



Commencez

Cloud Volumes ONTAP

NetApp
January 04, 2023

Table des matières

- Commencez 1
 - Découvrez Cloud Volumes ONTAP 1
 - Versions prises en charge pour les nouveaux déploiements 2
 - Lancez-vous dans Amazon Web Services 3
 - Commencez avec Microsoft Azure 75
 - Lancez-vous dans Google Cloud 115

Commencez

Découvrez Cloud Volumes ONTAP

Avec Cloud Volumes ONTAP, vous optimisez les performances et les coûts de stockage cloud tout en améliorant la protection, la sécurité et la conformité des données.

Cloud Volumes ONTAP est une appliance de stockage exclusivement logicielle qui exécute le logiciel de gestion des données ONTAP dans le cloud. Il offre un système de stockage haute performance doté de plusieurs fonctionnalités clés :

- Fonctionnalités d'efficacité du stockage

Exploitez les fonctionnalités intégrées de déduplication et de compression des données, de provisionnement fin et de clonage pour réduire les coûts de stockage.

- Haute disponibilité

Fiabilité exceptionnelle et continuité de l'activité en cas de défaillances dans votre environnement cloud.

- Protection des données

Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication leader du secteur, pour répliquer les données sur site vers le cloud. Ainsi, il est possible de disposer de copies secondaires dans différents cas d'utilisation.

Cloud Volumes ONTAP s'intègre également avec Cloud Backup pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.

["En savoir plus sur Cloud Backup"](#)

- Tiering des données

Basculez entre pools de stockage hautes performances et faibles performances à la demande sans interrompre les applications.

- La cohérence des applications

Cohérence des copies NetApp Snapshot avec NetApp SnapCenter

["En savoir plus sur SnapCenter"](#)

- Sécurité des données

Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.

- Contrôles de conformité à la confidentialité

L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

["Pour en savoir plus sur Cloud Data Sense"](#)



Les licences des fonctionnalités ONTAP sont incluses dans Cloud Volumes ONTAP.

["Afficher les configurations Cloud Volumes ONTAP prises en charge"](#)

["En savoir plus sur Cloud Volumes ONTAP"](#)

Versions prises en charge pour les nouveaux déploiements

BlueXP vous permet de choisir parmi plusieurs versions ONTAP différentes lorsque vous créez un nouvel environnement de travail Cloud Volumes ONTAP.

Toutes les autres versions de Cloud Volumes ONTAP ne sont pas prises en charge par les nouveaux déploiements.

AWS

Un seul nœud

- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Paire HA

- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

Un seul nœud

- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8

- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

Paire HA

- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

Un seul nœud

- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

Paire HA

- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Lancez-vous dans Amazon Web Services

Démarrage rapide de Cloud Volumes ONTAP dans AWS

Découvrez Cloud Volumes ONTAP dans AWS en quelques étapes.



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 AWS](#)".

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, BlueXP (anciennement Cloud Manager) vous invite à déployer un connecteur si vous n'en avez pas encore.

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 >>"](#).

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. Activez l'accès Internet sortant à partir du VPC cible de sorte que le connecteur et le Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour ["Le connecteur et le Cloud Volumes ONTAP"](#).

3. Configurez un terminal VPC sur le service S3.

Un point de terminaison VPC est requis si vous souhaitez transférer des données à froid de Cloud Volumes ONTAP vers un stockage objet économique.

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

4

Configuration du KMS AWS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, vous devez vous assurer qu'une clé principale client (CMK) active existe. Vous devez également modifier la stratégie de clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations au connecteur en tant qu'utilisateur *key*. ["En savoir plus >>"](#).

5

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"](#)
- ["Lancement d'un connecteur depuis AWS Marketplace"](#)
- ["Installation du logiciel du connecteur sur un hôte Linux"](#)
- ["Ce que BlueXP fait avec les autorisations AWS"](#)

Planification de votre configuration Cloud Volumes ONTAP dans AWS

Lorsque vous déployez Cloud Volumes ONTAP dans AWS, 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 AWS. ["Afficher la liste complète des régions prises en charge"](#).

Les régions AWS plus récentes doivent être activées avant de pouvoir créer et gérer des ressources dans ces régions. ["Découvrez comment activer une région"](#).

Choisissez une instance prise en charge

Cloud Volumes ONTAP prend en charge plusieurs types d'instances, selon le type de licence choisi.

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

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 AWS"](#)

Dimensionnez votre système dans AWS

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 d'instance, d'un type de disque et d'une taille de disque :

Type d'instance

- Assurez-vous que les exigences de vos workloads correspondent aux valeurs maximales de débit et d'IOPS pour chaque type d'instance EC2.
- Si plusieurs utilisateurs écrivent dans le système en même temps, choisissez un type d'instance disposant de suffisamment de processeurs pour gérer les requêtes.
- Si votre champ d'application implique essentiellement la lecture, optez pour un système disposant de suffisamment de mémoire RAM.
 - ["Documentation AWS : types d'instances Amazon EC2"](#)

- ["Documentation AWS : instances optimisées pour Amazon EBS"](#)

Type de disque EBS

À un niveau élevé, les différences entre les types de disques EBS sont les suivantes. Pour en savoir plus sur les cas d'utilisation de disques EBS, consultez la ["Documentation AWS : types de volume EBS"](#).

- *Les disques SSD à usage générique (gp3)* sont les disques SSD les plus économiques qui permettent d'équilibrer les coûts et les performances pour une grande variété de charges de travail. Les performances sont définies en termes d'IOPS et de débit. Les disques gp3 sont pris en charge par Cloud Volumes ONTAP 9.7 et versions ultérieures.

Lorsque vous sélectionnez un disque gp3, BlueXP remplit les valeurs d'IOPS et de débit par défaut qui fournissent des performances équivalentes à un disque gp2 en fonction de la taille de disque sélectionnée. Vous pouvez augmenter les valeurs pour obtenir de meilleures performances à un coût plus élevé, mais nous ne prenons pas en charge des valeurs plus faibles, car cela peut entraîner des performances inférieures. En bref, collez-les avec les valeurs par défaut ou augmentez-les. Ne les baissez pas. ["En savoir plus sur les disques gp3 et leurs performances"](#).

Notez que Cloud Volumes ONTAP prend en charge la fonctionnalité Amazon EBS Elastic volumes avec des disques gp3. ["En savoir plus sur la prise en charge d'Elastic volumes"](#).

- *Disques SSD à usage générique (gp2)* permettent d'équilibrer les coûts et les performances pour une grande variété de charges de travail. La performance est définie en termes d'IOPS.
- *Les disques SSD (io1) d'IOPS provisionnés* sont destinés aux applications stratégiques qui exigent des performances élevées à un coût plus élevé.

Notez que Cloud Volumes ONTAP prend en charge la fonctionnalité Amazon EBS Elastic volumes avec des disques io1. ["En savoir plus sur la prise en charge d'Elastic volumes"](#).

- *Les disques durs à débit optimisé (st1)* sont destinés aux charges de travail fréquemment utilisées qui exigent un débit rapide et constant à un prix inférieur.



Il n'est pas recommandé de faire le Tiering des données dans le stockage objet lors de l'utilisation de disques durs à débit optimisé (st1).

Taille des disques EBS

Si vous choisissez une configuration qui ne prend pas en charge le ["Fonctionnalité Amazon EBS Elastic volumes"](#), Puis vous devez choisir une taille de disque initiale lorsque vous lancez un système Cloud Volumes ONTAP. Après cela, vous pouvez ["Laissez BlueXP gérer la capacité d'un système pour vous"](#), mais si vous voulez ["créez des agrégats vous-même"](#), soyez conscient des éléments suivants :

- Tous les disques qui composent un agrégat doivent être de la même taille.
- Les performances des disques EBS sont liées à leur taille. La taille détermine les IOPS de base et la durée maximale en rafale pour les disques SSD, ainsi que le débit de base et en rafale pour les disques HDD.
- Finalement, vous devez choisir la taille de disque qui vous donne le *performances soutenues* dont vous avez besoin.
- Même si vous choisissez des disques de plus grande capacité (par exemple six disques de 4 To), vous risquez de ne pas obtenir toutes les IOPS, car l'instance EC2 peut atteindre sa limite de bande passante.

Pour en savoir plus sur les performances des disques EBS, consultez la ["Documentation AWS : types"](#)

de volume EBS".

Comme indiqué ci-dessus, le choix de la taille de disque n'est pas pris en charge avec les configurations Cloud Volumes ONTAP qui prennent en charge la fonctionnalité Amazon EBS Elastic volumes. ["En savoir plus sur la prise en charge d'Elastic volumes"](#).

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 AWS"](#).



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

Préparez-vous à déployer Cloud Volumes ONTAP dans un post-production AWS

Si vous disposez d'un poste externe AWS, vous pouvez déployer Cloud Volumes ONTAP dans cet envoi en sélectionnant le VPC Outpost dans l'assistant Environnement de travail. L'expérience est la même que tout autre VPC qui réside dans AWS. Notez que vous devez d'abord déployer un connecteur dans votre courrier d'envoi AWS.

Quelques limites peuvent être souligner :

- Actuellement, seuls les systèmes Cloud Volumes ONTAP à un seul nœud sont pris en charge
- Les instances EC2 que vous pouvez utiliser avec Cloud Volumes ONTAP sont limitées à ce que votre Outpost propose
- Seuls les disques SSD polyvalents (gp2) sont pris en charge à l'heure actuelle

Collecte d'informations de mise en réseau

Lorsque vous lancez Cloud Volumes ONTAP dans AWS, vous devez spécifier des informations concernant votre réseau VPC. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Un seul nœud ou une paire haute disponibilité dans une seule zone de disponibilité

Informations sur AWS	Votre valeur
Région	
VPC	
Sous-réseau	
Groupe de sécurité (s'il s'agit du vôtre)	

Paire HA dans plusieurs AZS

Informations sur AWS	Votre valeur
Région	
VPC	
Groupe de sécurité (s'il s'agit du vôtre)	
Zone de disponibilité du nœud 1	
Sous-réseau de nœud 1	
Zone de disponibilité du nœud 2	
Sous-réseau de nœud 2	
Zone de disponibilité d'un médiateur	
Sous-réseau médiateur	
Paire de touches pour le médiateur	
Adresse IP flottante pour le port de gestion du cluster	
Adresse IP flottante pour les données du nœud 1	
Adresse IP flottante pour les données du nœud 2	
Tables de routage pour les adresses IP flottantes	

Choisissez une vitesse d'écriture

BlueXP vous permet de choisir un paramètre de vitesse d'écriture pour Cloud Volumes ONTAP. 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.

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

BlueXP (anciennement Cloud Manager) gère la configuration des composants réseau pour Cloud Volumes ONTAP, tels que les adresses IP, les masques réseau et les routes. Vous devez vous assurer que l'accès Internet sortant est disponible, que suffisamment d'adresses IP privées sont disponibles, que les bonnes connexions sont en place, et bien plus encore.

Exigences générales

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour l'AutoSupport, qui surveille 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 vous disposez d'une instance NAT, vous devez définir une règle de groupe de sécurité entrante qui autorise le trafic HTTPS du sous-réseau privé vers Internet.

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 condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous avez défini des règles sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité 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 BlueXP vous informe que les messages AutoSupport ne peuvent pas être envoyés, ["Résoudre les problèmes de configuration AutoSupport"](#).

Accès Internet sortant pour le médiateur haute disponibilité

L'instance de médiateur haute disponibilité doit disposer d'une connexion sortante au service AWS EC2 pour qu'il puisse faciliter le basculement du stockage. Pour fournir la connexion, vous pouvez ajouter une adresse IP publique, spécifier un serveur proxy ou utiliser une option manuelle.

L'option manuelle peut être une passerelle NAT ou un terminal VPC d'interface, du sous-réseau cible au service AWS EC2. Pour plus de détails sur les terminaux VPC, reportez-vous à "[Documentation AWS : terminaux VPC d'interface \(AWS PrivateLink\)](#)".

Adresses IP privées

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

Adresses IP d'un système à un seul nœud

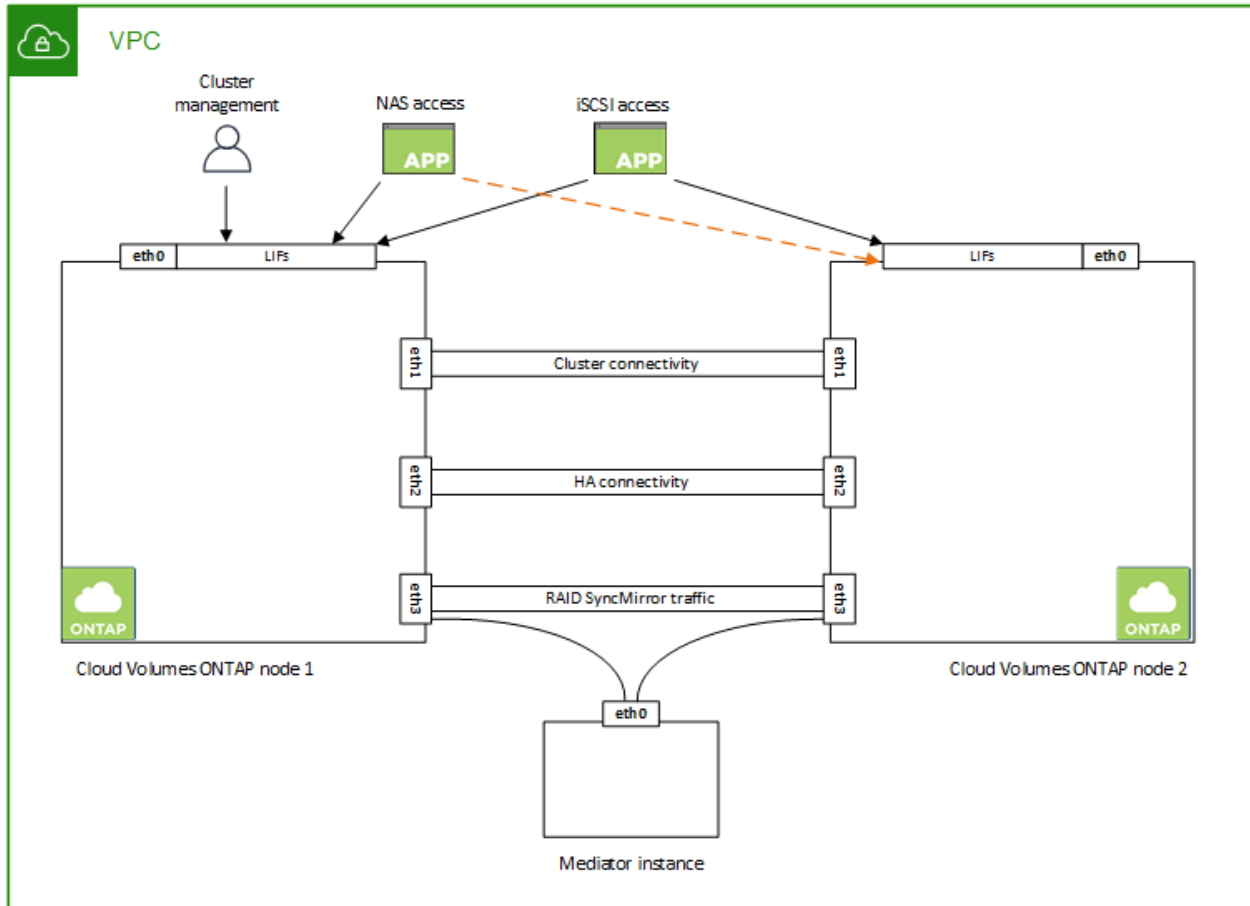
BlueXP alloue 6 adresses IP à un système à nœud unique :

- LIF Cluster-management
- FRV de gestion des nœuds
- FRV InterCluster
- LIF de données NAS
- LIF de données iSCSI
- LIF Storage VM management

Une LIF de gestion de machines virtuelles de stockage est utilisée avec des outils de gestion tels que SnapCenter.

