



Lancez-vous dans Amazon Web Services

Cloud Volumes ONTAP

NetApp
June 11, 2024

Sommaire

- Lancez-vous dans Amazon Web Services 1
 - Démarrage rapide de Cloud Volumes ONTAP dans AWS 1
 - Planification de votre configuration Cloud Volumes ONTAP dans AWS 2
 - Configurez votre réseau 6
 - Configuration du système AWS KMS 28
 - Configurer les rôles IAM pour Cloud Volumes ONTAP 31
 - Configuration des licences pour Cloud Volumes ONTAP dans AWS 40
 - Lancement d'Cloud Volumes ONTAP dans AWS 48
 - Déployez Cloud Volumes ONTAP dans des régions de cloud secret AWS et de cloud secret 62

Lancez-vous dans Amazon Web Services

Démarrage rapide de Cloud Volumes ONTAP dans AWS

Découvrez Cloud Volumes ONTAP dans AWS 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 AWS](#)"

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

2

Planification de la configuration

BlueXP offre des packages préconfigurés qui répondent à vos exigences de charge de travail, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez. "[En savoir plus >>](#)".

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 pour NetApp AutoSupport.

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

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

- ["Créez un connecteur dans AWS à partir de BlueXP"](#)
- ["Créez un connecteur à partir d'AWS Marketplace"](#)
- ["Installez et configurez un connecteur sur site"](#)
- ["Autorisations AWS pour le connecteur"](#)

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 zone locale prise en charge

Cloud Volumes ONTAP est pris en charge dans certaines zones locales AWS, y compris à Singapour. La sélection d'une zone locale est facultative.

["Afficher la liste complète des zones locales"](#).

Les zones locales doivent être activées avant de pouvoir créer et gérer des ressources dans ces zones.

["Découvrez comment activer une zone locale"](#).



Phoenix n'est pas une zone locale prise en charge.

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 soulignées :

- 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	

Informations sur AWS	Votre valeur
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 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

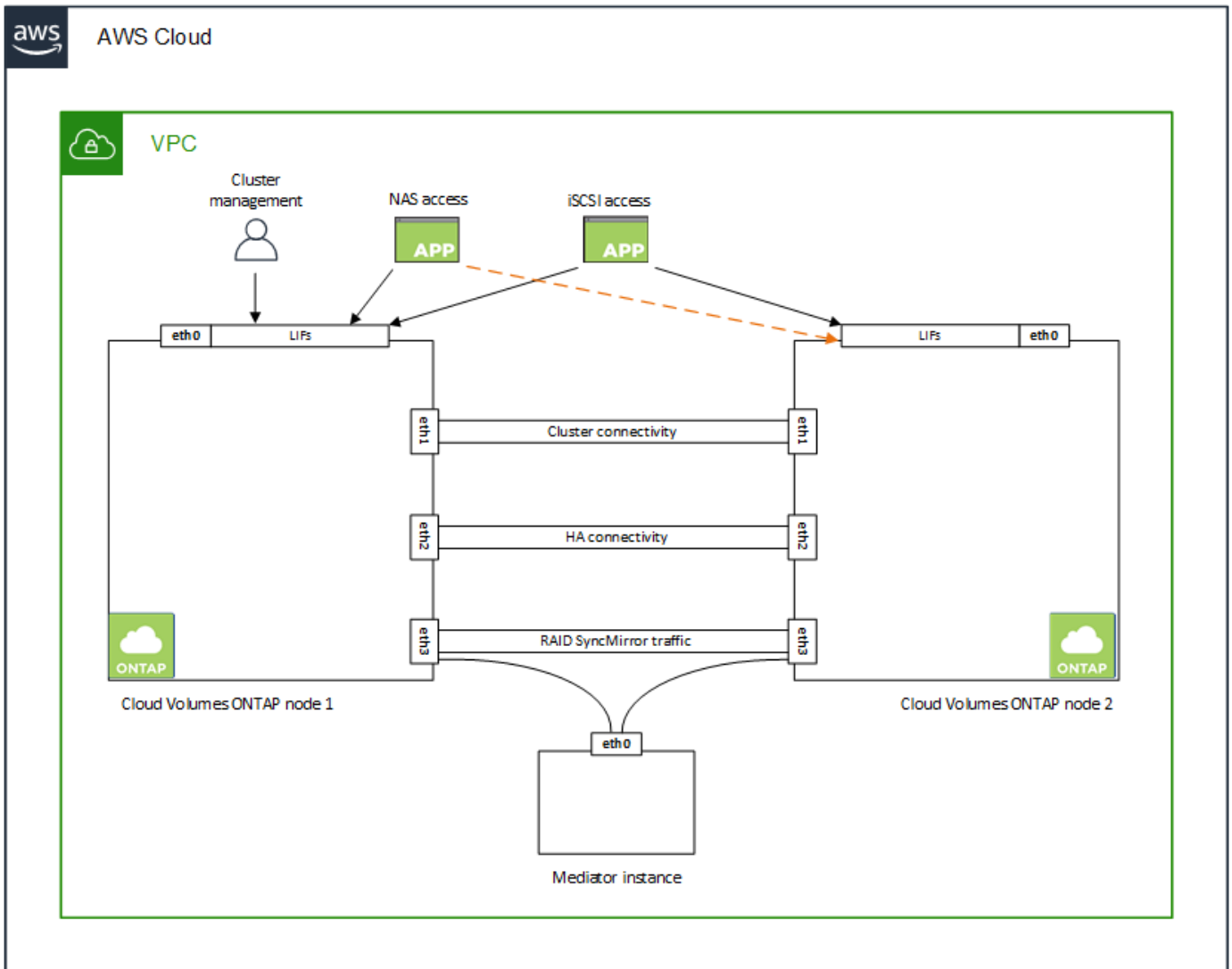
BlueXP alloue 6 adresses IP à un système à nœud unique.

Le tableau suivant fournit des informations détaillées sur les LIFs associées à chaque adresse IP privée.

LIF	Objectif
Gestion du cluster	Gestion administrative de l'ensemble du cluster (paire HA).
Gestion de nœuds	Gestion administrative d'un nœud.
Intercluster	Communication, sauvegarde et réplication entre les clusters
Données NAS	Accès client via les protocoles NAS.
Données iSCSI	Accès client via le protocole iSCSI. 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 machines virtuelles de stockage	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.
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. Ces LIFs gèrent également la migration d'adresses IP flottantes entre nœuds. Ces LIFs sont requises et ne doivent pas être supprimées.

