



# **Administration d'Azure**

## **Cloud Volumes ONTAP**

NetApp  
June 11, 2024

# Sommaire

- Administration d'Azure ..... 1
  - Modifier le type de machine virtuelle Azure pour Cloud Volumes ONTAP ..... 1
  - Remplacement des verrouillages CIFS pour les paires haute disponibilité Cloud Volumes ONTAP dans Azure ..... 2
  - Utilisez une liaison privée Azure ou des terminaux de service ..... 3
  - Déplacement de groupes de ressources ..... 7
  - Isolez le trafic SnapMirror dans Azure ..... 7

# Administration d'Azure

## Modifier le type de machine virtuelle Azure pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs types de machines virtuelles lorsque vous lancez Cloud Volumes ONTAP dans Microsoft Azure. Vous pouvez modifier à tout moment le type de machine virtuelle si vous déterminez qu'elle est sous-dimensionnée ou trop dimensionnée pour répondre à vos besoins.

### Description de la tâche

- Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

["Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"](#)

- La modification du type de machine virtuelle peut affecter les frais de service Microsoft Azure.
- L'opération redémarre Cloud Volumes ONTAP.

Pour les systèmes à nœud unique, les E/S sont interrompues.

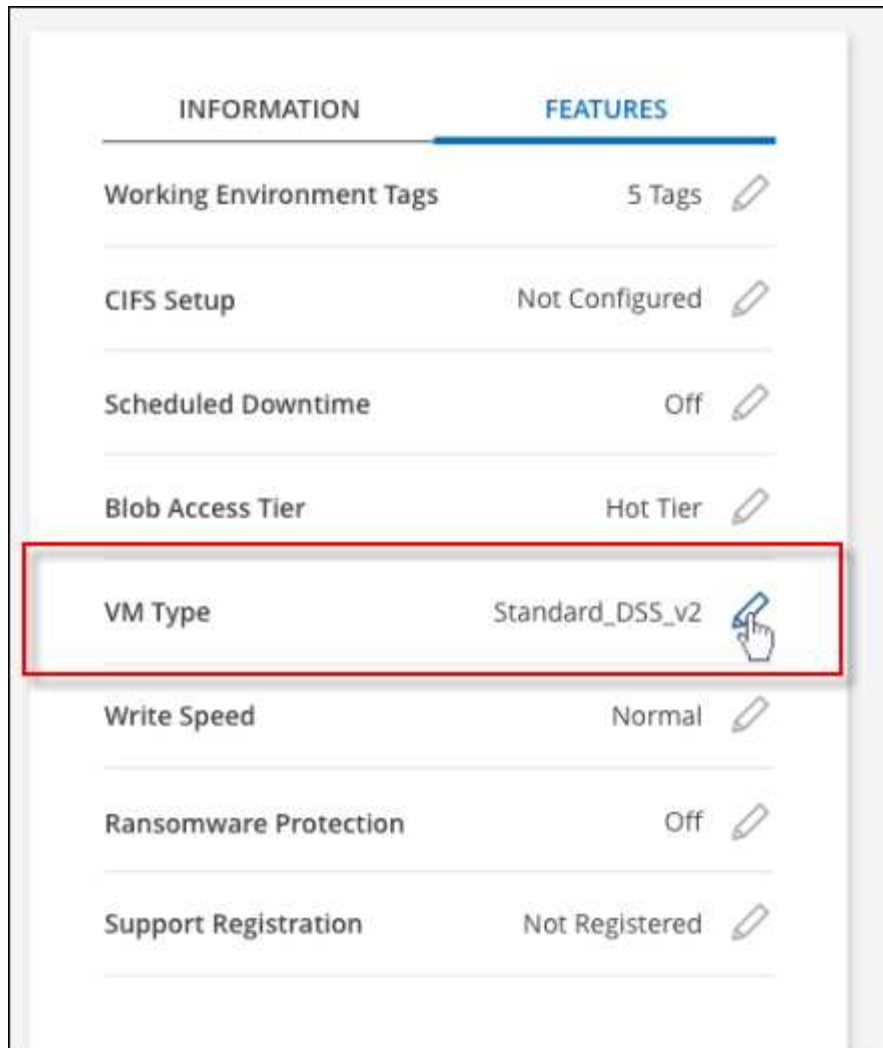
Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.



