Commencez dans AWS

Cloud Manager 3.8

NetApp
October 22, 2024

Sommaire

Commencez dans AWS

Mise en route avec Cloud Volumes ONTAP pour AWS

Découvrez Cloud Volumes ONTAP pour AWS en quelques étapes.

Créer un connecteur

Si vous n'avez pas de "Connecteur" Cependant, un administrateur de compte doit en créer un. "Découvrez comment créer un connecteur dans AWS".

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

Planification de la configuration

Cloud Manager propose des packages préconfigurés qui répondent aux exigences de vos workloads, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez. "En savoir plus >>".

Configurez votre réseau

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

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

3. Configurez un terminal VPC sur le service S3.

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

"En savoir plus sur les exigences de mise en réseau".

Configuration du KMS AWS

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

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

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

Liens connexes

- "L'évaluation"
- "Création d'un connecteur depuis Cloud Manager"
- "Lancement d'un connecteur depuis AWS Marketplace"
- "Installation du logiciel du connecteur sur un hôte Linux"
- "Ce que fait Cloud Manager avec les autorisations AWS"

Planification de votre configuration Cloud Volumes ONTAP dans AWS

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

Choix d'un type de licence

Deux options de tarification sont disponibles pour Cloud Volumes ONTAP : le paiement à l'utilisation ou le modèle BYOL (où vous apportez votre propre licence). Le paiement basé sur l'utilisation vous permet de choisir entre trois licences : explore, Standard ou Premium. Chacune d'elles fournit une capacité distincte et des options de calcul différentes.

"Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans AWS"

Compréhension des limites de stockage

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

"Limites de stockage pour Cloud Volumes ONTAP 9.7 dans AWS"

Dimensionnement de votre système dans AWS

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

Type d'instance

- Assurez-vous que les exigences de vos workloads correspondent aux valeurs maximales de débit et d'IOPS pour chaque type d'instance EC2.
- Si plusieurs utilisateurs écrivent dans le système en même temps, choisissez un type d'instance disposant de suffisamment de processeurs pour gérer les requêtes.

- Si votre champ d'application implique essentiellement la lecture, optez pour un système disposant de suffisamment de mémoire RAM.
  - "Documentation AWS : types d'instances Amazon EC2"
  - "Documentation AWS : instances optimisées pour Amazon EBS"

Type de disque EBS

Les SSD à usage générique sont les types de disques les plus courants pour les systèmes Cloud Volumes ONTAP. Pour en savoir plus sur les utilisations des disques EBS, reportez-vous à la section "Documentation AWS : types de volume EBS".

Taille des disques EBS

Lorsque vous lancez un système Cloud Volumes ONTAP, vous devez choisir une taille de disque initiale. Après cela, vous pouvez "Laissez Cloud Manager gérer la capacité d'un système à votre place", mais si vous voulez "créez des agrégats vous-même", soyez conscient des éléments suivants :

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

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

Pour plus d'informations sur le dimensionnement de votre système Cloud Volumes ONTAP dans AWS, visionnez la vidéo suivante :

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Choix d'une configuration qui prend en charge Flash cache

Certaines configurations Cloud Volumes ONTAP dans AWS incluent le stockage NVMe local, utilisé par Cloud Volumes ONTAP *Flash cache* pour de meilleures performances. "En savoir plus sur Flash cache".

Fiche technique d'informations sur le réseau AWS

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

Informations réseau pour Cloud Volumes ONTAP

Informations sur AWS	Votre valeur
Région	
VPC	
Sous-réseau	

Informations sur AWS	Votre valeur
Groupe de sécurité (s'il s'agit du vôtre)	

Informations réseau pour une paire HA dans plusieurs AZS

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

Sélection d'une vitesse d'écriture

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés et les risques et les recommandations lors de l'utilisation de la vitesse d'écriture élevée.

Différence entre une vitesse d'écriture standard et une vitesse d'écriture élevée

Lorsque vous choisissez la vitesse d'écriture standard, les données sont écrites directement sur le disque, réduisant ainsi le risque de perte de données en cas d'interruption imprévue du système.

Lorsque vous choisissez la vitesse d'écriture élevée, les données sont mises en tampon dans la mémoire

avant d'être écrites sur le disque, ce qui accélère les performances d'écriture. Toutefois, la mise en cache peut entraîner une perte de données en cas de panne système.

Le volume de données pouvant être perdues en cas de panne système correspond à l'étendue des deux derniers points de cohérence. Le point de cohérence consiste à écrire des données mises en tampon sur le disque. Un point de cohérence se produit lorsque le journal d'écriture est plein ou après 10 secondes (selon la première éventualité). Cependant, la performance des volumes AWS EBS peut affecter le temps de traitement des points de cohérence.

Quand utiliser une vitesse d'écriture élevée

Optez pour la vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides et que vous ne craignez pas de perdre des données.

Recommandations lors de l'utilisation d'une vitesse d'écriture élevée

Si vous activez la vitesse d'écriture élevée, vous devez assurer la protection de l'écriture au niveau de la couche applicative.

Choix d'un profil d'utilisation du volume

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

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

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

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

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

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

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

Conditions générales requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

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

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

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

  "Découvrez comment configurer AutoSupport".

Accès Internet sortant pour le médiateur haute disponibilité

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

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

Nombre d'adresses IP

Cloud Manager attribue le nombre suivant d'adresses IP à Cloud Volumes ONTAP dans AWS :

- Un seul nœud : 6 adresses IP
- Paires HA en simple AZS : 15 adresses
- Paires HAUTE DISPONIBILITÉ dans plusieurs adresses AZS : 15 ou 16 adresses IP

  Notez que Cloud Manager crée une LIF de gestion des SVM sur des systèmes à un seul nœud, mais pas sur des paires haute disponibilité dans une même zone de disponibilité. Vous pouvez choisir de créer ou non une LIF de gestion SVM sur des paires HA dans plusieurs AZS.

  Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car Cloud Manager le fait pour vous. Si vous devez utiliser votre propre, reportez-vous à la section "Règles de groupe de sécurité".

Connexion de Cloud Volumes ONTAP à AWS S3 pour le 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 est connecté à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d'un terminal de passerelle".

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

Volumes ONTAP ne peut pas se connecter au service S3.

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

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et ONTAP sur d'autres réseaux, vous devez disposer d'une connexion VPN entre AWS VPC et l'autre réseau, par exemple Azure VNet ou votre réseau d'entreprise. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : configuration d'une connexion VPN AWS".

DNS et Active Directory pour CIFS

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

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

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

Besoins en paires haute disponibilité dans plusieurs AZS

D'autres exigences de mise en réseau AWS s'appliquent aux configurations Cloud Volumes ONTAP HA qui utilisent plusieurs zones de disponibilité (AZS). Avant de lancer une paire haute disponibilité, vous devez consulter ces exigences car vous devez saisir les informations de mise en réseau dans Cloud Manager.

Pour comprendre le fonctionnement des paires haute disponibilité, voir "Paires haute disponibilité".

