Démarrer avec Amazon Web Services

Cloud Volumes ONTAP

NetApp
February 13, 2026

Sommaire

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	

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

Choisissez une vitesse d'écriture

La console vous permet de choisir un paramètre de vitesse d'écriture pour Cloud Volumes ONTAP. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés, ainsi que les risques et les recommandations lors de l'utilisation d'une vitesse d'écriture élevée. "En savoir plus sur la vitesse d'écriture" .

Choisissez un profil d'utilisation du volume

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

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

Provisionnement léger

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

Déduplication

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

Compression

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

Configurez votre réseau

Configurer la mise en réseau AWS pour Cloud Volumes ONTAP

La 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

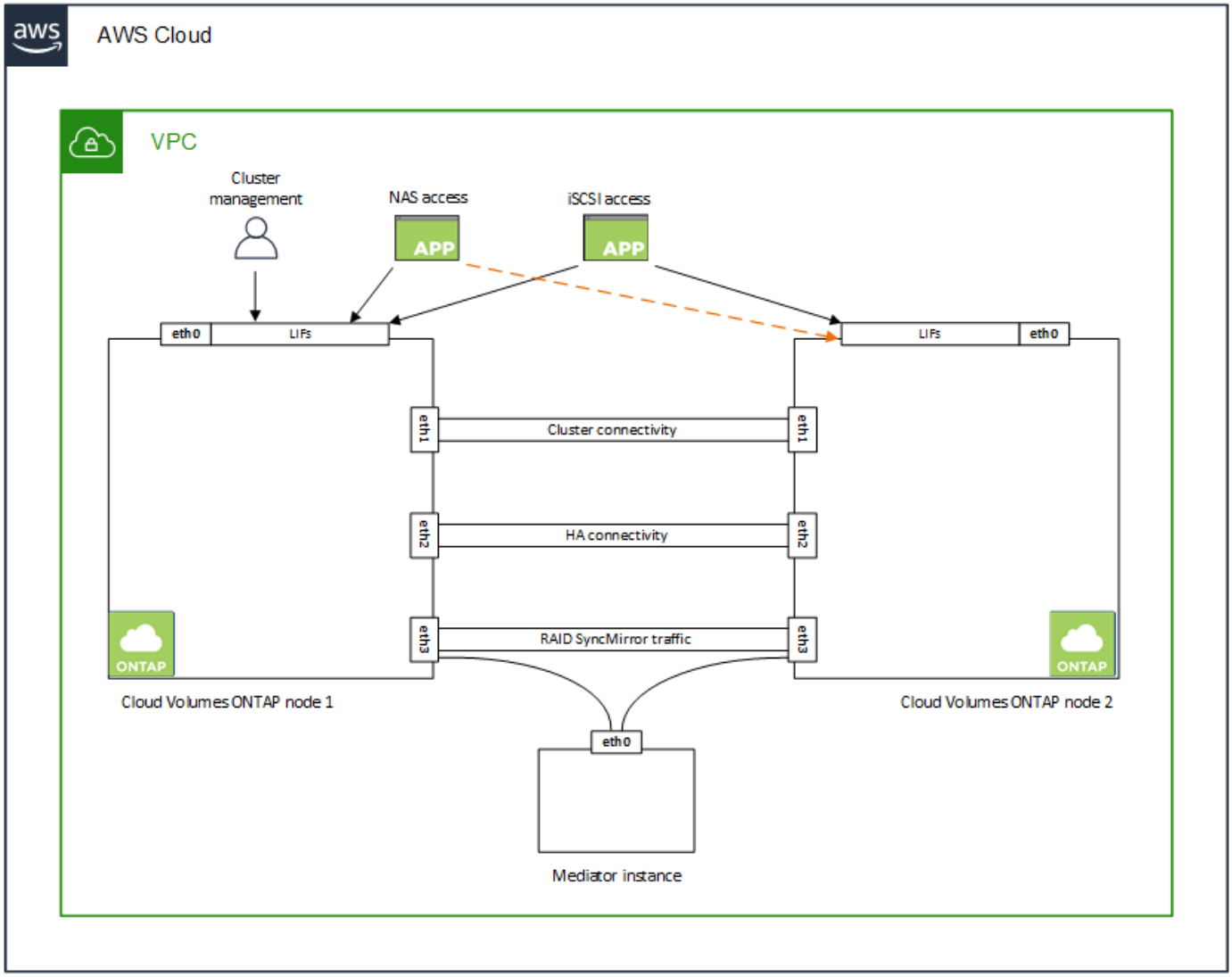
La NetApp Console alloue 6 adresses IP à un système à nœud unique.

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.
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.

FRV	Interface	Nœud	But
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" .

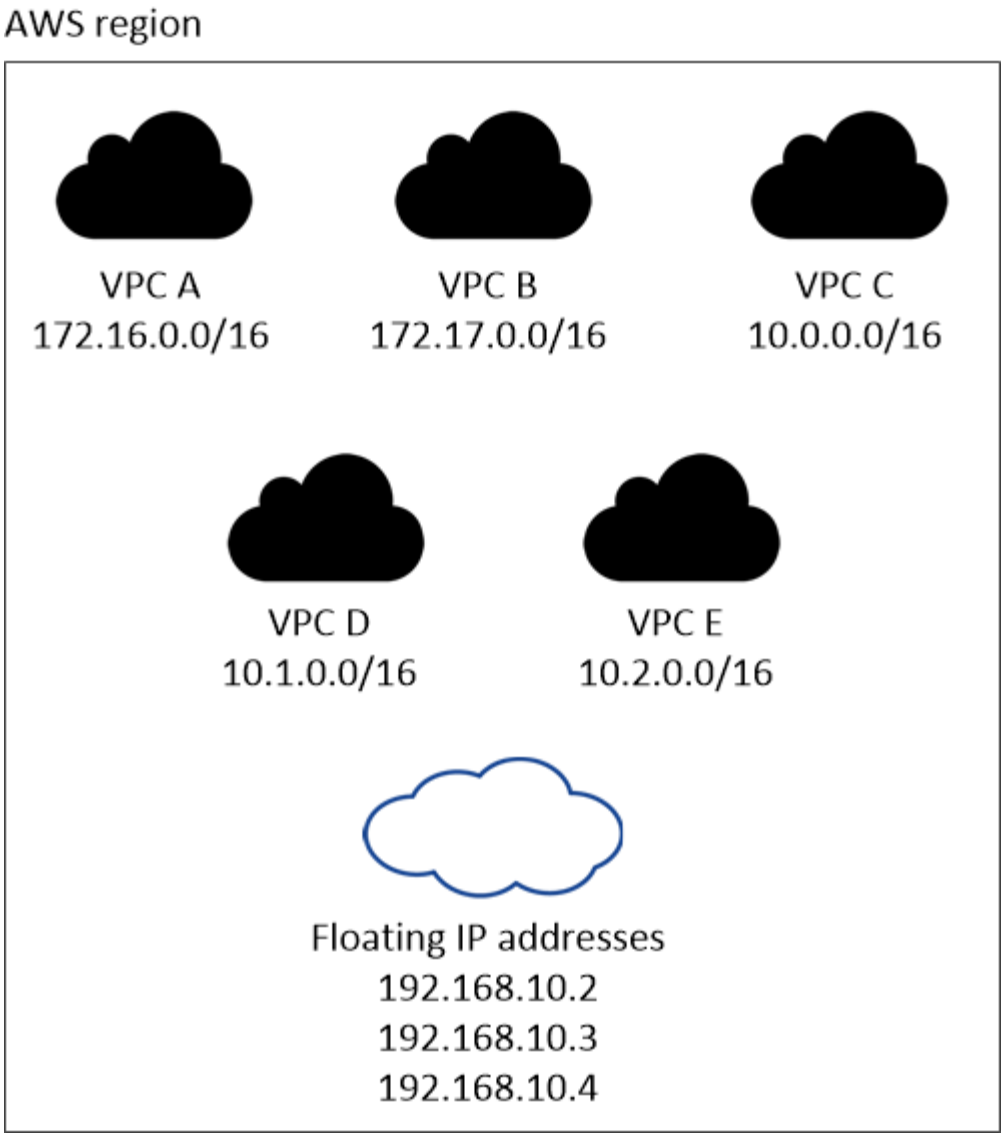
Une adresse IP flottante est destinée à la gestion du cluster, une autre aux données NFS/CIFS sur le nœud 1 et une autre aux données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante pour la gestion SVM est facultative.

> 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" .

