



# Documentation de Cloud Volumes ONTAP

## Cloud Volumes ONTAP

NetApp  
October 06, 2025

# Sommaire

- Documentation de Cloud Volumes ONTAP ..... 1
- Notes de version ..... 2
  - Quoi de neuf dans Cloud Volumes ONTAP ..... 2
    - 6 octobre 2025 ..... 2
    - 4 septembre 2025 ..... 2
    - 11 août 2025 ..... 2
    - 14 juillet 2025 ..... 3
    - 25 juin 2025 ..... 3
    - 29 mai 2025 ..... 3
    - 12 mai 2025 ..... 4
    - 16 avril 2025 ..... 4
    - 14 avril 2025 ..... 4
    - 3 avril 2025 ..... 4
    - 28 mars 2025 ..... 5
    - 12 mars 2025 ..... 5
    - 10 mars 2025 ..... 5
    - 6 mars 2025 ..... 5
    - 03 mars 2025 ..... 6
    - 18 février 2025 ..... 6
    - 10 février 2025 ..... 6
    - 9 décembre 2024 ..... 7
    - 11 novembre 2024 ..... 7
    - 25 octobre 2024 ..... 8
    - 7 octobre 2024 ..... 9
    - 9 septembre 2024 ..... 9
    - 23 août 2024 ..... 9
    - 22 août 2024 ..... 9
    - 8 août 2024 ..... 10
    - 10 juin 2024 ..... 10
    - 17 mai 2024 ..... 10
    - 23 avril 2024 ..... 11
    - 8 mars 2024 ..... 11
    - 5 mars 2024 ..... 11
    - 2 février 2024 ..... 12
    - 16 janvier 2024 ..... 12
    - 8 janvier 2024 ..... 12
    - 6 décembre 2023 ..... 12
    - 5 décembre 2023 ..... 13
    - 10 novembre 2023 ..... 13
    - 8 novembre 2023 ..... 13
    - 1er novembre 2023 ..... 14
    - 23 octobre 2023 ..... 14
    - 6 octobre 2023 ..... 14

10 septembre 2023	15
30 juillet 2023	15
26 juillet 2023	16
2 juillet 2023	16
26 juin 2023	16
4 juin 2023	16
7 mai 2023	17
4 avril 2023	17
3 avril 2023	18
13 mars 2023	20
5 mars 2023	20
5 février 2023	21
1er janvier 2023	22
15 décembre 2022	22
8 décembre 2022	22
4 décembre 2022	23
15 novembre 2022	23
6 novembre 2022	23
18 septembre 2022	24
31 juillet 2022	25
18 juillet 2022	26
3 juillet 2022	26
7 juin 2022	27
2 mai 2022	29
3 avril 2022	31
27 février 2022	31
9 février 2022	31
6 février 2022	32
30 janvier 2022	32
2 janvier 2022	32
28 novembre 2021	34
4 octobre 2021	35
2 septembre 2021	35
7 juillet 2021	36
30 mai 2021	39
24 mai 2021	40
11 avril 2021	40
8 mars 2021	40
4 janv. 2021	41
3 novembre 2020	43
Limitations connues	43
La console ne prend pas en charge la création de volumes FlexGroup	43
La console ne prend pas en charge S3 avec Cloud Volumes ONTAP	43
La console ne prend pas en charge la reprise après sinistre pour les machines virtuelles de stockage	43
Notes de version de Cloud Volumes ONTAP	44

Commencer	45
En savoir plus sur Cloud Volumes ONTAP	45
Versions ONTAP prises en charge pour les déploiements Cloud Volumes ONTAP	46
AWS	46
Azuré	47
Google Cloud	48
Démarrer avec Amazon Web Services	49
Démarrage rapide de Cloud Volumes ONTAP dans AWS	49
Planifiez votre configuration Cloud Volumes ONTAP dans AWS	50
Configurez votre réseau	54
Configurer Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans AWS	79
Configurer les rôles AWS IAM pour les nœuds Cloud Volumes ONTAP	83
Configurer les licences pour Cloud Volumes ONTAP dans AWS	92
Déployer Cloud Volumes ONTAP dans AWS à l'aide d'un déploiement rapide	100
Lancer Cloud Volumes ONTAP dans AWS	104
Déployer Cloud Volumes ONTAP dans AWS Secret Cloud ou AWS Top Secret Cloud	118
Démarrer avec Microsoft Azure	134
Découvrez les options de déploiement de Cloud Volumes ONTAP dans Azure	134
Démarrer dans la console NetApp	136
Déployer Cloud Volumes ONTAP depuis la place de marché Azure	188
Démarrer avec Google Cloud	192
Démarrage rapide de Cloud Volumes ONTAP dans Google Cloud	192
Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud	194
Configurer la mise en réseau Google Cloud pour Cloud Volumes ONTAP	197
Configurer VPC Service Controls pour déployer Cloud Volumes ONTAP dans Google Cloud	209
Créer un compte de service Google Cloud pour Cloud Volumes ONTAP	211
Utilisation de clés de chiffrement gérées par le client avec Cloud Volumes ONTAP	214
Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud	215
Lancer Cloud Volumes ONTAP dans Google Cloud	220
Vérification d'image de Google Cloud Platform	233
Utiliser Cloud Volumes ONTAP	245
Gestion des licences	245
Gérer les licences basées sur la capacité pour Cloud Volumes ONTAP	245
Gérer les abonnements Keystone pour Cloud Volumes ONTAP via la console NetApp	250
Gérer les licences basées sur les nœuds pour Cloud Volumes ONTAP	254
Administration des volumes et des LUN	259
Créer un FlexVol volume sur un système Cloud Volumes ONTAP	259
Gérer les volumes sur les systèmes Cloud Volumes ONTAP	266
Hiérarchisez les données Cloud Volumes ONTAP inactives vers un stockage d'objets à faible coût	275
Connectez-vous à un LUN sur Cloud Volumes ONTAP depuis votre système hôte	284
Accélérez l'accès aux données avec les volumes FlexCache sur un système Cloud Volumes ONTAP	284
Administration globale	286
Créer un agrégat pour les systèmes Cloud Volumes ONTAP	286
Gérer les agrégats pour les clusters Cloud Volumes ONTAP	288
Gérer la capacité globale de Cloud Volumes ONTAP sur un agent de console	289

Administration des machines virtuelles de stockage .....	291
Gérer les machines virtuelles de stockage pour Cloud Volumes ONTAP .....	291
Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans AWS .....	293
Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans Azure .....	300
Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans Google Cloud .....	303
Configurer la reprise après sinistre des machines virtuelles de stockage pour Cloud Volumes ONTAP .....	306
Sécurité et cryptage des données .....	307
Chiffrer les volumes sur Cloud Volumes ONTAP avec les solutions de chiffrement NetApp .....	307
Gérer les clés de chiffrement Cloud Volumes ONTAP avec AWS Key Management Service .....	307
Gérer les clés de chiffrement Cloud Volumes ONTAP avec Azure Key Vault .....	308
Gérer les clés de chiffrement Cloud Volumes ONTAP avec Google Cloud KMS .....	316
Activer les solutions de protection contre les ransomwares NetApp pour Cloud Volumes ONTAP .....	318
Créer des copies instantanées inviolables des fichiers WORM sur Cloud Volumes ONTAP .....	321
Administration du système .....	322
Mettre à niveau le logiciel Cloud Volumes ONTAP .....	322
Enregistrer les systèmes de paiement à l'utilisation Cloud Volumes ONTAP .....	331
Convertir une licence basée sur un nœud Cloud Volumes ONTAP en une licence basée sur la capacité .....	333
Démarrer et arrêter un système Cloud Volumes ONTAP .....	335
Synchroniser l'heure du système Cloud Volumes ONTAP à l'aide du serveur NTP .....	338
Modifier la vitesse d'écriture du système .....	338
Modifier le mot de passe administrateur du cluster Cloud Volumes ONTAP .....	339
Ajouter, supprimer ou supprimer des systèmes .....	340
Administration AWS .....	342
Administration Azure .....	345
Administration de Google Cloud .....	357
Administrer Cloud Volumes ONTAP à l'aide de System Manager .....	358
Administrer Cloud Volumes ONTAP depuis la CLI .....	361
Santé et événements du système .....	362
Vérifier la configuration AutoSupport pour Cloud Volumes ONTAP .....	362
Configurer EMS pour les systèmes Cloud Volumes ONTAP .....	366
Concepts .....	367
Licences .....	367
Licences pour Cloud Volumes ONTAP .....	367
En savoir plus sur les licences basées sur la capacité pour Cloud Volumes ONTAP .....	371
Stockage .....	376
Protocoles clients pris en charge pour Cloud Volumes ONTAP .....	376
Disques et agrégats utilisés pour les clusters Cloud Volumes ONTAP .....	376
En savoir plus sur la prise en charge d'AWS Elastic Volumes avec Cloud Volumes ONTAP .....	379
En savoir plus sur la hiérarchisation des données avec Cloud Volumes ONTAP dans AWS, Azure ou Google Cloud .....	385
Gestion du stockage Cloud Volumes ONTAP .....	390
Vitesse d'écriture .....	393
Cache Flash .....	396

En savoir plus sur le stockage WORM sur Cloud Volumes ONTAP .....	396
Paires à haute disponibilité .....	399
En savoir plus sur les paires Cloud Volumes ONTAP HA dans AWS .....	399
En savoir plus sur les paires Cloud Volumes ONTAP HA dans Azure .....	406
En savoir plus sur les paires Cloud Volumes ONTAP HA dans Google Cloud .....	412
Opérations indisponibles lorsqu'un nœud de la paire Cloud Volumes ONTAP HA est hors ligne .....	417
En savoir plus sur le cryptage des données et la protection contre les ransomwares de Cloud Volumes ONTAP .....	418
Chiffrement des données au repos .....	418
Analyse antivirus ONTAP .....	420
Protection contre les ransomwares .....	420
En savoir plus sur la surveillance des performances des charges de travail Cloud Volumes ONTAP .....	421
Rapports techniques de performance .....	421
performances du processeur .....	421
Gestion des licences pour BYOL basé sur les nœuds .....	422
Licences système BYOL .....	422
Gestion des licences pour un nouveau système .....	422
Expiration de la licence .....	422
Renouvellement de licence .....	423
Transfert de licence vers un nouveau système .....	423
Découvrez comment AutoSupport et Digital Advisor sont utilisés pour Cloud Volumes ONTAP .....	423
Configurations par défaut prises en charge pour Cloud Volumes ONTAP .....	424
Configuration par défaut .....	424
Disques internes pour les données système .....	426
Connaissances et soutien .....	430
Inscrivez-vous pour obtenir de l'aide .....	430
Présentation de l'enregistrement de l'assistance .....	430
Enregistrez BlueXP pour le support NetApp .....	430
Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP .....	433
Obtenir de l'aide .....	434
Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud .....	434
Utiliser les options d'auto-assistance .....	435
Créer un dossier auprès du support NetApp .....	435
Gérez vos demandes d'assistance (Aperçu) .....	437
Mentions légales .....	440
Copyright .....	440
Marques de commerce .....	440
Brevets .....	440
Politique de confidentialité .....	440
Open source .....	440

# Documentation de Cloud Volumes ONTAP

# Notes de version

## Quoi de neuf dans Cloud Volumes ONTAP

Découvrez les nouveautés de la gestion Cloud Volumes ONTAP dans la console NetApp .

Les améliorations décrites sur cette page sont spécifiques à la gestion de Cloud Volumes ONTAP via la console. Pour découvrir les nouveautés du logiciel Cloud Volumes ONTAP lui-même, "[Accédez aux notes de publication de Cloud Volumes ONTAP](#)" .

### 6 octobre 2025

#### BlueXP est désormais NetApp Console

La console NetApp , construite sur la base BlueXP améliorée et restructurée, fournit une gestion centralisée du stockage NetApp et des services de données NetApp dans les environnements sur site et cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée, hautement sécurisée et conforme.

Pour plus de détails sur ce qui a changé, consultez le "[Notes de version de la console NetApp](#)" .

#### Déploiement simplifié de Cloud Volumes ONTAP dans AWS

Vous pouvez désormais déployer Cloud Volumes ONTAP dans AWS à l'aide d'une méthode de déploiement rapide pour les configurations à nœud unique et à haute disponibilité (HA). Ce processus simplifié réduit le nombre d'étapes par rapport à la méthode avancée, définit automatiquement les valeurs par défaut sur une seule page et minimise la navigation, rendant le déploiement plus rapide et plus facile.

Pour plus d'informations, consultez "[Déployer Cloud Volumes ONTAP dans AWS à l'aide d'un déploiement rapide](#)" .

### 4 septembre 2025

#### Cloud Volumes ONTAP 9.17.1 RC

Vous pouvez désormais utiliser BlueXP pour déployer et gérer la version Release Candidate 1 de Cloud Volumes ONTAP 9.17.1 dans Azure et Google Cloud. Cependant, cette version n'est pas disponible pour le déploiement et la mise à niveau dans AWS.

"[En savoir plus sur cette version de Cloud Volumes ONTAP](#)" .

### 11 août 2025

#### Fin de disponibilité des licences optimisées

À compter du 11 août 2025, la licence Cloud Volumes ONTAP Optimized sera obsolète et ne sera plus disponible à l'achat ou au renouvellement sur les places de marché Azure et Google Cloud pour les abonnements à la carte (PAYGO). Si vous disposez d'un contrat annuel existant avec une licence optimisée, vous pouvez continuer à utiliser la licence jusqu'à la fin de votre contrat. Lorsque votre licence optimisée expire, vous pouvez opter pour les licences Cloud Volumes ONTAP Essentials ou Professional dans BlueXP.

Cependant, la possibilité d'ajouter ou de renouveler des licences optimisées sera disponible via les API.

Pour plus d'informations sur les packages de licence, reportez-vous à ["Licences pour Cloud Volumes ONTAP"](#)

Pour plus d'informations sur le passage à une autre méthode de charge, reportez-vous à ["Gérer les licences basées sur la capacité"](#) .

## 14 juillet 2025

### Prise en charge du proxy transparent

BlueXP prend désormais en charge les serveurs proxy transparents en plus des connexions proxy explicites existantes. Lors de la création ou de la modification du connecteur BlueXP , vous pouvez configurer un serveur proxy transparent pour gérer en toute sécurité le trafic réseau vers et depuis Cloud Volumes ONTAP.

Pour plus d'informations sur l'utilisation des serveurs proxy dans Cloud Volumes ONTAP, reportez-vous à :

- ["Configurations réseau pour prendre en charge le proxy Connector dans AWS"](#)
- ["Configurations réseau pour prendre en charge le proxy Connector dans Azure"](#)
- ["Configurations réseau pour prendre en charge le proxy Connector dans Google Cloud"](#)

### Nouveau type de machine virtuelle pris en charge pour Cloud Volumes ONTAP dans Azure

À partir de Cloud Volumes ONTAP 9.13.1, L8s\_v3 est pris en charge en tant que type de machine virtuelle dans les zones de disponibilité uniques et multiples Azure, pour les déploiements de paires haute disponibilité (HA) nouveaux et existants.

Pour plus d'informations, reportez-vous à ["Configurations prises en charge dans Azure"](#) .

## 25 juin 2025

### Disponibilité restreinte des licences BYOL pour Cloud Volumes ONTAP

À compter du 25 juin 2025, NetApp a restreint le modèle de licence BYOL (Bring Your Own License) pour Cloud Volumes ONTAP. Cette restriction s'applique à tous les clients et déploiements Cloud Volumes ONTAP sur AWS, Azure et Google Cloud. Les seules exceptions concernent les clients du secteur public américain et les déploiements en Chine.

Le support et les services NetApp seront maintenus jusqu'à l'expiration de votre contrat BYOL, mais vos licences expirées ne seront ni renouvelées ni prolongées. À l'expiration de vos licences BYOL, vous devrez les remplacer par des licences basées sur la capacité, achetées via vos abonnements à la place de marché cloud. Un modèle de licence basé sur la capacité, via les places de marché hyperscale, simplifie l'expérience de licence et offre de meilleurs avantages commerciaux. Contactez votre équipe de comptes NetApp ou vos représentants du service client pour discuter des options de conversion.

Pour plus d'informations, reportez-vous à ce communiqué client : ["CPC-00661 : Modifications de la politique BYOL de Cloud Volumes ONTAP"](#) .

## 29 mai 2025

## Déploiements en mode privé activés pour Cloud Volumes ONTAP 9.15.1

Vous pouvez désormais déployer Cloud Volumes ONTAP 9.15.1 en mode privé dans AWS, Azure et Google Cloud. Le mode privé est activé pour les déploiements à nœud unique et à haute disponibilité (HA) de Cloud Volumes ONTAP 9.15.1.

Pour plus d'informations sur les déploiements en mode privé, reportez-vous à <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode>["En savoir plus sur les modes de déploiement de BlueXP"].

## 12 mai 2025

### Découverte des déploiements réalisés via la marketplace Azure dans BlueXP

BlueXP a désormais la capacité de découvrir les systèmes Cloud Volumes ONTAP déployés directement via la place de marché Azure. Cela signifie que vous pouvez désormais ajouter et gérer ces systèmes en tant qu'environnements de travail dans BlueXP, comme tout autre système Cloud Volumes ONTAP .

["Déployer Cloud Volumes ONTAP depuis la place de marché Azure"](#)

## 16 avril 2025

### Nouvelles régions prises en charge dans Azure

Vous pouvez désormais déployer Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures dans des zones de disponibilité uniques et multiples dans Azure dans les régions suivantes. Cela inclut la prise en charge des déploiements à nœud unique et à haute disponibilité (HA).

- Espagne centrale
- Mexique central

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

## 14 avril 2025

### Création de machines virtuelles de stockage automatisée via les API de Google Cloud

Vous pouvez désormais utiliser les API BlueXP pour automatiser la création de machines virtuelles de stockage dans Google Cloud. Vous avez utilisé cette fonctionnalité dans les configurations haute disponibilité (HA) de Cloud Volumes ONTAP et vous pouvez désormais également l'utiliser dans les déploiements à nœud unique. En utilisant les API BlueXP , vous pouvez facilement créer, renommer et supprimer des machines virtuelles de stockage de données supplémentaires dans votre environnement Google Cloud, sans avoir à configurer manuellement les interfaces réseau, les LIF et les LIF de gestion requis. Cette automatisation simplifie le processus de gestion des machines virtuelles de stockage.

["Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans Google Cloud"](#)

## 3 avril 2025

### Prise en charge des régions chinoises pour Cloud Volumes ONTAP 9.13.1 dans AWS

Vous pouvez désormais déployer Cloud Volumes ONTAP 9.13.1 dans AWS dans les régions chinoises. Cela inclut la prise en charge des déploiements à nœud unique et à haute disponibilité (HA). Seules les licences

achetées directement auprès de NetApp sont prises en charge.

Pour connaître la disponibilité régionale, reportez-vous à la ["Cartes des régions mondiales pour Cloud Volumes ONTAP"](#) .

## 28 mars 2025

### Déploiements en mode privé activés pour Cloud Volumes ONTAP 9.14.1

Vous pouvez désormais déployer Cloud Volumes ONTAP 9.14.1 en mode privé dans AWS, Azure et Google Cloud. Le mode privé est activé pour les déploiements à nœud unique et à haute disponibilité (HA) de Cloud Volumes ONTAP 9.14.1.

Pour plus d'informations sur les déploiements en mode privé, reportez-vous à <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode>["En savoir plus sur les modes de déploiement de BlueXP"^] .

## 12 mars 2025

### Nouvelles régions prises en charge pour les déploiements de zones de disponibilité multiples dans Azure

Les régions suivantes prennent désormais en charge les déploiements de zones de disponibilité multiples HA dans Azure pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures :

- Centre des États-Unis
- Gouverneur des États-Unis de Virginie (Région gouvernementale des États-Unis - Virginie)

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

## 10 mars 2025

### Création de machines virtuelles de stockage automatisée via les API dans Azure

Vous pouvez désormais utiliser les API BlueXP pour créer, renommer et supprimer des machines virtuelles de stockage de données supplémentaires pour Cloud Volumes ONTAP dans Azure. L'utilisation des API automatise le processus de création de machines virtuelles de stockage, y compris la configuration des interfaces réseau requises, des LIF et d'une LIF de gestion, si vous devez utiliser une machine virtuelle de stockage à des fins de gestion.

["Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans Azure"](#)

## 6 mars 2025

### Cloud Volumes ONTAP 9.16.1 GA

Vous pouvez désormais utiliser BlueXP pour déployer et gérer la version de disponibilité générale de Cloud Volumes ONTAP 9.16.1 dans Azure et Google Cloud. Cependant, cette version n'est pas disponible pour le déploiement et la mise à niveau dans AWS.

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

**03 mars 2025**

### **Prise en charge de la région Nouvelle-Zélande Nord dans Azure**

La région Nouvelle-Zélande Nord est désormais prise en charge dans Azure pour les configurations à nœud unique et à haute disponibilité (HA) de Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures. Notez que le type d'instance Lsv3 n'est pas pris en charge dans cette région.

Pour une liste de toutes les régions prises en charge, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

**18 février 2025**

### **Présentation du déploiement direct sur la place de marché Azure**

Vous pouvez désormais profiter du déploiement direct de la place de marché Azure pour déployer facilement et rapidement Cloud Volumes ONTAP directement depuis la place de marché Azure. Grâce à cette méthode simplifiée, vous pouvez explorer les principales fonctionnalités et capacités de Cloud Volumes ONTAP dans votre environnement sans avoir à configurer le connecteur BlueXP ou à répondre à d'autres critères d'intégration requis pour le déploiement de Cloud Volumes ONTAP via BlueXP.

- ["Découvrez les options de déploiement de Cloud Volumes ONTAP dans Azure"](#)
- ["Déployer Cloud Volumes ONTAP depuis la place de marché Azure"](#)

**10 février 2025**

### **Authentification utilisateur activée pour accéder au Gestionnaire système depuis BlueXP**

En tant qu'administrateur BlueXP , vous pouvez désormais activer l'authentification pour les utilisateurs ONTAP accédant à ONTAP System Manager depuis BlueXP. Vous pouvez activer cette option en modifiant les paramètres du connecteur BlueXP . Cette option est disponible pour les modes standard et privé.

["Administrer Cloud Volumes ONTAP à l'aide de System Manager"](#) .

### **BlueXP Advanced View renommé en Gestionnaire système**

L'option de gestion avancée de Cloud Volumes ONTAP depuis BlueXP via ONTAP System Manager a été renommée de **Vue avancée** à **Gestionnaire système**.

["Administrer Cloud Volumes ONTAP à l'aide de System Manager"](#) .

### **Présentation d'un moyen plus simple de gérer les licences avec le BlueXP digital wallet**

Vous pouvez désormais bénéficier d'une gestion simplifiée des licences Cloud Volumes ONTAP en utilisant des points de navigation améliorés au sein du BlueXP digital wallet:

- Accédez facilement aux informations de votre licence Cloud Volumes ONTAP via les onglets **Administration > Licences et abonnements > Présentation/Licences directes**.
- Cliquez sur **Afficher** dans le panneau Cloud Volume ONTAP dans l'onglet **Présentation** pour obtenir une compréhension complète de vos licences basées sur la capacité. Cette vue avancée offre un aperçu détaillé de vos licences et abonnements.
- Si vous préférez l'interface précédente, vous pouvez cliquer sur le bouton **Passer à la vue héritée** pour afficher les détails de la licence par type et modifier les méthodes de facturation de vos licences.

["Gérer les licences basées sur la capacité"](#) .

## 9 décembre 2024

### Liste des machines virtuelles prises en charge mise à jour pour Azure afin de s'aligner sur les meilleures pratiques

Les familles de machines DS\_v2 et Es\_v3 ne sont plus disponibles pour la sélection sur BlueXP lors du déploiement de nouvelles instances de Cloud Volumes ONTAP dans Azure. Ces familles seront conservées et soutenues uniquement dans les systèmes plus anciens et existants. Les nouveaux déploiements de Cloud Volumes ONTAP sont pris en charge dans Azure uniquement à partir de la version 9.12.1. Nous vous recommandons de passer à Es\_v4 ou à toute autre série compatible avec Cloud Volumes ONTAP 9.12.1 et versions ultérieures. Les machines des séries DS\_v2 et Es\_v3 seront toutefois disponibles pour les nouveaux déploiements effectués via l'API.

["Configurations prises en charge dans Azure"](#)

## 11 novembre 2024

### Fin de disponibilité des licences basées sur des nœuds

NetApp a planifié la fin de la disponibilité (EOA) et la fin du support (EOS) des licences basées sur les nœuds Cloud Volumes ONTAP . À compter du 11 novembre 2024, la disponibilité limitée des licences basées sur des nœuds a pris fin. Le support des licences basées sur les nœuds prend fin le 31 décembre 2024. Après l'EOA de vos licences basées sur les nœuds, vous devez passer à des licences basées sur la capacité en utilisant l'outil de conversion de licence BlueXP .

Pour les engagements annuels ou à plus long terme, NetApp vous recommande de contacter votre représentant NetApp avant la date EOA ou la date d'expiration de la licence pour vous assurer que les conditions préalables à la transition sont en place. Si vous ne disposez pas d'un contrat à long terme pour un nœud Cloud Volumes ONTAP et que vous exécutez votre système avec un abonnement à la demande (PAYGO), il est important de planifier votre conversion avant la date EOS. Pour les contrats à long terme et les abonnements PAYGO, vous pouvez utiliser l'outil de conversion de licence BlueXP pour une conversion transparente.

["Fin de disponibilité des licences basées sur des nœuds"](#) ["Convertir une licence basée sur un nœud Cloud Volumes ONTAP en une licence basée sur la capacité"](#)

### Suppression des déploiements basés sur des nœuds de BlueXP

L'option permettant de déployer des systèmes Cloud Volumes ONTAP à l'aide de licences basées sur des nœuds est obsolète sur BlueXP. À l'exception de quelques cas particuliers, vous ne pouvez pas utiliser de licences basées sur des nœuds pour les déploiements Cloud Volumes ONTAP pour n'importe quel fournisseur de cloud.

NetApp reconnaît les exigences de licence uniques suivantes conformément aux obligations contractuelles et aux besoins opérationnels, et continuera à prendre en charge les licences basées sur les nœuds dans ces situations :

- Clients du secteur public américain
- Déploiements en mode privé
- Déploiements de Cloud Volumes ONTAP dans AWS en Chine

- Si vous disposez d'une licence BYOL valide et non expirée

["Fin de disponibilité des licences basées sur des nœuds"](#)

## **Ajout d'un niveau froid pour les données Cloud Volumes ONTAP sur le stockage Azure Blob**

BlueXP vous permet désormais de sélectionner un niveau froid pour stocker les données de niveau de capacité inactives sur le stockage Azure Blob. L'ajout du niveau froid aux niveaux chaud et froid existants vous offre une option de stockage plus abordable et une meilleure rentabilité.

["Hiérarchisation des données dans Azure"](#)

## **Option permettant de restreindre l'accès public au compte de stockage pour Azure**

Vous avez désormais la possibilité de restreindre l'accès public à votre compte de stockage pour les systèmes Cloud Volumes ONTAP dans Azure. En désactivant l'accès, vous pouvez sécuriser votre adresse IP privée contre toute exposition même au sein du même réseau virtuel, s'il est nécessaire de se conformer aux politiques de sécurité de votre organisation. Cette option désactive également la hiérarchisation des données pour vos systèmes Cloud Volumes ONTAP et s'applique aux paires à nœud unique et à haute disponibilité.

["Règles du groupe de sécurité"](#) .

## **Activation de WORM après le déploiement de Cloud Volumes ONTAP**

Vous avez désormais la possibilité d'activer le stockage WORM (Write Once, Read Many) sur un système Cloud Volumes ONTAP existant à l'aide de BlueXP. Cette fonctionnalité vous offre la flexibilité d'activer WORM sur un environnement de travail, même si WORM n'a pas été activé sur celui-ci lors de sa création. Une fois activé, vous ne pouvez pas désactiver WORM.

["Activation de WORM sur un environnement de travail Cloud Volumes ONTAP"](#)

## **25 octobre 2024**

### **Liste des machines virtuelles prises en charge mise à jour pour Google Cloud afin de s'aligner sur les meilleures pratiques**

Les machines de la série n1 ne sont plus disponibles pour la sélection sur BlueXP lors du déploiement de nouvelles instances de Cloud Volumes ONTAP dans Google Cloud. Les machines de la série n1 seront conservées et prises en charge uniquement dans les systèmes plus anciens et existants. Les nouveaux déploiements de Cloud Volumes ONTAP sont pris en charge dans Google Cloud uniquement à partir de la version 9.8. Nous vous recommandons de passer aux types de machines de la série n2 compatibles avec Cloud Volumes ONTAP 9.8 et versions ultérieures. Les machines de la série n1 seront toutefois disponibles pour de nouveaux déploiements effectués via l'API.

["Configurations prises en charge dans Google Cloud"](#) .

### **Prise en charge des zones locales pour Amazon Web Services en mode privé**

BlueXP prend désormais en charge les zones locales AWS pour les déploiements haute disponibilité (HA) Cloud Volumes ONTAP en mode privé. Le support qui était auparavant limité au mode standard uniquement a désormais été étendu pour inclure le mode privé.



Les zones locales AWS ne sont pas prises en charge lors de l'utilisation de BlueXP en mode restreint.

Pour plus d'informations sur les zones locales AWS avec déploiements HA, reportez-vous à "[Zones locales AWS](#)".

## 7 octobre 2024

### Expérience utilisateur améliorée dans la sélection de la version pour la mise à niveau

À partir de cette version, lorsque vous essayez de mettre à niveau Cloud Volumes ONTAP à l'aide de la notification BlueXP, vous recevrez des conseils sur les versions par défaut, les plus récentes et compatibles à utiliser. Vous pouvez également désormais sélectionner le dernier correctif ou la version majeure compatible avec votre instance Cloud Volumes ONTAP, ou saisir manuellement une version à mettre à niveau.

["Mettre à niveau le logiciel Cloud Volumes ONTAP"](#)

## 9 septembre 2024

### Les fonctionnalités WORM et ARP ne sont plus payantes

Les fonctionnalités intégrées de protection des données et de sécurité de WORM (Write Once Read Many) et ARP (Autonomous Ransomware Protection) seront proposées avec les licences Cloud Volumes ONTAP sans frais supplémentaires. Le nouveau modèle de tarification s'applique aux abonnements BYOL et PAYGO/marketplace nouveaux et existants d'AWS, Azure et Google Cloud. Les licences basées sur la capacité et sur les nœuds contiendront ARP et WORM pour toutes les configurations, y compris les paires à nœud unique et à haute disponibilité (HA), sans frais supplémentaires.

La tarification simplifiée vous apporte les avantages suivants :

- Les comptes qui incluent actuellement WORM et ARP n'entraîneront plus de frais pour ces fonctionnalités. À l'avenir, votre facturation ne comportera que des frais d'utilisation de la capacité, comme c'était le cas avant ce changement. WORM et ARP ne seront plus inclus dans vos futures factures.
- Si vos comptes actuels n'incluent pas ces fonctionnalités, vous pouvez désormais opter pour WORM et ARP sans frais supplémentaires.
- Toutes les offres Cloud Volumes ONTAP pour tous les nouveaux comptes excluront les frais pour WORM et ARP.

En savoir plus sur ces fonctionnalités :

- ["Activer les solutions de protection contre les ransomwares NetApp pour Cloud Volumes ONTAP"](#)
- ["Stockage de l'WORM"](#)

## 23 août 2024

### La région Canada Ouest est désormais prise en charge dans AWS

La région Canada Ouest est désormais prise en charge dans AWS pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

Pour une liste de toutes les régions, voir le "[Carte des régions mondiales sous AWS](#)".

## 22 août 2024

## Cloud Volumes ONTAP 9.15.1 GA

BlueXP peut désormais déployer et gérer la version de disponibilité générale de Cloud Volumes ONTAP 9.15.1 dans AWS, Azure et Google Cloud.

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

## 8 août 2024

### Les packages de licences Edge Cache sont obsolètes

Les packages de licences basés sur la capacité Edge Cache ne seront plus disponibles pour les futurs déploiements de Cloud Volumes ONTAP. Cependant, vous pouvez utiliser l'API pour bénéficier de cette fonctionnalité.

### Prise en charge minimale des versions pour Flash Cache dans Azure

La version minimale de Cloud Volumes ONTAP requise pour la configuration de Flash Cache dans Azure est 9.13.1 GA. Vous ne pouvez utiliser ONTAP 9.13.1 GA et les versions ultérieures pour déployer Flash Cache sur les systèmes Cloud Volumes ONTAP dans Azure.

Pour les configurations prises en charge, voir ["Configurations prises en charge dans Azure"](#) .

### Les essais gratuits pour les abonnements au marché sont obsolètes

La licence d'essai ou d'évaluation gratuite automatique de 30 jours pour les abonnements à la carte sur la place de marché du fournisseur de cloud ne sera plus disponible dans Cloud Volumes ONTAP. La facturation de tout type d'abonnement marketplace (PAYGO ou contrat annuel) sera activée dès la première utilisation, sans aucune période d'essai gratuite.

## 10 juin 2024

### Cloud Volumes ONTAP 9.15.0

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.15.0 dans AWS, Azure et Google Cloud.

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

## 17 mai 2024

### Prise en charge des zones locales d'Amazon Web Services

La prise en charge des zones locales AWS est désormais disponible pour les déploiements Cloud Volumes ONTAP HA. Les zones locales AWS sont un déploiement d'infrastructure où le stockage, le calcul, la base de données et d'autres services AWS sélectionnés sont situés à proximité de grandes villes et de zones industrielles.



Les zones locales AWS sont prises en charge lors de l'utilisation de BlueXP en mode standard. À l'heure actuelle, les zones locales AWS ne sont pas prises en charge lors de l'utilisation de BlueXP en mode restreint ou en mode privé.

Pour plus d'informations sur les zones locales AWS avec déploiements HA, reportez-vous à ["Zones locales AWS"](#) .

## 23 avril 2024

### Nouvelles régions prises en charge pour les déploiements de zones de disponibilité multiples dans Azure

Les régions suivantes prennent désormais en charge les déploiements de zones de disponibilité multiples HA dans Azure pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures :

- Allemagne Centre-Ouest
- Pologne centrale
- Ouest des États-Unis 3
- Israël Central
- Italie du Nord
- Canada Central

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

### La région de Johannesburg est désormais prise en charge dans Google Cloud

La région de Johannesburg(`africa-south1` (région)) est désormais pris en charge dans Google Cloud pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Google Cloud"](#) .

### Les modèles et balises de volume ne sont plus pris en charge

Vous ne pouvez plus créer un volume à partir d'un modèle ni modifier les balises d'un volume. Ces actions étaient associées au service de correction BlueXP , qui n'est plus disponible.

## 8 mars 2024

### Prise en charge du service de métadonnées instantanées Amazon v2

Dans AWS, Cloud Volumes ONTAP, le médiateur et le connecteur prennent désormais en charge Amazon Instant Metadata Service v2 (IMDSv2) pour toutes les fonctions. IMDSv2 offre une protection renforcée contre les vulnérabilités. Seul IMDSv1 était auparavant pris en charge.

Si vos politiques de sécurité l'exigent, vous pouvez configurer vos instances EC2 pour utiliser IMDSv2. Pour les instructions, reportez-vous à ["Documentation de configuration et d'administration BlueXP pour la gestion des connecteurs existants"](#) .

## 5 mars 2024

### Cloud Volumes ONTAP 9.14.1 GA

BlueXP peut désormais déployer et gérer la version de disponibilité générale de Cloud Volumes ONTAP 9.14.1 dans AWS, Azure et Google Cloud.

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

## 2 février 2024

### Prise en charge des machines virtuelles de la série Edv5 dans Azure

Cloud Volumes ONTAP prend désormais en charge les machines virtuelles de la série Edv5 suivantes à partir de la version 9.14.1.

- E4ds\_v5
- E8ds\_v5
- E20s\_v5
- E32ds\_v5
- E48ds\_v5
- E64ds\_v5

["Configurations prises en charge dans Azure"](#)

## 16 janvier 2024

### Versions de correctifs dans BlueXP

Les versions de correctifs sont disponibles dans BlueXP uniquement pour les trois dernières versions de Cloud Volumes ONTAP.

["Mettre à niveau Cloud Volumes ONTAP"](#)

## 8 janvier 2024

### Nouvelles machines virtuelles pour les zones de disponibilité multiples Azure

À partir de Cloud Volumes ONTAP 9.13.1, les types de machines virtuelles suivants prennent en charge plusieurs zones de disponibilité Azure pour les déploiements de paires haute disponibilité nouveaux et existants :

- L16s\_v3
- L32s\_v3
- L48s\_v3
- L64s\_v3

["Configurations prises en charge dans Azure"](#)

## 6 décembre 2023

### Cloud Volumes ONTAP 9.14.1 RC1

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.14.1 dans AWS, Azure et Google Cloud.

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

## Limite maximale de FlexVol volume de 300 TiB

Vous pouvez désormais créer un FlexVol volume jusqu'à la taille maximale de 300 TiB avec System Manager et ONTAP CLI à partir de Cloud Volumes ONTAP 9.12.1 P2 et 9.13.0 P2, et dans BlueXP à partir de Cloud Volumes ONTAP 9.13.1.

- ["Limites de stockage dans AWS"](#)
- ["Limites de stockage dans Azure"](#)
- ["Limites de stockage dans Google Cloud"](#)

## 5 décembre 2023

Les changements suivants ont été introduits.

### Prise en charge de nouvelles régions dans Azure

#### Prise en charge d'une région de zone de disponibilité unique

Les régions suivantes prennent désormais en charge les déploiements de zone de disponibilité unique hautement disponibles dans Azure pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures :

- Tel-Aviv
- Milan

#### Prise en charge de plusieurs régions de zone de disponibilité

Les régions suivantes prennent désormais en charge les déploiements de zones de disponibilité multiples hautement disponibles dans Azure pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures :

- Inde centrale
- Norvège de l'Est
- Suisse du Nord
- Afrique du Sud Nord
- Émirats arabes unis du Nord

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

## 10 novembre 2023

Le changement suivant a été introduit avec la version 3.9.35 du connecteur.

### La région de Berlin est désormais prise en charge dans Google Cloud

La région de Berlin est désormais prise en charge dans Google Cloud pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Google Cloud"](#) .

## 8 novembre 2023

Le changement suivant a été introduit avec la version 3.9.35 du connecteur.

## La région de Tel Aviv est désormais prise en charge dans AWS

La région de Tel Aviv est désormais prise en charge dans AWS pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous AWS"](#) .

## 1er novembre 2023

Le changement suivant a été introduit avec la version 3.9.34 du connecteur.

## La région de l'Arabie saoudite est désormais prise en charge dans Google Cloud

La région Arabie saoudite est désormais prise en charge dans Google Cloud pour Cloud Volumes ONTAP et Connector pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

Pour une liste de toutes les régions, reportez-vous à la ["Carte des régions mondiales sous Google Cloud"](#) .

## 23 octobre 2023

Le changement suivant a été introduit avec la version 3.9.34 du connecteur.

## Nouvelles régions prises en charge pour les déploiements de zones de disponibilité multiples HA dans Azure

Les régions suivantes dans Azure prennent désormais en charge les déploiements de zones de disponibilité multiples hautement disponibles pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures :

- Australie de l'Est
- Asie de l'Est
- France Centre
- Europe du Nord
- Qatar Central
- Suède centrale
- Europe de l'Ouest
- Ouest des États-Unis 2

Pour obtenir la liste de toutes les régions prenant en charge plusieurs zones de disponibilité, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

## 6 octobre 2023

Le changement suivant a été introduit avec la version 3.9.34 du connecteur.

## Cloud Volumes ONTAP 9.14.0

BlueXP peut désormais déployer et gérer la version de disponibilité générale de Cloud Volumes ONTAP 9.14.0 dans AWS, Azure et Google Cloud.

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

## 10 septembre 2023

Le changement suivant a été introduit avec la version 3.9.33 du connecteur.

### Prise en charge des machines virtuelles de la série Lsv3 dans Azure

Les types d'instances L48s\_v3 et L64s\_v3 sont désormais pris en charge avec Cloud Volumes ONTAP dans Azure pour les déploiements à nœud unique et à paires haute disponibilité avec des disques gérés partagés dans des zones de disponibilité uniques et multiples, à partir de la version 9.13.1. Ces types d'instances prennent en charge Flash Cache.

["Afficher les configurations prises en charge pour Cloud Volumes ONTAP dans Azure"](#) ["Afficher les limites de stockage pour Cloud Volumes ONTAP dans Azure"](#)

## 30 juillet 2023

Les modifications suivantes ont été introduites avec la version 3.9.32 du connecteur.

### Prise en charge du cache Flash et de la vitesse d'écriture élevée dans Google Cloud

Le cache Flash et la vitesse d'écriture élevée peuvent être activés séparément dans Google Cloud pour Cloud Volumes ONTAP 9.13.1 et versions ultérieures. Une vitesse d'écriture élevée est disponible sur tous les types d'instances pris en charge. Flash Cache est pris en charge sur les types d'instances suivants :

- n2-standard-16
- n2-standard-32
- n2-standard-48
- n2-standard-64

Vous pouvez utiliser ces fonctionnalités séparément ou ensemble sur des déploiements à nœud unique et à paires haute disponibilité.

["Lancer Cloud Volumes ONTAP dans Google Cloud"](#)

### Améliorations des rapports d'utilisation

Diverses améliorations des informations affichées dans les rapports d'utilisation sont désormais disponibles. Voici les améliorations apportées aux rapports d'utilisation :

- L'unité TiB est désormais incluse dans le nom des colonnes.
- Un nouveau champ « nœud(s) » pour les numéros de série est désormais inclus.
- Une nouvelle colonne « Type de charge de travail » est désormais incluse dans le rapport d'utilisation des machines virtuelles de stockage.
- Les noms d'environnement de travail sont désormais inclus dans les rapports d'utilisation des machines virtuelles de stockage et des volumes.
- Le type de volume « fichier » est désormais étiqueté « Principal (lecture/écriture) ».
- Le type de volume « secondaire » est désormais étiqueté « Secondaire (DP) ».

Pour plus d'informations sur les rapports d'utilisation, reportez-vous à ["Télécharger les rapports d'utilisation"](#) .

## 26 juillet 2023

Les modifications suivantes ont été introduites avec la version 3.9.31 du connecteur.

### Cloud Volumes ONTAP 9.13.1 GA

BlueXP peut désormais déployer et gérer la version de disponibilité générale de Cloud Volumes ONTAP 9.13.1 dans AWS, Azure et Google Cloud.

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

## 2 juillet 2023

Les modifications suivantes ont été introduites avec la version 3.9.31 du connecteur.

### Prise en charge des déploiements de zones de disponibilité multiples HA dans Azure

Le Japon Est et la Corée Centrale dans Azure prennent désormais en charge les déploiements de zones de disponibilité multiples HA pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

Pour obtenir la liste de toutes les régions prenant en charge plusieurs zones de disponibilité, reportez-vous à la ["Carte des régions mondiales sous Azure"](#) .

### Prise en charge de la protection autonome contre les ransomwares

La protection autonome contre les ransomwares (ARP) est désormais prise en charge sur Cloud Volumes ONTAP. La prise en charge ARP est disponible sur Cloud Volumes ONTAP version 9.12.1 et supérieure.

Pour en savoir plus sur ARP avec Cloud Volumes ONTAP, reportez-vous à ["Protection autonome contre les ransomwares"](#) .

## 26 juin 2023

Le changement suivant a été introduit avec la version 3.9.30 du connecteur.

### Cloud Volumes ONTAP 9.13.1 RC1

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.13.1 dans AWS, Azure et Google Cloud.

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

## 4 juin 2023

Le changement suivant a été introduit avec la version 3.9.30 du connecteur.

### Mise à jour du sélecteur de version de mise à niveau de Cloud Volumes ONTAP

Grâce à la page Mettre à niveau Cloud Volumes ONTAP , vous pouvez désormais choisir de mettre à niveau vers la dernière version disponible de Cloud Volumes ONTAP ou une version plus ancienne.

Pour en savoir plus sur la mise à niveau de Cloud Volumes ONTAP via BlueXP, reportez-vous à ["Mettre à niveau Cloud Volumes ONTAP"](#) .

## 7 mai 2023

Les modifications suivantes ont été introduites avec la version 3.9.29 du connecteur.

### **La région du Qatar est désormais prise en charge dans Google Cloud**

La région du Qatar est désormais prise en charge dans Google Cloud pour Cloud Volumes ONTAP et Connector pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

### **La région Suède Centre est désormais prise en charge dans Azure**

La région Suède centrale est désormais prise en charge dans Azure pour Cloud Volumes ONTAP et le connecteur pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

### **Prise en charge des déploiements multizones de haute disponibilité dans Azure Australie Est**

La région Australie Est dans Azure prend désormais en charge les déploiements de zones de disponibilité multiples HA pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

### **Répartition de l'utilisation de la charge**

Vous pouvez désormais savoir ce qui vous est facturé lorsque vous êtes abonné à des licences basées sur la capacité. Les types de rapports d'utilisation suivants sont disponibles en téléchargement à partir du portefeuille numérique dans BlueXP. Les rapports d'utilisation fournissent des détails sur la capacité de vos abonnements et vous indiquent comment vous êtes facturé pour les ressources de vos abonnements Cloud Volumes ONTAP. Les rapports téléchargeables peuvent être facilement partagés avec d'autres.

- Utilisation du package Cloud Volumes ONTAP
- Utilisation de haut niveau
- Utilisation des machines virtuelles de stockage
- Utilisation des volumes

Pour plus d'informations, consultez ["Gérer les licences basées sur la capacité"](#).

### **La notification s'affiche désormais lors de l'accès à BlueXP sans abonnement à la place de marché**

Une notification s'affiche désormais chaque fois que vous accédez à Cloud Volumes ONTAP dans BlueXP sans abonnement à la place de marché. La notification indique qu'« un abonnement au marché pour cet environnement de travail est requis pour être conforme aux conditions générales de Cloud Volumes ONTAP ».

## 4 avril 2023

### **Prise en charge des régions chinoises pour AWS**

À partir de Cloud Volumes ONTAP 9.12.1 GA, les régions de Chine sont désormais prises en charge dans AWS comme suit.

- Les systèmes à nœud unique sont pris en charge.
- Les licences achetées directement auprès de NetApp sont prises en charge.

Pour connaître la disponibilité régionale, reportez-vous à la ["Cartes des régions mondiales pour Cloud Volumes ONTAP"](#).

## 3 avril 2023

Les modifications suivantes ont été introduites avec la version 3.9.28 du connecteur.

### **La région de Turin est désormais prise en charge dans Google Cloud**

La région de Turin est désormais prise en charge dans Google Cloud pour Cloud Volumes ONTAP et Connector pour Cloud Volumes ONTAP 9.12.1 GA et versions ultérieures.

### **Amélioration du BlueXP digital wallet**

Le BlueXP digital wallet affiche désormais la capacité sous licence que vous avez achetée avec les offres privées du marché.

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

### **Prise en charge des commentaires lors de la création du volume**

Cette version vous permet de faire des commentaires lors de la création d'un volume Cloud Volumes ONTAP FlexGroup ou FlexVol volume lors de l'utilisation de l'API.

### **Refonte de l'interface utilisateur BlueXP pour les pages Présentation, Volumes et Agrégats de Cloud Volumes ONTAP**

BlueXP dispose désormais d'une interface utilisateur repensée pour les pages Présentation, Volumes et Agrégats de Cloud Volumes ONTAP . La conception basée sur des tuiles présente des informations plus complètes dans chaque tuile pour une meilleure expérience utilisateur.

The screenshot shows the NetApp console interface for Cloud Volumes ONTAP. The main content area is divided into several sections:

- Storage Efficiency:** 1.00:1
- Cloud Volumes ONTAP is up to date:** Version 9.17.1RC1
- Capacity Distribution:** 0 GiB Provisioned, 0 GiB Used Capacity, 0 GiB Available
- Volumes:** 0 Volumes (with 'Add Volume' and 'View Volumes' buttons)
- Aggregates:** 1 Aggregate (with 'Add Aggregate' and 'View Aggregates' buttons)
- Replications:** 0 Replications (with 'Go to Replication Settings' button)
- Backups:** 0 volumes Backups (with 'Go to Backup Settings' button)

The right-hand sidebar contains a table of features and system information:

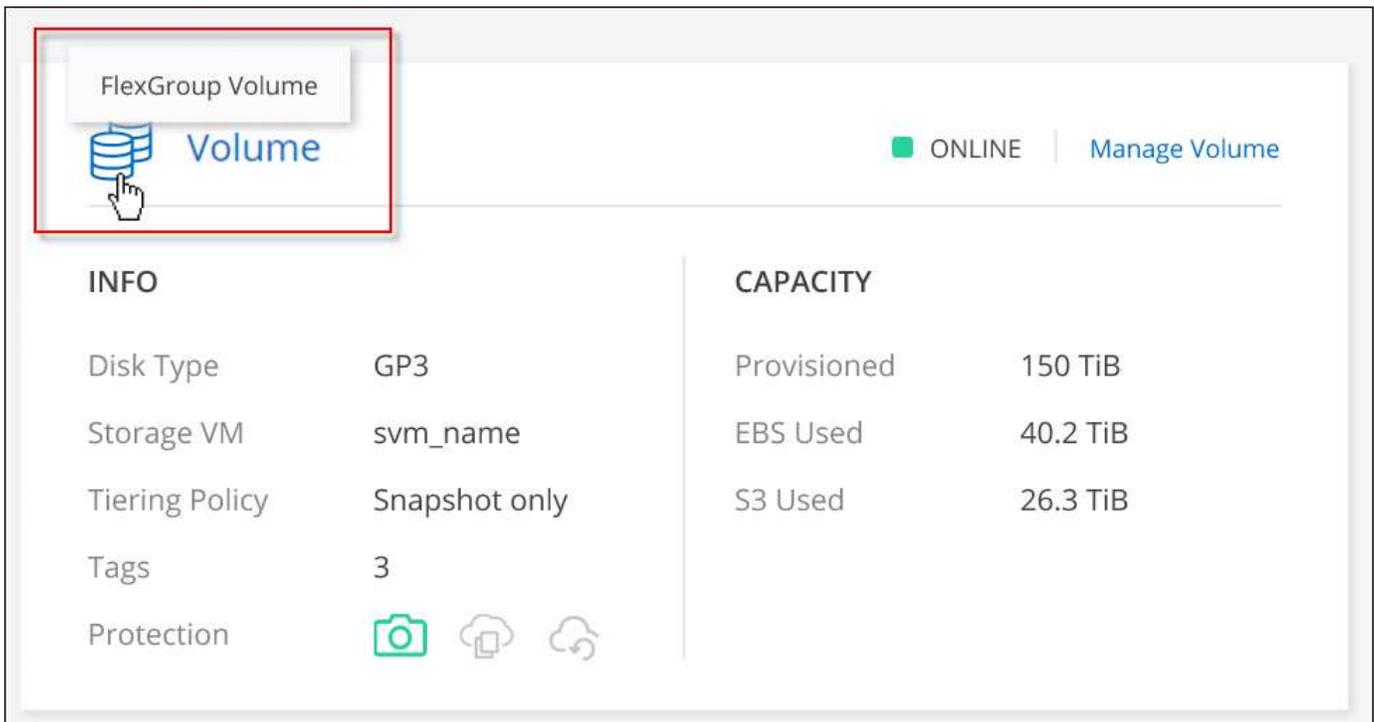
Information	Features
Cloud Volumes ONTAP	AWS Single
Charging Method: Freemium	
License in Use: Freemium	
Marketplace Subscription: Sub2-ByCapacityB...	
Region: us-east-1	
VPC: vpc-0...	
Cluster Management IP: ...	
Serial Number: ...	
Encryption: Enabled	

## Volumes FlexGroup visibles via Cloud Volumes ONTAP

Les volumes FlexGroup créés via ONTAP System Manager ou directement via l'interface de ligne de commande ONTAP sont désormais visibles via la mosaïque Volumes repensée dans BlueXP. Identique aux informations fournies pour les volumes FlexVol, BlueXP fournit des informations détaillées sur les volumes FlexGroup créés via une mosaïque Volumes dédiée.



Actuellement, vous ne pouvez afficher que les volumes FlexGroup existants sous BlueXP. La possibilité de créer des volumes FlexGroup dans BlueXP n'est pas disponible mais prévue pour une future version.



["En savoir plus sur l'affichage des volumes FlexGroup créés."](#)

## 13 mars 2023

### Prise en charge des régions chinoises dans Azure

La région Chine Nord 3 est désormais prise en charge pour les déploiements à nœud unique de Cloud Volumes ONTAP 9.12.1 GA et 9.13.0 GA dans Azure. Seules les licences achetées directement auprès de NetApp (licences BYOL) sont prises en charge dans ces régions.



Les nouveaux déploiements de Cloud Volumes ONTAP dans les régions de Chine sont pris en charge uniquement dans les versions 9.12.1 GA et 9.13.0 GA. Vous pouvez mettre à niveau ces versions vers des correctifs et des versions ultérieures de Cloud Volumes ONTAP. Si vous souhaitez déployer des versions ultérieures de Cloud Volumes ONTAP dans les régions chinoises, contactez le support NetApp .

Pour connaître la disponibilité régionale, reportez-vous à la ["Cartes des régions mondiales pour Cloud Volumes ONTAP"](#) .

## 5 mars 2023

Les modifications suivantes ont été introduites avec la version 3.9.27 du connecteur.

### Cloud Volumes ONTAP 9.13.0

BlueXP peut désormais déployer et gérer Cloud Volumes ONTAP 9.13.0 dans AWS, Azure et Google Cloud.

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

## Prise en charge de 16 Tio et 32 Tio dans Azure

Cloud Volumes ONTAP prend désormais en charge les tailles de disque de 16 Tio et 32 Tio pour les déploiements haute disponibilité exécutés sur des disques gérés dans Azure.

En savoir plus sur ["tailles de disque prises en charge dans Azure"](#) .

## Licence MTEKM

La licence Multi-tenant Encryption Key Management (MTEKM) est désormais incluse avec les systèmes Cloud Volumes ONTAP nouveaux et existants exécutant la version 9.12.1 GA ou ultérieure.

La gestion des clés externes multi-locataires permet aux machines virtuelles de stockage individuelles (SVM) de conserver leurs propres clés via un serveur KMIP lors de l'utilisation de NetApp Volume Encryption.

["Découvrez comment chiffrer des volumes avec les solutions de chiffrement NetApp"](#) .

## Prise en charge des environnements sans Internet

Cloud Volumes ONTAP est désormais pris en charge dans tout environnement cloud doté d'une isolation complète d'Internet. Seules les licences basées sur les nœuds (BYOL) sont prises en charge dans ces environnements. Les licences basées sur la capacité ne sont pas prises en charge. Pour commencer, installez manuellement le logiciel Connector, connectez-vous à la console BlueXP exécutée sur le Connector, ajoutez votre licence BYOL au BlueXP digital wallet, puis déployez Cloud Volumes ONTAP.

- ["Installer le connecteur dans un endroit sans accès Internet"](#)
- ["Accéder à la console BlueXP sur le connecteur"](#)
- ["Ajouter une licence non attribuée"](#)

## Cache Flash et vitesse d'écriture élevée dans Google Cloud

La prise en charge du cache Flash, d'une vitesse d'écriture élevée et d'une unité de transmission maximale (MTU) élevée de 8 896 octets est désormais disponible pour certaines instances avec la version Cloud Volumes ONTAP 9.13.0.

En savoir plus sur ["configurations prises en charge par licence pour Google Cloud"](#) .

## 5 février 2023

Les modifications suivantes ont été introduites avec la version 3.9.26 du connecteur.

### Création de groupe de placement dans AWS

Un nouveau paramètre de configuration est désormais disponible pour la création de groupes de placement avec les déploiements de zone de disponibilité unique (AZ) AWS HA. Vous pouvez désormais choisir de contourner les échecs de création de groupes de placement et de permettre aux déploiements AWS HA mono-AZ de se terminer avec succès.

Pour obtenir des informations détaillées sur la configuration du paramètre de création de groupe de placement, reportez-vous à ["Configurer la création d'un groupe de placement pour AWS HA Single AZ"](#) .

## Mise à jour de la configuration de la zone DNS privée

Un nouveau paramètre de configuration est désormais disponible pour vous permettre d'éviter de créer un lien entre une zone DNS privée et un réseau virtuel lors de l'utilisation d'Azure Private Links. La création est activée par défaut.

["Fournissez à BlueXP des détails sur votre DNS privé Azure"](#)

## Stockage WORM et hiérarchisation des données

Vous pouvez désormais activer à la fois la hiérarchisation des données et le stockage WORM lorsque vous créez un système Cloud Volumes ONTAP 9.8 ou version ultérieure. L'activation de la hiérarchisation des données avec le stockage WORM vous permet de hiérarchiser les données vers un magasin d'objets dans le cloud.

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

## 1er janvier 2023

Les modifications suivantes ont été introduites avec la version 3.9.25 du connecteur.

### Packages de licences disponibles dans Google Cloud

Des packages de licences optimisés et basés sur la capacité Edge Cache sont disponibles pour Cloud Volumes ONTAP sur Google Cloud Marketplace sous la forme d'une offre à la carte ou d'un contrat annuel.

Se référer à ["Licences Cloud Volumes ONTAP"](#) .

### Configuration par défaut pour Cloud Volumes ONTAP

La licence Multi-tenant Encryption Key Management (MTEKM) n'est plus incluse dans les nouveaux déploiements Cloud Volumes ONTAP .

Pour plus d'informations sur les licences de fonctionnalités ONTAP installées automatiquement avec Cloud Volumes ONTAP, reportez-vous à ["Configuration par défaut pour 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 incluses dans cette version de 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 la prise en charge de nouvelles fonctionnalités et de régions de fournisseurs de cloud supplémentaires.

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

## 4 décembre 2022

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

### **WORM + Cloud Backup désormais disponible lors de la création de Cloud Volumes ONTAP**

La possibilité d'activer les fonctionnalités d'écriture unique et de lecture multiple (WORM) et de sauvegarde dans le cloud est désormais disponible pendant le processus de création de Cloud Volumes ONTAP .

### **La région d'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 Connector pour Cloud Volumes ONTAP 9.11.1 P3 et versions ultérieures.

## 15 novembre 2022

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

### **Licence ONTAP S3 dans Google Cloud**

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

["Documentation ONTAP : découvrez comment configurer et gérer les services de stockage d'objets S3"](#)

## 6 novembre 2022

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

### **Déplacer des groupes de ressources dans Azure**

Vous pouvez désormais déplacer un environnement de travail d'un groupe de ressources vers un autre groupe de ressources dans Azure au sein du même abonnement Azure.

Pour plus d'informations, consultez ["Déplacer des groupes de ressources"](#) .

### **Certification de copie NDMP**

NDMP-copy est désormais certifié pour une utilisation avec Cloud Volume ONTAP.

Pour plus d'informations sur la configuration et l'utilisation de NDMP, reportez-vous au ["Documentation ONTAP : 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 désormais de chiffrer tous les disques gérés lors de leur création.

Pour plus d'informations sur cette nouvelle fonctionnalité, reportez-vous à ["Configurer 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 portefeuille numérique affiche désormais un résumé du package de licence d'E/S optimisé et de la capacité WORM provisionnée pour les systèmes Cloud Volumes ONTAP sur votre compte.

Ces détails peuvent vous aider à mieux comprendre comment vous êtes facturé et si vous devez acheter une capacité supplémentaire.

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

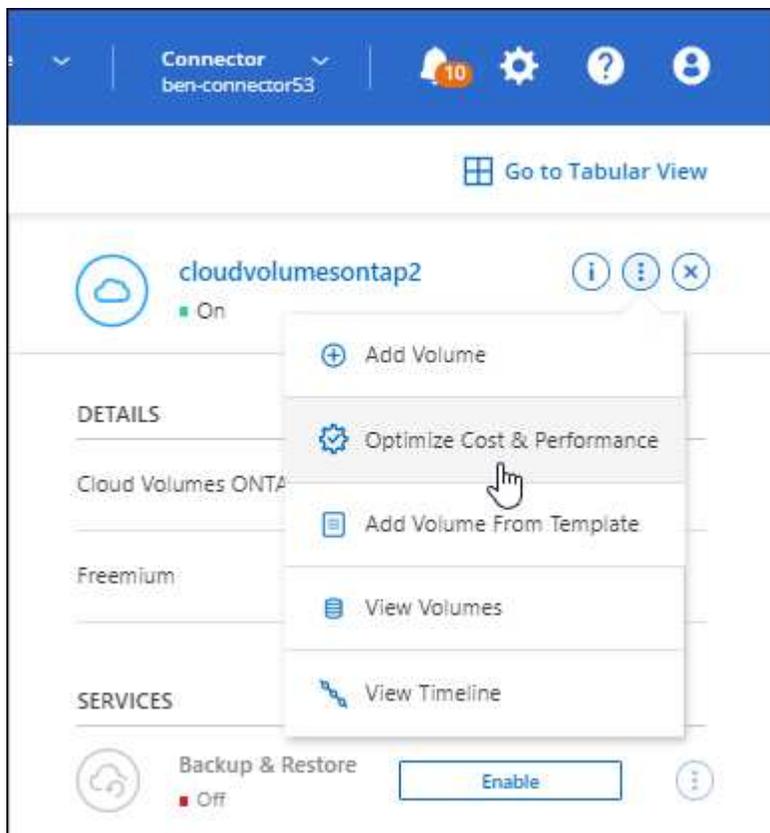
- Vous pouvez désormais passer d'une méthode de charge à la méthode de charge optimisée.

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

### Optimiser les coûts et les performances

Vous pouvez désormais optimiser le coût et les performances d'un système Cloud Volumes ONTAP directement depuis le Canvas.

Après avoir sélectionné un environnement de travail, vous pouvez choisir l'option **Optimiser les coûts et les performances** pour modifier le type d'instance pour Cloud Volumes ONTAP. Le choix 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 générera désormais une notification si un système Cloud Volumes ONTAP ne parvient pas à envoyer de messages AutoSupport . La notification inclut un lien vers des instructions que vous pouvez utiliser pour résoudre les problèmes de réseau.

## 31 juillet 2022

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

### Licence MTEKM

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

La gestion des clés externes multi-locataires permet aux machines virtuelles de stockage individuelles (SVM) de conserver leurs propres clés via un serveur KMIP lors de l'utilisation de NetApp Volume Encryption.

["Découvrez comment chiffrer des volumes avec les solutions de chiffrement NetApp"](#) .

### Serveur proxy

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

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

La seule exigence 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 avoir déployé le connecteur.

### Changer la méthode de charge

Vous pouvez désormais modifier la méthode de facturation d'un système Cloud Volumes ONTAP qui utilise des licences basées sur la capacité. Par exemple, si vous avez déployé un système Cloud Volumes ONTAP avec le package Essentials, vous pouvez le remplacer par le package Professional si les besoins de votre entreprise ont changé. Cette fonctionnalité est disponible à partir du portefeuille numérique.

["Apprenez à modifier 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 au sein du réseau sélectionné uniquement (recommandé) ou de 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 licences 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** : Licence pour "[Cache Edge Cloud Volumes](#)"

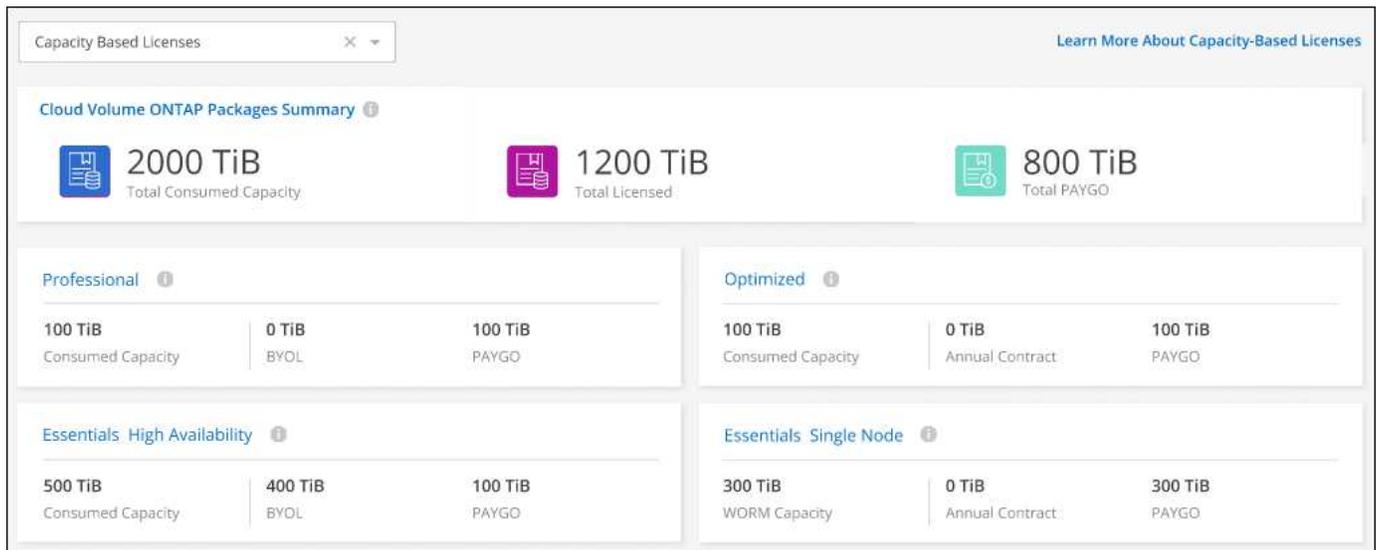
["En savoir plus sur ces packages de licences"](#) .

## 3 juillet 2022

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

### Portefeuille numérique

Le portefeuille numérique vous indique désormais la capacité totale consommée sur votre compte et la capacité consommée par package de licence. Cela peut vous aider à comprendre comment vous êtes facturé et si vous devez acheter une capacité supplémentaire.



## 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 Volumes élastiques est activée par défaut lors de l'utilisation de disques gp3 ou io1. Vous pouvez choisir la capacité initiale en fonction de vos besoins de stockage et la réviser après le déploiement de Cloud Volumes ONTAP .

["En savoir plus sur la prise en charge des volumes élastiques dans AWS"](#) .

## Licence ONTAP S3 dans AWS

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

["Documentation ONTAP : découvrez comment configurer et gérer les services de stockage d'objets S3"](#)

## Prise en charge de la nouvelle région Azure Cloud

À partir de 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 pour Cloud Volumes ONTAP"](#)

## Licence ONTAP S3 dans Azure

Une licence ONTAP S3 est désormais incluse sur les systèmes Cloud Volumes ONTAP nouveaux et existants exécutant la version 9.9.1 ou ultérieure dans Azure.

["Documentation ONTAP : découvrez comment configurer et gérer les services de stockage d'objets S3"](#)

## 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 la prise en charge de

nouvelles fonctionnalités et de régions de fournisseurs de cloud supplémentaires.

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

### **Nouvelle vue avancée**

Si vous devez effectuer une gestion avancée de Cloud Volumes ONTAP, vous pouvez le faire à l'aide d'ONTAP System Manager, une interface de gestion fournie avec un système ONTAP . Nous avons inclus l'interface du gestionnaire de système directement dans BlueXP afin que vous n'ayez pas besoin de quitter BlueXP pour une gestion avancée.

Cette vue avancée est disponible en tant qu'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. Veuillez nous envoyer vos commentaires en utilisant le chat intégré au produit.

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

### **Prise en charge des volumes élastiques Amazon EBS**

La prise en charge de la fonctionnalité Amazon EBS Elastic Volumes avec un agrégat Cloud Volumes ONTAP offre de meilleures performances et une capacité supplémentaire, tout en permettant à BlueXP d'augmenter automatiquement la capacité du disque sous-jacent selon les besoins.

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

["En savoir plus sur la prise en charge des volumes élastiques"](#) .

Notez que la prise en charge des volumes élastiques nécessite de nouvelles autorisations AWS pour le connecteur :

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

Assurez-vous de fournir ces autorisations à chaque ensemble d'informations d'identification AWS que vous avez ajoutées à BlueXP. ["Consultez la dernière politique de connecteur pour AWS"](#) .

### **Prise en charge du déploiement de paires HA dans des sous-réseaux AWS partagés**

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

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

### **Accès réseau limité lors de l'utilisation de points de terminaison de service**

BlueXP limite désormais l'accès au réseau lors de l'utilisation d'un point de terminaison 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

Plusieurs machines virtuelles de stockage sont désormais prises en charge avec Cloud Volumes ONTAP dans Google Cloud, à partir de la version 9.11.1. À partir de cette version du connecteur, BlueXP vous permet de créer des machines virtuelles de stockage sur des paires Cloud Volumes ONTAP HA dans Google Cloud à l'aide de l'API.

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

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

Notez que vous devez utiliser l'interface de ligne de commande ONTAP ou le gestionnaire de système pour créer une machine virtuelle de stockage sur un système à nœud unique.

- ["En savoir plus sur les limites des machines virtuelles de stockage dans Google Cloud"](#)
- ["Découvrez comment créer des machines virtuelles de stockage de 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 incluses dans cette version de Cloud Volumes ONTAP"](#) .

### Amélioration des mises à niveau du médiateur

Lorsque BlueXP met à niveau le médiateur pour une paire HA, il valide désormais qu'une nouvelle image de médiateur est disponible avant de supprimer le disque de démarrage. Cette modification garantit que le médiateur peut continuer à fonctionner avec succès 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 maintenant été supprimé.

### Contrat annuel dans Azure

Les packages Essentials et Professional sont désormais disponibles dans Azure via un contrat annuel. Vous pouvez contacter votre représentant commercial NetApp pour acheter un contrat annuel. Le contrat est disponible sous forme d'offre privée sur la Place de marché Azure.

Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à partir de la Place de marché Azure lors de la création de l'environnement de travail.

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

## Récupération instantanée du glacier S3

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

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

## Nouvelles autorisations AWS requises pour le connecteur

Les autorisations suivantes sont désormais requises pour créer un groupe de placement réparti AWS lors du déploiement d'une paire HA dans une seule zone de disponibilité (AZ) :

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

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

Assurez-vous de fournir ces autorisations à chaque ensemble d'informations d'identification AWS que vous avez ajoutées à BlueXP. ["Consultez la dernière politique de connecteur pour AWS"](#) .

## Nouvelle 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-Sud2)
- Melbourne (Australie-sud-est2)
- Milan (europe-west8) - nœud unique uniquement
- Santiago (southamerica-west1) - nœud unique uniquement

["Consultez la liste complète des régions prises en charge pour 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.

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

## Améliorations apportées aux stratégies de pare-feu de Google Cloud

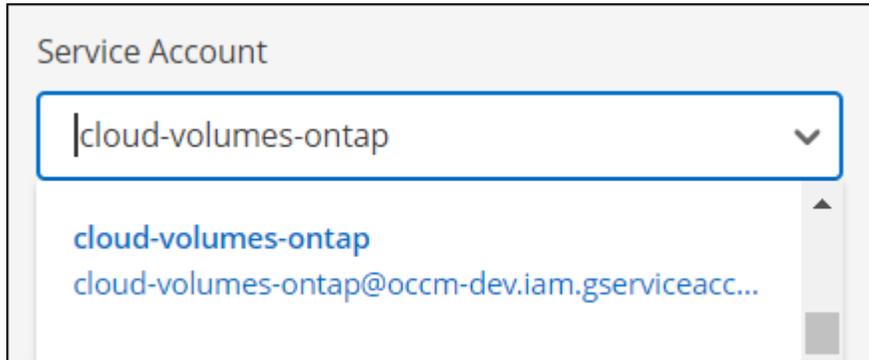
- Lorsque vous créez une paire Cloud Volumes ONTAP HA dans Google Cloud, BlueXP affiche désormais toutes les stratégies de pare-feu existantes dans un VPC.

Auparavant, BlueXP n'affichait aucune stratégie dans VPC-1, VPC-2 ou VPC-3 qui n'avait pas de balise cible.

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



### 3 avril 2022

#### Le lien vers le gestionnaire de système 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 saisissant l'adresse IP de gestion du cluster dans un navigateur Web disposant d'une connexion au système Cloud Volumes ONTAP . ["En savoir plus sur la connexion au Gestionnaire système"](#) .

#### Frais de stockage WORM

Maintenant que le tarif spécial de lancement a expiré, vous serez facturé pour l'utilisation du stockage WORM. La facturation est horaire, en fonction de la capacité totale provisionnée des volumes WORM. Ceci s'applique aux systèmes Cloud Volumes ONTAP nouveaux et existants.

["En savoir plus sur les tarifs du stockage WORM"](#) .

### 27 février 2022

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

#### Assistant de volume repensé

L'assistant de création de nouveau volume que nous avons récemment introduit est désormais disponible lors de la création d'un volume sur un agrégat spécifique à partir de l'option **Allocation avancée**.

["Apprenez à créer des volumes sur un agrégat spécifique"](#) .

### 9 février 2022

#### Mises à jour du marché

- Les packages Essentials et Professional sont désormais disponibles sur toutes les places de marché des fournisseurs de cloud.

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

Si vous disposez déjà d'un abonnement sur une place de marché cloud, vous êtes également automatiquement abonné à ces nouvelles offres. Vous pouvez choisir la facturation par capacité lorsque vous déployez un nouvel environnement de travail Cloud Volumes ONTAP .

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

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

Cette méthode de facturation est toujours disponible pour les clients existants qui ont un abonnement actif.

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

## 6 février 2022

### Échanger des licences non attribuées

Si vous disposez d'une licence basée sur un nœud non attribué pour Cloud Volumes ONTAP que vous n'avez pas utilisée, vous pouvez désormais échanger la licence 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 avec la même date d'expiration.

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

## 30 janvier 2022

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

### Sélection de licences repensée

Nous avons repensé l'écran de sélection de licence lors de la création d'un nouvel environnement de travail Cloud Volumes ONTAP . Les changements mettent en évidence les méthodes de facturation par capacité qui ont été introduites en juillet 2021 et prennent en charge les offres à venir via les marchés des fournisseurs de 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 machines virtuelles Azure supplémentaires

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

- E4ds\_v4
- E8ds\_v4
- E32ds\_v4
- E48ds\_v4

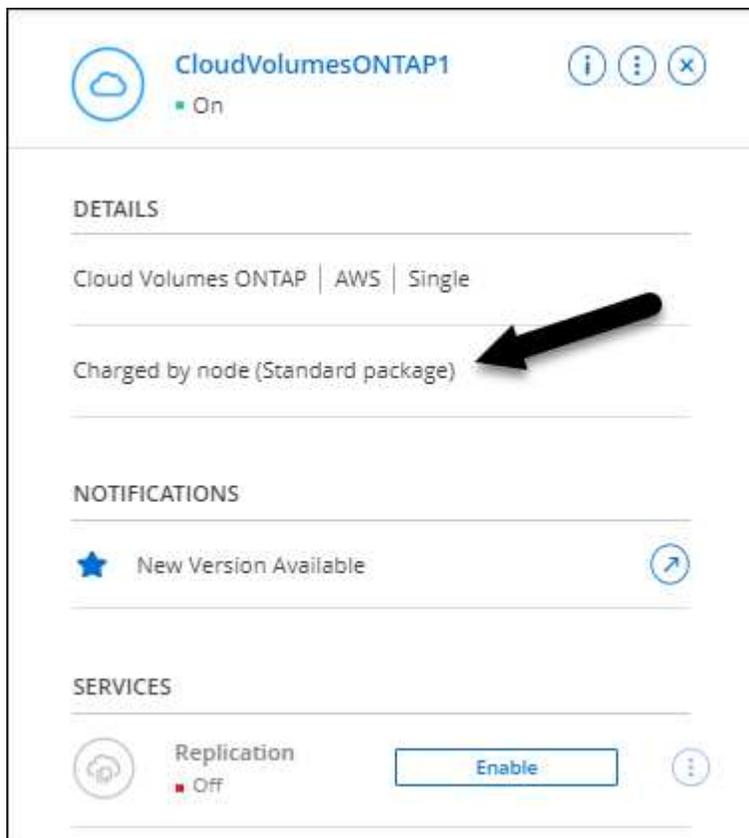
Aller à la "[Notes de version de Cloud Volumes ONTAP](#)" pour plus de détails sur les configurations prises en charge.

## Mise à jour de chargement de 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 .

## La méthode de charge est désormais affichée

BlueXP affiche désormais la méthode de facturation pour chaque environnement de travail Cloud Volumes ONTAP dans le panneau de droite du canevas.



## Choisissez votre nom d'utilisateur

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

Credentials

User Name

Password

Confirm Password

### Améliorations de la création de volumes

Nous avons apporté quelques améliorations à la création de volumes :

- Nous avons repensé l'assistant de création de volume pour plus de simplicité d'utilisation.
- Vous pouvez désormais choisir une politique d'exportation personnalisée pour NFS.

Details, Protection & Tags  
  2 Protocol  
  3 Disk Type  
  4 Usage Profile & Tiering Policy  
  5 Review

**Volumes Protocol**

Select the volume's protocol:  
 NFS Protocol  
 CIFS Protocol  
 iSCSI Protocol

Access Control

Export Policy (1 rule defined)

[Manage volume's export policy](#)

## 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 incluses dans cette version de Cloud Volumes ONTAP"](#) .

## Abonnements NetApp Keystone

Vous pouvez désormais utiliser les abonnements Keystone pour payer les paires Cloud Volumes ONTAP HA.

Un abonnement Keystone est un service d'abonnement à paiement progressif qui offre une expérience de cloud hybride transparente pour ceux qui préfèrent les modèles de consommation OpEx aux CapEx initiaux ou à la location.

Un abonnement Keystone 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 NetApp Keystone"](#) .
- ["Découvrez comment démarrer avec les abonnements Keystone dans BlueXP"](#) .

## Nouvelle prise en charge régionale AWS

Cloud Volumes ONTAP est désormais pris en charge dans la région AWS Asie-Pacifique (Osaka) (ap-northeast-3).

## Réduction du port

Les ports 8023 et 49000 ne sont plus ouverts sur les systèmes Cloud Volumes ONTAP dans Azure pour les systèmes à nœud unique et les paires HA.

Cette modification s'applique aux *nouveaux* systèmes Cloud Volumes ONTAP à partir de 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 incluses dans cette version de Cloud Volumes ONTAP"](#) .

## Temps de déploiement réduit

Nous avons réduit le temps nécessaire au déploiement d'un environnement de travail Cloud Volumes ONTAP dans Microsoft Azure ou dans Google Cloud lorsque la vitesse d'écriture normale est activée. Le temps de déploiement est désormais 3 à 4 minutes plus court en moyenne.

## 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 du service de stockage Azure"](#) avec une clé gérée par Microsoft. Mais vous pouvez désormais utiliser votre propre clé de chiffrement gérée par le client en suivant les étapes suivantes :

1. Depuis Azure, créez un coffre de clés, puis générez une clé dans ce coffre.

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 facturation sont disponibles pour Cloud Volumes ONTAP.

- **BYOL basé sur la capacité** : une licence basée sur la capacité vous permet de payer Cloud Volumes ONTAP par Tio de capacité. La licence est associée à votre compte NetApp et vous permet de créer plusieurs systèmes Cloud Volumes ONTAP , à condition qu'une capacité suffisante soit disponible via votre licence. Les licences basées sur la capacité sont disponibles sous la forme d'un package, soit *Essentials* ou *Professional*.
- **Offre Freemium** : Freemium vous permet d'utiliser gratuitement toutes les fonctionnalités de Cloud Volumes ONTAP de NetApp (des frais de fournisseur de cloud s'appliquent toujours). Vous êtes limité à 500 Gio de capacité provisionnée par système et il n'y a 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 facturation parmi lesquelles 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

Package

---

  Freemium (Up to 500GB)

---

### Stockage WORM disponible pour une utilisation générale

Le stockage WORM (Write once, read many) n'est plus en version Preview et est désormais disponible pour une utilisation générale avec Cloud Volumes ONTAP. ["En savoir plus sur le stockage WORM"](#) .

### Prise en charge de m5dn.24xlarge dans AWS

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

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

### Sélectionner des groupes de ressources Azure existants

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

### Location & Connectivity

<p><b>Location</b></p> <p>Azure Region</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">WEST US</div> <p>Availability Zone <span style="float: right;"><i>(Optional)</i></span></p> <div style="border: 1px solid #ccc; padding: 2px;">Select an Availability Zone</div>	<p><b>Connectivity</b></p> <p>Resource Group</p> <p> <input type="radio"/> Create a new group         <input checked="" type="radio"/> Use an existing group       </p> <p>Resource Group Name</p> <div style="border: 1px solid #ccc; padding: 2px;">RG1</div>
---	---

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

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

Assurez-vous de fournir ces autorisations à chaque ensemble d'informations d'identification Azure que vous avez ajoutées à BlueXP. ["Consultez la dernière politique de connecteur pour Azure"](#) .

### L'accès public aux blobs est désormais désactivé dans Azure

En tant qu'amélioration de sécurité, BlueXP désactive désormais **l'accès public Blob** 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 diagnostics de démarrage pour les nouveaux systèmes Cloud Volumes ONTAP .

Cela signifie que *tous* les comptes de stockage pour Cloud Volumes ONTAP utiliseront désormais un lien privé.

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

### Disques persistants équilibrés dans Google Cloud

À partir de la version 9.9.1, Cloud Volumes ONTAP prend désormais en charge les disques persistants équilibrés (pd-balanced).

Ces SSD équilibrent performances et coût en fournissant des IOPS par Gio inférieurs.

### custom-4-16384 n'est plus pris en charge dans Google Cloud

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

Si vous disposez déjà d'un système 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.

["Afficher 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 package professionnel dans AWS

Un nouveau package professionnel vous permet de regrouper Cloud Volumes ONTAP et Cloud Backup Service en utilisant un contrat annuel de la place de marché AWS. Le paiement s'effectue par Tio. Cet abonnement ne vous permet pas de sauvegarder les données sur site.

Si vous choisissez cette option de paiement, vous pouvez provisionner jusqu'à 2 PiB par système Cloud Volumes ONTAP via des disques EBS et une hiérarchisation vers le stockage d'objets S3 (nœud unique ou HA).

Aller à la ["Page AWS Marketplace"](#) pour afficher les détails des prix et accéder à la ["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 ont été créées précédemment après le déploiement de Cloud Volumes ONTAP .

Ce changement peut être utile si votre organisation utilise des politiques de contrôle des services (SCP) pour gérer les autorisations.

### Période de refroidissement minimale pour la politique de hiérarchisation automatique

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

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

### Amélioration des politiques d'exportation personnalisées

Lorsque vous créez un nouveau volume NFS, BlueXP affiche désormais les stratégies d'exportation personnalisées par ordre croissant, ce qui vous permet de trouver plus facilement la stratégie d'exportation dont vous avez besoin.

### Suppression des anciens instantanés du cloud

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

Cette amélioration permet de réduire les coûts des fournisseurs de cloud en supprimant les instantanés qui ne sont plus nécessaires.

Notez qu'un connecteur nécessite une nouvelle autorisation pour supprimer les instantanés Azure. ["Consultez la dernière politique de connecteur 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 incluses dans cette version de Cloud Volumes ONTAP"](#) .

## 11 avril 2021

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

### Rapports d'espace logique

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

Lorsque l'espace est signalé de manière logique, ONTAP signale l'espace du volume de telle sorte que tout l'espace physique économisé par les fonctionnalités d'efficacité du stockage soit également signalé comme utilisé.

### Prise en charge des disques gp3 dans AWS

Cloud Volumes ONTAP prend désormais en charge les disques SSD à usage général (gp3) à partir de la version 9.7. Les disques gp3 sont les SSD les moins chers qui équilibrent coût et performances pour une large gamme de charges de travail.

["Dimensionnez votre système dans AWS"](#) .

### Les disques durs froids ne sont plus pris en charge dans AWS

Cloud Volumes ONTAP ne prend plus en charge les disques Cold HDD (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 désormais 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 incluses dans cette version de Cloud Volumes ONTAP"](#) .

## Prise en charge de l'environnement AWS C2S

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

["Déployer Cloud Volumes ONTAP dans AWS Secret Cloud ou AWS Top Secret Cloud"](#) .

## Chiffrement AWS avec CMK gérés par le client

BlueXP vous a toujours permis de crypter les données Cloud Volumes ONTAP à l'aide d'AWS Key Management Service (KMS). À partir de Cloud Volumes ONTAP 9.9.0, les données sur les disques EBS et les données hiérarchisées sur S3 sont chiffrées si vous sélectionnez une CMK gérée par le client. Auparavant, seules les données EBS étaient cryptées.

Notez que vous devrez fournir au rôle IAM Cloud Volumes ONTAP un accès pour utiliser la CMK.

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

## Prise en charge d'Azure DoD

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

## Réduction de l'adresse 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 de moins est requise (nous avons unifié le LIF intercluster avec le LIF de gestion des nœuds). Vous avez également la possibilité d'ignorer la création du LIF de gestion SVM lors de l'utilisation de l'API, ce qui réduirait le besoin d'une adresse IP supplémentaire.

["En savoir plus sur les exigences en matière d'adresse IP dans Google Cloud"](#) .

## Prise en charge du VPC partagé dans Google Cloud

Lorsque vous déployez une paire Cloud Volumes ONTAP HA dans Google Cloud, vous pouvez désormais choisir des VPC partagés pour VPC-1, VPC-2 et VPC-3. Auparavant, seul VPC-0 pouvait être un VPC partagé. Cette modification est prise en charge avec Cloud Volumes ONTAP 9.8 et versions ultérieures.

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

## 4 janv. 2021

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

### Avant-postes AWS

Il y a quelques mois, nous avons annoncé que Cloud Volumes ONTAP avait obtenu la désignation Amazon Web Services (AWS) Outposts Ready. Aujourd'hui, nous sommes heureux d'annoncer que nous avons validé BlueXP et Cloud Volumes ONTAP avec AWS Outposts.

Si vous disposez d'un Outpost AWS, vous pouvez déployer Cloud Volumes ONTAP dans cet Outpost en sélectionnant le VPC Outpost dans l'assistant Environnement de travail. L'expérience est la même que pour tout autre VPC résidant dans AWS. Notez que vous devrez d'abord déployer un connecteur dans votre AWS Outpost.

Il y a quelques limitations à souligner :

- Seuls les systèmes Cloud Volumes ONTAP à nœud unique sont actuellement pris en charge
- Les instances EC2 que vous pouvez utiliser avec Cloud Volumes ONTAP sont limitées à ce qui est disponible dans votre Outpost
- Seuls les SSD à usage général (gp2) sont actuellement pris en charge

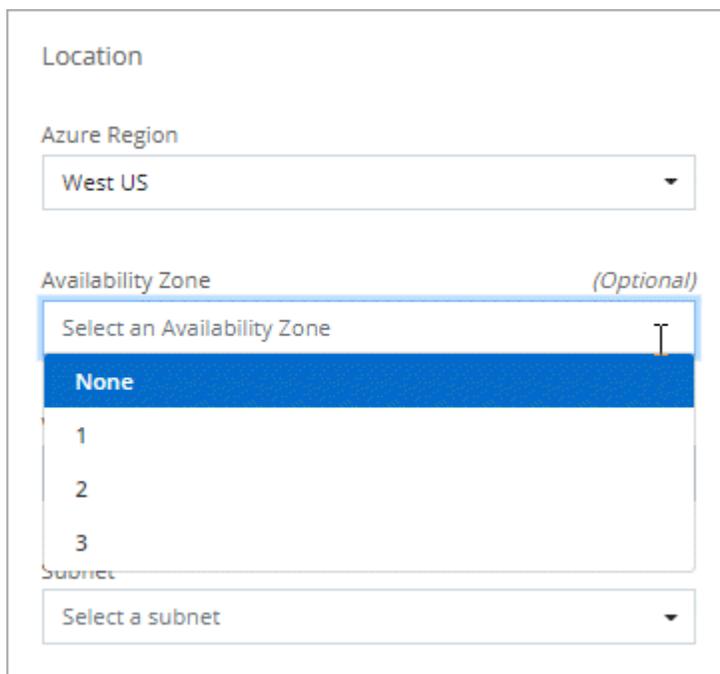
### Ultra SSD VNVRAM dans les régions Azure prises en charge

Cloud Volumes ONTAP peut désormais utiliser un SSD Ultra comme VNVRAM lorsque vous utilisez le type de machine virtuelle E32s\_v3 avec un système à nœud unique ["dans n'importe quelle région Azure prise en charge"](#) .

