



Démarrer avec Google Cloud

Cloud Volumes ONTAP

NetApp
February 26, 2026

Sommaire

Démarrer avec Google Cloud	1
Démarrage rapide de Cloud Volumes ONTAP dans Google Cloud	1
Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud	2
Choisissez une licence Cloud Volumes ONTAP	2
Choisissez une région prise en charge	2
Choisissez un type de machine pris en charge	2
Comprendre les limites de stockage	3
Dimensionnez votre système dans Google Cloud	3
Afficher les disques système par défaut	4
Recueillir des informations sur le réseau	4
Choisissez une vitesse d'écriture	5
Choisissez un profil d'utilisation du volume	5
Configurer la mise en réseau Google Cloud pour Cloud Volumes ONTAP	6
Exigences pour Cloud Volumes ONTAP	6
Exigences pour l'agent de console	18
Configurer VPC Service Controls pour déployer Cloud Volumes ONTAP dans Google Cloud	19
Comment les services NetApp communiquent avec les contrôles de service VPC	19
Images	19
Politiques de périmètre des contrôles de service VPC	20
Créer un compte de service Google Cloud pour Cloud Volumes ONTAP	21
Utilisation de clés de chiffrement gérées par le client avec Cloud Volumes ONTAP	24
Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud	25
Freemium	25
Licence basée sur la capacité	26
Abonnement Keystone	29
Licence basée sur les nœuds	30
Lancer Cloud Volumes ONTAP dans Google Cloud	30
Avant de commencer	30
Lancer un système à nœud unique dans Google Cloud	31
Lancer une paire HA dans Google Cloud	37
Vérification d'image de Google Cloud Platform	43
Découvrez comment l'image Google Cloud est vérifiée dans Cloud Volumes ONTAP	43
Convertir l'image Google Cloud au format brut pour Cloud Volumes ONTAP	44
Vérification de la signature de l'image	49

Démarrer avec Google Cloud

Démarrage rapide de Cloud Volumes ONTAP dans Google Cloud

Démarrez avec Cloud Volumes ONTAP dans Google Cloud en quelques étapes.

1

Créer un agent de console

Si vous n'avez pas de "Agent de console" Pourtant, vous devez en créer un. ["Découvrez comment créer un agent de console dans Google Cloud"](#)

Notez que si vous souhaitez déployer Cloud Volumes ONTAP dans un sous-réseau où aucun accès Internet n'est disponible, vous devez installer manuellement l'agent de console et accéder à la NetApp Console qui s'exécute sur cet agent de console. ["Découvrez comment installer manuellement l'agent de console dans un emplacement sans accès Internet"](#)

2

Planifiez votre configuration

La console propose des packages préconfigurés qui correspondent à vos exigences de charge de travail, ou vous pouvez créer votre propre configuration. Si vous choisissez votre propre configuration, vous devez comprendre les options qui s'offrent à vous.

["En savoir plus sur la planification de votre configuration"](#) .

3

Configurez votre réseau

1. Assurez-vous que votre VPC et vos sous-réseaux prendront en charge la connectivité entre l'agent de console et Cloud Volumes ONTAP.
2. Si vous prévoyez d'activer la hiérarchisation des données, ["configurer le sous-réseau Cloud Volumes ONTAP pour l'accès privé à Google"](#) .
3. Si vous déployez une paire HA, assurez-vous de disposer de quatre VPC, chacun avec son propre sous-réseau.
4. Si vous utilisez un VPC partagé, attribuez le rôle *Compute Network User* au compte de service de l'agent de la console.
5. Activez l'accès Internet sortant à partir du VPC cible pour NetApp AutoSupport.

Cette étape n'est pas requise si vous déployez Cloud Volumes ONTAP dans un emplacement où aucun accès Internet n'est disponible.

["En savoir plus sur les exigences de mise en réseau"](#) .

4

Configurer un compte de service

Cloud Volumes ONTAP nécessite un compte de service Google Cloud à deux fins. La première est lorsque vous activez ["hiérarchisation des données"](#) pour hiérarchiser les données froides vers un stockage d'objets à faible coût dans Google Cloud. La deuxième est lorsque vous activez le ["NetApp Backup and Recovery"](#) pour

sauvegarder des volumes sur un stockage d'objets à faible coût.

Vous pouvez configurer un compte de service et l'utiliser à ces deux fins. Le compte de service doit avoir le rôle **Administrateur de stockage**.

["Lisez les instructions étape par étape"](#) .

5

Activer les API Google Cloud

["Activez les API Google Cloud dans votre projet"](#). ["Ces API"](#), que vous avez peut-être déjà activées lors de la création de l'agent Console, sont nécessaires pour déployer Cloud Volumes ONTAP dans Google Cloud.

6

Lancer Cloud Volumes ONTAP à l'aide de la console

Cliquez sur **Ajouter un système**, sélectionnez le type de système que vous souhaitez déployer et suivez les étapes de l'assistant. ["Lisez les instructions étape par étape"](#) .

Liens connexes

- ["Création d'un agent de console"](#)
- ["Installation du logiciel agent de console sur un hôte Linux"](#)
- ["Autorisations Google Cloud pour l'agent de la console"](#)

Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud

Lorsque vous déployez Cloud Volumes ONTAP dans Google Cloud, vous pouvez choisir un système préconfiguré qui correspond à vos exigences de charge de travail ou créer votre propre configuration. Si vous choisissez votre propre configuration, vous devez comprendre les options qui s'offrent à vous.

Choisissez une licence Cloud Volumes ONTAP

Plusieurs options de licence sont disponibles pour Cloud Volumes ONTAP. Chaque option vous permet de choisir un modèle de consommation qui répond à vos besoins.

- ["En savoir plus sur les options de licence pour Cloud Volumes ONTAP"](#)
- ["Apprenez à configurer les licences"](#)

Choisissez une région prise en charge

Cloud Volumes ONTAP est pris en charge dans la plupart des régions Google Cloud. ["Afficher la liste complète des régions prises en charge"](#) .

Choisissez un type de machine pris en charge

Cloud Volumes ONTAP prend en charge plusieurs types de machines, selon le type de licence que vous choisissez.

["Configurations prises en charge pour Cloud Volumes ONTAP dans Google Cloud"](#)

Comprendre les limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP est liée à la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Vous devez être conscient de ces limites lorsque vous planifiez votre configuration.

["Limites de stockage pour Cloud Volumes ONTAP dans Google Cloud"](#)

Dimensionnez votre système dans Google Cloud

Le dimensionnement de votre système Cloud Volumes ONTAP peut vous aider à répondre aux exigences de performances et de capacité. Vous devez tenir compte de quelques points clés lors du choix d'un type de machine, d'un type de disque et d'une taille de disque :

Type de machine

Consultez les types de machines pris en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#). Consultez ensuite les informations détaillées de Google concernant chaque type de machine pris en charge. Adaptez vos exigences de charge de travail au nombre de vCPU et de mémoire pour le type de machine. Notez que chaque cœur de processeur augmente les performances du réseau.

Pour plus de détails, reportez-vous aux éléments suivants :

- ["Documentation Google Cloud : types de machines standard N1"](#)
- ["Documentation Google Cloud : Performances"](#)

Types de disques

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent que Cloud Volumes ONTAP utilise pour un disque. Le type de disque peut être l'un des suivants :

- *Disques persistants SSD zonaux* : les disques persistants SSD sont idéaux pour les charges de travail qui nécessitent des taux élevés d'IOPS aléatoires.
- *Disques persistants équilibrés par zone* : ces SSD équilibrent les performances et les coûts en fournissant des IOPS par Go inférieurs.
- *Disques persistants standard zonaux* : Les disques persistants standard sont économiques et peuvent gérer des opérations de lecture/écriture séquentielles.

Pour plus de détails, reportez-vous à la ["Documentation Google Cloud : Disques persistants zonaux \(standard et SSD\)"](#).

Taille du disque

Vous devez choisir une taille de disque initiale lorsque vous déployez un système Cloud Volumes ONTAP. Après cela, vous pouvez laisser la NetApp Console gérer la capacité d'un système pour vous, mais si vous souhaitez créer vous-même des agrégats, tenez compte des points suivants :

- Tous les disques d'un agrégat doivent avoir la même taille.
- Déterminez l'espace dont vous avez besoin, tout en prenant en compte les performances.
- Les performances des disques persistants évoluent automatiquement en fonction de la taille du disque et du nombre de vCPU disponibles pour le système.

Pour plus de détails, reportez-vous aux éléments suivants :

- ["Documentation Google Cloud : Disques persistants zonaux \(standard et SSD\)"](#)
- ["Documentation Google Cloud : Optimisation des performances des disques persistants et des SSD locaux"](#)

Afficher les disques système par défaut

En plus du stockage des données utilisateur, la console achète également du stockage cloud pour les données système Cloud Volumes ONTAP (données de démarrage, données racine, données principales et NVRAM). À des fins de planification, il peut être utile de vérifier ces détails avant de déployer Cloud Volumes ONTAP.

- ["Afficher les disques par défaut pour les données système Cloud Volumes ONTAP dans Google Cloud"](#) .
- ["Documentation Google Cloud : Présentation des quotas cloud"](#)

Google Cloud Compute Engine applique des quotas sur l'utilisation des ressources. Vous devez donc vous assurer que vous n'avez pas atteint votre limite avant de déployer Cloud Volumes ONTAP.



L'agent de console nécessite également un disque système. ["Afficher les détails sur la configuration par défaut de l'agent de console"](#) .

Recueillir des informations sur le réseau

Lorsque vous déployez Cloud Volumes ONTAP dans Google Cloud, vous devez spécifier les détails de votre réseau virtuel. Vous pouvez utiliser une feuille de calcul pour recueillir les informations auprès de votre administrateur.

Informations réseau pour un système à nœud unique

Informations Google Cloud	Votre valeur
Région	
Zone	
réseau VPC	
Sous-réseau	
Politique de pare-feu (si vous utilisez la vôtre)	

Informations réseau pour une paire HA dans plusieurs zones

Informations Google Cloud	Votre valeur
Région	
Zone pour le nœud 1	
Zone pour le nœud 2	
Zone pour le médiateur	
VPC-0 et sous-réseau	
VPC-1 et sous-réseau	

Informations Google Cloud	Votre valeur
VPC-2 et sous-réseau	
VPC-3 et sous-réseau	
Politique de pare-feu (si vous utilisez la vôtre)	

Informations réseau pour une paire HA dans une seule zone

Informations Google Cloud	Votre valeur
Région	
Zone	
VPC-0 et sous-réseau	
VPC-1 et sous-réseau	
VPC-2 et sous-réseau	
VPC-3 et sous-réseau	
Politique de pare-feu (si vous utilisez la vôtre)	

Choisissez une vitesse d'écriture

La console vous permet de choisir un paramètre de vitesse d'écriture pour Cloud Volumes ONTAP, à l'exception des paires haute disponibilité (HA) dans Google Cloud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés, ainsi que les risques et les recommandations lors de l'utilisation d'une vitesse d'écriture élevée. ["En savoir plus sur la vitesse d'écriture"](#).

Choisissez un profil d'utilisation du volume

ONTAP inclut plusieurs fonctionnalités d'efficacité de stockage qui peuvent réduire la quantité totale de stockage dont vous avez besoin. Lorsque vous créez un volume dans la console, vous pouvez choisir un profil qui active ces fonctionnalités ou un profil qui les désactive. Vous devriez en savoir plus sur ces fonctionnalités pour vous aider à décider quel profil utiliser.

