Configurez votre réseau

Cloud Volumes ONTAP

NetApp
December 09, 2022

Table des matières

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

BlueXP (anciennement Cloud Manager) gère la configuration des composants réseau pour Cloud Volumes ONTAP, tels que les adresses IP, les masques réseau et les routes. 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, et bien plus encore.

Exigences générales

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour l'AutoSupport, qui surveille de manière proactive l'état de santé de votre système et envoie des messages au support technique de NetApp.

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

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

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

Si aucune connexion Internet sortante n'est disponible pour envoyer des messages AutoSupport, BlueXP configure automatiquement vos systèmes Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy. La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous avez défini des règles sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Après avoir vérifié que l'accès Internet sortant est disponible, vous pouvez tester AutoSupport pour vous assurer qu'il peut envoyer des messages. Pour obtenir des instructions, reportez-vous à la section "Documentation ONTAP : configuration d'AutoSupport".

Si BlueXP vous informe que les messages AutoSupport ne peuvent pas être envoyés, "Résoudre les problèmes de configuration AutoSupport".

Accès Internet sortant pour le médiateur haute disponibilité

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

L'option manuelle peut être une passerelle NAT ou un terminal VPC d'interface, du sous-réseau cible au

service AWS EC2. Pour plus de détails sur les terminaux VPC, reportez-vous à "Documentation AWS : terminaux VPC d'interface (AWS PrivateLink)".

Adresses IP privées

BlueXP 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.

Le nombre de LIF alloués par BlueXP pour Cloud Volumes ONTAP dépend du déploiement d'un système à un seul nœud ou d'une paire haute disponibilité. Une LIF est une adresse IP associée à un port physique.

Adresses IP d'un système à un seul nœud

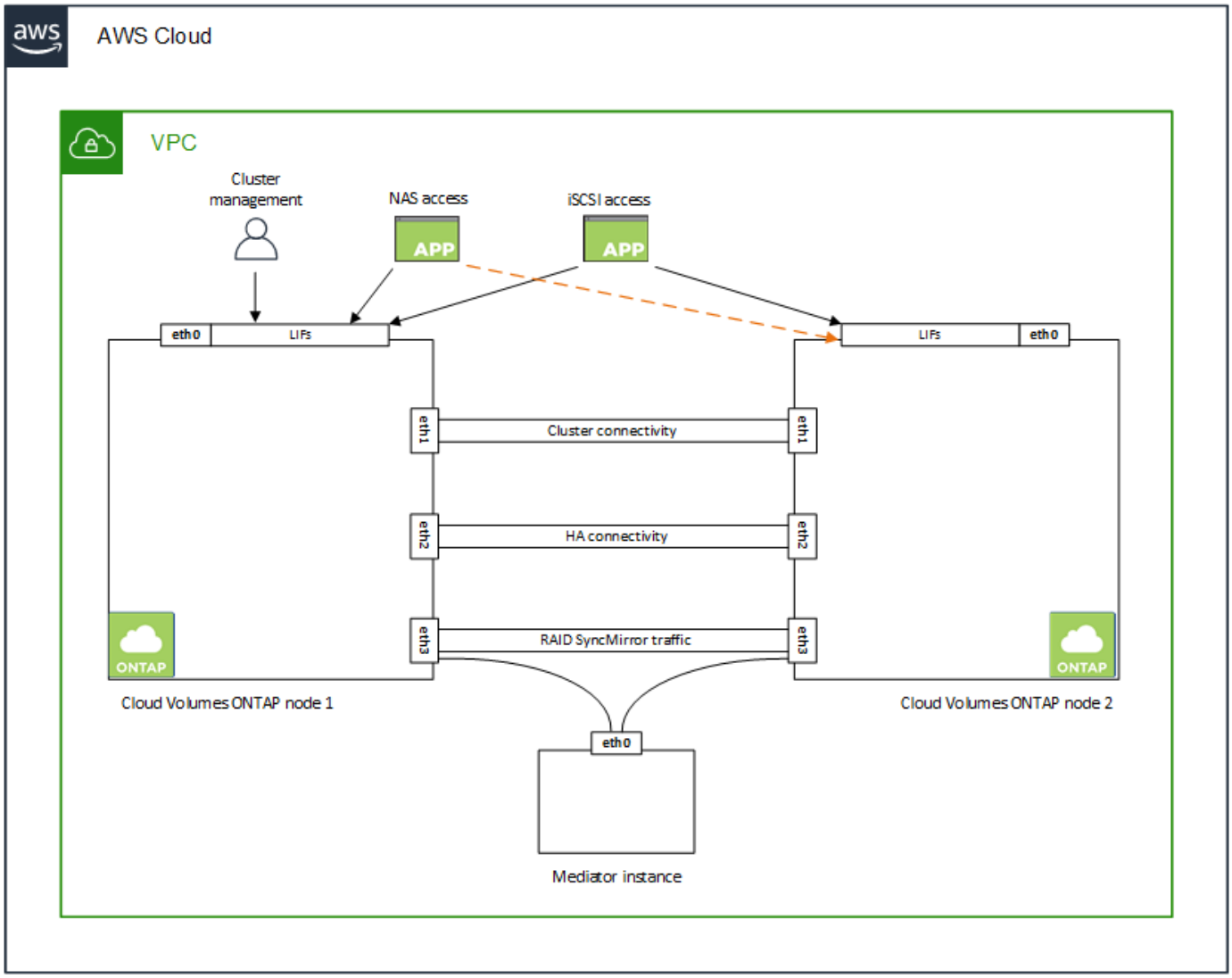
BlueXP alloue 6 adresses IP à un système à nœud unique :