BlueXP change aisément un nœud à la fois en lançant le basculement et en attente de retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers pendant ce processus et n'a rencontré aucun problème côté client. Au fur et à mesure des changements de connexion, nous avons constaté des tentatives d'E/S au niveau des E/S, mais la couche applicative a pu faire face à ces courtes « connexions » NFS/CIFS.

### Étapes

1. Sur la page Canevas, sélectionnez l'environnement de travail.
2. Dans l'onglet vue d'ensemble, cliquez sur le panneau fonctionnalités, puis cliquez sur l'icône en forme de crayon en regard de **VM type**.



a. Si vous utilisez une licence PAYGO basée sur des nœuds, vous pouvez choisir une autre licence et un autre type de machine virtuelle en cliquant sur l'icône en forme de crayon en regard de **Type de licence**.

3. Sélectionnez un type de VM, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **Modifier**.

#### Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

## Remplacement des verrouillages CIFS pour les paires haute disponibilité Cloud Volumes ONTAP dans Azure

L'administrateur du compte peut activer un paramètre dans BlueXP qui empêche tout problème lié au rétablissement du stockage Cloud Volumes ONTAP lors des événements de maintenance Azure. Lorsque vous activez ce paramètre, Cloud Volumes ONTAP vetoes les verrous CIFS et réinitialise les sessions CIFS actives.

#### Description de la tâche

Microsoft Azure planifie des événements de maintenance périodiques sur ses machines virtuelles. Lorsqu'un événement de maintenance se produit sur une paire haute disponibilité Cloud Volumes ONTAP, la paire haute

disponibilité déclenche le basculement du stockage. Si des sessions CIFS sont actives au cours de cet événement de maintenance, les verrous sur les fichiers CIFS peuvent empêcher tout rétablissement du stockage.

Si vous activez ce paramètre, Cloud Volumes ONTAP veto aux verrous et réinitialise les sessions CIFS actives. Par conséquent, la paire haute disponibilité peut terminer le rétablissement du stockage lors de ces événements de maintenance.



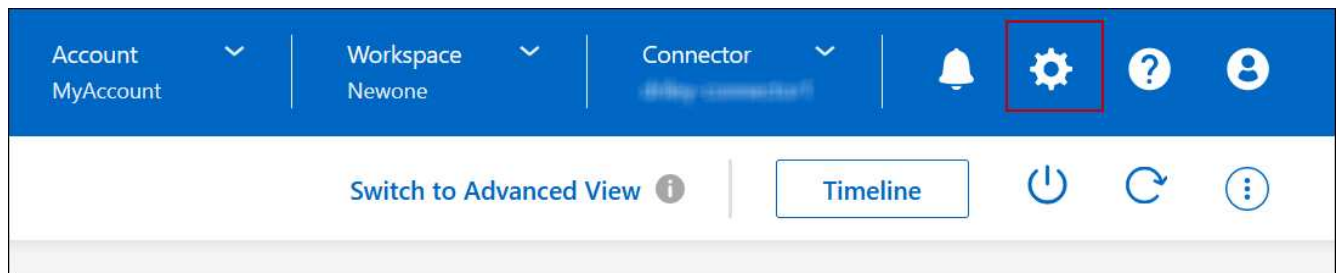
Ce processus peut entraîner des perturbations pour les clients CIFS. Les données qui ne sont pas validées auprès des clients CIFS pourraient être perdues.

### Ce dont vous avez besoin

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "[Découvrez comment](#)".

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres Cloud Volumes ONTAP**.



2. Sous **Azure**, cliquez sur **verrous CIFS Azure pour les environnements de travail Azure HA**.
3. Cochez la case pour activer la fonctionnalité, puis cliquez sur **Enregistrer**.

## Utilisez une liaison privée Azure ou des terminaux de service

Cloud Volumes ONTAP utilise une liaison privée Azure pour les connexions aux comptes de stockage associés. Si nécessaire, vous pouvez désactiver les liens privés Azure et utiliser les terminaux de service.

