Configurez votre réseau

Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/storage-management-cloud-volumes-ontap/reference-networking-aws.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Configurez votre réseau . . . 1
- Configurer la mise en réseau AWS pour Cloud Volumes ONTAP . . . 1
  - Exigences générales . . . 1
  - Exigences relatives aux paires HA dans plusieurs AZ . . . 7
  - Exigences pour l’agent de console . . . 11
- Configurer une passerelle de transit AWS pour les paires Cloud Volumes ONTAP HA . . . 12
- Déployer des paires Cloud Volumes ONTAP HA dans un sous-réseau partagé AWS . . . 17
- Configurer la création de groupes de placement pour les paires Cloud Volumes ONTAP HA dans les zones de disponibilité uniques AWS . . . 19
- Règles entrantes et sortantes du groupe de sécurité AWS pour Cloud Volumes ONTAP . . . 20
  - Règles pour Cloud Volumes ONTAP . . . 20
  - Règles pour le groupe de sécurité externe du médiateur HA . . . 25
  - Règles pour le groupe de sécurité interne de configuration HA . . . 26
  - Règles pour l’agent de console . . . 26

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

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact si le point de terminaison n'est pas disponible
\ 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.
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.

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact si le point de terminaison n'est pas disponible
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

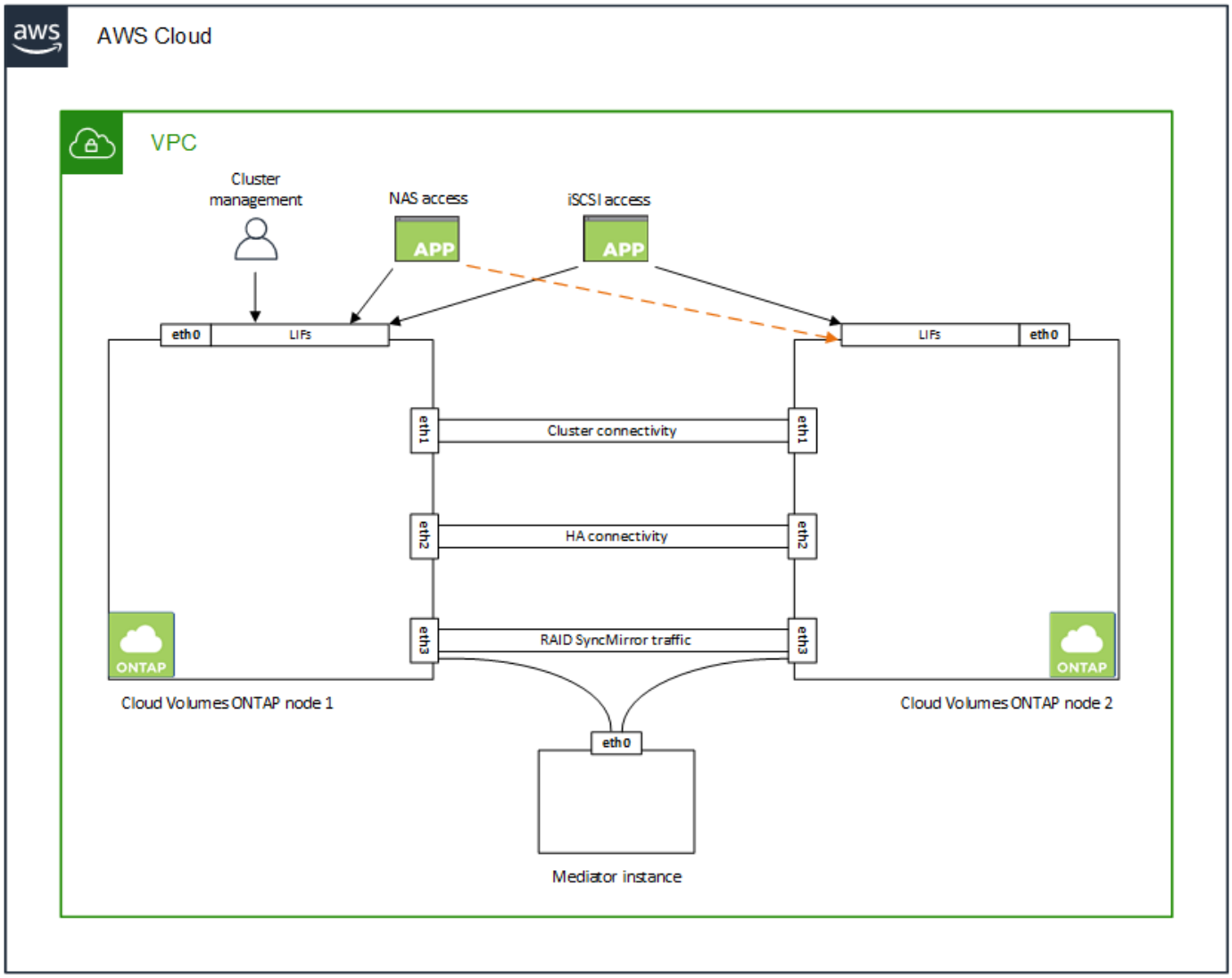
La NetApp Console alloue 6 adresses IP à un système à nœud unique.

