



Lancez-vous dans GCP

Cloud Manager 3.8

NetApp
October 22, 2024

Sommaire

- Lancez-vous dans GCP 1
 - Mise en route avec Cloud Volumes ONTAP pour Google Cloud 1
 - Planification de votre configuration Cloud Volumes ONTAP dans Google Cloud 2
 - Exigences de mise en réseau pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP 5
 - Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP 14
 - Lancement d'Cloud Volumes ONTAP dans GCP..... 16

Lancez-vous dans GCP

Mise en route avec Cloud Volumes ONTAP pour Google Cloud

Lancez-vous avec Cloud Volumes ONTAP pour GCP 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 GCP](#)".

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. Vérifiez que votre VPC 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 VPC cible de sorte que le connecteur et le Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

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](#)".



Configuration de GCP pour le Tiering des données

Deux exigences doivent être remplies pour transférer les données inactives de Cloud Volumes ONTAP vers un stockage objet à faible coût (un compartiment Google Cloud Storage) :

1. "[Configurez le sous-réseau Cloud Volumes ONTAP pour un accès privé à Google](#)".
2. "[Configurez un compte de service pour le Tiering des données](#)":
 - Attribuez le rôle *Storage Admin* prédéfini au compte de service de hiérarchisation.
 - Ajoutez le compte de service Connector en tant que *Service Account User* au compte de service

Tiering.

Vous pouvez indiquer le rôle d'utilisateur "[à l'étape 3 de l'assistant lorsque vous créez le compte de service de tiering](#)", ou "[attribuez le rôle après la création du compte de service](#)".

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, vous devrez sélectionner le compte de service de Tiering.

Si vous n'activez pas le Tiering des données et sélectionnez un compte de service lorsque vous créez le système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP à partir de la console GCP.



Activez les API Google Cloud

"[Activez les API Google Cloud suivantes dans votre projet](#)". Ces API sont nécessaires pour déployer le connecteur et Cloud Volumes ONTAP.

- API Cloud Deployment Manager V2
- API de journalisation cloud
- API Cloud Resource Manager
- API du moteur de calcul
- API de gestion des identités et des accès



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](#)"
- "[Installation du logiciel du connecteur sur un hôte Linux](#)"
- "[Avantages de Cloud Manager avec les autorisations GCP](#)"

Planification de votre configuration Cloud Volumes ONTAP dans Google Cloud

Lorsque vous déployez Cloud Volumes ONTAP dans Google Cloud, 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 GCP"](#)

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 GCP"](#)

Dimensionnement du système dans GCP

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 machine, d'un type de disque et d'une taille de disque :

Type de machine

Examiner les types de machine pris en charge dans le ["Notes de version de Cloud Volumes ONTAP"](#) Puis passez en revue les détails de Google concernant chaque type de machine pris en charge. Faites correspondre les exigences de vos charges de travail au nombre de CPU virtuels et à la mémoire correspondant au type de machine. Notez que chaque cœur de processeur augmente les performances réseau.

Pour plus de détails, reportez-vous aux sections suivantes :

- ["Documentation Google Cloud : types de machine standard N1"](#)
- ["Documentation Google Cloud : performances"](#)

Type de disque GCP

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent utilisé par Cloud Volumes ONTAP pour un disque. Le type de disque peut être soit *Zonal SSD persistent disks* soit *Zonal standard persistent disks*.

Les disques persistants des disques SSD sont parfaitement adaptés aux charges de travail qui exigent des taux élevés d'IOPS aléatoires, tandis que les disques persistants standard sont économiques et peuvent prendre en charge des opérations de lecture/écriture séquentielles. Pour plus de détails, voir ["Documentation Google Cloud : disques persistants zonés \(standard et SSD\)"](#).

Taille des disques GCP

Lorsque vous déployez un système Cloud Volumes ONTAP, vous devez choisir la taille de disque initiale. Après cela, Cloud Manager vous permet de gérer la capacité d'un système, mais si vous souhaitez créer vous-même des agrégats, sachez que :

- Tous les disques qui composent un agrégat doivent être de la même taille.
- Déterminez l'espace dont vous avez besoin tout en prenant en compte les performances.
- Les performances des disques persistants évoluent automatiquement en fonction de la taille des disques et du nombre de CPU virtuels disponibles pour le système.