### Présentation

Par défaut, BlueXP active une liaison privée Azure pour les connexions entre Cloud Volumes ONTAP et ses comptes de stockage associés. Azure Private Link sécurise les connexions entre les terminaux dans Azure et offre les avantages en termes de performances.

Si nécessaire, vous pouvez configurer Cloud Volumes ONTAP de sorte qu'il utilise des terminaux de service au lieu d'une liaison privée Azure.

Dans les deux cas, BlueXP limite toujours l'accès réseau pour les connexions entre Cloud Volumes ONTAP et les comptes de stockage. L'accès au réseau est limité au vnet sur lequel Cloud Volumes ONTAP est déployé et au vnet sur lequel le connecteur est déployé.

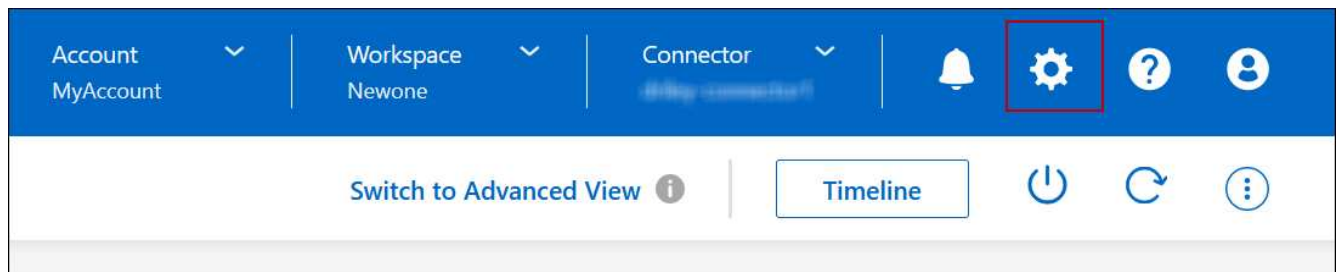
## Désactivez les liens privés Azure et utilisez plutôt les terminaux de service

Si votre entreprise le requiert, vous pouvez modifier un paramètre dans BlueXP afin qu'il configure Cloud Volumes ONTAP pour qu'il utilise des points de terminaison de service au lieu d'un lien privé Azure. La modification de ce paramètre s'applique aux nouveaux systèmes Cloud Volumes ONTAP que vous créez. Les terminaux de service ne sont pris en charge que dans "[Paires de régions Azure](#)" Entre le connecteur et les Cloud Volumes ONTAP VNets.

Le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère ou dans "[Paire de régions Azure](#)" Pour les systèmes Cloud Volumes ONTAP.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres Cloud Volumes ONTAP**.



2. Sous **Azure**, cliquez sur **Use Azure Private Link**.
3. Désélectionnez **connexion de liaison privée entre Cloud Volumes ONTAP et les comptes de stockage**.
4. Cliquez sur **Enregistrer**.

### Une fois que vous avez terminé

Si vous avez désactivé les liens privés Azure et que le connecteur utilise un serveur proxy, vous devez activer le trafic API direct.

["Découvrez comment activer le trafic API direct sur le connecteur"](#)

## Utilisation des liens privés Azure

Dans la plupart des cas, aucune action n'est nécessaire pour configurer des liens privés Azure avec Cloud Volumes ONTAP. BlueXP gère des liens privés Azure pour vous. Mais si vous utilisez une zone Azure Private DNS existante, vous devez modifier un fichier de configuration.

