



Lancez-vous dans Google Cloud

Cloud Volumes ONTAP

NetApp
June 27, 2024

Sommaire

- Lancez-vous dans Google Cloud 1
 - Démarrage rapide pour Cloud Volumes ONTAP dans Google Cloud 1
 - Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud 2
 - Exigences de mise en réseau pour Cloud Volumes ONTAP dans Google Cloud 6
 - Planification des contrôles de service VPC dans GCP 16
 - Créez un compte de service pour le Tiering des données et les sauvegardes 19
 - Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP 22
 - Configurez la licence pour Cloud Volumes ONTAP dans Google Cloud 23
 - Lancement d'Cloud Volumes ONTAP dans Google Cloud 28
 - Vérification des images Google Cloud Platform 42

Lancez-vous dans Google Cloud

Démarrage rapide pour Cloud Volumes ONTAP dans Google Cloud

Commencez à utiliser Cloud Volumes ONTAP pour Google Cloud en quelques étapes.

1

Créer un connecteur

Si vous n'avez pas de "Connecteur" Cependant, un administrateur de compte doit en créer un. "[Découvrez comment créer un connecteur dans Google Cloud](#)"

Si vous souhaitez déployer Cloud Volumes ONTAP dans un sous-réseau sans accès à Internet, vous devez installer manuellement le connecteur et accéder à l'interface utilisateur BlueXP qui s'exécute sur ce connecteur. "[Apprenez à installer manuellement le connecteur dans un emplacement sans accès à Internet](#)"

2

Planification de la configuration

BlueXP offre des packages préconfigurés qui répondent à vos exigences de charge de travail, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez.

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

3

Configurez votre réseau

1. Vérifiez que votre VPC et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Si vous prévoyez d'activer le Tiering des données, "[Configurez le sous-réseau Cloud Volumes ONTAP pour un accès privé à Google](#)".
3. Si vous déployez une paire haute disponibilité, assurez-vous d'avoir quatre VPC, chacun avec son propre sous-réseau.
4. Si vous utilisez un VPC partagé, indiquez le rôle *Compute Network User* au compte de service Connector.
5. Activez l'accès Internet sortant à partir du VPC cible pour NetApp AutoSupport.

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

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

4

Configurez un compte de service

Cloud Volumes ONTAP nécessite un compte de service Google Cloud pour deux raisons. La première est lorsque vous activez "[tiering des données](#)" Tiering des données inactives vers un stockage objet à faible coût dans Google Cloud. La seconde est lorsque vous activez le "[Sauvegarde et restauration BlueXP](#)" sauvegarde de volumes dans un stockage objet à faible coût

Vous pouvez configurer un seul compte de service et l'utiliser dans les deux cas. Le compte de service doit avoir le rôle **Administrateur de stockage**.

["Lisez les instructions détaillées"](#).

5

Activez les API Google Cloud

["Activez les API Google Cloud suivantes dans votre projet"](#). Ces API sont nécessaires pour déployer le connecteur et Cloud Volumes ONTAP.

- API Cloud Deployment Manager V2
- API de journalisation cloud
- API Cloud Resource Manager
- API du moteur de calcul
- API de gestion des identités et des accès

6

Lancez Cloud Volumes ONTAP avec BlueXP

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

Liens connexes

- ["Création d'un connecteur depuis BlueXP"](#)
- ["Installation du logiciel du connecteur sur un hôte Linux"](#)
- ["Rôle de BlueXP avec les autorisations Google Cloud"](#)

Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud

Lorsque vous déployez Cloud Volumes ONTAP dans Google Cloud, vous pouvez soit choisir un système préconfiguré qui correspond aux exigences de vos workloads, soit créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez.

Choisissez une licence Cloud Volumes ONTAP

Plusieurs options de licence sont disponibles pour Cloud Volumes ONTAP. Chacune d'elles vous permet de choisir un modèle de consommation adapté à vos besoins.

- ["Découvrez les options de licence pour Cloud Volumes ONTAP"](#)
- ["Découvrez comment 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 machine, selon le type de licence choisi.

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

Compréhension des limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP dépend de la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Il est important de connaître ces dernières lors de la planification de la configuration.

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

Dimensionnez votre système dans GCP

Le dimensionnement du système Cloud Volumes ONTAP permet de répondre à vos besoins de performance et de capacité. Quelques points clés sont à noter lors de la sélection d'un type de machine, d'un type de disque et d'une taille de disque :

Type de machine

Examiner les types de machine pris en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#) Puis passez en revue les détails de Google concernant chaque type de machine pris en charge. Faites correspondre les exigences de vos charges de travail au nombre de CPU virtuels et à la mémoire correspondant au type de machine. Notez que chaque cœur de processeur augmente les performances réseau.

Pour plus de détails, reportez-vous aux sections suivantes :

- ["Documentation Google Cloud : types de machine standard N1"](#)
- ["Documentation Google Cloud : performances"](#)

Type de disque GCP

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

- *Zonal disques persistants SSD* : les disques persistants SSD sont adaptés aux charges de travail qui requièrent des taux élevés d'IOPS aléatoires.
- *Disques persistants équilibrés* ces SSD équilibrent les performances et les coûts en fournissant des IOPS par Go plus faibles.
- *Zonal Standard persistent disks* : les disques persistants standard sont économiques et peuvent gérer des opérations de lecture/écriture séquentielles.

Pour plus de détails, voir ["Documentation Google Cloud : disques persistants zonés \(standard et SSD\)"](#).

Taille du disque GCP

Lorsque vous déployez un système Cloud Volumes ONTAP, vous devez choisir la taille de disque initiale. Ensuite, vous pouvez laisser BlueXP gérer la capacité d'un système pour vous, mais si vous souhaitez créer vous-même des agrégats, sachez des éléments suivants :

- Tous les disques qui composent un agrégat doivent être de 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 des disques et du nombre de CPU virtuels disponibles pour le système.

Pour plus de détails, reportez-vous aux sections suivantes :

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

Afficher les disques système par défaut

En plus du stockage pour les données utilisateur, BlueXP achète également le stockage cloud pour les données système Cloud Volumes ONTAP (données de démarrage, données racines, données centrales et NVRAM). Pour des raisons de planification, il peut vous être utile de vérifier ces informations avant de déployer Cloud Volumes ONTAP.

- ["Afficher les disques par défaut des données système Cloud Volumes ONTAP dans Google Cloud"](#).
- ["Documents Google Cloud : quotas de ressources"](#)

Google Cloud Compute Engine met en œuvre des quotas quant à l'utilisation des ressources. Vous devez donc vous assurer que vous n'avez pas atteint vos limites avant de déployer Cloud Volumes ONTAP.



Le connecteur nécessite également un disque système. ["Afficher des détails sur la configuration par défaut du connecteur"](#).

Collecte d'informations de mise en réseau

Lorsque vous déployez Cloud Volumes ONTAP dans GCP, vous devez spécifier des informations relatives à votre réseau virtuel. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Informations de réseau pour un système à un seul nœud

Informations GCP	Votre valeur
Région	
Zone	
Réseau VPC	
Sous-réseau	
Politique de pare-feu (s'il s'agit du vôtre)	

Informations de réseau pour une paire HA dans plusieurs zones

Informations GCP	Votre valeur
Région	
Zone pour le nœud 1	

Informations GCP	Votre valeur
Zone pour le nœud 2	
Zone du médiateur	
VPC-0 et le sous-réseau	
VPC-1 et sous-réseau	
VPC-2 et sous-réseau	
VPC-3 et sous-réseau	
Politique de pare-feu (s'il s'agit du vôtre)	

Informations de réseau pour une paire HA dans une seule zone

Informations GCP	Votre valeur
Région	
Zone	
VPC-0 et le sous-réseau	
VPC-1 et sous-réseau	
VPC-2 et sous-réseau	
VPC-3 et sous-réseau	
Politique de pare-feu (s'il s'agit du vôtre)	

Choisissez une vitesse d'écriture

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

Choisissez un profil d'utilisation du volume

ONTAP comprend plusieurs fonctionnalités d'efficacité du stockage qui permettent de réduire la quantité totale de stockage nécessaire. Lorsque vous créez un volume dans BlueXP, vous pouvez choisir un profil qui active ces fonctionnalités ou un profil qui les désactive. Vous devez en savoir plus sur ces fonctionnalités pour vous aider à choisir le profil à utiliser.