Zones de disponibilité

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

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

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

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

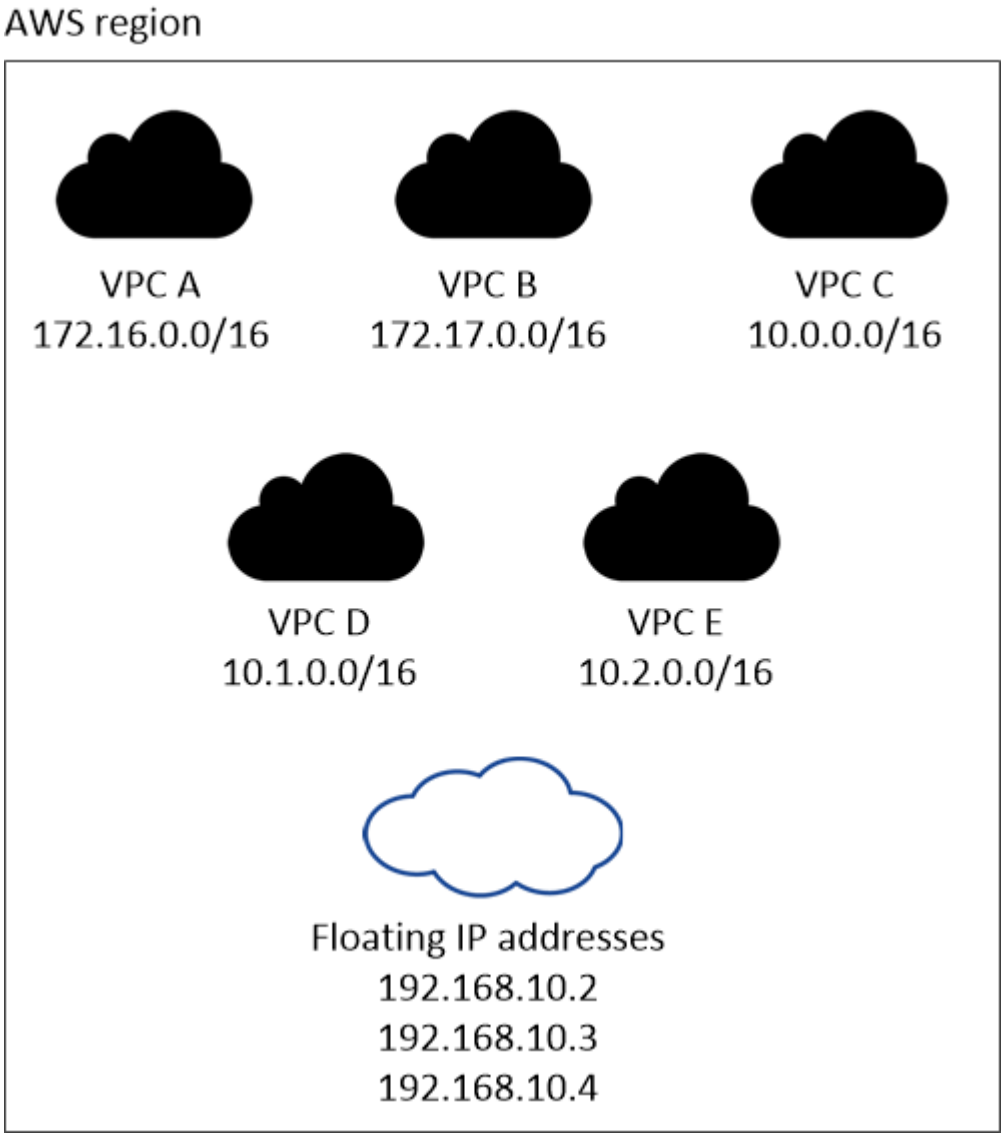
Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité. Si vous ne spécifiez pas l'adresse IP lors du déploiement du système, vous pouvez créer la LIF plus tard. Pour plus de détails, voir "Configuration de Cloud Volumes ONTAP".

Vous devez saisir les adresses IP flottantes dans Cloud Manager lors de la création d'un environnement de travail Cloud Volumes ONTAP HA. Cloud Manager alloue les adresses IP à la paire HA lors du lancement du système.

Les adresses IP flottantes doivent être en dehors des blocs CIDR sur tous les VPC de la région AWS dans

laquelle vous déployez la configuration HA. Considérez les adresses IP flottantes comme un sous-réseau logique en dehors des VPC de votre région.

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



Cloud Manager crée automatiquement des adresses IP statiques pour l'accès iSCSI et pour l'accès NAS des clients en dehors du VPC. Vous n'avez pas besoin de répondre à des exigences relatives à ces types d'adresses IP.

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

"Configuration d'une passerelle de transit AWS" Pour permettre l'accès aux adresses IP flottantes d'une paire haute disponibilité de l'extérieur du VPC où réside la paire haute disponibilité.

Tables de routage

Une fois que vous avez spécifié les adresses IP flottantes dans Cloud Manager, vous devez sélectionner les tables de route qui doivent inclure des routes vers les adresses IP flottantes. Cela permet au client d'accéder à la paire haute disponibilité.

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

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

Pour plus d'informations sur les tables de routage, voir "Documentation AWS : tables de routage".