- LIF Cluster-management
- FRV de gestion des nœuds
- FRV InterCluster
- LIF de données NAS
- LIF de données iSCSI
- LIF Storage VM management

  Une LIF de gestion de machines virtuelles de stockage est utilisée avec des outils de gestion tels que SnapCenter.

Adresses IP des paires haute disponibilité

Les paires HAUTE DISPONIBILITÉ requièrent plus d'adresses IP qu'un système à un seul nœud. 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 haute disponibilité dépend du modèle de déploiement choisi. Une paire haute disponibilité déployée dans une *single* AWS Availability zone (AZ) requiert 15 adresses IP privées, tandis qu'une paire haute disponibilité déployée dans *multiple* AZS nécessite 13 adresses IP privées.

Les tableaux suivants fournissent des informations détaillées sur les LIF associées à chaque adresse IP privée.

LIF pour les paires haute disponibilité dans une même zone de disponibilité

LIF	Interface	Nœud	Objectif
Gestion du cluster	eth0	nœud 1	Gestion administrative de l'ensemble du cluster (paire HA).
Gestion de nœuds	eth0	les nœuds 1 et 2	Gestion administrative d'un nœud.
Intercluster	eth0	les nœuds 1 et 2	Communication, sauvegarde et réplication entre les clusters
Données NAS	eth0	nœud 1	Accès client via les protocoles NAS.

LIF	Interface	Nœud	Objectif
Données iSCSI	eth0	les nœuds 1 et 2	Accès client via le protocole iSCSI. Également utilisé par le système pour d'autres flux de travail réseau importants. Ces LIFs sont requises et ne doivent pas être supprimées.
Connectivité au cluster	eth1	les nœuds 1 et 2	Permet aux nœuds de communiquer les uns avec les autres et de déplacer les données au sein du cluster.
Connectivité HAUTE DISPONIBILITÉ	eth2	les nœuds 1 et 2	Communication entre les deux nœuds en cas de basculement.
Trafic iSCSI RSM	eth3	les nœuds 1 et 2	Le trafic iSCSI RAID SyncMirror, ainsi que la communication entre les deux nœuds Cloud Volumes ONTAP et le médiateur.
Médiateur	eth0	Médiateur	Canal de communication entre les nœuds et le médiateur pour faciliter les processus de basculement et de rétablissement du stockage.

LIF pour paires haute disponibilité dans plusieurs systèmes AZS

LIF	Interface	Nœud	Objectif
Gestion de nœuds	eth0	les nœuds 1 et 2	Gestion administrative d'un nœud.
Intercluster	eth0	les nœuds 1 et 2	Communication, sauvegarde et réplication entre les clusters
Données iSCSI	eth0	les nœuds 1 et 2	Accès client via le protocole iSCSI. Cette LIF gère également la migration d'adresses IP flottantes entre les nœuds.
Connectivité au cluster	eth1	les nœuds 1 et 2	Permet aux nœuds de communiquer les uns avec les autres et de déplacer les données au sein du cluster.
Connectivité HAUTE DISPONIBILITÉ	eth2	les nœuds 1 et 2	Communication entre les deux nœuds en cas de basculement.
Trafic iSCSI RSM	eth3	les nœuds 1 et 2	Le trafic iSCSI RAID SyncMirror, ainsi que la communication entre les deux nœuds Cloud Volumes ONTAP et le médiateur.
Médiateur	eth0	Médiateur	Canal de communication entre les nœuds et le médiateur pour faciliter les processus de basculement et de rétablissement du stockage.

Lorsqu'il est déployé dans plusieurs zones de disponibilité, plusieurs LIF sont associées à "Adresses IP flottantes", Qui ne sont pas pris en compte par rapport à la limite IP privée AWS.

Groupes de sécurité

Il n'est pas nécessaire de créer des groupes de sécurité car BlueXP le fait pour vous. Si vous devez utiliser votre propre, reportez-vous à la section "Règles de groupe de sécurité".

Connexion pour le Tiering des données

Si vous souhaitez utiliser EBS comme niveau de performance et AWS S3 comme niveau de capacité, vous devez vous assurer que Cloud Volumes ONTAP est connecté à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d'un terminal de passerelle".

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

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

Connexions aux systèmes ONTAP

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

DNS et Active Directory pour CIFS

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

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

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

Partage de VPC

Depuis la version 9.11.1, les paires haute disponibilité Cloud Volumes ONTAP sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre entreprise 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 haute disponibilité dans un sous-réseau partagé".