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

Provisionnement fin

Met à la disposition des hôtes ou des utilisateurs une quantité de stockage logique supérieure au stockage effectivement présent dans votre pool physique. L'espace de stockage est alloué de manière dynamique, et non au préalable, à chaque volume lors de l'écriture des données.

Déduplication

Améliore l'efficacité en identifiant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins 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 les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Exigences de mise en réseau pour Cloud Volumes ONTAP dans Google Cloud

Configurez votre réseau Google Cloud pour que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement.

Si vous souhaitez déployer une paire haute disponibilité, vous devez ["Découvrez le fonctionnement des paires haute disponibilité dans Google Cloud"](#).

Conditions requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être satisfaites dans Google Cloud.

Besoins spécifiques aux systèmes à un seul nœud

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

Un VPC

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

Adresses IP privées

BlueXP alloue 3 ou 4 adresses IP privées à un système à nœud unique dans Google Cloud.

Vous pouvez ignorer la création de la LIF de gestion de VM de stockage (SVM) si vous déployez Cloud Volumes ONTAP à l'aide de l'API et spécifier le drapeau suivant :

```
skipSvmManagementLif: true
```



Une LIF est une adresse IP associée à un port physique. Une LIF de gestion de VM de stockage (SVM) est requise pour les outils de gestion tels que SnapCenter.

Besoins spécifiques aux paires haute disponibilité

Si vous souhaitez déployer une paire haute disponibilité, vérifiez que votre réseau répond aux exigences suivantes.

Une ou plusieurs zones

Vous pouvez assurer la haute disponibilité de vos données en déployant une configuration haute disponibilité sur plusieurs ou sur une seule zone. BlueXP vous invite à choisir plusieurs zones ou une seule zone lors de la

création de la paire haute disponibilité.

- Zones multiples (recommandé)

Le déploiement d'une configuration haute disponibilité sur trois zones garantit la disponibilité continue des données en cas de défaillance au sein d'une zone. Notez que les performances d'écriture sont légèrement inférieures à celles d'une seule zone, mais cela est minime.

- Zone unique

Lorsqu'elle est déployée dans une seule zone, la configuration Cloud Volumes ONTAP haute disponibilité utilise une règle de placement réparti. Cette règle garantit qu'une configuration haute disponibilité est protégée contre un point de défaillance unique dans la zone, sans avoir à utiliser des zones distinctes pour isoler les pannes.

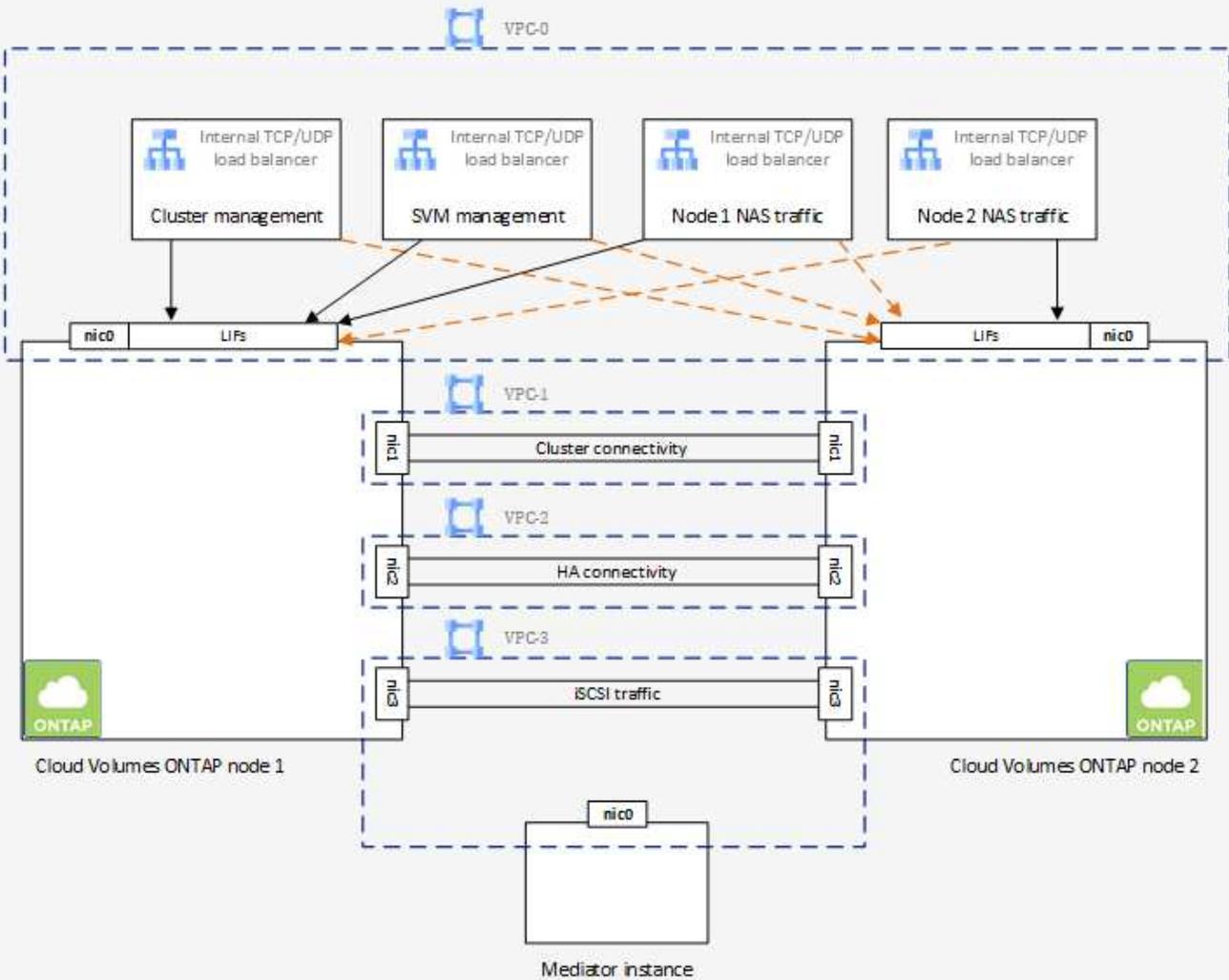
Ce modèle de déploiement réduit vos coûts, car il n'y a pas de frais de sortie de données entre les zones.

Quatre clouds privés virtuels

Quatre clouds privés virtuels (VPC) sont nécessaires dans le cadre d'une configuration haute disponibilité. Quatre VPC sont requis car Google Cloud exige que chaque interface réseau réside dans un réseau VPC distinct.

BlueXP vous invite à choisir quatre VPC lorsque vous créez la paire haute disponibilité :

- VPC-0 pour les connexions entrantes aux données et aux nœuds
- VPC-1, VPC-2 et VPC-3 pour les communications internes entre les nœuds et le médiateur haute disponibilité



Sous-réseaux

Un sous-réseau privé est requis pour chaque VPC.

Si vous placez le connecteur sur VPC-0, vous devez activer Private Google Access sur le sous-réseau pour accéder aux API et activer le Tiering des données.

Les sous-réseaux de ces VPC doivent avoir des plages CIDR distinctes. Les gammes CIDR ne peuvent pas être chevauchantes.

Adresses IP privées

BlueXP 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.

Le nombre de LIF alloués par BlueXP pour Cloud Volumes ONTAP dépend du déploiement d'un système à un seul nœud ou d'une paire haute disponibilité. Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

- **Nœud unique**

BlueXP alloue 4 adresses IP à un système à un seul nœud :

- FRV de gestion des nœuds
- LIF Cluster-management
- LIF de données iSCSI



Une LIF iSCSI fournit un accès client via le protocole iSCSI et est utilisée par le système pour d'autres flux de travail réseau importants. Ces LIFs sont requises et ne doivent pas être supprimées.

- LIF NAS

Vous pouvez ignorer la création de la LIF de gestion de VM de stockage (SVM) si vous déployez Cloud Volumes ONTAP à l'aide de l'API et spécifier le drapeau suivant :

```
skipSvmManagementLif: true
```

• Paire HA

BlueXP alloue 12-13 adresses IP à une paire haute disponibilité :

- 2 LIF de gestion de nœuds (e0a)
- 1 LIF de gestion de cluster (e0a)
- 2 LIF iSCSI (e0a)



Une LIF iSCSI fournit un accès client via le protocole iSCSI et est utilisée par le système pour d'autres flux de travail réseau importants. Ces LIFs sont requises et ne doivent pas être supprimées.

