Démarrer dans la NetApp Console

Cloud Volumes ONTAP

NetApp
February 17, 2026

Sommaire

Démarrer dans la NetApp Console

Démarrage rapide de Cloud Volumes ONTAP dans Azure

Démarrez avec Cloud Volumes ONTAP pour Azure en quelques étapes.

1 Créer un agent de console

Si vous n'avez pas de "Agent de console" mais il faut en créer un. "Découvrez comment créer un agent de console dans Azure"

Notez que si vous souhaitez déployer Cloud Volumes ONTAP dans un sous-réseau où aucun accès Internet n'est disponible, vous devez installer manuellement l'agent de console et accéder à la NetApp Console qui s'exécute sur cet agent de console. "Découvrez comment installer manuellement l'agent de console dans un emplacement sans accès Internet"

2 Planifiez votre configuration

La console propose des packages préconfigurés qui correspondent à vos exigences de charge de travail, ou vous pouvez créer votre propre configuration. Si vous choisissez votre propre configuration, vous devez comprendre les options qui s'offrent à vous. Pour plus d'informations, reportez-vous à"Planifiez votre configuration Cloud Volumes ONTAP dans Azure" .

3 Configurez votre réseau

1. Assurez-vous que votre réseau virtuel et vos sous-réseaux prendront en charge la connectivité entre l'agent de console et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du VPC cible pour NetApp AutoSupport.

   Cette étape n'est pas requise si vous déployez Cloud Volumes ONTAP dans un emplacement où aucun accès Internet n'est disponible.

"En savoir plus sur les exigences de mise en réseau" .

4 Lancer Cloud Volumes ONTAP

Cliquez sur **Ajouter un système**, sélectionnez le type de système que vous souhaitez déployer et suivez les étapes de l'assistant. "Lisez les instructions étape par étape" .

Liens connexes

- "Création d'un agent de console à partir de la console"
- "Création d'un agent de console à partir de la Place de marché Azure"
- "Installation du logiciel agent de console sur un hôte Linux"
- "Ce que fait la console avec les autorisations"

Planifiez votre configuration Cloud Volumes ONTAP dans Azure

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, vous pouvez choisir un système préconfiguré qui correspond à vos exigences de charge de travail ou créer votre propre configuration. Si vous choisissez votre propre configuration, vous devez comprendre les options qui s'offrent à vous.

Choisissez une licence Cloud Volumes ONTAP

Plusieurs options de licence sont disponibles pour Cloud Volumes ONTAP. Chaque option vous permet de choisir un modèle de consommation qui répond à vos besoins.

- "En savoir plus sur les options de licence pour Cloud Volumes ONTAP"
- "Apprenez à configurer les licences"

Choisissez une région prise en charge

Cloud Volumes ONTAP est pris en charge dans la plupart des régions Microsoft Azure. "Afficher la liste complète des régions prises en charge" .

Choisissez un type de machine virtuelle pris en charge

Cloud Volumes ONTAP prend en charge plusieurs types de machines virtuelles, selon le type de licence que vous choisissez.

"Configurations prises en charge pour Cloud Volumes ONTAP dans Azure"

Comprendre les limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP est liée à la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Vous devez être conscient de ces limites lorsque vous planifiez votre configuration.

"Limites de stockage pour Cloud Volumes ONTAP dans Azure"

Dimensionnez votre système dans Azure

Le dimensionnement de votre système Cloud Volumes ONTAP peut vous aider à répondre aux exigences de performances et de capacité. Vous devez tenir compte de quelques points clés lors du choix d'un type de machine virtuelle, d'un type de disque et d'une taille de disque :

Type de machine virtuelle

Consultez les types de machines virtuelles pris en charge dans le "Notes de version de Cloud Volumes ONTAP" puis examinez les détails de chaque type de machine virtuelle pris en charge. Sachez que chaque type de machine virtuelle prend en charge un nombre spécifique de disques de données.

- "Documentation Azure : Tailles de machines virtuelles à usage général"
- "Documentation Azure : Tailles de machines virtuelles optimisées en mémoire"

Type de disque Azure avec systèmes à nœud unique

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent que Cloud Volumes ONTAP utilise comme disque.

Les systèmes à nœud unique peuvent utiliser ces types de disques Azure Managed Disks :

- Les *disques gérés SSD Premium* offrent des performances élevées pour les charges de travail gourmandes en E/S à un coût plus élevé.
- Les *disques gérés SSD Premium v2* offrent des performances supérieures avec une latence plus faible à un coût inférieur, par rapport aux disques gérés SSD Premium.
- Les *disques gérés SSD standard* offrent des performances constantes pour les charges de travail nécessitant de faibles IOPS.
- Les *disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevés et que vous souhaitez réduire vos coûts.

Pour plus de détails sur les cas d'utilisation de ces disques, reportez-vous à "Documentation Microsoft Azure : Quels types de disques sont disponibles dans Azure ?" .

Type de disque Azure avec paires HA

Les systèmes HA utilisent des disques gérés partagés SSD Premium qui offrent tous deux des performances élevées pour les charges de travail gourmandes en E/S à un coût plus élevé. Les déploiements HA créés avant la version 9.12.1 utilisent des blobs de pages Premium.

Taille du disque Azure

Lorsque vous lancez des instances Cloud Volumes ONTAP , vous devez choisir la taille de disque par défaut pour les agrégats. La NetApp Console utilise cette taille de disque pour l'agrégat initial et pour tous les agrégats supplémentaires qu'elle crée lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente de la taille par défaut en"en utilisant l'option d'allocation avancée" .

Tous les disques d'un agrégat doivent avoir la même taille.

Lors du choix d'une taille de disque, vous devez prendre en compte plusieurs facteurs. La taille du disque a un impact sur le montant que vous payez pour le stockage, la taille des volumes que vous pouvez créer dans un agrégat, la capacité totale disponible pour Cloud Volumes ONTAP et les performances de stockage.

Les performances du stockage Azure Premium sont liées à la taille du disque. Les disques plus grands offrent des IOPS et un débit plus élevés. Par exemple, choisir des disques de 1 Tio peut offrir de meilleures performances que des disques de 500 Gio, à un coût plus élevé.

Il n'y a aucune différence de performances entre les tailles de disque pour le stockage standard. Vous devez choisir la taille du disque en fonction de la capacité dont vous avez besoin.

Consultez Azure pour connaître les IOPS et le débit par taille de disque :

- "Microsoft Azure : tarifs des disques gérés"
- "Microsoft Azure : tarifs des blobs de pages"

Afficher les disques système par défaut

En plus du stockage des données utilisateur, la console achète également du stockage cloud pour les données système Cloud Volumes ONTAP (données de démarrage, données racine, données principales et NVRAM). À des fins de planification, il peut être utile de vérifier ces détails avant de déployer Cloud Volumes ONTAP.

"Afficher les disques par défaut pour les données système Cloud Volumes ONTAP dans Azure" .

L'agent de console nécessite également un disque système. "Afficher les détails sur la configuration par défaut de l'agent de console" .

Recueillir des informations sur le réseau

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, vous devez spécifier les détails de votre réseau virtuel. Vous pouvez utiliser une feuille de travail pour recueillir les informations auprès de votre administrateur.

Informations Azure	Votre valeur
Région	
Réseau virtuel (VNet)	
Sous-réseau	
Groupe de sécurité réseau (si vous utilisez le vôtre)	

Choisissez une vitesse d'écriture

La console vous permet de choisir un paramètre de vitesse d'écriture pour Cloud Volumes ONTAP. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés, ainsi que les risques et les recommandations lors de l'utilisation d'une vitesse d'écriture élevée. "En savoir plus sur la vitesse d'écriture" .

Choisissez un profil d'utilisation du volume

ONTAP inclut plusieurs fonctionnalités d'efficacité de stockage qui peuvent réduire la quantité totale de stockage dont vous avez besoin. Lorsque vous créez un volume dans la console, vous pouvez choisir un profil qui active ces fonctionnalités ou un profil qui les désactive. Vous devriez en savoir plus sur ces fonctionnalités pour vous aider à décider quel profil utiliser.

Les fonctionnalités d'efficacité du stockage NetApp offrent les avantages suivants :

Provisionnement léger

Présente plus de stockage logique aux hôtes ou aux utilisateurs que ce dont vous disposez réellement dans votre pool de stockage physique. Au lieu de préallouer l'espace de stockage, l'espace de stockage est alloué dynamiquement à chaque volume au fur et à mesure que les données sont écrites.

Déduplication

Améliore l'efficacité en localisant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins en capacité de stockage en éliminant les blocs de données redondants qui résident dans le même volume.

Compression

Réduit la capacité physique requise pour stocker les données en compressant les données dans un volume sur le stockage principal, secondaire et d'archive.

Configurer la mise en réseau Azure pour Cloud Volumes ONTAP

La NetApp Console gère la configuration des composants réseau pour Cloud Volumes ONTAP, tels que les adresses IP, les masques de réseau et les itinéraires. Vous devez vous assurer que l'accès Internet sortant est disponible, que suffisamment d'adresses IP privées sont disponibles, que les bonnes connexions sont en place, etc.

Exigences pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être respectées dans Azure.

Accès Internet sortant

Les systèmes Cloud Volumes ONTAP nécessitent un accès Internet sortant pour accéder aux points de terminaison externes pour diverses fonctions. Cloud Volumes ONTAP ne peut pas fonctionner correctement si ces points de terminaison sont bloqués dans des environnements avec des exigences de sécurité strictes.

L'agent de console contacte également plusieurs points de terminaison pour les opérations quotidiennes. Pour plus d'informations sur les points de terminaison, reportez-vous à "Afficher les points de terminaison contactés depuis l'agent de la console" et "Préparer le réseau pour l'utilisation de la console" .

Points de terminaison Cloud Volumes ONTAP

Cloud Volumes ONTAP utilise ces points de terminaison pour communiquer avec divers services.

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact en cas d'indisponibilité
\ https://netapp-cloud-account.auth0.com	Authentification	Utilisé pour l'authentification dans la console.	Modes standard et restreint.	L'authentification de l'utilisateur échoue et les services suivants restent indisponibles : • Services Cloud Volumes ONTAP • Services ONTAP • Protocoles et services proxy

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact en cas d'indisponibilité
https://vault.azure.net	Coffre-fort à clés	Utilisé pour récupérer les clés secrètes du client à partir d'Azure Key Vault lors de l'utilisation de clés gérées par le client (CMK).	Modes standard, restreint et privé.	Les services Cloud Volumes ONTAP ne sont pas disponibles.
\ https://api.bluexp.netapp.com/tenancy	Location	Utilisé pour récupérer les ressources Cloud Volumes ONTAP à partir de la console pour autoriser les ressources et les utilisateurs.	Modes standard et restreint.	Les ressources Cloud Volumes ONTAP et les utilisateurs ne sont pas autorisés.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilisé pour envoyer des données de télémétrie AutoSupport au support NetApp .	Modes standard et restreint.	Les informations AutoSupport ne sont toujours pas livrées.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	Les régions publiques	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Région de Chine	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.

Points de terminaison	Applicable pour	But	Modes de déploiement	Impact en cas d'indisponibilité
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	Région Allemagne	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	régions gouvernementales	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	Régions du gouvernement du DoD	Communication avec les services Azure.	Modes standard, restreint et privé.	Cloud Volumes ONTAP ne peut pas communiquer avec le service Azure pour effectuer des opérations spécifiques pour la console dans Azure.

Configuration du proxy réseau de l'agent de la NetApp Console

Vous pouvez utiliser la configuration des serveurs proxy de l'agent NetApp Console pour activer l'accès Internet sortant à partir de Cloud Volumes ONTAP. La console prend en charge deux types de proxys :

- **Proxy explicite** : le trafic sortant de Cloud Volumes ONTAP utilise l'adresse HTTP du serveur proxy spécifié lors de la configuration du proxy de l'agent de la console. L'administrateur peut également avoir configuré des informations d'identification utilisateur et des certificats d'autorité de certification racine pour une authentification supplémentaire. Si un certificat d'autorité de certification racine est disponible pour le proxy explicite, assurez-vous d'obtenir et de télécharger le même certificat sur votre système Cloud Volumes ONTAP à l'aide de l' "ONTAP CLI : installation du certificat de sécurité" commande.
- **Proxy transparent** : le réseau est configuré pour acheminer automatiquement le trafic sortant de Cloud Volumes ONTAP via le proxy de l'agent de la console. Lors de la configuration d'un proxy transparent, l'administrateur doit fournir uniquement un certificat d'autorité de certification racine pour la connectivité à partir de Cloud Volumes ONTAP, et non l'adresse HTTP du serveur proxy. Assurez-vous d'obtenir et de télécharger le même certificat d'autorité de certification racine sur votre système Cloud Volumes ONTAP à l'aide de "ONTAP CLI : installation du certificat de sécurité" commande.

Pour plus d'informations sur la configuration des serveurs proxy, reportez-vous à la "Configurer l'agent de console pour utiliser un serveur proxy" .

adresses IP

La console alloue automatiquement le nombre requis d'adresses IP privées à Cloud Volumes ONTAP dans Azure. Vous devez vous assurer que votre réseau dispose de suffisamment d'adresses IP privées disponibles.

Le nombre d'interfaces logiques (LIF) allouées à Cloud Volumes ONTAP dépend du type de système déployé : mono-nœud ou paire haute disponibilité. Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est requise pour les outils de gestion tels que SnapCenter.

> Un LIF iSCSI fournit un accès client via le protocole iSCSI et est utilisé par le système pour d'autres flux de travail réseau importants. Ces LIF sont obligatoires et ne doivent pas être supprimés.

Adresses IP pour un système à nœud unique

La NetApp Console alloue 5 ou 6 adresses IP à un système à nœud unique :

- Gestion de cluster IP
- IP de gestion des nœuds
- IP intercluster pour SnapMirror
- IP NFS/CIFS
- IP iSCSI

> L'IP iSCSI fournit un accès client via le protocole iSCSI. Il est également utilisé par le système pour d'autres flux de travail réseau importants. Ce LIF est obligatoire et ne doit pas être supprimé.