Adresses IP des paires haute disponibilité

Les paires HAUTE DISPONIBILITÉ requièrent plus d'adresses IP qu'un système à un seul nœud. Ces adresses IP sont réparties sur différentes interfaces ethernet, comme illustré dans l'image suivante :



Le nombre d'adresses IP privées requises pour une paire haute disponibilité dépend du modèle de déploiement choisi. Une paire haute disponibilité déployée dans une *single* AWS Availability zone (AZ) requiert 15 adresses IP privées, tandis qu'une paire haute disponibilité déployée dans *multiple* AZS nécessite 13 adresses IP privées.

Les tableaux suivants fournissent des informations détaillées sur les LIF associées à chaque adresse IP privée.

LIF pour les paires haute disponibilité dans une même zone de disponibilité

LIF	Interface	Nœud	Objectif
Gestion du cluster	eth0	nœud 1	Gestion administrative de l'ensemble du cluster (paire HA).
Gestion de nœuds	eth0	les nœuds 1 et 2	Gestion administrative d'un nœud.
Intercluster	eth0	les nœuds 1 et 2	Communication, sauvegarde et réplication entre les clusters
Données NAS	eth0	nœud 1	Accès client via les protocoles NAS.

LIF	Interface	Nœud	Objectif
Données iSCSI	eth0	les nœuds 1 et 2	Accès client via le protocole iSCSI. Également utilisé par le système pour d'autres flux de travail réseau importants. Ces LIFs sont requises et ne doivent pas être supprimées.
Connectivité au cluster	eth1	les nœuds 1 et 2	Permet aux nœuds de communiquer les uns avec les autres et de déplacer les données au sein du cluster.
Connectivité HAUTE DISPONIBILITÉ	eth2	les nœuds 1 et 2	Communication entre les deux nœuds en cas de basculement.
Trafic iSCSI RSM	eth3	les nœuds 1 et 2	Le trafic iSCSI RAID SyncMirror, ainsi que la communication entre les deux nœuds Cloud Volumes ONTAP et le médiateur.
Médiateur	eth0	Médiateur	Canal de communication entre les nœuds et le médiateur pour faciliter les processus de basculement et de rétablissement du stockage.

LIF pour paires haute disponibilité dans plusieurs systèmes AZS

LIF	Interface	Nœud	Objectif
Gestion de nœuds	eth0	les nœuds 1 et 2	Gestion administrative d'un nœud.
Intercluster	eth0	les nœuds 1 et 2	Communication, sauvegarde et réplication entre les clusters
Données iSCSI	eth0	les nœuds 1 et 2	Accès client via le protocole iSCSI. Cette LIF gère également la migration d'adresses IP flottantes entre les nœuds.
Connectivité au cluster	eth1	les nœuds 1 et 2	Permet aux nœuds de communiquer les uns avec les autres et de déplacer les données au sein du cluster.
Connectivité HAUTE DISPONIBILITÉ	eth2	les nœuds 1 et 2	Communication entre les deux nœuds en cas de basculement.
Trafic iSCSI RSM	eth3	les nœuds 1 et 2	Le trafic iSCSI RAID SyncMirror, ainsi que la communication entre les deux nœuds Cloud Volumes ONTAP et le médiateur.
Médiateur	eth0	Médiateur	Canal de communication entre les nœuds et le médiateur pour faciliter les processus de basculement et de rétablissement du stockage.



Lorsqu'il est déployé dans plusieurs zones de disponibilité, plusieurs LIF sont associées à "Adresses IP flottantes", Qui ne sont pas pris en compte par rapport à la limite IP privée AWS.

Groupes de sécurité

Il n'est pas nécessaire de créer des groupes de sécurité car BlueXP le fait pour vous. Si vous devez utiliser votre propre, reportez-vous à la section ["Règles de groupe de sécurité"](#).

Connexion pour le Tiering des données

Si vous souhaitez utiliser EBS comme niveau de performance et AWS S3 comme niveau de capacité, vous devez vous assurer que Cloud Volumes ONTAP est connecté à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section ["Documentation AWS : création d'un terminal de passerelle"](#).

Lorsque vous créez le terminal VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l'instance Cloud Volumes ONTAP. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section ["Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l'aide d'un terminal VPC de passerelle ?"](#)

Connexions aux systèmes ONTAP

Pour répliquer les données entre un système Cloud Volumes ONTAP dans AWS et des systèmes ONTAP d'autres réseaux, vous devez disposer d'une connexion VPN entre le VPC AWS et l'autre réseau, par exemple votre réseau d'entreprise. Pour obtenir des instructions, reportez-vous à la section ["Documentation AWS : configuration d'une connexion VPN AWS"](#).

DNS et Active Directory pour CIFS

Si vous souhaitez provisionner le stockage CIFS, vous devez configurer DNS et Active Directory dans AWS ou étendre votre configuration sur site à AWS.

Le serveur DNS doit fournir des services de résolution de noms pour l'environnement Active Directory. Vous pouvez configurer les jeux d'options DHCP pour qu'ils utilisent le serveur DNS EC2 par défaut, qui ne doit pas être le serveur DNS utilisé par l'environnement Active Directory.

Pour obtenir des instructions, reportez-vous à la section ["Documentation AWS : active Directory Domain Services sur le cloud AWS : déploiement de référence rapide"](#).

Partage de VPC

Depuis la version 9.11.1, les paires haute disponibilité Cloud Volumes ONTAP sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre entreprise de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement AWS, puis déployer la paire HA à l'aide de l'API.

["Découvrez comment déployer une paire haute disponibilité dans un sous-réseau partagé"](#).

Besoins en paires haute disponibilité dans plusieurs AZS

D'autres exigences de mise en réseau AWS s'appliquent aux configurations Cloud Volumes ONTAP HA qui utilisent plusieurs zones de disponibilité (AZS). Vous devez vérifier ces exigences avant de lancer une paire haute disponibilité car vous devez entrer les informations de mise en réseau dans BlueXP lorsque vous créez l'environnement de travail.

Pour comprendre le fonctionnement des paires haute disponibilité, voir ["Paires haute disponibilité"](#).

Zones de disponibilité

Ce modèle de déploiement haute disponibilité utilise plusieurs AZS pour assurer la haute disponibilité de vos données. Vous devez utiliser un système AZ dédié pour chaque instance Cloud Volumes ONTAP et l'instance médiateur, qui fournit un canal de communication entre la paire HA.

Un sous-réseau doit être disponible dans chaque zone de disponibilité.

Adresses IP flottantes pour les données NAS et la gestion de cluster/SVM

Les configurations HAUTE DISPONIBILITÉ de plusieurs AZS utilisent des adresses IP flottantes qui migrent entre les nœuds en cas de défaillance. Sauf vous, ils ne sont pas accessibles de manière native depuis l'extérieur du VPC ["Configuration d'une passerelle de transit AWS"](#).

Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud 1 et l'autre les données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante est facultative pour la gestion des SVM.



Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité.

Vous devez entrer les adresses IP flottantes dans BlueXP lorsque vous créez un environnement de travail Cloud Volumes ONTAP HA. BlueXP alloue les adresses IP à la paire HA lors du lancement du système.

Les adresses IP flottantes doivent être en dehors des blocs CIDR sur tous les VPC de la région AWS dans laquelle vous déployez la configuration HA. Considérez les adresses IP flottantes comme un sous-réseau logique en dehors des VPC de votre région.

L'exemple suivant illustre la relation entre les adresses IP flottantes et les VPC d'une région AWS. Alors que les adresses IP flottantes sont en dehors des blocs CIDR pour tous les VPC, elles sont routables vers les sous-réseaux via des tables de routage.

AWS region



BlueXP crée automatiquement des adresses IP statiques pour l'accès iSCSI et pour l'accès NAS à partir de clients externes au VPC. Vous n'avez pas besoin de répondre à des exigences relatives à ces types d'adresses IP.

Passerelle de transport pour activer l'accès IP flottant depuis l'extérieur du VPC

Si besoin, "[Configuration d'une passerelle de transit AWS](#)" Pour permettre l'accès aux adresses IP flottantes d'une paire haute disponibilité de l'extérieur du VPC où réside la paire haute disponibilité.

Tables de routage

Après avoir spécifié les adresses IP flottantes dans BlueXP, vous êtes invité à sélectionner les tables de routage qui doivent inclure des routes vers les adresses IP flottantes. Cela permet au client d'accéder à la paire haute disponibilité.

Si vous ne disposez que d'une seule table de routage pour les sous-réseaux de votre VPC (la table de routage principale), BlueXP ajoute automatiquement les adresses IP flottantes à cette table de routage. Si vous avez plusieurs tables de routage, il est très important de sélectionner les tables de routage appropriées au lancement de la paire haute disponibilité. Dans le cas contraire, certains clients n'ont peut-être pas accès à Cloud Volumes ONTAP.

Par exemple, vous pouvez avoir deux sous-réseaux associés à différentes tables de routage. Si vous sélectionnez la table de routage A, mais pas la table de routage B, les clients du sous-réseau associé à la table de routage A peuvent accéder à la paire HA, mais les clients du sous-réseau associé à la table de routage B ne peuvent pas.

Pour plus d'informations sur les tables de routage, voir ["Documentation AWS : tables de routage"](#).

Connexion aux outils de gestion NetApp

Pour utiliser les outils de gestion NetApp avec des configurations haute disponibilité figurant dans plusieurs modèles AZS, vous disposez de deux options de connexion :

1. Déployez les outils de gestion NetApp sur un autre VPC et ["Configuration d'une passerelle de transit AWS"](#). La passerelle permet d'accéder à l'adresse IP flottante de l'interface de gestion du cluster à partir de l'extérieur du VPC.
2. Déployez les outils de gestion NetApp sur le même VPC avec une configuration de routage similaire à celle des clients NAS.

Exemple de configuration haute disponibilité

L'image suivante illustre les composants réseau propres à une paire HA dans plusieurs AZS : trois zones de disponibilité, trois sous-réseaux, des adresses IP flottantes et une table de routage.



Configuration requise pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.


Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur dans votre réseau d'entreprise, vous devez configurer une connexion VPN au réseau virtuel dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
https://support.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div> Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.bluexp.netapp.com » dans une prochaine version.</div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au ["Interface utilisateur locale"](#), que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

Il existe un conflit possible avec des adresses IP dans la plage 172. ["En savoir plus sur cette limitation"](#).

Configuration d'une passerelle de transit AWS pour les paires HA dans plusieurs AZS

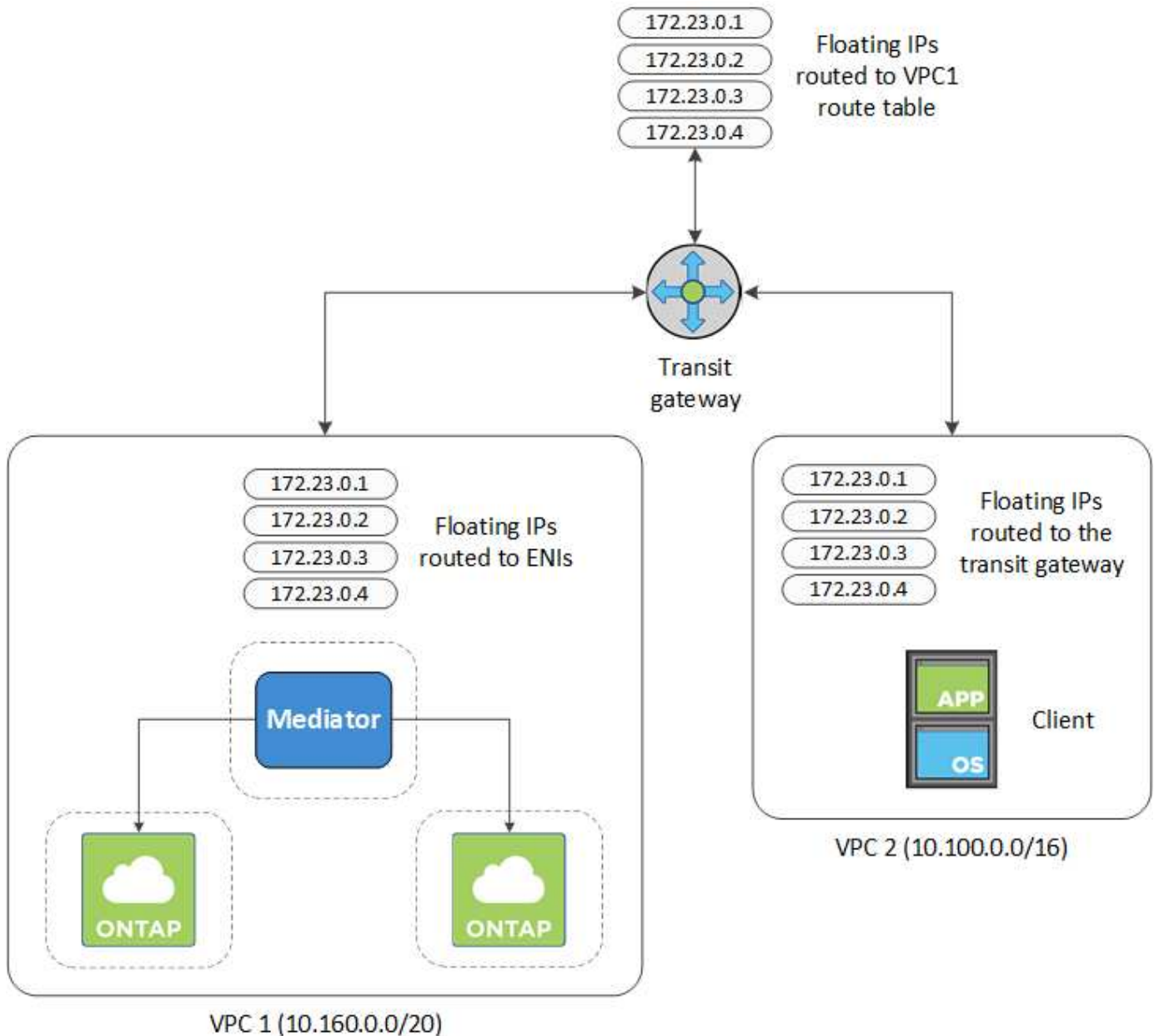
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA ["Adresses IP flottantes"](#) Depuis l'extérieur du VPC, où réside la paire HA.