### Condition requise pour les DNS personnalisés

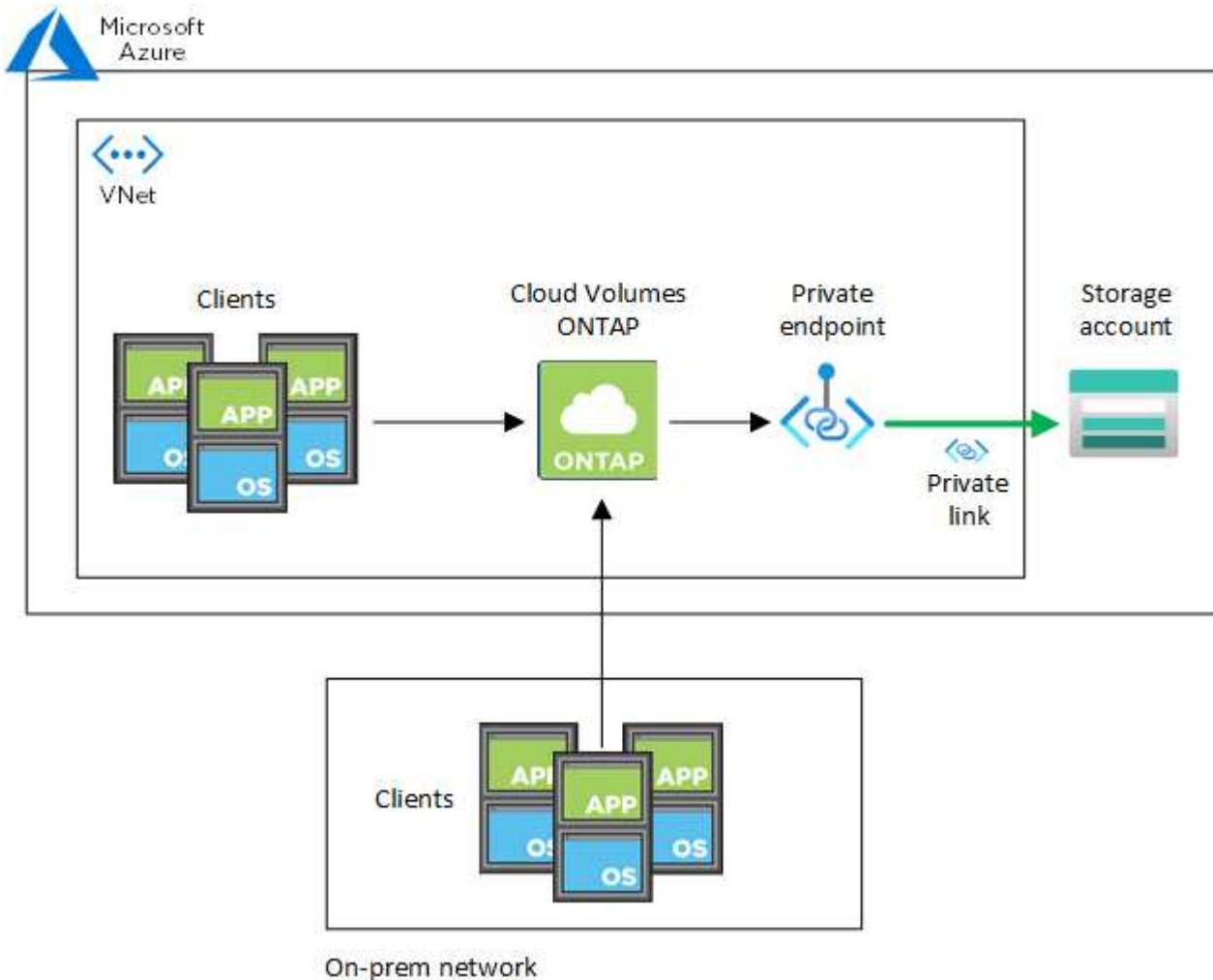
Si vous utilisez un DNS personnalisé, vous devez également créer un transitaire conditionnel vers la zone DNS privée Azure à partir de vos serveurs DNS personnalisés. Pour en savoir plus, reportez-vous à la section "[La documentation d'Azure sur l'utilisation d'un transitaire DNS](#)".

### Fonctionnement des connexions Private Link

Lorsque BlueXP déploie Cloud Volumes ONTAP dans Azure, il crée un noeud final privé dans le groupe de ressources. Le terminal privé est associé aux comptes de stockage pour Cloud Volumes ONTAP. Par conséquent, l'accès au stockage Cloud Volumes ONTAP transite par le réseau de backbone Microsoft.

L'accès client passe par la liaison privée lorsque les clients se trouvent dans le même VNet que Cloud Volumes ONTAP, dans les VNets périmétriques ou dans votre réseau sur site lors de l'utilisation d'une connexion VPN ou ExpressRoute privée au VNet.

Voici un exemple illustrant l'accès des clients par liaison privée à partir d'un même réseau vnet et d'un réseau sur site doté d'une connexion VPN ou ExpressRoute privée.



