NetApp pour GCP/GCVE

NetApp Solutions

NetApp
September 26, 2024

Sommaire

NetApp pour GCP/GCVE

Fonctionnalités NetApp pour Google Cloud Platform GCVE

Découvrez les fonctionnalités qu'NetApp apporte à Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) : de NetApp en tant que périphérique de stockage connecté par l'invité ou datastore NFS supplémentaire en tant que migration des workflows, extension/bursting dans le cloud, sauvegarde/restauration et reprise après incident.

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

- "Configuration de GCVE dans GCP"
- "Options de stockage NetApp pour GCVE"
- "Solutions clouds NetApp/VMware"

Configuration de GCVE dans GCP

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

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

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

Le processus de configuration peut être divisé en plusieurs étapes :

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

Afficher les détails "Étapes de configuration pour GCVE".

Options de stockage NetApp pour GCVE

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

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

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

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

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

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

Cas d'utilisation de la solution

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

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

"Découvrez les solutions NetApp pour Google Cloud GCVE"

Protection des charges de travail sur GCP/GCVE

Reprise d'activité cohérente avec les applications avec NetApp SnapCenter et Veeam Replication

La reprise d'activité dans le cloud est une solution résiliente et économique qui protège les charges de travail contre les pannes sur site et la corruption des données, comme les attaques par ransomware. NetApp SnapMirror permet de répliquer les charges de travail VMware sur site utilisant un stockage connecté à l'invité vers NetApp Cloud Volumes ONTAP exécuté dans Google Cloud.

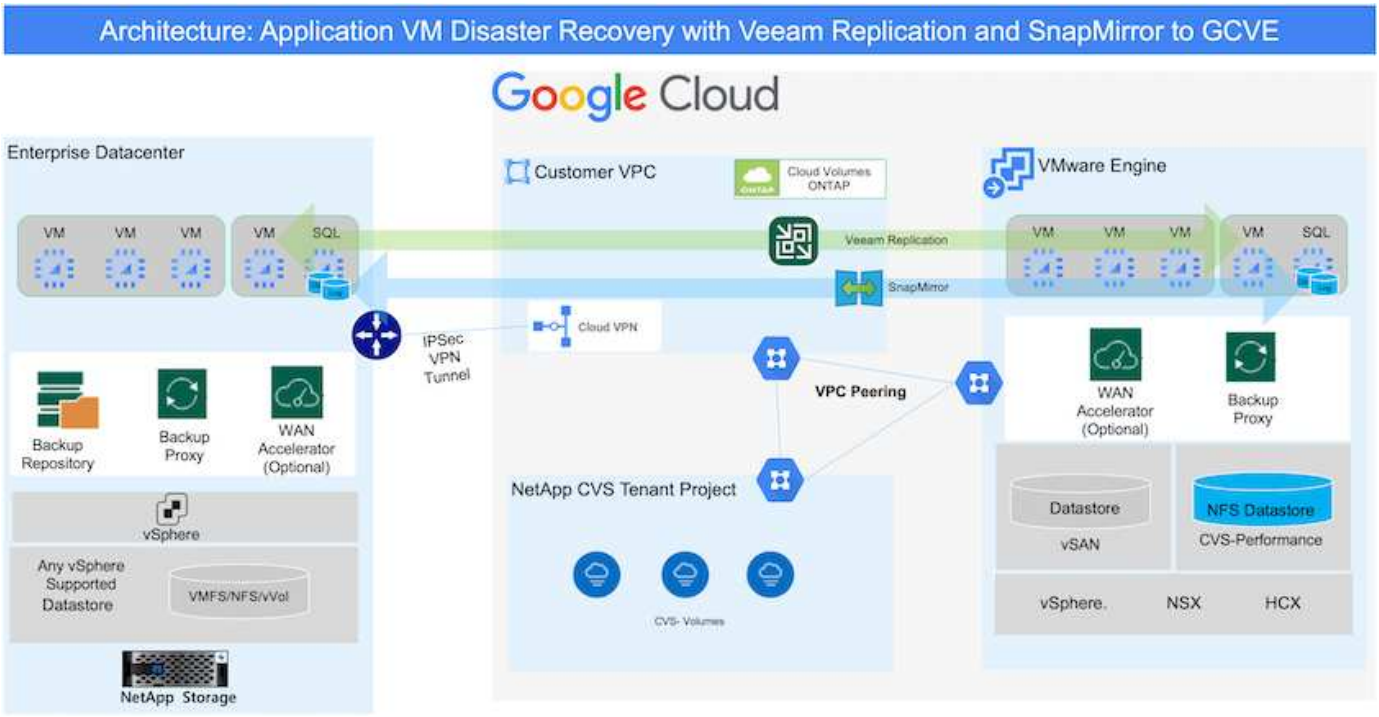
Auteurs : Suresh Thoppay, NetApp

Présentation

De nombreux clients recherchent une solution de reprise après incident efficace pour leurs machines virtuelles d'application hébergées sur VMware vSphere. La plupart d'entre eux utilisent leur solution de sauvegarde existante pour effectuer une restauration pendant les diaster.
La plupart du temps, cette solution augmente le RTO et ne répond pas à leurs attentes. Pour réduire les objectifs RPO et RTO, la réplication de machine virtuelle Veeam peut être utilisée même sur site vers GCVE dans la mesure où la connectivité réseau et l'environnement ne disposent pas des autorisations appropriées.
REMARQUE : Veeam VM Replication ne protège pas les dispositifs de stockage connectés invités d'une machine virtuelle, tels que les montages iSCSI ou NFS au sein de la machine virtuelle invitée. Ils doivent les protéger séparément.

Pour assurer une réplication cohérente avec les applications pour SQL VM et réduire l'objectif de durée de restauration, nous avons utilisé SnapCenter pour orchestrer les opérations snapmirror des volumes de bases de données et de journaux SQL.

Ce document propose une approche détaillée de la configuration et de l'exécution d'une reprise d'activité à l'aide de NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

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

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

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que une interconnexion dédiée ou un VPN cloud. Les segments doivent être créés en fonction de la conception VLAN sur site.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document. Consultez la documentation Google Cloud pour connaître la méthode de connectivité appropriée, du site vers Google.

Déploiement de la solution de reprise d'activité

Présentation du déploiement de la solution

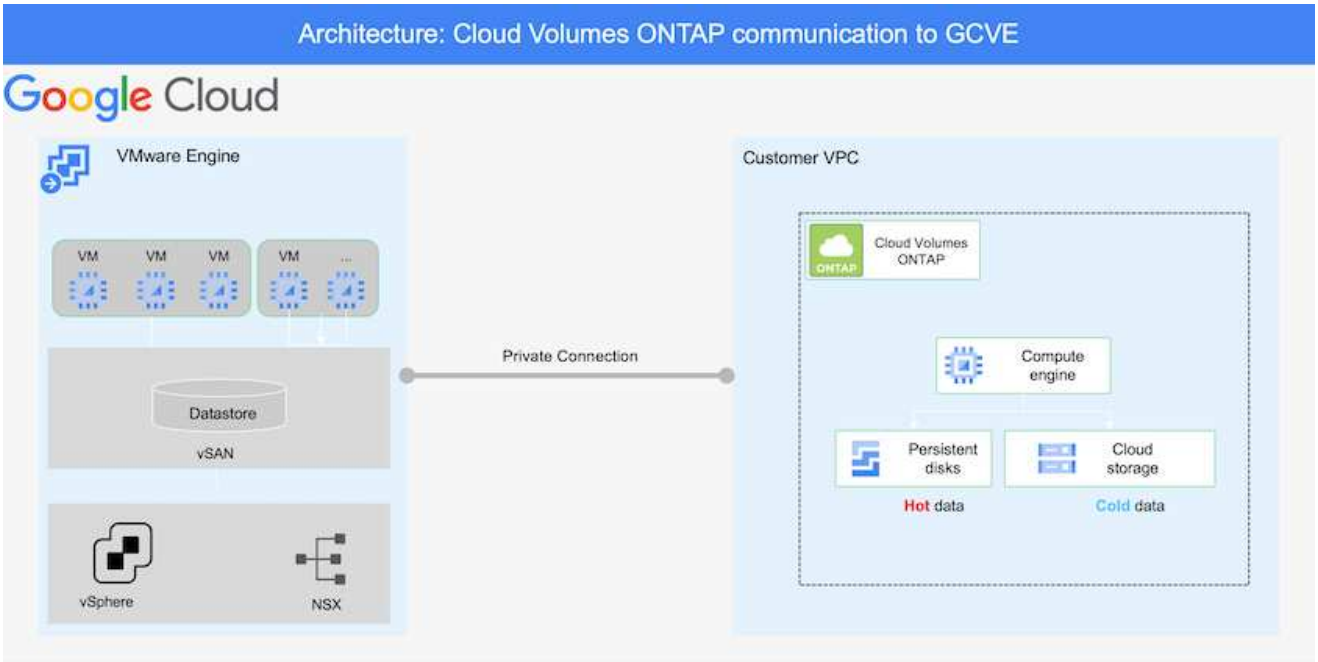
1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de BlueXP avec l'abonnement et le réseau virtuel appropriés.
   a. Configurer SnapMirror pour les volumes applicatifs concernés.
   b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.

3. Installez le logiciel Veeam et commencez à répliquer des machines virtuelles sur l'instance Google Cloud VMware Engine.
4. En cas d'incident, rompez la relation SnapMirror avec BlueXP et déclenchez le basculement des serveurs virtuels avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
   b. Permet de mettre les applications en ligne.
5. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Google Cloud et répliquez les volumes dans CVO

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



Pour obtenir des exemples d'instructions détaillées sur la configuration de SnapCenter et la réplication des données, reportez-vous à la section "Configurez la réplication avec SnapCenter"

Révision de la protection de SQL VM avec SnapCenter

Configurez l'accès aux données des hôtes GCVE et CVO

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

Le datastore NetApp Cloud Volume Service pour NFS et le journal et les bases de données Cloud Volumes ONTAP pour SQL peuvent être déployés sur n'importe quel VPC et GCVE doivent disposer d'une connexion privée à ce VPC pour monter le datastore NFS et se connecter aux LUN iSCSI par un VM.

Pour configurer GCVE SDDC, voir "Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)". Avant cela, vérifiez que les VM invités résidant sur les hôtes GCVE peuvent consommer des données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et GCVE ont été correctement configurés, commencez à configurer Veeam pour automatiser la restauration des workloads sur site vers GCVE (machines virtuelles avec VMDK d'application et VM avec stockage « Guest ») en utilisant la fonctionnalité de réplication Veeam et en utilisant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

Installer les composants Veeam

Selon le scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde à déployer. Pour ce cas d'utilisation, nul besoin de déployer un magasin d'objets pour Veeam et le référentiel scale-out non plus requis.
"Se référer à la documentation Veeam pour la procédure d'installation"
Pour plus d'informations, reportez-vous à la section "Migration avec Veeam Replication"

Configuration de la réplication de machine virtuelle avec Veeam

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere" À l'étape traitement invité de l'assistant, sélectionnez Désactiver le traitement de l'application, car nous utilisons SnapCenter pour la sauvegarde et la restauration intégrant la cohérence applicative.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Le basculement de la machine virtuelle Microsoft SQL Server

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.

- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
  - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- Veeam Replication permet de modifier les adresses IP des VM sur le site de reprise après incident.

Reprise après incident des applications avec SnapCenter, Cloud Volumes ONTAP et Veeam Replication

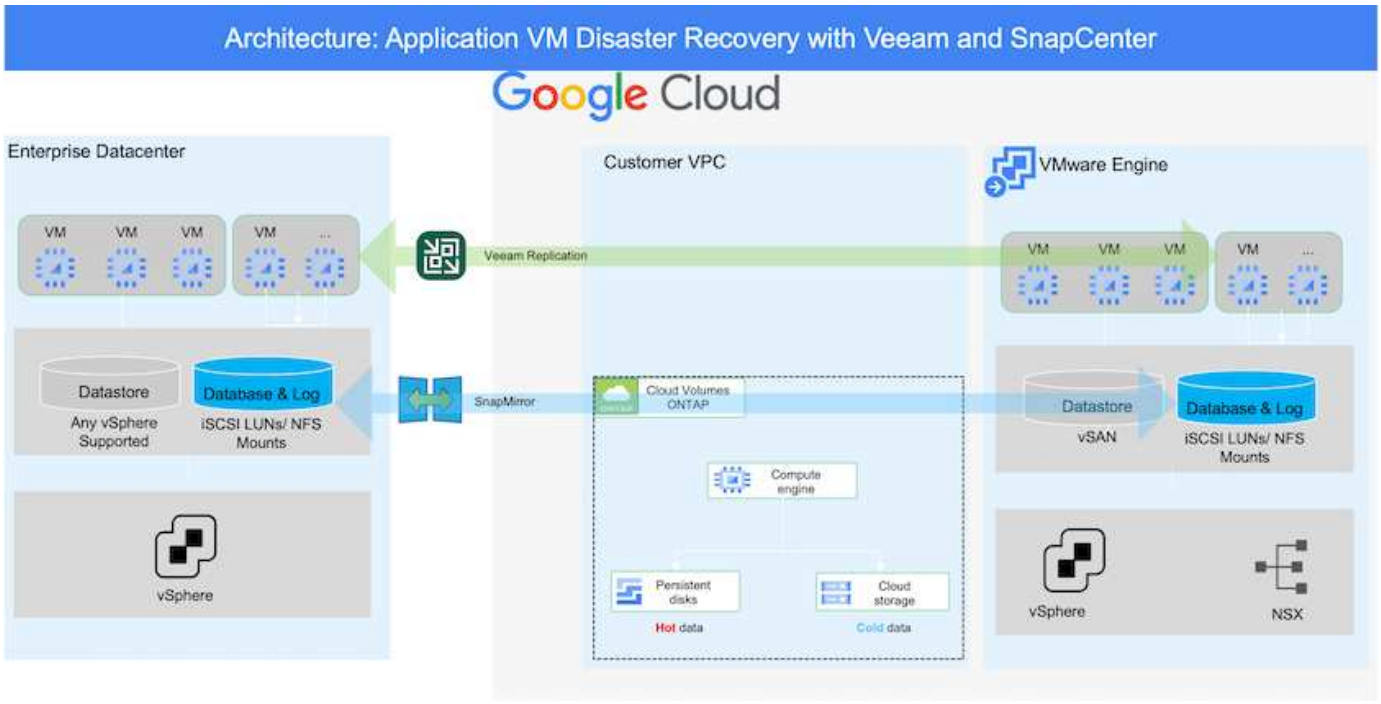
La reprise d'activité dans le cloud est une solution résiliente et économique qui protège les charges de travail contre les pannes sur site et la corruption des données, comme les attaques par ransomware. NetApp SnapMirror permet de répliquer les charges de travail VMware sur site utilisant un stockage connecté à l'invité vers NetApp Cloud Volumes ONTAP exécuté dans Google Cloud.

Auteurs : Suresh Thoppay, NetApp

Présentation

Il s'agit aussi des données applicatives, mais qu'en est-il des machines virtuelles elles-mêmes ? La reprise sur incident doit couvrir tous les composants dépendants, notamment les machines virtuelles, les VMDK ou les données d'application. Pour ce faire, SnapMirror et Veeam peuvent être utilisés pour restaurer de manière transparente les workloads répliqués depuis des sites sur Cloud Volumes ONTAP et en utilisant le stockage VSAN pour les VMDK de VM.

Ce document propose une approche détaillée de la configuration et de l'exécution d'une reprise d'activité à l'aide de NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

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

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

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que une interconnexion dédiée ou un VPN cloud. Les segments doivent être créés en fonction de la conception VLAN sur site.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document. Consultez la documentation Google Cloud pour connaître la méthode de connectivité appropriée, du site vers Google.

Déploiement de la solution de reprise d'activité

Présentation du déploiement de la solution

1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de Cloud Manager dans l'abonnement et le réseau virtuel appropriés.
   a. Configurer SnapMirror pour les volumes applicatifs concernés.
   b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer des machines virtuelles sur l'instance Google Cloud

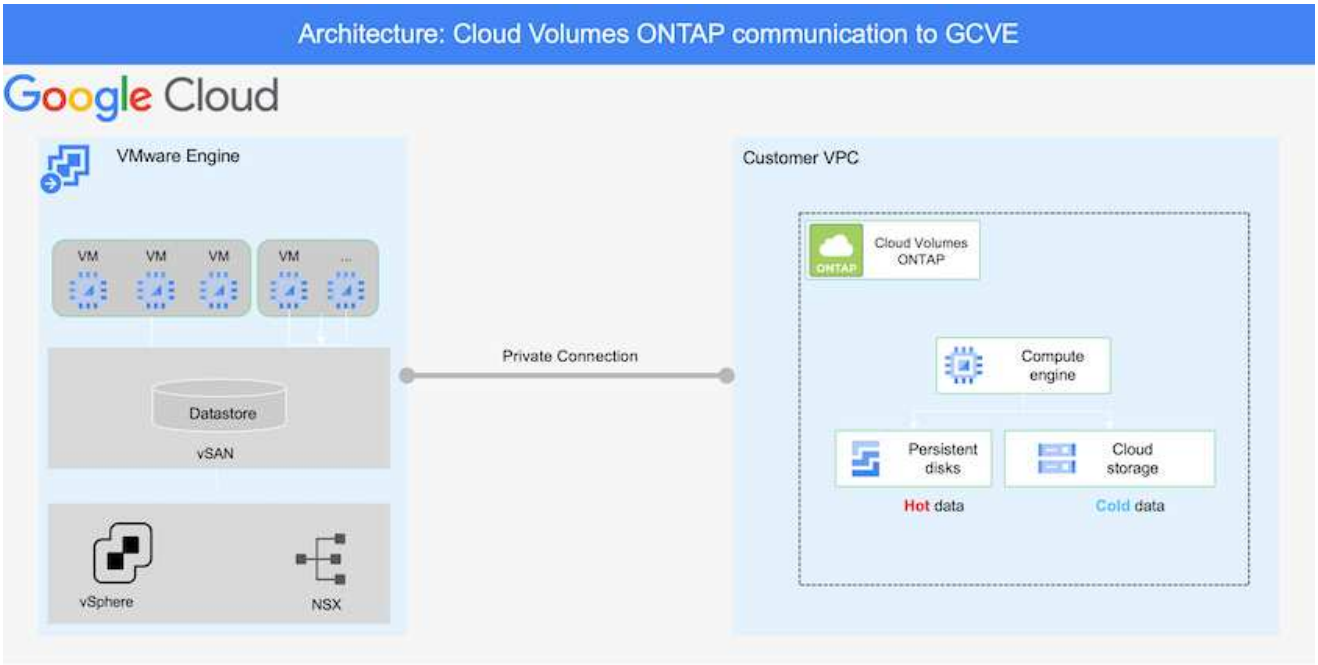
VMware Engine.

4. En cas d'incident, interrompre la relation SnapMirror avec Cloud Manager et déclencher le basculement des machines virtuelles avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
   b. Permet de mettre les applications en ligne.
5. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Google Cloud et répliquez les volumes dans CVO

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



Pour obtenir des exemples d'instructions détaillées sur la configuration de SnapCenter et la réplication des données, reportez-vous à la section "Configurez la réplication avec SnapCenter"

Configurez la réplication avec SnapCenter

Configurez l'accès aux données des hôtes GCVE et CVO

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

Cloud Volumes ONTAP peut être déployé sur n'importe quel VPC et GCVE doit disposer d'une connexion privée à ce VPC pour que la VM se connecte aux LUN iSCSI.

Pour configurer GCVE SDDC, voir "Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)". Avant cela, vérifiez que les VM invités résidant sur les hôtes GCVE peuvent consommer des données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et GCVE ont été correctement configurés, commencez à configurer Veeam pour automatiser la restauration des workloads sur site vers GCVE (machines virtuelles avec VMDK d'application et VM avec stockage « Guest ») en utilisant la fonctionnalité de réplication Veeam et en utilisant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

Installer les composants Veeam

Selon le scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde à déployer. Pour ce cas d'utilisation, nul besoin de déployer un magasin d'objets pour Veeam et le référentiel scale-out non plus requis.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Se référer à la documentation Veeam pour la procédure d'installation"]

Configuration de la réplication de machine virtuelle avec Veeam

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere" À l'étape traitement invité de l'assistant, sélectionnez Désactiver le traitement de l'application, car nous utilisons SnapCenter pour la sauvegarde et la restauration intégrant la cohérence applicative.

Configuration de la tâche de réplication de VM vSphere

Le basculement de la machine virtuelle Microsoft SQL Server

Le basculement de la machine virtuelle Microsoft SQL Server

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.

    - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
    - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
    - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- Veeam Replication permet de modifier les adresses IP des VM sur le site de reprise après incident.

Utilisation de la réplication Veeam et du datastore Google Cloud NetApp volumes pour la reprise d'activité vers Google Cloud VMware Engine

En temps de crise, un plan complet de reprise sur incident est essentiel pour les entreprises. De nombreuses entreprises exploitent le cloud computing pour leurs opérations quotidiennes et leur reprise après incident. Cette approche proactive peut réduire, voire éliminer les interruptions d'activité coûteuses.

Cet article décrit comment utiliser Veeam Backup & Replication pour configurer la reprise d'activité pour les machines virtuelles VMware sur site vers Google Cloud VMware Engine (GCVE) avec Google Cloud NetApp volumes (NetApp volumes).

Présentation

Google Cloud NetApp volumes est un service de stockage Google et NetApp disponible pour Google Cloud. Le service NetApp volumes fournit un stockage NFS/SMB haute performance. Le stockage NetApp volumes NFS certifié par VMware peut être utilisé en tant que datastore externe pour les hôtes ESXi dans GCVE. Les utilisateurs doivent établir une connexion de peering entre leur cloud privé GCVE et le projet NetApp volumes. Aucun frais réseau n'est facturé pour 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 datastores sur leurs hôtes ESXi.

Les datastores NFS basés sur NetApp volumes peuvent être utilisés pour répliquer les données depuis les environnements sur site à l'aide d'une solution tierce validée qui fournit des fonctionnalités de réplication de machines virtuelles. En ajoutant les datastores NetApp volumes, il permet un déploiement optimisé des coûts au lieu de créer un SDDC basé sur Google Cloud VMware Engine (GCVE) avec un grand nombre d'hôtes ESXi pour prendre en charge le stockage. Cette approche est appelée « groupe de témoins lumineux ». Un cluster de pilotes légers est une configuration hôte GCVE minimale (3 hôtes GCVE ESXi) et la capacité des datastores NetApp volumes permet une évolutivité indépendante pour répondre aux besoins en capacité.

L'objectif est de maintenir une infrastructure économique intégrant uniquement les composants de base pour gérer un basculement. Un cluster de pilotes peut se développer et ajouter d'autres hôtes GCVE en cas de basculement. Une fois le basculement résolu et le fonctionnement normal rétabli, le cluster voyant peut réduire sa taille et revenir à un mode de fonctionnement économique.

Objectifs du présent document

Cet article décrit l'utilisation d'un datastore Google Cloud NetApp volumes avec Veeam Backup & Replication pour configurer la reprise d'activité pour les machines virtuelles VMware sur site vers GCVE à l'aide des fonctionnalités du logiciel de réplication de machine virtuelle Veeam.

Veeam Backup & Replication est une application de sauvegarde et de réplication destinée aux environnements virtuels. Lors de la réplication des machines virtuelles, Veeam Backup & Replication crée une copie exacte des machines virtuelles au format VMware vSphere natif sur le cluster SDDC GCVE cible. Avec Veeam Backup & Replication, la copie reste synchronisée avec la machine virtuelle d'origine. La réplication offre le meilleur

objectif de délai de restauration (RTO), car une copie montée d'une machine virtuelle sur le site de reprise est prête à démarrer.

Ce mécanisme de réplication garantit que les charges de travail peuvent démarrer rapidement dans GCVE en cas d'incident. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. Il filtre également les blocs de données dupliqués, les blocs de données nuls, les fichiers swap et les « fichiers exclus du système d'exploitation invité des machines virtuelles ». Le logiciel compresse également le trafic de réplica. Pour éviter que les tâches de réplication ne consomment la totalité de la bande passante réseau, les accélérateurs WAN et les règles de restriction réseau peuvent être utilisés.

Dans Veeam Backup & Replication, le processus de réplication est piloté par des tâches, ce qui signifie que la réplication est effectuée via la configuration des tâches de réplication. En cas d'incident, le basculement peut être déclenché pour restaurer les machines virtuelles en basculant sur la copie de réplica. Lors d'un basculement, une machine virtuelle répliquée prend le rôle de la machine virtuelle d'origine. Le basculement peut être effectué vers l'état le plus récent d'une réplique ou vers l'un de ses points de restauration connus et corrects. La restauration est ainsi possible en cas d'attaque par ransomware ou de tests isolés les cas échéant. Veeam Backup & Replication propose plusieurs options pour gérer différents scénarios de reprise d'activité.

Présentation de la solution

Cette solution couvre les étapes générales suivantes :

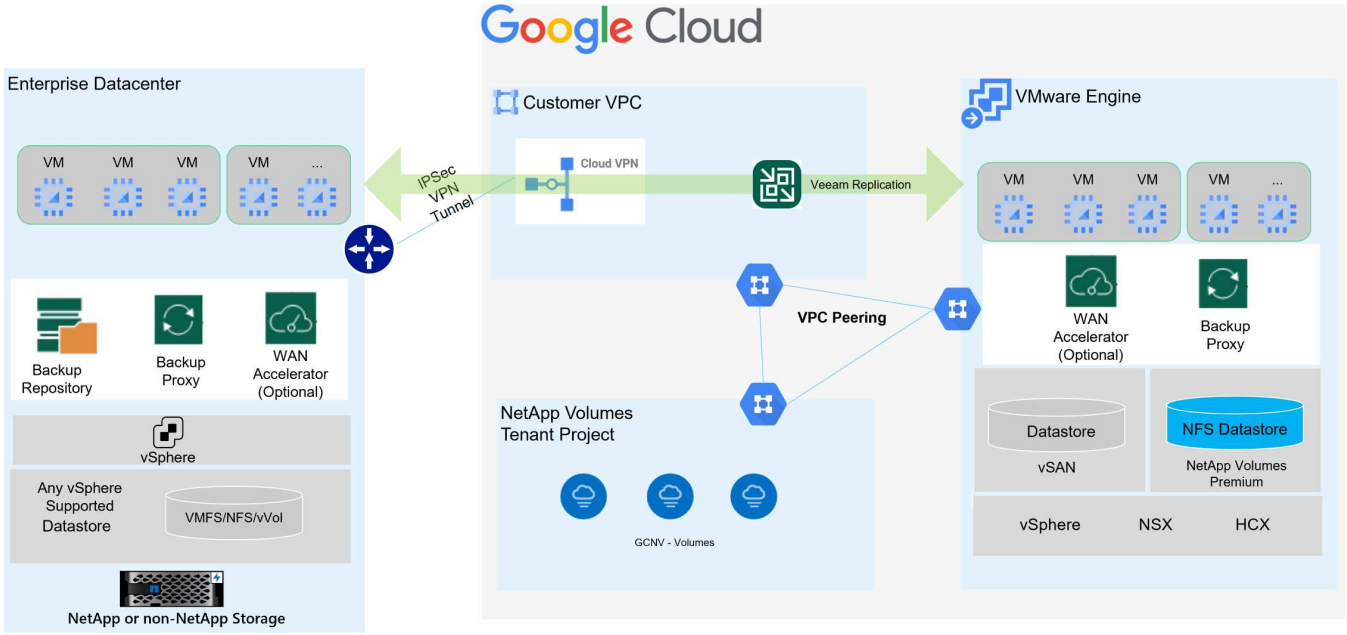
1. Créez un volume NFS à l'aide de Google Cloud NetApp volumes
2. Suivez le processus GCP pour créer un datastore GCVE à partir du volume NetApp volumes NFS.
3. Configuration d'une tâche de réplication pour créer des répliques de machine virtuelle à l'aide de Veeam Backup & Replication
4. Création d'un plan de basculement et basculement
5. Revenez aux machines virtuelles de production une fois l'incident terminé et le site principal en service.

Lors de la création d'un volume dans NetApp volumes, à utiliser en tant que datastore GCVE, seul NFS v3 est pris en charge.

Pour plus d'informations sur l'utilisation de volumes NetApp NFS en tant que datastores pour GCVE, consultez "Utilisation d'un volume NFS en tant que datastore vSphere hébergé par Google Cloud NetApp volumes" .

Architecture

Le schéma suivant illustre l'architecture de la solution présentée dans cette documentation. Il est recommandé d'utiliser un serveur Veeam Backup & Replication situé à la fois sur le site 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 disponibilité la plus élevée en cas de défaillance dans le data Center principal.



Pré-requis pour la réplication Veeam vers les datastores GCVE et NetApp volumes

Cette solution requiert les configurations et composants suivants :

1. Les volumes NetApp disposent d'un pool de stockage disposant de suffisamment de capacité disponible pour prendre en charge 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 à la source ainsi qu'aux clusters SDDC GCVE cibles.
4. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée aux machines virtuelles du serveur proxy Veeam au niveau des clusters GCVE source et cible.
5. Le serveur de sauvegarde doit pouvoir résoudre les noms abrégés et se connecter aux vCenters source et cible.

Les utilisateurs doivent établir une connexion de peering entre leur cloud privé GCVE et le projet NetApp volumes à l'aide des pages de peering de réseau VPC ou de connexions privées de l'interface utilisateur de la console cloud du moteur VMware.

> Veeam nécessite un compte utilisateur de solution GCVE avec un niveau élevé de Privileges lors de l'ajout du serveur GCVE vCenter à l'inventaire sauvegarde et réplication Veeam. Pour en savoir plus, consultez la documentation Google Cloud Platform (GCP), "VMware Engine Privileges : une solution qui va sans effet".

Pour plus d'informations, reportez-vous à "Considérations et limitations" la section de la documentation Veeam Backup & Replication.

Étapes de déploiement

Les sections suivantes présentent les différentes étapes de déploiement pour créer et monter un datastore NFS à l'aide de Google Cloud NetApp volumes, et utilisent Veeam Backup and Replication pour implémenter une solution complète de reprise d'activité entre un data Center sur site et Google Cloud VMware Engine.

Créez un volume NetApp volumes NFS et un datastore pour GCVE

Pour plus d' "Utilisation d’un volume NFS en tant que datastore vSphere hébergé par Google Cloud NetApp volumes"informations sur Google Cloud NetApp volumes en tant que datastore pour GCVE, reportez-vous au.

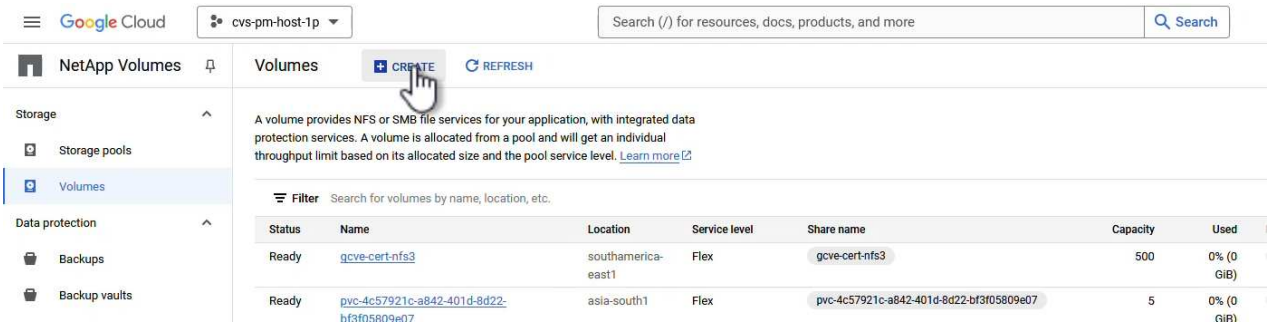
Procédez comme suit pour créer et utiliser un datastore NFS pour GCVE à l’aide de NetApp volumes :

Créez un volume NetApp volumes NFS

Google Cloud NetApp volumes est accessible depuis la console Google Cloud Platform (GCP).

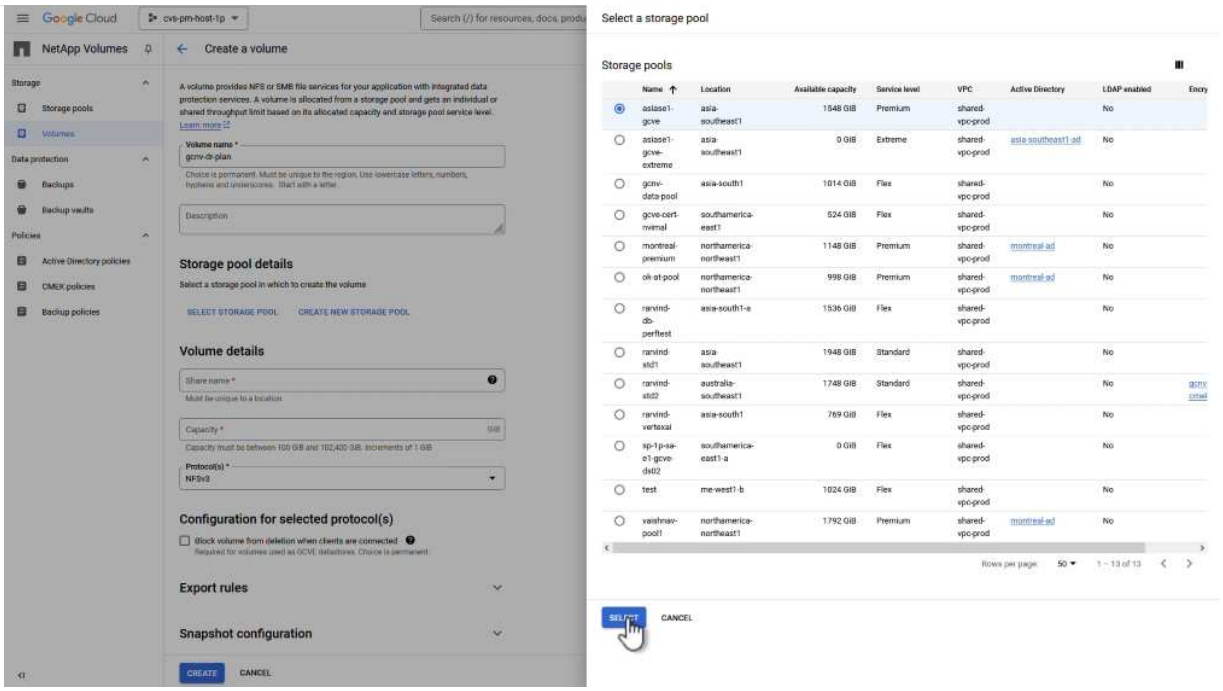
Pour "Créer un volume" plus d'informations sur cette étape, reportez-vous à la documentation de Google Cloud NetApp volumes.

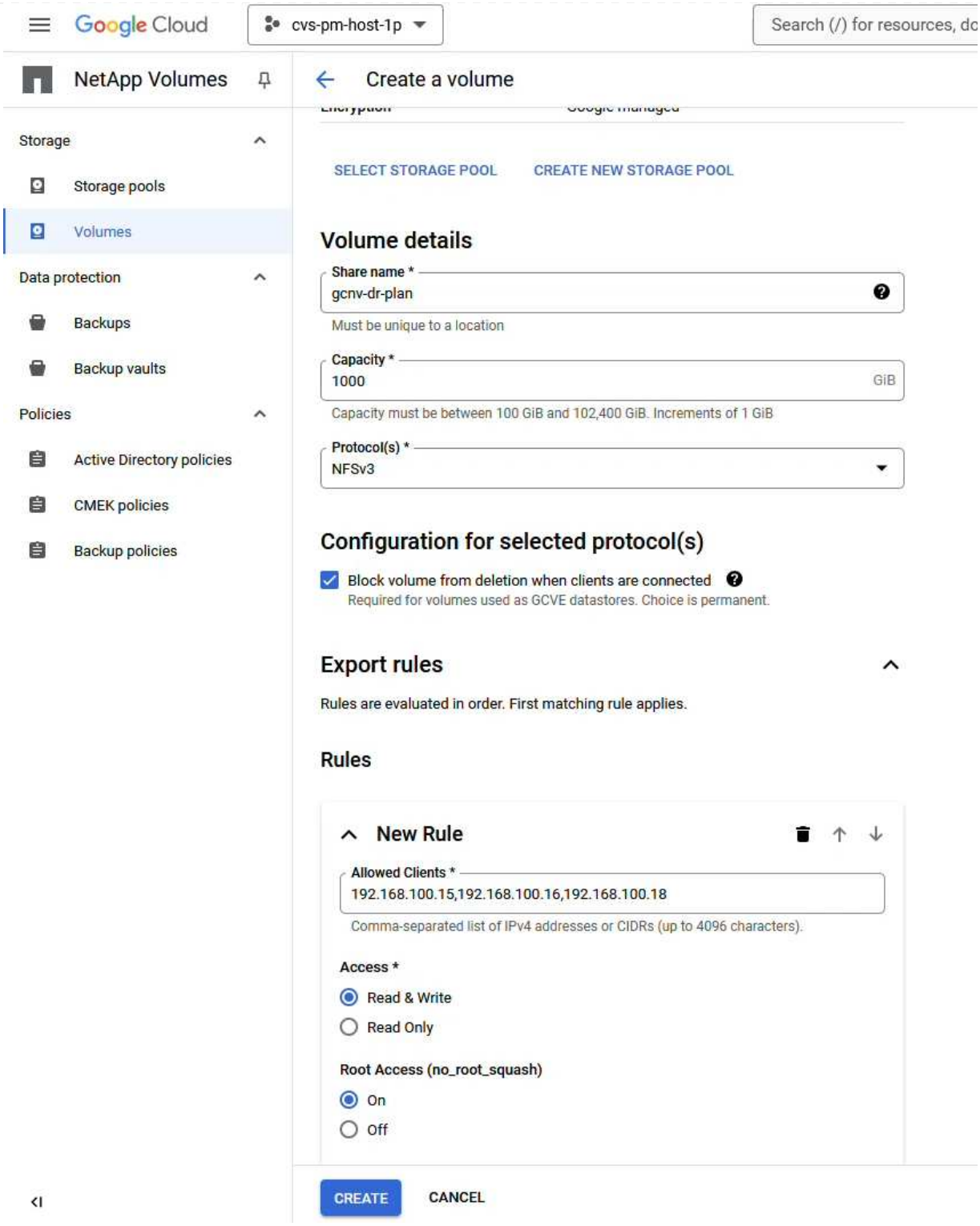
1. Dans un navigateur Web, accédez à https://console.cloud.google.com/ et connectez-vous à votre console GCP. Recherchez **NetApp volumes** pour commencer.
2. Dans l'interface de gestion **NetApp volumes**, cliquez sur **Create** pour commencer à créer un volume NFS.



3. Dans l'assistant **Créer un volume**, remplissez toutes les informations requises :
   - Nom du volume.
   - Pool de stockage sur lequel créer le volume.
   - Nom de partage utilisé lors du montage du volume NFS.
   - La capacité du volume en Gio.
   - Protocole de stockage à utiliser.
   - Cochez la case **bloquer le volume de la suppression lorsque les clients sont connectés** (requis par GCVE lors du montage en tant que datastore).
   - Règles d'export pour l'accès au volume. Il s'agit des adresses IP des adaptateurs ESXi sur le réseau NFS.
   - Planification de snapshots utilisée pour protéger le volume à l'aide de snapshots locaux.
   - Si vous le souhaitez, vous pouvez choisir de sauvegarder le volume et/ou de créer des étiquettes pour ce volume.

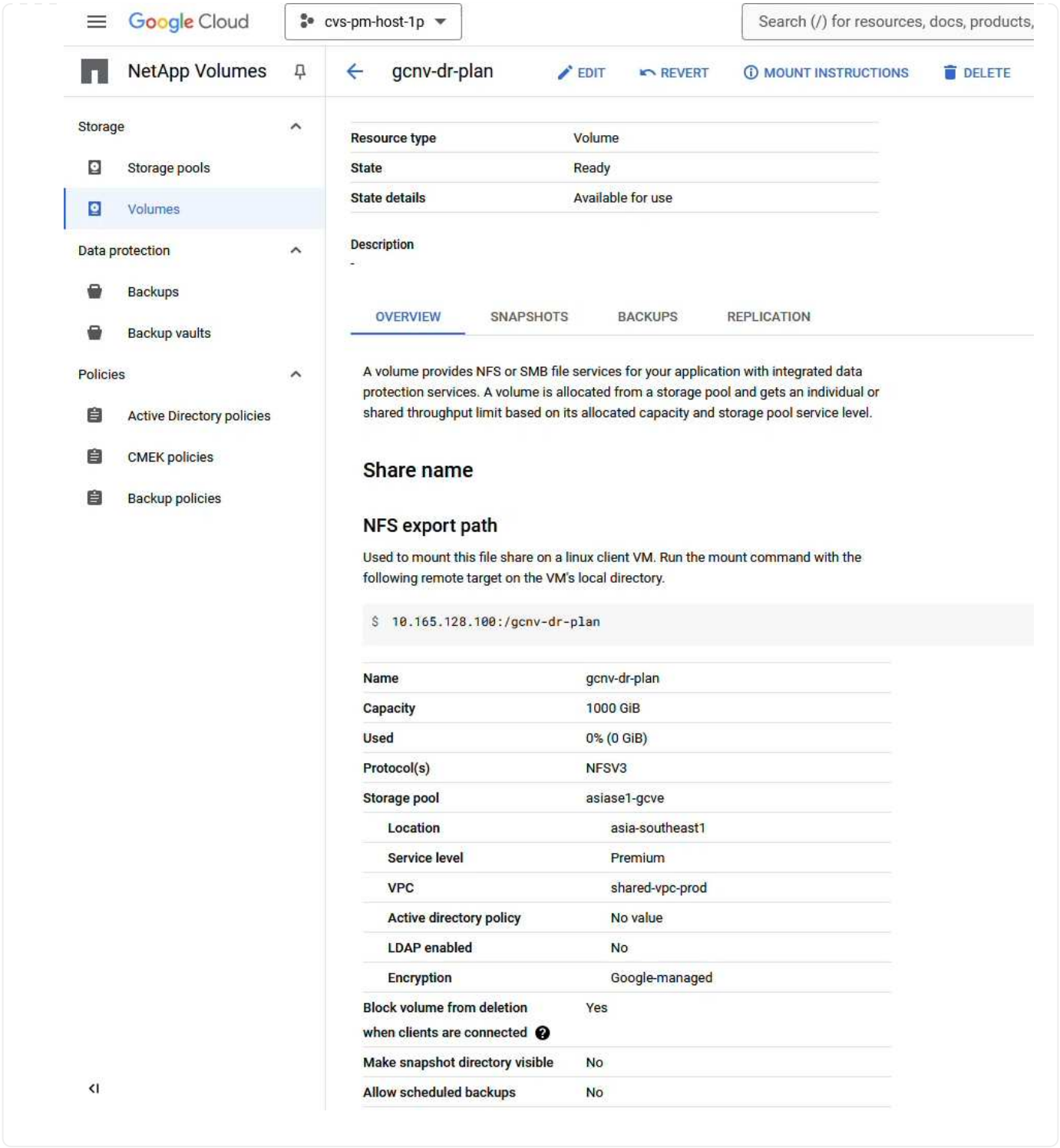
> Lors de la création d'un volume dans NetApp volumes, à utiliser en tant que datastore GCVE, seul NFS v3 est pris en charge.


Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as OCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL
Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
Encry
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
asia-southeast1
0 GiB
Extreme
shared-vpc-prod
asia-southeast1-ad
No
gcnv-data-pool
asia-south1
1014 GiB
Flex
shared-vpc-prod
No
gcve-cert-nvimal
southamerica-east1
524 GiB
Flex
shared-vpc-prod
No
montreal-premium
northamerica-northeast1
1148 GiB
Premium
shared-vpc-prod
montreal-ad
No
ok-at-pool
northamerica-northeast1
998 GiB
Premium
shared-vpc-prod
montreal-ad
No
ranvind-db-perftest
asia-south1-a
1536 GiB
Flex
shared-vpc-prod
No
ranvind-std1
asia-southeast1
1948 GiB
Standard
shared-vpc-prod
No
ranvind-std2
australia-southeast1
1748 GiB
Standard
shared-vpc-prod
No
gcnv cmek
ranvind-vertexai
asia-south1
769 GiB
Flex
shared-vpc-prod
No
sp-1p-sa-e1-gcve-ds02
southamerica-east1-a
0 GiB
Flex
shared-vpc-prod
No
test
me-west1-b
1024 GiB
Flex
shared-vpc-prod
No
vaishnav-pool1
northamerica-northeast1
1792 GiB
Premium
shared-vpc-prod
montreal-ad
No
Rows per page: 50
1 – 13 of 13
SELECT
CANCEL



cliquez sur **Create** 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 de propriétés du volume.



Montez le datastore NFS dans GCVE

Au moment d'écrire le processus de montage d'un datastore dans GCVE, vous devez ouvrir un ticket de support GCP pour que le volume soit monté en tant que datastore NFS.

Pour plus d'informations, reportez-vous à la section "Utilisation d'un volume NFS en tant que datastore vSphere hébergé par Google Cloud NetApp volumes" .

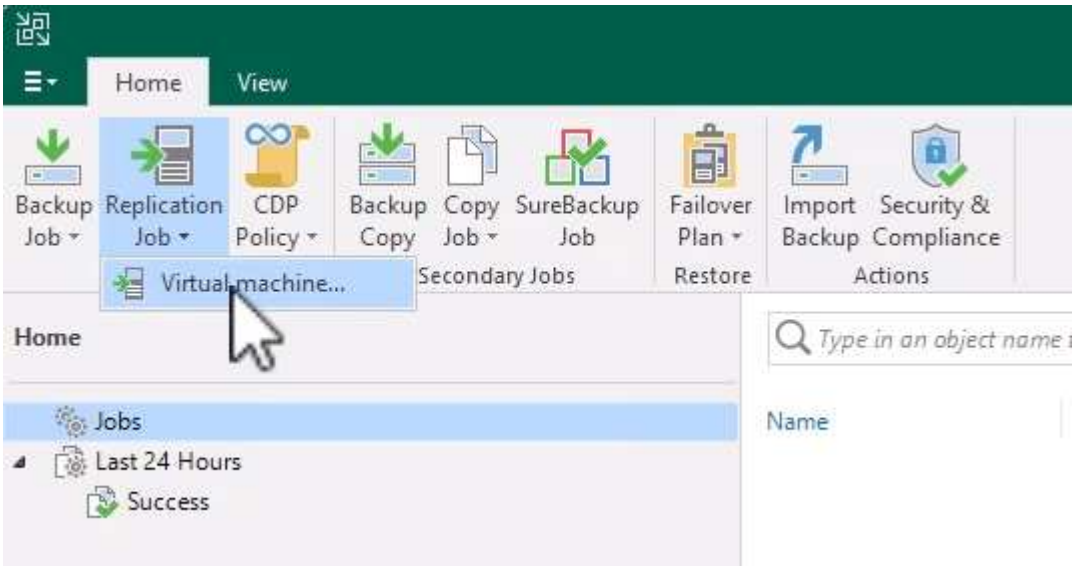
Répliquer les machines virtuelles vers GCVE et exécuter le plan de basculement et le retour arrière

Réplication de VM vers un datastore NFS dans GCVE

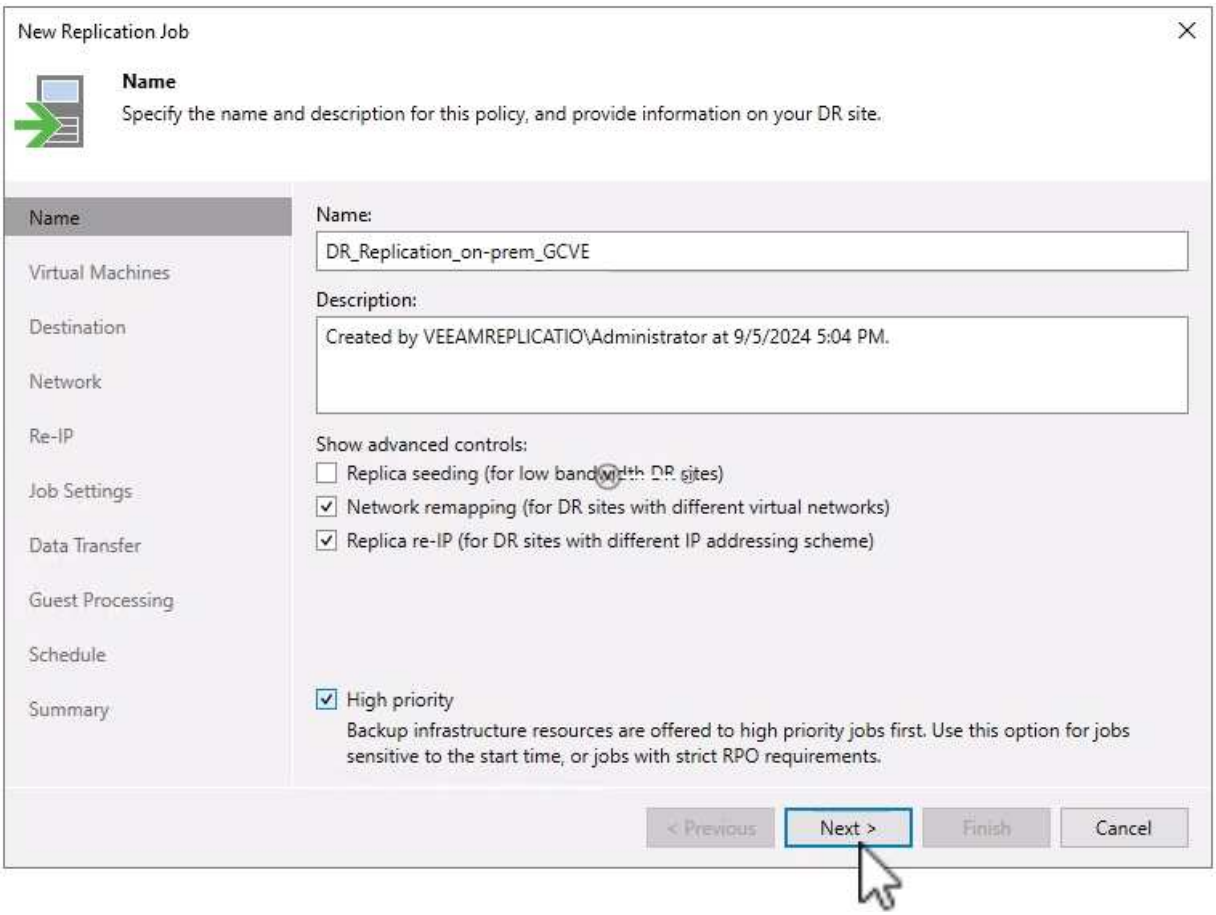
Veeam Backup & Replication exploite les fonctionnalités Snapshot de VMware vSphere pendant la réplication. Veeam Backup & Replication demande à VMware vSphere de créer un Snapshot de machine virtuelle. Le snapshot de machine virtuelle est la copie instantanée d'une machine virtuelle, qui comprend des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

Pour répliquer des machines virtuelles, procédez comme suit :

1. Ouvrez Veeam Backup & Replication Console.
2. Dans l'onglet **Home**, cliquez sur **Replication Job > Virtual machine…**

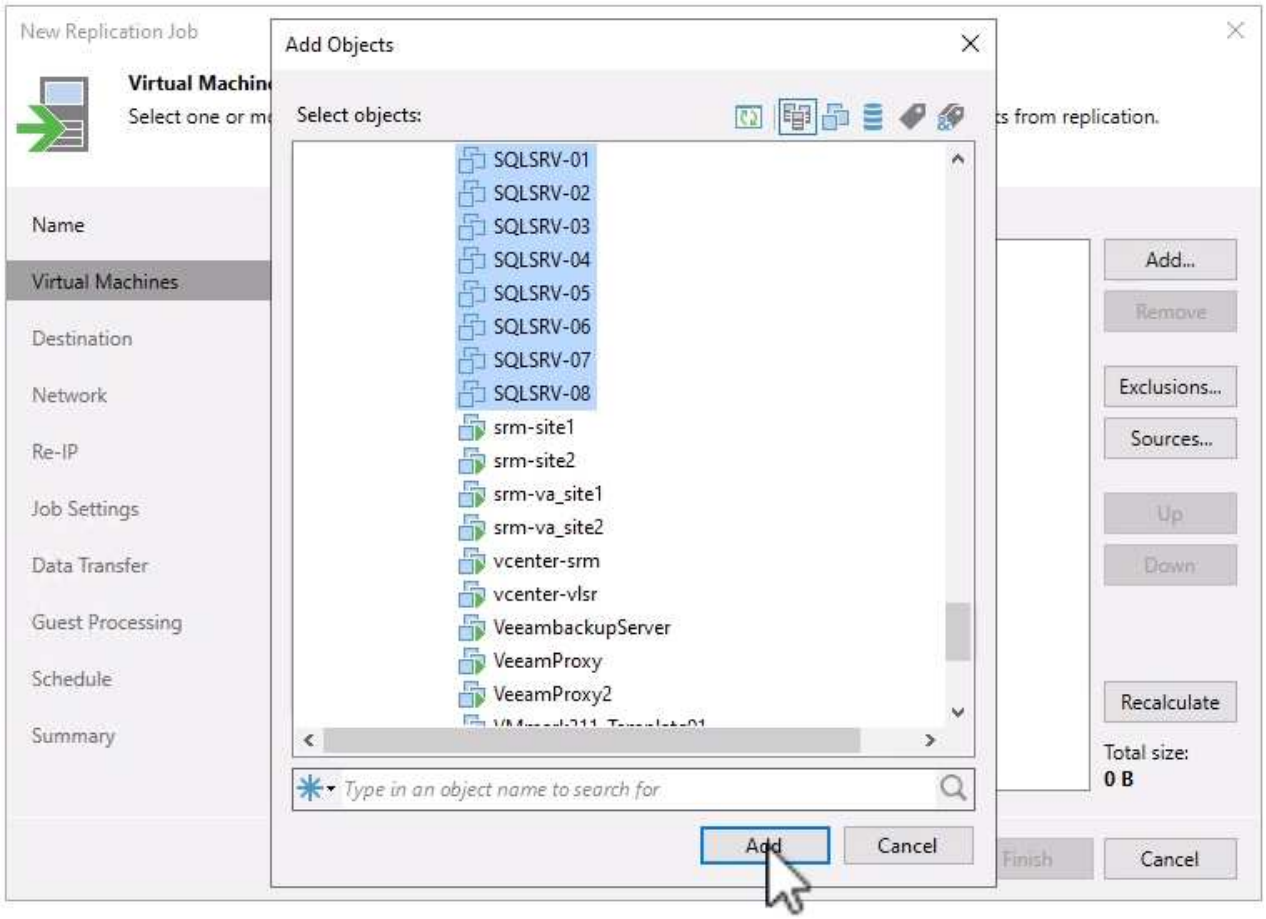


3. Sur la page **Name** de l'assistant **New Replication Job**, spécifiez un nom de travail et cochez les cases de contrôle avancé appropriées.
   - Cochez la case amorçage du réplica si la connectivité entre le site et GCP a une bande passante limitée.
   - Cochez la case remappage réseau (pour les sites SDDC GCVE avec différents réseaux) si les segments du SDDC GCVE ne correspondent pas à ceux des réseaux de sites sur site.
   - Cochez la case Replica re-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.

