



Documentation Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
December 15, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap/index.html> on December 15, 2022. Always check docs.netapp.com for the latest.

Table des matières

| | |
|---|-----|
| Documentation Cloud Volumes ONTAP | 1 |
| Notes de mise à jour | 2 |
| Quoi de neuf | 2 |
| Limites connues | 22 |
| Notes de version de Cloud Volumes ONTAP | 23 |
| Commencez | 24 |
| Découvrez Cloud Volumes ONTAP | 24 |
| Lancez-vous dans Amazon Web Services | 25 |
| Commencez avec Microsoft Azure | 96 |
| Lancez-vous dans Google Cloud | 136 |
| Utiliser Cloud Volumes ONTAP | 177 |
| Gestion des licences | 177 |
| Administration des volumes et des LUN | 189 |
| Administration d'agrégats | 213 |
| Administration des machines virtuelles de stockage | 216 |
| Sécurité et chiffrement des données | 249 |
| Administration du système | 256 |
| État de santé du système et événements | 284 |
| Concepts | 288 |
| Licences Cloud Volumes ONTAP | 288 |
| Stockage | 294 |
| Paires haute disponibilité | 316 |
| Sécurité | 334 |
| Performance | 336 |
| Gestion de licence pour le modèle BYOL basé sur les nœuds | 337 |
| Conseiller digital AutoSupport et Active IQ | 339 |
| Configuration par défaut pour Cloud Volumes ONTAP | 340 |
| Connaissances et support | 344 |
| S'inscrire pour obtenir de l'aide | 344 |
| Obtenez de l'aide | 348 |
| Mentions légales | 352 |
| Droits d'auteur | 352 |
| Marques déposées | 352 |
| Brevets | 352 |
| Politique de confidentialité | 352 |
| Source ouverte | 352 |

Documentation Cloud Volumes ONTAP

Notes de mise à jour

Quoi de neuf

Découvrez les nouveautés de la gestion Cloud Volumes ONTAP dans BlueXP (anciennement Cloud Manager).

Les améliorations décrites sur cette page sont spécifiques aux fonctions BlueXP qui permettent la gestion de Cloud Volumes ONTAP. Pour découvrir les nouveautés du logiciel Cloud Volumes ONTAP lui-même, ["Accédez aux notes de version de Cloud Volumes ONTAP"](#)

15 décembre 2022

Cloud Volumes ONTAP 9.12.0

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.12.0 dans AWS et Google Cloud.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#).

8 décembre 2022

Cloud Volumes ONTAP 9.12.1

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.12.1, qui inclut également la prise en charge de nouvelles fonctionnalités et de régions de fournisseurs de cloud supplémentaires.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#)

4 décembre 2022

Les modifications suivantes ont été introduites avec la version 3.9.24 du connecteur.

WORM + sauvegarde dans le cloud désormais disponible lors de la création de Cloud Volumes ONTAP

La possibilité d'activer les fonctionnalités WORM (Write Once, Read Many) et Cloud Backup est désormais disponible lors du processus de création de Cloud Volumes ONTAP.

La région Israël est désormais prise en charge dans Google Cloud

La région Israël est désormais prise en charge dans Google Cloud pour Cloud Volumes ONTAP et le connecteur pour Cloud Volumes ONTAP 9.11.1 P3 ou version ultérieure.

15 novembre 2022

Les modifications suivantes ont été introduites avec la version 3.9.23 du connecteur.

Licence ONTAP S3 dans GCP

Une licence ONTAP S3 est désormais incluse sur les systèmes Cloud Volumes ONTAP nouveaux et existants qui exécutent la version 9.12.1 ou une version ultérieure dans Google Cloud Platform.

["Découvrez comment configurer et gérer les services de stockage objet S3 dans ONTAP"](#)

6 novembre 2022

Les modifications suivantes ont été introduites avec la version 3.9.23 du connecteur.

Déplacement de groupes de ressources dans Azure

Vous pouvez maintenant déplacer un environnement de travail d'un groupe de ressources vers un autre groupe de ressources dans Azure dans le même abonnement Azure.

Pour plus d'informations, voir ["Déplacement de groupes de ressources"](#).

Certification NDMP-copie

NDMP-copy est désormais certifié pour Cloud Volume ONTAP.

Pour plus d'informations sur la configuration et l'utilisation de NDMP, reportez-vous à la section ["Présentation de la configuration NDMP"](#).

Prise en charge du chiffrement de disque géré pour Azure

Une nouvelle autorisation Azure a été ajoutée qui vous permet maintenant de chiffrer tous les disques gérés lors de leur création.

Pour plus d'informations sur cette nouvelle fonctionnalité, voir ["Configuration de Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans Azure"](#).

18 septembre 2022

Les modifications suivantes ont été introduites avec la version 3.9.22 du connecteur.

Améliorations du portefeuille numérique

- Le porte-monnaie numérique présente maintenant un résumé du package de licences d'E/S optimisées et de la capacité WORM provisionnée pour les systèmes Cloud Volumes ONTAP de votre compte.

Ces informations vous permettront de mieux comprendre la facturation et l'achat de capacité supplémentaire.

["Découvrez comment afficher la capacité consommée dans votre compte"](#).

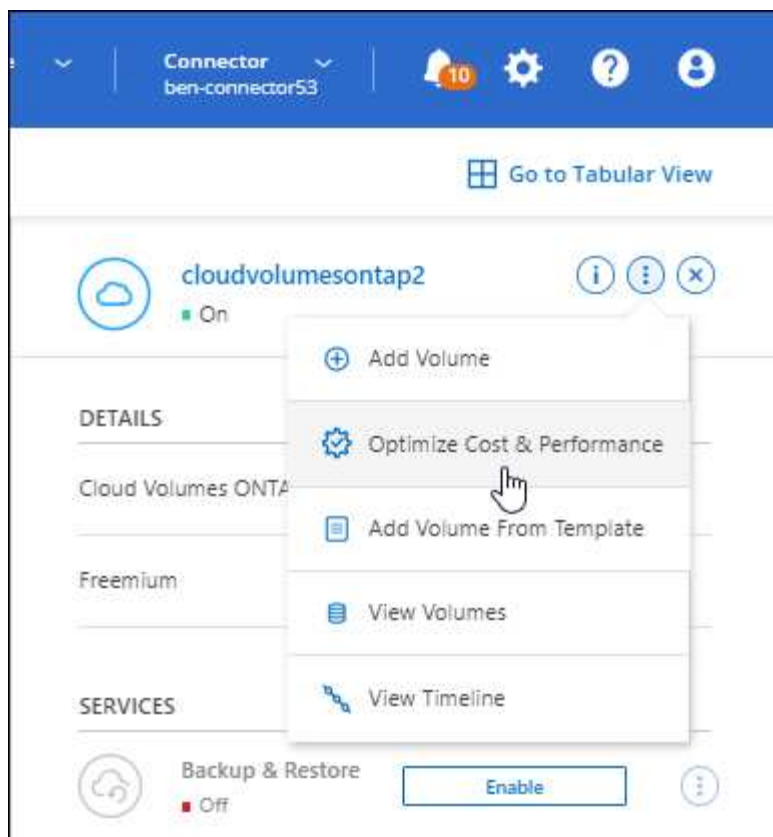
- Vous pouvez désormais passer d'une méthode de charge à la méthode de charge optimisée.

["Apprenez à changer les méthodes de charge"](#).

Optimisation des coûts et des performances

Vous pouvez désormais optimiser les coûts et les performances d'un système Cloud Volumes ONTAP directement à partir de la fenêtre Canvas.

Après avoir sélectionné un environnement de travail, vous pouvez choisir l'option **optimiser les coûts et les performances** pour changer le type d'instance de Cloud Volumes ONTAP. La sélection d'une instance de plus petite taille peut vous aider à réduire les coûts, tandis que le passage à une instance de plus grande taille peut vous aider à optimiser les performances.



Notifications AutoSupport

BlueXP va maintenant générer une notification si un système Cloud Volumes ONTAP ne parvient pas à envoyer de messages AutoSupport. La notification comprend un lien vers des instructions qui vous aideront à résoudre les problèmes de mise en réseau.

31 juillet 2022

Les modifications suivantes ont été introduites avec la version 3.9.21 du connecteur.

Licence MTEKM

La licence MTEKM (Multi-tenant Encryption Key Management) est désormais incluse dans les systèmes Cloud Volumes ONTAP nouveaux et existants qui exécutent la version 9.11.1 ou une version ultérieure.

La gestion externe et mutualisée des clés permet à chaque machine virtuelle de stockage (SVM) de gérer ses propres clés via un serveur KMIP grâce à NetApp Volume Encryption.

["Découvrez comment chiffrer les volumes à l'aide des solutions de cryptage NetApp".](#)

Serveur proxy

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

AutoSupport surveille de manière proactive l'état de santé de votre système et envoie des messages au support technique NetApp.

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.

Changer la méthode de charge

Vous pouvez désormais modifier la méthode de facturation d'un système Cloud Volumes ONTAP utilisant des licences basées sur la capacité. Par exemple, si vous avez déployé un système Cloud Volumes ONTAP avec le pack Essentials, vous pouvez le remplacer par le pack Professional si vos besoins évoluent. Cette fonction est disponible dans le porte-monnaie numérique.

["Apprenez à changer les méthodes de charge"](#).

Amélioration du groupe de sécurité

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, l'interface utilisateur vous permet désormais de choisir si vous souhaitez que le groupe de sécurité prédéfini autorise le trafic dans le réseau sélectionné uniquement (recommandé) ou sur tous les réseaux.



Connectivity

Security Group

☒ Generated security group ☐ Use existing security group

Allow traffic within:

The selected VPC only (recommended) ▼

SSH Authentication Method

☒ Password ☐ Key Pair

18 juillet 2022

Nouveaux packages de licences dans Azure

Deux nouveaux packages de licence basés sur la capacité sont disponibles pour Cloud Volumes ONTAP dans Azure lorsque vous payez via un abonnement Azure Marketplace :

- **Optimisé** : payez séparément la capacité provisionnée et les opérations d'E/S.
- **Edge cache** : licences pour ["Cloud volumes Edge cache"](#)

["En savoir plus sur ces packs de licences"](#).

3 juillet 2022

Les modifications suivantes ont été introduites avec la version 3.9.20 du connecteur.

Portefeuille numérique

Le porte-monnaie numérique vous indique maintenant la capacité totale consommée dans votre compte et la capacité consommée par le package de licences. Cela vous permet de mieux comprendre la façon dont vous achetez de la capacité supplémentaire et si celle-ci est nécessaire.



Amélioration des volumes élastiques

BlueXP prend désormais en charge la fonctionnalité Amazon EBS Elastic volumes lors de la création d'un environnement de travail Cloud Volumes ONTAP à partir de l'interface utilisateur. La fonctionnalité Elastic volumes est activée par défaut lors de l'utilisation de disques gp3 ou io1. 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"](#).

Licence ONTAP S3 dans AWS

Une licence ONTAP S3 est désormais incluse sur les systèmes Cloud Volumes ONTAP nouveaux et existants qui exécutent la version 9.11.0 ou une version ultérieure dans AWS.

["Découvrez comment configurer et gérer les services de stockage objet S3 dans ONTAP"](#)

Prise en charge de nouvelles régions Azure Cloud

Depuis la version 9.10.1, Cloud Volumes ONTAP est désormais pris en charge dans la région Azure West US 3.

["Consultez la liste complète des régions prises en charge par Cloud Volumes ONTAP"](#)

Licence ONTAP S3 dans Azure

Une licence ONTAP S3 est désormais incluse sur les systèmes Cloud Volumes ONTAP nouveaux et existants

qui exécutent la version 9.9.1 ou une version ultérieure dans Azure.

["Découvrez comment configurer et gérer les services de stockage objet S3 dans ONTAP"](#)

7 juin 2022

Les modifications suivantes ont été introduites avec la version 3.9.19 du connecteur.

Cloud Volumes ONTAP 9.11.1

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.11.1, qui inclut également la prise en charge de nouvelles fonctionnalités et de régions de fournisseurs de cloud supplémentaires.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#)

Nouvelle vue avancée

Si vous devez effectuer une gestion avancée de Cloud Volumes ONTAP, vous pouvez utiliser ONTAP System Manager, une interface de gestion fournie avec un système ONTAP. Nous avons inclus l'interface System Manager directement dans BlueXP afin que vous n'ayez pas besoin de laisser BlueXP pour une gestion avancée.

Cette vue avancée est disponible sous forme d'aperçu avec Cloud Volumes ONTAP 9.10.0 et versions ultérieures. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

["En savoir plus sur la vue avancée"](#).

Prise en charge d'Amazon EBS Elastic volumes

La prise en charge de la fonctionnalité Amazon EBS Elastic volumes intégrée dans un agrégat Cloud Volumes ONTAP améliore les performances et la capacité, et permet à BlueXP d'augmenter automatiquement la capacité du disque sous-jacent selon les besoins.

La prise en charge des volumes Elastic est disponible à partir des *nouveaux* systèmes Cloud Volumes ONTAP 9.11.0 et avec les types de disques gp3 et io1 EBS.

["En savoir plus sur la prise en charge d'Elastic volumes"](#).

Notez que la prise en charge d'Elastic volumes requiert de nouvelles autorisations AWS pour le connecteur :

```
"ec2:DescribeVolumesModifications",  
"ec2:ModifyVolume",
```

Veillez à fournir ces autorisations à chaque ensemble d'identifiants AWS que vous avez ajoutés à BlueXP.

["Consultez les dernières règles de connexion pour AWS"](#).

Prise en charge du déploiement de paires haute disponibilité dans des sous-réseaux AWS partagés

Cloud Volumes ONTAP 9.11.1 inclut la prise en charge du partage VPC AWS. Cette version de Connector vous permet de déployer une paire haute disponibilité dans un sous-réseau partagé AWS lors de l'utilisation de l'API.

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

Accès limité au réseau lors de l'utilisation de terminaux de service

BlueXP limite désormais l'accès au réseau lors de l'utilisation d'un terminal de service vnet pour les connexions entre Cloud Volumes ONTAP et les comptes de stockage. BlueXP utilise un point de terminaison de service si vous désactivez les connexions Azure Private Link.

["En savoir plus sur les connexions Azure Private Link avec Cloud Volumes ONTAP".](#)

Prise en charge de la création de machines virtuelles de stockage dans Google Cloud

Cloud Volumes ONTAP est désormais pris en charge par plusieurs machines virtuelles de stockage dans Google Cloud, à partir de la version 9.11.1. Depuis cette version du connecteur, BlueXP vous permet de créer des machines virtuelles de stockage sur des paires HA Cloud Volumes ONTAP dans Google Cloud à l'aide de l'API.

La prise en charge de la création de machines virtuelles de stockage requiert de nouvelles autorisations Google Cloud pour le connecteur :

- `compute.instanceGroups.get`
- `compute.addresses.get`

Notez que vous devez utiliser l'interface de ligne de commandes ou System Manager de ONTAP pour créer une machine virtuelle de stockage sur un système à un seul nœud.

- ["En savoir plus sur les limites des machines virtuelles de stockage dans Google Cloud"](#)
- ["Découvrez comment créer des machines virtuelles de stockage destinées aux données pour Cloud Volumes ONTAP dans Google Cloud"](#)

2 mai 2022

Les modifications suivantes ont été introduites avec la version 3.9.18 du connecteur.

Cloud Volumes ONTAP 9.11.0

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.11.0.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP".](#)

Amélioration des mises à niveau des médiateurs

Lorsque BlueXP met à niveau le médiateur pour une paire HA, il confirme qu'une nouvelle image médiateur est disponible avant de supprimer le disque d'amorçage. Cette modification garantit que le médiateur peut continuer à fonctionner correctement si le processus de mise à niveau échoue.

L'onglet K8s a été supprimé

L'onglet K8s était obsolète dans une version précédente et a été supprimé. Si vous souhaitez utiliser Kubernetes avec Cloud Volumes ONTAP, vous pouvez ajouter des clusters Kubernetes gérés dans la Canvas comme environnement de travail pour une gestion avancée des données.

["En savoir plus sur la gestion des données Kubernetes dans BlueXP"](#)

Contrat annuel dans Azure

Les packages Essentials et Professional sont désormais disponibles dans Azure sous forme de contrat annuel. Contactez votre ingénieur commercial NetApp pour souscrire un contrat annuel. Le contrat est disponible sous forme d'offre privée dans Azure Marketplace.

Une fois que NetApp vous a fait part de son offre privée, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à Azure Marketplace lors de la création d'un environnement de travail.

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

Récupération instantanée S3 Glacier

Vous pouvez désormais stocker des données hiérarchisées dans la classe de stockage Amazon S3 Glacier Instant Retrieval.

["Découvrez comment changer la classe de stockage des données hiérarchisées"](#).

Nouvelles autorisations AWS requises pour le connecteur

Les autorisations suivantes sont désormais nécessaires pour créer un groupe de placement AWS SprÃ ad se trouvant dans une même zone de disponibilité lors du déploiement d'une paire haute disponibilité :

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

Ces autorisations sont désormais nécessaires pour optimiser la façon dont BlueXP crée le groupe de placement.

Veillez à fournir ces autorisations à chaque ensemble d'identifiants AWS que vous avez ajoutés à BlueXP.

["Consultez les dernières règles de connexion pour AWS"](#).

Prise en charge de la région Google Cloud

Cloud Volumes ONTAP est désormais pris en charge dans les régions Google Cloud suivantes à partir de la version 9.10.1 :

- Delhi (asie-Sud 2)
- Melbourne (australie-southeast2)
- Milan (europe-ouest 8) - nœud unique uniquement
- Santiago (southamerica-west1) - nœud unique seulement

["Consultez la liste complète des régions prises en charge par Cloud Volumes ONTAP"](#)

Prise en charge de n2-standard-16 dans Google Cloud

Le type de machine n2-standard-16 est désormais pris en charge avec Cloud Volumes ONTAP dans Google Cloud, à partir de la version 9.10.1.

["Consultez les configurations prises en charge pour Cloud Volumes ONTAP dans Google Cloud"](#)

Améliorations des politiques de pare-feu Google Cloud

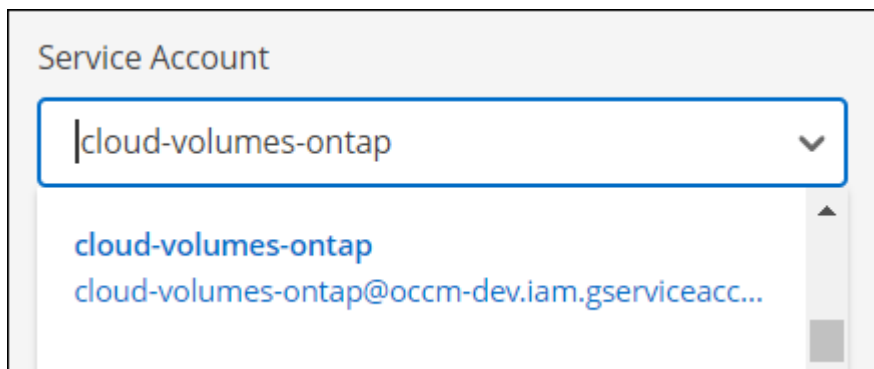
- Lorsque vous créez une paire HA Cloud Volumes ONTAP dans Google Cloud, BlueXP affichera désormais toutes les politiques de pare-feu existantes dans un VPC.

Auparavant, BlueXP n'affichera aucune règle dans les VPC-1, VPC-2 ou VPC-3 qui ne possèdent pas de balise cible.

- Lorsque vous créez un système Cloud Volumes ONTAP à nœud unique dans Google Cloud, vous pouvez désormais choisir si vous souhaitez que la stratégie de pare-feu prédéfinie autorise le trafic dans le VPC sélectionné uniquement (recommandé) ou dans tous les VPC.

Amélioration des comptes de service Google Cloud

Lorsque vous sélectionnez le compte de service Google Cloud à utiliser avec Cloud Volumes ONTAP, BlueXP affiche désormais l'adresse e-mail associée à chaque compte de service. L'affichage de l'adresse e-mail peut faciliter la distinction entre les comptes de service partageant le même nom.



3 avril 2022

Le lien vers System Manager a été supprimé

Nous avons supprimé le lien System Manager qui était auparavant disponible dans un environnement de travail Cloud Volumes ONTAP.

Vous pouvez toujours vous connecter à System Manager en entrant l'adresse IP de gestion du cluster dans un navigateur Web qui dispose d'une connexion au système Cloud Volumes ONTAP. ["En savoir plus sur la connexion à System Manager"](#).

En charge pour le stockage WORM

Maintenant que le tarif spécial d'introduction a expiré, vous serez facturé pour l'utilisation du stockage WORM. La charge est toutes les heures, selon la capacité totale provisionnée des volumes WORM. Cela s'applique aux systèmes Cloud Volumes ONTAP nouveaux et existants.

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

27 février 2022

Les modifications suivantes ont été introduites avec la version 3.9.16 du connecteur.

Assistant de volume reconçu

L'assistant Create New volume que nous avons récemment introduit est maintenant disponible lors de la création d'un volume sur un agrégat spécifique à partir de l'option **Advanced allocation**.

["Découvrez comment créer des volumes dans un agrégat spécifique"](#).

9 février 2022

Mises à jour de Marketplace

- Le pack Essentials et le pack Professional sont désormais disponibles sur tous les marchés des fournisseurs cloud.

Ces méthodes de facturation à la capacité vous permettent de payer à l'heure ou d'acheter un contrat annuel directement auprès de votre fournisseur cloud. Vous avez toujours la possibilité d'acheter une licence de capacité supplémentaire directement auprès de NetApp.

Si vous disposez déjà d'un abonnement dans Cloud Marketplace, vous êtes également automatiquement abonné à ces nouvelles offres. Vous pouvez choisir un mode de charge à la capacité lorsque vous déployez un nouvel environnement de travail Cloud Volumes ONTAP.

Si vous êtes un nouveau client, BlueXP vous invitera à vous abonner lorsque vous créez un nouvel environnement de travail.

- Les licences par nœud provenant de tous les marchés des fournisseurs cloud sont obsolètes et ne sont plus disponibles pour les nouveaux abonnés. Cela inclut les contrats annuels et les abonnements horaires (Explore, Standard et Premium).

Cette méthode de facturation est toujours disponible pour les clients existants disposant d'un abonnement actif.

["En savoir plus sur les options de licence pour Cloud Volumes ONTAP"](#).

6 février 2022

Licences Exchange non affectées

Si vous disposez d'une licence non attribuée à un nœud pour Cloud Volumes ONTAP dont vous n'avez pas utilisé de licence, vous pouvez désormais l'échanger en la convertissant en licence Cloud Backup, en licence Cloud Data Sense ou en licence Cloud Tiering.

Cette action révoque la licence Cloud Volumes ONTAP et crée une licence équivalente en dollars pour le service à la même date d'expiration.

["Découvrez comment échanger des licences de nœuds non attribuées"](#).

30 janvier 2022

Les modifications suivantes ont été introduites avec la version 3.9.15 du connecteur.

Nouvelle conception de la sélection de licences

Nous avons repensé l'écran de sélection des licences lors de la création d'un nouvel environnement de travail Cloud Volumes ONTAP. Ces modifications mettent en évidence les méthodes de facturation par capacité introduites en juillet 2021 et prennent en charge les offres à venir sur les marchés des fournisseurs de services cloud.

Mise à jour du portefeuille numérique

Nous avons mis à jour le **Portefeuille numérique** en consolidant les licences Cloud Volumes ONTAP dans un seul onglet.

2 janvier 2022

Les modifications suivantes ont été introduites avec la version 3.9.14 du connecteur.

Prise en charge de types de VM Azure supplémentaires

Cloud Volumes ONTAP est désormais pris en charge avec les types de machine virtuelle suivants dans Microsoft Azure, à partir de la version 9.10.1 :

- E4ds_v4
- E8ds_v4
- E23ds_v4
- E48ds_v4

Accédez au ["Notes de version de Cloud Volumes ONTAP"](#) pour plus d'informations sur les configurations prises en charge,

Mise à jour de la facturation FlexClone

Si vous utilisez un ["licence basée sur la capacité"](#) Pour Cloud Volumes ONTAP, vous n'êtes plus facturé pour la capacité utilisée par les volumes FlexClone.

Mode de charge désormais affiché

BlueXP montre maintenant la méthode de charge pour chaque environnement de travail Cloud Volumes ONTAP dans le panneau de droite de la toile.



Choisissez votre nom d'utilisateur

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, vous avez maintenant la possibilité d'entrer votre nom d'utilisateur préféré, au lieu du nom d'utilisateur admin par défaut.

Credentials

User Name

Password

Confirm Password

Améliorations de la création des volumes

Nous avons apporté quelques améliorations à la création des volumes :

- Nous avons repensé l'assistant de création de volumes pour en faciliter l'utilisation.
- Les balises que vous ajoutez à un volume sont désormais associées au service modèles d'applications, qui peut vous aider à organiser et simplifier la gestion de vos ressources.

- Vous pouvez désormais choisir une export policy personnalisée pour NFS.

28 novembre 2021

Les modifications suivantes ont été introduites avec la version 3.9.13 du connecteur.

Cloud Volumes ONTAP 9.10.1

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.10.1.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#).

Abonnements Keystone Flex

Vous pouvez désormais utiliser les abonnements Keystone Flex pour payer les paires haute disponibilité Cloud Volumes ONTAP.

Un abonnement Keystone Flex offre un service basé sur un abonnement avec paiement à l'utilisation. Vous bénéficiez d'une expérience de cloud hybride transparente pour les modèles de consommation des dépenses d'exploitation, de préférence en matière de CapEx ou de leasing à l'avance.

Un abonnement Keystone Flex est pris en charge avec toutes les nouvelles versions de Cloud Volumes ONTAP que vous pouvez déployer à partir de BlueXP.

- ["En savoir plus sur les abonnements Keystone Flex"](#).
- ["Découvrez comment vous lancer avec les abonnements Keystone Flex dans BlueXP"](#).

Prise en charge des nouvelles régions AWS

Le Cloud Volumes ONTAP est maintenant soutenu dans la région AWS Asie-Pacifique (Osaka) (ap-Nord-est-3).

Réduction de l'orifice

Les ports 8023 et 49000 ne sont plus ouverts sur les systèmes Cloud Volumes ONTAP dans Azure à la fois pour les systèmes à un seul nœud et les paires haute disponibilité.

Cette modification s'applique aux systèmes *New Cloud Volumes ONTAP* commençant par la version 3.9.13 du connecteur.

4 octobre 2021

Les modifications suivantes ont été introduites avec la version 3.9.11 du connecteur.

Cloud Volumes ONTAP 9.10.0

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.10.0.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#).

2 septembre 2021

Les modifications suivantes ont été introduites avec la version 3.9.10 du connecteur.

Clé de chiffrement gérée par le client dans Azure

Les données sont automatiquement chiffrées sur Cloud Volumes ONTAP dans Azure à l'aide de ["Chiffrement de service de stockage Azure"](#) Et elle est dotée d'une clé gérée par Microsoft. Mais vous pouvez désormais utiliser votre propre clé de chiffrement gérée par le client en procédant comme suit :

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

["En savoir plus sur ces étapes"](#).

7 juillet 2021

Les modifications suivantes ont été introduites avec la version 3.9.8 du connecteur.

Nouvelles méthodes de charge

De nouvelles méthodes de charge sont disponibles pour Cloud Volumes ONTAP.

- **BYOL** basée sur la capacité : une licence basée sur la capacité vous permet de payer pour Cloud Volumes ONTAP par To de capacité. La licence est associée à votre compte NetApp et vous permet de créer plusieurs systèmes Cloud Volumes ONTAP, tant que la capacité disponible par le biais de votre licence est suffisante. Une licence basée sur la capacité est disponible sous la forme d'un package, soit *Essentials* soit *Professional*.
- **Offre Freemium** : Freemium vous permet d'utiliser toutes les fonctionnalités Cloud Volumes ONTAP gratuitement auprès de NetApp (les fournisseurs de cloud sont toujours facturés). Vous êtes limité à 500 Gio de capacité provisionnée par système, et il n'existe pas de contrat de support. Vous pouvez avoir jusqu'à 10 systèmes Freemium.

["En savoir plus sur ces options de licence"](#).

Voici un exemple des méthodes de charge que vous pouvez choisir :

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

☐ Pay-As-You-Go by the hour

☒ Bring your own license

Bring your own license type

Capacity-Based

Package

Professional

☐ Freemium (Up to 500GB)

Stockage WORM disponible pour une utilisation générale

Le stockage WORM (Write Once, Read Many) n'est plus inclus dans la version Aperçu et peut désormais être utilisé de manière générale avec Cloud Volumes ONTAP. ["En savoir plus sur le stockage WORM"](#).

Prise en charge de m5dn.24xgrand dans AWS

Depuis la version 9.9.1, Cloud Volumes ONTAP prend désormais en charge le type d'instance m5dn.24xgrand avec les méthodes de chargement suivantes : PAYGO Premium, apportez votre propre licence (BYOL) et Freemium.

["Affichez les configurations prises en charge pour Cloud Volumes ONTAP dans AWS"](#).

Sélectionnez des groupes de ressources Azure existants

Lors de la création d'un système Cloud Volumes ONTAP dans Azure, vous avez maintenant la possibilité de sélectionner un groupe de ressources existant pour la machine virtuelle et ses ressources associées.

Location & Connectivity

Location

Azure Region
WEST US

Availability Zone (Optional)
Select an Availability Zone

Connectivity

Resource Group

☐ Create a new group ☒ Use an existing group

Resource Group Name
RG1

Les autorisations suivantes permettent à BlueXP de supprimer des ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec ou de suppression du déploiement :

```
"Microsoft.Network/privateEndpoints/delete",  
"Microsoft.Compute/availabilitySets/delete",
```

Veillez à fournir ces autorisations à chaque ensemble d'identifiants Azure que vous avez ajoutés à BlueXP. ["Découvrez la dernière règle de connecteurs pour Azure"](#).

L'accès public BLOB est désormais désactivé dans Azure

En tant qu'amélioration de la sécurité, BlueXP désactive maintenant **Blob public Access** lors de la création d'un compte de stockage pour Cloud Volumes ONTAP.

Amélioration d'Azure Private Link

Par défaut, BlueXP active désormais une connexion Azure Private Link sur le compte de stockage de diagnostic de démarrage pour les nouveaux systèmes Cloud Volumes ONTAP.

Cela signifie que les comptes de *All* stockage de Cloud Volumes ONTAP utiliseront désormais une liaison privée.

["En savoir plus sur l'utilisation d'un lien privé Azure avec Cloud Volumes ONTAP"](#).

Des disques persistants équilibrés dans Google Cloud

Depuis la version 9.9.1, Cloud Volumes ONTAP prend désormais en charge des disques persistants équilibrés (pd-équilibré).

Ces disques SSD permettent d'équilibrer les performances et les coûts grâce à une réduction des IOPS par Gio.

Custom-4-16384 n'est plus pris en charge par Google Cloud

Le type de machine Custom-4-16384 n'est plus pris en charge par les nouveaux systèmes Cloud Volumes ONTAP.

Si vous disposez d'un système existant fonctionnant sur ce type de machine, vous pouvez continuer à l'utiliser, mais nous vous recommandons de passer au type de machine n2-standard-4.

["Affichez les configurations prises en charge pour Cloud Volumes ONTAP dans GCP".](#)

30 mai 2021

Les modifications suivantes ont été introduites avec la version 3.9.7 du connecteur.

Nouveau pack professionnel dans AWS

Un nouveau pack professionnel permet d'être bundle Cloud Volumes ONTAP et Cloud Backup Service à l'aide d'un contrat annuel provenant d'AWS Marketplace. Le paiement est par Tio. Cet abonnement ne permet pas de sauvegarder les données sur site.

Si vous optez pour cette option de paiement, vous pouvez provisionner jusqu'à 2 Pio par système Cloud Volumes ONTAP via des disques EBS et effectuer le Tiering sur le stockage objet S3 (nœud unique ou HA).

Accédez au ["Page AWS Marketplace"](#) pour consulter les détails des prix et consulter le ["Notes de version de Cloud Volumes ONTAP"](#) pour en savoir plus sur cette option de licence.

Balises sur les volumes EBS dans AWS

BlueXP ajoute désormais des balises aux volumes EBS lorsqu'il crée un nouvel environnement de travail Cloud Volumes ONTAP. Les balises étaient préalablement créées après le déploiement de Cloud Volumes ONTAP.

Ce changement peut aider si votre organisation utilise des stratégies de contrôle de service (SCPS) pour gérer les autorisations.

Période de refroidissement minimale pour la règle de hiérarchisation automatique

Si vous avez activé le Tiering des données sur un volume à l'aide de la règle *auto* Tiering, vous pouvez désormais ajuster la période de refroidissement minimale à l'aide de l'API.

["Apprenez à régler la période de refroidissement minimum."](#)

Amélioration des règles d'exportation personnalisées

Lorsque vous créez un nouveau volume NFS, BlueXP affiche désormais les règles d'exportation personnalisées dans l'ordre croissant, ce qui facilite la recherche de la stratégie d'exportation dont vous avez besoin.

Suppression d'anciennes copies Snapshot cloud

BlueXP supprime désormais les anciens snapshots cloud des disques racine et de démarrage créés lorsqu'un système Cloud Volumes ONTAP est déployé et à chaque mise hors tension. Seuls les deux instantanés les plus récents sont conservés pour les volumes racine et de démarrage.

Cette amélioration contribue à réduire les coûts des fournisseurs de cloud en supprimant les snapshots qui ne sont plus nécessaires.

Notez qu'un connecteur requiert une nouvelle autorisation pour supprimer les snapshots Azure. ["Découvrez la dernière règle de connecteurs pour Azure"](#).

"Microsoft.Compute/snapshots/delete"

24 mai 2021

Cloud Volumes ONTAP 9.9.1

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.9.1.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#).

11 avril 2021

Les modifications suivantes ont été introduites avec la version 3.9.5 du connecteur.

Génération de rapports sur l'espace logique

BlueXP permet désormais de générer des rapports d'espace logique sur la machine virtuelle de stockage initiale qu'elle crée pour Cloud Volumes ONTAP.

Lorsqu'un espace est indiqué de manière logique, ONTAP indique l'espace volume afin que toutes les fonctionnalités d'efficacité du stockage soient également signalées comme utilisées.

Prise en charge des disques gp3 dans AWS

Cloud Volumes ONTAP prend désormais en charge les disques SSD *General Purpose SSD (gp3)*, en commençant par la version 9.7. Les disques gp3 sont les disques SSD les plus économiques qui permettent d'équilibrer les coûts et les performances pour un large éventail de charges de travail.

["En savoir plus sur l'utilisation de disques gp3 avec Cloud Volumes ONTAP"](#).

Les disques durs inactifs ne sont plus pris en charge par AWS

Cloud Volumes ONTAP ne prend plus en charge les disques durs à froid (sc1).

TLS 1.2 pour les comptes de stockage Azure

Lorsque BlueXP crée des comptes de stockage dans Azure pour Cloud Volumes ONTAP, la version TLS du compte de stockage est maintenant la version 1.2.

8 mars 2021

Les modifications suivantes ont été introduites avec la version 3.9.4 du connecteur.

Cloud Volumes ONTAP 9.9.0

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.9.0.

["Découvrez les nouvelles fonctionnalités de cette version d'Cloud Volumes ONTAP"](#).

Prise en charge de l'environnement C2S AWS

Vous pouvez désormais déployer Cloud Volumes ONTAP 9.8 dans l'environnement C2S (AWS commercial Cloud Services).

["Découvrez comment démarrer dans C2S".](#)

Chiffrement AWS avec des CMK gérés par le client

BlueXP vous a toujours permis de chiffrer les données Cloud Volumes ONTAP à l'aide du service AWS Key Management Service (KMS). Depuis Cloud Volumes ONTAP 9.9.0, les données stockées sur des disques EBS et envoyées vers S3 sont chiffrées si vous sélectionnez une CMK gérée par le client. Auparavant, seules les données EBS étaient chiffrées.

Notez que vous devrez fournir le rôle IAM Cloud Volumes ONTAP pour utiliser le CMK.

["En savoir plus sur la configuration du KMS AWS avec Cloud Volumes ONTAP".](#)

Prise en charge d'Azure DoD

Vous pouvez désormais déployer Cloud Volumes ONTAP 9.8 dans le service Azure Department of Defense (DoD) impact Level 6 (IL6).

Réduction des adresses IP dans Google Cloud

Nous avons réduit le nombre d'adresses IP requises pour Cloud Volumes ONTAP 9.8 et versions ultérieures dans Google Cloud. Par défaut, une adresse IP moins est requise (nous unifiées le LIF intercluster avec le LIF node management). Vous pouvez également ignorer la création de la LIF de gestion du SVM lors de l'utilisation de l'API, qui réduit la nécessité d'une adresse IP supplémentaire.

["Pour en savoir plus sur les exigences d'adresse IP, consultez Google Cloud".](#)

Prise en charge partagée des VPC dans Google Cloud

Lorsque vous déployez une paire haute disponibilité Cloud Volumes ONTAP dans Google Cloud, vous pouvez désormais choisir des VPC-1, VPC-2 et VPC-3. Auparavant, seul le VPC-0 peut être un VPC partagé. Cette modification est prise en charge par Cloud Volumes ONTAP 9.8 et versions ultérieures.

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

4 janvier 2021

Les modifications suivantes ont été introduites avec la version 3.9.2 du connecteur.

Sur AWS

Il y a quelques mois, nous avons annoncé que Cloud Volumes ONTAP avait obtenu le titre de partenaire prêt pour Amazon Web Services (AWS). Nous avons le plaisir de vous annoncer que nous avons validé les publications BlueXP et Cloud Volumes ONTAP avec 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

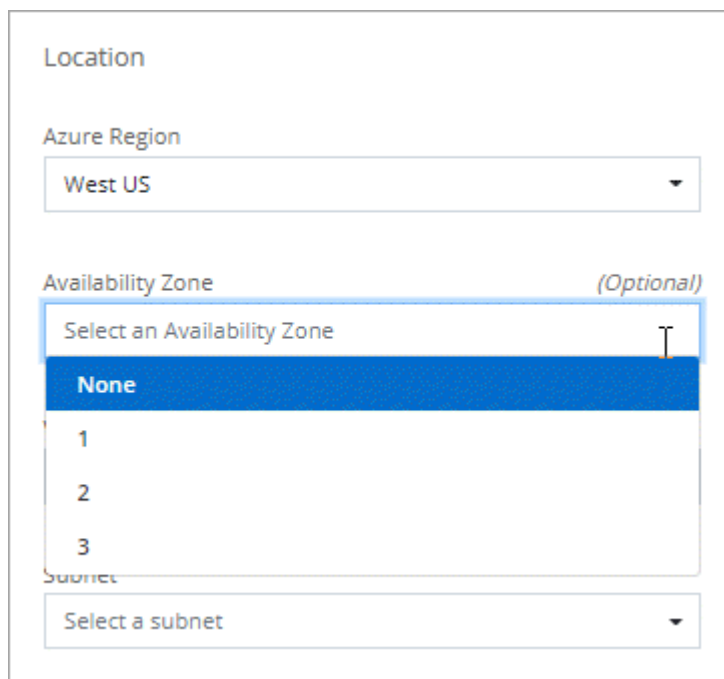
VNVRAM Ultra SSD dans les régions Azure prises en charge

Cloud Volumes ONTAP peut maintenant utiliser un disque SSD Ultra en tant que VNVRAM lorsque vous utilisez le type de machine virtuelle E32S_v3 avec un système à un seul nœud ["Dans toutes les régions Azure prises en charge"](#).

VNVRAM offre de meilleures performances en écriture.

Choisissez une zone de disponibilité dans Azure

Vous pouvez désormais choisir la zone de disponibilité dans laquelle vous souhaitez déployer un système Cloud Volumes ONTAP à un seul nœud. Si vous ne sélectionnez pas d'AZ, BlueXP en sélectionne une pour vous.



The screenshot shows a configuration window for Azure. Under the 'Location' section, 'Azure Region' is set to 'West US'. Below it, 'Availability Zone' is marked as '(Optional)' and has a dropdown menu open. The dropdown shows 'None' as the selected option, with '1', '2', and '3' as other available options. At the bottom, there is a 'Subnet' dropdown set to 'Select a subnet'.

Des disques de plus grande taille dans Google Cloud

Cloud Volumes ONTAP prend désormais en charge les disques de 64 To dans GCP.



La capacité système maximale avec les disques seuls reste à 256 To en raison des limites GCP.

Nouveaux types de machines dans Google Cloud

Cloud Volumes ONTAP prend désormais en charge les types de machine suivants :

- n2-standard-4 avec la licence Explore et avec BYOL

- n2-standard-8 avec licence Standard et BYOL
- n2-standard-32 avec licence Premium et BYOL

3 novembre 2020

Les modifications suivantes ont été introduites avec la version 3.9.0 du connecteur.

Lien privé Azure pour Cloud Volumes ONTAP

Par défaut, BlueXP autorise désormais une connexion Azure Private Link entre Cloud Volumes ONTAP et ses comptes de stockage associés. Une liaison privée sécurise les connexions entre les terminaux dans Azure.

- ["En savoir plus sur les liens privés Azure"](#)
- ["En savoir plus sur l'utilisation d'un lien privé Azure avec Cloud Volumes ONTAP"](#)

Limites connues

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Ces limitations sont spécifiques à la gestion de Cloud Volumes ONTAP dans BlueXP (anciennement Cloud Manager). Pour afficher les limites avec le logiciel Cloud Volumes ONTAP lui-même, ["Accédez aux notes de version de Cloud Volumes ONTAP"](#)

BlueXP ne prend pas en charge les volumes FlexGroup

Bien que Cloud Volumes ONTAP prenne en charge les volumes FlexGroup, BlueXP ne le fait pas. Si vous créez un volume FlexGroup à partir de System Manager ou de l'interface de ligne de commande, définissez le mode gestion de la capacité de BlueXP sur Manuel. Le mode automatique peut ne pas fonctionner correctement avec les volumes FlexGroup.

BlueXP ne prend pas en charge S3 avec Cloud Volumes ONTAP

Dans certains fournisseurs cloud, Cloud Volumes ONTAP prend en charge S3 en tant qu'option de stockage scale-out, mais BlueXP n'offre pas de fonctionnalités de gestion pour cette fonctionnalité. Il est recommandé d'utiliser l'interface de ligne de commandes pour configurer l'accès des clients S3 à partir d'Cloud Volumes ONTAP. Pour plus de détails, reportez-vous à la ["Guide de l'alimentation de la configuration S3"](#).

["En savoir plus sur la prise en charge de Cloud Volumes ONTAP pour S3 et d'autres protocoles client"](#).

BlueXP ne prend pas en charge la reprise après incident pour les machines virtuelles de stockage

BlueXP ne propose pas de prise en charge de la configuration ou de l'orchestration pour la reprise après incident des machines virtuelles de stockage. Vous devez utiliser System Manager ou l'interface de ligne de commandes.

- ["Guide de préparation rapide pour la reprise après incident du SVM"](#)
- ["Guide de reprise après incident de SVM Express"](#)

Notes de version de Cloud Volumes ONTAP

Les notes de version de Cloud Volumes ONTAP fournissent des informations spécifiques à la version. Nouveautés de la version, configurations prises en charge, limites de stockage et limitations ou problèmes connus susceptibles d'affecter le fonctionnement du produit.

["Accédez aux notes de version de Cloud Volumes ONTAP"](#)

Commencez

Découvrez Cloud Volumes ONTAP

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

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

- Fonctionnalités d'efficacité du stockage

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

- Haute disponibilité

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

- Protection des données

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

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

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

- Tiering des données

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

- La cohérence des applications

Cohérence des copies NetApp Snapshot avec NetApp SnapCenter

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

- Sécurité des données

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

- Contrôles de conformité à la confidentialité

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

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



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

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

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

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"](#).

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

2

Planification de la configuration

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

3

Configurez votre réseau

1. Vérifiez que votre VPC et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du VPC cible de sorte que le connecteur et le Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

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

3. Configurez un terminal VPC sur le service S3.

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

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

4

Configuration du KMS AWS

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

>>".

5

Lancez Cloud Volumes ONTAP avec BlueXP

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

Liens connexes

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

Planification de votre configuration Cloud Volumes ONTAP dans AWS

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

Choisissez une licence Cloud Volumes ONTAP

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

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

Choisissez une région prise en charge

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

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

Choisissez une instance prise en charge

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

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

Compréhension des limites de stockage

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

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

Dimensionnez votre système dans AWS

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

Type d'instance

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

Type de disque EBS

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

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

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

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

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

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

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



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

Taille des disques EBS

Si vous choisissez une configuration qui ne prend pas en charge le ["Fonctionnalité Amazon EBS Elastic](#)

volumes", Puis vous devez choisir une taille de disque initiale lorsque vous lancez un système Cloud Volumes ONTAP. Après cela, vous pouvez ["Laissez BlueXP gérer la capacité d'un système pour vous"](#), mais si vous voulez ["créez des agrégats vous-même"](#), soyez conscient des éléments suivants :

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

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

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

Afficher les disques système par défaut

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

["Afficher les disques par défaut des données système Cloud Volumes ONTAP dans AWS"](#).



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

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

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

Quelques limites peuvent être 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 | |
| Adresse IP flottante pour les données du nœud 2 | |
| Tables de routage pour les adresses IP flottantes | |

Choisissez une vitesse d'écriture

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

Choisissez un profil d'utilisation du volume

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

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

Provisionnement fin

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

Déduplication

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

Compression

Réduit la capacité physique requise pour stocker les données en les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

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

Exigences générales

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

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

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

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

Si vous disposez d'une instance NAT, vous devez définir une règle de groupe de sécurité entrante qui autorise le trafic HTTPS du sous-réseau privé vers Internet.

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

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

Si vous avez défini des règles sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

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

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

Accès Internet sortant pour le médiateur haute disponibilité

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

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

Adresses IP privées

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

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

Adresses IP d'un système à un seul nœud

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

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

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

Adresses IP des paires haute disponibilité

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



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

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

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

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

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

LIF pour paires haute disponibilité dans plusieurs systèmes AZS

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



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

Groupes de sécurité

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

Connexion pour le Tiering des données

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

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

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

Connexions aux systèmes ONTAP

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

DNS et Active Directory pour CIFS

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

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

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

Partage de VPC

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

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

Besoins en paires haute disponibilité dans plusieurs AZS

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

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

Zones de disponibilité

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

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

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

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

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



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

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

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

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

AWS region



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

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

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

Tables de routage

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

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

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

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

Connexion aux outils de gestion NetApp

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

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

Exemple de configuration haute disponibilité

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



Configuration requise pour le connecteur

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

Connexion aux réseaux cibles

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

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

Accès Internet sortant

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

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

Serveur proxy

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

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

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

Limitation de l'adresse IP

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

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

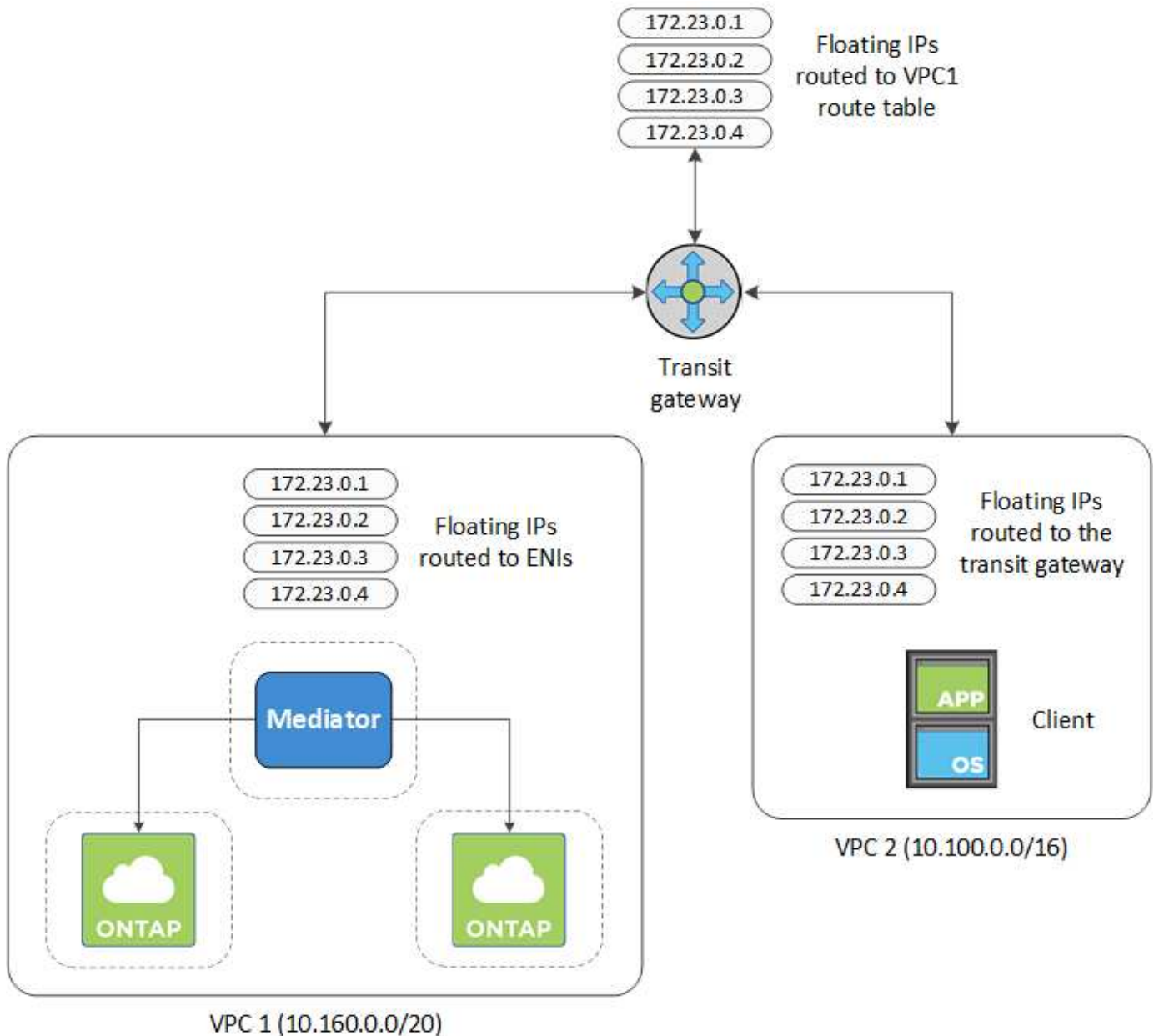
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA ["Adresses IP flottantes"](#) Depuis l'extérieur du VPC, où réside la paire HA.

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

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

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

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



Les étapes suivantes montrent comment configurer une configuration similaire.

Étapes

1. "Créez une passerelle de transit et connectez les VPC à la passerelle".
2. Associez les VPC à la table de routage de la passerelle de transit.

- 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 | Floating IP | static | active |
| <input type="checkbox"/> | 172.23.0.3/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |
| <input type="checkbox"/> | 172.23.0.4/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |

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

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

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

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

VPC1
Floating IP
Addresses

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

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

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

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

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

VPC2
Floating
act IP
Addresses

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

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

Volumes

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



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

["Découvrez comment modifier un volume"](#).

- Liens connexes*
- ["Paires haute disponibilité dans AWS"](#)
- ["Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"](#)

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

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

Avec ["Partage de VPC"](#), Une configuration Cloud Volumes ONTAP HA est répartie sur deux comptes :

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

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

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



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

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

Étapes

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

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

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

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

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

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

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

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

Notez que vous devez spécifier les champs suivants :

- « SecurityGroupIId »

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

- "AssumeRoleArn" dans l'objet "haParams"

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

Par exemple :

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

+

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

Règles de groupe de sécurité pour AWS

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

Règles pour Cloud Volumes ONTAP

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

Règles entrantes

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

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

| Protocole | Port | Objectif |
|--------------------------|---------|--|
| Tous les protocoles ICMP | Tout | Envoi d'une requête ping à l'instance |
| HTTP | 80 | Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster |
| HTTPS | 443 | Connectivité avec le connecteur et l'accès HTTPS à la console Web System Manager via l'adresse IP du LIF de cluster management |
| SSH | 22 | Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud |
| TCP | 111 | Appel de procédure à distance pour NFS |
| TCP | 139 | Session de service NetBIOS pour CIFS |
| TCP | 161-162 | Protocole de gestion de réseau simple |
| TCP | 445 | Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS |
| TCP | 658 | Montage NFS |
| TCP | 749 | Kerberos |
| TCP | 2049 | Démon du serveur NFS |
| TCP | 3260 | Accès iSCSI via le LIF de données iSCSI |
| TCP | 4045 | Démon de verrouillage NFS |
| TCP | 4046 | Surveillance de l'état du réseau pour NFS |
| TCP | 10000 | Sauvegarde avec NDMP |
| TCP | 11104 | Gestion des sessions de communication intercluster pour SnapMirror |
| TCP | 11105 | Transfert de données SnapMirror à l'aide de LIF intercluster |
| UDP | 111 | Appel de procédure à distance pour NFS |
| UDP | 161-162 | Protocole de gestion de réseau simple |
| UDP | 658 | Montage NFS |
| UDP | 2049 | Démon du serveur NFS |

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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



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

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

| Service | Protocole | Port | Source | Destination | Objectif |
|--------------------|----------------|----------------|--|--|--|
| AutoSupport | HTTPS | 443 | FRV de gestion des nœuds | support.netapp.com | AutoSupport (HTTPS est le protocole par défaut) |
| | HTTP | 80 | FRV de gestion des nœuds | support.netapp.com | AutoSupport (uniquement si le protocole de transport est passé de HTTPS à HTTP) |
| | TCP | 3128 | FRV de gestion des nœuds | Connecteur | Envoi de messages AutoSupport via un serveur proxy sur le connecteur, si aucune connexion Internet sortante n'est disponible |
| Sauvegarde vers S3 | TCP | 5010 | FRV InterCluster | Sauvegarder le terminal ou restaurer le terminal | Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3 |
| Cluster | Tout le trafic | Tout le trafic | Tous les LIF sur un nœud | Tous les LIF de l'autre nœud | Communications InterCluster (Cloud Volumes ONTAP HA uniquement) |
| | TCP | 3000 | FRV de gestion des nœuds | Ha médiateur | Appels ZAPI (Cloud Volumes ONTAP HA uniquement) |
| | ICMP | 1 | FRV de gestion des nœuds | Ha médiateur | Rester en vie (Cloud Volumes ONTAP HA uniquement) |
| DHCP | UDP | 68 | FRV de gestion des nœuds | DHCP | Client DHCP pour la première configuration |
| DHCPs | UDP | 67 | FRV de gestion des nœuds | DHCP | Serveur DHCP |
| DNS | UDP | 53 | FRV de gestion des nœuds et FRV de données (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 1860-1869 | FRV de gestion des nœuds | Serveurs de destination | Copie NDMP |
| SMTP | TCP | 25 | FRV de gestion des nœuds | Serveur de messagerie | Les alertes SMTP peuvent être utilisées pour AutoSupport |
| SNMP | TCP | 161 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | UDP | 161 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | TCP | 162 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | UDP | 162 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |

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

Règles pour le groupe de sécurité externe du médiateur de haute disponibilité

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

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

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

Règles de sortie

Le groupe de sécurité prédéfini du médiateur HA ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le médiateur haute disponibilité.

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

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



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

Règles du groupe de sécurité interne de la configuration haute disponibilité

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

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

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

Règles de sortie

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

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

Règles pour le connecteur

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

Règles entrantes

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

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



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

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

Configuration du système AWS KMS

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

Étapes

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

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

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

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

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

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

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

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

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

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



Other AWS accounts

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

arn:aws:iam::

Enter the ID of another AWS accou

:root

Remove

Add another AWS account

Cancel

Save changes

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

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


```

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

```

+

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

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

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

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

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

Configurer les rôles IAM pour Cloud Volumes ONTAP

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

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



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

Étapes

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

Régions standard

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

GovCloud (USA)

```

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

```

Environnement C2S

```

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

```

- Règle de sauvegarde pour les nœuds Cloud Volumes ONTAP

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

Régions standard

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

GovCloud (USA)

```

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

```

Environnement C2S

```

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

```

- Ha médiateur


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

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

Résultat

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

Plus d'informations

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

Configuration des licences pour Cloud Volumes ONTAP dans AWS

Après avoir décidé de l'option de licence que vous souhaitez utiliser avec Cloud Volumes ONTAP, quelques étapes sont nécessaires avant de pouvoir choisir cette option de licence lors de la création d'un nouvel environnement de travail.

Frémium

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

Étapes

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

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

Edit Credentials & Add Subscription

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

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

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

The next steps:

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

Continue

Cancel

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

Select Charging Method

☐ Professional

By capacity

▼

☐ Essential

By capacity

▼

☒ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

Licence basée sur la capacité

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

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

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

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

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

BYOL

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

Étapes

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

BlueXP interroge automatiquement le service des licences NetApp pour obtenir des informations sur les licences associées à votre compte sur le site de support NetApp. En l'absence d'erreurs, BlueXP ajoute automatiquement les licences au porte-monnaie numérique.

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

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

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

Edit Credentials & Add Subscription

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

☐ Pay-Per-TiB - Annual Contract

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

☒ Pay-as-you-go

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

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

2 Cloud Manager

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

Continue

Cancel

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

Select Charging Method

| | | |
|--|-------------|---|
| <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

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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



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

Contrat annuel

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

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

Étapes

1. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner au contrat annuel sur AWS Marketplace.

Edit Credentials & Add Subscription

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

☒ **Pay-Per-TiB - Annual Contract**

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

☐ **Pay-as-you-go**

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

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

2 Cloud Manager

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

Continue

Cancel

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

Select Charging Method

☒ **Professional**

By capacity



☐ **Essential**

By capacity



☐ **Freemium (Up to 500 GiB)**

By capacity



☐ **Per Node**

By node



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

Abonnement Keystone Flex

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

Étapes

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

Select Charging Method

☒ **Keystone** By capacity

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐ Professional By capacity

☐ Essential By capacity

☐ Freemium (Up to 500 GiB) By capacity

☐ Per Node By node

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

Lancement d'Cloud Volumes ONTAP dans AWS

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

Avant de commencer

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

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

Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir ["Planification de votre configuration Cloud Volumes ONTAP"](#).

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

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

- DNS et Active Directory pour les configurations CIFS.

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

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

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

Description de la tâche

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
4. Si vous y êtes invité, ["Créer un connecteur"](#).
5. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

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

| Champ | Description |
|--|--|
| Nom de l'environnement de travail | BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option. |
| Ajouter des étiquettes | Les étiquettes AWS sont des métadonnées pour vos ressources AWS. BlueXP ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation AWS : balisage des ressources Amazon EC2 ". |
| Nom d'utilisateur et mot de passe | Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé. |
| Modifier les informations d'identification | Sélectionnez les identifiants AWS associés au compte sur lequel vous souhaitez déployer le système. Vous pouvez également associer l'abonnement AWS Marketplace à ce système Cloud Volumes ONTAP. Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un nouvel abonnement AWS Marketplace. L'abonnement peut s'agir d'un contrat annuel ou d'un paiement pour Cloud Volumes ONTAP à l'heure. https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html ["Découvrez comment ajouter des identifiants AWS à BlueXP"^]. |

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

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

(video)

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



Cloud Manager (for Cloud Volumes ONTAP)

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

**Having issues signing up for your product?**

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

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

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

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

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

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

| Champ | Description |
|---|--|
| VPC | Si vous disposez d'un poste externe AWS, vous pouvez déployer un système Cloud Volumes ONTAP à un seul nœud dans cet envoi en sélectionnant le VPC Outpost. L'expérience est la même que tout autre VPC qui réside dans AWS. |
| Groupe de sécurité généré | Si vous laissez BlueXP générer le groupe de sécurité pour vous, vous devez choisir comment vous autorisez le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, la source du trafic entrant correspond à la plage de sous-réseau du VPC sélectionné et à la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VPC, la source du trafic entrant est la plage IP 0.0.0.0/0. |
| Utiliser un groupe de sécurité existant | Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" . |

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

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

compte ou un autre compte AWS.



