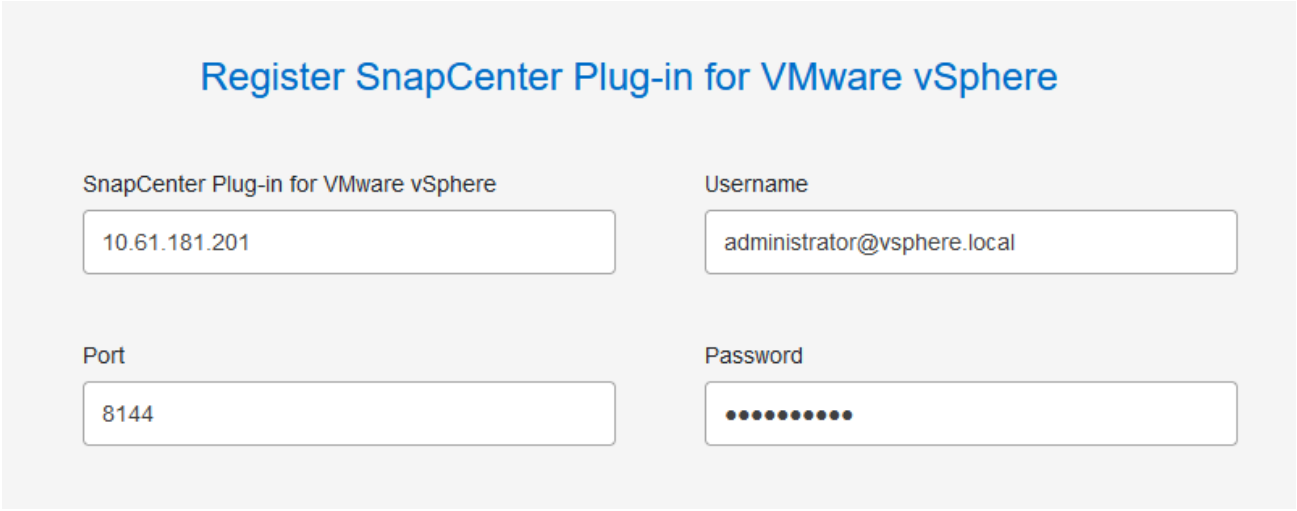
1. Dans le menu de gauche de NetApp Console, sélectionnez **Protection > Sauvegarde et restauration > Charges de travail > VMware**



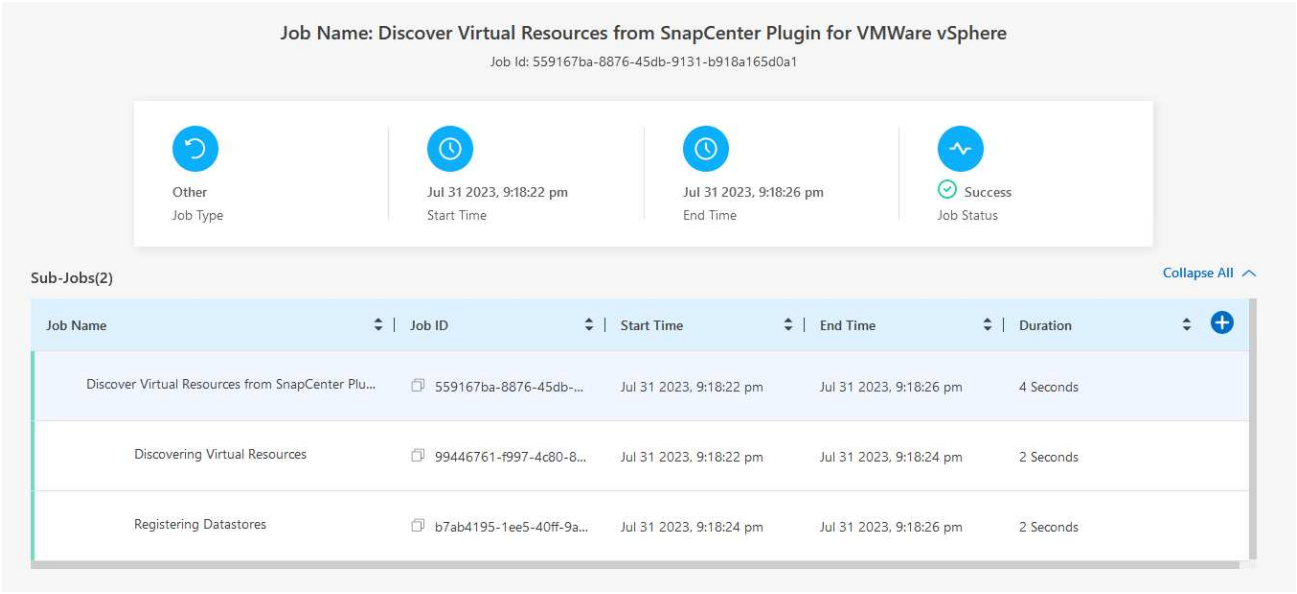
2. Depuis l'écran principal des machines virtuelles, accédez au menu déroulant **Paramètres** et sélectionnez * SnapCenter Plug-in for VMware vSphere*.



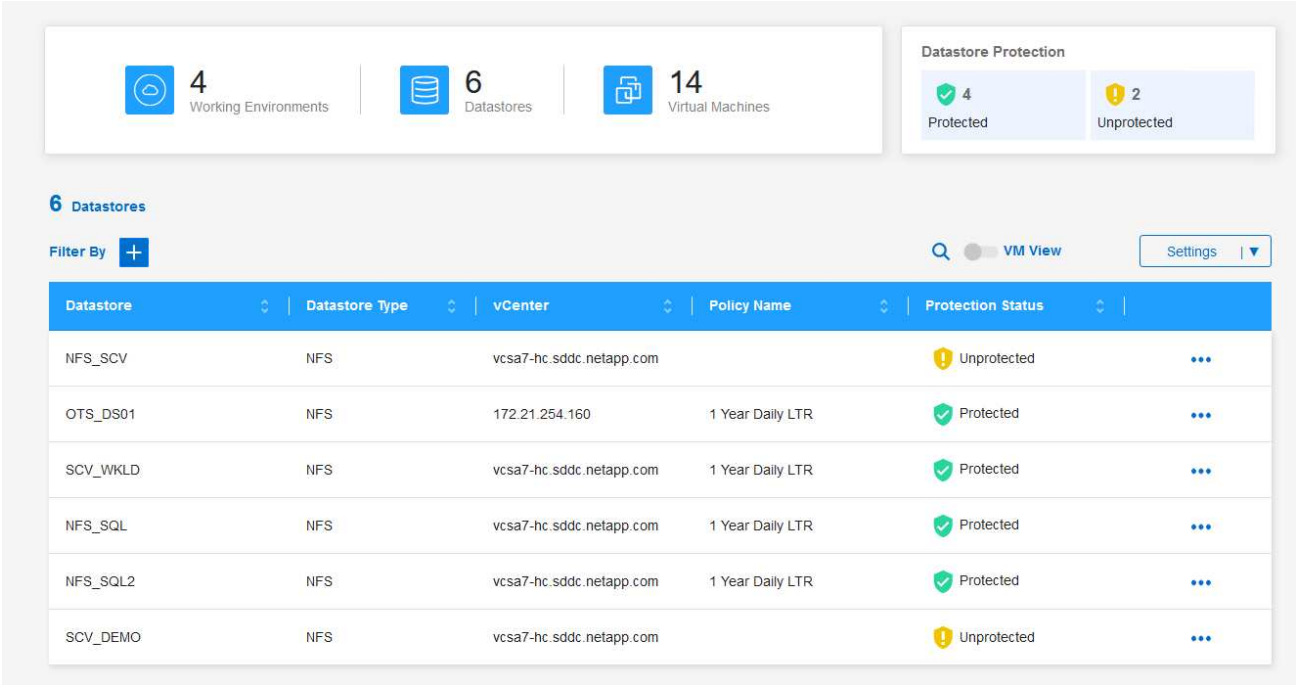
3. Cliquez sur le bouton **Enregistrer**, puis saisissez l'adresse IP et le numéro de port de l'appliance SnapCenter Plug-in, ainsi que le nom d'utilisateur et le mot de passe de l'appliance de gestion vCenter. Cliquez sur le bouton **S'inscrire** pour commencer le processus de découverte.



4. La progression des tâches peut être surveillée à partir de l'onglet Suivi des tâches.



5. Une fois la découverte terminée, vous pourrez afficher les banques de données et les machines virtuelles sur tous les appareils SCV découverts.

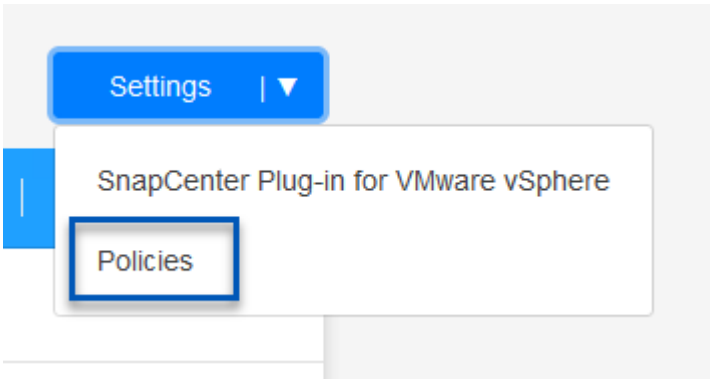


▼ Créer des politiques de sauvegarde

Dans NetApp Backup and Recovery for Virtual Machines, 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 groupes de protection, veuillez consulter "Créer un groupe de protection".

1. Depuis la page principale de NetApp Backup and Recovery for Virtual Machines, accédez au menu déroulant **Paramètres** et sélectionnez **Stratégies**.



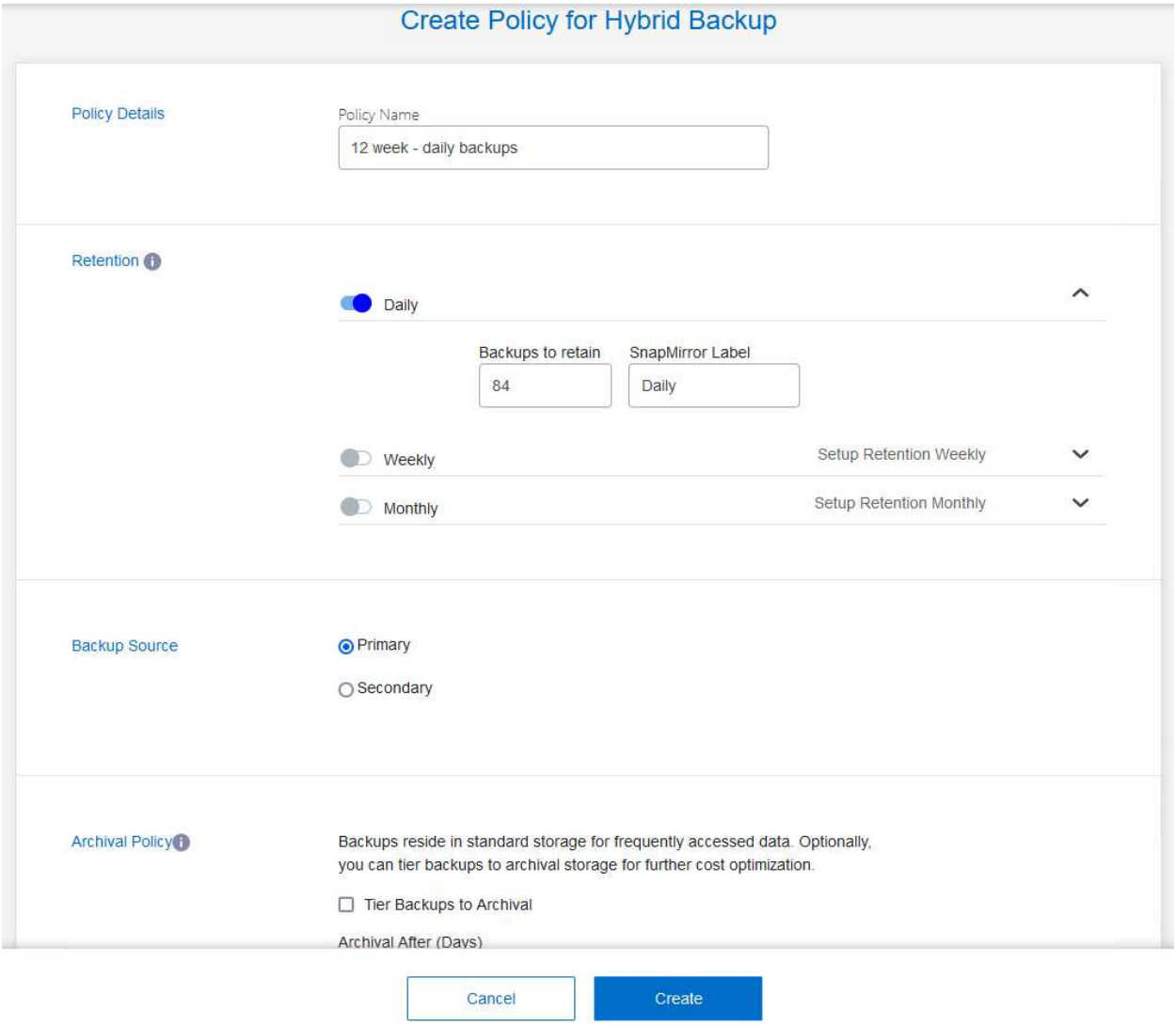
2. Cliquez sur **Créer une politique** pour accéder à la fenêtre **Créer une politique pour la sauvegarde hybride**.

   a. Ajouter un nom pour la politique

   b. Sélectionnez la durée de conservation souhaitée

   c. Sélectionnez si les sauvegardes proviendront du système de stockage ONTAP sur site principal ou secondaire

   d. Vous pouvez également spécifier après quelle période les sauvegardes seront transférées vers un stockage d'archivage pour des économies de coûts supplémentaires.



L'étiquette SnapMirror saisie ici est utilisée pour identifier les sauvegardes auxquelles appliquer la politique. Le nom de l'étiquette doit correspondre au nom de l'étiquette dans la stratégie SCV locale correspondante.

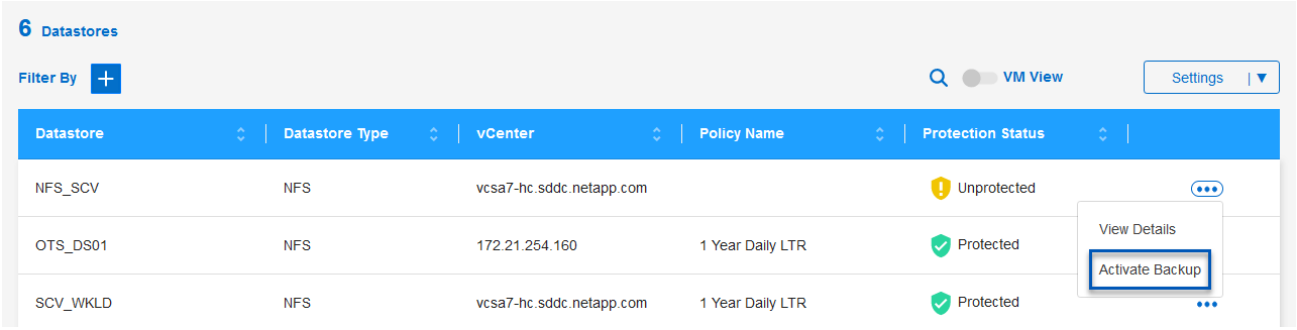
3. Cliquez sur **Créer** pour terminer la création de la politique.

▼ **Sauvegarder les banques de données sur Amazon Web Services**

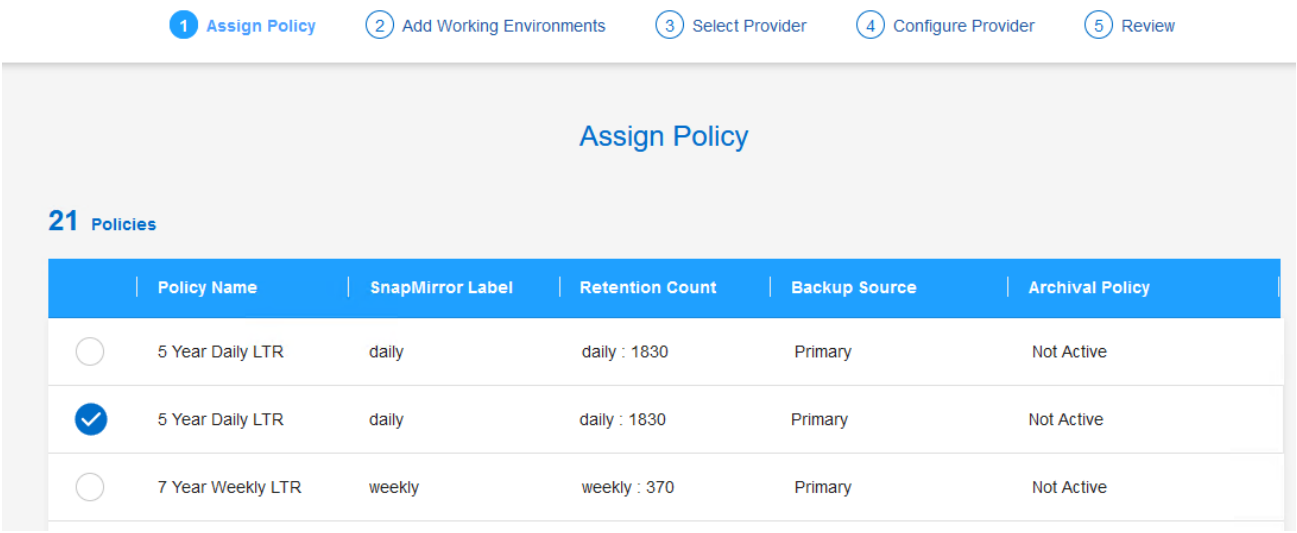
L'étape finale consiste à activer la protection des données pour les banques de données et les machines virtuelles individuelles. Les étapes suivantes décrivent comment activer les sauvegardes sur AWS.

Pour plus d'informations, consultez "Sauvegarder les charges de travail VMware".

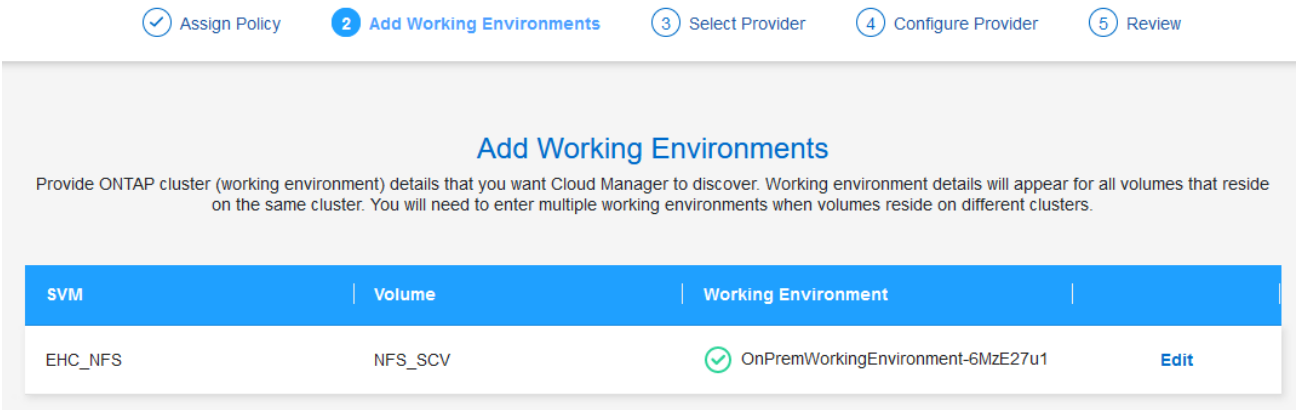
1. Depuis la page principale de NetApp Backup and Recovery for Virtual Machines, accédez au menu déroulant des paramètres de la banque de données à sauvegarder et sélectionnez **Activate Backup**.



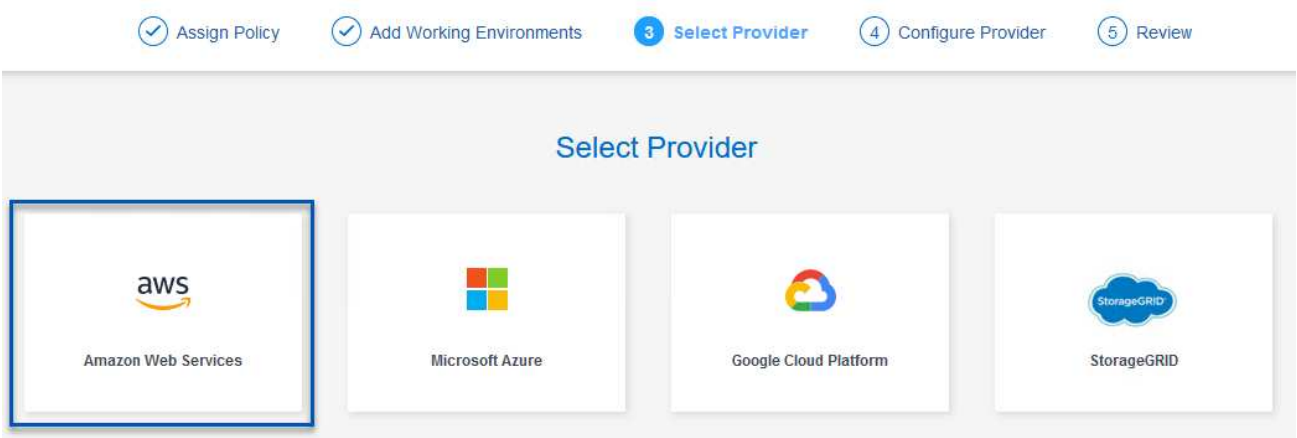
2. Attribuez la politique à utiliser pour l'opération de protection des données et cliquez sur **Suivant**.



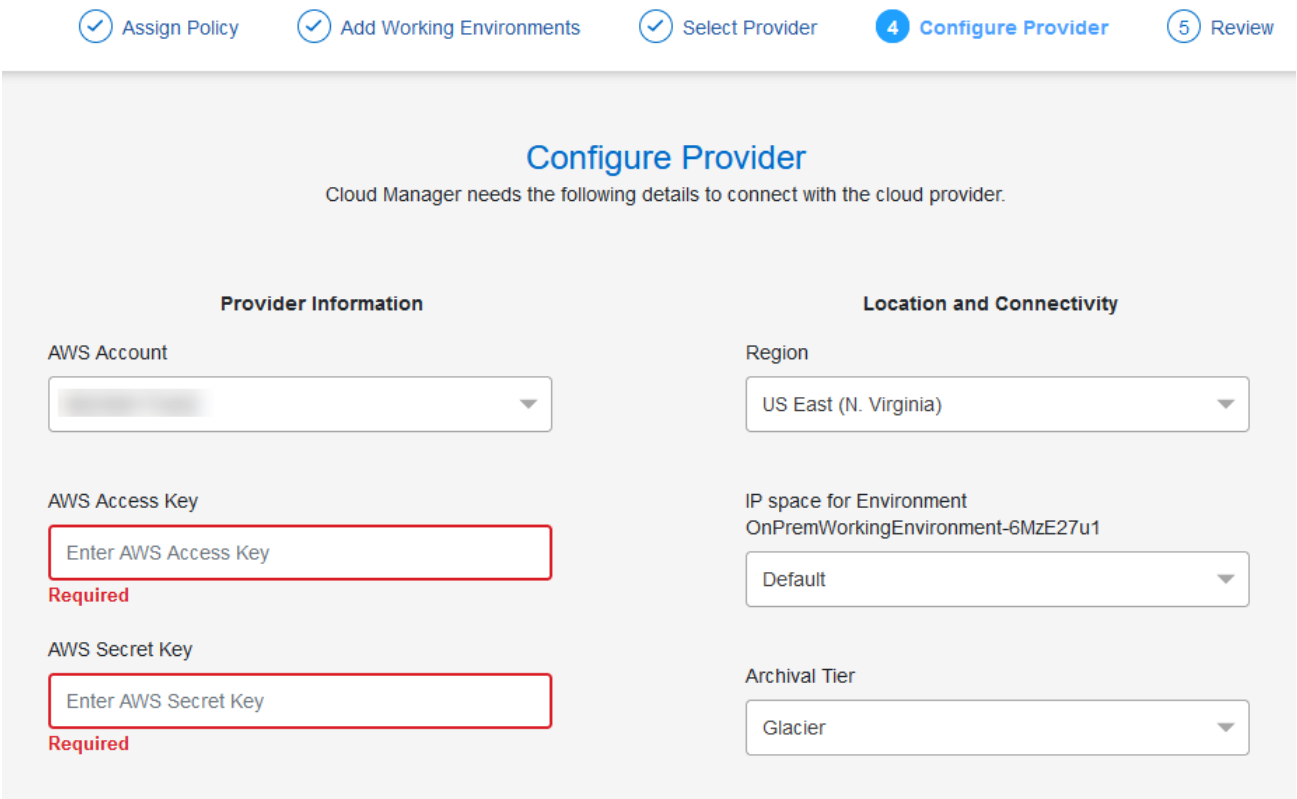
3. Sur la page **Ajouter des environnements de travail**, le magasin de données et l'environnement de travail avec une coche doivent apparaître si l'environnement de travail a déjà été découvert. Si l'environnement de travail n'a pas été découvert précédemment, vous pouvez l'ajouter ici. Cliquez sur **Suivant** pour continuer.



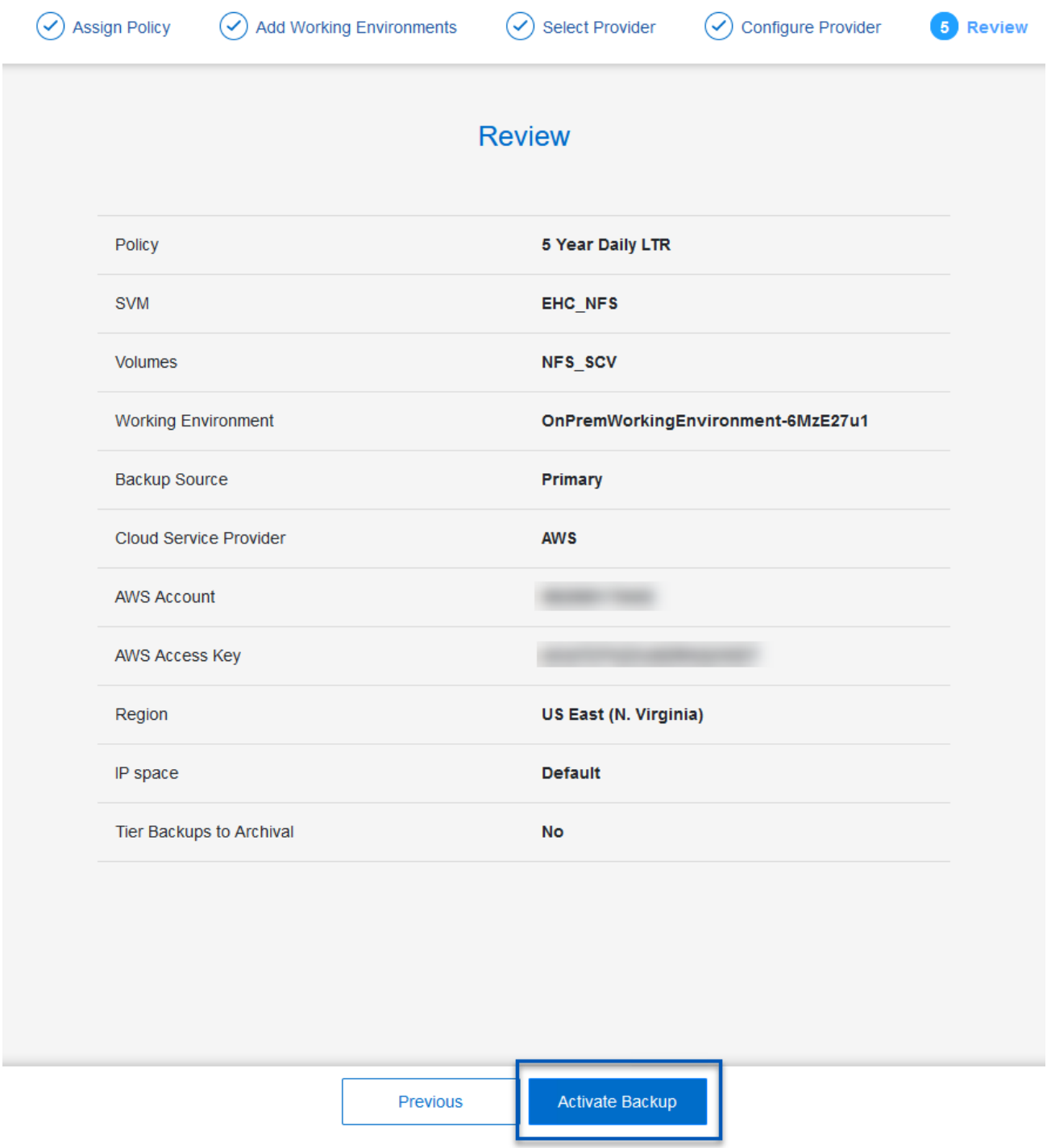
4. Sur la page **Sélectionner un fournisseur**, cliquez sur AWS, puis sur le bouton **Suivant** pour continuer.



5. Remplissez les informations d'identification spécifiques au fournisseur pour AWS, y compris la clé d'accès et la clé secrète AWS, la région et le niveau d'archivage à utiliser. Sélectionnez également l'espace IP ONTAP pour le système de stockage ONTAP sur site. Cliquez sur **Suivant**.



6. Enfin, vérifiez les détails de la tâche de sauvegarde et cliquez sur le bouton **Activer la sauvegarde** pour lancer la protection des données de la banque de données.



À ce stade, le transfert de données peut ne pas démarrer immédiatement. NetApp Backup and Recovery recherche toutes les heures les snapshots en attente, puis les transfère vers le stockage objet.

Restauration des machines virtuelles en cas de perte de données

Assurer la protection de vos données n'est qu'un aspect d'une protection complète des données. Tout aussi cruciale est la capacité de restaurer rapidement les données depuis n'importe quel emplacement en cas de perte de données ou d'attaque par ransomware. Cette capacité est essentielle pour maintenir des opérations commerciales fluides et atteindre les objectifs de point de récupération.

NetApp propose une stratégie 3-2-1 hautement adaptable, offrant un contrôle personnalisé sur les calendriers de conservation aux emplacements de stockage principal, secondaire et objet. Cette stratégie offre la flexibilité nécessaire pour adapter les approches de protection des données à des besoins spécifiques.

Cette section présente un aperçu du processus de restauration des données à partir de SnapCenter Plug-in for VMware vSphere et de NetApp Backup and Recovery pour les machines virtuelles.

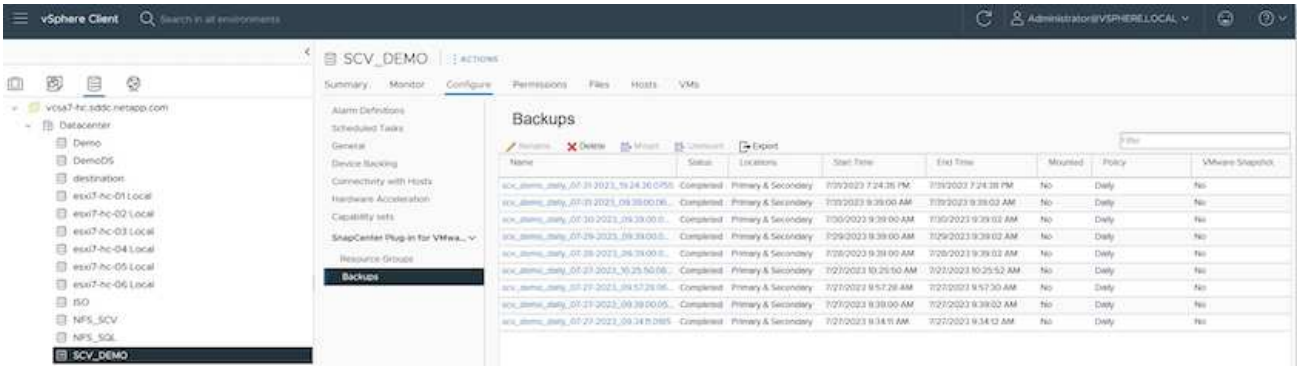
Restauration de machines virtuelles à partir du SnapCenter Plug-in for VMware vSphere

Pour cette solution, les machines virtuelles ont été restaurées à leurs emplacements d'origine et alternatifs. Tous les aspects des capacités de restauration des données de SCV ne seront pas couverts dans cette solution. Pour des informations détaillées sur tout ce que SCV a à offrir, reportez-vous au "Restaurer les machines virtuelles à partir de sauvegardes" dans la documentation du produit.

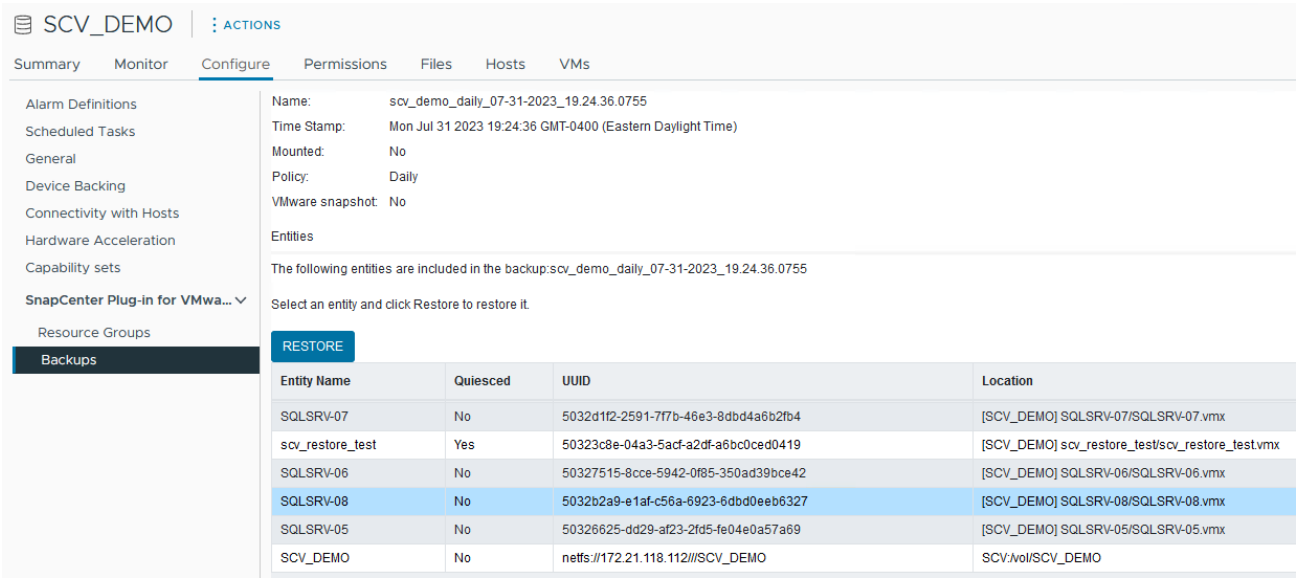
▼ **Restaurer les machines virtuelles à partir de SCV**

Suivez les étapes suivantes pour restaurer une machine virtuelle à partir d'un stockage principal ou secondaire.

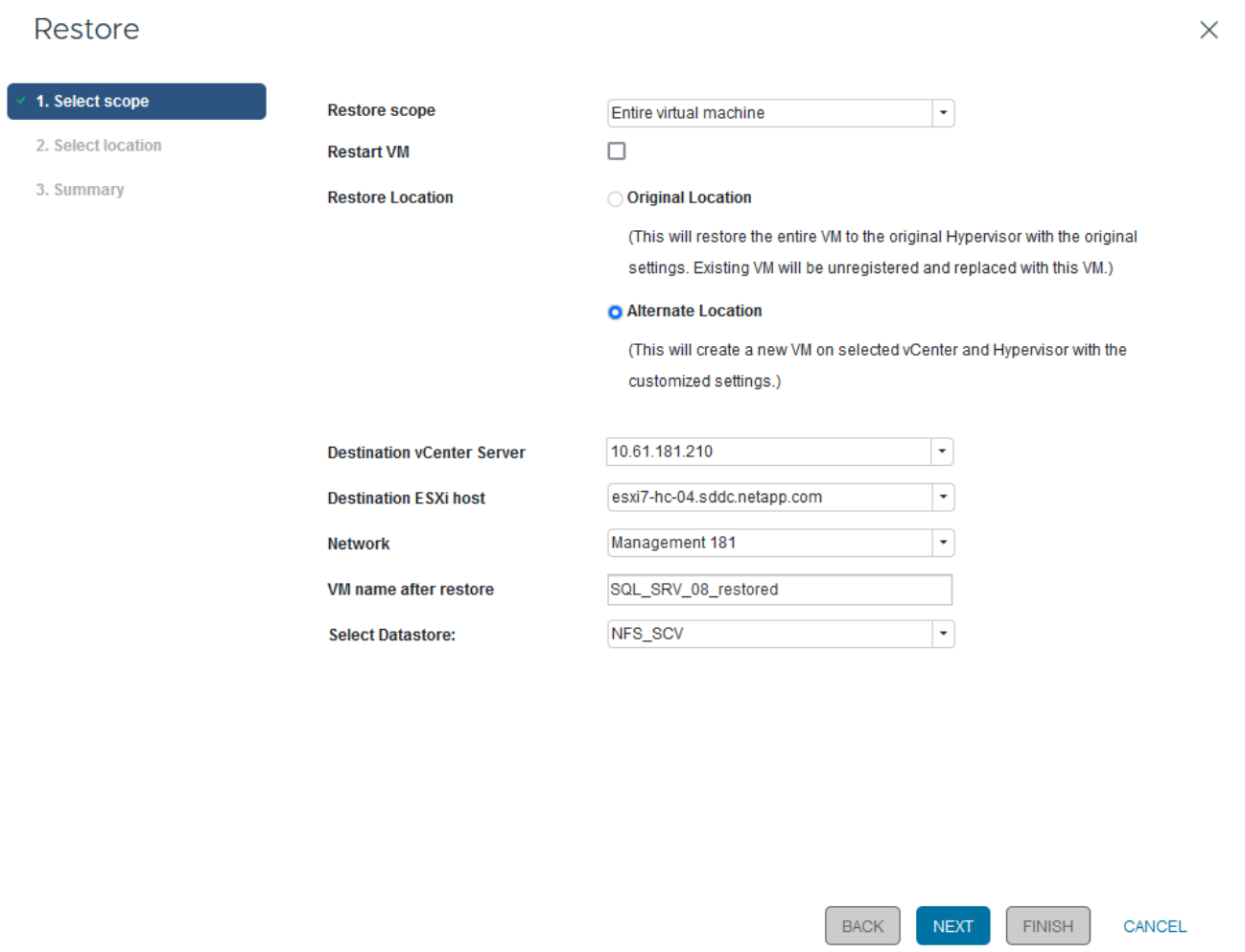
1. Depuis le client vCenter, accédez à **Inventaire > Stockage** et cliquez sur la banque de données contenant les machines virtuelles que vous souhaitez restaurer.
2. Depuis l'onglet **Configurer**, cliquez sur **Sauvegardes** pour accéder à la liste des sauvegardes disponibles.



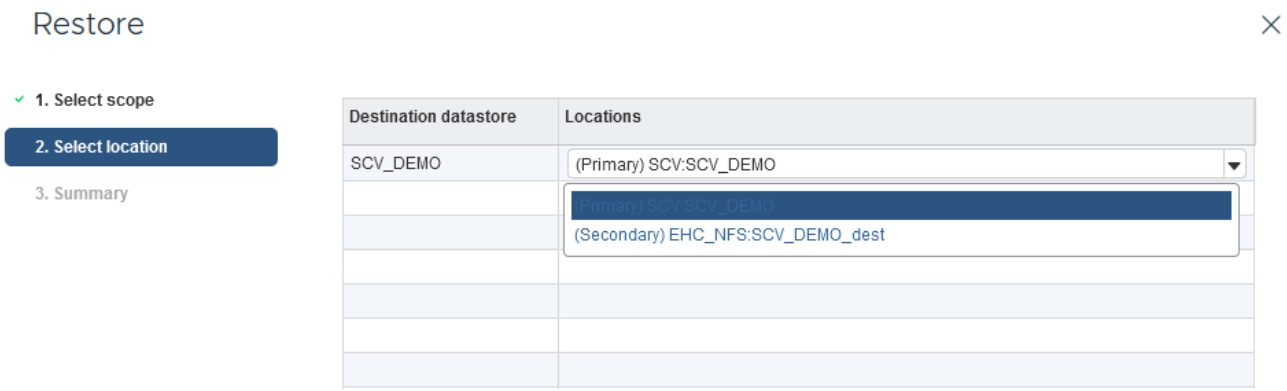
3. Cliquez sur une sauvegarde pour accéder à la liste des VM, puis sélectionnez une VM à restaurer. Cliquez sur **Restaurer**.



4. À partir de l'assistant de restauration, sélectionnez la restauration de la machine virtuelle entière ou d'un VMDK spécifique. Sélectionnez l'installation à l'emplacement d'origine ou à un autre emplacement, indiquez le nom de la machine virtuelle après la restauration et la banque de données de destination. Cliquez sur **Suivant**.



5. Choisissez de sauvegarder à partir de l'emplacement de stockage principal ou secondaire.



6. Enfin, examinez un résumé de la tâche de sauvegarde et cliquez sur Terminer pour commencer le processus de restauration.

Restauration de machines virtuelles à partir de NetApp Backup and Recovery for Virtual Machines

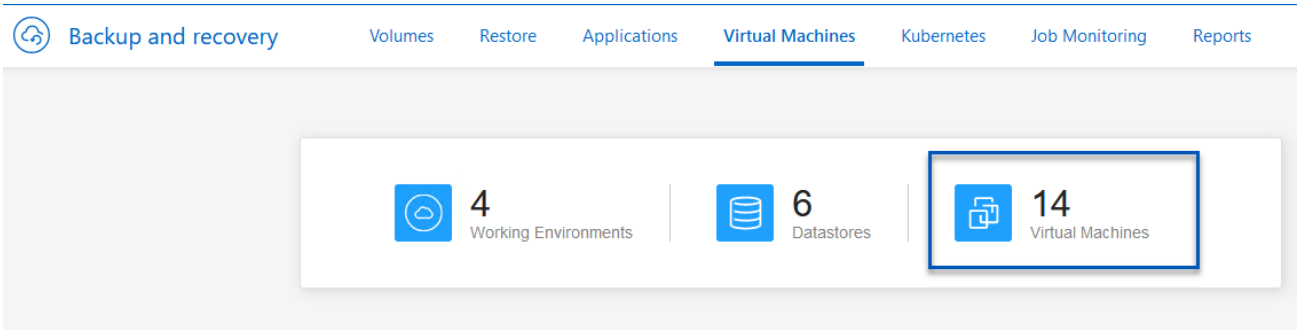
NetApp Backup and Recovery for Virtual Machines permet de restaurer des machines virtuelles à leur emplacement d'origine. Les fonctions de restauration sont accessibles via la console web NetApp Backup and Recovery.

Pour plus d'informations veuillez consulter "Restaurer les données des machines virtuelles depuis le cloud".

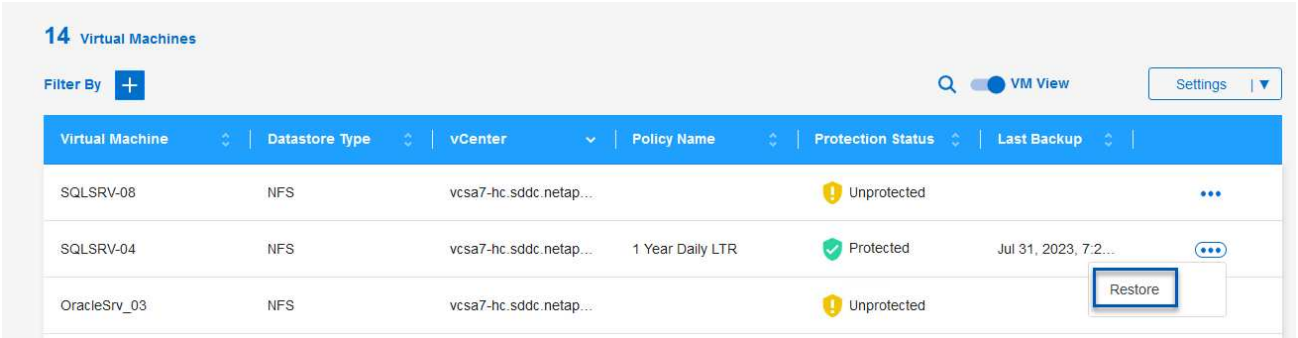
▼ **Restaurer des machines virtuelles depuis NetApp Backup and Recovery**

Pour restaurer une machine virtuelle à partir de NetApp Backup and Recovery, suivez les étapes suivantes.

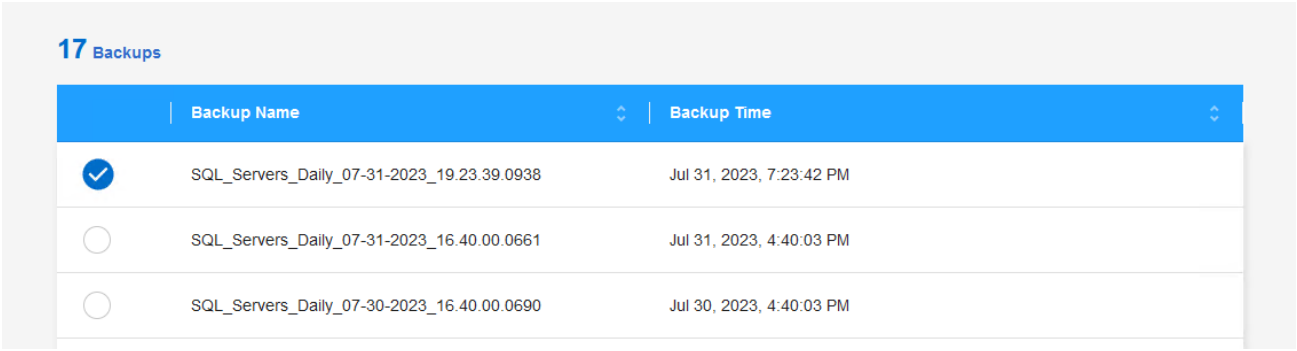
1. Accédez à **Protection > Sauvegarde et récupération > Machines virtuelles** et cliquez sur Machines virtuelles pour afficher la liste des machines virtuelles disponibles pour être restaurées.



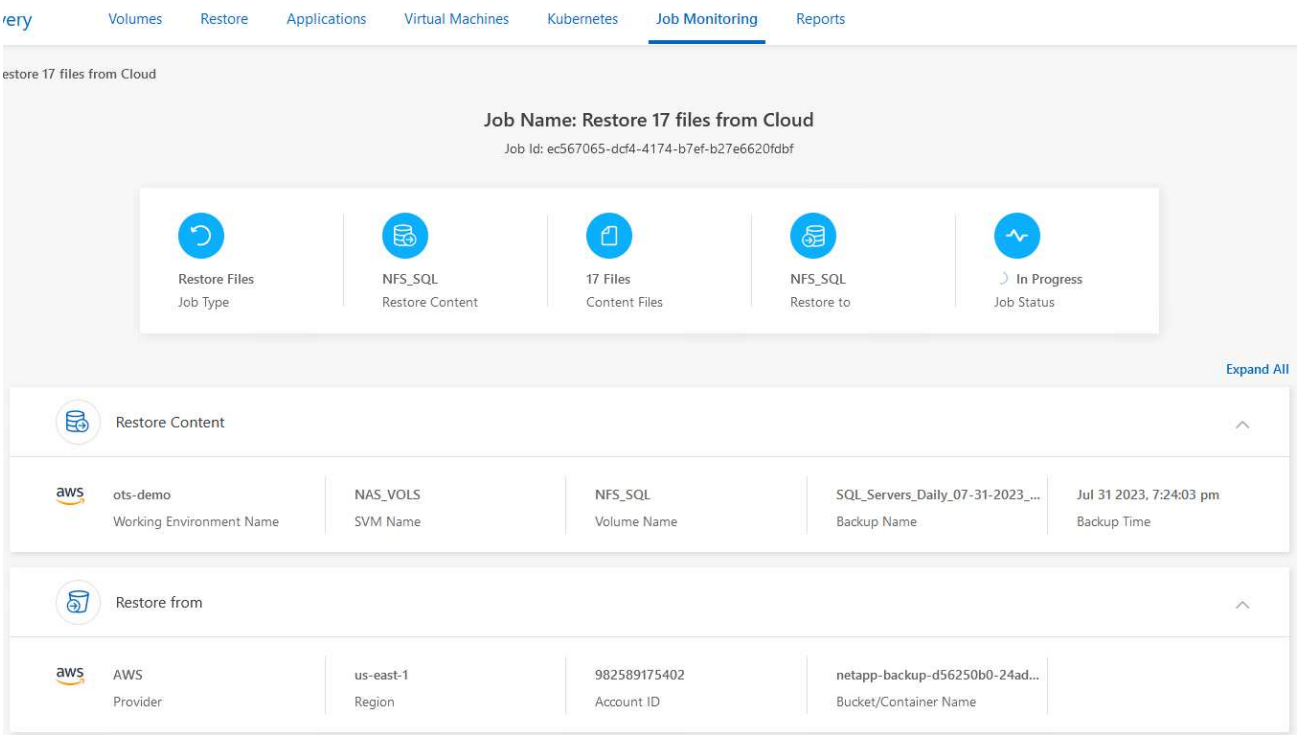
2. Accédez au menu déroulant des paramètres de la VM à restaurer et sélectionnez



3. Sélectionnez la sauvegarde à partir de laquelle restaurer et cliquez sur **Suivant**.



4. Consultez un résumé de la tâche de sauvegarde et cliquez sur **Restaurer** pour démarrer le processus de restauration.
5. Surveillez la progression de la tâche de restauration à partir de l'onglet **Surveillance des tâches**.



Conclusion

La stratégie de sauvegarde 3-2-1, lorsqu'elle est mise en œuvre avec SnapCenter Plug-in for VMware vSphere et NetApp Backup and Recovery pour les machines virtuelles, offre une solution robuste, fiable et économique pour la protection des données. Cette stratégie garantit non seulement la redondance et l'accessibilité des données, mais offre également la flexibilité de restaurer les données depuis n'importe quel emplacement, à partir des systèmes de stockage ONTAP sur site et du stockage objet basé sur le cloud.

L'utilisation présentée dans cette documentation se concentre sur des technologies éprouvées de protection des données qui mettent en évidence l'intégration entre NetApp, VMware et les principaux fournisseurs de cloud. Le SnapCenter Plug-in for VMware vSphere offre une intégration transparente avec VMware vSphere, permettant une gestion efficace et centralisée des opérations de protection des données. Cette intégration rationalise les processus de sauvegarde et de restauration des machines virtuelles, en permettant une planification, une surveillance et des opérations de restauration flexibles au sein de l'écosystème VMware.

NetApp Backup and Recovery for virtual machines fournit le un (1) du 3-2-1 en assurant des sauvegardes sécurisées et isolées des données des machines virtuelles vers un stockage objet basé sur le cloud. L'interface intuitive et le flux de travail logique fournissent une plateforme sécurisée pour l'archivage à long terme des données stratégiques.

Informations supplémentaires

Pour en savoir plus sur les technologies présentées dans cette solution, reportez-vous aux informations complémentaires suivantes.

- "Documentation du SnapCenter Plug-in for VMware vSphere"
- "Documentation NetApp Console"

NetApp Disaster Recovery

Aperçu

La reprise après sinistre est une priorité absolue pour tout administrateur VMware. Comme VMware encapsule des serveurs entiers dans une série de fichiers qui constituent la machine virtuelle, les administrateurs exploitent des techniques de stockage bloc telles que les clones, les snapshots et les réplicas pour protéger ces machines virtuelles. Les baies ONTAP offrent une réplication intégrée permettant de transférer les données de volume, et donc les machines virtuelles résidant sur les LUN du datastore désigné, d'un site à un autre. NetApp Disaster Recovery s'intègre à vSphere et automatise l'ensemble du workflow pour un basculement et un retour arrière transparents en cas de sinistre. En combinant la réplication du stockage à une automatisation intelligente, les administrateurs disposent désormais d'une méthode gérable non seulement pour configurer, automatiser et tester les plans de reprise après sinistre, mais aussi des moyens de les exécuter facilement en cas de sinistre.

Les étapes les plus chronophages d'un basculement DR dans un environnement VMware vSphere sont l'exécution des étapes nécessaires à l'inventaire, à l'enregistrement, à la reconfiguration et à la mise sous tension des machines virtuelles sur le site DR. Une solution idéale présente à la fois un faible RPO (mesuré en minutes) et un faible RTO (mesuré en minutes à heures). Un facteur souvent négligé dans une solution DR est la capacité à tester efficacement la solution DR à intervalle périodique.

Pour concevoir une solution de reprise après sinistre, gardez à l'esprit les facteurs suivants :

- L'objectif de temps de récupération (RTO). Le RTO correspond à la rapidité avec laquelle une entreprise peut se remettre d'une catastrophe ou, plus précisément, au temps nécessaire pour exécuter le processus de récupération afin de rendre les services commerciaux à nouveau disponibles.
- L'objectif de point de récupération (RPO). Le RPO correspond à l'âge des données récupérées après leur mise à disposition, par rapport au moment où la catastrophe s'est produite.
- Évolutivité et adaptabilité. Ce facteur inclut la capacité à augmenter progressivement les ressources de stockage à mesure que la demande augmente.

Pour plus d'informations techniques sur les solutions disponibles, veuillez consulter :

- "NetApp Disaster Recovery pour les datastores NFS"

- "NetApp Disaster Recovery pour les datastores VMFS"

NetApp Disaster Recovery pour les datastores NFS

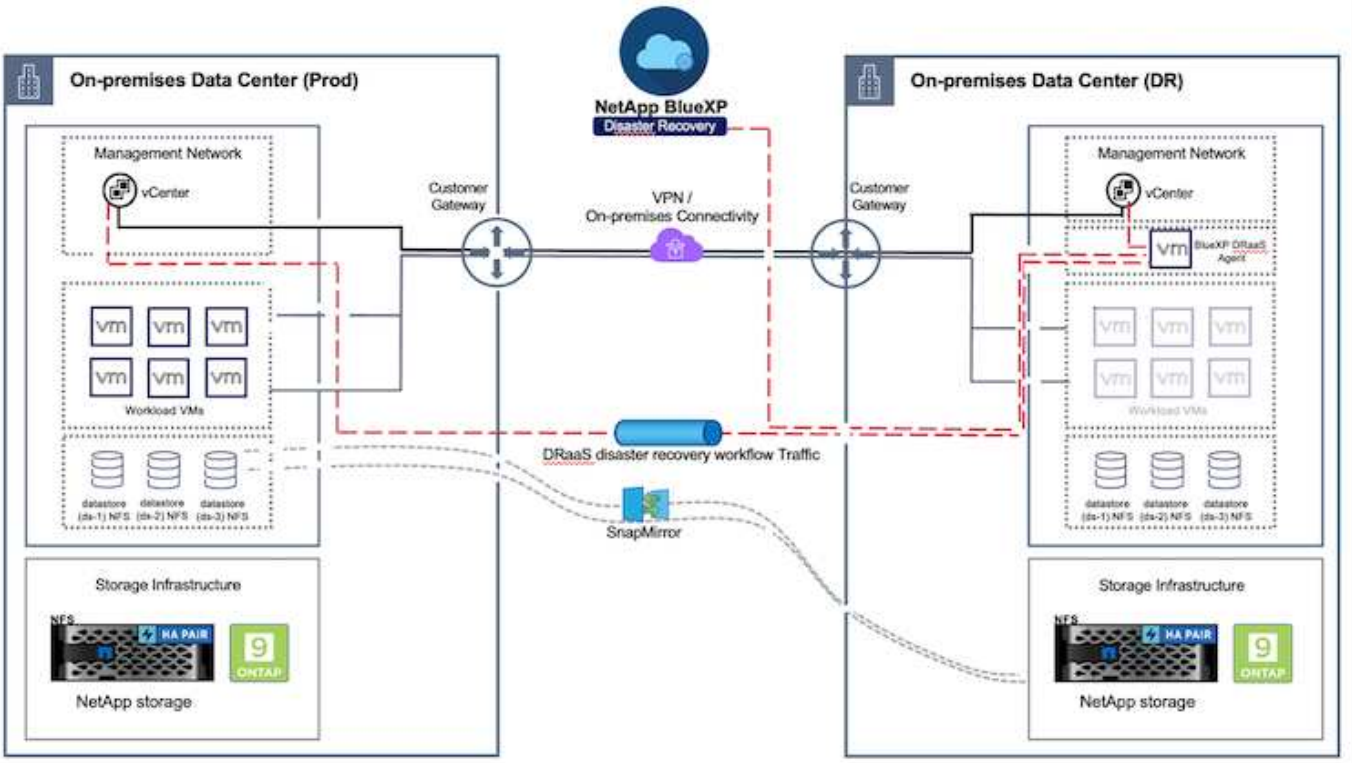
NetApp Disaster Recovery pour les datastores NFS

La mise en œuvre de la reprise après sinistre via la réplication au niveau des blocs du site de production vers le site de reprise après sinistre est une méthode résiliente et rentable pour protéger les charges de travail contre les pannes de site et les événements de corruption de données, tels que les attaques de ransomware. À l'aide de la réplication NetApp SnapMirror , les charges de travail VMware exécutées sur des systèmes ONTAP locaux avec une banque de données NFS peuvent être répliquées vers un autre système de stockage ONTAP situé dans un centre de données de récupération désigné où VMware est également déployé.

Cette section du document décrit la configuration de NetApp Disaster Recovery pour configurer la reprise après sinistre des VM VMware sur site vers un autre site désigné. Cette configuration comprend l'agent Console, l'intégration des baies ONTAP, la définition des sites et l'association de VMware vCenter. En outre, ce document détaille la configuration de la réplication entre les sites, ainsi que la mise en place et le test d'un plan de reprise. La dernière section fournit des instructions pour effectuer un basculement complet du site et pour revenir en arrière lorsque le site principal est rétabli et remis en ligne.

En utilisant Disaster Recovery, qui fait partie de NetApp Data Services, les entreprises peuvent facilement découvrir leurs vCenters VMware sur site et leur stockage ONTAP. Les organisations peuvent ensuite créer des groupes de ressources, créer un plan de reprise après sinistre, l'associer à des groupes de ressources et tester ou exécuter le basculement et le rétablissement. SnapMirror fournit une réplication de blocs au niveau du stockage pour maintenir les deux sites à jour avec les modifications incrémentielles, ce qui permet d'obtenir un objectif de point de récupération (RPO) pouvant aller jusqu'à 5 minutes. De plus, il est possible de simuler des procédures de reprise après sinistre sans affecter la production ni entraîner de coûts de stockage supplémentaires.

Disaster Recovery exploite la technologie ONTAP FlexClone pour créer une copie à faible encombrement du datastore NFS à partir du dernier Snapshot répliqué sur le site de reprise après sinistre. Une fois le test de reprise après sinistre terminé, les clients peuvent facilement supprimer l'environnement de test sans affecter les ressources de production répliquées. En cas de basculement réel, Disaster Recovery orchestre toutes les étapes nécessaires pour mettre automatiquement en ligne les machines virtuelles protégées sur le site de reprise après sinistre désigné en quelques clics. Le service inverse également la relation SnapMirror vers le site principal et réplique toutes les modifications du site secondaire vers le site principal pour une opération de rétablissement, si nécessaire. Toutes ces fonctionnalités sont proposées à une fraction du coût des autres solutions bien connues.

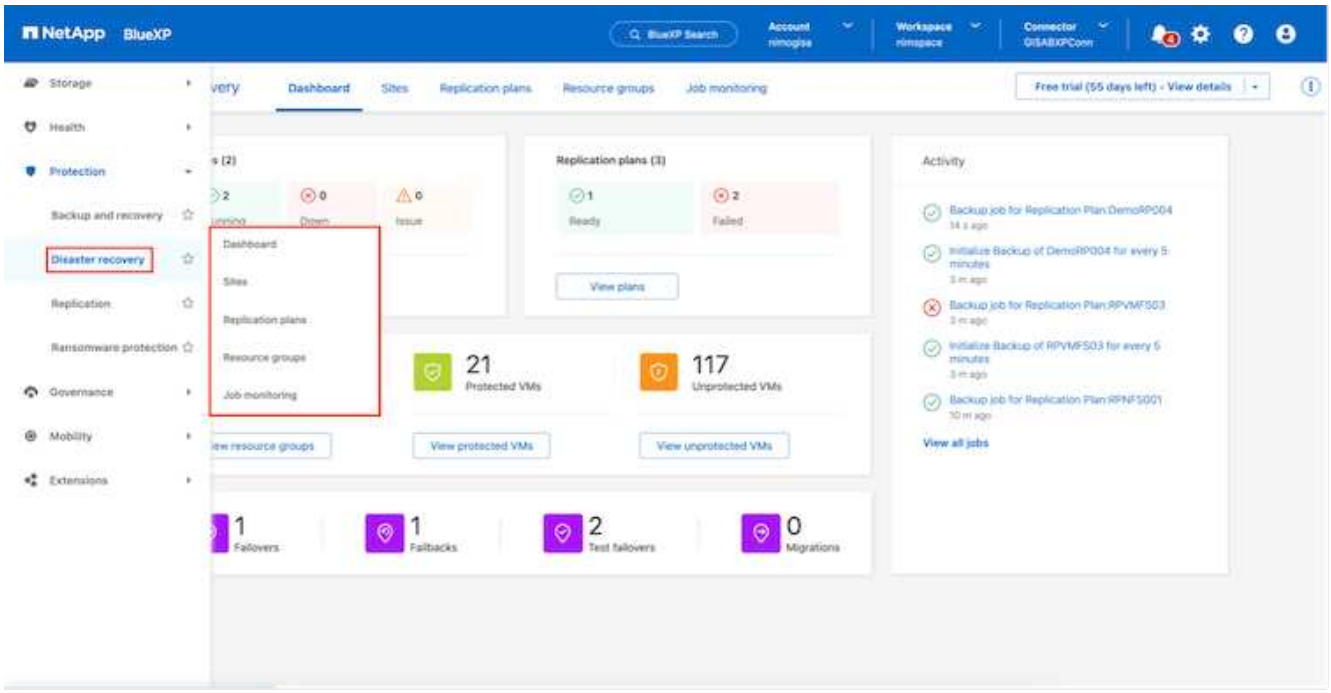


Pour obtenir des informations à jour et les versions prises en charge de vCenter Server, ESXi et ONTAP pour la reprise après sinistre, veuillez vous référer à "Configurations prises en charge pour la reprise après sinistre".

Commencer

Pour commencer avec NetApp Disaster Recovery, utilisez NetApp console, puis accédez au service.

1. Connectez-vous à Console.
2. Dans la navigation de gauche de Console, sélectionnez Protection > Reprise après sinistre.
3. Le Disaster Recovery Dashboard s’affiche.

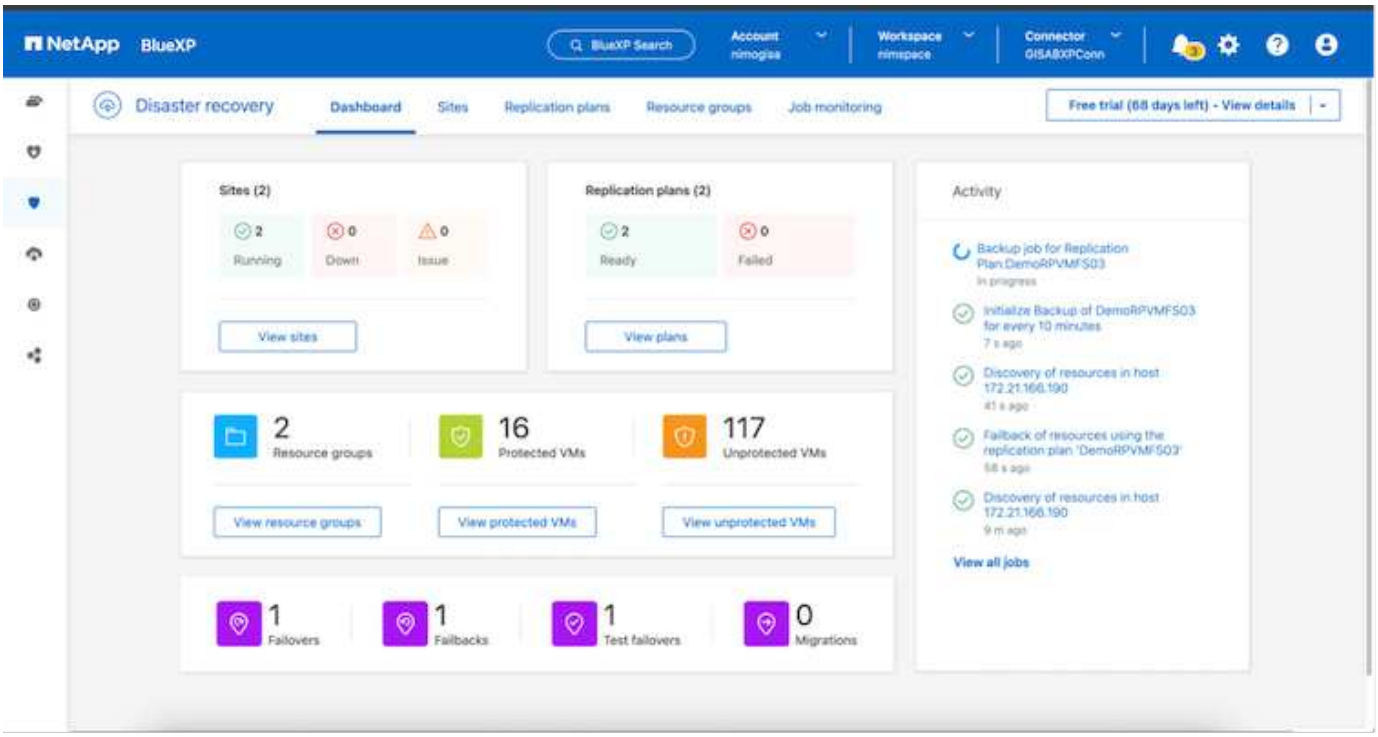


Avant de configurer le plan de reprise après sinistre, assurez-vous que les conditions préalables suivantes sont remplies :

- L'agent Console est déployé.
- L'agent dispose d'une connectivité aux systèmes de stockage ainsi qu'aux vCenter source et de destination.
- Un cluster ONTAP avec une SVM sur laquelle le service NFS est activé est disponible.
- Les systèmes de stockage NetApp sur site hébergeant des banques de données NFS pour VMware sont ajoutés dans Console.
- La résolution DNS doit être en place lors de l'utilisation de noms DNS. Sinon, utilisez les adresses IP pour le vCenter.
- La réplication SnapMirror est configurée pour les volumes de banque de données NFS désignés.
- Assurez-vous que l'environnement dispose de versions prises en charge des serveurs vCenter Server et ESXi.