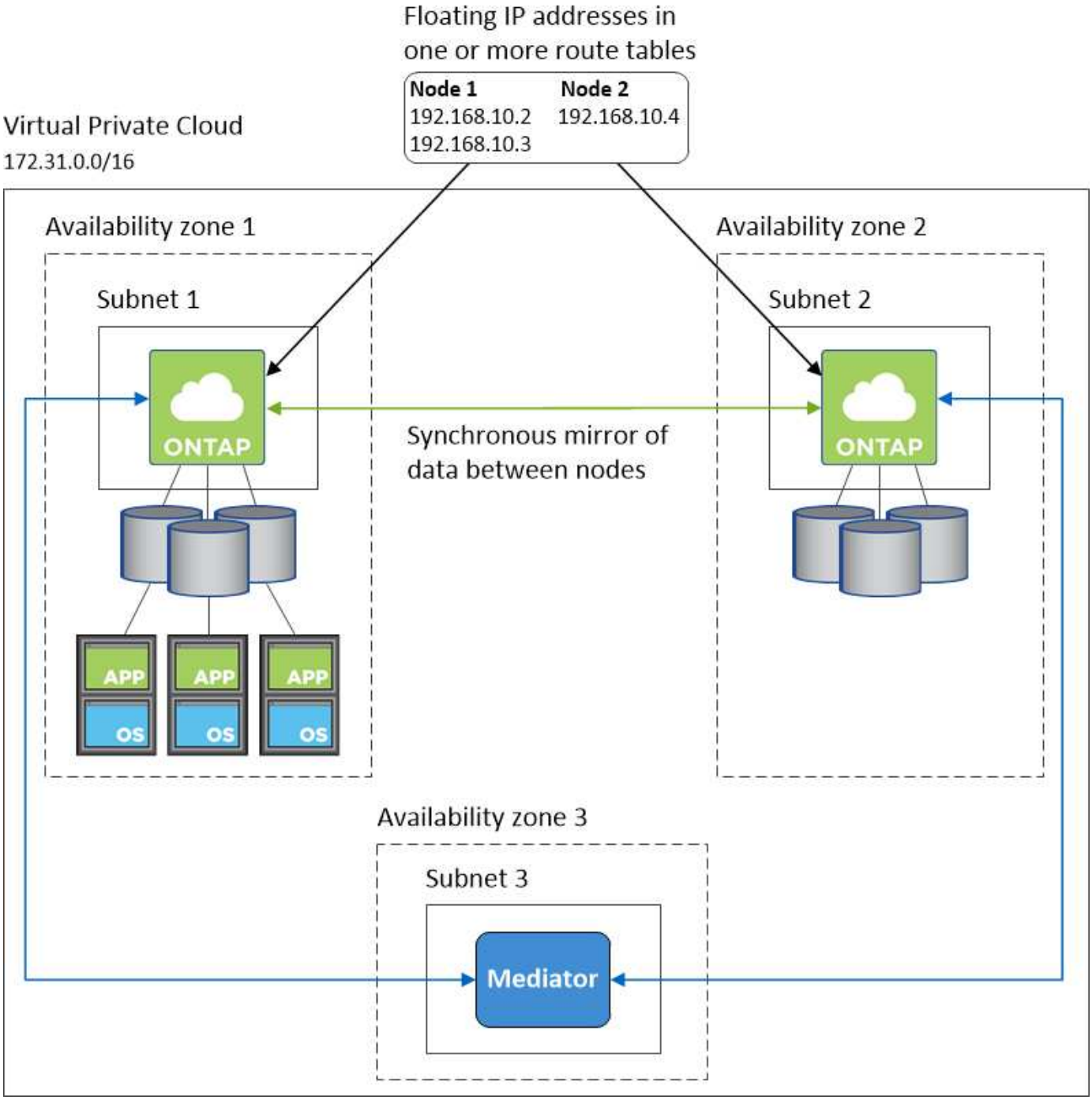
Connexion aux outils de gestion NetApp

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

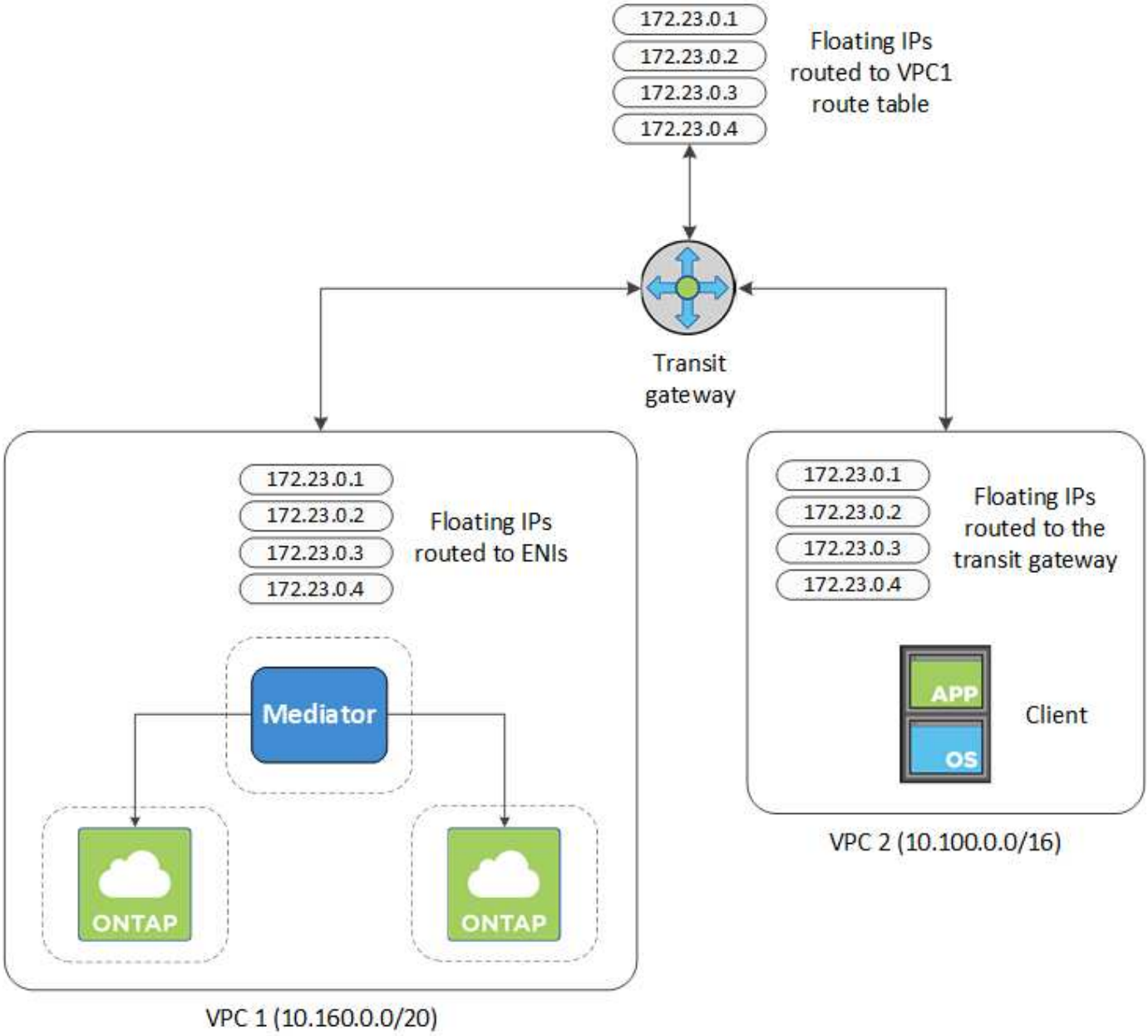
Configurer une passerelle de transit AWS pour permettre l'accès à une paire HA"adresses IP flottantes" depuis l'extérieur du VPC où réside la paire HA.

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.

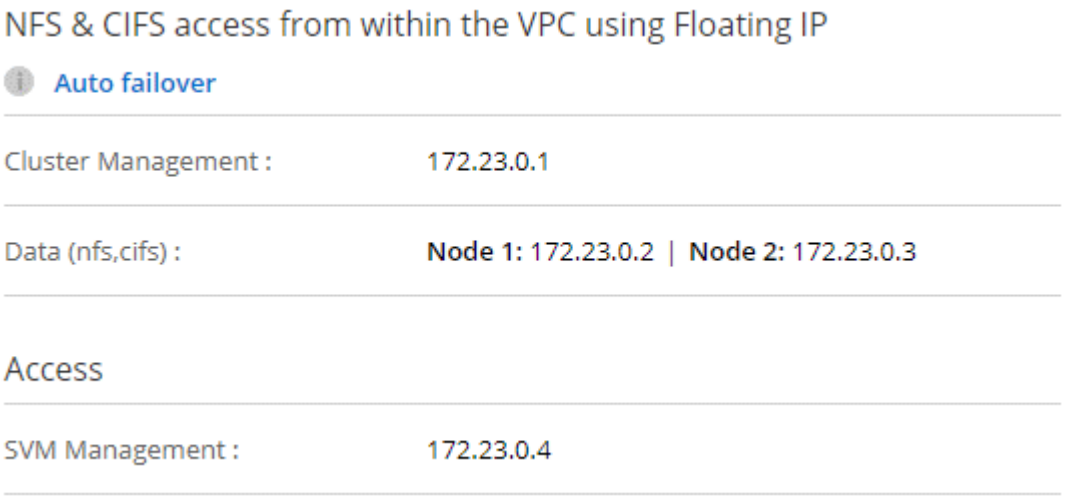


Les étapes suivantes illustrent comment configurer une configuration similaire.

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.