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

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

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

9. **Méthodes de chargement et compte NSS** : spécifiez l'option de chargement à utiliser avec ce système, puis spécifiez un compte sur le site de support NetApp.
 - ["Découvrez les options de licence pour Cloud Volumes ONTAP".](#)
 - ["Découvrez comment configurer les licences".](#)

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

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

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

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

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

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

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



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

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

Notez ce qui suit :

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

[AWS](#)".

- Si vous choisissez un disque gp2 ou st1, vous pouvez sélectionner une taille de disque pour tous les disques de l'agrégat initial et pour les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.
- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

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

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

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

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

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

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

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

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

| Champ | Description |
|--|---|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau. |
| Autorisations et utilisateurs/groupes (pour CIFS uniquement) | Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur. |
| Stratégie Snapshot | Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server. |
| Options avancées (pour NFS uniquement) | Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4. |

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

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

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

| Champ | Description |
|---|---|
| Adresse IP principale et secondaire DNS | Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. |
| Domaine Active Directory à rejoindre | Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS. |
| Informations d'identification autorisées à rejoindre le domaine | Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD. |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |

| Champ | Description |
|-------------------------|---|
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs,ou=corp dans ce champ. |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la " Documents d'automatisation BlueXP " pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS. |

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

Pour plus d'informations, voir "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

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

Résultat

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

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

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

Une fois que vous avez terminé

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

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

Lancement d'une paire Cloud Volumes ONTAP HA dans AWS

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

Restriction

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

Description de la tâche

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP HA**.
4. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

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

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

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

vos identifiants AWS :

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

(video)



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

Cloud Manager (for Cloud Volumes ONTAP)

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

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

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

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

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

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

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

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

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

| Champ | Description |
|---|--|
| Groupe de sécurité généré | Si vous laissez BlueXP générer le groupe de sécurité pour vous, vous devez choisir comment vous autorisez le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, la source du trafic entrant correspond à la plage de sous-réseau du VPC sélectionné et à la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VPC, la source du trafic entrant est la plage IP 0.0.0.0/0. |
| Utiliser un groupe de sécurité existant | Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" . |

8. **Connectivité et authentification SSH** : choisissez des méthodes de connexion pour la paire HA et le médiateur.

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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



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

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

Notez ce qui suit :

- Le type de disque est pour le volume initial (et l'agrégat). Vous pouvez choisir un autre type de disque pour les volumes suivants (et les agrégats).
- Si vous choisissez un disque gp3 ou io1, BlueXP utilise la fonctionnalité Elastic volumes d'AWS pour augmenter automatiquement la capacité des disques de stockage sous-jacents selon les besoins. Après le déploiement de Cloud Volumes ONTAP, vous pouvez choisir la capacité initiale en fonction de vos besoins en stockage, puis la réviser. ["En savoir plus sur la prise en charge d'Elastic volumes dans AWS"](#).
- Si vous choisissez un disque gp2 ou st1, vous pouvez sélectionner une taille de disque pour tous les disques de l'agrégat initial et pour les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.
- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

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

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

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

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

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

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

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

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

| Champ | Description |
|--|--|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau. |

| Champ | Description |
|--|---|
| Autorisations et utilisateurs/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

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS **CIFS** iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

| Champ | Description |
|---|---|
| Adresse IP principale et secondaire DNS | Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. |
| Domaine Active Directory à rejoindre | Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS. |
| Informations d'identification autorisées à rejoindre le domaine | Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD. |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs,ou=corp dans ce champ. |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Documents d'automatisation BlueXP" pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS. |

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

Pour plus d'informations, voir ["Présentation des profils d'utilisation des volumes"](#) et ["Vue d'ensemble du hiérarchisation des données"](#).

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

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

Résultat

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

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

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

Une fois que vous avez terminé

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

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

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

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

Versions prises en charge dans C2S

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

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



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

Fonctions prises en charge dans C2S

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

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

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

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

Limites

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

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

Présentation du déploiement

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

1. Préparation de votre environnement AWS

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

2. Installation du connecteur et configuration de Cloud Manager

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

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

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

Chacune de ces étapes est décrite ci-dessous.

Préparation de votre environnement AWS

Votre environnement AWS doit répondre à quelques exigences.

Configurez votre réseau

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

Étapes

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

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

Abonnez-vous à Cloud Volumes ONTAP

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

Étapes

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

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

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

Configurez les autorisations

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

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

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

Étapes

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

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

```

```

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

```

```

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

```

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

```

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

```

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

```

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

```

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

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

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

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

Configuration du KMS AWS

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

Étapes

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

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

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

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

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

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

Installation du connecteur et configuration de Cloud Manager

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

Étapes

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

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

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

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

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

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

Lancement de Cloud Volumes ONTAP à partir de Cloud Manager

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

Ce dont vous avez besoin

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

Étapes

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

Notez les éléments suivants lorsque vous terminez l'assistant :

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

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

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

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

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

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

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



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

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

Résultat

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

Règles de groupe de sécurité

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

Groupe de sécurité du connecteur

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

Règles entrantes

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

Règles de sortie

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

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

Groupe de sécurité pour Cloud Volumes ONTAP

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

Règles entrantes

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

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

| Protocole | Port | Objectif |
|--------------------------|------|---|
| Tous les protocoles ICMP | Tout | Envoi d'une requête ping à l'instance |
| HTTP | 80 | Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster |
| HTTPS | 443 | Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster |

| Protocole | Port | Objectif |
|-----------|---------|--|
| SSH | 22 | Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud |
| TCP | 111 | Appel de procédure à distance pour NFS |
| TCP | 139 | Session de service NetBIOS pour CIFS |
| TCP | 161-162 | Protocole de gestion de réseau simple |
| TCP | 445 | Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS |
| TCP | 658 | Montage NFS |
| TCP | 749 | Kerberos |
| TCP | 2049 | Démon du serveur NFS |
| TCP | 3260 | Accès iSCSI via le LIF de données iSCSI |
| TCP | 4045 | Démon de verrouillage NFS |
| TCP | 4046 | Surveillance de l'état du réseau pour NFS |
| TCP | 10000 | Sauvegarde avec NDMP |
| TCP | 11104 | Gestion des sessions de communication intercluster pour SnapMirror |
| TCP | 11105 | Transfert de données SnapMirror à l'aide de LIF intercluster |
| UDP | 111 | Appel de procédure à distance pour NFS |
| UDP | 161-162 | Protocole de gestion de réseau simple |
| UDP | 658 | Montage NFS |
| UDP | 2049 | Démon du serveur NFS |
| UDP | 4045 | Démon de verrouillage NFS |
| UDP | 4046 | Surveillance de l'état du réseau pour NFS |
| UDP | 4049 | Protocole NFS rquotad |

Règles de sortie

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

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

Groupe de sécurité externe pour le médiateur HA

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

entrantes et sortantes suivantes.

Règles entrantes

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

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

Règles de sortie

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

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

Groupe de sécurité interne du médiateur HA

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

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

Règles de sortie

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

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

Commencez avec Microsoft Azure

Démarrage rapide de Cloud Volumes ONTAP dans Azure

Découvrez Cloud Volumes ONTAP pour Azure en quelques étapes.

1

Créer un connecteur

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

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

2

Planification de la configuration

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

3

Configurez votre réseau

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

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

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

4

Lancez Cloud Volumes ONTAP avec BlueXP

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

Liens connexes

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

Planification de votre configuration Cloud Volumes ONTAP dans Azure

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

Choisissez une licence Cloud Volumes ONTAP

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

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

Choisissez une région prise en charge

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

Choisissez un type de machine virtuelle pris en charge

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

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

Compréhension des limites de stockage

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

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

Dimensionnez votre système en Azure

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

Type de machine virtuelle

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

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

Type de disque Azure avec des systèmes à un seul nœud

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

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

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

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

Type de disque Azure avec paires haute disponibilité

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

Taille des disques Azure

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



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

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

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

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

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

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

Afficher les disques système par défaut

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

["Afficher les disques par défaut des données système Cloud Volumes ONTAP dans Azure"](#).



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

Collecte d'informations de mise en réseau

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

| Informations sur Azure | Votre valeur |
|--|--------------|
| Région | |
| Réseau virtuel (vnet) | |
| Sous-réseau | |
| Groupe de sécurité réseau (s'il s'agit du vôtre) | |

Choisissez une vitesse d'écriture

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

Choisissez un profil d'utilisation du volume

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

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

Provisionnement fin

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

Déduplication

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

Compression

Réduit la capacité physique requise pour stocker les données en les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Configuration réseau requise pour Cloud Volumes ONTAP dans Azure

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

Conditions requises pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être satisfaites dans Azure.

Accès Internet sortant

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour l'AutoSupport, qui surveille de

manière proactive l'état de santé de votre système et envoie des messages au support technique de NetApp.

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

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

Si aucune connexion Internet sortante n'est disponible pour envoyer des messages AutoSupport, BlueXP configure automatiquement vos systèmes Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy. La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous avez défini des règles sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

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

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

Adresses IP

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

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



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

Adresses IP d'un système à un seul nœud

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

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



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

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

Adresses IP des paires haute disponibilité

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

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

NIC0

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



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

NIC1

- IP du réseau de cluster

NIC2

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

NIC3

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



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

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

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

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

Connexion sécurisée aux services Azure

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

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

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

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

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

Connexions à d'autres systèmes ONTAP

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

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

Port pour l'interconnexion haute disponibilité

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

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

Une seule paire HA dans un groupe de ressources Azure

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

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

Groupes de sécurité

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

Règles de groupe de sécurité

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

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

Règles entrantes pour les systèmes à nœud unique

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

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

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

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

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

Règles entrantes pour les systèmes HA

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

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



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

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

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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



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

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

| Service | Port | Prot ocol e | Source | Destination | Objectif |
|-------------|-------------|-------------------|--|--|--|
| AutoSupport | HTTPS | 443 | FRV de gestion des nœuds | support.netapp.com | AutoSupport (HTTPS est le protocole par défaut) |
| | HTTP | 80 | FRV de gestion des nœuds | support.netapp.com | AutoSupport (uniquement si le protocole de transport est passé de HTTPS à HTTP) |
| | TCP | 3128 | FRV de gestion des nœuds | Connecteur | Envoi de messages AutoSupport via un serveur proxy sur le connecteur, si aucune connexion Internet sortante n'est disponible |
| DHCP | 68 | UDP | FRV de gestion des nœuds | DHCP | Client DHCP pour la première configuration |
| DHCPs | 67 | UDP | FRV de gestion des nœuds | DHCP | Serveur DHCP |
| DNS | 53 | UDP | FRV de gestion des nœuds et FRV de données (NFS, CIFS) | DNS | DNS |
| NDMP | 18600-18699 | TCP | FRV de gestion des nœuds | Serveurs de destination | Copie NDMP |
| SMTP | 25 | TCP | FRV de gestion des nœuds | Serveur de messagerie | Les alertes SMTP peuvent être utilisées pour AutoSupport |
| SNMP | 161 | TCP | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | 161 | UDP | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | 162 | TCP | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | 162 | UDP | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| SnapMirror | 11104 | TCP | FRV InterCluster | Baies de stockage inter-clusters ONTAP | Gestion des sessions de communication intercluster pour SnapMirror |
| | 11105 | TCP | FRV InterCluster | Baies de stockage inter-clusters ONTAP | Transfert de données SnapMirror |
| Syslog | 514 | UDP | FRV de gestion des nœuds | Serveur Syslog | Messages de transfert syslog |

Configuration requise pour le connecteur

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

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

Connexion aux réseaux cibles

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

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

Accès Internet sortant

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

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

Serveur proxy

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

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

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

Limitation de l'adresse IP

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

Règles de groupe de sécurité

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

Règles entrantes

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

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



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

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

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

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

Présentation du chiffrement des données

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

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

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

Rotation des clés

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

Mode de cryptage des données

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

Zone de disponibilité Azure HA à plusieurs niveaux

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

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

Zone de disponibilité unique d’Azure HA

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

Un seul nœud

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

Note de bas de page

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

Créez un coffre-fort de clés et générez une clé

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

Étapes

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

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

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

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

Notez les exigences suivantes pour la clé :

- Le type de clé doit être **RSA**.

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

Créez un environnement de travail qui utilise la clé de cryptage

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

Autorisations requises

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

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

"Affichez la liste des autorisations les plus récentes"



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

Étapes

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

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

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

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

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

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

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

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

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

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

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

- a. Pour une paire haute disponibilité :

POST /azure/ha/working-environments

Le corps de la demande doit inclure les champs suivants :

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

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

b. Pour un système à un seul nœud :

POST /azure/vsa/working-environments

Le corps de la demande doit inclure les champs suivants :

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

+

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

Résultat

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

Configuration des licences pour Cloud Volumes ONTAP dans Azure

Après avoir décidé de l'option de licence que vous souhaitez utiliser avec Cloud Volumes ONTAP, quelques étapes sont nécessaires avant de pouvoir choisir cette option de licence lors de la création d'un nouvel environnement de travail.

Frémium

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.

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

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials
Managed Service Identity

Azure Subscription
OCCM Dev (Default)

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

+ Add Subscription

Apply Cancel

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

Select Charging Method

| | | |
|---|-------------|---|
| <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 Azure"](#).

Licence basée sur la capacité

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

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

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

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

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

BYOL

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

Étapes

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

BlueXP interroge automatiquement le service des licences NetApp pour obtenir des informations sur les licences associées à votre compte sur le site de support NetApp. En l'absence d'erreurs, BlueXP ajoute automatiquement les licences au porte-monnaie numérique.

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

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

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

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

+ Add Subscription

Apply Cancel

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

Select Charging Method

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

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

Abonnement PAYGO

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

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, BlueXP vous invite à vous abonner au contrat disponible sur Azure Marketplace. Cet abonnement est ensuite associé à l'environnement de travail

pour la facturation. Vous pouvez utiliser ce même abonnement pour d'autres environnements de travail.

Étapes

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity ▼

Azure Subscription

OCCM Dev (Default) ▼

Marketplace Subscription

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

[+ Add Subscription](#)

Apply **Cancel**

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

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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



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

Contrat annuel

Payez Cloud Volumes ONTAP annuellement par l'achat d'un contrat annuel.

Étapes

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

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

Une fois que NetApp vous a fait part de son offre privée, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à Azure Marketplace lors de la création d'un environnement de travail.

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

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

Abonnement Keystone Flex

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

Étapes

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

Select Charging Method

☒

Keystone

By capacity

^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐

Professional

By capacity

v

☐

Essential

By capacity

v

☐

Freemium (Up to 500 GiB)

By capacity

v

☐

Per Node

By node

v

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

Activez le mode haute disponibilité dans Azure

Le mode haute disponibilité de Microsoft Azure doit être activé pour réduire les temps de basculement non planifiés et permettre la prise en charge de NFSv4 pour Cloud Volumes ONTAP.

À partir de la version 9.10.1 d'Cloud Volumes ONTAP, nous avons réduit le temps de basculement non planifié pour les paires HA Cloud Volumes ONTAP qui s'exécutent dans Microsoft Azure et ajouté la prise en charge de NFSv4. Pour que ces améliorations soient disponibles dans Cloud Volumes ONTAP, vous devez activer la fonctionnalité de haute disponibilité de votre abonnement Azure.

BlueXP vous invite à entrer ces informations dans un message action requise lorsque la fonction doit être activée sur un abonnement Azure.

Notez ce qui suit :

- La haute disponibilité de votre paire haute disponibilité Cloud Volumes ONTAP est sans problème. Cette fonctionnalité Azure fonctionne de concert avec ONTAP pour réduire le temps d'interruption de l'application observée par le client pour les protocoles NFS résultant d'événements de basculement non planifiés.
- L'activation de cette fonctionnalité n'engendre pas d'interruption sur les paires haute disponibilité d'Cloud Volumes ONTAP.
- L'activation de cette fonctionnalité sur votre abonnement Azure n'entraîne aucun problème pour les autres machines virtuelles.

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

Étapes

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

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

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

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

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

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

Lancement d'Cloud Volumes ONTAP dans Azure

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

Ce dont vous avez besoin

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

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

Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau Azure auprès de votre administrateur. Pour plus de détails, voir "[Planification de votre configuration Cloud Volumes ONTAP](#)".

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

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

Description de la tâche

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

Risque de perte de données

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



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

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

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Microsoft Azure** et **Cloud Volumes ONTAP nœud unique**.
4. Si vous y êtes invité, "[Créer un connecteur](#)".
5. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, puis spécifiez les informations d'identification.

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

| Champ | Description |
|-----------------------------------|--|
| Nom de l'environnement de travail | BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option. |

| Champ | Description |
|--|--|
| Balises de groupe de ressources | Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, BlueXP les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure ". |
| Nom d'utilisateur et mot de passe | Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé. |
| Modifier les informations d'identification | Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. " Apprenez à ajouter des informations d'identification ". |

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

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

(video)

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

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

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

9. **Méthodes de chargement et compte NSS** : spécifiez l'option de chargement à utiliser avec ce système, puis spécifiez un compte sur le site de support NetApp.
- ["Découvrez les options de licence pour Cloud Volumes ONTAP"](#).
 - ["Découvrez comment configurer les licences"](#).

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

Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

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



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

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

Notez ce qui suit :

- Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
- La taille des disques correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

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

- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

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

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

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

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

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

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

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

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

| Champ | Description |
|--|---|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau. |
| Autorisations et utilisateurs/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

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS **CIFS** iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

| Champ | Description |
|---|---|
| Adresse IP principale et secondaire DNS | Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. |
| Domaine Active Directory à rejoindre | Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS. |
| Informations d'identification autorisées à rejoindre le domaine | Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD. |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs ADDC ou ou=utilisateurs ADDC dans ce champ. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"] |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la " Documents d'automatisation BlueXP " pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS. |

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

Pour plus d'informations, voir ["Présentation des profils d'utilisation des volumes"](#) et ["Vue d'ensemble du hiérarchisation des données"](#).

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

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

Résultat

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

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

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

Une fois que vous avez terminé

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

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

Lancement d'une paire HA Cloud Volumes ONTAP dans Azure

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. Si vous y êtes invité, ["Créer un connecteur"](#).
4. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, puis spécifiez les informations d'identification.

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

| Champ | Description |
|-----------------------------------|--|
| Nom de l'environnement de travail | BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option. |

| Champ | Description |
|--|--|
| Balises de groupe de ressources | Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, BlueXP les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure ". |
| Nom d'utilisateur et mot de passe | Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé. |
| Modifier les informations d'identification | Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. " Apprenez à ajouter des informations d'identification ". |

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

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

(video)

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

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

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

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


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

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

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

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

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

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

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

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

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

9. **Packages préconfigurés** : sélectionnez un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Modifier la configuration**.

Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

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



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

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

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

Notez ce qui suit :

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

Pour obtenir de l'aide sur le choix d'une taille de disque, reportez-vous à la section ["Dimensionnement du système dans Azure"](#).

- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

| Champ | Description |
|--|---|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau. |
| Autorisations et utilisateurs/groupes (pour CIFS uniquement) | Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur. |
| Stratégie Snapshot | Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server. |
| Options avancées (pour NFS uniquement) | Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4. |

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

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

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

| Champ | Description |
|---|---|
| Adresse IP principale et secondaire DNS | Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. |
| Domaine Active Directory à rejoindre | Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS. |
| Informations d'identification autorisées à rejoindre le domaine | Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD. |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |

| Champ | Description |
|-------------------------|--|
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer ou=ordinateurs ADDC ou ou=utilisateurs ADDC dans ce champ. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^] |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la " Documents d'automatisation BlueXP " pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS. |

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

Pour plus d'informations, voir "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

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

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

Résultat

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

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

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

Une fois que vous avez terminé

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

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

Lancez-vous dans Google Cloud

Démarrage rapide pour Cloud Volumes ONTAP dans Google Cloud

Lancez-vous avec Cloud Volumes ONTAP pour GCP en quelques étapes.

1

Créer un connecteur

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

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

2

Planification de la configuration

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

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

3

Configurez votre réseau

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

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

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

4

Configurez un compte de service

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

Vous pouvez configurer un seul compte de service et l'utiliser dans les deux cas. Le compte de service doit

avoir le rôle **Administrateur de stockage**.

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

5

Activez les API Google Cloud

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

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

6

Lancez Cloud Volumes ONTAP avec BlueXP

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

Liens connexes

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

Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud

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

Choisissez une licence Cloud Volumes ONTAP

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

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

Choisissez une région prise en charge

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

Choisissez un type de machine pris en charge

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

Compréhension des limites de stockage

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

"Limites de stockage pour Cloud Volumes ONTAP dans GCP"

Dimensionnez votre système dans GCP

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

Type de machine

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

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

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

Type de disque GCP

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

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

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

Taille des disques GCP

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

- Tous les disques qui composent un agrégat doivent être de la même taille.
- Déterminez l'espace dont vous avez besoin tout en prenant en compte les performances.
- Les performances des disques persistants évoluent automatiquement en fonction de la taille des disques et du nombre de CPU virtuels disponibles pour le système.

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

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

Afficher les disques système par défaut

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

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

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



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

Collecte d'informations de mise en réseau

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

Informations de réseau pour un système à un seul nœud

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

Informations de réseau pour une paire HA dans plusieurs zones

| Informations GCP | Votre valeur |
|-------------------------|--------------|
| Région | |
| Zone pour le nœud 1 | |
| Zone pour le nœud 2 | |
| Zone du médiateur | |
| VPC-0 et le sous-réseau | |
| VPC-1 et le sous-réseau | |

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

Informations de réseau pour une paire HA dans une seule zone

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

Choisissez une vitesse d'écriture

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

Choisissez un profil d'utilisation du volume

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

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

Provisionnement fin

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

Déduplication

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

Compression

Réduit la capacité physique requise pour stocker les données en les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Exigences de mise en réseau pour Cloud Volumes ONTAP dans GCP

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

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

Conditions requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être satisfaites dans GCP.

Équilibreurs de charge internes

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

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

La configuration de chaque équilibreur de charge est la suivante :

- Une adresse IP privée partagée
- Une vérification globale du système

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

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

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

Une ou plusieurs zones pour les paires haute disponibilité

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

- Zones multiples (recommandé)

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

- Zone unique

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

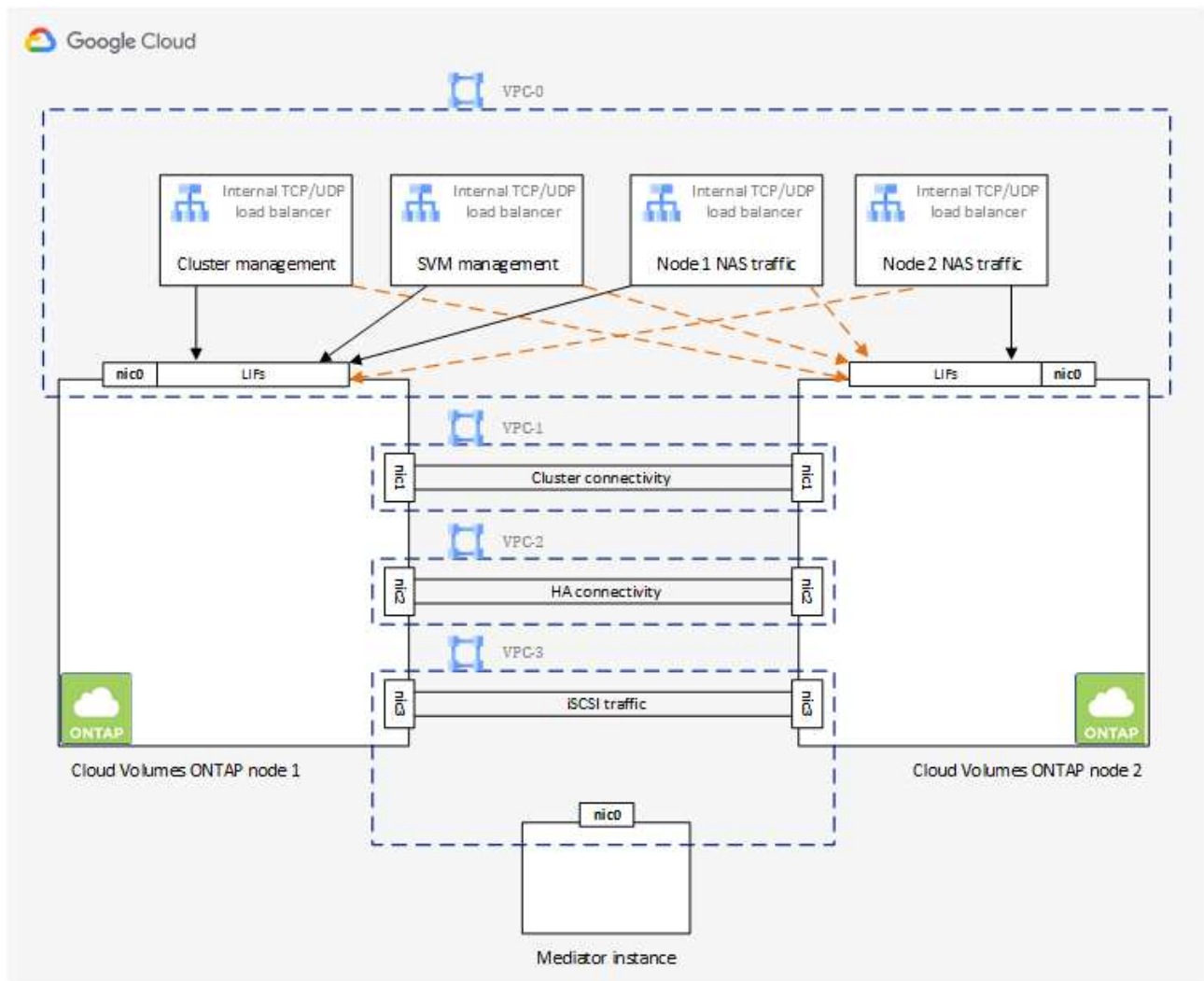
Ce modèle de déploiement réduit vos coûts, car il n'y a pas de frais de sortie de données entre les zones.

Quatre clouds privés virtuels pour les paires haute disponibilité

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

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

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



Sous-réseaux pour paires haute disponibilité

Un sous-réseau privé est requis pour chaque VPC.

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

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

Un cloud privé virtuel pour les systèmes à un seul nœud

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

VPC partagés

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

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

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

Un VPC partagé vous permet de configurer et de gérer de manière centralisée les réseaux virtuels dans plusieurs projets. Vous pouvez configurer des réseaux VPC partagés dans le projet *host* et déployer les instances de machines virtuelles Connector et Cloud Volumes ONTAP dans un projet *service*.

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

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

Duplication de paquets dans les VPC

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

Accès Internet sortant pour Cloud Volumes ONTAP

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

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

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

Si aucune connexion Internet sortante n'est disponible pour envoyer des messages AutoSupport, BlueXP configure automatiquement vos systèmes Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy. La seule exigence est de s'assurer que le pare-feu du connecteur autorise les connexions *Inbound* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

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

Après avoir vérifié que l'accès Internet sortant est disponible, vous pouvez tester AutoSupport pour

vous assurer qu'il peut envoyer des messages. Pour obtenir des instructions, reportez-vous à la section ["Documentation ONTAP : configuration d'AutoSupport"](#).



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

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

Adresses IP privées

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

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

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

```
skipSvmManagementLif: true
```

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

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

- 7 ou 8 adresses IP privées pour VPC-0

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

```
skipSvmManagementLif: true
```

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

Règles de pare-feu

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

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

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

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

Si vous souhaitez effectuer le Tiering des données inactives dans un compartiment de stockage Google Cloud, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour l'accès privé à Google (si vous utilisez une paire haute disponibilité, il s'agit du sous-réseau dans VPC-0). Pour obtenir des instructions, reportez-vous à la section ["Documentation Google Cloud : configuration de Private Google"](#).

[Access](#)".

Pour connaître les étapes supplémentaires nécessaires à la configuration du Tiering des données dans BlueXP, reportez-vous à la section "[Tiering des données inactives vers un stockage objet à faible coût](#)".

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer les données entre un système Cloud Volumes ONTAP dans GCP et des systèmes ONTAP d'autres réseaux, vous devez disposer d'une connexion VPN entre le VPC et l'autre réseau, par exemple votre réseau d'entreprise.

Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : présentation de Cloud VPN](#)".

Configuration requise pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur dans votre réseau d'entreprise, vous devez configurer une connexion VPN au réseau virtuel dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

| Terminaux | Objectif |
|--|--|
| <code>https://support.netapp.com</code> | Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp. |
| <code>https://*.api.bluexp.netapp.com</code> <code>https://api.bluexp.netapp.com</code> <code>https://*.cloudmanager.cloud.netapp.com</code> <code>https://cloudmanager.cloud.netapp.com</code> | <div> Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.bluexp.netapp.com » dans une prochaine version.</div> |
| <code>https://cloudmanagerinfraprod.azurecr.io</code> <code>https://*.blob.core.windows.net</code> | Pour mettre à niveau le connecteur et ses composants Docker. |

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au ["Interface utilisateur locale"](#), que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

Il existe un conflit possible avec des adresses IP dans la plage 172. ["En savoir plus sur cette limitation"](#).

Règles de pare-feu pour Cloud Volumes ONTAP

BlueXP crée des règles de pare-feu GCP qui incluent les règles entrantes et sortantes nécessaires au bon fonctionnement de Cloud Volumes ONTAP. Vous pouvez consulter les ports à des fins de test ou si vous préférez utiliser vos propres règles de pare-feu.

Les règles de pare-feu de Cloud Volumes ONTAP requièrent des règles entrantes et sortantes.

Si vous déployez une configuration haute disponibilité, ce sont les règles de pare-feu pour Cloud Volumes ONTAP dans VPC-0.

Règles entrantes

Lorsque vous créez un environnement de travail, vous pouvez choisir le filtre source de la politique de pare-feu prédéfinie pendant le déploiement :

- **VPC sélectionné uniquement** : le filtre source pour le trafic entrant est la plage de sous-réseau du VPC pour le système Cloud Volumes ONTAP et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.
- **Tous les VPC** : le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.

Si vous utilisez votre propre stratégie de pare-feu, assurez-vous d'ajouter tous les réseaux qui doivent communiquer avec Cloud Volumes ONTAP, mais aussi d'ajouter les deux plages d'adresses pour permettre à Google Load Balancer interne de fonctionner correctement. Ces adresses sont 130.211.0.0/22 et 35.191.0.0/16. Pour plus d'informations, reportez-vous à la section ["Documentation Google Cloud : règles du pare-feu Load Balancer"](#).

| Protocole | Port | Objectif |
|--------------------------|------|--|
| Tous les protocoles ICMP | Tout | Envoi d'une requête ping à l'instance |
| HTTP | 80 | Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster |
| HTTPS | 443 | Connectivité avec le connecteur et l'accès HTTPS à la console Web System Manager via l'adresse IP du LIF de cluster management |

| Protocole | Port | Objectif |
|-----------|-------------|---|
| SSH | 22 | Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud |
| TCP | 111 | Appel de procédure à distance pour NFS |
| TCP | 139 | Session de service NetBIOS pour CIFS |
| TCP | 161-162 | Protocole de gestion de réseau simple |
| TCP | 445 | Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS |
| TCP | 658 | Montage NFS |
| TCP | 749 | Kerberos |
| TCP | 2049 | Démon du serveur NFS |
| TCP | 3260 | Accès iSCSI via le LIF de données iSCSI |
| TCP | 4045 | Démon de verrouillage NFS |
| TCP | 4046 | Surveillance de l'état du réseau pour NFS |
| TCP | 10000 | Sauvegarde avec NDMP |
| TCP | 11104 | Gestion des sessions de communication intercluster pour SnapMirror |
| TCP | 11105 | Transfert de données SnapMirror à l'aide de LIF intercluster |
| TCP | 63001-63050 | Ports de sonde d'équilibrage de la charge pour déterminer quel nœud fonctionne (uniquement requis pour les paires HA) |
| UDP | 111 | Appel de procédure à distance pour NFS |
| UDP | 161-162 | Protocole de gestion de réseau simple |
| UDP | 658 | Montage NFS |
| UDP | 2049 | Démon du serveur NFS |
| UDP | 4045 | Démon de verrouillage NFS |
| UDP | 4046 | Surveillance de l'état du réseau pour NFS |
| UDP | 4049 | Protocole NFS rquotad |

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

| Protocole | Port | Objectif |
|--------------------------|------|------------------------|
| Tous les protocoles ICMP | Tout | Tout le trafic sortant |

| Protocole | Port | Objectif |
|-------------------------|------|------------------------|
| Tous les protocoles TCP | Tout | Tout le trafic sortant |
| Tous les protocoles UDP | Tout | Tout le trafic sortant |

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par Cloud Volumes ONTAP.



La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

| Service | Protocole | Port | Source | Destination | Objectif |
|------------------|------------|------|-----------------------------------|------------------------|--|
| Active Directory | TCP | 88 | FRV de gestion des nœuds | Forêt Active Directory | Authentification Kerberos V. |
| | UDP | 137 | FRV de gestion des nœuds | Forêt Active Directory | Service de noms NetBIOS |
| | UDP | 138 | FRV de gestion des nœuds | Forêt Active Directory | Service de datagrammes NetBIOS |
| | TCP | 139 | FRV de gestion des nœuds | Forêt Active Directory | Session de service NetBIOS |
| | TCP ET UDP | 389 | FRV de gestion des nœuds | Forêt Active Directory | LDAP |
| | TCP | 445 | FRV de gestion des nœuds | Forêt Active Directory | Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS |
| | TCP | 464 | FRV de gestion des nœuds | Forêt Active Directory | Modification et définition du mot de passe Kerberos V (SET_CHANGE) |
| | UDP | 464 | FRV de gestion des nœuds | Forêt Active Directory | Administration des clés Kerberos |
| | TCP | 749 | FRV de gestion des nœuds | Forêt Active Directory | Modification et définition du mot de passe Kerberos V (RPCSEC_GSS) |
| | TCP | 88 | LIF de données (NFS, CIFS, iSCSI) | Forêt Active Directory | Authentification Kerberos V. |
| | UDP | 137 | FRV de données (NFS, CIFS) | Forêt Active Directory | Service de noms NetBIOS |
| | UDP | 138 | FRV de données (NFS, CIFS) | Forêt Active Directory | Service de datagrammes NetBIOS |
| | TCP | 139 | FRV de données (NFS, CIFS) | Forêt Active Directory | Session de service NetBIOS |
| | TCP ET UDP | 389 | FRV de données (NFS, CIFS) | Forêt Active Directory | LDAP |
| | TCP | 445 | FRV de données (NFS, CIFS) | Forêt Active Directory | Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS |
| | TCP | 464 | FRV de données (NFS, CIFS) | Forêt Active Directory | Modification et définition du mot de passe Kerberos V (SET_CHANGE) |
| | UDP | 464 | FRV de données (NFS, CIFS) | Forêt Active Directory | Administration des clés Kerberos |
| | TCP | 749 | FRV de données (NFS, CIFS) | Forêt Active Directory | Modification et définition du mot de passe Kerberos V (RPCSEC_GSS) |

| Service | Protocole | Port | Source | Destination | Objectif |
|-------------|----------------|----------------|--|--|--|
| AutoSupport | HTTPS | 443 | FRV de gestion des nœuds | support.netapp.com | AutoSupport (HTTPS est le protocole par défaut) |
| | HTTP | 80 | FRV de gestion des nœuds | support.netapp.com | AutoSupport (uniquement si le protocole de transport est passé de HTTPS à HTTP) |
| | TCP | 3128 | FRV de gestion des nœuds | Connecteur | Envoi de messages AutoSupport via un serveur proxy sur le connecteur, si aucune connexion Internet sortante n'est disponible |
| Cluster | Tout le trafic | Tout le trafic | Tous les LIF sur un nœud | Tous les LIF de l'autre nœud | Communications InterCluster (Cloud Volumes ONTAP HA uniquement) |
| DHCP | UDP | 68 | FRV de gestion des nœuds | DHCP | Client DHCP pour la première configuration |
| DHCPs | UDP | 67 | FRV de gestion des nœuds | DHCP | Serveur DHCP |
| DNS | UDP | 53 | FRV de gestion des nœuds et FRV de données (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 1860-18699 | FRV de gestion des nœuds | Serveurs de destination | Copie NDMP |
| SMTP | TCP | 25 | FRV de gestion des nœuds | Serveur de messagerie | Les alertes SMTP peuvent être utilisées pour AutoSupport |
| SNMP | TCP | 161 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | UDP | 161 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | TCP | 162 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | UDP | 162 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| SnapMirror | TCP | 11104 | FRV InterCluster | Baies de stockage inter-clusters ONTAP | Gestion des sessions de communication intercluster pour SnapMirror |
| | TCP | 11105 | FRV InterCluster | Baies de stockage inter-clusters ONTAP | Transfert de données SnapMirror |
| Syslog | UDP | 514 | FRV de gestion des nœuds | Serveur Syslog | Messages de transfert syslog |

Règles de pare-feu pour VPC-1, VPC-2 et VPC-3

Dans GCP, une configuration haute disponibilité est déployée sur quatre VPC. Les règles de pare-feu nécessaires à la configuration haute disponibilité dans VPC-0 sont les suivantes [Répertoriées ci-dessus pour Cloud Volumes ONTAP](#).

Pendant ce temps, les règles de pare-feu prédéfinies que BlueXP crée pour les instances dans VPC-1, VPC-2 et VPC-3 permettent la communication via les protocoles et ports *All*. Ces règles permettent la communication entre les nœuds HA.

La communication entre les nœuds HA et le médiateur HA se fait via le port 3260 (iSCSI).

Règles de pare-feu pour le connecteur

Les règles de pare-feu du connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

| Protocole | Port | Objectif |
|-----------|------|---|
| SSH | 22 | Fournit un accès SSH à l'hôte du connecteur |
| HTTP | 80 | Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale |
| HTTPS | 443 | Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale |
| TCP | 3128 | Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement du connecteur. |

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

| Protocole | Port | Objectif |
|-------------------------|------|------------------------|
| Tous les protocoles TCP | Tout | Tout le trafic sortant |
| Tous les protocoles UDP | Tout | Tout le trafic sortant |

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



L'adresse IP source est l'hôte du connecteur.

| Service | Protocole | Port | Destination | Objectif |
|---------------------------|-----------|------|---|--|
| Appels API et AutoSupport | HTTPS | 443 | LIF de gestion de cluster ONTAP et Internet sortant | Appels d'API vers GCP et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp |
| DNS | UDP | 53 | DNS | Utilisé pour la résolution DNS par BlueXP |

Planification des contrôles de service VPC dans GCP

Lorsque vous choisissez de verrouiller votre environnement Google Cloud avec les contrôles de service VPC, vous devez comprendre comment BlueXP et Cloud Volumes ONTAP interagissent avec les API Google Cloud, ainsi que comment configurer votre périmètre de service pour déployer BlueXP et Cloud Volumes ONTAP.

Les contrôles de service VPC vous permettent de contrôler l'accès aux services gérés par Google en dehors d'un périmètre sécurisé, de bloquer l'accès aux données à partir de sites non fiables et de limiter les risques de transferts de données non autorisés. ["En savoir plus sur les contrôles de service Google Cloud VPC"](#).

La communication des services NetApp avec les contrôles de service VPC

BlueXP communique directement avec les API Google Cloud. Ceci est déclenché à partir d'une adresse IP externe en dehors de Google Cloud (par exemple à partir de `api.services.cloud.netapp.com`) ou dans Google Cloud à partir d'une adresse interne attribuée au connecteur BlueXP.

Selon le style de déploiement du connecteur, certaines exceptions peuvent être nécessaires pour votre périmètre de service.

Images

Cloud Volumes ONTAP et BlueXP utilisent toutes les deux des images d'un projet GCP géré par NetApp. Cela peut affecter le déploiement du connecteur BlueXP et de Cloud Volumes ONTAP, si votre organisation dispose d'une stratégie qui bloque l'utilisation d'images qui ne sont pas hébergées au sein de l'organisation.

Vous pouvez déployer un connecteur manuellement selon la méthode d'installation manuelle, mais Cloud Volumes ONTAP devra également extraire des images du projet NetApp. Vous devez fournir une liste autorisée pour déployer un connecteur et un Cloud Volumes ONTAP.

Déploiement d'un connecteur

L'utilisateur qui déploie un connecteur doit pouvoir référencer une image hébergée dans le projectId `netapp-cloudManager` et le numéro de projet `14190056516`.

Le déploiement de Cloud Volumes ONTAP

- Le compte de service BlueXP doit référencer une image hébergée dans le projectId *netapp-cloudManager* et le numéro de projet *14190056516* du projet de service.
- Le compte de service de l'agent de service Google API par défaut doit référencer une image hébergée dans le projectId *netapp-cloudManager* et le numéro de projet *14190056516* du projet de service.

Des exemples des règles requises pour extraire ces images avec les contrôles de service VPC sont définis ci-dessous.

Le service VPC contrôle les stratégies de périmètre

Les règles permettent des exceptions aux jeux de règles de contrôle de service VPC. Pour plus d'informations sur les politiques, veuillez consulter le ["Documentation sur les règles de contrôle du service VPC GCP"](#).

Pour définir les stratégies requises par BlueXP, accédez à vos contrôles de service VPC Perimeter dans votre entreprise et ajoutez les stratégies suivantes. Les champs doivent correspondre aux options indiquées dans la page de stratégie contrôles de service VPC. Notez également que **toutes** règles sont requises et que les paramètres **OU** doivent être utilisés dans le jeu de règles.

Règles d'entrée

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
    Service methods: All actions
    Service name: compute.googleapis.com
    Service methods:All actions
```

OU

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

OU

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

Règles de sortie

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



Le numéro de projet mentionné ci-dessus est le projet *netapp-cloudManager* utilisé par NetApp pour stocker des images pour le connecteur et pour Cloud Volumes ONTAP.

Créez un compte de service pour le Tiering des données et les sauvegardes

Cloud Volumes ONTAP nécessite un compte de service Google Cloud pour deux raisons. La première est lorsque vous activez "[tiering des données](#)" Tiering des données inactives vers un stockage objet à faible coût dans Google Cloud. La seconde est lorsque vous activez le "[Cloud Backup Service](#)" sauvegarde de volumes dans un stockage objet à faible coût

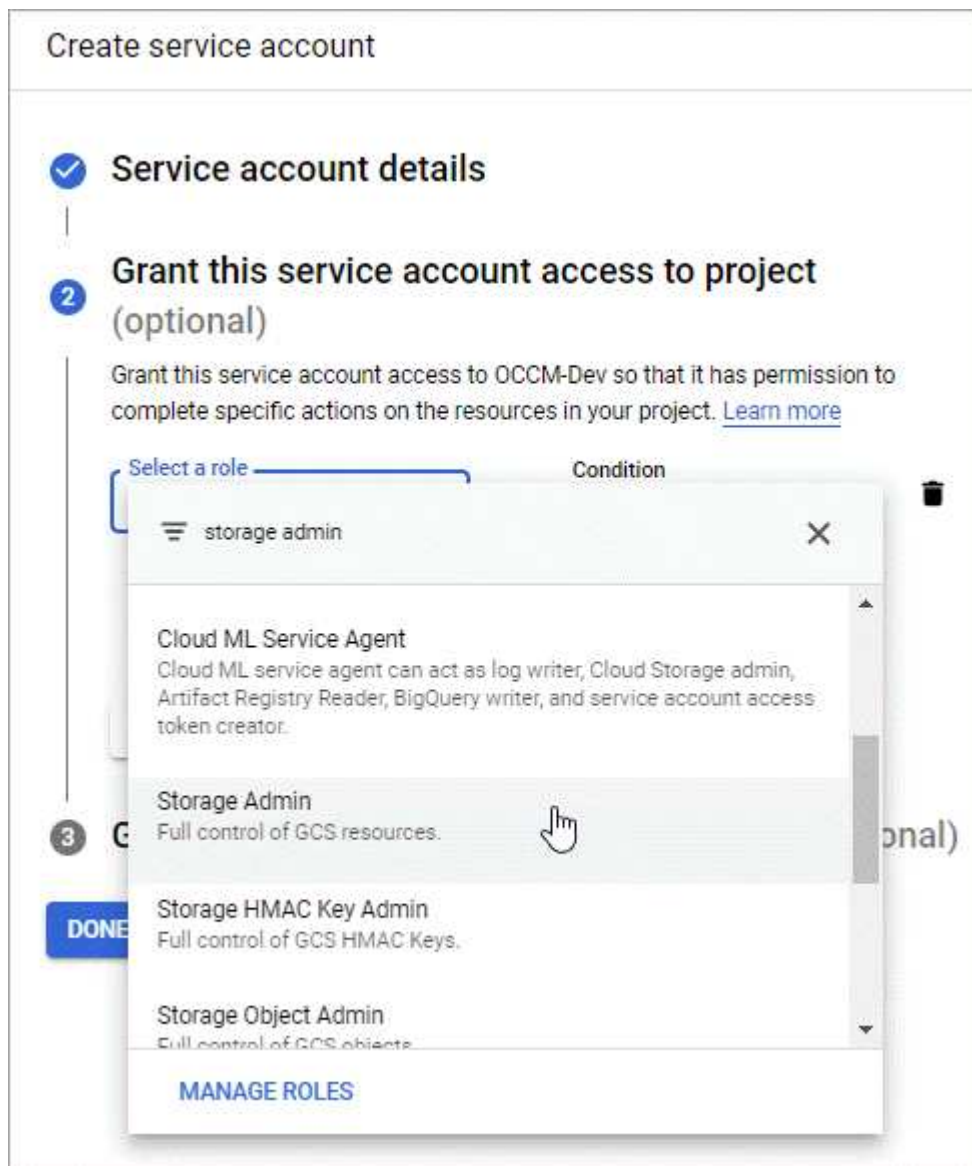
Cloud Volumes ONTAP utilise le compte de service pour accéder aux données hiérarchisées et les gérer dans un autre compartiment pour les sauvegardes.

Vous pouvez configurer un seul compte de service et l'utiliser dans les deux cas. Le compte de service doit avoir le rôle **Administrateur de stockage**.

Étapes

1. Dans la console Google Cloud, "[Accédez à la page comptes de service](#)".

2. Sélectionnez votre projet.
3. Cliquez sur **Créer un compte de service** et fournissez les informations requises.
 - a. **Détails du compte de service** : saisissez un nom et une description.
 - b. **Accordez à ce compte de service l'accès au projet** : sélectionnez le rôle **Administrateur de stockage**.



- c. **Accordez aux utilisateurs l'accès à ce compte de service** : ajoutez le compte de service Connector en tant qu'utilisateur *Service Account* à ce nouveau compte de service.

Cette étape est uniquement requise pour le Tiering des données. Ce n'est pas requis pour le Cloud Backup Service.

Create service account

✓

Service account details

|

✓

Grant this service account access to project (optional)

|

3

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com ✕ ?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

?

Grant users the permission to administer this service account

DONE

CANCEL

Et la suite ?

Vous devrez ensuite sélectionner le compte de service lors de la création d'un environnement de travail Cloud Volumes ONTAP.

Details and Credentials

default-project

gcp-sub2

Edit Project

Google Cloud Project

Marketplace Subscription

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account ⓘ

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser l'API BlueXP pour créer un système Cloud Volumes ONTAP qui utilise des clés de chiffrement *gérées par le client*. Il s'agit des clés que vous créez et gérez dans GCP à l'aide du service Cloud Key Management.

Étapes

1. Assurez-vous que le compte de service BlueXP Connector dispose des autorisations appropriées au niveau du projet, dans le projet où la clé est stockée.

Les autorisations sont fournies dans le "[Par défaut, Connector service account permissions](#)", Mais ne peut pas être appliqué si vous utilisez un autre projet pour le service Cloud Key Management.

Les autorisations sont les suivantes :

- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`

2. Assurez-vous que le compte de service du "[Agent de service Google Compute Engine](#)" Dispose d'autorisations de chiffrement/déchiffrement de clés KMS sur le Cloud.

Le nom du compte de service utilise le format suivant : "service-[service_Project_Number]@compute-system.iam.gserviceaccount.com".

["Google Cloud Documentation : utilisation de l'IAM avec Cloud KMS - attribution de rôles sur une ressource"](#)

3. Obtenir l'ID de la clé en invoquant la commande obtenir pour le `/gcp/vsa/metadata/gcp-encryption-keys` Ou en choisissant « Copy Resource Name » (Copier le nom de la ressource) sur la clé de la console GCP.
4. Si vous utilisez des clés de chiffrement gérées par le client et hiérarchise les données vers le stockage objet, BlueXP tente d'utiliser les clés qui sont utilisées pour chiffrer les disques persistants. Toutefois, vous devez d'abord activer les compartiments Google Cloud Storage pour utiliser les clés :
 - a. Recherchez l'agent de service Google Cloud Storage en suivant le ["Documentation Google Cloud : comment obtenir l'agent de service Cloud Storage"](#).
 - b. Accédez à la clé de chiffrement et attribuez l'agent de service Google Cloud Storage avec les autorisations de chiffrement/déchiffrement de Cloud KMS.

Pour plus d'informations, reportez-vous à la section ["Google Cloud Documentation : utilisation de clés de chiffrement gérées par le client"](#)

5. Utilisez le paramètre "GcpEncryption" avec votre requête API lors de la création d'un environnement de travail.

Exemple

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

Reportez-vous à la ["Documents d'automatisation BlueXP"](#) Pour plus d'informations sur l'utilisation du paramètre "GcpEncryption".

Configurez la licence pour Cloud Volumes ONTAP dans Google Cloud

Après avoir décidé de l'option de licence que vous souhaitez utiliser avec Cloud Volumes ONTAP, quelques étapes sont nécessaires avant de pouvoir choisir cette option de licence lors de la création d'un nouvel environnement de travail.

Frémium

Sélectionnez l'offre « Freemium » pour utiliser Cloud Volumes ONTAP gratuitement et bénéficier d'une capacité provisionnée de 500 Gio. ["En savoir plus sur l'offre Freemium"](#).

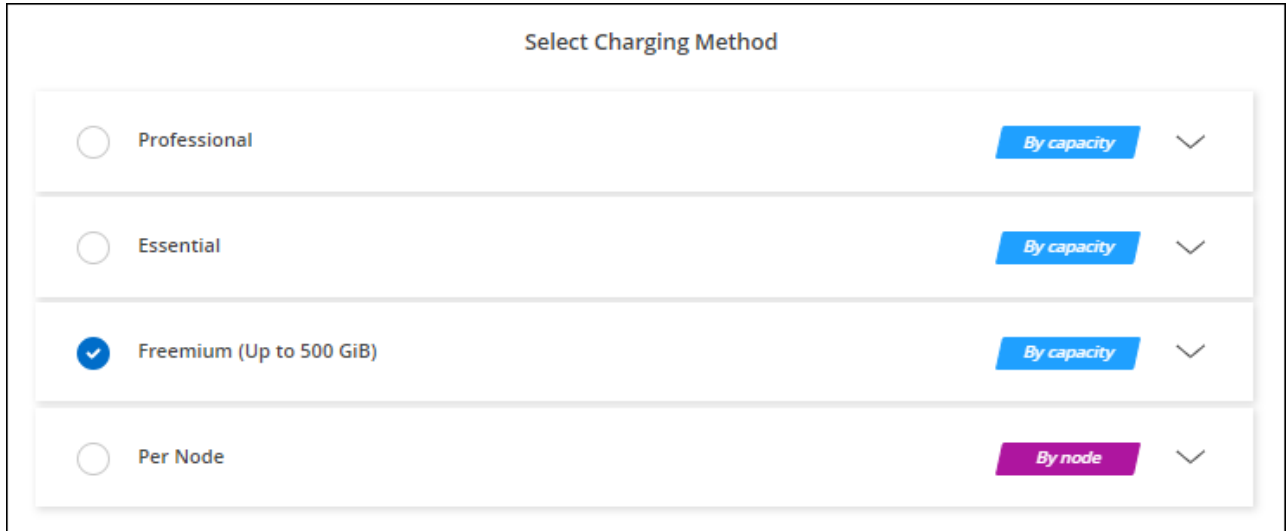
Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de

paiement basé sur l'utilisation dans Google Cloud Marketplace.

Vous ne serez pas facturé via l'abonnement Marketplace sauf si vous dépassez votre capacité provisionnée de 500 Gio, à l'heure où le système est automatiquement converti en ["Pack Essentials"](#).

- b. Après votre retour à BlueXP, sélectionnez **Freemium** lorsque vous atteignez la page méthodes de charge.



The screenshot shows a 'Select Charging Method' window with four radio button options. The 'Freemium (Up to 500 GiB)' option is selected, indicated by a blue checkmark. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The buttons for 'By capacity' are blue, while the button for 'By node' is purple.

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud"](#).

Licence basée sur la capacité

La licence basée sur la capacité vous permet de payer pour le Cloud Volumes ONTAP par Tio de capacité. Une licence basée sur la capacité est disponible sous la forme d'un *package* : le package Essentials ou le pack Professional.

Les packs Essentials et Professional sont disponibles avec les modèles de consommation suivants :

- Licence (BYOL) achetée auprès de NetApp
- Un abonnement à l'heure avec paiement à l'utilisation (PAYGO) à partir de Google Cloud Marketplace
- Un contrat annuel

["En savoir plus sur les licences basées sur la capacité"](#).

Les sections suivantes expliquent comment commencer avec chacun de ces modèles de consommation.

BYOL

Payez l'achat initial d'une licence (BYOL) auprès de NetApp pour le déploiement des systèmes Cloud Volumes ONTAP, quel que soit le fournisseur de cloud.

Étapes

1. ["Contactez l'équipe commerciale de NetApp pour obtenir une licence"](#)
2. ["Ajoutez votre compte sur le site de support NetApp à BlueXP"](#)

BlueXP interroge automatiquement le service des licences NetApp pour obtenir des informations sur les licences associées à votre compte sur le site de support NetApp. En l'absence d'erreurs, BlueXP ajoute

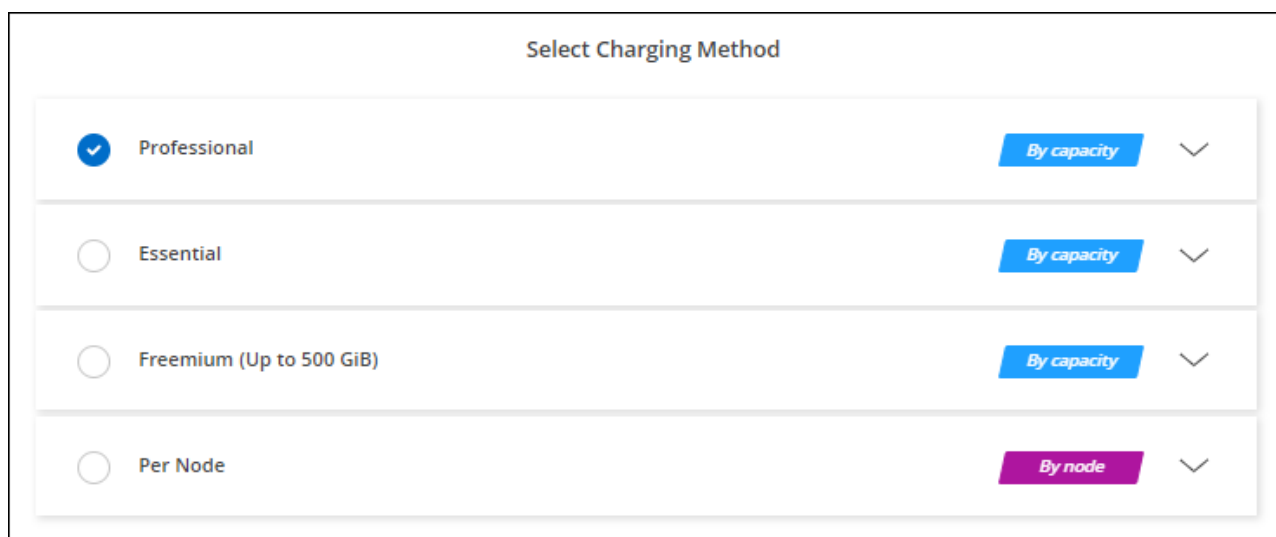
automatiquement les licences au porte-monnaie numérique.

Votre licence doit être disponible auprès du porte-monnaie numérique avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez "[Ajoutez manuellement la licence au porte-monnaie numérique](#)".

3. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement basé sur l'utilisation dans Google Cloud Marketplace.

La licence que vous avez achetée auprès de NetApp est toujours facturée en premier. Elle vous sera facturée à l'heure du marché en cas de dépassement de votre capacité autorisée ou d'expiration de la licence.

- b. Après votre retour à BlueXP, sélectionnez un package basé sur la capacité lorsque vous accédez à la page méthodes de charge.



| Select Charging Method | |
|--|-------------|
| <input checked="" type="radio"/> Professional | By capacity |
| <input type="radio"/> Essential | By capacity |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity |
| <input type="radio"/> Per Node | By node |

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud"](#).

Abonnement PAYGO

Payez votre abonnement à l'heure par abonnement à l'offre sur le marché de votre fournisseur cloud.

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, BlueXP vous invite à vous abonner au contrat disponible sur Google Cloud Marketplace. Cet abonnement est ensuite associé à l'environnement de travail pour la facturation. Vous pouvez utiliser ce même abonnement pour d'autres environnements de travail.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement basé sur l'utilisation dans Google Cloud Marketplace.
 - b. Après votre retour à BlueXP, sélectionnez un package basé sur la capacité lorsque vous accédez à la

page méthodes de charge.

| Select Charging Method | |
|--|-------------|
| <input checked="" type="radio"/> Professional | By capacity |
| <input type="radio"/> Essential | By capacity |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity |
| <input type="radio"/> Per Node | By node |

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud".](#)



Vous pouvez gérer les abonnements Google Cloud Marketplace associés à vos comptes à partir de la page Paramètres > informations d'identification. ["Découvrez comment gérer vos identifiants et abonnements Google Cloud"](#)

Contrat annuel

Payez Cloud Volumes ONTAP annuellement par l'achat d'un contrat annuel.

Étapes

1. Contactez votre ingénieur commercial NetApp pour acheter un contrat annuel.

Le contrat est disponible sous la forme d'une offre *privée* dans Google Cloud Marketplace.

Une fois que NetApp vous a proposé de partager son offre privée, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à Google Cloud Marketplace lors de la création de votre environnement de travail.

2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner au plan annuel dans Google Cloud Marketplace.
 - b. Dans Google Cloud, sélectionnez le plan annuel partagé avec votre compte, puis cliquez sur **Abonnez-vous**.
 - c. Après votre retour à BlueXP, sélectionnez un package basé sur la capacité lorsque vous accédez à la page méthodes de charge.

Select Charging Method

| | | |
|--|-------------|---|
| <input checked="" type="radio"/> Professional | By capacity | ▼ |
| <input type="radio"/> Essential | By capacity | ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node | By node | ▼ |

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud".](#)

Abonnement Keystone Flex

Un abonnement Keystone Flex est un service basé sur un abonnement avec paiement à l'utilisation. ["En savoir plus sur les abonnements Keystone Flex"](#).

Étapes

1. Si vous n'avez pas encore d'abonnement, ["Contactez NetApp"](#)
2. [Mailto:ng-keystone-success@netapp.com](mailto:ng-keystone-success@netapp.com)[contacter NetApp] pour autoriser votre compte utilisateur BlueXP avec un ou plusieurs abonnements Keystone Flex.
3. Après que NetApp autorise votre compte, ["Associez vos abonnements pour une utilisation avec Cloud Volumes ONTAP"](#).
4. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les étapes de BlueXP.
 - a. Sélectionnez la méthode de facturation de l'abonnement Keystone Flex lorsque vous êtes invité à choisir une méthode de charge.

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ **Professional** By capacity v

☐ **Essential** By capacity v

☐ **Freemium (Up to 500 GiB)** By capacity v

☐ **Per Node** By node v

["Consultez des instructions détaillées pour lancer Cloud Volumes ONTAP dans Google Cloud".](#)

Lancement d'Cloud Volumes ONTAP dans GCP

Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à un seul nœud ou en tant que paire HA dans Google Cloud Platform.

Avant de commencer

Vous avez besoin des éléments suivants pour créer un environnement de travail.