Une fois la connectivité établie entre les sites source et de destination, procédez aux étapes de configuration, qui devraient prendre quelques clics et environ 3 à 5 minutes.

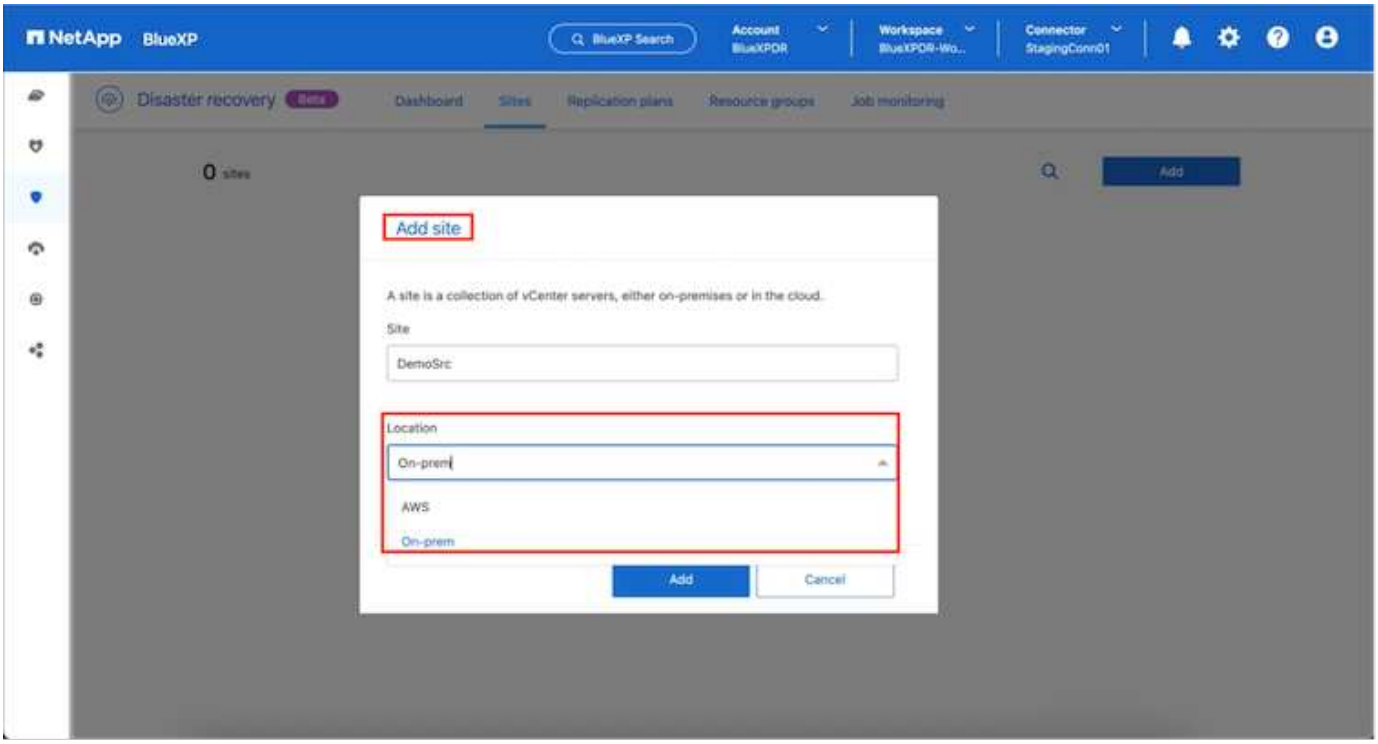
NetApp recommande de déployer le Console agent sur le site de destination ou sur un site tiers, afin que le Console agent puisse communiquer via le réseau avec les ressources source et de destination.



Configuration de NetApp Disaster Recovery

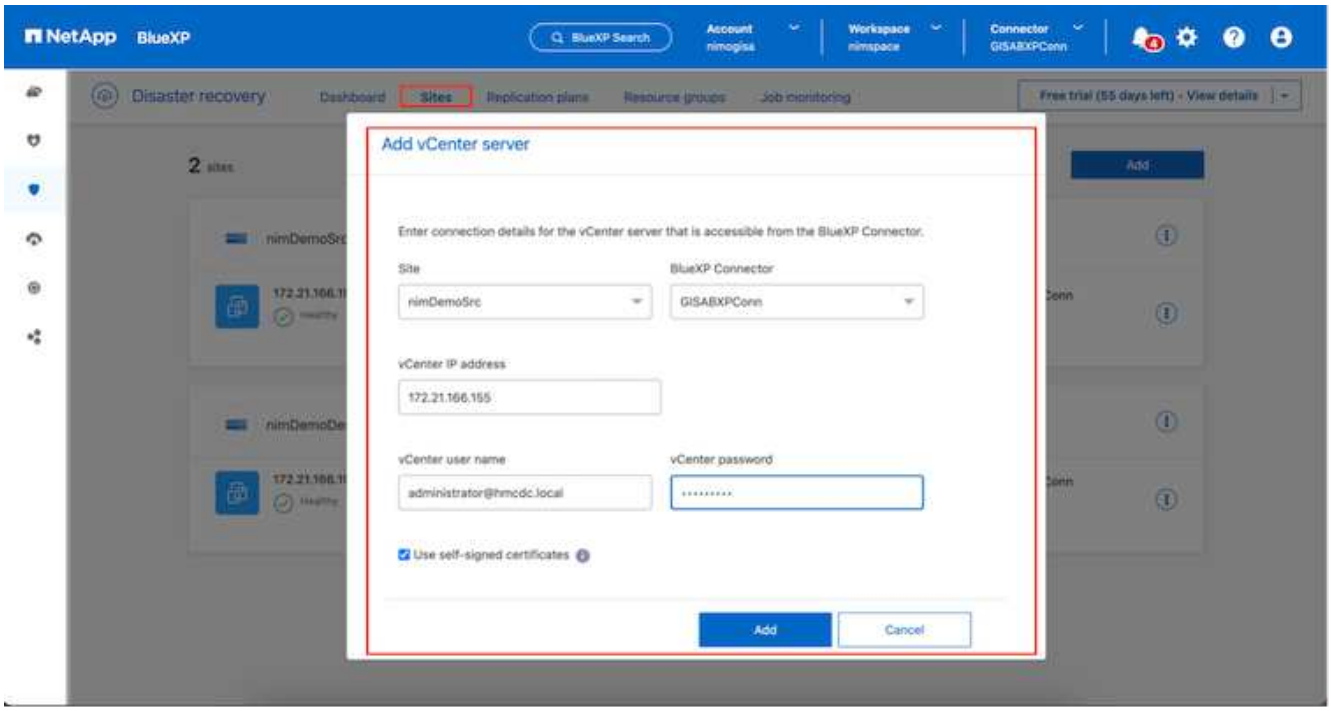
La première étape de la préparation à la reprise après sinistre consiste à détecter et à ajouter les ressources de stockage et vCenter sur site à NetApp Disaster Recovery.

Ouvrez Console et sélectionnez **Protection > Reprise après sinistre** dans le volet de navigation de gauche. Cliquez sur **Sites**, indiquez un nom et choisissez le type d'emplacement. Cliquez ensuite sur le bouton **Ajouter vCenter**.

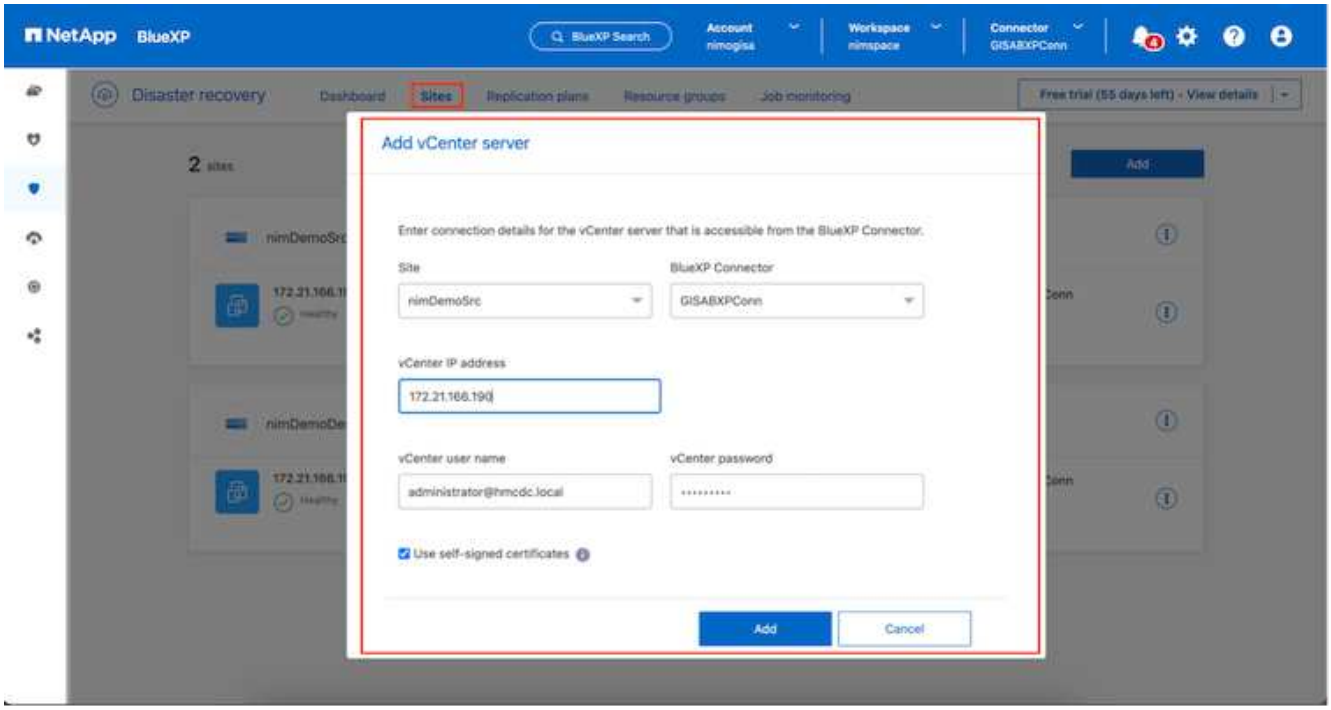


Ajoutez les plateformes suivantes :

- **Source**. vCenter sur site.



- **Destination**. VMC SDDC vCenter.



Une fois les vCenters ajoutés, la découverte automatisée est déclenchée.

Configuration de la réplication de stockage entre la matrice de sites source et la matrice de sites de destination

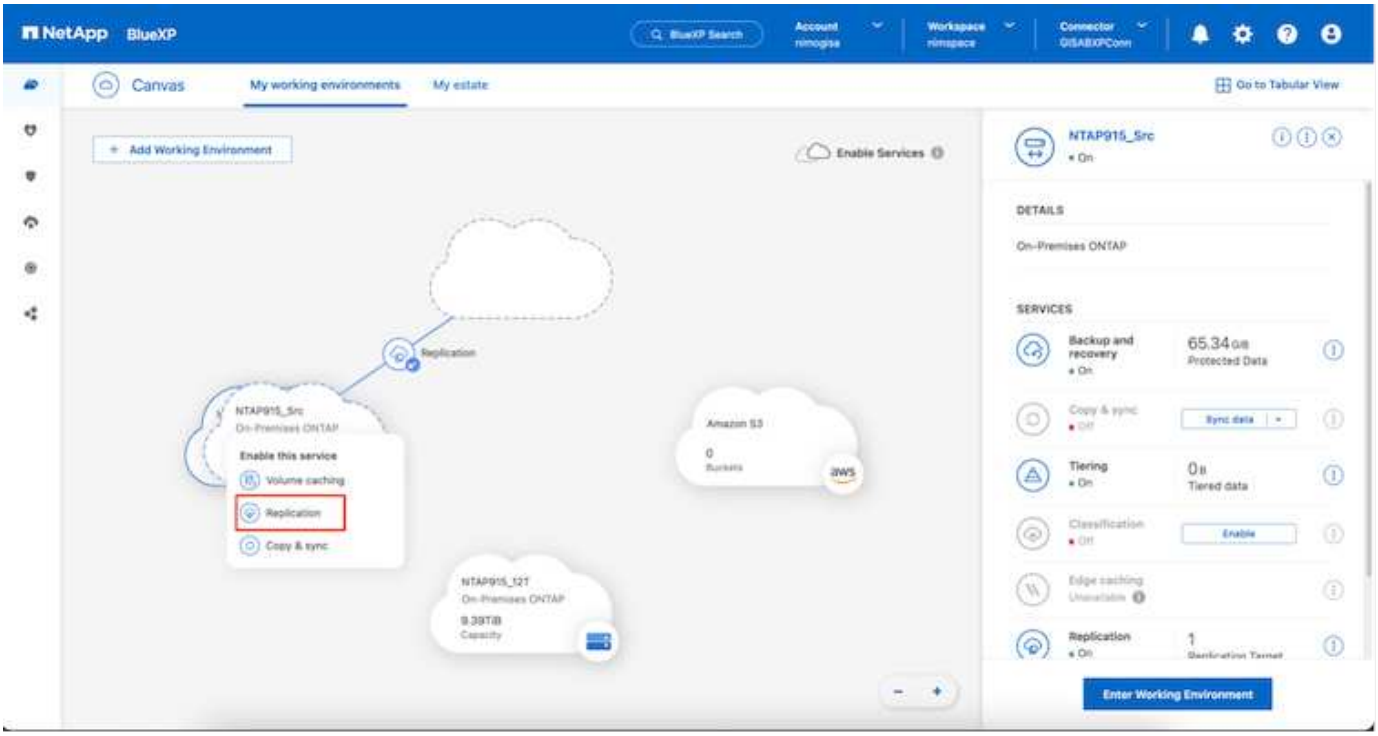
SnapMirror assure la réplication des données dans un environnement NetApp. Basée sur la technologie Snapshot de NetApp, la réplication SnapMirror est extrêmement efficace, car elle ne réplique que les blocs qui ont été modifiés ou ajoutés depuis la mise à jour précédente. SnapMirror se configure facilement à l'aide de NetApp OnCommand System Manager ou de l'interface de ligne de commande ONTAP. NetApp Data Services crée également la relation SnapMirror, à condition que le peering du cluster et du SVM soit configuré au préalable.

Dans les cas où le stockage principal n'est pas complètement perdu, SnapMirror offre un moyen efficace de resynchroniser les sites principal et de reprise après sinistre. SnapMirror peut resynchroniser les deux sites en retransférant uniquement les données modifiées ou nouvelles du site de reprise après sinistre vers le site principal, simplement en inversant les relations SnapMirror. Cela signifie que les plans de réplication dans Disaster Recovery peuvent être resynchronisés dans les deux sens après un basculement, sans recopier l'intégralité du volume. Si une relation est resynchronisée dans le sens inverse, seules les nouvelles données écrites depuis la dernière synchronisation réussie de la copie Snapshot sont renvoyées vers la destination.

Si une relation SnapMirror est déjà configurée pour le volume via l'interface de ligne de commande ou System Manager, NetApp Data Services reprend cette relation et poursuit le reste des opérations du flux de travail.

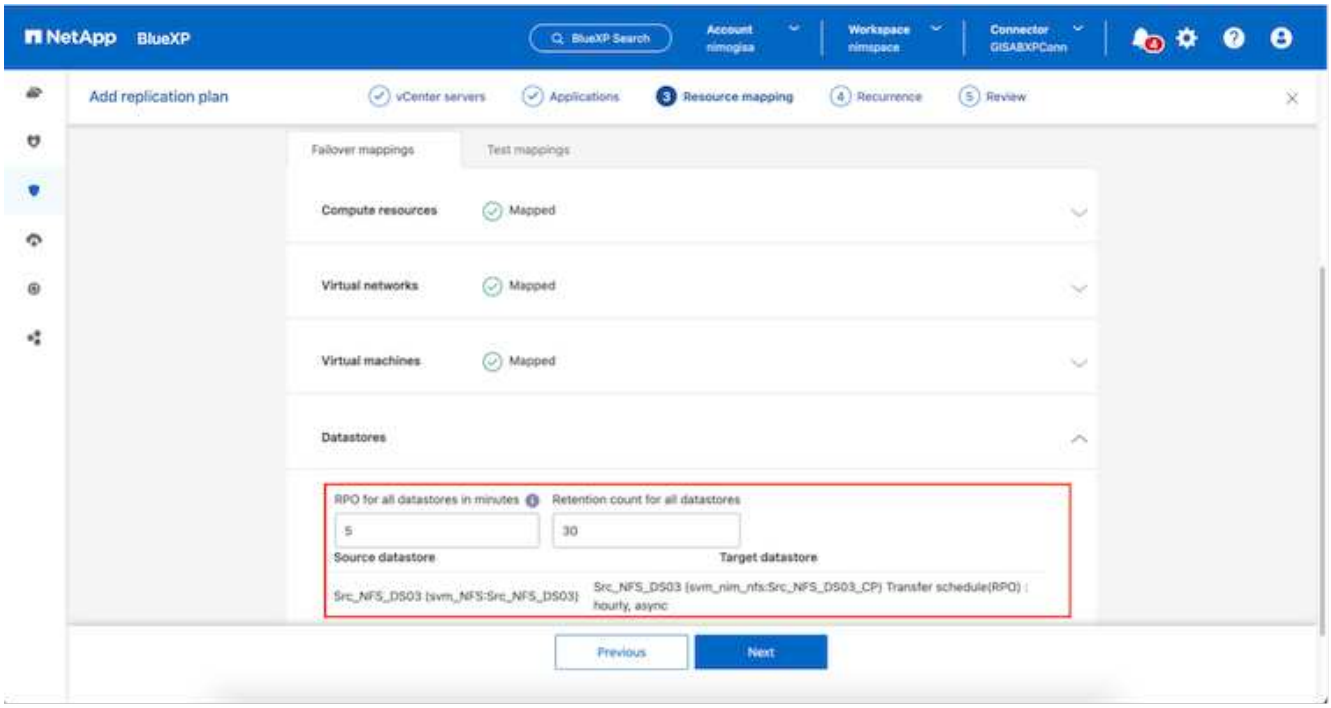
Comment le configurer pour la récupération après sinistre VMware

Le processus de création de la réplication SnapMirror reste le même pour toute application donnée. Le processus peut être manuel ou automatisé. La méthode la plus simple consiste à utiliser NetApp Console pour configurer la réplication SnapMirror en faisant simplement glisser-déposer le système ONTAP source de l'environnement vers la destination afin de lancer l'assistant qui vous guidera tout au long du reste du processus.



La reprise après sinistre peut également automatiser ce processus à condition que les deux critères suivants soient remplis :

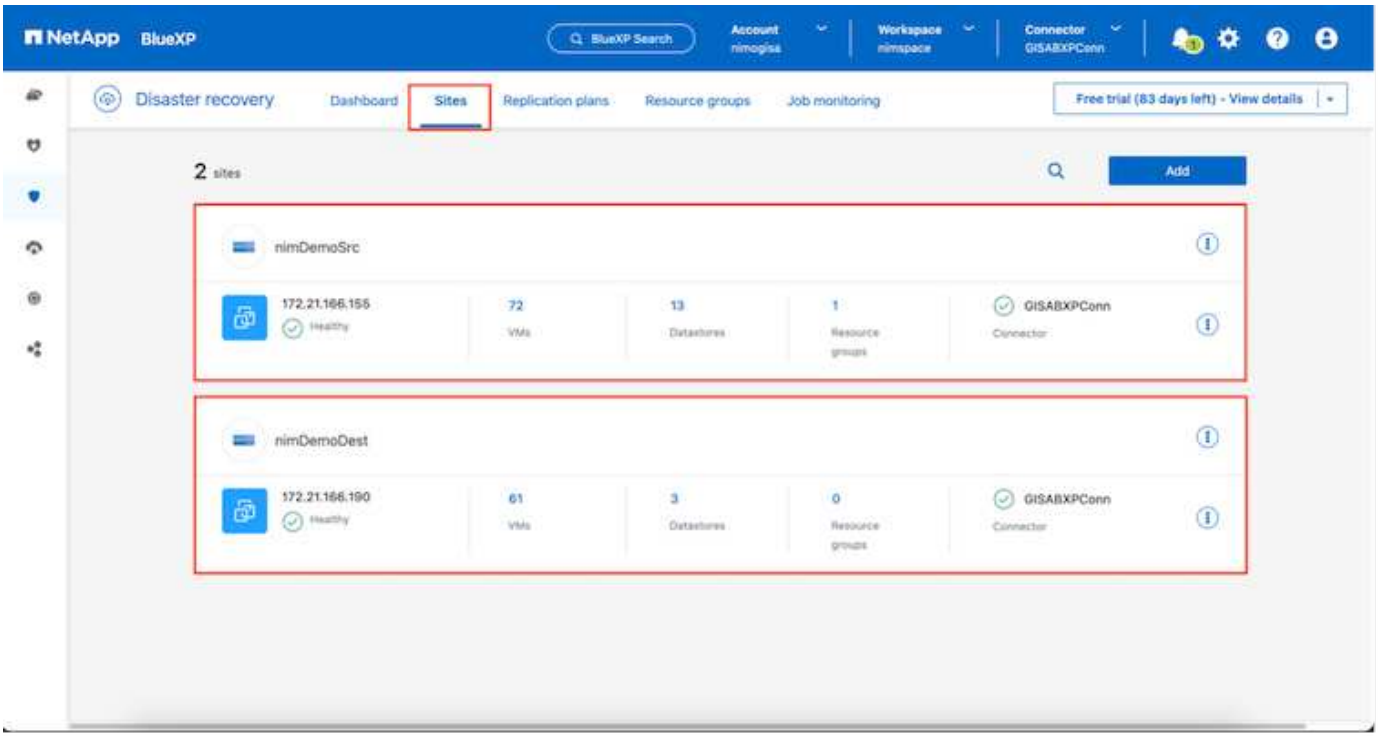
- Les clusters source et de destination ont une relation d'homologue.
- La SVM source et la SVM de destination ont une relation homologue.



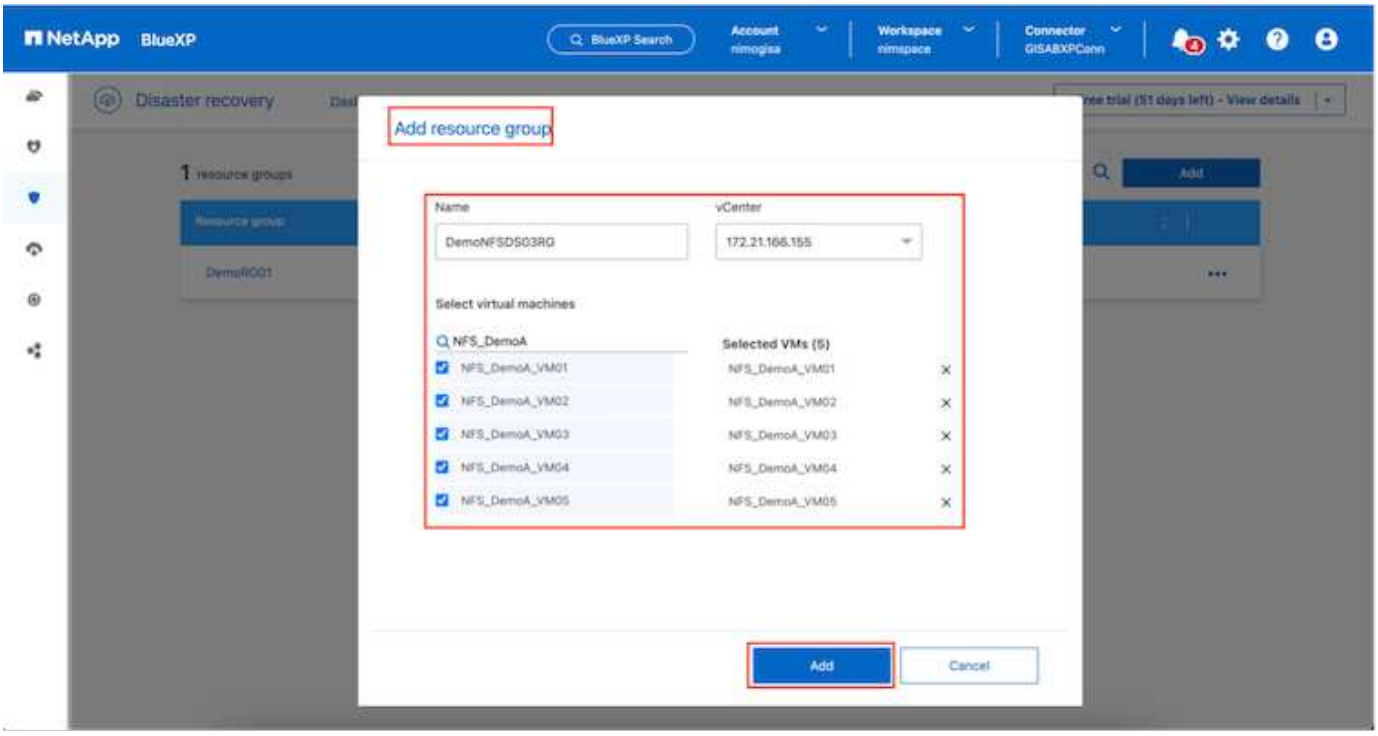
Si une relation SnapMirror est déjà configurée pour le volume via l'interface de ligne de commande (CLI), Disaster Recovery détecte la relation et poursuit le reste des opérations du workflow.

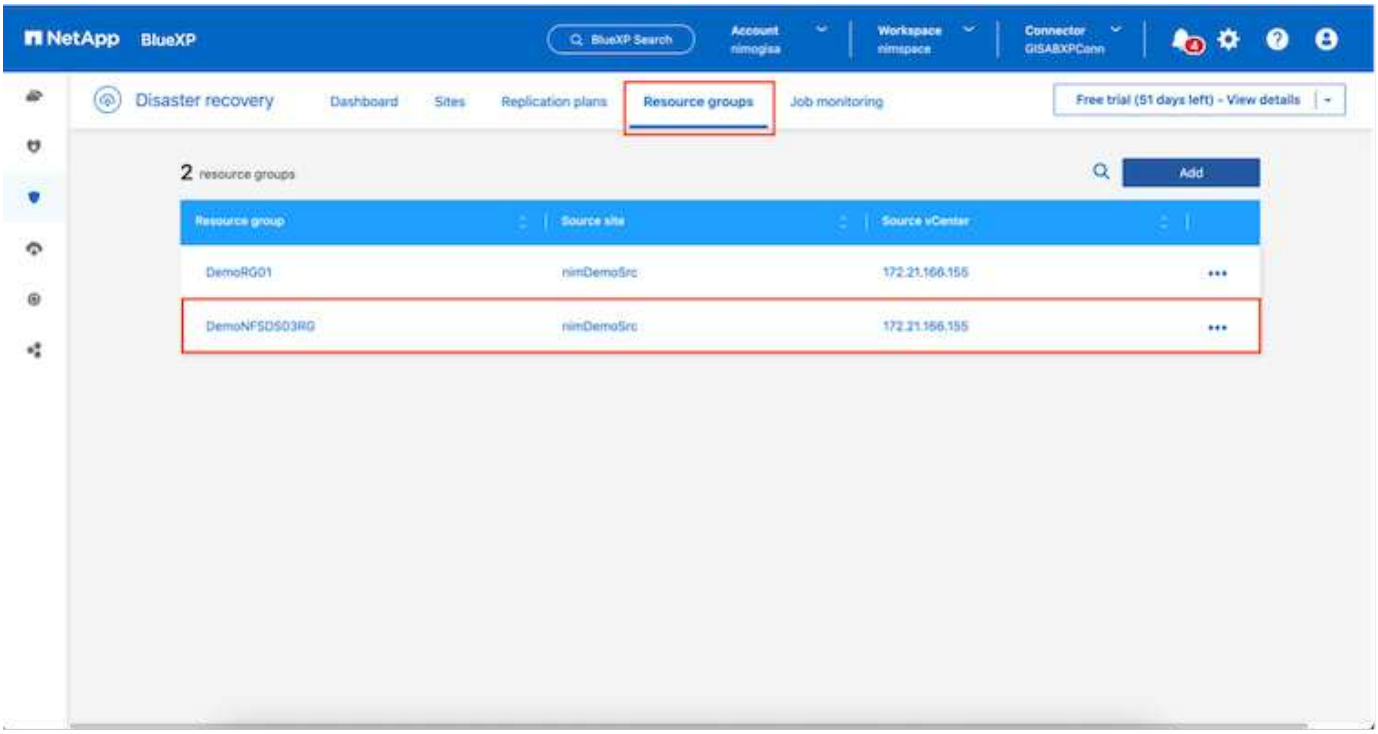
Que peut faire Disaster Recovery pour vous?

Une fois les sites source et de destination ajoutés, Disaster Recovery effectue une analyse approfondie automatique et affiche les machines virtuelles ainsi que leurs métadonnées associées. Disaster Recovery détecte et renseigne également automatiquement les réseaux et les groupes de ports utilisés par les machines virtuelles.



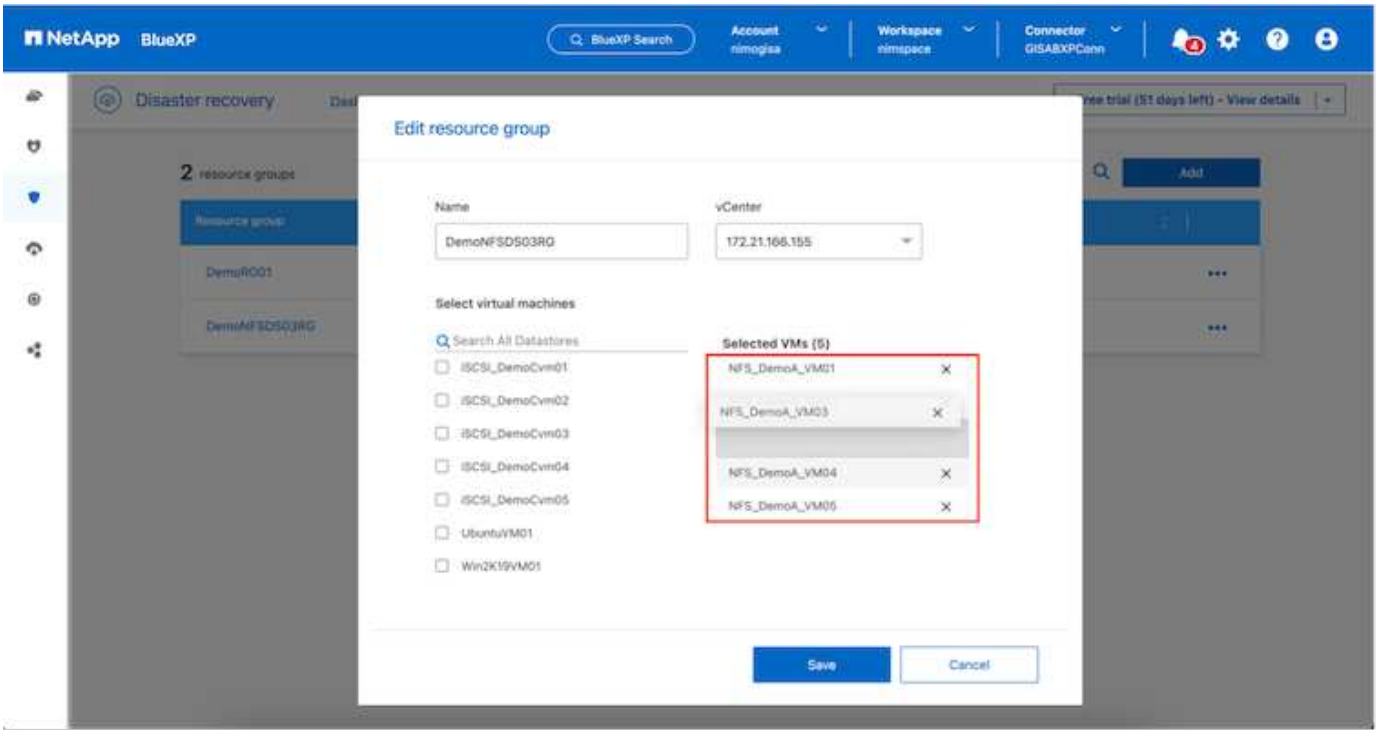
Une fois les sites ajoutés, les machines virtuelles peuvent être regroupées en groupes de ressources. Les groupes de ressources de reprise après sinistre vous permettent de regrouper un ensemble de machines virtuelles dépendantes en groupes logiques qui incluent leur ordre de démarrage et leurs délais de démarrage à appliquer lors de la reprise. Pour commencer à créer des groupes de ressources, accédez à **Groupes de ressources** et cliquez sur **Créer un groupe de ressources**.



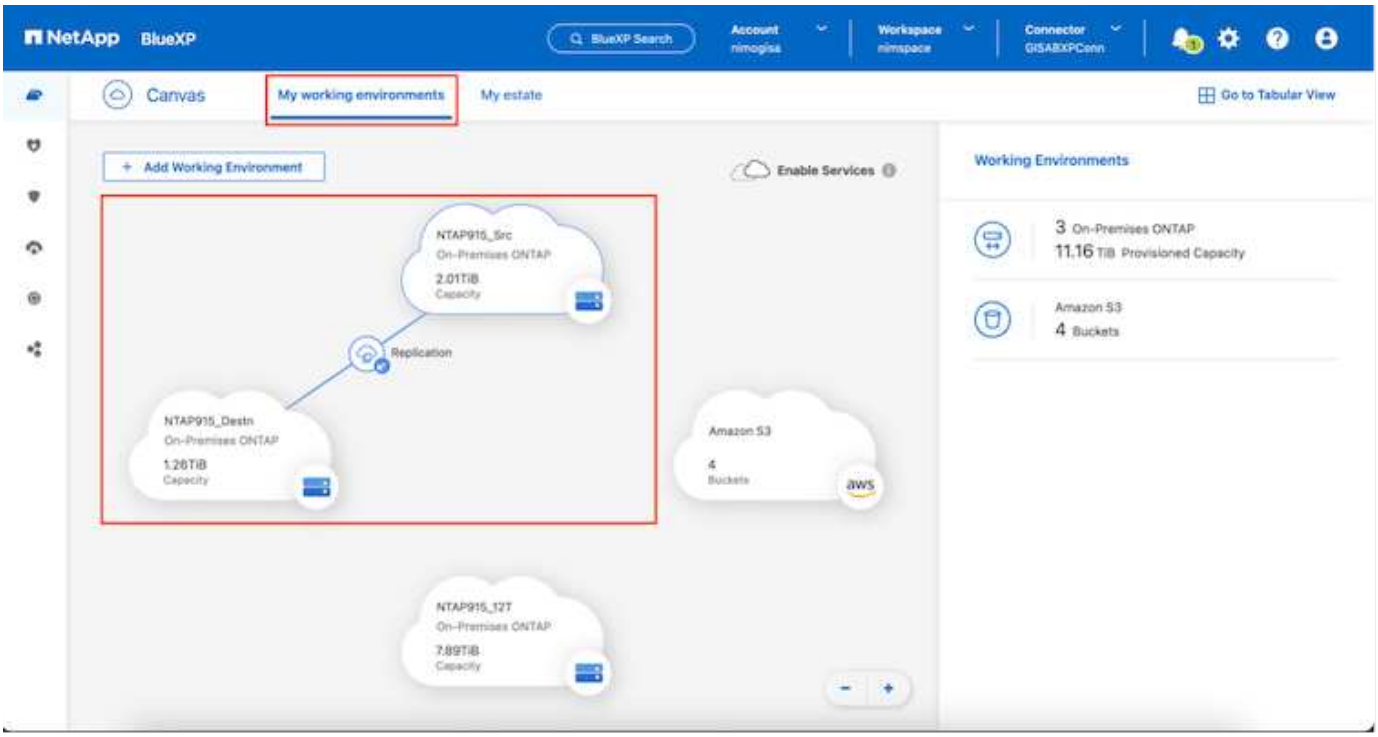


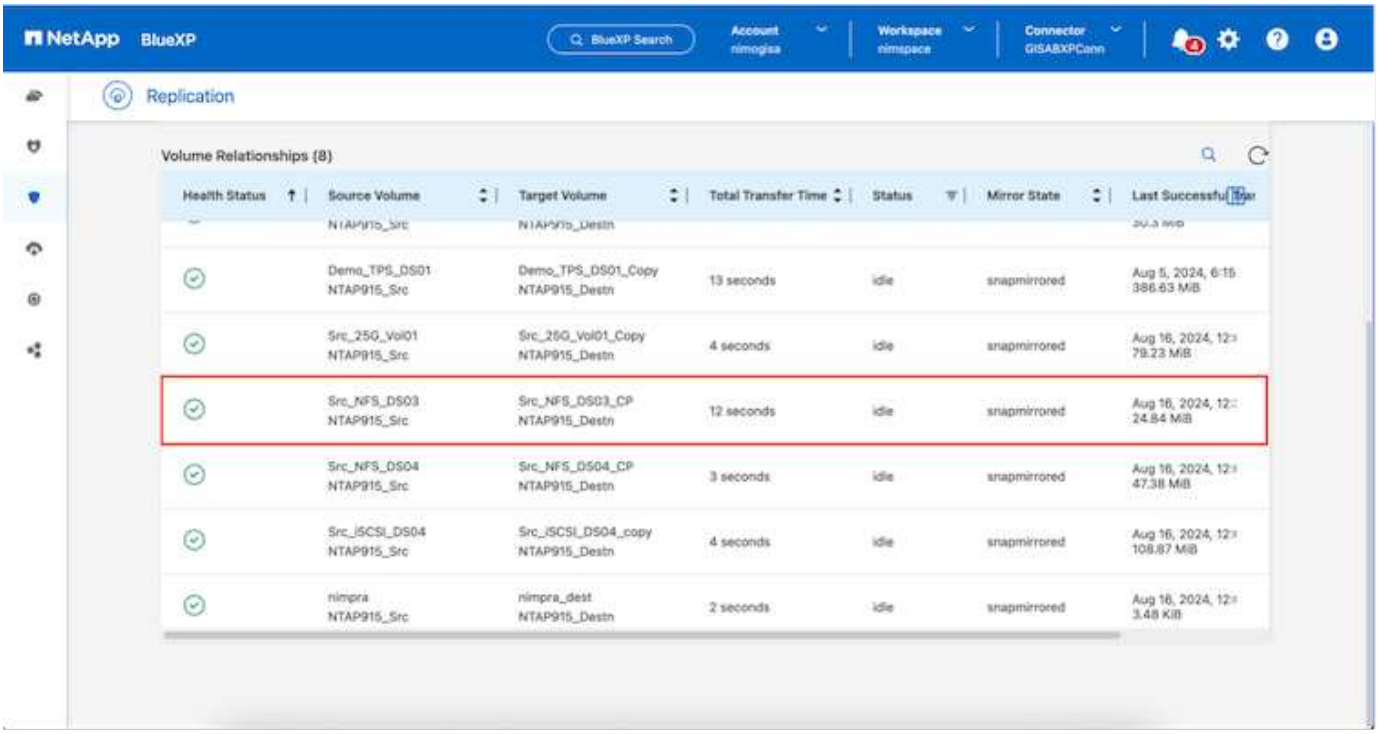
Le groupe de ressources peut également être créé lors de la création d'un plan de réplication.

L'ordre de démarrage des machines virtuelles peut être défini ou modifié lors de la création de groupes de ressources en utilisant un simple mécanisme de glisser-déposer.



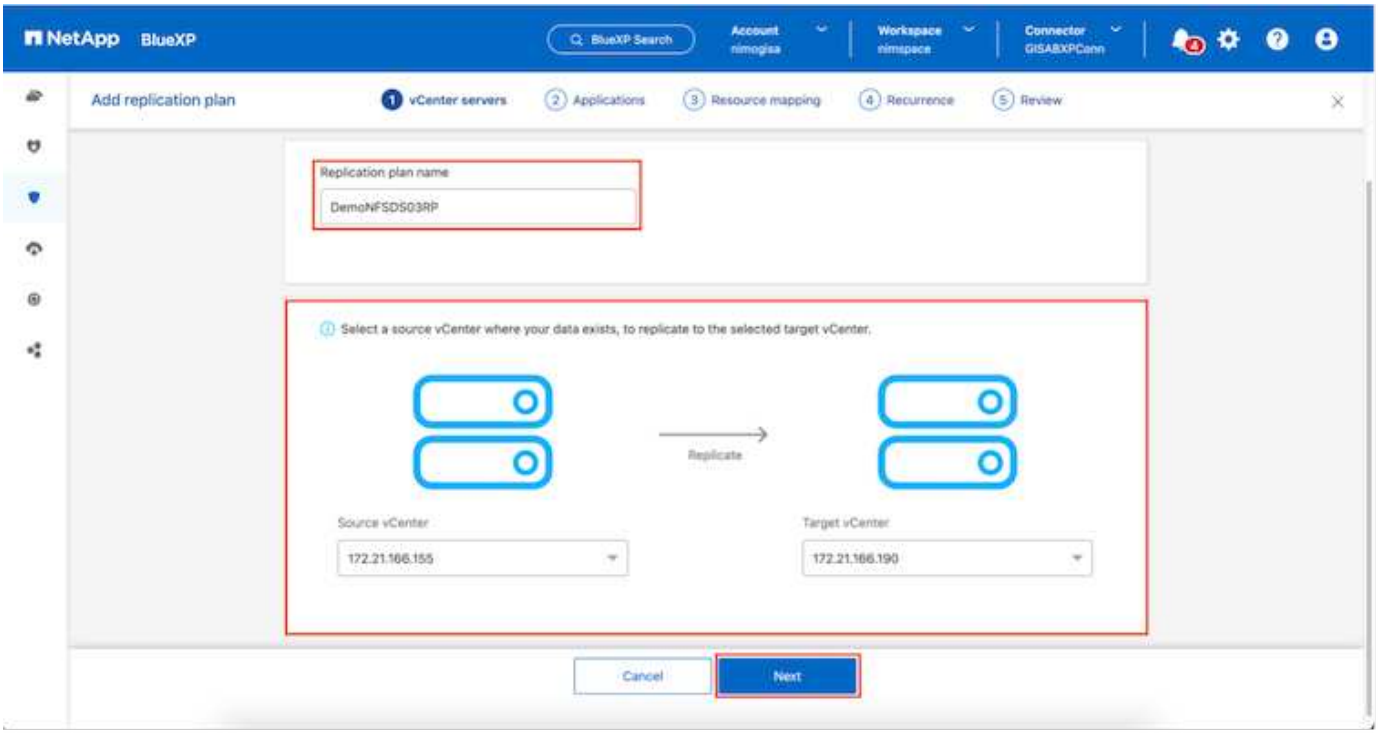
Une fois les groupes de ressources créés, l'étape suivante consiste à créer le plan d'exécution ou un plan de récupération des machines virtuelles et des applications en cas de sinistre. Comme mentionné dans les conditions préalables, la réplication SnapMirror peut être configurée au préalable ou DRaaS peut la configurer à l'aide du RPO et du nombre de rétention spécifiés lors de la création du plan de réplication.



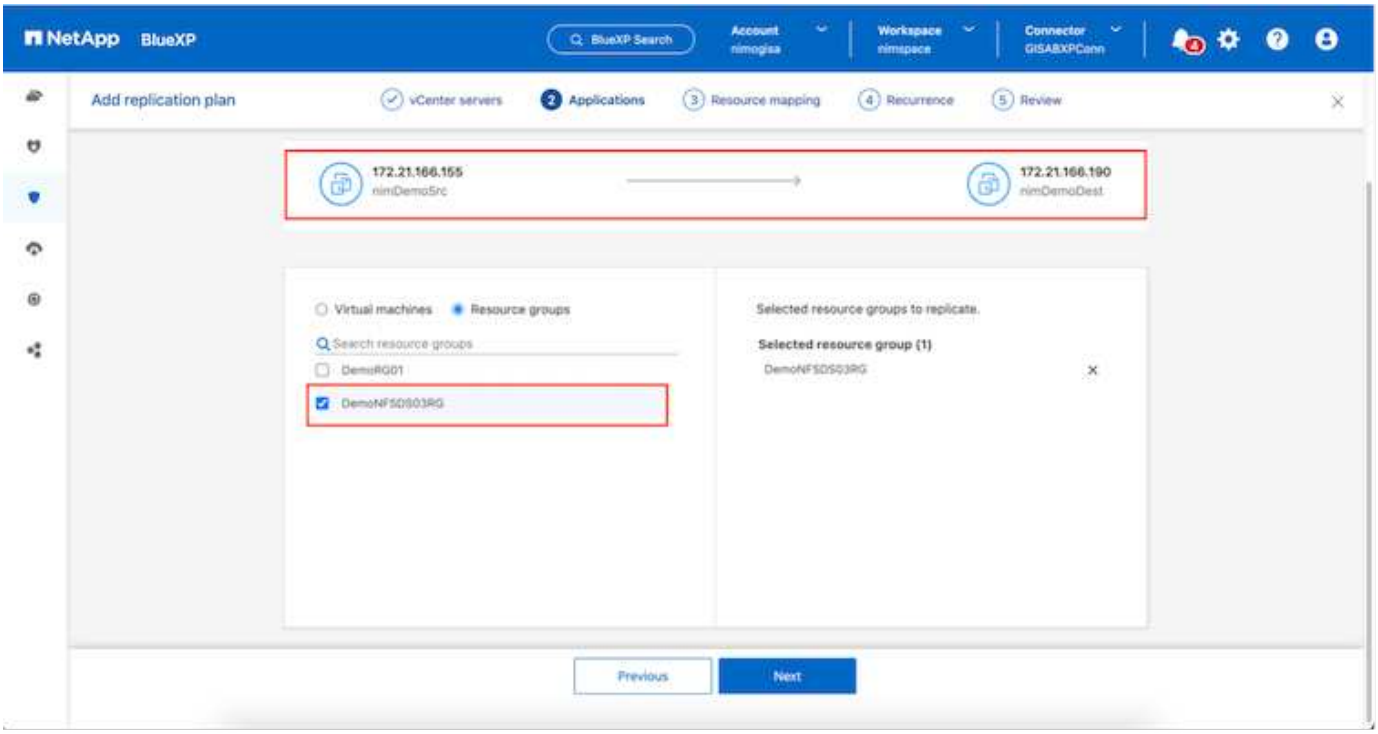


Configurez le plan de réplication en sélectionnant les plates-formes vCenter source et de destination dans la liste déroulante et choisissez les groupes de ressources à inclure dans le plan, ainsi que le regroupement de la manière dont les applications doivent être restaurées et mises sous tension et le mappage des clusters et des réseaux. Pour définir le plan de récupération, accédez à l'onglet **Plan de réplication** et cliquez sur **Ajouter un plan**.

Tout d'abord, sélectionnez le vCenter source, puis sélectionnez le vCenter de destination.



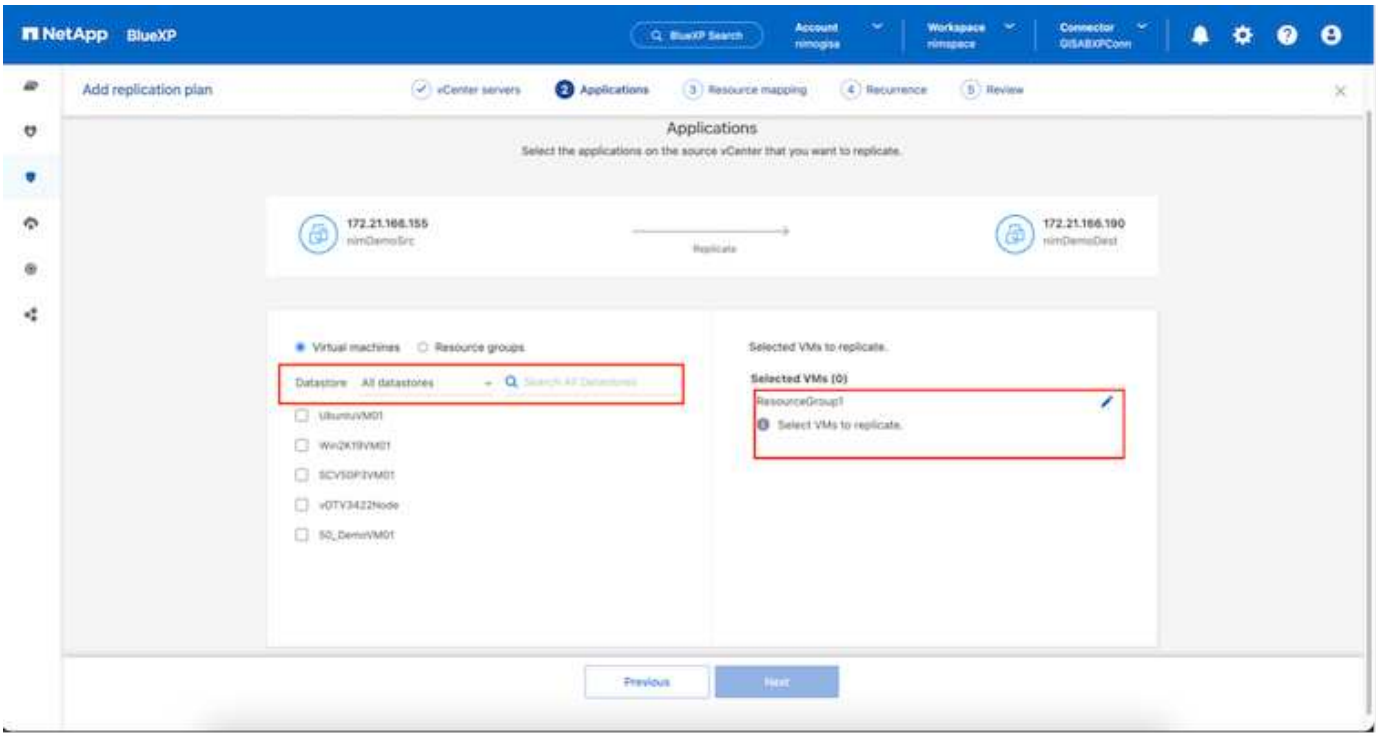
L'étape suivante consiste à sélectionner les groupes de ressources existants. Si aucun groupe de ressources n'est créé, l'assistant permet de regrouper les machines virtuelles requises (en créant essentiellement des groupes de ressources fonctionnels) en fonction des objectifs de récupération. Cela permet également de définir la séquence d'opérations selon laquelle les machines virtuelles d'application doivent être restaurées.



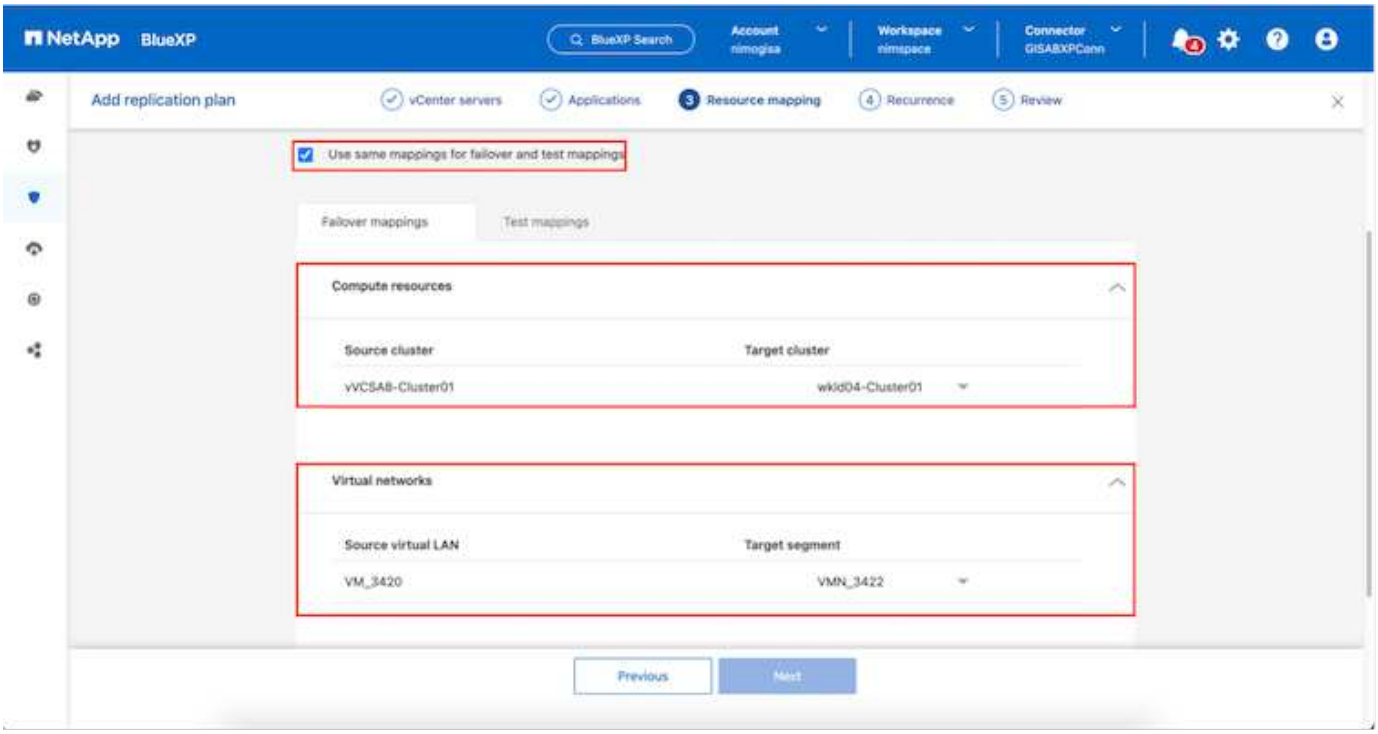
Le groupe de ressources permet de définir l'ordre de démarrage à l'aide de la fonctionnalité glisser-déposer. Il peut être utilisé pour modifier facilement l'ordre dans lequel les machines virtuelles seront mises sous tension pendant le processus de récupération.

Chaque machine virtuelle au sein d'un groupe de ressources est démarrée en séquence en fonction de l'ordre. Deux groupes de ressources sont démarrés en parallèle.

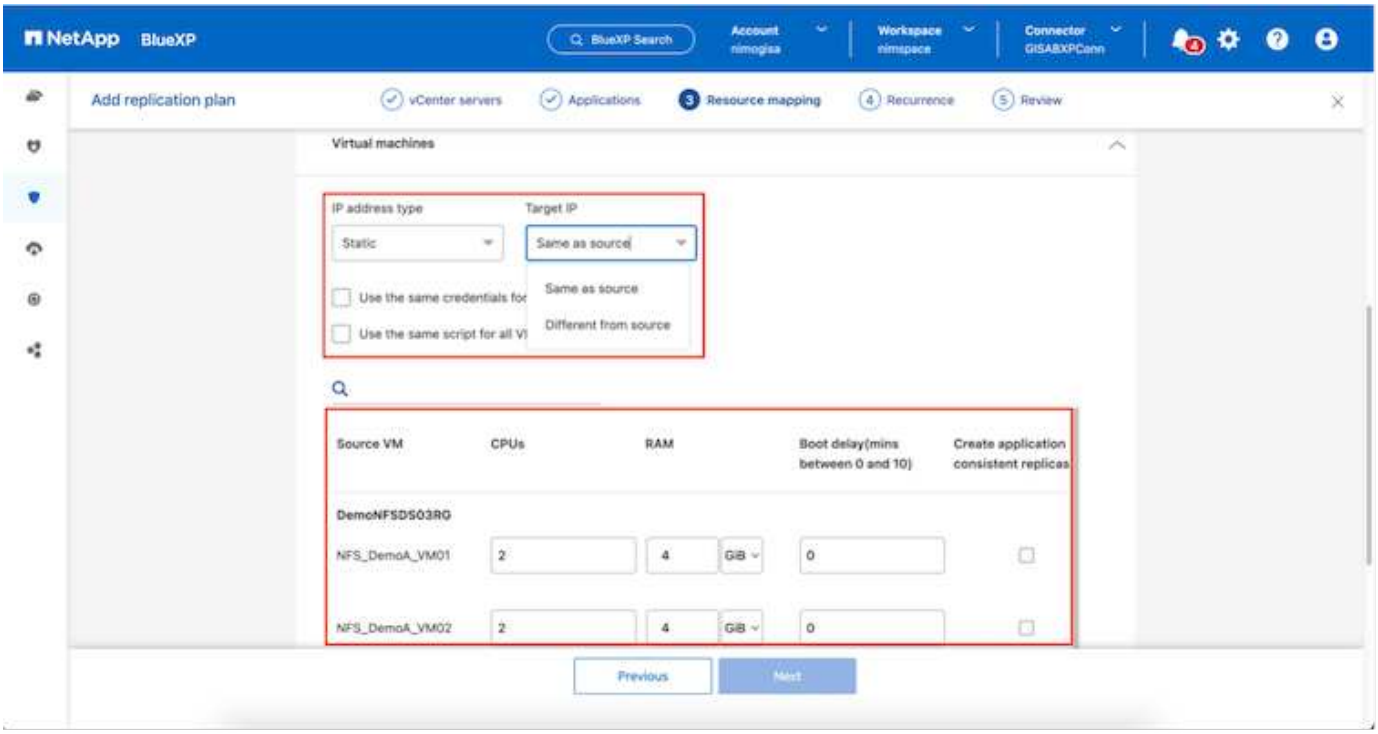
La capture d'écran ci-dessous montre l'option permettant de filtrer les machines virtuelles ou les banques de données spécifiques en fonction des exigences organisationnelles si les groupes de ressources ne sont pas créés au préalable.



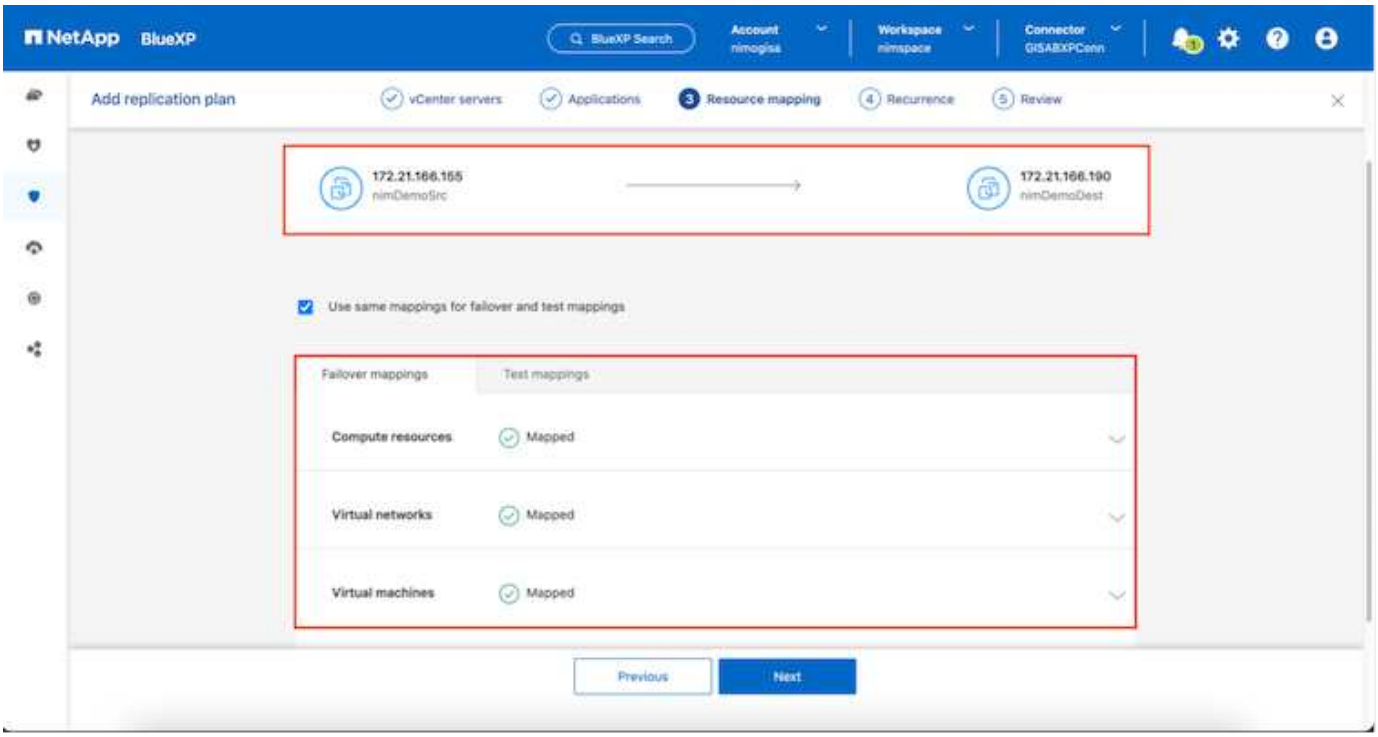
Une fois les groupes de ressources sélectionnés, créez les mappages de basculement. À cette étape, indiquez comment les ressources de l'environnement source sont mappées vers la destination. Cela inclut les ressources de calcul et les réseaux virtuels. La personnalisation des adresses IP, les scripts préalables et postérieurs, les délais de démarrage, la cohérence des applications, etc. Pour plus d'informations, consultez "Créer un plan de réplication".



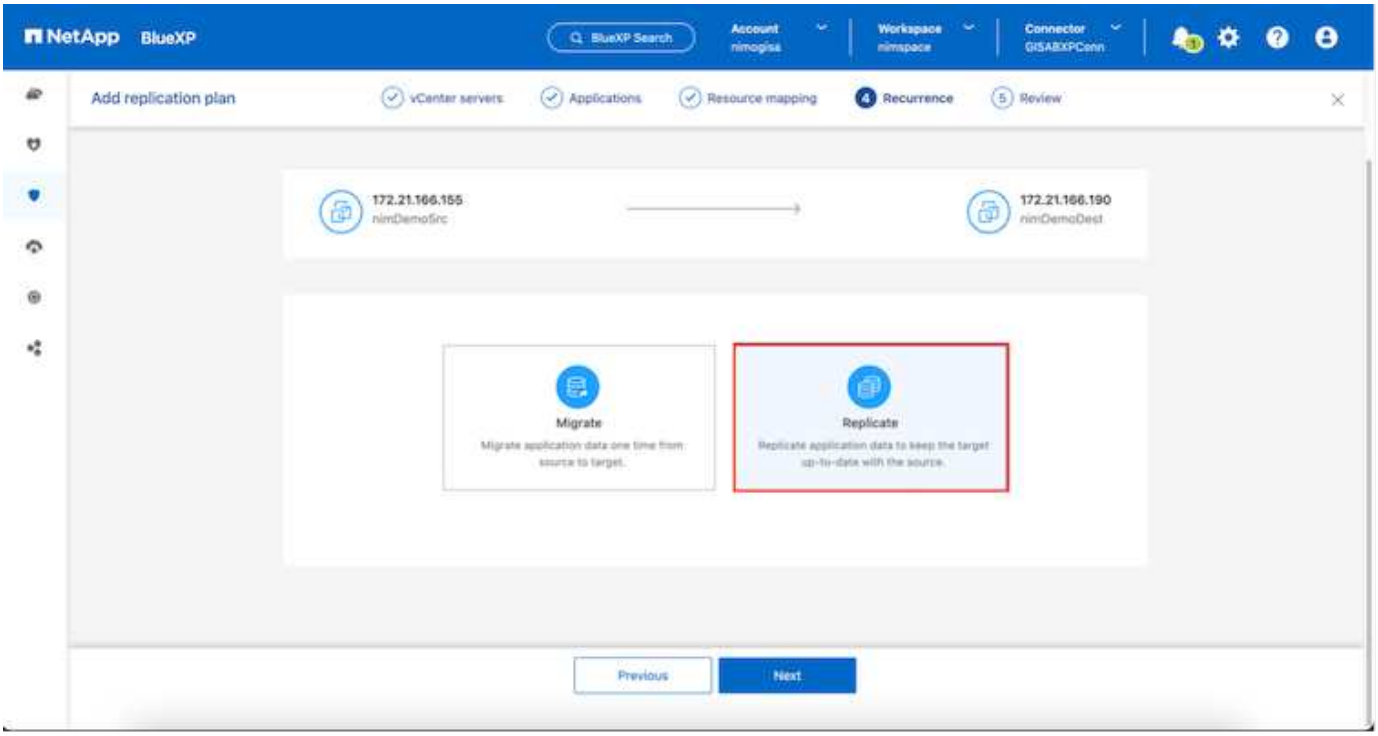
Par défaut, les mêmes paramètres de mappage sont utilisés pour les opérations de test et de basculement. Pour définir différents mappages pour l'environnement de test, sélectionnez l'option Mappage de test après avoir décoché la case comme indiqué ci-dessous :



Une fois le mappage des ressources terminé, cliquez sur Suivant.