Pour plus de détails, reportez-vous aux sections suivantes :

- ["Documentation Google Cloud : disques persistants zonés \(standard et SSD\)"](#)
- ["Documentation Google Cloud : optimisation des performances des disques persistants et des SSD locaux"](#)

Fiche technique d'informations réseau GCP

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

Informations GCP	Votre valeur
Région	
Zone	
Réseau VPC	
Sous-réseau	
Politique de pare-feu (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 de mise en réseau pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP

Configurez votre réseau Google Cloud Platform de manière 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 suivantes doivent être satisfaites dans GCP.

Cloud privé virtuel

Cloud Volumes ONTAP et le connecteur sont pris en charge dans un VPC partagé par Google Cloud et dans des VPC non partagés.

Un VPC partagé vous permet de configurer et de gérer de manière centralisée les réseaux virtuels dans plusieurs projets. Vous pouvez configurer des réseaux VPC partagés dans le projet *host* et déployer les instances de machines virtuelles Connector et Cloud Volumes ONTAP dans un projet *service*.

["Documentation Google Cloud : présentation du VPC partagé"](#).

La seule exigence concernant l'utilisation d'un VPC partagé est de fournir le ["Rôle utilisateur du réseau de calcul"](#) Vers le compte de service Connector. Cloud Manager a besoin de ces autorisations pour interroger les pare-feu, le VPC et les sous-réseaux du projet hôte.

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"](#).

Nombre d'adresses IP

Cloud Manager attribue 5 adresses IP à Cloud Volumes ONTAP dans GCP.

Notez que Cloud Manager ne crée pas de LIF de gestion des SVM pour Cloud Volumes ONTAP dans GCP.



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.

Règles de pare-feu

Inutile de créer des règles de pare-feu, car Cloud Manager le fait pour vous. Si vous devez vous en servir, reportez-vous aux règles de pare-feu répertoriées ci-dessous.

Connexion de Cloud Volumes ONTAP à Google Cloud Storage pour le Tiering des données

Pour transférer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : configuration de Private Google Access](#)".

Pour connaître les étapes supplémentaires requises pour la configuration du Tiering des données dans Cloud Manager, consultez la section "[Tiering des données inactives vers un stockage objet à faible coût](#)".

Connexions aux systèmes ONTAP dans d'autres réseaux

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

Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : présentation de Cloud VPN](#)".

Configuration requise pour le connecteur

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



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

Connexion aux réseaux cibles

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

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une

connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

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

Terminaux	Objectif
https://www.googleapis.com	Permet au connecteur de contacter les API Google pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP.
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 au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournies une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
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.

Terminaux	Objectif
<p>Divers sites tiers, par exemple :</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Les emplacements tiers sont sujets à modification.</p>	<p>Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.</p>

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

Terminaux	Objectif
L'hôte du connecteur	<p>Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager.</p> <p>En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte :</p> <ul style="list-style-type: none"> • 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 <p>Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.</p>
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	<p>Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.</p>
https://widget.intercom.io	<p>Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.</p>

Règles de pare-feu pour Cloud Volumes ONTAP

Cloud Manager crée des règles de pare-feu GCP qui incluent les règles entrantes et sortantes nécessaires au bon fonctionnement de Cloud Manager et d'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.

Les règles de pare-feu de Cloud Volumes ONTAP requièrent des règles entrantes et sortantes.

Règles entrantes

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

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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



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

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

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

Règles de pare-feu pour le connecteur

Les règles de pare-feu du connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans les règles de pare-feu prédéfinies est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent 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