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" .

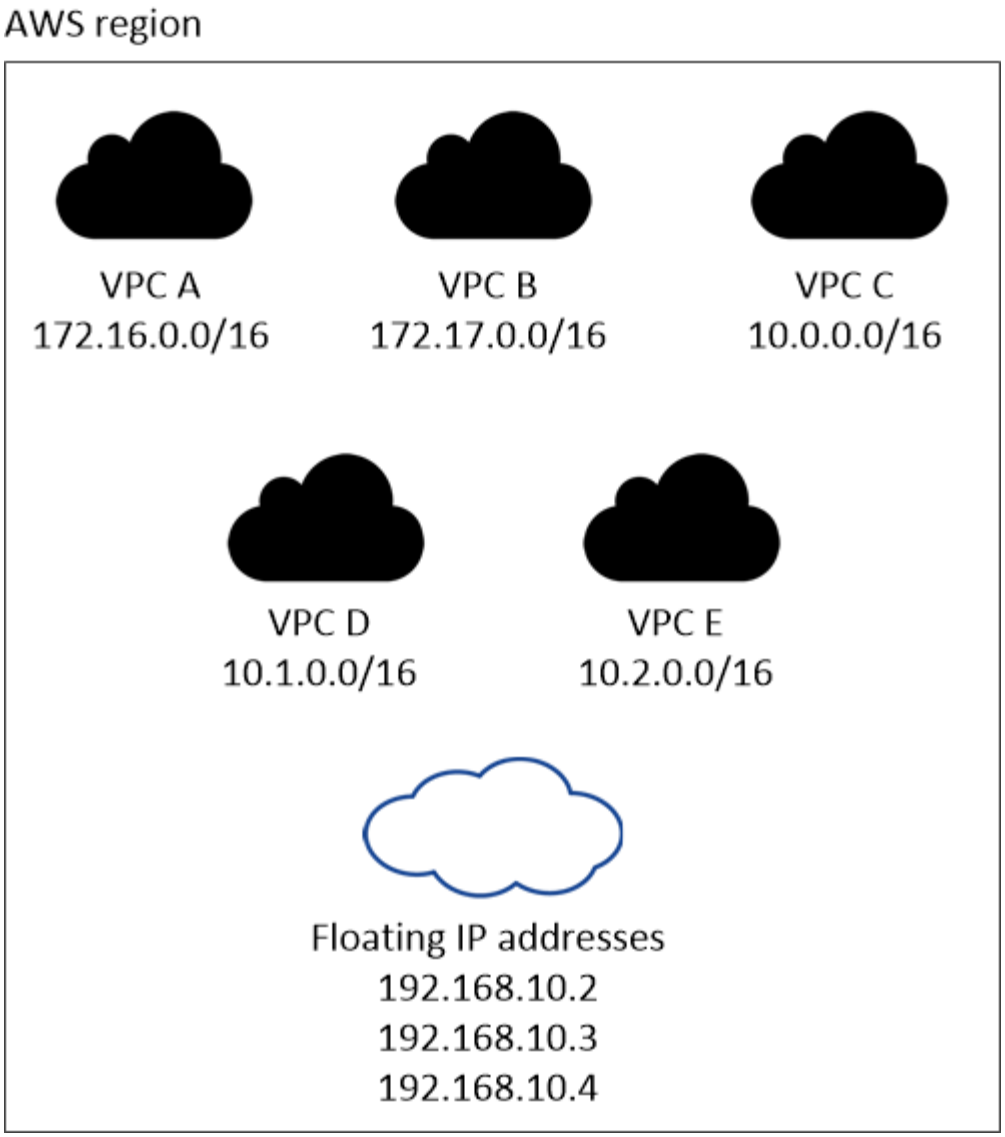
Une adresse IP flottante est destinée à la gestion du cluster, une autre aux données NFS/CIFS sur le nœud 1 et une autre aux données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante pour la gestion SVM est facultative.