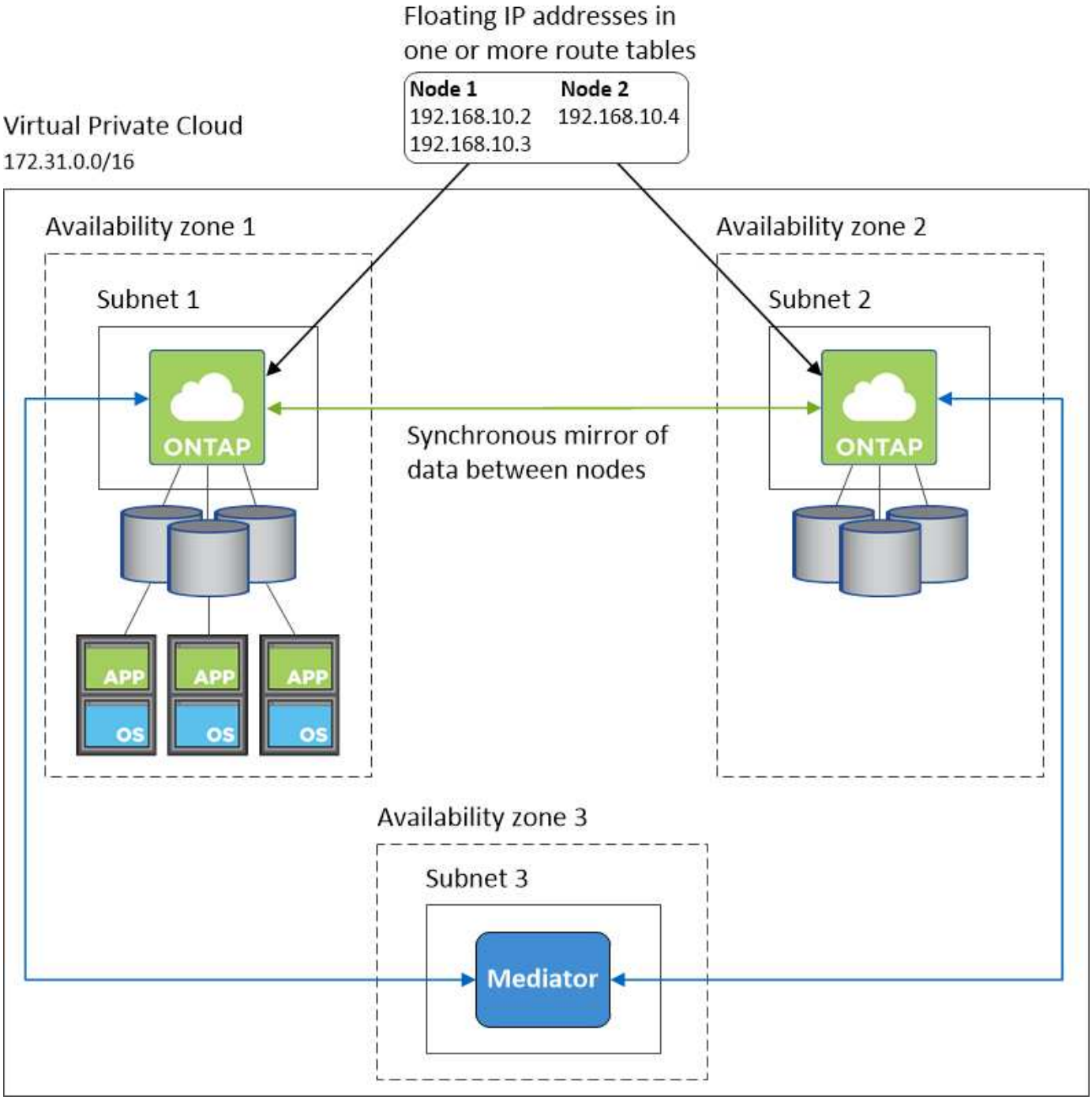
Connexion aux outils de gestion NetApp

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

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

Exemple de configuration haute disponibilité

L'image suivante montre une configuration HA optimale dans AWS fonctionnant comme une configuration active-passive :



Configuration requise pour le connecteur

Configurez votre réseau afin que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications vers Internet, vous pouvez spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration du connecteur pour utiliser un serveur proxy".

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau aux VPC et VNets dans lesquels vous souhaitez déployer Cloud Volumes ONTAP.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans AWS, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3) Le noeud final exact dépend de la région dans laquelle vous déployez Cloud Volumes ONTAP. "Reportez-vous à la documentation AWS pour plus de détails."	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans AWS.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.

Terminaux	Objectif
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Permet d'ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

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

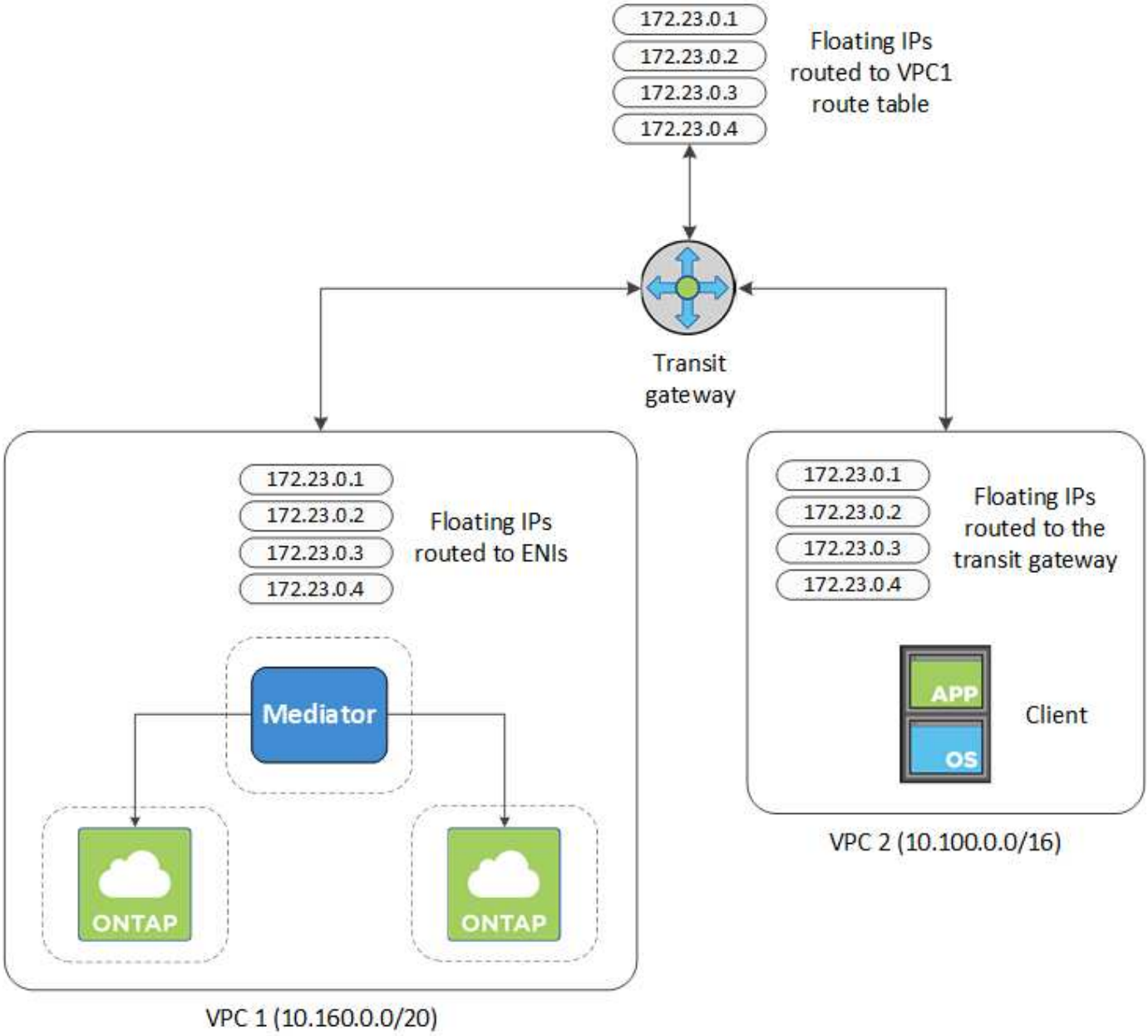
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA "Adresses IP flottantes" Depuis l'extérieur du VPC, où réside la paire HA.

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

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

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

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

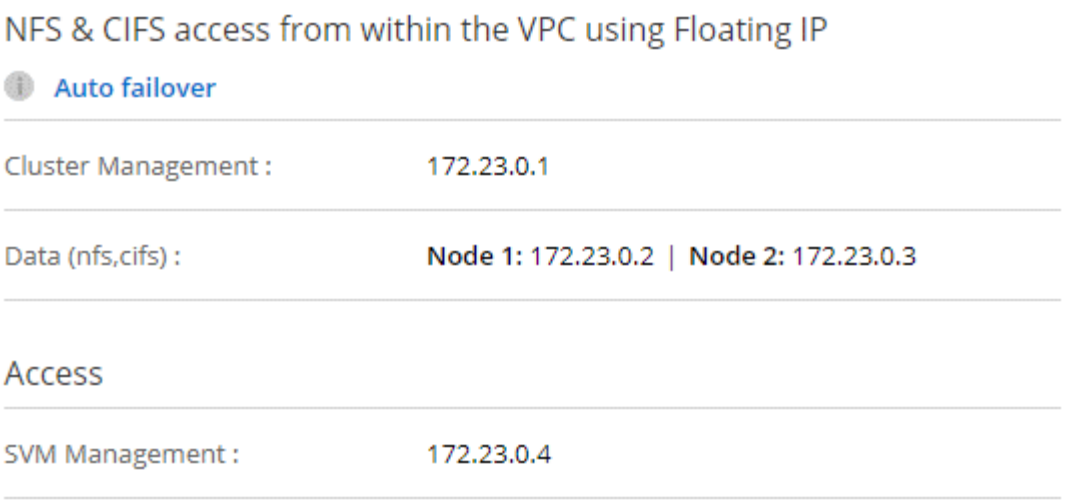


Les étapes suivantes montrent comment configurer une configuration similaire.