LIF	Interface	Nœud	Objectif
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

Vous n'avez pas besoin 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](#)".



Vous recherchez des informations sur le connecteur ? "[Afficher les règles de groupe de sécurité du connecteur](#)"

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.



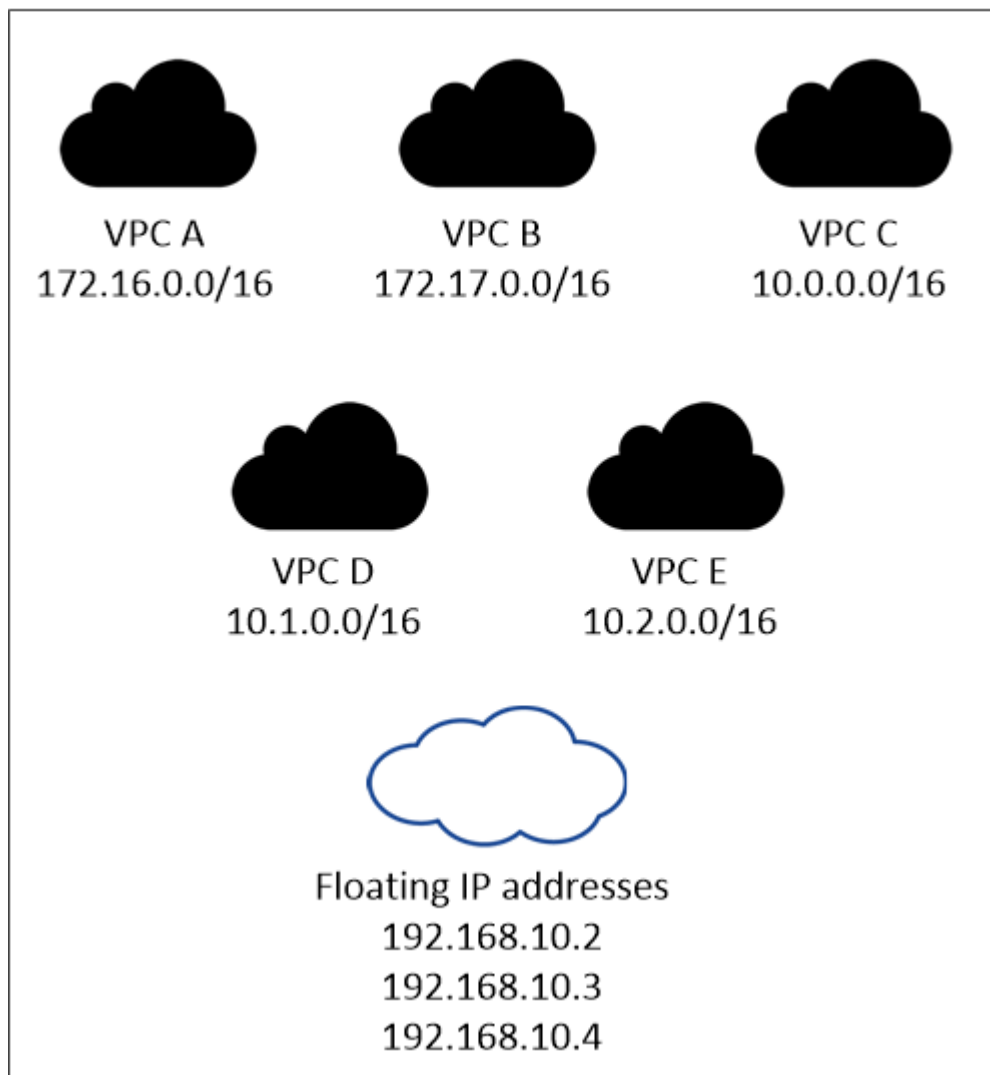
Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité.

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](#)".