- Gestion SVM (facultatif - non configuré par défaut)

Adresses IP pour les paires HA

La console alloue des adresses IP à 4 cartes réseau (par nœud) pendant le déploiement.

Notez que la NetApp Console crée une interface logique de gestion SVM sur les paires haute disponibilité, mais pas sur les systèmes à nœud unique dans Azure.

NIC0

- IP de gestion des nœuds
- IP intercluster
- IP iSCSI

> L'IP iSCSI fournit un accès client via le protocole iSCSI. Il est également utilisé par le système pour d'autres flux de travail réseau importants. Ce LIF est obligatoire et ne doit pas être supprimé.

NIC1

- IP du réseau en cluster

NIC2

- IP d'interconnexion de cluster (HA IC)

NIC3

- Pageblob NIC IP (accès disque)

> NIC3 s'applique uniquement aux déploiements HA qui utilisent le stockage d'objets blob de pages.

Les adresses IP ci-dessus ne migrent pas lors d'événements de basculement.

De plus, 4 adresses IP frontales (FIP) sont configurées pour migrer lors d'événements de basculement. Ces adresses IP frontales résident dans l'équilibreur de charge.

- Gestion de cluster IP
- IP de données NodeA (NFS/CIFS)
- IP de données NodeB (NFS/CIFS)
- IP de gestion SVM

Connexions sécurisées aux services Azure

Par défaut, la console active une liaison privée Azure pour les connexions entre Cloud Volumes ONTAP et les comptes de stockage d'objets blob de pages Azure.

Dans la plupart des cas, vous n'avez rien à faire : la console gère Azure Private Link pour vous. Mais si vous utilisez Azure Private DNS, vous devrez modifier un fichier de configuration. Vous devez également être conscient d'une exigence relative à l'emplacement de l'agent de console dans Azure.

Vous pouvez également désactiver la connexion Private Link, si les besoins de votre entreprise l'exigent. Si vous désactivez le lien, la console configure Cloud Volumes ONTAP pour utiliser un point de terminaison de service à la place.

"En savoir plus sur l'utilisation des liens privés Azure ou des points de terminaison de service avec Cloud Volumes ONTAP" .

Mise en réseau pour le chiffrement Azure VNet

Cloud Volumes ONTAP prend en charge "chiffrement Azure Virtual Network (VNet)" le chiffrement du trafic entre machines virtuelles au sein d'un VNet ou entre VNets appariés. Cette fonctionnalité est configurée au niveau du VNet Azure et est indépendante de la topologie Cloud Volumes ONTAP (nœud unique ou HA).

Il vous suffit de vérifier que la mise en réseau accélérée est activée sur les cartes réseau de la machine virtuelle et de consulter les exigences et limitations du chiffrement des réseaux virtuels Azure avant d'activer cette fonctionnalité. Vous ne devez pas modifier les objets d'équilibrage de charge gérés NetApp.

"Documentation Azure : chiffrement VNet et mise en réseau accélérée".

Connexions à d'autres systèmes ONTAP

Pour répliquer des données entre un système Cloud Volumes ONTAP dans Azure et des systèmes ONTAP dans d'autres réseaux, vous devez disposer d'une connexion VPN entre le réseau virtuel Azure et l'autre réseau, par exemple, votre réseau d'entreprise.

Pour les instructions, reportez-vous à la "Documentation Microsoft Azure : Créer une connexion site à site dans le portail Azure" .

Port pour l'interconnexion HA

Une paire Cloud Volumes ONTAP HA inclut une interconnexion HA, qui permet à chaque nœud de vérifier en permanence si son partenaire fonctionne et de mettre en miroir les données du journal pour la mémoire non volatile de l'autre. L'interconnexion HA utilise le port TCP 10006 pour la communication.

Par défaut, la communication entre les LIF d'interconnexion HA est ouverte et il n'existe aucune règle de groupe de sécurité pour ce port. Mais si vous créez un pare-feu entre les LIF d'interconnexion HA, vous devez vous assurer que le trafic TCP est ouvert pour le port 10006 afin que la paire HA puisse fonctionner correctement.

Une seule paire HA dans un groupe de ressources Azure

Vous devez utiliser un groupe de ressources *dédié* pour chaque paire Cloud Volumes ONTAP HA que vous déployez dans Azure. Une seule paire HA est prise en charge dans un groupe de ressources.

La console rencontre des problèmes de connexion si vous essayez de déployer une deuxième paire Cloud Volumes ONTAP HA dans un groupe de ressources Azure.

Règles du groupe de sécurité

La console crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes pour que Cloud Volumes ONTAP fonctionne correctement. "Afficher les règles du groupe de sécurité pour l'agent de la console" .

Les groupes de sécurité Azure pour Cloud Volumes ONTAP nécessitent que les ports appropriés soient ouverts pour la communication interne entre les nœuds. "En savoir plus sur les ports internes ONTAP" .

Nous ne recommandons pas de modifier les groupes de sécurité prédéfinis ni d'utiliser des groupes de sécurité personnalisés. Toutefois, si vous devez le faire, notez que le processus de déploiement nécessite que le système Cloud Volumes ONTAP dispose d'un accès complet au sein de son propre sous-réseau. Une fois le déploiement terminé, si vous décidez de modifier le groupe de sécurité réseau, assurez-vous de garder les ports du cluster et les ports réseau HA ouverts. Cela garantit une communication transparente au sein du cluster Cloud Volumes ONTAP (communication de bout en bout entre les nœuds).

Règles entrantes pour les systèmes à nœud unique

Lorsque vous ajoutez un système Cloud Volumes ONTAP et choisissez un groupe de sécurité prédéfini, vous pouvez choisir d'autoriser le trafic dans l'un des éléments suivants :

- **VNet sélectionné uniquement** : la source du trafic entrant est la plage de sous-réseaux du VNet pour le système Cloud Volumes ONTAP et la plage de sous-réseaux du VNet sur lequel réside l'agent de la console. C'est l'option recommandée.
- **Tous les réseaux virtuels** : la source du trafic entrant est la plage IP 0.0.0.0/0.
- **Désactivé** : cette option restreint l'accès au réseau public à votre compte de stockage et désactive la hiérarchisation des données pour les systèmes Cloud Volumes ONTAP . Il s'agit d'une option recommandée si vos adresses IP privées ne doivent pas être exposées même au sein du même réseau virtuel en raison des réglementations et des politiques de sécurité.

Priorité et nom	Port et protocole	Source et destination	Description
1000 entrants_ssh	22 TCP	N'importe lequel à n'importe lequel	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
1001 entrant_http	80 TCP	N'importe lequel à n'importe lequel	Accès HTTP à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
1002 entrant_111_tcp	111 TCP	N'importe lequel à n'importe lequel	Appel de procédure à distance pour NFS
1003 entrant_111_udp	111 UDP	N'importe lequel à n'importe lequel	Appel de procédure à distance pour NFS
1004 entrant_139	139 TCP	N'importe lequel à n'importe lequel	Session de service NetBIOS pour CIFS
1005 entrant_161-162 _tcp	161-162 TCP	N'importe lequel à n'importe lequel	Protocole simple de gestion de réseau
1006 entrant_161-162 _udp	161-162 UDP	N'importe lequel à n'importe lequel	Protocole simple de gestion de réseau
1007 entrant_443	443 TCP	N'importe lequel à n'importe lequel	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster
1008 entrant_445	445 TCP	N'importe lequel à n'importe lequel	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
1009 entrant_635_tcp	635 TCP	N'importe lequel à n'importe lequel	Montage NFS
1010 entrant_635_udp	635 UDP	N'importe lequel à n'importe lequel	Montage NFS
1011 entrant_749	749 TCP	N'importe lequel à n'importe lequel	Kerberos
1012 entrant_2049_tcp	2049 TCP	N'importe lequel à n'importe lequel	Démon du serveur NFS
1013 entrant_2049_udp	2049 UDP	N'importe lequel à n'importe lequel	Démon du serveur NFS
1014 entrant_3260	3260 TCP	N'importe lequel à n'importe lequel	Accès iSCSI via le LIF de données iSCSI
1015 entrant_4045-4046_tcp	4045-4046 TCP	N'importe lequel à n'importe lequel	Démon de verrouillage NFS et moniteur d'état du réseau

Priorité et nom	Port et protocole	Source et destination	Description
1016 entrant_4045-4046_udp	4045-4046 UDP	N'importe lequel à n'importe lequel	Démon de verrouillage NFS et moniteur d'état du réseau
1017 entrant_10000	10000 TCP	N'importe lequel à n'importe lequel	Sauvegarde à l'aide de NDMP
1018 entrant_11104-11105	11104-11105 TCP	N'importe lequel à n'importe lequel	Transfert de données SnapMirror
3000 inbound_deny _all_tcp	N'importe quel port TCP	N'importe lequel à n'importe lequel	Bloquer tout autre trafic TCP entrant
3001 inbound_deny _all_udp	N'importe quel port UDP	N'importe lequel à n'importe lequel	Bloquer tout autre trafic UDP entrant
65000 AutoriserVnetInBound	N'importe quel port N'importe quel protocole	Réseau virtuel vers réseau virtuel	Trafic entrant depuis le VNet
65001 Autoriser AzureLoad BalancerInBound	N'importe quel port N'importe quel protocole	AzureLoadBalancer vers n'importe quel	Trafic de données provenant de l'équilibreur de charge standard Azure
65500 RefuserToutEnLiaison	N'importe quel port N'importe quel protocole	N'importe lequel à n'importe lequel	Bloquer tout autre trafic entrant

Règles entrantes pour les systèmes HA

Lorsque vous ajoutez un système Cloud Volumes ONTAP et choisissez un groupe de sécurité prédéfini, vous pouvez choisir d'autoriser le trafic dans l'un des éléments suivants :

- **VNet sélectionné uniquement** : la source du trafic entrant est la plage de sous-réseaux du VNet pour le système Cloud Volumes ONTAP et la plage de sous-réseaux du VNet sur lequel réside l'agent de la console. C'est l'option recommandée.
- **Tous les réseaux virtuels** : la source du trafic entrant est la plage IP 0.0.0.0/0.

> Les systèmes à haute disponibilité (HA) comportent moins de règles entrantes que les systèmes à nœud unique, car le trafic de données entrant transite par l'équilibreur de charge standard Azure. Pour cette raison, le trafic provenant de l'équilibreur de charge doit être autorisé, comme indiqué dans la règle « AllowAzureLoadBalancerInBound ».

- **Désactivé** : cette option restreint l'accès au réseau public à votre compte de stockage et désactive la hiérarchisation des données pour les systèmes Cloud Volumes ONTAP . Il s'agit d'une option recommandée si vos adresses IP privées ne doivent pas être exposées même au sein du même réseau virtuel en raison des réglementations et des politiques de sécurité.

Priorité et nom	Port et protocole	Source et destination	Description
100 entrants_443	443 Tout protocole	N'importe lequel à n'importe lequel	Connectivité avec l'agent de console et accès HTTPS à la console Web ONTAP System Manager à l'aide de l'adresse IP du LIF de gestion du cluster

Priorité et nom	Port et protocole	Source et destination	Description
101 entrant_111_tcp	111 Tout protocole	N'importe lequel à n'importe lequel	Appel de procédure à distance pour NFS
102 entrant_2049_tcp	2049 Tout protocole	N'importe lequel à n'importe lequel	Démon du serveur NFS
111 entrant_ssh	22 Tout protocole	N'importe lequel à n'importe lequel	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
121 entrant_53	53 Tout protocole	N'importe lequel à n'importe lequel	DNS et CIFS
65000 AutoriserVnetInBound	N'importe quel port N'importe quel protocole	Réseau virtuel vers réseau virtuel	Trafic entrant depuis le VNet
65001 Autoriser AzureLoad BalancerInBound	N'importe quel port N'importe quel protocole	AzureLoadBalancer vers n'importe quel	Trafic de données provenant de l'équilibreur de charge standard Azure
65500 RefuserToutEnLiaison	N'importe quel port N'importe quel protocole	N'importe lequel à n'importe lequel	Bloquer tout autre trafic entrant

Règles de sortie

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

Règles de base pour les voyages sortants

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

Port	Protocole	But
Tous	Tout TCP	Tout le trafic sortant
Tous	Tout UDP	Tout le trafic sortant

Règles sortantes avancées

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

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

Service	Port	Protocole	Source	Destination	But
Active Directory	88	TCP	Gestion des nœuds LIF	Forêt Active Directory	Authentification Kerberos V
	137	UDP	Gestion des nœuds LIF	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	Gestion des nœuds LIF	Forêt Active Directory	Service de datagramme NetBIOS
	139	TCP	Gestion des nœuds LIF	Forêt Active Directory	Session de service NetBIOS
	389	TCP et UDP	Gestion des nœuds LIF	Forêt Active Directory	LDAP
	445	TCP	Gestion des nœuds LIF	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
	464	TCP	Gestion des nœuds LIF	Forêt Active Directory	Kerberos V changer et définir le mot de passe (SET_CHANGE)
	464	UDP	Gestion des nœuds LIF	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	Gestion des nœuds LIF	Forêt Active Directory	Kerberos V changer et définir le mot de passe (RPCSEC_GSS)
	88	TCP	Données LIF (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V
	137	UDP	Données LIF (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	Données LIF (NFS, CIFS)	Forêt Active Directory	Service de datagramme NetBIOS
	139	TCP	Données LIF (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	389	TCP et UDP	Données LIF (NFS, CIFS)	Forêt Active Directory	LDAP
	445	TCP	Données LIF (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec trame NetBIOS
	464	TCP	Données LIF (NFS, CIFS)	Forêt Active Directory	Kerberos V changer et définir le mot de passe (SET_CHANGE)
	464	UDP	Données LIF (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	Données LIF (NFS, CIFS)	Forêt Active Directory	Kerberos V changer et définir le mot de passe (RPCSEC_GSS)

Service	Port	Protocole	Source	Destination	But
AutoSupport	HTTPS	443	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (HTTPS est la valeur par défaut)
	HTTP	80	Gestion des nœuds LIF	monsupport.netapp.com	AutoSupport (uniquement si le protocole de transport est modifié de HTTPS à HTTP)
	TCP	3128	Gestion des nœuds LIF	Agent de console	Envoi de messages AutoSupport via un serveur proxy sur l'agent de la console, si une connexion Internet sortante n'est pas disponible
Sauvegardes de configuration	HTTP	80	Gestion des nœuds LIF	http://<adresse IP de l'agent de la console>/occm/offboxconfig	Envoyer des sauvegardes de configuration à l'agent de la console. "Documentation ONTAP" .
DHCP	68	UDP	Gestion des nœuds LIF	DHCP	Client DHCP pour la première configuration
DHCPS	67	UDP	Gestion des nœuds LIF	DHCP	serveur DHCP
DNS	53	UDP	Gestion des nœuds LIF et LIF de données (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Gestion des nœuds LIF	Serveurs de destination	Copie NDMP
SMTP	25	TCP	Gestion des nœuds LIF	Serveur de messagerie	Alertes SMTP, peuvent être utilisées pour AutoSupport
SNMP	161	TCP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	161	UDP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	162	TCP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
	162	UDP	Gestion des nœuds LIF	Serveur de surveillance	Surveillance par traps SNMP
SnapMirror	11104	TCP	LIF intercluster	LIF intercluster ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	11105	TCP	LIF intercluster	LIF intercluster ONTAP	Transfert de données SnapMirror
Syslog	514	UDP	Gestion des nœuds LIF	Serveur Syslog	Messages de transfert Syslog

Exigences pour l’agent de console

Si vous n’avez pas encore créé d’agent de console, vous devez également vérifier les exigences réseau pour l’agent de console.