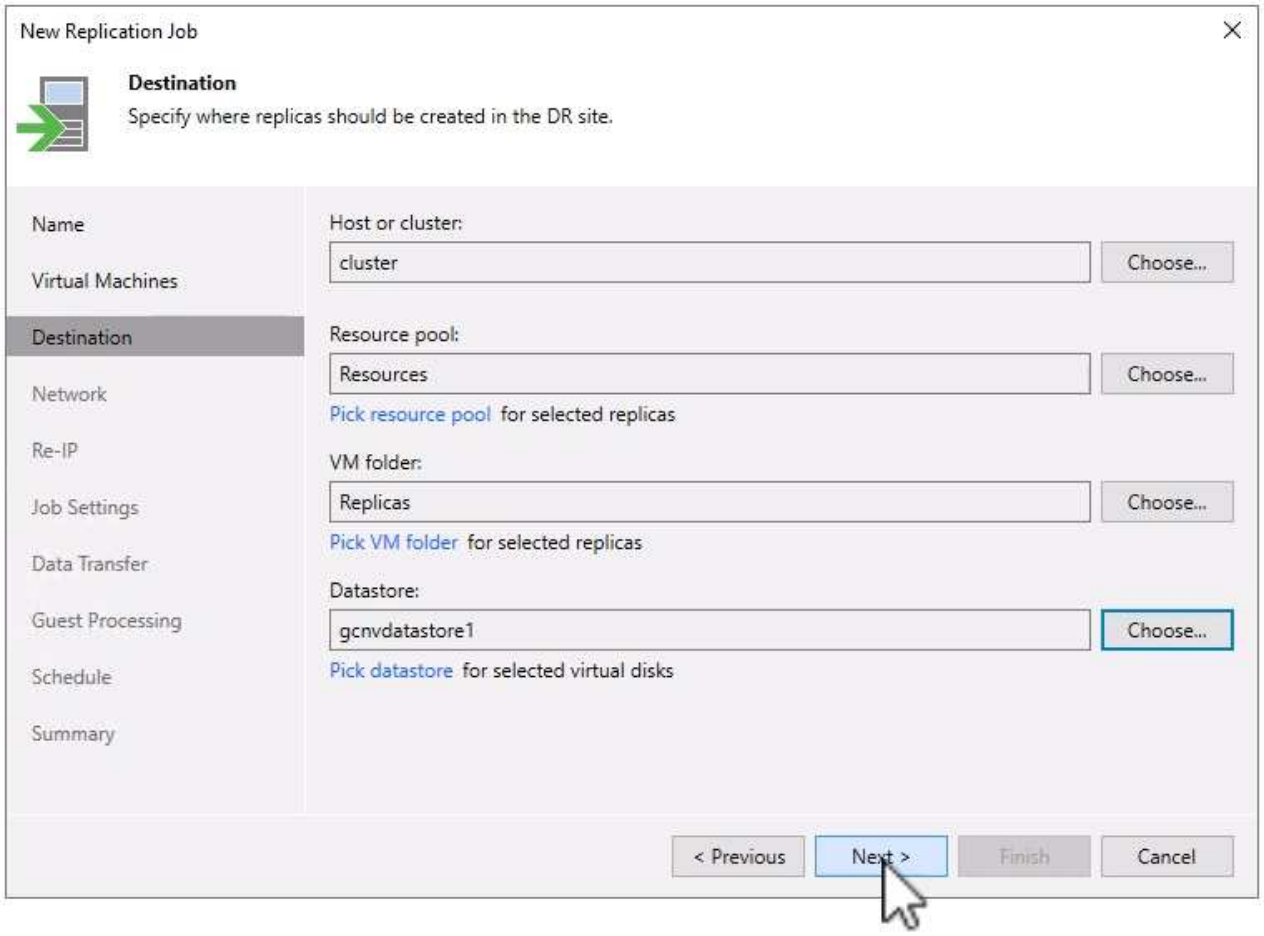


4. Sur la page **machines virtuelles**, sélectionnez les machines virtuelles à répliquer dans le datastore NetApp volumes rattaché à un SDDC GCVE. Cliquez sur **Ajouter**, puis dans la fenêtre **Ajouter un objet**, sélectionnez les machines virtuelles ou les conteneurs VM nécessaires et cliquez sur **Ajouter**. Cliquez sur **Suivant**.

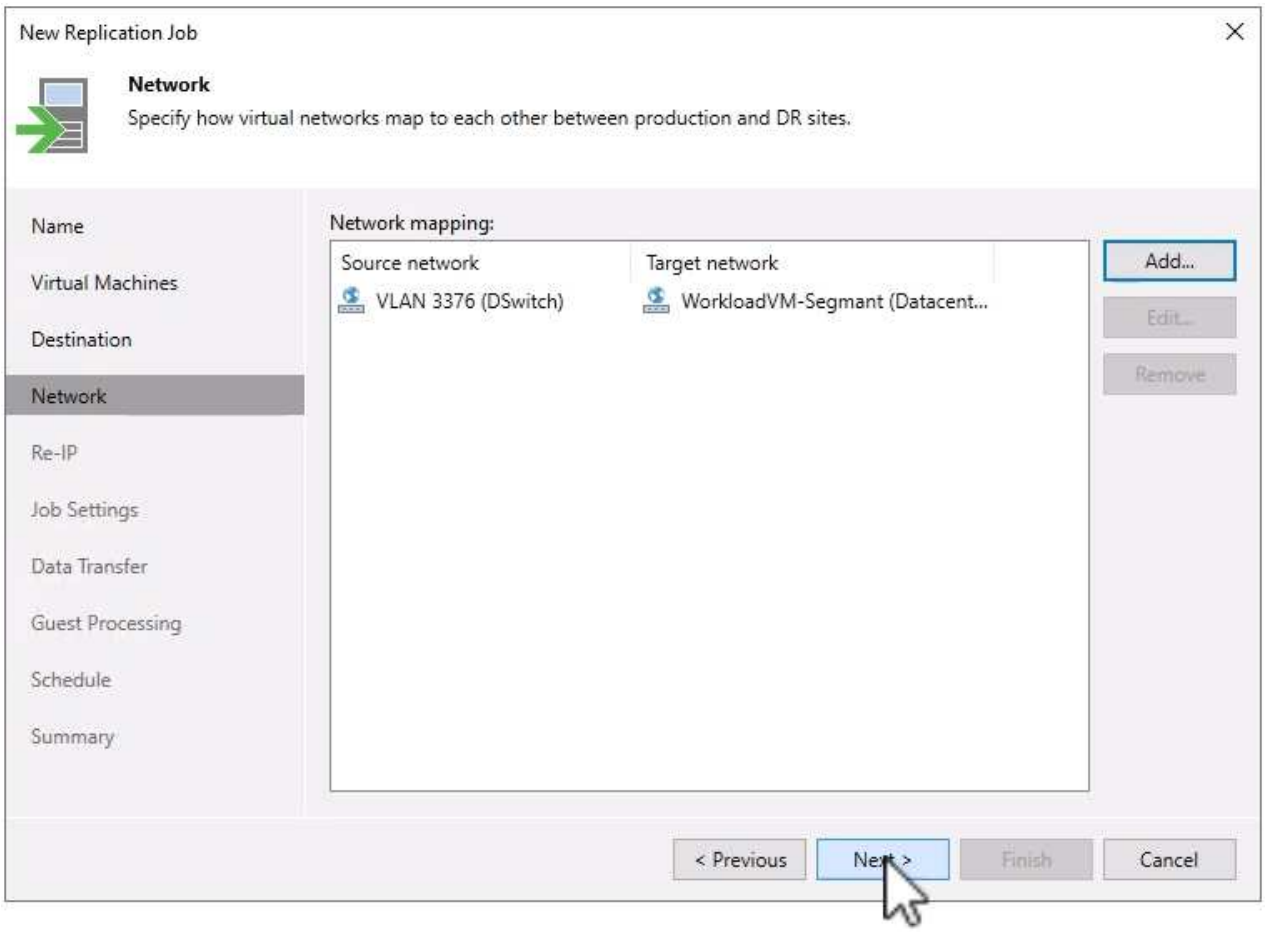
> Les machines virtuelles peuvent être placées sur VSAN pour remplir la capacité de datastore VSAN disponible. Dans un cluster piloté, la capacité utilisable d'un cluster VSAN à 3 nœuds sera limitée. Le reste des données peut être facilement placé dans les datastores Google Cloud NetApp volumes afin de pouvoir restaurer les machines virtuelles. Par la suite, le cluster peut être étendu pour répondre aux exigences de processeur/mètre.



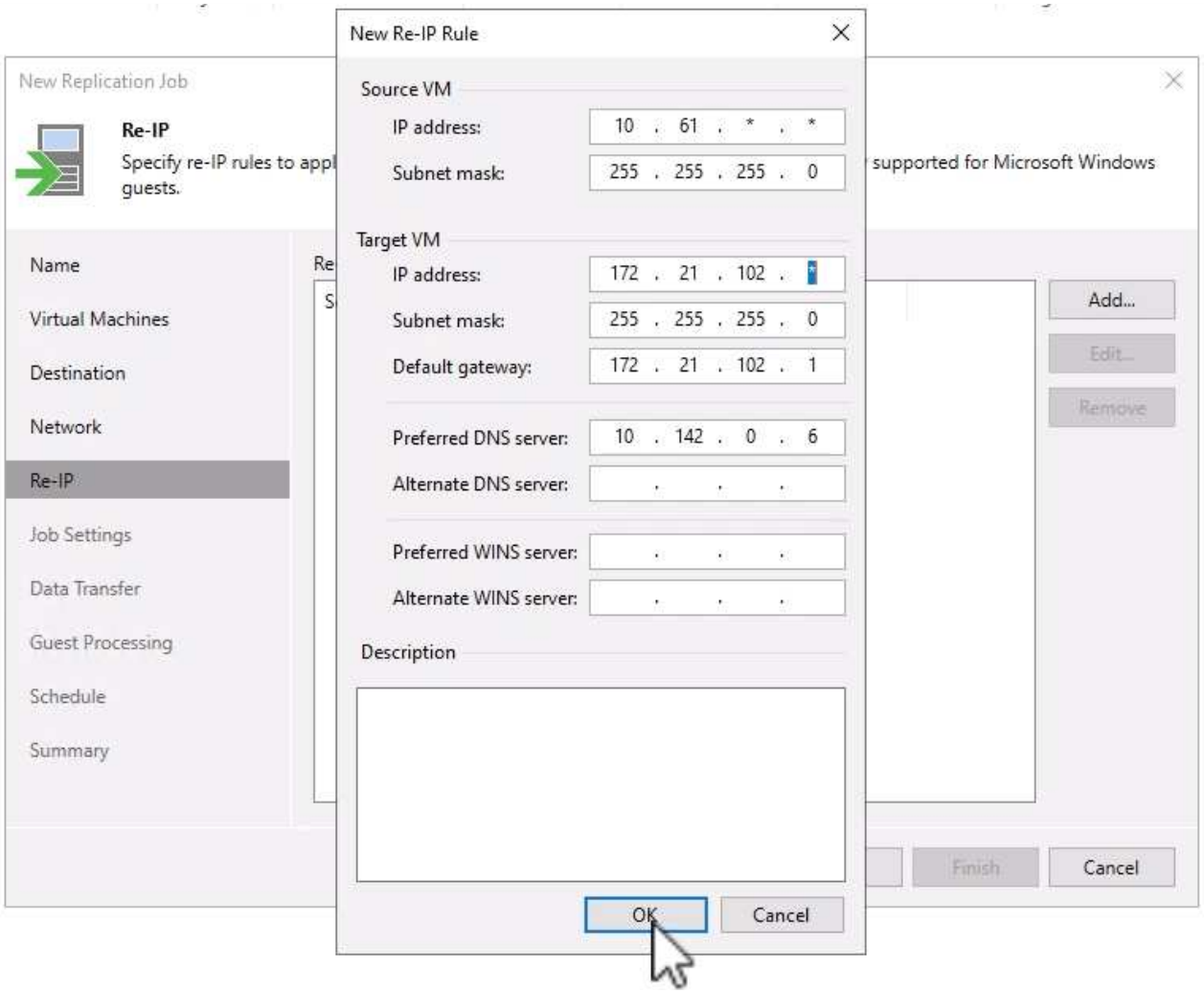
5. Sur la page **destination**, sélectionnez la destination en tant que cluster/hôtes SDDC GCVE et le pool de ressources, le dossier VM et le datastore GCNV appropriés pour les répliques VM. Cliquez sur **Suivant** pour continuer.



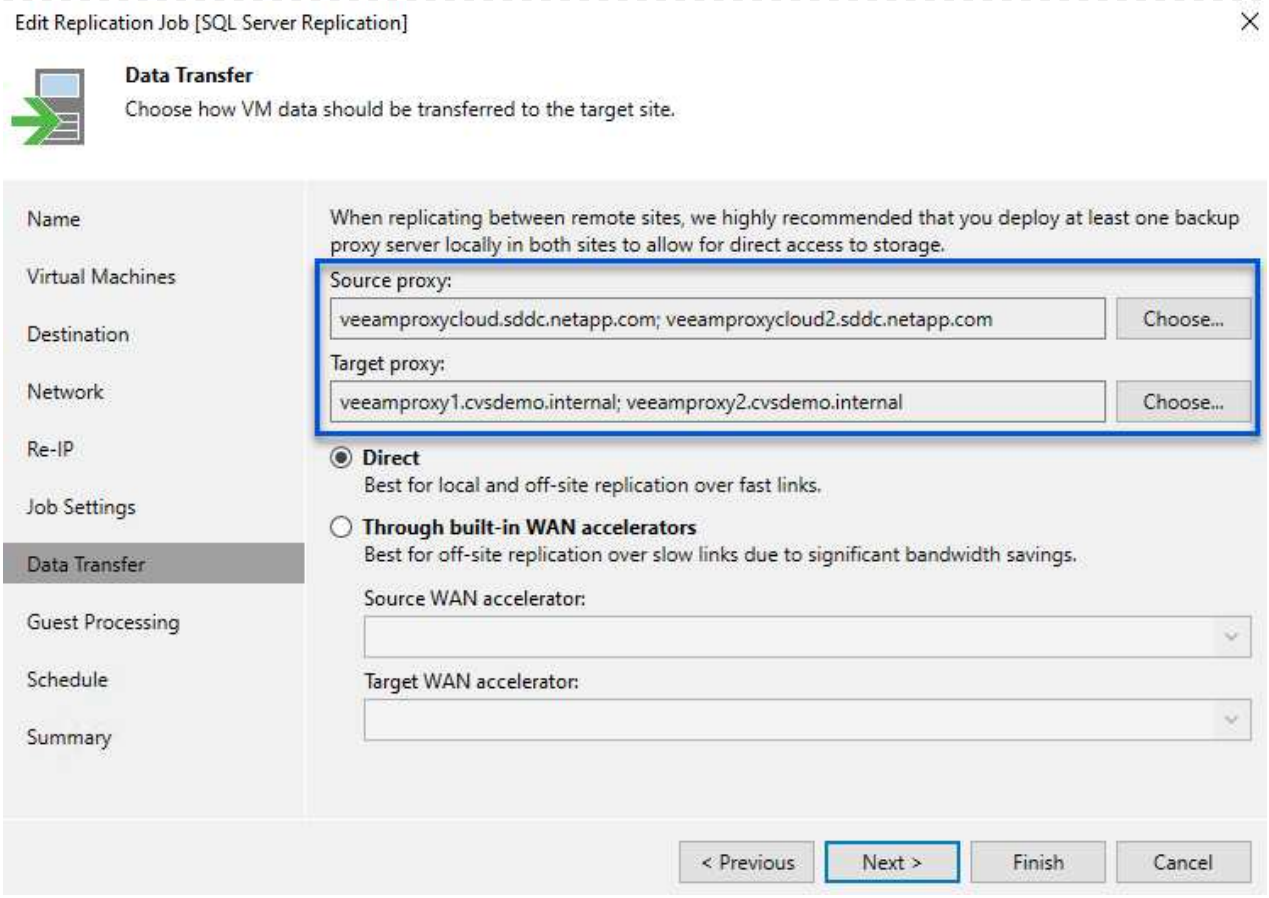
6. Sur la page **réseau**, créez le mappage entre les réseaux virtuels source et cible selon vos besoins. Cliquez sur **Suivant** pour continuer.



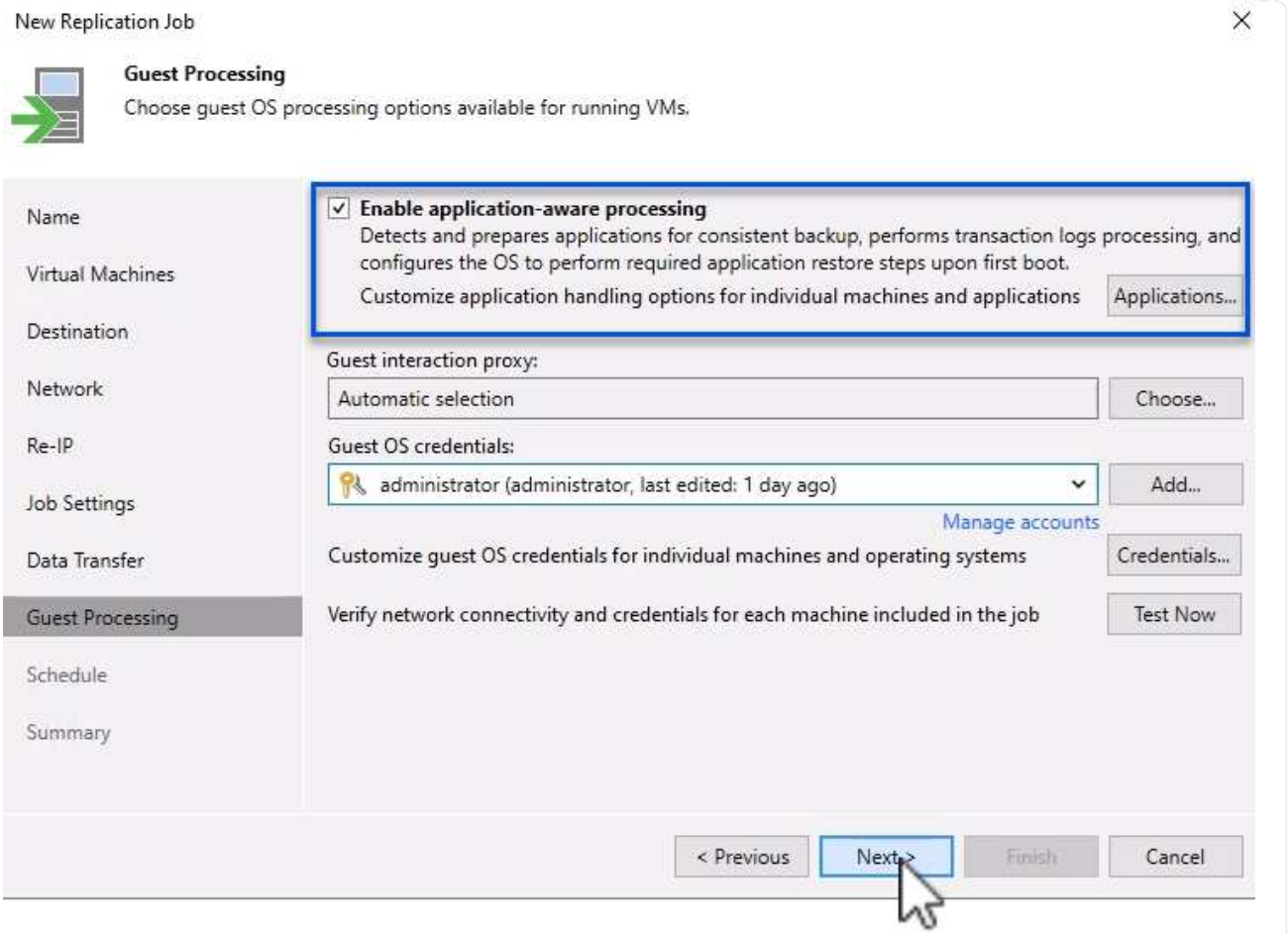
7. Sur la page **Re-IP**, cliquez sur le bouton **Ajouter…** pour ajouter une nouvelle règle re-ip. Remplissez les plages d'adresses ip de la machine virtuelle source et cible pour spécifier la mise en réseau qui sera appliquée à la machine virtuelle source en cas de basculement. Utilisez des astérisques pour spécifier une plage d'adresses est indiquée pour cet octet. Cliquez sur **Suivant** pour continuer.



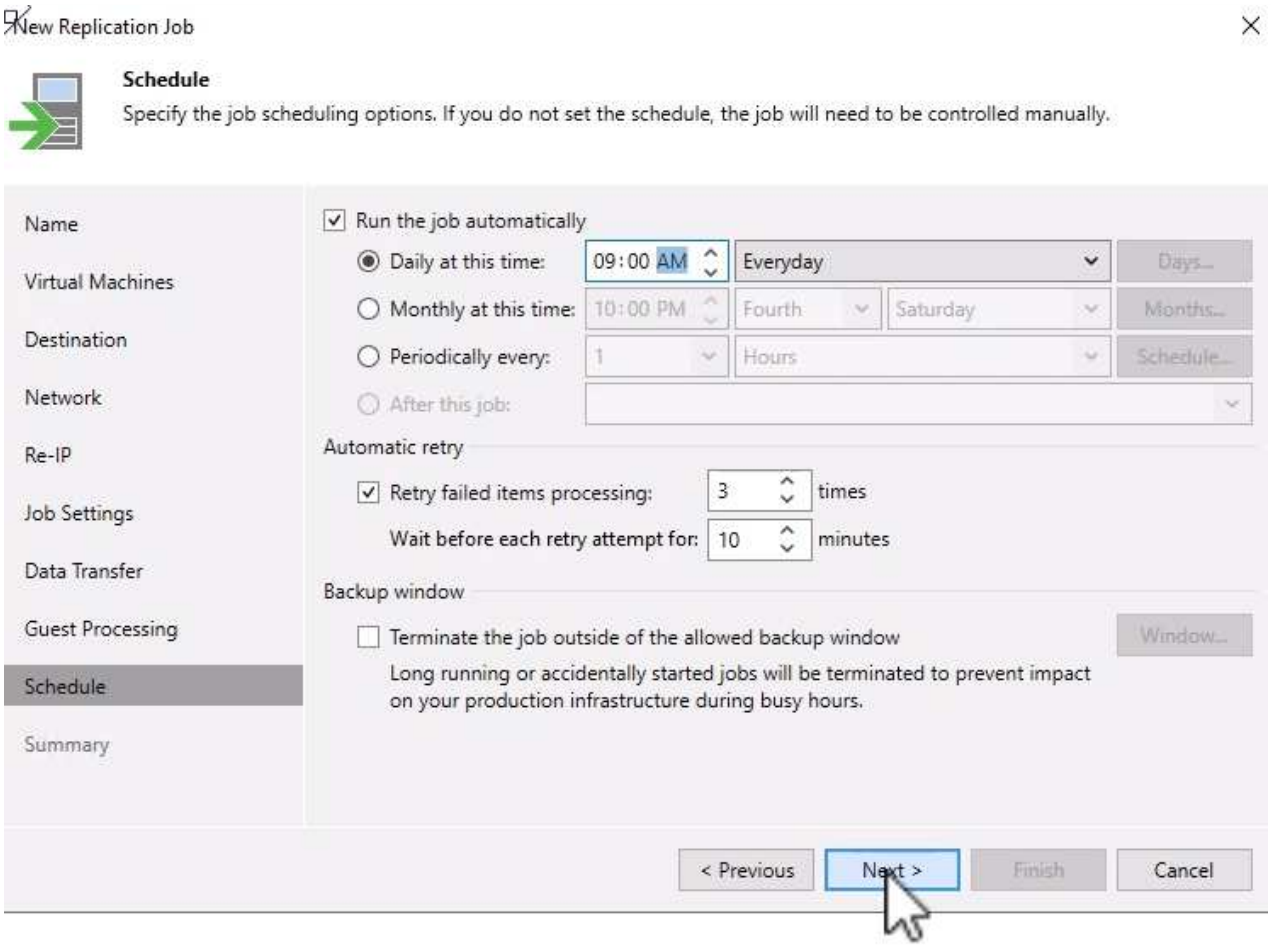
8. Sur la page **Paramètres du travail**, spécifiez le référentiel de sauvegarde qui stocke les métadonnées pour les répliques VM, la stratégie de rétention et sélectionnez le bouton en bas pour le bouton **Avancé…** en bas pour les paramètres de travail supplémentaires. Cliquez sur **Suivant** pour continuer.
9. Sur le **transfert de données**, sélectionnez les serveurs proxy qui résident sur les sites source et cible, et laissez l'option Direct sélectionnée. Les accélérateurs WAN peuvent également être sélectionnés ici, s'ils sont configurés. Cliquez sur **Suivant** pour continuer.



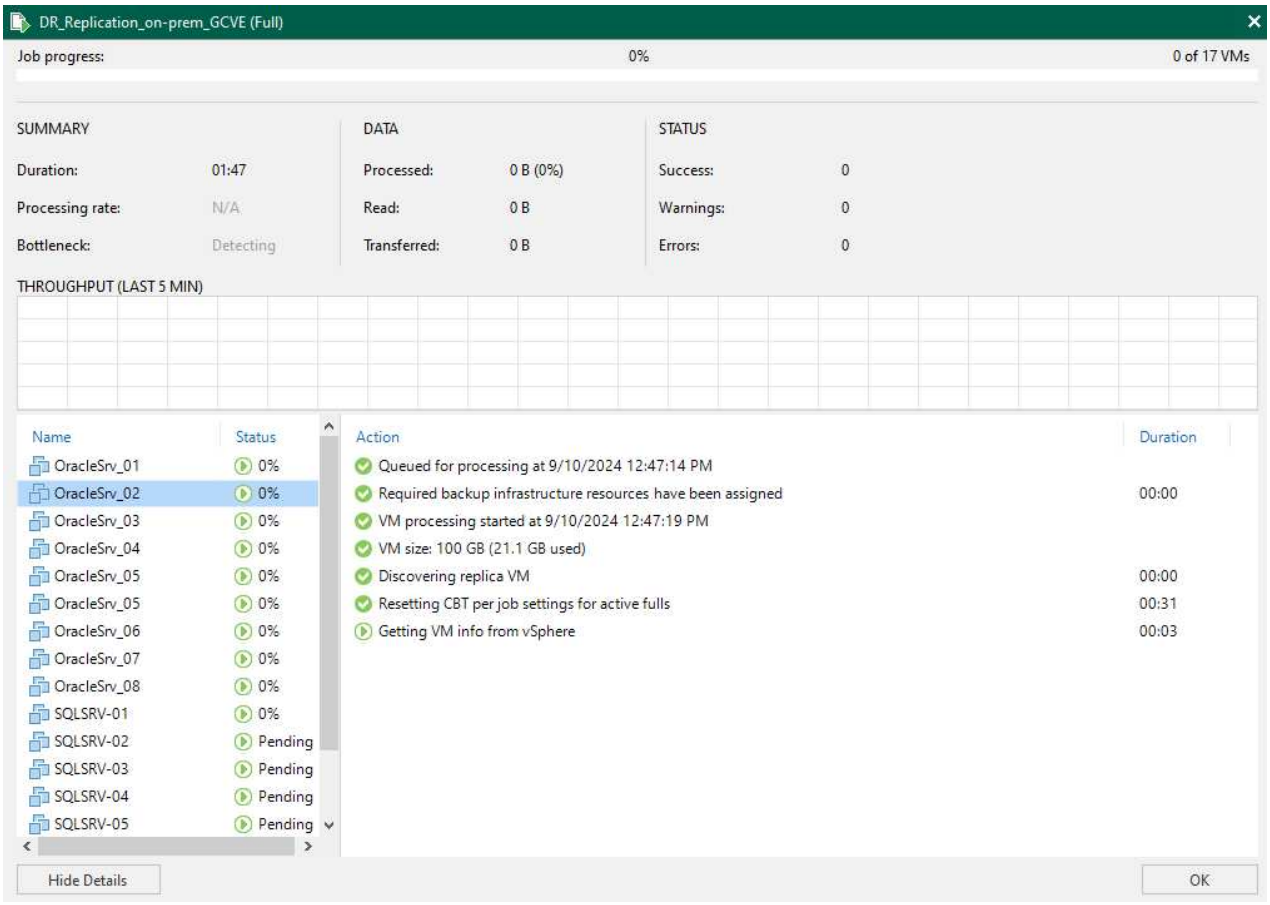
10. Sur la page **Guest Processing**, cochez la case **Enable application-Aware processing** selon les besoins et sélectionnez **Guest OS credentials**. Cliquez sur **Suivant** pour continuer.



11. Sur la page **Schedule**, définissez les heures et la fréquence d'exécution de la tâche de réplication. Cliquez sur **Suivant** pour continuer.



12. Enfin, passez en revue 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 exécutée, la tâche de réplication peut être affichée dans la fenêtre d'état de la tâche.



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

Créer un plan de basculement

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

Une fois la réplication ou l'amorçage initial terminé, créez un plan de basculement. Ce plan sert de référence stratégique pour l'orchestration du basculement des machines virtuelles dépendantes, individuellement ou en groupe. Il définit l'ordre de traitement des machines virtuelles, intègre les retards de démarrage nécessaires et veille à ce que les machines virtuelles dépendantes critiques soient opérationnelles avant les autres. En mettant en place un plan de basculement bien structuré, les entreprises peuvent rationaliser leur processus de reprise après incident, en réduisant les temps d'arrêt et en préservant l'intégrité des systèmes interdépendants lors d'un basculement.

Lors de la création du plan, Veeam Backup & Replication identifie automatiquement les points de restauration les plus récents pour initier les répliques de machine virtuelle.

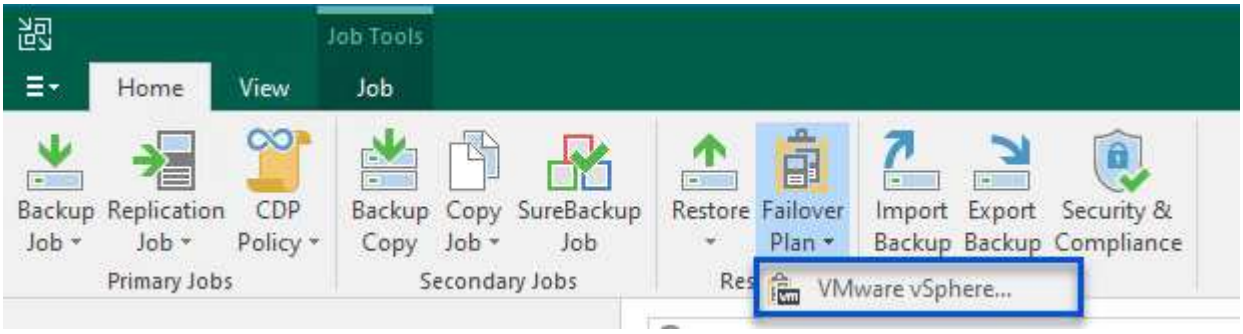
> Le plan de basculement ne peut être créé qu'une fois la réplication initiale terminée et les répliques de machine virtuelle à l'état prêt.

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

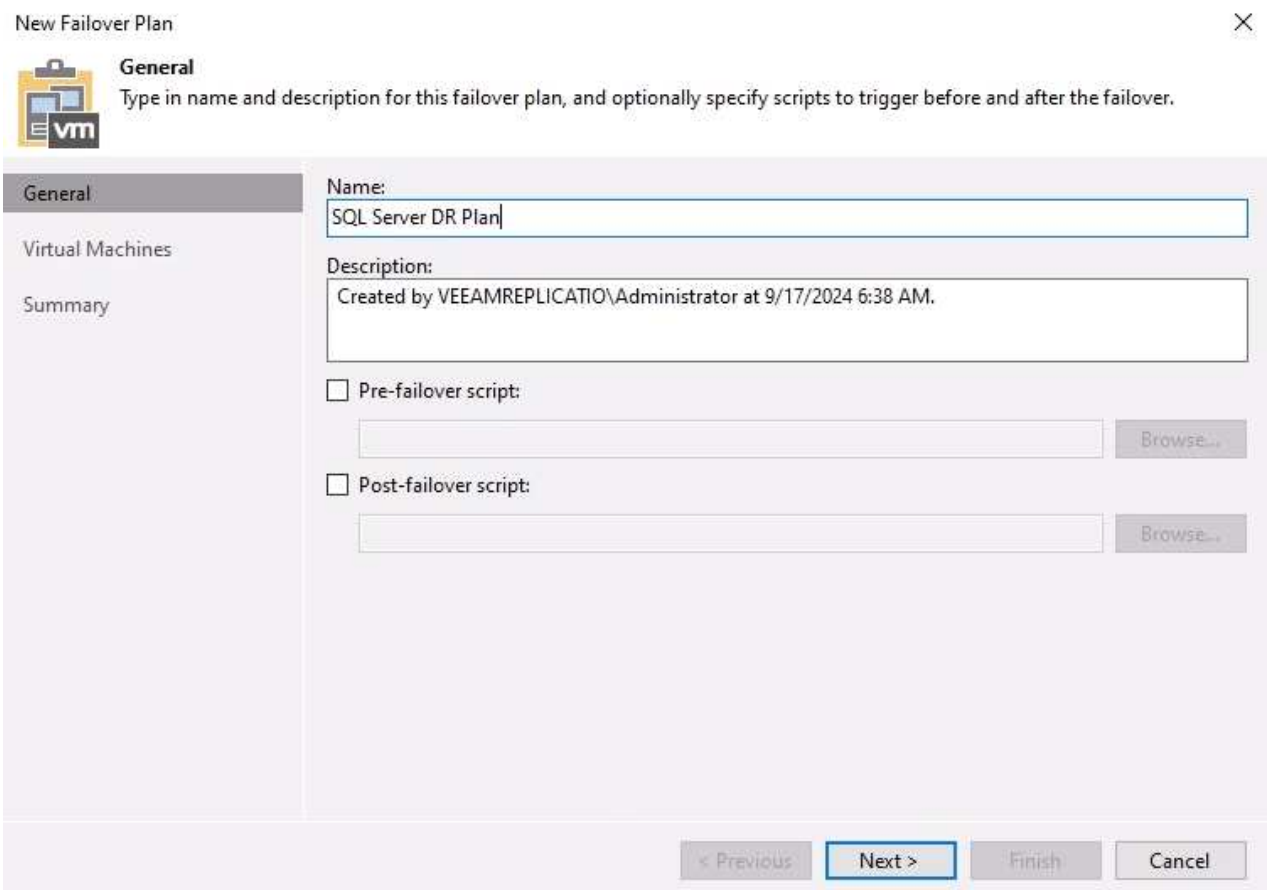
> Pendant le processus de basculement, les machines virtuelles source ne sont pas hors tension.

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

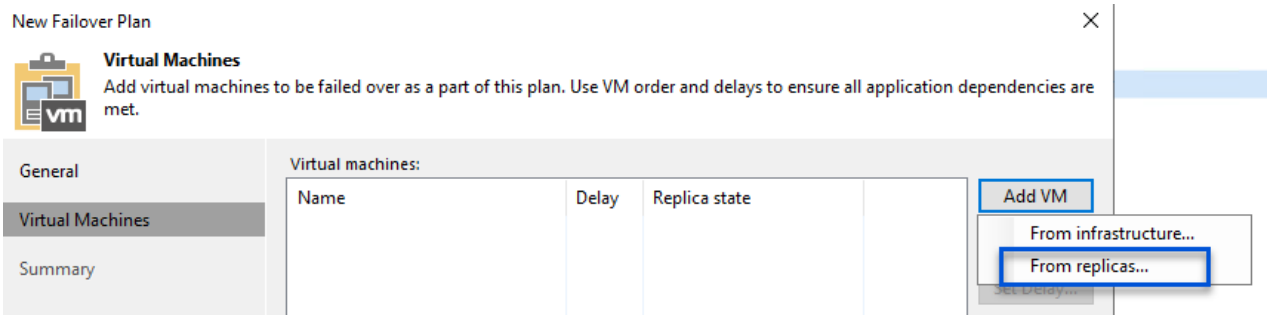
1. Dans la vue **Accueil**, cliquez sur le bouton **Plan de basculement** dans la section **Restaurer**. Dans la liste déroulante, sélectionnez **VMware vSphere…**

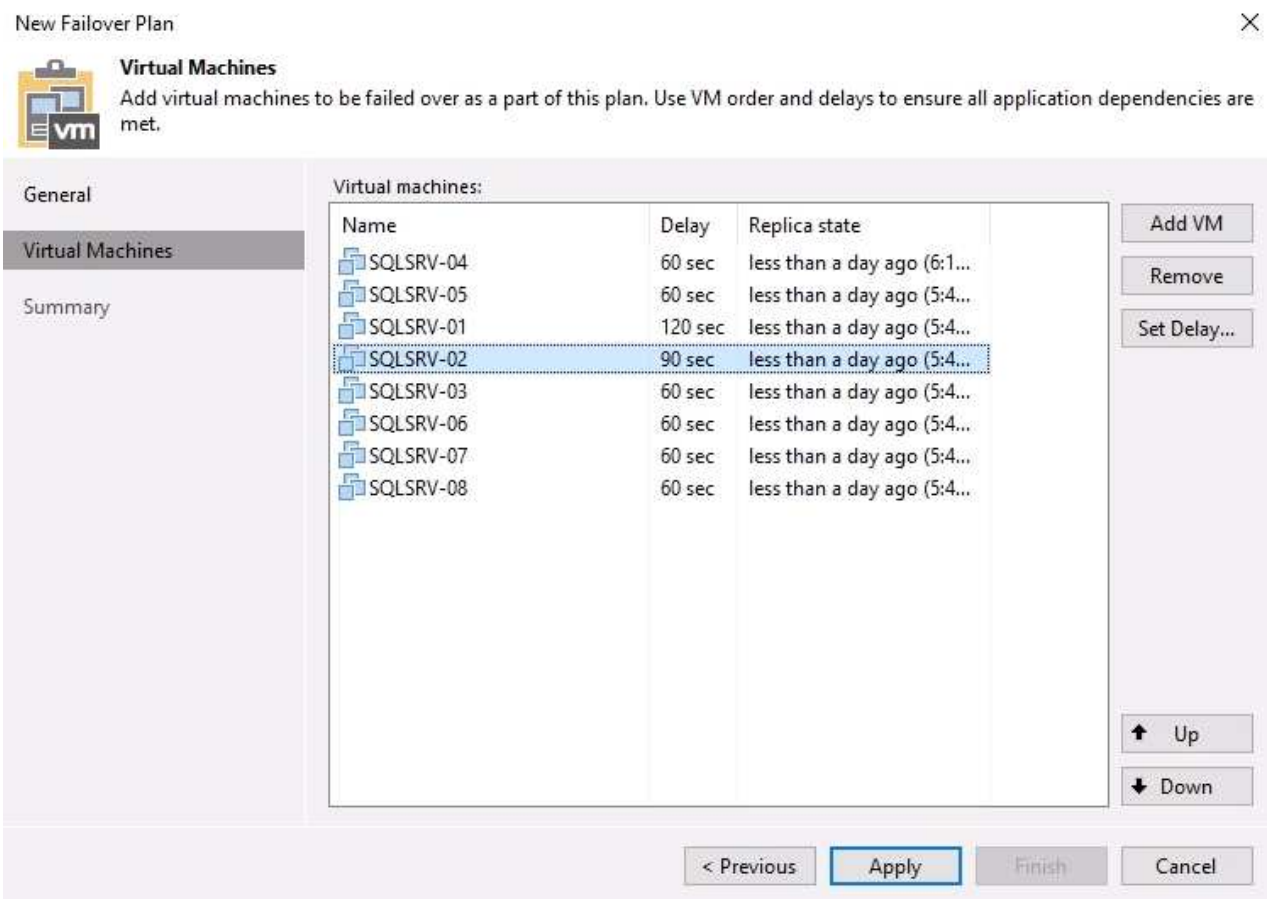


2. Sur la page **général** de l'assistant **Nouveau plan de basculement**, indiquez un nom et une description du plan. Des scripts de pré et post-basculement peuvent être ajoutés si nécessaire. Par exemple, exécutez un script pour arrêter les machines virtuelles avant de démarrer les machines virtuelles répliquées.



3. Sur la page **machines virtuelles**, cliquez sur le bouton **Ajouter VM** et sélectionnez **à partir des répliques…**. Choisissez les machines virtuelles à intégrer au plan de basculement, puis modifiez l'ordre de démarrage de la machine virtuelle et les délais de démarrage requis pour répondre aux dépendances des applications.





Cliquez sur **appliquer** pour continuer.

4. Enfin, passez en revue 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 "Création de travaux de réplication"à la section .

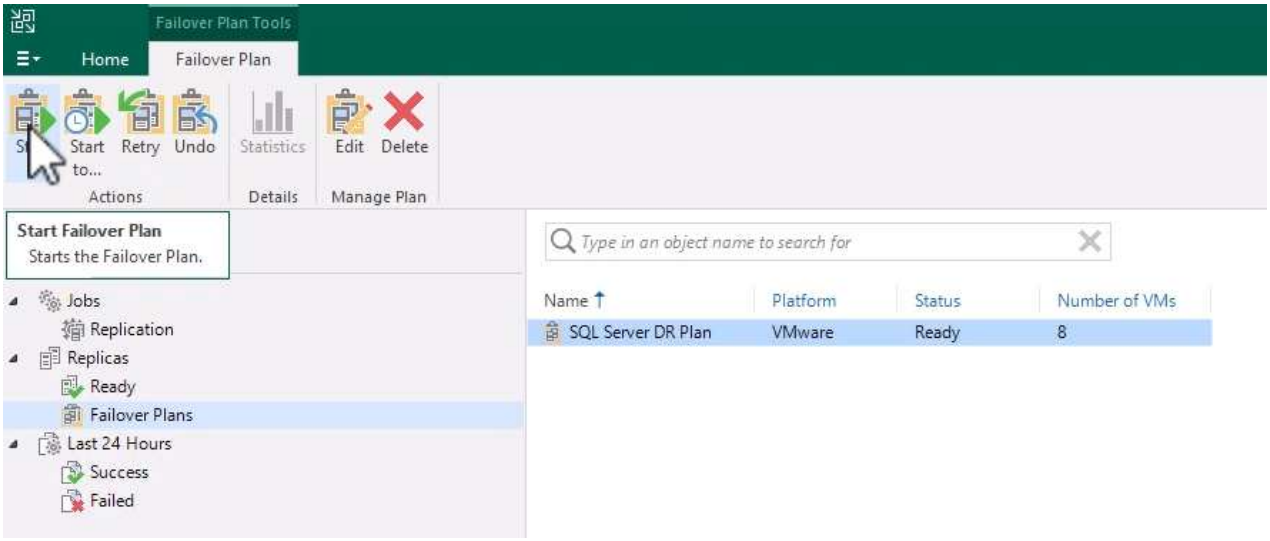
Exécutez le plan de basculement

Lors du basculement, la machine virtuelle source du site de production bascule sur sa réplique sur le site de reprise après incident. Dans le cadre de ce processus, Veeam Backup & Replication restaure le réplica de la machine virtuelle vers le point de restauration requis et transfère toutes les activités d'E/S depuis la machine virtuelle source vers son réplica. Les réplicas servent non seulement pour les incidents réels, mais aussi pour la simulation des exercices de reprise après incident. Lors de la simulation de basculement, la machine virtuelle source continue de s'exécuter. Une fois les tests nécessaires terminés, le basculement peut être annulé et les opérations reprennent normalement.

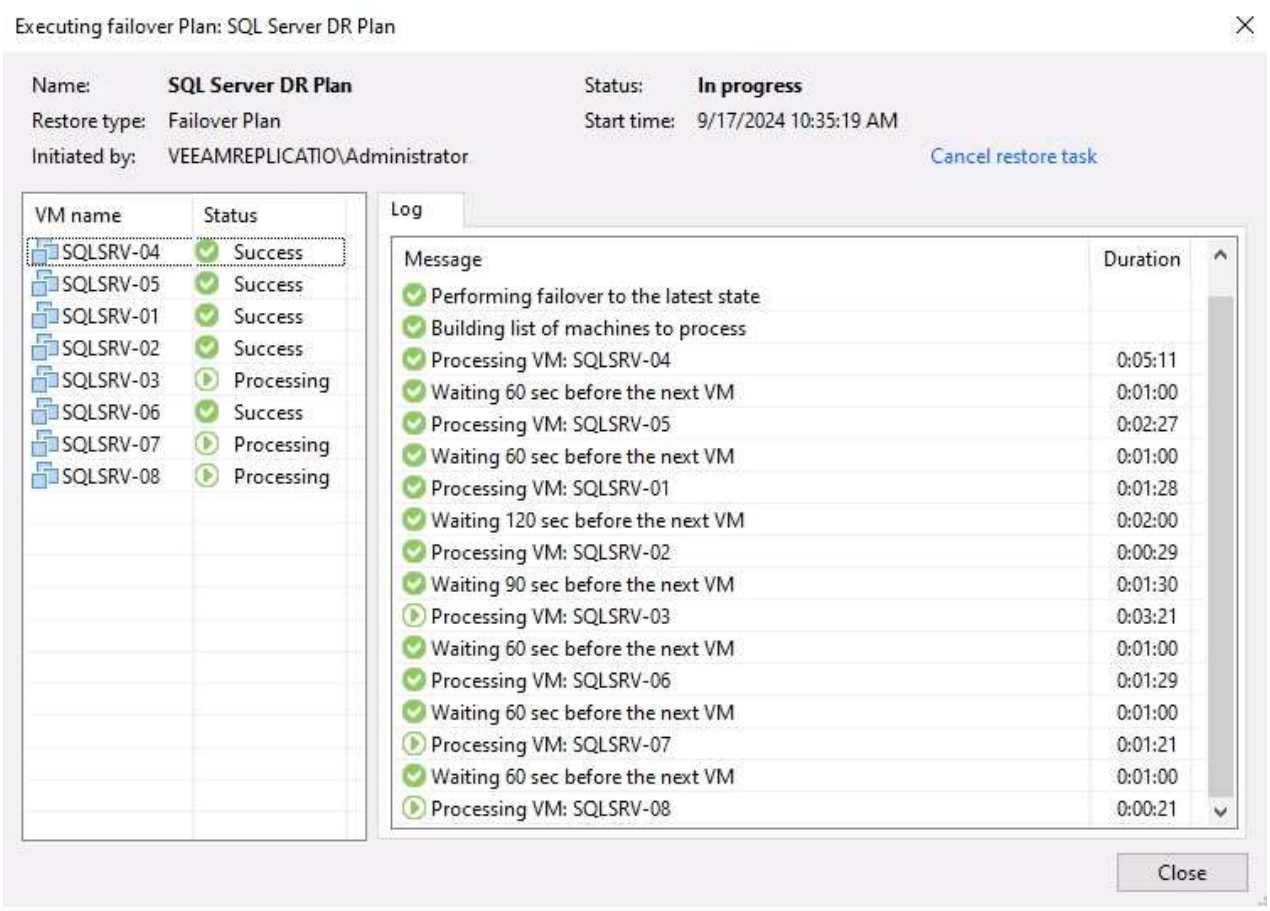
Assurez-vous que la segmentation réseau est en place pour éviter les conflits d'adresses IP lors du basculement.

