Commencez à Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

Commencez à Azure

Mise en route de Cloud Volumes ONTAP pour Azure

Découvrez Cloud Volumes ONTAP pour Azure en quelques étapes.

Créer un connecteur

Si vous n'avez pas de "Connecteur" Cependant, un administrateur de compte doit en créer un. "Découvrez comment créer un connecteur dans Azure".

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à déployer un connecteur si vous n'en possédez pas encore.

Planification de la configuration

Cloud Manager propose des packages préconfigurés qui répondent aux exigences de vos workloads, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez. "En savoir plus >>".

Configurez votre réseau

1. Assurez-vous que votre VNet et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du réseau vnet cible de sorte que le connecteur et Cloud Volumes ONTAP puissent contacter plusieurs noeuds finaux.

   Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour "Le connecteur et le Cloud Volumes ONTAP".

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

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

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

Liens connexes

- "L'évaluation"
- "Création d'un connecteur depuis Cloud Manager"
- "Création d'un connecteur à partir d'Azure Marketplace"
- "Installation du logiciel du connecteur sur un hôte Linux"

- "Ce que fait Cloud Manager avec les autorisations Azure"

Planification de votre configuration Cloud Volumes ONTAP dans Azure

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, vous pouvez soit choisir un système préconfiguré qui correspond aux exigences de vos workloads, soit créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez.

Choix d'un type de licence

Deux options de tarification sont disponibles pour Cloud Volumes ONTAP : le paiement à l'utilisation ou le modèle BYOL (où vous apportez votre propre licence). Le paiement basé sur l'utilisation vous permet de choisir entre trois licences : explore, Standard ou Premium. Chacune d'elles fournit une capacité distincte et des options de calcul différentes.

"Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans Azure"

Compréhension des limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP dépend de la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Il est important de connaître ces dernières lors de la planification de la configuration.

"Limites de stockage pour Cloud Volumes ONTAP 9.7 dans Azure"

Dimensionnement du système dans Azure

Le dimensionnement du système Cloud Volumes ONTAP permet de répondre à vos besoins de performance et de capacité. Quelques points clés sont à noter lors de la sélection d'un type de VM, d'un type de disque et d'une taille de disque :

Type de machine virtuelle

Examinez les types de machines virtuelles prises en charge dans le "Notes de version de Cloud Volumes ONTAP" Examinez ensuite toutes les informations sur chaque type de machine virtuelle pris en charge. Notez que chaque type de VM prend en charge un nombre spécifique de disques de données.

- "Documentation Azure : tailles de machine virtuelle à usage général"
- "Documentation Azure : tailles de machines virtuelles optimisées pour la mémoire"

Type de disque Azure

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

Les systèmes HAUTE DISPONIBILITÉ utilisent des objets blob de pages Premium. En parallèle, les systèmes à un seul nœud peuvent utiliser deux types de disques gérés Azure :

- *Des disques gérés SSD de premier choix* fournir des performances élevées aux charges de travail exigeantes en E/S à un coût plus élevé.

- *Des disques gérés SSD standard* assurent des performances prévisibles pour les charges de travail nécessitant un faible niveau d'IOPS.
- *Les disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevées et souhaitez réduire vos coûts.

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

Taille des disques Azure

Lorsque vous lancez des instances Cloud Volumes ONTAP, vous devez choisir la taille de disque par défaut des agrégats. Cloud Manager utilise cette taille de disque pour l'agrégat initial, et pour tous les agrégats supplémentaires que vous créez 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 "utilisation de l'option d'allocation avancée".

Tous les disques qui composent un agrégat doivent être de la même taille.

Lorsque vous choisissez une taille de disque, vous devez prendre en compte plusieurs facteurs. La taille des disques a une incidence sur le montant de vos frais de stockage, la taille des volumes que vous pouvez créer au sein d'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 des disques. Les disques de grande taille offrent des IOPS et un débit plus élevés. Par exemple, le choix de disques de 1 To peut fournir des performances supérieures à celles des disques de 500 Go, pour un coût plus élevé.

Avec un stockage standard, les performances sont les mêmes pour toutes les tailles de disques. Choisissez la taille de disque en fonction de la capacité dont vous avez besoin.