- "Afficher les exigences réseau pour l’agent de console"
- "Règles de groupe de sécurité dans Azure"

Sujets connexes

- "Vérifier la configuration AutoSupport pour Cloud Volumes ONTAP"
- "En savoir plus sur les ports internes ONTAP" .

Configurer Cloud Volumes ONTAP pour utiliser une clé gérée par le client dans Azure

Les données sont automatiquement chiffrées sur Cloud Volumes ONTAP dans Azure à l’aide du chiffrement du service de stockage Azure avec une clé gérée par Microsoft. Mais vous pouvez utiliser votre propre clé de cryptage en suivant les étapes sur cette page.

Présentation du cryptage des données

Les données Cloud Volumes ONTAP sont automatiquement chiffrées dans Azure à l’aide de "Chiffrement du service de stockage Azure" . L’implémentation par défaut utilise une clé gérée par Microsoft. Aucune configuration n’est requise.

Si vous souhaitez utiliser une clé gérée par le client avec Cloud Volumes ONTAP, vous devez suivre les étapes suivantes :

1. Depuis Azure, créez un coffre de clés, puis générez une clé dans ce coffre.
2. Depuis la NetApp Console, utilisez l’API pour créer un système Cloud Volumes ONTAP qui utilise la clé.

Comment les données sont cryptées

La console utilise un ensemble de chiffrement de disque, qui permet la gestion des clés de chiffrement avec des disques gérés et non des blobs de pages. Tous les nouveaux disques de données utilisent également le même ensemble de chiffrement de disque. Les versions inférieures utiliseront la clé gérée par Microsoft, au lieu de la clé gérée par le client.

Une fois que vous avez créé un système Cloud Volumes ONTAP configuré pour utiliser une clé gérée par le client, les données Cloud Volumes ONTAP sont chiffrées comme suit.

Configuration de Cloud Volumes ONTAP	Disques système utilisés pour le chiffrement des clés	Disques de données utilisés pour le cryptage des clés
Nœud unique	• Botte • Cœur • NVRAM	• Racine • Données

Configuration de Cloud Volumes ONTAP	Disques système utilisés pour le chiffrement des clés	Disques de données utilisés pour le cryptage des clés
Zone de disponibilité unique Azure HA avec objets blob de pages	• Botte • Cœur • NVRAM	Aucune
Zone de disponibilité unique Azure HA avec disques gérés partagés	• Botte • Cœur • NVRAM	• Racine • Données
Zones de disponibilité multiples Azure HA avec disques gérés partagés	• Botte • Cœur • NVRAM	• Racine • Données

Tous les comptes de stockage Azure pour Cloud Volumes ONTAP sont chiffrés à l'aide d'une clé gérée par le client. Si vous souhaitez crypter vos comptes de stockage lors de leur création, vous devez créer et fournir l'ID de la ressource dans la demande de création de Cloud Volumes ONTAP . Ceci s'applique à tous les types de déploiements. Si vous ne le fournissez pas, les comptes de stockage seront toujours chiffrés, mais la console crée d'abord les comptes de stockage avec le chiffrement à clé géré par Microsoft, puis met à jour les comptes de stockage pour utiliser la clé gérée par le client.

Rotation des clés dans Cloud Volumes ONTAP

Lorsque vous configurez vos clés de chiffrement, vous devez utiliser le portail Azure pour configurer et activer la rotation automatique des clés. La création et l'activation d'une nouvelle version de clés de chiffrement garantissent que Cloud Volumes ONTAP peut détecter et utiliser automatiquement la dernière version de clé pour le chiffrement, garantissant ainsi que vos données restent sécurisées sans intervention manuelle.

Pour plus d'informations sur la configuration de vos clés et la configuration de la rotation des clés, reportez-vous aux rubriques de documentation Microsoft Azure suivantes :

- "Configurer la rotation automatique des clés cryptographiques dans Azure Key Vault"
- "Azure PowerShell – Activer les clés gérées par le client"

> Après avoir configuré les touches, assurez-vous d'avoir sélectionné "*Activer la rotation automatique*" , afin que Cloud Volumes ONTAP puisse utiliser les nouvelles clés lorsque les clés précédentes expirent. Si vous n'activez pas cette option sur le portail Azure, Cloud Volumes ONTAP ne peut pas détecter automatiquement les nouvelles clés, ce qui peut entraîner des problèmes avec le provisionnement du stockage.

Créer une identité gérée attribuée par l'utilisateur

Vous avez la possibilité de créer une ressource appelée identité gérée attribuée par l'utilisateur. Cela vous permet de crypter vos comptes de stockage lorsque vous créez un système Cloud Volumes ONTAP . Nous vous recommandons de créer cette ressource avant de créer un coffre de clés et de générer une clé.

La ressource a l'ID suivant : `userassignedidentity` .

Étapes

1. Dans Azure, accédez aux services Azure et sélectionnez **Identités gérées**.
2. Cliquez sur **Créer**.
3. Fournissez les détails suivants :
   - **Abonnement** : Choisissez un abonnement. Nous vous recommandons de choisir le même abonnement que l'abonnement de l'agent Console.
   - **Groupe de ressources** : utilisez un groupe de ressources existant ou créez-en un nouveau.
   - **Région** : sélectionnez éventuellement la même région que l'agent de la console.
   - **Nom**: Saisissez un nom pour la ressource.
4. Ajoutez éventuellement des balises.
5. Cliquez sur **Créer**.

Créer un coffre de clés et générer une clé

Le coffre de clés doit résider dans le même abonnement Azure et la même région dans lesquels vous prévoyez de créer le système Cloud Volumes ONTAP .

Si tucréé une identité gérée attribuée par l'utilisateur , lors de la création du coffre de clés, vous devez également créer une politique d'accès pour le coffre de clés.

Étapes

1. "Créez un coffre de clés dans votre abonnement Azure" .

   Notez les exigences suivantes pour le coffre-fort de clés :

   - Le coffre de clés doit résider dans la même région que le système Cloud Volumes ONTAP .
   - Les options suivantes doivent être activées :
     - **Suppression logicielle** (cette option est activée par défaut, mais ne doit *pas* être désactivée)
     - **Protection contre la purge**
     - **Azure Disk Encryption for volume encryption** (pour les systèmes à nœud unique, les paires haute disponibilité dans plusieurs zones et les déploiements haute disponibilité dans une seule zone de disponibilité)

       L'utilisation des clés de chiffrement gérées par le client Azure dépend de l'activation du chiffrement de disque Azure pour le coffre de clés.

   - L'option suivante doit être activée si vous avez créé une identité gérée attribuée par l'utilisateur :
     - **Politique d'accès au coffre-fort**
2. Si vous avez sélectionné la stratégie d'accès au coffre-fort, cliquez sur Créer pour créer une stratégie d'accès pour le coffre-fort de clés. Sinon, passez à l'étape 3.
   a. Sélectionnez les autorisations suivantes :
      - obtenir
      - liste
      - décrypter

- crypter
- clé de déballage
- clé d'enveloppement
- vérifier
- signe

b. Sélectionnez l'identité gérée attribuée par l'utilisateur (ressource) comme principal.

c. Réviser et créer la politique d'accès.

3. "Générer une clé dans le coffre de clés" .

   Notez les exigences suivantes pour la clé :

   - Le type de clé doit être **RSA**.
   - La taille de clé RSA recommandée est **2048**, mais d'autres tailles sont prises en charge.

Créer un système qui utilise la clé de chiffrement

Après avoir créé le coffre de clés et généré une clé de chiffrement, vous pouvez créer un nouveau système Cloud Volumes ONTAP configuré pour utiliser la clé. Ces étapes sont prises en charge à l'aide de l'API.

Autorisations requises

Si vous souhaitez utiliser une clé gérée par le client avec un système Cloud Volumes ONTAP à nœud unique, assurez-vous que l'agent de la console dispose des autorisations suivantes :

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Afficher la dernière liste des autorisations"

Étapes

1. Obtenez la liste des coffres de clés de votre abonnement Azure à l'aide de l'appel d'API suivant.

   Pour une paire HA : `GET /azure/ha/metadata/vaults`

   Pour un seul nœud : `GET /azure/vsa/metadata/vaults`

   Prenez note du **nom** et du **resourceGroup**. Vous devrez spécifier ces valeurs à l'étape suivante.

   "En savoir plus sur cet appel d'API" .

2. Obtenez la liste des clés dans le coffre-fort en utilisant l'appel API suivant.

   Pour une paire HA : `GET /azure/ha/metadata/keys-vault`

Pour un nœud unique : `GET /azure/vsa/metadata/keys-vault`

Prenez note du **keyName**. Vous devrez spécifier cette valeur (ainsi que le nom du coffre-fort) à l'étape suivante.

"En savoir plus sur cet appel d'API" .

3. Créez un système Cloud Volumes ONTAP à l'aide de l'appel API suivant.

   a. Pour une paire HA :

      `POST /azure/ha/working-environments`

      Le corps de la requête doit inclure les champs suivants :

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      Inclure le `"userAssignedIdentity": " userAssignedIdentityId"` champ si vous avez créé cette ressource pour être utilisée pour le chiffrement du compte de stockage.

      "En savoir plus sur cet appel d'API" .

   b. Pour un système à nœud unique :

      `POST /azure/vsa/working-environments`

      Le corps de la requête doit inclure les champs suivants :

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      Inclure le `"userAssignedIdentity": " userAssignedIdentityId"` champ si vous avez créé cette ressource pour être utilisée pour le chiffrement du compte de stockage.

   "En savoir plus sur cet appel d'API" .

Résultat

Vous disposez d'un nouveau système Cloud Volumes ONTAP configuré pour utiliser votre clé gérée par le client pour le chiffrement des données.

Configurer les licences pour Cloud Volumes ONTAP dans Azure

Une fois que vous avez décidé quelle option de licence vous souhaitez utiliser avec Cloud Volumes ONTAP, quelques étapes sont nécessaires avant de pouvoir choisir cette option de licence lors de la création d'un nouveau système.

Freemium

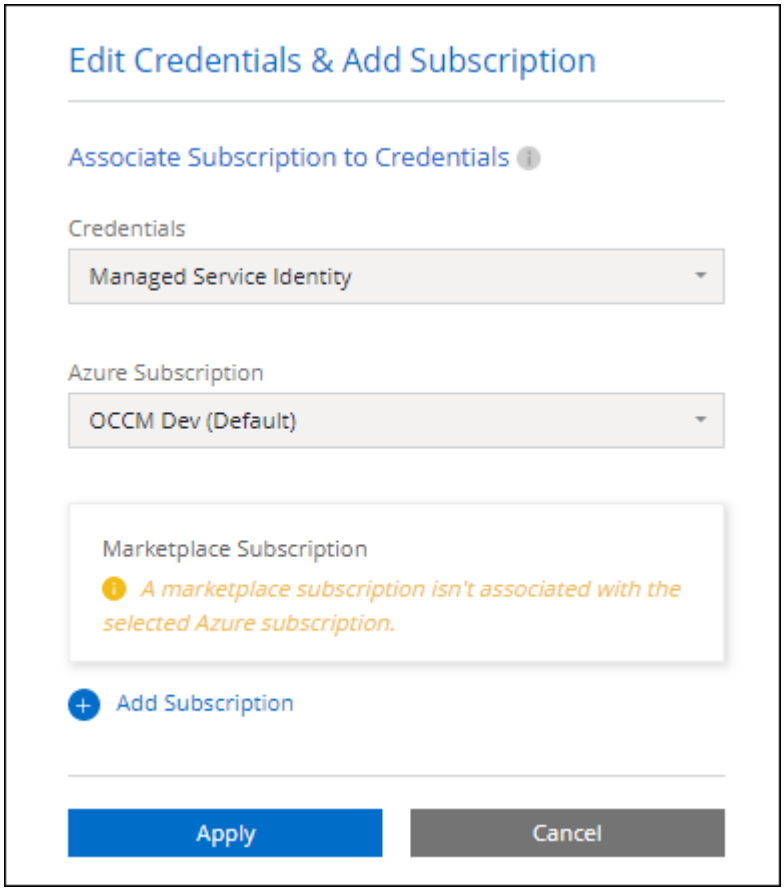
Sélectionnez l'offre Freemium pour utiliser Cloud Volumes ONTAP gratuitement avec jusqu'à 500 Gio de capacité provisionnée. "En savoir plus sur l'offre Freemium" .