Pour démarrer le plan de basculement, procédez comme suit :

1. Pour commencer, dans la vue **Accueil**, cliquez sur **répliques > plans de basculement** dans le menu de gauche, puis sur le bouton **Démarrer**. Vous pouvez également utiliser le bouton **Démarrer à…** 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 de la machine virtuelle source jusqu'à ce que son réplica revienne à l'état prêt.

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

Restauration vers le site de production

La réalisation d'un basculement est considérée comme une étape intermédiaire et doit être finalisée en fonction de l'exigence. Les options sont les suivantes :

- **Retour en production** - revenir à la machine virtuelle d'origine et synchroniser toutes les modifications apportées pendant la période active de la réplique vers la machine virtuelle source.

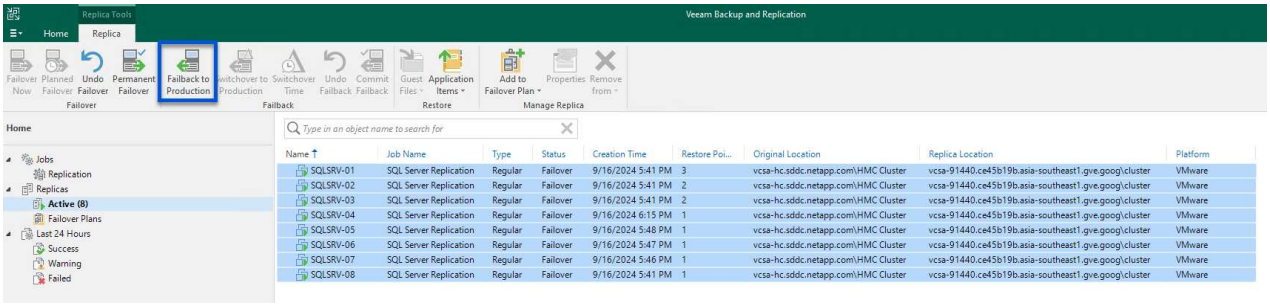
> Pendant le rétablissement, les modifications sont transférées mais ne sont pas appliquées immédiatement. Sélectionnez **COMMIT. Retour arrière** une fois la fonctionnalité de la machine virtuelle d'origine vérifiée. Vous pouvez également choisir **Annuler le retour arrière** pour revenir à la réplique 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 abandonnant toutes les modifications apportées à la réplique de la machine virtuelle pendant sa période opérationnelle.
- **Basculement permanent** - basculez de manière permanente de la machine virtuelle d'origine vers sa réplique, établissant la réplique comme nouvelle machine virtuelle primaire pour les opérations en cours.

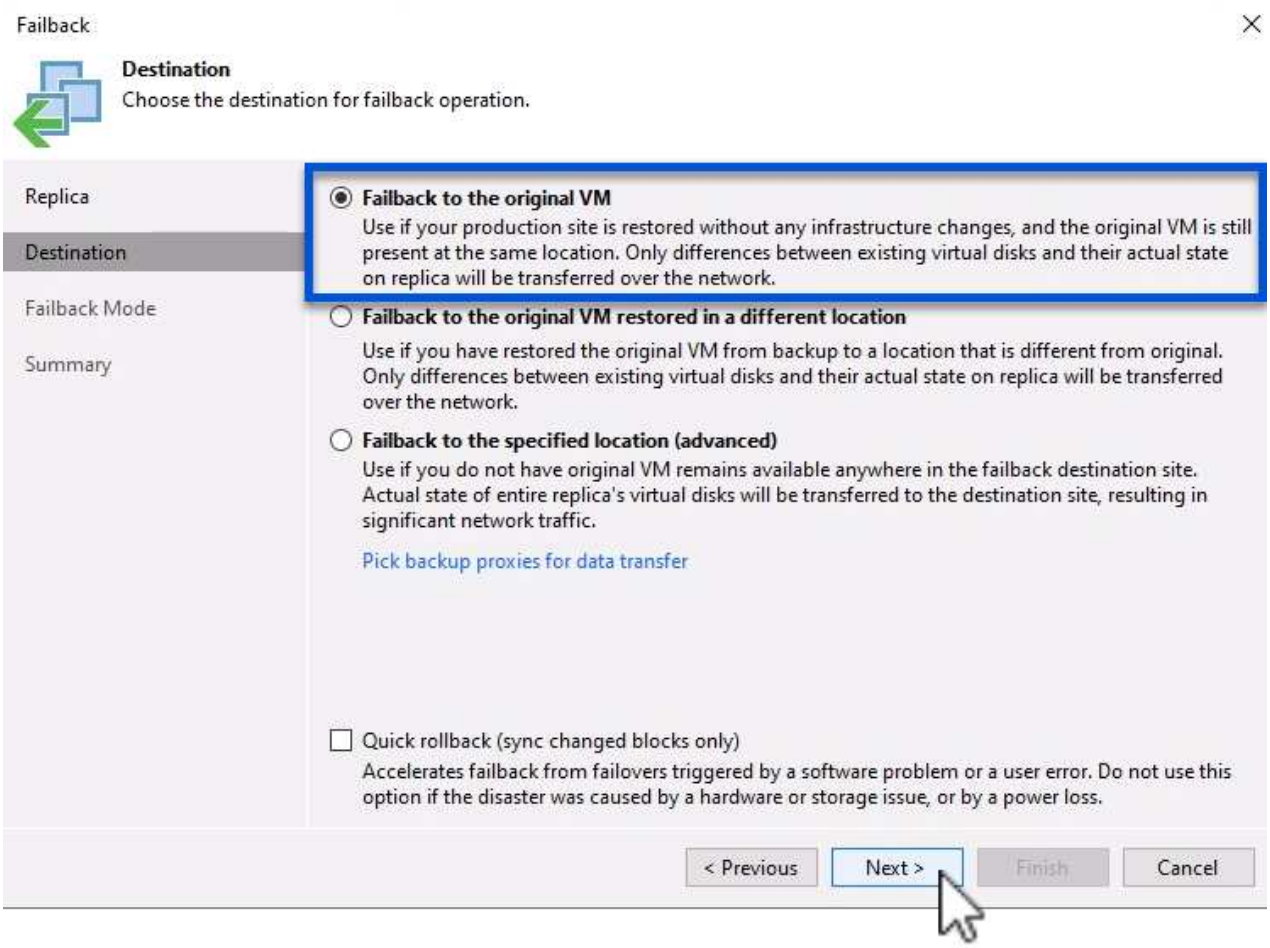
Dans ce scénario, l'option « revenir à la production » a été sélectionnée.

Pour effectuer un retour arrière sur le site de production, procédez comme suit :

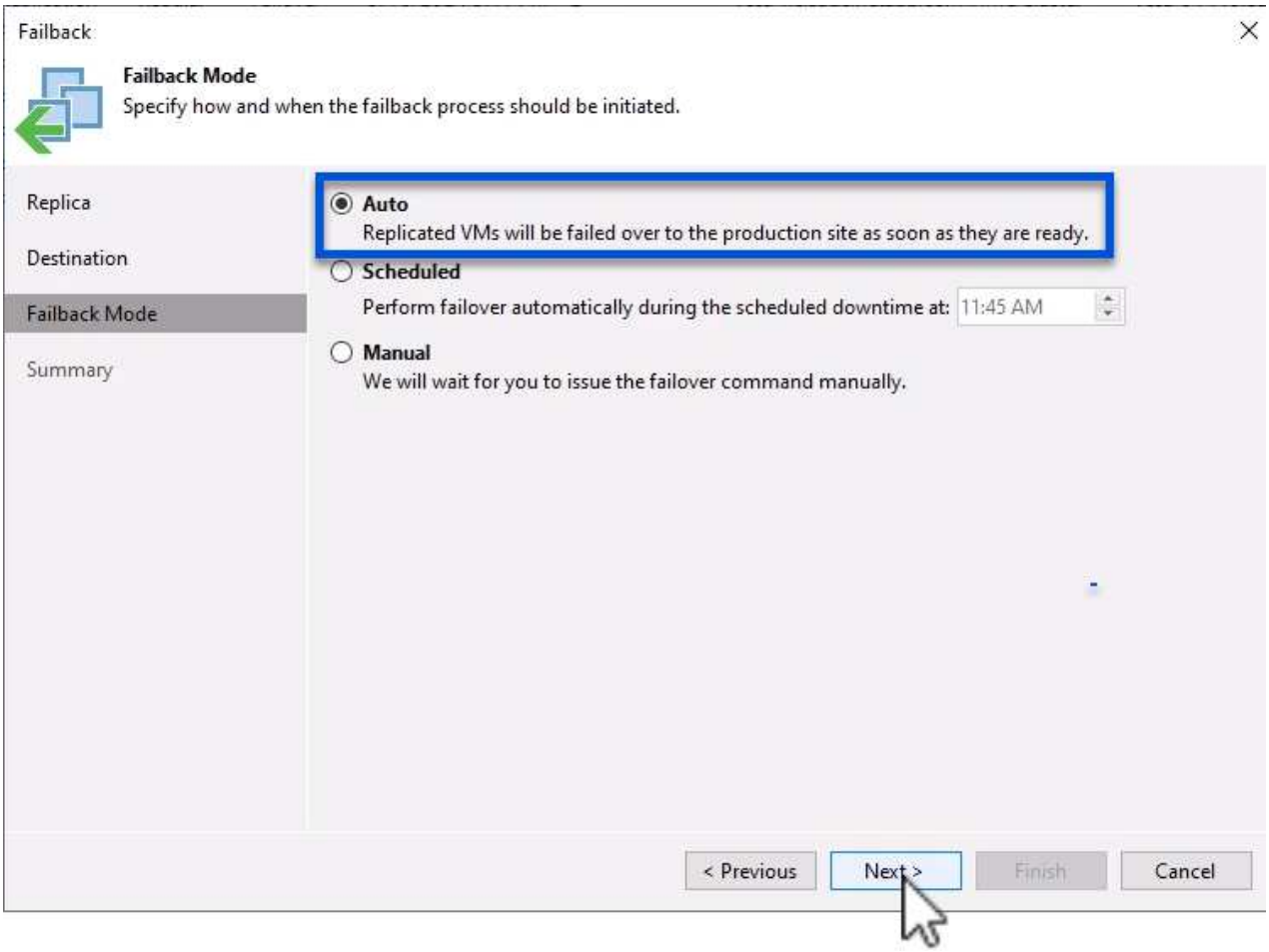
1. Dans la vue **Accueil**, cliquez sur **répliques > Active** dans le menu de gauche. Sélectionnez les machines virtuelles à inclure et cliquez sur le bouton **revenir à la production** dans le menu supérieur.



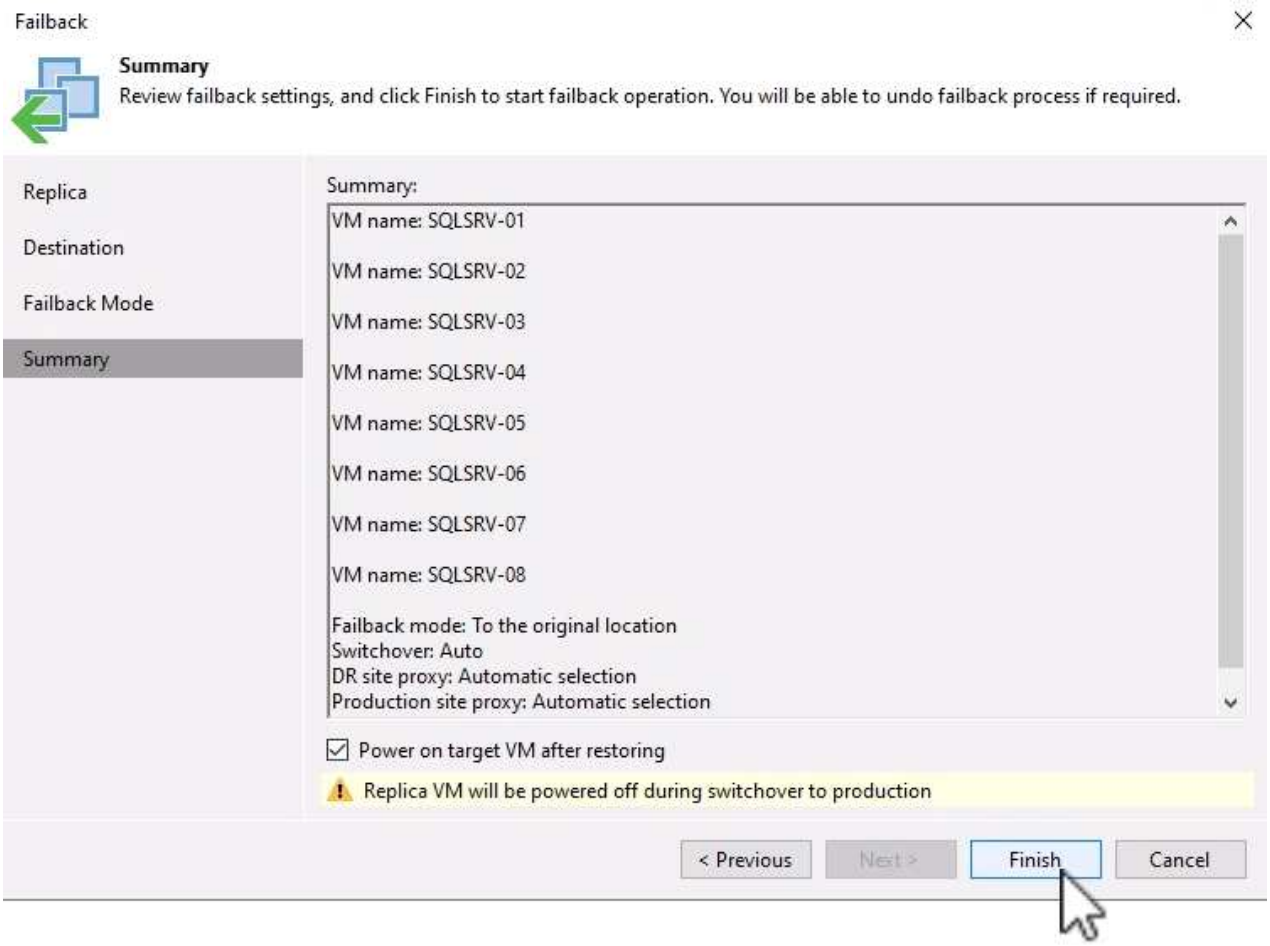
2. Sur la page **Replica** de l'assistant **Failback**, sélectionnez les répliques à inclure dans le travail de restauration automatique.
3. Sur la page **destination**, sélectionnez **Retour arrière à la VM** d'origine et cliquez sur **Suivant** pour continuer.



4. Sur la page **Failback mode**, sélectionnez **Auto** pour lancer le retour arrière le plus rapidement possible.

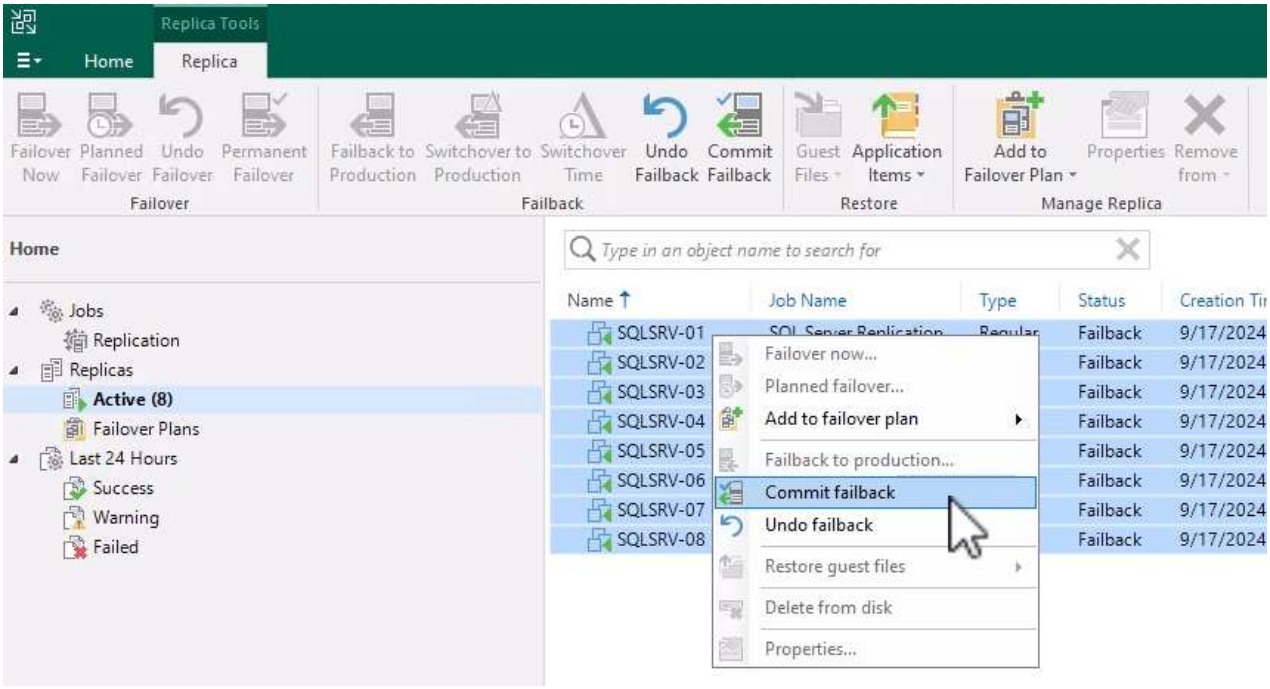


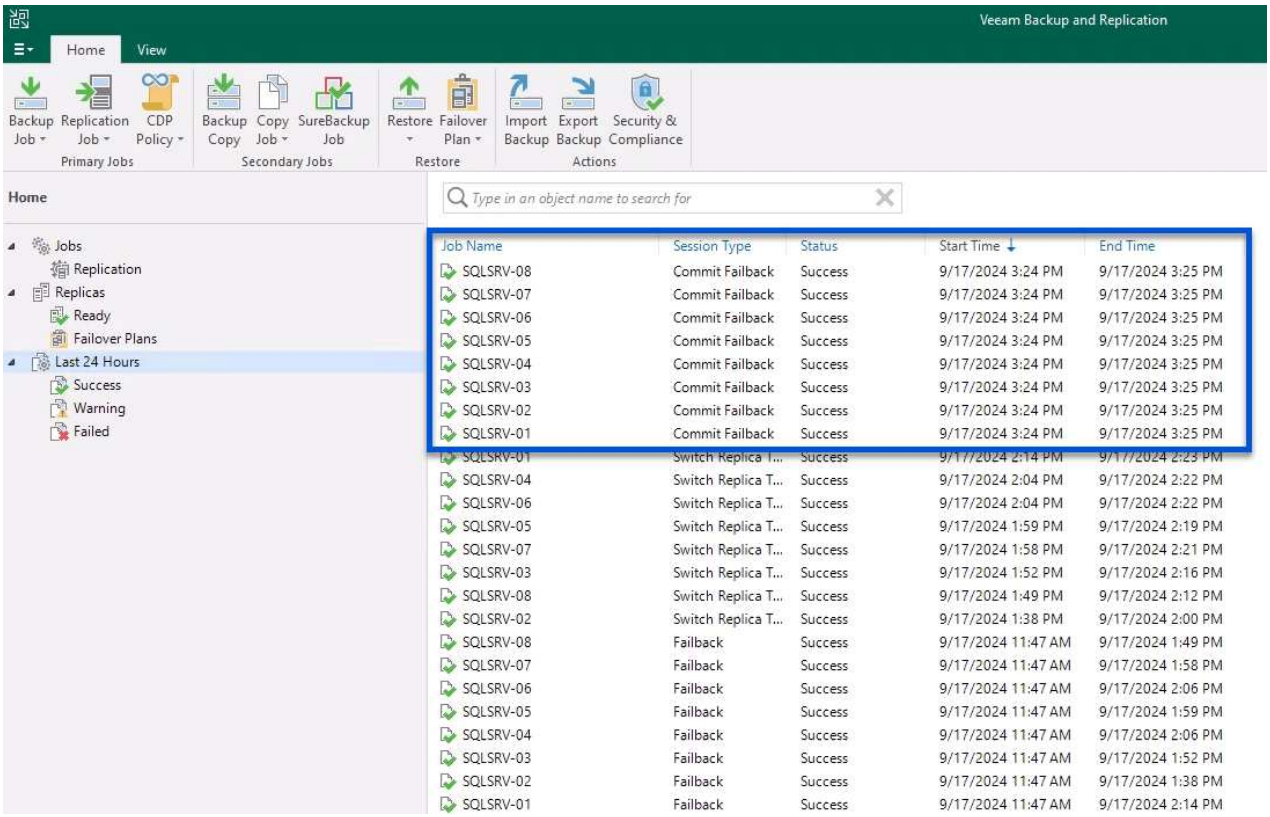
5. Sur la page **Résumé**, choisissez si **mettre sous tension la machine virtuelle cible après la restauration**, puis cliquez sur Terminer pour démarrer le travail de restauration.



La validation du retour arrière finalise l'opération de restauration, confirmant ainsi l'intégration réussie des modifications dans la machine virtuelle de production. Lorsqu'elle est validée, Veeam Backup & Replication reprend les activités de réplication régulières pour la machine virtuelle de production restaurée. L'état de la réplique restaurée passe de *Failback* à *Ready*.

1. Pour valider le retour arrière, accédez à **replicas > Active**, sélectionnez les VM à valider, cliquez avec le bouton droit de la souris et sélectionnez **commit retour arrière**.





une fois le retour en production réussi, les machines virtuelles sont toutes restaurées sur le site de production d'origine.

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

Conclusion

Grâce à la fonctionnalité de datastore de Google Cloud NetApp volumes, Veeam et d'autres outils tiers validés sont en mesure de proposer des solutions économiques de reprise d'activité. En utilisant des clusters Pilot light au lieu de grands clusters dédiés pour les réplicas de machines virtuelles, les entreprises peuvent réduire considérablement leurs dépenses. Cette approche permet de mettre en place des stratégies de reprise après incident sur mesure qui exploitent les solutions de sauvegarde internes existantes pour la reprise après incident basée sur le cloud, sans recourir à d'autres data centers sur site. En cas d'incident, le basculement peut être initié en un seul clic ou configuré pour s'exécuter automatiquement, garantissant ainsi la continuité de l'activité 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

Migration de workloads sur GCP/GCVE

Migrez vos workloads vers un datastore NetApp Cloud Volume Service sur Google Cloud VMware Engine avec VMware HCX - Guide de démarrage rapide

L'une des utilisations les plus courantes pour le magasin de données Google Cloud VMware Engine et Cloud Volume Service est la migration des charges de travail VMware. VMware HCX est une option privilégiée qui propose plusieurs mécanismes de migration pour transférer des machines virtuelles sur site et leurs données vers des datastores NFS Cloud Volume Service.

Auteur(s) : Ingénierie de solutions NetApp

Présentation : migration de machines virtuelles avec VMware HCX, datastores NetApp Cloud Volume Service et Google Cloud VMware Engine (GCVE)

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

Ce document fournit des instructions détaillées pour le provisionnement du datastore Cloud Volume Service, suivi du téléchargement, du déploiement et de la configuration de VMware HCX, y compris tous ses composants principaux sur site et Google Cloud VMware Engine, y compris l'interconnexion, l'extension réseau et l'optimisation WAN pour activer divers mécanismes de migration de machines virtuelles.

> VMware HCX fonctionne avec n'importe quel type de datastore lorsque la migration se trouve au niveau des VM. Ce document s'applique donc aux clients NetApp et aux clients non NetApp qui prévoient de déployer Cloud Volume Service avec Google Cloud VMware Engine pour un déploiement cloud VMware économique.

Étapes générales

Cette liste fournit les étapes générales nécessaires pour coupler et migrer les machines virtuelles vers HCX Cloud Manager sur le côté Google Cloud VMware Engine depuis HCX Connector sur site :

1. Préparez HCX à partir du portail Google VMware Engine.
2. Téléchargez et déployez le programme d'installation HCX Connector Open Virtualization Appliance (OVA) dans VMware vCenter Server sur site.
3. Activez HCX à l'aide de la clé de licence.
4. Couplez le connecteur VMware HCX sur site avec Google Cloud VMware Engine HCX Cloud Manager.
5. Configurez le profil réseau, le profil de calcul et le maillage de service.
6. (Facultatif) effectuez l'extension réseau pour éviter toute nouvelle IP pendant les migrations.
7. Validez l'état du système et assurez-vous que la migration est possible.
8. Migrer les workloads de VM.

Prérequis

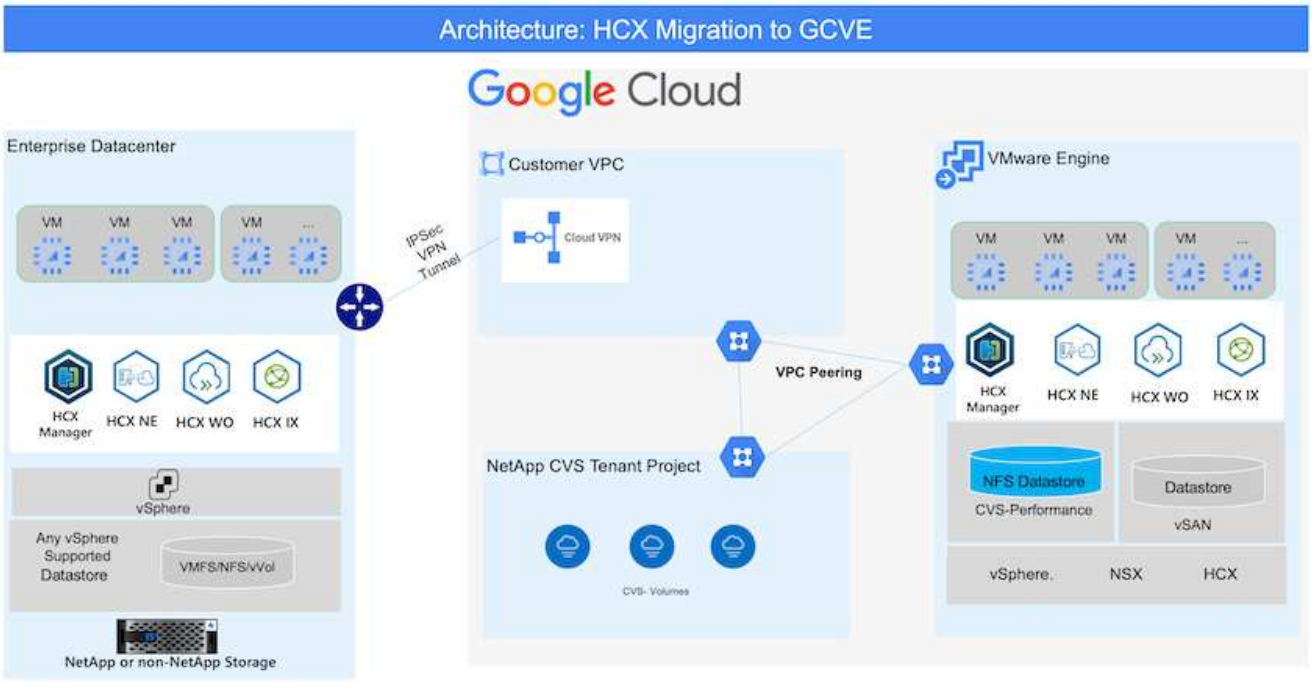
Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies. Pour plus d'informations, reportez-vous à ce document "lien". Une fois les prérequis, y compris la connectivité, téléchargez la clé de licence HCX sur le portail Google Cloud VMware Engine. Une fois le programme d'installation OVA téléchargé, procédez au processus d'installation comme décrit ci-dessous.

> HCX Advanced est l'option par défaut et VMware HCX Enterprise Edition est également disponible via un ticket d'assistance et pris en charge sans frais supplémentaires. Reportez-vous à "ce lien"

- L'utilisation d'un Software-Defined Data Center (SDDC) Google Cloud VMware Engine ou la création d'un cloud privé à l'aide de ce protocole "Lien NetApp" ou ceci "Lien Google".
- La migration des VM et des données associées depuis le data Center sur site compatible VMware vSphere nécessite une connectivité réseau du data Center vers l'environnement SDDC. Avant de migrer des workloads, "Configurez une connexion au cloud VPN ou à l'interconnexion du cloud" entre l'environnement sur site et le cloud privé respectif.
- Le chemin du réseau depuis l'environnement VMware vCenter Server sur site vers le cloud privé Google Cloud VMware Engine doit prendre en charge la migration des machines virtuelles à l'aide de vMotion.
- Assurez-vous que le nécessaire "règles et ports de pare-feu" Sont autorisées pour le trafic vMotion entre vCenter Server sur site et SDDC vCenter.
- Le volume NFS Cloud Volume Service doit être monté en tant que datastore dans Google Cloud VMware Engine. Suivez les étapes décrites dans ce document "lien" Ajout de datastores Cloud Volume Service à des hôtes Google Cloud VMware Engines.

Architecture de haut niveau

À des fins de test, l'environnement de laboratoire sur site utilisé pour cette validation a été connecté par le biais d'un VPN cloud, qui autorise la connectivité sur site à Google Cloud VPC.



Pour plus d'informations sur le schéma HCX, reportez-vous à "Lien VMware"

Déploiement de la solution

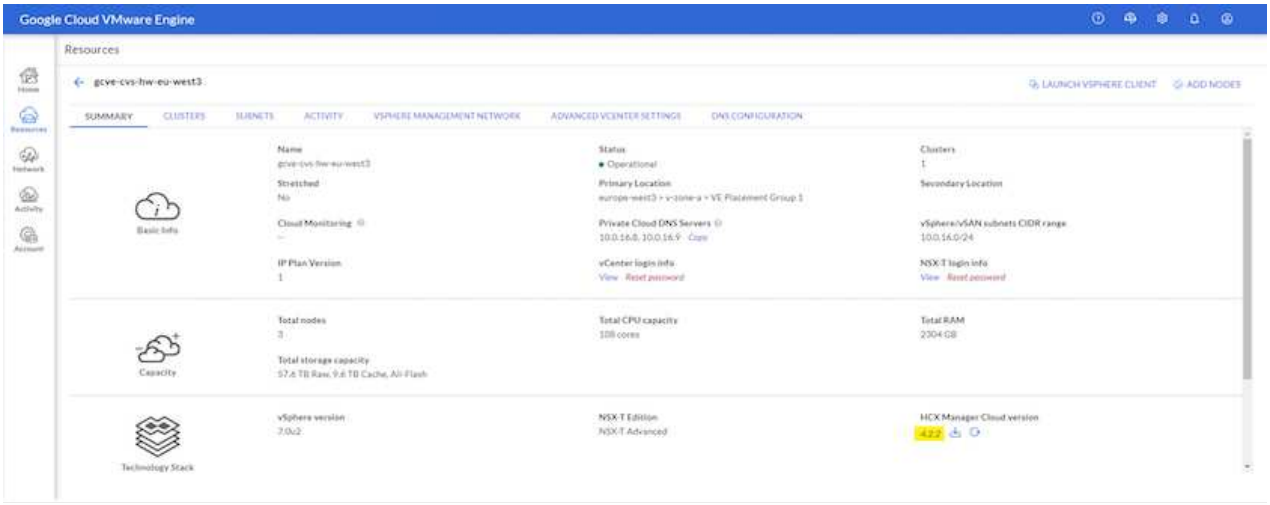
Suivez les étapes du déploiement de cette solution :

Étape 1 : préparer HCX via le portail Google VMware Engine

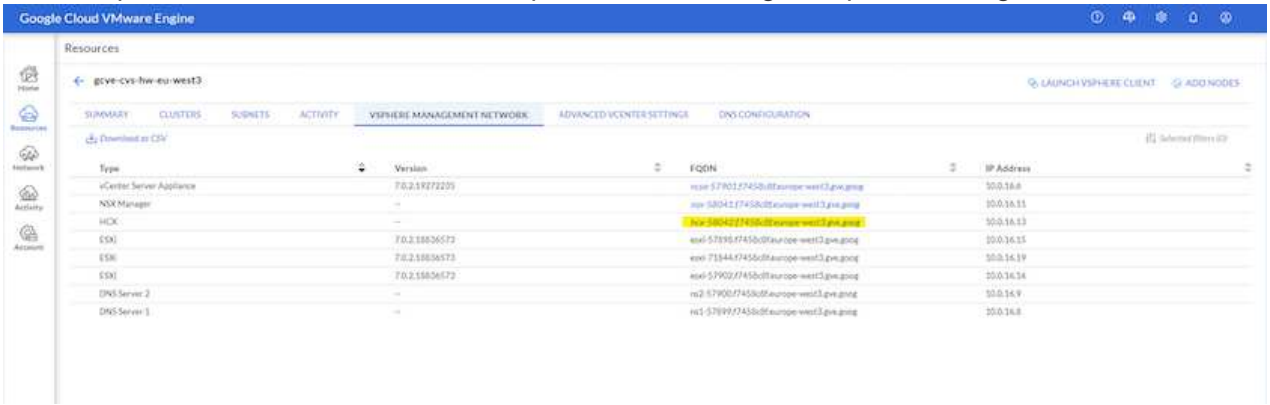
LE composant HCX Cloud Manager est automatiquement installé lorsque vous provisionnez le cloud privé avec VMware Engine. Pour préparer le couplage du site, procédez comme suit :

1. Connectez-vous au portail Google VMware Engine Portal et connectez-vous au HCX Cloud Manager.

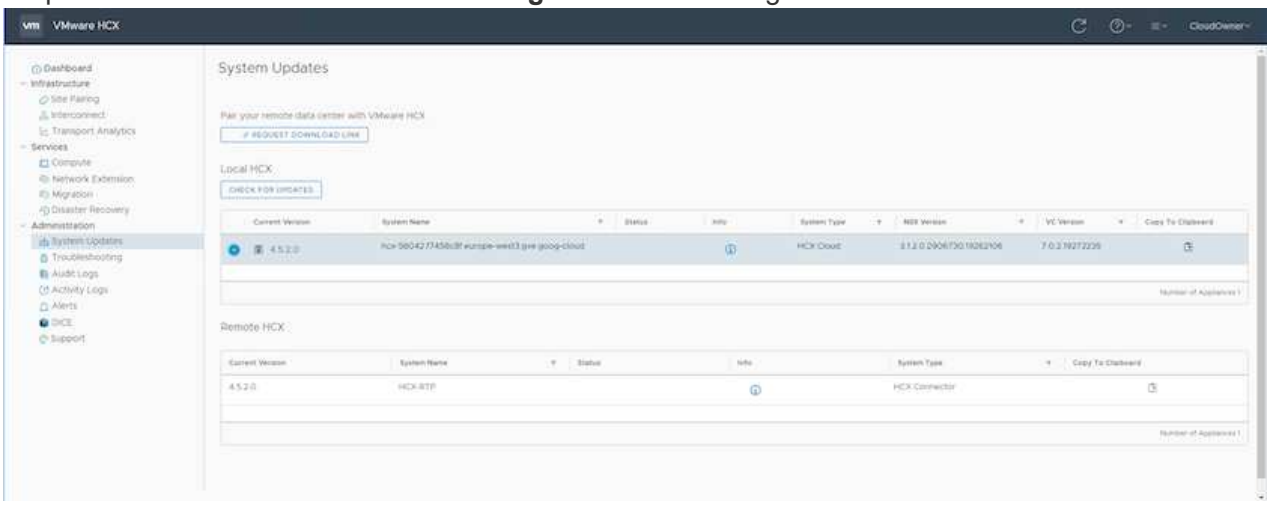
   Vous pouvez vous connecter à la console HCX en cliquant sur le lien de version HCX



   ou en cliquant sur le nom de domaine complet HCX sous l'onglet vSphere Management Network.



2. Dans HCX Cloud Manager, accédez à **Administration > mises à jour du système**.
3. Cliquez sur **demander le lien de téléchargement** et téléchargez le fichier OVA.



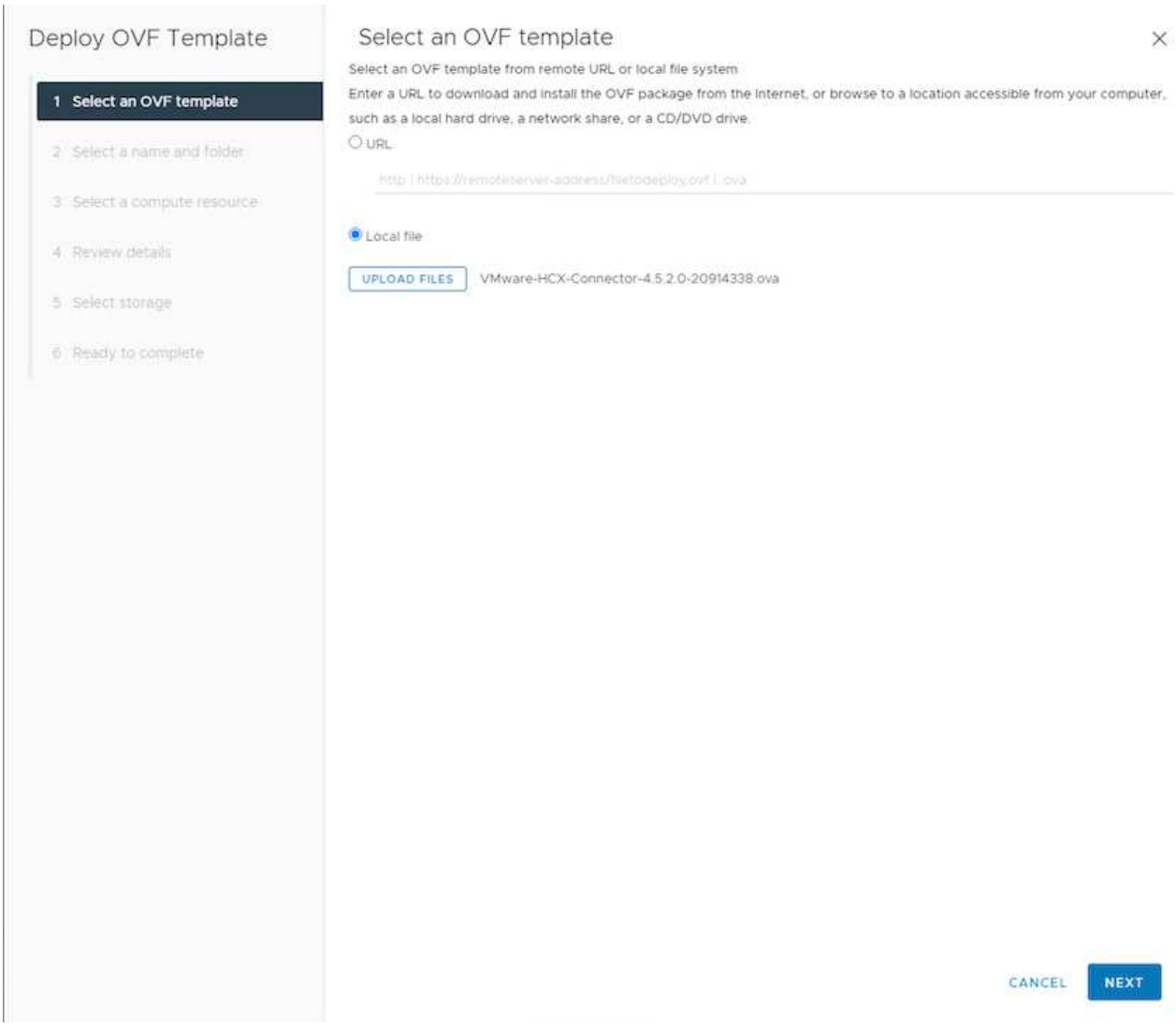
4. Mettez à jour HCX Cloud Manager vers la dernière version disponible depuis l'interface utilisateur HCX Cloud Manager.

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

Pour que le connecteur sur site puisse se connecter au HCX Manager dans Google Cloud VMware Engine, assurez-vous que les ports pare-feu appropriés sont ouverts dans l'environnement sur site.

Pour télécharger et installer HCX Connector dans le serveur vCenter sur site, procédez comme suit :

1. Téléchargez les ova depuis la console HCX sur Google Cloud VMware Engine, comme indiqué à l'étape précédente.
2. Une fois le fichier OVA téléchargé, déployez-le dans l'environnement VMware vSphere sur site à l'aide de l'option **Deploy OVF Template**.



3. Entrez toutes les informations requises pour le déploiement OVA, cliquez sur **Next**, puis sur **Finish** pour déployer le connecteur OVA VMware HCX.

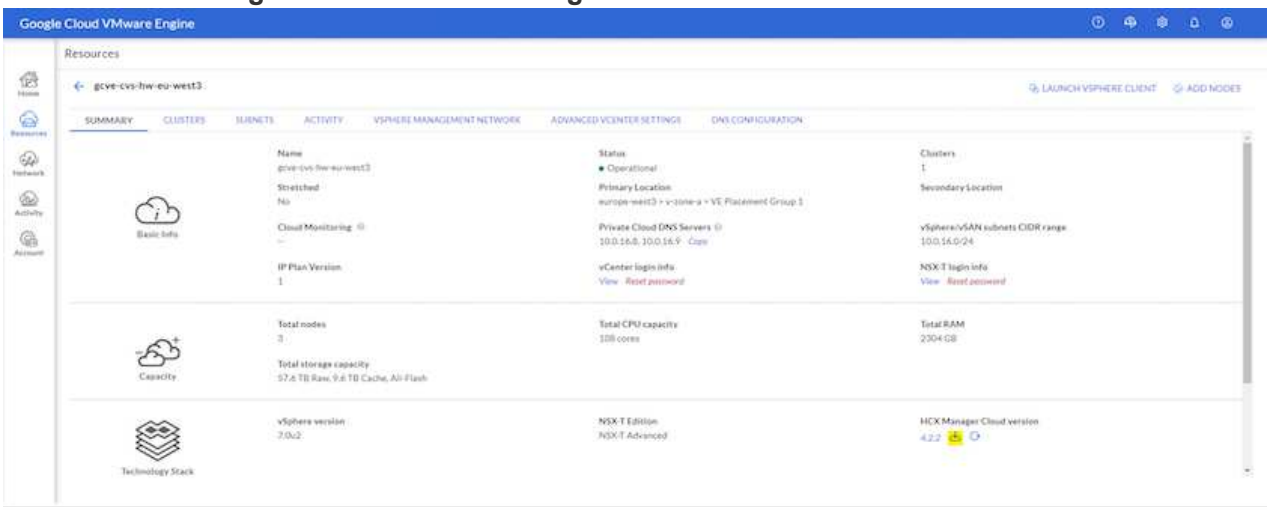
> Mettez l'appliance virtuelle sous tension manuellement.

Pour des instructions détaillées, reportez-vous à la "Guide de l'utilisateur VMware HCX".

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

Après avoir déployé le connecteur OVA VMware HCX sur site et démarré l'appliance, procédez comme suit pour activer le connecteur HCX. Générez la clé de licence à partir du portail Google Cloud VMware Engine et activez-la dans VMware HCX Manager.

1. Sur le portail VMware Engine, cliquez sur Ressources, sélectionnez le cloud privé et **cliquez sur l'icône de téléchargement sous HCX Manager Cloud version**.



   Ouvrez le fichier téléchargé et copiez la chaîne de clé de licence.

2. Connectez-vous au gestionnaire VMware HCX sur site à l'adresse `"https://hcxmanagerIP:9443"` utilisation des informations d'identification administrateur.

   > Utilisez l'hcxmangerIP et le mot de passe définis lors du déploiement du système OVA.

3. Dans la licence, entrez la clé copiée à partir de l'étape 3 et cliquez sur **Activer**.

   > Le connecteur HCX sur site doit disposer d'un accès Internet.

4. Sous **Datacenter Location**, indiquez l'emplacement le plus proche pour l'installation sur site de VMware HCX Manager. Cliquez sur **Continuer**.
5. Sous **Nom du système**, mettez à jour le nom et cliquez sur **Continuer**.
6. Cliquez sur **Oui, Continuer**.
7. Sous **Connect Your vCenter**, indiquez le nom de domaine complet (FQDN) ou l'adresse IP de vCenter Server et les informations d'identification appropriées, puis cliquez sur **Continuer**.

   > Utilisez le FQDN pour éviter les problèmes de connectivité ultérieurement.

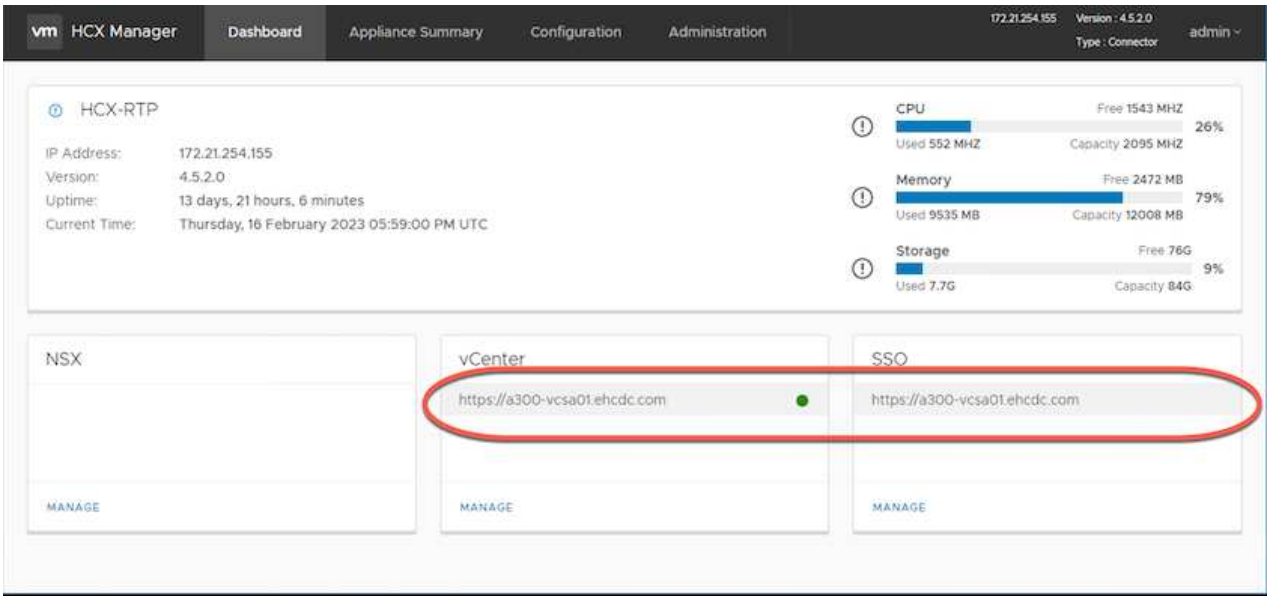
8. Sous **configurer SSO/PSC**, indiquez le FQDN ou l'adresse IP du contrôleur des services de plate-forme (PSC) et cliquez sur **Continuer**.

   > Pour Embedded PSC, entrez le nom de domaine complet ou l'adresse IP du serveur VMware vCenter.

9. Vérifiez que les informations saisies sont correctes et cliquez sur **redémarrer**.
10. Après le redémarrage des services, vCenter Server s'affiche en vert sur la page qui s'affiche. VCenter

Server et SSO doivent avoir les paramètres de configuration appropriés, qui doivent être identiques à la page précédente.

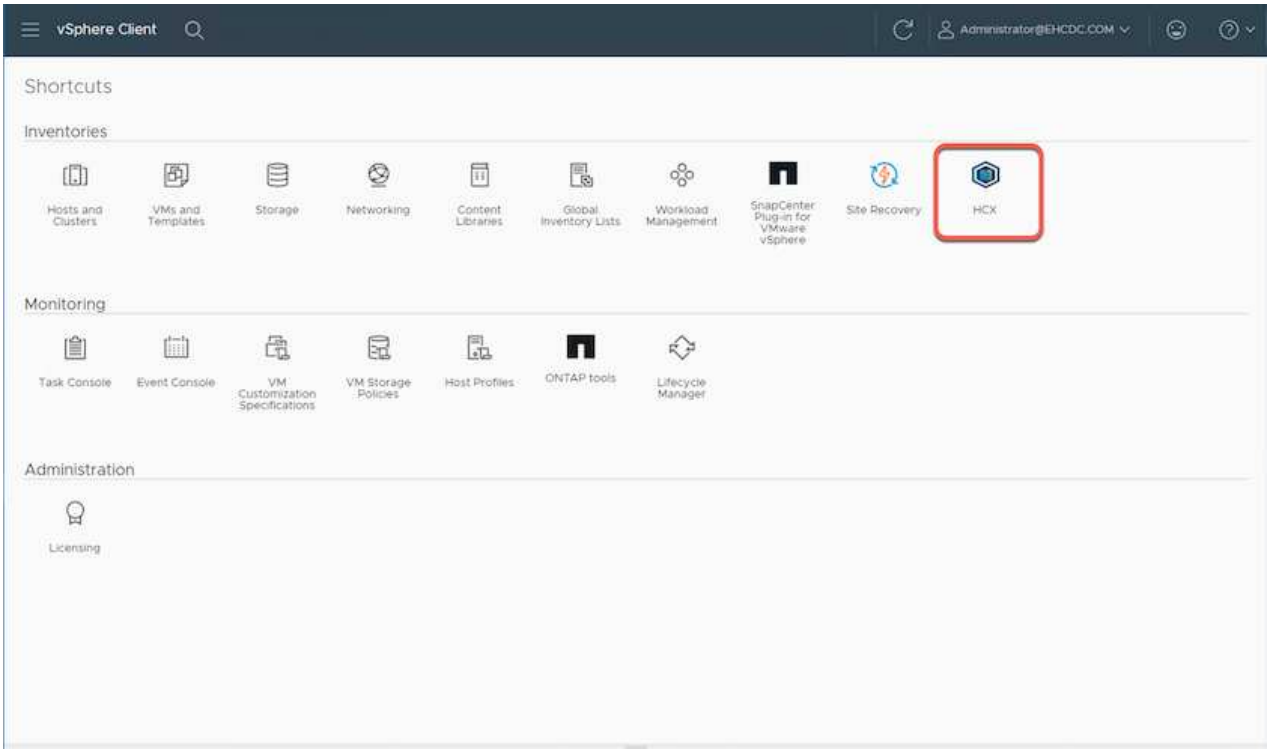
Ce processus dure environ 10 à 20 minutes et le plug-in doit être ajouté à vCenter Server.



