Administration d'Azure

Cloud Volumes ONTAP

NetApp
June 27, 2024

Sommaire

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.

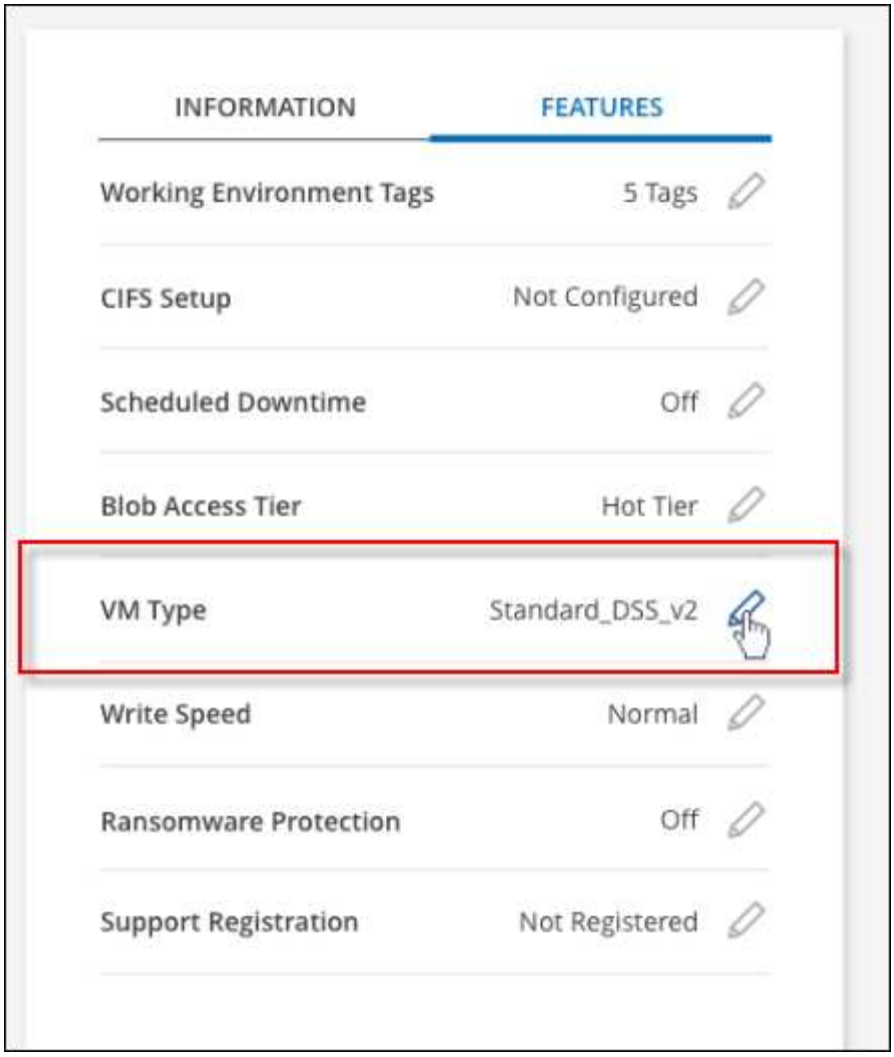
  Pour les systèmes à nœud unique, les E/S sont interrompues.

  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.

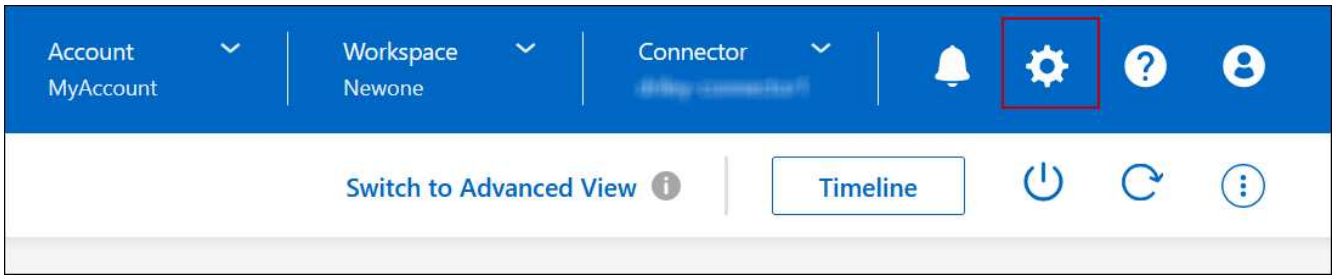
Ce processus peut entraîner des perturbations pour les clients CIFS. Les données qui ne sont pas validées auprès des clients CIFS pourraient être perdues.

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 du connecteur**.



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.