La VNVRAM offre de meilleures performances d'écriture.

### Choisir 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 nœud unique. Si vous ne sélectionnez pas d'AZ, BlueXP en sélectionnera un pour vous.



Location

Azure Region

West US

Availability Zone *(Optional)*

Select an Availability Zone

None

1

2

3

Subnet

Select a subnet

### Disques plus grands dans Google Cloud

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



La capacité maximale du système 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 machines suivants :

- n2-standard-4 avec la licence Explore et avec BYOL
- n2-standard-8 avec la licence Standard et avec BYOL
- n2-standard-32 avec la licence Premium et avec BYOL

## 3 novembre 2020

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

### Azure Private Link pour Cloud Volumes ONTAP

Par défaut, BlueXP active désormais une connexion Azure Private Link entre Cloud Volumes ONTAP et ses comptes de stockage associés. Un lien privé sécurise les connexions entre les points de terminaison dans Azure.

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

## Limitations connues

Les limitations connues identifient les plates-formes, les appareils ou les fonctions qui ne sont pas pris en charge par cette version du produit ou qui n'interagissent pas correctement avec elle. Examinez attentivement ces limitations.

Ces limitations sont spécifiques à la gestion de Cloud Volumes ONTAP dans la console NetApp . Pour afficher les limitations du logiciel Cloud Volumes ONTAP lui-même, ["Accédez aux notes de publication de Cloud Volumes ONTAP"](#) .

### La console ne prend pas en charge la création de volumes FlexGroup

Bien que Cloud Volumes ONTAP prenne en charge les volumes FlexGroup , la console ne prend actuellement pas en charge la création de volumes FlexGroup . Si vous créez un volume FlexGroup à partir d' ONTAP System Manager ou de l' ONTAP CLI, vous devez définir le mode de gestion de la capacité dans la console sur `Manual` . `Automatic` le mode peut ne pas fonctionner correctement avec les volumes FlexGroup .



La possibilité de créer des volumes FlexGroup dans la console est prévue pour une future version.

### La console ne prend pas en charge S3 avec Cloud Volumes ONTAP

Bien que Cloud Volumes ONTAP prenne en charge S3 comme option de stockage évolutif, la console ne fournit aucune capacité de gestion pour cette fonctionnalité. L'utilisation de l'interface de ligne de commande est la meilleure pratique pour configurer l'accès client S3 à partir de Cloud Volumes ONTAP. Pour plus de détails, reportez-vous à la ["Guide d'alimentation de configuration S3"](#) .

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

### La console ne prend pas en charge la reprise après sinistre pour les machines virtuelles de stockage

La console ne fournit aucune configuration ni support d'orchestration pour la reprise après sinistre de la

machine virtuelle de stockage (SVM). Vous devez utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP .

["En savoir plus sur la reprise après sinistre SVM"](#) .

## **Notes de version de Cloud Volumes ONTAP**

Les notes de publication 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 pouvant affecter les fonctionnalités du produit.

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

# Commencer

## En savoir plus sur Cloud Volumes ONTAP

Cloud Volumes ONTAP vous permet d'optimiser vos coûts et vos performances de stockage cloud tout en améliorant la protection, la sécurité et la conformité des données.

Cloud Volumes ONTAP est un dispositif de stockage uniquement logiciel qui exécute le logiciel de gestion de données ONTAP dans le cloud. Il offre un stockage de niveau professionnel avec les fonctionnalités clés suivantes :

- Efficacité du stockage

Tirez parti de la déduplication des données intégrée, de la compression des données, du provisionnement fin et du clonage pour minimiser les coûts de stockage.

- Haute disponibilité

Assurez la fiabilité de l'entreprise et la continuité des opérations en cas de panne de votre environnement cloud.

- Protection des données

Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication de pointe de NetApp, pour répliquer les données locales vers le cloud. Il est donc facile de disposer de copies secondaires disponibles pour plusieurs cas d'utilisation.

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

["En savoir plus sur la sauvegarde et la récupération"](#)

- hiérarchisation des données

Basculez entre les pools de stockage hautes et basses performances à la demande sans mettre les applications hors ligne.

- Cohérence des applications

Assurez la cohérence des copies NetApp Snapshot à l'aide de NetApp SnapCenter.

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

- Sécurité des données

Cloud Volumes ONTAP prend en charge le cryptage des données et offre une protection contre les virus et les ransomwares.

- Contrôles de conformité en matière de confidentialité

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

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



Les licences pour les fonctionnalités ONTAP sont incluses avec Cloud Volumes ONTAP.

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

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

## Versions ONTAP prises en charge pour les déploiements Cloud Volumes ONTAP

La console NetApp vous permet de choisir parmi plusieurs versions ONTAP différentes lorsque vous ajoutez un système Cloud Volumes ONTAP .

Les versions de Cloud Volumes ONTAP autres que celles répertoriées ici ne sont pas disponibles pour les nouveaux déploiements. Pour plus d'informations sur la mise à niveau, reportez-vous à ["Chemins de mise à niveau pris en charge"](#) .

### AWS

#### Nœud unique

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

#### paire HA

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA

- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

## **Azuré**

### **Nœud unique**

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9,8 P10
- 9.7 P6
- 9,5 P6

### **paire HA**

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9,8 P10
- 9.7 P6

## **Google Cloud**

### **Nœud unique**

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5

### **paire HA**

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA

- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8

## Démarrer avec Amazon Web Services

### Démarrage rapide de Cloud Volumes ONTAP dans AWS

Démarrez avec Cloud Volumes ONTAP dans AWS en quelques étapes.

1

#### Créer un agent de console

Si vous n'avez pas de ["Agent de console"](#) mais il faut en créer un. ["Découvrez comment créer un agent de console dans AWS"](#) .

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

2

#### Planifiez votre configuration

La console propose des packages préconfigurés qui correspondent à vos exigences de charge de travail, ou vous pouvez créer votre propre configuration. Si vous choisissez votre propre configuration, vous devez comprendre les options qui s'offrent à vous. ["Apprendre encore plus"](#) .

3

#### Configurez votre réseau

1. Assurez-vous que votre VPC et vos sous-réseaux prendront en charge la connectivité entre l'agent de console et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du VPC cible pour NetApp AutoSupport.

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

3. Configurez un point de terminaison VPC sur le service S3.

Un point de terminaison VPC est requis si vous souhaitez hiérarchiser les données froides de Cloud Volumes ONTAP vers un stockage d'objets à faible coût.

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

## 4

### Configurer AWS KMS

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 politique de clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations à l'agent de la console en tant qu'utilisateur clé. ["Apprendre encore plus"](#) .

## 5

### Lancer Cloud Volumes ONTAP à l'aide de la console

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

#### Liens connexes

- ["Créer un agent de console pour AWS"](#)
- ["Créer un agent de console à partir d'AWS Marketplace"](#)
- ["Installer et configurer un agent de console sur site"](#)
- ["Autorisations AWS pour l'agent de la console"](#)

## Planifiez votre configuration Cloud Volumes ONTAP dans AWS

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

### Choisissez une licence Cloud Volumes ONTAP

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

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

### Choisissez une région prise en charge

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

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

### Choisissez une zone locale prise en charge

La sélection d'une zone locale est facultative. Cloud Volumes ONTAP est pris en charge dans certaines zones locales AWS, notamment Singapour. Cloud Volumes ONTAP dans AWS prend en charge uniquement le mode haute disponibilité (HA) dans une seule zone de disponibilité. Les déploiements à nœud unique ne sont pas pris en charge.



Cloud Volumes ONTAP ne prend pas en charge la hiérarchisation des données et la hiérarchisation du cloud dans les zones locales AWS. De plus, les zones locales avec des instances qui n'ont pas été qualifiées pour Cloud Volumes ONTAP ne sont pas prises en charge. Miami en est un exemple : elle n'est pas disponible en tant que zone locale, car elle ne contient que des instances Gen6 qui ne sont ni prises en charge ni qualifiées.

["Documentation AWS : afficher la liste complète des zones locales"](#) . Les zones locales doivent être activées avant de pouvoir créer et gérer des ressources dans ces zones.

["Documentation AWS : Premiers pas avec les zones locales AWS"](#) .

## Choisissez une instance prise en charge

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

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

## Comprendre les limites de stockage

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

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

## Dimensionnez votre système dans AWS

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

### Type d'instance

- Adaptez vos exigences de charge de travail au débit maximal et aux IOPS pour chaque type d'instance EC2.
- Si plusieurs utilisateurs écrivent sur le système en même temps, choisissez un type d'instance disposant de suffisamment de processeurs pour gérer les requêtes.
- Si vous avez une application qui est principalement destinée à la lecture, choisissez un système avec suffisamment de 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 des disques EBS, reportez-vous à ["Documentation AWS : Types de volumes EBS"](#) .

- Les disques SSD à usage général (gp3) sont les SSD les moins chers qui équilibrent coût et performances pour une large gamme de charges de travail. Les performances sont définies en termes d'IOPS et de débit. Les disques gp3 sont pris en charge avec Cloud Volumes ONTAP 9.7 et versions ultérieures.

Lorsque vous sélectionnez un disque gp3, la console NetApp renseigne les valeurs d'IOPS et de débit

par défaut qui fournissent des performances équivalentes à celles d'un disque gp2 en fonction de la taille du disque sélectionné. Vous pouvez augmenter les valeurs pour obtenir de meilleures performances à un coût plus élevé, mais nous ne prenons pas en charge les valeurs inférieures car cela peut entraîner des performances inférieures. En bref, conservez les valeurs par défaut ou augmentez-les. Ne les baissez pas. "[Documentation AWS : 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 les disques gp3. "[En savoir plus sur la prise en charge d'Elastic Volumes](#)".

- Les disques SSD à usage général (gp2) équilibrent coût et performances pour une large gamme de charges de travail. Les performances sont définies en termes d'IOPS.
- Les disques SSD *IOPS provisionnés (io1)* sont destinés aux applications critiques qui nécessitent des performances optimales à un coût plus élevé.

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

- Les disques durs *Throughput Optimized HDD (st1)* sont destinés aux charges de travail fréquemment consultées qui nécessitent un débit rapide et constant à un prix inférieur.



La hiérarchisation des données vers AWS S3 n'est pas disponible dans les zones locales AWS en raison du manque de connectivité.

## Taille du disque EBS

Si vous choisissez une configuration qui ne prend pas en charge le "[Fonctionnalité Amazon EBS Elastic Volumes](#)", vous devez alors choisir une taille de disque initiale lorsque vous lancez un système Cloud Volumes ONTAP. Après cela, vous pouvez "[laissez la console gérer la capacité d'un système pour vous](#)", mais si tu veux "[crées vous-même des agrégats](#)", soyez conscient de ce qui suit :

- Tous les disques d'un agrégat doivent avoir la même taille.
- Les performances des disques EBS sont liées à la taille du disque. La taille détermine les IOPS de base et la durée maximale de rafale pour les disques SSD et le débit de base et de rafale pour les disques HDD.
- En fin de compte, vous devez choisir la taille de disque qui vous offre les *performances soutenues* dont vous avez besoin.
- Même si vous choisissez des disques plus grands (par exemple, six disques de 4 Tio), vous risquez de ne pas obtenir toutes les IOPS, car l'instance EC2 peut atteindre sa limite de bande passante.

Pour plus de détails sur les performances du disque EBS, reportez-vous à "[Documentation AWS : Types de volumes EBS](#)".

Comme indiqué ci-dessus, le choix d'une 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 des données utilisateur, la console achète également du stockage cloud pour les données système Cloud Volumes ONTAP (données de démarrage, données racine, données principales et NVRAM). À des fins de planification, il peut être utile de vérifier ces détails avant de déployer Cloud Volumes ONTAP.

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



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

## Préparez-vous à déployer Cloud Volumes ONTAP dans un AWS Outpost

Si vous disposez d'un AWS Outpost, vous pouvez déployer Cloud Volumes ONTAP dans cet Outpost en sélectionnant le VPC Outpost pendant le processus de déploiement. L'expérience est la même que pour tout autre VPC résidant dans AWS. Notez que vous devrez d'abord déployer un agent de console dans votre AWS Outpost.

Il y a quelques limitations à souligner :

- Seuls les systèmes Cloud Volumes ONTAP à nœud unique sont actuellement pris en charge
- Les instances EC2 que vous pouvez utiliser avec Cloud Volumes ONTAP sont limitées à ce qui est disponible dans votre Outpost
- Seuls les SSD à usage général (gp2) sont actuellement pris en charge

## Recueillir des informations sur le réseau

Lorsque vous lancez Cloud Volumes ONTAP dans AWS, vous devez spécifier les détails de votre réseau VPC. Vous pouvez utiliser une feuille de travail pour recueillir les informations auprès de votre administrateur.

### Nœud unique ou paire HA dans une seule AZ

Informations sur les AWS	Votre valeur
Région	
VPC	
Sous-réseau	
Groupe de sécurité (si vous utilisez le vôtre)	

### Paire HA dans plusieurs AZ

Informations sur les AWS	Votre valeur
Région	
VPC	
Groupe de sécurité (si vous utilisez le vôtre)	
Zone de disponibilité du nœud 1	
Sous-réseau du nœud 1	
Zone de disponibilité du nœud 2	
Sous-réseau du nœud 2	

Informations sur les AWS	Votre valeur
Zone de disponibilité du médiateur	
Sous-réseau médiateur	
Paire de clés pour le médiateur	
Adresse IP flottante pour le port de gestion du cluster	
Adresse IP flottante pour les données sur le nœud 1	
Adresse IP flottante pour les données sur le nœud 2	
Tables de routage pour les adresses IP flottantes	

### Choisissez une vitesse d'écriture

La console 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, ainsi que les risques et les recommandations lors de l'utilisation d'une vitesse d'écriture élevée. ["En savoir plus sur la vitesse d'écriture"](#) .

### Choisissez un profil d'utilisation du volume

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

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

#### Provisionnement léger

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

#### Déduplication

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

#### Compression

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

### Configurez votre réseau

## Configurer la mise en réseau AWS pour Cloud Volumes ONTAP

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

### Exigences générales

Assurez-vous d'avoir rempli les exigences suivantes dans AWS.

### Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

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

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

### Points de terminaison Cloud Volumes ONTAP

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

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact si le point de terminaison n'est pas disponible
<a href="https://netapp-cloud-account.auth0.com">\ https://netapp-cloud-account.auth0.com</a>	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : <ul style="list-style-type: none"><li>• Services Cloud Volumes ONTAP</li><li>• Services ONTAP</li><li>• Protocoles et services proxy</li></ul>
<a href="https://api.bluexp.netapp.com/tenancy">\ https://api.bluexp.netapp.com/tenancy</a>	Location	Utilisé pour récupérer la ressource Cloud Volumes ONTAP à partir de la console pour autoriser les ressources et les utilisateurs.	Modes standard et restreint.	Les ressources Cloud Volumes ONTAP et les utilisateurs ne sont pas autorisés.

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact si le point de terminaison n'est pas disponible
<p>\</p> <p><a href="https://mysupport.net/app.com/aods/asupmessage">https://mysupport.net/app.com/aods/asupmessage</a> \</p> <p><a href="https://mysupport.net/app.com/asupprod/post/1.0/postAsup">https://mysupport.net/app.com/asupprod/post/1.0/postAsup</a></p>	AutoSupport	Utilisé pour envoyer des données de télémétrie AutoSupport au support NetApp .	Modes standard et restreint.	Les informations AutoSupport ne sont toujours pas livrées.
<p>Le point de terminaison commercial exact pour le service AWS (suffixé avec amazonaws.com) dépend de la région AWS que vous utilisez. Reportez-vous à la "Documentation AWS pour plus de détails" .</p>	<ul style="list-style-type: none"> <li>• CloudFormation</li> <li>• Cloud de calcul élastique (EC2)</li> <li>• Gestion des identités et des accès (IAM)</li> <li>• Service de gestion des clés (KMS)</li> <li>• Service de jetons de sécurité (STS)</li> <li>• Service de stockage simple (S3)</li> </ul>	Communication avec les services AWS.	Modes standard et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service AWS pour effectuer des opérations spécifiques dans AWS.
<p>Le point de terminaison gouvernemental exact pour le service AWS dépend de la région AWS que vous utilisez. Les points de terminaison sont suffixés par amazonaws.com et c2s.ic.gov . Se référer à "Kit de développement logiciel (SDK) AWS" et "Documentation AWS" pour plus d'informations.</p>	<ul style="list-style-type: none"> <li>• CloudFormation</li> <li>• Cloud de calcul élastique (EC2)</li> <li>• Gestion des identités et des accès (IAM)</li> <li>• Service de gestion des clés (KMS)</li> <li>• Service de jetons de sécurité (STS)</li> <li>• Service de stockage simple (S3)</li> </ul>	Communication avec les services AWS.	Mode restreint.	Cloud Volumes ONTAP ne peut pas communiquer avec le service AWS pour effectuer des opérations spécifiques dans AWS.

### Accès Internet sortant pour le médiateur HA

L'instance de médiateur HA doit disposer d'une connexion sortante au service AWS EC2 afin de pouvoir 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 point de terminaison VPC d'interface du sous-réseau cible vers le service AWS EC2. Pour plus de détails sur les points de terminaison VPC, reportez-vous à la "[Documentation AWS : Points de terminaison d'interface VPC \(AWS PrivateLink\)](#)".

## Configuration du proxy réseau de l'agent de la console NetApp

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

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

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

## Adresses IP privées

La console 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 disponibles.

Le nombre de LIF que la console alloue à Cloud Volumes ONTAP dépend du fait que vous déployez un système à nœud unique ou une paire HA. Un LIF est une adresse IP associée à un port physique.

## Adresses IP pour un système à nœud unique

La console alloue 6 adresses IP à un seul système de nœud.

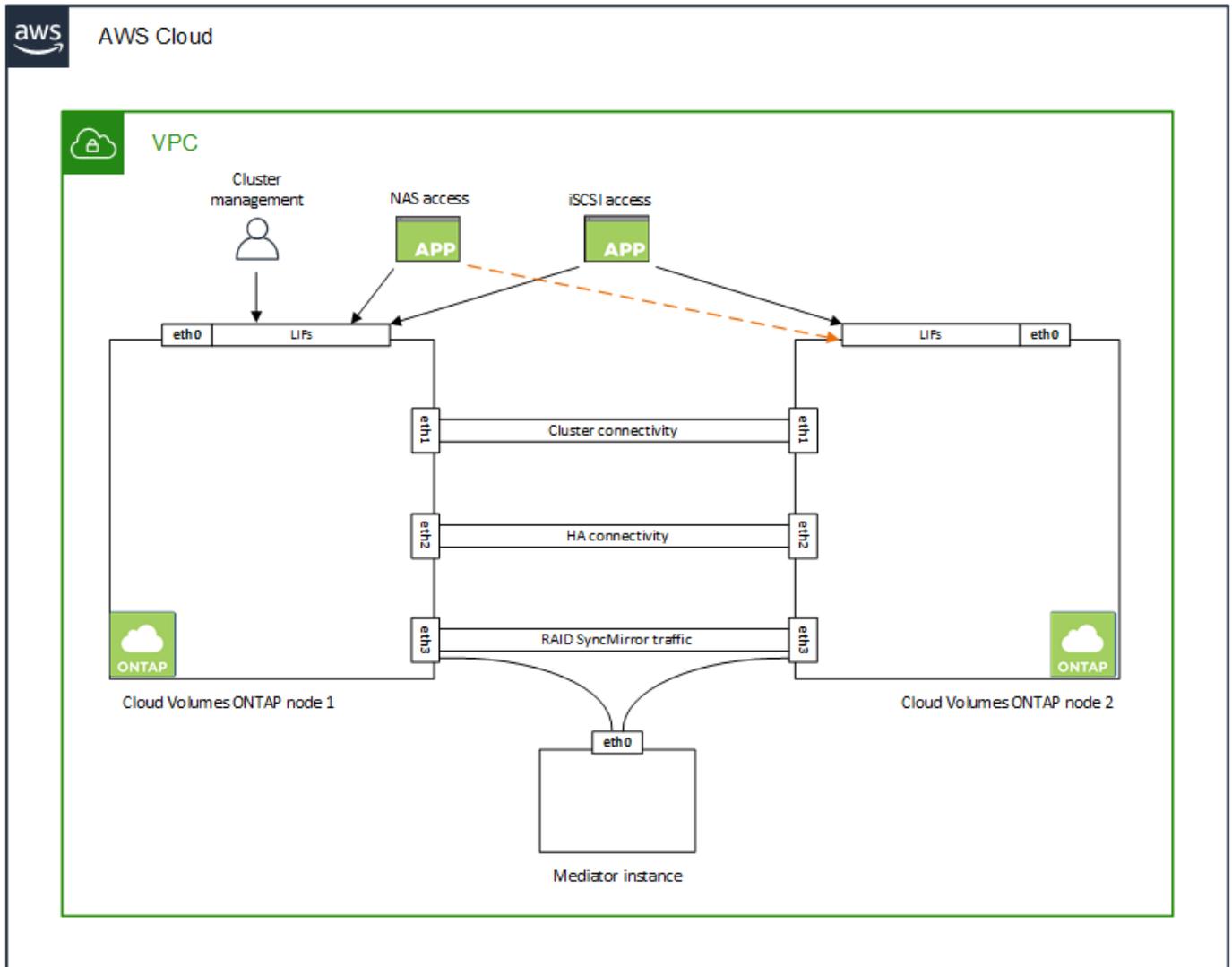
Le tableau suivant fournit des détails sur les LIF associés à chaque adresse IP privée.

FRV	But
Gestion des clusters	Gestion administrative de l'ensemble du cluster (paire HA).
Gestion des nœuds	Gestion administrative d'un nœud.
Intercluster	Communication, sauvegarde et réplication inter-cluster.
Données NAS	Accès client via les protocoles NAS.
données iSCSI	Accès client via le protocole iSCSI. Également utilisé par le système pour d'autres flux de travail réseau importants. Ce LIF est obligatoire et ne doit pas être supprimé.

<b>FRV</b>	<b>But</b>
Gestion des machines virtuelles de stockage	Un LIF de gestion de machine virtuelle de stockage est utilisé avec des outils de gestion tels que SnapCenter.

### Adresses IP pour les paires HA

Les paires HA nécessitent plus d'adresses IP qu'un système à nœud unique. 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 HA dépend du modèle de déploiement que vous choisissez. Une paire HA déployée dans une seule zone de disponibilité AWS (AZ) nécessite 15 adresses IP privées, tandis qu'une paire HA déployée dans plusieurs AZ nécessite 13 adresses IP privées.

Les tableaux suivants fournissent des détails sur les LIF associés à chaque adresse IP privée.

FRV	Interface	Nœud	But
Gestion des clusters	eth0	nœud 1	Gestion administrative de l'ensemble du cluster (paire HA).
Gestion des nœuds	eth0	nœud 1 et nœud 2	Gestion administrative d'un nœud.

FRV	Interface	Nœud	But
Intercluster	eth0	nœud 1 et nœud 2	Communication, sauvegarde et réplication inter-cluster.
Données NAS	eth0	nœud 1	Accès client via les protocoles NAS.
données iSCSI	eth0	nœud 1 et nœud 2	Accès client via le protocole iSCSI. Également utilisé par le système pour d'autres flux de travail réseau importants. Ces LIF sont obligatoires et ne doivent pas être supprimés.
Connectivité des clusters	eth1	nœud 1 et nœud 2	Permet aux nœuds de communiquer entre eux et de déplacer des données au sein du cluster.
Connectivité HA	eth2	nœud 1 et nœud 2	Communication entre les deux nœuds en cas de basculement.
Trafic iSCSI RSM	eth3	nœud 1 et nœud 2	Trafic iSCSI RAID SyncMirror , ainsi que la communication entre les deux nœuds Cloud Volumes ONTAP et le médiateur.
Médiateur	eth0	Médiateur	Un canal de communication entre les nœuds et le médiateur pour aider aux processus de prise de contrôle et de restitution du stockage.

FRV	Interface	Nœud	But
Gestion des nœuds	eth0	nœud 1 et nœud 2	Gestion administrative d'un nœud.
Intercluster	eth0	nœud 1 et nœud 2	Communication, sauvegarde et réplication inter-cluster.
données iSCSI	eth0	nœud 1 et nœud 2	Accès client via le protocole iSCSI. Ces LIF gèrent également la migration des adresses IP flottantes entre les nœuds. Ces LIF sont obligatoires et ne doivent pas être supprimés.
Connectivité des clusters	eth1	nœud 1 et nœud 2	Permet aux nœuds de communiquer entre eux et de déplacer des données au sein du cluster.
Connectivité HA	eth2	nœud 1 et nœud 2	Communication entre les deux nœuds en cas de basculement.
Trafic iSCSI RSM	eth3	nœud 1 et nœud 2	Trafic iSCSI RAID SyncMirror , ainsi que la communication entre les deux nœuds Cloud Volumes ONTAP et le médiateur.
Médiateur	eth0	Médiateur	Un canal de communication entre les nœuds et le médiateur pour aider aux processus de prise de contrôle et de restitution du stockage.



Lorsqu'ils sont déployés dans plusieurs zones de disponibilité, plusieurs LIF sont associés à ["adresses IP flottantes"](#) , qui ne sont pas comptabilisés dans la limite d'adresse IP privée AWS.

## Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car la console le fait pour vous. Si vous devez utiliser le vôtre, reportez-vous à ["Règles du groupe de sécurité"](#) .



Vous recherchez des informations sur l'agent Console ? ["Afficher les règles du groupe de sécurité pour l'agent de la console"](#)

## Connexion pour la hiérarchisation 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 dispose d'une connexion à S3. La meilleure façon de fournir cette connexion est de créer un point de terminaison VPC pour le service S3. Pour les instructions, reportez-vous à la ["Documentation AWS : Création d'un point de terminaison de passerelle"](#) .

Lorsque vous créez le point de terminaison VPC, assurez-vous de sélectionner la région, le VPC et la table de routage qui correspondent à l'instance Cloud Volumes ONTAP . Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui autorise le trafic vers le point de terminaison S3. Sinon, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

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

## Connexions aux systèmes ONTAP

Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et des systèmes ONTAP dans d'autres réseaux, vous devez disposer d'une connexion VPN entre AWS VPC et l'autre réseau, par exemple, votre réseau d'entreprise. Pour les instructions, reportez-vous à la ["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 des ensembles d'options DHCP pour utiliser le serveur DNS EC2 par défaut, qui ne doit pas être le serveur DNS utilisé par l'environnement Active Directory.

Pour les instructions, reportez-vous à la ["Documentation AWS : Services de domaine Active Directory sur le cloud AWS : Déploiement de référence de démarrage rapide"](#) .

## Partage VPC

À partir de la version 9.11.1, les paires Cloud Volumes ONTAP HA sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre organisation 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 HA dans un sous-réseau partagé"](#) .

## Exigences relatives aux paires HA dans plusieurs AZ

Des exigences de mise en réseau AWS supplémentaires s'appliquent aux configurations Cloud Volumes ONTAP HA qui utilisent plusieurs zones de disponibilité (AZ). Vous devez examiner ces exigences avant de lancer une paire HA, car vous devez saisir les détails de mise en réseau dans la console lorsque vous ajoutez un système Cloud Volumes ONTAP .

Pour comprendre le fonctionnement des paires HA, reportez-vous à "[Paires à haute disponibilité](#)" .

### Zones de disponibilité

Ce modèle de déploiement HA utilise plusieurs AZ pour garantir une haute disponibilité de vos données. Vous devez utiliser une zone de disponibilité dédiée pour chaque instance Cloud Volumes ONTAP et l'instance médiatrice, 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 des clusters/SVM

Les configurations HA dans plusieurs AZ utilisent des adresses IP flottantes qui migrent entre les nœuds en cas de panne. Ils ne sont pas accessibles nativement depuis l'extérieur du VPC, sauf si vous "[configurer une passerelle de transit AWS](#)" .

Une adresse IP flottante est destinée à la gestion du cluster, une autre aux données NFS/CIFS sur le nœud 1 et une autre aux données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante pour la gestion SVM est facultative.



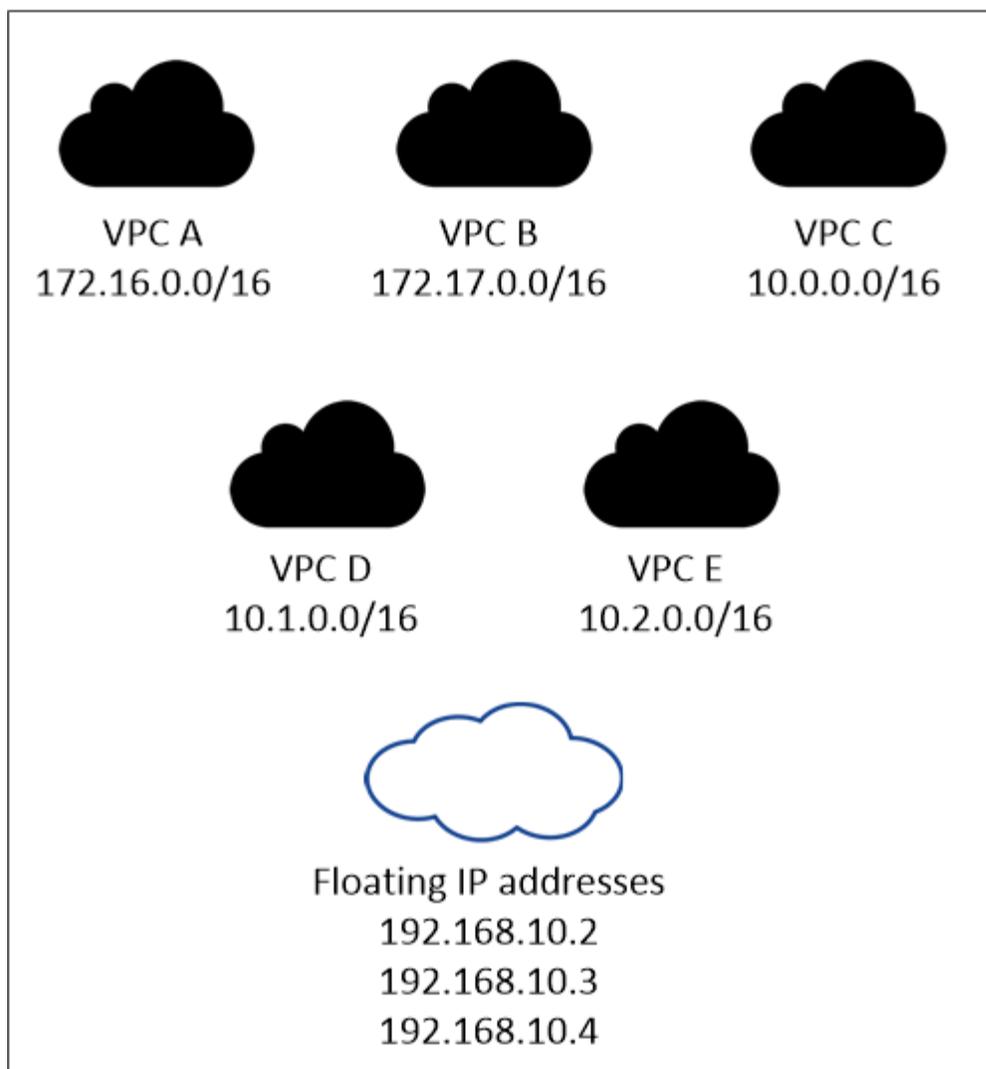
Une adresse IP flottante est requise pour le LIF de gestion SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire HA.

Vous devez saisir les adresses IP flottantes lorsque vous ajoutez un système Cloud Volumes ONTAP HA. La console alloue les adresses IP à la paire HA lorsqu'elle lance le système.

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

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

## AWS region



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

### Passerelle de transit pour permettre l'accès IP flottant depuis l'extérieur du VPC

Si nécessaire, "[configurer une passerelle de transit AWS](#)" pour permettre l'accès aux adresses IP flottantes d'une paire HA depuis l'extérieur du VPC où réside la paire HA.

### Tables de routage

Après avoir spécifié les adresses IP flottantes, vous êtes invité à sélectionner les tables de routage qui doivent inclure les itinéraires vers les adresses IP flottantes. Cela permet au client d'accéder à la paire HA.

Si vous n'avez qu'une seule table de routage pour les sous-réseaux de votre VPC (la table de routage principale), la console ajoute automatiquement les adresses IP flottantes à cette table de routage. Si vous disposez de plusieurs tables de routage, il est très important de sélectionner les tables de routage correctes lors du lancement de la paire HA. Sinon, certains clients risquent de ne pas avoir accès à Cloud Volumes ONTAP.

Par exemple, vous pouvez avoir deux sous-réseaux associés à des tables de routage différentes. 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 le peuvent pas.

Pour plus d'informations sur les tables de routage, reportez-vous à la "[Documentation AWS : Tables de routage](#)".

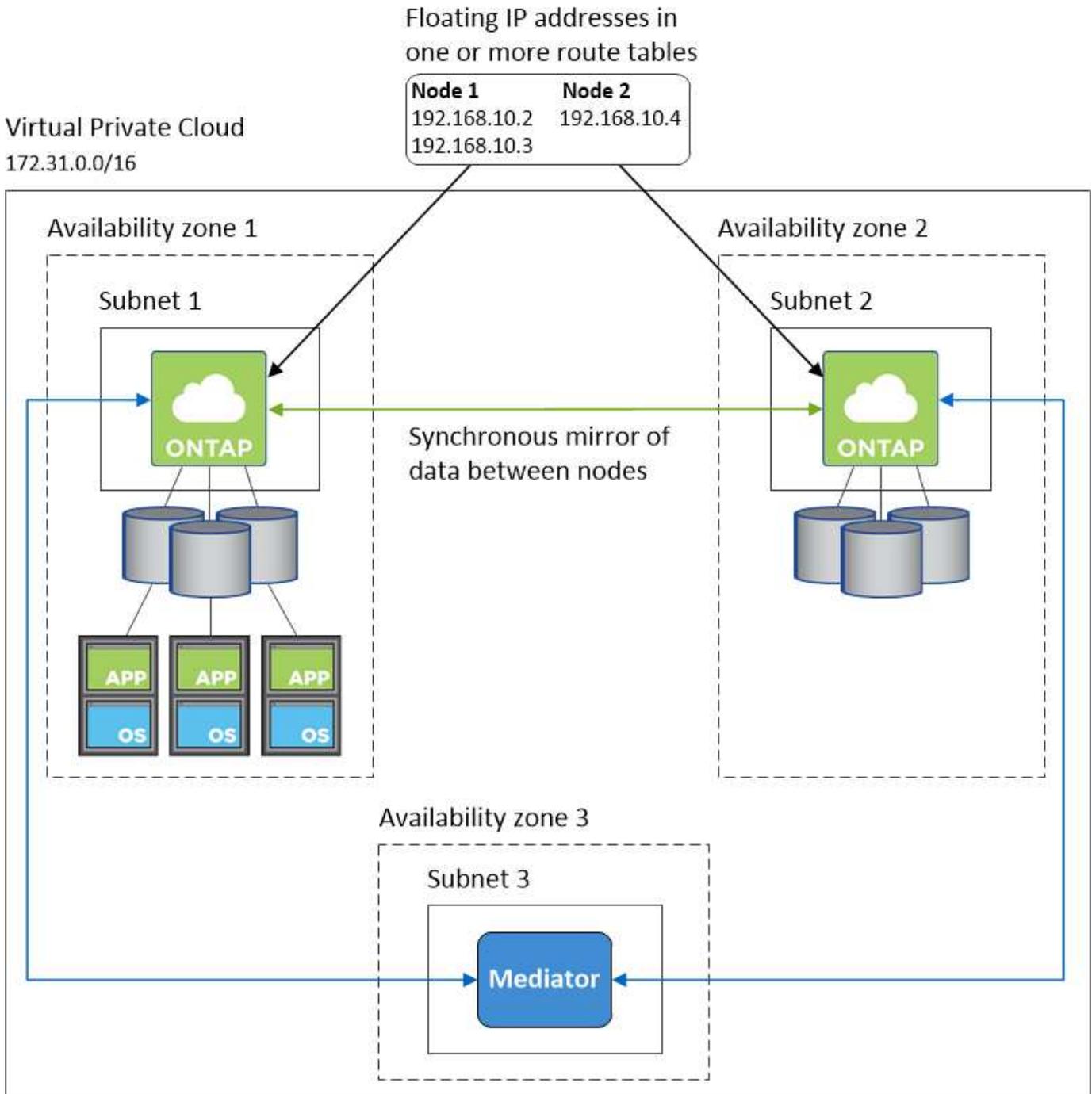
### Connexion aux outils de gestion NetApp

Pour utiliser les outils de gestion NetApp avec des configurations HA situées dans plusieurs zones de disponibilité, vous disposez de deux options de connexion :

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

### Exemple de configuration HA

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



### Exigences pour l'agent de console

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

- ["Afficher les exigences réseau pour l'agent de console"](#)
- ["Règles de groupe de sécurité dans AWS"](#)

### Sujets connexes

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

## Configurer une passerelle de transit AWS pour les paires Cloud Volumes ONTAP HA

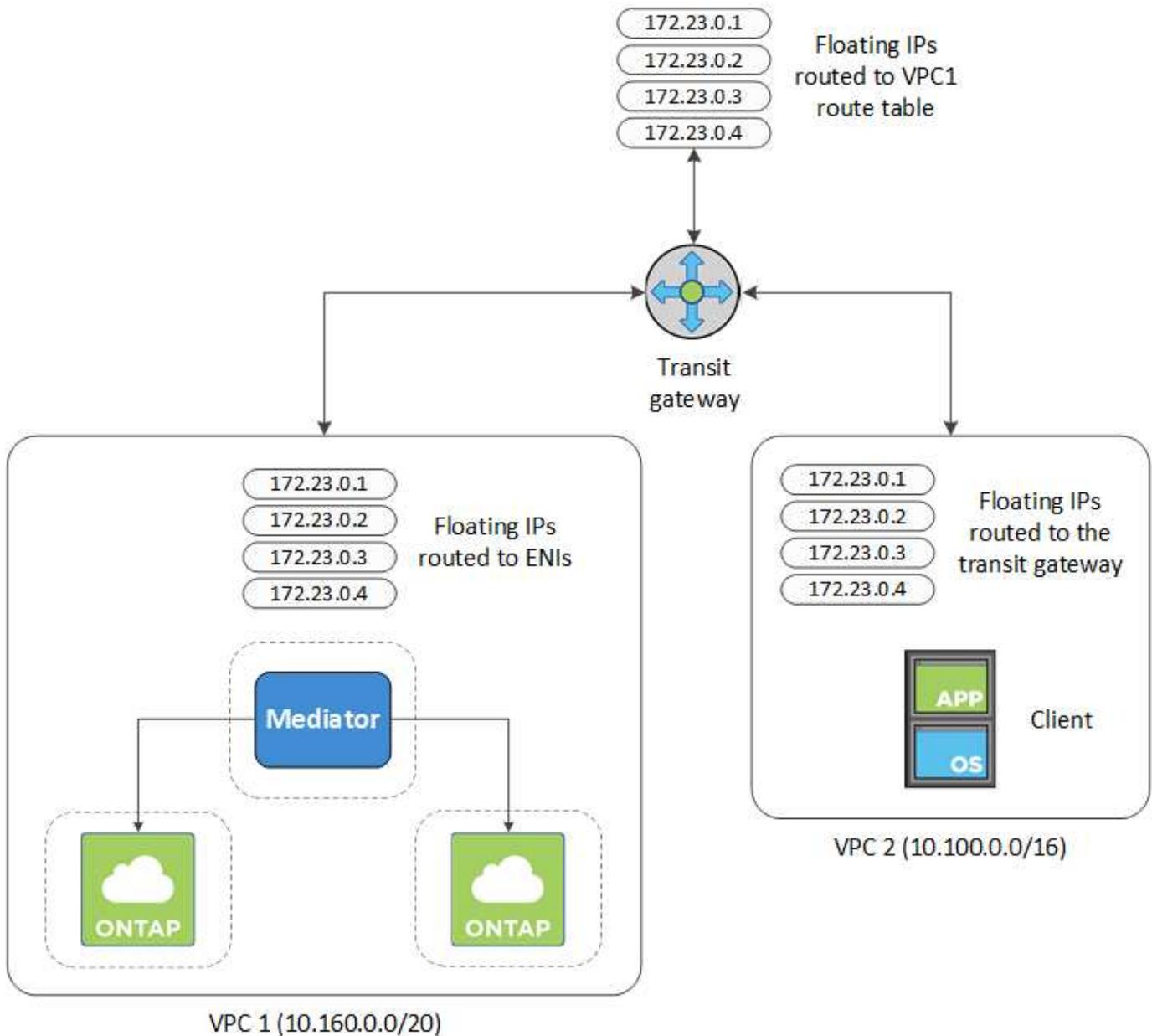
Configurer une passerelle de transit AWS pour permettre l'accès à une paire HA "adresses IP flottantes" depuis l'extérieur du VPC où réside la paire HA.

Lorsqu'une configuration Cloud Volumes ONTAP HA est répartie sur plusieurs zones de disponibilité AWS, des adresses IP flottantes sont requises pour l'accès aux données NAS à partir du VPC. Ces adresses IP flottantes peuvent migrer entre les nœuds en cas de panne, mais elles ne sont pas accessibles nativement depuis l'extérieur du VPC. Des adresses IP privées distinctes permettent un accès aux données depuis l'extérieur du VPC, mais elles ne fournissent pas de basculement automatique.

Des adresses IP flottantes sont également requises pour l'interface de gestion de cluster et le LIF de gestion SVM en option.

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

Voici un exemple qui montre deux VPC connectés par une passerelle de transit. Un système HA réside dans un VPC, tandis qu'un client réside dans l'autre. Vous pouvez ensuite monter un volume NAS sur le client en utilisant l'adresse IP flottante.



Les étapes suivantes illustrent comment configurer une configuration similaire.

### Étapes

1. "Créez une passerelle de transit et attachez 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 **Tables de routage de passerelle de transit**.
  - b. Sélectionnez la table de routage.
  - c. Cliquez sur **Associations** puis sélectionnez **Créer une association**.
  - d. Choisissez les pièces jointes (les VPC) à associer puis cliquez sur **Créer une association**.
3. Créez des itinéraires dans la table de routage de la passerelle de transit en spécifiant les adresses IP flottantes de la paire HA.

Vous pouvez trouver les adresses IP flottantes sur la page d'informations système de la console NetApp .  
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 de la passerelle de transit. Il comprend des itinéraires vers les blocs CIDR des deux VPC et quatre adresses IP flottantes utilisées par Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

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

Create route Replace route Delete route

Filter by attributes or search by keyword

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

**Floating IP Addresses**

4. Modifiez la table de routage des VPC qui doivent accéder aux adresses IP flottantes.

- Ajoutez des entrées d'itinéraire aux adresses IP flottantes.
- Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

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

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

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

VPC1  
Floating IP Addresses

- Modifiez la table de routage du VPC de la paire HA en ajoutant une route au VPC qui a besoin d'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. Il comprend un itinéraire vers les adresses IP flottantes et vers le VPC 2, où réside un client. La console a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire HA.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

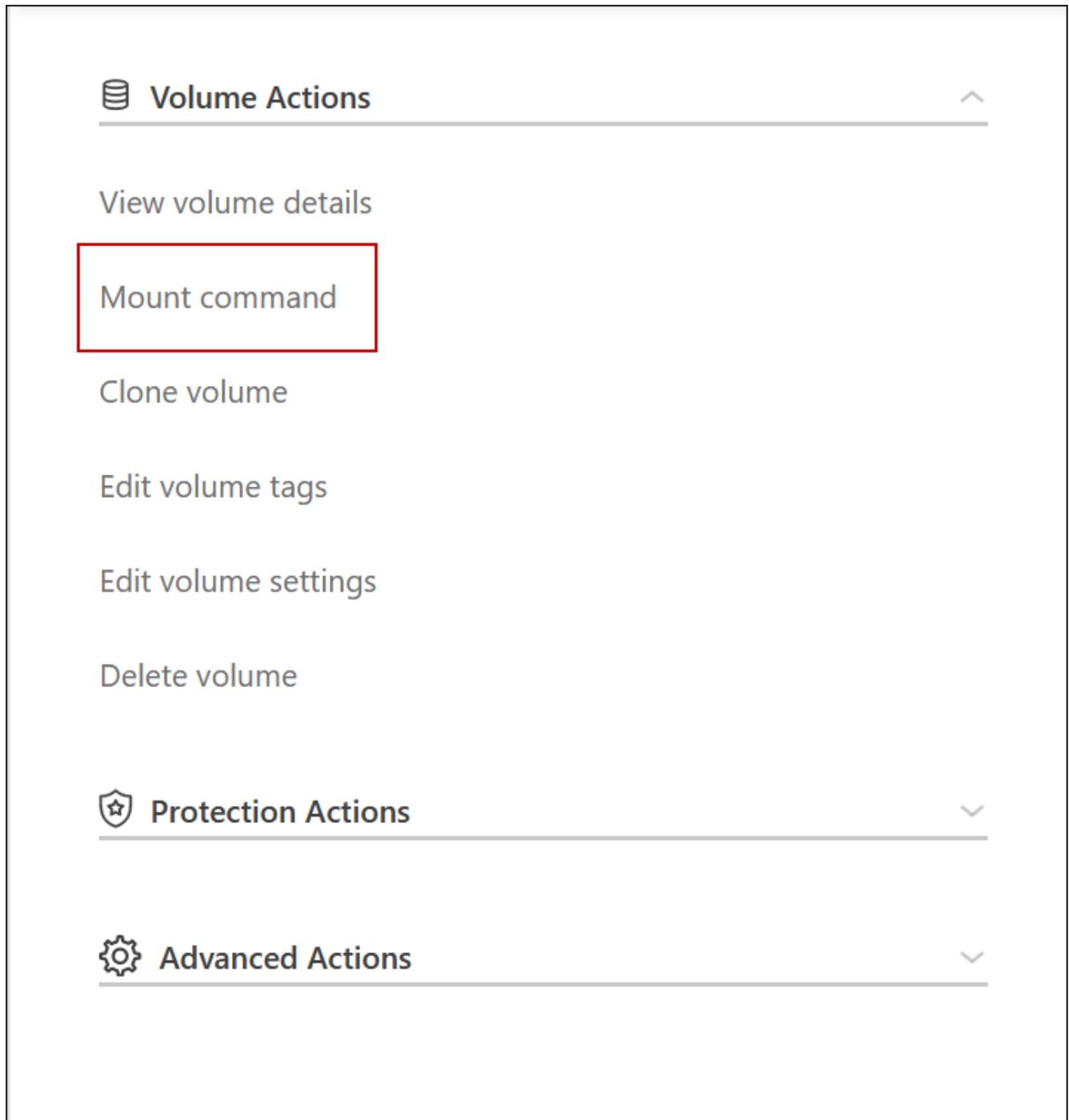
Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active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

VPC2  
Floating IP Addresses

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

Vous pouvez trouver l'adresse IP correcte dans la console via l'option **Commande de montage** sous le

panneau Gérer les volumes dans la console.



8. Si vous montez un volume NFS, configurez la stratégie d'exportation pour qu'elle corresponde au sous-réseau du VPC client.

["Apprenez à modifier un volume"](#) .

#### Liens connexes

- ["Paires à haute disponibilité dans AWS"](#)
- ["Exigences réseau pour Cloud Volumes ONTAP dans AWS"](#)

## Déployer des paires Cloud Volumes ONTAP HA dans un sous-réseau partagé AWS

À partir de la version 9.11.1, les paires Cloud Volumes ONTAP HA sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre organisation 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 VPC](#)", une configuration Cloud Volumes ONTAP HA est répartie sur deux comptes :

- Le compte propriétaire du VPC, qui possède 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 (cela inclut 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 du 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 :



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

["Consultez les règles du groupe de sécurité pour Cloud Volumes ONTAP"](#) . Notez que vous n'avez pas besoin de créer un groupe de sécurité pour le médiateur HA. La console le fait pour vous.

3. Dans le compte propriétaire du 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 pour créer un nouveau système Cloud Volumes ONTAP .

Notez que vous devez spécifier les champs suivants :

- « securityGroupId »

Le champ « securityGroupId » doit spécifier le groupe de sécurité que vous avez créé dans le compte propriétaire du VPC (voir l'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 du VPC (voir l'étape 3 ci-dessus).

Par exemple:

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

+

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

## Configurer la création de groupes de placement pour les paires Cloud Volumes ONTAP HA dans les zones de disponibilité uniques AWS

Les déploiements haute disponibilité (HA) de Cloud Volumes ONTAP dans la zone de disponibilité unique (AZ) AWS peuvent échouer et revenir en arrière si la création du groupe de placement échoue. La création du groupe de placement échoue également et le déploiement est annulé si le nœud Cloud Volumes ONTAP et l'instance du médiateur

ne sont pas disponibles. Pour éviter cela, vous pouvez modifier la configuration pour permettre au déploiement de se terminer même si la création du groupe de placement échoue.

En contournant le processus de restauration, le processus de déploiement de Cloud Volumes ONTAP se termine avec succès et vous avertit que la création du groupe de placement est incomplète.

### Étapes

1. Utilisez SSH pour vous connecter à l'hôte de l'agent de la console NetApp et vous connecter.
2. Accéder à `/opt/application/netapp/cloudmanager/docker_occm/data`.
3. Modifier `app.conf` en changeant la valeur de la `rollback-on-placement-group-failure` paramètre à `false`. La valeur par défaut de ce paramètre est `true`.

```
{
  "occm" : {
    "aws" : {
      "rollback-on-placement-group-failure" : false
    }
  }
}
```

4. Enregistrez le fichier et déconnectez-vous de l'agent de la console. Vous n'avez pas besoin de redémarrer l'agent de la console.

### Règles entrantes et sortantes du groupe de sécurité AWS pour Cloud Volumes ONTAP

La console NetApp crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes dont Cloud Volumes ONTAP a besoin pour fonctionner correctement. Vous souhaitez peut-être vous référer aux ports à des fins de test ou si vous préférez utiliser vos propres groupes de sécurité.

#### Règles pour Cloud Volumes ONTAP

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

#### Règles entrantes

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

Protocole	Port	But
Tous les ICMP	Tous	Ping de l'instance
HTTP	80	Accès HTTP à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
HTTPS	443	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole simple de gestion de réseau
TCP	445	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
TCP	635	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Moniteur d'état du réseau pour NFS
TCP	10000	Sauvegarde à l'aide de NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole simple de gestion de réseau
UDP	635	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Moniteur d'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

## Règles de sortie

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

## Règles de base pour les voyages sortants

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

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

### Règles sortantes avancées

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



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

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

Service	Protocole	Port	Source	Destination	But
AutoSupport	HTTPS	443	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (HTTPS est la valeur par défaut)
	HTTP	80	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (uniquement si le protocole de transport est modifié de HTTPS à HTTP)
	TCP	3128	Gestion des nœuds LIF	Agent de console	Envoi de messages AutoSupport via un serveur proxy sur l'agent de la console, si une connexion Internet sortante n'est pas disponible
Sauvegarde sur S3	TCP	5010	LIF intercluster	Point de terminaison de sauvegarde ou point de terminaison de restauration	Opérations de sauvegarde et de restauration pour la fonctionnalité de sauvegarde sur S3
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un seul nœud	Tous les LIF sur l'autre nœud	Communications intercluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	Gestion des nœuds LIF	Médiateur HA	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	Gestion des nœuds LIF	Médiateur HA	Keep alive (Cloud Volumes ONTAP HA uniquement)
Sauvegarde de configuration	HTTP	80	Gestion des nœuds LIF	http://<adresse IP de l'agent de la console>/occm/offboxconfig	Envoyer des sauvegardes de configuration à l'agent de la console. " <a href="#">Documentation ONTAP</a> "
DHCP	UDP	68	Gestion des nœuds LIF	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	Gestion des nœuds LIF	DHCP	serveur DHCP
DNS	UDP	53	Gestion des nœuds LIF et LIF de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	Gestion des nœuds LIF	Serveurs de destination	Copie NDMP
SMTP	TCP	25	Gestion des nœuds LIF	Serveur de messagerie	Alertes SMTP, peuvent être utilisées pour AutoSupport

Service	Protocole	Port	Source	Destination	But
SNMP	TCP	161	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	UDP	161	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	TCP	162	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	UDP	162	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
SnapMirror	TCP	11104	LIF intercluster	LIF intercluster ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	LIF intercluster	LIF intercluster ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	Gestion des nœuds LIF	Serveur Syslog	Messages de transfert Syslog

#### Règles pour le groupe de sécurité externe du médiateur HA

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

#### Règles entrantes

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

Protocole	Port	Source	But
TCP	3000	CIDR de l'agent de console	Accès API RESTful depuis l'agent de la console

#### Règles de sortie

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

#### Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour le médiateur HA inclut les règles sortantes suivantes.

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

## Règles sortantes avancées

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

Protocole	Port	Destination	But
HTTP	80	Adresse IP de l'agent de console sur l'instance AWS EC2	Téléchargez les mises à niveau pour le médiateur
HTTPS	443	ec2.amazonaws.com	Aide au basculement du stockage
UDP	53	ec2.amazonaws.com	Aide au basculement du stockage



Au lieu d'ouvrir les ports 443 et 53, vous pouvez créer un point de terminaison VPC d'interface à partir du sous-réseau cible vers le service AWS EC2.

## Règles pour le groupe de sécurité interne de configuration HA

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

La console crée toujours ce groupe de sécurité. Vous n'avez pas la possibilité d'utiliser le vôtre.

## Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

## Règles de sortie

Le groupe de sécurité prédéfini inclut les règles sortantes suivantes.

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

## Règles pour l'agent de console

["Afficher les règles du groupe de sécurité pour l'agent de la console"](#)

## Configurer Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans AWS

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

### Étapes

1. Assurez-vous 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 la console NetApp et Cloud Volumes ONTAP ou dans un autre compte AWS.

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

2. Modifiez la politique de clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations à la console en tant qu'utilisateur clé.

L'ajout du rôle Identity and Access Management (IAM) en tant qu'utilisateur clé donne à la console les autorisations d'utiliser la CMK avec Cloud Volumes ONTAP.

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

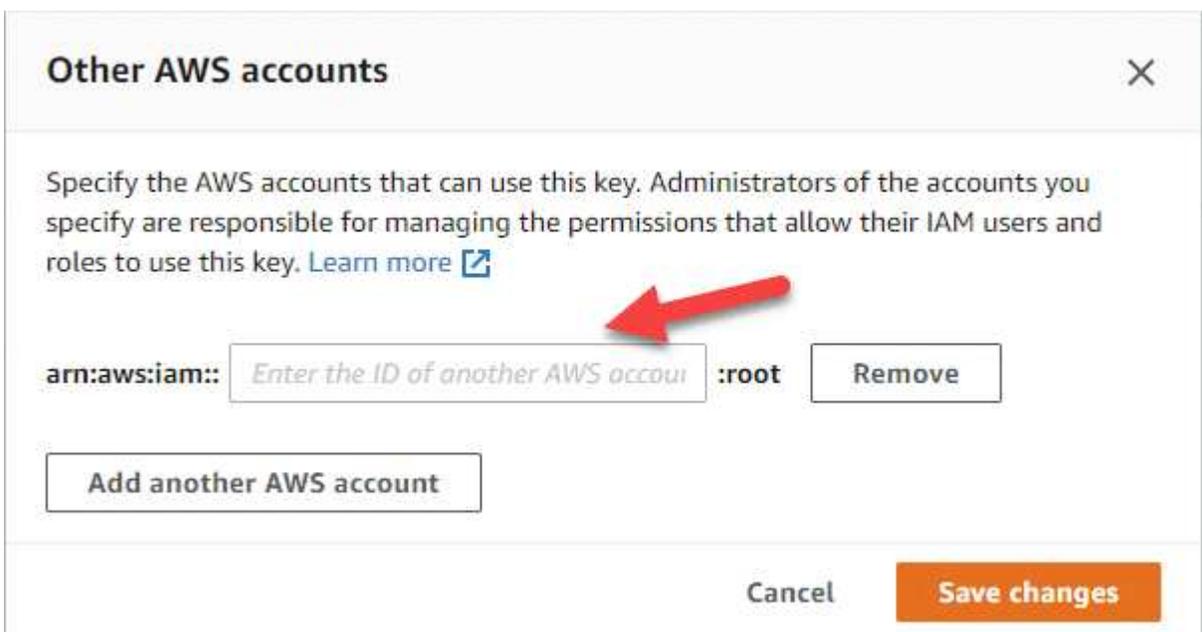
3. Si la CMK se trouve dans un autre compte AWS, procédez comme suit :

- a. Accédez à la console KMS à partir du compte sur lequel réside la CMK.
- b. Sélectionnez la clé.
- c. Dans le volet **Configuration générale**, copiez l'ARN de la clé.

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

- d. Dans le volet **Autres comptes AWS**, ajoutez le compte AWS qui fournit des autorisations à la console.

En règle générale, il s'agit du compte sur lequel la console est déployée. Si la console n'est pas installée dans AWS, utilisez le compte pour lequel vous avez fourni des clés d'accès AWS à la console.



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

La politique suivante fournit les autorisations dont la console a besoin pour utiliser la CMK à partir du compte AWS externe. Assurez-vous de modifier la région et l'ID de compte dans les sections « Ressources ».

```

{
  "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 de détails sur ce processus, reportez-vous à la ["Documentation AWS : autoriser les utilisateurs d'autres comptes à utiliser une clé KMS"](#) .

4. Si vous utilisez une CMK gérée par le client, modifiez la stratégie de clé de la CMK en ajoutant le rôle IAM Cloud Volumes ONTAP en tant qu'utilisateur clé.

Cette étape est requise si vous avez activé la hiérarchisation des données sur Cloud Volumes ONTAP et souhaitez crypter les données stockées dans le bucket S3.

Vous devrez effectuer cette étape *après* avoir déployé Cloud Volumes ONTAP, car le rôle IAM est créé lorsque vous créez un système Cloud Volumes ONTAP . (Bien sûr, vous avez la possibilité d'utiliser un rôle IAM Cloud Volumes ONTAP existant, il est donc possible d'effectuer cette étape avant.)

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

## Configurer les rôles AWS IAM pour les nœuds Cloud Volumes ONTAP

Les rôles AWS Identity and Access Management (IAM) avec les autorisations requises doivent être attachés à chaque nœud Cloud Volumes ONTAP . Il en va de même pour le médiateur HA. Il est plus simple de laisser la console NetApp créer les rôles IAM pour vous, mais vous pouvez utiliser vos propres rôles.

Cette tâche est facultative. Lorsque vous créez un système Cloud Volumes ONTAP , l'option par défaut consiste à laisser la console 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.



Il est nécessaire de fournir votre propre rôle IAM dans AWS Secret Cloud. ["Découvrez comment déployer Cloud Volumes ONTAP dans C2S"](#) .

### Étapes

1. Accédez à la console AWS IAM.
2. Créez des politiques IAM qui incluent les autorisations suivantes :
  - Politique 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"
  }
]
```

## Régions GovCloud (États-Unis)

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

## Régions top secrètes

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

## Régions secrètes

```

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

```

- Politique de sauvegarde pour les nœuds Cloud Volumes ONTAP

Si vous prévoyez d'utiliser NetApp Backup and Recovery avec vos systèmes Cloud Volumes ONTAP , le rôle IAM des nœuds doit inclure la deuxième stratégie 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"
    }
  ]
}
```

## Régions GovCloud (États-Unis)

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

## Régions top secrètes

```

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

```

## Régions secrètes

```

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

```

- Médiateur HA

```

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

```

3. Créez un rôle IAM et attachez les stratégies que vous avez créées au rôle.

### Résultat

Vous disposez désormais de rôles IAM que vous pouvez sélectionner lorsque vous créez un nouveau système Cloud Volumes ONTAP .

### Plus d'informations

- ["Documentation AWS : Création de politiques IAM"](#)
- ["Documentation AWS : Création de rôles IAM"](#)

## Configurer les licences pour Cloud Volumes ONTAP dans AWS

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

### Freemium

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

### Étapes

1. Dans le menu de navigation de gauche de la console NetApp , sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

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

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

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

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

### Licence basée sur la capacité

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

Les forfaits Essentiels et Professionnel sont disponibles avec les modèles de consommation suivants :

- Une licence (apportez votre propre licence (BYOL)) achetée auprès de NetApp
- Un abonnement horaire à la carte (PAYGO) de la place de marché AWS
- Un contrat annuel de la place de marché AWS

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

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

#### Apportez votre propre vin

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

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

#### Étapes

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

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

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

3. Sur la page **Systèmes** de la console, cliquez sur **Ajouter un système** et suivez les étapes.

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

La licence que vous avez achetée auprès de NetApp est toujours facturée en premier, mais vous serez facturé au tarif horaire du marché si vous dépassez votre capacité sous licence ou si la durée de votre licence expire.

**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 être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des 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 les instructions étape par étape pour lancer Cloud Volumes ONTAP dans AWS"](#) .

### Abonnement PAYGO

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

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

### Étapes

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

### Select Charging Method

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

"Consultez les instructions étape par étape 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. "[Apprenez à gérer vos comptes et abonnements AWS](#)"

### Contrat annuel

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

Semblable à un abonnement horaire, la console vous invite à souscrire au contrat annuel disponible sur AWS Marketplace.

### Étapes

1. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les 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 être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des 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 les instructions étape par étape pour lancer Cloud Volumes ONTAP dans AWS"](#) .

### Abonnement Keystone

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

#### Étapes

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

### Select Charging Method

KeystoneBy capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 ▾

ProfessionalBy capacity ▾

EssentialBy capacity ▾

Freemium (Up to 500 GiB)By capacity ▾

Per NodeBy node ▾

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

## Déployer Cloud Volumes ONTAP dans AWS à l'aide d'un déploiement rapide

Vous pouvez déployer Cloud Volumes ONTAP dans AWS à l'aide d'une méthode de déploiement rapide pour les configurations à nœud unique et à haute disponibilité (HA). Ce processus simplifié réduit les étapes de déploiement par rapport à la méthode avancée. Il offre également plus de clarté dans le flux de travail en définissant automatiquement des valeurs par défaut sur une seule page et en minimisant la navigation.

### Avant de commencer

Vous avez besoin des éléments suivants pour ajouter un système Cloud Volumes ONTAP dans AWS à partir de la console NetApp .

- Un agent de console opérationnel.
  - Vous devriez avoir un ["Agent de console associé à votre projet ou espace de travail"](#) .
  - ["Vous devez être prêt à laisser l'agent de la console en cours d'exécution à tout moment."](#) .
- Une compréhension de la configuration que vous souhaitez utiliser.

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

100

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

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

- DNS et Active Directory pour les configurations CIFS.

Pour plus de détails, reportez-vous à ["Exigences réseau pour Cloud Volumes ONTAP dans AWS"](#) .

### À propos de cette tâche

Immédiatement après avoir créé le système Cloud Volumes ONTAP , la console NetApp lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de succès, la console termine immédiatement l'instance, puis commence à déployer le système. Si la console ne peut pas vérifier la connectivité, la création du système échoue. L'instance de test est soit une `t2.nano` (pour la location VPC par défaut) ou un `m3.medium` (pour la location VPC dédiée).

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page Canvas, cliquez sur **Ajouter un système** et suivez les instructions.
3. Sélectionnez **Amazon Web Services > \* Cloud Volumes ONTAP\* > Ajouter un nouveau**. L'option **Création rapide** est sélectionnée par défaut.



**Quick create**  
Use the recommended and default configuration options. You can change most of these options later.



**Advanced create**  
You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

**System details** Show API request

Cloud provider account	Instance Profile   Account ID: ██████████2	▼
Name	ⓘ Action required	▼
ONTAP Credentials	ⓘ Action required	▼
Tags	0 Tags	▼

**Deployment and Configuration**

Deployment Type	Single node	▼
Network configuration	US East - N. Virginia   VPC name - 172.31.0.0/16   Subnet name - ██████████	▼

**Charging and Services**

Marketplace subscription	Sub2-ByCapacityByNodePYGO_delete_after_1234	▼
License	Freemium (Up to 500 GiB)	▼
Data services and features	Netapp Backup and Recovery	▼
NetApp Support Site account	No existing account	▼

**Summary**

Overview	▼
----------	---

Create
Cancel

## détails du système

1. **Compte fournisseur cloud** : les détails du compte sont automatiquement renseignés en fonction de l'agent de console que vous avez sélectionné. Si vous avez plusieurs comptes, sélectionnez celui que vous souhaitez utiliser. Si un agent de console n'est pas disponible, vous serez invité à "[créer un agent de console](#)".
2. **Nom** : Le nom du système. La console utilise le nom du système (cluster) pour nommer 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.
3. \* Informations d'identification ONTAP \* Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP. Vous pouvez conserver le nom d'utilisateur par défaut *admin* ou le remplacer par un nom d'utilisateur personnalisé.

4. **Tags** Les balises AWS sont des métadonnées pour vos ressources AWS. La console ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à 15 balises à partir de l'interface utilisateur lors de la création d'un système Cloud Volumes ONTAP , puis vous pouvez en ajouter davantage après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les balises, reportez-vous à ["Documentation AWS : Balisage de vos ressources Amazon EC2"](#) .

## Déploiement et configuration

1. **Type de déploiement** : sélectionnez le type de déploiement que vous souhaitez utiliser : nœud unique, haute disponibilité (HA) dans une seule zone de disponibilité (AZ) ou HA dans plusieurs AZ.
2. **Configuration réseau** : Saisissez les informations réseau que vous avez enregistrées dans le ["Feuille de travail AWS"](#) .
  - a. **Région AWS** : par défaut, la région du compte cloud associé qui dispose d'un VPC avec des ressources de sous-réseau est sélectionnée.
  - b. **VPC** : saisissez un VPC pour la région AWS avec un sous-réseau. S'il n'y a pas de sous-réseaux, la valeur par défaut du VPC est sélectionnée.
  - c. **Sous-réseau** : vous pouvez sélectionner un sous-réseau pour le VPC uniquement pour un déploiement à nœud unique ou un déploiement HA dans une seule zone de disponibilité.

## Haute disponibilité

Si vous avez sélectionné la configuration HA, saisissez les informations suivantes :

### HA dans une seule AZ

1. **Accès médiateur** : spécifiez les informations d'accès au médiateur. Le médiateur est une instance distincte qui surveille l'état de santé de la paire HA et fournit le quorum en cas de panne. Fournissez le nom de la paire de clés pour permettre à l'instance de médiateur de se connecter au service AWS EC2 et sélectionnez la méthode de connexion.

### HA dans plusieurs AZ

1. **Zones de disponibilité et médiateur** : sélectionnez les zones de disponibilité (AZ) pour chaque nœud et le médiateur ainsi que les sous-réseaux correspondants où vous souhaitez déployer la paire Cloud Volumes ONTAP HA.
2. **IP flottantes** : si vous avez choisi plusieurs AZ, spécifiez les adresses IP flottantes pour les services NFS et CIFS et la gestion du cluster et de la SVM. Les adresses IP doivent être en dehors du bloc CIDR pour tous les VPC de la région. Pour plus de détails, reportez-vous à ["Exigences réseau AWS pour Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité"](#) .
3. **Accès médiateur** : spécifiez les informations d'accès au médiateur. Le médiateur est une instance distincte qui surveille l'état de santé de la paire HA et fournit le quorum en cas de panne. Fournissez le nom de la paire de clés pour permettre à l'instance de médiateur de se connecter au service AWS EC2 et sélectionnez la méthode de connexion.
4. **Tables de routage** : si vous avez choisi plusieurs AZ, sélectionnez les tables de routage qui incluent les routes vers les adresses IP flottantes. Si vous disposez de plusieurs tables de routage, il est important de sélectionner les tables de routage correctes. Dans le cas contraire, certains clients risquent de ne pas avoir accès à la paire Cloud Volumes ONTAP HA. Pour plus d'informations sur les tables de routage, reportez-vous à la ["Documentation AWS : Tables de routage"](#) .

## Recharge et services

1. **Abonnement Marketplace** : sélectionnez l'abonnement Marketplace AWS que vous souhaitez utiliser

avec ce système Cloud Volumes ONTAP .

2. **Licence** : sélectionnez le type de licence que vous souhaitez utiliser avec ce système Cloud Volumes ONTAP . Vous pouvez choisir entre les licences Professionnelles, Essentielles et Premium. Pour plus d'informations sur les différentes licences, reportez-vous à ["En savoir plus sur les licences Cloud Volumes ONTAP"](#) .
3. **Services et fonctionnalités de données** : Gardez les services activés ou désactivez les services que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
  - ["En savoir plus sur la classification NetApp"](#)
  - ["En savoir plus sur NetApp Backup and Recovery"](#)
  - ["En savoir plus sur le stockage WORM sur Cloud Volumes ONTAP"](#)



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

- \* Compte du site de support NetApp \* : si vous avez plusieurs comptes, sélectionnez celui que vous souhaitez utiliser.

## Résumé

Vérifiez ou modifiez les détails que vous avez saisis, puis cliquez sur **Créer**.

## Liens connexes

- ["Planification de votre configuration Cloud Volumes ONTAP"](#)
- ["Déployer Cloud Volumes ONTAP dans AWS à l'aide d'un déploiement avancé"](#)

## Lancer Cloud Volumes ONTAP dans AWS

Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à système unique ou en tant que paire HA dans AWS. Cette méthode offre une expérience de déploiement avancée qui offre plus d'options de configuration et de flexibilité que la méthode de déploiement rapide.

## Avant de commencer

Vous avez besoin des éléments suivants avant de commencer.

- Un agent de console opérationnel.
  - Vous devriez avoir un ["Agent de console associé à votre système"](#) .
  - ["Vous devez être prêt à laisser l'agent de la console en cours d'exécution à tout moment."](#) .
- Une compréhension de la configuration que vous souhaitez utiliser.

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

- Une compréhension de ce qui est nécessaire pour configurer les licences pour Cloud Volumes ONTAP.  
["Apprenez à configurer les licences"](#) .

- DNS et Active Directory pour les configurations CIFS.

Pour plus de détails, reportez-vous à ["Exigences réseau pour Cloud Volumes ONTAP dans AWS"](#) .

## Lancer un système Cloud Volumes ONTAP à nœud unique dans AWS

Si vous souhaitez lancer Cloud Volumes ONTAP dans AWS, vous devez créer un nouveau système dans la console NetApp .

### À propos de cette tâche

Immédiatement après la création du système, la console lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, la console met immédiatement fin à l'instance, puis commence à déployer le système Cloud Volumes ONTAP . Si la connectivité ne peut pas être vérifiée, la création du système échoue. L'instance de test est soit une `t2.nano` (pour la location VPC par défaut) ou `m3.medium` (pour la location VPC dédiée).

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. Sélectionnez **Amazon Web Services** et \* Cloud Volumes ONTAP Single Node\*.
4. Sélectionnez **Création avancée**. Étant donné que le mode **Création rapide** est sélectionné par défaut, vous pouvez voir un message concernant les valeurs par défaut. Cliquez sur **Continuer**.
5. Si vous y êtes invité, "[créer un agent de console](#)" .
6. **Détails et informations d'identification** : Modifiez éventuellement les informations d'identification et l'abonnement AWS, saisissez un nom de système, ajoutez des balises si nécessaire, puis saisissez un mot de passe.

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

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des balises	Les balises AWS sont des métadonnées pour vos ressources AWS. La console 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 système, puis vous pouvez en ajouter davantage après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les balises, reportez-vous à <a href="#">"Documentation AWS : Balisage de vos ressources Amazon EC2"</a> .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <code>admin</code> ou remplacez-le par un nom d'utilisateur personnalisé.

Champ	Description
Modifier les informations d'identification	Choisissez les informations d'identification AWS associées au compte sur lequel vous souhaitez déployer ce système. Vous pouvez également associer l'abonnement AWS Marketplace à utiliser avec ce système Cloud Volumes ONTAP . Cliquez sur <b>Ajouter un abonnement</b> pour associer les identifiants sélectionnés à un nouvel abonnement Marketplace AWS. L'abonnement peut être annuel ou payant pour Cloud Volumes ONTAP à un tarif horaire. <a href="#">"Découvrez comment ajouter des informations d'identification AWS supplémentaires à la console NetApp"</a> .

Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Une fois que le premier utilisateur s'est abonné, la place de marché AWS informe les utilisateurs suivants qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour le compte AWS, 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 la console et terminer le processus.



**NetApp Cloud Volumes ONTAP (CVO), delivered by ePlus** info

---

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

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

- ["En savoir plus sur la classification des données NetApp"](#)
- ["En savoir plus sur NetApp Backup and Recovery"](#)



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

8. **Emplacement et connectivité** : saisissez les informations réseau que vous avez enregistrées dans le ["Feuille de travail AWS"](#) .

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

Champ	Description
VPC	Si vous disposez d'un Outpost AWS, vous pouvez déployer un système Cloud Volumes ONTAP à nœud unique dans cet Outpost en sélectionnant le VPC Outpost. L'expérience est la même que pour tout autre VPC résidant dans AWS.

Champ	Description
Groupe de sécurité généré	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : <ul style="list-style-type: none"> <li>• Si vous choisissez <b>VPC sélectionné uniquement</b>, la source du trafic entrant est la plage de sous-réseaux du VPC sélectionné et la plage de sous-réseaux du VPC sur lequel réside l'agent de la console. C'est l'option recommandée.</li> <li>• Si vous choisissez <b>Tous les VPC</b>, la source du trafic entrant est la plage IP 0.0.0.0/0.</li> </ul>
Utiliser le groupe de sécurité existant	Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. <a href="#">"En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP"</a> .

9. **Cryptage des données** : choisissez aucun cryptage de données ou un cryptage géré par AWS.

Pour le chiffrement géré par AWS, vous pouvez choisir une clé principale client (CMK) différente de votre compte ou d'un autre compte AWS.



Vous ne pouvez pas modifier la méthode de chiffrement des données AWS après avoir créé un système Cloud Volumes ONTAP .

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

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

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

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

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

11. \* Configuration Cloud Volumes ONTAP \* (contrat annuel de la place de marché AWS uniquement) : vérifiez la configuration par défaut et cliquez sur **Continuer** ou cliquez 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.

12. **Packages préconfigurés** : sélectionnez l'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.

13. **Rôle IAM** : il est préférable de conserver l'option par défaut pour laisser la console créer le rôle pour vous.

Si vous préférez utiliser votre propre politique, elle doit répondre ["exigences de politique pour les nœuds Cloud Volumes ONTAP"](#) .

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



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

15. **Ressources de stockage sous-jacentes** : choisissez un type de disque, configurez le stockage sous-jacent et choisissez si vous souhaitez conserver la hiérarchisation des données activée.

Notez ce qui suit :

- Le type de disque correspond au volume initial (et à l'agrégat). Vous pouvez choisir un type de disque différent pour les volumes (et agrégats) suivants.
- Si vous choisissez un disque gp3 ou io1, la console utilise la fonctionnalité Elastic Volumes dans AWS pour augmenter automatiquement la capacité du disque de stockage sous-jacent selon les besoins. Vous pouvez choisir la capacité initiale en fonction de vos besoins de stockage et la réviser après le déploiement de Cloud Volumes ONTAP . ["En savoir plus sur la prise en charge des volumes élastiques 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 tous les agrégats supplémentaires créés par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.
- Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants.

["Découvrez comment fonctionne la hiérarchisation des données"](#) .

16. **Vitesse d'écriture et WORM** :

- a. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

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

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

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

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

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

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

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

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

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

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

### Volume Details & Protection

Volume Name <span style="float: right;">i</span> <input type="text" value="ABDcv5689"/>	Storage VM (SVM) <input type="text" value="svm_c...CVO1"/>
Volume Size <span style="float: right;">i</span> Unit <input type="text" value="100"/> <input type="text" value="GiB"/>	Snapshot Policy <input type="text" value="default"/>

default policy i

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

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Si vous configurez AWS Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, vous devez saisir <b>OU=Computers,OU=corp</b> 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 le même que le domaine AD.
Serveur NTP	Sélectionnez <b>Utiliser le domaine Active Directory</b> pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la <a href="#">"Documentation sur l'automatisation de la console NetApp"</a> pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

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

Pour plus d'informations, reportez-vous à ["Comprendre les profils d'utilisation du volume"](#) , ["Présentation de](#)

la hiérarchisation des données" , et "KB : Quelles fonctionnalités d'efficacité du stockage en ligne sont prises en charge avec CVO ?"

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

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

### Résultat

La console lance l'instance Cloud Volumes ONTAP . Vous pouvez suivre la progression sur la page **Audit**.

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

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

### Après avoir terminé

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

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

### Lancer une paire Cloud Volumes ONTAP HA dans AWS

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans AWS, vous devez créer un système HA dans la console.

### Limitation

À l'heure actuelle, les paires HA ne sont pas prises en charge avec AWS Outposts.

### À propos de cette tâche

Immédiatement après avoir créé le système Cloud Volumes ONTAP , la console lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, la console met immédiatement fin à l'instance, puis commence à déployer le système Cloud Volumes ONTAP . Si la connectivité ne peut pas être vérifiée, la création du système échoue. L'instance de test est soit une `t2.nano` (pour la location VPC par défaut) ou `m3.medium` (pour la location VPC dédiée).

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. Sélectionnez **Amazon Web Services** et \* Cloud Volumes ONTAP HA\*.

Certaines zones locales AWS sont disponibles.

Avant de pouvoir utiliser les zones locales AWS, vous devez activer les zones locales et créer un sous-

réseau dans la zone locale de votre compte AWS. Suivez les étapes **Inscription à une zone locale AWS** et **Étendez votre Amazon VPC à la zone locale** dans le "[Tutoriel AWS « Démarrer le déploiement d'applications à faible latence avec les zones locales AWS »](#)".

Si vous exécutez l'agent de console 3.9.36 ou une version antérieure, vous devez ajouter le `DescribeAvailabilityZones` autorisation au rôle AWS dans la console AWS EC2.

4. **Détails et informations d'identification** : Modifiez éventuellement les informations d'identification et l'abonnement AWS, saisissez un nom de système, ajoutez des balises si nécessaire, puis saisissez un mot de passe.

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

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des balises	Les balises AWS sont des métadonnées pour vos ressources AWS. La console 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 système, puis vous pouvez en ajouter davantage après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les balises, reportez-vous à " <a href="#">Documentation AWS : Balisage de vos ressources Amazon EC2</a> ".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier les informations d'identification	Choisissez les identifiants AWS et l'abonnement Marketplace à utiliser avec ce système Cloud Volumes ONTAP . Cliquez sur <b>Ajouter un abonnement</b> pour associer les identifiants sélectionnés à un nouvel abonnement Marketplace AWS. L'abonnement peut être annuel ou payant pour Cloud Volumes ONTAP à un tarif horaire. Si vous avez acheté une licence directement auprès de NetApp (BYOL), un abonnement AWS n'est pas requis. NetApp a restreint l'achat, la prolongation et le renouvellement des licences BYOL. Pour plus d'informations, consultez " <a href="#">Disponibilité restreinte des licences BYOL pour Cloud Volumes ONTAP</a> ". " <a href="#">Découvrez comment ajouter des informations d'identification AWS supplémentaires à la console</a> ".

Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Une fois que le premier utilisateur s'est abonné, la place de marché AWS informe les utilisateurs suivants qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour le compte AWS, 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 la console et terminer le processus.



**NetApp Cloud Volumes ONTAP (CVO), delivered by ePlus** Info

---

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

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

[Subscribe](#)

You are already subscribed to this product

---

**Pricing Details**

Software Fees

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

- ["En savoir plus sur la classification des données NetApp"](#)
- ["En savoir plus sur la sauvegarde et la récupération"](#)



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

6. **Modèles de déploiement HA** : choisissez une configuration HA.

Pour un aperçu des modèles de déploiement, reportez-vous à ["Cloud Volumes ONTAP HA pour AWS"](#) .

7. **Emplacement et connectivité** (zone de disponibilité unique (AZ)) ou **Région et VPC** (plusieurs AZ) : saisissez les informations réseau que vous avez enregistrées dans la feuille de calcul AWS.

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

Champ	Description
Groupe de sécurité généré	<p>Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic :</p> <ul style="list-style-type: none"> <li>• Si vous choisissez <b>VPC sélectionné uniquement</b>, la source du trafic entrant est la plage de sous-réseaux du VPC sélectionné et la plage de sous-réseaux du VPC sur lequel réside l'agent de la console. C'est l'option recommandée.</li> <li>• Si vous choisissez <b>Tous les VPC</b>, la source du trafic entrant est la plage IP 0.0.0.0/0.</li> </ul>
Utiliser le groupe de sécurité existant	<p>Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. <a href="#">"En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP"</a> .</p>

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

9. **IP flottantes** : si vous avez choisi plusieurs AZ, spécifiez les adresses IP flottantes.

Les adresses IP doivent être en dehors du bloc CIDR pour tous les VPC de la région. Pour plus de détails, reportez-vous à ["Exigences réseau AWS pour Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité"](#) .

10. **Tables de routage** : si vous avez choisi plusieurs AZ, 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 risquent de ne pas avoir accès à la paire Cloud Volumes ONTAP HA. Pour plus d'informations sur les tables de routage, reportez-vous à la ["Documentation AWS : Tables de routage"](#) .

11. **Cryptage des données** : choisissez aucun cryptage de données ou un cryptage géré par AWS.

Pour le chiffrement géré par AWS, vous pouvez choisir une clé principale client (CMK) différente de votre compte ou d'un autre compte AWS.



Vous ne pouvez pas modifier la méthode de chiffrement des données AWS après avoir créé un système Cloud Volumes ONTAP .

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

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

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

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

13. \* Configuration Cloud Volumes ONTAP \* (contrat annuel AWS Marketplace uniquement) : vérifiez la configuration par défaut et cliquez sur **Continuer** ou cliquez 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** (horaires ou BYOL uniquement) : sélectionnez l'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. **Rôle IAM** : il est préférable de conserver l'option par défaut pour laisser la console créer le rôle pour vous.

Si vous préférez utiliser votre propre politique, elle doit répondre ["exigences de politique 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 de l'instance.



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

17. **Ressources de stockage sous-jacentes** : choisissez un type de disque, configurez le stockage sous-jacent et choisissez si vous souhaitez conserver la hiérarchisation des données activée.

Notez ce qui suit :

- Le type de disque correspond au volume initial (et à l'agrégat). Vous pouvez choisir un type de disque différent pour les volumes (et agrégats) suivants.
- Si vous choisissez un disque gp3 ou io1, la console utilise la fonctionnalité Elastic Volumes dans AWS pour augmenter automatiquement la capacité du disque de stockage sous-jacent selon les besoins. Vous pouvez choisir la capacité initiale en fonction de vos besoins de stockage et la réviser après le déploiement de Cloud Volumes ONTAP . ["En savoir plus sur la prise en charge des volumes élastiques 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 tous les agrégats supplémentaires créés par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.
- Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants.

["Découvrez comment fonctionne la hiérarchisation des données"](#) .

18. **Vitesse d'écriture et WORM** :

- a. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

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

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

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

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

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

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

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

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

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

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

### Volume Details & Protection

Volume Name <span style="float: right;">i</span> <input type="text" value="ABDcv5689"/>	Storage VM (SVM) <input type="text" value="svm_c...CVO1"/>
Volume Size <span style="float: right;">i</span> Unit <input type="text" value="100"/> <input type="text" value="GiB"/>	Snapshot Policy <input type="text" value="default"/>

default policy i

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

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Si vous configurez AWS Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, vous devez saisir <b>OU=Computers,OU=corp</b> 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 le même que le domaine AD.
Serveur NTP	Sélectionnez <b>Utiliser le domaine Active Directory</b> pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la <a href="#">"Documentation sur l'automatisation de la console NetApp"</a> pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

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

Pour plus d'informations, reportez-vous à ["Choisissez un profil d'utilisation du volume"](#) et ["Présentation de la](#)

[hiérarchisation des données](#) .

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

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

### Résultat

La console lance la paire Cloud Volumes ONTAP HA. Vous pouvez suivre la progression sur la page **Audit**.

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

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

### Après avoir terminé

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

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

### Liens connexes

- "[Planification de votre configuration Cloud Volumes ONTAP](#)"
- "[Déployer Cloud Volumes ONTAP dans AWS à l'aide d'un déploiement rapide](#)"

## Déployer Cloud Volumes ONTAP dans AWS Secret Cloud ou AWS Top Secret Cloud

Similaire à une région AWS standard, vous pouvez utiliser la console NetApp dans "[Cloud secret AWS](#)" et dans "[Cloud AWS Top Secret](#)" pour déployer Cloud Volumes ONTAP, qui fournit des fonctionnalités de classe entreprise pour votre stockage cloud. AWS Secret Cloud et Top Secret Cloud sont des régions fermées spécifiques à la communauté du renseignement américaine ; les instructions sur cette page s'appliquent uniquement aux utilisateurs des régions AWS Secret Cloud et Top Secret Cloud.

### Avant de commencer

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

- Consultez les versions prises en charge suivantes dans AWS Secret Cloud et Top Secret Cloud :
  - Cloud Volumes ONTAP 9.12.1 P2
  - Version 3.9.32 de l'agent Console

L'agent de console est requis pour déployer et gérer Cloud Volumes ONTAP dans AWS. Vous vous

connecterez à la console à partir du logiciel installé sur l'instance de l'agent de la console. Le site Web SaaS pour la console n'est pas pris en charge dans AWS Secret Cloud et Top Secret Cloud.

- En savoir plus sur le mode privé

Dans AWS Secret Cloud et Top Secret Cloud, la console fonctionne en *mode privé*. En mode privé, il n'y a pas de connectivité à la couche SaaS depuis la console. Vous pouvez accéder à la console via une application Web locale qui peut accéder à l'agent de la console.

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

## Étape 1 : Configurez votre réseau

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

### Étapes

1. Choisissez le VPC et les sous-réseaux dans lesquels vous souhaitez lancer l'instance de l'agent de console et les instances Cloud Volumes ONTAP .
2. Assurez-vous que votre VPC et vos sous-réseaux prendront en charge la connectivité entre l'agent de console et Cloud Volumes ONTAP.
3. Configurez un point de terminaison VPC sur le service S3.

Un point de terminaison VPC est requis si vous souhaitez hiérarchiser les données froides de Cloud Volumes ONTAP vers un stockage d'objets à faible coût.

## Étape 2 : Configurer les autorisations

Configurez des stratégies et des rôles IAM qui fournissent à l'agent de console et à Cloud Volumes ONTAP les autorisations dont ils ont besoin pour effectuer des actions dans AWS Secret Cloud ou Top Secret Cloud.

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

- L'instance de l'agent de console
- Instances Cloud Volumes ONTAP
- Pour les paires HA, l'instance de médiateur Cloud Volumes ONTAP HA (si vous souhaitez déployer des paires HA)

### Étapes

1. Accédez à la console AWS IAM et cliquez sur **Politiques**.
2. Créez une politique pour l'instance de l'agent de console.



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

## Régions secrètes

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",
```

```

        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```

```

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

```

### Régions top secrètes

```

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

```

```
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2>DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2>DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2>DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
"cloudformation>DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"iam:PassRole",
"iam:CreateRole",
"iam>DeleteRole",
"iam:PutRolePolicy",
"iam:ListInstanceProfiles",
"iam:CreateInstanceProfile",
"iam>DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam>DeleteInstanceProfile",
"s3:GetObject",
"s3:ListBucket",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"kms:List*",
"kms:Describe*",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"ec2:DescribeInstanceAttribute",
"ec2:CreatePlacementGroup",
"ec2>DeletePlacementGroup"
```

```

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

```

```
}
```

3. Créez une politique pour Cloud Volumes ONTAP.

## Régions secrètes

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

## Régions top secrètes

```

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

```

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