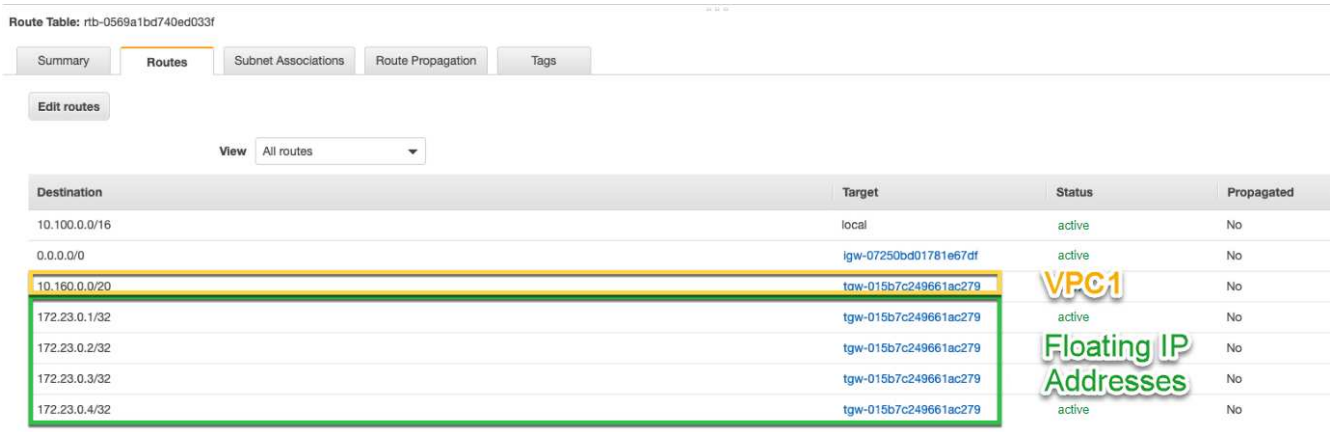
   Vous pouvez trouver les adresses IP flottantes sur la page d'informations système dans la NetApp Console. Voici un exemple :



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.

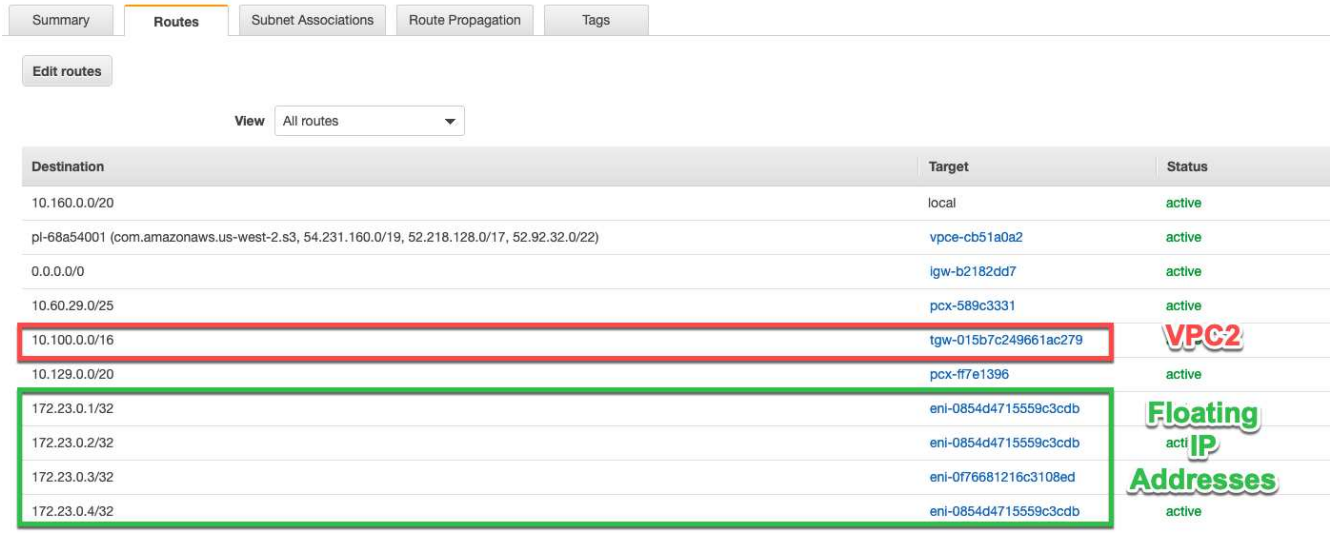
      L'exemple d'image suivant montre la table de routage pour VPC 2, qui inclut les routes vers VPC 1 et les adresses IP flottantes.



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.

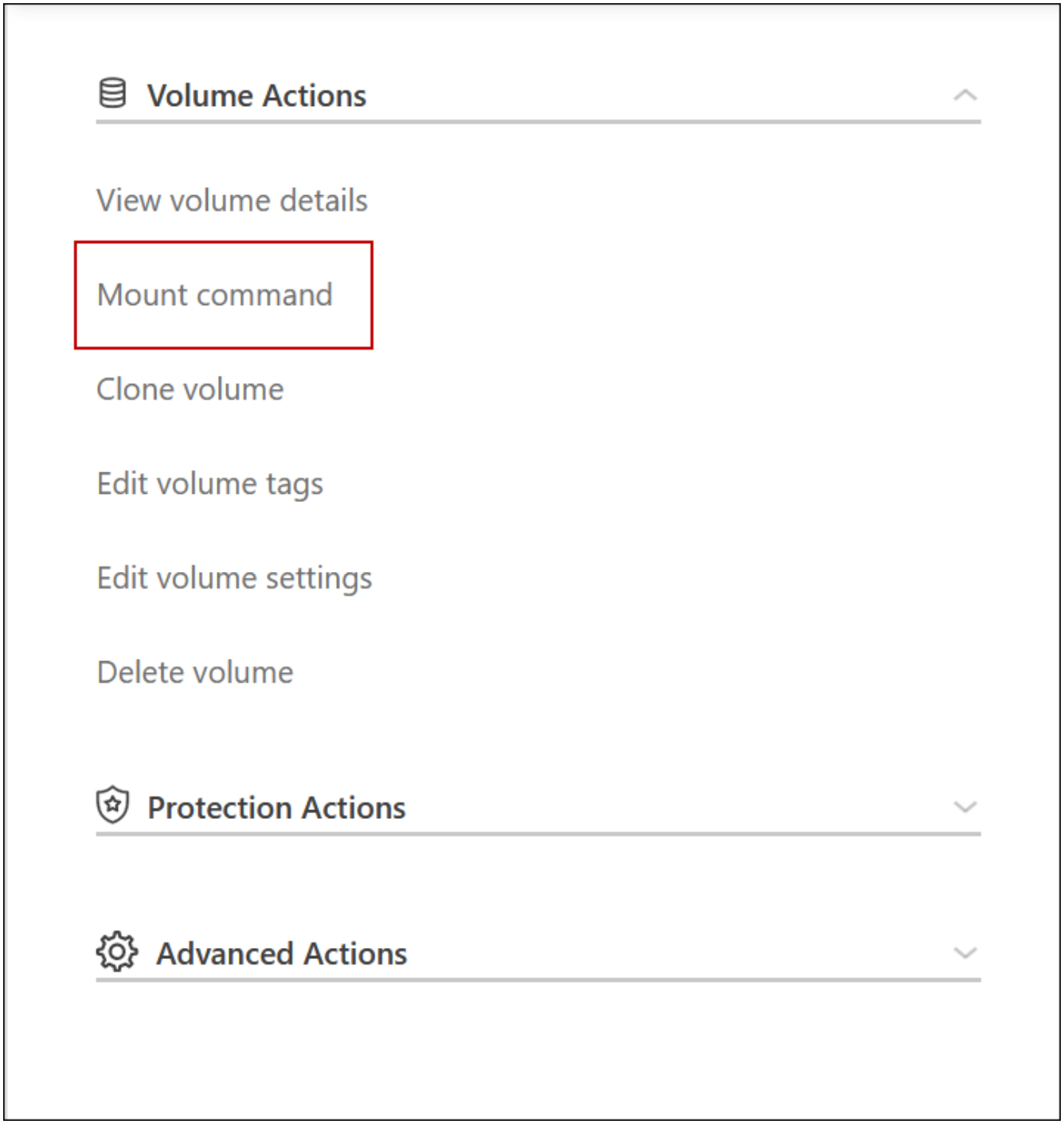
   L'exemple d'image suivant montre la table de routage pour VPC 1. Il comprend un itinéraire vers les adresses IP flottantes et vers le VPC 2, où réside un client. La console a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire HA.