Lorsqu'une configuration Cloud Volumes ONTAP HA est répartie sur plusieurs zones de disponibilité AWS, des adresses IP flottantes sont nécessaires pour l'accès aux données NAS depuis le VPC. Ces adresses IP flottantes peuvent migrer entre les nœuds en cas de défaillance, mais elles ne sont pas accessibles de manière native en dehors du VPC. Des adresses IP privées séparées permettent un accès aux données depuis l'extérieur du VPC, mais elles ne permettent pas de procéder à un basculement automatique.

Des adresses IP flottantes sont également nécessaires pour l'interface de gestion du cluster et la LIF de gestion du SVM facultative.

Si vous configurez une passerelle de transit AWS, vous activez l'accès aux adresses IP flottantes depuis l'extérieur sur le VPC où réside la paire haute disponibilité. Les clients NAS et les outils de gestion NetApp en dehors du VPC peuvent accéder aux adresses IP flottantes.

Voici un exemple illustrant deux VPC connectés par une passerelle de transit. Un système haute disponibilité réside dans un VPC, tandis qu'un client réside dans l'autre. Vous pouvez ensuite monter un volume NAS sur le client à l'aide de l'adresse IP flottante.



Les étapes suivantes montrent comment configurer une configuration similaire.

Étapes

1. ["Créez une passerelle de transit et connectez les VPC à la passerelle"](#).
2. Associez les VPC à la table de routage de la passerelle de transit.

- Dans le service **VPC**, cliquez sur **Transit Gateway route tables**.
 - Sélectionnez la table de routage.
 - Cliquez sur **associations**, puis sélectionnez **Créer association**.
 - Choisissez les pièces jointes (les VPC) à associer, puis cliquez sur **Créer une association**.
3. Créer des routes dans la table de routage de la passerelle de transit en spécifiant les adresses IP flottantes de la paire HA.

Vous trouverez les adresses IP flottantes sur la page informations sur l'environnement de travail dans BlueXP. Voici un exemple :

NFS & CIFS access from within the VPC using Floating IP

 **Auto failover**

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

L'exemple d'image suivant montre la table de routage pour la passerelle de transit. Il comprend les routes vers les blocs CIDR des deux VPC et quatre adresses IP flottantes utilisées par Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	Floating IP	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	Floating IP	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	Floating IP	static	active

4. Modifiez la table de routage des VPC qui doivent accéder aux adresses IP flottantes.
- Ajoutez des entrées de route aux adresses IP flottantes.
 - Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP
Addresses

5. Modifiez la table de routage du VPC de la paire HA en ajoutant une route vers le VPC qui doit accéder aux adresses IP flottantes.

Cette étape est importante car elle termine le routage entre les VPC.

L'exemple d'image suivant montre la table de routage pour VPC 1. Elle inclut une route vers les adresses IP flottantes et vers VPC 2, c'est-à-dire où réside un client. BlueXP a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire HA.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-f7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2
Floating
act IP
Addresses

6. Montez les volumes sur des clients à l'aide de l'adresse IP flottante.

Vous pouvez trouver l'adresse IP correcte dans BlueXP en sélectionnant un volume et en cliquant sur **Mount Command**.

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



7. Si vous montez un volume NFS, configurez la export policy pour qu'elle corresponde au sous-réseau du VPC client.

"Découvrez comment modifier un volume".

- Liens connexes*
- "Paires haute disponibilité dans AWS"
- "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"

Déploiement d'une paire haute disponibilité dans un sous-réseau partagé

Depuis la version 9.11.1, les paires haute disponibilité Cloud Volumes ONTAP sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre entreprise de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement AWS, puis déployer la paire HA à l'aide de l'API.

Avec "Partage de VPC", Une configuration Cloud Volumes ONTAP HA est répartie sur deux comptes :

- Le compte propriétaire du VPC, qui détient le réseau (le VPC, les sous-réseaux, les tables de routage et le groupe de sécurité Cloud Volumes ONTAP)
- Le compte participant, où les instances EC2 sont déployées dans des sous-réseaux partagés (incluant les deux nœuds HA et le médiateur)

Dans le cas d'une configuration Cloud Volumes ONTAP HA déployée sur plusieurs zones de disponibilité, le médiateur HA a besoin d'autorisations spécifiques pour écrire dans les tables de routage du compte propriétaire VPC. Vous devez fournir ces autorisations en configurant un rôle IAM que le médiateur peut assumer.

L'image suivante montre les composants impliqués dans ce déploiement :



Comme décrit dans les étapes ci-dessous, vous devrez partager les sous-réseaux avec le compte du participant, puis créer le rôle IAM et le groupe de sécurité dans le compte propriétaire VPC.

Lorsque vous créez l'environnement de travail Cloud Volumes ONTAP, BlueXP crée et attache automatiquement un rôle IAM au médiateur. Il part du rôle IAM que vous avez créé dans le compte propriétaire VPC afin de modifier les tables de routage associées à la paire haute disponibilité.

Étapes

1. Partagez les sous-réseaux du compte propriétaire VPC avec le compte du participant.

Cette étape est requise pour déployer la paire haute disponibilité dans les sous-réseaux partagés.

["Documentation AWS : partagez un sous-réseau"](#)

2. Dans le compte propriétaire VPC, créez un groupe de sécurité pour Cloud Volumes ONTAP.

["Voir les règles de groupe de sécurité pour Cloud Volumes ONTAP"](#). Sachez que vous n'avez pas besoin de créer un groupe de sécurité pour le médiateur HA. BlueXP le fait pour vous.

3. Dans le compte propriétaire VPC, créez un rôle IAM qui inclut les autorisations suivantes :

```
"Action": [
    "ec2:AssignPrivateIpAddresses",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcs",
    "ec2:ReplaceRoute",
    "ec2:UnassignPrivateIpAddresses"
```

4. Utilisez l'API BlueXP pour créer un nouvel environnement de travail Cloud Volumes ONTAP.

Notez que vous devez spécifier les champs suivants :

- « SecurityGroupIid »

Le champ « securityGroupIid » doit spécifier le groupe de sécurité que vous avez créé dans le compte propriétaire VPC (voir étape 2 ci-dessus).

- "AssumeRoleArn" dans l'objet "haParams"

Le champ "assumeRoleArn" doit inclure l'ARN du rôle IAM que vous avez créé dans le compte propriétaire VPC (voir l'étape 3 ci-dessus).

Par exemple :

```
"haParams": {
  "assumeRoleArn":
  "arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+

["Découvrez l'API Cloud Volumes ONTAP"](#)

Règles de groupe de sécurité pour AWS

BlueXP crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes que le connecteur et Cloud Volumes ONTAP doivent fonctionner correctement. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Règles pour Cloud Volumes ONTAP

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes

Lorsque vous créez un environnement de travail et choisissez un groupe de sécurité prédéfini, vous pouvez choisir d'autoriser le trafic dans l'un des éléments suivants :

- **VPC sélectionné uniquement** : la source du 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** : la source du trafic entrant est la plage IP 0.0.0.0/0.

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
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
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

Protocole	Port	Objectif
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de 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 les protocoles 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
Sauvegarde vers S3	TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3
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)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
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 le groupe de sécurité externe du médiateur de haute disponibilité

Le groupe de sécurité externe prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles entrantes et sortantes suivantes.

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Connexions SSH au médiateur haute disponibilité
TCP	3000	Accès à l'API RESTful depuis le connecteur

Règles de sortie

Le groupe de sécurité prédéfini du médiateur HA 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 du médiateur HA inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles 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 le médiateur haute disponibilité.

Protocole	Port	Destination	Objectif
HTTP	80	Adresse IP du connecteur	Télécharger les mises à niveau pour le médiateur

Protocole	Port	Destination	Objectif
HTTPS	443	Services API AWS	Assistance pour le basculement du stockage
UDP	53	Services API AWS	Assistance pour le basculement du stockage



Plutôt que d'ouvrir les ports 443 et 53, vous pouvez créer un terminal VPC d'interface à partir du sous-réseau cible vers le service AWS EC2.

Règles du groupe de sécurité interne de la configuration haute disponibilité

Le groupe de sécurité interne prédéfini pour une configuration Cloud Volumes ONTAP HA comprend les règles suivantes. Ce groupe de sécurité permet la communication entre les nœuds HA et entre le médiateur et les nœuds.

BlueXP crée toujours ce groupe de sécurité. Vous n'avez pas la possibilité d'utiliser vos propres ressources.

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles de sortie

Le groupe de sécurité prédéfini inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles pour le connecteur

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers l'interface utilisateur locale et les connexions à partir de Cloud Data SENSE
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement du connecteur.

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur 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 le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles 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 le connecteur.



L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers AWS et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	ONTAP HA médiateur	Communication avec le médiateur ONTAP HA
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP
Sens des données cloud	HTTP	80	Instance Cloud Data Sense	Des solutions clouds adaptées à Cloud Volumes ONTAP

Configuration du système AWS KMS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, vous devez configurer le service AWS Key Management Service (KMS).

Étapes

1. S'assurer qu'une clé principale client (CMK) active existe.

La CMK peut être une CMK gérée par AWS ou une CMK gérée par le client. Il peut se trouver dans le même compte AWS que BlueXP et Cloud Volumes ONTAP ou dans un autre compte AWS.

["Documentation AWS : clés principales client \(CMK\)"](#)

2. Modifiez la stratégie clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations à BlueXP en tant qu'utilisateur *key*.

L'ajout du rôle IAM en tant qu'utilisateur principal donne aux autorisations BlueXP d'utiliser le CMK avec Cloud Volumes ONTAP.

["Documentation AWS : modification des clés"](#)

3. Si le CMK se trouve dans un autre compte AWS, procédez comme suit :
 - a. Accédez à la console KMS à partir du compte où réside la CMK.
 - b. Sélectionnez la touche.
 - c. Dans le volet **Configuration générale**, copiez l'ARN de la clé.

Vous devrez fournir l'ARN à BlueXP lorsque vous créez le système Cloud Volumes ONTAP.

- d. Dans le volet **autres comptes AWS**, ajoutez le compte AWS qui fournit des autorisations BlueXP.

Dans la plupart des cas, c'est le compte où réside BlueXP. Si BlueXP n'était pas installé dans AWS, ce serait le compte pour lequel vous avez fourni les clés d'accès AWS à BlueXP.



Other AWS accounts

×

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam::

:

root

Remove

Add another AWS account

Cancel

Save changes

- e. Passez maintenant au compte AWS qui fournit des autorisations BlueXP et ouvrez la console IAM.
- f. Créez une stratégie IAM qui inclut les autorisations répertoriées ci-dessous.
- g. Associez la politique au rôle IAM ou à l'utilisateur IAM qui fournit des autorisations à BlueXP.

La stratégie suivante fournit les autorisations dont BlueXP a besoin pour utiliser CMK à partir du compte AWS externe. Veillez à modifier la région et l'ID de compte dans les sections « ressource ».

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

Pour plus d'informations sur ce processus, reportez-vous à la section ["Documentation AWS : possibilité pour les utilisateurs d'autres comptes d'utiliser une clé KMS"](#).

4. Si vous utilisez un CMK géré par le client, modifiez la stratégie clé pour le CMK en ajoutant le rôle IAM Cloud Volumes ONTAP en tant qu'utilisateur `key`.

Cette étape est nécessaire si le Tiering des données sur Cloud Volumes ONTAP est activé et que vous souhaitez chiffrer les données stockées dans le compartiment S3.

Vous devrez effectuer cette étape *After* déployer Cloud Volumes ONTAP car le rôle IAM est créé lorsque vous créez un environnement de travail. (Bien sûr, vous avez la possibilité d'utiliser un rôle IAM Cloud Volumes ONTAP existant afin d'effectuer cette étape auparavant.)

["Documentation AWS : modification des clés"](#)

Configurer les rôles IAM pour Cloud Volumes ONTAP

Les rôles IAM avec les autorisations requises doivent être associés à chaque nœud Cloud Volumes ONTAP. Il en va de même pour le médiateur HA. Il est plus facile de laisser BlueXP créer les rôles IAM pour vous, mais vous pouvez utiliser vos propres rôles.

Cette tâche est facultative. Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, l'option par défaut est de laisser BlueXP créer les rôles IAM pour vous. Si les politiques de sécurité de votre entreprise exigent que vous créiez vous-même les rôles IAM, suivez les étapes ci-dessous.



La fourniture de votre propre rôle IAM est requise dans l'environnement des services cloud AWS commerciaux. ["Découvrez comment déployer Cloud Volumes ONTAP dans C2S"](#).

Étapes

1. Accédez à la console IAM AWS.
2. Créez des règles IAM qui incluent les autorisations suivantes :
 - Règle de base pour les nœuds Cloud Volumes ONTAP

Régions standard

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

GovCloud (USA)

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-us-gov:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

Environnement C2S

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

- Règle de sauvegarde pour les nœuds Cloud Volumes ONTAP

Si vous prévoyez d'utiliser Cloud Backup avec vos systèmes Cloud Volumes ONTAP, le rôle IAM pour les nœuds doit inclure la seconde règle indiquée ci-dessous.

Régions standard

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}
```

GovCloud (USA)

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

Environnement C2S

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}

```

- Ha médiateur

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}

```

3. Créez un rôle IAM et associez les règles que vous avez créées au rôle.

Résultat

Vous disposez désormais de rôles IAM que vous pouvez sélectionner lorsque vous créez un nouvel environnement de travail Cloud Volumes ONTAP.

Plus d'informations

- ["Documentation AWS : création de règles IAM"](#)
- ["Documentation AWS : création des rôles IAM"](#)

Configuration des licences pour Cloud Volumes ONTAP dans AWS

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 sur AWS 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](#)".

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ **Pay-Per-TiB - Annual Contract**
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ **Pay-as-you-go**
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

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

Select Charging Method

☐ Professional

By capacity

▼

☐ Essential

By capacity

▼

☒ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans AWS".

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 d'AWS Marketplace
- Un contrat annuel sur AWS Marketplace

["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. En l'absence d'erreurs, BlueXP ajoute automatiquement les licences au porte-monnaie numérique.

Votre licence doit être disponible auprès du porte-monnaie numérique avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez ["Ajoutez manuellement la licence au porte-monnaie numérique"](#).

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 sur AWS 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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ Pay-Per-TiB - Annual Contract

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ Pay-as-you-go

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

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

Select Charging Method



Professional

By capacity



Essential

By capacity



Freemium (Up to 500 GiB)

By capacity



Per Node

By node



"Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans AWS".

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 AWS 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 sur AWS Marketplace.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ **Pay-Per-TiB - Annual Contract**
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ **Pay-as-you-go**
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

- 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

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans AWS".



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

Contrat annuel

Payez annuellement en achetant un contrat annuel sur le marché de votre fournisseur cloud.

À l'instar d'un abonnement horaire, BlueXP vous invite à vous abonner au contrat annuel disponible sur AWS Marketplace.

Étapes

1. 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 contrat annuel sur AWS Marketplace.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☒ **Pay-Per-TiB - Annual Contract**

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☐ **Pay-as-you-go**

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

- 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

☒ **Professional**

By capacity



☐ **Essential**

By capacity



☐ **Freemium (Up to 500 GiB)**

By capacity



☐ **Per Node**

By node



"Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans AWS".

Abonnement Keystone Flex

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

Étapes

1. Si vous n'avez pas encore d'abonnement, "[Contactez NetApp](#)"
2. Mailto:ng-keystone-success@netapp.com[contacter NetApp] pour autoriser votre compte utilisateur BlueXP avec un ou plusieurs abonnements Keystone Flex.
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 Flex lorsque vous êtes invité à choisir une méthode de charge.

