Commencer

Cloud Volumes ONTAP

NetApp
February 13, 2026

Sommaire

Commencer . . . 1
- En savoir plus sur Cloud Volumes ONTAP . . . 1
- Versions ONTAP prises en charge pour les déploiements Cloud Volumes ONTAP . . . 2
  - AWS . . . 2
  - Azuré . . . 3
  - Google Cloud . . . 4
- Démarrer avec Amazon Web Services . . . 5
  - Démarrage rapide de Cloud Volumes ONTAP dans AWS . . . 5
  - Planifiez votre configuration Cloud Volumes ONTAP dans AWS . . . 6
  - Configurez votre réseau . . . 10
  - Configurer Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans AWS . . . 35
  - Configurer les rôles AWS IAM pour les nœuds Cloud Volumes ONTAP . . . 39
  - Configurer les licences pour Cloud Volumes ONTAP dans AWS . . . 48
  - Déployer Cloud Volumes ONTAP dans AWS à l'aide d'un déploiement rapide . . . 56
  - Lancer Cloud Volumes ONTAP dans AWS . . . 60
  - Déployer Cloud Volumes ONTAP dans AWS Secret Cloud ou AWS Top Secret Cloud . . . 74
- Démarrer avec Microsoft Azure . . . 91
  - Découvrez les options de déploiement de Cloud Volumes ONTAP dans Azure . . . 91
  - Démarrer dans la NetApp Console . . . 93
  - Déployer Cloud Volumes ONTAP depuis la place de marché Azure . . . 146
- Démarrer avec Google Cloud . . . 150
  - Démarrage rapide de Cloud Volumes ONTAP dans Google Cloud . . . 150
  - Planifiez votre configuration Cloud Volumes ONTAP dans Google Cloud . . . 151
  - Configurer la mise en réseau Google Cloud pour Cloud Volumes ONTAP . . . 155
  - Configurer VPC Service Controls pour déployer Cloud Volumes ONTAP dans Google Cloud . . . 167
  - Créer un compte de service Google Cloud pour Cloud Volumes ONTAP . . . 169
  - Utilisation de clés de chiffrement gérées par le client avec Cloud Volumes ONTAP . . . 172
  - Configurer les licences pour Cloud Volumes ONTAP dans Google Cloud . . . 173
  - Lancer Cloud Volumes ONTAP dans Google Cloud . . . 178
  - Vérification d'image de Google Cloud Platform . . . 191

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 NetApp Console 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 listées ici ne sont pas disponibles pour les nouveaux déploiements. Le correctif ou la version générique (General Availability) d'une version ici représente la version de base disponible pour le déploiement. Pour plus d'informations sur les correctifs disponibles, consultez la "notes de version avec gestion des versions" pour chaque version.

Pour plus d'informations sur la mise à niveau, consultez "Chemins de mise à niveau pris en charge".

AWS

Nœud unique

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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

- 9.18.1

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

paire HA

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Nœud unique

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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 NetApp Console 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 vers le service Amazon Simple Storage Service (Amazon 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

- Faites correspondre 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 NetApp Console 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 à débit optimisé (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 Amazon Simple Storage Service (Amazon S3) n'est pas prise en charge si votre système Cloud Volumes ONTAP se trouve dans une zone locale AWS, car l'accès aux compartiments Amazon S3 en dehors de la zone locale implique une latence plus élevée et impacte les activités de Cloud Volumes ONTAP.

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"créez 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 zone de disponibilité

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	
Zone de disponibilité du médiateur	
Sous-réseau médiateur	
Paire de clés pour le médiateur	
Adresse IP flottante pour le port de gestion du cluster	

Informations sur les AWS	Votre valeur
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 NetApp Console 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
\ https://netapp-cloud-account.auth0.com	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : • Services Cloud Volumes ONTAP • Services ONTAP • Protocoles et services proxy
\ https://api.bluexp.netapp.com/tenancy	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.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	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	Modes de déploiement	Impact si le point de terminaison n'est pas disponible
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" .	• CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Amazon Simple Storage Service (S3)	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.
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.	• CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	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 établir 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 NetApp Console

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 d'interfaces logiques (LIF) que la NetApp Console alloue pour Cloud Volumes ONTAP dépend du fait que vous déployiez un système à nœud unique ou une paire haute disponibilité. Une LIF est une adresse IP associée à un port physique.

Adresses IP pour un système à nœud unique

La NetApp Console alloue 6 adresses IP à un système à nœud unique.

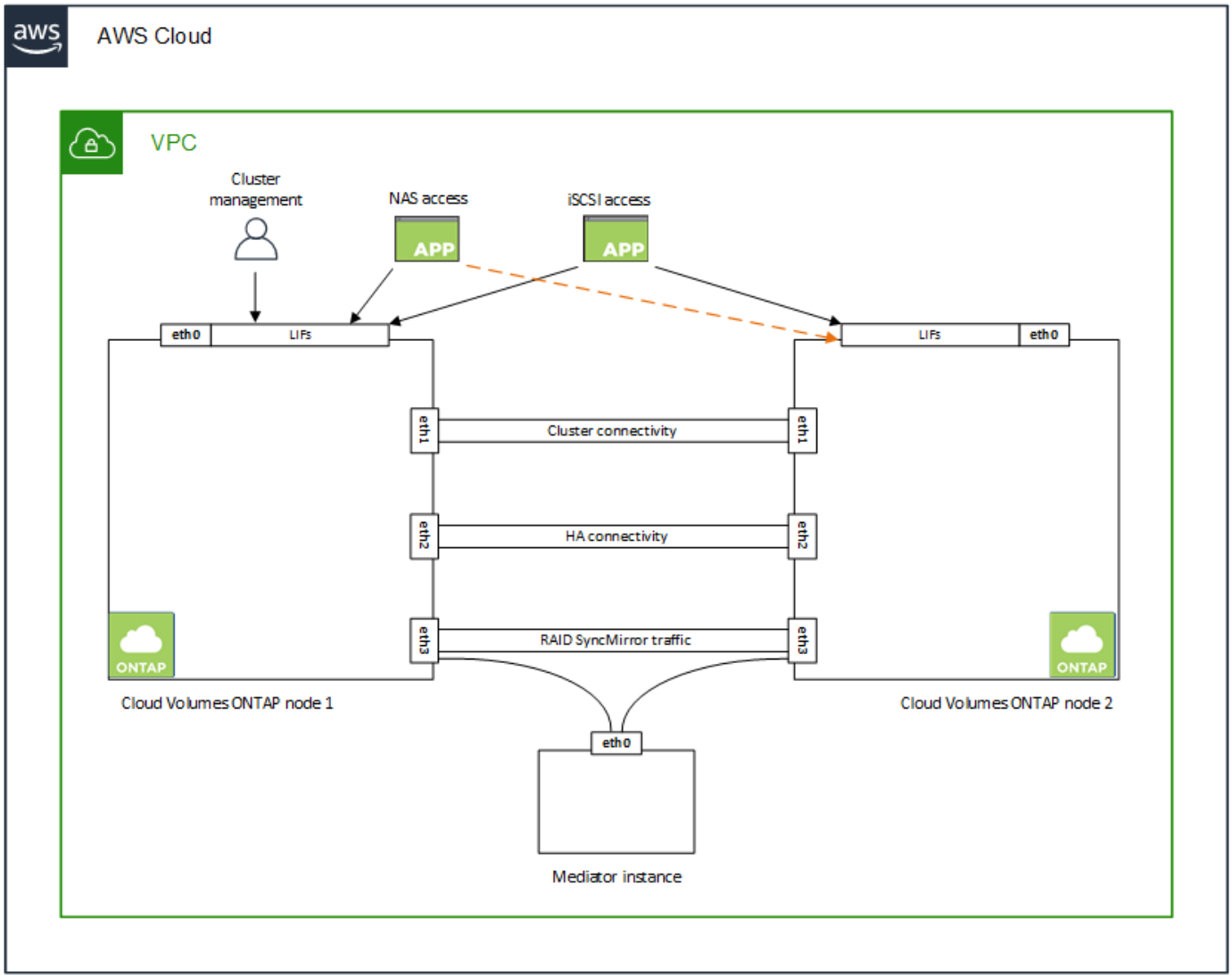
Le tableau suivant fournit des détails sur les LIF associés à chaque adresse IP privée.

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.
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 haute disponibilité 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.
Intercluster	eth0	nœud 1 et nœud 2	Communication, sauvegarde et réplication inter-cluster.
Données NAS	eth0	nœud 1	Accès client via les protocoles NAS.

FRV	Interface	Nœud	But
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 Amazon 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 vers le service S3. Pour obtenir des instructions, consultez le "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 la gestion des données NAS et 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" .

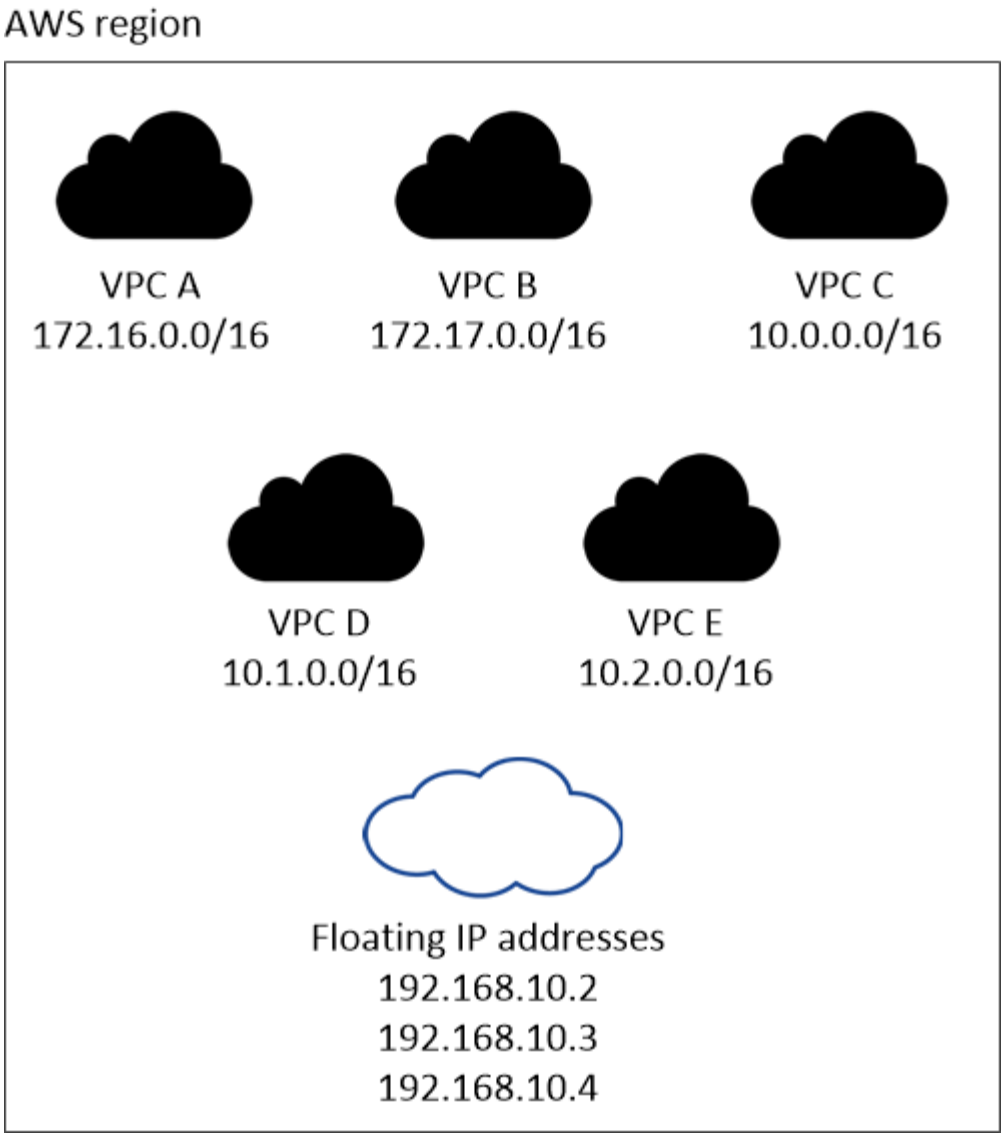
Une adresse IP flottante est destinée à la gestion du cluster, une autre aux données NFS/CIFS sur le nœud 1 et une autre aux données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante pour la gestion SVM est facultative.

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.



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" .

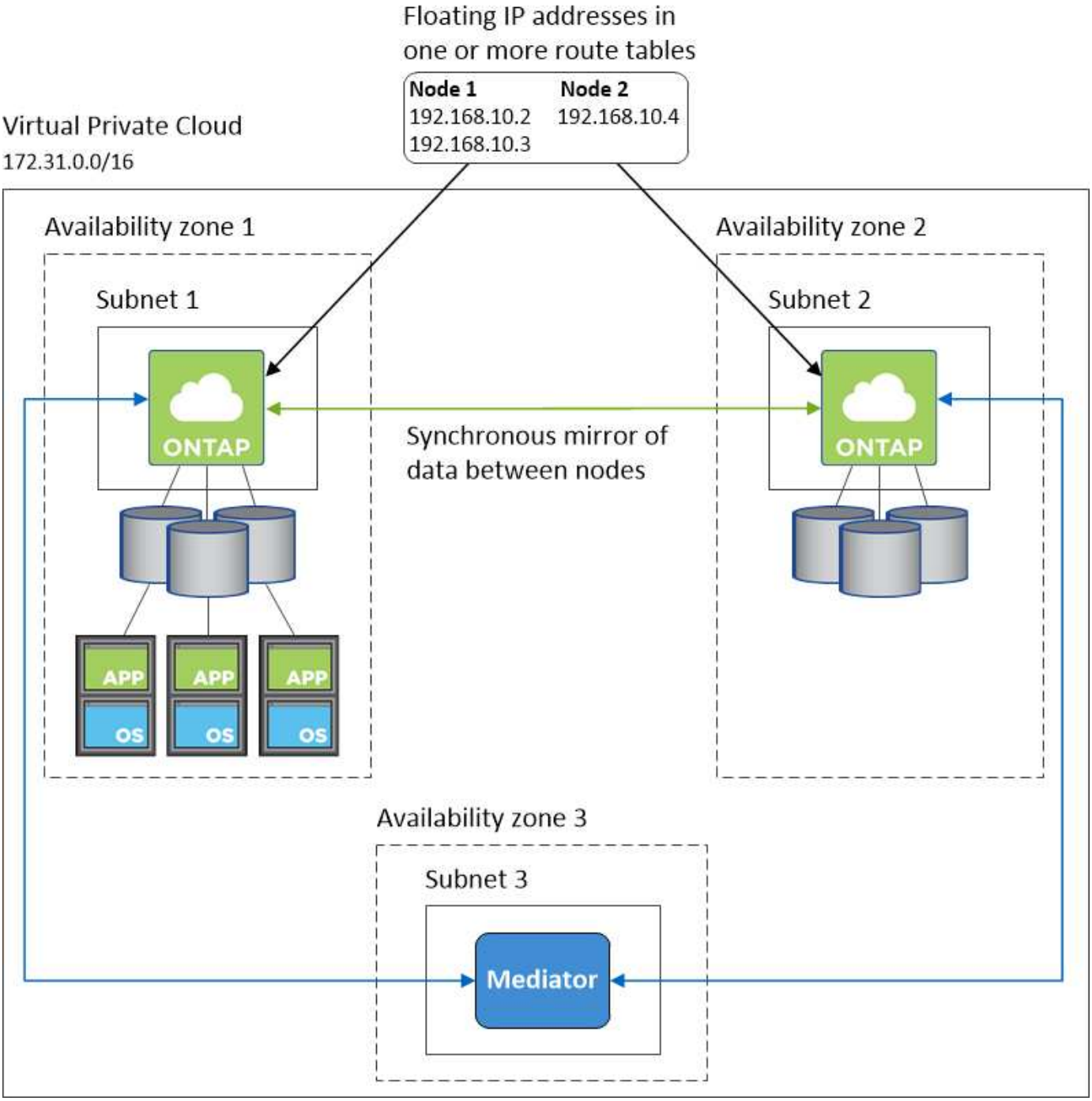
Connexion aux outils de gestion NetApp

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

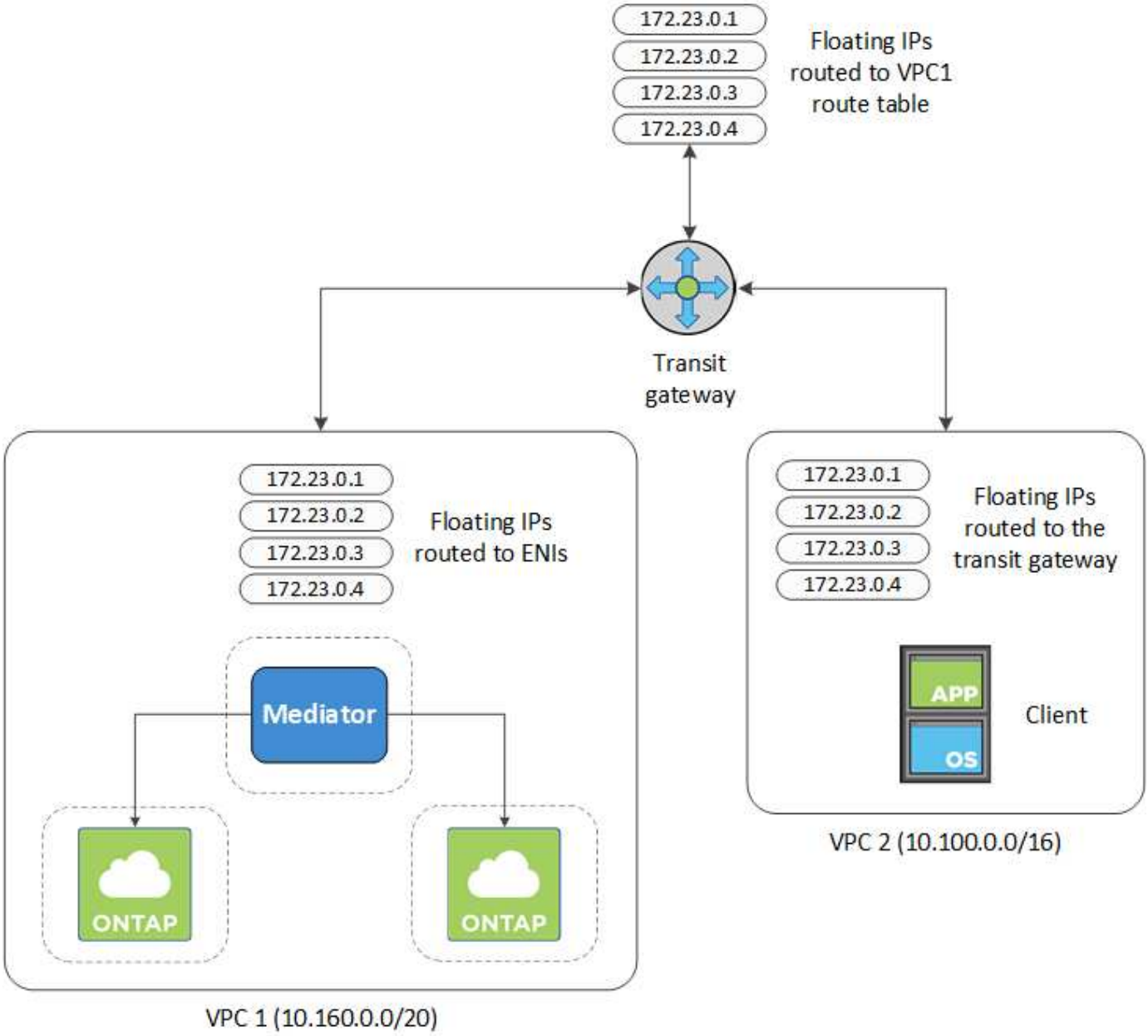
Configurer une passerelle de transit AWS pour permettre l'accès à une paire HA"adresses IP flottantes" depuis l'extérieur du VPC où réside la paire HA.

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.