- Un connecteur opérationnel.
 - Vous devez avoir un ["Connecteur associé à votre espace de travail"](#).
 - ["Vous devez être prêt à laisser le connecteur fonctionner en permanence"](#).
 - Compte de service associé au connecteur ["doit disposer des autorisations requises"](#)
- Compréhension de la configuration que vous voulez utiliser.

Vous devez vous préparer en choisissant une configuration et en obtenant des informations de mise en réseau GCP de votre administrateur. Pour plus de détails, voir ["Planification de votre configuration Cloud Volumes ONTAP"](#).

- Comprendre les exigences de configuration des licences pour Cloud Volumes ONTAP.

["Découvrez comment configurer les licences"](#).

- Les API Google Cloud doivent être de "[activé dans votre projet](#)":
 - API Cloud Deployment Manager V2
 - API de journalisation cloud
 - API Cloud Resource Manager
 - API du moteur de calcul
 - API de gestion des identités et des accès

Lancement d'un système à un seul nœud dans GCP


Créez un environnement de travail dans BlueXP pour lancer Cloud Volumes ONTAP dans GCP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP**.
4. Si vous y êtes invité, "[Créer un connecteur](#)".
5. **Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, sélectionnez éventuellement un compte de service, ajoutez éventuellement des étiquettes, puis spécifiez les informations d'identification.

Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

| Champ | Description |
|-----------------------------------|--|
| Nom de l'environnement de travail | BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance de machine virtuelle GCP. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option. |
| Nom du compte de service | Si vous prévoyez d'utiliser " tiering des données " ou " La sauvegarde dans le cloud " Avec Cloud Volumes ONTAP, vous devez alors activer compte de service et sélectionner un compte de service disposant du rôle d'administrateur de stockage prédéfini. " Découvrez comment créer un compte de service ". |
| Ajouter des étiquettes | Les étiquettes sont des métadonnées pour les ressources GCP. BlueXP ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Google Cloud : étiquetage des ressources ". |
| Nom d'utilisateur et mot de passe | Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé. |

| Champ | Description |
|--------------------|--|
| Modifier le projet | <p>Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet où réside BlueXP.</p> <p>Si vous ne voyez pas de projets supplémentaires dans la liste déroulante, alors vous n'avez pas encore associé le compte de service BlueXP à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <div>  <p>Il s'agit du compte de service que vous avez configuré pour BlueXP, "comme décrit sur cette page".</p> </div> <p>Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.</p> |

La vidéo suivante explique comment associer un abonnement Marketplace basé sur l'utilisation à votre projet GCP. Vous pouvez également suivre les étapes pour vous abonner à la "[Association d'un abonnement Marketplace aux informations d'identification GCP](#)" section.

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

6. **Services** : sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner Cloud Backup ou utiliser Tiering, vous devez avoir spécifié le compte de service à l'étape 3.
7. **Localisation et connectivité** : sélectionnez un emplacement, choisissez une stratégie de pare-feu et confirmez la connectivité réseau au stockage Google Cloud pour le Tiering des données.

Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

| Champ | Description |
|---|---|
| Vérification de la connectivité | Pour déplacer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section " Documentation Google Cloud : configuration de Private Google Access ". |
| Politique de pare-feu générée | Si vous laissez BlueXP générer la stratégie de pare-feu pour vous, vous devez choisir comment autoriser le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, le filtre source pour le trafic entrant est la plage de sous-réseau du VPC sélectionné et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VPC, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0. |
| Utilisez la politique de pare-feu existante | Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises. " En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP ". |

8. **Méthodes de chargement et compte NSS** : spécifiez l'option de chargement à utiliser avec ce système, puis spécifiez un compte sur le site de support NetApp.
 - "[Découvrez les options de licence pour Cloud Volumes ONTAP](#)".
 - "[Découvrez comment configurer les licences](#)".
9. **Packages préconfigurés** : sélectionnez un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP en fonction des besoins et sélectionnez un type de machine.



Si une version plus récente, General Availability ou patch est disponible pour la version sélectionnée, BlueXP met à jour le système vers cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.10.1 et 9.10.1 P4. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

11. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque et la taille de chaque disque.

Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.

La taille des disques correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section ["Dimensionnement du système dans GCP"](#).

12. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

["En savoir plus sur la vitesse d'écriture"](#).

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

["En savoir plus sur le stockage WORM"](#).

13. **Tiering de données dans Google Cloud Platform** : choisissez d'activer ou non le Tiering des données sur l'agrégat initial, choisissez une classe de stockage pour les données hiérarchisées, puis sélectionnez un compte de service disposant du rôle d'administrateur de stockage prédéfini (requis pour Cloud Volumes ONTAP 9.7 ou version ultérieure). Ou sélectionnez un compte GCP (obligatoire pour Cloud Volumes ONTAP 9.6).

Notez ce qui suit :

- BlueXP définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. Assurez-vous d'ajouter le compte de service Connector en tant qu'utilisateur du compte de service Tiering, sinon, vous ne pouvez pas le sélectionner dans BlueXP
- Pour obtenir de l'aide sur l'ajout d'un compte GCP, reportez-vous à ["Configuration et ajout de comptes GCP pour le Tiering des données avec la version 9.6"](#).
- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants, mais vous devrez désactiver le système et ajouter un compte de service à partir de la console GCP.

["En savoir plus sur le Tiering des données"](#).

14. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

["En savoir plus sur les versions et les protocoles clients pris en charge"](#).

Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

| Champ | Description |
|--------|--|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |

| Champ | Description |
|--|---|
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau. |
| Autorisations et utilisateurs/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

Volume Name:

Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS **CIFS** iSCSI

Share name:

Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

15. Configuration CIFS : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

| Champ | Description |
|---|--|
| Adresse IP principale et secondaire DNS | Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254. |
| Domaine Active Directory à rejoindre | Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS. |
| Informations d'identification autorisées à rejoindre le domaine | Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD. |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer Google Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs,ou=Cloud dans ce champ. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Google Cloud Documentation : les unités organisationnelles de Google Managed Microsoft AD"] |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la " Documents d'automatisation BlueXP " pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS. |

16. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

Pour plus d'informations, voir "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

17. **Revue et approbation** : consultez et confirmez vos choix.

- Consultez les détails de la configuration.
- Cliquez sur **plus d'informations** pour en savoir plus sur l'assistance et les ressources GCP que BlueXP achètera.
- Cochez les cases **Je comprends....**
- Cliquez sur **Go**.

Résultat

BlueXP déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP, consultez le

message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur **recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, consultez la page ["Prise en charge de NetApp Cloud Volumes ONTAP"](#).

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Lancement d'une paire haute disponibilité dans GCP


Créez un environnement de travail dans BlueXP pour lancer Cloud Volumes ONTAP dans GCP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
3. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP HA**.
4. **Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, sélectionnez éventuellement un compte de service, ajoutez éventuellement des étiquettes, puis spécifiez les informations d'identification.

Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

| Champ | Description |
|-----------------------------------|---|
| Nom de l'environnement de travail | BlueXP utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance de machine virtuelle GCP. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option. |
| Nom du compte de service | Si vous avez l'intention d'utiliser le "Tiering" ou "La sauvegarde dans le cloud" Services, vous devez activer le commutateur compte de service , puis sélectionner le compte de service qui a le rôle d'administrateur de stockage prédéfini. |
| Ajouter des étiquettes | Les étiquettes sont des métadonnées pour les ressources GCP. BlueXP ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Google Cloud : étiquetage des ressources" . |

| Champ | Description |
|-----------------------------------|--|
| Nom d'utilisateur et mot de passe | Il s'agit des identifiants du compte d'administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes. Conservez le nom d'utilisateur <i>admin</i> par défaut ou remplacez-le par un nom d'utilisateur personnalisé. |
| Modifier le projet | <p>Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet où réside BlueXP.</p> <p>Si vous ne voyez pas de projets supplémentaires dans la liste déroulante, alors vous n'avez pas encore associé le compte de service BlueXP à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <div>  <p>Il s'agit du compte de service que vous avez configuré pour BlueXP, "comme décrit sur cette page".</p> </div> <p>Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.</p> |

La vidéo suivante explique comment associer un abonnement Marketplace basé sur l'utilisation à votre projet GCP. Vous pouvez également suivre les étapes pour vous abonner à la "[Association d'un abonnement Marketplace aux informations d'identification GCP](#)" section.

► https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

5. **Services** : sélectionnez les services que vous souhaitez utiliser sur ce système. Pour sélectionner Cloud Backup ou utiliser Tiering, vous devez avoir spécifié le compte de service à l'étape 3.
6. **Modèles de déploiement haute disponibilité** : choisissez plusieurs zones (recommandé) ou une seule zone pour la configuration haute disponibilité. Sélectionnez ensuite une région et des zones.

["En savoir plus sur les modèles de déploiement pour la haute disponibilité"](#).

7. **Connectivité** : sélectionnez quatre VPC différents pour la configuration HA, un sous-réseau dans chaque VPC, puis choisissez une stratégie de pare-feu.

["En savoir plus sur les exigences de mise en réseau"](#).

Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

| Champ | Description |
|---------------------|---|
| Règle générée | Si vous laissez BlueXP générer la stratégie de pare-feu pour vous, vous devez choisir comment autoriser le trafic : <ul style="list-style-type: none">• Si vous choisissez VPC sélectionné uniquement, le filtre source pour le trafic entrant est la plage de sous-réseau du VPC sélectionné et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.• Si vous choisissez tous les VPC, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0. |
| Utiliser l'existant | Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" . |

8. **Méthodes de chargement et compte NSS** : spécifiez l'option de chargement à utiliser avec ce système, puis spécifiez un compte sur le site de support NetApp.
 - ["Découvrez les options de licence pour Cloud Volumes ONTAP"](#).
 - ["Découvrez comment configurer les licences"](#).
9. **Packages préconfigurés** : sélectionnez un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP en fonction des besoins et sélectionnez un type de machine.



Si une version plus récente, General Availability ou patch est disponible pour la version sélectionnée, BlueXP met à jour le système vers cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.10.1 et 9.10.1 P4. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

11. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de

disque et la taille de chaque disque.

Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.

La taille des disques correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par BlueXP lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section ["Dimensionnement du système dans GCP"](#).

12. **WORM** : activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

IMPOSSIBLE D'activer WORM si le Tiering des données était activé. ["En savoir plus sur le stockage WORM"](#).

13. **Tiering de données dans Google Cloud Platform** : choisissez d'activer ou non le Tiering de données sur l'agrégat initial, choisissez une classe de stockage pour les données hiérarchisées, puis sélectionnez un compte de service avec le rôle d'administrateur de stockage prédéfini.

Notez ce qui suit :

- BlueXP définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. Assurez-vous d'ajouter le compte de service Connector en tant qu'utilisateur du compte de service Tiering, sinon, vous ne pouvez pas le sélectionner dans BlueXP.
- Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants, mais vous devrez désactiver le système et ajouter un compte de service à partir de la console GCP.

["En savoir plus sur le Tiering des données"](#).

14. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

["En savoir plus sur les versions et les protocoles clients pris en charge"](#).

Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

| Champ | Description |
|--|--|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau. |

| Champ | Description |
|--|---|
| Autorisations et utilisateurs/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

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS **CIFS** iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

15. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

| Champ | Description |
|---|--|
| Adresse IP principale et secondaire DNS | Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra. Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254. |
| Domaine Active Directory à rejoindre | Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS. |
| Informations d'identification autorisées à rejoindre le domaine | Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD. |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer Google Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs,ou=Cloud dans ce champ. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Google Cloud Documentation : les unités organisationnelles de Google Managed Microsoft AD"] |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez utiliser le domaine Active Directory pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la " Documents d'automatisation BlueXP " pour plus d'informations. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS. |

16. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

Pour plus d'informations, voir "[Présentation des profils d'utilisation des volumes](#)" et "[Vue d'ensemble du hiérarchisation des données](#)".

17. **Revue et approbation** : consultez et confirmez vos choix.

- Consultez les détails de la configuration.
- Cliquez sur **plus d'informations** pour en savoir plus sur l'assistance et les ressources GCP que BlueXP achètera.
- Cochez les cases **Je comprends....**
- Cliquez sur **Go**.

Résultat

BlueXP déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP, consultez le

message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur **recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, consultez la page ["Prise en charge de NetApp Cloud Volumes ONTAP"](#).

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Utiliser Cloud Volumes ONTAP

Gestion des licences

Gestion des licences basées sur la capacité

Gérez vos licences de capacité avec l'Portefeuille digital pour vérifier que votre compte NetApp présente la capacité suffisante pour vos systèmes Cloud Volumes ONTAP.

Licences basées sur la capacité vous pouvez payer pour Cloud Volumes ONTAP par Tio de capacité.

Le *Portefeuille numérique* vous permet de gérer les licences de Cloud Volumes ONTAP à partir d'un seul emplacement. Vous pouvez ajouter de nouvelles licences et mettre à jour des licences existantes.

["En savoir plus sur les licences Cloud Volumes ONTAP"](#).

Comment les licences sont ajoutées au porte-monnaie numérique

Une fois que vous aurez acheté une licence auprès de votre ingénieur commercial NetApp, NetApp vous enverra un e-mail contenant le numéro de série et les informations supplémentaires relatives aux licences.

En attendant, BlueXP interroge automatiquement le service des licences NetApp pour obtenir des informations sur les licences associées à votre compte du site de support NetApp. En l'absence d'erreurs, BlueXP ajoute automatiquement les licences au porte-monnaie numérique.

Si BlueXP ne peut pas ajouter la licence, vous devrez les ajouter manuellement au porte-monnaie numérique vous-même. Par exemple, si le connecteur est installé dans un emplacement qui n'a pas accès à Internet, vous devrez ajouter vous-même les licences. [Découvrez comment ajouter des licences achetées à votre compte](#).

Affichez la capacité consommée dans votre compte

Le porte-monnaie numérique vous indique la capacité totale consommée dans votre compte et la capacité consommée par le package de licences. Cela vous permet de mieux comprendre la façon dont vous achetez de la capacité supplémentaire et si celle-ci est nécessaire.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Si vous sélectionnez **licences basées sur la capacité**, affichez le résumé des packages, qui indique la capacité consommée, la capacité totale sous licence et la capacité totale en PAYGO.
 - *Capacité totale consommée* correspond à la capacité totale provisionnée de tous les systèmes Cloud Volumes ONTAP de votre compte NetApp. La charge dépend de la taille de provisionnement de chaque volume, peu importe l'espace local, utilisé, stocké ou effectif au sein du volume.
 - *Total sous licence* correspond à la capacité totale sous licence (BYOL) que vous avez achetée auprès de NetApp.
 - *Total PAYGO* est la capacité totale provisionnée via des abonnements Cloud Marketplace. La facturation via PAYGO n'est utilisée que si la capacité consommée est supérieure à la capacité sous licence ou si aucune licence BYOL n'est disponible dans le portefeuille numérique.

Voici un exemple de compte ayant une capacité consommée de 2000 Tio :



3. Sous le récapitulatif, consultez la capacité consommée pour chaque package de licences.

- *Consul Capacity* vous indique la capacité totale des volumes pour ce paquet. Pour plus de détails sur un pack spécifique, placez le curseur de la souris sur l'info-bulle.

Pour mieux comprendre les capacités affichées dans le pack Essentials, vous devez connaître le fonctionnement de la charge. "[En savoir plus sur le chargement pour le pack Essentials](#)".

- *BYOL* vous indique la capacité sous licence que vous avez achetée auprès de NetApp.
- *PAYGO* vous indique la capacité totale consommée par modèle de consommation de licence.

Voici un exemple de compte avec plusieurs packages de licences :



Ajoutez des licences achetées à votre compte

Si vous ne voyez pas vos licences achetées dans le porte-monnaie numérique, vous devrez ajouter les licences à BlueXP pour que la capacité soit disponible pour Cloud Volumes ONTAP.

Ce dont vous avez besoin

- Vous devez fournir à BlueXP le numéro de série de la licence ou du fichier de licence.
- Pour saisir le numéro de série, vous devez d'abord le faire "[Ajoutez votre compte sur le site de support NetApp à BlueXP](#)". Il s'agit du compte du site de support NetApp autorisé à accéder au numéro de série.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences basées sur la capacité** et cliquez sur **Ajouter licence**.

3. Entrez le numéro de série de la licence basée sur la capacité ou téléchargez le fichier de licence.

Si vous avez saisi un numéro de série, vous devez également sélectionner le compte du site de support NetApp autorisé à accéder au numéro de série.

4. Cliquez sur **Ajouter une licence**.

Mettez à jour une licence basée sur la capacité

Si vous avez acheté de la capacité supplémentaire ou si vous avez prolongé la durée de votre licence, BlueXP met automatiquement à jour la licence dans le porte-monnaie numérique. Vous n'avez rien à faire.

Cependant, si vous avez déployé BlueXP dans un emplacement qui n'a pas d'accès à Internet, vous devrez mettre à jour la licence manuellement dans BlueXP.

Ce dont vous avez besoin

Le fichier de licence (ou *files* si vous avez une paire HA).

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, cliquez sur le menu d'action en regard de la licence et sélectionnez **mettre à jour la licence**.
3. Téléchargez le fichier de licence.
4. Cliquez sur **Télécharger la licence**.

Changer les méthodes de charge

Vous pouvez modifier la méthode de facturation d'un système Cloud Volumes ONTAP utilisant des licences basées sur la capacité. Par exemple, si vous avez déployé un système Cloud Volumes ONTAP avec le pack Essentials, vous pouvez le remplacer par le pack Professional si vos besoins évoluent.

Restriction

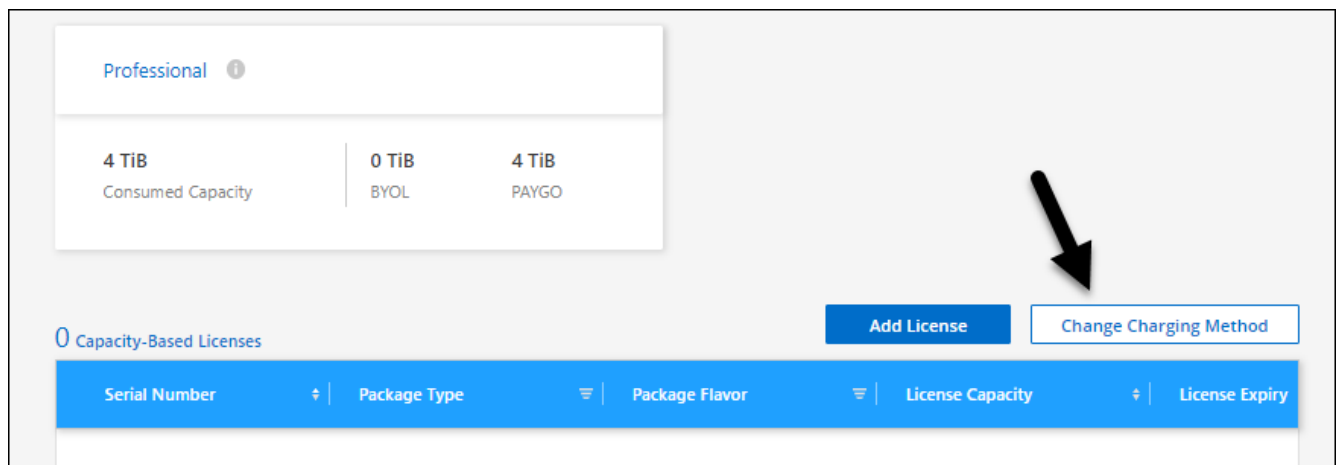
La modification de la licence Edge cache depuis ou vers n'est pas prise en charge.

Remarque importante

Si vous disposez d'une offre ou d'un contrat privé sur le marché de votre fournisseur cloud, le fait de changer de méthode de facturation non incluse dans votre contrat entraînera une facturation en fonction du modèle BYOL (si vous avez acheté une licence auprès de NetApp) ou du modèle de facturation PAYGO.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, cliquez sur **changer la méthode de chargement**.



3. Sélectionnez un environnement de travail, choisissez la nouvelle méthode de charge, puis confirmez que

la modification du type de colis affectera les frais de service.



Change Charging Method

Select a working environment

CloudVolumesONTAP2

Current Cloud Volumes ONTAP charging method

Freemium

Select new Cloud Volumes ONTAP charging method

Essential

☒ I understand that changing the package type will affect service charges

Change Charging Method Cancel

4. Cliquez sur **changer la méthode de charge**.

Résultat

BlueXP modifie la méthode de charge du système Cloud Volumes ONTAP.

Vous pouvez également remarquer que le porte-monnaie numérique actualise la capacité consommée pour chaque type de paquet pour tenir compte de la modification que vous venez de faire.

Suppression d'une licence basée sur la capacité

Si une licence basée sur la capacité a expiré et n'est plus utilisée, vous pouvez la supprimer à tout moment.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, cliquez sur le menu d'action en regard de la licence et sélectionnez **Supprimer la licence**.
3. Cliquez sur **Supprimer** pour confirmer.

Gérez les abonnements Keystone Flex

Gérez vos abonnements Keystone Flex à partir du portefeuille digital en activant les abonnements pour une utilisation avec Cloud Volumes ONTAP. Vous pouvez également demander des modifications à la capacité engagée et annuler la liaison des

abonnements.

Un *Keystone Flex Subscription* est un service de stockage NetApp qui offre un modèle de paiement à l'utilisation.

Le *Portefeuille numérique* vous permet de gérer les licences de Cloud Volumes ONTAP à partir d'un seul emplacement. Vous pouvez ajouter de nouvelles licences et mettre à jour des licences existantes.

["En savoir plus sur les licences Cloud Volumes ONTAP"](#).

Autoriser votre compte

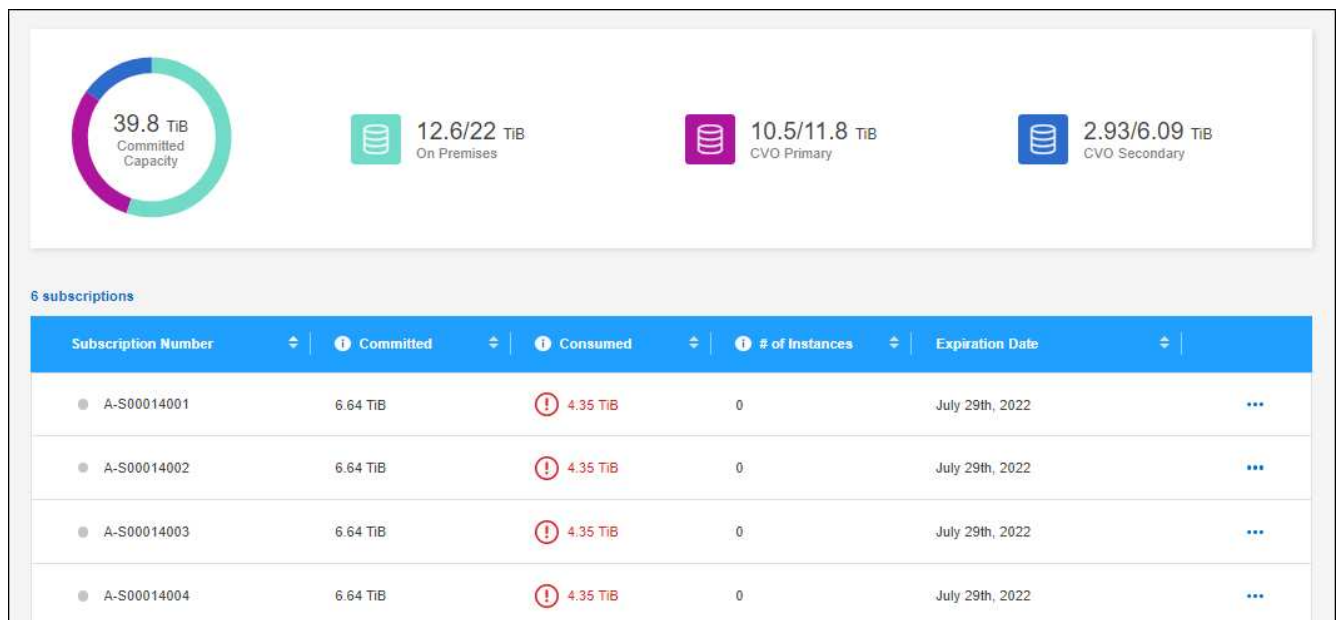
Avant de pouvoir utiliser et gérer les abonnements Keystone Flex dans BlueXP, vous devez contacter NetApp pour autoriser votre compte utilisateur BlueXP avec vos abonnements Keystone Flex.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Cliquez sur **abonnement Keystone Flex**.
3. Si vous voyez la page **Bienvenue dans NetApp Keystone**, envoyez un e-mail à l'adresse indiquée sur la page.

Un représentant NetApp traitera votre demande en autorisant votre compte utilisateur à accéder aux abonnements.

4. Revenez à l'abonnement **Keystone Flex** pour afficher vos abonnements.



Et la suite ?

Associez les abonnements que vous souhaitez utiliser avec Cloud Volumes ONTAP.

Associer un abonnement

Après avoir autorisé votre compte, vous devez lier des abonnements Keystone Flex à utiliser avec Cloud Volumes ONTAP. Cette action permet aux utilisateurs de sélectionner l'abonnement comme méthode de facturation pour les nouveaux systèmes Cloud Volumes ONTAP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Cliquez sur **abonnement Keystone Flex**.
3. Pour l'abonnement que vous souhaitez lier, cliquez sur **...** Et sélectionnez **Link**.

| Subscription Number | Committed | Consumed | # of Instances | Expiration Date | |
|---------------------|-----------|----------|----------------|-----------------|----------------------|
| A-S00014001 | 6.64 TiB | 4.35 TiB | 0 | July 29th, 2022 | ... |
| A-S00014002 | 6.64 TiB | 4.35 TiB | 0 | July 29th, 2022 | View detail and edit |
| A-S00014003 | 6.64 TiB | 4.35 TiB | 0 | July 29th, 2022 | Link |

Résultat

L'abonnement est désormais lié à votre compte BlueXP et disponible pour la création d'un environnement de travail Cloud Volumes ONTAP.

Demandez plus ou moins de capacité dédiée

Si vous devez ajuster la capacité engagée pour un abonnement, vous pouvez envoyer une demande directement à partir de l'interface BlueXP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Cliquez sur **abonnement Keystone Flex**.
3. Pour l'abonnement pour lequel vous souhaitez ajuster la capacité, cliquez sur **...** Et sélectionnez **Afficher le détail et modifier**.
4. Saisissez la capacité d'engagement requise pour un ou plusieurs abonnements.

Subscription Modification for A-S00014001

| Service Level | Current Committed Capacity | Current Consumed Capacity | Requested Committed Capacity |
|---------------|----------------------------|---|---|
| Extreme | 0.977 TiB | 0.293 TiB | <input type="text" value="Enter amount"/> TiB |
| Premium | 0.977 TiB | 0.488 TiB | <input type="text" value="Enter amount"/> TiB |
| Performance | 0 TiB | 0 TiB | <input type="text" value="Enter amount"/> TiB |
| Standard | 0.732 TiB | 0.439 TiB | <input type="text" value="Enter amount"/> TiB |
| Value | 0.977 TiB |  0.879 TiB | <input type="text" value="Enter amount"/> TiB |
| Data Tiering | 0 TiB | 0 TiB | <input type="text" value="Enter amount"/> TiB |
| CVO Primary | 1.96 TiB |  1.76 TiB | <input type="text" value="3"/> TiB |
| CVO Secondary | 1.02 TiB | 0.488 TiB | <input type="text" value="Enter amount"/> TiB |

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

5. Faites défiler vers le bas, saisissez les détails supplémentaires de la demande, puis cliquez sur **Envoyer**.

Résultat

Votre demande crée un ticket dans le système NetApp.

Dissocier un abonnement

Si vous ne souhaitez plus utiliser un abonnement Keystone Flex avec de nouveaux systèmes Cloud Volumes ONTAP, vous pouvez annuler la liaison de l'abonnement. Notez que vous ne pouvez dissocier qu'un abonnement qui n'est pas associé à un abonnement Cloud Volumes ONTAP existant.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Cliquez sur **abonnement Keystone Flex**.
3. Pour l'abonnement que vous souhaitez dissocier, cliquez sur **...** Et sélectionnez **Unlink**.

Résultat

L'abonnement n'est plus lié à votre compte BlueXP et ne peut plus être sélectionné lors de la création d'un environnement de travail Cloud Volumes ONTAP.

Gestion des licences basées sur des nœuds

Gérez les licences par nœud dans le portefeuille numérique pour vous assurer que chaque système Cloud Volumes ONTAP dispose d'une licence valide avec la capacité requise.

Les licences par nœud sont le modèle de licence de génération précédente (et non disponible pour les nouveaux clients) :

- Licences BYOL achetées auprès de NetApp
- Des abonnements avec facturation à l'utilisation (PAYGO) à partir du marché de votre fournisseur cloud

Le *Portefeuille numérique* vous permet de gérer les licences de Cloud Volumes ONTAP à partir d'un seul emplacement. Vous pouvez ajouter de nouvelles licences et mettre à jour des licences existantes.

["En savoir plus sur les licences Cloud Volumes ONTAP"](#).

Gérez les licences PAYGO

La page porte-monnaie numérique vous permet d'afficher des détails sur chacun de vos systèmes Cloud Volumes ONTAP PAYGO, y compris le numéro de série et le type de licence PAYGO.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Cliquez sur **PAYGO**.
4. Pour en savoir plus, consultez le tableau relatif à chacune de vos licences PAYGO.

| 5 Total Licenses | | License Distribution | | 1 BYOL Licenses | 4 PAYGO Licenses | 0 Free Trial | 0 Eval |
|--------------------------|-------------------|--|----------|--------------------------------------|---------------------|-----------------|-----------|
| BYOL (1) | | PAYGO (4) | | EVAL (0) | | | |
| Cloud Volumes ONTAP Name | Type | Serial Number | Package | | | | |
| CVOPAYGO | Single Node | 90920130000000001043 | standard | Manage PAYGO License | | | |
| CVOPAYGO2 | High Availability | Node 1 : 90920140000000001010 Node 2 : 90920140000000001011 | standard | Manage PAYGO License | | | |
| cvopaygo3 | Single Node | 90920130000000001045 | premium | Manage PAYGO License | | | |

5. Si nécessaire, cliquez sur **Manage PAYGO License** pour modifier la licence PAYGO ou pour changer le type d'instance.

Gérez les licences BYOL

Gérez les licences que vous avez achetées directement auprès de NetApp en ajoutant et en supprimant des licences système et des licences de capacité supplémentaire.

Ajouter des licences non affectées

Ajoutez une licence basée sur un nœud au porte-monnaie numérique pour pouvoir sélectionner la licence lorsque vous créez un nouveau système Cloud Volumes ONTAP. Le porte-monnaie numérique identifie ces licences comme *non affectées*.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille 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.

Si vous n'avez pas encore le fichier de licence, reportez-vous à la section ci-dessous.

6. Cliquez sur **Ajouter une licence**.

Résultat

BlueXP ajoute la licence au porte-monnaie numérique. La licence sera identifiée comme non affectée jusqu'à ce que vous l'associez à un nouveau système Cloud Volumes ONTAP. Ensuite, la licence passe à l'onglet **BYOL** du porte-monnaie numérique.

Licences Exchange non attribuées basées sur des nœuds

Si vous disposez d'une licence non attribuée à un nœud pour Cloud Volumes ONTAP que vous n'avez pas utilisée, vous pouvez échanger la licence en la convertissant en licence Cloud Backup, en licence Cloud Data Sense ou en licence Cloud Tiering.

L'échange de la licence révoque la licence Cloud Volumes ONTAP et crée une licence équivalente en dollars pour le service :

- Les licences d'une paire haute disponibilité Cloud Volumes ONTAP sont converties en licence de service de données de 51 Tio
- Les licences d'un nœud Cloud Volumes ONTAP unique sont converties en licence de service de données de 32 Tio

La licence convertie a la même date d'expiration que la licence Cloud Volumes ONTAP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Cliquez sur **non affecté**.
4. Cliquez sur **Exchange License**.

| BYOL (14) | Eval (2) | Unassigned (3) | PAYGO (6) |  Add Unassigned Licenses | | |
|-----------------------|-------------|---|-----------------|---|----------------------------------|-----|
| Serial Number | Type | Cloud Provider | License Expiry | Status | | |
| 012345678901234567890 | Single Node | All Providers | April 20, 2022 | Unassigned | Exchange License | ... |
| 012345678901234567891 | Single Node |  Azure | April 20, 2022 | Unassigned | Exchange License | ... |
| 012345678901234567892 | Single Node |  AWS | January 1, 2022 | Exchanged to Cloud Tiering on August 1, 2021 | | ... |

- Sélectionnez le service avec lequel vous souhaitez échanger la licence.
- Si vous y êtes invité, sélectionnez une licence supplémentaire pour la paire haute disponibilité.
- Lisez le consentement légal et cliquez sur **J'accepte**.

Résultat

BlueXP convertit la licence non attribuée au service que vous avez sélectionné. Vous pouvez afficher la nouvelle licence dans l'onglet **Data Services Licenses**.

Obtenir un fichier de licence système

Dans la plupart des cas, BlueXP peut obtenir automatiquement votre fichier de licence à l'aide de votre compte sur le site de support NetApp. Si ce n'est pas le cas, vous devrez charger manuellement le fichier de licence. Si vous n'avez pas le fichier de licence, vous pouvez l'obtenir sur netapp.com.

Étapes

- Accédez au "[Générateur de fichiers de licences NetApp](#)" Et connectez-vous en utilisant vos identifiants du site du support NetApp.
- 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**.

Exemple

Password*

Product Line*

Product Serial #*

NetApp ONTAP Cloud BYOL for AWS

90120130000000000555

Not only is protecting your data required by law, but your privacy is also very important to us. Please read and agree to the NetApp [Data Privacy Policy](#) before you continue. For information related to NetApp's privacy policy please click here [Privacy Policy](#) or contact privacy@netapp.com.

☒ I have read NetApp's new [Global Data Privacy Policy](#) and understand how NetApp and its selected partners may use my personal data.

Submit

- Choisissez si vous souhaitez recevoir le fichier numéro de série.NLF JSON par e-mail ou par téléchargement direct.

Mettre à jour une licence système

Lorsque vous renouvelez un abonnement BYOL en contactant un représentant NetApp, BlueXP obtient automatiquement la nouvelle licence auprès de NetApp et l'installe sur le système Cloud Volumes ONTAP.

Si BlueXP ne parvient pas à accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le télécharger manuellement vers BlueXP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP.
4. Cliquez sur le menu d'action en regard de la licence système et sélectionnez **mettre à jour la licence**.
5. Téléchargez le fichier de licence (ou les fichiers si vous disposez d'une paire HA).
6. Cliquez sur **mettre à jour la licence**.

Résultat

BlueXP met à jour la licence sur le système Cloud Volumes ONTAP.

Gérez les licences de capacité supplémentaire

Vous pouvez acheter des licences de capacité supplémentaire pour un système Cloud Volumes ONTAP BYOL afin d'allouer plus de 368 To de capacité, si la licence du système BYOL est fournie. Par exemple, vous pouvez acheter une capacité de licence supplémentaire pour allouer une capacité allant jusqu'à 736 Tio à Cloud Volumes ONTAP. Vous pouvez également acheter trois licences de capacité supplémentaire pour obtenir jusqu'à 1.4 Pio.

Le nombre de licences que vous pouvez acheter pour un système à un seul nœud ou une paire HA est illimité.

Ajoutez des licences de capacité

Achetez une licence de capacité supplémentaire en nous contactant par l'icône de chat dans le coin inférieur droit de BlueXP. Une fois la licence achetée, vous pouvez l'appliquer sur un système Cloud Volumes ONTAP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP.
4. Cliquez sur **Ajouter une licence de capacité**.
5. Saisissez le numéro de série ou téléchargez le fichier de licence (ou les fichiers si vous disposez d'une paire HA).
6. Cliquez sur **Ajouter une licence de capacité**.

Mettez à jour les licences de capacité

Si vous avez prolongé la durée d'une licence de capacité supplémentaire, vous devez mettre à jour la licence dans BlueXP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP.
4. Cliquez sur le menu d'action en regard de la licence de capacité et sélectionnez **mettre à jour la licence**.
5. Téléchargez le fichier de licence (ou les fichiers si vous disposez d'une paire HA).
6. Cliquez sur **mettre à jour la licence**.

Éliminez les licences de capacité

Si une licence de capacité supplémentaire a expiré et n'est plus utilisée, vous pouvez la supprimer à tout moment.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP.
4. Cliquez sur le menu d'action en regard de la licence de capacité et sélectionnez **Supprimer la licence**.
5. Cliquez sur **Supprimer**.

Convertissez une licence d'évaluation en licence BYOL

Une licence d'évaluation est valable 30 jours. Vous pouvez appliquer une nouvelle licence BYOL à la licence d'évaluation pour une mise à niveau sur place.

Lorsque vous convertissez une licence d'évaluation en licence BYOL, BlueXP redémarre le système Cloud Volumes ONTAP.

- Pour un système à un seul nœud, le redémarrage entraîne une interruption des E/S lors du processus de redémarrage.
- Pour une paire haute disponibilité, le redémarrage lance le basculement et le rétablissement pour continuer à transmettre des E/S aux clients.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Portefeuille numérique**.
2. Dans l'onglet **Cloud Volumes ONTAP**, sélectionnez **licences par nœud** dans la liste déroulante.
3. Cliquez sur **Eval**.
4. Dans le tableau, cliquez sur **convertir en licence BYOL** pour un système Cloud Volumes ONTAP.
5. Entrez le numéro de série ou téléchargez le fichier de licence.
6. Cliquez sur **convertir la licence**.

Résultat

BlueXP démarre le processus de conversion. Cloud Volumes ONTAP redémarre automatiquement dans le cadre de ce processus. Lors de la sauvegarde, les informations de licence reflètent la nouvelle licence.

PAYGO à la solution BYOL

Convertir un système en licences PAYGO par nœud en licences BYOL (et inversement) n'est pas pris en

charge. Si vous souhaitez basculer entre un abonnement avec paiement à l'utilisation et un abonnement BYOL, vous devez déployer un nouveau système et répliquer les données depuis le système existant vers le nouveau.

Étapes

1. Créez un nouvel environnement de travail Cloud Volumes ONTAP.
2. Configuration d'une réplication unique des données entre les systèmes pour chaque volume à répliquer

["Découvrez comment répliquer des données entre les systèmes"](#)

3. Mettez fin au système Cloud Volumes ONTAP dont vous n'avez plus besoin en supprimant l'environnement de travail d'origine .

["Découvrez comment supprimer un environnement de travail Cloud Volumes ONTAP".](#)

Administration des volumes et des LUN

Créer des volumes FlexVol

Si vous avez besoin de plus de stockage après le lancement de votre système Cloud Volumes ONTAP initial, vous pouvez créer de nouveaux volumes FlexVol pour NFS, CIFS ou iSCSI à partir de BlueXP.

BlueXP offre plusieurs façons de créer un nouveau volume :

- Spécifiez les détails d'un nouveau volume et laissez BlueXP gérer pour vous les agrégats de données sous-jacents. [En savoir plus >>](#).
- Créez un volume sur un agrégat de données de votre choix. [En savoir plus >>](#).
- Créer un volume à partir d'un modèle afin d'optimiser le volume en fonction des besoins de workloads pour certaines applications, telles que les bases de données ou les services de streaming. [En savoir plus >>](#).
- Créer un volume sur le second nœud dans une configuration HA. [En savoir plus >>](#).

Avant de commencer

Remarques sur le provisionnement des volumes :

- 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](#).
- Vous pouvez créer des LUN supplémentaires depuis System Manager ou l'interface de ligne de commandes.
- Si vous souhaitez utiliser CIFS dans AWS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir ["Configuration réseau requise pour Cloud Volumes ONTAP pour AWS"](#).
- Si votre configuration Cloud Volumes ONTAP prend en charge la fonctionnalité Amazon EBS Elastic volumes, vous pouvez vouloir la faire ["en savoir plus sur ce qui se passe lorsque vous créez un volume"](#).

Créer un volume

La manière la plus courante de créer un volume est de spécifier le type de volume dont vous avez besoin, puis

BlueXP gère l'allocation de disque pour vous. Mais vous pouvez également choisir l'agrégat spécifique sur lequel vous voulez créer le volume.

Étapes

- 1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
- 2. Sur la page Canevas, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez provisionner un volume FlexVol.
- 3. Créez un nouveau volume en laissant BlueXP gérer l'allocation de disque pour vous ou choisissez un agrégat spécifique pour le volume.

Il est recommandé de choisir un agrégat spécifique uniquement si vous comprenez bien les agrégats de données de votre système Cloud Volumes ONTAP.

Tout agrégat

Dans l'onglet volumes, cliquez sur **Ajouter un volume > Nouveau volume**.

Agrégat spécifique

- a. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
- b. Cliquez sur le menu correspondant à un agrégat.
- c. Cliquez sur **Créer un volume**.

- 4. Suivez les étapes de l'assistant pour créer le volume.
 - a. **Détails, protection et balises** : saisissez les informations de base sur le volume et sélectionnez une stratégie d'instantané.

Certains des champs de cette page sont explicites. La liste suivante décrit les champs pour lesquels vous pourriez avoir besoin de conseils :

| Champ | Description |
|--------------------|--|
| Taille du volume | 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. |
| Étiquettes | Les balises que vous ajoutez à un volume sont associées à l' " Service modèles d'applications ", qui peut vous aider à organiser et à simplifier la gestion de vos ressources. |
| 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. |

- b. **Protocole** : Choisissez un protocole pour le volume (NFS, CIFS ou iSCSI), puis fournissez les informations requises.

Si vous sélectionnez CIFS et qu'un serveur n'est pas configuré, BlueXP vous invite à configurer la connectivité CIFS après avoir cliqué sur **Suivant**.

["En savoir plus sur les versions et les protocoles clients pris en charge"](#).

Les sections suivantes décrivent les champs pour lesquels vous aurez peut-être besoin de conseils.
Les descriptions sont organisées par protocole.

NFS

Contrôle d'accès

Choisissez une export policy personnalisée pour que le volume soit disponible pour les clients.

Export-policy

Définit les clients dans le sous-réseau qui peuvent accéder au volume. Par défaut, BlueXP entre une valeur qui donne accès à toutes les instances du sous-réseau.

CIFS

Autorisations et utilisateurs/groupes

Permet de contrôler le niveau d'accès à un partage SMB 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 au format domaine\nom_utilisateur.

Adresse IP principale et secondaire DNS

Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.

Si vous configurez Google Managed Active Directory, l'accès à AD est possible par défaut avec l'adresse IP 169.254.169.254.

Domaine Active Directory à rejoindre

Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.

Informations d'identification autorisées à rejoindre le domaine

Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.

Nom NetBIOS du serveur CIFS

Nom de serveur CIFS unique dans le domaine AD.

Unité organisationnelle

Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers.

- Pour configurer Microsoft AD géré par AWS en tant que serveur AD pour Cloud Volumes ONTAP, entrez **ou=ordinateurs,ou=corp** dans ce champ.
- Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez **ou=ordinateurs ADDC** ou **ou=utilisateurs ADDC** dans ce champ. <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou>["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"]
- Pour configurer Google Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez **ou=ordinateurs,ou=Cloud** dans ce champ. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud Documentation : les unités organisationnelles de Google Managed Microsoft AD"]

Domaine DNS

Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.

Serveur NTP

Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la ["Documents d'automatisation BlueXP"](#) pour plus d'informations.

Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Elle n'est pas configurable après la création du serveur CIFS.

ISCSI

LUN

Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Lorsque vous créez un volume iSCSI, BlueXP crée automatiquement un LUN pour vous. Nous l'avons simplifié en créant un seul LUN par volume, ce qui évite toute intervention de gestion. Une fois le volume créé, ["Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes"](#).

Groupe initiateur

Groupes initiateurs (igroups) spécifiez les hôtes qui peuvent accéder aux LUN spécifiés sur le système de stockage

Initiateur hôte (IQN)

Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN).

a. **Type de disque** : choisissez un type de disque sous-jacent pour le volume en fonction de vos besoins en termes de performances et de coûts.

- ["Dimensionnement de votre système dans AWS"](#)
- ["Dimensionnement du système dans Azure"](#)
- ["Dimensionnement du système dans Google Cloud"](#)

5. **Profil d'utilisation et stratégie de hiérarchisation** : choisissez d'activer ou de désactiver les fonctions d'efficacité du stockage sur le volume, puis sélectionnez un ["règle de tiering des volumes"](#).

ONTAP comprend plusieurs fonctionnalités d'efficacité du stockage qui permettent de réduire la quantité totale de stockage nécessaire. 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.

6. **Revue** : consultez les détails du volume, puis cliquez sur **Ajouter**.

Résultat

BlueXP crée le volume sur le système Cloud Volumes ONTAP.

Créer un volume à partir d'un modèle

Si votre entreprise a créé des modèles de volume Cloud Volumes ONTAP pour vous permettre de déployer des volumes optimisés pour répondre aux besoins de workloads de certaines applications, suivez les étapes de cette section.

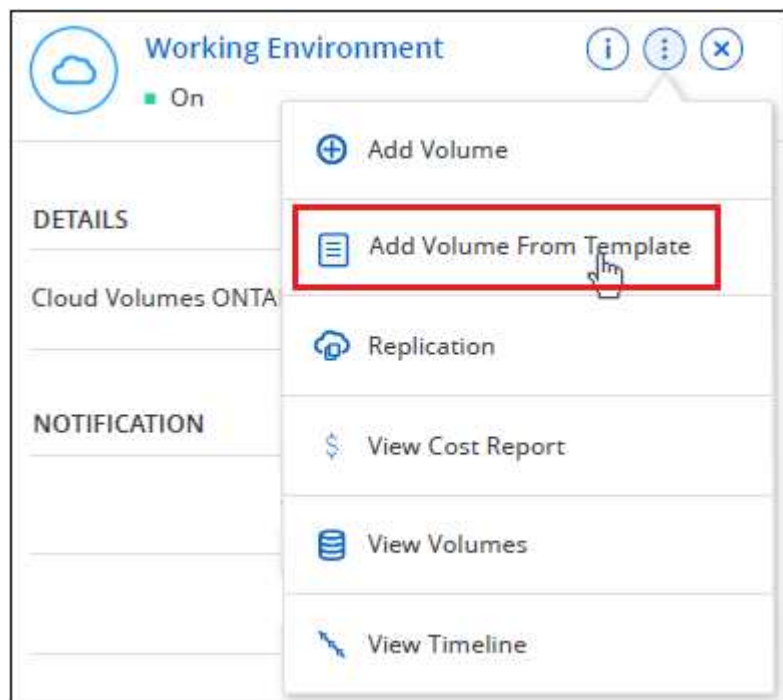
Le modèle doit faciliter votre travail car certains paramètres de volume seront déjà définis dans le modèle, tels que le type de disque, la taille, le protocole, la stratégie Snapshot, le fournisseur de cloud, entre autres. Lorsqu'un paramètre est déjà prédéfini, il vous suffit de passer au paramètre de volume suivant.



Vous pouvez créer des volumes NFS ou CIFS uniquement lors de l'utilisation de modèles.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur le nom du système Cloud Volumes ONTAP dans lequel vous souhaitez provisionner un volume.
3. Cliquez sur > **Ajouter un volume à partir du modèle**.



4. Dans la page *Select Template*, sélectionnez le modèle à utiliser pour créer le volume et cliquez sur **Next**.

Add Volume From Template

Select Template

Define Parameters

Select Template

2 Templates

| Template Name | Template Description | Created by | Last Modified | Parameters |
|---------------------------------|------------------------------------|------------|-------------------------|------------|
| ✓ AWS CVO volume for production | High efficiency with daily backup | Rabin | Apr 05 2021, 1:39:30 pm | View |
| AWS CVO volume for staging | High efficiency with weekly backup | Rabin | Apr 05 2021, 1:34:20 pm | View |

La page *Define Parameters* s'affiche.

Define Parameters

Enter your values for the actions. Parameters that are locked by the template are not editable.

Actions

Create Volume in Cloud Volumes ONTAP (1)

Enable Cloud Backup (1)

Details

Volume Name

Volume Name should start with "staging"

Volume Size (GB)

Minimum value is 160, Maximum value is 185

Protection

Snapshot Policy

Default

Usage Profile

Storage Efficiency

No Storage Efficiency

Disk Type

Disk Type

GP2 - General Purpose SSD

☐ Show read-only parameters



Vous pouvez cliquer sur la case à cocher **Afficher les paramètres en lecture seule** pour afficher tous les champs qui ont été verrouillés par le modèle si vous souhaitez voir les valeurs de ces paramètres. Par défaut, ces champs prédéfinis sont masqués et seuls les champs à compléter sont affichés.

- Dans la zone *context*, l'environnement de travail est rempli avec le nom de l'environnement de travail avec lequel vous avez commencé. Vous devez sélectionner la **VM de stockage** où le volume sera créé.
- Ajoutez des valeurs pour tous les paramètres qui ne sont pas codés en dur à partir du modèle. Voir [Créer un volume](#) Pour déployer un volume Cloud Volumes ONTAP, consultez la section relative aux paramètres à respecter.
- S'il n'y a pas d'autres actions à définir (par exemple, configuration de Cloud Backup), cliquez sur **Exécuter le modèle**.

S'il existe d'autres actions, cliquez sur l'action dans le volet gauche pour afficher les paramètres à compléter.



Par exemple, si l'action Activer la sauvegarde dans le cloud requiert que vous sélectionniez une stratégie de sauvegarde, vous pouvez le faire maintenant.

8. Cliquez sur **Exécuter le modèle**.

Résultat

Cloud Volumes ONTAP provisionne le volume et affiche une page afin que vous puissiez voir sa progression.



Creating your resources

This process can take a few minutes.

Keep this page open to monitor progress, or you can close this page and check the [Timeline](#) later for details.

Actions status

| | | |
|---|--------------------------------------|---------|
|  | Create Volume in Cloud Volumes ONTAP | Success |
|  | Enable Cloud Backup | Pending |

En outre, si une action secondaire est implémentée dans le modèle, par exemple, l'activation de Cloud Backup sur le volume, cette action est également effectuée.

Créer un volume sur le second nœud dans une configuration HA

Par défaut, BlueXP crée des volumes sur le premier nœud d'une configuration HA. Si vous avez besoin d'une configuration active-active, dans laquelle les deux nœuds servent les données aux clients, vous devez créer des agrégats et des volumes sur le second nœud.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, double-cliquez sur le nom de l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
3. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.

4. Cliquez sur **Ajouter agrégat**, puis créez l'agrégat.
5. Pour le nœud principal, choisissez le second nœud dans la paire HA.
6. Une fois que BlueXP a créé l'agrégat, sélectionnez-le, puis cliquez sur **Créer un volume**.
7. Entrez les détails du nouveau volume, puis cliquez sur **Créer**.

Résultat

BlueXP crée le volume sur le second nœud de la paire haute disponibilité.



Pour les paires HA déployées dans plusieurs zones de disponibilité AWS, vous devez monter le volume sur les clients en utilisant l'adresse IP flottante du nœud sur lequel réside le volume.

Après avoir créé un volume

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, vous devez utiliser 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.

Gérer les volumes existants


BlueXP vous permet de gérer des volumes et des serveurs CIFS. Il vous invite également à déplacer des volumes afin d'éviter les problèmes de capacité.



Gérer les volumes

Vous pouvez gérer les volumes en fonction de l'évolution des besoins de stockage. Vous pouvez afficher, modifier, cloner, restaurer et supprimer des volumes.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
3. Gérez vos volumes :

| Tâche | Action |
|---|---|
| Afficher des informations sur un volume | Sélectionnez un volume, puis cliquez sur Info . |
| Modifier un volume (volumes en lecture-écriture uniquement) | <ol style="list-style-type: none"> a. Sélectionnez un volume, puis cliquez sur Modifier. b. Modifiez la stratégie Snapshot du volume, la version du protocole NFS, la liste de contrôle d'accès NFS (export policy) ou les autorisations de partage, puis cliquez sur Update. <div>  Si vous avez besoin de règles Snapshot personnalisées, vous pouvez les créer à l'aide de System Manager. </div> |

| Tâche | Action |
|---|--|
| Clonez un volume | <p>a. Sélectionnez un volume, puis cliquez sur Clone.</p> <p>b. Modifiez le nom du clone selon vos besoins, puis cliquez sur Clone.</p> <p>Ce processus crée un volume FlexClone. Un volume FlexClone est une copie inscriptible, ponctuelle et efficace dans l'espace, car il utilise une petite quantité d'espace pour les métadonnées, puis ne consomme que de l'espace supplémentaire lorsque les données sont modifiées ou ajoutées.</p> <p>Pour en savoir plus sur les volumes FlexClone, consultez le "Guide de gestion du stockage logique ONTAP 9".</p> |
| Restaurer les données d'une copie Snapshot vers un nouveau volume | <p>a. Sélectionnez un volume, puis cliquez sur Restaurer à partir de la copie Snapshot.</p> <p>b. Sélectionnez une copie Snapshot, indiquez le nom du nouveau volume, puis cliquez sur Restore.</p> |
| Créez une copie Snapshot à la demande | <p>a. Sélectionnez un volume, puis cliquez sur Créer une copie snapshot.</p> <p>b. Modifiez le nom, si nécessaire, puis cliquez sur Créer.</p> |
| Obtenez la commande NFS mount | <p>a. Sélectionnez un volume, puis cliquez sur Mount Command.</p> <p>b. Cliquez sur Copier.</p> |
| Afficher l'IQN cible d'un volume iSCSI | <p>a. Sélectionnez un volume, puis cliquez sur IQN cible.</p> <p>b. Cliquez sur Copier.</p> <p>c. "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".</p> |
| Modifiez le type de disque sous-jacent | <p>a. Sélectionnez un volume, puis cliquez sur Modifier le type de disque et la stratégie de hiérarchisation.</p> <p>b. Sélectionnez le type de disque, puis cliquez sur changer.</p> <div>  <p>BlueXP déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné ou crée un nouvel agrégat pour le volume.</p> </div> |
| Modifiez la stratégie de hiérarchisation | <p>a. Sélectionnez un volume, puis cliquez sur Modifier le type de disque et la stratégie de hiérarchisation.</p> <p>b. Cliquez sur Modifier la stratégie.</p> <p>c. Sélectionnez une autre stratégie et cliquez sur Modifier.</p> <div>  <p>BlueXP déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné avec hiérarchisation, ou crée un nouvel agrégat pour le volume.</p> </div> |

| Tâche | Action |
|---------------------|---|
| Supprimer un volume | a. Sélectionnez un volume, puis cliquez sur Supprimer . b. Cliquez à nouveau sur Supprimer pour confirmer. |

Redimensionner un volume

Par défaut, une taille maximale de volume augmente automatiquement lorsqu'il est à court d'espace. La valeur par défaut est 1,000, ce qui signifie que le volume peut atteindre 11 fois sa taille. Cette valeur peut être configurée dans les paramètres d'un connecteur.

Si vous devez redimensionner le volume, vous pouvez le faire ["ONTAP System Manager"](#). Veillez à tenir compte des limites de capacité de votre système lors du redimensionnement des volumes. Accédez au ["Notes de version de Cloud Volumes ONTAP"](#) pour en savoir plus.

Modifier le serveur CIFS

Si vous modifiez vos serveurs DNS ou votre domaine Active Directory, vous devez modifier le serveur CIFS dans Cloud Volumes ONTAP pour pouvoir continuer à servir le stockage aux clients.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > Configuration CIFS**.
2. Spécifiez les paramètres du serveur CIFS :

| Tâche | Action |
|---|--|
| 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. Ifdef::gcp[] si vous configurez Google Managed Active Directory, AD est accessible par défaut avec l'adresse IP 169.254.169.254. end if::gcp[] |
| 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. |

| Tâche | Action |
|-------------------------|--|
| Unité organisationnelle | <p>Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers.</p> <ul style="list-style-type: none"> • Pour configurer Microsoft AD géré par AWS en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs,ou=corp dans ce champ. • Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs ADDC ou ou=utilisateurs ADDC dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^] • Pour configurer Google Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, entrez ou=ordinateurs,ou=Cloud dans ce champ.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud Documentation : les unités organisationnelles de Google Managed Microsoft AD"^] |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |

3. Cliquez sur **Enregistrer**.

Résultat

Cloud Volumes ONTAP met à jour le serveur CIFS avec les modifications.

Déplacer un volume

Déplacer les volumes pour optimiser l'utilisation de la capacité et les performances, et satisfaire les contrats de niveau de service.

Vous pouvez déplacer un volume dans System Manager en sélectionnant un volume et l'agrégat de destination, en commençant l'opération de déplacement de volume et, éventuellement, en surveillant la tâche de déplacement de volume. Avec System Manager, une opération de déplacement de volume se termine automatiquement.

Étapes

1. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.

Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

Pour obtenir des instructions, reportez-vous au ["Guide de migration de volumes ONTAP 9 Express"](#).

Déplacer un volume lorsque BlueXP affiche un message action requise

BlueXP peut afficher un message action requise indiquant que le déplacement d'un volume est nécessaire pour éviter les problèmes de capacité, mais que vous devez corriger vous-même le problème. Dans ce cas,

vous devez identifier comment corriger le problème, puis déplacer un ou plusieurs volumes.



BlueXP affiche ces messages action requise lorsqu'un agrégat a atteint 90 % de capacité utilisée. Si le Tiering des données est activé, les messages s'affichent lorsqu'un agrégat a atteint 80 % de capacité utilisée. Par défaut, 10 % d'espace libre est réservé pour le Tiering des données. "[En savoir plus sur le ratio d'espace libre pour le Tiering des données](#)".

Étapes

1. [Identifier la manière de corriger le problème](#).
2. En fonction de votre analyse, déplacez les volumes pour éviter les problèmes de capacité :
 - [Déplacement des volumes vers un autre système](#).
 - [Déplacement des volumes vers un autre agrégat du même système](#).

Identifiez la manière de corriger les problèmes de capacité

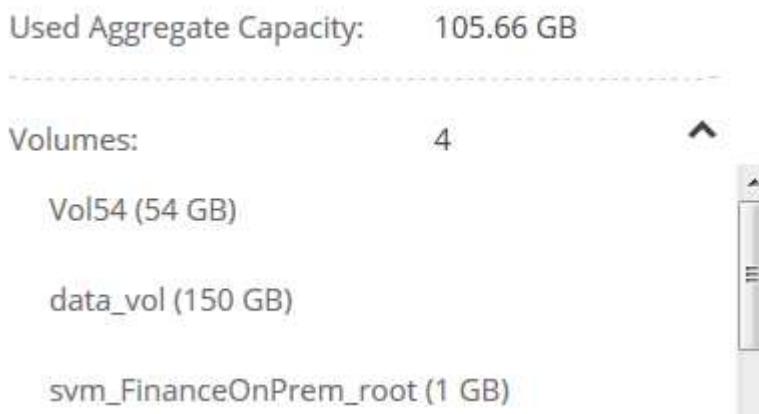
Si BlueXP ne peut pas fournir de recommandations pour le déplacement d'un volume afin d'éviter tout problème de capacité, vous devez identifier les volumes que vous devez déplacer et si vous devez les déplacer vers un autre agrégat du même système ou vers un autre système.

Étapes

1. Consultez les informations avancées du message Action requise pour identifier l'agrégat ayant atteint sa limite de capacité.

Par exemple, l'information avancée devrait dire quelque chose de similaire à ce qui suit : aggr1 global a atteint sa limite de capacité.

2. Identifiez un ou plusieurs volumes à sortir de l'agrégat :
 - a. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
 - b. Sélectionnez l'agrégat, puis cliquez sur **Info**.
 - c. Développez la liste des volumes.



- d. Passez en revue la taille de chaque volume et choisissez un ou plusieurs volumes pour sortir de l'agrégat.

Vous devez choisir des volumes suffisamment volumineux pour libérer de l'espace dans l'agrégat afin d'éviter d'autres problèmes de capacité à l'avenir.

3. Si le système n'a pas atteint la limite de disque, vous devez déplacer les volumes vers un agrégat existant ou vers un nouvel agrégat sur le même système.