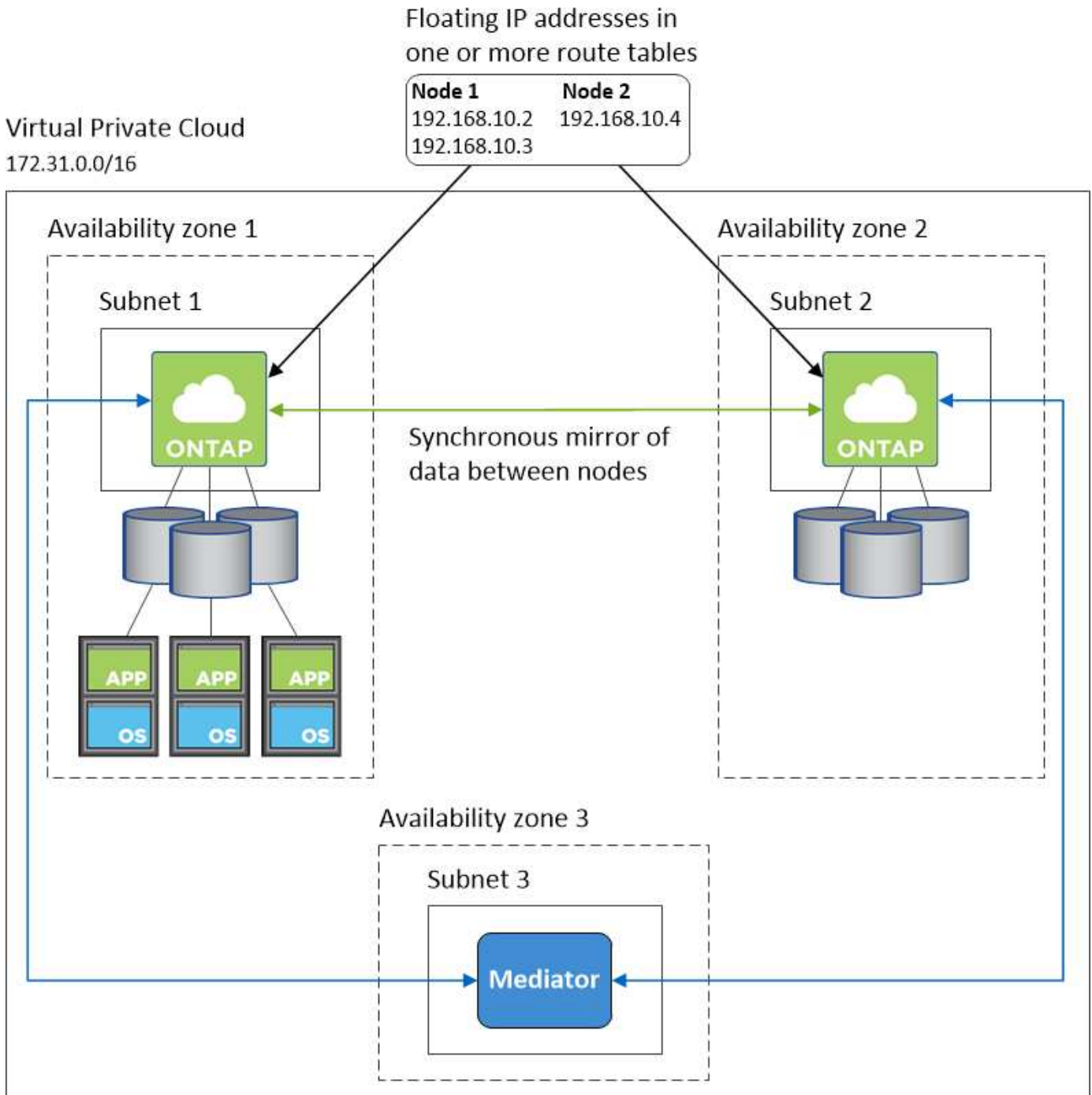
Connexion aux outils de gestion NetApp

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

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

- ["Afficher les exigences de mise en réseau du connecteur"](#)
- ["Règles de groupe de sécurité dans AWS"](#)

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

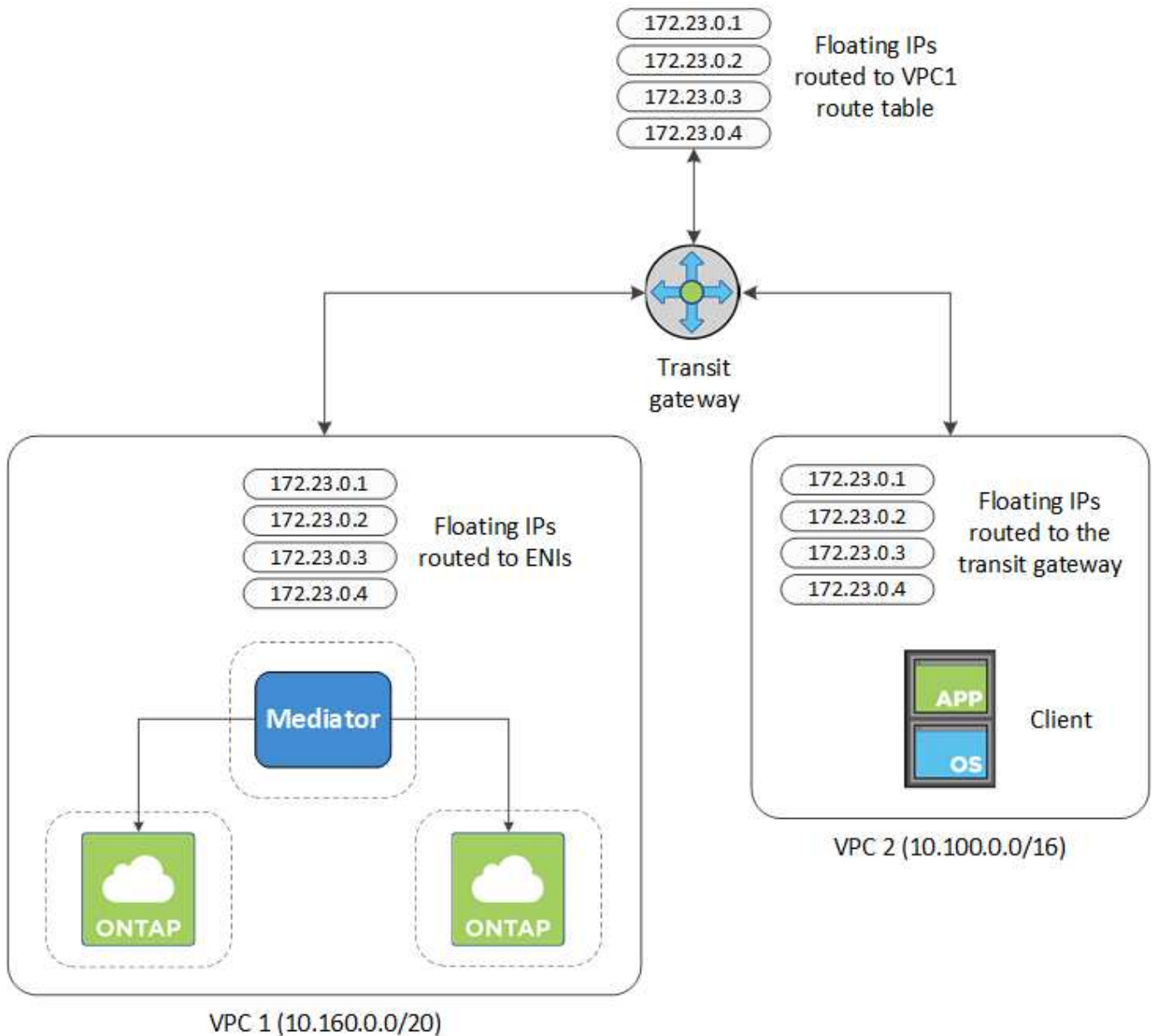
"Adresses IP flottantes" Depuis l'extérieur du VPC, où réside la paire HA.

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.
 - a. Dans le service **VPC**, cliquez sur **Transit Gateway route tables**.
 - b. Sélectionnez la table de routage.
 - c. Cliquez sur **associations**, puis sélectionnez **Créer association**.
 - d. 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	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active

