



Concepts relatifs à ONTAP

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Concepts relatifs à ONTAP 1
 - Présentation des concepts 1
 - Plateformes ONTAP 1
 - Stockage en cluster 1
 - Paires haute disponibilité 2
 - Conseiller digital AutoSupport et Active IQ 4
 - Architecture du réseau 4
 - Protocoles clients 8
 - Disques et agrégats 9
 - Volumes, qtrees, fichiers et LUN 14
 - Virtualisation du stockage 16
 - Basculement de chemin 20
 - Équilibrage de la charge 23
 - La réplication 26
 - Efficacité du stockage 33
 - Sécurité 43
 - Gestion des données intégrant la cohérence applicative 49
 - FabricPool 50

Concepts relatifs à ONTAP

Présentation des concepts

Les concepts suivants informent le logiciel de gestion des données ONTAP, y compris le stockage en cluster, la haute disponibilité, la virtualisation, la protection des données, Efficacité du stockage, sécurité et FabricPool. Avant de configurer votre solution de stockage, vous devez connaître l'ensemble des fonctionnalités et avantages de ONTAP.

Pour plus d'informations, consultez les documents suivants :

- ["Administration des clusters et des SVM"](#)
- ["Paires haute disponibilité \(HA\)"](#)
- ["Gestion du réseau et des LIF"](#)
- ["Gestion des disques et des agrégats"](#)
- ["Les volumes FlexVol, la technologie FlexClone et les fonctionnalités d'efficacité du stockage"](#)
- ["Provisionnement d'hôtes SAN"](#)
- Un accès aux fichiers NAS
 - ["Gestion NFS"](#)
 - ["Gestion SMB"](#)
- ["Reprise après incident et archivage"](#)

Plateformes ONTAP

Le logiciel de gestion des données ONTAP offre un stockage unifié pour les applications qui lisent et écrivent des données sur des protocoles d'accès de niveau bloc ou fichier, dans des configurations de stockage allant du Flash haut débit aux supports rotatifs à moindre prix, en passant par le stockage en mode objet basé sur le cloud.

Les implémentations ONTAP s'exécutent sur les plateformes FAS, AFF A-Series et C-Series spécialisées NetApp, ainsi que sur les baies ASA 100 % Flash SAN, ainsi que sur du matériel générique (ONTAP Select) et dans les clouds privés, publics ou hybrides (Cloud Volumes ONTAP). Une implémentation spécialisée offre la meilleure infrastructure convergée (data Center FlexPod).

Ensemble, ces implémentations forment la structure de base de la structure de données *NetApp*, à l'aide d'une approche Software-defined commune de la gestion des données et d'une réplication rapide et efficace entre les plateformes.

Stockage en cluster

L'itération actuelle de ONTAP a été développée à l'origine pour notre architecture de stockage scale-out *cluster*. C'est l'architecture que vous trouvez généralement dans les implémentations de data Center de ONTAP. Comme cette implémentation met en œuvre la plupart des fonctionnalités d'ONTAP, il est judicieux de commencer par comprendre les

concepts qui la technologie ONTAP.

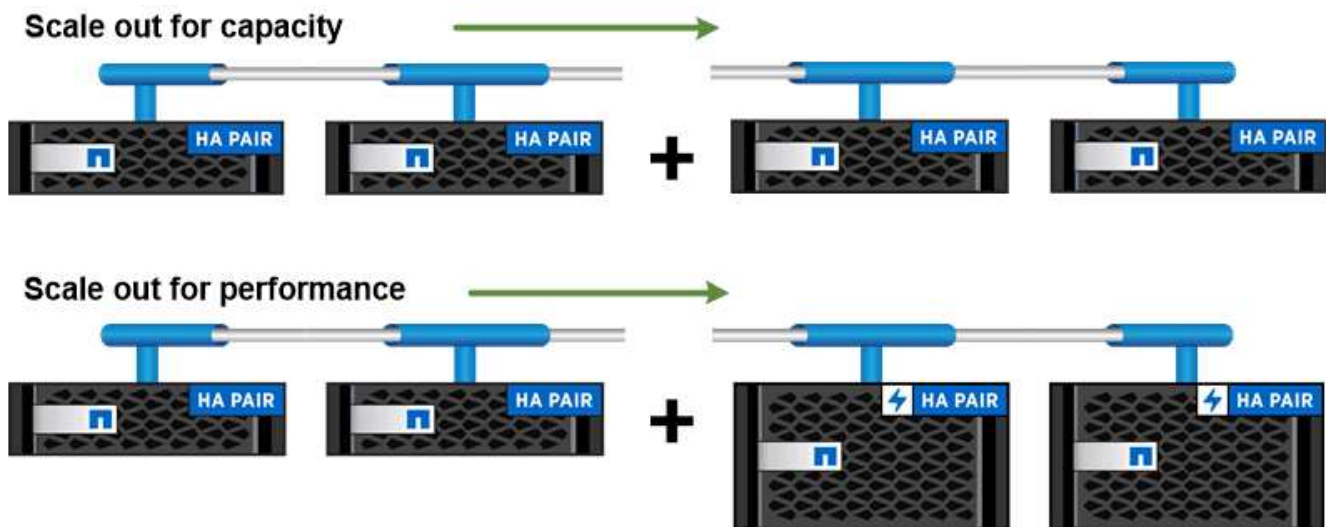
Les architectures de data Center déploient généralement des contrôleurs FAS ou AFF dédiés qui exécutent le logiciel de gestion des données ONTAP. Chaque contrôleur, son stockage, sa connectivité réseau et l'instance d'ONTAP exécutée sur le contrôleur sont appelés « nœud__ »

Les nœuds sont jumelés pour la haute disponibilité (HA). Ensemble, ces paires (jusqu'à 12 nœuds pour les SAN, jusqu'à 24 nœuds pour les NAS) constituent le cluster. Les nœuds communiquent les uns avec les autres via une interconnexion de cluster dédiée et privée.

Selon le modèle de contrôleur, le stockage des nœuds se compose de disques Flash, de disques haute capacité ou des deux. Les ports réseau du contrôleur permettent d'accéder aux données. Les ressources de stockage physique et de connectivité réseau sont virtualisées, visibles uniquement pour les administrateurs du cluster, et non pour les clients NAS ou les hôtes SAN.

Les nœuds d'une paire haute disponibilité doivent utiliser le même modèle de baie de stockage. Vous pouvez également utiliser toute combinaison de contrôleurs prise en charge. Vous pouvez faire évoluer horizontalement la capacité par l'ajout de nœuds avec des modèles de baie de stockage similaires ou pour la performance en ajoutant des nœuds aux baies de stockage plus haut de gamme.

Vous pouvez bien sûr évoluer verticalement comme vous le souhaitez, en mettant à niveau les disques et les contrôleurs selon vos besoins. L'infrastructure de stockage virtualisée d'ONTAP permet de déplacer facilement les données sans interrompre l'activité. Ainsi, vous pouvez évoluer verticalement ou horizontalement sans interruption.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

Pairs haute disponibilité

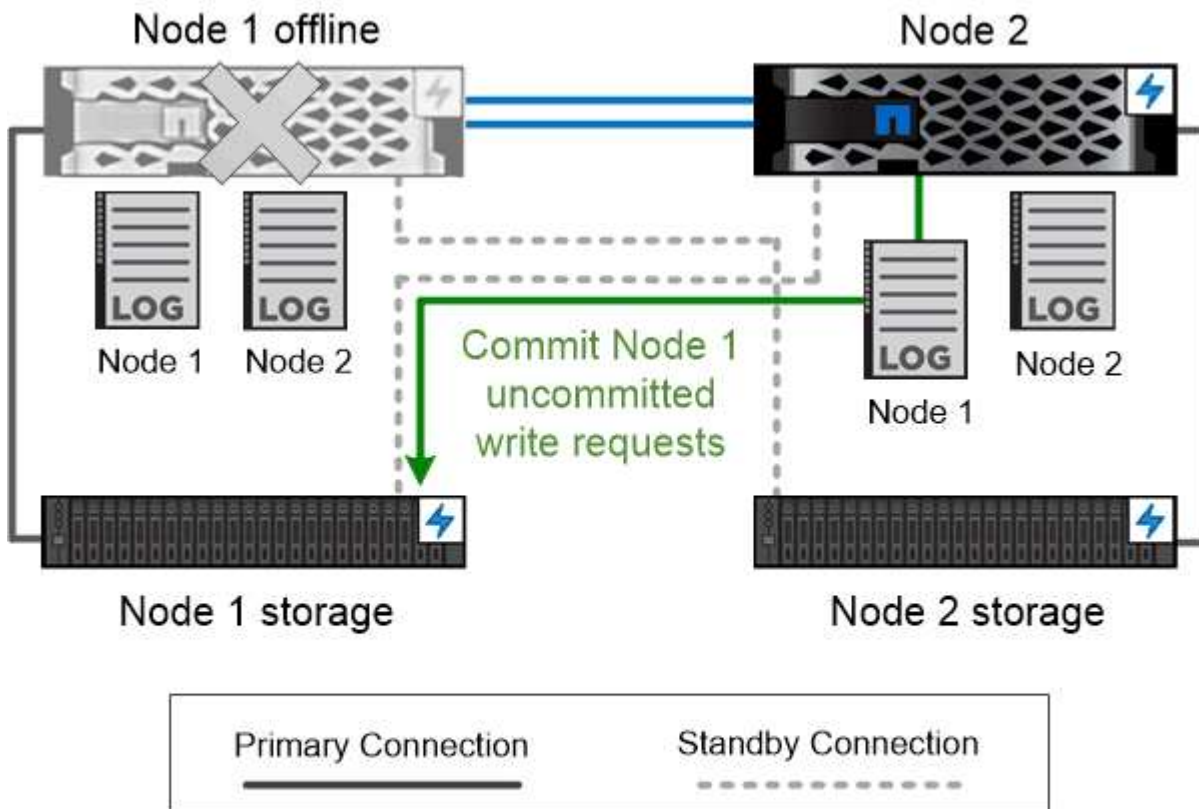
Les nœuds de cluster sont configurés sous forme de paires haute disponibilité__ pour la tolérance aux pannes et la continuité de l'activité. Si un nœud tombe en panne ou si vous devez arrêter un nœud pour assurer la maintenance de routine, son partenaire peut *reprendre* son stockage et continuer à transmettre les données à partir de celui-ci. Le partenaire *fournit* du stockage supplémentaire lorsque le nœud est revenu en ligne.

Les paires HAUTE DISPONIBILITÉ se composent toujours de modèles de contrôleurs similaires. Les contrôleurs se trouvent généralement dans le même châssis avec des blocs d'alimentation redondants.

Les paires haute disponibilité sont des nœuds tolérants aux pannes qui peuvent communiquer entre eux de différentes manières, ce qui permet à chaque nœud de vérifier en permanence si son partenaire fonctionne et de mettre en miroir les données des journaux pour la mémoire non volatile de l'autre nœud. Lorsqu'une requête d'écriture est formulée sur un nœud, celle-ci est connectée en NVRAM sur les deux nœuds avant qu'une réponse ne soit renvoyée au client ou à l'hôte. Lors du basculement, le partenaire survivant engage les demandes d'écriture non validées du nœud défaillant vers le disque, pour assurer la cohérence des données.