```

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

```

4. Créez des rôles IAM avec le type de rôle Amazon EC2 et attachez les stratégies que vous avez créées aux étapes précédentes.

#### Créer le rôle :

Comme pour les stratégies, vous devez disposer d'un rôle IAM pour l'agent de console et d'un autre pour les nœuds Cloud Volumes ONTAP . Pour les paires HA : comme pour les stratégies, vous devez disposer d'un rôle IAM pour l'agent de console, d'un pour les nœuds Cloud Volumes ONTAP et d'un pour le médiateur HA (si vous souhaitez déployer des paires HA).

#### Sélectionnez le rôle :

Vous devez sélectionner le rôle IAM de l'agent de console lorsque vous lancez l'instance de l'agent de console. Vous pouvez sélectionner les rôles IAM pour Cloud Volumes ONTAP lorsque vous créez un système Cloud Volumes ONTAP à partir de la console. Pour les paires HA, vous pouvez sélectionner les rôles IAM pour Cloud Volumes ONTAP et le médiateur HA lorsque vous créez un système Cloud Volumes ONTAP .

### Étape 3 : Configurer AWS KMS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, assurez-vous que les exigences sont respectées pour AWS Key Management Service (KMS).

#### Étapes

1. Assurez-vous qu'une clé principale 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 la CMK se trouve dans un compte AWS distinct du compte sur lequel vous prévoyez de déployer Cloud Volumes ONTAP, vous devez obtenir l'ARN de cette clé.

Vous devez fournir l'ARN à la console lorsque vous créez le système Cloud Volumes ONTAP .

3. Ajoutez le rôle IAM de l'instance à la liste des utilisateurs clés pour une CMK.

Cela donne à la console les autorisations d'utiliser le CMK avec Cloud Volumes ONTAP.

#### Étape 4 : installer l'agent de console et configurer la console

Avant de pouvoir commencer à utiliser la console pour déployer Cloud Volumes ONTAP dans AWS, vous devez installer et configurer l'agent de la console. Il permet à la console de gérer les ressources et les processus au sein de votre environnement de cloud public (cela inclut Cloud Volumes ONTAP).

#### Étapes

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



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

Vous devez télécharger le certificat pendant le processus de configuration. La console utilise le certificat de confiance lors de l'envoi de requêtes à AWS via HTTPS.

2. Lancez l'instance de l'agent Console :
  - a. Accédez à la page AWS Intelligence Community Marketplace pour la console.
  - b. Dans l'onglet Lancement personnalisé, choisissez l'option permettant de lancer l'instance à partir de la console EC2.
  - c. Suivez les invites pour configurer l'instance.

Notez les points suivants lorsque vous configurez l'instance :

- Nous recommandons `t3.xlarge`.
- Vous devez choisir le rôle IAM que vous avez créé lors de la configuration des autorisations.
- Vous devez conserver les options de stockage par défaut.
- Les méthodes de connexion requises pour l'agent de console sont les suivantes : SSH, HTTP et HTTPS.

3. Configurez la console à partir d'un hôte disposant d'une connexion à l'instance :
  - a. Ouvrez un navigateur Web et entrez `<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>` où `<em>ipaddress</em>` est l'adresse IP de l'hôte Linux sur lequel vous avez installé l'agent de console.
  - 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 instructions pour configurer un nouveau système.
    - **Détails du système** : saisissez un nom pour l'agent de la console et le nom de votre entreprise.

- **Créer un utilisateur administrateur** : Créez l'utilisateur administrateur du système.

Ce compte utilisateur s'exécute localement sur le système. Il n'y a aucune connexion au service auth0 disponible via la console.

- **Révision** : Vérifiez les détails, acceptez le contrat de licence, puis sélectionnez **Configurer**.

e. Pour terminer l'installation du certificat signé par l'autorité de certification, redémarrez l'instance de l'agent de console à partir de la console EC2.

4. Une fois l'agent de console redémarré, connectez-vous à l'aide du compte d'utilisateur administrateur que vous avez créé dans l'assistant d'installation.

## Étape 5 : (facultatif) Installer un certificat en mode privé

Cette étape est facultative pour les régions AWS Secret Cloud et Top Secret Cloud et n'est requise que si vous disposez de certificats supplémentaires en plus des certificats racine que vous avez installés à l'étape précédente.

### Étapes

1. Répertorier les certificats installés existants.

- a. Pour collecter l'ID Docker du conteneur occm (nom identifié « ds-occm-1 »), exécutez la commande suivante :

```
docker ps
```

- b. Pour accéder au conteneur occm, exécutez la commande suivante :

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

- c. Pour collecter le mot de passe de la variable d'environnement « TRUST\_STORE\_PASSWORD », exécutez la commande suivante :

```
env
```

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

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

2. Ajouter un certificat.

- a. Pour collecter l'ID Docker du conteneur occm (nom identifié « ds-occm-1 »), exécutez la commande suivante :

```
docker ps
```

b. Pour accéder au conteneur occm, exécutez la commande suivante :

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

Enregistrez le nouveau fichier de certificat à l'intérieur.

c. Pour collecter le mot de passe de la variable d'environnement « TRUST\_STORE\_PASSWORD », exécutez la commande suivante :

```
env
```

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

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

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

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

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

```
exit
```

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

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

## Étape 6 : Ajouter une licence à la console

Si vous avez acheté une licence auprès de NetApp, vous devez l'ajouter à la console afin de pouvoir sélectionner la licence lorsque vous créez un nouveau système Cloud Volumes ONTAP . Ces licences restent non attribuées jusqu'à ce que vous les associiez à un nouveau système Cloud Volumes ONTAP .

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Licences et abonnements**.
2. Dans le panneau \* Cloud Volumes ONTAP\*, sélectionnez **Afficher**.
3. Dans l'onglet \* Cloud Volumes ONTAP\*, sélectionnez **Licences > Licences basées sur les nœuds**.
4. Cliquez sur **Non attribué**.
5. Cliquez sur **Ajouter des licences non attribuées**.

6. Saisissez le numéro de série de la licence ou téléchargez le fichier de licence.
7. Si vous ne disposez pas encore du fichier de licence, vous devrez télécharger manuellement le fichier de licence depuis netapp.com.
  - a. Aller à la "[Générateur de fichiers de licence NetApp](#)" et connectez-vous à l'aide de vos informations d'identification du site de support NetApp .
  - b. Saisissez votre mot de passe, choisissez votre produit, saisissez le numéro de série, confirmez que vous avez lu et accepté la politique de confidentialité, puis cliquez sur **Soumettre**.
  - c. Choisissez si vous souhaitez recevoir le fichier JSON serialnumber.NLF par e-mail ou par téléchargement direct.
8. Cliquez sur **Ajouter une licence**.

## Résultat

La console ajoute la licence comme non attribuée jusqu'à ce que vous l'associez à un nouveau système Cloud Volumes ONTAP . Vous pouvez voir la licence dans le menu de navigation de gauche sous **Licences et abonnements > Cloud Volumes ONTAP > Afficher > Licences**.

## Étape 7 : Lancer Cloud Volumes ONTAP depuis la console

Vous pouvez lancer des instances Cloud Volumes ONTAP dans AWS Secret Cloud et Top Secret Cloud en créant de nouveaux systèmes dans la console.

### Avant de commencer

Pour les paires HA, une paire de clés est requise pour activer l'authentification SSH basée sur une clé auprès du médiateur HA.

### Étapes

1. Sur la page **Systèmes**, cliquez sur **Ajouter un système**.
2. Sous **Créer**, sélectionnez Cloud Volumes ONTAP.

Pour HA : sous **Créer**, sélectionnez Cloud Volumes ONTAP ou Cloud Volumes ONTAP HA.

3. Suivez les étapes de l'assistant pour lancer le système Cloud Volumes ONTAP .



Lorsque vous effectuez des sélections via l'assistant, ne sélectionnez pas **Data Sense & Compliance** et **Backup to Cloud** sous **Services**. Sous **Packages préconfigurés**, sélectionnez **Modifier la configuration** uniquement et assurez-vous de n'avoir sélectionné aucune autre option. Les packages préconfigurés ne sont pas pris en charge dans les régions AWS Secret Cloud et Top Secret Cloud, et s'ils sont sélectionnés, votre déploiement échouera.

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

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

- Vous devez configurer une passerelle de transit lorsque vous déployez Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité (AZ). Pour les instructions, reportez-vous à "[Configurer une passerelle de transit AWS](#)".
- Déployez la configuration comme suit, car seules deux zones de disponibilité étaient disponibles dans le cloud AWS Top Secret au moment de la publication :
  - Nœud 1 : Zone de disponibilité A

- Nœud 2 : Zone de disponibilité B
- Médiateur : Zone de disponibilité A ou B

## Remarques sur le déploiement de Cloud Volumes ONTAP dans des nœuds simples et HA

Notez les points suivants lorsque vous terminez l'assistant :

- Vous devez laisser l'option par défaut pour utiliser un groupe de sécurité généré.

Le groupe de sécurité prédéfini inclut les règles dont Cloud Volumes ONTAP a besoin pour fonctionner correctement. Si vous souhaitez utiliser le vôtre, vous pouvez vous référer à la section 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 est destiné au volume Cloud Volumes ONTAP initial.

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

- Les performances des disques AWS sont liées à la taille du disque.

Vous devez choisir la taille de disque qui vous offre les performances durables dont vous avez besoin. Consultez la documentation AWS pour plus de détails sur les performances d'EBS.

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



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

## Résultat

L'instance Cloud Volumes ONTAP est lancée. Vous pouvez suivre la progression dans la page **Audit**.

## Étape 8 : Installer des certificats de sécurité pour la hiérarchisation des données

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

### Avant de commencer

1. Créer des buckets S3.



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

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

### Étapes

1. Copiez le texte des certificats racines que vous avez installés dans `step 4`.
2. Connectez-vous en toute sécurité au système Cloud Volumes ONTAP à l'aide de la CLI.
3. Installez les certificats racine. Vous devrez peut-être appuyer sur la touche `ENTER` plusieurs fois :

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

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



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

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

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

## Démarrer avec Microsoft Azure

### Découvrez les options de déploiement de Cloud Volumes ONTAP dans Azure

NetApp propose deux options pour déployer Cloud Volumes ONTAP sur Azure. Cloud Volumes ONTAP s'appuie traditionnellement sur la console NetApp pour le déploiement et l'orchestration. À partir de Cloud Volumes ONTAP 9.16.1, vous pouvez profiter du déploiement direct de la place de marché Azure, un processus simplifié qui donne accès à un ensemble limité, mais toujours puissant, de fonctionnalités et d'options Cloud Volumes ONTAP .

Lorsque vous déployez Cloud Volumes ONTAP directement à partir de la place de marché Azure, vous n'êtes pas obligé de configurer l'agent de la console ni de respecter d'autres critères de sécurité et d'intégration requis pour le déploiement de Cloud Volumes ONTAP via la console. Depuis la place de marché Azure, vous pouvez déployer rapidement Cloud Volumes ONTAP en quelques clics et explorer ses principales fonctionnalités et capacités dans votre environnement.

Une fois le déploiement sur la place de marché Azure terminé, vous pouvez découvrir ces systèmes dans la

console. Après la découverte, vous pouvez les gérer en tant que systèmes Cloud Volumes ONTAP et profiter de toutes les fonctionnalités de la console. ["Découvrez les systèmes déployés dans la console"](#) .

Voici la comparaison des fonctionnalités entre les deux options. Notez que les fonctionnalités d'une instance autonome déployée via la place de marché Azure changent lorsqu'elle est découverte dans la console.

	Place de marché Azure	Console NetApp
<b>Intégration</b>	Plus court et plus simple, préparation minimale requise pour un déploiement direct	Processus d'intégration plus long, y compris l'installation de l'agent de la console
<b>Types de machines virtuelles (VM) pris en charge</b>	Types d'instances Eds_v5 et Ls_v3	Gamme complète de types de machines virtuelles. <a href="https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html">https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html</a> ["Configurations prises en charge dans Azure"^]
<b>Licence</b>	Licence gratuite	Toute licence basée sur la capacité. <a href="#">"Licences Cloud Volumes ONTAP"</a>
* Prise en charge de NetApp *	Non inclus	Disponible, en fonction du type de licence
<b>Capacité</b>	Jusqu'à 500 Gio	Extensible par configuration
<b>Modèle de déploiement</b>	Déploiement en mode haute disponibilité (HA) dans une zone de disponibilité unique (AZ)	Toutes les configurations prises en charge, y compris les modes nœud unique et HA, les déploiements AZ simples et multiples
<b>Type de disque pris en charge</b>	Disques gérés SSD Premium v2	Un soutien plus large. <a href="#">"Configuration par défaut pour Cloud Volumes ONTAP"</a>
<b>Vitesse d'écriture (mode d'écriture rapide)</b>	Non pris en charge	Pris en charge, en fonction de votre configuration. <a href="#">"En savoir plus sur les vitesses d'écriture dans Cloud Volumes ONTAP"</a> .
<b>Capacités d'orchestration</b>	Non disponible	Disponible via la console NetApp , en fonction du type de licence
<b>Nombre de machines virtuelles de stockage prises en charge</b>	Un par déploiement	Plusieurs machines virtuelles de stockage, en fonction de votre configuration. <a href="#">"Nombre de machines virtuelles de stockage prises en charge"</a>
<b>Modification du type d'instance</b>	Non pris en charge	Soutenu
* Hiérarchisation de FabricPool *	Non pris en charge	Soutenu

#### Liens connexes

- Déploiement direct sur la place de marché Azure : ["Déployer Cloud Volumes ONTAP depuis la place de marché Azure"](#)

- Déploiement via la console : "[Démar­rage rapide de Cloud Volumes ONTAP dans Azure](#)"
- "[Documentation de la console NetApp](#)"

## Démarrer dans la console NetApp

### Démarrage rapide de Cloud Volumes ONTAP dans Azure

Démarrez avec Cloud Volumes ONTAP pour Azure en quelques étapes.

1

#### Créer un agent de console

Si vous n'avez pas de "Agent de console" mais il faut en créer un. "[Découvrez comment créer un agent de console dans Azure](#)"

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

2

#### Planifiez votre configuration

La console propose des packages préconfigurés qui correspondent à vos exigences de charge de travail, ou vous pouvez créer votre propre configuration. Si vous choisissez votre propre configuration, vous devez comprendre les options qui s'offrent à vous. Pour plus d'informations, reportez-vous à "[Planifiez votre configuration Cloud Volumes ONTAP dans Azure](#)".

3

#### Configurez votre réseau

1. Assurez-vous que votre réseau virtuel et vos sous-réseaux prendront en charge la connectivité entre l'agent de console et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du VPC cible pour NetApp AutoSupport.

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

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

4

#### Lancer Cloud Volumes ONTAP

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

#### Liens connexes

- "[Création d'un agent de console à partir de la console](#)"
- "[Création d'un agent de console à partir de la Place de marché Azure](#)"
- "[Installation du logiciel agent de console sur un hôte Linux](#)"
- "[Ce que fait la console avec les autorisations](#)"

## Planifiez votre configuration Cloud Volumes ONTAP dans Azure

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

### Choisissez une licence Cloud Volumes ONTAP

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

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

### Choisissez une région prise en charge

Cloud Volumes ONTAP est pris en charge dans la plupart des régions 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 machines virtuelles, selon le type de licence que vous choisissez.

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

### Comprendre les limites de stockage

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

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

### Dimensionnez votre système dans Azure

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

#### Type de machine virtuelle

Consultez les types de machines virtuelles pris en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#) puis examinez les détails de chaque type de machine virtuelle pris en charge. Sachez que chaque type de machine virtuelle prend en charge un nombre spécifique de disques de données.

- ["Documentation Azure : Tailles de machines virtuelles à usage général"](#)
- ["Documentation Azure : Tailles de machines virtuelles optimisées en mémoire"](#)

#### Type de disque Azure avec systèmes à nœud unique

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

Les systèmes à nœud unique peuvent utiliser ces types de disques gérés Azure :

- Les *disques gérés SSD Premium* offrent des performances élevées pour les charges de travail gourmandes en E/S à un coût plus élevé.
- Les *disques gérés SSD Premium v2* offrent des performances supérieures avec une latence plus faible à un coût inférieur, par rapport aux disques gérés SSD Premium.
- Les *disques gérés SSD standard* offrent des performances constantes pour les charges de travail nécessitant de faibles IOPS.
- Les *disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevés et que vous souhaitez réduire vos coûts.

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

### Type de disque Azure avec paires HA

Les systèmes HA utilisent des disques gérés partagés SSD Premium qui offrent tous deux des performances élevées pour les charges de travail gourmandes en E/S à un coût plus élevé. Les déploiements HA créés avant la version 9.12.1 utilisent des blobs de pages Premium.

### Taille du disque Azure

Lorsque vous lancez des instances Cloud Volumes ONTAP , vous devez choisir la taille de disque par défaut pour les agrégats. La console NetApp utilise cette taille de disque pour l'agrégat initial et pour tous les agrégats supplémentaires qu'elle 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 en "[en utilisant l'option d'allocation avancée](#)".



Tous les disques d'un agrégat doivent avoir la même taille.

Lors du choix d'une taille de disque, vous devez prendre en compte plusieurs facteurs. La taille du disque a un impact sur le montant que vous payez pour le stockage, la taille des volumes que vous pouvez créer dans 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 du disque. Les disques plus grands offrent des IOPS et un débit plus élevés. Par exemple, choisir des disques de 1 Tio peut offrir de meilleures performances que des disques de 500 Gio, à un coût plus élevé.

Il n'y a aucune différence de performances entre les tailles de disque pour le stockage standard. Vous devez choisir la taille du disque en fonction de la capacité dont vous avez besoin.

Consultez Azure pour connaître les IOPS et le débit par taille de disque :

- "[Microsoft Azure : tarifs des disques gérés](#)"
- "[Microsoft Azure : tarifs des blobs de pages](#)"

### Afficher les disques système par défaut

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

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



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

### Recueillir des informations sur le réseau

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

Informations Azure	Votre valeur
Région	
Réseau virtuel (VNet)	
Sous-réseau	
Groupe de sécurité réseau (si vous utilisez le vôtre)	

### Choisissez une vitesse d'écriture

La console 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, ainsi que les risques et les recommandations lors de l'utilisation d'une vitesse d'écriture élevée. ["En savoir plus sur la vitesse d'écriture"](#) .

### Choisissez un profil d'utilisation du volume

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

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

#### Provisionnement léger

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

#### Déduplication

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

#### Compression

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

### Configurer le réseau Azure pour Cloud Volumes ONTAP

La console NetApp gère la configuration des composants réseau pour Cloud Volumes ONTAP, tels que les adresses IP, les masques de réseau et les itinéraires. Vous devez vous assurer que l'accès Internet sortant est disponible, que suffisamment d'adresses IP

privées sont disponibles, que les bonnes connexions sont en place, etc.

### Exigences pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être respectées dans Azure.

#### Accès Internet sortant

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

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

#### Points de terminaison Cloud Volumes ONTAP

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

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact en cas d'indisponibilité
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : <ul style="list-style-type: none"><li>• Services Cloud Volumes ONTAP</li><li>• Services ONTAP</li><li>• Protocoles et services proxy</li></ul>
<a href="https://vault.azure.net">https://vault.azure.net</a>	Coffre-fort à clés	Utilisé pour récupérer les clés secrètes du client à partir d'Azure Key Vault lors de l'utilisation de clés gérées par le client (CMK).	Modes standard, restreint et privé.	Les services Cloud Volumes ONTAP ne sont pas disponibles.
<a href="https://api.bluexp.net/app.com/tenancy">https://api.bluexp.net/app.com/tenancy</a>	Location	Utilisé pour récupérer les ressources Cloud Volumes ONTAP depuis la console pour autoriser les ressources et les utilisateurs.	Modes standard et restreint.	Les ressources Cloud Volumes ONTAP et les utilisateurs ne sont pas autorisés.

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact en cas d'indisponibilité
<a href="https://mysupport.net/app.com/aods/asupmessage">https://mysupport.net/app.com/aods/asupmessage</a> \ <a href="https://mysupport.net/app.com/asupprod/post/1.0/postAsup">https://mysupport.net/app.com/asupprod/post/1.0/postAsup</a>	AutoSupport	Utilisé pour envoyer des données de télémétrie AutoSupport au support NetApp .	Modes standard et restreint.	Les informations AutoSupport ne sont toujours pas livrées.
<a href="https://management.azure.com">https://management.azure.com</a> \ <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> \ <a href="https://bluexpinfrapro.d.eastus2.data.azurecr.io">https://bluexpinfrapro.d.eastus2.data.azurecr.io</a> \ <a href="https://core.windows.net">https://core.windows.net</a>	Les régions publiques	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> \ <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> \ <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> \ <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Région de Chine	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> \ <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a> \ <a href="https://blob.core.cloudapi.de">https://blob.core.cloudapi.de</a> \ <a href="https://core.cloudapi.de">https://core.cloudapi.de</a>	Région Allemagne	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> \ <a href="https://login.microsoftonline.us">https://login.microsoftonline.us</a> \ <a href="https://blob.core.usgovcloudapi.net">https://blob.core.usgovcloudapi.net</a> \ <a href="https://core.usgovcloudapi.net">https://core.usgovcloudapi.net</a>	régions gouvernementales	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact en cas d'indisponibilité
\ <a href="https://management.azure.microsoft.scloud">https://management.azure.microsoft.scloud</a> \ <a href="https://login.microsoftonline.microsoft.scloud">https://login.microsoftonline.microsoft.scloud</a> \ <a href="https://blob.core.microsoft.scloud">https://blob.core.microsoft.scloud</a> \ <a href="https://core.microsoft.scloud">https://core.microsoft.scloud</a>	Régions du gouvernement du DoD	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.

## Configuration du proxy réseau de l'agent de la console NetApp

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

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

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

## adresses IP

La console 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 disponibles.

Le nombre de LIF alloués à Cloud Volumes ONTAP dépend du fait que vous déployez un système à nœud unique ou une paire HA. Un LIF est une adresse IP associée à un port physique. Un LIF de gestion SVM est requis pour les outils de gestion tels que SnapCenter.



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

## Adresses IP pour un système à nœud unique

La console alloue 5 ou 6 adresses IP à un seul système de nœud :

- Gestion de cluster IP
- IP de gestion des nœuds
- IP intercluster pour SnapMirror
- IP NFS/CIFS
- 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. Ce LIF est obligatoire et ne doit pas être supprimé.

- Gestion SVM (facultatif - non configuré par défaut)

### Adresses IP pour les paires HA

La console alloue des adresses IP à 4 cartes réseau (par nœud) pendant le déploiement.

Notez que la console crée un LIF de gestion SVM sur les paires HA, mais pas sur les systèmes à nœud unique dans Azure.

#### NIC0

- IP de gestion des 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. Ce LIF est obligatoire et ne doit pas être supprimé.

#### NIC1

- IP du réseau de cluster

#### NIC2

- IP d'interconnexion de cluster (HA IC)

#### NIC3

- Pageblob NIC IP (accès disque)



NIC3 s'applique uniquement aux déploiements HA qui utilisent le stockage d'objets blob de pages.

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

De plus, 4 adresses IP frontales (FIP) sont configurées pour migrer lors d'événements de basculement. Ces adresses IP frontales résident dans l'équilibreur de charge.

- Gestion de cluster IP

- IP de données NodeA (NFS/CIFS)
- IP de données NodeB (NFS/CIFS)
- IP de gestion SVM

## Connexions sécurisées aux services Azure

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

Dans la plupart des cas, vous n'avez rien à faire : la console gère Azure Private Link pour vous. Mais si vous utilisez Azure Private DNS, vous devrez modifier un fichier de configuration. Vous devez également être conscient d'une exigence relative à l'emplacement de l'agent de console dans Azure.

Vous pouvez également désactiver la connexion Private Link, si les besoins de votre entreprise l'exigent. Si vous désactivez le lien, la console configure Cloud Volumes ONTAP pour utiliser un point de terminaison de service à la place.

["En savoir plus sur l'utilisation des liens privés Azure ou des points de terminaison 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 dans d'autres réseaux, vous devez disposer d'une connexion VPN entre le réseau virtuel Azure et l'autre réseau, par exemple, votre réseau d'entreprise.

Pour les instructions, reportez-vous à la ["Documentation Microsoft Azure : Créer une connexion site à site dans le portail Azure"](#) .

## Port pour l'interconnexion HA

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

Par défaut, la communication entre les LIF d'interconnexion HA 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 HA, vous devez vous assurer que le trafic TCP est ouvert pour le port 10006 afin que la paire HA puisse fonctionner correctement.

## Une seule paire HA dans un groupe de ressources Azure

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

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

## Règles du groupe de sécurité

La console crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes pour que Cloud Volumes ONTAP fonctionne correctement. ["Afficher les règles du groupe de sécurité pour l'agent de la console"](#) .

Les groupes de sécurité Azure pour Cloud Volumes ONTAP nécessitent que les ports appropriés soient ouverts pour la communication interne entre les nœuds. "[En savoir plus sur les ports internes ONTAP](#)".

Nous ne recommandons pas de modifier les groupes de sécurité prédéfinis ni d'utiliser des groupes de sécurité personnalisés. Toutefois, si vous devez le faire, notez que le processus de déploiement nécessite que le système Cloud Volumes ONTAP dispose d'un accès complet au sein de son propre sous-réseau. Une fois le déploiement terminé, si vous décidez de modifier le groupe de sécurité réseau, assurez-vous de garder les ports du cluster et les ports réseau HA ouverts. Cela garantit une communication transparente au sein du cluster Cloud Volumes ONTAP (communication de bout en bout entre les nœuds).

### Règles entrantes pour les systèmes à nœud unique

Lorsque vous ajoutez un système Cloud Volumes ONTAP 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-réseaux du VNet pour le système Cloud Volumes ONTAP et la plage de sous-réseaux du VNet sur lequel réside l'agent de la console. C'est l'option recommandée.
- **Tous les réseaux virtuels** : la source du trafic entrant est la plage IP 0.0.0.0/0.
- **Désactivé** : cette option restreint l'accès au réseau public à votre compte de stockage et désactive la hiérarchisation des données pour les systèmes Cloud Volumes ONTAP . Il s'agit d'une option recommandée si vos adresses IP privées ne doivent pas être exposées même au sein du même réseau virtuel en raison des réglementations et des politiques de sécurité.

Priorité et nom	Port et protocole	Source et destination	Description
1000 entrants_ssh	22 TCP	N'importe lequel à n'importe lequel	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
1001 entrant_http	80 TCP	N'importe lequel à n'importe lequel	Accès HTTP à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
1002 entrant_111_tcp	111 TCP	N'importe lequel à n'importe lequel	Appel de procédure à distance pour NFS
1003 entrant_111_udp	111 UDP	N'importe lequel à n'importe lequel	Appel de procédure à distance pour NFS
1004 entrant_139	139 TCP	N'importe lequel à n'importe lequel	Session de service NetBIOS pour CIFS
1005 entrant_161-162_tcp	161-162 TCP	N'importe lequel à n'importe lequel	Protocole simple de gestion de réseau
1006 entrant_161-162_udp	161-162 UDP	N'importe lequel à n'importe lequel	Protocole simple de gestion de réseau

Priorité et nom	Port et protocole	Source et destination	Description
1007 entrant_443	443 TCP	N'importe lequel à n'importe lequel	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
1008 entrant_445	445 TCP	N'importe lequel à n'importe lequel	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
1009 entrant_635_tcp	635 TCP	N'importe lequel à n'importe lequel	Montage NFS
1010 entrant_635_udp	635 UDP	N'importe lequel à n'importe lequel	Montage NFS
1011 entrant_749	749 TCP	N'importe lequel à n'importe lequel	Kerberos
1012 entrant_2049_tcp	2049 TCP	N'importe lequel à n'importe lequel	Démon du serveur NFS
1013 entrant_2049_udp	2049 UDP	N'importe lequel à n'importe lequel	Démon du serveur NFS
1014 entrant_3260	3260 TCP	N'importe lequel à n'importe lequel	Accès iSCSI via le LIF de données iSCSI
1015 entrant_4045-4046_tcp	4045-4046 TCP	N'importe lequel à n'importe lequel	Démon de verrouillage NFS et moniteur d'état du réseau
1016 entrant_4045-4046_udp	4045-4046 UDP	N'importe lequel à n'importe lequel	Démon de verrouillage NFS et moniteur d'état du réseau
1017 entrant_10000	10000 TCP	N'importe lequel à n'importe lequel	Sauvegarde à l'aide de NDMP
1018 entrant_11104-11105	11104-11105 TCP	N'importe lequel à n'importe lequel	Transfert de données SnapMirror
3000 inbound_deny_all_tcp	N'importe quel port TCP	N'importe lequel à n'importe lequel	Bloquer tout autre trafic TCP entrant
3001 inbound_deny_all_udp	N'importe quel port UDP	N'importe lequel à n'importe lequel	Bloquer tout autre trafic UDP entrant
65000 AutoriserVnetInBound	N'importe quel port N'importe quel protocole	Réseau virtuel vers réseau virtuel	Trafic entrant depuis le VNet
65001 Autoriser AzureLoad BalancerInBound	N'importe quel port N'importe quel protocole	AzureLoadBalancer vers n'importe quel	Trafic de données provenant de l'équilibreur de charge standard Azure
65500 RefuserToutEnLiaison	N'importe quel port N'importe quel protocole	N'importe lequel à n'importe lequel	Bloquer tout autre trafic entrant

## Règles entrantes pour les systèmes HA

Lorsque vous ajoutez un système Cloud Volumes ONTAP 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-réseaux du VNet pour le système Cloud Volumes ONTAP et la plage de sous-réseaux du VNet sur lequel réside l'agent de la console. C'est l'option recommandée.
- **Tous les réseaux virtuels** : la source du trafic entrant est la plage IP 0.0.0.0/0.



Les systèmes HA ont moins de règles entrantes que les systèmes à nœud unique, car le trafic de données entrant passe par Azure Standard Load Balancer. Pour cette raison, le trafic provenant de l'équilibreur de charge doit être ouvert, comme indiqué dans la règle « AllowAzureLoadBalancerInBound ».

- **Désactivé** : cette option restreint l'accès au réseau public à votre compte de stockage et désactive la hiérarchisation des données pour les systèmes Cloud Volumes ONTAP . Il s'agit d'une option recommandée si vos adresses IP privées ne doivent pas être exposées même au sein du même réseau virtuel en raison des réglementations et des politiques de sécurité.

Priorité et nom	Port et protocole	Source et destination	Description
100 entrants_443	443 Tout protocole	N'importe lequel à n'importe lequel	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
101 entrant_111_tcp	111 Tout protocole	N'importe lequel à n'importe lequel	Appel de procédure à distance pour NFS
102 entrant_2049_tcp	2049 Tout protocole	N'importe lequel à n'importe lequel	Démon du serveur NFS
111 entrant_ssh	22 Tout protocole	N'importe lequel à n'importe lequel	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
121 entrant_53	53 Tout protocole	N'importe lequel à n'importe lequel	DNS et CIFS
65000 AutoriserVnetInBound	N'importe quel port N'importe quel protocole	Réseau virtuel vers réseau virtuel	Trafic entrant depuis le VNet
65001 Autoriser AzureLoad BalancerInBound	N'importe quel port N'importe quel protocole	AzureLoadBalancer vers n'importe quel	Trafic de données provenant de l'équilibreur de charge standard Azure
65500 RefuserToutEnLiaison	N'importe quel port N'importe quel protocole	N'importe lequel à n'importe lequel	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 sortie de base. Si vous avez besoin de règles plus rigides, utilisez les règles sortantes

avancées.

### Règles de base pour les voyages sortants

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

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

### Règles sortantes avancées

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



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

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

Service	Port	Protocole	Source	Destination	But
AutoSupport	HTTPS	443	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (HTTPS est la valeur par défaut)
	HTTP	80	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (uniquement si le protocole de transport est modifié de HTTPS à HTTP)
	TCP	3128	Gestion des nœuds LIF	Agent de console	Envoi de messages AutoSupport via un serveur proxy sur l'agent de la console, si une connexion Internet sortante n'est pas disponible
Sauvegardes de configuration	HTTP	80	Gestion des nœuds LIF	http://<adresse IP de l'agent de la console>/occm/offboxconfig	Envoyer des sauvegardes de configuration à l'agent de la console. " <a href="#">Documentation ONTAP</a> ".
DHCP	68	UDP	Gestion des nœuds LIF	DHCP	Client DHCP pour la première configuration
DHCPS	67	UDP	Gestion des nœuds LIF	DHCP	serveur DHCP
DNS	53	UDP	Gestion des nœuds LIF et LIF de données (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Gestion des nœuds LIF	Serveurs de destination	Copie NDMP
SMTP	25	TCP	Gestion des nœuds LIF	Serveur de messagerie	Alertes SMTP, peuvent être utilisées pour AutoSupport
SNMP	161	TCP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	161	UDP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	162	TCP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	162	UDP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
SnapMirror	11104	TCP	LIF intercluster	LIF intercluster ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	11105	TCP	LIF intercluster	LIF intercluster ONTAP	Transfert de données SnapMirror
Syslog	514	UDP	Gestion des nœuds LIF	Serveur Syslog	Messages de transfert Syslog

## Exigences pour l'agent de console

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

- ["Afficher les exigences réseau pour l'agent de console"](#)
- ["Règles de groupe de sécurité dans Azure"](#)

## Sujets connexes

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

## Configurer 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 du chiffrement du service de stockage Azure avec une clé gérée par Microsoft. Mais vous pouvez utiliser votre propre clé de cryptage en suivant les étapes sur cette page.

### Présentation du cryptage des données

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

Si vous souhaitez utiliser une clé gérée par le client avec Cloud Volumes ONTAP, vous devez suivre les étapes suivantes :

1. Depuis Azure, créez un coffre de clés, puis générez une clé dans ce coffre.
2. Depuis la console NetApp , utilisez l'API pour créer un système Cloud Volumes ONTAP qui utilise la clé.

### Comment les données sont cryptées

La console utilise un ensemble de chiffrement de disque, qui permet la gestion des clés de chiffrement avec des disques gérés et non des blobs de pages. Tous les nouveaux disques de données utilisent également le même ensemble de chiffrement de disque. Les versions inférieures utiliseront la clé gérée par Microsoft, au lieu de la clé gérée par le client.

Une fois que vous avez créé un système Cloud Volumes ONTAP configuré pour utiliser une clé gérée par le client, les données Cloud Volumes ONTAP sont chiffrées comme suit.

<b>Configuration de Cloud Volumes ONTAP</b>	<b>Disques système utilisés pour le chiffrement des clés</b>	<b>Disques de données utilisés pour le cryptage des clés</b>
Nœud unique	<ul style="list-style-type: none"><li>• Botte</li><li>• Cœur</li><li>• NVRAM</li></ul>	<ul style="list-style-type: none"><li>• Racine</li><li>• Données</li></ul>

Configuration de Cloud Volumes ONTAP	Disques système utilisés pour le chiffrement des clés	Disques de données utilisés pour le cryptage des clés
Zone de disponibilité unique Azure HA avec objets blob de pages	<ul style="list-style-type: none"> <li>• Botte</li> <li>• Cœur</li> <li>• NVRAM</li> </ul>	Aucune
Zone de disponibilité unique Azure HA avec disques gérés partagés	<ul style="list-style-type: none"> <li>• Botte</li> <li>• Cœur</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• Racine</li> <li>• Données</li> </ul>
Zones de disponibilité multiples Azure HA avec disques gérés partagés	<ul style="list-style-type: none"> <li>• Botte</li> <li>• Cœur</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• Racine</li> <li>• Données</li> </ul>

Tous les comptes de stockage Azure pour Cloud Volumes ONTAP sont chiffrés à l'aide d'une clé gérée par le client. Si vous souhaitez crypter vos comptes de stockage lors de leur création, vous devez créer et fournir l'ID de la ressource dans la demande de création de Cloud Volumes ONTAP . Ceci s'applique à tous les types de déploiements. Si vous ne le fournissez pas, les comptes de stockage seront toujours chiffrés, mais la console crée d'abord les comptes de stockage avec le chiffrement à clé géré par Microsoft, puis met à jour les comptes de stockage pour utiliser la clé gérée par le client.

#### Rotation des clés dans Cloud Volumes ONTAP

Lorsque vous configurez vos clés de chiffrement, vous devez utiliser le portail Azure pour configurer et activer la rotation automatique des clés. La création et l'activation d'une nouvelle version de clés de chiffrement garantissent que Cloud Volumes ONTAP peut détecter et utiliser automatiquement la dernière version de clé pour le chiffrement, garantissant ainsi que vos données restent sécurisées sans intervention manuelle.

Pour plus d'informations sur la configuration de vos clés et la configuration de la rotation des clés, reportez-vous aux rubriques de documentation Microsoft Azure suivantes :

- ["Configurer la rotation automatique des clés cryptographiques dans Azure Key Vault"](#)
- ["Azure PowerShell - Activer les clés gérées par le client"](#)



Après avoir configuré les touches, assurez-vous d'avoir sélectionné "[Activer la rotation automatique](#)", afin que Cloud Volumes ONTAP puisse utiliser les nouvelles clés lorsque les clés précédentes expirent. Si vous n'activez pas cette option sur le portail Azure, Cloud Volumes ONTAP ne peut pas détecter automatiquement les nouvelles clés, ce qui peut entraîner des problèmes avec le provisionnement du stockage.

#### Créer une identité gérée attribuée par l'utilisateur

Vous avez la possibilité de créer une ressource appelée identité gérée attribuée par l'utilisateur. Cela vous permet de crypter vos comptes de stockage lorsque vous créez un système Cloud Volumes ONTAP . Nous vous recommandons de créer cette ressource avant de créer un coffre de clés et de générer une clé.

La ressource a l'ID suivant : `userassignedidentity` .

## Étapes

1. Dans Azure, accédez aux services Azure et sélectionnez **Identités gérées**.
2. Cliquez sur **Créer**.
3. Fournissez les détails suivants :
  - **Abonnement** : Choisissez un abonnement. Nous vous recommandons de choisir le même abonnement que l'abonnement de l'agent Console.
  - **Groupe de ressources** : utilisez un groupe de ressources existant ou créez-en un nouveau.
  - **Région** : sélectionnez éventuellement la même région que l'agent de la console.
  - **Nom**: Saisissez un nom pour la ressource.
4. Ajoutez éventuellement des balises.
5. Cliquez sur **Créer**.

### Créer un coffre de clés et générer une clé

Le coffre de clés doit résider dans le même abonnement Azure et la même région dans lesquels vous prévoyez de créer le système Cloud Volumes ONTAP .

Si tu créé une [identité gérée attribuée par l'utilisateur](#) , lors de la création du coffre de clés, vous devez également créer une politique d'accès pour le coffre de clés.

## Étapes

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

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

- Le coffre de clés doit résider dans la même région que le système Cloud Volumes ONTAP .
- Les options suivantes doivent être activées :
  - **Suppression logicielle** (cette option est activée par défaut, mais ne doit *pas* être désactivée)
  - **Protection contre la purge**
  - **Azure Disk Encryption pour le chiffrement des volumes** (pour les systèmes à nœud unique, les paires HA dans plusieurs zones et les déploiements HA mono-AZ)



L'utilisation des clés de chiffrement gérées par le client Azure dépend de l'activation du chiffrement de disque Azure pour le coffre de clés.

- L'option suivante doit être activée si vous avez créé une identité gérée attribuée par l'utilisateur :
    - **Politique d'accès au coffre-fort**
2. Si vous avez sélectionné la stratégie d'accès au coffre-fort, cliquez sur Créer pour créer une stratégie d'accès pour le coffre-fort de clés. Sinon, passez à l'étape 3.
    - a. Sélectionnez les autorisations suivantes :
      - obtenir
      - liste
      - décrypter
      - crypter

- clé de déballage
- clé d'enveloppement
- vérifier
- signe

b. Sélectionnez l'identité gérée attribuée par l'utilisateur (ressource) comme principal.

c. Réviser et créer la politique d'accès.

### 3. "Générer une clé dans le coffre 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.

#### Créer un système qui utilise la clé de chiffrement

Après avoir créé le coffre de clés et généré une clé de chiffrement, 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.

#### Autorisations requises

Si vous souhaitez utiliser une clé gérée par le client avec un système Cloud Volumes ONTAP à nœud unique, assurez-vous que l'agent de la console 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"
```

#### "Afficher la dernière liste des autorisations"

##### Étapes

1. Obtenez la liste des coffres de clés de votre abonnement Azure à l'aide de l'appel d'API suivant.

Pour une paire HA : GET /azure/ha/metadata/vaults

Pour un nœud unique : GET /azure/vsa/metadata/vaults

Prenez note du **nom** et du **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 en utilisant l'appel API suivant.

Pour une paire HA : GET /azure/ha/metadata/keys-vault

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

Prenez note du **keyName**. Vous devrez spécifier cette valeur (ainsi que 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 API suivant.

a. Pour une paire HA :

```
POST /azure/ha/working-environments
```

Le corps de la requête doit inclure les champs suivants :

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```



Inclure le "userAssignedIdentity": " userAssignedIdentityId" champ si vous avez créé cette ressource pour être utilisée pour le chiffrement du compte de stockage.

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

b. Pour un système à nœud unique :

```
POST /azure/vsa/working-environments
```

Le corps de la requête doit inclure les champs suivants :

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```



Inclure le "userAssignedIdentity": " userAssignedIdentityId" champ si vous avez créé cette ressource pour être utilisée pour le chiffrement du compte de stockage.

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

## Résultat

Vous disposez d'un nouveau système Cloud Volumes ONTAP configuré pour utiliser votre clé gérée par le client pour le chiffrement des données.

## Configurer les licences pour Cloud Volumes ONTAP dans Azure

Une fois que vous avez décidé quelle option de licence vous souhaitez utiliser avec

Cloud Volumes ONTAP, quelques étapes sont nécessaires avant de pouvoir choisir cette option de licence lors de la création d'un nouveau système.

## Freemium

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

## Étapes

1. Dans le menu de navigation de gauche de la console NetApp, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement à l'utilisation sur la Place de marché Azure.

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

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

Select Charging Method

<input type="radio"/>	Professional	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Essential	By capacity <span style="font-size: 0.8em;">▼</span>
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Per Node	By node <span style="font-size: 0.8em;">▼</span>

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

### Licence basée sur la capacité

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

Les forfaits Essentiels et Professionnel sont disponibles avec les modèles de consommation suivants :

- Une licence (apportez votre propre licence (BYOL)) achetée auprès de NetApp
- Un abonnement horaire à la carte (PAYGO) de la Place de marché Azure
- Un contrat annuel

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

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

### Apportez votre propre vin

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



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

### Étapes

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

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

Votre licence doit être disponible depuis la console avant de pouvoir l'utiliser avec Cloud Volumes ONTAP.

Si nécessaire, vous pouvez "[ajouter manuellement la licence à la console](#)".

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

La licence que vous avez achetée auprès de NetApp est toujours facturée en premier, mais vous serez facturé au tarif horaire du marché si vous dépassez votre capacité sous licence ou si la durée de votre licence expire.

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

Select Charging Method

<input checked="" type="radio"/> Professional	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1em;">▼</span>
<input type="radio"/> Essential	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1em;">▼</span>
<input type="radio"/> Freemium (Up to 500 GiB)	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1em;">▼</span>
<input type="radio"/> Per Node	<span style="background-color: #6f42c1; color: white; padding: 2px 5px;">By node</span> <span style="font-size: 1em;">▼</span>

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

### Abonnement PAYGO

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

Lorsque vous créez un système Cloud Volumes ONTAP , la console vous invite à vous abonner au contrat disponible sur la Place de marché Azure. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes supplémentaires.

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systemes**, cliquez sur **Ajouter un système** et suivez les étapes.
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement à l'utilisation sur la Place de marché Azure.

## Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Azure Subscription

Marketplace Subscription

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

[+ Add Subscription](#)

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

### Select Charging Method

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

"Consultez les instructions étape par étape 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. ["Apprenez à gérer vos comptes et abonnements Azure"](#)

## Contrat annuel

Payez Cloud Volumes ONTAP annuellement en achetant un contrat annuel.

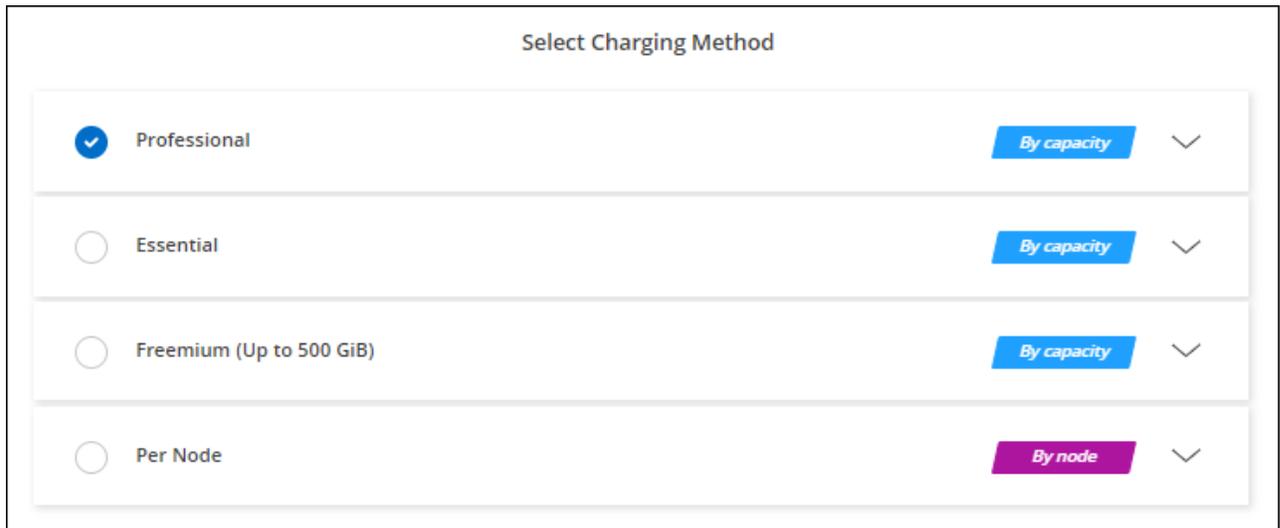
### Étapes

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

Le contrat est disponible sous forme d'offre *privée* sur la Place de marché Azure.

Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à partir de la Place de marché Azure lors de la création du système.

2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement > Continuer**.
  - b. Dans le portail Azure, sélectionnez le plan annuel qui a été partagé avec votre compte Azure, puis cliquez sur **S'abonner**.
  - c. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



Select Charging Method	
<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 les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure"](#) .

### Abonnement Keystone

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

### Étapes

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

- a. Sélectionnez la méthode de facturation de l'abonnement Keystone lorsque vous êtes invité à choisir une méthode de facturation.

The screenshot shows a 'Select Charging Method' dialog box. The 'Keystone' option is selected, indicated by a blue checkmark. Below the 'Keystone' option, there is a dropdown menu for 'Keystone Subscription' with the value 'A-AMRITA1'. Other options include 'Professional', 'Essential', 'Freemium (Up to 500 GiB)', and 'Per Node'. Each option has a 'By capacity' or 'By node' button and a chevron icon.

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

### Activer le mode haute disponibilité pour Cloud Volumes ONTAP dans Azure

Le mode haute disponibilité (HA) de Microsoft Azure doit être activé pour réduire les temps de basculement imprévus et pour activer la prise en charge NFSv4 pour Cloud Volumes ONTAP. Dans ce mode, vos nœuds Cloud Volumes ONTAP HA peuvent atteindre un objectif de temps de récupération (RTO) faible (60 secondes) lors de basculements non planifiés sur les clients CIFS et NFSv4.

À partir de Cloud Volumes ONTAP 9.10.1, nous avons réduit le temps de basculement non planifié pour les paires Cloud Volumes ONTAP HA exécutées dans Microsoft Azure et ajouté la prise en charge de NFSv4. Pour rendre ces améliorations disponibles pour Cloud Volumes ONTAP, vous devez activer la fonctionnalité de haute disponibilité sur votre abonnement Azure.

La console NetApp vous demande ces détails lorsque la fonctionnalité doit être activée sur un abonnement Azure.

Notez ce qui suit :

- Il n'y a aucun problème avec la haute disponibilité de votre paire Cloud Volumes ONTAP HA. Cette fonctionnalité Azure fonctionne de concert avec ONTAP pour réduire le temps d'interruption d'application

observé par le client pour les protocoles NFS résultant d'événements de basculement non planifiés.

- L'activation de cette fonctionnalité n'interrompt pas les paires Cloud Volumes ONTAP HA.
- L'activation de cette fonctionnalité sur votre abonnement Azure ne pose aucun problème aux autres machines virtuelles.
- Cloud Volumes ONTAP utilise un équilibreur de charge Azure interne lors des basculements des LIF de gestion de cluster et de SVM sur les clients CIFS et NFS.
- Lorsque le mode HA est activé, la console analyse le système toutes les 12 heures pour mettre à jour les règles internes d'Azure Load Balancer.

Un utilisateur Azure disposant des privilèges « Propriétaire » peut activer la fonctionnalité à partir de l'interface de ligne de commande Azure.

## Étapes

1. ["Accéder à Azure Cloud Shell depuis le portail Azure"](#)
2. Enregistrer la fonctionnalité du 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. Vérifiez éventuellement que la fonctionnalité est désormais enregistrée :

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

L'interface de ligne de commande Azure doit renvoyer un résultat similaire au suivant :

```
{
  "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"
}
```

## Activer VMOrchestratorZonalMultiFD pour Cloud Volumes ONTAP dans Azure

Pour déployer des instances de machine virtuelle dans des zones de disponibilité unique (AZ) de stockage localement redondant (LRS), vous devez activer Microsoft

Microsoft.Compute/VMOrchestratorZonalMultiFD fonctionnalité pour vos abonnements. En mode haute disponibilité (HA), cette fonctionnalité facilite le déploiement de nœuds dans des domaines de pannes distincts dans la même zone de disponibilité.

À moins que vous n'activiez cette fonctionnalité, le déploiement zonal ne se produit pas et le déploiement non zonal LRS précédent devient effectif.

Pour plus d'informations sur le déploiement de machines virtuelles dans une zone de disponibilité unique, reportez-vous à ["Paires à haute disponibilité dans Azure"](#) .

Effectuez ces étapes en tant qu'utilisateur avec des privilèges « Propriétaire » :

### Étapes

1. Accédez à Azure Cloud Shell depuis le portail Azure. Pour plus d'informations, reportez-vous à la ["Documentation Microsoft Azure : Prise en main d'Azure Cloud Shell"](#) .
2. Inscrivez-vous au Microsoft.Compute/VMOrchestratorZonalMultiFD fonctionnalité en exécutant cette commande :

```
az account set -s <nom_ou_ID_d_abonnement_Azure> az feature register --name
VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

3. Vérifiez l'état d'enregistrement et l'échantillon de sortie :

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id":
"/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestra
torZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state":
"Registered" }, "type": "Microsoft.Features/providers/features" }
```

### Lancer Cloud Volumes ONTAP dans Azure

Vous pouvez lancer un système à nœud unique ou une paire HA dans Azure en créant un système Cloud Volumes ONTAP dans la console NetApp .

#### Avant de commencer

Vous avez besoin des éléments suivants avant de commencer.

- Un agent de console opérationnel.
  - Vous devriez avoir un ["Agent de console associé à votre système"](#) .
  - ["Vous devez être prêt à laisser l'agent de la console en cours d'exécution à tout moment."](#) .
- Une compréhension de la configuration que vous souhaitez utiliser.

Vous devez avoir une configuration planifiée et les détails de mise en réseau Azure nécessaires auprès de votre administrateur. Pour plus d'informations, reportez-vous à ["Planification de votre configuration Cloud Volumes ONTAP"](#) .

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

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

## À propos de cette tâche

Lorsque la console crée un système Cloud Volumes ONTAP dans Azure, elle 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

La meilleure pratique consiste à utiliser un nouveau groupe de ressources dédié pour chaque système Cloud Volumes ONTAP .



Le déploiement de Cloud Volumes ONTAP dans un groupe de ressources partagé existant n'est pas recommandé en raison du risque de perte de données. Bien que la console puisse supprimer les ressources Cloud Volumes ONTAP d'un groupe de ressources partagé en cas d'échec de déploiement ou de suppression, un utilisateur Azure peut supprimer accidentellement les ressources Cloud Volumes ONTAP d'un groupe de ressources partagé.

## Lancer un système Cloud Volumes ONTAP à nœud unique dans Azure

Si vous souhaitez lancer un système Cloud Volumes ONTAP à nœud unique dans Azure, vous devez créer un système à nœud unique dans la console.

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. **Choisissez un emplacement** : sélectionnez **Microsoft Azure** et \* Cloud Volumes ONTAP Single Node\*.
4. Si vous y êtes invité, "[créer un agent de console](#)" .
5. **Détails et informations d'identification** : vous pouvez modifier les informations d'identification et l'abonnement Azure, spécifier un nom de cluster, ajouter des balises si nécessaire, puis spécifier les informations d'identification.

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

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Balises du groupe de ressources	Les balises sont des métadonnées pour vos ressources Azure. Lorsque vous entrez des balises dans ce champ, la console 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 système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les balises, reportez-vous à la " <a href="#">Documentation Microsoft Azure : Utilisation de balises pour organiser vos ressources Azure</a> " .

Champ	Description
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier les informations d'identification	Vous pouvez choisir différentes informations d'identification Azure et un abonnement Azure différent à utiliser avec ce système Cloud Volumes ONTAP . Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné afin de déployer un système Cloud Volumes ONTAP à la carte. " <a href="#">Apprenez à ajouter des informations d'identification</a> " .

6. **Services** : activez ou désactivez les services individuels que vous souhaitez ou ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
- "[En savoir plus sur la classification des données NetApp](#)"
  - "[En savoir plus sur NetApp Backup and Recovery](#)"



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

7. **Emplacement** : sélectionnez une région, une zone de disponibilité, un réseau virtuel et un sous-réseau, puis cochez la case pour confirmer la connectivité réseau entre l'agent de la console et l'emplacement cible.



Pour les régions de Chine, les déploiements à nœud unique sont pris en charge uniquement dans Cloud Volumes ONTAP 9.12.1 GA et 9.13.0 GA. Vous pouvez mettre à niveau ces versions vers des correctifs et des versions ultérieures de Cloud Volumes ONTAP. Si vous souhaitez déployer des versions ultérieures de Cloud Volumes ONTAP dans les régions chinoises, contactez le support NetApp . Seules les licences achetées directement auprès de NetApp sont prises en charge dans les régions chinoises ; les abonnements au marché ne sont pas disponibles.

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

Le tableau suivant décrit les domaines pour lesquels vous pourriez 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. La meilleure pratique consiste à utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Bien qu'il soit possible de déployer Cloud Volumes ONTAP dans un groupe de ressources partagé existant, cela n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  Si le compte Azure que vous utilisez possède le "<a href="#">autorisations requises</a>", la console supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec de déploiement ou de suppression. </div>
Groupe de sécurité généré	<p>Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic :</p> <ul style="list-style-type: none"> <li>• Si vous choisissez <b>Réseau virtuel sélectionné uniquement</b>, la source du trafic entrant est la plage de sous-réseaux du réseau virtuel sélectionné et la plage de sous-réseaux du réseau virtuel sur lequel réside l'agent de la console. C'est l'option recommandée.</li> <li>• Si vous choisissez <b>Tous les réseaux virtuels</b>, la source du trafic entrant est la plage IP 0.0.0.0/0.</li> </ul>
Utiliser l'existant	<p>Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP . "<a href="#">Afficher le groupe de sécurité par défaut</a>" .</p>

9. \* Méthodes de facturation et compte NSS \* : spécifiez l'option de facturation que vous souhaitez utiliser avec ce système, puis spécifiez un compte de site de support NetApp .
    - "[En savoir plus sur les options de licence pour Cloud Volumes ONTAP](#)" .
    - "[Apprenez à configurer les licences](#)" .
  10. **Package préconfiguré** : sélectionnez l'un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.
- Si vous choisissez l'un des packages, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.
11. **Licence** : modifiez la version de Cloud Volumes ONTAP si nécessaire et sélectionnez un type de machine virtuelle.



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

12. **S'abonner depuis la Place de marché Azure** : cette page s'affiche si la console n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP. Suivez les étapes indiquées à l'écran. se référer à "[Déploiement programmatique des produits Marketplace](#)" pour plus d'informations.

13. **Ressources de stockage sous-jacentes** : choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données vers le stockage Blob doit être activée.

Notez ce qui suit :

- Si l'accès public à votre compte de stockage est désactivé dans le VNet, vous ne pouvez pas activer la hiérarchisation des données dans votre système Cloud Volumes ONTAP . Pour plus d'informations, reportez-vous à ["Règles du groupe de sécurité"](#) .
- Le type de disque correspond au volume initial. Vous pouvez choisir un type de disque différent pour les volumes suivants.
- La taille du disque concerne tous les disques de l'agrégat initial et tous les agrégats supplémentaires créés par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.

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

- Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants.

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

14. **Vitesse d'écriture et WORM** :

- a. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

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

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

Cette option n'est disponible que pour certains types de machines virtuelles. Pour savoir quels types de machines virtuelles sont pris en charge, reportez-vous à ["Configurations prises en charge par licence pour les paires HA"](#) .

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

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

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

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

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

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

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

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

### Volume Details & Protection

Volume Name <span style="float: right;">i</span> <input type="text" value="ABDcv5689"/>	Storage VM (SVM) <input type="text" value="svm_c...CVO1"/>
Volume Size <span style="float: right;">i</span> Unit <input type="text" value="100"/> <input type="text" value="GiB"/>	Snapshot Policy <input type="text" value="default"/>

default policy i

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

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Pour configurer Azure AD Domain Services comme serveur AD pour Cloud Volumes ONTAP, vous devez saisir <b>OU=AADDCC Computers</b> ou <b>OU=AADDCC Users</b> dans ce champ. <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["Documentation Azure : Créer une unité d'organisation (UO) dans un domaine géré par 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 le même que le domaine AD.
Serveur NTP	Sélectionnez <b>Utiliser le domaine Active Directory</b> pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la <a href="#">"Documentation sur l'automatisation de la console NetApp"</a> pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

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

nécessaire.

Pour plus d'informations, reportez-vous à "[Comprendre les profils d'utilisation du volume](#)" et "[Présentation de la hiérarchisation des données](#)".

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

- a. Consultez les détails de la configuration.
- b. Cliquez sur **Plus d'informations** pour consulter les détails sur le support et les ressources Azure que la console achètera.
- c. Cochez les cases **Je comprends....**
- d. Cliquez sur **Aller**.

### Résultat

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

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

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

### Après avoir terminé

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

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

### Lancer une paire Cloud Volumes ONTAP HA dans Azure

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans Azure, vous devez créer un système HA dans la console.

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. Si vous y êtes invité, "[créer un agent de console](#)".
4. **Détails et informations d'identification** : vous pouvez modifier les informations d'identification et l'abonnement Azure, spécifier un nom de cluster, ajouter des balises si nécessaire, puis spécifier les informations d'identification.

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

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et 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 du groupe de ressources	Les balises sont des métadonnées pour vos ressources Azure. Lorsque vous entrez des balises dans ce champ, la console 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 système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les balises, reportez-vous à la " <a href="#">Documentation Microsoft Azure : Utilisation de balises pour organiser vos ressources Azure</a> " .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier les informations d'identification	Vous pouvez choisir différentes informations d'identification Azure et un abonnement Azure différent à utiliser avec ce système Cloud Volumes ONTAP . Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné afin de déployer un système Cloud Volumes ONTAP à la carte. " <a href="#">Apprenez à ajouter des informations d'identification</a> " .

5. **Services** : activez ou désactivez les services individuels selon que vous souhaitez les utiliser avec Cloud Volumes ONTAP.

- "[En savoir plus sur la classification des données NetApp](#)"
- "[En savoir plus sur NetApp Backup and Recovery](#)"



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

6. **Modèles de déploiement HA:**

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

- Pour les zones de disponibilité uniques, sélectionnez une région Azure, une zone de disponibilité, un réseau virtuel et un sous-réseau.

À partir de Cloud Volumes ONTAP 9.15.1, vous pouvez déployer des instances de machine virtuelle (VM) en mode HA dans des zones de disponibilité uniques (AZ) dans Azure. Vous devez sélectionner une zone et une région qui prennent en charge ce déploiement. Si la zone ou la région ne prend pas en charge le déploiement zonal, le mode de déploiement non zonal précédent pour LRS est suivi. Pour comprendre les configurations prises en charge pour les disques gérés partagés, reportez-vous à "[Configuration de zone de disponibilité unique HA avec disques gérés partagés](#)" .

- Pour plusieurs zones de disponibilité, sélectionnez une région, un réseau virtuel, un sous-réseau, une zone pour le nœud 1 et une zone pour le nœud 2.

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

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

Le tableau suivant décrit les domaines pour lesquels vous pourriez 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. La meilleure pratique consiste à utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Bien qu'il soit possible de déployer Cloud Volumes ONTAP dans un groupe de ressources partagé existant, cela 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 Cloud Volumes ONTAP HA que vous déployez dans Azure. Une seule paire HA est prise en charge dans un groupe de ressources. La console rencontre des problèmes de connexion si vous essayez de déployer une deuxième paire Cloud Volumes ONTAP HA dans un groupe de ressources Azure.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Si le compte Azure que vous utilisez possède le "<a href="#">autorisations requises</a>", la console supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec de déploiement ou de suppression.</p> </div>
Groupe de sécurité généré	<p>Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic :</p> <ul style="list-style-type: none"> <li>• Si vous choisissez <b>Réseau virtuel sélectionné uniquement</b>, la source du trafic entrant est la plage de sous-réseaux du réseau virtuel sélectionné et la plage de sous-réseaux du réseau virtuel sur lequel réside l'agent de la console. C'est l'option recommandée.</li> <li>• Si vous choisissez <b>Tous les réseaux virtuels</b>, la source du trafic entrant est la plage IP 0.0.0.0/0.</li> </ul>
Utiliser l'existant	<p>Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP . "<a href="#">Afficher le groupe de sécurité par défaut</a>" .</p>

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

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

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

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

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



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

11. **Abonnez-vous depuis la Place de marché Azure** : suivez les étapes si la console n'a pas pu 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 la hiérarchisation des données vers le stockage Blob doit être activée.

Notez ce qui suit :

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

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

- Si l'accès public à votre compte de stockage est désactivé dans le VNet, vous ne pouvez pas activer la hiérarchisation des données dans votre système Cloud Volumes ONTAP . Pour plus d'informations, reportez-vous à ["Règles du groupe de sécurité"](#) .
- Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
- Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants.

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

- À partir de Cloud Volumes ONTAP 9.15.0P1, les blobs de pages Azure ne sont plus pris en charge pour les nouveaux déploiements de paires haute disponibilité. Si vous utilisez actuellement des blobs de pages Azure dans des déploiements de paires haute disponibilité existants, vous pouvez migrer vers des types d'instances de machine virtuelle plus récents dans les machines virtuelles des séries Edsv4 et Edsv5.

["En savoir plus sur les configurations prises en charge dans Azure"](#) .

### 13. **Vitesse d'écriture et WORM** :

- a. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

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

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

Cette option n'est disponible que pour certains types de machines virtuelles. Pour savoir quels types de machines virtuelles sont pris en charge, reportez-vous à ["Configurations prises en charge par licence pour les paires HA"](#) .

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

est bloqué après l'activation de WORM et de la hiérarchisation.

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

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

14. \* Communication sécurisée avec le stockage et WORM \* : choisissez d'activer ou non une connexion HTTPS aux comptes de stockage Azure et d'activer le stockage WORM (écriture unique, lecture multiple), si vous le souhaitez.

La connexion HTTPS provient d'une paire Cloud Volumes ONTAP 9.7 HA vers des 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 le système.

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

WORM ne peut pas être activé si la hiérarchisation des données a été activée.

["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 protocoles et versions clients pris en charge"](#) .

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

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation ou non du provisionnement dynamique, qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une politique d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, la console entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur en utilisant le format domaine\nom d'utilisateur.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.

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 d'initiateurs sont des tables de noms de nœuds d'hôtes iSCSI et contrôlent quels initiateurs ont accès à quels LUN. Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, " <a href="#">utilisez l'IQN pour vous connecter au LUN depuis vos hôtes</a> ".

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

The screenshot shows a configuration window titled "Volume Details & Protection". It contains several input fields and dropdown menus:

- Volume Name:** A text input field containing "ABDcv5689".
- Storage VM (SVM):** A dropdown menu showing "svm\_c...CVO1".
- Volume Size:** A text input field containing "100".
- Unit:** A dropdown menu showing "GiB".
- Snapshot Policy:** A dropdown menu showing "default".
- Below the Snapshot Policy dropdown, there is a label "default policy" with an information icon.

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

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Pour configurer Azure AD Domain Services comme serveur AD pour Cloud Volumes ONTAP, vous devez saisir <b>OU=AADDCC Computers</b> ou <b>OU=AADDCC Users</b> dans ce champ. <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["Documentation Azure : Créer une unité d'organisation (UO) dans un domaine géré par 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 le même que le domaine AD.
Serveur NTP	Sélectionnez <b>Utiliser le domaine Active Directory</b> pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la <a href="#">"Documentation sur l'automatisation de la console NetApp"</a> pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

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

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

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

- Consultez les détails de la configuration.
- Cliquez sur **Plus d'informations** pour consulter les détails sur le support et les ressources Azure que la console achètera.
- Cochez les cases **Je comprends....**
- Cliquez sur **Aller**.

### Résultat

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

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

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

### Après avoir terminé

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

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

## Vérifier l'image de la plateforme Azure

### Vérification d'image de la place de marché Azure pour Cloud Volumes ONTAP

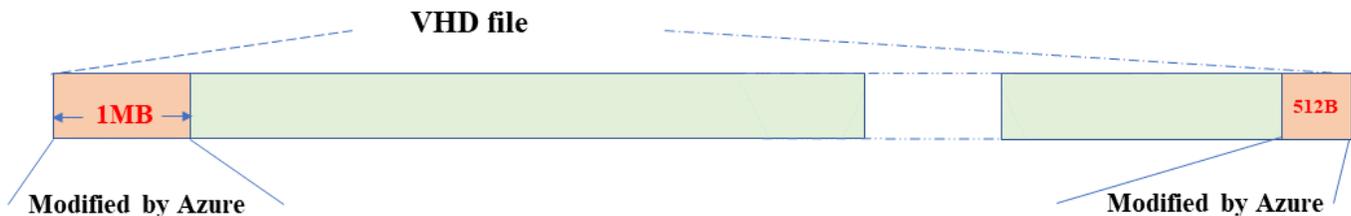
La vérification des images Azure est conforme aux exigences de sécurité renforcées de NetApp . La vérification d'un fichier image est un processus simple. Cependant, la vérification de la signature de l'image Azure nécessite des considérations spécifiques pour le fichier image Azure VHD, car il est modifié sur la place de marché Azure.



La vérification d'image Azure est prise en charge sur Cloud Volumes ONTAP 9.15.0 et versions ultérieures.

### Modification des fichiers VHD publiés par Azure

Les 1 Mo (1048576 octets) au début et les 512 octets à la fin du fichier VHD sont modifiés par Azure. NetApp signe le fichier VHD restant.



Dans l'exemple, le fichier VHD est de 10 Go. La partie signée par NetApp est marquée en vert (10 Go - 1 Mo - 512 octets).

### Liens connexes

- ["Blog sur les erreurs de page : Comment signer et vérifier avec OpenSSL"](#)
- ["Utiliser l'image Azure Marketplace pour créer une image de machine virtuelle pour votre GPU Azure Stack Edge Pro | Microsoft Learn"](#)
- ["Exporter/copier un disque géré vers un compte de stockage via Azure CLI | Microsoft Learn"](#)
- ["Démarrage rapide d'Azure Cloud Shell - Bash | Microsoft Learn"](#)
- ["Comment installer Azure CLI | Microsoft Learn"](#)
- ["Copie de blob de stockage AZ | Microsoft Learn"](#)
- ["Sign in avec Azure CLI — Connexion et authentification | Microsoft Learn"](#)

### Téléchargez le fichier image Azure pour Cloud Volumes ONTAP

Vous pouvez télécharger le fichier image Azure à partir du ["Site de support NetApp"](#) .

Le fichier *tar.gz* contient les fichiers nécessaires à la vérification de la signature de l'image. En plus du fichier *tar.gz*, vous devez également télécharger le fichier *checksum* de l'image. Le fichier de somme de contrôle contient le md5 et sha256 sommes de contrôle du fichier *tar.gz*.

### Étapes

1. Aller à la ["Page produit Cloud Volumes ONTAP sur le site de support NetApp"](#) et téléchargez la version du logiciel requise à partir de la section **Téléchargements**.
2. Sur la page de téléchargement de Cloud Volumes ONTAP , cliquez sur le fichier téléchargeable pour

l'image Azure et téléchargez le fichier *tar.gz*.

## Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

### Cloud Volumes ONTAP

#### Non-Restricted Countries

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

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ [2.58 GB]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ.PEM [451 B]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ.SIG [256 B]**

[View and download checksums](#)

### Cloud Volumes ONTAP

#### Restricted Countries

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

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ [2.58 GB]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ.PEM [451 B]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ.SIG [256 B]**

[View and download checksums](#)

### Cloud Volumes ONTAP

**DOWNLOAD GCP-9-15-0P1\_PKG.TAR.GZ [7.49 KB]**

[View and download checksums](#)

**DOWNLOAD AZURE-9-15-0P1\_PKG.TAR.GZ [7.64 KB]**

[View and download checksums](#)

3. Sous Linux, exécutez `md5sum AZURE-<version>_PKG.TAR.GZ` .

Sur macOS, exécutez `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Vérifiez que le `md5sum` et `sha256sum` les valeurs correspondent à celles de l'image Azure téléchargée.

5. Sous Linux et macOS, extrayez le fichier *tar.gz* à l'aide de la commande `tar -xzf` commande.

Le fichier *tar.gz* extrait contient le fichier digest (*.sig*), le fichier de certificat de clé publique (*.pem*) et le fichier de certificat de chaîne (*.pem*).

#### Exemple de sortie après extraction du fichier *tar.gz* :

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp 384 May 13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May 13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 version_readme
```

#### Exporter des images VHD pour Cloud Volumes ONTAP depuis la place de marché Azure

Une fois l'image VHD publiée sur le cloud Azure, elle n'est plus gérée par NetApp. Au lieu de cela, l'image publiée est placée sur la place de marché Azure. Lorsque l'image est préparée et publiée sur la place de marché Azure, Azure modifie 1 Mo au début et 512 octets à la fin du VHD. Pour vérifier la signature du fichier VHD, vous devez exporter

l'image VHD modifiée par Azure à partir de la place de marché Azure.

### Avant de commencer

Assurez-vous que l'interface de ligne de commande Azure est installée sur votre système ou qu'Azure Cloud Shell est disponible via le portail Azure. Pour plus d'informations sur l'installation de l'interface de ligne de commande Azure, reportez-vous à la ["Documentation Microsoft : Comment installer Azure CLI"](#) .

### Étapes

1. Mappez la version Cloud Volumes ONTAP sur votre système à la version de l'image de la place de marché Azure à l'aide du contenu du fichier `version_readme`. La version Cloud Volumes ONTAP est représentée par `buildname` et la version de l'image de la place de marché Azure est représentée par `version` dans les mappages de versions.

Dans l'exemple suivant, la version Cloud Volumes ONTAP 9.15.0P1 est mappé à la version de l'image de la place de marché Azure 9150.01000024.05090105 . Cette version d'image de la place de marché Azure est utilisée ultérieurement pour définir l'URN de l'image.

```
[
  "buildname": "9.15.0P1",
  "publisher": "netapp",
  "version": "9150.01000024.05090105"
]
```

2. Identifiez la région dans laquelle vous souhaitez créer les machines virtuelles. Le nom de la région est utilisé comme valeur pour le `locName` variable lors de la définition de l'URN de l'image du marché. Pour lister les régions disponibles, exécutez cette commande :

```
az account list-locations -o table
```

Dans ce tableau, le nom de la région apparaît dans le `Name` champ.

```
$ az account list-locations -o table
DisplayName          Name          RegionalDisplayName
-----
East US              eastus        (US) East US
East US 2            eastus2       (US) East US 2
South Central US    southcentralus (US) South Central US
...
```

3. Consultez les noms de référence (SKU) pour les versions Cloud Volumes ONTAP correspondantes et les types de déploiement de machine virtuelle dans le tableau ci-dessous. Le nom du SKU est utilisé comme valeur pour le `skuName` variable lors de la définition de l'URN de l'image du marché.

Par exemple, tous les déploiements à nœud unique avec Cloud Volumes ONTAP 9.15.0 doivent utiliser

ontap\_cloud\_byol comme nom de référence.

* Version Cloud Volumes ONTAP *	Déploiement de VM via	Nom du SKU
9.17.1 et versions ultérieures	La place de marché Azure	ontap_cloud_direct_gen2
9.17.1 et versions ultérieures	La console NetApp	ontap_cloud_gen2
9.16.1	La place de marché Azure	ontap_cloud_direct
9.16.1	La console	ontap_cloud
9.15.1	La console	ontap_cloud
9.15.0	La console, déploiements à nœud unique	ontap_cloud_byol
9.15.0	La console, déploiements haute disponibilité (HA)	ontap_cloud_byol_ha

4. Après avoir mappé la version ONTAP et l'image de la place de marché Azure, exportez le fichier VHD à partir de la place de marché Azure à l'aide d'Azure Cloud Shell ou d'Azure CLI.

### Exporter un fichier VHD à l'aide d'Azure Cloud Shell sous Linux

À partir d'Azure Cloud Shell, exportez l'image de la place de marché vers le fichier VHD (par exemple, *9150.01000024.05090105.vhd*) et téléchargez-la sur votre système Linux local. Effectuez ces étapes pour obtenir l'image VHD à partir de la place de marché Azure.

#### Étapes

1. Définissez l'URN et d'autres paramètres de l'image du marché. Le format URN est `<publisher>:<offer>:<sku>:<version>`. Vous pouvez également répertorier les images du marché NetApp pour confirmer la version d'image correcte.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Créez un nouveau disque géré à partir de l'image du marketplace avec la version d'image correspondante :

```

PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnfl"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas

```

- Exportez le fichier VHD du disque géré vers le stockage Azure. Créez un conteneur avec le niveau d'accès approprié. Dans cet exemple, nous avons utilisé un conteneur nommé `vm-images` avec `Container` niveau d'accès. Obtenez la clé d'accès au compte de stockage à partir du portail Azure : **Comptes de stockage > *examplesname* > Clé d'accès > *key1* > *key* > Afficher > <copie>**

```

PS /home/user1> $storageAccountName = "examplesname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container $containerName
-Context $destContext -Blob $destBlobName

```

- Téléchargez l'image générée sur votre système Linux. Utilisez le `wget` commande pour télécharger le fichier VHD :

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

L'URL suit un format standard. Pour l'automatisation, vous pouvez dériver la chaîne URL comme indiqué ci-dessous. Vous pouvez également utiliser l'interface de ligne de commande Azure. `az` commande pour obtenir l'URL. Exemple d'URL : `https://examplesname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd`

- Nettoyer le disque géré

```

PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName

```

## Exporter un fichier VHD à l'aide d'Azure CLI sous Linux

Exportez l'image de la place de marché vers un fichier VHD à l'aide de l'interface de ligne de commande Azure à partir d'un système Linux local.

### Étapes

1. Connectez-vous à l'interface de ligne de commande Azure et répertoriez les images de la place de marché :

```
% az login --use-device-code
```

2. Pour vous connecter, utilisez un navigateur Web pour ouvrir la page <https://microsoft.com/devicelogin> et entrez le code d'authentification.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
  "architecture": "x64",
  "offer": "netapp-ontap-cloud",
  "publisher": "netapp",
  "sku": "ontap_cloud_byol",
  "urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
  "version": "9150.01000024.05090105"
},
...
```

3. Créez un nouveau disque géré à partir de l'image du marché avec la version d'image correspondante.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluelxpinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluelxpinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Pour automatiser le processus, le SAS doit être extrait de la sortie standard. Consultez les documents appropriés pour obtenir des conseils.

4. Exportez le fichier VHD à partir du disque géré.

- a. Créez un conteneur avec le niveau d'accès approprié. Dans cet exemple, un conteneur nommé `vm-images` avec `Container` le niveau d'accès est utilisé.
- b. Obtenez la clé d'accès au compte de stockage à partir du portail Azure : **Comptes de stockage > *examplesaname* > Clé d'accès > *key1* > *key* > Afficher > <copie>**

Vous pouvez également utiliser le `az` commande pour cette étape.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Vérifiez l'état de la copie du blob.

```

% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.bluelxpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....

```

## 6. Téléchargez l'image générée sur votre serveur Linux.

```

wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>

```

L'URL suit un format standard. Pour l'automatisation, vous pouvez dériver la chaîne URL comme indiqué ci-dessous. Vous pouvez également utiliser l'interface de ligne de commande Azure. `az` commande pour obtenir l'URL. Exemple d'URL :`https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd`

## 7. Nettoyer le disque géré

```

az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes

```

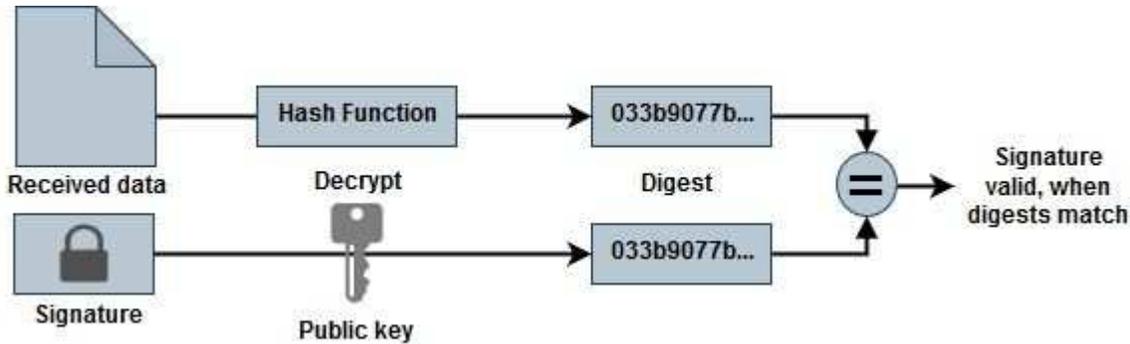
### Vérifier la signature du fichier

### Vérification de la signature d'image de la place de marché Azure pour Cloud Volumes ONTAP

Le processus de vérification d'image Azure génère un fichier de résumé à partir du fichier VHD en supprimant 1 Mo au début et 512 octets à la fin, puis en appliquant une fonction de hachage. Pour correspondre à la procédure de signature, `sha256` est utilisé pour le hachage.

## Résumé du flux de travail de vérification de la signature du fichier

Voici un aperçu du processus de vérification de la signature du fichier.



- Téléchargement de l'image Azure à partir du "[Site de support NetApp](#)" et extraire le fichier digest (.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem). Consultez "[Téléchargez le fichier de résumé de l'image Azure](#)" pour plus d'informations.
- Vérification de la chaîne de confiance.
- Extraction de la clé publique (.pub) du certificat de clé publique (.pem).
- Décryptage du fichier digest en utilisant la clé publique extraite.
- Comparaison du résultat avec un condensé nouvellement généré d'un fichier temporaire créé à partir du fichier image après avoir supprimé 1 Mo au début et 512 octets à la fin. Cette étape est réalisée à l'aide de l'outil de ligne de commande OpenSSL. L'outil OpenSSL CLI affiche un message approprié en cas de réussite ou d'échec de la correspondance des fichiers.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

## Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur Linux

La vérification d'une signature de fichier VHD exportée sous Linux comprend la validation de la chaîne de confiance, la modification du fichier et la vérification de la signature.

### Étapes

1. Téléchargez le fichier image Azure à partir du "[Site de support NetApp](#)" et extrayez le fichier digest (.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

Se référer à "[Téléchargez le fichier de résumé de l'image Azure](#)" pour plus d'informations.

2. Vérifier la chaîne de confiance.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Supprimez 1 Mo (1 048 576 octets) au début et 512 octets à la fin du fichier VHD. Lors de l'utilisation `tail`

, le `-c +K` l'option génère des octets à partir du K-ième octet du fichier. Par conséquent, il passe 1048577 à `tail -c`.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilisez OpenSSL pour extraire la clé publique du certificat et vérifiez le fichier dépouillé (`sign.tmp`) avec le fichier de signature et la clé publique.

L'invite de commande affiche des messages indiquant la réussite ou l'échec en fonction de la vérification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Nettoyer l'espace de travail.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur macOS

La vérification d'une signature de fichier VHD exportée sous Linux comprend la validation de la chaîne de confiance, la modification du fichier et la vérification de la signature.

### Étapes

1. Téléchargez le fichier image Azure à partir du ["Site de support NetApp"](#) et extrayez le fichier digest (`.sig`), le fichier de certificat de clé publique (`.pem`) et le fichier de certificat de chaîne (`.pem`).

Se référer à ["Téléchargez le fichier de résumé de l'image Azure"](#) pour plus d'informations.

2. Vérifier la chaîne de confiance.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Supprimez 1 Mo (1 048 576 octets) au début et 512 octets à la fin du fichier VHD. Lors de l'utilisation `tail`, le `-c +K` l'option génère des octets à partir du K-ième octet du fichier. Par conséquent, il passe 1048577 à `tail -c`. Notez que sur macOS, l'exécution de la commande `tail` peut prendre environ dix minutes.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilisez OpenSSL pour extraire la clé publique du certificat et vérifiez le fichier dépouillé (`sign.tmp`) avec le fichier de signature et la clé publique. L'invite de commande affiche des messages indiquant la réussite ou l'échec en fonction de la vérification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Nettoyer l'espace de travail.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## Déployer Cloud Volumes ONTAP depuis la place de marché Azure

Vous pouvez utiliser le déploiement direct de la place de marché Azure pour déployer rapidement et facilement Cloud Volumes ONTAP. Depuis la place de marché Azure, vous pouvez déployer rapidement Cloud Volumes ONTAP en quelques clics et explorer ses principales fonctionnalités et capacités dans votre environnement.

Pour plus d'informations sur cette offre, reportez-vous à ["Découvrez les offres Cloud Volumes ONTAP dans la console NetApp et sur la place de marché"](#).

### À propos de cette tâche

Le système Cloud Volumes ONTAP déployé à l'aide du déploiement direct de la place de marché Azure possède ces propriétés. Notez que les fonctionnalités d'une instance autonome déployée via la place de marché Azure changent lorsqu'elle est découverte dans la console NetApp.

- La dernière version de Cloud Volumes ONTAP (9.16.1 ou ultérieure).