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

Vous pouvez ignorer la création de la LIF de gestion de VM de stockage (SVM) si vous déployez Cloud Volumes ONTAP à l'aide de l'API et spécifier le drapeau suivant :

```
skipSvmManagementLif: true
```

Équilibreurs de charge internes

BlueXP crée automatiquement quatre équilibreurs de charge internes (TCP/UDP) Google Cloud qui gèrent le trafic entrant vers la paire haute disponibilité Cloud Volumes ONTAP. Aucune configuration n'est requise de votre fin Nous avons répertorié cette exigence pour vous informer du trafic réseau et pour limiter les problèmes de sécurité.

Un équilibreur de charge est destiné à la gestion du cluster, un pour la gestion des VM de stockage (SVM), un pour le trafic NAS vers le nœud 1, et le dernier pour le trafic NAS vers le nœud 2.

La configuration de chaque équilibreur de charge est la suivante :

- Une adresse IP privée partagée

- Une vérification globale du système

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

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

Même si l'accès global est désactivé par défaut, l'activation du post-déploiement informatique est prise en charge. Nous l'avons désactivée car le trafic entre les régions sera considérablement plus élevé. Nous voulions nous assurer que vous n'avez pas eu d'expérience négative en raison de montages accidentels entre les régions. L'activation de cette option est spécifique aux besoins de votre entreprise.

VPC partagés

Cloud Volumes ONTAP et le connecteur sont pris en charge dans un VPC partagé par Google Cloud, ainsi que dans des VPC autonomes.

S'il s'agit d'un système à un seul nœud, le VPC peut être un VPC partagé ou un VPC autonome.

Pour une paire haute disponibilité, 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 peut être un VPC autonome.

Un VPC partagé vous permet de configurer et de gérer de manière centralisée les réseaux virtuels dans plusieurs projets. Vous pouvez configurer des réseaux VPC partagés dans le projet *host* et déployer les instances de machines virtuelles Connector et Cloud Volumes ONTAP dans un projet *service*. "[Documentation Google Cloud : présentation du VPC partagé](#)".

["Vérifiez les autorisations VPC partagées requises couvertes par le déploiement du connecteur"](#)

Duplication de paquets dans les VPC

"[Mise en miroir de paquets](#)" Doit être désactivé dans le VPC Google Cloud dans lequel vous déployez Cloud Volumes ONTAP. Cloud Volumes ONTAP ne peut pas fonctionner correctement si la mise en miroir des paquets est activée.

Accès Internet sortant

Cloud Volumes ONTAP nécessite un accès Internet sortant pour l'AutoSupport, qui contrôle de manière proactive l'état de santé de votre système et envoie des messages au support technique de NetApp.

Les règles de routage et de pare-feu doivent autoriser le trafic HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

Si aucune connexion Internet sortante n'est disponible pour envoyer des messages AutoSupport, BlueXP configure automatiquement vos systèmes Cloud Volumes ONTAP pour utiliser le connecteur comme serveur

proxy. La seule exigence est de s'assurer que le pare-feu du connecteur autorise les connexions *Inbound* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous avez défini des règles de trafic sortant strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le pare-feu Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Après avoir vérifié que l'accès Internet sortant est disponible, vous pouvez tester AutoSupport pour vous assurer qu'il peut envoyer des messages. Pour obtenir des instructions, reportez-vous à la section "[Documentation ONTAP : configuration d'AutoSupport](#)".



Si vous utilisez une paire haute disponibilité, le médiateur haute disponibilité ne nécessite pas d'accès à Internet sortant.

Si BlueXP vous informe que les messages AutoSupport ne peuvent pas être envoyés, "[Résoudre les problèmes de configuration AutoSupport](#)".

Règles de pare-feu

Il n'est pas nécessaire de créer des règles de pare-feu car BlueXP le fait pour vous. Si vous devez vous en servir, reportez-vous aux règles de pare-feu répertoriées ci-dessous.

Notez que deux jeux de règles de pare-feu sont nécessaires pour une configuration haute disponibilité :

- Un ensemble de règles pour les composants HA dans VPC-0. Ces règles permettent l'accès aux données à Cloud Volumes ONTAP. [En savoir plus >>](#).
- Un autre ensemble de règles pour les composants HA dans les VPC-1, VPC-2 et VPC-3. Ces règles sont ouvertes pour les communications entrantes et sortantes entre les composants HA. [En savoir plus >>](#).

Si vous souhaitez effectuer le Tiering des données inactives dans un compartiment de stockage Google Cloud, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour l'accès privé à Google (si vous utilisez une paire haute disponibilité, il s'agit du sous-réseau dans VPC-0). Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : configuration de Private Google Access](#)".

Pour connaître les étapes supplémentaires nécessaires à la configuration du Tiering des données dans BlueXP, reportez-vous à la section "[Tiering des données inactives vers un stockage objet à faible coût](#)".

Connexions aux systèmes ONTAP dans d'autres réseaux

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

Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : présentation de Cloud VPN](#)".

Règles de pare-feu

BlueXP crée des règles de pare-feu Google Cloud qui incluent les règles entrantes et sortantes nécessaires au bon fonctionnement de Cloud Volumes ONTAP. Vous pouvez consulter les ports à des fins de test ou si vous préférez utiliser vos propres règles de pare-feu.

Les règles de pare-feu de Cloud Volumes ONTAP requièrent des règles entrantes et sortantes. Si vous déployez une configuration haute disponibilité, ce sont les règles de pare-feu pour Cloud Volumes ONTAP dans VPC-0.

Notez que deux jeux de règles de pare-feu sont nécessaires pour une configuration haute disponibilité :

- Un ensemble de règles pour les composants HA dans VPC-0. Ces règles permettent l'accès aux données à Cloud Volumes ONTAP.
- Un autre ensemble de règles pour les composants HA dans les VPC-1, VPC-2 et VPC-3. Ces règles sont ouvertes pour les communications entrantes et sortantes entre les composants HA. [En savoir plus >>](#).



Vous recherchez des informations sur le connecteur ? ["Afficher les règles de pare-feu du connecteur"](#)

Règles entrantes

Lorsque vous créez un environnement de travail, vous pouvez choisir le filtre source de la politique de pare-feu prédéfinie pendant le déploiement :

- **VPC sélectionné uniquement** : le filtre source pour le trafic entrant est la plage de sous-réseau du VPC pour le système Cloud Volumes ONTAP et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de 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 aussi d'ajouter les deux plages d'adresses pour permettre à Google Load Balancer 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 section "[Documentation Google Cloud : règles du pare-feu Load Balancer](#)".

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Connectivité avec le connecteur et l'accès HTTPS à la console Web System Manager via l'adresse IP du LIF de cluster management
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 de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS

Protocole	Port	Objectif
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec 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 la charge pour déterminer quel nœud fonctionne (uniquement requis pour les paires HA)
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS quotad

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 base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

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

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Tout le trafic sortant
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous UDP	Tout	Tout le trafic sortant

Règles de sortie 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.



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

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)

Service	Protocole	Port	Source	Destination	Objectif
AutoSupport	HTTPS	443	FRV de gestion des nœuds	support.netapp.com	AutoSupport (HTTPS est le protocole par défaut)
	HTTP	80	FRV de gestion des nœuds	support.netapp.com	AutoSupport (uniquement si le protocole de transport est passé de HTTPS à HTTP)
	TCP	3128	FRV de gestion des nœuds	Connecteur	Envoi de messages AutoSupport via un serveur proxy sur le connecteur, si aucune connexion Internet sortante n'est disponible
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
Sauvegardes de la configuration	HTTP	80	FRV de gestion des nœuds	\\Http://<connector-IP-address>/occm/offbo xconfig	Envoyer des sauvegardes de configuration au connecteur. " En savoir plus sur les fichiers de sauvegarde de configuration ".
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-1869	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP

Service	Protocole	Port	Source	Destination	Objectif
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles pour VPC-1, VPC-2 et VPC-3

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

Pendant ce temps, les règles de pare-feu prédéfinies que BlueXP crée pour les instances dans VPC-1, VPC-2 et VPC-3 permettent la communication via les protocoles et ports *All*. Ces règles permettent la communication entre les nœuds HA.

La communication entre les nœuds HA et le médiateur HA se fait via le port 3260 (iSCSI).