Étapes

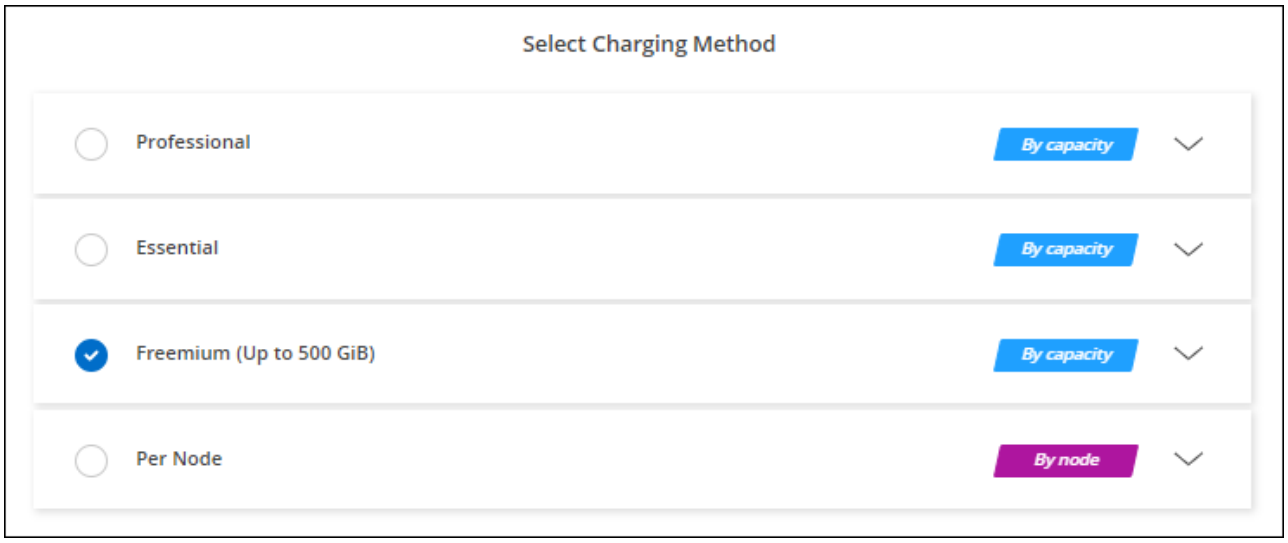
1. Dans le menu de navigation de gauche de la NetApp Console, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

    a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement à l'utilisation sur la Place de marché Azure.

    Vous ne serez pas facturé via l'abonnement du marché à moins que vous ne dépassiez 500 Gio de capacité provisionnée, auquel cas le système est automatiquement converti en"Forfait Essentiel" .



    a. Après être revenu à la console, sélectionnez **Freemium** lorsque vous atteignez la page des méthodes de facturation.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

Licence basée sur la capacité

Les licences basées sur la capacité vous permettent de payer Cloud Volumes ONTAP par Tio de capacité. Les licences basées sur la capacité sont disponibles sous la forme d'un *package* : le package Essentials ou le package Professional.

Les formules Essentiel et Professionnel sont disponibles avec les modèles de consommation ou options d'achat suivants :

- Une licence (apportez votre propre licence (BYOL)) achetée auprès de NetApp
- Un abonnement horaire à la carte (PAYGO) de la Place de marché Azure
- Un contrat annuel

"En savoir plus sur les licences basées sur la capacité" .

Les sections suivantes décrivent comment démarrer avec chacun de ces modèles de consommation.

Apportez votre propre vin

Payez à l'avance en achetant une licence (BYOL) auprès de NetApp pour déployer les systèmes Cloud Volumes ONTAP chez n'importe quel fournisseur de cloud.

NetApp a restreint l'achat, la prolongation et le renouvellement des licences BYOL. Pour plus d'informations, consultez "Disponibilité restreinte des licences BYOL pour Cloud Volumes ONTAP" .

Étapes

1. "Contactez le service commercial NetApp pour obtenir une licence"
2. "Ajoutez votre compte de site de support NetApp à la console"

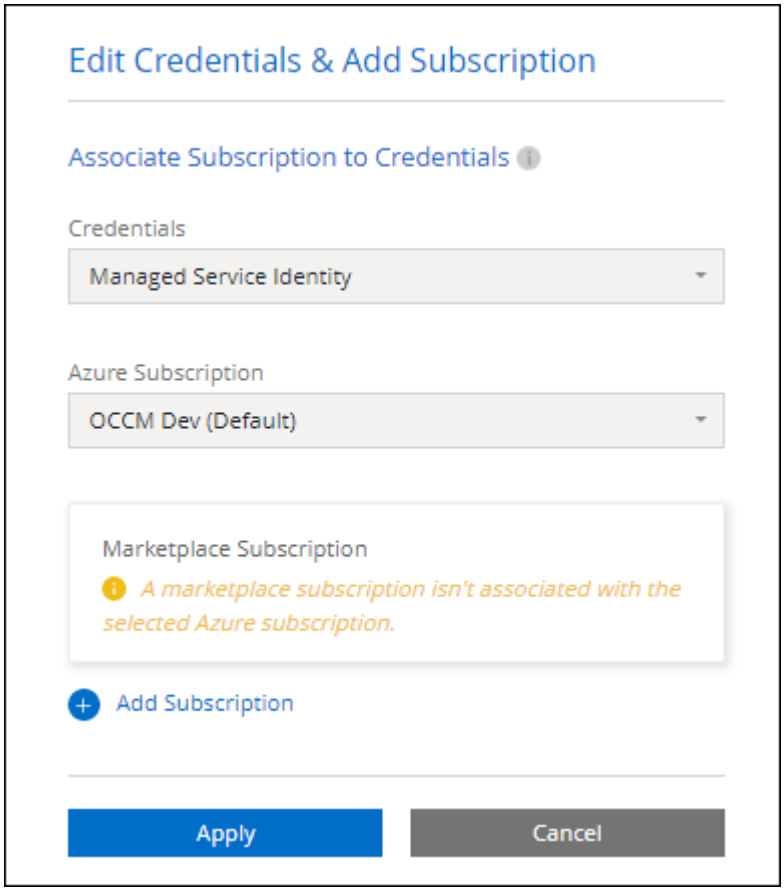
   La console interroge automatiquement le service de licences de NetApp pour obtenir des détails sur les licences associées à votre compte de site de support NetApp . S'il n'y a pas d'erreur, la console ajoute automatiquement les licences à la console.

Votre licence doit être disponible depuis la console avant de pouvoir l'utiliser avec Cloud Volumes ONTAP. Si nécessaire, vous pouvez"ajouter manuellement la licence à la console" .

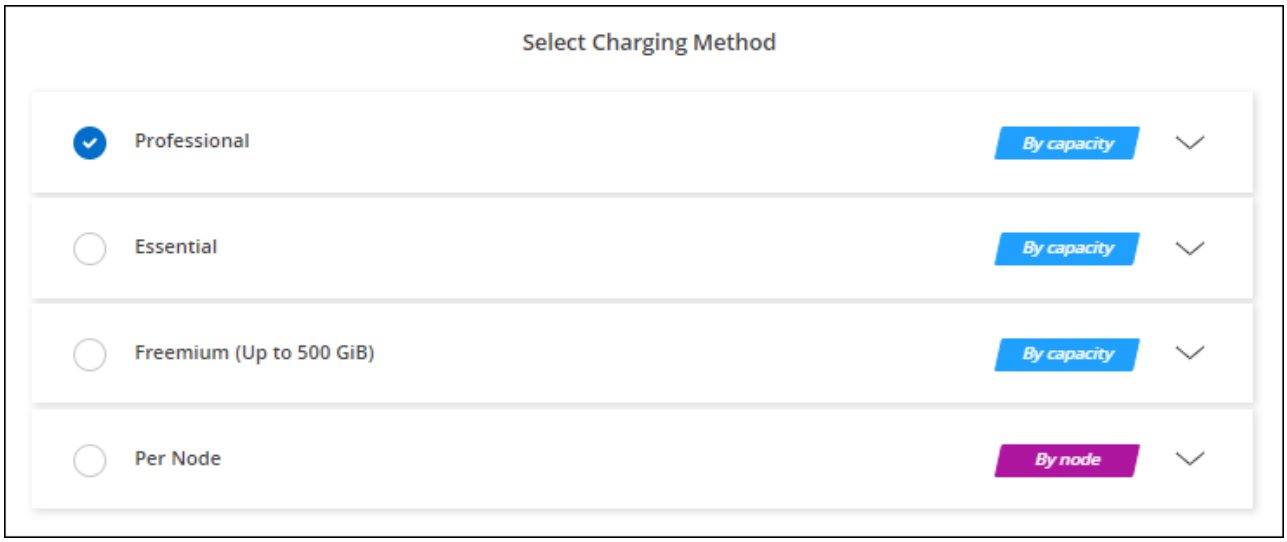
3. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

   a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement à l'utilisation sur la Place de marché Azure.

      La licence que vous avez achetée auprès de NetApp est toujours facturée en premier, mais vous serez facturé au tarif horaire du marché si vous dépassez votre capacité sous licence ou si la durée de votre licence expire.



   a. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

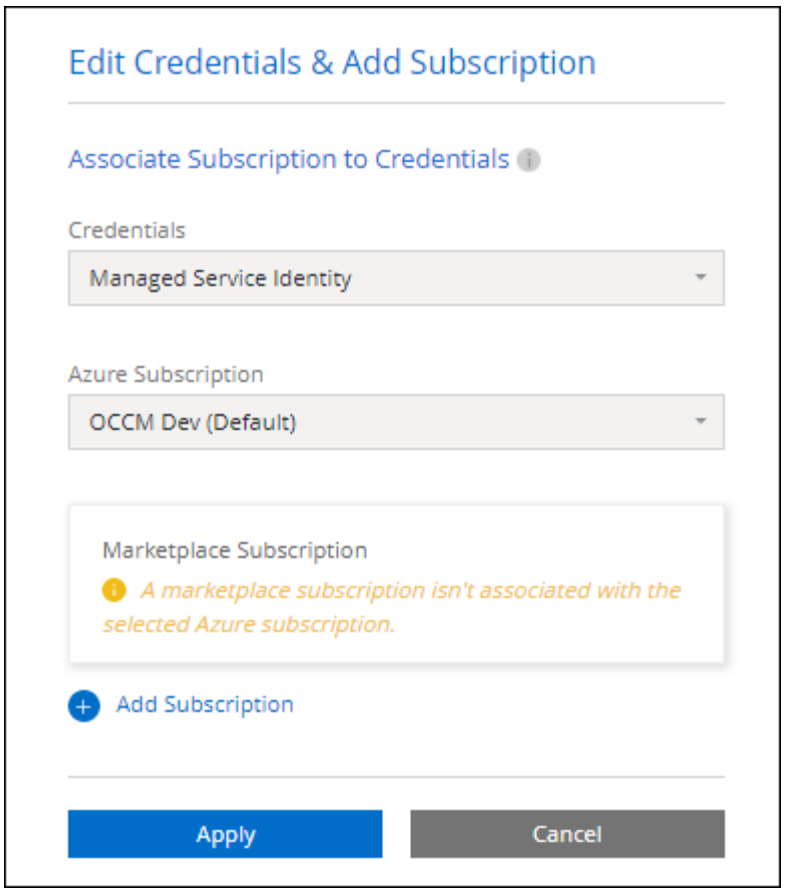
Abonnement PAYGO

Payez à l'heure en souscrivant à l'offre depuis la marketplace de votre fournisseur cloud.

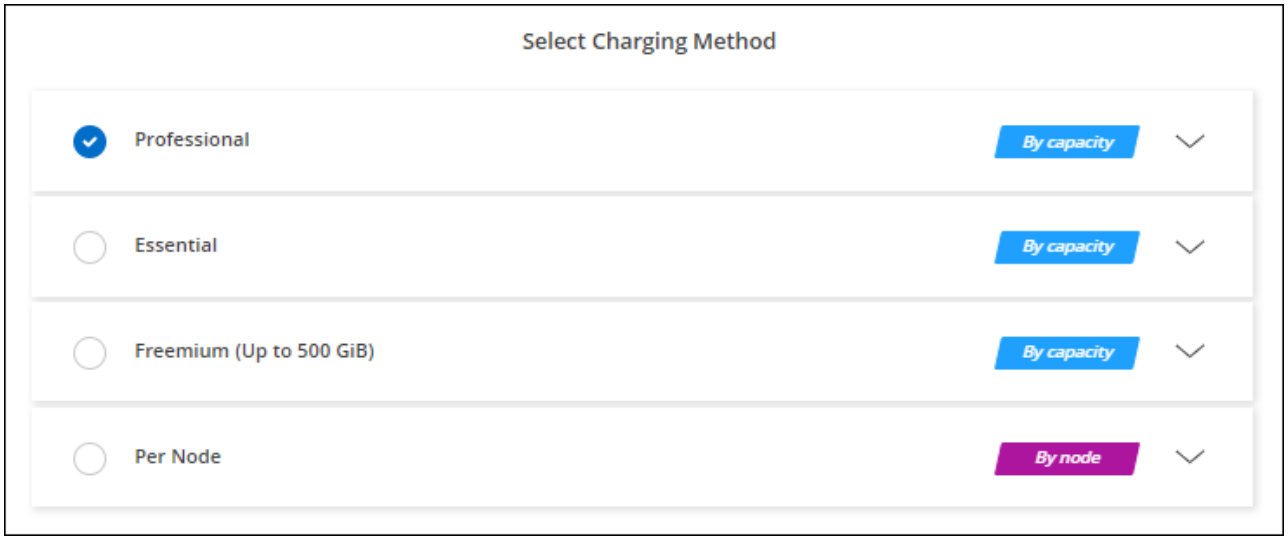
Lorsque vous créez un système Cloud Volumes ONTAP , la console vous invite à vous abonner au contrat disponible sur la Place de marché Azure. Cet abonnement est ensuite associé au système de facturation. Vous pouvez utiliser ce même abonnement pour des systèmes supplémentaires.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
   a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement**, puis suivez les invites pour vous abonner à l'offre de paiement à l'utilisation sur la Place de marché Azure.



b. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

Vous pouvez gérer les abonnements Azure Marketplace associés à vos comptes Azure à partir de la page Paramètres > Informations d'identification. "Apprenez à gérer vos comptes et abonnements Azure"

Contrat annuel

Payez Cloud Volumes ONTAP annuellement en achetant un contrat annuel.

