



Configurez votre réseau

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

- Configurez votre réseau 1
 - Configuration réseau requise pour Cloud Volumes ONTAP dans AWS 1
 - Configuration d'une passerelle de transit AWS pour les paires HA dans plusieurs AZS 8
 - Règles de groupe de sécurité pour AWS 12

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

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

Conditions générales requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

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

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

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

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

["Découvrez comment configurer AutoSupport"](#).

Accès Internet sortant pour le médiateur haute disponibilité

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

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

Nombre d'adresses IP

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

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

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



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

Groupes de sécurité

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

Connexion de Cloud Volumes ONTAP à AWS S3 pour le hiérarchisation des données

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

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

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

Connexions aux systèmes ONTAP dans d'autres réseaux

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

DNS et Active Directory pour CIFS

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

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

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

Besoins en paires haute disponibilité dans plusieurs AZS

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

Pour comprendre le fonctionnement des paires haute disponibilité, voir "[Paires haute disponibilité](#)".

Zones de disponibilité

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

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

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

Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud

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



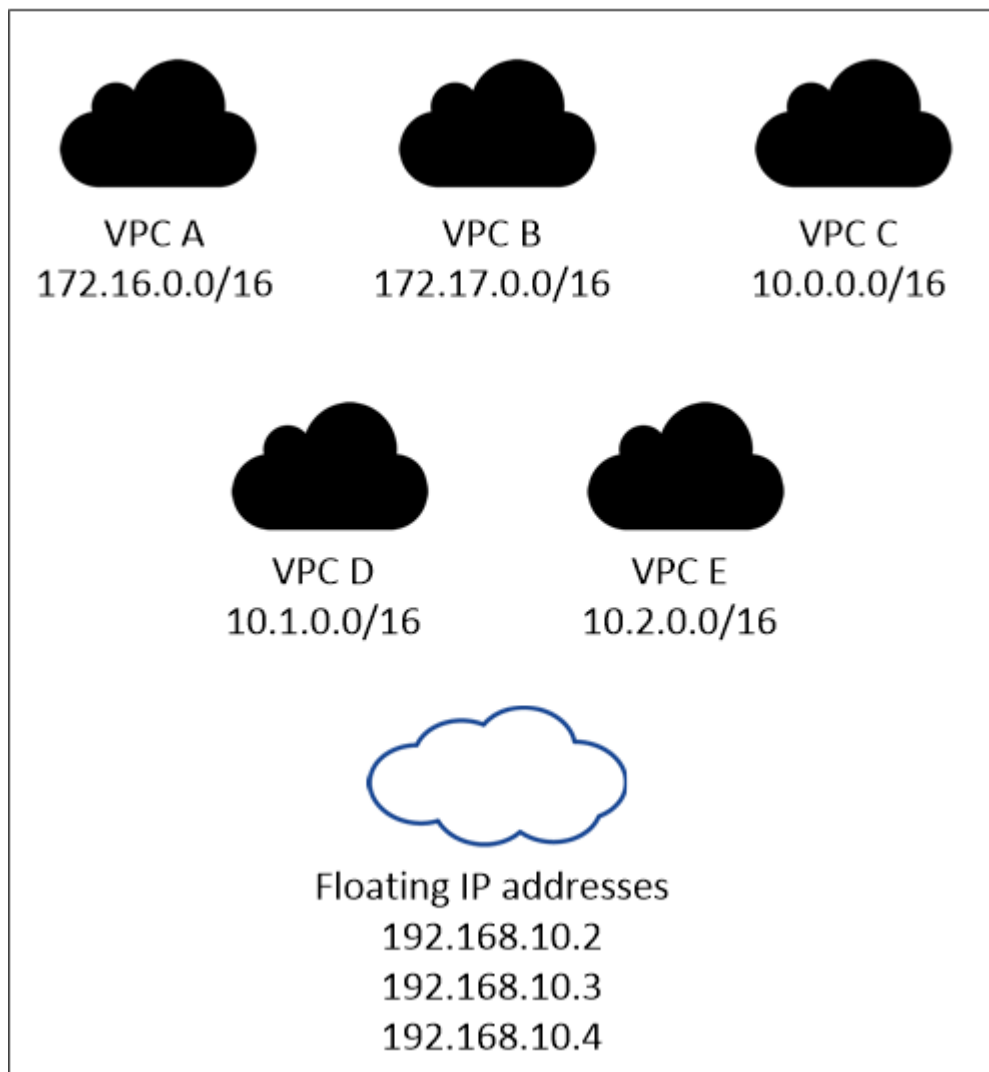
Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité. Si vous ne spécifiez pas l'adresse IP lors du déploiement du système, vous pouvez créer la LIF plus tard. Pour plus de détails, voir "[Configuration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