Étape 4 : connecteur VMware HCX sur site avec Google Cloud VMware Engine HCX Cloud Manager

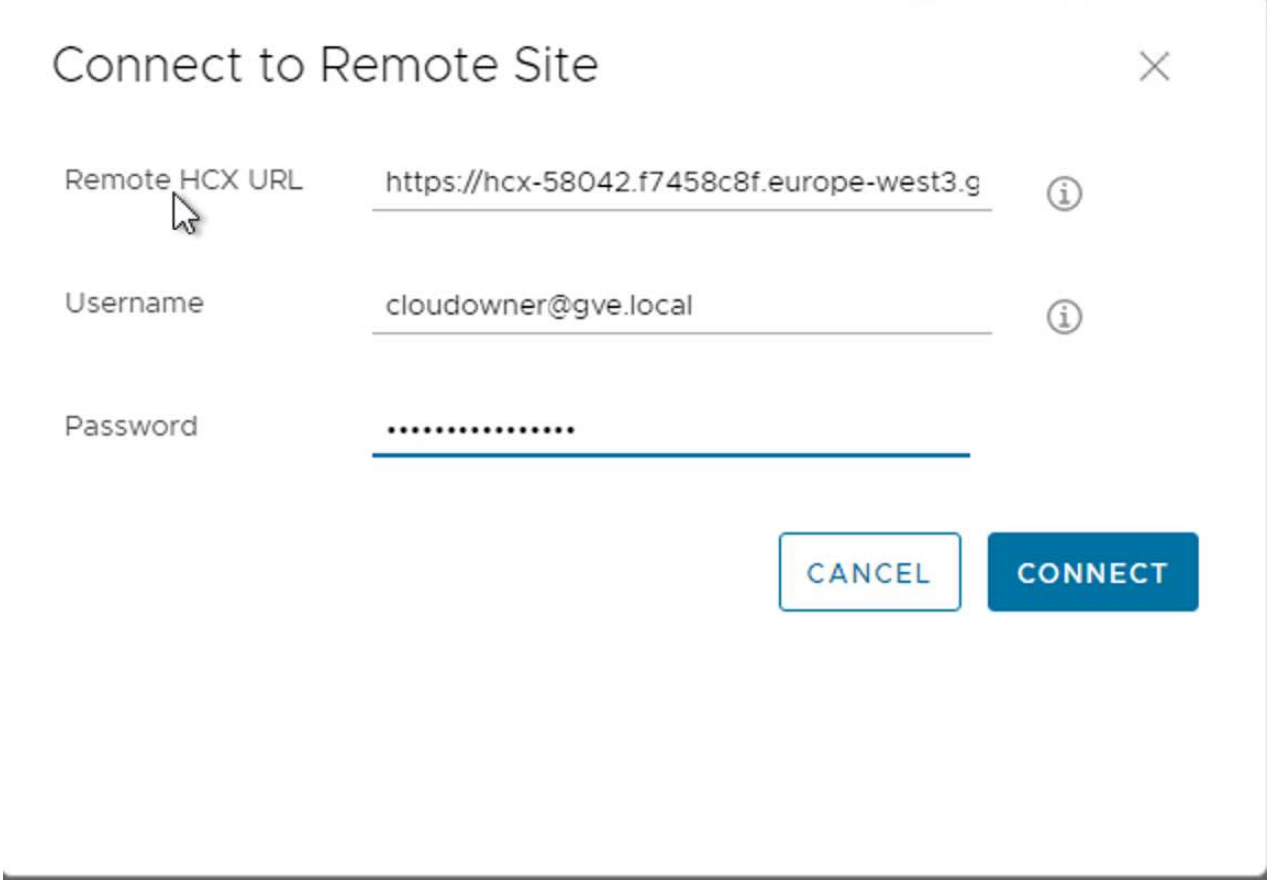
Une fois que HCX Connector est déployé et configuré sur site vCenter, établissez une connexion à Cloud Manager en ajoutant le couplage. Pour configurer le couplage du site, procédez comme suit :

1. Pour créer une paire de sites entre l'environnement vCenter sur site et Google Cloud VMware Engine SDDC, connectez-vous au serveur vCenter sur site et accédez au nouveau plug-in client Web HCX vSphere.



2. Sous Infrastructure, cliquez sur **Ajouter un couplage de site**.

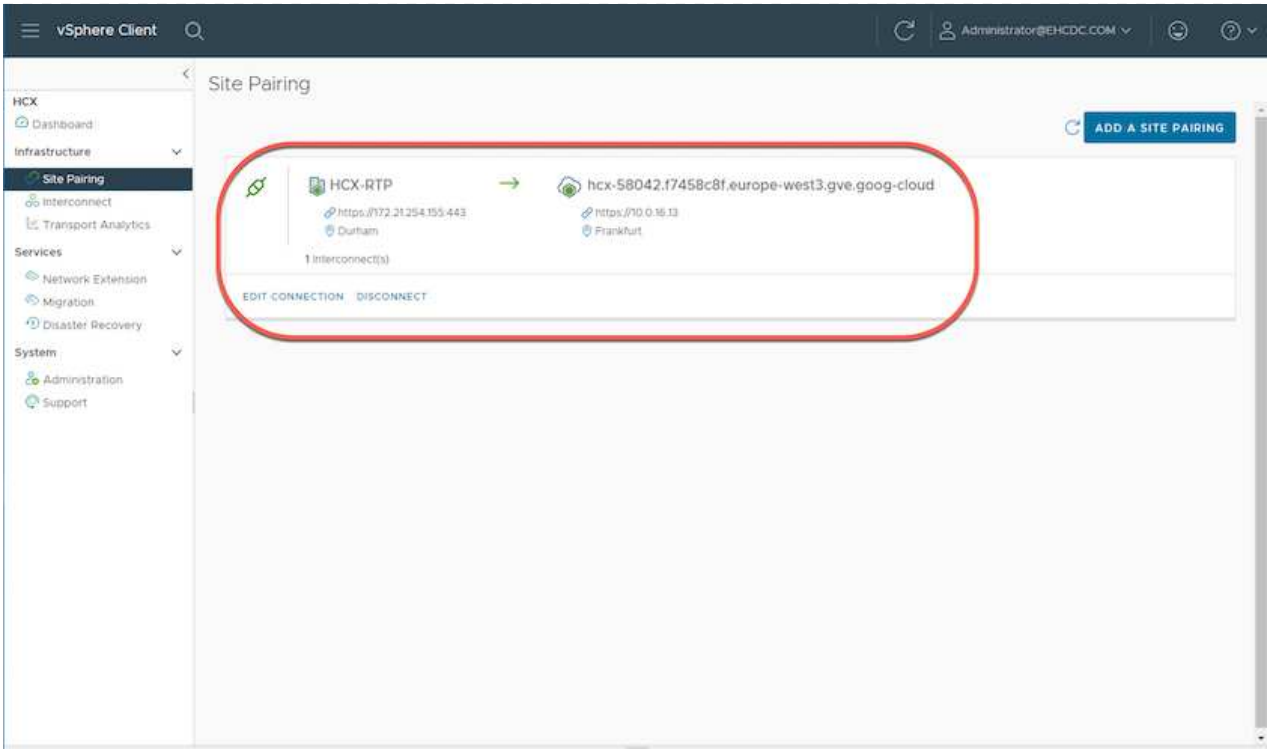
Entrez l'URL ou l'adresse IP Google Cloud VMware Engine HCX Cloud Manager et les identifiants de l'utilisateur disposant des privilèges de rôle propriétaire cloud pour accéder au cloud privé.



3. Cliquez sur **connexion**.

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

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

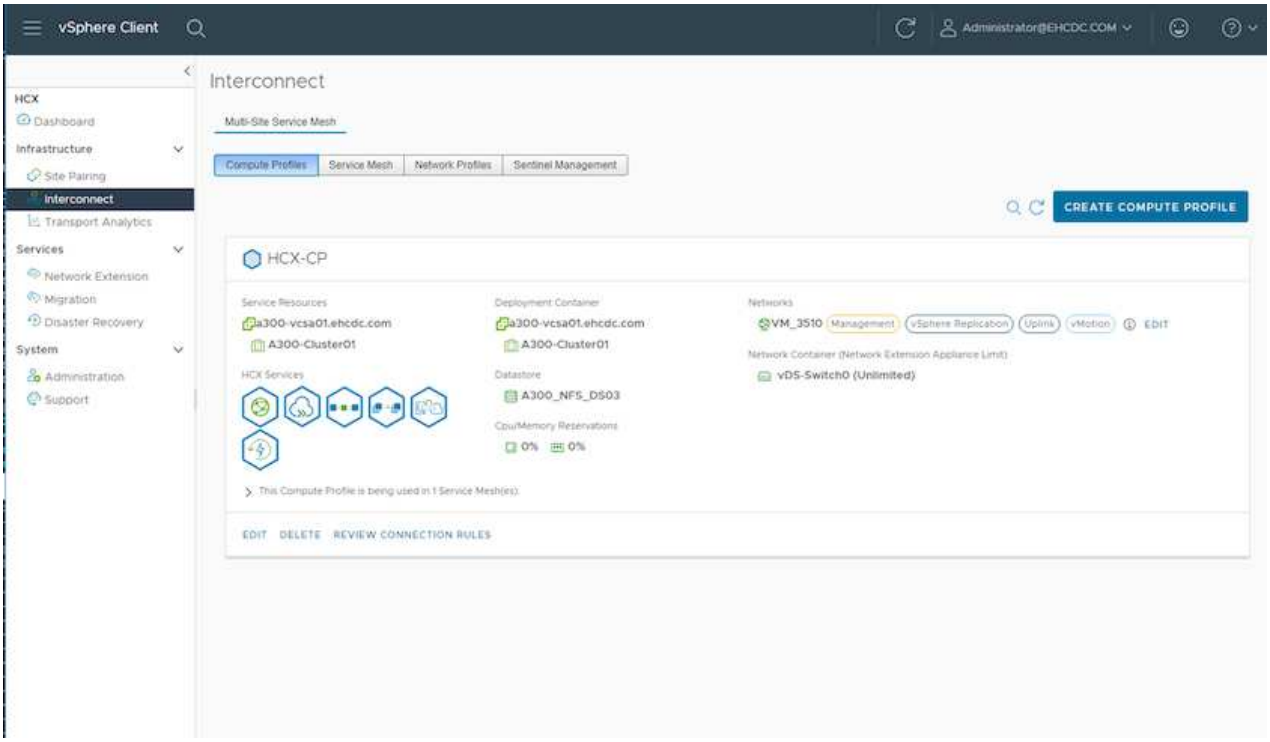

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

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

Le dispositif d'interconnexion VMware HCX offre des fonctionnalités de réplication et de migration basée sur vMotion via Internet et des connexions privées vers le site cible. L'interconnexion offre le cryptage, l'ingénierie du trafic et la mobilité des machines virtuelles. Pour créer une appliance de service d'interconnexion, procédez comme suit :

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

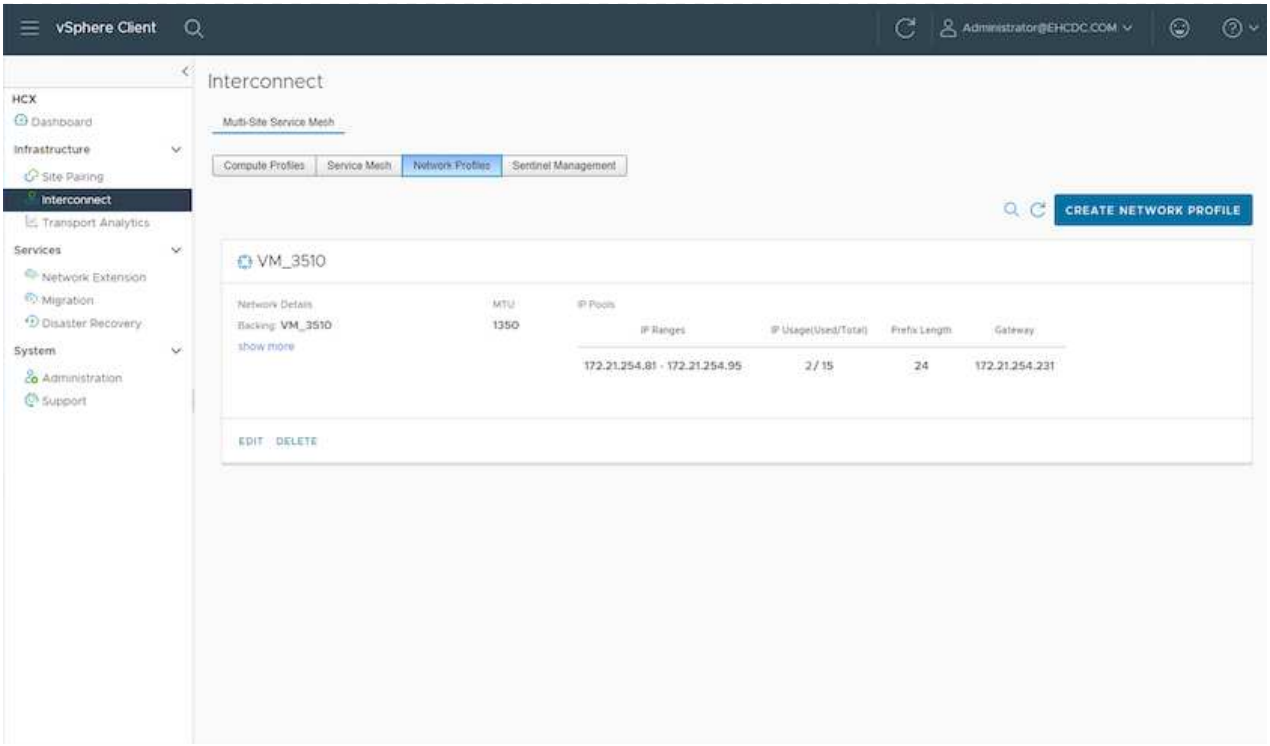
   Les profils de calcul définissent les paramètres de déploiement, y compris les appliances déployées et la partie du data Center VMware accessible au service HCX.



2. Une fois le profil de calcul créé, créez les profils réseau en sélectionnant **maillage de service multisite > profils réseau > Créer profil réseau**.

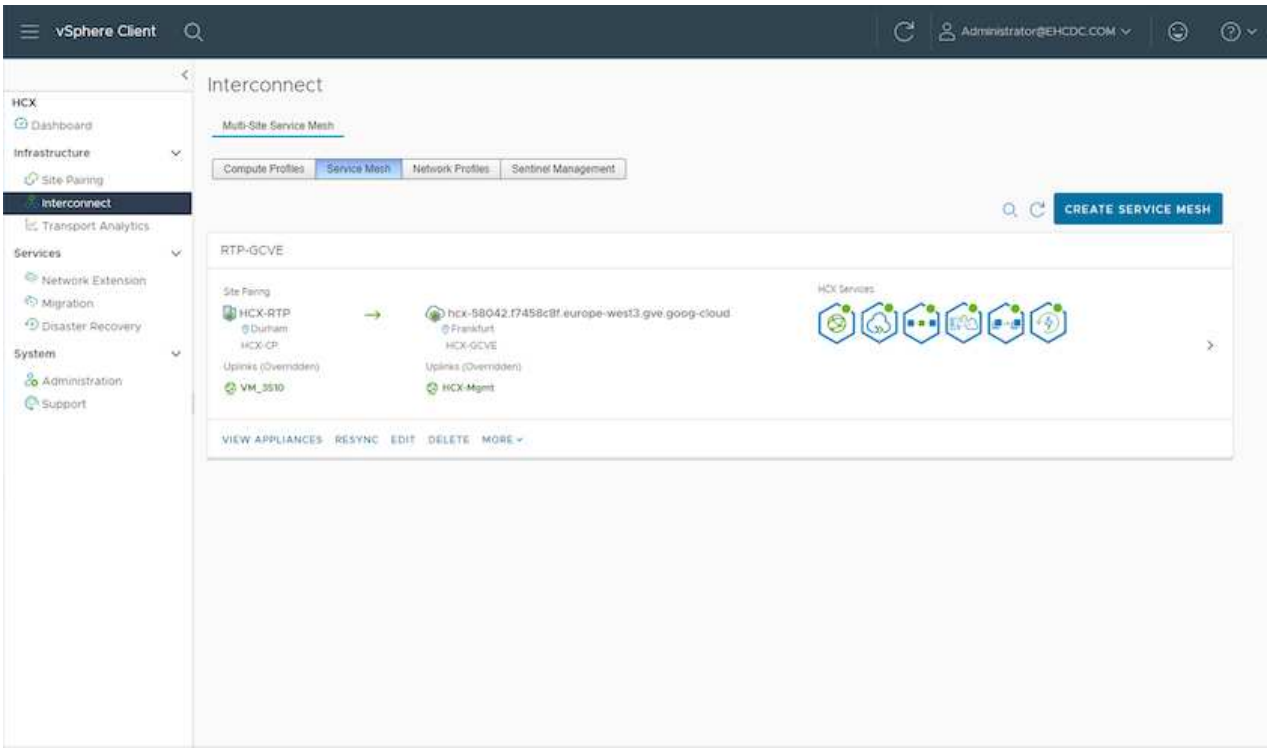
   Le profil réseau définit une plage d'adresses IP et de réseaux utilisés par HCX pour ses appliances virtuelles.

   Cette étape nécessite au moins deux adresses IP. Ces adresses IP sont attribuées depuis le réseau de gestion aux dispositifs d'interconnexion.

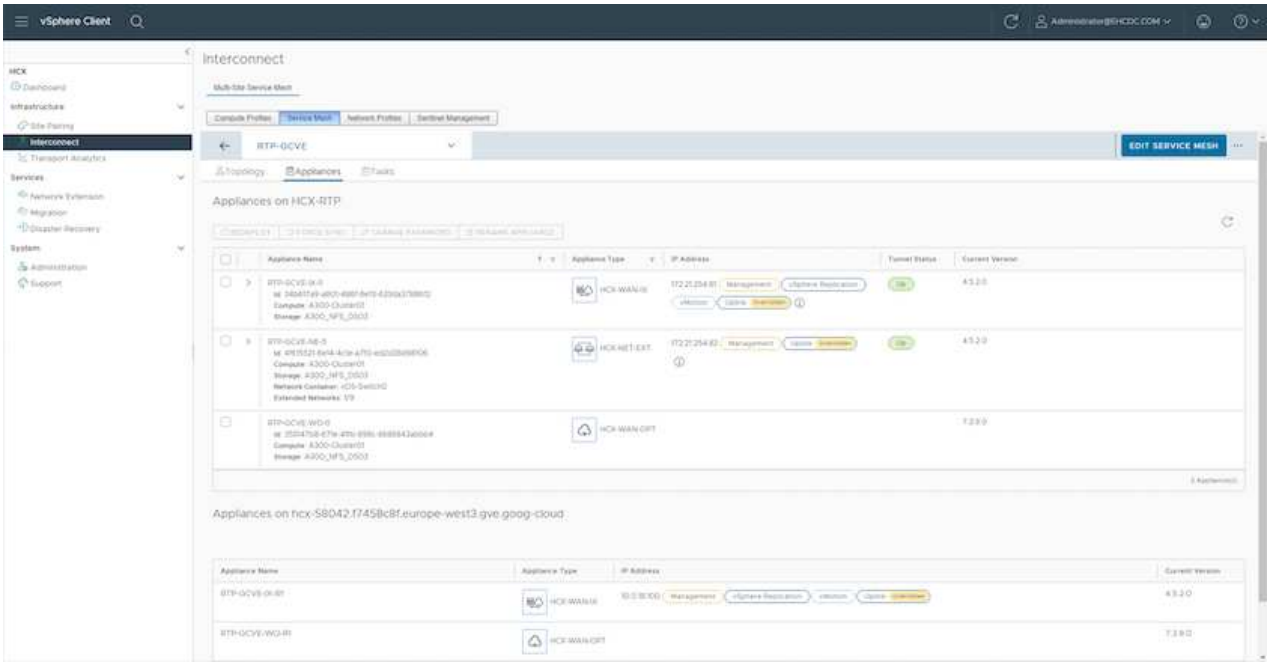


3. A ce stade, les profils de calcul et de réseau ont été créés avec succès.
4. Créez le maillage de service en sélectionnant l'onglet **maillage de service** dans l'option **Interconnexion** et sélectionnez les sites SDDC sur site et GCVE.
5. Le maillage de service spécifie une paire de profils réseau et de calcul locale et distante.

Dans le cadre de ce processus, les appliances HCX sont déployées et configurées automatiquement sur les sites source et cible afin de créer une structure de transport sécurisée.



6. Il s’agit de la dernière étape de la configuration. Le déploiement devrait s’effectuer en 30 minutes environ. Une fois le maillage de service configuré, l’environnement est prêt avec les tunnels IPsec créés pour migrer les VM de charge de travail.



Étape 6 : migrer les workloads

Les charges de travail peuvent être migrées de façon bidirectionnelle entre les SDDC sur site et GCVE à l'aide de diverses technologies de migration HCX de VMware. Les machines virtuelles peuvent être déplacées vers et depuis des entités activées par VMware HCX à l'aide de plusieurs technologies de migration telles que la migration en bloc HCX, HCX vMotion, la migration à froid HCX, l'option vMotion par réplication assistée par HCX (disponible avec l'édition Enterprise de HCX) et la migration assistée par système d'exploitation HCX (disponible avec l'édition Enterprise de HCX).

Pour en savoir plus sur les différents mécanismes de migration HCX, voir "Types de migration VMware HCX".

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

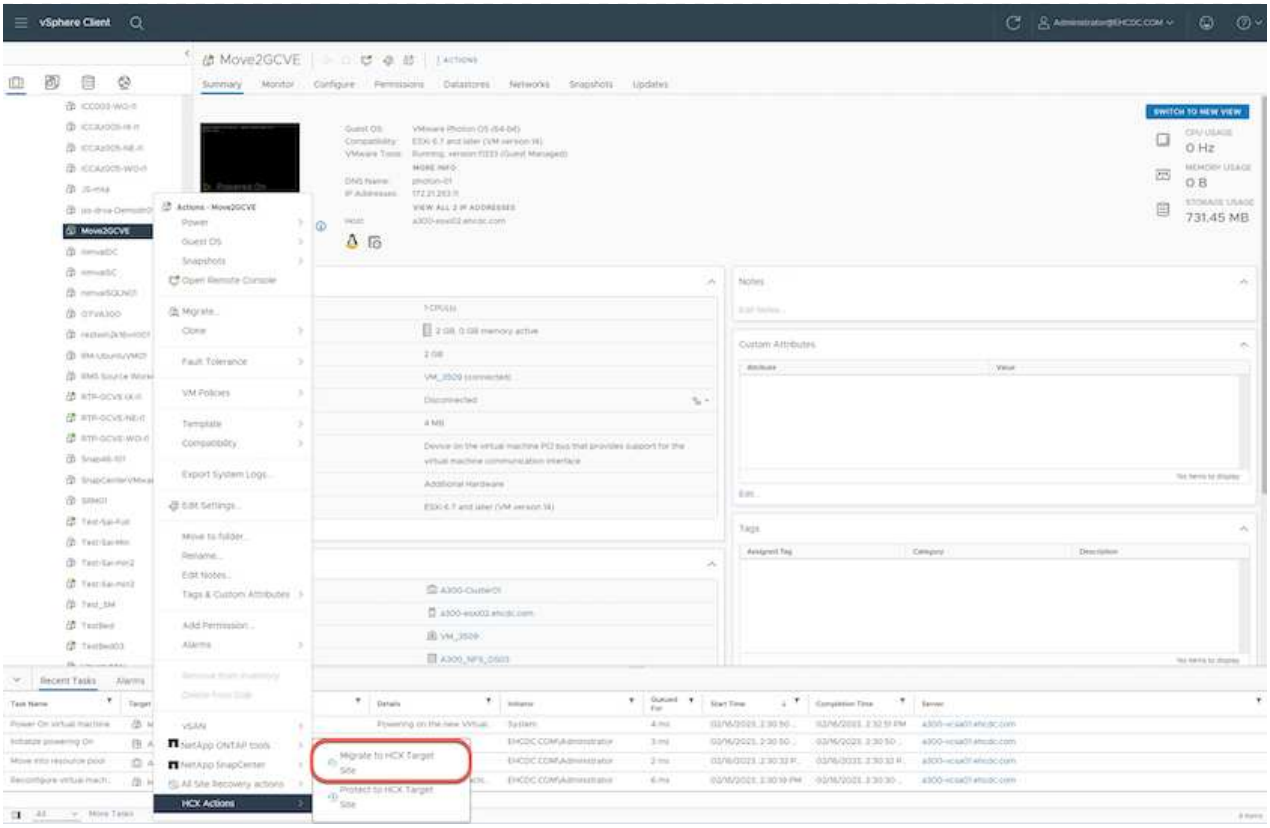
> ⓘ L'appliance HCX-IX ajoute le service Mobility Agent en tant qu'objet hôte dans vCenter Server. Les ressources processeur, mémoire, stockage et réseau affichées sur cet objet ne représentent pas la consommation réelle sur l'hyperviseur physique hébergeant l'appliance IX.

HCX vMotion

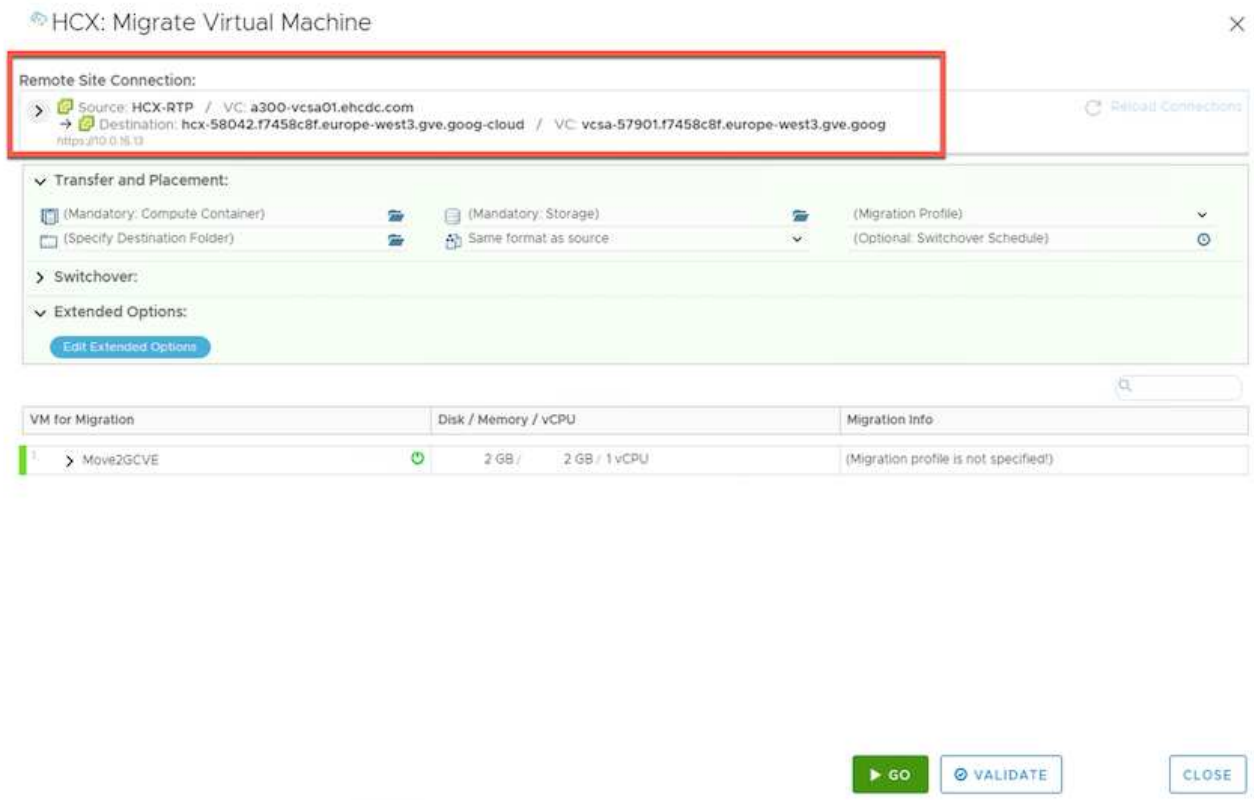
Cette section décrit le mécanisme HCX vMotion. Cette technologie de migration utilise le protocole VMware vMotion pour migrer un VM vers GCVE. L'option de migration vMotion permet de migrer l'état d'une machine virtuelle unique à la fois. Il n'y a pas d'interruption de service pendant cette méthode de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

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

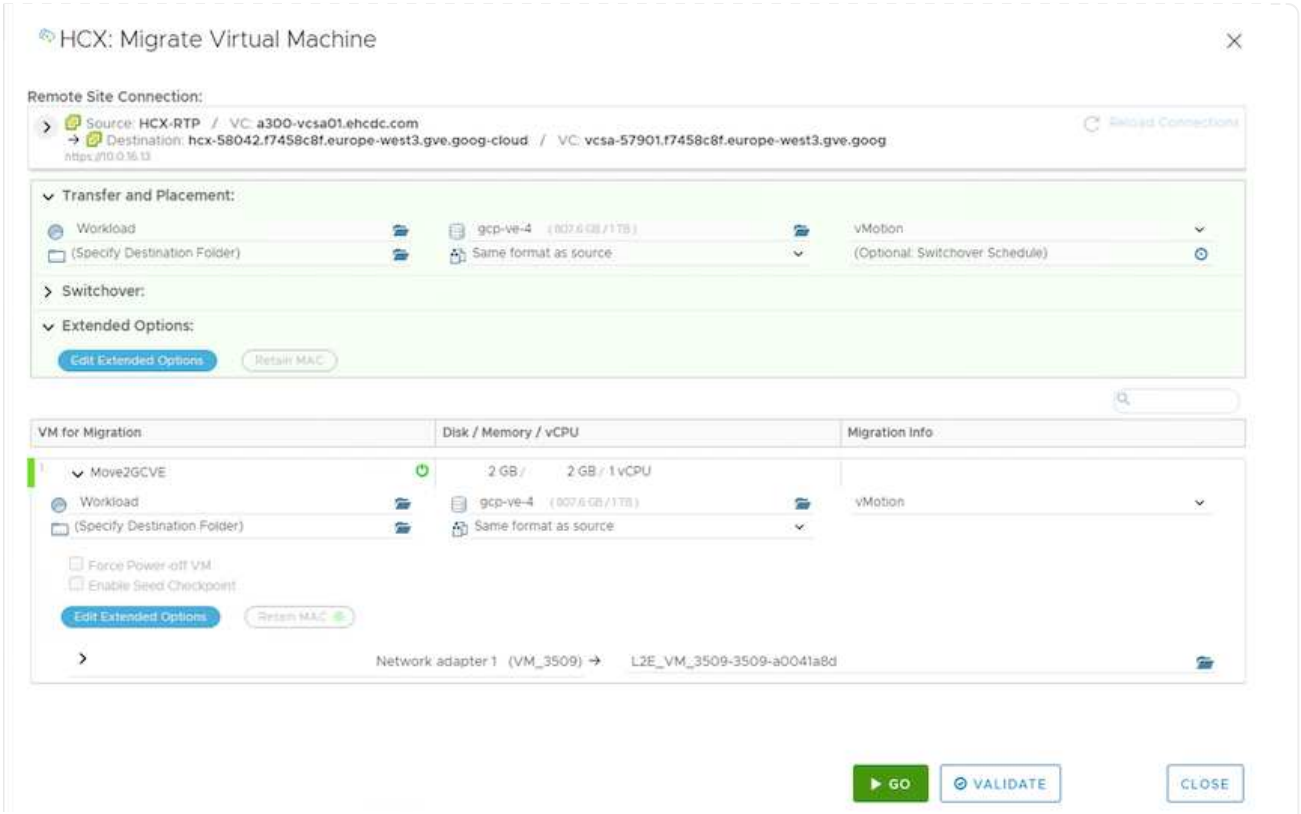
1. Depuis le client vSphere sur site, accédez à Inventory, faites un clic droit sur la machine virtuelle à migrer, puis sélectionnez HCX actions > Migrate to HCX site cible.



2. Dans l’assistant de migration d’ordinateur virtuel, sélectionnez connexion de site distant (GCVE cible).



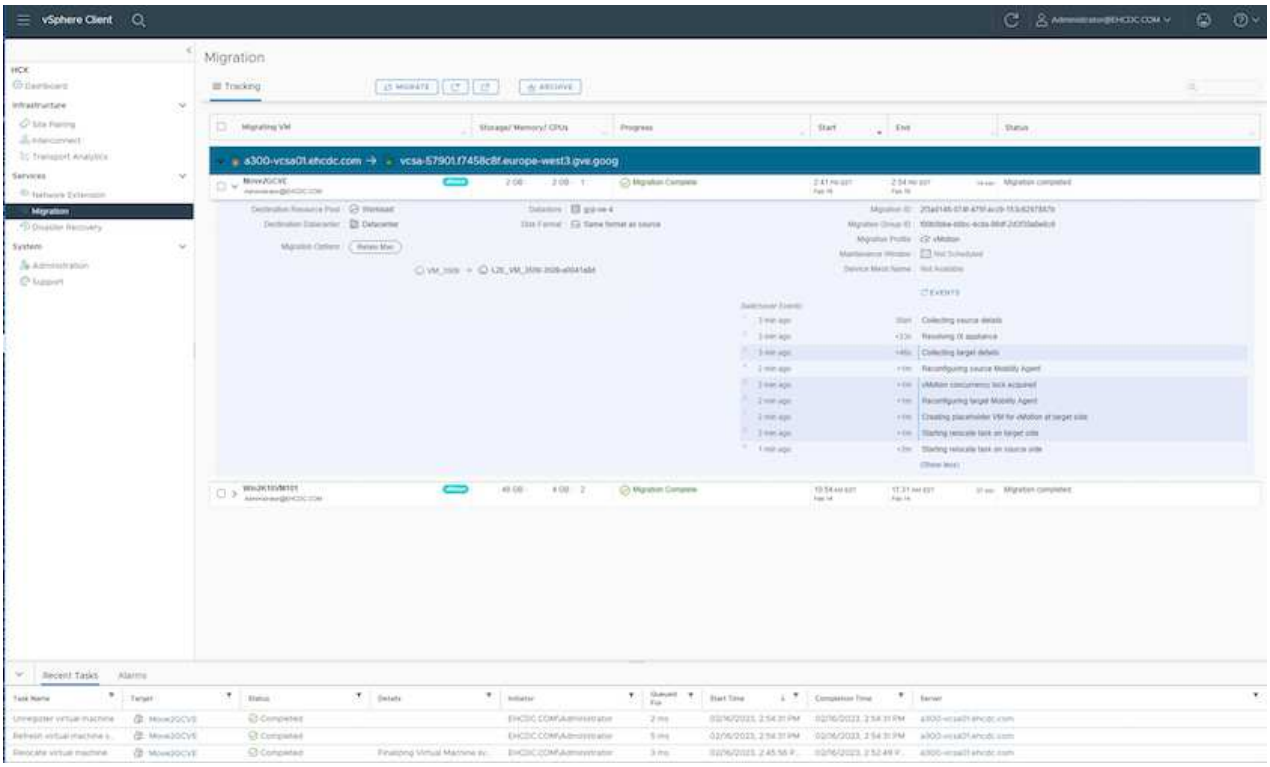
3. Mettez à jour les champs obligatoires (Cluster, Storage et destination Network), puis cliquez sur Validate.



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

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

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



L'espace requis pour le datastore NFS CVS cible doit être suffisant pour gérer la migration.

Conclusion

Que vous ciblez les clouds ou les clouds hybrides et les données qui résident sur un stockage sur site de tout type ou fournisseur, Cloud Volume Service et HCX offrent d'excellentes options pour déployer et migrer les charges de travail applicatives tout en réduisant le coût total de possession en rendant les besoins en données transparents vers la couche applicative. Quelles que soient les utilisations, choisissez Google Cloud VMware Engine et Cloud Volume Service pour bénéficier rapidement des avantages du cloud, d'une infrastructure cohérente et des opérations entre plusieurs clouds et sur site, de la portabilité bidirectionnelle des charges de travail, et de la capacité et des performances élevées. Il s'agit du même processus et procédures que celui utilisé pour connecter le stockage et migrer les machines virtuelles à l'aide de VMware vSphere Replication, VMware vMotion ou même de la copie de fichiers réseau (NFC).

Messages clés

Les points clés de ce document sont les suivants :

- Il est désormais possible d'utiliser Cloud Volume Service comme datastore sur Google Cloud VMware Engine SDDC.
- Vous pouvez facilement migrer les données depuis des installations sur site vers le datastore Cloud Volume Service.
- Vous pouvez facilement étendre et réduire le datastore Cloud Volume Service pour répondre aux exigences de capacité et de performances lors de l'activité de migration.

Vidéos de référence de Google et VMware

De Google

- "Déployer le connecteur HCX avec GCVE"
- "Configurez le maillage HCX avec GCVE"
- "Migrer VM avec HCX vers GCVE"

À l'aide de VMware

- "Déploiement DU connecteur HCX pour GCVE"
- "Configuration SERVICEMESH HCX pour GCVE"
- "Migration de la charge DE travail HCX vers GCVE"

Où trouver des informations complémentaires

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

- Documentation Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentation du service Cloud volumes

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- Guide de l'utilisateur VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

Migration de machines virtuelles vers un datastore NFS NetApp Cloud Volume Service sur Google Cloud VMware Engine utilisant la fonctionnalité de réplication de Veeam

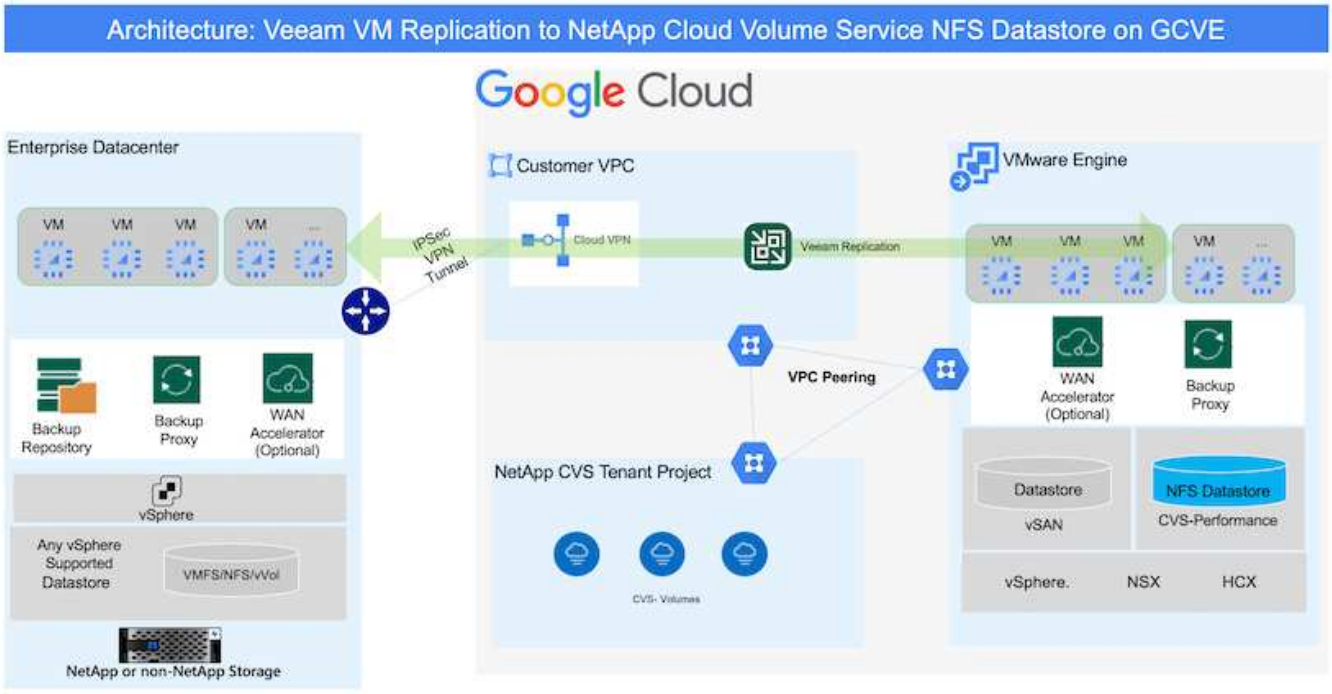
Les clients qui utilisent Veeam pour répondre à leurs exigences en matière de protection des données continuent à utiliser cette solution pour migrer les workloads vers GCVE et profitent des avantages des datastores NetApp Cloud volumes Service NFS.

Présentation

Auteurs : Suresh Thoppay, NetApp

Les charges de travail de machines virtuelles exécutées sur VMware vSphere peuvent être migrées vers Google Cloud VMware Engine (GCVE) à l'aide de la fonctionnalité de réplication Veeam.

Ce document présente une approche détaillée de la configuration et de la migration de serveurs virtuels qui utilise NetApp Cloud Volume Service, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Dans ce document, vous devez disposer d'un VPN Google Cloud, d'une interconnexion de cloud ou d'une autre option de mise en réseau pour établir une connectivité réseau entre les serveurs vSphere existants et Google Cloud VMware Engine.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document.
> Reportez-vous à la "Documentation Google Cloud" Pour la méthode de connectivité appropriée du stockage sur site vers Google.

Déploiement de la solution de migration

Présentation du déploiement de la solution

1. Assurez-vous que le datastore NFS du service NetApp Cloud Volume est monté sur GCVE vCenter.
2. Assurez-vous que Veeam Backup Recovery est déployé dans l'environnement VMware vSphere existant
3. Créez une tâche de réplication pour lancer la réplication des machines virtuelles vers une instance Google Cloud VMware Engine.
4. Effectuer le basculement de la tâche de réplication Veeam.
5. Effectuez un basculement permanent sur Veeam.

Détails du déploiement

Assurez-vous que le datastore NFS du service NetApp Cloud Volume est monté sur GCVE vCenter

Connectez-vous à GCVE vCenter et assurez-vous que le datastore NFS disposant d'un espace suffisant est disponible.
Si ce n'est pas le cas, veuillez vous reporter à "Montez NetApp CVS en tant que datastore NFS sur GCVE"

Assurez-vous que Veeam Backup Recovery est déployé dans l'environnement VMware vSphere existant

Veuillez vous reporter à "Composants de réplication Veeam" documentation d'installation des composants requis.

Créez une tâche de réplication pour lancer la réplication des machines virtuelles vers une instance Google Cloud VMware Engine.

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere"
Voici une vidéo expliquant comment
"Configurer la tâche de réplication".

> La machine virtuelle de réplica peut avoir une adresse IP différente de la machine virtuelle source et peut également être connectée à différents groupes de ports. Pour plus de détails, consultez la vidéo ci-dessus.

Effectuer le basculement de la tâche de réplication Veeam

Pour migrer des machines virtuelles, effectuez "Effectuer un basculement"

Effectuez un basculement permanent sur Veeam.

Pour traiter GCVE comme votre nouvel environnement source, exécutez "Basculement permanent"

Avantages de cette solution

- L'infrastructure de sauvegarde Veeam existante peut être utilisée pour la migration.
- Veeam Replication permet de modifier les adresses IP de VM sur le site cible.
- Possibilité de remmapper les données existantes répliquées en dehors de Veeam (comme les données répliquées de BlueXP)
- A la capacité de spécifier différents groupes de ports réseau sur le site cible.
- Peut spécifier l'ordre de mise sous tension des machines virtuelles.
- Utilise le suivi des blocs de modifications VMware pour réduire la quantité de données à envoyer sur le réseau WAN.
- Possibilité d'exécuter des scripts pré et post pour la réplication.
- Possibilité d'exécuter des scripts pré et post pour les snapshots.

Disponibilité de région – datastore NFS supplémentaire pour Google Cloud Platform (GCP)

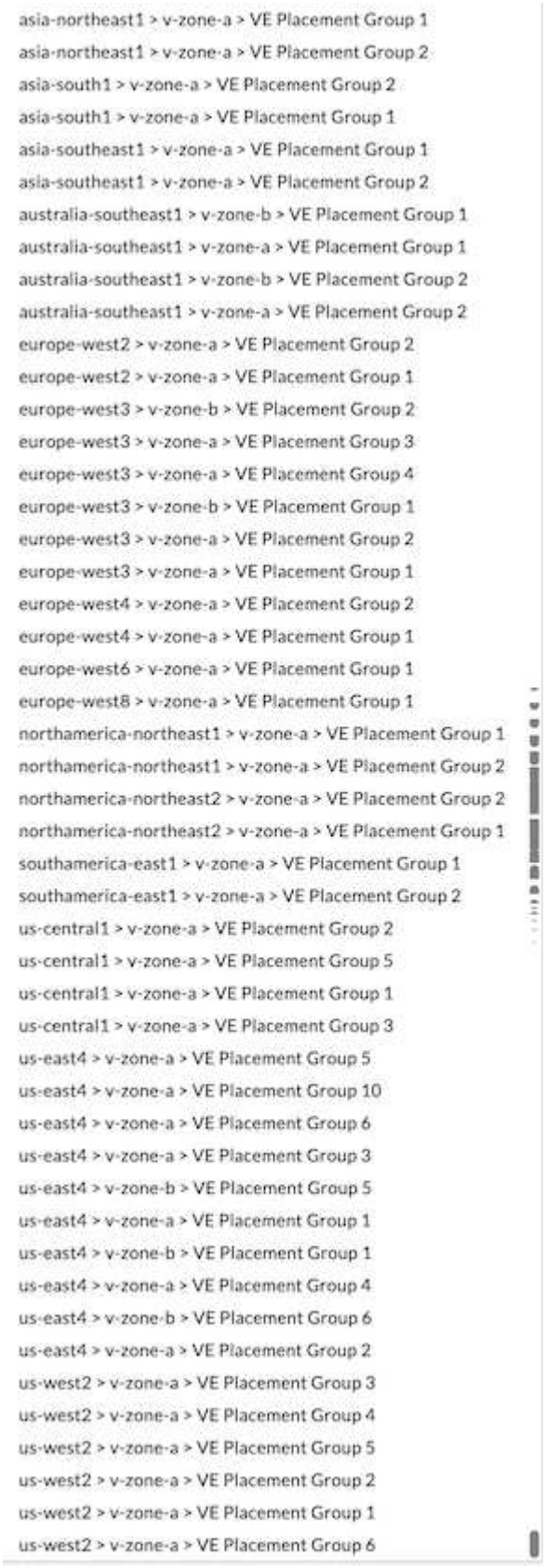
En savoir plus sur la prise en charge par région globale pour GCP, GCVE et CVS.

> Un datastore NFS sera disponible dans les régions où les deux services (GCVE et CVS Performance) sont disponibles.

Un datastore NFS supplémentaire pour GCVE est pris en charge avec le service NetApp Cloud Volume.

Seuls les volumes CVS-Performance peuvent être utilisés pour les datastores GCVE NFS. Pour connaître l'emplacement disponible, reportez-vous à la section "Carte de région globale"

Google Cloud VMware Engine est disponible aux emplacements suivants :



Pour minimiser la latence, le volume NetApp CVS et GCVE dans lesquels vous avez l'intention de monter le volume doivent se trouver dans la même zone de disponibilité. Collaborez avec les architectes de solutions Google et NetApp pour optimiser la disponibilité et le TCO.

Présentation de la sécurité - NetApp Cloud Volumes Service (CVS) dans Google Cloud

Tr-4918 : présentation de la sécurité - NetApp Cloud Volumes Service dans Google Cloud

Oliver Krause, Justin Parisi, NetApp

La sécurité, notamment dans le cloud où l'infrastructure ne contrôle pas les administrateurs du stockage, est primordiale pour faire confiance aux données des offres de services des fournisseurs cloud. Ce document présente les offres de sécurité de NetApp "Cloud Volumes Service fournit dans Google Cloud".

Public visé

Le public visé par ce document comprend, mais sans s'y limiter, les rôles suivants :

- Fournisseurs de cloud
- Administrateurs du stockage
- Les architectes du stockage
- Ressources sur site
- Décideurs de l'entreprise

Pour toute question sur le contenu de ce rapport technique, consultez la section "« Contactez-nous. »"

Abréviation	Définition
CVS-SW	Cloud Volumes Service, CVS de type de service
CVS-Performance	Cloud volumes Service, CVS-Performance type de service
PSA	

Comment sécuriser vos données avec Cloud Volumes Service dans Google Cloud

Avec Cloud Volumes Service dans Google Cloud, vous pouvez sécuriser vos données de manière native,

Architecture et modèle de colocation sécurisés

Cloud Volumes Service procure une architecture sécurisée dans Google Cloud en segmentant la gestion des services (plan de contrôle) et l'accès aux données (plan de contrôle) entre différents terminaux de sorte qu'ils ne puissent en aucun cas affecter l'autre (voir la section) "« Architecture Cloud Volumes Service »"). Il utilise Google "accès aux services privés" (PSA) pour fournir le service. Cette structure distingue le producteur de services fourni et exploité par NetApp, et le consommateur de services, qui est un cloud privé virtuel (VPC)

dans un projet client, en hébergeant les clients souhaitant accéder aux partages de fichiers Cloud Volumes Service.

Dans cette architecture, les locataires (voir la section "« Modèle de colocation »") Sont définis comme des projets Google Cloud complètement isolés les uns des autres, sauf s'ils sont explicitement connectés par l'utilisateur. Les locataires autorisent une isolation complète des volumes de données, des services de noms externes et des autres éléments essentiels de la solution par rapport à d'autres locataires via la plateforme de volumes Cloud Volumes Service. Comme la plateforme Cloud Volumes Service est connectée via le peering VPC, cette isolation s'applique également à celle-ci. Vous pouvez activer le partage de volumes Cloud Volumes Service entre plusieurs projets à l'aide d'un VPC partagé (voir la section) ""VPC partagés"). Vous pouvez appliquer des contrôles d'accès aux partages SMB et aux exportations NFS pour limiter les personnes ou les données qui peuvent afficher ou modifier les jeux de données.