> 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" .

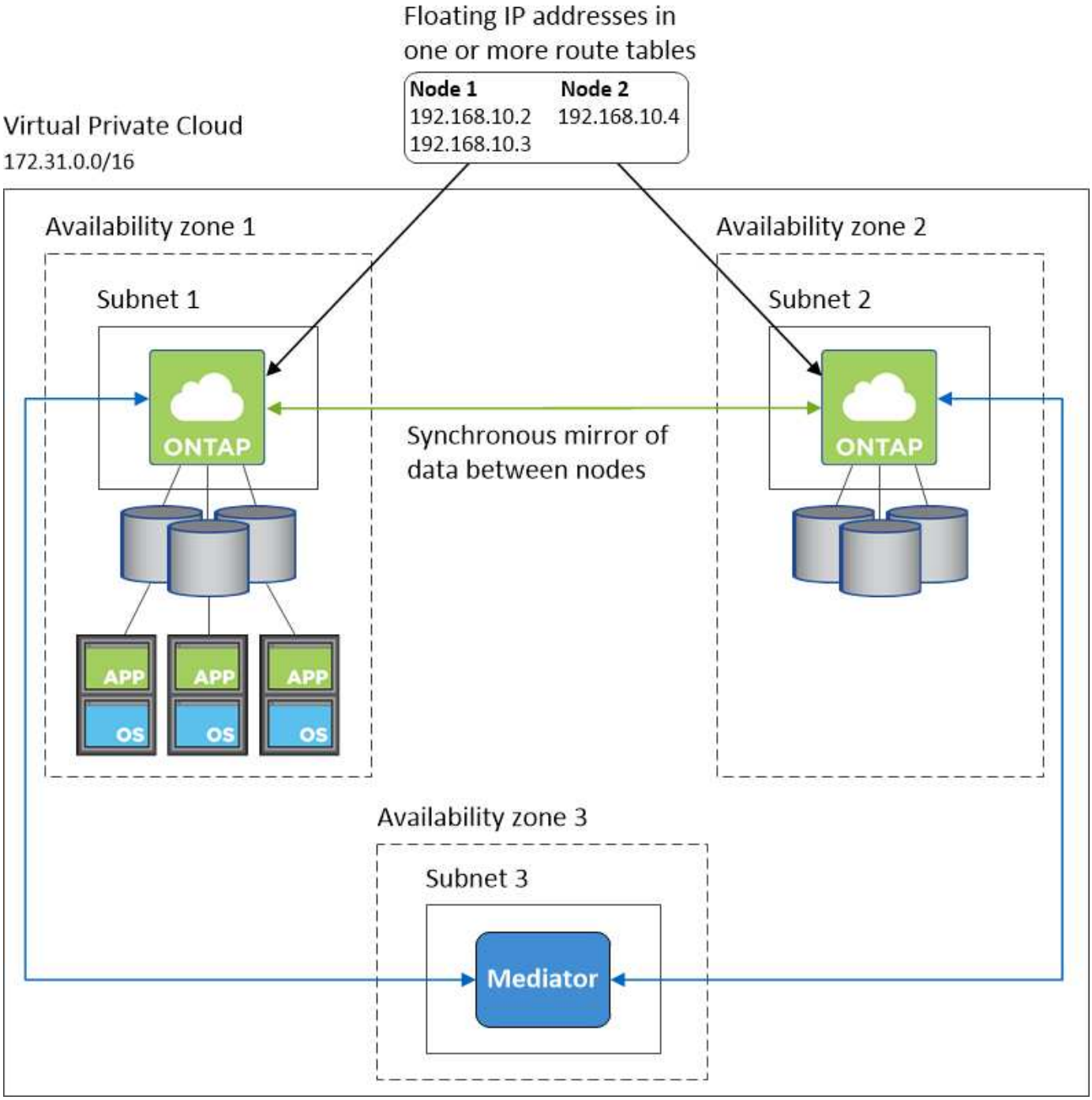
Connexion aux outils de gestion NetApp

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