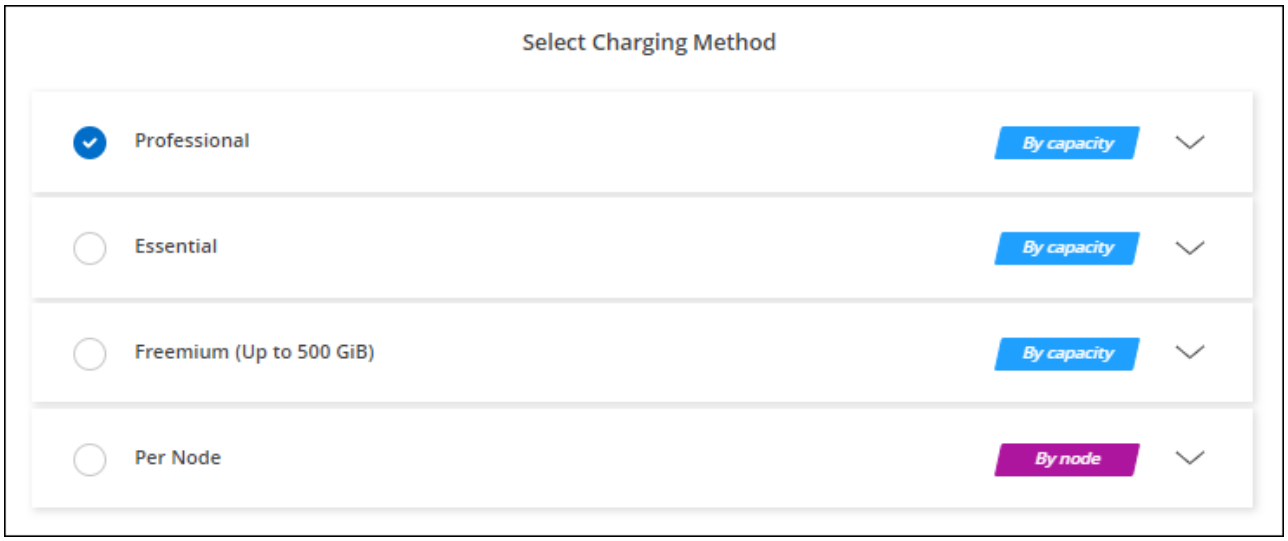
Étapes

1. Contactez votre représentant commercial NetApp pour acheter un contrat annuel.

   Le contrat est disponible sous forme d'offre *privée* sur la Place de marché Azure.

   Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à partir de la Place de marché Azure lors de la création du système.

2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.
   a. Sur la page **Détails et informations d'identification**, cliquez sur **Modifier les informations d'identification > Ajouter un abonnement > Continuer**.
   b. Dans le portail Azure, sélectionnez le plan annuel qui a été partagé avec votre compte Azure, puis cliquez sur **S'abonner**.
   c. Après être revenu à la console, sélectionnez un forfait basé sur la capacité lorsque vous atteignez la page des méthodes de charge.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

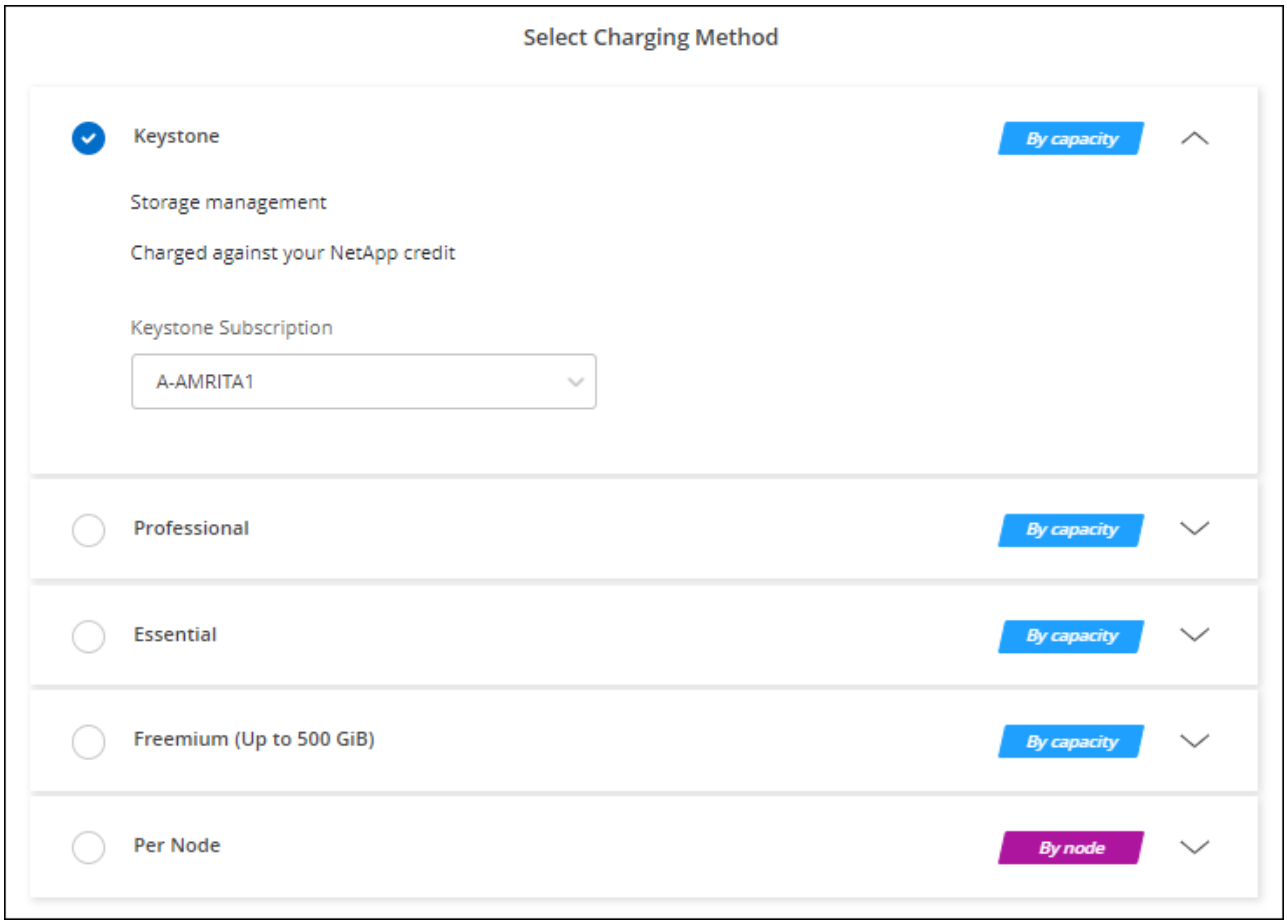
Abonnement Keystone

Un abonnement Keystone est un service d'abonnement à paiement progressif. "En savoir plus sur les abonnements NetApp Keystone" .

Étapes

1. Si vous n'avez pas encore d'abonnement, "contacter NetApp"
2. Contacter NetApp pour autoriser votre compte utilisateur dans la console avec un ou plusieurs abonnements Keystone .
3. Une fois que NetApp a autorisé votre compte,"liez vos abonnements pour les utiliser avec Cloud Volumes ONTAP" .
4. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les étapes.

a. Sélectionnez la méthode de facturation de l'abonnement Keystone lorsque vous êtes invité à choisir une méthode de facturation.



"Consultez les instructions étape par étape pour lancer Cloud Volumes ONTAP dans Azure" .

Licence basée sur les nœuds

Une licence basée sur les nœuds est la licence de génération précédente pour Cloud Volumes ONTAP. Une licence basée sur les nœuds peut être obtenue auprès de NetApp (BYOL) et est disponible pour le renouvellement de licence, uniquement dans des cas spécifiques. Pour plus d'informations, consultez :

- "Fin de disponibilité des licences basées sur des nœuds"
- "Fin de disponibilité des licences basées sur des nœuds"
- "Convertir une licence basée sur les nœuds en une licence basée sur la capacité"

Activer le mode haute disponibilité pour Cloud Volumes ONTAP dans Azure

Il est recommandé d'activer le mode haute disponibilité (HA) de Microsoft Azure afin de réduire les temps de basculement imprévus et d'activer la prise en charge de NFSv4 pour Cloud Volumes ONTAP. Si vous activez ce mode, vos nœuds Cloud Volumes ONTAP HA peuvent atteindre un objectif de temps de récupération (RTO) faible (60 secondes) lors de basculements imprévus sur les clients CIFS et NFSv4.

À partir de Cloud Volumes ONTAP 9.10.1, nous avons réduit le temps de basculement non planifié pour les paires Cloud Volumes ONTAP HA exécutées dans Microsoft Azure et ajouté la prise en charge de NFSv4. Pour rendre ces améliorations disponibles pour Cloud Volumes ONTAP, vous devez activer la fonctionnalité de haute disponibilité sur votre abonnement Azure.

À propos de cette tâche

NetApp Console vous invite à fournir ces informations lorsque la fonctionnalité doit être activée sur un abonnement Azure. Notez les points suivants :

- Il n'y a aucun problème avec la haute disponibilité de votre paire Cloud Volumes ONTAP HA. Cette fonctionnalité Azure fonctionne de concert avec ONTAP pour réduire le temps d'interruption d'application observé par le client pour les protocoles NFS résultant d'événements de basculement non planifiés.
- L'activation de cette fonctionnalité n'interrompt pas les paires Cloud Volumes ONTAP HA.
- L'activation de cette fonctionnalité sur votre abonnement Azure ne pose aucun problème aux autres machines virtuelles.
- Cloud Volumes ONTAP utilise un équilibreur de charge Azure interne lors des basculements des LIF de gestion de cluster et de SVM sur les clients CIFS et NFS.
- Lorsque le mode HA est activé, la console analyse le système toutes les 12 heures pour mettre à jour les règles internes d'Azure Load Balancer.

Étapes

Un utilisateur Azure disposant des privilèges *Owner* peut activer la fonctionnalité à partir de l'Azure CLI.

1. "Accéder à Azure Cloud Shell depuis le portail Azure"
2. Enregistrer la fonctionnalité du mode haute disponibilité :

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Vérifiez éventuellement que la fonctionnalité est désormais enregistrée :

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

L'interface de ligne de commande Azure doit renvoyer un résultat similaire au suivant :

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Liens connexes

1. "Documentation Microsoft Azure : vue d'ensemble des ports à haute disponibilité"
2. "Microsoft Azure documentation : Premiers pas avec Azure CLI"

Activer VMOrchestratorZonalMultiFD pour Cloud Volumes ONTAP dans Azure

Pour déployer des instances de machine virtuelle dans des zones de disponibilité unique (AZ) de stockage localement redondant (LRS), vous devez activer Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` fonctionnalité pour vos abonnements. En mode haute disponibilité (HA), cette fonctionnalité facilite le déploiement de nœuds dans des domaines de pannes distincts dans la même zone de disponibilité.

À moins que vous n'activiez cette fonctionnalité, le déploiement zonal ne se produit pas et le déploiement non zonal LRS précédent devient effectif.

Pour plus d'informations sur le déploiement de machines virtuelles dans une zone de disponibilité unique, reportez-vous à"Paires à haute disponibilité dans Azure" .

Effectuez ces étapes en tant qu'utilisateur avec des privilèges « Propriétaire » :

Étapes

1. Accédez à Azure Cloud Shell depuis le portail Azure. Pour plus d'informations, reportez-vous à la "Documentation Microsoft Azure : Prise en main d'Azure Cloud Shell" .
2. Inscrivez-vous au `Microsoft.Compute/VMOrchestratorZonalMultiFD` fonctionnalité en exécutant cette commande :