Pour les IOPS et le débit par taille de disque, consultez Azure :

- "Microsoft Azure : tarification des disques gérés"
- "Microsoft Azure : tarification Blobs de page"

Choix d'une configuration qui prend en charge Flash cache

Une configuration Cloud Volumes ONTAP dans Azure inclut un stockage NVMe local, que Cloud Volumes ONTAP utilise comme *Flash cache* pour de meilleures performances. "En savoir plus sur Flash cache".

Fiche d'informations sur le réseau Azure

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, vous devez spécifier des informations concernant votre réseau virtuel. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Informations sur Azure	Votre valeur
Région	
Réseau virtuel (vnet)	
Sous-réseau	

Informations sur Azure	Votre valeur
Groupe de sécurité réseau (s'il s'agit du vôtre)	

Sélection d'une vitesse d'écriture

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés et les risques et les recommandations lors de l'utilisation de la vitesse d'écriture élevée.

Différence entre une vitesse d'écriture standard et une vitesse d'écriture élevée

Lorsque vous choisissez la vitesse d'écriture standard, les données sont écrites directement sur le disque, réduisant ainsi le risque de perte de données en cas d'interruption imprévue du système.

Lorsque vous choisissez la vitesse d'écriture élevée, les données sont mises en tampon dans la mémoire avant d'être écrites sur le disque, ce qui accélère les performances d'écriture. Toutefois, la mise en cache peut entraîner une perte de données en cas de panne système.

Le volume de données pouvant être perdues en cas de panne système correspond à l'étendue des deux derniers points de cohérence. Le point de cohérence consiste à écrire des données mises en tampon sur le disque. Un point de cohérence se produit lorsque le journal d'écriture est plein ou après 10 secondes (selon la première éventualité). Cependant, la performance des volumes AWS EBS peut affecter le temps de traitement des points de cohérence.

Quand utiliser une vitesse d'écriture élevée

Optez pour la vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides et que vous ne craignez pas de perdre des données.

Recommandations lors de l'utilisation d'une vitesse d'écriture élevée

Si vous activez la vitesse d'écriture élevée, vous devez assurer la protection de l'écriture au niveau de la couche applicative.

Choix d'un profil d'utilisation du volume

ONTAP comprend plusieurs fonctionnalités d'efficacité du stockage qui permettent de réduire la quantité totale de stockage nécessaire. Lorsque vous créez un volume dans Cloud Manager, vous pouvez choisir un profil qui active ou désactive ces fonctionnalités. Vous devez en savoir plus sur ces fonctionnalités pour vous aider à choisir le profil à utiliser.

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

Provisionnement fin

Met à la disposition des hôtes ou des utilisateurs une quantité de stockage logique supérieure au stockage effectivement présent dans votre pool physique. L'espace de stockage est alloué de manière dynamique, et non au préalable, à chaque volume lors de l'écriture des données.

Déduplication

Améliore l'efficacité en identifiant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins 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 les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Exigences réseau pour déployer et gérer Cloud Volumes ONTAP dans Azure

Configurez votre réseau Azure de façon à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

Conditions requises pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être satisfaites dans Azure.

Accès Internet sortant pour Cloud Volumes ONTAP

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

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

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

"Découvrez comment configurer AutoSupport".

Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car Cloud Manager le fait pour vous. Si vous devez utiliser votre propre système, reportez-vous aux règles du groupe de sécurité répertoriées ci-dessous.

Nombre d'adresses IP

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

- Un seul nœud : 5 adresses IP
- Paire HA : 16 adresses IP

Notez que Cloud Manager crée une LIF de gestion des SVM sur des paires haute disponibilité, mais pas sur des systèmes à un seul nœud dans Azure.

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

Connexion de Cloud Volumes ONTAP au stockage Azure Blob pour le hiérarchisation des données

Si vous souhaitez transférer les données inactives vers un stockage Azure Blob, vous n'avez pas besoin de configurer de connexion entre le Tier de performance et le Tier de capacité tant que Cloud Manager dispose des autorisations nécessaires. Cloud Manager active un terminal de service VNet pour vous si la

règle Cloud Manager dispose des autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Ces autorisations sont incluses dans la dernière version "Politique de Cloud Manager".

Pour plus d'informations sur la configuration du Tiering des données, voir "Tiering des données inactives vers un stockage objet à faible coût".

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP sur les systèmes Azure et ONTAP sur d'autres réseaux, vous devez disposer d'une connexion VPN entre Azure VNet et l'autre réseau, par exemple un VPC AWS ou votre réseau d'entreprise.