- Une licence gratuite pour Cloud Volumes ONTAP limitée à 500 Gio de capacité provisionnée. Cette licence n'inclut aucun support NetApp et n'a pas de date d'expiration.
- Deux nœuds configurés en mode haute disponibilité (HA) dans une seule zone de disponibilité (AZ), provisionnés avec des numéros de série par défaut. Les machines virtuelles de stockage (VM de stockage) sont déployées dans un ["mode d'orchestration flexible"](#) .
- Un agrégat pour l'instance créée par défaut.
- Un disque géré SSD v2 Premium d'une capacité provisionnée de 500 Gio, ainsi qu'un disque racine et un disque de données.
- Une machine virtuelle de stockage de données déployée, avec des services de données NFS, CIFS, iSCSI et NVMe/TCP. Vous ne pouvez pas ajouter de machines virtuelles de stockage de données supplémentaires.
- Licences installées pour NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock et SnapMirror.
- ["Efficacité du stockage sensible à la température ONTAP \(TSSE\)"](#), chiffrage du volume et gestion des clés externes activés par défaut.
- Ces fonctionnalités ne sont pas prises en charge :
  - Hiérarchisation de FabricPool
  - Modification du type de machine virtuelle de stockage
  - Mode d'écriture rapide

## Avant de commencer

- Assurez-vous que vous disposez d'un abonnement à la place de marché Azure valide.
- Assurez-vous de répondre aux exigences de mise en réseau pour un ["Déploiement HA dans une seule zone de disponibilité"](#) dans Azure. ["Configurer le réseau Azure pour Cloud Volumes ONTAP"](#) .
- L'un de ces rôles Azure doit vous être attribué pour déployer Cloud Volumes ONTAP:
  - Le `contributor` rôle avec les autorisations par défaut. Pour plus d'informations, reportez-vous à la ["Documentation Microsoft Azure : rôles intégrés Azure"](#) .
  - Un rôle RBAC personnalisé avec les autorisations suivantes. Pour plus d'informations, reportez-vous à la ["Documentation Azure : rôles personnalisés Azure"](#) .

```
"permissions": [ { "actions": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```



Si vous avez enregistré le fournisseur de ressources « Microsoft.storage » dans votre abonnement, vous n'avez pas besoin du `Microsoft.AAD/register/action` autorisation. Pour plus d'informations, reportez-vous à la "[Documentation Azure : autorisations Azure pour le stockage](#)".

## Étapes

1. Depuis le site de la place de marché Azure, recherchez les produits NetApp .
2. Sélectionnez \* NetApp Cloud Volumes ONTAP direct\*.
3. Cliquez sur **Créer** pour lancer l'assistant de déploiement.
4. Sélectionnez un plan. La liste **Plan** affiche généralement les dernières versions de Cloud Volumes ONTAP.
5. Dans l'onglet **Bases**, fournissez les détails suivants :
  - **Abonnement** : Sélectionnez un abonnement. Le déploiement sera lié au numéro d'abonnement.
  - **Groupe de ressources** : utilisez un groupe de ressources existant ou créez-en un nouveau. Les groupes de ressources aident à allouer toutes les ressources, telles que les disques et les machines virtuelles de stockage, au sein d'un seul groupe pour un système Cloud Volumes ONTAP .
  - **Région** : sélectionnez une région qui prend en charge le déploiement d'Azure HA dans une seule zone de disponibilité. Vous ne voyez que les régions disponibles dans la liste.
  - **Taille** : sélectionnez une taille de machine virtuelle de stockage pour le disque géré SSD Premium v2 pris en charge.
  - **Zone** : sélectionnez une zone pour la région que vous avez sélectionnée.
  - **Mot de passe administrateur** : définissez un mot de passe. Vous utilisez ce mot de passe administrateur pour vous connecter au système après le déploiement.
  - **Confirmer le mot de passe** : saisissez à nouveau le même mot de passe pour confirmation.
    - Dans l'onglet **Réseau**, ajoutez un réseau virtuel et un sous-réseau, ou sélectionnez-les dans les listes.



Pour respecter les restrictions de Microsoft Azure, vous devez créer un nouveau sous-réseau lors de la configuration d'un nouveau réseau virtuel. De même, si vous choisissez un réseau existant, vous devez sélectionner un sous-réseau existant.

- Pour sélectionner un groupe de sécurité réseau prédéfini, sélectionnez **Oui**. Sélectionnez **Non** pour attribuer un groupe de sécurité réseau Azure prédéfini avec les règles de trafic nécessaires. Pour plus d'informations, reportez-vous à "[Règles de groupe de sécurité pour Azure](#)".
- Dans l'onglet **Avancé**, confirmez si les deux fonctionnalités Azure nécessaires à ce déploiement ont été définies. Se référer à "[Activer une fonctionnalité Azure pour les déploiements Cloud Volumes ONTAP à zone de disponibilité unique](#)" et "[Activer le mode haute disponibilité pour Cloud Volumes ONTAP dans Azure](#)".
- Vous pouvez définir des paires nom et valeur pour les ressources ou les groupes de ressources dans l'onglet **Tags**.
- Dans l'onglet **Réviser + créer**, vérifiez les détails et démarrez le déploiement.

## Après avoir terminé

Sélectionnez l'icône de notification pour afficher la progression de votre déploiement. Une fois Cloud Volumes ONTAP déployé, vous pouvez afficher la machine virtuelle de stockage répertoriée pour les opérations.

Une fois accessible, utilisez ONTAP System Manager ou ONTAP CLI pour vous connecter à la machine virtuelle de stockage avec les informations d'identification d'administrateur que vous avez définies. Par la suite, vous pouvez créer des volumes, des LUN ou des partages et commencer à utiliser les capacités de stockage de Cloud Volumes ONTAP.

## Résoudre les problèmes de déploiement

Les systèmes Cloud Volumes ONTAP déployés directement via la place de marché Azure n'incluent pas la prise en charge de NetApp. Si des problèmes surviennent pendant le déploiement, vous pouvez les résoudre de manière autonome.

### Étapes

1. Sur le site de la place de marché Azure, accédez à **Diagnostics de démarrage > Journal série**.
2. Téléchargez et examinez les journaux série.
3. Consultez la documentation du produit et les articles de la base de connaissances (KB) pour le dépannage.
  - ["Documentation de la place de marché Azure"](#)
  - ["Documentation NetApp"](#)
  - ["Articles de la base de connaissances NetApp"](#)

## Découvrez les systèmes déployés dans la console

Vous pouvez découvrir les systèmes Cloud Volumes ONTAP que vous avez déployés à l'aide du déploiement direct de la place de marché Azure et les gérer sur la page **Systèmes** de la console. L'agent de la console découvre les systèmes, les ajoute et applique les licences nécessaires, et déverrouille toutes les fonctionnalités de la console pour ces systèmes. La configuration HA d'origine dans une seule zone de disponibilité avec les disques gérés PSSD v2 est conservée et le système est enregistré sur le même abonnement Azure et le même groupe de ressources que le déploiement d'origine.

### À propos de cette tâche

Lors de la découverte des systèmes Cloud Volumes ONTAP déployés à l'aide du déploiement direct de la place de marché Azure, l'agent de la console exécute les tâches suivantes :

- Remplace les licences gratuites des systèmes découverts par des licences standard basées sur la capacité "[Licences Freemium](#)".
- Conserve les capacités existantes des systèmes déployés et ajoute les capacités supplémentaires de la console, telles que la protection des données, la gestion des données et les fonctionnalités de sécurité.
- Remplace les licences installées sur les nœuds par de nouvelles licences ONTAP pour NFS, CIFS (SMB), iSCSI, ARP, SnapLock et SnapMirror.
- Convertit les numéros de série des nœuds génériques en numéros de série uniques.
- Attribue de nouvelles balises système aux ressources selon les besoins.
- Convertit les adresses IP dynamiques de l'instance en adresses IP statiques.
- Permet les fonctionnalités de "[Hiérarchisation de FabricPool](#)", "[AutoSupport](#)", et "[écriture unique et lecture multiple](#)" Stockage (WORM) sur les systèmes déployés. Vous pouvez activer ces fonctionnalités depuis la console lorsque vous en avez besoin.
- Enregistre les instances sur les comptes NSS utilisés pour les découvrir.
- Active les fonctionnalités de gestion de la capacité dans "[modes automatique et manuel](#)" pour les systèmes découverts.

## Avant de commencer

Assurez-vous que le déploiement est terminé sur la place de marché Azure. L'agent de console peut découvrir les systèmes uniquement lorsque le déploiement est terminé et qu'ils sont disponibles pour la découverte.

## Étapes

Dans la console, vous suivez la procédure standard pour découvrir les systèmes existants. ["Ajouter un système Cloud Volumes ONTAP existant à la console"](#) .

## Après avoir terminé

Une fois la découverte terminée, vous pouvez afficher les systèmes répertoriés sur la page **Systemes** de la console. Vous pouvez effectuer diverses tâches de gestion, telles que ["élargir l'agrégat"](#) , ["ajout de volumes"](#) , ["provisionnement de machines virtuelles de stockage supplémentaires"](#) , et ["changer les types d'instances"](#) .

## Liens connexes

Reportez-vous à la documentation ONTAP pour plus d'informations sur la création de stockage :

- ["Créer des volumes pour NFS"](#)
- ["Créer des LUN pour iSCSI"](#)
- ["Créer des partages pour CIFS"](#)

# Démarrer avec Google Cloud

## Démarrage rapide de Cloud Volumes ONTAP dans Google Cloud

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

1

### Créer un agent de console

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

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

2

### Planifiez votre configuration

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

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

3

### Configurez votre réseau

1. Assurez-vous que votre VPC et vos sous-réseaux prendront en charge la connectivité entre l'agent de console et Cloud Volumes ONTAP.

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

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

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

## 4

### Configurer un compte de service

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

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

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

## 5

### Activer les API Google Cloud

["Activez les API Google Cloud suivantes dans votre projet"](#) . Ces API sont requises pour déployer l'agent de console et Cloud Volumes ONTAP.

- API du gestionnaire de déploiement cloud V2
- API de journalisation dans le cloud
- API du gestionnaire de ressources cloud
- API Compute Engine
- API de gestion des identités et des accès (IAM)

## 6

### Lancer Cloud Volumes ONTAP à l'aide de la console

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

#### Liens connexes

- ["Création d'un agent de console"](#)
- ["Installation du logiciel agent de console sur un hôte Linux"](#)
- ["Ce que fait la console avec les autorisations Google Cloud"](#)

## Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud

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

### Choisissez une licence Cloud Volumes ONTAP

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

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

### Choisissez une région prise en charge

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

### Choisissez un type de machine pris en charge

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

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

### Comprendre les limites de stockage

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

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

### Dimensionnez votre système dans GCP

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

#### Type de machine

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

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

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

## Type de disque GCP

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

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

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

## Taille du disque GCP

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

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

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

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

## Afficher les disques système par défaut

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

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

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



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

## Recueillir des informations sur le réseau

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

### Informations réseau pour un système à nœud unique

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

### Informations réseau pour une paire HA dans plusieurs zones

Informations sur les GCP	Votre valeur
Région	
Zone pour le nœud 1	
Zone pour le nœud 2	
Zone pour le médiateur	
VPC-0 et sous-réseau	
VPC-1 et sous-réseau	
VPC-2 et sous-réseau	
VPC-3 et sous-réseau	
Politique de pare-feu (si vous utilisez la vôtre)	

### Informations réseau pour une paire HA dans une seule zone

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

### Choisissez une vitesse d'écriture

La console vous permet de choisir un paramètre de vitesse d'écriture pour Cloud Volumes ONTAP, à l'exception des paires haute disponibilité (HA) dans Google Cloud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés, ainsi que les risques et les

recommandations lors de l'utilisation d'une vitesse d'écriture élevée. ["En savoir plus sur la vitesse d'écriture"](#) .

## Choisissez un profil d'utilisation du volume

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

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

### Provisionnement léger

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

### Déduplication

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

### Compression

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

## Configurer la mise en réseau Google Cloud pour Cloud Volumes ONTAP

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

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

## Exigences pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans Google Cloud.

### Exigences spécifiques aux systèmes à nœud unique

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

#### Un VPC

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

#### Adresses IP privées

Pour un système à nœud unique dans Google Cloud, la console alloue des adresses IP privées aux éléments suivants :

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

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

```
skipSvmManagementLif: true
```



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

### Exigences spécifiques aux paires HA

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

### Une ou plusieurs zones

Vous pouvez garantir la haute disponibilité de vos données en déployant une configuration HA sur plusieurs zones ou dans une seule zone. La console vous invite à choisir plusieurs zones ou une seule zone lorsque vous créez la paire HA.

- Zones multiples (recommandé)

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

- Zone unique

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

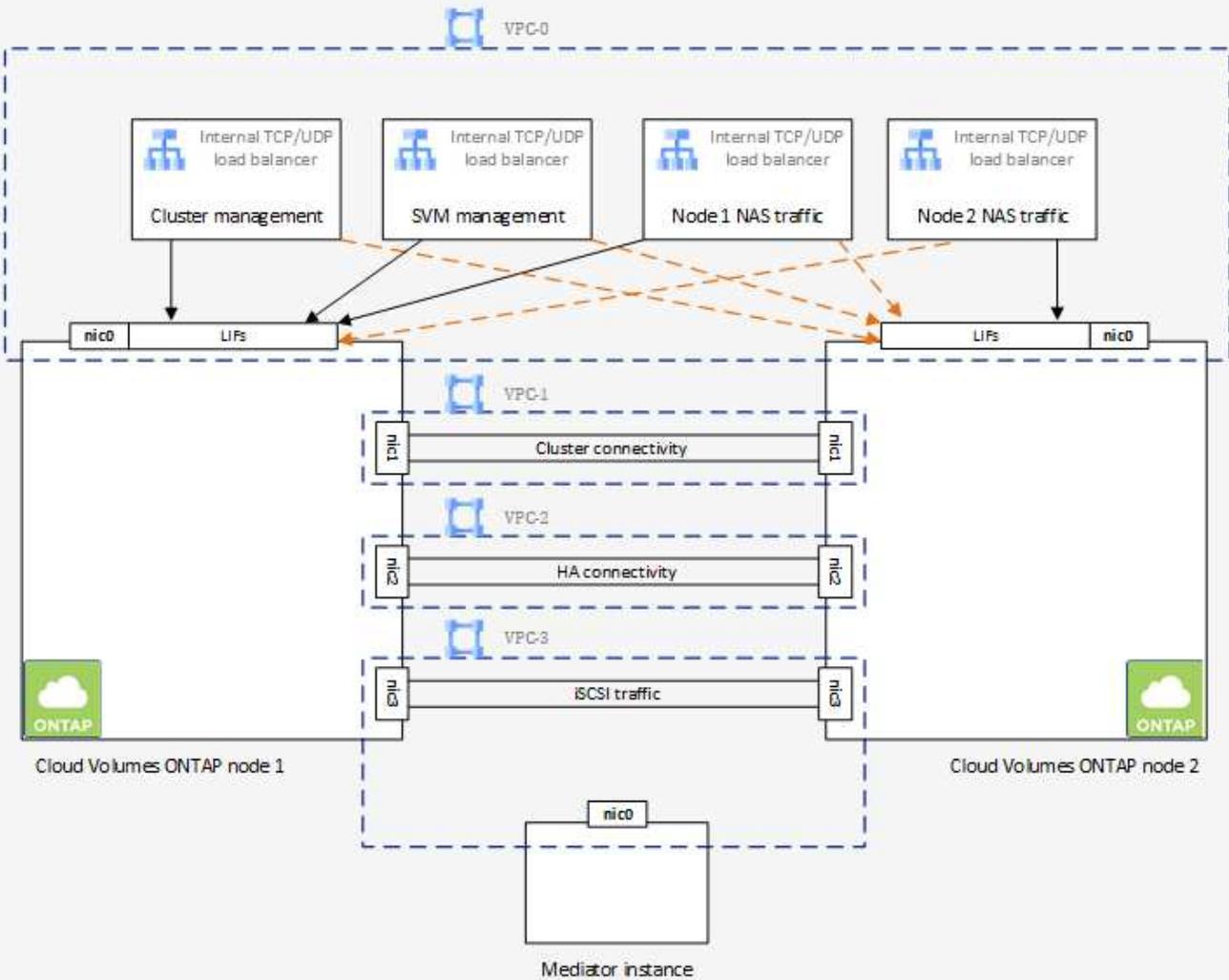
Ce modèle de déploiement réduit vos coûts car il n'y a pas de frais de sortie de données entre les zones.

### Quatre clouds privés virtuels

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

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

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



## Sous-réseaux

Un sous-réseau privé est requis pour chaque VPC.

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

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

## Adresses IP privées

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

Le nombre de LIF alloués à Cloud Volumes ONTAP dépend du fait que vous déployez un système à nœud unique ou une paire HA. Un LIF est une adresse IP associée à un port physique. Un LIF de gestion SVM est requis pour les outils de gestion tels que SnapCenter.

- **Nœud unique** La console alloue 4 adresses IP à un système à nœud unique :

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



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

- NAS LIF

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

```
skipSvmManagementLif: true
```

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

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



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

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

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

```
skipSvmManagementLif: true
```

## Équilibreurs de charge internes

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

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

La configuration de chaque équilibreur de charge est la suivante :

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

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

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

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

### **VPC partagés**

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

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

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

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

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

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

### **Mise en miroir des paquets dans les VPC**

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

### **Accès Internet sortant**

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

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

### **Points de terminaison Cloud Volumes ONTAP**

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

Points de terminaison	Applicable pour	But	Mode de déploiement	Impact si le point de terminaison n'est pas disponible
\ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : <ul style="list-style-type: none"> <li>• Services Cloud Volumes ONTAP</li> <li>• Services ONTAP</li> <li>• Protocoles et services proxy</li> </ul>
\ <a href="https://api.bluexp.netapp.com/tenancy">https://api.bluexp.netapp.com/tenancy</a>	Location	Utilisé pour récupérer la ressource Cloud Volumes ONTAP à partir de la console pour autoriser les ressources et les utilisateurs.	Modes standard et restreint.	Les ressources Cloud Volumes ONTAP et les utilisateurs ne sont pas autorisés.
\ <a href="https://mysupport.netapp.com/aods/asupmessage">https://mysupport.netapp.com/aods/asupmessage</a> \ <a href="https://mysupport.netapp.com/asupprod/post/1.0/postAsup">https://mysupport.netapp.com/asupprod/post/1.0/postAsup</a>	AutoSupport	Utilisé pour envoyer des données de télémétrie AutoSupport au support NetApp .	Modes standard et restreint.	Les informations AutoSupport ne sont toujours pas livrées.

Points de terminaison	Applicable pour	But	Mode de déploiement	Impact si le point de terminaison n'est pas disponible
\ <a href="https://www.googleapis.com/compute/v1/projects/">https://www.googleapis.com/compute/v1/projects/</a> \ <a href="https://cloudresource-manager.googleapis.com/v1/projects/">https://cloudresource-manager.googleapis.com/v1/projects</a> \ <a href="https://www.googleapis.com/compute/beta/">https://www.googleapis.com/compute/beta/</a> \ <a href="https://storage.googleapis.com/storage/v1/">https://storage.googleapis.com/storage/v1/</a> \ <a href="https://www.googleapis.com/storage/v1/">https://www.googleapis.com/storage/v1/</a> \ <a href="https://iam.googleapis.com/v1/">https://iam.googleapis.com/v1/</a> \ <a href="https://cloudkms.googleapis.com/v1/">https://cloudkms.googleapis.com/v1/</a> \ <a href="https://www.googleapis.com/deploymentmanager/v2/projects/">https://www.googleapis.com/deploymentmanager/v2/projects</a> \ <a href="https://compute.googleapis.com/compute/v1/">https://compute.googleapis.com/compute/v1</a>	Google Cloud (utilisation commerciale).	Communication avec les services Google Cloud.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Google Cloud pour effectuer des opérations spécifiques pour la console dans Google Cloud.

### Connexions aux systèmes ONTAP dans d'autres réseaux

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

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

### Règles du pare-feu

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

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

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

- Un ensemble de règles pour les composants HA dans VPC-0. Ces règles permettent l'accès aux données de Cloud Volumes ONTAP.
- Un autre ensemble de règles pour les composants HA dans VPC-1, VPC-2 et VPC-3. Ces règles sont

ouvertes à la communication entrante et sortante entre les composants HA. [Apprendre encore plus](#) .



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

## Règles entrantes

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

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

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

Protocole	Port	But
Tous les ICMP	Tous	Ping de l'instance
HTTP	80	Accès HTTP à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
HTTPS	443	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole simple de gestion de réseau
TCP	445	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
TCP	635	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Moniteur d'état du réseau pour NFS
TCP	10000	Sauvegarde à l'aide de NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster

Protocole	Port	But
TCP	63001-63050	Ports de sonde d'équilibrage de charge pour déterminer quel nœud est sain (requis pour les paires HA uniquement)
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole simple de gestion de réseau
UDP	635	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Moniteur d'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

### Règles de sortie

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

### Règles de base pour les voyages sortants

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

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

### Règles sortantes avancées

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



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

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

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

## Règles pour VPC-1, VPC-2 et VPC-3

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

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

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



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

## Exigences pour l'agent de console

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

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

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

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

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

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

## Configurer les balises réseau pour Cloud Volumes ONTAP dans Google Cloud

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

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

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

### Sujets connexes

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

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

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

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

### Comment les services NetApp communiquent avec les contrôles de service VPC

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

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

### Images

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

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

### Déploiement d'un agent de console

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

### Déploiement de Cloud Volumes ONTAP

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

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

## Politiques de périmètre des contrôles de service VPC

Les politiques autorisent des exceptions aux ensembles de règles VPC Service Controls. Pour plus d'informations sur les politiques, veuillez visiter le ["Documentation de la politique de contrôle des services VPC GCP"](#).

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

### Règles d'entrée

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

OU

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

OU

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

### Règles de sortie

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



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

## Créer un compte de service Google Cloud pour Cloud Volumes ONTAP

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

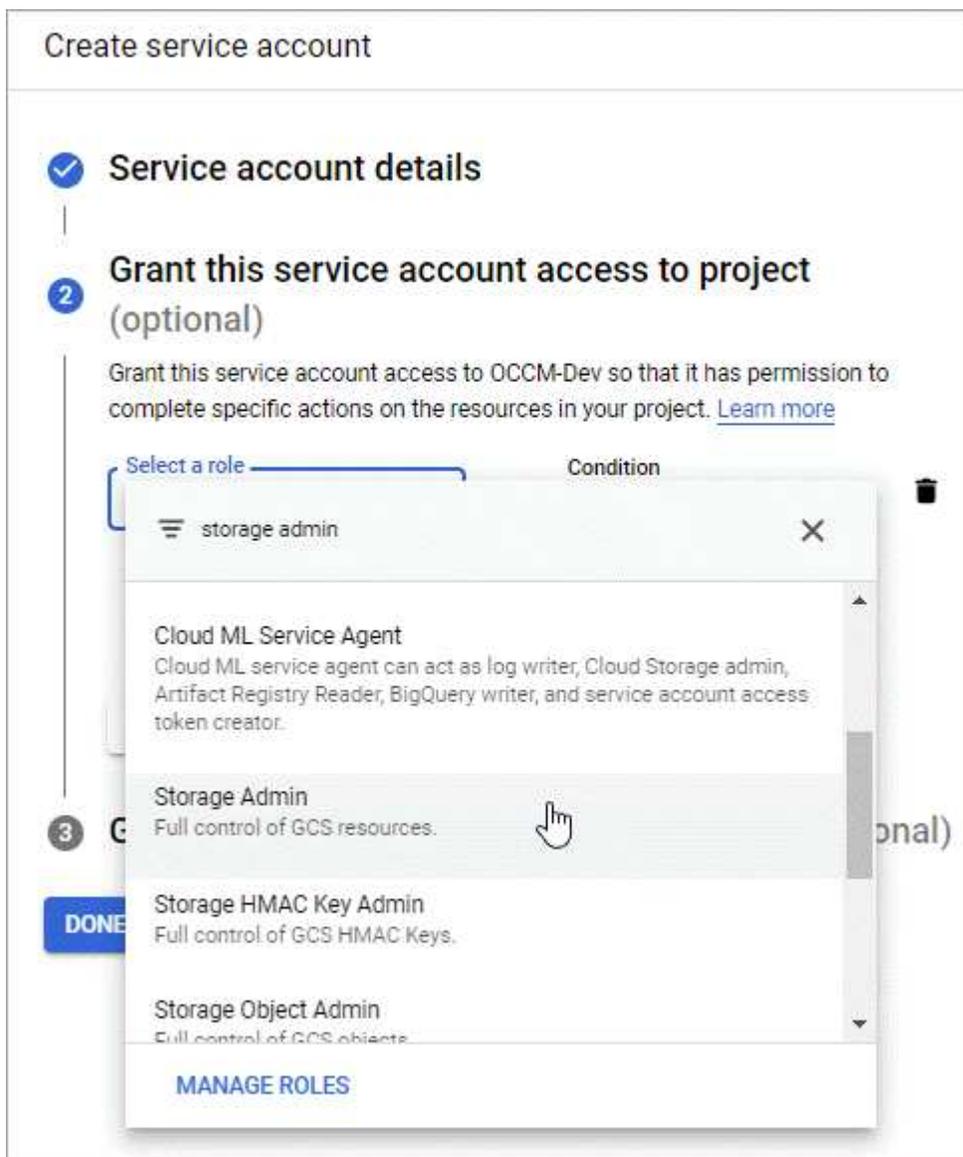
Cloud Volumes ONTAP utilise le compte de service pour accéder et gérer un bucket pour les données hiérarchisées et un autre bucket pour les sauvegardes.

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

### Étapes

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

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



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

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

Create service account

- ✓ Service account details
- ✓ Grant this service account access to project (optional)
- 3 Grant users access to this service account (optional)  
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

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

Service account admins role

Grant users the permission to administer this service account

**DONE** CANCEL

**Quelle est la prochaine étape ?**

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

## Details and Credentials

default-project Google Cloud Project	gcp-sub2 Marketplace Subscription	<a href="#">Edit Project</a>
---	--------------------------------------	------------------------------

### Details

Working Environment Name (Cluster Name)

Service Account

Service Account Name

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

### Credentials

User Name

Password

Confirm Password

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

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

### Étapes

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

Les autorisations sont fournies dans le "[les autorisations du compte de service par défaut](#)", mais peut ne pas 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 pour le "[Agent de service Google Compute Engine](#)" dispose des autorisations Cloud KMS Encrypter/Decrypter sur la clé.

Le nom du compte de service utilise le format suivant : « service-[numéro\_de\_projet\_service]@compute-system.iam.gserviceaccount.com ».

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

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

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

5. Utilisez le paramètre « GcpEncryption » avec votre requête API lors de la création d'un système.

### Exemple

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

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

## Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud

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

### Freemium

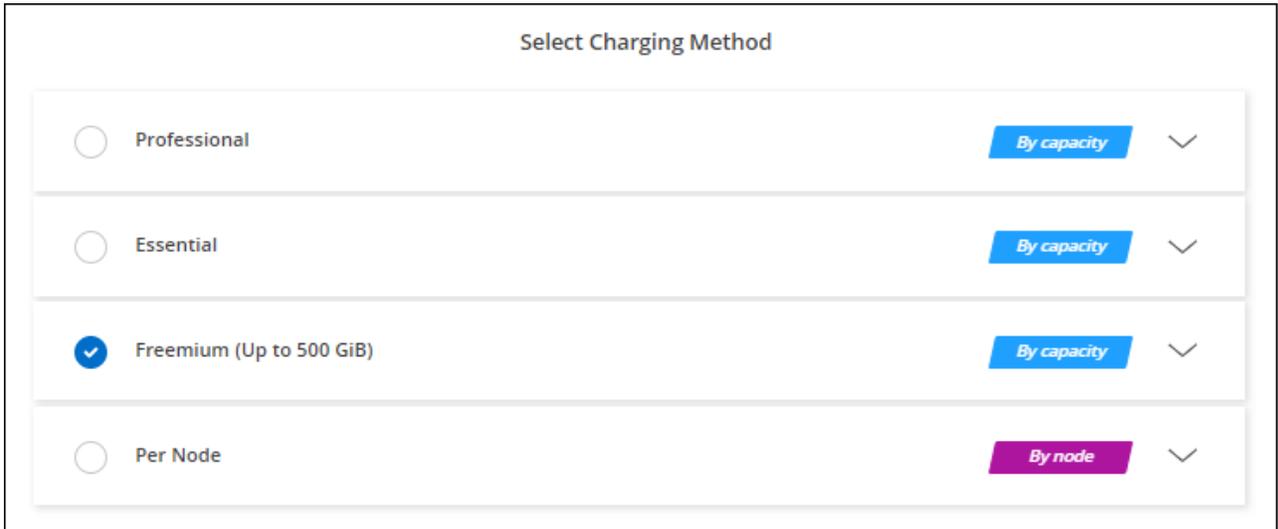
Sélectionnez l'offre Freemium pour utiliser Cloud Volumes ONTAP gratuitement avec jusqu'à 500 Gio de capacité provisionnée. ["En savoir plus sur l'offre Freemium"](#) .

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes de la console NetApp .
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner à l'offre de paiement à l'utilisation sur Google Cloud Marketplace.

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

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



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

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

### Licence basée sur la capacité

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

Les forfaits Essentiels et Professionnel sont disponibles avec les modèles de consommation suivants :

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

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

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

#### Apportez votre propre vin

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



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

### Étapes

1. ["Contactez le service commercial NetApp pour obtenir une licence"](#)

## 2. "Ajoutez votre compte de site de support NetApp à la console NetApp"

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

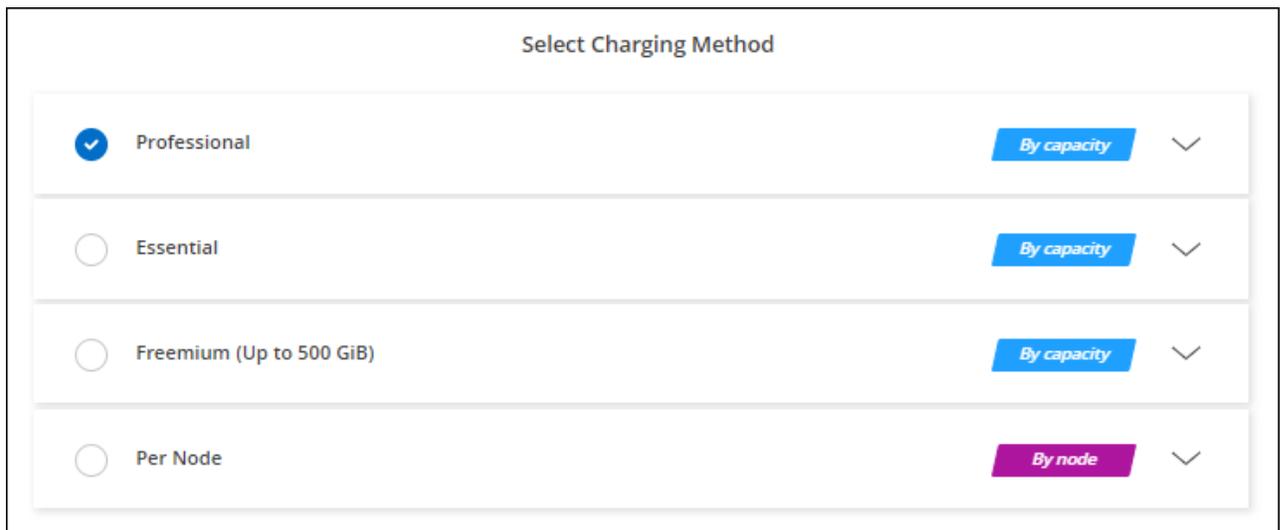
Votre licence doit être disponible depuis la console avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez "[ajouter manuellement la licence à la console](#)" .

## 3. Sur la page **Systemes**, cliquez sur **Ajouter un système** et suivez les étapes.

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

La licence que vous avez achetée auprès de NetApp est toujours facturée en premier, mais vous serez facturé au tarif horaire du marché si vous dépassez votre capacité sous licence ou si la durée de votre licence expire.

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



Select Charging Method	
<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 les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud](#)" .

### Abonnement PAYGO

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

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

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systemes**, cliquez sur **Ajouter un système** et suivez les étapes.
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner à l'offre de

paiement à l'utilisation sur Google Cloud Marketplace.

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

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



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

### Contrat annuel

Payez Cloud Volumes ONTAP annuellement en achetant un contrat annuel.

### Étapes

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

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

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

2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
  - a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les instructions pour vous abonner au forfait annuel sur Google Cloud Marketplace.
  - b. Dans Google Cloud, sélectionnez le forfait annuel partagé avec votre compte, puis cliquez sur **S'abonner**.
  - c. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.

Select Charging Method

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

### Abonnement Keystone

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

#### Étapes

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

### Select Charging Method

**Keystone**

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1
▼

By capacity

^

---

**Professional**

By capacity

▼

---

**Essential**

By capacity

▼

---

**Freemium (Up to 500 GiB)**

By capacity

▼

---

**Per Node**

By node

▼

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

## Lancer Cloud Volumes ONTAP dans Google Cloud

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

### Avant de commencer

Vous avez besoin des éléments suivants avant de commencer.

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

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

- Une compréhension de ce qui est nécessaire pour configurer les licences pour Cloud Volumes ONTAP.
  - ["Apprenez à configurer les licences"](#) .

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

## Lancer un système à nœud unique dans Google Cloud

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

### Étapes

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

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

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et l'instance de machine virtuelle Google Cloud. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Nom du compte de service	Si vous prévoyez d'utiliser <a href="#">"hiérarchisation des données"</a> ou <a href="#">"Sauvegarde et récupération NetApp"</a> avec Cloud Volumes ONTAP, vous devez activer <b>Compte de service</b> et sélectionner un compte de service doté du rôle d'administrateur de stockage prédéfini. <a href="#">"Apprenez à créer un compte de service"</a> .
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour vos ressources Google Cloud. La console ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources Google Cloud associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un système. Pour plus d'informations sur les étiquettes, reportez-vous à la <a href="#">"Documentation Google Cloud : Étiquetage des ressources"</a> .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.

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 se trouve la Console.</p> <p>Si vous ne voyez aucun projet supplémentaire dans la liste déroulante, cela signifie que vous n'avez pas encore associé le compte de service 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 que vous utilisez pour la console à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Il s'agit du compte de service que vous avez configuré pour la console, <a href="#">"comme décrit sur cette page"</a> . </div> <p>Cliquez sur <b>Ajouter un abonnement</b> pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP à la carte, vous devez sélectionner un projet Google Cloud associé à un abonnement à Cloud Volumes ONTAP sur la place de marché Google Cloud. Se référer à <a href="#">"Associer un abonnement Marketplace aux identifiants Google Cloud"</a> .</p>

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



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

7. **Emplacement et connectivité** : sélectionnez un emplacement, choisissez une politique de pare-feu et confirmez la connectivité réseau au stockage Google Cloud pour la hiérarchisation des données.

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

Champ	Description
Vérification de la connectivité	Pour hiérarchiser les données froides vers un bucket Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour l'accès privé à Google. Pour les instructions, reportez-vous à <a href="#">"Documentation Google Cloud : Configuration de l'accès privé à Google"</a> .
Politique de pare-feu générée	<p>Si vous laissez la console générer la politique de pare-feu pour vous, vous devez choisir comment vous autoriserez le trafic :</p> <ul style="list-style-type: none"> <li>• Si vous choisissez <b>VPC sélectionné uniquement</b>, le filtre source pour le trafic entrant est la plage de sous-réseaux du VPC sélectionné et la plage de sous-réseaux du VPC sur lequel réside l'agent de la console. C'est l'option recommandée.</li> <li>• Si vous choisissez <b>Tous les VPC</b>, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.</li> </ul>

Champ	Description
Utiliser la politique de pare-feu existante	Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises : " <a href="#">En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP</a> "

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

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

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

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

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



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

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

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

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

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

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

a. Activez **Flash Cache**, si vous le souhaitez.



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

b. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

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



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

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

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

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

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

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

Notez ce qui suit :

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

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

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

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

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

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

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 en utilisant le format domaine\nom d'utilisateur.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes d'initiateurs sont des tables de noms de nœuds d'hôtes iSCSI et contrôlent quels initiateurs ont accès à quels LUN. Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, " <a href="#">utilisez l'IQN pour vous connecter au LUN depuis vos hôtes</a> ".

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

The screenshot displays the 'Volume Details & Protection' configuration interface. It contains the following fields and values:

- Volume Name:** ABDcv5689
- Storage VM (SVM):** svm\_c...CVO1
- Volume Size:** 100
- Unit:** GiB
- Snapshot Policy:** default

Information icons (i) are present next to the Volume Name, Unit, and Snapshot Policy labels.

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

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

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

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

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

## Résultat

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

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

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

### Après avoir terminé

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

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

### Lancer une paire HA dans Google Cloud

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

#### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Stockage > Système** et suivez les instructions.
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 domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et l'instance de machine virtuelle Google Cloud. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Nom du compte de service	Si vous prévoyez d'utiliser le " <a href="#">Hiérarchisation du cloud NetApp</a> " ou " <a href="#">Sauvegarde et récupération</a> " services, vous devez activer le commutateur <b>Compte de service</b> , puis sélectionner le compte de service qui possède le rôle d'administrateur de stockage prédéfini.
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour vos ressources Google Cloud. La console ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources Google Cloud associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un système. Pour plus d'informations sur les étiquettes, reportez-vous à " <a href="#">Documentation Google Cloud : Étiquetage des ressources</a> ".

Champ	Description
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut <i>admin</i> ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	<p>Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet de la Console.</p> <p>Si vous ne voyez aucun projet supplémentaire dans la liste déroulante, cela signifie que vous n'avez pas encore associé le compte de service 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 que vous utilisez pour la console à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Il s'agit du compte de service que vous avez configuré pour la console, "<a href="#">comme décrit sur cette page</a>" . </div> <p>Cliquez sur <b>Ajouter un abonnement</b> pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP à la carte, vous devez sélectionner un projet Google Cloud associé à un abonnement à Cloud Volumes ONTAP sur Google Cloud Marketplace. Se référer à "<a href="#">Associer un abonnement Marketplace aux identifiants Google Cloud</a>" .</p>

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



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

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

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

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

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

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

Champ	Description
Politique générée	<p>Si vous laissez la console générer la politique de pare-feu pour vous, vous devez choisir comment vous autoriserez le trafic :</p> <ul style="list-style-type: none"> <li>• Si vous choisissez <b>VPC sélectionné uniquement</b>, le filtre source pour le trafic entrant est la plage de sous-réseaux du VPC sélectionné et la plage de sous-réseaux du VPC sur lequel réside l'agent de la console. C'est l'option recommandée.</li> <li>• Si vous choisissez <b>Tous les VPC</b>, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.</li> </ul>
Utiliser l'existant	<p>Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. <a href="#">"En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP"</a> .</p>

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

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

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

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

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



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

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

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

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

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

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

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



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

b. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

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



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

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

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

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

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

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

Notez ce qui suit :

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

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

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

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

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

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

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

### Volume Details & Protection

Volume Name <span style="float: right;">i</span> <input type="text" value="ABDcv5689"/>	Storage VM (SVM) <input type="text" value="svm_c...CVO1"/>
Volume Size <span style="float: right;">i</span> Unit <input type="text" value="100"/> <input type="text" value="GiB"/>	Snapshot Policy <input type="text" value="default"/>

default policy i

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

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

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

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

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

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

### Résultat

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

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

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

### Après avoir terminé

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

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

## Vérification d'image de Google Cloud Platform

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

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



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

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

L'image utilisée pour déployer de nouvelles instances, des mises à niveau ou utilisée

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

#### **Pourquoi cette étape est-elle nécessaire ?**

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

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

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

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

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

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

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

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

## Cliquez pour afficher

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

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

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

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

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

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

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

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

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

## Extraire les fichiers zippés

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



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

## Vérification de la signature de l'image

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

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

### Résumé du flux de travail de vérification des images signées

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

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

# Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

## Cloud Volumes ONTAP

### Non-Restricted Countries

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

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ [2.58 GB]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ.PEM [451 B]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ.SIG [256 B]**

[View and download checksums](#)

## Cloud Volumes ONTAP

### Restricted Countries

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

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ [2.58 GB]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ.PEM [451 B]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ.SIG [256 B]**

[View and download checksums](#)

## Cloud Volumes ONTAP

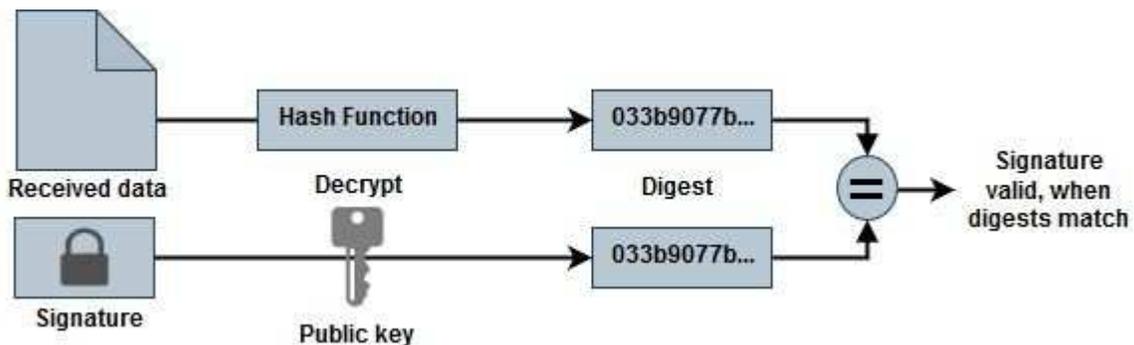
**DOWNLOAD GCP-9-15-0P1\_PKG.TAR.GZ [7.49 KB]**

[View and download checksums](#)

**DOWNLOAD AZURE-9-15-0P1\_PKG.TAR.GZ [7.64 KB]**

[View and download checksums](#)

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



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

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



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

## Étapes

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

## Cliquez pour afficher

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

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

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

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

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

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

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

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

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

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

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5

Cert Status: good

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

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

Signature Algorithm: sha512WithRSAEncryption

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