Les fonctionnalités d'efficacité du stockage NetApp offrent les avantages suivants :

Provisionnement léger

Présente plus de stockage logique aux hôtes ou aux utilisateurs que ce dont vous disposez réellement dans votre pool de stockage physique. Au lieu de préallouer l'espace de stockage, l'espace de stockage est alloué dynamiquement à chaque volume au fur et à mesure que les données sont écrites.

Déduplication

Améliore l'efficacité en localisant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins en capacité de stockage en éliminant les blocs de données redondants qui résident dans le même volume.

Compression

Réduit la capacité physique requise pour stocker les données en compressant les données dans un volume sur le stockage principal, secondaire et d'archive.

Configurer la mise en réseau Google Cloud pour Cloud Volumes ONTAP

La NetApp Console gère la configuration des composants réseau pour Cloud Volumes ONTAP, tels que les adresses IP, les masques de réseau et les itinéraires. Vous devez vous assurer que l'accès Internet sortant est disponible, que suffisamment d'adresses IP privées sont disponibles, que les bonnes connexions sont en place, etc.

Si vous souhaitez déployer une paire HA, vous devez [découvrez comment fonctionnent les paires HA dans Google Cloud](#).

Exigences pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans Google Cloud.

Exigences spécifiques aux systèmes à nœud unique

Si vous souhaitez déployer un système à nœud unique, assurez-vous que votre réseau réponde aux exigences suivantes.

Un VPC

Un cloud privé virtuel (VPC) est nécessaire pour un système à nœud unique.

Adresses IP privées

Pour un système à nœud unique dans Google Cloud, la NetApp Console attribue des adresses IP privées aux éléments suivants :

- Nœud
- Cluster
- Machine virtuelle de stockage
- Données NAS LIF
- Données iSCSI LIF

Vous pouvez ignorer la création du LIF de gestion de la machine virtuelle de stockage (SVM) si vous déployez Cloud Volumes ONTAP à l'aide de l'API et spécifiez l'indicateur suivant :

```
skipSvmManagementLif: true
```



Un LIF est une adresse IP associée à un port physique. Un LIF de gestion de machine virtuelle de stockage (SVM) est requis pour les outils de gestion tels que SnapCenter.

Exigences spécifiques aux paires HA

Si vous souhaitez déployer une paire HA, assurez-vous que votre réseau répond aux exigences suivantes.

Une ou plusieurs zones

Vous pouvez garantir la haute disponibilité de vos données en déployant une configuration HA sur plusieurs

zones ou dans une seule zone. La console vous invite à choisir plusieurs zones ou une seule zone lorsque vous créez la paire HA.

- Zones multiples (recommandé)

Le déploiement d'une configuration HA sur trois zones garantit une disponibilité continue des données en cas de panne dans une zone. Notez que les performances d'écriture sont légèrement inférieures à celles de l'utilisation d'une seule zone, mais elles sont minimales.

- Zone unique

Lorsqu'elle est déployée dans une zone unique, une configuration Cloud Volumes ONTAP HA utilise une stratégie de placement répartie. Cette politique garantit qu'une configuration HA est protégée contre un point de défaillance unique au sein de la zone, sans avoir à utiliser des zones distinctes pour obtenir l'isolement des pannes.

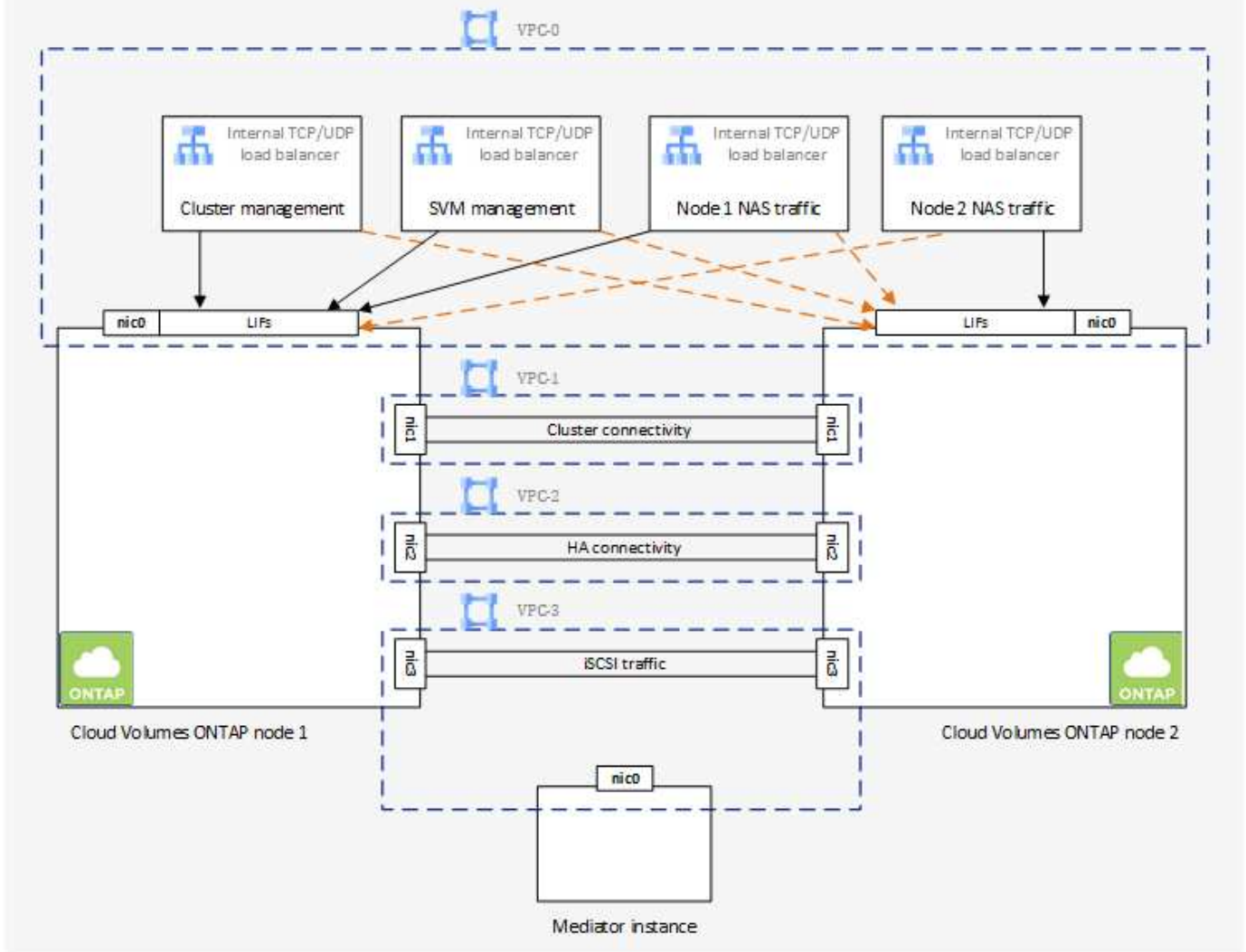
Ce modèle de déploiement réduit vos coûts car il n'y a pas de frais de sortie de données entre les zones.

Quatre clouds privés virtuels

Quatre clouds privés virtuels (VPC) sont nécessaires pour une configuration HA. Quatre VPC sont requis car Google Cloud exige que chaque interface réseau réside dans un réseau VPC distinct.

La console vous invite à choisir quatre VPC lorsque vous créez la paire HA :

- VPC-0 pour les connexions entrantes aux données et aux nœuds
- VPC-1, VPC-2 et VPC-3 pour la communication interne entre les nœuds et le médiateur HA



Sous-réseaux

Un sous-réseau privé est requis pour chaque VPC.

Si vous placez l'agent de console dans VPC-0, vous devrez activer l'accès privé à Google sur le sous-réseau pour accéder aux API et activer la hiérarchisation des données.

Les sous-réseaux de ces VPC doivent avoir des plages CIDR distinctes. Ils ne peuvent pas avoir de plages CIDR qui se chevauchent.

Adresses IP privées

La console alloue automatiquement le nombre requis d'adresses IP privées à Cloud Volumes ONTAP dans Google Cloud. Vous devez vous assurer que votre réseau dispose de suffisamment d'adresses privées disponibles.

Le nombre d'interfaces logiques (LIF) allouées à Cloud Volumes ONTAP dépend du type de système déployé : mono-nœud ou paire haute disponibilité. Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est requise pour les outils de gestion tels que SnapCenter.

- **Nœud unique** NetApp Console alloue 4 adresses IP à un système à nœud unique :

- Gestion des nœuds LIF
- Gestion des clusters LIF
- LIF de données iSCSI



Un LIF iSCSI fournit un accès client via le protocole iSCSI et est utilisé par le système pour d'autres flux de travail réseau importants. Ces LIF sont obligatoires et ne doivent pas être supprimés.

- NAS LIF

Vous pouvez ignorer la création du LIF de gestion de la machine virtuelle de stockage (SVM) si vous déployez Cloud Volumes ONTAP à l'aide de l'API et spécifiez l'indicateur suivant :

```
skipSvmManagementLif: true
```

- **Paire HA** La console alloue 12 à 13 adresses IP à une paire HA :

- 2 LIF de gestion de nœuds (e0a)
- 1 Gestion des clusters LIF (e0a)
- 2 LIF iSCSI (e0a)



Un LIF iSCSI fournit un accès client via le protocole iSCSI et est utilisé par le système pour d'autres flux de travail réseau importants. Ces LIF sont obligatoires et ne doivent pas être supprimés.

- 1 ou 2 NAS LIF (e0a)
- 2 LIF en cluster (e0b)
- 2 adresses IP d'interconnexion HA (e0c)
- 2 adresses IP iSCSI RSM (e0d)

Vous pouvez ignorer la création du LIF de gestion de la machine virtuelle de stockage (SVM) si vous déployez Cloud Volumes ONTAP à l'aide de l'API et spécifiez l'indicateur suivant :

```
skipSvmManagementLif: true
```

Équilibreurs de charge internes

La console crée quatre équilibreurs de charge internes Google Cloud (TCP/UDP) qui gèrent le trafic entrant vers la paire Cloud Volumes ONTAP HA. Aucune configuration n'est requise de votre part. Nous avons répertorié cela comme une exigence simplement pour vous informer du trafic réseau et pour atténuer tout problème de sécurité.

Un équilibreur de charge est destiné à la gestion des clusters, un autre à la gestion des machines virtuelles de stockage (SVM), un autre au trafic NAS vers le nœud 1 et le dernier au trafic NAS vers le nœud 2.

La configuration de chaque équilibreur de charge est la suivante :

- Une adresse IP privée partagée
- Un bilan de santé mondial

Par défaut, les ports utilisés par le contrôle d'état sont 63001, 63002 et 63003.

- Un service backend TCP régional
- Un service backend UDP régional
- Une règle de transfert TCP
- Une règle de transfert UDP
- L'accès global est désactivé

Même si l'accès global est désactivé par défaut, son activation après le déploiement est prise en charge. Nous l'avons désactivé car le trafic interrégional aura des latences considérablement plus élevées. Nous voulions nous assurer que vous n'ayez pas d'expérience négative en raison de montages interrégionaux accidentels. L'activation de cette option est spécifique aux besoins de votre entreprise.

VPC partagés

Cloud Volumes ONTAP et l'agent de console sont pris en charge dans un VPC partagé Google Cloud ainsi que dans les VPC autonomes.