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

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

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

AWS region





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

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

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

Tables de routage

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

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

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

Pour plus d'informations sur les tables de routage, voir ["Documentation AWS : tables de routage"](#).

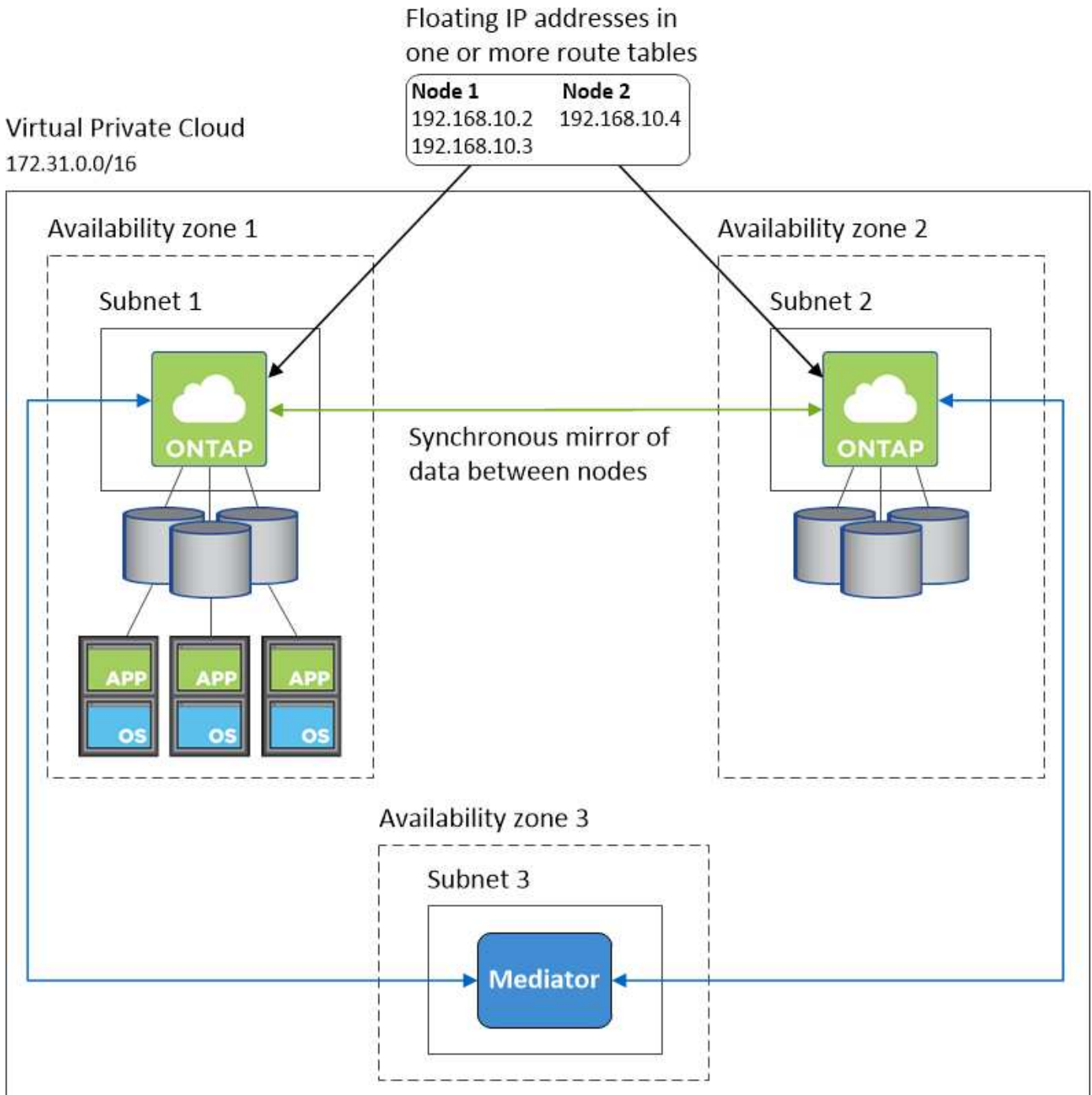
Connexion aux outils de gestion NetApp

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

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

Exemple de configuration haute disponibilité

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



Configuration requise pour le connecteur

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



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

Connexion aux réseaux cibles

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

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

Accès Internet sortant

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

| Terminaux | Objectif |
|---|---|
| Services AWS (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Cloud de calcul élastique (EC2)• Service de gestion des clés (KMS)• Service de jetons de sécurité (STS)• Service de stockage simple (S3) Le noeud final exact dépend de la région dans laquelle vous déployez Cloud Volumes ONTAP. "Reportez-vous à la documentation AWS pour plus de détails." | Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans AWS. |
| https://api.services.cloud.netapp.com:443 | Demandes d'API à NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Permet d'accéder aux images logicielles, aux manifestes et aux modèles. |
| https://repo.cloud.support.netapp.com | Permet de télécharger les dépendances de Cloud Manager. |
| http://repo.mysql.com/ | Utilisé pour télécharger MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger. |