Forte gestion des identités pour le plan de contrôle

Dans le plan de contrôle où se déroule la configuration Cloud Volumes Service, la gestion des identités est gérée à l'aide de "Gestion des accès aux identités". IAM est un service standard qui vous permet de contrôler l'authentification (connexions) et l'autorisation (autorisations) des instances de projet Google Cloud. Toutes les configurations sont effectuées avec des API Cloud Volumes Service sur un transport HTTPS sécurisé via le cryptage TLS 1.2, et l'authentification est effectuée à l'aide de jetons JWT pour une sécurité accrue. L'interface utilisateur de la console Google pour Cloud Volumes Service convertit les entrées utilisateur en appels de l'API Cloud Volumes Service.

Renforcement de la sécurité - limitation des surfaces d'attaque

Une partie de la sécurité efficace limite le nombre de surfaces d'attaque disponibles dans un service. Les surfaces d'attaque peuvent inclure divers éléments, notamment les données au repos, les transferts à la volée, les connexions et les jeux de données eux-mêmes.

Un service géré supprime certaines des surfaces d'attaque par nature dans sa conception. Gestion de l'infrastructure, comme décrit dans la section ""Fonctionnement de l'entretien"," est gérée par une équipe dédiée et automatisée afin de réduire le nombre d'interventions humaines liées aux configurations, ce qui permet de réduire le nombre d'erreurs intentionnelles et non intentionnelles. La mise en réseau est clôturée de sorte que seuls les services nécessaires peuvent accéder les uns aux autres. Le chiffrement est intégré au stockage des données et seul le plan de données nécessite une attention particulière de la part des administrateurs Cloud Volumes Service. En masquant la majeure partie de la gestion derrière une interface API, la sécurité est obtenue en limitant les surfaces d'attaque.

Modèle « zéro confiance »

Historiquement, la philosophie de sécurité INFORMATIQUE a été de faire confiance mais de vérifier, et se manifeste comme s'appuyant uniquement sur des mécanismes externes (tels que des pare-feu et des systèmes de détection d'intrusion) pour atténuer les menaces. Cependant, les attaques et les violations ont évolué pour contourner la vérification dans les environnements par le biais du phishing, de l'ingénierie sociale, des menaces internes et d'autres méthodes qui permettent de vérifier l'entrée en réseau et de causer des ravages.

La confiance zéro est devenue une nouvelle méthodologie de sécurité, avec le mantra actuel comme « n'avoir confiance en rien tout en vérifiant tout ». Par conséquent, aucun accès n'est autorisé par défaut. Ce mantra est appliqué de diverses façons, notamment les pare-feu standard et les systèmes de détection des intrusions (IDS), ainsi que les méthodes suivantes :

- Méthodes d'authentification fortes (telles que les jetons Kerberos ou JWT chiffrés AES)
- Sources d'identités solides uniques (telles que Windows Active Directory, LDAP (Lightweight Directory

Access Protocol) et Google IAM)

- Segmentation réseau et colocation sécurisée (seuls les locataires sont autorisés à accéder par défaut)
- Contrôles d'accès granulaires avec les règles d'accès les moins privilégiées
- Petites listes exclusives d'administrateurs dédiés et fiables avec audit numérique et pistes papier

L'exécution de Cloud Volumes Service dans Google Cloud adhère au modèle « zéro confiance » en mettant en œuvre la politique « confiance en rien et vérification de tout ».

Le cryptage

Chiffrement des données au repos (voir la section "« Chiffrement des données au repos »") En utilisant le chiffrement XTS-AES-256 avec NetApp Volume Encryption (NVE) et en transit avec ""Chiffrement SMB"" Ou NFS Kerberos 5p pris en charge. Soyez tranquille car les transferts de réplication entre régions sont protégés par le chiffrement TLS 1.2 (voir la section « réplication interrégionale »). En outre, Google Networking fournit également des communications cryptées (voir la section ""Chiffrement des données en transit"") pour une couche supplémentaire de protection contre les attaques. Pour plus d'informations sur le chiffrement de transport, reportez-vous à la section "« Réseau Google Cloud »".

Protection des données et sauvegardes

La sécurité ne se limite pas à la prévention des attaques. Il s'agit également de la manière dont nous parvenons à nous remettre des attaques si elles se produisent ou quand elles se produisent. Cette stratégie inclut la protection des données et les sauvegardes. Cloud Volumes Service propose des méthodes de réplication vers d'autres régions en cas de panne (voir la section) "« Réplication inter-région »") ou si un dataset est affecté par une attaque par ransomware. Il peut également effectuer des sauvegardes asynchrones de données vers des emplacements situés en dehors de l'instance Cloud Volumes Service à l'aide de "Sauvegarde Cloud Volumes Service". Grâce aux sauvegardes régulières, la réduction des événements de sécurité peut prendre moins de temps et faire des économies et des problèmes d'administration.

Atténuation rapide des ransomwares grâce aux copies Snapshot leaders du secteur

Outre la protection des données et les sauvegardes, Cloud Volumes Service prend en charge les copies Snapshot immuables (voir la section "« Copies Snapshot immuables »") de volumes qui permettent la restauration suite à des attaques par ransomware (voir la section ""Fonctionnement de l'entretien"") en quelques secondes après la découverte du problème et avec une interruption minimale. Le temps et les effets de la restauration dépendent du calendrier Snapshot. Toutefois, vous pouvez créer des copies Snapshot qui permettent de définir des données modifiées d'une heure ou moins dans le cadre d'attaques par ransomware. Les copies Snapshot ont un impact négligeable sur les performances et l'utilisation de la capacité. Elles constituent une approche à faible risque et à haut rendement pour la protection de vos datasets.

Considérations de sécurité et surfaces d'attaque

Pour comprendre comment sécuriser vos données, il faut d'abord identifier les risques et les surfaces d'attaque potentielles.

Ces mesures comprennent (sans s'y limiter) les éléments suivants :

- Administration et connexions
- Au repos
- Données en cours de vol

- Réseau et pare-feu
- Attaques par ransomware, logiciel malveillant et virus

Comprendre les surfaces d'attaque peut vous aider à mieux sécuriser vos environnements. Cloud Volumes Service dans Google Cloud prend déjà en compte bon nombre de ces sujets et implémente la fonctionnalité de sécurité par défaut, sans aucune interaction administrative.

Assurer des connexions sécurisées

Lors de la sécurisation des composants d'infrastructure critiques, il est impératif de s'assurer que seuls les utilisateurs approuvés peuvent se connecter et gérer vos environnements. Si de mauvais acteurs violent vos informations d'identification administratives, ils ont les clés du château et peuvent faire tout ce qu'ils veulent : changer de configuration, supprimer des volumes et des sauvegardes, créer des backdoors ou désactiver les planifications de snapshots.

Cloud Volumes Service pour Google Cloud protège contre les connexions administratives non autorisées grâce à l'obfuscation du stockage à la demande. Cloud Volumes Service est entièrement géré par le fournisseur cloud, sans qu'il soit possible de se connecter en externe. Toutes les opérations d'installation et de configuration sont entièrement automatisées. De ce fait, un administrateur humain n'a jamais à interagir avec les systèmes, sauf dans de rares circonstances.

Si vous devez vous connecter, Cloud Volumes Service dans Google Cloud sécurise vos connexions en maintenant une liste très courte d'administrateurs de confiance qui ont accès aux systèmes. Ce contrôle d'accès contribue à réduire le nombre de mauvais acteurs potentiels avec accès. De plus, la mise en réseau Google Cloud masque les systèmes derrière des couches de sécurité réseau et expose uniquement ce qui est nécessaire pour le monde extérieur. Pour plus d'informations sur Google Cloud, l'architecture Cloud Volumes Service, consultez la section "« Architecture Cloud Volumes Service »."

Mises à niveau et administration du cluster

Deux domaines présentant des risques de sécurité potentiels incluent l'administration du cluster (que se passe-t-il si un acteur défectueux a accès administrateur) et les mises à niveau (que se passe-t-il si une image logicielle est compromise).

L'administration du stockage

Le stockage fourni à la demande élimine le risque supplémentaire d'exposition des administrateurs en les supprimant pour l'accès aux utilisateurs finaux en dehors du data Center cloud. En effet, la seule configuration effectuée concerne le plan d'accès aux données par les clients. Chaque locataire gère ses propres volumes, et aucun locataire ne peut accéder à d'autres instances Cloud Volumes Service. Le service est géré par l'automatisation, avec une très petite liste d'administrateurs de confiance qui ont accès aux systèmes via les processus décrits dans la section ""Fonctionnement de l'entretien.""

Le type de service CVS-Performance offre une réplication entre régions en tant que possibilité de protéger les données vers une autre région en cas de défaillance d'une région. Dans ce cas, Cloud Volumes Service peut basculer vers une région non affectée pour maintenir l'accès aux données.

Mises à niveau du service

Les mises à jour permettent de protéger les systèmes vulnérables. Chaque mise à jour fournit des améliorations de sécurité et des correctifs de bogues qui réduisent les surfaces d'attaque. Les mises à jour logicielles sont téléchargées à partir de référentiels centralisés et sont validées avant que les mises à jour ne soient autorisées à vérifier que les images officielles sont utilisées et que les mises à niveau ne sont pas compromises par les acteurs défectueux.

Avec Cloud Volumes Service, les mises à jour sont gérées par les équipes des fournisseurs cloud, ce qui élimine les risques pour les équipes d'administration. Les experts maîtrisent la configuration et les mises à niveau de manière automatisée et entièrement testée. Les mises à niveau ne entraînent pas de perturbation et Cloud Volumes Service effectue les mises à jour les plus récentes pour des résultats globaux optimaux.

Pour plus d'informations sur l'équipe d'administration qui effectue ces mises à niveau de service, reportez-vous à la section ""Fonctionnement de l'entretien.""

Sécurisation des données au repos

Le chiffrement des données au repos est important pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque. Les données au repos Cloud Volumes Service sont protégées au moyen du chiffrement logiciel.

- Les clés générées par Google sont utilisées pour CVS-SW.
- Pour CVS-Performance, les clés par volume sont stockées dans un gestionnaire de clés intégré dans Cloud Volumes Service, qui utilise NetApp ONTAP CryptoMod pour générer des clés de cryptage AES-256. CryptoMod figure dans la liste des modules validés CCVP FIPS 140-2. Voir "Certificat no FIPS 140-2-4144".

Depuis novembre 2021, CVS-Performance a mis à disposition une fonctionnalité de chiffrement géré par le client (CMEK). Cette fonctionnalité vous permet de chiffrer les clés par volume avec des clés principales par projet et par région hébergées dans Google Key Management Service (KMS). LES KILOMÈTRES vous permettent d'associer des gestionnaires de clés externes.

Pour plus d'informations sur la configuration de KMS pour CVS-Performance, "Consultez la documentation Cloud Volumes Service".

Pour plus d'informations sur l'architecture, voir la section "« Architecture Cloud Volumes Service »."

Sécurisation des données à la volée

En plus de sécuriser les données au repos, vous devez également être à même de sécuriser les données lorsqu'elles sont en transit entre l'instance Cloud Volumes Service et un client ou une cible de réplication. Cloud Volumes Service permet le chiffrement des données à la volée sur les protocoles NAS à l'aide de méthodes de chiffrement, telles que le chiffrement SMB via Kerberos, la signature/chiffrement des paquets et NFS Kerberos 5p pour le chiffrement complet des transferts de données.

La réplication des volumes Cloud Volumes Service utilise le protocole TLS 1.2, qui tire parti des méthodes de chiffrement AES-GCM.

La plupart des protocoles en vol non sécurisés tels que telnet, NDMP, etc. Sont désactivés par défaut. Toutefois, le DNS n'est pas chiffré par Cloud Volumes Service (pas de prise en charge de DNS sec) et doit être chiffré en utilisant le cryptage réseau externe lorsque cela est possible. Voir la section ""Chiffrement des données en transit"" pour en savoir plus sur la sécurisation des données à la volée.

Pour plus d'informations sur le cryptage du protocole NAS, reportez-vous à la section "« Protocoles NAS »."

Utilisateurs et groupes pour les autorisations NAS

Une partie de la sécurisation de vos données dans le cloud implique une authentification adéquate des utilisateurs et des groupes, où les utilisateurs accédant aux données sont vérifiés en tant qu'utilisateurs réels dans l'environnement et où les groupes contiennent des utilisateurs valides. Ces utilisateurs et groupes offrent un accès initial au partage et à l'exportation, ainsi qu'une validation des autorisations pour les fichiers et dossiers du système de stockage.

Cloud Volumes Service utilise l'authentification standard d'utilisateur et de groupe Windows basée sur Active Directory pour les partages SMB et les autorisations de style Windows. Le service peut également tirer parti de fournisseurs d'identités UNIX tels que le LDAP pour les utilisateurs et groupes UNIX pour les exportations NFS, la validation des ID NFSv4, l'authentification Kerberos et les ACL NFSv4.

Actuellement, seul Active Directory LDAP est pris en charge avec la fonctionnalité Cloud Volumes Service pour LDAP.

La détection, la prévention et la réduction des ransomwares, des malwares et des virus

Les ransomwares, les malwares et les virus sont une menace persistante pour les administrateurs, et la détection, la prévention et la réduction de ces menaces sont toujours une priorité absolue pour les entreprises. En cas d'attaque par ransomware d'un jeu de données stratégique, vous pouvez coûter plusieurs millions de dollars. Il est donc préférable de faire ce que vous pouvez minimiser ce risque.

Bien que Cloud Volumes Service n'inclut actuellement pas de mesures de détection ou de prévention natives, telles que la protection antivirus ou "détection automatique des ransomwares", Il existe des moyens de récupérer rapidement après un événement ransomware en activant des planifications Snapshot régulières. Les copies Snapshot sont immuables et les pointeurs en lecture seule vers les blocs modifiés dans le système de fichiers sont quasi instantanés, ont un impact minimal sur les performances et utilisent uniquement de l'espace lorsque les données sont modifiées ou supprimées. Vous pouvez définir des calendriers pour les copies Snapshot en fonction de l'objectif de point de récupération (RPO)/objectif de durée de restauration (RTO) souhaité. Vous pouvez également conserver jusqu'à 1,024 copies Snapshot par volume.

La prise en charge des snapshots est incluse sans frais supplémentaires (en plus des frais de stockage de données pour les blocs/données modifiés conservés par les copies Snapshot) avec Cloud Volumes Service et, en cas d'attaque par ransomware, elle peut être utilisée pour restaurer la copie Snapshot avant l'attaque. Les restaurations Snapshot ne prennent que quelques secondes et vous permettent ensuite de rétablir le service des données normal. Pour plus d'informations, voir "Solution NetApp pour ransomware".

Pour empêcher les ransomwares d'affecter votre activité, vous devez adopter une approche à plusieurs couches :

- Protection des terminaux
- Protection contre les menaces externes grâce à des pare-feu réseau
- Détection des anomalies de données
- Plusieurs sauvegardes (sur site et hors site) de jeux de données stratégiques
- Tests réguliers de restauration des sauvegardes
- Copies Snapshot NetApp immuables en lecture seule
- Authentification multifacteur pour les infrastructures stratégiques
- Audits de sécurité des connexions système

Cette liste est loin d'être exhaustive, mais elle constitue un bon plan à suivre pour gérer le potentiel d'attaques par ransomware. Cloud Volumes Service dans Google Cloud fournit plusieurs façons de vous protéger contre les événements par ransomware et de réduire leurs effets.

Copies Snapshot immuables

Cloud Volumes Service fournit de manière native des copies Snapshot immuables en lecture seule, qui sont mises en œuvre dans un calendrier personnalisable pour une restauration instantanée rapide en cas de suppression de données ou si un volume entier a été victime d'une attaque par ransomware. Les restaurations

Snapshot vers les précédentes copies Snapshot sont rapides et limitent la perte de données en fonction de la période de conservation de vos planifications Snapshot et des objectifs RTO/RPO. L'impact de la technologie Snapshot sur les performances est négligeable.

Étant donné que les copies Snapshot dans Cloud Volumes Service sont en lecture seule, elles ne peuvent pas être infectées par un ransomware à moins que ces dernières aient proliféré dans le dataset inaperçu et que les copies Snapshot ont été prises en compte par les données infectées par un ransomware. C'est pourquoi vous devez également envisager la détection par ransomware basée sur les anomalies de données. Cloud Volumes Service n'offre pas actuellement de fonction de détection native, mais vous pouvez utiliser un logiciel de surveillance externe.

Les sauvegardes et les restaurations

Cloud Volumes Service fournit des fonctionnalités standard de sauvegarde client NAS (sauvegardes sur NFS ou SMB).

- CVS-Performance offre une réplication de volume entre régions vers d'autres volumes CVS-Performance. Pour plus d'informations, voir "réplication de volume" Dans la documentation Cloud Volumes Service.
- CVS-SW offre des fonctionnalités de sauvegarde/restauration de volume natives des services. Pour plus d'informations, voir "la sauvegarde dans le cloud" Dans la documentation Cloud Volumes Service.

La réplication de volume fournit une copie exacte du volume source pour un basculement rapide en cas d'incident, y compris en cas d'attaque par ransomware.

Réplication entre les régions

CVS-Performance vous permet de répliquer en toute sécurité des volumes entre les régions Google Cloud pour la protection des données et les archives à l'aide du chiffrement TLS1.2 AES 256 GCM sur un réseau de service back-end contrôlé par NetApp à l'aide d'interfaces spécifiques utilisées pour la réplication sur le réseau Google. Un volume primaire (source) contient les données de production actives et effectue une réplication vers un volume secondaire (destination) afin de fournir une réplique exacte du jeu de données primaire.

La réplication initiale transfère tous les blocs, mais les mises à jour ne transmettent que les blocs modifiés dans un volume primaire. Par exemple, si une base de données de 1 To résidant sur un volume primaire est répliquée sur le volume secondaire, alors 1 To d'espace est transféré sur la réplication initiale. Si cette base de données a quelques centaines de lignes (hypothetiquement, quelques Mo) qui changent entre l'initialisation et la mise à jour suivante, seuls les blocs avec les lignes modifiées sont répliqués sur le secondaire (quelques Mo). Cela permet de s'assurer que les temps de transfert restent faibles et de limiter les coûts de réplication.

Toutes les autorisations des fichiers et dossiers sont répliquées sur le volume secondaire, mais les autorisations d'accès au partage (telles que les export-policies et les règles ou les partages SMB et les ACL de partage) doivent être gérées de manière indépendante. Dans le cas d'un basculement de site, le site de destination doit utiliser les mêmes services de nom et les mêmes connexions de domaine Active Directory pour assurer un traitement cohérent des identités et autorisations des utilisateurs et des groupes. En cas d'incident, il est possible d'utiliser un volume secondaire comme cible de basculement afin de briser la relation de réplication, qui convertit le volume secondaire en lecture/écriture.

Les répliques de volumes sont en lecture seule, ce qui permet d'obtenir une copie inaltérable des données hors site pour une restauration rapide des données lorsqu'un virus a infecté des données ou où un ransomware a chiffré le jeu de données principal. Les données en lecture seule ne sont pas cryptées, mais, en cas de volume primaire affecté et de réplication, les blocs infectés sont également répliqués. Vous pouvez utiliser des copies Snapshot plus anciennes et non affectées pour effectuer une restauration, mais les SLA peuvent tomber dans la plage des RTO/RPO promis en fonction de la rapidité de détection d'une attaque.

De plus, vous pouvez empêcher les actions administratives malveillantes, telles que les suppressions de

volumes, les suppressions de snapshots ou les modifications de planifications de snapshots, dans le cadre de la gestion de la réplication multi-région (CRR) dans Google Cloud. Pour ce faire, des rôles personnalisés séparent les administrateurs de volumes, qui peuvent supprimer des volumes source sans interrompre les miroirs et ne peuvent donc pas supprimer des volumes de destination des administrateurs CRR, qui ne peuvent pas effectuer d'opérations de volume. Voir "Considérations de sécurité" Dans la documentation Cloud Volumes Service pour les autorisations autorisées par chaque groupe d'administrateurs.

Sauvegarde Cloud Volumes Service

Bien que Cloud Volumes Service assure une durabilité élevée des données, les événements externes peuvent entraîner des pertes de données. En cas d'incident de sécurité tel qu'un virus ou un ransomware, les sauvegardes et les restaurations sont essentielles pour la reprise de l'accès aux données en temps opportun. Un administrateur peut accidentellement supprimer un volume Cloud Volumes Service. Ou il suffit aux utilisateurs de conserver les versions de sauvegarde de leurs données pendant plusieurs mois et de conserver l'espace supplémentaire de copie Snapshot dans le volume peut représenter un défi de coût. Même si les copies Snapshot doivent être le moyen le plus conseillé de conserver les versions de sauvegarde pendant les dernières semaines pour restaurer les données perdues, elles se trouvent à l'intérieur du volume et sont perdues en cas de perte du volume.

Pour toutes ces raisons, NetApp Cloud Volumes Service propose des services de sauvegarde par l'intermédiaire de "Sauvegarde Cloud Volumes Service".

La sauvegarde Cloud Volumes Service génère une copie du volume sur Google Cloud Storage (GCS). Il sauvegarde uniquement les données réelles stockées au sein du volume, et non l'espace libre. Cela fonctionne comme une opération incrémentielle à l'infini. Cela signifie qu'il transfère le contenu du volume une fois et depuis là, il continue de sauvegarder les données modifiées uniquement. Comparé aux concepts de sauvegarde classiques à plusieurs sauvegardes complètes, elle permet d'économiser une grande quantité de stockage de sauvegarde, ce qui réduit les coûts. Le prix mensuel de l'espace de sauvegarde est inférieur à celui d'un volume. C'est l'endroit idéal pour conserver les versions de sauvegarde plus longtemps.

Les utilisateurs peuvent utiliser une sauvegarde Cloud Volumes Service pour restaurer toute version de sauvegarde sur un volume identique ou différent dans la même région. Si le volume source est supprimé, les données de sauvegarde sont conservées et doivent être gérées indépendamment (par exemple, supprimées).

Cloud Volumes Service Backup est intégré à Cloud Volumes Service en option. Les utilisateurs peuvent décider des volumes à protéger en activant la sauvegarde Cloud Volumes Service sur la base de chaque volume. Voir la "Documentation de sauvegarde Cloud Volumes Service" pour plus d'informations sur les sauvegardes, le "nombre maximal de versions de sauvegarde prises en charge", planification, et "tarifs".

Toutes les données de sauvegarde d'un projet sont stockées dans un compartiment GCS, géré par le service et non visible par l'utilisateur. Chaque projet utilise un compartiment différent. Actuellement, les compartiments se trouvent dans la même région que les volumes Cloud Volumes Service, mais davantage d'options sont présentées. Consultez la documentation pour connaître l'état le plus récent.

Le transport des données d'un compartiment Cloud Volumes Service vers GCS utilise des réseaux Google internes et externes avec HTTPS et TLS1.2. Les données sont chiffrées au repos à l'aide de clés gérées par Google.

Pour gérer la sauvegarde Cloud Volumes Service (création, suppression et restauration de sauvegardes), un utilisateur doit disposer du "roles/netappdevolumes.admin" rôle.

Architecture

Présentation

L'architecture et la sécurité font partie des processus de confiance aux solutions cloud. Cette section décrit différents aspects de l'architecture Cloud Volumes Service de Google qui contribuent à réduire les risques de sécurisation des données et indique les domaines dans lesquels des étapes de configuration supplémentaires peuvent être nécessaires pour obtenir le déploiement le plus sécurisé.

L'architecture générale d'Cloud Volumes Service peut être décomposée en deux composants principaux : le plan de contrôle et le plan de données.

Plan de contrôle

Le plan de contrôle d'Cloud Volumes Service est l'infrastructure back-end gérée par les administrateurs Cloud Volumes Service et le logiciel d'automatisation natif de NetApp. Ce plan est totalement transparent pour les utilisateurs finaux. Il inclut des fonctionnalités de mise en réseau, du matériel de stockage, des mises à jour logicielles, etc. Pour que les solutions hébergées dans le cloud telles que Cloud Volumes Service puissent apporter de la valeur ajoutée.

Plan de données

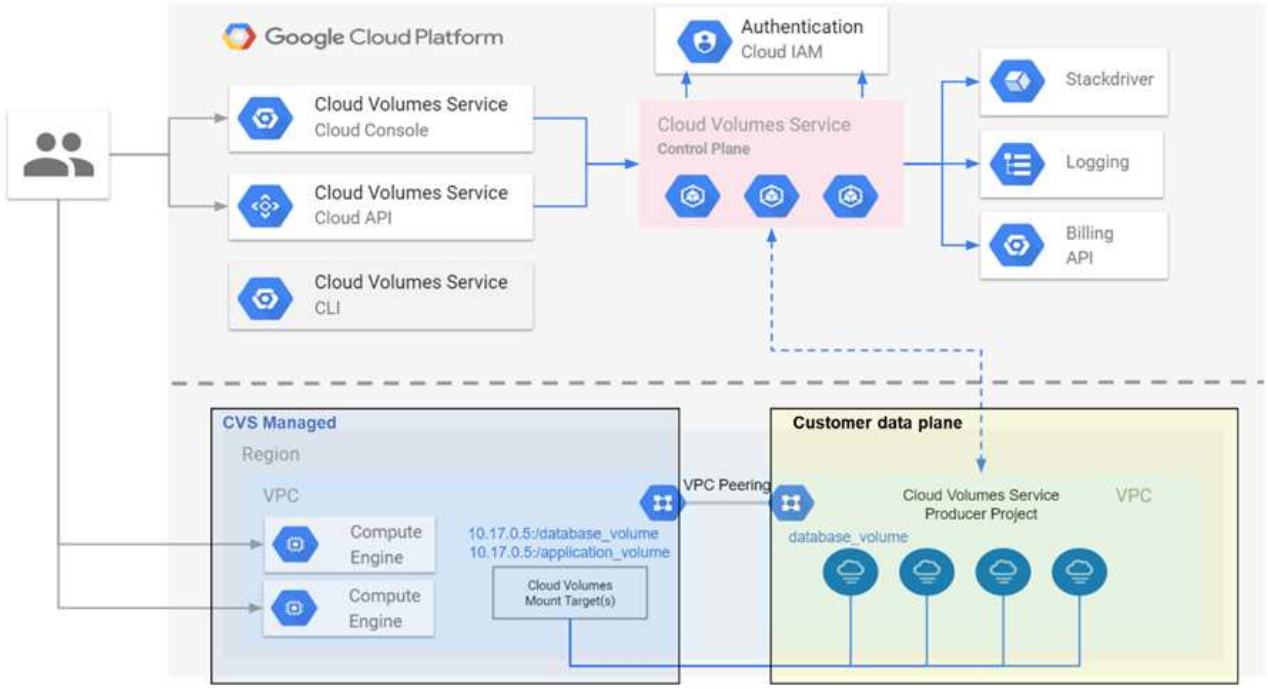
Le plan de données de Cloud Volumes Service inclut les volumes de données réels et la configuration Cloud Volumes Service globale (contrôle d'accès, authentification Kerberos, etc.). Le plan de données est entièrement sous le contrôle des utilisateurs finaux et des consommateurs de la plateforme Cloud Volumes Service.

La façon dont chaque plan est sécurisé et géré est différente. Ces différences sont en commençant par la présentation de l'architecture Cloud Volumes Service.

Architecture Cloud Volumes Service

De la même manière que d'autres services Google Cloud natifs, tels que CloudSQL, Google Cloud VMware Engine (GCVE) et filestore, utilise Cloud Volumes Service "Google PSA" pour fournir le service. Dans PSA, les services sont intégrés à un projet de producteur de services, qui utilise "Peering de réseau VPC" pour se connecter au consommateur de services. Le producteur de service est fourni et exploité par NetApp, et le consommateur du service est un VPC dans un projet client qui héberge les clients souhaitant accéder aux partages de fichiers Cloud Volumes Service.

La figure suivante, référencée à partir du "section architecture" De la documentation Cloud Volumes Service, affiche une vue générale.



La partie au-dessus de la ligne pointillée montre le plan de contrôle du service, qui contrôle le cycle de vie du volume. La partie sous la ligne pointillée montre le plan de données. La zone bleue gauche représente le VPC (Service Consumer) de l'utilisateur, la zone bleue droite est le producteur de services fourni par NetApp. Les deux sont connectés via le peering VPC.

Modèle de location

Dans Cloud Volumes Service, chaque projet est considéré comme un locataire unique. Cela signifie que la manipulation des volumes et des copies Snapshot, etc., est effectuée sur la base de chaque projet. En d'autres termes, tous les volumes sont détenus par le projet dans lequel ils ont été créés, et seul ce projet peut gérer et accéder aux données qui leur sont propres par défaut. Cette vue est considérée comme le plan de contrôle du service.

VPC partagés

Dans la vue du plan de données, Cloud Volumes Service peut se connecter à un VPC partagé. Vous pouvez créer des volumes dans le projet d'hébergement ou dans l'un des projets de service connectés au VPC partagé. Tous les projets (hôte ou service) connectés à ce VPC partagé peuvent atteindre les volumes au niveau de la couche réseau (TCP/IP). Étant donné que tous les clients disposant d'une connectivité réseau sur le VPC partagé peuvent accéder aux données via les protocoles NAS, vous devez utiliser le contrôle d'accès sur chacun des volumes (listes de contrôle d'accès (ACL) d'utilisateur/de groupe, ainsi que les noms d'hôte/adresses IP pour les exportations NFS) pour contrôler qui peut accéder aux données.

Vous pouvez connecter Cloud Volumes Service à cinq VPC maximum par projet client. Sur le plan de contrôle, le projet vous permet de gérer tous les volumes créés, quel que soit le VPC auquel ils sont connectés. Sur le plan de données, les VPC sont isolés les uns des autres et chaque volume ne peut être connecté qu'à un VPC.

L'accès aux volumes individuels est contrôlé par des mécanismes de contrôle d'accès spécifiques à un protocole (NFS/SMB).

En d'autres termes, sur la couche réseau, tous les projets connectés au VPC partagé peuvent voir le volume,

tandis que, du point de vue de la gestion, le plan de contrôle ne permet au projet propriétaire de voir le volume que.

Contrôles du service VPC

Les contrôles du service VPC établissent un périmètre de contrôle d'accès autour des services Google Cloud reliés à Internet et accessibles dans le monde entier. Ces services permettent le contrôle d'accès par le biais d'identités utilisateur, mais ne peuvent pas limiter les demandes d'emplacement réseau. Les contrôles de service VPC comblent ce fossé en introduisant des capacités permettant de limiter l'accès aux réseaux définis.

Le plan de données Cloud Volumes Service n'est pas connecté à Internet externe mais à des VPC privés avec des limites de réseau bien définies (périmètres). Sur ce réseau, chaque volume utilise un contrôle d'accès spécifique au protocole. Toute connectivité réseau externe est créée de manière explicite par les administrateurs de projet Google Cloud. Le plan de contrôle, cependant, n'offre pas les mêmes protections que le plan de données et peut être accessible par n'importe qui à partir de n'importe où avec des informations d'identification valides ("Jetons JWT").

En bref, le plan de données Cloud Volumes Service offre la possibilité de contrôler l'accès au réseau sans devoir prendre en charge les contrôles de service VPC et n'utilise pas explicitement les contrôles de service VPC.

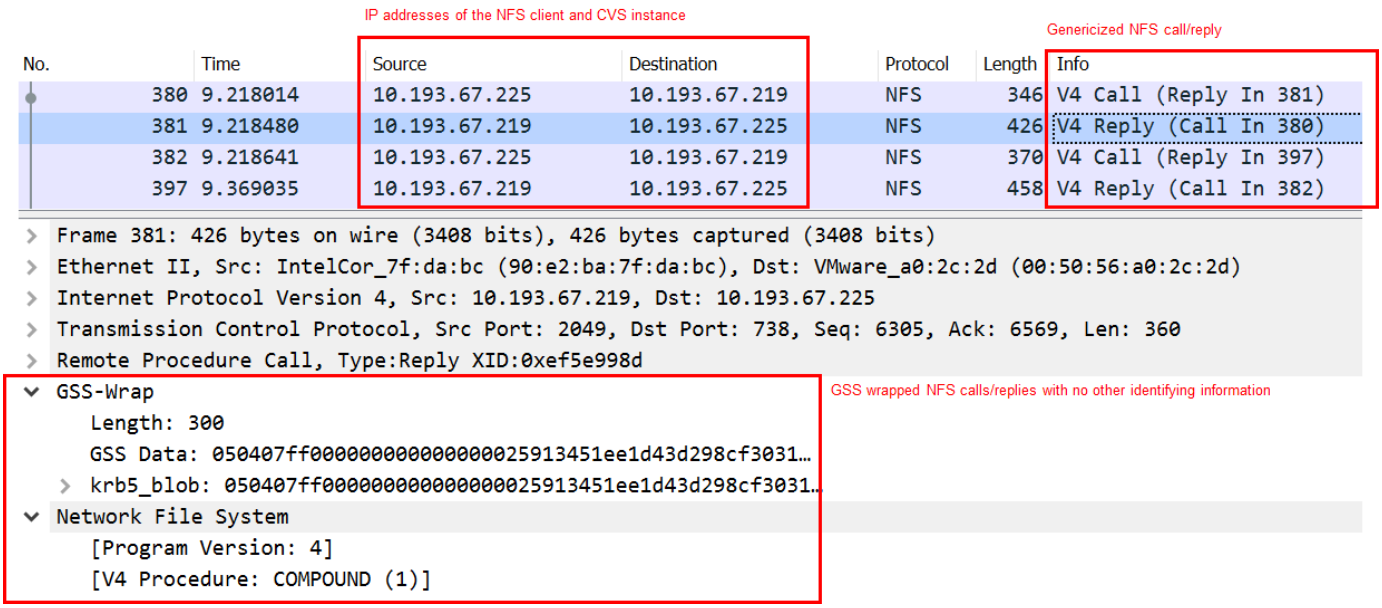
Considérations relatives à la détection et à la détection des paquets

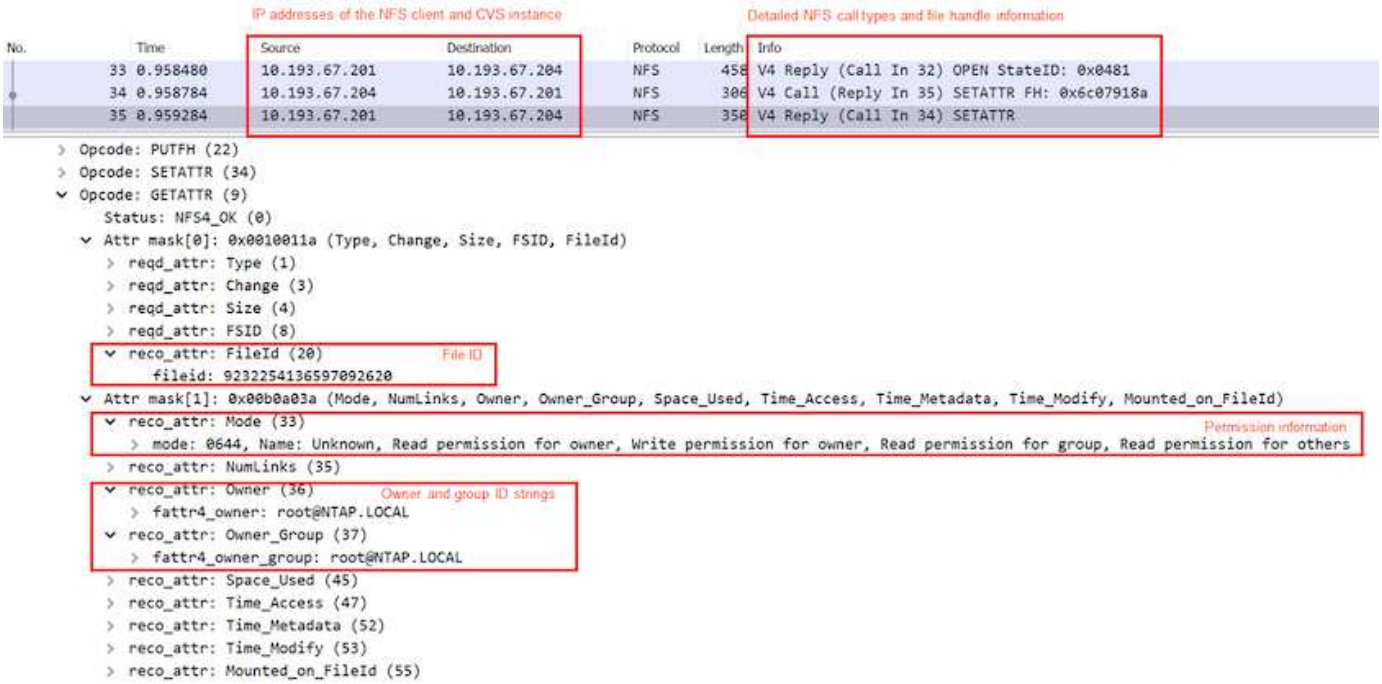
Les captures de paquets peuvent être utiles pour résoudre des problèmes réseau ou d'autres problèmes (autorisations NAS, connectivité LDAP, etc.), mais peuvent également être utilisées de manière malveillante pour obtenir des informations sur les adresses IP réseau, les adresses MAC, les noms d'utilisateurs et de groupes, ainsi que le niveau de sécurité utilisé sur les noeuds finaux. En raison de la configuration de la mise en réseau Google Cloud, des VPC et des règles de pare-feu, l'accès non autorisé aux paquets réseau devrait être difficile à obtenir sans identifiants de connexion utilisateur ou "Jetons JWT" dans les instances cloud. Les captures de paquets ne sont possibles que sur les terminaux (tels que les machines virtuelles) et uniquement sur les terminaux internes au VPC, à moins qu'un VPC partagé et/ou un tunnel/IP de réseau externe ne soit utilisé pour permettre explicitement le trafic externe vers les terminaux. Il n'y a pas de moyen de sniff trafic en dehors des clients.

Lorsque des VPC partagés sont utilisés, le chiffrement à la volée avec NFS Kerberos et/ou "Chiffrement SMB" peut masquer une grande partie des informations tirées de traces. Cependant, un certain trafic est encore envoyé en texte clair, par exemple "DNS" et "Requêtes LDAP". La figure suivante montre une capture de paquet à partir d'une requête LDAP en texte clair provenant de Cloud Volumes Service et les informations d'identification potentielles qui sont exposées. Les requêtes LDAP dans Cloud Volumes Service ne prennent actuellement pas en charge le cryptage ou LDAP sur SSL. CVS-Performance prend en charge la signature LDAP, si Active Directory en fait la demande. CVS-SW ne prend pas en charge la signature LDAP.

UnixUserPassword est interrogé par LDAP et n'est pas envoyé en texte clair, mais plutôt dans un hash salé. Par défaut, Windows LDAP ne renseigne pas les champs unixUserPassword. Ce champ est uniquement obligatoire si vous devez utiliser Windows LDAP pour les connexions interactives via LDAP aux clients. Cloud Volumes Service ne prend pas en charge les connexions LDAP interactives vers les instances.

La figure suivante montre une capture de paquets d'une conversation Kerberos NFS à côté d'une capture de NFS sur AUTH_SYS. Notez que les informations disponibles dans une trace diffèrent entre les deux et que l'activation du cryptage à la volée offre une sécurité globale accrue pour le trafic NAS.





Interfaces réseau des VM

Une astuce peut tenter d'ajouter une nouvelle carte d'interface réseau (NIC) à une machine virtuelle dans "mode promiscueux" (Mise en miroir des ports) ou activez le mode promiscuous sur une carte réseau existante afin de sniiser tout le trafic. Dans Google Cloud, l'ajout d'une nouvelle carte réseau nécessite l'arrêt complet d'une machine virtuelle, ce qui génère des alertes, ce qui rend les pirates informatiques inaperçus.

De plus, les cartes réseau ne peuvent pas être configurées en mode promiscuous et déclencheront des alertes dans Google Cloud.

Architecture du plan de contrôle

Toutes les actions de gestion vers Cloud Volumes Service sont effectuées par l'intermédiaire d'une API. La gestion Cloud Volumes Service intégrée à la console GCP Cloud utilise également l'API Cloud Volumes Service.

Gestion des identités et des accès

Gestion des identités et des accès ("IAM") Est un service standard qui vous permet de contrôler l'authentification (connexions) et l'autorisation (autorisations) des instances de projet Google Cloud. Google IAM fournit une piste d'audit complète des autorisations et des suppressions. Actuellement, Cloud Volumes Service ne fournit pas d'audit du plan de contrôle.

Présentation de l'autorisation/autorisation

IAM propose des autorisations granulaires intégrées pour Cloud Volumes Service. Vous pouvez trouver un "liste complète des autorisations granulaires ici".

IAM propose également deux rôles prédéfinis appelés `netappcloudvolumes.admin` et `netappcloudvolumes.viewer`. Ces rôles peuvent être attribués à des utilisateurs ou à des comptes de service spécifiques.

Attribuez les rôles et les autorisations appropriés pour permettre aux utilisateurs IAM de gérer Cloud Volumes

Service.

Voici quelques exemples d'utilisation d'autorisations granulaires :

- Créez un rôle personnalisé avec uniquement les autorisations obtenir/liste/créer/mettre à jour pour que les utilisateurs ne puissent pas supprimer de volumes.
- Utilisez un rôle personnalisé avec uniquement `snapshot.*` Autorisations permettant de créer un compte de service utilisé pour créer une intégration Snapshot cohérente avec les applications.
- Définissez un rôle personnalisé à déléguer `volumereplication.*` pour des utilisateurs spécifiques.

Comptes de service

Pour passer des appels API Cloud Volumes Service par le biais de scripts ou "Terraform", vous devez créer un compte de service avec `roles/netappcloudvolumes.admin` rôle. Vous pouvez utiliser ce compte de service pour générer les jetons JWT requis pour authentifier les requêtes API Cloud Volumes Service de deux manières différentes :

- Générez une clé JSON et utilisez les API Google pour dériver un jeton JWT. C'est l'approche la plus simple, mais elle implique une gestion manuelle des secrets (clé JSON).
- Utiliser "Emprunt d'identité du compte de service" avec `roles/iam.serviceAccountTokenCreator`. Le code (script, Terraform, etc.) s'exécute avec "Informations d'identification par défaut de l'application" et emprunt de l'identité du compte de service pour obtenir ses autorisations. Cette approche reflète les bonnes pratiques de sécurité de Google.

Voir "Création de votre compte de service et de votre clé privée" Dans la documentation Google Cloud pour plus d'informations.

API Cloud Volumes Service

L'API Cloud Volumes Service utilise une API REST en utilisant HTTPS (TLSv1.2) comme transport réseau sous-jacent. Vous trouverez la définition d'API la plus récente "ici" Et des informations sur l'utilisation de l'API à l'adresse "API Cloud volumes dans la documentation Google Cloud".

Le terminal API est exploité et sécurisé par NetApp à l'aide de la fonctionnalité HTTPS standard (TLSv1.2).

Jetons JWT

L'authentification à l'API est effectuée avec des jetons de support JWT ("RFC-7519"). Les jetons JWT valides doivent être obtenus via l'authentification Google Cloud IAM. Pour ce faire, il faut récupérer un jeton depuis IAM en fournissant une clé JSON de compte de service.

Consignation des audits

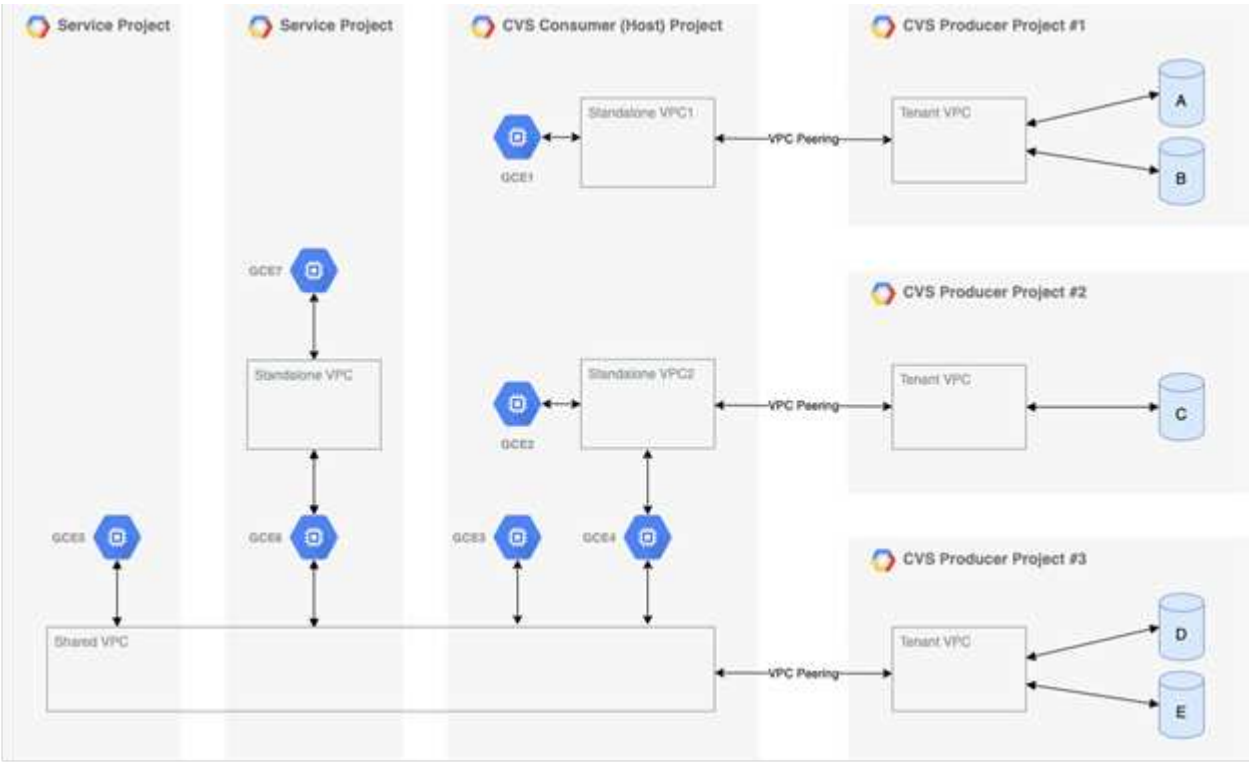
Aucun journal d'audit du plan de contrôle accessible par l'utilisateur n'est actuellement disponible.

Architecture de plan de données

Cloud Volumes Service pour Google Cloud s'appuie sur Google Cloud "accès aux services privés" structure. Dans ce cadre, les utilisateurs peuvent se connecter à Cloud Volumes Service. Cette structure utilise des services de mise en réseau et des constructions de peering de VPC comme d'autres services Google Cloud, qui assurent une isolation complète entre les locataires.

Pour obtenir une présentation de l'architecture de Cloud Volumes Service pour Google Cloud, rendez-vous sur "Architecture pour Cloud Volumes Service".

Les VPC utilisateur (autonomes ou partagés) sont associés à des VPC au sein de projets de locataires gérés Cloud Volumes Service, qui hébergent les volumes.



La figure précédente montre un projet (projet CVS de milieu de gamme) avec trois réseaux VPC connectés à Cloud Volumes Service et plusieurs VM de moteur de calcul (GCE1-7) partageant des volumes :

- VPC1 permet à GCE1 d'accéder aux volumes A et B.
- Le VPC2 permet aux GCE2 et GCE4 d'accéder au volume C.
- Le troisième réseau VPC est un VPC partagé, partagé avec deux projets de service. Il permet aux GCE3, GCE4, GCE5 et GCE6 d'accéder aux volumes D et E. Les réseaux VPC partagés ne sont pris en charge que pour les volumes du type de service CVS-Performance.

Le GCE7 ne peut accéder à aucun volume.

Les données peuvent être chiffrées à la fois en transit (par le chiffrement Kerberos et/ou SMB) et au repos dans Cloud Volumes Service.

Chiffrement des données en transit

Les données en transit peuvent être chiffrées au niveau de la couche de protocole NAS et le réseau Google Cloud lui-même est chiffré, comme décrit dans les sections suivantes.

Réseau Google Cloud

Google Cloud chiffre le trafic au niveau du réseau comme décrit à la section "Chiffrement en transit" Dans la

documentation Google. Comme indiqué dans la section « architecture de services Cloud volumes », Cloud Volumes Service est fourni à partir d'un projet de production PSA contrôlé par NetApp.

Dans le cas de CVS-SW, le locataire exécute les machines virtuelles Google pour fournir le service. Le trafic entre les VM utilisateur et les machines virtuelles Cloud Volumes Service est automatiquement chiffré par Google.

Bien que le chemin d'accès aux données de CVS-Performance ne soit pas intégralement chiffré sur la couche réseau, NetApp et Google utilisent une combinaison "De cryptage IEEE 802.1AE (MACSec)", "encapsulation" (Chiffrement des données) et des réseaux physiquement restreints pour protéger les données en transit entre le type de service Cloud Volumes Service CVS-Performance et Google Cloud.

Protocoles NAS

Les protocoles NAS NFS et SMB fournissent un chiffrement de transport en option au niveau de la couche de protocoles.

Chiffrement SMB

"Chiffrement SMB" Offre un cryptage de bout en bout des données SMB et protège les données contre les occurrences de réseaux non fiables. Vous pouvez activer le cryptage à la fois pour la connexion de données client/serveur (uniquement disponible pour les clients compatibles SMB3.x) et pour l'authentification du contrôleur serveur/domaine.

Lorsque le cryptage SMB est activé, les clients qui ne prennent pas en charge le cryptage ne peuvent pas accéder au partage.

Cloud Volumes Service prend en charge le chiffrement de sécurité RC4-HMAC, AES-128-CTS-HMAC-SHA1 et AES-256-CTS-HMAC-SHA1 pour le cryptage SMB. SMB négocie le type de cryptage le plus élevé pris en charge par le serveur.

Kerberos NFSv4.1

Pour NFSv4.1, CVS-Performance propose l'authentification Kerberos, comme décrit dans "RFC7530". Vous pouvez activer Kerberos par volume.

Le type de chiffrement le plus puissant actuellement disponible pour Kerberos est AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service prend en charge AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 et DES pour NFS. Il prend également en charge ARCFOUR-HMAC (RC4) pour le trafic CIFS/SMB, mais pas pour NFS.

Kerberos propose trois niveaux de sécurité différents pour les montages NFS qui offrent des options de sécurité Kerberos.

Selon RedHat "Options de montage courantes" documentation :

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

En règle générale, plus le niveau de sécurité Kerberos est important, plus les performances sont faibles, car le client et le serveur passent du temps à chiffrer et déchiffrer les opérations NFS pour chaque paquet envoyé. De nombreux clients et serveurs NFS prennent en charge le transfert AES-ni vers les processeurs pour une meilleure expérience globale. Cependant, l'impact sur les performances de Kerberos 5p (chiffrement complet de bout en bout) est considérablement plus important que l'impact de Kerberos 5 (authentification utilisateur).