Pour un système à nœud unique, le VPC peut être soit un VPC partagé, soit un VPC autonome.

Pour une paire HA, quatre VPC sont nécessaires. Chacun de ces VPC peut être partagé ou autonome. Par exemple, VPC-0 peut être un VPC partagé, tandis que VPC-1, VPC-2 et VPC-3 peuvent être des VPC autonomes.

Un VPC partagé vous permet de configurer et de gérer de manière centralisée des réseaux virtuels sur plusieurs projets. Vous pouvez configurer des réseaux VPC partagés dans le *projet hôte* et déployer l'agent de console et les instances de machine virtuelle Cloud Volumes ONTAP dans un *projet de service*.

["Documentation Google Cloud : Présentation du VPC partagé"](#) .

["Consultez les autorisations VPC partagées requises décrites dans le déploiement de l'agent de console."](#)

Mise en miroir des paquets dans les VPC

["Mise en miroir des paquets"](#) doit être désactivé dans le sous-réseau Google Cloud dans lequel vous déployez Cloud Volumes ONTAP.

Accès Internet sortant

Les systèmes Cloud Volumes ONTAP nécessitent un accès Internet sortant pour accéder aux points de terminaison externes pour diverses fonctions. Cloud Volumes ONTAP ne peut pas fonctionner correctement si ces points de terminaison sont bloqués dans des environnements avec des exigences de sécurité strictes.

L'agent de console contacte également plusieurs points de terminaison pour les opérations quotidiennes. Pour plus d'informations sur les points de terminaison, reportez-vous à ["Afficher les points de terminaison contactés depuis l'agent de la console"](#) et ["Préparer le réseau pour l'utilisation de la console"](#) .

Points de terminaison Cloud Volumes ONTAP

Cloud Volumes ONTAP utilise ces points de terminaison pour communiquer avec divers services.

Points de terminaison	Applicable pour	But	Mode de déploiement	Impact si le point de terminaison n'est pas disponible
\ https://netapp-cloud-account.auth0.com	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : • Services Cloud Volumes ONTAP • Services ONTAP • Protocoles et services proxy
\ https://api.bluexp.net/app.com/tenancy	Location	Utilisé pour récupérer la ressource Cloud Volumes ONTAP à partir de la console pour autoriser les ressources et les utilisateurs.	Modes standard et restreint.	Les ressources Cloud Volumes ONTAP et les utilisateurs ne sont pas autorisés.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilisé pour envoyer des données de télémétrie AutoSupport au support NetApp .	Modes standard et restreint.	Les informations AutoSupport ne sont toujours pas livrées.

Points de terminaison	Applicable pour	But	Mode de déploiement	Impact si le point de terminaison n'est pas disponible
https://cloudbuild.googleapis.com/v1 (pour les déploiements en mode privé uniquement) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (utilisation commerciale).	Communication avec les services Google Cloud.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Google Cloud pour effectuer des opérations spécifiques pour la console dans Google Cloud.

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP dans Google Cloud et des systèmes ONTAP dans d'autres réseaux, vous devez disposer d'une connexion VPN entre le VPC et l'autre réseau, par exemple, votre réseau d'entreprise.

"[Documentation Google Cloud : Présentation du VPN Cloud](#)".

Règles du pare-feu

La console crée des règles de pare-feu Google Cloud qui incluent les règles entrantes et sortantes dont Cloud Volumes ONTAP a besoin pour fonctionner correctement. Vous souhaitez peut-être vous référer aux ports à

des fins de test ou si vous préférez utiliser vos propres règles de pare-feu.

Les règles de pare-feu pour Cloud Volumes ONTAP nécessitent des règles entrantes et sortantes. Si vous déployez une configuration HA, voici les règles de pare-feu pour Cloud Volumes ONTAP dans VPC-0.

Notez que deux ensembles de règles de pare-feu sont requis pour une configuration HA :

- Un ensemble de règles pour les composants HA dans VPC-0. Ces règles permettent l'accès aux données de Cloud Volumes ONTAP.
- Un autre ensemble de règles pour les composants HA dans VPC-1, VPC-2 et VPC-3. Ces règles sont ouvertes à la communication entrante et sortante entre les composants HA. [Apprendre encore plus](#) .



Vous recherchez des informations sur l'agent Console ? ["Afficher les règles de pare-feu pour l'agent de console"](#)

Règles entrantes

Lorsque vous ajoutez un système Cloud Volumes ONTAP , vous pouvez choisir le filtre source pour la stratégie de pare-feu prédéfinie lors du déploiement :

- **VPC sélectionné uniquement** : le filtre source pour le trafic entrant est la plage de sous-réseaux du VPC pour le système Cloud Volumes ONTAP et la plage de sous-réseaux du VPC où réside l'agent de la console. C'est l'option recommandée.
- **Tous les VPC** : le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.

Si vous utilisez votre propre stratégie de pare-feu, assurez-vous d'ajouter tous les réseaux qui doivent communiquer avec Cloud Volumes ONTAP, mais assurez-vous également d'ajouter les deux plages d'adresses pour permettre à l'équilibreur de charge Google interne de fonctionner correctement. Ces adresses sont 130.211.0.0/22 et 35.191.0.0/16. Pour plus d'informations, reportez-vous à la ["Documentation Google Cloud : Règles de pare-feu de l'équilibreur de charge"](#) .

Protocole	Port	But
Tous les ICMP	Tous	Ping de l'instance
HTTP	80	Accès HTTP à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
HTTPS	443	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole simple de gestion de réseau
TCP	445	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
TCP	635	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS

Protocole	Port	But
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Moniteur d'état du réseau pour NFS
TCP	10000	Sauvegarde à l'aide de NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
TCP	63001-63050	Ports de sonde d'équilibrage de charge pour déterminer quel nœud est sain (requis pour les paires HA uniquement)
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole simple de gestion de réseau
UDP	635	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Moniteur d'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de sortie de base. Si vous avez besoin de règles plus rigides, utilisez les règles sortantes avancées.

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les ICMP	Tous	Tout le trafic sortant
Tout TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par Cloud Volumes ONTAP. Les clusters Cloud Volumes ONTAP utilisent les ports suivants pour réguler le trafic des nœuds.



La source est l'interface (adresse IP) du système Cloud Volumes ONTAP .

Service	Protocole	Port	Source	Destination	But
Active Directory	TCP	88	Gestion des nœuds LIF	Forêt Active Directory	Authentification Kerberos V
	UDP	137	Gestion des nœuds LIF	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Gestion des nœuds LIF	Forêt Active Directory	Service de datagramme NetBIOS
	TCP	139	Gestion des nœuds LIF	Forêt Active Directory	Session de service NetBIOS
	TCP et UDP	389	Gestion des nœuds LIF	Forêt Active Directory	LDAP
	TCP	445	Gestion des nœuds LIF	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
	TCP	464	Gestion des nœuds LIF	Forêt Active Directory	Kerberos V changer et définir le mot de passe (SET_CHANGE)
	UDP	464	Gestion des nœuds LIF	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	Gestion des nœuds LIF	Forêt Active Directory	Kerberos V changer et définir le mot de passe (RPCSEC_GSS)
	TCP	88	Données LIF (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V
	UDP	137	Données LIF (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Données LIF (NFS, CIFS)	Forêt Active Directory	Service de datagramme NetBIOS
	TCP	139	Données LIF (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP et UDP	389	Données LIF (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	Données LIF (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
	TCP	464	Données LIF (NFS, CIFS)	Forêt Active Directory	Kerberos V changer et définir le mot de passe (SET_CHANGE)
	UDP	464	Données LIF (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	Données LIF (NFS, CIFS)	Forêt Active Directory	Kerberos V changer et définir le mot de passe (RPCSEC_GSS)

Service	Protocole	Port	Source	Destination	But
AutoSupport	HTTPS	443	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (HTTPS est la valeur par défaut)
	HTTP	80	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (uniquement si le protocole de transport est modifié de HTTPS à HTTP)
	TCP	3128	Gestion des nœuds LIF	Agent de console	Envoi de messages AutoSupport via un serveur proxy sur l'agent de la console, si une connexion Internet sortante n'est pas disponible
Sauvegarde de configuration	HTTP	80	Gestion des nœuds LIF	http://<adresse IP de l'agent de la console>/occm/offboxconfig	Envoyer des sauvegardes de configuration à l'agent de la console. "Documentation ONTAP"
DHCP	UDP	68	Gestion des nœuds LIF	DHCP	Client DHCP pour la première configuration
DHCPs	UDP	67	Gestion des nœuds LIF	DHCP	serveur DHCP
DNS	UDP	53	Gestion des nœuds LIF et LIF de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	Gestion des nœuds LIF	Serveurs de destination	Copie NDMP
SMTP	TCP	25	Gestion des nœuds LIF	Serveur de messagerie	Alertes SMTP, peuvent être utilisées pour AutoSupport
SNMP	TCP	161	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	UDP	161	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	TCP	162	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	UDP	162	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
SnapMirror	TCP	11104	LIF intercluster	LIF intercluster ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	LIF intercluster	LIF intercluster ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	Gestion des nœuds LIF	Serveur Syslog	Messages de transfert Syslog

Règles pour VPC-1, VPC-2 et VPC-3

Dans Google Cloud, une configuration HA est déployée sur quatre VPC. Les règles de pare-feu nécessaires à la configuration HA dans VPC-0 sont [répertorié ci-dessus pour Cloud Volumes ONTAP](#).

Pendant ce temps, les règles de pare-feu prédéfinies créées pour les instances de VPC-1, VPC-2 et VPC-3 permettent la communication entrante sur *tous* les protocoles et ports. Ces règles permettent la communication entre les nœuds HA.

La communication entre les nœuds HA et le médiateur HA s'effectue via le port 3260 (iSCSI).



Pour permettre une vitesse d'écriture élevée pour les nouveaux déploiements de paires Google Cloud HA, une unité de transmission maximale (MTU) d'au moins 8 896 octets est requise pour VPC-1, VPC-2 et VPC-3. Si vous choisissez de mettre à niveau les VPC-1, VPC-2 et VPC-3 existants vers un MTU de 8 896 octets, vous devez arrêter tous les systèmes HA existants utilisant ces VPC pendant le processus de configuration.

Configuration d'Infrastructure Manager pour les déploiements en mode privé

Si vous souhaitez déployer Cloud Volumes ONTAP 9.16.1 ou une version ultérieure en mode privé, vous devez effectuer quelques modifications de configuration afin que Cloud Volumes ONTAP puisse utiliser Google Cloud Infrastructure Manager comme service de déploiement au lieu de Deployment Manager, que Google finira par abandonner.

Avant de commencer

- Assurez-vous que votre système Cloud Volumes ONTAP est en version 9.16.1 ou ultérieure. Si ce n'est pas le cas, mettez votre système à niveau. Consultez "[Mettre à niveau Cloud Volumes ONTAP](#)" pour obtenir des instructions.
- Assurez-vous que les API Google Cloud sont activées. Voir "[Activer les API Google Cloud](#)".
- Assurez-vous que l'API Cloud Build est activée. Consultez "[Activez l'API Cloud Build ici](#)".
- Vérifiez que le compte de service de l'agent Console dispose de toutes les autorisations standard. Assurez-vous également que le compte de service dispose des autorisations `cloudbuild.workerpools.get` et `cloudbuild.workerpools.list`. Reportez-vous à "[Autorisations Google Cloud pour l'agent de la console](#)".