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

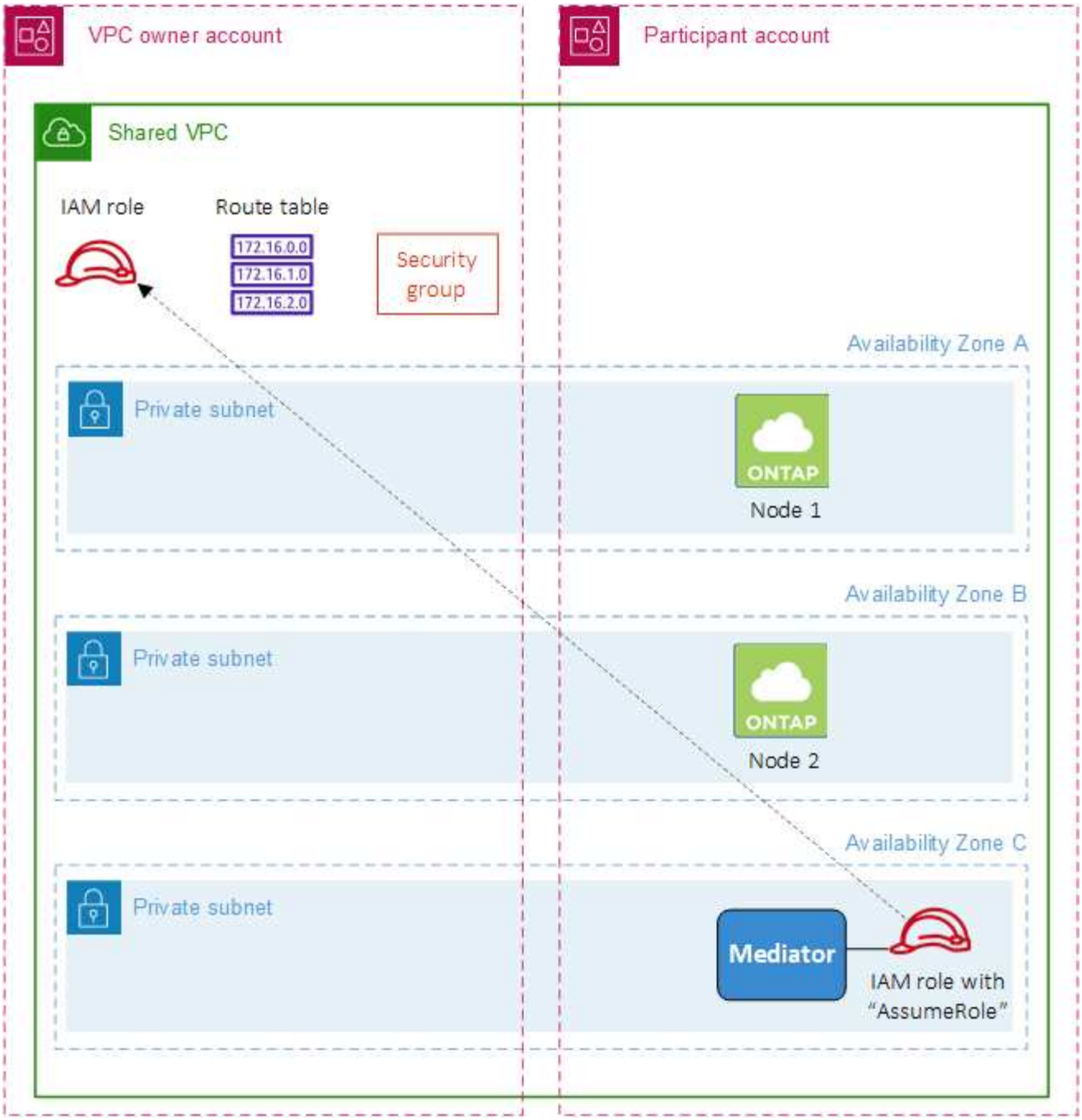
À partir de la version 9.11.1, les paires Cloud Volumes ONTAP HA sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre organisation de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement AWS, puis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

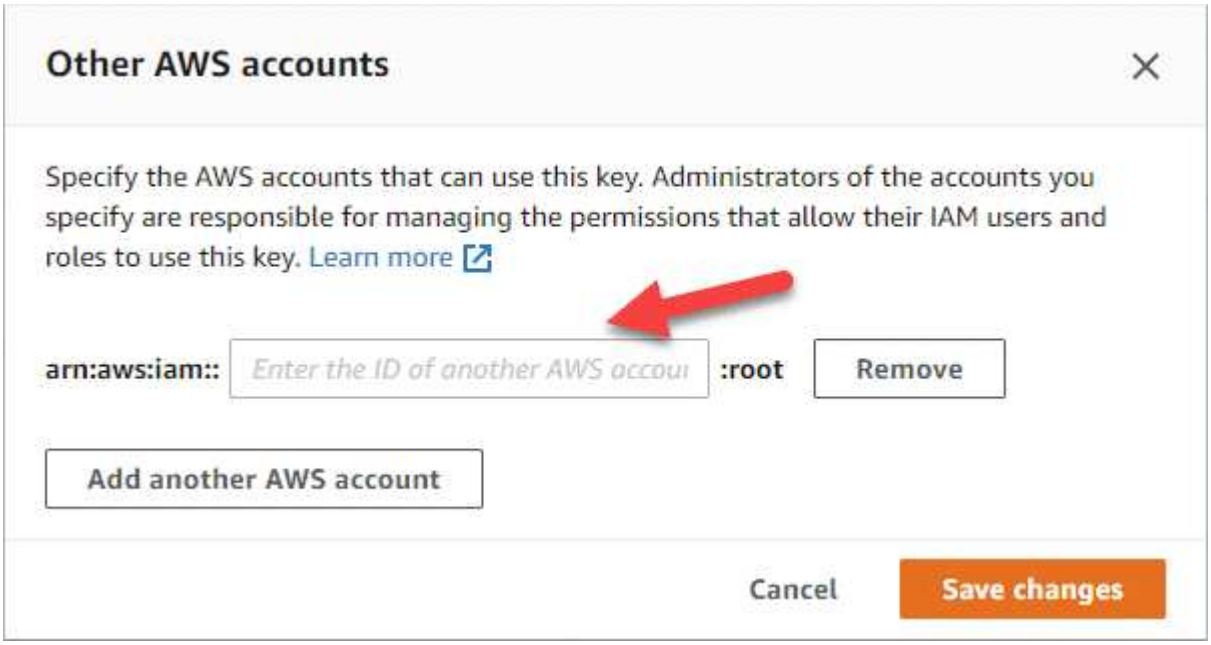
3. Si la CMK se trouve dans un autre compte AWS, procédez comme suit :

   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" .