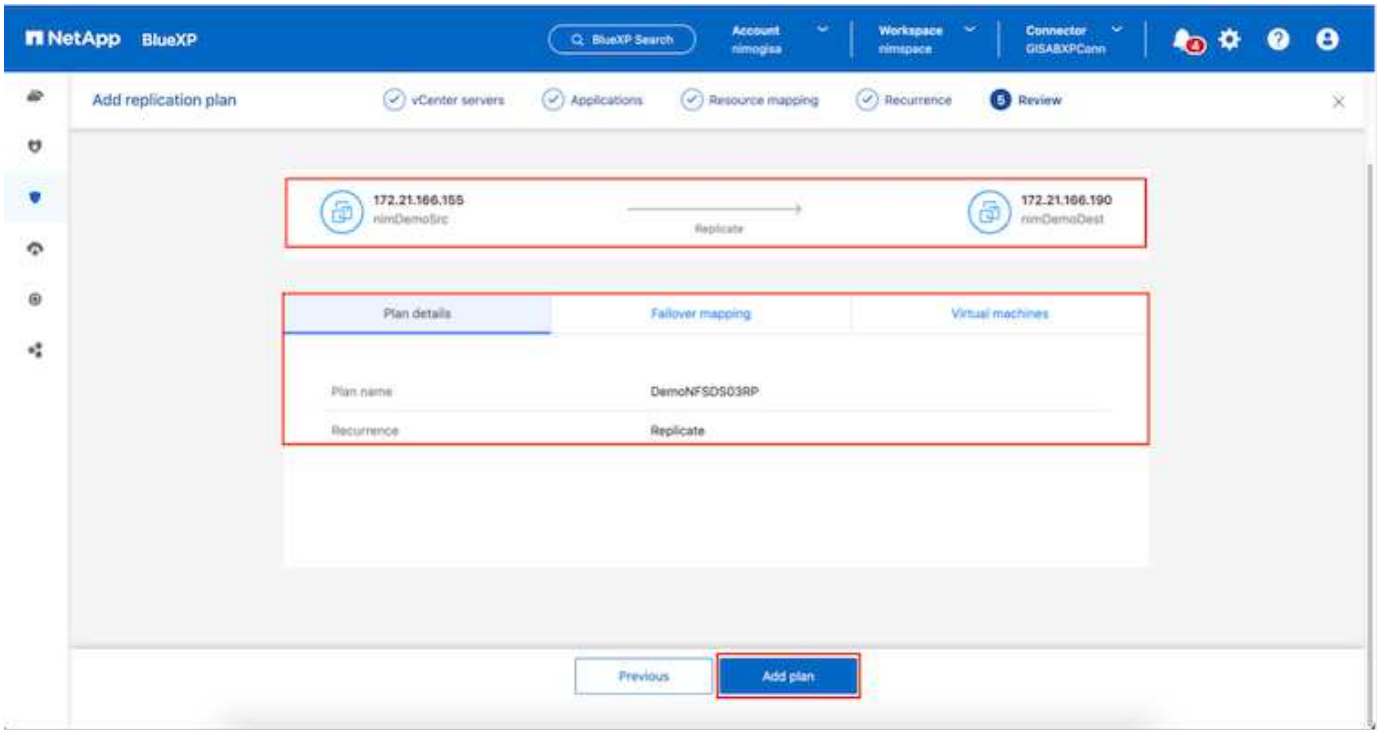
Sélectionnez le type de récurrence. En termes simples, sélectionnez l'option Migrer (migration unique utilisant le basculement) ou la réplication continue récurrente. Dans cette procédure pas à pas, l'option Répliquer est sélectionnée.

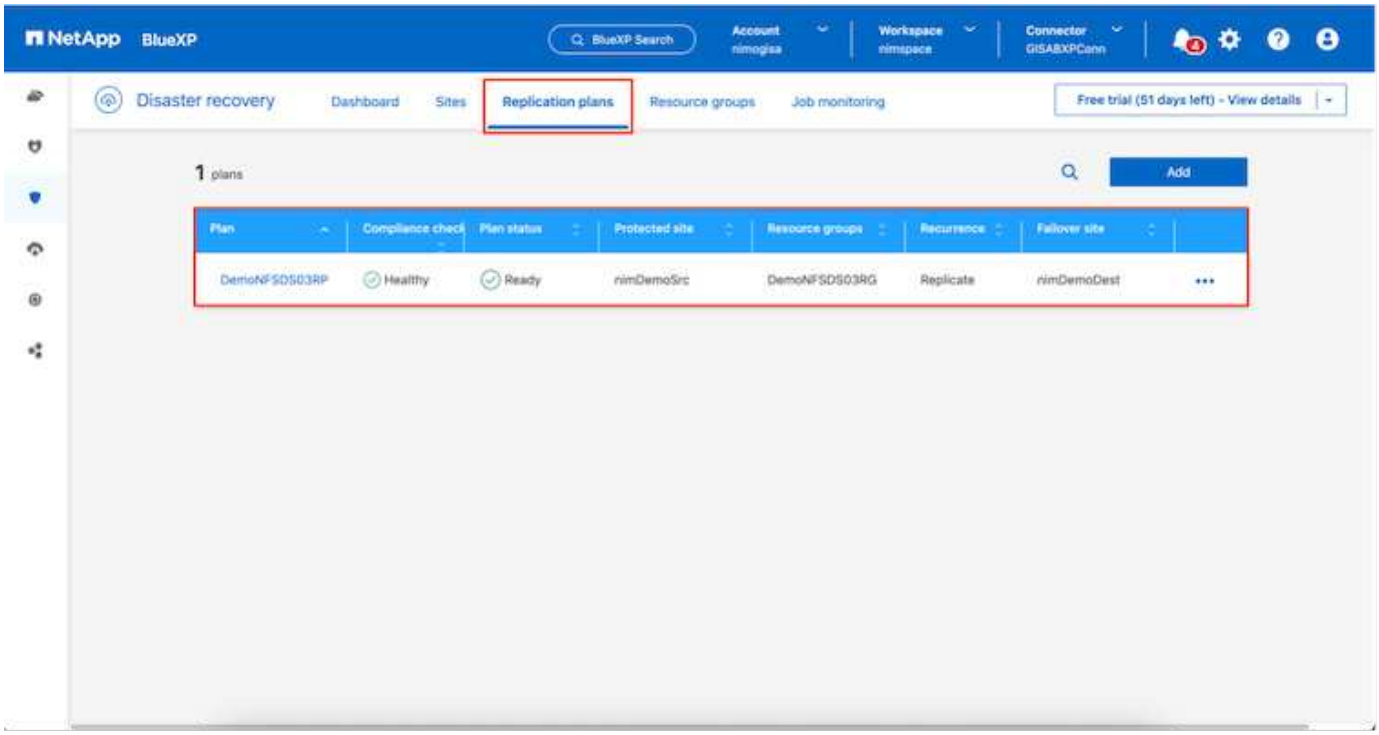


Une fois terminé, vérifiez les mappages créés, puis cliquez sur **Ajouter un plan**.

Les machines virtuelles (VM) provenant de différents volumes et SVM peuvent être incluses dans un plan de réplication. Selon l'emplacement des VM (sur le même volume ou sur des volumes distincts au sein de la même SVM, ou encore sur des volumes distincts dans

différentes SVM), Disaster Recovery crée un instantané de groupe de cohérence.



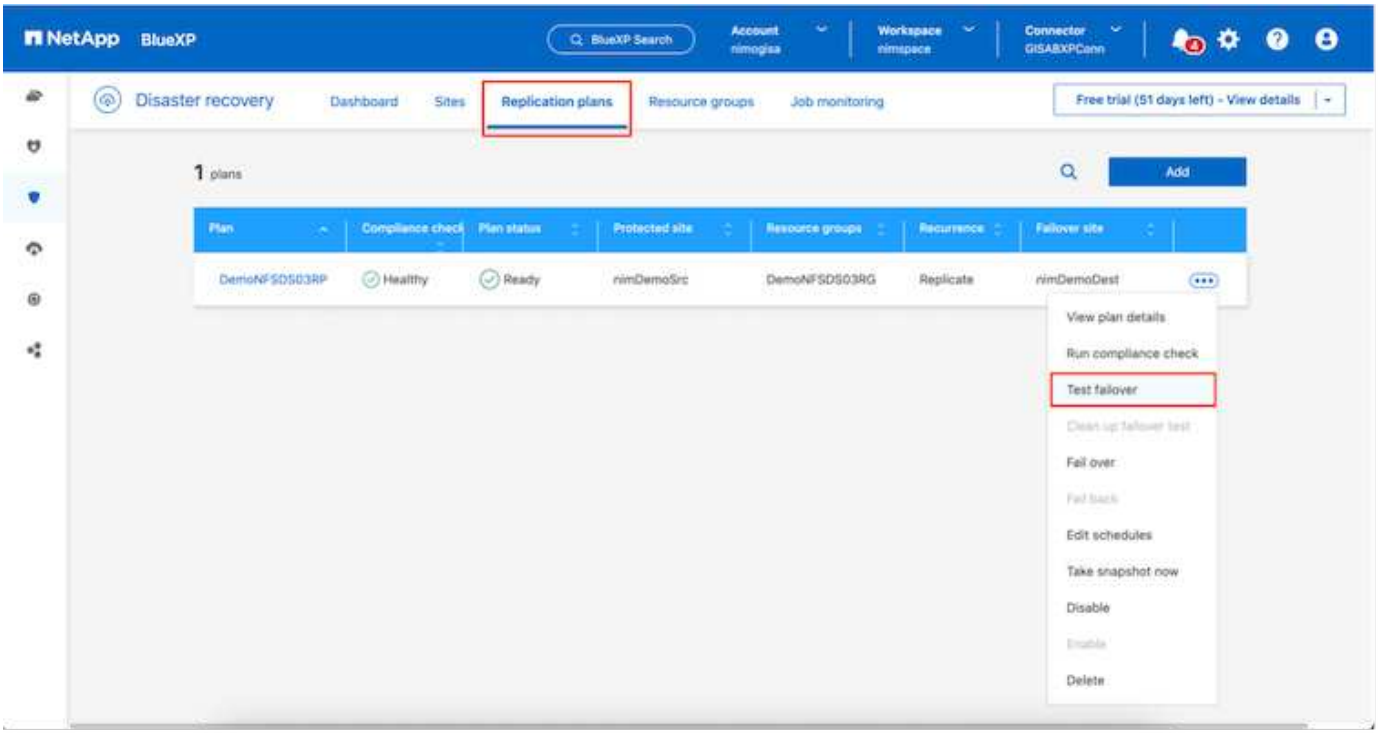


La reprise après sinistre comprend les flux de travail suivants :

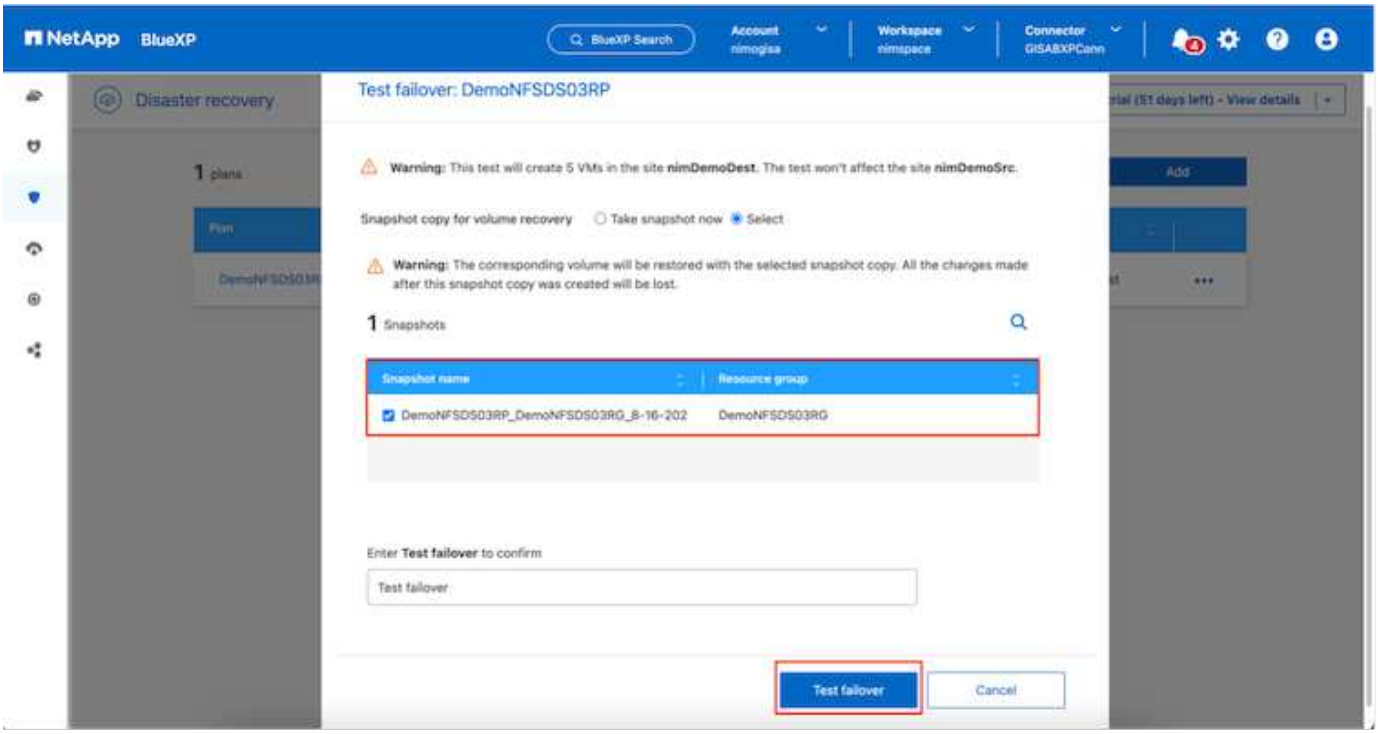
- Test de basculement (y compris les simulations automatisées périodiques)
- Test de basculement de nettoyage
- Basculement
- Retour arrière

Test de basculement

Le test de basculement dans Disaster Recovery est une procédure opérationnelle qui permet aux administrateurs VMware de valider entièrement leurs plans de reprise sans perturber leurs environnements de production. Lors d'un test de basculement, Disaster Recovery crée des copies NetApp FlexClone à faible encombrement des volumes de datastore NFS répliqués sur le système de stockage DR. Ces volumes FlexClone sont ensuite montés sur les hôtes ESXi du site DR, et les VM sont mises sous tension dans un réseau de test isolé. Ce processus permet aux administrateurs de vérifier que leurs plans de reprise après sinistre fonctionneront comme prévu en cas de sinistre réel.

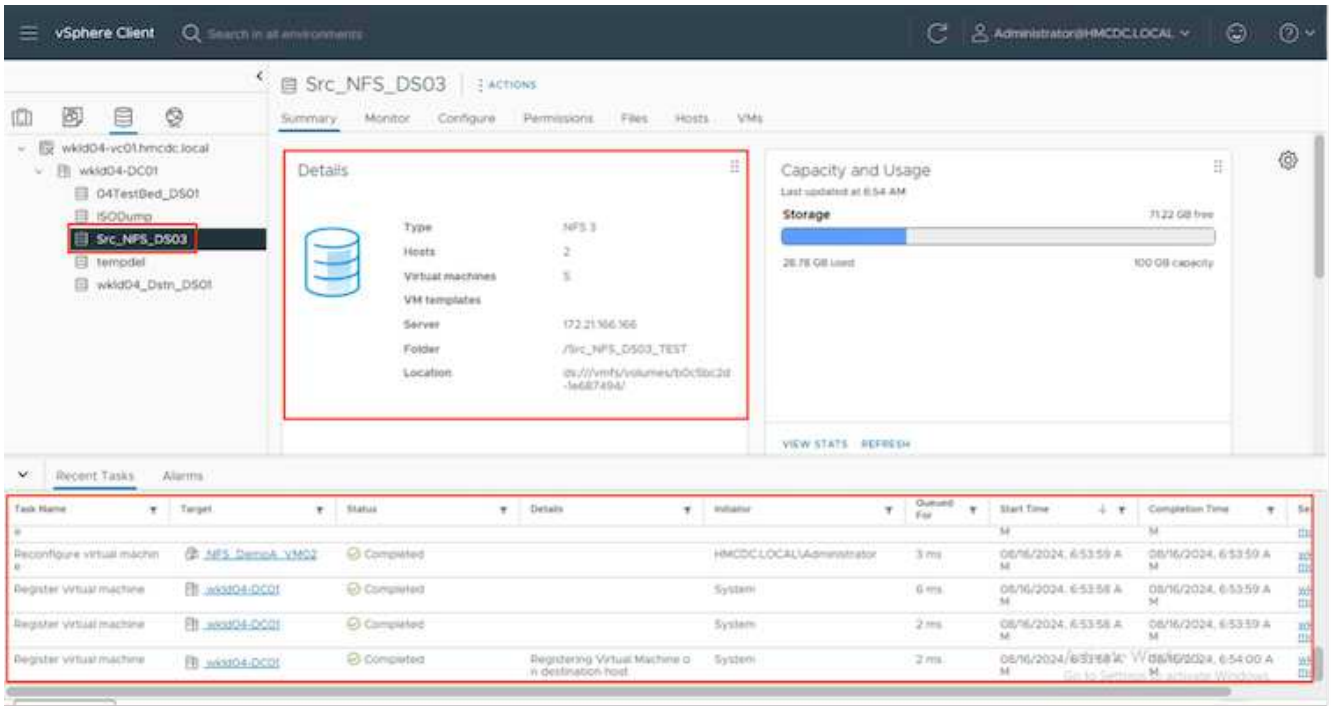


La reprise après sinistre intègre la possibilité de sélectionner l'instantané comme fonctionnalité facultative lors de l'opération de test de basculement. Cette fonctionnalité permet à l'administrateur VMware de vérifier que toutes les modifications récemment apportées à l'environnement sont répliquées vers le site de destination et sont donc présentes pendant le test. Ces modifications incluent les correctifs du système d'exploitation invité de la machine virtuelle



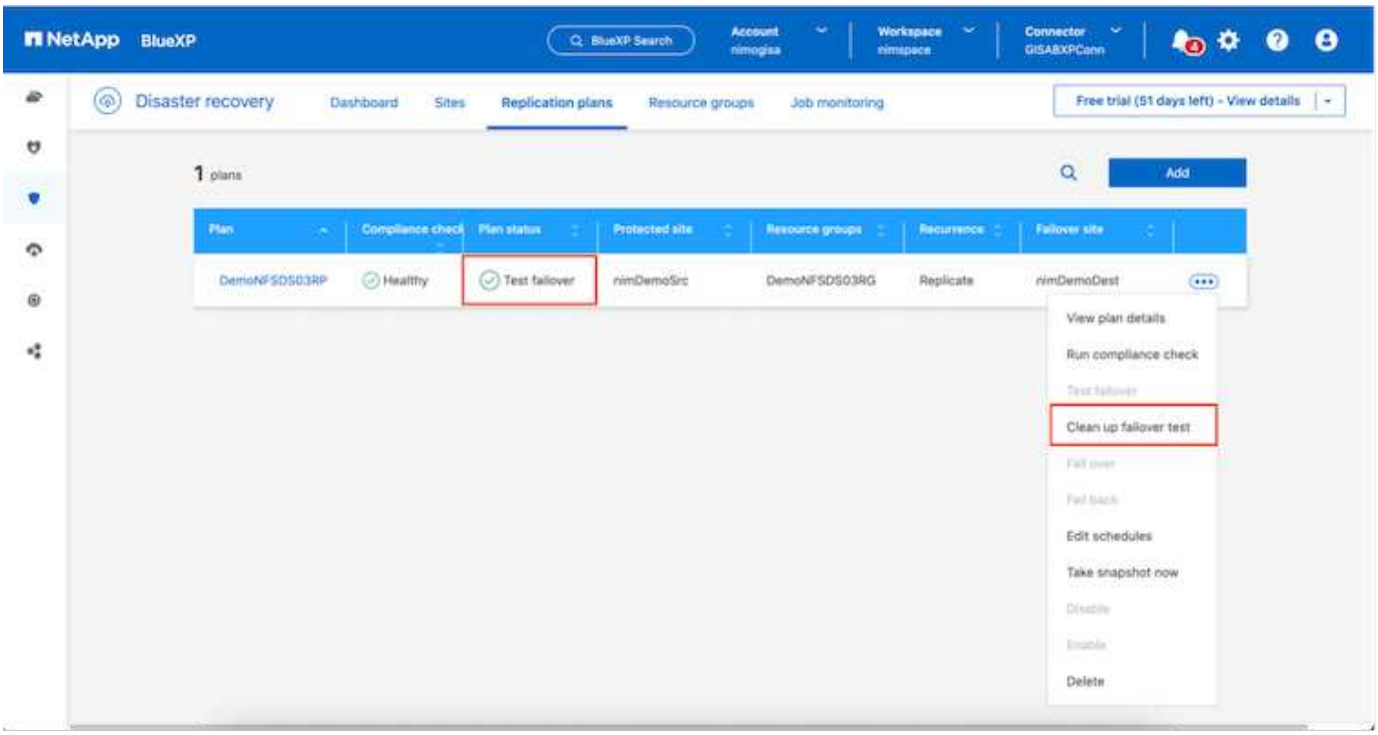
Lorsqu'un administrateur VMware exécute une opération de basculement de test, Disaster Recovery automatise les tâches suivantes :

- Déclenchement des relations SnapMirror pour mettre à jour le stockage sur le site de destination avec toutes les modifications récentes apportées sur le site de production.
- Création de volumes NetApp FlexClone des volumes FlexVol sur la baie de stockage DR.
- Connexion des banques de données NFS dans les volumes FlexClone aux hôtes ESXi sur le site DR.
- Connexion des adaptateurs réseau VM au réseau de test spécifié lors du mappage.
- Reconfiguration des paramètres réseau du système d'exploitation invité de la machine virtuelle tels que définis pour le réseau sur le site DR.
- Exécution de toutes les commandes personnalisées qui ont été stockées dans le plan de réplication.
- Mise sous tension des machines virtuelles dans l'ordre défini dans le plan de réplication.



Opération de test de basculement de nettoyage

L'opération de test de basculement de nettoyage se produit une fois le test du plan de réplication terminé et l'administrateur VMware répond à l'invite de nettoyage.



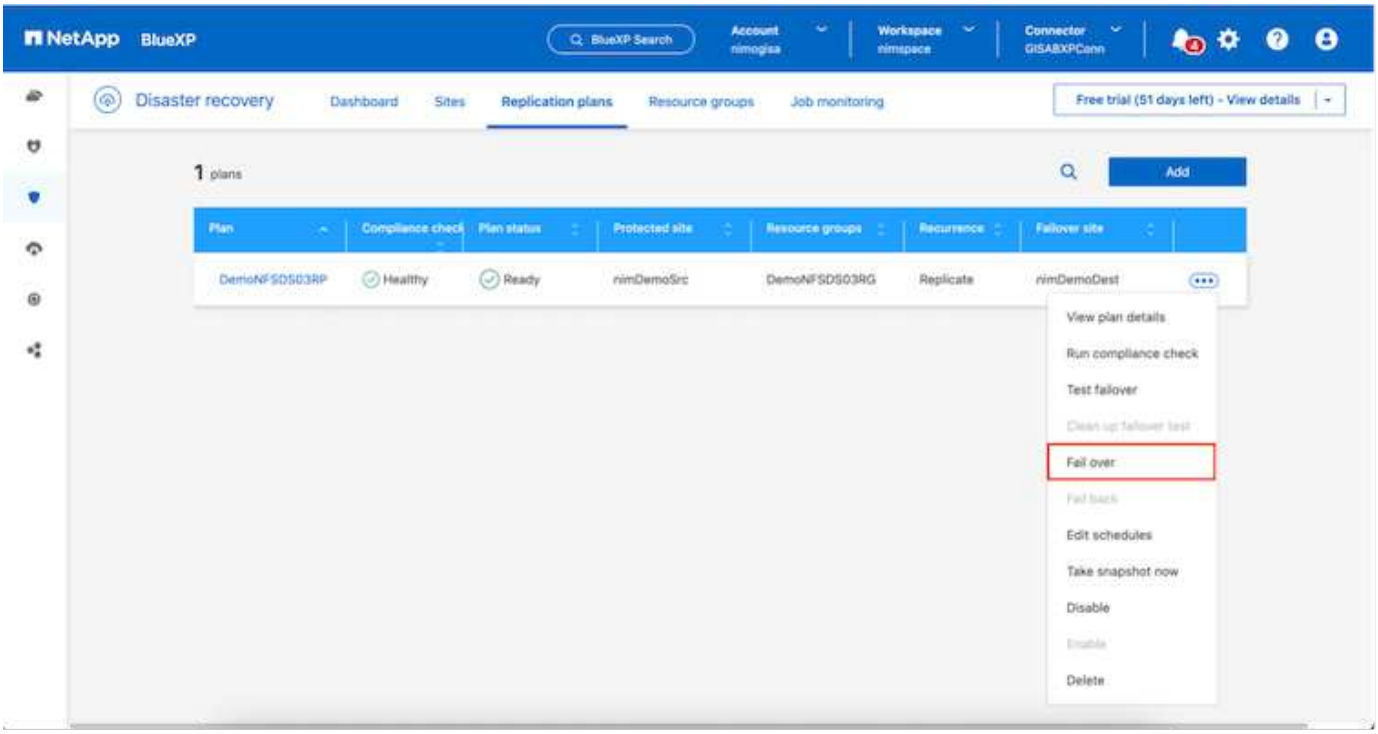
Cette action réinitialisera les machines virtuelles (VM) et l'état du plan de réplication à l'état prêt.

Lorsqu'un administrateur VMware effectue une opération de récupération, Disaster Recovery suit le processus suivant :

1. Il met hors tension chaque machine virtuelle récupérée dans la copie FlexClone qui a été utilisée pour les tests.
2. Il supprime le volume FlexClone qui a été utilisé pour présenter les machines virtuelles récupérées pendant le test.

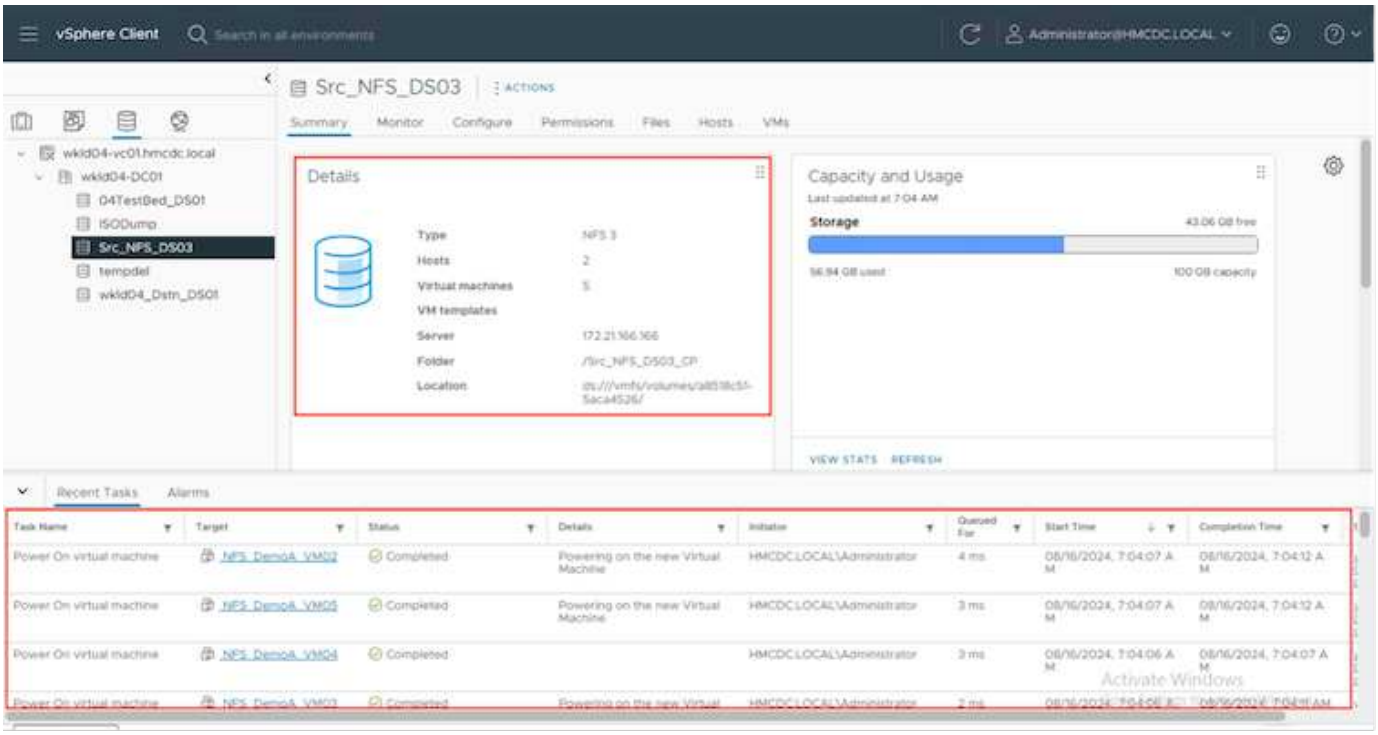
Migration planifiée et basculement

Disaster Recovery propose deux méthodes pour effectuer un basculement réel : la migration planifiée et le basculement. La première méthode, la migration planifiée, intègre l'arrêt des VM et la synchronisation de la réplication du stockage dans le processus afin de récupérer ou de déplacer effectivement les VM vers le site de destination. La migration planifiée nécessite un accès au site source. La seconde méthode, le basculement, est un basculement planifié ou non planifié dans lequel les VM sont récupérées sur le site de destination à partir du dernier intervalle de réplication du stockage qui a pu s'achever. Selon le RPO défini dans la solution, une certaine perte de données est à prévoir dans le scénario de DR.



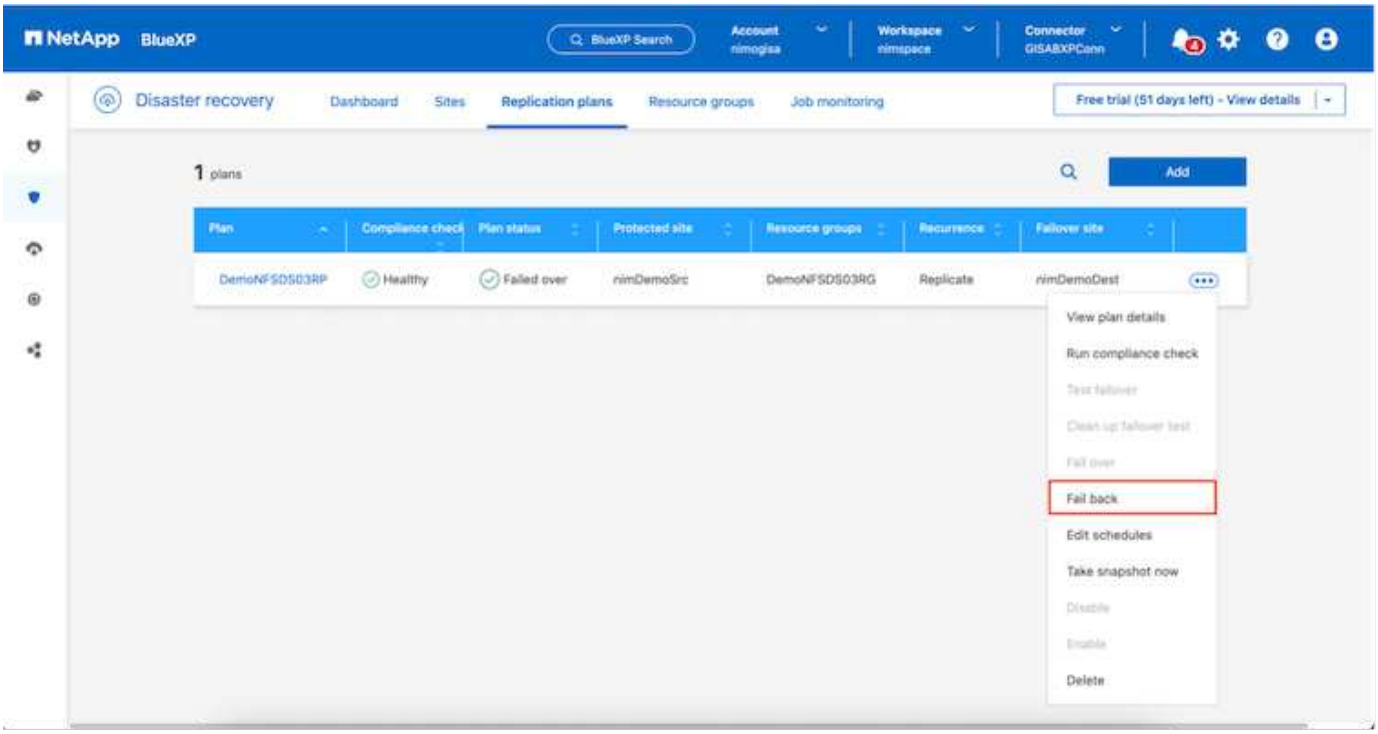
Lorsqu'un administrateur VMware effectue une opération de basculement, Disaster Recovery automatise les tâches suivantes :

- Interrompez et basculez les relations NetApp SnapMirror .
- Connectez les banques de données NFS répliquées aux hôtes ESXi sur le site DR.
- Connectez les adaptateurs réseau VM au réseau du site de destination approprié.
- Reconfigurez les paramètres réseau du système d'exploitation invité de la machine virtuelle tels que définis pour le réseau sur le site de destination.
- Exécutez toutes les commandes personnalisées (le cas échéant) qui ont été stockées dans le plan de réplication.
- Mettez sous tension les machines virtuelles dans l'ordre défini dans le plan de réplication.



Retour arrière

Une restauration est une procédure facultative qui restaure la configuration d'origine des sites source et de destination après une récupération.



Les administrateurs VMware peuvent configurer et exécuter une procédure de restauration automatique lorsqu'ils sont prêts à restaurer les services sur le site source d'origine.

REMARQUE : Disaster Recovery réplique (resynchronise) toutes les modifications vers la machine virtuelle source d'origine avant d'inverser le sens de la réplication. Ce processus démarre à partir d'une relation ayant

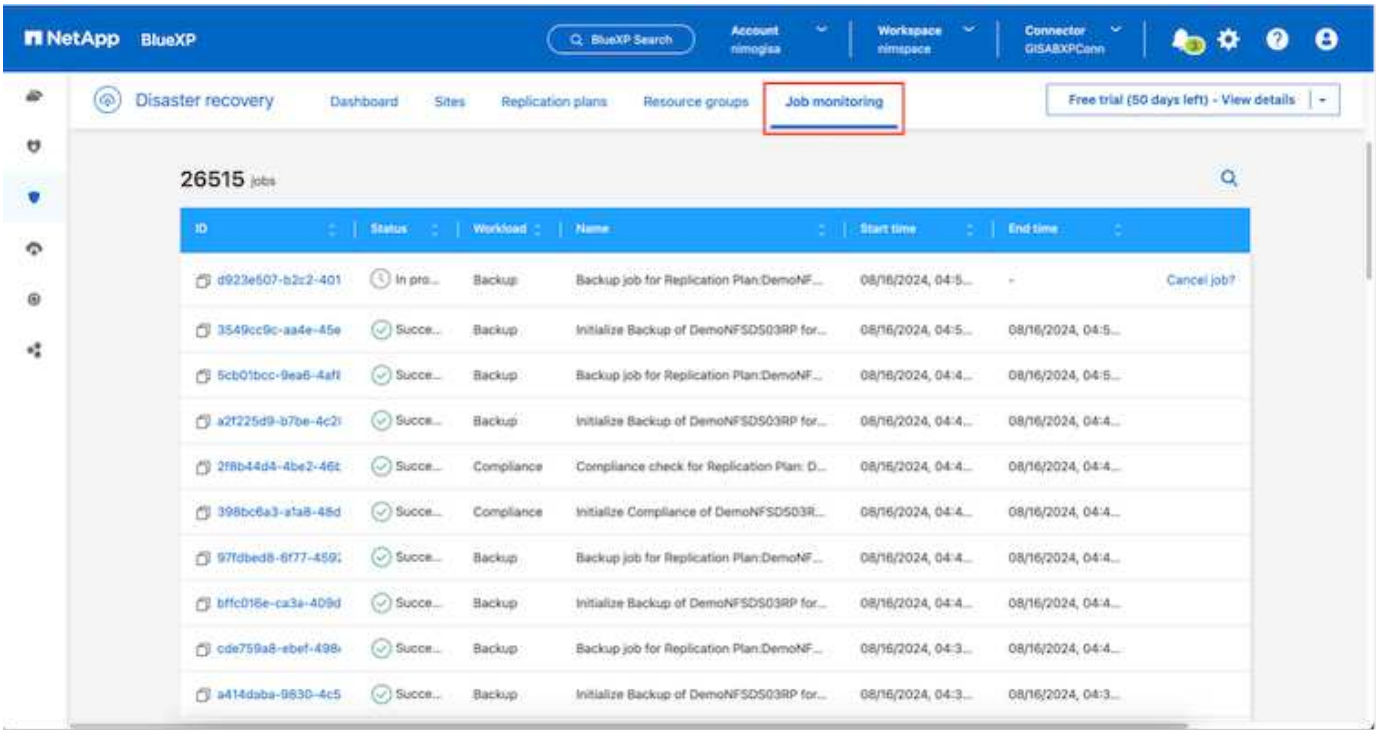
terminé le basculement vers une cible et comprend les étapes suivantes :

- Mettez hors tension et désenregistrez les machines virtuelles et les volumes sur le site de destination sont démontés.
- Rompre la relation SnapMirror sur la source d'origine est rompue pour la rendre en lecture/écriture.
- Resynchronisez la relation SnapMirror pour inverser la réplication.
- Montez le volume sur la source, mettez sous tension et enregistrez les machines virtuelles sources.

Pour plus de détails sur l'accès à Disaster Recovery et sa configuration, consultez le "Découvrez NetApp Disaster Recovery pour VMware".

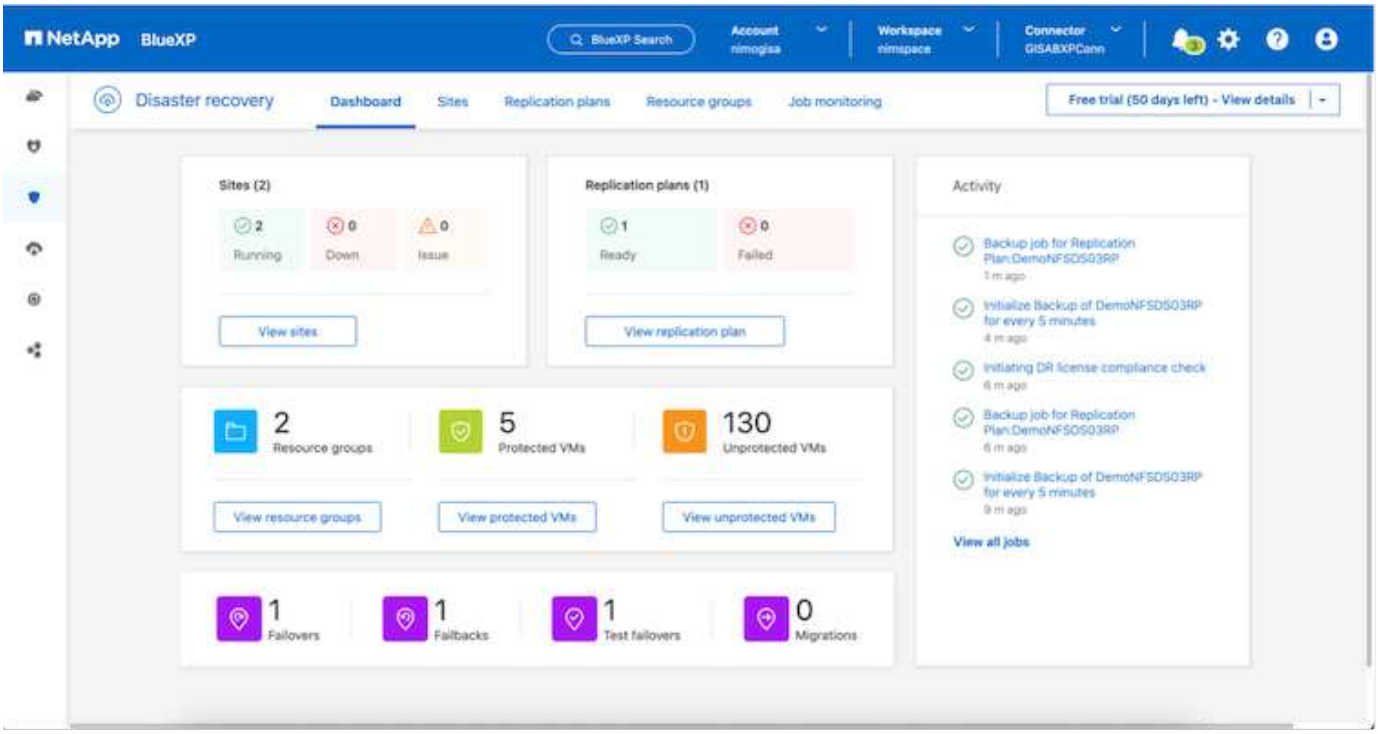
Surveillance et tableau de bord

Depuis Console ou l'ONTAP CLI, vous pouvez surveiller l'état de santé de la réplication des volumes de datastore appropriés, et suivre l'état d'un basculement ou d'un test de basculement via Job Monitoring.



Si un travail est actuellement en cours ou en file d'attente et que vous souhaitez l'arrêter, il existe une option pour l'annuler.

Le tableau de bord de reprise après sinistre permet d'évaluer en toute confiance l'état des sites de reprise après sinistre et des plans de réplication. Les administrateurs peuvent ainsi identifier rapidement les sites et les plans sains, déconnectés ou dégradés.



Cela fournit une solution puissante pour gérer un plan de reprise après sinistre personnalisé et sur mesure. Le basculement peut être effectué sous forme de basculement planifié ou de basculement en un clic lorsqu'un sinistre survient et qu'une décision est prise d'activer le site DR.

Pour en savoir plus sur ce processus, n'hésitez pas à suivre la vidéo détaillée ou à utiliser le"simulateur de solutions" .

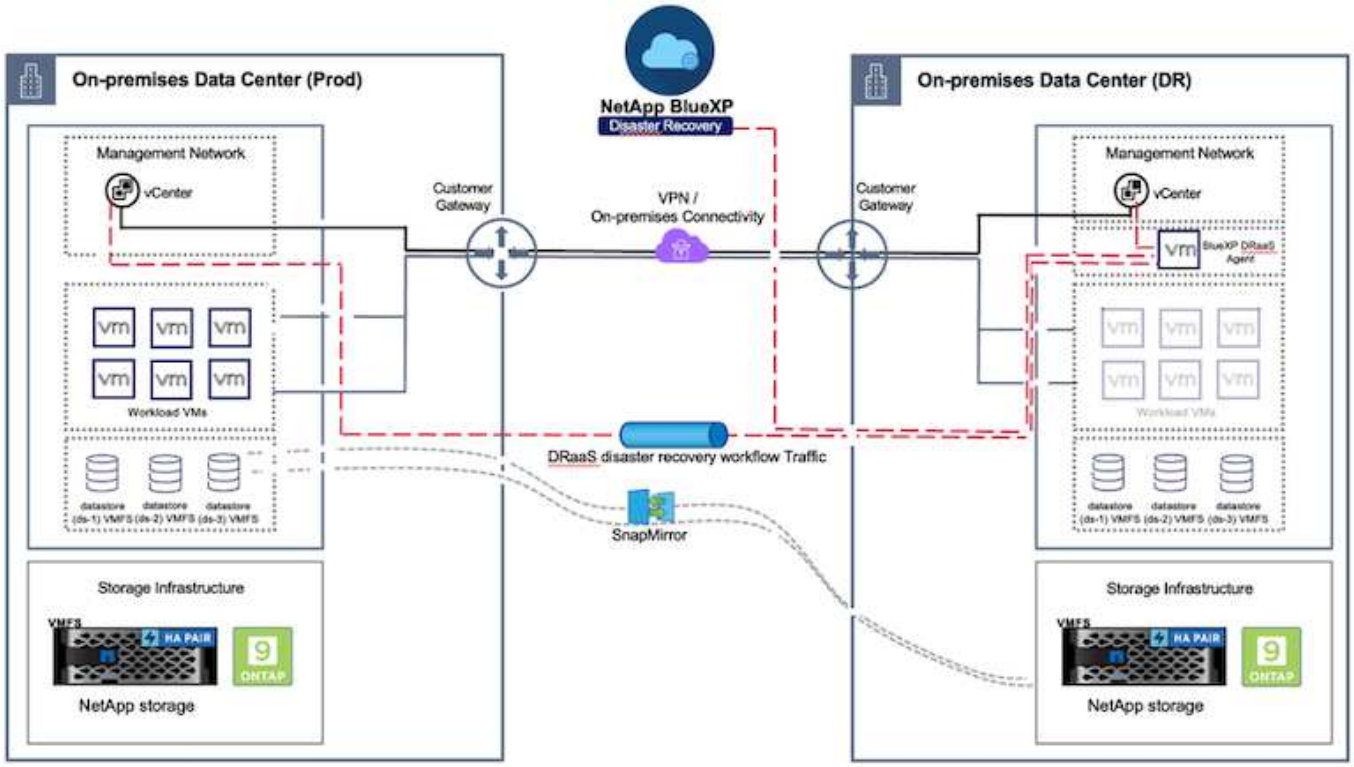
NetApp Disaster Recovery pour les datastores VMFS

La reprise après sinistre utilisant la réplication au niveau des blocs du site de production vers le site de reprise après sinistre est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données, comme les attaques de ransomware. Avec la réplication NetApp SnapMirror , les charges de travail VMware exécutant des systèmes ONTAP sur site utilisant une banque de données VMFS peuvent être répliquées vers un autre système de stockage ONTAP dans un centre de données de récupération désigné où réside VMware.

Cette section du document décrit la configuration de NetApp Disaster Recovery pour configurer la reprise après sinistre des machines virtuelles VMware sur site vers un autre site désigné. Dans le cadre de cette configuration, il s'agit de l'agent Console, de l'intégration des baies ONTAP, de la définition des sites et de l'association de VMware vCenter. En outre, ce document décrit en détail comment configurer la réplication entre les sites et comment mettre en place et tester un plan de reprise. La dernière section fournit des instructions pour effectuer un basculement complet du site et pour revenir en arrière lorsque le site principal est rétabli et remis en ligne.

En utilisant Disaster Recovery, qui fait partie de NetApp Data Services, les clients peuvent découvrir leurs vCenters VMware sur site ainsi que le stockage ONTAP, créer des groupes de ressources, créer un plan de reprise après sinistre, l'associer à des groupes de ressources, et tester ou exécuter le basculement et le rétablissement. SnapMirror fournit une réplication des blocs au niveau du stockage pour maintenir les deux sites à jour avec les modifications incrémentielles, ce qui permet d'obtenir un RPO pouvant atteindre 5 minutes. Il est également possible de simuler les procédures de DR comme exercice régulier sans affecter les

datastores de production et répliqués ni entraîner de coûts de stockage supplémentaires. NetApp Data Services tire parti de la technologie FlexClone d'ONTAP pour créer une copie à faible encombrement du datastore VMFS à partir du dernier Snapshot répliqué sur le site de DR. Une fois le test de DR terminé, les clients peuvent simplement supprimer l'environnement de test, là encore sans aucun impact sur les ressources de production répliquées réelles. Lorsqu'un basculement réel est nécessaire (planifié ou non), en quelques clics, Disaster Recovery orchestrera toutes les étapes nécessaires pour démarrer automatiquement les machines virtuelles protégées sur le site de reprise après sinistre désigné. Le service inversera également la relation SnapMirror vers le site principal et répliquera, si nécessaire, toute modification du site secondaire vers le site principal pour une opération de rétablissement. Tout cela peut être réalisé pour une fraction du coût par rapport à d'autres alternatives bien connues.

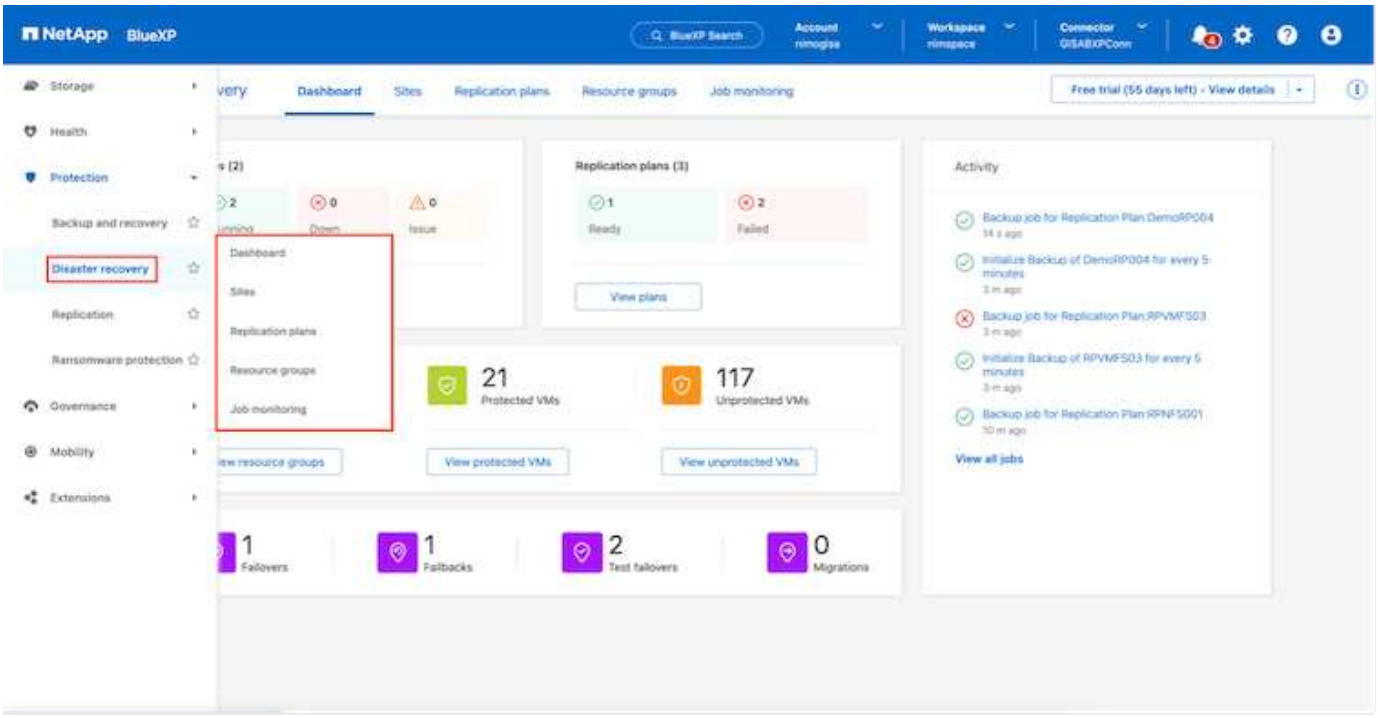


Pour obtenir des informations à jour et les versions prises en charge de vCenter Server, ESXi et ONTAP pour la reprise après sinistre, veuillez vous référer à "Configurations prises en charge pour la reprise après sinistre".

Commencer

Pour commencer avec Disaster Recovery, utilisez NetApp Console, puis accédez au service.

1. Connectez-vous à Console.
2. Dans le volet de navigation de gauche de Console, sélectionnez Protection > Reprise après sinistre.
3. Le Disaster Recovery Dashboard s'affiche.

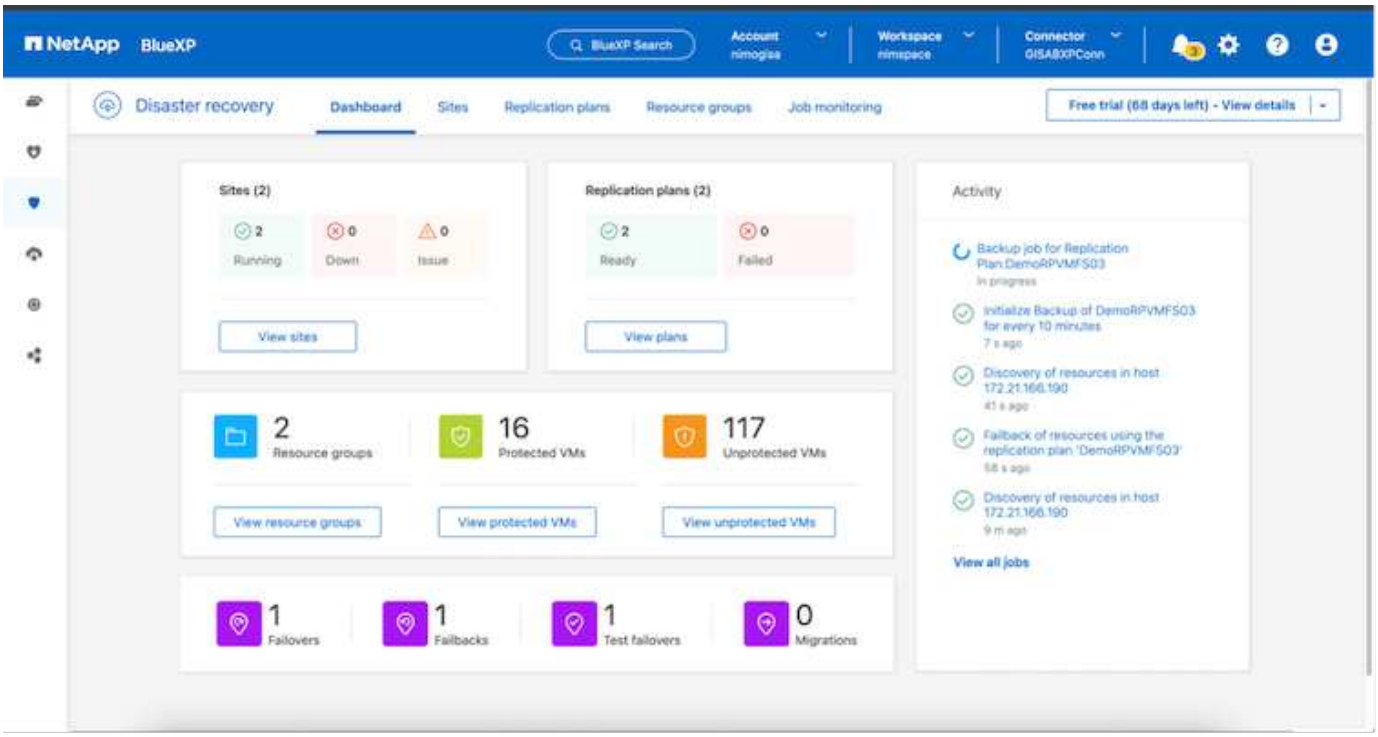


Avant de configurer le plan de reprise après sinistre, assurez-vous que les conditions préalables suivantes sont remplies :

- L'agent Console est déployé dans un VPC AWS.
- L'instance de l'agent Console dispose d'une connectivité aux systèmes vCenter source et de destination, ainsi qu'aux systèmes de stockage.
- Les systèmes de stockage NetApp sur site hébergeant des banques de données VMFS pour VMware sont ajoutés dans Console.
- La résolution DNS doit être en place lors de l'utilisation de noms DNS. Sinon, utilisez les adresses IP pour le vCenter.
- La réplication SnapMirror est configurée pour les volumes de banque de données basés sur VMFS désignés.

Une fois la connectivité établie entre les sites source et de destination, procédez aux étapes de configuration, qui devraient prendre environ 3 à 5 minutes.

NetApp recommande de déployer l'agent Console sur le site de reprise après sinistre ou sur un site tiers, afin que l'agent Console puisse communiquer via le réseau avec les ressources source et de destination lors de pannes réelles ou de catastrophes naturelles.

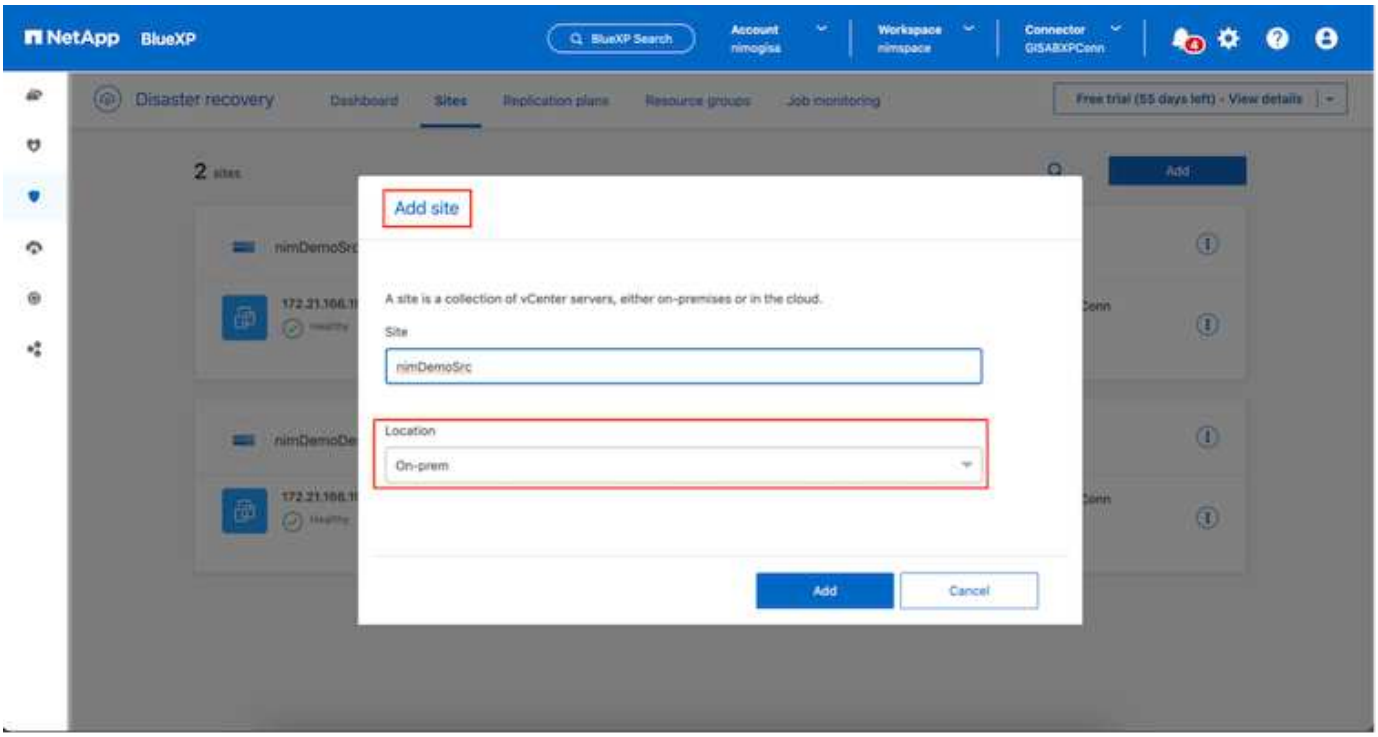


La prise en charge des banques de données VMFS sur site vers sur site est en version préliminaire technologique lors de la rédaction de ce document. Cette fonctionnalité est prise en charge avec les banques de données VMFS basées sur les protocoles FC et ISCSI.

Configuration de reprise après sinistre

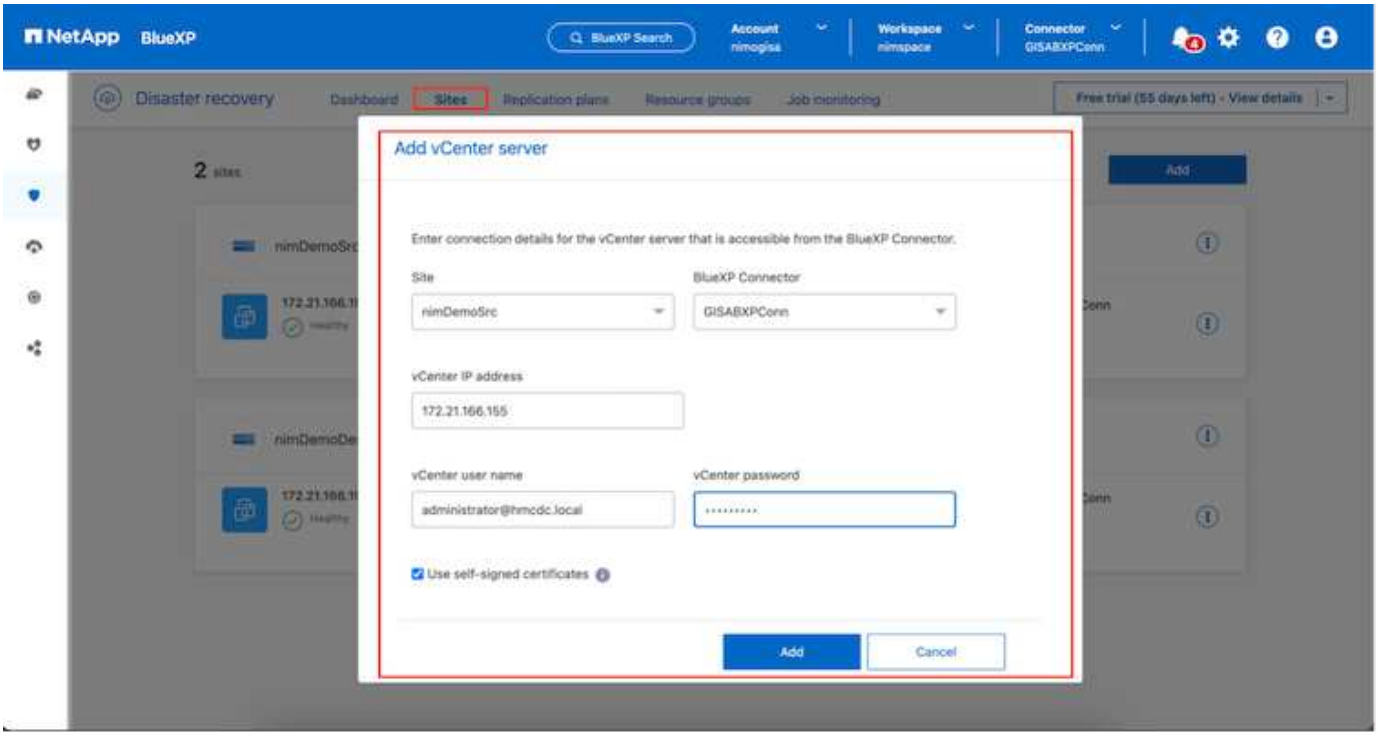
La première étape de la préparation à la reprise après sinistre consiste à découvrir et à ajouter les ressources vCenter et de stockage sur site à Disaster Recovery.

Assurez-vous que les systèmes de stockage ONTAP sont ajoutés à l'environnement de travail dans le canevas. Ouvrez Console et sélectionnez **Protection > Disaster Recovery** dans le volet de navigation de gauche. Sélectionnez **Découvrir les serveurs vCenter** ou utilisez le menu supérieur, puis sélectionnez **Sites > Add > Add vCenter**.

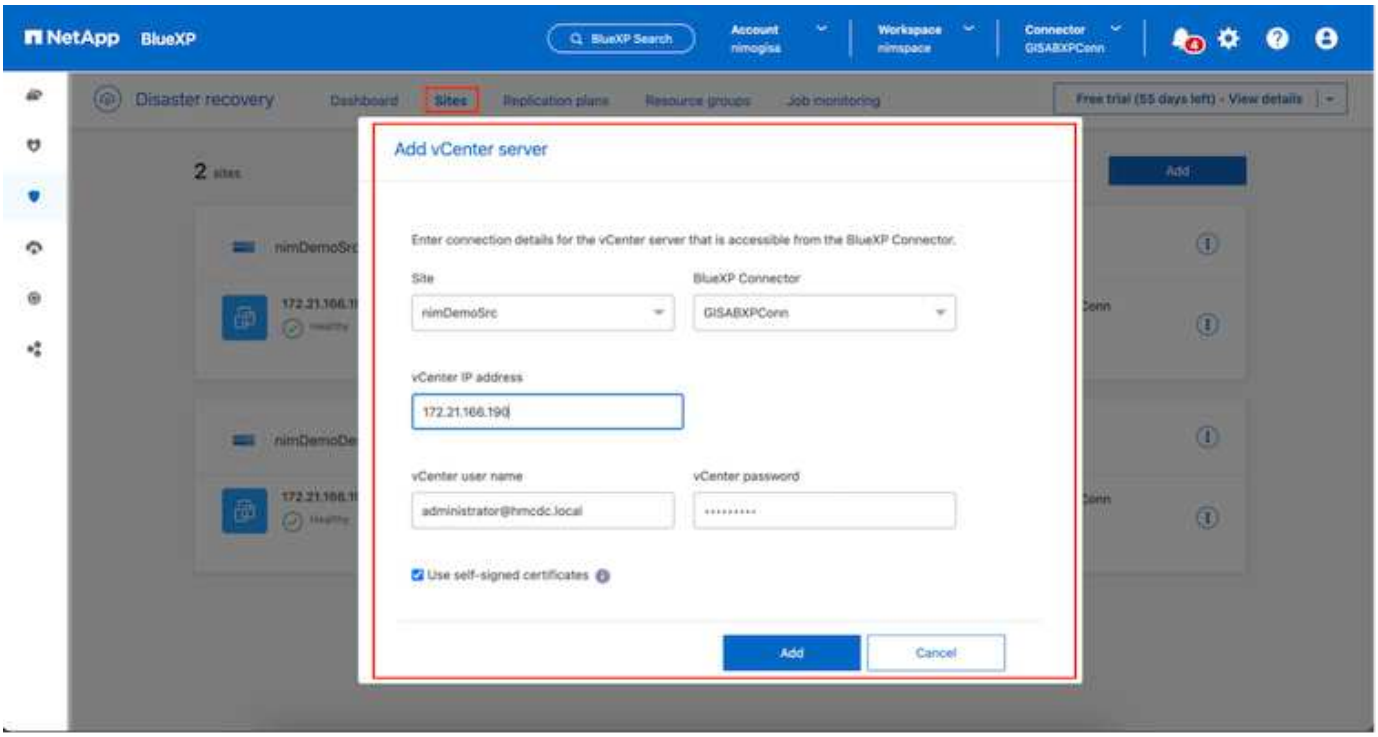


Ajoutez les plateformes suivantes :

- **Source**. vCenter sur site.