Floating IP Addresses

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

- 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

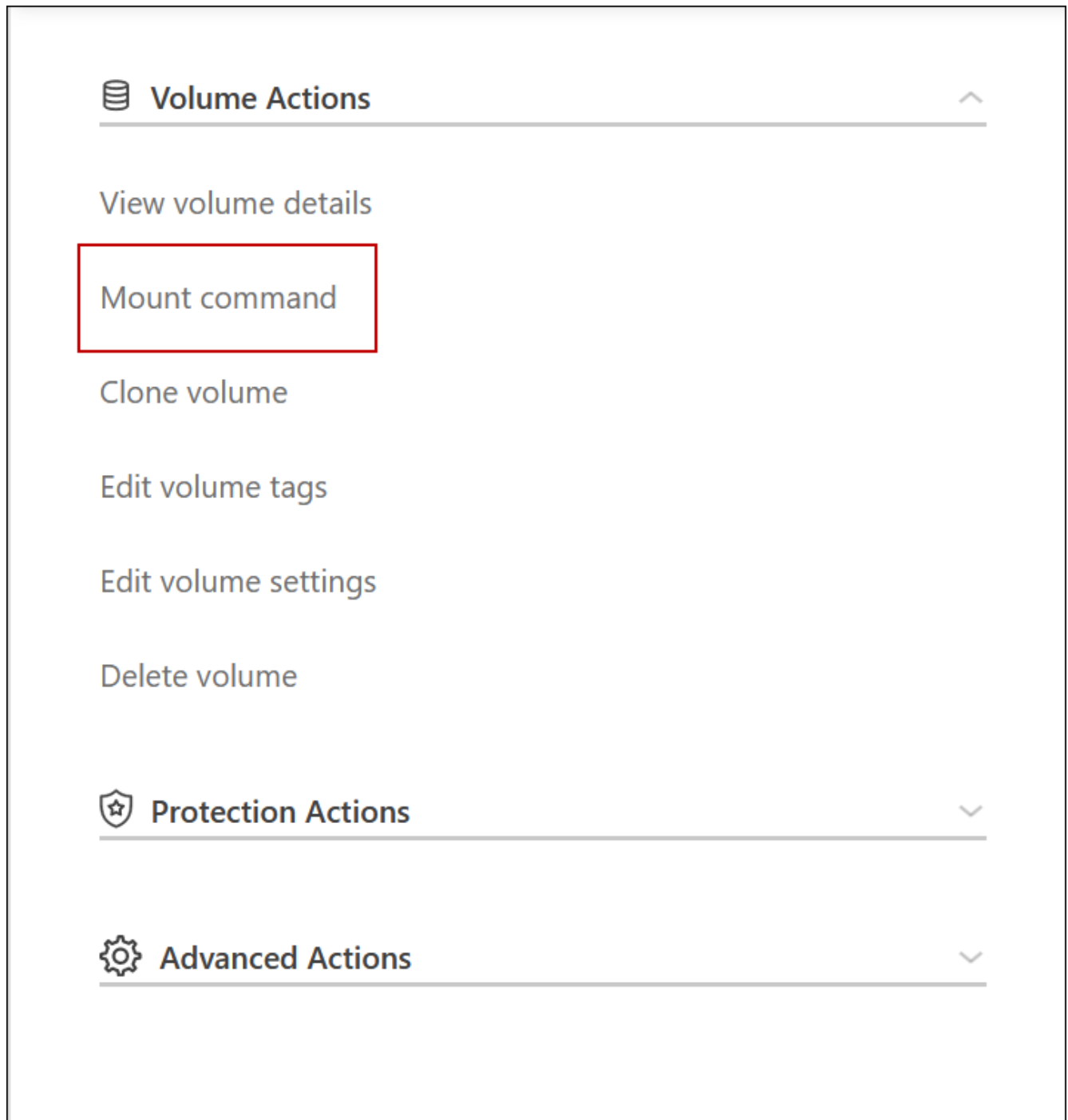
Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-076681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2
Floating act IP Addresses

- Mettez à jour les paramètres des groupes de sécurité sur tout le trafic pour le VPC.
 - Sous Cloud privé virtuel, cliquez sur **sous-réseaux**.
 - Cliquez sur l'onglet **Table de routage**, sélectionnez l'environnement souhaité pour l'une des adresses IP flottantes d'une paire HA.
 - Cliquez sur **groupes de sécurité**.
 - Sélectionnez **Modifier les règles entrantes**.
 - Cliquez sur **Ajouter règle**.
 - Sous Type, sélectionnez **tout le trafic**, puis sélectionnez l'adresse IP VPC.
 - Cliquez sur **Enregistrer les règles** pour appliquer les modifications.
- Montez les volumes sur des clients à l'aide de l'adresse IP flottante.

Vous pouvez trouver l'adresse IP correcte dans BlueXP via l'option **Mount Command** sous le panneau

gérer les volumes de BlueXP.



8. 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

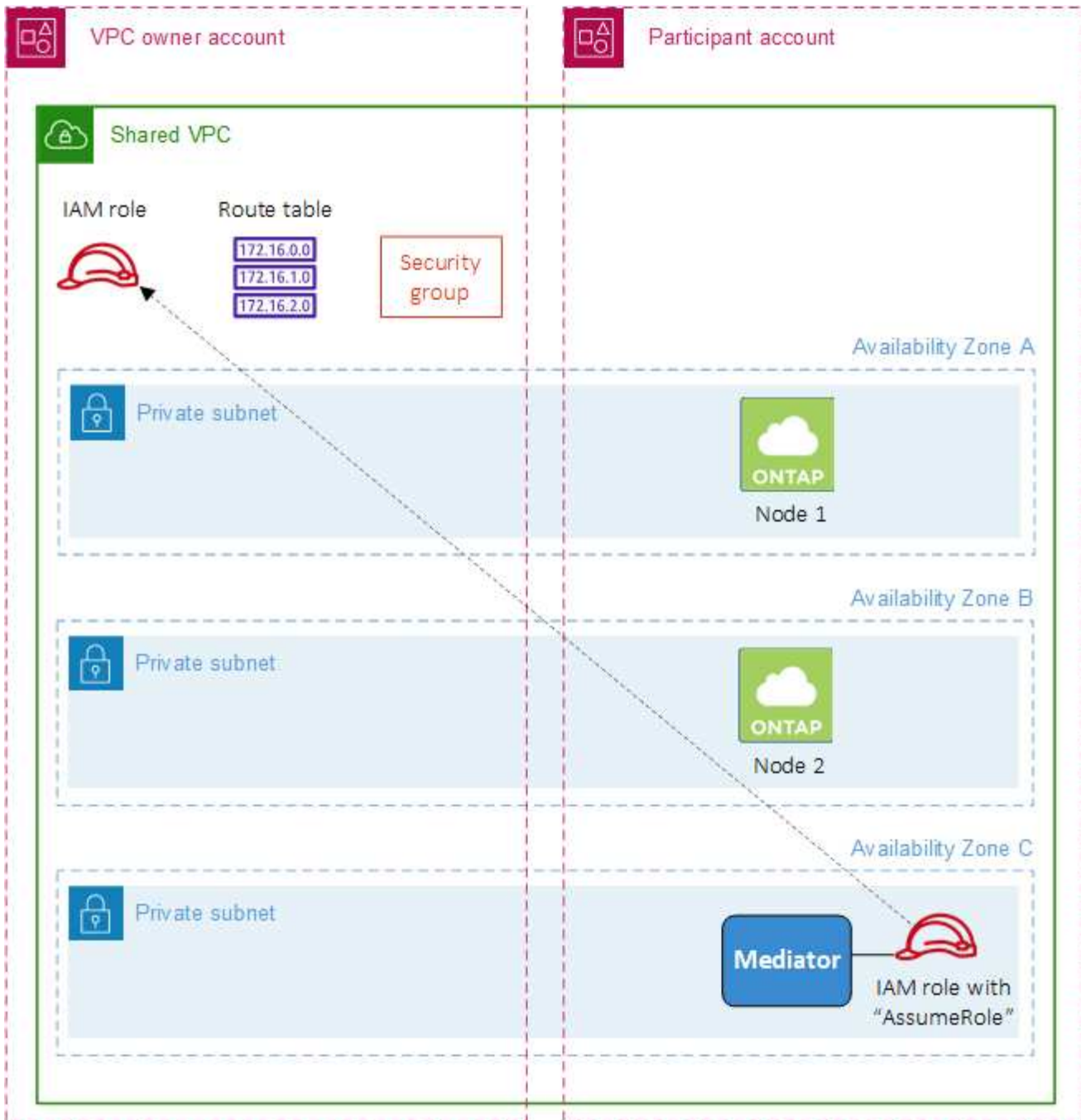
Depuis la version 9.11.1, les paires haute disponibilité Cloud Volumes ONTAP sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre entreprise de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement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