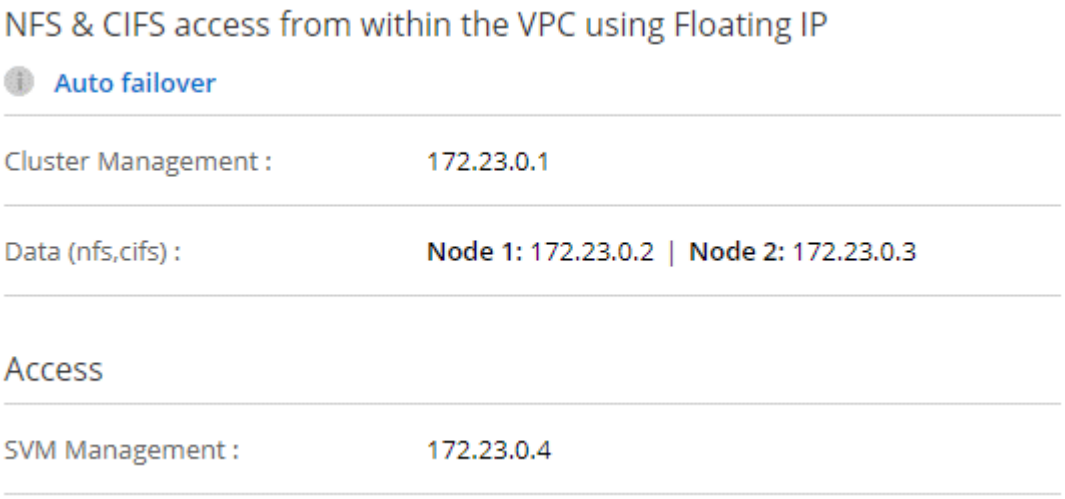


Les étapes suivantes illustrent comment configurer une configuration similaire.

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.

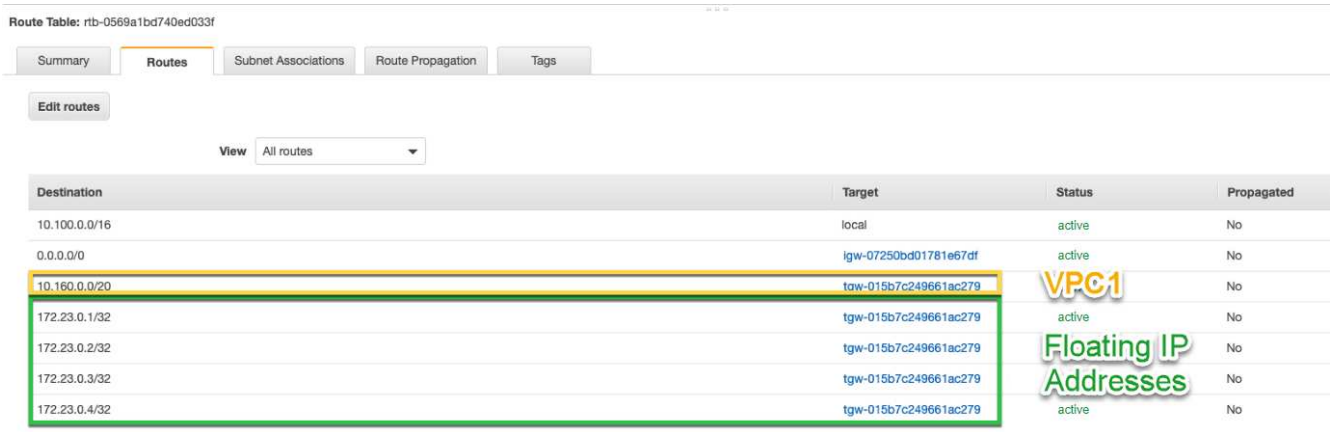
   Vous pouvez trouver les adresses IP flottantes sur la page d'informations système dans la NetApp Console. Voici un exemple :



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.

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

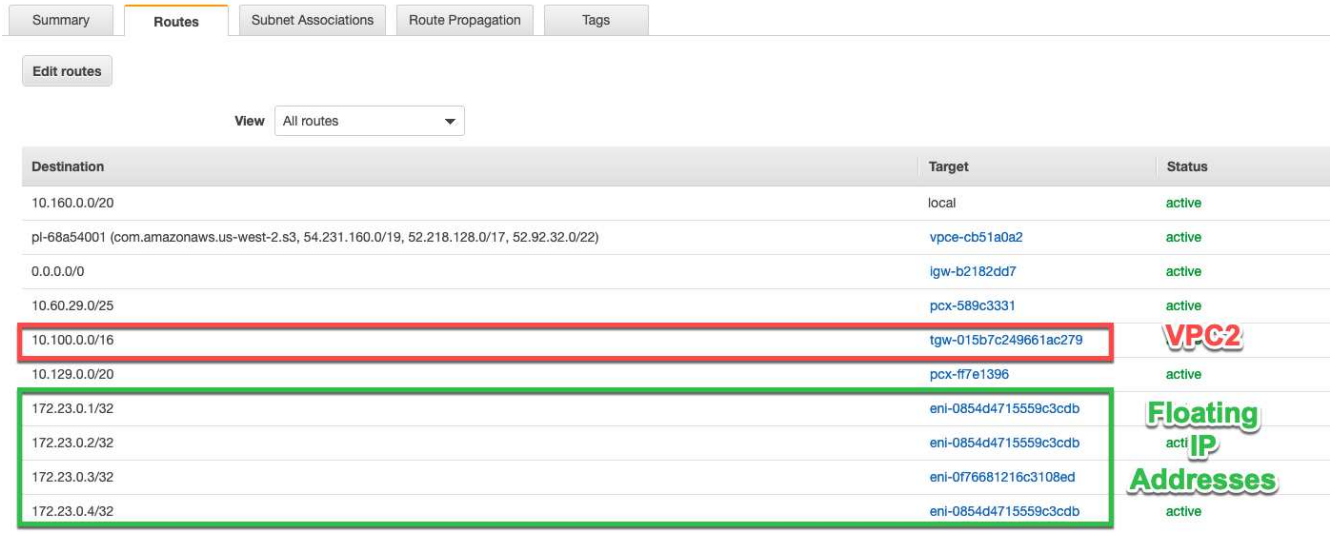
      L'exemple d'image suivant montre la table de routage pour VPC 2, qui inclut les routes vers VPC 1 et les adresses IP flottantes.



5. 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.

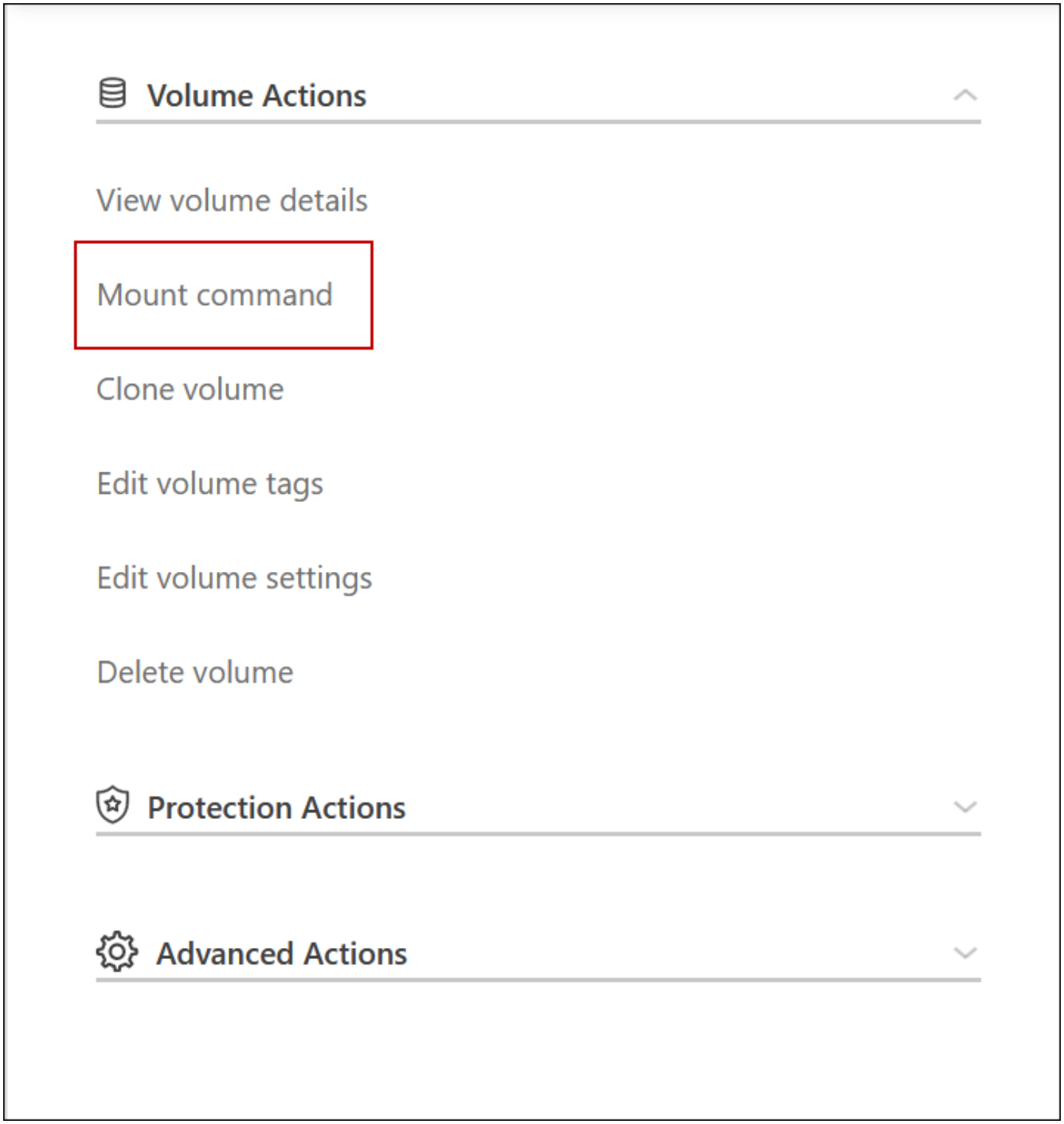
   L'exemple d'image suivant montre la table de routage pour VPC 1. Il comprend un itinéraire vers les adresses IP flottantes et vers le VPC 2, où réside un client. La console a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire HA.



6. Mettez à jour les paramètres des groupes de sécurité sur Tout le trafic pour le VPC.
   a. Sous Cloud privé virtuel, cliquez sur **Sous-réseaux**.
   b. Cliquez sur l'onglet **Table de routage**, sélectionnez l'environnement souhaité pour l'une des adresses IP flottantes pour une paire HA.
   c. Cliquez sur **Groupes de sécurité**.
   d. Sélectionnez **Modifier les règles entrantes**.
   e. Cliquez sur **Ajouter une règle**.
   f. Sous Type, sélectionnez **Tout le trafic**, puis sélectionnez l'adresse IP du VPC.
   g. Cliquez sur **Enregistrer les règles** pour appliquer les modifications.
7. 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

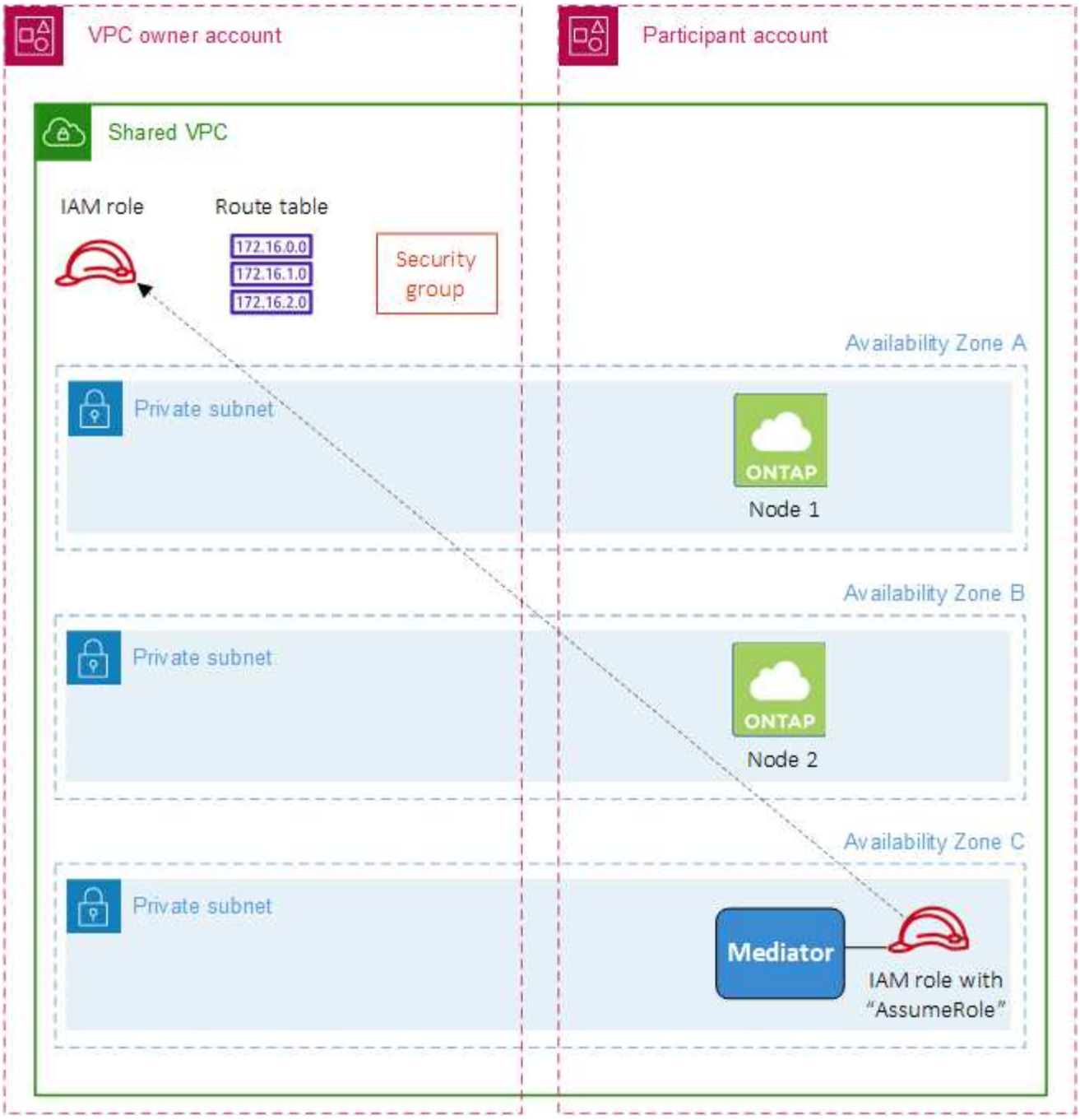
À partir de la version 9.11.1, les paires Cloud Volumes ONTAP HA sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre organisation de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement AWS, puis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



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

Lorsque vous créez le système Cloud Volumes ONTAP , la NetApp Console crée et attache automatiquement un rôle IAM au médiateur. Ce rôle assume le rôle IAM que vous avez créé dans le compte propriétaire du VPC afin d'apporter des modifications aux tables de routage associées à la paire HA.

Étapes

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

   Cette étape est nécessaire pour déployer la paire HA dans des sous-réseaux partagés.

   "Documentation AWS : Partager un sous-réseau"

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) 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 NetApp Console 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 NetApp Console crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes dont Cloud Volumes ONTAP a besoin pour fonctionner correctement. Vous souhaiterez 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)
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."Documentation ONTAP"
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	18600–18699	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 NetApp Console 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 nécessaires pour utiliser la CMK avec Cloud Volumes ONTAP.

   "Documentation AWS : Modification des clés"

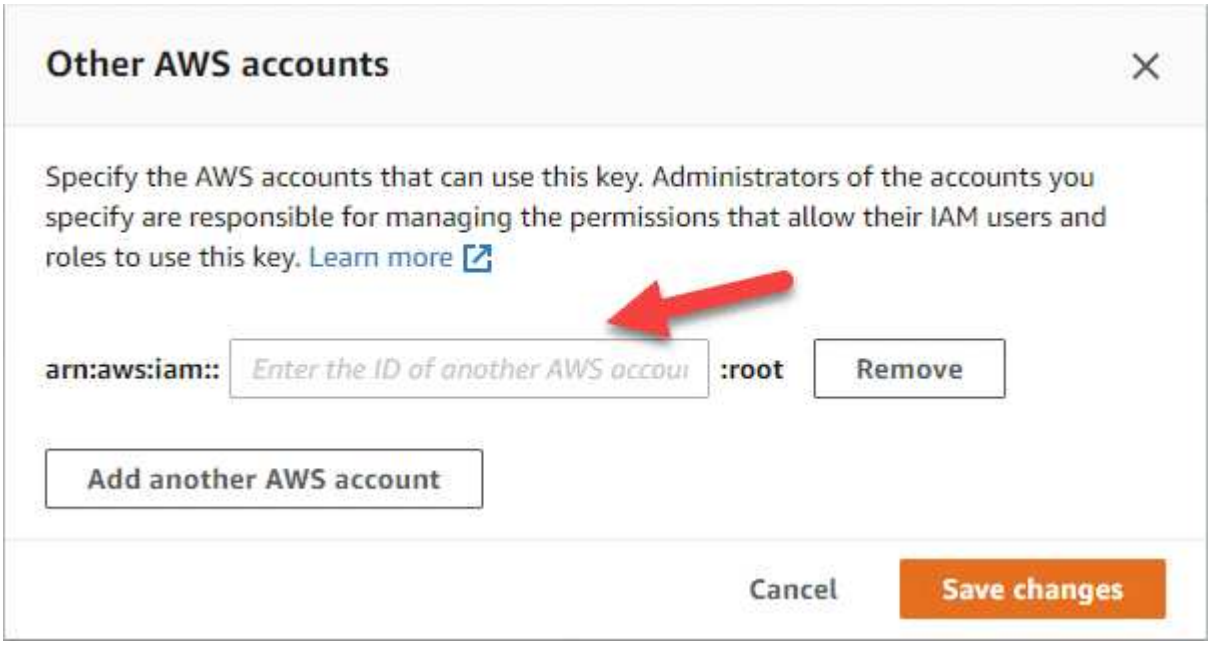
3. Si la CMK se trouve dans un autre compte AWS, procédez comme suit :

   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 nécessaire si vous avez activé la hiérarchisation des données sur Cloud Volumes ONTAP et que vous souhaitez chiffrer les données stockées dans le compartiment Amazon Simple Storage Service (Amazon 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 NetApp Console 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

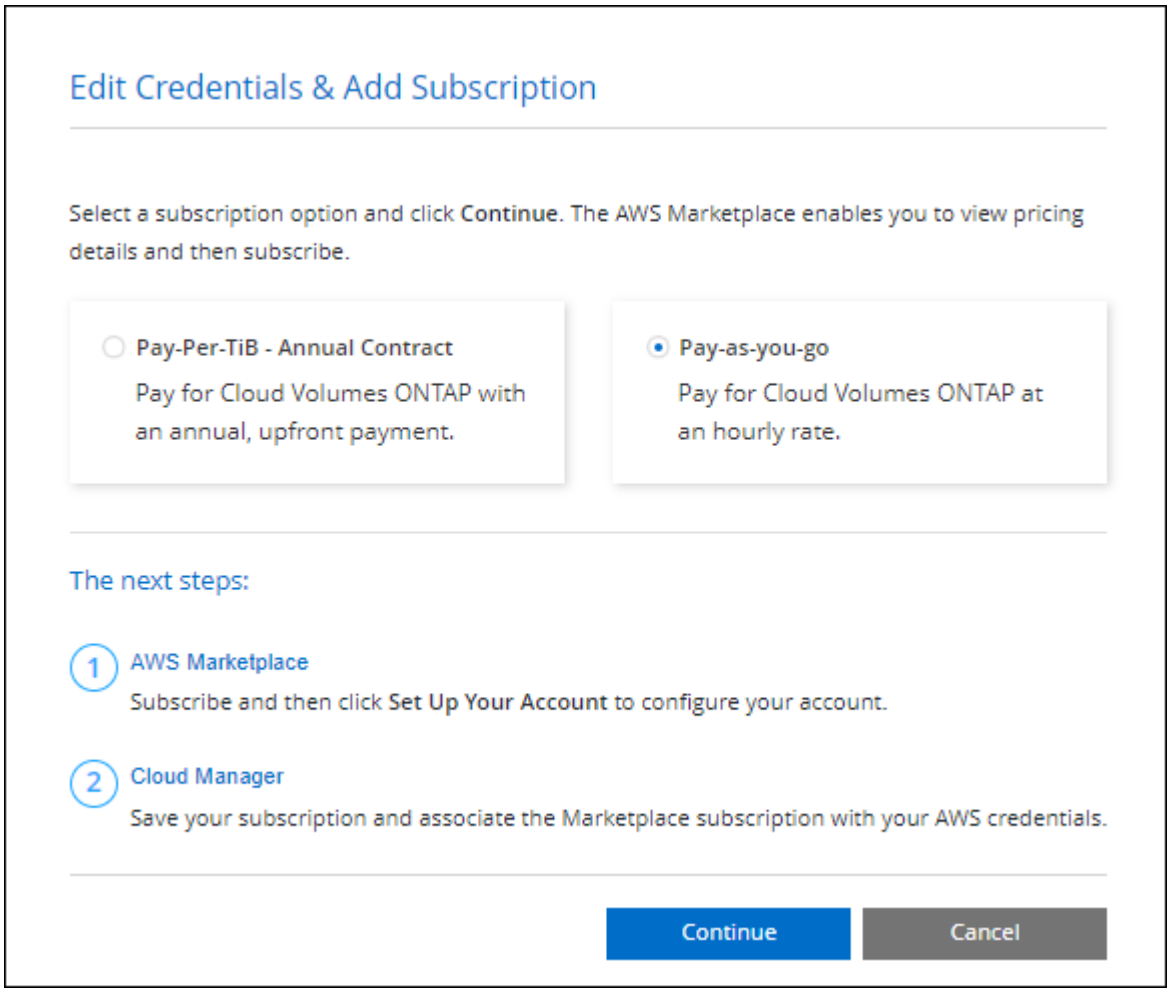
Sélectionnez l'offre Freemium pour utiliser Cloud Volumes ONTAP gratuitement avec jusqu'à 500 Gio de capacité provisionnée. "En savoir plus sur l'offre Freemium" .