The screenshot displays the 'Select Charging Method' window. It features a list of subscription options. The 'Keystone' option is selected, indicated by a blue checkmark. Below it, details for the Keystone subscription are shown: 'Storage management', 'Charged against your NetApp credit', and a 'Keystone Subscription' dropdown menu currently set to 'A-AMRITA1'. Other options include 'Professional', 'Essential', and 'Freemium (Up to 500 GiB)', all with 'By capacity' billing. The 'Per Node' option is at the bottom with 'By node' billing.

Charging Method	Billing Method
<input checked="" type="radio"/> Keystone Storage management Charged against your NetApp credit Keystone Subscription: A-AMRITA1	By capacity
<input 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 AWS](#)".

Lancement d'Cloud Volumes ONTAP dans AWS

Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à système unique ou en tant que paire haute disponibilité dans AWS.

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"](#).
- Compréhension de la configuration que vous voulez utiliser.

Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès 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"](#).

- DNS et Active Directory pour les configurations CIFS.

Pour plus de détails, voir ["Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"](#).

Lancement d'un système Cloud Volumes ONTAP à un seul nœud dans AWS

Si vous voulez lancer Cloud Volumes ONTAP dans AWS, vous devez créer un nouvel environnement de travail dans BlueXP

Description de la tâche

Immédiatement après avoir créé l'environnement de travail, BlueXP lance une instance de test dans le VPC spécifié pour vérifier la connectivité. S'il réussit, BlueXP met immédiatement fin à l'instance et démarre le déploiement du système Cloud Volumes ONTAP. Si BlueXP ne peut pas vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

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 **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
4. Si vous y êtes invité, ["Créer un connecteur"](#).
5. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

Certains champs de cette page sont explicites. 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 Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. BlueXP ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation AWS : balisage des ressources Amazon EC2 ".
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 les informations d'identification	Sélectionnez les identifiants AWS associés au compte sur lequel vous souhaitez déployer le système. Vous pouvez également associer l'abonnement AWS Marketplace à ce système Cloud Volumes ONTAP. Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un nouvel abonnement AWS Marketplace. L'abonnement peut s'agir d'un contrat annuel ou d'un paiement pour Cloud Volumes ONTAP à l'heure. https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html ["Découvrez comment ajouter des identifiants AWS à BlueXP"^].

Découvrez dans cette vidéo comment associer un abonnement payant basé sur l'utilisation Marketplace à vos identifiants AWS :

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4


(video)

Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS *account*, chaque utilisateur IAM doit s'associer à cet abonnement. Si vous voyez le message ci-dessous, cliquez sur le lien **cliquez ici** pour accéder au site Web de BlueXP et terminer le processus.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

**Having issues signing up for your product?**
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)
You are already subscribed to this product

Pricing Details

Software Fees

6. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.

- ["Pour en savoir plus sur Cloud Data Sense"](#)
- ["En savoir plus sur Cloud Backup"](#)

7. **Localisation et connectivité** : saisissez les informations de réseau que vous avez enregistrées dans le ["Fiche AWS"](#).

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

Champ	Description
VPC	Si vous disposez d'un poste externe AWS, vous pouvez déployer un système Cloud Volumes ONTAP à un seul nœud dans cet envoi en sélectionnant le VPC Outpost. L'expérience est la même que tout autre VPC qui réside dans AWS.
Groupe de sécurité généré	Si vous laissez BlueXP générer le groupe de sécurité pour vous, vous devez choisir comment vous autorisez le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, la source du trafic entrant correspond à la plage de sous-réseau du VPC sélectionné et à la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VPC, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser un groupe de sécurité 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. **Data Encryption** : choisissez pas de cryptage de données ou de cryptage géré par AWS.

Pour le chiffrement géré par AWS, vous pouvez choisir une autre clé maître client (CMK) dans votre

compte ou un autre compte AWS.



Une fois que vous avez créé un système Cloud Volumes ONTAP, vous ne pouvez pas modifier la méthode de chiffrement des données AWS.

["Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".](#)

["En savoir plus sur les technologies de cryptage prises en charge".](#)

9. **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".](#)

10. **Configuration Cloud Volumes ONTAP** (contrat AWS Marketplace annuel uniquement) : consultez la configuration par défaut et cliquez sur **Continuer** ou sur **Modifier la configuration** pour sélectionner votre propre configuration.

Si vous conservez la configuration par défaut, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.

11. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement Cloud Volumes ONTAP ou cliquez sur **Modifier la configuration** pour sélectionner votre propre configuration.

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

12. **IAM role**: Il est préférable de conserver l'option par défaut pour permettre à BlueXP de créer le rôle pour vous.

Si vous préférez utiliser votre propre police, elle doit satisfaire ["Configuration requise pour les nœuds Cloud Volumes ONTAP"](#).

13. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins et sélectionnez un type d'instance et la location d'instance.



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.

14. **Ressources de stockage sous-jacentes** : Choisissez un type de disque, configurez le stockage sous-jacent et choisissez si le Tiering des données doit être activé.

Notez ce qui suit :

- Le type de disque est pour le volume initial (et l'agrégat). Vous pouvez choisir un autre type de disque pour les volumes suivants (et les agrégats).
- Si vous choisissez un disque gp3 ou io1, BlueXP utilise la fonctionnalité Elastic volumes d'AWS pour augmenter automatiquement la capacité des disques de stockage sous-jacents selon les besoins. Après le déploiement de Cloud Volumes ONTAP, vous pouvez choisir la capacité initiale en fonction de vos besoins en stockage, puis la réviser. ["En savoir plus sur la prise en charge d'Elastic volumes dans"](#)

[AWS](#)".

- Si vous choisissez un disque gp2 ou st1, vous pouvez sélectionner une taille de disque pour tous les disques de l'agrégat initial et pour 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.
- 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.

["Découvrez le fonctionnement du Tiering des données"](#).

15. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

["En savoir plus sur la vitesse d'écriture"](#).

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

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

16. **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.

Champ	Description
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. 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). 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" .

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

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
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.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs,ou=corp dans ce champ.
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.

18. **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 "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

19. **Revue et approbation** : consultez et confirmez vos choix.
- Consultez les détails de la configuration.
 - Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que BlueXP achètera.
 - Cochez les cases **Je comprends....**
 - Cliquez sur **Go**.

Résultat

BlueXP lance l'instance Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du lancement de l'instance Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur Re-create environment.

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 Cloud Volumes ONTAP HA dans AWS

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans AWS, vous devez créer un environnement de travail haute disponibilité dans BlueXP.

Restriction

À l'heure actuelle, les paires haute disponibilité ne sont pas prises en charge avec les posts d'AWS.

Description de la tâche

Immédiatement après avoir créé l'environnement de travail, BlueXP lance une instance de test dans le VPC spécifié pour vérifier la connectivité. S'il réussit, BlueXP met immédiatement fin à l'instance et démarre le déploiement du système Cloud Volumes ONTAP. Si BlueXP ne peut pas vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

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 **Amazon Web Services** et **Cloud Volumes ONTAP HA**.
4. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

Certains champs de cette page sont explicites. 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 Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. BlueXP ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation AWS : balisage des ressources Amazon EC2 ".
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 les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un nouvel abonnement AWS Marketplace. L'abonnement peut s'agir d'un contrat annuel ou d'un paiement pour Cloud Volumes ONTAP à l'heure. Si vous achetez une licence directement auprès de NetApp (BYOL), un abonnement AWS n'est pas requis. https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html ["Découvrez comment ajouter des identifiants AWS à BlueXP"].

Découvrez dans cette vidéo comment associer un abonnement payant basé sur l'utilisation Marketplace à

vos identifiants AWS :

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4

(video)



Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS *account*, chaque utilisateur IAM doit s'associer à cet abonnement. Si vous voyez le message ci-dessous, cliquez sur le lien **cliquez ici** pour accéder au site Web de BlueXP et terminer le processus.

Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

5. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec ce système Cloud Volumes ONTAP.

- ["Pour en savoir plus sur Cloud Data Sense"](#)
- ["En savoir plus sur Cloud Backup"](#)

6. **Modèles de déploiement haute disponibilité** : choisir une configuration haute disponibilité.

Pour obtenir un aperçu des modèles de déploiement, voir ["Cloud Volumes ONTAP HA pour AWS"](#).

7. **Localisation et connectivité** (AZ simple) ou **région et VPC** (AZS multiples) : saisissez les informations de réseau que vous avez enregistrées dans la fiche de travail AWS.

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

Champ	Description
Groupe de sécurité généré	Si vous laissez BlueXP générer le groupe de sécurité pour vous, vous devez choisir comment vous autorisez le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, la source du trafic entrant correspond à la plage de sous-réseau du VPC sélectionné et à la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VPC, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser un groupe de sécurité 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. **Connectivité et authentification SSH** : choisissez des méthodes de connexion pour la paire HA et le médiateur.

9. **IP flottantes** : si vous choisissez plusieurs adresses AZS, spécifiez les adresses IP flottantes.

Les adresses IP doivent se trouver en dehors du bloc CIDR pour tous les VPC de la région. Pour plus de détails, voir ["Configuration réseau AWS requise pour Cloud Volumes ONTAP HA dans plusieurs AZS"](#).

10. **Tables de routage** : si vous choisissez plusieurs AZS, sélectionnez les tables de routage qui doivent inclure les routes vers les adresses IP flottantes.

Si vous disposez de plusieurs tables de routage, il est très important de sélectionner les tables de routage correctes. Dans le cas contraire, certains clients n'ont peut-être pas accès à la paire Cloud Volumes ONTAP HA. Pour plus d'informations sur les tables de routage, voir ["Documentation AWS : tables de routage"](#).

11. **Data Encryption** : choisissez pas de cryptage de données ou de cryptage géré par AWS.

Pour le chiffrement géré par AWS, vous pouvez choisir une autre clé maître client (CMK) dans votre compte ou un autre compte AWS.



Une fois que vous avez créé un système Cloud Volumes ONTAP, vous ne pouvez pas modifier la méthode de chiffrement des données AWS.

["Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP"](#).

["En savoir plus sur les technologies de cryptage prises en charge"](#).

12. **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"](#).

13. **Configuration Cloud Volumes ONTAP** (contrat AWS Marketplace annuel uniquement) : consultez la configuration par défaut et cliquez sur **Continuer** ou sur **Modifier la configuration** pour sélectionner votre propre configuration.

Si vous conservez la configuration par défaut, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.

14. **Packages préconfigurés** (horaire ou BYOL uniquement) : sélectionnez un des packages pour lancer rapidement Cloud Volumes ONTAP, ou cliquez sur **Modifier la configuration** pour sélectionner votre propre configuration.

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

15. **IAM role**: Il est préférable de conserver l'option par défaut pour permettre à BlueXP de créer le rôle pour vous.

Si vous préférez utiliser votre propre police, elle doit satisfaire ["Configuration requise pour les nœuds Cloud Volumes ONTAP et le médiateur HA"](#).

16. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins et sélectionnez un type d'instance et la location d'instance.



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.

17. **Ressources de stockage sous-jacentes** : Choisissez un type de disque, configurez le stockage sous-jacent et choisissez si le Tiering des données doit être activé.

Notez ce qui suit :

- Le type de disque est pour le volume initial (et l'agrégat). Vous pouvez choisir un autre type de disque pour les volumes suivants (et les agrégats).
- Si vous choisissez un disque gp3 ou io1, BlueXP utilise la fonctionnalité Elastic volumes d'AWS pour augmenter automatiquement la capacité des disques de stockage sous-jacents selon les besoins. Après le déploiement de Cloud Volumes ONTAP, vous pouvez choisir la capacité initiale en fonction de vos besoins en stockage, puis la réviser. ["En savoir plus sur la prise en charge d'Elastic volumes dans AWS"](#).
- Si vous choisissez un disque gp2 ou st1, vous pouvez sélectionner une taille de disque pour tous les disques de l'agrégat initial et pour 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.
- 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.

["Découvrez le fonctionnement du Tiering des données"](#).

18. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

["En savoir plus sur la vitesse d'écriture"](#).

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

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

19. **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.

Champ	Description
Autorisations et utilisateurs/groupe (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur 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)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. 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 bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). 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" .

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

20. **Configuration CIFS** : si vous avez sélectionné le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
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	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs,ou=corp dans ce champ.
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.

21. **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 ["Présentation des profils d'utilisation des volumes"](#) et ["Vue d'ensemble du hiérarchisation des données"](#).

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

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

Résultat

BlueXP lance la paire haute disponibilité Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du lancement de la paire HA, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur Re-create environment.

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.

Commencez à utiliser Cloud Volumes ONTAP dans l'environnement AWS C2S

À l'instar d'une région AWS standard, vous pouvez utiliser Cloud Manager dans le "[AWS commercial Cloud Services \(C2S\)](#)" Environnement à déployer Cloud Volumes ONTAP, qui fournit des fonctionnalités de grande qualité pour votre stockage cloud. AWS C2S est une région fermée spécifique aux États-Unis Intelligence Community : les instructions de cette page s'appliquent uniquement aux utilisateurs de la région AWS C2S.

Versions prises en charge dans C2S

- Cloud Volumes ONTAP 9.8 est pris en charge
- La version 3.9.4 du connecteur est prise en charge

Il s'agit du logiciel requis pour déployer et gérer Cloud Volumes ONTAP dans AWS. Vous allez vous connecter à Cloud Manager à partir du logiciel installé sur l'instance de connecteur. Le site Web SaaS pour Cloud Manager n'est pas pris en charge dans l'environnement C2S.



Cloud Manager a été récemment renommé BlueXP, mais nous continuons à le qualifier de Cloud Manager dans C2S, car l'interface utilisateur incluse dans la version 3.9.4 du connecteur est toujours appelée Cloud Manager.

Fonctions prises en charge dans C2S

Cloud Manager inclut les fonctionnalités suivantes dans l'environnement C2S :

- Cloud Volumes ONTAP
- Réplication des données
- Un calendrier pour l'audit

Pour Cloud Volumes ONTAP, vous pouvez créer un système à un seul nœud ou une paire HA. Ces deux options de licence sont disponibles : paiement à l'utilisation et BYOL (Bring Your Own License).

Le Tiering des données vers S3 est également pris en charge par Cloud Volumes ONTAP dans C2S.

Limites

- Aucun des services cloud de NetApp n'est disponible dans Cloud Manager.
- Comme il n'y a pas d'accès à Internet dans l'environnement C2S, les fonctions suivantes ne sont pas disponibles :
 - Mises à niveau logicielles automatisées depuis Cloud Manager

- NetApp AutoSupport
- Informations sur les coûts AWS pour les ressources Cloud Volumes ONTAP
- Les licences Freemium ne sont pas prises en charge dans l'environnement C2S.

Présentation du déploiement

La mise en route de Cloud Volumes ONTAP dans C2S comprend quelques étapes.

1. Préparation de votre environnement AWS

Vous pouvez notamment configurer la mise en réseau, vous abonner à Cloud Volumes ONTAP, configurer des autorisations et éventuellement configurer le KMS AWS.