```

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

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

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

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

```

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

## Cliquez pour afficher

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

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

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

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

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

# Utiliser Cloud Volumes ONTAP

## Gestion des licences

### Gérer les licences basées sur la capacité pour Cloud Volumes ONTAP

Gérez vos licences basées sur la capacité depuis la console NetApp pour vous assurer que votre compte NetApp dispose d'une capacité suffisante pour vos systèmes Cloud Volumes ONTAP .

Les *licences basées sur la capacité* vous permettent de payer Cloud Volumes ONTAP par Tio de capacité.

Vous pouvez gérer les licences Cloud Volumes ONTAP basées sur la capacité à partir de la console NetApp .



Bien que l'utilisation et la mesure réelles des produits et services gérés dans la console soient toujours calculées en Gio et en Tio, les termes Go/Gio et To/Tio sont utilisés de manière interchangeable. Cela se reflète dans les listes de Cloud Marketplace, les devis, les descriptions des listes et dans d'autres documents justificatifs.

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

### Comment les licences sont ajoutées à la console NetApp

Après avoir acheté une licence auprès de votre représentant commercial NetApp , NetApp vous enverra un e-mail contenant le numéro de série et des détails de licence supplémentaires.

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

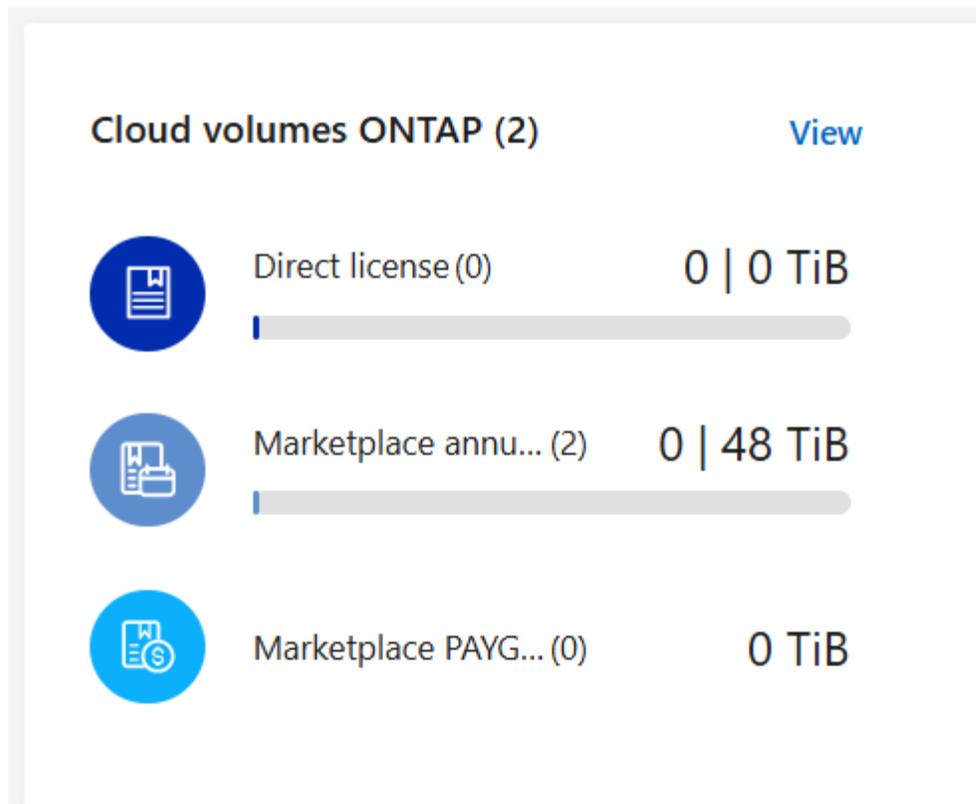
Si la console ne peut pas ajouter la licence, vous devrez l'ajouter manuellement. Par exemple, si l'agent de console est installé à un emplacement qui ne dispose pas d'accès Internet, vous devrez ajouter les licences vous-même. ["Découvrez comment ajouter des licences achetées à votre compte"](#) .

### Consultez la capacité consommée sur votre compte

La console vous indique la capacité totale consommée dans votre compte et la capacité consommée par package de licence. Cela peut vous aider à comprendre comment vous êtes facturé et si vous devez acheter une capacité supplémentaire.

#### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Dans l'onglet **Aperçu**, la mosaïque Cloud Volumes ONTAP affiche la capacité actuelle provisionnée pour votre compte.



- *Licence directe* correspond à la capacité totale provisionnée de tous les systèmes Cloud Volumes ONTAP de votre compte NetApp . La facturation est basée sur la taille provisionnée de chaque volume, quel que soit l'espace local, utilisé, stocké ou effectif au sein du volume.
- *Le contrat annuel* correspond à la capacité totale sous licence (apportez votre propre licence (BYOL) ou contrat Marketplace) que vous avez achetée auprès de NetApp.
- *PAYGO* est la capacité totale provisionnée à l'aide des abonnements au marché cloud. La facturation via PAYGO n'est utilisée que si la capacité consommée est supérieure à la capacité sous licence ou s'il n'y a pas de licence BYOL disponible dans la console.

3. Sélectionnez **Afficher** pour voir la capacité consommée pour chacun de vos packages de licence.
4. Sélectionnez l'onglet **Licences** pour voir les détails de chaque licence de package que vous avez achetée.

Pour mieux comprendre les capacités affichées pour le forfait Essentials, vous devez vous familiariser avec le fonctionnement de la charge. ["En savoir plus sur la facturation du forfait Essentials"](#) .

5. Sélectionnez l'onglet **Abonnements** pour voir la capacité consommée par modèle de consommation de licence. Cet onglet inclut les licences PAYGO et les licences de contrat annuel.

Vous ne verrez que les abonnements associés à l'organisation que vous consultez actuellement.

6. Lorsque vous consultez les informations sur vos abonnements, vous pouvez interagir avec les détails du tableau. Développez une ligne pour afficher plus de détails.
  - Sélectionner  pour choisir les colonnes qui apparaissent dans le tableau. Notez que les colonnes Durée et Renouvellement automatique n'apparaissent pas par défaut. La colonne Renouvellement automatique affiche les informations de renouvellement pour les contrats Azure uniquement.

## Affichage des détails du package

Vous pouvez afficher les détails sur la capacité utilisée par package en passant en mode hérité sur la page Cloud Volumes ONTAP .

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Dans l'onglet **Aperçu**, la mosaïque Cloud Volumes ONTAP affiche la capacité actuelle provisionnée pour votre compte.
3. Sélectionnez **Afficher** pour voir la capacité provisionnée pour chacun de vos packages de licence.
4. Sélectionnez **Passer à la vue avancée**.

The screenshot shows the 'Cloud Volumes ONTAP' overview page in 'Switch to advanced View' mode. At the top, there are three summary cards: 'Marketplace annual con... (2)' with 0 | 48 TiB, 'Marketplace PAYGO (0)' with 0 TiB, and 'Direct license (0)' with 0 | 0 TiB. Below these, there are tabs for 'Subscriptions (2)' and 'Licenses (0)'. The 'Subscriptions (2)' tab is active, showing a table of subscriptions.

Provider	Name	Type	Start date	End date	Status	
	DWdemoAnnualSmall123	Annual Contract	Jan 22, 2025	Jan 21, 2026	Subscribed	⋮
	cvo_team_bycap_bynode_annual	Annual Contract	Mar 12, 2025	Mar 11, 2026	Subscribed	⋮

5. Consultez les détails du package que vous souhaitez voir.

The screenshot shows the 'Cloud Volumes ONTAP' overview page in 'Switch to standard View' mode. At the top, there is a 'Cloud Volumes ONTAP Packages Summary' section with three cards: 'Total consumed capacity' (0 TiB), 'Total precommitted capacity' (48 TiB), and 'Total PAYGO' (0 TiB). Below this, there are two detailed package views: 'Essentials Secondary Single Node' and 'Professional'. Each view shows 'Consumed Capacity' (0 TiB), 'Precommitted capacity' (6 TiB), and 'PAYGO' (0 TiB). Underneath, it lists 'BYOL' (0 TiB) and 'Marketplace Contracts' (6 TiB).

## Changer les méthodes de charge

Les licences basées sur la capacité sont disponibles sous la forme d'un *package*. Lorsque vous créez un système Cloud Volumes ONTAP , vous pouvez choisir parmi plusieurs packages de licences en fonction des

besoins de votre entreprise. Si vos besoins changent après la création du système, vous pouvez modifier le package à tout moment. Par exemple, vous pouvez passer du forfait Essentials au forfait Professionnel.

["En savoir plus sur les packages de licences basés sur la capacité"](#) .

### À propos de cette tâche

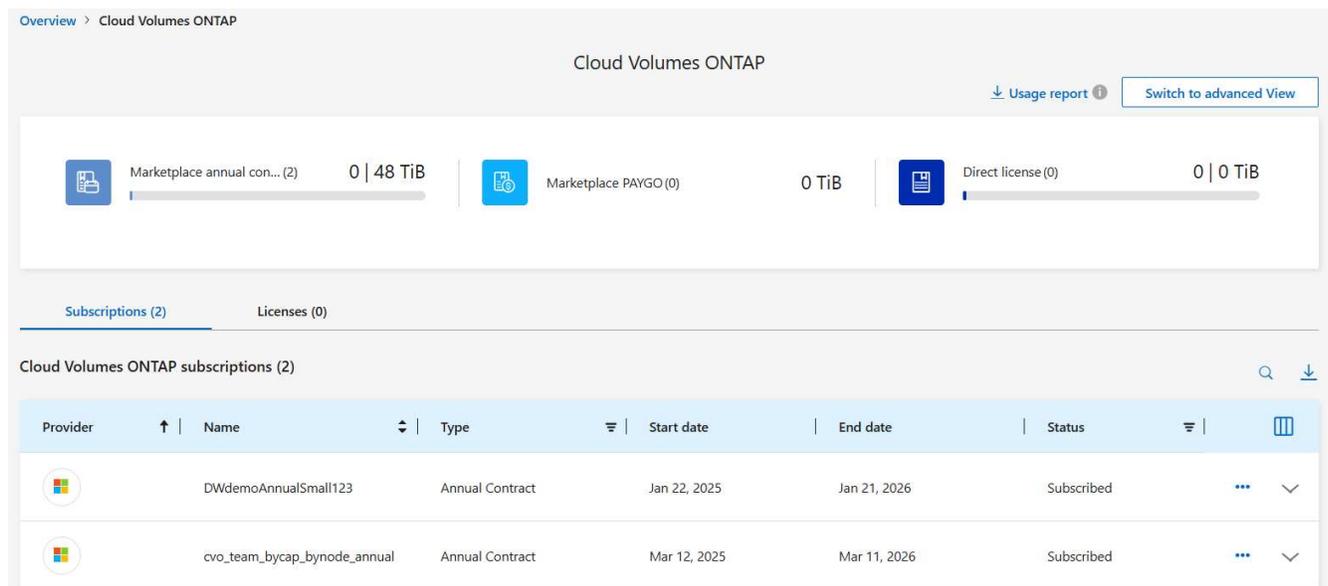
- La modification du mode de facturation n'a aucune incidence sur le fait que vous soyez facturé via une licence achetée auprès de NetApp (BYOL) ou via l'abonnement PAYGO (pay-as-you-go) de la place de marché de votre fournisseur de cloud.

La console tente toujours de facturer d'abord une licence. Si une licence n'est pas disponible, elle est facturée sur un abonnement au marché. Vous n'avez pas besoin de convertir un abonnement BYOL en abonnement marketplace ou vice versa.

- Si vous disposez d'une offre ou d'un contrat privé auprès de la place de marché de votre fournisseur de cloud, le passage à une méthode de facturation qui n'est pas incluse dans votre contrat entraînera une facturation sur BYOL (si vous avez acheté une licence auprès de NetApp) ou PAYGO.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
4. Sélectionnez **Passer à la vue avancée**.



Cloud Volumes ONTAP

Usage report ⓘ Switch to advanced View

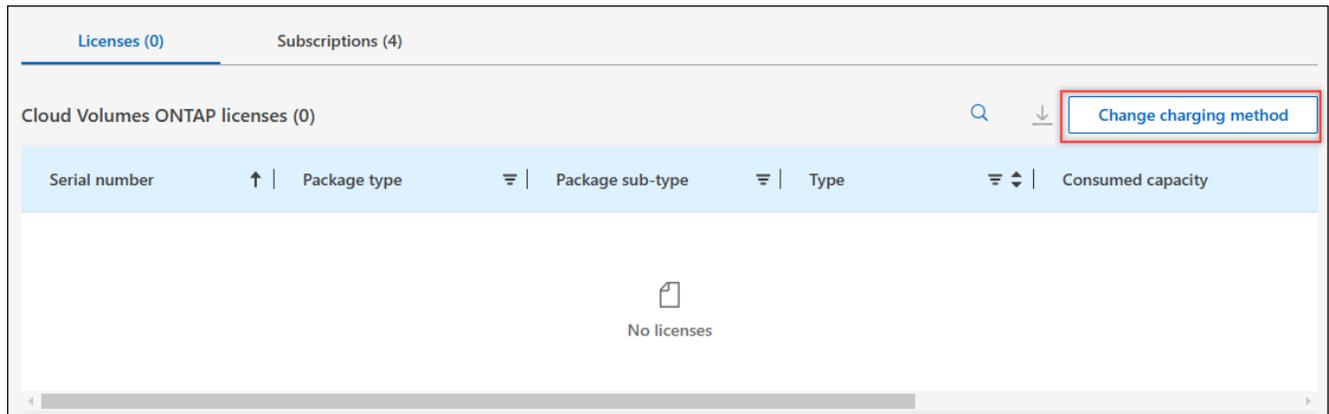
Marketplace annual con... (2) 0 | 48 TiB | Marketplace PAYGO (0) 0 TiB | Direct license (0) 0 | 0 TiB

Subscriptions (2) Licenses (0)

Cloud Volumes ONTAP subscriptions (2)

Provider	Name	Type	Start date	End date	Status	
	DWdemoAnnualSmall123	Annual Contract	Jan 22, 2025	Jan 21, 2026	Subscribed	⋮ ↓
	cvo_team_bycap_bynode_annual	Annual Contract	Mar 12, 2025	Mar 11, 2026	Subscribed	⋮ ↓

5. Faites défiler jusqu'au tableau **Licence basée sur la capacité** et sélectionnez **Modifier la méthode de facturation**.



6. Dans la fenêtre contextuelle **Modifier la méthode de facturation**, sélectionnez un système Cloud Volumes ONTAP , choisissez la nouvelle méthode de facturation, puis confirmez que vous comprenez que la modification du type de package affectera les frais de service.

7. Sélectionnez **Modifier la méthode de charge**.

### Télécharger les rapports d'utilisation

Vous pouvez télécharger quatre rapports d'utilisation depuis la console. Ces rapports d'utilisation fournissent des détails sur la capacité de vos abonnements et vous indiquent comment vous êtes facturé pour les ressources de vos abonnements Cloud Volumes ONTAP . Les rapports téléchargeables capturent les données à un moment donné et peuvent être facilement partagés avec d'autres.



Les rapports suivants sont disponibles en téléchargement. Les valeurs de capacité indiquées sont en Tio.

- **Utilisation de haut niveau** : Ce rapport comprend les informations suivantes :
  - Capacité totale consommée
  - Capacité totale préengagée
  - Capacité totale BYOL
  - Capacité totale des contrats du Marketplace
  - Capacité totale PAYGO
- **\* Utilisation du package Cloud Volumes ONTAP \*** : Ce rapport inclut les informations suivantes pour chaque package :
  - Capacité totale consommée
  - Capacité totale préengagée
  - Capacité totale BYOL
  - Capacité totale des contrats du Marketplace
  - Capacité totale PAYGO
- **Utilisation des machines virtuelles de stockage** : ce rapport montre comment la capacité facturée est

répartie entre les systèmes Cloud Volumes ONTAP et les machines virtuelles de stockage (SVM). Cette information n'est disponible que dans le rapport. Il contient les informations suivantes :

- ID et nom du système (apparaît comme l'UUID)
  - Nuage
  - ID de compte NetApp
  - Configuration du système
  - Nom du SVM
  - Capacité provisionnée
  - Aperçu de la capacité chargée
  - Conditions de facturation du marché
  - Package ou fonctionnalité Cloud Volumes ONTAP
  - Nom de l'abonnement à la place de marché SaaS de facturation
  - ID d'abonnement à la place de marché SaaS de facturation
  - Type de charge de travail
- **Utilisation des volumes** : ce rapport montre comment la capacité facturée est répartie par volumes dans un système Cloud Volumes ONTAP . Ces informations ne sont disponibles sur aucun écran de la console. Il comprend les informations suivantes :
- ID et nom du système (apparaît comme l'UUID)
  - Nom du SVN
  - ID du volume
  - Type de volume
  - Capacité provisionnée en volume



Les volumes FlexClone ne sont pas inclus dans ce rapport car ces types de volumes n'entraînent pas de frais.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Dans l'onglet **Aperçu**, sélectionnez **Afficher** dans la mosaïque Cloud Volumes ONTAP .
3. Sélectionnez **Rapport d'utilisation**.

Le rapport d'utilisation est téléchargé.

4. Ouvrez le fichier téléchargé pour accéder aux rapports.

## Gérer les abonnements Keystone pour Cloud Volumes ONTAP via la console NetApp

Gérez vos abonnements Keystone à partir du BlueXP digital wallet en activant les abonnements à utiliser avec Cloud Volumes ONTAP et en demandant des modifications de la capacité engagée pour les niveaux de service de votre abonnement. La demande de capacité supplémentaire pour un niveau de service fournit davantage de stockage pour les clusters ONTAP sur site ou pour les systèmes Cloud Volumes ONTAP .

NetApp Keystone est un service d'abonnement flexible et évolutif qui offre une expérience de cloud hybride aux clients qui préfèrent les dépenses d'exploitation aux dépenses d'investissement ou à la location.

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

## Autorisez votre compte

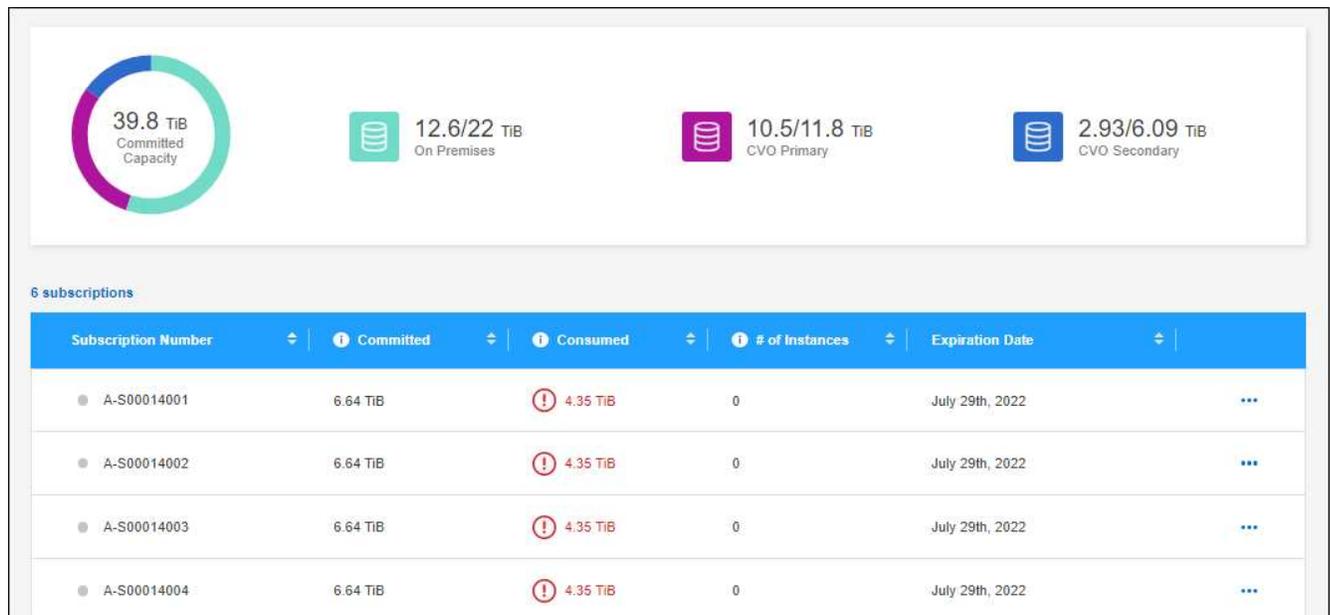
Avant de pouvoir utiliser et gérer les abonnements Keystone dans BlueXP, vous devez contacter NetApp pour autoriser votre compte utilisateur BlueXP avec vos abonnements Keystone .

### Étapes

1. Dans le menu de navigation BlueXP , sélectionnez **Gouvernance > Portefeuille numérique**.
2. Sélectionnez \* Abonnements Keystone \*.
3. Si vous voyez la page **Bienvenue sur 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'onglet \* Abonnements Keystone \* pour afficher vos abonnements.



## Lier un abonnement

Une fois que NetApp a autorisé votre compte, vous pouvez lier les abonnements Keystone 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 BlueXP , sélectionnez **Gouvernance > Portefeuille numérique**.
2. Sélectionnez \* Abonnements Keystone \*.
3. Pour l'abonnement que vous souhaitez lier, cliquez sur **...** et sélectionnez **Lien**.

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 organisation ou compte BlueXP et peut être sélectionné lors de la création d'un environnement de travail Cloud Volumes ONTAP .

## Demander une capacité plus ou moins engagée

Si vous souhaitez modifier la capacité engagée pour les niveaux de service de votre abonnement, vous pouvez envoyer une demande à NetApp directement depuis BlueXP. La demande de capacité supplémentaire pour un niveau de service fournit davantage de stockage pour les clusters sur site ou pour les systèmes Cloud Volumes ONTAP .

## Étapes

1. Dans le menu de navigation BlueXP , sélectionnez **Gouvernance > Portefeuille numérique**.
2. Sélectionnez \* Abonnements Keystone \*.
3. Pour l'abonnement dont vous souhaitez ajuster la capacité, cliquez sur ⋮ et sélectionnez **Afficher les détails et modifier**.
4. Saisissez la capacité engagée demandée 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.

Enter your notes here

5. Faites défiler vers le bas, saisissez tous les détails supplémentaires pour la demande, puis cliquez sur **Soumettre**.

### Résultat

Votre demande crée un ticket dans le système NetApp pour traitement.

### Surveiller l'utilisation

Le tableau de bord du BlueXP digital advisor vous permet de surveiller l'utilisation de l'abonnement Keystone et de générer des rapports.

["En savoir plus sur la surveillance de l'utilisation des abonnements"](#)

### Dissocier un abonnement

Si vous ne souhaitez plus utiliser un abonnement Keystone avec BlueXP, vous pouvez dissocier 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 BlueXP, sélectionnez **Gouvernance > Portefeuille numérique**.
2. Sélectionnez \* Keystone\*.
3. Pour l'abonnement que vous souhaitez dissocier, cliquez sur **...** et sélectionnez **Dissocier**.

## Résultat

L'abonnement est dissocié de votre organisation ou de votre compte BlueXP et n'est plus disponible à la sélection lors de la création d'un environnement de travail Cloud Volumes ONTAP .

## Gérer les licences basées sur les nœuds pour Cloud Volumes ONTAP

Gérez les licences basées sur les nœuds dans la console NetApp pour garantir que chaque système Cloud Volumes ONTAP dispose d'une licence valide avec la capacité requise.

Les *licences basées sur les nœuds* sont le modèle de licence de la génération précédente (et ne sont pas disponibles pour les nouveaux clients) :

- Licences BYOL (Apportez votre propre licence) achetées auprès de NetApp
- Abonnements horaires à la carte (PAYGO) depuis la place de marché de votre fournisseur cloud

Vous pouvez gérer les licences Cloud Volumes ONTAP basées sur des nœuds à partir de la console NetApp .

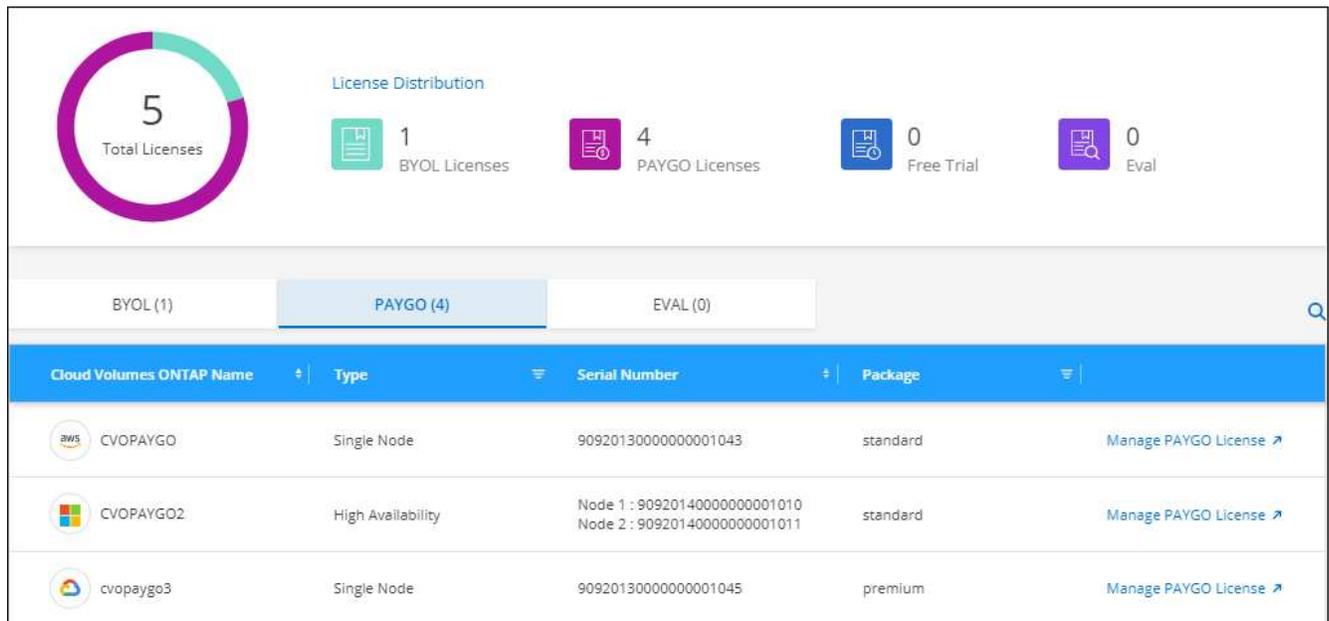
["En savoir plus sur les licences Cloud Volumes ONTAP"](#) .

## Gérer les licences PAYGO

Le menu Licences et abonnements vous permet d'afficher les détails de chacun de vos systèmes PAYGO Cloud Volumes ONTAP , y compris le numéro de série et le type de licence PAYGO.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
4. Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
5. Cliquez sur **PAYGO**.
6. Consultez les détails dans le tableau concernant chacune de vos licences PAYGO.



- Si nécessaire, cliquez sur **Gérer la licence PAYGO** pour modifier la licence PAYGO ou pour modifier le type d'instance.

## Gérer 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.



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

### Ajouter des licences non attribuées

Ajoutez une licence basée sur un nœud à la console afin de pouvoir sélectionner la licence lorsque vous créez un nouveau système Cloud Volumes ONTAP . La console identifie ces licences comme *non attribuées*.

### Étapes

- Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
- Sélectionnez l'onglet **Aperçu**.
- Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
- Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
- Cliquez sur **Non attribué**.
- Cliquez sur **Ajouter des licences non attribuées**.
- 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.

- Cliquez sur **Ajouter une licence**.

### Résultat

La console ajoute la licence. La licence sera identifiée comme non attribuée jusqu'à ce que vous l'associiez

à un nouveau système Cloud Volumes ONTAP . Une fois cela fait, la licence est déplacée vers l'onglet **BYOL** dans **Licences et abonnements**.

### Échanger des licences basées sur des nœuds non attribués

Si vous disposez d'une licence basée sur un nœud non attribué pour Cloud Volumes ONTAP que vous n'avez pas utilisée, vous pouvez échanger la licence en la convertissant en une licence NetApp Backup and Recovery, une licence NetApp Data Classification ou une licence NetApp Cloud Tiering.

L'échange de licence révoque la licence Cloud Volumes ONTAP et crée une licence équivalente en dollars pour le service :

- La licence pour une paire Cloud Volumes ONTAP HA est convertie en une licence directe de 51 Tio
- La licence pour un nœud unique Cloud Volumes ONTAP est convertie en une licence directe de 32 Tio

La licence convertie a la même date d'expiration que la licence Cloud Volumes ONTAP .

"Consultez la procédure pas à pas expliquant comment échanger des licences basées sur des nœuds."

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
4. Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
5. Cliquez sur **Non attribué**.
6. Cliquez sur **Échanger la licence**.

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	

7. Sélectionnez le service avec lequel vous souhaitez échanger la licence.
8. Si vous y êtes invité, sélectionnez une licence supplémentaire pour la paire HA.
9. Lisez le consentement légal et cliquez sur **Accepter**.

### Résultat

La console convertit la licence non attribuée au service que vous avez sélectionné. Vous pouvez consulter la nouvelle licence dans l'onglet **Licences des services de données**.

### Obtenir un fichier de licence système

Dans la plupart des cas, la console peut obtenir automatiquement votre fichier de licence à l'aide de votre compte de site de support NetApp . Mais si ce n'est pas le cas, vous devrez télécharger manuellement le

fichier de licence. Si vous ne disposez pas du fichier de licence, vous pouvez l'obtenir sur netapp.com.

## Étapes

1. Aller à la "[Générateur de fichiers de licence NetApp](#)" et connectez-vous à l'aide de vos informations d'identification du site de support NetApp .
2. Saisissez votre mot de passe, choisissez votre produit, saisissez le numéro de série, confirmez que vous avez lu et accepté la politique de confidentialité, puis cliquez sur **Soumettre**.

## Exemple

**License Generator**

The following fields are pre-populated based on the NetApp SSO login provided.  
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name: Ben

Last Name: [Redacted]

Company: Network Appliance, Inc

Email Address: [Redacted]

Username: [Redacted]

Product Line\* [Dropdown menu open]

- ONTAP Select - Standard
- ONTAP Select - Premium
- ONTAP Select - Premium XL
- Cloud Volumes ONTAP for AWS (single node)
- Cloud Volumes ONTAP for AWS (HA)
- Cloud Volumes ONTAP for GCP (single node or HA)
- Cloud Volumes ONTAP for Microsoft Azure (single node)
- Cloud Volumes ONTAP for Microsoft Azure (HA)
- Service Level Manager - SLO Advanced
- StorageGRID Webscale
- StorageGRID WhiteBox
- SnapCenter Standard (capacity-based)

Not only is protecting your data required by law, but it's also the right thing to do. [Learn more](#)

I have read NetApp's new **Global Data Privacy Policy** and I agree to the terms. [Learn more](#)

3. Choisissez si vous souhaitez recevoir le fichier JSON serialnumber.NLF par e-mail ou par téléchargement direct.

## Mettre à jour une licence système

Lorsque vous renouvelez un abonnement BYOL en contactant un représentant NetApp , la console obtient automatiquement la nouvelle licence auprès de NetApp et l'installe sur le système Cloud Volumes ONTAP . Si la console ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis télécharger le fichier manuellement.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
4. Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
5. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP .

6. Cliquez sur le menu d'action à côté de la licence système et sélectionnez **Mettre à jour la licence**.
7. Téléchargez le fichier de licence (ou les fichiers si vous avez une paire HA).
8. Cliquez sur **Mettre à jour la licence**.

## Résultat

La console met à jour la licence sur le système Cloud Volumes ONTAP .

## Gérer les licences de capacité supplémentaire

Vous pouvez acheter des licences de capacité supplémentaires pour un système Cloud Volumes ONTAP BYOL afin d'allouer plus que les 368 Tio de capacité fournis avec une licence système BYOL. Par exemple, vous pouvez acheter une capacité de licence supplémentaire pour allouer jusqu'à 736 Tio de capacité à Cloud Volumes ONTAP. Ou vous pouvez acheter trois licences de capacité supplémentaires pour obtenir jusqu'à 1,4 PiB.

Le nombre de licences disponibles pour un système à nœud unique ou une paire HA est illimité.

## Ajouter des licences de capacité

Achetez une licence de capacité supplémentaire en nous contactant via l'icône de chat en bas à droite de la console. Après avoir acheté la licence, vous pouvez l'appliquer à un système Cloud Volumes ONTAP .

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
4. Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
5. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP .
6. Cliquez sur **Ajouter une licence de capacité**.
7. Saisissez le numéro de série ou téléchargez le fichier de licence (ou les fichiers si vous avez une paire HA).
8. Cliquez sur **Ajouter une licence de capacité**.

## Mettre à jour les licences de capacité

Si vous avez prolongé la durée d'une licence de capacité supplémentaire, vous devrez mettre à jour la licence dans la console.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP , sélectionnez **Afficher**.
4. Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
5. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP .
6. Cliquez sur le menu d'action à côté de la licence de capacité et sélectionnez **Mettre à jour la licence**.
7. Téléchargez le fichier de licence (ou les fichiers si vous avez une paire HA).

8. Cliquez sur **Mettre à jour la licence**.

### Supprimer 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 volet de navigation de gauche, sélectionnez **Administration > Licences et abonnements**.
2. Sélectionnez l'onglet **Aperçu**.
3. Sur la mosaïque Cloud Volumes ONTAP, sélectionnez **Afficher**.
4. Sélectionnez **Licences basées sur les nœuds** dans la liste déroulante.
5. Dans l'onglet **BYOL**, développez les détails d'un système Cloud Volumes ONTAP.
6. Cliquez sur le menu d'action à côté de la licence de capacité et sélectionnez **Supprimer la licence**.
7. Cliquez sur **Supprimer**.

### Passer du PAYGO au BYOL

La conversion d'un système de licences PAYGO par nœud en licences BYOL par nœud (et vice versa) n'est pas prise en charge. Si vous souhaitez passer d'un abonnement à la carte à un abonnement BYOL, vous devez déployer un nouveau système et répliquer les données du système existant vers le nouveau système.

#### Étapes

1. Créez un nouveau système Cloud Volumes ONTAP.
2. Configurez une réplique de données unique entre les systèmes pour chaque volume que vous devez répliquer.

["Apprenez à répliquer des données entre des systèmes"](#)

3. Mettez fin au système Cloud Volumes ONTAP dont vous n'avez plus besoin en supprimant le système d'origine.

["Découvrez comment supprimer un système Cloud Volumes ONTAP"](#).

#### Liens connexes

lien: ["Fin de disponibilité des licences basées sur des nœuds"](#) ["Convertir les licences basées sur les nœuds en licences basées sur la capacité"](#)

## Administration des volumes et des LUN

### Créer un FlexVol volume sur un système Cloud Volumes ONTAP

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 la console NetApp.

Vous disposez de plusieurs manières pour créer un nouveau volume :

- Spécifiez les détails d'un nouveau volume et laissez la console gérer les agrégats de données sous-jacents pour vous.[Apprendre encore plus](#)
- Créez un volume sur un agrégat de données de votre choix.[Apprendre encore plus](#)
- Créez un volume sur le deuxième nœud dans une configuration HA.[Apprendre encore plus](#)

## Avant de commencer

Quelques notes sur le provisionnement des volumes :

- Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, ["utilisez l'IQN pour vous connecter au LUN depuis vos hôtes"](#) .
- Vous pouvez créer des LUN supplémentaires à partir d' ONTAP System Manager ou de l' ONTAP CLI.
- Si vous souhaitez utiliser CIFS dans AWS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, reportez-vous à ["Exigences réseau pour Cloud Volumes ONTAP pour AWS"](#) .
- Si votre configuration Cloud Volumes ONTAP prend en charge la fonctionnalité Amazon EBS Elastic Volumes, vous souhaitez peut-être ["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 consiste à spécifier le type de volume dont vous avez besoin, puis à laisser la console gérer l'allocation de disque pour vous. Mais vous avez également la possibilité de choisir l'agrégat spécifique sur lequel vous souhaitez créer le volume.

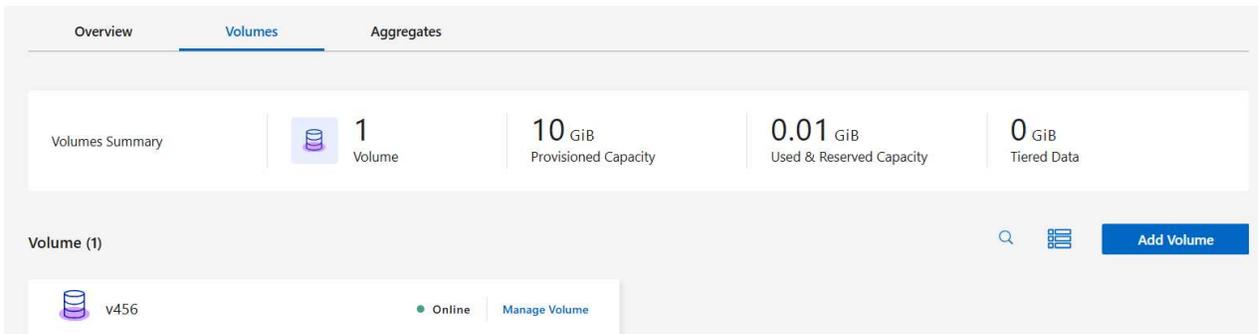
### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez provisionner un FlexVol volume.

Vous pouvez créer un volume en laissant la console gérer l'allocation de disque pour vous ou choisir un agrégat spécifique pour le volume. Le choix d'un agrégat spécifique n'est recommandé que si vous avez une bonne compréhension des agrégats de données sur votre système Cloud Volumes ONTAP .

## Tout agrégat

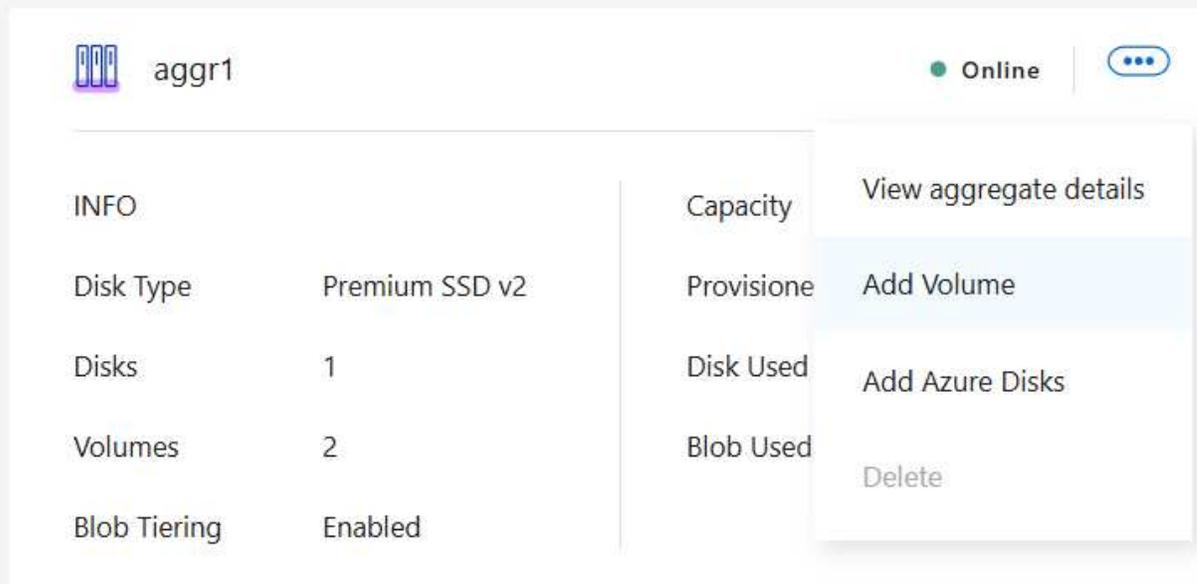
Sélectionnez l'onglet Volumes et cliquez sur **Ajouter un volume**



## Agrégat spécifique

- Dans l'onglet **Agrégats**, accédez à l'agrégat requis et cliquez sur le bouton **...** icône.
- Sélectionnez **Ajouter un volume**

## Aggregate (1)



3. Suivez les étapes de l'assistant pour créer le volume.

- Détails, protection et balises** : saisissez les détails de base sur le volume et sélectionnez une politique de capture instantanée.

Certains champs de cette page sont explicites. La liste suivante décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Nom du volume	Le nom identifiable que vous pouvez saisir pour le nouveau volume.

Champ	Description
Taille du volume	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation ou non du provisionnement dynamique, qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Machine virtuelle de stockage (SVM)	Une machine virtuelle de stockage est une machine virtuelle exécutée dans ONTAP qui fournit des services de stockage et de données à vos clients. Vous connaissez peut-être cela sous le nom de SVM ou de vserver. Cloud Volumes ONTAP est configuré avec une machine virtuelle de stockage par défaut, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires. Vous pouvez spécifier la machine virtuelle de stockage pour le nouveau volume.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.

- b. **Protocole** : Choisissez un protocole pour le volume (NFS, CIFS ou iSCSI), puis fournissez les informations requises.

Si vous sélectionnez CIFS et qu'aucun serveur n'est configuré, la console vous invite à configurer la connectivité CIFS après avoir cliqué sur **Suivant**.

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

Les sections suivantes décrivent les domaines pour lesquels vous pourriez avoir besoin de conseils. Les descriptions sont organisées par protocole.

## NFS

### Contrôle d'accès

Choisissez une politique d'exportation personnalisée pour rendre le volume disponible pour les clients.

### Politique d'exportation

Définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, la console entre une valeur qui donne accès à toutes les instances du sous-réseau.

## CIFS

### Autorisations et utilisateurs/groupes

Vous 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 en utilisant le format domaine\nom d'utilisateur.

### Adresse IP primaire et secondaire DNS

Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.

Si vous configurez Google Managed Active Directory, AD est accessible par défaut avec l'adresse IP 169.254.169.254.

### Domaine Active Directory à rejoindre

Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.

### Informations d'identification autorisées pour rejoindre le domaine

Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.

### Nom NetBIOS du serveur CIFS

Un nom de serveur CIFS unique dans le domaine AD.

### Unité organisationnelle

L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs.

- Pour configurer AWS Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, saisissez **OU=Computers,OU=corp** dans ce champ.
- Pour configurer Azure AD Domain Services comme serveur AD pour Cloud Volumes ONTAP, saisissez **OU=AADDC Computers** ou **OU=AADDC Users** dans ce champ. <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou>["Documentation Azure : Créer une unité d'organisation (UO) dans un domaine géré par Azure AD Domain Services"]
- Pour configurer Google Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, saisissez **OU=Computers,OU=Cloud** dans ce champ. <https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory->

objects#organizational\_units["Documentation Google Cloud : Unités organisationnelles dans Google Managed Microsoft AD"]

### Domaine DNS

Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est le même que le domaine AD.

### Serveur NTP

Sélectionnez **Utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Pour plus d'informations, reportez-vous à la "[Documentation sur l'automatisation de la console NetApp](#)".

Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

### 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, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, "[utilisez l'IQN pour vous connecter au LUN depuis vos hôtes](#)".

#### Groupe initiateur

Les groupes d'initiateurs (igroups) spécifient quels hôtes peuvent accéder aux LUN spécifiés sur le système de stockage

#### Initiateur hôte (IQN)

Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiées 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 performances et de vos exigences de coût.

- "[Dimensionnement de votre système dans AWS](#)"
  - "[Dimensionnement de votre système dans Azure](#)"
  - "[Dimensionnement de votre système dans Google Cloud](#)"

4. **Profil d'utilisation et politique de hiérarchisation** : Choisissez d'activer ou de désactiver les fonctionnalités d'efficacité du stockage sur le volume, puis sélectionnez un "[politique de hiérarchisation des volumes](#)".

ONTAP inclut plusieurs fonctionnalités d'efficacité de stockage qui peuvent réduire la quantité totale de stockage dont vous avez besoin. Les fonctionnalités d'efficacité du stockage NetApp offrent les avantages suivants :

#### Provisionnement léger

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

## Déduplication

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

## Compression

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

5. **Révision** : Vérifiez les détails du volume, puis cliquez sur **Ajouter**.

## Résultat

La console crée le volume sur le système Cloud Volumes ONTAP .

## Créer un volume sur le deuxième nœud dans une configuration HA

Par défaut, la console 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 fournissent des données aux clients, vous devez créer des agrégats et des volumes sur le deuxième nœud.

## Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
3. Dans l'onglet Agrégats, cliquez sur **Ajouter un agrégat** et créez l'agrégat.

The screenshot shows the 'Aggregates Summary' page in the AWS Management Console. At the top, there are four summary cards: 'Total Aggregates' (1), 'Aggregates with Tiering' (1), 'Aggregates without Tiering' (0), and 'Allocated Disks' (1). Below this, the 'Aggregate (1)' section is visible, showing a search icon, a list icon, and an 'Add Aggregate' button. The main content area displays details for an aggregate named 'aggr1', which is 'Online'. The details are organized into two columns: 'INFO' and 'Capacity'.

INFO		Capacity	
Disk Type	Premium SSD v2	Provisioned size	907.18 GiB
Disks	1	Disk Used	1.15 GiB
Volumes	2	Blob Used	0 GiB
Blob Tiering	Enabled		

4. Pour le nœud domestique, choisissez le deuxième nœud de la paire HA.
5. Une fois que la console a créé l'agrégat, sélectionnez-le, puis cliquez sur **Créer un volume**.
6. Saisissez les détails du nouveau volume, puis cliquez sur **Créer**.

## Résultat

La console crée le volume sur le deuxième nœud de la paire HA.



Pour les paires HA déployées dans plusieurs zones de disponibilité AWS, vous devez monter le volume sur les clients à l'aide de l'adresse IP flottante du nœud sur lequel réside le volume.

## Après avoir créé un volume

Si vous avez provisionné un partage CIFS, accordez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.

Si vous souhaitez appliquer des quotas aux volumes, vous devez utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP . Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

## Gérer les volumes sur les systèmes Cloud Volumes ONTAP

Vous pouvez gérer les volumes et les serveurs CIFS dans la console NetApp . Vous pouvez également déplacer des volumes pour éviter les problèmes de capacité.

Vous pouvez gérer les volumes dans la vue standard de la console NetApp ou via ONTAP System Manager inclus dans la console pour une gestion avancée des volumes. La vue standard fournit un ensemble limité d'options pour modifier vos volumes. System Manager offre un niveau de gestion avancé, tel que le clonage, le redimensionnement, la modification des paramètres anti-ransomware, l'analyse, la protection et le suivi des activités, ainsi que le déplacement de volumes entre les niveaux. Pour plus d'informations, reportez-vous à "[Administrer Cloud Volumes ONTAP à l'aide de System Manager](#)".

### Gérer les volumes

En utilisant la vue standard de la console, vous pouvez gérer les volumes en fonction de vos besoins de stockage. Vous pouvez afficher, modifier, cloner, restaurer et supprimer des volumes.

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le système Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
3. Sélectionnez l'onglet **Volumes**.

INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection			

4. Sur la mosaïque de volume requise, cliquez sur **Gérer le volume**.

Tâche	Action
Afficher les informations sur un volume	Sous Actions de volume dans le panneau Gérer les volumes, cliquez sur <b>Afficher les détails du volume</b> .
Obtenir la commande de montage NFS	<p>a. Sous Actions de volume dans le panneau Gérer les volumes, cliquez sur <b>Commande de montage</b>.</p> <p>b. Cliquez sur <b>Copier</b>.</p>
Cloner un volume	<p>a. Sous Actions de volume dans le panneau Gérer les volumes, cliquez sur <b>Cloner le volume</b>.</p> <p>b. Modifiez le nom du clone selon vos besoins, puis cliquez sur <b>Cloner</b>.</p> <p>Ce processus crée un volume FlexClone . Un volume FlexClone est une copie inscriptible, ponctuelle et efficace en termes d'espace, car elle utilise une petite quantité d'espace pour les métadonnées et ne consomme ensuite de l'espace supplémentaire qu'à mesure que les données sont modifiées ou ajoutées.</p> <p>Pour en savoir plus sur les volumes FlexClone , reportez-vous à la "<a href="#">Guide de gestion du stockage logique ONTAP 9</a>" .</p>
Modifier un volume (volumes en lecture-écriture uniquement)	<p>a. Sous Actions de volume dans le panneau Gérer les volumes, cliquez sur <b>Modifier les paramètres de volume</b></p> <p>b. Modifiez la stratégie de capture instantanée du volume, la version du protocole NFS, la liste de contrôle d'accès NFS (stratégie d'exportation) ou les autorisations de partage, puis cliquez sur <b>Appliquer</b>.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Si vous avez besoin de stratégies d'instantané personnalisées, vous pouvez les créer à l'aide d' ONTAP System Manager.</p> </div>
Supprimer un volume	<p>a. Sous Actions de volume dans le panneau Gérer les volumes, cliquez sur <b>Supprimer le volume</b>.</p> <p>b. Sous la fenêtre Supprimer le volume, entrez le nom du volume que vous souhaitez supprimer.</p> <p>c. Cliquez à nouveau sur <b>Supprimer</b> pour confirmer.</p>
Créer une copie instantanée à la demande	<p>a. Sous Actions de protection dans le panneau Gérer les volumes, cliquez sur <b>Créer une copie instantanée</b>.</p> <p>b. Modifiez le nom, si nécessaire, puis cliquez sur <b>Créer</b>.</p>

Tâche	Action
Restaurer les données d'une copie instantanée vers un nouveau volume	<p>a. Sous Actions de protection dans le panneau Gérer les volumes, cliquez sur <b>Restaurer à partir d'une copie instantanée</b>.</p> <p>b. Sélectionnez une copie instantanée, entrez un nom pour le nouveau volume, puis cliquez sur <b>Restaurer</b>.</p>
Modifier le type de disque sous-jacent	<p>a. Sous Actions avancées dans le panneau Gérer les volumes, cliquez sur <b>Modifier le type de disque</b>.</p> <p>b. Sélectionnez le type de disque, puis cliquez sur <b>Modifier</b>.</p> <p> La console déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné ou crée un nouvel agrégat pour le volume.</p>
Modifier la politique de hiérarchisation	<p>a. Sous Actions avancées dans le panneau Gérer les volumes, cliquez sur <b>Modifier la politique de hiérarchisation</b>.</p> <p>b. Sélectionnez une politique différente et cliquez sur <b>Modifier</b>.</p> <p> La console déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné avec hiérarchisation, ou elle crée un nouvel agrégat pour le volume.</p>
Supprimer un volume	<p>a. Sélectionnez un volume, puis cliquez sur <b>Supprimer</b>.</p> <p>b. Tapez le nom du volume dans la boîte de dialogue.</p> <p>c. Cliquez à nouveau sur <b>Supprimer</b> pour confirmer.</p>

## Redimensionner un volume

Par défaut, un volume atteint automatiquement une taille maximale lorsqu'il n'y a plus d'espace. La valeur par défaut est 1 000, ce qui signifie que le volume peut atteindre 11 fois sa taille. Cette valeur est configurable dans les paramètres de l'agent de la console.

Si vous devez redimensionner votre volume, vous pouvez le faire à partir d' ONTAP System Manager dans la console.

### Étapes

1. Cliquez sur la vue Gestionnaire système pour redimensionner un volume via ONTAP System Manager. ["Comment commencer"](#) .
2. Dans le menu de navigation de gauche, sélectionnez **Stockage > Volumes**.
3. Dans la liste des volumes, identifiez celui que vous devez redimensionner.
4. Cliquez sur l'icône des options  .
5. Sélectionnez **Redimensionner**.
6. Sur l'écran **Redimensionner le volume**, modifiez la capacité et le pourcentage de réserve d'instantanés selon vos besoins. Vous pouvez comparer l'espace existant et disponible avec la capacité modifiée.

7. Cliquez sur **Enregistrer**.

**Resize volume** [X]

CAPACITY

25 [↑][↓] GiB [v]

SNAPSHOT RESERVE %

1 [↑][↓]

<b>Existing</b>	<b>New</b>
DATA SPACE	DATA SPACE
20 GiB	24.75 GiB
SNAPSHOT RESERVE	SNAPSHOT RESERVE
0 Bytes	256 MiB

Cancel Save

Assurez-vous de prendre en compte les limites de capacité de votre système lorsque vous redimensionnez les volumes. Aller à la "[Notes de version de Cloud Volumes ONTAP](#)" pour plus d'informations.

### 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 afin qu'il puisse continuer à fournir du stockage aux clients.

#### Étapes

1. Dans l'onglet **Vue d'ensemble** du système Cloud Volumes ONTAP , cliquez sur l'onglet **Fonctionnalité** sous le panneau de droite.
2. Sous le champ Configuration CIFS, cliquez sur l'icône **crayon** pour afficher la fenêtre Configuration CIFS.
3. Spécifiez les paramètres du serveur CIFS :

Tâche	Action
Sélectionner une machine virtuelle de stockage (SVM)	La sélection de la machine virtuelle de stockage Cloud Volume ONTAP (SVM) affiche ses informations CIFS configurées.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.

Tâche	Action
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine que le serveur CIFS rejoindra. ifdef::gcp[] Si vous configurez Google Managed Active Directory, AD est accessible par défaut avec l'adresse IP 169.254.169.254. endif::gcp[]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est le même que le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	<p>L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs.</p> <ul style="list-style-type: none"> <li>• Pour configurer AWS Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, saisissez <b>OU=Computers,OU=corp</b> dans ce champ.</li> <li>• Pour configurer Azure AD Domain Services comme serveur AD pour Cloud Volumes ONTAP, saisissez <b>OU=AADDC Computers</b> ou <b>OU=AADDC Users</b> dans ce champ. "<a href="#">Documentation Azure : Créer une unité d'organisation (UO) dans un domaine géré par Azure AD Domain Services</a>"</li> <li>• Pour configurer Google Managed Microsoft AD comme serveur AD pour Cloud Volumes ONTAP, saisissez <b>OU=Computers,OU=Cloud</b> dans ce champ. "<a href="#">Documentation Google Cloud : Unités organisationnelles dans Google Managed Microsoft AD</a>"</li> </ul>

4. Cliquez sur **Définir**.

### Résultat

Cloud Volumes ONTAP met à jour le serveur CIFS avec les modifications.

### Déplacer un volume

Déplacez des volumes pour optimiser l'utilisation des capacités, améliorer les performances et satisfaire aux accords de niveau de service.

Vous pouvez déplacer un volume dans ONTAP System Manager en sélectionnant un volume et l'agrégat de destination, en démarrant l'opération de déplacement du volume et en surveillant éventuellement le travail de déplacement du volume. Lorsque vous utilisez le Gestionnaire système, une opération de déplacement de volume se termine automatiquement.

### Étapes

1. Utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP pour déplacer les volumes

vers l'agrégat.

Dans la plupart des situations, vous pouvez utiliser le Gestionnaire système pour déplacer des volumes.

Pour les instructions, reportez-vous à la ["Guide de déplacement express de volumes ONTAP 9"](#) .

## Déplacer un volume lorsque la console affiche un message d'action requise

La console 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 le problème vous-même. Si cela se produit, vous devez identifier comment corriger le problème, puis déplacer un ou plusieurs volumes.



La console affiche ces messages d'action requise lorsqu'un agrégat a atteint 90 % de sa capacité utilisée. Si la hiérarchisation des données est activée, les messages s'affichent lorsqu'un agrégat a atteint 80 % de sa capacité utilisée. Par défaut, 10 % d'espace libre sont réservés à la hiérarchisation des données. ["En savoir plus sur le ratio d'espace libre pour la hiérarchisation des données"](#) .

### Étapes

1. [Identifier comment corriger les problèmes de capacité](#) .
2. En fonction de votre analyse, déplacez les volumes pour éviter les problèmes de capacité :
  - [Déplacez les volumes vers un autre système pour éviter les problèmes de capacité](#) .
  - [Déplacer les volumes vers un autre agrégat pour éviter les problèmes de capacité](#) .

### Identifier comment corriger les problèmes de capacité

Si la console ne peut pas fournir de recommandations pour déplacer un volume afin d'éviter des problèmes de capacité, vous devez identifier les volumes que vous devez déplacer et si vous devez les déplacer vers un autre agrégat sur le même système ou vers un autre système.

### Étapes

1. Consultez les informations avancées dans le message Action requise pour identifier l'agrégat qui a atteint sa limite de capacité.

Par exemple, les informations avancées devraient indiquer quelque chose de similaire à ce qui suit :  
L'agrégat aggr1 a atteint sa limite de capacité.

2. Identifiez un ou plusieurs volumes à retirer de l'agrégat :
  - a. Dans le système Cloud Volumes ONTAP , cliquez sur l'onglet **Agrégats**.
  - b. Sur la tuile agrégée, cliquez sur le **...** icône puis cliquez sur **Afficher les détails agrégés**.
  - c. Sous l'onglet **Aperçu** de l'écran **Détails agrégés**, vérifiez la taille de chaque volume et choisissez un ou plusieurs volumes à déplacer hors de l'agrégat.

Vous devez choisir des volumes suffisamment grands pour libérer de l'espace dans l'ensemble afin d'éviter des problèmes de capacité supplémentaires à l'avenir.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	iblog1-01
Encryption Type	cloudEncrypted
Volumes	2 ^ vvv_iblog1_001 (1 GiB) vvv_iblog1_002 (500 GiB)

3. Si le système n'a pas atteint la limite de disque, vous devez déplacer les volumes vers un agrégat existant ou un nouvel agrégat sur le même système.

Pour plus d'informations, reportez-vous à [Déplacer les volumes vers un autre agrégat pour éviter les problèmes de capacité](#).

4. Si le système a atteint la limite du 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 d'informations, reportez-vous à [Déplacer les 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 d'informations, reportez-vous à [Déplacer les volumes vers un autre agrégat pour éviter les problèmes de capacité](#).

#### Déplacez les 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.

#### À propos de cette tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

Le déplacement d'un volume est nécessaire pour éviter les problèmes de capacité ; cependant, la console ne peut pas effectuer cette action pour vous car le système a atteint la limite du disque.

## Étapes

1. Identifiez un système Cloud Volumes ONTAP disposant d'une capacité disponible ou déployez un nouveau système.
2. Faites glisser et déposez le système source sur le système cible pour effectuer une réplication ponctuelle des données du volume.

Pour plus d'informations, reportez-vous à "[Réplication des données entre les systèmes](#)".

3. Accédez à la page État de réplication, puis rompez la relation SnapMirror pour convertir le volume répliqué d'un volume de protection des données en un volume de lecture/écriture.

Pour plus d'informations, reportez-vous à "[Gestion des planifications et des relations de réplication des données](#)".

4. Configurer 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 "[Guide express de reprise après sinistre sur volume ONTAP 9](#)".

5. Supprimez le volume d'origine.

Pour plus d'informations, reportez-vous à "[Gérer les volumes](#)".

## Déplacer 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.

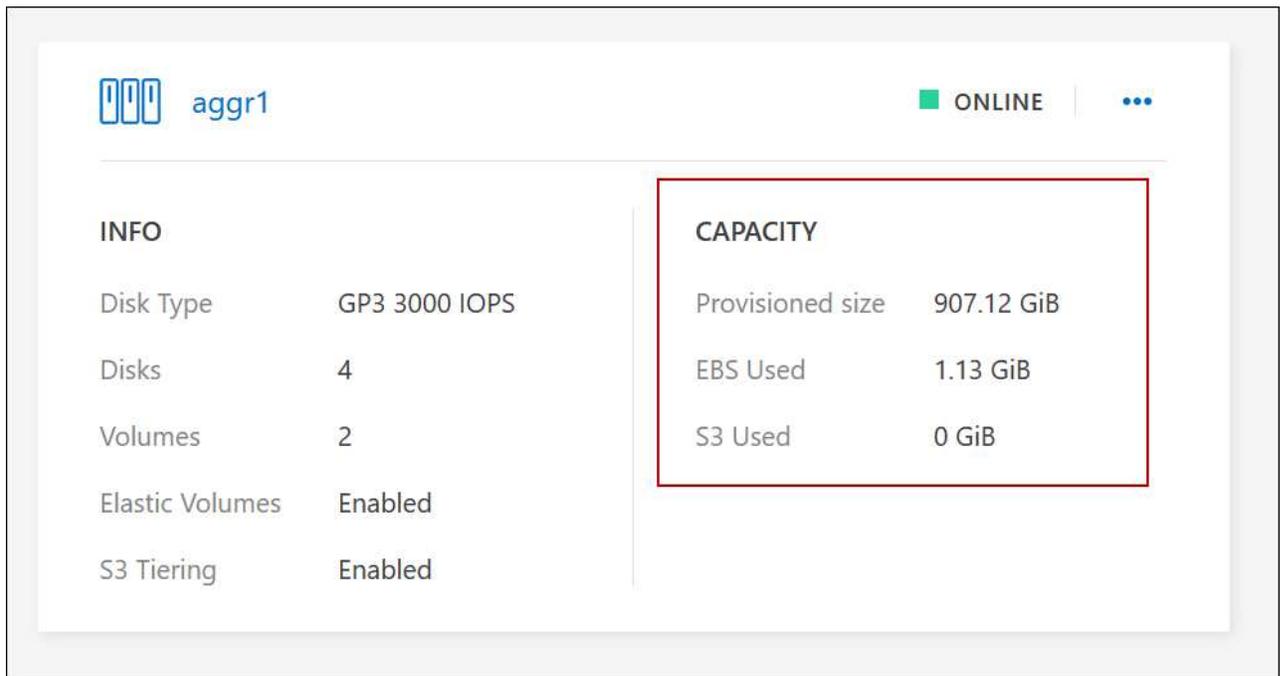
### À propos de cette tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

Le déplacement de deux volumes ou plus est nécessaire pour éviter les problèmes de capacité ; cependant, la console ne peut pas effectuer cette action à votre place.

## Étapes

1. Vérifiez si un agrégat existant dispose d'une capacité disponible pour les volumes que vous devez déplacer :
  - a. Sur le système Cloud Volumes ONTAP , cliquez sur l'onglet **Agrégats**.
  - b. Sur la tuile d'agrégat requise, cliquez sur le bouton  puis **Afficher les détails agrégés** pour afficher la capacité disponible (taille provisionnée moins capacité agrégée utilisée).



2. Si nécessaire, ajoutez des disques à un agrégat existant :
  - a. Sélectionnez l'agrégat, puis cliquez sur le bouton **...** icône > **Ajouter des disques**.
  - b. Sélectionnez le nombre de disques à ajouter, puis cliquez sur **Ajouter**.
3. Si aucun agrégat n'a de capacité disponible, créez un nouvel agrégat.  
 Pour plus d'informations, reportez-vous à "[Création d'agrégats](#)".
4. Utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP pour déplacer les volumes vers l'agrégat.
5. Dans la plupart des situations, vous pouvez utiliser le Gestionnaire système pour déplacer des volumes.  
 Pour les instructions, reportez-vous à la "[Guide de déplacement express de volumes ONTAP 9](#)".

### Raisons pour lesquelles un mouvement de volume peut être lent

Le déplacement d'un volume peut prendre plus de temps que prévu si l'une des conditions suivantes est vraie pour Cloud Volumes ONTAP:

- Le volume est un clone.
- Le volume est le parent d'un clone.
- L'agrégat source ou de destination possède un seul disque dur à débit optimisé (st1).
- L'un des agrégats utilise un ancien schéma de dénomination pour les objets. Les deux agrégats doivent utiliser le même format de nom.

Un schéma de dénomination plus ancien est utilisé si la hiérarchisation des données a été activée sur un agrégat dans la version 9.4 ou antérieure.

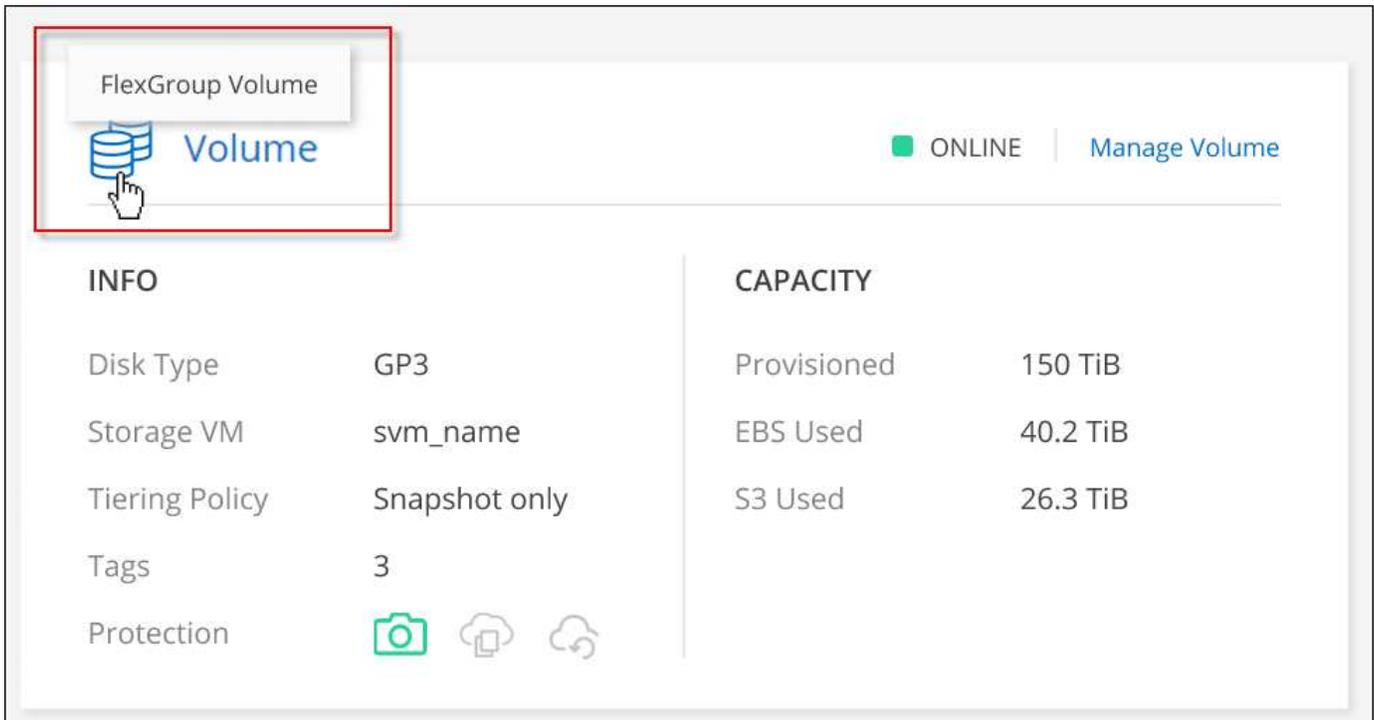
- Les paramètres de chiffrement ne correspondent pas sur les agrégats source et de destination, ou une nouvelle clé est en cours.
- L'option *-tiering-policy* a été spécifiée lors du déplacement du volume pour modifier la politique de

hiérarchisation.

- L'option `-generate-destination-key` a été spécifiée lors du déplacement du volume.

## Afficher les volumes FlexGroup

Vous pouvez afficher les volumes FlexGroup créés via ONTAP System Manager ou l'interface de ligne de commande ONTAP directement via l'onglet Volumes de la console. Vous pouvez voir des informations détaillées sur les volumes FlexGroup via une mosaïque **Volumes** dédiée, où vous pouvez identifier chaque groupe de volumes FlexGroup grâce au texte de survol de l'icône. De plus, vous pouvez identifier et trier les volumes FlexGroup sous la vue de liste des volumes via la colonne Style de volume.



INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection			



Actuellement, vous ne pouvez afficher que les volumes FlexGroup existants sous la console. Vous ne pouvez pas créer de volumes FlexGroup dans la console.

## Hiérarchisez les données Cloud Volumes ONTAP inactives vers un stockage d'objets à faible coût

Vous pouvez réduire les coûts de stockage pour Cloud Volumes ONTAP en combinant un niveau de performance SSD ou HDD pour les données chaudes avec un niveau de capacité de stockage d'objets pour les données inactives. La hiérarchisation des données est alimentée par la technologie FabricPool . Pour un aperçu de haut niveau, reportez-vous à "[Présentation de la hiérarchisation des données](#)".

Pour configurer la hiérarchisation des données, vous devez procéder comme suit :



### 1 Choisissez une configuration prise en charge

La plupart des configurations sont prises en charge. Si vous disposez d'un système Cloud Volumes ONTAP exécutant la version la plus récente, vous êtes prêt à partir. "[Apprendre encore plus](#)".

**2**

### Assurer la connectivité entre Cloud Volumes ONTAP et le stockage d'objets

- Pour AWS, vous aurez besoin d'un point de terminaison VPC vers S3. [Apprendre encore plus](#) .
- Pour Azure, vous n'aurez rien à faire tant que la console NetApp dispose des autorisations requises. [Apprendre encore plus](#) .
- Pour Google Cloud, vous devez configurer le sous-réseau pour l'accès privé à Google et configurer un compte de service. [Apprendre encore plus](#) .

**3**

### Assurez-vous d'avoir un agrégat avec la hiérarchisation activée

La hiérarchisation des données doit être activée sur un agrégat pour pouvoir l'activer sur un volume. Vous devez connaître les exigences relatives aux nouveaux volumes et aux volumes existants. [Apprendre encore plus](#) .

**4**

### Choisissez une politique de hiérarchisation lors de la création, de la modification ou de la réplication d'un volume

La console NetApp vous invite à choisir une stratégie de hiérarchisation lorsque vous créez, modifiez ou répliquez un volume.

- "Données hiérarchisées à partir de volumes en lecture-écriture"
- "Données hiérarchisées à partir des volumes de protection des données"

#### Qu'est-ce qui n'est pas requis pour la hiérarchisation des données ?

- Vous n'avez pas besoin d'installer une licence de fonctionnalité pour activer la hiérarchisation des données.
- Vous n'avez pas besoin de créer un magasin d'objets pour le niveau de capacité. La console le fait pour vous.
- Vous n'avez pas besoin d'activer la hiérarchisation des données au niveau du système.



La console crée un magasin d'objets pour les données froides lors de la création du système, [tant qu'il n'y a pas de problèmes de connectivité ou d'autorisations](#) . Après cela, il vous suffit d'activer la hiérarchisation des données sur les volumes (et dans certains cas, [sur les agrégats](#) ).

## Configurations prenant en charge la hiérarchisation des données

Vous pouvez activer la hiérarchisation des données lorsque vous utilisez des configurations et des fonctionnalités spécifiques.

### Prise en charge dans AWS

- La hiérarchisation des données est prise en charge dans AWS à partir de Cloud Volumes ONTAP 9.2.
- Le niveau de performance peut être des SSD à usage général (gp3 ou gp2) ou des SSD IOPS provisionnés (io1).



Nous ne recommandons pas de hiérarchiser les données vers le stockage d'objets lors de l'utilisation de disques durs à débit optimisé (st1).

- Les données inactives sont hiérarchisées dans les compartiments Amazon S3. La hiérarchisation vers d'autres fournisseurs n'est pas prise en charge.

#### Support dans Azure

- La hiérarchisation des données est prise en charge dans Azure comme suit :
  - Version 9.4 avec systèmes à nœud unique
  - Version 9.6 avec paires HA
- Le niveau de performance peut être des disques gérés par SSD Premium, des disques gérés par SSD Standard ou des disques gérés par HDD Standard.
- Les données inactives sont hiérarchisées vers Microsoft Azure Blob. La hiérarchisation vers d'autres fournisseurs n'est pas prise en charge.

#### Assistance dans Google Cloud

- La hiérarchisation des données est prise en charge dans Google Cloud à partir de Cloud Volumes ONTAP 9.6.
- Le niveau de performance peut être constitué de disques persistants SSD, de disques persistants équilibrés ou de disques persistants standard.
- Les données inactives sont hiérarchisées vers Google Cloud Storage. La hiérarchisation vers d'autres fournisseurs n'est pas prise en charge.

#### Interopérabilité des fonctionnalités

- La hiérarchisation des données est prise en charge par des technologies de cryptage.
- Le provisionnement léger doit être activé sur les volumes.

#### Exigences

Selon votre fournisseur de cloud, certaines connexions et autorisations doivent être configurées pour que Cloud Volumes ONTAP puisse hiérarchiser les données froides vers le stockage d'objets.

#### Exigences pour hiérarchiser les données froides 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 point de terminaison VPC pour le service S3. Pour les instructions, reportez-vous à la "[Documentation AWS : Création d'un point de terminaison de passerelle](#)".

Lorsque vous créez le point de terminaison VPC, assurez-vous de sélectionner la région, le VPC et la table de routage qui correspondent à l'instance Cloud Volumes ONTAP. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui autorise le trafic vers le point de terminaison S3. Sinon, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

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

## Conditions requises pour hiérarchiser les données froides vers le stockage Azure Blob

Vous n'avez pas besoin de configurer une connexion entre le niveau de performance et le niveau de capacité tant que la console dispose des autorisations requises. La console active un point de terminaison de service VNet pour vous si le rôle personnalisé de l'agent de console dispose des autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

Le rôle personnalisé inclut les autorisations par défaut. ["Afficher l'autorisation Azure pour l'agent de la console"](#)

## Conditions requises pour hiérarchiser les données froides vers un bucket Google Cloud Storage

- Le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour l'accès privé à Google. Pour les instructions, reportez-vous à ["Documentation Google Cloud : Configuration de l'accès privé à Google"](#) .
- Un compte de service doit être associé à Cloud Volumes ONTAP.

["Découvrez comment configurer ce compte de service"](#) .

Vous êtes invité à sélectionner ce compte de service lorsque vous créez un système Cloud Volumes ONTAP .

Si vous ne sélectionnez pas de compte de service lors du déploiement, vous devrez arrêter Cloud Volumes ONTAP, accéder à la console Google Cloud, puis attacher le compte de service aux instances Cloud Volumes ONTAP . Vous pouvez ensuite activer la hiérarchisation des données comme décrit dans la section suivante.

- Pour chiffrer le bucket avec des clés de chiffrement gérées par le client, activez le bucket de stockage Google Cloud pour utiliser la clé.

["Découvrez comment utiliser les clés de chiffrement gérées par le client avec Cloud Volumes ONTAP"](#) .

## Activer la hiérarchisation des données après la mise en œuvre des exigences

La console crée un magasin d'objets pour les données froides lors de la création du système, à condition qu'il n'y ait pas de problèmes de connectivité ou d'autorisations. Si vous n'avez pas implémenté les exigences répertoriées ci-dessus avant de créer le système, vous devrez activer manuellement la hiérarchisation via l'API ou ONTAP System Manager, qui crée le magasin d'objets.



La possibilité d'activer la hiérarchisation via la console sera disponible dans une future version de Cloud Volumes ONTAP .

## Assurez-vous que la hiérarchisation est activée sur les agrégats

La hiérarchisation des données doit être activée sur un agrégat afin d'activer la hiérarchisation des données sur un volume. Vous devez connaître les exigences relatives aux nouveaux volumes et aux volumes existants.

### • Nouveaux volumes

Si vous activez la hiérarchisation des données sur un nouveau volume, vous n'avez pas à vous soucier de l'activation de la hiérarchisation des données sur un agrégat. La console crée le volume sur un agrégat

existant pour lequel la hiérarchisation est activée, ou elle crée un nouvel agrégat pour le volume si aucun agrégat pour lequel la hiérarchisation des données est activée n'existe déjà.

#### • Volumes existants

Pour activer la hiérarchisation des données sur un volume existant, assurez-vous qu'elle est activée sur l'agrégat sous-jacent. Si la hiérarchisation des données n'est pas activée sur l'agrégat existant, vous devrez utiliser ONTAP System Manager pour attacher un agrégat existant au magasin d'objets.

#### Étapes pour confirmer si la hiérarchisation est activée sur un agrégat

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Ouvrez le système Cloud Volumes ONTAP .
3. Sélectionnez l'onglet **Agrégats** et vérifiez si la hiérarchisation est activée ou désactivée sur l'agrégat.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

#### Étapes pour activer la hiérarchisation sur un agrégat

1. Dans ONTAP System Manager, cliquez sur **Stockage > Niveaux**.
2. Cliquez sur le menu d'action pour l'agrégat et sélectionnez **Attacher les niveaux de cloud**.
3. Sélectionnez le niveau de cloud à joindre et cliquez sur **Enregistrer**.

#### Quelle est la prochaine étape ?

Vous pouvez désormais activer la hiérarchisation des données sur les volumes nouveaux et existants, comme expliqué dans la section suivante.

#### Données hiérarchisées à partir de volumes en lecture-écriture

Cloud Volumes ONTAP peut hiérarchiser les données inactives sur des volumes en lecture-écriture vers un stockage d'objets rentable, libérant ainsi le niveau de performances pour les données chaudes.

#### Étapes

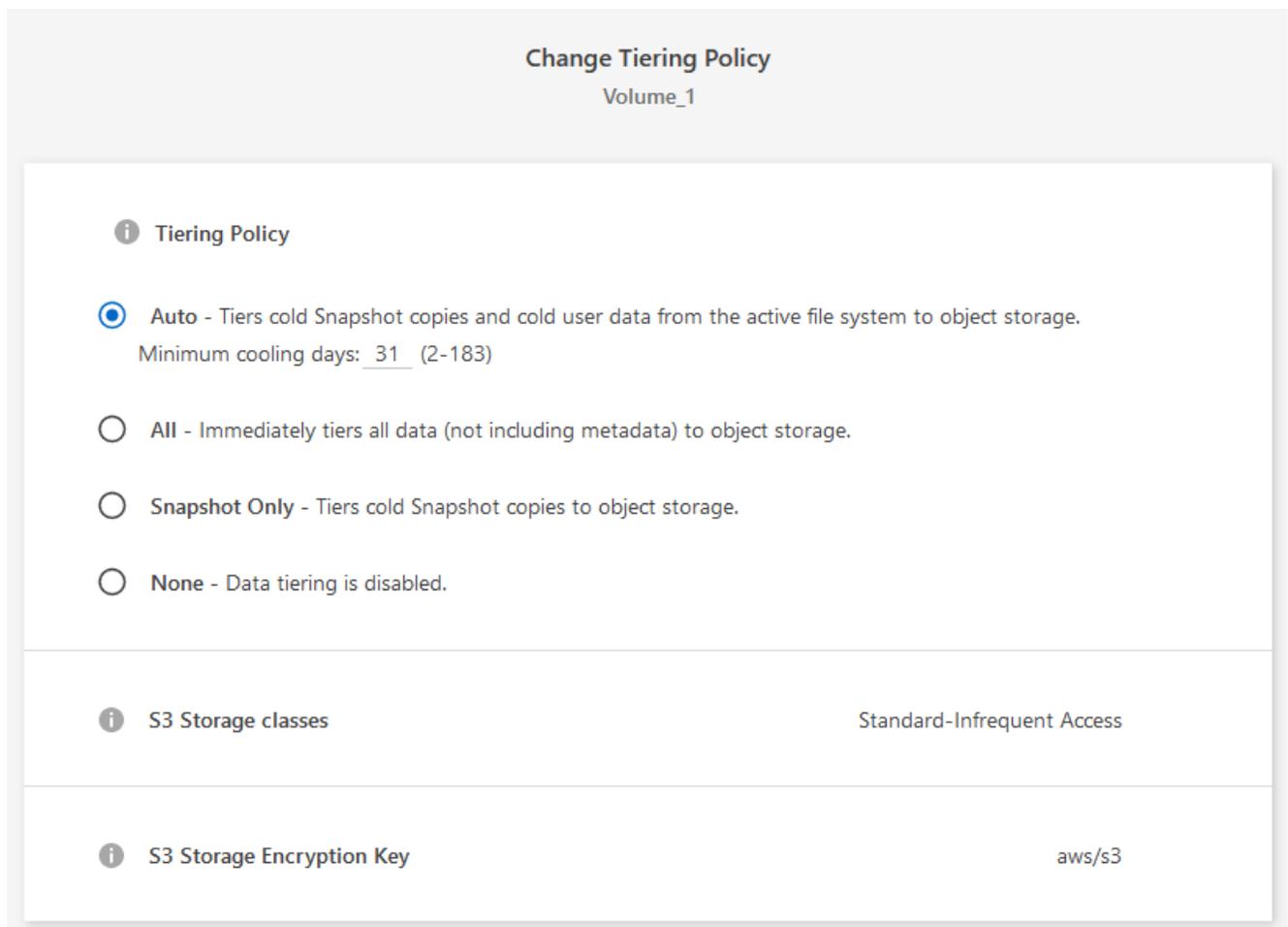
1. Dans l'onglet **Volumes** sous le système, créez un nouveau volume ou modifiez le niveau d'un volume existant :

Tâche	Action
Créer un nouveau volume	Cliquez sur <b>Ajouter un nouveau volume</b> .
Modifier un volume existant	Sélectionnez la mosaïque de volume souhaitée, cliquez sur <b>Gérer le volume</b> pour accéder au panneau de droite Gérer les volumes, puis cliquez sur <b>Actions avancées</b> et <b>Modifier la politique de hiérarchisation</b> sous le panneau de droite.

2. Sélectionnez une politique de hiérarchisation.

Pour une description de ces politiques, reportez-vous à "[Présentation de la hiérarchisation des données](#)".

### Exemple



La console crée un nouvel agrégat pour le volume si aucun agrégat compatible avec la hiérarchisation des données n'existe déjà.

### Données hiérarchisées à partir des volumes de protection des données

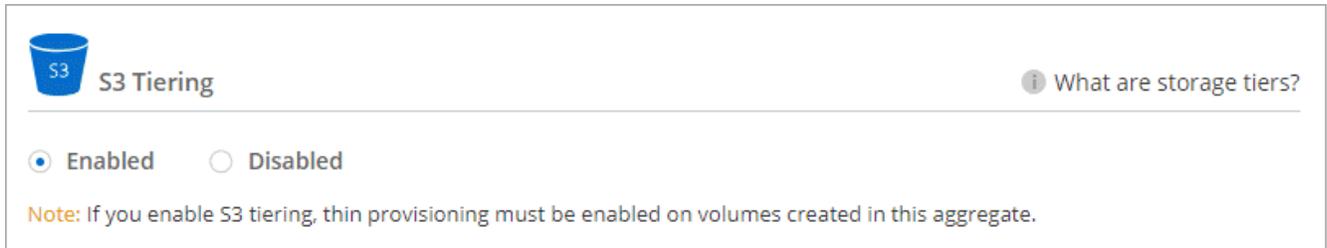
Cloud Volumes ONTAP peut hiérarchiser les données d'un volume de protection des données vers un niveau de capacité. Si vous activez le volume de destination, les données sont progressivement déplacées vers le

niveau de performance au fur et à mesure de leur lecture.

## Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, sélectionnez le système Cloud Volumes ONTAP qui contient le volume source, puis faites-le glisser vers le système sur lequel vous souhaitez répliquer le volume.
3. Suivez les invites jusqu'à ce que vous atteigniez la page de hiérarchisation et activez la hiérarchisation des données pour le stockage d'objets.

## Exemple



Pour obtenir de l'aide sur la réplication des données, reportez-vous à ["Réplication des données vers et depuis le cloud"](#) .

## Modifier la classe de stockage pour les données hiérarchisées

Après avoir déployé Cloud Volumes ONTAP, vous pouvez réduire vos coûts de stockage en modifiant la classe de stockage des données inactives qui n'ont pas été consultées depuis 30 jours. Les coûts d'accès sont plus élevés si vous accédez aux données, vous devez donc en tenir compte avant de modifier la classe de stockage.

La classe de stockage pour les données hiérarchisées s'applique à l'ensemble du système, et non par volume.

Pour plus d'informations sur les classes de stockage prises en charge, reportez-vous à ["Présentation de la hiérarchisation des données"](#) .

## Étapes

1. Sur le système Cloud Volumes ONTAP , cliquez sur l'icône de menu, puis sur **Classes de stockage** ou **Niveau de stockage Blob**.
2. Choisissez une classe de stockage, puis cliquez sur **Enregistrer**.

## Modifier le ratio d'espace libre pour la hiérarchisation des données

Le ratio d'espace libre pour la hiérarchisation des données définit la quantité d'espace libre requise sur les SSD/HDD Cloud Volumes ONTAP lors de la hiérarchisation des données vers le stockage d'objets. Le paramètre par défaut est de 10 % d'espace libre, mais vous pouvez modifier le paramètre en fonction de vos besoins.

Par exemple, vous pouvez choisir moins de 10 % d'espace libre pour vous assurer d'utiliser la capacité achetée. La console peut ensuite acheter des disques supplémentaires pour vous lorsque une capacité supplémentaire est requise (jusqu'à ce que vous atteigniez la limite de disque pour l'agrégat).



S'il n'y a pas suffisamment d'espace, Cloud Volumes ONTAP ne peut pas déplacer les données et vous risquez de subir une dégradation des performances. Tout changement doit être effectué avec prudence. Si vous n'êtes pas sûr, contactez le support NetApp pour obtenir des conseils.

Le ratio est important pour les scénarios de reprise après sinistre car, à mesure que les données sont lues à partir du magasin d'objets, Cloud Volumes ONTAP déplace les données vers des disques SSD/HDD pour offrir de meilleures performances. S'il n'y a pas suffisamment d'espace, Cloud Volumes ONTAP ne peut pas déplacer les données. Tenez-en compte lorsque vous modifiez le ratio afin de pouvoir répondre aux besoins de votre entreprise.

## Étapes

1. Dans le volet de navigation de gauche, accédez à **Administration > Agents**.
2. Cliquez sur le **...** icône pour l'agent de console qui gère votre système Cloud Volumes ONTAP .
3. Sélectionnez \* Paramètres Cloud Volumes ONTAP \*.

The screenshot shows the NetApp console interface. On the left, there is a navigation menu with 'Agents' selected. The main area displays a table of agents. The table has columns for Name, Location, Status, and Deployment Type. Three agents are listed: 'AWSAgent' (US East (N. Virginia), Active, AWS), 'eastus' (eastus, Active, Microsoft), and 'AWS' (US East (N. Virginia), Active, AWS). A context menu is open for the 'eastus' agent, showing options: 'Edit Agent', 'Go to local UI', 'Agent Id: [redacted]', 'HTTPS Setup', 'Cloud Volumes ONTAP Settings' (highlighted with a red box), and 'Remove Agent'.

Name	Location	Status (1)	Deployment Type
AWSAgent	US East (N. Virginia)	Active	aws
eastus	eastus	Active	Microsoft
AWS	US East (N. Virginia)	Active	AWS

4. Sous **Capacité**, cliquez sur **Seuils de capacité globale - Ratio d'espace libre pour la hiérarchisation des données**.

## Edit Cloud Volumes ONTAP settings

## Capacity

Capacity Management Mode	Automatic Mode	▼
Aggregate Capacity Thresholds - Free Space Ratio	10%	▼
Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%	▼
Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%	▼

## General

Automatic Cloud Volumes ONTAP update during deployment	On	▼
--	----	---

## Azure

Azure CIFS locks for Azure HA systems	Off	▼
Use Azure Private Link	On	▼

5. Modifiez le ratio d'espace libre en fonction de vos besoins et cliquez sur **Enregistrer**.

### Modifier la période de refroidissement pour la politique de hiérarchisation automatique

Si vous avez activé la hiérarchisation des données sur un volume Cloud Volumes ONTAP à l'aide de la stratégie de hiérarchisation *auto*, vous pouvez ajuster la période de refroidissement par défaut en fonction des besoins de votre entreprise. Cette action est prise en charge uniquement via ONTAP CLI et API.

La période de refroidissement est le nombre de jours pendant lesquels les données utilisateur d'un volume doivent rester inactives avant d'être considérées comme « froides » et déplacées vers le stockage d'objets.

La période de refroidissement par défaut pour la politique de hiérarchisation automatique est de 31 jours. Vous pouvez modifier la période de refroidissement comme suit :

- 9.8 ou version ultérieure : 2 à 183 jours
- 9.7 ou version antérieure : 2 à 63 jours

#### Étape

1. Utilisez le paramètre *minimumCoolingDays* avec votre requête API lors de la création d'un volume ou de la modification d'un volume existant.

### Supprimer un bucket S3 lors de la mise hors service d'un système

Vous pouvez supprimer un compartiment S3 avec les données hiérarchisées à partir d'un système Cloud Volumes ONTAP lorsque vous mettez hors service l'environnement.

Vous pouvez supprimer le compartiment S3 uniquement si :

- Le système Cloud Volume ONTAP est supprimé de la console.
- Tous les objets sont supprimés du bucket et le bucket S3 est vide.

Lorsque vous désaffectez un système Cloud Volumes ONTAP , le bucket S3 créé pour l'environnement n'est pas supprimé automatiquement. Au lieu de cela, il reste dans un état orphelin pour éviter toute perte accidentelle de données. Vous pouvez supprimer les objets du bucket, puis supprimer le bucket S3 lui-même ou le conserver pour une utilisation ultérieure. Se référer à "[CLI ONTAP : suppression du compartiment du serveur de stockage d'objets vserver](#)".

## Connectez-vous à un LUN sur Cloud Volumes ONTAP depuis votre système hôte

Lorsque vous créez un volume iSCSI, la console NetApp crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume, utilisez l'IQN pour vous connecter au LUN à partir de vos hôtes.

Notez ce qui suit :

- La gestion automatique de la capacité de la console ne s'applique pas aux LUN. Lorsqu'il crée un LUN, il désactive la fonction de croissance automatique.
- Vous pouvez créer des LUN supplémentaires à partir d' ONTAP System Manager ou de l' ONTAP CLI.

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le système Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
3. Dans le système, sélectionnez l'onglet **Volumes**.
4. Accédez à la mosaïque de volume requise, puis sélectionnez **Gérer le volume** pour accéder au panneau Gérer les volumes sur la droite.
5. Cliquez sur **Cible iQN**.
6. Cliquez sur **Copier** pour copier le nom iQN.
7. Configurez une connexion iSCSI de l'hôte au LUN.
  - "[Configuration express iSCSI ONTAP 9 pour Red Hat Enterprise Linux : démarrage des sessions iSCSI avec la cible](#)"
  - "[Configuration express iSCSI ONTAP 9 pour Windows : démarrage de sessions iSCSI avec la cible](#)"
  - "[Configuration de l'hôte SAN ONTAP](#)"

## Accélérez l'accès aux données avec les volumes FlexCache sur un système Cloud Volumes ONTAP

Un volume FlexCache est un volume de stockage qui met en cache les données de lecture SMB et NFS à partir d'un volume d'origine (ou source). Les lectures ultérieures des données mises en cache entraînent un accès plus rapide à ces données.

Vous pouvez utiliser les volumes FlexCache 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 aux mêmes données à plusieurs reprises, car les données peuvent être servies directement sans avoir à accéder au volume d'origine. Les volumes FlexCache fonctionnent bien pour les charges de travail système nécessitant beaucoup de lecture.

La console NetApp permet la gestion des volumes FlexCache avec le ["Mise en cache des volumes NetApp"](#) .

Vous pouvez également utiliser ONTAP CLI ou ONTAP System Manager pour créer et gérer des volumes FlexCache :

- ["Guide d'alimentation des volumes FlexCache pour un accès plus rapide aux données"](#)
- ["Création de volumes FlexCache dans System Manager"](#)



## Travailler avec FlexCache lorsque l'origine est cryptée

Lors de la configuration de FlexCache sur un système Cloud Volumes ONTAP où le volume d'origine est chiffré, des étapes supplémentaires sont requises pour garantir que le volume FlexCache peut accéder correctement aux données chiffrées et les mettre en cache.

### Avant de commencer

1. **Configuration du chiffrement** : Assurez-vous que le volume source est entièrement chiffré et opérationnel. Pour les systèmes Cloud Volumes ONTAP , cela implique l'intégration avec des services de gestion de clés spécifiques au cloud.

Pour AWS, cela signifie généralement utiliser AWS Key Management Service (KMS). Pour plus d'informations, reportez-vous à ["Gérer les clés avec AWS Key Management Service"](#) .

Pour Azure, vous devez configurer Azure Key Vault pour NetApp Volume Encryption (NVE). Pour plus d'informations, reportez-vous à ["Gérer les clés avec Azure Key Vault"](#) .

Pour Google Cloud, il s'agit du service de gestion des clés Google Cloud. Pour plus d'informations, reportez-

vous à ["Gérez les clés avec le service de gestion des clés cloud de Google"](#) .

1. **Services de gestion de clés** : avant de créer un volume FlexCache , vérifiez que les services de gestion de clés sont correctement configurés sur le système Cloud Volumes ONTAP . Cette configuration est essentielle pour que le volume FlexCache décrypte les données du volume d'origine.
2. **Licence** : Confirmez qu'une licence FlexCache valide est disponible et activée sur le système Cloud Volumes ONTAP .
3. \* Version ONTAP \* : assurez-vous que la version ONTAP de votre système Cloud Volumes ONTAP prend en charge FlexCache avec des volumes chiffrés. Consultez les dernières ["Notes de version ONTAP"](#) ou matrice de compatibilité pour plus d'informations.
4. **Configuration réseau** : Assurez-vous que la configuration réseau permet une communication transparente entre le volume d'origine et le volume FlexCache . Cela inclut un routage approprié et une résolution DNS dans un environnement cloud.

## Étapes

Créez un volume FlexCache sur votre système Cloud Volumes ONTAP avec un volume source chiffré. Pour les étapes détaillées et les considérations supplémentaires, reportez-vous aux sections suivantes :

- ["Guide d'alimentation des volumes FlexCache pour un accès plus rapide aux données"](#)
- ["Création de volumes FlexCache dans System Manager"](#)

# Administration globale

## Créer un agrégat pour les systèmes Cloud Volumes ONTAP

Vous pouvez créer des agrégats vous-même ou laisser la console NetApp le faire pour vous lorsqu'elle crée des volumes. L'avantage de créer vous-même des agrégats est que vous pouvez choisir la taille du disque sous-jacent, ce qui vous permet de dimensionner votre agrégat en fonction de la capacité ou des performances dont vous avez besoin.



Tous les disques et agrégats doivent être créés et supprimés directement depuis la console. 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 potentiellement générer des frais de fournisseur de cloud redondants.

## Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
3. Dans l'onglet Agrégats, cliquez sur **Ajouter un 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 ["Planifiez 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 qui prend en charge la fonctionnalité Amazon EBS Elastic Volumes. La capture d'écran suivante montre un exemple d'un nouvel agrégat composé de disques gp3.

1 Disk Type    2 Aggregate details    3 Tiering Data    4 Review

### Select Disk Type

Disk Type

GP3 - General Purpose SSD Dynamic Performance

General Purpose SSD (gp3) Disk Properties

Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value    Throughput MB/s

12000    250

["En savoir plus sur la prise en charge des volumes élastiques"](#) .

## Azuré

Pour obtenir de l'aide sur le type et la taille du disque, reportez-vous à ["Planifiez votre configuration Cloud Volumes ONTAP dans Azure"](#) .

## Google Cloud

Pour obtenir de l'aide sur le type et la taille du disque, reportez-vous à ["Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud"](#) .

4. Cliquez sur **Ajouter**, puis sur **Approuver et acheter**.

## Gérer les agrégats pour les clusters Cloud Volumes ONTAP

Gérez vous-même les agrégats en ajoutant des disques, en affichant des informations sur les agrégats et en les supprimant.



Tous les disques et agrégats doivent être créés et supprimés directement à partir de la console NetApp . 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 potentiellement générer des frais de fournisseur de cloud redondants.

### Avant de commencer

Si vous souhaitez supprimer un agrégat, vous devez d'abord avoir supprimé les volumes de l'agrégat.

### À propos de cette tâche

Si un agrégat manque d'espace, vous pouvez déplacer des volumes vers un autre agrégat à l'aide d' ONTAP System Manager.

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le système Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
3. Dans les détails du système, cliquez sur l'onglet **Agrégats**.
4. Pour l'agrégat requis, cliquez sur le **...** icône pour les actions de gestion.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

5. Gérez vos agrégats à partir des options disponibles dans le **...** menu.



Pour ajouter des disques à un agrégat, tous les disques de l'agrégat doivent être de la même taille.

Pour AWS, vous pouvez augmenter la capacité d'un agrégat prenant en charge Amazon EBS Elastic Volumes.

1. Sous le **...** menu, cliquez sur **Augmenter la capacité**.
2. Saisissez la capacité supplémentaire que vous souhaitez ajouter, puis cliquez sur **Augmenter**.

Notez que vous devez augmenter la capacité de l'agrégat d'au moins 256 Gio ou 10 % de la taille de l'agrégat. Par exemple, si vous avez un agrégat de 1,77 Tio, 10 % correspondent à 181 Gio. C'est inférieur à 256 Gio, donc la taille de l'agrégat doit être augmentée du minimum de 256 Gio.

## Gérer la capacité globale de Cloud Volumes ONTAP sur un agent de console

Chaque agent de console dispose de paramètres qui déterminent la manière dont il gère la capacité globale de Cloud Volumes ONTAP.

Ces paramètres affectent tous les systèmes Cloud Volumes ONTAP gérés par un agent de console. Si vous disposez d'un autre agent de console, il peut être configuré différemment.

### Autorisations requises

Vous avez besoin des privilèges d'administrateur d'organisation ou de compte de la console NetApp pour modifier les paramètres Cloud Volumes ONTAP .

### Étapes

1. Dans le volet de navigation de gauche, accédez à **Administration > Agents**.
2. Cliquez sur le **...** icône pour l'agent de console qui gère votre système Cloud Volumes ONTAP .
3. Sélectionnez **\* Paramètres Cloud Volumes ONTAP \***.

The screenshot shows the NetApp Console interface. The top navigation bar includes the NetApp logo, 'Console', and dropdown menus for 'Organization' (NetAppNew) and 'Project' (Project-1). On the left, a sidebar shows 'Agents' and 'Overview'. The main content area displays 'Agents (3 / 58)' with a search icon and a 'Deploy agent' button. A table lists three agents:

Name	Location	Status (1)	Deployment Type
AWSSAgent	US East (N. Virginia)	Active	aws
5678	eastus	Active	
itAWS	US East (N. Virginia)	Active	

A context menu is open for the first agent, showing options: 'Edit Agent', 'Go to local UI', 'Agent Id: [id]', 'HTTPS Setup', 'Cloud Volumes ONTAP Settings' (highlighted with a red box), and 'Remove Agent'.

4. Sous **Capacité**, modifiez l'un des paramètres suivants :

## Edit Cloud Volumes ONTAP settings

### Capacity

Capacity Management Mode	Automatic Mode	▼
Aggregate Capacity Thresholds - Free Space Ratio	10%	▼
Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%	▼
Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%	▼

### General

Automatic Cloud Volumes ONTAP update during deployment	On	▼
--	----	---

### Azure

Azure CIFS locks for Azure HA systems	Off	▼
Use Azure Private Link	On	▼

## Mode de gestion de la capacité

Choisissez si la console doit vous informer des décisions en matière de capacité de stockage ou si elle doit gérer automatiquement les besoins en capacité pour vous.

["Découvrez comment fonctionne le mode de gestion de la capacité"](#) .

## Seuil de capacité globale - Rapport espace libre

Ce ratio est un paramètre clé dans les décisions de gestion de la capacité, et il est essentiel de comprendre son impact, que vous soyez en mode automatique ou manuel de gestion de la capacité. Il est recommandé de définir ce seuil en tenant compte de vos besoins de stockage spécifiques et de la croissance prévue afin de maintenir un équilibre entre l'utilisation des ressources et les coûts.

En mode manuel, si le ratio d'espace libre sur un agrégat tombe en dessous du seuil spécifié, il déclenche une notification, vous avertissant que vous devez prendre des mesures pour remédier au faible ratio d'espace libre. Il est important de surveiller ces notifications et de gérer manuellement la capacité globale pour éviter toute interruption de service et garantir des performances optimales.

Le ratio d'espace libre est calculé comme suit :  $(\text{capacité globale} - \text{capacité totale utilisée sur l'agrégat}) / \text{capacité globale}$

Se référer à "[Gestion automatique des capacités](#)" pour en savoir plus, la capacité est désormais gérée automatiquement dans Cloud Volumes ONTAP.

### **Seuils de capacité globale - Ratio d'espace libre pour la hiérarchisation des données**

Définit la quantité d'espace libre requise sur le niveau de performance (disques) lors de la hiérarchisation des données vers un niveau de capacité (stockage d'objets).

Le ratio est important pour les scénarios de reprise après sinistre. À mesure que les données sont lues à partir du niveau de capacité, Cloud Volumes ONTAP déplace les données vers le niveau de performance pour offrir de meilleures performances. S'il n'y a pas suffisamment d'espace, Cloud Volumes ONTAP ne peut pas déplacer les données.

5. Cliquez sur **Enregistrer**.

## **Administration des machines virtuelles de stockage**

### **Gérer les machines virtuelles de stockage pour Cloud Volumes ONTAP**

Une machine virtuelle de stockage est une machine virtuelle exécutée dans ONTAP qui fournit des services de stockage et de données à vos clients. Vous connaissez peut-être cela sous le nom de *SVM* ou *vserver*. Cloud Volumes ONTAP est configuré avec une machine virtuelle de stockage par défaut, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

#### **Nombre de machines virtuelles de stockage prises en charge**

Plusieurs machines virtuelles de stockage sont prises en charge avec certaines configurations. Aller à la ["Notes de version de Cloud Volumes ONTAP"](#) pour vérifier le nombre de machines virtuelles de stockage prises en charge pour votre version de Cloud Volumes ONTAP.

#### **Travailler avec plusieurs machines virtuelles de stockage**

La console NetApp prend en charge toutes les machines virtuelles de stockage supplémentaires que vous créez à partir d' ONTAP System Manager ou de l'interface de ligne de commande ONTAP .

Par exemple, l'image suivante montre comment vous pouvez choisir une machine virtuelle de stockage lorsque vous créez un volume.

### Details & Protection

Storage VM Name ?

svm\_name1 v

Volume Name Size (GiB) ?

Snapshot Policy

default v

? Default Policy

L'image suivante montre comment vous pouvez choisir une machine virtuelle de stockage lors de la réplication d'un volume vers un autre système.

Destination Volume Name

volume\_copy

Destination Storage VM Name

svm\_name1 v

Destination Aggregate

Automatically select the best aggregate v

#### Modifier le nom de la machine virtuelle de stockage par défaut

La console nomme automatiquement la machine virtuelle de stockage unique qu'elle crée pour Cloud Volumes ONTAP. À partir d' ONTAP System Manager, de l'interface de ligne de commande ONTAP ou de l'API, vous pouvez modifier le nom de la machine virtuelle de stockage si vous avez des normes de dénomination strictes. Par exemple, vous souhaitez peut-être que le nom corresponde à la manière dont vous nommez les machines virtuelles de stockage pour vos clusters ONTAP .

## Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans AWS

Une machine virtuelle de stockage est une machine virtuelle exécutée dans ONTAP qui fournit des services de stockage et de données à vos clients. Vous connaissez peut-être cela sous le nom de *SVM* ou *vserver*. Cloud Volumes ONTAP est configuré avec une machine virtuelle de stockage par défaut, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

Pour créer des machines virtuelles de stockage de service de données supplémentaires, 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 prises 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. Aller à la "[Notes de version de Cloud Volumes ONTAP](#)" pour vérifier le nombre de machines virtuelles de stockage prises en charge pour votre version de Cloud Volumes ONTAP.

Toutes les autres configurations Cloud Volumes ONTAP prennent en charge une machine virtuelle de stockage de service de données et une machine virtuelle de stockage de destination utilisée pour la reprise après sinistre. Vous pouvez activer la machine virtuelle de stockage de destination pour l'accès 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 le "[Section Limites de stockage dans les notes de publication de Cloud Volumes ONTAP](#)" .
2. Identifiez le nombre maximal d'adresses IP par interface pour votre type d'instance.
3. Notez ce numéro car vous en aurez besoin dans la section suivante lorsque vous allouerez des adresses IP dans AWS.

### Attribuer des adresses IP dans AWS

Les adresses IPv4 privées doivent être attribuées au port e0a dans AWS avant de créer des LIF pour la nouvelle machine virtuelle de stockage.

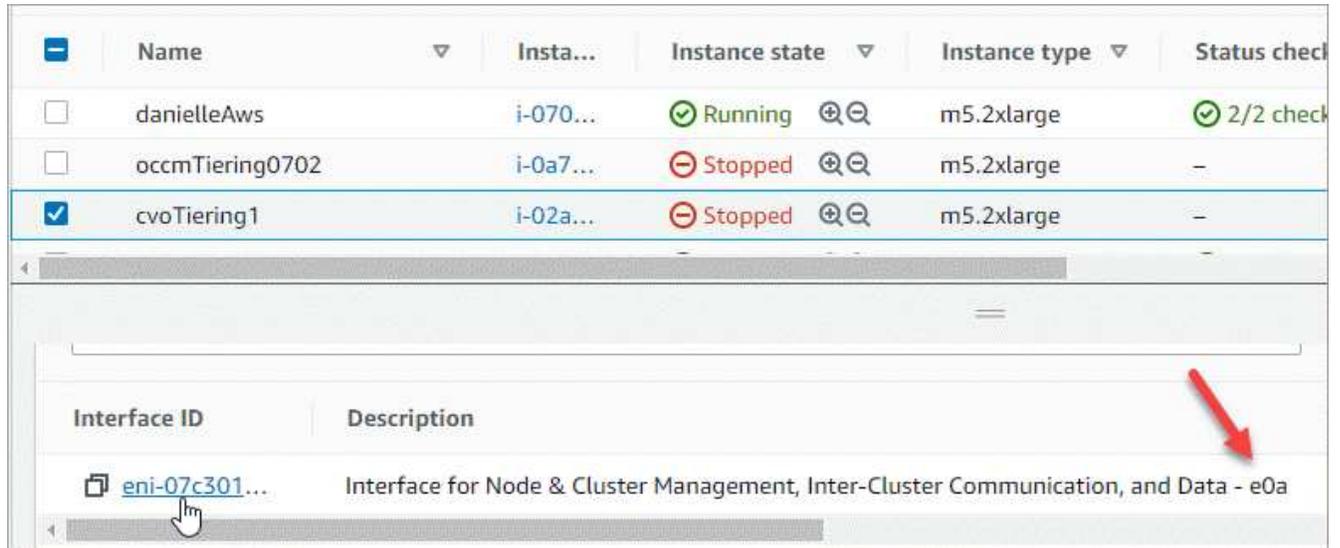
Notez qu'un LIF de gestion facultatif pour une machine virtuelle de stockage nécessite une adresse IP privée sur un système à nœud unique et sur une paire HA dans une seule zone de disponibilité. Ce LIF de gestion fournit une connexion à des outils de gestion comme SnapCenter.

#### 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 HA, sélectionnez le nœud 1.

3. Faites défiler jusqu'à **Interfaces réseau** et cliquez sur l'**ID d'interface** pour le port e0a.



Name	Insta...	Instance state	Instance type	Status check
danielleAws	i-070...	Running	m5.2xlarge	2/2 check
occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
eni-07c301...	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - e0a

4. Sélectionnez l'interface réseau et cliquez sur **Actions > Gérer les adresses IP**.

5. Développez la liste des adresses IP pour e0a.

6. Vérifiez les adresses IP :

- Comptez le nombre d'adresses IP allouées pour confirmer que le port dispose de suffisamment d'espace pour des adresses IP supplémentaires.

Vous devriez avoir identifié le nombre maximal d'adresses IP prises en charge par interface dans la section précédente de cette page.

- Facultatif : accédez à l'interface de ligne de commande ONTAP 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 dont vous avez besoin pour la nouvelle machine virtuelle de stockage.

- Système à nœud unique : une adresse IP privée secondaire inutilisée est requise.

Une adresse IP privée secondaire facultative est requise si vous souhaitez créer un LIF de gestion sur la machine virtuelle de stockage.

- Paire HA dans une seule AZ : une IP privée secondaire inutilisée est requise sur le nœud 1.

Une adresse IP privée secondaire facultative est requise si vous souhaitez créer un LIF de gestion sur la machine virtuelle de stockage.

- Paire HA dans plusieurs AZ : une IP privée secondaire inutilisée est requise sur chaque nœud.

8. Si vous allouez l'adresse IP sur une paire HA dans une seule zone de disponibilité, activez **Autoriser la réattribution des adresses IPv4 privées secondaires**.

9. Cliquez sur **Enregistrer**.

10. Si vous avez une paire HA dans plusieurs AZ, vous devrez répéter ces étapes pour le nœud 2.

### Créer une machine virtuelle de stockage sur un système à nœud unique

Ces étapes créent une nouvelle machine virtuelle de stockage sur un système à nœud unique. Une adresse IP privée est requise pour créer un NAS LIF et une autre adresse IP privée facultative est nécessaire si vous souhaitez créer un LIF de gestion.

#### Étapes

1. Créez la machine virtuelle de stockage et un itinéraire vers la machine virtuelle 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 un NAS LIF.

```
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 IP privée secondaire inutilisée sur e0a.

3. Facultatif : créez un 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 IP privée secondaire inutilisée sur e0a.

4. Affectez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est nécessaire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur la machine virtuelle de stockage.

### Créer une machine virtuelle de stockage sur une paire HA dans une seule zone de disponibilité

Ces étapes créent une nouvelle machine virtuelle de stockage sur une paire HA dans une seule zone de disponibilité. Une adresse IP privée est requise pour créer un NAS LIF et une autre adresse IP privée

facultative est nécessaire si vous souhaitez créer un LIF de gestion.

Ces deux LIF sont alloués sur le nœud 1. Les adresses IP privées peuvent se déplacer entre les nœuds en cas de panne.

## Étapes

1. Créez la machine virtuelle de stockage et un itinéraire vers la machine virtuelle 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. Créez un NAS LIF 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 IP privée secondaire inutilisée sur e0a de cvo-node1. Cette adresse IP peut être déplacée vers l'e0a de cvo-node2 en cas de prise de contrôle car la politique de service default-data-files indique que les IP peuvent migrer vers le nœud partenaire.

3. Facultatif : créez un LIF de gestion de machine virtuelle 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 IP privée secondaire inutilisée sur e0a.

4. Affectez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est nécessaire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur la machine virtuelle de stockage.

5. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou une version ultérieure, modifiez les stratégies de service réseau pour la machine virtuelle de stockage.

La modification des services est nécessaire car elle garantit que Cloud Volumes ONTAP peut utiliser le 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

```

## Créer une machine virtuelle de stockage sur une paire HA dans plusieurs AZ

Ces étapes créent une nouvelle machine virtuelle de stockage sur une paire HA dans plusieurs AZ.

Une adresse IP *flottante* est requise pour un NAS LIF et est facultative pour un LIF de gestion. Ces adresses IP flottantes ne nécessitent pas que vous allouiez des adresses IP privées dans AWS. Au lieu de cela, 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 avec ONTAP, une adresse IP privée doit être configurée sur chaque machine virtuelle de stockage sur chaque nœud. Cela se reflète dans les étapes ci-dessous où un LIF iSCSI est créé sur le nœud 1 et sur le nœud 2.

### Étapes

1. Créez la machine virtuelle de stockage et un itinéraire vers la machine virtuelle 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. Créez un NAS LIF 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 en dehors 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 IP peuvent migrer vers le nœud partenaire.

## 3. Facultatif : créez un LIF de gestion de machine virtuelle 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. Créez un 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
```

- Ce LIF iSCSI est requis pour prendre en charge la migration LIF des IP flottantes dans la machine virtuelle de stockage. Il n'est pas nécessaire qu'il s'agisse d'un LIF iSCSI, mais il ne peut pas être configuré 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. Créez un 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
```

- Ce LIF iSCSI est requis pour prendre en charge la migration LIF des IP flottantes dans la machine virtuelle de stockage. Il n'est pas nécessaire qu'il s'agisse d'un LIF iSCSI, mais il ne peut pas être configuré 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. Affectez un ou plusieurs agrégats à la machine virtuelle de stockage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Cette étape est nécessaire car la nouvelle machine virtuelle de stockage doit accéder à au moins un agrégat avant de pouvoir créer des volumes sur la machine virtuelle de stockage.

7. Si vous exécutez Cloud Volumes ONTAP 9.11.1 ou une version ultérieure, modifiez les stratégies de service réseau pour la machine virtuelle de stockage.

La modification des services est nécessaire car elle garantit que Cloud Volumes ONTAP peut utiliser le 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

```

## Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans Azure

Une machine virtuelle de stockage est une machine virtuelle exécutée dans ONTAP qui fournit des services de stockage et de données à vos clients. Vous connaissez peut-être cela sous le nom de *SVM* ou *vserver*. Cloud Volumes ONTAP est configuré avec une machine virtuelle de stockage par défaut, mais vous pouvez créer des machines virtuelles de stockage supplémentaires lors de l'exécution de Cloud Volumes ONTAP dans Azure.

Pour créer et gérer des machines virtuelles de stockage de données supplémentaires dans Azure, vous devez utiliser les API. Cela est dû au fait que les API automatisent le processus de création des machines virtuelles de stockage et de configuration des interfaces réseau requises. Lors de la création des machines virtuelles de stockage, la console NetApp configure les services LIF requis, ainsi qu'un LIF iSCSI requis pour les

communications SMB/CIFS sortantes à partir de la machine virtuelle de stockage.

Pour plus d'informations sur l'exécution des appels d'API Cloud Volumes ONTAP , reportez-vous à "[Votre premier appel d'API](#)".

### Nombre de machines virtuelles de stockage prises en charge

À partir de Cloud Volumes ONTAP 9.9.0, en fonction de votre licence, plusieurs machines virtuelles de stockage sont prises en charge avec des configurations spécifiques. Reportez-vous à la "[Notes de version de Cloud Volumes ONTAP](#)" pour vérifier le nombre de machines virtuelles de stockage prises en charge pour votre version de Cloud Volumes ONTAP.

Toutes les versions de Cloud Volumes ONTAP antérieures à la version 9.9.0 prennent en charge une machine virtuelle de stockage de service de données et une machine virtuelle de stockage de destination utilisée pour la reprise après sinistre. Vous pouvez activer la machine virtuelle de stockage de destination pour l'accès aux données en cas de panne sur la machine virtuelle de stockage source.

### Créer une machine virtuelle de stockage

En fonction de votre configuration et de votre type de licence, vous pouvez créer plusieurs machines virtuelles de stockage sur un système à nœud unique ou dans une configuration haute disponibilité (HA) à l'aide des API de la console NetApp .

#### À propos de cette tâche

Lorsque vous créez des machines virtuelles de stockage à l'aide des API, en plus de configurer les interfaces réseau requises, la console modifie également les `default-data-files` politiques sur les machines virtuelles de stockage de données en supprimant les services suivants du LIF de données NAS et en les ajoutant au LIF de données iSCSI utilisé pour les connexions de gestion sortantes :

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

#### Avant de commencer

L'agent de console nécessite des autorisations spécifiques pour créer des machines virtuelles de stockage pour Cloud Volumes ONTAP. Les autorisations requises sont incluses dans "[les politiques fournies par NetApp](#)".

#### Système à nœud unique

Utilisez l'appel d'API suivant pour créer une machine virtuelle de stockage sur un système à nœud unique.

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{ "svmName": "myNewSvm1"
  "svmPassword": "optional, the API takes the cluster password if not
provided"
  "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

## paire HA

Utilisez l'appel d'API suivant pour créer une machine virtuelle de stockage sur une paire HA :

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
  "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

## Gérer les machines virtuelles de stockage sur des systèmes à nœud unique et des paires HA

À l'aide des API, vous pouvez renommer et supprimer des machines virtuelles de stockage dans les configurations à nœud unique et HA.

### Avant de commencer

L'agent de console nécessite des autorisations spécifiques pour gérer les machines virtuelles de stockage pour Cloud Volumes ONTAP. Les autorisations requises sont incluses dans ["les politiques fournies par NetApp"](#) .

### Renommer une machine virtuelle de stockage

Pour renommer une machine virtuelle de stockage, vous devez fournir les noms de la machine virtuelle de stockage existante et de la nouvelle machine virtuelle de stockage comme paramètres.

### Étapes

- Utilisez l'appel d'API suivant pour renommer une machine virtuelle de stockage sur un système à nœud unique :

```
PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

- Utilisez l'appel d'API suivant pour renommer une machine virtuelle de stockage sur une paire HA :

```
PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

### Supprimer une machine virtuelle de stockage

Dans une configuration à nœud unique ou HA, vous pouvez supprimer une machine virtuelle de stockage si elle ne possède aucun volume actif.

#### Étapes

- Utilisez l'appel d'API suivant pour supprimer une machine virtuelle de stockage sur un système à nœud unique :

```
DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Utilisez l'appel d'API suivant pour supprimer une machine virtuelle de stockage sur une paire HA :

```
DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

#### Informations connexes

- ["Préparez-vous à utiliser l'API"](#)
- ["Flux de travail Cloud Volumes ONTAP"](#)
- ["Obtenir les identifiants requis"](#)
- ["Utiliser les API REST pour la console NetApp"](#)

## Gérer les machines virtuelles de stockage de données pour Cloud Volumes ONTAP dans Google Cloud

Une machine virtuelle de stockage est une machine virtuelle exécutée dans ONTAP qui fournit des services de stockage et de données à vos clients. Vous connaissez peut-être cela sous le nom de *SVM* ou *vserver*. Cloud Volumes ONTAP est configuré avec une machine virtuelle de stockage par défaut, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

Pour créer et gérer des machines virtuelles de stockage de données supplémentaires dans Google Cloud, vous devez utiliser les API. Cela est dû au fait que les API automatisent le processus de création des machines virtuelles de stockage et de configuration des interfaces réseau requises. Lors de la création des machines virtuelles de stockage, la console NetApp configure les services LIF requis, ainsi qu'un LIF iSCSI requis pour les communications SMB/CIFS sortantes à partir de la machine virtuelle de stockage.

Pour plus d'informations sur l'exécution des appels d'API Cloud Volumes ONTAP , reportez-vous à ["Votre](#)

[premier appel d'API](#) .

## Nombre de machines virtuelles de stockage prises en charge

À partir de Cloud Volumes ONTAP 9.11.1, en fonction de votre licence, plusieurs machines virtuelles de stockage sont prises en charge avec des configurations spécifiques. Reportez-vous à la "[Notes de version de Cloud Volumes ONTAP](#)" pour vérifier le nombre de machines virtuelles de stockage prises en charge pour votre version de Cloud Volumes ONTAP.

Toutes les versions de Cloud Volumes ONTAP antérieures à la version 9.11.1 prennent en charge une machine virtuelle de stockage de service de données et une machine virtuelle de stockage de destination utilisée pour la reprise après sinistre. Vous pouvez activer la machine virtuelle de stockage de destination pour l'accès aux données en cas de panne sur la machine virtuelle de stockage source.

## Créer une machine virtuelle de stockage

En fonction de votre configuration et de votre type de licence, vous pouvez créer plusieurs machines virtuelles de stockage sur un système à nœud unique ou dans une configuration haute disponibilité (HA) à l'aide des API.

### À propos de cette tâche

Lorsque vous créez des machines virtuelles de stockage à l'aide des API, en plus de configurer les interfaces réseau requises, la console modifie également les `default-data-files` politiques sur les machines virtuelles de stockage de données en supprimant les services suivants du LIF de données NAS et en les ajoutant au LIF de données iSCSI utilisé pour les connexions de gestion sortantes :

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

### Avant de commencer

L'agent de console nécessite des autorisations spécifiques pour créer des machines virtuelles de stockage pour les paires Cloud Volumes ONTAP HA. Les autorisations requises sont incluses dans "[les politiques fournies par NetApp](#)" .

### Systeme à nœud unique

Utilisez l'appel d'API suivant pour créer une machine virtuelle de stockage sur un système à nœud unique.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
  "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

## paire HA

Utilisez l'appel d'API suivant pour créer une machine virtuelle de stockage sur une paire HA :

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

Incluez les paramètres suivants dans le corps de la requête :

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

## Gérer les machines virtuelles de stockage

À l'aide des API, vous pouvez renommer et supprimer des machines virtuelles de stockage dans les configurations à nœud unique et HA.

### Avant de commencer

L'agent de console nécessite des autorisations spécifiques pour gérer les machines virtuelles de stockage pour les paires Cloud Volumes ONTAP HA. Les autorisations requises sont incluses dans ["les politiques fournies par NetApp"](#) .

### Renommer une machine virtuelle de stockage

Pour renommer une machine virtuelle de stockage, vous devez fournir les noms de la machine virtuelle de stockage existante et de la nouvelle machine virtuelle de stockage comme paramètres.

### Étapes

- Utilisez l'appel d'API suivant pour renommer une machine virtuelle de stockage sur un système à nœud unique :

```
PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

- Utilisez l'appel d'API suivant pour renommer une machine virtuelle de stockage sur une paire HA :

```
PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm
```

Incluez les paramètres suivants dans le corps de la requête :

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

### Supprimer une machine virtuelle de stockage

Dans une configuration à nœud unique ou HA, vous pouvez supprimer une machine virtuelle de stockage si elle ne possède aucun volume actif.

#### Étapes

- Utilisez l'appel d'API suivant pour supprimer une machine virtuelle de stockage sur un système à nœud unique :

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Utilisez l'appel d'API suivant pour supprimer une machine virtuelle de stockage sur une paire HA :

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

#### Informations connexes

- ["Préparez-vous à utiliser l'API"](#)
- ["Flux de travail Cloud Volumes ONTAP"](#)
- ["Obtenir les identifiants requis"](#)
- ["Utiliser les API REST pour la console NetApp"](#)

## Configurer la reprise après sinistre des machines virtuelles de stockage pour Cloud Volumes ONTAP

La console NetApp n'offre pas de prise en charge de la configuration ou de l'orchestration pour la reprise après sinistre des machines virtuelles de stockage (SVM). Pour effectuer ces tâches, utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP .

Si vous configurez la réplication SnapMirror SVM entre deux systèmes Cloud Volumes ONTAP , la réplication doit être effectuée entre deux systèmes à paires HA ou deux systèmes à nœud unique. Vous ne pouvez pas configurer la réplication SnapMirror SVM entre une paire HA et un système à nœud unique.

Reportez-vous aux documents suivants pour obtenir les instructions de l'interface de ligne de commande ONTAP .

- ["Guide de préparation express à la reprise après sinistre SVM"](#)

- ["Guide de récupération express après sinistre SVM"](#)

## Sécurité et cryptage des données

### Chiffrer les volumes sur Cloud Volumes ONTAP avec les solutions de chiffrement 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 des volumes conforme à la norme FIPS 140-2. ["En savoir plus sur ces solutions de cryptage"](#) .

NVE et NAE sont tous deux pris en charge avec un gestionnaire de clés externe.

```
] fin si::aws[] ifdef::azure[] fin si::azure[] ifdef::gcp[] fin si::gcp[] ifdef::aws[] fin si::aws[] ifdef::azure[] fin
si::azure[] ifdef::gcp[] fin si::gcp[]
```

### Gérer les clés de chiffrement Cloud Volumes ONTAP avec AWS Key Management Service

Vous pouvez utiliser ["Service de gestion des clés \(KMS\) d'AWS"](#) pour protéger vos clés de chiffrement ONTAP dans une application déployée sur AWS.

La gestion des clés avec AWS KMS peut être activée avec l'interface de ligne de commande ou l'API REST ONTAP .

Lorsque vous utilisez le KMS, sachez que par défaut, le LIF d'un SVM de données est utilisé pour communiquer avec le point de terminaison de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification d'AWS. Si le réseau du cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

#### Avant de commencer

- Cloud Volumes ONTAP doit exécuter la version 9.12.0 ou ultérieure
- Vous devez avoir installé la licence Volume Encryption (VE) et
- Vous devez avoir installé la licence Multi-tenant Encryption Key Management (MTEKM).
- Vous devez être un administrateur de cluster ou de SVM
- Vous devez avoir un abonnement AWS actif



Vous ne pouvez configurer que des clés pour un SVM de données.

#### Configuration

##### AWS

1. Vous devez créer un ["accorder"](#) pour la clé AWS KMS qui sera utilisée par le rôle IAM gérant le chiffrement. Le rôle IAM doit inclure une politique qui autorise les opérations suivantes :
  - DescribeKey
  - Encrypt

- `Decrypt` Pour créer une subvention, reportez-vous à "[Documentation AWS](#)".
2. "[Ajoutez une politique au rôle IAM approprié.](#)" La politique devrait soutenir la `DescribeKey`, `Encrypt`, et `Decrypt` opérations.

### Cloud Volumes ONTAP

1. Basculez vers votre environnement Cloud Volumes ONTAP .
2. Passer au niveau de privilège avancé :  
`set -privilege advanced`
3. Activer le gestionnaire de clés AWS :  
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Lorsque vous y êtes invité, entrez la clé secrète.
5. Confirmez que AWS KMS a été correctement configuré :  
`security key-manager external aws show -vserver svm_name`

## Gérer les clés de chiffrement Cloud Volumes ONTAP avec Azure Key Vault

Vous pouvez utiliser Azure Key Vault (AKV) pour protéger vos clés de chiffrement ONTAP dans une application déployée par Azure. Reportez-vous à la "[Documentation Microsoft](#)".

AKV peut être utilisé pour protéger les clés NetApp Volume Encryption (NVE) uniquement pour les SVM de données. Pour plus d'informations, reportez-vous à la "[Documentation ONTAP](#)".

La gestion des clés avec AKV peut être activée avec la CLI ou l'API REST ONTAP .

Lorsque vous utilisez AKV, sachez que par défaut, un LIF SVM de données est utilisé pour communiquer avec le point de terminaison 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 du cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

### Avant de commencer

- 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 )
- Vous devez disposer d'une licence de gestion des clés de chiffrement multi-locataires (`MT_EK_MGMT`)
- Vous devez être un administrateur de cluster ou de SVM
- Un abonnement Azure actif

### Limites

- AKV ne peut être configuré que sur un SVM de données
- NAE ne peut pas être utilisé avec AKV. NAE nécessite un serveur KMIP pris en charge en externe.
- Les nœuds Cloud Volumes ONTAP interrogent AKV toutes les 15 minutes pour confirmer l'accessibilité et la disponibilité des clés. Cette période d'interrogation n'est pas configurable et après quatre échecs consécutifs dans la tentative d'interrogation (totalisant 1 heure), les volumes sont mis hors ligne.

## Processus de configuration

Les étapes décrites expliquent comment enregistrer votre configuration Cloud Volumes ONTAP auprès d'Azure et comment créer un coffre de clés Azure et des clés. Si vous avez déjà effectué ces étapes, assurez-vous d'avoir les paramètres de configuration corrects, en particulier dans [Créer un coffre de clés Azure](#) , puis passez à [Configuration de Cloud Volumes ONTAP](#) .

- [Enregistrement d'application Azure](#)
- [Créer un secret client Azure](#)
- [Créer un coffre de clés Azure](#)
- [Créer une clé de cryptage](#)
- [Créer un point de terminaison Azure Active Directory \(HA uniquement\)](#)
- [Configuration de Cloud Volumes ONTAP](#)

### Enregistrement d'application Azure

1. Vous devez d'abord enregistrer votre application dans l'abonnement Azure que vous souhaitez que Cloud Volumes ONTAP utilise pour accéder à Azure Key Vault. Dans le portail Azure, sélectionnez **Inscriptions d'applications**.
2. Sélectionnez **Nouvelle inscription**.
3. Donnez un nom à 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 **S'inscrire**.
4. Dans la fenêtre Présentation d'Azure, sélectionnez l'application que vous avez enregistrée. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)** dans un emplacement sécurisé. Ils seront exigés plus tard dans le processus d'inscription.

### Créer un secret client Azure

1. Dans le portail Azure pour l'inscription de votre application Azure Key Vault, sélectionnez le volet **Certificats et secrets**.
2. Sélectionnez **Nouveau secret client**. Saisissez un nom significatif pour votre secret client. NetApp recommande une période d'expiration de 24 mois ; cependant, vos politiques de gouvernance cloud spécifiques peuvent nécessiter un paramètre différent.
3. Cliquez sur **Ajouter** pour créer le secret client. Copiez la chaîne secrète répertoriée dans la colonne **Valeur** et stockez-la dans un endroit sûr pour une utilisation ultérieure. [Configuration de Cloud Volumes ONTAP](#) . La valeur secrète ne sera plus affichée après avoir quitté la page.

### Créer un coffre de clés Azure

1. Si vous disposez d'un Azure Key Vault existant, vous pouvez le connecter à votre configuration Cloud Volumes ONTAP ; toutefois, vous devez adapter les stratégies d'accès aux paramètres de ce processus.
2. Dans le portail Azure, accédez à la section **Key Vaults**.
3. Cliquez sur **+Créer** et saisissez les informations requises, notamment le groupe de ressources, la région et le niveau de tarification. De plus, saisissez le nombre de jours pendant lesquels conserver les coffres supprimés et sélectionnez **Activer la protection contre la purge** sur le coffre de clés.
4. Sélectionnez **Suivant** pour choisir une politique d'accès.
5. Sélectionnez les options suivantes :
  - a. Sous **Configuration d'accès**, sélectionnez la **Stratégie d'accès au coffre-fort**.
  - b. Sous **Accès aux ressources**, sélectionnez **Azure Disk Encryption pour le chiffrement du volume**.

6. Sélectionnez **+Créer** pour ajouter une politique d'accès.
7. Sous **Configurer à partir d'un modèle**, cliquez sur le menu déroulant, puis sélectionnez le modèle **Gestion des clés, des secrets et des certificats**.
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 devriez avoir :
  - **Autorisations clés** : 20 sélectionnées
  - **Autorisations secrètes** : 8 sélectionnées
  - **Autorisations de certificat** : 16 sélectionnés

# Create an access policy



- 1 **Permissions**   2 Principal   3 Application (optional)   4 Review + create

Configure from a template

Key, Secret, & Certificate Management ▼

## Key permissions

### Key Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore

### Cryptographic Operations

- Select all
- Decrypt
- Encrypt
- Unwrap Key
- Wrap Key
- Verify
- Sign

### Privileged Key Operations

- Select all
- Purge
- Release

### Rotation Policy Operations

- Select all
- Rotate
- Get Rotation Policy
- Set Rotation Policy

## Secret permissions

### Secret Management Operations

- Select all
- Get
- List
- Set
- Delete
- Recover
- Backup
- Restore

### Privileged Secret Operations

- Select all
- Purge

## Certificate permissions

### Certificate Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore
- Manage Contacts
- Manage Certificate Authorities
- Get Certificate Authorities
- List Certificate Authorities
- Set Certificate Authorities
- Delete Certificate Authorities

### Privileged Certificate Operations

- Select all
- Purge

Previous

Next

9. Cliquez sur **Suivant** pour sélectionner l'application enregistrée Azure **Principale** que vous avez créée dans [Enregistrement d'application Azure](#) . Sélectionnez **Suivant**.



Un seul principal peut être attribué par politique.

## Create an access policy

1 Permissions **2 Principal** 3 Application (optional) 4 Review + create

Only 1 principal can be assigned per access policy.  
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

**Selected item**

No item selected

Previous **Next**

10. Cliquez sur **Suivant** deux fois jusqu'à arriver à **Vérifier et créer**. Ensuite, cliquez sur **Créer**.
11. Sélectionnez **Suivant** pour passer aux options **Réseau**.
12. Choisissez la méthode d'accès au réseau appropriée ou sélectionnez **Tous les réseaux** et **Réviser + Créer** pour créer le coffre-fort de clés. (La méthode d'accès au réseau peut être prescrite par une politique de gouvernance ou par votre équipe de sécurité cloud d'entreprise.)
13. Enregistrez l'URI du coffre de clés : dans le coffre de clés que vous avez créé, accédez au menu Présentation et copiez l'**URI du coffre** dans la colonne de droite. Vous en aurez besoin pour une étape ultérieure.

### Créer une clé de cryptage

1. Dans le menu du Key Vault que vous avez créé pour Cloud Volumes ONTAP, accédez à l'option **Clés**.
2. Sélectionnez **Générer/importer** pour créer une nouvelle clé.
3. Laissez l'option par défaut définie 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 chiffrement.
6. Revenez au menu **Clés** et sélectionnez la clé que vous venez de créer.
7. Sélectionnez l'ID de clé sous **Version actuelle** pour afficher les propriétés de la clé.
8. Localisez le champ **Identifiant de clé**. Copiez l'URI jusqu'à la chaîne hexadécimale, mais sans l'inclure.

#### **Créer un point de terminaison Azure Active Directory (HA uniquement)**

1. Ce processus n'est requis que si vous configurez Azure Key Vault pour un système HA Cloud Volumes ONTAP .
2. Dans le portail Azure, accédez à **Réseaux virtuels**.
3. Sélectionnez le réseau virtuel sur lequel vous avez déployé le système Cloud Volumes ONTAP et sélectionnez le menu **Sous-réseaux** sur le côté gauche de la page.
4. Sélectionnez le nom du sous-réseau pour votre déploiement Cloud Volumes ONTAP dans la liste.
5. Accédez à la rubrique **Points de terminaison de service**. Dans le menu déroulant, sélectionnez les éléments suivants :
  - **Microsoft.AzureActiveDirectory**
  - **Microsoft.KeyVault**
  - **Microsoft.Storage** (facultatif)

**SERVICE ENDPOINTS**

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

**SUBNET DELEGATION**

Delegate subnet to a service ⓘ

None

**NETWORK POLICY FOR PRIVATE ENDPOINTS**

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

**Save** **Cancel**

6. Sélectionnez **Enregistrer** pour capturer vos paramètres.

### Configuration de Cloud Volumes ONTAP

1. Connectez-vous au LIF de gestion de cluster avec votre client SSH préféré.
2. Entrez le mode privilège avancé dans ONTAP:

```
set advanced -con off
```

3. Identifiez le SVM de données souhaité et vérifiez 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 la SVM de données qui pointe vers le DNS Azure, le DNS privé ou le serveur local. Cela doit correspondre à l'entrée pour le SVM d'administration du cluster :

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. Vérifiez que le service DNS a été créé pour le SVM de données :

```
vserver services name-service dns show
```

4. Activez Azure Key Vault 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 key_vault_URI -key-id  
full_key_URI
```



Le `_full_key_URI` la valeur doit utiliser le `<https:// <key vault host name>/keys/<key label>` format.

5. Une fois Azure Key Vault activé avec succès, entrez le `client secret value` lorsque vous y êtes invité.

6. Vérifiez l'état du gestionnaire de clés :

```
security key-manager external azure check
```

Le résultat ressemblera à :

```
::*> 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` le statut n'est pas `OK` , le SVM ne peut pas atteindre le service Azure Key Vault avec toute la connectivité et les autorisations requises. Assurez-vous que vos stratégies réseau et votre routage Azure n'empêchent pas votre réseau virtuel privé d'atteindre le point de terminaison public

Azure Key Vault. Si tel est le cas, envisagez d'utiliser un point de terminaison privé Azure pour accéder au coffre de clés à partir du réseau virtuel. Vous devrez peut-être également ajouter une entrée d'hôtes statiques sur votre SVM pour résoudre l'adresse IP privée de votre point de terminaison.

Le `kms_wrapped_key_status` fera un rapport UNKNOWN lors de la configuration initiale. Son statut changera en OK après que le premier volume soit crypté.

7. FACULTATIF : créez un volume de test pour vérifier la fonctionnalité de NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

Si configuré correctement, Cloud Volumes ONTAP créera automatiquement le volume et activera le chiffrement du volume.

8. Confirmez que le volume a été créé et chiffré correctement. Si c'est le cas, le `-is-encrypted` le paramètre s'affichera comme `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

9. Facultatif : si vous souhaitez mettre à jour les informations d'identification sur le certificat d'authentification Azure Key Vault, utilisez la commande suivante :

```
security key-manager external azure update-credentials -vserver v1
-authentication-method certificate
```

#### Liens connexes

- ["Configurer Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans Azure"](#)
- ["Documentation Microsoft Azure : À propos d'Azure Key Vault"](#)
- ["Guide de référence des commandes ONTAP"](#)

## Gérer les clés de chiffrement Cloud Volumes ONTAP avec Google Cloud KMS

Vous pouvez utiliser ["Service de gestion des clés de Google Cloud Platform \(Cloud KMS\)"](#) pour protéger vos clés de chiffrement Cloud Volumes ONTAP dans une application déployée sur Google Cloud Platform.

La gestion des clés avec Cloud KMS peut être activée avec l'interface de ligne de commande ONTAP ou l'API REST ONTAP .

Lorsque vous utilisez Cloud KMS, sachez que par défaut, le LIF d'un SVM de données est utilisé pour communiquer avec le point de terminaison 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 du cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

#### Avant de commencer

- Votre système doit exécuter Cloud Volumes ONTAP 9.10.1 ou une version ultérieure
- Vous devez utiliser un SVM de données. Cloud KMS ne peut être configuré que sur un SVM de données.
- Vous devez être un administrateur de cluster ou de SVM
- La licence Volume Encryption (VE) doit être installée sur le SVM
- À partir de Cloud Volumes ONTAP 9.12.1 GA, la licence multi-locataire Encryption Key Management (MTEKM) doit également être installée

- Un abonnement actif à Google Cloud Platform est requis

## Configuration

### Google Cloud

1. Dans votre environnement Google Cloud, "[créer un trousseau de clés et une clé GCP symétriques](#)".
2. Attribuez un rôle personnalisé à la clé Cloud KMS et au compte de service Cloud Volumes ONTAP.
  - a. Créer le rôle personnalisé :

```
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.locations.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

- b. Attribuez le rôle personnalisé que vous avez créé :

```
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
```



Si vous utilisez Cloud Volumes ONTAP 9.13.0 ou une version ultérieure, vous n'avez pas besoin de créer un rôle personnalisé. Vous pouvez attribuer le prédéfini[cloudkms.cryptoKeyEncrypterDecrypter ^] rôle.