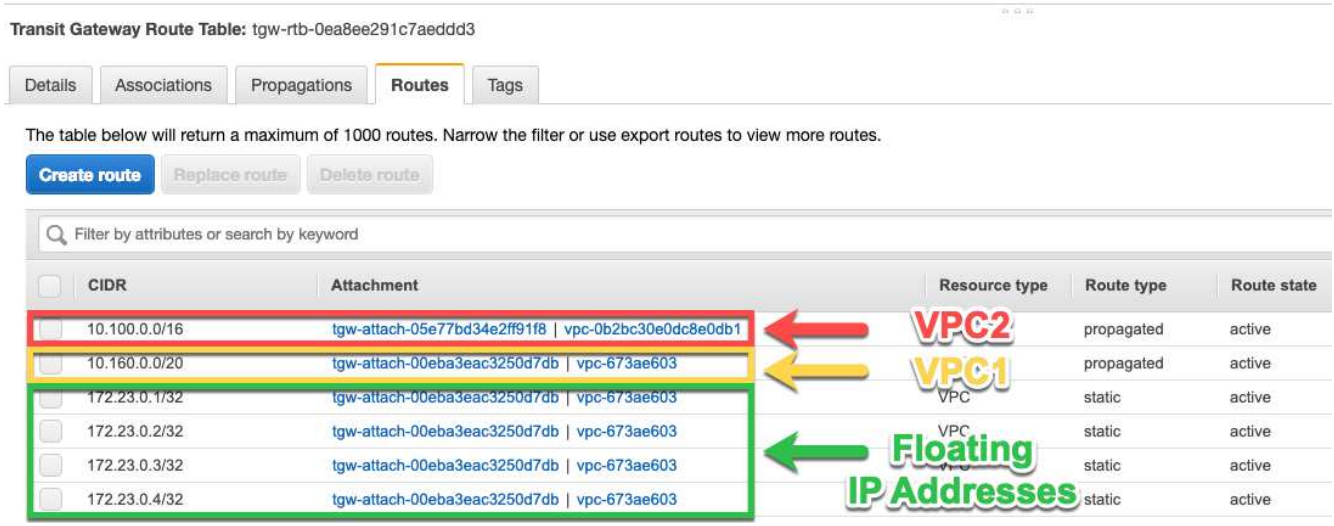
Étapes

1. "Créez une passerelle de transit et connectez les VPC à la passerelle".
2. Créer des routes dans la table de routage de la passerelle de transit en spécifiant les adresses IP flottantes de la paire HA.

   Les adresses IP flottantes se trouvent sur la page des informations sur l'environnement de travail dans Cloud Manager. Voici un exemple :



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

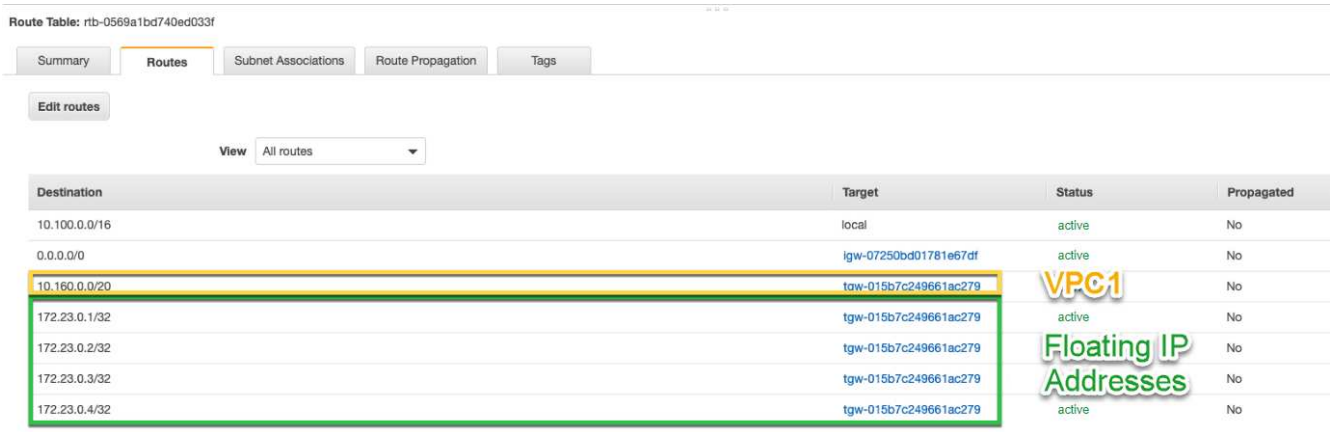


3. Modifiez la table de routage des VPC qui doivent accéder aux adresses IP flottantes.

   a. Ajoutez des entrées de route aux adresses IP flottantes.

   b. Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

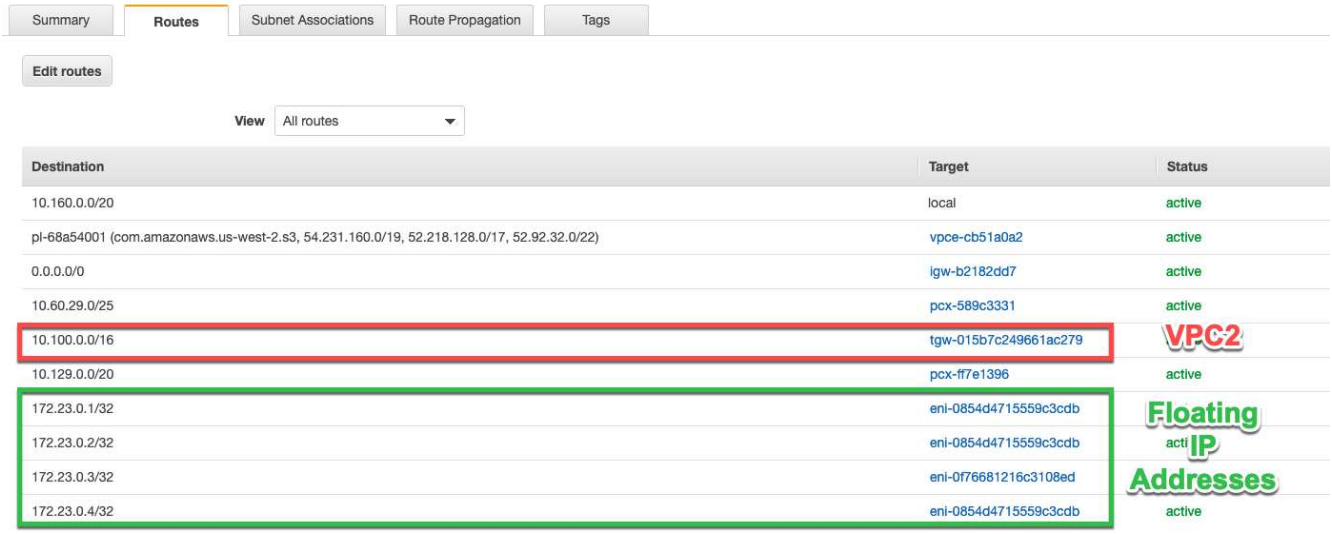
      L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.