Le tableau ci-dessous présente les différences par rapport à chaque niveau pour la sécurité et les performances.

Niveau de sécurité	Sécurité	Performance
NFSv3 : sys	• Moins sécurisé ; texte brut avec ID utilisateur numérique/ID de groupe • Possibilité d'afficher les UID, GID, adresses IP client, chemins d'exportation, noms de fichiers, autorisations dans les captures de paquets	• Idéal pour la plupart des cas
NFSv4.x — sys	• Plus sûr que NFSv3 (ID client, correspondance de chaîne de nom/chaîne de domaine) mais texte brut • Possibilité d'afficher les UID, GID, adresses IP des clients, chaînes de noms, ID de domaine, chemins d'exportation, noms de fichiers, autorisations dans les captures de paquets	• Adapté aux charges de travail séquentielles (VM, bases de données, fichiers volumineux) • Erreurs avec un nombre élevé de fichiers/métadonnées élevées (30 à 50 % en moins)

Niveau de sécurité	Sécurité	Performance
NFS - krb5	• Le chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS — enveloppe l'UID/GID des utilisateurs/groupes dans les appels RPC dans l'encapsuleur GSS • L'utilisateur qui demande l'accès au montage a besoin d'un ticket Kerberos valide (via nom d'utilisateur/mot de passe ou par échange manuel de clés) ; le ticket expire après une période spécifiée et l'utilisateur doit de nouveau s'authentifier pour l'accès • Aucun chiffrement pour les opérations NFS ou les protocoles annexes tels que mount/portmapper/nlm (peut voir les chemins d'exportation, les adresses IP, les pointeurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets)	• Le meilleur dans la plupart des cas pour Kerberos ; pire que AUTH_SYS

Niveau de sécurité	Sécurité	Performance
NFS - krb5i	• Le chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS — enveloppe l'UID/GID des utilisateurs/groupes dans les appels RPC dans l'encapsuleur GSS • L'utilisateur qui demande l'accès au montage doit disposer d'un ticket Kerberos valide (via nom d'utilisateur/mot de passe ou échange manuel par onglet) ; le ticket expire après une période spécifiée et l'utilisateur doit de nouveau s'authentifier pour l'accès • Aucun chiffrement pour les opérations NFS ou les protocoles annexes tels que mount/portmapper/nlm (peut voir les chemins d'exportation, les adresses IP, les pointeurs de fichiers, les autorisations, les noms de fichiers, atime/mtime dans les captures de paquets) • La somme de contrôle GSS Kerberos est ajoutée à chaque paquet pour garantir que rien n'intercepte les paquets. Si les checksums correspondent, la conversation est autorisée.	• Supérieur à krb5p parce que la charge NFS n'est pas chiffrée. Seule la surcharge supplémentaire par rapport à krb5 est la somme de contrôle d'intégrité. Les performances de krb5i ne seront pas beaucoup plus mauvais que krb5, mais il y aura une certaine dégradation.

Niveau de sécurité	Sécurité	Performance
NFS – krb5p	• Le chiffrement Kerberos pour les informations d'identification dans chaque paquet NFS — enveloppe l'UID/GID des utilisateurs/groupes dans les appels RPC dans l'encapsuleur GSS • L'utilisateur qui demande l'accès au montage doit disposer d'un ticket Kerberos valide (via nom d'utilisateur/mot de passe ou échange manuel de clavier) ; le ticket expire après la période spécifiée et l'utilisateur doit de nouveau s'authentifier pour l'accès • Tous les payload de paquets NFS sont cryptés avec l'encapsuleur GSS (ne peut pas voir les descripteurs de fichier, les autorisations, les noms de fichier, atime/mtime dans les captures de paquets). • Inclut le contrôle d'intégrité. • Le type d'opération NFS est visible (FSINFO, ACCESS, GETATTR, etc.). • Les protocoles auxiliaires (montage, portmap, nlm, etc.) ne sont pas cryptés (voir chemins d'exportation, adresses IP)	• Performances les plus faibles des niveaux de sécurité ; la krb5p doit chiffrer/décrypter plus. • Performances supérieures à celles du krb5p avec NFSv4.x pour les workloads avec un nombre élevé de fichiers.

Dans Cloud Volumes Service, un serveur Active Directory configuré est utilisé comme serveur Kerberos et serveur LDAP (pour rechercher les identités d'utilisateur à partir d'un schéma compatible RFC2307). Aucun autre serveur Kerberos ou LDAP n'est pris en charge. NetApp vous recommande vivement d'utiliser le protocole LDAP pour la gestion des identités dans Cloud Volumes Service. Pour plus d'informations sur la manière dont NFS Kerberos est affiché dans les captures de paquets, reportez-vous à la section « considérations relatives à la détection/trace de paquets ».

Chiffrement des données au repos

Tous les volumes Cloud Volumes Service sont chiffrés au repos à l'aide du chiffrement AES-256, qui signifie que toutes les données utilisateur écrites sur le support sont chiffrées et ne peuvent être déchiffrées qu'à l'aide d'une clé par volume.

- Pour CVS-SW, des clés générées par Google sont utilisées.
- Pour CVS-Performance, les clés par volume sont stockées dans un gestionnaire de clés intégré dans

Cloud Volumes Service.

Depuis novembre 2021, un aperçu des fonctionnalités de clés de chiffrement gérées par les clients (CMEK) a été disponible. Vous pouvez ainsi chiffrer les clés par volume avec une clé principale par projet et par région hébergée dans "Google Key Management Service (KMS)." LES KILOMÈTRES vous permettent d'associer des gestionnaires de clés externes.

Pour plus d'informations sur la configuration de KMS pour CVS-Performance, reportez-vous à la section "La configuration des clés de chiffrement gérées par le client".

Pare-feu

Cloud Volumes Service expose plusieurs ports TCP pour servir les partages NFS et SMB :

- "Ports requis pour l'accès NFS"
- "Ports requis pour l'accès SMB"

En outre, SMB, NFS avec LDAP, y compris Kerberos, et des configurations à double protocole requièrent l'accès à un domaine Windows Active Directory. Les connexions Active Directory doivent être de "configuré" par région. Les contrôleurs de domaine (DC) Active Directory sont identifiés à l'aide de "Découverte de data Center basée sur DNS" Utilisation des serveurs DNS spécifiés. Tous les DCS renvoyés sont utilisés. La liste des DCS admissibles peut être limitée en spécifiant un site Active Directory.

Cloud Volumes Service atteint son niveau avec les adresses IP de la plage CIDR allouée à l' `gcloud compute address` commande pendant "Intégration de la Cloud Volumes Service". Vous pouvez utiliser ce CIDR comme adresses source pour configurer les pare-feu entrants sur vos contrôleurs de domaine Active Directory.

Les contrôleurs de domaine Active Directory doivent "Exposer les ports aux rapports CIDR Cloud Volumes Service comme indiqué ici".

Protocoles NAS

Présentation des protocoles NAS

Les protocoles NAS incluent NFS (v3 et v4.1) et SMB/CIFS (2.x et 3.x). Ces protocoles sont la façon dont CVS permet un accès partagé aux données entre plusieurs clients NAS. Par ailleurs, Cloud Volumes Service permet d'accéder simultanément aux clients NFS et SMB/CIFS (double protocole) tout en respectant l'ensemble des paramètres d'identité et d'autorisation sur les fichiers et les dossiers des partages NAS. Pour préserver un niveau maximal de sécurité des transferts de données, Cloud Volumes Service prend en charge le chiffrement de protocole à la volée avec le chiffrement SMB et NFS Kerberos 5p.

Le double protocole est disponible avec CVS-Performance uniquement.

Notions de base sur les protocoles NAS

Les protocoles NAS permettent à plusieurs clients sur un réseau d'accéder aux mêmes données sur un système de stockage, notamment Cloud Volumes Service sur GCP. NFS

et SMB sont les protocoles NAS définis et fonctionnent sur une base client/serveur où Cloud Volumes Service fait office de serveur. Les clients envoient des demandes d'accès, de lecture et d'écriture au serveur, et le serveur est responsable de la coordination des mécanismes de verrouillage des fichiers, du stockage des autorisations et du traitement des demandes d'identité et d'authentification.

Par exemple, le processus général suivant est suivi si un client NAS souhaite créer un nouveau fichier dans un dossier.

1. Le client demande au serveur des informations sur le répertoire (autorisations, propriétaire, groupe, ID de fichier, espace disponible, et ainsi de suite) ; le serveur répond avec les informations si le client et l'utilisateur demandeur disposent des autorisations nécessaires sur le dossier parent.
2. Si les autorisations du répertoire autorisent l'accès, le client demande alors au serveur si le nom de fichier en cours de création existe déjà dans le système de fichiers. Si le nom de fichier est déjà utilisé, la création échoue. Si le nom de fichier n'existe pas, le serveur indique au client qu'il peut continuer.
3. Le client envoie un appel au serveur pour créer le fichier avec le descripteur de répertoire et le nom du fichier et définit l'accès et les heures modifiées. Le serveur émet un ID de fichier unique pour s'assurer qu'aucun autre fichier n'est créé avec le même ID de fichier.
4. Le client envoie un appel pour vérifier les attributs du fichier avant l'opération D'ÉCRITURE. Si les autorisations le permettent, le client écrit le nouveau fichier. Si le verrouillage est utilisé par le protocole/l'application, le client demande au serveur un verrouillage pour empêcher les autres clients d'accéder au fichier lorsqu'il est verrouillé afin d'éviter la corruption des données.

NFS

NFS est un protocole de système de fichiers distribué qui est une norme IETF ouverte définie dans la norme RFC (Request for Comments) qui permet à quiconque d'implémenter le protocole.

Les volumes de Cloud Volumes Service sont partagés avec les clients NFS en exportant un chemin accessible à un client ou à un ensemble de clients. Les autorisations de monter ces exportations sont définies par des règles et des règles d'exportation, qui peuvent être configurées par les administrateurs Cloud Volumes Service.

L'implémentation NFS de NetApp est considérée comme une norme Gold pour le protocole et elle est utilisée dans d'innombrables environnements NAS d'entreprise. Les sections suivantes présentent le protocole NFS ainsi que les fonctionnalités de sécurité spécifiques disponibles dans Cloud Volumes Service et leur mise en œuvre.

Utilisateurs et groupes UNIX locaux par défaut

Cloud Volumes Service contient plusieurs utilisateurs et groupes UNIX par défaut pour diverses fonctionnalités de base. Ces utilisateurs et ces groupes ne peuvent actuellement pas être modifiés ou supprimés. Actuellement, les nouveaux utilisateurs et groupes locaux ne peuvent pas être ajoutés à Cloud Volumes Service. Les utilisateurs et groupes UNIX hors des utilisateurs et des groupes par défaut doivent être fournis par un service de noms LDAP externe.

Le tableau suivant indique les utilisateurs et groupes par défaut et leurs ID numériques correspondants. NetApp recommande de ne pas créer de nouveaux utilisateurs ou groupes dans LDAP ou sur les clients locaux qui utilisent à nouveau ces ID numériques.

Utilisateurs par défaut : ID numériques	Groupes par défaut : ID numériques
• racine : 0 • pcuser:65534 • personne:65535	• racine : 0 • démon:1 • pcuser:65534 • personne:65535

Lors de l'utilisation de NFSv4.1, l'utilisateur root peut s'afficher comme personne lors de l'exécution des commandes de liste de répertoires sur les clients NFS. Ceci est dû à la configuration du mappage de domaine d'ID du client. Voir la section appelée NFSv4.1 et personne utilisateur/groupe pour plus de détails sur ce problème et sur la façon de le résoudre.

L'utilisateur root

Sous Linux, le compte racine a accès à toutes les commandes, fichiers et dossiers d'un système de fichiers Linux. En raison de la puissance de ce compte, les bonnes pratiques en matière de sécurité exigent souvent que l'utilisateur root soit désactivé ou restreint d'une façon ou d'une autre. Dans les exportations NFS, la puissance dont dispose un utilisateur root sur les fichiers et les dossiers peut être contrôlée dans Cloud Volumes Service au moyen de règles et de stratégies d'exportation et d'un concept appelé « squash racine ».

Le scaling racine garantit que l'utilisateur root accédant à un montage NFS est écrasé à l'utilisateur numérique anonyme 65534 (voir la section «L'utilisateur anonyme") et n'est actuellement disponible que lors de l'utilisation de CVS-Performance en sélectionnant Désactivé pour l'accès racine lors de la création de règles d'export. Si l'utilisateur root est écrasé par l'utilisateur anonyme, il n'a plus accès à exécuter CHown ou "commandes setuid/setgid (le bit collant)" Sur les fichiers ou dossiers du montage NFS, et les fichiers ou dossiers créés par l'utilisateur root affichent l'UID d'anon comme propriétaire/groupe. En outre, les ACL NFSv4 ne peuvent pas être modifiés par l'utilisateur root. Cependant, l'utilisateur root a toujours accès aux fichiers chmod et supprimés pour lesquels il n'a pas d'autorisations explicites. Si vous souhaitez limiter l'accès aux autorisations de fichier et de dossier d'un utilisateur root, envisagez d'utiliser un volume avec des listes de contrôle d'accès NTFS, créant un utilisateur Windows nommé `root`, et application des autorisations souhaitées aux fichiers ou dossiers.

L'utilisateur anonyme

L'ID utilisateur anonyme (anon) spécifie un ID utilisateur UNIX ou un nom d'utilisateur qui est mappé aux requêtes client qui arrivent sans identifiants NFS valides. Cela peut inclure l'utilisateur racine lorsque le squaing racine est utilisé. L'utilisateur d'anon dans Cloud Volumes Service est 65534.

Cet UID est normalement associé au nom d'utilisateur `nobody` ou `nfsnobody` Dans les environnements Linux. Cloud Volumes Service utilise également 65534 comme pcuser UNIX local (voir la section «Utilisateurs et groupes UNIX locaux par défaut"), qui est également l'utilisateur de secours par défaut pour les mappages de noms Windows à UNIX lorsqu'aucun utilisateur UNIX correspondant valide n'est trouvé dans LDAP.

En raison des différences entre les noms d'utilisateur Linux et Cloud Volumes Service pour UID 65534, la chaîne de nom des utilisateurs mappés sur 65534 risque de ne pas correspondre lors de l'utilisation de NFSv4.1. Vous pouvez donc voir `nobody` en tant qu'utilisateur sur certains fichiers et dossiers. Voir la section «NFSv4.1 et personne utilisateur/groupe" pour plus d'informations sur ce problème et sur la façon de le résoudre.

Contrôle d'accès/exportations

L'accès initial aux exportations/partages pour les montages NFS est contrôlé par le biais de règles d'export policy basées sur les hôtes, figurant dans une export policy. Une adresse IP hôte, un nom d'hôte, un sous-réseau, un groupe réseau ou un domaine sont définis pour permettre l'accès au montage du partage NFS et le niveau d'accès autorisé à l'hôte. Les options de configuration des règles d'export-policy dépendent du niveau Cloud Volumes Service.

Pour CVS-SW, les options suivantes sont disponibles pour la configuration des export-policy :

- **Correspondance client.** liste d'adresses IP séparées par des virgules, liste de noms d'hôte séparés par des virgules, sous-réseaux, groupes réseau, noms de domaine.
- **Règles d'accès RO/RW.** sélectionnez lecture/écriture ou lecture seule pour contrôler le niveau d'accès à l'exportation.CVS-Performance fournit les options suivantes :
- **Correspondance client.** liste d'adresses IP séparées par des virgules, liste de noms d'hôte séparés par des virgules, sous-réseaux, groupes réseau, noms de domaine.
- **Règles d'accès RO/RW.** sélectionnez lecture/écriture ou lecture seulement pour contrôler le niveau d'accès à l'exportation.
- **Accès racine (activé/désactivé).** configure le squash racine (voir la section «L'utilisateur root« pour plus de détails).
- **Type de protocole.** cette option limite l'accès au montage NFS à une version de protocole spécifique. Lorsque vous spécifiez à la fois NFS v3 et NFS v4.1 pour le volume, laissez les deux vides ou cochez les deux cases.
- **Niveau de sécurité Kerberos (lorsque l'option Activer Kerberos est sélectionnée).** fournit les options de krb5, krb5i et/ou krb5p pour l'accès en lecture seule ou en lecture/écriture.

Changer la propriété (chown) et le groupe de changement (chgrp)

NFS sur Cloud Volumes Service ne permet à l'utilisateur root d'exécuter chown/chgrp que sur des fichiers et des dossiers. Les autres utilisateurs voient un `Operation not permitted` erreur : même sur les fichiers qu'ils possèdent. Si vous utilisez du squash racine (comme décrit dans la section «L'utilisateur root"), la racine est écrasée à un utilisateur non root et ne peut pas accéder à chown et chgrp. Il n'existe actuellement aucune solution de contournement dans Cloud Volumes Service pour permettre aux chown et aux chgrp de non-root utilisateurs. Si des modifications de propriété sont requises, envisagez d'utiliser des volumes à double protocole et définissez le style de sécurité sur NTFS pour contrôler les autorisations du côté Windows.

Gestion des autorisations

Cloud Volumes Service prend en charge les deux bits de mode (par exemple 644, 777, etc. Pour rwx) et les ACL NFSv4.1 pour contrôler les autorisations sur les clients NFS pour les volumes qui utilisent le style de sécurité UNIX. La gestion des autorisations standard est utilisée pour ces clients (tels que chmod, chown ou nfs4_setfacl) et avec n'importe quel client Linux qui les prend en charge.

En outre, lorsque des volumes à double protocole sont définis sur NTFS, les clients NFS peuvent tirer parti du mappage de noms Cloud Volumes Service aux utilisateurs Windows, qui sont ensuite utilisés pour résoudre les autorisations NTFS. Pour ce faire, une connexion LDAP à Cloud Volumes Service doit fournir des traductions d'ID numérique vers nom d'utilisateur car Cloud Volumes Service nécessite un nom d'utilisateur UNIX valide pour être correctement mappé à un nom d'utilisateur Windows.

Fournissant des listes de contrôle d'accès granulaires pour NFSv3

Les autorisations bits du mode couvrent uniquement le propriétaire, le groupe et tous les autres éléments de la

sémantique, ce qui signifie qu'aucun contrôle granulaire des accès utilisateur n'est mis en place pour les données NFSv3 de base. Cloud Volumes Service ne prend pas en charge les listes de contrôle d'accès POSIX, ni les attributs étendus (tels que chattr). Les listes de contrôle d'accès granulaires ne sont donc possibles que dans les scénarios suivants avec NFSv3 :

- Volumes de style de sécurité NTFS (serveur CIFS requis) avec des mappages utilisateur UNIX vers Windows valides.
- NFS v4.1 a été appliqué à l'aide d'un client admin montage NFSv4.1 pour appliquer les ACL.

Ces deux méthodes nécessitent une connexion LDAP pour la gestion des identités UNIX et des informations utilisateur et groupe UNIX valides (voir la section "« LDAP »") Et ne sont disponibles qu'avec des instances CVS-Performance. Pour utiliser des volumes de style de sécurité NTFS avec le protocole NFS, vous devez utiliser le protocole double (SMB et NFS v3) ou le double protocole (SMB et NFS v4.1), même si aucune connexion SMB n'est établie. Pour utiliser les listes de contrôle d'accès NFSv4.1 avec montages NFSv3, vous devez sélectionner `Both (NFSv3/NFSv4.1)` comme type de protocole.

Les bits standard en mode UNIX ne fournissent pas le même niveau de granularité dans les autorisations que les ACL NTFS ou NFSv4.x fournissent. Le tableau suivant compare la granularité des autorisations entre les bits en mode NFS v3 et les ACL NFSv4.1. Pour plus d'informations sur les listes de contrôle d'accès NFSv4.1, voir "Nfs4_acl - listes de contrôle d'accès NFSv4".

Bits de mode NFSv3	Listes de contrôle d'accès NFSv4.1
• Définir l'ID utilisateur lors de l'exécution • Définir l'ID du groupe lors de l'exécution • Enregistrer le texte échangé (non défini dans POSIX) • Autorisation de lecture du propriétaire • Autorisation d'écriture pour le propriétaire • Exécutez l'autorisation de propriétaire sur un fichier ou recherchez (recherchez) l'autorisation de propriétaire dans le répertoire • Autorisation de lecture pour le groupe • Autorisation d'écriture pour le groupe • Exécutez l'autorisation de groupe sur un fichier ou recherchez (recherchez) l'autorisation de groupe dans le répertoire • Autorisation de lecture pour les autres utilisateurs • Autorisation d'écriture pour les autres • Exécutez l'autorisation pour les autres utilisateurs d'un fichier ou recherchez (recherchez) l'autorisation pour d'autres personnes dans le répertoire	Types d'entrée de contrôle d'accès (ACE) (Allow/Deny/Audit) * indicateurs d'héritage * Directory-Hériter * fichier-Hériter * no-Propagate-Hériter * hériter-only Autorisations * lecture-données (fichiers) / répertoire-liste (répertoires) * écriture-données (fichiers) / création-fichier (répertoires) * ajout-données (fichiers) / création-sous-répertoire (répertoires) * exécution (fichiers) / changement-répertoire (répertoires) * suppression * suppression-enfant * lecture-attributs * écriture-attributs * liste de contrôle d'accès * lecture-écriture * liste de contrôle d'accès *

Enfin, l'appartenance au groupe NFS (dans NFSv3 et NFSV4.x) est limitée à un maximum par défaut de 16 pour AUTH_SYS selon les limites de paquets RPC. NFS Kerberos fournit jusqu'à 32 groupes et les ACL NFSv4 suppriment la limite par le biais de listes de contrôle d'accès granulaires des utilisateurs et des groupes (jusqu'à 1024 entrées par ACE).

En outre, Cloud Volumes Service offre une prise en charge étendue des groupes pour étendre le nombre maximal de groupes pris en charge jusqu'à 32. Pour ce faire, une connexion LDAP à un serveur LDAP qui contient des identités d'utilisateur et de groupe UNIX valides est nécessaire. Pour plus d'informations sur cette configuration, reportez-vous à la section "Création et gestion des volumes NFS" Dans la documentation Google.

ID d'utilisateur et de groupe NFSv3

Les ID utilisateur et groupe NFSv3 sont répartis sur le fil sous forme d'ID numériques plutôt que de noms. Cloud Volumes Service ne résout pas le nom d'utilisateur de ces ID numériques avec NFSv3, avec des volumes de style de sécurité UNIX utilisant des bits de mode uniquement. Lorsque des listes de contrôle d'accès NFSv4.1 sont présentes, une recherche d'ID numérique et/ou une recherche de chaîne de nom est nécessaire pour résoudre correctement la liste de contrôle d'accès, même en cas d'utilisation de NFS v3. Avec les volumes de style de sécurité NTFS, Cloud Volumes Service doit résoudre un ID numérique à un utilisateur UNIX valide, puis le mapper à un utilisateur Windows valide pour négocier les droits d'accès.

Limitations de sécurité des ID d'utilisateur et de groupe NFSv3

Avec NFSv3, le client et le serveur n'ont jamais à confirmer que l'utilisateur qui tente de lire ou d'écrire avec un ID numérique est un utilisateur valide ; il est simplement implicitement approuvé. Cela ouvre le système de fichiers jusqu'à des failles potentielles simplement en usurper n'importe quel ID numérique. Pour éviter les trous de sécurité de ce type, il existe quelques options pour Cloud Volumes Service.

- L'implémentation de Kerberos pour NFS oblige les utilisateurs à s'authentifier avec un nom d'utilisateur et un mot de passe ou un fichier keytab afin d'obtenir un ticket Kerberos pour autoriser l'accès à un montage. Kerberos est disponible avec des instances CVS-Performance et uniquement avec NFSv4.1.
- En limitant la liste des hôtes des règles d'export policy, les clients NFSv3 disposent d'un accès au volume Cloud Volumes Service.
- L'utilisation de volumes à double protocole et l'application de listes de contrôle d'accès NTFS au volume oblige les clients NFSv3 à résoudre des ID numériques à des noms d'utilisateur UNIX valides afin de s'authentifier correctement pour accéder aux montages. Pour cela, il est nécessaire d'activer LDAP et de configurer les identités d'utilisateur et de groupe UNIX.
- L'affaissement de l'utilisateur root limite les dommages qu'un utilisateur root peut faire sur un montage NFS, mais ne élimine pas complètement les risques. Pour plus d'informations, reportez-vous à la section «L'utilisateur root. »

En fin de compte, la sécurité NFS est limitée à la version de protocole que vous utilisez. NFS v3, bien que plus performant que NFSv4.1, n'offre pas le même niveau de sécurité.

NFSv4.1

NFSv4.1 offre une sécurité et une fiabilité supérieures par rapport à NFS v3, pour les raisons suivantes :

- Verrouillage intégré grâce à un mécanisme de location
- Sessions avec état
- Toutes les fonctionnalités NFS sur un seul port (2049)
- TCP uniquement
- Mappage du domaine d'ID
- Intégration Kerberos (NFSv3 peut utiliser Kerberos, mais uniquement pour NFS, pas pour les protocoles auxiliaires tels que NLM)

Dépendances NFSv4.1

En raison des fonctions de sécurité ajoutées dans NFSv4.1, certaines dépendances externes étaient impliquées dans l'utilisation de NFSv3 (semblable au mode d'utilisation requis par SMB, comme Active Directory).

Listes de contrôle d'accès NFSv4.1

Cloud Volumes Service prend en charge les listes de contrôle d'accès NFSv4.x, qui offrent des avantages distincts par rapport aux autorisations de style POSIX standard, notamment :

- Contrôle granulaire de l'accès des utilisateurs aux fichiers et aux répertoires
- Sécurité NFS renforcée
- Interopérabilité améliorée avec CIFS/SMB
- Suppression de la limitation NFS de 16 groupes par utilisateur avec sécurité AUTH_SYS
- Les ACL contournent le besoin en résolution d'ID de groupe (GID), qui supprime efficacement les ACL limitésNFS sont contrôlées par les clients NFS, et non par Cloud Volumes Service. Pour utiliser les listes de contrôle d'accès NFS NFSv4.1, assurez-vous que la version logicielle de votre client les prend en charge et que les utilitaires NFS appropriés sont installés.

Compatibilité entre les listes de contrôle d'accès NFSv4.1 et les clients SMB

Les ACL NFSv4 ne sont pas plus les ACL de niveau fichier (ACL NTFS) de Windows, mais possèdent une fonctionnalité similaire. Cependant, dans les environnements NAS multiprotocoles, si vous disposez de listes de contrôle d'accès NFSv4.1 et que vous utilisez un accès double protocole (NFS et SMB sur les mêmes datasets), les clients qui utilisent SMB2.0 et versions ultérieures ne pourront pas afficher ni gérer les listes de contrôle d'accès à partir des onglets de sécurité Windows.

Fonctionnement des listes de contrôle d'accès NFSv4.1

Pour référence, les termes suivants sont définis :

- **Liste de contrôle d'accès (ACL).** liste des entrées d'autorisations.
- **Entrée de contrôle d'accès (ACE).** Entrée d'autorisation dans la liste.

Lorsqu'un client définit une liste de contrôle d'accès NFSv4.1 sur un fichier lors d'une opération SETATTR, Cloud Volumes Service définit cette liste de contrôle d'accès sur l'objet en remplaçant toute liste de contrôle d'accès existante. S'il n'y a pas de liste de contrôle d'accès sur un fichier, les autorisations de mode sur ce fichier sont calculées à partir DE OWNER@, GROUP@ et EVERYONE@. S'il existe des SUID/SGID/bits COLLANTS sur le fichier, ils ne sont pas affectés.

Lorsqu'un client obtient une liste de contrôle d'accès NFS (ACL) NFSv4.1 sur un fichier au cours d'une opération GETATTR, Cloud Volumes Service lit la liste de contrôle d'accès NFS (ACL) associée à l'objet, construit une liste d'ACE et renvoie la liste au client. Si le fichier possède une liste de contrôle d'accès NT ou des bits de mode, une liste de contrôle d'accès est construite à partir de bits de mode et renvoyée au client.

L'accès est refusé si une ACE DE REFUS est présente dans la liste de contrôle d'accès ; l'accès est accordé si une ACE D'AUTORISATION existe. Toutefois, l'accès est également refusé si aucun des ACE n'est présent dans l'ACL.

Un descripteur de sécurité se compose d'une liste de contrôle d'accès (SACL) et d'une liste de contrôle d'accès discrétionnaire (DACL). Lorsque NFSv4.1 interagit avec CIFS/SMB, le DACL est mappé à NFSv4 et CIFS. La DACL se compose des ACCE AUTORISER et REFUSER.

Si un niveau de base `chmod` Est exécuté sur un fichier ou un dossier avec les ACL NFSv4.1 définies, les listes de contrôle d'accès utilisateur et groupe existantes sont conservées, mais le PROPRIÉTAIRE par défaut@, GROUPE@, EVERYONE@ ACL sont modifiés.

Un client utilisant des listes de contrôle d'accès NFSv4.1 peut définir et afficher des listes de contrôle d'accès pour les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire comportant une liste de contrôle d'accès, cet objet hérite de tous les ACE de la liste de contrôle d'accès qui ont été marqués avec le nom approprié "indicateurs d'héritage".

Si un fichier ou un répertoire possède une liste de contrôle d'accès NFSv4.1, cette liste de contrôle d'accès est utilisée pour contrôler l'accès, quel que soit le protocole utilisé pour accéder au fichier ou au répertoire.

Les fichiers et les répertoires héritent des ACE des listes de contrôle d'accès NFSv4 sur les répertoires parents (éventuellement avec les modifications appropriées) tant que les ACE ont été balisés avec les indicateurs d'héritage corrects.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une requête NFSv4, la liste de contrôle d'accès du fichier ou répertoire résultant dépend du fait que la demande de création de fichier inclut une liste de contrôle d'accès ou uniquement les autorisations d'accès aux fichiers UNIX standard. La liste de contrôle d'accès dépend également de la présence ou non d'une liste de contrôle d'accès dans le répertoire parent.

- Si la requête inclut une liste de contrôle d'accès, cette liste de contrôle d'accès est utilisée.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent ne dispose pas d'ACL, le mode fichier client est utilisé pour définir les autorisations d'accès aux fichiers UNIX standard.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent dispose d'une liste de contrôle d'accès non héritable, une liste de contrôle d'accès par défaut basée sur les bits de mode transmis à la requête est définie sur le nouvel objet.
- Si la demande comprend uniquement des autorisations d'accès aux fichiers UNIX standard mais que le répertoire parent possède une ACL, les ACE de l'ACL du répertoire parent sont hérités par le nouveau fichier ou répertoire tant que les ACE ont été balisés avec les indicateurs d'héritage appropriés.

Autorisations ACE

Les autorisations de listes de contrôle d'accès NFSv4.1 utilisent une série de valeurs de lettres majuscules et minuscules (par exemple `rxtncy`) pour contrôler l'accès. Pour plus d'informations sur ces valeurs de lettre, reportez-vous à la section "COMMENT : utiliser NFSv4 ACL".

Comportement ACL NFSv4.1 avec umask et héritage ACL

"Les ACL NFSv4 permettent d'offrir l'héritage ACL". L'héritage ACL signifie que les fichiers ou les dossiers créés sous des objets avec des listes de contrôle d'accès NFSv4.1 peuvent hériter des listes de contrôle d'accès basées sur la configuration du "Indicateur d'héritage ACL".

"Umask" permet de contrôler le niveau d'autorisation auquel les fichiers et dossiers sont créés dans un répertoire sans interaction avec l'administrateur. Par défaut, Cloud Volumes Service permet à umask de remplacer les listes de contrôle d'accès héritées, ce qui est le comportement attendu selon "RFC 5661".

Formatage ACL

Les ACL NFSv4.1 ont un formatage spécifique. L'exemple suivant est un ensemble ACE sur un fichier :

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

L'exemple précédent suit les directives de format ACL de :

```
type:flags:principal:permissions
```

Un type de `A` signifie « autoriser ». Les indicateurs hériter ne sont pas définis dans ce cas, car le principal n'est pas un groupe et n'inclut pas l'héritage. De plus, comme l'ACE n'est pas une entrée D'AUDIT, il n'est pas nécessaire de définir les indicateurs d'audit. Pour plus d'informations sur les listes de contrôle d'accès NFSv4.1, voir "http://linux.die.net/man/5/nfs4_acl".

Si la liste de contrôle d'accès NFSv4.1 n'est pas définie correctement (ou si une chaîne de nom ne peut pas être résolue par le client et le serveur), la liste de contrôle d'accès peut ne pas se comporter comme prévu, ou si la modification de la liste de contrôle d'accès échoue à s'appliquer et générer une erreur.

Les exemples d'erreurs sont les suivants :

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

REFUS explicite

Les autorisations NFSv4.1 peuvent inclure des attributs DE REFUS explicites pour LE PROPRIÉTAIRE, LE GROUPE et TOUT LE MONDE. En effet, les listes de contrôle d'accès NFSv4.1 étant des listes de contrôle d'accès par défaut, ce qui signifie que si une liste de contrôle d'accès n'est pas explicitement accordée par une ACE, elle est alors refusée. Les attributs DE REFUS explicite remplacent les ACE D'ACCÈS, explicites ou non.

LES ACE DE REFUS sont définis avec une balise d'attribut de `D`.

Dans l'exemple ci-dessous, GROUP@ est autorisé à toutes les autorisations de lecture et d'exécution, mais a refusé tout accès en écriture.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DANS la mesure du possible, LES ACE DE REFUS doivent être évités parce qu'ils peuvent être confus et compliqués ; AUTORISER les listes de contrôle d'accès qui ne sont pas explicitement définies sont refusées implicitement. Lorsque LES ACE DE REFUS sont définis, les utilisateurs peuvent se voir refuser l'accès lorsqu'ils s'attendent à bénéficier de l'accès.

L'ensemble précédent d'ACE est équivalent à 755 bits de mode, ce qui signifie :

- Le propriétaire a tous les droits.
- Les groupes ont lecture seule.
- D'autres ont lecture seule.

Cependant, même si les autorisations sont ajustées à l'équivalent 775, l'accès peut être refusé en raison du REFUS explicite défini sur TOUT LE MONDE.

Dépendances de mappage de domaine ID NFSv4.1

NFSv4.1 s'appuie sur la logique de mappage de domaine d'ID en tant que couche de sécurité pour garantir qu'un utilisateur qui tente d'accéder à un montage NFSv4.1 est en effet celui qu'il prétend être. Dans ce cas, le nom d'utilisateur et le nom de groupe provenant du client NFSv4.1 ajoute une chaîne de nom et l'envoie à l'instance Cloud Volumes Service. Si cette combinaison nom d'utilisateur/groupe et chaîne ID ne correspond pas, alors l'utilisateur et/ou le groupe est écrasé par défaut, aucun utilisateur spécifié dans le `/etc/idmapd.conf` fichier sur le client.

Cette chaîne d'ID est une exigence pour le respect correct des autorisations, en particulier lorsque des ACL NFSv4.1 et/ou Kerberos sont utilisés. Par conséquent, des dépendances au niveau du serveur de service de noms, telles que les serveurs LDAP, sont nécessaires pour assurer la cohérence entre les clients et Cloud Volumes Service afin de permettre une résolution appropriée de l'identité des noms d'utilisateur et de groupe.

Cloud Volumes Service utilise une valeur de nom de domaine d'ID par défaut statique de `defaultv4iddomain.com`. Les clients NFS utilisent par défaut le nom de domaine DNS pour ses paramètres de nom de domaine ID, mais vous pouvez régler manuellement le nom de domaine ID dans `/etc/idmapd.conf`.

Si le protocole LDAP est activé dans Cloud Volumes Service, Cloud Volumes Service automatise le domaine d'ID NFS pour modifier ce qui est configuré pour le domaine de recherche dans DNS et les clients n'ont pas besoin d'être modifiés à moins qu'ils n'utilisent des noms de recherche de domaine DNS différents.

Lorsque Cloud Volumes Service peut résoudre un nom d'utilisateur ou un nom de groupe dans les fichiers locaux ou LDAP, la chaîne de domaine est utilisée et les ID de domaine ne sont pas identiques. Si Cloud Volumes Service ne parvient pas à trouver un nom d'utilisateur ou un nom de groupe dans les fichiers locaux ou LDAP, la valeur d'ID numérique est utilisée et le client NFS résout correctement le nom (ceci est similaire au comportement NFSv3).

Sans modifier le domaine d'ID NFSv4.1 du client pour correspondre à l'utilisation du volume Cloud Volumes Service, le comportement suivant s'affiche :

- Les utilisateurs et groupes UNIX avec des entrées locales dans Cloud Volumes Service (comme root, comme défini dans les utilisateurs et groupes UNIX locaux) sont écrasés sur la valeur personne.
- Les utilisateurs et groupes UNIX dont les entrées sont dans LDAP (si Cloud Volumes Service est configuré pour utiliser LDAP) ne s'acclaent à personne si les domaines DNS sont différents entre les clients NFS et Cloud Volumes Service.
- Les utilisateurs et groupes UNIX sans entrées locales ou LDAP utilisent la valeur d'ID numérique et résolvez le nom spécifié sur le client NFS. Si aucun nom n'existe sur le client, seul l'ID numérique est affiché.

Voici les résultats du scénario précédent :

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Lorsque les domaines d'ID client et serveur correspondent, voici l'apparence de la même liste de fichiers :

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Pour plus d'informations sur ce problème et sur la façon de le résoudre, reportez-vous à la section «NFSv4.1 et personne utilisateur/groupe. »

Les dépendances Kerberos

Si vous prévoyez d'utiliser Kerberos avec NFS, vous devez disposer des éléments suivants en Cloud Volumes Service :

- Domaine Active Directory pour les services du centre de distribution Kerberos (KDC)
- Domaine Active Directory avec des attributs utilisateur et groupe renseignés avec des informations UNIX pour la fonctionnalité LDAP (le protocole Kerberos NFS dans Cloud Volumes Service requiert un mappage utilisateur SPN vers UNIX pour assurer le bon fonctionnement du système).
- LDAP activée sur l'instance Cloud Volumes Service
- Domaine Active Directory pour les services DNS

NFSv4.1 et personne utilisateur/groupe

L'un des problèmes les plus courants rencontrés avec une configuration NFSv4.1 est lorsqu'un fichier ou un dossier est affiché dans une liste à l'aide de `ls` appartenant au `user:group` combinaison de `nobody:nobody`.

Par exemple :

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

Et l'ID numérique est `99`.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

Dans certains cas, le fichier peut indiquer le propriétaire correct, mais `nobody` en tant que groupe.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Qui n'est personne?

Le `nobody` L'utilisateur dans NFSv4.1 est différent de `nfsnobody` utilisateur. Vous pouvez afficher la manière dont un client NFS voit chaque utilisateur en exécutant le `id` commande :

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Avec NFSv4.1, le `nobody` l'utilisateur est l'utilisateur par défaut défini par le `idmapd.conf` et peut être défini comme n'importe quel utilisateur que vous voulez utiliser.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Pourquoi cela se produit-il ?

Étant donné que la sécurité par mappage de chaînes de noms est un principe clé des opérations NFSv4.1, le comportement par défaut lorsqu'une chaîne de noms ne correspond pas correctement est de court-courser cet utilisateur à un utilisateur qui n'aura normalement pas accès aux fichiers et dossiers appartenant aux utilisateurs et aux groupes.

Lorsque vous voyez `nobody` Pour l'utilisateur et/ou le groupe dans les listes de fichiers, cela signifie généralement que quelque chose dans NFSv4.1 est mal configuré. La sensibilité de la casse peut être ici en jeu.

Par exemple, si utilisateur1@CVSDEMO.LOmabL (uid 1234, gid 1234) accède à une exportation, alors Cloud Volumes Service doit pouvoir trouver utilisateur1@CVSDEMO.LOMOL (uid 1234, gid 1234). Si l'utilisateur dans Cloud Volumes Service est USER1@CVSDEMO.LOmabmacop, il ne correspond pas (majuscules UTILISATEUR1 contre minuscules utilisateur1). Dans de nombreux cas, vous pouvez voir ce qui suit dans le fichier de messages sur le client :

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Le client et le serveur doivent tous deux convenir qu'un utilisateur est effectivement celui qu'il prétend être. Vous devez donc vérifier les éléments suivants pour vous assurer que l'utilisateur que le client voit dispose des mêmes informations que l'utilisateur que celui que Cloud Volumes Service voit.

- **Domaine ID NFSv4.x.** client : `idmapd.conf` Fichier ; utilisations de Cloud Volumes Service `defaultv4iddomain.com` et ne peut pas être modifié manuellement. En cas d'utilisation de LDAP avec NFSv4.1, Cloud Volumes Service modifie le domaine d'ID en fonction de ce que le domaine de recherche DNS utilise, ce qui est le même que le domaine AD.
- **Nom d'utilisateur et ID numériques.** Ceci détermine l'endroit où le client recherche des noms d'utilisateur et utilise la configuration du commutateur de service de nom—client: `nsswitch.conf` Et/ou fichiers de passwd et de groupe locaux ; Cloud Volumes Service n'autorise pas les modifications à ceci mais ajoute automatiquement LDAP à la configuration lorsqu'elle est activée.
- **Nom de groupe et ID numériques.** cette option détermine où le client recherche des noms de groupe et utilise la configuration du commutateur de service de nom—client : `nsswitch.conf` Et/ou fichiers de passwd et de groupe locaux ; Cloud Volumes Service n'autorise pas les modifications à ceci mais ajoute automatiquement LDAP à la configuration lorsqu'elle est activée.

Dans presque tous les cas, si vous voyez `nobody` Dans les listes d'utilisateurs et de groupes des clients, le problème est la traduction de l'ID de domaine de nom d'utilisateur ou de groupe entre Cloud Volumes Service et le client NFS. Pour éviter ce scénario, utilisez LDAP pour résoudre les informations d'utilisateur et de groupe entre les clients et Cloud Volumes Service.

Affichage des chaînes d'ID de nom pour NFSv4.1 sur les clients

Si vous utilisez NFSv4.1, un mappage de chaîne de nom a lieu lors des opérations NFS, comme décrit précédemment.

En plus de l'utilisation `/var/log/messages` Pour trouver un problème avec les ID NFSv4, vous pouvez utiliser le "nfsidmap -l" Commande sur le client NFS pour afficher les noms d'utilisateur qui sont correctement mappés au domaine NFSv4.

Par exemple, ceci est la sortie de la commande après un utilisateur qui peut être trouvé par le client et que Cloud Volumes Service accède à un montage NFSv4.x :

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Lorsqu'un utilisateur qui ne se mappe pas correctement dans le domaine ID NFSv4.1 (dans ce cas, `netapp-user`) essaie d'accéder au même montage et touche un fichier, ils sont affectés `nobody:nobody`, comme

prévu.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

Le `nfsidmap -l` la sortie affiche l'utilisateur `pcuser` à l'écran, mais pas `netapp-user`; il s'agit de l'utilisateur anonyme dans notre règle d'export-policy (`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

PME

"PME" Est un protocole de partage de fichiers réseau développé par Microsoft qui fournit une authentification utilisateur/groupe centralisée, des autorisations, un verrouillage et un partage de fichiers à plusieurs clients SMB sur un réseau Ethernet. Les fichiers et les dossiers sont présentés aux clients par le biais de partages, qui peuvent être configurés avec diverses propriétés de partage et offre un contrôle d'accès par le biais d'autorisations de niveau partage. SMB peut être présenté à n'importe quel client prenant en charge le protocole, y compris les clients Windows, Apple et Linux.

Cloud Volumes Service prend en charge les versions SMB 2.1 et 3.x du protocole.

Contrôle d'accès/partages SMB

- Lorsqu'un nom d'utilisateur Windows demande l'accès au volume Cloud Volumes Service, Cloud Volumes Service recherche un nom d'utilisateur UNIX en utilisant les méthodes configurées par les administrateurs Cloud Volumes Service.

- Si un fournisseur d'identités UNIX externe (LDAP) est configuré et que les noms d'utilisateur Windows/UNIX sont identiques, les noms d'utilisateur Windows mappent les noms d'utilisateur 1:1 vers UNIX sans configuration supplémentaire. Lorsque LDAP est activée, Active Directory est utilisé pour héberger ces attributs UNIX pour les objets utilisateur et groupe.
- Si les noms Windows et UNIX ne correspondent pas de la même manière, LDAP doit être configurée pour permettre à Cloud Volumes Service d'utiliser la configuration du mappage de noms LDAP (voir la section ""Utilisation du protocole LDAP pour le mappage de noms asymétrique"").
- Si LDAP n'est pas utilisé, les utilisateurs Windows SMB mappent un utilisateur UNIX local par défaut nommé `pcuser` À Cloud Volumes Service. Cela signifie que les fichiers écrits dans Windows par les utilisateurs qui font correspondre à `pcuser` Afficher la propriété UNIX sous `pcuser` Dans des environnements NAS multiprotocoles. `pcuser` voici le `nobody` Utilisateur dans les environnements Linux (UID 65534).

Dans les déploiements avec SMB uniquement, le `pcuser` Le mappage a toujours lieu, mais cela n'a aucune importance, car la propriété des utilisateurs et des groupes Windows est correctement affichée et l'accès NFS au volume SMB uniquement n'est pas autorisé. De plus, les volumes SMB uniquement ne prennent pas en charge la conversion en volumes NFS ou à double protocole après leur création.

Windows utilise Kerberos pour l'authentification par nom d'utilisateur avec les contrôleurs de domaine Active Directory, qui nécessitent un échange nom d'utilisateur/mot de passe avec les DCS AD, qui est externe à l'instance Cloud Volumes Service. L'authentification Kerberos est utilisée lors de l'utilisation de `\\SERVERNAME` Le chemin UNC est utilisé par les clients SMB et le suivant est vrai :

- L'entrée DNS A/AAAA existe pour NOM_SERVEUR
- Un code SPN valide pour l'accès SMB/CIFS existe pour NOM DE SERVEUR

Lorsqu'un volume SMB Cloud Volumes Service est créé, le nom du compte machine est créé comme défini dans la section "« Comment Cloud Volumes Service s'affiche dans Active Directory. »" Ce nom de compte machine devient également le chemin d'accès au partage SMB car Cloud Volumes Service utilise le DNS dynamique (DDNS) pour créer les entrées A/AAAA et PTR nécessaires dans le DNS et les entrées SPN nécessaires sur le principal du compte machine.

> Pour que les entrées PTR soient créées, la zone de recherche inversée de l'adresse IP de l'instance Cloud Volumes Service doit exister sur le serveur DNS.

Par exemple, ce volume Cloud Volumes Service utilise le chemin de partage UNC suivant : `\\cvs-east-433d.cvsdemo.local`.

Dans Active Directory, il s'agit des entrées SPN générées par le service Cloud volumes :

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Il s'agit du résultat de recherche DNS avant/arrière :

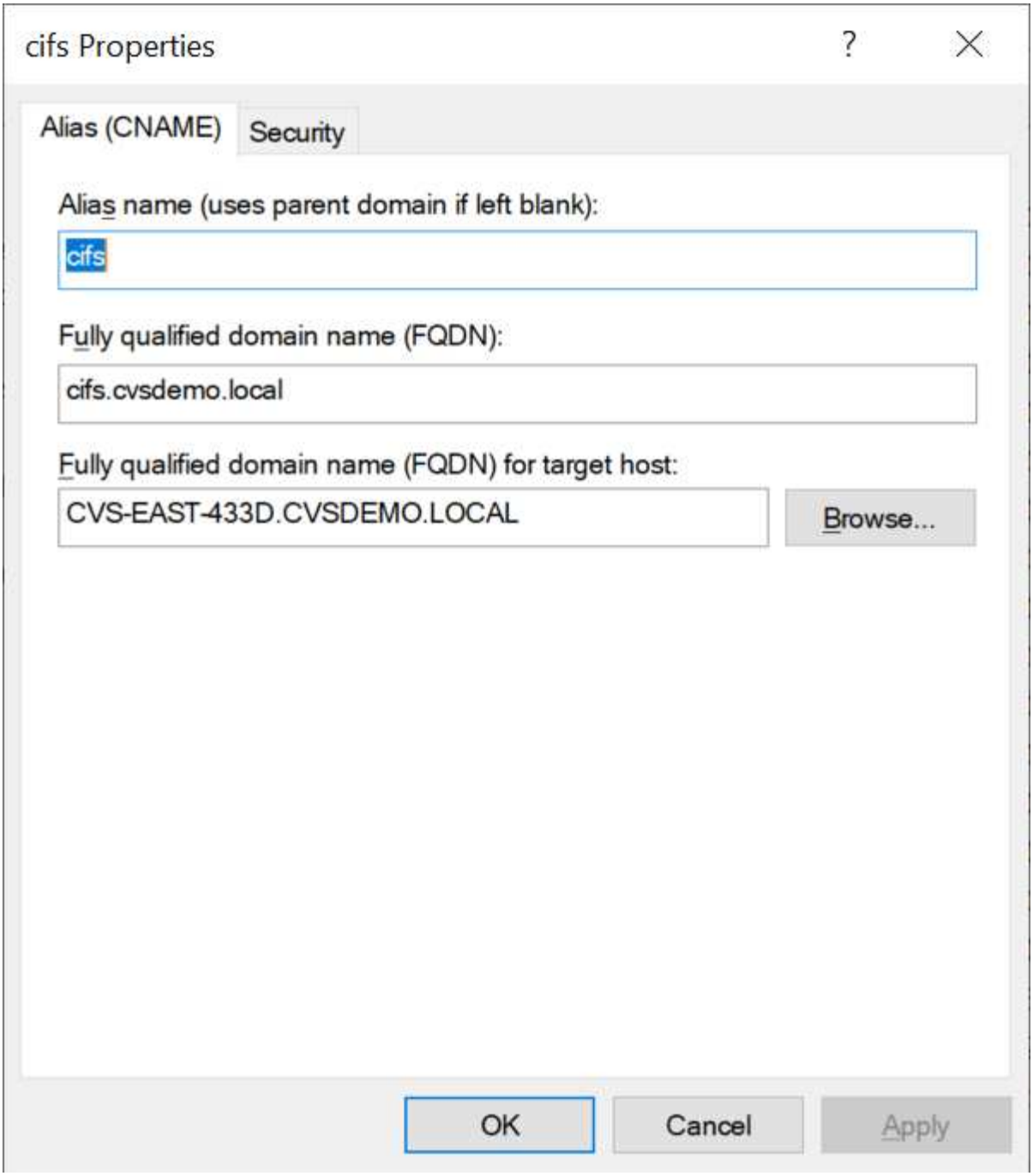
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Par ailleurs, un contrôle d'accès plus important peut être appliqué en activant/exigeant un chiffrement SMB pour les partages SMB dans Cloud Volumes Service. Si le chiffrement SMB n'est pas pris en charge par l'un des noeuds finaux, l'accès n'est pas autorisé.