- **Destination**. VMC SDDC vCenter.



Une fois les vCenters ajoutés, la découverte automatisée est déclenchée.

Configuration de la réplication de stockage entre le site source et le site de destination

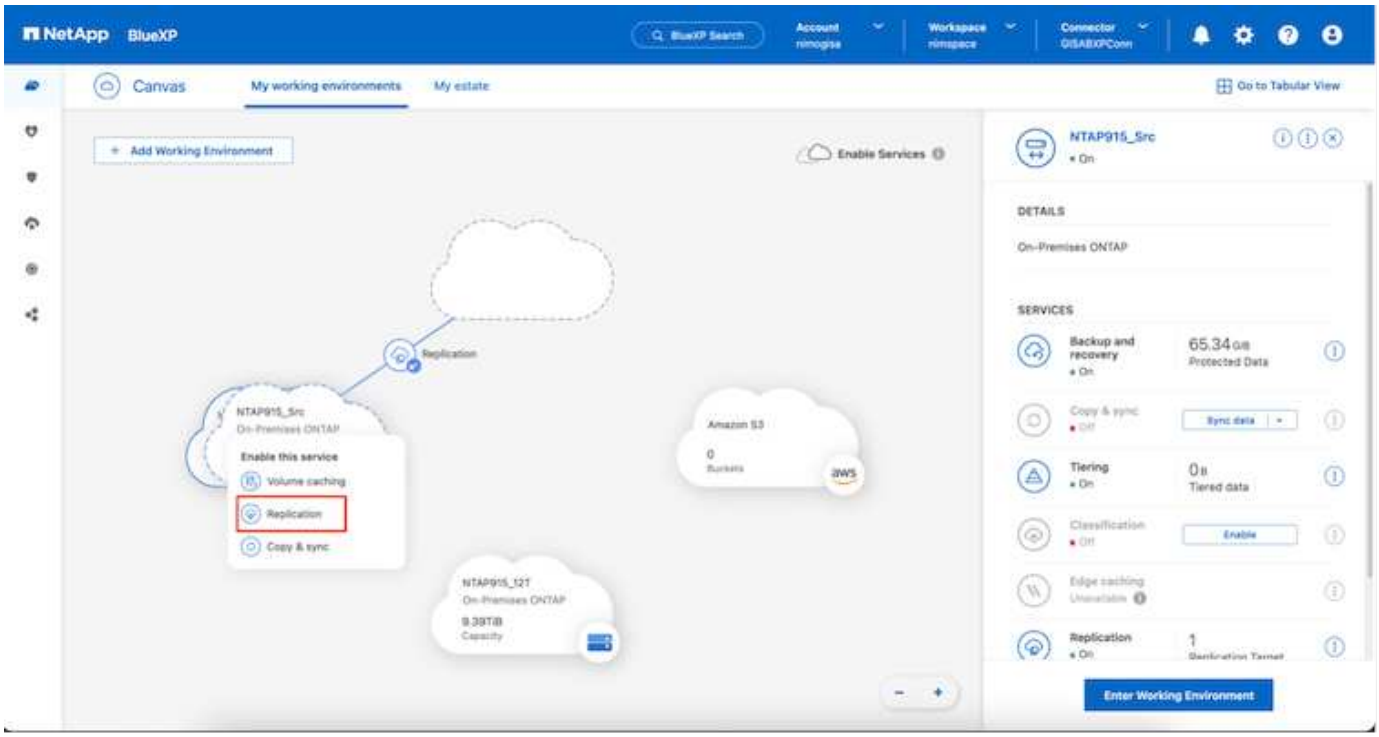
SnapMirror utilise des instantanés ONTAP pour gérer le transfert de données d'un emplacement à un autre. Initialement, une copie complète basée sur un instantané du volume source est copiée vers la destination pour effectuer une synchronisation de base. À mesure que des modifications de données se produisent à la source, un nouvel instantané est créé et comparé à l'instantané de base. Les blocs qui ont changé sont ensuite répliqués vers la destination, le nouvel instantané devenant la ligne de base actuelle ou le dernier instantané commun. Cela permet de répéter le processus et d'envoyer des mises à jour incrémentielles à la destination.

Lorsqu'une relation SnapMirror a été établie, le volume de destination est dans un état de lecture seule en ligne et est donc toujours accessible. SnapMirror fonctionne avec des blocs de stockage physiques, plutôt qu'à un fichier ou à un autre niveau logique. Cela signifie que le volume de destination est une réplique identique de la source, y compris les instantanés, les paramètres de volume, etc. Si les fonctionnalités d'efficacité de l'espace ONTAP , telles que la compression et la déduplication des données, sont utilisées par le volume source, le volume répliqué conservera ces optimisations.

La rupture de la relation SnapMirror rend le volume de destination accessible en écriture et serait généralement utilisé pour effectuer un basculement lorsque SnapMirror est utilisé pour synchroniser les données avec un environnement DR. SnapMirror est suffisamment sophistiqué pour permettre aux données modifiées sur le site de basculement d'être efficacement resynchronisées vers le système principal, s'il revient en ligne ultérieurement, puis de rétablir la relation SnapMirror d'origine.

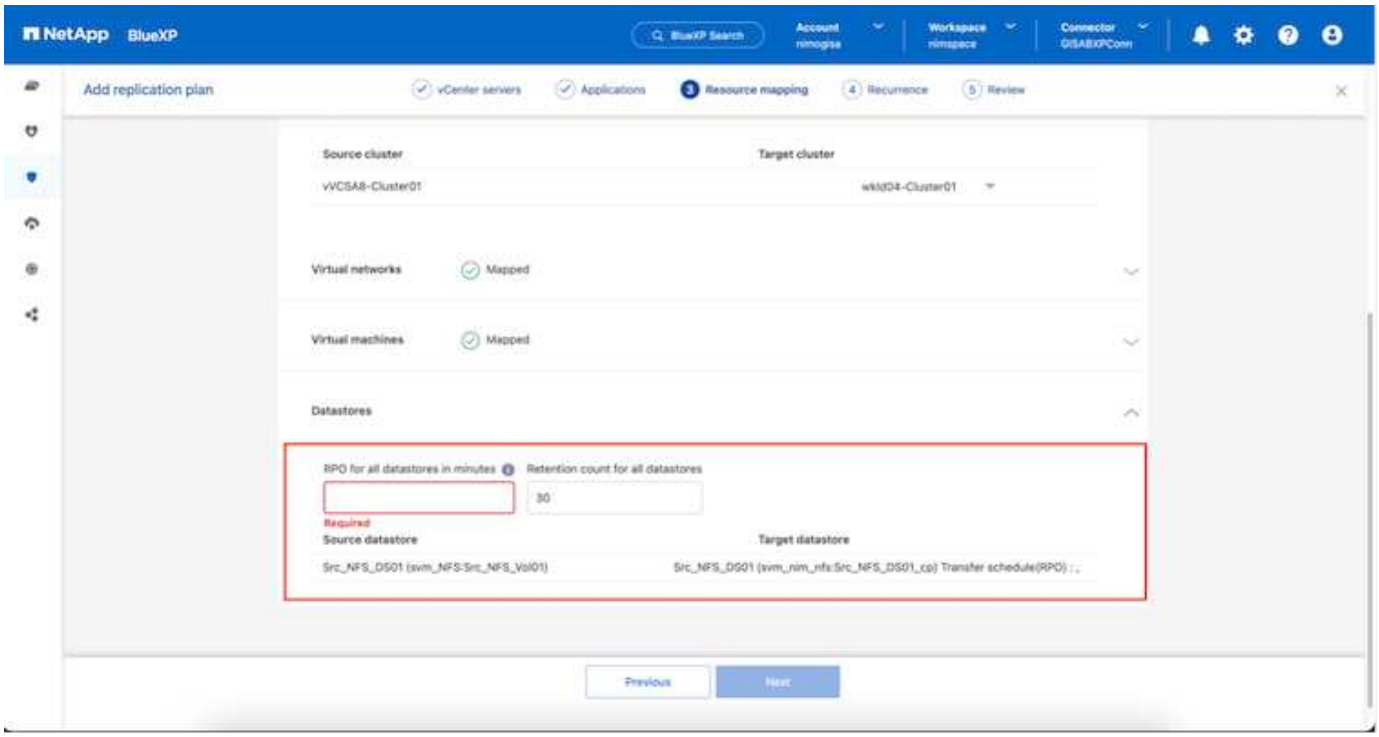
Comment le configurer pour la récupération après sinistre VMware

Le processus de création de la réplication SnapMirror reste le même pour toute application donnée. Le processus peut être manuel ou automatisé. Le moyen le plus simple consiste à utiliser Console pour configurer la réplication SnapMirror en faisant simplement glisser-déposer le système ONTAP source de l'environnement vers la destination afin de lancer l'assistant qui vous guidera pour le reste du processus.



NetApp Data Services peut également automatiser ce processus à condition que les deux critères suivants soient remplis :

- Les clusters source et de destination ont une relation d'homologue.
- La SVM source et la SVM de destination ont une relation homologue.

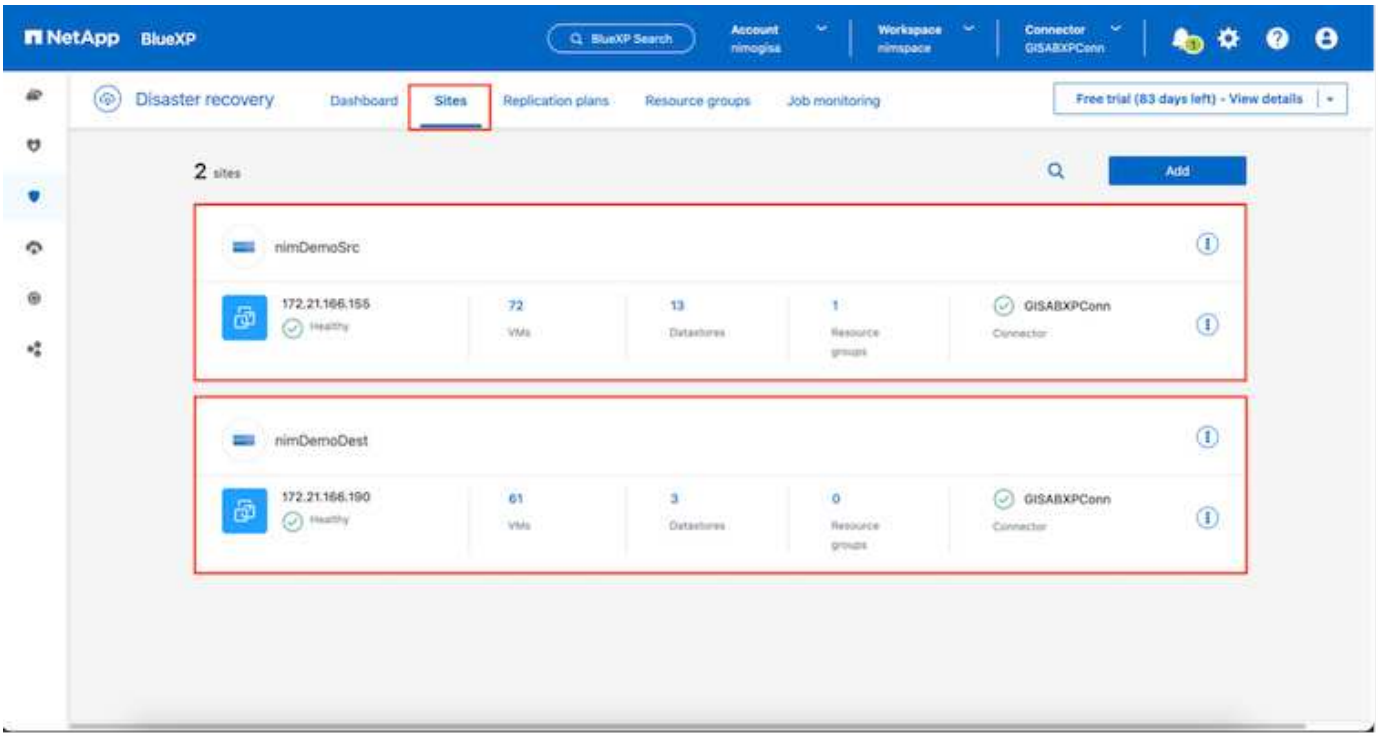


Si une relation SnapMirror est déjà configurée pour le volume via l'interface de ligne de commande (CLI), Console détecte la relation et poursuit le reste des opérations du flux de travail.

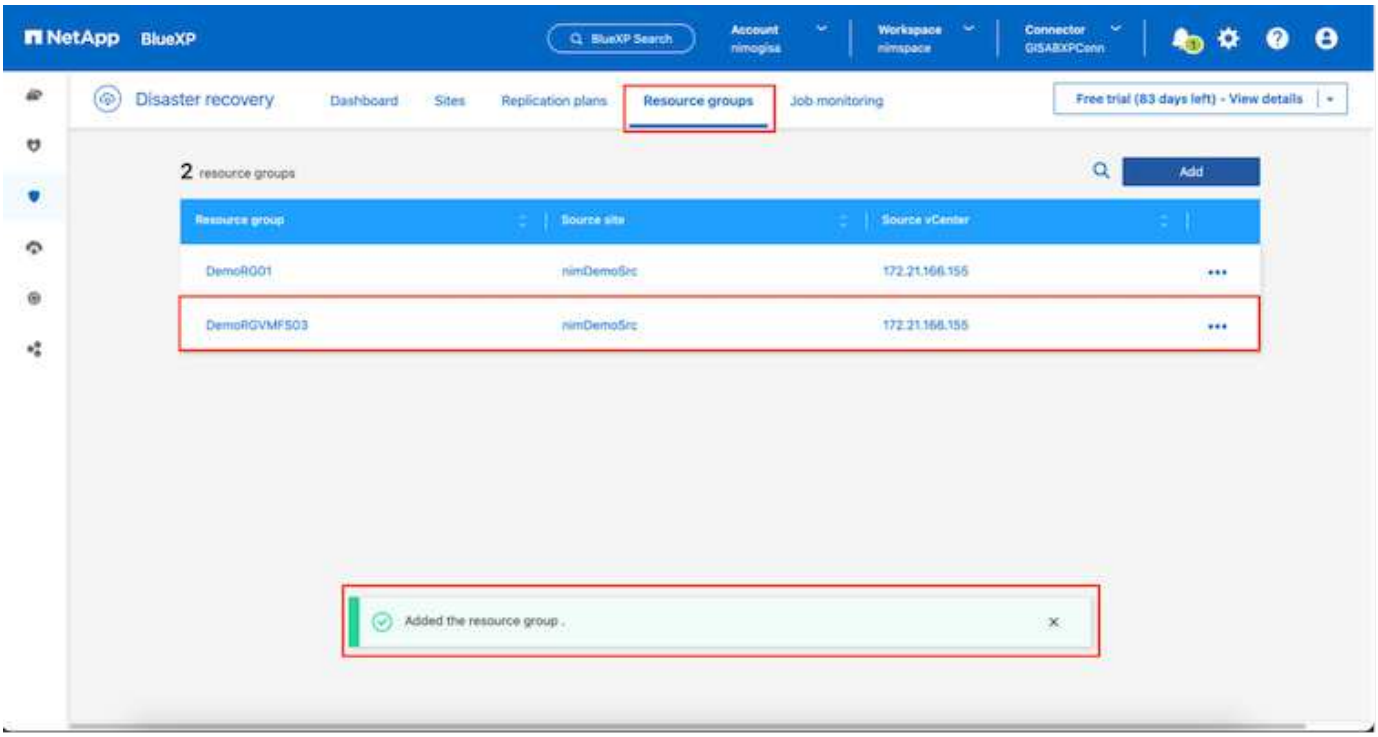
Outre les méthodes mentionnées ci-dessus, la réplication SnapMirror peut également être créée via l'interface de ligne de commande ONTAP ou System Manager. Quelle que soit la méthode utilisée pour synchroniser les données à l'aide de SnapMirror, Disaster Recovery orchestre le flux de travail pour des opérations de reprise après sinistre fluides et efficaces.

Que peut faire Disaster Recovery pour vous?

Une fois les sites source et de destination ajoutés, Disaster Recovery effectue une analyse approfondie automatique et affiche les machines virtuelles ainsi que leurs métadonnées associées. Disaster Recovery détecte et renseigne également automatiquement les réseaux et les groupes de ports utilisés par les machines virtuelles.

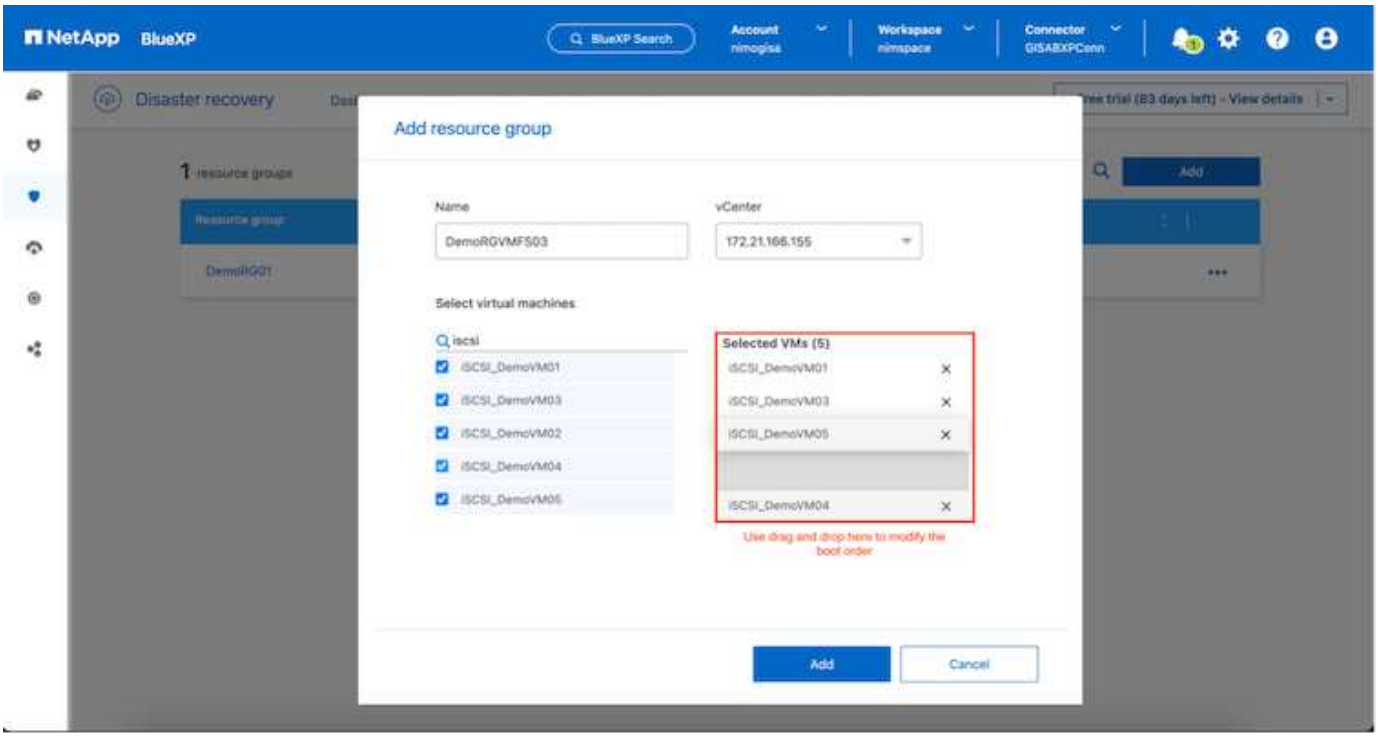


Une fois les sites ajoutés, les machines virtuelles peuvent être regroupées en groupes de ressources. Les groupes de ressources de reprise après sinistre vous permettent de regrouper un ensemble de machines virtuelles dépendantes en groupes logiques qui incluent leur ordre de démarrage et leurs délais de démarrage à appliquer lors de la reprise. Pour commencer à créer des groupes de ressources, accédez à **Groupes de ressources** et cliquez sur **Créer un groupe de ressources**.

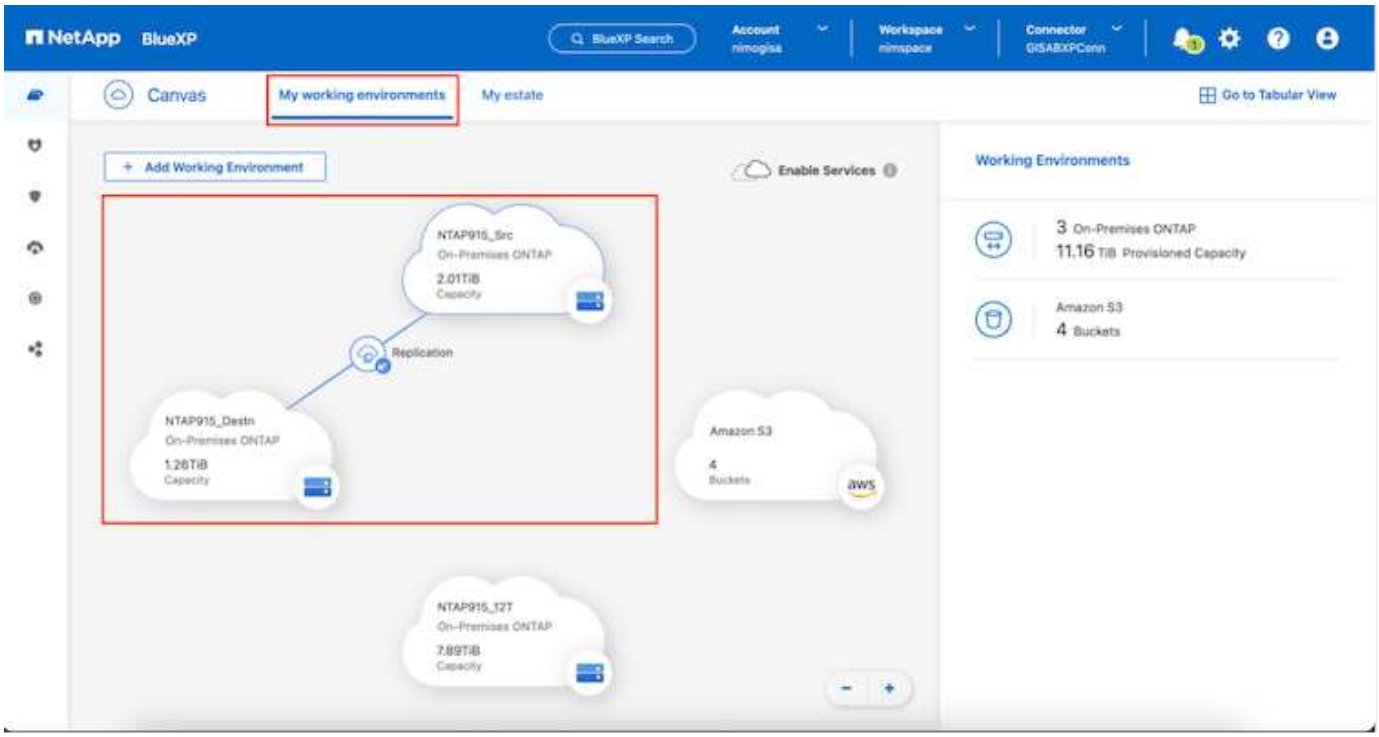


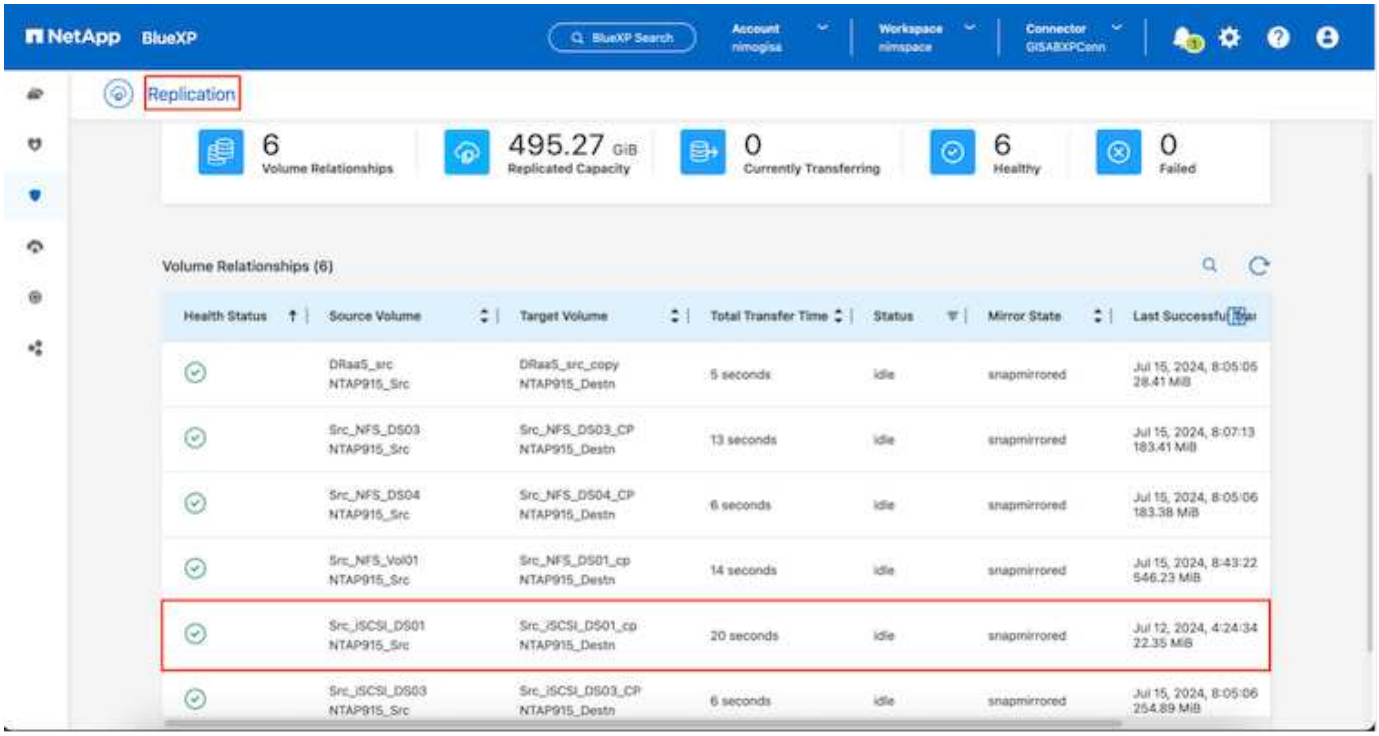
Le groupe de ressources peut également être créé lors de la création d'un plan de réplication.

L'ordre de démarrage des machines virtuelles peut être défini ou modifié lors de la création de groupes de ressources en utilisant un simple mécanisme de glisser-déposer.



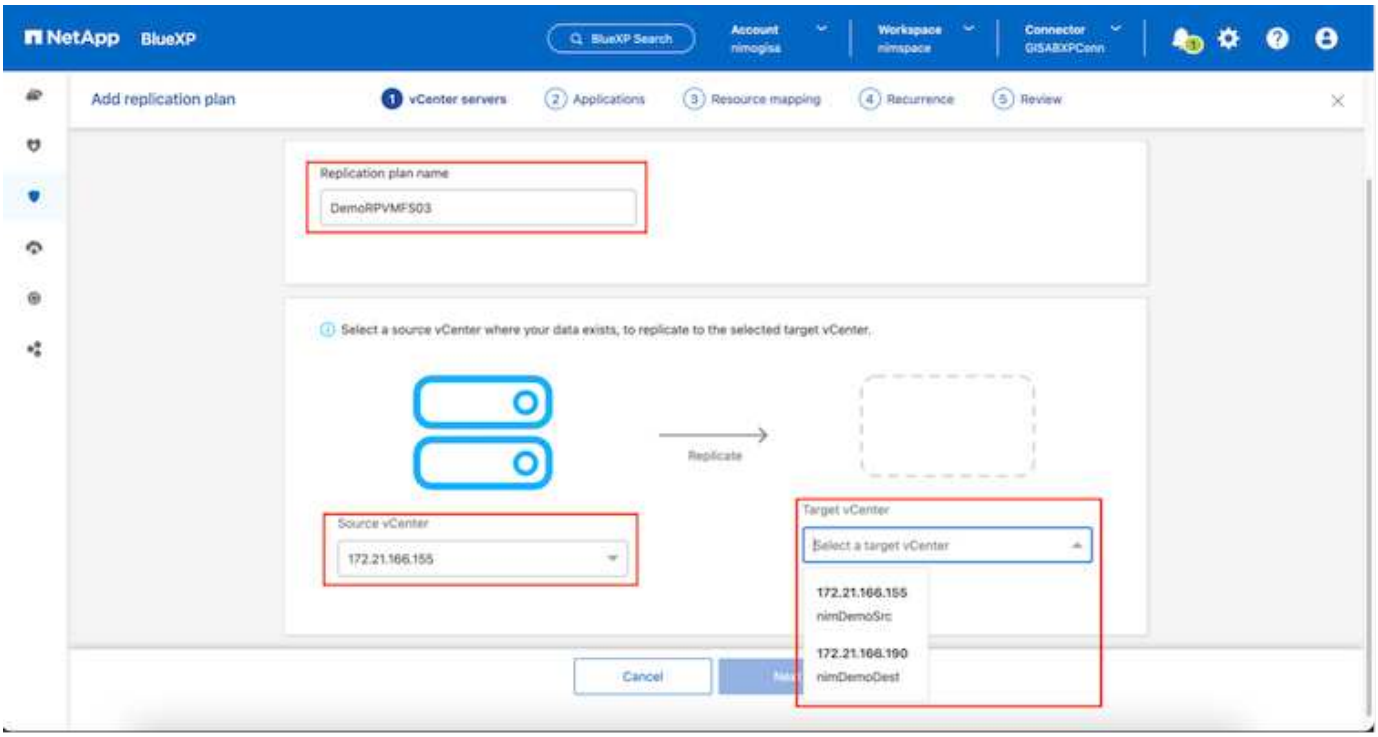
Une fois les groupes de ressources créés, l'étape suivante consiste à créer le plan d'exécution ou un plan de récupération des machines virtuelles et des applications en cas de sinistre. Comme mentionné dans les conditions préalables, la réplication SnapMirror peut être configurée au préalable ou DRaaS peut la configurer à l'aide du RPO et du nombre de rétention spécifiés lors de la création du plan de réplication.



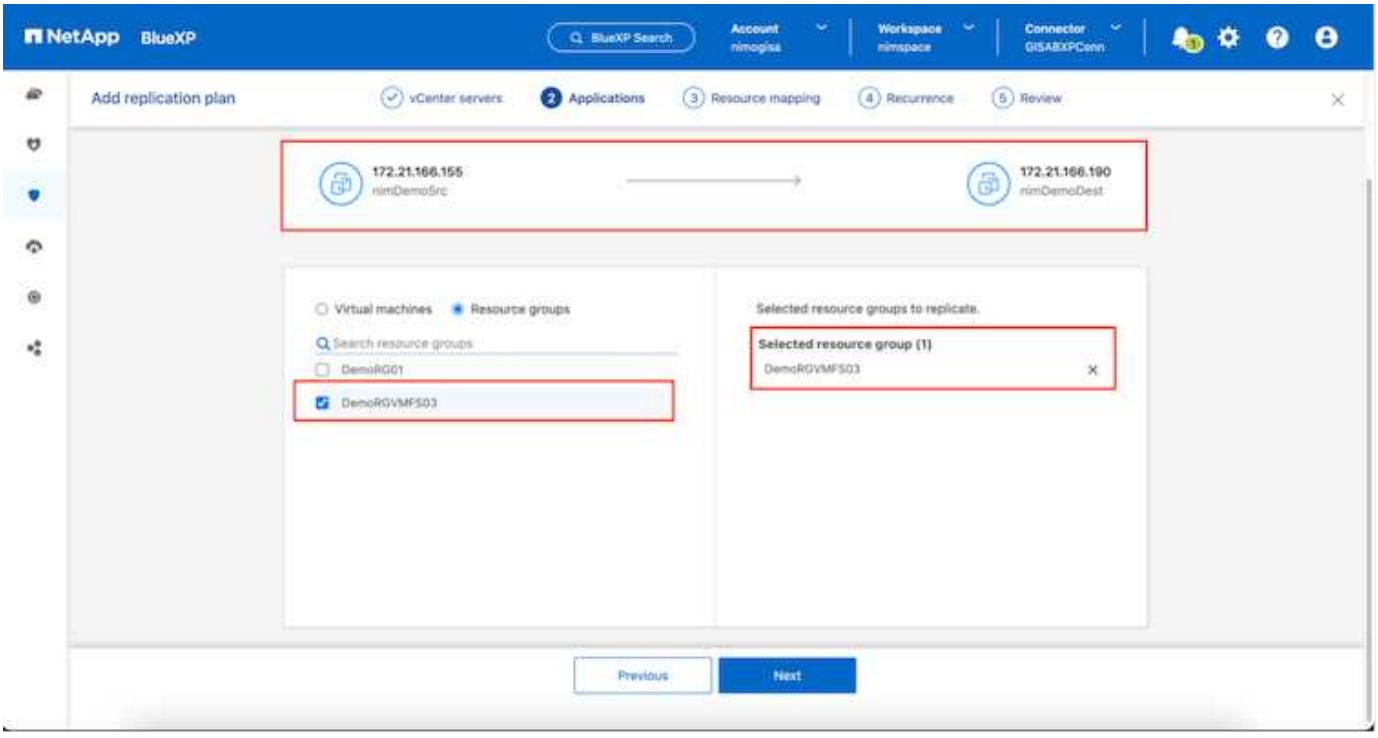


Configurez le plan de réplication en sélectionnant les plates-formes vCenter source et de destination dans la liste déroulante et choisissez les groupes de ressources à inclure dans le plan, ainsi que le regroupement de la manière dont les applications doivent être restaurées et mises sous tension et le mappage des clusters et des réseaux. Pour définir le plan de récupération, accédez à l'onglet **Plan de réplication** et cliquez sur **Ajouter un plan**.

Tout d'abord, sélectionnez le vCenter source, puis sélectionnez le vCenter de destination.



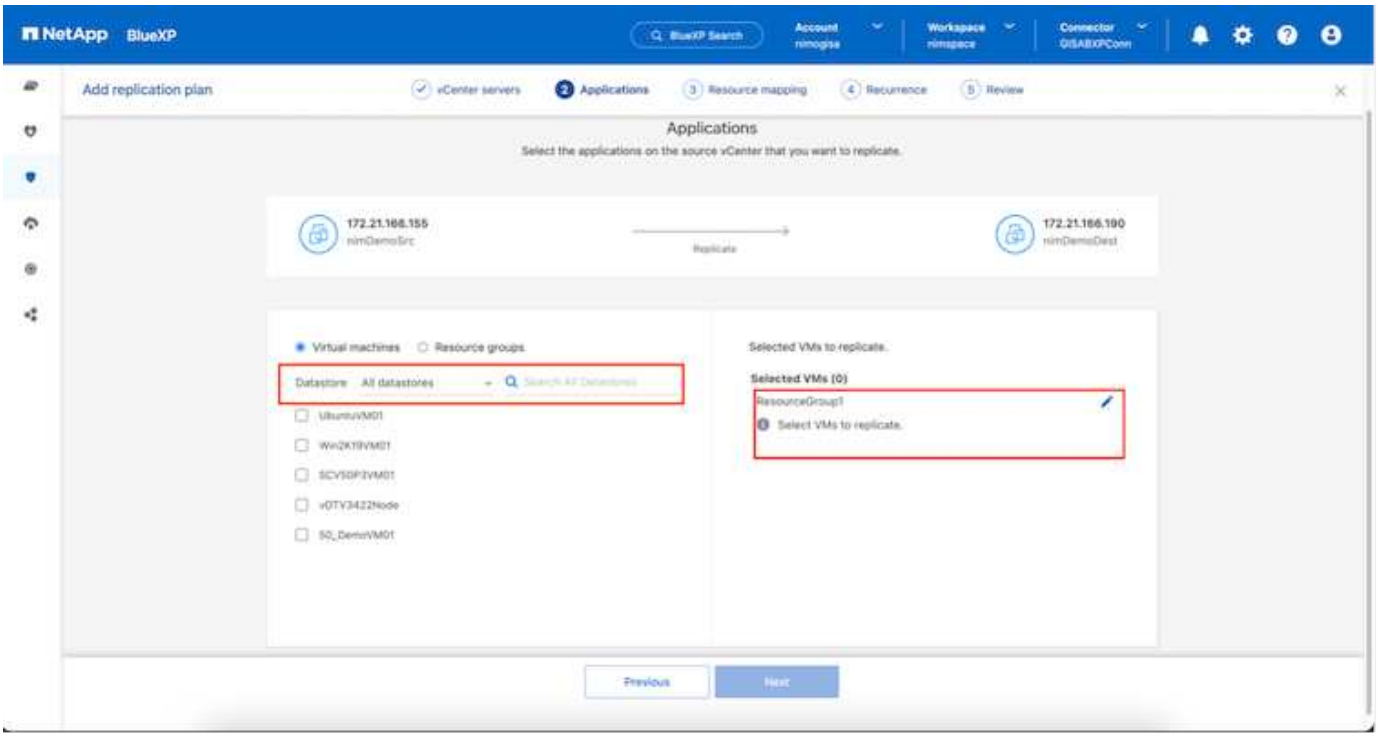
L'étape suivante consiste à sélectionner les groupes de ressources existants. Si aucun groupe de ressources n'est créé, l'assistant permet de regrouper les machines virtuelles requises (en créant essentiellement des groupes de ressources fonctionnels) en fonction des objectifs de récupération. Cela permet également de définir la séquence d'opérations selon laquelle les machines virtuelles d'application doivent être restaurées.



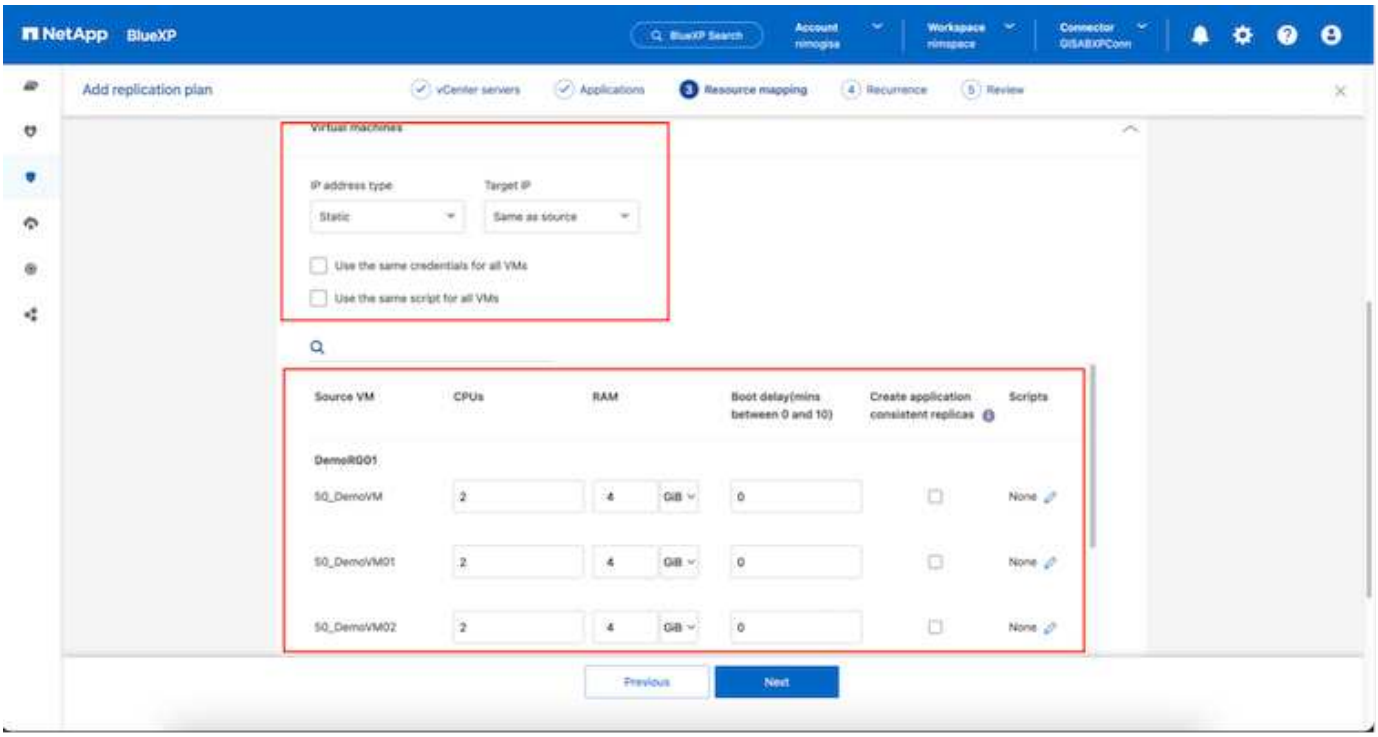
Le groupe de ressources permet de définir l'ordre de démarrage à l'aide de la fonctionnalité glisser-déposer. Il peut être utilisé pour modifier facilement l'ordre dans lequel les machines virtuelles seront mises sous tension pendant le processus de récupération.

Chaque machine virtuelle au sein d'un groupe de ressources est démarrée en séquence en fonction de l'ordre. Deux groupes de ressources sont démarrés en parallèle.

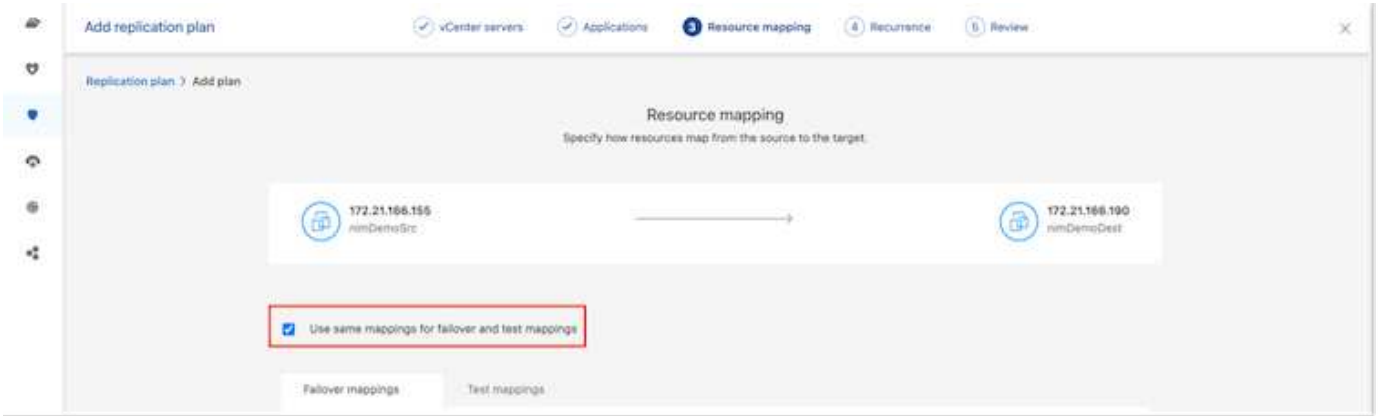
La capture d'écran ci-dessous montre l'option permettant de filtrer les machines virtuelles ou les banques de données spécifiques en fonction des exigences organisationnelles si les groupes de ressources ne sont pas créés au préalable.



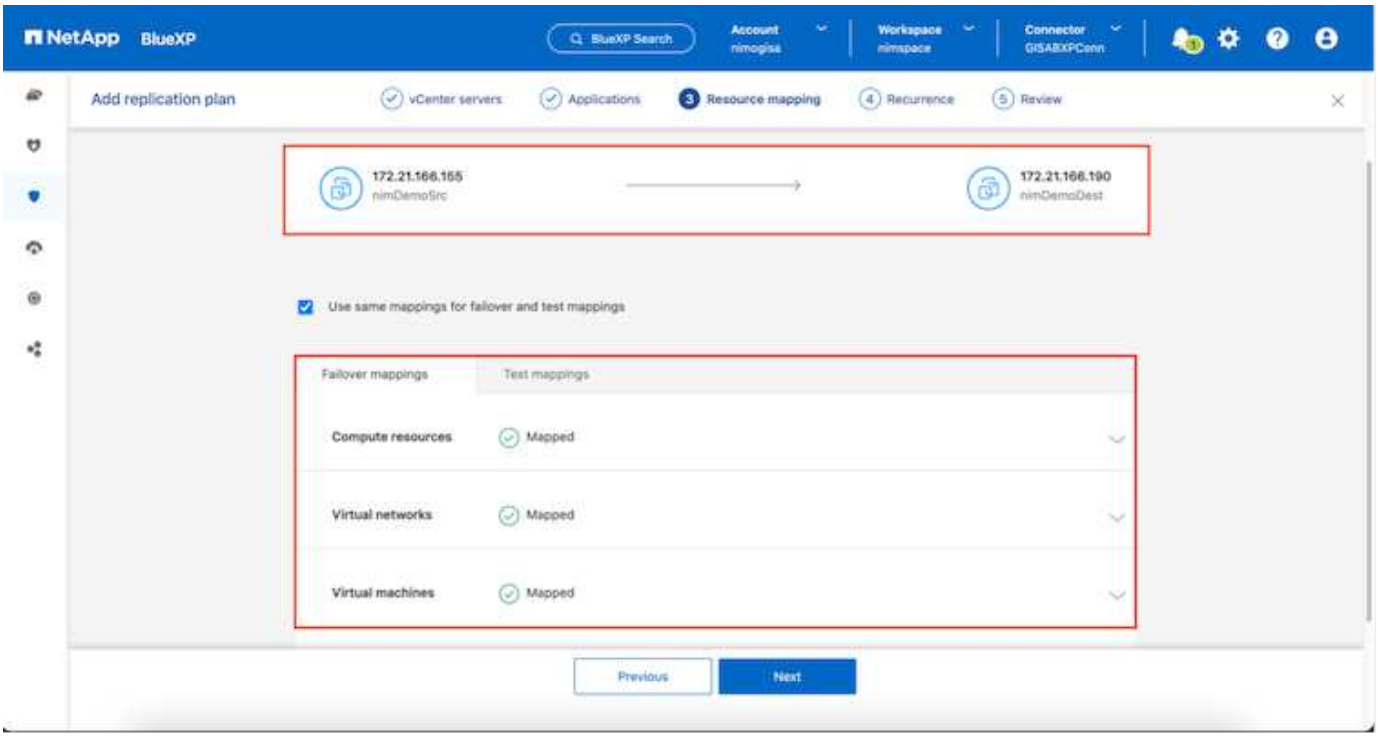
Une fois les groupes de ressources sélectionnés, créez les mappages de basculement. À cette étape, indiquez comment les ressources de l'environnement source sont mappées vers la destination. Cela inclut les ressources de calcul et les réseaux virtuels, la personnalisation des adresses IP, les scripts de pré- et post-traitement, les délais de démarrage, la cohérence des applications, etc. Pour plus d'informations, consultez "Créer un plan de réplication".



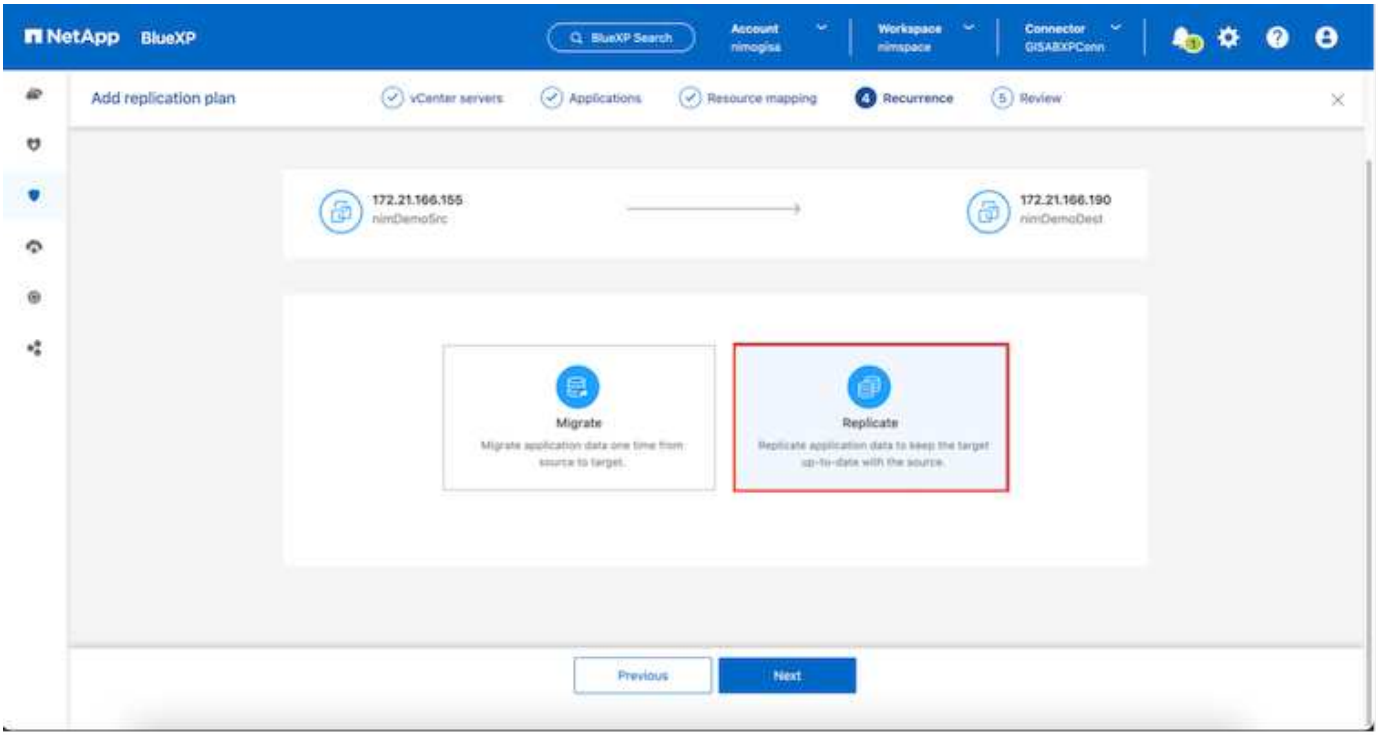
Par défaut, les mêmes paramètres de mappage sont utilisés pour les opérations de test et de basculement. Pour appliquer différents mappages pour l'environnement de test, sélectionnez l'option Mappage de test après avoir décoché la case comme indiqué ci-dessous :



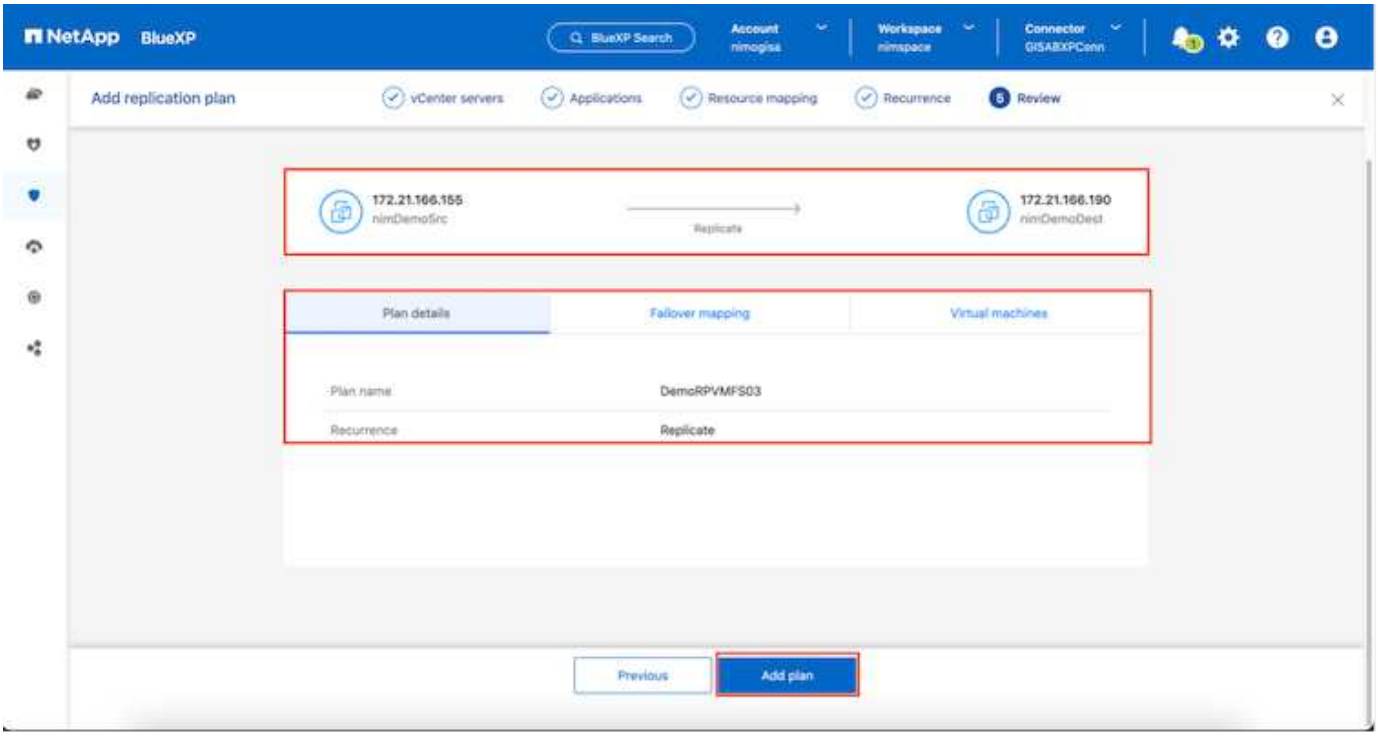
Une fois le mappage des ressources terminé, cliquez sur Suivant.

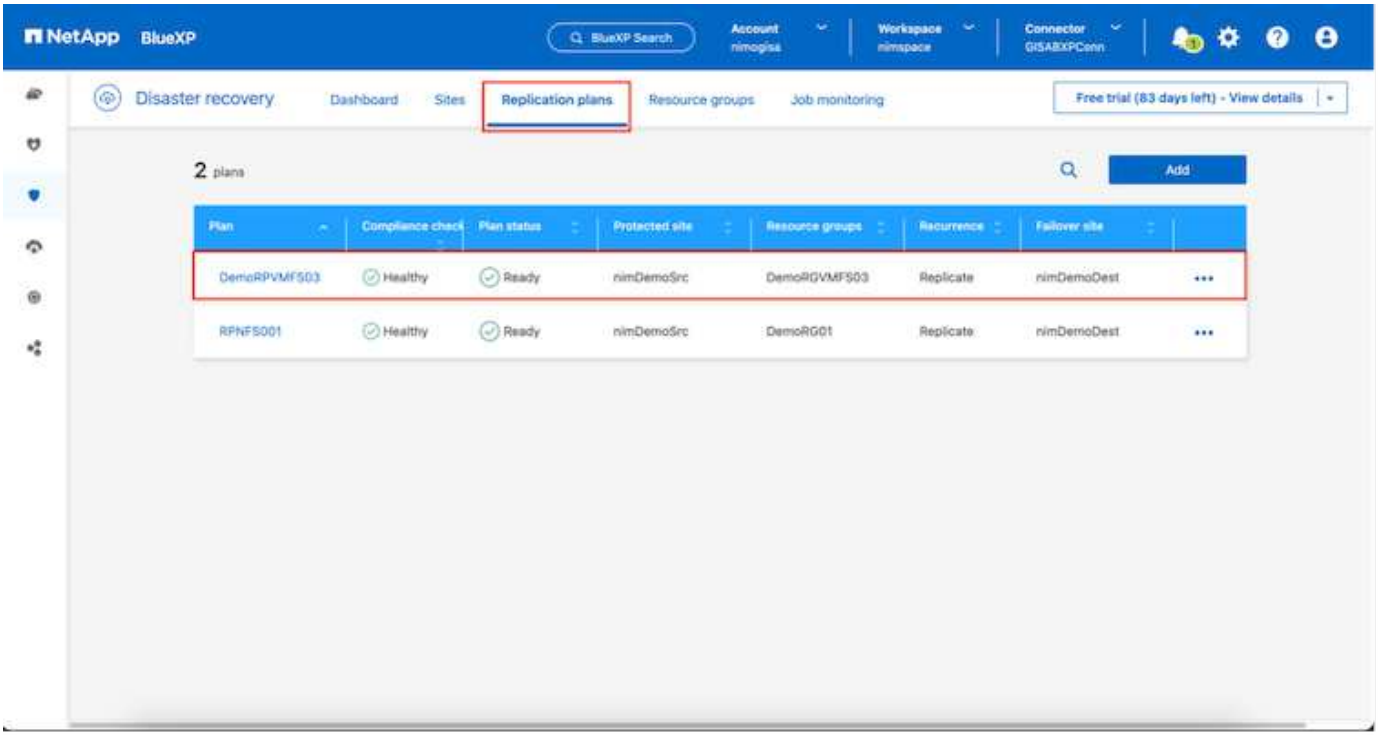


Sélectionnez le type de récurrence. En termes simples, sélectionnez l'option Migrer (migration unique utilisant le basculement) ou la réplication continue récurrente. Dans cette procédure pas à pas, l'option Répliquer est sélectionnée.

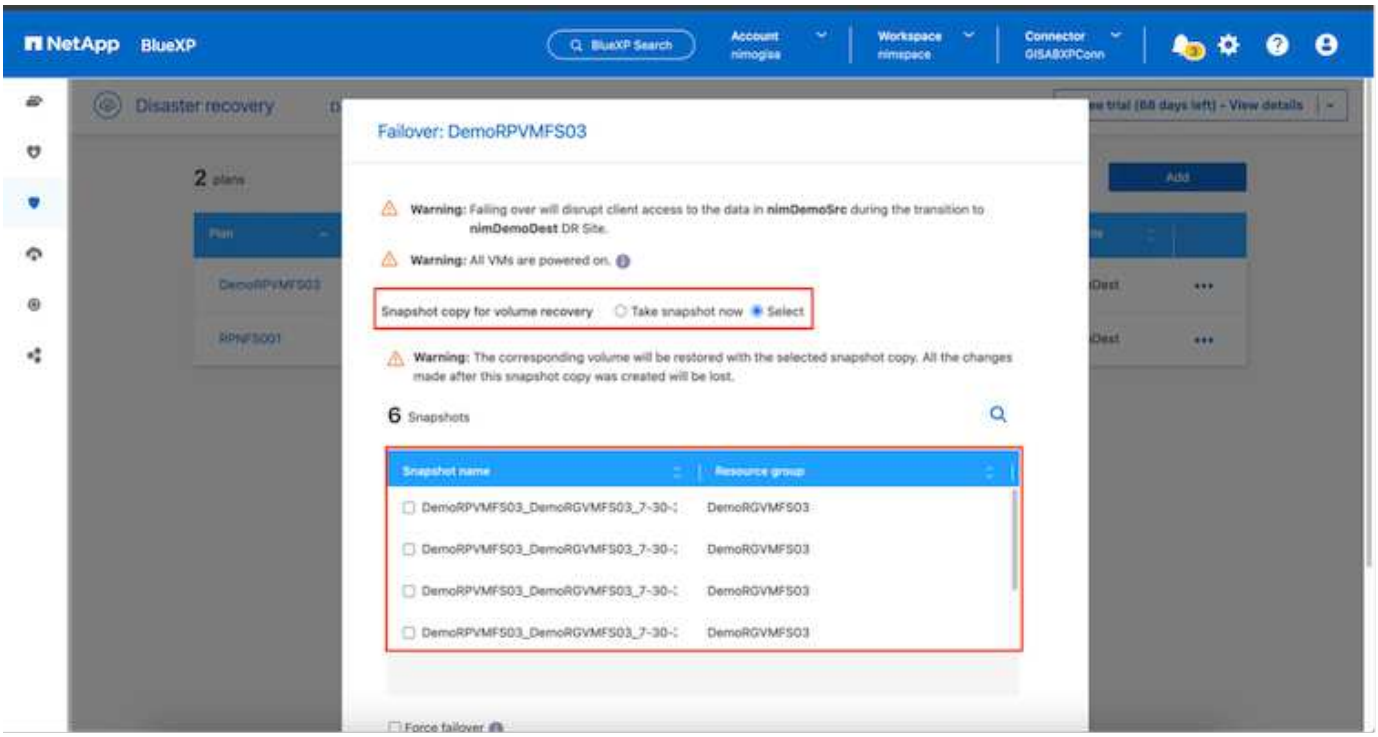


Une fois terminé, vérifiez les mappages créés, puis cliquez sur Ajouter un plan.

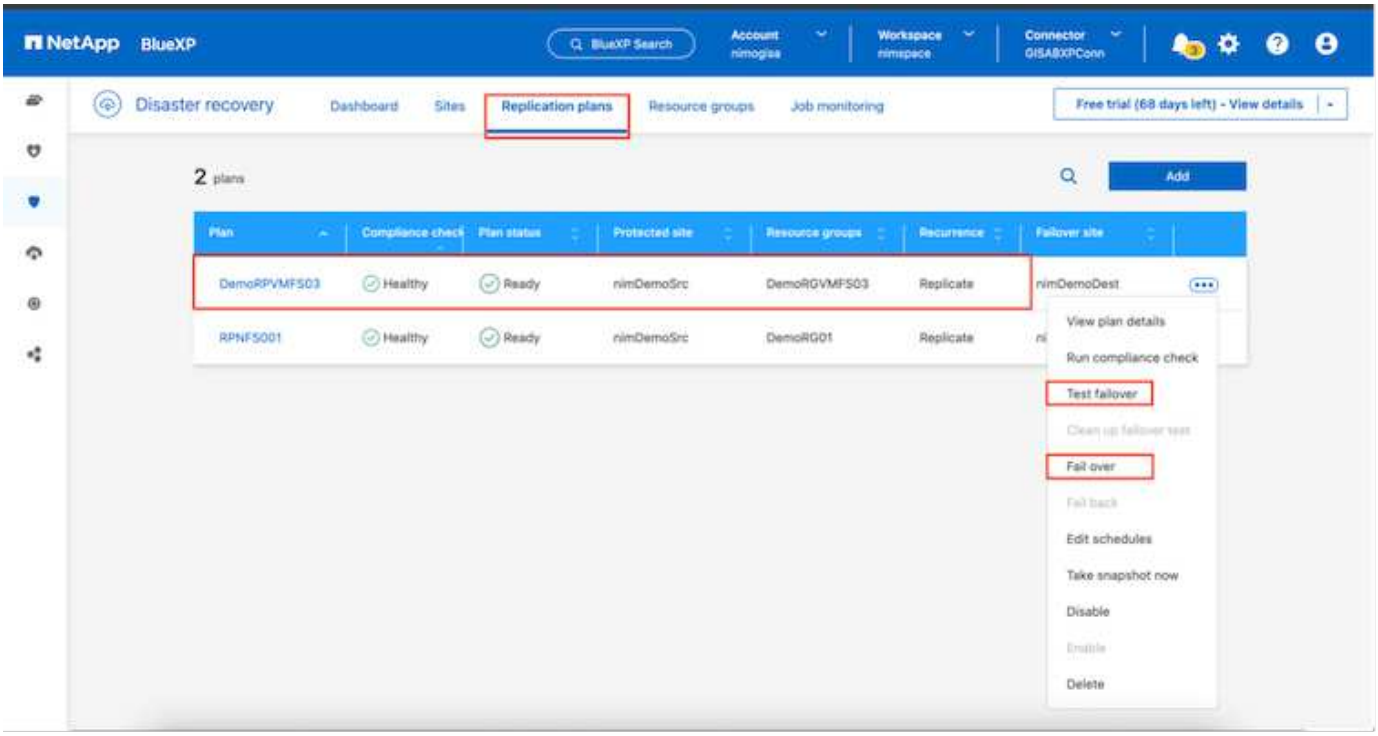




Une fois le plan de réplication créé, le basculement peut être effectué selon les besoins en sélectionnant l'option de basculement, l'option de test de basculement ou l'option de migration. Disaster Recovery garantit que le processus de réplication est exécuté conformément au plan toutes les 30 minutes. Lors des options de basculement et de test de basculement, vous pouvez utiliser la copie Snapshot SnapMirror la plus récente, ou vous pouvez sélectionner une copie Snapshot spécifique à un instant donné (conformément à la politique de conservation de SnapMirror). L'option à un instant donné peut s'avérer très utile en cas de corruption des données, comme lors d'une attaque par ransomware, lorsque les réplicas les plus récents sont déjà compromis ou chiffrés. Disaster Recovery affiche tous les points de récupération disponibles.



Pour déclencher un basculement ou un test de basculement avec la configuration spécifiée dans le plan de réplication, cliquez sur **Basculement** ou **Tester le basculement**.