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

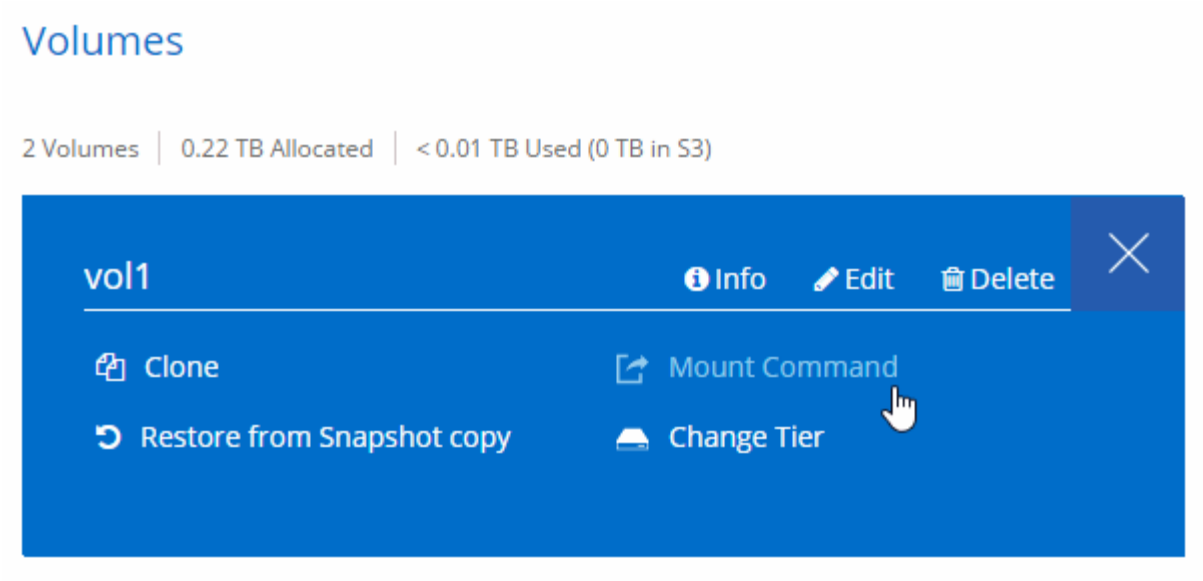
   Cette étape est importante car elle termine le routage entre les VPC.

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



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

   Vous trouverez l'adresse IP correcte dans Cloud Manager en sélectionnant un volume et en cliquant sur **Mount Command**.



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

Règles de groupe de sécurité pour AWS

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

Règles pour Cloud Volumes ONTAP

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

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

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

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
Sauvegarde vers S3	TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3

Service	Protocole	Port	Source	Destination	Objectif
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

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

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

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

Protocole	Port	Destination	Objectif
HTTP	80	Adresse IP du connecteur	Télécharger les mises à niveau pour le médiateur
HTTPS	443	Services API AWS	Assistance pour le basculement du stockage
UDP	53	Services API AWS	Assistance pour le basculement du stockage

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

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

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

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

Règles de sortie

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

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

Règles pour le connecteur

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

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers l'interface utilisateur locale et les connexions à partir de Cloud Compliance
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Fournit l'instance Cloud Compliance avec un accès Internet si votre réseau AWS n'utilise pas de NAT ou de proxy

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager
Conformité cloud	HTTP	80	Instance Cloud Compliance	Cloud Compliance pour Cloud Volumes ONTAP

Configuration du système AWS KMS

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

Étapes

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

   La CMK peut être une CMK gérée par AWS ou une CMK gérée par le client. Il peut être hébergé sur le même compte AWS que Cloud Manager et Cloud Volumes ONTAP ou dans un autre compte AWS.

   "Documentation AWS : clés principales client (CMK)"

2. Modifiez la stratégie clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations à Cloud Manager en tant que *utilisateur clé*.

   L'ajout du rôle IAM en tant qu'utilisateur clé donne aux utilisateurs Cloud Manager les autorisations d'utiliser le CMK avec Cloud Volumes ONTAP.

   "Documentation AWS : modification des clés"

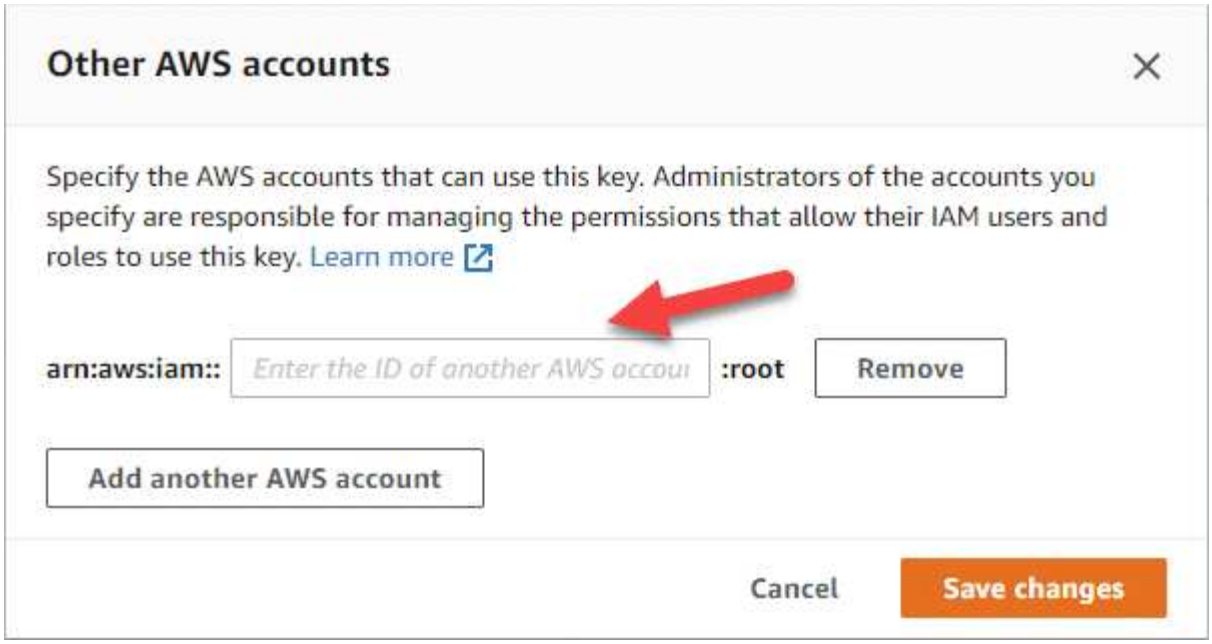
3. Si le CMK se trouve dans un autre compte AWS, procédez comme suit :

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

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

   d. Dans le volet **autres comptes AWS**, ajoutez le compte AWS qui fournit les autorisations à Cloud Manager.

      Dans la plupart des cas, il s'agit du compte sur lequel réside Cloud Manager. Si Cloud Manager n'a pas été installé dans AWS, il s'agit du compte sur lequel vous avez fourni les clés d'accès AWS à Cloud Manager.



e. Passez maintenant au compte AWS qui fournit les autorisations nécessaires à Cloud Manager et ouvrez la console IAM.

f. Créez une stratégie IAM qui inclut les autorisations répertoriées ci-dessous.

g. Associez la règle au rôle IAM ou à l'utilisateur IAM qui donne des autorisations à Cloud Manager.