Étapes

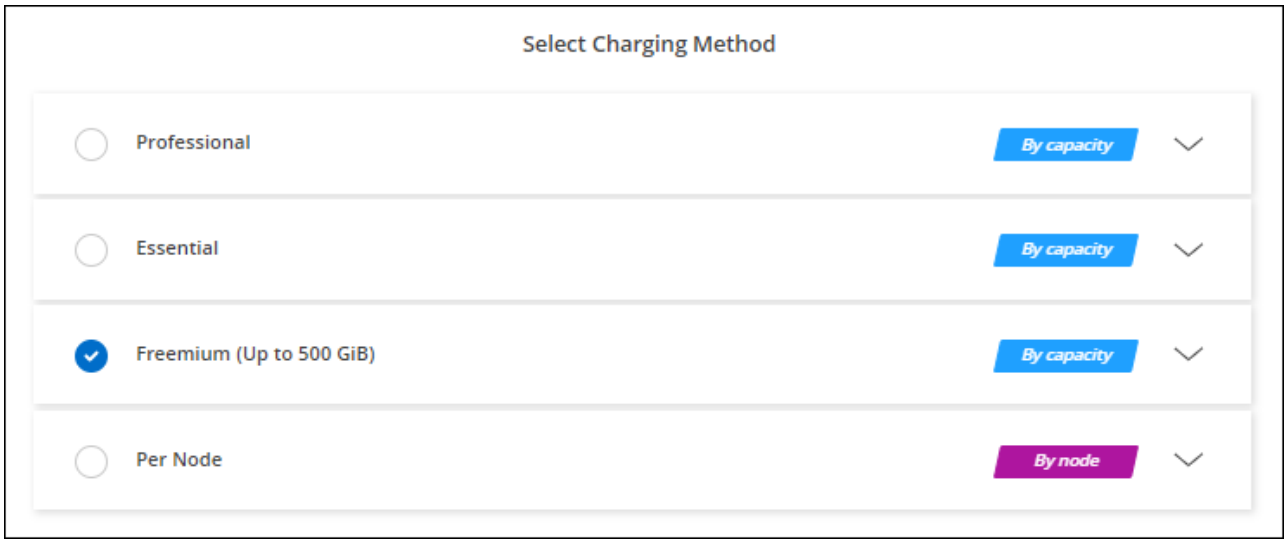
1. Dans le menu de navigation de gauche de la NetApp Console, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

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" .



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



"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 formules Essentiel et Professionnel sont disponibles avec les modèles de consommation ou options d'achat 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.

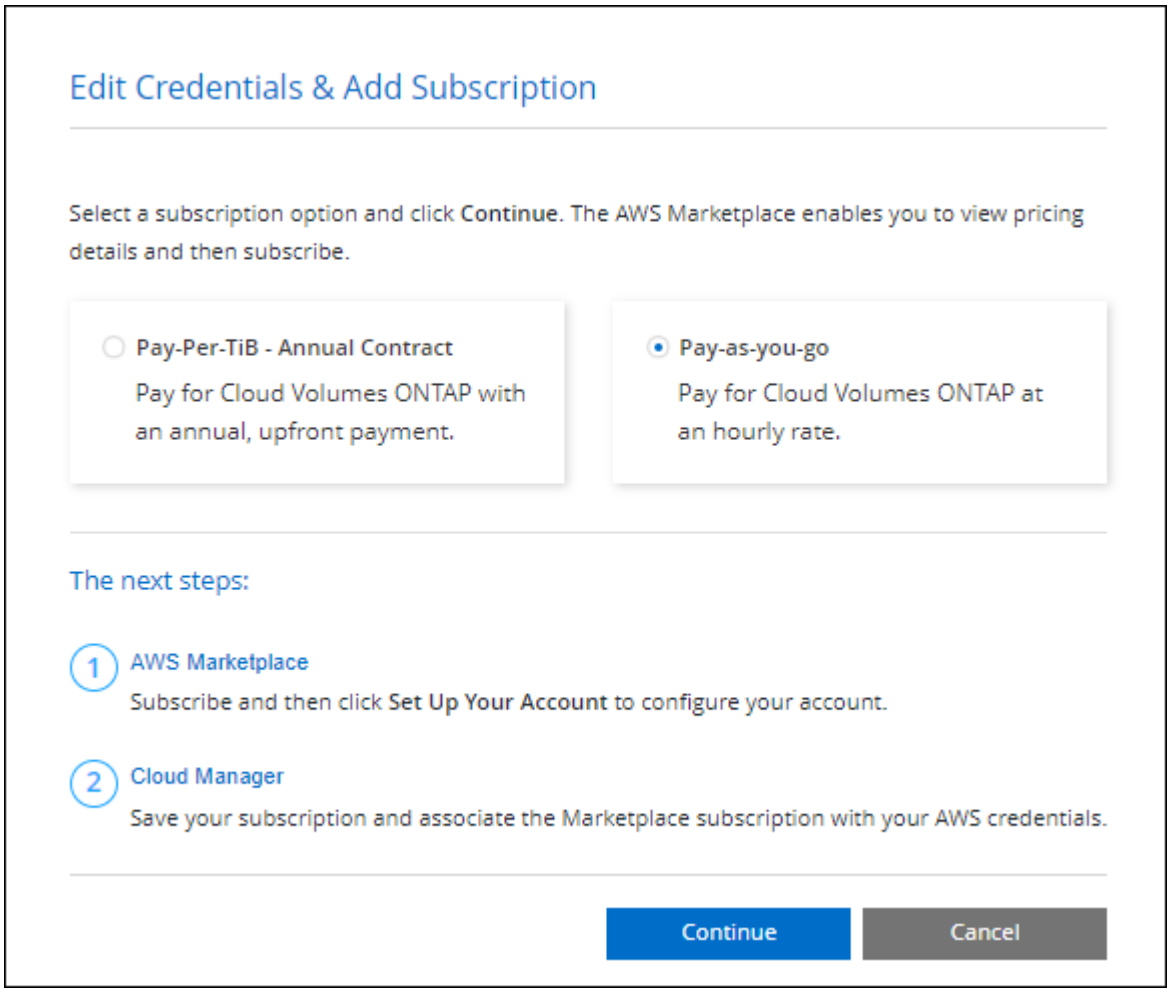
   Votre licence doit être disponible depuis la console avant de pouvoir l'utiliser avec Cloud Volumes ONTAP.

Si nécessaire, vous pouvez"ajouter manuellement la licence à la console" .

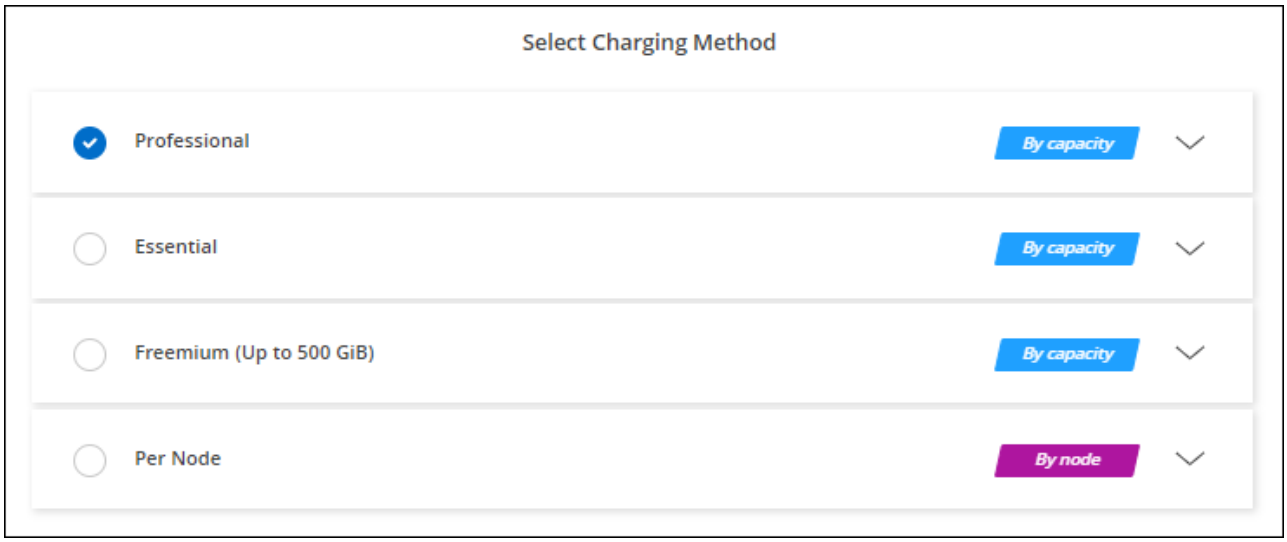
3. Sur la page **Systèmes** de la console, cliquez sur **Ajouter un système** et suivez les étapes.

   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.



   a. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans AWS" .

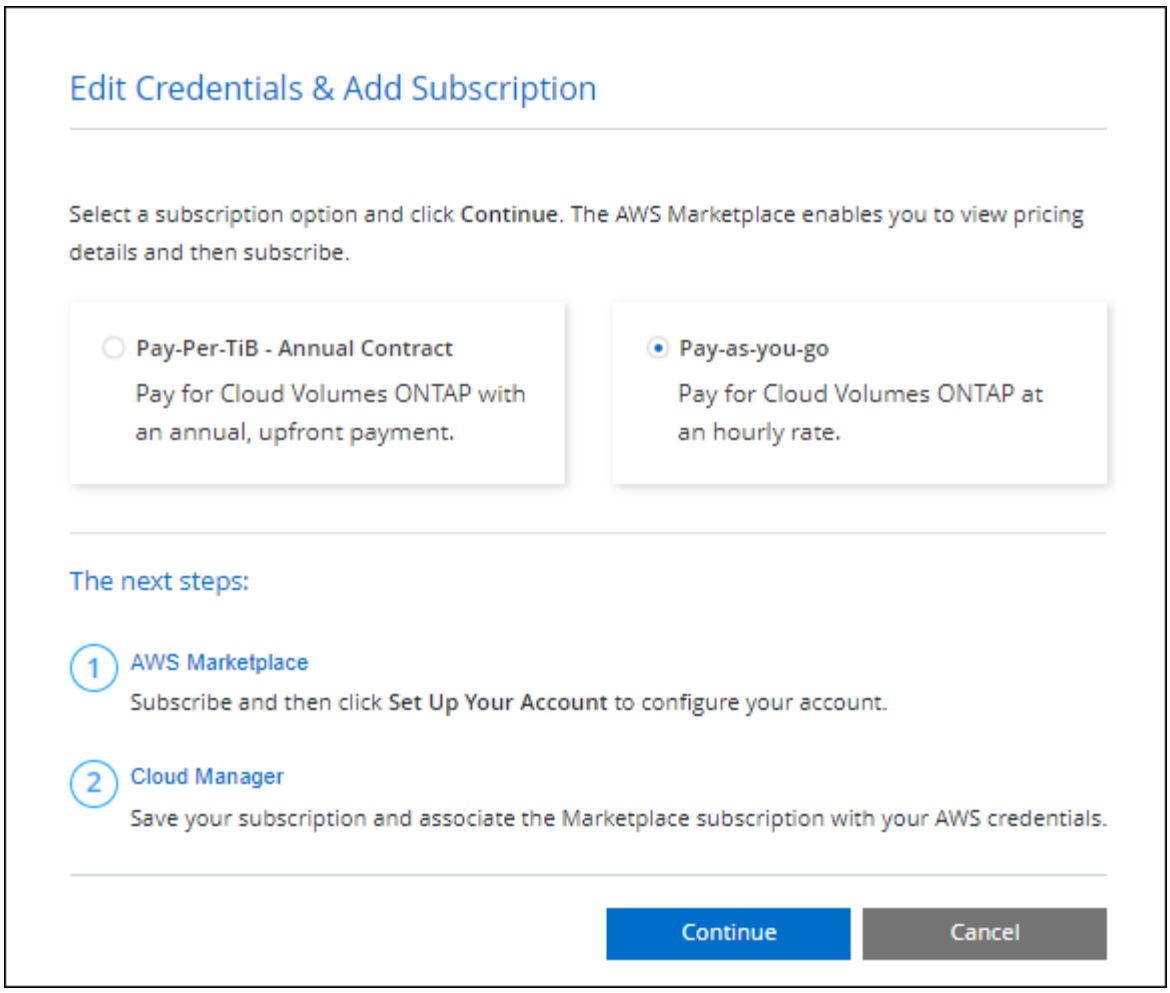
Abonnement PAYGO

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

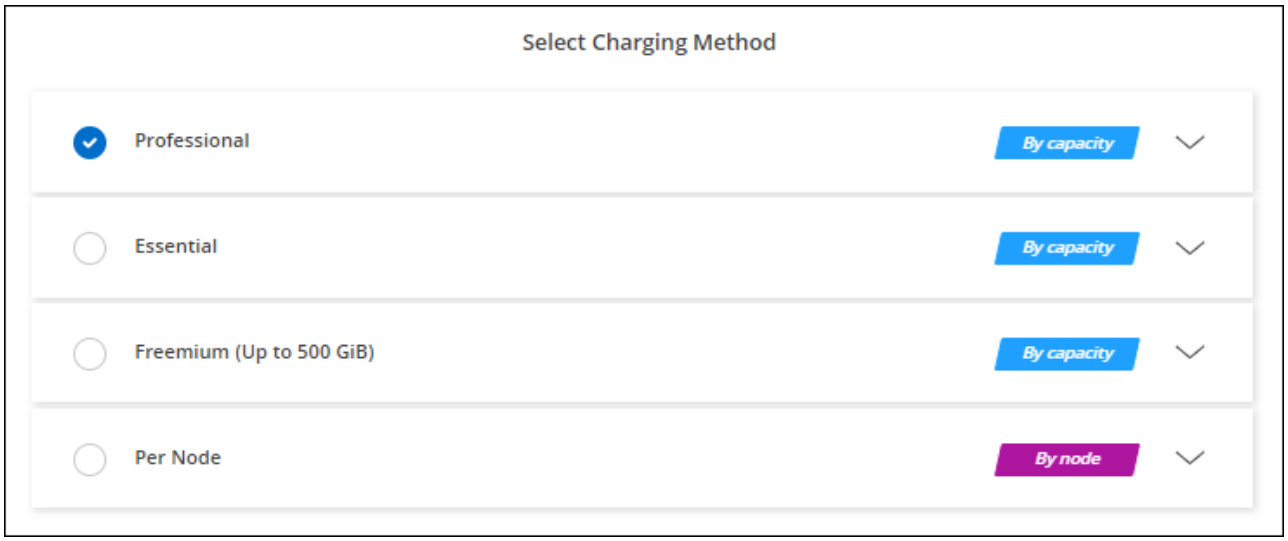
Lorsque vous créez un système Cloud Volumes ONTAP , la console vous invite à vous abonner à l'accord disponible sur AWS Marketplace. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes Cloud Volumes ONTAP supplémentaires.

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



b. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"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"

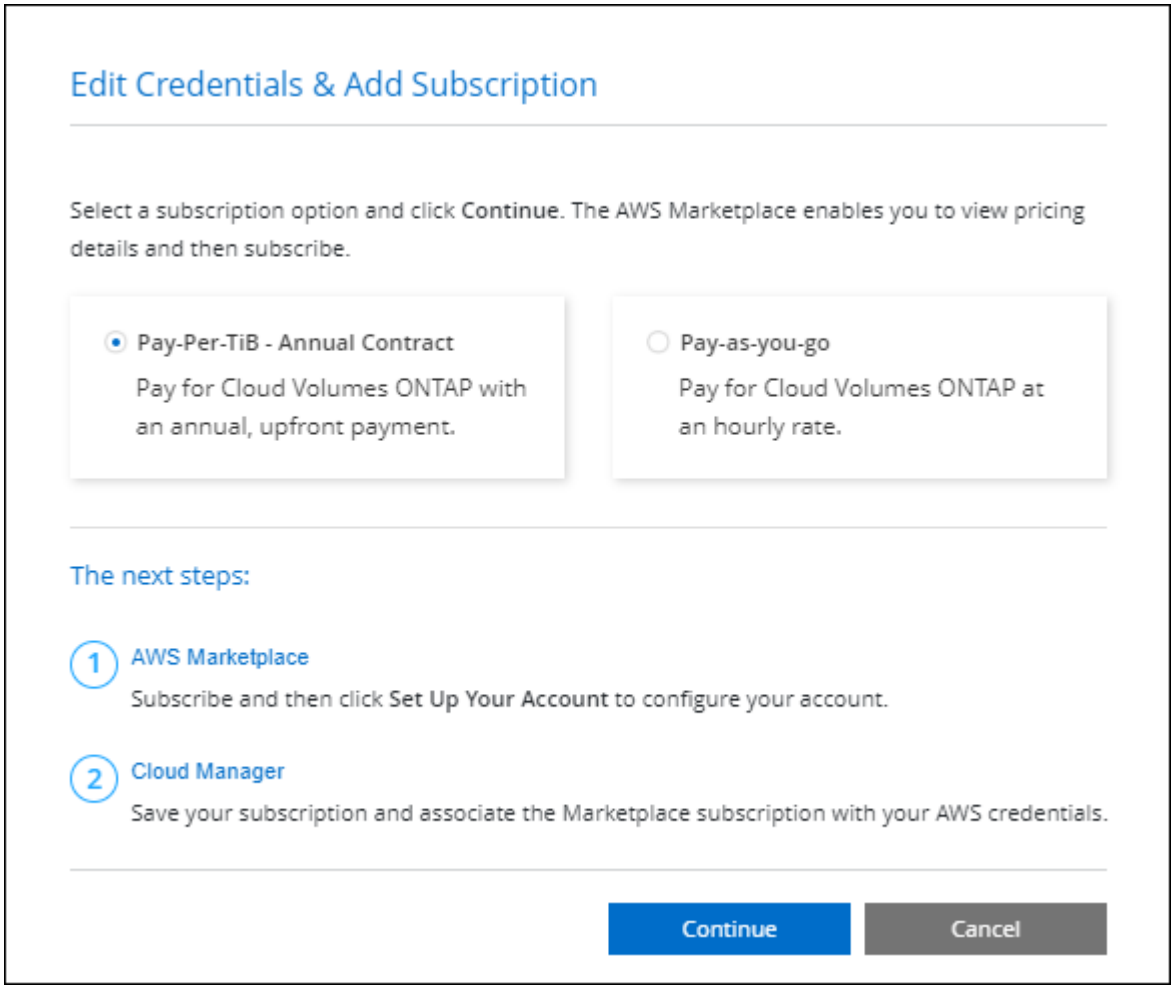
Contrat annuel

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

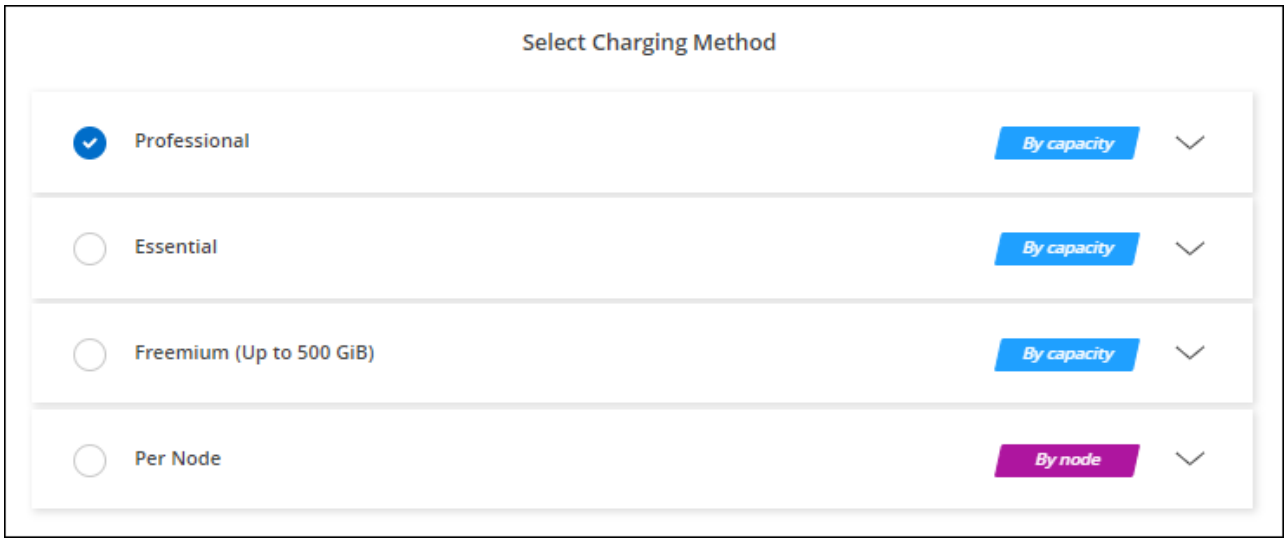
Semblable à un abonnement horaire, la console vous invite à souscrire au contrat annuel disponible sur AWS Marketplace.