Pour obtenir des instructions, reportez-vous à la section "Documentation Microsoft Azure : créez une connexion de site à site dans le portail Azure".

Configuration requise pour le connecteur

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

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

Connexions aux réseaux cibles

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

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

Accès Internet sortant

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

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans la plupart des régions d'Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure US Gov.

Terminaux	Objectif
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
*.blob.core.windows.net	Requis pour les paires haute disponibilité lors de l'utilisation d'un proxy.

Terminaux	Objectif
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

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

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Règles de groupe de sécurité pour Cloud Volumes ONTAP

Cloud Manager crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes nécessaires au fonctionnement de Cloud Volumes ONTAP. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

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

Règles entrantes pour les systèmes à nœud unique

Les règles énumérées ci-dessous autorisent le trafic, sauf si la description indique qu'il bloque un trafic entrant spécifique.

Priorité et nom	Port et protocole	Source et destination	Description
1000 inbound_ssh	22 TCP	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
1001 inbound_http	80 TCP	De tous les types à tous	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1002 inbound_111_tcp	111 TCP	De tous les types à tous	Appel de procédure à distance pour NFS
1003 inbound_111_udp	111 UDP	De tous les types à tous	Appel de procédure à distance pour NFS
1004 entrant_139	139 TCP	De tous les types à tous	Session de service NetBIOS pour CIFS
1005 inbound_161-162 _tcp	161-162 TCP	De tous les types à tous	Protocole de gestion de réseau simple
1006 inbound_161-162 _udp	161-162 UDP	De tous les types à tous	Protocole de gestion de réseau simple
1007 entrant_443	443 TCP	De tous les types à tous	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1008 entrant_445	445 TCP	De tous les types à tous	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
1009 inbound_635_tcp	635 TCP	De tous les types à tous	Montage NFS
1010 inbound_635_udp	635 UDP	De tous les types à tous	Montage NFS
1011 entrant_749	749 TCP	De tous les types à tous	Kerberos
1012 inbound_2049_tcp	2049 TCP	De tous les types à tous	Démon du serveur NFS
1013 inbound_2049_udp	2049 UDP	De tous les types à tous	Démon du serveur NFS
1014 entrant_3260	3260 TCP	De tous les types à tous	Accès iSCSI via le LIF de données iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau

Priorité et nom	Port et protocole	Source et destination	Description
1016 inbound_4045-4046_udp	4045-4046 UDP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau
1017 entrant_10000	10000 TCP	De tous les types à tous	Sauvegarde avec NDMP
1018 entrant_11104-11105	11104-11105 TCP	De tous les types à tous	Transfert de données SnapMirror
3000 inbound_deny _all_tcp	Tout port TCP	De tous les types à tous	Bloquer tout autre trafic TCP entrant
3001 inbound_deny _all_udp	Tout port UDP	De tous les types à tous	Bloquer tout autre trafic entrant UDP
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

Règles entrantes pour les systèmes HA

Les règles énumérées ci-dessous autorisent le trafic, sauf si la description indique qu'il bloque un trafic entrant spécifique.

Les systèmes HAUTE DISPONIBILITÉ disposent de règles entrantes moins strictes que les systèmes à un seul nœud, car le trafic des données entrantes transite par Azure Standard Load Balancer. Pour cette raison, le trafic provenant du Load Balancer doit être ouvert, comme indiqué dans la règle AllowAzureLoadBalancerInBound.

Priorité et nom	Port et protocole	Source et destination	Description
100 entrant_443	443 tout protocole	De tous les types à tous	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
101 inbound_111_tcp	111 tout protocole	De tous les types à tous	Appel de procédure à distance pour NFS
102 inbound_2049_tcp	2049 tout protocole	De tous les types à tous	Démon du serveur NFS
111 inbound_ssh	22 tout protocole	De tous les types à tous	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	De tous les types à tous	DNS et CIFS

Priorité et nom	Port et protocole	Source et destination	Description
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	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 base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

Service	Port	Protocole	Source	Destination	Objectif
Active Directory	88	TCP	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	137	UDP	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	139	TCP	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	389	TCP ET UDP	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	445	TCP	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	464	UDP	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	88	TCP	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	137	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	139	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	389	TCP ET UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	445	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	464	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
DHCP	68	UDP	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration

Service	Port	Protocole	Source	Destination	Objectif
DHCPS	67	UDP	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	53	UDP	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	25	TCP	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	161	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	161	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	11104	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	11105	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	514	UDP	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles de groupe de sécurité pour le connecteur

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

Règles entrantes

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

Port	Protocole	Objectif
22	SSH	Fournit un accès SSH à l'hôte du connecteur
80	HTTP	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale

Port	Protocole	Objectif
443	HTTPS	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

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

Lancement d'Cloud Volumes ONTAP dans Azure

Vous pouvez lancer un système à un seul nœud ou une paire HA dans Azure en créant un environnement de travail Cloud Volumes ONTAP dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau Azure auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Pour déployer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence) pour chaque nœud.