- « SecurityGroupld »

Le champ « securityGroupld » 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 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 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)
Sauvegardes de la configuration	HTTP	80	FRV de gestion des nœuds	\Http://<connector-IP-address>/occm/offbo xconfig	Envoyer des sauvegardes de configuration au connecteur. " En savoir plus sur les fichiers de sauvegarde de configuration ".
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	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

Service	Protocole	Port	Source	Destination	Objectif
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 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

Le groupe de sécurité prédéfini pour le médiateur HA inclut la règle entrante suivante.

Protocole	Port	Source	Objectif
TCP	3000	CIDR du connecteur	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 sur l'instance AWS EC2	Télécharger les mises à niveau pour le médiateur
HTTPS	443	ec2.amazonaws.com	Assistance pour le basculement du stockage
UDP	53	ec2.amazonaws.com	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

["Afficher les règles de groupe de sécurité du connecteur"](#)

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"

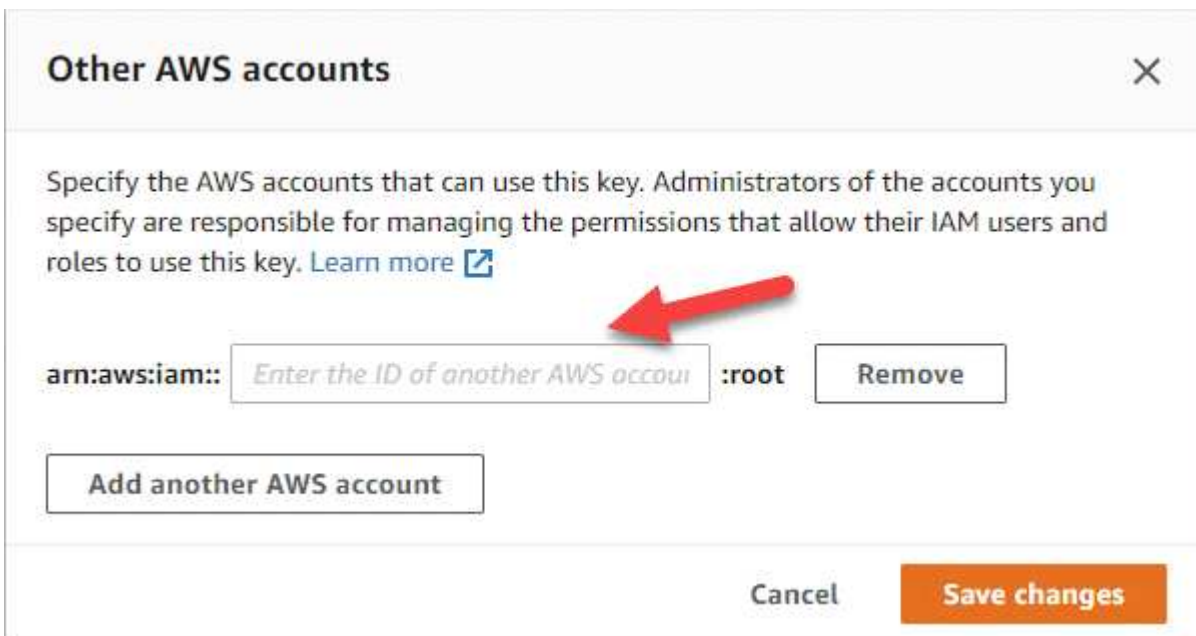
3. Si le CMK se trouve dans un autre compte AWS, procédez comme suit :

- 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.



- 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.



Vous devez fournir votre propre rôle IAM dans AWS Secret Cloud. ["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"
  }]
}
```

Régions les plus secrètes

```
{
  "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"
  }]
}
```

Régions secrètes

```

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

```

- Règle de sauvegarde pour les nœuds Cloud Volumes ONTAP

Si vous prévoyez d'utiliser la sauvegarde et la restauration BlueXP avec vos systèmes Cloud Volumes ONTAP, le rôle IAM des nœuds doit inclure la seconde règle présentée 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"
    }
  ]
}

```

Régions les plus secrètes

```

{
  "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"
    }
  ]
}