   La règle suivante fournit les autorisations requises par Cloud Manager pour utiliser le CMK à partir du compte AWS externe. Veillez à modifier la région et l'ID de compte dans les sections « ressource ».

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

+
Pour plus d'informations sur ce processus, reportez-vous à la section "Documentation AWS : autoriser les comptes AWS externes à accéder à un CMK".

Lancement d’Cloud Volumes ONTAP dans AWS

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

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

Si vous souhaitez lancer Cloud Volumes ONTAP dans AWS, vous devez créer un nouvel environnement de travail dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

> Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l’avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Si vous souhaitez lancer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence).
- Si vous souhaitez utiliser CIFS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS".

Description de la tâche

Immédiatement après la création de l’environnement de travail, Cloud Manager lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, Cloud Manager met immédiatement fin à l’instance, puis lance le déploiement du système Cloud Volumes ONTAP. Si Cloud Manager ne parvient pas à vérifier la connectivité, la création de l’environnement de travail échoue. L’instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
3. **Détails et informations d’identification** : modifiez éventuellement les informations d’identification et l’abonnement AWS, entrez un nom d’environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

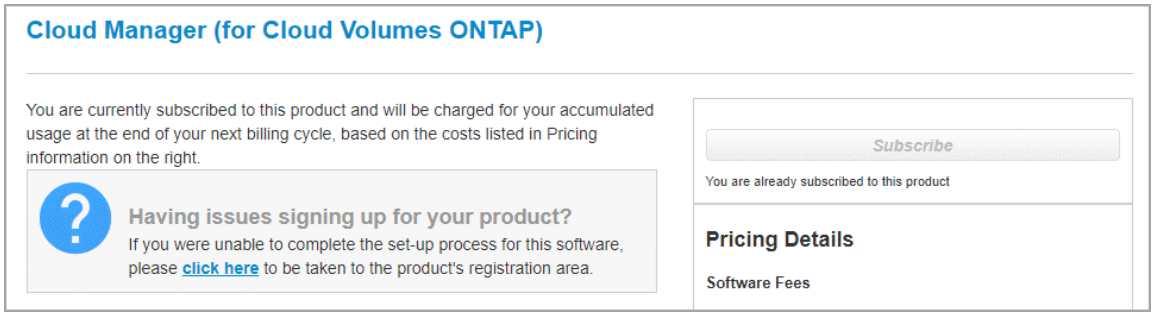
   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à l'utilisation, vous devez sélectionner les identifiants AWS associés à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP 9.6 ou ultérieur de PAYGO que vous créez et chaque fonctionnalité d'extension activée."Découvrez comment ajouter des identifiants AWS à Cloud Manager".

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

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

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

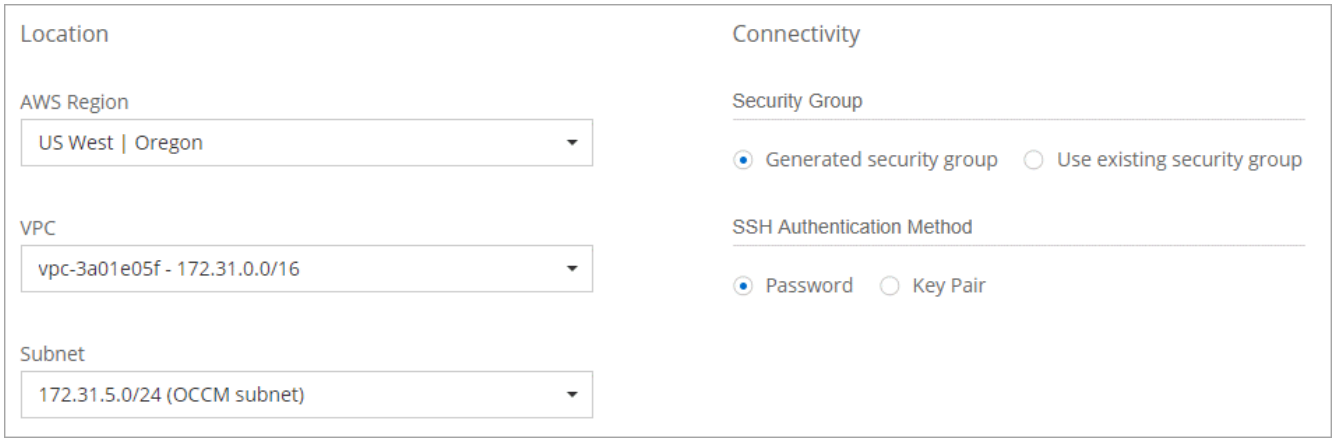


4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.

- "En savoir plus sur Cloud Compliance".
- "En savoir plus sur la sauvegarde dans le cloud".
- "En savoir plus sur la surveillance".

5. **Location & Connectivity** : saisissez les informations de réseau que vous avez enregistrées dans la fiche de travail AWS.

   L'image suivante montre la page remplie :



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

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

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

   "Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".

   "En savoir plus sur les technologies de cryptage prises en charge".

7. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

   Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

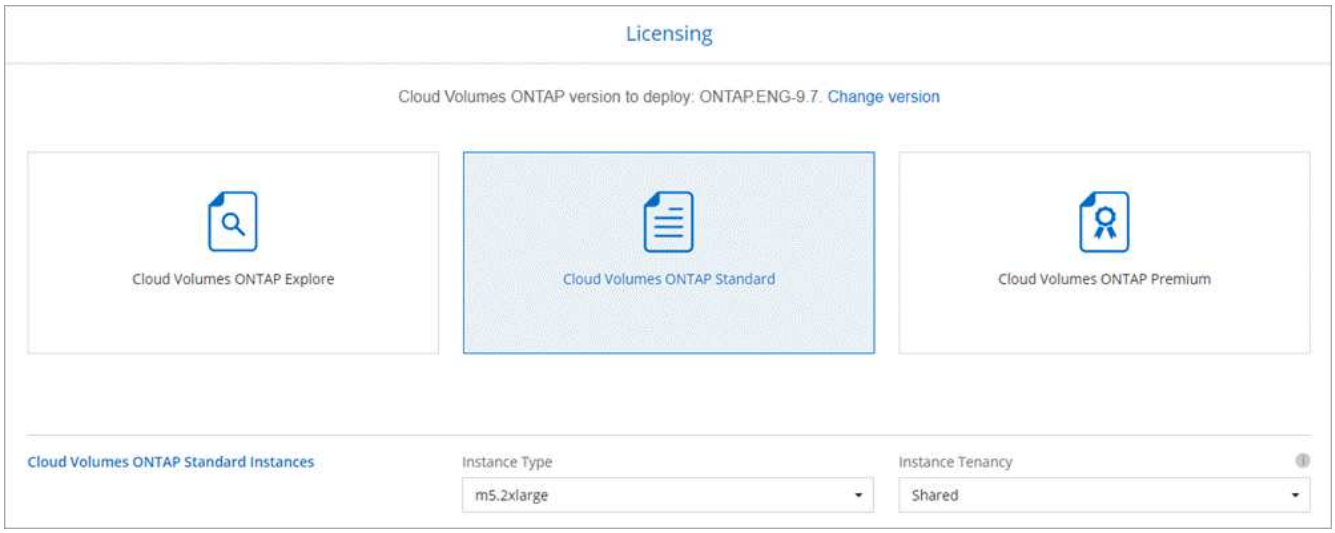
8. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement Cloud Volumes ONTAP, ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

9. **Rôle IAM** : vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer le rôle pour vous.