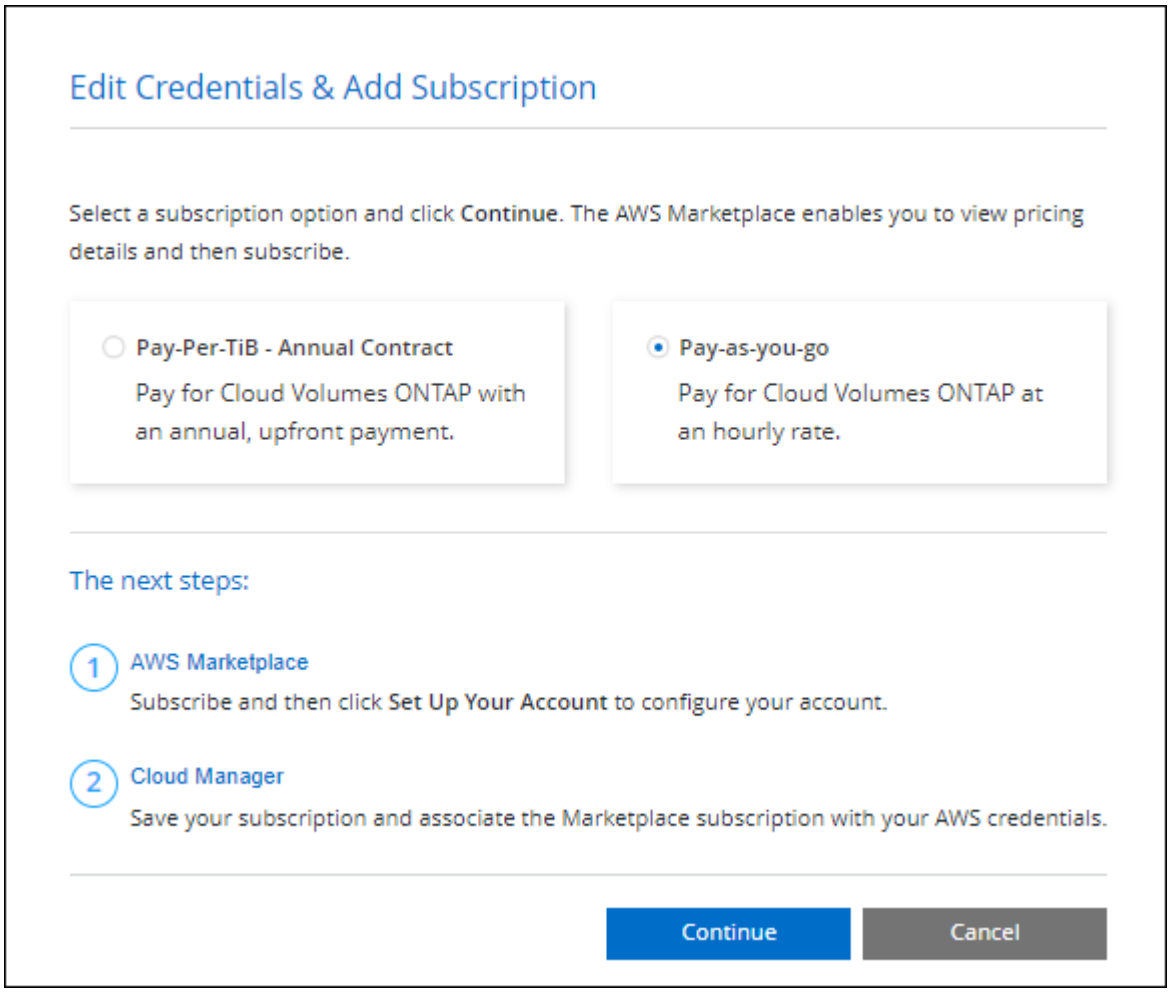
Étapes

1. Dans le menu de navigation de gauche de la NetApp Console, sélectionnez **Stockage > Gestion**.

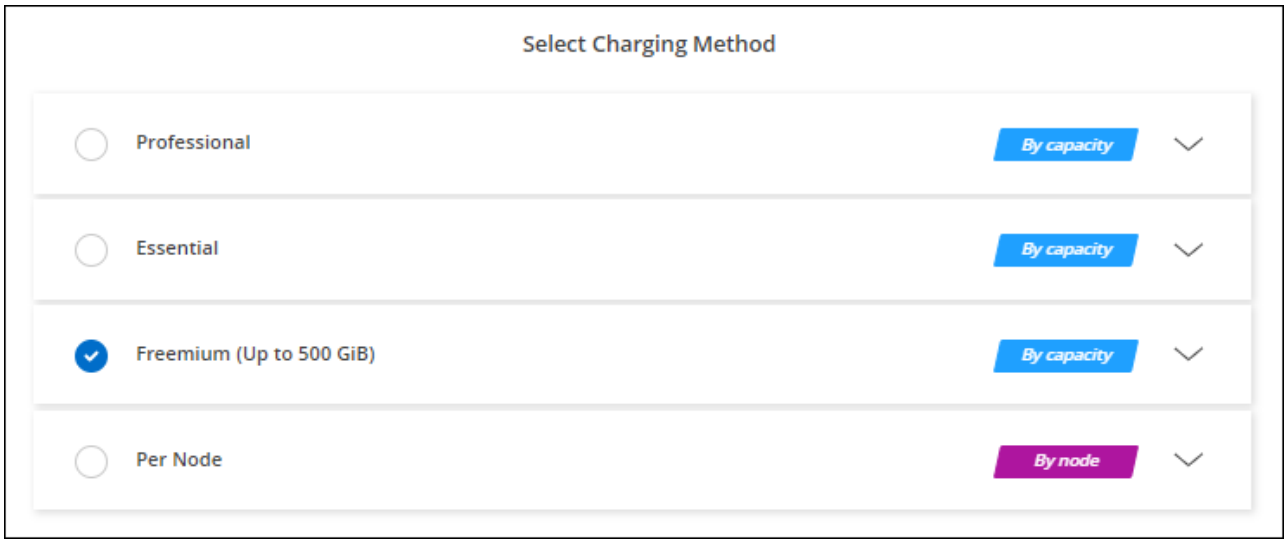
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

   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.

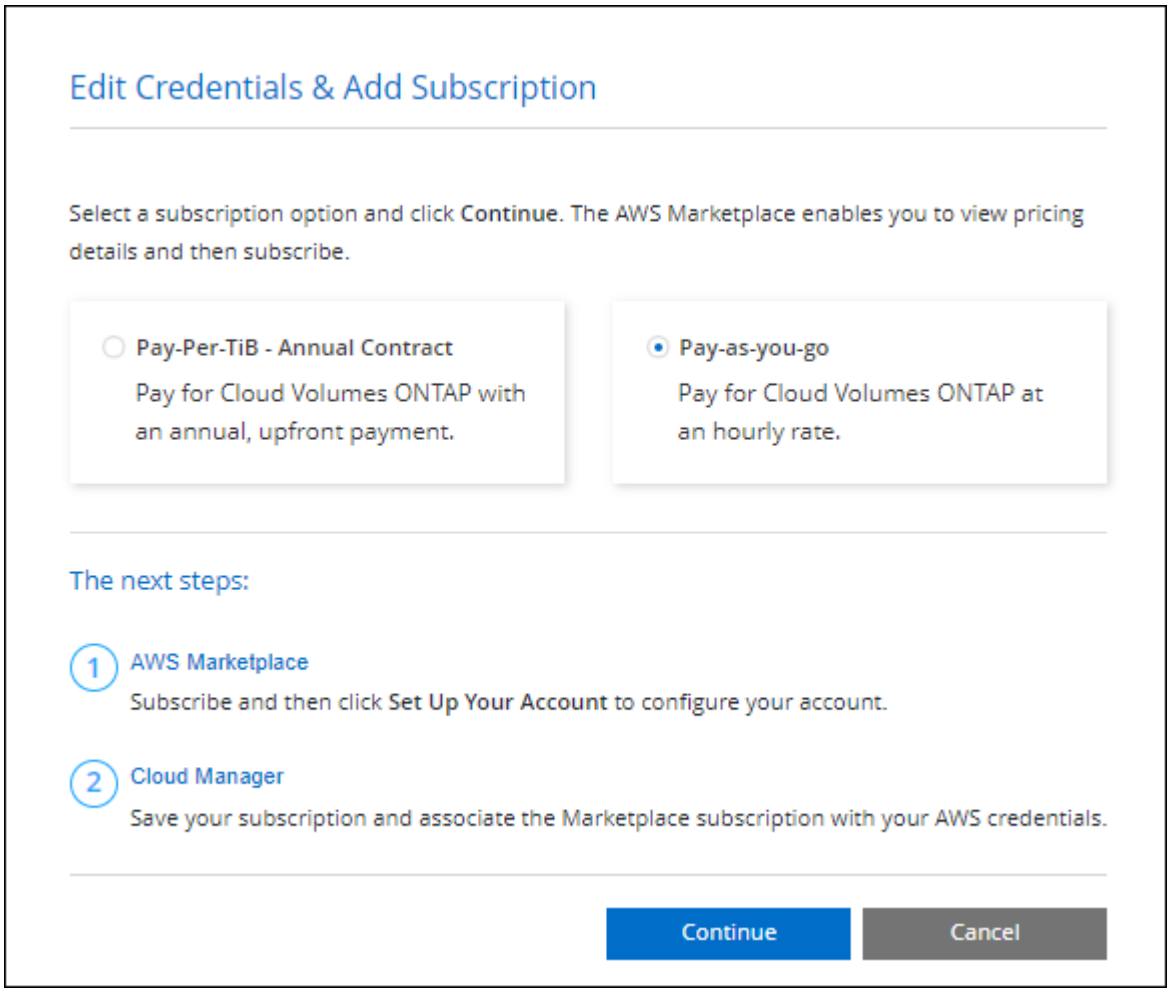
   Votre licence doit être disponible depuis la console avant de pouvoir l'utiliser avec Cloud Volumes ONTAP.

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

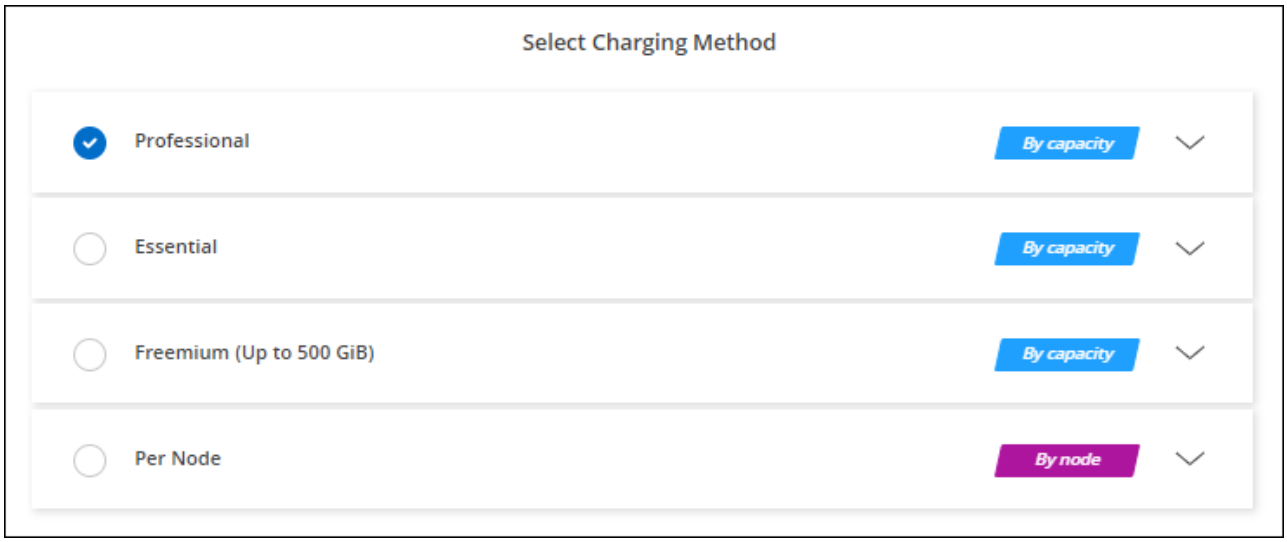
3. Sur la page **Systèmes** de la console, cliquez sur **Ajouter un système** et suivez les étapes.

   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" .