Si le connecteur et les systèmes Cloud Volumes ONTAP sont déployés dans différents VNets, vous devez configurer le peering de vnet entre le vnet où le connecteur est déployé et le vnet où les systèmes Cloud Volumes ONTAP sont déployés.

### Fournissez BlueXP avec des informations détaillées sur votre DNS privé Azure

Si vous utilisez "DNS privé Azure", Vous devez ensuite modifier un fichier de configuration sur chaque connecteur. Sinon, BlueXP ne peut pas activer la connexion Azure Private Link entre Cloud Volumes ONTAP et les comptes de stockage associés.

Notez que le nom DNS doit correspondre aux exigences de nommage des DNS Azure "Comme illustré dans la documentation Azure".

### Étapes

1. SSH vers l'hôte du connecteur et connectez-vous.

2. Accédez au répertoire suivant : `/opt/application/netapp/cloudManager/docker_ocm/data`
3. Modifiez APP.conf en ajoutant le paramètre "User-private-dns-zone-settings" avec les paires de valeur-mot-clé suivantes :

```
"user-private-dns-zone-settings" : {  
  "resource-group" : "<resource group name of the DNS zone>",  
  "subscription" : "<subscription ID>",  
  "use-existing" : true,  
  "create-private-dns-zone-link" : true  
}
```

Le paramètre doit être entré au même niveau que « system-ID » comme indiqué ci-dessous :

```
"system-id" : "<system ID>",  
"user-private-dns-zone-settings" : {
```

Notez que le mot-clé d'abonnement n'est requis que si la zone DNS privée existe dans un abonnement différent de celui du connecteur.

4. Enregistrez le fichier et déconnectez le connecteur.

Aucun redémarrage n'est requis.

### Activer la restauration en cas d'échec

Si BlueXP ne parvient pas à créer un lien privé Azure dans le cadre d'actions spécifiques, il termine l'action sans la connexion Azure Private Link. Cela peut se produire lors de la création d'un environnement de travail (nœud unique ou paire HA), ou lors des actions suivantes sur une paire HA : création d'un agrégat, ajout de disques à un agrégat existant ou création d'un nouveau compte de stockage lorsque l'on dépasse les 32 Tio.

Vous pouvez modifier ce comportement par défaut en activant la restauration si BlueXP ne parvient pas à créer Azure Private Link. Cela permet de vous assurer que vous êtes en parfaite conformité avec les réglementations de sécurité de votre entreprise.

Si vous activez la restauration, BlueXP arrête l'action et annule toutes les ressources créées dans le cadre de l'action.

Vous pouvez activer le retour arrière via l'API ou en mettant à jour le fichier APP.conf.

### Activer le retour arrière via l'API

#### Étape

1. Utilisez le PUT `/occm/config` Appel d'API avec le corps de demande suivant :

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

### Activer le retour arrière en mettant à jour app.conf



## Étapes

1. SSH vers l'hôte du connecteur et connectez-vous.
2. Accédez au répertoire suivant : `/opt/application/netapp/cloudManager/docker_ocm/data`
3. Modifiez APP.conf en ajoutant le paramètre et la valeur suivants :

```
"rollback-on-private-link-failure": true  
. Enregistrez le fichier et déconnectez le connecteur.
```

Aucun redémarrage n'est requis.

## Déplacement de groupes de ressources

Cloud Volumes ONTAP prend en charge les déplacements des groupes de ressources Azure, mais le workflow se produit uniquement dans la console Azure.

Vous pouvez déplacer un environnement de travail d'un groupe de ressources vers un autre groupe de ressources dans Azure au sein du même abonnement Azure. Le déplacement de groupes de ressources entre différents abonnements Azure n'est pas pris en charge.

### Étapes

1. Supprimez l'environnement de travail de **Canvas**.

Pour savoir comment supprimer un environnement de travail, voir ["Suppression des environnements de travail Cloud Volumes ONTAP"](#).

2. Exécutez le déplacement du groupe de ressources dans la console Azure.

Pour terminer le déplacement, reportez-vous à la section ["Déplacez des ressources vers un nouveau groupe de ressources ou un nouvel abonnement dans la documentation de Microsoft Azure"](#).