Des connexions au support de stockage des autres contrôleurs permettent à chaque nœud d'accéder au stockage de l'autre contrôleur en cas de basculement. Les mécanismes de basculement de chemin réseau garantissent que les clients et les hôtes continuent de communiquer avec le nœud survivant.

Pour assurer la disponibilité, vous devez continuer à utiliser la capacité de performance sur l'un des nœuds à 50 % pour gérer les charges de travail supplémentaires en cas de basculement. Pour la même raison, il peut être préférable de ne pas configurer plus de 50 % du nombre maximal d'interfaces de réseau virtuel NAS pour un nœud.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

le basculement et le retour dans les implémentations ONTAP virtualisées

Le stockage n'est pas partagé entre les nœuds dans les implémentations ONTAP virtualisées « sans partage » telles que Cloud Volumes ONTAP pour AWS ou ONTAP Select. Lorsqu'un nœud tombe en panne, son partenaire continue de transmettre des données à partir d'une copie en miroir synchrone des données du nœud. Il ne prend pas le relais du stockage du nœud, mais uniquement sa fonction de service des données.

Conseiller digital AutoSupport et Active IQ

ONTAP propose un contrôle et un reporting basés sur l'intelligence artificielle via un portail Web et une application mobile. Le composant AutoSupport de ONTAP envoie une télémétrie analysée par le conseiller digital Active IQ.

Active IQ vous permet d'optimiser votre infrastructure de données dans l'ensemble de votre cloud hybride grâce à un portail cloud et à une application mobile qui offrent des analyses prédictives et un support proactif. Les informations et les recommandations basées sur les données de Active IQ sont accessibles à tous les clients NetApp qui possèdent un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques avantages que vous pouvez faire avec Active IQ :

- Planification des mises à niveau. Active IQ identifie les problèmes qui peuvent être résolus dans votre environnement en effectuant une mise à niveau vers la plus récente version d'ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.
- Voir le bien-être du système. Votre tableau de bord Active IQ signale tout problème éventuel et vous aide à le corriger. Surveillez la capacité du système pour vous assurer que votre espace de stockage est insuffisant.
- Gestion des performances. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur les performances.
- Optimisez l'efficacité. Affichez les mesures de l'efficacité du stockage et identifiez des moyens de stocker plus de données dans moins d'espace.
- Voir l'inventaire et la configuration. Active IQ affiche des informations complètes sur l'inventaire et la configuration logicielle et matérielle. Voyez quand les contrats de service arrivent à expiration pour vous assurer de rester couverts.

Informations associées

["Documentation NetApp : conseiller digital Active IQ"](#)

["Lancez Active IQ"](#)

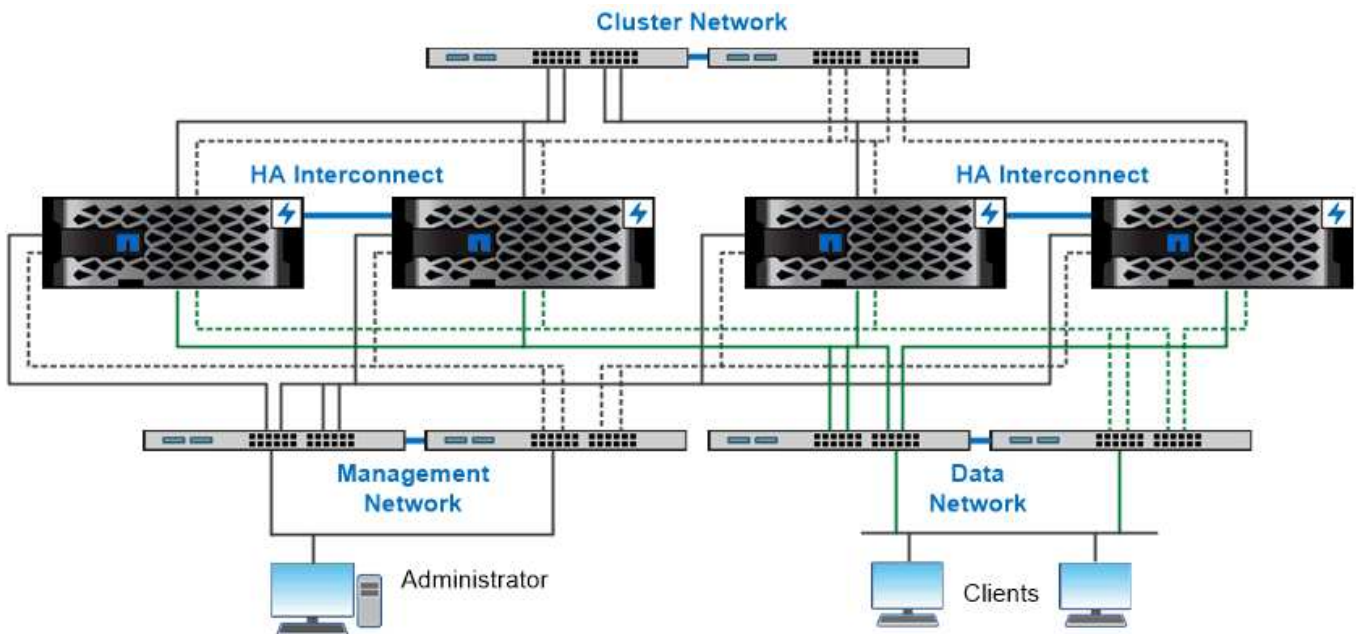
["Services SupportEdge"](#)

Architecture du réseau

Présentation de l'architecture réseau

L'architecture réseau d'une implémentation de data Center ONTAP se compose généralement d'une interconnexion de cluster, d'un réseau de gestion pour

l'administration de clusters et d'un réseau de données. Les cartes réseau (cartes d'interface réseau) fournissent des ports physiques pour les connexions Ethernet. Les HBA (adaptateurs de bus hôte) fournissent des ports physiques pour les connexions FC.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

Ports logiques

Outre les ports physiques fournis sur chaque nœud, vous pouvez utiliser *Logical ports* pour gérer le trafic réseau. Les ports logiques sont des groupes d'interfaces ou des VLAN.

Groupes d'interface

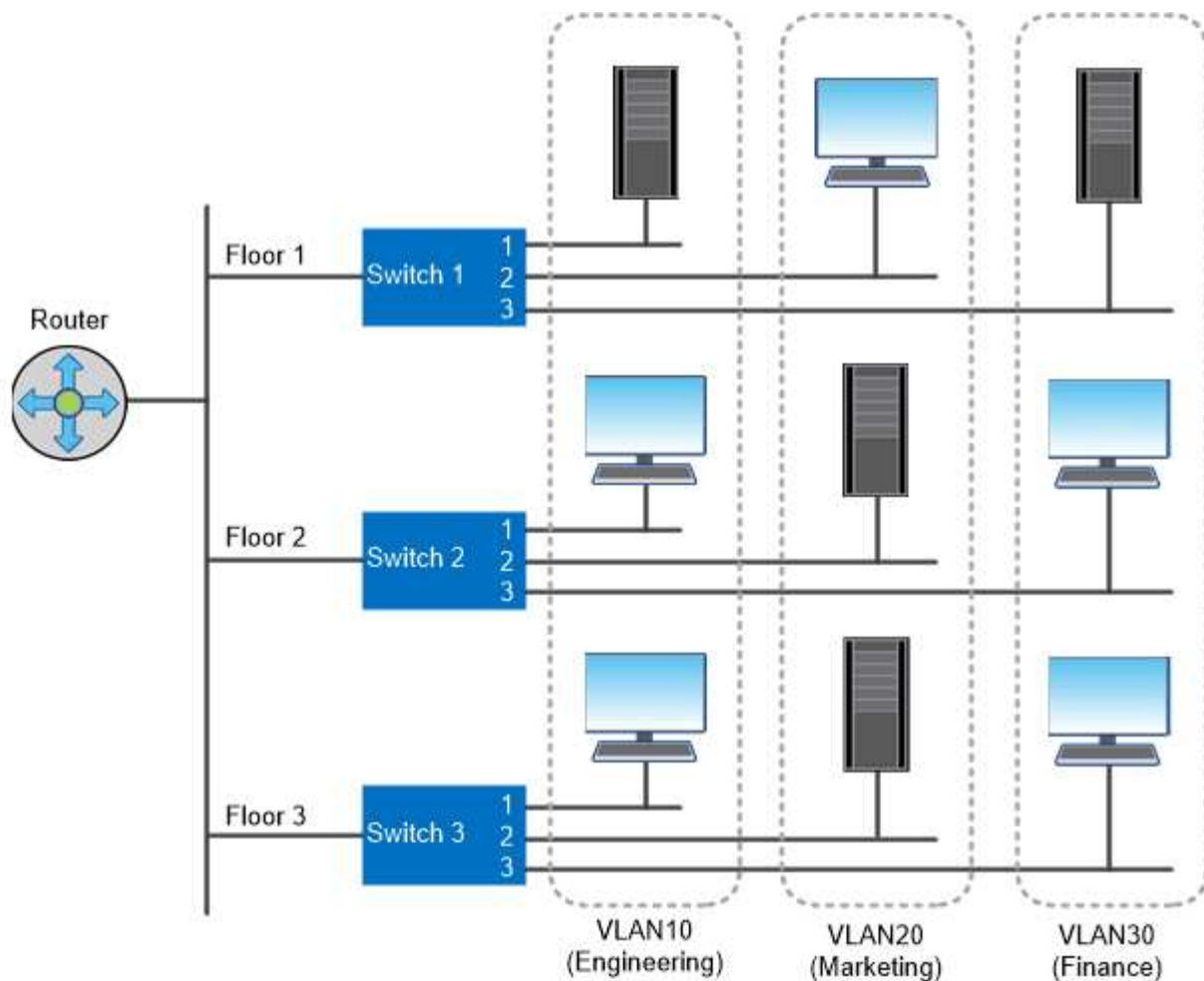
Interface Groups combine plusieurs ports physiques en un seul « port de jonction » logique. Vous pourriez vouloir créer un groupe d'interface composé de ports de cartes réseau dans différents emplacements PCI pour vous assurer qu'en cas de défaillance d'un slot, le trafic stratégique est réduit.

Un groupe d'interface peut être multimode ou dynamique en mode unique. Chaque mode offre différents niveaux de tolérance aux pannes. Vous pouvez utiliser l'un ou l'autre type de groupe d'interface multimode pour équilibrer la charge du trafic réseau.

VLAN

VLAN séparer le trafic d'un port réseau (qui peut être un groupe d'interfaces) en segments logiques définis sur une base de port de commutateur, plutôt que sur des limites physiques. Les *end-stations* appartenant à un VLAN sont liés par fonction ou application.

Vous pouvez regrouper les postes finaux par service, comme Ingénierie et Marketing, ou par projet, comme release1 et release2. Étant donné que la proximité physique des terminaux radio n'est pas pertinente dans un VLAN, les terminaux radio peuvent être géographiquement éloignés.



You can use VLANs to segregate traffic by department.

Prise en charge des technologies réseau standard

ONTAP prend en charge l'ensemble des principales technologies réseau standard de l'industrie. Les technologies clés sont les IPspaces, l'équilibrage de la charge DNS et les interruptions SNMP.