Besoins en paires haute disponibilité dans plusieurs AZS

D'autres exigences de mise en réseau AWS s'appliquent aux configurations Cloud Volumes ONTAP HA qui utilisent plusieurs zones de disponibilité (AZS). Vous devez vérifier ces exigences avant de lancer une paire haute disponibilité car vous devez entrer les informations de mise en réseau dans BlueXP lorsque vous créez l'environnement de travail.

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

Zones de disponibilité

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

Un sous-réseau doit être disponible dans chaque zone de disponibilité.

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

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

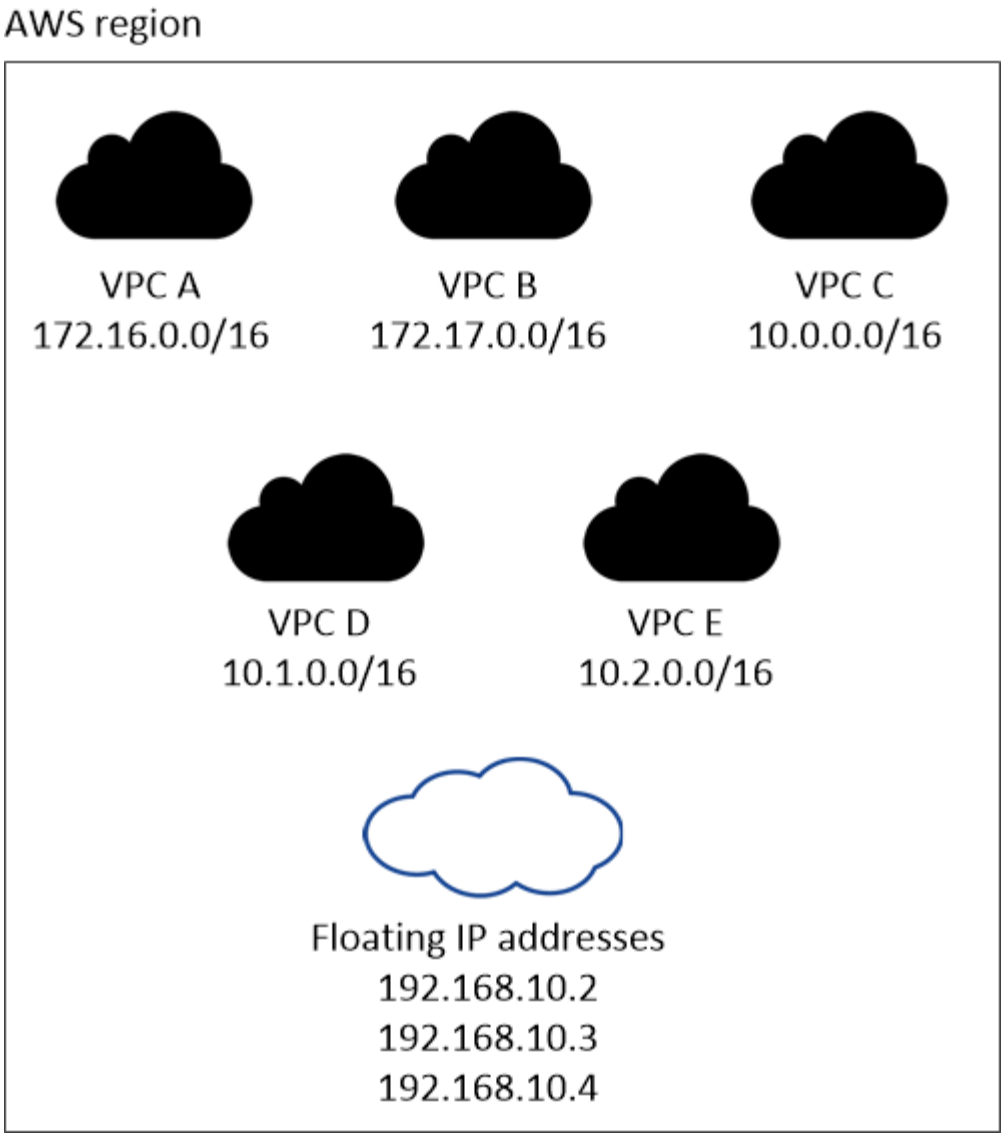
Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud 1 et l'autre les données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante est facultative pour la gestion des SVM.

Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité.

Vous devez entrer les adresses IP flottantes dans BlueXP lorsque vous créez un environnement de travail Cloud Volumes ONTAP HA. BlueXP alloue les adresses IP à la paire HA lors du lancement du système.

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

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



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

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

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

Tables de routage

Après avoir spécifié les adresses IP flottantes dans BlueXP, vous êtes invité à sélectionner les tables de routage qui doivent inclure des routes vers les adresses IP flottantes. Cela permet au client d'accéder à la paire haute disponibilité.