   ```
   az account set -s <nom_ou_ID_d'abonnement_Azure> az feature register --name
   VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Vérifiez l'état d'enregistrement et l'échantillon de sortie :

az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/subscriptions/<*ID*>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "Registered" }, "type": "Microsoft.Features/providers/features" }

Lancer Cloud Volumes ONTAP dans Azure

Vous pouvez lancer un système à nœud unique ou une paire haute disponibilité dans Azure en créant un système Cloud Volumes ONTAP dans NetApp Console.

Avant de commencer

Vous avez besoin des éléments suivants avant de commencer.

- Un agent de console opérationnel.
  - Vous devriez avoir un "Agent de console associé à votre système" .
  - "Vous devez être prêt à laisser l'agent de la console en cours d'exécution à tout moment." .
- Une compréhension de la configuration que vous souhaitez utiliser.

  Vous devez avoir une configuration planifiée et les détails de mise en réseau Azure nécessaires auprès de votre administrateur. Pour plus d'informations, reportez-vous à "Planification de votre configuration Cloud Volumes ONTAP" .
- Une compréhension de ce qui est nécessaire pour configurer les licences pour Cloud Volumes ONTAP.

  "Apprenez à configurer les licences" .

À propos de cette tâche

Lorsque la console crée un système Cloud Volumes ONTAP dans Azure, elle crée plusieurs objets Azure, tels qu'un groupe de ressources, des interfaces réseau et des comptes de stockage. Vous pouvez consulter un résumé des ressources à la fin de l'assistant.

Risque de perte de données

La meilleure pratique consiste à utiliser un nouveau groupe de ressources dédié pour chaque système Cloud Volumes ONTAP .

Le déploiement de Cloud Volumes ONTAP dans un groupe de ressources partagé existant n'est pas recommandé en raison du risque de perte de données. Bien que la console puisse supprimer les ressources Cloud Volumes ONTAP d'un groupe de ressources partagé en cas d'échec de déploiement ou de suppression, un utilisateur Azure peut supprimer accidentellement les ressources Cloud Volumes ONTAP d'un groupe de ressources partagé.

Lancer un système Cloud Volumes ONTAP à nœud unique dans Azure

Si vous souhaitez lancer un système Cloud Volumes ONTAP à nœud unique dans Azure, vous devez créer un système à nœud unique dans la Console.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.

2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. **Choisissez un emplacement** : sélectionnez **Microsoft Azure** et * Cloud Volumes ONTAP Single Node*.
4. Si vous y êtes invité, "créer un agent de console" .
5. **Détails et informations d'identification** : Modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, puis spécifiez les informations d'identification.

   Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Balises du groupe de ressources	Les balises sont des métadonnées pour vos ressources Azure. Lorsque vous entrez des balises dans ce champ, la console les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP . Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les étiquettes, veuillez consulter le "Documentation Microsoft Azure : Utilisation de balises pour organiser vos ressources Azure" .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut *admin* ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier les informations d'identification	Vous pouvez choisir différentes informations d'identification Azure et un abonnement Azure différent à utiliser avec ce système Cloud Volumes ONTAP . Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné afin de déployer un système Cloud Volumes ONTAP à la carte. "Apprenez à ajouter des informations d'identification" .

6. **Services** : activez ou désactivez les services individuels que vous souhaitez ou ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
   - "En savoir plus sur la NetApp Data Classification"
   - "En savoir plus sur NetApp Backup and Recovery"

   Si vous souhaitez utiliser WORM et la hiérarchisation des données, vous devez désactiver la sauvegarde et la récupération et déployer un système Cloud Volumes ONTAP avec la version 9.8 ou supérieure.

7. **Emplacement** : sélectionnez une région, une zone de disponibilité, un réseau virtuel et un sous-réseau, puis cochez la case pour confirmer la connectivité réseau entre l'agent de la console et l'emplacement cible.

Pour les régions de Chine, les déploiements à nœud unique sont pris en charge uniquement dans Cloud Volumes ONTAP 9.12.1 GA et 9.13.0 GA. Vous pouvez mettre à niveau ces versions vers des correctifs et des versions ultérieurs de Cloud Volumes ONTAP comme"pris en charge dans Azure" . Si vous souhaitez déployer des versions ultérieures de Cloud Volumes ONTAP dans les régions chinoises, contactez le support NetApp . Seules les licences achetées directement auprès de NetApp sont prises en charge dans les régions chinoises ; les abonnements au marché ne sont pas disponibles.

8. **Connectivité** : Choisissez un groupe de ressources nouveau ou existant, puis choisissez d'utiliser le groupe de sécurité prédéfini ou le vôtre.

   Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Groupe de ressources	Créez un nouveau groupe de ressources pour Cloud Volumes ONTAP ou utilisez un groupe de ressources existant. La meilleure pratique consiste à utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Bien qu'il soit possible de déployer Cloud Volumes ONTAP dans un groupe de ressources partagé existant, cela n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails. Si le compte Azure que vous utilisez possède le "autorisations requises" , la console supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec de déploiement ou de suppression.
Groupe de sécurité généré	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **Réseau virtuel sélectionné uniquement**, la source du trafic entrant est la plage de sous-réseaux du réseau virtuel sélectionné et la plage de sous-réseaux du réseau virtuel sur lequel réside l'agent de la console. C'est l'option recommandée. • Si vous choisissez **Tous les réseaux virtuels**, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP . "Afficher le groupe de sécurité par défaut" .

9. * Méthodes de facturation et compte NSS * : spécifiez l'option de facturation que vous souhaitez utiliser avec ce système, puis spécifiez un compte de site de support NetApp .
   - "En savoir plus sur les options de licence pour Cloud Volumes ONTAP" .
   - "Apprenez à configurer les licences" .
10. **Packages préconfigurés** : sélectionnez l'un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

    Si vous choisissez l'un des packages, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.

11. **Licence** : modifiez la version de Cloud Volumes ONTAP si nécessaire et sélectionnez un type de machine virtuelle.

    Si une version candidate à la publication, une version de disponibilité générale ou une version de correctif plus récente est disponible pour la version sélectionnée, BlueXP met à jour le système vers cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.16.1 P3 et 9.16.1 P4 est disponible. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.15 à la version 9.16.

12. **S'abonner depuis la Place de marché Azure** : cette page s'affiche si la console n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP. Suivez les étapes indiquées à l'écran. se référer à "Déploiement programmatique des produits Marketplace" pour plus d'informations.
13. **Ressources de stockage sous-jacentes** : choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données vers le stockage Blob doit être activée.

    Notez ce qui suit :

    - Si l'accès public à votre compte de stockage est désactivé dans le VNet, vous ne pouvez pas activer la hiérarchisation des données dans votre système Cloud Volumes ONTAP . Pour plus d'informations, reportez-vous à"Règles du groupe de sécurité" .
    - Le type de disque correspond au volume initial. Vous pouvez choisir un type de disque différent pour les volumes suivants.
    - La taille du disque concerne tous les disques de l'agrégat initial et tous les agrégats supplémentaires créés par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix d'un type et d'une taille de disque, reportez-vous à"Dimensionnement de votre système dans Azure" .

    - Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants.

      "En savoir plus sur la hiérarchisation des données" .

14. **Vitesse d'écriture et WORM** :

    a. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

       "En savoir plus sur la vitesse d'écriture" .

    b. Activez le stockage WORM (écriture unique, lecture multiple), si vous le souhaitez.

       Cette option n'est disponible que pour certains types de machines virtuelles. Pour savoir quels types de machines virtuelles sont pris en charge, reportez-vous à"Configurations prises en charge par licence pour les paires HA" .

       WORM ne peut pas être activé si la hiérarchisation des données a été activée pour les versions 9.7 et inférieures de Cloud Volumes ONTAP . Le retour ou la rétrogradation vers Cloud Volumes ONTAP 9.8 est bloqué après l'activation de WORM et de la hiérarchisation.

"En savoir plus sur le stockage WORM" .

a. Si vous activez le stockage WORM, sélectionnez la période de conservation.

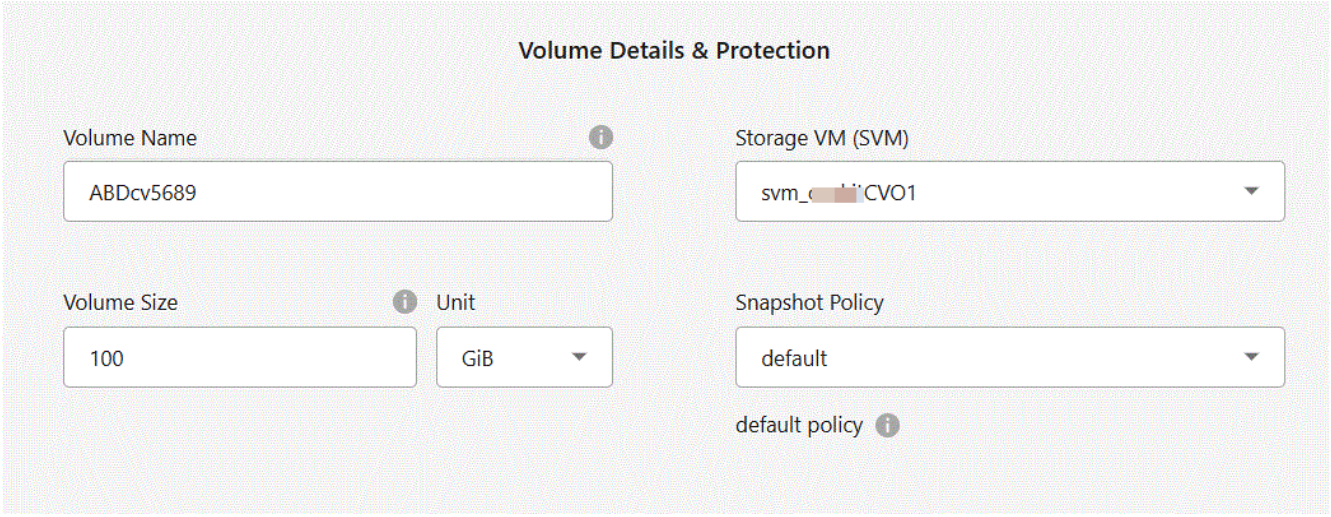
15. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

"En savoir plus sur les protocoles et versions clients pris en charge" .

Certains champs de cette page sont explicites. Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation ou non du provisionnement dynamique, qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une politique d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, la console entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur en utilisant le format domaine\nom d'utilisateur.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes d'initiateurs sont des tables de noms de nœuds d'hôtes iSCSI et contrôlent quels initiateurs ont accès à quels LUN. Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



16. **Configuration CIFS** : Si vous avez choisi le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Pour configurer Azure AD Domain Services comme serveur AD pour Cloud Volumes ONTAP, vous devez saisir **OU=AADDC Computers** ou **OU=AADDC Users** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : Créer une unité d'organisation (UO) dans un domaine géré par Azure AD Domain Services"^]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est le même que le domaine AD.
Serveur NTP	Sélectionnez **Utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la "Documentation sur l'automatisation de la NetApp Console" pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

17. **Profil d'utilisation, type de disque et politique de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifier la politique de hiérarchisation des volumes, si

nécessaire.

Pour plus d'informations, reportez-vous à"Comprendre les profils d'utilisation du volume" et"Présentation de la hiérarchisation des données" .

18. **Réviser et approuver** : Révisez et confirmez vos sélections.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **Plus d'informations** pour consulter les détails sur le support et les ressources Azure que la console achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Aller**.

Résultat

La console déploie le système Cloud Volumes ONTAP . Vous pouvez suivre la progression sur la page Audit.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP , consultez le message d'échec. Vous pouvez également sélectionner le système et cliquer sur **Recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, rendez-vous sur "Prise en charge de NetApp Cloud Volumes ONTAP" .

Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Azure, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

Après avoir terminé

- Si vous avez provisionné un partage CIFS, accordez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP .

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Lancer une paire Cloud Volumes ONTAP HA dans Azure

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans Azure, vous devez créer un système HA dans la console.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Stockage > Gestion**.
2. Sur la page **Systèmes**, cliquez sur **Ajouter un système** et suivez les instructions.
3. Si vous y êtes invité, "créer un agent de console" .
4. **Détails et informations d'identification** : Modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster, ajoutez des balises si nécessaire, puis spécifiez les informations d'identification.

   Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Nom du système	La console utilise le nom du système pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Balises du groupe de ressources	Les balises sont des métadonnées pour vos ressources Azure. Lorsque vous entrez des balises dans ce champ, la console les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP . Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un système, puis vous pouvez en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un système. Pour plus d'informations sur les étiquettes, veuillez consulter le "Documentation Microsoft Azure : Utilisation de balises pour organiser vos ressources Azure" .
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte administrateur du cluster Cloud Volumes ONTAP . Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via ONTAP System Manager ou l'interface de ligne de commande ONTAP . Conservez le nom d'utilisateur par défaut *admin* ou remplacez-le par un nom d'utilisateur personnalisé.
Modifier les informations d'identification	Vous pouvez choisir différentes informations d'identification Azure et un abonnement Azure différent à utiliser avec ce système Cloud Volumes ONTAP . Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné afin de déployer un système Cloud Volumes ONTAP à la carte. "Apprenez à ajouter des informations d'identification" .

5. **Services** : activez ou désactivez les services individuels selon que vous souhaitez les utiliser avec Cloud Volumes ONTAP.
   - "En savoir plus sur la NetApp Data Classification"
   - "En savoir plus sur NetApp Backup and Recovery"

   Si vous souhaitez utiliser WORM et la hiérarchisation des données, vous devez désactiver la sauvegarde et la récupération et déployer un système Cloud Volumes ONTAP avec la version 9.8 ou supérieure.

6. **Modèles de déploiement HA**:
   a. Sélectionnez **Zone de disponibilité unique** ou **Zone de disponibilité multiple**.
      - Pour les zones de disponibilité uniques, sélectionnez une région Azure, une zone de disponibilité, un réseau virtuel et un sous-réseau.

        À partir de Cloud Volumes ONTAP 9.15.1, vous pouvez déployer des instances de machine virtuelle (VM) en mode HA dans des zones de disponibilité uniques (AZ) dans Azure. Vous devez sélectionner une zone et une région qui prennent en charge ce déploiement. Si la zone ou la région ne prend pas en charge le déploiement zonal, le mode de déploiement non zonal précédent pour LRS est suivi. Pour comprendre les configurations prises en charge pour les disques gérés partagés, reportez-vous à"Configuration de zone de disponibilité unique HA avec disques gérés partagés" .

      - Pour plusieurs zones de disponibilité, sélectionnez une région, un réseau virtuel, un sous-réseau, une zone pour le nœud 1 et une zone pour le nœud 2.

   b. Cochez la case **J'ai vérifié la connectivité réseau…**.

7. **Connectivité** : Choisissez un groupe de ressources nouveau ou existant, puis choisissez d'utiliser le groupe de sécurité prédéfini ou le vôtre.

   Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Groupe de ressources	Créez un nouveau groupe de ressources pour Cloud Volumes ONTAP ou utilisez un groupe de ressources existant. La meilleure pratique consiste à utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Bien qu'il soit possible de déployer Cloud Volumes ONTAP dans un groupe de ressources partagé existant, cela n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails. Vous devez utiliser un groupe de ressources dédié pour chaque paire Cloud Volumes ONTAP HA que vous déployez dans Azure. Une seule paire HA est prise en charge dans un groupe de ressources. La console rencontre des problèmes de connexion si vous essayez de déployer une deuxième paire Cloud Volumes ONTAP HA dans un groupe de ressources Azure. Si le compte Azure que vous utilisez possède le "autorisations requises" , la console supprime les ressources Cloud Volumes ONTAP d'un groupe de ressources, en cas d'échec de déploiement ou de suppression.
Groupe de sécurité généré	Si vous laissez la console générer le groupe de sécurité pour vous, vous devez choisir comment vous autoriserez le trafic : • Si vous choisissez **Réseau virtuel sélectionné uniquement**, la source du trafic entrant est la plage de sous-réseaux du réseau virtuel sélectionné et la plage de sous-réseaux du réseau virtuel sur lequel réside l'agent de la console. C'est l'option recommandée. • Si vous choisissez **Tous les réseaux virtuels**, la source du trafic entrant est la plage IP 0.0.0.0/0.
Utiliser l'existant	Si vous choisissez un groupe de sécurité existant, il doit répondre aux exigences de Cloud Volumes ONTAP . "Afficher le groupe de sécurité par défaut" .