| https://cloudmanagerinfraprod.azurecr.io | Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournies une solution pour les intégrations des services avec Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com | Permet à NetApp de diffuser des données à partir d'enregistrements d'audit. |
| https://cloudmanager.cloud.netapp.com | Communication avec le service Cloud Manager, notamment les comptes Cloud Central. |

| Terminaux | Objectif |
|--|---|
| https://netapp-cloud-account.auth0.com | Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs. |
| https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist | Permet d'ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3. |
| https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup | Communication avec NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Communication avec NetApp pour les licences système et l'inscription au support. |
| https://ipa-signer.cloudmanager.netapp.com | Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident. |
| Divers sites tiers, par exemple : <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Les emplacements tiers sont sujets à modification.</p> | Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces. |

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

| Terminaux | Objectif |
|---|---|
| L'hôte du connecteur | <p data-bbox="719 157 1485 226">Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager.</p> <p data-bbox="719 258 1448 359">En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte :</p> <ul data-bbox="743 394 1463 541" style="list-style-type: none"> <li data-bbox="743 394 1463 457">• Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel <li data-bbox="743 478 1463 541">• Un IP public fonctionne dans tous les scénarios de mise en réseau <p data-bbox="719 577 1485 709">Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.</p> |
| https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com | <p data-bbox="719 762 1485 867">Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.</p> |
| https://widget.intercom.io | <p data-bbox="719 888 1433 951">Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.</p> |