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.



   b. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans AWS" .

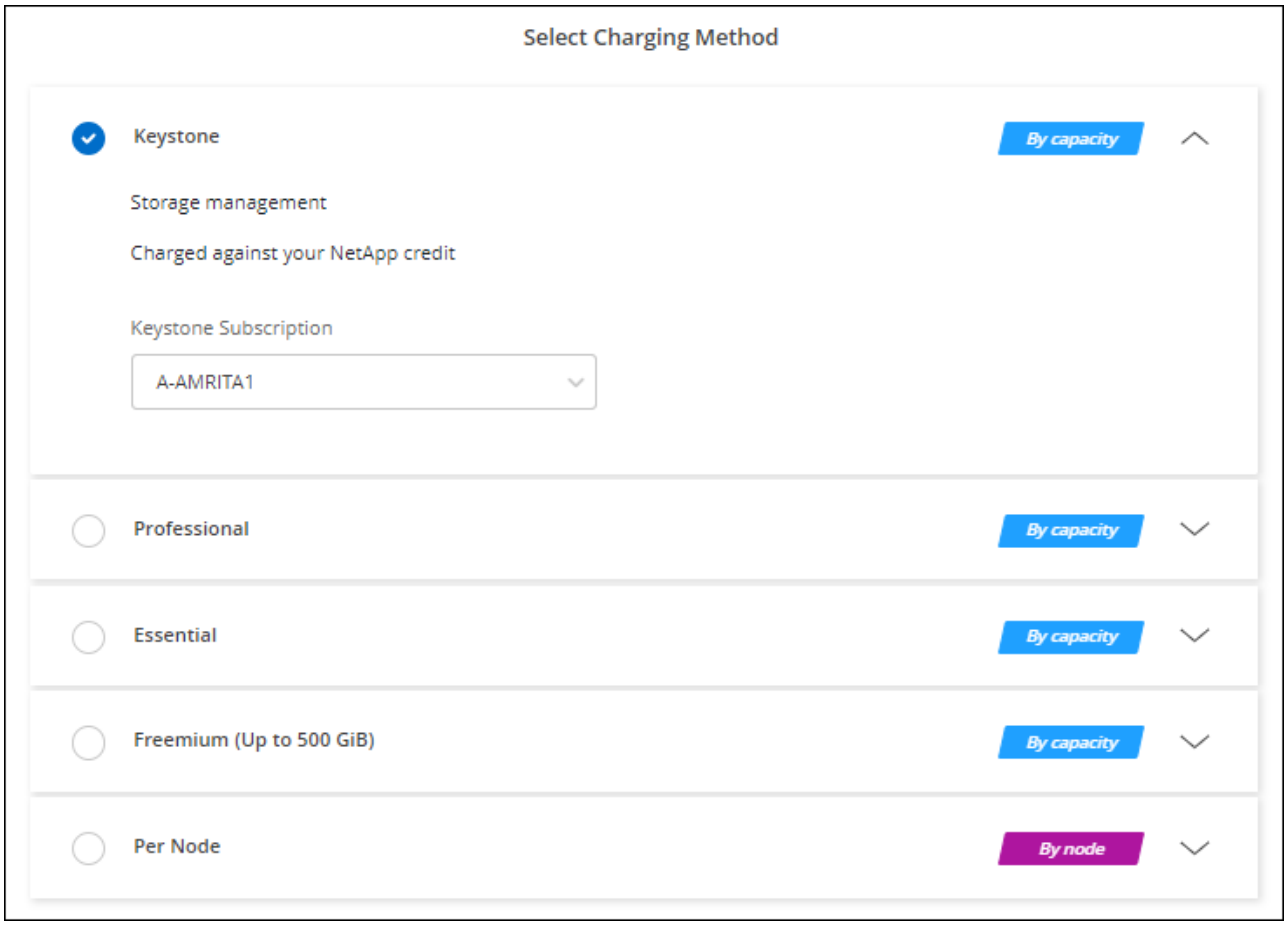
Abonnement Keystone

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 **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.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans AWS" .

Licence basée sur les nœuds

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. Pour plus d'informations, consultez :

- "Fin de disponibilité des licences basées sur des nœuds"
- "Fin de disponibilité des licences basées sur des nœuds"
- "Convertir une licence basée sur les nœuds en une licence basée sur la capacité"

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 NetApp Console.

- 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" .
- 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.

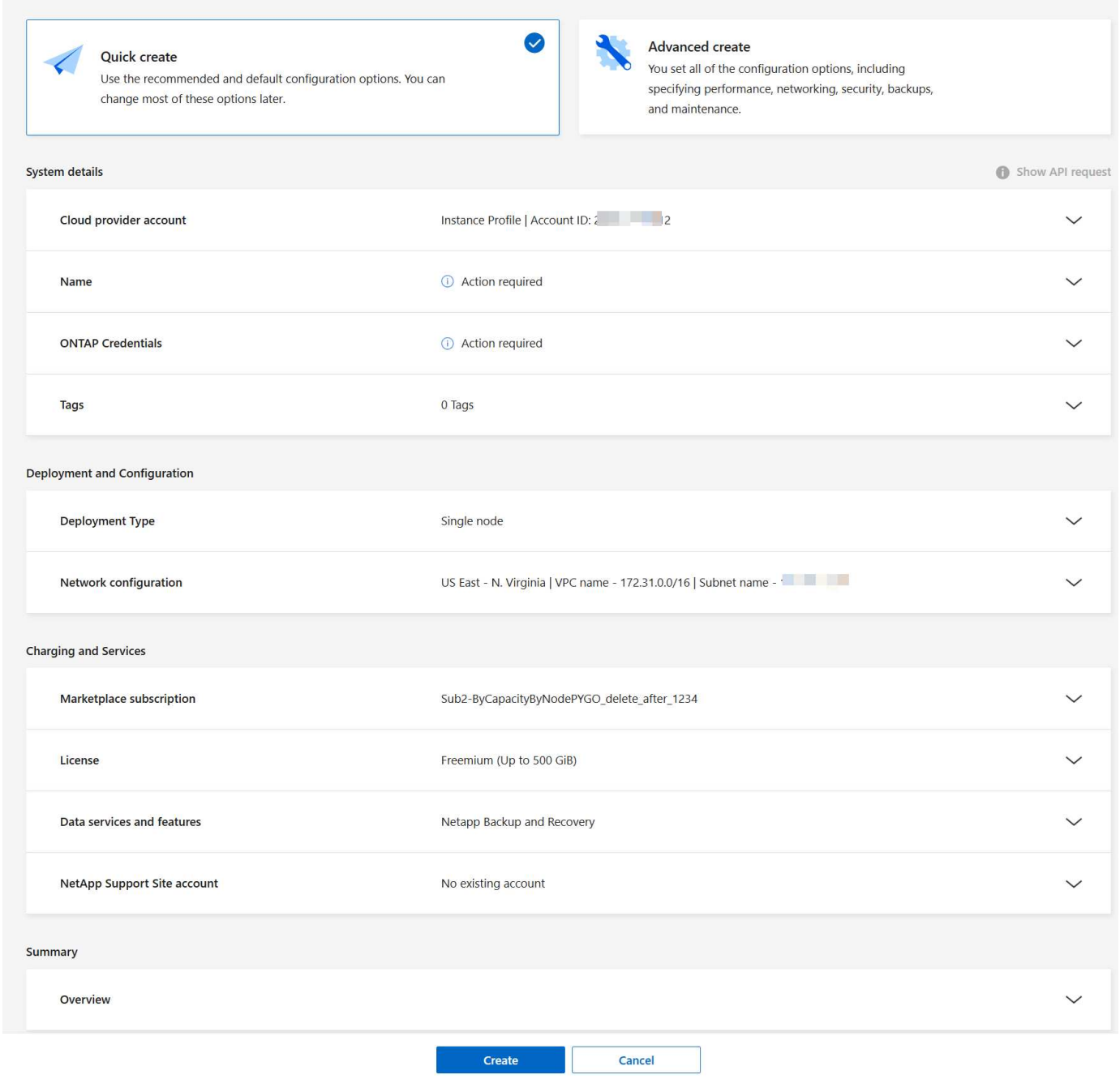
  Pour plus de détails, reportez-vous à"Exigences réseau pour Cloud Volumes ONTAP dans AWS" .

À propos de cette tâche

Immédiatement après avoir créé le système Cloud Volumes ONTAP , la NetApp Console 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.



détails du système

1. **Compte fournisseur cloud** : les détails du compte sont automatiquement renseignés en fonction de l'agent de console 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**.

Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail cloud AWS, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

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 NetApp Console.

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

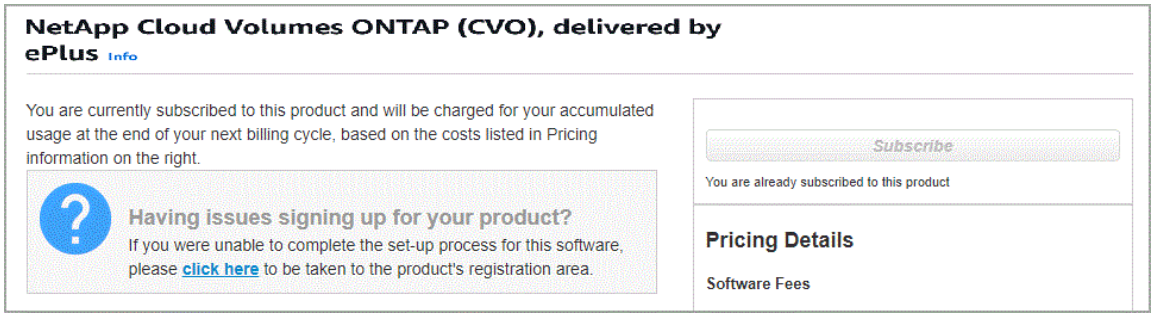
1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. Sélectionnez **Amazon Web Services** et * Cloud Volumes ONTAP Single Node*.
4. Sélectionnez **Création avancée**. Étant donné que 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 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 "Documentation AWS : Balisage de vos ressources Amazon EC2" .

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 *admin* ou remplacez-le par un nom d'utilisateur personnalisé.
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 **Ajouter un abonnement** 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. "Découvrez comment ajouter des informations d'identification AWS supplémentaires à la NetApp Console" .

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.



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 NetApp Data Classification"
   - "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.
Groupe de sécurité généré	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **VPC sélectionné uniquement**, 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. • Si vous choisissez **Tous les VPC**, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser le groupe de sécurité existant	Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" .

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.

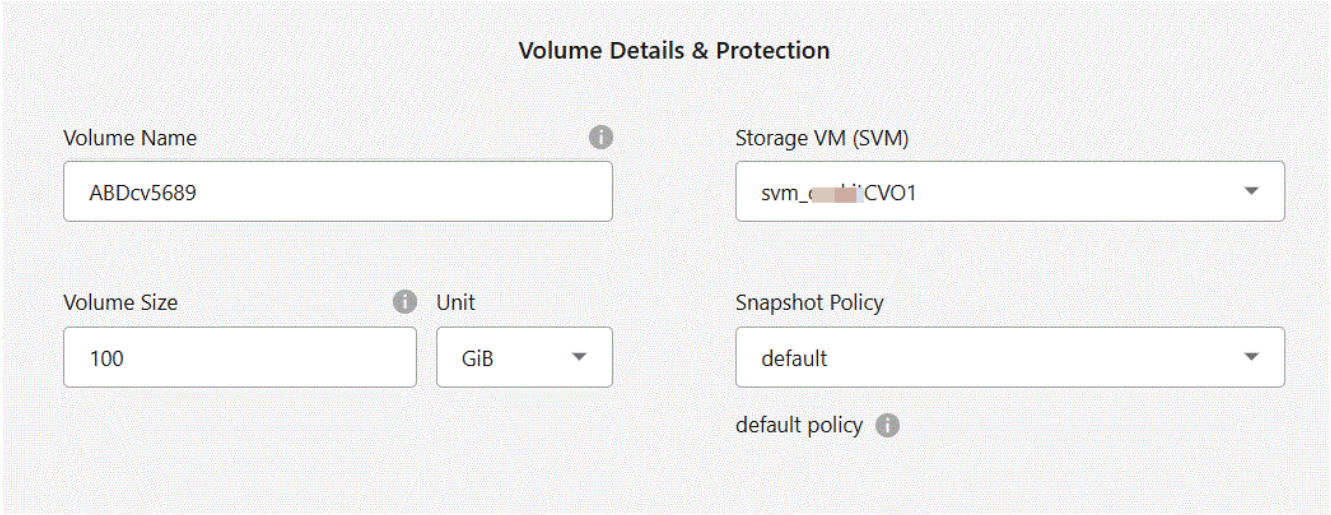
17. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    "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,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



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 **OU=Computers,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 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. Se référer à la "Documentation sur l'automatisation de la NetApp Console" 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** : Révisez 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" .

Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail cloud AWS, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

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 »" .

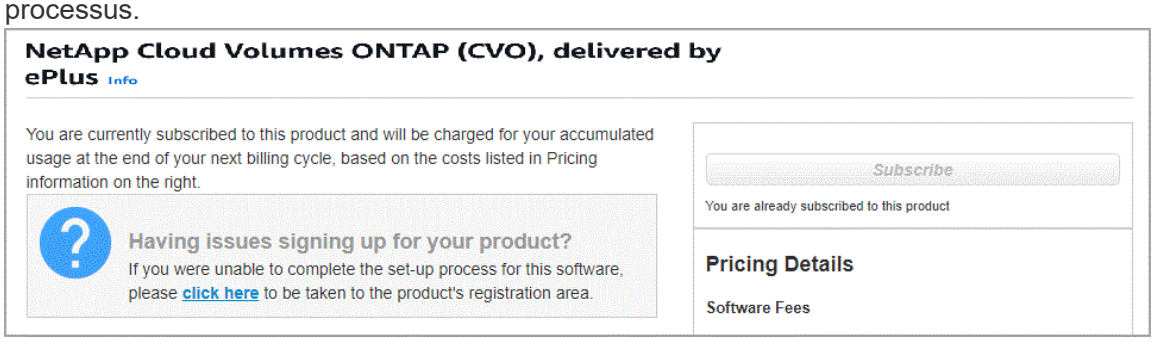
   Si vous exécutez l'agent de console 3.9.36 ou une version antérieure, vous devez ajouter le `DescribeAvailabilityZones` autorisation au rôle AWS dans la console AWS EC2.

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 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 "Documentation AWS : Balisage de vos ressources Amazon EC2" .
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 *admin* 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 **Ajouter un abonnement** 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 "Disponibilité restreinte des licences BYOL pour Cloud Volumes ONTAP" . "Découvrez comment ajouter des informations d'identification AWS supplémentaires à la console" .

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.



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 NetApp Data Classification"
   - "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	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **VPC sélectionné uniquement**, 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. • Si vous choisissez **Tous les VPC**, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser le groupe de sécurité existant	Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" .

8. **Connectivité et authentification SSH** : Choisissez 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.

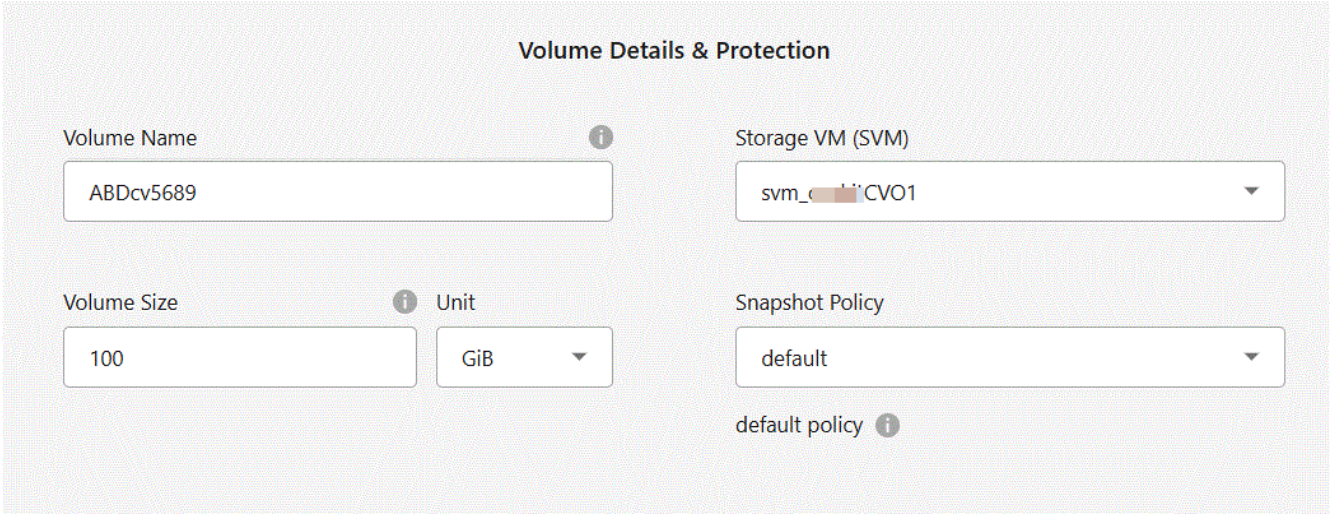
19. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    "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,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



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 **OU=Computers,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 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. Se référer à la "Documentation sur l'automatisation de la NetApp Console" 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** : Révisez 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.

> Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail cloud AWS, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

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 NetApp Console 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 vers le service Amazon Simple Storage Service (Amazon 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 https://ipaddress où ipaddress 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 * Licenses and subscriptions*.
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'associiez à un nouveau système Cloud Volumes ONTAP . Vous pouvez voir la licence dans le menu de navigation de gauche sous * Licenses and subscriptions > 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` touche 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 NetApp Console 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	**NetApp Console**
Intégration	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
Types de machines virtuelles (VM) pris en charge	Types d'instances Eds_v5 et Ls_v3	Gamme complète de types de machines virtuelles.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Configurations prises en charge dans Azure"^]
Licence	Licence gratuite	Toute licence basée sur la capacité."Licences Cloud Volumes ONTAP"
* Prise en charge de NetApp *	Non inclus	Disponible, en fonction du type de licence
Capacité	Jusqu'à 500 Gio	Extensible par configuration
Modèle de déploiement	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
Type de disque pris en charge	Disques gérés SSD Premium v2	Un soutien plus large."Configuration par défaut pour Cloud Volumes ONTAP"
Vitesse d'écriture (mode d'écriture rapide)	Non pris en charge	Pris en charge, en fonction de votre configuration. "En savoir plus sur les vitesses d'écriture dans Cloud Volumes ONTAP" .
Capacités d'orchestration	Non disponible	Disponible via la NetApp Console, en fonction du type de licence
Nombre de machines virtuelles de stockage prises en charge	Un par déploiement	Plusieurs machines virtuelles de stockage, en fonction de votre configuration."Nombre de machines virtuelles de stockage prises en charge"
Modification du type d'instance	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 NetApp Console"

Démarrer dans la NetApp Console

Démarrage rapide de Cloud Volumes ONTAP dans Azure

Démarrez avec Cloud Volumes ONTAP pour Azure en quelques étapes.

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 NetApp Console qui s'exécute sur cet agent de console. "Découvrez comment installer manuellement l'agent de console dans un emplacement sans accès Internet"

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" .

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" .

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 Azure Managed Disks :

- 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 NetApp Console 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 la mise en réseau Azure pour Cloud Volumes ONTAP

La NetApp Console 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
\ https://netapp-cloud-account.auth0.com	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : • Services Cloud Volumes ONTAP • Services ONTAP • Protocoles et services proxy
https://vault.azure.net	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.
\ https://api.bluexp.netapp.com/tenancy	Location	Utilisé pour récupérer les ressources 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 en cas d'indisponibilité
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilisé pour envoyer des données de télémétrie AutoSupport au support NetApp .	Modes standard et restreint.	Les informations AutoSupport ne sont toujours pas livrées.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	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.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	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.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	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.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	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
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	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 NetApp Console

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 d'interfaces logiques (LIF) allouées à Cloud Volumes ONTAP dépend du type de système déployé : mono-nœud ou paire haute disponibilité. Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est requise 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 NetApp Console alloue 5 ou 6 adresses IP à un système à nœud unique :

- 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 NetApp Console crée une interface logique de gestion SVM sur les paires haute disponibilité, 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 en 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 à haute disponibilité (HA) comportent moins de règles entrantes que les systèmes à nœud unique, car le trafic de données entrant transite par l'équilibreur de charge standard Azure. Pour cette raison, le trafic provenant de l'équilibreur de charge doit être autorisé, 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. "Documentation ONTAP" .
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 NetApp Console, 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.

Configuration de Cloud Volumes ONTAP	Disques système utilisés pour le chiffrement des clés	Disques de données utilisés pour le cryptage des clés
Nœud unique	• Botte • Cœur • NVRAM	• Racine • Données

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	• Botte • Cœur • NVRAM	Aucune
Zone de disponibilité unique Azure HA avec disques gérés partagés	• Botte • Cœur • NVRAM	• Racine • Données
Zones de disponibilité multiples Azure HA avec disques gérés partagés	• Botte • Cœur • NVRAM	• Racine • Données

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 tucréé 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 for volume encryption** (pour les systèmes à nœud unique, les paires haute disponibilité dans plusieurs zones et les déploiements haute disponibilité dans une seule zone de disponibilité)

       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 seul nœud : `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 nœud unique : `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

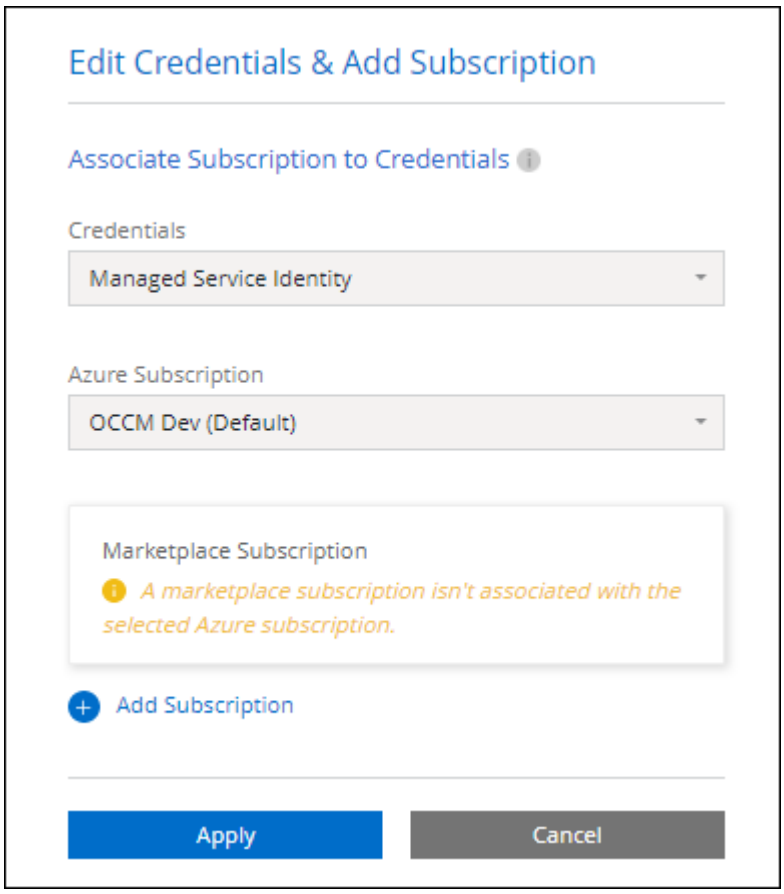
Sélectionnez l'offre Freemium pour utiliser Cloud Volumes ONTAP gratuitement avec jusqu'à 500 Gio de capacité provisionnée. "En savoir plus sur l'offre Freemium" .

Étapes

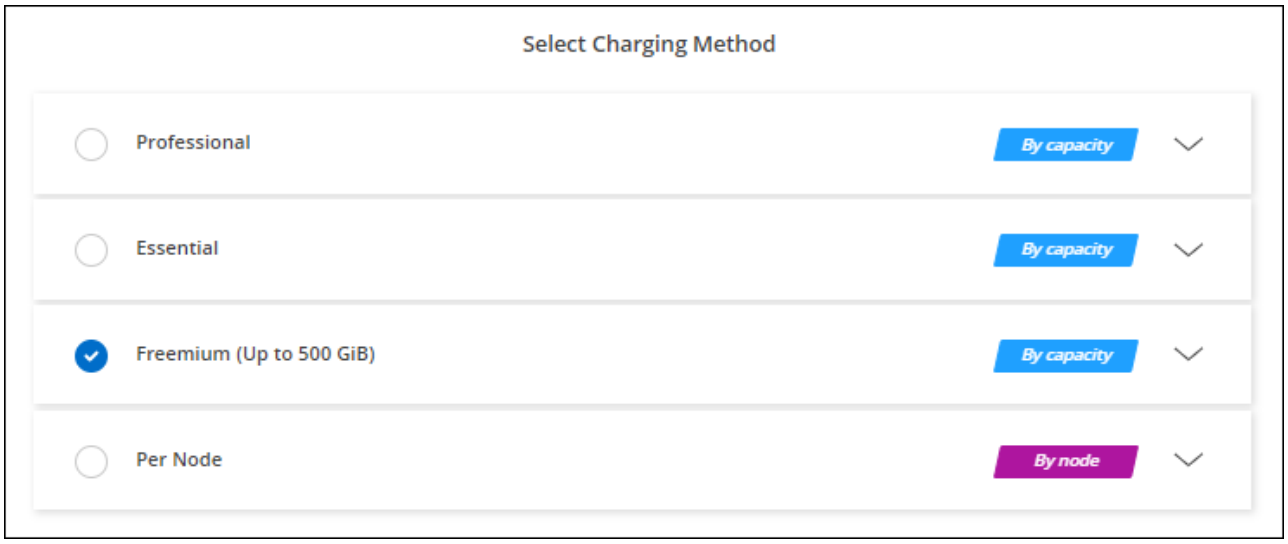
1. Dans le menu de navigation de gauche de la NetApp Console, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

   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" .



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



"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 formules Essentiel et Professionnel sont disponibles avec les modèles de consommation ou options d'achat 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"

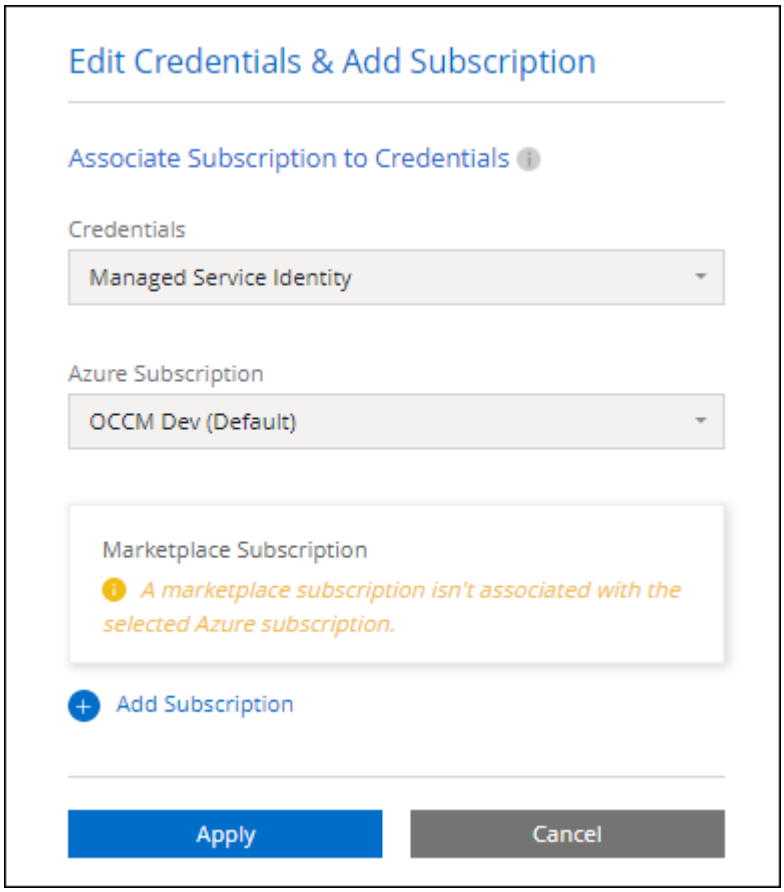
   La console interroge automatiquement le service de licences de NetApp pour obtenir des détails sur les licences associées à votre compte de site de support NetApp . S'il n'y a pas d'erreur, la console ajoute automatiquement les licences à la console.

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" .

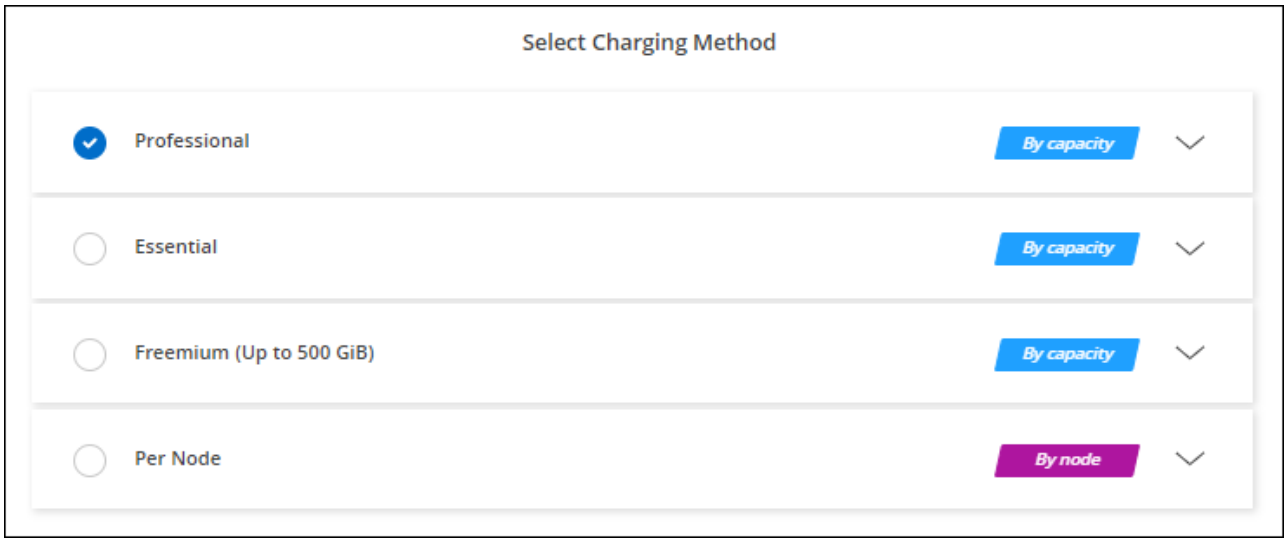
3. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

   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.



   a. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

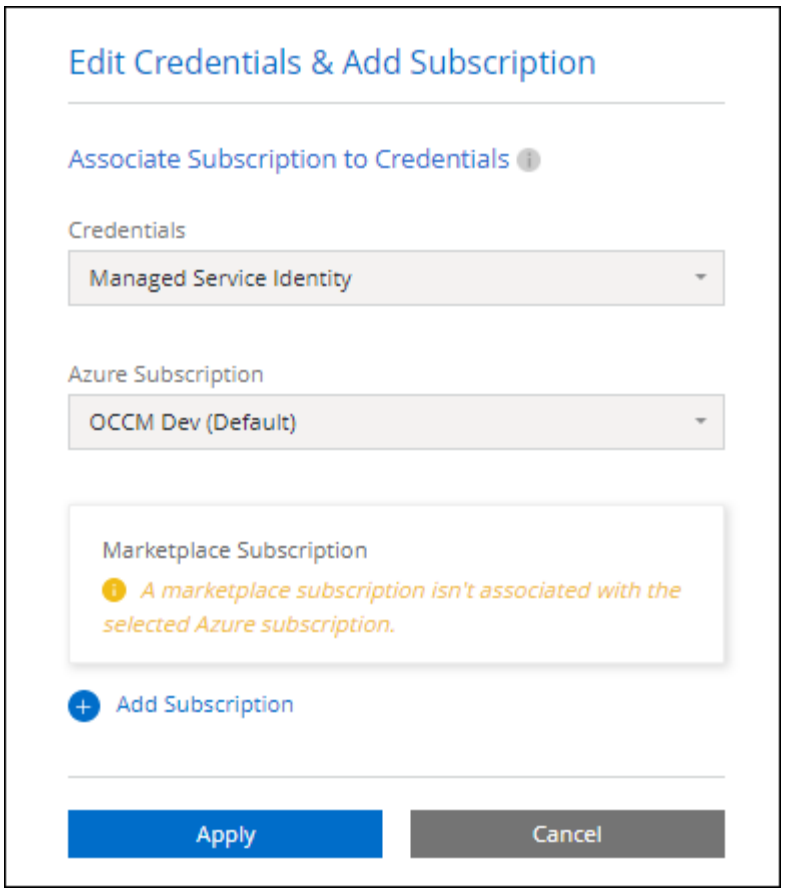
Abonnement PAYGO

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

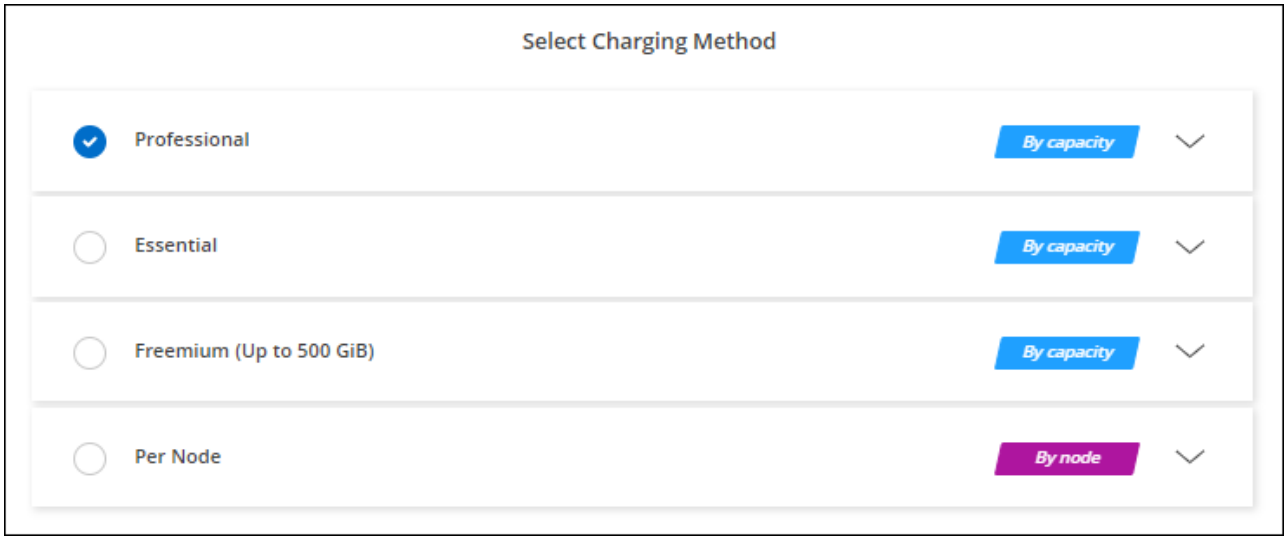
Lorsque vous créez un système Cloud Volumes ONTAP , la console vous invite à vous abonner au contrat disponible sur la Place de marché Azure. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes supplémentaires.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **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.



b. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"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.