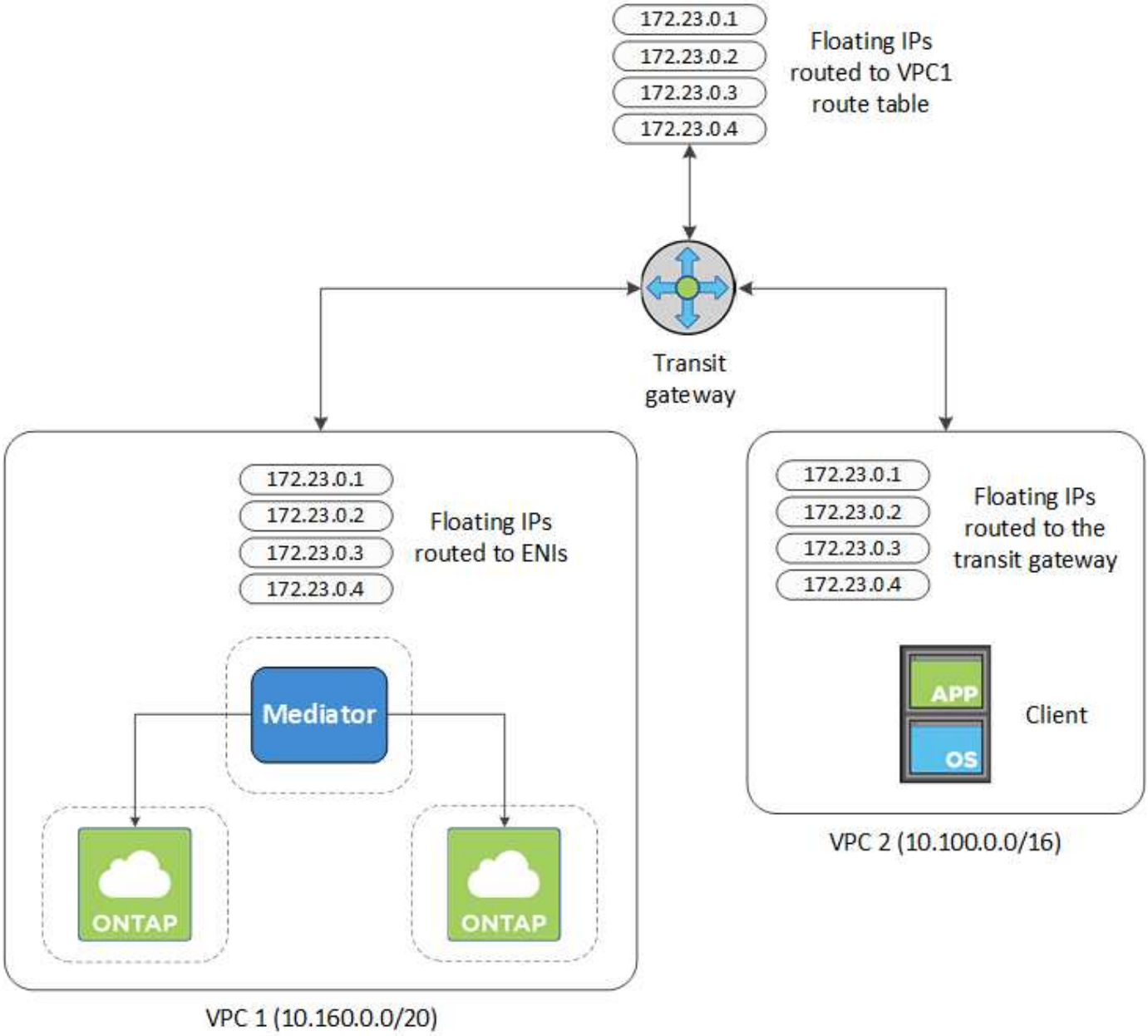
Configurer une passerelle de transit AWS pour permettre l'accès à une paire HA"adresses IP flottantes" depuis l'extérieur du VPC où réside la paire HA.