Les domaines de diffusion, les groupes de basculement et les sous-réseaux sont décrits dans le [Basculement de chemin NAS](#).

Les IPspaces

Vous pouvez utiliser un *IPspace* pour créer un espace d'adresse IP distinct pour chaque serveur de données virtuel dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

Par exemple, un fournisseur de services peut configurer des IPspaces différents pour les locataires à l'aide des mêmes adresses IP pour accéder à un cluster.

Équilibrage de charge DNS

Vous pouvez utiliser *DNS load balancing* pour distribuer le trafic réseau des utilisateurs à travers les ports disponibles. Un serveur DNS sélectionne dynamiquement une interface réseau pour le trafic en fonction du nombre de clients montés sur l'interface.

Interruptions SNMP

Vous pouvez utiliser *SNMP traps* pour vérifier périodiquement la présence de seuils ou d'échecs opérationnels. Les interruptions SNMP capturent les informations de surveillance système envoyées de façon asynchrone d'un agent SNMP à un gestionnaire SNMP.

Conformité FIPS

ONTAP est conforme à la norme FIPS (Federal Information Processing Standards) 140-2 pour toutes les connexions SSL. Vous pouvez activer et désactiver le mode SSL FIPS, définir globalement les protocoles SSL et désactiver tout chiffrement faible tel que RC4.

Présentation de RDMA

Les offres RDMA (Remote Direct Memory Access) d'ONTAP prennent en charge les charges de travail à large bande passante et sensibles à la latence. RDMA permet de copier directement les données entre la mémoire du système de stockage et la mémoire du système hôte, ce qui évite les interruptions du processeur et la surcharge.

NFS sur RDMA

Vous pouvez le configurer avec ONTAP 9.10.1 ["NFS sur RDMA"](#) Pour permettre l'utilisation du stockage NVIDIA GPUDirect pour les workloads avec accélération par processeur graphique sur des hôtes équipés de processeurs graphiques NVIDIA pris en charge.

Interconnexion de cluster RDMA

L'interconnexion de cluster RDMA réduit la latence, réduit les temps de basculement et accélère la communication entre les nœuds d'un cluster.

À partir de ONTAP 9.10.1, le protocole RDMA d'interconnexion de cluster est pris en charge pour certains systèmes matériels lorsqu'il est utilisé avec des cartes réseau de cluster X1151A. À partir de ONTAP 9.13.1, les cartes réseau X91153A prennent également en charge le protocole RDMA d'interconnexion de cluster. Consultez le tableau pour connaître les systèmes pris en charge dans les différentes versions de ONTAP.

Systèmes	Versions de ONTAP prises en charge
<ul style="list-style-type: none">• A400• ASA A400	ONTAP 9.10.1 et versions ultérieures
<ul style="list-style-type: none">• AFF A900• ASA A900• FAS9500	ONTAP 9.13.1 et versions ultérieures

Étant donné la configuration appropriée du système de stockage, aucune configuration supplémentaire n'est

nécessaire pour utiliser l'interconnexion RDMA.

Protocoles clients

ONTAP prend en charge tous les principaux protocoles client standard de l'industrie : NFS, SMB, FC, FCoE, iSCSI, NVMe/FC et S3.

NFS

NFS est le protocole d'accès classique aux fichiers pour les systèmes UNIX et LINUX. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles suivants.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- PNFS

Vous pouvez contrôler l'accès aux fichiers à l'aide d'autorisations de style UNIX, d'autorisations de style NTFS ou d'une combinaison des deux.

Les clients peuvent accéder aux mêmes fichiers à l'aide des protocoles NFS et SMB.

PME

SMB est le protocole d'accès aux fichiers traditionnel pour les systèmes Windows. Les clients peuvent accéder aux fichiers des volumes ONTAP à l'aide des protocoles SMB 2.0, SMB 2.1, SMB 3.0 et SMB 3.1.1. Tout comme avec NFS, plusieurs styles d'autorisation sont pris en charge.

SMB 1.0 est disponible mais désactivé par défaut dans les versions ONTAP 9.3 et ultérieures.

FC

Fibre Channel est le protocole de bloc en réseau d'origine. Au lieu de fichiers, un protocole de bloc présente l'ensemble d'un disque virtuel à un client. Le protocole FC traditionnel utilise un réseau FC dédié avec des commutateurs FC spécialisés et requiert que l'ordinateur client possède des interfaces réseau FC.

Une LUN représente le disque virtuel et une ou plusieurs LUN sont stockées dans un volume ONTAP. La même LUN est accessible via les protocoles FC, FCoE et iSCSI, mais plusieurs clients ne peuvent accéder à la même LUN que s'ils font partie d'un cluster qui empêche les collisions d'écriture.

FCoE

FCoE est en gros le même protocole que FC, mais utilise un réseau Ethernet de data Center à la place du transport FC classique. Le client requiert toujours une interface réseau spécifique à FCoE.

iSCSI

iSCSI est un protocole de bloc capable de s'exécuter sur les réseaux Ethernet standard. La plupart des systèmes d'exploitation clients proposent un initiateur logiciel qui fonctionne sur un port Ethernet standard. iSCSI est un bon choix pour quand un protocole de bloc est nécessaire pour une application particulière, mais

ne dispose pas d'une mise en réseau FC dédiée.

NVMe/FC

Le tout dernier protocole en mode bloc, NVMe/FC, est spécifiquement conçu pour fonctionner avec le stockage Flash. Dotée de sessions évolutives, d'une réduction considérable de la latence et d'une augmentation du parallélisme, cette solution convient parfaitement aux applications à faible latence et à haut débit, telles que les bases de données en mémoire et les analyses.

Contrairement à FC et iSCSI, NVMe n'utilise pas de LUN. Il utilise plutôt des espaces de noms, qui sont stockés dans un volume ONTAP. Les espaces de noms NVMe sont uniquement accessibles via le protocole NVMe.

S3

À partir de ONTAP 9.8, vous pouvez activer un serveur ONTAP simple Storage Service (S3) dans un cluster ONTAP, qui vous permet d'accéder aux données du stockage objet à l'aide des compartiments S3.

ONTAP prend en charge deux scénarios d'utilisation sur site pour la gestion du stockage objet S3 :

- FabricPool Tiering dans un compartiment du cluster local (Tier vers un compartiment local) ou du cluster distant (Tier cloud)
- L'application client S3 permet d'accéder à un compartiment sur le cluster local ou à distance.



ONTAP S3 est adapté si vous souhaitez utiliser des fonctionnalités S3 dans les clusters déjà en place, sans nécessiter de matériel ni de gestion supplémentaire. Pour des déploiements de plus de 300 To, le logiciel NetApp StorageGRID continue à être la solution phare de NetApp pour le stockage objet. Découvrez "[StorageGRID](#)".

Disques et agrégats

= :allow-uri-read:

Niveaux locaux (agrégats) et groupes RAID

Les technologies RAID modernes protègent contre les défaillances de disque en reconstruisant les données d'un disque défaillant sur un disque de secours. Le système compare les informations d'index sur un « disque de parité » avec les données des disques restants en bonne santé pour reconstruire les données manquantes, le tout sans temps d'arrêt ni coûts de performances significatifs.

Un niveau local (agrégat) se compose d'un ou plusieurs *RAID Groups*. Le *RAID type* du niveau local détermine le nombre de disques de parité du groupe RAID et le nombre de pannes de disque simultanées que la configuration RAID protège contre.

Le type RAID par défaut, RAID-DP (RAID-double parité), requiert deux disques de parité par groupe RAID et protège contre les pertes de données en cas de défaillance simultanée de deux disques. Pour le RAID-DP, la taille de groupe RAID recommandée est comprise entre 12 et 20 disques durs et entre 20 et 28 disques SSD.

Vous pouvez répartir le coût supplémentaire des disques de parité en créant des groupes RAID à la partie supérieure des recommandations de dimensionnement. Ceci est particulièrement vrai pour les disques SSD,

qui sont bien plus fiables que les disques haute capacité. Pour les niveaux locaux utilisant des disques durs, il est conseillé de choisir entre l'optimisation du stockage sur disque et les facteurs compensatoires, comme le délai de reconstruction plus long requis pour les groupes RAID plus volumineux.

Niveaux locaux en miroir et sans mise en miroir (agrégats)

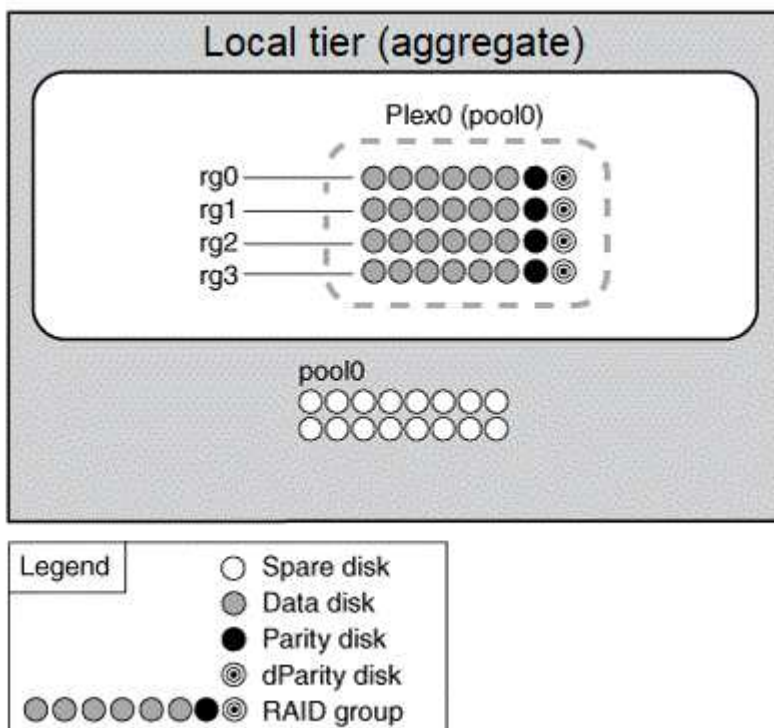
ONTAP dispose d'une fonction optionnelle appelée *SyncMirror* que vous pouvez utiliser pour mettre en miroir les données de niveau local (agrégat) de manière synchrone dans des copies, ou *plex*, stockées dans différents groupes RAID. Les plexes permettent d'éviter les pertes de données en cas de panne de l'ensemble des disques de type RAID, ou en cas de perte de connectivité aux disques du groupe RAID.

Lorsque vous créez un niveau local avec System Manager ou depuis l'interface de ligne de commandes, vous pouvez spécifier que le niveau local est mis en miroir ou non.