3. Dans **Canvas**, découvrez l'environnement de travail.
4. Recherchez le nouveau groupe de ressources dans les informations relatives à l'environnement de travail.

### Résultat

L'environnement de travail et ses ressources (machines virtuelles, disques, comptes de stockage, interfaces réseau, snapshots) font partie du nouveau groupe de ressources.

## Isolez le trafic SnapMirror dans Azure

Avec Cloud Volumes ONTAP dans Azure, vous pouvez isoler le trafic de réplication SnapMirror du trafic de données et du trafic de gestion. Pour isoler le trafic de réplication SnapMirror de votre trafic de données, vous allez ajouter une nouvelle carte d'interface réseau (NIC), une LIF intercluster associée et un sous-réseau non routable.

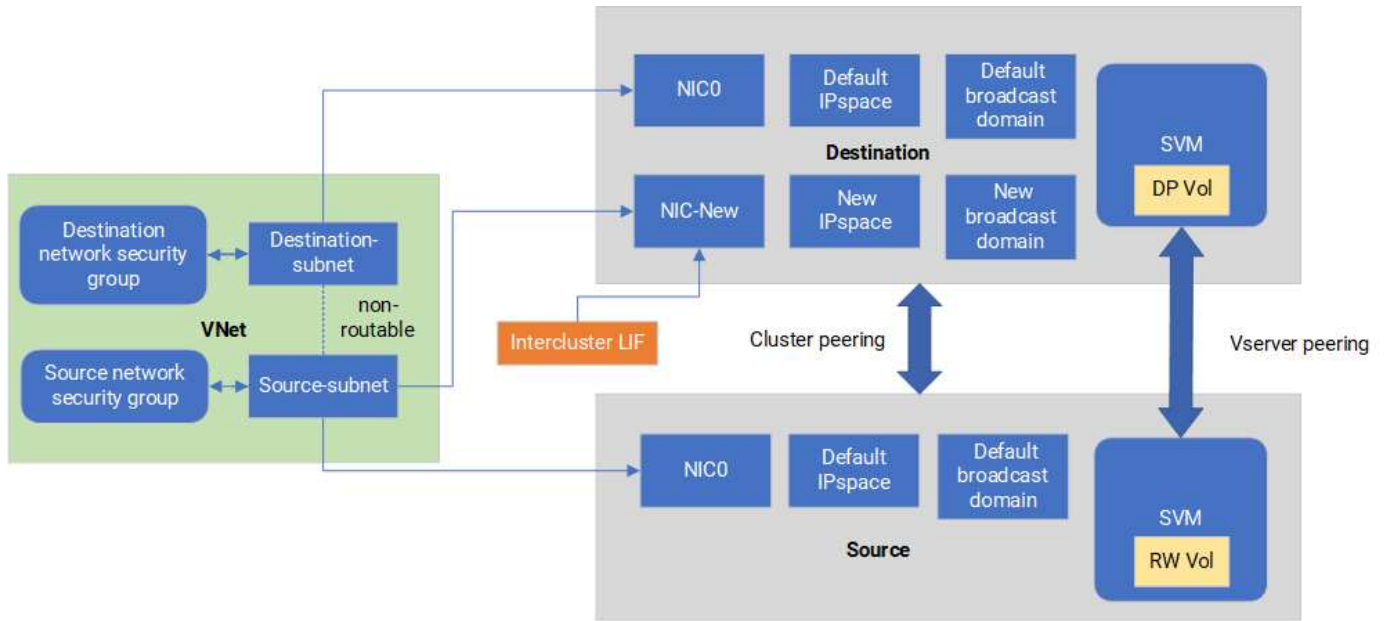
### À propos de la ségrégation du trafic SnapMirror dans Azure

Par défaut, BlueXP configure toutes les cartes réseau et LIF d'un déploiement Cloud Volumes ONTAP sur le

même sous-réseau. Dans de telles configurations, le trafic de réplication SnapMirror et le trafic de données et de gestion utilisent le même sous-réseau. La ségrégation du trafic SnapMirror exploite un sous-réseau supplémentaire qui n'est pas routable vers le sous-réseau existant utilisé pour le trafic de données et de gestion.