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

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

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

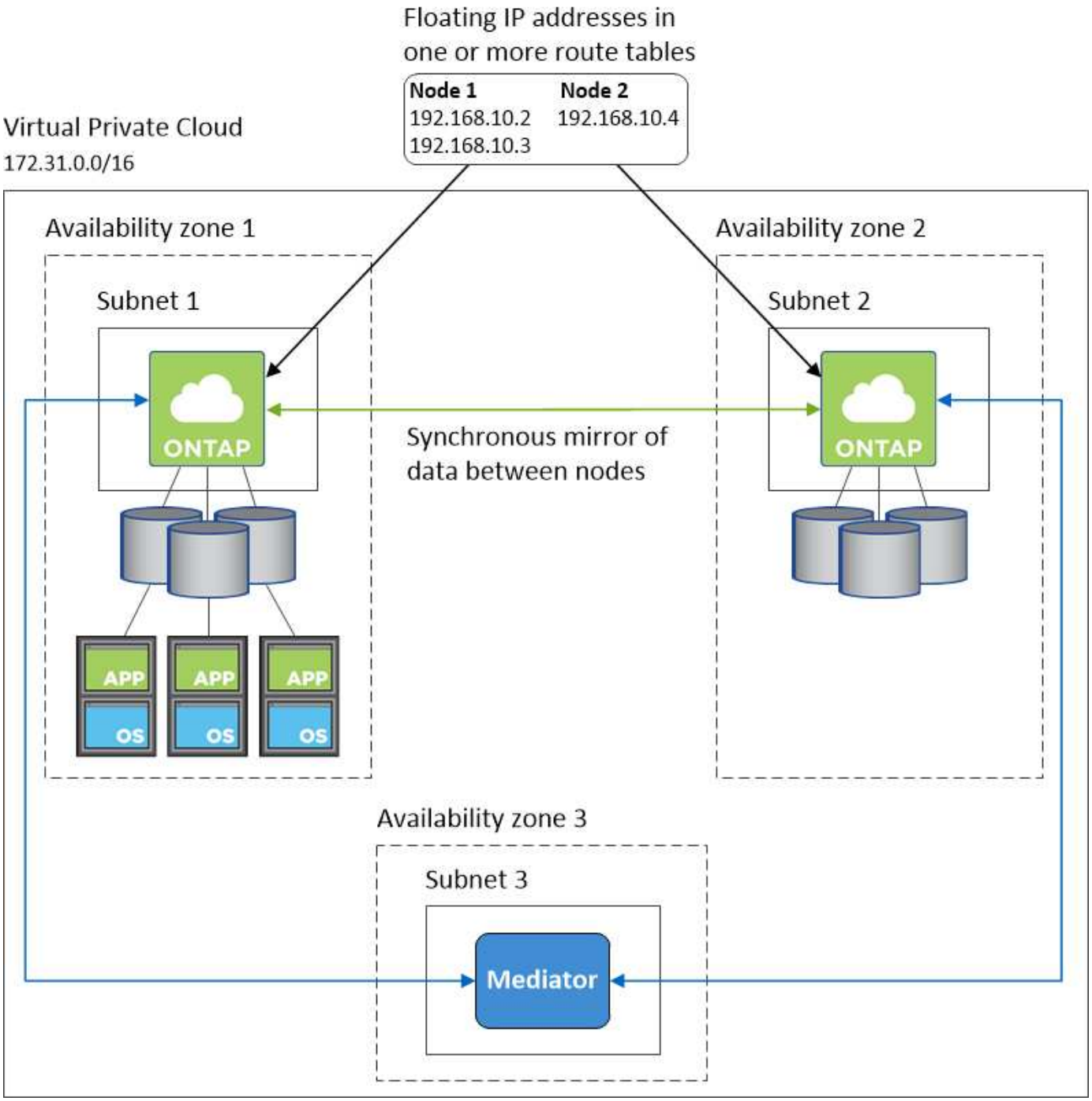
Connexion aux outils de gestion NetApp

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

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

Exemple de configuration haute disponibilité

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



Configuration requise pour le connecteur

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

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

Connexion aux réseaux cibles

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

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

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
https://support.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	Pour fournir des fonctions et des services SaaS dans BlueXP.
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.