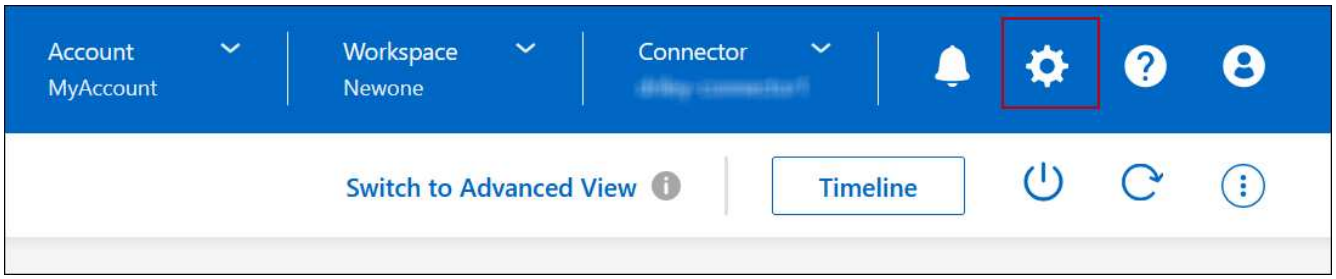
Désactivez les liens privés Azure et utilisez plutôt les terminaux de service

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 du connecteur**.



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

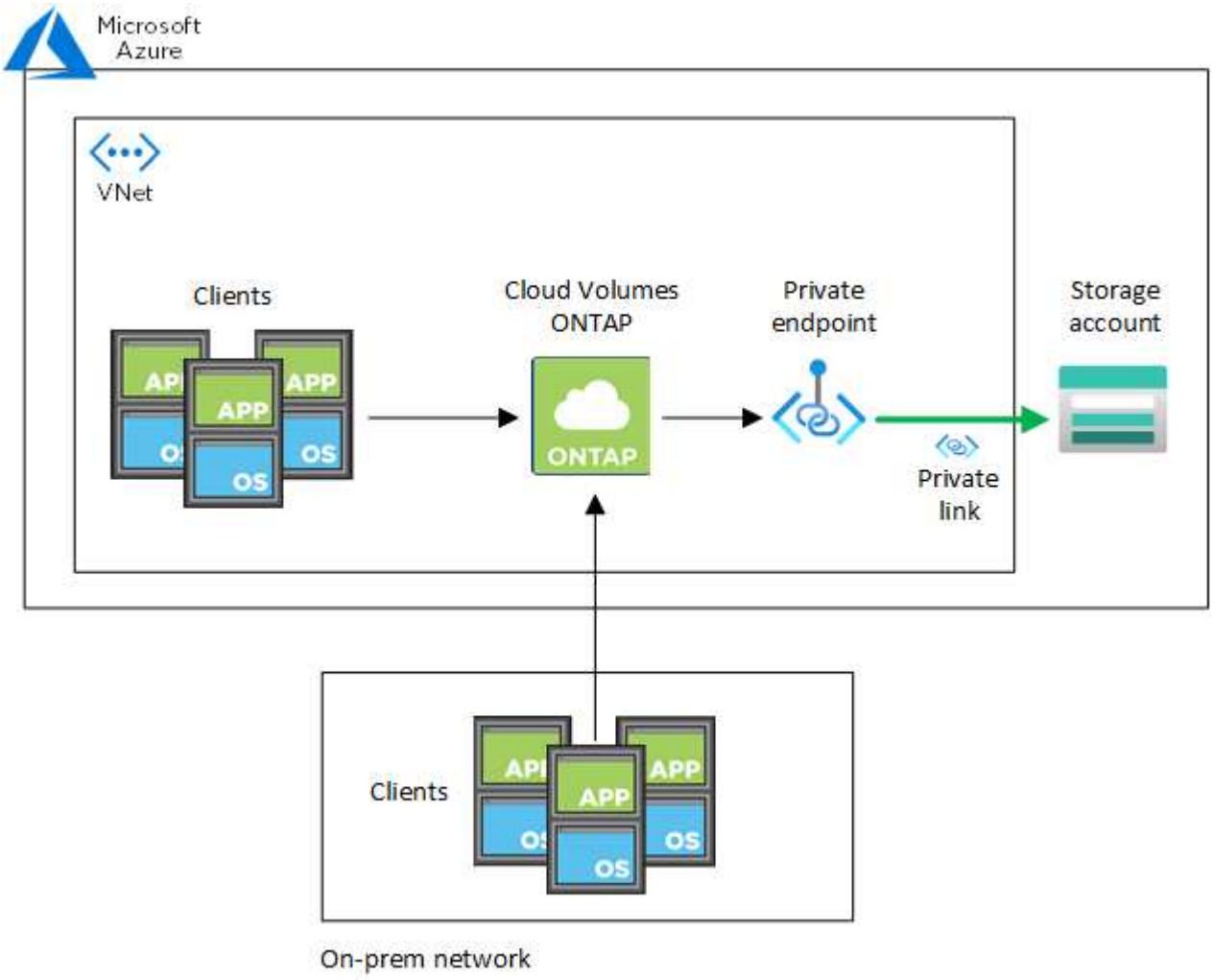
Si vous utilisez un DNS personnalisé, vous devez également créer un transitaire conditionnel vers la zone DNS privée Azure à partir de vos serveurs DNS personnalisés. Pour en savoir plus, reportez-vous à la section "La documentation d'Azure sur l'utilisation d'un transitaire DNS".

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 péré 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.

Informations sur le copyright

Informations sur les marques commerciales