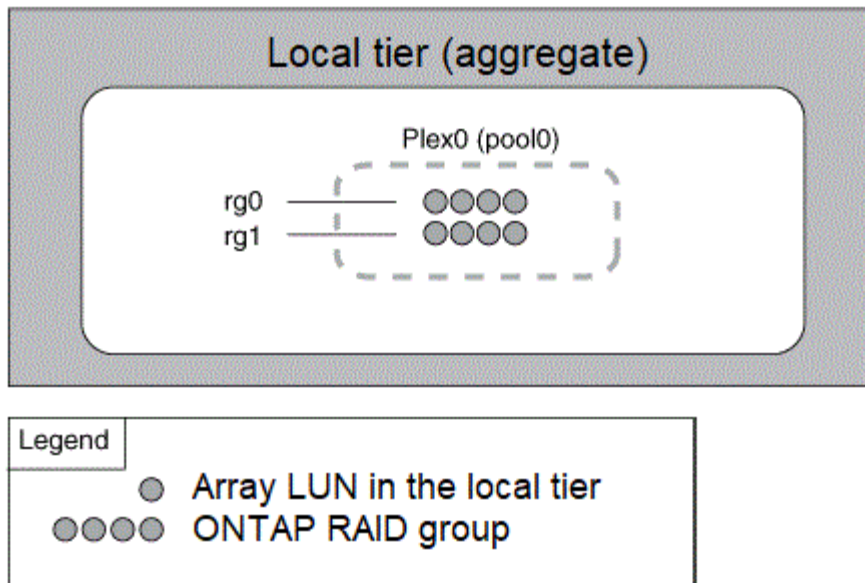
Fonctionnement des niveaux locaux non mis en miroir (agrégats)

Si vous ne spécifiez pas que les niveaux locaux sont mis en miroir, ils sont créés en tant que niveaux locaux non mis en miroir (agrégats). Les niveaux locaux non mis en miroir ne possèdent qu'un seul *plex* (une copie de leurs données), qui contient tous les groupes RAID appartenant à ce niveau local.

Le schéma suivant montre un niveau local non mis en miroir composé de disques, avec son plex unique. Le niveau local a quatre groupes RAID : rg0, rg1, rg2 et rg3. Chaque groupe RAID comporte six disques de données, un disque de parité et un disque de parité (double parité). Tous les disques utilisés par le niveau local proviennent du même pool, "pool0".



Le schéma suivant présente un niveau local non mis en miroir avec des LUN de matrice, avec son plex unique. Il dispose de deux groupes RAID, rg0 et rg1. Toutes les LUN de baie utilisées par le niveau local proviennent du même pool, « pool0 ».



Fonctionnement des niveaux locaux en miroir (agrégats)

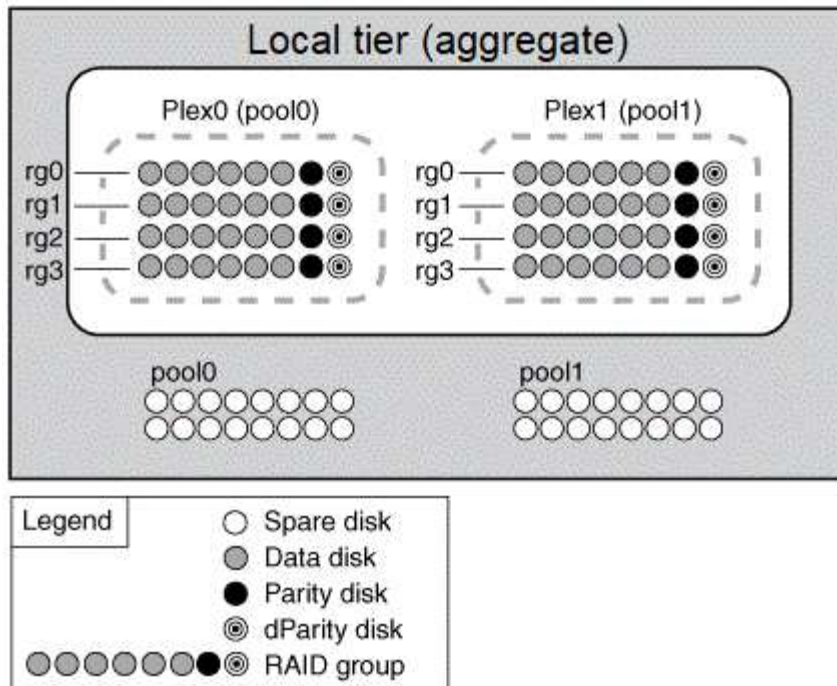
Les agrégats en miroir possèdent deux plexes_ (copies de leurs données), qui exploitent la fonctionnalité SyncMirror pour dupliquer les données pour assurer la redondance.

Lorsque vous créez un niveau local, vous pouvez spécifier qu'il s'agit d'un niveau local mis en miroir. En outre, vous pouvez ajouter un second plex à un niveau local non mis en miroir existant pour en faire un niveau en miroir. Grâce à la fonctionnalité SyncMirror, ONTAP copie les données du plex d'origine (plex0) sur le nouveau plex (plex1). Les plexes sont séparés physiquement (chaque plex dispose de ses propres groupes RAID et de son propre pool), et les plex sont mis à jour simultanément.

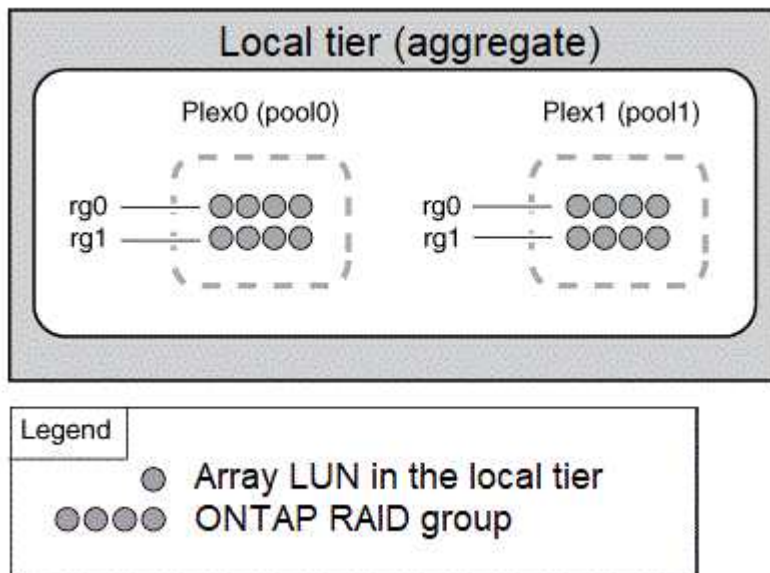
Cette configuration renforce la protection contre la perte de données en cas de défaillance de plus de disques que le niveau RAID de l'agrégat assure la protection contre ou en cas de perte de connectivité, car le plex non affecté continue de transmettre les données pendant que vous corrigez la cause de la défaillance. Une fois le plex qui avait un problème résolu, les deux plexes se synchronisent et rétablissent la relation du miroir.

Les disques et les unités logiques de baie du système sont répartis en deux pools : « pool0 » et « pool1 ». Plex0 obtient son stockage de pool0 et plex1 obtient son stockage de pool1.

Le schéma suivant présente un niveau local composé de disques pour que la fonctionnalité SyncMirror soit activée et implémentée. Un second plex a été créé pour le niveau local, « plex1 ». Les données dans le plex1 sont une copie des données dans le plex0 et les groupes RAID sont également identiques. Les 32 disques de réserve sont alloués à pool0 ou pool1 en utilisant 16 disques par pool.



Le schéma suivant présente un niveau local composé de LUN de baie dont la fonctionnalité SyncMirror est activée et implémentée. Un second plex a été créé pour le niveau local, « plex1 ». Plex1 est une copie de plex0 et les groupes RAID sont également identiques.



Pour optimiser les performances et la disponibilité du stockage, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces meilleures pratiques peut avoir un impact négatif sur les performances.

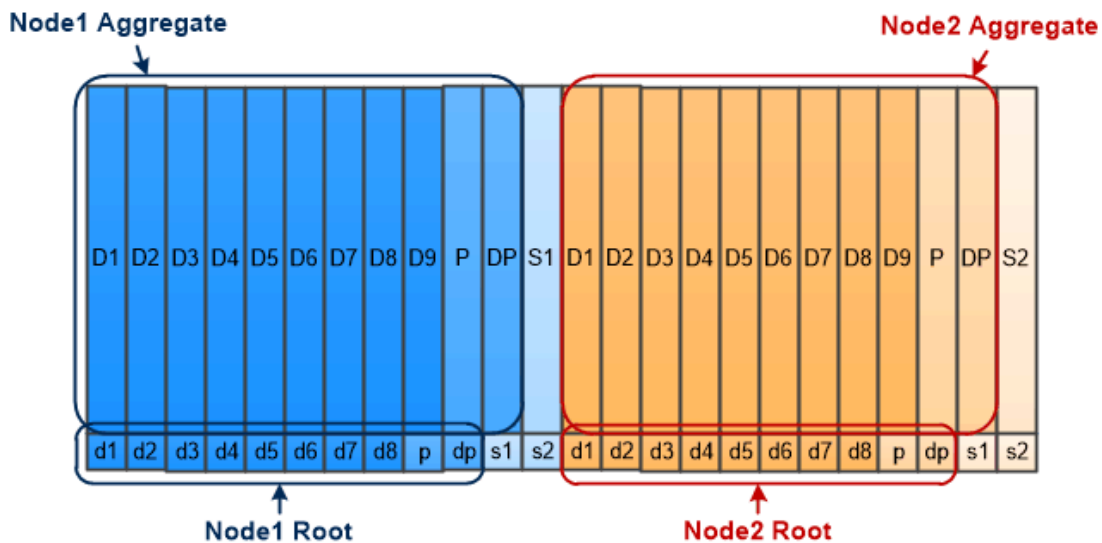
Partitionnement données-racines

Chaque nœud doit disposer d'un agrégat racine pour les fichiers de configuration du système de stockage. L'agrégat root dispose du type RAID de l'agrégat de données.

System Manager ne prend pas en charge le partitionnement données-racines ou données-racines.

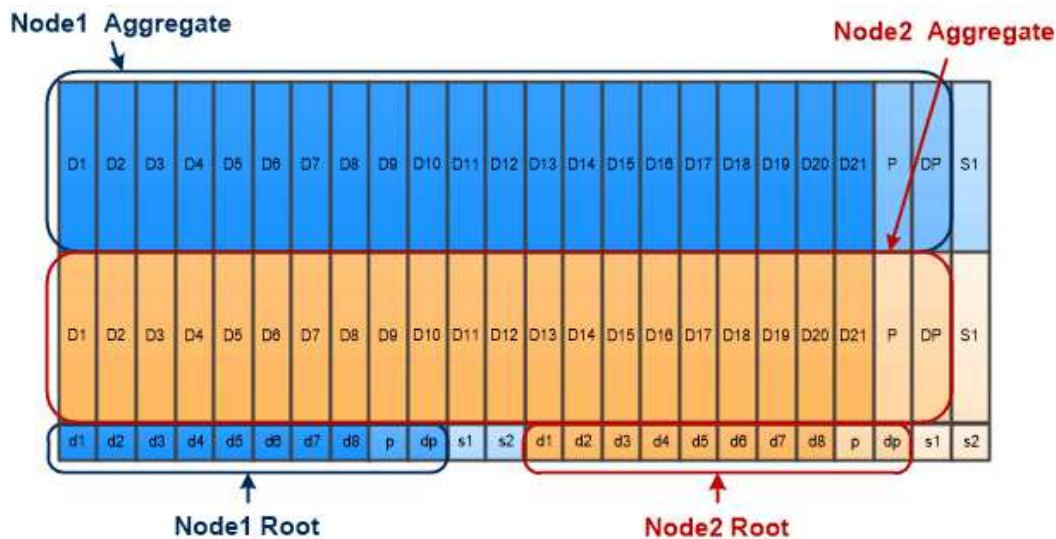
Un agrégat racine de type RAID-DP se compose généralement d'un disque de données et de deux disques de parité. Il s'agit là d'un surcoût important « parité » pour payer les fichiers du système de stockage, lorsque le système réserve déjà deux disques en tant que disques de parité pour chaque groupe RAID de l'agrégat.