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

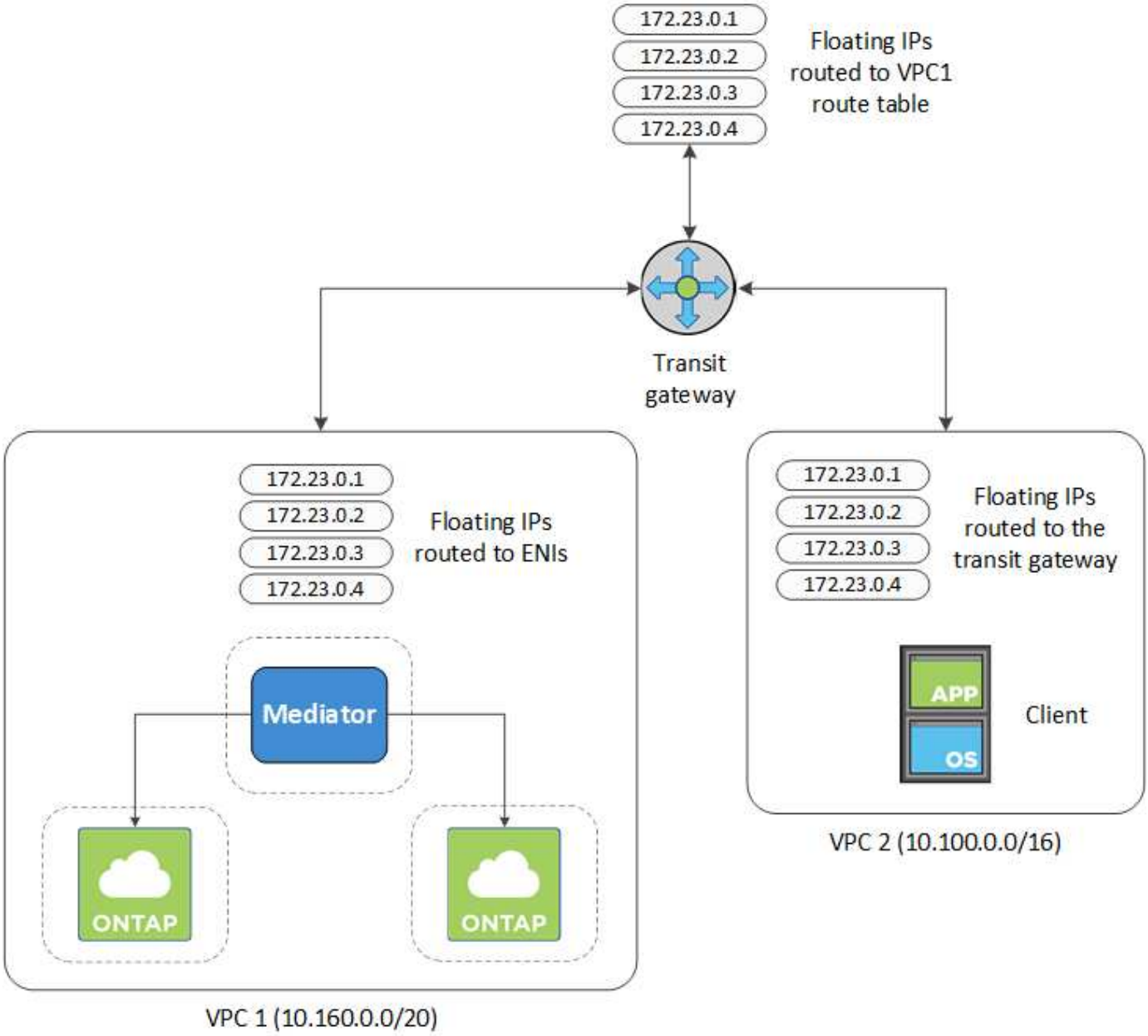
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA "Adresses IP flottantes" Depuis l'extérieur du VPC, où réside la paire HA.

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

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

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

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

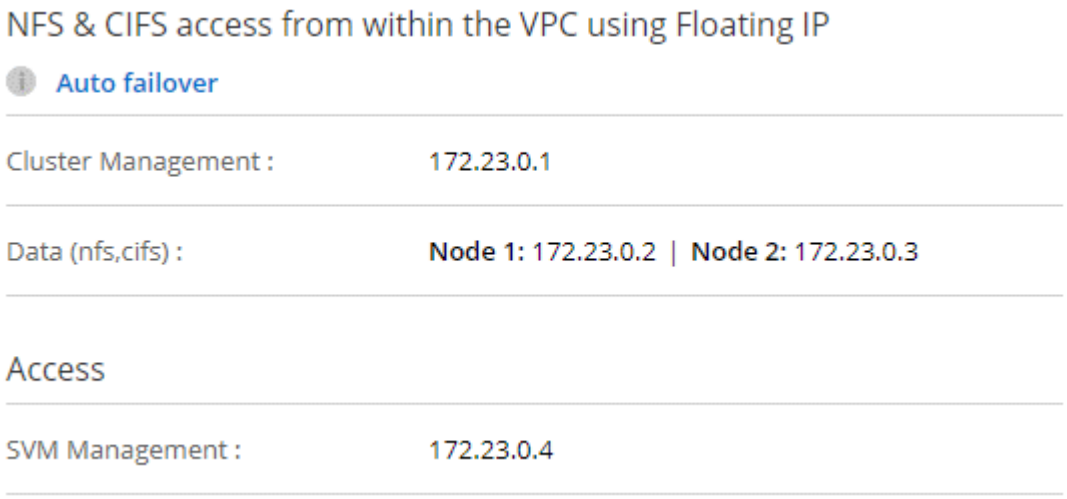


Les étapes suivantes montrent comment configurer une configuration similaire.