```

Régions secrètes


```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso-b: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-b: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",
      "sts:AssumeRole",
      "ec2:DescribeSubnets"
    ],
    "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

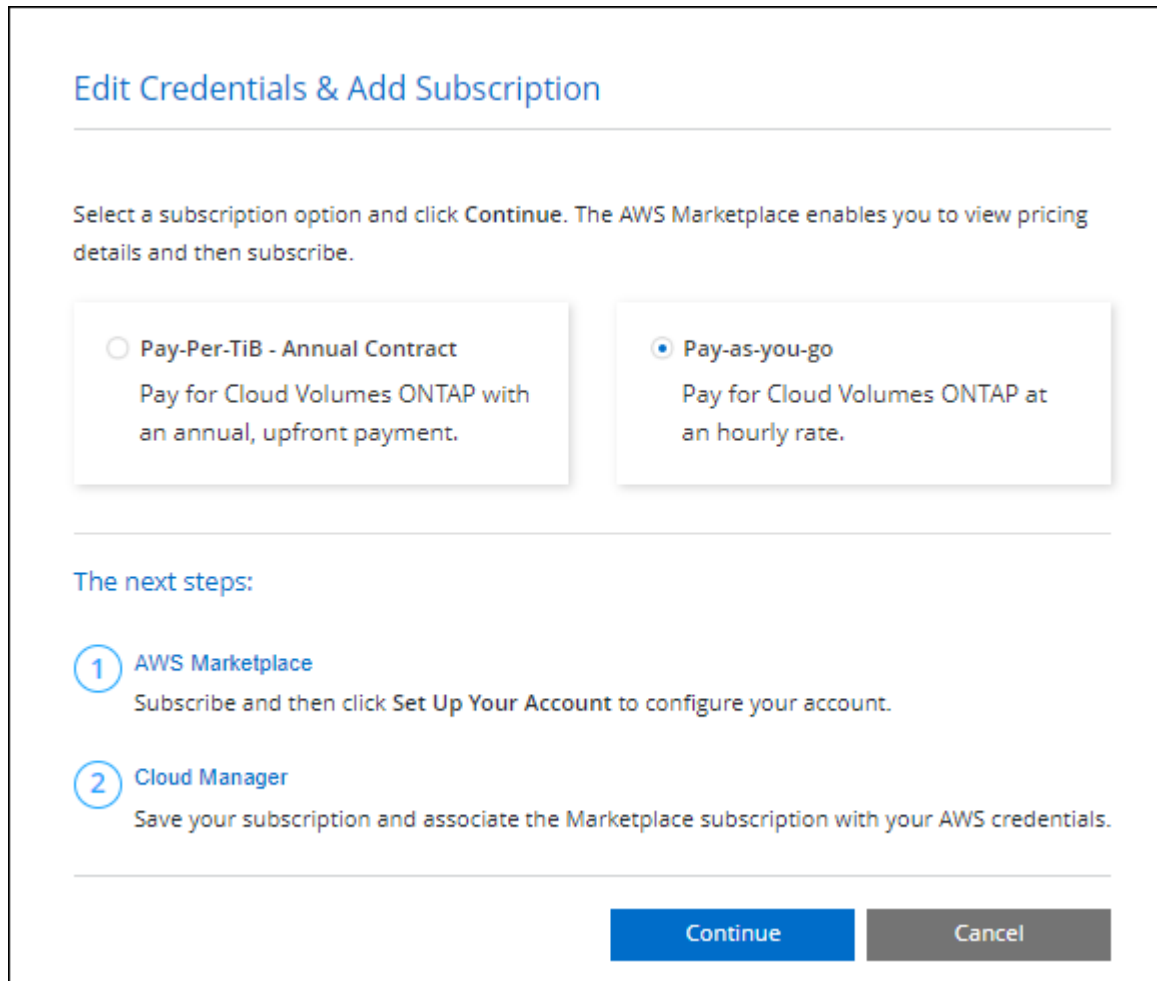
Sélectionnez l'offre « Freemium » pour utiliser Cloud Volumes ONTAP gratuitement et bénéficier d'une capacité provisionnée de 500 Gio. ["En savoir plus sur l'offre Freemium"](#).

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

<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 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. S'il n'y a pas d'erreur, BlueXP ajoute automatiquement les licences au portefeuille digital.

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

3. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.

- a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement basé sur l'utilisation 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

<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 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

<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 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

<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 AWS".

Abonnement Keystone

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

Étapes

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

Select Charging Method

KeystoneBy capacity^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1v

ProfessionalBy capacityv

EssentialBy capacityv

Freemium (Up to 500 GiB)By capacityv

Per NodeBy nodev

["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.

Champ	Description
Modifier les informations d'identification	<p>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.</p> <p>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.</p> <p>"Découvrez comment ajouter des identifiants AWS à BlueXP".</p>

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

Abonnez-vous à BlueXP sur AWS Marketplace

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.

- ["En savoir plus sur la classification BlueXP"](#)
- ["En savoir plus sur la sauvegarde et la restauration BlueXP"](#)



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

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** :

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

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

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

LA FONCTION WORM ne peut pas être activée si le Tiering des données était activé pour les versions Cloud Volumes ONTAP 9.7 et ultérieures. La restauration ou la restauration à partir de Cloud Volumes ONTAP 9.8 est bloquée après l'activation de WORM et de la hiérarchisation.

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

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

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.
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	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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.
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	<p>Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Documents d'automatisation BlueXP" pour plus d'informations.</p> <p>Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS.</p>

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.

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

Certaines zones locales AWS sont disponibles.

Avant de pouvoir utiliser les zones locales AWS, vous devez activer les zones locales et créer un sous-réseau dans la zone locale de votre compte AWS. Suivez les étapes **opt in to an AWS local zone** et **exteNd your Amazon VPC to the local zone** de la "[Tutoriel AWS « commencer à déployer des applications à faible latence avec des zones locales AWS](#)".

Si vous exécutez un connecteur version 3.9.36 ou antérieure, vous devez ajouter l'autorisation suivante au rôle du connecteur AWS dans la console AWS EC2 : DescribeAvailabilityzones.

- 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. "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 :

[Abonnez-vous à BlueXP sur AWS Marketplace](#)

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

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

- ["En savoir plus sur la classification BlueXP"](#)
- ["En savoir plus sur la sauvegarde et la restauration BlueXP"](#)



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

6. **Modèles de déploiement haute disponibilité** : 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	<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 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	<p>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".</p>

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** :

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

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

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

LA FONCTION WORM ne peut pas être activée si le Tiering des données était activé pour les versions Cloud Volumes ONTAP 9.7 et ultérieures. La restauration ou la restauration à partir de Cloud Volumes ONTAP 9.8 est bloquée après l'activation de WORM et de la hiérarchisation.

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

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

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.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	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	Protocol
<p>Volume Name: <input style="width: 80%;" type="text" value="vol"/> Size (GB): <input style="width: 50%;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 80%;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> NFS CIFS iSCSI </p> <p>Share name: <input style="width: 80%;" type="text" value="vol_share"/> Permissions: <input style="width: 50%;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 80%;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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	<p>Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Documents d'automatisation BlueXP" pour plus d'informations.</p> <p>Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS.</p>

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

22. **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 AWS que BlueXP achètera.
- c. Cochez les cases **Je comprends....**
- d. 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.

Déployez Cloud Volumes ONTAP dans des régions de cloud secret AWS et de cloud secret

Comme pour une région AWS standard, vous pouvez utiliser BlueXP dans ["Cloud secret AWS"](#) et ["Le cloud le plus secret d'AWS"](#) De déployer Cloud Volumes ONTAP, qui fournit des fonctionnalités de grande qualité pour votre stockage cloud. AWS Secret Cloud et Top Secret Cloud sont des régions fermées spécifiques aux États-Unis Communauté de renseignement ; les instructions de cette page s'appliquent uniquement aux utilisateurs de la région du cloud secret AWS et du cloud secret supérieur.

Avant de commencer

Avant de commencer, consultez les versions prises en charge dans AWS Secret Cloud et Top Secret Cloud, et découvrez le mode privé dans BlueXP.

- Consultez les versions prises en charge suivantes dans AWS Secret Cloud et Top Secret Cloud :
 - Cloud Volumes ONTAP 9.12.1 P2
 - Version 3.9.32 du connecteur

Il s'agit du logiciel requis pour déployer et gérer Cloud Volumes ONTAP dans AWS. Vous vous connecterez à BlueXP à partir du logiciel installé sur l'instance de connecteur. Le site Web SaaS pour

BlueXP n'est pas pris en charge dans AWS Secret Cloud et Top Secret Cloud.

- En savoir plus sur le mode privé

Dans AWS Secret Cloud et Top Secret Cloud, BlueXP fonctionne en *mode privé*. En mode privé, la couche SaaS de BlueXP n'est pas connectée. Les utilisateurs accèdent à BlueXP en local à partir de la console web disponible depuis le connecteur, et non depuis la couche SaaS.

Pour en savoir plus sur le fonctionnement du mode privé, reportez-vous à la section "[Mode de déploiement privé BlueXP](#)".

Étape 1 : configuration du 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.

Étape 2 : configurer les autorisations

Configurez des stratégies et des rôles IAM qui fournissent au connecteur et à Cloud Volumes ONTAP les autorisations dont ils ont besoin pour effectuer des actions dans le cloud secret AWS ou le cloud top secret.

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
- Pour les paires HA, l'instance 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.



Vous créez ces règles pour prendre en charge les compartiments S3 dans votre environnement AWS. Lors de la création ultérieure des compartiments, assurez-vous que les noms des compartiments sont préfixés à l'aide de `fabric-pool-`. Cette exigence s'applique à la fois aux régions AWS Secret Cloud et Top Secret Cloud.

Régions secrètes