8. * Méthodes de facturation et compte NSS * : spécifiez l'option de facturation que vous souhaitez utiliser avec ce système, puis spécifiez un compte de site de support NetApp .
   - "En savoir plus sur les options de licence pour Cloud Volumes ONTAP" .
   - "Apprenez à configurer les licences" .
9. **Packages préconfigurés** : sélectionnez l'un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Modifier la configuration**.

   Si vous choisissez l'un des packages, il vous suffit de spécifier un volume, puis de vérifier et d'approuver la configuration.

10. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins et sélectionnez un type de machine virtuelle.

Si une version candidate à la publication, une version de disponibilité générale ou une version de correctif plus récente est disponible pour la version sélectionnée, la console met à jour le système vers cette version lors de sa création. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.13.1 et 9.13.1 P4 est disponible. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.13 à la version 9.14.

11. **Abonnez-vous depuis la Place de marché Azure** : suivez les étapes si la console n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP.
12. **Ressources de stockage sous-jacentes** : choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données vers le stockage Blob doit être activée.

    Notez ce qui suit :

    - La taille du disque concerne tous les disques de l'agrégat initial et tous les agrégats supplémentaires créés par la console lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente en utilisant l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix d'une taille de disque, reportez-vous à"Dimensionnez votre système dans Azure" .

    - Si l'accès public à votre compte de stockage est désactivé dans le VNet, vous ne pouvez pas activer la hiérarchisation des données dans votre système Cloud Volumes ONTAP . Pour plus d'informations, reportez-vous à"Règles du groupe de sécurité" .
    - Vous pouvez choisir une stratégie de hiérarchisation de volume spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez la hiérarchisation des données, vous pouvez l'activer sur les agrégats suivants.

      "En savoir plus sur la hiérarchisation des données" .

    - À partir de Cloud Volumes ONTAP 9.15.0P1, les blobs de pages Azure ne sont plus pris en charge pour les nouveaux déploiements de paires haute disponibilité. Si vous utilisez actuellement des blobs de pages Azure dans des déploiements de paires haute disponibilité existants, vous pouvez migrer vers des types d'instances de machine virtuelle plus récents dans les machines virtuelles des séries Edsv4 et Edsv5.

      "En savoir plus sur les configurations prises en charge dans Azure" .

13. **Vitesse d'écriture et WORM** :

    a. Choisissez une vitesse d'écriture **Normale** ou **Élevée**, si vous le souhaitez.

       "En savoir plus sur la vitesse d'écriture" .

    b. Activez le stockage WORM (écriture unique, lecture multiple), si vous le souhaitez.

       Cette option n'est disponible que pour certains types de machines virtuelles. Pour savoir quels types de machines virtuelles sont pris en charge, reportez-vous à"Configurations prises en charge par licence pour les paires HA" .

       WORM ne peut pas être activé si la hiérarchisation des données a été activée pour les versions 9.7 et inférieures de Cloud Volumes ONTAP . Le retour ou la rétrogradation vers Cloud Volumes ONTAP 9.8

est bloqué après l'activation de WORM et de la hiérarchisation.

"En savoir plus sur le stockage WORM" .

a. Si vous activez le stockage WORM, sélectionnez la période de conservation.

14. * Communication sécurisée avec le stockage et WORM * : choisissez d'activer ou non une connexion HTTPS aux comptes de stockage Azure et d'activer le stockage WORM (écriture unique, lecture multiple), si vous le souhaitez.

    La connexion HTTPS provient d'une paire Cloud Volumes ONTAP 9.7 HA vers des comptes de stockage d'objets blob de pages Azure. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé le système.

    "En savoir plus sur le stockage WORM" .

    WORM ne peut pas être activé si la hiérarchisation des données a été activée.

    "En savoir plus sur le stockage WORM" .

15. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

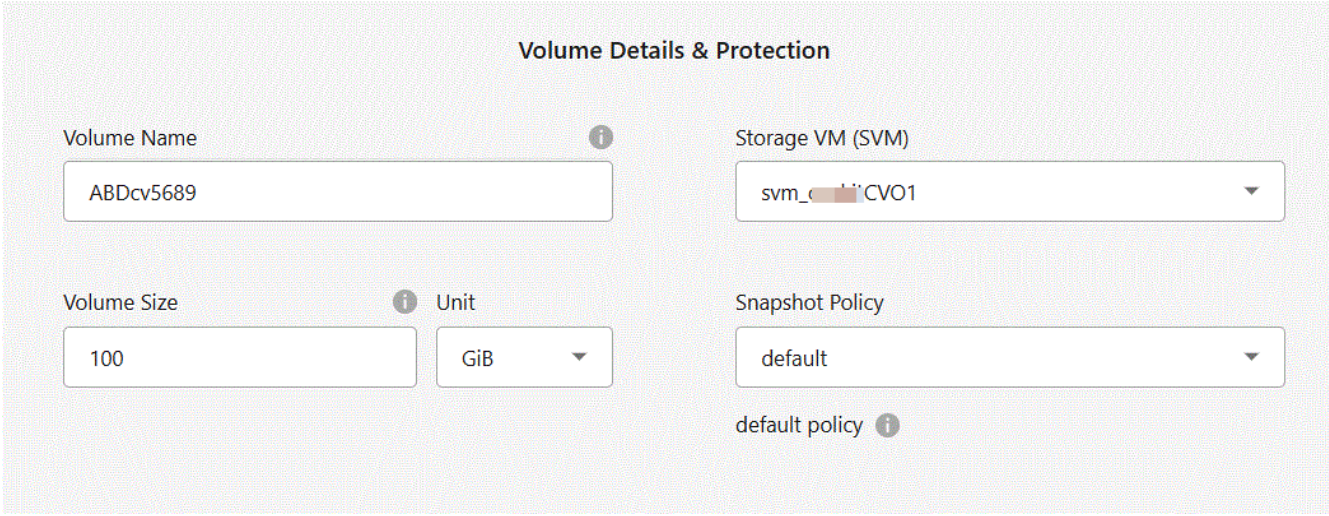
    "En savoir plus sur les protocoles et versions clients pris en charge" .

    Certains champs de cette page sont explicites. Le tableau suivant décrit les domaines pour lesquels vous pourriez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation ou non du provisionnement dynamique, qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une politique d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, la console entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur en utilisant le format domaine\nom d'utilisateur.
Politique d'instantané	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot NetApp créées automatiquement. Une copie NetApp Snapshot est une image de système de fichiers à un instant T qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la politique par défaut ou aucune. Vous pouvez choisir « aucun » pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.

Champ	Description
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes d'initiateurs sont des tables de noms de nœuds d'hôtes iSCSI et contrôlent quels initiateurs ont accès à quels LUN. Les cibles iSCSI se connectent au réseau via des adaptateurs réseau Ethernet standard (NIC), des cartes de moteur de déchargement TCP (TOE) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de bus hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, la console crée automatiquement un LUN pour vous. Nous avons simplifié les choses en créant un seul LUN par volume, il n'y a donc aucune gestion impliquée. Après avoir créé le volume,"utilisez l'IQN pour vous connecter au LUN depuis vos hôtes" .

L'image suivante montre la première page de l'assistant de création de volume :



16. **Configuration CIFS** : Si vous avez choisi le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP primaire et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires pour localiser les serveurs LDAP Active Directory et les contrôleurs de domaine pour le domaine auquel le serveur CIFS rejoindra.
Domaine Active Directory à rejoindre	Le nom de domaine complet du domaine Active Directory (AD) auquel vous souhaitez que le serveur CIFS se joigne.
Informations d'identification autorisées pour rejoindre le domaine	Le nom et le mot de passe d'un compte Windows avec des privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation (UO) spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Un nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	L'unité organisationnelle au sein du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Ordinateurs. Pour configurer Azure AD Domain Services comme serveur AD pour Cloud Volumes ONTAP, vous devez saisir **OU=AADDC Computers** ou **OU=AADDC Users** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : Créer une unité d'organisation (UO) dans un domaine géré par Azure AD Domain Services"^]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est le même que le domaine AD.
Serveur NTP	Sélectionnez **Utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une adresse différente, vous devez utiliser l'API. Se référer à la "Documentation sur l'automatisation de la NetApp Console" pour plus de détails. Notez que vous ne pouvez configurer un serveur NTP que lors de la création d'un serveur CIFS. Il n'est pas configurable après avoir créé le serveur CIFS.

17. **Profil d'utilisation, type de disque et politique de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifier la politique de hiérarchisation des volumes, si nécessaire.

    Pour plus d'informations, reportez-vous à"Choisissez un profil d'utilisation du volume" ,"Présentation de la hiérarchisation des données" , et "KB : Quelles fonctionnalités d'efficacité du stockage en ligne sont prises en charge avec CVO ?"

18. **Réviser et approuver** : Révisez et confirmez vos sélections.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **Plus d'informations** pour consulter les détails sur le support et les ressources Azure que la console achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Aller**.

Résultat

La console déploie le système Cloud Volumes ONTAP . Vous pouvez suivre la progression sur la page Audit.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP , consultez le message d'échec. Vous pouvez également sélectionner le système et cliquer sur **Recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, rendez-vous sur "Prise en charge de NetApp Cloud Volumes ONTAP" .

Après avoir terminé

- Si vous avez provisionné un partage CIFS, accordez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez ONTAP System Manager ou l'interface de ligne de commande ONTAP .

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Une fois le processus de déploiement terminé, ne modifiez pas les configurations Cloud Volumes ONTAP générées par le système dans le portail Azure, en particulier les balises système. Toute modification apportée à ces configurations peut entraîner un comportement inattendu ou une perte de données.

Liens connexes

*"Planification de votre configuration Cloud Volumes ONTAP dans Azure" *"Déployer Cloud Volumes ONTAP dans Azure depuis la Place de marché Azure"

Vérifier l'image de la plateforme Azure

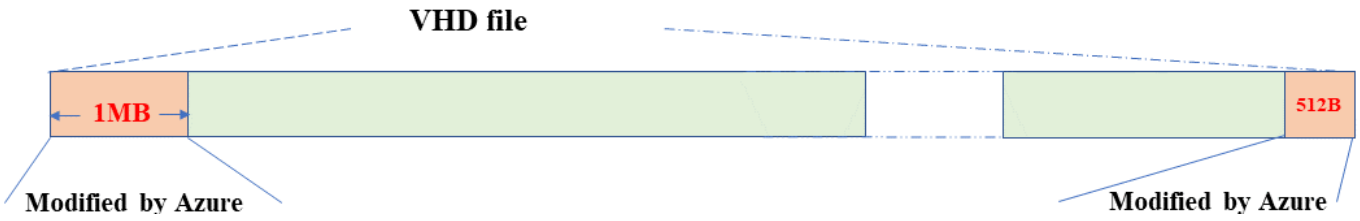
Vérification d'image de la place de marché Azure pour Cloud Volumes ONTAP

La vérification des images Azure est conforme aux exigences de sécurité renforcées de NetApp . La vérification d'un fichier image est un processus simple. Cependant, la vérification de la signature de l'image Azure nécessite des considérations spécifiques pour le fichier image Azure VHD, car il est modifié sur la place de marché Azure.

La vérification d'image Azure est prise en charge sur Cloud Volumes ONTAP 9.15.0 et versions ultérieures.

Modification des fichiers VHD publiés par Azure

Les 1 Mo (1048576 octets) au début et les 512 octets à la fin du fichier VHD sont modifiés par Azure. NetApp signe le fichier VHD restant.



Dans l'exemple, le fichier VHD est de 10 Go. La partie signée par NetApp est marquée en vert (10 Go - 1 Mo - 512 octets).

Liens connexes

- "Blog sur les erreurs de page : Comment signer et vérifier avec OpenSSL"
- "Utiliser l'image Azure Marketplace pour créer une image de machine virtuelle pour votre GPU Azure Stack Edge Pro | Microsoft Learn"
- "Exporter/copier un disque géré vers un compte de stockage via Azure CLI | Microsoft Learn"
- "Démarrage rapide d'Azure Cloud Shell - Bash | Microsoft Learn"
- "Comment installer Azure CLI | Microsoft Learn"
- "Copie de blob de stockage AZ | Microsoft Learn"
- "Sign in avec Azure CLI — Connexion et authentification | Microsoft Learn"

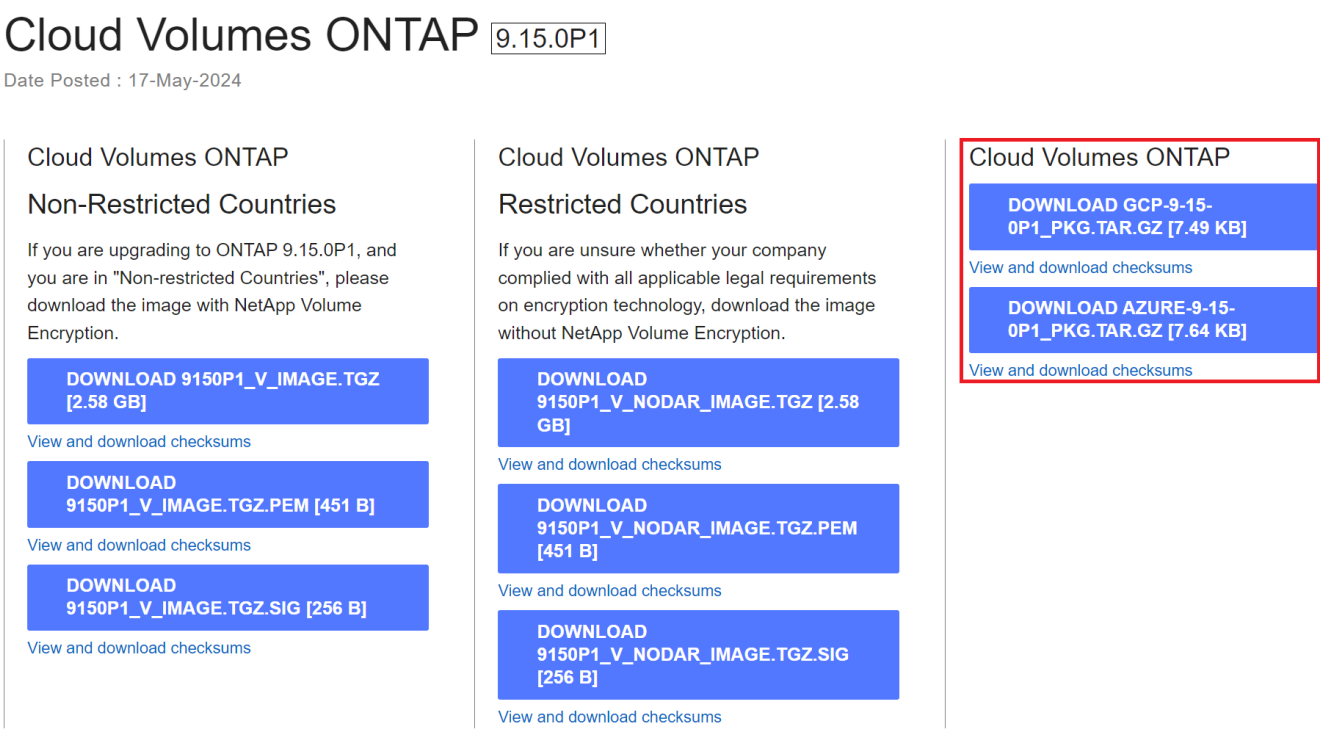
Téléchargez le fichier image Azure pour Cloud Volumes ONTAP

Vous pouvez télécharger le fichier image Azure à partir du "Site de support NetApp" .

Le fichier *tar.gz* contient les fichiers nécessaires à la vérification de la signature de l'image. En plus du fichier *tar.gz*, vous devez également télécharger le fichier *checksum* de l'image. Le fichier de somme de contrôle contient le `md5` et `sha256` sommes de contrôle du fichier *tar.gz*.

Étapes

1. Aller à la "Page produit Cloud Volumes ONTAP sur le site de support NetApp" et téléchargez la version du logiciel requise à partir de la section **Téléchargements**.
2. Sur la page de téléchargement de Cloud Volumes ONTAP , cliquez sur le fichier téléchargeable pour l'image Azure et téléchargez le fichier *tar.gz*.



3. Sous Linux, exécutez `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Sur macOS, exécutez `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Vérifiez que le `md5sum` et `sha256sum` les valeurs correspondent à celles de l'image Azure téléchargée.
5. Sous Linux et macOS, extrayez le fichier *tar.gz* à l'aide de la commande `tar -xzf` commande.

   Le fichier *tar.gz* extrait contient le fichier digest (*.sig*), le fichier de certificat de clé publique (*.pem*) et le fichier de certificat de chaîne (*.pem*).

   Exemple de sortie après extraction du fichier tar.gz :

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Exporter des images VHD pour Cloud Volumes ONTAP depuis la place de marché Azure

Une fois l'image VHD publiée sur le cloud Azure, elle n'est plus gérée par NetApp. Au lieu de cela, l'image publiée est placée sur la place de marché Azure. Lorsque l'image est préparée et publiée sur la place de marché Azure, Azure modifie 1 Mo au début et 512 octets à la fin du VHD. Pour vérifier la signature du fichier VHD, vous devez exporter l'image VHD modifiée par Azure à partir de la place de marché Azure.

Avant de commencer

Assurez-vous que l'interface de ligne de commande Azure est installée sur votre système ou qu'Azure Cloud Shell est disponible via le portail Azure. Pour plus d'informations sur l'installation de l'interface de ligne de commande Azure, reportez-vous à la "Documentation Microsoft : Comment installer Azure CLI" .

Étapes

1. Mappez la version Cloud Volumes ONTAP sur votre système à la version de l'image de la place de marché Azure à l'aide du contenu du fichier *version_readme*. La version Cloud Volumes ONTAP est représentée par `buildname` et la version de l'image de la place de marché Azure est représentée par `version` dans les mappages de versions.

   Dans l'exemple suivant, la version Cloud Volumes ONTAP `9.15.0P1` est mappé à la version de l'image de la place de marché Azure `9150.01000024.05090105` . Cette version d'image de la place de marché Azure est utilisée ultérieurement pour définir l'URN de l'image.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifiez la région dans laquelle vous souhaitez créer les machines virtuelles. Le nom de la région est utilisé comme valeur pour le `locName` variable lors de la définition de l'URN de l'image du marché. Pour lister les régions disponibles, exécutez cette commande :

   ```
   az account list-locations -o table
   ```

Dans ce tableau, le nom de la région apparaît dans le `Name` champ.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Consultez les noms de référence (SKU) pour les versions Cloud Volumes ONTAP correspondantes et les types de déploiement de machine virtuelle dans le tableau ci-dessous. Le nom du SKU est utilisé comme valeur pour le `skuName` variable lors de la définition de l'URN de l'image du marché.

   Par exemple, tous les déploiements à nœud unique avec Cloud Volumes ONTAP 9.15.0 doivent utiliser `ontap_cloud_byol` comme nom de référence.

* Version Cloud Volumes ONTAP *	**Déploiement de VM via**	**Nom du SKU**
9.17.1 et versions ultérieures	La place de marché Azure	ontap_cloud_direct_gen2
9.17.1 et versions ultérieures	La NetApp Console	ontap_cloud_gen2
9.16.1	La place de marché Azure	ontap_cloud_direct
9.16.1	La console	ontap_cloud
9.15.1	La console	ontap_cloud
9.15.0	La console, déploiements à nœud unique	ontap_cloud_byol
9.15.0	La console, déploiements haute disponibilité (HA)	ontap_cloud_byol_ha

4. Après avoir mappé la version ONTAP et l'image de la place de marché Azure, exportez le fichier VHD à partir de la place de marché Azure à l'aide d'Azure Cloud Shell ou d'Azure CLI.

Exporter un fichier VHD à l'aide d'Azure Cloud Shell sous Linux

À partir d'Azure Cloud Shell, exportez l'image de la place de marché vers le fichier VHD (par exemple, *9150.01000024.05090105.vhd*) et téléchargez-la sur votre système Linux local. Effectuez ces étapes pour obtenir l'image VHD à partir de la place de marché Azure.

Étapes

1. Définissez l'URN et d'autres paramètres de l'image du marché. Le format URN est `<publisher>:<offer>:<sku>:<version>` . Vous pouvez également répertorier les images du marché NetApp pour confirmer la version d'image correcte.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Créez un nouveau disque géré à partir de l'image du marketplace avec la version d'image correspondante :

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Exportez le fichier VHD du disque géré vers le stockage Azure. Créez un conteneur avec le niveau d'accès approprié. Dans cet exemple, nous avons utilisé un conteneur nommé `vm-images` avec `Container` niveau d'accès. Obtenez la clé d'accès au compte de stockage à partir du portail Azure : **Comptes de stockage > *examplesaname* > Clé d'accès > *key1* > *key* > Afficher > <*copie*>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Téléchargez l’image générée sur votre système Linux. Utilisez le `wget` commande pour télécharger le fichier VHD :

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

L’URL suit un format standard. Pour l’automatisation, vous pouvez dériver la chaîne URL comme indiqué ci-dessous. Vous pouvez également utiliser l’interface de ligne de commande Azure. `az` commande pour obtenir l’URL. Exemple d’URL :https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Nettoyer le disque géré

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exporter un fichier VHD à l’aide d’Azure CLI sous Linux

Exportez l’image de la place de marché vers un fichier VHD à l’aide de l’interface de ligne de commande Azure à partir d’un système Linux local.

Étapes

1. Connectez-vous à l’interface de ligne de commande Azure et répertoriez les images de la place de marché :