Étapes

1. Créez un pool de workers privé avec cette configuration dans la même région que les déploiements Cloud Volumes ONTAP. Pour obtenir des informations sur la création d'un pool de workers privé, consultez "[Google Cloud documentation : Créer et gérer des pools privés](#)" et "[Tarification Google Cloud Build](#)".

Le pool de travailleurs doit avoir la configuration suivante :

- Type de machine : e2-medium
- Taille du disque : 100 Go
- Attribuer une adresse IP externe : False
- Réseau : Par défaut ou privé.
- Le sous-réseau configuré pour accéder "[API Google](#)". Procédez comme suit pour garantir que le sous-réseau peut accéder aux API Google :
 - i. Assurez-vous que « Private Google Access » est activé pour le sous-réseau.
 - ii. Accédez à **Niveau VPC Network > Onglet Private Service Access > Allocated IP ranges for**

services.

- iii. Sélectionnez **Allocate IP range** et allouez la plage d'adresses IP internes pour la connexion privée au Google Compute Service.
 - iv. Dans **Connexion privée aux services**, sélectionnez **Créer une connexion**.
 - v. Sélectionnez **Connected service producer = Google Cloud Platform**.
 - vi. Attribuez l'allocation à la plage d'adresses IP de connexion privée que vous avez créée à l'étape précédente.
2. Déployez ce pool de nœuds de calcul et maintenez-le actif pour la gestion de Cloud Volumes ONTAP. Google Cloud utilise ce pool pour exécuter toutes les opérations Terraform dans un environnement isolé.
 3. Lors du déploiement de Cloud Volumes ONTAP en mode privé, sélectionnez le nom de ce worker pool dans le champ **GCP Worker Pool**. Consultez ["Lancer Cloud Volumes ONTAP dans Google Cloud"](#) pour obtenir des instructions.

Exigences pour l'agent de console

Si vous n'avez pas encore créé d'agent de console, vous devez vérifier les exigences réseau.

- ["Afficher les exigences réseau pour l'agent de console"](#)
- ["Règles de pare-feu dans Google Cloud"](#)

Configurations réseau pour prendre en charge le proxy de l'agent de console

Vous pouvez utiliser les serveurs proxy configurés pour l'agent de console pour activer l'accès Internet sortant à partir de Cloud Volumes ONTAP. La console prend en charge deux types de proxys :

- **Proxy explicite** : le trafic sortant de Cloud Volumes ONTAP utilise l'adresse HTTP du serveur proxy spécifié lors de la configuration du proxy de l'agent de console. L'administrateur de l'agent de la console peut également avoir configuré les informations d'identification de l'utilisateur et les certificats d'autorité de certification racine pour une authentification supplémentaire. Si un certificat d'autorité de certification racine est disponible pour le proxy explicite, assurez-vous d'obtenir et de télécharger le même certificat sur votre système Cloud Volumes ONTAP à l'aide de l' ["ONTAP CLI : installation du certificat de sécurité"](#) commande.
- **Proxy transparent** : le réseau est configuré pour acheminer automatiquement le trafic sortant de Cloud Volumes ONTAP via le proxy de l'agent de la console. Lors de la configuration d'un proxy transparent, l'administrateur de l'agent de la console doit fournir uniquement un certificat d'autorité de certification racine pour la connectivité à partir de Cloud Volumes ONTAP, et non l'adresse HTTP du serveur proxy. Assurez-vous d'obtenir et de télécharger le même certificat d'autorité de certification racine sur votre système Cloud Volumes ONTAP à l'aide de ["ONTAP CLI : installation du certificat de sécurité"](#) commande.

Pour plus d'informations sur la configuration des serveurs proxy pour l'agent de console, reportez-vous à la ["Configurer un agent de console pour utiliser un serveur proxy"](#) .

Configurer les balises réseau pour Cloud Volumes ONTAP dans Google Cloud

Lors de la configuration du proxy transparent de l'agent de la console, l'administrateur ajoute une balise réseau pour Google Cloud. Vous devez obtenir et ajouter manuellement la même balise réseau pour votre configuration Cloud Volumes ONTAP . Cette balise est nécessaire au bon fonctionnement du serveur proxy.

1. Dans la console Google Cloud, localisez votre système Cloud Volumes ONTAP.
2. Accédez à **Détails > Réseau > Balises réseau**.

3. Ajoutez la balise utilisée pour l'agent de console et enregistrez la configuration.

Sujets connexes

- ["Vérifier la configuration AutoSupport pour Cloud Volumes ONTAP"](#)
- ["En savoir plus sur les ports internes ONTAP"](#) .

Configurer VPC Service Controls pour déployer Cloud Volumes ONTAP dans Google Cloud

Lorsque vous choisissez de verrouiller votre environnement Google Cloud avec VPC Service Controls, vous devez comprendre comment NetApp Console et Cloud Volumes ONTAP interagissent avec les API Google Cloud, ainsi que comment configurer votre périmètre de service pour déployer la console et Cloud Volumes ONTAP.

Les contrôles de service VPC vous permettent de contrôler l'accès aux services gérés par Google en dehors d'un périmètre approuvé, de bloquer l'accès aux données à partir d'emplacements non approuvés et d'atténuer les risques de transfert de données non autorisé. ["En savoir plus sur les contrôles de service VPC de Google Cloud"](#) .

Comment les services NetApp communiquent avec les contrôles de service VPC

La console communique directement avec les API Google Cloud. Cela est déclenché soit à partir d'une adresse IP externe en dehors de Google Cloud (par exemple, à partir de `api.services.cloud.netapp.com`), soit dans Google Cloud à partir d'une adresse interne attribuée à l'agent de la console.

Selon le style de déploiement de l'agent de console, certaines exceptions peuvent devoir être prévues pour votre périmètre de service.

Images

Cloud Volumes ONTAP et la Console utilisent tous deux des images provenant d'un projet au sein de Google Cloud qui est géré par NetApp. Cela peut affecter le déploiement de l'agent de la Console et de Cloud Volumes ONTAP, si votre organisation a une politique qui bloque l'utilisation d'images qui ne sont pas hébergées au sein de l'organisation.

Vous pouvez déployer un agent de console manuellement à l'aide de la méthode d'installation manuelle, mais Cloud Volumes ONTAP devra également extraire des images du projet NetApp . Vous devez fournir une liste autorisée pour déployer un agent de console et Cloud Volumes ONTAP.

Déploiement d'un agent de console

L'utilisateur qui déploie un agent de console doit pouvoir référencer une image hébergée dans le projectId `netapp-cloudmanager` et le numéro de projet `14190056516`.

Déploiement de Cloud Volumes ONTAP

- Le compte de service de la console doit référencer une image hébergée dans le projectId `netapp-cloudmanager` et le numéro de projet `14190056516` du projet de service.
- Le compte de service de l'agent de service Google API par défaut doit référencer une image hébergée dans le projectId `netapp-cloudmanager` et le numéro de projet `14190056516` du projet de service.

Des exemples de règles nécessaires pour extraire ces images avec VPC Service Controls sont définis ci-dessous.

Politiques de périmètre des contrôles de service VPC

Les politiques permettent de déroger aux règles de contrôle des services VPC. Pour plus d'informations sur les politiques, veuillez consulter la ["Documentation relative à la politique de contrôle des services VPC de Google Cloud"](#).

Pour définir les stratégies requises par la console, accédez à votre périmètre VPC Service Controls au sein de votre organisation et ajoutez les stratégies suivantes. Les champs doivent correspondre aux options indiquées dans la page de stratégie VPC Service Controls. Notez également que **toutes** les règles sont obligatoires et que les paramètres **OU** doivent être utilisés dans l'ensemble de règles.