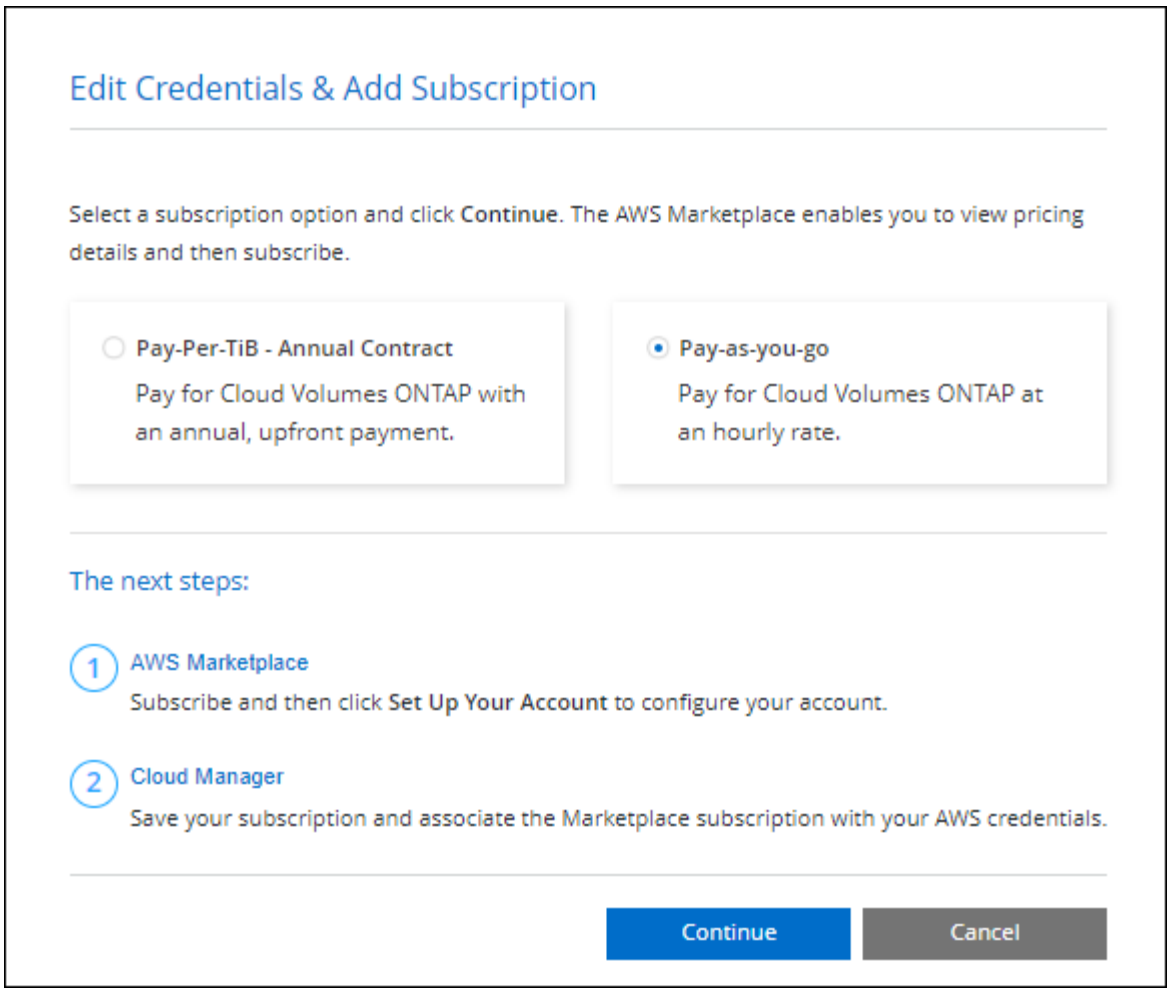
Abonnement PAYGO

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

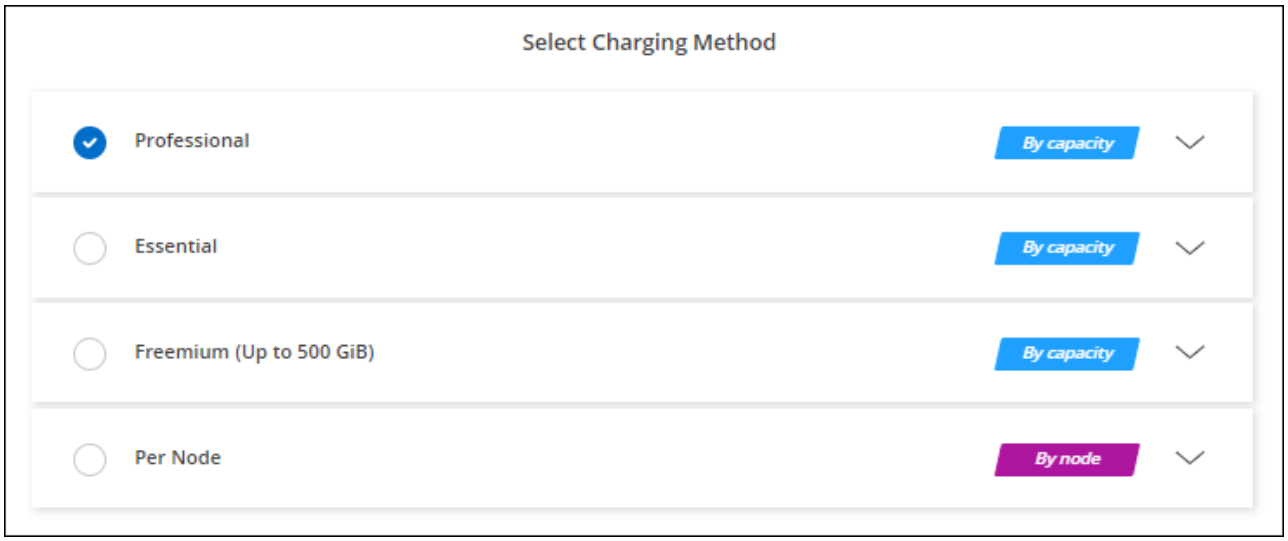
Lorsque vous créez un système Cloud Volumes ONTAP , la console vous invite à vous abonner à l'accord disponible sur AWS Marketplace. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes Cloud Volumes ONTAP supplémentaires.

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"