```
% az login --use-device-code
```

2. Pour vous connecter, utilisez un navigateur Web pour ouvrir la page https://microsoft.com/devicelogin et entrez le code d’authentification.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Créez un nouveau disque géré à partir de l'image du marché avec la version d'image correspondante.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Pour automatiser le processus, le SAS doit être extrait de la sortie standard. Consultez les documents appropriés pour obtenir des conseils.

4. Exportez le fichier VHD à partir du disque géré.

   a. Créez un conteneur avec le niveau d'accès approprié. Dans cet exemple, un conteneur nommé `vm-images` avec `Container` le niveau d'accès est utilisé.

   b. Obtenez la clé d'accès au compte de stockage à partir du portail Azure : **Comptes de stockage > *examplesaname* > Clé d'accès > *key1* > *key* > Afficher > <*copie*>**

      Vous pouvez également utiliser le `az` commande pour cette étape.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Vérifiez l'état de la copie du blob.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Téléchargez l'image générée sur votre serveur Linux.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

L'URL suit un format standard. Pour l'automatisation, vous pouvez dériver la chaîne URL comme indiqué ci-dessous. Vous pouvez également utiliser l'interface de ligne de commande Azure. `az` commande pour obtenir l'URL. Exemple d'URL :https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Nettoyer le disque géré

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

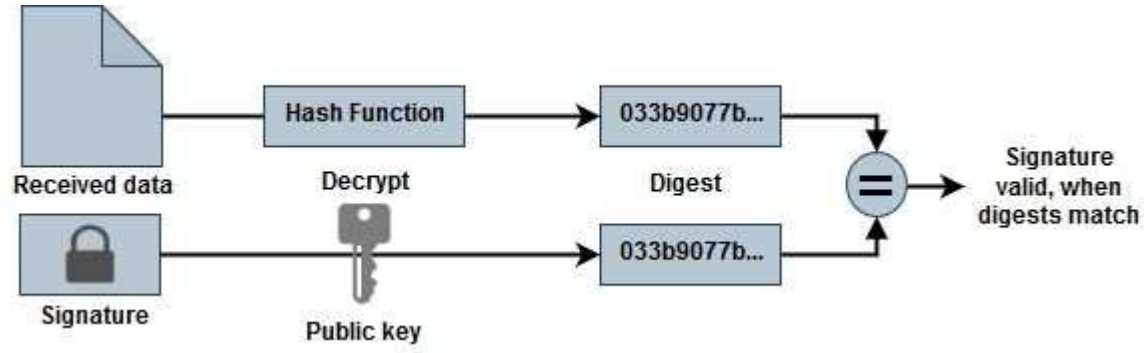
Vérifier la signature du fichier

Vérification de la signature d'image de la place de marché Azure pour Cloud Volumes ONTAP

Le processus de vérification d'image Azure génère un fichier de résumé à partir du fichier VHD en supprimant 1 Mo au début et 512 octets à la fin, puis en appliquant une fonction de hachage. Pour correspondre à la procédure de signature, *sha256* est utilisé pour le hachage.

Résumé du flux de travail de vérification de la signature du fichier

Voici un aperçu du processus de vérification de la signature du fichier.



- Téléchargement de l'image Azure à partir du "Site de support NetApp" et extraire le fichier digest (.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem). Consultez "Téléchargez le fichier de résumé de l'image Azure" pour plus d'informations.
- Vérification de la chaîne de confiance.
- Extraction de la clé publique (.pub) du certificat de clé publique (.pem).
- Décryptage du fichier digest en utilisant la clé publique extraite.
- Comparaison du résultat avec un condensé nouvellement généré d'un fichier temporaire créé à partir du fichier image après avoir supprimé 1 Mo au début et 512 octets à la fin. Cette étape est réalisée à l'aide de l'outil de ligne de commande OpenSSL. L'outil OpenSSL CLI affiche un message approprié en cas de réussite ou d'échec de la correspondance des fichiers.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur Linux

La vérification d'une signature de fichier VHD exportée sous Linux comprend la validation de la chaîne de confiance, la modification du fichier et la vérification de la signature.

Étapes

1. Téléchargez le fichier image Azure à partir du "Site de support NetApp" et extrayez le fichier digest (.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

   Se référer à "Téléchargez le fichier de résumé de l'image Azure" pour plus d'informations.

2. Vérifier la chaîne de confiance.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Supprimez 1 Mo (1 048 576 octets) au début et 512 octets à la fin du fichier VHD. Lors de l'utilisation `tail` , le `-c +K` l'option génère des octets à partir du K-ième octet du fichier. Par conséquent, il passe 1048577 à `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilisez OpenSSL pour extraire la clé publique du certificat et vérifiez le fichier dépouillé (sign.tmp) avec le fichier de signature et la clé publique.

   L'invite de commande affiche des messages indiquant la réussite ou l'échec en fonction de la vérification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Nettoyer l'espace de travail.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur macOS

La vérification d'une signature de fichier VHD exportée sous Linux comprend la validation de la chaîne de confiance, la modification du fichier et la vérification de la signature.

Étapes

1. Téléchargez le fichier image Azure à partir du "Site de support NetApp" et extrayez le fichier digest (.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

   Se référer à "Téléchargez le fichier de résumé de l'image Azure" pour plus d'informations.

2. Vérifier la chaîne de confiance.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Supprimez 1 Mo (1 048 576 octets) au début et 512 octets à la fin du fichier VHD. Lors de l'utilisation `tail` , le `-c +K` l'option génère des octets à partir du K-ième octet du fichier. Par conséquent, il passe 1048577 à `tail -c` . Notez que sur macOS, l'exécution de la commande tail peut prendre environ dix minutes.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilisez OpenSSL pour extraire la clé publique du certificat et vérifiez le fichier dépouillé (sign.tmp) avec le fichier de signature et la clé publique. L'invite de commande affiche des messages indiquant la réussite ou l'échec en fonction de la vérification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Nettoyer l’espace de travail.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```