Pour permettre une vitesse d'écriture élevée dans les nouveaux déploiements de paires haute disponibilité Google Cloud, une unité de transmission (MTU) maximale est requise d'au moins 8,896 octets pour les 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 1 8,896 octets, vous devez arrêter tous les systèmes haute disponibilité existants en utilisant ces VPC lors du processus de configuration.

Configuration requise pour le connecteur

Si vous n'avez pas encore créé de connecteur, vous devez également consulter les exigences de mise en réseau pour le connecteur.

- ["Afficher les exigences de mise en réseau du connecteur"](#)
- ["Règles de pare-feu dans Google Cloud"](#)

Planification des contrôles de service VPC dans GCP

Lorsque vous choisissez de verrouiller votre environnement Google Cloud avec les contrôles de service VPC, vous devez comprendre comment BlueXP et Cloud Volumes ONTAP interagissent avec les API Google Cloud, ainsi que comment configurer votre périmètre de service pour déployer BlueXP 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 sécurisé, de bloquer l'accès aux données à partir de sites non fiables et de limiter les risques de transferts de données non autorisés. ["En savoir plus sur les contrôles de service Google Cloud VPC"](#).

La communication des services NetApp avec les contrôles de service VPC

BlueXP communique directement avec les API Google Cloud. Ceci est déclenché à partir d'une adresse IP externe en dehors de Google Cloud (par exemple à partir de `api.services.cloud.netapp.com`) ou dans Google Cloud à partir d'une adresse interne attribuée au connecteur BlueXP.

Selon le style de déploiement du connecteur, certaines exceptions peuvent être nécessaires pour votre périmètre de service.

Images

Cloud Volumes ONTAP et BlueXP utilisent toutes les deux des images d'un projet GCP géré par NetApp. Cela peut affecter le déploiement du connecteur BlueXP et de Cloud Volumes ONTAP, si votre organisation dispose d'une stratégie qui bloque l'utilisation d'images qui ne sont pas hébergées au sein de l'organisation.

Vous pouvez déployer un connecteur manuellement selon 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 connecteur et un Cloud Volumes ONTAP.

Déploiement d'un connecteur

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

Le déploiement de Cloud Volumes ONTAP

- Le compte de service BlueXP 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 des règles requises pour extraire ces images avec les contrôles de service VPC sont définis ci-dessous.

Le service VPC contrôle les stratégies de périmètre

Les règles permettent des exceptions aux jeux de règles de contrôle de service VPC. Pour plus d'informations sur les politiques, veuillez consulter le ["Documentation sur les règles de contrôle du service VPC GCP"](#).

Pour définir les stratégies requises par BlueXP, accédez à vos contrôles de service VPC Perimeter dans votre entreprise et ajoutez les stratégies suivantes. Les champs doivent correspondre aux options indiquées dans la page de stratégie contrôles de service VPC. Notez également que **toutes** règles sont requises et que les paramètres **OU** doivent être utilisés dans le jeu 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 mentionné ci-dessus est le projet *netapp-cloudManager* utilisé par NetApp pour stocker des images pour le connecteur et pour Cloud Volumes ONTAP.

Créez un compte de service pour le Tiering des données et les sauvegardes

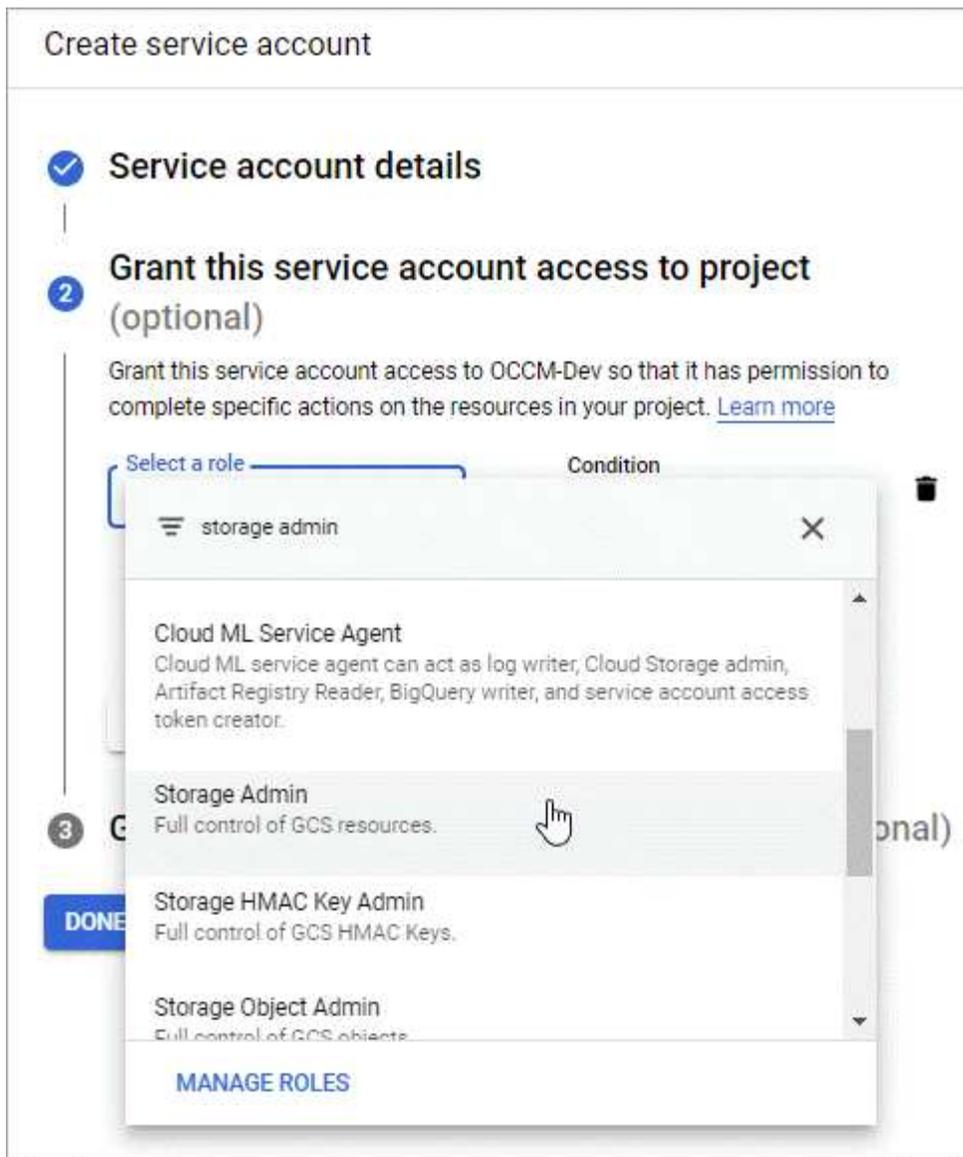
Cloud Volumes ONTAP nécessite un compte de service Google Cloud pour deux raisons. La première est lorsque vous activez "[tiering des données](#)" Tiering des données inactives vers un stockage objet à faible coût dans Google Cloud. La seconde est lorsque vous activez le "[Sauvegarde et restauration BlueXP](#)" sauvegarde de volumes dans un stockage objet à faible coût

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

Vous pouvez configurer un seul compte de service et l'utiliser dans les deux cas. Le compte de service doit avoir le rôle **Administrateur de stockage**.

Étapes

1. Dans la console Google Cloud, "[Accédez 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. **Accordez à ce compte de service l'accès au projet** : sélectionnez le rôle **Administrateur de stockage**.



- c. **Accordez aux utilisateurs l'accès à ce compte de service** : ajoutez le compte de service Connector en tant qu'utilisateur *Service Account* à ce nouveau compte de service.

Cette étape est uniquement requise pour le Tiering des données. Elle n'est pas requise pour la sauvegarde et la restauration BlueXP.

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

Et la suite ?

Vous devrez ensuite sélectionner le compte de service lors de la création d'un environnement de travail Cloud Volumes ONTAP.

Details and Credentials

default-project	gcp-sub2	Edit Project
Google Cloud Project	Marketplace Subscription	

Details

Working Environment Name (Cluster Name)

Service Account

Service Account Name

[+ Add Labels](#) Optional Field | Up to four labels

Credentials

User Name

Password

Confirm Password

Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser l'API BlueXP pour créer un système Cloud Volumes ONTAP qui utilise des clés de chiffrement *gérées par le client*. Il s'agit des clés que vous créez et gérez dans GCP à l'aide du service Cloud Key Management.

Étapes

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

Les autorisations sont fournies dans le "[Par défaut, Connector service account permissions](#)", Mais ne peut pas être appliqué si vous utilisez un autre projet pour le service Cloud Key Management.