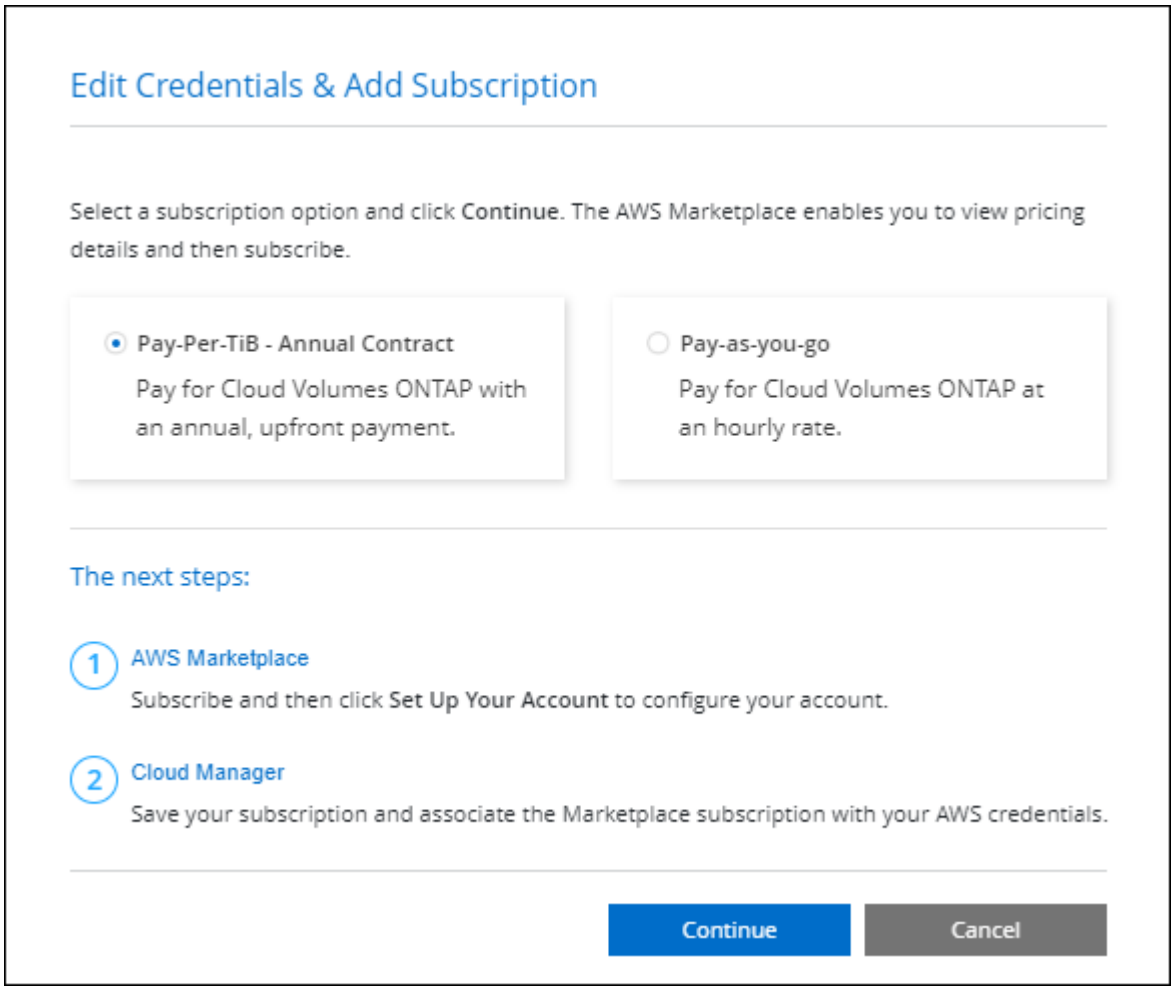
Contrat annuel

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

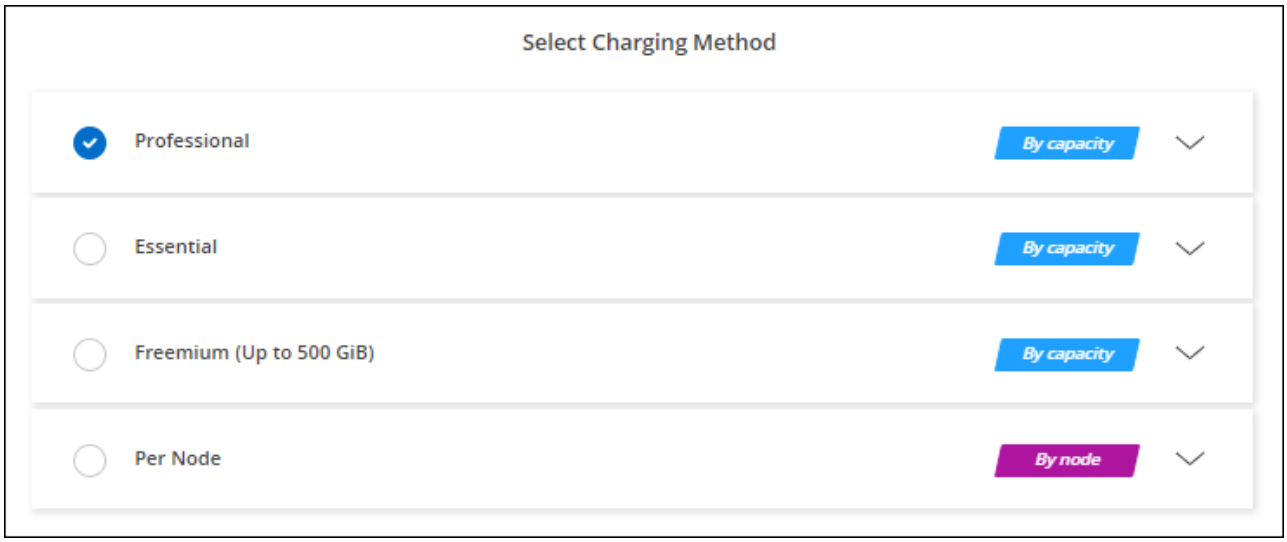
Semblable à un abonnement horaire, la console vous invite à souscrire au contrat annuel disponible sur AWS Marketplace.

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" .

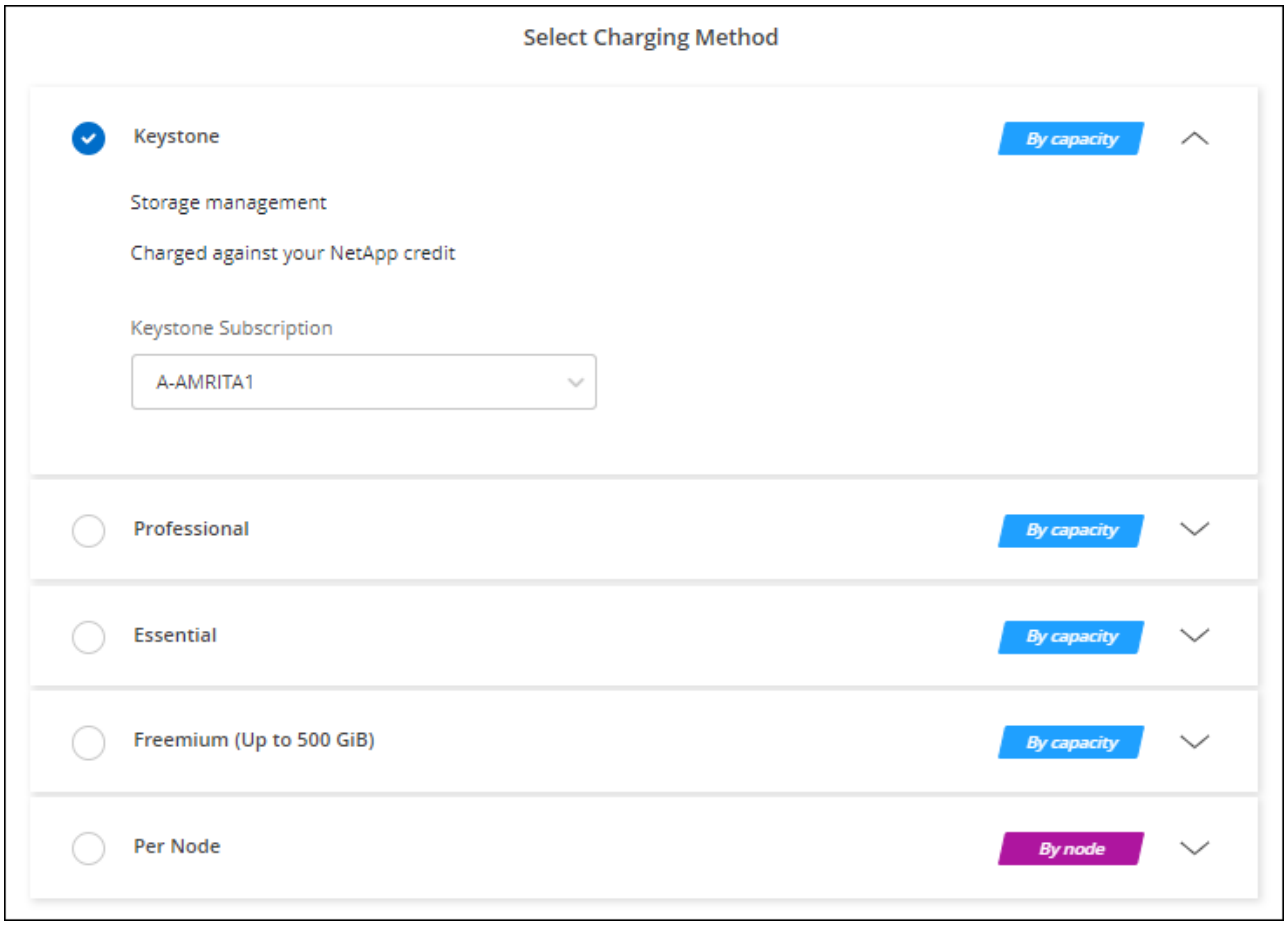
Abonnement Keystone

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.

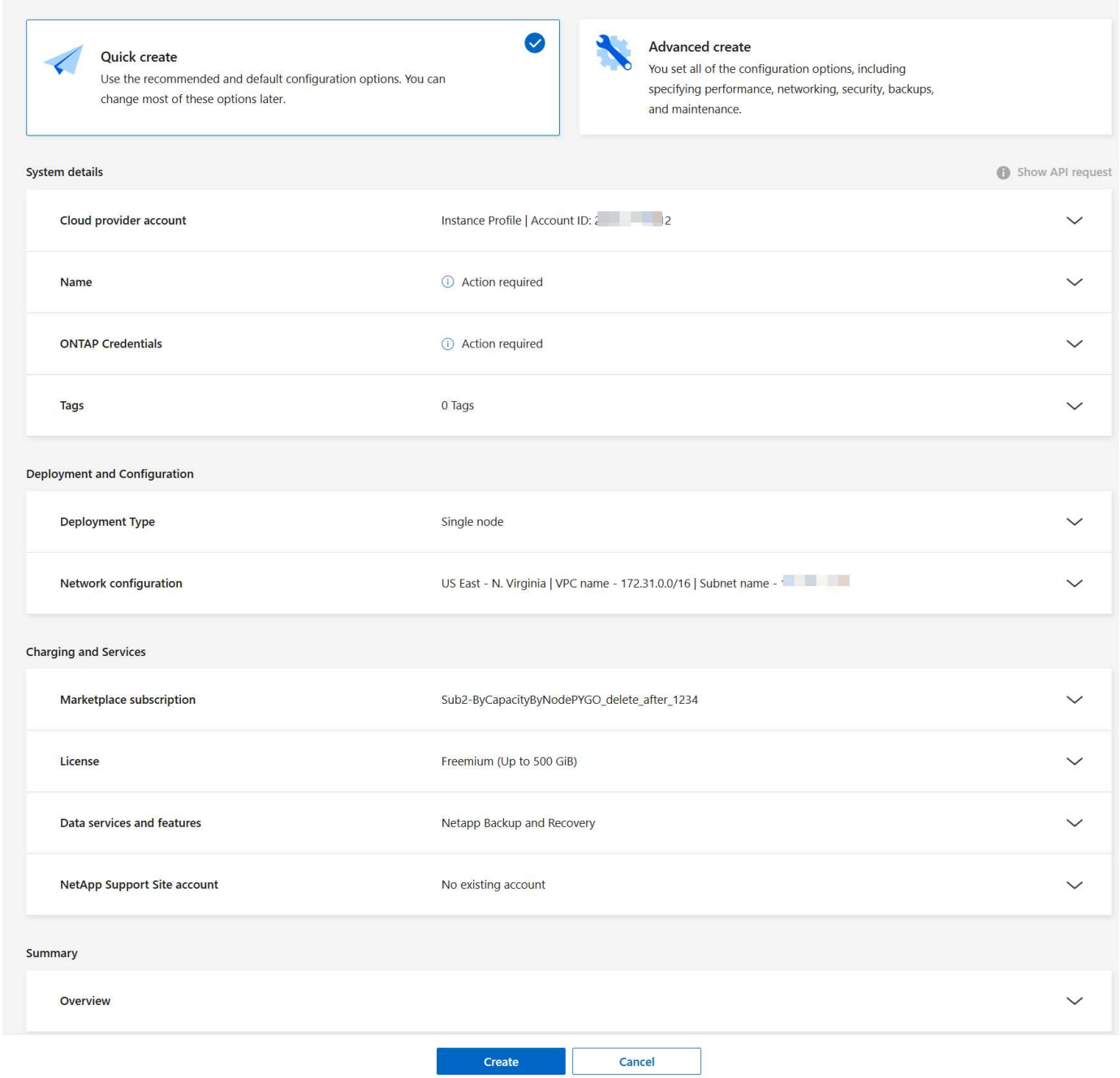
  Pour plus de détails, reportez-vous à"Exigences réseau pour Cloud Volumes ONTAP dans AWS" .