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

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



Si vos besoins changent après le lancement de l'instance, vous pouvez modifier la licence ou le type d'instance ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

11. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données doit être activée.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement de votre système dans AWS".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "Découvrez le fonctionnement du Tiering des données".

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

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

"En savoir plus sur la vitesse d'écriture".

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

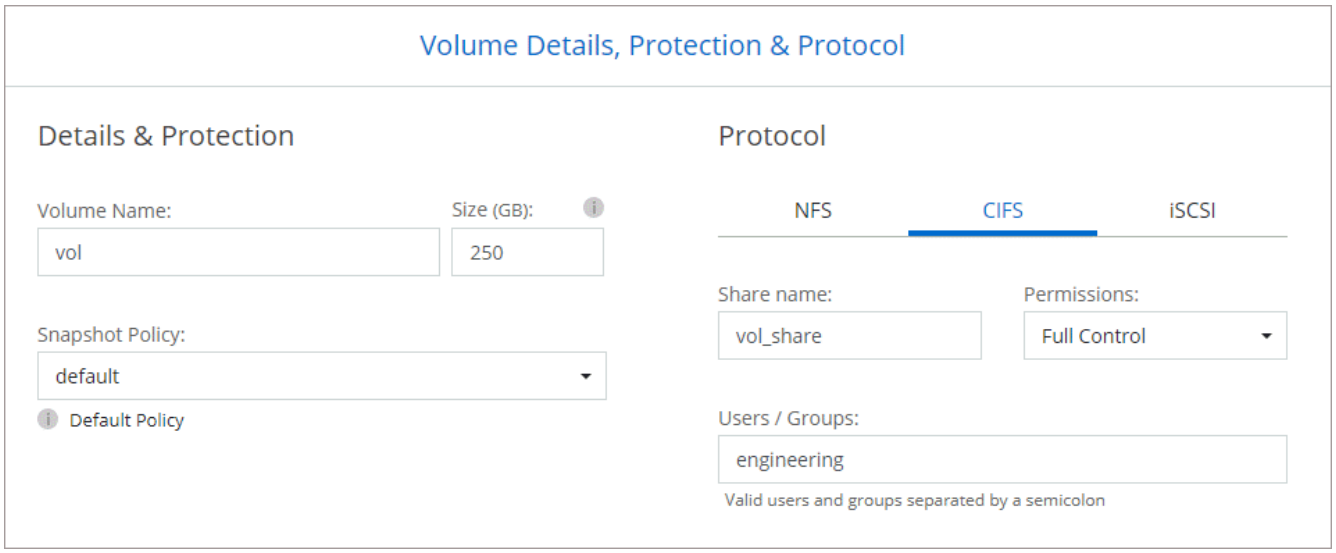
"En savoir plus sur le stockage WORM".

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

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

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

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



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

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

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

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

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

a. Consultez les détails de la configuration.

b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.

c. Cochez les cases **Je comprends…**.

d. Cliquez sur **Go**.

Résultat

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

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

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

Une fois que vous avez terminé

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

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

Lancement d'une paire Cloud Volumes ONTAP HA dans AWS

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

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

  Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Si vous avez acheté des licences BYOL, vous devez disposer d'un numéro de série à 20 chiffres (clé de licence) pour chaque nœud.
- Si vous souhaitez utiliser CIFS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS".

Restriction

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

Description de la tâche

Immédiatement après la création de l'environnement de travail, Cloud Manager lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, Cloud Manager met immédiatement fin à l'instance, puis lance le déploiement du système Cloud Volumes ONTAP. Si Cloud Manager ne parvient pas à vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

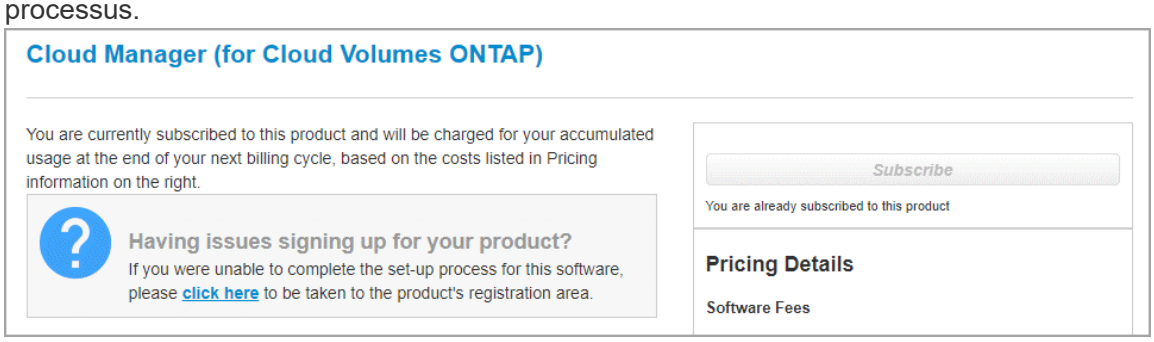
   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à l'utilisation, vous devez sélectionner les identifiants AWS associés à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP 9.6 ou ultérieur de PAYGO que vous créez et chaque fonctionnalité d'extension activée."Découvrez comment ajouter des identifiants AWS à Cloud Manager".

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

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

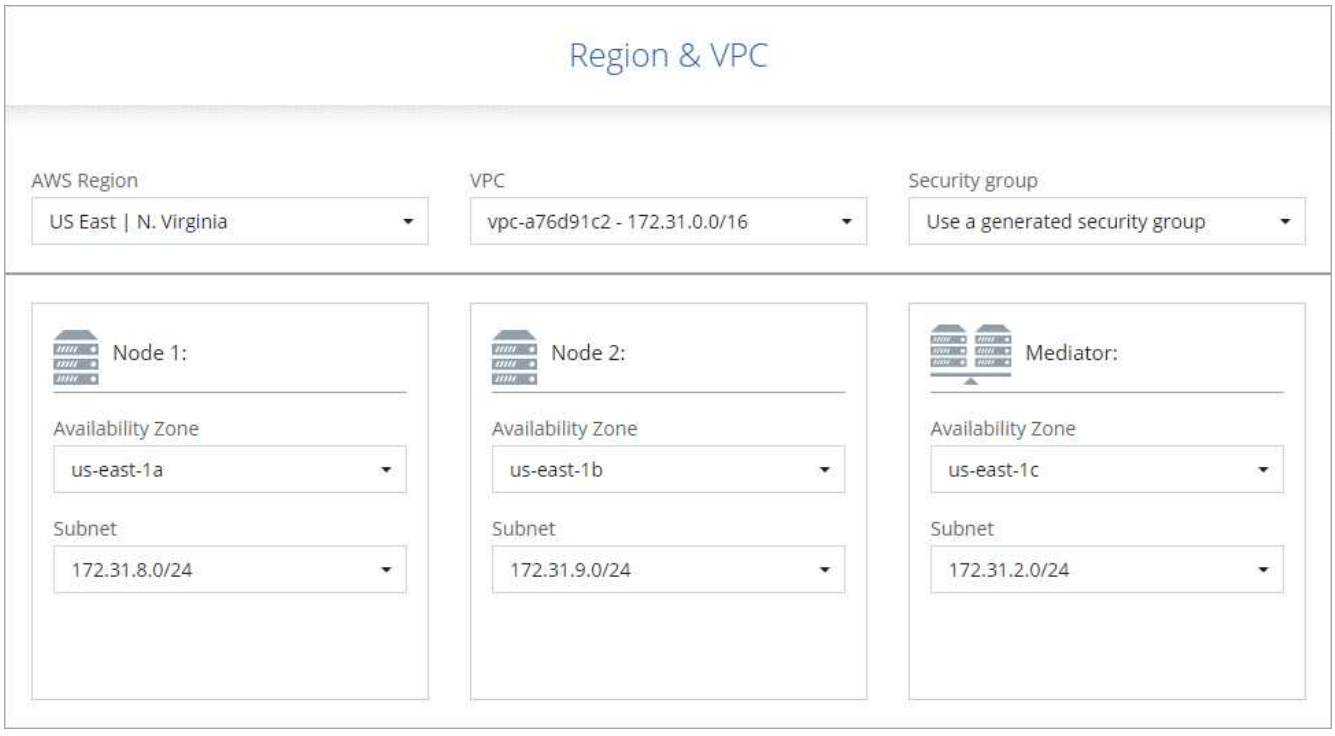
Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS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