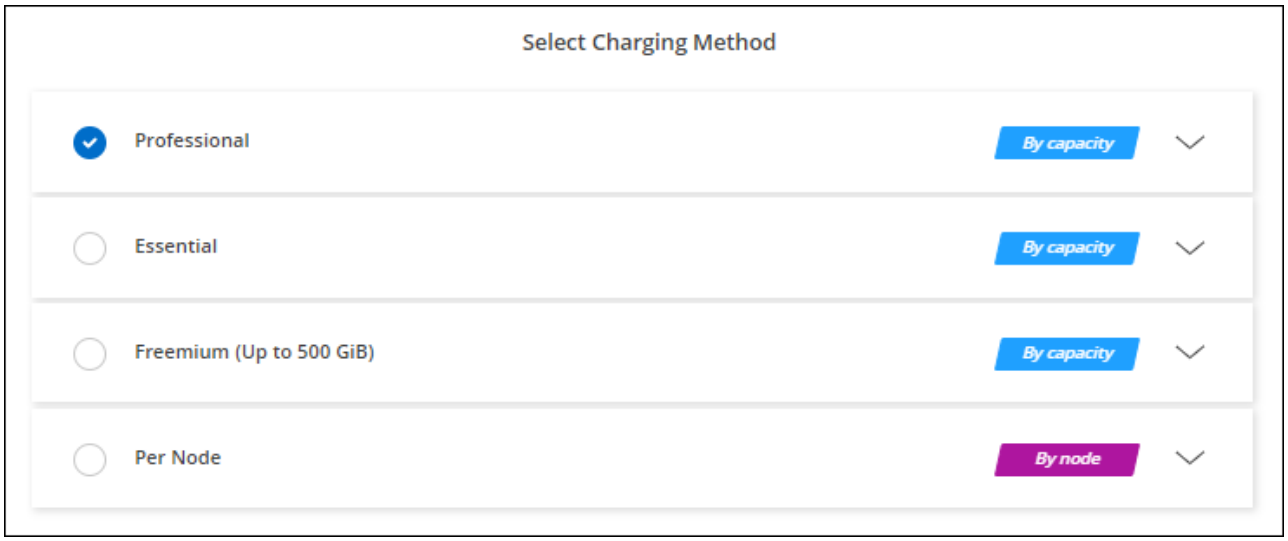
Étapes

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.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

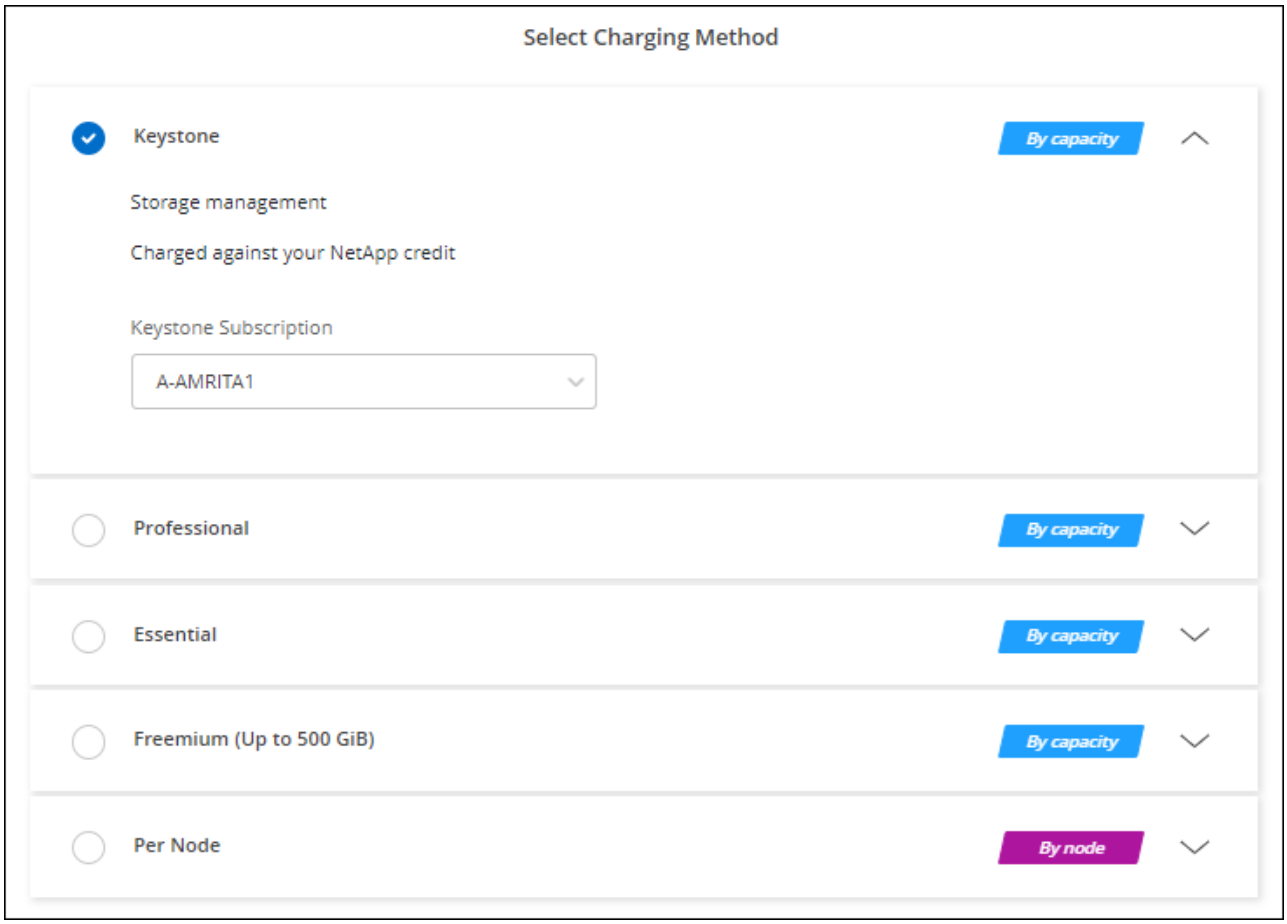
Abonnement Keystone

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.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

Licence basée sur les nœuds

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. Pour plus d'informations, consultez :

- "Fin de disponibilité des licences basées sur des nœuds"
- "Fin de disponibilité des licences basées sur des nœuds"
- "Convertir une licence basée sur les nœuds en une licence basée sur la capacité"

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 NetApp Console 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/VMOrchestratorZonalMultiFD", "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 haute disponibilité dans Azure en créant un système Cloud Volumes ONTAP dans NetApp Console.

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** : Modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, puis spécifiez les informations d'identification.

Le tableau suivant décrit les 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 étiquettes, veuillez consulter le "Documentation Microsoft Azure : Utilisation de balises pour organiser vos ressources Azure" .
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 *admin* 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. "Apprenez à ajouter des informations d'identification" .

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 NetApp Data Classification"
   - "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 ultérieurs de Cloud Volumes ONTAP comme"pris en charge dans Azure" . 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	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. Si le compte Azure que vous utilisez possède le "autorisations requises" , la console supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec de déploiement ou de suppression.
Groupe de sécurité généré	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **Réseau virtuel sélectionné uniquement**, 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. • Si vous choisissez **Tous les réseaux virtuels**, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP . "Afficher le groupe de sécurité par défaut" .

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. **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.

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, BlueXP met à jour le système vers cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.16.1 P3 et 9.16.1 P4 est disponible. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.15 à la version 9.16.

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.

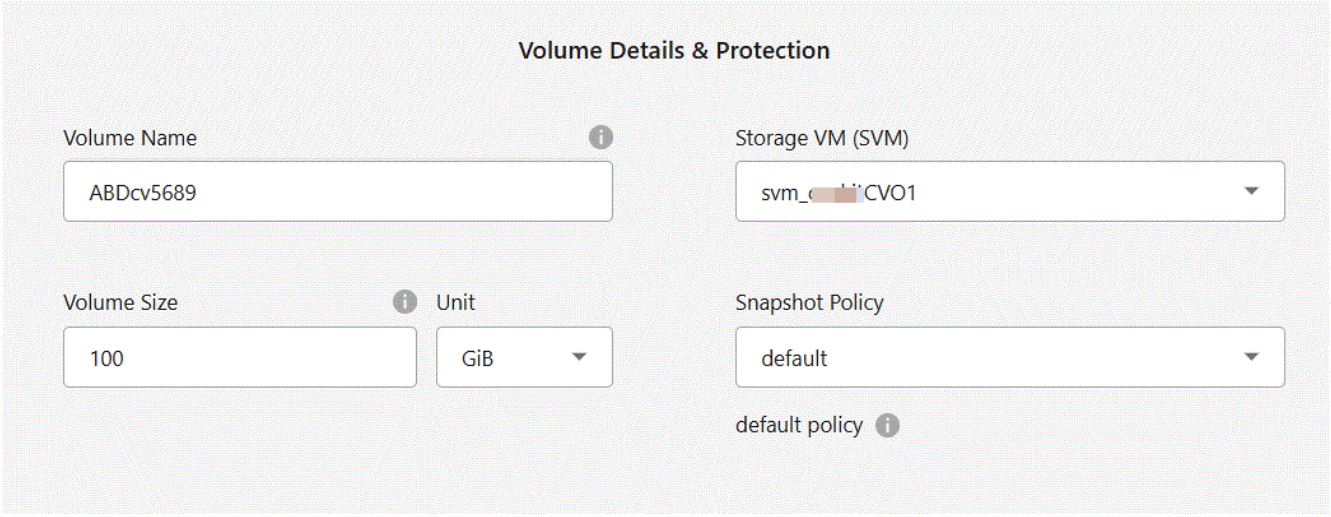
15. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    "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,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



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 **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"^]
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. Se référer à la "Documentation sur l'automatisation de la NetApp Console" 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** : Révisez 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" .

Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Azure, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

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** : Modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, puis spécifiez les informations d'identification.

   Le tableau suivant décrit les 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 étiquettes, veuillez consulter le "Documentation Microsoft Azure : Utilisation de balises pour organiser vos ressources Azure" .
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 *admin* 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. "Apprenez à ajouter des informations d'identification" .

5. **Services** : activez ou désactivez les services individuels selon que vous souhaitez les utiliser avec Cloud Volumes ONTAP.
   - "En savoir plus sur la NetApp Data Classification"
   - "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	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. 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. Si le compte Azure que vous utilisez possède le "autorisations requises" , la console supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec de déploiement ou de suppression.
Groupe de sécurité généré	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **Réseau virtuel sélectionné uniquement**, 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. • Si vous choisissez **Tous les réseaux virtuels**, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP . "Afficher le groupe de sécurité par défaut" .

8. * Méthodes de 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**.

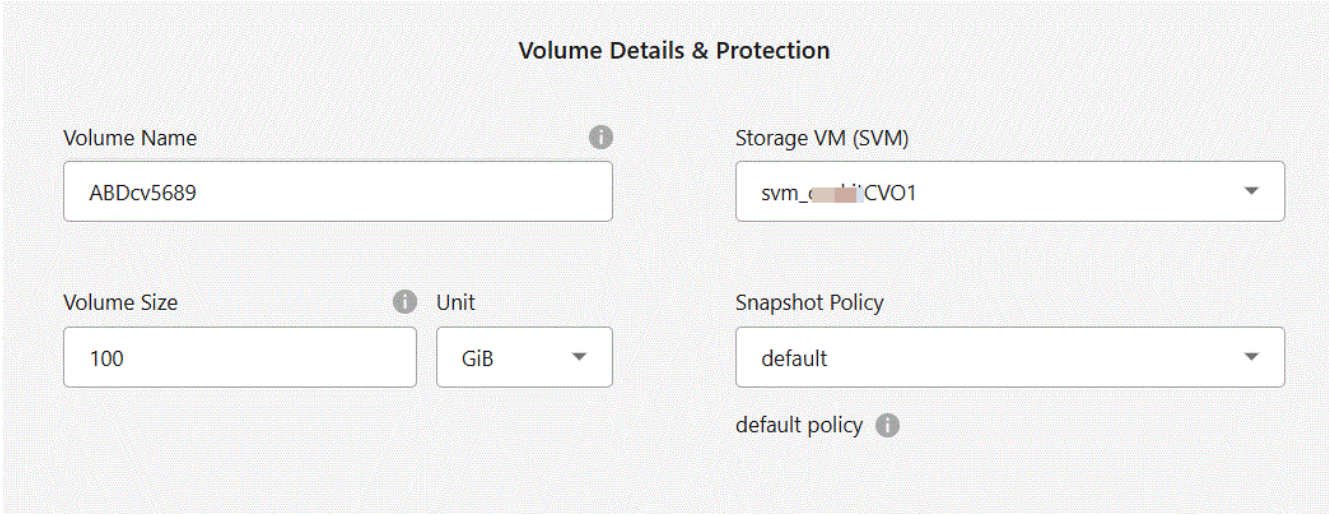
    "En savoir plus sur les protocoles et versions clients pris en charge" .

    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,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



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 **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"^]
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. Se référer à la "Documentation sur l'automatisation de la NetApp Console" 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** : Révisez 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.

Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Azure, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

Liens connexes

*"Planification de votre configuration Cloud Volumes ONTAP dans Azure" *"Déployer Cloud Volumes ONTAP dans Azure depuis la Place de marché Azure"

Vérifier l'image de la plateforme Azure

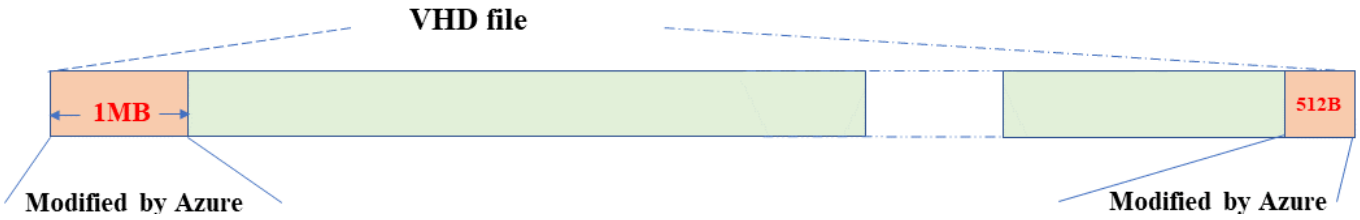
Vérification d'image de la place de marché Azure pour Cloud Volumes ONTAP

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"

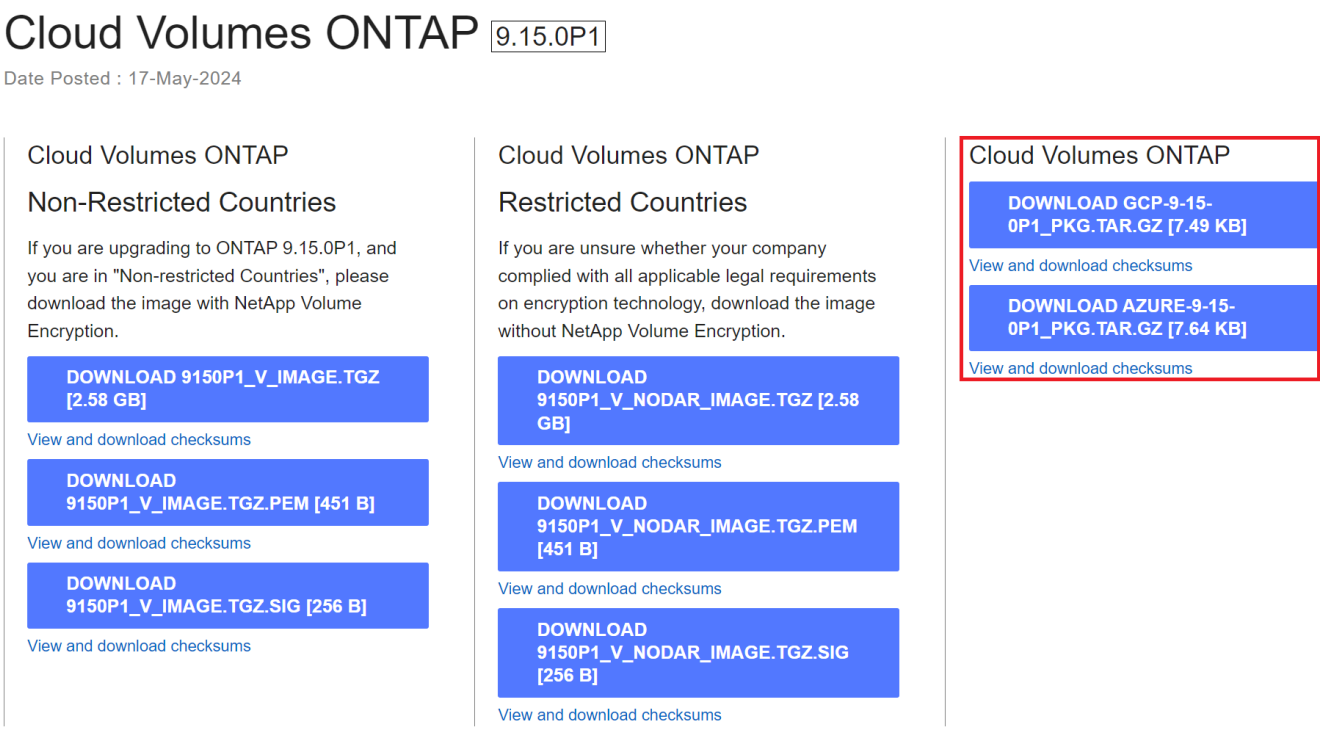
Téléchargez le fichier image Azure pour Cloud Volumes ONTAP

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*.



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 NetApp Console	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 = "fnf1"
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
```

3. 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 > *examplesaname* > Clé d'accès > *key1* > *key* > Afficher > <*copie*>**

```
PS /home/user1> $storageAccountName = “examplesaname”
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
```

4. 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://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 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.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/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="xxxxxxxxxx"
% 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": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "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-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.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.bluexpinfraprod.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
```

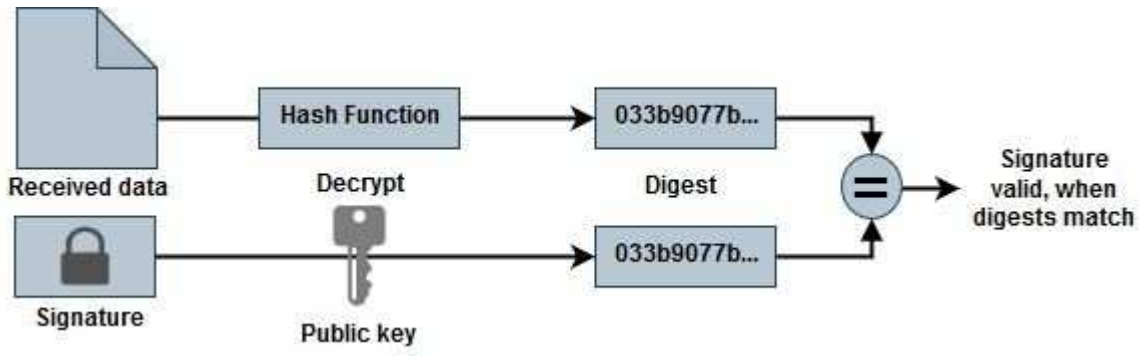
Vérifier la signature du fichier

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 NetApp Console 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 NetApp Console.

- 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)", chiffrement 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 la mise en 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" .

> Pendant la découverte, vous pouvez voir des messages d'échec, mais vous pouvez les ignorer jusqu'à ce que le processus de découverte soit terminé. Ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail de la place de marché Azure pendant la découverte, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu du système.

Après avoir terminé

Une fois la découverte terminée, vous pouvez afficher les systèmes répertoriés sur la page **Systèmes** 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" Pourtant, vous devez 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 NetApp Console 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 *Compute Network User* 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 "NetApp Backup and Recovery" 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"
- "Autorisations Google Cloud pour l'agent de la console"

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 Google Cloud"

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 Google Cloud"

Dimensionnez votre système dans Google Cloud

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" Consultez ensuite les informations détaillées de Google concernant 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"

Types de disques

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

Vous devez choisir une taille de disque initiale lorsque vous déployez un système Cloud Volumes ONTAP . Après cela, vous pouvez laisser la NetApp Console 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 : Présentation des quotas cloud"

  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 Google Cloud, vous devez spécifier les détails de votre réseau virtuel. Vous pouvez utiliser une feuille de calcul pour recueillir les informations auprès de votre administrateur.

Informations réseau pour un système à nœud unique

Informations Google Cloud	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 Google Cloud	Votre valeur
Région	
Zone pour le nœud 1	
Zone pour le nœud 2	

Informations Google Cloud	Votre valeur
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 Google Cloud	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 NetApp Console 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 réponde aux exigences suivantes.

Un VPC

Un cloud privé virtuel (VPC) est nécessaire pour un système à nœud unique.

Adresses IP privées

Pour un système à nœud unique dans Google Cloud, la NetApp Console attribue 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 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.

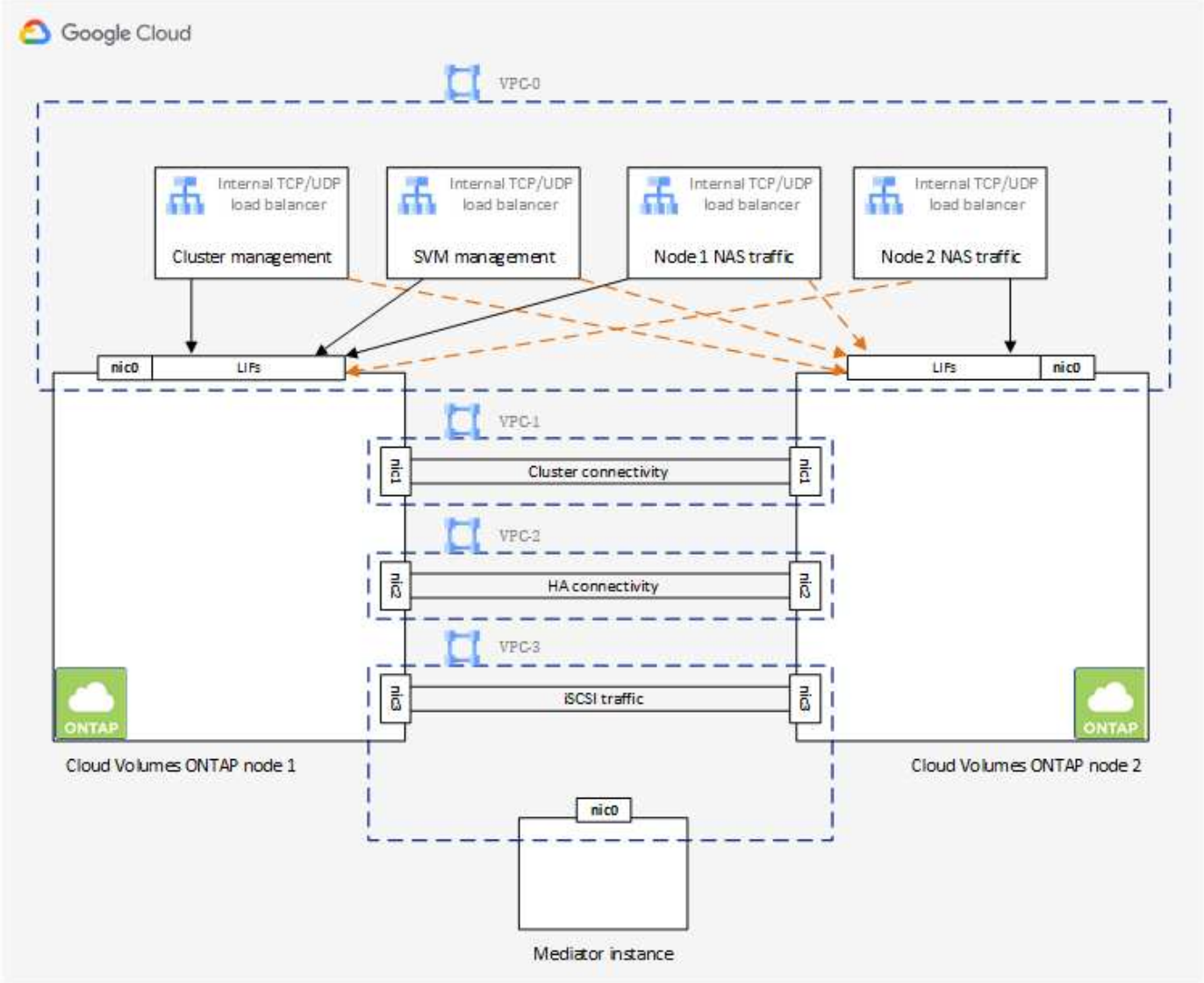
  Ce modèle de déploiement réduit vos coûts car il n'y a pas de frais de sortie de données entre les zones.