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

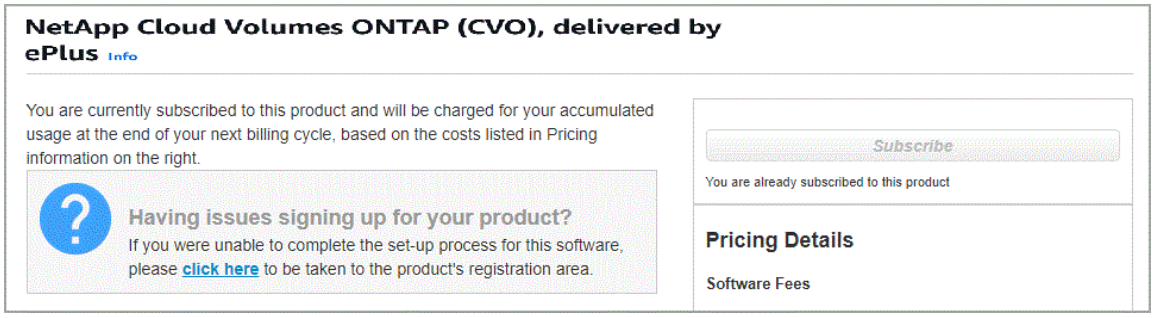
1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. Sélectionnez **Amazon Web Services** et * Cloud Volumes ONTAP Single Node*.
4. Sélectionnez **Création avancée**. Étant donné que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

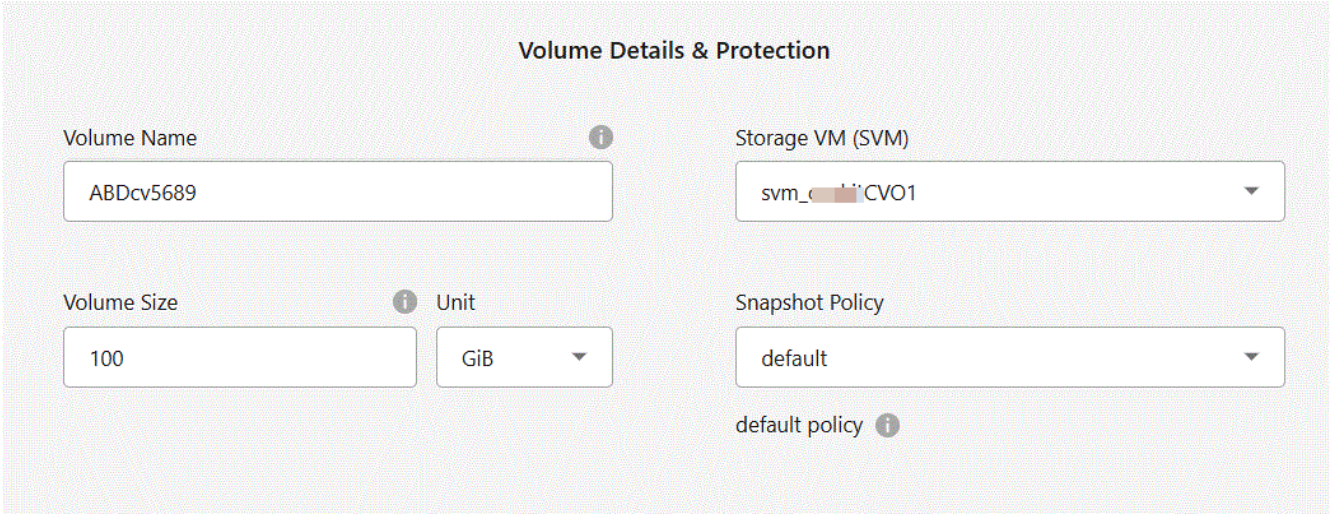
17. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    "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 »" .

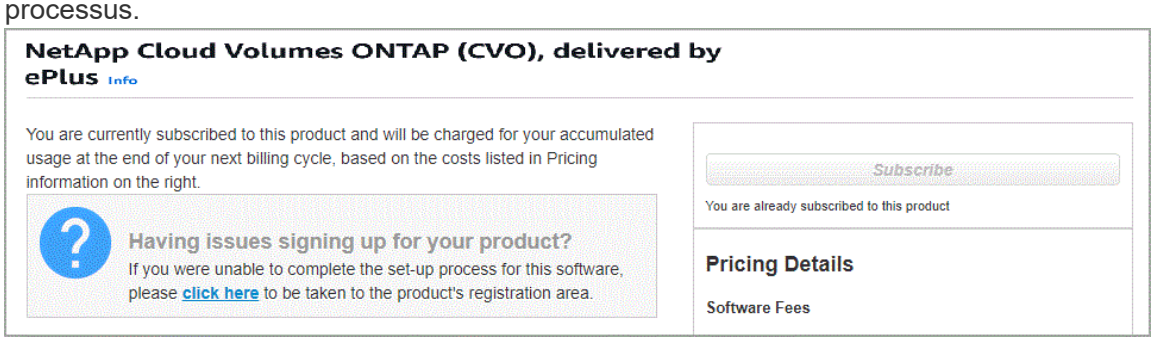
   Si vous exécutez l'agent de console 3.9.36 ou une version antérieure, vous devez ajouter le `DescribeAvailabilityZones` autorisation au rôle AWS dans la console AWS EC2.

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.

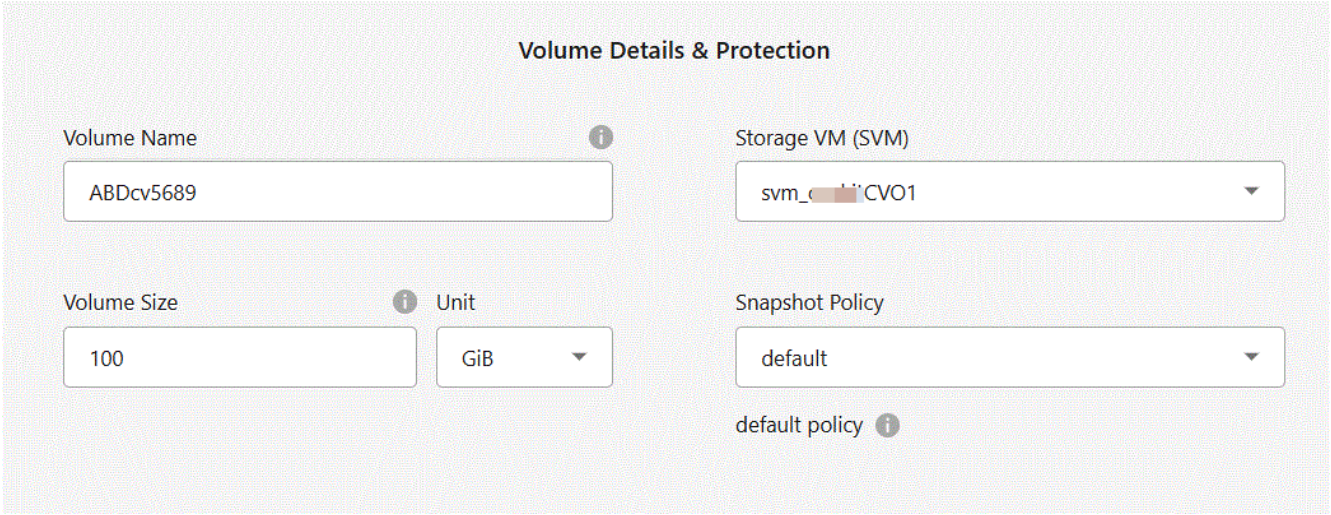
19. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    "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>`