Description de la tâche

Lorsque Cloud Manager crée un système Cloud Volumes ONTAP dans Azure, il crée plusieurs objets Azure, comme 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

Le déploiement d'Cloud Volumes ONTAP dans un groupe de ressources existant et partagées n'est pas recommandé en raison du risque de perte de données. Lorsque la restauration est actuellement désactivée par défaut lors de l'utilisation de l'API pour le déploiement dans un groupe de ressources existant, la suppression de Cloud Volumes ONTAP risque de supprimer d'autres ressources de ce groupe partagé.

Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Il s'agit de l'option par défaut et uniquement recommandée pour le déploiement de Cloud Volumes ONTAP dans Azure à partir de Cloud Manager.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Microsoft Azure** et **Cloud Volumes ONTAP nœud unique** ou **Cloud Volumes ONTAP haute disponibilité**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster et de groupe de ressources, ajoutez des balises si nécessaire, puis spécifiez des informations d'identification.

   Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail 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.

Champ	Description
Nom du groupe de ressources	Conservez le nom par défaut du nouveau groupe de ressources ou décochez **utiliser par défaut** et entrez votre propre nom pour le nouveau groupe de ressources. Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. S'il est possible de déployer Cloud Volumes ONTAP dans un groupe de ressources existant et partagé à l'aide de l'API, il n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails.
Étiquettes	Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, Cloud Manager 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 environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. "Apprenez à ajouter des informations d'identification".

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
   - "En savoir plus sur Cloud Compliance".
   - "En savoir plus sur la sauvegarde dans le cloud".
5. **Localisation et connectivité** : sélectionnez un emplacement et un groupe de sécurité et cochez la case pour confirmer la connectivité réseau entre Cloud Manager et l'emplacement cible.
6. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

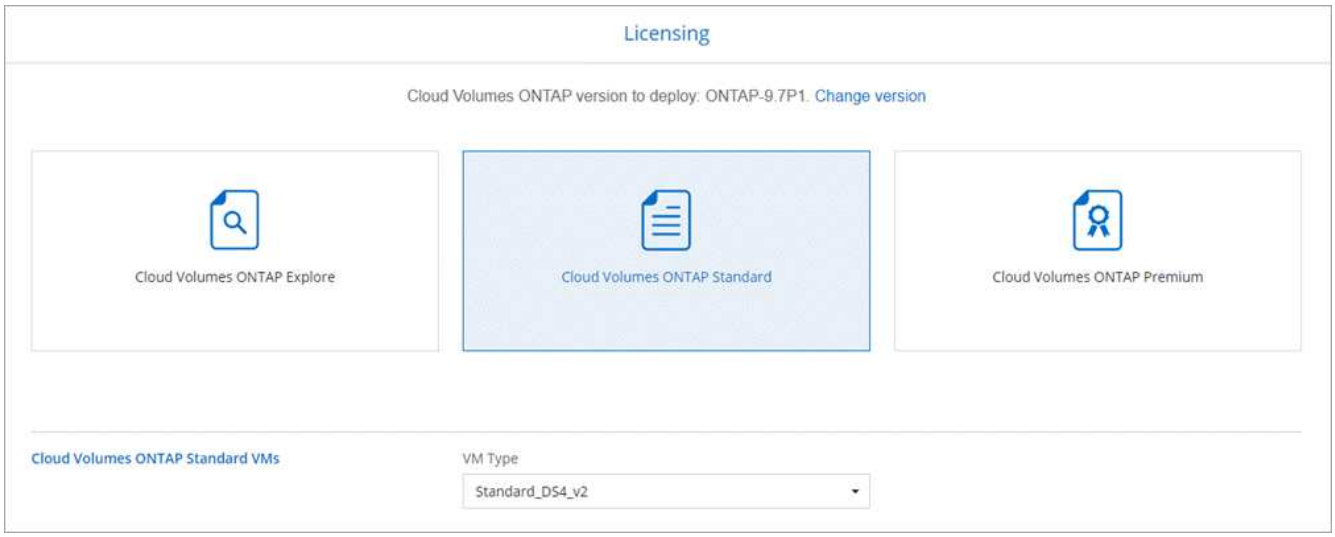
   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

   Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

7. **Packages préconfigurés** : Shelect 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, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

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



Si vos besoins changent après le lancement du système, vous pouvez modifier la licence ou le type de machine virtuelle ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à 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 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

9. **Abonnez-vous à partir d'Azure Marketplace**: Suivez les étapes si Cloud Manager n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP.
10. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si le Tiering des données vers stockage Blob doit être activé.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

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

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "En savoir plus sur le Tiering des données".

11. **Vitesse d'écriture et WORM** (systèmes à un seul nœud uniquement) : choisissez **Normal** ou **vitesse d'écriture élevée** et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

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

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

"En savoir plus sur le stockage WORM".

12. **Secure communication to Storage & WORM** (HA uniquement) : permet d'activer ou non une connexion HTTPS aux comptes de stockage Azure et d'activer le stockage WORM (Write Once, Read Many), si nécessaire.

    La connexion HTTPS est établie depuis une paire HA Cloud Volumes ONTAP 9.7 vers les comptes de stockage 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 l'environnement de travail.

    "En savoir plus sur le stockage WORM".

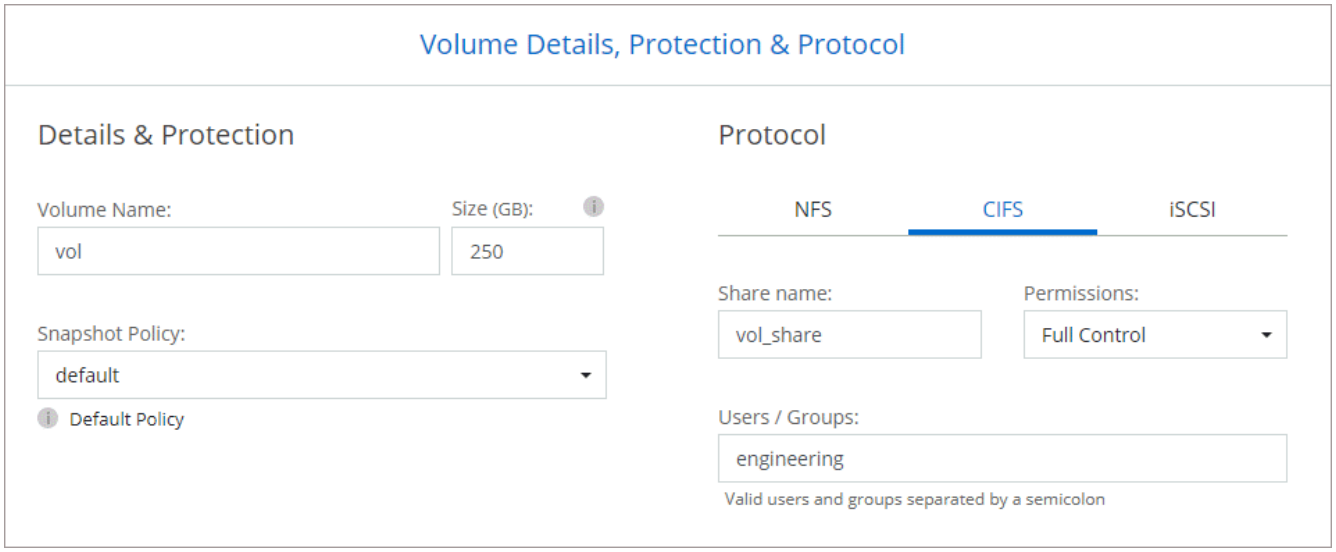
13. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

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

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager 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 à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune 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 initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

L'image suivante montre la page Volume remplie pour le protocole CIFS :



14. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale 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 à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs ADDC** ou **ou=utilisateurs ADDC** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : créez une unité organisationnelle dans un domaine géré 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 identique au 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 autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

15. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

16. **Revue et approbation** : consultez et confirmez vos choix.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources Azure que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

Résultat

Cloud Manager déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

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

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez 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 System Manager ou l'interface de ligne de commande.

  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.

Informations sur le copyright

Informations sur les marques commerciales