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.

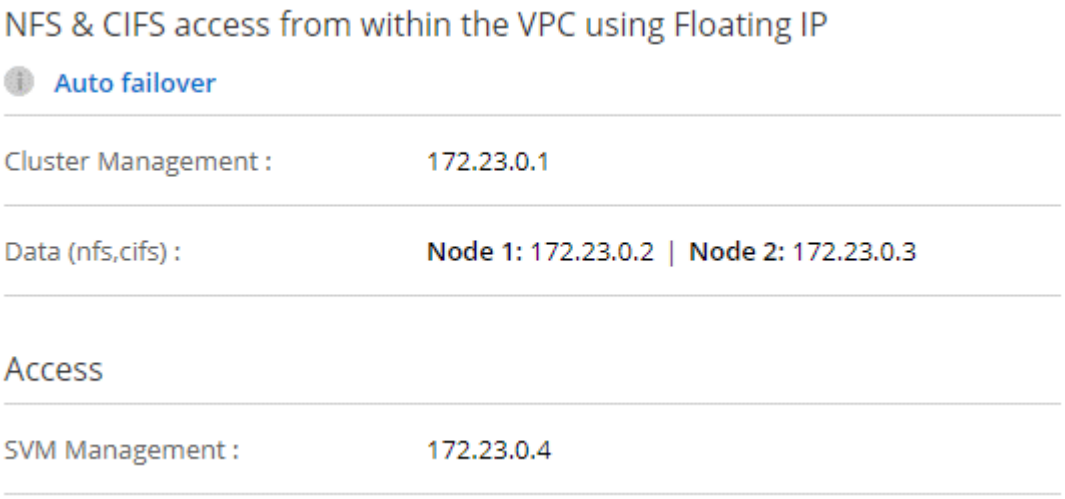


Les étapes suivantes illustrent comment configurer une configuration similaire.

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 :