4. **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 Cloud Compliance".
   - "En savoir plus sur la sauvegarde dans le cloud".
   - "En savoir plus sur la surveillance".
5. **Modèles de déploiement haute disponibilité** : choisir une configuration haute disponibilité.

   Pour obtenir un aperçu des modèles de déploiement, voir "Cloud Volumes ONTAP HA pour AWS".
6. **Région et VPC** : saisissez les informations de réseau que vous avez enregistrées dans la fiche AWS.

   L'image suivante montre la page remplie pour une configuration plusieurs AZ :



7. **Connectivité et authentification SSH** : choisissez des méthodes de connexion pour la paire HA et le médiateur.
8. **IP flottantes** : si vous choisissez plusieurs adresses AZS, spécifiez les adresses IP flottantes.

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

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

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

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

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

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

    "Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".

    "En savoir plus sur les technologies de cryptage prises en charge".

11. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

    Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

    Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

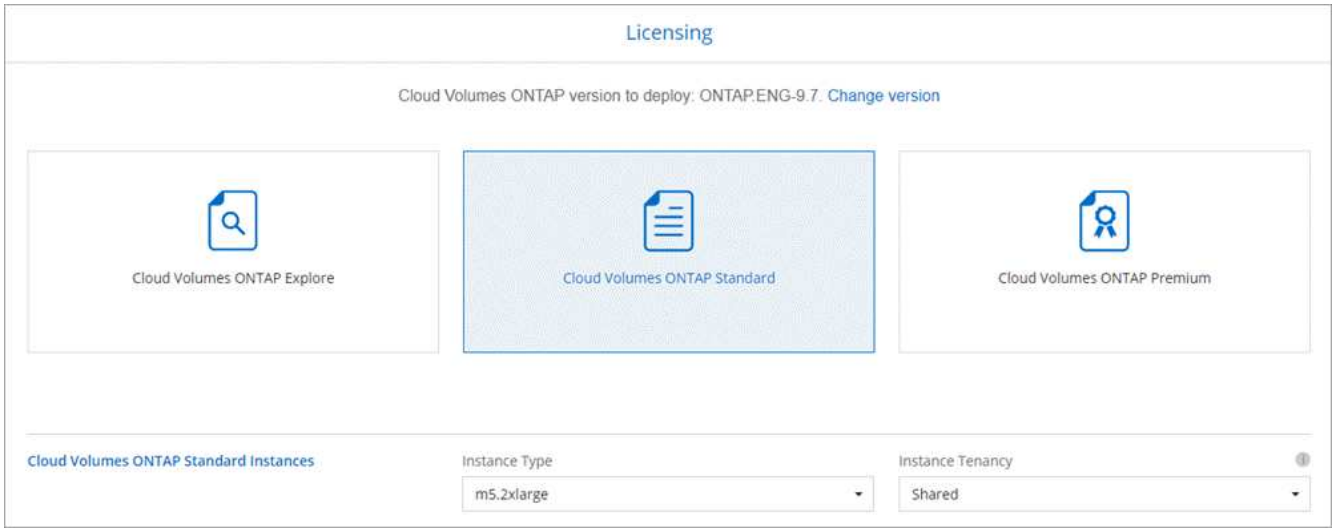
12. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

    Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

13. **Rôle IAM** : vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer les rôles pour vous.

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

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



Si vos besoins changent après le lancement des instances, vous pouvez modifier la licence ou le type d'instance ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

15. **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 doit être activée.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement de votre système dans AWS".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "Découvrez le fonctionnement du Tiering des données".

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

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

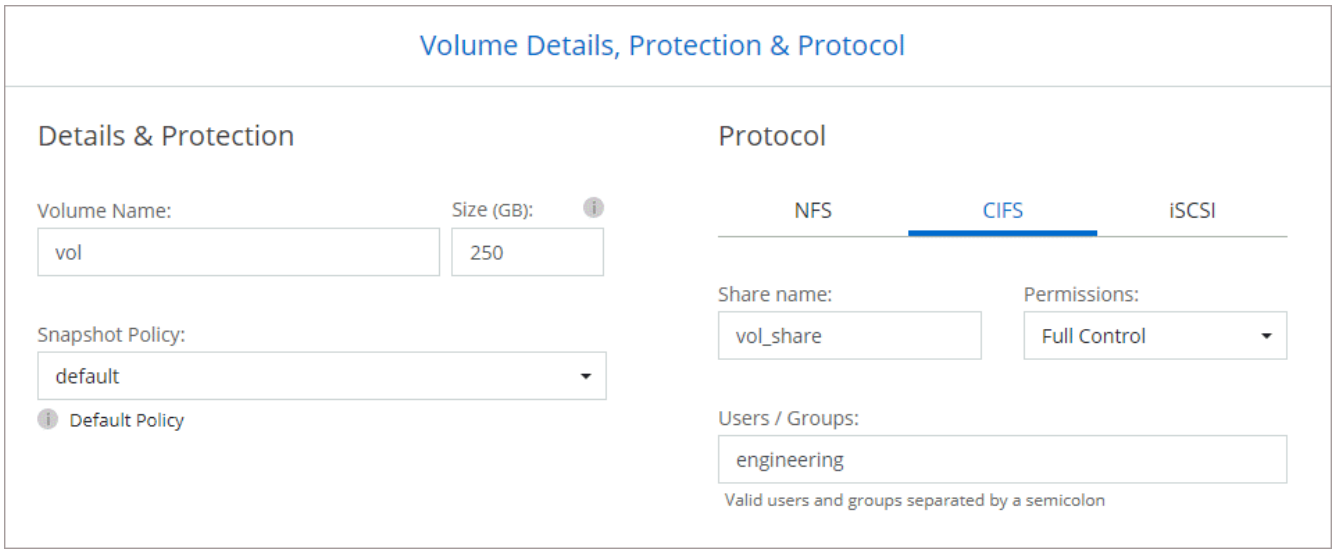
    "En savoir plus sur le stockage WORM".

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

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

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

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



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

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

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

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

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

a. Consultez les détails de la configuration.

b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.

c. Cochez les cases **Je comprends…**.

d. Cliquez sur **Go**.

Résultat

Cloud Manager lance la paire Cloud Volumes ONTAP HA. Vous pouvez suivre la progression dans la chronologie.

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

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

Une fois que vous avez terminé

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

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

Informations sur le copyright

Informations sur les marques commerciales