Règles d'entrée

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
    Service methods: All actions
    Service name: compute.googleapis.com
    Service methods: All actions
```

OU

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

OU

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

Règles de sortie

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



Le numéro de projet décrit ci-dessus est le projet *netapp-cloudmanager* utilisé par NetApp pour stocker des images pour l'agent de console et pour Cloud Volumes ONTAP.

Créer un compte de service Google Cloud pour Cloud Volumes ONTAP

Cloud Volumes ONTAP nécessite un compte de service Google Cloud à deux fins. La première est lorsque vous activez "[hiérarchisation des données](#)" pour hiérarchiser les données froides vers un stockage d'objets à faible coût dans Google Cloud. La deuxième est lorsque vous activez le "[NetApp Backup and Recovery](#)" pour sauvegarder des volumes sur un stockage d'objets à faible coût.

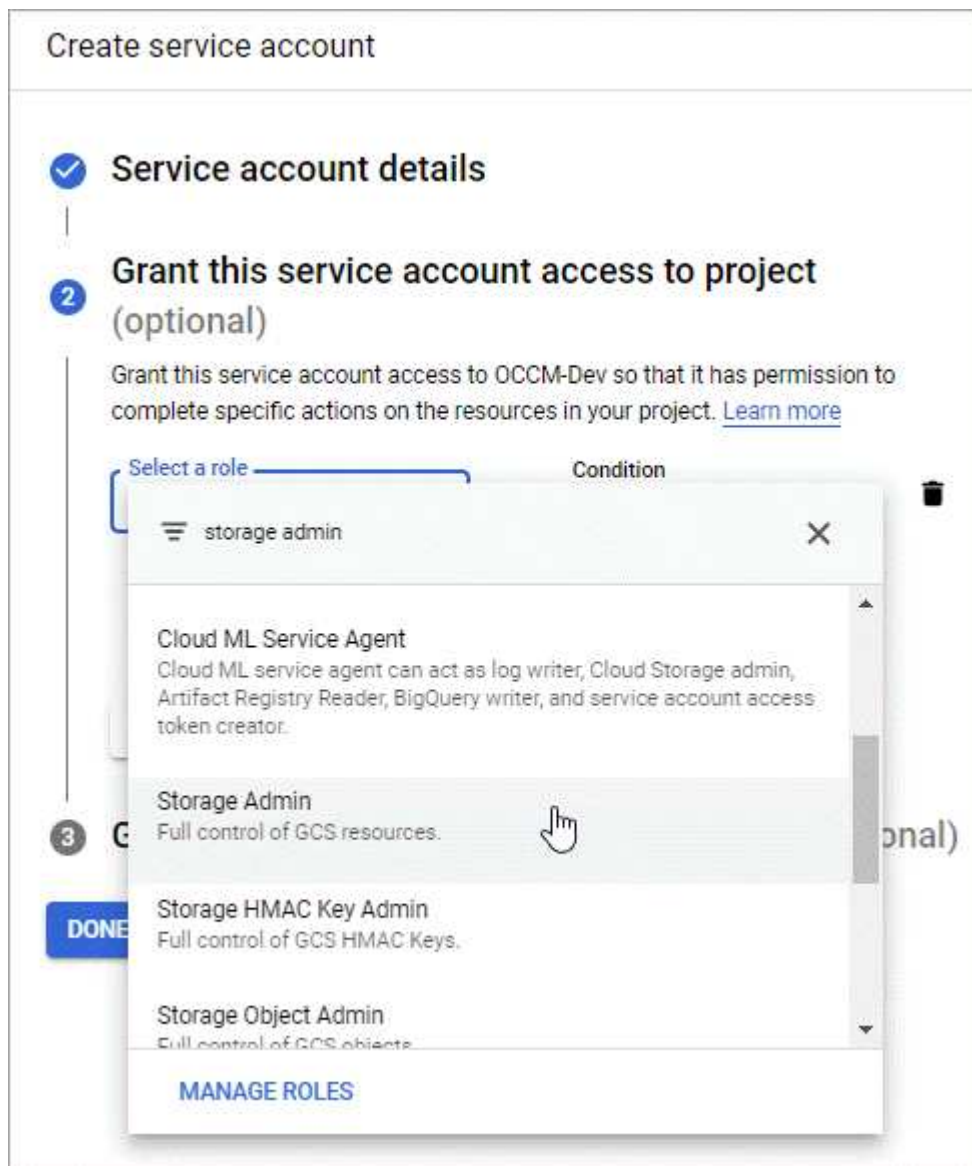
Cloud Volumes ONTAP utilise le compte de service pour accéder et gérer un bucket pour les données hiérarchisées et un autre bucket pour les sauvegardes.

Vous pouvez configurer un compte de service et l'utiliser à ces deux fins. Le compte de service doit avoir le rôle **Administrateur de stockage**.

Étapes

1. Dans la console Google Cloud, "[aller à la page Comptes de service](#)".

2. Sélectionnez votre projet.
3. Cliquez sur **Créer un compte de service** et fournissez les informations requises.
 - a. **Détails du compte de service** : saisissez un nom et une description.
 - b. **Accorder à ce compte de service l'accès au projet** : Sélectionnez le rôle **Administrateur de stockage**.



- c. **Accorder aux utilisateurs l'accès à ce compte de service** : ajoutez le compte de service de l'agent de console en tant qu'*utilisateur de compte de service* à ce nouveau compte de service.

Cette étape est requise uniquement pour la hiérarchisation des données. Ce n'est pas nécessaire pour la sauvegarde et la récupération.

Create service account

✓

Service account details

|

✓

Grant this service account access to project (optional)

|

3

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com ✕ ?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

?

Grant users the permission to administer this service account

DONE

CANCEL

Quelle est la prochaine étape ?

Vous devrez sélectionner le compte de service ultérieurement lorsque vous créerez un système Cloud Volumes ONTAP .

Details and Credentials

default-project

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

Utilisation de clés de chiffrement gérées par le client avec Cloud Volumes ONTAP

Bien que Google Cloud Storage chiffre toujours vos données avant qu'elles ne soient écrites sur le disque, vous pouvez utiliser les API pour créer un système Cloud Volumes ONTAP qui utilise des *clés de chiffrement gérées par le client*. Il s'agit de clés que vous générez et gérez dans GCP à l'aide du service Cloud Key Management.

Étapes

1. Assurez-vous que le compte de service de l'agent de console dispose des autorisations appropriées au niveau du projet, dans le projet où la clé est stockée.

Les autorisations sont fournies dans le ["les autorisations du compte de service par défaut"](#) , mais peut ne pas s'appliquer si vous utilisez un autre projet pour le service de gestion des clés cloud.

Les autorisations sont les suivantes :

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

2. Assurez-vous que le compte de service pour le ["Agent de service Google Compute Engine"](#) dispose des

autorisations Cloud KMS Encrypter/Decrypter sur la clé.

Le nom du compte de service utilise le format suivant : « service-[numéro_de_projet_service]@compute-system.iam.gserviceaccount.com ».

["Documentation Google Cloud : Utilisation d'IAM avec Cloud KMS – Attribution de rôles sur une ressource"](#)

3. Obtenez l'« id » de la clé en appelant la commande get pour le `/gcp/vsa/metadata/gcp-encryption-keys` Appel d'API ou en choisissant « Copier le nom de la ressource » sur la clé dans la console GCP.
 4. Si vous utilisez des clés de chiffrement gérées par le client et que vous hiérarchisez les données vers le stockage d'objets, la NetApp Console tente d'utiliser les mêmes clés que celles utilisées pour chiffrer les disques persistants. Mais vous devrez d'abord activer les buckets Google Cloud Storage pour utiliser les clés :
 - a. Recherchez l'agent de service Google Cloud Storage en suivant les instructions ["Documentation Google Cloud : Obtenir l'agent de service Cloud Storage"](#) .
 - b. Accédez à la clé de chiffrement et attribuez à l'agent de service Google Cloud Storage les autorisations Cloud KMS Encrypter/Decrypter.
- Pour plus d'informations, reportez-vous à ["Documentation Google Cloud : Utilisation des clés de chiffrement gérées par le client"](#)
5. Utilisez le paramètre « gcpEncryption » avec votre requête API lors de la création d'un système.

Exemple

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

Reportez-vous à la ["Documentation sur l'automatisation de la NetApp Console"](#) pour plus de détails sur l'utilisation du paramètre « GcpEncryption ».

Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud

Une fois que vous avez décidé quelle option de licence vous souhaitez utiliser avec Cloud Volumes ONTAP, quelques étapes sont nécessaires avant de pouvoir choisir cette option de licence lors de la création d'un nouveau système.

Freemium

Sélectionnez l'offre Freemium pour utiliser Cloud Volumes ONTAP gratuitement avec jusqu'à 500 Gio de capacité provisionnée. ["En savoir plus sur l'offre Freemium"](#) .

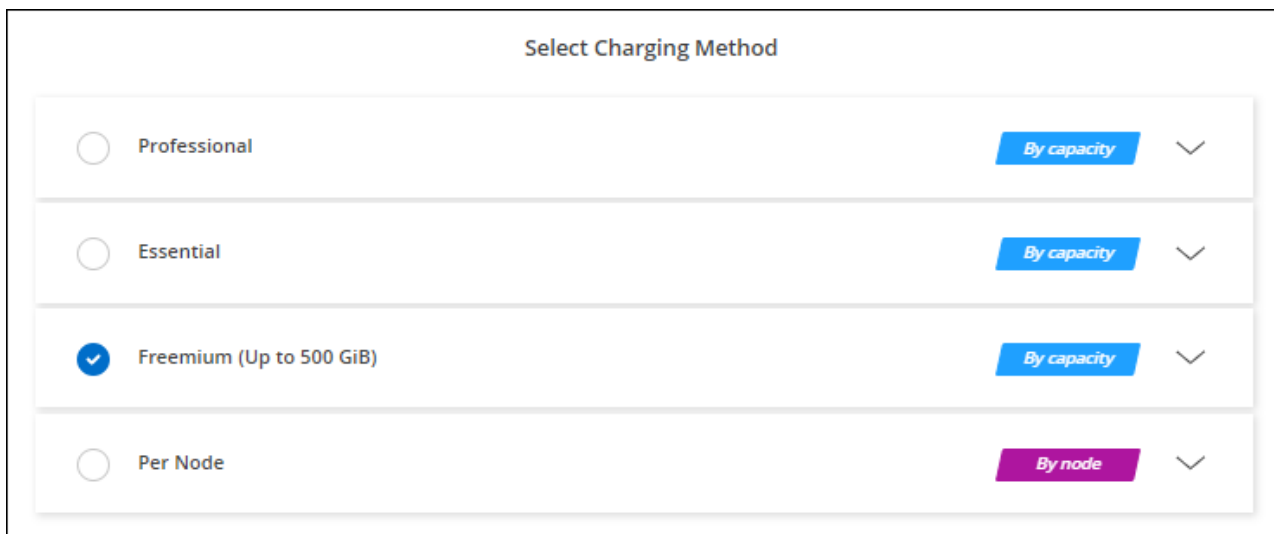
Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.

2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes de la NetApp Console.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner à l'offre de paiement à l'utilisation sur Google Cloud Marketplace.

Vous ne serez pas facturé via l'abonnement du marché à moins que vous ne dépassiez 500 Gio de capacité provisionnée, auquel cas le système est automatiquement converti en "[Forfait Essentiel](#)".

- b. Après être revenu à la console, sélectionnez **Freemium** lorsque vous atteignez la page des méthodes de facturation.



The screenshot shows a 'Select Charging Method' dialog box with four options:

- ☐ Professional: By capacity (blue button)
- ☐ Essential: By capacity (blue button)
- ☒ Freemium (Up to 500 GiB): By capacity (blue button)
- ☐ Per Node: By node (purple button)

["Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud"](#).

Licence basée sur la capacité

Les licences basées sur la capacité vous permettent de payer Cloud Volumes ONTAP par Tio de capacité. Les licences basées sur la capacité sont disponibles sous la forme d'un *package* : le package Essentials ou Professional.

Les formules Essentiel et Professionnel sont disponibles avec les modèles de consommation ou options d'achat suivants :

- Une licence (apportez votre propre licence (BYOL)) achetée auprès de NetApp
- Un abonnement horaire à la carte (PAYGO) de Google Cloud Marketplace
- Un contrat annuel

["En savoir plus sur les licences basées sur la capacité"](#).

Les sections suivantes décrivent comment démarrer avec chacun de ces modèles de consommation.

Apportez votre propre vin

Payez à l'avance en achetant une licence (BYOL) auprès de NetApp pour déployer les systèmes Cloud Volumes ONTAP chez n'importe quel fournisseur de cloud.



NetApp a restreint l'achat, la prolongation et le renouvellement des licences BYOL. Pour plus d'informations, consultez "[Disponibilité restreinte des licences BYOL pour Cloud Volumes ONTAP](#)".

Étapes

1. "[Contactez le service commercial NetApp pour obtenir une licence](#)"
2. "[Ajoutez votre compte de site de support NetApp à la NetApp Console](#)"

La console interroge automatiquement le service de licences de NetApp pour obtenir des détails sur les licences associées à votre compte de site de support NetApp. S'il n'y a pas d'erreur, la console ajoute les licences.

Votre licence doit être disponible depuis la console avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez "[ajouter manuellement la licence à la console](#)".

3. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner à l'offre de paiement à l'utilisation sur Google Cloud Marketplace.

La licence que vous avez achetée auprès de NetApp est toujours facturée en premier, mais vous serez facturé au tarif horaire du marché si vous dépassez votre capacité sous licence ou si la durée de votre licence expire.
 - b. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.

Select Charging Method

☒ Professional	By capacity	▼
☐ Essential	By capacity	▼
☐ Freemium (Up to 500 GiB)	By capacity	▼
☐ Per Node	By node	▼

"[Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud](#)".

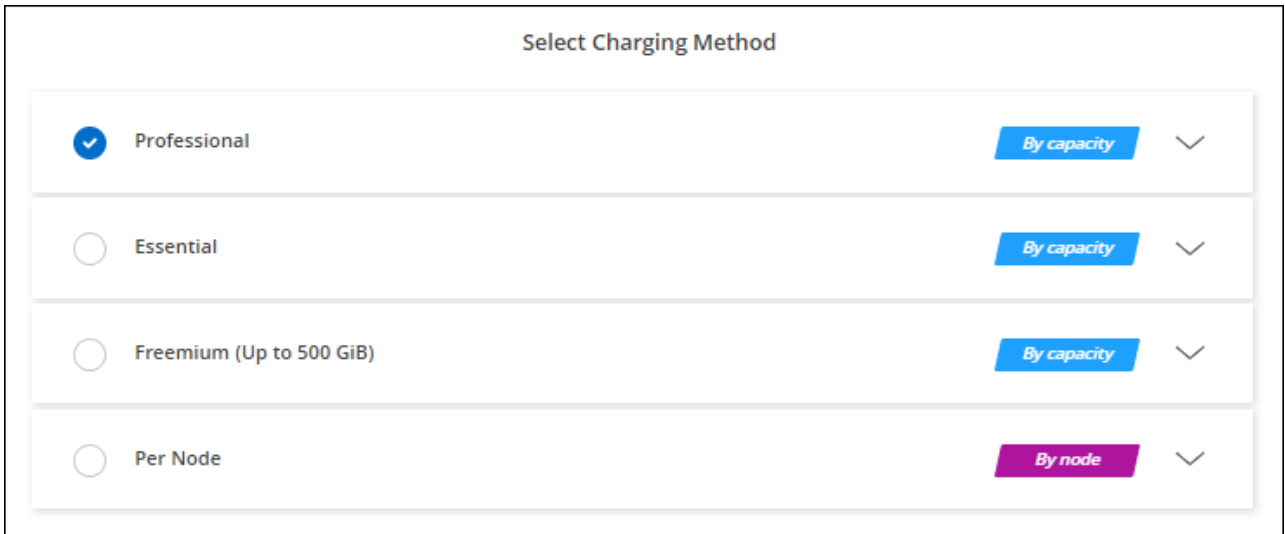
Abonnement PAYGO

Payez à l'heure en souscrivant à l'offre depuis la marketplace de votre fournisseur cloud.

Lorsque vous créez un système Cloud Volumes ONTAP, la console vous invite à souscrire à l'accord disponible sur Google Cloud Marketplace. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes supplémentaires.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner à l'offre de paiement à l'utilisation sur Google Cloud Marketplace.
 - b. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



The screenshot shows a 'Select Charging Method' dialog box with four radio button options. The 'Professional' option is selected, indicated by a blue checkmark in its radio button. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The buttons for 'By capacity' are blue, while the button for 'By node' is purple.

Charging Method	Button Label
☒ Professional	By capacity
☐ Essential	By capacity
☐ Freemium (Up to 500 GiB)	By capacity
☐ Per Node	By node

"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud" .



Vous pouvez gérer les abonnements Google Cloud Marketplace associés à vos comptes à partir de la page Paramètres > Informations d'identification. "[Découvrez comment gérer vos identifiants et abonnements Google Cloud](#)"

Contrat annuel

Payez Cloud Volumes ONTAP annuellement en achetant un contrat annuel.

Étapes

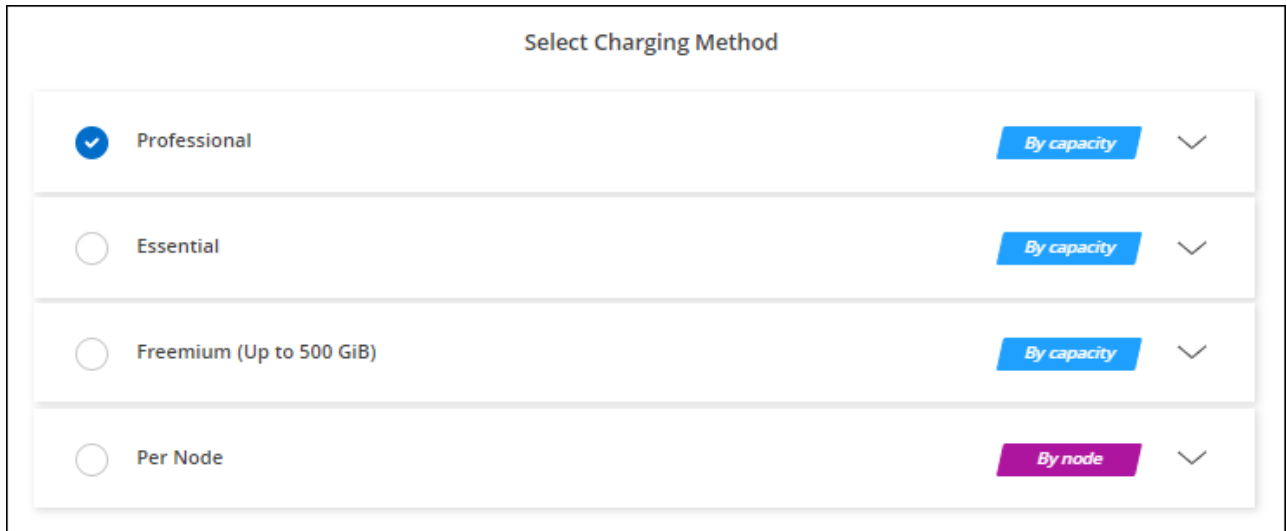
1. Contactez votre représentant commercial NetApp pour acheter un contrat annuel.

Le contrat est disponible sous forme d'offre *privée* sur Google Cloud Marketplace.

Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le forfait annuel lorsque vous vous abonnez à partir de Google Cloud Marketplace lors de la création du système.

2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner au forfait annuel sur Google Cloud Marketplace.
 - b. Dans Google Cloud, sélectionnez le forfait annuel partagé avec votre compte, puis cliquez sur **S'abonner**.

- c. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



Select Charging Method	
☒ Professional	By capacity
☐ Essential	By capacity
☐ Freemium (Up to 500 GiB)	By capacity
☐ Per Node	By node

"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud" .

Abonnement Keystone

Un abonnement Keystone est un service d'abonnement à paiement progressif. "En savoir plus sur les abonnements NetApp Keystone" .

Étapes

1. Si vous n'avez pas encore d'abonnement, "[contacter NetApp](#)"
2. [Contacter NetApp](#) pour autoriser votre compte utilisateur de la console avec un ou plusieurs abonnements Keystone .
3. Une fois que NetApp a autorisé votre compte, "[liez vos abonnements pour les utiliser avec Cloud Volumes ONTAP](#)" .
4. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
 - a. Sélectionnez la méthode de facturation de l'abonnement Keystone lorsque vous êtes invité à choisir une méthode de facturation.

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ **Professional** By capacity v

☐ **Essential** By capacity v

☐ **Freemium (Up to 500 GiB)** By capacity v

☐ **Per Node** By node v

["Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud"](#) .

Licence basée sur les nœuds

Une licence basée sur les nœuds est la licence de génération précédente pour Cloud Volumes ONTAP. Une licence basée sur les nœuds peut être obtenue auprès de NetApp (BYOL) et est disponible pour le renouvellement de licence, uniquement dans des cas spécifiques. Pour plus d'informations, consultez :

- ["Fin de disponibilité des licences basées sur des nœuds"](#)
- ["Fin de disponibilité des licences basées sur des nœuds"](#)
- ["Convertir une licence basée sur les nœuds en une licence basée sur la capacité"](#)

Lancer Cloud Volumes ONTAP dans Google Cloud

Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à nœud unique ou en tant que paire HA dans Google Cloud.

Avant de commencer

Vous avez besoin des éléments suivants avant de commencer.

- Un agent NetApp Console en cours d'exécution.
 - Vous devriez avoir un ["Agent de console associé à votre système"](#) .

- ["Vous devez être prêt à laisser l'agent de la console en cours d'exécution à tout moment."](#) .
- Le compte de service associé à l'agent de la console ["devrait avoir les autorisations requises"](#)
- Une compréhension de la configuration que vous souhaitez utiliser.