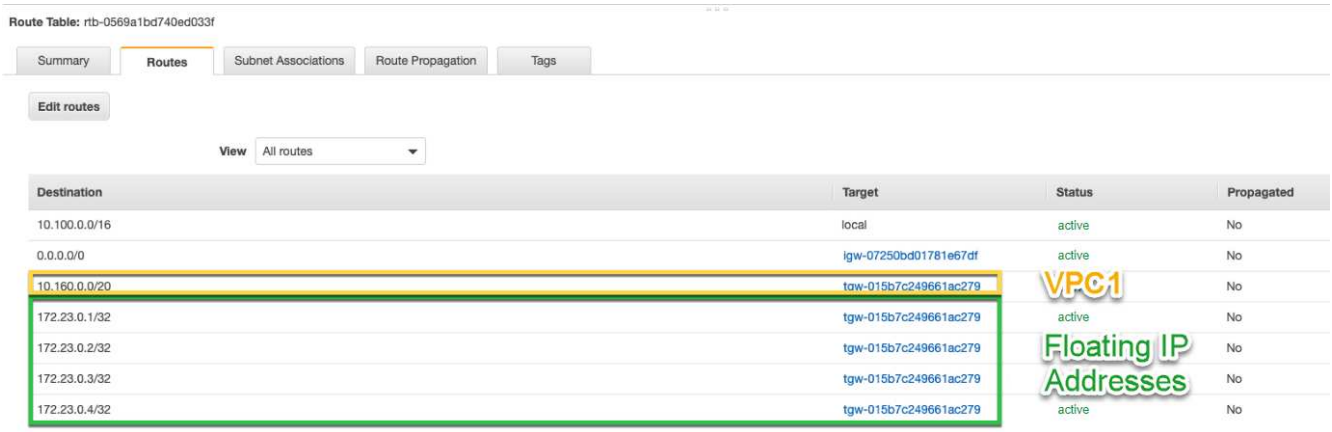
L'exemple d'image suivant montre la table de routage de la passerelle de transit. Il comprend des itinéraires vers les blocs CIDR des deux VPC et quatre adresses IP flottantes utilisées par Cloud Volumes ONTAP.

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.

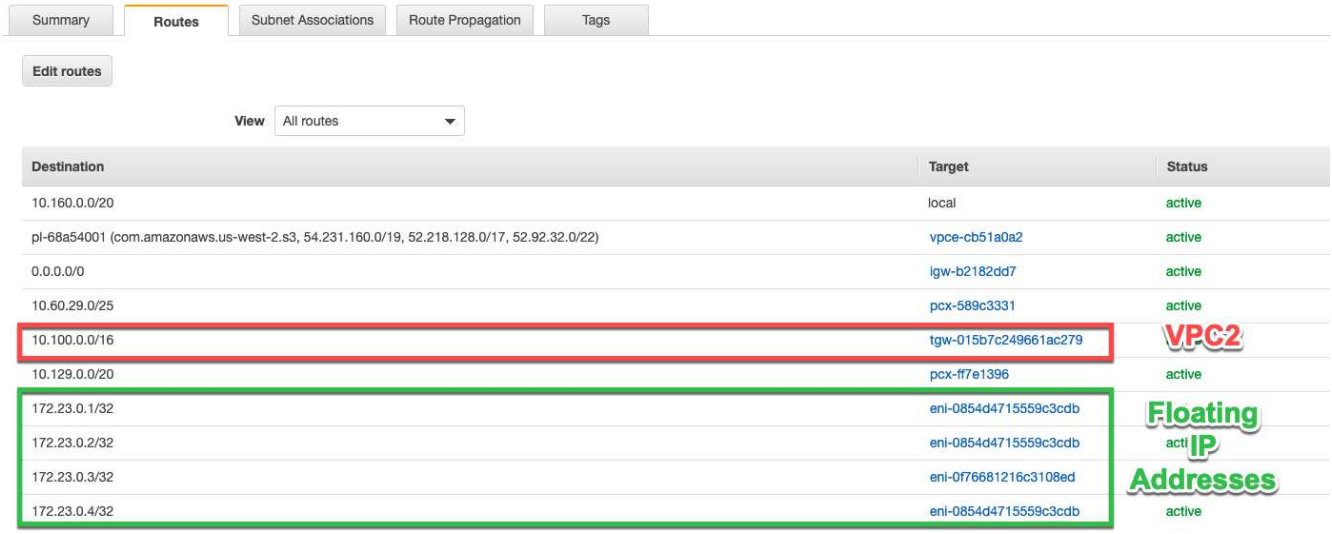
      L'exemple d'image suivant montre la table de routage pour VPC 2, qui inclut les routes vers VPC 1 et les adresses IP flottantes.



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.