Root-Data partition réduit les taxes sur les parité en répartissant l'agrégat racine sur les partitions de disque, en réservant une petite partition sur chaque disque en tant que partition racine et une grande partition pour les données.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

Comme l'indique l'illustration, plus le nombre de disques utilisés pour stocker l'agrégat racine est important, plus la partition racine est petite. C'est également le cas d'une forme de partitionnement données-racines appelée *root-data-partition*, qui crée une petite partition comme partition racine et deux partitions de taille égale pour les données.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Les deux types de partitionnement données-racines font partie de la fonctionnalité ONTAP *Advanced Drive Partitionnement (ADP)*. Les deux sont configurés en usine : partitionnement données-racines pour les systèmes d'entrée de gamme FAS2xxx, FAS9000, FAS8200, FAS80xx et AFF, partitionnement données-racines uniquement pour les systèmes AFF.

En savoir plus sur ["Partitionnement de disque avancé"](#).

Disques partitionnés et utilisés pour l'agrégat racine

Les disques partitionnés à utiliser dans l'agrégat racine dépendent de la configuration du système.

Connaître le nombre de disques utilisés pour l'agrégat racine vous aide à déterminer la capacité des disques consacrée à la partition racine, et la quantité disponible pour un agrégat de données.

La fonctionnalité de partitionnement données-racines est prise en charge pour les plateformes d'entrée de gamme, les plateformes FAS 100 % Flash et les plateformes FAS uniquement associées à des disques SSD.

Pour les plateformes d'entrée de gamme, seuls les disques internes sont partitionnés.

Pour toutes les plateformes FAS Flash et FAS avec uniquement des disques SSD connectés, tous les disques reliés au contrôleur lors de l'initialisation du système sont partitionnés, dans la limite de 24 par nœud. Les disques ajoutés après la configuration du système ne sont pas partitionnés.

Volumes, qtrees, fichiers et LUN

ONTAP fournit les données aux clients et aux hôtes à partir des conteneurs logiques appelés *FlexVol volumes*. ces volumes étant associés uniquement à leur agrégat contenant, ils offrent une plus grande flexibilité de gestion des données que les volumes traditionnels.

Vous pouvez attribuer plusieurs volumes FlexVol à un agrégat, chacun dédié à une autre application ou service. Vous pouvez étendre et réduire un volume FlexVol, déplacer un volume FlexVol et effectuer des copies efficaces d'un volume FlexVol. Vous pouvez utiliser des qtrees_ pour partitionner un volume FlexVol en

unités plus gérables et *quotas* pour limiter l'utilisation des ressources des volumes.

Les volumes contiennent des systèmes de fichiers dans un environnement NAS et des LUN dans un environnement SAN. Une LUN (numéro d'unité logique) est un identifiant pour un périphérique appelé une unité logique adressée par un protocole SAN.

Les LUN sont l'unité de stockage de base dans une configuration SAN. L'hôte Windows considère que des LUN de votre système de stockage sont des disques virtuels. Vous pouvez déplacer des LUN vers d'autres volumes sans interruption.

Outre les volumes de données, vous devez connaître quelques volumes spéciaux :

- Un *node root volume* (en général « vol0 ») contient des informations sur la configuration du nœud et des journaux.
- Un *SVM root volume* sert de point d'entrée au namespace fourni par le SVM et contient des informations sur le répertoire d'espace de noms.
- *System volumes* contient des métadonnées spéciales telles que les journaux d'audit de service.

Vous ne pouvez pas utiliser ces volumes pour stocker des données.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

volumes FlexGroup

Dans certaines entreprises, un seul namespace peut nécessiter plusieurs pétaoctets de stockage, voire même une capacité de 100 To d'un volume FlexVol.

Un *FlexGroup volume* prend en charge jusqu'à 400 milliards de fichiers avec 200 volumes de membres constitutifs qui travaillent en collaboration afin d'équilibrer de façon dynamique la charge et l'allocation d'espace entre les différents membres.

Les volumes FlexGroup ne nécessitent aucune surcharge administrative ou de maintenance. Il vous suffit de créer le volume FlexGroup et de le partager avec vos clients NAS. ONTAP se charge du reste.

Virtualisation du stockage

Présentation de la virtualisation du stockage

Utilisez *Storage Virtual machines (SVM)* pour fournir des données aux clients et aux hôtes. À l'instar d'une machine virtuelle fonctionnant sur un hyperviseur, un SVM est une entité logique qui extrait les ressources physiques. L'accès aux données via la SVM n'est pas limité à un emplacement de stockage. L'accès réseau au SVM n'est pas lié à un port physique.



Les SVM étaient auparavant appelés « vservers ». L'interface de ligne de commande de ONTAP utilise toujours le terme « vserver ».

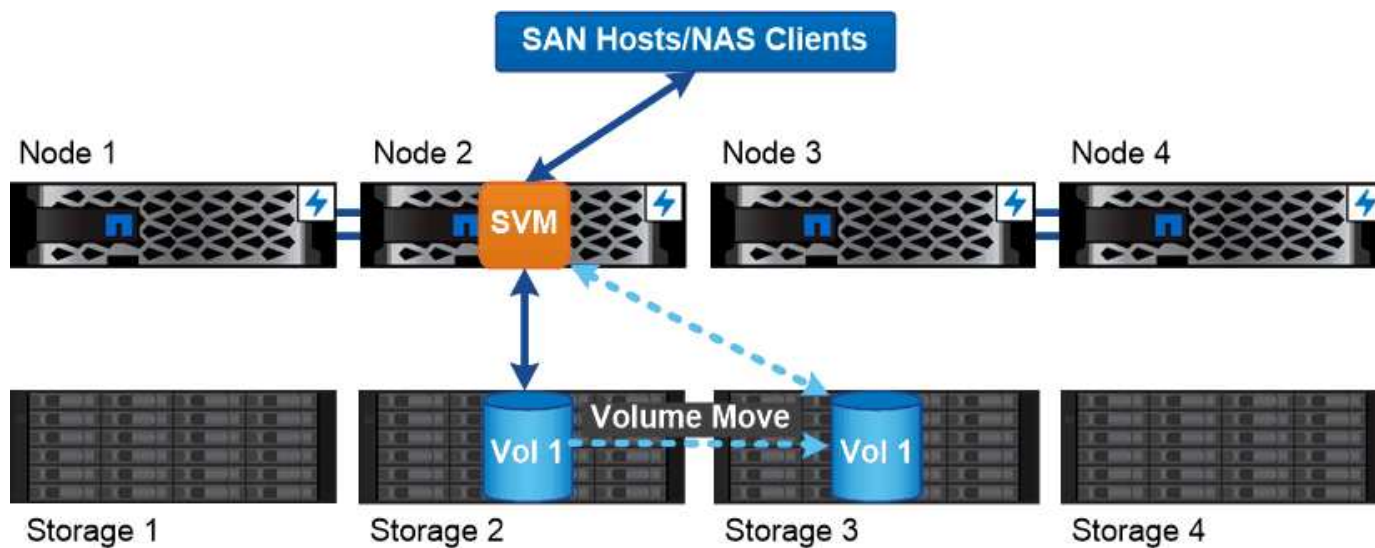
Un SVM fournit des données aux clients et hôtes depuis un ou plusieurs volumes via une ou plusieurs interfaces logiques réseau (LIF). Les volumes peuvent être affectés à n'importe quel agrégat de données du cluster. Les LIFs peuvent être hébergées par n'importe quel port physique ou logique. Les volumes et les LIF peuvent être déplacés sans interrompre le service de données, que vous travailliez pour des mises à niveau matérielles, des nœuds, des équilibrer les performances ou optimiser la capacité entre les agrégats.

La même SVM peut disposer d'une LIF pour le trafic NAS et d'une LIF pour le trafic SAN. Les clients et les hôtes ont uniquement besoin de l'adresse de la LIF (adresse IP pour NFS, SMB ou iSCSI ; WWPN pour FC) pour accéder à la SVM. Les LIF conservent leur adresse lors de leur déplacement. Les ports peuvent héberger de multiples LIFs. Chaque SVM possède son propre système de sécurité, d'administration et de namespace.

En plus des SVM de données, ONTAP déploie des SVM spéciaux pour l'administration :

- Un SVM *admin* est créé lorsque le cluster est configuré.
- Un *node SVM* est créé lorsqu'un nœud rejoint un cluster nouveau ou existant.
- Un SVM_System_ est automatiquement créé pour les communications au niveau du cluster dans un IPspace.

Vous ne pouvez pas utiliser ces SVM pour fournir des données. Il existe également des LIF spéciales permettant le trafic au sein des clusters et entre eux, et pour la gestion du cluster et des nœuds.