**Figure 1**

Les diagrammes suivants illustrent la ségrégation du trafic de réplication SnapMirror avec une carte réseau supplémentaire, une LIF intercluster associée et un sous-réseau non routable dans un déploiement à un seul nœud. Un déploiement de paires haute disponibilité diffère légèrement.



### Avant de commencer

Consultez les considérations suivantes :

- Vous ne pouvez ajouter qu'une seule carte réseau à un seul nœud Cloud Volumes ONTAP ou à un déploiement par paire haute disponibilité (instance de machine virtuelle) pour la ségrégation du trafic SnapMirror.
- Pour ajouter une nouvelle carte réseau, le type d'instance de machine virtuelle que vous déployez doit avoir une carte réseau inutilisée.
- Les clusters source et cible doivent avoir accès au même réseau virtuel (vnet). Le cluster de destination est un système Cloud Volumes ONTAP dans Azure. Le cluster source peut être un système Cloud Volumes ONTAP dans Azure ou un système ONTAP.

## Étape 1 : créez une carte réseau supplémentaire et connectez-la à la machine virtuelle de destination

Cette section fournit des instructions sur la création d'une carte réseau supplémentaire et sa connexion à la machine virtuelle de destination. La machine virtuelle de destination est le système à un seul nœud ou paire haute disponibilité dans Cloud Volumes ONTAP Azure où vous souhaitez configurer votre carte réseau supplémentaire.

### Étapes

1. Dans l'interface de ligne de commandes de ONTAP, arrêtez le nœud.

```
dest::> halt -node <dest_node-vm>
```

2. Sur le portail Azure, vérifier que l'état de la machine virtuelle (nœud) est arrêté.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>  
--query instanceView.statuses[1].displayStatus
```

3. Utilisez l'environnement de hachage dans Azure Cloud Shell pour arrêter le nœud.

- a. Arrêtez le nœud.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

- b. Désallouer le nœud.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-  
vm>
```

4. Configurez les règles du groupe de sécurité réseau de manière à ce que les deux sous-réseaux (sous-réseau de cluster source et sous-réseau de cluster de destination) ne soient pas routables les uns par rapport aux autres.

- a. Créez la nouvelle carte réseau sur la machine virtuelle de destination.
- b. Recherchez l'ID de sous-réseau du sous-réseau du cluster source.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet  
-name <vnet> --query id
```

- c. Créez la nouvelle carte réseau sur la machine virtuelle de destination avec l'ID de sous-réseau du sous-réseau de cluster source. Entrez ici le nom de la nouvelle carte réseau.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>  
--subnet <id_from_prev_command> --accelerated-networking true
```

- d. Enregistrez l'adresse IP privée. Cette adresse IP, <new\_added\_nic\_primary\_addr>, est utilisée pour créer une LIF intercluster dans [Broadcast domain, LIF intercluster pour le nouveau NIC](#).

5. Connectez la nouvelle carte réseau à la machine virtuelle.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics  
<dest_node-vm-nic-new>
```

6. Démarrer la machine virtuelle (nœud).

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. Sur le portail Azure, accédez à **Networking** et vérifiez que la nouvelle carte réseau, par exemple nic-New, existe et que la mise en réseau accélérée est activée.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg  
--query "[].{NIC: name, VM: virtualMachine.id}"
```

Pour les déploiements de paires haute disponibilité, répétez les étapes pour le nœud partenaire.

## Étape 2 : créer un IPspace, broadcast domain et LIF intercluster pour le nouveau NIC

Un IPspace séparé pour les LIF intercluster assure une séparation logique entre les fonctionnalités de mise en réseau pour la réplication entre les clusters.

Pour les étapes suivantes, utilisez l'interface de ligne de commandes ONTAP.

### Étapes

1. Créez le nouvel IPspace (New\_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Créez un broadcast domain sur le nouveau IPspace (New\_ipspace) et ajoutez le nic-New port.

```
dest::> network port show
```

3. Pour les systèmes à un seul nœud, le nouveau port ajouté est *e0b*. Pour les déploiements de paires haute disponibilité avec des disques gérés, le nouveau port ajouté est *e0d*. Pour les déploiements de paires haute disponibilité avec des blobs de page, le nouveau port ajouté est *e0e*. Utilisez le nom du nœud et non le nom de la machine virtuelle. Recherchez le nom du nœud en exécutant `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500  
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Créer un LIF intercluster sur le nouveau broadcast-domain (New\_bd) et sur le nouveau NIC (nic-New)

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-  
lif> -service-policy default-intercluster -address  
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask  
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Vérifier la création du nouveau LIF intercluster.

```
dest::> net int show
```

Pour les déploiements de paires haute disponibilité, répétez les étapes pour le nœud partenaire.