2. Installation du connecteur et configuration de Cloud Manager

Avant de pouvoir commencer à utiliser Cloud Manager pour déployer Cloud Volumes ONTAP, vous devez créer un *Connector*. Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public (y compris Cloud Volumes ONTAP).

Vous allez vous connecter à Cloud Manager à partir du logiciel installé sur l'instance de connecteur.

3. Lancement de Cloud Volumes ONTAP à partir de Cloud Manager

Chacune de ces étapes est décrite ci-dessous.

Préparation de votre environnement AWS

Votre environnement AWS doit répondre à quelques exigences.

Configurez votre réseau

Configurez votre réseau AWS pour que Cloud Volumes ONTAP puisse fonctionner correctement.

Étapes

1. Choisissez le VPC et les sous-réseaux dans lesquels vous souhaitez lancer l'instance de connecteur et les instances Cloud Volumes ONTAP.
2. Vérifiez que votre VPC et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
3. Configurez un terminal VPC sur le service S3.

Un point de terminaison VPC est requis si vous souhaitez transférer des données à froid de Cloud Volumes ONTAP vers un stockage objet économique.

Abonnez-vous à Cloud Volumes ONTAP

Un abonnement Marketplace est nécessaire pour déployer Cloud Volumes ONTAP depuis Cloud Manager.

Étapes

1. Accédez au Marketplace de la communauté AWS Intelligence et recherchez Cloud Volumes ONTAP.
2. Sélectionnez l'offre que vous prévoyez de déployer.
3. Vérifiez les termes et cliquez sur **Accept**.

4. Répétez ces étapes pour les autres offres si vous prévoyez de les déployer.

Vous devez utiliser Cloud Manager pour lancer les instances Cloud Volumes ONTAP. Vous ne devez pas lancer des instances Cloud Volumes ONTAP à partir de la console EC2.

Configurez les autorisations

Définissez des règles et des rôles IAM qui fournissent au connecteur et à Cloud Volumes ONTAP les autorisations nécessaires pour effectuer des actions dans l'environnement des services cloud AWS commerciaux.

Vous avez besoin d'une politique IAM et d'un rôle IAM pour chacun des éléments suivants :

- L'instance de connecteur
- Instances Cloud Volumes ONTAP
- L'instance de médiateur Cloud Volumes ONTAP HA (si vous souhaitez déployer des paires HA)

Étapes

1. Accédez à la console IAM AWS et cliquez sur **Policies**.
2. Créez une stratégie pour l'instance de connecteur.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",

```

```

        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2>DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",

```

```

        "Action": [
            "s3:DeleteBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions"
        ],
        "Resource": [
            "arn:aws-iso:s3:::fabric-pool*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso:ec2:*:*:volume/*"
        ]
    }
]
}

```

3. Création d'une policy pour Cloud Volumes ONTAP.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

4. Si vous prévoyez de déployer une paire Cloud Volumes ONTAP HA, créez une règle pour le médiateur haute disponibilité.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}

```

5. Créez des rôles IAM avec le type de rôle Amazon EC2 et associez les règles créées aux étapes précédentes.

De la même manière que les règles, vous devez avoir un rôle IAM pour le connecteur, un pour les nœuds Cloud Volumes ONTAP et un pour le médiateur HA (si vous souhaitez déployer des paires HA).

Vous devez sélectionner le rôle IAM de connecteur lorsque vous lancez l'instance de connecteur.

Vous pouvez sélectionner les rôles IAM pour Cloud Volumes ONTAP et le médiateur HA lorsque vous créez un environnement de travail Cloud Volumes ONTAP à partir de Cloud Manager.

Configuration du KMS AWS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, assurez-vous que les exigences du service de gestion des clés AWS sont respectées.

Étapes

1. Assurez-vous qu'une clé maître client (CMK) active existe dans votre compte ou dans un autre compte AWS.

La CMK peut être une CMK gérée par AWS ou une CMK gérée par le client.

2. Si le CMK se trouve dans un compte AWS séparé du compte sur lequel vous prévoyez de déployer Cloud Volumes ONTAP, vous devez obtenir l'ARN de cette clé.

Vous devrez fournir l'ARN dans Cloud Manager lors de la création du système Cloud Volumes ONTAP.

3. Ajoutez le rôle IAM de l'instance de connecteur à la liste des utilisateurs clés d'un CMK.

Cela permet à Cloud Manager d'utiliser le CMK avec Cloud Volumes ONTAP.

Installation du connecteur et configuration de Cloud Manager

Avant de lancer des systèmes Cloud Volumes ONTAP dans AWS, vous devez d'abord lancer l'instance de connecteur à partir d'AWS Marketplace, puis vous connecter et configurer Cloud Manager.

Étapes

1. Obtenir un certificat racine signé par une autorité de certification (CA) au format X.509 encodé base-64 de Privacy Enhanced Mail (PEM). Consultez les politiques et procédures de votre organisation pour obtenir le certificat.

Vous devrez télécharger le certificat pendant le processus d'installation. Cloud Manager utilise le certificat de confiance pour l'envoi de demandes vers AWS sur HTTPS.

2. Lancez l'instance de connecteur :
 - a. Accédez à la page AWS Intelligence Community Marketplace pour Cloud Manager.
 - b. Dans l'onglet Custom Launch, sélectionnez l'option de lancement de l'instance à partir de la console EC2.
 - c. Suivez les invites pour configurer l'instance.

Notez les éléments suivants lors de la configuration de l'instance :

- Nous recommandons une instance t3.XLarge.
- Vous devez choisir le rôle IAM que vous avez créé lors de la préparation de votre environnement AWS.
- Vous devez conserver les options de stockage par défaut.
- Les méthodes de connexion requises pour le connecteur sont les suivantes : SSH, HTTP et HTTPS.

3. Configurez Cloud Manager à partir d'un hôte connecté à l'instance de connecteur :
 - a. Ouvrez un navigateur Web et entrez l'URL suivante : <http://ipaddress>
 - b. Spécifiez un serveur proxy pour la connectivité aux services AWS.
 - c. Téléchargez le certificat que vous avez obtenu à l'étape 1.
 - d. Suivez les étapes de l'assistant d'installation pour configurer Cloud Manager.
 - **Détails du système** : saisissez un nom pour cette instance de Cloud Manager et indiquez le nom de votre entreprise.
 - **Créer un utilisateur** : créez l'utilisateur Admin que vous utiliserez pour administrer Cloud Manager.
 - **Revue** : passez en revue les détails et approuvez le contrat de licence de l'utilisateur final.
 - e. Pour terminer l'installation du certificat signé par l'autorité de certification, redémarrez l'instance de connecteur à partir de la console EC2.
4. Une fois le connecteur redémarré, connectez-vous à l'aide du compte utilisateur administrateur que vous avez créé dans l'assistant de configuration.

Lancement de Cloud Volumes ONTAP à partir de Cloud Manager

Vous pouvez lancer des instances Cloud Volumes ONTAP dans l'environnement AWS commercial Cloud Services en créant de nouveaux environnements de travail dans Cloud Manager.

Ce dont vous avez besoin

- Si vous avez acheté une licence, vous devez disposer du fichier de licence que vous avez reçu de NetApp. Le fichier de licence est un fichier .NLF au format JSON.
- Une paire de clés est requise pour activer l'authentification SSH basée sur des clés au médiateur HA.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sous Créer, sélectionnez Cloud Volumes ONTAP ou Cloud Volumes ONTAP HA.
3. Suivez les étapes de l'assistant pour lancer le système Cloud Volumes ONTAP.

Notez les éléments suivants lorsque vous terminez l'assistant :

- Si vous souhaitez déployer Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité, déployez la configuration comme suit, car seuls deux AZS étaient disponibles dans l'environnement AWS commercial Cloud Services au moment de la publication :
 - Nœud 1 : zone de disponibilité A
 - Nœud 2 : zone de disponibilité B
 - Médiateur : zone de disponibilité A ou B
- Vous devez laisser l'option par défaut pour utiliser un groupe de sécurité généré.

Le groupe de sécurité prédéfini comprend les règles dont Cloud Volumes ONTAP a besoin pour fonctionner correctement. Si vous avez besoin d'utiliser votre propre, vous pouvez vous reporter à la section du groupe de sécurité ci-dessous.

- Vous devez choisir le rôle IAM que vous avez créé lors de la préparation de votre environnement AWS.
- Le type de disque AWS sous-jacent concerne le volume Cloud Volumes ONTAP initial.

Vous pouvez choisir un autre type de disque pour les volumes suivants.

- Les performances des disques AWS sont liées à leur taille.

Choisissez la taille qui offre les performances dont vous avez besoin. Pour plus d'informations sur les performances d'EBS, consultez la documentation AWS.

- La taille du disque est la taille par défaut de tous les disques du système.



Si vous avez besoin d'une taille différente par la suite, vous pouvez utiliser l'option d'allocation avancée pour créer un agrégat qui utilise des disques d'une taille spécifique.

- Les fonctionnalités d'efficacité du stockage améliorent l'utilisation du stockage et réduisent la quantité totale de stockage nécessaire.

Résultat

Cloud Manager lance l'instance Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Règles de groupe de sécurité

Cloud Manager crée des groupes de sécurité comprenant les règles entrantes et sortantes que Cloud Manager et Cloud Volumes ONTAP doivent fonctionner avec succès dans le cloud. Vous pouvez consulter les ports à des fins de test ou si vous préférez utiliser vos propres groupes de sécurité.

Groupe de sécurité du connecteur

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

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

Groupe de sécurité pour Cloud Volumes ONTAP

Le groupe de sécurité des nœuds Cloud Volumes ONTAP nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Lorsque vous créez un environnement de travail et choisissez un groupe de sécurité prédéfini, vous pouvez choisir d'autoriser le trafic dans l'un des éléments suivants :

- **VPC sélectionné uniquement** : la source du 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** : la source du trafic entrant est la plage IP 0.0.0.0/0.

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	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster

Protocole	Port	Objectif
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
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
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 rquotad

Règles de sortie

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 les protocoles UDP	Tout	Tout le trafic sortant

Groupe de sécurité externe pour le médiateur HA

Le groupe de sécurité externe prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles

entrantes et sortantes suivantes.

Règles entrantes

La source des règles entrantes est le trafic du VPC où réside le connecteur.

Protocole	Port	Objectif
SSH	22	Connexions SSH au médiateur haute disponibilité
TCP	3000	Accès à l'API RESTful depuis le connecteur

Règles de sortie

Le groupe de sécurité prédéfini du médiateur HA inclut les règles de sortie suivantes.

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

Groupe de sécurité interne du médiateur HA

Le groupe de sécurité interne prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles suivantes. Cloud Manager crée toujours ce groupe de sécurité. Vous n'avez pas la possibilité d'utiliser votre propre.

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles de sortie

Le groupe de sécurité prédéfini inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Commencez avec Microsoft Azure

Démarrage rapide de Cloud Volumes ONTAP dans Azure

Découvrez Cloud Volumes ONTAP pour Azure 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 Azure"](#).

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, BlueXP (anciennement Cloud Manager) vous invite à déployer un connecteur si vous n'en avez pas encore.

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 >>"](#).

3

Configurez votre réseau

1. Assurez-vous que votre VNet et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du réseau vnet cible de sorte que le connecteur et Cloud Volumes ONTAP puissent contacter plusieurs noeuds finaux.

Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour ["Le connecteur et le Cloud Volumes ONTAP"](#).

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

4

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"](#)
- ["Création d'un connecteur à partir d'Azure Marketplace"](#)
- ["Installation du logiciel du connecteur sur un hôte Linux"](#)
- ["Ce que BlueXP fait avec les autorisations"](#)

Planification de votre configuration Cloud Volumes ONTAP dans Azure

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, 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 Microsoft Azure. ["Afficher la liste complète des régions prises en charge"](#).

Choisissez un type de machine virtuelle pris en charge

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

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

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 Azure"](#)

Dimensionnez votre système en Azure

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 VM, d'un type de disque et d'une taille de disque :

Type de machine virtuelle

Examinez les types de machines virtuelles prises en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#) Examinez ensuite toutes les informations sur chaque type de machine virtuelle pris en charge. Notez que chaque type de VM prend en charge un nombre spécifique de disques de données.

- ["Documentation Azure : tailles de machine virtuelle à usage général"](#)
- ["Documentation Azure : tailles de machines virtuelles optimisées pour la mémoire"](#)

Type de disque Azure avec des systèmes à un seul nœud

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent utilisé par Cloud Volumes ONTAP comme disque.

Les systèmes à un seul nœud peuvent utiliser trois types de disques gérés Azure :

- *Des disques gérés SSD de premier choix* fournir des performances élevées aux charges de travail exigeantes en E/S à un coût plus élevé.
- *Des disques gérés SSD standard* assurent des performances prévisibles pour les charges de travail nécessitant un faible niveau d'IOPS.
- *Les disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevées et souhaitez réduire vos coûts.

Pour plus d'informations sur les cas d'utilisation de ces disques, reportez-vous à la section ["Documentation Microsoft Azure : quels types de disques sont disponibles dans Azure ?"](#).

Type de disque Azure avec paires haute disponibilité

Les systèmes HAUTE DISPONIBILITÉ utilisent des disques gérés partagés Premium SSD, qui offrent à la fois des performances élevées pour les charges de travail exigeantes en E/S, à un coût plus élevé. Les déploiements HAUTE DISPONIBILITÉ créés avant la version 9.12.1 utilisent des objets blob de pages Premium.

Taille des disques Azure

Lorsque vous lancez des instances Cloud Volumes ONTAP, vous devez choisir la taille de disque par défaut des agrégats. BlueXP utilise cette taille de disque pour l'agrégat initial et pour tous les agrégats supplémentaires qu'il crée lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente de la taille par défaut ["utilisation de l'option d'allocation avancée"](#).



Tous les disques qui composent un agrégat doivent être de la même taille.

Lorsque vous choisissez une taille de disque, vous devez prendre en compte plusieurs facteurs. La taille des disques a une incidence sur le montant de vos frais de stockage, la taille des volumes que vous pouvez créer au sein d'un agrégat, la capacité totale disponible pour Cloud Volumes ONTAP et les performances de stockage.

Les performances du stockage Azure Premium sont liées à la taille des disques. Les disques de grande taille offrent des IOPS et un débit plus élevés. Par exemple, le choix de disques de 1 To peut offrir des performances supérieures à 500 Gio, pour un coût plus élevé.

Avec un stockage standard, les performances sont les mêmes pour toutes les tailles de disques. Choisissez la taille de disque en fonction de la capacité dont vous avez besoin.

Pour les IOPS et le débit par taille de disque, consultez Azure :

- ["Microsoft Azure : tarification des disques gérés"](#)
- ["Microsoft Azure : tarification Blobs de page"](#)

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 Azure"](#).



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 Azure, vous devez spécifier des informations concernant votre réseau virtuel. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Informations sur Azure	Votre valeur
Région	
Réseau virtuel (vnet)	
Sous-réseau	
Groupe de sécurité réseau (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. 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.

Configuration réseau requise pour Cloud Volumes ONTAP dans Azure

Configurez votre réseau Azure de façon à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

Conditions requises pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être satisfaites dans Azure.