3. 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 au LIF de gestion de cluster avec votre client SSH préféré.
2. Passer au niveau de privilège avancé :

```
set -privilege advanced
```
3. Créez un DNS pour les données SVM.

```
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, saisissez la clé JSON du 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 : créer un volume pour tester le chiffrement `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

## Dépannage

Si vous avez besoin de résoudre un problème, vous pouvez suivre les journaux bruts de l'API REST dans les deux dernières étapes ci-dessus :

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

## Activer les solutions de protection contre les ransomwares NetApp pour Cloud Volumes ONTAP

Les attaques de ransomware peuvent coûter du temps, des ressources et de la réputation à une entreprise. La console NetApp vous permet de mettre en œuvre deux solutions NetApp contre les ransomwares : la protection contre les extensions de fichiers de ransomware courantes et la protection autonome contre les ransomwares (ARP). Ces solutions fournissent des outils efficaces de visibilité, de détection et de correction.

### Protection contre les extensions de fichiers courantes de ransomware

Disponible sur la console, le paramètre Protection contre les ransomwares vous permet d'utiliser la fonctionnalité ONTAP FPolicy pour vous protéger contre les types d'extensions de fichiers de ransomwares courants.

### Étapes

1. Sur la page **Systemes**, double-cliquez sur le nom du système Cloud Volumes ONTAP que vous configurez pour utiliser la protection contre les ransomwares.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Protection contre les ransomwares**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. Mettre en œuvre la solution NetApp contre les ransomwares :

- a. Cliquez sur **Activer la stratégie de snapshot**, si vous avez des volumes pour lesquels aucune stratégie de snapshot n'est activée.

La technologie NetApp Snapshot fournit la meilleure solution du secteur pour la correction des ransomwares. La clé d'une récupération réussie est la restauration à partir de sauvegardes non infectées. Les copies instantanées sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également fournir la granularité nécessaire pour créer des images d'une copie de fichier unique ou une solution complète de reprise après sinistre.

- b. Cliquez sur **Activer FPolicy** pour activer la solution FPolicy d'ONTAP, qui peut bloquer les opérations sur les fichiers en fonction de l'extension d'un fichier.

Cette solution préventive améliore la protection contre les attaques de ransomware en bloquant les types de fichiers de ransomware courants.

La portée FPolicy par défaut bloque les fichiers qui ont les extensions suivantes :

micro, chiffré, verrouillé, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, bien, MDR !, OMG !, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



Cette étendue est créée lorsque vous activez FPolicy sur Cloud Volumes ONTAP. La liste est basée sur les types de fichiers de ransomware courants. Vous pouvez personnaliser les extensions de fichiers bloquées à l'aide des commandes `vserver fpolicy policy scope` 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

## Protection autonome contre les ransomwares

Cloud Volumes ONTAP prend en charge la fonctionnalité Autonomous Ransomware Protection (ARP), qui effectue des analyses sur les charges de travail pour détecter et avertir de manière proactive des activités anormales pouvant indiquer une attaque de ransomware.

Indépendamment des protections d'extension de fichier fournies par le "[paramètre de protection contre les ransomwares](#)", la fonctionnalité ARP utilise l'analyse de la charge de travail pour alerter l'utilisateur sur les attaques potentielles en fonction d'une « activité anormale » détectée. Le paramètre de protection contre les ransomwares et la fonction ARP peuvent être utilisés conjointement pour une protection complète contre les ransomwares.

La fonctionnalité ARP est disponible pour une utilisation avec les abonnements BYOL (Bring Your Own License) et Marketplace pour vos licences sans frais supplémentaires.

Les volumes compatibles ARP ont un état désigné « Mode d'apprentissage » ou « Actif ».

La configuration d'ARP pour les volumes est effectuée via ONTAP System Manager et ONTAP CLI.

Pour plus d'informations sur la façon d'activer ARP avec ONTAP System Manager et l'ONTAP CLI, reportez-vous à la "[Documentation ONTAP : Activer la protection autonome contre les ransomwares](#)".

## Autonomous Ransomware Protection

0 TiB

Protected Capacity

100 TiB

Precommitted capacity

0 TiB

PAYGO

BYOL

100 TiB

Marketplace Contracts

0 TiB

## Créer des copies instantanées inviolables des fichiers WORM sur Cloud Volumes ONTAP

Vous pouvez créer des copies Snapshot inviolables de fichiers WORM (écriture unique, lecture multiple) sur un système Cloud Volumes ONTAP et conserver les snapshots sous une forme non modifiée pendant une période de conservation spécifique. Cette fonctionnalité est alimentée par la technologie SnapLock et fournit une couche supplémentaire de protection des données et de conformité.

### Avant de commencer

Assurez-vous que le volume que vous utilisez pour créer des copies Snapshot est un volume SnapLock . Pour plus d'informations sur l'activation de la protection SnapLock sur les volumes, reportez-vous à la ["Documentation ONTAP : Configurer SnapLock"](#) .

### Étapes

1. Créez des copies instantanées à partir du volume SnapLock . Pour plus d'informations sur la création de copies instantanées à l'aide de l'interface de ligne de commande ou du Gestionnaire système, reportez-vous au ["Documentation ONTAP : Présentation de la gestion des copies Snapshot locales"](#) .

Les copies Snapshot héritent des propriétés WORM du volume, ce qui les rend inviolables. La technologie SnapLock sous-jacente garantit qu'un instantané reste protégé contre toute modification ou suppression jusqu'à ce que la période de conservation spécifiée soit écoulée.

2. Vous pouvez modifier la période de conservation s'il est nécessaire de modifier ces instantanés. Pour plus d'informations, reportez-vous à la ["Documentation ONTAP : définir la durée de rétention"](#) .



Même si une copie Snapshot est protégée pendant une période de conservation spécifique, le volume source peut être supprimé par un administrateur de cluster, car le stockage WORM dans Cloud Volumes ONTAP fonctionne sous un modèle « administrateur de stockage approuvé ». De plus, un administrateur cloud de confiance peut supprimer les données WORM en agissant sur les ressources de stockage cloud.

# Administration du système

## Mettre à niveau le logiciel Cloud Volumes ONTAP

Mettez à niveau Cloud Volumes ONTAP à partir de la console NetApp pour accéder aux dernières nouvelles fonctionnalités et améliorations. Vous devez préparer les systèmes Cloud Volumes ONTAP avant de mettre à niveau le logiciel.

### Présentation de la mise à niveau

Vous devez tenir compte des éléments suivants avant de démarrer le processus de mise à niveau de Cloud Volumes ONTAP .

### Mise à niveau à partir de la console uniquement

Vous ne devez pas mettre à niveau Cloud Volumes ONTAP à l'aide ONTAP System Manager ou de l'interface de ligne de commande ONTAP , mais uniquement de la console. Dans le cas contraire, cela pourrait avoir un impact sur la stabilité du système.

### Comment mettre à niveau

La console propose deux manières de mettre à niveau Cloud Volumes ONTAP:

- En suivant les notifications de mise à niveau qui apparaissent dans le système
- En plaçant l'image de mise à niveau à un emplacement HTTPS, puis en fournissant à la console l'URL

### Chemins de mise à niveau pris en charge

La version de Cloud Volumes ONTAP vers laquelle vous pouvez effectuer une mise à niveau dépend de la version de Cloud Volumes ONTAP que vous exécutez actuellement.

Version actuelle	Versions vers lesquelles vous pouvez directement mettre à niveau
9.16.1 (pour Azure et Google Cloud uniquement)	9.17.1 (pour Azure et Google Cloud uniquement)
9.15.1	9.16.1 (pour Azure et Google Cloud uniquement)
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1

Version actuelle	Versions vers lesquelles vous pouvez directement mettre à niveau
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 qui s'affichent dans un système, la console vous invitera à effectuer une mise à niveau vers une version qui suit ces chemins de mise à niveau pris en charge.
- Si vous effectuez une mise à niveau en plaçant une image de mise à niveau dans un emplacement HTTPS, assurez-vous de suivre ces chemins de mise à niveau pris en charge.
- Dans certains cas, vous devrez peut-être effectuer plusieurs mises à niveau pour atteindre votre version cible.

Par exemple, si vous utilisez la version 9.8 et que vous souhaitez effectuer une mise à niveau vers la version 9.10.1, vous devez d'abord effectuer une mise à niveau vers la version 9.9.1, puis vers la version 9.10.1.

#### Versions de correctifs

À partir de janvier 2024, les mises à niveau de correctifs ne sont disponibles que s'il existe une version de

correctif pour les trois dernières versions de Cloud Volumes ONTAP. Des versions de correctifs sont parfois disponibles pour le déploiement, lorsque la version RC ou GA n'est pas disponible pour le déploiement.

Nous utilisons la dernière version GA pour déterminer les trois dernières versions à afficher dans la console. Par exemple, si la version GA actuelle est 9.13.1, les correctifs pour 9.11.1-9.13.1 apparaissent dans la console. Si vous souhaitez effectuer une mise à niveau vers une version de correctif pour les versions 9.11.1 ou inférieures, vous devrez utiliser la procédure de mise à niveau manuelle en [téléchargement de l'image ONTAP](#).

En règle générale, pour les versions de correctifs (P), vous pouvez effectuer une mise à niveau d'une version vers n'importe quelle version P de la version actuelle que vous exécutez ou de la version suivante.

Voici quelques exemples :

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

### Retour ou rétrogradation

La restauration ou la rétrogradation de Cloud Volumes ONTAP vers une version précédente n'est pas prise en charge.

### Enregistrement du support

Cloud Volumes ONTAP doit être enregistré auprès du support NetApp pour pouvoir mettre à niveau le logiciel à l'aide de l'une des méthodes décrites sur cette page. Ceci s'applique à la fois au paiement à l'utilisation (PAYGO) et à l'apportez votre propre permis (BYOL). Vous aurez besoin de "[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 logicielle qui apparaissent dans la console 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

La console met également à jour l'instance du médiateur selon les besoins pendant le processus de mise à niveau de Cloud Volumes ONTAP.

### Mises à niveau dans AWS avec les types d'instances EC2 c4, m4 et r4

Cloud Volumes ONTAP ne prend plus en charge les types d'instances EC2 c4, m4 et r4. Vous pouvez mettre à niveau les déploiements existants vers les versions Cloud Volumes ONTAP 9.8 à 9.12.1 avec ces types d'instances. Avant de procéder à la mise à niveau, nous vous recommandons de [changer le type d'instance](#). Si vous ne pouvez pas modifier le type d'instance, vous devez [activer la mise en réseau améliorée](#) avant de procéder à la mise à niveau. Lisez les sections suivantes pour en savoir plus sur la modification du type d'instance et l'activation de la mise en réseau améliorée.

Dans Cloud Volumes ONTAP exécutant les versions 9.13.0 et supérieures, vous ne pouvez pas effectuer de mise à niveau avec les types d'instances EC2 c4, m4 et r4. Dans ce cas, vous devez réduire le nombre de disques, puis [changer le type d'instance](#) ou déployez une nouvelle configuration de paire HA avec les types d'instances EC2 c5, m5 et r5 et migrez les données.

## Modifier le type d'instance

Les types d'instances EC2 c4, m4 et r4 autorisent plus de disques par nœud que les types d'instances EC2 c5, m5 et r5. Si le nombre de disques par nœud pour l'instance EC2 c4, m4 ou r4 que vous exécutez est inférieur à l'allocation de disque maximale par nœud pour les instances c5, m5 et r5, vous pouvez modifier le type d'instance EC2 en c5, m5 ou r5.

["Vérifier les limites de disque et de hiérarchisation par instance EC2"](#) ["Modifier le type d'instance EC2 pour Cloud Volumes ONTAP"](#)

Si vous ne pouvez pas modifier le type d'instance, suivez les étapes décrites dans [Activer la mise en réseau améliorée](#).

## Activer la mise en réseau améliorée

Pour effectuer une mise à niveau vers les versions 9.8 et ultérieures de Cloud Volumes ONTAP, vous devez activer la *mise en réseau améliorée* sur le cluster exécutant le type d'instance c4, m4 ou r4. Pour activer ENA, reportez-vous à l'article de la base de connaissances ["Comment activer la mise en réseau améliorée comme SR-IOV ou ENA sur les instances AWS Cloud Volumes ONTAP"](#).

## Préparez-vous à la mise à niveau

Avant d'effectuer une mise à niveau, vous devez vérifier que vos systèmes sont prêts et apporter les modifications de configuration requises.

- [Prévoyez des temps d'arrêt](#)
- [Vérifiez que le retour automatique est toujours activé](#)
- [Suspendre les transferts SnapMirror](#)
- [Vérifiez que les agrégats sont en ligne](#)
- [Vérifiez que tous les LIF sont sur les ports d'origine](#)

### Prévoyez des temps d'arrêt

Lorsque vous mettez à niveau un système à nœud unique, le processus de mise à niveau met le système hors ligne pendant 25 minutes maximum, pendant lesquelles les E/S sont interrompues.

Dans de nombreux cas, la mise à niveau d'une paire HA est non perturbatrice et les E/S sont ininterrompues. Au cours de ce processus de mise à niveau non perturbateur, chaque nœud est mis à niveau en tandem pour continuer à fournir des E/S aux clients.

Les protocoles orientés session peuvent entraîner des effets indésirables sur les clients et les applications dans certains domaines lors des mises à niveau. Pour plus de détails, reportez-vous à la ["Documentation ONTAP"](#)

### Vérifiez que le retour automatique est toujours activé

La restitution automatique doit être activée sur une paire Cloud Volumes ONTAP HA (il s'agit du paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP : commandes de configuration du retour automatique"](#)

## Suspendre les transferts SnapMirror

Si un système Cloud Volumes ONTAP possède 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 échecs de SnapMirror . Vous devez suspendre les transferts depuis le système de destination.



Même si NetApp Backup and Recovery utilise une implémentation de SnapMirror pour créer des fichiers de sauvegarde (appelée SnapMirror Cloud), les sauvegardes n'ont pas besoin d'être suspendues lorsqu'un système est mis à niveau.

### À propos de cette tâche

Ces étapes décrivent comment utiliser ONTAP System Manager pour la version 9.3 et ultérieure.

#### Étapes

1. Connectez-vous au Gestionnaire système à partir du système de destination.

Vous pouvez vous connecter au Gestionnaire système en pointant votre navigateur Web vers l'adresse IP du LIF de gestion de cluster. Vous pouvez trouver l'adresse IP dans le système Cloud Volumes ONTAP .



L'ordinateur à partir duquel vous accédez à la console doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être vous connecter à la console à partir d'un hôte de saut qui se trouve dans le réseau de votre fournisseur de cloud.

2. Cliquez sur **Protection > Relations**.
3. Sélectionnez la relation et cliquez sur **Opérations > Mettre en pause**.

#### 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 s'ils ne le sont pas, vous devez les mettre en ligne.

### À propos de cette tâche

Ces étapes décrivent comment utiliser ONTAP System Manager pour la version 9.3 et ultérieure.

#### Étapes

1. Sur le système Cloud Volumes ONTAP , cliquez sur l'onglet **Agrégats**.
2. Sur la tuile d'agrégat requise, cliquez sur le bouton **...** icône, puis sélectionnez **Afficher les détails agrégés**.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	#####
Encryption Type	cloudEncrypted
Volumes	2

3. Si l'agrégat est hors ligne, utilisez ONTAP 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 > Statut > En ligne**.

#### Vérifiez que tous les LIF sont sur les ports d'origine

Avant de procéder à la mise à niveau, tous les LIF doivent être sur les ports d'origine. Reportez-vous à la documentation ONTAP pour "[vérifier que tous les LIF sont sur leurs ports d'attache](#)".

Si une erreur d'échec de mise à niveau se produit, consultez l'article de la base de connaissances (KB) "[Échec de la mise à niveau de Cloud Volumes ONTAP](#)".

#### Mettre à niveau Cloud Volumes ONTAP

La console 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 d'informations, consultez la section [Mise à niveau à partir des notifications de la console](#).

Une autre façon d'effectuer des mises à niveau logicielles est d'utiliser une image sur une URL externe. Cette option est utile si la console ne peut pas accéder au compartiment S3 pour mettre à niveau le logiciel ou si un correctif vous a été fourni. Pour plus d'informations, consultez la section [Mise à niveau à partir d'une image disponible à une URL](#).

#### Mise à niveau à partir des notifications de la console

La console affiche une notification dans les environnements de travail Cloud Volumes ONTAP lorsqu'une nouvelle version de Cloud Volumes ONTAP est disponible :



Avant de pouvoir mettre à niveau Cloud Volumes ONTAP via les notifications, vous devez disposer d'un compte sur le site de support NetApp.

Vous pouvez démarrer le processus de mise à niveau à partir de cette notification, qui automatise le processus en obtenant l'image logicielle à partir d'un bucket S3, en installant l'image, puis en redémarrant le système.

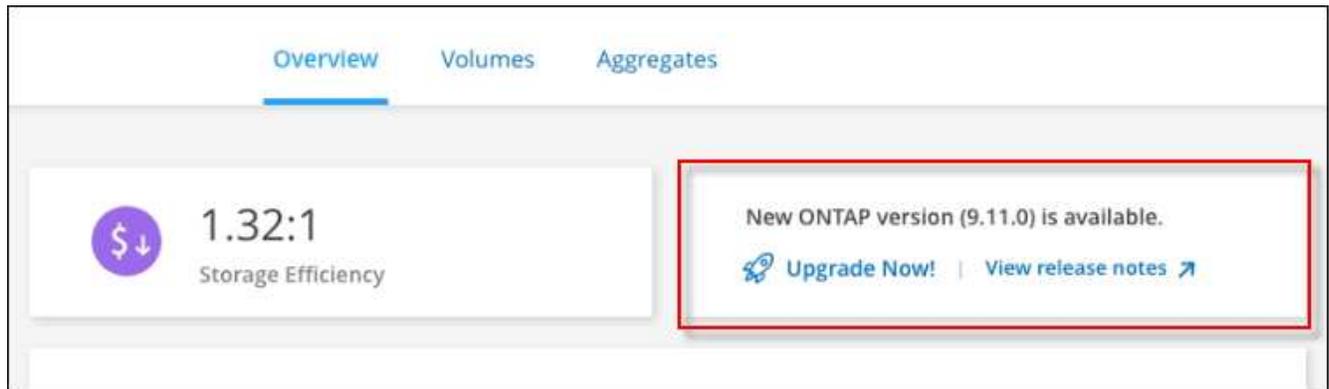
## Avant de commencer

Les opérations telles que la création de volumes ou d'agrégats ne doivent pas être en cours sur le système Cloud Volumes ONTAP .

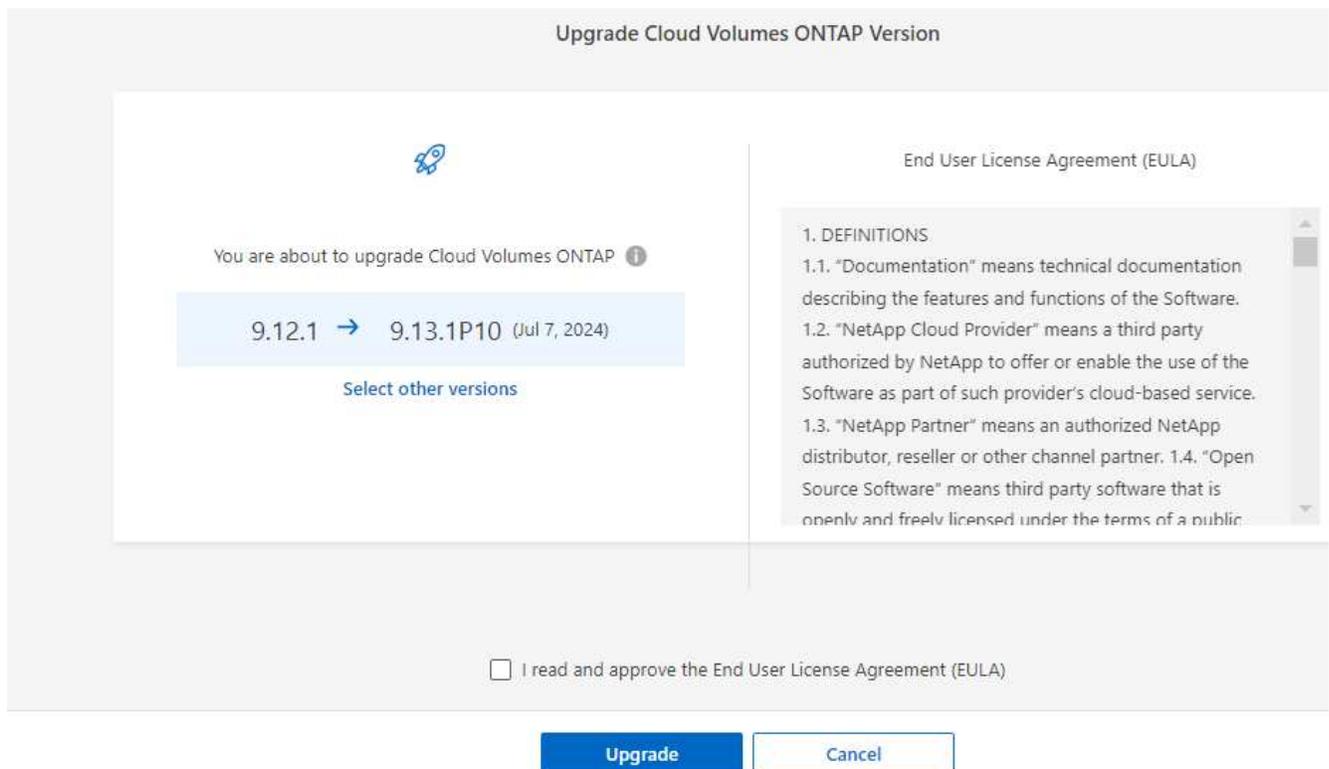
## Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sélectionnez un système Cloud Volumes ONTAP .

Une notification apparaît dans l'onglet Aperçu si une nouvelle version est disponible :



3. Si vous souhaitez mettre à niveau la version installée de Cloud Volumes ONTAP, cliquez sur **Mettre à niveau maintenant !** Par défaut, vous voyez la dernière version compatible pour la mise à niveau.



Si vous souhaitez passer à une autre version, cliquez sur **Sélectionner d'autres versions**. Vous voyez les dernières versions de Cloud Volumes ONTAP répertoriées qui sont également compatibles avec la version installée sur votre système. Par exemple, la version installée sur votre système est 9.12.1P3 et les versions compatibles suivantes sont disponibles :

- 9.12.1P4 à 9.12.1P14
  - 9.13.1 et 9.13.1P1 Vous voyez 9.13.1P1 comme version par défaut pour la mise à niveau, et 9.12.1P13, 9.13.1P14, 9.13.1 et 9.13.1P1 comme les autres versions disponibles.
4. Vous pouvez également cliquer sur **Toutes les versions** pour saisir une autre version vers laquelle vous souhaitez effectuer la mise à niveau (par exemple, le prochain patch de la version installée). Pour un chemin de mise à niveau compatible de votre version actuelle de Cloud Volumes ONTAP , reportez-vous à "[Chemins de mise à niveau pris en charge](#)" .
  5. Cliquez sur **Enregistrer**, puis sur **Appliquer**

Select the ONTAP version you want to upgrade to:

Version	Date
<input type="radio"/> 9.12.1P14	Aug 22, 2024
<input type="radio"/> 9.12.1P13	Jul 7, 2024
<input type="radio"/> 9.13.1P10	Jul 7, 2024
<input type="radio"/> 9.13.1P9	May 9, 2024

All versions ^

Write the version you want to upgrade to:

Write the version here

Save Cancel

6. Sur la page Mettre à niveau Cloud Volumes ONTAP , lisez le CLUF, puis sélectionnez **J'ai lu et approuvé le CLUF**.
7. Sélectionnez **Mettre à niveau**.
8. Pour afficher la progression, sur le système Cloud Volumes ONTAP , sélectionnez **Audit**.

### Résultat

La console démarre la mise à niveau du logiciel. Vous pouvez effectuer des actions sur le système lorsque la mise à jour du logiciel est terminée.

### Après avoir terminé

Si vous avez suspendu les transferts SnapMirror , utilisez le Gestionnaire système pour reprendre les

transferts.

### Mise à niveau à partir d'une image disponible à une URL

Vous pouvez placer l'image du logiciel Cloud Volumes ONTAP sur l'agent de la console ou sur un serveur HTTP, puis lancer la mise à niveau du logiciel à partir de la console. Vous pouvez utiliser cette option si la console ne peut pas accéder au bucket S3 pour mettre à niveau le logiciel.

### Avant de commencer

- Les opérations telles que la création de volumes ou d'agrégats 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, causés par des certificats manquants. La solution de contournement consiste à générer et à installer un certificat signé par une autorité de certification à utiliser pour l'authentification entre ONTAP et la console.

Accédez à la base de connaissances NetApp pour afficher les instructions étape par étape :

["Base de connaissances NetApp : Comment configurer la console comme serveur HTTPS pour héberger des images de mise à niveau"](#)

### Étapes

1. Facultatif : configurez un serveur HTTP pouvant héberger l'image du logiciel Cloud Volumes ONTAP .

Si vous disposez d'une connexion VPN au réseau virtuel, vous pouvez placer l'image du logiciel 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 autorise les connexions HTTP sortantes par défaut.

3. Obtenez l'image du logiciel à partir de ["le site d'assistance NetApp"](#) .
4. Copiez l'image du logiciel dans un répertoire de l'agent de la console ou sur un serveur HTTP à partir duquel le fichier sera diffusé.

Deux chemins sont disponibles. Le chemin correct dépend de la version de votre agent de console.

- `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
- `/opt/application/netapp/cloudmanager/ontap/images/`

5. Sur le système, cliquez sur le **...** icône, puis cliquez sur **Mettre à jour Cloud Volumes ONTAP**.
6. Sur la page Mettre à jour la version de Cloud Volumes ONTAP , saisissez l'URL, puis cliquez sur **Modifier l'image**.

Si vous avez copié l'image du logiciel dans l'agent de la console dans le chemin indiqué ci-dessus, vous devez saisir l'URL suivante :

`http://<Adresse IP privée de l'agent de la console>/ontap/images/<nom du fichier image>`



Dans l'URL, **image-file-name** doit suivre le format « cot.image.9.13.1P2.tgz ».

7. Cliquez sur **Continuer** pour confirmer.

## Résultat

La console démarre la mise à jour du logiciel. Vous pouvez effectuer des actions sur le système une fois la mise à jour du logiciel terminée.

## Après avoir terminé

Si vous avez suspendu les transferts SnapMirror, utilisez le Gestionnaire système pour reprendre les transferts.

## Corriger les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT

L'agent de console 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 parties dans lesquelles l'image du logiciel est divisée. Vous devez utiliser les API pour terminer cette étape.

## Étape

1. Soumettez une requête PUT à `/occm/^config` avec le JSON suivant comme corps :

```
{
  "maxDownloadSessions": 32
}
```

La valeur de `maxDownloadSessions` peut être 1 ou tout entier supérieur à 1. Si la valeur est 1, l'image téléchargée ne sera pas divisée.

Notez que 32 est une valeur d'exemple. 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 d'API /occm/config"](#) .

## Enregistrer les systèmes de paiement à l'utilisation Cloud Volumes ONTAP

Le support de NetApp est inclus avec les systèmes Cloud Volumes ONTAP Pay-as-you-Go (PAYGO), mais vous devez d'abord activer le support en enregistrant les systèmes auprès de NetApp.

L'enregistrement d'un système PAYGO auprès de NetApp est requis pour mettre à niveau le logiciel ONTAP à l'aide de l'une des méthodes ["décrit sur cette page"](#) .



Un système qui n'est pas enregistré pour le support recevra toujours les notifications de mise à jour logicielle qui s'affichent dans la console NetApp 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 de site de support NetApp à la console, accédez à **Paramètres du compte** et ajoutez-le maintenant.

"Découvrez comment ajouter des comptes de site de support NetApp" .

2. Sur la page **Systèmes**, double-cliquez sur le nom du système que vous souhaitez enregistrer.
3. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Enregistrement de l'assistance**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

4. Sélectionnez un compte de site de support NetApp et cliquez sur **S'inscrire**.

## Résultat

Le système est enregistré auprès de NetApp.

## Convertir une licence basée sur un nœud Cloud Volumes ONTAP en une licence basée sur la capacité

Après la fin de la disponibilité (EOA) de vos licences basées sur les nœuds, vous devez passer à des licences basées sur la capacité à l'aide de l'outil de conversion de licence dans la console NetApp .

Pour les engagements annuels ou à plus long terme, NetApp vous recommande de contacter votre représentant NetApp avant la date EOA (11 novembre 2024) ou la date d'expiration de la licence pour vous assurer que les conditions préalables à la transition sont en place. Si vous ne disposez pas d'un contrat à long terme pour un nœud Cloud Volumes ONTAP et que vous exécutez votre système avec un abonnement à la demande (PAYGO), il est important de planifier votre conversion avant la fin du support (EOS) le 31 décembre 2024. Dans les deux cas, vous devez vous assurer que votre système répond aux exigences avant d'utiliser l'outil de conversion de licence dans la console NetApp pour une transition transparente.

Pour plus d'informations sur l'EOA et l'EOS, reportez-vous à "[Fin de disponibilité des licences basées sur des nœuds](#)" .

### À propos de cette tâche

- Lorsque vous utilisez l'outil de conversion de licence, la transition du modèle de licence basé sur les nœuds au modèle de licence basé sur la capacité s'effectue sur place et en ligne, ce qui élimine le besoin de migration de données ou de provisionnement de ressources cloud supplémentaires.
- Il s'agit d'une opération non perturbatrice, et aucune interruption de service ni aucun temps d'arrêt d'application ne se produit.
- Les données de compte et d'application de votre système Cloud Volumes ONTAP restent intactes.
- Les ressources cloud sous-jacentes restent inchangées après la conversion.
- L'outil de conversion de licence prend en charge tous les types de déploiement, tels que le nœud unique, la haute disponibilité (HA) dans une zone de disponibilité unique (AZ), la haute disponibilité dans plusieurs AZ, apportez votre propre licence (BYOL) et PAYGO.
- L'outil prend en charge toutes les licences basées sur les nœuds comme source et toutes les licences basées sur la capacité comme destination. Par exemple, si vous possédez une licence PAYGO Standard basée sur les nœuds, vous pouvez la convertir en n'importe quelle licence basée sur la capacité achetée sur la place de marché. NetApp a restreint l'achat, la prolongation et le renouvellement des licences BYOL. Pour plus d'informations, consultez "[Disponibilité restreinte des licences BYOL pour Cloud Volumes ONTAP](#)" .
- La conversion est prise en charge pour tous les fournisseurs de cloud, AWS, Azure et Google Cloud.
- Après la conversion, le numéro de série de la licence basée sur les nœuds sera remplacé par un format basé sur la capacité. Cela s'effectue dans le cadre de la conversion et est reflété sur votre compte NetApp Support Site (NSS).
- Lorsque vous passez au modèle basé sur la capacité, vos données continuent d'être conservées au même emplacement que la licence basée sur les nœuds. Cette approche garantit l'absence de perturbation dans le placement des données et respecte les principes de souveraineté des données tout au long de la transition.

### Avant de commencer

- Vous devez disposer d'un compte NSS avec accès client ou accès administrateur.
- Votre compte NSS doit être enregistré avec les informations d'identification utilisateur que vous avez

utilisées pour accéder à la console.

- Le système Cloud Volumes ONTAP doit être lié au compte NSS avec un accès client ou un accès administrateur.
- Vous devez disposer d'une licence valide basée sur la capacité, soit une licence BYOL, soit un abonnement au marché.
- Une licence basée sur la capacité devrait être disponible sur votre compte. Cette licence peut être un abonnement marketplace ou un package BYOL/offre privée disponible sous **Licences et abonnements** dans la Console.
- Comprendre les critères suivants avant de sélectionner un forfait de destination :
  - Si le compte dispose d'une licence BYOL basée sur la capacité, le package de destination sélectionné doit correspondre aux licences BYOL basées sur la capacité du compte :
    - Quand `Professional` est sélectionné comme package de destination, le compte doit avoir une licence BYOL avec un package Professionnel :
    - Quand `Essentials` est sélectionné comme package de destination, le compte doit avoir une licence BYOL avec le package Essentials.
  - Si le package de destination ne correspond pas à la disponibilité de la licence BYOL du compte, cela implique que la licence basée sur la capacité peut ne pas inclure le package sélectionné. Dans ce cas, vous serez facturé via votre abonnement marketplace.
  - S'il n'existe pas de licence BYOL basée sur la capacité mais uniquement un abonnement au marché, vous devez vous assurer que le package sélectionné est inclus dans votre abonnement au marché basé sur la capacité.
  - S'il n'y a pas suffisamment de capacité dans votre licence basée sur la capacité existante et si vous disposez d'un abonnement Marketplace pour facturer l'utilisation de la capacité supplémentaire, la capacité supplémentaire vous sera facturée via votre abonnement Marketplace.
  - S'il n'y a pas suffisamment de capacité dans votre licence basée sur la capacité existante et que vous ne disposez pas d'un abonnement Marketplace pour facturer l'utilisation de la capacité supplémentaire, la conversion ne peut pas avoir lieu. Vous devez ajouter un abonnement au marché pour facturer la capacité supplémentaire ou étendre la capacité disponible à votre licence actuelle.
  - Si le package de destination ne correspond pas à la disponibilité de la licence BYOL du compte et s'il n'y a pas suffisamment de capacité dans votre licence basée sur la capacité existante, vous serez facturé via votre abonnement au marché.



Si l'une de ces exigences n'est pas remplie, la conversion de licence n'a pas lieu. Dans des cas spécifiques, la licence peut être convertie, mais ne peut pas être utilisée. Cliquez sur l'icône d'information pour identifier les problèmes et prendre des mesures correctives.

## Étapes

1. Sur la page **Systèmes**, double-cliquez sur le nom du système pour lequel vous souhaitez modifier le type de licence.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités.
3. Vérifiez l'icône en forme de crayon à côté de **Méthode de chargement**. Si la méthode de charge de votre système est `Node Based`, vous pouvez le convertir en charge par capacité.



L'icône est désactivée si votre système Cloud Volumes ONTAP est déjà chargé par capacité ou si l'une des exigences n'est pas remplie.

4. Sur l'écran **Convertir les licences basées sur les nœuds en licences basées sur la capacité**, vérifiez le nom du système et les détails de la licence source.
5. Sélectionnez le package de destination pour convertir la licence existante :
  - Essentiel. La valeur par défaut est `Essentials`.
  - Professionnel
6. Si vous disposez d'une licence BYOL, vous pouvez cocher la case pour supprimer la licence basée sur les nœuds de la console une fois la conversion terminée. Si la conversion est toujours en cours, la sélection de cette case à cocher ne supprimera pas la licence de la console. Cette option n'est pas disponible pour les abonnements à la place de marché.
7. Cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **Continuer**.

### Après avoir terminé

Affichez le nouveau numéro de série de la licence et vérifiez les modifications dans le menu **Licences et abonnements** de la console.

### Tarification dans différents hyperscalaires

Pour plus de détails sur les prix, rendez-vous sur le "[Site Web de la console NetApp](#)".

Pour plus d'informations sur les offres privées dans des hyperscalaires spécifiques, écrivez à :

- AWS - [awsrepo@netapp.com](mailto:awsrepo@netapp.com)
- Azure - [azurepo@netapp.com](mailto:azurepo@netapp.com)
- Google Cloud - [gcppo@netapp.com](mailto:gcppo@netapp.com)

## Démarrer et arrêter un système Cloud Volumes ONTAP

Vous pouvez arrêter et démarrer Cloud Volumes ONTAP à partir de la console NetApp pour gérer vos coûts de calcul cloud.

### Planification des arrêts automatiques de Cloud Volumes ONTAP

Vous souhaitez peut-être arrêter Cloud Volumes ONTAP pendant des intervalles de temps spécifiques pour réduire vos coûts de calcul. Plutôt que de le faire manuellement, vous pouvez configurer la console pour qu'elle arrête automatiquement puis redémarre les systèmes à des heures précises.

#### À propos de cette tâche

- Lorsque vous planifiez un arrêt automatique de votre système Cloud Volumes ONTAP, la console reporte l'arrêt si un transfert de données actif est en cours.

Il arrête le système une fois le transfert terminé.

- Cette tâche planifie les arrêts automatiques des deux nœuds d'une paire HA.
- Les instantanés des disques de démarrage et racine ne sont pas créés lors de la désactivation de Cloud Volumes ONTAP via des arrêts planifiés.

Les instantanés sont créés automatiquement uniquement lors d'un arrêt manuel, comme décrit dans la section suivante.

## Étapes

1. Sur la page **Systèmes**, double-cliquez sur le système Cloud Volumes ONTAP .
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Temps d'arrêt planifié**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	On 
S3 Storage Classes	Standard 
Instance Type	m5.xlarge 
Charging Method	Capacity-based 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. Spécifiez le calendrier d'arrêt :
  - a. Choisissez si vous souhaitez arrêter le système tous les jours, tous les jours de la semaine, tous les week-ends ou toute combinaison des trois options.

- b. Indiquez quand vous souhaitez éteindre le système et pendant combien de temps vous souhaitez qu'il soit éteint.

### Exemple

L'image suivante montre un calendrier qui demande à la console d'arrêter le système tous les samedis à 20h00 (20h00) pendant 12 heures. La console redémarre le système tous les lundis à 00h00

### Schedule Downtime

Console Time Zone: 13:48 UTC

Select when to turn off your system:

<b>Turn off every day</b> Sun, Mon, Tue, Wed, Thu, Fri, Sat	at	20	:	00	for	12	hours (1-24)
Turn off every weekdays Mon, Tue, Wed, Thu, Fri	at	20	:	00	for	12	hours (1-24)
Turn off every weekend Sat	at	08	:	00	for	48	hours (1-48)

4. Cliquez sur **Enregistrer**.

### Résultat

Le planning est enregistré. La ligne de temps d'arrêt planifié correspondante sous le panneau Fonctionnalités affiche « Activé ».

### Arrêt de Cloud Volumes ONTAP

L'arrêt de Cloud Volumes ONTAP vous évite d'accumuler des coûts de calcul et crée des instantanés des disques racine et de démarrage, ce qui peut être utile pour le dépannage.



Pour réduire les coûts, la console supprime périodiquement les anciens instantanés des disques racine et de démarrage. Seuls les deux instantanés les plus récents sont conservés pour les disques racine et de démarrage.

### À propos de cette tâche

Lorsque vous arrêtez une paire HA, la console arrête les deux nœuds.

## Étapes

1. Depuis le système, cliquez sur l'icône **Désactiver**.



2. Gardez l'option de création d'instantanés activée, car les instantanés peuvent permettre 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 **Systemes**.



Les instantanés sont créés automatiquement au redémarrage.

## Synchroniser l'heure du système Cloud Volumes ONTAP à l'aide du serveur 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 d'heure.

Spécifiez un serveur NTP à l'aide du "[API de la console NetApp](#)" ou depuis l'interface utilisateur lorsque vous "[créer un serveur CIFS](#)".

## Modifier la vitesse d'écriture du système

Vous pouvez choisir une vitesse d'écriture normale ou élevée pour Cloud Volumes ONTAP dans la console NetApp. La vitesse d'écriture par défaut est normale. Vous pouvez passer à une vitesse d'écriture élevée si des performances d'écriture rapides sont requises pour votre charge de travail.

Une vitesse d'écriture élevée est prise en charge avec tous les types de systèmes à nœud unique et certaines configurations de paires HA. Afficher 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](#)".

### À propos de cette tâche

- Assurez-vous que des opérations telles que la création de volumes ou d'agrégats ne sont pas en cours.
- Sachez que cette modification redémarre le système Cloud Volumes ONTAP. Il s'agit d'un processus

perturbateur qui nécessite un temps d'arrêt pour l'ensemble du système.

## Étapes

1. Sur la page **Systemes**, double-cliquez sur le nom du système que vous configurez pour la vitesse d'écriture.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Vitesse d'écriture**.
3. Sélectionnez **Normal** ou **Élevé**.

Si vous choisissez Élevé, vous devrez lire la déclaration « Je comprends... » et confirmer en cochant la case.



L'option de vitesse d'écriture **Élevée** est prise en charge avec les paires Cloud Volumes ONTAP HA dans Google Cloud à partir de la version 9.13.0.

4. Cliquez sur **Enregistrer**, vérifiez le message de confirmation, puis cliquez sur **Approuver**.

## Modifier le mot de passe administrateur du cluster Cloud Volumes ONTAP

Cloud Volumes ONTAP inclut un compte administrateur de cluster. Vous pouvez modifier le mot de passe de ce compte à partir de la console NetApp, si nécessaire.



Vous ne devez pas modifier le mot de passe du compte administrateur via ONTAP System Manager ou ONTAP CLI. Le mot de passe ne sera pas reflété dans la console. Par conséquent, la console ne peut pas surveiller correctement l'instance.

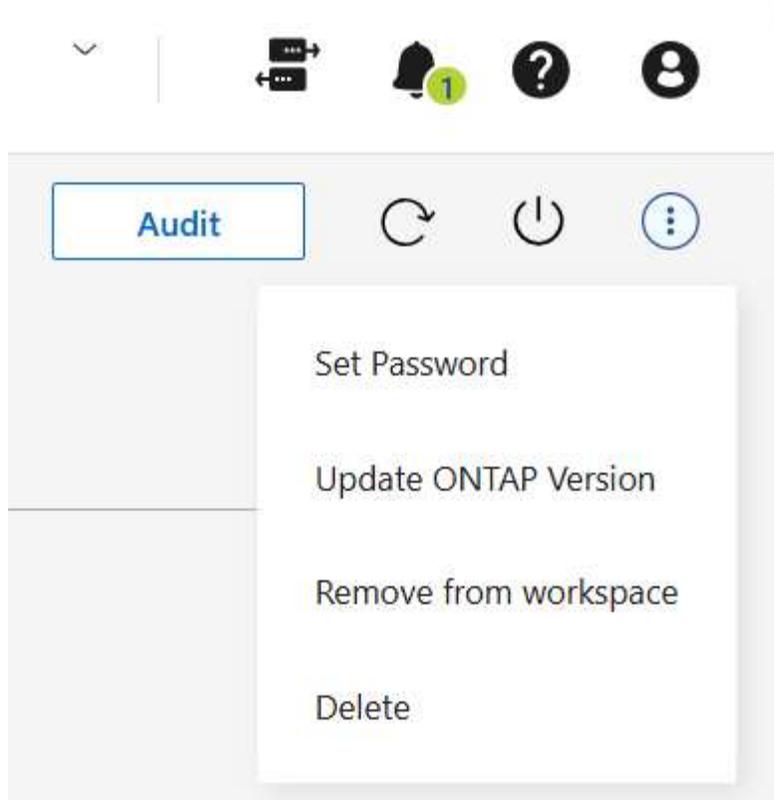
### À propos de cette tâche

Le mot de passe doit respecter quelques règles. Le nouveau mot de passe:

- Ne devrait pas contenir le mot `admin`
- Doit comporter entre huit et 50 caractères
- Doit contenir au moins une lettre anglaise et un chiffre
- Ne doit pas contenir ces caractères spéciaux : / ( ) { } [ ] # : % " ? \

## Étapes

1. Sur la page **Systemes**, double-cliquez sur le nom du système Cloud Volumes ONTAP.
2. En haut à droite de la console, cliquez sur le **...** icône et sélectionnez **Définir le mot de passe**.



## Ajouter, supprimer ou supprimer des systèmes

### Ajouter un système Cloud Volumes ONTAP existant à la console NetApp

Vous pouvez découvrir et ajouter des systèmes Cloud Volumes ONTAP existants à la console NetApp . Vous pouvez le faire si vous déployez un nouveau système.

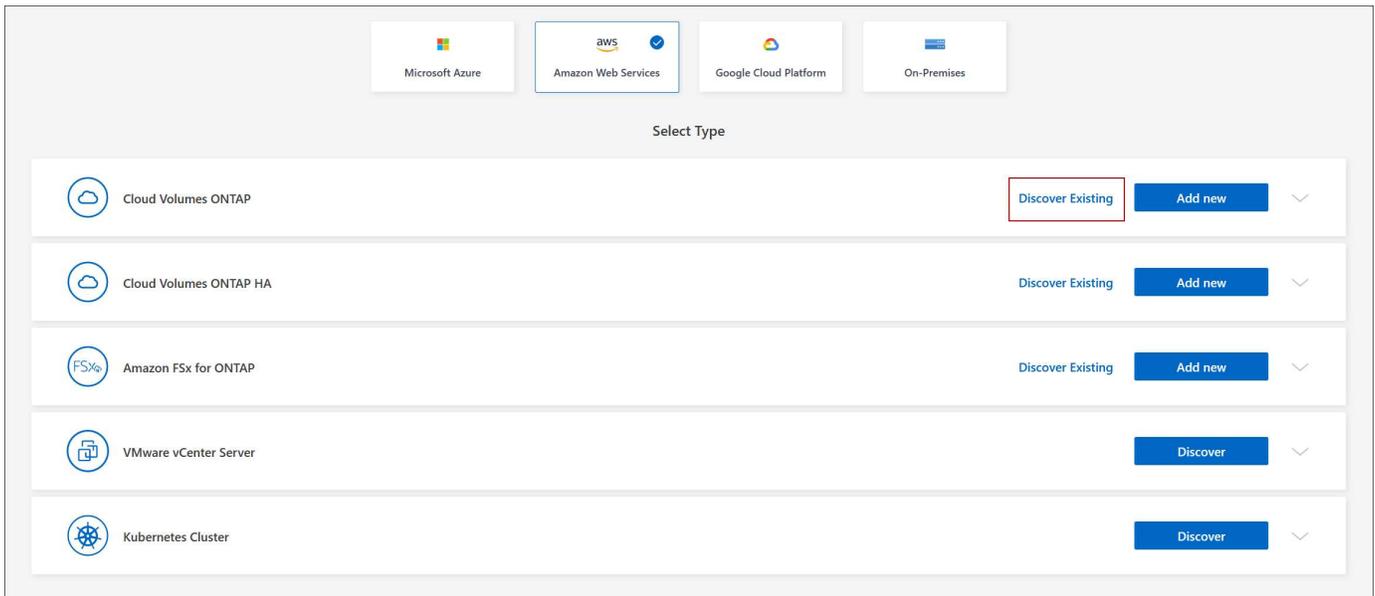
#### Avant de commencer

Vous devez connaître le mot de passe du compte utilisateur administrateur Cloud Volumes ONTAP .

#### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Système**, cliquez sur **Ajouter un système**.
3. Sélectionnez le fournisseur de cloud dans lequel réside le système.
4. Choisissez le type de système Cloud Volumes ONTAP à ajouter.
5. Cliquez sur le lien pour découvrir un système existant.

+



1. Sur la page Région, sélectionnez une région. Vous pouvez voir les systèmes en cours d'exécution dans la région sélectionnée.



Les systèmes Cloud Volumes ONTAP sont représentés sous forme d'instances sur cette page. Dans la liste, vous pouvez sélectionner uniquement les instances enregistrées avec le compte actuel.

2. Sur la page Informations d'identification, saisissez le mot de passe de l'utilisateur administrateur Cloud Volumes ONTAP , puis sélectionnez **Aller**.

### Résultat

La console ajoute les systèmes Cloud Volumes ONTAP à la page **Systèmes**.

### Supprimer un système Cloud Volumes ONTAP de la console NetApp

Vous pouvez supprimer un système Cloud Volumes ONTAP pour le déplacer vers un autre système ou pour résoudre des problèmes de découverte.

#### À propos de cette tâche

La suppression d'un système Cloud Volumes ONTAP le supprime de la console NetApp . Il ne supprime pas le système Cloud Volumes ONTAP . Vous pourrez ultérieurement redécouvrir le système si vous en avez besoin.

#### Étapes

1. Sur la page **Systèmes**, double-cliquez sur le système que vous souhaitez supprimer.
2. En haut à droite de la console, cliquez sur le **...** icône et sélectionnez **Supprimer de l'espace de travail**.
3. Dans la fenêtre **Supprimer de l'espace de travail**, cliquez sur **Supprimer**.

### Résultat

La console supprime le système. Les utilisateurs peuvent redécouvrir le système supprimé à partir de la page **Systèmes** à tout moment.

## Supprimer un système Cloud Volumes ONTAP de la console NetApp

Vous devez toujours supprimer les systèmes Cloud Volumes ONTAP de la console NetApp, plutôt que de l'application de votre fournisseur de cloud. Par exemple, si vous résiliez une instance Cloud Volumes ONTAP sous licence auprès de votre fournisseur de cloud, vous ne pouvez pas utiliser la clé de licence pour une autre instance. Vous devez supprimer le système Cloud Volumes ONTAP de la console pour libérer la licence.

Lorsque vous supprimez un système, la console met fin aux instances Cloud Volumes ONTAP et supprime les disques et les snapshots.



D'autres ressources, telles que les sauvegardes gérées par NetApp Backup and Recovery et les instances de NetApp Data Classification, ne sont pas supprimées lorsque vous supprimez un système. Vous devez les supprimer manuellement. Si vous ne le faites pas, vous continuerez à payer des frais pour ces ressources.

Lorsque la console déploie Cloud Volumes ONTAP chez votre fournisseur de cloud, elle active la protection contre la résiliation sur les instances. Cette option permet d'éviter toute interruption accidentelle.

### Étapes

1. Si vous avez activé la sauvegarde et la récupération sur le système, déterminez si les données sauvegardées sont toujours nécessaires, puis ["supprimer les sauvegardes, si nécessaire"](#).

La sauvegarde et la récupération sont indépendantes de Cloud Volumes ONTAP par conception. Backup and Recovery ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système Cloud Volumes ONTAP, et il n'existe actuellement aucune prise en charge dans l'interface utilisateur pour supprimer les sauvegardes une fois le système supprimé.

2. Si vous avez activé la classification des données sur ce système et qu'aucun autre système n'utilise ce service, vous devez supprimer l'instance du service.

["En savoir plus sur l'instance de classification des données"](#).

3. Supprimez le système Cloud Volumes ONTAP.
  - a. Sur la page **Systèmes**, double-cliquez sur le nom du système Cloud Volumes ONTAP que vous souhaitez supprimer.
  - b. En haut à droite de la console, cliquez sur le **...** icône et sélectionnez **Supprimer**.
  - c. Tapez le nom du système que vous souhaitez supprimer, puis cliquez sur **Supprimer**. La suppression d'un système peut prendre jusqu'à cinq minutes.



La sauvegarde et la récupération sont gratuites uniquement pour les licences Cloud Volumes ONTAP Professional. Cet avantage gratuit ne s'applique pas aux environnements supprimés. Si des copies sauvegardées de l'environnement Cloud Volumes ONTAP sont conservées dans une instance de sauvegarde et de récupération, les copies sauvegardées vous seront facturées jusqu'à leur suppression.

## Administration AWS

## Modifier le type d'instance EC2 pour un système Cloud Volumes ONTAP dans AWS

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 par rapport à vos besoins.

### À propos de cette tâche

- La restitution automatique doit être activée sur une paire Cloud Volumes ONTAP HA (il s'agit du paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : Commandes de configuration du retour 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 fournir des données.



La console NetApp modifie un nœud à la fois en lançant la prise de contrôle et en attendant le retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers au cours de ce processus et n'a constaté aucun problème côté client. À mesure que les connexions changeaient, certaines nouvelles tentatives ont été observées au niveau des E/S, mais la couche application a surmonté le recâblage des connexions NFS/CIFS.

### Référence

Pour obtenir la liste des types d'instances pris en charge dans AWS, reportez-vous à ["Instances EC2 prises en charge"](#).

Si vous ne pouvez pas modifier le type d'instance à partir des instances c4, m4 ou r4, reportez-vous à l'article de la base de connaissances ["Conversion d'une instance AWS Xen CVO en Nitro \(KVM\)"](#).

### Étapes

1. Sur la page **Systemes**, sélectionnez le système.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Type d'instance**.

Information	Features
System Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

Si vous utilisez une licence PAYGO (paiement à l'utilisation) basée sur des nœuds, vous pouvez éventuellement choisir une licence et un type d'instance différents en cliquant sur l'icône en forme de crayon à côté de **Type de licence**.

3. Choisissez un type d'instance, cochez la case pour confirmer que vous comprenez les implications du

changement, puis cliquez sur **Modifier**.

## Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

## Modifier les tables de routage pour les paires Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité AWS

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 (AZ). Vous pouvez le faire si de nouveaux clients NFS ou CIFS doivent accéder à une paire HA dans AWS.

## Étapes

1. Sur la page **Systèmes**, sélectionnez le système.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Tables de routage**.
3. Modifiez la liste des tables de routage sélectionnées, puis cliquez sur **Enregistrer**.

## Résultat

La console NetApp envoie une requête AWS pour modifier les tables de routage.

## Administration 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 le type de machine virtuelle à tout moment si vous déterminez qu'elle est sous-dimensionnée ou surdimensionnée par rapport à vos besoins.

### À propos de cette tâche

- La restitution automatique doit être activée sur une paire Cloud Volumes ONTAP HA (il s'agit du paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : Commandes de configuration du retour 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 fournir des données.



La console NetApp modifie un nœud à la fois en lançant la prise de contrôle et en attendant le retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers au cours de ce processus et n'a constaté aucun problème côté client. À mesure que les connexions changeaient, certaines nouvelles tentatives ont été observées au niveau des E/S, mais la couche application a surmonté le recâblage des connexions NFS/CIFS.

## Étapes

1. Sur la page **Systemes**, sélectionnez le système.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon en regard de **Type de machine virtuelle**.

Si vous utilisez une licence PAYGO (pay-as-you-go) basée sur des nœuds, vous pouvez éventuellement choisir une licence et un type de machine virtuelle différents en cliquant sur l'icône en forme de crayon à côté de **Type de licence**.

3. Sélectionnez un type de machine virtuelle, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **Modifier**.

## Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

## Remplacer les verrous CIFS pour les paires Cloud Volumes ONTAP HA dans Azure

L'administrateur de l'organisation ou du compte peut activer un paramètre dans la console NetApp qui empêche les problèmes de restitution du stockage Cloud Volumes ONTAP lors des événements de maintenance Azure. Lorsque vous activez ce paramètre, Cloud Volumes ONTAP oppose son veto aux verrous CIFS et réinitialise les sessions CIFS actives.

### À propos de cette tâche

Microsoft Azure planifie des événements de maintenance périodiques sur ses machines virtuelles. Lorsqu'un événement de maintenance se produit sur une paire Cloud Volumes ONTAP HA, la paire HA lance la prise de contrôle du stockage. S'il existe des sessions CIFS actives pendant cet événement de maintenance, les verrous sur les fichiers CIFS peuvent empêcher la restitution du stockage.

Si vous activez ce paramètre, Cloud Volumes ONTAP opposera son veto aux verrous et réinitialisera les sessions CIFS actives. Par conséquent, la paire HA peut effectuer la restitution du stockage pendant ces événements de maintenance.



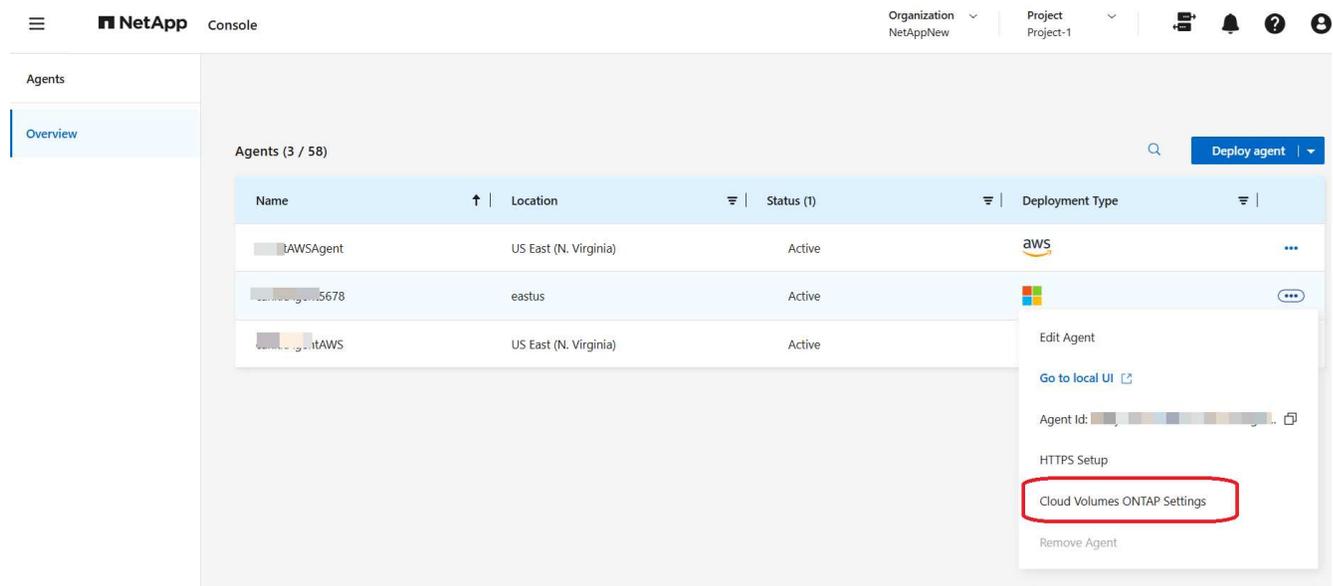
Ce processus peut être perturbateur pour les clients CIFS. Les données qui ne sont pas validées par les clients CIFS peuvent être perdues.

### Avant de commencer

Vous devez créer un agent de console avant de pouvoir modifier les paramètres de la console. "[Apprenez comment](#)".

## Étapes

1. Dans le volet de navigation de gauche, accédez à **Administration > Agents**.
2. Cliquez sur le **...** icône pour l'agent de console qui gère votre système Cloud Volumes ONTAP.
3. Sélectionnez \* Paramètres Cloud Volumes ONTAP \*.



4. Sous **Azure**, cliquez sur **Verrous Azure CIFS pour les systèmes Azure HA**.
5. Cliquez sur la case à cocher pour activer la fonctionnalité, puis cliquez sur **Enregistrer**.

## Utiliser un lien privé Azure ou des points de terminaison de service pour les systèmes Cloud Volumes ONTAP

Cloud Volumes ONTAP utilise un lien privé Azure pour les connexions à ses comptes de stockage associés. Si nécessaire, vous pouvez désactiver Azure Private Links et utiliser des points de terminaison de service à la place.

### Aperçu

Par défaut, la console NetApp active une liaison privée Azure pour les connexions entre Cloud Volumes ONTAP et ses comptes de stockage associés. Un lien privé Azure sécurise les connexions entre les points de terminaison dans Azure et offre des avantages en termes de performances.

Si nécessaire, vous pouvez configurer Cloud Volumes ONTAP pour utiliser des points de terminaison de service au lieu d'un lien privé Azure.

Quelle que soit la configuration, la console limite toujours l'accès au réseau pour les connexions entre Cloud Volumes ONTAP et les comptes de stockage. L'accès au réseau est limité au réseau virtuel sur lequel Cloud Volumes ONTAP est déployé et au réseau virtuel sur lequel l'agent de console est déployé.

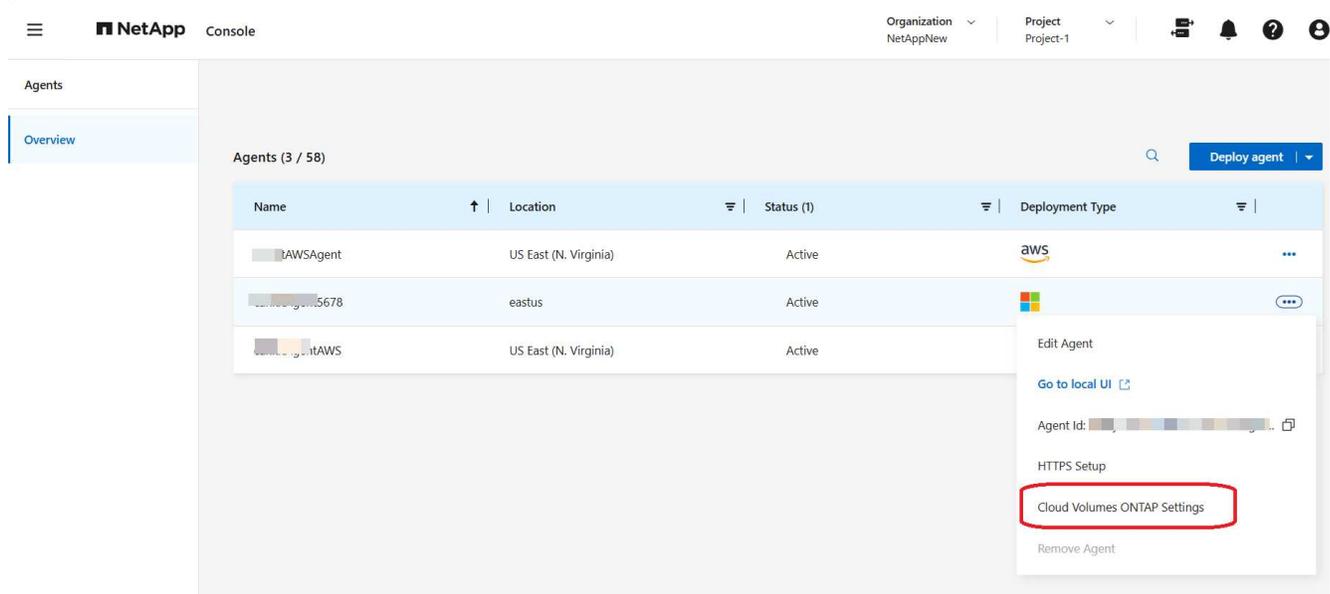
### Désactiver les liens privés Azure et utiliser des points de terminaison de service à la place

Si votre entreprise l'exige, vous pouvez modifier un paramètre dans la console afin qu'il configure Cloud Volumes ONTAP pour utiliser 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. Les points de terminaison de service ne sont pris en charge que dans "**Paires de régions Azure**" entre l'agent de console et les réseaux virtuels Cloud Volumes ONTAP .

L'agent de console doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans la "**Paire de régions Azure**" pour les systèmes Cloud Volumes ONTAP .

### Étapes

1. Dans le volet de navigation de gauche, accédez à **Administration > Agents**.
2. Cliquez sur le **...** icône pour l'agent de console qui gère votre système Cloud Volumes ONTAP .
3. Sélectionnez **\* Paramètres Cloud Volumes ONTAP \***.



4. Sous **Azure**, cliquez sur **Utiliser Azure Private Link**.
5. Désélectionnez **Connexion par lien privé entre Cloud Volumes ONTAP et les comptes de stockage**.
6. Cliquez sur **Enregistrer**.

### Après avoir terminé

Si vous avez désactivé Azure Private Links et que l'agent de la console utilise un serveur proxy, vous devez activer le trafic API direct.

["Découvrez comment activer le trafic API direct sur l'agent de la console"](#)

### Travailler avec Azure Private Links

Dans la plupart des cas, vous n'avez rien à faire pour configurer des liaisons privées Azure avec Cloud Volumes ONTAP. La console gère les liens privés Azure pour vous. Mais si vous utilisez une zone DNS privée Azure existante, vous devrez modifier un fichier de configuration.

### Exigence pour un DNS personnalisé

En option, si vous travaillez avec un DNS personnalisé, vous devez créer un redirecteur conditionnel vers la zone DNS privée Azure à partir de vos serveurs DNS personnalisés. Pour en savoir plus, consultez ["Documentation d'Azure sur l'utilisation d'un redirecteur DNS"](#) .

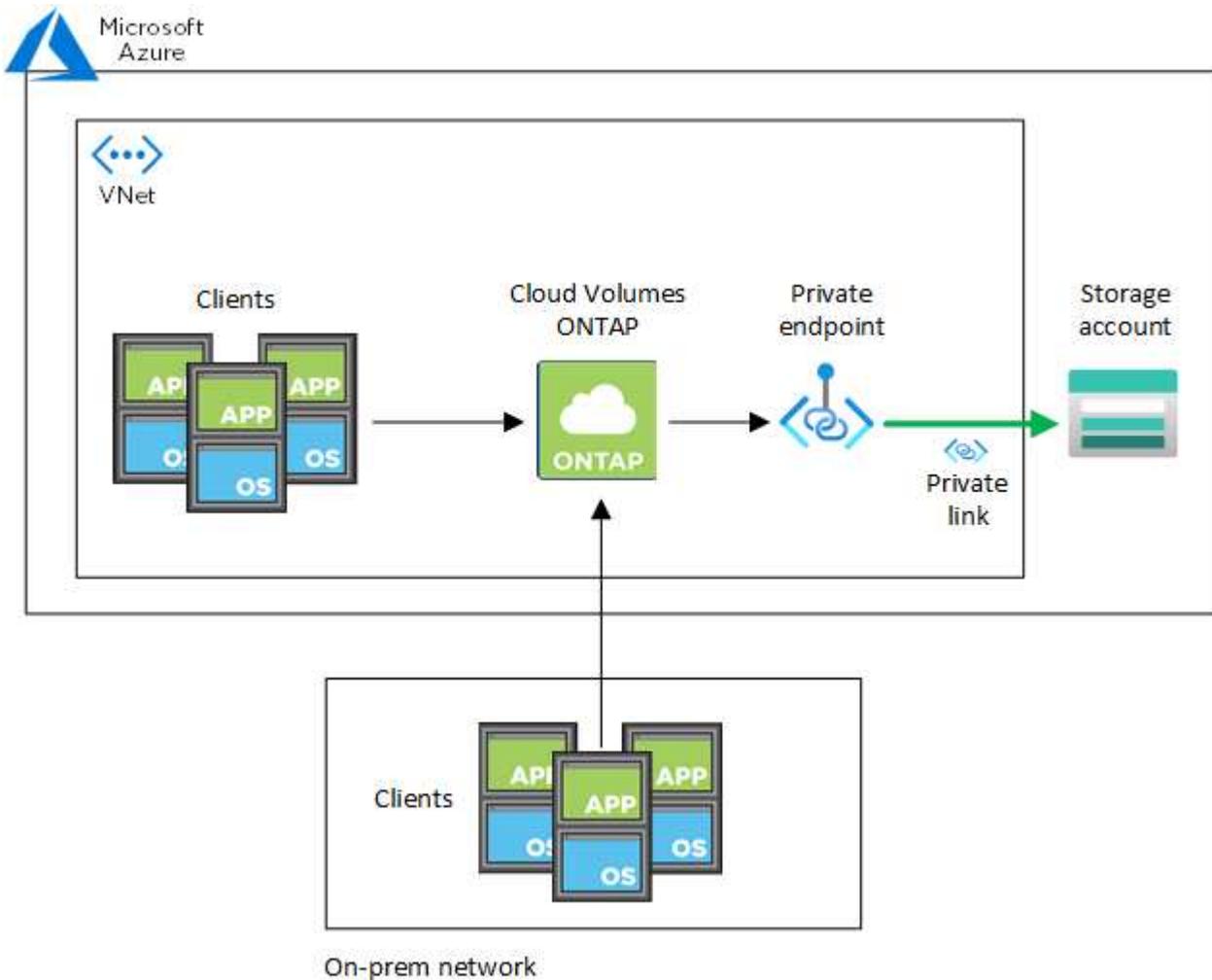
### Comment fonctionnent les connexions Private Link

Lorsque la console déploie Cloud Volumes ONTAP dans Azure, elle crée un point de terminaison privé dans le groupe de ressources. Le point de terminaison privé est associé aux comptes de stockage pour Cloud Volumes ONTAP. Par conséquent, l'accès au stockage Cloud Volumes ONTAP transite par le réseau principal de Microsoft.

L'accès client passe par la liaison privée lorsque les clients se trouvent dans le même réseau virtuel que Cloud

Volumes ONTAP, dans des réseaux virtuels homologues ou dans votre réseau local lorsque vous utilisez une connexion VPN privée ou ExpressRoute au réseau virtuel.

Voici un exemple qui montre l'accès client via une liaison privée à partir du même réseau virtuel et à partir d'un réseau local doté d'une connexion VPN privée ou ExpressRoute.



Si l'agent de console et les systèmes Cloud Volumes ONTAP sont déployés dans des réseaux virtuels différents, vous devez configurer l'appariement de réseaux virtuels entre le réseau virtuel sur lequel l'agent de console est déployé et le réseau virtuel sur lequel les systèmes Cloud Volumes ONTAP sont déployés.

### Fournissez des détails sur votre DNS privé Azure

Si vous utilisez "DNS privé Azure", vous devez alors modifier un fichier de configuration sur chaque agent de console. Sinon, la console ne peut pas définir la connexion Azure Private Link entre Cloud Volumes ONTAP et ses comptes de stockage associés.

Notez que le nom DNS doit correspondre aux exigences de dénomination DNS Azure "[comme indiqué dans la documentation Azure](#)".

### Étapes

1. Connectez-vous en SSH à l'hôte de l'agent de la console et connectez-vous.

2. Accédez au `/opt/application/netapp/cloudmanager/docker_occm/data` annuaire.
3. Modifier `app.conf` en ajoutant le `user-private-dns-zone-settings` paramètre avec les paires mot-clé-valeur suivantes :

```
"user-private-dns-zone-settings" : {
  "resource-group" : "<resource group name of the DNS zone>",
  "subscription" : "<subscription ID>",
  "use-existing" : true,
  "create-private-dns-zone-link" : true
}
```

Le `subscription` Le mot clé n'est requis que si la zone DNS privée se trouve dans un abonnement différent de celui de l'agent de la console.

4. Enregistrez le fichier et déconnectez-vous de l'agent de la console.

Un redémarrage n'est pas nécessaire.

### Activer la restauration en cas d'échec

Si la console ne parvient pas à créer un lien privé Azure dans le cadre d'actions spécifiques, elle termine l'action sans la connexion au lien privé Azure. Cela peut se produire lors de la création d'un nouveau système (nœud unique ou paire HA), ou lorsque les actions suivantes se produisent sur une paire HA : création d'un nouvel agrégat, ajout de disques à un agrégat existant ou création d'un nouveau compte de stockage lorsque l'on dépasse 32 TiO.

Vous pouvez modifier ce comportement par défaut en activant la restauration si la console ne parvient pas à créer le lien privé Azure. Cela peut vous aider à garantir que vous êtes entièrement conforme aux réglementations de sécurité de votre entreprise.

Si vous activez la restauration, la console arrête l'action et restaure toutes les ressources créées dans le cadre de l'action.

Vous pouvez activer la restauration via l'API ou en mettant à jour le fichier `app.conf`.

### Activer la restauration via l'API

#### Étape

1. Utilisez le `PUT /occm/config` Appel d'API avec le corps de requête suivant :

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

### Activer la restauration en mettant à jour `app.conf`

#### Étapes

1. Connectez-vous en SSH à l'hôte de l'agent de la console et connectez-vous.
2. Accédez au répertoire suivant : `/opt/application/netapp/cloudmanager/docker_occm/data`

3. Modifiez app.conf en ajoutant le paramètre et la valeur suivants :

```
"rollback-on-private-link-failure": true  
. Enregistrez le fichier et déconnectez-vous de l'agent de la console.
```

Un redémarrage n'est pas nécessaire.

## Déplacer un groupe de ressources Azure pour Cloud Volumes ONTAP dans la console Azure

Cloud Volumes ONTAP prend en charge les déplacements de groupes de ressources Azure, mais le flux de travail se produit uniquement dans la console Azure.

Vous pouvez déplacer un système Cloud Volumes ONTAP 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 le système Cloud Volumes ONTAP . ["Suppression des systèmes Cloud Volumes ONTAP"](#) .
2. Exécutez le déplacement du groupe de ressources dans la console Azure.

Pour terminer le déplacement, reportez-vous à ["Déplacer des ressources vers un nouveau groupe de ressources ou un abonnement dans la documentation de Microsoft Azure"](#) .

3. Sur la page **Systèmes**, découvrez le système.
4. Recherchez le nouveau groupe de ressources dans les informations du système.

### Résultat

Le système et ses ressources (machines virtuelles, disques, comptes de stockage, interfaces réseau, snapshots) se trouvent dans le nouveau groupe de ressources.

## Séparer le trafic SnapMirror dans Azure

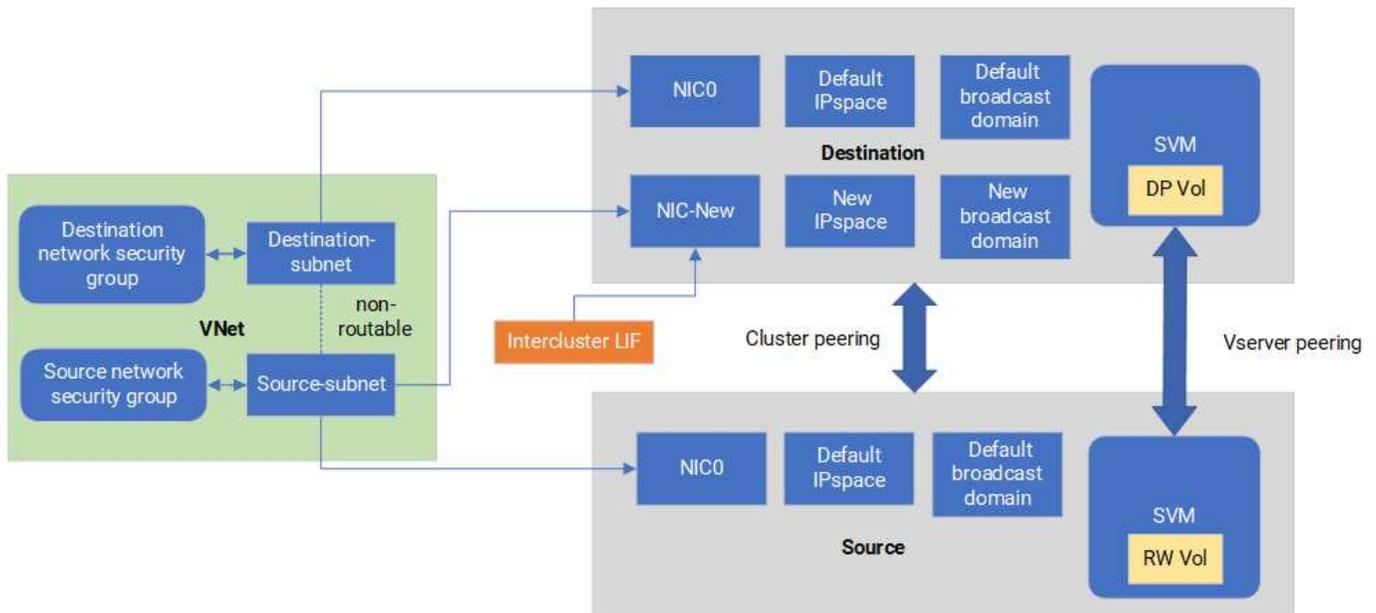
Avec Cloud Volumes ONTAP dans Azure, vous pouvez séparer le trafic de réplication SnapMirror du trafic de données et de gestion. Pour séparer le trafic de réplication SnapMirror de votre trafic de données, vous ajouterez une nouvelle carte d'interface réseau (NIC), un LIF intercluster associé et un sous-réseau non routable.

### À propos de la séparation du trafic SnapMirror dans Azure

Par défaut, la console NetApp configure toutes les cartes réseau et LIF dans un déploiement Cloud Volumes ONTAP sur le même sous-réseau. Dans de telles configurations, le trafic de réplication SnapMirror et le trafic de données et de gestion utilisent le même sous-réseau. La séparation du trafic SnapMirror exploite un sous-réseau supplémentaire qui n'est pas routable vers le sous-réseau existant utilisé pour le trafic de données et de gestion.

### Figure 1

Les diagrammes suivants montrent la séparation du trafic de réplication SnapMirror avec une carte réseau supplémentaire, un LIF intercluster associé et un sous-réseau non routable dans un déploiement à nœud unique. Le déploiement d'une paire HA diffère légèrement.



## Avant de commencer

Passez en revue les considérations suivantes :

- Vous ne pouvez ajouter qu'une seule carte réseau à un déploiement de nœud unique ou de paire HA Cloud Volumes ONTAP (instance de machine virtuelle) pour la séparation du trafic SnapMirror .
- Pour ajouter une nouvelle carte réseau, le type d'instance de machine virtuelle que vous déployez doit avoir une carte réseau inutilisée.
- Les clusters source et de destination doivent avoir accès au même réseau virtuel (VNet). Le cluster de destination est un système Cloud Volumes ONTAP dans Azure. Le cluster source peut être un système Cloud Volumes ONTAP dans Azure ou un système ONTAP .

## Étape 1 : Créez une carte réseau supplémentaire et connectez-la à la machine virtuelle de destination

Cette section fournit des instructions sur la façon de créer une carte réseau supplémentaire et de la connecter à la machine virtuelle de destination. La machine virtuelle de destination est le nœud unique ou le système à paire HA dans Cloud Volumes ONTAP dans Azure où vous souhaitez configurer votre carte réseau supplémentaire.

### Étapes

1. Dans l'interface de ligne de commande ONTAP , arrêtez le nœud.

```
dest::> halt -node <dest_node-vm>
```

2. Dans le portail Azure, vérifiez que l'état de la machine virtuelle (nœud) est arrêté.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Utilisez l'environnement Bash dans Azure Cloud Shell pour arrêter le nœud.
  - a. Arrêtez le nœud.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Désallouer le nœud.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Configurez les règles du groupe de sécurité réseau pour rendre les deux sous-réseaux (sous-réseau du cluster source et sous-réseau du cluster de destination) non routables l'un vers l'autre.

a. Créez la nouvelle carte réseau sur la machine virtuelle de destination.

b. Recherchez l'ID de sous-réseau du sous-réseau du cluster source.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

c. Créez la nouvelle carte réseau sur la machine virtuelle de destination avec l'ID de sous-réseau du sous-réseau du cluster source. Entrez ici le nom de la nouvelle carte réseau.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

d. Enregistrez l'adresse IP privée. Cette adresse IP, <new\_added\_nic\_primary\_addr>, est utilisée pour créer un LIF intercluster dans [domaine de diffusion](#), [LIF intercluster pour la nouvelle carte réseau](#).

5. Connectez la nouvelle carte réseau à la machine virtuelle.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. Démarrer la VM (nœud).

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. Dans le portail Azure, accédez à **Réseau** et confirmez que la nouvelle carte réseau, par exemple nic-new, existe et que la mise en réseau accélérée est activée.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

Pour les déploiements par paire HA, répétez les étapes pour le nœud partenaire.

## Étape 2 : créer un nouvel espace IP, un domaine de diffusion et un LIF intercluster pour la nouvelle carte réseau

Un espace IP distinct pour les LIF interclusters fournit une séparation logique entre les fonctionnalités réseau pour la réplication entre les clusters.

Utilisez l'interface de ligne de commande ONTAP pour les étapes suivantes.

### Étapes

1. Créez le nouvel espace IP (`new_ipspace`).

```
dest::> network ipspace create -ip-space <new_ipspace>
```

2. Créez un domaine de diffusion sur le nouvel espace IP (`new_ipspace`) et ajoutez le port `nic-new`.

```
dest::> network port show
```

3. Pour les systèmes à nœud unique, le port nouvellement ajouté est `e0b`. Pour les déploiements de paires HA avec des disques gérés, le port nouvellement ajouté est `e0d`. Pour les déploiements de paires HA avec des blobs de pages, le port nouvellement ajouté est `e0e`. Utilisez le nom du nœud et non le nom de la machine virtuelle. Recherchez le nom du nœud en exécutant `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500  
-ip-space <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Créez un LIF intercluster sur le nouveau domaine de diffusion (`new_bd`) et sur la nouvelle carte réseau (`nic-new`).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-  
lif> -service-policy default-intercluster -address  
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask  
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Vérifier la création du nouveau LIF intercluster.

```
dest::> net int show
```

Pour les déploiements par paire HA, répétez les étapes pour le nœud partenaire.

## Étape 3 : Vérifier l'appairage de cluster entre les systèmes source et de destination

Cette section fournit des instructions sur la manière de vérifier l'homologation entre les systèmes source et de destination.

Utilisez l'interface de ligne de commande ONTAP pour les étapes suivantes.

## Étapes

1. Vérifiez que le LIF intercluster du cluster de destination peut envoyer une requête ping au LIF intercluster du cluster source. Étant donné que le cluster de destination exécute cette commande, l'adresse IP de destination est l'adresse IP LIF intercluster sur la source.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Vérifiez que le LIF intercluster du cluster source peut envoyer un ping au LIF intercluster du cluster de destination. La destination est l'adresse IP de la nouvelle carte réseau créée sur la destination.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Pour les déploiements par paire HA, répétez les étapes pour le nœud partenaire.

### Étape 4 : créer un peering SVM entre le système source et le système de destination

Cette section fournit des instructions sur la façon de créer un peering SVM entre le système source et le système de destination.

Utilisez l'interface de ligne de commande ONTAP pour les étapes suivantes.

## Étapes

1. Créez un peering de cluster sur la destination en utilisant l'adresse IP LIF intercluster source comme `-peer-addr`s . Pour les paires HA, indiquez l'adresse IP LIF intercluster source pour les deux nœuds comme `-peer-addr`s .

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ipspace
<new_ipspace>
```

2. Saisissez et confirmez la phrase secrète.
3. Créez un peering de cluster sur la source en utilisant l'adresse IP LIF du cluster de destination comme `peer-addr`s . Pour les paires HA, indiquez l'adresse IP LIF intercluster de destination pour les deux nœuds comme `-peer-addr`s .

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. Saisissez et confirmez la phrase secrète.
5. Vérifiez que le cluster est apparié.

```
src::> cluster peer show
```

Un peering réussi affiche **Disponible** dans le champ de disponibilité.

6. Créez un peering SVM sur la destination. Les SVM source et de destination doivent être des SVM de données.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Accepter le peering SVM.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Vérifiez que le SVM est appairé.

```
dest::> vserver peer show
```

Les émissions des États pairs\*peered\* et les applications de peering montrent\*snapmirror\*.

#### Étape 5 : Créer une relation de réplication SnapMirror entre le système source et le système de destination

Cette section fournit des instructions sur la façon de créer une relation de réplication SnapMirror entre le système source et le système de destination.

Pour déplacer une relation de réplication SnapMirror existante, vous devez d'abord rompre la relation de réplication SnapMirror existante avant de créer une nouvelle relation de réplication SnapMirror .

Utilisez l'interface de ligne de commande ONTAP pour les étapes suivantes.

#### Étapes

1. Créez un volume protégé par des données sur le SVM de destination.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Créez la relation de réplication SnapMirror sur la destination qui inclut la politique SnapMirror et la planification de la réplication.

```
dest::> snapmirror create -source-path src_svm:src_vol -destination
-path dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Initialisez la relation de réplication SnapMirror sur la destination.

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. Dans l'interface de ligne de commande ONTAP , validez l'état de la relation SnapMirror en exécutant la commande suivante :

```
dest::> snapmirror show
```

Le statut de la relation est `Snapmirrored` et la santé de la relation est `true` .

5. Facultatif : dans l'interface de ligne de commande ONTAP , exécutez la commande suivante pour afficher l'historique des actions pour la relation SnapMirror .