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

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

Règles de sortie avancées

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



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

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

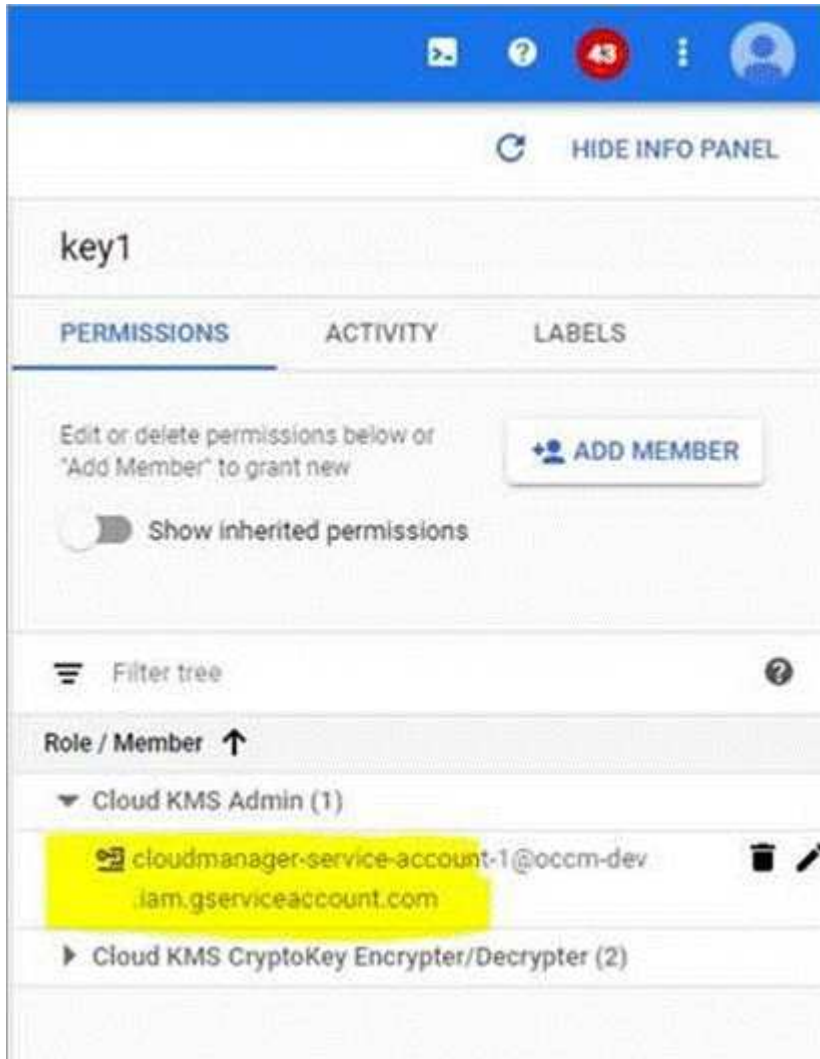
Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser les API Cloud Manager pour créer un système Cloud Volumes ONTAP qui utilise des clés de chiffrement *gérées par le client*. Il s'agit des clés que vous

créez et gérez dans GCP à l'aide du service Cloud Key Management.

Étapes

1. Donnez au compte de service Connector l'autorisation d'utiliser la clé de cryptage.



2. Obtenir l'ID de la clé en invoquant la commande GET pour l'API /gcp/vsa/Metadata/gcp-Encryption-keys
3. Utilisez le paramètre "GcpEncryption" avec votre requête API lors de la création d'un environnement de travail.

Exemple

```
"gcpEncryptionParameters": {  
  "key": "projects/tlv-support/locations/us-east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"  
}
```

Reportez-vous à la ["Guide du développeur API"](#) Pour plus d'informations sur l'utilisation du paramètre "GcpEncryption".

Lancement d'Cloud Volumes ONTAP dans GCP

Vous pouvez lancer un système Cloud Volumes ONTAP à nœud unique dans GCP en créant un environnement de travail.

Ce dont vous avez besoin

- 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 GCP 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.
- Il convient de définir les API Google Cloud suivantes ["activé dans votre projet"](#):
 - API Cloud Deployment Manager V2
 - API de journalisation cloud
 - API Cloud Resource Manager
 - API du moteur de calcul
 - API de gestion des identités et des accès

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP**.
3. **Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, ajoutez éventuellement des étiquettes, puis spécifiez les 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 le système Cloud Volumes ONTAP et l'instance de machine virtuelle GCP. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour les ressources GCP. Cloud Manager ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section " Documentation Google Cloud : étiquetage des ressources ".
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 identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes.
Modifier le projet	<p>Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet sur lequel réside Cloud Manager.</p> <p>Si d'autres projets ne s'affichent pas dans la liste déroulante, le compte de service Cloud Manager n'est pas encore associé à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle Cloud Manager à ce projet. Vous devrez répéter cette étape pour chaque projet.</p> <p> Il s'agit du compte de service que vous configurez pour Cloud Manager, "comme décrit à l'étape 2b sur cette page".</p> <p>Cliquez sur Ajouter un abonnement pour associer les informations d'identification sélectionnées à un abonnement.</p> <p>Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.</p>

Découvrez dans cette vidéo comment associer un abonnement Marketplace basé sur l'utilisation à votre projet GCP :

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

- Localisation et connectivité** : sélectionnez un emplacement, choisissez une stratégie de pare-feu et cochez la case pour confirmer la connectivité réseau au stockage Google Cloud pour le Tiering des données.