Pour plus de détails, voir ["Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité"](#).

4. Si le système a atteint la limite de disque, effectuez l'une des opérations suivantes :

- a. Supprimez tous les volumes inutilisés.
- b. Réorganiser les volumes pour libérer de l'espace sur un agrégat.

Pour plus de détails, voir ["Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité"](#).

- c. Déplacez deux volumes ou plus vers un autre système disposant d'espace.

Pour plus de détails, voir ["Déplacement des volumes vers un autre système pour éviter les problèmes de capacité"](#).

Déplacement des volumes vers un autre système pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre système Cloud Volumes ONTAP pour éviter les problèmes de capacité. Vous devrez peut-être le faire si le système a atteint sa limite de disque.

Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
Moving a volume is necessary to avoid capacity issues; however, BlueXP cannot perform this action for you because the system has reached the disk limit.
```

.Étapes

- . Identifiez un système Cloud Volumes ONTAP doté de la capacité disponible ou déployez un nouveau système.
- . Faites glisser et déposez l'environnement de travail source sur l'environnement de travail cible pour effectuer une réplication unique du volume.

+

Pour plus de détails, voir ["Réplication des données entre les systèmes"](#).

1. Accédez à la page Etat de la réplication, puis rompez la relation SnapMirror pour convertir le volume répliqué d'un volume de protection des données en volume en lecture/écriture.

Pour plus de détails, voir ["Gestion des planifications et des relations de réplication des données"](#).

2. Configurez le volume pour l'accès aux données.

Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données, reportez-vous à la section ["Guide rapide de reprise après incident de volumes ONTAP 9"](#).

3. Supprimez le volume d'origine.

Pour plus de détails, voir ["Gérer les volumes"](#).

Déplacez les volumes vers un autre agrégat pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre agrégat pour éviter les problèmes de capacité.

Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

Moving two or more volumes is necessary to avoid capacity issues; however, BlueXP cannot perform this action for you.

.Étapes

. Vérifiez si un agrégat existant a la capacité disponible pour les volumes que vous devez déplacer :

- +
- .. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
- .. Sélectionnez chaque agrégat, cliquez sur **Info**, puis affichez la capacité disponible (capacité d'agrégat moins la capacité d'agrégat utilisée).

+

aggr1

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

1. Si nécessaire, ajoutez des disques à un agrégat existant :
 - a. Sélectionner l'agrégat, puis cliquer sur **Add disks**.
 - b. Sélectionnez le nombre de disques à ajouter, puis cliquez sur **Ajouter**.

2. Si aucun agrégat n'a de capacité disponible, créez un nouvel agrégat.

Pour plus de détails, voir ["Création d'agrégats"](#).

3. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.
4. Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

Pour obtenir des instructions, reportez-vous au ["Guide de migration de volumes ONTAP 9 Express"](#).

Raisons de la lenteur d'un déplacement de volume

Le déplacement d'un volume peut prendre plus de temps que ce que vous attendez si l'une des conditions suivantes est vraie pour Cloud Volumes ONTAP :

- Le volume est un clone.

- Le volume est parent d'un clone.
- L'agrégat source ou de destination dispose d'un seul disque dur (st1) à débit optimisé.
- L'un des agrégats utilise un ancienne schéma de nommage des objets. Les deux agrégats doivent utiliser le même format de nom.

Une ancienne méthode de nommage est utilisée si le Tiering des données était activé sur un agrégat dans la version 9.4 ou antérieure.

- Les paramètres de chiffrement ne correspondent pas aux agrégats source et de destination, ou une nouvelle clé est en cours.
- L'option *-Tiering-policy* a été spécifiée sur le déplacement de volumes pour modifier la règle de Tiering.
- L'option *-generate-destination-key* a été spécifiée lors du déplacement du volume.

Tiering des données inactives vers un stockage objet à faible coût

Vous pouvez réduire les coûts de stockage pour Cloud Volumes ONTAP en combinant un Tier de performance SSD ou HDD pour les données actives avec un Tier de capacité de stockage objet pour les données inactives. La hiérarchisation des données est optimisée par la technologie FabricPool. Pour une vue d'ensemble de haut niveau, voir "[Vue d'ensemble du hiérarchisation des données](#)".

Pour configurer le Tiering des données, vous devez procéder comme suit :

1

Choisissez une configuration prise en charge

La plupart des configurations sont prises en charge. Si vous avez un système Cloud Volumes ONTAP exécutant la version la plus récente, vous devriez avoir un bon choix. ["En savoir plus >>"](#).

2

Assurez la connectivité entre le Cloud Volumes ONTAP et le stockage objet

- Pour AWS, vous avez besoin d'un terminal VPC vers S3. [En savoir plus >>](#).
- Pour Azure, vous n'aurez rien à faire tant que BlueXP dispose des autorisations requises. [En savoir plus >>](#).
- Pour Google Cloud, vous devez configurer le sous-réseau pour Private Google Access et configurer un compte de service. [En savoir plus >>](#).

3

Assurez-vous que vous disposez d'un agrégat sur lequel le Tiering est activé

Le Tiering des données doit être activé sur un agrégat pour que le Tiering des données puisse être activé sur un volume. Vous devez connaître les exigences relatives aux nouveaux volumes et aux volumes existants. [En savoir plus >>](#).

4

Choisissez une règle de Tiering lors de la création, de la modification ou de la réplication d'un volume

BlueXP vous invite à choisir une stratégie de hiérarchisation lorsque vous créez, modifiez ou répliquez un volume.

- "Hiérarchisation des données sur les volumes en lecture-écriture"
- "Hiérarchisation des données sur les volumes de protection des données"



Quelles sont les's non requis pour le Tiering des données ?

- Vous n'avez pas besoin d'installer une licence pour activer le Tiering des données.
- Il n'est pas nécessaire de créer un magasin d'objets pour le Tier de capacité. BlueXP le fait pour vous.
- Inutile d'activer le Tiering des données au niveau du système.

BlueXP crée un magasin d'objets pour les données inactives lorsque le système est créé, [tant qu'il n'y a aucun problème de connectivité ou d'autorisation](#). Après cela, il vous suffit d'activer le Tiering des données sur les volumes (et dans certains cas, [sur les agrégats](#)).

Configurations prenant en charge le tiering des données

Vous pouvez activer le Tiering des données lors de l'utilisation de configurations et de fonctionnalités spécifiques.

Prise en charge dans AWS

- Le Tiering des données est pris en charge dans AWS à partir de Cloud Volumes ONTAP 9.2.
- Le Tier de performance peut être des SSD polyvalents (gp3 ou gp2) ou des SSD IOPS provisionnés (io1).



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).

Prise en charge dans Azure

- Le Tiering des données est pris en charge par Azure comme suit :
 - Version 9.4 avec des systèmes à un seul nœud
 - Version 9.6 avec paires haute disponibilité
- Le Tier de performance peut être des disques gérés SSD premium, des disques gérés SSD standard ou des disques gérés HDD standard.

Prise en charge dans Google Cloud

- Le Tiering des données est pris en charge dans Google Cloud à partir de Cloud Volumes ONTAP 9.6.
- Le Tier de performance peut être soit des disques persistants SSD, soit des disques persistants équilibrés, soit des disques persistants standard.

Interopérabilité des fonctionnalités

- Le Tiering des données est pris en charge grâce aux technologies de chiffrement.
- Le provisionnement fin doit être activé sur les volumes.

De formation

Selon le fournisseur cloud, certaines connexions et autorisations doivent être configurées de sorte que Cloud

Volumes ONTAP puisse transférer les données inactives vers le stockage objet.

Conditions requises pour le Tiering des données inactives vers AWS S3

Assurez-vous que Cloud Volumes ONTAP dispose d'une connexion 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 ?"](#).

Il est nécessaire de déplacer les données inactives vers le stockage Azure Blob

Vous n'avez pas besoin de configurer de connexion entre le niveau de performance et le niveau de capacité tant que BlueXP dispose des autorisations requises. BlueXP active un point de terminaison de service VNet pour vous si le rôle personnalisé du connecteur possède les autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

Les autorisations sont incluses dans le rôle personnalisé par défaut. ["Afficher l'autorisation Azure pour le connecteur"](#)

Il est donc nécessaire de transférer les données inactives vers un compartiment Google Cloud Storage

- Le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès privé à Google. Pour obtenir des instructions, reportez-vous à la section ["Documentation Google Cloud : configuration de Private Google Access"](#).
- Un compte de service doit être joint à Cloud Volumes ONTAP.

["Découvrez comment configurer ce compte de service"](#).

Vous êtes invité à sélectionner ce compte de service lorsque vous créez un environnement de travail Cloud Volumes ONTAP.

Si vous ne sélectionnez pas de compte de service pendant le déploiement, vous devez arrêter Cloud Volumes ONTAP, accédez à la console Google Cloud, puis joindre le compte de service aux instances Cloud Volumes ONTAP. Vous pouvez ensuite activer le Tiering des données, comme décrit dans la section suivante.

- Pour chiffrer le compartiment avec des clés de chiffrement gérées par le client, activez le compartiment de stockage Google Cloud pour utiliser la clé.

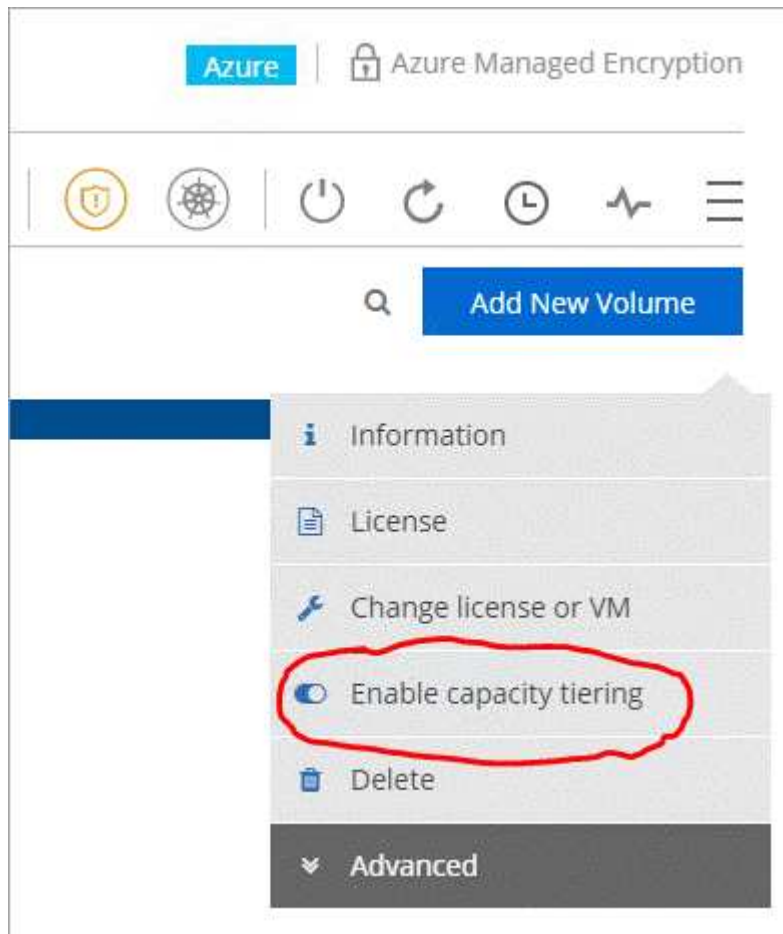
["Découvrez comment utiliser des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP"](#).

Activation du Tiering des données après la mise en œuvre des exigences

BlueXP crée un magasin d'objets pour les données inactives lorsque le système est créé, tant qu'il n'y a aucun problème de connectivité ou d'autorisation. Si vous n'avez pas mis en œuvre les exigences énumérées ci-dessus jusqu'à ce que vous ayez créé le système, vous devrez activer manuellement le Tiering, qui crée le magasin d'objets.

Étapes

1. [Assurez-vous que vous avez satisfait à toutes les exigences.](#)
2. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
3. Sur la page Canvas, double-cliquez sur le nom de l'instance Cloud Volumes ONTAP.
4. Cliquez sur l'icône de menu et sélectionnez **Activer la hiérarchisation de capacité.**



Cette option ne s'affiche que si le Tiering des données n'a pas pu être activé lorsque BlueXP a créé le système.

Dans Google Cloud, un compte de service doit être joint à Cloud Volumes ONTAP avant que cette option ne s'affiche. [Assurez-vous que vous avez satisfait à toutes les exigences.](#)

5. Cliquez sur **Activer** pour que BlueXP puisse créer le magasin d'objets que ce système Cloud Volumes ONTAP utilisera pour les données hiérarchisées.

S'assurer que le Tiering est activé sur les agrégats

Le Tiering des données doit être activé sur un agrégat pour que le Tiering des données puisse être activé sur

un volume. Vous devez connaître les exigences relatives aux nouveaux volumes et aux volumes existants.

- **Nouveaux volumes**

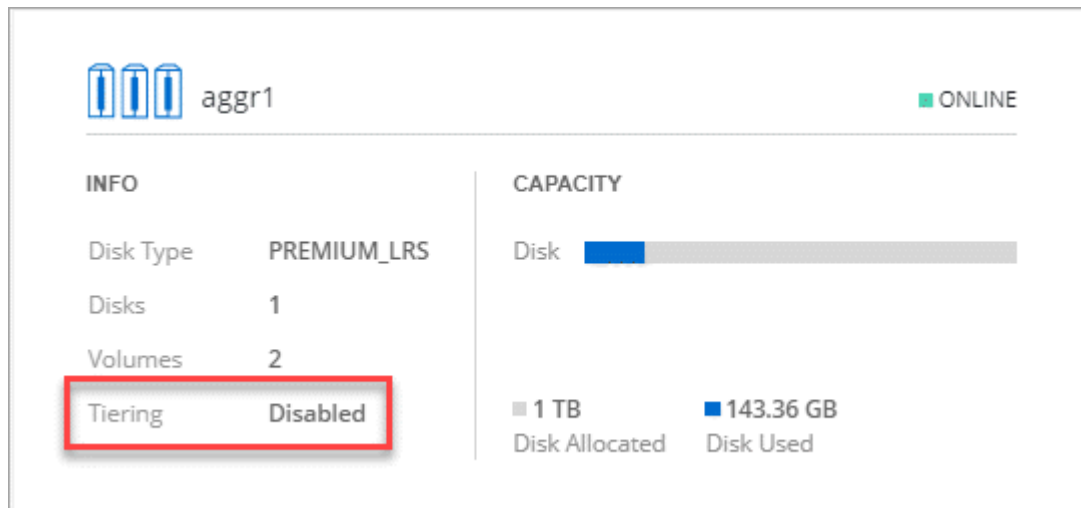
Si vous activez le Tiering des données sur un nouveau volume, vous n'avez plus à vous soucier de l'activation du Tiering des données dans un agrégat. BlueXP crée le volume sur un agrégat existant dont le Tiering est activé ou crée un nouvel agrégat pour le volume si un agrégat n'existe pas déjà.

- **Volumes existants**

Pour activer le Tiering des données sur un volume existant, vous devez vous assurer que le Tiering des données est activé sur l'agrégat sous-jacent. Si le Tiering des données n'est pas activé sur l'agrégat existant, vous devez utiliser System Manager pour associer un agrégat existant au magasin d'objets.

Étapes pour vérifier si la hiérarchisation est activée sur un agrégat

1. Ouvrez l'environnement de travail dans BlueXP.
2. Cliquez sur l'icône du menu, puis sur **Avancé**, puis sur **attribution avancée**.
3. Vérifiez que le Tiering est activé ou désactivé sur l'agrégat.



Les étapes permettant d'activer la hiérarchisation sur un agrégat

1. Dans System Manager, cliquez sur **stockage > niveaux**.
2. Cliquez sur le menu d'action de l'agrégat et sélectionnez **attacher Cloud tiers**.
3. Sélectionnez le Tier de cloud à attacher et cliquez sur **Enregistrer**.

Et la suite ?

Vous pouvez désormais activer le Tiering des données sur les volumes, nouveaux ou existants, comme expliqué dans la section suivante.

Tiering des données à partir de volumes en lecture/écriture

Cloud Volumes ONTAP peut déplacer les données inactives sur des volumes en lecture/écriture vers un stockage objet économique, libérant ainsi le Tier de performance pour les données actives.

Étapes

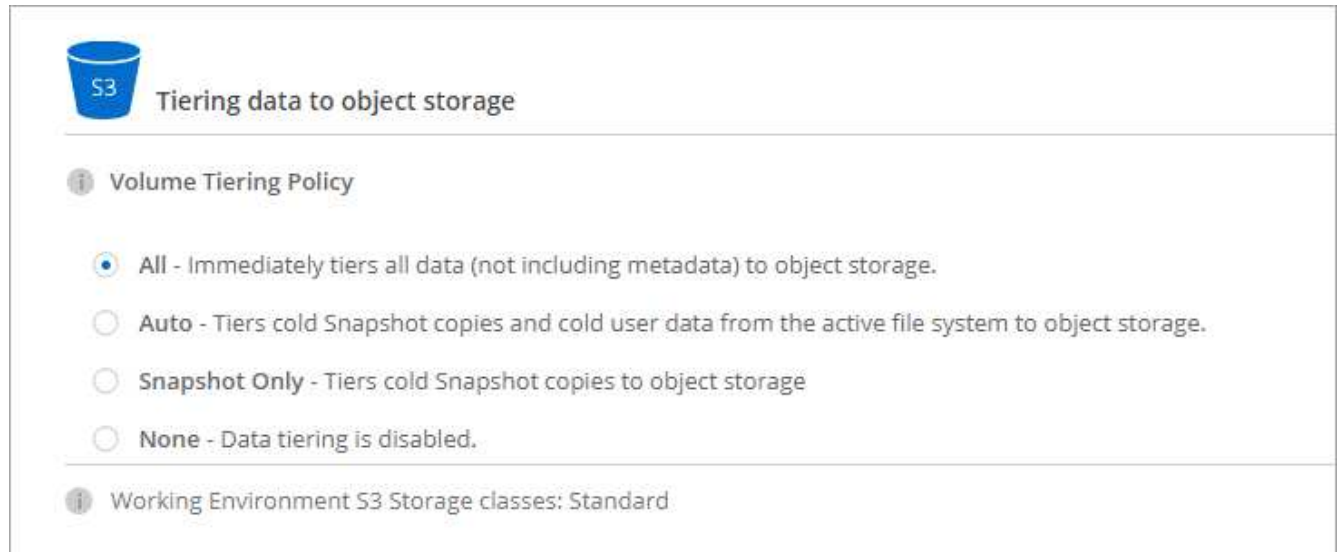
1. Dans l'environnement de travail, créez un nouveau volume ou modifiez le niveau d'un volume existant :

| Tâche | Action |
|-----------------------------|--|
| Créer un nouveau volume | Cliquez sur Ajouter nouveau volume . |
| Modifier un volume existant | Sélectionnez le volume et cliquez sur Modifier le type de disque et la stratégie de hiérarchisation . |

2. Sélectionnez une règle de hiérarchisation.

Pour obtenir une description de ces politiques, reportez-vous à la section "[Vue d'ensemble du hiérarchisation des données](#)".

Exemple



BlueXP crée un nouvel agrégat pour le volume si un agrégat sur lequel le Tiering des données est déjà activé.

Tiering des données à partir des volumes de protection des données

Cloud Volumes ONTAP permet de hiérarchiser les données d'un volume de protection des données vers un niveau de capacité. Si vous activez le volume de destination, les données passent progressivement au niveau de performance tel qu'il est lu.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail auquel vous souhaitez répliquer le volume.
3. Suivez les invites jusqu'à ce que vous atteigniez la page de hiérarchisation et que vous activiez le tiering des données vers le stockage d'objets.

Exemple



S3 Tiering

What are storage tiers?

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

Pour obtenir de l'aide sur la réplication des données, voir ["Réplication des données depuis et vers le cloud"](#).

Modification de la classe de stockage pour les données hiérarchisées

Une fois déployé Cloud Volumes ONTAP, vous pouvez réduire les coûts de stockage en modifiant la classe de stockage pour les données inactives inutilisées depuis 30 jours. Les coûts d'accès sont plus élevés si vous accédez aux données. Vous devez donc prendre en compte ces coûts avant de changer de classe de stockage.

it stockage des données hiérarchisées est disponible dans l'ensemble du système, et non dans chaque volume.

Pour plus d'informations sur les classes de stockage prises en charge, reportez-vous à la section ["Vue d'ensemble du hiérarchisation des données"](#).

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **classes de stockage** ou **stockage Blob Storage Tiering**.
2. Choisissez une classe de stockage, puis cliquez sur **Enregistrer**.

Modification du ratio d'espace libre pour le Tiering des données

Le ratio d'espace libre pour le Tiering des données définit la quantité d'espace disponible requise sur les disques SSD/HDD Cloud Volumes ONTAP lors du Tiering des données vers le stockage objet. Le paramètre par défaut est 10 % d'espace libre, mais vous pouvez ajuster le paramètre en fonction de vos besoins.

Par exemple, vous pouvez choisir un espace libre inférieur à 10 % pour vérifier que vous utilisez la capacité achetée. BlueXP peut ensuite vous acheter des disques supplémentaires lorsque vous avez besoin de capacité supplémentaire (jusqu'à atteindre la limite de disques pour l'agrégat).



Si l'espace est insuffisant, Cloud Volumes ONTAP ne peut pas déplacer les données et vous risquez de subir une dégradation des performances. Toute modification doit être effectuée avec précaution. Si vous ne savez pas ce que vous devez faire, n'hésitez pas à contacter le service de support NetApp.

Le ratio est important pour les scénarios de reprise d'activité, car lors de la lecture des données à partir du magasin d'objets, Cloud Volumes ONTAP déplace les données vers des disques SSD/HDD pour de meilleures performances. Si l'espace est insuffisant, Cloud Volumes ONTAP ne peut pas déplacer les données. Prenez en compte ces changements pour répondre aux besoins de votre entreprise.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône **Paramètres**, puis sélectionnez **Paramètres du connecteur**.



2. Sous **capacité**, cliquez sur **seuils de capacité d'agrégat - ratio d'espace libre pour le Tiering des données**.
3. Modifiez le ratio d'espace libre en fonction de vos besoins et cliquez sur **Enregistrer**.

Modification de la période de refroidissement de la règle de hiérarchisation automatique

Si vous avez activé le Tiering des données sur un volume Cloud Volumes ONTAP à l'aide de la règle *auto* Tiering, vous pouvez ajuster la période de refroidissement par défaut en fonction des besoins de votre entreprise. Cette action est prise en charge à l'aide de l'API uniquement.

La période de refroidissement correspond au nombre de jours pendant lesquels les données utilisateur d'un volume doivent rester inactives avant qu'elles ne soient considérées comme « inactives » et déplacées vers le stockage objet.

La période de refroidissement par défaut de la règle de hiérarchisation automatique est de 31 jours. Vous pouvez modifier la période de refroidissement comme suit :

- 9.8 ou ultérieure: 2 jours à 183 jours
- 9.7 ou antérieure: 2 jours à 63 jours

Étape

1. Utilisez le paramètre *minimumCoolingDays* avec votre demande d'API lors de la création d'un volume ou de la modification d'un volume existant.

Connectez une LUN à un hôte

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, ce qui n'implique aucune gestion. Une fois le volume créé, utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes.

Notez ce qui suit :

- La gestion automatique de la capacité de BlueXP ne s'applique pas aux LUN. Lorsque BlueXP crée un LUN, il désactive la fonction Autogrow.
- Vous pouvez créer des LUN supplémentaires depuis System Manager ou l'interface de ligne de commandes.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
3. Sélectionnez un volume, puis cliquez sur **IQN cible**.
4. Cliquez sur **Copy** pour copier le nom IQN.
5. Configurez une connexion iSCSI de l'hôte vers le LUN.

- ["Configuration iSCSI express ONTAP 9 pour Red Hat Enterprise Linux : démarrage des sessions iSCSI avec la cible"](#)
- ["Configuration iSCSI express de ONTAP 9 pour Windows : démarrage des sessions iSCSI avec la cible"](#)
- ["Configuration de l'hôte SAN ONTAP"](#)

Accélération de l'accès aux données avec les volumes FlexCache

Un volume FlexCache est un volume de stockage qui met en cache les données lues par NFS à partir d'un volume d'origine (ou source). Les lectures suivantes des données mises en cache permettent un accès plus rapide à ces données.

Les volumes FlexCache peuvent être utilisés pour accélérer l'accès aux données ou pour décharger le trafic des volumes fortement sollicités. Les volumes FlexCache contribuent à améliorer les performances, en particulier lorsque les clients doivent accéder de façon répétée aux mêmes données, car elles peuvent être servies directement sans avoir à accéder au volume d'origine. Les volumes FlexCache fonctionnent parfaitement pour les charges de travail système intensives en lecture.

BlueXP n'offre pas pour le moment la gestion des volumes FlexCache, mais vous pouvez utiliser l'interface de ligne de commande ONTAP ou ONTAP System Manager pour créer et gérer des volumes FlexCache :

- ["Guide de puissance des volumes FlexCache pour un accès plus rapide aux données"](#)
- ["Création de volumes FlexCache dans System Manager"](#)

À partir de la version 3.7.2, BlueXP génère une licence FlexCache pour tous les nouveaux systèmes Cloud Volumes ONTAP. La licence inclut une limite d'utilisation de 500 Gio.



Administration d'agrégats

Créer des agrégats

Vous pouvez créer des agrégats vous-même ou laisser BlueXP le faire pour vous lors de la création de volumes. L'avantage de créer des agrégats vous-même est de choisir la taille du disque sous-jacent, ce qui vous permet de dimensionner l'agrégat en fonction de la capacité ou des performances requises.



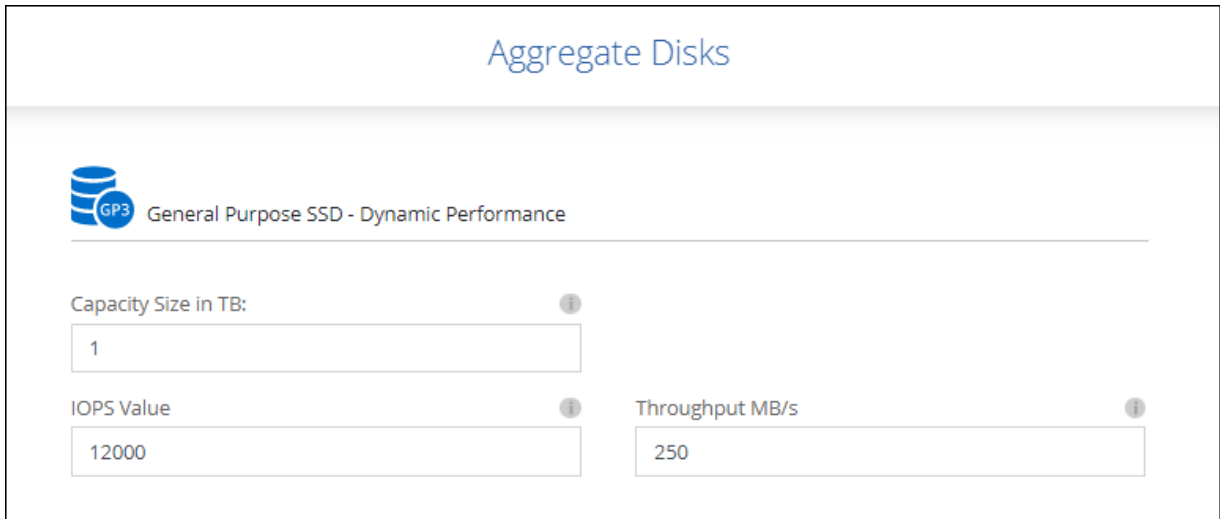
Tous les disques et agrégats doivent être créés et supprimés directement depuis BlueXP. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Étapes


1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, double-cliquez sur le nom de l'instance Cloud Volumes ONTAP dans laquelle vous souhaitez gérer les agrégats.
3. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
4. Cliquez sur **Ajouter agrégat**, puis spécifiez les détails de l'agrégat.

AWS

- Si vous êtes invité à choisir un type et une taille de disque, reportez-vous à la section ["Planification de votre configuration Cloud Volumes ONTAP dans AWS"](#).
- Si vous êtes invité à saisir la taille de la capacité de l'agrégat, vous créez un agrégat sur une configuration prenant en charge la fonctionnalité Amazon EBS Elastic volumes. La capture d'écran suivante montre un exemple d'un nouvel agrégat composé de disques gp3.



Aggregate Disks

 General Purpose SSD - Dynamic Performance

Capacity Size in TB:

IOPS Value

Throughput MB/s

["En savoir plus sur la prise en charge d'Elastic volumes"](#).

Azure

Pour obtenir de l'aide sur le type et la taille de disque, reportez-vous à la section ["Planification de votre configuration Cloud Volumes ONTAP dans Azure"](#).

Google Cloud

Pour obtenir de l'aide sur le type et la taille de disque, reportez-vous à la section ["Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud"](#).

5. Cliquez sur **Go**, puis sur **approuver et acheter**.

Gestion des agrégats

Gérez vous-même les agrégats en ajoutant des disques, en affichant les informations sur les agrégats et en les supprimant.



Tous les disques et agrégats doivent être créés et supprimés directement depuis BlueXP. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Avant de commencer


Si vous souhaitez supprimer un agrégat, vous devez d'abord supprimer les volumes de l'agrégat.

Description de la tâche

Si un agrégat manque d'espace de stockage, il est possible de déplacer des volumes vers un autre agrégat via System Manager.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP dans lequel vous souhaitez gérer les agrégats.
3. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
4. Gérez vos agrégats :

| Tâche | Action |
|---|---|
| Afficher des informations sur un agrégat | Sélectionnez un agrégat et cliquez sur Info . |
| Créez un volume sur un agrégat spécifique | Sélectionnez un agrégat et cliquez sur Create volume . |
| Ajoutez des disques à un agrégat | <div><div><div>a. Sélectionnez un agrégat et cliquez sur Add disks.</div><div>b. Sélectionnez le nombre de disques que vous souhaitez ajouter et cliquez sur Ajouter.</div></div><div> Tous les disques qui composent un agrégat doivent être de la même taille.</div></div> |
| Augmentation de la capacité d'un agrégat prenant en charge Amazon EBS Elastic volumes | <div><div><div>a. Sélectionnez un agrégat et cliquez sur augmenter la capacité.</div><div>b. Saisissez la capacité supplémentaire que vous souhaitez ajouter, puis cliquez sur Ajouter.</div></div><div><p>Notez que vous devez augmenter la capacité de l'agrégat d'au moins 256 Gio ou 10 % de la taille de l'agrégat.</p><p>Par exemple, si vous avez un agrégat de 1.77 Tio, 10 % est égal au 181 Gio. Soit plus faible que 256 Gio, donc la taille de l'agrégat doit être augmentée de 256 Gio au minimum.</p></div></div> |
| Supprimer un agrégat | <div><div><div>a. Sélectionnez un agrégat qui ne contient aucun volume et cliquez sur Supprimer.</div><div>b. Cliquez à nouveau sur Supprimer pour confirmer.</div></div></div> |

Gérer les paramètres de capacité sur un connecteur

Chaque connecteur dispose de paramètres qui déterminent la façon dont il gère la capacité d'agrégat pour Cloud Volumes ONTAP.

Ces paramètres affectent tous les systèmes Cloud Volumes ONTAP gérés par un connecteur. Si vous avez un autre connecteur, il peut être configuré différemment.

Autorisations requises

Des privilèges d'administrateur de compte sont requis pour modifier les paramètres de connecteur.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.
2. Sous **Capacity**, modifiez l'un des paramètres suivants :

Mode de gestion de la capacité

Choisissez si BlueXP vous informe des décisions relatives à la capacité de stockage ou si BlueXP gère automatiquement les besoins en capacité pour vous.

["Découvrez le fonctionnement du mode de gestion de la capacité"](#).

Rapport d'espace libre

Déclenche une notification lorsque le taux d'espace libre sur un agrégat chute en dessous du seuil spécifié.

Le rapport d'espace libre est calculé comme suit :

(capacité de l'agrégat : capacité totale utilisée sur l'agrégat) / capacité de l'agrégat

Ratio d'espace libre pour le Tiering des données

Définit la quantité d'espace disponible requise sur le Tier de performance (disques) lors du Tiering des données vers un Tier de capacité (stockage objet).

Le ratio est important pour les scénarios de reprise après incident. Lorsque les données sont lues depuis le niveau de capacité, Cloud Volumes ONTAP les déplace vers le Tier de performance pour de meilleures performances. Si l'espace est insuffisant, Cloud Volumes ONTAP ne peut pas déplacer les données.

3. Cliquez sur **Enregistrer**.

Administration des machines virtuelles de stockage

Gérez vos machines virtuelles de stockage dans BlueXP

Une VM de stockage est une machine virtuelle exécutée dans ONTAP, qui fournit des services de données et de stockage à vos clients. Vous pouvez le connaître comme *SVM* ou *vserver*. La solution Cloud Volumes ONTAP est configurée par défaut avec une seule machine virtuelle de stockage, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

Nombre de machines virtuelles de stockage pris en charge

Plusieurs machines virtuelles de stockage sont prises en charge dans certaines configurations. Accédez au ["Notes de version de Cloud Volumes ONTAP"](#) Pour vérifier le nombre de machines virtuelles de stockage pris en charge pour votre version de Cloud Volumes ONTAP.

Utilisation de plusieurs machines virtuelles de stockage

BlueXP prend en charge toutes les machines virtuelles de stockage supplémentaires que vous créez à partir de System Manager ou de l'interface de ligne de commande.

Par exemple, l'image suivante montre comment choisir une VM de stockage lors de la création d'un volume.

Details & Protection

Storage VM Name

svm_name1

Volume Name

Size (GiB)

Volume size

Snapshot Policy

default

Default Policy

L'image suivante montre comment choisir une VM de stockage lors de la réplication d'un volume sur un autre système.

Destination Volume Name

volume_copy

Destination Storage VM Name

svm_name1

Destination Aggregate

Automatically select the best aggregate

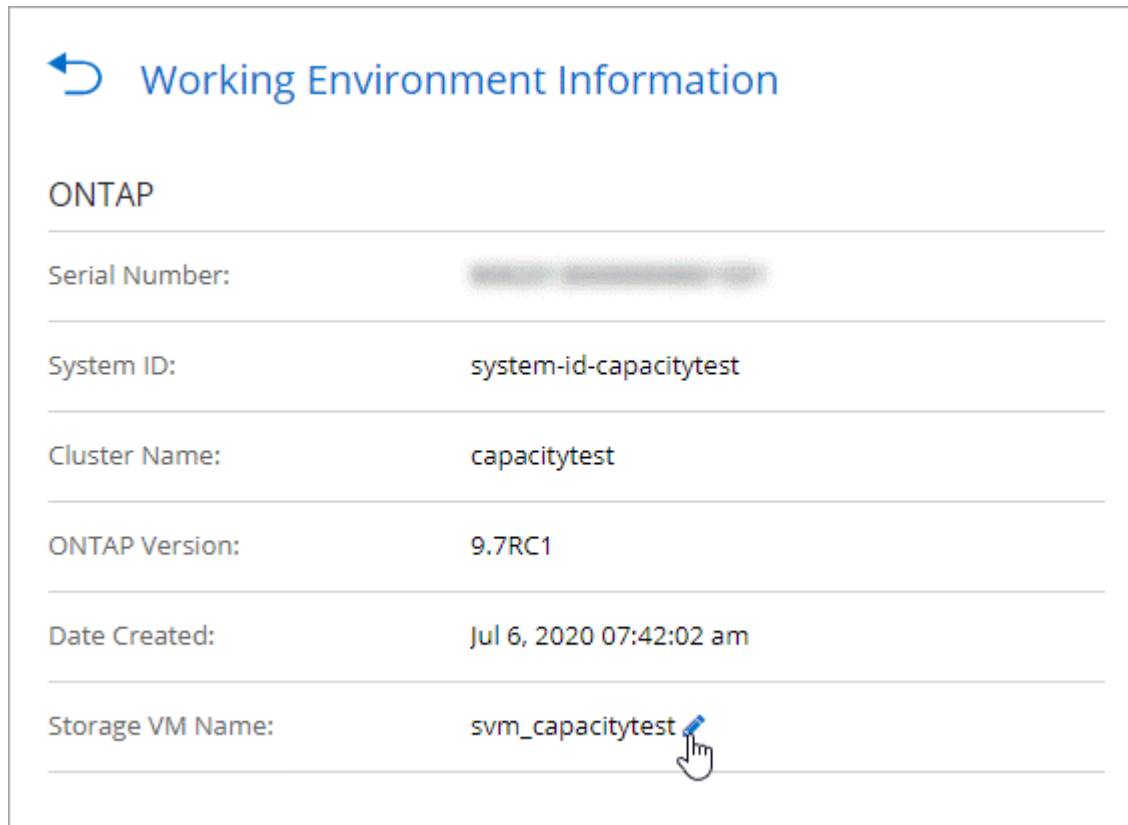
Modifier le nom de la VM de stockage par défaut


BlueXP nomme automatiquement la machine virtuelle de stockage unique qu'elle crée pour Cloud Volumes ONTAP. Si vous avez des normes de nommage très strictes, vous pouvez modifier le nom de la machine virtuelle de stockage. Par exemple, vous pouvez indiquer le nom des machines virtuelles de stockage dans vos clusters ONTAP.

Si vous avez créé des machines virtuelles de stockage supplémentaires pour Cloud Volumes ONTAP, vous ne pouvez pas renommer ces machines virtuelles de BlueXP. Pour ce faire, vous devez utiliser System Manager ou l'interface de ligne de commandes directement dans Cloud Volumes ONTAP.


Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur l'icône d'édition située à droite du nom de la VM de stockage.



 Working Environment Information

ONTAP


Serial Number: 

System ID: system-id-capacitytest

Cluster Name: capacitytest

ONTAP Version: 9.7RC1

Date Created: Jul 6, 2020 07:42:02 am

Storage VM Name: svm_capacitytest 

3. Dans la boîte de dialogue Modifier le nom du SVM, modifiez le nom, puis cliquez sur **Enregistrer**.

Gérer les machines virtuelles de stockage pour la reprise après incident

BlueXP ne propose pas de prise en charge de la configuration ou de l'orchestration pour la reprise après incident des machines virtuelles de stockage. Vous devez utiliser System Manager ou l'interface de ligne de commandes.

- ["Guide de préparation rapide pour la reprise après incident du SVM"](#)
- ["Guide de reprise après incident de SVM Express"](#)

Créez des machines virtuelles de stockage destinées aux données pour Cloud Volumes ONTAP dans AWS

Une VM de stockage est une machine virtuelle exécutée dans ONTAP, qui fournit des services de données et de stockage à vos clients. Vous pouvez le connaître comme *SVM* ou *vserver*. La solution Cloud Volumes ONTAP est configurée par défaut avec une seule machine virtuelle de stockage, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

Pour créer des machines virtuelles de stockage supplémentaires qui assurent le service des données, vous devez allouer des adresses IP dans AWS, puis exécuter des commandes ONTAP en fonction de votre configuration Cloud Volumes ONTAP.

Nombre de machines virtuelles de stockage pris en charge

Plusieurs machines virtuelles de stockage sont prises en charge avec des configurations Cloud Volumes ONTAP spécifiques à partir de la version 9.7. Accédez au "[Notes de version de Cloud Volumes ONTAP](#)" Pour vérifier le nombre de machines virtuelles de stockage pris en charge pour votre version de Cloud Volumes ONTAP.

Toutes les autres configurations Cloud Volumes ONTAP prennent en charge une VM de stockage servant aux données et une VM de stockage de destination utilisée pour la reprise après incident. Vous pouvez activer la machine virtuelle de stockage de destination pour accéder aux données en cas de panne sur la machine virtuelle de stockage source.

Vérifiez les limites de votre configuration

Chaque instance EC2 prend en charge un nombre maximal d'adresses IPv4 privées par interface réseau. Vous devez vérifier la limite avant d'allouer des adresses IP dans AWS pour la nouvelle machine virtuelle de stockage.

Étapes

1. Allez à "[Limites de stockage dans les notes de mise à jour de Cloud Volumes ONTAP](#)".
2. Identifiez le nombre maximal d'adresses IP par interface pour votre type d'instance.
3. Notez ce nombre, car vous en aurez besoin dans la section suivante lorsque vous allouez des adresses IP dans AWS.

Allouez des adresses IP dans AWS

Les adresses IPv4 privées doivent être attribuées au port e0a dans AWS avant de créer les LIF du nouveau VM de stockage.

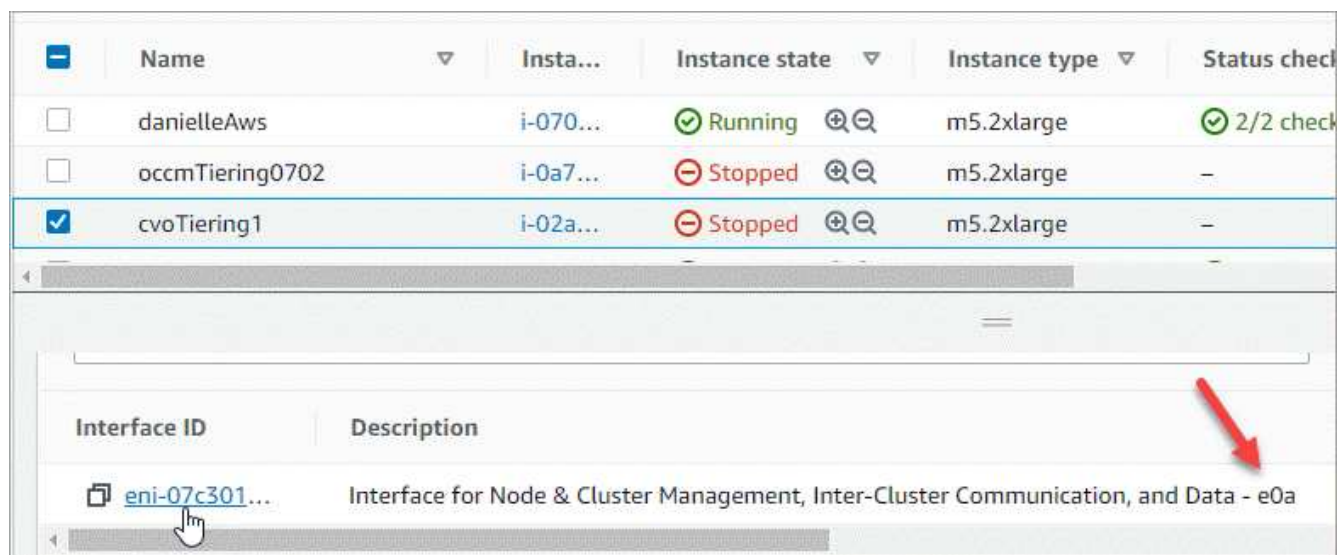
Notez qu'une LIF de gestion en option pour une machine virtuelle de stockage nécessite une adresse IP privée sur un système à un seul nœud et sur une paire haute disponibilité dans une même zone de disponibilité. Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

Étapes

1. Connectez-vous à AWS et ouvrez le service EC2.
2. Sélectionnez l'instance Cloud Volumes ONTAP et cliquez sur **réseau**.

Si vous créez une machine virtuelle de stockage sur une paire haute disponibilité, sélectionnez le nœud 1.

3. Faites défiler jusqu'à **interfaces réseau** et cliquez sur **ID d'interface** pour le port e0a.



4. Sélectionnez l'interface réseau et cliquez sur **actions > gérer les adresses IP**.

5. Développer la liste des adresses IP pour e0a.

6. Vérifiez les adresses IP :

- Comptez le nombre d'adresses IP allouées pour confirmer que le port a de la place pour les adresses IP supplémentaires.

Dans la section précédente de cette page, vous devez avoir identifié le nombre maximal d'adresses IP prises en charge par interface.

- Facultatif : accédez à l'interface de ligne de commande pour Cloud Volumes ONTAP et exécutez **network interface show** pour confirmer que chacune de ces adresses IP est utilisée.

Si une adresse IP n'est pas utilisée, vous pouvez l'utiliser avec la nouvelle machine virtuelle de stockage.

7. De retour dans la console AWS, cliquez sur **attribuer une nouvelle adresse IP** pour attribuer des adresses IP supplémentaires en fonction de la quantité nécessaire pour la nouvelle VM de stockage.

- Système à un seul nœud : une adresse IP privée secondaire inutilisée est requise.

Une adresse IP privée secondaire facultative est requise si vous souhaitez créer une LIF de gestion sur la machine virtuelle de stockage.

- Paire HA dans un seul groupe de disponibilité : une adresse IP privée secondaire inutilisée est requise sur le nœud 1.

Une adresse IP privée secondaire facultative est requise si vous souhaitez créer une LIF de gestion sur la machine virtuelle de stockage.

- Paire HA dans plusieurs AZS : une adresse IP secondaire non utilisée est requise sur chaque nœud.

8. Si vous attribuez l'adresse IP sur une paire HA dans une même AZ, activez **Autoriser la réaffectation d'adresses IPv4 privées secondaires**.

9. Cliquez sur **Enregistrer**.

10. Si vous avez une paire haute disponibilité dans plusieurs AZS, vous devez répéter ces étapes pour le nœud 2.

Créez une VM de stockage sur un système à un seul nœud

Cette procédure permet de créer une nouvelle machine virtuelle de stockage sur un système à un seul nœud. Une adresse IP privée est nécessaire pour créer une LIF NAS et une autre adresse IP privée facultative est requise si vous souhaitez créer une LIF de gestion.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Créer une LIF NAS.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Où *private_ip_x* est une adresse IP privée secondaire inutilisée sur e0a.

3. Facultatif : créez une LIF de gestion de machine virtuelle de stockage.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Où *private_ip_y* est une autre adresse IP privée secondaire inutilisée sur e0a.

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

Créez une machine virtuelle de stockage sur une paire haute disponibilité en une seule zone de disponibilité

Ces étapes créent une nouvelle machine virtuelle de stockage sur une paire haute disponibilité en une seule zone de disponibilité. Une adresse IP privée est nécessaire pour créer une LIF NAS et une autre adresse IP privée facultative est requise si vous souhaitez créer une LIF de gestion.

Ces deux LIF sont allouées au nœud 1. Les adresses IP privées peuvent se déplacer entre les nœuds en cas de panne.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Créer une LIF NAS sur le nœud 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Où *private_ip_x* est une adresse IP privée secondaire inutilisée sur e0a de cvo-node1. Cette adresse IP peut être déplacée vers le fournisseur e0a de cvo-node2 en cas de basculement, car les fichiers de données par défaut de la politique de service indiquent que les adresses IP peuvent migrer vers le nœud partenaire.

3. Facultatif : créez une LIF de gestion de VM de stockage sur le nœud 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Où *private_ip_y* est une autre adresse IP privée secondaire inutilisée sur e0a.

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

5. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou version ultérieure, modifiez les stratégies de service réseau pour la VM de stockage.

La modification des services est requise, car elle permet à Cloud Volumes ONTAP d'utiliser la LIF iSCSI pour les connexions de gestion sortantes.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Créez une machine virtuelle de stockage sur une paire haute disponibilité dans plusieurs AZS

Ces étapes créent une nouvelle machine virtuelle de stockage sur une paire haute disponibilité dans plusieurs AZS.

Une adresse *flottante* IP est requise pour une LIF NAS et elle est facultative pour une LIF de gestion. Ces adresses IP flottantes ne vous demandent pas d'attribuer des adresses IP privées dans AWS. En revanche, les adresses IP flottantes sont automatiquement configurées dans la table de routage AWS pour pointer vers l'ENI d'un nœud spécifique dans le même VPC.

Pour que les adresses IP flottantes fonctionnent sur ONTAP, une adresse IP privée doit être configurée sur chaque VM de stockage sur chaque nœud. Cela est reflété dans les étapes ci-dessous où une LIF iSCSI est créée sur le nœud 1 et sur le nœud 2.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Créer une LIF NAS sur le nœud 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- L'adresse IP flottante doit être hors des blocs CIDR pour tous les VPC de la région AWS dans laquelle vous déployez la configuration HA. 192.168.209.27 est un exemple d'adresse IP flottante. ["En savoir plus sur le choix d'une adresse IP flottante"](#).
- `-service-policy default-data-files` Indique que les adresses IP peuvent migrer vers le nœud partenaire.

3. Facultatif : créez une LIF de gestion de VM de stockage sur le nœud 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Créer une LIF iSCSI sur le nœud 1.

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmask node1Mask -lif  
ip_node1_iscsi_2 -home-node cvo-node1
```

- Cette LIF iSCSI est nécessaire pour prendre en charge la migration LIF des adresses IP flottantes sur la machine virtuelle de stockage. Il n'est pas nécessaire de disposer d'une LIF iSCSI, mais elle ne peut pas être configurée pour migrer entre les nœuds.
- `-service-policy default-data-block` Indique qu'une adresse IP ne migre pas entre les nœuds.
- *Private_ip* est une adresse IP privée secondaire inutilisée sur eth0 (e0a) de cvo_node1.

5. Créer une LIF iSCSI sur le nœud 2.

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif  
ip_node2_iscsi_2 -home-node cvo-node2
```

- Cette LIF iSCSI est nécessaire pour prendre en charge la migration LIF des adresses IP flottantes sur la machine virtuelle de stockage. Il n'est pas nécessaire de disposer d'une LIF iSCSI, mais elle ne peut pas être configurée pour migrer entre les nœuds.
- `-service-policy default-data-block` Indique qu'une adresse IP ne migre pas entre les nœuds.
- *Private_ip* est une adresse IP privée secondaire inutilisée sur eth0 (e0a) de cvo_node2.

6. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

7. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou version ultérieure, modifiez les stratégies de service réseau pour la VM de stockage.

La modification des services est requise, car elle permet à Cloud Volumes ONTAP d'utiliser la LIF iSCSI pour les connexions de gestion sortantes.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

Création de VM de stockage servant à la transmission des données pour Cloud Volumes ONTAP dans Azure

Une VM de stockage est une machine virtuelle exécutée dans ONTAP, qui fournit des services de données et de stockage à vos clients. Vous pouvez le connaître comme *SVM* ou *vserver*. Cloud Volumes ONTAP est configuré avec une seule machine virtuelle de stockage par défaut, mais des machines virtuelles de stockage supplémentaires sont prises en charge lors de l'exécution de Cloud Volumes ONTAP dans Azure.

Pour créer des VM de stockage supplémentaires qui assurent le service des données, vous devez allouer des adresses IP dans Azure, puis exécuter des commandes ONTAP pour créer la VM de stockage et les LIF de données.

Nombre de machines virtuelles de stockage pris en charge

Plusieurs machines virtuelles de stockage sont prises en charge avec des configurations Cloud Volumes ONTAP spécifiques à partir de la version 9.9.0. Accédez au ["Notes de version de Cloud Volumes ONTAP"](#) Pour vérifier le nombre de machines virtuelles de stockage pris en charge pour votre version de Cloud Volumes ONTAP.

Toutes les autres configurations Cloud Volumes ONTAP prennent en charge une VM de stockage servant aux données et une VM de stockage de destination utilisée pour la reprise après incident. Vous pouvez activer la machine virtuelle de stockage de destination pour accéder aux données en cas de panne sur la machine virtuelle de stockage source.

Allouez des adresses IP dans Azure

Vous devez allouer des adresses IP dans Azure avant de créer une VM de stockage et d'allouer des LIF.

Système à un seul nœud

Les adresses IP doivent être attribuées à nic0 dans Azure avant de créer une machine virtuelle de stockage et d'allouer des LIF.

Vous devez créer une adresse IP pour l'accès LIF de données et une autre adresse IP en option pour une LIF de gestion de SVM (Storage VM). Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

Étapes

1. Connectez-vous au portail Azure et ouvrez le service **Virtual machine**.
2. Cliquez sur le nom de la machine virtuelle Cloud Volumes ONTAP.
3. Cliquez sur **réseau**.
4. Cliquez sur le nom de l'interface réseau pour nic0.
5. Sous **Paramètres**, cliquez sur **configurations IP**.
6. Cliquez sur **Ajouter**.
7. Entrez un nom pour la configuration IP, sélectionnez **Dynamic**, puis cliquez sur **OK**.
8. Cliquez sur le nom de la configuration IP que vous venez de créer, remplacez **Assignment** par **Static**, puis cliquez sur **Save**.

Il est préférable d'utiliser une adresse IP statique car une adresse IP statique garantit que l'adresse IP ne change pas, ce qui peut aider à éviter les pannes inutiles de votre application.

Pour créer une LIF de management du SVM, répétez la procédure ci-dessous afin de créer une adresse IP supplémentaire.

Une fois que vous avez terminé

Copiez les adresses IP privées que vous venez de créer. Vous devrez spécifier ces adresses IP lorsque vous créez des LIF pour la nouvelle machine virtuelle de stockage.

Paire HA

La façon dont vous allouez des adresses IP pour une paire haute disponibilité dépend du protocole de stockage que vous utilisez.

ISCSI

Les adresses IP iSCSI doivent être attribuées à nic0 dans Azure avant de créer une machine virtuelle de stockage et d'allouer des LIF. IPS pour iSCSI est affecté à nic0 et non à l'équilibreur de charge, car iSCSI utilise le protocole ALUA pour le basculement.

Vous devez créer les adresses IP suivantes :

- Une adresse IP pour l'accès aux LIF de données iSCSI depuis le nœud 1
- Une adresse IP pour l'accès aux LIF de données iSCSI depuis le nœud 2
- Une adresse IP facultative pour une LIF de gestion de VM de stockage (SVM)

Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

Étapes

1. Connectez-vous au portail Azure et ouvrez le service **Virtual machine**.
2. Cliquez sur le nom de la machine virtuelle Cloud Volumes ONTAP pour le nœud 1.
3. Cliquez sur **réseau**.
4. Cliquez sur le nom de l'interface réseau pour nic0.
5. Sous **Paramètres**, cliquez sur **configurations IP**.
6. Cliquez sur **Ajouter**.
7. Entrez un nom pour la configuration IP, sélectionnez **Dynamic**, puis cliquez sur **OK**.
8. Cliquez sur le nom de la configuration IP que vous venez de créer, remplacez **Assignment** par **Static**, puis cliquez sur **Save**.

Il est préférable d'utiliser une adresse IP statique car une adresse IP statique garantit que l'adresse IP ne change pas, ce qui peut aider à éviter les pannes inutiles de votre application.

9. Répétez cette procédure sur le nœud 2.
10. Pour créer une LIF de management du SVM, répétez ces étapes sur le nœud 1.

NFS

Les adresses IP que vous utilisez pour NFS sont allouées au équilibreur de charge afin que les adresses IP puissent migrer vers l'autre nœud en cas d'événements de basculement.

Vous devez créer les adresses IP suivantes :

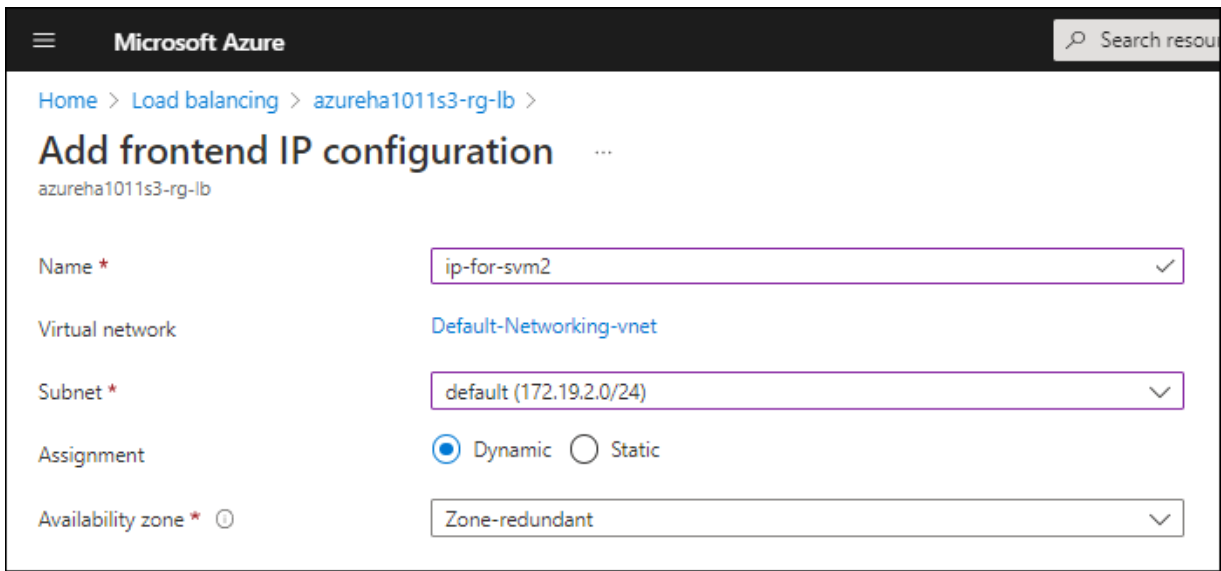
- Une adresse IP pour l'accès LIF de données NAS depuis le nœud 1
- Une adresse IP pour l'accès LIF de données NAS depuis le nœud 2
- Une adresse IP facultative pour une LIF de gestion de VM de stockage (SVM)

Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

Étapes

1. Dans le portail Azure, ouvrez le service **Load balancers**.
2. Cliquez sur le nom du équilibreur de charge pour la paire HA.

3. Créez une configuration IP front-end pour l'accès aux LIF de données depuis le nœud 1, une autre pour l'accès aux LIF de données depuis le nœud 2 et une autre LIF front-end facultative pour la gestion d'une machine virtuelle de stockage (SVM).
 - a. Sous **Paramètres**, cliquez sur **Configuration IP Frontend**.
 - b. Cliquez sur **Ajouter**.
 - c. Entrez un nom pour l'IP front-end, sélectionnez le sous-réseau pour la paire HA Cloud Volumes ONTAP, laissez **Dynamic** sélectionné et, dans les régions avec des zones de disponibilité, laissez **zone redondante** sélectionné pour vous assurer que l'adresse IP reste disponible en cas d'échec d'une zone.



The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A text input field containing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone ***: A dropdown menu showing 'Zone-redundant' with a downward arrow and an information icon.

- d. Cliquez sur le nom de la configuration IP front-end que vous venez de créer, définissez **Assignment** sur **Static**, puis cliquez sur **Save**.

Il est préférable d'utiliser une adresse IP statique car une adresse IP statique garantit que l'adresse IP ne change pas, ce qui peut aider à éviter les pannes inutiles de votre application.

4. Ajoutez une sonde de santé pour chaque IP front-end que vous venez de créer.

- a. Sous **Paramètres** de l'équilibreur de charge, cliquez sur **sondes de santé**.
 - b. Cliquez sur **Ajouter**.
 - c. Saisissez un nom pour la sonde de santé et entrez un numéro de port compris entre 63005 et 65000. Conservez les valeurs par défaut des autres champs.

Il est important que le numéro de port soit compris entre 63005 et 65000. Par exemple, si vous créez trois sondes de santé, vous pouvez entrer des sondes utilisant les numéros de port 63005, 63006 et 63007.

Microsoft Azure

Search resources, services, and

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe

...

azureha1011s3-rg-lb

Name *

svm2-health-probe1

Protocol *

TCP

Port * ⓘ

63005

Interval * ⓘ

5

seconds

Unhealthy threshold * ⓘ

2

consecutive failures

Used by ⓘ

Not used

5. Créer de nouvelles règles d'équilibrage de charge pour chaque IP front-end.

a. Sous **Paramètres** de l'équilibreur de charge, cliquez sur **règles d'équilibrage de charge**.

b. Cliquez sur **Ajouter** et entrez les informations requises :

- **Nom** : saisissez un nom pour la règle.
- **IP version** : sélectionnez **IPv4**.
- **Adresse IP Frontend** : sélectionnez l'une des adresses IP frontend que vous venez de créer.
- **Ports HA** : activez cette option.
- **Backend pool**: Conservez le pool Backend par défaut qui a déjà été sélectionné.
- **Health Probe** : sélectionnez la sonde de santé que vous avez créée pour l'IP front-end sélectionnée.
- **Persistance de session** : sélectionnez **aucun**.
- **IP flottante** : sélectionnez **Enabled**.

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule ✓

IP Version *

☒ IPv4 ☐ IPv6

Frontend IP address * ⓘ

10.1.0.156 (dataAFIP) ▼

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines) ▼

Health probe ⓘ

dataProbe (TCP:63002) ▼

Session persistence ⓘ

None ▼

Floating IP ⓘ

☐ Disabled ☒ Enabled

6. Assurez-vous que les règles de groupe de sécurité réseau pour Cloud Volumes ONTAP permettent à l'équilibreur de charge d'envoyer des sondes TCP pour les sondes d'intégrité créées à l'étape 4 ci-dessus. Notez que cette option est autorisée par défaut.

PME

Les adresses IP utilisées pour les données SMB sont allouées au équilibreur de charge afin que les adresses IP puissent migrer vers l'autre nœud en cas d'événements de basculement.

Vous devez créer les adresses IP suivantes :

- Une adresse IP pour l'accès LIF de données NAS depuis le nœud 1
- Une adresse IP pour l'accès LIF de données NAS depuis le nœud 2
- Une adresse IP pour une LIF iSCSI sur le nœud 1
- Une adresse IP pour une LIF iSCSI sur le nœud 2

Les LIFs iSCSI sont requises pour les communications DNS et SMB. Une LIF iSCSI est utilisée à cette fin, car elle ne migre pas au basculement.

- Une adresse IP facultative pour une LIF de gestion de VM de stockage (SVM)

Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

Étapes

1. Dans le portail Azure, ouvrez le service **Load balancers**.
2. Cliquez sur le nom du équilibreur de charge pour la paire HA.
3. Créez le nombre requis de configurations IP frontales :
 - a. Sous **Paramètres**, cliquez sur **Configuration IP Frontend**.
 - b. Cliquez sur **Ajouter**.
 - c. Entrez un nom pour l'IP front-end, sélectionnez le sous-réseau pour la paire HA Cloud Volumes ONTAP, laissez **Dynamic** sélectionné et, dans les régions avec des zones de disponibilité, laissez **zone redondante** sélectionné pour vous assurer que l'adresse IP reste disponible en cas d'échec d'une zone.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone * ⓘ**: A dropdown menu showing 'Zone-redundant' with a downward arrow icon.

- d. Cliquez sur le nom de la configuration IP front-end que vous venez de créer, définissez **Assignment** sur **Static**, puis cliquez sur **Save**.

Il est préférable d'utiliser une adresse IP statique car une adresse IP statique garantit que l'adresse IP ne change pas, ce qui peut aider à éviter les pannes inutiles de votre application.

4. Ajoutez une sonde de santé pour chaque IP front-end que vous venez de créer.
 - a. Sous **Paramètres** de l'équilibreur de charge, cliquez sur **sondes de santé**.
 - b. Cliquez sur **Ajouter**.
 - c. Saisissez un nom pour la sonde de santé et entrez un numéro de port compris entre 63005 et 65000. Conservez les valeurs par défaut des autres champs.

Il est important que le numéro de port soit compris entre 63005 et 65000. Par exemple, si vous créez trois sondes de santé, vous pouvez entrer des sondes utilisant les numéros de port 63005, 63006 et 63007.

Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

Add health probe

azureha1011s3-rg-lb

| | | |
|-------------------------|--------------------|----------------------|
| Name * | svm2-health-probe1 | ✓ |
| Protocol * | TCP | ▼ |
| Port * ⓘ | 63005 | ✓ |
| Interval * ⓘ | 5 | seconds |
| Unhealthy threshold * ⓘ | 2 | consecutive failures |
| Used by ⓘ | Not used | |

5. Créer de nouvelles règles d'équilibrage de charge pour chaque IP front-end.

a. Sous **Paramètres** de l'équilibreur de charge, cliquez sur **règles d'équilibrage de charge**.

b. Cliquez sur **Ajouter** et entrez les informations requises :

- **Nom** : saisissez un nom pour la règle.
- **IP version** : sélectionnez **IPv4**.
- **Adresse IP Frontend** : sélectionnez l'une des adresses IP frontend que vous venez de créer.
- **Ports HA** : activez cette option.
- **Backend pool**: Conservez le pool Backend par défaut qui a déjà été sélectionné.
- **Health Probe** : sélectionnez la sonde de santé que vous avez créée pour l'IP front-end sélectionnée.
- **Persistance de session** : sélectionnez **aucun**.
- **IP flottante** : sélectionnez **Enabled**.

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule ✓

IP Version *

☒ IPv4 ☐ IPv6

Frontend IP address * ⓘ

10.1.0.156 (dataAFIP) ▼

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines) ▼

Health probe ⓘ

dataProbe (TCP:63002) ▼

Session persistence ⓘ

None ▼

Floating IP ⓘ

☐ Disabled ☒ Enabled

- Assurez-vous que les règles de groupe de sécurité réseau pour Cloud Volumes ONTAP permettent à l'équilibreur de charge d'envoyer des sondes TCP pour les sondes d'intégrité créées à l'étape 4 ci-dessus. Notez que cette option est autorisée par défaut.

Une fois que vous avez terminé

Copiez les adresses IP privées que vous venez de créer. Vous devrez spécifier ces adresses IP lorsque vous créez des LIF pour la nouvelle machine virtuelle de stockage.

Créez un VM de stockage et des LIF

Une fois que vous avez alloué des adresses IP dans Azure, vous pouvez créer une nouvelle machine virtuelle de stockage sur un système à un seul nœud ou sur une paire haute disponibilité.

Système à un seul nœud

La création d'une VM de stockage et de LIF sur un système à un seul nœud dépend du protocole de stockage que vous utilisez.

ISCSI

Suivez ces étapes pour créer une nouvelle machine virtuelle de stockage et les LIF nécessaires.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Créer une LIF de données :

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

3. Facultatif : créez une LIF de gestion de machine virtuelle de stockage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

NFS

Suivez ces étapes pour créer une nouvelle machine virtuelle de stockage et les LIF nécessaires.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Créer une LIF de données :

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

3. Facultatif : créez une LIF de gestion de machine virtuelle de stockage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

PME

Suivez ces étapes pour créer une nouvelle machine virtuelle de stockage et les LIF nécessaires.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Créer une LIF de données :

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs--ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

3. Facultatif : créez une LIF de gestion de machine virtuelle de stockage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

Paire HA

La création d'un VM de stockage et de LIF sur une paire haute disponibilité dépend du protocole de stockage que vous utilisez.

ISCSI

Suivez ces étapes pour créer une nouvelle machine virtuelle de stockage et les LIF nécessaires.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Création de LIF de données :

- a. Utiliser la commande suivante pour créer une LIF iSCSI sur le nœud 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. Utiliser la commande suivante pour créer une LIF iSCSI sur le nœud 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

3. Facultatif : créez une LIF de gestion de VM de stockage sur le nœud 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un

agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

5. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou version ultérieure, modifiez les stratégies de service réseau pour la VM de stockage.

La modification des services est requise, car elle permet à Cloud Volumes ONTAP d'utiliser la LIF iSCSI pour les connexions de gestion sortantes.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

Suivez ces étapes pour créer une nouvelle machine virtuelle de stockage et les LIF nécessaires.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Création de LIF de données :

- a. Utiliser la commande suivante pour créer une LIF NAS sur le nœud 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs--ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Utiliser la commande suivante pour créer une LIF NAS sur le nœud 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. Facultatif : créez une LIF de gestion de VM de stockage sur le nœud 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default -probe-port <port-number-  
for-azure-health-probe3>
```

Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

4. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

5. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou version ultérieure, modifiez les stratégies de service réseau pour la VM de stockage.