```
{
  "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-b: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-b:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:volume/*"
    ]
}
]
}

```

Régions les plus secrètes

```

{
    "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.

Régions secrètes

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

Régions les plus secrètes


```

{
  "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"
  }]
}

```

Pour les paires HA, si vous prévoyez de déployer une paire Cloud Volumes ONTAP HA, créez une règle pour le médiateur HA.

```

{
  "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": "*"
  }
]
}

```

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

Créer le rôle :

De la même manière que les règles, vous devez avoir un rôle IAM pour le connecteur et un pour les nœuds Cloud Volumes ONTAP.

Pour les paires HA : comme 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).

Sélectionnez le rôle :

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 lorsque vous créez un environnement de travail Cloud Volumes ONTAP à partir de BlueXP.

Pour les paires HA, 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 BlueXP.

Étape 3 : configuration du serveur KMS AWS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, vérifiez que les exigences du service de gestion des clés AWS (KMS) 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 à BlueXP lorsque vous créez le système Cloud Volumes ONTAP.

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

Cela donne des autorisations BlueXP pour utiliser le CMK avec Cloud Volumes ONTAP.

Étape 4 : installez le connecteur et configurez BlueXP

Avant de pouvoir commencer à utiliser BlueXP pour déployer Cloud Volumes ONTAP dans AWS, vous devez installer et configurer le connecteur BlueXP. BlueXP peut ainsi gérer les ressources et les processus au sein de votre environnement de cloud public (y compris Cloud Volumes ONTAP).

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.



Pour les régions du cloud secret AWS, vous devez télécharger le `NSS Root CA 2` Et pour Top Secret Cloud, le `Amazon Root CA 4` certificat. Assurez-vous de télécharger uniquement ces certificats et non l'ensemble de la chaîne. Le fichier de la chaîne de certificats est volumineux et le téléchargement peut échouer. Si vous avez d'autres certificats, vous pouvez les télécharger ultérieurement, comme décrit à l'étape suivante.

Vous devrez télécharger le certificat pendant le processus d'installation. BlueXP utilise le certificat de confiance pour envoyer des demandes vers AWS via HTTPS.

2. Lancez l'instance de connecteur :
 - a. Accédez à la page AWS Intelligence Community Marketplace pour BlueXP.
 - 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 configuration des autorisations.
- 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 BlueXP à partir d'un hôte qui a une connexion à l'instance de connecteur :
 - a. Ouvrez un navigateur Web et entrez `https://ipaddress` Où `ipaddress` est l'adresse IP de l'hôte Linux où vous avez installé le connecteur.
 - b. Spécifiez un serveur proxy pour la connectivité aux services AWS.
 - c. Téléchargez le certificat que vous avez obtenu à l'étape 1.
 - d. Sélectionnez **configurer Nouveau BlueXP** et suivez les invites pour configurer le système.
 - **Détails du système** : saisissez un nom pour le connecteur et le nom de votre société.

- **Créer un utilisateur Admin** : créez l'utilisateur admin pour le système.

Ce compte utilisateur s'exécute localement sur le système. Il n'y a pas de connexion au service auth0 disponible via BlueXP.

- **Révision** : consultez les détails, acceptez le contrat de licence, puis sélectionnez **configurer**.

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.

Étape 5 : (facultatif) installez un certificat en mode privé

Cette étape est facultative pour les régions Cloud secret AWS et Cloud secret principal, et n'est requise que si vous avez des certificats supplémentaires, à l'exception des certificats racine que vous avez installés à l'étape précédente.