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

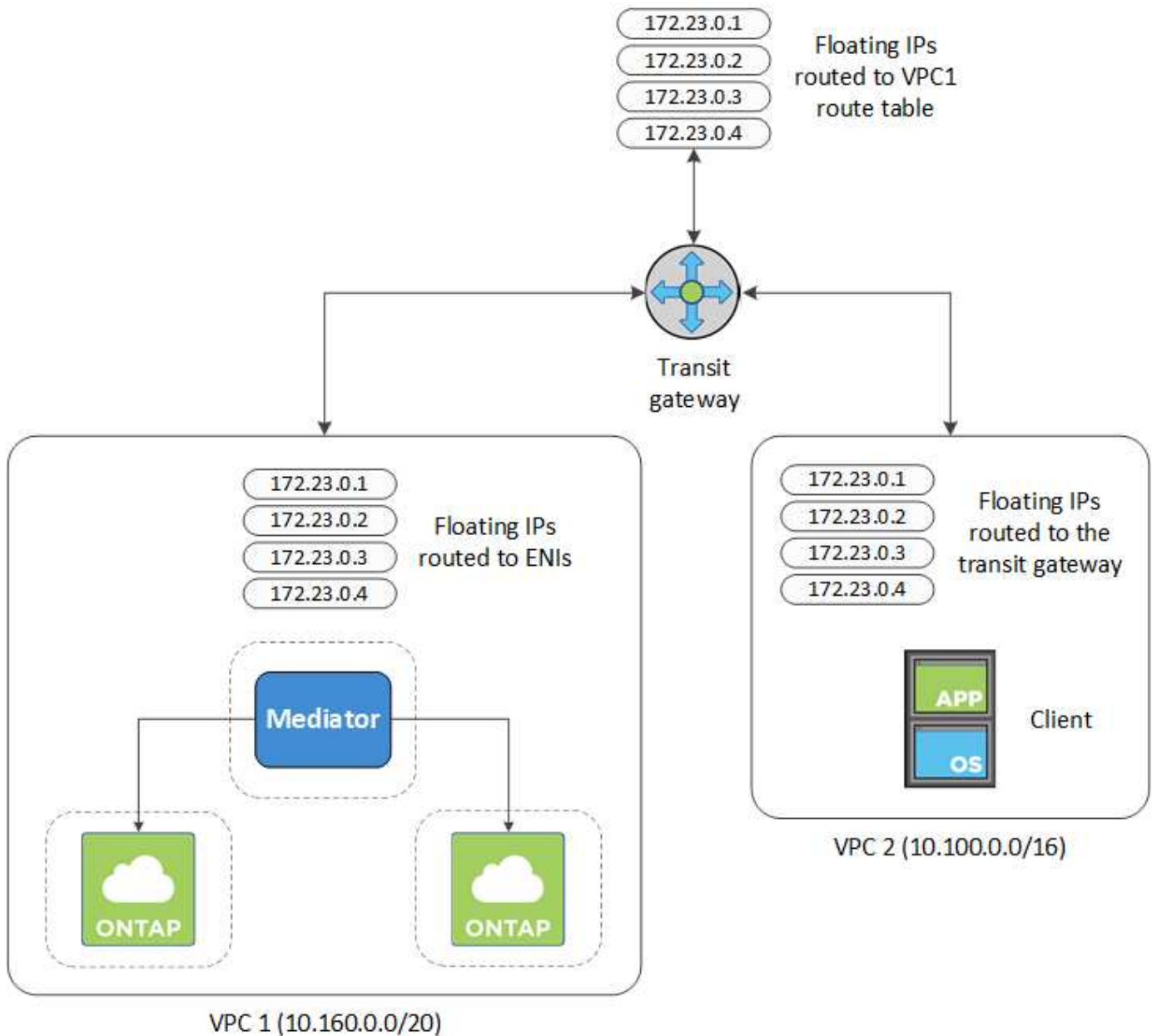
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA "[Adresses IP flottantes](#)" Depuis l'extérieur du VPC, où réside la paire HA.

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

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

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

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.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

| CIDR | Attachment | Resource type | Route type | Route state |
|---------------|--|---------------|------------|-------------|
| 10.100.0.0/16 | tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1 | VPC2 | propagated | active |
| 10.160.0.0/20 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC1 | propagated | active |
| 172.23.0.1/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC | static | active |
| 172.23.0.2/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC | static | active |
| 172.23.0.3/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC | static | active |
| 172.23.0.4/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC | static | active |

Floating IP Addresses

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

- a. Ajoutez des entrées de route aux adresses IP flottantes.
- b. Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

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

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status | Propagated |
|---------------|-----------------------|--------|------------|
| 10.100.0.0/16 | local | active | No |
| 0.0.0.0/0 | igw-07250bd01781e67df | active | No |
| 10.160.0.0/20 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.1/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.2/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.3/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.4/32 | tgw-015b7c249661ac279 | active | No |

VPC1
Floating IP Addresses

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

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

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

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status |
|---|-----------------------|--------|
| 10.160.0.0/20 | local | active |
| pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22) | vpce-cb51a0a2 | active |
| 0.0.0.0/0 | igw-b2182dd7 | active |
| 10.60.29.0/25 | pcx-589c3331 | active |
| 10.100.0.0/16 | tgw-015b7c249661ac279 | active |
| 10.129.0.0/20 | pcx-ff7e1396 | active |
| 172.23.0.1/32 | eni-0854d4715559c3cdb | active |
| 172.23.0.2/32 | eni-0854d4715559c3cdb | active |
| 172.23.0.3/32 | eni-0f76681216c3108ed | active |
| 172.23.0.4/32 | eni-0854d4715559c3cdb | active |