Étapes

1. "Créez une passerelle de transit et connectez les VPC à la passerelle".
2. Associez les VPC à la table de routage de la passerelle de transit.
   a. Dans le service **VPC**, cliquez sur **Transit Gateway route tables**.
   b. Sélectionnez la table de routage.
   c. Cliquez sur **associations**, puis sélectionnez **Créer association**.
   d. Choisissez les pièces jointes (les VPC) à associer, puis cliquez sur **Créer une association**.
3. Créer des routes dans la table de routage de la passerelle de transit en spécifiant les adresses IP flottantes de la paire HA.

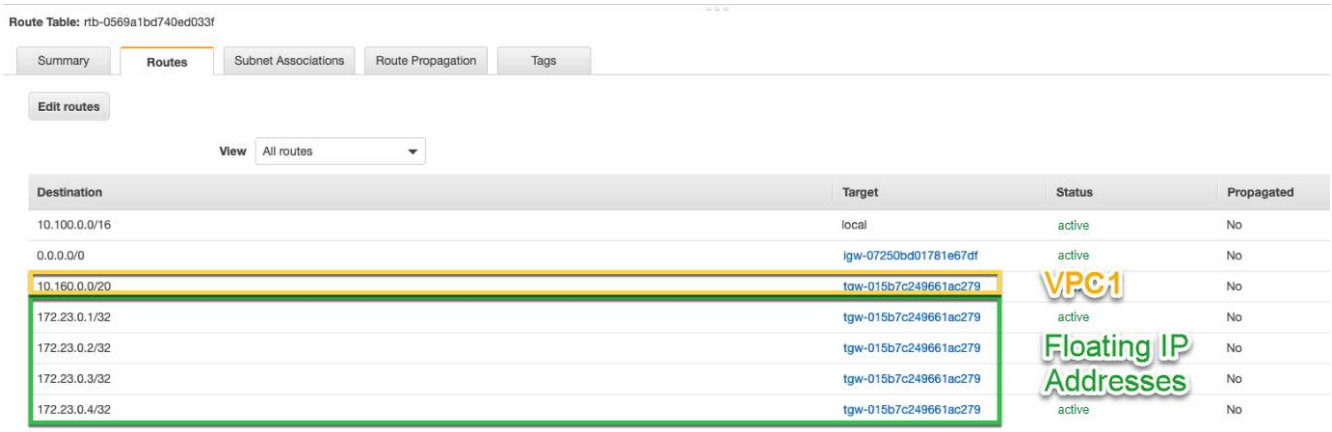
   Vous trouverez les adresses IP flottantes sur la page informations sur l'environnement de travail dans BlueXP. Voici un exemple :



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

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

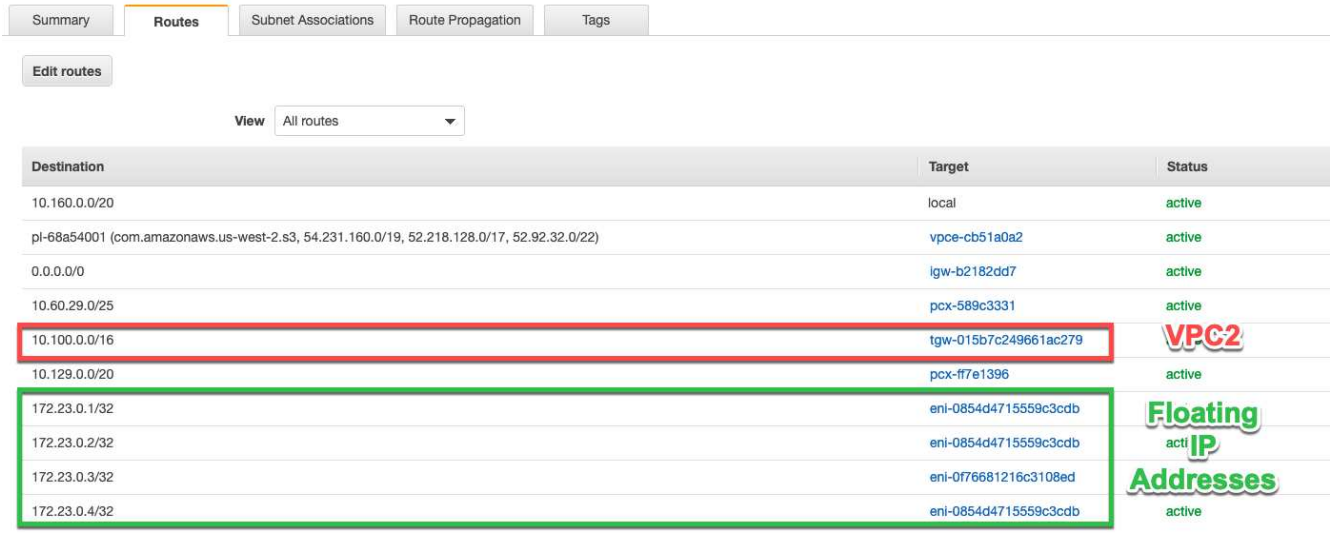
      L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.