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 d'interfaces logiques (LIF) allouées à Cloud Volumes ONTAP dépend du type de système déployé : mono-nœud ou paire haute disponibilité. Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est requise pour les outils de gestion tels que SnapCenter.

- **Nœud unique** NetApp 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
\ https://netapp-cloud-account.auth0.com	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : • Services Cloud Volumes ONTAP • Services ONTAP • Protocoles et services proxy
\ https://api.bluexp.netapp.com/tenancy	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.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	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
https://cloudbuild.googleapis.com/v1 (pour les déploiements en mode privé uniquement) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	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 souhaiterez 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

Protocole	Port	But
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
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."Documentation ONTAP"
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	18600–18699	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 sontrépertorié 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, localisez 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 prévues pour votre périmètre de service.

Images

Cloud Volumes ONTAP et la Console utilisent tous deux des images provenant d'un projet au sein de Google Cloud qui est géré par NetApp. Cela peut affecter le déploiement de l'agent de la Console et de Cloud Volumes ONTAP, si votre organisation a 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 permettent de déroger aux règles de contrôle des services VPC. Pour plus d'informations sur les politiques, veuillez consulter la "Documentation relative à la politique de contrôle des services VPC de Google Cloud".

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 "NetApp Backup and Recovery" 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**.

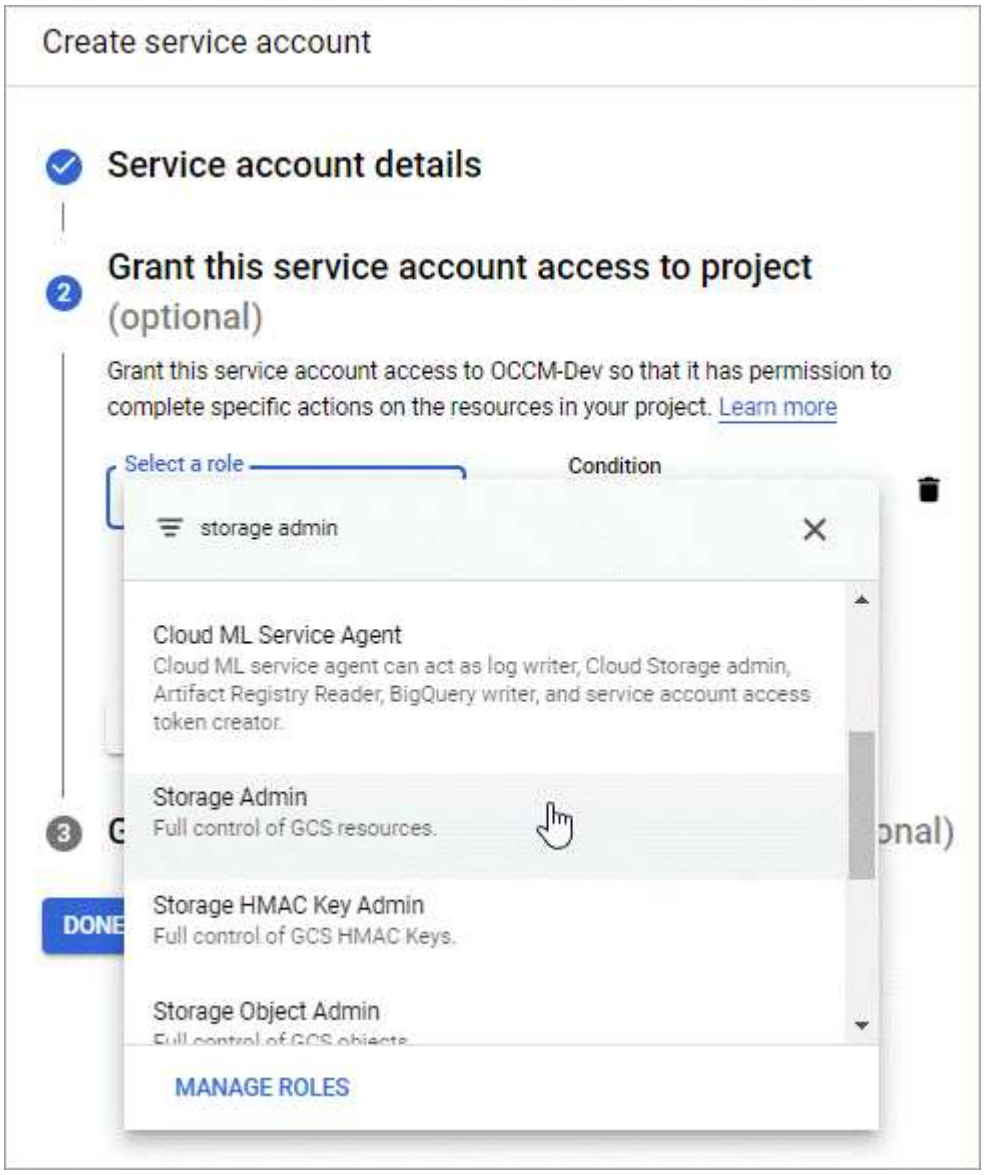
Étapes

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.

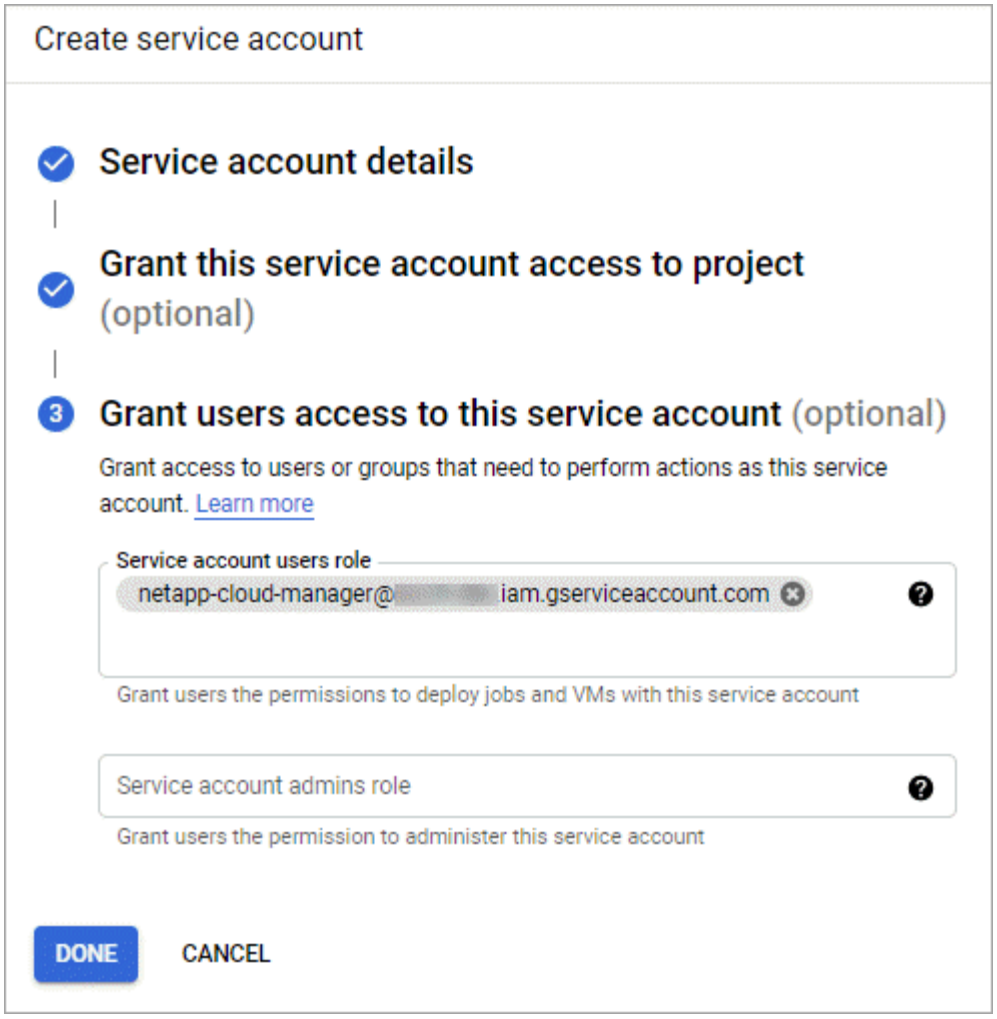
   a. **Détails du compte de service** : saisissez un nom et une description.

   b. **Accorder à ce compte de service l'accès au projet** : Sélectionnez le rôle **Administrateur de stockage**.



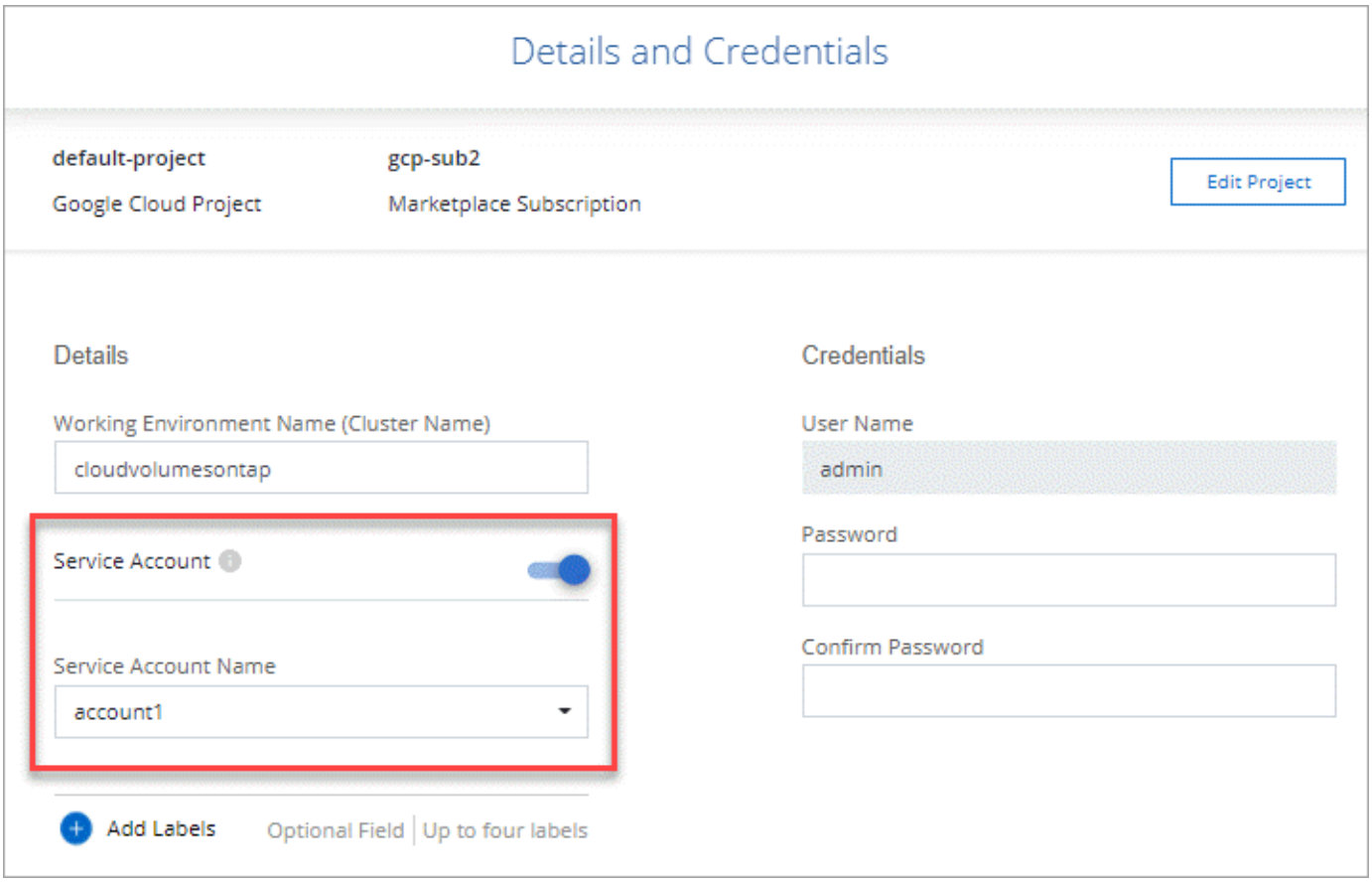
   c. **Accorder aux utilisateurs l'accès à ce compte de service** : ajoutez le compte de service de l'agent de console en tant qu'*utilisateur de compte de service* à ce nouveau compte de service.

      Cette étape est requise uniquement pour la hiérarchisation des données. Ce n'est pas nécessaire pour la sauvegarde et la récupération.



Quelle est la prochaine étape ?

Vous devrez sélectionner le compte de service ultérieurement lorsque vous créerez un système Cloud Volumes ONTAP .



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 s'appliquer si vous utilisez un autre projet pour le service de gestion des clés cloud.

   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 NetApp Console 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 NetApp Console" 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

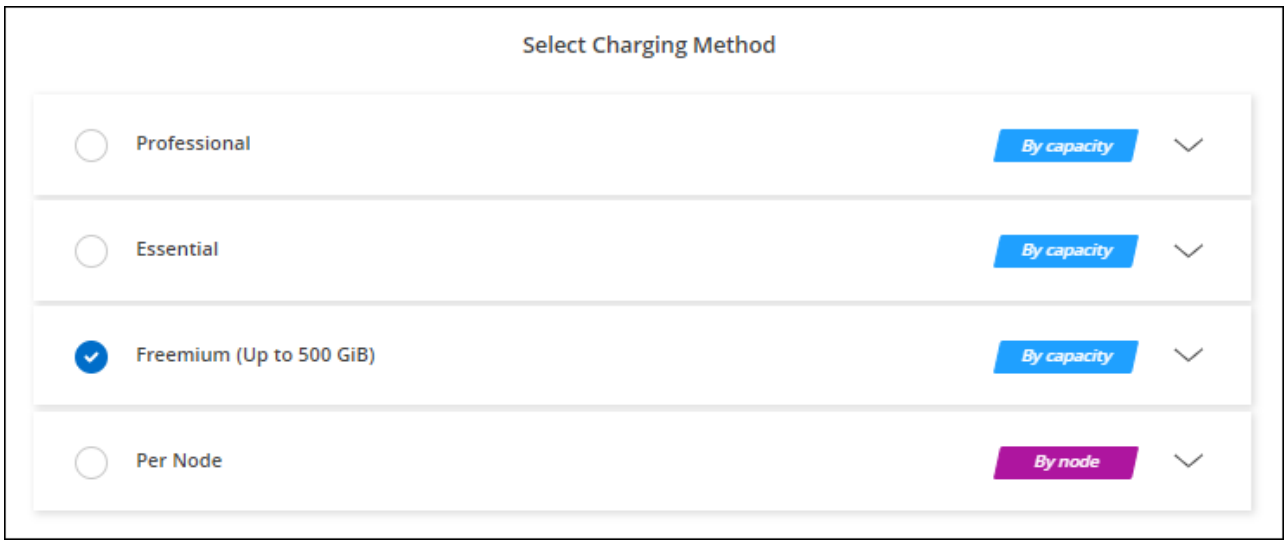
Sélectionnez l'offre Freemium pour utiliser Cloud Volumes ONTAP gratuitement avec jusqu'à 500 Gio de capacité provisionnée. "En savoir plus sur l'offre Freemium" .

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 NetApp Console.
   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.



"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 formules Essentiel et Professionnel sont disponibles avec les modèles de consommation ou options d'achat 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 NetApp Console"

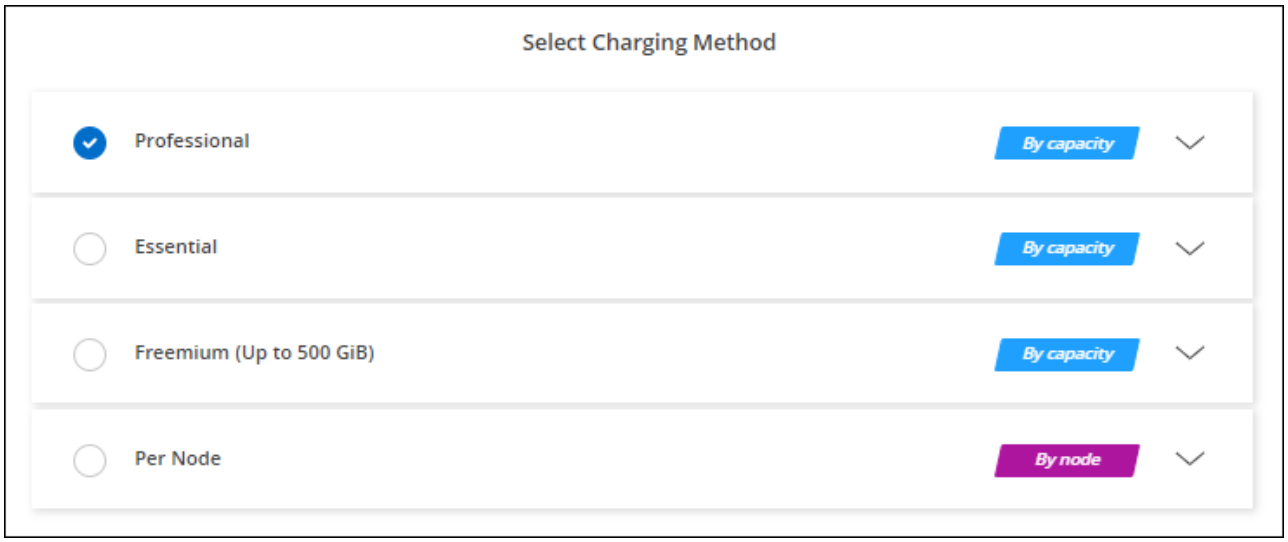
   La console interroge automatiquement le service de licences de NetApp pour obtenir des détails sur les licences associées à votre compte de site de support NetApp . S'il n'y a pas d'erreur, la console ajoute les licences.

   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 **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 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.



"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.