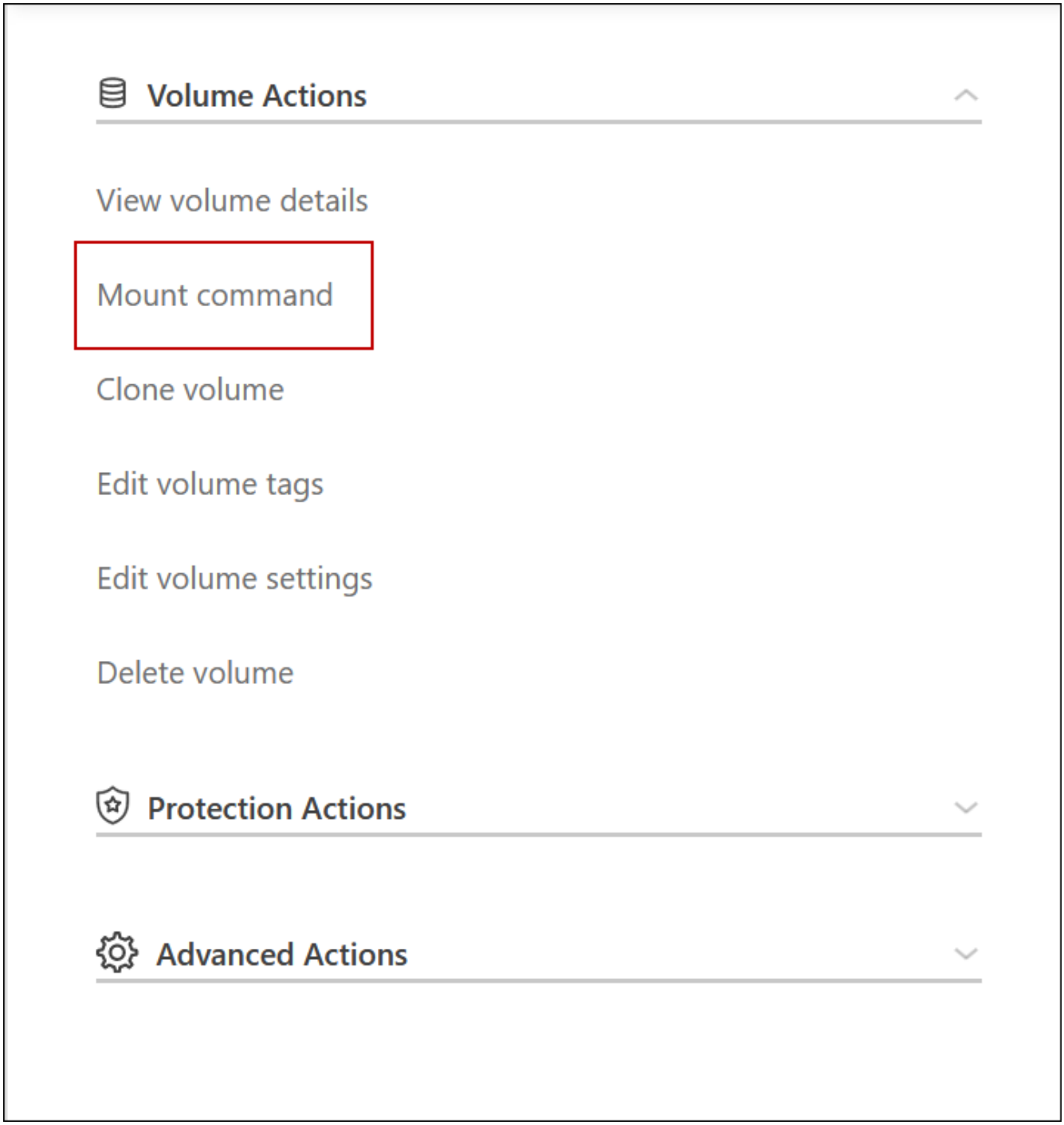
   L'exemple d'image suivant montre la table de routage pour VPC 1. Il comprend un itinéraire vers les adresses IP flottantes et vers le VPC 2, où réside un client. La console a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire HA.