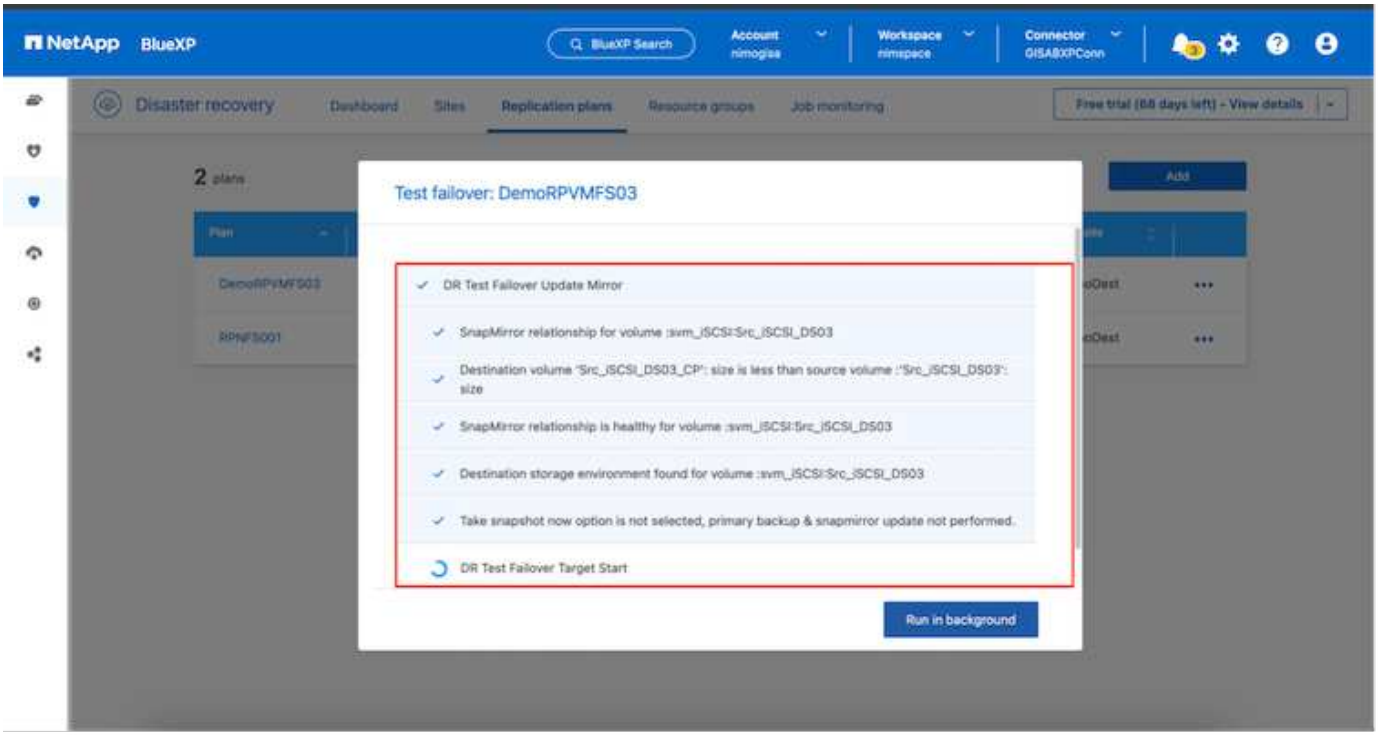


Que se passe-t-il lors d'une opération de basculement ou de test de basculement ?

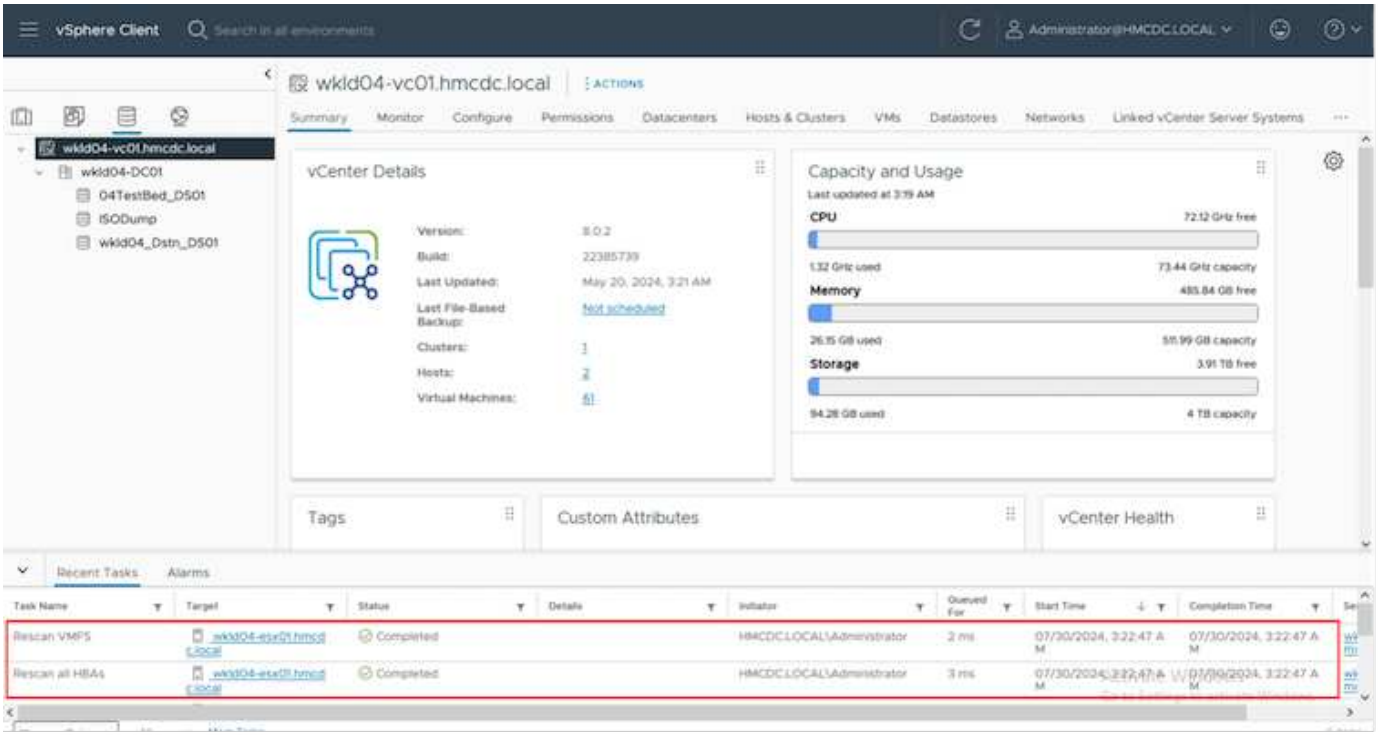
Lors d'une opération de basculement test, Disaster Recovery crée un volume FlexClone® sur le système de stockage ONTAP de destination à l'aide de la copie Snapshot la plus récente ou d'un snapshot sélectionné du volume de destination.

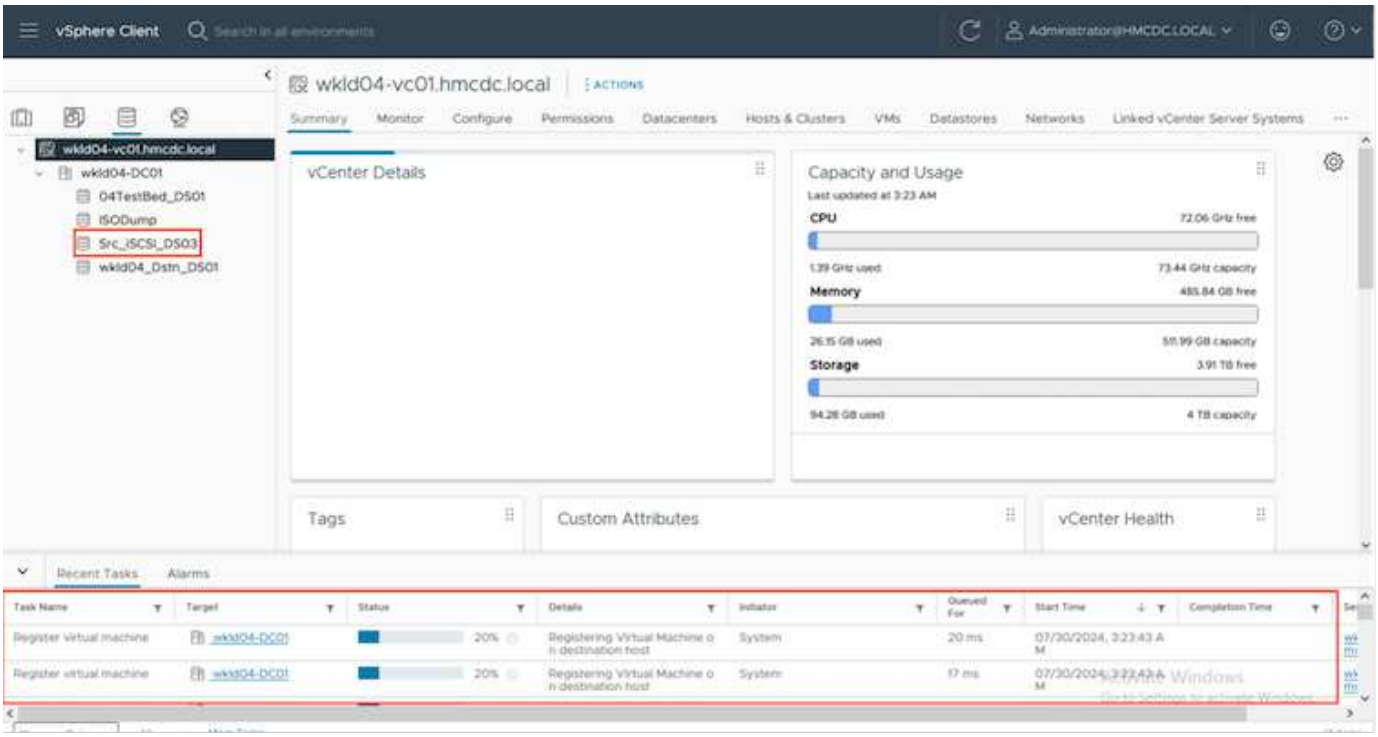
Une opération de basculement de test crée un volume cloné sur le système de stockage ONTAP de destination.

L'exécution d'une opération de récupération de test n'affecte pas la réplication SnapMirror .



Pendant le processus, Disaster Recovery ne mappe pas le volume cible d'origine. À la place, il crée un nouveau volume FlexClone® à partir du Snapshot sélectionné et un datastore temporaire adossé au volume FlexClone® est mappé sur les hôtes ESXi.

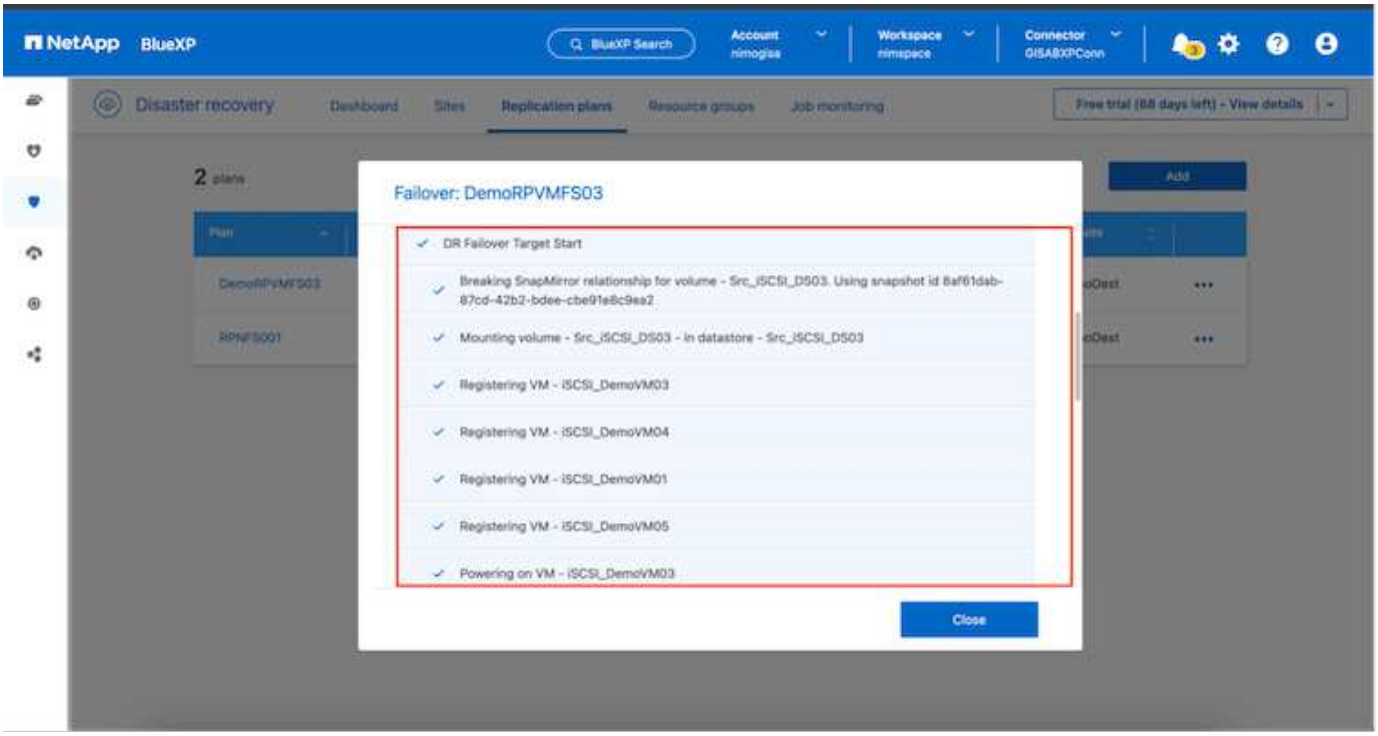




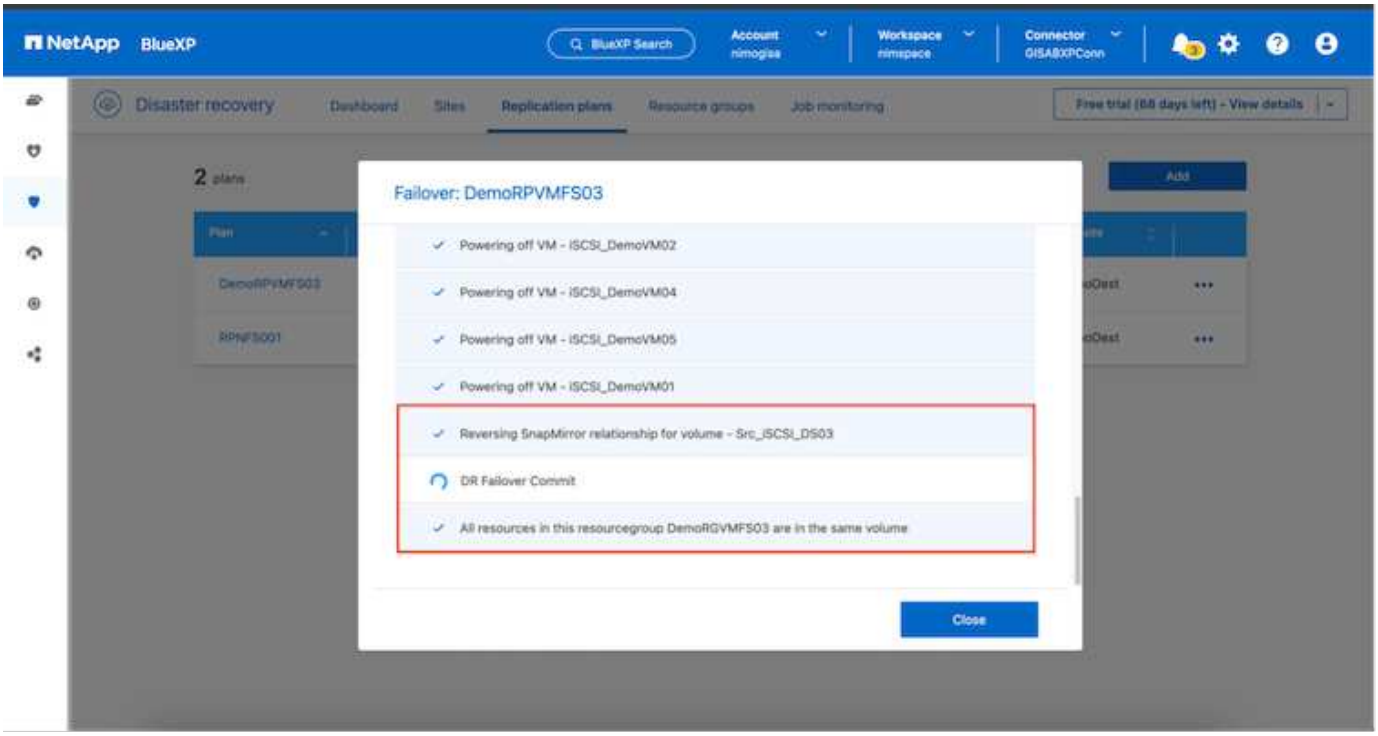
Une fois l'opération de basculement de test terminée, l'opération de nettoyage peut être déclenchée à l'aide de **« Clean Up failover test »**. Au cours de cette opération, Disaster Recovery détruit le volume FlexClone utilisé dans l'opération.

En cas de catastrophe réelle, Disaster Recovery effectue les étapes suivantes :

1. Rompt la relation SnapMirror entre les sites.
2. Monte le volume de la banque de données VMFS après la resignature pour une utilisation immédiate.
3. Enregistrer les machines virtuelles
4. Mise sous tension des machines virtuelles

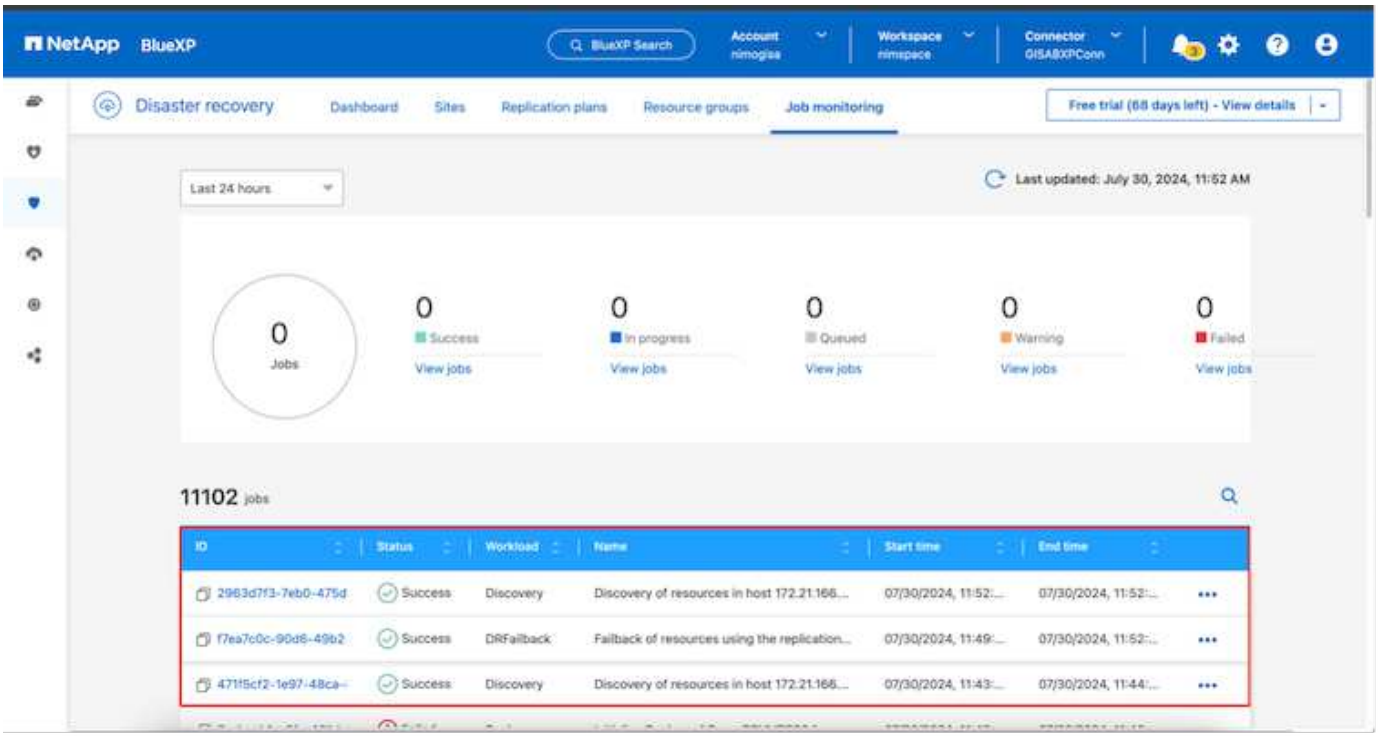


Une fois le site principal opérationnel, Disaster Recovery permet la resynchronisation inverse pour SnapMirror et permet le rétablissement, qui peut également être effectué d'un simple clic.



Et si l'option de migration est choisie, elle est considérée comme un événement de basculement planifié. Dans ce cas, une étape supplémentaire est déclenchée qui consiste à arrêter les machines virtuelles sur le site source. Le reste des étapes reste le même que pour l'événement de basculement.

Depuis Console ou l'ONTAP CLI, vous pouvez surveiller l'état de santé de la réplication des volumes de datastore appropriés, et suivre l'état d'un basculement ou d'un test de basculement via Job Monitoring.



Cela fournit une solution puissante pour gérer un plan de reprise après sinistre personnalisé et sur mesure. Le basculement peut être effectué sous forme de basculement planifié ou de basculement en un clic lorsqu'un sinistre survient et qu'une décision est prise d'activer le site DR.

Pour en savoir plus sur ce processus, n'hésitez pas à suivre la vidéo détaillée ou à utiliser le"simulateur de solutions" .

Charges de travail de conteneurs multicloud hybride NetApp avec Red Hat OpenShift

Commencer

Solutions multicloud hybrides NetApp pour les charges de travail des conteneurs Red Hat OpenShift

NetApp constate une augmentation significative du nombre de clients modernisant leurs applications d'entreprise existantes et créant de nouvelles applications à l'aide de conteneurs et de plates-formes d'orchestration construites autour de Kubernetes. Red Hat OpenShift Container Platform est un exemple que nous voyons adopté par bon nombre de nos clients.

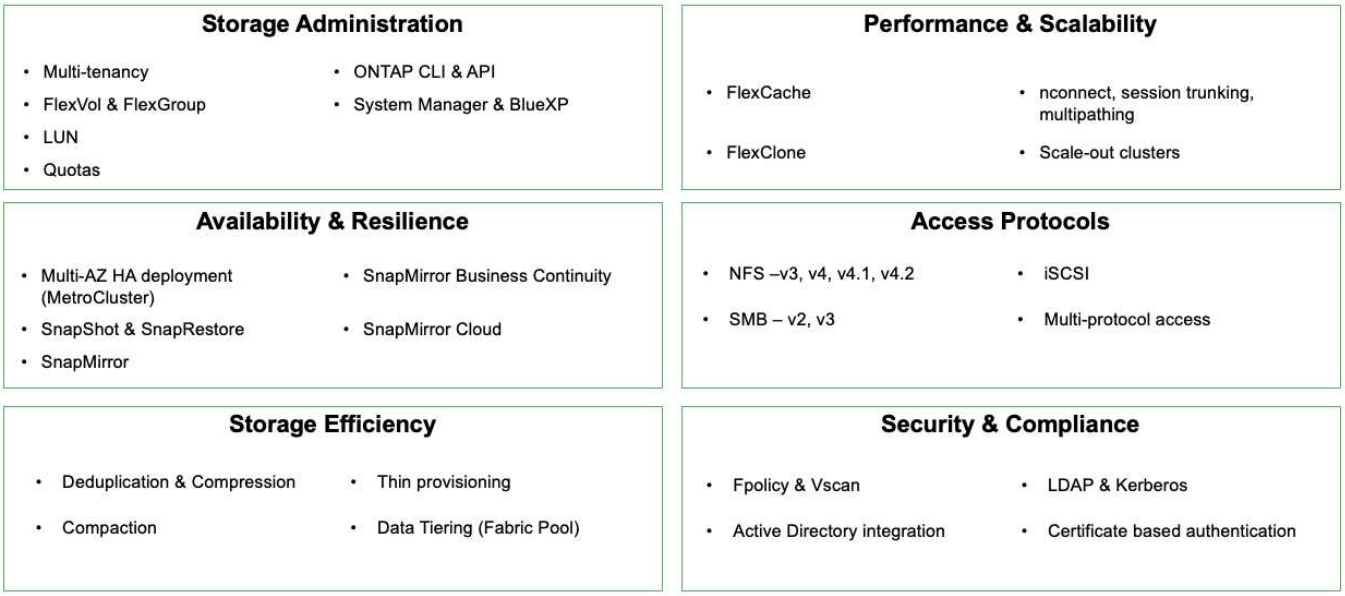
Aperçu

Alors que de plus en plus de clients commencent à adopter des conteneurs au sein de leurs entreprises, 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 des données, la sécurité des données et la migration des données. Cependant, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différentes.

Les options de stockage basées sur **NetApp ONTAP** répertoriées ci-dessous offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

- Stockage autogéré sur site :
  - Stockage en réseau NetApp (FAS), baies NetApp All Flash FAS (AFF), baies NetApp All SAN (ASA) et ONTAP Select
- Stockage géré par le fournisseur sur site :
  - NetApp Keystone fournit du 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 le fournisseur dans le cloud :
  - Amazon FSx for NetApp ONTAP, Azure NetApp Files et Google Cloud NetApp Volumes fournissent un stockage basé sur des fichiers dans le cloud.

ONTAP feature highlights

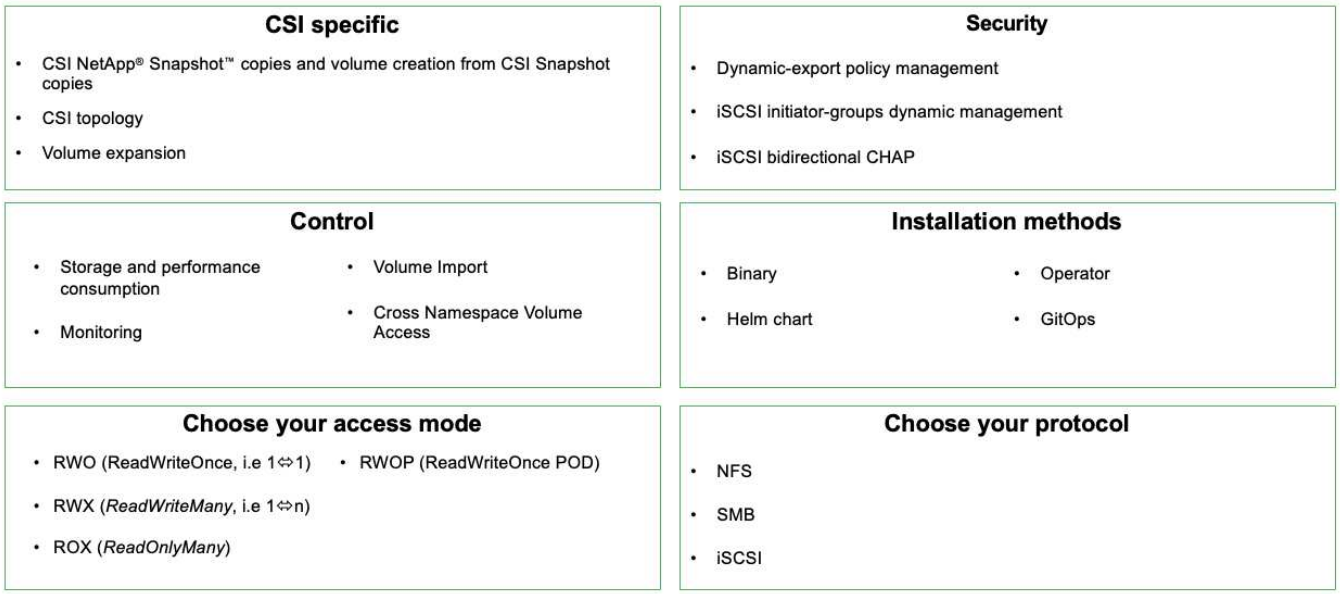


NetApp Console vous permet de gérer tous vos actifs de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser NetApp Console pour créer et administrer le stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), pour déplacer, protéger et analyser des données, et pour contrôler de nombreux périphériques de stockage sur site et en périphérie.

- NetApp Trident** est un orchestrateur de stockage conforme CSI qui permet une consommation rapide et facile du stockage persistant soutenu par une variété d'options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source maintenu et pris en charge par NetApp.

Astra Trident CSI feature highlights



Les charges de travail critiques des conteneurs nécessitent plus que de simples volumes persistants. Leurs exigences en matière de gestion des données nécessitent également la protection et la migration des objets Kubernetes de l'application.

> Les données d'application incluent les objets Kubernetes en plus des données utilisateur : Voici quelques exemples : - objets Kubernetes tels que les spécifications des pods, 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 les CR et les CRD

NetApp Trident Protect, disponible gratuitement en tant qu'extension de NetApp Trident, offre des capacités avancées de gestion des données applicatives qui améliorent la fonctionnalité et la disponibilité des applications Kubernetes avec état, soutenues par les systèmes de stockage NetApp ONTAP. Trident Protect simplifie la gestion, la protection et le déplacement des charges de travail conteneurisées, aussi bien dans les clouds publics que dans les environnements sur site. Il offre également des capacités d'automatisation robustes via son API et son CLI.

Cette documentation de référence fournit la validation de la protection des données des applications basées sur des conteneurs, déployées sur la plate-forme RedHat OpenShift à l'aide de Trident Protect. De plus, la solution fournit des détails de haut niveau pour le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plates-formes de conteneurs. Le document met également en évidence les détails de l'intégration du stockage NetApp avec les plates-formes de conteneurs Red Hat OpenShift à l'aide du provisionneur Trident CSI.

Propositions de valeur des solutions NetApp Hybrid Multicloud pour les charges de travail Red Hat OpenShift Container

La plupart des clients ne se contentent pas de créer des environnements basés sur Kubernetes sans aucune infrastructure existante. Il s'agit peut-être d'un magasin informatique traditionnel exécutant 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 deviennent plus répandues à mesure que 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 peut répondre 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 réorganiser l'ensemble de leur infrastructure et de leur organisation. Que les applications et les données des clients soient hébergées sur site, dans le cloud, exécutées sur des machines virtuelles ou sur des conteneurs, NetApp peut fournir une gestion, une protection, une sécurité et une portabilité cohérentes des données. Grâce à ces nouvelles solutions, la même valeur que NetApp a fournie dans les environnements de centres de données sur site pendant des décennies sera disponible sur l'ensemble de l'horizon de données de l'entreprise, sans nécessiter d'investissement important pour se réorganiser, acquérir de nouvelles compétences ou constituer de nouvelles équipes. NetApp est bien placé pour aider les clients à résoudre ces défis commerciaux, quelle

que soit la phase de leur parcours vers le cloud.

NetApp Hybrid Multi-Cloud avec Red Hat Openshift :

- Fournit aux clients des conceptions et des pratiques validées qui démontrent les meilleures façons pour les clients de gérer, protéger, sécuriser et migrer leurs données et applications lors de l'utilisation de Red Hat OpenShift avec des solutions de stockage basées sur NetApp .
- Présentez 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.
- Démontrer des stratégies et des options pour les environnements sur site et dans le cloud, ainsi que pour les environnements hybrides où les deux sont utilisés.

Solutions prises en charge par NetApp Hybrid Multicloud pour les charges de travail Red Hat OpenShift Container

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 Console et NetApp Trident Protect.

Pour cette solution, les scénarios suivants sont testés et validés par NetApp. La solution est divisée en plusieurs scénarios en fonction des caractéristiques suivantes :

- sur site
- nuage
  - clusters OpenShift autogérés et stockage NetApp autogéré
  - clusters OpenShift gérés par le fournisseur et stockage NetApp géré par le fournisseur

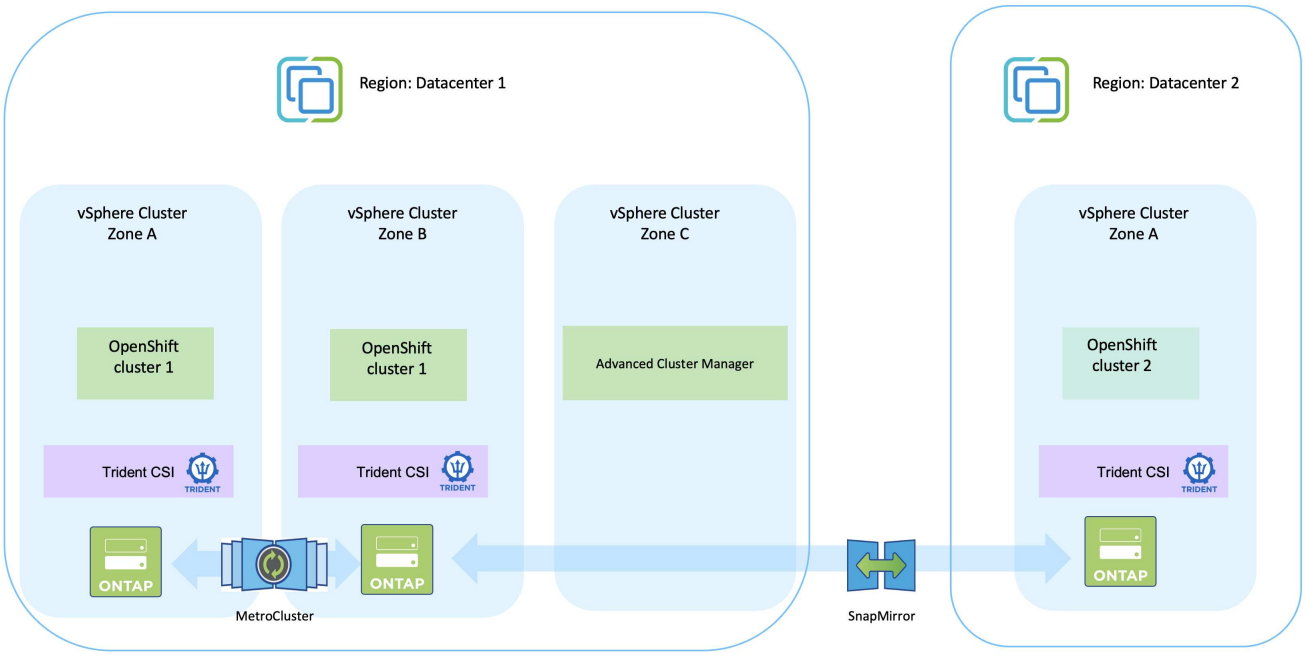
Nous développerons des solutions et des cas d'utilisation supplémentaires à l'avenir.

Scénario 1 : Protection et migration des données dans l'environnement sur site à l'aide de Trident Protect

Sur site : clusters OpenShift autogérés et stockage NetApp autogéré

- Utilisez Trident Protect pour protéger les applications et prendre en charge la migration entre les clusters sur site.

Scénario 1

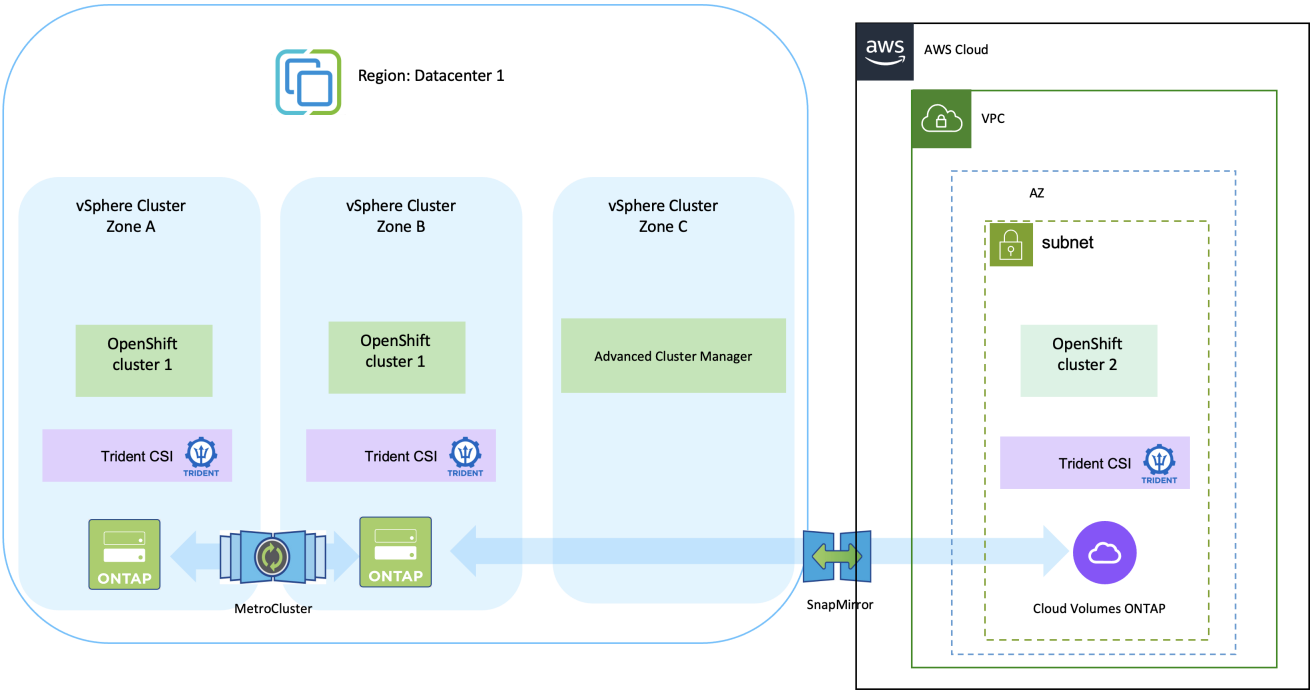


Scénario 2 : Protection des données et migration de l'environnement sur site vers l'environnement AWS à l'aide de Trident Protect

Sur site : cluster OpenShift autogéré et stockage autogéré Cloud AWS : cluster OpenShift autogéré et stockage autogéré

- Utilisez Trident Protect pour protéger les applications et faciliter la migration entre les clusters sur site et les clusters OpenShift autogérés dans AWS.

Scénario 2

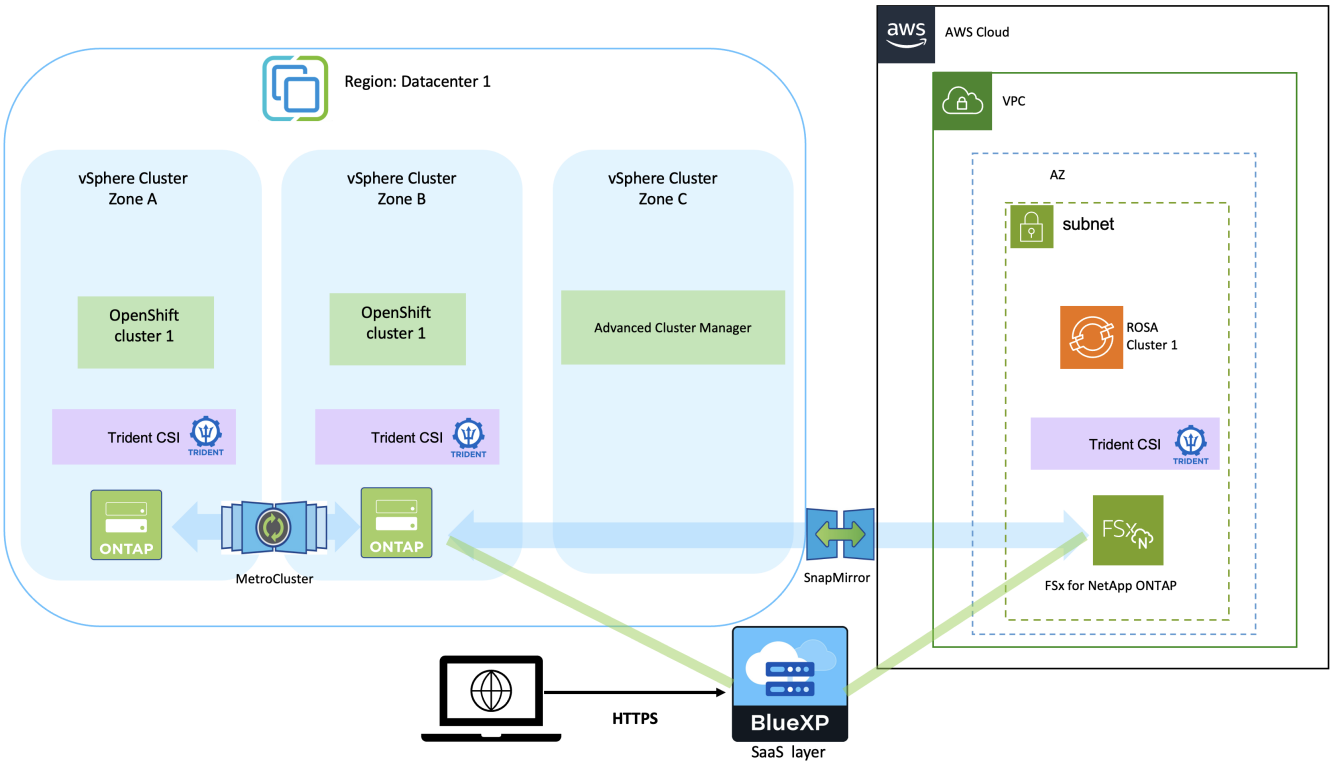


Scénario 3 : Protection des données et migration de l'environnement sur site vers l'environnement AWS

Sur site : cluster OpenShift autogéré et stockage autogéré AWS Cloud : cluster OpenShift géré par le fournisseur (ROSA) et stockage géré par le fournisseur (FSx ONTAP)

- À l'aide de NetApp Console, effectuez la réplication des volumes persistants (FSx ONTAP).
- À l'aide d'OpenShift GitOps, recréez les métadonnées de l'application.

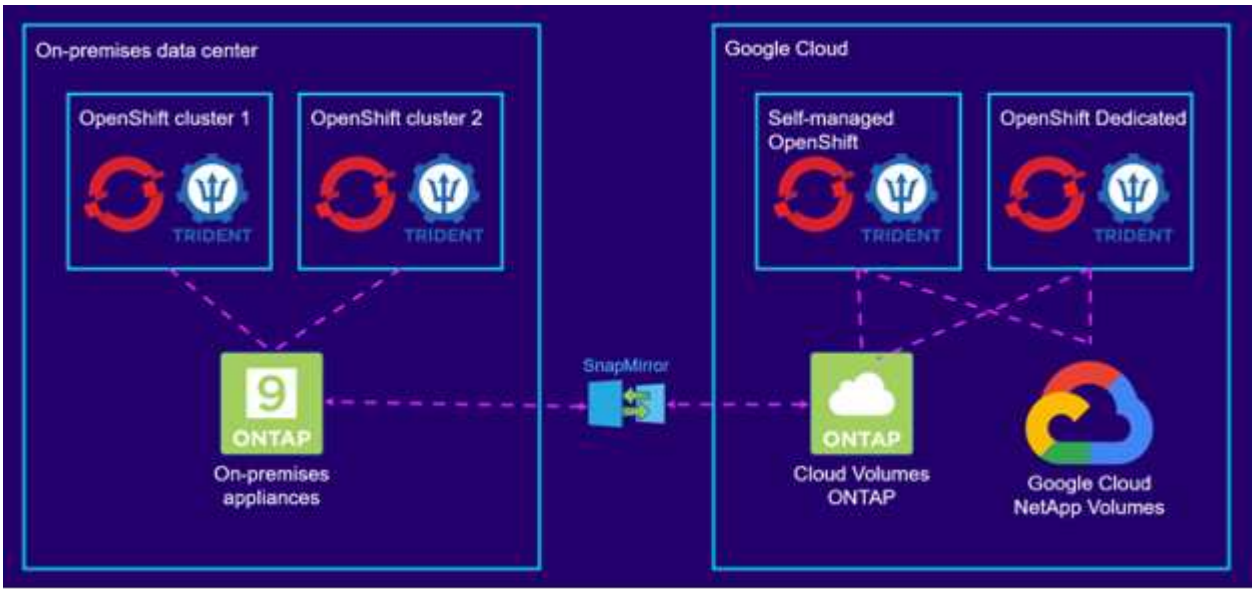
Scénario 3



Scénario 4 : Protection des données et migration de l'environnement sur site vers l'environnement GCP à l'aide de Trident Protect

Sur site : cluster OpenShift autogéré et stockage autogéré Google Cloud : cluster OpenShift autogéré et stockage autogéré

- Utilisez Trident Protect pour protéger les applications et prendre en charge la migration entre les clusters OpenShift sur site et Google Cloud.

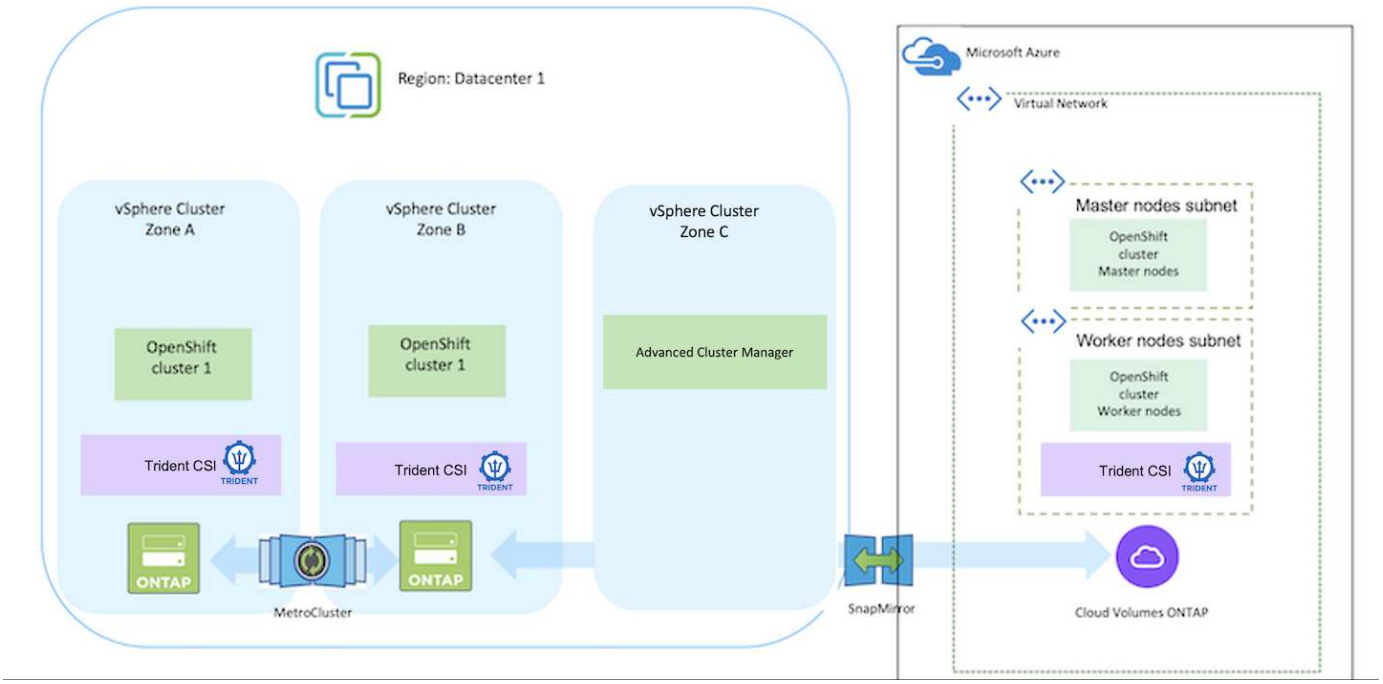


Pour les considérations relatives à l'utilisation ONTAP dans une configuration MetroCluster , reportez-vous à"ici" .

Scénario 5 : Protection des données et migration de l'environnement local vers l'environnement Azure à l'aide de Trident Protect

Sur site : cluster OpenShift autogéré et stockage autogéré Azure Cloud : cluster OpenShift autogéré et stockage autogéré

- Utilisez Trident Protect pour protéger les applications et prendre en charge la migration entre les environnements locaux et les clusters OpenShift dans Azure.



Pour les considérations relatives à l'utilisation ONTAP dans une configuration MetroCluster , reportez-vous à"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 la plate-forme de conteneurs OpenShift, OpenShift Advanced Cluster Manager, NetApp ONTAP et NetApp Trident Protect.

Les scénarios 1, 2 et 3 de la solution ont été validés à l'aide des versions présentées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Groupe de pôles	OpenShift 4.11.34
Clusters source et destination	OpenShift 4.12.9 sur site et dans AWS
* NetApp Trident*	Serveur et client Trident 23.04.0
* NetApp Trident Protect*	Trident Protect 22.11.0-82

* NetApp ONTAP*	ONTAP 9.12.1
AWS FSx ONTAP	AZ unique

Le scénario 4 de la solution a été validé en utilisant les versions comme indiqué dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Groupe de pôles	OpenShift 4.13.13
Clusters source et destination	OpenShift 4.13.12 sur site et dans Google Cloud
* NetApp Trident*	Serveur et client Trident 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	AZ unique, nœud unique, 9.14.0

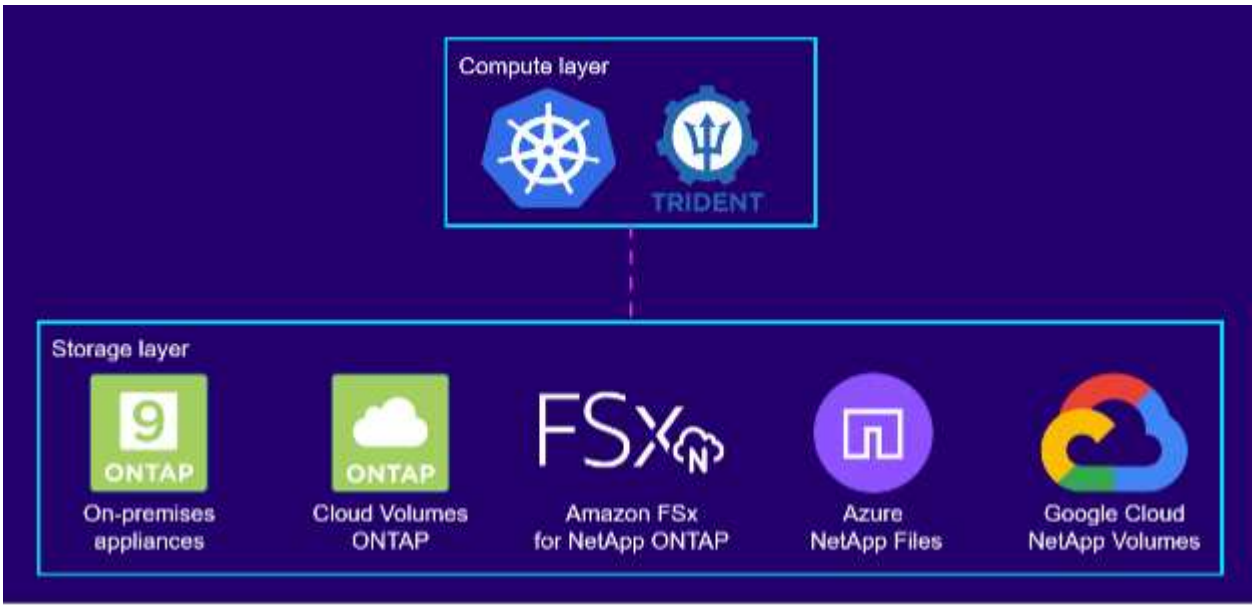
Le scénario 5 de la solution a été validé en utilisant les versions comme indiqué dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Clusters source et destination	OpenShift 4.13.25 sur site et dans Azure
* NetApp Trident*	Serveur et client Trident 23.10.0
* NetApp Trident Protect*	Trident Protect 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	AZ unique, nœud unique, 9.14.0

Intégrations de stockage NetApp prises en charge avec les conteneurs Red Hat OpenShift

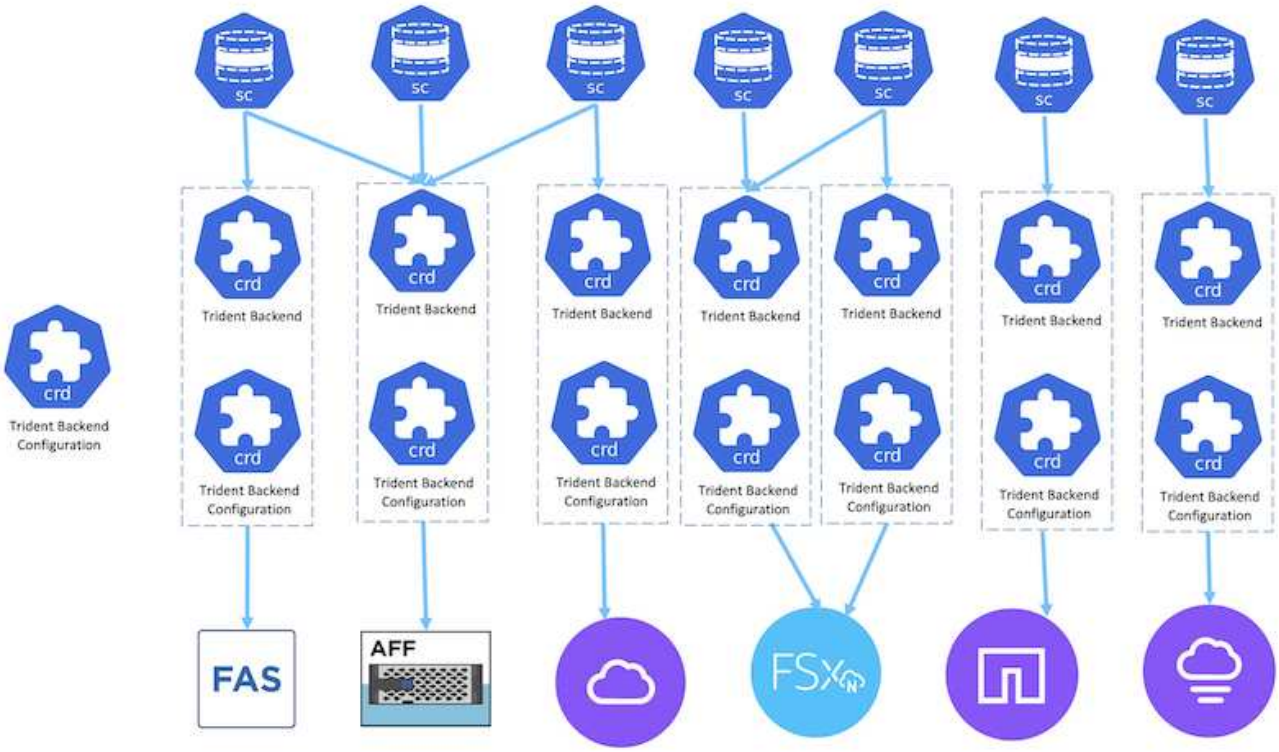
Que les conteneurs Red Hat OpenShift s’exécutent sur VMware ou dans les hyperscalers, NetApp Trident peut être utilisé comme provisionneur CSI pour les différents types de stockage NetApp back-end qu’il prend en charge.

Le diagramme suivant illustre les différents stockages back-end NetApp qui peuvent être intégrés aux clusters OpenShift à l’aide de NetApp Trident.



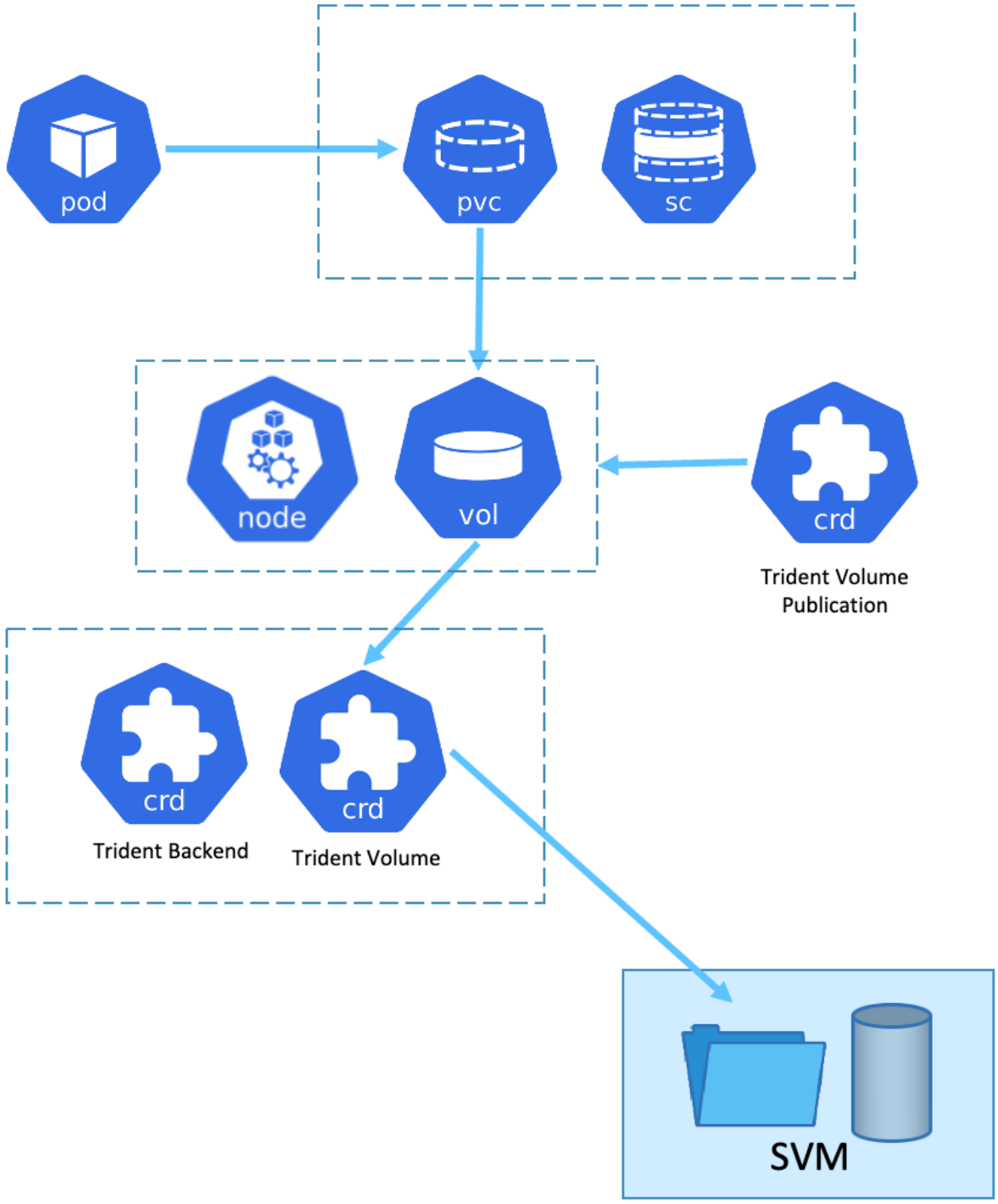
La machine virtuelle de stockage ONTAP (SVM) fournit une multilocation sécurisée. Un cluster OpenShift unique peut se connecter à un seul SVM ou à plusieurs SVM ou même à plusieurs clusters ONTAP . La classe de stockage filtre le stockage backend en fonction de paramètres ou d'étiquettes. Les administrateurs de stockage définissent les paramètres de connexion au système de stockage à l'aide de la configuration backend Trident. Une fois la connexion établie avec succès, le backend trident est créé et les informations que la classe de stockage peut filtrer sont renseignées.

La relation entre la classe de stockage et le backend est indiquée ci-dessous.



Le propriétaire de l'application demande un volume persistant à l'aide de la classe de stockage. La classe de stockage filtre le stockage backend.

La relation entre le pod et le stockage backend est illustrée ci-dessous.



Options de l'interface de stockage de conteneurs (CSI)

Dans les environnements vSphere, les clients peuvent choisir le pilote VMware CSI et/ou Trident CSI pour s'intégrer à ONTAP. Avec VMware CSI, les volumes persistants sont consommés en tant que disques SCSI locaux, tandis qu'avec Trident, ils sont consommés 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. Avec les déploiements basés sur FC, VMware CSI est

préféré et SnapMirror Business Continuity (SMBC) offre une haute disponibilité au niveau de la zone.

VMware CSI prend en charge

- Magasins de données basés sur Core Block (FC, FCoE, iSCSI, NVMeoF)
- Magasins de données basés sur des fichiers de base (NFS v3, v4)
- Magasins de données vVol (blocs et fichiers)

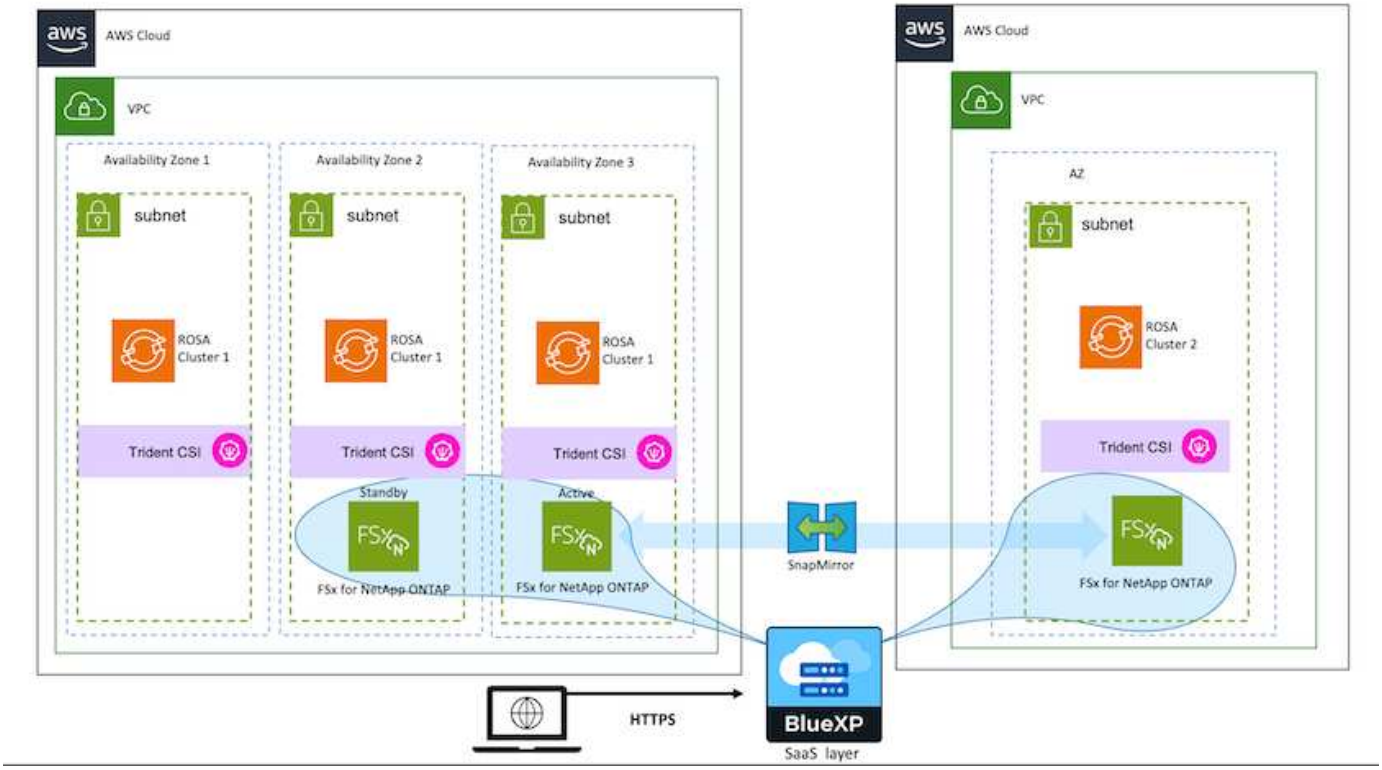
Trident dispose des pilotes suivants pour prendre en charge ONTAP

- ontap-san (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 Trident CSI, ONTAP prend en charge nconnect, session trunking, Kerberos, etc. pour NFS et multipathing, authentification chap, etc. pour les protocoles de blocs.

Dans AWS, Amazon FSx for NetApp ONTAP (FSx ONTAP) peut être déployé dans une seule zone de disponibilité (AZ) ou dans plusieurs AZ. Pour les charges de travail de production nécessitant une haute disponibilité, le multi-AZ offre une tolérance aux pannes au niveau zonal et dispose d'un meilleur cache de lecture NVMe par rapport au AZ unique. Pour plus d'informations, consultez"Directives de performance AWS" .

Pour réduire les coûts sur le site de reprise après sinistre, un seul AZ FSx ONTAP peut être utilisé.