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

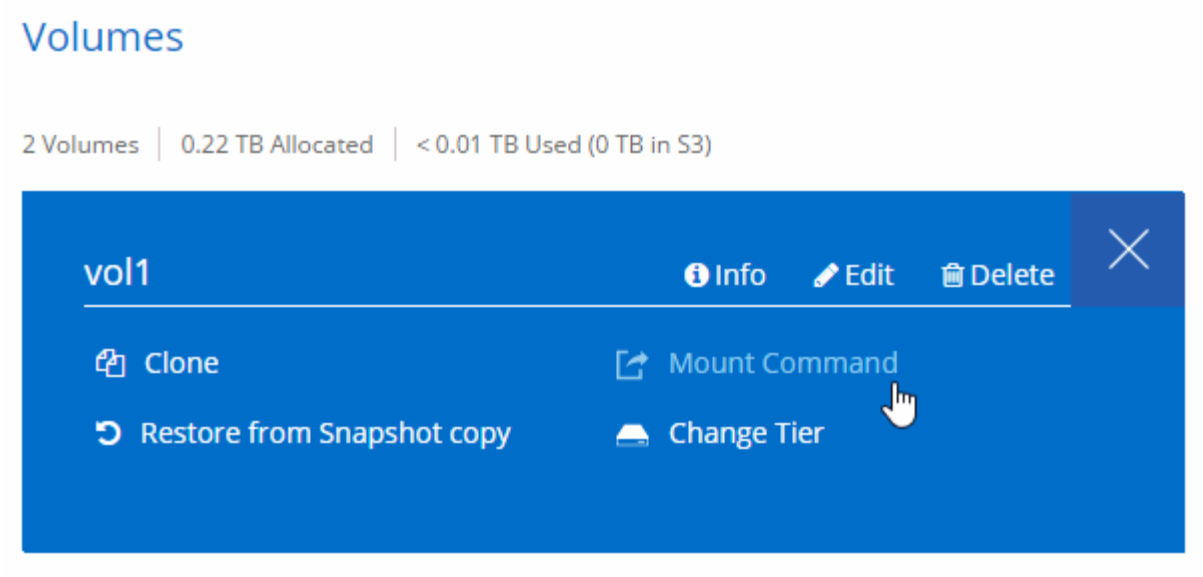
   Cette étape est importante car elle termine le routage entre les VPC.

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



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

   Vous pouvez trouver l'adresse IP correcte dans BlueXP en sélectionnant un volume et en cliquant sur **Mount Command**.



7. Si vous montez un volume NFS, configurez la export policy pour qu'elle corresponde au sous-réseau du VPC client.

   "Découvrez comment modifier un volume".

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

Déploiement d'une paire haute disponibilité dans un sous-réseau partagé

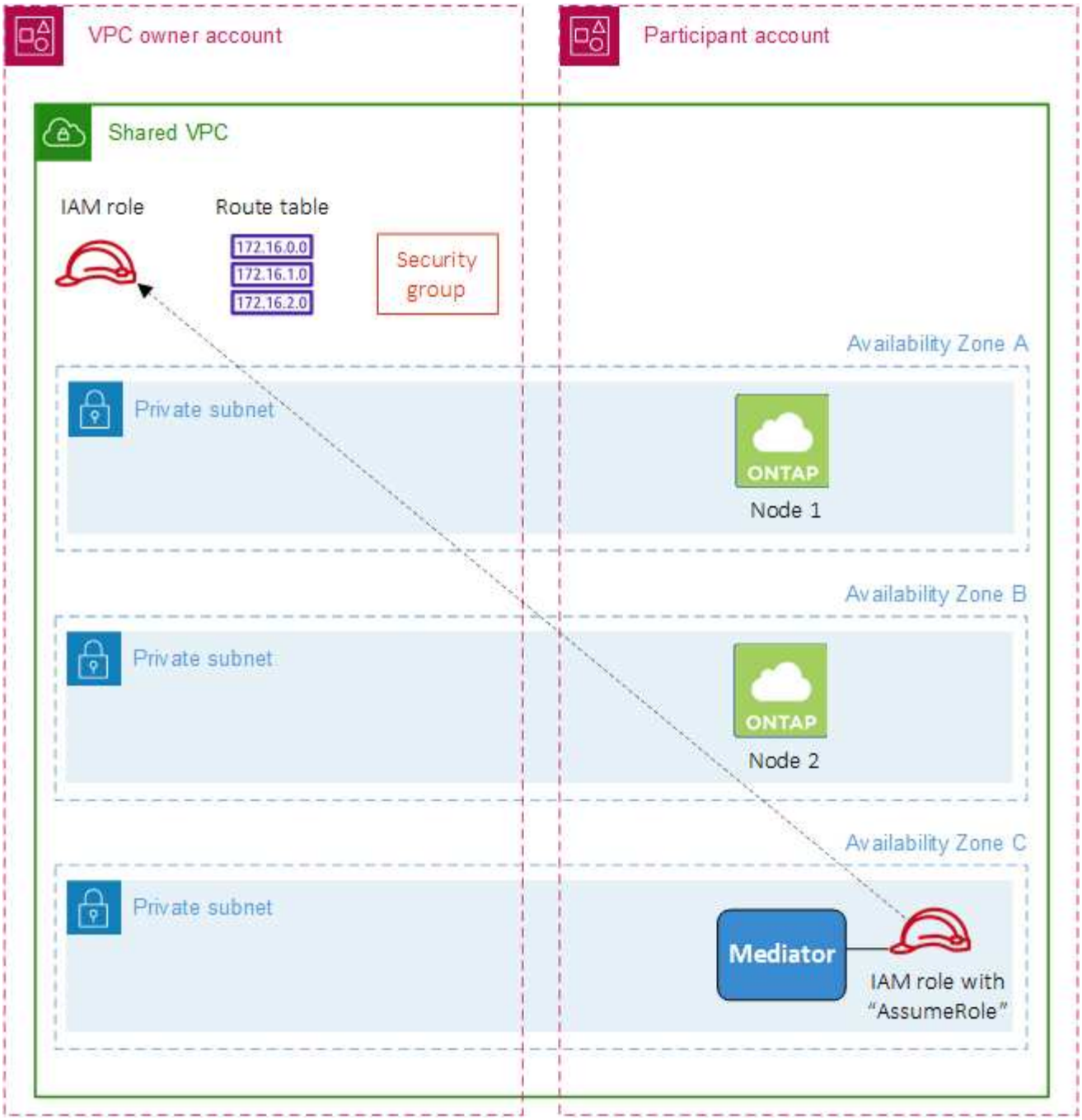
Depuis la version 9.11.1, les paires haute disponibilité Cloud Volumes ONTAP sont prises en charge dans AWS avec le partage VPC. Le partage VPC permet à votre entreprise de partager des sous-réseaux avec d'autres comptes AWS. Pour utiliser cette configuration, vous devez configurer votre environnement AWS, puis déployer la paire HA à l'aide de l'API.