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 du "[Agent de service Google Compute Engine](#)" Dispose

d'autorisations de chiffrement/déchiffrement de clés KMS sur le Cloud.

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

["Google Cloud Documentation : utilisation de l'IAM avec Cloud KMS - attribution de rôles sur une ressource"](#)

3. Obtenir l'ID de la clé en invoquant la commande obtenir pour le `/gcp/vsa/metadata/gcp-encryption-keys` Ou en choisissant « Copy Resource Name » (Copier le nom de la ressource) sur la clé de la console GCP.
4. Si vous utilisez des clés de chiffrement gérées par le client et hiérarchise les données vers le stockage objet, BlueXP tente d'utiliser les clés qui sont utilisées pour chiffrer les disques persistants. Toutefois, vous devez d'abord activer les compartiments Google Cloud Storage pour utiliser les clés :
 - a. Recherchez l'agent de service Google Cloud Storage en suivant le ["Documentation Google Cloud : comment obtenir l'agent de service Cloud Storage"](#).
 - b. Accédez à la clé de chiffrement et attribuez l'agent de service Google Cloud Storage avec les autorisations de chiffrement/déchiffrement de Cloud KMS.

Pour plus d'informations, reportez-vous à la section ["Google Cloud Documentation : utilisation de clés de chiffrement gérées par le client"](#)

5. Utilisez le paramètre "GcpEncryption" avec votre requête API lors de la création d'un environnement de travail.

Exemple

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

Reportez-vous à la ["Documents d'automatisation BlueXP"](#) Pour plus d'informations sur l'utilisation du paramètre "GcpEncryption".

Configurez la licence pour Cloud Volumes ONTAP dans Google Cloud

Après avoir décidé de l'option de licence que 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 nouvel environnement de travail.

Frémium

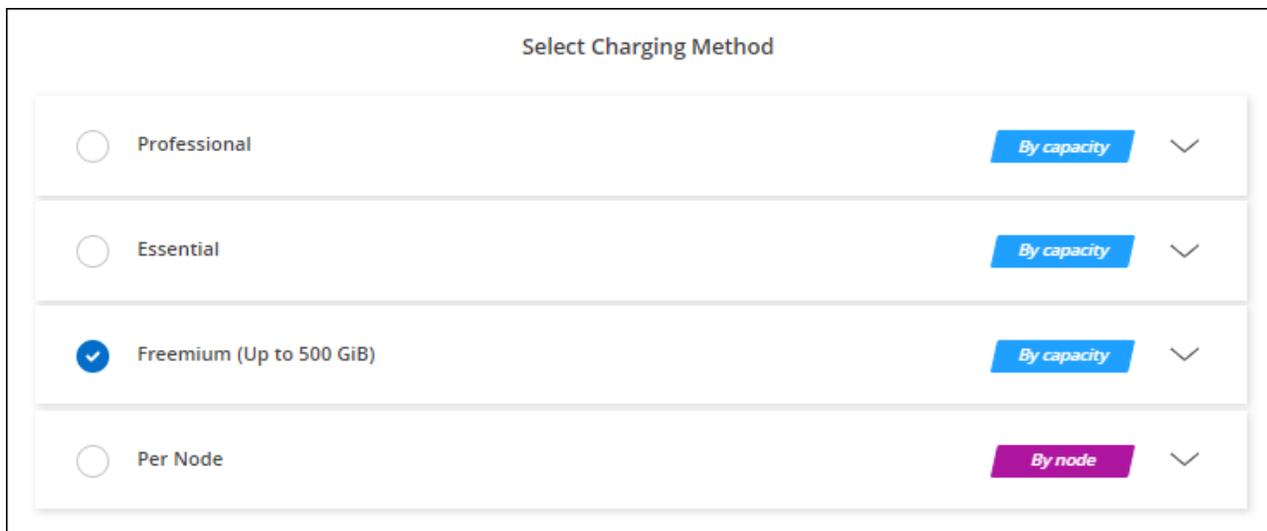
Sélectionnez l'offre « Freemium » pour utiliser Cloud Volumes ONTAP gratuitement et bénéficier d'une capacité provisionnée de 500 Gio. ["En savoir plus sur l'offre Freemium"](#).

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement basé sur l'utilisation dans Google Cloud Marketplace.

Vous ne serez pas facturé via l'abonnement Marketplace sauf si vous dépassez votre capacité provisionnée de 500 Gio, à l'heure où le système est automatiquement converti en "[Pack Essentials](#)".

- b. Après votre retour à BlueXP, sélectionnez **Freemium** lorsque vous atteignez la page méthodes de charge.



The screenshot shows a 'Select Charging Method' dialog box with four rows. Each row contains a radio button, a label, a button, and a dropdown arrow. The 'Freemium (Up to 500 GiB)' row is selected, indicated by a blue checkmark in the radio button and a blue 'By capacity' button. The other rows have unselected radio buttons and blue 'By capacity' buttons. The 'Per Node' row has a purple 'By node' button.

Charging Method	Selected	Button
Professional	No	By capacity
Essential	No	By capacity
Freemium (Up to 500 GiB)	Yes	By capacity
Per Node	No	By node

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud"](#).

Licence basée sur la capacité

La licence basée sur la capacité vous permet de payer pour le Cloud Volumes ONTAP par Tio de capacité. Une licence basée sur la capacité est disponible sous la forme d'un *package* : le package Essentials ou le pack Professional.

Les packs Essentials et Professional sont disponibles avec les modèles de consommation suivants :

- Licence (BYOL) achetée auprès de NetApp
- Un abonnement à l'heure avec paiement à l'utilisation (PAYGO) à partir de Google Cloud Marketplace
- Un contrat annuel

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

Les sections suivantes expliquent comment commencer avec chacun de ces modèles de consommation.

BYOL

Payez l'achat initial d'une licence (BYOL) auprès de NetApp pour le déploiement des systèmes Cloud Volumes ONTAP, quel que soit le fournisseur de cloud.

Étapes

1. ["Contactez l'équipe commerciale de NetApp pour obtenir une licence"](#)
2. ["Ajoutez votre compte sur le site de support NetApp à BlueXP"](#)

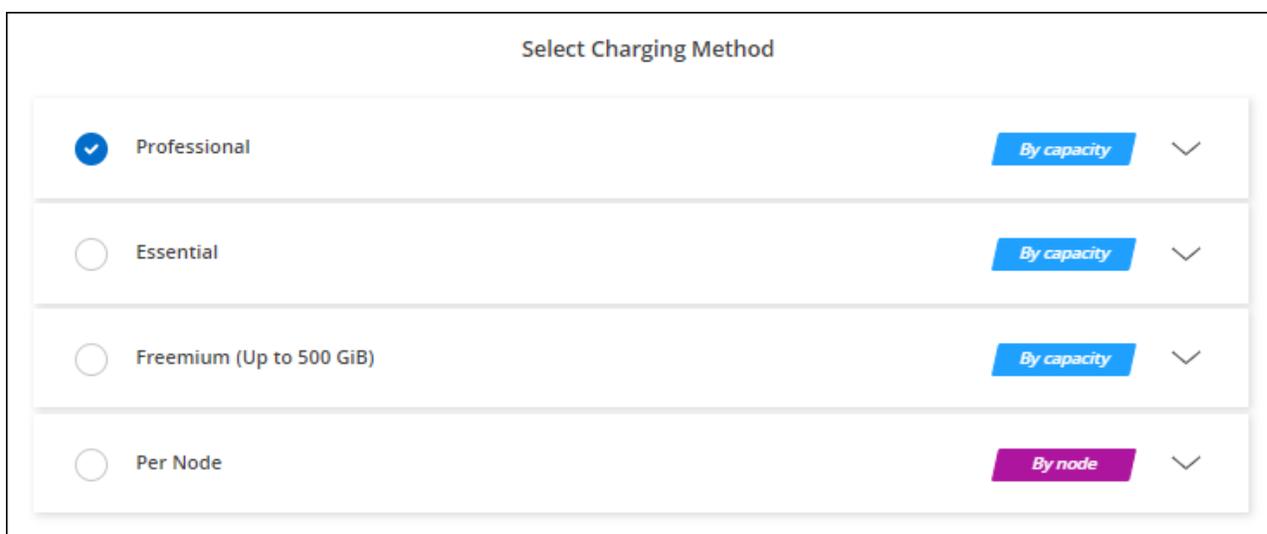
BlueXP interroge automatiquement le service des licences NetApp pour obtenir des informations sur les licences associées à votre compte sur le site de support NetApp. S'il n'y a pas d'erreur, BlueXP ajoute automatiquement les licences au portefeuille digital.