Pour connaître le nombre de SVM pris en charge par FSx ONTAP, reportez-vous à"gestion de la machine virtuelle de stockage FSx ONTAP"

Documentation supplémentaire

Voici quelques documents supplémentaires pour référence :

1. "VMware vSphere"
2. "Documentation produit de la plateforme OpenShift Container"
3. "Installation des clusters de la plateforme de conteneurs OpenShift"
4. "Documentation du produit de gestion avancée des clusters"
5. "Création d'un cluster à l'aide d'ACM"
6. "Déploiement de Red Hat Quay sur OpenShift"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - Verda (logiciel libre) propose une collection de hooks d'exécution de référence pour des applications cloud natives populaires à forte intensité de données
10. "NetApp services de données"
11. "Architecture classique du service Red Hat OpenShift sur AWS"
12. "Amazon FSx ONTAP"
13. "Installation de clusters OpenShift sur GCP"
14. "Installation de clusters OpenShift sur Azure"

Openshift pour sur site

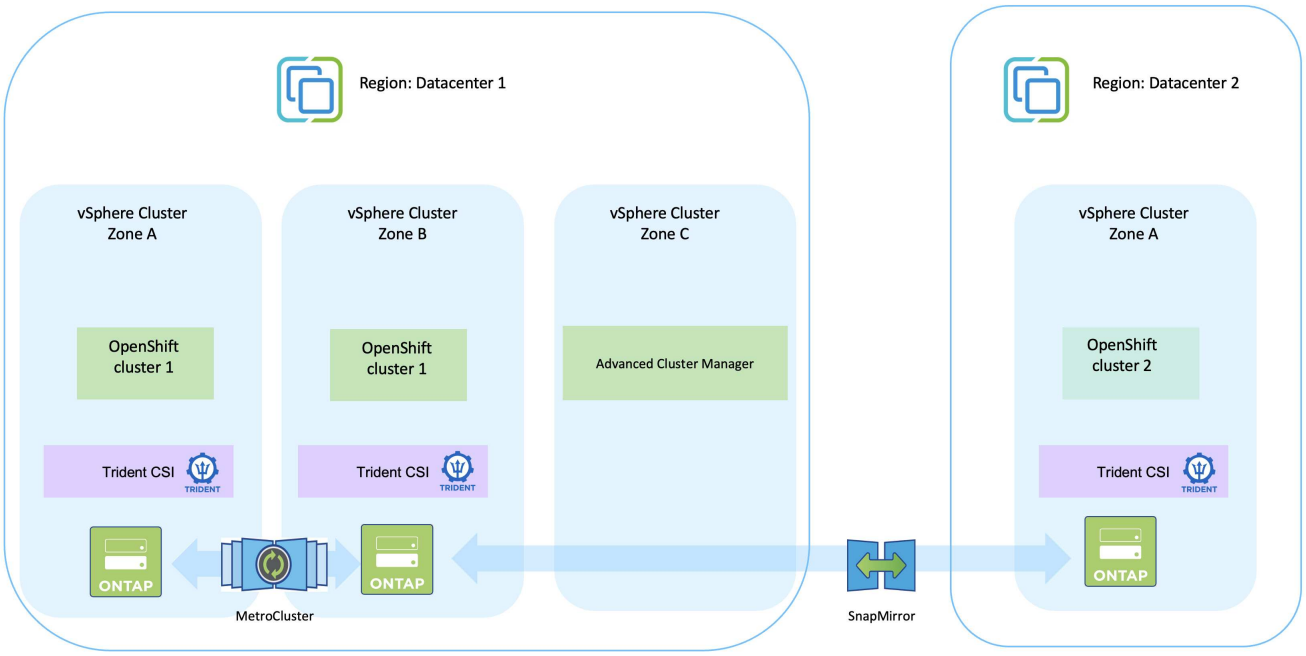
Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift sur VMware

Si les clients ont besoin d'exécuter leurs applications conteneurisées modernes sur l'infrastructure de leurs centres de données privés, ils peuvent le faire. Ils doivent planifier et déployer la plateforme de conteneurs Red Hat OpenShift (OCP) pour un environnement prêt pour la production afin de déployer leurs charges de travail de conteneurs. Leurs clusters OCP peuvent être déployés sur VMware ou sur du bare metal.

Le stockage NetApp ONTAP offre une protection des données, une fiabilité et une flexibilité pour les déploiements de conteneurs. Trident sert de fournisseur de stockage dynamique pour consommer le stockage ONTAP persistant pour les applications avec état des clients. NetApp Trident Protect peut être utilisé pour les nombreuses exigences de gestion des données des applications avec état telles que la protection des données, la migration et la continuité des activités.

Avec VMware vSphere, les outils NetApp ONTAP fournissent un plug-in vCenter qui peut être utilisé pour provisionner des banques de données. Appliquez des balises et utilisez-les avec OpenShift pour stocker la configuration et les données du nœud. Le stockage basé sur NVMe offre une latence plus faible et des performances élevées.

Solution de protection et de migration des données pour les charges de travail OpenShift Container à l'aide de Trident Protect

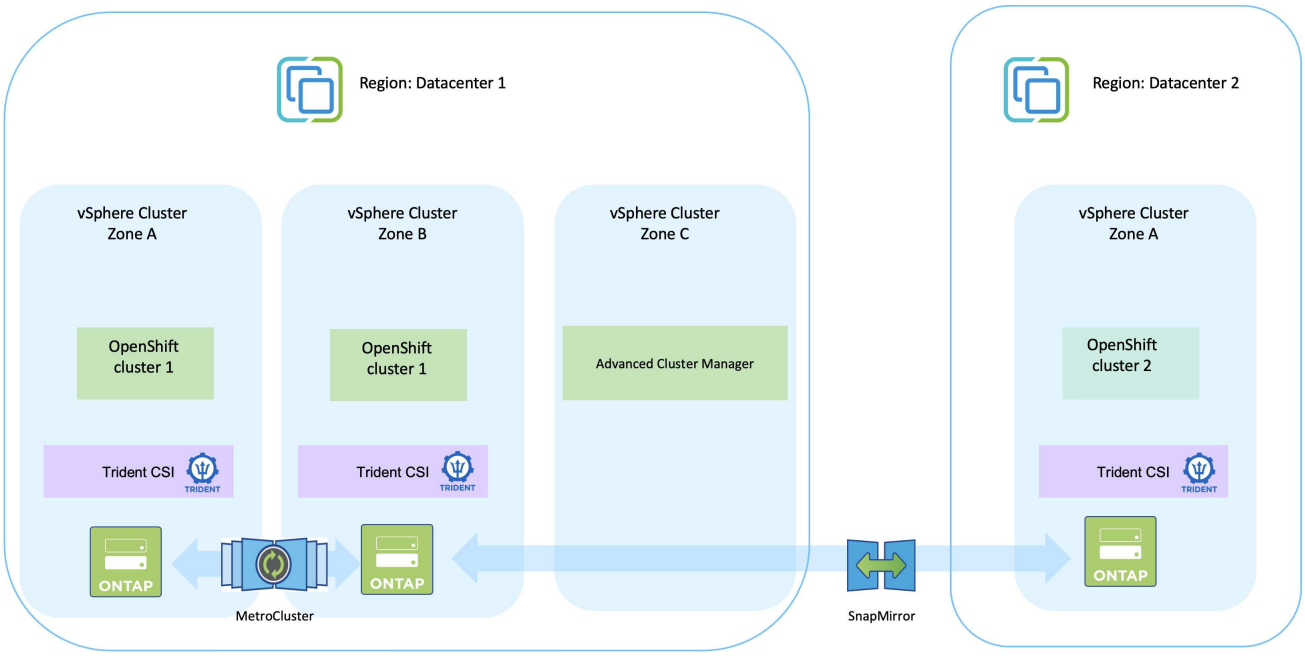


Déployer et configurer la plateforme Red Hat OpenShift Container sur VMware

Cette section décrit un flux de travail de haut niveau sur la façon de configurer et de gérer les clusters OpenShift et de gérer les applications avec état sur eux. Il montre l'utilisation des baies de stockage NetApp ONTAP avec l'aide de Trident pour fournir des volumes persistants.

> Il existe plusieurs façons de déployer des clusters de plateforme Red Hat OpenShift Container. 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"section ressources" .

Voici un diagramme qui illustre les clusters déployés sur VMware dans un centre de données.



Le processus de configuration peut être décomposé selon les étapes suivantes :

▼ **Déployer et configurer une machine virtuelle CentOS**

- Il est déployé dans l'environnement VMware vSphere.
- Cette machine virtuelle est utilisée pour déployer certains composants tels que NetApp Trident et NetApp Trident Protect pour la solution.
- Un utilisateur root est configuré sur cette machine virtuelle lors de l'installation.

▼ **Déployer et configurer un cluster OpenShift Container Platform sur VMware vSphere (Hub Cluster)**

Consultez les instructions relatives à la méthode "Déploiement assisté" pour déployer un cluster OCP.

N'oubliez pas ce qui suit : - Créez une clé publique et privée SSH à fournir au programme d'installation. Ces clés seront utilisées pour se connecter aux nœuds maître et travailleur si nécessaire. - Téléchargez le programme d'installation à partir de l'installateur assisté. Ce programme est utilisé pour démarrer les machines virtuelles que vous créez dans l'environnement VMware vSphere pour les nœuds maître et travailleur. - Les machines virtuelles doivent avoir les exigences minimales en matière de CPU, de mémoire et de disque dur. (Reportez-vous aux commandes vm create sur"ce" (page pour le maître et les nœuds de travail qui fournissent ces informations) - Le diskUUID doit être activé sur toutes les machines virtuelles. - Créez 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 VMware vSphere.

▼ **Installer Advanced Cluster Management sur le cluster Hub**

Ceci est installé à l'aide de l'opérateur de gestion de cluster avancé sur le cluster Hub. Se référer 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.

- Veuillez vous référer aux instructions "ici".

▼ **Configurer le stockage NetApp ONTAP**

- Installez un cluster ONTAP avec connectivité aux machines virtuelles OCP dans l'environnement VMWare.
- Créer un SVM.
- Configurez NAS Data Lif pour accéder au stockage dans SVM.

▼ **Installer NetApp Trident sur les clusters OCP**

- Installez NetApp Trident sur les trois clusters : clusters hub, source et de destination
- Veuillez vous référer aux instructions "ici".
- Créez un backend de stockage pour ontap-nas .
- Créez une classe de stockage pour ontap-nas.
- Se référer aux instructions"ici" .

▼ **Déployer une application sur le cluster source**

Utilisez OpenShift GitOps pour déployer une application. (par exemple Postgres, Ghost)

L'étape suivante consiste à utiliser Trident Protect pour la protection des données et la migration des données du cluster source vers le cluster de destination. Référer"ici" pour les instructions.

Protection des données avec Trident Protect

Cette page présente les options de protection des données pour les applications Red Hat OpenShift Container basées sur VMware vSphere utilisant Trident Protect.

Au fur et à mesure que les utilisateurs modernisent 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 requise à des fins réglementaires ou de conformité afin de protéger leurs données contre un sinistre.

Les exigences en matière de protection des données varient du retour à une copie ponctuelle au basculement automatique vers un autre domaine de panne sans aucune intervention humaine. De nombreux clients choisissent ONTAP comme plate-forme de stockage préférée pour leurs applications Kubernetes en raison de ses fonctionnalités riches telles que la multilocation, le multiprotocole, les offres de hautes performances et de capacité, la réplication et la mise en cache pour les emplacements multisites, la sécurité et la flexibilité.

Pour plus de détails sur la protection et la migration des charges de travail conteneurisées à l'aide de Trident Protect, consultez la section suivante : "Protégez et migrez les applications conteneur à l'aide de Trident Protect"

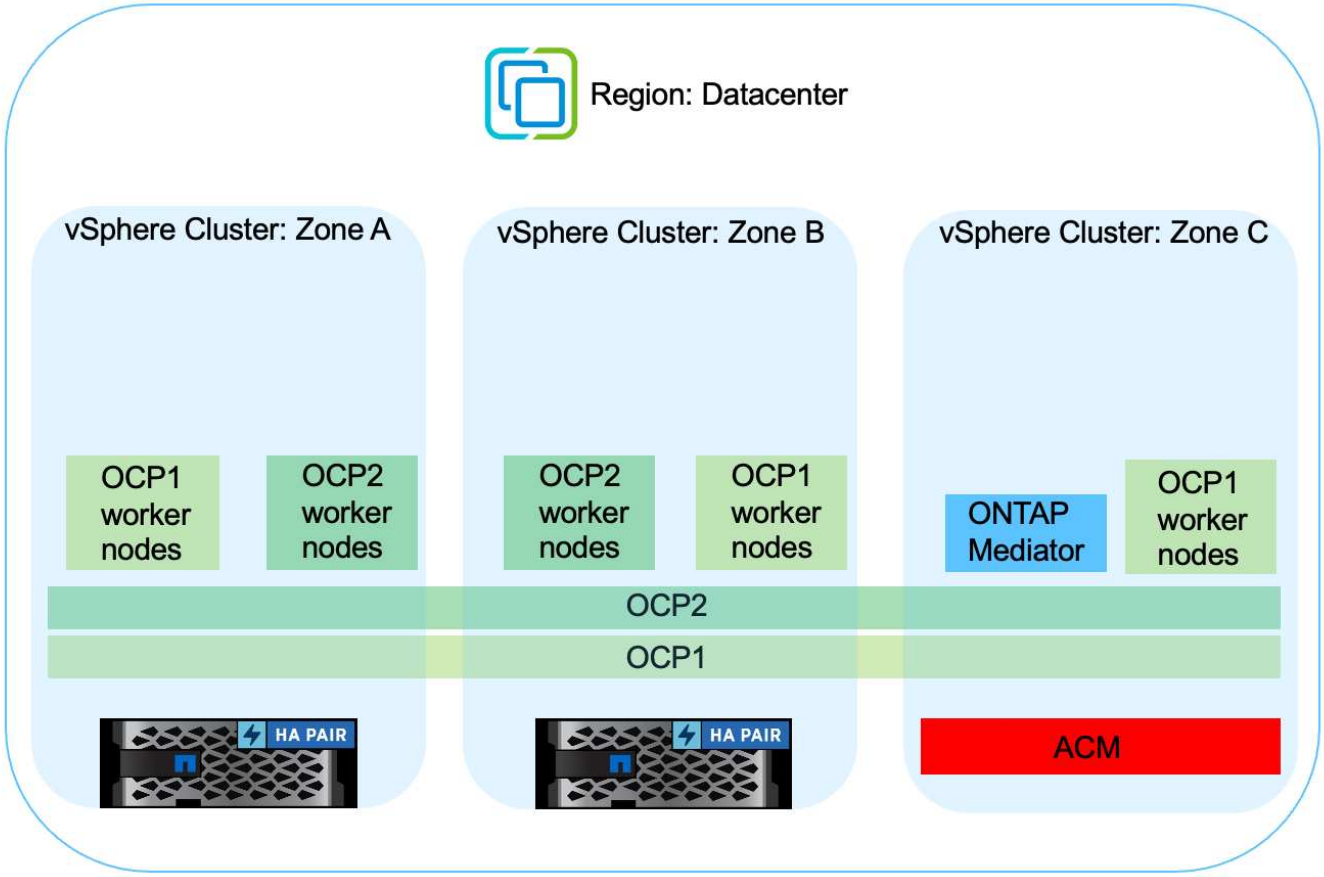
Continuité des activités avec MetroCluster

La plupart de nos plateformes matérielles pour ONTAP disposent de fonctionnalités de haute disponibilité pour protéger contre les pannes de périphériques, évitant ainsi la nécessité d'effectuer une récupération après sinistre. Mais pour se protéger des incendies ou de toute autre catastrophe et pour poursuivre l'activité avec un RPO nul et un RTO faible, une solution MetroCluster est souvent utilisée.

Les clients qui disposent actuellement d'un système ONTAP peuvent étendre leur service à MetroCluster en ajoutant des systèmes ONTAP pris en charge dans les limites de distance pour assurer une reprise après sinistre au niveau de la zone. Trident, le CSI (Container Storage Interface) prend en charge NetApp ONTAP, y

compris la configuration MetroCluster , ainsi que d'autres options telles que Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP, etc. Trident fournit cinq options de pilote de stockage pour ONTAP et toutes sont prises en charge pour la configuration MetroCluster . Référer"ici" pour plus de détails sur les pilotes de stockage ONTAP pris en charge par Trident.

La solution MetroCluster nécessite une extension de réseau de couche 2 ou la capacité d'accéder à la même adresse réseau à partir des deux domaines de pannes. Une fois la configuration de MetroCluster en place, la solution est transparente pour les propriétaires d'applications car tous les volumes du svm MetroCluster sont protégés et bénéficient des avantages de SyncMirror (zéro RPO).



Pour la configuration du backend Trident (TBC), ne spécifiez pas le dataLIF et le SVM lors de l'utilisation de la configuration MetroCluster . Spécifiez l'adresse IP de gestion SVM pour managementLIF et utilisez les informations d'identification du rôle vsadmin.

Des informations détaillées sur les fonctionnalités de protection des données de Trident Protect sont disponibles "ici".

Cloud hybride avec composants autogérés

Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift dans le cloud hybride

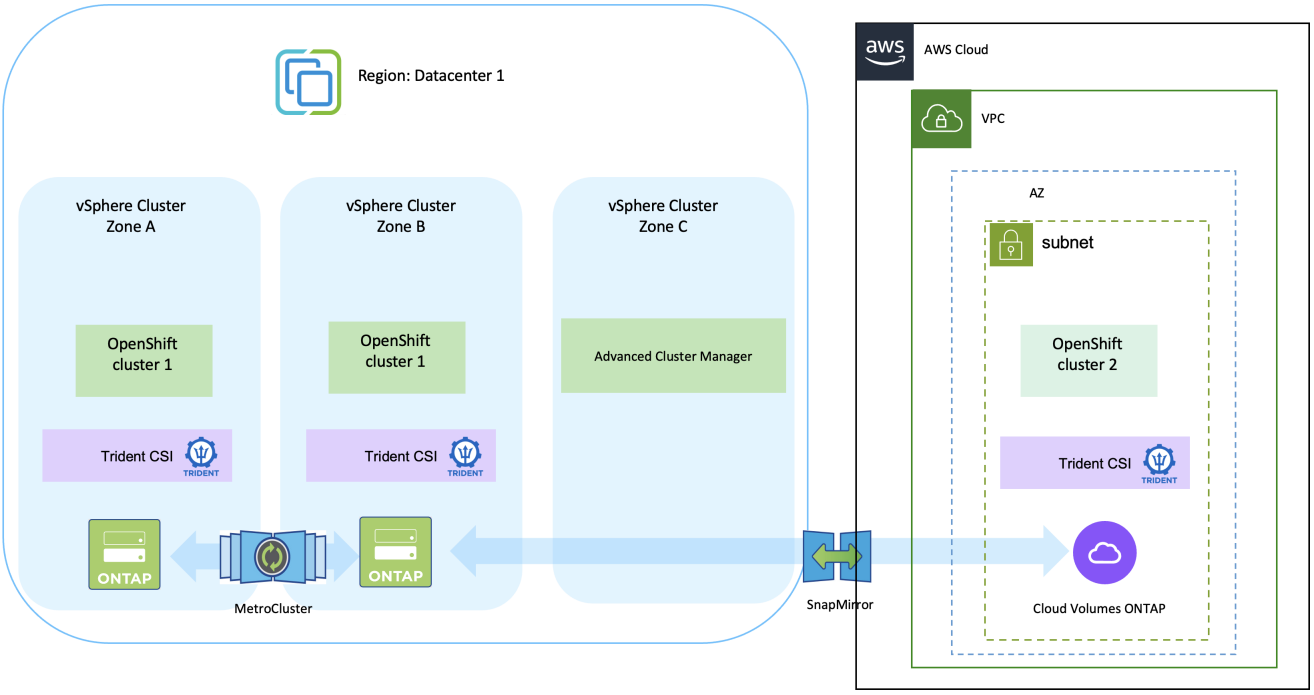
Les clients peuvent être à un stade de leur parcours de modernisation où ils sont prêts à déplacer certaines charges de travail sélectionnées ou toutes les charges de travail de leurs centres de données vers le cloud. Ils peuvent choisir d'utiliser des conteneurs

OpenShift autogérés et un stockage NetApp autogéré dans le cloud pour diverses raisons. Ils doivent planifier et déployer la plateforme de conteneurs Red Hat OpenShift (OCP) dans le cloud pour un environnement prêt pour la production afin de migrer leurs charges de travail de conteneurs depuis leurs centres de données. Leurs clusters OCP peuvent être déployés sur VMware ou Bare Metal dans leurs centres de données et sur AWS, Azure ou Google Cloud dans l'environnement cloud.

NetApp Cloud Volumes ONTAP offre protection des données, fiabilité et flexibilité pour les déploiements de conteneurs dans AWS, Azure et Google Cloud. Trident sert de provisionneur de stockage dynamique pour consommer le stockage persistant Cloud Volumes ONTAP pour les applications avec état des clients. Trident Protect peut être utilisé pour les exigences de gestion des données des applications avec état, telles que la protection des données, la migration et la continuité d'activité.

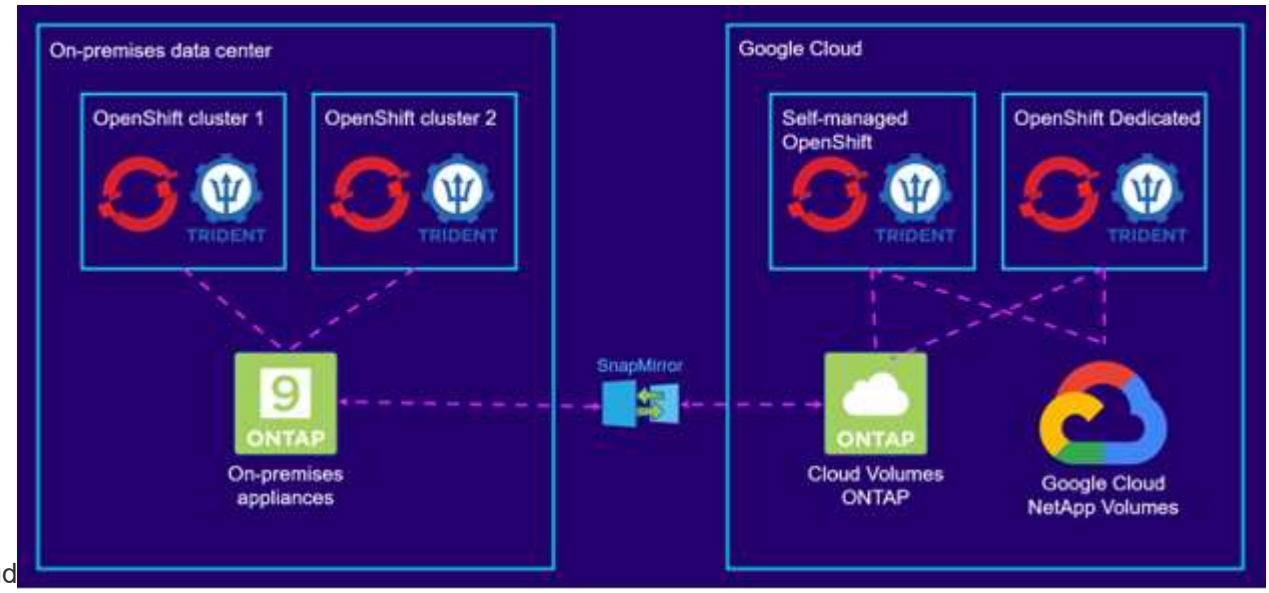
Solution de protection et de migration des données pour les charges de travail OpenShift Container dans un cloud hybride à l'aide de Trident Protect

Sur site et
AWS

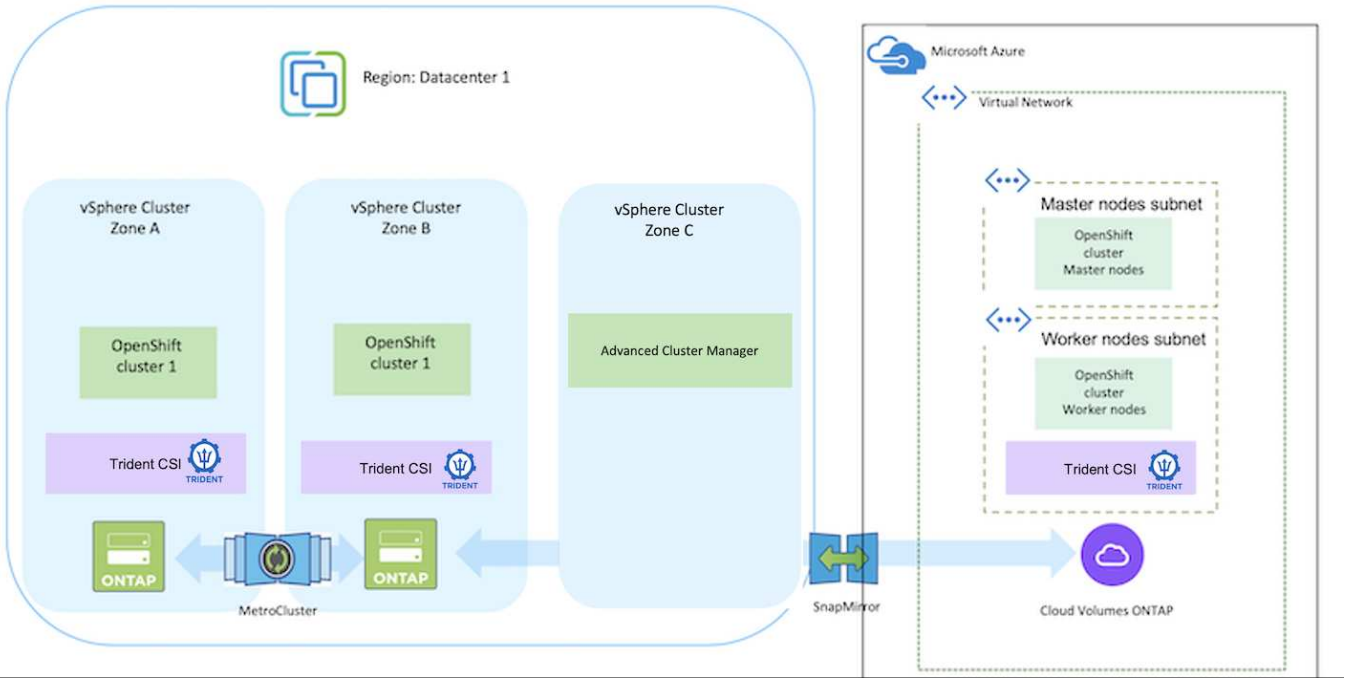


Sur site et Google

Cloud



Sur site et Cloud Azure



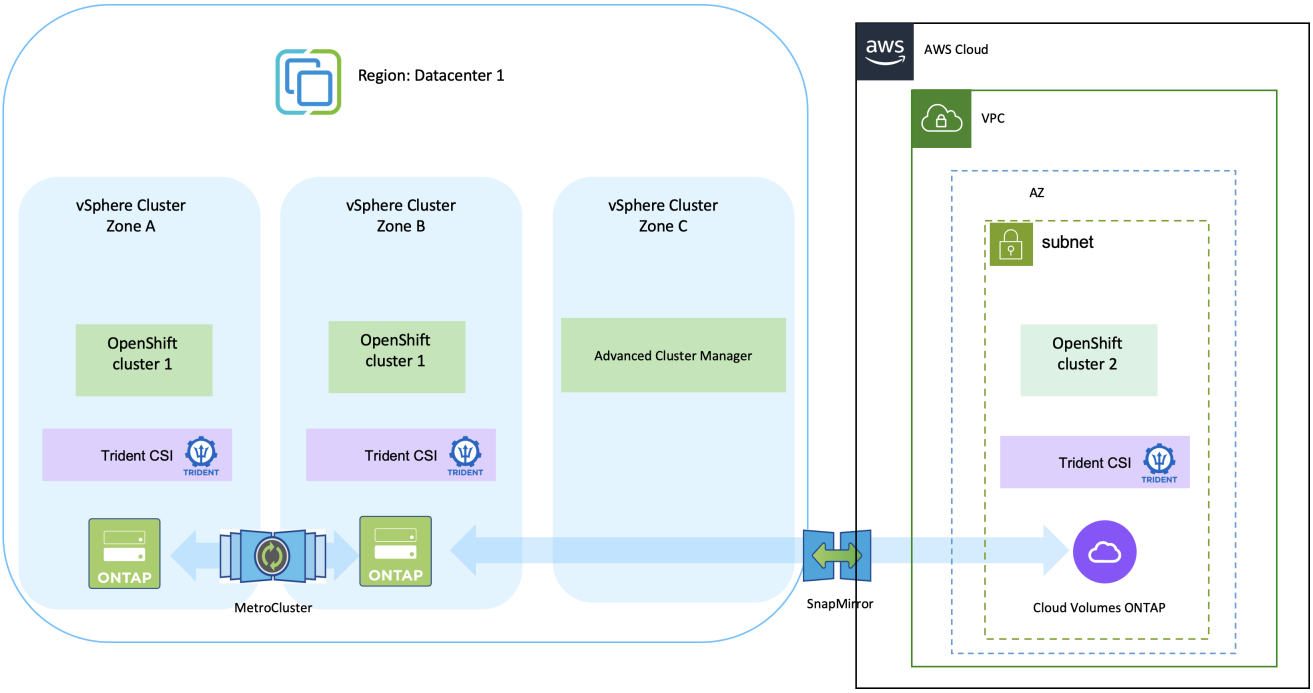
Déployer et configurer la plateforme Red Hat OpenShift Container sur AWS

Cette section décrit un flux de travail de haut niveau expliquant comment configurer et gérer les clusters OpenShift dans AWS et déployer des applications avec état sur eux. Il montre l'utilisation du stockage NetApp Cloud Volumes ONTAP avec l'aide de Trident pour fournir des volumes persistants. Des détails sont fournis sur l'utilisation de Trident Protect pour effectuer des activités de protection et de migration des données pour les applications avec état.

Il existe plusieurs façons de déployer des clusters de plateforme Red Hat OpenShift Container

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"section ressources" .

Voici un diagramme qui illustre les clusters déployés sur AWS et connectés au centre de données à l'aide d'un VPN.



Le processus de configuration peut être décomposé selon les étapes suivantes :

▼ **Installez un cluster OCP sur AWS à partir de la gestion avancée des clusters.**

- Créez un VPC avec une connexion VPN de site à site (à l'aide de pfsense) pour vous connecter au réseau local.
- Le réseau sur site dispose d'une connectivité Internet.
- Créez 3 sous-réseaux privés dans 3 AZ différents.
- Créez une zone hébergée privée Route 53 et un résolveur DNS pour le VPC.

Créez un cluster OpenShift sur AWS à partir de l'assistant Advanced Cluster Management (ACM). Consultez les instructions "ici".

Vous pouvez également créer le cluster dans AWS depuis la console Hybrid Cloud OpenShift. Consultez "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 formulaire. Une fois le cluster créé, vous pouvez vous connecter via SSH aux nœuds du cluster pour le dépannage ou une configuration manuelle supplémentaire. Utilisez la clé ssh que vous avez fournie lors de l'installation et le nom d'utilisateur core pour vous connecter.

▼ **Déployer Cloud Volumes ONTAP dans AWS à l'aide de NetApp Console.**

- Installez le connecteur dans un environnement VMware sur site. Se référer aux instructions"ici" .
- Déployez une instance CVO dans AWS à l'aide du connecteur. Se référer aux instructions"ici" .

> Le connecteur peut également être installé dans l'environnement cloud. Référer"ici" pour plus d'informations.

▼ **Installer Trident dans le cluster OCP**

- Déployez l'opérateur Trident à l'aide de Helm. Consultez les instructions "ici"
- Créez un backend et une classe de stockage. Se référer aux instructions"ici" .

Utilisation de la fonctionnalité Topologie CSI de Trident pour les architectures multizones

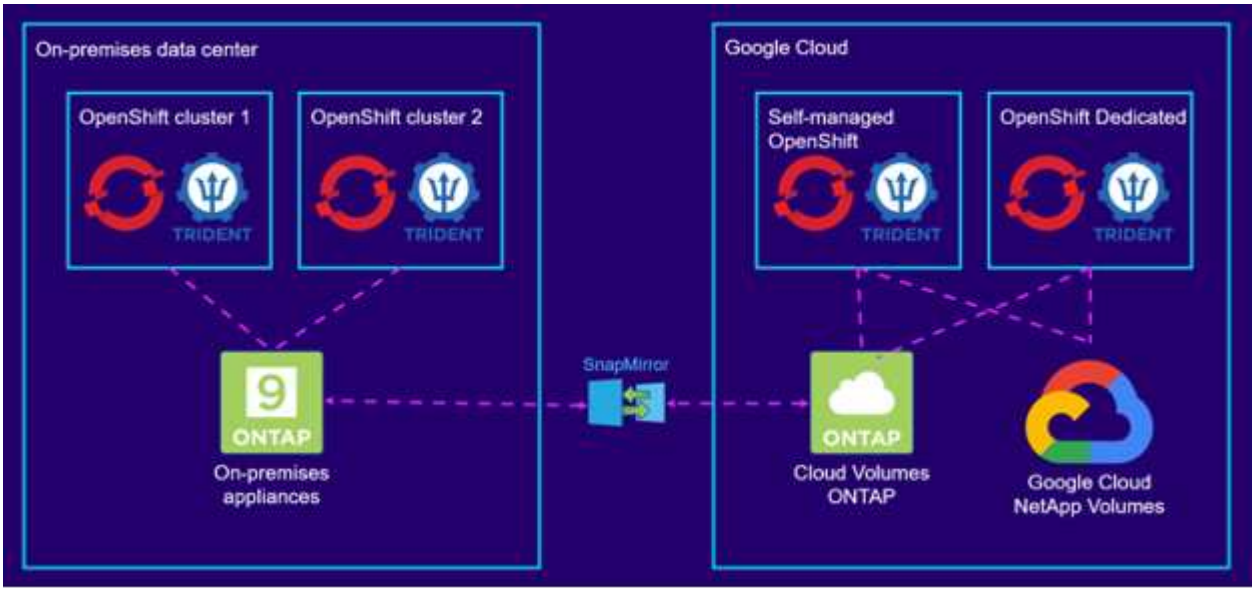
Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de générer des nœuds de clusters basés sur des zones. Les nœuds peuvent être situés dans différentes zones de disponibilité au sein d'une région ou dans plusieurs régions. Pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multizone, Trident utilise la topologie CSI. À l'aide de la fonctionnalité Topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Référer"ici" pour plus de détails.

> Kubernetes prend en charge deux modes de liaison de volume : - Lorsque ***VolumeBindingMode* est défini sur *Immediate*** (par défaut), Trident crée le volume sans aucune connaissance de la topologie. Les volumes persistants sont créés sans aucune dépendance aux exigences de planification du pod demandeur. - Lorsque ***VolumeBindingMode* est défini sur *WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour un PVC sont retardées jusqu'à ce qu'un pod utilisant le PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification imposées par les exigences de topologie. Les backends de stockage Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (backend prenant en compte la topologie). Pour les StorageClasses qui utilisent un tel backend, un volume ne sera créé que s'il est demandé par une application planifiée dans une région/zone prise en charge. (Classe de stockage prenant en compte la topologie) Référez-vous"ici" pour plus de détails.

Déployer et configurer la plateforme de conteneurs Red Hat OpenShift sur Google Cloud

Cette section décrit un flux de travail de haut niveau sur la façon de configurer et de gérer les clusters OpenShift dans GCP et de déployer des applications avec état sur eux. Il montre l'utilisation du stockage Google Cloud NetApp Volumes et NetApp Cloud Volumes ONTAP avec l'aide de Trident pour fournir des volumes persistants.

Voici un schéma qui montre les clusters déployés sur GCP et connectés au centre de données à l'aide d'un VPN.



Il existe plusieurs façons de déployer des clusters de plateforme Red Hat OpenShift Container 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"section ressources" .

Le processus de configuration peut être décomposé selon les étapes suivantes :

Installer un cluster OCP sur GCP à partir de la CLI

- Assurez-vous d'avoir rempli toutes les conditions préalables énoncées "ici".
- Pour la connectivité VPN entre le site local et GCP, une machine virtuelle pfsense a été créée et configurée. Pour les instructions, voir "ici" .
  - L'adresse de passerelle distante dans pfsense ne peut être configurée qu'après avoir créé une passerelle VPN dans Google Cloud Platform.
  - Les adresses IP du 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 les composants d'infrastructure du cluster créés par le programme d'installation.
- Installez maintenant le cluster OpenShift sur GCP.
  - Obtenez le programme d'installation et le pull secret, puis 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 A.
    - Utilisez l'adresse de bloc CIDR du réseau VPC pour configurer le pfsense et établir la connexion VPN. Assurez-vous que les pare-feu sont correctement configurés.
    - Ajoutez des enregistrements A dans le DNS de l'environnement local à l'aide de l'adresse IP dans les enregistrements A du DNS Google Cloud.
  - L'installation du cluster se termine et fournira un fichier kubeconfig ainsi qu'un nom d'utilisateur et un mot de passe pour se connecter à la console du cluster.

Déployer des Google Cloud NetApp Volumes

- Les Google Cloud NetApp Volumes peuvent être ajoutés à vos projets comme indiqué"ici" .

Déployer Cloud Volumes ONTAP dans GCP à l'aide de NetApp Console

- Installez un agent Console dans Google Cloud. Consultez les instructions "ici".
- Déployez une instance CVO dans Google Cloud à l'aide de l'agent. Consultez les instructions "ici".

Installer Trident dans le cluster OCP dans GCP

- Il existe de nombreuses méthodes pour déployer Trident, comme indiqué "ici".
- Pour ce projet, Trident a été installé en déployant Trident Operator manuellement en suivant les instructions "ici".
- Créez un backend et des classes de stockage. Se référer aux instructions"ici" .

Utilisation de la fonctionnalité Topologie CSI de Trident pour les architectures multizones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de générer des nœuds de clusters basés sur des zones. Les nœuds peuvent être situés dans différentes zones de disponibilité au sein d'une région ou dans plusieurs régions. Pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multizone, Trident utilise la topologie CSI. À l'aide de la fonctionnalité Topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Référer"ici" pour plus de détails.

> Kubernetes prend en charge deux modes de liaison de volume : - Lorsque ***VolumeBindingMode*** **est défini sur** ***Immediate*** (par défaut), Trident crée le volume sans aucune connaissance de la topologie. Les volumes persistants sont créés sans aucune dépendance aux exigences de planification du pod demandeur. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour un PVC sont retardées jusqu'à ce qu'un pod utilisant le PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification imposées par les exigences de topologie. Les backends de stockage Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (backend prenant en compte la topologie). Pour les StorageClasses qui utilisent un tel backend, un volume ne sera créé que s'il est demandé par une application planifiée dans une région/zone prise en charge. (Classe de stockage prenant en compte la topologie) Référez-vous"ici" pour plus de détails.

Vidéo de démonstration

Installation d'OpenShift Cluster sur Google Cloud Platform

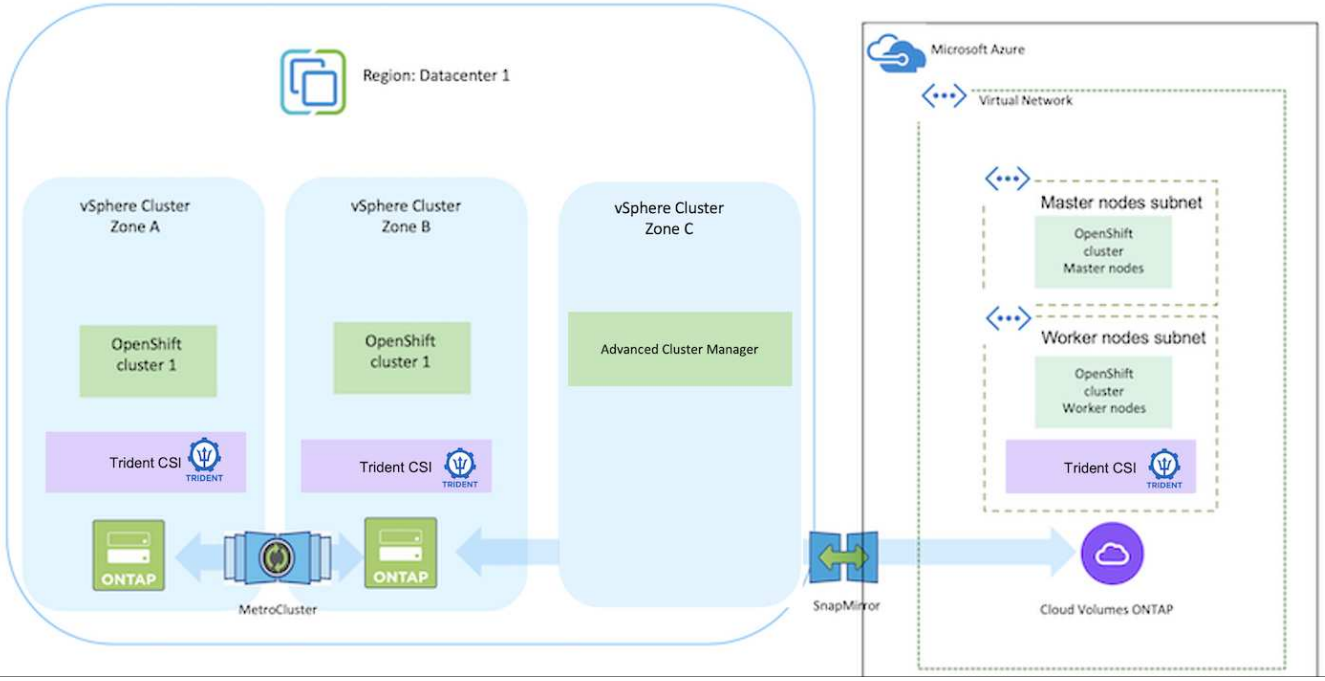
Importation de clusters OpenShift dans Trident Protect

Déployer et configurer la plateforme Red Hat OpenShift Container sur Azure

Cette section décrit un flux de travail de haut niveau expliquant comment configurer et gérer les clusters OpenShift dans Azure et déployer des applications avec état sur ceux-ci. Il montre l'utilisation du stockage NetApp Cloud Volumes ONTAP avec l'aide de Trident pour fournir des volumes persistants. Des détails sont fournis sur l'utilisation de Trident Protect pour effectuer des activités de protection et de migration des données pour les applications avec état.

Voici un schéma qui montre les clusters déployés sur Azure et connectés au centre de données à l'aide d'un

VPN.



Il existe plusieurs façons de déployer des clusters de plateforme Red Hat OpenShift Container 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"section ressources" .

Le processus de configuration peut être décomposé selon les étapes suivantes :

▼ **Installez un cluster OCP sur Azure à partir de l'interface de ligne de commande.**

- Assurez-vous d'avoir rempli toutes les conditions préalables énoncées "ici".
- Créez un VPN, des sous-réseaux et des groupes de sécurité réseau et une zone DNS privée. Créez une passerelle VPN et une connexion VPN de site à site.
- Pour la connectivité VPN entre le site local et Azure, une machine virtuelle pfsense a été créée et configurée. Pour les instructions, voir"ici" .
- Obtenez le programme d'installation et le secret d'extraction, puis déployez le cluster en suivant les étapes fournies dans la documentation "ici".
- L'installation du cluster se termine et fournira un fichier kubeconfig ainsi qu'un nom d'utilisateur et un mot de passe pour se connecter à la console du cluster.

Un exemple de fichier install-config.yaml est donné 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:
```

▼ **Déployer Cloud Volumes ONTAP dans Azure à l'aide de NetApp Console.**

- Installez un agent NetApp Console dans Azure. Consultez les instructions "ici".
- Déployez une instance CVO dans Azure à l'aide de l'agent. Consultez les instructions "ici".

Utilisation de la fonctionnalité Topologie CSI de Trident pour les architectures multizones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de générer des nœuds de clusters basés sur des zones. Les nœuds peuvent être situés dans différentes zones de disponibilité au sein d'une région ou dans plusieurs régions. Pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multizone, Trident utilise la topologie CSI. À l'aide de la fonctionnalité Topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Référer"ici" pour plus de détails.

> Kubernetes prend en charge deux modes de liaison de volume : - Lorsque ***VolumeBindingMode* est défini sur *Immediate*** (par défaut), Trident crée le volume sans aucune connaissance de la topologie. Les volumes persistants sont créés sans aucune dépendance aux exigences de planification du pod demandeur. - Lorsque ***VolumeBindingMode* est défini sur *WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour un PVC sont retardées jusqu'à ce qu'un pod utilisant le PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification imposées par les exigences de topologie. Les backends de stockage Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (backend prenant en compte la topologie). Pour les StorageClasses qui utilisent un tel backend, un volume ne sera créé que s'il est demandé par une application planifiée dans une région/zone prise en charge. (Classe de stockage prenant en compte la topologie) Référez-vous"ici" pour plus de détails.

Protection des données avec Trident Protect

Pour plus de détails sur la protection et la migration des charges de travail conteneurisées à l'aide de Trident Protect, consultez la section suivante : "Protégez et migrez les applications conteneur à l'aide de Trident Protect"

Cloud hybride avec composants gérés par le fournisseur

Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift gérées

Les clients peuvent être « nés dans le cloud » ou être à un stade de leur parcours de modernisation où ils sont prêts à déplacer certaines charges de travail sélectionnées ou toutes les charges de travail de leurs centres de données vers le cloud. Ils peuvent choisir d'utiliser des conteneurs OpenShift gérés par le fournisseur et un stockage NetApp géré par le fournisseur dans le cloud pour exécuter leurs charges de travail. Ils doivent planifier et déployer les clusters de conteneurs Red Hat OpenShift gérés dans le cloud pour un environnement prêt pour la production pour leurs charges de travail de conteneurs. NetApp propose des offres de stockage entièrement gérées pour les solutions Red Hat gérées dans les trois principaux clouds publics.

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

FSx ONTAP offre une protection des données, une fiabilité et une flexibilité pour les déploiements de conteneurs dans AWS. Trident sert de fournisseur de stockage dynamique pour consommer le stockage persistant FSx ONTAP pour les applications avec état des clients.

Comme ROSA peut être déployé 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 offre une haute disponibilité et une protection contre les pannes AZ.

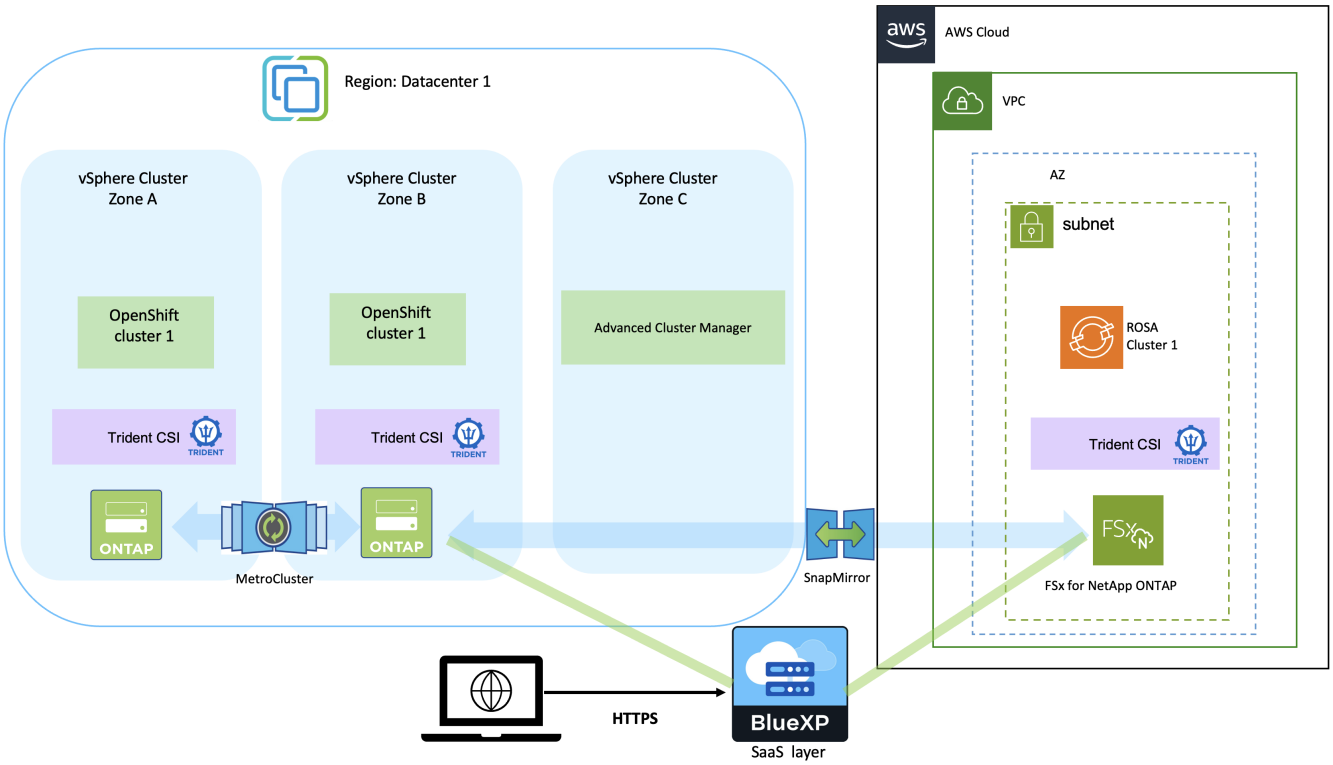
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated est une plateforme d'applications entièrement gérée qui vous permet de créer, de déployer et de faire évoluer rapidement des applications dans le cloud hybride. Google Cloud NetApp Volumes fournit des volumes persistants apportant la suite complète des fonctionnalités de gestion des données d'entreprise d'ONTAP aux déploiements OpenShift dans Google Cloud.

Déployer et configurer la plateforme Managed Red Hat OpenShift Container sur AWS

Cette section décrit un flux de travail de haut niveau pour la configuration des clusters Red Hat OpenShift gérés sur AWS (ROSA). Elle montre l'utilisation de Amazon FSx for NetApp ONTAP (FSx ONTAP) géré comme backend de stockage par Trident pour fournir des volumes persistants. Des détails sont fournis sur le déploiement de FSx ONTAP sur AWS à l'aide de NetApp Console. Des détails sont également fournis sur l'utilisation de NetApp Console et de OpenShift GitOps (Argo CD) pour effectuer des opérations de protection des données et de migration pour les applications avec état sur les clusters ROSA.

Voici un diagramme qui illustre les clusters ROSA déployés sur AWS et utilisant FSx ONTAP comme stockage backend.



Cette solution a été vérifiée en utilisant deux clusters ROSA dans deux VPC dans AWS. Chaque cluster ROSA a été intégré à FSx ONTAP à l'aide de Trident. Il existe plusieurs façons de déployer des clusters ROSA et FSx ONTAP 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"section ressources" .

Le processus de configuration peut être décomposé selon les étapes suivantes :

Installer les clusters ROSA

- Créez deux VPC et configurez la connectivité de peering VPC entre les VPC.
- Consultez "ici" pour obtenir des instructions sur l'installation des clusters ROSA.

Installer FSx ONTAP

- Installez FSx ONTAP sur les VPC depuis NetApp Console. Consultez "ici" pour créer un compte NetApp Console et commencer. Consultez "ici" pour installer FSx ONTAP. Consultez "ici" pour créer un connecteur dans AWS afin de gérer FSx ONTAP.
- Déployez FSx ONTAP à l'aide d'AWS. Référer"ici" pour le déploiement à l'aide de la console AWS.

Installer Trident sur les clusters ROSA (à l'aide du graphique Helm)

- Utilisez le chart Helm pour installer Trident sur les clusters ROSA. Consultez le lien vers la documentation : here.

Intégration de FSx ONTAP avec Trident pour les clusters ROSA

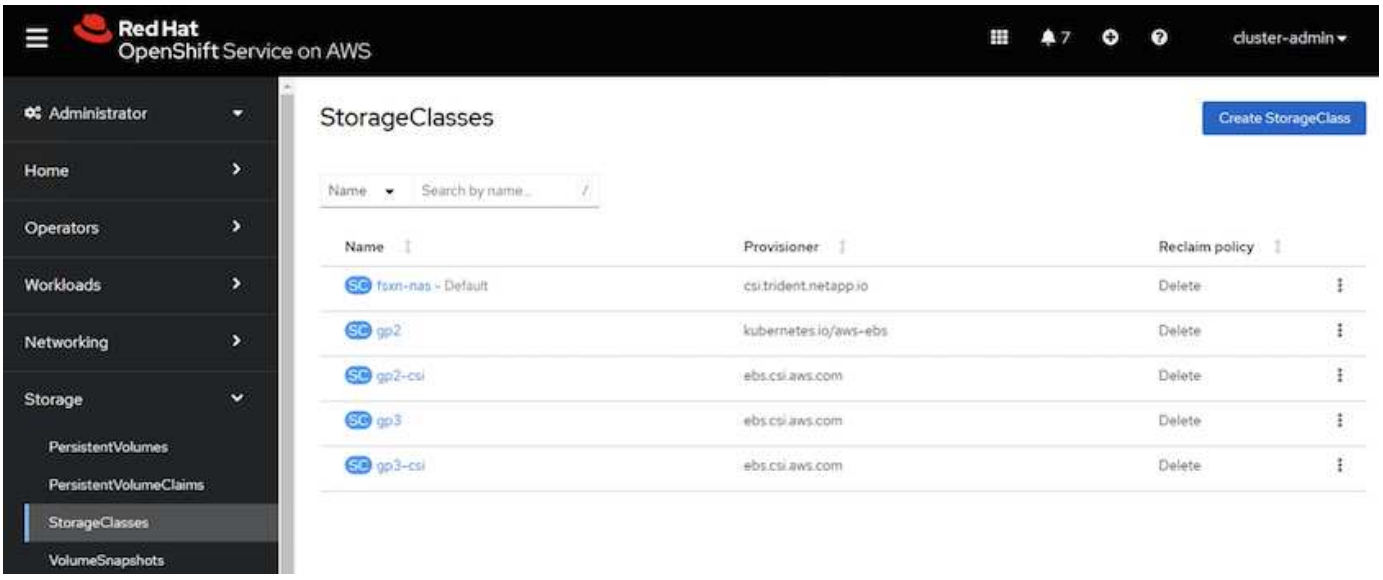
OpenShift GitOps peut être utilisé pour déployer Trident CSI sur tous les clusters gérés au fur et à mesure qu'ils sont enregistrés sur ArgoCD à l'aide d'ApplicationSet.

```yaml
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
```



Créer des classes backend et de stockage à l'aide de Trident (pour FSx ONTAP)

- Référer"ici" pour plus de détails sur la création d'un backend et d'une classe de stockage.
- Créez la classe de stockage créée pour FsxN avec Trident CSI par défaut à partir de 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. Consultez les instructions "ici".
- SetUp une nouvelle instance Argo CD pour le cluster. Consultez les instructions "ici".

Ouvrez la console d'Argo CD et déployez une application. Par exemple, vous pouvez déployer une application Jenkins à l'aide d'Argo CD avec un Helm Chart. Lors de la création de l'application, les informations suivantes

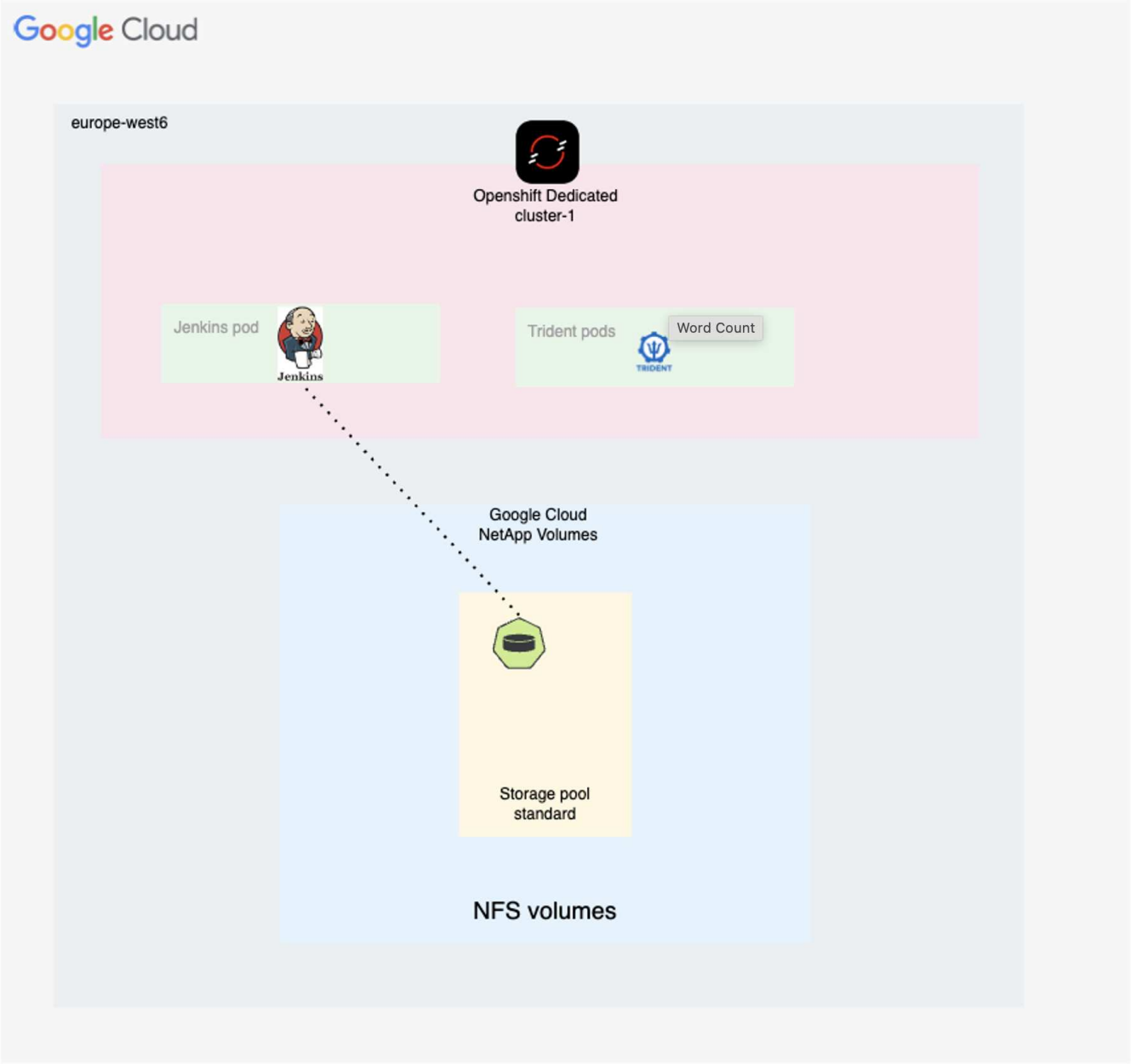
ont été fournies : Project: default cluster: 'https://kubernetes.default.svc'[] (sans les guillemets) Namespace: Jenkins L'URL du Helm Chart : 'https://charts.bitnami.com/bitnami'[] (sans les guillemets)

Paramètres Helm : global.storageClass : fsxn-nas

Déployer et configurer OpenShift Dedicated sur Google Cloud avec Google Cloud NetApp Volumes

Cette section décrit un flux de travail de haut niveau pour la configuration de clusters OpenShift Dedicated (OSD) sur la plate-forme Google Cloud. Il montre NetApp Trident utilisant Google Cloud NetApp Volumes comme backend de stockage pour fournir des volumes persistants pour les applications avec état exécutées avec Kubernetes.

Voici un diagramme qui illustre un cluster OSD déployé sur Google Cloud et utilisant NetApp Volumes comme stockage backend.



Le processus de configuration peut être décomposé selon les étapes suivantes :

Installer des clusters OSD dans Google Cloud

- Si vous souhaitez utiliser un VPC existant pour le cluster, vous devez créer le VPC, deux sous-réseaux, un routeur cloud et deux NAT cloud GCP pour le cluster OSD. Référer"ici" pour les instructions.
- Consultez "ici" pour obtenir des instructions sur l'installation de clusters OSD sur GCP à l'aide du modèle de facturation Customer Cloud Subscription (CCS). OSD est également disponible sur Google Cloud Marketplace. Une vidéo montrant comment installer OSD à l'aide de la solution Google Cloud Marketplace est disponible "ici".

Activer les Google Cloud NetApp Volumes

- Référer"ici" pour plus d'informations sur la configuration de l'accès à Google Cloud NetApp Volumes. Suivez toutes les étapes jusqu'à et y compris
- Créer un pool de stockage. Référer"ici" pour plus d'informations sur la configuration d'un pool de stockage sur Google Cloud NetApp Volumes. Les volumes pour les applications Kubernetes avec état exécutées sur OSD seront créés dans le pool de stockage.

Installer Trident sur les clusters OSD (à l'aide du graphique Helm)

- Utilisez un Helm chart pour installer Trident sur les clusters OSD. Consultez "ici" pour obtenir des instructions sur l'installation du Helm chart.

Intégration de NetApp Volumes avec NetApp Trident pour les clusters OSD

Créer des classes backend et de stockage à l'aide de Trident (pour Google Cloud NetApp Volumes)

- Consultez ici pour plus de détails sur la création du backend.
- Si l'une des classes de stockage actuelles dans Kubernetes est marquée comme par défaut, supprimez cette annotation en modifiant la classe de stockage.
- Créez au moins une classe de stockage pour les volumes NetApp avec le provisionneur Trident CSI. Faites d'une seule des classes de stockage la valeur par défaut à l'aide d'une annotation. Cela permettra à un PVC d'utiliser cette classe de stockage lorsqu'elle n'est pas explicitement appelée dans le manifeste PVC. Un exemple avec l'annotation est montré ci-dessous.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

Déployer une application à l'aide d'OpenShift GitOps (Argo CD)

- Installez l'opérateur OpenShift GitOps sur le cluster. Consultez les instructions "ici".
- SetUp une nouvelle instance Argo CD pour le cluster. Consultez les instructions "ici".

Ouvrez la console d'Argo CD et déployez une application. Par exemple, vous pouvez déployer une application Jenkins à l'aide d'Argo CD avec un Helm Chart. Lors de la création de l'application, les informations suivantes ont été fournies : Project: default cluster: 'https://kubernetes.default.svc'[] (sans les guillemets) Namespace: Jenkins L'URL du Helm Chart : 'https://charts.bitnami.com/bitnami'[] (sans les guillemets)

Protection des données

Pour plus de détails sur la protection et la migration des charges de travail conteneurisées à l'aide de Trident Protect, consultez la section suivante : "Protégez et migrez les applications conteneur à l'aide de Trident Protect"

Solutions NetApp Hybrid Multicloud supplémentaires pour les charges de travail Red Hat OpenShift

Voir les solutions complémentaires suivantes :

- "Solution de conteneurs Red Hat OpenShift sur site"
- "Solution de conteneur Red Hat OpenShift Service on AWS"
- "Solution de virtualisation Red Hat OpenShift sur site"
- "Solution de virtualisation Red Hat OpenShift Service on AWS"

Protégez vos données avec Trident Protect

Protection des données pour les applications conteneurisées dans la plateforme OpenShift Container à l'aide de Trident Protect

Cette section du document de référence fournit des détails sur la création d'instantanés et de sauvegardes d'applications conteneurisées à l'aide de Trident Protect. NetApp Trident Protect offre des capacités avancées de gestion des données applicatives qui améliorent la fonctionnalité et la disponibilité des applications Kubernetes avec état, soutenues par les systèmes de stockage NetApp ONTAP et le provisionneur de stockage NetApp Trident CSI. Trident Protect crée des instantanés et des sauvegardes d'applications. Cela signifie que des instantanés et des sauvegardes sont créés non seulement pour les données applicatives dans les volumes persistants, mais aussi pour les métadonnées applicatives. Les instantanés et les sauvegardes créés par Trident Protect peuvent être stockés dans n'importe lequel des stockages objet suivants et restaurés à partir de ceux-ci ultérieurement.

- AWS S3
- Stockage d'objets blob Azure
- Stockage Google Cloud
- ONTAP S3
- Grille de stockage
- Tout autre stockage compatible S3

Trident Protect utilise le modèle Kubernetes de contrôle d'accès basé sur les rôles (RBAC). Par défaut, Trident

Protect fournit un espace de noms système unique appelé trident-protect et son compte de service par défaut associé. Si vous avez une organisation avec de nombreux utilisateurs ou des besoins de sécurité spécifiques, vous pouvez utiliser les fonctionnalités RBAC de Trident Protect pour obtenir un contrôle plus granulaire sur l'accès aux ressources et aux espaces de noms.

Des informations supplémentaires sur le contrôle d'accès basé sur les rôles (RBAC) dans Trident Protect sont disponibles dans le "Documentation Trident Protect"

> ⓘ L'administrateur du cluster a accès aux ressources de l'espace de noms trident-protect par défaut et peut également accéder aux ressources de tous les autres espaces de noms. Les utilisateurs ne peuvent pas créer de ressources personnalisées de gestion des données d'application (CR) telles que des CR d'instantané et de sauvegarde dans l'espace de noms trident-protect. En tant que meilleure pratique, les utilisateurs devront créer ces CR dans l'espace de noms de l'application.

Trident Protect peut être installé en suivant les instructions fournies dans la documentation "ici". Cette section présentera le workflow pour la protection des données des applications conteneurisées et la restauration des applications à l'aide de Trident Protect. 1. Création d'un instantané (à la demande ou planifiée) 2. Restauration à partir d'un instantané (restauration dans le même espace de noms ou dans un espace de noms différent) 3. Création d'une sauvegarde 4. Restauration à partir d'une sauvegarde

▼ **Condition préalable**

Avant de créer les instantanés et les sauvegardes pour une application, le stockage d'objets doit être configuré dans Trident Protect pour stocker les instantanés et les sauvegardes. Cela se fait à l'aide de la CR bucket. Seuls les administrateurs peuvent créer une CR bucket et la configurer. La CR bucket est appelée AppVault dans Trident Protect. Les objets AppVault sont la représentation déclarative du workflow Kubernetes d'un bucket de stockage. Une CR AppVault contient les configurations nécessaires pour qu'un bucket soit utilisé dans les opérations de protection, telles que les sauvegardes, les instantanés, les opérations de restauration et la réplication SnapMirror.

Dans cet exemple, nous allons montrer l'utilisation de ONTAP S3 comme stockage d'objets. Voici le workflow pour créer un CR AppVault pour ONTAP S3 : 1. Créez un serveur de stockage d'objets S3 dans la SVM du cluster ONTAP. 2. Créez un bucket dans le serveur de stockage d'objets. 3. Créez un utilisateur S3 dans la SVM. Conservez la clé d'accès et la clé secrète en lieu sûr. 4. Dans OpenShift, créez un secret pour stocker les identifiants ONTAP S3. 5. Créez un objet AppVault pour ONTAP S3

Configurer Trident Protect AppVault pour ONTAP S3

Exemple de fichier YAML pour configurer Trident Protect avec ONTAP S3 comme AppVault

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
```

```
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

Exemple de fichier yaml pour l'installation de l'application postgresql

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
```

```
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ Créer des instantanés

Création d'un instantané à la demande

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+----------------+--------------+-----------+-----+-------+
|      NAME      |   APP REF    |   STATE   | AGE | ERROR |
+----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                        READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49   1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb     1         1         1       3h47m

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                  Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                  SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS          SNAPSHOTCONTENT
          CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                      53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                        368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

Création d'une planification À l'aide de la commande suivante, des instantanés seront créés quotidiennement à 15h33 et deux instantanés et sauvegardes seront conservés.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily --hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+----------------------+---------+-------+-----+-------+
|   NAME    |     APP     |       SCHEDULE       | ENABLED | STATE | AGE | ERROR |
+-----------+-------------+----------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+-------------+----------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

Création d'un planning à l'aide de yaml

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP     |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+-------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+-------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

Vous pouvez voir les instantanés créés selon ce calendrier.

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

Des instantanés de volume sont également créés.

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                  READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ **Supprimer l'application pour simuler la perte de l'application**

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ **Restaurer à partir d'un instantané vers le même espace de noms**

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

L'application et son PVC sont restaurés dans le même espace de noms.

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ Restaurer à partir d'un instantané vers un espace de noms différent

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

Vous pouvez voir que l'application a été restaurée dans un nouvel espace de noms.

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                  Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ Créer des sauvegardes

Création d'une sauvegarde à la demande

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+-------------+-----------+--------+-------+
|             NAME             |   APP REF   |   STATE   |  AGE   | ERROR |
+------------------------------+-------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1             | postgres-app | Completed | 6m19s  |       |
+------------------------------+-------------+-----------+--------+-------+
```

Création d’un calendrier de sauvegarde

Les sauvegardes quotidiennes et horaires de la liste ci-dessus sont créées à partir du calendrier défini précédemment.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ **Restaurer à partir d’une sauvegarde**

Supprimez l’application et les PVC pour simuler une perte de données.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Restaurer vers le même espace de noms #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" créé.