Utilisation des alias de nom SMB

Dans certains cas, les utilisateurs finaux ne pourront pas connaître le nom du compte de la machine utilisé pour Cloud Volumes Service et ce, sans problèmes de sécurité. Dans d'autres cas, vous souhaiterez peut-être fournir aux utilisateurs un chemin d'accès plus simple. Dans ces cas, vous pouvez créer des alias SMB.

Si vous souhaitez créer des alias pour le chemin du partage SMB, vous pouvez exploiter ce qu'on appelle un enregistrement CNAME dans DNS. Par exemple, si vous souhaitez utiliser le nom `\\CIFS` pour accéder aux partages au lieu de `\\cvs-east- 433d.cvsdemo.local`, Mais vous souhaitez toujours utiliser l'authentification Kerberos, un CNAME dans DNS qui pointe vers l'enregistrement A/AAAA existant et un SPN supplémentaire ajouté au compte de machine existant fournit l'accès Kerberos.



Il s'agit du résultat de la recherche de transfert DNS après l'ajout d'un CNAME :

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Il s'agit de la requête SPN qui s'affiche après l'ajout de nouveaux SPN :

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Dans une capture de paquets, nous pouvons voir la demande de configuration de session en utilisant le SPN associé au CNAME.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
    name-type: kRB5-NT-SRV-INST (2)
    sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
enc-part
    etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Dialectes d'authentification SMB

Cloud Volumes Service prend en charge les éléments suivants "dialectes" Pour l'authentification SMB :

- LM
- NTLM
- NTLMv2
- Kerberos

L'authentification Kerberos pour l'accès au partage SMB est le niveau d'authentification le plus sécurisé que vous pouvez utiliser. Avec le cryptage AES et SMB activé, le niveau de sécurité est encore amélioré.

Cloud Volumes Service prend également en charge la rétrocompatibilité pour l'authentification LM et NTLM. Lorsque Kerberos est mal configuré (par exemple lors de la création d'alias SMB), l'accès au partage revient à des méthodes d'authentification plus faibles (telles que NTLMv2). Comme ces mécanismes sont moins sécurisés, ils sont désactivés dans certains environnements Active Directory. Si les méthodes d'authentification les plus faibles sont désactivées et que Kerberos n'est pas configuré correctement, l'accès au partage échoue car il n'existe pas de méthode d'authentification valide pour revenir à.

Pour plus d'informations sur la configuration/l'affichage des niveaux d'authentification pris en charge dans Active Directory, reportez-vous à la section "Sécurité du réseau : niveau d'authentification de LAN Manager".

Modèles d'autorisation

Autorisations NTFS/File

Les autorisations NTFS sont les autorisations appliquées aux fichiers et dossiers dans les systèmes de fichiers qui adhèrent à la logique NTFS. Vous pouvez appliquer des autorisations NTFS dans `Basic` ou `Advanced` et peut être défini sur `Allow` ou `Deny` pour le contrôle d'accès.

Les autorisations de base incluent les éléments suivants :

- Contrôle total
- Modifier
- Lecture et exécution
- Lecture
- Écriture

Lorsque vous définissez les autorisations d'un utilisateur ou d'un groupe, appelées ACE, elles résident dans une liste de contrôle d'accès. Les autorisations NTFS utilisent les mêmes principes de base en lecture/écriture/exécution que les bits du mode UNIX, mais elles peuvent également s'étendre à des contrôles d'accès plus granulaires et étendus (également appelés autorisations spéciales), tels que prendre propriété, Créer des dossiers/ajouter des données, écrire des attributs, etc.

Les bits standard du mode UNIX ne fournissent pas le même niveau de granularité que les autorisations NTFS (par exemple, la possibilité de définir des autorisations pour des objets individuels utilisateur et groupe dans une ACL ou la définition d'attributs étendus). Cependant, les listes de contrôle d'accès NFSv4.1 offrent les mêmes fonctionnalités que les listes de contrôle d'accès NTFS.

Les autorisations NTFS sont plus spécifiques que les autorisations de partage et peuvent être utilisées conjointement avec les autorisations de partage. Avec les structures d'autorisation NTFS, la plus restrictive s'applique. Ainsi, les refus explicites d'un utilisateur ou d'un groupe remplacent même le contrôle total lors de la définition des droits d'accès.

Les autorisations NTFS sont contrôlées à partir de clients SMB Windows.

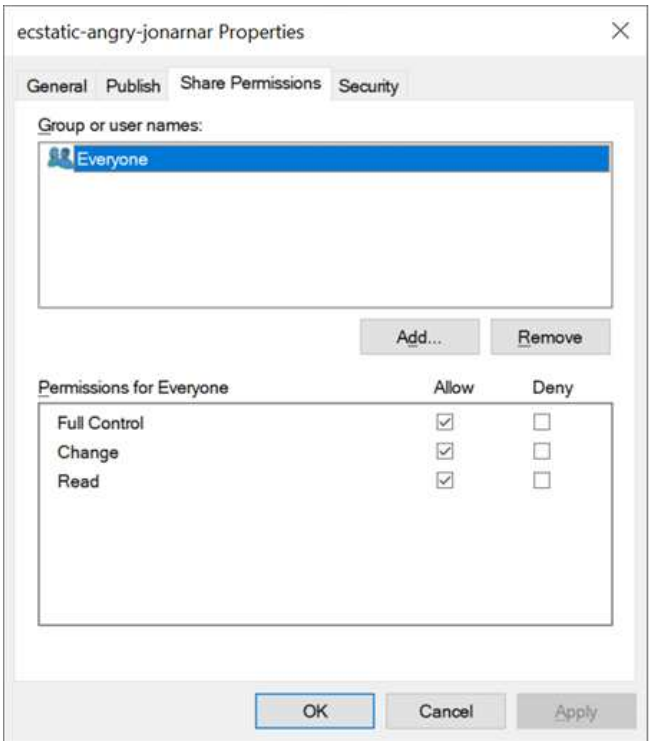
Partager les autorisations

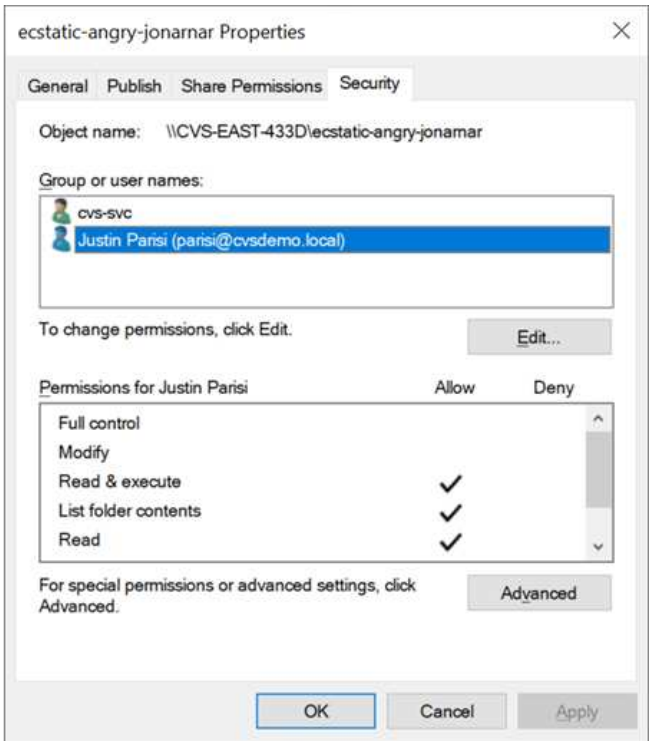
Les autorisations de partage sont plus générales que les autorisations NTFS (lecture/modification/contrôle total uniquement) et contrôlez l'entrée initiale dans un partage SMB, à l'instar des règles de règles d'export NFS.

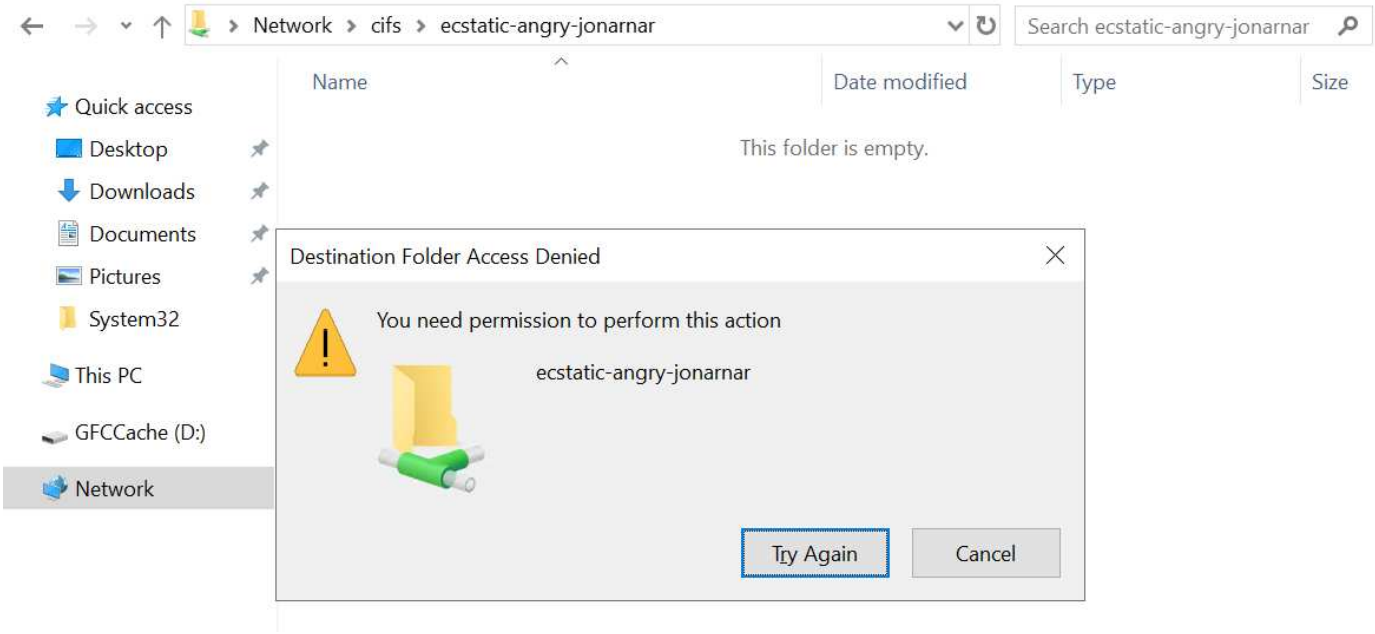
Bien que les règles d'export NFS contrôlent l'accès via des informations basées sur l'hôte telles que des adresses IP ou des noms d'hôte, les autorisations de partage SMB peuvent contrôler l'accès à l'aide d'ACE d'utilisateur et de groupe dans une liste de contrôle d'accès de partage. Vous pouvez définir des listes de contrôle d'accès de partage depuis le client Windows ou depuis l'interface utilisateur de gestion Cloud Volumes Service.

Par défaut, les listes de contrôle d'accès de partage et les listes de contrôle d'accès de volume initiales incluent tous les utilisateurs ayant un contrôle total. Les listes de contrôle d'accès du fichier doivent être modifiées, mais les autorisations de partage sont surdéfinies par les autorisations de fichier sur les objets du partage.

Par exemple, si un utilisateur n'est autorisé que l'accès en lecture à la liste de contrôle d'accès de fichier de volume Cloud Volumes Service, il est refusé d'accéder à la création de fichiers et de dossiers, même si la liste de contrôle d'accès du partage est définie sur tous les utilisateurs bénéficiant d'un contrôle total, comme indiqué dans la figure suivante.







Pour obtenir les meilleurs résultats en matière de sécurité, procédez comme suit :

- Supprimez tout le monde des listes de contrôle d'accès de partage et de fichiers et définissez plutôt l'accès de partage pour les utilisateurs ou les groupes.
- Pour faciliter la gestion des utilisateurs individuels, vous pouvez utiliser des groupes pour le contrôle d'accès, et pour accélérer la suppression et l'ajout d'utilisateurs pour partager ces listes via la gestion de groupes.
- Autorisez un accès plus général et moins restrictif au partage aux ACE depuis les autorisations de partage et verrouillez l'accès aux utilisateurs et aux groupes avec des autorisations de fichier pour un contrôle d'accès plus granulaire.
- Évitez l'utilisation générale des listes de contrôle d'accès de refus explicites, car elles remplacent les listes

de contrôle d'accès d'autorisation. Limiter l'utilisation des listes de contrôle d'accès de refus explicites pour les utilisateurs ou les groupes qui doivent être restreints rapidement d'un accès à un système de fichiers.

- Assurez-vous d'accorder votre attention au "Héritage ACL" paramètres lors de la modification des autorisations ; la définition de l'indicateur d'héritage au niveau supérieur d'un répertoire ou d'un volume avec un nombre élevé de fichiers signifie que chaque fichier sous ce répertoire ou volume possède des autorisations héritées ajoutées à celui-ci, ce qui peut créer un comportement indésirable tel qu'un accès/un refus involontaire et une longue perte de modification des autorisations au fur et à mesure que chaque fichier est ajusté.

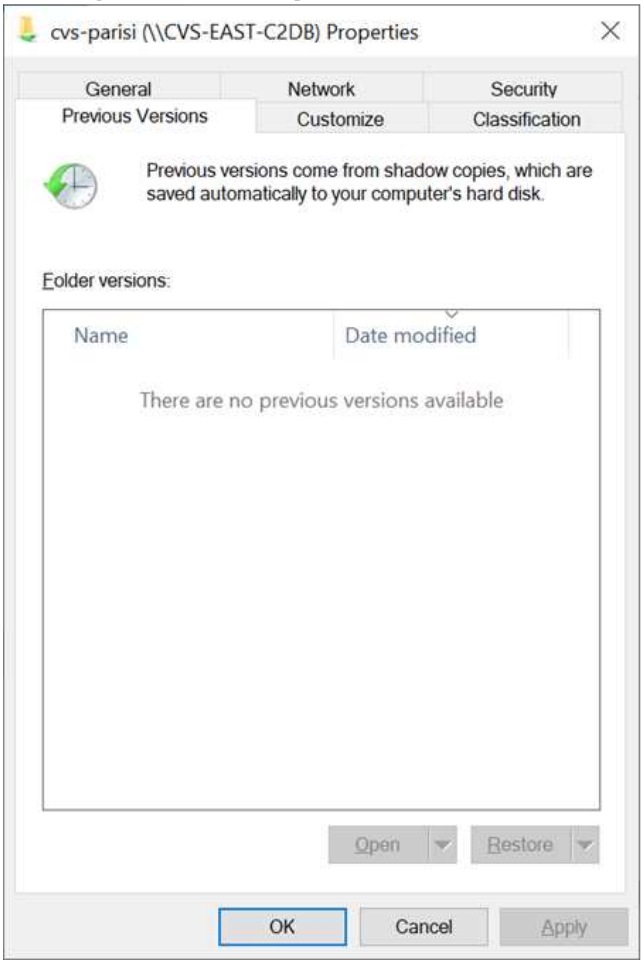
Fonctionnalités de sécurité de partage SMB

Lorsque vous créez un volume avec accès SMB dans Cloud Volumes Service pour la première fois, vous disposez d'une série d'options pour sécuriser ce volume.

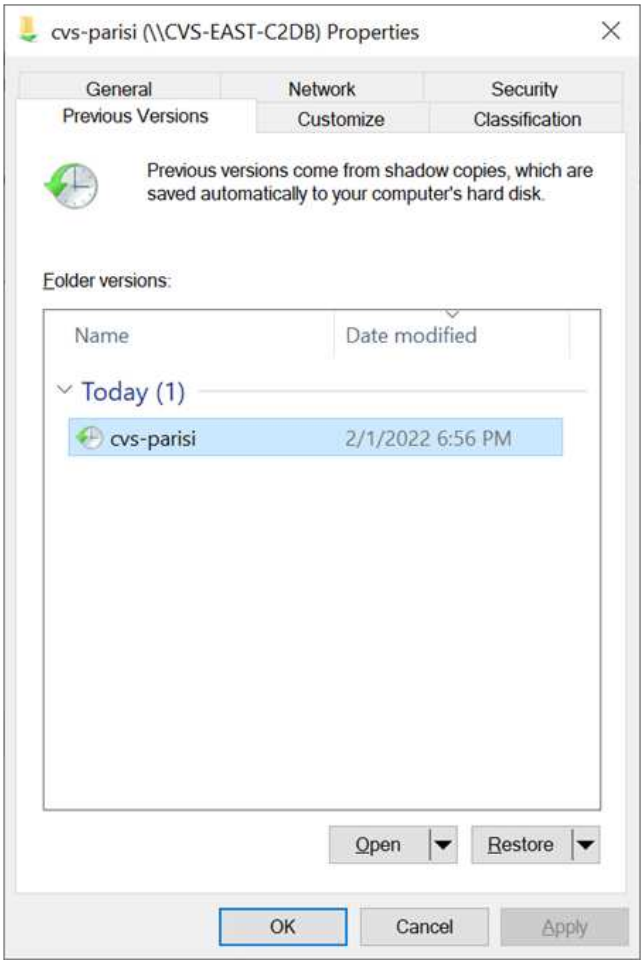
Les options suivantes dépendent du niveau Cloud Volumes Service (performances ou logiciels) et sont proposées :

- **Rendre le répertoire snapshot visible (disponible pour CVS-Performance et CVS-SW).** cette option permet de contrôler si les clients SMB peuvent accéder au répertoire snapshot dans un partage SMB (`\\server\share\~snapshot` Et/ou l'onglet versions précédentes). Le paramètre par défaut n'est pas coché, ce qui signifie que le volume par défaut est masqué et interdit l'accès au `~snapshot` Et aucune copie Snapshot n'apparaît dans l'onglet versions précédentes du volume.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Le masquage des copies Snapshot à partir des utilisateurs finaux peut être souhaité pour des raisons de

sécurité, de performances (masquage de ces dossiers à partir d'analyses antivirus) ou de préférence. Les snapshots Cloud Volumes Service sont en lecture seule. Par conséquent, même si ces snapshots sont visibles, les utilisateurs finaux ne peuvent pas supprimer ou modifier les fichiers dans le répertoire Snapshot. Autorisations liées aux fichiers ou dossiers au moment de la copie Snapshot. Si les autorisations d'un fichier ou d'un dossier changent entre les copies Snapshot, les modifications s'appliquent également aux fichiers ou dossiers du répertoire Snapshot. Les utilisateurs et les groupes peuvent accéder à ces fichiers ou dossiers en fonction des autorisations. Lorsque des suppressions ou des modifications de fichiers dans le répertoire Snapshot ne sont pas possibles, il est possible de copier des fichiers ou des dossiers à partir du répertoire Snapshot.

- **Activer le chiffrement SMB (disponible pour CVS-Performance et CVS-SW).** le chiffrement SMB est désactivé par défaut sur le partage SMB (non vérifié). La case active le chiffrement SMB, ce qui signifie que le trafic entre le client SMB et le serveur est crypté à la volée avec les niveaux de cryptage les plus élevés pris en charge négociés. Cloud Volumes Service prend en charge le chiffrement AES-256 pour SMB. L'activation du cryptage SMB a des retombées sur les performances de vos clients SMB, c'est-à-dire dans une plage de 10 à 20 %. NetApp encourage fortement les tests à vérifier si les performances sont acceptables.
- **Masquer le partage SMB (disponible pour CVS-Performance et CVS-SW).** définir cette option masque le chemin du partage SMB à partir de la navigation normale. Cela signifie que les clients qui ne connaissent pas le chemin du partage ne peuvent pas voir les partages lorsqu'ils accèdent au chemin UNC par défaut (par exemple `\\CVS-SMB`). Lorsque la case est cochée, seuls les clients qui connaissent explicitement le chemin du partage SMB ou qui ont le chemin du partage défini par un objet de stratégie de groupe peuvent y accéder (sécurité via obfuscation).
- **Activer l'énumération basée sur l'accès (ABE) (CVS-SW uniquement).** Ceci est similaire à masquer le partage SMB, sauf que les partages ou fichiers sont masqués uniquement des utilisateurs ou des groupes qui n'ont pas les autorisations d'accéder aux objets. Par exemple, si utilisateur Windows `joe` N'est pas autorisé au moins l'accès en lecture via les autorisations, puis l'utilisateur Windows `joe` Impossible de voir le partage SMB ou les fichiers. Cette option est désactivée par défaut et vous pouvez l'activer en cochant la case. Pour en savoir plus sur ABE, consultez l'article de la base de connaissances NetApp "Comment fonctionne l'énumération basée sur l'accès (ABE) ?"
- **Activer le support de partage disponible en continu (CA) (CVS-Performance uniquement).** "Partages SMB disponibles en permanence" Offrir un moyen de réduire les interruptions des applications lors des basculements en répliquant les États de verrouillage sur les nœuds du système back-end Cloud Volumes Service. Il ne s'agit pas d'une fonctionnalité de sécurité, mais elle offre une meilleure résilience globale. Actuellement, seules les applications SQL Server et FSLogix sont prises en charge pour cette fonctionnalité.

Partages masqués par défaut

Lorsqu'un serveur SMB est créé dans Cloud Volumes Service, il y a "partages administratifs masqués" (Avec la convention de nommage $) créées en plus du partage SMB du volume de données. Il s'agit notamment de C$ (accès à l'espace de noms) et IPC$ (partage de canaux nommés pour la communication entre les programmes, tels que les appels de procédure distante (RPC) utilisés pour l'accès à la console MMC (Microsoft Management Console)).

Le partage IPC$ ne contient pas de listes de contrôle d'accès partagées et ne peut pas être modifié – il est strictement utilisé pour les appels RPC et "Windows interdit l'accès anonyme à ces partages par défaut".

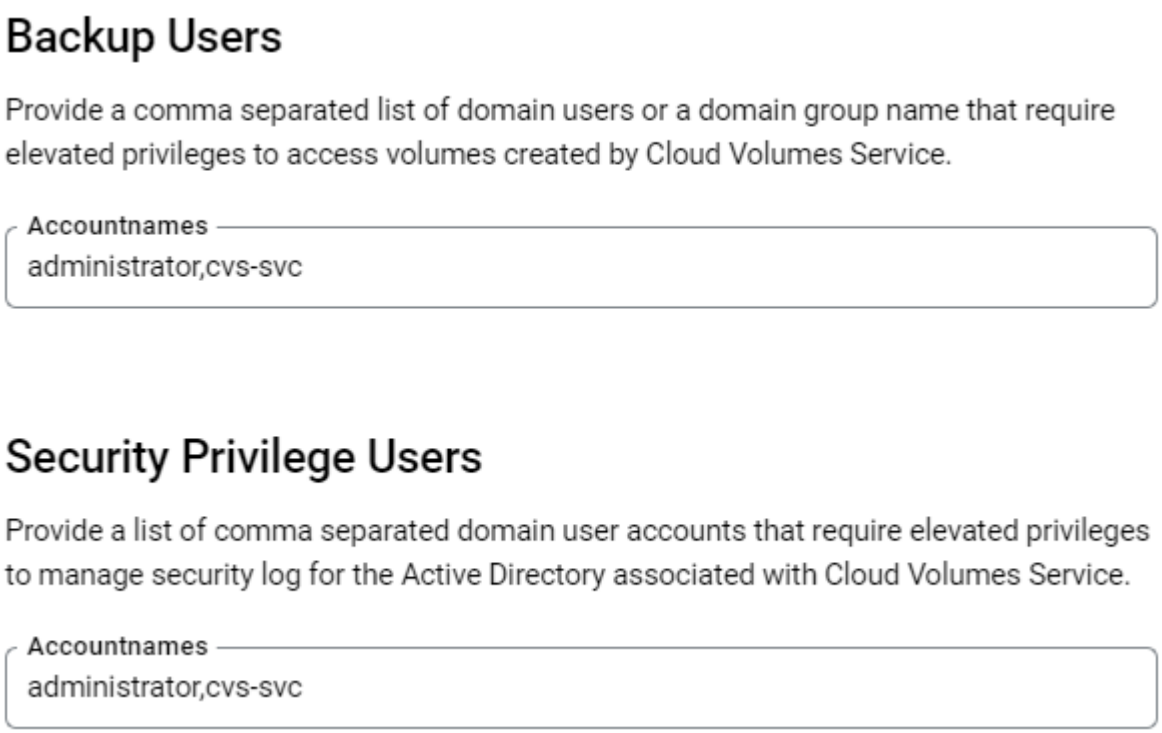
Le partage C$ permet l'accès par défaut à BUILTIN/Administrators, mais l'automatisation Cloud Volumes Service supprime la liste de contrôle d'accès de partage et n'autorise l'accès à personne car l'accès au partage C$ permet la visibilité de tous les volumes montés dans les systèmes de fichiers Cloud Volumes Service. Par conséquent, tente de naviguer vers `\\SERVER\C$` echec.

Comptes avec droits d'administrateur/de sauvegarde local/BUILTIN

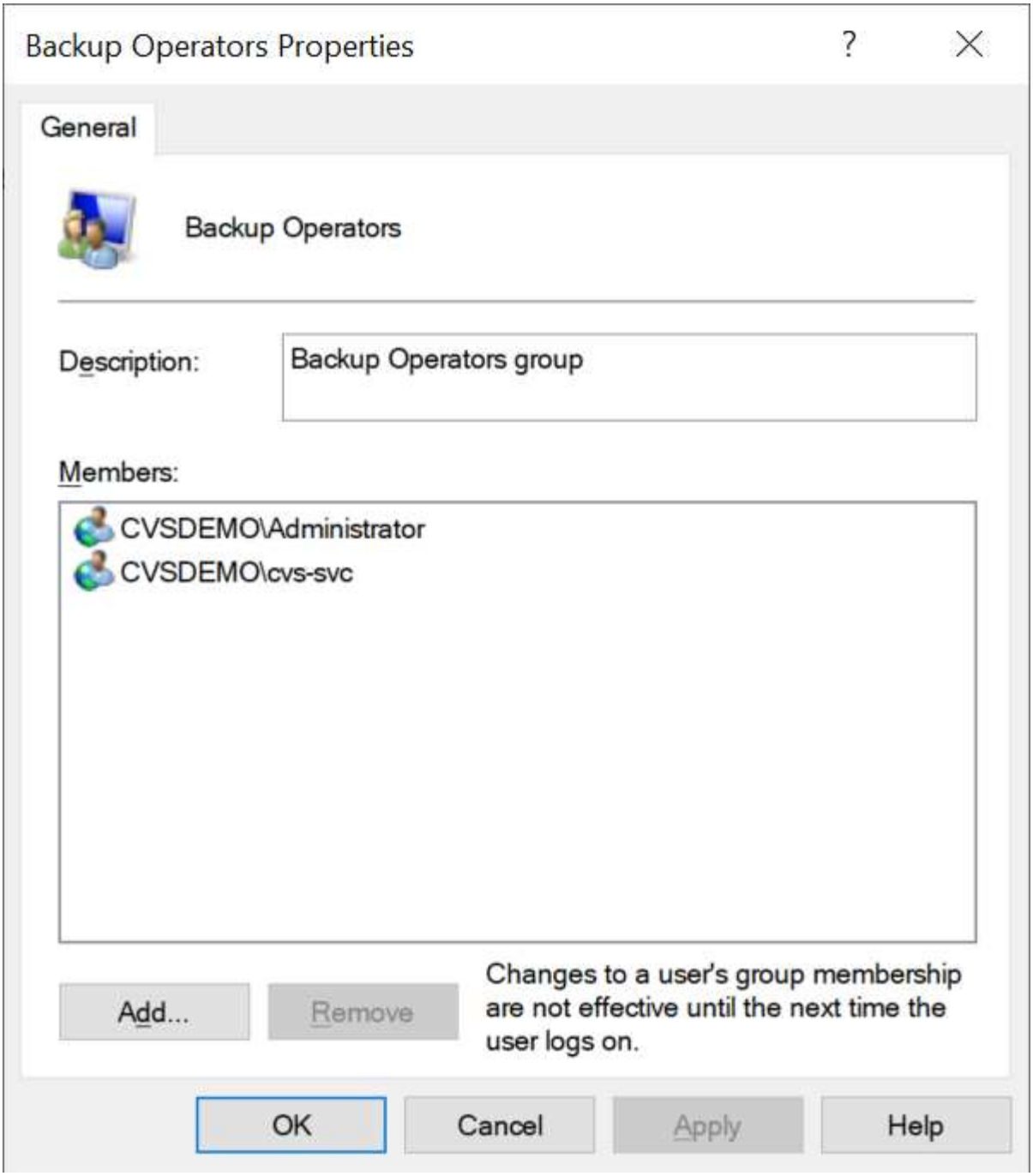
Les serveurs Cloud Volumes Service SMB conservent des fonctionnalités similaires aux serveurs Windows SMB classiques, dans la mesure où des groupes locaux (tels que BUILTIN\Administrators) appliquent des droits d'accès à certains utilisateurs et groupes de domaine.

Lorsque vous spécifiez un utilisateur à ajouter aux utilisateurs de sauvegarde, l'utilisateur est ajouté au groupe BULILTIN\opérateurs de sauvegarde de l'instance Cloud Volumes Service qui utilise cette connexion Active Directory, qui obtient ensuite le "SeBackupPrivilege et SeRestorePrivilege".

Lorsque vous ajoutez un utilisateur à des utilisateurs de privilèges de sécurité, l'utilisateur reçoit le privilège de sécurité, ce qui est utile dans certains cas d'utilisation d'application, tels que "SQL Server sur des partages SMB".



Vous pouvez afficher les membres du groupe local Cloud Volumes Service par l'intermédiaire de la console MMC avec les privilèges appropriés. La figure suivante montre les utilisateurs qui ont été ajoutés à l'aide de la console Cloud Volumes Service.

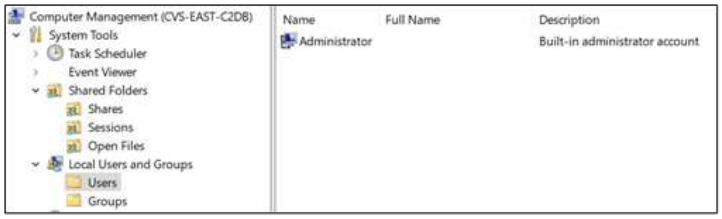


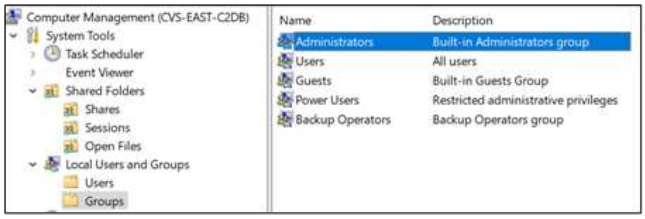
Le tableau suivant présente la liste des groupes par défaut BUILTIN et les utilisateurs/groupes ajoutés par défaut.

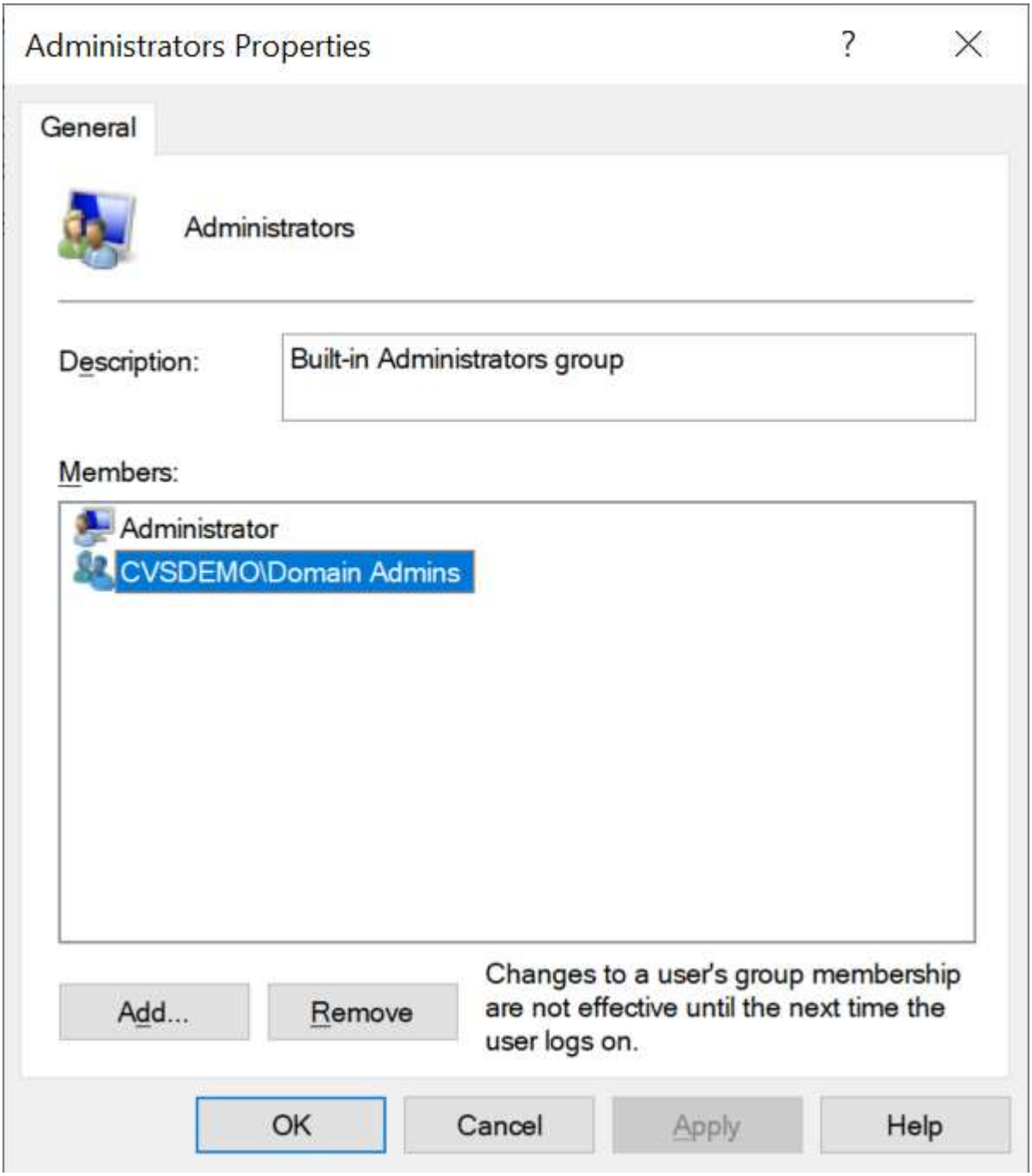
Groupe local/BUILTIN	Membres par défaut
INTÉGRÉ\administrateurs*	Administrateurs DE DOMAINE
INTÉGRÉ\opérateurs de sauvegarde*	Aucune
INTÉGRÉ\clients	Invités DOMAINE/domaine
UTILISATEURS INTENSIFS ET INTÉGRÉS	Aucune
Utilisateurs DE DOMAINE/INTÉGRÉ	Utilisateurs DU DOMAINE

*Appartenance au groupe contrôlée dans la configuration de connexion Cloud Volumes Service Active Directory.

Vous pouvez afficher des utilisateurs et des groupes locaux (et des membres de groupe) dans la fenêtre MMC, mais vous ne pouvez pas ajouter ou supprimer des objets ou modifier les appartenances de groupe à partir de cette console. Par défaut, seul le groupe administrateurs de domaine et l'administrateur sont ajoutés au groupe BULILTIN\Administrators dans Cloud Volumes Service. Actuellement, vous ne pouvez pas le modifier.







Accès MMC/gestion de l'ordinateur

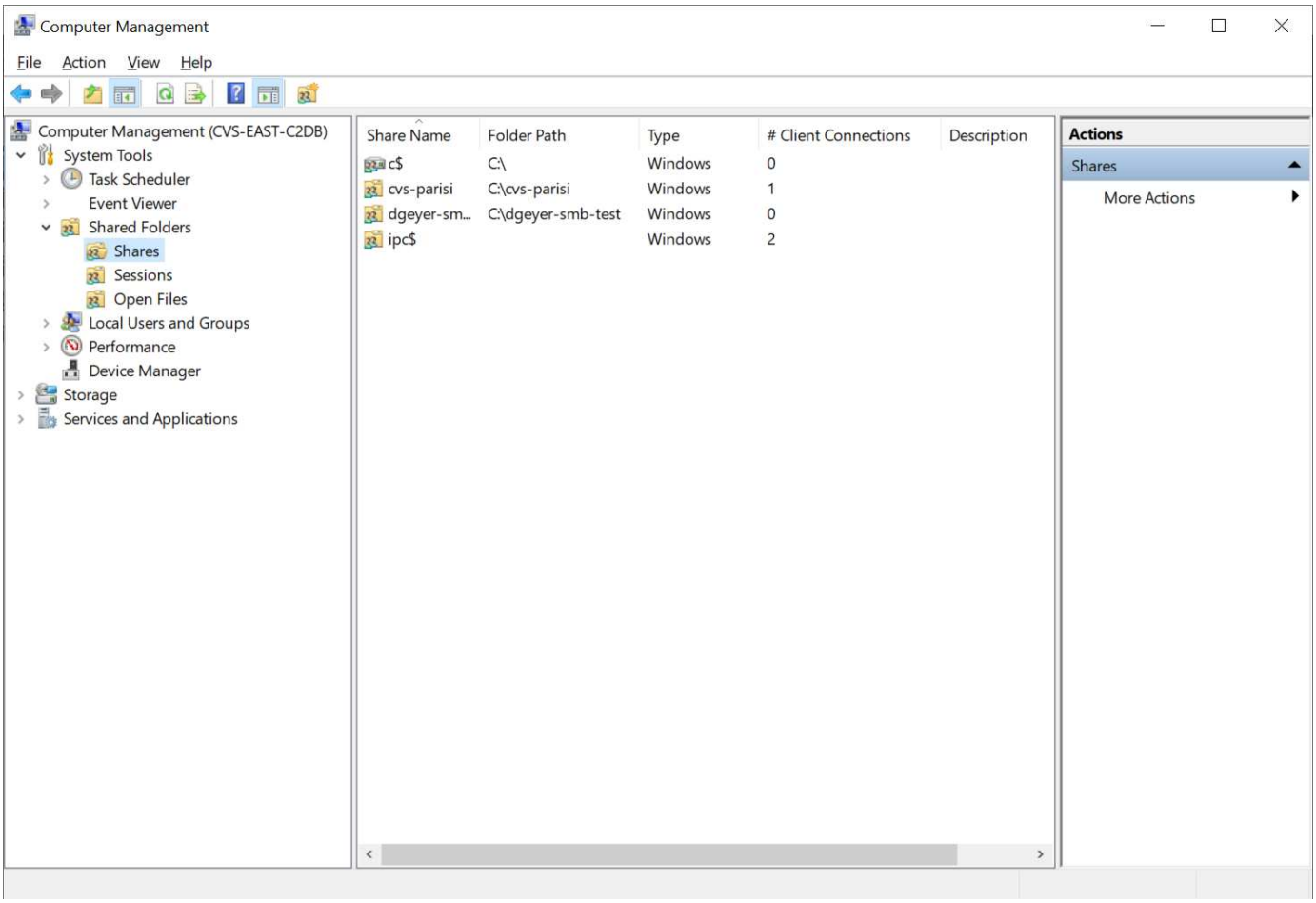
L'accès SMB dans Cloud Volumes Service fournit une connexion à la console MMC Computer Management, qui vous permet d'afficher les partages, de gérer les listes de contrôle d'accès de partage, d'afficher/gérer les sessions SMB et les fichiers ouverts.

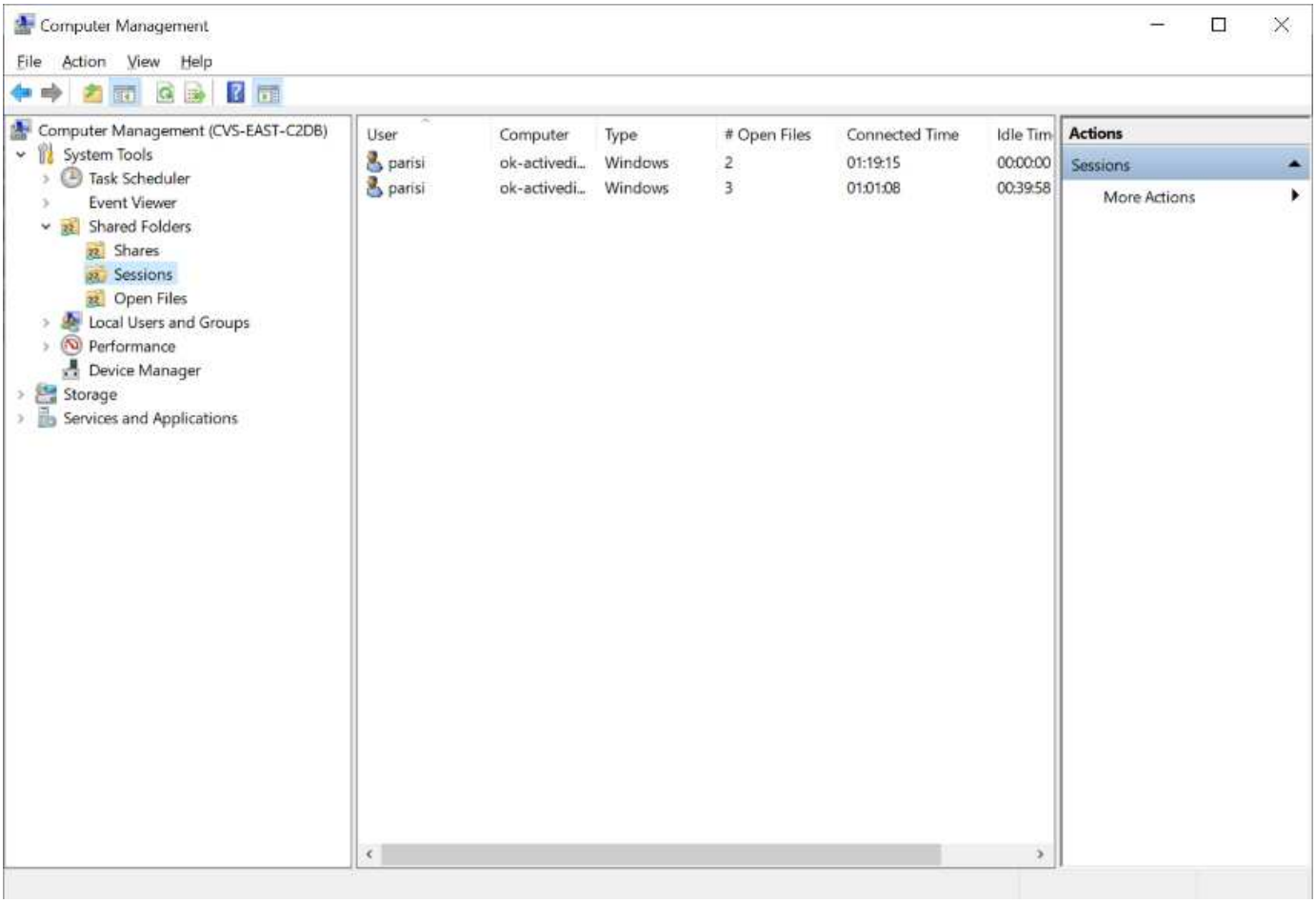
Pour utiliser la console MMC pour afficher les partages et sessions SMB dans Cloud Volumes Service, l'utilisateur connecté doit actuellement être un administrateur de domaine. Les autres utilisateurs sont autorisés à accéder à l'affichage ou à la gestion du serveur SMB à partir de MMC et reçoivent une boîte de dialogue vous n'avez pas d'autorisations lors de la tentative d'affichage de partages ou de sessions sur l'instance SMB de Cloud Volumes Service.

Pour vous connecter au serveur SMB, ouvrez gestion de l'ordinateur, cliquez avec le bouton droit de la souris sur gestion de l'ordinateur, puis sélectionnez connexion à un autre ordinateur. La boîte de dialogue Sélectionner un ordinateur s'ouvre, dans laquelle vous pouvez saisir le nom du serveur SMB (dans les informations sur le volume Cloud Volumes Service).

Lorsque vous affichez des partages SMB avec les autorisations appropriées, tous les partages disponibles de l'instance Cloud Volumes Service partageant la connexion Active Directory s'affichent. Pour contrôler ce comportement, définissez l'option Masquer les partages SMB sur l'instance de volume Cloud Volumes Service.

N'oubliez pas qu'une seule connexion Active Directory est autorisée par région.





Le tableau suivant présente la liste des fonctionnalités prises en charge/non prises en charge pour la console MMC.

Fonctions prises en charge	Fonctions non prises en charge
• Afficher les partages • Afficher les sessions SMB actives • Afficher les fichiers ouverts • Affichez les utilisateurs et groupes locaux • Afficher les membres du groupe local • Énumérer la liste des sessions, des fichiers et des connexions d'arborescence dans le système • Fermez les fichiers ouverts dans le système • Fermer les sessions ouvertes • Création/gestion de partages	• Création de nouveaux utilisateurs/groupes locaux • Gestion/affichage des utilisateurs/groupes locaux existants • Affichez les journaux d'événements ou de performances • La gestion du stockage • Gestion des services et des applications

Informations sur la sécurité du serveur SMB

Le serveur SMB de Cloud Volumes Service utilise un ensemble d'options qui définissent les stratégies de sécurité des connexions SMB, notamment l'inclinaison de l'horloge Kerberos, l'ancienneté des tickets, le cryptage, etc.

Le tableau suivant contient la liste de ces options, leur rôle et les configurations par défaut, si elles peuvent être modifiées avec Cloud Volumes Service. Certaines options ne s'appliquent pas à Cloud Volumes Service.

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Hauteur maximale de l'horloge Kerberos (minutes)	Décalage de temps maximal entre les contrôleurs Cloud Volumes Service et de domaine. Si l'écart de temps dépasse 5 minutes, l'authentification Kerberos échoue. Cette valeur est définie sur la valeur par défaut d'Active Directory.	5	Non
Durée de vie d'un ticket Kerberos (en heures)	Durée maximale pendant laquelle un ticket Kerberos reste valide avant d'exiger un renouvellement. Si aucun renouvellement n'a lieu avant les 10 heures, vous devez obtenir un nouveau billet. Cloud Volumes Service effectue automatiquement ces renouvellements. 10 heures est la valeur par défaut d'Active Directory.	10	Non
Renouvellement maximal de ticket Kerberos (jours)	Nombre maximum de jours pendant lesquels un ticket Kerberos peut être renouvelé avant qu'une nouvelle demande d'autorisation ne soit nécessaire. Cloud Volumes Service renouvelle automatiquement les billets pour les connexions des PME. Sept jours est la valeur par défaut d'Active Directory.	7	Non
Expiration du délai de connexion KDC Kerberos (secondes)	Nombre de secondes avant qu'une connexion KDC ne se soit interrompue.	3	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Signature requise pour le trafic SMB entrant	Paramètre pour exiger la signature pour le trafic SMB. Si la valeur est true, les clients qui ne prennent pas en charge la connexion échouent.	Faux	
Exiger la complexité du mot de passe pour les comptes d'utilisateur locaux	Utilisé pour les mots de passe des utilisateurs SMB locaux. Cloud Volumes Service ne prend pas en charge la création d'utilisateur local, donc cette option ne s'applique pas à Cloud Volumes Service.	Vrai	Non
Utilisez START_tls pour les connexions LDAP Active Directory	Utilisé pour activer les connexions TLS de démarrage pour Active Directory LDAP. Cloud Volumes Service ne prend pas encore en charge la mise en œuvre de cette fonctionnalité.	Faux	Non
Est compatible avec le chiffrement AES-128 et AES-256 pour Kerberos	Cette option permet de contrôler si le chiffrement AES est utilisé pour les connexions Active Directory et est contrôlé à l'aide de l'option Activer le chiffrement AES pour l'authentification Active Directory lors de la création/modification de la connexion Active Directory.	Faux	Oui.
Niveau de compatibilité LM	Niveau de dialectes d'authentification pris en charge pour les connexions Active Directory. Voir la section «Dialectes d'authentification SMB" pour plus d'informations.	ntlmv2-krb	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Cryptage SMB requis pour le trafic CIFS entrant	Chiffrement SMB requis pour tous les partages. Cette fonction n'est pas utilisée par Cloud Volumes Service ; définissez plutôt le chiffrement par volume (voir la section «Fonctionnalités de sécurité de partage SMB").	Faux	Non
Sécurité de la session client	Définit la signature et/ou le chiffrement pour la communication LDAP. Ce paramètre n'est pas actuellement défini dans Cloud Volumes Service mais peut être nécessaire dans les prochaines versions pour traiter . La résolution des problèmes d'authentification LDAP dus au correctif Windows est traitée dans la section ""Liaison de canal LDAP."".	Aucune	Non
SMB2 activé pour les connexions CC	Utilise SMB2 pour les connexions CC. Activé par défaut.	Système par défaut	Non
Poursuite des recommandations LDAP	Lors de l'utilisation de plusieurs serveurs LDAP, la recherche de références permet au client de se référer à d'autres serveurs LDAP de la liste lorsqu'une entrée est introuvable dans le premier serveur. Cette opération n'est actuellement pas prise en charge par Cloud Volumes Service.	Faux	Non
Utilisez LDAPS pour les connexions Active Directory sécurisées	Permet l'utilisation de LDAP sur SSL. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non

Option de sécurité	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Le cryptage est requis pour la connexion CC	Nécessite un chiffrement pour des connexions CC réussies. Désactivé par défaut dans Cloud Volumes Service.	Faux	Non

Double protocole/multiprotocole

Cloud Volumes Service permet de partager les mêmes datasets avec les clients SMB et NFS tout en maintenant les autorisations d'accès adéquates ("double protocole"). Pour ce faire, le mappage d'identités entre les protocoles et un serveur LDAP back-end centralisé permettent de fournir les identités UNIX à Cloud Volumes Service. Vous pouvez utiliser Windows Active Directory pour fournir à la fois aux utilisateurs Windows et UNIX la facilité d'utilisation.

Contrôle d'accès

- **Partage des contrôles d'accès.** déterminer quels clients et/ou utilisateurs et groupes peuvent accéder à un partage NAS. Dans le cas de NFS, les export-policy et les règles contrôlent l'accès client aux exports. Les exportations NFS sont gérées à partir de l'instance Cloud Volumes Service. SMB utilise les partages CIFS/SMB et les listes de contrôle d'accès de partage pour fournir un contrôle plus granulaire au niveau de l'utilisateur et du groupe. Vous pouvez uniquement configurer des listes de contrôle d'accès de niveau partage à partir de clients SMB en utilisant MMC/Computer Management avec un compte disposant de droits d'administrateur sur l'instance Cloud Volumes Service (voir la section « comptes avec des droits d'administrateur/de sauvegarde local/BUILTIN »).
- **Contrôles d'accès aux fichiers.** les autorisations de contrôle au niveau d'un fichier ou d'un dossier sont toujours gérées à partir du client NAS. Les clients NFS peuvent utiliser les bits de mode classiques (rwx) ou les listes de contrôle d'accès NFSv4. Les clients SMB exploitent les autorisations NTFS.