Accès Internet sortant

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour l'AutoSupport, qui surveille 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 condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous avez défini des règles sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité 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 BlueXP vous informe que les messages AutoSupport ne peuvent pas être envoyés, ["Résoudre les problèmes de configuration AutoSupport"](#).

Adresses IP

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



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.

Adresses IP d'un système à un seul nœud

BlueXP alloue 5 ou 6 adresses IP à un système à un seul nœud :

- IP de gestion du cluster
- IP de gestion de nœuds
- IP intercluster pour SnapMirror
- NFS/CIFS IP
- IP iSCSI



L'IP iSCSI fournit un accès client via le protocole iSCSI. Il est également utilisé par le système pour d'autres flux de travail réseau importants. Cette LIF est requise et ne doit pas être supprimée.

- Gestion des SVM (facultatif - non configuré par défaut)

Adresses IP des paires haute disponibilité

BlueXP alloue des adresses IP à 4 NIC (par nœud) pendant le déploiement.

Notez que BlueXP crée une LIF de gestion SVM sur des paires haute disponibilité, mais pas sur des systèmes à un seul nœud dans Azure.

NIC0

- IP de gestion de nœuds
- IP intercluster
- IP iSCSI



L'IP iSCSI fournit un accès client via le protocole iSCSI. Il est également utilisé par le système pour d'autres flux de travail réseau importants. Cette LIF est requise et ne doit pas être supprimée.

NIC1

- IP du réseau de cluster

NIC2

- IP d'interconnexion de cluster (ci haute disponibilité)

NIC3

- IP de la carte réseau Pageblob (accès au disque)



NIC3 s'applique uniquement aux déploiements haute disponibilité qui utilisent le stockage d'objets blob de page.

Les adresses IP ci-dessus ne migrent pas lors des événements de basculement.

En outre, 4 adresses IP front-end (FIPS) sont configurées pour migrer lors des événements de basculement. Ces IP frontales résident dans l'équilibreur de charge.

- IP de gestion du cluster
- IP de données NODEA (NFS/CIFS)
- IP de données du nœud B (NFS/CIFS)
- IP de gestion SVM

Connexion sécurisée aux services Azure

Par défaut, BlueXP active une liaison privée Azure pour les connexions entre les comptes de stockage d'objets blob de pages Cloud Volumes ONTAP et Azure.

Dans la plupart des cas, rien n'est nécessaire : BlueXP gère l'Azure Private Link pour vous. Cependant, si vous utilisez Azure Private DNS, vous devez modifier un fichier de configuration. Vous devez également connaître une exigence pour l'emplacement du connecteur dans Azure.

Vous pouvez également désactiver la connexion Private Link, si nécessaire par vos besoins. Si vous

désactivez le lien, BlueXP configure Cloud Volumes ONTAP pour qu'il utilise un point de terminaison de service à la place.

["En savoir plus sur l'utilisation de liens privés Azure ou de terminaux de service avec Cloud Volumes ONTAP".](#)

Connexions à d'autres systèmes ONTAP

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

Pour obtenir des instructions, reportez-vous à la section ["Documentation Microsoft Azure : créez une connexion de site à site dans le portail Azure"](#).

Port pour l'interconnexion haute disponibilité

Une paire Cloud Volumes ONTAP HA inclut une interconnexion haute disponibilité qui permet à chaque nœud de vérifier en permanence si son partenaire fonctionne et de mettre en miroir les données de journal pour la mémoire non volatile de l'autre. L'interconnexion haute disponibilité utilise le port TCP 10006 pour la communication.

Par défaut, la communication entre les LIFs d'interconnexion haute disponibilité est ouverte et il n'existe aucune règle de groupe de sécurité pour ce port. Mais si vous créez un pare-feu entre les LIF d'interconnexion haute disponibilité, vous devez vous assurer que le trafic TCP est ouvert pour le port 10006 afin que la paire haute disponibilité puisse fonctionner correctement.

Une seule paire HA dans un groupe de ressources Azure

Vous devez utiliser un groupe de ressources *dédié* pour chaque paire HA Cloud Volumes ONTAP que vous déployez dans Azure. Une seule paire haute disponibilité est prise en charge dans un groupe de ressources.

BlueXP rencontre des problèmes de connexion si vous essayez de déployer une seconde paire HA Cloud Volumes ONTAP dans un groupe de ressources Azure.

Groupes de sécurité

Vous n'avez pas besoin de créer des groupes de sécurité car BlueXP le fait pour vous. Si vous devez utiliser votre propre système, reportez-vous aux règles du groupe de sécurité répertoriées ci-dessous.

Règles de groupe de sécurité

BlueXP crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes nécessaires au bon fonctionnement de Cloud Volumes ONTAP. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre système utilise ses propres groupes de sécurité.

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes pour les systèmes à nœud unique

Lorsque vous créez un environnement de travail et choisissez un groupe de sécurité prédéfini, vous pouvez choisir d'autoriser le trafic dans l'un des éléments suivants :

- **VNet sélectionné uniquement** : la source du trafic entrant est la plage de sous-réseau du vnet pour le système Cloud Volumes ONTAP et la plage de sous-réseau du vnet où réside le connecteur. Il s'agit de l'option recommandée.

- **Tous les VNets** : la source du trafic entrant est la plage IP 0.0.0.0/0.

Priorité et nom	Port et protocole	Source et destination	Description
1000 inbound_ssh	22 TCP	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
1001 inbound_http	80 TCP	De tous les types à tous	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1002 inbound_111_tcp	111 TCP	De tous les types à tous	Appel de procédure à distance pour NFS
1003 inbound_111_udp	111 UDP	De tous les types à tous	Appel de procédure à distance pour NFS
1004 entrant_139	139 TCP	De tous les types à tous	Session de service NetBIOS pour CIFS
1005 inbound_161-162_tcp	161-162 TCP	De tous les types à tous	Protocole de gestion de réseau simple
1006 inbound_161-162_udp	161-162 UDP	De tous les types à tous	Protocole de gestion de réseau simple
1007 entrant_443	443 TCP	De tous les types à tous	Connectivité avec le connecteur et l'accès HTTPS à la console Web System Manager via l'adresse IP du LIF de cluster management
1008 entrant_445	445 TCP	De tous les types à tous	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
1009 inbound_635_tcp	635 TCP	De tous les types à tous	Montage NFS
1010 inbound_635_udp	635 UDP	De tous les types à tous	Montage NFS
1011 entrant_749	749 TCP	De tous les types à tous	Kerberos
1012 inbound_2049_tcp	2049 TCP	De tous les types à tous	Démon du serveur NFS
1013 inbound_2049_udp	2049 UDP	De tous les types à tous	Démon du serveur NFS
1014 entrant_3260	3260 TCP	De tous les types à tous	Accès iSCSI via le LIF de données iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau
1016 inbound_4045-4046_udp	4045-4046 UDP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau

Priorité et nom	Port et protocole	Source et destination	Description
1017 entrant_10000	10000 TCP	De tous les types à tous	Sauvegarde avec NDMP
1018 entrant_11104-11105	11104-11105 TCP	De tous les types à tous	Transfert de données SnapMirror
3000 inbound_deny_all_tcp	Tout port TCP	De tous les types à tous	Bloquer tout autre trafic TCP entrant
3001 inbound_deny_all_udp	Tout port UDP	De tous les types à tous	Bloquer tout autre trafic entrant UDP
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoadBalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

Règles entrantes pour les systèmes HA

Lorsque vous créez un environnement de travail et choisissez un groupe de sécurité prédéfini, vous pouvez choisir d'autoriser le trafic dans l'un des éléments suivants :

- **VNet sélectionné uniquement** : la source du trafic entrant est la plage de sous-réseau du vnet pour le système Cloud Volumes ONTAP et la plage de sous-réseau du vnet où réside le connecteur. Il s'agit de l'option recommandée.
- **Tous les VNets** : la source du trafic entrant est la plage IP 0.0.0.0/0.



Les systèmes HAUTE DISPONIBILITÉ disposent de règles entrantes moins strictes que les systèmes à un seul nœud, car le trafic des données entrantes transite par Azure Standard Load Balancer. Pour cette raison, le trafic provenant du Load Balancer doit être ouvert, comme indiqué dans la règle AllowAzureLoadBalancerInBound.

Priorité et nom	Port et protocole	Source et destination	Description
100 entrant_443	443 tout protocole	De tous les types à tous	Connectivité avec le connecteur et l'accès HTTPS à la console Web System Manager via l'adresse IP du LIF de cluster management
101 inbound_111_tcp	111 tout protocole	De tous les types à tous	Appel de procédure à distance pour NFS
102 inbound_2049_tcp	2049 tout protocole	De tous les types à tous	Démon du serveur NFS
111 inbound_ssh	22 tout protocole	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud

Priorité et nom	Port et protocole	Source et destination	Description
121 entrant_53	53 tout protocole	De tous les types à tous	DNS et CIFS
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

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.

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

Service	Port	Prot ocol e	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
DHCP	68	UDP	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	67	UDP	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	53	UDP	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	25	TCP	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	161	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	161	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	11104	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	11105	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	514	UDP	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Configuration requise pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le

connecteur, vous devez vous assurer que les exigences suivantes sont respectées.


Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur dans votre réseau d'entreprise, vous devez configurer une connexion VPN au réseau virtuel dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
https://support.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div> Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.blueexp.netapp.com » dans une prochaine version.</div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au "[Interface utilisateur locale](#)", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

Il existe un conflit possible avec des adresses IP dans la plage 172. "[En savoir plus sur cette limitation](#)".

Règles de groupe de sécurité

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Port	Protocole	Objectif
22	SSH	Fournit un accès SSH à l'hôte du connecteur
80	HTTP	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
443	HTTPS	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement du connecteur.

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur 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 le connecteur inclut les règles de trafic sortant suivantes.

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



L'adresse IP source est l'hôte du connecteur.

Service	Port	Protocole	Destination	Objectif
Appels API et AutoSupport	443	HTTPS	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers Azure et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
DNS	53	UDP	DNS	Utilisé pour la résolution DNS par BlueXP

Configuration de Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans Azure

Les données sont automatiquement chiffrées sur Cloud Volumes ONTAP dans Azure à l'aide de "[Chiffrement de service de stockage Azure](#)". Et elle est dotée d'une clé gérée par Microsoft. Mais vous pouvez utiliser votre propre clé de cryptage en suivant les étapes de cette page.

Présentation du chiffrement des données

Les données Cloud Volumes ONTAP sont automatiquement chiffrées dans Azure à l'aide de "[Chiffrement de service de stockage Azure](#)". L'implémentation par défaut utilise une clé gérée par Microsoft. Aucune configuration n'est requise.

Pour utiliser une clé gérée par le client avec Cloud Volumes ONTAP, vous devez effectuer les opérations suivantes :

1. Depuis Azure, créez un coffre-fort de clés, puis générez une clé dans ce coffre-fort
2. Depuis BlueXP, utilisez l'API pour créer un environnement de travail Cloud Volumes ONTAP qui utilise la clé

Rotation des clés

Si vous créez une nouvelle version de votre clé, Cloud Volumes ONTAP utilise automatiquement la dernière version de la clé.

Mode de cryptage des données

Après avoir créé un environnement de travail Cloud Volumes ONTAP configuré pour utiliser une clé gérée par le client, les données Cloud Volumes ONTAP sont chiffrées comme suit.

Zone de disponibilité Azure HA à plusieurs niveaux

- Tous les comptes de stockage Azure pour Cloud Volumes ONTAP sont chiffrés à l'aide d'une clé gérée par le client.¹
- Pour les disques racine, de démarrage, NVRAM, de cœur et de données, BlueXP utilise un ensemble de cryptage de disque, qui permet de gérer les clés de cryptage avec des disques gérés.

- Les nouveaux disques de données utilisent également le même jeu de cryptage de disque.

Zone de disponibilité unique d’Azure HA

- Tous les comptes de stockage Azure pour Cloud Volumes ONTAP sont chiffrés à l’aide d’une clé gérée par le client.¹
- Tous les nouveaux comptes de stockage (par exemple, lorsque vous ajoutez des disques ou des agrégats) utilisent également la même clé.¹
- À partir de ONTAP 9.10.1P3, pour la NVRAM et le disque principal, BlueXP utilise un ["jeu de cryptage de disques"](#), qui permet la gestion des clés de cryptage avec des disques gérés. Les versions inférieures utilisent une clé gérée par Microsoft au lieu de la clé gérée par le client.

Un seul nœud

- Tous les comptes de stockage Azure pour Cloud Volumes ONTAP sont chiffrés à l’aide d’une clé gérée par le client.¹
- Pour les disques racine, de démarrage et de données, BlueXP utilise un ["jeu de cryptage de disques"](#), qui permet la gestion des clés de cryptage avec des disques gérés.
- Les nouveaux disques de données utilisent également le même jeu de cryptage de disque.
- À partir de ONTAP 9.9.1P7, pour la NVRAM et le disque central, BlueXP utilise un ensemble de cryptage de disque qui permet de gérer les clés de cryptage avec des disques gérés. Les versions inférieures utilisent une clé gérée par Microsoft au lieu de la clé gérée par le client.

Note de bas de page

1. Pour chiffrer vos comptes de stockage pendant leur création, vous devez créer et fournir l’ID de la ressource dans la demande de création CVO. Cela s’applique à tous les types de déploiements. Si vous ne le fournissez pas, les comptes de stockage seront toujours cryptés, mais BlueXP créera d’abord les comptes de stockage avec cryptage de clé géré par Microsoft, puis mettra à jour les comptes de stockage pour utiliser la clé gérée par le client.

Créez un coffre-fort de clés et générez une clé

Le coffre-fort de clés doit résider dans la même région et l’abonnement Azure dans laquelle vous prévoyez de créer le système Cloud Volumes ONTAP.

Étapes

1. ["Créez un coffre-fort de clés dans votre abonnement Azure"](#).

Notez les exigences suivantes pour le coffre-fort de clés :

- Le coffre-fort de clés doit résider dans la même région que le système Cloud Volumes ONTAP.
- Les options suivantes doivent être activées :
 - **Soft-delete** (cette option est activée par défaut, mais doit *not* être désactivée)
 - **Protection de purge**
 - **Chiffrement de disque Azure pour chiffrement de volume** (pour les systèmes à un seul nœud ou les paires HA dans plusieurs zones)

2. ["Générez une clé dans le coffre-fort de clés"](#).

Notez les exigences suivantes pour la clé :

- Le type de clé doit être **RSA**.

- La taille de clé RSA recommandée est **2048**, mais d'autres tailles sont prises en charge.

Créez un environnement de travail qui utilise la clé de cryptage

Après avoir créé le coffre-fort de clés et généré une clé de cryptage, vous pouvez créer un nouveau système Cloud Volumes ONTAP configuré pour utiliser la clé. Ces étapes sont prises en charge à l'aide de l'API BlueXP.