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

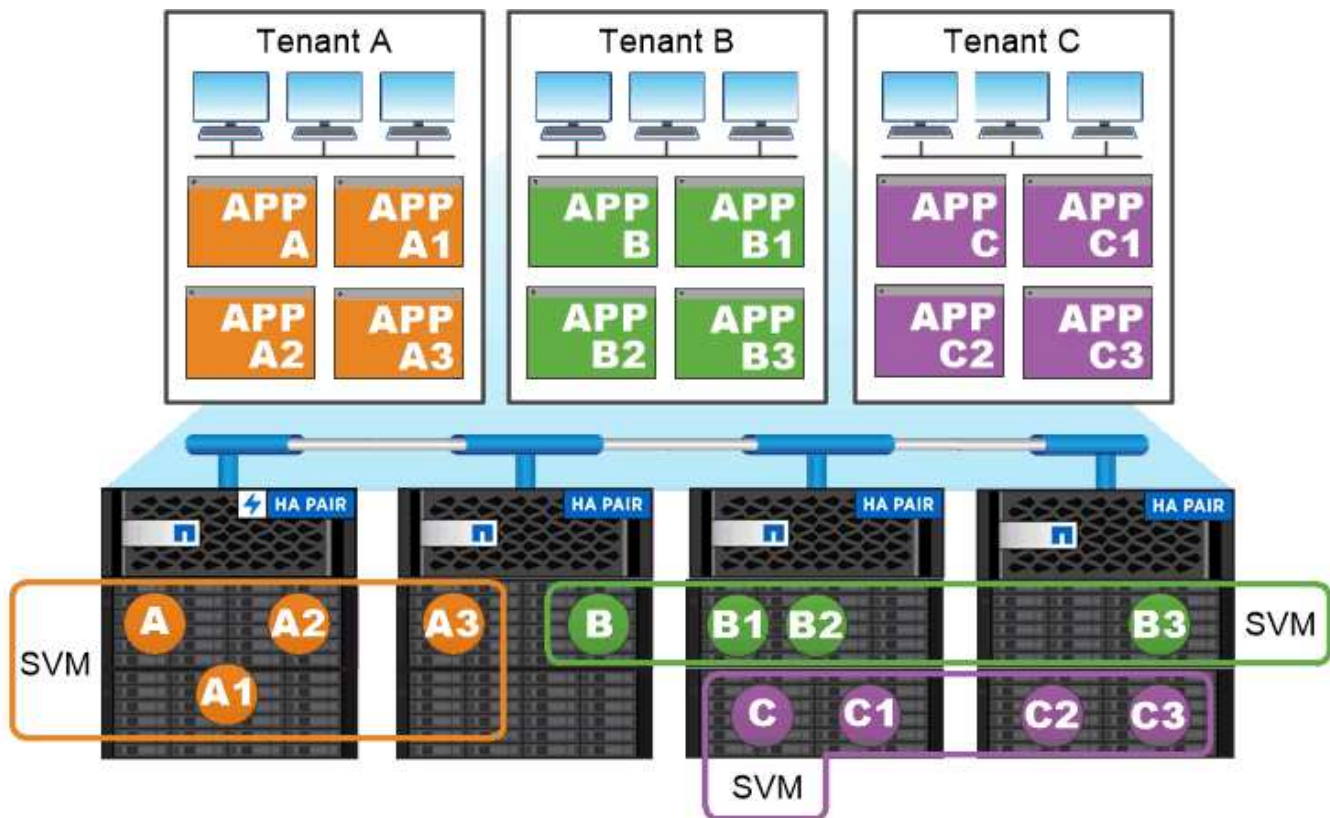
Pourquoi ONTAP est comme le middleware

Les objets logiques utilisés par ONTAP pour les tâches de gestion du stockage servent les objectifs familiers d'un paquet de middleware bien conçu : protéger l'administrateur des détails de mise en œuvre de bas niveau et isoler la configuration des modifications de caractéristiques physiques telles que les nœuds et les ports. De base, l'administrateur doit pouvoir déplacer facilement des volumes et des LIF en reconfigurer quelques champs au lieu de l'intégralité de l'infrastructure de stockage.

Cas d'utilisation de SVM

Les Service Providers utilisent des SVM dans le cadre d'accords de colocation sécurisée afin d'isoler les données de chaque locataire, de fournir à chacun d'eux ses propres fonctionnalités d'authentification et d'administration, et de simplifier la refacturation. Vous pouvez attribuer plusieurs LIF à la même SVM afin de répondre aux différents besoins des clients et utiliser la qualité de service pour vous protéger des charges de travail mutualisées et « brider » les charges de travail des autres locataires.

Les administrateurs utilisent des SVM à des fins similaires dans l'entreprise. Vous pouvez isoler les données de différents départements ou préserver l'accès aux volumes de stockage des hôtes dans un SVM et les volumes de partage d'utilisateurs dans un autre. Certains administrateurs placent les LUN iSCSI/FC et les datastores NFS dans un partage SVM et SMB dans un autre.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

Administration des clusters et des SVM

Un *cluster Administrator* accède au SVM d'admin pour le cluster. La SVM d'admin et un administrateur du cluster avec le nom réservé `admin` sont automatiquement créés lorsque le cluster est configuré.

Un administrateur de cluster avec la valeur par défaut `admin` le rôle peut administrer l'ensemble du cluster et ses ressources. L'administrateur du cluster peut créer d'autres administrateurs de cluster disposant de différents rôles selon les besoins.

Un *administrateur SVM* accède à un SVM de données. L'administrateur du cluster crée des SVM de données et des administrateurs SVM si nécessaire.

Les administrateurs du SVM sont affectés à `vsadmin` rôle par défaut. L'administrateur du cluster peut attribuer différents rôles aux administrateurs du SVM si nécessaire.

contrôle d'accès basé sur les rôles (RBAC)

Le *role* attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Espaces de noms et points de jonction

Un NAS *namespace* est un regroupement logique de volumes regroupés à *Junction points* pour créer une seule hiérarchie de système de fichiers. Un client disposant des autorisations suffisantes peut accéder aux fichiers dans l'espace de noms sans spécifier l'emplacement des fichiers dans le stockage. Des volumes regroupés dans le cluster peuvent se trouver n'importe où.

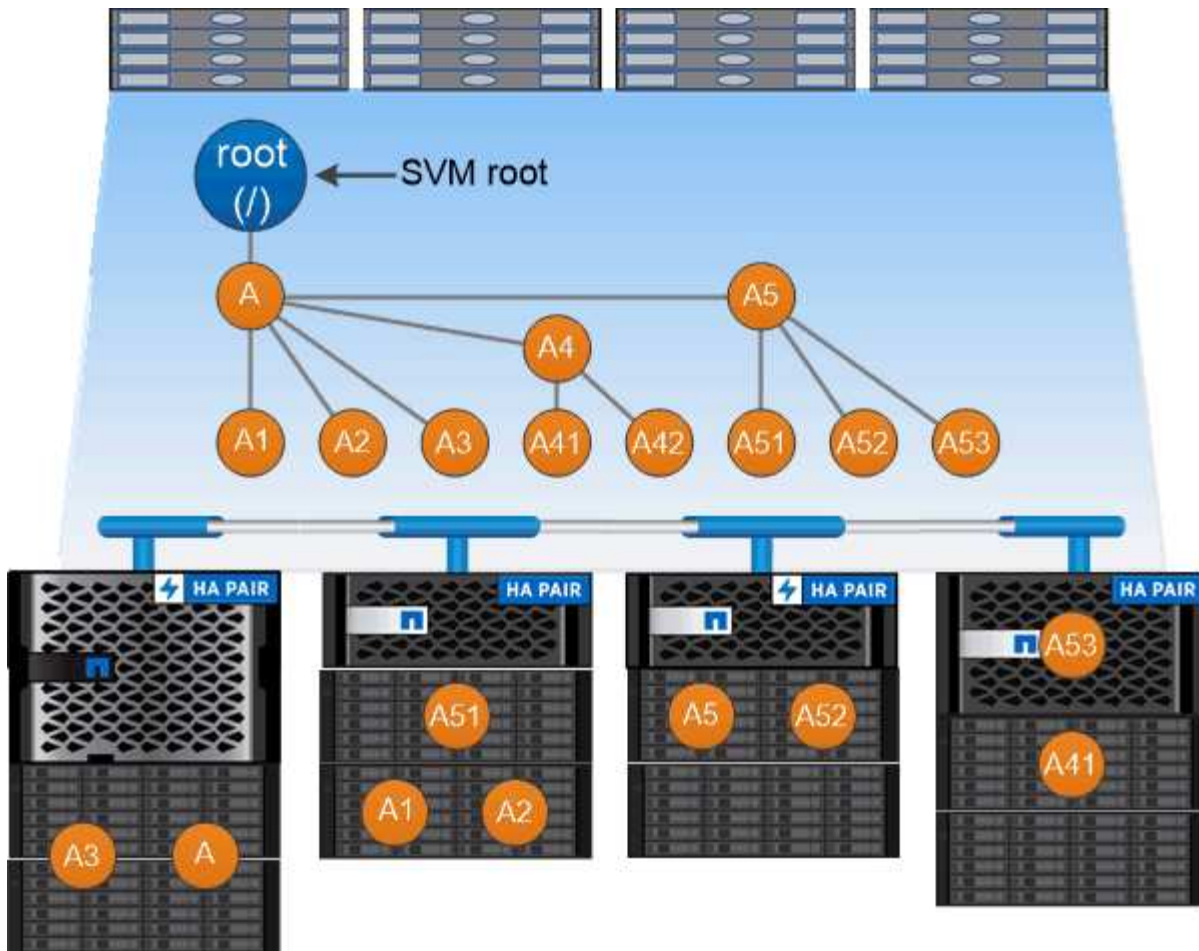
Plutôt que de monter chaque volume contenant un fichier d'intérêt, les clients NAS monter un NFS *export* ou accéder à un partage SMB. L'exportation ou le partage représente l'intégralité de l'espace de noms ou un emplacement intermédiaire dans l'espace de noms. Le client n'accède qu'aux volumes montés sous son point d'accès.

Vous pouvez ajouter des volumes au namespace selon vos besoins. Vous pouvez créer des points de jonction directement en-dessous d'une jonction de volume parent ou sur un répertoire au sein d'un volume. Il se peut qu'un chemin vers une jonction de volume pour un volume nommé « vol3 » soit possible /vol1/vol2/vol3, ou /vol1/dir2/vol3, ou même /dir1/dir2/vol3. Le chemin est appelé *Junction path*.

Chaque SVM possède un espace de noms unique. Le volume root du SVM est le point d'entrée de la hiérarchie de l'espace de noms.



Pour garantir la disponibilité des données en cas de panne du nœud ou de basculement, vous devez créer une copie *load-sharing mirror* pour le volume root du SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Basculement de chemin

Présentation du basculement de chemin

La gestion du basculement de chemin dans les topologies NAS et SAN est deux différences importantes dans la façon dont ONTAP gère ce basculement. Une LIF NAS migre automatiquement vers un autre port réseau après une panne de liaison. Une LIF SAN ne migre pas (sauf si vous la déplacez manuellement après la panne). La technologie de chemins d'accès multiples sur l'hôte transfère le trafic vers une autre

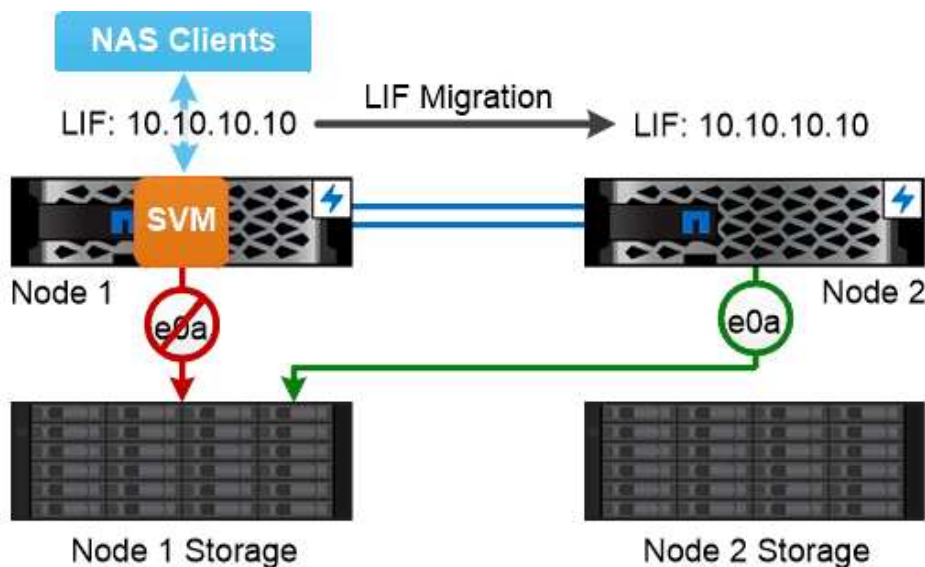
LIF—sur le même SVM, mais vers un autre port réseau.

Basculement de chemin NAS

Une LIF NAS migre automatiquement vers un port réseau survivant après une panne de liaison sur son port actuel. Le port vers lequel la LIF migre doit être membre de la *failover group* pour la LIF. La *failover group policy* permet de rétrécir les cibles de basculement pour une LIF de données vers les ports sur le nœud qui possède les données et son partenaire de haute disponibilité.