Pour transférer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : configuration de Private Google Access](#)".

- Compte du 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.

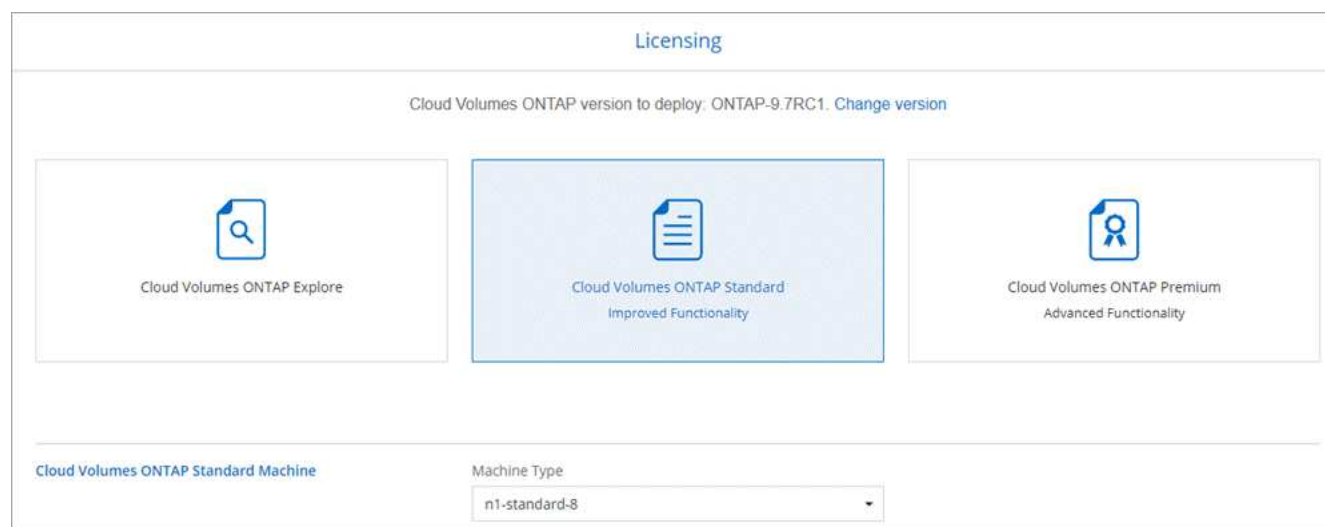
Pour comprendre le fonctionnement des licences, reportez-vous à la section "[Licences](#)".

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](#)".

6. **Packages préconfigurés** : sélectionnez 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.

7. **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.

8. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque et la taille de chaque disque.

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 GCP](#)".

9. **Vitesse d'écriture et WORM** : 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"](#).

10. **Tiering de données dans Google Cloud Platform:** Choisissez d'activer ou non le Tiering des données sur l'agrégat initial, de choisir une classe de stockage pour les données hiérarchisées, puis de sélectionner un compte de service disposant du rôle d'administrateur de stockage prédéfini (requis pour Cloud Volumes ONTAP 9.7) ou de sélectionner un compte GCP (requis pour Cloud Volumes ONTAP 9.6).

Notez ce qui suit :

- Cloud Manager définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. N'oubliez pas d'ajouter le compte de service Cloud Manager en tant qu'utilisateur du compte de service de Tiering ou bien ne pouvez pas le sélectionner depuis Cloud Manager.
- Pour obtenir de l'aide sur l'ajout d'un compte GCP, reportez-vous à ["Configuration et ajout de comptes GCP pour le Tiering des données avec la version 9.6"](#).
- 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, mais vous devrez désactiver le système et ajouter un compte de service à partir de la console GCP.

["En savoir plus sur le Tiering des données"](#).

11. **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.

Champ	Description
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 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 :

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS
 CIFS
 iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

12. **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.
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.

13. **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](#)".

14. **Revue et approbation** : consultez et confirmez vos choix.

- Consultez les détails de la configuration.
- Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources GCP que Cloud Manager achètera.
- Cochez les cases **Je comprends....**
- 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

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.