Autorisations requises

Si vous souhaitez utiliser une clé gérée par le client avec un système Cloud Volumes ONTAP à un seul nœud, assurez-vous que le connecteur BlueXP dispose des autorisations suivantes :

```
"Microsoft.Compute/diskEncryptionSets/read"  
"Microsoft.Compute/diskEncryptionSets/write",  
"Microsoft.Compute/diskEncryptionSets/delete"  
"Microsoft.KeyVault/vaults/deploy/action",  
"Microsoft.KeyVault/vaults/read",  
"Microsoft.KeyVault/vaults/accessPolicies/write"  
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Affichez la liste des autorisations les plus récentes"



Les autorisations ne sont pas nécessaires pour les paires haute disponibilité dans une seule zone.

Étapes

1. Obtenez la liste des coffres-forts de clés dans votre abonnement Azure en utilisant l'appel d'API BlueXP suivant.

Pour une paire haute disponibilité : `GET /azure/ha/metadata/vaults`

Pour un seul nœud : `GET /azure/vsa/metadata/vaults`

Notez les **name** et **ResourceGroup**. Vous devrez spécifier ces valeurs à l'étape suivante.

["En savoir plus sur cet appel d'API"](#).

2. Obtenez la liste des clés dans le coffre-fort à l'aide de l'appel d'API BlueXP suivant.

Pour une paire haute disponibilité : `GET /azure/ha/metadata/keys-vault`

Pour un seul nœud : `GET /azure/vsa/metadata/keys-vault`

Notez le **keyName**. Vous devrez spécifier cette valeur (avec le nom du coffre-fort) à l'étape suivante.

["En savoir plus sur cet appel d'API"](#).

3. Créez un système Cloud Volumes ONTAP à l'aide de l'appel d'API BlueXP suivant.

- a. Pour une paire haute disponibilité :

POST /azure/ha/working-environments

Le corps de la demande doit inclure les champs suivants :

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName",  
  "userAssignedIdentity": " userAssignedIdentityId",  
  [Optional] ***  
}
```

["En savoir plus sur cet appel d'API".](#)

b. Pour un système à un seul nœud :

POST /azure/vsa/working-environments

Le corps de la demande doit inclure les champs suivants :

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName",  
  "userAssignedIdentity": " userAssignedIdentityId",  
  [Optional] ***  
}
```

+

["En savoir plus sur cet appel d'API".](#)

Résultat

Un nouveau système Cloud Volumes ONTAP est configuré pour utiliser la clé gérée par le client pour le chiffrement des données.

Configuration des licences pour Cloud Volumes ONTAP dans Azure

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 Azure 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](#)".

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

Select Charging Method

☐ Professional By capacity ▼

☐ Essential By capacity ▼

☒ Freemium (Up to 500 GiB) By capacity ▼

☐ Per Node By node ▼

"Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Azure".

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 d'Azure 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. En l'absence d'erreurs, BlueXP ajoute automatiquement les licences au porte-monnaie numérique.

Votre licence doit être disponible auprès du porte-monnaie numérique avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez ["Ajoutez manuellement la licence au porte-monnaie numérique"](#).

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 Azure 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.

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. 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 Azure".

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 Azure 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 Azure Marketplace.

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity ▼

Azure Subscription

OCCM Dev (Default) ▼

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- 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 Azure".](#)



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

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 Azure Marketplace.

Une fois que NetApp vous a fait part de son offre privée, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à Azure Marketplace lors de la création d'un 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 > Continuer**.
 - b. Dans le portail Azure, sélectionnez le plan annuel partagé avec votre compte Azure, puis cliquez sur **Subscribe**.
 - 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

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

Abonnement Keystone Flex

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

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)[contacter NetApp] pour autoriser votre compte utilisateur BlueXP avec un ou plusieurs abonnements Keystone Flex.
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 Flex lorsque vous êtes invité à choisir une méthode de charge.

Un utilisateur Azure disposant de privilèges « propriétaire » peut activer cette fonctionnalité à partir de l'interface de ligne de commande Azure.

Étapes

1. ["Accédez au shell cloud Azure depuis le portail Azure"](#)
2. Enregistrez la fonction de mode haute disponibilité :

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Vous pouvez également vérifier que la fonction est maintenant enregistrée :

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Le résultat de l'interface de ligne de commandes Azure doit être similaire à ce qui suit :

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Lancement d'Cloud Volumes ONTAP dans Azure

Vous pouvez lancer un système à un seul nœud ou une paire haute disponibilité dans Azure en créant un environnement de travail Cloud Volumes ONTAP dans BlueXP.

Ce dont vous avez besoin

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"](#).
- Compréhension de la configuration que vous voulez utiliser.

Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau Azure auprès 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"](#).

Description de la tâche

Lorsque BlueXP crée un système Cloud Volumes ONTAP dans Azure, il crée plusieurs objets Azure, tels qu'un groupe de ressources, des interfaces réseau et des comptes de stockage. Vous pouvez consulter un résumé des ressources à la fin de l'assistant.

Risque de perte de données

Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour chaque système Cloud Volumes ONTAP.



Le déploiement d'Cloud Volumes ONTAP dans un groupe de ressources existant et partagées n'est pas recommandé en raison du risque de perte de données. BlueXP peut supprimer les ressources Cloud Volumes ONTAP d'un groupe de ressources partagées en cas d'échec ou de suppression du déploiement. Cependant, un utilisateur Azure peut accidentellement supprimer des ressources Cloud Volumes ONTAP d'un groupe de ressources partagé.

Lancement d'un système Cloud Volumes ONTAP à un seul nœud dans Azure

Si vous souhaitez lancer un système Cloud Volumes ONTAP à un seul nœud dans Azure, vous devez créer un environnement de travail à un seul nœud dans BlueXP.

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 **Microsoft Azure** et **Cloud Volumes ONTAP nœud unique**.
4. Si vous y êtes invité, "[Créer un connecteur](#)".
5. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, 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 la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Balises de groupe de ressources	Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, BlueXP les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure ".
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 les informations d'identification	Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. " Apprenez à ajouter des informations d'identification ".

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_azure.mp4

(video)

6. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
- ["Pour en savoir plus sur Cloud Data Sense"](#)
 - ["En savoir plus sur Cloud Backup"](#)
7. **Emplacement** : sélectionnez une région, une zone de disponibilité, un réseau vnet et un sous-réseau, puis cochez la case pour confirmer la connectivité réseau entre le connecteur et l'emplacement cible.
- Pour les systèmes à un seul nœud, vous pouvez choisir la zone de disponibilité dans laquelle vous souhaitez déployer Cloud Volumes ONTAP. Si vous ne sélectionnez pas d'AZ, BlueXP en sélectionne un pour vous.
8. **Connectivité** : choisissez un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez d'utiliser le groupe de sécurité prédéfini ou de l'utiliser.

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

Champ	Description
Groupe de ressources	<p>Créez un nouveau groupe de ressources pour Cloud Volumes ONTAP ou utilisez un groupe de ressources existant. Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. S'il est possible de déployer Cloud Volumes ONTAP dans un groupe de ressources existant et partagées, il n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails.</p> <div><p>Si le compte Azure que vous utilisez possède le "autorisations requises", BlueXP supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec ou de suppression du déploiement.</p></div>
Groupe de sécurité généré	<p>Si vous laissez BlueXP générer le groupe de sécurité pour vous, vous devez choisir comment vous autorisez le trafic :</p> <ul style="list-style-type: none">• Si vous choisissez VNet sélectionné uniquement, la source du trafic entrant correspond à la plage de sous-réseau du VNet sélectionné et à la plage de sous-réseau du VNet où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VNets, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	<p>Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP. "Afficher le groupe de sécurité par défaut".</p>

9. **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"](#).

10. **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.

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



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.

12. **Abonnez-vous à partir du marché Azure**: Suivez les étapes si BlueXP ne pouvait pas activer les déploiements programmatiques de Cloud Volumes ONTAP.
13. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si le Tiering des données vers stockage Blob doit être activé.

Notez ce qui suit :

- 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 ["Dimensionnement du système dans Azure"](#).

- 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.

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

14. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

["En savoir plus sur la vitesse d'écriture"](#).

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

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

15. **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/groupe (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur 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)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. 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). 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" .

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

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

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
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	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs ADDC ou ou=utilisateurs ADDC dans ce champ. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"]
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.

17. **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 ["Présentation des profils d'utilisation des volumes"](#) et ["Vue d'ensemble du hiérarchisation des données"](#).

18. **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 Azure 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 Cloud Volumes ONTAP dans Azure

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans Azure, vous devez créer un environnement de travail haute disponibilité dans BlueXP.

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. Si vous y êtes invité, ["Créer un connecteur"](#).
4. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, 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 la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Balises de groupe de ressources	Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, BlueXP les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure ".
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 les informations d'identification	Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. " Apprenez à ajouter des informations d'identification ".

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_azure.mp4

(video)

5. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.

- ["Pour en savoir plus sur Cloud Data Sense"](#)
- ["En savoir plus sur Cloud Backup"](#)

6. **Modèles de déploiement haute disponibilité** :

a. Sélectionnez **zone de disponibilité unique** ou **zone de disponibilité multiple**.


b. **Emplacement et connectivité** (AZ simple) et **région et connectivité** (AZS multiple)

- Pour une zone AZ unique, sélectionnez une région, un réseau VNet et un sous-réseau.
- Pour plusieurs AZS, sélectionnez une région, un réseau VNet, un sous-réseau, une zone pour le nœud 1 et une zone pour le nœud 2.

c. Cochez la case **J'ai vérifié la connectivité réseau...**

7. **Connectivité** : choisissez un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez d'utiliser le groupe de sécurité prédéfini ou de l'utiliser.

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

Champ	Description
Groupe de ressources	<p>Créez un nouveau groupe de ressources pour Cloud Volumes ONTAP ou utilisez un groupe de ressources existant. Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. S'il est possible de déployer Cloud Volumes ONTAP dans un groupe de ressources existant et partagées, il n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails.</p> <p>Vous devez utiliser un groupe de ressources dédié pour chaque paire HA Cloud Volumes ONTAP que vous déployez dans Azure. Une seule paire haute disponibilité est prise en charge dans un groupe de ressources. BlueXP rencontre des problèmes de connexion si vous essayez de déployer une seconde paire HA Cloud Volumes ONTAP dans un groupe de ressources Azure.</p> <div><p>Si le compte Azure que vous utilisez possède le "autorisations requises", BlueXP supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec ou de suppression du déploiement.</p></div>
Groupe de sécurité généré	<p>Si vous laissez BlueXP générer le groupe de sécurité pour vous, vous devez choisir comment vous autorisez le trafic :</p> <ul style="list-style-type: none">• Si vous choisissez VNet sélectionné uniquement, la source du trafic entrant correspond à la plage de sous-réseau du VNet sélectionné et à la plage de sous-réseau du VNet où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VNets, la source du trafic entrant est la plage IP 0.0.0.0/0.

Champ	Description
Utiliser l'existant	Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP. "Afficher le groupe de sécurité par défaut" .

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 **Modifier la 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 selon vos besoins et sélectionnez un type de machine virtuelle.



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. **Abonnez-vous à partir du marché Azure**: Suivez les étapes si BlueXP ne pouvait pas activer les déploiements programmatiques de Cloud Volumes ONTAP.

12. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si le Tiering des données vers stockage Blob doit être activé.

Notez ce qui suit :

- 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 d'une taille de disque, reportez-vous à la section ["Dimensionnement du système dans Azure"](#).

- 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.

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

13. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

["En savoir plus sur la vitesse d'écriture"](#).

Cette option n'est disponible que pour certains types de VM. Pour connaître les types de VM pris en

charge, reportez-vous à la section ["Configurations prises en charge par licence pour les paires haute disponibilité"](#).

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

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

14. **Communication sécurisée au stockage et WORM** : choisissez d'activer ou non une connexion HTTPS aux comptes de stockage Azure et d'activer le stockage WORM (Write Once, Read Many), si vous le souhaitez.

La connexion HTTPS est établie depuis une paire haute disponibilité Cloud Volumes ONTAP 9.7 vers les comptes de stockage d'objets blob de pages Azure. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé l'environnement de travail.

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

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

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

15. **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)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. 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). 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" .

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

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
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.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs ADDC ou ou=utilisateurs ADDC dans ce champ. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^]
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.

17. **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 "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

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

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

Lancez-vous dans Google Cloud

Démarrage rapide pour Cloud Volumes ONTAP dans Google Cloud

Lancez-vous avec Cloud Volumes ONTAP pour GCP 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 GCP"](#).

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, BlueXP (anciennement Cloud Manager) vous invite à déployer un connecteur si vous n'en avez pas encore.

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 de sorte que le connecteur et le Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour ["Le connecteur et le Cloud Volumes ONTAP"](#).

["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 ["Cloud Backup Service"](#) 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"](#)
- ["Avantages de BlueXP avec les autorisations GCP"](#)

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.

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 des disques 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	
Zone pour le nœud 2	
Zone du médiateur	
VPC-0 et le sous-réseau	
VPC-1 et le sous-réseau	

Informations GCP	Votre valeur
VPC-2 et le 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 le sous-réseau	
VPC-2 et le 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 GCP

Configurez votre réseau Google Cloud Platform de manière à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

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

Conditions requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être satisfaites dans GCP.

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.

Une ou plusieurs zones pour les paires haute disponibilité

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.

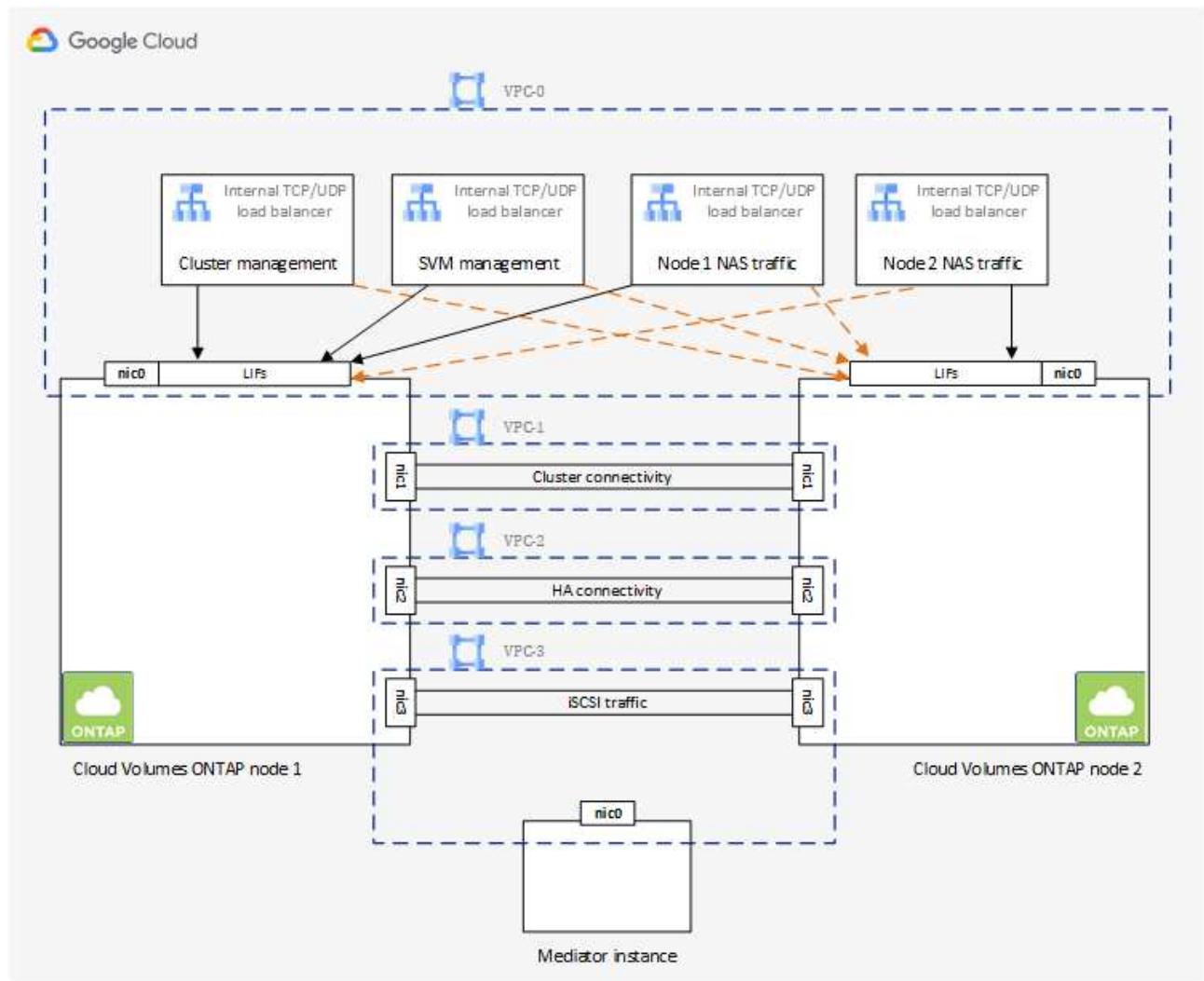
Ce modèle de déploiement réduit vos coûts, car il n'y a pas de frais de sortie de données entre les zones.

Quatre clouds privés virtuels pour les paires haute disponibilité

Quatre clouds privés virtuels (VPC) sont nécessaires dans le cadre d'une configuration haute disponibilité. Quatre VPC sont requis, car GCP 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 pour paires haute disponibilité

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.

Un cloud privé virtuel pour les systèmes à un seul nœud

Un VPC est nécessaire pour un système à un seul nœud.

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 pour Cloud Volumes ONTAP

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"](#).

Adresses IP privées

BlueXP alloue le nombre d'adresses IP privées suivant à Cloud Volumes ONTAP dans GCP :

- **Nœud unique** : 3 ou 4 adresses IP privées

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.

- **Paire HA** : 14 ou 15 adresses IP privées

- 7 ou 8 adresses IP privées pour VPC-0

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
```