### Étape 3 : vérification du peering de cluster entre les systèmes source et destination

Cette section fournit des instructions pour vérifier le peering entre les systèmes source et de destination.

Pour les étapes suivantes, utilisez l'interface de ligne de commandes ONTAP.

#### Étapes

1. Vérifier que le LIF intercluster du cluster destination peut envoyer une requête ping au LIF intercluster du cluster source. Étant donné que le cluster de destination exécute cette commande, l'adresse IP de destination est l'adresse IP du LIF intercluster sur la source.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>  
-destination <10.161.189.6>
```

2. Vérifier que le LIF intercluster du cluster source peut envoyer une requête ping au LIF intercluster du cluster destination La destination est l'adresse IP de la nouvelle carte réseau créée sur la destination.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination  
<10.161.189.18>
```

Pour les déploiements de paires haute disponibilité, répétez les étapes pour le nœud partenaire.

### Étape 4 : créer le peering de SVM entre le système source et le système de destination

Cette section fournit des instructions pour la création du peering de SVM entre le système source et le système de destination.

Pour les étapes suivantes, utilisez l'interface de ligne de commandes ONTAP.

#### Étapes

1. Créer le peering de cluster sur la destination en utilisant l'adresse IP du LIF intercluster source en tant que `-peer-addr`s. Pour les paires HA, lister l'adresse IP du LIF intercluster source pour les deux nœuds

comme `-peer-addr`s.

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ip-space
<new_ipspace>
```

2. Saisissez et confirmez la phrase de passe.
3. Créer le peering de cluster sur la source en utilisant l'adresse IP de la LIF du cluster de destination comme `peer-addr`s. Pour les paires HA, lister l'adresse IP du LIF intercluster de destination pour les deux nœuds comme `-peer-addr`s.

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. Saisissez et confirmez la phrase de passe.
5. Vérifier que le cluster a bien été peering.

```
src::> cluster peer show
```

Le peering réussi affiche **disponible** dans le champ de disponibilité.

6. Créer le peering de SVM sur la destination. Les SVM source et destination doivent être des SVM de données.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Accepter le peering de SVM.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Vérifier que le SVM a bien peering.

```
dest::> vserver peer show
```

L'état homologue s'affiche **peered** et les applications de peering montrent **snapmirror**.

## Étape 5 : création d'une relation de réplication SnapMirror entre le système source et le système de destination

Cette section fournit des instructions sur la création d'une relation de réplication SnapMirror entre le système source et le système de destination.

Pour déplacer une relation de réplication SnapMirror existante, vous devez d'abord interrompre la relation de

réplication SnapMirror existante avant de créer une nouvelle relation de réplication SnapMirror.

Pour les étapes suivantes, utilisez l'interface de ligne de commandes ONTAP.

## Étapes

1. Créer un volume protégé des données sur le SVM de destination

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Créer la relation de réplication SnapMirror sur la destination qui inclut la règle SnapMirror et la planification de la réplication.

```
dest::> snapmirror create -source-path src_svm:src_vol -destination
-path dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Initialiser la relation de réplication SnapMirror sur la destination

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. Dans l'interface de ligne de commandes de ONTAP, valider le statut de la relation SnapMirror en exécutant la commande suivante :

```
dest::> snapmirror show
```

L'état de la relation est `Snapmirrored` et la santé de la relation est `true`.

5. Facultatif : dans l'interface de ligne de commandes de ONTAP, exécutez la commande suivante pour afficher l'historique des actions de la relation SnapMirror.

```
dest::> snapmirror show-history
```

Vous pouvez également monter les volumes source et de destination, écrire un fichier sur la source et vérifier que le volume est répliqué vers la destination.

## 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 DÉLICTELLE (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.