Avec "Partage de VPC", Une configuration Cloud Volumes ONTAP HA est répartie sur deux comptes :

- Le compte propriétaire du VPC, qui détient 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 (incluant 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 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 du participant, puis créer le rôle IAM et le groupe de sécurité dans le compte propriétaire VPC.

Lorsque vous créez l'environnement de travail Cloud Volumes ONTAP, BlueXP crée et attache automatiquement un rôle IAM au médiateur. Il part du rôle IAM que vous avez créé dans le compte propriétaire VPC afin de modifier les tables de routage associées à la paire haute disponibilité.

Étapes

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

   Cette étape est requise pour déployer la paire haute disponibilité dans les sous-réseaux partagés.

   "Documentation AWS : partagez un sous-réseau"

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

   "Voir les règles de groupe de sécurité pour Cloud Volumes ONTAP". Sachez que vous n'avez pas besoin de créer un groupe de sécurité pour le médiateur HA. BlueXP le fait pour vous.

3. Dans le compte propriétaire 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 BlueXP pour créer un nouvel environnement de travail 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 VPC (voir 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 VPC (voir l'étape 3 ci-dessus).

     Par exemple :

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

   +
   "Découvrez l'API Cloud Volumes ONTAP"

Règles de groupe de sécurité pour AWS

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

Règles pour Cloud Volumes ONTAP

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

Règles entrantes

Lorsque vous créez un environnement de travail 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-réseau du VPC pour le système Cloud Volumes ONTAP et la plage de sous-réseau du VPC où réside le connecteur. Il s'agit de l'option recommandée.
- **Tous les VPC** : la source du trafic entrant est la plage IP 0.0.0.0/0.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Connectivité avec le connecteur et l'accès HTTPS à la console Web System Manager via l'adresse IP du LIF de cluster management
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 de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS

Protocole	Port	Objectif
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)

Service	Protocole	Port	Source	Destination	Objectif
AutoSupport	HTTPS	443	FRV de gestion des nœuds	support.netapp.com	AutoSupport (HTTPS est le protocole par défaut)
	HTTP	80	FRV de gestion des nœuds	support.netapp.com	AutoSupport (uniquement si le protocole de transport est passé de HTTPS à HTTP)
	TCP	3128	FRV de gestion des nœuds	Connecteur	Envoi de messages AutoSupport via un serveur proxy sur le connecteur, si aucune connexion Internet sortante n'est disponible
Sauvegarde vers S3	TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP

Service	Protocole	Port	Source	Destination	Objectif
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

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

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

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

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

Règles du groupe de sécurité interne de la configuration haute disponibilité

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

BlueXP crée toujours ce groupe de sécurité. Vous n'avez pas la possibilité d'utiliser vos propres ressources.

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

Règles de sortie

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

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

Règles pour le connecteur

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

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers l'interface utilisateur locale et les connexions à partir de Cloud Data SENSE
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Protocole	Port	Objectif
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement du connecteur.

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers AWS et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	ONTAP HA médiateur	Communication avec le médiateur ONTAP HA
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

Service	Protocole	Port	Destination	Objectif
Sens des données cloud	HTTP	80	Instance Cloud Data Sense	Des solutions clouds adaptées à Cloud Volumes ONTAP