Pour des raisons de commodité administrative, ONTAP crée un groupe de basculement pour chaque *broadcast domain* dans l'architecture réseau. Les domaines de diffusion regroupent des ports appartenant au même réseau de couche 2. Si vous utilisez des VLAN, par exemple, pour isoler le trafic par département (ingénierie, marketing, finance, etc.), chaque VLAN définit un domaine de diffusion distinct. Le groupe de basculement associé au domaine de diffusion est automatiquement mis à jour chaque fois que vous ajoutez ou supprimez un port de broadcast domain.

Il est presque toujours bon d'utiliser un domaine de diffusion pour définir un groupe de basculement pour s'assurer que le groupe de basculement reste à jour. Toutefois, vous pouvez parfois définir un groupe de basculement qui n'est pas associé à un domaine de diffusion. Par exemple, vous pouvez vouloir que les LIFs échouent uniquement en cas de ports d'un sous-ensemble des ports définis dans le broadcast domain.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

sous-réseaux

A *subnet* réserve un bloc d'adresses IP dans un domaine de diffusion. Ces adresses appartiennent au même réseau de couche 3 et sont allouées aux ports du broadcast domain lorsque vous créez une LIF. Il est généralement plus facile et moins sujette aux erreurs pour spécifier un nom de sous-réseau lorsque vous définissez une adresse LIF qu'il ne doit spécifier une adresse IP et un masque réseau.

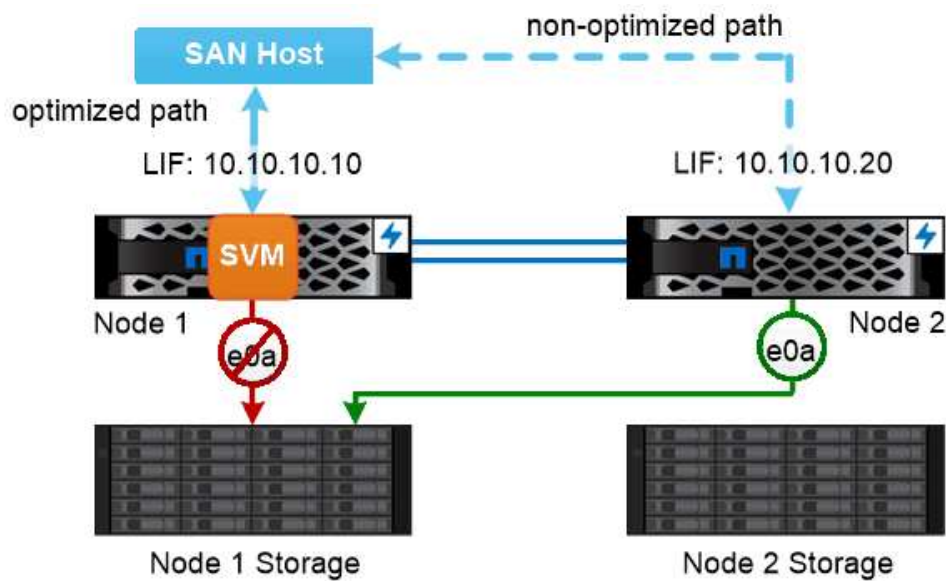
Basculement de chemin SAN

Un hôte SAN utilise le protocole ALUA (Asymmetric Logical Unit Access) et MPIO (chemins d'accès E/S multiples) pour rediriger le trafic vers un LIF survivant après une défaillance de liaison. Les chemins prédéfinis déterminent les voies possibles vers la LUN desservie par la SVM.

Dans un environnement SAN, les hôtes sont considérés comme des *initiateurs* des requêtes vers des LUN *Targets*. MPIO active plusieurs chemins d'accès des initiateurs aux cibles. ALUA identifie les chemins les plus directs, appelés « chemins optimisés ».

Vous configurez généralement plusieurs chemins optimisés vers les LIF sur le nœud propriétaire de la LUN, ainsi que plusieurs chemins non optimisés vers ceux-ci sur son partenaire haute disponibilité. Si un port tombe en panne sur le nœud propriétaire, l'hôte achemine le trafic vers les ports survivants. Si tous les ports échouent, l'hôte achemine le trafic sur les chemins non optimisés.

Par défaut, ONTAP Selective LUN Map (SLM) limite le nombre de chemins d'accès de l'hôte à une LUN. Une LUN nouvellement créée est accessible uniquement via des chemins vers le nœud qui possède la LUN ou son partenaire de haute disponibilité. Vous pouvez également limiter l'accès à une LUN en configurant des LIFs dans un *port set* pour l'initiateur.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

déplacement de volumes dans des environnements SAN

Par défaut, *ONTAP Selective LUN Map (SLM)* limite le nombre de chemins d'accès à une LUN à partir d'un hôte SAN. Une LUN nouvellement créée n'est accessible qu'via des chemins vers le nœud qui possède la LUN ou son partenaire de haute disponibilité, le *node reporting* pour la LUN.

En effet, lorsque vous déplacez un volume vers un nœud d'une autre paire haute disponibilité, vous devez ajouter des nœuds de reporting pour la paire haute disponibilité de destination au mappage de LUN. Vous pouvez ensuite spécifier les nouveaux chemins dans la configuration de MPIO. Une fois le déplacement de volume terminé, vous pouvez supprimer des nœuds de reporting de la paire haute disponibilité source du mappage.

Équilibrage de la charge

Les performances des charges de travail commencent à être affectées par la latence lorsque le volume de travail d'un nœud dépasse les ressources disponibles. Vous pouvez gérer un nœud surchargé en augmentant les ressources disponibles (mise à niveau des disques ou du processeur) ou en réduisant la charge (déplacement de volumes ou de LUN vers des nœuds différents selon les besoins).

Vous pouvez également utiliser la qualité de service (QoS) du stockage ONTAP_ pour garantir que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes :

- Vous pouvez fixer un plafond de débit QoS pour une charge de travail concurrente afin de limiter son impact sur les ressources système (QoS Max).
- Vous pouvez définir un débit QoS *sol* pour une charge de travail stratégique, afin de vous assurer qu'il répond aux objectifs de débit minimaux indépendamment de la demande des charges de travail concurrentes (QoS min).
- Vous pouvez définir un plafond et un sol QoS pour la même charge de travail.

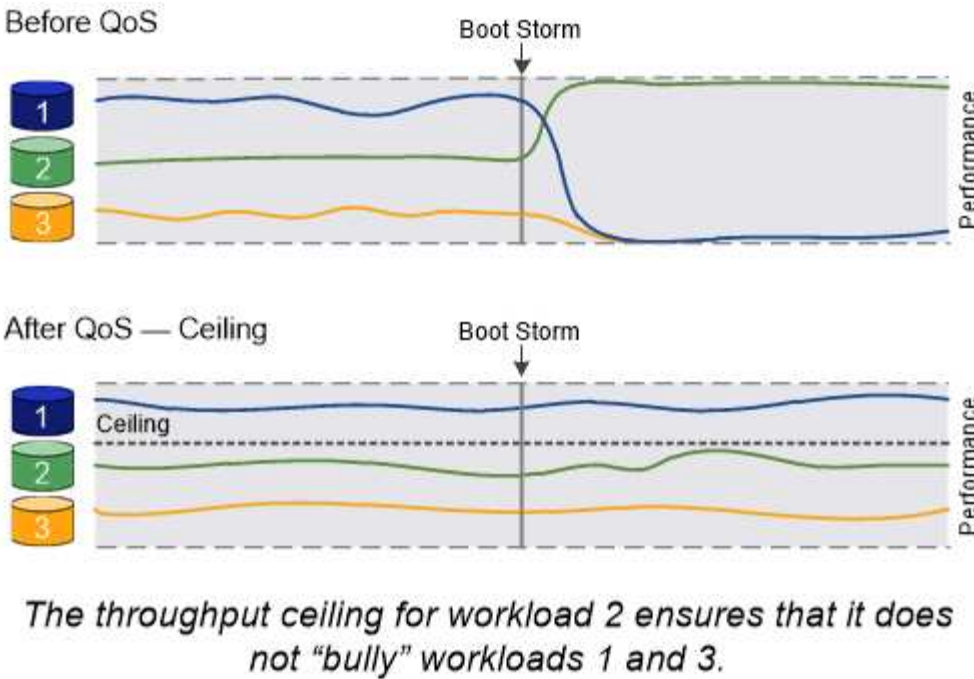
Plafonds de débit

Un plafond de débit limite le débit d'une charge de travail à un nombre maximal d'IOPS ou de Mo/s. Dans la figure ci-dessous, le plafond de débit pour la charge de travail 2 garantit qu'il ne s'agit pas de charges de travail « dominantes » 1 et 3.

Un *policy group* définit le plafond de débit pour une ou plusieurs charges de travail. Une charge de travail représente les opérations d'E/S pour un objet de *stockage* : un volume, un fichier ou une LUN, ou tous les volumes, fichiers ou LUN d'un SVM. Vous pouvez spécifier le plafond lorsque vous créez le groupe de règles ou attendre jusqu'à ce que vous contrôliez les charges de travail pour les spécifier.



Le débit des charges de travail peut dépasser jusqu'à 10 % le plafond spécifié, en particulier si une charge de travail a des variations rapides du débit. Le plafond peut être dépassé de 50 % pour gérer les rafales.



Le niveau de débit

Un étage de débit garantit que le débit d'une charge de travail ne se trouve pas en dessous du nombre minimal d'IOPS. Dans la figure ci-dessous, les niveaux de débit pour la charge de travail 1 et la charge de travail 3 s'assurent qu'ils répondent aux objectifs de débit minimum, indépendamment de la demande par charge de travail 2.

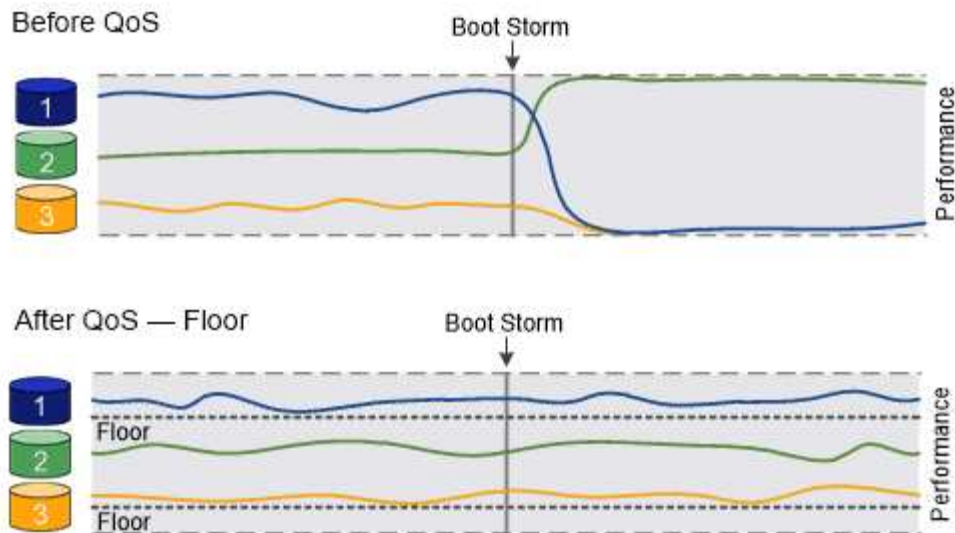


Comme le suggèrent les exemples, un plafond de débit accélère directement le débit. Un plancher de débit accélère indirectement le débit en donnant la priorité aux charges de travail pour lesquelles le sol a été défini.