Étapes

1. Répertoriez les certificats installés existants.

a. Pour collecter l'ID docker du conteneur ocm (nommé « ds-octm-1 »), exécutez la commande suivante :

```
docker ps
```

b. Pour accéder à l'intérieur du conteneur octm, exécutez la commande suivante :

```
docker exec -it <docker-id> /bin/sh
```

c. Pour collecter le mot de passe à partir de la variable d'environnement « TRUST_STORE_PASSWORD », exécutez la commande suivante :

```
env
```

d. Pour répertorier tous les certificats installés dans truststore, exécutez la commande suivante et utilisez le mot de passe collecté à l'étape précédente :

```
keytool -list -v -keystore ocm.truststore
```

2. Ajouter un certificat.

a. Pour collecter l'ID docker du conteneur ocm (nommé « ds-octm-1 »), exécutez la commande suivante :

```
docker ps
```

b. Pour accéder à l'intérieur du conteneur octm, exécutez la commande suivante :

```
docker exec -it <docker-id> /bin/sh
```

Enregistrez le nouveau fichier de certificat à l'intérieur.

- c. Pour collecter le mot de passe à partir de la variable d'environnement « TRUST_STORE_PASSWORD », exécutez la commande suivante :

```
env
```

- d. Pour ajouter le certificat au magasin de confiance, exécutez la commande suivante et utilisez le mot de passe de l'étape précédente :

```
keytool -import -alias <alias-name> -file <certificate-file-name>  
-keystore occm.truststore
```

- e. Pour vérifier que le certificat est installé, exécutez la commande suivante :

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

- f. Pour quitter le conteneur octm, exécutez la commande suivante :

```
exit
```

- g. Pour réinitialiser le conteneur octm, exécutez la commande suivante :

```
docker restart <docker-id>
```

Étape 6 : ajoutez une licence au portefeuille digital BlueXP

Si vous avez acheté une licence auprès de NetApp, vous devez l'ajouter au portefeuille digital BlueXP afin de sélectionner la licence lors de la création d'un nouveau système Cloud Volumes ONTAP. Le portefeuille numérique identifie ces licences comme non attribuées.

Étapes

1. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Cliquez sur **non affecté**.
4. Cliquez sur **Ajouter des licences non attribuées**.
5. Saisissez le numéro de série de la licence ou téléchargez le fichier de licence.
6. Si vous n'avez pas encore le fichier de licence, vous devrez télécharger manuellement le fichier de licence

à partir de netapp.com.

- a. Accédez au "[Générateur de fichiers de licences NetApp](#)" Et connectez-vous en utilisant vos identifiants du site du support NetApp.
- b. Entrez votre mot de passe, choisissez votre produit, entrez le numéro de série, confirmez que vous avez lu et accepté la politique de confidentialité, puis cliquez sur **Envoyer**.
- c. Choisissez si vous souhaitez recevoir le fichier numéro de série.NLF JSON par e-mail ou par téléchargement direct.

7. Cliquez sur **Ajouter une licence**.

Résultat

BlueXP ajoute la licence au portefeuille digital. La licence sera identifiée comme non affectée jusqu'à ce que vous l'associez à un nouveau système Cloud Volumes ONTAP. À ce stade, la licence est déplacée vers l'onglet BYOL du portefeuille digital.

Étape 7 : lancez Cloud Volumes ONTAP à partir de BlueXP

Vous pouvez lancer des instances Cloud Volumes ONTAP dans le cloud secret AWS et le cloud secret en créant de nouveaux environnements de travail dans BlueXP.

Avant de commencer

Pour les paires HA, 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.

Pour HA : 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.



Lors de la sélection à l'aide de l'assistant, ne sélectionnez pas **Data Sense & Compliance** et **Backup to Cloud** sous **Services**. Sous **Packages préconfigurés**, sélectionnez **Modifier la configuration** uniquement et assurez-vous que vous n'avez sélectionné aucune autre option. Les packages préconfigurés ne sont pas pris en charge dans les régions AWS Secret Cloud et Top Secret Cloud, et si cette option est sélectionnée, votre déploiement échouera.

Remarques sur le déploiement de Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité

Notez les points suivants lorsque vous terminez l'assistant pour les paires haute disponibilité.

- Vous devez configurer une passerelle de transit lorsque vous déployez Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité (AZ). Voir "[Configuration d'une passerelle de transit AWS](#)".
- Déployez la configuration comme suit car seulement deux zones de disponibilité étaient disponibles dans le Top Secret Cloud d'AWS au moment de la publication :
 - Nœud 1 : zone de disponibilité A
 - Nœud 2 : zone de disponibilité B
 - Médiateur : zone de disponibilité A ou B

Remarques sur le déploiement de Cloud Volumes ONTAP dans un nœud unique ou haute disponibilité

Notez les éléments suivants lorsque vous terminez l'assistant :

- 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.

Résultat

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

Étape 8 : installez les certificats de sécurité pour la hiérarchisation des données

Vous devez installer manuellement des certificats de sécurité pour activer le Tiering des données dans les régions AWS Secret Cloud et Top Secret Cloud.

Avant de commencer

1. Création de compartiments S3.



Assurez-vous que les noms de compartiment sont préfixés par `fabric-pool-`. Par exemple `fabric-pool-testbucket`.

2. Conservez les certificats racine que vous avez installés dans `step 4` pratique.

Étapes

1. Copiez le texte des certificats racine que vous avez installés dans `step 4`.
2. Connexion sécurisée au système Cloud Volumes ONTAP via l'interface de ligne de commande.
3. Installez les certificats racine. Vous devrez peut-être appuyer sur `ENTER` saisir plusieurs fois :

```
security certificate install -type server-ca -cert-name <certificate-name>
```

4. Lorsque vous y êtes invité, entrez le texte intégralement copié, y compris et de ----- BEGIN CERTIFICATE ----- à ----- END CERTIFICATE -----.
5. Conservez une copie du certificat numérique signé par l'autorité de certification pour référence ultérieure.
6. Conservez le nom de l'autorité de certification et le numéro de série du certificat.
7. Configurez le magasin d'objets pour les régions AWS Secret Cloud et Top Secret Cloud : `set -privilege advanced -confirmations off`
8. Exécutez cette commande pour configurer le magasin d'objets.



Tous les noms de ressources Amazon (ARN) doivent être accompagnés du suffixe `-iso-b`, comme `arn:aws-iso-b`. Par exemple, si une ressource requiert un ARN avec une région, pour Top Secret Cloud, utilisez la convention de dénomination comme `us-iso-b` pour le `-server` drapeau. Pour le cloud secret AWS, utilisez `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Vérifiez que le magasin d'objets a été créé avec succès : `storage aggregate object-store show -instance`
10. Reliez le magasin d'objets à l'agrégat. Cette opération doit être répétée pour chaque nouvel agrégat : `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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