Vous devez vous préparer en choisissant une configuration et en obtenant des informations sur le réseau Google Cloud auprès de votre administrateur. Pour plus de détails, reportez-vous à ["Planification de votre configuration Cloud Volumes ONTAP"](#) .

- Une compréhension de ce qui est nécessaire pour configurer les licences pour Cloud Volumes ONTAP.

["Apprenez à configurer les licences"](#) .

- Les API Google Cloud devraient être ["activé dans votre projet"](#) :
 - API du gestionnaire de déploiement cloud V2
 - API de journalisation dans le cloud
 - API du gestionnaire de ressources cloud
 - API Compute Engine
 - API de gestion des identités et des accès (IAM)

Lancer un système à nœud unique dans Google Cloud

Créez un système dans la NetApp Console pour lancer Cloud Volumes ONTAP dans Google Cloud.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. **Choisissez un emplacement** : sélectionnez **Google Cloud** et * Cloud Volumes ONTAP*.
4. Si vous y êtes invité, ["créer un agent de console"](#) .
5. **Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, sélectionnez éventuellement un compte de service, ajoutez éventuellement des étiquettes, puis spécifiez les informations d'identification.

Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et l'instance de machine virtuelle Google Cloud. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Nom du compte de service	Si vous prévoyez d'utiliser "hiérarchisation des données" ou "NetApp Backup and Recovery" avec Cloud Volumes ONTAP, vous devez activer Compte de service et sélectionner un compte de service doté du rôle d'administrateur de stockage prédéfini. "Apprenez à créer un compte de service" .

Champ	Description
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour vos ressources Google Cloud. La console ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources Google Cloud associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un système. Pour plus d'informations sur les étiquettes, reportez-vous à la "Documentation Google Cloud : Étiquetage des ressources" .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP. Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet où se trouve la Console. Si aucun projet supplémentaire n'apparaît dans la liste déroulante, cela signifie que vous n'avez pas encore associé le compte de service à d'autres projets. Accédez à la Google Cloud Console, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle que vous utilisez pour la Console à ce projet. Vous devrez répéter cette étape pour chaque projet.  Il s'agit du compte de service que vous avez configuré pour la console, "comme décrit sur cette page". Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à la carte, vous devez sélectionner un projet Google Cloud associé à un abonnement à Cloud Volumes ONTAP sur la place de marché Google Cloud. Se référer à "Associer un abonnement Marketplace aux identifiants Google Cloud".

6. **Services** : Sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner Sauvegarde et récupération ou utiliser NetApp Cloud Tiering, vous devez avoir spécifié le compte de service à l'étape 3.



Si vous souhaitez utiliser WORM et la hiérarchisation des données, vous devez désactiver la sauvegarde et la récupération et déployer un système Cloud Volumes ONTAP avec la version 9.8 ou supérieure.

7. **Emplacement et connectivité** : Sélectionnez la région et la zone Google Cloud pour votre système, choisissez une politique de pare-feu et confirmez la connectivité réseau au stockage Google Cloud pour la hiérarchisation des données.

Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Vérification de la connectivité	Pour hiérarchiser les données froides vers un bucket Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour l'accès privé à Google. Pour les instructions, reportez-vous à "Documentation Google Cloud : Configuration de l'accès privé à Google" .
Politique de pare-feu générée	Si vous laissez la console générer la politique de pare-feu pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez VPC sélectionné uniquement, le filtre source pour le trafic entrant est la plage de sous-réseaux du VPC sélectionné et la plage de sous-réseaux du VPC sur lequel réside l'agent de la console. C'est l'option recommandée. • Si vous choisissez Tous les VPC, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.
Utiliser la politique de pare-feu existante	Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises : "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP"

8. * Méthodes de facturation et compte NSS * : Spécifiez l'option de facturation que vous souhaitez utiliser avec ce système, puis spécifiez un compte de site de support NetApp :
- ["En savoir plus sur les options de licence pour Cloud Volumes ONTAP"](#)
 - ["Apprenez à configurer les licences"](#)
9. **Packages préconfigurés** : Sélectionnez l'un des packages pour déployer rapidement un système Cloud Volumes ONTAP, ou cliquez sur **Créer ma propre configuration**. Les packages préconfigurés varient selon la version Cloud Volumes ONTAP sélectionnée. Par exemple, pour Cloud Volumes ONTAP 9.18.1 et versions ultérieures, la Console affiche des packages avec des machines virtuelles C3, y compris des disques Hyperdisk Balanced. Vous pouvez modifier les configurations, telles que les paramètres d'IOPS et de débit, en fonction des besoins de votre charge de travail.

Si vous choisissez l'un des packages, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins et sélectionnez un type de machine.



Si une version candidate à la publication, une version de disponibilité générale ou une version de correctif plus récente est disponible pour une version sélectionnée, la console met à jour le système vers cette version lors de sa création. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.13.1 et 9.13.1 P4 est disponible. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.13 à la version 9.14.

11. **Ressources de stockage sous-jacentes** : choisissez les paramètres de l'agrégat initial : un type de disque et la taille de chaque disque.

Le type de disque correspond au volume initial. Vous pouvez choisir un type de disque différent pour les volumes suivants.

La taille du disque concerne tous les disques de l'agrégat initial et tous les agrégats supplémentaires créés

par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.

Pour obtenir de l'aide sur le choix d'un type et d'une taille de disque, reportez-vous à ["Dimensionnez votre système dans Google Cloud"](#).

12. Cache Flash, vitesse d'écriture et WORM :

- a. Activez **Flash Cache** ou choisissez **Normal** ou **High** comme vitesse d'écriture si vous en avez besoin.

Apprenez-en davantage sur ["Cache Flash"](#) et ["vitesse d'écriture"](#).



Une vitesse d'écriture élevée et une unité de transmission maximale (MTU) supérieure de 8 896 octets sont disponibles via l'option de vitesse d'écriture **Élevée**. De plus, le MTU supérieur de 8 896 nécessite la sélection de VPC-1, VPC-2 et VPC-3 pour le déploiement. Pour plus d'informations sur VPC-1, VPC-2 et VPC-3, reportez-vous à ["Règles pour VPC-1, VPC-2 et VPC-3"](#).

- b. Activez le stockage WORM (écriture unique, lecture multiple), si vous le souhaitez.

WORM ne peut pas être activé si la hiérarchisation des données a été activée pour les versions 9.7 et inférieures de Cloud Volumes ONTAP. Le retour ou la rétrogradation vers Cloud Volumes ONTAP 9.8 est bloqué après l'activation de WORM et de la hiérarchisation.

["En savoir plus sur le stockage WORM"](#).

- a. Si vous activez le stockage WORM, sélectionnez la période de conservation.

13. * Hiérarchisation des données dans Google Cloud Platform* : choisissez d'activer ou non la hiérarchisation des données sur l'agrégat initial, choisissez une classe de stockage pour les données hiérarchisées, puis sélectionnez un compte de service doté du rôle d'administrateur de stockage prédéfini (requis pour Cloud Volumes ONTAP 9.7 ou version ultérieure) ou sélectionnez un compte Google Cloud (requis pour Cloud Volumes ONTAP 9.6).

Notez ce qui suit :

- La console définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations pour la hiérarchisation des données vers un bucket Google Cloud Storage. Assurez-vous d'ajouter le compte de service de l'agent de la console en tant qu'utilisateur du compte de service de hiérarchisation, sinon vous ne pourrez pas le sélectionner à partir de la console.
- Pour obtenir de l'aide sur l'ajout d'un compte Google Cloud, reportez-vous à ["Configuration et ajout de comptes Google Cloud pour la hiérarchisation des données avec 9.6"](#).
- Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants, mais vous devrez éteindre le système et ajouter un compte de service depuis le Google Cloud Console.

["En savoir plus sur la hiérarchisation des données"](#).

14. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

["En savoir plus sur les protocoles et versions clients pris en charge"](#).

Certains champs de cette page sont explicites. Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation ou non du provisionnement dynamique, qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une politique d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, la console entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur en utilisant le format domaine\nom d'utilisateur.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes d'initiateurs sont des tables de noms de nœuds d'hôtes iSCSI et contrôlent quels initiateurs ont accès à quels LUN. Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, "utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :

Volume Details & Protection

Volume Name i

ABDcv5689

Volume Size i

100

Storage VM (SVM)

svm_...CVO1 ▼

Unit

GiB ▼

Snapshot Policy

default ▼

default policy i

15. **Configuration CIFS** : Si vous avez choisi le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra. Si vous configurez Google Managed Active Directory, AD est accessible par défaut avec l'adresse IP 169.254.169.254.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Pour configurer Google Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, saisissez OU=Computers,OU=Cloud dans ce champ. <a :="" ad\"]"="" cloud="" dans="" documentation="" google="" href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units[\" managed="" microsoft="" organisationnelles="" unités="">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units[\"Documentation Google Cloud : Unités organisationnelles dans Google Managed Microsoft AD\"]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est le même que le domaine AD.
Serveur NTP	Sélectionnez Utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Pour plus d'informations, reportez-vous à la "Documentation sur l'automatisation de la NetApp Console" pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

16. **Profil d'utilisation, type de disque et politique de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifier la politique de hiérarchisation des volumes, si nécessaire.

Pour plus d'informations, reportez-vous à "[Choisissez un profil d'utilisation du volume](#)", "[Présentation de la hiérarchisation des données](#)", et "[KB : Quelles fonctionnalités d'efficacité du stockage en ligne sont prises en charge avec CVO ?](#)"

17. **Réviser et approuver** : Réviser et confirmez vos sélections.

- Consultez les détails de la configuration.
- Cliquez sur **Plus d'informations** pour consulter les détails sur l'assistance et les ressources Google Cloud que la console achètera.
- Cochez les cases **Je comprends....**
- Cliquez sur **Aller**.

Résultat

La console déploie le système Cloud Volumes ONTAP . Vous pouvez suivre la progression sur la page **Audit**.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP , consultez le message d'échec. Vous pouvez également sélectionner le système et cliquer sur **Recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, rendez-vous sur "[Prise en charge de NetApp Cloud Volumes ONTAP](#)".

Après avoir terminé

- Si vous avez provisionné un partage CIFS, accordez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP .

Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.



Après la fin du processus de déploiement, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Google Cloud, telles que les balises système et les étiquettes définies dans les ressources Google Cloud. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

Lancer une paire HA dans Google Cloud

Créez un système dans la console pour lancer Cloud Volumes ONTAP dans Google Cloud.

Étapes

- Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
- Sur la page **Systèmes**, cliquez sur **Stockage > Système** et suivez les instructions.
- Choisissez un emplacement** : sélectionnez **Google Cloud** et * Cloud Volumes ONTAP HA*.
- Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, sélectionnez éventuellement un compte de service, ajoutez éventuellement des étiquettes, puis spécifiez les informations d'identification.

Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et l'instance de machine virtuelle Google Cloud. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Nom du compte de service	Si vous prévoyez d'utiliser le "NetApp Cloud Tiering" ou "Sauvegarde et récupération" services, vous devez activer le commutateur Compte de service , puis sélectionner le compte de service qui possède le rôle d'administrateur de stockage prédéfini.
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour vos ressources Google Cloud. La console ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources Google Cloud associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un système. Pour plus d'informations sur les étiquettes, reportez-vous à "Documentation Google Cloud : Étiquetage des ressources" .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Si aucun projet supplémentaire n'apparaît dans la liste déroulante, cela signifie que vous n'avez pas encore associé le compte de service à d'autres projets. Accédez à la Google Cloud Console, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle que vous utilisez pour la Console à ce projet. Vous devrez répéter cette étape pour chaque projet.  Il s'agit du compte de service que vous avez configuré pour la console, "comme décrit sur cette page" . Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à la carte, vous devez sélectionner un projet Google Cloud associé à un abonnement à Cloud Volumes ONTAP sur Google Cloud Marketplace. Se référer à "Associer un abonnement Marketplace aux identifiants Google Cloud" .

- Services** : Sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner Sauvegarde et récupération ou pour utiliser NetApp Cloud Tiering, vous devez avoir spécifié le compte de service à l'étape 3.



Si vous souhaitez utiliser WORM et la hiérarchisation des données, vous devez désactiver la sauvegarde et la récupération et déployer un système Cloud Volumes ONTAP avec la version 9.8 ou supérieure.

6. **Modèles de déploiement HA** : Choisissez plusieurs zones (recommandé) ou une seule zone pour la configuration HA. Sélectionnez ensuite une région et une zone.

["En savoir plus sur les modèles de déploiement HA"](#) .

7. **Connectivité** : sélectionnez quatre VPC différents pour la configuration HA, un sous-réseau dans chaque VPC, puis choisissez une stratégie de pare-feu.

["En savoir plus sur les exigences de mise en réseau"](#) .

Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Politique générée	Si vous laissez la console générer la politique de pare-feu pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez VPC sélectionné uniquement, le filtre source pour le trafic entrant est la plage de sous-réseaux du VPC sélectionné et la plage de sous-réseaux du VPC sur lequel réside l'agent de la console. C'est l'option recommandée. • Si vous choisissez Tous les VPC, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" .

8. * Méthodes de facturation et compte NSS * : spécifiez l'option de facturation que vous souhaitez utiliser avec ce système, puis spécifiez un compte de site de support NetApp .

- ["En savoir plus sur les options de licence pour Cloud Volumes ONTAP"](#) .
- ["Apprenez à configurer les licences"](#) .

9. **Packages préconfigurés** : sélectionnez l'un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

Si vous choisissez l'un des packages, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins et sélectionnez un type de machine.



Si une version candidate à la publication, une version de disponibilité générale ou une version de correctif plus récente est disponible pour la version sélectionnée, la console met à jour le système vers cette version lors de sa création. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.13.1 et 9.13.1 P4 est disponible. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.13 à la version 9.14.

11. **Ressources de stockage sous-jacentes** : choisissez les paramètres de l'agrégat initial : un type de disque et la taille de chaque disque.

Le type de disque correspond au volume initial. Vous pouvez choisir un type de disque différent pour les volumes suivants.

La taille du disque concerne tous les disques de l'agrégat initial et tous les agrégats supplémentaires créés par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.

Pour obtenir de l'aide sur le choix d'un type et d'une taille de disque, reportez-vous à ["Dimensionnez votre système dans Google Cloud"](#) .

12. **Cache Flash, vitesse d'écriture et WORM** :

- a. Activez **Flash Cache** ou choisissez **Normal** ou **High** comme vitesse d'écriture si vous en avez besoin.

Apprenez-en davantage sur ["Cache Flash"](#) et ["vitesse d'écriture"](#).



Une vitesse d'écriture élevée et une unité de transmission maximale (MTU) supérieure de 8 896 octets sont disponibles via l'option de vitesse d'écriture **Élevée** avec les types d'instances n2-standard-16, n2-standard-32, n2-standard-48 et n2-standard-64. De plus, le MTU supérieur de 8 896 nécessite la sélection de VPC-1, VPC-2 et VPC-3 pour le déploiement. Une vitesse d'écriture élevée et un MTU de 8 896 dépendent des fonctionnalités et ne peuvent pas être désactivés individuellement dans une instance configurée. Pour plus d'informations sur VPC-1, VPC-2 et VPC-3, reportez-vous à ["Règles pour VPC-1, VPC-2 et VPC-3"](#) .

- b. Activez le stockage WORM (écriture unique, lecture multiple), si vous le souhaitez.

WORM ne peut pas être activé si la hiérarchisation des données a été activée pour les versions 9.7 et inférieures de Cloud Volumes ONTAP . Le retour ou la rétrogradation vers Cloud Volumes ONTAP 9.8 est bloqué après l'activation de WORM et de la hiérarchisation.

["En savoir plus sur le stockage WORM"](#) .

- a. Si vous activez le stockage WORM, sélectionnez la période de conservation.

13. * Hiérarchisation des données dans Google Cloud* : choisissez d'activer ou non la hiérarchisation des données sur l'agrégat initial, choisissez une classe de stockage pour les données hiérarchisées, puis sélectionnez un compte de service doté du rôle d'administrateur de stockage prédéfini.

Notez ce qui suit :

- La console définit le compte de service sur l'instance Cloud Volumes ONTAP . Ce compte de service fournit des autorisations pour la hiérarchisation des données vers un bucket Google Cloud Storage. Assurez-vous d'ajouter le compte de service de l'agent de la console en tant qu'utilisateur du compte de service de hiérarchisation, sinon vous ne pourrez pas le sélectionner à partir de la console.
- Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants, mais vous devrez éteindre le système et ajouter un compte de service depuis le Google Cloud Console.

["En savoir plus sur la hiérarchisation des données"](#) .

14. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

["En savoir plus sur les protocoles et versions clients pris en charge"](#) .

Certains champs de cette page sont explicites. Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation ou non du provisionnement dynamique, qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une politique d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, la console entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupe (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur en utilisant le format domaine\nom d'utilisateur.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes d'initiateurs sont des tables de noms de nœuds d'hôtes iSCSI et contrôlent quels initiateurs ont accès à quels LUN. Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, "utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :

Volume Details & Protection

Volume Name i

ABDcv5689

Volume Size i

100

Storage VM (SVM)

svm_...CVO1

Unit

GiB

Snapshot Policy

default

default policy i

15. **Configuration CIFS** : Si vous avez choisi le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra. Si vous configurez Google Managed Active Directory, AD est accessible par défaut avec l'adresse IP 169.254.169.254.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Pour configurer Google Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, saisissez OU=Computers,OU=Cloud dans ce champ. <a :="" ad\"]"="" cloud="" dans="" documentation="" google="" href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units[\" managed="" microsoft="" organisationnelles="" unités="">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units[\"Documentation Google Cloud : Unités organisationnelles dans Google Managed Microsoft AD\"]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est le même que le domaine AD.
Serveur NTP	Sélectionnez Utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la \"Documentation sur l'automatisation de la NetApp Console\" pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

16. **Profil d'utilisation, type de disque et politique de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifier la politique de hiérarchisation des volumes, si nécessaire.

Pour plus d'informations, reportez-vous à "[Choisissez un profil d'utilisation du volume](#)", "[Présentation de la hiérarchisation des données](#)", et "[KB : Quelles fonctionnalités d'efficacité du stockage en ligne sont prises en charge avec CVO ?](#)"

17. **Réviser et approuver** : Réviser et confirmez vos sélections.

- Consultez les détails de la configuration.
- Cliquez sur **Plus d'informations** pour consulter les détails sur l'assistance et les ressources Google Cloud que la console achètera.
- Cochez les cases **Je comprends....**
- Cliquez sur **Aller**.

Résultat

La console déploie le système Cloud Volumes ONTAP . Vous pouvez suivre la progression sur la page **Audit**.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP , consultez le message d'échec. Vous pouvez également sélectionner le système et cliquer sur **Recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, rendez-vous sur "[Prise en charge de NetApp Cloud Volumes ONTAP](#)".

Après avoir terminé

- Si vous avez provisionné un partage CIFS, accordez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP .

Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.



Après la fin du processus de déploiement, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Google Cloud, telles que les balises système et les étiquettes définies dans les ressources Google Cloud. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

Liens connexes

- "[Planification de votre configuration Cloud Volumes ONTAP dans Google Cloud](#)"

Vérification d'image de Google Cloud Platform

Découvrez comment l'image Google Cloud est vérifiée dans Cloud Volumes ONTAP

La vérification d'image Google Cloud est conforme aux exigences de sécurité améliorées de NetApp . Des modifications ont été apportées au script générant les images pour signer l'image en cours de route à l'aide de clés privées spécifiquement générées pour cette tâche. Vous pouvez vérifier l'intégrité de l'image Google Cloud en utilisant le résumé signé et le certificat public pour Google Cloud qui peuvent être téléchargés via

"NSS" pour une version spécifique.



La vérification d'image Google Cloud est prise en charge sur le logiciel Cloud Volumes ONTAP version 9.13.0 ou supérieure.

Convertir l'image Google Cloud au format brut pour Cloud Volumes ONTAP

L'image utilisée pour déployer de nouvelles instances, des mises à niveau ou utilisée dans des images existantes sera partagée avec les clients via ["le site d'assistance NetApp \(NSS\)"](#). Le résumé signé et les certificats seront disponibles en téléchargement via le portail NSS. Assurez-vous de télécharger le résumé et les certificats pour la bonne version correspondant à l'image partagée par le support NetApp. Par exemple, les images 9.13.0 auront un condensé signé 9.13.0 et des certificats disponibles sur NSS.

Pourquoi cette étape est-elle nécessaire ?

Les images de Google Cloud ne peuvent pas être téléchargées directement. Afin de vérifier l'image par rapport au résumé signé et aux certificats, vous devez disposer d'un mécanisme permettant de comparer les deux fichiers et de télécharger l'image. Pour ce faire, vous devez exporter/convertir l'image au format disk.raw et enregistrer les résultats dans un bucket de stockage dans Google Cloud. Le fichier disk.raw est goudronné et compressé au cours du processus.

L'utilisateur/compte de service aura besoin de privilèges pour effectuer les opérations suivantes :

- Accès au compartiment de stockage Google
- Écrire dans le bucket de stockage Google
- Créer des tâches de création de cloud (utilisées pendant le processus d'exportation)
- Accéder à l'image souhaitée
- Créer des tâches d'exportation d'images

Pour vérifier l'image, elle doit être convertie au format disk.raw puis téléchargée.

Utilisez la ligne de commande Google Cloud pour exporter l'image Google Cloud

La méthode préférée pour exporter une image vers Cloud Storage est d'utiliser le ["commande d'exportation d'images de calcul gcloud"](#). Cette commande prend l'image fournie et la convertit en un fichier disk.raw qui est compressé et compressé. Le fichier généré est enregistré à l'URL de destination et peut ensuite être téléchargé pour vérification.

L'utilisateur/compte doit disposer de privilèges pour accéder et écrire dans le bucket souhaité, exporter l'image et les builds cloud (utilisés par Google pour exporter l'image) pour exécuter cette opération.

Exporter l'image Google Cloud à l'aide de gcloud