La modification des services est requise, car elle permet à Cloud Volumes ONTAP d'utiliser la LIF iSCSI pour les connexions de gestion sortantes.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

PME

Suivez ces étapes pour créer une nouvelle machine virtuelle de stockage et les LIF nécessaires.

Étapes

1. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Création de LIF de données NAS :

- a. Utiliser la commande suivante pour créer une LIF NAS sur le nœud 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Utiliser la commande suivante pour créer une LIF NAS sur le nœud 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. Créez des LIFs iSCSI pour fournir des communications DNS et SMB :

- a. Utiliser la commande suivante pour créer une LIF iSCSI sur le nœud 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. Utiliser la commande suivante pour créer une LIF iSCSI sur le nœud 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

4. Facultatif : créez une LIF de gestion de VM de stockage sur le nœud 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Cette LIF de gestion fournit une connexion à des outils de gestion tels que SnapCenter.

5. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

6. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou version ultérieure, modifiez les stratégies de service réseau pour la VM de stockage.

La modification des services est requise, car elle permet à Cloud Volumes ONTAP d'utiliser la LIF iSCSI pour les connexions de gestion sortantes.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

Et la suite ?

Après avoir créé un serveur virtuel de stockage sur une paire haute disponibilité, il est préférable d'attendre 12 heures avant de provisionner le stockage sur ce SVM. Depuis la version Cloud Volumes ONTAP 9.10.1, BlueXP analyse les paramètres de l'équilibreur de charge d'une paire HA à un intervalle de 12 heures. S'il existe de nouveaux SVM, BlueXP activation d'un paramètre qui permet un basculement non planifié plus court.

Création de machines virtuelles de stockage destinées aux données pour Cloud Volumes ONTAP dans Google Cloud

Une VM de stockage est une machine virtuelle exécutée dans ONTAP, qui fournit des services de données et de stockage à vos clients. Vous pouvez le connaître comme SVM ou *vserver*. La solution Cloud Volumes ONTAP est configurée par défaut avec une seule machine virtuelle de stockage, mais certaines configurations prennent en charge des

machines virtuelles de stockage supplémentaires.

Nombre de machines virtuelles de stockage pris en charge

Plusieurs machines virtuelles de stockage sont prises en charge avec des configurations Cloud Volumes ONTAP spécifiques dans Google Cloud à partir de la version 9.11.1. Accédez au ["Notes de version de Cloud Volumes ONTAP"](#) Pour vérifier le nombre de machines virtuelles de stockage pris en charge pour votre version de Cloud Volumes ONTAP.

Toutes les autres configurations Cloud Volumes ONTAP prennent en charge une VM de stockage servant aux données et une VM de stockage de destination utilisée pour la reprise après incident. Vous pouvez activer la machine virtuelle de stockage de destination pour accéder aux données en cas de panne sur la machine virtuelle de stockage source.

Créez une machine virtuelle de stockage

Si votre licence est prise en charge, vous pouvez créer plusieurs machines virtuelles de stockage sur un système à un seul nœud ou sur une paire haute disponibilité. Notez que vous devez utiliser l'API BlueXP pour créer une machine virtuelle de stockage sur une paire haute disponibilité, tandis que vous pouvez utiliser l'interface de ligne de commande ou System Manager pour créer une machine virtuelle de stockage sur un système à un seul nœud.

Système à un seul nœud

Ces étapes créent une nouvelle machine virtuelle de stockage sur un système à un seul nœud via l'interface de ligne de commande. Une adresse IP privée est nécessaire pour créer une LIF de données et une autre adresse IP privée facultative est requise si vous souhaitez créer une LIF de gestion.

Étapes

1. Dans Google Cloud, allez à l'instance Cloud Volumes ONTAP et ajoutez une adresse IP à nic0 pour chaque LIF.

Edit network interface

Network *
default

Subnetwork *
default IPv4 (10.138.0.0/20)

i To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

IP stack type
☒ IPv4 (single-stack)
☐ IPv4 and IPv6 (dual-stack)

Primary internal IP
gcpcvo-vm-ip-nic0-nodemgmt (10.138.0.46)

Alias IP ranges

| | |
|---|--------------------------------------|
| Subnet range 1 Primary (10.138.0.0/20) | Alias IP range 1 * 10.138.0.25/32 |
| Subnet range 2 Primary (10.138.0.0/20) | Alias IP range 2 * 10.138.0.23/32 |
| Subnet range 3 Primary (10.138.0.0/20) | Alias IP range 3 * 10.138.0.21/32 |
| Subnet range 4 Primary (10.138.0.0/20) | Alias IP range 4 * 10.138.0.31/32 |

+ ADD IP RANGE

External IPv4 address
None

Vous avez besoin d'une adresse IP pour une LIF de données et d'une autre adresse IP facultative si vous souhaitez créer une LIF de gestion sur la machine virtuelle de stockage.

["Documentation Google Cloud : ajout de plages d'adresses IP d'alias à une instance existante"](#)

2. Créer la VM de stockage et une route vers la VM de stockage

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```


3. Créez une LIF de données en spécifiant l'adresse IP que vous avez ajoutée dans Google Cloud.

ISCSI

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

NFS ou SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

4. Facultatif : créez une LIF de gestion de VM de stockage en spécifiant l'adresse IP que vous avez ajoutée dans Google Cloud.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data  
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length  
<length> -home-node <name-of-node1> -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false  
-failover-group Default
```

5. Attribuez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

Cette étape est obligatoire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur cette machine virtuelle de stockage.

Paire HA

Vous devez utiliser l'API BlueXP pour créer une machine virtuelle de stockage sur un système Cloud Volumes ONTAP dans Google Cloud. L'utilisation de l'API (et non de System Manager ou de l'interface de ligne de commande) est requise, car BlueXP configure la machine virtuelle de stockage avec les services LIF requis, ainsi qu'une LIF iSCSI requise pour les communications SMB/CIFS sortantes.

Notez que BlueXP alloue les adresses IP requises dans Google Cloud et crée la machine virtuelle de stockage avec une LIF de données pour les accès SMB/NFS et une LIF iSCSI pour les communications SMB sortantes.

Autorisations Google Cloud requises

Depuis la version 3.9.19, le connecteur requiert les autorisations suivantes pour créer et gérer des machines virtuelles de stockage pour les paires haute disponibilité Cloud Volumes ONTAP :

- `compute.instanceGroups.get`
- `compute.addresses.get`

Ces autorisations sont incluses dans ["Règles fournies par NetApp"](#).

Étapes

1. Utilisez l'appel d'API suivant pour créer une machine virtuelle de stockage :

```
POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
```

Le corps de la demande doit comprendre les éléments suivants :

```
{ "svmName": "myNewSvm1" }
```

Gérer les machines virtuelles de stockage sur des paires haute disponibilité

L'API BlueXP prend également en charge le changement de nom et la suppression des machines virtuelles de stockage sur les paires HA.

Renommer une machine virtuelle de stockage

Si besoin, vous pouvez à tout moment modifier le nom d'une machine virtuelle de stockage.

Étapes

1. Utiliser l'appel d'API suivant pour renommer une VM de stockage :

```
PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
```

Le corps de la demande doit comprendre les éléments suivants :

```
{  
  "svmNewName": "newSvmName",  
  "svmName": "oldSvmName"  
}
```

Supprimer une machine virtuelle de stockage

Si vous n'avez plus besoin d'une machine virtuelle de stockage, vous pouvez la supprimer de Cloud Volumes ONTAP.

Étapes

1. Utilisez l'appel d'API suivant pour supprimer une VM de stockage :

```
DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
```

Sécurité et chiffrement des données

Cryptage de volumes grâce aux solutions de cryptage NetApp

Cloud Volumes ONTAP prend en charge NetApp Volume Encryption (NVE) et NetApp Aggregate Encryption (NAE). NVE et NAE sont des solutions logicielles qui permettent le chiffrement des données au repos conforme à la norme FIPS 140-2. ["En savoir plus sur ces solutions de cryptage"](#).

NVE et NAE sont pris en charge par un gestionnaire de clés externe.

NAE est activé sur les nouveaux agrégats par défaut après avoir configuré un gestionnaire de clés externe. NVE est activé par défaut sur les nouveaux volumes qui ne font pas partie d'un agrégat NAE (par exemple, si des agrégats existants ont été créés avant de configurer un gestionnaire de clés externe).

Cloud Volumes ONTAP ne prend pas en charge la gestion intégrée des clés.

Ce dont vous avez besoin

Votre système Cloud Volumes ONTAP doit être enregistré auprès du support NetApp. Une licence NetApp Volume Encryption est automatiquement installée sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp.

- ["Ajout de comptes du site de support NetApp à BlueXP"](#)
- ["Enregistrement des systèmes de paiement à l'utilisation"](#)



BlueXP n'installe pas la licence NVE sur les systèmes qui résident dans la région Chine.

Étapes

1. Consultez la liste des gestionnaires de clés pris en charge dans le ["Matrice d'interopérabilité NetApp"](#).



Recherchez la solution **gestionnaires de clés**.

2. ["Connectez-vous à l'interface de ligne de commandes de Cloud Volumes ONTAP"](#).
3. Configurez la gestion externe des clés.
 - AWS : ["Pour obtenir des instructions, consultez la documentation ONTAP"](#)
 - Azure : ["Azure Key Vault \(AKV\)"](#)
 - Google Cloud : ["Service Google Cloud Key Management"](#)

Gérez les clés avec Azure Key Vault

Vous pouvez utiliser ["Azure Key Vault \(AKV\)"](#) Afin de protéger vos clés de chiffrement ONTAP dans une application déployée dans Azure.

AKV peut être utilisé pour protéger ["Clés NetApp Volume Encryption \(NVE\)"](#) Uniquement pour les SVM de données.

La gestion des clés via AKV peut être activée via l'interface de ligne de commande ou l'API REST ONTAP.

Lorsque vous utilisez AKV, notez que par défaut une LIF de SVM de données permet de communiquer avec le

terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur de cloud (login.microsoftonline.com). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Prérequis

- Cloud Volumes ONTAP doit exécuter la version 9.10.1 ou ultérieure
- Licence Volume Encryption (VE) installée (la licence NetApp Volume Encryption est automatiquement installée sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp).
- Licence MTEKM (Multi-tenant Encryption Key Management) installée
- Vous devez être un administrateur de cluster ou de SVM
- Un abonnement Active Azure

Limites

- AKV ne peut être configuré que sur un SVM de données

Processus de configuration

La procédure décrite ci-dessus décrit comment enregistrer votre configuration Cloud Volumes ONTAP avec Azure et comment créer un coffre-fort de clés Azure et des clés. Si vous avez déjà effectué ces étapes, vérifiez que vous disposez des paramètres de configuration corrects, notamment dans [Créez un coffre-fort de clés Azure](#), puis passer à [Configuration Cloud Volumes ONTAP](#).

- [Inscription aux applications Azure](#)
- [Créez le secret du client Azure](#)
- [Créez un coffre-fort de clés Azure](#)
- [Créez une clé de chiffrement](#)
- [Création d'un terminal Azure Active Directory \(HA uniquement\)](#)
- [Configuration Cloud Volumes ONTAP](#)

Inscription aux applications Azure

1. Vous devez d'abord enregistrer votre application dans l'abonnement Azure que vous souhaitez que Cloud Volumes ONTAP utilise pour accéder au coffre-fort de clés Azure. Dans le portail Azure, sélectionnez **enregistrements d'applications**.
2. Sélectionnez **Nouvelle inscription**.
3. Indiquez un nom pour votre application et sélectionnez un type d'application pris en charge. Le locataire unique par défaut suffit pour l'utilisation d'Azure Key Vault. Sélectionnez **Enregistrer**.
4. Dans la fenêtre Présentation d'Azure, sélectionnez l'application que vous avez enregistrée. Copiez l'ID de l'application (client) **et l'ID du répertoire** (locataire)** dans un emplacement sécurisé. Elles seront requises plus tard dans le processus d'inscription.

Créez le secret du client Azure

1. Dans le portail Azure de votre application Cloud Volumes ONTAP, sélectionnez le volet **Certificats & secrets**.
2. Sélectionnez **Nouveau secret client** Entrez un nom significatif pour votre secret client. NetApp recommande une période d'expiration de 24 mois. Toutefois, vos règles de gouvernance cloud peuvent nécessiter un paramétrage différent.
3. Sélectionnez **Ajouter** pour enregistrer le secret client. Copiez immédiatement la valeur ** du secret et

stockez-la quelque part en toute sécurité pour une configuration future. La valeur secrète ne s'affiche pas lorsque vous vous éloignez de la page.

Créez un coffre-fort de clés Azure

1. Si vous disposez déjà d'un coffre-fort de clés Azure, vous pouvez le connecter à votre configuration Cloud Volumes ONTAP, mais vous devez adapter les règles d'accès aux paramètres de ce processus.
2. Dans le portail Azure, accédez à la section **Key Vaults**.
3. Sélectionnez **Créer**. Entrez les informations requises, y compris le groupe de ressources, la région et le niveau de prix, et effectuez des sélections pour les jours de conservation des coffres-forts supprimés et si la protection de purge est activée ou non. Les valeurs par défaut sont suffisantes pour cette configuration. Toutefois, vos règles de gouvernance de cloud peuvent nécessiter des paramètres différents.
4. Sélectionnez **Suivant** pour choisir une stratégie d'accès.
5. Sélectionnez **chiffrement de disque Azure** pour l'option de chiffrement de volume et **politique d'accès au coffre-fort** pour le modèle d'autorisation.
6. Sélectionnez **Ajouter une stratégie d'accès**.
7. Sélectionnez le point adjacent au champ **configurer à partir du modèle (facultatif)**. Sélectionnez ensuite **Key, Secret, & Certification Management**.
8. Choisissez chacun des menus déroulants d'autorisations (clé, secret, certificat), puis **Sélectionner tout** en haut de la liste des menus pour sélectionner toutes les autorisations disponibles. Vous devez avoir :
 - **Autorisations clés** : 19 sélectionnées
 - **Autorisations secrètes**: 8 sélectionnées
 - **Autorisations de certificat**: 16 sélectionné
9. Sélectionnez **Ajouter** pour créer la stratégie d'accès.
10. Sélectionnez **Suivant** pour passer aux options **mise en réseau**.
11. Choisissez la méthode d'accès au réseau appropriée ou sélectionnez **tous les réseaux** et **Revue + Créer** pour créer le coffre-fort de clés. (La méthode d'accès au réseau peut être prescrite par une gouvernance ou par votre équipe de sécurité cloud.)
12. Enregistrez l'URI du coffre-fort de clés : dans le coffre-fort de clés que vous avez créé, accédez au menu Aperçu et copiez l'URI du coffre-fort ** dans la colonne de droite. Vous en aurez besoin pour une étape ultérieure.

Créez une clé de chiffrement

1. Dans le menu du coffre-fort de clés créé pour Cloud Volumes ONTAP, accédez à l'option **touches**.
2. Sélectionnez **générer/importer** pour créer une nouvelle clé.
3. Laissez l'option par défaut sur **générer**.
4. Fournissez les informations suivantes :
 - Nom de la clé de chiffrement
 - Type de clé : RSA
 - Taille de la clé RSA : 2048
 - Activé : Oui
5. Sélectionnez **Créer** pour créer la clé de cryptage.
6. Revenez au menu **touches** et sélectionnez la touche que vous venez de créer.
7. Sélectionnez l'ID de clé sous **version actuelle** pour afficher les propriétés de la clé.

8. Repérez le champ **Key identifiant**. Copiez l'URI vers mais sans inclure la chaîne hexadécimale.

Création d'un terminal Azure Active Directory (HA uniquement)

1. Ce processus n'est requis que si vous configurez Azure Key Vault pour un environnement de travail Cloud Volumes ONTAP haute disponibilité.
2. Dans le portail Azure, accédez à **réseaux virtuels**.
3. Sélectionnez le réseau virtuel sur lequel vous avez déployé l'environnement de travail Cloud Volumes ONTAP et sélectionnez le menu **sous-réseaux** sur le côté gauche de la page.
4. Sélectionnez dans la liste le nom de sous-réseau de votre déploiement Cloud Volumes ONTAP.
5. Naviguez jusqu'à l'en-tête **points d'extrémité du service**. Dans le menu déroulant, sélectionnez **Microsoft.AzureActiveDirectory** dans la liste.
6. Sélectionnez **Enregistrer** pour capturer vos paramètres.

Configuration Cloud Volumes ONTAP

1. Connectez-vous à la LIF de gestion du cluster avec votre client SSH préféré.
2. Entrez le mode de privilège avancé dans ONTAP :
`set advanced -con off``
3. Identifier le SVM de données souhaité et vérifier sa configuration DNS :
`vserver services name-service dns show`
 - a. Si une entrée DNS pour le SVM de données souhaité existe et qu'elle contient une entrée pour le DNS Azure, aucune action n'est requise. Si ce n'est pas le cas, ajoutez une entrée de serveur DNS pour le SVM de données qui pointe vers le DNS Azure, le DNS privé ou le serveur sur site. Ceci doit correspondre à l'entrée pour le SVM admin du cluster :
`vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`
 - b. Vérifier que le service DNS a été créé pour le SVM de données :
`vserver services name-service dns show`
4. Activez le coffre-fort de clés Azure à l'aide de l'ID client et de l'ID locataire enregistrés après l'enregistrement de l'application :
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_name -key-id Azure_key_ID`
5. Vérifiez la configuration du gestionnaire de clés :
`security key-manager external azure show`
6. Vérifier le statut du gestionnaire de clés :
``security key-manager external azure check``Le résultat sera le suivant :

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
Status: OK

Category: ekvip_server
Status: OK

Category: kms_wrapped_key_status
Status: UNKNOWN
Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Si le `service_reachability` l'état n'est pas OK, La SVM ne peut pas atteindre le service Azure Key Vault avec toutes les connectivités et autorisations requises. Le `kms_wrapped_key_status` rapports UNKNOWN lors de la configuration initiale. Son statut devient OK une fois le premier volume crypté.

7. FACULTATIF : créez un volume de test pour vérifier le fonctionnement de NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

S'il est correctement configuré, Cloud Volumes ONTAP crée automatiquement le volume et active le chiffrement de volume.

8. Confirmez que le volume a été créé et chiffré correctement. Si c'est le cas, le `-is-encrypted` le paramètre s'affiche comme `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

Gérez les clés à l'aide du service Cloud Key Management de Google

Vous pouvez utiliser "[Service de gestion des clés \(KMS cloud\) de Google Cloud Platform](#)" Pour protéger vos clés de chiffrement ONTAP dans une application déployée sur Google Cloud Platform.

La gestion des clés via le serveur Cloud KMS peut être activée via l'interface de ligne de commande ou l'API REST de ONTAP.

Lorsque vous utilisez le KMS, notez que, par défaut, une LIF de data SVM est utilisée pour communiquer avec le terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur de cloud (`oauth2.googleapis.com`). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Prérequis

- Cloud Volumes ONTAP doit exécuter la version 9.10.1 ou ultérieure

- Licence VE (Volume Encryption) installée
- Licence MTEKM (Multi-tenant Encryption Key Management) installée
- Vous devez être un administrateur de cluster ou de SVM
- Un abonnement actif à Google Cloud Platform

Limites

- Cloud KMS peut uniquement être configuré sur un SVM de données

Configuration

Google Cloud

1. Dans votre environnement Google Cloud, "[Créez une clé et une clé GCP symétriques](#)".
2. Créez un rôle personnalisé pour votre compte de service Cloud Volumes ONTAP.

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. Attribuez le rôle personnalisé à la clé KMS cloud et au compte de service Cloud Volumes ONTAP :

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. Télécharger la clé JSON du compte de service :

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. Connectez-vous à la LIF de gestion du cluster avec votre client SSH préféré.
2. Basculer vers le niveau de privilège avancé :

```
set -privilege advanced
```
3. Créer un DNS pour le SVM de données.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```
4. Créer une entrée CMEK :

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```
5. Lorsque vous y êtes invité, entrez la clé JSON de compte de service de votre compte GCP.

6. Confirmer que le processus activé a réussi :

```
security key-manager external gcp check -vserver svm_name
```

7. FACULTATIF : créez un volume pour tester le chiffrement `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Résoudre les problèmes

Si vous avez besoin d'effectuer un dépannage, vous pouvez consulter les journaux d'API REST bruts dans les deux dernières étapes ci-dessus :

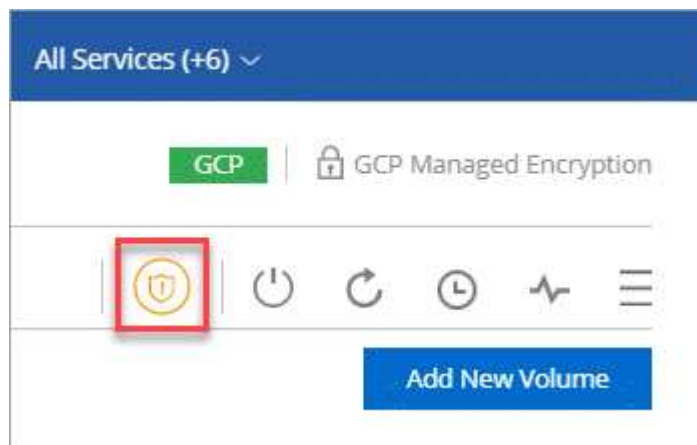
1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Renforcer la protection contre les attaques par ransomware

Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. BlueXP vous permet d'implémenter la solution NetApp pour ransomware. Elle fournit des outils efficaces pour la visibilité, la détection et la résolution de problèmes.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **ransomware**.



2. Implémentez la solution NetApp en cas d'attaque par ransomware :
 - a. Cliquez sur **Activer la stratégie de snapshot**, si des volumes n'ont pas de règle de snapshot activée.

La technologie Snapshot de NetApp offre la meilleure solution du secteur pour résoudre les problèmes liés aux attaques par ransomware. Le mieux pour réussir la récupération est d'effectuer une restauration à partir de sauvegardes non infectées. Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

- b. Cliquez sur **Activer FPolicy** pour activer la solution FPolicy d'ONTAP, qui peut bloquer les opérations de fichiers en fonction de l'extension d'un fichier.

Cette solution préventive améliore la protection contre les attaques par ransomware en bloquant les types de fichiers généralement utilisés.

Les fichiers de blocs d'étendue FPolicy par défaut qui possèdent les extensions suivantes :

micro, chiffré, verrouillé, crypto, crypt, Crinf, r5a, XRNT, XTBL, R16M01D05, Pzdc, Good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, enciphed, LeChiffre



BlueXP crée ce périmètre lorsque vous activez FPolicy sur Cloud Volumes ONTAP. La liste est basée sur les types de fichiers ransomware les plus courants. Vous pouvez personnaliser les extensions de fichiers bloqués en utilisant les commandes `vserver fpolicy policy scope` à partir de l'interface de ligne de commande Cloud Volumes ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection ⓘ

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

2 Block Ransomware File Extensions ⓘ

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names ⓘ](#)

Activate FPolicy

Administration du système

Mettez à niveau le logiciel Cloud Volumes ONTAP

Mettez à niveau Cloud Volumes ONTAP depuis BlueXP pour accéder aux dernières nouvelles fonctionnalités et améliorations. Préparez les systèmes Cloud Volumes ONTAP avant de mettre à niveau le logiciel.

Présentation de la mise à niveau

Avant de démarrer le processus de mise à niveau Cloud Volumes ONTAP, vous devez avoir connaissance des points suivants.

Mise à niveau depuis BlueXP uniquement

Les mises à niveau de Cloud Volumes ONTAP doivent être effectuées depuis BlueXP. Vous ne devez pas mettre à niveau Cloud Volumes ONTAP à l'aide de System Manager ou de l'interface de ligne de commandes. Cela peut affecter la stabilité du système.

Comment mettre à niveau

BlueXP offre deux façons de mettre à niveau Cloud Volumes ONTAP :

- En suivant les notifications de mise à niveau qui apparaissent dans l'environnement de travail

- En plaçant l'image de mise à niveau dans un emplacement HTTPS, puis en fournissant BlueXP avec l'URL

Chemins de mise à niveau pris en charge

La version de Cloud Volumes ONTAP sur laquelle vous pouvez effectuer la mise à niveau dépend de la version de Cloud Volumes ONTAP que vous utilisez actuellement.

| Version actuelle | Versions pouvant être directement mises à niveau vers |
|------------------|---|
| 9.12.0 | 9.12.1 |
| 9.11.1 | 9.12.1 |
| | 9.12.0 |
| 9.11.0 | 9.11.1 |
| 9.10.1 | 9.11.1 |
| | 9.11.0 |
| 9.10.0 | 9.10.1 |
| 9.9.1 | 9.10.1 |
| | 9.10.0 |
| 9.9.0 | 9.9.1 |
| 9.8 | 9.9.1 |
| 9.7 | 9.8 |
| 9.6 | 9.7 |
| 9.5 | 9.6 |
| 9.4 | 9.5 |
| 9.3 | 9.4 |
| 9.2 | 9.3 |
| 9.1 | 9.2 |
| 9.0 | 9.1 |
| 8.3 | 9.0 |

Notez ce qui suit :

- Les chemins de mise à niveau pris en charge pour Cloud Volumes ONTAP sont différents de ceux d'un cluster ONTAP sur site.
- Si vous effectuez une mise à niveau en suivant les notifications de mise à niveau qui apparaissent dans un environnement de travail, BlueXP vous invite à effectuer une mise à niveau vers une version qui suit ces chemins de mise à niveau pris en charge.
- Si vous mettez une image de mise à niveau sur un emplacement HTTPS, veuillez à suivre les chemins de mise à niveau pris en charge.
- Dans certains cas, vous devrez peut-être procéder à une mise à niveau plusieurs fois pour atteindre la version cible.

Par exemple, si vous utilisez la version 9.8 et que vous voulez passer à la version 9.10.1, vous devez d'abord passer à la version 9.9.1 puis à la version 9.10.1.

Rétablissement ou rétrogradation

La restauration ou la rétrogradation d'une version antérieure de Cloud Volumes ONTAP n'est pas prise en charge.

Inscription au support

Cloud Volumes ONTAP doit être enregistré auprès du service de support de NetApp pour mettre à niveau le logiciel à l'aide de l'une des méthodes décrites sur cette page. Cela s'applique à la fois à PAYGO et à BYOL. Vous devez le faire "[Enregistrer manuellement les systèmes PAYGO](#)", Tandis que les systèmes BYOL sont enregistrés par défaut.



Un système qui n'est pas enregistré pour le support recevra toujours les notifications de mise à jour de logiciel qui apparaissent dans BlueXP lorsqu'une nouvelle version est disponible. Mais vous devrez enregistrer le système avant de pouvoir mettre à niveau le logiciel.

Mises à niveau du médiateur HA

BlueXP met également à jour l'instance de médiateur si nécessaire lors du processus de mise à niveau de Cloud Volumes ONTAP.

Préparation à la mise à niveau

Avant d'effectuer une mise à niveau, vous devez vérifier que vos systèmes sont prêts et apporter les modifications nécessaires à la configuration.

- [https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap/Planifiez les temps d&.html#8217;indisponibilité](https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap/Planifiez%20les%20temps%20d%27indisponibilit%C3%A9)
- [Vérifier que le rétablissement automatique est toujours activé](#)
- [Suspendre les transferts SnapMirror](#)
- [Vérifiez que les agrégats sont en ligne](#)

Planifiez les temps d'indisponibilité

Lorsque vous mettez à niveau un système à un seul nœud, le processus de mise à niveau met le système hors ligne pendant 25 minutes au cours desquelles les E/S sont interrompues.

La mise à niveau d'une paire haute disponibilité s'effectue sans interruption et les E/S sont continues. Au cours de ce processus de mise à niveau sans interruption, chaque nœud est mis à niveau en tandem afin de continuer à traiter les E/S aux clients.

Vérifier que le rétablissement automatique est toujours activé

Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"](#)

Suspendre les transferts SnapMirror

Si un système Cloud Volumes ONTAP a des relations SnapMirror actives, il est préférable de suspendre les transferts avant de mettre à jour le logiciel Cloud Volumes ONTAP. La suspension des transferts empêche les défaillances de SnapMirror. Vous devez suspendre les transferts depuis le système de destination.



Même si Cloud Backup utilise une implémentation de SnapMirror pour créer des fichiers de sauvegarde (appelée SnapMirror Cloud), les sauvegardes n'ont pas besoin d'être suspendues lors de la mise à niveau d'un système.

Description de la tâche

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

Étapes

1. Connectez-vous à System Manager à partir du système de destination.

Vous pouvez vous connecter à System Manager en pointant votre navigateur Web sur l'adresse IP de la LIF de gestion du cluster. L'adresse IP est disponible dans l'environnement de travail Cloud Volumes ONTAP.



L'ordinateur à partir duquel vous accédez à BlueXP doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être vous connecter à BlueXP à partir d'un hôte de saut situé dans le réseau de votre fournisseur de cloud.

2. Cliquez sur **protection > relations**.
3. Sélectionnez la relation et cliquez sur **opérations > Quiesce**.

Vérifiez que les agrégats sont en ligne

Les agrégats pour Cloud Volumes ONTAP doivent être en ligne avant de mettre à jour le logiciel. Les agrégats doivent être en ligne dans la plupart des configurations, mais si ce n'est pas le cas, vous devez les mettre en ligne.

Description de la tâche

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
2. Sélectionnez un agrégat, cliquez sur **Info**, puis vérifiez que l'état est en ligne.

| | | |
|--------------------------|----------|---|
| aggr1 | | |
| Aggregate Capacity: | 88.57 GB | |
| ----- | | |
| Used Aggregate Capacity: | 1.07 GB | |
| ----- | | |
| Volumes: | 2 | ▼ |
| ----- | | |
| AWS Disks: | 1 | ▼ |
| ----- | | |
| State: | online | |
| ----- | | |

3. Si l'agrégat est hors ligne, utilisez System Manager pour mettre l'agrégat en ligne :
 - a. Cliquez sur **stockage > agrégats et disques > agrégats**.
 - b. Sélectionnez l'agrégat, puis cliquez sur **plus d'actions > État > en ligne**.

Mettez à niveau Cloud Volumes ONTAP

BlueXP vous avertit lorsqu'une nouvelle version est disponible pour la mise à niveau. Vous pouvez démarrer le processus de mise à niveau à partir de cette notification. Pour plus de détails, voir [Mise à niveau depuis les notifications BlueXP](#).

Une autre façon d'effectuer des mises à niveau logicielles à l'aide d'une image sur une URL externe. Cette option est utile si BlueXP ne peut pas accéder au compartiment S3 pour mettre à niveau le logiciel ou si vous avez reçu un correctif. Pour plus de détails, voir [https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap/Mise à niveau à partir d'une image disponible sur une URL](https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap/Mise%20à%20niveau%20à%20partir%20d'une%20image%20disponible%20sur%20une%20URL).

Mise à niveau depuis les notifications BlueXP

BlueXP affiche une notification dans les environnements de travail Cloud Volumes ONTAP lorsqu'une nouvelle version de Cloud Volumes ONTAP est disponible :



Vous pouvez lancer le processus de mise à niveau à partir de cette notification, qui automatise le processus en obtenant l'image logicielle à partir d'un compartiment S3, en installant l'image, puis en redémarrant le système.

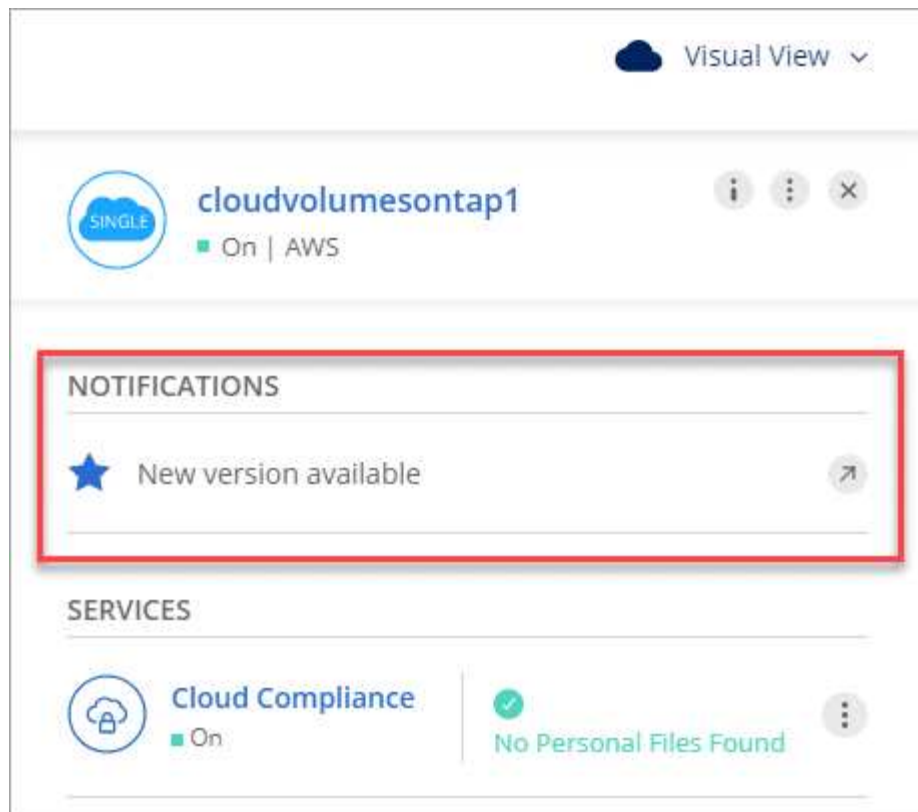
Avant de commencer

Les opérations BlueXP, telles que la création de volume ou d'agrégat, ne doivent pas être en cours sur le système Cloud Volumes ONTAP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sélectionnez un environnement de travail.

Une notification s'affiche dans le volet droit si une nouvelle version est disponible :



3. Si une nouvelle version est disponible, cliquez sur **Upgrade**.
4. Dans la page informations sur la version, cliquez sur le lien pour lire les notes de version de la version spécifiée, puis cochez la case **J'ai lu...**
5. Dans la page du contrat de licence utilisateur final (CLUF), lisez le CLUF, puis sélectionnez **J'ai lu et approuvé le CLUF**.
6. Dans la page Revue et approbation, lisez les notes importantes, sélectionnez **Je comprends...**, puis cliquez sur **Go**.

Résultat

BlueXP démarre la mise à niveau du logiciel. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Mise à niveau à partir d'une image disponible sur une URL

Vous pouvez placer l'image du logiciel Cloud Volumes ONTAP sur le connecteur ou sur un serveur HTTP, puis lancer la mise à niveau du logiciel depuis BlueXP. Vous pouvez utiliser cette option si BlueXP ne peut pas accéder au compartiment S3 pour mettre à niveau le logiciel.

Avant de commencer

- Les opérations BlueXP, telles que la création de volume ou d'agrégat, ne doivent pas être en cours sur le système Cloud Volumes ONTAP.
- Si vous utilisez HTTPS pour héberger des images ONTAP, la mise à niveau peut échouer en raison de problèmes d'authentification SSL, qui sont causés par des certificats manquants. La solution consiste à générer et à installer un certificat signé CA à utiliser pour l'authentification entre ONTAP et BlueXP.

Accédez à la base de connaissances NetApp pour obtenir des instructions détaillées :

["Base de connaissances NetApp : comment configurer BlueXP en tant que serveur HTTPS pour héberger les images de mise à niveau"](#)

Étapes

1. Facultatif : configurez un serveur HTTP pouvant héberger l'image logicielle Cloud Volumes ONTAP.

Si vous disposez d'une connexion VPN au réseau virtuel, vous pouvez placer l'image logicielle Cloud Volumes ONTAP sur un serveur HTTP de votre propre réseau. Sinon, vous devez placer le fichier sur un serveur HTTP dans le cloud.

2. Si vous utilisez votre propre groupe de sécurité pour Cloud Volumes ONTAP, assurez-vous que les règles sortantes autorisent les connexions HTTP afin que Cloud Volumes ONTAP puisse accéder à l'image logicielle.



Le groupe de sécurité Cloud Volumes ONTAP prédéfini permet par défaut les connexions HTTP sortantes.

3. Obtenez l'image logicielle de ["Le site de support NetApp"](#).
4. Copiez l'image du logiciel dans un répertoire du connecteur ou sur un serveur HTTP à partir duquel le fichier sera servi.

Deux chemins sont disponibles. Le chemin correct dépend de la version de votre connecteur.

- ° /opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
- ° /opt/application/netapp/cloudmanager/ontap/images/

5. Dans l'environnement de travail de BlueXP, cliquez sur l'icône de menu, puis sur **Avancé > mettre à jour Cloud Volumes ONTAP**.
6. Sur la page de mise à jour du logiciel, entrez l'URL, puis cliquez sur **changer l'image**.

Si vous avez copié l'image logicielle sur le connecteur dans le chemin indiqué ci-dessus, entrez l'URL suivante :

`http://<Connector-private-IP-address>/ontap/images/<image-file-name>`

7. Cliquez sur **Continuer** pour confirmer.

Résultat

BlueXP démarre la mise à jour logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Corrigez les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT

Le connecteur télécharge automatiquement les mises à jour logicielles pour Cloud Volumes ONTAP. Le téléchargement peut échouer si votre configuration utilise une passerelle NAT Google Cloud. Vous pouvez corriger ce problème en limitant le nombre de pièces dans lesquelles l'image logicielle est divisée. Cette étape doit être effectuée à l'aide de l'API BlueXP.

Étape

1. Soumettre une demande PUT à /ocm/config au format JSON suivant :