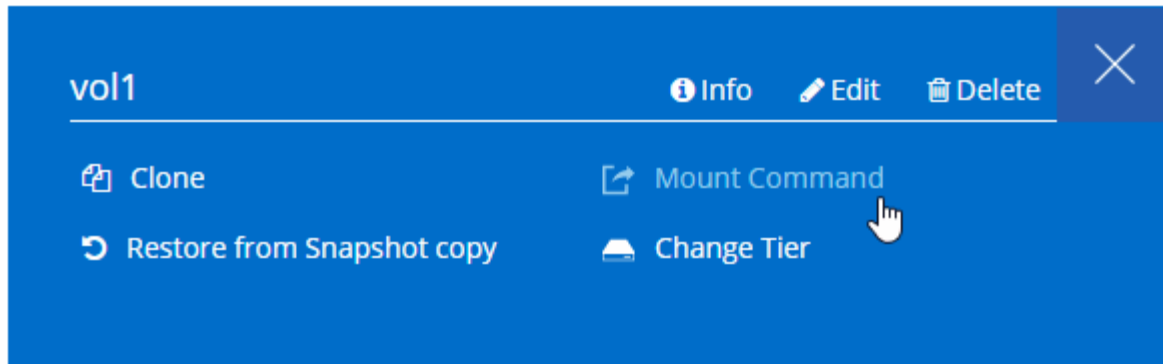
VPC2
Floating act IP Addresses

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

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

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



- Liens connexes*
- ["Paires haute disponibilité dans AWS"](#)
- ["Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"](#)

Règles de groupe de sécurité pour AWS

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

Règles pour Cloud Volumes ONTAP

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

Règles entrantes

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

| Protocole | Port | Objectif |
|--------------------------|------|---|
| Tous les protocoles ICMP | Tout | Envoi d'une requête ping à l'instance |
| HTTP | 80 | Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster |
| HTTPS | 443 | Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster |
| SSH | 22 | Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud |
| TCP | 111 | Appel de procédure à distance pour NFS |

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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



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

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

| Service | Protocole | Port | Source | Destination | Objectif |
|------------|----------------|----------------|--|--|--|
| Cluster | Tout le trafic | Tout le trafic | Tous les LIF sur un nœud | Tous les LIF de l'autre nœud | Communications InterCluster (Cloud Volumes ONTAP HA uniquement) |
| | TCP | 3000 | FRV de gestion des nœuds | Ha médiateur | Appels ZAPI (Cloud Volumes ONTAP HA uniquement) |
| | ICMP | 1 | FRV de gestion des nœuds | Ha médiateur | Rester en vie (Cloud Volumes ONTAP HA uniquement) |
| DHCP | UDP | 68 | FRV de gestion des nœuds | DHCP | Client DHCP pour la première configuration |
| DHCPS | UDP | 67 | FRV de gestion des nœuds | DHCP | Serveur DHCP |
| DNS | UDP | 53 | FRV de gestion des nœuds et FRV de données (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 1860-18699 | FRV de gestion des nœuds | Serveurs de destination | Copie NDMP |
| SMTP | TCP | 25 | FRV de gestion des nœuds | Serveur de messagerie | Les alertes SMTP peuvent être utilisées pour AutoSupport |
| SNMP | TCP | 161 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | UDP | 161 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | TCP | 162 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| | UDP | 162 | FRV de gestion des nœuds | Serveur de surveillance | Surveillance par des interruptions SNMP |
| SnapMirror | TCP | 11104 | FRV InterCluster | Baies de stockage inter-clusters ONTAP | Gestion des sessions de communication intercluster pour SnapMirror |
| | TCP | 11105 | FRV InterCluster | Baies de stockage inter-clusters ONTAP | Transfert de données SnapMirror |
| Syslog | UDP | 514 | FRV de gestion des nœuds | Serveur Syslog | Messages de transfert syslog |

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

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

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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



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

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

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

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

Règles de sortie

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

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

Règles pour le connecteur

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

Règles entrantes

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

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour

ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



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

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

| Service | Protocole | Port | Destination | Objectif |
|------------------|------------------|-------------|---------------------------|---|
| Conformité cloud | HTTP | 80 | Instance Cloud Compliance | Cloud Compliance pour Cloud Volumes ONTAP |

Informations sur le copyright

Copyright © 2024 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 DÉLICTEUELLE (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.