```
$ gcloud compute images export \  
  --destination-uri DESTINATION_URI \  
  --image IMAGE_NAME  
  
# For our example:  
$ gcloud compute images export \  
  --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-  
gcp-demo \  
  --image example-user-20230120115139  
  
## DEMO ##  
# Step 1 - Optional: Checking access and listing objects in the  
destination bucket  
$ gsutil ls gs://example-user-export-image-bucket/  
  
# Step 2 - Exporting the desired image to the bucket  
$ gcloud compute images export --image example-user-export-image-demo  
--destination-uri gs://example-user-export-image-bucket/export-  
demo.tar.gz  
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-  
project/locations/us-central1/builds/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-  
export-image-demo" from project "example-demo-project".  
[image-export]: 2023-01-25T18:13:49Z Validating workflow  
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"  
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-  
export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "setup-disks"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "run-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "wait-for-inst-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "copy-image-object"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "delete-inst"  
[image-export]: 2023-01-25T18:13:51Z Validation Complete  
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-  
project  
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```

[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":

```

```

StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \" /dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \" /root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \" /dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\" /dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."

```

```

[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Finished export in 48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: <serial-output key:'target-size-gb' value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step "delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk" (IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz

# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION

```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-  
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz  
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to  
file://CVO_GCP_Signed_Digest.tar.gz  
Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s
```

```
Average throughput: 213.3MiB/s
```

```
$ ls -l  
total 1565036  
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44  
CVO_GCP_Signed_Digest.tar.gz
```

Extraire les fichiers zippés

```
# Extracting files from the digest  
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```



Pour plus d'informations sur la façon d'exporter une image via Google Cloud, reportez-vous à la ["Documentation Google Cloud sur l'exportation d'une image"](#) .

Vérification de la signature de l'image

Vérification de la signature d'image Google Cloud pour Cloud Volumes ONTAP

Pour vérifier l'image signée Google Cloud exportée, vous devez télécharger le fichier de résumé de l'image à partir du NSS pour valider le fichier disk.raw et le contenu du fichier de résumé.

Résumé du flux de travail de vérification des images signées

Voici un aperçu du processus de vérification des images signées de Google Cloud.

- De la ["NSS"](#) , téléchargez l'archive Google Cloud contenant les fichiers suivants :
 - Digest signé (.sig)
 - Certificat contenant la clé publique (.pem)
 - Chaîne de certificats (.pem)

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

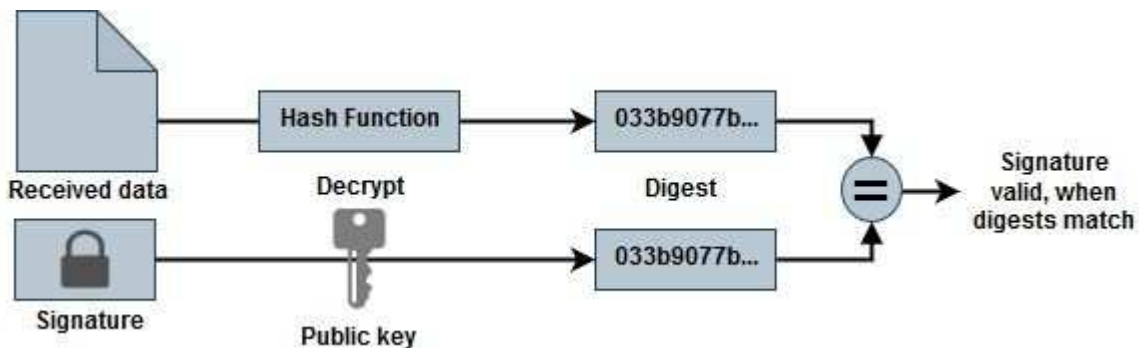
DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

- Téléchargez le fichier disk.raw converti
- Valider le certificat à l'aide de la chaîne de certificats
- Valider le condensé signé à l'aide du certificat contenant la clé publique
 - Décrypter le condensé signé à l'aide de la clé publique pour extraire le condensé du fichier image
 - Créer un condensé du fichier disk.raw téléchargé
 - Comparez les deux fichiers digest pour validation



Vérifiez le fichier disk.raw de l'image Google Cloud pour Cloud Volumes ONTAP à l'aide d'OpenSSL

Vous pouvez vérifier le fichier disk.raw téléchargé par Google Cloud par rapport au contenu du fichier digest disponible via le "NSS" en utilisant OpenSSL.



Les commandes OpenSSL pour valider l'image sont compatibles avec les machines Linux, macOS et Windows.

Étapes

1. Vérifiez le certificat à l'aide d'OpenSSL.

Cliquez pour afficher

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OSCP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OSCP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -url ${ocsp_url} -resp_text
-respout resp.der
```

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2

Produced At: Jan 19 15:14:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5

Cert Status: good

This Update: Jan 19 15:00:00 2023 GMT

Next Update: Jan 26 14:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:

```

e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
  This Update: Jan 19 15:00:00 2023 GMT
  Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK

```

2. Placez le fichier disk.raw téléchargé, la signature et les certificats dans un répertoire.
3. Extraire la clé publique du certificat à l'aide d'OpenSSL.
4. Décryptez la signature à l'aide de la clé publique extraite et vérifiez le contenu du fichier disk.raw téléchargé.

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff   Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff   Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff   Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff   Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff   Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff   Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff   Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff   Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff   Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.