```
{
  "maxDownloadSessions": 32
}
```

La valeur de *maxDownloadSessions* peut être 1 ou n'importe quel entier supérieur à 1. Si la valeur est 1, l'image téléchargée ne sera pas divisée.

Notez que 32 est un exemple de valeur. La valeur que vous devez utiliser dépend de votre configuration NAT et du nombre de sessions que vous pouvez avoir simultanément.

["En savoir plus sur l'appel API /ocm/config"](#).

Enregistrement des systèmes de paiement à l'utilisation

Le support de NetApp est inclus avec les systèmes de facturation Cloud Volumes ONTAP, mais vous devez d'abord activer le support en enregistrant les systèmes NetApp.

L'enregistrement d'un système PAYGO avec NetApp est requis pour mettre à niveau le logiciel ONTAP à l'aide des méthodes indiquées ["décrit sur cette page"](#).



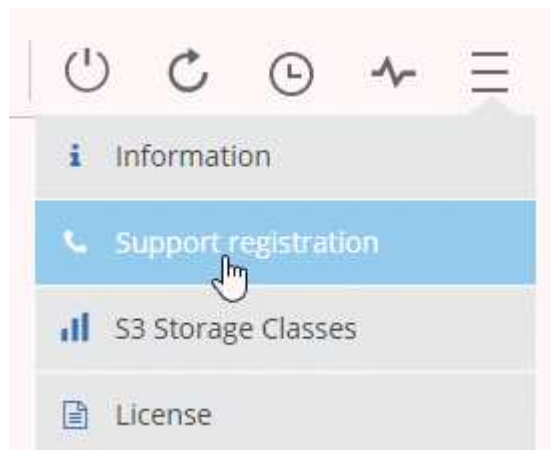
Un système qui n'est pas enregistré pour le support recevra toujours les notifications de mise à jour de logiciel qui apparaissent dans BlueXP lorsqu'une nouvelle version est disponible. Mais vous devrez enregistrer le système avant de pouvoir mettre à niveau le logiciel.

Étapes

1. Si vous n'avez pas encore ajouté votre compte sur le site de support NetApp à BlueXP, accédez à **Paramètres du compte** et ajoutez-le maintenant.

["Découvrez comment ajouter des comptes au site de support NetApp"](#).

2. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**
3. Sur la page Canevas, double-cliquez sur le nom du système que vous souhaitez enregistrer.
4. Cliquez sur l'icône du menu, puis sur **support Registration** :



5. Sélectionnez un compte sur le site de support NetApp et cliquez sur **Register**.

Résultat

BlueXP enregistre le système avec NetApp.

Gestion de l'état du Cloud Volumes ONTAP

Vous pouvez arrêter et démarrer Cloud Volumes ONTAP depuis BlueXP pour gérer vos coûts de calcul du cloud.

Planification des arrêts automatiques de Cloud Volumes ONTAP

Vous pouvez arrêter Cloud Volumes ONTAP à des intervalles réguliers afin de réduire les coûts de calcul. Au lieu de le faire manuellement, vous pouvez configurer BlueXP pour qu'il s'arrête automatiquement puis redémarre les systèmes à des moments spécifiques.

Description de la tâche

- Lorsque vous planifiez un arrêt automatique de votre système Cloud Volumes ONTAP, BlueXP reporte l'arrêt si un transfert de données actif est en cours.

BlueXP arrête le système une fois le transfert terminé.

- Cette tâche planifie les arrêts automatiques des deux nœuds d'une paire haute disponibilité.
- Les snapshots des disques de démarrage et racine ne sont pas créés lors de la mise hors tension de Cloud Volumes ONTAP au cours des arrêts programmés.

Les instantanés sont automatiquement créés uniquement lors d'un arrêt manuel, comme décrit dans la section suivante.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône horloge :



2. Spécifiez la planification de l'arrêt :

- a. Choisissez si vous souhaitez arrêter le système tous les jours, tous les jours de semaine, tous les week-ends ou toute combinaison des trois options.
- b. Indiquez quand vous souhaitez désactiver le système et pendant combien de temps vous voulez le désactiver.

Exemple


L'image suivante montre un programme qui demande à BlueXP d'arrêter le système tous les samedis à 12 h 00 pendant 48 heures. BlueXP redémarre le système tous les lundis à 12:00

☐ **Turn off every weekday**
 Mon, Tue, Wed, Thu, Fri
 turn off at 08 : 00 PM for 12 Hours (1-24)

☒ **Turn off every weekend**
 Sat
 turn off at 12 : 00 AM for 48 Hours (1-48)

3. Cliquez sur **Enregistrer**.

Résultat

BlueXP enregistre le planning. L'icône de l'horloge change pour indiquer qu'un programme est défini : 

Arrêt d'Cloud Volumes ONTAP

L'arrêt de Cloud Volumes ONTAP vous permet d'économiser de l'espace de calcul et de créer des snapshots des disques racines et de démarrage, ce qui peut être utile pour la résolution des problèmes.



Pour réduire les coûts, BlueXP supprime régulièrement les anciens snapshots des disques racine et de démarrage. Seuls les deux instantanés les plus récents sont conservés pour les disques racine et de démarrage.

Description de la tâche

Lorsque vous arrêtez une paire haute disponibilité, BlueXP arrête les deux nœuds.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **Désactiver**.



2. Conservez l'option de création de snapshots activés car les snapshots peuvent activer la récupération du système.

3. Cliquez sur **Désactiver**.

L'arrêt du système peut prendre jusqu'à quelques minutes. Vous pouvez redémarrer les systèmes ultérieurement à partir de la page de l'environnement de travail.

Synchronisez l'heure du système à l'aide du protocole NTP

La spécification d'un serveur NTP synchronise l'heure entre les systèmes de votre réseau, ce qui peut aider à éviter les problèmes dus aux différences de temps.

Spécifiez un serveur NTP à l'aide de ["API BlueXP"](#) ou depuis l'interface utilisateur lorsque vous ["Créer un serveur CIFS"](#).

Modifier la vitesse d'écriture du système

BlueXP vous permet de choisir une vitesse d'écriture normale ou élevée pour Cloud Volumes ONTAP. La vitesse d'écriture par défaut est normale. Vous pouvez passer à une vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides.

Une vitesse d'écriture élevée est prise en charge avec tous les types de systèmes à un nœud et certaines configurations de paires HA. Affichez les configurations prises en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#)

Avant de modifier la vitesse d'écriture, vous devez ["comprendre les différences entre les réglages normaux et élevés"](#).

Description de la tâche

- Assurez-vous que les opérations telles que la création de volume ou d'agrégat ne sont pas en cours.
- Notez que cette modification redémarre le système Cloud Volumes ONTAP. Il s'agit d'un processus perturbateur qui requiert des temps d'indisponibilité pour l'ensemble du système.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > vitesse d'écriture**.
2. Sélectionnez **Normal** ou **Haut**.

Si vous choisissez Haut, vous devrez lire l'énoncé « Je comprends... » et confirmer en cochant la case.

3. Cliquez sur **Enregistrer**, vérifiez le message de confirmation, puis cliquez sur **Continuer**.

Changer le mot de passe pour Cloud Volumes ONTAP

Cloud Volumes ONTAP inclut un compte d'administration de cluster. Vous pouvez modifier le mot de passe de ce compte depuis BlueXP, si nécessaire.



Vous ne devez pas modifier le mot de passe du compte admin via System Manager ou l'interface de ligne de commande. Le mot de passe ne sera pas reflété dans BlueXP. Par conséquent, BlueXP ne peut pas contrôler l'instance correctement.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > définir mot de passe**.
2. Saisissez le nouveau mot de passe deux fois, puis cliquez sur **Enregistrer**.

Le nouveau mot de passe doit être différent de l'un des six derniers mots de passe utilisés.

Ajouter, supprimer ou supprimer des systèmes

Ajout de systèmes Cloud Volumes ONTAP existants à BlueXP

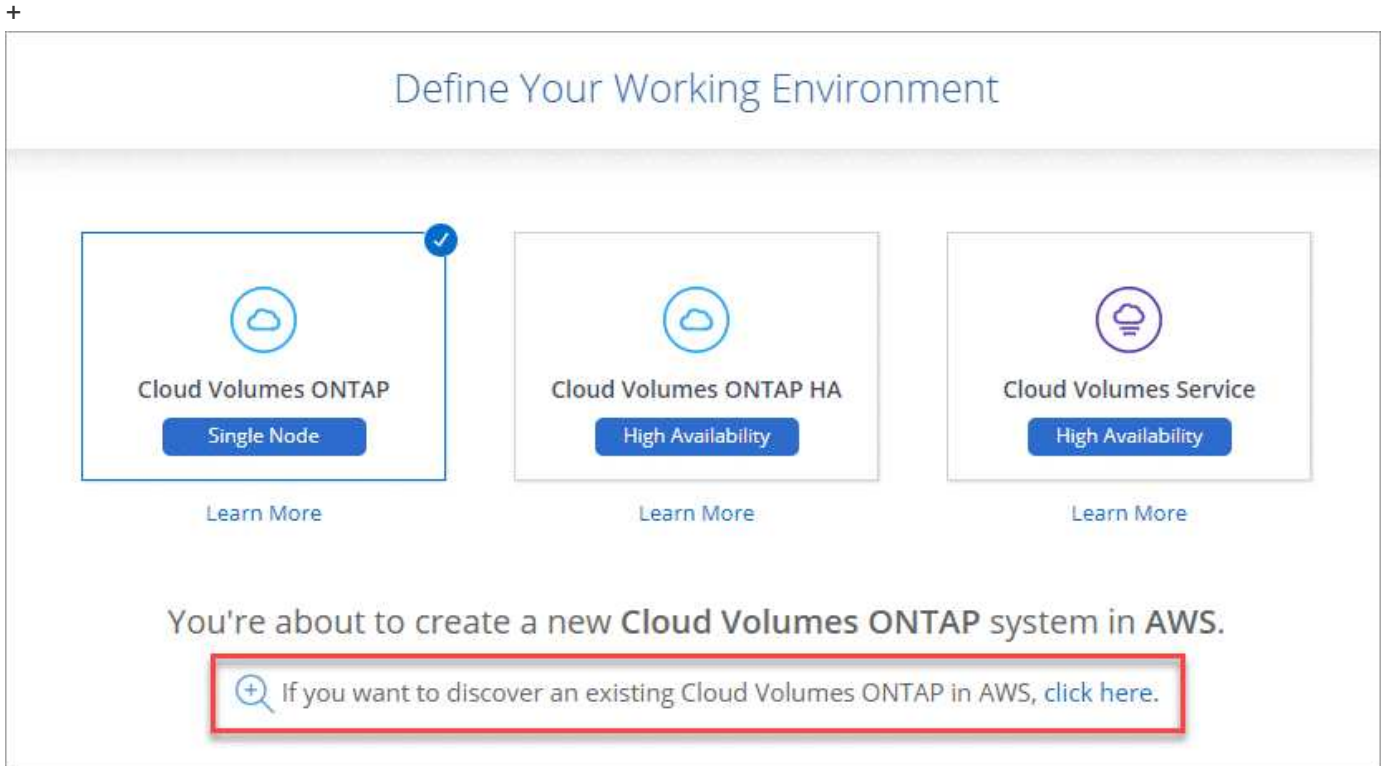
Vous pouvez découvrir et ajouter des systèmes Cloud Volumes ONTAP existants à BlueXP. Vous pouvez le faire si vous avez déployé un nouveau système BlueXP.

Avant de commencer

Vous devez connaître le mot de passe du compte d'administrateur Cloud Volumes ONTAP.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, cliquez sur **Ajouter un environnement de travail**.
3. Sélectionnez le fournisseur de cloud dans lequel réside le système.
4. Choisissez le type de système Cloud Volumes ONTAP.
5. Cliquez sur le lien pour découvrir un système existant.



1. Sur la page Région, choisissez la région dans laquelle les instances sont exécutées, puis sélectionnez les instances.
2. Sur la page informations d'identification, entrez le mot de passe de l'utilisateur administrateur Cloud Volumes ONTAP, puis cliquez sur **Go**.

Résultat

BlueXP ajoute les instances Cloud Volumes ONTAP à l'espace de travail.

Suppression des environnements de travail Cloud Volumes ONTAP

L'administrateur des comptes peut supprimer un environnement de travail Cloud Volumes ONTAP pour le déplacer vers un autre système ou pour résoudre les problèmes de détection.

Description de la tâche

La suppression d'un environnement de travail Cloud Volumes ONTAP le supprime de BlueXP. Il ne supprime pas le système Cloud Volumes ONTAP. Vous pourrez par la suite redécouvrir l'environnement de travail.

La suppression d'un environnement de travail de BlueXP vous permet d'effectuer les opérations suivantes :

- Redécouvrez-le dans un autre espace de travail
- Redécouvrez-le à partir d'un autre système BlueXP
- Redécouvrez-le si vous avez rencontré des problèmes lors de la découverte initiale

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **Outils**.



2. Dans la page Outils, cliquez sur **lancer**.
3. Sélectionnez l'environnement de travail Cloud Volumes ONTAP que vous souhaitez supprimer.
4. Sur la page Revue et approbation, cliquez sur **Go**.

Résultat

BlueXP supprime l'environnement de travail. Les utilisateurs peuvent redécouvrir cet environnement de travail à tout moment à partir de la page Canvas.

Suppression d'un système Cloud Volumes ONTAP

Vous devez toujours supprimer des systèmes Cloud Volumes ONTAP de BlueXP, plutôt que de la console de votre fournisseur cloud. Par exemple, si vous terminez une instance Cloud Volumes ONTAP sous licence par votre fournisseur cloud, vous ne pouvez pas utiliser la clé de licence pour une autre instance. Vous devez supprimer l'environnement de travail de BlueXP pour libérer la licence.

Lorsque vous supprimez un environnement de travail, BlueXP met fin aux instances Cloud Volumes ONTAP et supprime les disques et les snapshots.

Les ressources gérées par d'autres services, tels que les sauvegardes dans le cloud Backup et les instances de Cloud Data Sense and Monitoring, ne sont pas supprimées lors de la suppression d'un environnement de travail. Vous devrez les supprimer manuellement vous-même. Si ce n'est pas le cas, vous continuerez à recevoir des frais pour ces ressources.



Lorsque BlueXP déploie Cloud Volumes ONTAP dans votre fournisseur cloud, il assure la protection des instances. Cette option permet d'éviter les raccords accidentels.

Étapes

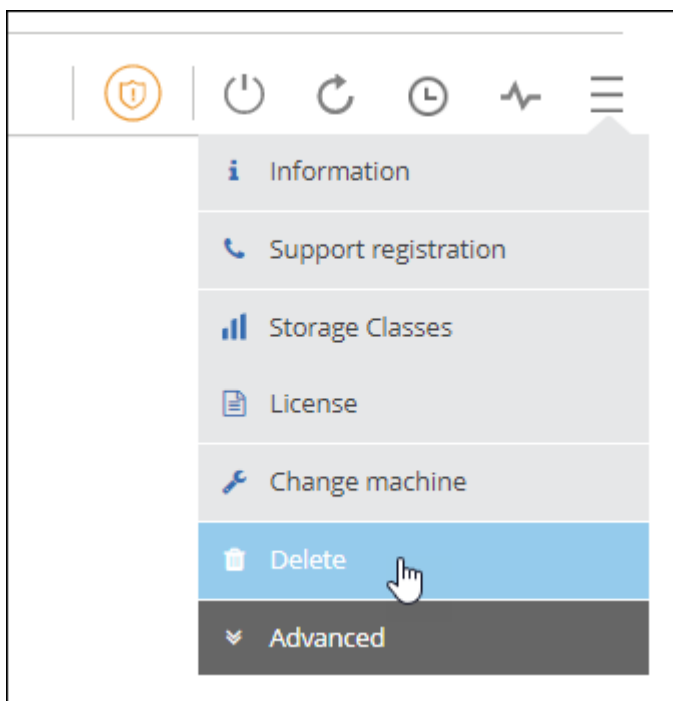
1. Si vous avez activé Cloud Backup dans l'environnement de travail, déterminez si les données sauvegardées sont toujours requises, puis ["supprimez les sauvegardes, si nécessaire"](#).

Cloud Backup est indépendant de Cloud Volumes ONTAP de par sa conception. Cloud Backup ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système Cloud Volumes ONTAP et l'interface utilisateur ne prend pas en charge la suppression des sauvegardes après la suppression du système.

2. Si vous avez activé Cloud Data sur cet environnement de travail et qu'aucun autre environnement de travail n'utilise ce service, vous devrez supprimer l'instance du service.

["En savoir plus sur l'instance Cloud Data SENSE".](#)

3. Supprimer l'environnement de travail Cloud Volumes ONTAP.
 - a. Sur la page Canevas, double-cliquez sur le nom de l'environnement de travail Cloud Volumes ONTAP que vous souhaitez supprimer.
 - b. Cliquez sur l'icône de menu, puis sur **Supprimer**.



- c. Saisissez le nom de l'environnement de travail, puis cliquez sur **Supprimer**.

La suppression de l'environnement de travail peut prendre jusqu'à 5 minutes.

Administration AWS

Modifiez le type d'instance EC2 pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs instances ou types lorsque vous lancez Cloud Volumes ONTAP dans AWS. Vous pouvez modifier le type d'instance à tout moment si vous déterminez qu'il est sous-dimensionné ou surdimensionné en fonction de vos besoins.

Description de la tâche

- Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"](#)

- La modification du type d'instance peut affecter les frais de service AWS.

- L'opération redémarre Cloud Volumes ONTAP.

Pour les systèmes à nœud unique, les E/S sont interrompues.

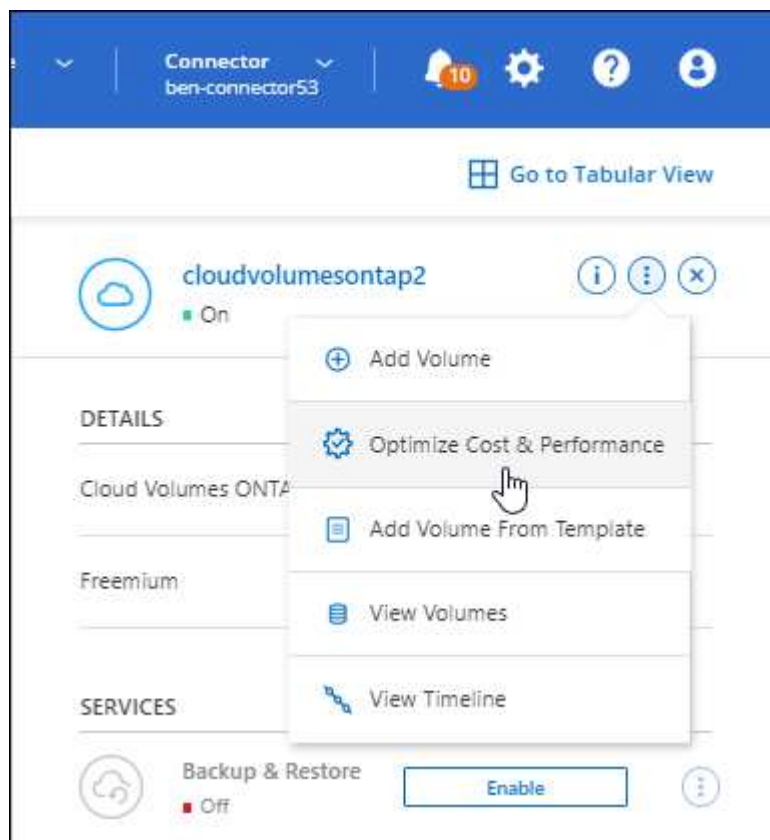
Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.



BlueXP change aisément un nœud à la fois en lançant le basculement et en attente de retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers pendant ce processus et n'a rencontré aucun problème côté client. Au fur et à mesure des changements de connexion, nous avons constaté des tentatives d'E/S au niveau des E/S, mais la couche applicative a pu faire face à ces courtes « connexions » NFS/CIFS.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Dans la zone de travail, sélectionnez l'environnement de travail.
3. Dans le volet de droite, cliquez sur l'icône de menu et sélectionnez **optimiser les coûts et les performances**.



Cette option est également disponible en entrant dans l'environnement de travail, en ouvrant le menu d'action et en sélectionnant **Modifier l'instance**.

4. Si vous utilisez une licence PAYGO basée sur un nœud, vous pouvez éventuellement choisir une licence différente.
5. Choisissez un type d'instance, cochez la case pour confirmer que vous comprenez les implications de la modification, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

Modifier les tables de routage pour les paires HA dans plusieurs AZS

Vous pouvez modifier les tables de routage AWS qui incluent des routes vers les adresses IP flottantes pour une paire HA déployée dans plusieurs zones de disponibilité AWS (AZS). Vous pouvez le faire si les nouveaux clients NFS ou CIFS ont besoin d'accéder à une paire haute disponibilité dans AWS.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur **tables de routage**.
3. Modifiez la liste des tables de routage sélectionnées, puis cliquez sur **Enregistrer**.

Résultat

BlueXP envoie une demande AWS pour modifier les tables de routage.

Contrôle des coûts des ressources AWS

BlueXP vous permet de consulter les coûts des ressources associés à l'exécution de Cloud Volumes ONTAP dans AWS. Vous pouvez également voir les économies réalisées grâce aux fonctionnalités NetApp qui permettent de réduire les coûts de stockage.

Description de la tâche

BlueXP met à jour les coûts lorsque vous actualisez la page. Vous devez vous référer à AWS pour plus de détails sur le coût final.

Étape

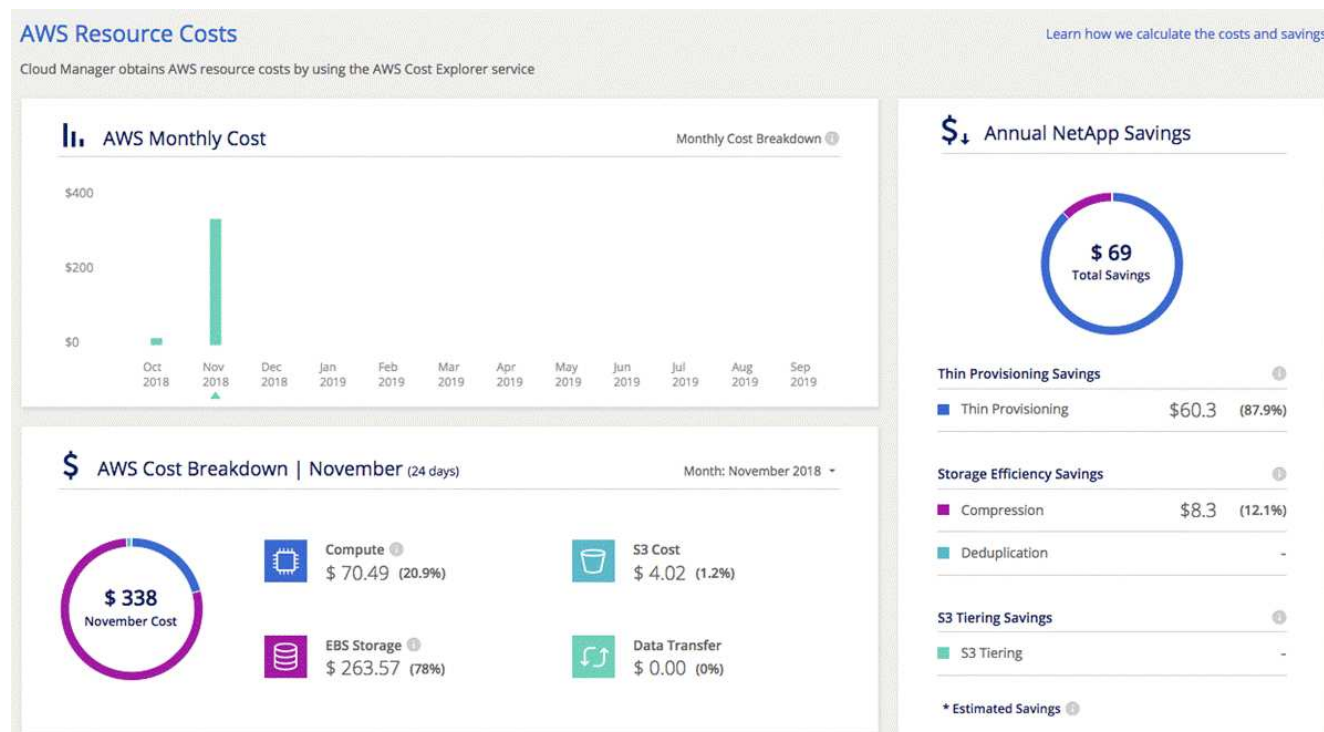
1. Vérifiez que BlueXP peut obtenir des informations de coût depuis AWS :
 - a. Assurez-vous que la stratégie IAM qui fournit des autorisations à BlueXP inclut les autorisations requises.

["Afficher les autorisations requises"](#)
 - b. ["Activer la balise WorkingEnvironnement"](#).

Pour suivre vos coûts AWS, BlueXP attribue une balise d'allocation des coûts aux instances Cloud Volumes ONTAP. Après avoir créé votre premier environnement de travail, activez la balise **WorkingEnvironment,Id**. Les balises définies par l'utilisateur n'apparaissent pas dans les rapports de facturation AWS tant que vous ne les activez pas dans la console de facturation et de gestion des coûts.
2. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
3. Sur la page Canvas, sélectionnez un environnement de travail Cloud Volumes ONTAP, puis cliquez sur **coût**.

La page coûts affiche les coûts des mois actuels et précédents et présente vos économies annuelles sur les produits NetApp, si vous avez activé les fonctions d'économies de volumes offertes par NetApp.

L'image suivante montre un exemple de page de coût :



Administration d'Azure

Modifier le type de machine virtuelle Azure pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs types de machines virtuelles lorsque vous lancez Cloud Volumes ONTAP dans Microsoft Azure. Vous pouvez modifier à tout moment le type de machine virtuelle si vous déterminez qu'elle est sous-dimensionnée ou trop dimensionnée pour répondre à vos besoins.

Description de la tâche

- Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"](#)

- La modification du type de machine virtuelle peut affecter les frais de service Microsoft Azure.
- L'opération redémarre Cloud Volumes ONTAP.

Pour les systèmes à nœud unique, les E/S sont interrompues.

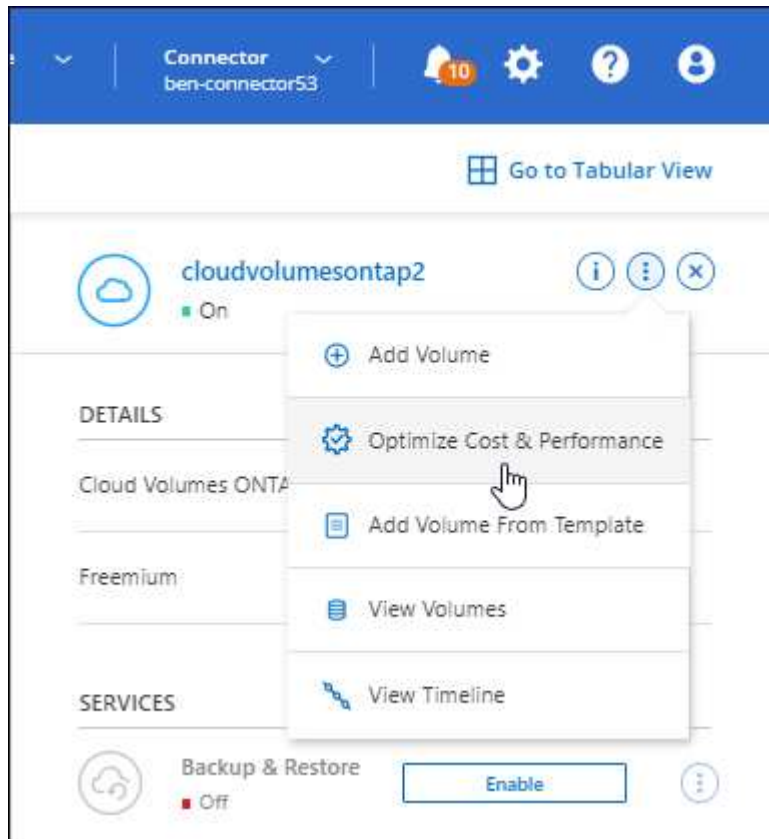
Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.



BlueXP change aisément un nœud à la fois en lançant le basculement et en attente de retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers pendant ce processus et n'a rencontré aucun problème côté client. Au fur et à mesure des changements de connexion, nous avons constaté des tentatives d'E/S au niveau des E/S, mais la couche applicative a pu faire face à ces courtes « connexions » NFS/CIFS.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Dans la zone de travail, sélectionnez l'environnement de travail.
3. Dans le volet de droite, cliquez sur l'icône de menu et sélectionnez **optimiser les coûts et les performances**.



Cette option est également disponible en entrant dans l'environnement de travail, en ouvrant le menu d'action et en sélectionnant **changer VM**.

4. Si vous utilisez une licence PAYGO basée sur un nœud, vous pouvez éventuellement choisir une licence différente.
5. Sélectionnez un type de VM, cochez la case pour confirmer que vous comprenez les implications de la modification, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

Remplacement des verrouillages CIFS pour les paires haute disponibilité Cloud Volumes ONTAP dans Azure

L'administrateur du compte peut activer un paramètre dans BlueXP qui empêche tout problème lié au rétablissement du stockage Cloud Volumes ONTAP lors des événements de maintenance Azure. Lorsque vous activez ce paramètre, Cloud Volumes ONTAP vetoes les verrous CIFS et réinitialise les sessions CIFS actives.

Description de la tâche

Microsoft Azure planifie des événements de maintenance périodiques sur ses machines virtuelles. Lorsqu'un événement de maintenance se produit sur une paire haute disponibilité Cloud Volumes ONTAP, la paire haute disponibilité déclenche le basculement du stockage. Si des sessions CIFS sont actives au cours de cet événement de maintenance, les verrous sur les fichiers CIFS peuvent empêcher tout rétablissement du stockage.

Si vous activez ce paramètre, Cloud Volumes ONTAP veto aux verrous et réinitialise les sessions CIFS actives. Par conséquent, la paire haute disponibilité peut terminer le rétablissement du stockage lors de ces événements de maintenance.



Ce processus peut entraîner des perturbations pour les clients CIFS. Les données qui ne sont pas validées auprès des clients CIFS pourraient être perdues.

Ce dont vous avez besoin

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. ["Découvrez comment"](#).

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.



2. Sous **Azure**, cliquez sur **verrous CIFS Azure pour les environnements de travail Azure HA**.
3. Cochez la case pour activer la fonctionnalité, puis cliquez sur **Enregistrer**.

Utilisez une liaison privée Azure ou des terminaux de service

Cloud Volumes ONTAP utilise une liaison privée Azure pour les connexions aux comptes de stockage associés. Si nécessaire, vous pouvez désactiver les liens privés Azure et utiliser les terminaux de service.

Présentation

Par défaut, BlueXP active une liaison privée Azure pour les connexions entre Cloud Volumes ONTAP et ses comptes de stockage associés. Azure Private Link sécurise les connexions entre les terminaux dans Azure et offre les avantages en termes de performances.

Si nécessaire, vous pouvez configurer Cloud Volumes ONTAP de sorte qu'il utilise des terminaux de service au lieu d'une liaison privée Azure.

Dans les deux cas, BlueXP limite toujours l'accès réseau pour les connexions entre Cloud Volumes ONTAP et les comptes de stockage. L'accès au réseau est limité au vnet sur lequel Cloud Volumes ONTAP est déployé et au vnet sur lequel le connecteur est déployé.

Désactivez les liens privés Azure et utilisez plutôt les terminaux de service

Si votre entreprise le requiert, vous pouvez modifier un paramètre dans BlueXP afin qu'il configure Cloud Volumes ONTAP pour qu'il utilise des points de terminaison de service au lieu d'un lien privé Azure. La modification de ce paramètre s'applique aux nouveaux systèmes Cloud Volumes ONTAP que vous créez.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.
2. Sous **Azure**, cliquez sur **Use Azure Private Link**.
3. Désélectionnez **connexion de liaison privée entre Cloud Volumes ONTAP et les comptes de stockage**.
4. Cliquez sur **Enregistrer**.

Utilisation des liens privés Azure

Dans la plupart des cas, rien n'est nécessaire pour configurer des liens privés Azure avec Cloud Volumes ONTAP. BlueXP gère des liens privés Azure pour vous. Mais si vous utilisez le DNS privé Azure, vous devrez modifier un fichier de configuration. Vous devez également connaître une exigence pour l'emplacement du connecteur dans Azure.

Fonctionnement des connexions Private Link

Lorsque BlueXP déploie Cloud Volumes ONTAP dans Azure, il crée un noeud final privé dans le groupe de ressources. Le terminal privé est associé aux comptes de stockage pour Cloud Volumes ONTAP. Par conséquent, l'accès au stockage Cloud Volumes ONTAP transite par le réseau de backbone Microsoft.

L'accès client passe par la liaison privée lorsque les clients se trouvent dans le même VNet que Cloud Volumes ONTAP, dans les VNets péré ou dans votre réseau sur site lors de l'utilisation d'une connexion VPN ou ExpressRoute privée au VNet.

Voici un exemple illustrant l'accès des clients par liaison privée à partir d'un même réseau vnet et d'un réseau sur site doté d'une connexion VPN ou ExpressRoute privée.



Emplacement du connecteur dans Azure

Le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère ou dans ["Paire de régions Azure"](#) Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

Fournissez BlueXP avec des informations détaillées sur votre DNS privé Azure

Si vous utilisez ["DNS privé Azure"](#), Vous devez ensuite modifier un fichier de configuration sur chaque connecteur. Sinon, BlueXP ne peut pas activer la connexion Azure Private Link entre Cloud Volumes ONTAP et les comptes de stockage associés.

Notez que le nom DNS doit correspondre aux exigences de nommage des DNS Azure ["Comme illustré dans la documentation Azure"](#).

Étapes

1. SSH vers l'hôte du connecteur et connectez-vous.
2. Accédez au répertoire suivant : `/opt/application/netapp/cloudManager/docker_ocm/data`
3. Modifiez APP.conf en ajoutant le paramètre "User-private-dns-zone-settings" avec les paires de valeur-mot-clé suivantes :

```
"user-private-dns-zone-settings" : {  
  "resource-group" : "<resource group name of the DNS zone>",  
  "subscription" : "<subscription ID>",  
  "use-existing" : true  
}
```

Le paramètre doit être entré au même niveau que « system-ID » comme indiqué ci-dessous :

```
"system-id" : "<system ID>",  
"user-private-dns-zone-settings" : {
```

Notez que le mot-clé d'abonnement n'est requis que si la zone DNS privée existe dans un abonnement différent de celui du connecteur.

4. Enregistrez le fichier et déconnectez le connecteur.

Aucun redémarrage n'est requis.

Activer la restauration en cas d'échec

Si BlueXP ne parvient pas à créer un lien privé Azure dans le cadre d'actions spécifiques, il termine l'action sans la connexion Azure Private Link. Cela peut se produire lors de la création d'un environnement de travail (nœud unique ou paire HA), ou lors des actions suivantes sur une paire HA : création d'un agrégat, ajout de disques à un agrégat existant ou création d'un nouveau compte de stockage lorsque l'on dépasse les 32 Tio.

Vous pouvez modifier ce comportement par défaut en activant la restauration si BlueXP ne parvient pas à créer Azure Private Link. Cela permet de vous assurer que vous êtes en parfaite conformité avec les réglementations de sécurité de votre entreprise.

Si vous activez la restauration, BlueXP arrête l'action et annule toutes les ressources créées dans le cadre de l'action.

L'activation de la restauration est prise en charge via l'API uniquement.

Étape

1. Utilisez le PUT `/occm/config` Appel d'API avec le corps de demande suivant :

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Déplacement de groupes de ressources

Cloud Volumes ONTAP prend en charge les déplacements des groupes de ressources Azure, mais le workflow se produit uniquement dans la console Azure.

Vous pouvez déplacer un environnement de travail d'un groupe de ressources vers un autre groupe de ressources dans Azure au sein du même abonnement Azure. Le déplacement de groupes de ressources entre différents abonnements Azure n'est pas pris en charge.

Étapes

1. Supprimez l'environnement de travail de **Canvas**.

Pour savoir comment supprimer un environnement de travail, voir ["Suppression des environnements de travail Cloud Volumes ONTAP"](#).

2. Exécutez le déplacement du groupe de ressources dans la console Azure.

Pour terminer le déplacement, reportez-vous à la section ["Déplacez des ressources vers un nouveau groupe de ressources ou un nouvel abonnement dans la documentation de Microsoft Azure"](#).

3. Dans **Canvas**, découvrez l'environnement de travail.
4. Recherchez le nouveau groupe de ressources dans les informations relatives à l'environnement de travail.

Résultat

L'environnement de travail et ses ressources (machines virtuelles, disques, comptes de stockage, interfaces réseau, snapshots) font partie du nouveau groupe de ressources.

Administration Google Cloud

Modifier le type de machine Google Cloud pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs types de machines lorsque vous lancez Cloud Volumes ONTAP dans Google Cloud. Vous pouvez modifier l'instance ou le type de machine à tout moment si vous déterminez qu'elle est sous-dimensionnée ou surdimensionnée en fonction de vos besoins.

Description de la tâche

- Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"](#)

- La modification du type de machine peut affecter les frais de service Google Cloud.
- L'opération redémarre Cloud Volumes ONTAP.

Pour les systèmes à nœud unique, les E/S sont interrompues.

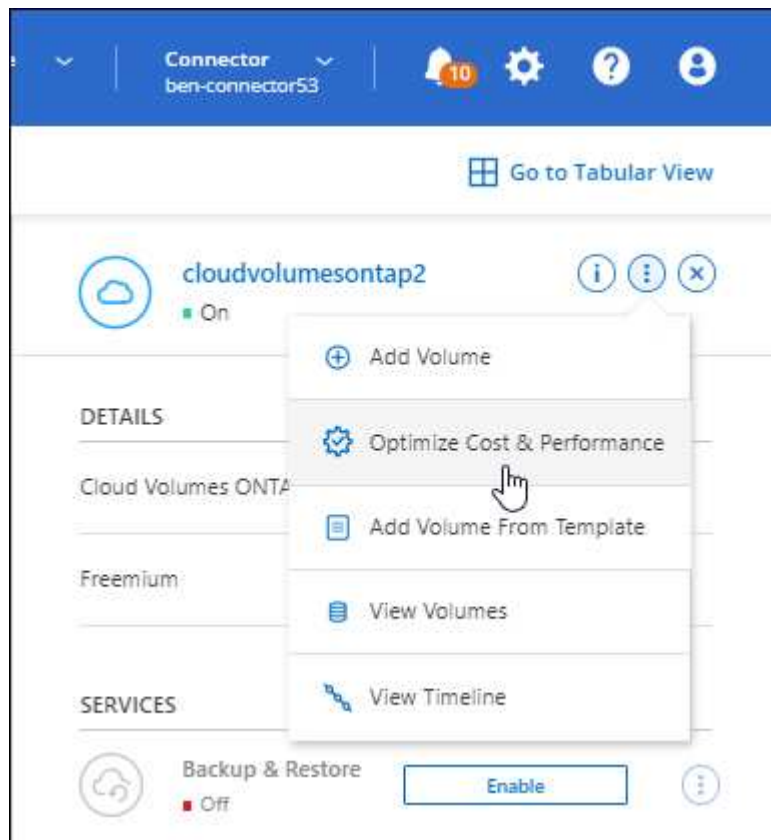
Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.



BlueXP change aisément un nœud à la fois en lançant le basculement et en attente de retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers pendant ce processus et n'a rencontré aucun problème côté client. Au fur et à mesure des changements de connexion, nous avons constaté des tentatives d'E/S au niveau des E/S, mais la couche applicative a pu faire face à ces courtes « connexions » NFS/CIFS.

Étapes

1. Dans la zone de travail, sélectionnez l'environnement de travail.
2. Dans le volet de droite, cliquez sur l'icône de menu et sélectionnez **optimiser les coûts et les performances**.



Cette option est également disponible en entrant dans l'environnement de travail, en ouvrant le menu d'action et en sélectionnant **changer machine**.

3. Si vous utilisez une licence PAYGO basée sur un nœud, vous pouvez éventuellement choisir une licence différente.
4. Sélectionnez un type de machine, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

Administrer Cloud Volumes ONTAP à l'aide de la vue avancée

Si vous avez besoin d'effectuer une gestion avancée d'Cloud Volumes ONTAP, vous pouvez utiliser ONTAP System Manager, interface de gestion fournie avec un système ONTAP. Nous avons inclus l'interface System Manager directement dans BlueXP afin que vous n'ayez pas besoin de laisser BlueXP pour une gestion avancée.

Cette vue avancée est disponible sous forme d'aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

Caractéristiques

La vue avancée de BlueXP vous donne accès à des fonctions de gestion supplémentaires :

- Gestion avancée du stockage

Gestion des groupes de cohérence, des partages, des qtrees, des quotas et des machines virtuelles de stockage.

- Gestion de la mise en réseau

Gérez les IPspaces, les interfaces réseau, les ensembles de ports et les ports ethernet.

- Événements et travaux

Affichez les journaux d'événements, les alertes système, les tâches et les journaux d'audit.

- Protection avancée des données

Protection des VM de stockage, des LUN et des groupes de cohérence

- Gestion des hôtes

Configurez les groupes initiateurs SAN et les clients NFS.

Configurations compatibles

La gestion avancée via System Manager est prise en charge avec Cloud Volumes ONTAP 9.10.0 et versions ultérieures dans les régions cloud standard.

L'intégration de System Manager n'est pas prise en charge dans les régions GovCloud ni dans les régions ne disposant pas d'accès Internet sortant.

Limites

Quelques fonctionnalités qui s'affichent dans l'interface de System Manager ne sont pas prises en charge avec Cloud Volumes ONTAP :

- Tiering dans le cloud

Le service NetApp Cloud Tiering n'est pas pris en charge par Cloud Volumes ONTAP. Le Tiering des données vers le stockage objet doit être configuré directement depuis la vue standard de BlueXP lors de la création de volumes.

- Tiers

La gestion des agrégats (y compris les niveaux locaux et les niveaux cloud) n'est pas prise en charge par System Manager. Vous devez gérer des agrégats directement depuis BlueXP Standard View.

- Mises à niveau du micrologiciel

Les mises à jour automatiques du micrologiciel de la page **Cluster > Paramètres** ne sont pas prises en charge avec Cloud Volumes ONTAP.

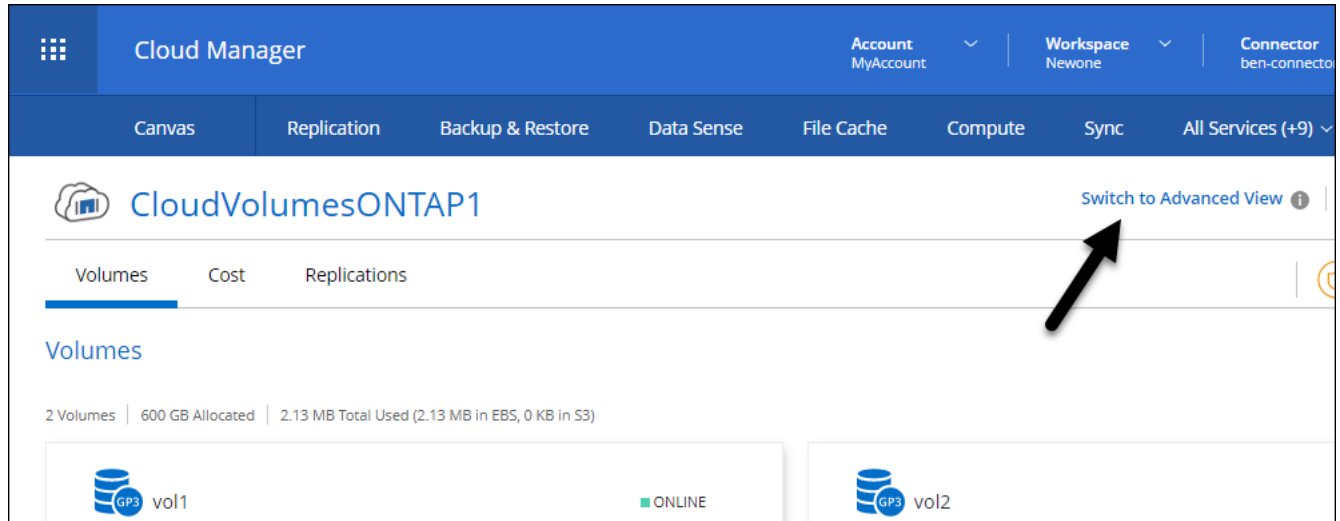
Par ailleurs, le contrôle d'accès basé sur des rôles depuis System Manager n'est pas pris en charge.

Comment démarrer

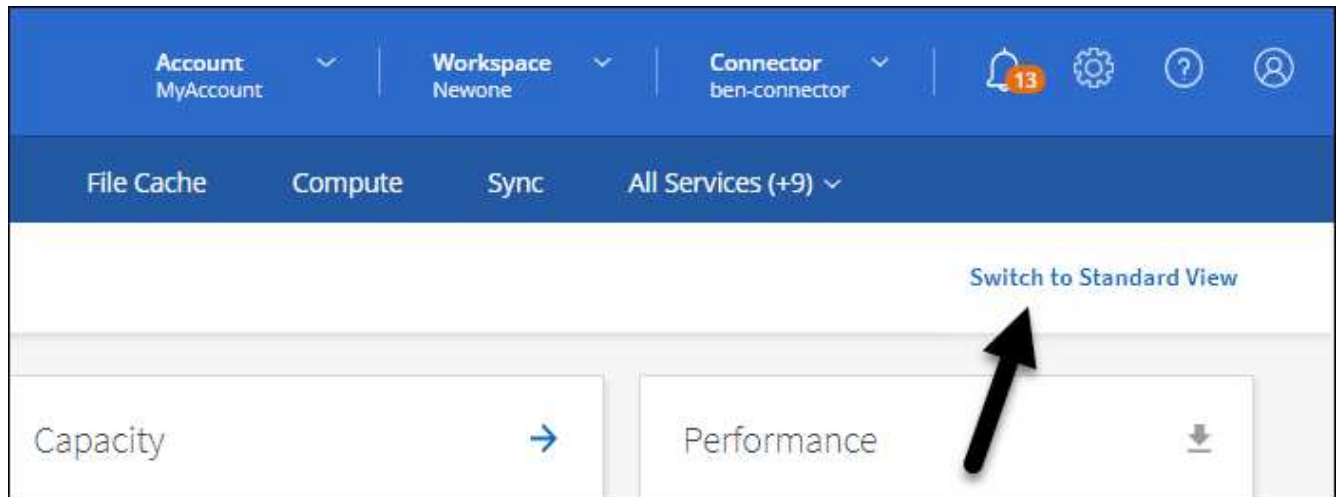
Ouvrez un environnement de travail Cloud Volumes ONTAP et cliquez sur l'option vue avancée.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
2. Sur la page Canvas, double-cliquez sur le nom d'un système Cloud Volumes ONTAP.
3. Dans le coin supérieur droit, cliquez sur **basculer vers la vue avancée**.



4. Si le message de confirmation apparaît, lisez-le et cliquez sur **Fermer**.
5. Utilisez System Manager pour gérer Cloud Volumes ONTAP.
6. Si nécessaire, cliquez sur **basculer vers la vue standard** pour revenir à la gestion standard via BlueXP.



Aide sur l'utilisation de System Manager

Si vous avez besoin d'aide pour utiliser System Manager avec Cloud Volumes ONTAP, vous pouvez voir ["Documentation ONTAP"](#) pour obtenir des instructions détaillées. Voici quelques liens utiles :

- ["Gestion des volumes et des LUN"](#)
- ["Gestion du réseau"](#)

- "Protection des données"

Administration de Cloud Volumes ONTAP à partir de l'interface de ligne de commandes

L'interface de ligne de commandes Cloud Volumes ONTAP vous permet d'exécuter toutes les commandes d'administration et de choisir les tâches avancées ou si vous vous sentez plus à l'aide de l'interface de ligne de commandes. Vous pouvez vous connecter à l'interface de ligne de commande à l'aide de Secure Shell (SSH).

Avant de commencer

L'hôte à partir duquel vous utilisez SSH pour vous connecter à Cloud Volumes ONTAP doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être utiliser SSH d'un hôte sauter qui se trouve sur le réseau de votre fournisseur de cloud.



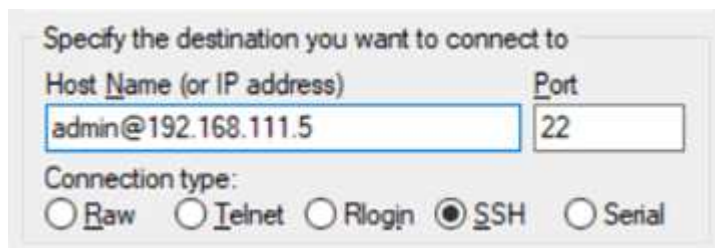
Lorsqu'elles sont déployées dans plusieurs environnements AZS, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion de cluster, ce qui signifie que le routage externe n'est pas disponible. Vous devez vous connecter à partir d'un hôte faisant partie du même domaine de routage.

Étapes

1. Dans BlueXP, identifiez l'adresse IP de l'interface de gestion de cluster :
 - a. Dans le menu de navigation de gauche, sélectionnez **stockage > Canvas**.
 - b. Sur la page Canevas, sélectionnez le système Cloud Volumes ONTAP.
 - c. Copiez l'adresse IP de gestion du cluster qui apparaît dans le volet droit.
2. Utilisez SSH pour vous connecter à l'adresse IP de l'interface de gestion du cluster à l'aide du compte admin.

Exemple

L'image suivante montre un exemple utilisant PuTTY :



3. À l'invite de connexion, entrez le mot de passe du compte admin.

Exemple

```
Password: *****
COT2::>
```

État de santé du système et événements

Vérifiez la configuration de AutoSupport

AutoSupport surveille de manière proactive l'état de santé de votre système et envoie des messages au support technique NetApp. Par défaut, AutoSupport est activé sur chaque nœud pour envoyer des messages au support technique via le protocole de transport HTTPS. Il est préférable de vérifier que AutoSupport peut envoyer ces messages.

La seule étape de configuration requise consiste à s'assurer que Cloud Volumes ONTAP dispose d'une connexion Internet sortante. Pour plus d'informations, consultez les exigences de mise en réseau de votre fournisseur de cloud.

Conditions requises pour le AutoSupport

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour l'AutoSupport, qui surveille de manière proactive l'état de santé de votre système et envoie des messages au support technique de NetApp.

Les règles de routage et de pare-feu doivent autoriser le trafic HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

Si aucune connexion Internet sortante n'est disponible pour envoyer des messages AutoSupport, BlueXP configure automatiquement vos systèmes Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy. La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous avez défini des règles sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Après avoir vérifié que l'accès Internet sortant est disponible, vous pouvez tester AutoSupport pour vous assurer qu'il peut envoyer des messages. Pour obtenir des instructions, reportez-vous à la section ["Documentation ONTAP : configuration d'AutoSupport"](#).

Résoudre les problèmes de configuration AutoSupport

Si une connexion sortante n'est pas disponible et que BlueXP ne peut pas configurer votre système Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy, vous recevrez une notification de BlueXP intitulée "<nom de l'environnement de travail> ne peut pas envoyer de messages AutoSupport".

Vous recevez probablement ce message en raison de problèmes de réseau.

Procédez comme suit pour résoudre ce problème.

Étapes

1. SSH vers le système Cloud Volumes ONTAP afin que vous puissiez gérer le système à partir de l'interface de ligne de commandes.

["Découvrez comment SSH vers Cloud Volumes ONTAP"](#).

2. Afficher l'état détaillé du sous-système AutoSupport :

```
autosupport check show-details
```

La réponse doit être similaire à ce qui suit :

```
Category: smtp
  Component: mail-server
    Status: failed
    Detail: SMTP connectivity check failed for destination:
            mailhost. Error: Could not resolve host -
'mailhost'
    Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
    Status: ok
    Detail: Successfully connected to:
            <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
    Status: ok
    Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
    Status: ok
    Detail: Successfully connected to:
            https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
    Status: ok
    Detail: No configuration issues found.
5 entries were displayed.
```

Si l'état de la catégorie http-https est « ok », cela signifie que AutoSupport est configuré correctement et que des messages peuvent être envoyés.

3. Si l'état n'est pas ok, vérifiez l'URL du proxy pour chaque noeud Cloud Volumes ONTAP :

```
autosupport show -fields proxy-url
```

4. Si le paramètre d'URL du proxy est vide, configurez Cloud Volumes ONTAP pour utiliser le connecteur comme proxy :

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. Vérifiez à nouveau l'état du disque AutoSupport :

```
autosupport check show-details
```

6. Si l'état est toujours échec, vérifiez qu'il y a une connectivité entre Cloud Volumes ONTAP et le connecteur sur le port 3128.
7. Si l'ID d'état échoue toujours après vérification de la connectivité, SSH vers le connecteur.

["En savoir plus sur la connexion à la VM Linux pour le connecteur"](#)

8. Accédez à /opt/application/netapp/cloudmanager/docker_occm/data/
9. Ouvrez le fichier de configuration du proxy squid.conf

La structure de base du fichier est la suivante :

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

La valeur localnet src est le CIDR du système Cloud Volumes ONTAP.

10. Si le bloc CIDR du système Cloud Volumes ONTAP n'est pas dans la plage spécifiée dans le fichier, mettez à jour la valeur ou ajoutez une nouvelle entrée comme suit :

```
acl cvonet src <cidr>
```

Si vous ajoutez cette nouvelle entrée, n'oubliez pas d'ajouter également une entrée Autoriser :

```
http_access allow cvonet
```

Voici un exemple :


```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. Après avoir modifié le fichier de configuration, redémarrez le conteneur proxy comme suit :

```
docker restart squid
```

12. Retournez à l'interface de ligne de commandes de Cloud Volumes ONTAP et vérifiez que Cloud Volumes ONTAP peut envoyer des messages AutoSupport :

```
autosupport check show-details
```

Configurer EMS

Le système de gestion des événements (EMS) collecte et affiche des informations sur les événements qui se produisent sur les systèmes ONTAP. Pour recevoir des notifications d'événements, vous pouvez définir des destinations d'événements (adresses e-mail, hôtes de trap SNMP ou serveurs syslog) et des routes d'événements pour un événement particulier.

Vous pouvez configurer EMS à l'aide de l'interface de ligne de commande. Pour obtenir des instructions, reportez-vous à la section "[Documents ONTAP : présentation de la configuration EMS](#)".

Concepts

Licences 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.

Présentation des licences

Des options de licence sont disponibles pour les nouveaux clients :

Licences basées sur la capacité

Payez plusieurs systèmes Cloud Volumes ONTAP sur votre compte NetApp grâce à la capacité provisionnée. Inclut la possibilité d'acheter des services de données cloud supplémentaires.

Abonnement Keystone Flex

Service basé sur un abonnement avec paiement à l'utilisation qui offre une expérience de cloud hybride transparente pour les paires haute disponibilité.

Le modèle de licence par nœud précédent reste disponible pour les clients qui ont déjà acheté une licence ou qui disposent d'un abonnement actif sur le marché.

Les sections suivantes fournissent plus de détails sur chacune de ces options.

Licences basées sur la capacité

Les packs de licence basés sur la capacité vous permettent de payer le Cloud Volumes ONTAP par To de capacité. La licence est associée à votre compte NetApp et vous permet de facturer plusieurs systèmes par rapport à la licence, tant que la capacité disponible par le biais de la licence est suffisante.

Par exemple, vous pouvez acheter une seule licence de 20 Tio, déployer quatre systèmes Cloud Volumes ONTAP puis allouer un volume de 5 Tio à chaque système, pour un total de 20 Tio. La capacité est disponible pour les volumes de chaque système Cloud Volumes ONTAP déployé sur ce compte.

Une licence basée sur la capacité est disponible sous la forme d'un *package*. Lorsque vous déployez un système Cloud Volumes ONTAP, vous avez le choix entre plusieurs packages de licences en fonction des besoins de votre entreprise.

Packs

Les packages basés sur la capacité suivants sont disponibles pour Cloud Volumes ONTAP.

Frémium

Fournit toutes les fonctionnalités Cloud Volumes ONTAP gratuitement auprès de NetApp (frais des fournisseurs cloud toujours applicables).

- Aucune licence ni contrat n'est nécessaire.
- L'assistance de NetApp n'est pas incluse.
- Votre système Cloud Volumes ONTAP est limité à 500 Gio de capacité provisionnée.

- Vous pouvez utiliser jusqu'à 10 systèmes Cloud Volumes ONTAP avec l'offre « Freemium » par compte NetApp, quel que soit le fournisseur de cloud.
- Si la capacité provisionnée d'un système Cloud Volumes ONTAP dépasse 500 Gio, BlueXP convertit le système en package Essentials.

Dès qu'un système est converti au package Essentials, le [charge minimale](#) s'applique.

Tous les autres systèmes dont la capacité provisionnée est inférieure à 500 Gio restent sur « Freemium » (tant qu'ils ont été déployés à l'aide de l'offre Freemium).

Optimisé

Payez séparément la capacité provisionnée et les opérations d'E/S.

- Cloud Volumes ONTAP à un seul nœud ou haute disponibilité
- Le chargement repose sur deux facteurs de coûts : le stockage et l'utilisation (E/S)

Vous ne serez pas facturé pour les E/S liées à la réplication de données (SnapMirror) ou NDMP.

- Disponible uniquement sur Azure Marketplace comme offre de paiement à l'utilisation ou comme contrat annuel
- Prise en charge avec certains types de VM : E4S_v3, E4ds_v4, DS4_v2, DS13_v2, E8s_v3, Et E8ds_v4
- Ajoutez des services de données cloud de NetApp à vos frais supplémentaires

Points essentiels

Payez en fonction de la capacité de Cloud Volumes ONTAP dans différentes configurations.

- Choisissez votre configuration Cloud Volumes ONTAP :
 - Un seul nœud ou un système HA
 - Stockage basé sur des fichiers ou des blocs ou données secondaires pour la reprise après incident
- Ajoutez des services de données cloud de NetApp à vos frais supplémentaires

Professionnel

Payez par capacité pour tout type de configuration Cloud Volumes ONTAP avec des sauvegardes illimitées.

- Licence pour toute configuration Cloud Volumes ONTAP

Un seul nœud ou haute disponibilité avec chargement de la capacité pour les volumes primaires et secondaires au même rythme

- Inclut les sauvegardes d'un volume illimité avec Cloud Backup, mais uniquement pour les systèmes Cloud Volumes ONTAP déployés avec le package Professional
- Ajoutez des services de données cloud de NetApp à vos frais supplémentaires

Cache de périphérie

Fournit des licences pour Cloud volumes Edge cache.

- Les mêmes fonctionnalités que l'offre professionnelle, avec continuité de l'activité et protection des

données pour une entreprise distribuée

- Mise en cache intelligente de la périphérie via une machine virtuelle Windows à empreinte réduite sur chaque site
- 30 To au minimum avec six nœuds de périphérie inclus
- Un nœud Edge avec chaque tranche de 3 tibs de capacité supplémentaire achetée
- Disponible uniquement sur Azure Marketplace comme offre de paiement à l'utilisation ou comme contrat annuel

["Découvrez comment Cloud volumes Edge cache peut aider votre entreprise"](#)

Modèles de consommation

Des packs de licence basés sur la capacité sont disponibles avec les modèles de consommation suivants :

- **BYOL** : licence achetée auprès de NetApp et utilisable pour déployer Cloud Volumes ONTAP dans n'importe quel fournisseur de cloud.

+ Notez que les modules optimisé et Edge cache ne sont pas disponibles avec BYOL.

- **PAYGO** : un abonnement à l'heure sur le marché de votre fournisseur de services cloud.
- **Annuel** : contrat annuel sur le marché de votre fournisseur cloud.

Notez ce qui suit :

- Si vous achetez une licence auprès de NetApp (BYOL), vous devez également vous abonner à l'offre PAYGO depuis le marché de votre fournisseur cloud.

Votre licence est toujours facturée en premier, mais vous devrez payer à l'heure sur le marché dans les cas suivants :

- Si vous dépassez votre capacité autorisée
- Si la durée de votre licence expire
- Si vous avez un contrat annuel provenant d'un marché, les systèmes *All* Cloud Volumes ONTAP que vous déployez sont facturés pour ce contrat. Vous ne pouvez pas combiner un contrat annuel de marché avec BYOL.

Modification des packages

Après le déploiement, vous pouvez modifier le package d'un système Cloud Volumes ONTAP utilisant des licences basées sur la capacité. Par exemple, si vous avez déployé un système Cloud Volumes ONTAP avec le pack Essentials, vous pouvez le remplacer par le pack Professional si vos besoins évoluent.

["Apprenez à changer les méthodes de charge"](#).

Tarifs

Pour plus d'informations sur les prix, rendez-vous sur ["Site Web NetApp BlueXP"](#).

Essais gratuits

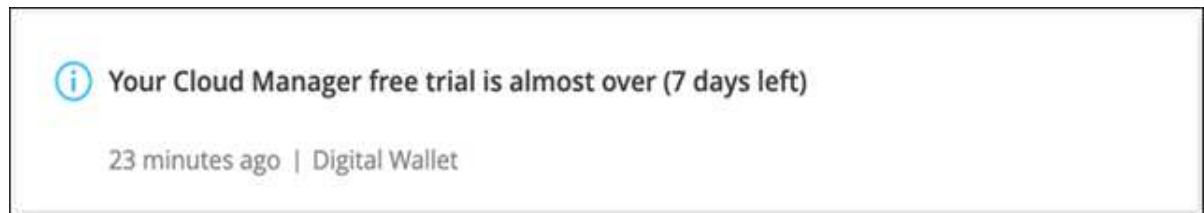
Vous pouvez bénéficier d'un essai gratuit de 30 jours sur l'abonnement au paiement à l'utilisation disponible sur le marché de votre fournisseur cloud. Profitez de notre offre d'essai gratuit : Cloud Volumes ONTAP et

Cloud Backup. La version d'évaluation commence lorsque vous vous inscrivez à l'offre sur le marché.

Il n'y a aucune limite d'instance ou de capacité. Vous pouvez déployer autant de systèmes Cloud Volumes ONTAP que vous le souhaitez et allouer gratuitement la capacité nécessaire pendant 30 jours. L'essai gratuit est automatiquement converti en abonnement payant à l'heure après 30 jours.

Il n'y a pas de frais de licence logicielle pour Cloud Volumes ONTAP à l'heure, mais des frais d'infrastructure sont toujours applicables par votre fournisseur cloud.

Vous recevrez une notification dans BlueXP dès le début de l'essai gratuit, lorsqu'il reste 7 jours, et quand il reste 1 jour. Par exemple :



Configurations compatibles

Les packages de licence basés sur la capacité sont disponibles avec Cloud Volumes ONTAP 9.7 et les versions ultérieures.

Limite de capacité

Avec ce modèle de licence, chaque système Cloud Volumes ONTAP peut supporter jusqu'à 2 Plo de capacité via les disques et la hiérarchisation au stockage objet.

Il n'y a pas de limitation de la capacité maximale lorsqu'il s'agit de la licence elle-même.

Nombre max. De systèmes

Avec une licence basée sur la capacité, le nombre maximal de systèmes Cloud Volumes ONTAP est limité à 20 par compte NetApp. Un *système* est une paire HA Cloud Volumes ONTAP, un système Cloud Volumes ONTAP à un seul nœud ou toute machine virtuelle de stockage supplémentaire que vous créez. La VM de stockage par défaut ne tient pas compte de la limite. Cette limite s'applique à tous les modèles de licence.

Imaginons par exemple que vous ayez trois environnements de travail :

- Un système Cloud Volumes ONTAP à un seul nœud avec une machine virtuelle de stockage (il s'agit de la machine virtuelle de stockage par défaut créée lors du déploiement de Cloud Volumes ONTAP)

Cet environnement de travail ne compte qu'un seul système.

- Un système Cloud Volumes ONTAP à un seul nœud doté de deux machines virtuelles de stockage (VM de stockage par défaut et une VM de stockage supplémentaire que vous avez créée)

Cet environnement de travail compte deux systèmes : un pour le système à un nœud et un pour le serveur virtuel de stockage supplémentaire.

- Une paire haute disponibilité Cloud Volumes ONTAP avec trois machines virtuelles de stockage (la machine virtuelle de stockage par défaut, plus deux machines virtuelles de stockage supplémentaires que vous avez créées)

Cet environnement de travail compte trois systèmes : un pour la paire haute disponibilité et deux pour les machines virtuelles de stockage supplémentaires.

Ce total compte six systèmes. Vous aurez alors de la place pour 14 systèmes supplémentaires dans votre compte.

Si vous disposez d'un déploiement de grande envergure nécessitant plus de 20 systèmes, contactez votre ingénieur commercial ou votre responsable de compte.

["En savoir plus sur les comptes NetApp".](#)

Remarques sur le chargement

Les informations suivantes peuvent vous aider à comprendre le fonctionnement de la charge avec les licences basées sur la capacité.

Charge minimale

Chaque machine virtuelle de stockage servant de données dispose d'au moins un volume primaire (lecture-écriture), ce supplément de 4 Tio au moins. Si la somme des volumes primaires est inférieure à 4 Tio, BlueXP applique la charge minimale de 4 Tio à cette machine virtuelle de stockage.

Si vous n'avez pas encore provisionné de volumes, le coût minimum n'est pas appliqué.

Les frais de capacité minimale de 4 Tio ne s'appliquent pas aux machines virtuelles de stockage contenant uniquement des volumes secondaires (protection des données). Par exemple, si vous disposez d'une machine virtuelle de stockage avec 1 To de données secondaires, vous êtes facturé uniquement pour cette To de données.

Surâge

Si vous dépassez votre capacité BYOL ou si votre licence expire, vous serez facturé pour les suppléments de capacité au tarif horaire selon votre abonnement sur le marché.

Pack Essentials

Le pack Essentials est facturé par type de déploiement (haute disponibilité ou nœud unique) et par type de volume (primaire ou secondaire). Par exemple, *Essentials HA* a des prix différents de ceux de *Essentials Secondary HA*.

Si vous avez acheté une licence Essentials auprès de NetApp (BYOL) et que vous dépassez la capacité de licence requise pour ce déploiement et ce type de volume, le porte-monnaie numérique facture les frais supplémentaires par rapport à une licence Essentials à un tarif plus élevé (le cas échéant). Cela arrive parce que nous utilisons la capacité disponible que vous avez déjà achetée en tant que capacité prépayée avant de payer par rapport au Marketplace. La facturation sur le marché ajouterait des coûts à votre facture mensuelle.

Voici un exemple. Imaginons que vous ayez les licences suivantes pour le pack Essentials :

- Une licence HA_ secondaire _Essentials de 500 Tio qui a une capacité engagée de 500 Tio
- Une licence *Essentials Single Node* de 500 Tio qui n'a que 100 Tio de capacité engagée

Une autre de 50 To est provisionnée sur une paire haute disponibilité avec des volumes secondaires. Au lieu de facturer ce 50 Tio à PAYGO, le porte-monnaie numérique facture le surplus de 50 Tio par rapport à la licence *Essentials Single Node*. Le prix de cette licence est supérieur à celui de *Essentials Secondary HA*,

mais il est moins cher que le taux de facturation.

Dans le porte-monnaie numérique, 50 Tio seront affichées comme facturés par rapport à la licence *Essentials Single Node*.

Machines virtuelles de stockage

- Aucun coût de licence supplémentaire n'est requis pour les machines virtuelles de stockage destinées aux données, mais une charge de capacité minimale de 4 Tio est élevée par SVM servant de données.
- Les SVM de reprise après incident sont facturés en fonction de la capacité provisionnée.

Paires HA

Pour les paires haute disponibilité, la capacité provisionnée n'est nécessaire qu'à un nœud. Vous n'êtes pas facturé pour les données qui sont mises en miroir de manière synchrone sur le nœud partenaire.

Volumes FlexClone et FlexCache

- La capacité utilisée par les volumes FlexClone ne vous sera pas facturée.
- Les volumes FlexCache source et de destination sont considérés comme des données primaires et facturés en fonction de l'espace provisionné.

Comment démarrer

Découvrez comment utiliser les licences basées sur la capacité :

- ["Configuration des licences pour Cloud Volumes ONTAP dans AWS"](#)
- ["Configuration des licences pour Cloud Volumes ONTAP dans Azure"](#)
- ["Configurez la licence pour Cloud Volumes ONTAP dans Google Cloud"](#)

Abonnement Keystone Flex

Service basé sur un abonnement avec paiement à l'utilisation qui offre une expérience de cloud hybride transparente, pour les modèles de consommation OpEx, qui préfèrent les CapEx ou les crédits sur investissement en amont.

Le chargement est basé sur la taille de la capacité engagée pour une ou plusieurs paires haute disponibilité Cloud Volumes ONTAP dans votre abonnement Keystone Flex.

La capacité provisionnée pour chaque volume est agrégée et comparée à la capacité dédiée à votre abonnement Keystone Flex. Les suppléments de capacité excédentaire sont facturés en rafale sur votre abonnement Keystone Flex.

["En savoir plus sur les abonnements Keystone Flex"](#).

Configurations compatibles

Les abonnements Keystone Flex sont pris en charge avec des paires haute disponibilité. Cette option de licence n'est pas prise en charge pour le moment avec des systèmes à un seul nœud.

Limite de capacité

Chaque système Cloud Volumes ONTAP peut atteindre jusqu'à 2 Pio de capacité maximale grâce à des

disques et à une hiérarchisation sur le stockage objet.

Comment démarrer

Découvrez comment se lancer avec un abonnement Keystone Flex :

- ["Configuration des licences pour Cloud Volumes ONTAP dans AWS"](#)
- ["Configuration des licences pour Cloud Volumes ONTAP dans Azure"](#)
- ["Configurez la licence pour Cloud Volumes ONTAP dans Google Cloud"](#)

Licence basée sur les nœuds

La licence basée sur les nœuds est le modèle de licence de la génération précédente qui vous permet d'obtenir une licence Cloud Volumes ONTAP par nœud. Ce modèle de licence n'est pas disponible pour les nouveaux clients et aucune évaluation gratuite n'est disponible. Le chargement par nœud a été remplacé par les méthodes de charge par capacité décrites ci-dessus.

Une licence basée sur les nœuds est toujours disponible pour les clients existants :

- Si vous disposez d'une licence active, BYOL est uniquement disponible avec les renouvellements de licence.
- Si vous disposez d'un abonnement Marketplace actif, le service de facturation est toujours disponible via cet abonnement.

Conversions de licence

La conversion d'un système Cloud Volumes ONTAP existant en une autre méthode de licence n'est pas prise en charge. Les trois méthodes de licence actuelles sont les licences basées sur la capacité, les abonnements Keystone Flex et les licences basées sur les nœuds. Par exemple, vous ne pouvez pas convertir un système d'un système en licence basée sur des nœuds vers un système de licence basé sur la capacité (et inversement).

Si vous souhaitez passer à un autre mode de licence, vous pouvez acheter une licence, déployer un nouveau système Cloud Volumes ONTAP avec cette licence, puis répliquer les données sur ce nouveau système.

Notez que la conversion d'un système depuis le modèle de facturation PAYGO par nœud vers un modèle de licence BYOL (et inversement) n'est pas prise en charge. Vous devez déployer un nouveau système, puis répliquer les données sur ce système. ["Apprenez à changer de modèle PAYGO et BYOL"](#).

Stockage

Protocoles clients

Cloud Volumes ONTAP prend en charge les protocoles client iSCSI, NFS, SMB, NVMe-TCP et S3.

ISCSI

ISCSI est un protocole de bloc capable de s'exécuter sur les réseaux Ethernet standard. La plupart des systèmes d'exploitation clients proposent un initiateur logiciel qui fonctionne sur un port Ethernet standard.

NFS

NFS est le protocole d'accès classique aux fichiers pour les systèmes UNIX et LINUX. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles NFS v3, NFS V4 et NFS v4.1. Vous pouvez contrôler l'accès aux fichiers à l'aide d'autorisations de style UNIX, d'autorisations de style NTFS ou d'une combinaison des deux.

Les clients peuvent accéder aux mêmes fichiers à l'aide des protocoles NFS et SMB.

PME

SMB est le protocole d'accès aux fichiers traditionnel pour les systèmes Windows. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles SMB 2.0, SMB 2.1, SMB 3.0 et SMB 3.1.1. Tout comme avec NFS, plusieurs styles d'autorisation sont pris en charge.

S3

Cloud Volumes ONTAP prend en charge S3 en option pour le stockage scale-out. La prise en charge du protocole S3 permet de configurer l'accès des clients S3 aux objets contenus dans un compartiment d'une machine virtuelle de stockage (SVM).

["Découvrez comment configurer et gérer les services de stockage objet S3 dans ONTAP".](#)

NVMe-TCP

Le protocole NVMe-TCP est pris en charge par les fournisseurs cloud si vous utilisez Cloud Volumes ONTAP version 9.12.1 ou ultérieure. BlueXP ne propose pas de fonctionnalités de gestion pour NVMe-TCP.

Pour plus d'informations sur la configuration de NVMe via ONTAP, reportez-vous à la section ["Configuration d'une VM de stockage pour NVMe"](#).

Disques et agrégats

Comprendre comment Cloud Volumes ONTAP utilise le stockage cloud pour vous aider à comprendre vos coûts de stockage.



Tous les disques et agrégats doivent être créés et supprimés directement depuis BlueXP. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Présentation

Cloud Volumes ONTAP utilise le stockage du fournisseur cloud comme disques et les regroupe dans un ou plusieurs agrégats. Les agrégats fournissent du stockage à un ou plusieurs volumes.



Plusieurs types de disques clouds sont pris en charge. Lorsque vous déployez Cloud Volumes ONTAP, vous choisissez le type de disque lorsque vous créez un volume et la taille de disque par défaut.



Le volume total de stockage acheté auprès d'un fournisseur cloud est la *capacité brute*. La *capacité utilisable* est inférieure car environ 12 à 14 % représente la surcharge réservée à l'utilisation de Cloud Volumes ONTAP. Par exemple, si BlueXP crée un agrégat de 500 Gio, la capacité utilisable est de 442.94 Gio.

Le stockage AWS

Dans AWS, Cloud Volumes ONTAP utilise le stockage EBS pour les données utilisateur et le stockage NVMe local en tant que Flash cache sur certains types d'instances EC2.

Stockage EBS

Dans AWS, un agrégat peut contenir jusqu'à 6 disques de même taille. Cependant, si vous disposez d'une configuration prenant en charge la fonctionnalité Amazon EBS Elastic volumes, un agrégat peut contenir jusqu'à 8 disques. ["En savoir plus sur la prise en charge d'Elastic volumes"](#).

La taille maximale de disque est de 16 Tio.

Le type de disque EBS sous-jacent peut être soit des disques SSD polyvalents (gp3 ou gp2), soit des SSD IOPS provisionnés (io1), soit des disques durs optimisés en termes de débit (st1). Vous pouvez associer un disque EBS à Amazon S3 pour ["déplacez les données inactives vers un stockage objet à faible coût"](#).