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

L’application et les PVC sont restaurés dans le même espace de noms.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w   1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                 Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

Restaurer vers un espace de noms différent Créer un nouvel espace de noms. Restaurer à partir d’une sauvegarde vers le nouvel espace de noms.

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                 Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ Migrer les applications

Pour cloner ou migrer une application vers un autre cluster (effectuer un clonage inter-cluster), créez une sauvegarde sur le cluster source, puis restaurez la sauvegarde sur un cluster différent. Assurez-vous que Trident Protect est installé sur le cluster de destination.

Sur le cluster source, effectuez les étapes comme indiqué dans l’image ci-dessous :

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

À partir du cluster source, basculez le contexte vers le cluster de destination. Ensuite, assurez-vous que l'AppVault est accessible à partir du contexte du cluster de destination et récupérez le contenu de l'AppVault à partir du cluster de destination.

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+---------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-------------------------------------------------------------------------------+
|    CLUSTER    |     APP     |  TYPE  |            NAME             |        TIMESTAMP        |
                    PATH                                                       |
+---------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-------------------------------------------------------------------------------+
| ocp-cluster11 | bbox        | backup | bboxbackup1                 | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                 |
| ocp-cluster11 | postgres-app | backup | backup1                     | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3             |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300  | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd  |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300  | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d  |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031 |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1    | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3    |
```

Utilisez le chemin de sauvegarde de la liste et créez un objet CR de sauvegarde et de restauration comme indiqué dans la commande ci-dessous.

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|          NAME            |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

Vous pouvez maintenant voir que les pods d'application et les pvc sont créés dans le cluster de destination.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                   READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                         STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Protégez les machines virtuelles dans Red Hat OpenShift Virtualization à l'aide de Trident Protect

Protégez les machines virtuelles dans OpenShift Virtualization à l'aide de snapshots et de sauvegardes. Cette procédure comprend la création d'un AppVault à l'aide du stockage d'objets ONTAP S3, la configuration de Trident Protect pour capturer les données des machines virtuelles, y compris les objets de ressources Kubernetes, les volumes persistants et les images internes, ainsi que la restauration des données si nécessaire.

Les machines virtuelles dans l'environnement de virtualisation OpenShift sont des applications conteneurisées qui s'exécutent dans les nœuds de travail de votre plateforme OpenShift Container. Il est important de protéger les métadonnées des machines virtuelles ainsi que les disques persistants des machines virtuelles, afin que lorsqu'elles sont perdues ou corrompues, vous puissiez les récupérer.

Les disques persistants des machines virtuelles OpenShift peuvent être soutenus par le stockage ONTAP intégré au cluster OpenShift à l'aide de "Trident CSI". Dans cette section, nous utilisons "Trident Protect" pour créer des instantanés et des sauvegardes des machines virtuelles, y compris leurs volumes de données, vers le stockage objet ONTAP.

Nous restaurons ensuite à partir d'un instantané ou d'une sauvegarde lorsque cela est nécessaire.

Trident Protect permet la création de snapshots, la sauvegarde, la restauration et la reprise après sinistre des applications et des machines virtuelles sur un cluster OpenShift. Pour les machines virtuelles OpenShift Virtualization, les données pouvant être protégées avec Trident Protect incluent les objets de ressources Kubernetes associés aux machines virtuelles, les volumes persistants et les images internes.

Voici les versions des différents composants utilisés pour les exemples de cette section

- "OpenShift Cluster 4.17"
- "OpenShift Virtualization installé via OpenShift Virtualization Operator fourni par Red Hat"
- "Trident 25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

Créer AppVault pour le stockage d'objets

▼ **Créer AppVault**

Avant de créer les instantanés et les sauvegardes pour une application ou une machine virtuelle, le stockage objet doit être configuré dans Trident Protect pour stocker les instantanés et les sauvegardes. Cela se fait à l'aide de la CR bucket. Seuls les administrateurs peuvent créer une CR bucket et la configurer. La CR bucket est appelée AppVault dans Trident Protect. Les objets AppVault sont la représentation déclarative du workflow Kubernetes d'un bucket de stockage. Une CR AppVault contient les configurations nécessaires pour qu'un bucket soit utilisé dans les opérations de protection, telles que les sauvegardes, les instantanés, les opérations de restauration et la réplication SnapMirror.

Dans cet exemple, nous allons montrer l'utilisation de ONTAP S3 comme stockage d'objets. Voici le workflow pour créer un AppVault CR pour ONTAP S3 : 1. Créez un serveur de stockage d'objets S3 dans la SVM dans ONTAP Cluster. 2. Créez un bucket dans le serveur de stockage d'objets. 3. Créez un utilisateur S3 dans la SVM. Conservez la clé d'accès et la clé secrète dans un endroit sûr. 4. Dans OpenShift, créez un secret pour stocker les identifiants ONTAP S3. 5. Créez un objet AppVault pour ONTAP S3

Configurer Trident Protect AppVault pour ONTAP S3

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
```

```
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+-------------------+----------+-----------+-------+---------+-------+
|       NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+-------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault | OntapS3  | Available |       |         | 8d17h |
+-------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

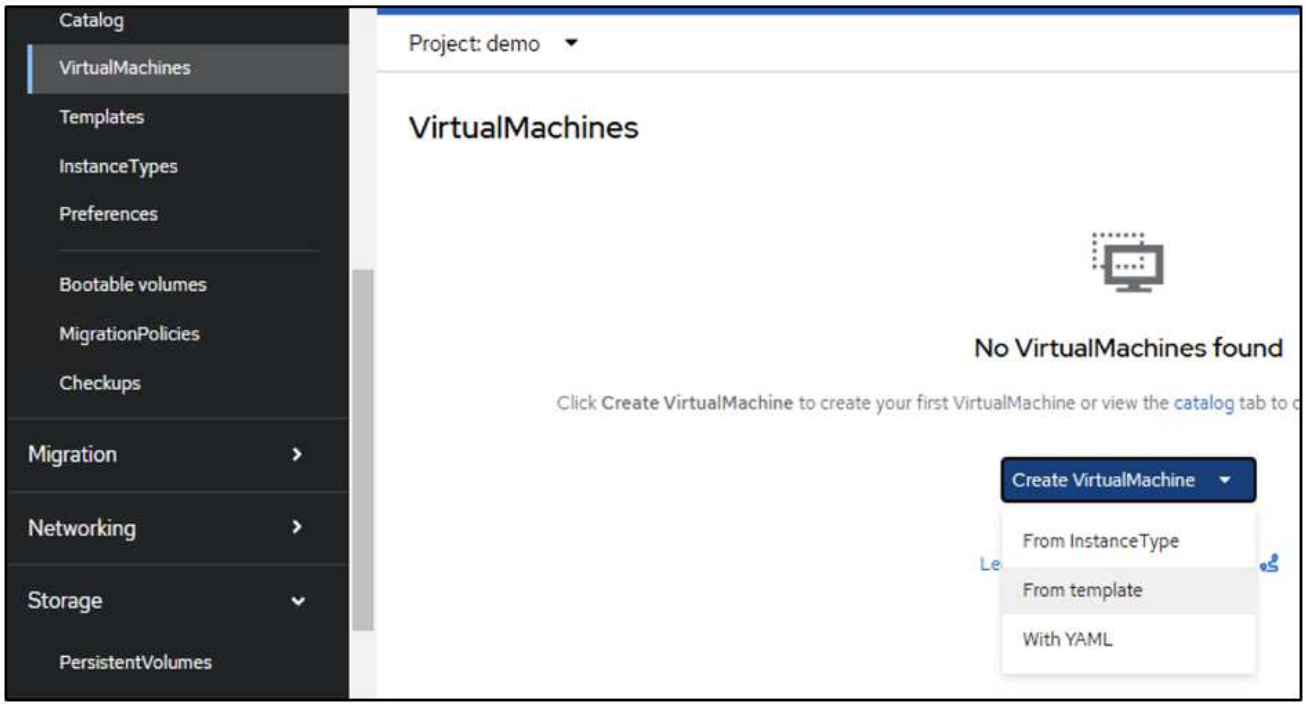
Créer une machine virtuelle dans OpenShift Virtualization

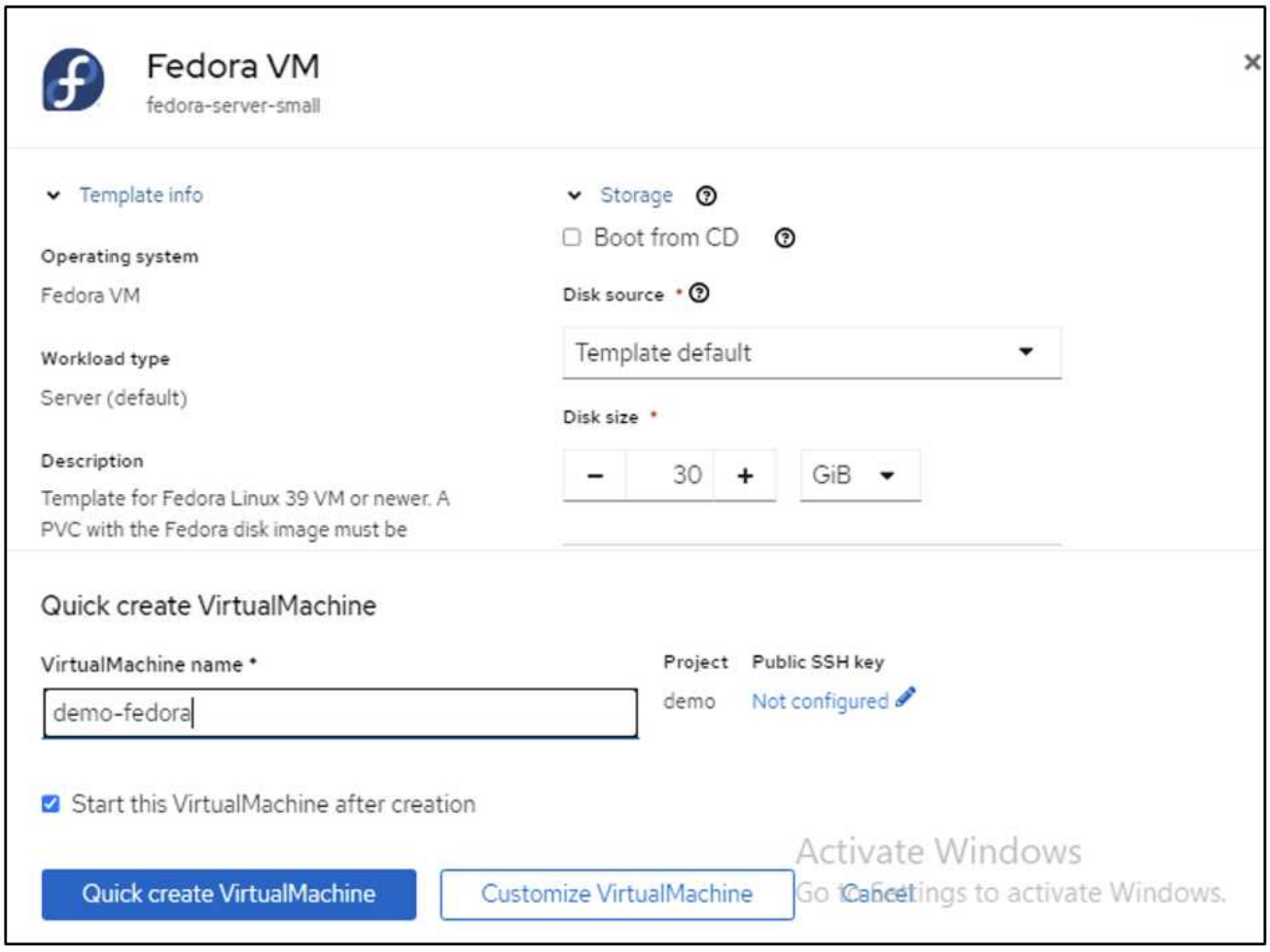
▼ **Créer une machine virtuelle dans OpenShift Virtualization**

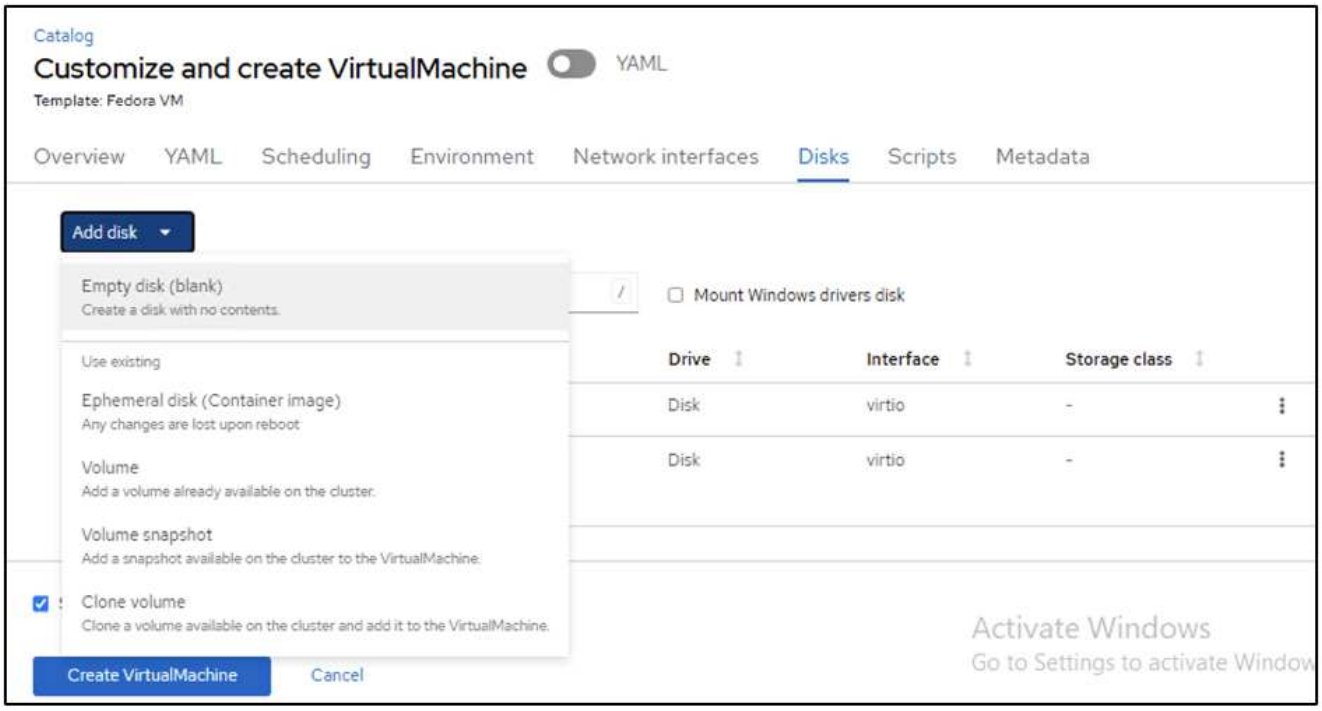
Les captures d'écran suivantes montrent la création de la VM (demo-fedora dans l'espace de noms demo) à partir de la console à l'aide du modèle. Le disque racine choisit automatiquement la classe de stockage par défaut. Vérifiez donc que la classe de stockage par défaut est définie de manière appropriée. Dans cette configuration, la classe de stockage par défaut est **sc-zonea-san**. Assurez-vous que lorsque vous créez le disque supplémentaire, vous choisissez la classe de stockage sc-zonea-san et cochez la case « **Appliquer les paramètres de stockage optimisés** ». Cela définira les modes d'accès sur RWX et le mode volume sur Bloquer.

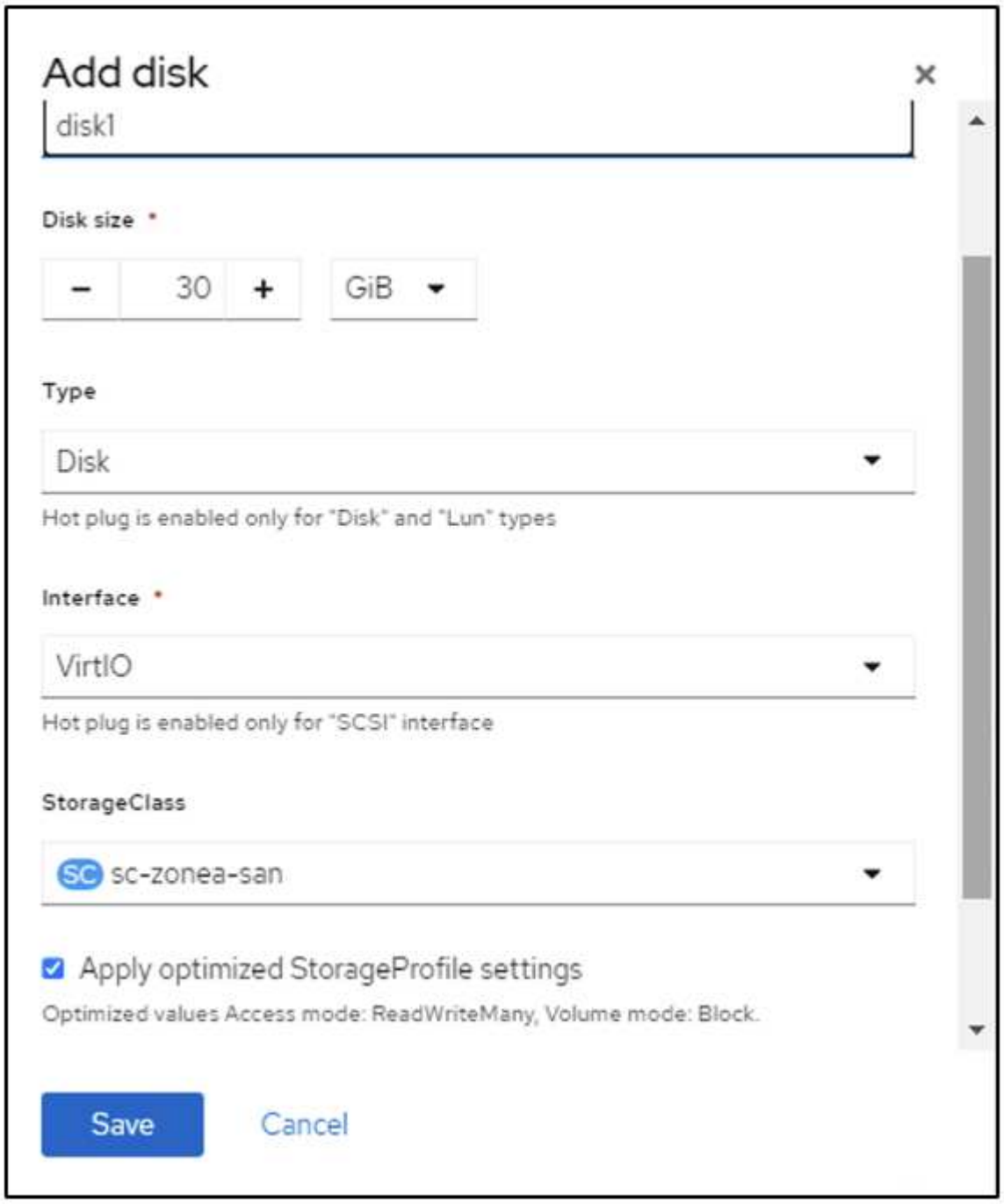
> ⓘ Trident prend en charge le mode d'accès RWX en mode Block Volume pour SAN (iSCSI, NVMe/TCP et FC). (C'est le mode d'accès par défaut pour le NAS). Le mode d'accès RWX est requis si vous devez effectuer une migration en direct des machines virtuelles ultérieurement.

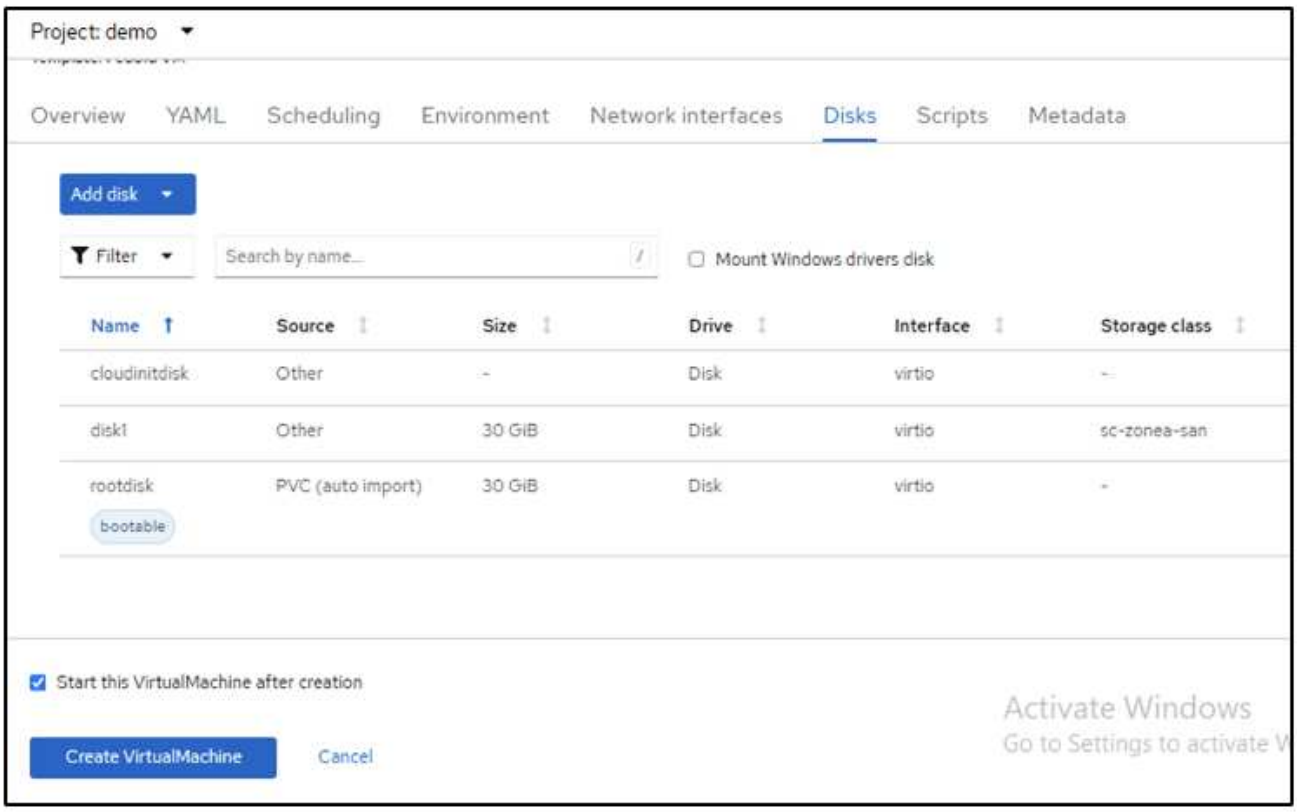



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Activate Windows
Go to Settings to activate Windows.
Quick create VirtualMachine
Customize VirtualMachine
Cancel


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Créer une application

▼ **Créer une application**

Créer une application Trident Protect pour la machine virtuelle

Dans l'exemple, le namespace de démonstration comporte une VM et toutes les ressources du namespace sont incluses lors de la création de l'app.

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
```

```
  namespace: demo
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

Protégez l'application en créant une sauvegarde

▼ **Créer des sauvegardes**

Créer une sauvegarde à la demande

Créez une sauvegarde pour l'application (demo-vm) créée précédemment qui inclut toutes les ressources de l'espace de noms de démonstration. Indiquez le nom de l'Appvault où les sauvegardes seront stockées.

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Créer des sauvegardes selon un calendrier

Créez une planification pour les sauvegardes en spécifiant la granularité et le nombre de sauvegardes à conserver.

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Restaurer à partir d'une sauvegarde

▼ **Restaurer à partir de sauvegardes**

Restaurer la machine virtuelle dans le même espace de noms

Dans l'exemple, la sauvegarde demo-vm-backup-on-demand contient la sauvegarde avec demo-app pour la VM Fedora.

Tout d'abord, supprimez la VM et assurez-vous que les PVC, le pod et les objets VM sont supprimés de l'espace de noms « demo »

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

Créez maintenant un objet de restauration de sauvegarde sur place.

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Vérifiez que la VM, les pods et les PVC sont restaurés

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                     Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Restaurer la machine virtuelle dans un espace de noms différent

Créez d'abord un nouvel espace de noms dans lequel vous souhaitez restaurer l'application, dans cet exemple demo2. Créez ensuite un objet de restauration de sauvegarde

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
```

```
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+---------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |   AGE   |
+----------------------+--------------------+-----------+-------+---------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+---------+
```

Vérifiez que la VM, les pods et les pvcs sont créés dans le nouvel espace de noms demo2.

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Protégez l'application à l'aide de snapshots

▼ **Créer des instantanés**

Créer un instantané à la demande Créez un instantané pour l'application et spécifiez le coffre d'applications dans lequel il doit être stocké.

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
```

```
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Créer un calendrier pour les instantanés Créez un calendrier pour les instantanés. Spécifiez la granularité et le nombre d'instantanés à conserver.

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-------------------------------------------+---------+----------------+-----------+-------+--------+
|                   NAME                    |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand                 | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000               | demo-vm | Delete         | Completed |       | 1m29s  |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Restaurer à partir d'un instantané

▼ Restaurer à partir d'un instantané

Restaurer la VM à partir du snapshot vers le même espace de noms Supprimez la VM demo-fedora de l'espace de noms demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

Créez un objet de restauration instantanée sur place à partir de l'instantané de la machine virtuelle.

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
```

```
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+----------------------------------+-------------------+-----------+-------+--------+
|               NAME               |     APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Vérifiez que la machine virtuelle et ses PVC sont créés dans l'espace de noms de démonstration.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                STATUS   VOLUME
persistentvolumeclaim/demo-fedora                   Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

Restaurer la machine virtuelle à partir du snapshot vers un espace de noms différent

Supprimez la machine virtuelle dans l'espace de noms demo2 précédemment restauré à partir de la sauvegarde.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                             Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                             Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34     Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

Créez l'objet de restauration d'instantané à partir de l'instantané et fournissez le mappage d'espace de noms.

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+--------------------+-----------+-------+--------+
|                NAME               |      APPVAULT      |   STATE   | ERROR |  AGE   |
+-----------------------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+--------------------+-----------+-------+--------+
```

Vérifiez que la VM et ses PVC sont restaurés dans le nouvel espace de noms demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san   <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san   <unset>                 29h
[root@localhost RedHat]#
```

Restaurer une machine virtuelle spécifique

▼ Sélection de machines virtuelles spécifiques dans un espace de noms pour créer des instantanés/sauvegardes et restaurer

Dans l'exemple précédent, nous avions une seule machine virtuelle dans un espace de noms. En incluant l'intégralité de l'espace de noms dans la sauvegarde, toutes les ressources associées à cette machine virtuelle ont été capturées. Dans l'exemple suivant, nous ajoutons une autre machine virtuelle au même espace de noms et créons une application uniquement pour cette nouvelle machine virtuelle à l'aide d'un sélecteur d'étiquettes.

Créez une nouvelle VM (demo-centos vm) dans l'espace de noms de démonstration

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora   81m     Running   True

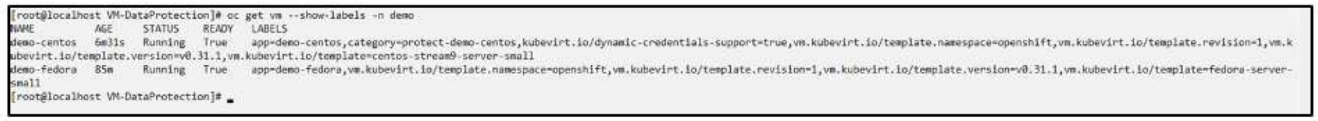
NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

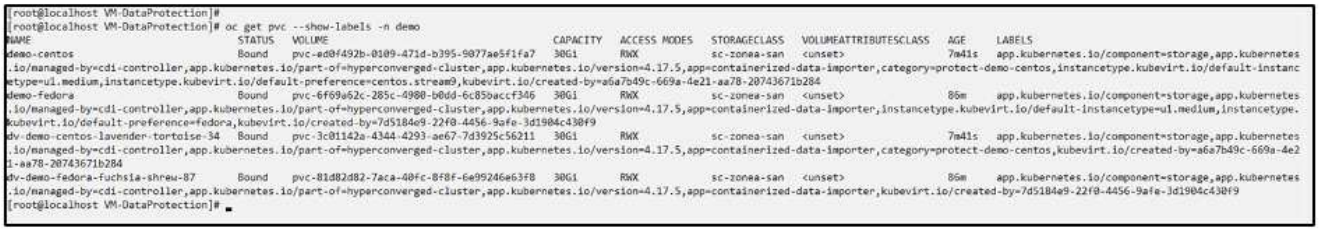
NAME                                                    STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                       Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                       Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Étiquetez la machine virtuelle demo-centos et ses ressources associées

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

Vérifiez que la machine virtuelle demo-centos et les pvcs ont les étiquettes





Créez une application pour une machine virtuelle spécifique (demo-centos) à l'aide du sélecteur d'étiquettes

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+------------------+------------+-------+------+
|      NAME        | NAMESPACES | STATE | AGE  |
+------------------+------------+-------+------+
| demo-centos-app  | demo       | Ready | 56s  |
| demo-vm          | demo       | Ready | 4h6m |
+------------------+------------+-------+------+
```

La méthode de création de sauvegardes et d'instantanés à la demande et selon une planification est la même que celle indiquée précédemment. Étant donné que l'application Trident-Protect utilisée pour créer les instantanés ou les sauvegardes ne contient que la machine virtuelle spécifique de l'espace de noms, la restauration à partir de ces derniers ne restaure qu'une machine virtuelle spécifique. Un exemple d'opération de sauvegarde/restauration est présenté ci-dessous.

Créer une sauvegarde d'une machine virtuelle spécifique dans un espace de noms en utilisant son application correspondante

Dans les étapes précédentes, une application a été créée à l'aide de sélecteurs d'étiquettes pour inclure uniquement la machine virtuelle centos dans l'espace de noms de démonstration. Créez une sauvegarde (sauvegarde à la demande, dans cet exemple) pour cette application.

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME             |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+------------------------------+-----------------+----------------+-----------+-------+--------+
```

Restaurer une VM spécifique dans le même espace de noms La sauvegarde d'une VM spécifique (centos) a été créée à l'aide de l'application correspondante. Si une sauvegarde sur place ou une restauration de sauvegarde est créée à partir de cela, seule cette machine virtuelle spécifique est restaurée. Supprimez la machine virtuelle Centos.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora   4m27s   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                    STATUS   VOLUME
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

Créez une restauration de sauvegarde sur place à partir de demo-centos-backup-on-demand et vérifiez que la machine virtuelle Centos a été recréée.

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

Activate
Go to Sett

Restaurer une machine virtuelle spécifique vers un espace de noms différent Créez une restauration de sauvegarde vers un espace de noms différent (demo3) à partir de demo-centos-backup-on-demand et vérifiez que la machine virtuelle centos a été recréée.

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

Démonstration vidéo

La vidéo suivante montre une démonstration de la protection d'une machine virtuelle à l'aide de snapshots

Protéger une machine virtuelle

Protégez les applications conteneurisées à l'aide d'outils tiers

Protection des données pour les applications conteneurisées dans OpenShift Container Platform à l'aide de l'API OpenShift pour la protection des données (OADP)

Cette section du document de référence fournit des détails sur la création de sauvegardes d'applications conteneurisées à l'aide de l'API OpenShift pour la protection des données (OADP) avec Velero sur NetApp ONTAP S3 ou NetApp StorageGRID S3. Les sauvegardes des ressources limitées à l'espace de noms, y compris les volumes persistants (PV) de l'application, sont créées à l'aide de snapshots CSI Trident .

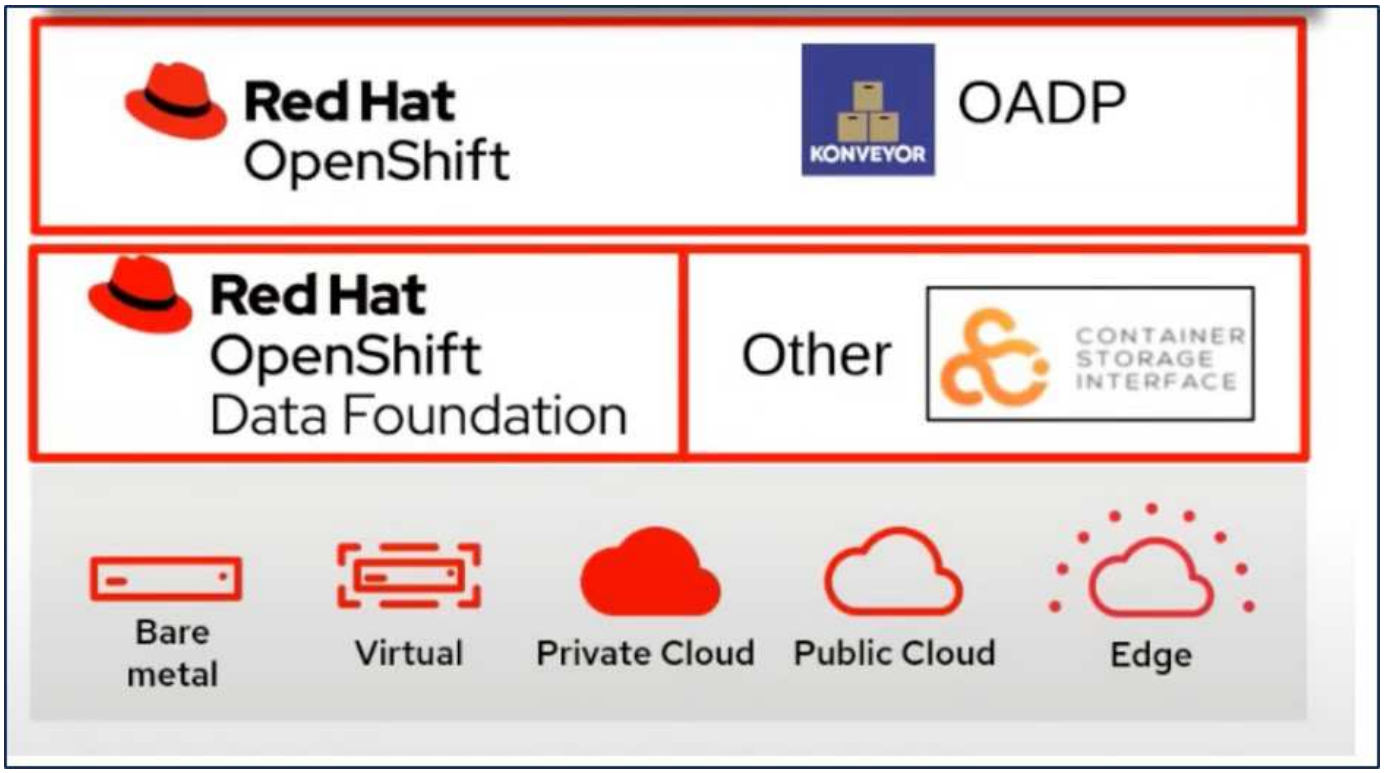
Le stockage persistant des applications conteneurisées peut être assuré par le stockage ONTAP intégré au

cluster OpenShift à l'aide de "Trident CSI". Dans cette section, nous utilisons "API OpenShift pour la protection des données (OADP)" pour effectuer la sauvegarde des applications, y compris de leurs volumes de données, vers

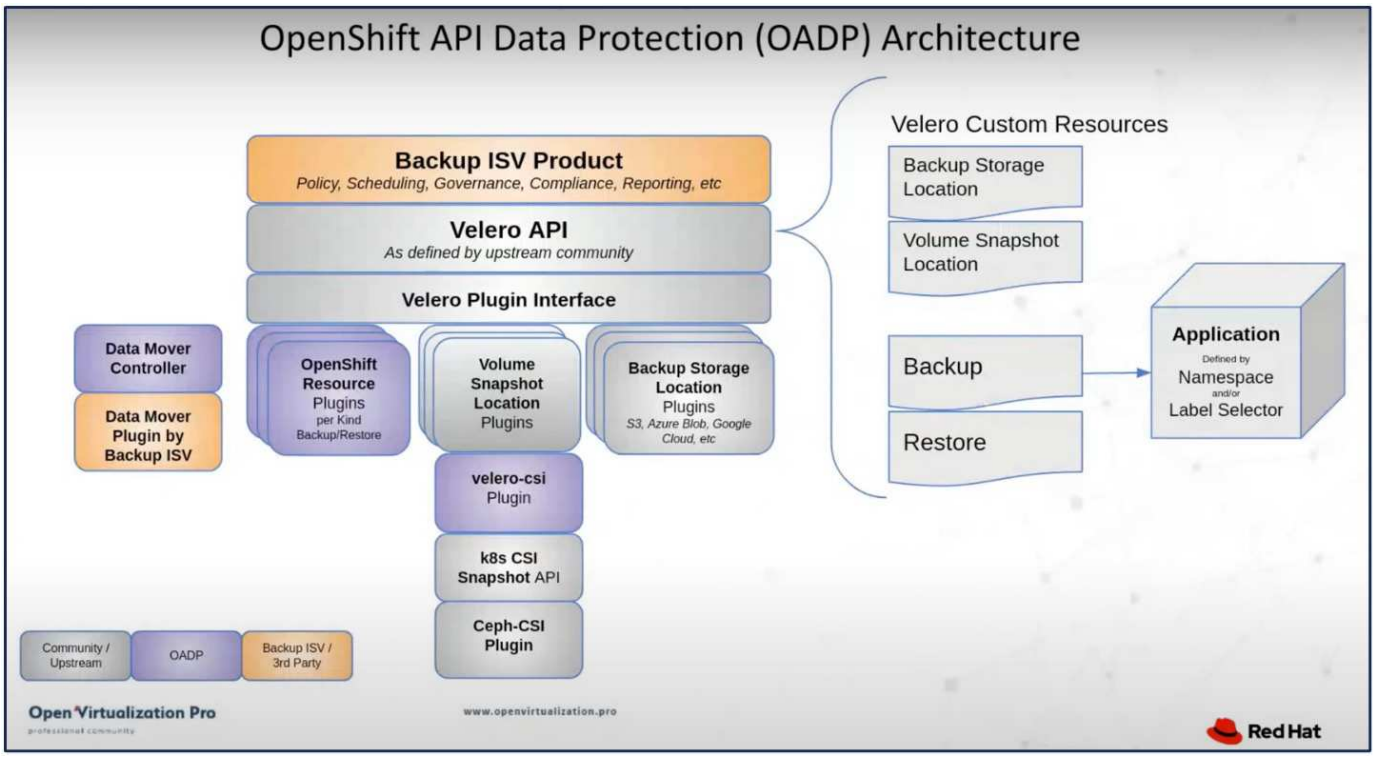
- Stockage d'objets ONTAP
- Grille de stockage

Nous restaurons ensuite à partir de la sauvegarde lorsque cela est nécessaire. Veuillez noter que l'application ne peut être restaurée que sur le cluster à partir duquel la sauvegarde a été créée.

OADP permet la sauvegarde, la restauration et la reprise après sinistre des applications sur un cluster OpenShift. Les données qui peuvent être protégées avec OADP incluent les objets de ressources Kubernetes, les volumes persistants et les images internes.



Red Hat OpenShift a exploité les solutions développées par les communautés OpenSource pour la protection des données. "Velero" est un outil open source permettant de sauvegarder et de restaurer en toute sécurité, d'effectuer une reprise après sinistre et de migrer les ressources de cluster Kubernetes et les volumes persistants. Pour utiliser Velero facilement, OpenShift a développé l'opérateur OADP et le plugin Velero pour s'intégrer aux pilotes de stockage CSI. Le cœur des API OADP exposées est basé sur les API Velero. Après avoir installé l'opérateur OADP et l'avoir configuré, les opérations de sauvegarde/restauration qui peuvent être effectuées sont basées sur les opérations exposées par l'API Velero.



OADP 1.3 est disponible à partir du hub opérateur du cluster OpenShift 4.12 et versions ultérieures. Il dispose d'un Data Mover intégré qui peut déplacer des instantanés de volume CSI vers un magasin d'objets distant. Cela offre portabilité et durabilité en déplaçant les instantanés vers un emplacement de stockage d'objets pendant la sauvegarde. Les instantanés sont ensuite disponibles pour restauration après sinistre.

Voici les versions des différents composants utilisés pour les exemples de cette section

- OpenShift Cluster 4.14
- Opérateur OADP 1.13 fourni par Red Hat
- Velero CLI 1.13 pour Linux
- Trident 24.02
- ONTAP 9.12
- postgresql installé en utilisant helm.

"Trident CSI" "API OpenShift pour la protection des données (OADP)" "Velero"

Installation de l'opérateur OpenShift API for Data Protection (OADP)

Cette section décrit l'installation de l'opérateur OpenShift API for Data Protection (OADP).

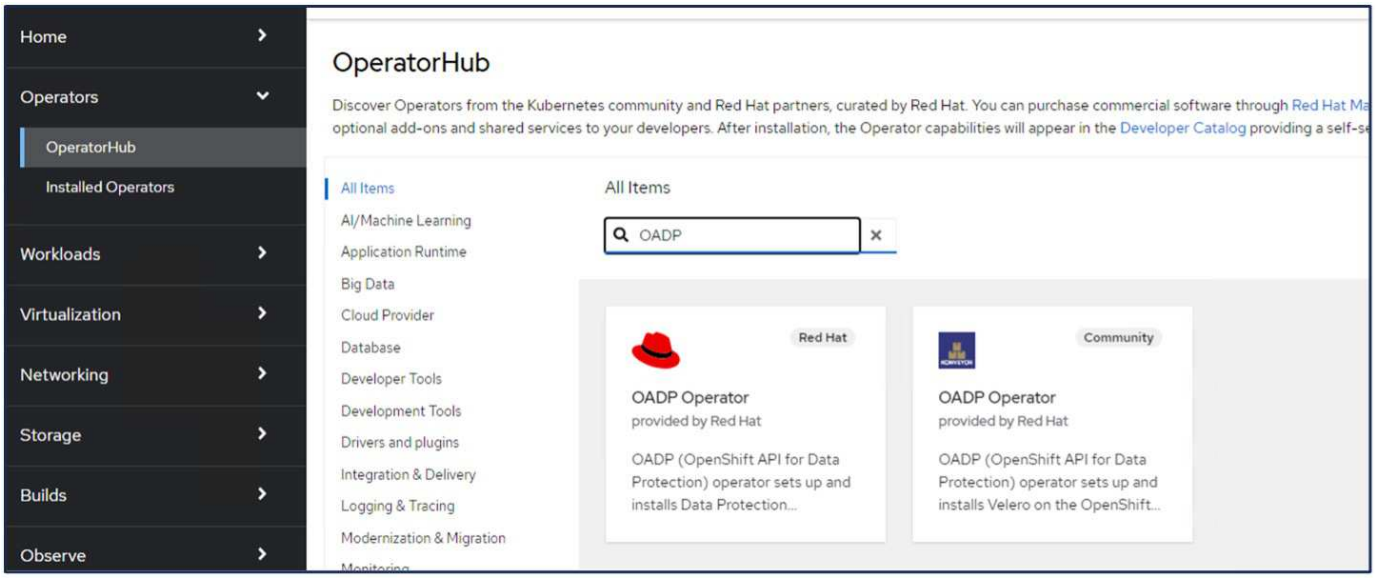
Prérequis

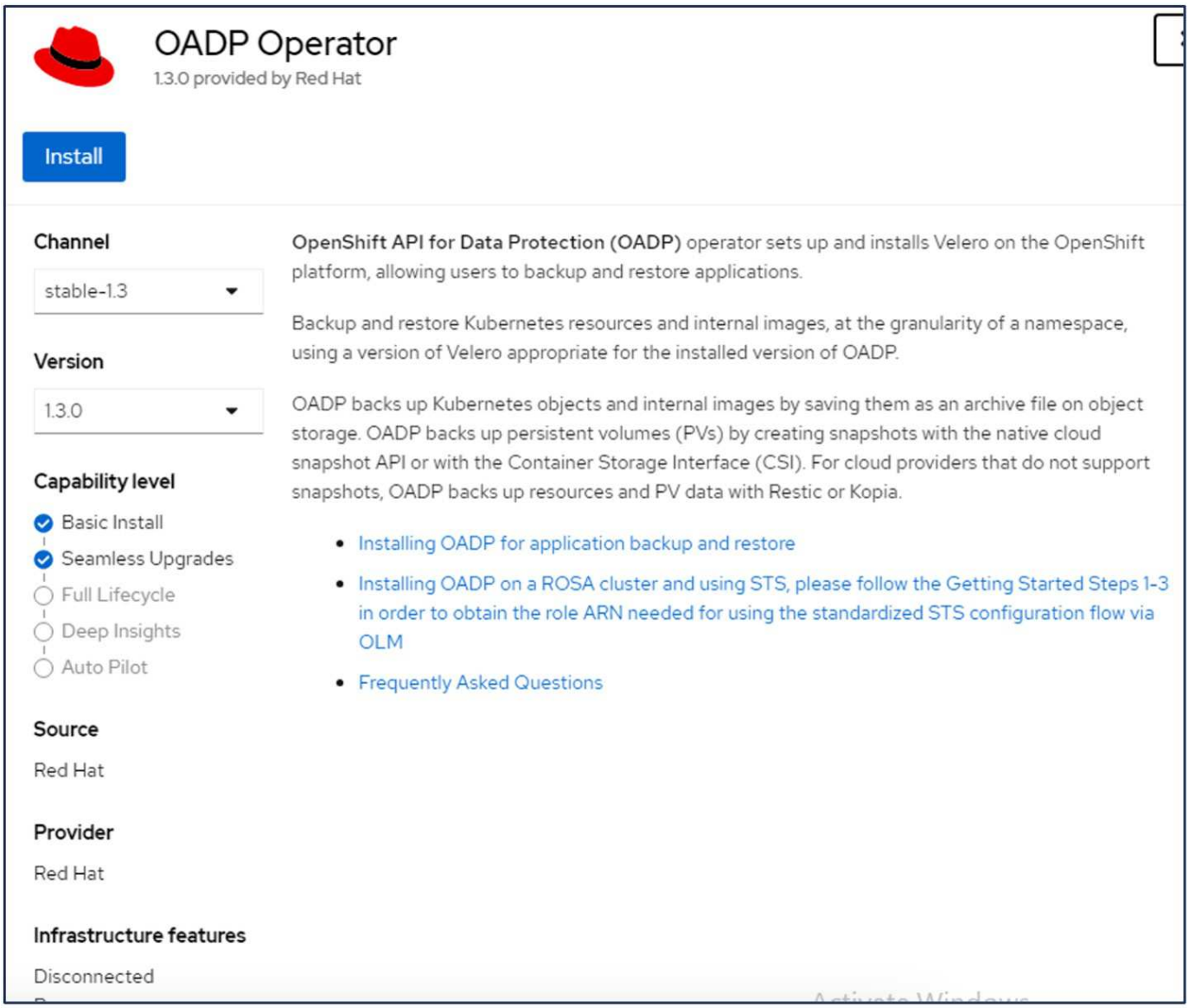
- Un cluster Red Hat OpenShift (version ultérieure à la version 4.12) installé sur une infrastructure bare-metal avec des nœuds de travail RHCOS
- Un cluster NetApp ONTAP intégré au cluster à l'aide de Trident
- Un backend Trident configuré avec un SVM sur un cluster ONTAP
- Une StorageClass configurée sur le cluster OpenShift avec Trident comme provisionneur

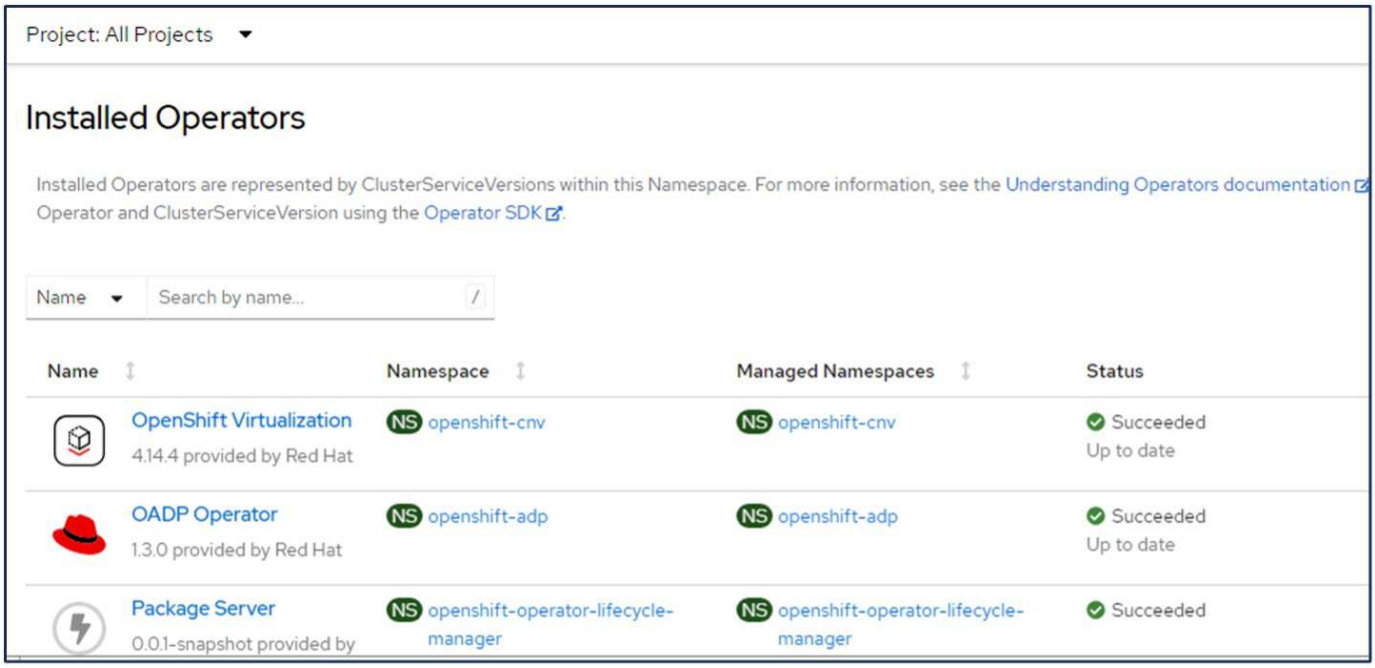
- Classe Trident Snapshot créée sur le cluster
- Accès administrateur du cluster au cluster Red Hat OpenShift
- Accès administrateur au cluster NetApp ONTAP
- Une application, par exemple postgresql, déployée sur le cluster
- Un poste de travail administrateur avec les outils tridentctl et oc installés et ajoutés à $PATH

Étapes d'installation de l'opérateur OADP

1. Accédez au hub opérateur du cluster et sélectionnez l'opérateur Red Hat OADP. Dans la page Installer, utilisez toutes les sélections par défaut et cliquez sur Installer. Sur la page suivante, utilisez à nouveau tous les paramètres par défaut et cliquez sur Installer. L'opérateur OADP sera installé dans l'espace de noms openshift-adp.




OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions


Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation
Operator and ClusterServiceVersion using the Operator SDK
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
Succeeded
Up to date
OADP Operator
1.3.0 provided by Red Hat
openshift-adp
openshift-adp
Succeeded
Up to date
Package Server
0.0.1-snapshot provided by
openshift-operator-lifecycle-manager
openshift-operator-lifecycle-manager
Succeeded

Prérequis pour la configuration de Velero avec Ontap S3

Une fois l'installation de l'opérateur réussie, configurez l'instance de Velero. Velero peut être configuré pour utiliser le stockage d'objets compatible S3. Configurez ONTAP S3 à l'aide des procédures indiquées dans le"Section Gestion du stockage d'objets de la documentation ONTAP" . Vous aurez besoin des informations suivantes de votre configuration ONTAP S3 pour l'intégration avec Velero.

- Une interface logique (LIF) qui peut être utilisée pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3 qui incluent la clé d'accès et la clé d'accès secrète
- Un nom de bucket dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage d'objets, le certificat TLS doit être installé sur le serveur de stockage d'objets.

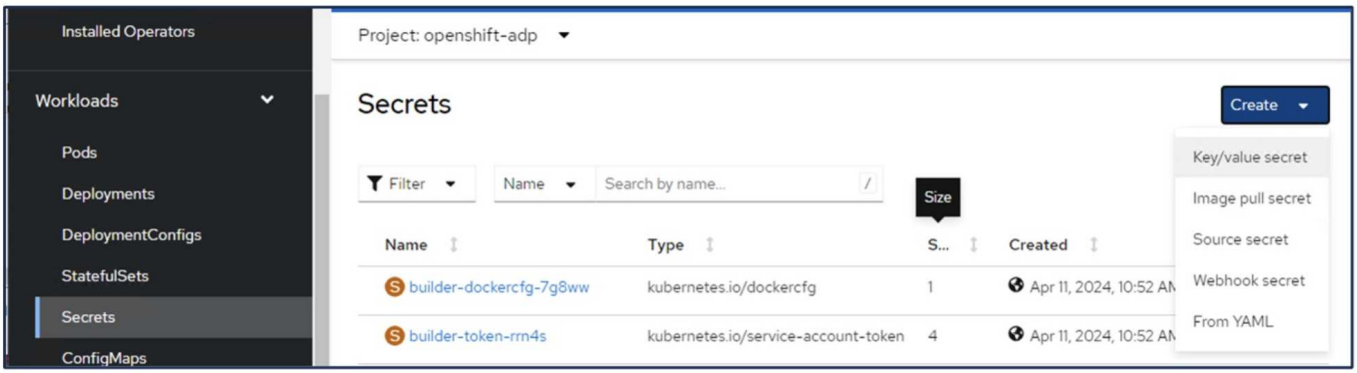
Prérequis pour la configuration de Velero avec StorageGrid S3

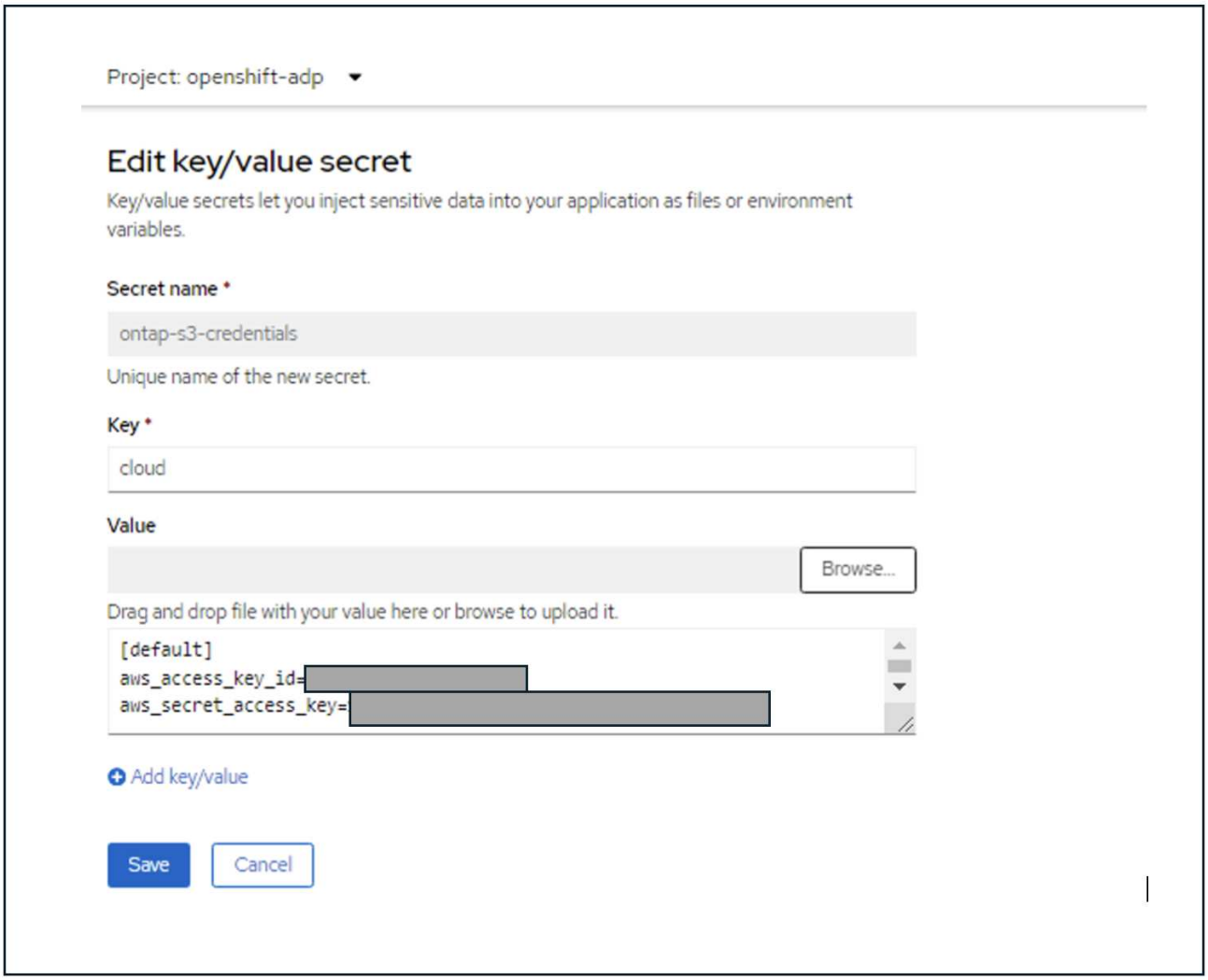
Velero peut être configuré pour utiliser le stockage d'objets compatible S3. Vous pouvez configurer StorageGrid S3 en utilisant les procédures indiquées dans le"Documentation de StorageGrid" . Vous aurez besoin des informations suivantes de votre configuration StorageGrid S3 pour l'intégrer à Velero.

- Le point de terminaison qui peut être utilisé pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3 qui incluent la clé d'accès et la clé d'accès secrète
- Un nom de bucket dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage d'objets, le certificat TLS doit être installé sur le serveur de stockage d'objets.

Étapes pour configurer Velero

- Tout d'abord, créez un secret pour les informations d'identification d'un utilisateur ONTAP S3 ou d'un locataire StorageGrid. Cela sera utilisé pour configurer Velero plus tard. Vous pouvez créer un secret à partir de la CLI ou de la console Web. Pour créer un secret à partir de la console Web, sélectionnez Secrets, puis cliquez sur Clé/Valeur secrète. Fournissez les valeurs pour le nom des informations d'identification, la clé et la valeur comme indiqué. Assurez-vous d'utiliser l'ID de clé d'accès et la clé d'accès secrète de votre utilisateur S3. Nommez le secret de manière appropriée. Dans l'exemple ci-dessous, un secret avec les informations d'identification de l'utilisateur ONTAP S3 nommé ontap-s3-credentials est créé.





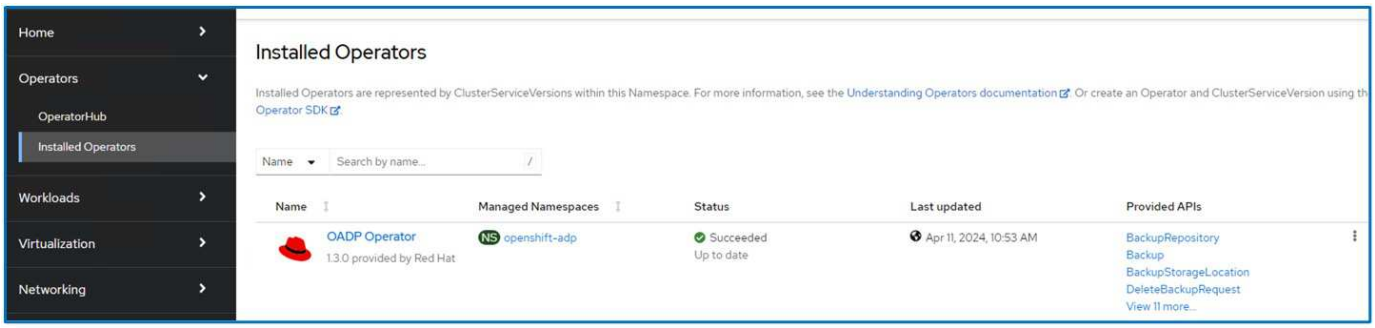
Pour créer un secret nommé sg-s3-credentials à partir de la CLI, vous pouvez utiliser la commande suivante.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

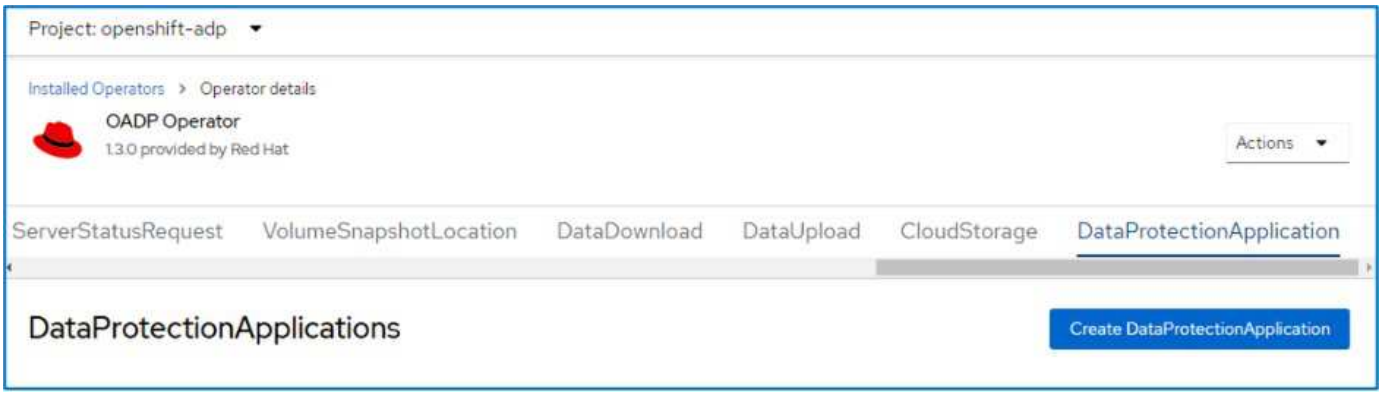
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- Ensuite, pour configurer Velero, sélectionnez Opérateurs installés dans l'élément de menu sous Opérateurs, cliquez sur Opérateur OADP, puis sélectionnez l'onglet **DataProtectionApplication**.



Cliquez sur Créer une application de protection des données. Dans la vue formulaire, indiquez un nom pour l'application DataProtection ou utilisez le nom par défaut.



Accédez maintenant à la vue YAML et remplacez les informations de spécification comme indiqué dans les exemples de fichiers yaml ci-dessous.