Votre licence doit être disponible auprès du portefeuille digital BlueXP avant que vous ne puissiez l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez ["Ajoutez manuellement la licence au portefeuille digital BlueXP"](#).

3. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement basé sur l'utilisation dans Google Cloud Marketplace.

La licence que vous avez achetée auprès de NetApp est toujours facturée en premier. Elle vous sera facturée à l'heure du marché en cas de dépassement de votre capacité autorisée ou d'expiration de la licence.

- b. Après votre retour à BlueXP, sélectionnez un package basé sur la capacité lorsque vous accédez à la page méthodes de charge.



Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud"](#).

Abonnement PAYGO

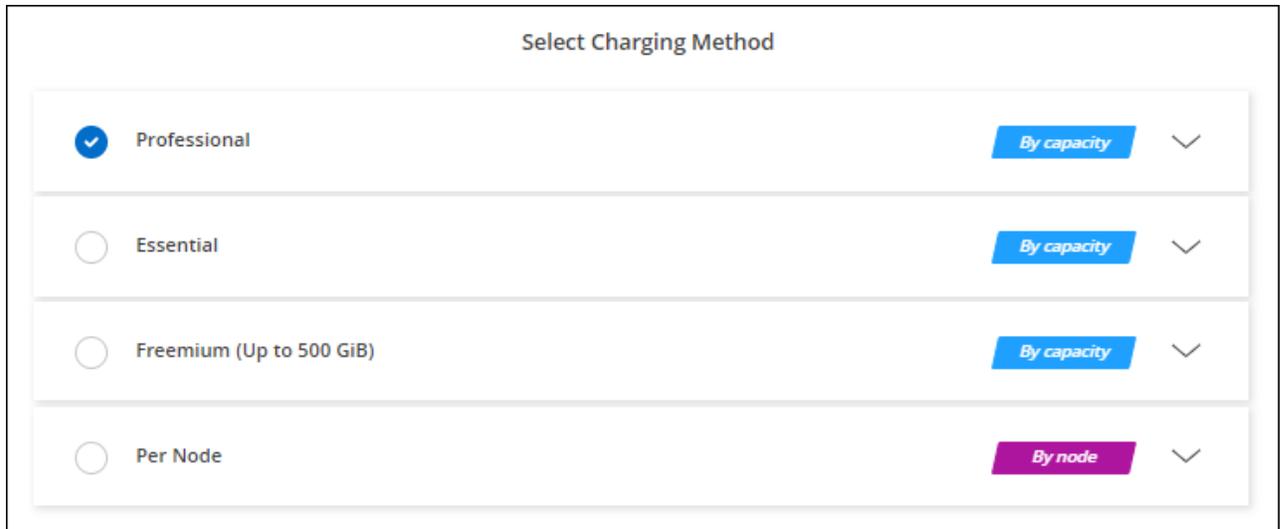
Payez votre abonnement à l'heure par abonnement à l'offre sur le marché de votre fournisseur cloud.

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, BlueXP vous invite à vous abonner au contrat disponible sur Google Cloud Marketplace. Cet abonnement est ensuite associé à l'environnement de travail pour la facturation. Vous pouvez utiliser ce même abonnement pour d'autres environnements de travail.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.

2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement basé sur l'utilisation dans Google Cloud Marketplace.
 - b. Après votre retour à BlueXP, sélectionnez un package basé sur la capacité lorsque vous accédez à la page méthodes de charge.



The screenshot shows a 'Select Charging Method' dialog box with four options. The 'Professional' option is selected, indicated by a blue checkmark in a circle. 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-pointing chevron icon. The buttons for 'By capacity' are blue, while the button for 'By node' is purple.

["Consultez des instructions détaillées 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 par l'achat d'un contrat annuel.

Étapes

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

Le contrat est disponible sous la forme d'une offre *privée* dans Google Cloud Marketplace.

Une fois que NetApp vous a proposé de partager son offre privée, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à Google Cloud Marketplace lors de la création de votre environnement de travail.

2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner au plan annuel dans Google Cloud Marketplace.
 - b. Dans Google Cloud, sélectionnez le plan annuel partagé avec votre compte, puis cliquez sur **Abonnez-vous**.
 - c. Après votre retour à BlueXP, sélectionnez un package basé sur la capacité lorsque vous accédez à la page méthodes de charge.

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	∨
<input type="radio"/> Essential	By capacity	∨
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	∨
<input type="radio"/> Per Node	By node	∨

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud"](#).

Abonnement Keystone

L'abonnement Keystone est un service d'abonnement avec paiement basé sur l'utilisation. ["En savoir plus sur les abonnements NetApp Keystone"](#).

Étapes

1. Si vous n'avez pas encore d'abonnement, ["Contactez NetApp"](#)
2. [Mailto:ng-keystone-success@netapp.com](mailto:ng-keystone-success@netapp.com)[Contactez NetApp] pour autoriser votre compte utilisateur BlueXP avec un ou plusieurs abonnements Keystone.
3. Après que NetApp autorise votre compte, ["Associez vos abonnements pour une utilisation avec Cloud Volumes ONTAP"](#).
4. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - 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 des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud".](#)

Lancement d'Cloud Volumes ONTAP dans Google Cloud

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

Avant de commencer

Vous avez besoin des éléments suivants pour créer un environnement de travail.

- Un connecteur opérationnel.
 - Vous devez avoir un ["Connecteur associé à votre espace de travail"](#).
 - ["Vous devez être prêt à laisser le connecteur fonctionner en permanence"](#).
 - Compte de service associé au connecteur ["doit disposer des autorisations requises"](#)
- Compréhension de la configuration que vous voulez utiliser.

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

- Comprendre les exigences de configuration des licences pour Cloud Volumes ONTAP.

["Découvrez comment configurer les licences"](#).

- Les API Google Cloud doivent être de ["activé dans votre projet"](#):
 - API Cloud Deployment Manager V2
 - API de journalisation cloud
 - API Cloud Resource Manager
 - API du moteur de calcul
 - API de gestion des identités et des accès

Lancement d'un système à un seul nœud dans Google Cloud

Créez un environnement de travail dans BlueXP pour lancer Cloud Volumes ONTAP dans Google Cloud.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP**.
4. Si vous y êtes invité, ["Créer un connecteur"](#).
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 champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Google Cloud VM. 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 "tiering des données" ou "Sauvegarde et restauration BlueXP" Avec Cloud Volumes ONTAP, vous devez alors activer compte de service et sélectionner un compte de service disposant du rôle d'administrateur de stockage prédéfini. "Découvrez comment créer un compte de service" .
Ajouter des étiquettes	<p>Les étiquettes sont des métadonnées pour vos ressources Google Cloud. BlueXP ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources Google Cloud associées au système.</p> <p>Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail.</p> <p>Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Google Cloud : étiquetage des ressources".</p>

Champ	Description
Nom d'utilisateur et mot de passe	Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	<p>Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet où réside BlueXP.</p> <p>Si vous ne voyez pas de projets supplémentaires dans la liste déroulante, alors vous n'avez pas encore associé le compte de service BlueXP à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Il s'agit du compte de service que vous avez configuré pour BlueXP, "comme décrit sur cette page". </div> <p>Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet Google Cloud associé à un abonnement à Cloud Volumes ONTAP depuis Google Cloud Marketplace.</p>

La vidéo suivante explique comment associer un abonnement au Marketplace à paiement basé sur l'utilisation à votre projet Google Cloud. Vous pouvez également suivre les étapes pour vous abonner à la "[Association d'un abonnement Marketplace aux identifiants Google Cloud](#)" section.

► https://docs.netapp.com/fr-fr/test//media/video_subscribing_gcp.mp4 (video)

- Services** : sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner la sauvegarde et la restauration BlueXP ou pour utiliser le Tiering BlueXP, vous devez avoir spécifié le compte de service à l'étape 3.



Si vous souhaitez utiliser le Tiering WORM et des données, vous devez désactiver la sauvegarde et la restauration BlueXP et déployer un environnement de travail Cloud Volumes ONTAP avec la version 9.8 ou supérieure.

- Localisation et connectivité** : sélectionnez un emplacement, choisissez une stratégie de pare-feu et confirmez la connectivité réseau au stockage Google Cloud pour le Tiering des données.

Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Vérification de la connectivité	Pour déplacer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section " Documentation Google Cloud : configuration de Private Google Access ".

Champ	Description
Politique de pare-feu générée	<p>Si vous laissez BlueXP générer la stratégie de pare-feu pour vous, vous devez choisir comment autoriser le trafic :</p> <ul style="list-style-type: none"> • Si vous choisissez VPC sélectionné uniquement, le filtre source pour le trafic entrant est la plage de sous-réseau du VPC sélectionné et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de 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.
Utilisez la politique de pare-feu existante	<p>Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises. Lien : Learn à propos des règles de pare-feu pour Cloud Volumes ONTAP.</p>

8. **Méthodes de chargement et compte NSS** : spécifiez l'option de chargement à utiliser avec ce système, puis spécifiez un compte sur le site de support NetApp.

- "[Découvrez les options de licence pour Cloud Volumes ONTAP](#)".
- "[Découvrez comment configurer les licences](#)".

9. **Packages préconfigurés** : sélectionnez 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, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP en fonction des besoins et sélectionnez un type de machine.



Si une version plus récente, General Availability ou patch est disponible pour la version sélectionnée, BlueXP met à jour le système vers cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.10.1 et 9.10.1 P4. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

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 autre type de disque pour les volumes suivants.

La taille des disques correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

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

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

- Activez **Flash cache**, si vous le souhaitez.



À partir de Cloud Volumes ONTAP 9.13.1, *Flash cache* est pris en charge sur les types d'instances n2-standard-16, n2-standard-32, n2-standard-48 et n2-standard-64. Vous ne pouvez pas désactiver Flash cache après le déploiement.

b. Choisissez **Normal** ou **vitesse d'écriture élevée**, si vous le souhaitez.

["En savoir plus sur la 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**. En outre, pour augmenter la MTU de 9 8,896, les VPC-1, VPC-2 et VPC-3 doivent être sélectionnés pour le déploiement. Pour plus d'informations sur les modèles VPC-1, VPC-2 et VPC-3, reportez-vous à la section ["Règles pour VPC-1, VPC-2 et VPC-3"](#).

c. Activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

LA FONCTION WORM ne peut pas être activée si le Tiering des données était activé pour les versions Cloud Volumes ONTAP 9.7 et ultérieures. La restauration ou la restauration à partir de Cloud Volumes ONTAP 9.8 est bloquée 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. **Tiering de données dans Google Cloud Platform** : choisissez d'activer ou non le Tiering des données sur l'agrégat initial, choisissez une classe de stockage pour les données hiérarchisées, puis sélectionnez un compte de service disposant du rôle d'administrateur de stockage prédéfini (requis pour Cloud Volumes ONTAP 9.7 ou version ultérieure). Ou sélectionnez un compte Google Cloud (obligatoire pour Cloud Volumes ONTAP 9.6).

Notez ce qui suit :

- BlueXP définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. Assurez-vous d'ajouter le compte de service Connector en tant qu'utilisateur du compte de service Tiering, sinon, vous ne pouvez pas le sélectionner dans BlueXP
- Pour obtenir de l'aide sur l'ajout d'un compte Google Cloud, consultez la section ["Configuration et ajout de comptes Google Cloud pour le Tiering des données avec 9.6"](#).
- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants, mais vous devrez désactiver le système et ajouter un compte de service depuis la console Google Cloud.

["En savoir plus sur le Tiering des données"](#).

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

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

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

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP 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 à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune 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)	<p>Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard.</p> <p>Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN.</p> <p>Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN).</p> <p>Lorsque vous créez un volume iSCSI, BlueXP crée automatiquement un LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".</p>

L'image suivante montre la page Volume remplie pour le protocole CIFS :

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS
 CIFS
 iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

15. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	<p>Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS.</p> <p>Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.</p> <p>Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254.</p>
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	<p>Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers.</p> <p>Pour configurer Google Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs,ou=Cloud dans ce champ.</p> <p>"Google Cloud Documentation : les unités organisationnelles de Google Managed Microsoft AD"</p>
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.

Champ	Description
Serveur NTP	<p>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 autre adresse, vous devez utiliser l'API. Voir la "Documents d'automatisation BlueXP" pour plus d'informations.</p> <p>Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS.</p>

16. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

Pour plus d'informations, voir "[Choisissez un profil d'utilisation du volume](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

17. **Revue et approbation** : consultez et confirmez vos choix.

- a. Consultez les détails de la configuration.
- b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources Google Cloud que BlueXP achètera.
- c. Cochez les cases **Je comprends....**
- d. Cliquez sur **Go**.

Résultat

BlueXP déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

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

Pour obtenir de l'aide supplémentaire, consultez la page "[Prise en charge de NetApp Cloud Volumes ONTAP](#)".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez 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 System Manager ou l'interface de ligne de commande.

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.

Lancement d'une paire HA dans Google Cloud

Créez un environnement de travail dans BlueXP pour lancer Cloud Volumes ONTAP dans Google Cloud.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP HA**.

4. **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 champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Google Cloud VM. 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 avez l'intention d'utiliser le " Tiering BlueXP " ou " Sauvegarde et restauration BlueXP " Services, vous devez activer le commutateur compte de service , puis sélectionner le compte de service qui a le rôle d'administrateur de stockage prédéfini.
Ajouter des étiquettes	<p>Les étiquettes sont des métadonnées pour vos ressources Google Cloud. BlueXP ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources Google Cloud associées au système.</p> <p>Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail.</p> <p>Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Google Cloud : étiquetage des ressources".</p>
Nom d'utilisateur et mot de passe	Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	<p>Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet où réside BlueXP.</p> <p>Si vous ne voyez pas de projets supplémentaires dans la liste déroulante, alors vous n'avez pas encore associé le compte de service BlueXP à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Il s'agit du compte de service que vous avez configuré pour BlueXP, "comme décrit sur cette page". </div> <p>Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet Google Cloud associé à un abonnement à Cloud Volumes ONTAP depuis Google Cloud Marketplace.</p>

La vidéo suivante explique comment associer un abonnement au Marketplace à paiement basé sur l'utilisation à votre projet Google Cloud. Vous pouvez également suivre les étapes pour vous abonner à la "Association d'un abonnement Marketplace aux identifiants Google Cloud" section.

► https://docs.netapp.com/fr-fr/test//media/video_subscribing_gcp.mp4 (video)

5. **Services** : sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner la sauvegarde et la restauration BlueXP, ou pour utiliser le Tiering BlueXP, vous devez avoir spécifié le compte de service à l'étape 3.



Si vous souhaitez utiliser le Tiering WORM et des données, vous devez désactiver la sauvegarde et la restauration BlueXP et déployer un environnement de travail Cloud Volumes ONTAP avec la version 9.8 ou supérieure.

6. **Modèles de déploiement haute disponibilité** : choisissez plusieurs zones (recommandé) ou une seule zone pour la configuration haute disponibilité. Sélectionnez ensuite une région et des zones.

"En savoir plus sur les modèles de déploiement pour la haute disponibilité".

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 champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Règle générée	Si vous laissez BlueXP générer la stratégie de pare-feu pour vous, vous devez choisir comment autoriser le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, le filtre source pour le trafic entrant est la plage de sous-réseau du VPC sélectionné et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de 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 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 chargement et compte NSS** : spécifiez l'option de chargement à utiliser avec ce système, puis spécifiez un compte sur le site de support NetApp.
 - "Découvrez les options de licence pour Cloud Volumes ONTAP".
 - "Découvrez comment configurer les licences".
9. **Packages préconfigurés** : sélectionnez 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, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP en fonction des besoins et sélectionnez un type de machine.



Si une version plus récente, General Availability ou patch est disponible pour la version sélectionnée, BlueXP met à jour le système vers cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.10.1 et 9.10.1 P4. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

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 autre type de disque pour les volumes suivants.

La taille des disques correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

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

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

- a. Activez **Flash cache**, si vous le souhaitez.



À partir de Cloud Volumes ONTAP 9.13.1, *Flash cache* est pris en charge sur les types d'instances n2-standard-16, n2-standard-32, n2-standard-48 et n2-standard-64. Vous ne pouvez pas désactiver Flash cache après le déploiement.

- b. Choisissez **Normal** ou **vitesse d'écriture élevée**, si vous le souhaitez.