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

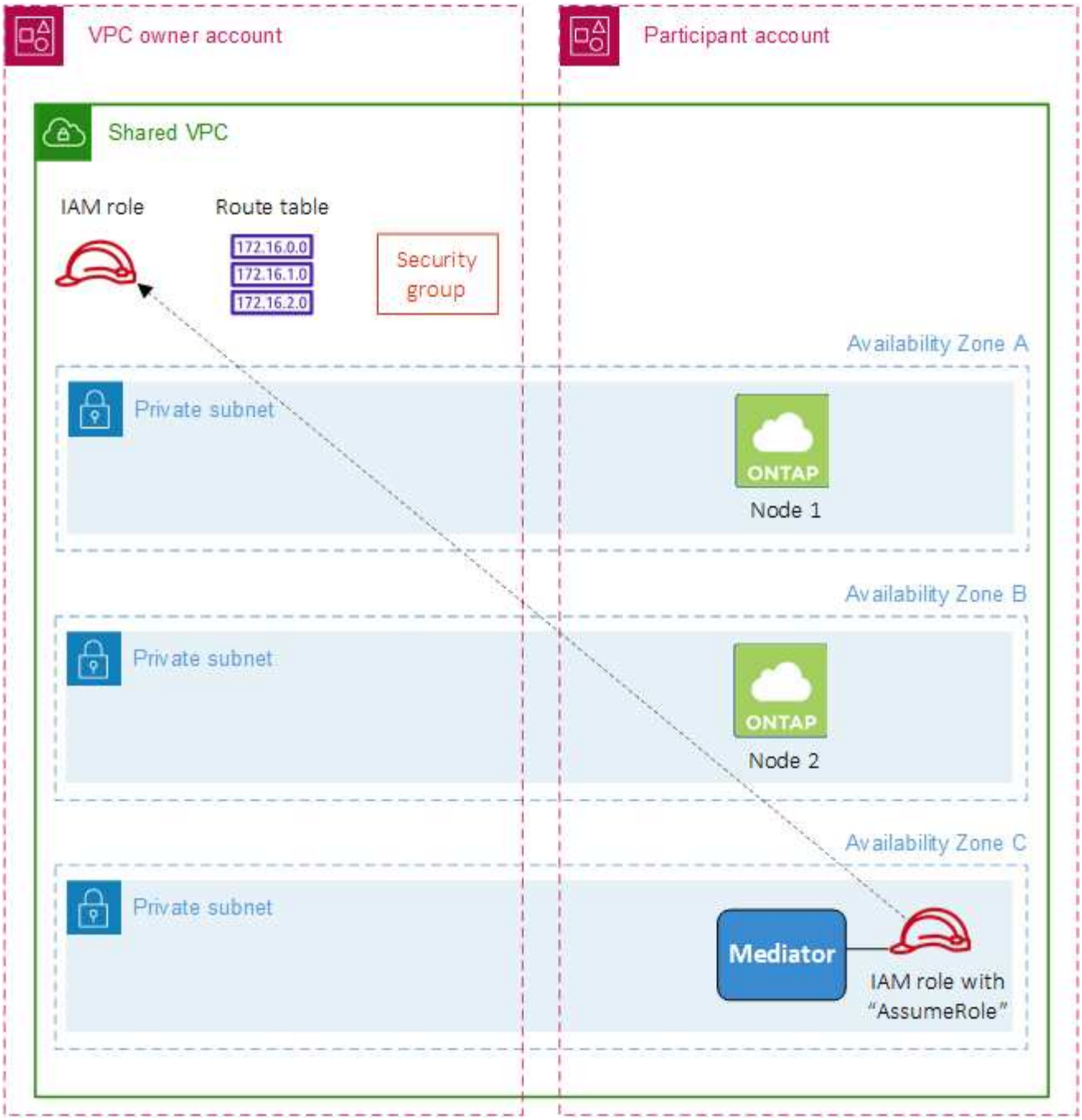
À partir de la version 9.11.1, les paires Cloud Volumes ONTAP HA sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre organisation de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement AWS, puis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

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.