Le contrôle d'accès pour les volumes qui fournissent des données à la fois aux protocoles NFS et SMB dépend du protocole utilisé. Pour plus d'informations sur les autorisations avec double protocole, reportez-vous à la section «Modèle d'autorisation. »

Mappage d'utilisateurs

Lorsqu'un client accède à un volume, Cloud Volumes Service tente de mapper l'utilisateur entrant vers un utilisateur valide dans la direction opposée. Cela est nécessaire pour que l'accès soit déterminé dans l'ensemble des protocoles et pour s'assurer que l'utilisateur qui demande l'accès est bien celui qu'il prétend être.

Par exemple, si un utilisateur Windows nommé `joe` Tente d'accéder à un volume avec des autorisations UNIX via SMB, puis Cloud Volumes Service effectue une recherche pour trouver un utilisateur UNIX correspondant nommé `joe`. Le cas échéant, les fichiers qui sont écrits dans un partage SMB en tant qu'utilisateur Windows `joe` S'affiche en tant qu'utilisateur UNIX `joe` À partir de clients NFS.

Sinon, si un utilisateur UNIX nommé `joe` Tente d'accéder à un volume Cloud Volumes Service avec des autorisations Windows, puis l'utilisateur UNIX doit pouvoir mapper un utilisateur Windows valide. Dans le cas contraire, l'accès au volume est refusé.

Actuellement, seul Active Directory est pris en charge pour la gestion externe des identités UNIX avec LDAP. Pour plus d'informations sur la configuration de l'accès à ce service, reportez-vous à la section "Création d'une connexion AD".

Modèle d'autorisation

Lors de l'utilisation de configurations à double protocole, Cloud Volumes Service utilise des styles de sécurité pour les volumes afin de déterminer le type de liste de contrôle d'accès. Ces styles de sécurité sont définis en fonction du protocole NAS spécifié, ou dans le cas d'un double protocole, en fait l'option choisie au moment de la création du volume Cloud Volumes Service.

- Si vous utilisez uniquement NFS, les volumes Cloud Volumes Service utilisent des autorisations UNIX.
- Si vous utilisez uniquement SMB, les volumes Cloud Volumes Service utilisent des autorisations NTFS.

Si vous créez un volume à double protocole, vous pouvez choisir le style ACL lors de la création du volume. Cette décision doit être prise en fonction de la gestion des autorisations souhaitée. Si vos utilisateurs gèrent les autorisations des clients Windows/SMB, sélectionnez NTFS. Si vos utilisateurs préfèrent utiliser des clients NFS et chmod/chown, utilisez des styles de sécurité UNIX.

Considérations relatives à la création de connexions Active Directory

Cloud Volumes Service permet de connecter votre instance Cloud Volumes Service à un serveur Active Directory externe pour la gestion des identités tant pour les utilisateurs SMB que UNIX. La création d'une connexion Active Directory est nécessaire pour utiliser SMB dans Cloud Volumes Service.

La configuration offre plusieurs options qui nécessitent d'être prises en compte pour la sécurité. Le serveur Active Directory externe peut être une instance sur site ou un cloud natif. Si vous utilisez un serveur Active Directory sur site, n'exposez pas le domaine au réseau externe (par exemple avec une DMZ ou une adresse IP externe). Au lieu de cela, utilisez des tunnels privés sécurisés ou des VPN, des fiducies forestières à sens unique ou des connexions réseau dédiées aux réseaux sur site avec "Accès privé à Google". Consultez la documentation Google Cloud pour plus d'informations sur "Bonnes pratiques avec Active Directory dans Google Cloud".

> CVS-SW nécessite que les serveurs Active Directory soient situés dans la même région. Si une connexion CC est tentée dans CVS-SW vers une autre région, la tentative échoue. Lorsque vous utilisez CVS-SW, veillez à créer des sites Active Directory incluant les DCS Active Directory, puis spécifiez des sites dans Cloud Volumes Service pour éviter les tentatives de connexion CC entre régions.

Informations d'identification Active Directory

Lorsque SMB ou LDAP pour NFS est activé, Cloud Volumes Service interagit avec les contrôleurs Active Directory pour créer un objet de compte de machine à utiliser pour l'authentification. Ce n'est pas différent de la façon dont un client SMB Windows rejoint un domaine et nécessite les mêmes droits d'accès aux unités organisationnelles (UO) dans Active Directory.

Dans de nombreux cas, les groupes de sécurité n'autorisent pas l'utilisation d'un compte administrateur Windows sur des serveurs externes tels que Cloud Volumes Service. Dans certains cas, l'utilisateur de l'administrateur Windows est entièrement désactivé en tant que meilleure pratique de sécurité.

Autorisations nécessaires pour créer des comptes de machine SMB

Pour ajouter des objets machine Cloud Volumes Service à un Active Directory, un compte qui possède des droits d'administration sur le domaine ou a "autorisations déléguées pour créer et modifier des objets de compte machine" À une UO spécifiée est nécessaire. Pour ce faire, vous pouvez créer une tâche personnalisée avec l'assistant délégation de contrôle d'Active Directory qui fournit un accès utilisateur à la création/suppression d'objets d'ordinateur avec les autorisations d'accès suivantes :

- Lecture/écriture
- Créer/Supprimer tous les objets enfants
- Lire/écrire toutes les propriétés
- Modifier/Réinitialiser le mot de passe

Cette opération ajoute automatiquement une liste de contrôle d'accès de sécurité pour l'utilisateur défini à l'UO dans Active Directory et réduit l'accès à l'environnement Active Directory. Après la délégation d'un utilisateur, ce nom d'utilisateur et ce mot de passe peuvent être fournis en tant qu'informations d'identification Active Directory dans cette fenêtre.

> Le nom d'utilisateur et le mot de passe transmis au domaine Active Directory exploitent le chiffrement Kerberos lors de la requête et de la création d'objet de compte machine pour une sécurité supplémentaire.

Détails de la connexion à Active Directory

Le "Détails de connexion Active Directory" Indiquez les champs permettant aux administrateurs de fournir des informations spécifiques sur le schéma Active Directory pour le placement de compte machine, par exemple :

- **Type de connexion Active Directory.** utilisé pour spécifier si la connexion Active Directory dans une région est utilisée pour les volumes de type de service Cloud Volumes Service ou CVS-Performance. Si ce paramètre n'est pas défini correctement sur une connexion existante, il est possible qu'il ne fonctionne pas correctement lorsqu'il est utilisé ou modifié.
- **Domaine.** le nom de domaine Active Directory.
- **Site.** limite les serveurs Active Directory à un site spécifique pour la sécurité et les performances "considérations". Ceci est nécessaire lorsque plusieurs serveurs Active Directory s'étendent sur des régions car Cloud Volumes Service ne prend pas en charge actuellement l'autorisation d'autoriser les requêtes d'authentification Active Directory à des serveurs Active Directory dans une région différente de celle de l'instance Cloud Volumes Service. (Par exemple, le contrôleur de domaine Active Directory se trouve dans une région qui ne prend en charge que CVS-Performance mais vous voulez un partage SMB dans une instance CVS-SW.)
- **Serveurs DNS.** serveurs DNS à utiliser dans les recherches de noms.
- **Nom NetBIOS (facultatif).** si vous le souhaitez, le nom NetBIOS du serveur. Ce qui est utilisé lorsque de nouveaux comptes machine sont créés à l'aide de la connexion Active Directory. Par exemple, si le nom NetBIOS est défini sur CVS-EAST, les noms des comptes machine seront CVS-EAST-{1234}. Voir la section "Comment Cloud Volumes Service s'affiche dans Active Directory" pour en savoir plus.
- **Unité organisationnelle (UO).** l'UO spécifique pour créer le compte d'ordinateur. Ceci est utile si vous déléguez le contrôle à un utilisateur pour les comptes machine à une unité d'organisation spécifique.
- **Cryptage AES.** vous pouvez également cocher ou décocher la case Activer le cryptage AES pour l'authentification AD. L'activation du cryptage AES pour l'authentification Active Directory offre une sécurité supplémentaire pour la communication entre Cloud Volumes Service et Active Directory au cours des recherches utilisateur et de groupe. Avant d'activer cette option, vérifiez auprès de votre administrateur de

domaine que les contrôleurs de domaine Active Directory prennent en charge l'authentification AES.

> Par défaut, la plupart des serveurs Windows ne désactivent pas les chiffrements plus faibles (tels QUE DES ou RC4-HMAC), mais si vous choisissez de désactiver les chiffrements plus faibles, confirmez que la connexion Cloud Volumes Service Active Directory a été configurée pour activer AES. Dans le cas contraire, des échecs d'authentification se produisent. L'activation du cryptage AES ne désactive pas les chiffrements plus faibles mais ajoute au contraire la prise en charge du chiffrement AES au compte de la machine Cloud Volumes Service SMB.

Détails du domaine Kerberos

Cette option ne s'applique pas aux serveurs SMB. Elles sont plutôt utilisées lors de la configuration de Kerberos par NFS pour le système Cloud Volumes Service. Lorsque ces informations sont renseignées, le domaine Kerberos NFS est configuré (similaire à un fichier krb5.conf sous Linux) et utilisé lorsque NFS Kerberos est spécifié dans la création du volume Cloud Volumes Service, car la connexion Active Directory fait office de centre de distribution Kerberos NFS (KDC).

> Actuellement, les KDC non Windows ne sont pas pris en charge pour une utilisation avec Cloud Volumes Service.

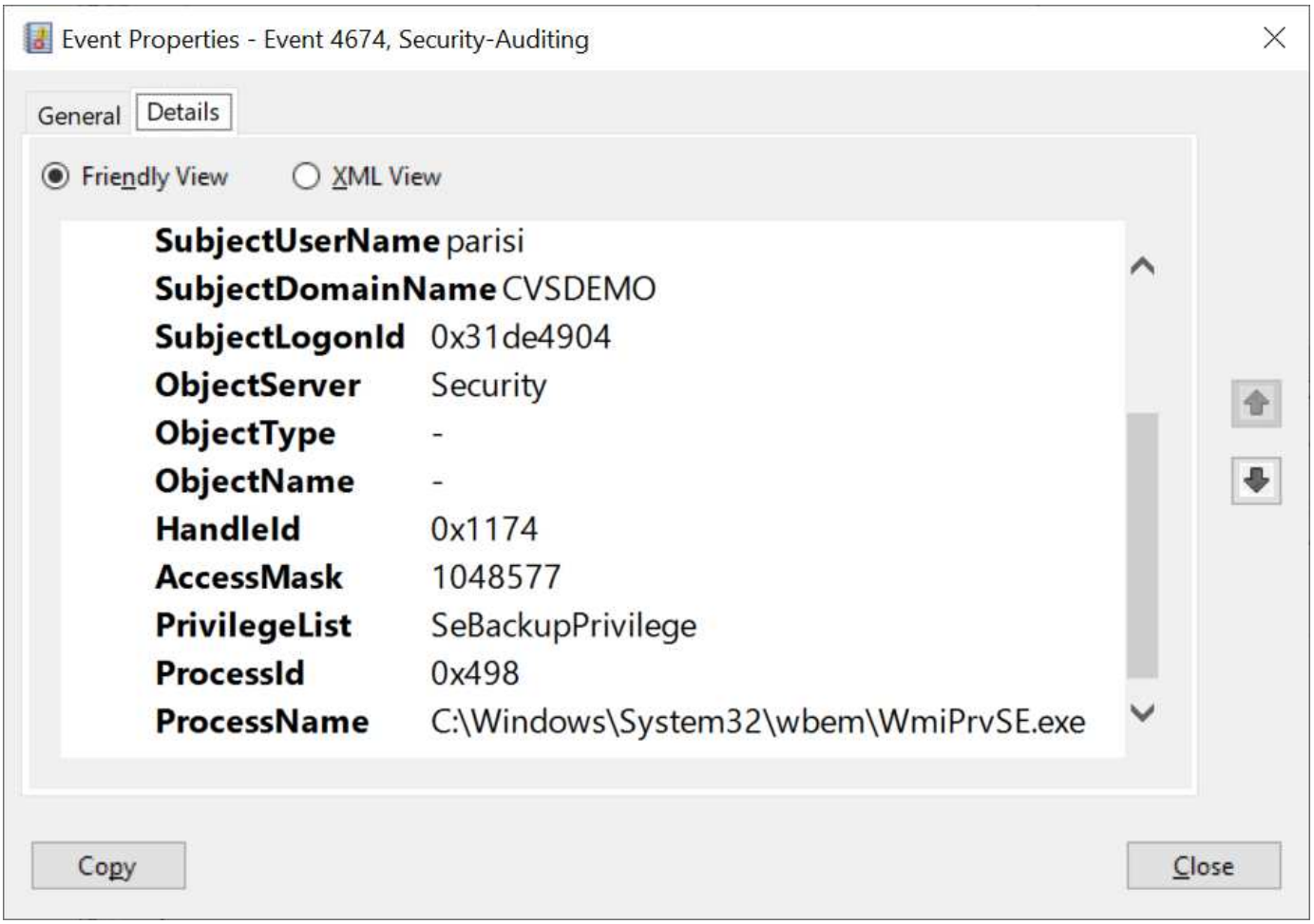
Région

Une région vous permet de spécifier l'emplacement où réside la connexion Active Directory. Cette région doit être la même région que le volume Cloud Volumes Service.

- **Utilisateurs NFS locaux avec LDAP.** dans cette section, il existe également une option permettant aux utilisateurs NFS locaux avec LDAP. Cette option doit être désélectionnée si vous souhaitez étendre votre prise en charge d'appartenance à un groupe d'utilisateurs UNIX au-delà de la limite de 16 groupes de NFS (groupes étendus). Cependant, l'utilisation de groupes étendus nécessite un serveur LDAP configuré pour les identités UNIX. Si vous ne disposez pas d'un serveur LDAP, laissez cette option non sélectionnée. Si vous disposez d'un serveur LDAP et souhaitez également utiliser des utilisateurs UNIX locaux (comme root), sélectionnez cette option.

Utilisateurs de la sauvegarde

Cette option vous permet de spécifier les utilisateurs Windows disposant d'autorisations de sauvegarde sur le volume Cloud Volumes Service. Les privilèges de sauvegarde (SeBackupPrivilege) sont nécessaires pour que certaines applications puissent sauvegarder et restaurer correctement les données dans des volumes NAS. Cet utilisateur dispose d'un haut niveau d'accès aux données du volume. Vous devez donc tenir compte de cet aspect "activation de l'audit de cet accès utilisateur". Une fois activée, les événements d'audit s'affichent dans Event Viewer > Windows Logs > Security.



Utilisateurs disposant des privilèges de sécurité

Cette option vous permet de spécifier les utilisateurs Windows disposant d'autorisations de modification de sécurité pour le volume Cloud Volumes Service. Des privilèges de sécurité (SeSecurityPrivilege) sont nécessaires pour certaines applications ("Tels que SQL Server") pour définir correctement les autorisations lors de l'installation. Ce privilège est nécessaire pour gérer le journal de sécurité. Bien que ce privilège ne soit pas aussi puissant que SeBackupPrivilege, NetApp recommande "audit de l'accès des utilisateurs" avec ce niveau de privilège, le cas échéant.

Pour plus d'informations, voir "Privilèges spéciaux attribués à la nouvelle connexion".

Comment Cloud Volumes Service s'affiche dans Active Directory

Cloud Volumes Service apparaît dans Active Directory comme un objet de compte machine normal. Les conventions de nom sont les suivantes.

- CIFS/SMB et NFS Kerberos créent des objets de compte de machine distincts.
- Le protocole NFS avec LDAP activé crée un compte machine dans Active Directory pour les liaisons LDAP Kerberos.
- Les volumes à double protocole avec LDAP partagent le compte de machine CIFS/SMB pour LDAP et SMB.
- Les comptes de machine CIFS/SMB utilisent une convention de dénomination de NOM-1234 (identifiant aléatoire à quatre chiffres avec tiret ajouté à <10 caractères name) pour le compte de machine. Vous pouvez définir LE NOM à l'aide du paramètre Nom NetBIOS de la connexion Active Directory (voir la

section «Détails de la connexion à Active Directory”).

- NFS Kerberos utilise NFS-NAME-1234 comme convention de nommage (15 caractères au maximum). Si plus de 15 caractères sont utilisés, le nom est NFS-TRONQUÉ-NAME-1234.
- Les instances CVS-Performance uniquement avec LDAP activées créent un compte de machine SMB pour la liaison au serveur LDAP avec la même convention de nommage que les instances CIFS/SMB.
- Lorsqu’un compte de machine SMB est créé, les partages admin masqués par défaut (voir la section "« Partages masqués par défaut »") Sont également créés (c$, admin$, ipc$), mais ces partages n’ont pas de listes de contrôle d’accès attribuées et sont inaccessibles.
- Les objets de compte machine sont placés par défaut dans CN=Computers, mais un vous pouvez spécifier une autre UO si nécessaire. Voir la section «Autorisations nécessaires pour créer des comptes de machine SMB” Pour plus d’informations sur les droits d’accès nécessaires pour ajouter/supprimer des objets de compte machine pour Cloud Volumes Service.

Lorsque Cloud Volumes Service ajoute le compte de machine SMB à Active Directory, les champs suivants sont renseignés :

- cn (avec le nom de serveur SMB spécifié)
- DnsHostName (avec SMBserver.domain.com)
- MSDS-SupportedEncryptionTypes (autorise LES_CBC_MD5, RC4_HMAC_MD5 si le chiffrement AES n’est pas activé ; si le chiffrement AES est activé, DES_CBC_MD5, RC4_HMAC_MD5, AES128_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1 est autorisé pour l’échange avec le compte SMB_96)
- Nom (avec le nom du serveur SMB)
- SAMAccountName (avec SMBserver$)
- ServicePrincipalName (avec hôte/smbserver.domain.com et SPN hôte/smbserver pour Kerberos)

Si vous souhaitez désactiver les types de cryptage Kerberos les plus faibles (type d’enc) sur le compte de la machine, vous pouvez modifier la valeur MSDS-SupportedEncryptionTypes sur le compte de la machine à l’une des valeurs du tableau suivant pour n’autoriser que AES.

MSDS-SupportedEncryptionTypes valeur	Type d’encan activé
2	DES_CBC_MD5
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96 UNIQUEMENT
16	AES256_CTS_HMAC_SHA1_96 UNIQUEMENT
24	AES128_CTS_HMAC_SHA1_96 ET AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 ET AES256_CTS_HMAC_SHA1_96

Pour activer le cryptage AES pour les comptes de machine SMB, cliquez sur Activer le cryptage AES pour l’authentification AD lors de la création de la connexion Active Directory.

Pour activer le chiffrement AES pour NFS Kerberos, "Consultez la documentation Cloud Volumes Service".

Autres dépendances des services d'infrastructure NAS (KDC, LDAP et DNS)

Lorsque vous utilisez Cloud Volumes Service pour les partages NAS, certaines dépendances externes peuvent être requises pour assurer le bon fonctionnement des partages. Ces dépendances sont en jeu dans des circonstances spécifiques. Le tableau suivant présente différentes options de configuration et le cas échéant, quelles dépendances sont nécessaires.

Configuration	Dépendances requises
NFSv3 uniquement	Aucune
Kerberos NFSv3 uniquement	Windows Active Directory : * KDC * DNS * LDAP
NFSv4.1 uniquement	Configuration du mappage d'ID client (/etc/idmap.conf)
NFSv4.1 Kerberos uniquement	• Configuration du mappage d'ID client (/etc/idmap.conf) • Windows Active Directory : LDAP KDC DNS
PME uniquement	Active Directory : * KDC * DNS
NAS multiprotocole (NFS et SMB)	• Configuration du mappage des ID client (NFSv4.1 uniquement ; /etc/idmap.conf) • Windows Active Directory : LDAP KDC DNS

La rotation/mot de passe de l'onglet clé Kerberos est réinitialisée pour les objets du compte machine

Avec les comptes machine SMB, Cloud Volumes Service planifie régulièrement les réinitialisations de mots de passe pour le compte machine SMB. Ces réinitialisations de mot de passe se produisent à l'aide du chiffrement Kerberos et fonctionnent sur une programmation de tous les 4 dimanches à une heure aléatoire comprise entre 23 H et 1 H. Ces réinitialisations de mot de passe modifient les versions de clé Kerberos, font pivoter les onglets enregistrés sur le système Cloud Volumes Service et permettent de maintenir un niveau de sécurité supérieur pour les serveurs SMB exécutés dans Cloud Volumes Service. Les mots de passe du compte machine sont randomisés et ne sont pas connus des administrateurs.

Pour les comptes de machine Kerberos NFS, les réinitialisations de mot de passe n'ont lieu que lorsqu'un nouveau keytab est créé/échangé avec le KDC. Actuellement, il n'est pas possible de le faire dans Cloud Volumes Service.

Ports réseau à utiliser avec LDAP et Kerberos

Lorsque vous utilisez LDAP et Kerberos, vous devez déterminer les ports réseau utilisés par ces services. La liste complète des ports utilisés par Cloud Volumes Service se trouve dans le "Documentation Cloud Volumes Service sur les considérations de sécurité".

LDAP

Cloud Volumes Service agit comme un client LDAP et utilise des requêtes de recherche LDAP standard pour les recherches utilisateur et de groupe pour les identités UNIX. LDAP est nécessaire si vous avez l'intention d'utiliser des utilisateurs et des groupes en dehors des utilisateurs standard par défaut fournis par Cloud Volumes Service. LDAP est également nécessaire si vous prévoyez d'utiliser NFS Kerberos avec des

principes utilisateur (tels que user1@domain.com). Actuellement, seul LDAP utilisant Microsoft Active Directory est pris en charge.

Pour utiliser Active Directory en tant que serveur LDAP UNIX, vous devez renseigner les attributs UNIX nécessaires pour les utilisateurs et groupes que vous souhaitez utiliser pour les identités UNIX. Cloud Volumes Service utilise un modèle de schéma LDAP par défaut qui interroge les attributs sur la base "RFC-2307-bis". Par conséquent, le tableau suivant montre les attributs Active Directory minimum requis pour remplir pour les utilisateurs et les groupes et pour quels attributs sont utilisés.

Pour plus d'informations sur la définition des attributs LDAP dans Active Directory, reportez-vous à la section "Gestion de l'accès double protocole."

Attribut	Ce qu'il fait
uid*	Spécifie le nom d'utilisateur UNIX
Numéro uidNumber*	Spécifie l'ID numérique de l'utilisateur UNIX
Numéro gidNumber*	Spécifie l'ID numérique du groupe principal de l'utilisateur UNIX
Objectclass*	Spécifie le type d'objet utilisé ; Cloud Volumes Service nécessite que "user" soit inclus dans la liste des classes d'objets (inclus dans la plupart des déploiements Active Directory par défaut).
nom	Informations générales sur le compte (nom réel, numéro de téléphone, etc., également connu sous le nom de gecos)
Mot de passe unixUserPassword	Inutile de le définir ; non utilisé dans les recherches d'identité UNIX pour l'authentification NAS. Cette option place la valeur unixUserPassword configurée dans le texte en texte clair.
UnixHomeDirectory	Définit le chemin d'accès aux répertoires locaux UNIX lorsqu'un utilisateur s'authentifie auprès de LDAP à partir d'un client Linux. Définissez cette option si vous souhaitez utiliser la fonctionnalité de répertoire local LDAP pour UNIX.
LoginShell	Définit le chemin d'accès au shell bash/de profil pour les clients Linux lorsqu'un utilisateur s'authentifie auprès de LDAP.

*L'attribut Denotes est requis pour une fonctionnalité correcte avec Cloud Volumes Service. Les autres attributs sont uniquement destinés à un usage côté client.

Attribut	Ce qu'il fait
cn*	Spécifie le nom du groupe UNIX. Lors de l'utilisation d'Active Directory pour LDAP, ce paramètre est défini lors de la création de l'objet, mais il peut être modifié ultérieurement. Ce nom ne peut pas être identique à celui des autres objets. Par exemple, si votre utilisateur UNIX nommé user1 appartient à un groupe nommé user1 sur votre client Linux, Windows n'autorise pas deux objets avec le même attribut cn. Pour contourner ce problème, renommez l'utilisateur Windows en un nom unique (tel que user1-UNIX) ; LDAP dans Cloud Volumes Service utilise l'attribut uid pour les noms d'utilisateur UNIX.
Numéro gidNumber*	Spécifie l'ID numérique du groupe UNIX.
Objectclass*	Indique le type d'objet utilisé ; Cloud Volumes Service nécessite que le groupe soit inclus dans la liste des classes d'objets (cet attribut est inclus par défaut dans la plupart des déploiements Active Directory).
MemberUid	Indique quels utilisateurs UNIX sont membres du groupe UNIX. Avec Active Directory LDAP dans Cloud Volumes Service, ce champ n'est pas nécessaire. Le schéma LDAP Cloud Volumes Service utilise le champ membre pour les appartenances de groupe.
Membre*	Requis pour les membres de groupe/groupes UNIX secondaires. Ce champ est rempli en ajoutant des utilisateurs Windows aux groupes Windows. Cependant, si les attributs UNIX des groupes Windows ne sont pas renseignés, ils ne sont pas inclus dans les listes d'appartenance aux groupes de l'utilisateur UNIX. Tous les groupes devant être disponibles dans NFS doivent remplir les attributs de groupe UNIX requis répertoriés dans ce tableau.

*L'attribut Denotes est requis pour une fonctionnalité correcte avec Cloud Volumes Service. Les autres attributs sont uniquement destinés à un usage côté client.

Informations de liaison LDAP

Pour interroger les utilisateurs dans LDAP, Cloud Volumes Service doit se lier (connexion) au service LDAP. Cette connexion possède des autorisations en lecture seule et est utilisée pour interroger les attributs LDAP UNIX pour les recherches de répertoire. Actuellement, les liaisons LDAP ne sont possibles qu'à l'aide d'un compte de machine SMB.

Vous pouvez uniquement activer LDAP pour `CVS-Performance` Instances et s'utilisent pour les volumes NFS v3, NFS v4.1 ou double protocole. Une connexion Active Directory doit être établie dans la même région que le volume Cloud Volumes Service pour le déploiement réussi du volume LDAP.

Lorsque LDAP est activée, les opérations suivantes se produisent dans des scénarios spécifiques.

- Si seul NFSv3 ou NFSv4.1 est utilisé pour le projet Cloud Volumes Service, un nouveau compte machine est créé dans le contrôleur de domaine Active Directory et le client LDAP dans Cloud Volumes Service se

lie à Active Directory à l'aide des informations d'identification du compte machine. Aucun partage SMB n'est créé pour le volume NFS et les partages administratifs masqués par défaut (voir la section "« Partages masqués par défaut »") Ont supprimé les ACL de partage.

- Si des volumes à double protocole sont utilisés pour le projet Cloud Volumes Service, seul le compte de machine unique créé pour l'accès SMB est utilisé pour lier le client LDAP de Cloud Volumes Service à Active Directory. Aucun compte machine supplémentaire n'est créé.
- Si des volumes SMB dédiés sont créés séparément (avant ou après l'activation des volumes NFS avec LDAP), le compte machine pour les liaisons LDAP est partagé avec le compte de machine SMB.
- Si NFS Kerberos est également activé, deux comptes machine sont créés : un pour les partages SMB et/ou des liaisons LDAP et un pour l'authentification Kerberos NFS.

Requêtes LDAP

Bien que les liaisons LDAP soient cryptées, les requêtes LDAP sont transmises sur le réseau en texte clair à l'aide du port LDAP commun 389. Ce port connu ne peut actuellement pas être modifié dans Cloud Volumes Service. Par conséquent, une personne ayant accès au sniffing de paquets dans le réseau peut voir les noms d'utilisateur et de groupe, les ID numériques et les appartenances de groupe.

Cependant, les machines virtuelles Google Cloud ne peuvent pas sniff le trafic unicast d'autres machines virtuelles. Seules les machines virtuelles participant activement au trafic LDAP (c'est-à-dire en mesure de lier) peuvent voir le trafic à partir du serveur LDAP. Pour plus d'informations sur le sniffing de paquets dans Cloud Volumes Service, reportez-vous à la section ""Considérations sur la capture et la détection des paquets.""

Paramètres par défaut de configuration du client LDAP

Lorsque LDAP est activée dans une instance Cloud Volumes Service, une configuration client LDAP est créée par défaut avec des détails de configuration spécifiques. Dans certains cas, les options ne s'appliquent pas à Cloud Volumes Service (non prises en charge) ou ne peuvent pas être configurées.

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Liste des serveurs LDAP	Définit les noms de serveur LDAP ou les adresses IP à utiliser pour les requêtes. Ceci n'est pas utilisé pour Cloud Volumes Service. À la place, Active Directory Domain est utilisé pour définir les serveurs LDAP.	Non défini	Non
Domaine Active Directory	Définit le domaine Active Directory à utiliser pour les requêtes LDAP. Cloud Volumes Service utilise les enregistrements SRV pour LDAP dans DNS pour trouver des serveurs LDAP dans le domaine.	Définissez le domaine Active Directory spécifié dans la connexion Active Directory.	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Serveurs Active Directory préférés	Définit les serveurs Active Directory préférés à utiliser pour LDAP. Non pris en charge par Cloud Volumes Service. Utilisez plutôt les sites Active Directory pour contrôler la sélection du serveur LDAP.	Non défini.	Non
Lier à l'aide des informations d'identification du serveur SMB	Se lie à LDAP à l'aide du compte de machine SMB. Actuellement, la seule méthode de liaison LDAP prise en charge dans Cloud Volumes Service.	Vrai	Non
Modèle de schéma	Modèle de schéma utilisé pour les requêtes LDAP.	MS-AD-BIS	Non
Port du serveur LDAP	Numéro de port utilisé pour les requêtes LDAP. Cloud Volumes Service utilise actuellement uniquement le port LDAP standard 389. Le port LDAPS/636 n'est pas pris en charge actuellement.	389	Non
LDAPS est activé	Contrôle si LDAP sur SSL (Secure Sockets Layer) est utilisé pour les requêtes et les liaisons. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non
Délai d'expiration de la requête (secondes)	Délai d'attente pour les requêtes. Si les requêtes prennent plus de temps que la valeur spécifiée, les requêtes échouent.	3	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Niveau d'authentification de liaison minimum	Niveau de liaison minimum pris en charge. Étant donné que Cloud Volumes Service utilise des comptes machine pour les liaisons LDAP et qu'Active Directory ne prend pas en charge les liaisons anonymes par défaut, cette option n'est pas en jeu pour la sécurité.	Anonyme	Non
Lier DN	Nom d'utilisateur/nom distinctif (DN) utilisé pour les liaisons lorsque la liaison simple est utilisée. Cloud Volumes Service utilise des comptes machine pour les liaisons LDAP et ne prend actuellement pas en charge l'authentification BIND simple.	Non défini	Non
DN de base	Le DN de base utilisé pour les recherches LDAP.	Le domaine Windows utilisé pour la connexion Active Directory, au format DN (c.c.=domaine, c.c.=local).	Non
Étendue de la recherche de base	Domaine de recherche pour les recherches de DN de base. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service prend uniquement en charge les recherches dans les sous-arborescences.	Sous-arbre	Non
Nom unique de l'utilisateur	Définit le DN où l'utilisateur recherche les requêtes LDAP. Actuellement non pris en charge pour Cloud Volumes Service, toutes les recherches d'utilisateur commencent par le NA de base.	Non défini	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Étendue de la recherche utilisateur	Domaine de recherche pour les recherches de DN utilisateur. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service ne prend pas en charge la définition de l'étendue de la recherche utilisateur.	Sous-arbre	Non
DN du groupe	Définit le DN où le groupe recherche les requêtes LDAP. Actuellement non pris en charge pour Cloud Volumes Service, toutes les recherches de groupe commencent par le NA de base.	Non défini	Non
Étendue de la recherche de groupe	Domaine de recherche pour les recherches de DN de groupe. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service ne prend pas en charge la définition de l'étendue de la recherche de groupe.	Sous-arbre	Non
DN du groupe réseau	Définit le DN où le groupe réseau recherche les requêtes LDAP. Actuellement non pris en charge pour Cloud Volumes Service, toutes les recherches de groupe réseau commencent par le DN de base.	Non défini	Non
Domaine de recherche de groupe réseau	Domaine de recherche pour les recherches de DN de groupe réseau. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Cloud Volumes Service ne prend pas en charge la définition de l'étendue de recherche du groupe réseau.	Sous-arbre	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Utilisez START_tls sur LDAP	Utilise Start TLS pour les connexions LDAP basées sur des certificats via le port 389. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non
Activez la recherche netgroup-by-host	Active les recherches de groupe réseau par nom d'hôte plutôt que d'étendre les groupes réseau pour répertorier tous les membres. Actuellement non pris en charge par Cloud Volumes Service.	Faux	Non
DN netgroup-by-host	Définit le DN où les recherches de netgroup-par-hôte commencent pour les requêtes LDAP. Netgroup-by-host n'est actuellement pas pris en charge pour Cloud Volumes Service.	Non défini	Non
Étendue de recherche netgroup-by-host	Étendue de recherche pour les recherches de DN netgroup-par-hôte. Les valeurs peuvent inclure la base, l'élévation ou la sous-arborescence. Netgroup-by-host n'est actuellement pas pris en charge pour Cloud Volumes Service.	Sous-arbre	Non
Sécurité de session client	Définit le niveau de sécurité de session utilisé par LDAP (signe, sceau ou aucun). La signature LDAP est prise en charge par CVS-Performance, sur demande d'Active Directory. CVS-SW ne prend pas en charge la signature LDAP. Pour les deux types d'entretien, le scellage n'est actuellement pas pris en charge.	Aucune	Non

Option client LDAP	Ce qu'il fait	Valeur par défaut	Est-il possible de modifier ?
Renvoi LDAP à la recherche	Lors de l'utilisation de plusieurs serveurs LDAP, la recherche de références permet au client de se référer à d'autres serveurs LDAP de la liste lorsqu'une entrée est introuvable dans le premier serveur. Cette opération n'est actuellement pas prise en charge par Cloud Volumes Service.	Faux	Non
Filtre d'appartenance au groupe	Fournit un filtre de recherche LDAP personnalisé à utiliser lors de la recherche d'appartenance à un groupe à partir d'un serveur LDAP. Non pris en charge actuellement avec Cloud Volumes Service.	Non défini	Non

Utilisation de LDAP pour le mappage de noms asymétrique

Par défaut, Cloud Volumes Service mappe les utilisateurs Windows et les utilisateurs UNIX avec des noms d'utilisateur identiques, dans le même sens, sans configuration spéciale. Tant que Cloud Volumes Service peut trouver un utilisateur UNIX valide (avec LDAP), un mappage de nom 1:1 se produit. Par exemple, si utilisateur Windows `johnsmith` Est utilisé, alors, si Cloud Volumes Service peut trouver un utilisateur UNIX nommé `johnsmith` Dans LDAP, le mappage de noms réussit pour cet utilisateur, tous les fichiers/dossiers créés par `johnsmith` Affiche la propriété correcte de l'utilisateur et toutes les listes de contrôle d'accès qui affectent `johnsmith` Sont honorés quel que soit le protocole NAS utilisé. Il s'agit d'un mappage de nom symétrique.

Le mappage de nom asymétrique est utilisé lorsque l'identité utilisateur Windows et l'identité utilisateur UNIX ne correspondent pas. Par exemple, si utilisateur Windows `johnsmith` Possède une identité UNIX de `jsmith`, Cloud Volumes Service a besoin d'une façon d'être racontée sur la variation. Cloud Volumes Service ne prenant actuellement pas en charge la création de règles de mappage de noms statiques, LDAP doit être utilisé pour rechercher l'identité des utilisateurs pour les identités Windows et UNIX afin d'assurer la propriété correcte des fichiers et dossiers et des autorisations attendues.

Par défaut, Cloud Volumes Service inclut `LDAP` Dans le commutateur ns-switch de l'instance de la base de données de mappage de noms, afin de fournir une fonctionnalité de mappage de noms en utilisant LDAP pour les noms asymétriques, il vous suffit de modifier certains attributs utilisateur/groupe pour refléter ce que recherche Cloud Volumes Service.

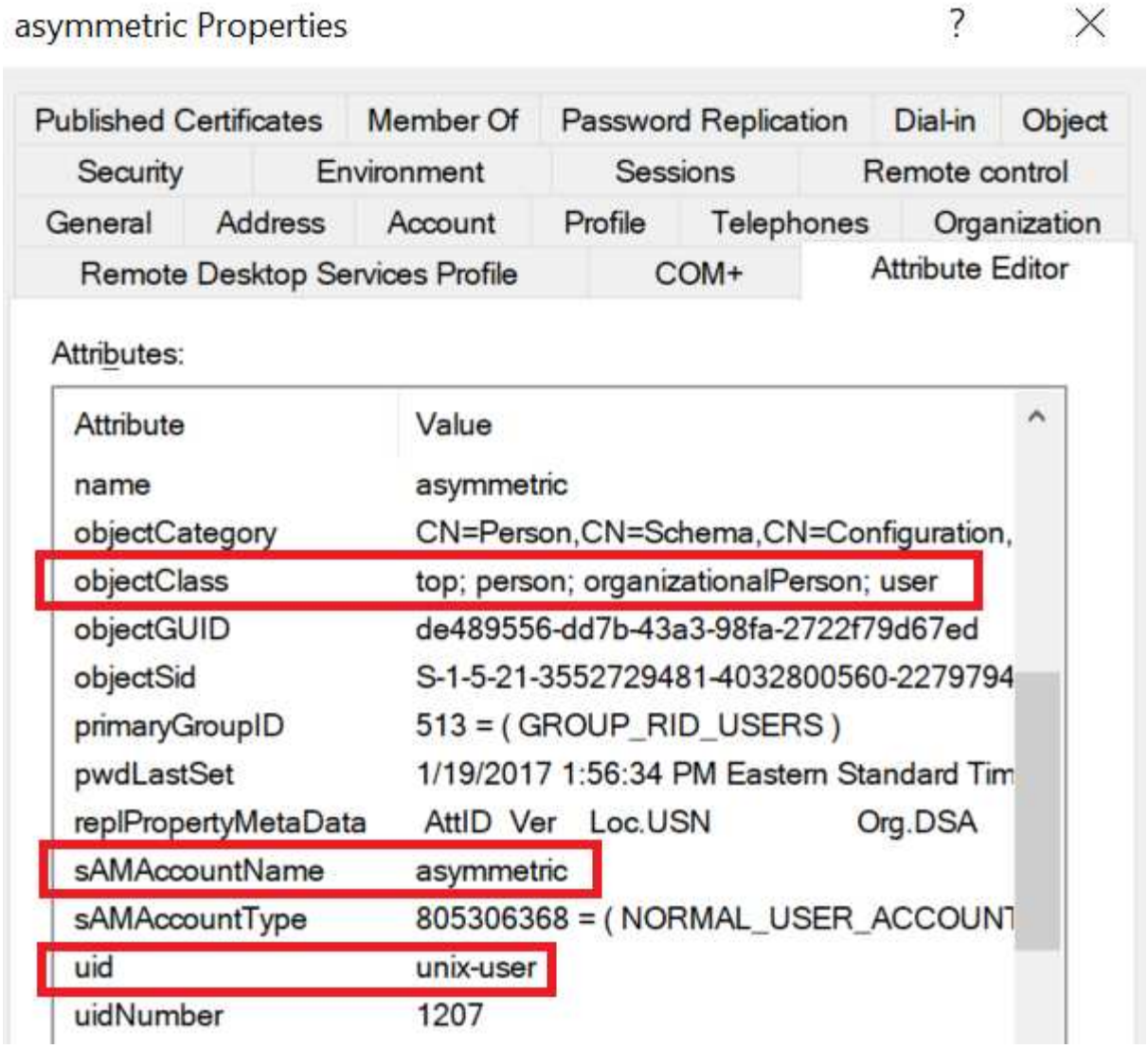
Le tableau suivant indique quels attributs doivent être renseignés dans LDAP pour la fonctionnalité de mappage de noms asymétriques. Dans la plupart des cas, Active Directory est déjà configuré pour le faire.

Attribut Cloud Volumes Service	Ce qu'il fait	Valeur utilisée par Cloud Volumes Service pour le mappage de noms
ObjectClass de Windows à UNIX	Spécifie le type d'objet utilisé. (C'est-à-dire utilisateur, groupe, posixAccount, etc.)	Doit inclure l'utilisateur (peut contenir plusieurs autres valeurs, si nécessaire).
Attribut Windows à UNIX	Qui définit le nom d'utilisateur Windows lors de sa création. Cloud Volumes Service utilise cette fonction pour les recherches Windows vers UNIX.	Aucune modification n'est nécessaire ici ; sAMAccountName est identique au nom de connexion Windows.
UID	Définit le nom d'utilisateur UNIX.	Nom d'utilisateur UNIX souhaité.

Cloud Volumes Service n'utilise actuellement pas de préfixes de domaine dans les recherches LDAP, de sorte que plusieurs environnements LDAP de domaine ne fonctionnent pas correctement avec les recherches de carte de noms LDAP.

L'exemple suivant montre un utilisateur portant le nom Windows `asymmetric`, Le nom UNIX `unix-user`, Et le comportement suivant lors de l'écriture de fichiers à partir de SMB et NFS.

La figure suivante montre l'apparence des attributs LDAP à partir du serveur Windows.



À partir d'un client NFS, vous pouvez interroger le nom UNIX mais pas le nom Windows :

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Lorsqu'un fichier est écrit à partir de NFS en tant que `unix-user`, Le résultat suivant est celui du client NFS :

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

À partir d'un client Windows, vous pouvez voir que le propriétaire du fichier est défini sur l'utilisateur Windows approprié :

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Inversement, les fichiers créés par l'utilisateur Windows `asymmetric` À partir d'un client SMB, montrer le propriétaire UNIX approprié, comme indiqué dans le texte suivant.

SMB :

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS :

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Liaison de canal LDAP

En raison d'une vulnérabilité avec les contrôleurs de domaine Windows Active Directory, "Avis de sécurité de Microsoft ADV190023" Modifie la façon dont le DCS autorise les liaisons LDAP.

L'impact pour Cloud Volumes Service est le même que pour tous les clients LDAP. Cloud Volumes Service ne prend actuellement pas en charge la liaison de canaux. Étant donné que Cloud Volumes Service prend en charge la signature LDAP par défaut via la négociation, la liaison du canal LDAP ne doit pas poser problème. Si vous rencontrez des problèmes de liaison avec LDAP alors que la liaison des canaux est activée, suivez les étapes de correction décrites dans ADV190023 pour permettre aux liaisons LDAP à partir de Cloud Volumes Service de réussir.

DNS

Active Directory et Kerberos ont tous deux des dépendances sur DNS pour la résolution du nom d'hôte à IP/IP vers le nom d'hôte. Le DNS requiert l'ouverture du port 53. Cloud Volumes Service n'apporte aucune modification aux enregistrements DNS et ne prend actuellement en charge l'utilisation de "DNS dynamique" sur les interfaces réseau.

Vous pouvez configurer Active Directory DNS pour limiter les serveurs qui peuvent mettre à jour les enregistrements DNS. Pour plus d'informations, voir "Un DNS Windows sécurisé".

Notez que les ressources d'un projet Google utilisent par défaut Google Cloud DNS, qui n'est pas connecté à Active Directory DNS. Les clients utilisant le DNS du cloud ne peuvent pas résoudre les chemins UNC renvoyés par Cloud Volumes Service. Les clients Windows joints au domaine Active Directory sont configurés

pour utiliser Active Directory DNS et peuvent résoudre de tels chemins UNC.

Pour joindre un client à Active Directory, vous devez configurer sa configuration DNS pour utiliser Active Directory DNS. Vous pouvez également configurer Cloud DNS pour transférer les demandes vers Active Directory DNS. Voir "Pourquoi mon client ne parvient-il pas à résoudre le nom NetBIOS du SMB ?"pour en savoir plus.

Cloud Volumes Service ne prend pas actuellement en charge les requêtes DNSSEC et DNS sont exécutées en texte clair.

Audit de l'accès aux fichiers

Actuellement non pris en charge par Cloud Volumes Service.

Protection antivirus

Vous devez effectuer une analyse antivirus dans Cloud Volumes Service au niveau du client vers un partage NAS. Il n'existe actuellement pas d'intégration antivirus native avec Cloud Volumes Service.

Opération d'entretien

L'équipe Cloud Volumes Service gère les services de back-end dans Google Cloud et exploite plusieurs stratégies pour sécuriser la plateforme et empêcher les accès non autorisés.

Chaque client bénéficie de son propre sous-réseau unique, qui dispose d'un accès clôturé par défaut par rapport à d'autres clients. Par ailleurs, chaque locataire de Cloud Volumes Service dispose de son propre espace de noms et VLAN pour assurer l'isolation totale des données. Après l'authentification d'un utilisateur, le moteur de fourniture de services (SDE) peut uniquement lire les données de configuration spécifiques à ce locataire.

Sécurité physique

Une fois la préapprobation adéquate obtenue, seuls les ingénieurs sur site et les ingénieurs de support de terrain (FSE) certifiés NetApp ont accès à la cage et aux racks pour les travaux physiques. La gestion du réseau et du stockage n'est pas autorisée. Seules ces ressources sur site sont en mesure d'effectuer les tâches de maintenance du matériel.

Pour les ingénieurs sur site, un ticket est émis pour l'énoncé des travaux (SOW) qui inclut l'ID de rack et l'emplacement du périphérique (RU). Toutes les autres informations sont incluses dans le ticket. Pour les FSE NetApp, un ticket de visite sur site doit être levé avec la COLOCATION. Le ticket inclut également les détails, la date et l'heure du visiteur à des fins d'audit. Le cahier des charges du FSE est communiqué à NetApp en interne.

Équipe chargée des opérations

L'équipe des opérations de Cloud Volumes Service se compose de l'ingénierie de production et d'un ingénieur de fiabilité de site (SRE) pour les services de volume cloud, ainsi que des ingénieurs de support sur site de NetApp et des partenaires pour le matériel. Tous les membres de l'équipe des opérations sont accrédités pour travailler dans Google Cloud et des dossiers de travail détaillés sont conservés pour chaque billet émis. De plus, un processus rigoureux de contrôle et d'approbation du changement est en place pour s'assurer que chaque décision est examinée de façon appropriée.

L'équipe SRE gère le plan de contrôle et la manière dont les données sont acheminées depuis les demandes

d'interface utilisateur vers le matériel et les logiciels back-end dans Cloud Volumes Service. L'équipe SRE gère également les ressources système, telles que les volumes et les volumes d'inode maximaux. Les SRES ne sont pas autorisés à interagir avec les données clients ou à y accéder. SRES assure également la coordination des autorisations de renvoi de matériel (RMA), telles que les demandes de remplacement de nouveau disque ou de mémoire pour le matériel interne.

Obligations du client

Les clients de Cloud Volumes Service gèrent Active Directory et la gestion des rôles utilisateur de leur entreprise, ainsi que les opérations de volume et de données. Les clients peuvent disposer de rôles administratifs et déléguer des autorisations à d'autres utilisateurs au sein du même projet Google Cloud à l'aide des deux rôles prédéfinis de NetApp et Google Cloud (Administrateur et Viewer).

L'administrateur peut homologue à Cloud Volumes Service tout VPC dans le projet du client, que le client détermine approprié. Il est de la responsabilité du client de gérer l'accès à son abonnement à Google Cloud Marketplace et de gérer les VPC qui ont accès au plan de données.

Protection de SRE malveillante

Une préoccupation pouvant survenir est la façon dont Cloud Volumes Service protège-t-elle contre les scénarios dans lesquels il existe un SRE malveillant ou lorsque les informations d'identification des SRE ont été compromises ?

L'accès à l'environnement de production n'est possible qu'avec un nombre limité de SRE particuliers. Les privilèges administratifs sont en outre limités à une poignée d'administrateurs expérimentés. Toutes les actions réalisées par toute personne dans l'environnement de production Cloud Volumes Service sont consignées et toute anomalie affectant une activité de base ou suspecte est détectée par notre plateforme de veille centralisée des informations de sécurité et des événements (SIEM) pour les menaces. Ainsi, les actions malveillantes peuvent être suivies et atténuées avant que le back-end Cloud Volumes Service ne soit trop endommagé.

Cycle de vie du volume

Cloud Volumes Service gère uniquement les objets au sein du service, pas les données au sein des volumes. Seuls les clients qui accèdent aux volumes peuvent gérer les données, les listes de contrôle d'accès, les propriétaires de fichiers, etc. Les données de ces volumes sont chiffrées au repos et l'accès est limité aux locataires de l'instance Cloud Volumes Service.

Le cycle de vie des volumes pour Cloud Volumes Service est create-update-delete. Les volumes conservent des copies Snapshot de volumes jusqu'à leur suppression et seuls les administrateurs Cloud Volumes Service validés peuvent supprimer des volumes dans Cloud Volumes Service. Lorsqu'un administrateur demande la suppression d'un volume, une étape supplémentaire de la saisie du nom du volume est requise pour vérifier la suppression. Un volume est supprimé et ne peut plus être restauré.

Dans les cas où un contrat Cloud Volumes Service a été résilié, NetApp marque la suppression des volumes au bout d'une période donnée. Avant l'expiration de cette période, vous pouvez récupérer des volumes à la demande du client.

Certifications

Cloud volumes Services pour Google Cloud est actuellement certifié conforme aux normes ISO/IEC 27001:2013 et ISO/IEC 27018:2019. Le service a aussi récemment reçu son rapport d'attestation de type I de la SOC2. Pour plus d'informations sur l'engagement de NetApp en matière de sécurité et de confidentialité des données, consultez la page "Conformité : sécurité et confidentialité des données".

LE RGPD

Notre engagement en matière de confidentialité et de conformité avec le RGPD est disponible dans un certain nombre de nos "contrats clients", comme notre "Addenda relatif au traitement des données client", qui inclut le "Clauses contractuelles standard" Fourni par la Commission européenne. Nous prenons également ces engagements dans notre politique de confidentialité, soutenue par les valeurs fondamentales énoncées dans notre Code de conduite d'entreprise.

Informations complémentaires et coordonnées

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

- Documentation Google Cloud pour Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Service privé Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentation des produits NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Programme de module de validation cryptographique : NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- Solution NetApp pour ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- Tr-4616 : NFS Kerberos dans ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Contactez-nous

Dites-nous comment nous pourrions améliorer ce rapport technique.

Contactez-nous à l'adresse : doccomments@netapp.com. Incluez LE RAPPORT TECHNIQUE 4918 dans la ligne d'objet.

Informations sur le copyright

Informations sur les marques commerciales