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).

Stockage NVMe local

Certains types d'instances EC2 incluent le stockage NVMe local, qui est utilisé par Cloud Volumes ONTAP ["Flash cache"](#).

- Liens connexes*
- ["Documentation AWS : types de volume EBS"](#)
- ["Découvrez comment choisir les types et les tailles de disques pour vos systèmes dans AWS"](#)
- ["Consultez les limites de stockage pour Cloud Volumes ONTAP dans AWS"](#)
- ["Étude des configurations pour Cloud Volumes ONTAP prises en charge dans AWS"](#)

Le stockage Azure

Dans Azure, un agrégat peut contenir jusqu'à 12 disques de même taille. Le type de disque et la taille de disque maximale dépendent de l'utilisation d'un système à un seul nœud ou d'une paire haute disponibilité :

Systèmes à un seul nœud

Les systèmes à un seul nœud peuvent utiliser trois types de disques gérés Azure :

- *Des disques gérés SSD de premier choix* fournir des performances élevées aux charges de travail exigeantes en E/S à un coût plus élevé.
- *Des disques gérés SSD standard* assurent des performances prévisibles pour les charges de travail nécessitant un faible niveau d'IOPS.
- *Les disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevées et souhaitez réduire vos coûts.

Chaque type de disque géré a une taille de disque maximale de 32 Tio.

Vous pouvez coupler un disque géré avec le stockage Azure Blob à ["déplacez les données inactives vers un stockage objet à faible coût"](#).

Paires HA

Les paires HAUTE DISPONIBILITÉ utilisent deux types de disques qui offrent des performances élevées pour les charges de travail exigeantes en E/S à un coût plus élevé :

- *Premium page Blobs* avec une taille de disque maximale de 8 Tio
- *Disques gérés* avec une taille de disque maximale de 32 Tio
- Liens connexes*
- ["Documentation Microsoft Azure : types de disques gérés Azure"](#)
- ["Documentation Microsoft Azure : présentation des objets blob de pages Azure"](#)
- ["Découvrez comment choisir les types et les tailles de disques pour vos systèmes dans Azure"](#)
- ["Consultez les limites de stockage pour Cloud Volumes ONTAP dans Azure"](#)

Stockage Google Cloud

Dans Google Cloud, un agrégat peut contenir jusqu'à 6 disques de même taille. La taille maximale de disque est de 64 Tio.

Le type de disque peut être soit *Zonal SSD persistent disks*, *Zonal équilibré persistent disks*, soit *Zonal*

standard persistent disks. Vous pouvez coupler des disques persistants avec un compartiment Google Storage vers ["déplacez les données inactives vers un stockage objet à faible coût"](#).

- Liens connexes*
- ["Documentation Google Cloud : options de stockage"](#)
- ["Consultez les limites de stockage de Cloud Volumes ONTAP dans Google Cloud"](#)

Type de RAID

Pour chaque agrégat Cloud Volumes ONTAP, le type RAID est RAID0 (répartition). Cloud Volumes ONTAP fait appel au fournisseur cloud pour assurer la disponibilité et la durabilité des disques. Aucun autre type de RAID n'est pris en charge.

Disques de secours

RAID0 ne prend pas en charge l'utilisation de disques de rechange à chaud pour assurer la redondance.

La création de disques inutilisés (disques de secours) associés à une instance Cloud Volumes ONTAP engendre des dépenses superflues et peut empêcher de provisionner de l'espace supplémentaire si nécessaire. Par conséquent, ce n'est pas recommandé.

Volumes flexibles dans AWS

La prise en charge de la fonctionnalité Amazon EBS Elastic volumes intégrée dans un agrégat Cloud Volumes ONTAP améliore les performances et la capacité, et permet à BlueXP d'augmenter automatiquement la capacité du disque sous-jacent selon les besoins.

Avantages

- Croissance dynamique des disques

BlueXP peut augmenter dynamiquement la taille des disques tandis que Cloud Volumes ONTAP est en cours d'exécution et que les disques sont toujours connectés.

- Performances améliorées

Les agrégats activés avec Elastic volumes peuvent disposer de huit disques utilisés de la même manière sur deux groupes RAID. Cette configuration offre un débit plus élevé et des performances cohérentes.

- Agrégats de taille supérieure

La prise en charge de huit disques fournit une capacité totale maximale de 128 Tio. Ces limites sont supérieures à la limite de six disques et de 96 Tio pour les agrégats qui ne sont pas activés avec la fonctionnalité Elastic volumes.

Notez que les limites de capacité totale du système restent les mêmes.

["En savoir plus sur Elastic volumes d'AWS"](#)

Configurations compatibles

La fonctionnalité Amazon EBS Elastic volumes est prise en charge avec des versions Cloud Volumes ONTAP spécifiques et des types de disques EBS spécifiques.

Version Cloud Volumes ONTAP

La fonction Elastic volumes est prise en charge avec les systèmes *New* Cloud Volumes ONTAP créés à partir de la version 9.11.0 ou ultérieure. Cette fonction est *non* prise en charge avec les systèmes Cloud Volumes ONTAP existants déployés avant 9.11.0.

Par exemple, la fonctionnalité Elastic volumes n'est pas prise en charge si vous avez créé un système Cloud Volumes ONTAP 9.9.0 puis mis à niveau ce système vers la version 9.11.0. Il doit s'agir d'un nouveau système déployé à l'aide de la version 9.11.0 ou ultérieure.

Types de disques EBS

La fonctionnalité Elastic volumes est automatiquement activée au niveau de l'agrégat lors de l'utilisation de disques SSD à usage général (gp3) ou de disques SSD d'IOPS provisionnés (io1). La fonctionnalité Elastic volumes n'est pas prise en charge avec les agrégats utilisant n'importe quel autre type de disque.

Autorisations AWS requises

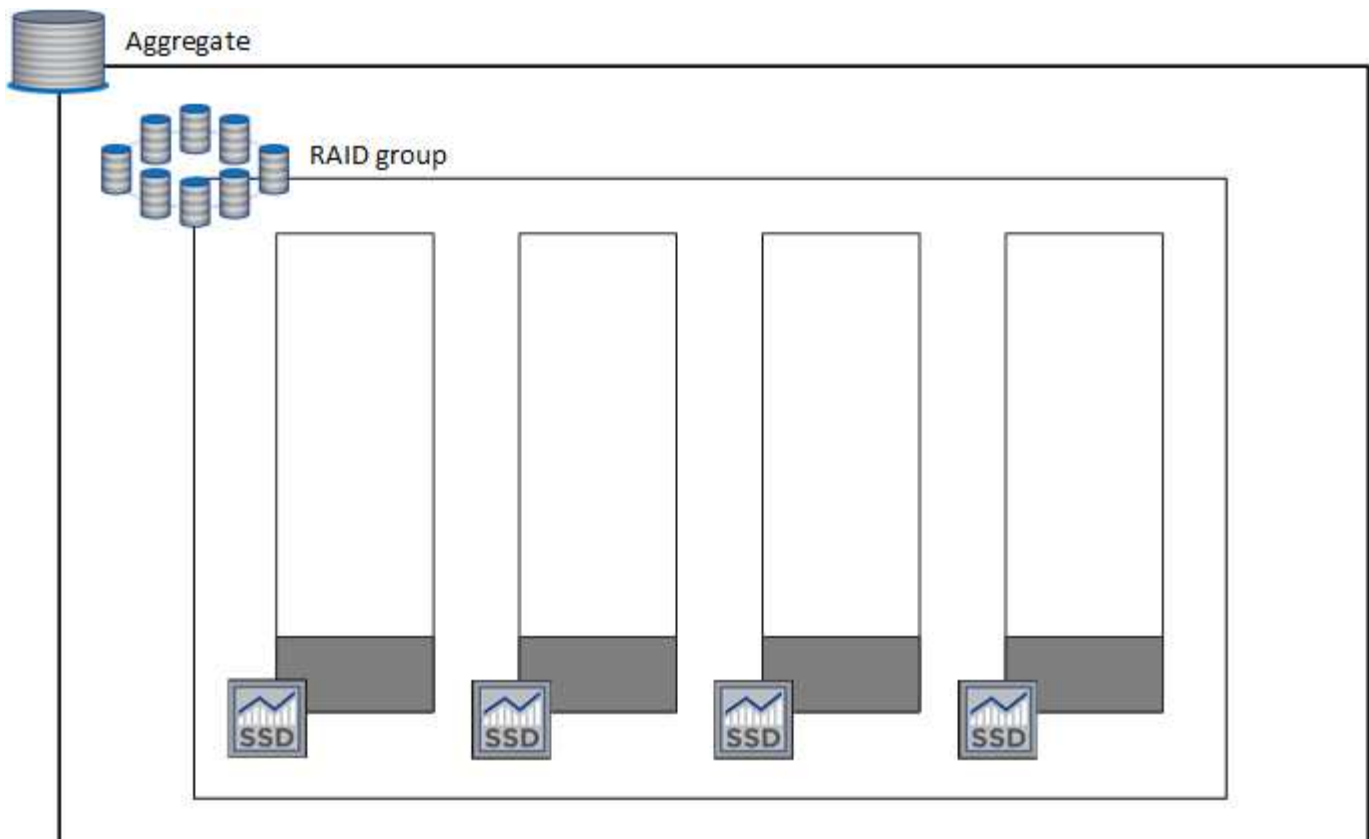
Depuis la version 3.9.19, le connecteur nécessite les autorisations suivantes pour activer et gérer la fonctionnalité Elastic volumes sur un agrégat Cloud Volumes ONTAP :

- ec2:Describvolumesmodificateurs
- ec2 : Modifier le volume

Ces autorisations sont incluses dans ["Règles fournies par NetApp"](#)

Fonctionnement de la prise en charge d'Elastic volumes

Un agrégat sur lequel la fonctionnalité Elastic volumes est activée se compose d'un ou deux groupes RAID. Chaque groupe RAID dispose de quatre disques identiques de même capacité. Voici un exemple d'agrégat de 10 Tio qui contient quatre disques sur 2.5 Tio chacun :



Lorsque BlueXP crée un agrégat, il commence par un groupe RAID. Si de la capacité supplémentaire est nécessaire, BlueXP augmente l'agrégat en augmentant de la même quantité la capacité de tous les disques du groupe RAID. L'augmentation de la capacité est soit un minimum de 256 Gio, soit 10 % de la taille de l'agrégat.

Par exemple, si vous avez un agrégat de 1 To, chaque disque est de 250 Gio. 10 % de la capacité de l'agrégat est de 100 Gio. Soit inférieure à 256 Gio, donc la taille de l'agrégat est augmentée de 256 Gio au minimum (ou 64 Gio pour chaque disque).

BlueXP augmente la taille des disques tandis que le système Cloud Volumes ONTAP est en cours d'exécution et que les disques sont toujours connectés. Le changement ne perturbe pas les opérations.

Si un agrégat atteint 64 Tio (ou 16 Tio sur chaque disque), BlueXP crée un second groupe RAID pour la capacité supplémentaire. Ce deuxième groupe RAID fonctionne comme le premier : il possède quatre disques ayant la même capacité et peut atteindre 64 Tio. Cela signifie qu'un agrégat peut avoir une capacité maximale de 128 Tio.

Voici un exemple d'agrégat avec deux groupes RAID. La limite de capacité a été atteinte sur le premier groupe RAID, tandis que les disques du second groupe RAID disposent d'une quantité importante d'espace disponible.



Que se passe-t-il lorsque vous créez un volume

Si vous créez un volume qui utilise des disques gp3 ou io1, BlueXP crée le volume sur un agrégat de la manière suivante :

- Si un agrégat gp3 ou io1 est déjà activé avec Elastic volumes, BlueXP crée le volume sur cet agrégat.

- Si plusieurs agrégats gp3 ou io1 sont activés, BlueXP crée le volume sur l'agrégat qui requiert la plus faible quantité de ressources.
- Si le système ne dispose que d'agrégats gp3 ou io1 pas activés pour les volumes Elastic, le volume est créé sur cet agrégat.

Bien que ce scénario soit peu probable, il est possible dans deux cas :



- La fonctionnalité Elastic volumes est explicitement désactivée lors de la création d'un agrégat à partir de l'API.
- Vous avez créé un nouveau système Cloud Volumes ONTAP depuis l'interface utilisateur. Dans ce cas, la fonctionnalité Elastic volumes est désactivée sur l'agrégat initial. Révision [Limites](#) ci-dessous pour en savoir plus.

- Si aucun agrégat n'a la capacité suffisante, BlueXP crée l'agrégat avec les volumes Elastic activés, puis crée le volume sur cet nouvel agrégat.

La taille de l'agrégat dépend de la taille du volume demandée et d'une capacité supplémentaire de 10 %.

Mode de gestion de la capacité

Le mode de gestion de la capacité pour un connecteur fonctionne avec les volumes Elastic comme il fonctionne avec d'autres types d'agrégats :

- Lorsque le mode automatique est activé (il s'agit du paramètre par défaut), BlueXP augmente automatiquement la taille des agrégats si vous avez besoin de capacité supplémentaire.
- Si vous changez le mode de gestion de la capacité en mode Manuel, BlueXP vous demande d'obtenir votre autorisation pour acquérir de la capacité supplémentaire.

["En savoir plus sur le mode gestion de la capacité".](#)

Limites

L'augmentation de la taille d'un agrégat peut prendre jusqu'à 6 heures. Pendant ce temps, BlueXP ne peut pas demander de capacité supplémentaire pour cet agrégat.

Fonctionnement avec Elastic volumes

Vous pouvez utiliser Elastic volumes dans BlueXP comme suit :

- Créez un nouveau système sur lequel les volumes élastiques sont activés sur l'agrégat initial lors de l'utilisation de disques gp3 ou io1

["Découvrez comment créer un système Cloud Volumes ONTAP"](#)

- Créez un nouveau volume sur un agrégat sur lequel Elastic volumes est activé

Si vous créez un volume qui utilise des disques gp3 ou io1, BlueXP crée automatiquement le volume sur un agrégat sur lequel Elastic volumes est activé. Pour plus de détails, reportez-vous à [Que se passe-t-il lorsque vous créez un volume.](#)

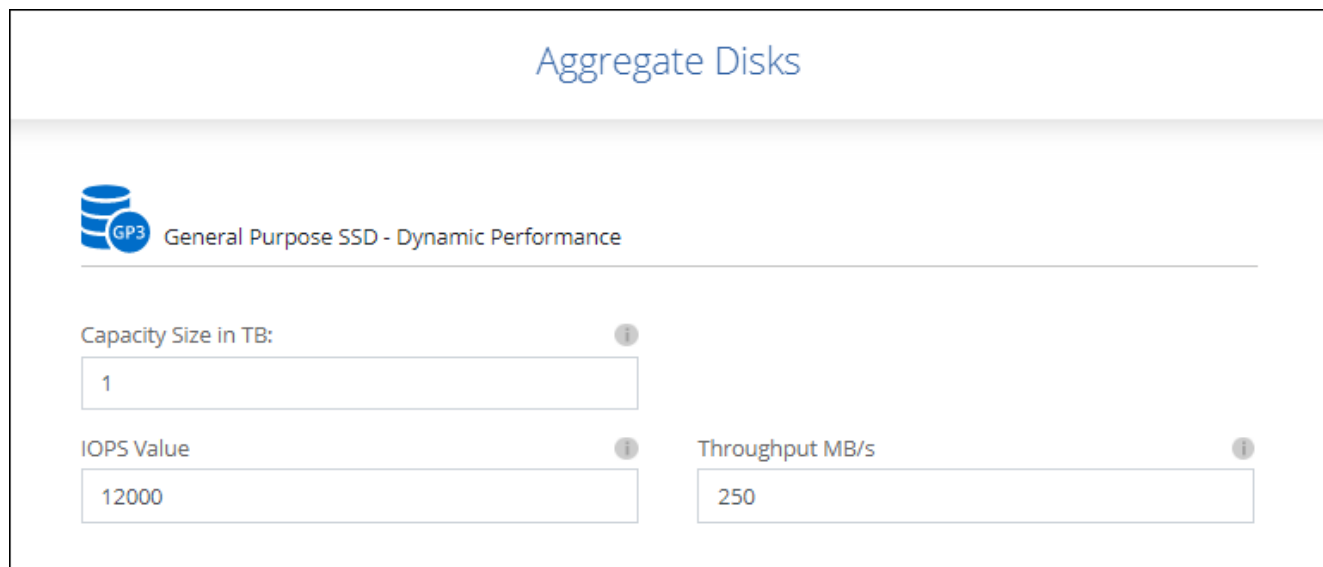
["Découvrez comment créer des volumes".](#)

- Créez un nouvel agrégat pour lequel Elastic volumes est activé

Les volumes élastiques sont automatiquement activés sur les nouveaux agrégats qui utilisent des disques gp3 ou io1, tant que le système Cloud Volumes ONTAP a été créé à partir de la version 9.11.0 ou ultérieure.

Lorsque vous créez l'agrégat, BlueXP vous invite à indiquer la taille de la capacité de l'agrégat. Cette configuration est différente des autres configurations dans lesquelles vous choisissez une taille de disque et un nombre de disques.

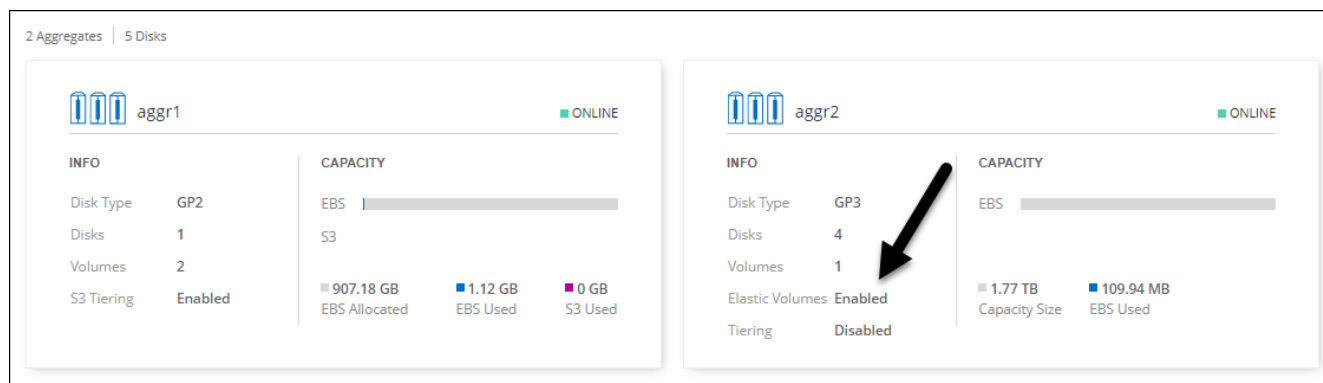
La capture d'écran suivante montre un exemple d'un nouvel agrégat composé de disques gp3.



["Découvrez comment créer des agrégats".](#)

- Identifiez les agrégats pour lesquels Elastic volumes est activé

Lorsque vous accédez à la page allocation avancée, vous pouvez déterminer si la fonctionnalité Elastic volumes est activée ou non sur un agrégat. Dans l'exemple suivant, aggr2 possède les volumes Elastic activés, contrairement à aggr1.



- Accroître la capacité d'un agrégat

BlueXP ajoute automatiquement de la capacité aux agrégats selon les besoins, mais vous pouvez également augmenter vous-même la capacité.

["Découvrez comment augmenter la capacité des agrégats".](#)

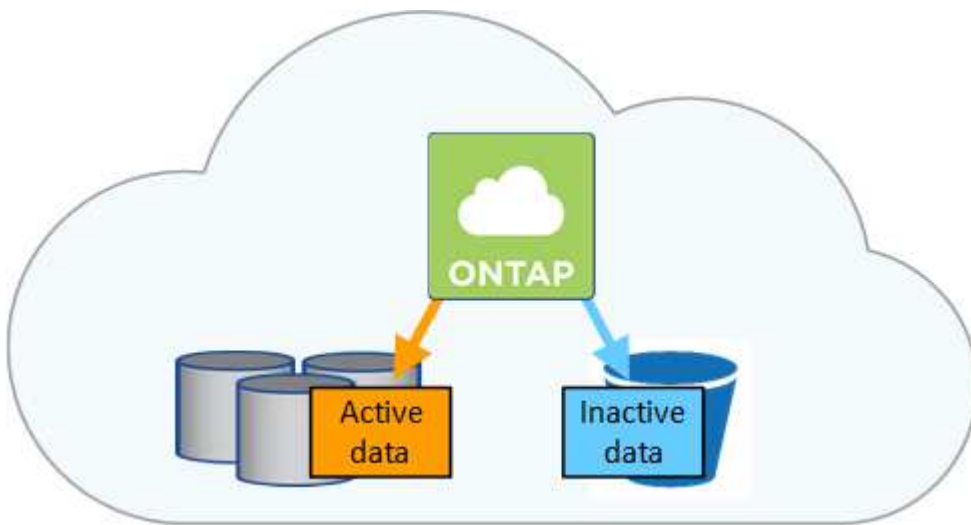
- Répliquez les données dans un agrégat sur lequel Elastic volumes est activé

Si le système Cloud Volumes ONTAP de destination prend en charge les volumes Elastic, un volume de destination sera placé sur un agrégat sur lequel les volumes élastiques sont activés (tant que vous choisissez un disque gp3 ou io1).

["Découvrez comment configurer la réplication des données"](#)

Vue d'ensemble du hiérarchisation des données

Réduisez vos coûts de stockage en permettant le Tiering automatisé des données inactives vers un stockage objet à faible coût. Les données actives conservent les disques SSD ou HDD haute performance, tandis que les données inactives sont envoyées vers un stockage objet à faible coût. Vous pouvez ainsi récupérer de l'espace sur votre stockage principal et réduire le stockage secondaire.



La hiérarchisation des données est optimisée par la technologie FabricPool.



Inutile d'installer une licence pour activer le Tiering des données (FabricPool).

Tiering des données dans AWS

Lorsque vous activez le Tiering des données dans AWS, Cloud Volumes ONTAP utilise EBS comme Tier de performance pour les données actives et AWS S3 comme Tier de capacité pour les données inactives.

Tier de performance

Le Tier de performance peut être des SSD polyvalents (gp3 ou gp2) ou des SSD IOPS provisionnés (io1).

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).

Des disques SSD/HDD FAS

Un système Cloud Volumes ONTAP déplace les données inactives vers un seul compartiment S3.

BlueXP crée un compartiment S3 unique pour chaque environnement de travail et le nomme « fabric-pool-
_cluster unique ». Un compartiment S3 différent n'est pas créé pour chaque volume.

Lorsque BlueXP crée le compartiment S3, il utilise les paramètres par défaut suivants :

- Classe de stockage : standard
- Chiffrement par défaut : désactivé
- Bloquer l'accès public : bloquer tous les accès publics
- Propriété d'objet : ACL activées
- Gestion des versions de compartiment : désactivée
- Verrouillage d'objet : désactivé

Classes de stockage

La classe de stockage par défaut pour les données hiérarchisées dans AWS est *Standard*. La norme est idéale pour les données fréquemment consultées stockées dans plusieurs zones de disponibilité.

Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en remplaçant la classe de stockage par l'une des catégories suivantes : *Intelligent Tiering*, *One-zone Infrequent Access*, *Standard-Infrequent Access* ou *S3 Glacier Instant Retrieval*. Lorsque vous modifiez la classe de stockage, les données inactives commencent dans la classe de stockage Standard et sont transférées vers la classe de stockage que vous avez sélectionnée, si les données ne sont pas accessibles après 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données. Prenez donc ces considérations avant de changer la classe de stockage. ["En savoir plus sur les classes de stockage Amazon S3"](#).

Vous pouvez sélectionner une classe de stockage lors de la création de l'environnement de travail et la modifier à tout moment après. Pour plus de détails sur la modification de la classe de stockage, voir ["Tiering des données inactives vers un stockage objet à faible coût"](#).

La classe de stockage du Tiering des données est étendue au système - elle n'est pas par volume.

Tiering des données dans Azure

Lorsque vous activez le Tiering des données dans Azure, Cloud Volumes ONTAP utilise des disques gérés Azure comme un Tier de performance pour les données actives et le stockage Azure Blob comme un Tier de capacité pour les données inactives.

Tier de performance

Le Tier de performance peut être soit des disques SSD, soit des disques durs.

Des disques SSD/HDD FAS

Un système Cloud Volumes ONTAP transfère les données inactives vers un seul conteneur Blob.

BlueXP crée un nouveau compte de stockage avec un conteneur pour chaque environnement de travail Cloud Volumes ONTAP. Le nom du compte de stockage est aléatoire. Un container différent n'est pas créé pour chaque volume.

BlueXP crée le compte de stockage avec les paramètres suivants :

- Tier d'accès : chaud
- Performance : standard
- Redondance : stockage redondant localement (LRS)

- Compte : StorageV2 (usage général v2)
- Transfert sécurisé requis pour les opérations d'API REST activées
- Accès à la clé du compte de stockage : activé
- Version TLS minimale : version 1.2
- Chiffrement de l'infrastructure : désactivé

Les niveaux d'accès au stockage

Le niveau d'accès au stockage par défaut pour les données hiérarchisées dans Azure est le *hot* Tier. Le Tier actif est idéal pour les données fréquemment utilisées.

Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en utilisant le niveau de stockage *cool*. Lorsque vous modifiez le niveau de stockage, les données inactives commencent dans le Tier de stockage à chaud et se transfère sur le Tier de stockage à froid, si les données ne sont pas accessibles au bout de 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données, prenez donc ces considérations avant de changer le Tier de stockage. ["En savoir plus sur les tiers d'accès au stockage Azure Blob"](#).

Vous pouvez sélectionner un niveau de stockage lors de la création de l'environnement de travail et le modifier à tout moment après. Pour plus d'informations sur la modification du niveau de stockage, reportez-vous à la section ["Tiering des données inactives vers un stockage objet à faible coût"](#).

Le niveau d'accès au stockage pour le Tiering des données concerne l'ensemble du système - il ne s'agit pas de par volume.

Tiering des données dans Google Cloud

Lorsque vous activez le Tiering des données dans Google Cloud, Cloud Volumes ONTAP utilise des disques persistants comme Tier de performance pour les données actives et un compartiment Google Cloud Storage comme Tier de capacité pour les données inactives.

Tier de performance

Le Tier de performance peut être soit des disques persistants SSD, soit des disques persistants équilibrés, soit des disques persistants standard.

Des disques SSD/HDD FAS

Un système Cloud Volumes ONTAP transfère les données inactives vers un seul compartiment de stockage Google Cloud.

BlueXP crée un compartiment pour chaque environnement de travail et le nomme *Fabric-pool-cluster unique identificateur*. Un compartiment différent n'est pas créé pour chaque volume.

Lorsque BlueXP crée le compartiment, il utilise les paramètres par défaut suivants :

- Type d'emplacement : région
- Classe de stockage : standard
- Accès public : sous réserve de listes de contrôle d'accès d'objet
- Contrôle d'accès : grain fin
- Protection : aucune
- Chiffrement des données : clé gérée par Google

Classes de stockage

La classe de stockage par défaut pour les données hiérarchisées est la classe *Standard Storage*. Si les données sont rarement utilisées, vous pouvez réduire vos coûts de stockage en utilisant *Nearline Storage* ou *Coldline Storage*. Lorsque vous modifiez la classe de stockage, les données inactives commencent dans la classe de stockage standard et sont transférées vers la classe de stockage que vous avez sélectionnée, si les données ne sont pas accessibles après 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données. Prenez donc ces considérations avant de changer la classe de stockage. ["En savoir plus sur les classes de stockage pour Google Cloud Storage"](#).

Vous pouvez sélectionner un niveau de stockage lors de la création de l'environnement de travail et le modifier à tout moment après. Pour plus de détails sur la modification de la classe de stockage, voir ["Tiering des données inactives vers un stockage objet à faible coût"](#).

La classe de stockage du Tiering des données est étendue au système - elle n'est pas par volume.

Tiering des données et limites de capacité

Si vous activez le Tiering des données, la limite de capacité d'un système reste la même. La limite est répartie entre le niveau de performance et le niveau de capacité.

Stratégies de hiérarchisation des volumes

Pour activer la hiérarchisation des données, vous devez sélectionner une stratégie de hiérarchisation des volumes lorsque vous créez, modifiez ou répliquez un volume. Vous pouvez sélectionner une stratégie différente pour chaque volume.

Certaines stratégies de hiérarchisation ont une période de refroidissement minimale associée, qui définit le temps pendant lequel les données utilisateur d'un volume doivent rester inactives pour que les données soient considérées comme "froides" et déplacées vers le niveau de capacité. La période de refroidissement commence lorsque les données sont écrites sur l'agrégat.



Vous pouvez modifier la période de refroidissement minimale et le seuil global par défaut de 50 % (plus d'informations sur ce point ci-dessous). ["Découvrez comment changer la période de refroidissement"](#) et ["découvrez comment modifier le seuil"](#).

BlueXP vous permet de choisir parmi les stratégies de hiérarchisation de volume suivantes lorsque vous créez ou modifiez un volume :

Snapshot uniquement

Après avoir atteint une capacité de 50 %, Cloud Volumes ONTAP met à niveau les données utilisateur à froid des copies Snapshot qui ne sont pas associées au système de fichiers actif au niveau de la capacité. La période de refroidissement est d'environ 2 jours.

En cas de lecture, les blocs de données à froid sur le niveau de capacité deviennent chauds et sont déplacés vers le niveau de performance.

Tout

Toutes les données (sans les métadonnées) sont immédiatement marquées comme inactives et hiérarchisées vers le stockage objet dès que possible. Il n'est pas nécessaire d'attendre 48 heures que les nouveaux blocs d'un volume soient inactifs. Notez que les blocs situés dans le volume avant la définition de toutes les règles exigent 48 heures pour être froids.

Si les blocs de données inactives du Tier cloud sont lus, ceux-ci restent inactives et ne sont pas réécrits sur

le Tier de performance. Cette règle est disponible à partir de ONTAP 9.6.

Auto

Après avoir atteint une capacité de 50 %, Cloud Volumes ONTAP met à niveau des blocs de données à froid dans un volume vers un niveau de capacité. Les données à froid comprennent non seulement des copies Snapshot, mais aussi des données utilisateur à froid provenant du système de fichiers actif. La période de refroidissement est d'environ 31 jours.

Cette stratégie est prise en charge à partir de Cloud Volumes ONTAP 9.4.

En cas de lecture aléatoire, les blocs de données à froid du niveau de capacité deviennent chauds et passent au niveau de performance. Si elles sont lues par des lectures séquentielles, telles que celles associées aux analyses d'index et d'antivirus, les blocs de données à froid restent froids et ne passent pas au niveau de performance.

Aucune

Conserve les données d'un volume dans le niveau de performance, ce qui empêche leur déplacement vers le niveau de capacité.

Lorsque vous répliquez un volume, vous pouvez choisir le Tiering des données dans le stockage objet. Dans ce cas, BlueXP applique la stratégie **Backup** au volume de protection des données. Depuis Cloud Volumes ONTAP 9.6, la règle de hiérarchisation **All** remplace la règle de sauvegarde.

La désactivation de Cloud Volumes ONTAP a des répercussions sur la période de refroidissement

Les blocs de données sont refroidis par des analyses de refroidissement. Durant ce processus, la température des blocs pendant lesquels leur température de bloc n'a pas été utilisée est déplacée (refroidie) vers la valeur inférieure suivante. La durée de refroidissement par défaut dépend de la règle de Tiering du volume :

- Auto : 31 jours
- Snapshot uniquement : 2 jours

Cloud Volumes ONTAP doit être en cours d'exécution pour que l'acquisition de refroidissement fonctionne. Si le Cloud Volumes ONTAP est désactivé, le refroidissement s'arrête également. Les temps de refroidissement peuvent ainsi être plus longs.



Lorsque Cloud Volumes ONTAP est désactivé, la température de chaque bloc est préservée jusqu'au redémarrage du système. Par exemple, si la température d'un bloc est 5 lorsque vous mettez le système hors tension, la température est toujours 5 lorsque vous rallumez le système.

Configuration du tiering des données

Pour obtenir des instructions et une liste des configurations prises en charge, reportez-vous à la section ["Tiering des données inactives vers un stockage objet à faible coût"](#).

Gestion du stockage

BlueXP (anciennement Cloud Manager) offre une gestion simplifiée et avancée du stockage Cloud Volumes ONTAP.



Tous les disques et agrégats doivent être créés et supprimés directement depuis BlueXP. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Provisionnement du stockage

BlueXP simplifie le provisionnement du stockage pour Cloud Volumes ONTAP en vous achetant des disques et en gérant des agrégats. Il vous suffit de créer des volumes. Si vous le souhaitez, vous pouvez utiliser une option d'allocation avancée pour provisionner vous-même des agrégats.

Provisionnement simplifié

Les agrégats fournissent un stockage cloud aux volumes. BlueXP crée des agrégats pour vous lors du lancement d'une instance et pour le provisionnement de volumes supplémentaires.

Lorsque vous créez un volume, BlueXP fait l'une des trois choses suivantes :

- Il place le volume sur un agrégat existant qui dispose d'un espace libre suffisant.
- Il place le volume sur un agrégat existant en achetant plus de disques pour cet agrégat.

+ dans le cas d'un agrégat AWS qui prend en charge Elastic volumes, BlueXP augmente également la taille des disques d'un groupe RAID. ["En savoir plus sur la prise en charge d'Elastic volumes"](#).

- Il achète des disques pour un nouvel agrégat et place le volume sur cet agrégat.

BlueXP détermine où placer un nouveau volume en se intéressant à plusieurs facteurs : la taille maximale d'un agrégat, l'activation ou non du provisionnement fin et les seuils d'espace disponible pour les agrégats.



L'administrateur du compte peut modifier les seuils d'espace libre à partir de la page **Paramètres**.

Sélection de la taille du disque pour les agrégats dans AWS

Lorsque BlueXP crée de nouveaux agrégats pour Cloud Volumes ONTAP dans AWS, il augmente progressivement la taille du disque dans un agrégat, à mesure que le nombre d'agrégats du système augmente. BlueXP vous garantit ainsi que vous pouvez utiliser la capacité maximale du système avant d'atteindre le nombre maximal de disques de données autorisés par AWS.

Par exemple, BlueXP peut choisir les tailles de disque suivantes :

| Numéro d'agrégat | Taille du disque | Capacité d'agrégat max. |
|------------------|------------------|-------------------------|
| 1 | 500 Gio | 3 To |
| 4 | 1 To | 6 To |
| 6 | 2 To | 12 To |



Ce comportement ne s'applique pas aux agrégats qui prennent en charge la fonctionnalité Amazon EBS Elastic volumes. Les agrégats sur lesquels Elastic volumes sont activés comprennent un ou deux groupes RAID. Chaque groupe RAID dispose de quatre disques identiques de même capacité. ["En savoir plus sur la prise en charge d'Elastic volumes"](#).

Vous pouvez choisir vous-même la taille du disque en utilisant l'option d'allocation avancée.

Allocation avancée

Au lieu de laisser BlueXP gérer des agrégats pour vous, vous pouvez le faire vous-même. "[À partir de la page allocation avancée](#)", vous pouvez créer de nouveaux agrégats qui incluent un nombre spécifique de disques, ajouter des disques à un agrégat existant et créer des volumes dans des agrégats spécifiques.

Gestion de la capacité

L'administrateur du compte peut choisir si BlueXP vous informe des décisions relatives à la capacité de stockage ou si BlueXP gère automatiquement les besoins en capacité pour vous.

Ce comportement est déterminé par le *Capacity Management mode* sur un connecteur. Le mode de gestion de la capacité concerne tous les systèmes Cloud Volumes ONTAP gérés par ce connecteur. Si vous avez un autre connecteur, il peut être configuré différemment.

Gestion automatique de la capacité

Le mode de gestion de la capacité est défini sur automatique par défaut. Dans ce mode, BlueXP achète automatiquement de nouveaux disques pour les instances Cloud Volumes ONTAP lorsque davantage de capacité est nécessaire, supprime les ensembles de disques (agrégats) inutilisés, déplace des volumes entre les agrégats si nécessaire et tente de tomber en panne des disques.

Les exemples suivants illustrent le fonctionnement de ce mode :

- Si un agrégat atteint le seuil de capacité et dispose d'espace pour plus de disques, BlueXP achète automatiquement de nouveaux disques pour cet agrégat afin que les volumes puissent continuer à augmenter.

BlueXP vérifie le ratio d'espace libre toutes les 15 minutes pour déterminer s'il doit acheter des disques supplémentaires.

+ dans le cas d'un agrégat AWS qui prend en charge Elastic volumes, BlueXP augmente également la taille des disques d'un groupe RAID. "[En savoir plus sur la prise en charge d'Elastic volumes](#)".

- Lorsqu'un agrégat atteint le seuil de capacité et qu'il ne prend pas en charge de disques supplémentaires, BlueXP déplace automatiquement un volume de cet agrégat vers un agrégat disposant de la capacité disponible ou vers un nouvel agrégat.

Si BlueXP crée un nouvel agrégat pour le volume, il choisit une taille de disque adaptée à la taille de ce volume.

Notez que l'espace libre est désormais disponible sur l'agrégat d'origine. Les volumes existants ou les nouveaux volumes peuvent utiliser cet espace. Dans ce scénario, l'espace ne peut pas être retourné dans le Cloud provoqué.

- Si un agrégat ne contient aucun volume pendant plus de 12 heures, BlueXP le supprime.

Gestion des LUN avec gestion automatique de la capacité

La gestion automatique de la capacité de BlueXP ne s'applique pas aux LUN. Lorsque BlueXP crée un LUN, il désactive la fonction Autogrow.

Gestion manuelle de la capacité

Si l'administrateur de compte définit le mode gestion de la capacité sur manuel, BlueXP affiche les messages action requise lorsque des décisions de capacité doivent être prises. Les mêmes exemples décrits en mode automatique s'appliquent au mode manuel, mais il vous appartient d'accepter les actions.

En savoir plus >>

["Apprenez à modifier le mode de gestion de la capacité".](#)

Vitesse d'écriture

BlueXP vous permet de choisir une vitesse d'écriture normale ou élevée pour la plupart des configurations 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.

Vitesse d'écriture standard

Lorsque vous choisissez la vitesse d'écriture standard, les données sont écrites directement sur le disque. Lors de l'écriture directe des données sur le disque, réduit le risque de perte de données en cas de panne système non planifiée ou de défaillance en cascade impliquant une panne système non planifiée (paires haute disponibilité uniquement).

La vitesse d'écriture normale est l'option par défaut.

Vitesse d'écriture élevée

Lorsque vous choisissez la vitesse d'écriture élevée, les données sont mises en tampon dans la mémoire avant d'être écrites sur le disque, ce qui accélère les performances d'écriture. Toutefois, la mise en cache peut entraîner une perte de données en cas de panne système.

Le volume de données pouvant être perdues en cas de panne système correspond à l'étendue des deux derniers points de cohérence. Le point de cohérence consiste à écrire des données mises en tampon sur le disque. Un point de cohérence se produit lorsque le journal d'écriture est plein ou après 10 secondes (selon la première éventualité). Toutefois, les performances du stockage fournies par votre fournisseur cloud peuvent affecter le temps de traitement des points de cohérence.

Quand utiliser une vitesse d'écriture élevée

Optez pour la vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides et que vous ne craignez pas de perdre des données en cas de panne système non planifiée ou de défaillance en cascade impliquant une panne système non planifiée (paires haute disponibilité uniquement).

Recommandations lors de l'utilisation d'une vitesse d'écriture élevée

Si vous activez la vitesse d'écriture élevée, vous devez assurer la protection de l'écriture au niveau de la couche applicative ou que les applications tolèrent la perte de données, si elle se produit.

Vitesse d'écriture élevée avec une paire HA dans AWS

Si vous prévoyez d'activer une vitesse d'écriture élevée sur une paire haute disponibilité dans AWS, vous devriez connaître les différences de niveaux de protection entre un déploiement de plusieurs zones de disponibilité (AZ) et un déploiement d'AZ unique. Le déploiement d'une paire haute disponibilité dans plusieurs

AZS offre davantage de résilience et peut aider à limiter les risques de perte de données.

["En savoir plus sur les paires haute disponibilité dans AWS".](#)

Configurations qui prennent en charge une vitesse d'écriture élevée

Toutes les configurations Cloud Volumes ONTAP ne prennent pas en charge une vitesse d'écriture élevée. Ces configurations utilisent la vitesse d'écriture standard par défaut.

AWS

Si vous utilisez un système à un seul nœud, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec tous les types d'instances.

Dès la version 9.8, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec des paires HA lorsque vous utilisez presque tous les types d'instances EC2 pris en charge, sauf pour les instances m5.XLarge et r5.XLarge.

["En savoir plus sur les instances Amazon EC2 prises en charge par Cloud Volumes ONTAP".](#)

Azure

Si vous utilisez un système à un seul nœud, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée pour tous les types de VM.

Si vous utilisez une paire haute disponibilité, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec plusieurs types de VM, à partir de la version 9.8.1. Accédez au ["Notes de version de Cloud Volumes ONTAP"](#) Pour afficher les types de VM qui prennent en charge une vitesse d'écriture élevée.

Google Cloud

Si vous utilisez un système à un seul nœud, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée pour tous les types de machines.

Cloud Volumes ONTAP ne prend pas en charge une vitesse d'écriture élevée avec les paires HA dans Google Cloud.

["Découvrez plus en détail les types de machines Google Cloud pris en charge par Cloud Volumes ONTAP".](#)

Comment sélectionner une vitesse d'écriture

Vous pouvez choisir une vitesse d'écriture lorsque vous créez un nouvel environnement de travail et que vous le pouvez ["modifier la vitesse d'écriture d'un système existant"](#).

Que faut-il attendre si une perte de données se produit

Si une perte de données est due à une vitesse d'écriture élevée, le système de gestion des événements (EMS) signale les deux événements suivants :

- Cloud Volumes ONTAP 9.12.1 ou version ultérieure

```
NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 à 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 à 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

Dans ce cas, Cloud Volumes ONTAP doit être capable de démarrer et de continuer à transmettre des données sans l'intervention de l'utilisateur.

Comment arrêter l'accès aux données en cas de perte

Si vous êtes préoccupé par la perte de données, que les applications cessent de s'exécuter en cas de perte de données et que l'accès aux données doit être repris après que le problème de perte de données a été correctement résolu, vous pouvez utiliser l'option NVFAIL de la CLI pour atteindre cet objectif.

Pour activer l'option NVFAIL

```
vol modify -volume <vol-name> -nvfail on
```

Pour vérifier les paramètres NVFAIL

```
vol show -volume <vol-name> -fields nvfail
```

Pour désactiver l'option NVFAIL

```
vol modify -volume <vol-name> -nvfail off
```

En cas de perte de données, un volume NFS ou iSCSI avec NVFAIL activé devrait cesser de transmettre les données (le protocole CIFS n'a aucun impact, ce qui est sans état, n'a aucun impact). Pour plus de détails, reportez-vous à ["Impact de NVFAIL sur l'accès aux volumes NFS ou aux LUN"](#).

Pour vérifier l'état NVFAIL