Exemple de fichier YAML pour la configuration de Velero avec ONTAP S3 comme emplacement de sauvegarde

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
```

```
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

Exemple de fichier YAML pour la configuration de Velero avec StorageGrid S3 comme emplacement de sauvegarde

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
```

```
        - openshift
        - aws
        - kubevirt
```

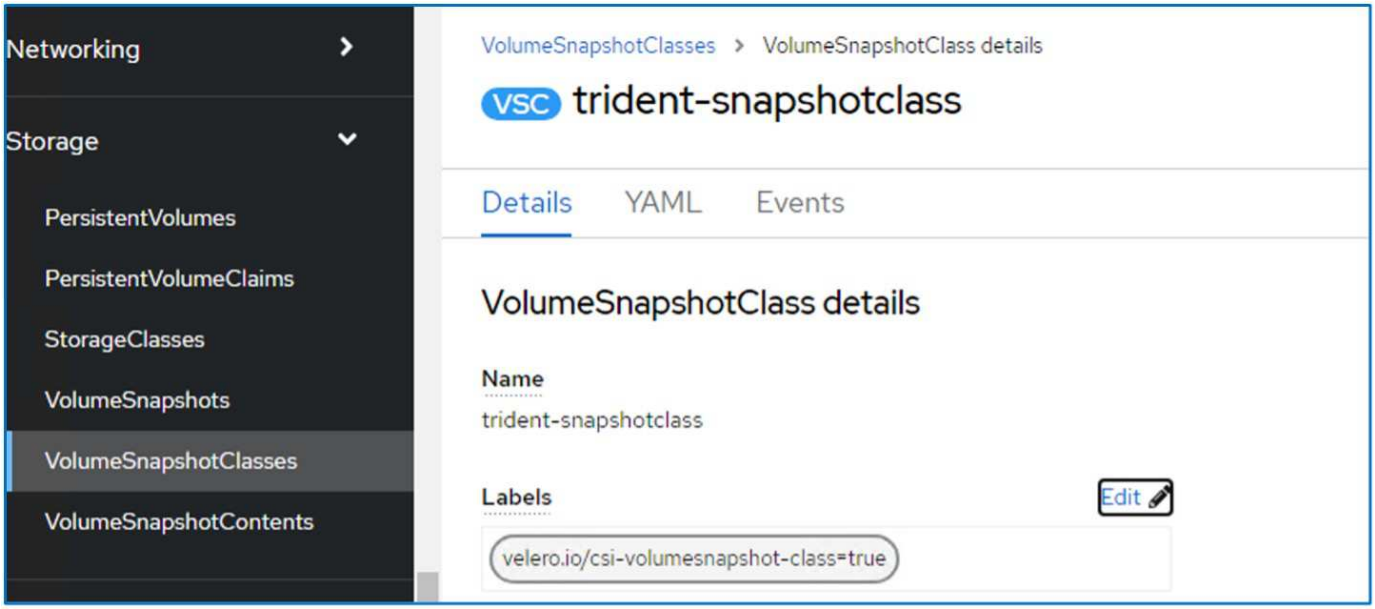
La section spec dans le fichier yaml doit être configurée de manière appropriée pour les paramètres suivants, similaires à l'exemple ci-dessus

backupLocations ONTAP S3 ou StorageGrid S3 (avec ses informations d'identification et autres informations telles qu'indiquées dans le fichier yaml) est configuré comme BackupLocation par défaut pour velero.

snapshotLocations Si vous utilisez des snapshots Container Storage Interface (CSI), vous n'avez pas besoin de spécifier un emplacement de snapshot, car vous créerez un CR VolumeSnapshotClass pour enregistrer le pilote CSI. Dans notre exemple, vous utilisez Trident CSI et vous avez précédemment créé VolumeSnapShotClass CR à l'aide du pilote Trident CSI.

Activer le plugin CSI Ajoutez csi aux plugins par défaut pour Velero pour sauvegarder les volumes persistants avec des instantanés CSI. Les plugins Velero CSI, pour sauvegarder les PVC sauvegardés par CSI, choisiront le VolumeSnapshotClass dans le cluster sur lequel l'étiquette **velero.io/csi-volumesnapshot-class** est définie. Pour ça

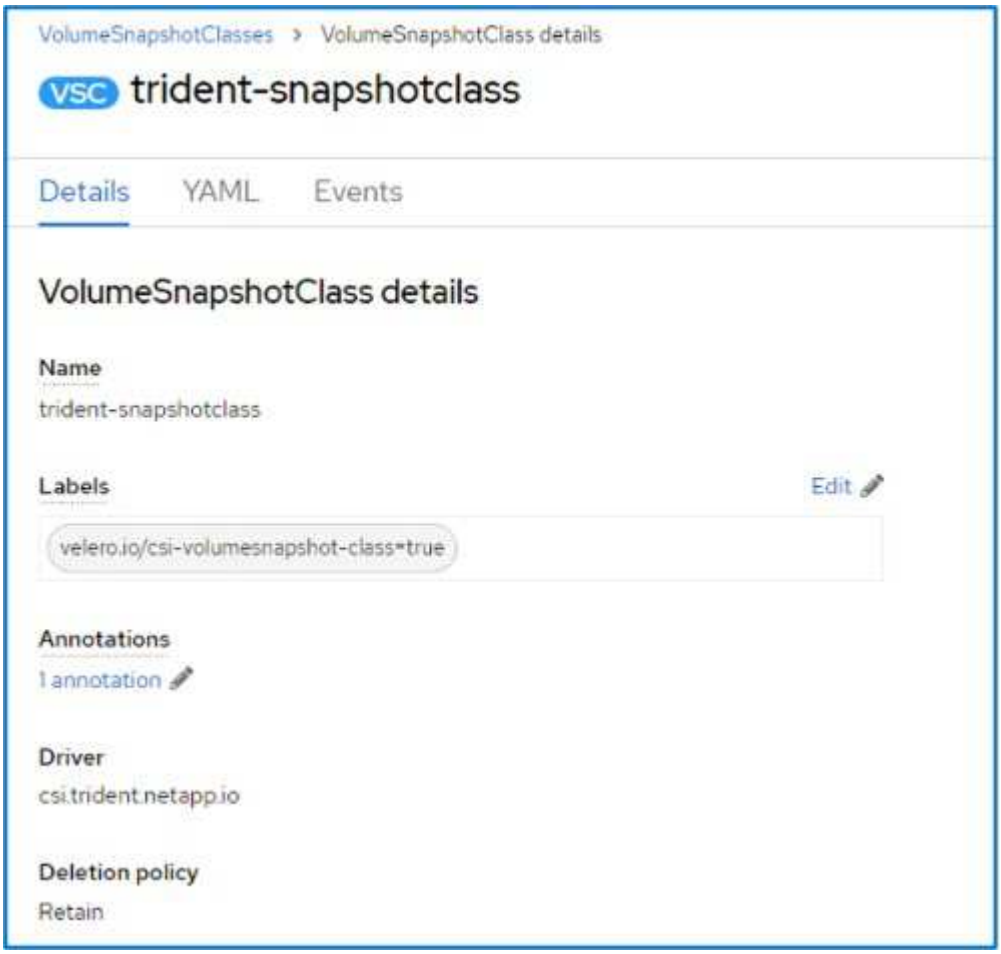
- Vous devez avoir créé le trident VolumeSnapshotClass.
- Modifiez l'étiquette de trident-snapshotclass et définissez-la sur **velero.io/csi-volumesnapshot-class=true** comme indiqué ci-dessous.



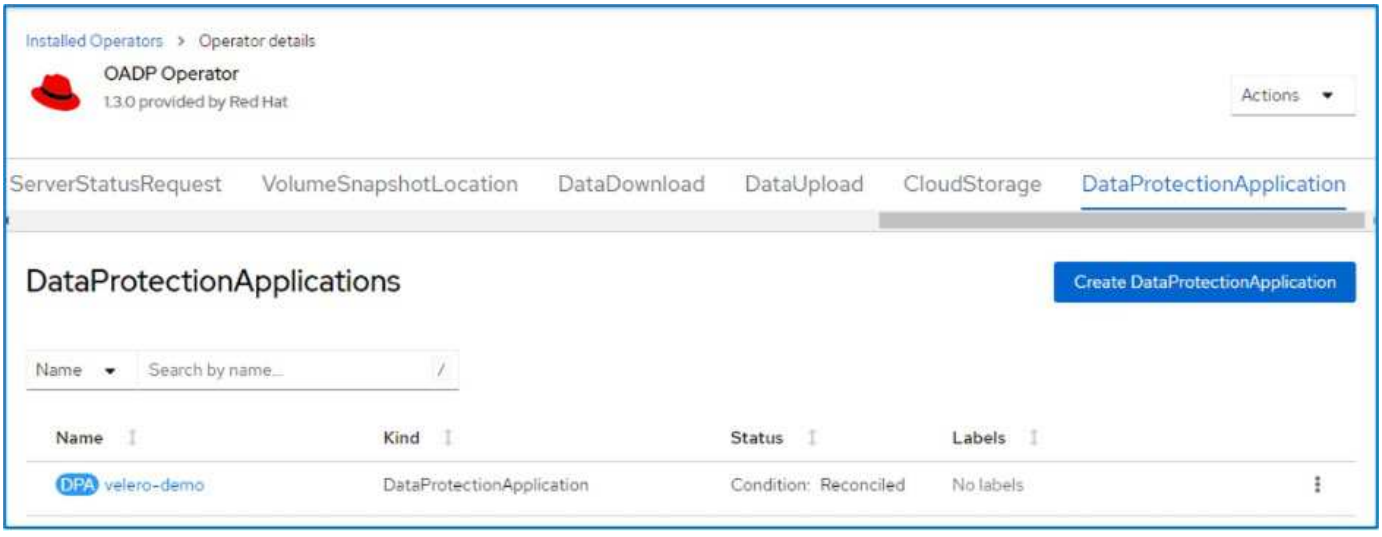
Assurez-vous que les instantanés peuvent persister même si les objets VolumeSnapshot sont supprimés. Cela peut être fait en définissant **deletionPolicy** sur Retain. Dans le cas contraire, la suppression d'un espace de noms entraînera la perte complète de tous les PVC sauvegardés dans celui-ci.

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
```

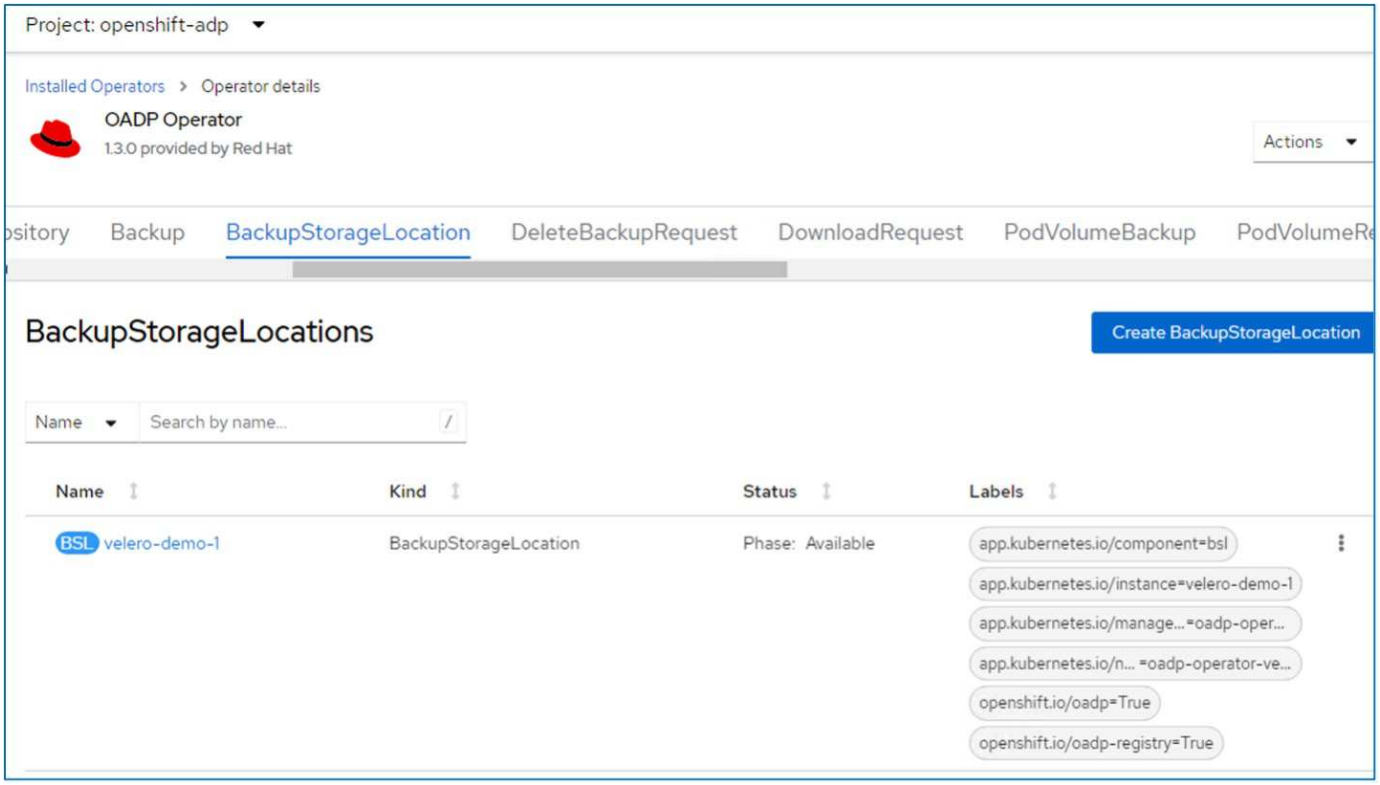
```
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Assurez-vous que DataProtectionApplication est créée et qu'elle est dans l'état : Réconcilié.



L'opérateur OADP créera un BackupStorageLocation correspondant. Celui-ci sera utilisé lors de la création d'une sauvegarde.



Création d'une sauvegarde à la demande pour les applications dans OpenShift Container Platform

Cette section décrit comment créer une sauvegarde à la demande pour les machines virtuelles dans OpenShift Virtualization.

Étapes pour créer une sauvegarde d'une application

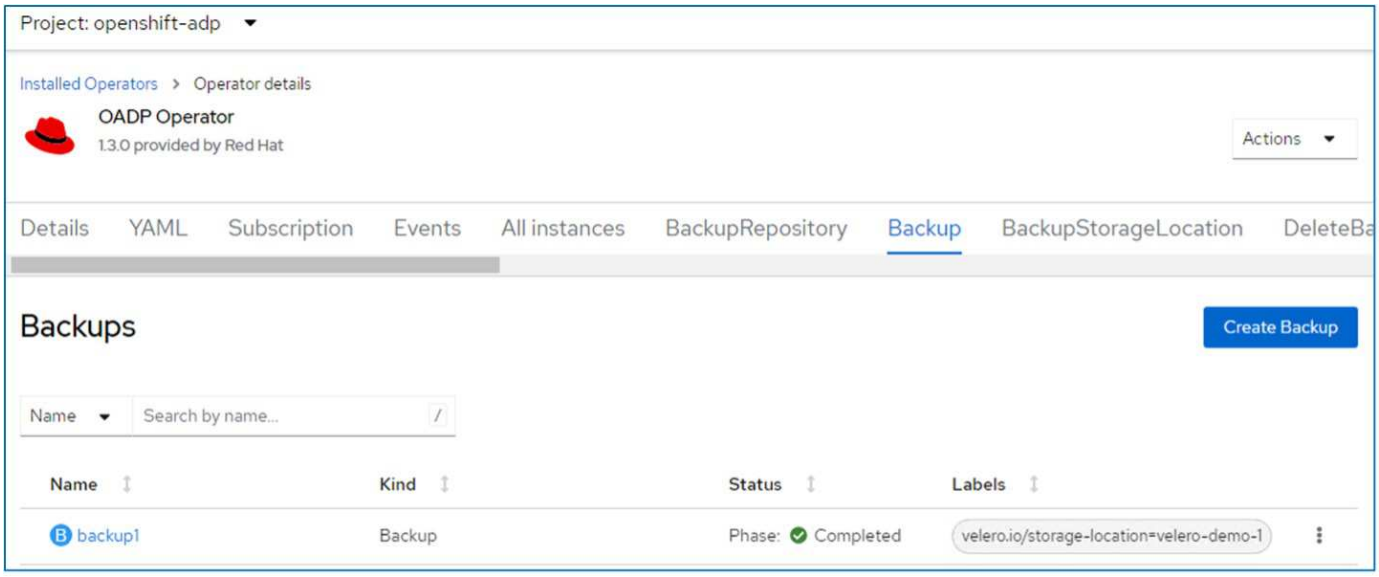
Pour créer une sauvegarde à la demande d'une application (métadonnées de l'application et volumes persistants de l'application), cliquez sur l'onglet **Backup** pour créer une ressource personnalisée Backup (CR). Un exemple de fichier yaml est fourni pour créer la ressource personnalisée Backup. À l'aide de ce fichier yaml, l'application et son stockage persistant dans l'espace de noms spécifié seront sauvegardés. Des paramètres supplémentaires peuvent être définis, comme indiqué dans "documentation".

Un instantané des volumes persistants et des ressources d'application dans l'espace de noms spécifié sera créé par le CSI. Cet instantané sera stocké dans l'emplacement de sauvegarde spécifié dans le yaml. La sauvegarde restera dans le système pendant 30 jours comme spécifié dans le ttl.

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
```

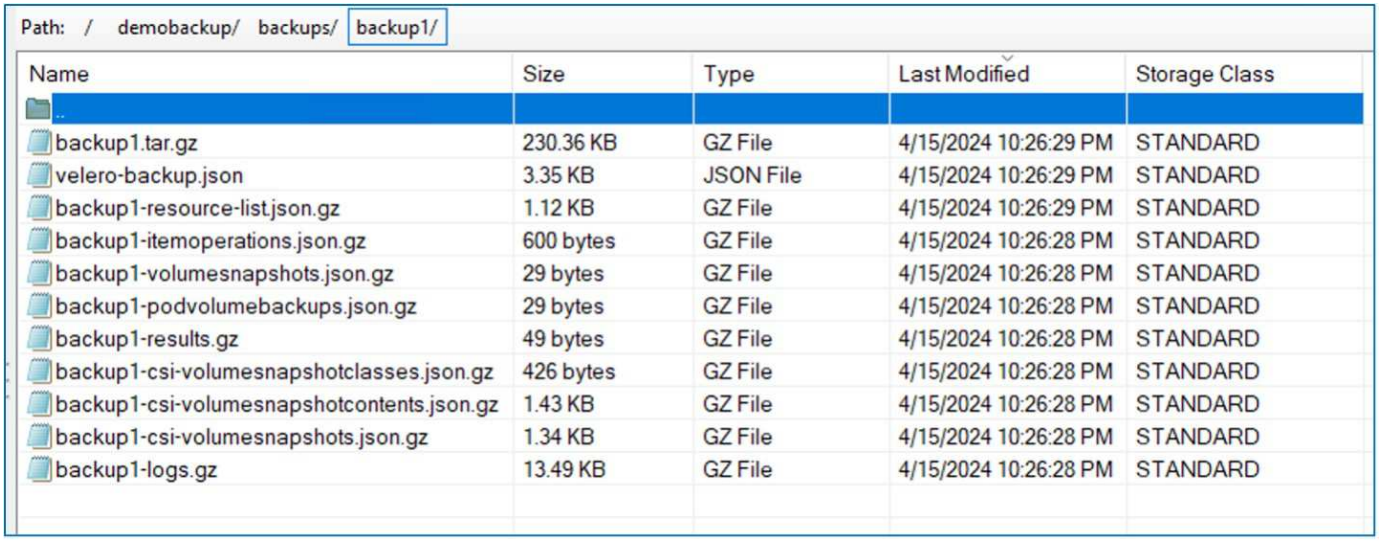
```
  ttl: 720h0m0s
```

Une fois la sauvegarde terminée, sa phase s'affichera comme terminée.



Vous pouvez inspecter la sauvegarde dans le stockage d'objets à l'aide d'une application de navigateur S3. Le chemin de la sauvegarde apparaît dans le bucket configuré avec le nom de préfixe (velero/container-demo-backup). Vous pouvez voir que le contenu de la sauvegarde comprend les instantanés de volume, les journaux et d'autres métadonnées de l'application.

Dans StorageGrid, vous pouvez également utiliser la console S3 disponible à partir du gestionnaire de locataires pour afficher les objets de sauvegarde.



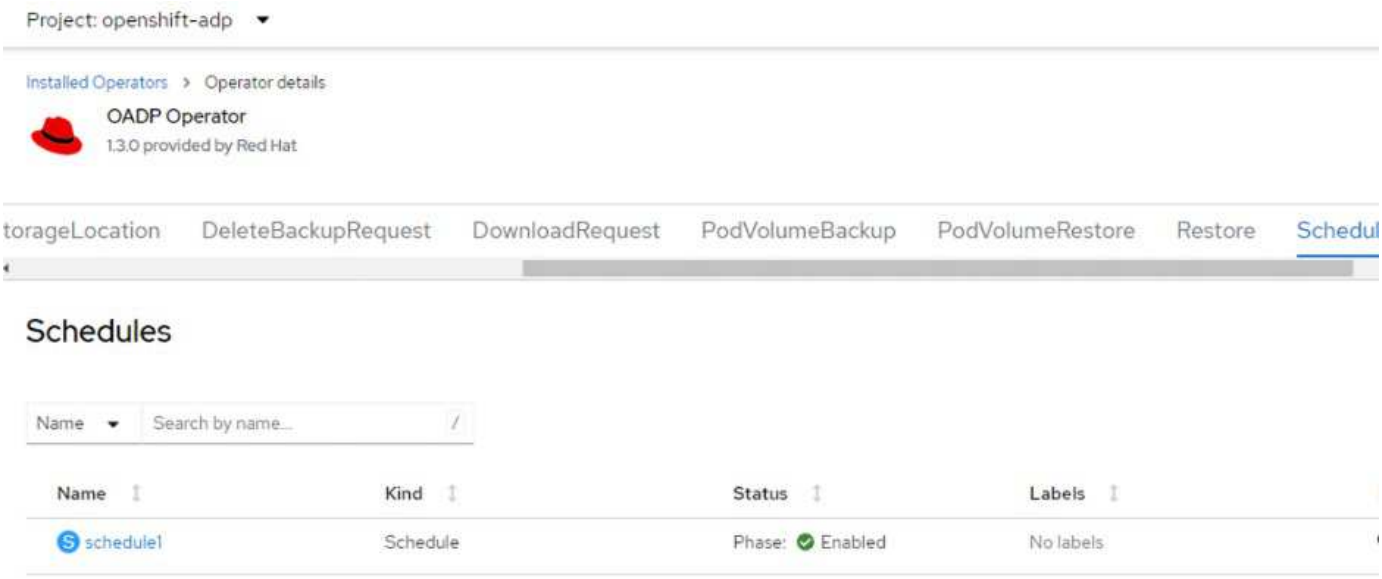
Création de sauvegardes planifiées pour les applications

Pour créer des sauvegardes selon une planification, vous devez créer une CR de planification. La planification est simplement une expression Cron vous permettant de spécifier l'heure à laquelle vous souhaitez créer la sauvegarde. Un exemple de fichier yaml pour créer un CR de planification est présenté ci-dessous.

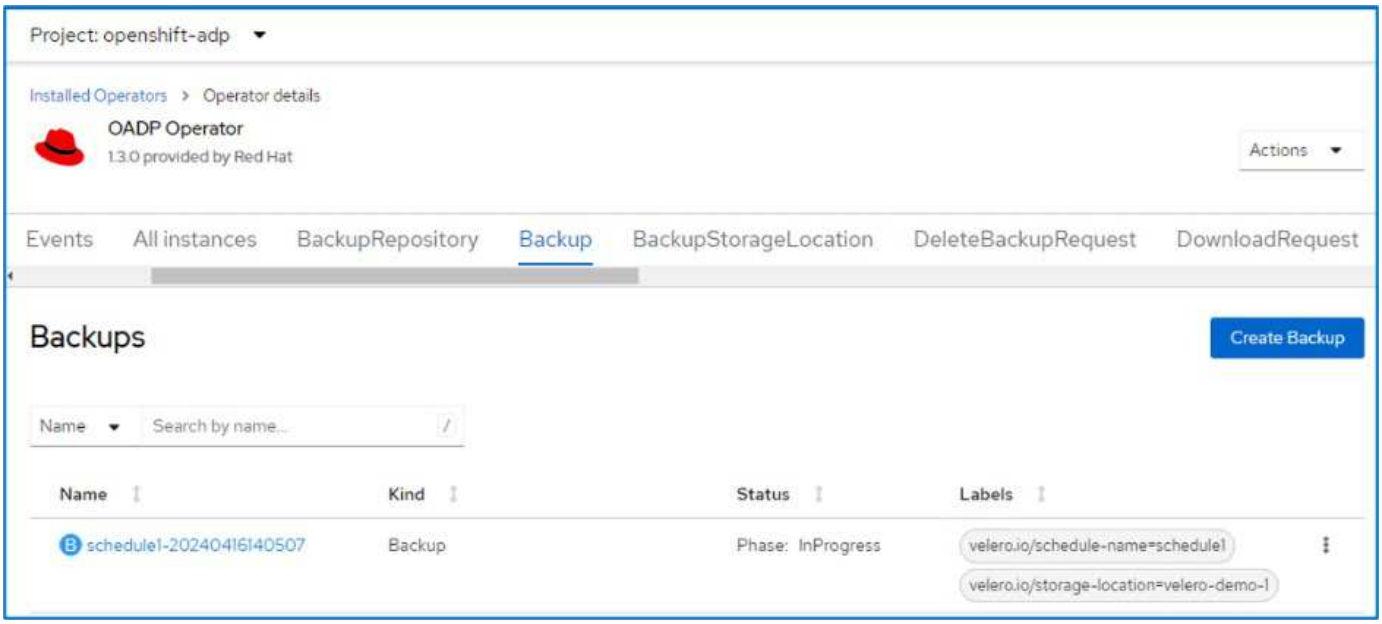
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

L'expression Cron 0 7 * * * signifie qu'une sauvegarde sera créée à 7h00 tous les jours. Les espaces de noms à inclure dans la sauvegarde et l'emplacement de stockage de la sauvegarde sont également spécifiés. Ainsi, au lieu d'un CR de sauvegarde, le CR planifié est utilisé pour créer une sauvegarde à l'heure et à la fréquence spécifiées.

Une fois le calendrier créé, il sera activé.



Les sauvegardes seront créées selon ce calendrier et pourront être consultées à partir de l'onglet Sauvegarde.



Migrer une application d'un cluster à un autre

Les capacités de sauvegarde et de restauration de Velero en font un outil précieux pour migrer vos données entre clusters. Cette section décrit comment migrer des applications d'un cluster vers un autre en créant une sauvegarde de l'application dans le stockage d'objets d'un cluster, puis en restaurant l'application du même stockage d'objets vers un autre cluster. .

▼ **Sauvegarde du premier cluster**

Prérequis sur le Cluster 1

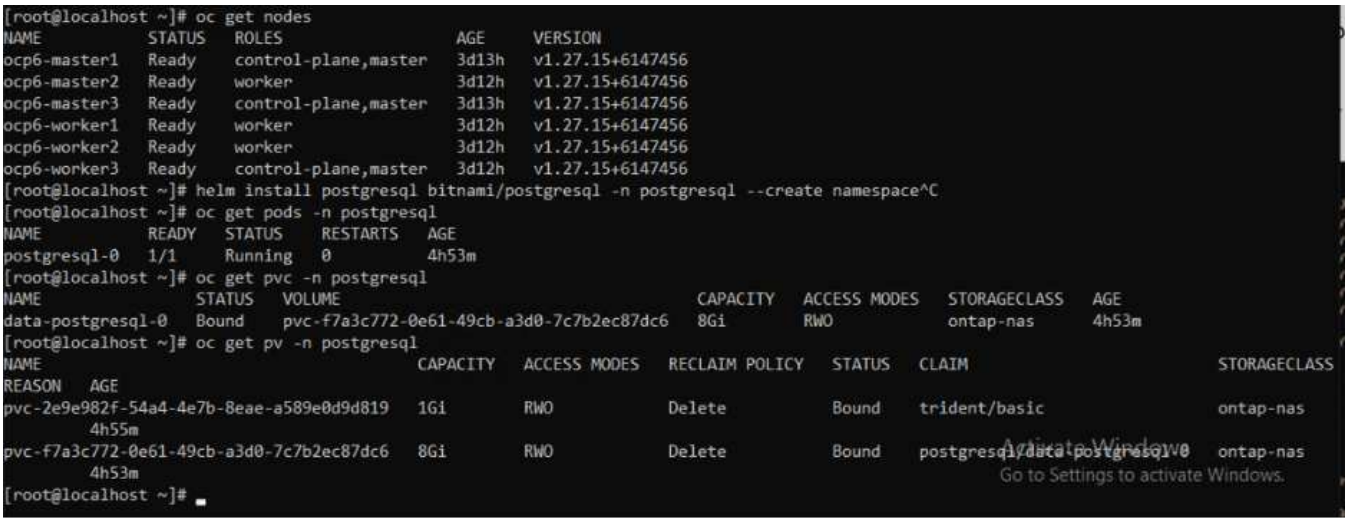
- Trident doit être installé sur le cluster.
- Un backend trident et une classe de stockage doivent être créés.
- L'opérateur OADP doit être installé sur le cluster.
- L'application DataProtectionApplication doit être configurée.

Utilisez la spécification suivante pour configurer l'objet DataProtectionApplication.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
```

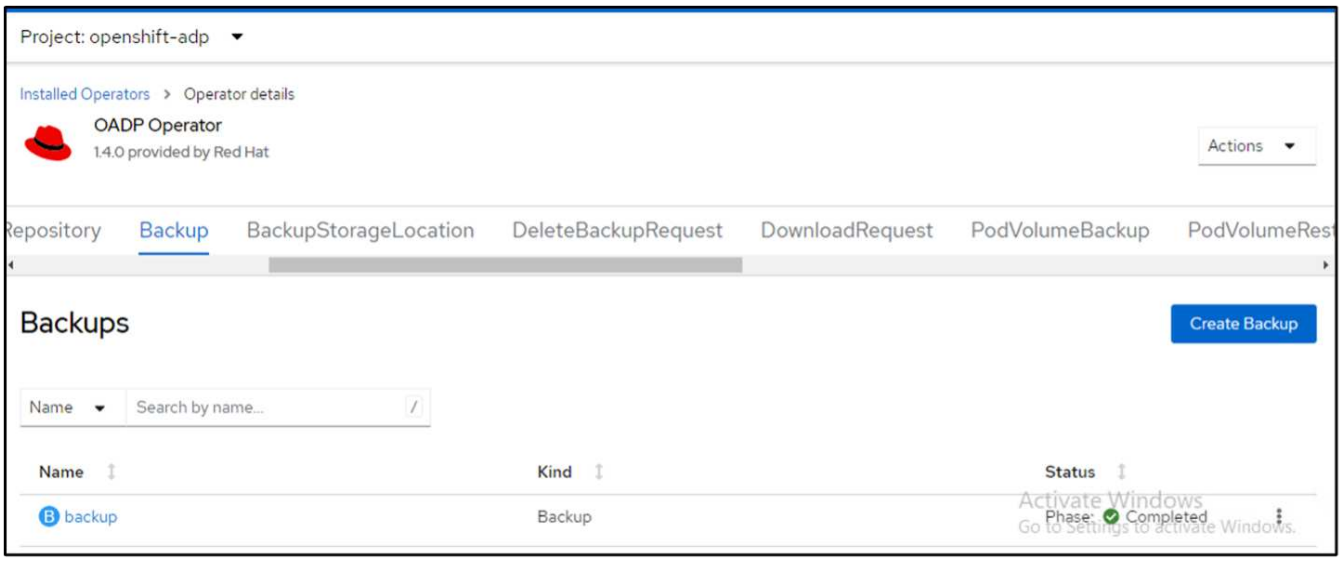
```
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- Créez une application sur le cluster et effectuez une sauvegarde de cette application. À titre d'exemple, installez une application Postgres.



- Utilisez la spécification suivante pour le CR de sauvegarde :

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



Vous pouvez cliquer sur l'onglet **Toutes les instances** pour voir les différents objets en cours de création et passer par différentes phases pour finalement arriver à la phase de sauvegarde **terminée**.

Une sauvegarde des ressources dans l'espace de noms postgresql sera stockée dans l'emplacement de stockage d'objets (ONTAP S3) spécifié dans backupLocation dans la spécification OADP.

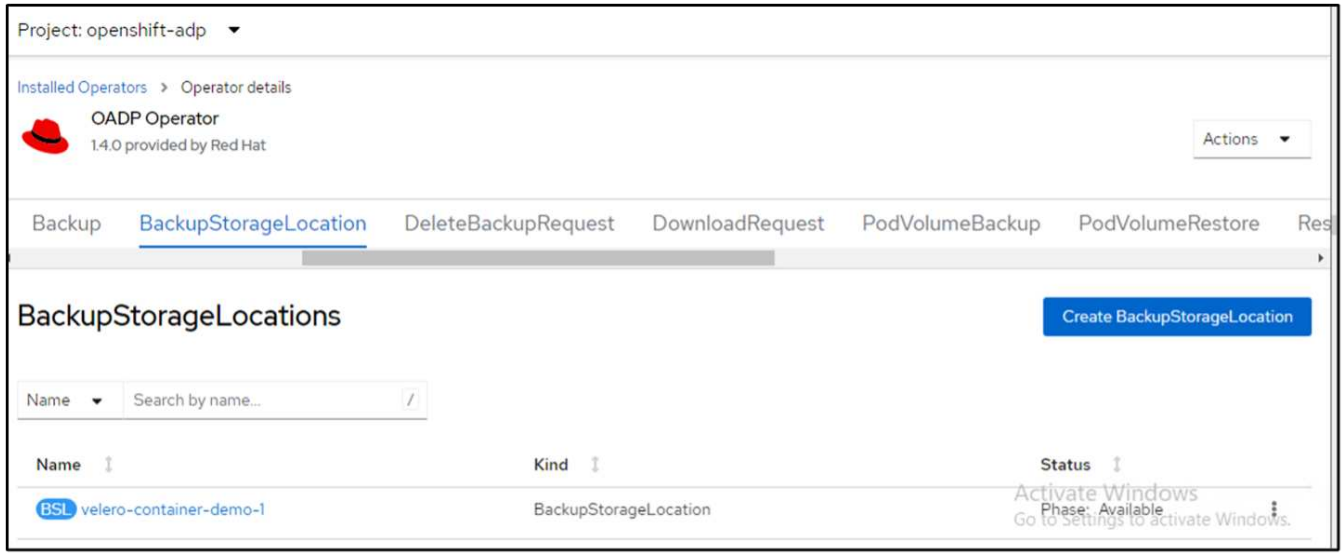
▼ **Restaurer vers un deuxième cluster**

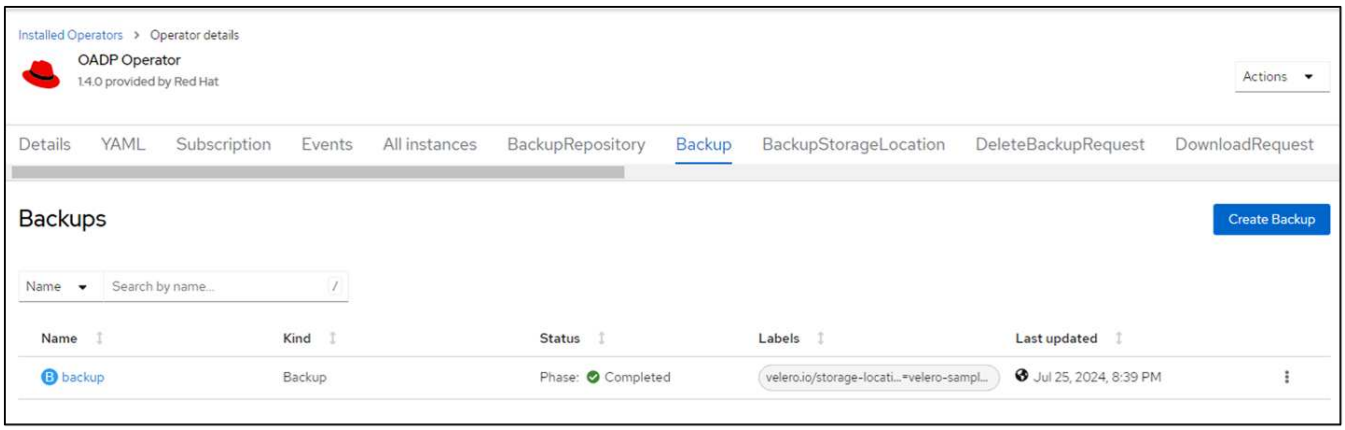
Prérequis sur le Cluster 2

- Trident doit être installé sur le cluster 2.
- L'application postgresql ne doit PAS être déjà installée dans l'espace de noms postgresql.
- L'opérateur OADP doit être installé sur le cluster 2 et l'emplacement BackupStorage doit pointer vers le même emplacement de stockage d'objets où la sauvegarde a été stockée à partir du premier cluster.
- Le CR de sauvegarde doit être visible depuis le deuxième cluster.

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                 STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic         ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc      vsphere-sc              2d7
h
[root@localhost ~]#
```



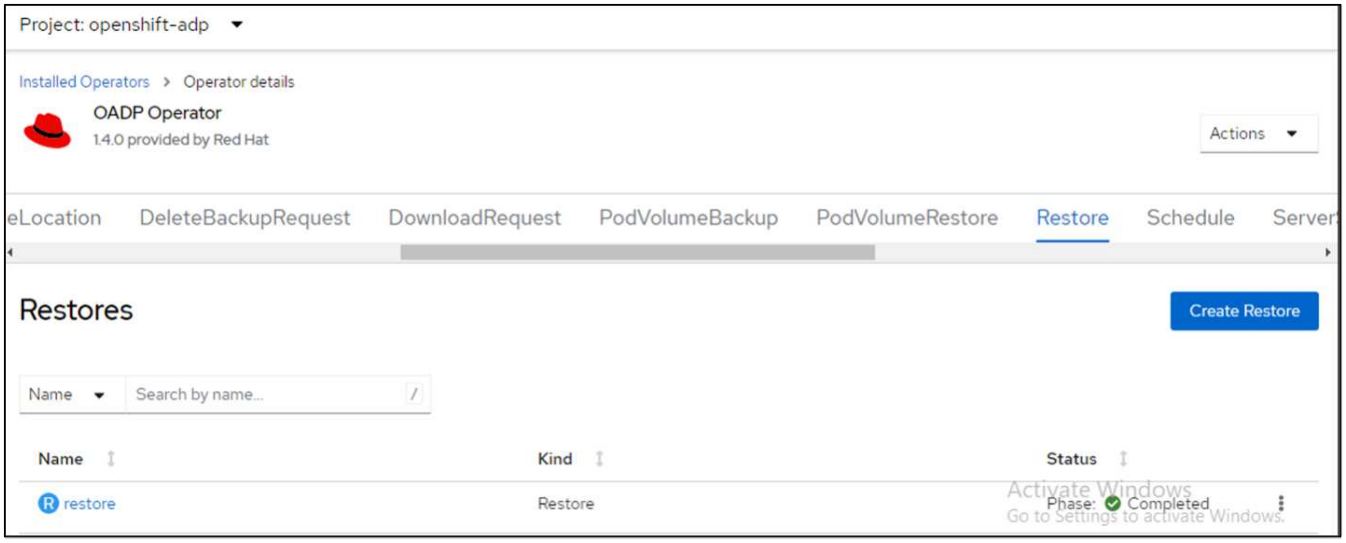


Restaurez l'application sur ce cluster à partir de la sauvegarde. Utilisez le fichier yaml suivant pour créer le CR de restauration.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
```

```
spec:
  backupName: backup
  restorePVs: true
```

Une fois la restauration terminée, vous verrez que l'application postgresql s'exécute sur ce cluster et est associée au pvc et à un pv correspondant. L'état de l'application est le même que lorsque la sauvegarde a été effectuée.




```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE    VERSION
ocp7-master1  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3  Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                           STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                   ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0    ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc                vsphere-sc
         2d10h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

Restaurer une application à partir d'une sauvegarde

Cette section décrit comment restaurer des applications à partir d'une sauvegarde.

Prérequis

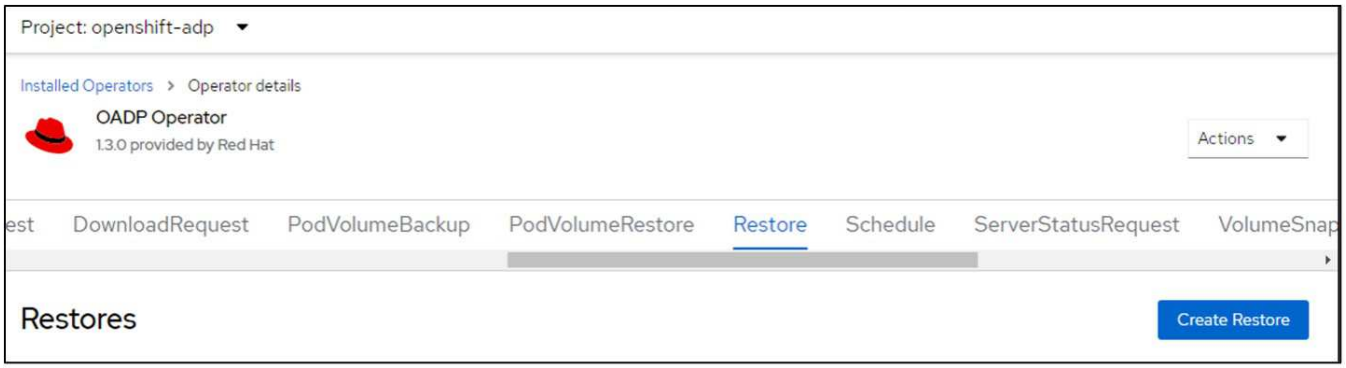
Pour restaurer à partir d'une sauvegarde, supposons que l'espace de noms où l'application existait a été supprimé accidentellement.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

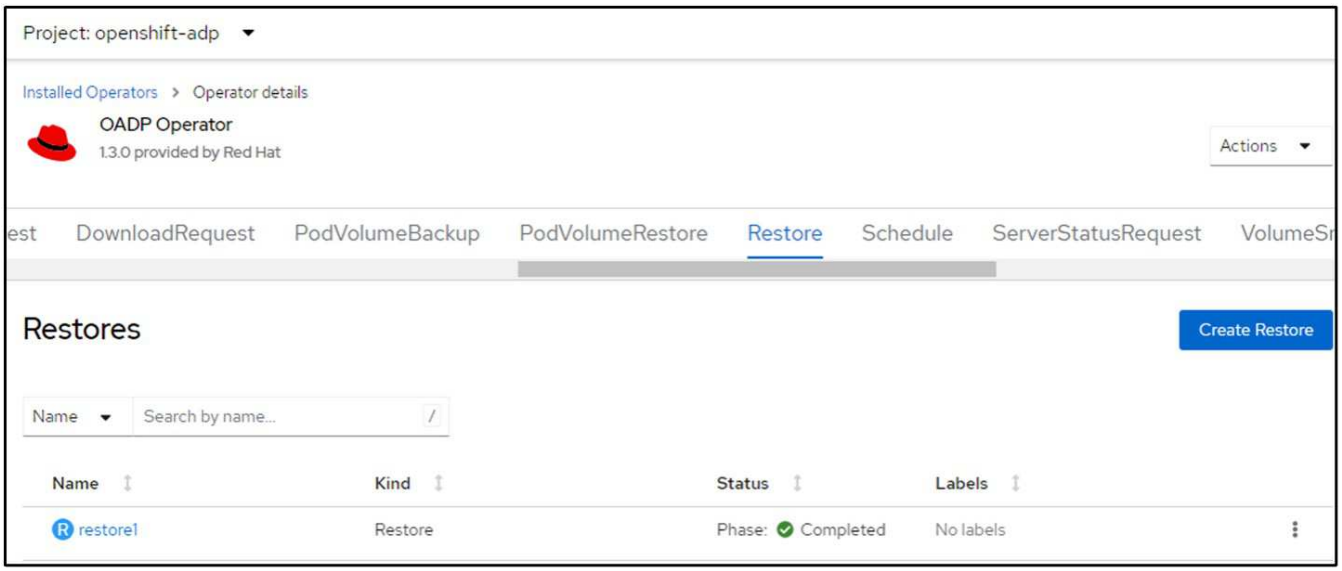
▼ **Restaurer vers le même espace de noms**

Pour effectuer une restauration à partir de la sauvegarde que nous venons de créer, nous devons créer une ressource personnalisée (CR) de restauration. Nous devons lui attribuer un nom, indiquer le nom de la sauvegarde à partir de laquelle nous souhaitons effectuer la restauration et définir restorePVs sur true. Des paramètres supplémentaires peuvent être définis comme indiqué dans la "documentation". Cliquez sur le bouton Créer.




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Lorsque la phase est terminée, vous pouvez voir que l'application a été restaurée à l'état dans lequel l'instantané a été pris. L'application est restaurée dans le même espace de noms.




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ **Restaurer vers un espace de noms différent**

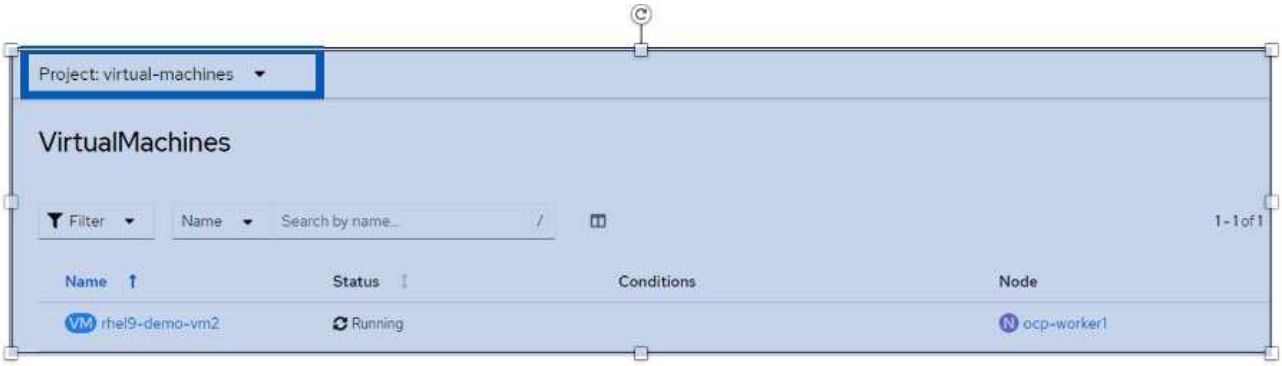
Pour restaurer l'application dans un espace de noms différent, vous pouvez fournir un namespaceMapping dans la définition yaml du CR de restauration.

L'exemple de fichier yaml suivant crée un CR de restauration pour restaurer une application et son stockage persistant à partir de l'espace de noms postgresql, vers le nouvel espace de noms postgresql-restored.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
```

```
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

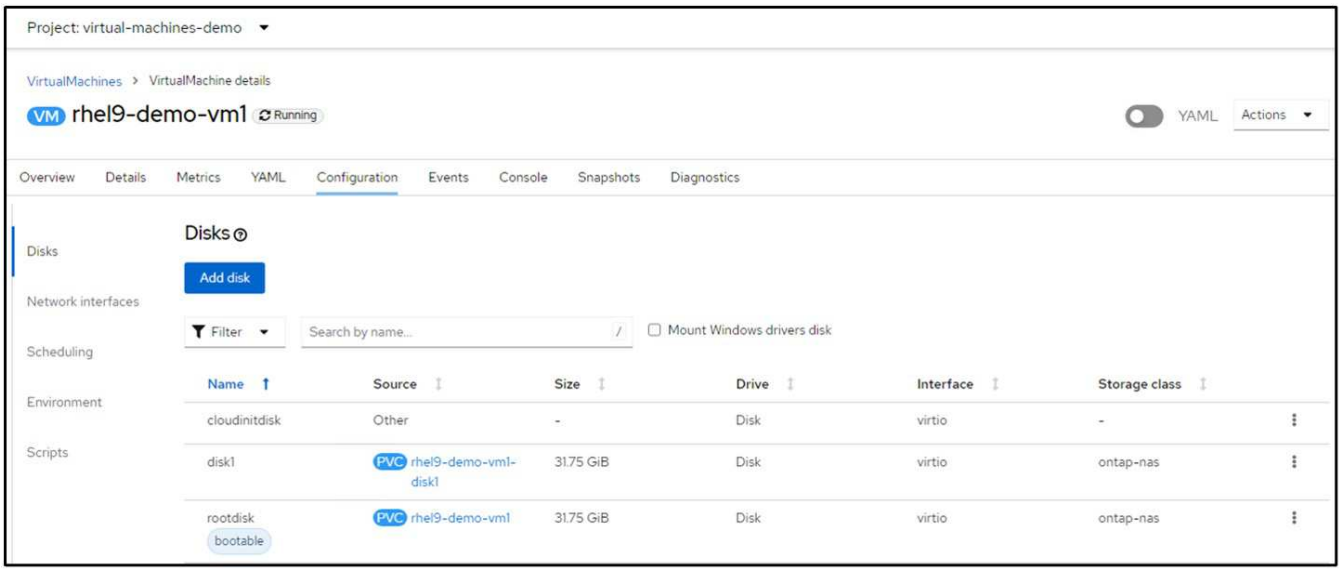
Lorsque la phase est terminée, vous pouvez voir que l'application a été restaurée à l'état dans lequel l'instantané a été pris. L'application est restaurée dans un espace de noms différent tel que spécifié dans le yaml.

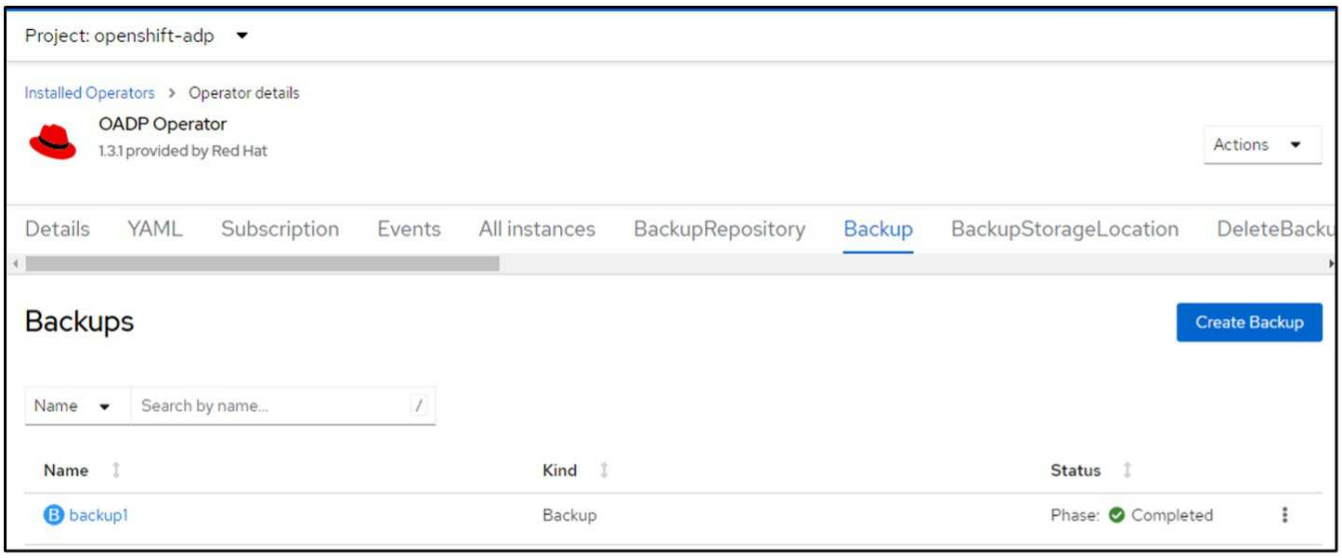


▼ **Restaurer vers une classe de stockage différente**

Velero fournit une capacité générique pour modifier les ressources pendant la restauration en spécifiant des correctifs json. Les correctifs JSON sont appliqués aux ressources avant leur restauration. Les correctifs json sont spécifiés dans une configmap et la configmap est référencée dans la commande de restauration. Cette fonctionnalité vous permet de restaurer à l'aide de différentes classes de stockage.

Dans l'exemple ci-dessous, l'application, lors du déploiement, utilise ontap-nas comme classe de stockage pour ses volumes persistants. Une sauvegarde de l'application nommée backup-postgresql-ontaps3 est créée.





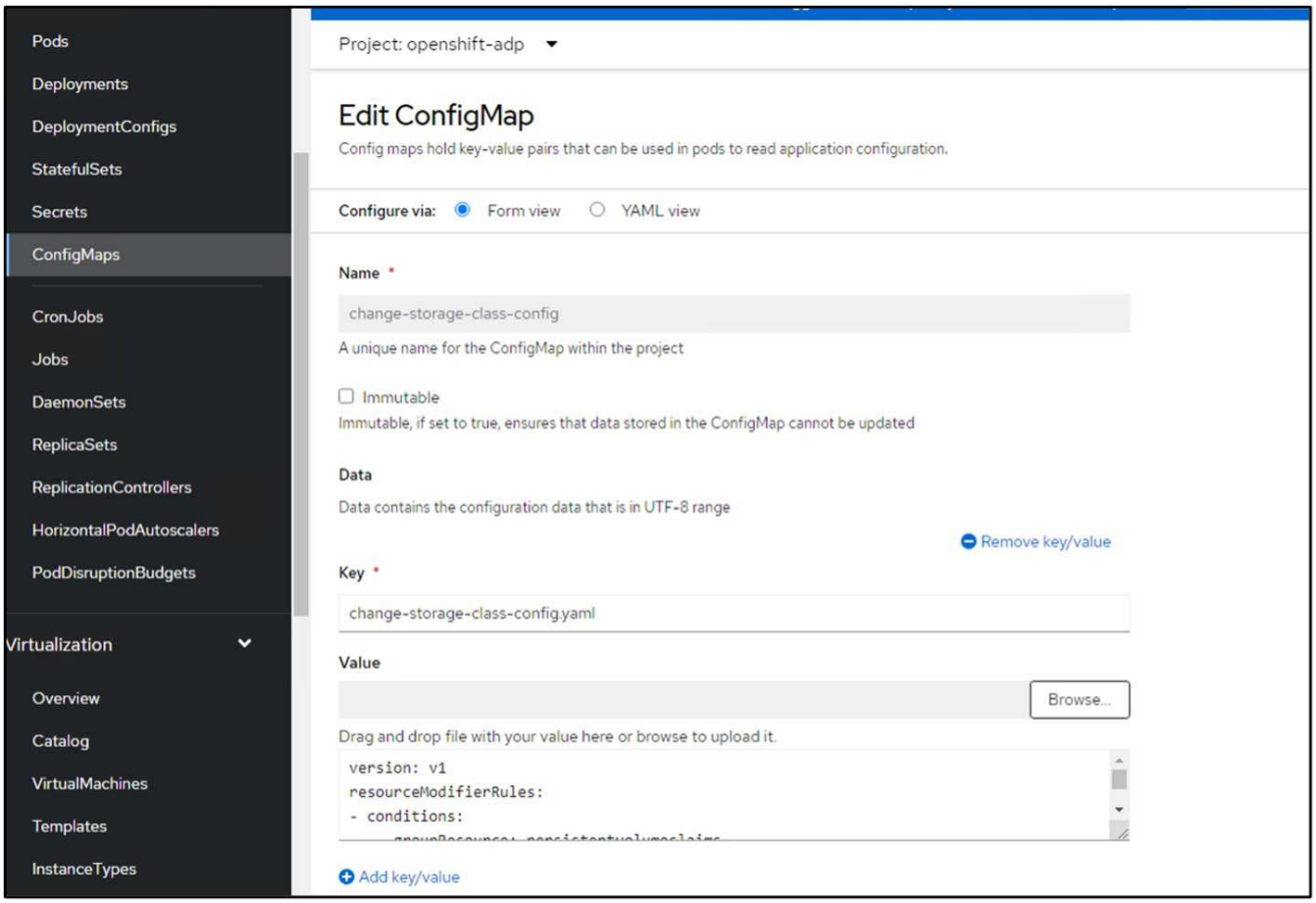
Simulez une perte de l'application en désinstallant l'application.

Pour restaurer la machine virtuelle à l'aide d'une classe de stockage différente, par exemple, la classe de stockage ontap-nas-eco, vous devez effectuer les deux étapes suivantes :

Étape 1

Créez une carte de configuration (console) dans l'espace de noms openshift-adp comme suit : Remplissez les détails comme indiqué dans la capture d'écran : Sélectionnez l'espace de noms : openshift-adp Nom : change-ontap-sc (peut être n'importe quel nom) Clé : change-ontap-sc-config.yaml : Valeur :

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



L’objet de carte de configuration résultant devrait ressembler à ceci (CLI) :

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"



BinaryData
====

Events:  <none>
```

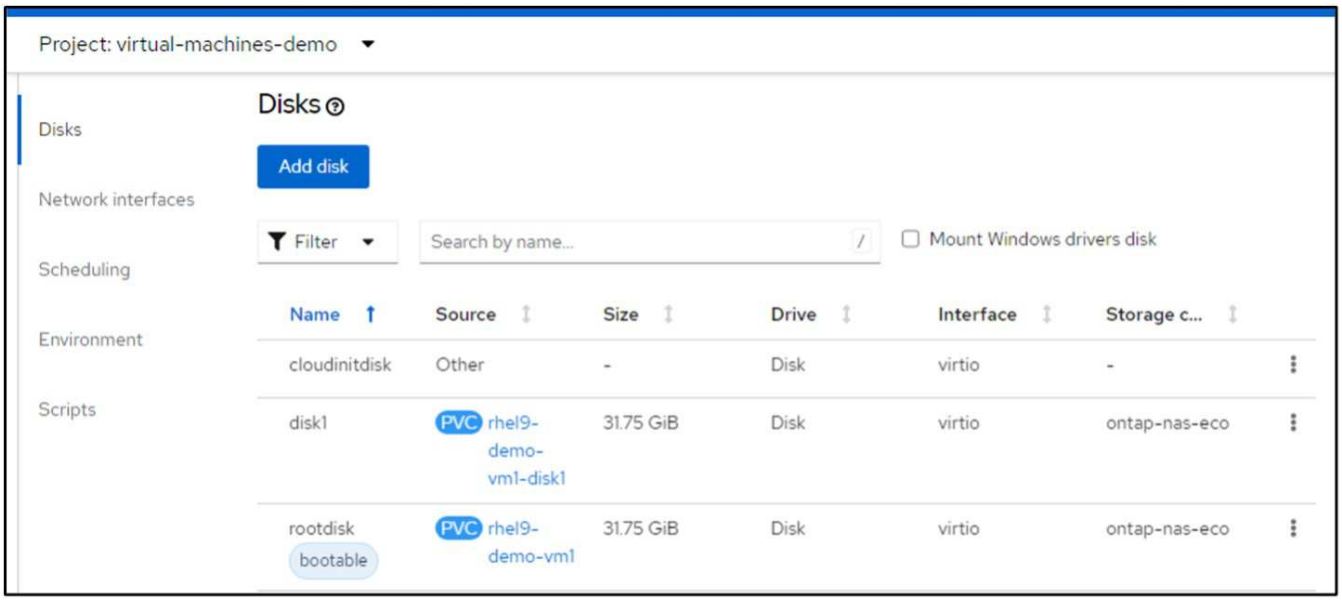
Cette carte de configuration appliquera la règle de modification des ressources lors de la création de la restauration. Un correctif sera appliqué pour remplacer le nom de la classe de stockage par ontap-nas-eco pour toutes les revendications de volume persistant commençant par rhel.

Étape 2

Pour restaurer la machine virtuelle, utilisez la commande suivante depuis la CLI Velero :

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

L'application est restaurée dans le même espace de noms avec les revendications de volume persistant créées à l'aide de la classe de stockage ontap-nas-eco.



Suppression des sauvegardes et des restaurations lors de l'utilisation de Velero

Cette section décrit comment supprimer les sauvegardes et les restaurations d'applications dans la plateforme de conteneurs OpenShift à l'aide de Velero.

Lister toutes les sauvegardes

Vous pouvez répertorier tous les CR de sauvegarde à l'aide de l'outil OC CLI ou de l'outil Velero CLI. Téléchargez le Velero CLI comme indiqué dans les instructions du"Documentation Velero" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Supprimer une sauvegarde

Vous pouvez supprimer un CR de sauvegarde sans supprimer les données de stockage d'objets à l'aide de l'outil OC CLI. La sauvegarde sera supprimée de la sortie CLI/Console. Cependant, comme la sauvegarde correspondante n'est pas supprimée du stockage d'objets, elle réapparaîtra dans la sortie CLI/console.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                           AGE
backup-postgresql-ontaps3      23h
schedule1-20240717070005       6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                           AGE
backup-postgresql-ontaps3      23h
backup2                        24s
schedule1-20240717070005       6h50m
[root@localhost ~]#
```

Si vous souhaitez supprimer le CR de sauvegarde ET les données de stockage d'objets associées, vous pouvez le faire à l'aide de l'outil CLI Velero.

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                      STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3 Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
backup2                   Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
schedule1-20240717070005  Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                      STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3 Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
schedule1-20240717070005  Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
[root@localhost ~]#
```

Suppression de la restauration

Vous pouvez supprimer l'objet CR de restauration en utilisant l'interface de ligne de commande OC ou l'interface de ligne de commande Velero.

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME      BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore   backup-postgresql-ontaps3 Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1  backup-postgresql-ontaps3 Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME      BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore   backup-postgresql-ontaps3 Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

Regardez des vidéos et des démonstrations sur les solutions multicloud hybrides avec NetApp

Regardez des vidéos sur les solutions multicloud hybrides pour Amazon Web Services avec NetApp

Explorez la bibliothèque vidéo complète de NetApp présentant des solutions multicloud hybrides pour AWS avec NetApp. Regardez des vidéos sur le stockage connecté aux invités, les économies de coût total de possession, les banques de données supplémentaires et les flux de travail de migration pour VMware Cloud sur AWS et Amazon FSx pour ONTAP, y compris les scénarios Windows et Linux.

Stockage connecté aux invités

Stockage invité Windows connecté avec FSx ONTAP à l'aide d'iSCSI

Stockage invité Linux connecté avec FSx ONTAP utilisant NFS

TCO et magasins de données supplémentaires

Économies TCO VMware Cloud sur AWS avec Amazon FSx ONTAP

Banque de données supplémentaire VMware Cloud sur AWS avec Amazon FSx ONTAP

Flux de travail de migration (HCX)

Déploiement et configuration de VMware HCX pour VMC

Démonstration de migration vMotion avec VMware HCX pour VMC et FSx ONTAP

Démonstration de migration à froid avec VMware HCX pour VMC et FSx ONTAP

Regardez des vidéos sur les solutions multicloud hybrides pour Azure VMware Cloud avec NetApp

Explorez la bibliothèque vidéo complète de NetApp présentant des solutions multicloud hybrides pour Azure VMware Solution (AVS) avec NetApp. Cette collection comprend des vidéos sur les magasins de données supplémentaires, la reprise après sinistre et les flux de travail de migration.

Magasins de données supplémentaires

Présentation du magasin de données supplémentaire Azure VMware Solution avec Azure NetApp Files

Reprise après sinistre

Solution Azure VMware DR avec Cloud Volumes ONTAP, SnapCenter et JetStream

Flux de travail de migration (HCX)

Démonstration de migration à froid avec VMware HCX pour AVS et ANF

Démonstration de vMotion avec VMware HCX pour AVS et ANF

Démonstration de migration en masse avec VMware HCX pour AVS et ANF

Regardez des vidéos sur les solutions multicloud hybrides pour Red Hat OpenShift avec NetApp

Explorez la bibliothèque vidéo complète de NetApp présentant des solutions multicloud hybrides pour Red Hat OpenShift avec NetApp. Cette collection comprend des démonstrations sur les instantanés et la restauration pour OpenShift sur AWS (ROSA) avec FSx ONTAP, l'intégration avec Trident, le basculement et la restauration pour les applications, ainsi que le déploiement automatisé d'Oracle RAC sur FlexPod avec Ansible.

Instantanés et restauration

Instantané/Restauration pour les applications sur les clusters Red Hat OpenShift Service sur AWS (ROSA) avec stockage Amazon FSx ONTAP

Intégration du stockage

Intégration de FSx ONTAP avec Trident

Basculement et restauration automatique

Basculement et restauration des applications sur ROSA avec FSx ONTAP

Automatisation des solutions



Déploiement automatisé d'Oracle 19c RAC sur FlexPod avec Ansible

Lisez les blogs sur les solutions cloud des experts NetApp

Lisez les blogs qui offrent des conseils pratiques et des bonnes pratiques pour l'intégration du stockage ONTAP aux solutions cloud NetApp .

Intégration de VMware avec AWS et Amazon FSx pour ONTAP

- "Migrer des machines virtuelles VMware vers AWS à l'aide du protocole iSCSI Amazon EC2 et Amazon FSx ONTAP"
- "Amazon EVS s'intègre désormais à FSx pour ONTAP"
- "Amazon EVS annonce la prise en charge de FSx pour ONTAP"
- "Configurer un cloud hybride avec FSx ONTAP et VMware Cloud sur AWS SDDC à l'aide de VMware HCX"

Solution Azure VMware

- "Optimisez le stockage et les charges de travail VMware gourmandes en données dans n'importe quel cloud"
- "Charges de travail VMware vers Azure VMware Solution ? Lisez ceci en premier."

Moteur VMware de Google Cloud

- "Prise en charge du magasin de données Google Cloud NetApp Volumes pour Google Cloud VMware Engine (NetApp)"
- "Comment utiliser les volumes NetApp comme banques de données pour Google Cloud VMware Engine (Google)"
- "Blog NetApp : une meilleure façon de migrer vos applications riches en stockage vers Google Cloud"

Protection et gestion des données

- "Protection des données 3-2-1 pour VMware avec SnapCenter Plug-in et NetApp Backup and Recovery for VMs"
- "Observabilité pour le centre de données moderne avec NetApp Cloud Insights"

Charges de travail de conteneurs NetApp pour OpenShift

- "NetApp ONTAP sert également de stockage pour les journaux dans la plateforme de conteneurs Red Hat OpenShift"

VMware Sovereign Cloud

- "Présentation de la nouvelle initiative Sovereign Cloud"

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.