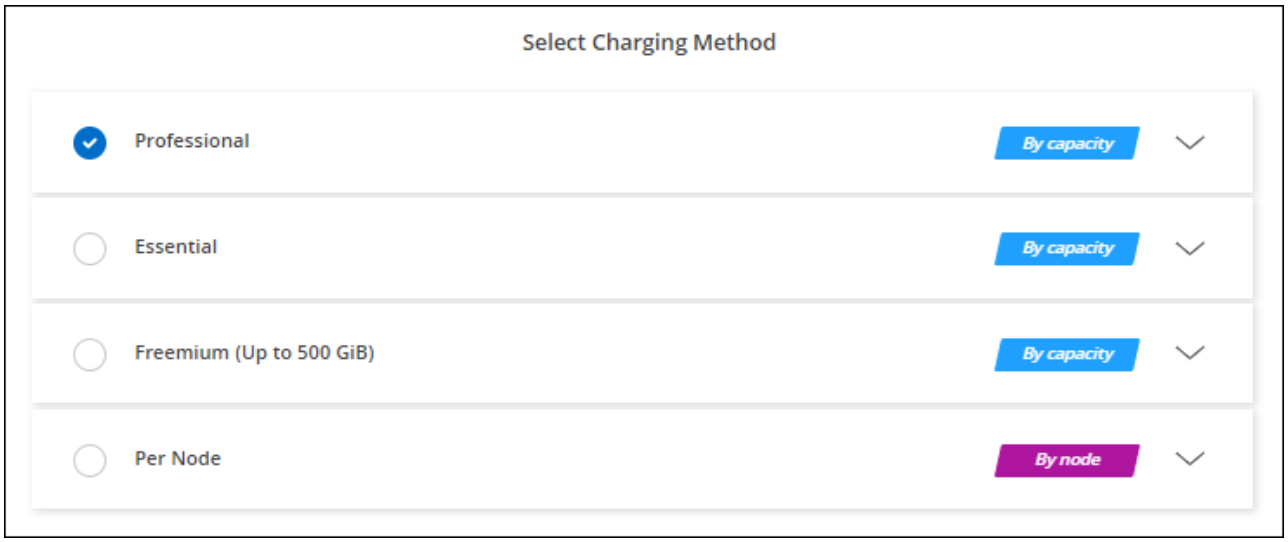
Lorsque vous créez un système Cloud Volumes ONTAP , la console vous invite à souscrire à l'accord disponible sur Google Cloud Marketplace. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes supplémentaires.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **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 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.



"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.

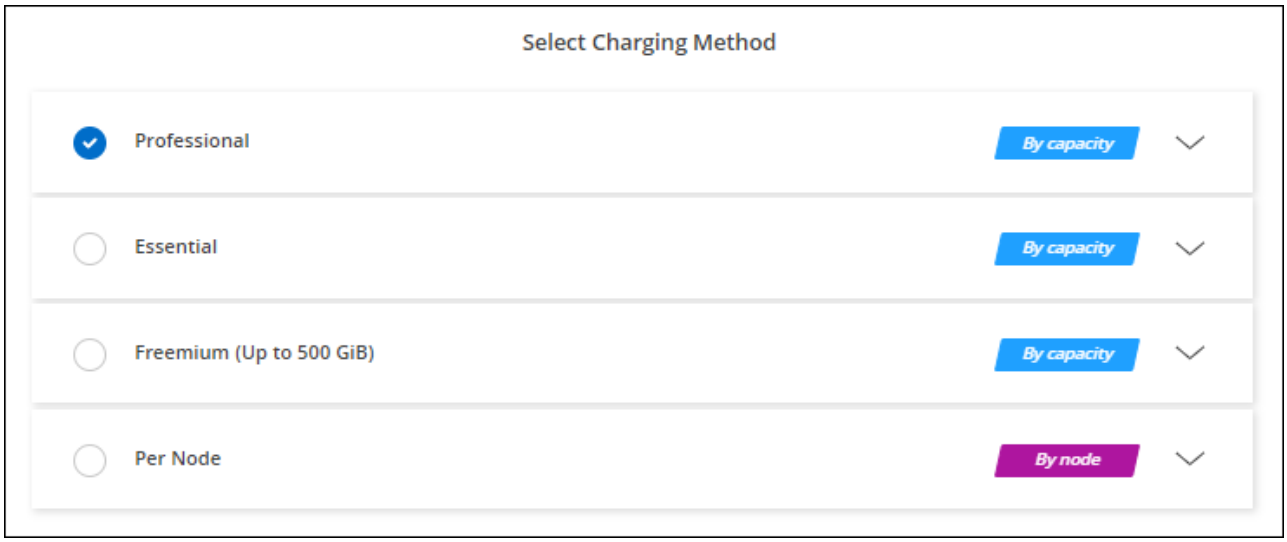
Étapes

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.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud" .

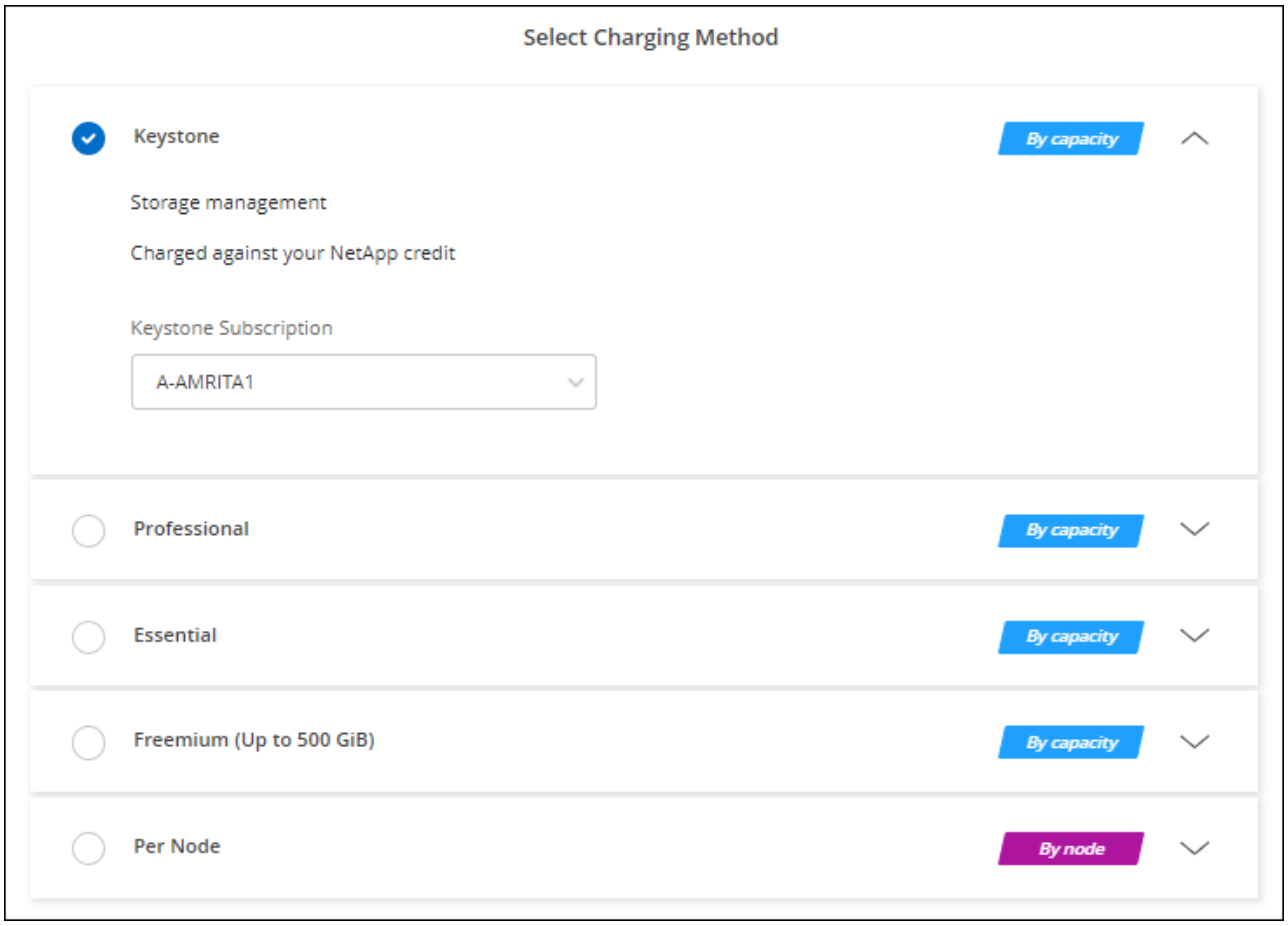
Abonnement Keystone

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 **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.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Google Cloud" .

Licence basée sur les nœuds

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. Pour plus d'informations, consultez :

- "Fin de disponibilité des licences basées sur des nœuds"
- "Fin de disponibilité des licences basées sur des nœuds"
- "Convertir une licence basée sur les nœuds en une licence basée sur la capacité"

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 NetApp Console en cours d'exécution.
  - 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 la 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 NetApp 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 **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"hiérarchisation des données" ou "NetApp Backup and Recovery" avec Cloud Volumes ONTAP, vous devez activer **Compte de service** et sélectionner un compte de service doté du rôle d'administrateur de stockage prédéfini. "Apprenez à créer un compte de service" .

Champ	Description
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 "Documentation Google Cloud : Étiquetage des ressources" .
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 *admin* ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet où se trouve la Console. Si aucun projet supplémentaire n'apparaît dans la liste déroulante, cela signifie que vous n'avez pas encore associé le compte de service à d'autres projets. Accédez à la Google Cloud Console, 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. Il s'agit du compte de service que vous avez configuré pour la console,"comme décrit sur cette page" . Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. 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 "Associer un abonnement Marketplace aux identifiants Google Cloud" .

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 la région et la zone Google Cloud pour votre système, 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 "Documentation Google Cloud : Configuration de l'accès privé à Google" .
Politique de pare-feu générée	Si vous laissez la console générer la politique de pare-feu pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **VPC sélectionné uniquement**, 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. • Si vous choisissez **Tous les VPC**, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.
Utiliser la politique de pare-feu existante	Si vous utilisez une politique de pare-feu existante, assurez-vous qu'elle inclut les règles requises :"En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP"

8. * Méthodes de 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 éteindre le système et ajouter un compte de service depuis le Google Cloud Console.

    "En savoir plus sur la hiérarchisation des données" .

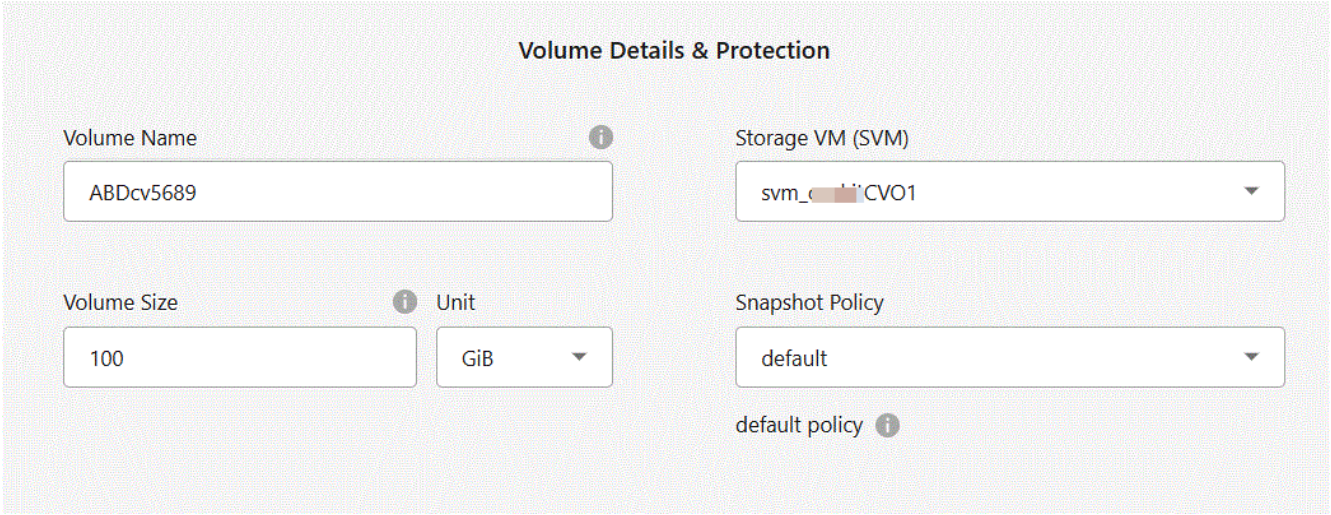
14. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

"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,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



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 **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 NetApp Console" 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** : Révisez 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.

> Après la fin du processus de déploiement, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Google Cloud, telles que les balises système et les étiquettes définies dans les ressources Google Cloud. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

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"NetApp Cloud Tiering" ou "Sauvegarde et récupération" services, vous devez activer le commutateur **Compte de service**, 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 "Documentation Google Cloud : Étiquetage des ressources" .
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 *admin* ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier le projet	Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet de la Console. Si aucun projet supplémentaire n'apparaît dans la liste déroulante, cela signifie que vous n'avez pas encore associé le compte de service à d'autres projets. Accédez à la Google Cloud Console, 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. Il s'agit du compte de service que vous avez configuré pour la console,"comme décrit sur cette page" . Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. 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 "Associer un abonnement Marketplace aux identifiants Google Cloud" .

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 une zone.

   "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	Si vous laissez la console générer la politique de pare-feu pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **VPC sélectionné uniquement**, 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. • Si vous choisissez **Tous les VPC**, le filtre source pour le trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	Si vous utilisez une stratégie de pare-feu existante, assurez-vous qu'elle inclut les règles requises. "En savoir plus sur les règles de pare-feu pour Cloud Volumes ONTAP" .

8. * Méthodes de 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 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** :

    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** 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 éteindre le système et ajouter un compte de service depuis le Google Cloud Console.

  "En savoir plus sur la hiérarchisation des données" .

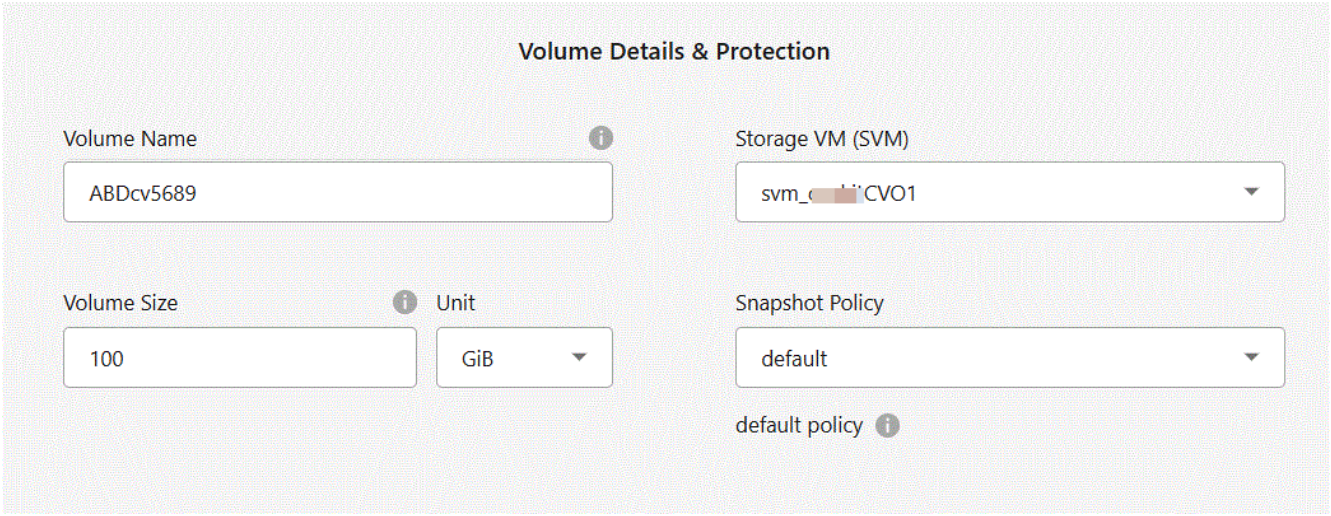
14. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    "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,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

    L'image suivante montre la première page de l'assistant de création de volume :



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 **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. Se référer à la "Documentation sur l'automatisation de la NetApp Console" 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** : Révisez 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.

> Après la fin du processus de déploiement, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Google Cloud, telles que les balises système et les étiquettes définies dans les ressources Google Cloud. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

Liens connexes

- "Planification de votre configuration Cloud Volumes ONTAP dans Google Cloud"

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/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[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

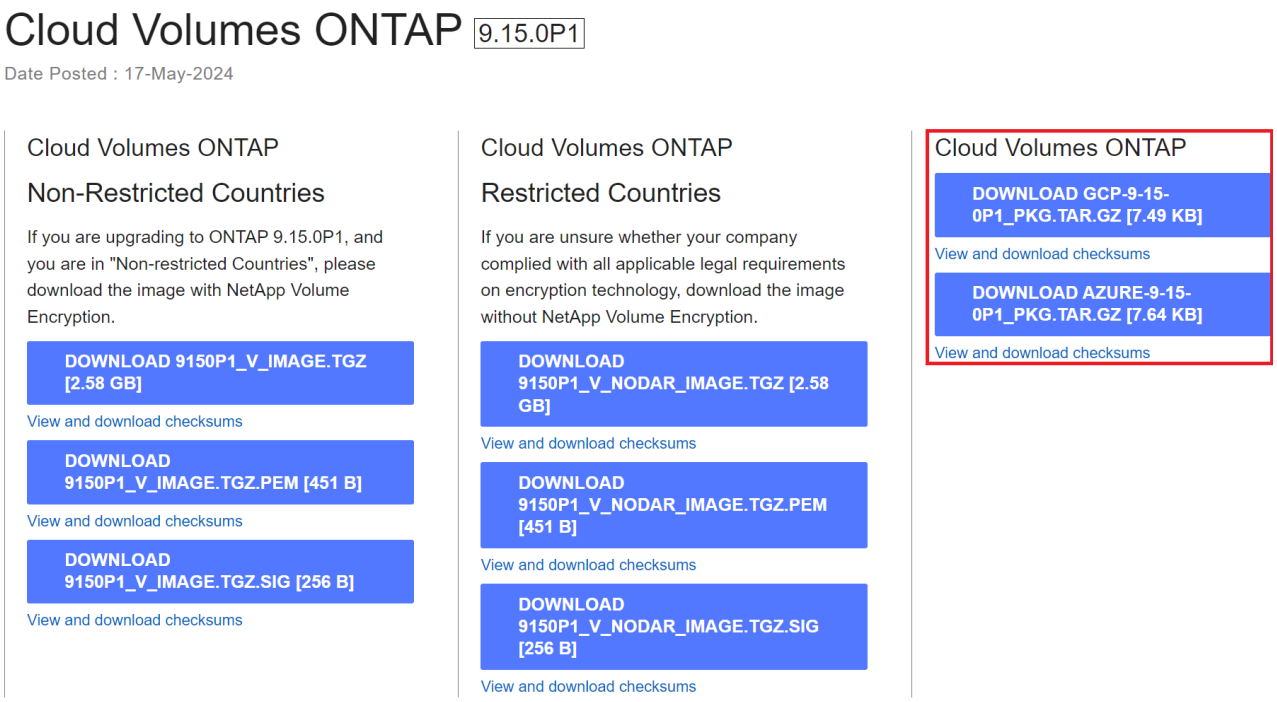
Vérification de la signature d'image Google Cloud pour Cloud Volumes ONTAP

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.

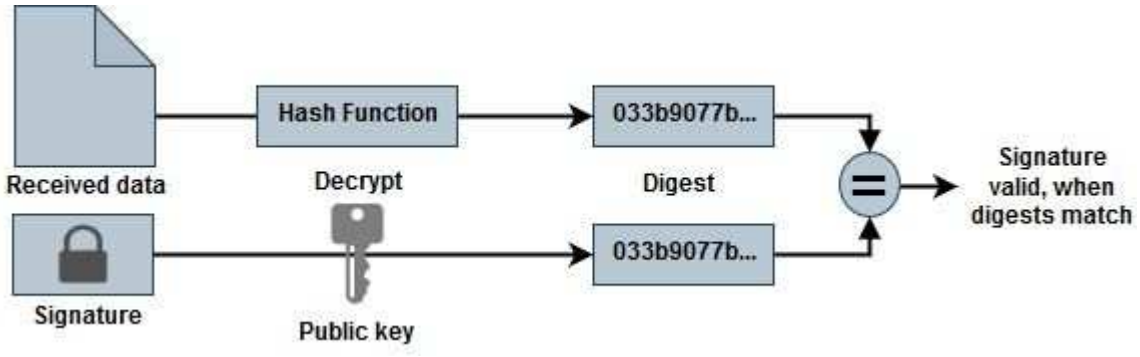
Résumé du flux de travail de vérification des images signées

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)



- 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 OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -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 OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -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: CE894F8251AA15A28462CA312361D261FBF8FE78
      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
```