```
vol show -fields in-nvfailed-state
```

Une fois le problème de perte de données résolu, vous pouvez effacer l'état NVFAIL et le volume sera disponible pour l'accès aux données.

Pour effacer l'état NVFAIL

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash cache

Certaines configurations Cloud Volumes ONTAP incluent le stockage NVMe local, que Cloud Volumes ONTAP utilise *Flash cache* pour de meilleures performances.

Qu'est-ce que Flash cache ?

Flash cache accélère l'accès aux données grâce à la mise en cache intelligente en temps réel des données utilisateur et des métadonnées NetApp lues récemment. Elle est efficace pour les charges de travail exigeant une capacité de lecture aléatoire maximale, dont les bases de données, la messagerie et les services de fichiers.

Configurations compatibles

Flash cache est pris en charge avec des configurations Cloud Volumes ONTAP spécifiques. Affichez les configurations prises en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#)

Limites

- La compression doit être désactivée sur tous les volumes pour tirer parti des améliorations des performances de Flash cache.

Choisissez l'absence d'efficacité du stockage lors de la création d'un volume depuis BlueXP, ou créez un volume puis ["Désactiver la compression des données à l'aide de l'interface de ligne de commande"](#).

- La réactivation du cache après un redémarrage n'est pas prise en charge avec Cloud Volumes ONTAP.

Stockage WORM

Vous pouvez activer le stockage WORM (écriture unique) en lecture seule sur un système Cloud Volumes ONTAP pour conserver les fichiers sous forme non modifiée pendant une période de conservation spécifiée. Le stockage WORM dans le cloud est optimisé par la technologie SnapLock, ce qui signifie que les fichiers WORM sont protégés au niveau des fichiers.

Fonctionnement du stockage WORM

Une fois qu'un fichier a été alloué au stockage WORM, il ne peut pas être modifié, même après l'expiration de la période de conservation. Une horloge inviolable détermine le moment où la période de conservation d'un fichier WORM s'est écoulée.

Une fois la période de conservation écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin.

Chargement

La charge du stockage WORM est horaire, selon la capacité totale provisionnée des volumes WORM.

Vous devez comprendre le comportement de charge suivant avec Cloud Volumes ONTAP 9.10.1 et versions ultérieures :

- Depuis ONTAP 9.10.1, des volumes WORM et non-WORM peuvent exister sur le même agrégat.
- Si vous activez WORM lorsque vous créez un environnement de travail Cloud Volumes ONTAP, tous les volumes que vous créez à partir de BlueXP sont compatibles WORM. Toutefois, vous pouvez utiliser l'interface de ligne de commandes ou System Manager ONTAP pour créer des volumes dont le protocole WORM est désactivé. Ces volumes ne sont pas facturés au taux WORM.
- Si vous n'activez pas WORM lorsque vous créez un environnement de travail, le mode WORM est désactivé pour chaque volume créé à partir de BlueXP. Vous n'êtes pas facturé au débit WORM pour ces volumes. Vous pouvez cependant utiliser l'interface de ligne de commandes ou System Manager de ONTAP pour créer des volumes compatibles WORM. Ces volumes seront facturés au taux WORM.

["En savoir plus sur la tarification pour le stockage WORM"](#)

Activation du stockage WORM

Vous pouvez activer le stockage WORM sur un système Cloud Volumes ONTAP lorsque vous créez un nouvel environnement de travail. Cela inclut la définition de la période de conservation par défaut pour les fichiers.



Vous ne pouvez pas activer le stockage WORM sur des volumes individuels :-WORM doit être activé au niveau du système.

L'image suivante montre comment activer le stockage WORM lors de la création d'un environnement de travail :

The screenshot shows the 'Create a New Working Environment' wizard in the Cloud Manager interface. The current step is 'WORM (write once, read many)'. On the left, under 'Write Speed', there are two options: 'Normal' (selected) and 'High'. The 'Normal' option description states: 'Data is written directly to disk, reducing the likelihood of data loss in the event of an unplanned system outage.' The 'High' option description states: 'Data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss in the event of an unplanned system outage.' On the right, under 'WORM', there is a description: 'You can use write once, read many (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level. [Learn More](#)'. Below this, there are two radio buttons: 'Disable WORM' and 'Activate WORM' (selected). A notice states: 'Notice: If you activate WORM storage, data tiering to object storage will be disabled on the system.' At the bottom, there is a 'Retention Period' field set to '15' years. A 'Continue' button is at the bottom center. The footer shows 'Cloud Manager 3.9.9 Build: 0 Jun 30, 2021 02:52:27 pm UTC Environment: staging'.

Validation de fichiers sur WORM

Vous pouvez utiliser une application pour valider des fichiers sur WORM via NFS ou CIFS, ou utiliser l'interface de ligne de commande ONTAP pour auto-valider des fichiers sur WORM automatiquement. Vous pouvez

également utiliser un fichier WORM inscriptible pour conserver les données écrites de façon incrémentielle, comme les informations de journal.

Après avoir activé le stockage WORM sur un système Cloud Volumes ONTAP, vous devez utiliser l'interface de ligne de commande ONTAP pour toute la gestion du stockage WORM. Pour obtenir des instructions, reportez-vous à la section "[Documentation ONTAP](#)".

Limites

- Le stockage WORM dans Cloud Volumes ONTAP fonctionne selon un modèle « administrateur de stockage de confiance ». Les fichiers WORM sont protégés contre les modifications ou modifications, mais un administrateur du cluster peut supprimer des volumes, même si ces volumes contiennent des données WORM non expirées.
- En plus du modèle d'administrateur de stockage de confiance, le stockage WORM dans Cloud Volumes ONTAP fonctionne aussi implicitement sous un modèle d'administrateur cloud reconnu. Un administrateur cloud peut supprimer des données WORM avant leur date d'expiration en supprimant ou en modifiant directement le stockage cloud du fournisseur cloud.
- Lorsque le stockage WORM est activé, le Tiering des données vers le stockage objet ne peut pas être activé.

Paires haute disponibilité

Paires haute disponibilité dans AWS

Une configuration haute disponibilité (HA) Cloud Volumes ONTAP assure des opérations sans interruption et une tolérance aux pannes. Dans AWS, les données sont mises en miroir de manière synchrone entre les deux nœuds.

Composants DE HAUTE DISPONIBILITÉ

Dans AWS, les configurations haute disponibilité de Cloud Volumes ONTAP incluent les composants suivants :

- Deux nœuds Cloud Volumes ONTAP dont les données sont mises en miroir de manière synchrone.
- Instance médiateur qui fournit un canal de communication entre les nœuds pour faciliter les processus de reprise et de remise du stockage.

Médiateur

Voici quelques informations clés sur l'instance de médiateur dans AWS :

Type d'instance

t2 micro

Disques

Un disque magnétique EBS d'environ 8 Gio.

Système d'exploitation

Debian 11



Pour Cloud Volumes ONTAP 9.10.0 et les versions antérieures, Debian 10 a été installée sur le médiateur.

Mises à niveau

Lorsque vous mettez à niveau Cloud Volumes ONTAP, BlueXP met également à jour l'instance médiateur si nécessaire.

Accès à l'instance

Lorsque vous créez une paire Cloud Volumes ONTAP HA à partir de BlueXP, vous êtes invité à fournir une paire de clés pour l'instance de médiateur. Vous pouvez utiliser cette paire de clés pour accéder à SSH à l'aide de l'admin utilisateur.

Agents tiers

Les agents tiers ou les extensions VM ne sont pas pris en charge sur l'instance médiateur.

Reprise et remise du stockage

Si un nœud tombe en panne, l'autre nœud peut servir les données à son partenaire pour fournir un service de données continu. Les clients peuvent accéder aux mêmes données à partir du nœud partenaire, car les données ont été mises en miroir de manière synchrone auprès du partenaire.

Après le redémarrage du nœud, le partenaire doit resynchroniser les données avant de pouvoir retourner le stockage. Le temps nécessaire à la resynchronisation des données dépend de la quantité de données modifiées pendant la panne du nœud.

Le basculement, la resynchronisation et le rétablissement du stockage sont automatiques par défaut. Aucune action de l'utilisateur n'est requise.

RPO et RTO

Une configuration haute disponibilité maintient la haute disponibilité de vos données comme suit :

- L'objectif du point de récupération (RPO) est de 0 seconde. Vos données sont transactionnelles, sans perte de données.
- L'objectif de temps de récupération (RTO) est de 60 secondes. En cas de panne, les données doivent être disponibles en 60 secondes ou moins.

Modèles de déploiement HA

Vous pouvez garantir la haute disponibilité de vos données en déployant une configuration haute disponibilité sur plusieurs zones de disponibilité (AZS) ou dans un seul AZ. Vous devriez consulter plus de détails sur chaque configuration afin de choisir celle qui répond le mieux à vos besoins.

Plusieurs zones de disponibilité

Le déploiement d'une configuration haute disponibilité dans plusieurs zones de disponibilité (AZS) garantit une haute disponibilité de vos données en cas de défaillance avec un système AZ ou une instance exécutant un nœud Cloud Volumes ONTAP. Vous devez comprendre l'impact des adresses IP NAS sur l'accès aux données et le basculement du stockage.

Accès aux données NFS et CIFS

Lorsqu'une configuration haute disponibilité est répartie entre plusieurs zones de disponibilité, *adresses IP flottantes* activez l'accès client NAS. Les adresses IP flottantes, qui doivent se trouver en dehors des blocs CIDR pour tous les VPC de la région, peuvent migrer entre les nœuds en cas de défaillance. Les clients ne sont pas accessibles de manière native en dehors du VPC, sauf si vous ["Configuration d'une passerelle de](#)

[transit AWS](#)".

Si vous ne pouvez pas configurer de passerelle de transit, des adresses IP privées sont disponibles pour les clients NAS qui ne sont pas du VPC. Cependant, ces adresses IP sont statiques ; elles ne peuvent pas basculer d'un nœud à l'autre.

Avant de déployer une configuration haute disponibilité sur plusieurs zones de disponibilité, vous devez consulter les exigences relatives aux adresses IP flottantes et aux tables de routage. Vous devez spécifier les adresses IP flottantes lors du déploiement de la configuration. Les adresses IP privées sont automatiquement créées par BlueXP.

Pour plus de détails, voir "[Configuration réseau AWS requise pour Cloud Volumes ONTAP HA dans plusieurs AZS](#)".

Accès aux données iSCSI

La communication de données entre VPC n'est pas un problème car iSCSI n'utilise pas d'adresses IP flottantes.

Basculement et rétablissement pour iSCSI

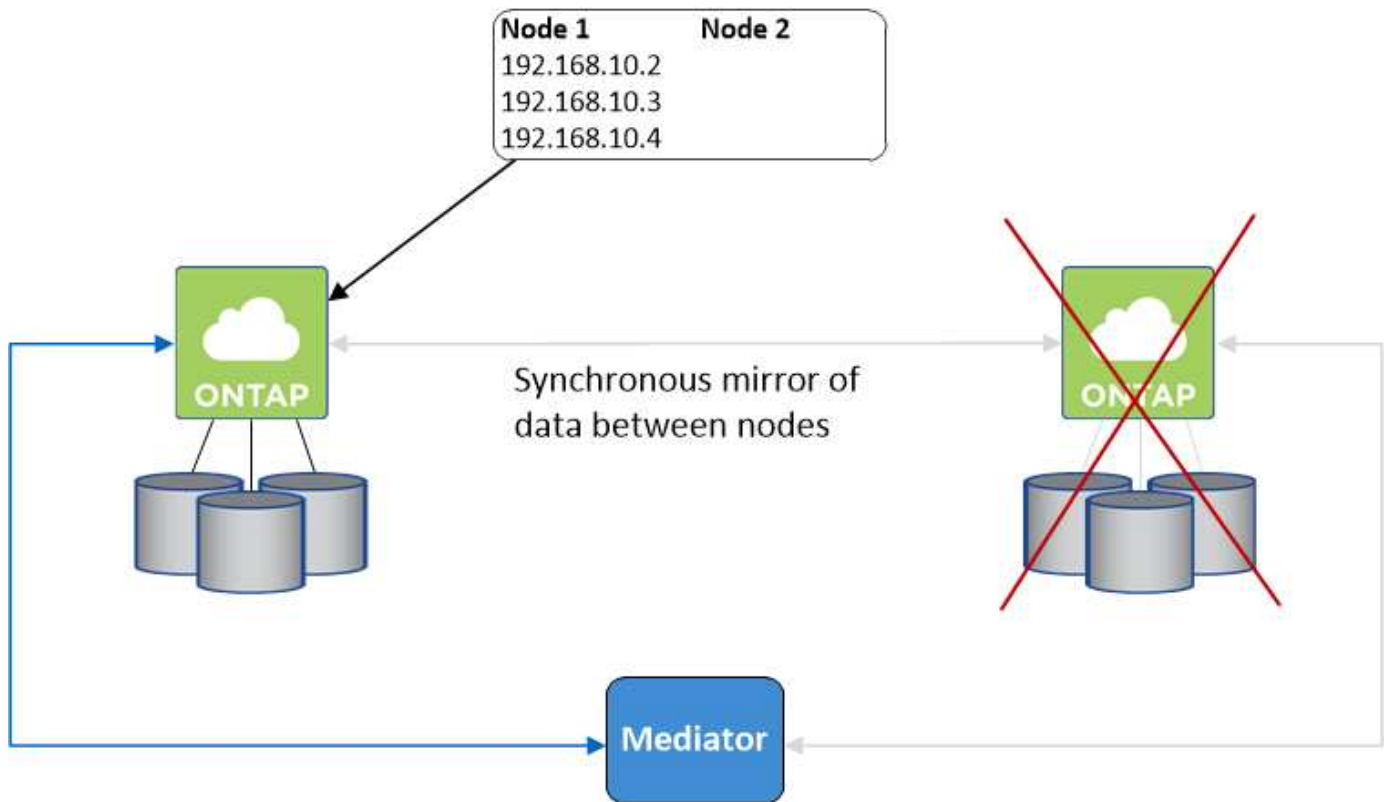
Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multichemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés et non optimisés.



Pour plus d'informations sur les configurations hôtes spécifiques qui prennent en charge ALUA, consultez le "[Matrice d'interopérabilité NetApp](#)" Et le Guide d'installation et de configuration des utilitaires hôtes pour votre système d'exploitation hôte.

Basculement et rétablissement pour NAS

Lorsque le basculement se produit dans une configuration NAS utilisant des adresses IP flottantes, l'adresse IP flottante du nœud que les clients utilisent pour accéder aux données transférées sur l'autre nœud. L'image suivante illustre la reprise du stockage dans une configuration NAS à l'aide d'adresses IP flottantes. Si le nœud 2 s'arrête, l'adresse IP flottante du nœud 2 passe au nœud 1.



Les adresses IP de données NAS utilisées pour l'accès VPC externe ne peuvent pas migrer entre les nœuds en cas de défaillance. Si un nœud est hors ligne, vous devez remonter manuellement les volumes vers des clients en dehors du VPC à l'aide de l'adresse IP de l'autre nœud.

Une fois le nœud défaillant remis en ligne, remontez les clients vers les volumes à l'aide de l'adresse IP d'origine. Cette étape est nécessaire pour éviter le transfert de données inutiles entre deux nœuds HA, ce qui peut entraîner un impact significatif sur les performances et la stabilité.

Vous pouvez facilement identifier l'adresse IP correcte dans BlueXP en sélectionnant le volume et en cliquant sur **Mount Command**.

Zone de disponibilité unique

Le déploiement d'une configuration HA dans une seule zone de disponibilité (AZ) peut garantir une haute disponibilité de vos données en cas de défaillance d'une instance exécutant un nœud Cloud Volumes ONTAP. Toutes les données sont accessibles en mode natif depuis l'extérieur du VPC.

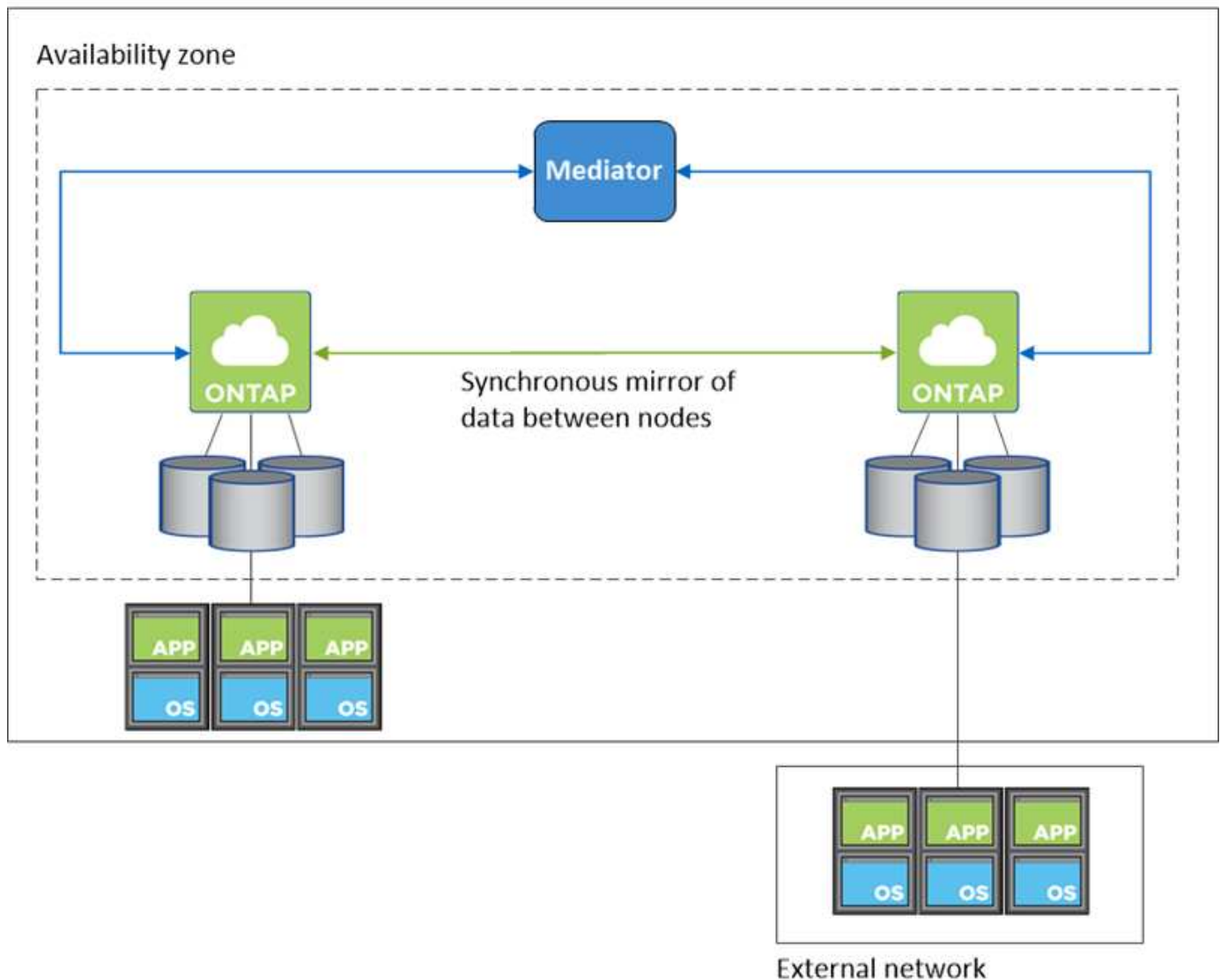


BlueXP crée un "**Groupe de placement AWS réparti**" Et lance les deux nœuds haute disponibilité de ce groupe de placement. Le groupe de placement réduit le risque de défaillances simultanées en répartissant les instances sur un matériel sous-jacent distinct. Cette fonctionnalité améliore la redondance en termes de calcul, et non en termes de défaillance des disques.

Accès aux données

Cette configuration étant dans un seul AZ, elle ne nécessite pas d'adresses IP flottantes. Vous pouvez utiliser la même adresse IP pour accéder aux données depuis le VPC et depuis l'extérieur du VPC.

L'image suivante montre une configuration HA dans un seul AZ. Les données sont accessibles depuis le VPC et depuis l'extérieur du VPC.



Takeover et Giveback

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multichemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés et non optimisés.



Pour plus d'informations sur les configurations hôtes spécifiques qui prennent en charge ALUA, consultez le "[Matrice d'interopérabilité NetApp](#)" Et le Guide d'installation et de configuration des utilitaires hôtes pour votre système d'exploitation hôte.

Pour les configurations NAS, les adresses IP des données peuvent migrer entre les nœuds HA en cas de défaillance. Cela garantit l'accès du client au stockage.

Fonctionnement du stockage dans une paire haute disponibilité

Contrairement à un cluster ONTAP, le stockage dans une paire Cloud Volumes ONTAP HA n'est pas partagé entre les nœuds. En revanche, les données sont mises en miroir de manière synchrone entre les nœuds afin que les données soient disponibles en cas de panne.

Allocation du stockage

Lorsque vous créez un nouveau volume et que vous avez besoin de disques supplémentaires, BlueXP alloue le même nombre de disques aux deux nœuds, crée un agrégat en miroir, puis crée le nouveau volume. Par exemple, si deux disques sont requis pour le volume, BlueXP alloue deux disques par nœud pour un total de quatre disques.

Configurations de stockage

Vous pouvez utiliser une paire HA comme configuration active-active, dans laquelle les deux nœuds servent les données aux clients ou comme configuration active-passive, dans laquelle le nœud passif répond aux demandes de données uniquement s'il a pris en charge le stockage pour le nœud actif.



Vous ne pouvez configurer une configuration active/active que si vous utilisez BlueXP dans la vue du système de stockage.

Attentes en matière de performances

Une configuration Cloud Volumes ONTAP HA réplique de manière synchrone les données entre les nœuds, ce qui consomme de la bande passante réseau. Par conséquent, vous pouvez vous attendre aux performances suivantes par rapport à une configuration Cloud Volumes ONTAP à nœud unique :

- Pour les configurations haute disponibilité qui ne servent que des données provenant d'un seul nœud, les performances de lecture sont comparables aux performances de lecture d'une configuration à un nœud, alors que les performances d'écriture sont plus faibles.
- Pour les configurations haute disponibilité qui servent les données des deux nœuds, les performances de lecture sont supérieures aux performances de lecture d'une configuration à nœud unique et les performances d'écriture sont identiques ou supérieures.

Pour plus d'informations sur les performances de Cloud Volumes ONTAP, reportez-vous à ["Performance"](#).

Accès client au stockage

Les clients doivent accéder aux volumes NFS et CIFS en utilisant l'adresse IP de données du nœud sur lequel réside le volume. Si les clients NAS accèdent à un volume en utilisant l'adresse IP du nœud partenaire, le trafic passe entre les deux nœuds, ce qui réduit les performances.

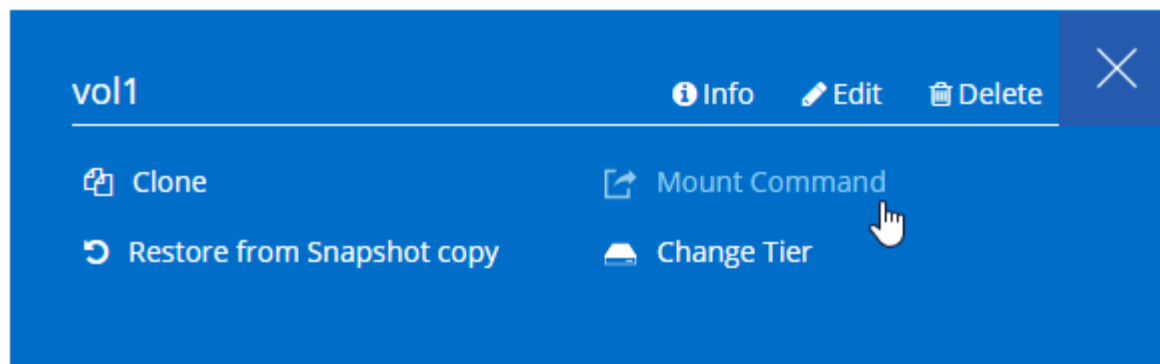


Si vous déplacez un volume entre les nœuds d'une paire HA, vous devez remonter le volume en utilisant l'adresse IP de l'autre nœud. Sinon, vous pouvez bénéficier d'une performance réduite. Si les clients prennent en charge les renvois NFSv4 ou la redirection de dossiers pour CIFS, vous pouvez activer ces fonctionnalités sur les systèmes Cloud Volumes ONTAP pour éviter de remanier le volume. Pour plus d'informations, consultez la documentation ONTAP.

Vous pouvez facilement identifier l'adresse IP appropriée à partir de BlueXP :

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



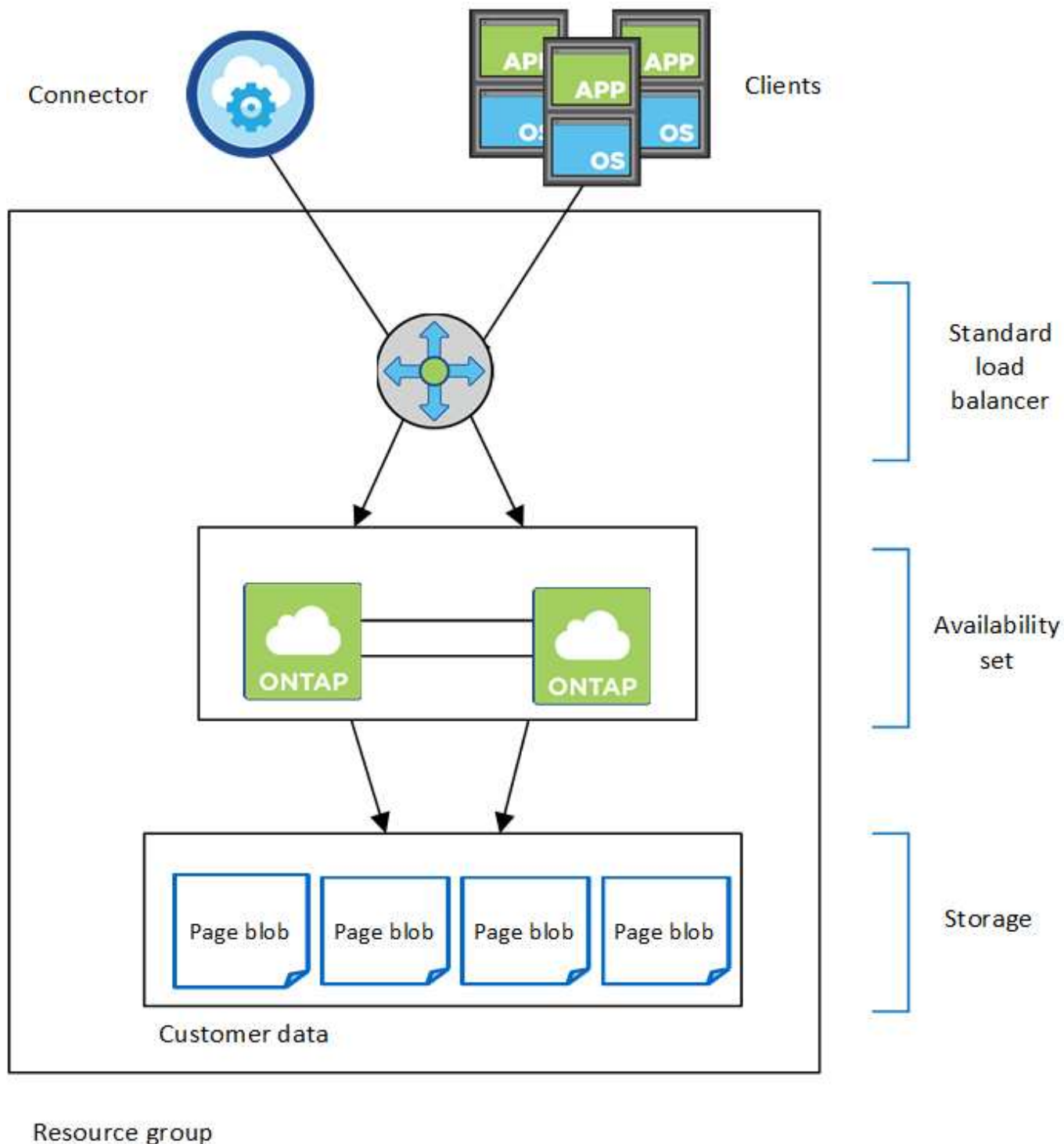
Paired high availability in Azure

A paired high availability Cloud Volumes ONTAP offers exceptional reliability and continuity of activity in case of failures in your cloud environment. In Azure, the storage is shared between the two nodes.

Components of HIGH AVAILABILITY

Configuration of unique availability zone **HIGH AVAILABILITY** with blob objects and pages

The configuration of Cloud Volumes ONTAP HA in Azure includes the following components:



Notez les éléments suivants concernant les composants Azure que BlueXP déploie pour vous :

Équilibreur de la charge Azure Standard

Le répartiteur de charge gère le trafic entrant vers la paire haute disponibilité Cloud Volumes ONTAP.

Ensemble de disponibilité

Le jeu de disponibilité Azure est un regroupement logique des nœuds Cloud Volumes ONTAP. L'ensemble de disponibilité garantit que les nœuds se trouvent dans des domaines de défaillance et de mise à jour différents pour assurer la redondance et la disponibilité. ["Pour en savoir plus sur les ensembles de disponibilité, consultez la documentation Azure".](#)

Disques

Les données client résident sur les blobs de la page Premium Storage. Chaque nœud a accès au stockage de l'autre nœud. Du stockage supplémentaire est également requis pour "des données « boot », « root » et « core »".

Comptes de stockage

- Un seul compte de stockage est nécessaire pour les disques gérés.
- Un ou plusieurs comptes de stockage sont requis pour les blobs de la page stockage Premium, car la limite de capacité de disque par compte de stockage est atteinte.

["Documentation Azure : objectifs d'évolutivité et de performances du stockage Azure pour les comptes de stockage"](#).

- Un seul compte de stockage est nécessaire pour le Tiering des données vers le stockage Azure Blob.
- Depuis Cloud Volumes ONTAP 9.7, les comptes de stockage créés par BlueXP pour les paires haute disponibilité sont des comptes de stockage v2 à usage général.
- Vous pouvez activer une connexion HTTPS à partir d'une paire haute disponibilité Cloud Volumes ONTAP 9.7 vers des comptes de stockage Azure lors de la création d'un environnement de travail. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé l'environnement de travail.

Configuration à zone de disponibilité unique HAUTE DISPONIBILITÉ avec disques gérés partagés

Une configuration à zone de disponibilité unique de Cloud Volumes ONTAP HA s'exécutant sur le disque géré partagé comprend les composants suivants :



Notez les éléments suivants concernant les composants Azure que BlueXP déploie pour vous :

Équilibreur de la charge Azure Standard

Le répartiteur de charge gère le trafic entrant vers la paire haute disponibilité Cloud Volumes ONTAP.

Ensemble de disponibilité

Le jeu de disponibilité Azure est un regroupement logique des nœuds Cloud Volumes ONTAP. L'ensemble de disponibilité garantit que les nœuds se trouvent dans des domaines de défaillance et de mise à jour différents pour assurer la redondance et la disponibilité. ["Pour en savoir plus sur les ensembles de disponibilité, consultez la documentation Azure".](#)

Disques

Les données client résident sur des disques gérés LRS (stockage redondant local). Chaque nœud a accès au stockage de l'autre nœud. Du stockage supplémentaire est également requis pour "[Données d'amorçage](#), [racine](#), [racine du partenaire](#), [cœur](#) et [données NVRAM](#)".

Comptes de stockage

Les comptes de stockage sont utilisés pour les déploiements sur disques gérés pour la gestion des journaux de diagnostic et le Tiering sur le stockage d'objets blob.

Configuration HAUTE DISPONIBILITÉ de plusieurs zones de disponibilité

Une configuration de plusieurs zones de disponibilité Cloud Volumes ONTAP HA dans Azure inclut les composants suivants :



Notez les éléments suivants concernant les composants Azure que BlueXP déploie pour vous :

Équilibreur de la charge Azure Standard

Le répartiteur de charge gère le trafic entrant vers la paire haute disponibilité Cloud Volumes ONTAP.

Zones de disponibilité

Deux nœuds Cloud Volumes ONTAP sont déployés sur différentes zones de disponibilité. Les zones de disponibilité garantissent que les nœuds se trouvent dans différents domaines de défaillance. ["En savoir plus sur la redondance du stockage Azure dans les documents Azure"](#).

Disques

Les données clients résident sur des disques gérés ZRS (zone-redondant Storage). Chaque nœud a accès au stockage de l'autre nœud. Du stockage supplémentaire est également requis pour "[données de démarrage, racine, racine partenaire et données principales](#)".

Comptes de stockage

Les comptes de stockage sont utilisés pour les déploiements sur disques gérés pour la gestion des journaux de diagnostic et le Tiering sur le stockage d'objets blob.

RPO et RTO

Une configuration haute disponibilité maintient la haute disponibilité de vos données comme suit :

- L'objectif du point de récupération (RPO) est de 0 seconde. Vos données sont transactionnelles, sans perte de données.
- L'objectif de temps de récupération (RTO) est de 60 secondes. En cas de panne, les données doivent être disponibles en 60 secondes ou moins.

Reprise et remise du stockage

À l'instar d'un cluster ONTAP physique, le stockage d'une paire HA Azure est partagé entre les nœuds. Des connexions au stockage du partenaire permettent à chaque nœud d'accéder au stockage de l'autre nœud dans le cas d'un *basculement*. Les mécanismes de basculement de chemin réseau garantissent que les clients et les hôtes continuent de communiquer avec le nœud survivant. Le partenaire *fournit* du stockage supplémentaire lorsque le nœud est revenu en ligne.

Pour les configurations NAS, les adresses IP des données migrent automatiquement entre les nœuds haute disponibilité en cas de défaillance.

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multichemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés et non optimisés.



Pour plus d'informations sur les configurations hôtes spécifiques qui prennent en charge ALUA, consultez le "[Matrice d'interopérabilité NetApp](#)" Et le Guide d'installation et de configuration des utilitaires hôtes pour votre système d'exploitation hôte.

Le basculement, la resynchronisation et le rétablissement du stockage sont automatiques par défaut. Aucune action de l'utilisateur n'est requise.

Configurations de stockage

Vous pouvez utiliser une paire HA comme configuration active-active, dans laquelle les deux nœuds servent les données aux clients ou comme configuration active-passive, dans laquelle le nœud passif répond aux demandes de données uniquement s'il a pris en charge le stockage pour le nœud actif.

Paires haute disponibilité dans Google Cloud

Une configuration haute disponibilité (HA) Cloud Volumes ONTAP assure des opérations sans interruption et une tolérance aux pannes. Dans Google Cloud, les données sont mises en miroir de manière synchrone entre les deux nœuds.

Composants DE HAUTE DISPONIBILITÉ

Les configurations de haute disponibilité de Cloud Volumes ONTAP dans Google Cloud incluent les composants suivants :

- Deux nœuds Cloud Volumes ONTAP dont les données sont mises en miroir de manière synchrone.
- Instance médiateur qui fournit un canal de communication entre les nœuds pour faciliter les processus de reprise et de remise du stockage.
- Une ou trois zones (recommandé).

Si vous choisissez trois zones, les deux nœuds et le médiateur se trouvent dans des zones Google Cloud distinctes.

- Quatre clouds privés virtuels (VPC).

La configuration utilise quatre VPC, car GCP exige que chaque interface réseau réside dans un réseau VPC distinct.

- Quatre équilibreurs de charge internes (TCP/UDP) Google Cloud qui gèrent le trafic entrant vers la paire HA Cloud Volumes ONTAP.

["En savoir plus sur les exigences de mise en réseau"](#), Y compris plus de détails sur les équilibreurs de charge, les VPC, les adresses IP internes, les sous-réseaux, etc.

L'image conceptuelle suivante montre une paire haute disponibilité Cloud Volumes ONTAP et ses composants :



Médiateur

Voici quelques informations clés sur l'instance de médiateur dans Google Cloud :

Type d'instance

e2-micro (une instance f1-micro était auparavant utilisée)

Disques

Deux disques persistants standard de 10 Gio chacun

Système d'exploitation

Debian 11



Pour Cloud Volumes ONTAP 9.10.0 et les versions antérieures, Debian 10 a été installée sur le médiateur.

Mises à niveau

Lorsque vous mettez à niveau Cloud Volumes ONTAP, BlueXP met également à jour l'instance médiateur si nécessaire.

Accès à l'instance

Pour Debian, l'utilisateur de Cloud par défaut est `admin`. Google Cloud crée et ajoute des certificats pour le `admin` Utilisateur lorsque l'accès SSH est demandé via la console Google Cloud ou la ligne de commande `gcloud`. Vous pouvez spécifier `sudo` pour obtenir des privilèges root.

Agents tiers

Les agents tiers ou les extensions VM ne sont pas pris en charge sur l'instance médiateur.

Reprise et remise du stockage

Si un nœud tombe en panne, l'autre nœud peut servir les données à son partenaire pour fournir un service de données continu. Les clients peuvent accéder aux mêmes données à partir du nœud partenaire, car les données ont été mises en miroir de manière synchrone auprès du partenaire.

Après le redémarrage du nœud, le partenaire doit resynchroniser les données avant de pouvoir retourner le stockage. Le temps nécessaire à la resynchronisation des données dépend de la quantité de données modifiées pendant la panne du nœud.

Le basculement, la resynchronisation et le rétablissement du stockage sont automatiques par défaut. Aucune action de l'utilisateur n'est requise.

RPO et RTO

Une configuration haute disponibilité maintient la haute disponibilité de vos données comme suit :

- L'objectif du point de récupération (RPO) est de 0 seconde.

Vos données sont transactionnaires, sans perte de données.

- L'objectif de temps de récupération (RTO) est de 60 secondes.

En cas de panne, les données doivent être disponibles en 60 secondes ou moins.

Modèles de déploiement HA

Vous pouvez assurer la haute disponibilité de vos données en déployant une configuration haute disponibilité dans plusieurs zones ou sur une seule zone.

Zones multiples (recommandé)

Le déploiement d'une configuration haute disponibilité sur trois zones garantit la disponibilité continue des données en cas de défaillance au sein d'une zone. Notez que les performances d'écriture sont légèrement inférieures à celles d'une seule zone, mais cela est minime.

Zone unique

Lorsqu'elle est déployée dans une seule zone, la configuration Cloud Volumes ONTAP haute disponibilité utilise une règle de placement réparti. Cette règle garantit qu'une configuration haute disponibilité est protégée contre un point de défaillance unique dans la zone, sans avoir à utiliser des zones distinctes pour isoler les pannes.

Ce modèle de déploiement réduit vos coûts, car il n'y a pas de frais de sortie de données entre les zones.

Fonctionnement du stockage dans une paire haute disponibilité

À la différence d'un cluster ONTAP, le stockage dans une paire haute disponibilité Cloud Volumes ONTAP dans GCP n'est pas partagé entre les nœuds. En revanche, les données sont mises en miroir de manière synchrone entre les nœuds afin que les données soient disponibles en cas de panne.

Allocation du stockage

Lorsque vous créez un nouveau volume et que vous avez besoin de disques supplémentaires, BlueXP alloue le même nombre de disques aux deux nœuds, crée un agrégat en miroir, puis crée le nouveau volume. Par exemple, si deux disques sont requis pour le volume, BlueXP alloue deux disques par nœud pour un total de quatre disques.

Configurations de stockage

Vous pouvez utiliser une paire HA comme configuration active-active, dans laquelle les deux nœuds servent les données aux clients ou comme configuration active-passive, dans laquelle le nœud passif répond aux demandes de données uniquement s'il a pris en charge le stockage pour le nœud actif.

Attentes en matière de performances pour une configuration haute disponibilité

Une configuration Cloud Volumes ONTAP HA réplique de manière synchrone les données entre les nœuds, ce qui consomme de la bande passante réseau. Par conséquent, vous pouvez vous attendre aux performances suivantes par rapport à une configuration Cloud Volumes ONTAP à nœud unique :

- Pour les configurations haute disponibilité qui ne servent que des données provenant d'un seul nœud, les performances de lecture sont comparables aux performances de lecture d'une configuration à un nœud, alors que les performances d'écriture sont plus faibles.
- Pour les configurations haute disponibilité qui servent les données des deux nœuds, les performances de lecture sont supérieures aux performances de lecture d'une configuration à nœud unique et les performances d'écriture sont identiques ou supérieures.

Pour plus d'informations sur les performances de Cloud Volumes ONTAP, reportez-vous à ["Performance"](#).

Accès client au stockage

Les clients doivent accéder aux volumes NFS et CIFS en utilisant l'adresse IP de données du nœud sur lequel réside le volume. Si les clients NAS accèdent à un volume en utilisant l'adresse IP du nœud partenaire, le trafic passe entre les deux nœuds, ce qui réduit les performances.

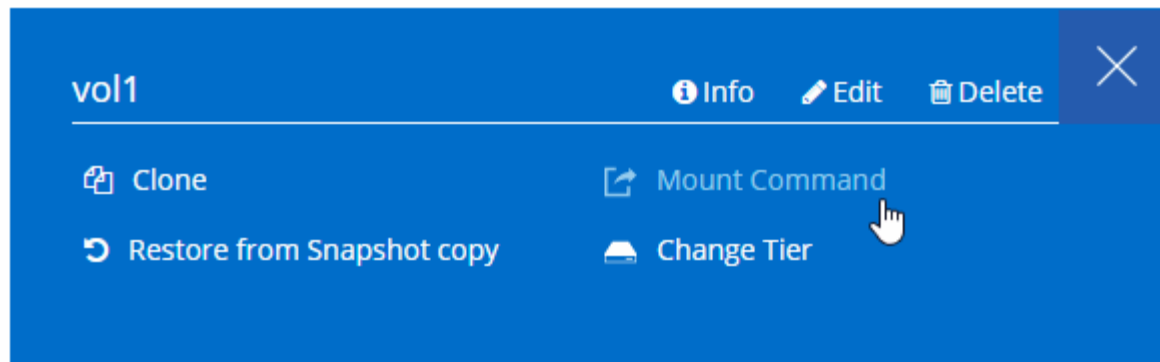


Si vous déplacez un volume entre les nœuds d'une paire HA, vous devez remonter le volume en utilisant l'adresse IP de l'autre nœud. Sinon, vous pouvez bénéficier d'une performance réduite. Si les clients prennent en charge les renvois NFSv4 ou la redirection de dossiers pour CIFS, vous pouvez activer ces fonctionnalités sur les systèmes Cloud Volumes ONTAP pour éviter de remanier le volume. Pour plus d'informations, consultez la documentation ONTAP.

Vous pouvez facilement identifier l'adresse IP appropriée à partir de BlueXP :

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



Liens connexes

- ["En savoir plus sur les exigences de mise en réseau"](#)
- ["Découvrez comment utiliser GCP"](#)

Actions non disponibles lors du basculement

Lorsqu'un nœud d'une paire HA n'est pas disponible, l'autre nœud transmet les données à son partenaire pour assurer la continuité du service de données. Il s'agit de la *_prise de contrôle_* du stockage. Plusieurs actions sont indisponibles jusqu'à la fin du rétablissement dans le stockage.



Lorsqu'un nœud d'une paire HA n'est pas disponible, l'état de l'environnement de travail dans BlueXP est *dégradé*.

Les actions suivantes ne sont pas disponibles depuis BlueXP Storage Takeover :

- Inscription au support
- Modifications de licence
- Modifications du type d'instance ou de VM
- Modification de la vitesse d'écriture
- Configuration CIFS
- Modification de l'emplacement des sauvegardes de configuration
- Définition du mot de passe du cluster
- Gestion des disques et des agrégats (allocation avancée)

Ces actions sont à nouveau disponibles une fois le rétablissement du stockage terminé et l'état de l'environnement de travail revenir à la normale.

Sécurité

Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.

Cryptage des données au repos

Cloud Volumes ONTAP prend en charge les technologies de cryptage suivantes :

- Solutions de chiffrement NetApp (NVE et NAE)
- Service de gestion des clés AWS
- Chiffrement de service de stockage Azure
- Chiffrement par défaut Google Cloud Platform

Les solutions de cryptage NetApp sont compatibles avec le chiffrement natif de votre fournisseur cloud, qui crypte les données au niveau de l'hyperviseur. Cela permettrait de fournir un double chiffrement, ce qui peut être souhaité pour des données très sensibles. Lors de l'accès aux données chiffrées, elles sont non chiffrées à deux reprises au niveau de l'hyperviseur (à l'aide de clés fournies par le fournisseur cloud), puis à l'aide des solutions de chiffrement NetApp (à l'aide de clés fournies par un gestionnaire de clés externe).

Solutions de chiffrement NetApp (NVE et NAE)

Prise en charge de Cloud Volumes ONTAP ["NetApp Volume Encryption \(NVE\) et chiffrement d'agrégat NetApp \(NAE\)"](#). NVE et NAE sont des solutions logicielles qui permettent le chiffrement des données au repos (conformes à la norme FIPS) de volumes 140-2. NVE et NAE utilisent tous deux le chiffrement AES 256 bits.

- NVE chiffre les données au repos un volume à la fois. Chaque volume de données dispose de sa propre clé de chiffrement unique.
- NAE est une extension de NVE qui chiffre les données pour chaque volume, tandis que les volumes partagent une clé dans l'ensemble de l'agrégat. NAE permet également la déduplication de blocs communs à tous les volumes de l'agrégat.

NVE et NAE sont pris en charge par un gestionnaire de clés externe.

Par défaut, NetApp Aggregate Encryption (NAE) est activé sur les nouveaux agrégats après la configuration d'un gestionnaire de clés externe. Pour les nouveaux volumes qui ne font pas partie d'un agrégat NAE, NetApp Volume Encryption (NVE) est activé par défaut (par exemple, si des agrégats existants ont été créés avant de configurer un gestionnaire de clés externe).

La configuration d'un gestionnaire de clés pris en charge est la seule étape requise. Pour les instructions de configuration, reportez-vous à la section ["Cryptage de volumes grâce aux solutions de cryptage NetApp"](#).

Service de gestion des clés AWS

Lorsque vous lancez un système Cloud Volumes ONTAP dans AWS, vous pouvez activer le chiffrement des données à l'aide du ["AWS Key Management Service \(KMS\)"](#). BlueXP demande des clés de données à l'aide d'une clé maître client (CMK).



Une fois que vous avez créé un système Cloud Volumes ONTAP, vous ne pouvez pas modifier la méthode de chiffrement des données AWS.

Si vous souhaitez utiliser cette option de cryptage, vous devez vous assurer que le système AWS KMS est correctement configuré. Pour plus de détails, voir ["Configuration du système AWS KMS"](#).

Chiffrement de service de stockage Azure

Les données sont automatiquement chiffrées sur Cloud Volumes ONTAP dans Azure à l'aide de ["Chiffrement de service de stockage Azure"](#) Et elle est dotée d'une clé gérée par Microsoft.

Si vous préférez, vous pouvez utiliser vos propres clés de chiffrement. ["Découvrez comment configurer Cloud Volumes ONTAP de manière à utiliser une clé gérée par le client dans Azure"](#).

Chiffrement par défaut Google Cloud Platform

["Chiffrement des données au repos Google Cloud Platform"](#) Est activé par défaut pour Cloud Volumes ONTAP. Aucune configuration n'est requise.

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser les API BlueXP pour créer un système Cloud Volumes ONTAP qui utilise des clés de chiffrement *gérées par le client*. Il s'agit des clés que vous créez et gérez dans GCP à l'aide du service Cloud Key Management. ["En savoir plus >>"](#).

Analyse antivirus ONTAP

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur les systèmes ONTAP pour protéger les données contre les virus ou tout autre code malveillant.

L'analyse antivirus ONTAP, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, voir le ["Matrice d'interopérabilité NetApp"](#).

Pour plus d'informations sur la configuration et la gestion de la fonctionnalité antivirus sur les systèmes ONTAP, consultez la ["Guide de configuration antivirus ONTAP 9"](#).

Protection par ransomware

Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. BlueXP vous permet d'implémenter la solution NetApp pour ransomware. Elle fournit des outils efficaces pour la visibilité, la détection et la résolution de problèmes.

- BlueXP identifie les volumes qui ne sont pas protégés par une règle Snapshot et vous permet d'activer la stratégie Snapshot par défaut sur ces volumes.

Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

- BlueXP vous permet également de bloquer les extensions de fichiers ransomware courantes en activant la solution FPolicy d'ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection ⓘ

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

2 Block Ransomware File Extensions ⓘ



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names ⓘ](#)

Activate FPolicy

"Découvrez comment implémenter la solution NetApp contre les attaques par ransomware".

Performance

Vous pouvez consulter les résultats des performances pour déterminer les charges de travail appropriées à Cloud Volumes ONTAP.

Rapports techniques sur les performances

- Cloud Volumes ONTAP pour AWS

["Rapport technique NetApp 4383 : caractérisation des performances de Cloud Volumes ONTAP dans Amazon Web Services avec des charges de travail applicatives"](#)

- Cloud Volumes ONTAP pour Microsoft Azure

["Rapport technique NetApp 4671 : caractérisation des performances de Cloud Volumes ONTAP dans Azure avec les charges de travail applicatives"](#)

- Cloud Volumes ONTAP pour Google Cloud

["Rapport technique NetApp 4816 : caractérisation des performances d'Cloud Volumes ONTAP pour Google Cloud"](#)

Performances du processeur

Les nœuds Cloud Volumes ONTAP sont pleinement exploités (plus de 90 %) à partir des outils de contrôle de votre fournisseur cloud. En effet, ONTAP se réserve tous les CPU virtuels présentés à la machine virtuelle afin qu'ils soient disponibles en cas de besoin.

Pour obtenir de l'aide, reportez-vous au ["Article de la base de connaissances NetApp sur la façon de surveiller l'utilisation du CPU ONTAP à l'aide de l'interface de ligne de commande"](#)

Gestion de licence pour le modèle BYOL basé sur les nœuds

Chaque système Cloud Volumes ONTAP associé à un modèle BYOL basé sur des nœuds doit disposer d'une licence système installée avec un abonnement actif. BlueXP simplifie le processus en gérant les licences pour vous et en affichant un avertissement avant leur expiration.



Une licence basée sur des nœuds est la génération précédente (BYOL) pour Cloud Volumes ONTAP. Une licence basée sur les nœuds est disponible uniquement pour les renouvellements de licence.

["En savoir plus sur les options des licences Cloud Volumes ONTAP"](#).

Licences de système BYOL

Une licence basée sur les nœuds offre jusqu'à 368 Tio de capacité pour une seule nœud ou paire HA.

Vous pouvez acheter plusieurs licences pour un système Cloud Volumes ONTAP BYOL pour allouer plus de 368 Tio de capacité. Par exemple, vous pouvez acheter deux licences pour allouer une capacité allant jusqu'à 736 Tio à Cloud Volumes ONTAP. Vous pouvez également acheter quatre licences pour obtenir jusqu'à 1.4 Pio.

Le nombre de licences que vous pouvez acheter pour un système à un seul nœud ou une paire HA est illimité.



Certains systèmes de stockage ONTAP sur site que vous avez achetés peuvent inclure une licence Cloud Volumes ONTAP gratuite. Vous pouvez utiliser la licence pour créer un système Cloud Volumes ONTAP. Vous pouvez également appliquer la licence à un système Cloud Volumes ONTAP existant afin d'étendre la capacité. ["Voyez si vous disposez de licences disponibles à utiliser"](#).

Notez que les limites de disques peuvent vous empêcher d'atteindre la limite de capacité en utilisant des disques seuls. Vous pouvez aller au-delà de la limite des disques de ["tiering des données inactives vers le stockage objet"](#). Pour plus d'informations sur les limites de disques, reportez-vous à la section ["Limites de stockage dans les notes de mise à jour de Cloud Volumes ONTAP"](#).

Gestion des licences pour un nouveau système

Lorsque vous créez un système BYOL basé sur des nœuds, BlueXP vous demande le numéro de série de votre licence et votre compte sur le site de support NetApp. BlueXP utilise le compte pour télécharger le fichier de licence depuis NetApp et l'installer sur le système Cloud Volumes ONTAP.

["Découvrez comment ajouter des comptes au site de support NetApp à BlueXP"](#).

Si BlueXP ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez ["Procurez-vous le fichier vous-même, puis téléchargez manuellement le fichier dans BlueXP"](#).

Expiration de la licence

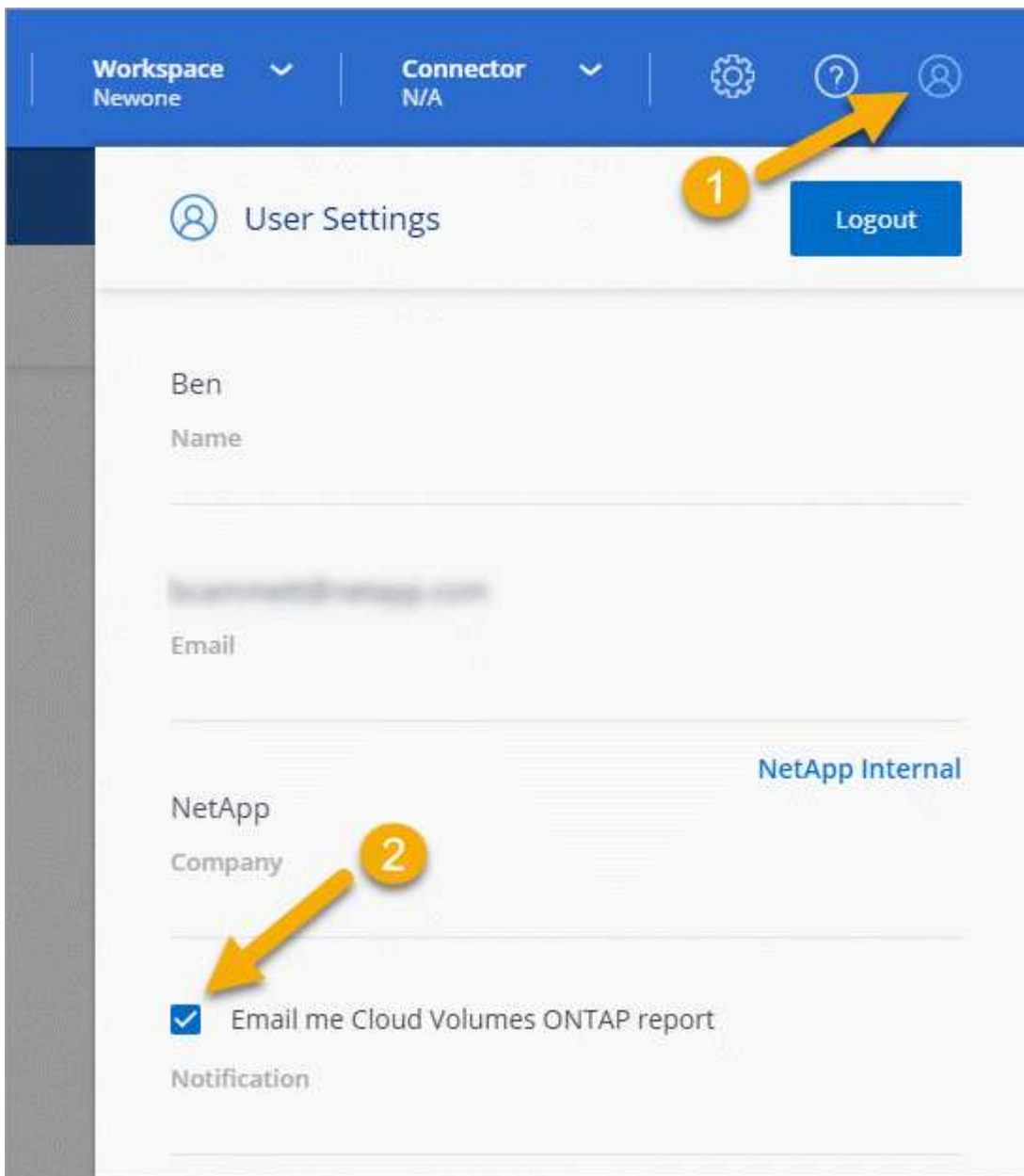
BlueXP affiche un avertissement 30 jours avant l'expiration d'une licence basée sur un nœud, puis une nouvelle fois lorsque la licence expire. L'image suivante affiche un avertissement d'expiration de 30 jours qui

s'affiche dans l'interface utilisateur :



Vous pouvez sélectionner l'environnement de travail pour consulter le message.

BlueXP inclut un avertissement d'expiration de licence dans le rapport Cloud Volumes ONTAP qui vous est envoyé par e-mail, si vous êtes un administrateur de compte et que vous avez activé l'option :



Le rapport envoyé par e-mail comprend l'avertissement d'expiration de la licence toutes les deux semaines.

Si vous ne renouvelez pas la licence à temps, le système Cloud Volumes ONTAP s'arrête. Si vous le redémarrez, il s'arrête de nouveau.

Renouvellement de la licence

Lorsque vous renouvelez un abonnement BYOL basé sur les nœuds en contactant un représentant NetApp, BlueXP obtient automatiquement la nouvelle licence NetApp et l'installe sur le système Cloud Volumes ONTAP.

Si BlueXP ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez ["Procurez-vous le fichier vous-même, puis téléchargez manuellement le fichier dans BlueXP"](#).

Transfert de licence vers un nouveau système

Lorsque vous supprimez un système existant, une licence BYOL basée sur des nœuds est transférable entre les systèmes Cloud Volumes ONTAP, puis créez un nouveau système en utilisant la même licence.

Par exemple, vous pouvez supprimer un système sous licence existant, puis utiliser la licence avec un nouveau système BYOL dans un autre fournisseur VPC/vNet ou cloud. Notez que seuls les numéros de série *indépendants du cloud peuvent fonctionner dans n'importe quel fournisseur cloud. Les numéros de série indépendants du cloud commencent par le préfixe _908xxxx*.

Il est important de noter que la licence BYOL est liée à votre entreprise et à un ensemble spécifique d'informations d'identification sur le site de support NetApp.

Conseiller digital AutoSupport et Active IQ

Le composant AutoSupport de ONTAP collecte les données de télémétrie et les envoie pour analyse. Le conseiller digital Active IQ analyse les données d'AutoSupport et fournit un support proactif et une optimisation. Avec l'intelligence artificielle, Active IQ peut identifier les problèmes potentiels et vous aider à les résoudre avant qu'ils n'affectent votre activité.

Active IQ vous permet d'optimiser votre infrastructure de données dans l'ensemble de votre cloud hybride grâce à un portail cloud et à une application mobile qui offrent des analyses prédictives et un support proactif. Les informations et les recommandations basées sur les données de Active IQ sont accessibles à tous les clients NetApp qui possèdent un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques avantages que vous pouvez faire avec Active IQ :

- Planification des mises à niveau.

Active IQ identifie les problèmes qui peuvent être résolus dans votre environnement en effectuant une mise à niveau vers la plus récente version d'ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.

- Voir le bien-être du système.

Votre tableau de bord Active IQ signale tout problème éventuel et vous aide à le corriger. Surveillez la capacité du système pour vous assurer que votre espace de stockage est insuffisant. Consultez les dossiers de demande de support de votre système.

- Gestion des performances.

Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans ONTAP System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur les performances. Optimisez l'efficacité. Affichez les mesures de l'efficacité du stockage et identifiez des moyens de stocker plus de données dans moins d'espace.

- Voir l'inventaire et la configuration.

Active IQ affiche des informations complètes sur l'inventaire et la configuration logicielle et matérielle. Voyez quand les contrats de service arrivent à expiration et renouvelez-les pour vous assurer que vous restez pris en charge.

Informations associées

- ["Documentation NetApp : conseiller digital Active IQ"](#)
- ["Lancez Active IQ"](#)
- ["Services SupportEdge"](#)

Configuration par défaut pour Cloud Volumes ONTAP

La configuration par défaut de Cloud Volumes ONTAP peut vous aider à configurer et administrer vos systèmes, surtout si vous connaissez ONTAP, car la configuration par défaut de Cloud Volumes ONTAP est différente de ONTAP.

Configuration par défaut

- BlueXP crée une VM de stockage qui assure le service des données lors du déploiement de Cloud Volumes ONTAP. Certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires. ["En savoir plus sur la gestion des machines virtuelles de stockage"](#).

Depuis la version BlueXP 3.9.5, le reporting de l'espace logique est activé sur la machine virtuelle de stockage initiale. Lorsqu'un espace est indiqué de manière logique, ONTAP indique l'espace volume afin que toutes les fonctionnalités d'efficacité du stockage soient également signalées comme utilisées.

- BlueXP installe automatiquement les licences de fonction ONTAP suivantes sur Cloud Volumes ONTAP :
 - CIFS
 - FlexCache
 - FlexClone
 - iSCSI
 - Gestion des clés de chiffrement mutualisée (MTEKM), à partir de Cloud Volumes ONTAP 9.11.1
 - Chiffrement de volume NetApp (uniquement pour les systèmes BYOL ou enregistrés de PAYGO)
 - NFS
- SnapMirror
- SnapRestore
- SnapVault
 - Plusieurs interfaces réseau sont créées par défaut :

- Un LIF de gestion de cluster
- Un FRV intercluster
- LIF de gestion SVM sur des systèmes HA dans Azure
- LIF de gestion SVM sur des systèmes HA dans Google Cloud
- Une LIF de gestion SVM sur des systèmes à un seul nœud dans AWS
- Un LIF de gestion des nœuds

+ dans Google Cloud, cette LIF est associée au LIF intercluster.

- Un LIF de données iSCSI
- Un LIF de données CIFS et NFS



Le basculement de LIF est désactivé par défaut pour Cloud Volumes ONTAP en raison des exigences du fournisseur de cloud. La migration d'un LIF vers un port différent rompt le mappage externe entre les adresses IP et les interfaces réseau de l'instance, ce qui rend le LIF inaccessible.

- Cloud Volumes ONTAP envoie des sauvegardes de configuration au connecteur via HTTPS.

Les sauvegardes sont accessibles à partir de <https://ipaddress/occm/offboxconfig/> Où *ipaddress* est l'adresse IP de l'hôte du connecteur.

- BlueXP définit quelques attributs de volume différemment des autres outils de gestion (System Manager ou CLI, par exemple).

Le tableau suivant répertorie les attributs de volume définis par BlueXP différemment des valeurs par défaut :

| Attribut | Valeur définie par BlueXP |
|-------------------------------------|--|
| Mode Autosize | Grandir |
| Positionnement automatique maximum | 1 000 pour cent  L'administrateur du compte peut modifier cette valeur à partir de la page Paramètres. |
| Style de sécurité | NTFS pour les volumes CIFS UNIX pour les volumes NFS |
| Style de garantie de l'espace | Aucune |
| Autorisations UNIX (NFS uniquement) | 776 |

+

Voir la "[ONTAP volume create man page](#)" pour plus d'informations sur ces attributs.

Disques internes pour les données système

En plus du stockage des données utilisateur, BlueXP achète également le cloud pour les données système.

AWS

- Trois disques par nœud pour les données de démarrage, root et core :
 - Disque io1 de 45 Gio pour les données de démarrage
 - Disque gp3 140 Gio pour les données racines
 - Disque gp2 540 Gio pour les données centrales
- Un instantané EBS pour chaque disque d'initialisation et disque racine
- Pour les paires HA, un volume EBS pour l'instance Mediator, qui est d'environ 8 Gio
- Lorsque vous activez le chiffrement des données dans AWS à l'aide du service de gestion des clés (KMS), les disques racine et de démarrage pour Cloud Volumes ONTAP sont également chiffrés. Cela comprend le disque de démarrage de l'instance médiateur dans une paire HA. Les disques sont chiffrés à l'aide du CMK que vous sélectionnez lors de la création de l'environnement de travail.



Dans AWS, la mémoire NVRAM est sur le disque de démarrage.

Azure (un seul nœud)

- Trois disques SSD Premium :
 - Un disque de 10 Gio pour les données de démarrage
 - Un disque de 140 Gio pour les données racines
 - Un disque de 512 Gio pour la NVRAM

Si la machine virtuelle que vous choisissez pour Cloud Volumes ONTAP prend en charge les disques SSD Ultra, le système utilise un SSD Ultra de 32 Gio pour la mémoire NVRAM, plutôt qu'un SSD Premium.

- Un disque dur standard de 1024 Gio pour économiser les coûts
- Un snapshot Azure pour chaque disque d'initialisation et disque racine
- Par défaut, chaque disque dans Azure est chiffré au repos.

Azure (paire HA)

Paires HA avec un blob de pages

- Deux disques SSD Premium de 10 Gio pour le volume de démarrage (un par nœud)
- Deux blobs de page Premium de stockage de 140 Gio pour le volume racine (un par nœud)
- Deux disques durs standard de 1024 Gio pour les coûts économiques (un par nœud)
- Deux disques SSD Premium de 512 Gio pour la NVRAM (un par nœud)
- Un snapshot Azure pour chaque disque d'initialisation et disque racine
- Par défaut, chaque disque dans Azure est chiffré au repos.

Paires HAUTE DISPONIBILITÉ dans plusieurs zones de disponibilité

- Deux disques SSD Premium de 10 Gio pour le volume de démarrage (un par nœud)

- Deux blobs de page Premium de stockage de 512 Gio pour le volume racine (un par nœud)
- Deux disques durs standard de 1024 Gio pour les cœurs économiques (un par nœud)
- Deux disques SSD Premium de 512 Gio pour la NVRAM (un par nœud)
- Un snapshot Azure pour chaque disque d'initialisation et disque racine
- Par défaut, chaque disque dans Azure est chiffré au repos.

Google Cloud (nœud unique)

- Un disque persistant SSD de 10 Gio pour les données de démarrage
- Un disque persistant SSD de 64 Gio pour les données racines
- Un disque persistant SSD de 500 Gio pour la NVRAM
- Un disque persistant standard de 315 Gio pour économiser les cœurs
- Snapshots pour les données de démarrage et racines
- Les disques de démarrage et racine sont chiffrés par défaut.

Google Cloud (paire HA)

- Deux disques persistants SSD de 10 Gio pour les données de démarrage
- Quatre disques persistants SSD de 64 Gio pour les données racines
- Deux disques persistants SSD de 500 Gio pour la NVRAM
- Deux disques persistants standard de 315 Gio pour économiser les cœurs
- Un disque persistant standard de 10 Gio pour les données médiateurs
- Un disque persistant standard de 10 Gio pour les données de démarrage médiateur
- Snapshots pour les données de démarrage et racines
- Les disques de démarrage et racine sont chiffrés par défaut.

Où résident les disques

BlueXP dispose du stockage comme suit :

- Les données de démarrage résident sur un disque relié à l'instance ou à la machine virtuelle.
Ce disque, qui contient l'image d'amorçage, n'est pas disponible pour Cloud Volumes ONTAP.
- Les données root, qui contiennent la configuration du système et les journaux, résident dans aggr0.
- Le volume racine de la machine virtuelle de stockage (SVM) réside dans aggr1.
- Les volumes de données résident également dans aggr1.

Connaissances et support

S'inscrire pour obtenir de l'aide

Avant d'ouvrir un dossier de demande de support auprès du support technique NetApp, vous devez ajouter un compte sur le site du support NetApp (NSS) à BlueXP, puis vous inscrire pour obtenir du support.

Présentation de l'inscription au support

Il existe deux types d'inscription pour activer les droits d'assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxx se trouve sur la page des ressources de support de BlueXP).

Il sert d'ID d'abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L'enregistrement des deux types de numéros de série offre des fonctionnalités telles que l'ouverture de tickets de support et la génération automatique de tickets.

La façon dont vous vous inscrivez dépend de votre présence ou de votre présence chez un client ou un partenaire nouveau ou existant.

- Client ou partenaire existant

En tant que client ou partenaire NetApp, vous pouvez utiliser votre compte SSO du site de support NetApp pour effectuer les enregistrements suivants. Dans le tableau de bord support, BlueXP fournit une page **NSS Management** où vous pouvez ajouter votre compte NSS. Une fois votre compte NSS ajouté, BlueXP enregistre automatiquement ces numéros de série pour vous.

[Découvrez comment ajouter votre compte NSS.](#)

- Nouveaux partenaires NetApp

Si vous êtes nouveau chez NetApp, vous devez enregistrer votre numéro de série BlueXP sur le site d'inscription du support NetApp. Une fois que vous avez terminé cette inscription et créé un nouveau compte NSS, vous pouvez utiliser ce compte dans BlueXP pour vous inscrire automatiquement à l'avenir.

[Découvrez comment vous inscrire auprès de NetApp.](#)

Ajouter un compte NSS à BlueXP

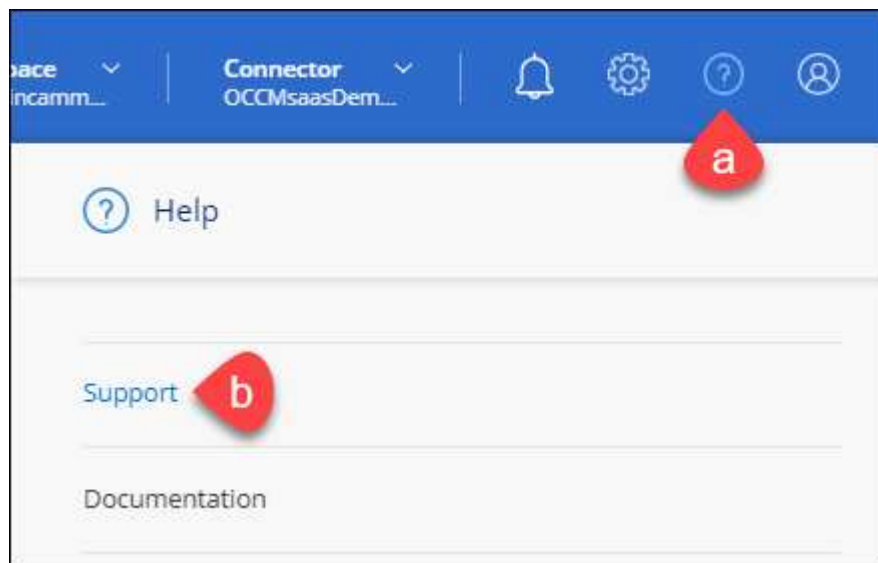
Le tableau de bord du support vous permet d'ajouter et de gérer vos comptes du site de support NetApp pour BlueXP.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.

- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

Notez ce qui suit :

- Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS. Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du **...** menu.
- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le **...** menu. Cette option vous invite à vous reconnecter.

Inscrivez-vous auprès de NetApp

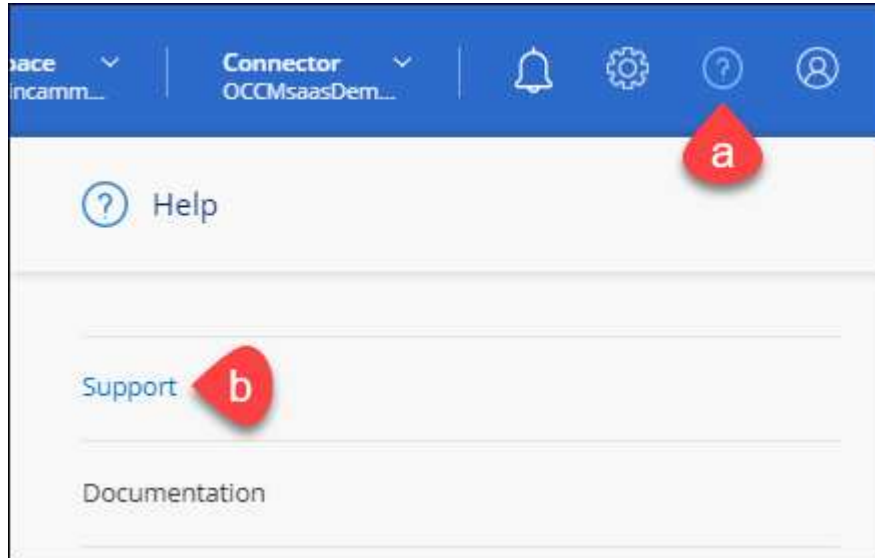
Le fait de vous inscrire au support NetApp dépend de la présence ou non d'un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

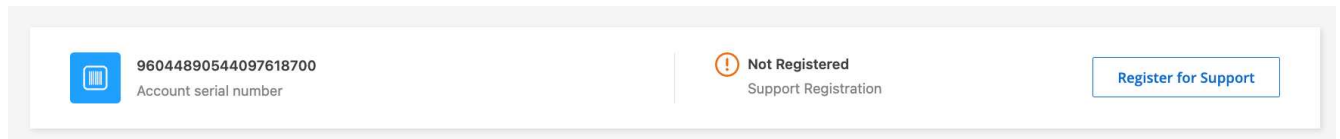
Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Si ce n'est déjà fait, ajoutez votre compte NSS à BlueXP.
3. Sur la page **Ressources**, cliquez sur **s'inscrire au support**.



Client existant mais aucun compte NSS

Si vous êtes déjà client NetApp avec des licences et des numéros de série existants mais que *no* NSS, il vous suffit de créer un compte NSS.

Étapes

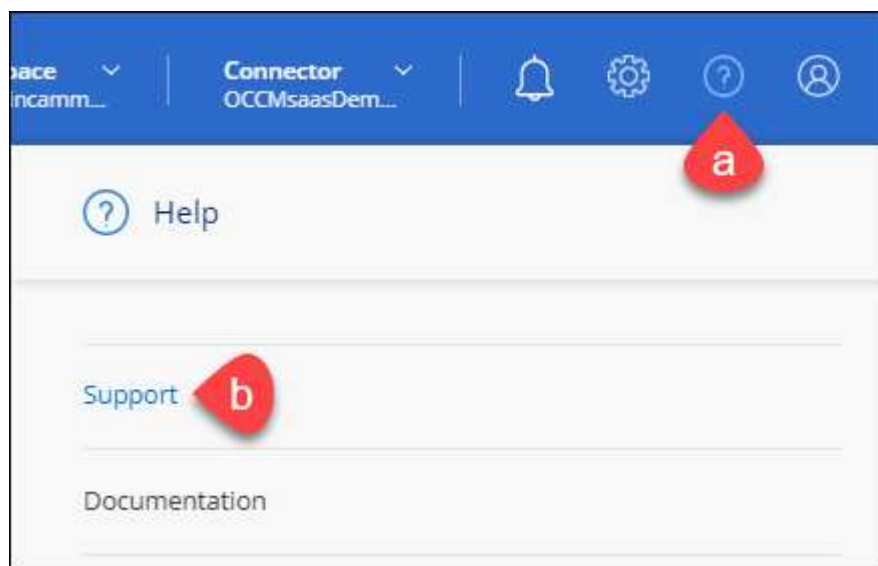
1. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

Découvrez la toute nouvelle gamme NetApp

Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "[Site d'inscription au support NetApp](#)" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

Une fois que vous avez terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois votre compte sur le site de support NetApp, vous pouvez accéder à BlueXP et ajouter ce compte NSS pour les inscriptions futures.

Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

Auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- ["Base de connaissances"](#)

Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

- Documentation

La documentation BlueXP que vous consultez actuellement.

- Courrier électronique : ng-cloudmanager-feedback@netapp.com[E-mail de commentaires]

Nous accordons une grande importance à vos commentaires. Envoyez vos commentaires pour nous aider à améliorer BlueXP.

Support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Avant de commencer

Pour utiliser la fonction **Créer un cas**, vous devez d'abord effectuer un enregistrement unique de votre numéro de série d'ID de compte BlueXP (par exemple 960xxxx) avec NetApp. ["Découvrez comment vous inscrire à de l'aide"](#).

Étapes

1. Dans BlueXP, cliquez sur **aide > support**.
2. Choisissez l'une des options disponibles sous support technique :
 - a. Cliquez sur **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.
 - b. Cliquez sur **Créer un dossier** pour ouvrir un dossier auprès des spécialistes du support NetApp :
 - **Compte sur le site de support NetApp** : sélectionnez le compte NSS applicable associé à la personne qui ouvre le dossier de support. Cette personne sera le contact principal avec NetApp en plus de l'e-mail ci-dessous.

Si vous ne voyez pas votre compte NSS, vous pouvez accéder à l'onglet **NSS Management** de la section support de BlueXP pour l'ajouter.

- **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
- **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.

La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.

Create a Case

TESTCLOUD2NTAP 

NetApp Support Site Account

Service

Cloud Manager 

Working Environment

Select... 

Case Priority 

Low- General Guidance 

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour consulter l'historique de vos dossiers d'assistance, vous pouvez cliquer sur **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton à l'extrême droite vous permet de développer l'action pour voir les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

« Vous n'êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la

même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez consulter votre liste de comptes NSS en haut du formulaire **Créer un dossier** pour trouver la correspondance appropriée, ou vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à <https://mysupport.netapp.com/site/help>

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

<http://www.netapp.com/us/legal/copyright.aspx>

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/us/media/patents-page.pdf>

Politique de confidentialité

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- ["Note pour BlueXP"](#)
- ["Avis du médiateur de Cloud Volumes ONTAP"](#)
- ["Notification relative à ONTAP"](#)

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.