["En savoir plus sur la 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. En outre, pour augmenter la MTU de 9 8,896, les VPC-1, VPC-2 et VPC-3 doivent être sélectionnés pour le déploiement. Une vitesse d'écriture élevée et un MTU de 9 8,896 dépendent des fonctionnalités et ne peuvent pas être désactivés individuellement dans une instance configurée. Pour plus d'informations sur les modèles VPC-1, VPC-2 et VPC-3, reportez-vous à la section "[Règles pour VPC-1, VPC-2 et VPC-3](#)".

- c. Activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

LA FONCTION WORM ne peut pas être activée si le Tiering des données était activé pour les versions Cloud Volumes ONTAP 9.7 et ultérieures. La restauration ou la restauration à partir de Cloud Volumes ONTAP 9.8 est bloquée 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. **Tiering de données dans Google Cloud** : choisissez d'activer ou non le Tiering de données sur l'agrégat

initial, choisissez une classe de stockage pour les données hiérarchisées, puis sélectionnez un compte de service avec le rôle d'administrateur de stockage prédéfini.

Notez ce qui suit :

- BlueXP définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. Assurez-vous d'ajouter le compte de service Connector en tant qu'utilisateur du compte de service Tiering, sinon, vous ne pouvez pas le sélectionner dans BlueXP.
- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants, mais vous devrez désactiver le système et ajouter un compte de service depuis la console Google Cloud.

["En savoir plus sur le Tiering des données"](#).

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

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

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

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP 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 à l'aide du format domaine\nnom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune 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.

Champ	Description
Groupe initiateur et IQN (pour iSCSI uniquement)	<p>Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard.</p> <p>Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN.</p> <p>Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN).</p> <p>Lorsque vous créez un volume iSCSI, BlueXP crée automatiquement un LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".</p>

L'image suivante montre la page Volume remplie pour le protocole CIFS :

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS
 CIFS
 iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

15. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	<p>Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS.</p> <p>Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.</p> <p>Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254.</p>
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.

Champ	Description
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer Google Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs,ou=Cloud dans ce champ. "Google Cloud Documentation : les unités organisationnelles de 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 identique au 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 autre adresse, vous devez utiliser l'API. Voir la "Documents d'automatisation BlueXP" pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS.

16. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

Pour plus d'informations, voir ["Choisissez un profil d'utilisation du volume"](#) et ["Vue d'ensemble du hiérarchisation des données"](#).

17. **Revue et approbation** : consultez et confirmez vos choix.

- a. Consultez les détails de la configuration.
- b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources Google Cloud que BlueXP achètera.
- c. Cochez les cases **Je comprends....**
- d. Cliquez sur **Go**.

Résultat

BlueXP déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

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

Pour obtenir de l'aide supplémentaire, consultez la page ["Prise en charge de NetApp Cloud Volumes ONTAP"](#).

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez 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 System Manager ou l'interface de ligne de commande.

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.

Vérification des images Google Cloud Platform

Présentation de la vérification des images Google Cloud

La vérification des images 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 GCP à l'aide du résumé signé et du certificat public pour Google Cloud qui peuvent être téléchargés via "[NSS](#)" pour une version spécifique.



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

Convertissez l'image au format brut sur Google Cloud

L'image utilisée pour déployer de nouvelles instances, mettre à niveau ou être utilisée dans des images existantes sera partagée avec les clients via "[Site du support NetApp \(NSS\)](#)". Le résumé signé et les certificats seront disponibles au téléchargement sur le portail NSS. Assurez-vous de télécharger le résumé et les certificats de la version appropriée correspondant à l'image partagée par le support NetApp. Par exemple, 9.13.0 images auront un condensé signé de 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. Pour vérifier l'image par rapport au Digest signé et aux certificats, vous devez disposer d'un mécanisme pour comparer les deux fichiers et télécharger l'image. Pour ce faire, vous devez exporter/convertir l'image au format disk.RAW et enregistrer les résultats dans un compartiment de stockage sur Google Cloud. Le fichier disk.RAW est barré et gzippé dans le processus.

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

- Accès au compartiment de stockage Google
- Écrire dans le compartiment Google Storage
- Création de travaux de construction de nuage (utilisés lors du processus d'exportation)
- Permet d'accéder à l'image souhaitée
- Créer des tâches d'exportation d'images

Pour vérifier l'image, celle-ci 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 le stockage cloud est d'utiliser le "[commande d'exportation des images de calcul gcloud](#)". Cette commande prend l'image fournie et la convertit en un fichier disk.RAW qui est tarred et gzip. Le fichier généré est enregistré à l'URL de destination et peut ensuite être téléchargé pour vérification.

L'utilisateur/le compte doit disposer des privilèges d'accès et d'écriture au compartiment souhaité, exporter l'image et les versions de Cloud (utilisées par Google pour exporter l'image) pour exécuter cette opération.

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

Cliquez pour afficher le script

```
$ 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 des fichiers compressés

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



Voir "[Document Google Cloud sur l'exportation d'une image](#)" Pour plus d'informations sur l'exportation d'une image via Google Cloud.

Vérification de la signature d'image

Vérifier les images signées Google Cloud

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

Résumé du flux de travail de vérification des images signées

Voici une présentation du workflow de vérification des images signées Google Cloud.

- À partir du "[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 9.13.0

Date Posted:

Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software.

A state license for importing encryption equipment is required to import ONTAP 9.1 (or later) with NetApp Volume Encryption into Member States of the Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to this software.

Consult your legal advisor on this matter.

Cloud Volumes ONTAP
Non-Restricted Countries

If you are upgrading to ONTAP 9.13.0, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9130_V_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_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 9130_V_NODAR_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP
Google Image Digest Files

[DOWNLOAD GCP-X-9-13-0_PKG.TAR.GZ \[7.52 KB\]](#)

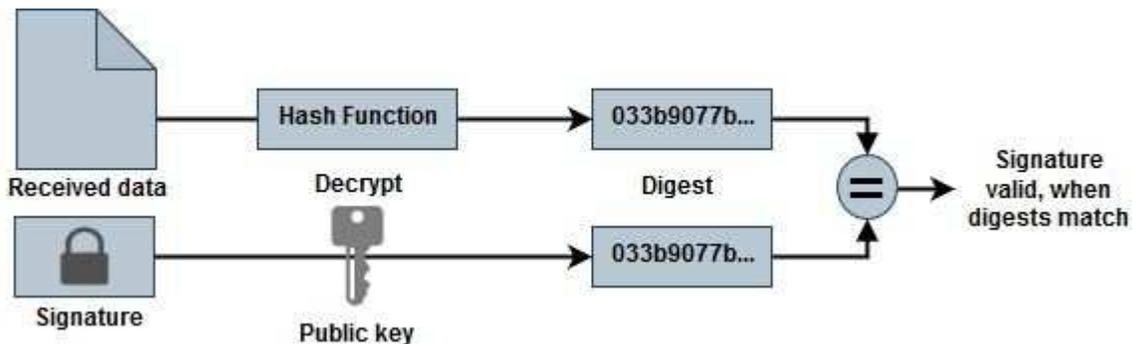
[View and download checksums](#)

Azure Image Digest File

[DOWNLOAD AZURE-9.13.0_PKG.TAR.GZ \[7.55 KB\]](#)

[View and download checksums](#)

- Téléchargez le fichier disque.RAW converti
- Validez le certificat à l'aide de la chaîne de certificats
- Validez le résumé signé à l'aide du certificat contenant la clé publique
 - Déchiffrez le résumé signé à l'aide de la clé publique pour extraire le résumé du fichier image
 - Créez un résumé du fichier disk.RAW téléchargé
 - Comparez les deux fichiers d'analyse pour validation



Vérification du contenu des fichiers disk.RAW et digest à l'aide d'OpenSSL

Vous pouvez vérifier le fichier Disk.RAW téléchargé de Google Cloud par rapport au contenu du fichier condensé disponible via le "NSS" Utilisation d'OpenSSL.



Les commandes OpenSSL permettant de valider l'image sont compatibles avec les machines Linux, Mac OS et Windows.

Étapes

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

Cliquez pour afficher le script

```
# 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 ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsf -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 ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocspl -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: CE894F8251AA15A28462CA312361D261F8F8FE78

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. Extrayez la clé publique du certificat à l'aide d'OpenSSL.
4. Déchiffrez la signature à l'aide de la clé publique extraite et vérifiez le contenu du fichier disk.RAW téléchargé.

Cliquez pour afficher le script

```
# 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 © 2024 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 DÉLICTEUELLE (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.