```
dest::> snapmirror show-history
```

En option, vous pouvez monter les volumes source et de destination, écrire un fichier sur la source et vérifier que le volume est répliqué vers la destination.

## Administration de 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 le type d'instance ou de machine à tout moment si vous déterminez qu'il est sous-dimensionné ou surdimensionné par rapport à vos besoins.

#### À propos de cette tâche

- La restitution automatique doit être activée sur une paire Cloud Volumes ONTAP HA (il s'agit du paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : Commandes de configuration du retour 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.

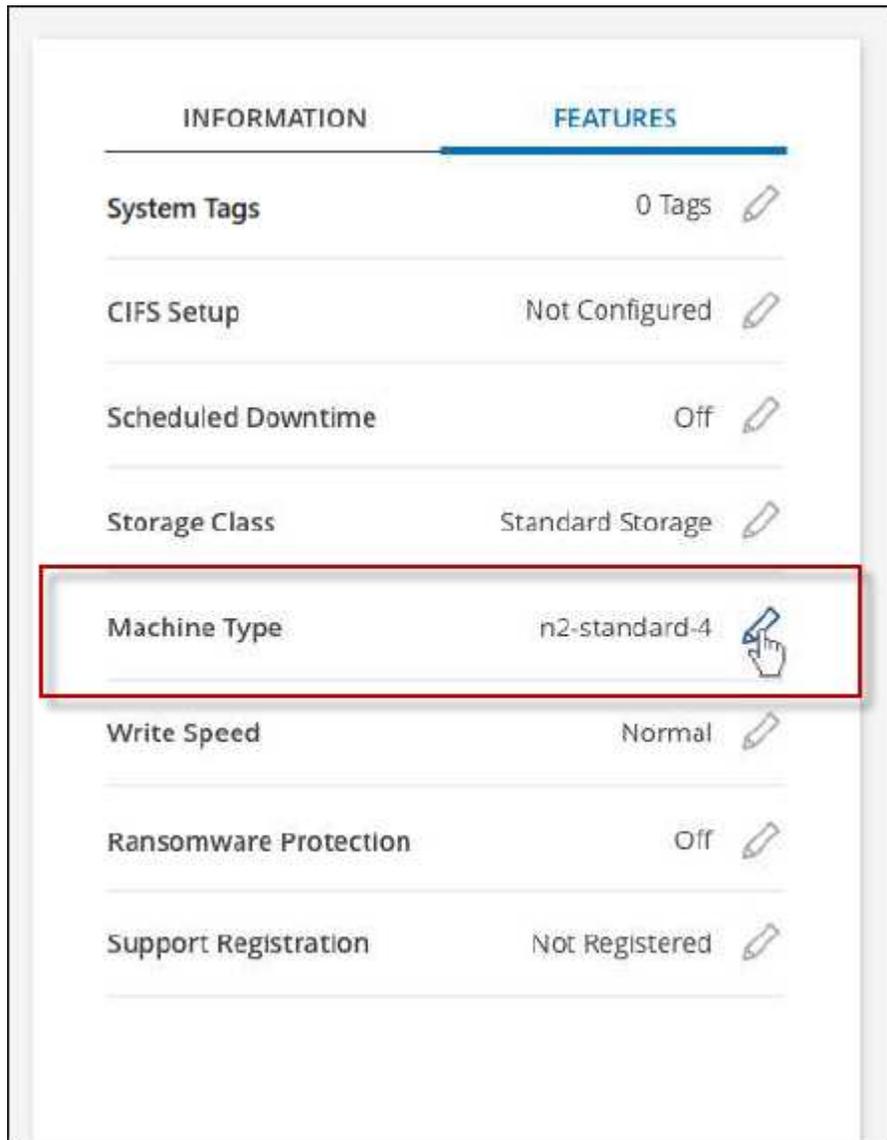
Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de fournir des données.



La console NetApp modifie un nœud à la fois en lançant la prise de contrôle et en attendant le retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers au cours de ce processus et n'a constaté aucun problème côté client. À mesure que les connexions changeaient, certaines nouvelles tentatives ont été observées au niveau des E/S, mais la couche application a surmonté le recâblage des connexions NFS/CIFS.

## Étapes

1. Sur la page **Systèmes**, sélectionnez le système.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **Type de machine**.



Si vous utilisez une licence PAYGO (pay-as-you-go) basée sur des nœuds, vous pouvez éventuellement choisir une licence et un type de machine différents en cliquant sur l'icône en forme de crayon à côté de **Type de licence**.

1. Choisissez un type de machine, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **Modifier**.

## Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

## Administrer Cloud Volumes ONTAP à l'aide de System Manager

Les fonctionnalités avancées de gestion du stockage dans Cloud Volumes ONTAP sont

disponibles via ONTAP System Manager, une interface de gestion fournie avec les systèmes ONTAP . Vous pouvez accéder au Gestionnaire système directement depuis la console NetApp .

## Caractéristiques

Vous pouvez exécuter diverses fonctions de gestion du stockage à l'aide d' ONTAP System Manager dans la console. La liste suivante inclut certaines de ces fonctionnalités, mais elle n'est pas exhaustive :

- Gestion avancée du stockage : gérez les groupes de cohérence, les partages, les qtrees, les quotas et les machines virtuelles de stockage.
- Déplacement du volume : "[Déplacer un volume vers un autre agrégat.](#)"
- Gestion du réseau : gérez les espaces IP, les interfaces réseau, les ensembles de ports et les ports Ethernet.
- Gestion des volumes FlexGroup : vous pouvez créer et gérer des volumes FlexGroup uniquement via le Gestionnaire système. La console ne prend pas en charge la création de volumes FlexGroup .
- Événements et tâches : affichez les journaux d'événements, les alertes système, les tâches et les journaux d'audit.
- Protection avancée des données : protégez les machines virtuelles de stockage, les LUN et les groupes de cohérence.
- Gestion des hôtes : configurez les groupes d'initiateurs SAN et les clients NFS.
- Gestion du stockage d'objets S3 : les fonctionnalités de gestion du stockage S3 dans Cloud Volumes ONTAP sont disponibles uniquement dans System Manager, et non dans la console.

## Configurations prises en charge

- La gestion avancée du stockage via ONTAP System Manager est disponible dans 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 ou dans les régions qui n'ont pas d'accès Internet sortant.

## Limites

Certaines fonctionnalités qui apparaissent dans l'interface du Gestionnaire système ne sont pas prises en charge avec Cloud Volumes ONTAP:

- NetApp Cloud Tiering : Cloud Volumes ONTAP ne prend pas en charge Cloud Tiering. Vous devez configurer la hiérarchisation des données vers le stockage d'objets directement à partir de la vue standard lors de la création de volumes.
- Niveaux : la gestion des agrégats (y compris les niveaux locaux et cloud) n'est pas prise en charge par le Gestionnaire système. Vous devez gérer les agrégats directement à partir de la vue standard.
- Mises à niveau du micrologiciel : Cloud Volumes ONTAP ne prend pas en charge les mises à jour automatiques du micrologiciel à partir de la page **Cluster > Paramètres** du Gestionnaire système.
- Contrôle d'accès basé sur les rôles : le contrôle d'accès basé sur les rôles du Gestionnaire système n'est pas pris en charge.
- Disponibilité continue SMB (CA) : Cloud Volumes ONTAP ne prend pas en charge "[actions SMB disponibles en continu](#)" pour des opérations non perturbatrices.

## Configurer l'authentification pour accéder au Gestionnaire système

En tant qu'administrateur, vous pouvez activer l'authentification pour les utilisateurs accédant à ONTAP System Manager à partir de la console. Vous pouvez déterminer le niveau approprié d'autorisations d'accès en fonction des rôles d'utilisateur ONTAP et activer ou désactiver l'authentification selon les besoins. Si vous activez l'authentification, les utilisateurs doivent saisir leurs informations d'identification d'utilisateur ONTAP chaque fois qu'ils accèdent à System Manager à partir de la console ou lorsque la page est rechargée, car la console ne stocke pas les informations d'identification en interne. Si vous désactivez l'authentification, les utilisateurs peuvent accéder au Gestionnaire système à l'aide des informations d'identification de l'administrateur.



Ce paramètre s'applique à chaque agent de console pour les utilisateurs ONTAP de votre organisation ou de votre compte, quel que soit le système Cloud Volumes ONTAP .

### Autorisations requises

Vous devez disposer des privilèges d'administrateur d'organisation ou de compte pour modifier les paramètres de l'agent de console pour l'authentification utilisateur Cloud Volumes ONTAP .

### Étapes

1. Dans le volet de navigation de gauche, accédez à **Administration > Agents**.
2. Cliquez sur le **...** icône pour l'agent de console requis et sélectionnez **Modifier l'agent de console**.
3. Sous **Forcer les informations d'identification de l'utilisateur**, cochez la case **Activer/Désactiver**. Par défaut, l'authentification est désactivée.



Si vous définissez cette valeur sur **Activer**, l'authentification est réinitialisée et vous devez modifier tous les flux de travail existants pour prendre en compte ce changement.

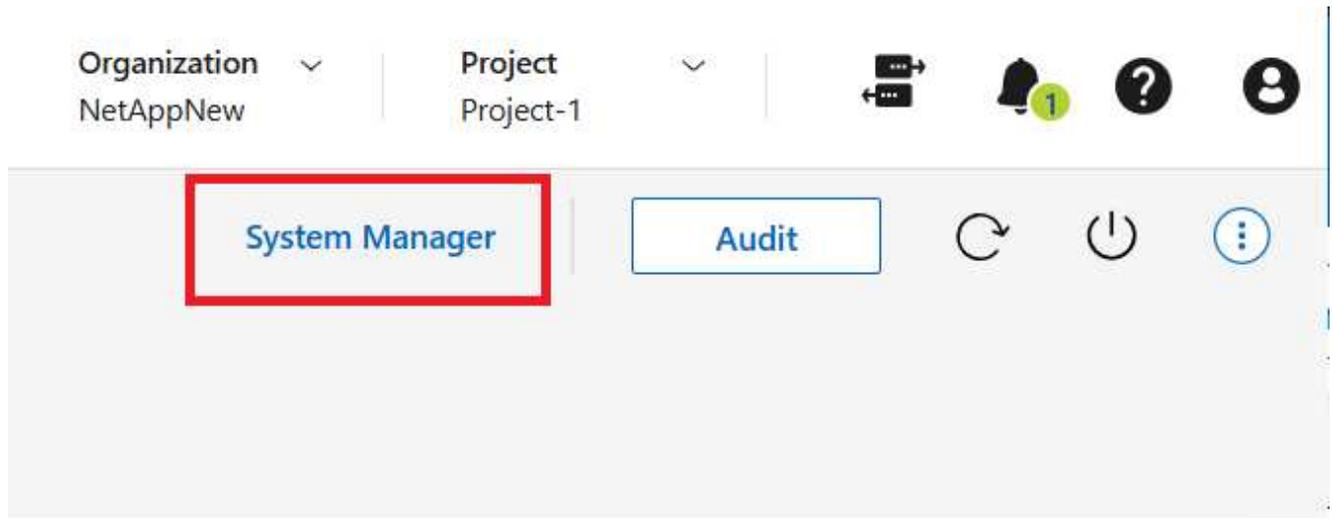
4. Cliquez sur **Enregistrer**.

### Démarrer avec System Manager

Vous pouvez accéder à ONTAP System Manager à partir d'un système Cloud Volumes ONTAP .

### Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, double-cliquez sur le système Cloud Volumes ONTAP requis.
3. Cliquez sur **Gestionnaire système**.



4. Si vous y êtes invité, saisissez vos informations d'identification d'utilisateur ONTAP et cliquez sur **Connexion**.
5. Si un message de confirmation apparaît, lisez-le et cliquez sur **Fermer**.

Utilisez System Manager pour gérer votre système Cloud Volumes ONTAP . Vous pouvez cliquer sur **Retour** pour revenir à la console.

### Aide à l'utilisation du Gestionnaire système

Si vous avez besoin d'aide pour utiliser System Manager avec Cloud Volumes ONTAP, vous pouvez vous référer au "[Documentation ONTAP](#)" pour des instructions étape par étape. Voici quelques liens vers la documentation ONTAP qui pourraient vous aider :

- "[Rôles, applications et authentification ONTAP](#)"
- "[Utiliser le Gestionnaire système pour accéder à un cluster](#)" .
- "[Gestion des volumes et des LUN](#)"
- "[Gestion de réseau](#)"
- "[Protection des données](#)"
- "[Créer des partages SMB disponibles en continu](#)"

### Administrer Cloud Volumes ONTAP depuis la CLI

L'interface de ligne de commande Cloud Volumes ONTAP vous permet d'exécuter toutes les commandes d'administration et constitue un bon choix pour les tâches avancées ou si vous êtes plus à l'aise avec l'interface de ligne de commande. Vous pouvez vous connecter à la CLI 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 vous connecter en SSH à partir d'un hôte de saut qui se trouve dans le réseau de votre fournisseur de cloud.



Lorsqu'elles sont déployées dans plusieurs zones de disponibilité, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion du 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 la console NetApp , identifiez l'adresse IP de l'interface de gestion du cluster :
  - a. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
  - b. Sur la page **Systèmes**, sélectionnez le système Cloud Volumes ONTAP .
  - c. Copiez l'adresse IP de gestion du cluster qui apparaît dans le volet de droite.
2. Utilisez SSH pour vous connecter à l'adresse IP de l'interface de gestion du cluster à l'aide du compte administrateur.

## Exemple

L'image suivante montre un exemple utilisant PuTTY :



3. À l'invite de connexion, entrez le mot de passe du compte administrateur.

## Exemple

```
Password: *****  
COT2:::>
```

# Santé et événements du système

## Vérifier la configuration AutoSupport pour Cloud Volumes ONTAP

AutoSupport surveille de manière proactive l'état 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 à l'aide du protocole de transport HTTPS. Il est préférable de vérifier AutoSupport peut envoyer ces messages.

La seule étape de configuration requise consiste à s'assurer que Cloud Volumes ONTAP dispose d'une connectivité Internet sortante. Pour plus de détails, reportez-vous aux exigences réseau de votre fournisseur de cloud.

## Exigences AutoSupport

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

Les stratégies de routage et de pare-feu doivent autoriser le trafic HTTPS vers les points de terminaison suivants afin que Cloud Volumes ONTAP puisse envoyer des messages AutoSupport :

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

Si une connexion Internet sortante n'est pas disponible pour envoyer des messages AutoSupport , la console NetApp configure automatiquement vos systèmes Cloud Volumes ONTAP pour utiliser l'agent de la console comme serveur proxy. La seule exigence est de s'assurer que le groupe de sécurité de l'agent de console autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après avoir déployé l'agent de console.

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.



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

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

## Dépannez votre configuration AutoSupport

Si aucune connexion sortante n'est disponible et que la console ne peut pas configurer votre système Cloud Volumes ONTAP pour utiliser l'agent de la console comme serveur proxy, vous recevrez une notification de la console intitulée « <nom du système> ne peut pas envoyer de messages AutoSupport ».

Vous recevez probablement ce message en raison de problèmes de réseau.

Suivez ces étapes pour résoudre ce problème.

### Étapes

1. Connectez-vous en SSH au système Cloud Volumes ONTAP afin de pouvoir administrer le système à partir de l'interface de ligne de commande ONTAP .

["Découvrez comment vous connecter à Cloud Volumes ONTAP"](#) .

2. Afficher l'état détaillé du sous-système AutoSupport :

```
autosupport check show-details
```

La réponse devrait être similaire à la suivante :

```

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 le statut de la catégorie http-https est « ok », cela signifie AutoSupport est correctement configuré et que les messages peuvent être envoyés.

3. Si l'état n'est pas correct, vérifiez l'URL du proxy pour chaque nœud Cloud Volumes ONTAP :

```
autosupport show -fields proxy-url
```

4. Si le paramètre d'URL du proxy est vide, configurez Cloud Volumes ONTAP pour utiliser l'agent de la console comme proxy :

```
autosupport modify -proxy-url http://<console agent private ip>:3128
```

5. Vérifiez à nouveau le statut AutoSupport :

```
autosupport check show-details
```

6. Si l'état est toujours en échec, vérifiez qu'il existe une connectivité entre Cloud Volumes ONTAP et l'agent de console via le port 3128.
7. Si l'ID d'état échoue toujours après avoir vérifié qu'il existe une connectivité, connectez-vous à l'agent de la console via SSH.

["En savoir plus sur la connexion à la machine virtuelle Linux pour l'agent de console"](#)

8. Aller à `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Ouvrir 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 `src localnet` 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 d'autorisation :

```
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 en tant que `sudo` :

```
docker restart squid
```

12. Revenez à la CLI Cloud Volumes ONTAP et vérifiez que Cloud Volumes ONTAP peut envoyer des messages AutoSupport :

```
autosupport check show-details
```

## Configurer EMS pour les systèmes Cloud Volumes ONTAP

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 d'interruption SNMP ou serveurs Syslog) et des itinéraires d'événements pour une gravité d'événement particulière.

Vous pouvez configurer EMS à l'aide de la CLI. Pour les instructions, reportez-vous à la "[Documentation ONTAP : Présentation de la configuration EMS](#)".

# Concepts

## Licences

### Licences pour Cloud Volumes ONTAP

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

#### Aperçu des licences

Les options de licence suivantes sont disponibles pour les nouveaux clients.

#### Licences basées sur la capacité

Payez plusieurs systèmes Cloud Volumes ONTAP dans votre compte NetApp par capacité provisionnée. Inclut la possibilité d'acheter des services de données cloud complémentaires. Pour plus d'informations sur les modèles de consommation dans les licences basées sur la capacité, reportez-vous à ["En savoir plus sur les licences basées sur la capacité"](#).

#### Abonnement Keystone

Un service par abonnement à paiement progressif qui offre une expérience de cloud hybride transparente pour les paires haute disponibilité (HA).

Les sections suivantes fournissent plus de détails sur chacune de ces options.



L'assistance n'est pas disponible pour l'utilisation de fonctionnalités sous licence sans licence.

#### Licences basées sur la capacité

Les packages de licences basés sur la capacité vous permettent de payer Cloud Volumes ONTAP par Tio de capacité. La licence est associée à votre compte NetApp et vous permet de facturer plusieurs systèmes sur la licence, à condition qu'une capacité suffisante soit disponible via la licence.

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 sur chaque système Cloud Volumes ONTAP déployé dans ce compte.

Les licences basées sur la capacité sont disponibles sous la forme d'un *package*. Lorsque vous déployez un système Cloud Volumes ONTAP, vous pouvez choisir parmi plusieurs packages de licences en fonction des besoins de votre entreprise.



Bien que l'utilisation et la mesure réelles des produits et services gérés dans la console NetApp soient toujours calculées en Gio et Tio, les termes Go/Gio et To/Tio sont utilisés de manière interchangeable. Cela se reflète dans les listes de la place de marché Cloud, les devis de prix, les descriptions des listes et dans d'autres documents justificatifs.

#### Forfaits

Les packages basés sur la capacité suivants sont disponibles pour Cloud Volumes ONTAP. Pour plus d'informations sur les packages de licences basés sur la capacité, reportez-vous à ["En savoir plus sur les licences basées sur la capacité"](#).

Pour obtenir la liste des types de machines virtuelles pris en charge avec les packages basés sur la capacité suivants, reportez-vous à :

- ["Configurations prises en charge dans Azure"](#)
- ["Configurations prises en charge dans Google Cloud"](#)

## Freemium

Fournit toutes les fonctionnalités Cloud Volumes ONTAP gratuitement de NetApp (des frais de fournisseur de cloud s'appliquent toujours). Un forfait Freemium présente ces caractéristiques :

- Aucune licence ou contrat n'est nécessaire.
- Le support de NetApp n'est pas inclus.
- Vous êtes limité à 500 Gio de capacité provisionnée par système Cloud Volumes ONTAP .
- Vous pouvez utiliser jusqu'à 10 systèmes Cloud Volumes ONTAP avec l'offre Freemium par compte NetApp , pour n'importe quel fournisseur de cloud.
- Si la capacité provisionnée pour un système Cloud Volumes ONTAP dépasse 500 Gio, la console convertit le système en package Essentials.

Dès qu'un système est converti au package Essentials, ["charge minimale"](#) s'applique à elle.

Un système Cloud Volumes ONTAP qui a été converti en package Essentials ne peut pas être reconverti en Freemium même si la capacité provisionnée est réduite à moins de 500 Gio. Les autres systèmes avec moins de 500 Gio de capacité provisionnée restent sur Freemium (à condition qu'ils aient été déployés à l'aide de l'offre Freemium).

## Essentiel

Vous pouvez payer par capacité dans un certain nombre de configurations différentes :

- Choisissez votre configuration Cloud Volumes ONTAP :
  - Un nœud unique ou un système HA
  - Stockage de fichiers et de blocs ou de données secondaires pour la reprise après sinistre (DR)
- Ajoutez l'un des services de données cloud de NetApp moyennant un coût supplémentaire

## Professionnel

Payez à la capacité pour tout type de configuration Cloud Volumes ONTAP avec sauvegardes illimitées.

- Fournit des licences pour toute configuration Cloud Volumes ONTAP

Nœud unique ou HA avec facturation de capacité pour les volumes primaires et secondaires au même tarif

- Inclut des sauvegardes de volumes illimitées à l'aide de NetApp Backup and Recovery, mais uniquement pour les systèmes Cloud Volumes ONTAP qui utilisent le package Professionnel.



Un abonnement à la carte (PAYGO) est requis pour la sauvegarde et la récupération, mais aucun frais ne sera facturé pour l'utilisation de ce service. Pour plus d'informations sur la configuration des licences pour la sauvegarde et la récupération, reportez-vous à ["Configurer les licences pour la sauvegarde et la récupération"](#) .

- Ajoutez l'un des services de données cloud de NetApp moyennant un coût supplémentaire

### Disponibilité des licences basées sur la capacité

La disponibilité des licences PAYGO et BYOL pour les systèmes Cloud Volumes ONTAP nécessite que l'agent de la console soit opérationnel.

["En savoir plus sur les agents de console"](#) .



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

### Comment commencer

Découvrez comment démarrer avec les licences basées sur la capacité :

- ["Configurer les licences pour Cloud Volumes ONTAP dans AWS"](#)
- ["Configurer les licences pour Cloud Volumes ONTAP dans Azure"](#)
- ["Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud"](#)

### Abonnement Keystone

Un service par abonnement à paiement progressif qui offre une expérience de cloud hybride transparente pour ceux qui préfèrent les modèles de consommation OpEx aux CapEx initiaux ou à la location.

La facturation est basée sur la taille de votre capacité engagée pour une ou plusieurs paires Cloud Volumes ONTAP HA dans votre abonnement Keystone .

La capacité provisionnée pour chaque volume est agrégée et comparée périodiquement à la capacité engagée sur votre abonnement Keystone , et tout dépassement est facturé en rafale sur votre abonnement Keystone .

["En savoir plus sur NetApp Keystone"](#) .

### Configurations prises en charge

Les abonnements Keystone sont pris en charge avec les paires HA. Cette option de licence n'est pas prise en charge avec les systèmes à nœud unique pour le moment.

### Limite de capacité

Dans le modèle de licence basé sur la capacité, chaque système Cloud Volumes ONTAP prend en charge la hiérarchisation du stockage d'objets, et la capacité hiérarchisée totale peut évoluer jusqu'à la limite de compartiment du fournisseur de cloud. Bien que la licence n'impose pas de restrictions de capacité, suivez les ["Bonnes pratiques de FabricPool"](#) pour garantir des performances, une fiabilité et une rentabilité optimales lors de la configuration et de la gestion de la hiérarchisation.

Pour plus d'informations sur les limites de capacité de chaque fournisseur de cloud, reportez-vous à leur documentation :

- ["Documentation AWS"](#)
- ["Documentation Azure pour les disques gérés"](#) et ["Documentation Azure pour le stockage d'objets blob"](#)
- ["Documentation Google Cloud"](#)

## Comment commencer

Découvrez comment démarrer avec un abonnement Keystone :

- ["Configurer les licences pour Cloud Volumes ONTAP dans AWS"](#)
- ["Configurer les licences pour Cloud Volumes ONTAP dans Azure"](#)
- ["Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud"](#)

## Licences basées sur les nœuds

Les licences basées sur les nœuds constituent le modèle de licence de la génération précédente qui vous permettait d'octroyer une licence à Cloud Volumes ONTAP par nœud. Ce modèle de licence n'est pas disponible pour les nouveaux clients. La facturation par nœud a été remplacée par les méthodes de facturation par capacité décrites ci-dessus.

NetApp a planifié la fin de la disponibilité (EOA) et du support (EOS) des licences basées sur les nœuds. Après l'EOA et l'EOS, les licences basées sur les nœuds devront être converties en licences basées sur la capacité.

Pour plus d'informations, reportez-vous à ["Communiqué client : CPC-00589"](#) .

## Fin de disponibilité des licences basées sur des nœuds

À compter du 11 novembre 2024, la disponibilité limitée des licences basées sur des nœuds a pris fin. Le support des licences basées sur les nœuds prend fin le 31 décembre 2024.

Si vous disposez d'un contrat valide basé sur des nœuds qui s'étend au-delà de la date EOA, vous pouvez continuer à utiliser la licence jusqu'à l'expiration du contrat. Une fois le contrat expiré, il sera nécessaire de passer au modèle de licence basé sur la capacité. Si vous ne disposez pas d'un contrat à long terme pour un nœud Cloud Volumes ONTAP , il est important de planifier votre conversion avant la date EOS.

Apprenez-en davantage sur chaque type de licence et l'impact de l'EOA sur celui-ci à partir de ce tableau :

Type de licence	Impact après l'EOA
Licence valide basée sur des nœuds achetée via Bring Your Own License (BYOL)	La licence reste valable jusqu'à son expiration. Les licences basées sur des nœuds inutilisées existantes peuvent être utilisées pour déployer de nouveaux systèmes Cloud Volumes ONTAP .
Licence basée sur les nœuds expirée achetée via BYOL	Vous ne serez pas autorisé à déployer de nouveaux systèmes Cloud Volumes ONTAP à l'aide de cette licence. Les systèmes existants peuvent continuer à fonctionner, mais vous ne recevrez aucune assistance ni mise à jour pour vos systèmes après la date EOS.
Licence valide basée sur les nœuds avec abonnement PAYGO	Vous cesserez de bénéficier du support NetApp après la date EOS, jusqu'à ce que vous passiez à une licence basée sur la capacité.

## Exclusions

NetApp reconnaît que certaines situations nécessitent une attention particulière, et les EOA et EOS des licences basées sur les nœuds ne s'appliqueront pas aux cas suivants :

- Clients du secteur public américain
- Déploiements en mode privé
- Déploiements de Cloud Volumes ONTAP dans AWS en Chine

Pour ces scénarios particuliers, NetApp offrira un support pour répondre aux exigences de licence uniques, conformément aux obligations contractuelles et aux besoins opérationnels.



Même dans ces scénarios, les nouvelles licences basées sur des nœuds et les renouvellements de licences sont valables pendant un an maximum à compter de la date d'approbation.

## Conversion de licence

La console permet une conversion transparente des licences basées sur les nœuds en licences basées sur la capacité via l'outil de conversion de licence. Pour plus d'informations sur l'EOA des licences basées sur les nœuds, reportez-vous à "[Fin de disponibilité des licences basées sur des nœuds](#)".

Avant de procéder à la transition, il est bon de vous familiariser avec la différence entre les deux modèles de licence. Les licences basées sur les nœuds incluent une capacité fixe pour chaque instance ONTAP, ce qui peut restreindre la flexibilité. Les licences basées sur la capacité, en revanche, permettent de partager un pool de stockage sur plusieurs instances, offrant ainsi une flexibilité accrue, optimisant l'utilisation des ressources et réduisant le risque de pénalités financières lors de la redistribution des charges de travail. La charge basée sur la capacité s'adapte de manière transparente aux besoins de stockage changeants.

Pour savoir comment effectuer cette conversion, reportez-vous à "[Convertir une licence Cloud Volumes ONTAP basée sur un nœud en une licence basée sur la capacité](#)".



La conversion d'un système de licences basé sur la capacité à un système de licences basé sur les nœuds n'est pas prise en charge.

## En savoir plus sur les licences basées sur la capacité pour Cloud Volumes ONTAP

Vous devez être familiarisé avec la facturation et l'utilisation de la capacité pour les licences basées sur la capacité

### Modèles de consommation

Des packages de licences basés sur la capacité sont disponibles avec les modèles de consommation suivants :

- **BYOL** : Apportez votre propre permis de conduire (BYOL). Une licence achetée auprès de NetApp qui peut être utilisée pour déployer Cloud Volumes ONTAP chez n'importe quel fournisseur de cloud.



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

- **PAYGO** : Un abonnement à la carte (PAYGO) est un abonnement horaire proposé par la place de marché de votre fournisseur de cloud.

- **Annuel** : Un contrat annuel de la place de marché de votre fournisseur de cloud.

Notez ce qui suit :

- Si vous achetez une licence auprès de NetApp (BYOL), vous devez également souscrire à l'offre PAYGO sur la marketplace de votre fournisseur cloud. NetApp a restreint les licences BYOL. À l'expiration de vos licences BYOL, vous devez les remplacer par des abonnements à la marketplace cloud.

Votre licence est toujours facturée en premier, mais vous serez facturé au tarif horaire du marché dans ces cas :

- Si vous dépassez votre capacité autorisée
- Si la durée de votre licence expire
- Si vous disposez d'un contrat annuel auprès d'une place de marché, *tous* les systèmes Cloud Volumes ONTAP que vous déployez sont facturés sur ce contrat. Vous ne pouvez pas combiner un contrat de marché annuel avec BYOL.
- Seuls les systèmes à nœud unique avec BYOL sont pris en charge en Chine. Les déploiements en Chine sont exemptés des restrictions de licence BYOL.

## Changement de forfait

Après le déploiement, vous pouvez modifier le package pour un système Cloud Volumes ONTAP qui utilise des licences basées sur la capacité. Par exemple, si vous avez déployé un système Cloud Volumes ONTAP avec le package Essentials, vous pouvez le remplacer par le package Professional si les besoins de votre entreprise ont changé.

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

Pour plus d'informations sur la conversion des licences basées sur les nœuds en licences basées sur la capacité, consultez

## Tarification et configurations prises en charge

Pour plus de détails sur les prix, rendez-vous sur le ["Site Web de la console NetApp"](#) .

Les packages de licences basés sur la capacité sont disponibles avec Cloud Volumes ONTAP 9.7 et versions ultérieures.

## Machines virtuelles de stockage

- Il n'y a pas de frais de licence supplémentaires pour les machines virtuelles de stockage de données supplémentaires (SVM), mais il y a des frais de capacité minimum de 4 Tio par SVM de stockage de données.
- Les SVM de reprise après sinistre sont facturés en fonction de la capacité provisionnée.

## paires HA

Pour les paires HA, vous n'êtes facturé que pour la capacité provisionnée sur un nœud. Vous n'êtes pas facturé pour les données mises en miroir de manière synchrone sur le nœud partenaire.

## Volumes FlexClone et FlexCache

- Vous ne serez pas facturé pour la capacité utilisée par les volumes FlexClone .

- Les volumes FlexCache source et de destination sont considérés comme des données principales et facturés en fonction de l'espace provisionné.

## Limite de capacité

Dans le modèle de licence basé sur la capacité, chaque système Cloud Volumes ONTAP prend en charge la hiérarchisation du stockage d'objets, et la capacité hiérarchisée totale peut évoluer jusqu'à la limite de compartiment du fournisseur de cloud. Bien que la licence n'impose pas de restrictions de capacité, suivez les ["Bonnes pratiques de FabricPool"](#) pour garantir des performances, une fiabilité et une rentabilité optimales lors de la configuration et de la gestion de la hiérarchisation.

Pour plus d'informations sur les limites de capacité de chaque fournisseur de cloud, reportez-vous à leur documentation :

- ["Documentation AWS"](#)
- ["Documentation Azure pour les disques gérés"](#) et ["Documentation Azure pour le stockage d'objets blob"](#)
- ["Documentation Google Cloud"](#)

## Nombre maximal de systèmes

Avec les licences basées sur la capacité, le nombre maximal de systèmes Cloud Volumes ONTAP est limité à 24 par compte NetApp Console. Un *système* est une paire Cloud Volumes ONTAP HA, un système à nœud unique Cloud Volumes ONTAP ou toute machine virtuelle de stockage supplémentaire que vous créez. La machine virtuelle de stockage par défaut n'est pas prise en compte dans la limite. Cette limite s'applique à tous les modèles de licence.

Par exemple, disons que vous avez trois systèmes :

- Un système Cloud Volumes ONTAP à nœud unique avec une machine virtuelle de stockage (il s'agit de la machine virtuelle de stockage par défaut créée lorsque vous déployez Cloud Volumes ONTAP)

Ce système compte comme un seul système.

- Un système Cloud Volumes ONTAP à nœud unique avec deux machines virtuelles de stockage (la machine virtuelle de stockage par défaut, plus une machine virtuelle de stockage supplémentaire que vous avez créée)

Ce système compte comme deux systèmes : un pour le système à nœud unique et un pour la machine virtuelle de stockage supplémentaire.

- Une paire Cloud Volumes ONTAP HA avec trois machines virtuelles de stockage (la machine virtuelle de stockage par défaut, plus deux machines virtuelles de stockage supplémentaires que vous avez créées)

Ce système compte trois systèmes : un pour la paire HA et deux pour les machines virtuelles de stockage supplémentaires.

Cela représente six systèmes au total. Vous auriez alors de la place pour 14 systèmes supplémentaires sur votre compte.

Si vous avez un déploiement important qui nécessite plus de 24 systèmes, contactez votre représentant de compte ou votre équipe commerciale.

["En savoir plus sur les comptes de console"](#) .

## Remarques sur la charge

Les détails suivants peuvent vous aider à comprendre comment fonctionne la facturation avec les licences basées sur la capacité.

### Frais minimum

Des frais minimum de 4 Tio sont appliqués pour chaque machine virtuelle de stockage de données possédant au moins un volume principal (lecture-écriture). Si la somme des volumes principaux est inférieure à 4 Tio, la console applique les frais minimum de 4 Tio à cette machine virtuelle de stockage.

Si vous n'avez pas encore provisionné de volumes, les frais minimum ne s'appliquent pas.

Pour le package Essentials, les frais de capacité minimale de 4 Tio ne s'appliquent pas aux machines virtuelles de stockage qui contiennent uniquement des volumes secondaires (protection des données). Par exemple, si vous disposez d'une machine virtuelle de stockage avec 1 Tio de données secondaires, vous êtes facturé uniquement pour ces 1 Tio de données. Avec le type de forfait Professionnel, la facturation de capacité minimale de 4 Tio s'applique quel que soit le type de volume.

### Dépassements

Si vous dépassez votre capacité BYOL, les dépassements vous seront facturés au tarif horaire de votre abonnement à la place de marché. Les dépassements sont facturés au tarif de la place de marché, la capacité disponible des autres licences étant privilégiée. Si votre licence BYOL expire, vous devrez passer à un modèle de licence basé sur la capacité via les places de marché cloud.

### Forfait Essentiel

Avec le forfait Essentials, vous êtes facturé en fonction du type de déploiement (HA ou nœud unique) et du type de volume (principal ou secondaire). La tarification du plus élevé au plus bas est présentée dans l'ordre suivant : *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA* et *Essentials Secondary Single Node*. Alternativement, lorsque vous achetez un contrat de marché ou acceptez une offre privée, les frais de capacité sont les mêmes pour tout type de déploiement ou de volume.

L'octroi de licences est entièrement basé sur le type de volume créé dans les systèmes Cloud Volumes ONTAP :

- Essentials Single Node : volumes en lecture/écriture créés sur un système Cloud Volumes ONTAP à l'aide d'un seul nœud ONTAP .
- Essentials HA : volumes de lecture/écriture à l'aide de deux nœuds ONTAP pouvant basculer l'un vers l'autre pour un accès aux données sans interruption.
- Essentials Secondary Single Node : volumes de type Data Protection (DP) (généralement des volumes de destination SnapMirror ou SnapVault en lecture seule) créés sur un système Cloud Volumes ONTAP à l'aide d'un seul nœud ONTAP .



Si un volume en lecture seule/DP devient un volume principal, la console le considère comme des données principales et les coûts de facturation sont calculés en fonction du temps pendant lequel le volume était en mode lecture/écriture. Lorsque le volume est à nouveau rendu en lecture seule/DP, il considère à nouveau le volume comme des données secondaires et facture en conséquence en utilisant la licence la plus correspondante dans la console.

- Essentials Secondary HA : volumes de type Data Protection (DP) (généralement des volumes de destination SnapMirror ou SnapVault en lecture seule) créés sur un système Cloud Volumes ONTAP à l'aide de deux nœuds ONTAP qui peuvent basculer l'un vers l'autre pour un accès aux données sans interruption.

### Apportez votre propre vin

Si vous avez acheté une licence Essentials auprès de NetApp (BYOL) et que vous dépassez la capacité sous licence pour ce déploiement et ce type de volume, la console facture les dépassements sur une licence Essentials à prix plus élevé (si vous en avez une et qu'il y a de la capacité disponible). Cela se produit parce que nous utilisons d'abord la capacité disponible que vous avez déjà achetée en tant que capacité prépayée avant de la facturer sur le marché. S'il n'y a pas de capacité disponible avec votre licence BYOL, la capacité dépassée sera facturée aux tarifs horaires à la demande du marché (PAYGO) et ajoutera des coûts à votre facture mensuelle.

Voici un exemple. Disons que vous disposez des licences suivantes pour le package Essentials :

- Une licence *Essentials Secondary HA* de 500 Tio avec 500 Tio de capacité engagée
- Une licence *Essentials Single Node* de 500 Tio qui ne dispose que de 100 Tio de capacité engagée

50 Tio supplémentaires sont provisionnés sur une paire HA avec des volumes secondaires. Au lieu de facturer ces 50 Tio au PAYGO, la console facture le dépassement de 50 Tio sur la licence *Essentials Single Node*. Cette licence est plus chère que *Essentials Secondary HA*, mais elle utilise une licence que vous avez déjà achetée et n'ajoutera pas de frais à votre facture mensuelle.

Dans **Administration > Licences et abonnements**, vous pouvez voir 50 Tio facturés sur la licence *Essentials Single Node*.

Voici un autre exemple. Disons que vous disposez des licences suivantes pour le package Essentials :

- Une licence *Essentials Secondary HA* de 500 Tio avec 500 Tio de capacité engagée
- Une licence *Essentials Single Node* de 500 Tio qui ne dispose que de 100 Tio de capacité engagée

100 Tio supplémentaires sont provisionnés sur une paire HA avec des volumes primaires. La licence que vous avez achetée ne dispose pas de capacité engagée *Essentials Primary HA*. La licence *Essentials Primary HA* est proposée à un prix plus élevé que les licences *Essentials Primary Single Node* et *Essentials Secondary HA*.

Dans cet exemple, la console facture les dépassements au tarif du marché pour les 100 Tio supplémentaires. Les frais de dépassement apparaîtront sur votre facture mensuelle.

### Contrats de marché ou offres privées

Si vous avez acheté une licence Essentials dans le cadre d'un contrat de place de marché ou d'une offre privée, la logique BYOL ne s'applique pas et vous devez disposer du type de licence exact pour l'utilisation. Le type de licence inclut le type de volume (principal ou secondaire) et le type de déploiement (HA ou nœud unique).

Par exemple, supposons que vous déployez une instance Cloud Volumes ONTAP avec la licence Essentials. Vous provisionnez ensuite des volumes en lecture-écriture (nœud unique principal) et des volumes en lecture seule (nœud unique secondaire). Votre contrat de place de marché ou votre offre privée doit inclure la capacité pour *Essentials Single Node* et *Essentials Secondary Single Node* pour couvrir la capacité provisionnée. Toute capacité provisionnée qui ne fait pas partie de votre contrat de place de marché ou de votre offre privée sera facturée aux tarifs horaires à la demande (PAYGO) et ajoutera des coûts à votre facture mensuelle.

# Stockage

## Protocoles clients pris en charge pour Cloud Volumes ONTAP

Cloud Volumes ONTAP prend en charge les protocoles clients iSCSI, NFS, SMB, NVMe-TCP et S3.

### iSCSI

iSCSI est un protocole de bloc qui peut fonctionner sur des réseaux Ethernet standard. La plupart des systèmes d'exploitation clients proposent un initiateur logiciel qui s'exécute sur un port Ethernet standard.

### NFS

NFS est le protocole d'accès aux fichiers traditionnel pour les systèmes UNIX et LINUX. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles NFSv3, NFSv4 et NFSv4.1. 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 en utilisant les 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, un mélange de styles d'autorisation est pris en charge.

### S3

Cloud Volumes ONTAP prend en charge S3 comme option de stockage évolutif. La prise en charge du protocole S3 vous permet de configurer l'accès client S3 aux objets contenus dans un bucket dans une machine virtuelle de stockage (SVM).

["Documentation ONTAP : découvrez comment fonctionne le multiprotocole S3"](#) . ["Documentation ONTAP : découvrez comment configurer et gérer les services de stockage d'objets S3 dans ONTAP"](#) .

### NVMe-TCP

À partir de la version 9.12.1 ONTAP , NVMe-TCP est pris en charge pour les fournisseurs de cloud. La console NetApp ne fournit aucune fonctionnalité de gestion pour NVMe-TCP.

Pour plus d'informations sur la configuration de NVMe via ONTAP, reportez-vous au ["Documentation ONTAP : Configurer une machine virtuelle de stockage pour NVMe"](#) .

## Disques et agrégats utilisés pour les clusters Cloud Volumes ONTAP

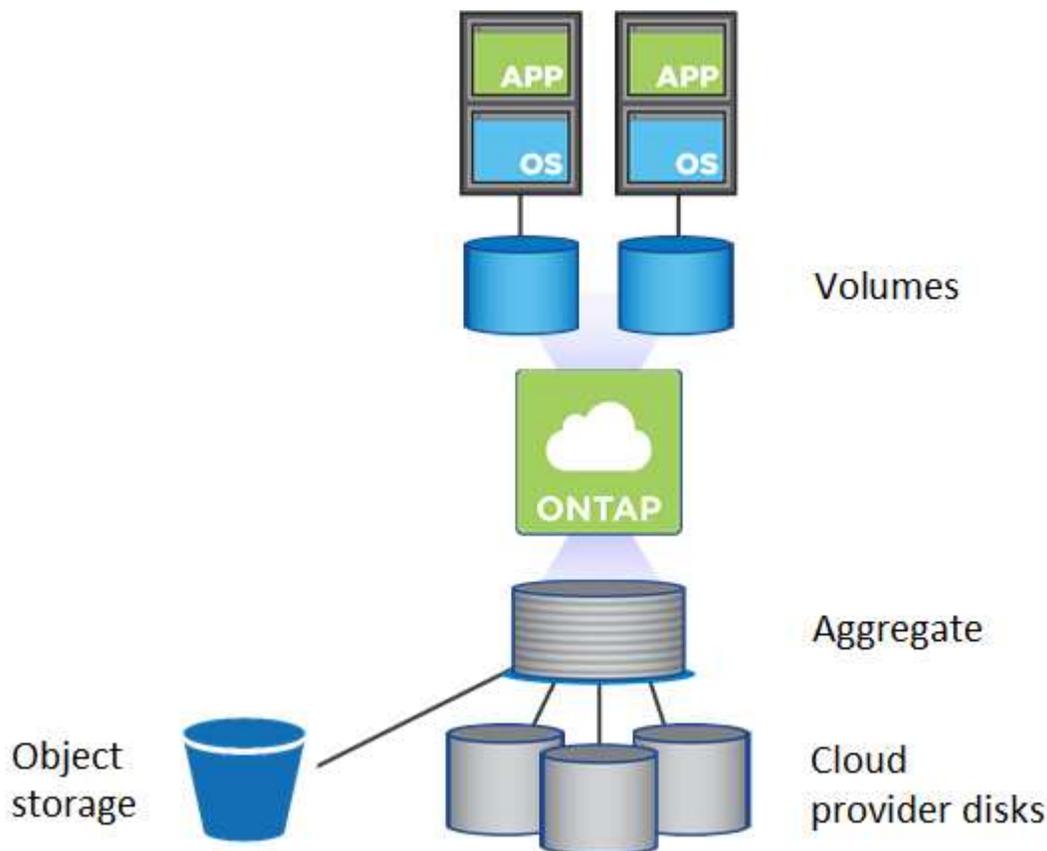
Comprendre comment Cloud Volumes ONTAP utilise le stockage cloud peut vous aider à comprendre vos coûts de stockage.



Vous devez créer et supprimer tous les disques et agrégats de la console NetApp . 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 potentiellement générer des frais de fournisseur de cloud redondants.

## Aperçu

Cloud Volumes ONTAP utilise le stockage du fournisseur cloud sous forme de disques et les regroupe en un ou plusieurs agrégats. Les agrégats fournissent un stockage à un ou plusieurs volumes.



Plusieurs types de disques cloud sont pris en charge. Vous choisissez le type de disque lorsque vous créez un volume et la taille de disque par défaut lorsque vous déployez Cloud Volumes ONTAP.



La quantité totale de stockage achetée auprès d'un fournisseur de cloud est la *capacité brute*. La *capacité utilisable* est inférieure car environ 12 à 14 pour cent de la charge utile est réservée à l'utilisation de Cloud Volumes ONTAP . Par exemple, si la console crée un agrégat de 500 Gio, la capacité utilisable est de 442,94 Gio.

## Stockage de l'AWS

Dans AWS, Cloud Volumes ONTAP utilise le stockage EBS pour les données utilisateur et le stockage NVMe local comme cache Flash sur certains types d'instances EC2.

## Stockage de l'EBS

Dans AWS, un agrégat peut contenir jusqu'à 6 disques qui ont tous la même taille. Mais si vous disposez d'une configuration qui prend en charge la fonctionnalité Amazon EBS Elastic Volumes, un agrégat peut contenir jusqu'à 8 disques. ["En savoir plus sur la prise en charge des volumes élastiques"](#) .

La taille maximale du disque est de 16 Tio.

Le type de disque EBS sous-jacent peut être un SSD à usage général (gp3 ou gp2), un SSD IOPS provisionné (io1) ou un disque dur à débit optimisé (st1). Vous pouvez associer un disque EBS à Amazon S3 pour "[stockage d'objets à faible coût](#)".



La hiérarchisation des données vers le stockage d'objets n'est pas recommandée lors de l'utilisation de disques durs à débit optimisé (st1).

### Stockage NVMe local

Certains types d'instances EC2 incluent un stockage NVMe local, que Cloud Volumes ONTAP utilise comme "[Cache Flash](#)".

### Liens connexes

- "[Documentation AWS : types de volumes EBS](#)"
- "[Découvrez comment choisir les types et les tailles de disque pour vos systèmes dans AWS](#)"
- "[Examiner les limites de stockage pour Cloud Volumes ONTAP dans AWS](#)"
- "[Consultez les configurations prises en charge pour Cloud Volumes ONTAP dans AWS](#)"

### Stockage Azure

Dans Azure, un agrégat peut contenir jusqu'à 12 disques de même taille. Le type de disque et la taille maximale du disque dépendent du fait que vous utilisez un système à nœud unique ou une paire HA :

#### Systemes à nœud unique

Les systèmes à nœud unique peuvent utiliser ces types de disques gérés Azure :

- Les *disques gérés SSD Premium* offrent des performances élevées pour les charges de travail gourmandes en E/S à un coût plus élevé.
- Les *disques gérés SSD Premium v2* offrent des performances supérieures avec une latence plus faible à un coût inférieur pour les paires de nœuds uniques et HA, par rapport aux disques gérés SSD Premium.
- Les *disques gérés SSD standard* offrent des performances constantes pour les charges de travail nécessitant de faibles IOPS.
- Les *disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevés et que vous souhaitez réduire vos coûts.

Chaque type de disque géré a une taille de disque maximale de 32 Tio.

Vous pouvez associer un disque géré au stockage Azure Blob pour "[stockage d'objets à faible coût](#)".

#### paires HA

Les paires HA utilisent deux types de disques qui offrent des performances élevées pour les charges de travail gourmandes en E/S à un coût plus élevé :

- *Blobs de pages Premium* avec une taille de disque maximale de 8 Tio
- *Disques gérés* avec une taille de disque maximale de 32 Tio

### Liens connexes

- ["Découvrez comment choisir les types et les tailles de disque pour vos systèmes dans Azure"](#)
- ["Lancer une paire Cloud Volumes ONTAP HA dans Azure"](#)
- ["Documentation Microsoft Azure : types de disques gérés par Azure"](#)
- ["Documentation Microsoft Azure : Présentation des blobs de pages Azure"](#)
- ["Examiner 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 du disque est de 64 TiB.

Le type de disque peut être *Disques persistants SSD zonaux*, *Disques persistants équilibrés zonaux* ou *Disques persistants standard zonaux*. Vous pouvez associer des disques persistants à un bucket de stockage Google pour ["stockage d'objets à faible coût"](#).

## Liens connexes

- ["Documentation Google Cloud : Options de stockage"](#)
- ["Consultez les limites de stockage pour Cloud Volumes ONTAP dans Google Cloud"](#)

## Type de RAID

Le type RAID pour chaque agrégat Cloud Volumes ONTAP est RAID0 (striping). Cloud Volumes ONTAP s'appuie sur le fournisseur de cloud pour la disponibilité et la durabilité du disque. Aucun autre type de RAID n'est pris en charge.

## Disques de secours à chaud

RAID0 ne prend pas en charge l'utilisation de disques de secours à chaud pour la redondance.

La création de disques inutilisés (disques de secours) attachés à une instance Cloud Volumes ONTAP constitue une dépense inutile et peut empêcher le provisionnement d'espace supplémentaire selon les besoins. Par conséquent, ce n'est pas recommandé.

## En savoir plus sur la prise en charge d'AWS Elastic Volumes avec Cloud Volumes ONTAP

La prise en charge de la fonctionnalité Amazon EBS Elastic Volumes avec un agrégat Cloud Volumes ONTAP offre de meilleures performances et une capacité supplémentaire, tout en permettant à la console NetApp d'augmenter automatiquement la capacité du disque sous-jacent selon les besoins.

## Avantages

- Croissance dynamique du disque

La console peut augmenter dynamiquement la taille des disques pendant que Cloud Volumes ONTAP est en cours d'exécution et que les disques sont toujours connectés.

- Meilleures performances

Les agrégats activés avec Elastic Volumes peuvent avoir jusqu'à huit disques qui sont utilisés de manière égale dans deux groupes RAID. Cette configuration offre un débit plus élevé et des performances constantes.

- Agrégats plus gros

La prise en charge de huit disques offre une capacité globale maximale de 128 Tio. Ces limites sont supérieures à la limite de six disques et à la limite 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.

["Documentation AWS : En savoir plus sur Elastic Volumes d'AWS"](#)

## Configurations prises en charge

La fonctionnalité Amazon EBS Elastic Volumes est prise en charge avec des versions spécifiques de Cloud Volumes ONTAP et des types de disques EBS spécifiques.

### Version Cloud Volumes ONTAP

La fonctionnalité Elastic Volumes est prise en charge avec les nouveaux systèmes Cloud Volumes ONTAP créés à partir de la version 9.11.0 ou ultérieure. La fonctionnalité n'est pas prise en charge avec les systèmes Cloud Volumes ONTAP existants qui ont été déployés avant la version 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 Volumes élastiques est automatiquement activée au niveau agrégé lors de l'utilisation de SSD à usage général (gp3) ou de SSD IOPS provisionnés (io1). La fonctionnalité Volumes élastiques n'est pas prise en charge avec les agrégats qui utilisent un autre type de disque.

## Autorisations AWS requises

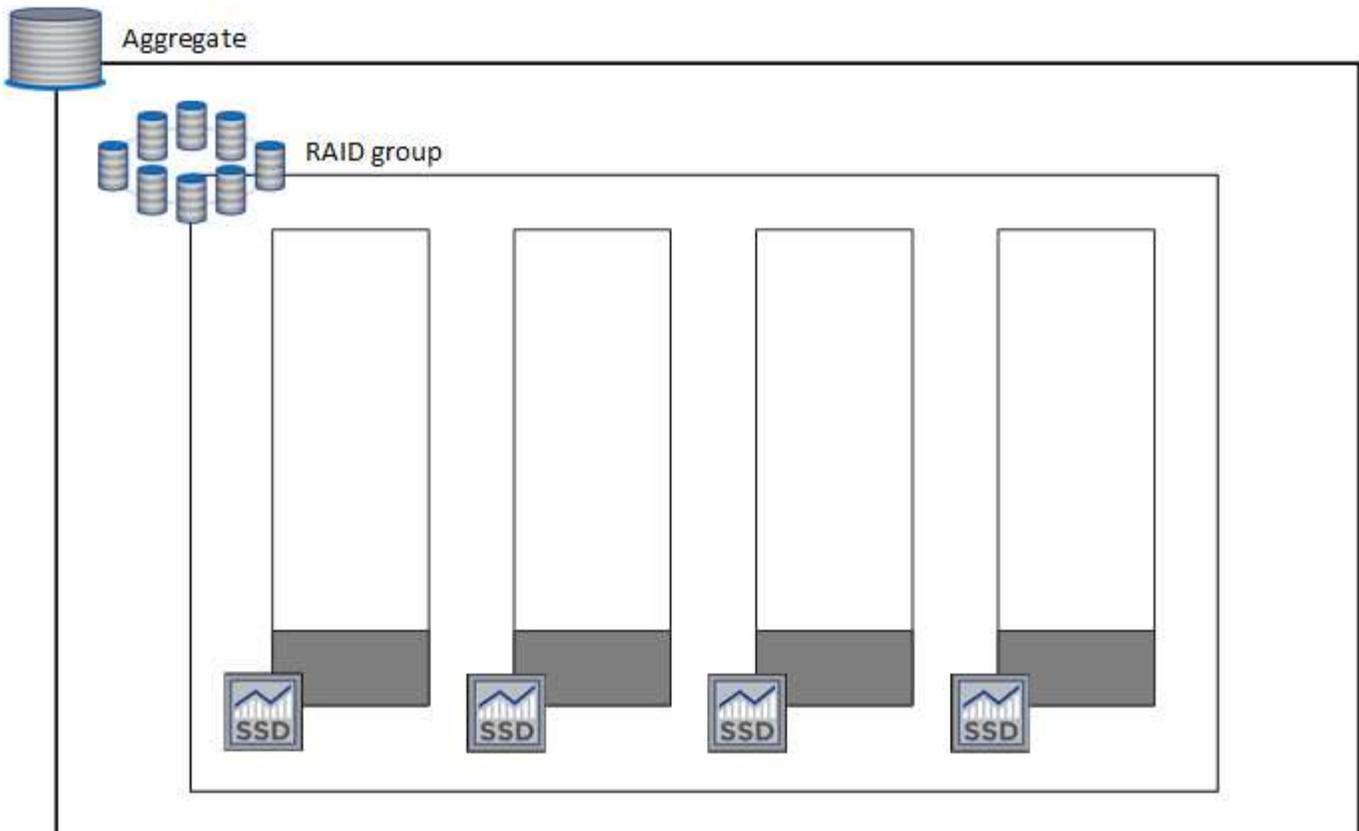
À partir de la version 3.9.19, l'agent de console nécessite les autorisations suivantes pour activer et gérer la fonctionnalité Elastic Volumes sur un agrégat Cloud Volumes ONTAP :

- ec2 : Décrire les modifications des volumes
- ec2:ModifierVolume

Ces autorisations sont incluses dans ["les politiques fournies par NetApp"](#)

## Fonctionnement de la prise en charge des volumes élastiques

Un agrégat sur lequel la fonctionnalité Volumes élastiques est activée est composé d'un ou deux groupes RAID. Chaque groupe RAID dispose de quatre disques identiques ayant la même capacité. Voici un exemple d'un agrégat de 10 Tio qui comporte quatre disques de 2,5 Tio chacun :



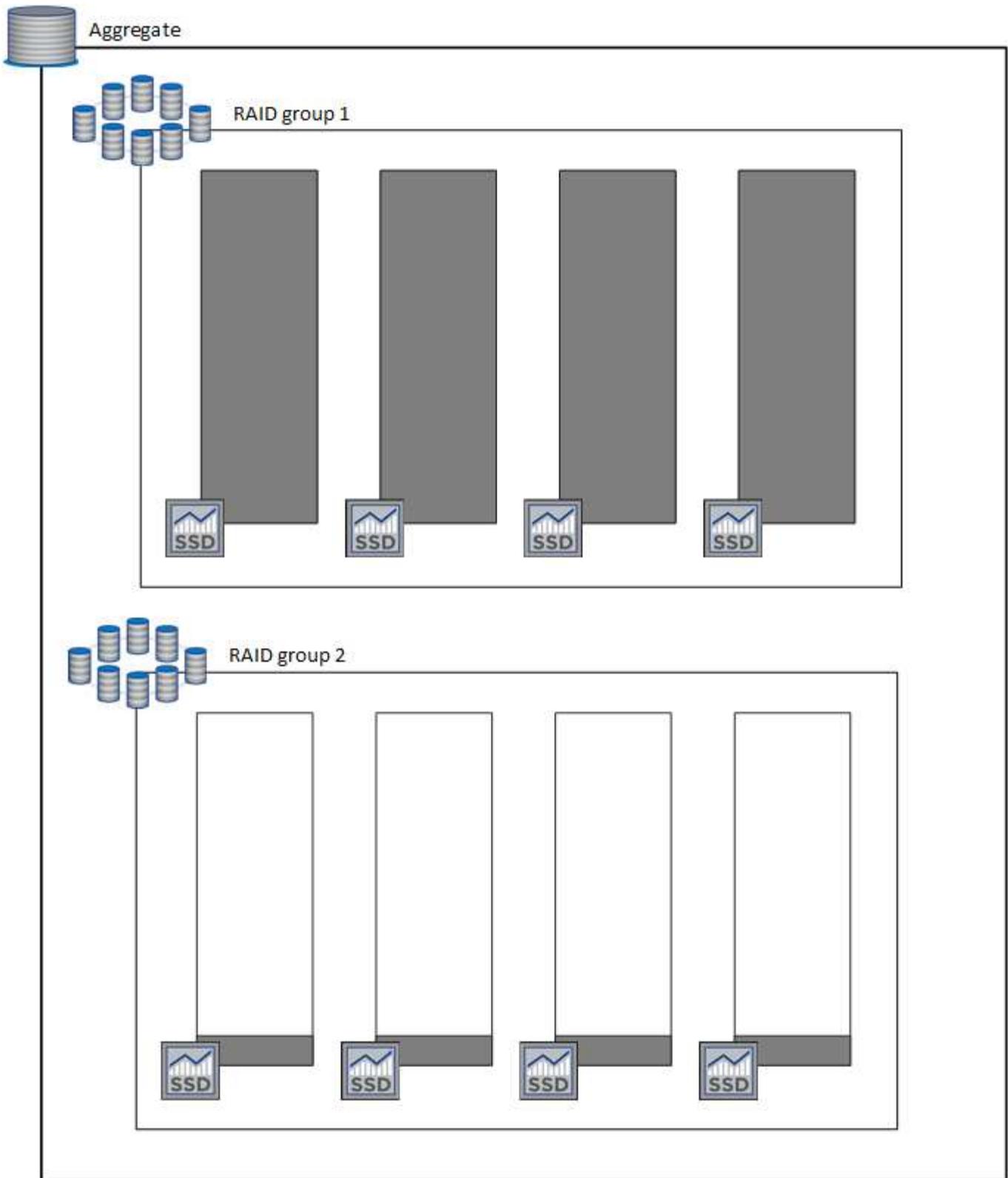
Lorsque la console crée un agrégat, elle démarre avec un groupe RAID. Si une capacité supplémentaire est nécessaire, l'agrégat augmente en augmentant la capacité de tous les disques du groupe RAID du même montant. L'augmentation de capacité est soit d'au moins 256 Gio, soit de 10 % de la taille de l'agrégat.

Par exemple, si vous avez un agrégat de 1 Tio, chaque disque représente 250 Gio. 10 % de la capacité de l'agrégat représente 100 Gio. C'est inférieur à 256 Gio, donc la taille de l'agrégat est augmentée du minimum de 256 Gio (ou 64 Gio pour chaque disque).

La console augmente la taille des disques pendant que le système Cloud Volumes ONTAP est en cours d'exécution et que les disques sont toujours connectés. Le changement n'est pas perturbateur.

Si un agrégat atteint 64 Tio (ou 16 Tio sur chaque disque), la console crée un deuxième groupe RAID pour une capacité supplémentaire. Ce deuxième groupe RAID fonctionne exactement comme le premier : il dispose de quatre disques qui ont exactement la même capacité et il 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 deuxième groupe RAID disposent de beaucoup d'espace libre.



### Que se passe-t-il lorsque vous créez un volume

Si vous créez un volume qui utilise des disques gp3 ou io1, la console crée le volume sur un agrégat comme suit :

- S'il existe un agrégat gp3 ou io1 sur lequel les volumes élastiques sont activés, la console crée le volume sur cet agrégat.

- S'il existe plusieurs agrégats gp3 ou io1 sur lesquels les volumes élastiques sont activés, la console crée le volume sur l'agrégat qui nécessite le moins de ressources.
- Si le système ne dispose que d'agrégats gp3 ou io1 qui ne sont pas activés pour les volumes élastiques, le volume est créé sur cet agrégat.



Bien que ce scénario soit peu probable, il est possible dans deux cas :

- Vous avez explicitement désactivé la fonctionnalité Elastic Volumes lors de la création d'un agrégat à partir de l'API.
- Vous avez créé un nouveau système Cloud Volumes ONTAP à partir de l'interface utilisateur, auquel cas la fonctionnalité Elastic Volumes est désactivée sur l'agrégat initial. Revoir [Limites](#) ci-dessous pour en savoir plus.

- Si aucun agrégat existant n'a suffisamment de capacité, la console crée l'agrégat avec les volumes élastiques activés, puis crée le volume sur ce nouvel agrégat.

La taille de l'agrégat est basée sur le volume demandé plus une capacité supplémentaire de 10 %.

### Mode de gestion de la capacité

Le mode de gestion de la capacité pour un agent de console fonctionne avec les volumes élastiques de la même manière qu'il fonctionne avec d'autres types d'agrégats :

- Lorsque le mode automatique est activé (il s'agit du paramètre par défaut), la console augmente automatiquement la taille des agrégats si une capacité supplémentaire est nécessaire.
- Si vous modifiez le mode de gestion de la capacité sur Manuel, la console demande votre approbation pour acheter une capacité supplémentaire.

["En savoir plus sur le mode de gestion de la capacité"](#) .

### Limites

L'augmentation de la taille d'un agrégat peut prendre jusqu'à 6 heures. Pendant ce temps, la console ne peut demander aucune capacité supplémentaire pour cet agrégat.

### Comment travailler avec les volumes élastiques

Vous pouvez effectuer ces tâches avec Elastic Volumes :

- Créez un nouveau système avec les volumes élastiques activés sur l'agrégat initial lors de l'utilisation de disques gp3 ou io1

["Découvrez comment créer un système Cloud Volumes ONTAP"](#)

- Créer un nouveau volume sur un agrégat sur lequel les volumes élastiques sont activés

Si vous créez un volume qui utilise des disques gp3 ou io1, la console crée automatiquement le volume sur un agrégat sur lequel les volumes élastiques sont activés. Pour plus de détails, reportez-vous à [Que se passe-t-il lorsque vous créez un volume](#) .

["Apprenez à créer des volumes"](#) .

- Créer un nouvel agrégat avec les volumes élastiques activés

Elastic Volumes est automatiquement activé sur les nouveaux agrégats qui utilisent des disques gp3 ou io1, à condition que le système Cloud Volumes ONTAP ait été créé à partir de la version 9.11.0 ou ultérieure.

Lorsque vous créez l'agrégat, la console vous demande la taille de la capacité de l'agrégat. Ceci est différent des autres configurations où 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.

The screenshot shows the 'Select Disk Type' step in the AWS console. At the top, there are four numbered steps: 1. Disk Type, 2. Aggregate details, 3. Tiering Data, and 4. Review. The main content area is titled 'Select Disk Type'. Underneath, there is a 'Disk Type' dropdown menu currently showing 'GP3 - General Purpose SSD Dynamic Performance'. Below the dropdown is a card for 'General Purpose SSD (gp3) Disk Properties'. The card includes a description: 'General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)'. At the bottom of the card, there are two properties: 'IOPS Value' with a value of 12000 and 'Throughput MB/s' with a value of 250. Both properties have an information icon and a dropdown arrow.

["Apprenez à créer des agrégats"](#) .

- Identifier les agrégats pour lesquels les volumes élastiques sont activés

Lorsque vous accédez à la page Allocation avancée, vous pouvez identifier si la fonctionnalité Volumes élastiques est activée sur un agrégat. Dans l'exemple suivant, agr1 a Elastic Volumes activé.

The screenshot shows the configuration for an aggregate named 'aggr1'. At the top right, there is a green 'ONLINE' status indicator and a three-dot menu icon. The configuration is divided into two columns: 'INFO' and 'CAPACITY'.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

- Ajouter de la capacité à un agrégat

Alors que la console ajoute automatiquement de la capacité aux agrégats selon les besoins, vous pouvez augmenter manuellement la capacité vous-même.

["Apprenez à augmenter la capacité globale"](#) .

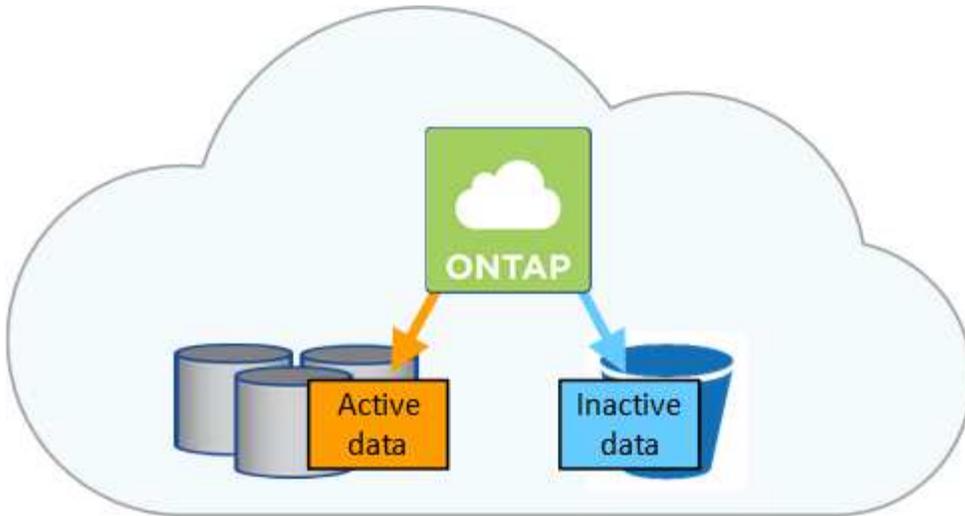
- Répliquer les données vers un agrégat sur lequel les volumes élastiques sont activés

Si le système Cloud Volumes ONTAP de destination prend en charge les volumes élastiques, un volume de destination sera placé sur un agrégat sur lequel les volumes élastiques sont activés (à condition que vous choisissiez un disque gp3 ou io1).

["Apprenez à configurer la réplique des données"](#)

## En savoir plus sur la hiérarchisation des données avec Cloud Volumes ONTAP dans AWS, Azure ou Google Cloud

Réduisez vos coûts de stockage en activant la hiérarchisation automatisée des données inactives vers un stockage d'objets à faible coût. Les données actives restent dans des SSD ou des disques durs hautes performances, tandis que les données inactives sont hiérarchisées vers un stockage d'objets à faible coût. Cela vous permet de récupérer de l'espace sur votre stockage principal et de réduire le stockage secondaire.



La hiérarchisation des données est alimentée par la technologie FabricPool . Cloud Volumes ONTAP fournit une hiérarchisation des données pour tous les clusters Cloud Volumes ONTAP sans licence supplémentaire. Lorsque vous activez la hiérarchisation des données, les données hiérarchisées vers le stockage d'objets entraînent des frais. Consultez la documentation de votre fournisseur de cloud pour plus de détails sur les coûts de stockage d'objets.

### Hiérarchisation des données dans AWS

Lorsque vous activez la hiérarchisation des données dans AWS, Cloud Volumes ONTAP utilise EBS comme niveau de performances pour les données chaudes et AWS S3 comme niveau de capacité pour les données inactives.

#### Niveau de performance

Le niveau de performance peut être des SSD à usage général (gp3 ou gp2) ou des SSD IOPS provisionnés (io1).

La hiérarchisation des données vers le stockage d'objets n'est pas recommandée lors de l'utilisation de disques durs à débit optimisé (st1).

#### Niveau de capacité

Un système Cloud Volumes ONTAP hiérarchise les données inactives dans un seul compartiment S3.

La console NetApp crée un seul compartiment S3 pour chaque système et le nomme *fabric-pool-cluster identifiant unique*. Un compartiment S3 différent n'est pas créé pour chaque volume.

Lorsque la console crée le bucket S3, elle utilise les paramètres par défaut suivants :

- Classe de stockage : Standard
- Cryptage par défaut : désactivé
- Bloquer l'accès public : Bloquer tous les accès publics
- Propriété de l'objet : ACL activées
- Gestion des versions du bucket : 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 modifiant la classe de stockage sur l'une des 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 démarrent dans la classe de stockage Standard et passent à la classe de stockage que vous avez sélectionnée, si les données ne sont pas consultées après 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données, alors tenez-en compte avant de changer la classe de stockage. "[Documentation Amazon S3 : En savoir plus sur les classes de stockage Amazon S3](#)".

Vous pouvez sélectionner une classe de stockage lorsque vous créez le système et vous pouvez la modifier à tout moment par la suite. Pour obtenir des instructions sur la modification de la classe de stockage, reportez-vous à "[Hiérarchiser les données inactives vers un stockage d'objets à faible coût](#)".

La classe de stockage pour la hiérarchisation des données s'applique à l'ensemble du système, et non par volume.

## Hiérarchisation des données dans Azure

Lorsque vous activez la hiérarchisation des données dans Azure, Cloud Volumes ONTAP utilise les disques gérés Azure comme niveau de performances pour les données chaudes et le stockage Azure Blob comme niveau de capacité pour les données inactives.

### Niveau de performance

Le niveau de performance peut être soit des SSD, soit des disques durs.

### Niveau de capacité

Un système Cloud Volumes ONTAP hiérarchise les données inactives dans un seul conteneur Blob.

La console crée un nouveau compte de stockage avec un conteneur pour chaque système Cloud Volumes ONTAP. Le nom du compte de stockage est aléatoire. Un conteneur différent n'est pas créé pour chaque volume.

La console crée le compte de stockage avec les paramètres suivants :

- Niveau d'accès : Chaud
- Performances : Standard
- Redondance : conformément au déploiement de Cloud Volume ONTAP
  - Zone de disponibilité unique : stockage localement redondant (LRS)
  - Zone de disponibilité multiple : stockage redondant dans une zone (ZRS)
- Compte : StorageV2 (usage général v2)
- Exiger un transfert sécurisé pour les opérations de l'API REST : Activé
- Accès à la clé du compte de stockage : Activé
- Version TLS minimale : Version 1.2
- Cryptage de l'infrastructure : désactivé

## Niveaux d'accès au stockage

Le niveau d'accès au stockage par défaut pour les données hiérarchisées dans Azure est le niveau *hot*. Le niveau chaud est idéal pour les données fréquemment consultées dans le niveau de capacité.

Si vous ne prévoyez pas d'accéder aux données inactives dans le niveau de capacité, vous pouvez choisir le niveau de stockage *cool*, où les données inactives sont conservées pendant au moins 30 jours. Vous pouvez également opter pour le niveau *froid*, où les données inactives sont stockées pendant au moins 90 jours. En fonction de vos besoins de stockage et de vos considérations de coût, vous pouvez sélectionner le niveau qui correspond le mieux à vos besoins. Lorsque vous modifiez le niveau de stockage sur *cool* ou *cold*, les données du niveau de capacité inactif sont déplacées directement vers le niveau de stockage froid ou froid. Les niveaux froid et froid offrent des coûts de stockage inférieurs par rapport au niveau chaud, mais ils entraînent des coûts d'accès plus élevés, alors tenez-en compte avant de changer de niveau de stockage. Se référer à "[Documentation Microsoft Azure : En savoir plus sur les niveaux d'accès au stockage Azure Blob](#)".

Vous pouvez sélectionner un niveau de stockage lorsque vous ajoutez un système Cloud Volumes ONTAP et vous pouvez le modifier à tout moment par la suite. Pour plus de détails sur la modification du niveau de stockage, reportez-vous à "[Hiérarchiser les données inactives vers un stockage d'objets à faible coût](#)".

Le niveau d'accès au stockage pour la hiérarchisation des données s'applique à l'ensemble du système et non par volume.

## Hiérarchisation des données dans Google Cloud

Lorsque vous activez la hiérarchisation des données dans Google Cloud, Cloud Volumes ONTAP utilise des disques persistants comme niveau de performances pour les données chaudes et un bucket Google Cloud Storage comme niveau de capacité pour les données inactives.

### Niveau de performance

Le niveau de performance peut être constitué de disques persistants SSD, de disques persistants équilibrés ou de disques persistants standard.

### Niveau de capacité

Un système Cloud Volumes ONTAP hiérarchise les données inactives dans un seul bucket Google Cloud Storage.

La console crée un bucket pour chaque système et le nomme *fabric-pool-cluster identifiant unique*. Un bucket différent n'est pas créé pour chaque volume.

Lorsque la console crée le bucket, elle utilise les paramètres par défaut suivants :

- Type de lieu : Région
- Classe de stockage : Standard
- Accès public : soumis aux listes de contrôle d'accès des objets
- Contrôle d'accès : à granularité fine
- Protection : Aucune
- Cryptage 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 consultées, vous pouvez réduire vos coûts de stockage en optant pour *Nearline Storage* ou *Coldline Storage*. Lorsque vous modifiez la classe de stockage, les données inactives suivantes

sont déplacées directement vers la classe que vous avez sélectionnée.



Toutes les données inactives existantes conserveront la classe de stockage par défaut lorsque vous modifiez la classe de stockage. Pour modifier la classe de stockage des données inactives existantes, vous devez effectuer la désignation manuellement.

Les coûts d'accès sont plus élevés si vous accédez aux données, alors tenez-en compte avant de changer la classe de stockage. Pour en savoir plus, reportez-vous à la ["Documentation Google Cloud : classes de stockage"](#) .

Vous pouvez sélectionner un niveau de stockage lors de la création du système et vous pouvez le modifier à tout moment par la suite. Pour plus de détails sur la modification de la classe de stockage, reportez-vous à ["Hiérarchiser les données inactives vers un stockage d'objets à faible coût"](#) .

La classe de stockage pour la hiérarchisation des données s'applique à l'ensemble du système, et non par volume.

### Hiérarchisation des données et limites de capacité

Si vous activez la hiérarchisation 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.

### Politiques 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 politique différente pour chaque volume.

Certaines stratégies de hiérarchisation ont une période de refroidissement minimale associée, qui définit la durée pendant laquelle 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 dans l'agrégat.



Vous pouvez modifier la période de refroidissement minimale et le seuil global par défaut de 50 % (plus d'informations à ce sujet ci-dessous). ["Apprenez à modifier la période de refroidissement"](#) et ["apprenez à modifier le seuil"](#) .

La console vous permet de choisir parmi les stratégies de hiérarchisation des volumes suivantes lorsque vous créez ou modifiez un volume :

#### Instantané uniquement

Une fois qu'un agrégat a atteint 50 % de sa capacité, Cloud Volumes ONTAP hiérarchise les données utilisateur froides des copies Snapshot qui ne sont pas associées au système de fichiers actif vers le niveau de capacité. La période de refroidissement est d'environ 2 jours.

Si les blocs de données froids sont lus au niveau de capacité, ils deviennent chauds et sont déplacés vers le niveau de performance.

#### Tous

Toutes les données (à l'exception des métadonnées) sont immédiatement marquées comme froides et hiérarchisées vers le stockage d'objets dès que possible. Il n'est pas nécessaire d'attendre 48 heures pour que les nouveaux blocs d'un volume deviennent froids. Notez que les blocs situés dans le volume avant la définition de la politique All nécessitent 48 heures pour devenir froids.

Si les blocs de données froids sont lus sur le niveau cloud, ils restent froids et ne sont pas réécrits sur le niveau de performance. Cette politique est disponible à partir d' ONTAP 9.6.

### Automatique

Une fois qu'un agrégat a atteint 50 % de sa capacité, Cloud Volumes ONTAP hiérarchise les blocs de données froids d'un volume selon un niveau de capacité. Les données froides incluent non seulement des copies instantanées, mais également des données utilisateur froides provenant du système de fichiers actif. La période de refroidissement est d'environ 31 jours.

Cette politique est prise en charge à partir de Cloud Volumes ONTAP 9.4.

Si les données sont lues de manière aléatoire, les blocs de données froids du niveau de capacité deviennent chauds et passent au niveau de performance. Si les données sont lues par des lectures séquentielles, telles que celles associées aux analyses d'index et d'antivirus, les blocs de données froids restent froids et ne passent pas au niveau de performance.

### Aucune

Conserve les données d'un volume dans le niveau de performance, empêchant ainsi leur déplacement vers le niveau de capacité.

Lorsque vous répliquez un volume, vous pouvez choisir de hiérarchiser les données vers le stockage d'objets. Si vous le faites, la console applique la politique **Sauvegarde** au volume de protection des données. À partir de Cloud Volumes ONTAP 9.6, la politique de hiérarchisation **Tout** remplace la politique de sauvegarde.

### La désactivation de Cloud Volumes ONTAP affecte la période de refroidissement

Les blocs de données sont refroidis par des analyses de refroidissement. Au cours de ce processus, la température des blocs qui n'ont pas été utilisés est déplacée (refroidie) vers la valeur inférieure suivante. Le temps de refroidissement par défaut dépend de la politique de hiérarchisation des volumes :

- Auto : 31 jours
- Instantané uniquement : 2 jours

Cloud Volumes ONTAP doit être en cours d'exécution pour que l'analyse de refroidissement fonctionne. Si Cloud Volumes ONTAP est désactivé, le refroidissement s'arrêtera également. Vous bénéficiez ainsi de temps de refroidissement plus longs.



Lorsque Cloud Volumes ONTAP est désactivé, la température de chaque bloc est conservée jusqu'au redémarrage du système. Par exemple, si la température d'un bloc est de 5 lorsque vous éteignez le système, la température est toujours de 5 lorsque vous rallumez le système.

### Configuration de la hiérarchisation des données

Pour obtenir des instructions et une liste des configurations prises en charge, reportez-vous à "[Hiérarchiser les données inactives vers un stockage d'objets à faible coût](#)".

## Gestion du stockage Cloud Volumes ONTAP

La console NetApp offre une gestion simplifiée et avancée du stockage Cloud Volumes ONTAP .



Vous devez créer et supprimer tous les disques et agrégats directement depuis la console. 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 potentiellement générer des frais de fournisseur de cloud redondants.

## Provisionnement du stockage

La console facilite le provisionnement du stockage pour Cloud Volumes ONTAP en achetant des disques et en gérant les agrégats pour vous. Il vous suffit de créer des volumes. Vous pouvez utiliser une option d'allocation avancée pour provisionner vous-même des agrégats, si vous le souhaitez.

### Provisionnement simplifié

Les agrégats fournissent un stockage cloud aux volumes. La console crée des agrégats pour vous lorsque vous lancez une instance et lorsque vous provisionnez des volumes supplémentaires.

Lorsque vous créez un volume, la console effectue l'une des trois opérations suivantes :

- Il place le volume sur un agrégat existant qui dispose de suffisamment d'espace libre.
- Il place le volume sur un agrégat existant en achetant plus de disques pour cet agrégat.

+ Dans le cas d'un agrégat dans AWS qui prend en charge les volumes élastiques, cela augmente également la taille des disques dans un groupe RAID. ["En savoir plus sur la prise en charge des volumes élastiques"](#) .

- Il achète des disques pour un nouvel agrégat et place le volume sur cet agrégat.

La console détermine où placer un nouveau volume en examinant plusieurs facteurs : la taille maximale d'un agrégat, si le provisionnement léger est activé et les seuils d'espace libre pour les agrégats.

### Sélection de la taille du disque pour les agrégats dans AWS

Lorsque la console crée de nouveaux agrégats pour Cloud Volumes ONTAP dans AWS, elle augmente progressivement la taille des disques à mesure que les nombres d'agrégats augmentent pour maximiser la capacité du système avant d'atteindre les limites des disques de données AWS.

Par exemple, la console peut choisir les tailles de disque suivantes :

Nombre total	Taille du disque	Capacité maximale globale
1	500 Gio	3 Tio
4	1 Tio	6 Tio
6	2 Tio	12 Tio



Ce comportement ne s'applique pas aux agrégats qui prennent en charge la fonctionnalité Amazon EBS Elastic Volumes. Les agrégats sur lesquels les volumes élastiques sont activés sont constitués d'un ou deux groupes RAID. Chaque groupe RAID dispose de quatre disques identiques ayant la même capacité. ["En savoir plus sur la prise en charge des volumes élastiques"](#) .

Vous pouvez choisir vous-même la taille du disque en utilisant l'option d'allocation avancée.

## Allocation avancée

Vous pouvez également gérer les agrégats. "[Depuis 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 des capacités

L'administrateur de l'organisation ou du compte peut configurer la console pour vous informer des décisions en matière de capacité de stockage ou pour gérer automatiquement les besoins en capacité pour vous.

Ce comportement est déterminé par le *Mode de gestion de la capacité* sur un agent de console. Le mode de gestion de la capacité affecte tous les systèmes Cloud Volumes ONTAP gérés par cet agent de console. Si vous disposez d'un autre agent de console, il peut être configuré différemment.

### Gestion automatique des capacités

Le mode de gestion de la capacité est défini sur automatique par défaut. Dans ce mode, la console vérifie le ratio d'espace libre toutes les 15 minutes pour déterminer si le ratio d'espace libre tombe en dessous du seuil spécifié. Si davantage de capacité est nécessaire, il lance l'achat de nouveaux disques, supprime les collections de disques inutilisées (agrégats), déplace les volumes entre les agrégats selon les besoins et tente d'empêcher une panne de disque.

Les exemples suivants illustrent le fonctionnement de ce mode :

- Si un agrégat atteint le seuil de capacité et qu'il dispose de suffisamment d'espace pour davantage de disques, la console achète automatiquement de nouveaux disques pour cet agrégat afin que les volumes puissent continuer à croître.

Dans le cas d'un agrégat dans AWS qui prend en charge les volumes élastiques, il augmente également la taille des disques dans un groupe RAID. "[En savoir plus sur la prise en charge des volumes élastiques](#)".

- + \* Si un agrégat atteint le seuil de capacité et qu'il ne peut pas prendre en charge de disques supplémentaires, la console déplace automatiquement un volume de cet agrégat vers un agrégat avec une capacité disponible ou vers un nouvel agrégat.
- + Si la console crée un nouvel agrégat pour le volume, elle 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. L'espace ne peut pas être restitué au fournisseur de cloud dans ce scénario.
- Si un agrégat ne contient aucun volume pendant plus de 12 heures, la console le supprime.

### Gestion des LUN avec gestion automatique de la capacité

La gestion automatique de la capacité de la console ne s'applique pas aux LUN. Lorsqu'il crée un LUN, il désactive la fonction de croissance automatique.

### Gestion manuelle des capacités

Si l'organisation ou l'administrateur du compte définit le mode de gestion de la capacité sur manuel, la console vous informe de prendre les mesures appropriées pour les décisions de capacité. Les mêmes exemples décrits dans le mode automatique s'appliquent au mode manuel, mais c'est à vous d'accepter les actions.

**Apprendre encore plus**

["Apprenez à modifier le mode de gestion de la capacité"](#) .

## **Vitesse d'écriture**

La console NetApp 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, ainsi que les risques et les recommandations lors de l'utilisation d'une vitesse d'écriture élevée.

### **Vitesse d'écriture normale**

Lorsque vous choisissez une vitesse d'écriture normale, les données sont écrites directement sur le disque. Lorsque les données sont écrites directement sur le disque, cela réduit le risque de perte de données en cas de panne système imprévue ou de panne en cascade impliquant une panne système imprévue (paires HA uniquement).

La vitesse d'écriture normale est l'option par défaut.

### **Vitesse d'écriture élevée**

Lorsque vous choisissez une vitesse d'écriture élevée, les données sont mises en mémoire tampon avant d'être écrites sur le disque, ce qui offre des performances d'écriture plus rapides. En raison de cette mise en cache, il existe un risque de perte de données en cas de panne imprévue du système.

La quantité de données pouvant être perdue en cas de panne imprévue du système correspond à la durée des deux derniers points de cohérence. Un point de cohérence est l'acte d'écrire des données mises en mémoire 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). Cependant, les performances du stockage fourni par votre fournisseur de cloud peuvent affecter le temps de traitement du point de cohérence.

### **Quand utiliser une vitesse d'écriture élevée**

Une vitesse d'écriture élevée est un bon choix si des performances d'écriture rapides sont requises pour votre charge de travail et que vous pouvez résister au risque de perte de données en cas de panne système imprévue ou de panne en cascade impliquant une panne système imprévue (paires HA uniquement).

### **Recommandations lors de l'utilisation d'une vitesse d'écriture élevée**

Si vous activez une vitesse d'écriture élevée, vous devez garantir la protection en écriture au niveau de la couche application ou que les applications peuvent tolérer 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 HA dans AWS, vous devez comprendre la différence de niveaux de protection entre un déploiement à zones de disponibilité multiples (AZ) et un déploiement à AZ unique. Le déploiement d'une paire HA sur plusieurs AZ offre davantage de résilience et peut contribuer à atténuer le risque de perte de données.

["En savoir plus sur les paires HA dans AWS"](#) .

## Configurations prenant 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 une vitesse d'écriture normale par défaut.

### AWS

Si vous utilisez un système à nœud unique, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec tous les types d'instances.

À partir de la version 9.8, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec des paires HA lors de l'utilisation de presque tous les types d'instances EC2 pris en charge, à l'exception de m5.xlarge et r5.xlarge.

["En savoir plus sur les instances Amazon EC2 prises en charge par Cloud Volumes ONTAP"](#) .

### Azuré

Si vous utilisez un système à nœud unique, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec tous les types de machines virtuelles.

Si vous utilisez une paire HA, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec plusieurs types de machines virtuelles, à partir de la version 9.8. Aller à la ["Notes de version de Cloud Volumes ONTAP"](#) pour afficher les types de machines virtuelles qui prennent en charge une vitesse d'écriture élevée.

### Google Cloud

Si vous utilisez un système à nœud unique, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec tous les types de machines.

Si vous utilisez une paire HA, Cloud Volumes ONTAP prend en charge une vitesse d'écriture élevée avec plusieurs types de machines virtuelles, à partir de la version 9.13.0. Aller à la ["Notes de version de Cloud Volumes ONTAP"](#) pour afficher les types de machines virtuelles qui prennent en charge une vitesse d'écriture élevée.

["En savoir plus sur 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 ajoutez un nouveau système Cloud Volumes ONTAP et vous pouvez ["modifier la vitesse d'écriture d'un système existant"](#) .

## À quoi s'attendre en cas de perte de données

Si une perte de données se produit en raison d'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.
```

Lorsque cela se produit, Cloud Volumes ONTAP doit pouvoir démarrer et continuer à diffuser des données sans intervention de l'utilisateur.