- Deux adresses IP privées pour VPC-1
- Deux adresses IP privées pour VPC-2
- Trois adresses IP privées pour VPC-3

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 >>](#).

Connexion de Cloud Volumes ONTAP à Google Cloud Storage pour le Tiering des données

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 GCP et des systèmes ONTAP 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](#)".

Configuration requise pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.


Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur dans votre réseau d'entreprise, vous devez configurer une connexion VPN au réseau virtuel dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
https://support.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div> Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.bluexp.netapp.com » dans une prochaine version.</div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au ["Interface utilisateur locale"](#), que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

Il existe un conflit possible avec des adresses IP dans la plage 172. ["En savoir plus sur cette limitation"](#).

Règles de pare-feu pour Cloud Volumes ONTAP

BlueXP crée des règles de pare-feu GCP 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.

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

Protocole	Port	Objectif
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
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 rquotad

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de 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

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles 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)
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	1860-18699	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
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 de pare-feu pour VPC-1, VPC-2 et VPC-3

Dans GCP, 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).

Règles de pare-feu pour le connecteur

Les règles de pare-feu du connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement du connecteur.

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent 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

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles 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 le connecteur.



L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers GCP et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

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 projetId *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 "[Cloud Backup Service](#)" sauvegarde de volumes dans un stockage objet à faible coût

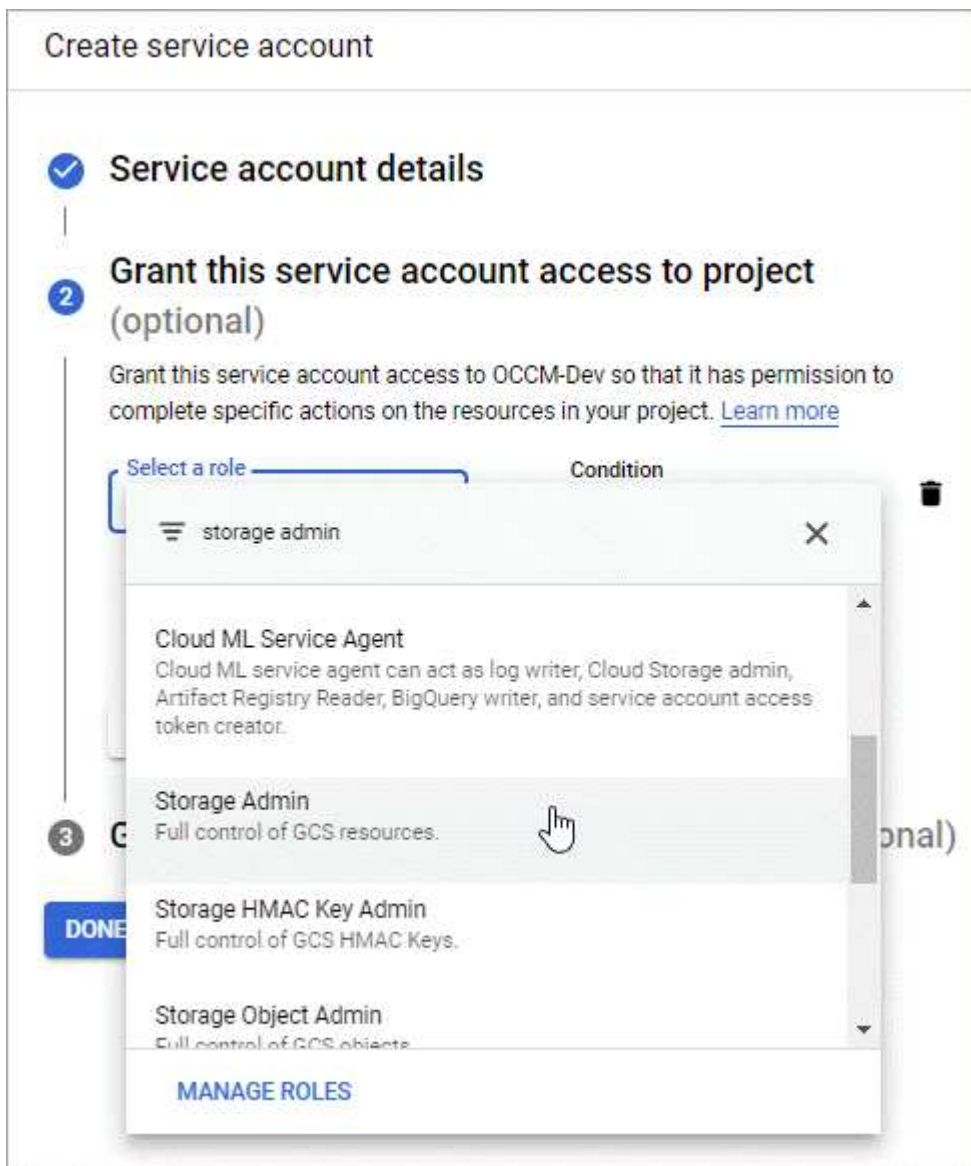
Cloud Volumes ONTAP utilise le compte de service pour accéder aux données hiérarchisées et les gérer dans un autre compartiment pour les sauvegardes.

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. Ce n'est pas requis pour le Cloud Backup Service.

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

Google Cloud Project

Marketplace Subscription

Edit Project

Details

Credentials

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account ⓘ

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

User Name

admin

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"](#).

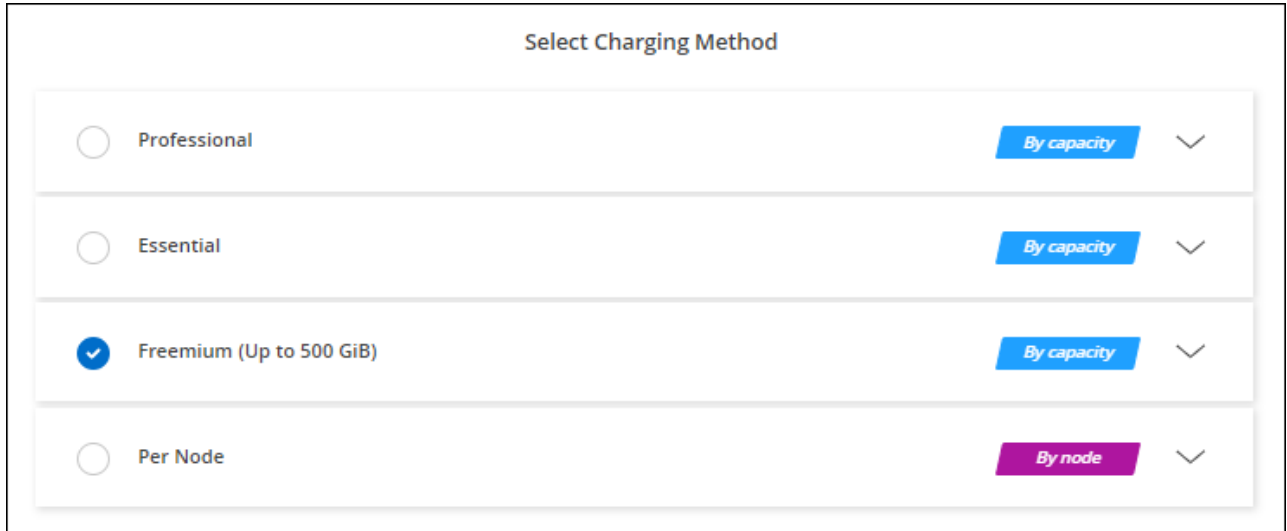
Étapes

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.



Select Charging Method		
<input type="radio"/>	Professional	By capacity
<input type="radio"/>	Essential	By capacity
<input checked="" 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"](#).

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. En l'absence d'erreurs, BlueXP ajoute

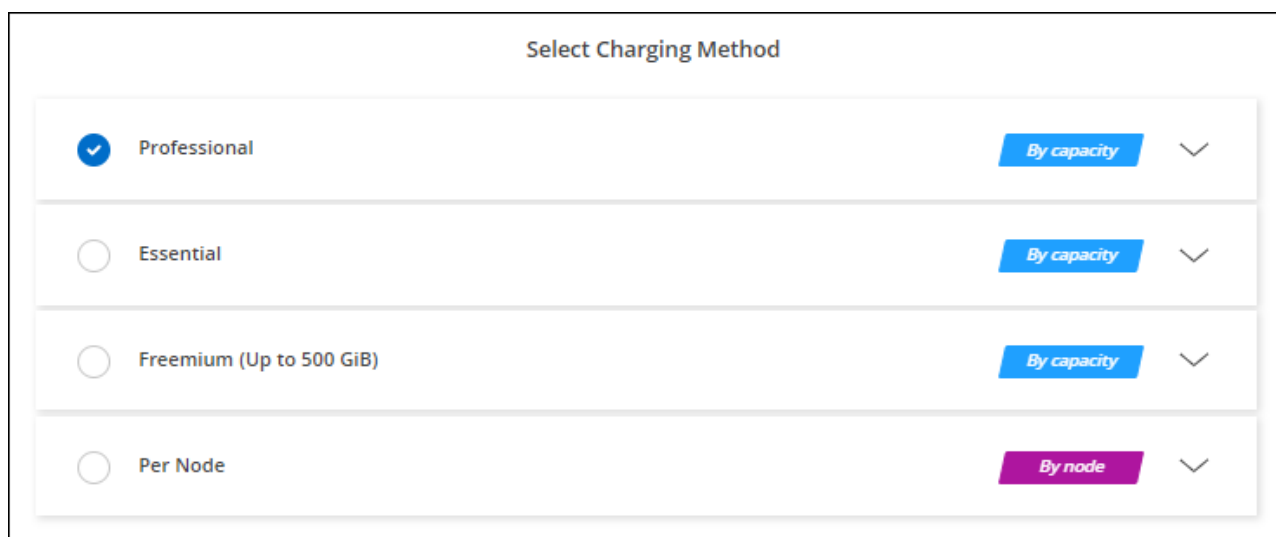
automatiquement les licences au porte-monnaie numérique.

Votre licence doit être disponible auprès du porte-monnaie numérique avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez "[Ajoutez manuellement la licence au porte-monnaie numérique](#)".

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.



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

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

["Consultez 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.

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".](#)



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

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

Abonnement Keystone Flex

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

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)[contacter NetApp] pour autoriser votre compte utilisateur BlueXP avec un ou plusieurs abonnements Keystone Flex.
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 Flex lorsque vous êtes invité à choisir une méthode de charge.

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 GCP

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

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 GCP 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 GCP


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

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 de machine virtuelle GCP. 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 " La sauvegarde dans le cloud " 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	Les étiquettes sont des métadonnées pour les ressources GCP. BlueXP ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. 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. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Google Cloud : étiquetage des ressources ".
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.

Champ	Description
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>  <p>Il s'agit du compte de service que vous avez configuré pour BlueXP, "comme décrit sur cette page".</p> </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 GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.</p>

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

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

6. **Services** : sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner Cloud Backup ou utiliser Tiering, vous devez avoir spécifié le compte de service à l'étape 3.
7. **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 ".
Politique de pare-feu 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.
Utilisez la politique de pare-feu existante	Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises. " En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP ".

8. **Méthodes de 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 ["Dimensionnement du système dans GCP"](#).

12. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

["En savoir plus sur la vitesse d'écriture"](#).

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

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

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 GCP (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 GCP, reportez-vous à ["Configuration et ajout de comptes GCP pour le Tiering des données avec la version 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 à partir de la console GCP.

["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.

Champ	Description
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/groupe (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur 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)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. 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). 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" .

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	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254.
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	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. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["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 "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

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

- Consultez les détails de la configuration.
- Cliquez sur **plus d'informations** pour en savoir plus sur l'assistance et les ressources GCP que BlueXP achètera.
- Cochez les cases **Je comprends....**
- 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 haute disponibilité dans GCP


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

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 de machine virtuelle GCP. 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" ou "La sauvegarde dans le cloud" 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	Les étiquettes sont des métadonnées pour les ressources GCP. BlueXP ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. 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. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Google Cloud : étiquetage des ressources" .

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>  <p>Il s'agit du compte de service que vous avez configuré pour BlueXP, "comme décrit sur cette page".</p> </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 GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.</p>

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

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

5. **Services** : sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner Cloud Backup ou utiliser Tiering, vous devez avoir spécifié le compte de service à l'étape 3.
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 ["Dimensionnement du système dans GCP"](#).

12. **WORM** : activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

IMPOSSIBLE D'activer WORM si le Tiering des données était activé. ["En savoir plus sur le stockage WORM"](#).

13. **Tiering de données dans Google Cloud Platform** : 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 à partir de la console GCP.

["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.

Champ	Description
Autorisations et utilisateurs/groupe (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur 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)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. 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 bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). 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" .

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	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254.
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	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. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["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 "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

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

- Consultez les détails de la configuration.
- Cliquez sur **plus d'informations** pour en savoir plus sur l'assistance et les ressources GCP que BlueXP achètera.
- Cochez les cases **Je comprends....**
- 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.

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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