### Comment arrêter l'accès aux données en cas de perte de données

Si vous êtes préoccupé par la perte de données, que vous souhaitez que les applications cessent de s'exécuter en cas de perte de données et que l'accès aux données reprenne une fois le problème de perte de données 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 doit cesser de diffuser des données (il n'y a aucun impact sur CIFS qui est un protocole sans état). Pour plus de détails, reportez-vous à ["Comment NVFAIL affecte 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 correctement 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
```

## Cache Flash

Certaines configurations Cloud Volumes ONTAP incluent un stockage NVMe local, que Cloud Volumes ONTAP utilise comme *Cache Flash* 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 récemment lues et des métadonnées NetApp . Il est efficace pour les charges de travail à lecture intensive aléatoire, y compris les bases de données, la messagerie électronique et les services de fichiers.

### Configurations prises en charge

Flash Cache est pris en charge avec des configurations Cloud Volumes ONTAP spécifiques. Afficher les configurations prises en charge dans le "[Notes de version de Cloud Volumes ONTAP](#)"

### Limites

- Lors de la configuration de Flash Cache pour Cloud Volumes ONTAP 9.12.0 ou version antérieure dans AWS, la compression doit être désactivée sur tous les volumes pour profiter des améliorations des performances de Flash Cache. Lorsque vous déployez ou effectuez une mise à niveau vers Cloud Volumes ONTAP 9.12.1 ou une version ultérieure, vous n'avez pas besoin de désactiver la compression.

Ignorez la sélection des paramètres d'efficacité de stockage lors de la création d'un volume à partir de la console NetApp , ou créez un volume, puis "[désactiver la compression des données à l'aide de la CLI](#)" .

- Le réchauffement du cache après un redémarrage n'est pas pris en charge avec Cloud Volumes ONTAP.

## En savoir plus sur le stockage WORM sur Cloud Volumes ONTAP

Vous pouvez activer le stockage WORM (Write Once, Read Many) sur un système Cloud Volumes ONTAP pour conserver les fichiers sous une forme non modifiée pendant une période de conservation spécifiée. Le stockage Cloud WORM est alimenté par la technologie SnapLock , ce qui signifie que les fichiers WORM sont protégés au niveau du fichier.

La fonctionnalité WORM est disponible pour une utilisation avec les abonnements BYOL (Bring Your Own License) et Marketplace pour vos licences sans frais supplémentaires. Contactez votre représentant commercial NetApp pour ajouter WORM à votre licence actuelle.

### Comment fonctionne le stockage WORM

Une fois qu'un fichier a été enregistré dans le stockage WORM, il ne peut pas être modifié, même après l'expiration de la période de conservation. Une horloge inviolable détermine quand la période de conservation d'un fichier WORM est écoulée.

Une fois la période de conservation écoulée, vous êtes responsable de la suppression de tous les fichiers dont vous n'avez plus besoin.

## Activation du stockage WORM

La manière dont vous activez le stockage WORM dépend de la version de Cloud Volumes ONTAP que vous utilisez.

### Version 9.10.1 et ultérieures

À partir de Cloud Volumes ONTAP 9.10.1, vous avez la possibilité d'activer ou de désactiver WORM au niveau du volume.

Lorsque vous ajoutez un système Cloud Volumes ONTAP, vous êtes invité à activer ou désactiver le stockage WORM :

- Si vous activez le stockage WORM lors de l'ajout d'un système, chaque volume que vous créez à partir de la console NetApp a WORM activé. Mais vous pouvez utiliser ONTAP System Manager ou l' ONTAP CLI pour créer des volumes sur lesquels WORM est désactivé.
- Si vous désactivez le stockage WORM lors de l'ajout d'un système, chaque volume que vous créez à partir de la console, ONTAP System Manager ou de l' ONTAP CLI a WORM désactivé.

### Version 9.10.0 et antérieures

Vous pouvez activer le stockage WORM sur un système Cloud Volumes ONTAP lorsque vous ajoutez un nouveau système. Chaque volume que vous créez à partir de la console a WORM activé. Vous ne pouvez pas désactiver le stockage WORM sur des volumes individuels.

## Validation des fichiers dans 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 valider automatiquement des fichiers sur WORM. Vous pouvez également utiliser un fichier WORM pouvant être ajouté pour conserver les données écrites de manière 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 les instructions, reportez-vous à la "[Documentation ONTAP sur SnapLock](#)".

## Activation de WORM sur un système Cloud Volumes ONTAP

Vous pouvez activer le stockage WORM lors de la création d'un système Cloud Volumes ONTAP sur la console. Vous pouvez également activer WORM sur un système si WORM n'est pas activé sur celui-ci lors de la création. Une fois activé, vous ne pouvez pas désactiver WORM.

### À propos de cette tâche

- WORM est pris en charge sur ONTAP 9.10.1 et versions ultérieures.
- WORM avec sauvegarde est pris en charge sur ONTAP 9.11.1 et versions ultérieures.

### Étapes

1. Sur la page **Systèmes**, double-cliquez sur le nom du système sur lequel vous souhaitez activer WORM.
2. Dans l'onglet Présentation, cliquez sur le panneau Fonctionnalités, puis cliquez sur l'icône en forme de crayon à côté de **WORM**.

Si WORM est déjà activé sur le système, l'icône en forme de crayon est désactivée.

3. Sur la page **WORM**, définissez la période de conservation de l'horloge de conformité du cluster.

Pour plus d'informations, reportez-vous à la "[Documentation ONTAP : Initialiser l'horloge de conformité](#)".

4. Cliquez sur **Définir**.

### Après avoir terminé

Vous pouvez vérifier l'état de **WORM** dans le panneau Fonctionnalités. Une fois WORM activé, la licence SnapLock est automatiquement installée sur le cluster. Vous pouvez afficher la licence SnapLock sur ONTAP System Manager.

### Suppression des fichiers WORM

Vous pouvez supprimer les fichiers WORM pendant la période de conservation à l'aide de la fonction de suppression privilégiée.

Pour les instructions, reportez-vous à la "[Documentation ONTAP](#)".

### WORM et hiérarchisation des données

Lorsque vous créez un nouveau système Cloud Volumes ONTAP 9.8 ou version ultérieure, vous pouvez activer à la fois la hiérarchisation des données et le stockage WORM. L'activation de la hiérarchisation des données avec le stockage WORM vous permet de hiérarchiser les données vers un magasin d'objets dans le cloud.

Vous devez comprendre les points suivants concernant l'activation de la hiérarchisation des données et du stockage WORM :

- Les données hiérarchisées vers le stockage d'objets n'incluent pas la fonctionnalité ONTAP WORM. Pour garantir la fonctionnalité WORM de bout en bout, vous devez configurer correctement les autorisations du bucket.
- Les données hiérarchisées vers le stockage d'objets ne comportent pas la fonctionnalité WORM, ce qui signifie que techniquement, toute personne disposant d'un accès complet aux buckets et aux conteneurs peut supprimer les objets hiérarchisés par ONTAP.
- Le retour ou la rétrogradation vers Cloud Volumes ONTAP 9.8 est bloqué après l'activation de WORM et de la hiérarchisation.

### Limites

- Le stockage WORM dans Cloud Volumes ONTAP fonctionne selon un modèle « administrateur de stockage de confiance ». Bien que les fichiers WORM soient protégés contre toute altération ou modification, les volumes peuvent être supprimés par un administrateur de cluster même si ces volumes contiennent des données WORM non expirées.
- Outre le modèle d'administrateur de stockage de confiance, le stockage WORM dans Cloud Volumes ONTAP fonctionne également implicitement sous un modèle « d'administrateur cloud de confiance ». Un administrateur cloud peut supprimer les données WORM avant leur date d'expiration en supprimant ou en modifiant le stockage cloud directement auprès du fournisseur cloud.

### Lien connexe

- "[Créer des copies instantanées inviolables pour le stockage WORM](#)"

# Paires à haute disponibilité

## En savoir plus sur les paires Cloud Volumes ONTAP HA dans AWS

Une configuration haute disponibilité (HA) Cloud Volumes ONTAP offre 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 HA

Dans AWS, les configurations Cloud Volumes ONTAP HA incluent les composants suivants :

- Deux nœuds Cloud Volumes ONTAP dont les données sont mises en miroir de manière synchrone entre eux.
- Une instance de médiateur qui fournit un canal de communication entre les nœuds pour aider aux processus de prise de contrôle et de restitution du stockage.

### Médiateur

Voici quelques détails clés sur l'instance de médiateur dans AWS :

#### Type d'instance

t3-micro

#### Disques

Deux disques st1 de 8 Gio et 4 Gio

#### Système opérateur

Debian 11



Pour Cloud Volumes ONTAP 9.10.0 et versions antérieures, Debian 10 a été installé sur le médiateur.

### Mises à niveau

Lorsque vous mettez à niveau Cloud Volumes ONTAP, la console NetApp met également à jour l'instance du médiateur selon les besoins.

### Accès à l'instance

Lorsque vous créez une paire Cloud Volumes ONTAP HA à partir de la console, vous êtes invité à fournir une paire de clés pour l'instance de médiateur. Vous pouvez utiliser cette paire de clés pour l'accès SSH en utilisant le `admin` utilisateur.

### Agents tiers

Les agents tiers ou les extensions de machine virtuelle ne sont pas pris en charge sur l'instance du médiateur.

### Reprise et restitution du stockage

Si un nœud tombe en panne, l'autre nœud peut fournir des données à son partenaire afin de 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 sur le partenaire.

Après le redémarrage du nœud, le partenaire doit resynchroniser les données avant de pouvoir renvoyer le stockage. Le temps nécessaire à la resynchronisation des données dépend de la quantité de données modifiées pendant que le nœud était en panne.

La prise de contrôle du stockage, la resynchronisation et la restitution sont toutes automatiques par défaut. Aucune action de l'utilisateur n'est requise.

## RPO et RTO

Une configuration HA maintient la haute disponibilité de vos données comme suit :

- L'objectif de point de récupération (RPO) est de 0 seconde. Vos données sont cohérentes sur le plan transactionnel, sans aucune perte de données.
- L'objectif de temps de récupération (RTO) est de 120 secondes. En cas de panne, les données devraient être disponibles en 120 secondes ou moins.

## Modèles de déploiement HA

Vous pouvez garantir la haute disponibilité de vos données en déployant une configuration HA sur plusieurs zones de disponibilité (AZ) ou dans une seule zone de disponibilité (AZ). Vous devriez examiner plus en détail chaque configuration pour choisir celle qui correspond le mieux à vos besoins.

### Plusieurs zones de disponibilité

Le déploiement d'une configuration HA dans plusieurs zones de disponibilité (AZ) garantit une haute disponibilité de vos données en cas de panne d'une AZ ou d'une instance qui exécute un nœud Cloud Volumes ONTAP . Vous devez comprendre comment les adresses IP NAS impactent l'accès aux données et le basculement du stockage.

### Accès aux données NFS et CIFS

Lorsqu'une configuration HA est répartie sur plusieurs zones de disponibilité, les *adresses IP flottantes* permettent l'accès du client NAS. Les adresses IP flottantes, qui doivent être en dehors des blocs CIDR pour tous les VPC de la région, peuvent migrer entre les nœuds en cas de panne. Ils ne sont pas accessibles nativement aux clients qui se trouvent en dehors du VPC, sauf si vous ["configurer une passerelle de transit AWS"](#) .

Si vous ne pouvez pas configurer une passerelle de transit, des adresses IP privées sont disponibles pour les clients NAS qui se trouvent en dehors du VPC. Cependant, ces adresses IP sont statiques : elles ne peuvent pas basculer entre les nœuds.

Vous devez examiner les exigences relatives aux adresses IP flottantes et aux tables de routage avant de déployer une configuration HA sur plusieurs zones de disponibilité. Vous devez spécifier les adresses IP flottantes lorsque vous déployez la configuration. Les adresses IP privées sont créées automatiquement.

Pour plus d'informations, reportez-vous à ["Exigences réseau AWS pour Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité"](#) .

### Accès aux données iSCSI

La communication de données entre VPC n'est pas un problème puisque iSCSI n'utilise pas d'adresses IP flottantes.

## Reprise et restitution pour iSCSI

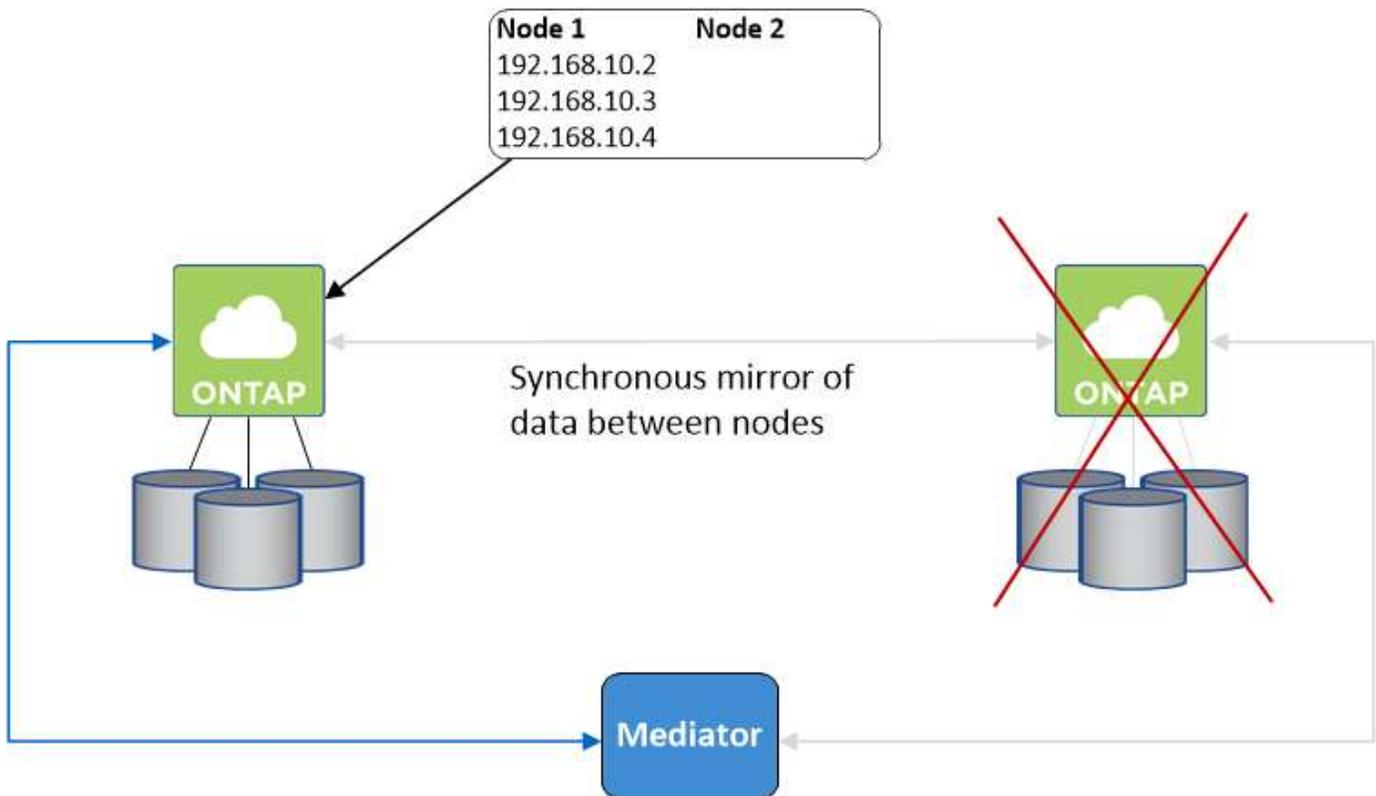
Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multi-chemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés actifs et non optimisés.



Pour plus d'informations sur les configurations d'hôte spécifiques qui prennent en charge ALUA, reportez-vous à la "[Outil de matrice d'interopérabilité NetApp](#)" et le "[Guide des hôtes SAN et des clients cloud](#)" pour votre système d'exploitation hôte.

## Reprise et restitution pour NAS

Lorsqu'une prise de contrôle 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 se déplace vers l'autre nœud. L'image suivante illustre la prise de contrôle du stockage dans une configuration NAS utilisant des adresses IP flottantes. Si le nœud 2 tombe en panne, l'adresse IP flottante du nœud 2 est déplacée vers le nœud 1.



Les adresses IP de données NAS utilisées pour l'accès VPC externe ne peuvent pas migrer entre les nœuds en cas de panne. Si un nœud est hors ligne, vous devez remonter manuellement les volumes sur les clients extérieurs au VPC en utilisant l'adresse IP de l'autre nœud.

Une fois le nœud défaillant remis en ligne, remontez les clients sur les volumes en utilisant l'adresse IP d'origine. Cette étape est nécessaire pour éviter de transférer des données inutiles entre deux nœuds HA, ce qui peut entraîner un impact significatif sur les performances et la stabilité.

Vous pouvez localiser l'adresse IP correcte à partir de la console en sélectionnant le volume et en cliquant sur **Commande de montage**.

## 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 si une instance qui exécute un nœud Cloud Volumes ONTAP échoue. Toutes les données sont nativement accessibles depuis l'extérieur du VPC.

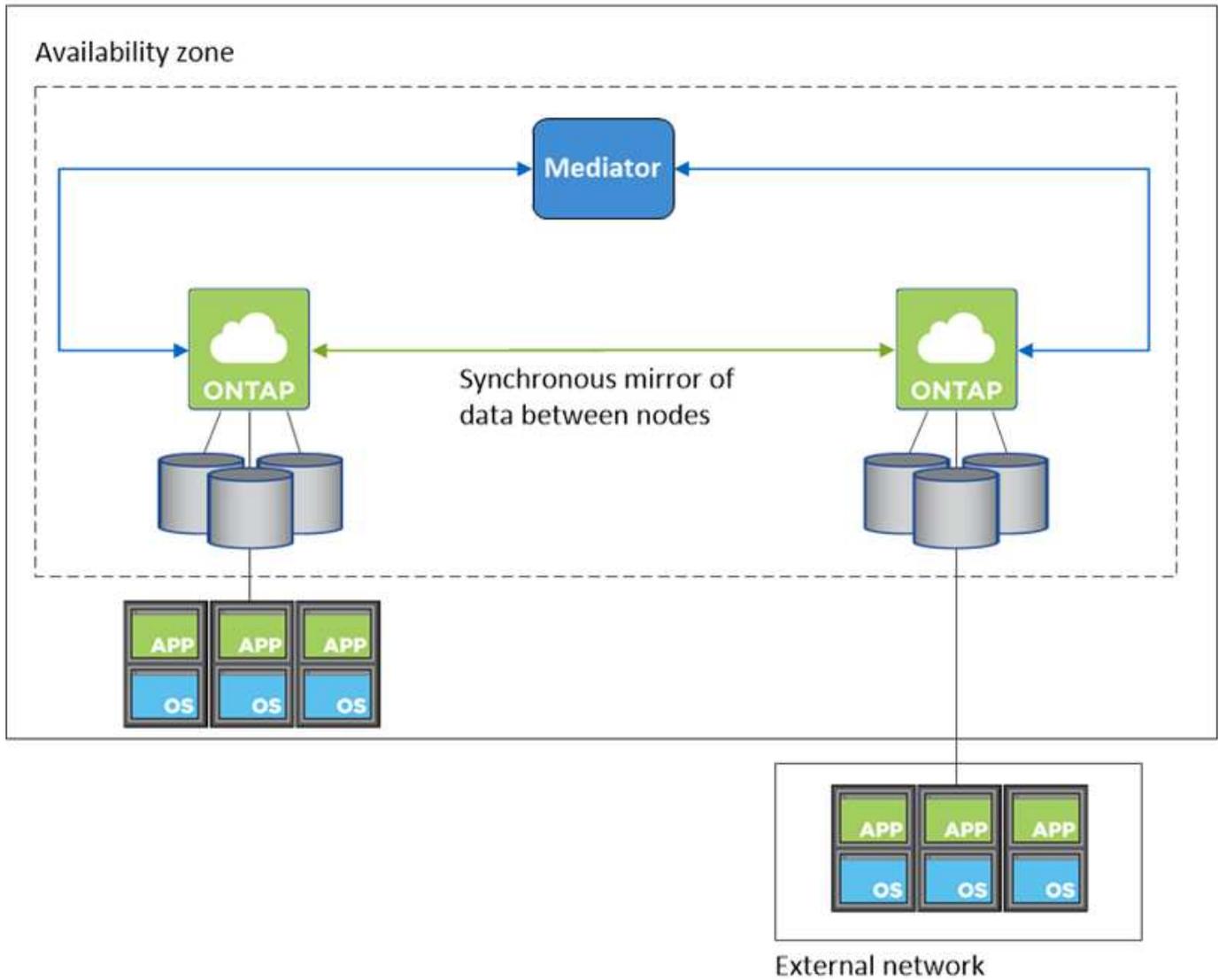


La console crée un "[Documentation AWS : Groupe de placement de spread AWS](#)" et lance les deux nœuds HA dans ce groupe de placement. Le groupe de placement réduit le risque de pannes simultanées en répartissant les instances sur des matériels sous-jacents distincts. Cette fonctionnalité améliore la redondance du point de vue du calcul et non du point de vue des pannes de disque.

## Accès aux données

Étant donné que cette configuration se trouve dans une seule zone de disponibilité, elle ne nécessite pas d'adresses IP flottantes. Vous pouvez utiliser la même adresse IP pour l'accès aux données depuis l'intérieur du VPC et depuis l'extérieur du VPC.

L'image suivante montre une configuration HA dans une seule AZ. Les données sont accessibles depuis l'intérieur du VPC et depuis l'extérieur du VPC.



### Prise de contrôle et restitution

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multi-chemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés actifs et non optimisés.



Pour plus d'informations sur les configurations d'hôte spécifiques qui prennent en charge ALUA, reportez-vous à la "[Outil de matrice d'interopérabilité NetApp](#)" et le "[Guide des hôtes SAN et des clients cloud](#)" pour votre système d'exploitation hôte.

Pour les configurations NAS, les adresses IP de données peuvent migrer entre les nœuds HA en cas de panne. Cela garantit l'accès du client au stockage.

### Zones locales AWS

Les zones locales AWS sont un déploiement d'infrastructure où le stockage, le calcul, la base de données et d'autres services AWS sélectionnés sont situés à proximité de grandes villes et de zones industrielles. Avec AWS Local Zones, vous pouvez rapprocher les services AWS de vous, ce qui améliore la latence de vos charges de travail et maintient les bases de données localement. Sur Cloud Volumes ONTAP,

Vous pouvez déployer une configuration AZ unique ou multiple dans les zones locales AWS.



Les zones locales AWS sont prises en charge lors de l'utilisation de la console en modes standard et privé. À l'heure actuelle, les zones locales AWS ne sont pas prises en charge en mode restreint.

### Exemples de configurations de zone locale AWS

Cloud Volumes ONTAP dans AWS prend en charge uniquement le mode haute disponibilité (HA) dans une seule zone de disponibilité. Les déploiements à nœud unique ne sont pas pris en charge.

Cloud Volumes ONTAP ne prend pas en charge la hiérarchisation des données, la hiérarchisation du cloud et les instances non qualifiées dans les zones locales AWS.

Voici quelques exemples de configurations :

- Zone de disponibilité unique : les deux nœuds du cluster et le médiateur se trouvent dans la même zone locale.
- Zones de disponibilité multiples Dans les configurations à zones de disponibilité multiples, il existe trois instances, deux nœuds et un médiateur. Une instance sur trois doit se trouver dans une zone distincte. Vous pouvez choisir comment vous souhaitez configurer cela.

Voici trois exemples de configurations :

- Chaque nœud de cluster se trouve dans une zone locale différente et le médiateur dans une zone de disponibilité publique.
- Un nœud de cluster dans une zone locale, le médiateur dans une zone locale et le deuxième nœud de cluster se trouve dans une zone de disponibilité.
- Chaque nœud de cluster et le médiateur se trouvent dans des zones locales distinctes.

### Types de disques et d'instances pris en charge

Le seul type de disque pris en charge est GP2. Les familles de types d'instances EC2 suivantes avec des tailles xlarge à 4xlarge sont actuellement prises en charge :

- M5
- C5
- C5d
- R5
- R5d



Cloud Volumes ONTAP prend en charge uniquement ces configurations. La sélection de types de disques non pris en charge ou d'instances non qualifiées dans la configuration de la zone locale AWS peut entraîner l'échec du déploiement. La hiérarchisation des données vers AWS S3 n'est pas disponible dans les zones locales AWS en raison du manque de connectivité.

["Documentation AWS : types d'instances EC2 dans les zones locales"](#) .

## Comment fonctionne le stockage dans une paire HA

Contrairement à un cluster ONTAP, le stockage dans une paire Cloud Volumes ONTAP HA n'est pas partagé entre les nœuds. Au lieu de cela, les données sont mises en miroir de manière synchrone entre les nœuds afin que les données soient disponibles en cas de panne.

### Allocation de stockage

Lorsque vous créez un nouveau volume et que des disques supplémentaires sont requis, la console 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, la console 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 fournissent des 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 du nœud actif.



Vous pouvez configurer une configuration active-active uniquement lorsque vous utilisez la console dans la vue Système de stockage.

### Attentes de performance

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 HA qui diffusent des données à partir d'un seul nœud, les performances de lecture sont comparables aux performances de lecture d'une configuration à nœud unique, tandis que les performances d'écriture sont inférieures.
- Pour les configurations HA qui diffusent des données à partir des deux nœuds, les performances de lecture sont supérieures à celles d'une configuration à nœud unique, et les performances d'écriture sont identiques ou supérieures.

Pour plus de détails sur les performances de Cloud Volumes ONTAP, reportez-vous à "[Performances](#)".

### 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 circule entre les deux nœuds, ce qui réduit les performances.



Si vous déplacez un volume entre des nœuds d'une paire HA, vous devez remonter le volume en utilisant l'adresse IP de l'autre nœud. Dans le cas contraire, vous risquez de constater une diminution des performances. Si les clients prennent en charge les références NFSv4 ou la redirection de dossiers pour CIFS, vous pouvez activer ces fonctionnalités sur les systèmes Cloud Volumes ONTAP pour éviter de remonter le volume. Pour plus de détails, reportez-vous à la documentation ONTAP.

Vous pouvez facilement identifier l'adresse IP correcte grâce à l'option *Mount Command* sous le panneau de gestion des volumes.

## Volume Actions

---

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

## Protection Actions

---

## Advanced Actions

---

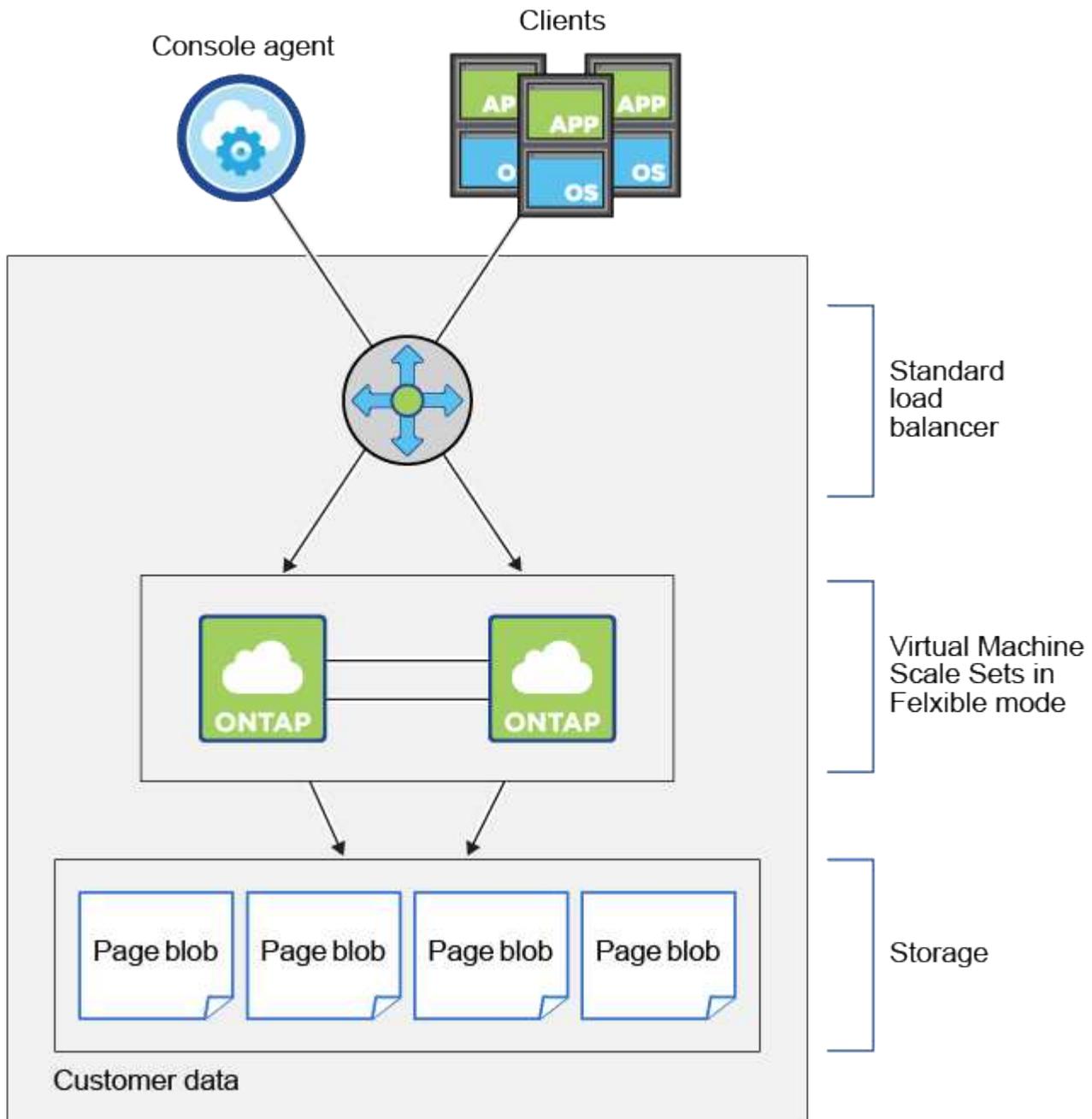
### En savoir plus sur les paires Cloud Volumes ONTAP HA dans Azure

Une paire haute disponibilité (HA) Cloud Volumes ONTAP offre une fiabilité d'entreprise et des opérations continues en cas de panne dans votre environnement cloud. Dans Azure, le stockage est partagé entre les deux nœuds.

#### Composants HA

## Configuration de zone de disponibilité unique HA avec des blobs de pages

Une configuration d'objet blob de pages Cloud Volumes ONTAP HA dans Azure inclut les composants suivants :



### Resource group

Notez les points suivants concernant les composants Azure que la console NetApp déploie pour vous :

#### Équilibreur de charge standard Azure

L'équilibreur de charge gère le trafic entrant vers la paire Cloud Volumes ONTAP HA.

#### Machines virtuelles dans des zones de disponibilité uniques

À partir de Cloud Volumes ONTAP 9.15.1, vous pouvez créer et gérer des machines virtuelles (VM)

hétérogènes dans une seule zone de disponibilité (AZ). Vous pouvez déployer des nœuds haute disponibilité (HA) dans des domaines de pannes distincts au sein de la même zone de disponibilité, garantissant ainsi une disponibilité optimale. Pour en savoir plus sur le mode d'orchestration flexible qui permet cette fonctionnalité, reportez-vous à la "[Documentation Microsoft Azure : Ensembles de machines virtuelles identiques](#)".

## Disques

Les données client résident sur des blobs de page de stockage Premium. Chaque nœud a accès au stockage de l'autre nœud. Un stockage supplémentaire est également nécessaire pour "[données de démarrage, racine et de base](#)".

## Comptes de stockage

- Un compte de stockage est requis pour les disques gérés.
- Un ou plusieurs comptes de stockage sont requis pour les blobs de page Stockage Premium, car la limite de capacité du disque par compte de stockage est atteinte.

["Documentation Microsoft Azure : Objectifs d'évolutivité et de performances du stockage Azure pour les comptes de stockage"](#).

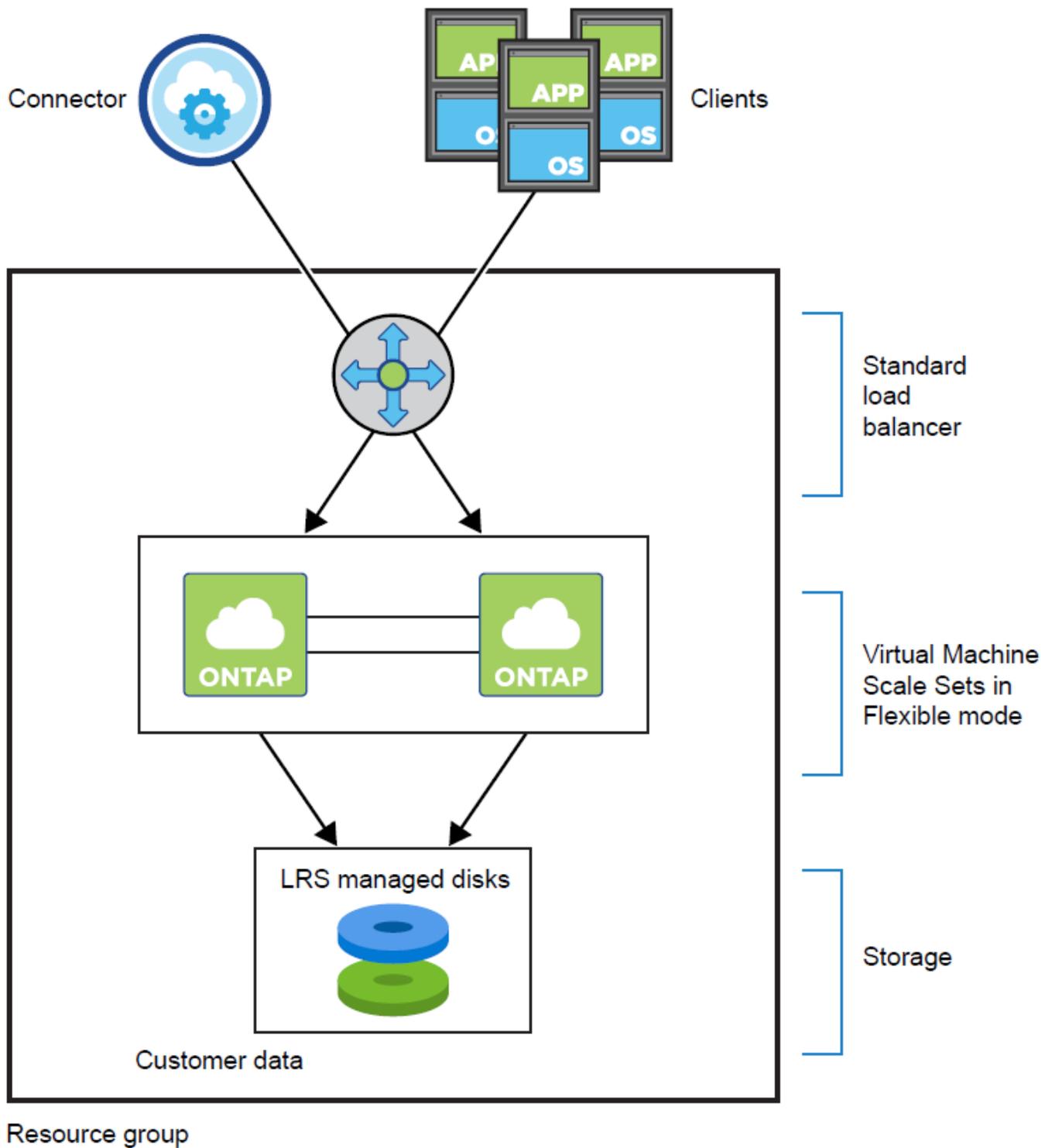
- Un compte de stockage est requis pour la hiérarchisation des données vers le stockage Azure Blob.
- À partir de Cloud Volumes ONTAP 9.7, les comptes de stockage créés par la console pour les paires HA sont des comptes de stockage v2 à usage général.
- Vous pouvez activer une connexion HTTPS à partir d'une paire Cloud Volumes ONTAP 9.7 HA vers des comptes de stockage Azure lors de l'ajout d'un système Cloud Volumes ONTAP. 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 le système.



À partir de Cloud Volumes ONTAP 9.15.0P1, les blobs de pages Azure ne sont plus pris en charge pour les nouveaux déploiements de paires haute disponibilité. Si vous utilisez actuellement des blobs de pages Azure dans des déploiements de paires haute disponibilité existants, vous pouvez migrer vers des types d'instances de machine virtuelle plus récents dans les machines virtuelles des séries Edsv4 et Edsv5. "[En savoir plus sur les configurations prises en charge dans Azure](#)".

## Configuration de zone de disponibilité unique HA avec disques gérés partagés

Une configuration de zone de disponibilité unique Cloud Volumes ONTAP HA exécutée sur un disque géré partagé comprend les composants suivants :



Notez les points suivants concernant les composants Azure que la console déploie pour vous :

### Équilibreur de charge standard Azure

L'équilibreur de charge gère le trafic entrant vers la paire Cloud Volumes ONTAP HA.

### Machines virtuelles dans des zones de disponibilité uniques

À partir de Cloud Volumes ONTAP 9.15.1, vous pouvez créer et gérer des machines virtuelles (VM) hétérogènes dans une seule zone de disponibilité (AZ). Vous pouvez déployer des nœuds haute disponibilité (HA) dans des domaines de pannes distincts au sein de la même zone de disponibilité, garantissant ainsi une disponibilité optimale. Pour en savoir plus sur le mode d'orchestration flexible qui

permet cette fonctionnalité, reportez-vous à la ["Documentation Microsoft Azure : Ensembles de machines virtuelles identiques"](#) .

Le déploiement zonal utilise des disques gérés Premium SSD v2 lorsque les conditions suivantes sont remplies :

- La version de Cloud Volumes ONTAP est 9.15.1 ou ultérieure.
- La région et la zone sélectionnées prennent en charge les disques gérés Premium SSD v2. Pour plus d'informations sur les régions prises en charge, reportez-vous à ["Site Web Microsoft Azure : produits disponibles par région"](#) .
- L'abonnement est enregistré auprès de Microsoft ["Fonctionnalité Microsoft.Compute/VMOrchestratorZonalMultiFD"](#) .

## Disques

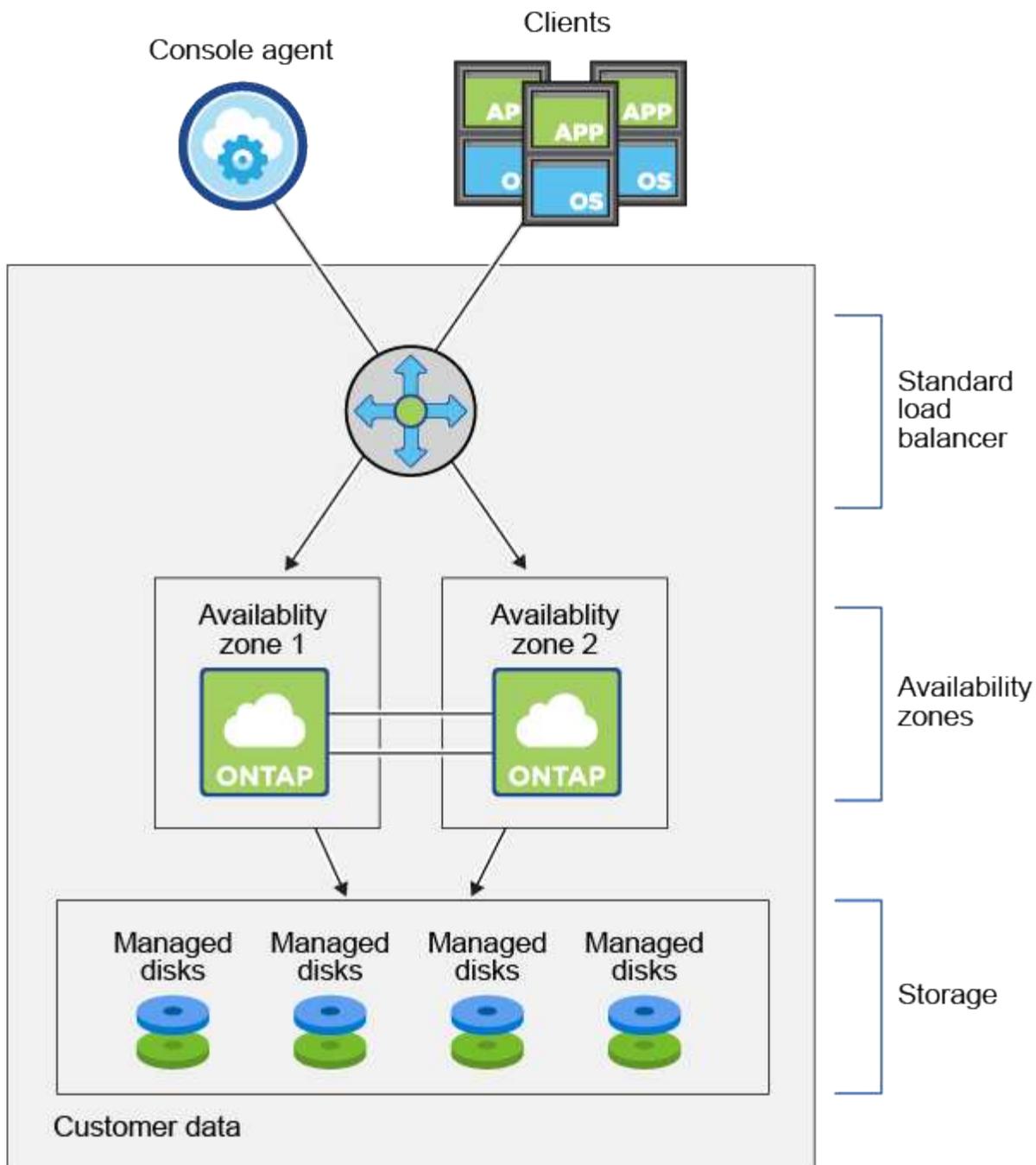
Les données client résident sur des disques gérés par stockage localement redondant (LRS). Chaque nœud a accès au stockage de l'autre nœud. Un stockage supplémentaire est également nécessaire pour ["données de démarrage, racine, racine partenaire, cœur et NVRAM"](#) .

## Comptes de stockage

Les comptes de stockage sont utilisés pour les déploiements basés sur des disques gérés afin de gérer les journaux de diagnostic et la hiérarchisation du stockage blob.

## Configuration de zones de disponibilité multiples HA

Une configuration de zone de disponibilité multiple Cloud Volumes ONTAP HA dans Azure inclut les composants suivants :



## Resource group

Notez les points suivants concernant les composants Azure que la console déploie pour vous :

### Équilibreur de charge standard Azure

L'équilibreur de charge gère le trafic entrant vers la paire Cloud Volumes ONTAP HA.

### Zones de disponibilité

La configuration de zones de disponibilité multiples HA utilise un modèle de déploiement dans lequel deux nœuds Cloud Volumes ONTAP sont déployés dans différentes zones de disponibilité, garantissant que les nœuds se trouvent dans des domaines de pannes différents pour assurer la redondance et la disponibilité. Pour savoir comment les ensembles de machines virtuelles identiques en mode d'orchestration flexible peuvent utiliser les zones de disponibilité dans Azure, reportez-vous à la ["Documentation Microsoft Azure"](#) :

[Créer un groupe de machines virtuelles identiques utilisant des zones de disponibilité](#) .

## Disques

Les données client résident sur des disques gérés par stockage redondant par zone (ZRS). Chaque nœud a accès au stockage de l'autre nœud. Un stockage supplémentaire est également nécessaire pour "[données de démarrage, racine, racine partenaire et données de base](#)" .

## Comptes de stockage

Les comptes de stockage sont utilisés pour les déploiements basés sur des disques gérés afin de gérer les journaux de diagnostic et la hiérarchisation du stockage blob.

## RPO et RTO

Une configuration HA maintient une haute disponibilité de vos données comme suit :

- L'objectif de point de récupération (RPO) est de 0 seconde. Vos données sont cohérentes sur le plan transactionnel, sans aucune perte de données.
- L'objectif de temps de récupération (RTO) est de 120 secondes. En cas de panne, les données devraient être disponibles en 120 secondes ou moins.

## Reprise et restitution du stockage

Semblable à un cluster ONTAP physique, le stockage dans une paire Azure HA est partagé entre les nœuds. Les connexions au stockage du partenaire permettent à chaque nœud d'accéder au stockage de l'autre en cas de *prise de contrôle*. Les mécanismes de basculement du chemin réseau garantissent que les clients et les hôtes continuent de communiquer avec le nœud survivant. Le partenaire *rend* le stockage lorsque le nœud est remis en ligne.

Pour les configurations NAS, les adresses IP de données migrent automatiquement entre les nœuds HA en cas de panne.

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multi-chemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés actifs et non optimisés.



Pour plus d'informations sur les configurations d'hôte spécifiques qui prennent en charge ALUA, reportez-vous à la "[Outil de matrice d'interopérabilité NetApp](#)" et le "[Guide des hôtes SAN et des clients cloud](#)" pour votre système d'exploitation hôte.

La prise de contrôle du stockage, la resynchronisation et la restitution sont toutes 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 fournissent des données aux clients, ou comme configuration active-passive, dans laquelle le nœud passif répond aux demandes de données uniquement s'il a repris le stockage du nœud actif.

## En savoir plus sur les paires Cloud Volumes ONTAP HA dans Google Cloud

Une configuration haute disponibilité (HA) Cloud Volumes ONTAP offre 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 HA

Les configurations Cloud Volumes ONTAP HA dans Google Cloud incluent les composants suivants :

- Deux nœuds Cloud Volumes ONTAP dont les données sont mises en miroir de manière synchrone entre eux.
- Une instance de médiateur qui fournit un canal de communication entre les nœuds pour aider aux processus de prise de contrôle et de restitution du stockage.
- Une zone ou trois zones (recommandé).

Si vous choisissez trois zones, les deux nœuds et le médiateur se trouvent dans des zones Google Cloud distinctes.

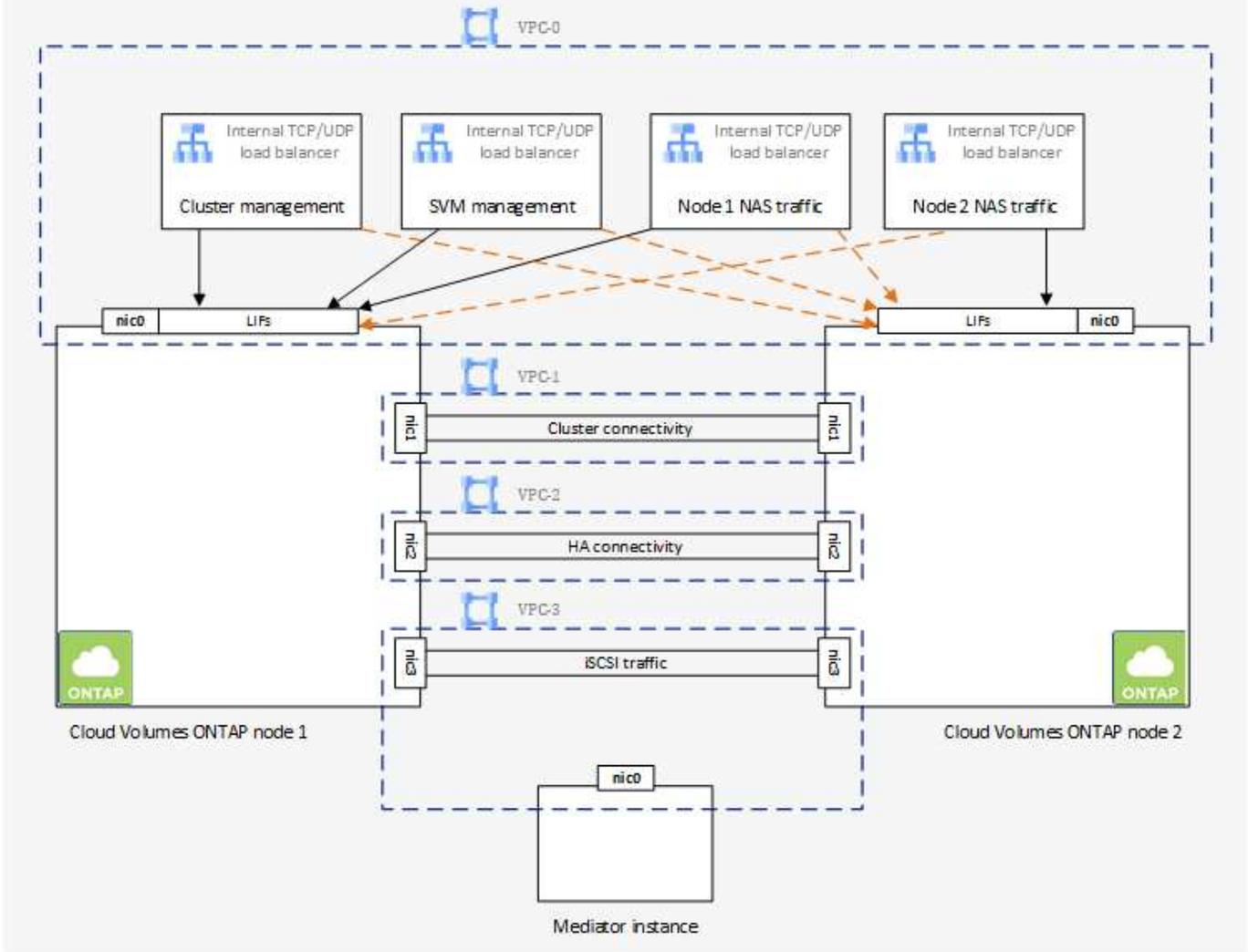
- Quatre clouds privés virtuels (VPC).

La configuration utilise quatre VPC car GCP exige que chaque interface réseau réside dans un réseau VPC distinct.

- Quatre équilibreurs de charge internes Google Cloud (TCP/UDP) qui gèrent le trafic entrant vers la paire Cloud Volumes ONTAP HA.

["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 Cloud Volumes ONTAP HA et ses composants :



### Médiateur

Voici quelques détails clés sur l'instance de médiateur dans Google Cloud :

### Type d'instance

e2-micro (une instance f1-micro a été utilisée précédemment)

### Disques

Deux disques persistants standard de 10 Gio chacun

### Système opéracteur

Debian 11



Pour Cloud Volumes ONTAP 9.10.0 et versions antérieures, Debian 10 a été installé sur le médiateur.

### Mises à niveau

Lorsque vous mettez à niveau Cloud Volumes ONTAP, la console NetApp met également à jour l'instance du médiateur selon les besoins.

## Accès à l'instance

Pour Debian, l'utilisateur 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 les privilèges root.

## Agents tiers

Les agents tiers ou les extensions de machine virtuelle ne sont pas pris en charge sur l'instance du médiateur.

## Reprise et restitution du stockage

Si un nœud tombe en panne, l'autre nœud peut fournir des données à son partenaire afin de 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 sur le partenaire.

Après le redémarrage du nœud, le partenaire doit resynchroniser les données avant de pouvoir renvoyer le stockage. Le temps nécessaire à la resynchronisation des données dépend de la quantité de données modifiées pendant que le nœud était en panne.

La prise de contrôle du stockage, la resynchronisation et la restitution sont toutes automatiques par défaut. Aucune action de l'utilisateur n'est requise.

## RPO et RTO

Une configuration HA maintient une haute disponibilité de vos données comme suit :

- L'objectif de point de récupération (RPO) est de 0 seconde.

Vos données sont cohérentes sur le plan transactionnel, sans aucune perte de données.

- L'objectif de temps de récupération (RTO) est de 120 secondes.

En cas de panne, les données devraient être disponibles en 120 secondes ou moins.

## Modèles de déploiement HA

Vous pouvez garantir la haute disponibilité de vos données en déployant une configuration HA dans plusieurs zones ou dans une seule zone.

### Zones multiples (recommandé)

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

### Zone unique

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

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

## Comment fonctionne le stockage dans une paire HA

Contrairement à un cluster ONTAP , le stockage dans une paire Cloud Volumes ONTAP HA dans GCP n'est pas partagé entre les nœuds. Au lieu de cela, les données sont mises en miroir de manière synchrone entre les nœuds afin que les données soient disponibles en cas de panne.

### Allocation de stockage

Lorsque vous créez un nouveau volume et que des disques supplémentaires sont requis, la console 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, la console 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 fournissent des 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 du nœud actif.

### Attentes de performances pour une configuration HA

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 HA qui diffusent des données à partir d'un seul nœud, les performances de lecture sont comparables aux performances de lecture d'une configuration à nœud unique, tandis que les performances d'écriture sont inférieures.
- Pour les configurations HA qui diffusent des données à partir des deux nœuds, les performances de lecture sont supérieures à celles d'une configuration à nœud unique, et les performances d'écriture sont identiques ou supérieures.

Pour plus de détails sur les performances de Cloud Volumes ONTAP , reportez-vous à "[Performances](#)".

### 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 circule entre les deux nœuds, ce qui réduit les performances.



Si vous déplacez un volume entre des nœuds d'une paire HA, vous devez remonter le volume en utilisant l'adresse IP de l'autre nœud. Dans le cas contraire, vous risquez de constater une diminution des performances. Si les clients prennent en charge les références NFSv4 ou la redirection de dossiers pour CIFS, vous pouvez activer ces fonctionnalités sur les systèmes Cloud Volumes ONTAP pour éviter de remonter le volume. Pour plus de détails, reportez-vous à la documentation ONTAP .

Vous pouvez localiser l'adresse IP correcte à partir de la console en sélectionnant le volume et en cliquant sur **Commande de montage**.

## Volume Actions

---

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

## Protection Actions

---

## Advanced Actions

---

### Liens connexes

- ["En savoir plus sur les exigences de mise en réseau"](#)
- ["Découvrez comment démarrer avec GCP"](#)

### Opérations indisponibles lorsqu'un nœud de la paire Cloud Volumes ONTAP HA est hors ligne

Lorsqu'un nœud d'une paire HA n'est pas disponible, l'autre nœud fournit des données à son partenaire pour fournir un service de données continu. C'est ce qu'on appelle la *prise*

de contrôle du stockage. Plusieurs actions ne sont pas disponibles tant que la restitution en stockage n'est pas terminée.



Lorsqu'un nœud d'une paire HA n'est pas disponible, l'état du système dans la console NetApp est *Dégradé*.

Les actions suivantes ne sont pas disponibles à partir de la prise de contrôle du stockage :

- Enregistrement du support
- Modifications de licence
- Modifications du type d'instance ou de machine virtuelle
- Modifications 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 la restitution du stockage terminée et l'état du système redevient normal.

## En savoir plus sur le cryptage des données et la protection contre les ransomwares de Cloud Volumes ONTAP

Cloud Volumes ONTAP prend en charge le cryptage des données et offre une protection contre les virus et les ransomwares.

### Chiffrement des données au repos

Cloud Volumes ONTAP prend en charge les technologies de chiffrement suivantes :

- Solutions de chiffrement NetApp (NVE et NAE)
- Service de gestion des clés AWS
- Chiffrement du service de stockage Azure
- Cryptage par défaut de Google Cloud Platform

Vous pouvez utiliser les solutions de chiffrement NetApp avec le chiffrement natif de votre fournisseur de cloud, qui chiffre les données au niveau de l'hyperviseur. Cela permettrait d'obtenir un double cryptage, ce qui pourrait être souhaitable pour les données très sensibles. Lorsque les données chiffrées sont accessibles, elles sont déchiffrées deux fois : une fois au niveau de l'hyperviseur (à l'aide de clés du fournisseur de cloud), puis à nouveau à l'aide de solutions de chiffrement NetApp (à l'aide de clés d'un gestionnaire de clés externe).

### Solutions de chiffrement NetApp (NVE et NAE)

Cloud Volumes ONTAP prend en charge ["Chiffrement de volume NetApp \(NVE\) et chiffrement agrégé NetApp \(NAE\)"](#) . NVE et NAE sont des solutions logicielles qui permettent le chiffrement des données au repos des volumes conforme à la norme (FIPS) 140-2. NVE et NAE utilisent tous deux le cryptage AES 256 bits.

- NVE crypte les données au repos un volume à la fois. Chaque volume de données possède sa propre clé de cryptage unique.
- NAE est une extension de NVE : il crypte les données de chaque volume et les volumes partagent une clé sur l'ensemble. NAE permet également de dédupliquer les blocs communs à tous les volumes de l'agrégat.

Cloud Volumes ONTAP prend en charge NVE et NAE avec des services de gestion de clés externes (EKM) fournis par AWS, Azure et Google Cloud, y compris des solutions tierces, telles que Fortanix. Contrairement à ONTAP, pour Cloud Volumes ONTAP, les clés de chiffrement sont générées côté fournisseur de cloud, et non dans ONTAP.

Cloud Volumes ONTAP utilise les services standard KMIP (Key Management Interoperability Protocol) utilisés par ONTAP . Pour plus d'informations sur les services pris en charge, reportez-vous à la "[Outil de matrice d'interopérabilité](#)" .

Si vous utilisez NVE, vous avez la possibilité d'utiliser le coffre-fort de clés de votre fournisseur de cloud pour protéger les clés de chiffrement ONTAP :

- Service de gestion des clés AWS (KMS)
- Coffre de clés Azure (AKV)
- Service de gestion des clés Google Cloud

Les nouveaux agrégats ont le chiffrement d'agrégats NetApp (NAE) activé par défaut après la configuration d'un gestionnaire de clés externe. Les nouveaux volumes qui ne font pas partie d'un agrégat NAE ont NVE activé par défaut (par exemple, si vous avez des agrégats existants qui ont été créés avant la configuration d'un gestionnaire de clés externe).

La configuration d'un gestionnaire de clés pris en charge est la seule étape requise. Pour les instructions d'installation, reportez-vous à "[Chiffrer les volumes avec les solutions de chiffrement 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 de l' "[Service de gestion des clés AWS \(KMS\)](#)" . La console NetApp demande des clés de données à l'aide d'une clé principale client (CMK).



Vous ne pouvez pas modifier la méthode de chiffrement des données AWS après avoir créé un système Cloud Volumes ONTAP .

Si vous souhaitez utiliser cette option de chiffrement, vous devez vous assurer que AWS KMS est configuré de manière appropriée. Pour plus d'informations, reportez-vous à "[Configuration d'AWS KMS](#)" .

### Chiffrement du service de stockage Azure

Les données sont automatiquement chiffrées sur Cloud Volumes ONTAP dans Azure à l'aide de "[Chiffrement du service de stockage Azure](#)" avec une clé gérée par Microsoft.

Vous pouvez utiliser vos propres clés de cryptage si vous préférez. "[Découvrez comment configurer Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans Azure](#)" .

## Cryptage par défaut de Google Cloud Platform

"[Chiffrement des données au repos de Google Cloud Platform](#)" est activé par défaut pour Cloud Volumes ONTAP. Aucune configuration n'est requise.

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

## Analyse antivirus ONTAP

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur les systèmes ONTAP pour protéger les données contre toute compromission par des virus ou d'autres codes malveillants.

L'analyse antivirus ONTAP, appelée *Vscan*, combine le meilleur logiciel antivirus tiers de sa catégorie avec les fonctionnalités ONTAP qui vous offrent la flexibilité dont vous avez besoin pour contrôler quels fichiers sont analysés et quand.

Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, reportez-vous au "[Matrice d'interopérabilité NetApp](#)".

Pour plus d'informations sur la configuration et la gestion de la fonctionnalité antivirus sur les systèmes ONTAP, reportez-vous au "[Guide de configuration de l'antivirus ONTAP 9](#)".

## Protection contre les ransomwares

Les attaques de ransomware peuvent coûter du temps, des ressources et de la réputation à une entreprise. La console vous permet de mettre en œuvre la solution NetApp pour les ransomwares, qui fournit des outils efficaces de visibilité, de détection et de correction.

- La console identifie les volumes qui ne sont pas protégés par une stratégie de snapshot et vous permet d'activer la stratégie de snapshot par défaut sur ces volumes.

Les copies instantanées sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également fournir la granularité nécessaire pour créer des images d'une copie de fichier unique ou une solution complète de reprise après sinistre.

- La console vous permet également de bloquer les extensions de fichiers de 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 mettre en œuvre la solution NetApp contre les ransomwares"](#) .

## En savoir plus sur la surveillance des performances des charges de travail Cloud Volumes ONTAP

Vous pouvez consulter les résultats de performances pour vous aider à décider quelles charges de travail sont appropriées pour Cloud Volumes ONTAP.

### Rapports techniques de performance

- Cloud Volumes ONTAP pour AWS

["Rapport technique NetApp 4383 : Caractérisation des performances des Cloud Volumes ONTAP dans Amazon Web Services avec charges de travail applicatives"](#)

- Cloud Volumes ONTAP pour Microsoft Azure

["Rapport technique NetApp 4671 : Caractérisation des performances des Cloud Volumes ONTAP dans Azure avec charges de travail applicatives"](#)

- Cloud Volumes ONTAP pour Google Cloud

["Rapport technique NetApp 4816 : Caractérisation des performances de Cloud Volumes ONTAP pour Google Cloud"](#)

### performances du processeur

Les nœuds Cloud Volumes ONTAP s'affichent comme étant très utilisés (plus de 90 %) selon les outils de surveillance de votre fournisseur de cloud. Cela est dû au fait ONTAP réserve tous les vCPU présentés à la machine virtuelle afin qu'ils soient disponibles en cas de besoin.

Pour plus d'informations, reportez-vous à la ["Article de la base de connaissances NetApp sur la surveillance de l'utilisation du processeur ONTAP à l'aide de l'interface de ligne de commande"](#)

# Gestion des licences pour BYOL basé sur les nœuds

Chaque système Cloud Volumes ONTAP doté d'une licence BYOL (Apportez votre propre licence) basée sur un nœud doit disposer d'une licence système installée avec un abonnement actif. La console NetApp simplifie le processus en gérant les licences pour vous et en affichant un avertissement avant leur expiration.



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

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

["En savoir plus sur la gestion des licences basées sur les nœuds"](#) .

## Licences système BYOL

Les licences basées sur les nœuds peuvent être obtenues auprès de NetApp. Le nombre de licences disponibles pour un système à nœud unique ou une paire HA est illimité.



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

Une licence basée sur un nœud offre jusqu'à 368 Tio de capacité pour un nœud ou une paire HA. Vous avez peut-être acheté plusieurs licences pour un système Cloud Volumes ONTAP BYOL afin d'allouer plus de 368 Tio de capacité. Par exemple, vous pouvez disposer de deux licences pour allouer jusqu'à 736 Tio de capacité à Cloud Volumes ONTAP. Vous pouvez également disposer de quatre licences pour atteindre jusqu'à 1,4 Tio.

Sachez que les limites de disque peuvent vous empêcher d'atteindre la limite de capacité en utilisant uniquement les disques. Vous pouvez dépasser la limite du disque en ["hiérarchisation des données inactives vers le stockage d'objets"](#) . Pour plus d'informations sur les limites du disque, reportez-vous à ["limites de stockage dans les notes de publication de Cloud Volumes ONTAP"](#) .

## Gestion des licences pour un nouveau système

Lorsque vous créez un système BYOL basé sur des nœuds, la console vous demande le numéro de série de votre licence et votre compte de site de support NetApp . La console 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 de site de support NetApp à la console"](#) .

Si la console ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez ["obtenir le fichier vous-même, puis télécharger-le manuellement sur la console"](#) .

## Expiration de la licence

La console affiche un avertissement 30 jours avant l'expiration d'une licence basée sur un nœud et à nouveau lorsque la licence expire. L'image suivante montre un avertissement d'expiration de 30 jours qui apparaît dans l'interface utilisateur :



Vous pouvez sélectionner le système pour examiner le message.

La console 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 d'organisation ou de compte et que vous avez activé l'option. Le rapport envoyé par courrier électronique inclut l'avertissement d'expiration de la licence toutes les 2 semaines.

Si vous ne renouvelez pas la licence à temps, le système Cloud Volumes ONTAP s'arrête. Si vous le redémarrez, il s'éteint à nouveau.

## Renouvellement de licence

Si vous renouvelez un abonnement BYOL basé sur un nœud en contactant un représentant NetApp, la console obtient automatiquement la nouvelle licence auprès de NetApp et l'installe sur le système Cloud Volumes ONTAP.

Si la console ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez ["obtenez le fichier vous-même, puis téléchargez-le manuellement sur la console"](#).

## Transfert de licence vers un nouveau système

Une licence BYOL basée sur un nœud est transférable entre les systèmes Cloud Volumes ONTAP lorsque vous supprimez un système existant, puis en créez un nouveau en utilisant la même licence.

Par exemple, vous souhaitez peut-être 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* fonctionnent chez n'importe quel fournisseur de cloud. Les numéros de série indépendants du cloud commencent par le préfixe *908xxxx*.

Il est important de noter que votre licence BYOL est liée à votre entreprise et à un ensemble spécifique d'informations d'identification du site de support NetApp.

## Découvrez comment AutoSupport et Digital Advisor sont utilisés pour Cloud Volumes ONTAP

Le composant AutoSupport d'ONTAP collecte la télémétrie et l'envoie pour analyse. Active IQ Digital Advisor (également connu sous le nom de Digital Advisor) analyse les données d'AutoSupport et fournit des soins et une optimisation proactifs. Grâce à l'intelligence artificielle, Digital Advisor peut identifier les problèmes potentiels et vous aider à les résoudre avant qu'ils n'affectent votre entreprise.

Digital Advisor vous permet d'optimiser votre infrastructure de données sur votre cloud hybride mondial en fournissant des analyses prédictives exploitables et une assistance proactive via un portail basé sur le cloud et une application mobile. Les informations et recommandations basées sur les données de Digital Advisor sont

disponibles pour tous les clients NetApp disposant d'un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques choses que vous pouvez faire avec Digital Advisor:

- Planifier des mises à niveau.

Digital Advisor identifie les problèmes de votre environnement qui peuvent être résolus par une mise à niveau vers une version plus récente d' ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.

- Afficher le bien-être du système.

Votre tableau de bord Digital Advisor signale tout problème de bien-être et vous aide à les corriger. Surveillez la capacité du système pour vous assurer de ne jamais manquer d'espace de stockage. Consultez les cas d'assistance pour votre système.

- Gérer les performances.

Digital Advisor affiche les performances du système sur une période plus longue que celle que vous pouvez voir dans ONTAP System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur vos performances. Maximiser l'efficacité. Consultez les mesures d'efficacité du stockage et identifiez les moyens de stocker plus de données dans moins d'espace.

- Afficher l'inventaire et la configuration.

Digital Advisor affiche l'inventaire complet et les informations de configuration logicielle et matérielle. Voyez quand les contrats de service expirent et renouvelez-les pour vous assurer de continuer à bénéficier d'une assistance.

#### Liens connexes

- ["Documentation NetApp : Digital Advisor"](#)
- ["Lancement de Digital Advisor"](#)
- ["Services SupportEdge"](#)

## Configurations par défaut prises en charge pour Cloud Volumes ONTAP

Comprendre comment Cloud Volumes ONTAP est configuré par défaut peut vous aider à configurer et à administrer vos systèmes, en particulier si vous connaissez ONTAP , car la configuration par défaut de Cloud Volumes ONTAP est différente de celle ONTAP.

### Configuration par défaut

- La console NetApp crée une machine virtuelle de stockage de service de données lorsqu'elle déploie 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"](#) .

À partir de la version 3.9.5, les rapports d'espace logique sont activés sur la machine virtuelle de stockage initiale. Lorsque l'espace est signalé de manière logique, ONTAP signale l'espace du volume de telle sorte que tout l'espace physique économisé par les fonctionnalités d'efficacité du stockage soit également signalé comme utilisé. Pour plus d'informations sur les fonctionnalités d'efficacité du stockage en ligne,

reportez-vous à l'article de la base de connaissances "[KB : Quelles fonctionnalités d'efficacité du stockage en ligne sont prises en charge avec CVO ?](#)"

- La console installe automatiquement les licences de fonctionnalités ONTAP suivantes sur Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Gestion des clés de chiffrement multi-locataires (MTEKM), à partir de Cloud Volumes ONTAP 9.12.1 GA
  - Chiffrement de volume NetApp (uniquement pour les systèmes BYOL (apportez votre propre licence) ou PAYGO (pay-as-you-go) enregistrés)
  - NFS `ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]`
  - SnapMirror
  - SnapRestore
  - SnapVault
- Plusieurs interfaces réseau sont créées par défaut :
  - Un LIF de gestion de cluster
  - Un LIF intercluster
- Un LIF de gestion SVM sur les systèmes HA dans Azure
- Un LIF de gestion SVM sur les systèmes HA dans Google Cloud
- Un LIF de gestion SVM sur des systèmes à nœud unique dans AWS
- Un LIF de gestion de nœuds

+ Dans Google Cloud, ce LIF est combiné avec le LIF intercluster.

- Un LIF de données iSCSI
- Un LIF de données CIFS et NFS



Le basculement 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 interrompt le mappage externe entre les adresses IP et les interfaces réseau sur l'instance, rendant le LIF inaccessible.

- Cloud Volumes ONTAP envoie des sauvegardes de configuration à l'agent de console via HTTP.

Les sauvegardes sont accessibles depuis `http://ipaddress/occm/offboxconfig/` où *ipaddress* est l'adresse IP de l'hôte de l'agent de la console.

Vous pouvez utiliser les sauvegardes pour reconfigurer votre système Cloud Volumes ONTAP . Pour plus d'informations sur les sauvegardes de configuration, reportez-vous à la "[Documentation ONTAP](#)" .

- La console définit quelques attributs de volume différemment des autres outils de gestion (ONTAP System Manager ou ONTAP CLI, par exemple).

Le tableau suivant répertorie les attributs de volume définis différemment des valeurs par défaut :

Attribut	Valeur que la console configure
Mode de taille automatique	grandir
Taille automatique maximale	1 000 pour cent  L'organisation ou 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 d'espace	aucun
Autorisations UNIX (NFS uniquement)	777

+

Pour plus d'informations sur ces attributs, reportez-vous à "[Page de manuel ONTAP volume create](#)".

## Disques internes pour les données système

En plus du stockage des données utilisateur, la console achète également du stockage cloud pour les données système.

### AWS

- Trois disques par nœud pour les données de démarrage, racine et principales :
  - Disque io1 de 47 Gio pour les données de démarrage
  - Disque gp3 de 140 Gio pour les données racine
  - Disque gp2 de 540 Gio pour les données de base
- Pour les paires HA :
  - Deux volumes EBS st1 pour l'instance du médiateur, l'un d'environ 8 Gio comme disque racine et l'autre de 4 Gio comme disque de données
  - Un disque gp3 de 140 Gio dans chaque nœud pour contenir une copie des données racine de l'autre nœud



Dans certaines zones, le type de disque EBS disponible ne peut être que gp2.

- Un instantané EBS pour chaque disque de démarrage et disque racine



Les instantanés sont créés automatiquement au redémarrage.

- Lorsque vous activez le chiffrement des données dans AWS à l'aide du service de gestion des clés (KMS),

les disques de démarrage et racine de Cloud Volumes ONTAP sont également chiffrés. Cela inclut le disque de démarrage de l'instance de médiateur dans une paire HA. Les disques sont chiffrés à l'aide de la CMK que vous sélectionnez lorsque vous ajoutez un système Cloud Volumes ONTAP .



Dans AWS, la NVRAM se trouve sur le disque de démarrage.

### Azure (nœud unique)

- Trois disques SSD Premium :
  - Un disque de 10 Gio pour les données de démarrage
  - Un disque de 140 Gio pour les données racine
  - Un disque de 512 Gio pour la NVRAM

Si la machine virtuelle que vous avez choisie pour Cloud Volumes ONTAP prend en charge les SSD Ultra, le système utilise un SSD Ultra de 32 Gio pour la NVRAM, plutôt qu'un SSD Premium.

- Un disque dur standard de 1 024 Gio pour la sauvegarde des cœurs
- Un instantané Azure pour chaque disque de démarrage et disque racine
- Par défaut, chaque disque dans Azure est chiffré au repos.

Si la machine virtuelle que vous avez choisie pour Cloud Volumes ONTAP prend en charge les disques gérés Premium SSD v2 comme disques de données, le système utilise un disque géré Premium SSD v2 de 32 Gio pour la NVRAM et un autre comme disque racine.

### Azure (paire HA)

#### HA s'associe à un blob de pages

- Deux disques SSD Premium de 10 Gio pour le volume de démarrage (un par nœud)
- Deux blobs de pages de stockage Premium de 140 Gio pour le volume racine (un par nœud)
- Deux disques durs standard de 1 024 Gio pour la sauvegarde des cœurs (un par nœud)
- Deux disques SSD Premium de 512 Gio pour la NVRAM (un par nœud)
- Un instantané Azure pour chaque disque de démarrage et disque racine



Les instantanés sont créés automatiquement au redémarrage.

- Par défaut, chaque disque dans Azure est chiffré au repos.

#### Paires HA avec disques gérés partagés dans plusieurs zones de disponibilité

- Deux disques SSD Premium de 10 Gio pour le volume de démarrage (un par nœud)
- Deux disques SSD Premium de 512 Gio pour le volume racine (un par nœud)
- Deux disques durs standard de 1 024 Gio pour la sauvegarde des cœurs (un par nœud)
- Deux disques SSD Premium de 512 Gio pour la NVRAM (un par nœud)
- Un instantané Azure pour chaque disque de démarrage et disque racine



Les instantanés sont créés automatiquement au redémarrage.

- Par défaut, chaque disque dans Azure est chiffré au repos.

### **Paires HA avec disques gérés partagés dans des zones de disponibilité uniques**

- Deux disques SSD Premium de 10 Gio pour le volume de démarrage (un par nœud)
- Deux disques SSD Premium partagés gérés de 512 Gio pour le volume racine (un par nœud)
- Deux disques durs standard de 1 024 Gio pour la sauvegarde des cœurs (un par nœud)
- Deux disques SSD Premium gérés de 512 Gio pour NVRAM (un par nœud)

Si votre machine virtuelle prend en charge les disques gérés Premium SSD v2 comme disques de données, elle utilise 32 Gio de disques gérés Premium SSD v2 pour la NVRAM et 512 Gio de disques gérés partagés Premium SSD v2 pour le volume racine.

Vous pouvez déployer des paires HA dans une seule zone de disponibilité et utiliser des disques gérés Premium SSD v2 lorsque les conditions suivantes sont remplies :

- La version de Cloud Volumes ONTAP est 9.15.1 ou ultérieure.
- La région et la zone sélectionnées prennent en charge les disques gérés Premium SSD v2. Pour plus d'informations sur les régions prises en charge, reportez-vous à "[Site Web Microsoft Azure : produits disponibles par région](#)".
- L'abonnement est enregistré auprès de Microsoft "[Fonctionnalité Microsoft.Compute/VMOrchestratorZonalMultiFD](#)".

### **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 racine
- Un disque persistant SSD de 500 Gio pour la NVRAM
- Un disque persistant standard de 315 Gio pour la sauvegarde des cœurs
- Instantanés des données de démarrage et de racine



Les instantanés sont créés automatiquement au redémarrage.

- 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 racine
- Deux disques persistants SSD de 500 Gio pour NVRAM
- Deux disques persistants standard de 315 Gio pour la sauvegarde des cœurs
- Un disque persistant standard de 10 Gio pour les données du médiateur
- Un disque persistant standard de 10 Gio pour les données de démarrage du médiateur
- Instantanés des données de démarrage et de racine



Les instantanés sont créés automatiquement au redémarrage.

- Les disques de démarrage et racine sont chiffrés par défaut.

## **Où résident les disques**

Disposition du stockage :

- Les données de démarrage résident sur un disque attaché à l'instance ou à la machine virtuelle.

Ce disque, qui contient l'image de démarrage, n'est pas disponible pour Cloud Volumes ONTAP.

- Les données racine, 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 soutien

## Inscrivez-vous pour obtenir de l'aide

L'enregistrement du support est requis pour recevoir un support technique spécifique à BlueXP et à ses solutions et services de stockage. L'enregistrement du support est également requis pour activer les flux de travail clés pour les systèmes Cloud Volumes ONTAP .

L'inscription au support n'active pas la prise en charge NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à « Obtenir de l'aide » dans la documentation BlueXP de ce produit.

- ["Amazon FSx pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

## Présentation de l'enregistrement de l'assistance

Il existe deux formes d'inscription pour activer le droit au support :

- Enregistrement du numéro de série de votre compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxxx situé sur la page Ressources d'assistance dans BlueXP).

Il s'agit de votre identifiant d'abonnement d'assistance unique pour tout service au sein de BlueXP. Chaque abonnement de support au niveau du compte BlueXP doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur la place de marché de votre fournisseur de cloud (il s'agit de numéros de série 909201xxxxxxxx à 20 chiffres).

Ces numéros de série sont communément appelés *numéros de série PAYGO* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP .

L'enregistrement des deux types de numéros de série permet des fonctionnalités telles que l'ouverture de tickets d'assistance et la génération automatique de dossiers. L'enregistrement est terminé en ajoutant des comptes NetApp Support Site (NSS) à BlueXP comme décrit ci-dessous.

## Enregistrez BlueXP pour le support NetApp

Pour vous inscrire au support et activer le droit de support, un utilisateur de votre organisation (ou compte) BlueXP doit associer un compte de site de support NetApp à sa connexion BlueXP . La manière dont vous vous inscrivez au support NetApp dépend du fait que vous possédez déjà ou non un compte NetApp Support Site (NSS).

### Client existant avec un compte NSS

Si vous êtes un client NetApp avec un compte NSS, il vous suffit de vous inscrire pour bénéficier du support via BlueXP.

### Étapes

1. En haut à droite de la console BlueXP , sélectionnez l'icône Paramètres, puis sélectionnez **Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite d'authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'inscription a réussi, sélectionnez l'icône Aide, puis sélectionnez **Assistance**.

La page **Ressources** devrait indiquer que votre organisation BlueXP est enregistrée pour bénéficier du support.



Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé un compte de site de support NetApp à leur connexion BlueXP . Cependant, cela ne signifie pas que votre organisation BlueXP n'est pas enregistrée pour bénéficier du support. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre organisation a été enregistrée.

### Client existant mais pas de compte NSS

Si vous êtes un client NetApp existant avec des licences et des numéros de série existants mais pas de compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP .

#### Étapes

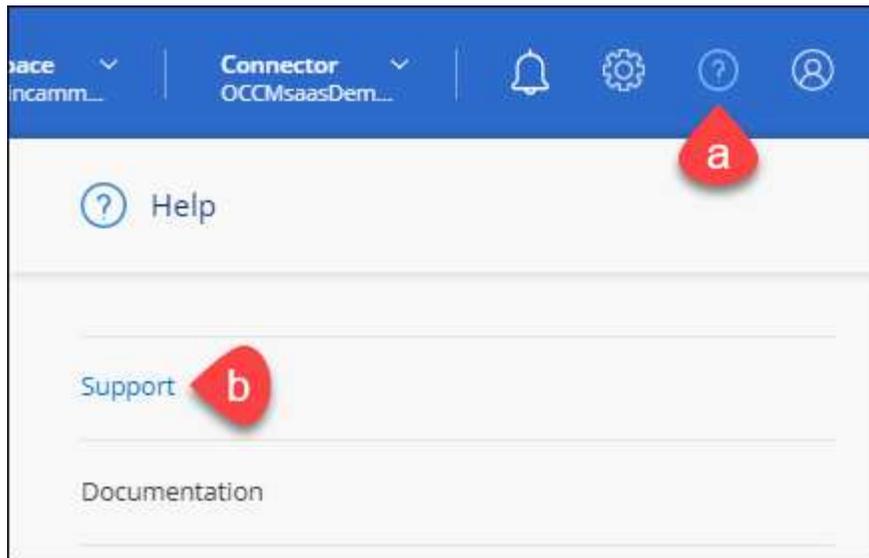
1. Créez un compte sur le site de support NetApp en remplissant le "[Formulaire d'inscription des utilisateurs du site de support NetApp](#)"
  - a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement \* Client/Utilisateur final NetApp \*.
  - b. Assurez-vous de copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement du compte.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes ci-dessous [Client existant avec un compte NSS](#) .

### Tout nouveau chez NetApp

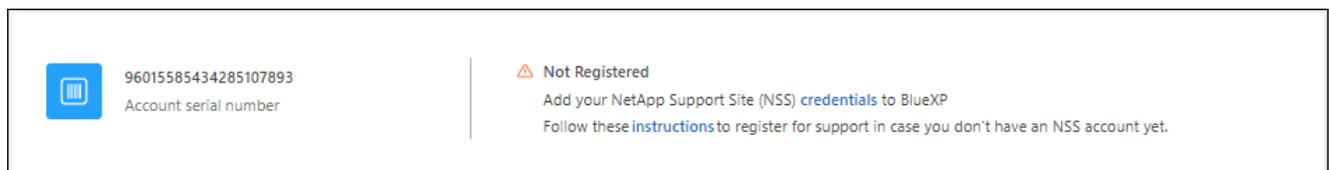
Si vous êtes nouveau sur NetApp et que vous n'avez pas de compte NSS, suivez chaque étape ci-dessous.

#### Étapes

1. Dans le coin supérieur droit de la console BlueXP , sélectionnez l'icône Aide, puis sélectionnez **Support**.



2. Recherchez le numéro de série de votre identifiant de compte sur la page d'inscription au support.



3. Accéder à "[Site d'inscription au support de 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 **Gamme de produits**, sélectionnez **Cloud Manager**, puis sélectionnez votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, effectuez la vérification de sécurité, puis confirmez que vous avez lu la politique de confidentialité des données mondiales de NetApp.

Un email est immédiatement envoyé à la boîte mail prévue à cet effet pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers spam si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action depuis l'e-mail.

La confirmation soumet 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 remplissant le "[Formulaire d'inscription des utilisateurs du site de support NetApp](#)"
  - a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement \* Client/Utilisateur final NetApp \*.
  - b. Assurez-vous de copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement.

### Après avoir 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 que vous avez votre compte de site de support NetApp , associez le compte à votre connexion BlueXP en suivant les étapes ci-dessous [Client existant avec un compte NSS](#) .

## Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP

L'association des informations d'identification du site de support NetApp à votre organisation BlueXP est requise pour activer les workflows clés suivants pour Cloud Volumes ONTAP :

- Enregistrement des systèmes Cloud Volumes ONTAP prépayés pour le support

Fournir votre compte NSS est nécessaire pour activer le support de votre système et pour accéder aux ressources de support technique NetApp .

- Déploiement de Cloud Volumes ONTAP lorsque vous apportez votre propre licence (BYOL)

Il est nécessaire de fournir votre compte NSS pour que BlueXP puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut les mises à jour automatiques pour les renouvellements de mandat.

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

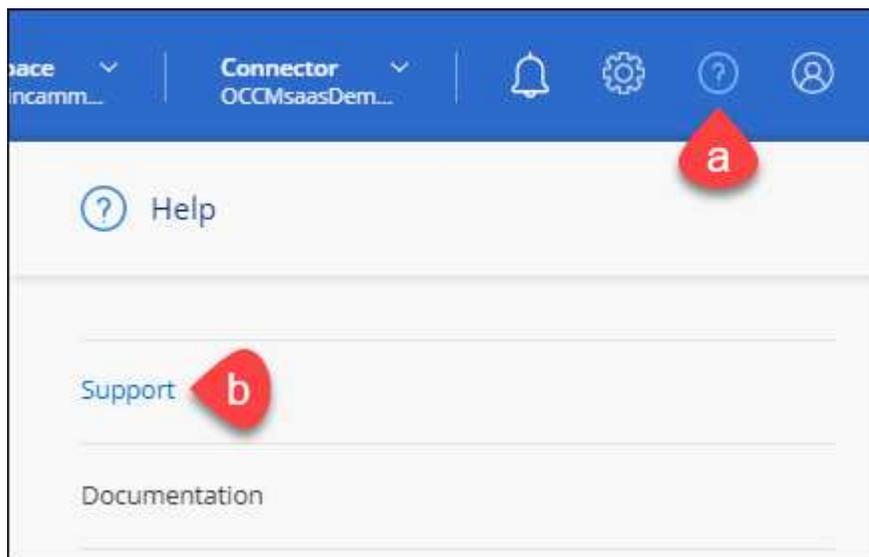
L'association des informations d'identification NSS à votre organisation BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP .

Ces informations d'identification NSS sont associées à votre ID d'organisation BlueXP spécifique. Les utilisateurs appartenant à l'organisation BlueXP peuvent accéder à ces informations d'identification depuis **Support > Gestion NSS**.

- Si vous disposez d'un compte client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous disposez d'un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés aux côtés des comptes de niveau client.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP , sélectionnez l'icône Aide, puis sélectionnez **Support**.



2. Sélectionnez **Gestion NSS > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp pour effectuer le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des tâches telles que les téléchargements de licences, la vérification des mises à niveau de logiciels et les futures inscriptions au support.

Notez ce qui suit :

- Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS au niveau client.
- Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS au niveau client et qu'un compte au niveau partenaire existe, vous obtiendrez le message d'erreur suivant :

« Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de types différents. »

Il en va de même si vous disposez de comptes NSS préexistants au niveau client et que vous essayez d'ajouter un compte au niveau partenaire.

- Une fois la connexion réussie, NetApp stockera le nom d'utilisateur NSS.

Il s'agit d'un identifiant généré par le système qui correspond à votre e-mail. Sur la page **Gestion NSS**, vous pouvez afficher votre e-mail 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.

L'utilisation de cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

## Obtenir de l'aide

NetApp propose une assistance pour BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24h/24 et 7j/7, telles que des articles de la base de connaissances et un forum communautaire. Votre inscription au support inclut une assistance technique à distance via un ticket web.

### Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud

Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à « Obtenir de l'aide » dans la documentation BlueXP de ce produit.

- ["Amazon FSx pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Pour recevoir une assistance technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options d'assistance décrites ci-dessous.

## Utiliser les options d'auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

La documentation BlueXP que vous consultez actuellement.

- ["Base de connaissances"](#)

Recherchez dans la base de connaissances BlueXP pour trouver des articles utiles pour résoudre les problèmes.

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre les discussions en cours ou en créer de nouvelles.

## Créer un dossier auprès du support NetApp

En plus des options d'auto-assistance ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tout problème après avoir activé le support.

### Avant de commencer

- Pour utiliser la fonctionnalité **Créer un dossier**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion BlueXP . ["Découvrez comment gérer les informations d'identification associées à votre connexion BlueXP"](#) .
- Si vous ouvrez un dossier pour un système ONTAP doté d'un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

### Étapes

1. Dans BlueXP, sélectionnez **Aide > Support**.
2. Sur la page **Ressources**, choisissez l'une des options disponibles sous Support technique :
  - a. Sélectionnez **Appelez-nous** si vous souhaitez parler à quelqu'un au téléphone. Vous serez redirigé vers une page sur netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.
  - b. Sélectionnez **Créer un dossier** pour ouvrir un ticket avec un spécialiste du support NetApp :
    - **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 champ d'application de l'organisation

BlueXP (ou du compte), du projet (ou de l'espace de travail) et du connecteur que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : Choisissez la priorité du cas, qui peut être Faible, Moyenne, Élevée ou Critique.

Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information à côté du nom du champ.

- **Description du problème** : Fournissez une description détaillée de votre problème, y compris tous les messages d'erreur applicables ou les étapes de dépannage que vous avez effectuées.
- **Adresses e-mail supplémentaires** : saisissez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.
- **Pièce jointe (facultatif)** : Téléchargez jusqu'à cinq pièces jointes, une à la fois.

Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.

The screenshot shows a web form titled "ntapitdemo" and "NetApp Support Site Account". It contains several sections:

- Service**: A dropdown menu with "Select" as the current option.
- Working Environment**: A dropdown menu with "Select" as the current option.
- Case Priority**: A dropdown menu with "Low - General guidance" as the current option. An information icon (i) is visible to the right.
- Issue Description**: A large text area with the placeholder text "Provide detailed description of problem, applicable error messages and troubleshooting steps taken."
- Additional Email Addresses (Optional)**: A text input field with the placeholder "Type here". An information icon (i) is visible to the right.
- Attachment (Optional)**: A file upload area showing "No files selected". It includes an "Upload" button with an upward arrow icon and a trash can icon with a hand cursor over it. An information icon (i) is also present.

### Après avoir terminé

Une fenêtre contextuelle apparaîtra avec votre numéro de dossier d'assistance. Un spécialiste du support

NetApp examinera votre cas et vous répondra dans les plus brefs délais.

Pour un historique de vos demandes d'assistance, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées « créer une demande d'assistance ». 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 lorsque vous essayez de créer un dossier :

« Vous n'êtes pas autorisé à créer un dossier contre le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement à laquelle il est associé ne sont pas la même société d'enregistrement pour le numéro de série du compte BlueXP (c'est-à-dire. 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat intégré au produit
- Soumettez un cas non technique à <https://mysupport.netapp.com/site/help>

## Gérez vos demandes d'assistance (Aperçu)

Vous pouvez afficher et gérer les cas d'assistance actifs et résolus directement depuis BlueXP. Vous pouvez gérer les cas associés à votre compte NSS et à votre entreprise.

La gestion des cas est disponible en aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Veuillez nous envoyer vos commentaires en utilisant le chat intégré au produit.

Notez ce qui suit :

- Le tableau de bord de gestion des cas en haut de la page offre deux vues :
  - La vue de gauche montre le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte utilisateur NSS que vous avez fourni.
  - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte utilisateur NSS.

Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.

- Vous pouvez ajouter ou supprimer des colonnes d'intérêt et filtrer le contenu des colonnes telles que Priorité et Statut. D'autres colonnes fournissent simplement des capacités de tri.

Consultez les étapes ci-dessous pour plus de détails.

- Au niveau de chaque cas, nous offrons la possibilité de mettre à jour les notes du cas ou de fermer un cas qui n'est pas déjà au statut Fermé ou En attente de fermeture.

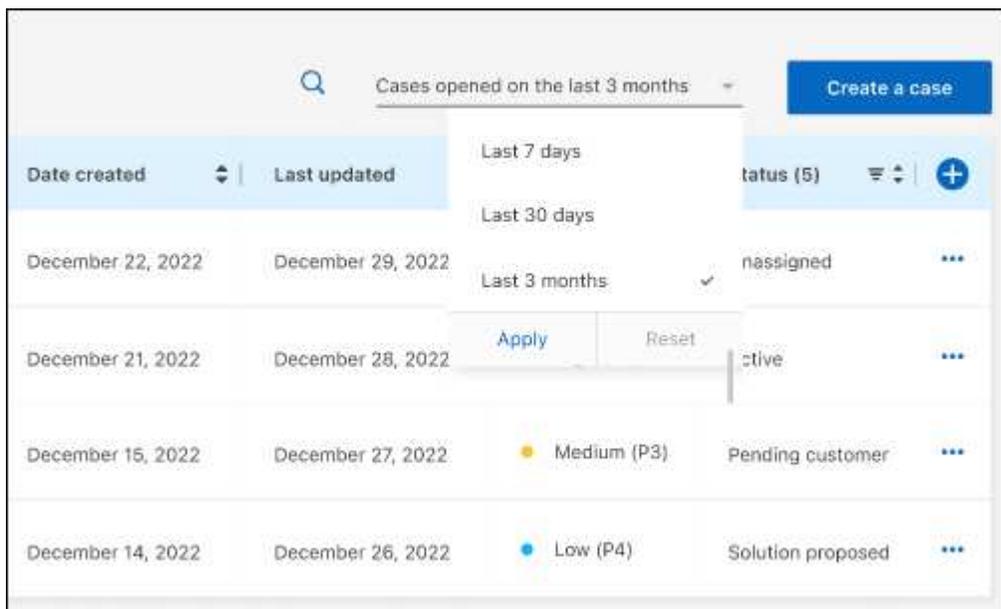
### Étapes

1. Dans BlueXP, sélectionnez **Aide > Support**.
2. Sélectionnez **Gestion des cas** et si vous y êtes invité, ajoutez votre compte NSS à BlueXP.

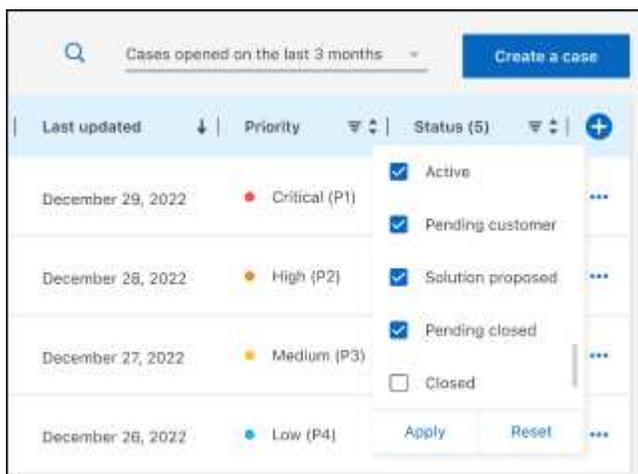
La page **Gestion des cas** affiche les cas ouverts liés au compte NSS associé à votre compte utilisateur BlueXP . Il s'agit du même compte NSS qui apparaît en haut de la page **Gestion NSS**.

3. Modifiez éventuellement les informations qui s'affichent dans le tableau :

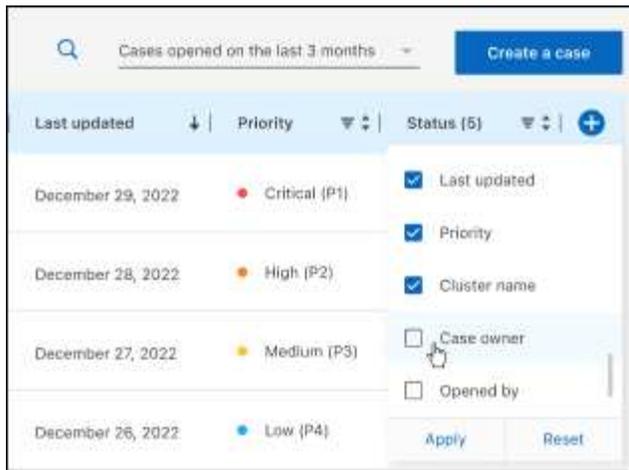
- Sous **Cas de l'organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre entreprise.
- Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une période différente.



- Filtrer le contenu des colonnes.



- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant  et ensuite choisir les colonnes que vous souhaitez afficher.

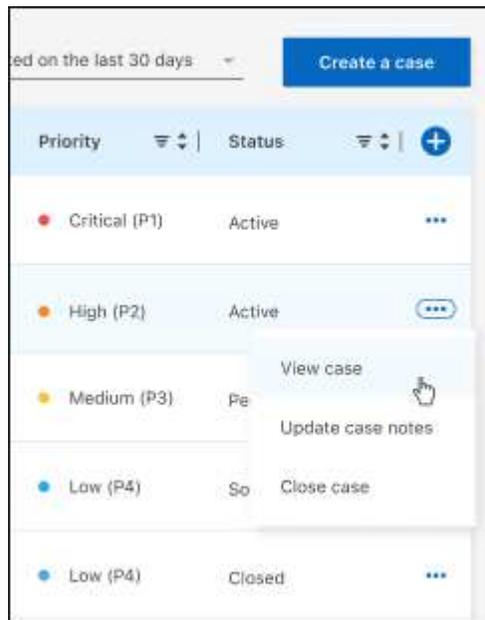


4. Gérer un dossier existant en sélectionnant... et en sélectionnant l'une des options disponibles :

- **Voir le cas** : Afficher tous les détails sur un cas spécifique.
- **Mettre à jour les notes du cas** : fournissez des détails supplémentaires sur votre problème ou sélectionnez **Télécharger des fichiers** pour joindre jusqu'à un maximum de cinq fichiers.

Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.

- **Fermer le dossier** : Fournissez des détails sur les raisons pour lesquelles vous fermez le dossier et sélectionnez **Fermer le dossier**.



# Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

## Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques 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.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

- ["Avis concernant la console NetApp"](#)
- ["Avis concernant Cloud Volumes ONTAP"](#)
- ["Avis pour ONTAP"](#)

## Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

## Informations sur les marques commerciales

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