Une charge de travail représente les opérations d'E/S d'un volume, d'une LUN ou, en commençant par un fichier ONTAP 9.3. Un groupe de règles qui définit un étage de débit ne peut pas être appliqué à un SVM. Vous pouvez spécifier l'étage lors de la création du groupe de règles ou attendre jusqu'à ce que vous surveilliez les charges de travail pour le spécifier.



Le débit d'une charge de travail peut tomber en dessous du seuil spécifié si la capacité de performance est insuffisante (marge) sur le nœud ou l'agrégat, ou lors des opérations stratégiques comme `volume move trigger-cutover`. Même lorsque vous disposez d'une capacité suffisante et que vos opérations stratégiques ne sont pas effectuées, le débit d'une charge de travail peut tomber en dessous du seuil spécifié de 5 %.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

La QoS adaptative

En principe, la valeur du groupe de règles que vous attribuez à un objet de stockage est fixe. Vous devez modifier la valeur manuellement lorsque la taille de l'objet de stockage change. Une augmentation de l'espace utilisé sur un volume, par exemple, nécessite généralement une augmentation correspondante du plafond de débit spécifié pour le volume.

Adaptive QoS ajuste automatiquement la valeur du groupe de règles en fonction de la taille de la charge de travail, en maintenant le rapport IOPS/To|Go en fonction de la taille des modifications de la charge de travail. C'est un avantage considérable pour la gestion de centaines, voire de milliers de charges de travail dans le cadre d'un déploiement à grande échelle.

Généralement, vous utilisez la QoS adaptative pour ajuster les plafonds de débit, mais vous pouvez également l'utiliser pour gérer le débit (en cas d'augmentation de la taille des charges de travail). La taille du workload est exprimée en espace alloué à l'objet de stockage ou en espace utilisé par l'objet de stockage.



L'espace utilisé est disponible pour les étages de débit dans ONTAP 9.5 et versions ultérieures. Elle n'est pas prise en charge pour les étages de débit dans ONTAP 9.4 et les versions antérieures.

+ À partir de la ONTAP 9.13.1, vous pouvez utiliser la QoS adaptative pour définir des planchers et des plafonds de débit au niveau des SVM.

- Une politique *Allocated space* maintient le ratio IOPS/To|Go en fonction de la taille nominale de l'objet de stockage. Si le rapport est de 100 IOPS/Go, un volume de 150 Go plafonné à 15,000 IOPS, tant que la taille du volume reste celle-ci. Si le volume a été redimensionné de façon à 300 Go, la QoS adaptative ajuste le débit au plafond à 30,000 000 IOPS.
- Une règle *Used space* (par défaut) maintient le ratio IOPS/To|Go en fonction de la quantité de données réelles stockées avant le stockage efficace. Si le rapport est de 100 IOPS/Go, un volume de 150 Go contenant 100 Go de données stockées aurait un débit plafond de 10,000 000 IOPS. À mesure que la quantité d'espace utilisée change, la QoS adaptative ajuste le plafond de débit en fonction du rapport.

La réplication

Copies Snapshot

Les technologies de réplication ONTAP exigeaient les reprises après incident et les archivages. Avec l'avènement des services cloud, la réplication ONTAP a été adaptée au transfert des données entre les terminaux dans l'environnement NetApp Data Fabric. Ces utilisations reposent sur la technologie Snapshot de ONTAP.

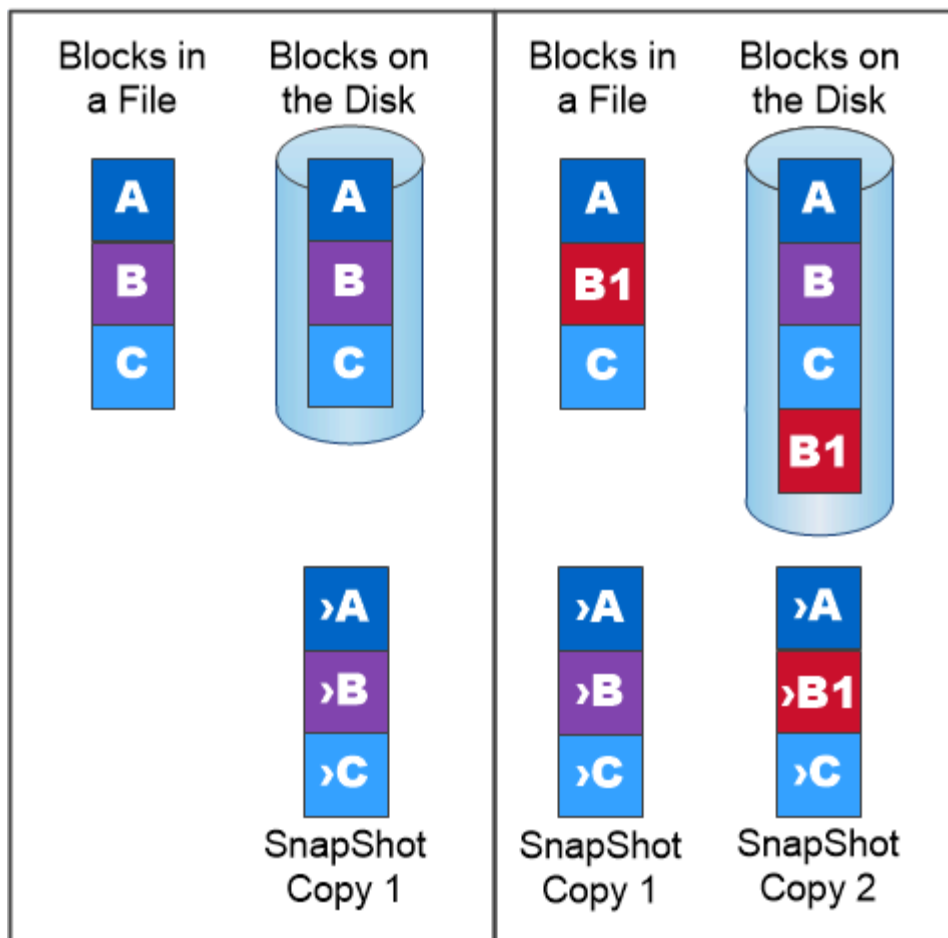
Une *copie snapshot* est une image ponctuelle en lecture seule d'un volume. Après la création d'une copie Snapshot, le système de fichiers actif et la copie Snapshot pointent vers les mêmes blocs de disque. Ainsi, la copie Snapshot n'utilise pas d'espace disque supplémentaire. Au fil du temps, l'image consomme un espace de stockage minimal et implique un impact négligeable sur les performances, car elle n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot.

Les copies Snapshot doivent leur efficacité à la technologie de virtualisation du stockage principale d'ONTAP, sa *WAFL (Write Anywhere File Layout)*. comme une base de données, WAFL utilise des métadonnées pour pointer les blocs de données réels du disque. Contrairement à une base de données, WAFL ne remplace pas les blocs existants. Il écrit les données mises à jour sur un nouveau bloc et modifie les métadonnées.

Les copies Snapshot sont efficaces car, au lieu de copier des blocs de données, ONTAP référence les métadonnées lors de la création d'une copie Snapshot. Ainsi, vous éliminez à la fois le temps de recherche que d'autres systèmes impliquent pour localiser les blocs à copier et le coût lié à la copie.

Vous pouvez utiliser une copie Snapshot pour restaurer des fichiers ou des LUN individuels, ou pour restaurer l'ensemble du contenu d'un volume. ONTAP compare les informations du pointeur de la copie Snapshot aux données d'un disque pour reconstruire l'objet manquant ou endommagé, sans temps d'indisponibilité ni coûts de performance significatifs.

Une règle *Snapshot* définit la façon dont le système crée des copies Snapshot de volumes. La règle indique quand créer les copies Snapshot, le nombre de copies à conserver, comment les nommer et comment les étiqueter pour la réplication. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes, les nommer « diotidienne » (ajoutée avec un horodatage) et les étiqueter « dootidienne » pour la réplication.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Reprise sur incident et transfert de données SnapMirror

SnapMirror est une technologie de reprise après incident conçue pour le basculement du stockage primaire vers le stockage secondaire sur un site distant. Comme son nom l'indique, SnapMirror crée une réplique ou *mirror* de vos données de travail dans un stockage secondaire à partir duquel vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.

Les données sont mises en miroir au niveau du volume. La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation *protection des données* ». les clusters dans lesquels résident les volumes et les SVM qui fournissent des données à partir de ces volumes doivent être *peered*. Une relation de pairs permet l'échange de clusters et de SVM sécurité des données.



Vous pouvez également créer une relation de protection des données entre les SVM. Dans ce type de relation, toute ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB vers le RBAC, est répliquée, ainsi que les données au sein des volumes dont est propriétaire le SVM.

À partir de ONTAP 9.10.1, vous pouvez créer des relations de protection des données entre les compartiments

S3 à l'aide de SnapMirror S3. Les compartiments de destination peuvent être sur les systèmes ONTAP locaux ou distants, ou sur les systèmes non ONTAP tels qu'StorageGRID et AWS.

La première fois que vous appelez SnapMirror, il effectue un *transfert de base* du volume source vers le volume de destination. Le transfert de base implique généralement les étapes suivantes :

- Créer une copie Snapshot du volume source.
- Transférez la copie Snapshot et tous les blocs de données qu'elle référence vers le volume de destination.
- Transférez les copies Snapshot restantes et moins récentes sur le volume source vers le volume de destination pour toute utilisation en cas de corruption du miroir « actif ».

Une fois le transfert de base terminé, SnapMirror transfère uniquement les nouvelles copies Snapshot vers le miroir. Les mises à jour sont asynchrones, en fonction du planning que vous configurez. La conservation met en miroir la règle Snapshot sur la source. Vous pouvez activer le volume de destination en cas d'incident au niveau du site primaire et réactiver le volume source une fois le service restauré.

Étant donné que SnapMirror transfère uniquement les copies Snapshot après la création de la copie de base, la réplication est rapide et sans interruption. Comme l'indique le cas de basculement, les contrôleurs du système secondaire doivent être équivalents ou presque équivalents aux contrôleurs du système primaire pour assurer un service efficace des données à partir du stockage en miroir.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

utilisation de SnapMirror pour le transfert de données

Vous pouvez également utiliser SnapMirror pour répliquer les données entre les terminaux de NetApp Data Fabric. Lorsque vous créez la règle SnapMirror, vous avez le choix entre une réplication ponctuelle ou une réplication récurrente.

Sauvegardes SnapMirror dans le cloud sur le stockage objet

SnapMirror est une technologie de sauvegarde et de restauration conçue pour les utilisateurs ONTAP qui souhaitent migrer leurs workflows de protection des données vers

le cloud. Les entreprises qui se détournent de leurs architectures de sauvegarde sur bande existantes peuvent utiliser le stockage objet comme référentiel alternatif pour la conservation et l'archivage des données à long terme. SnapMirror Cloud permet la réplication du stockage ONTAP vers objet dans le cadre d'une stratégie de sauvegarde incrémentielle à l'infini.

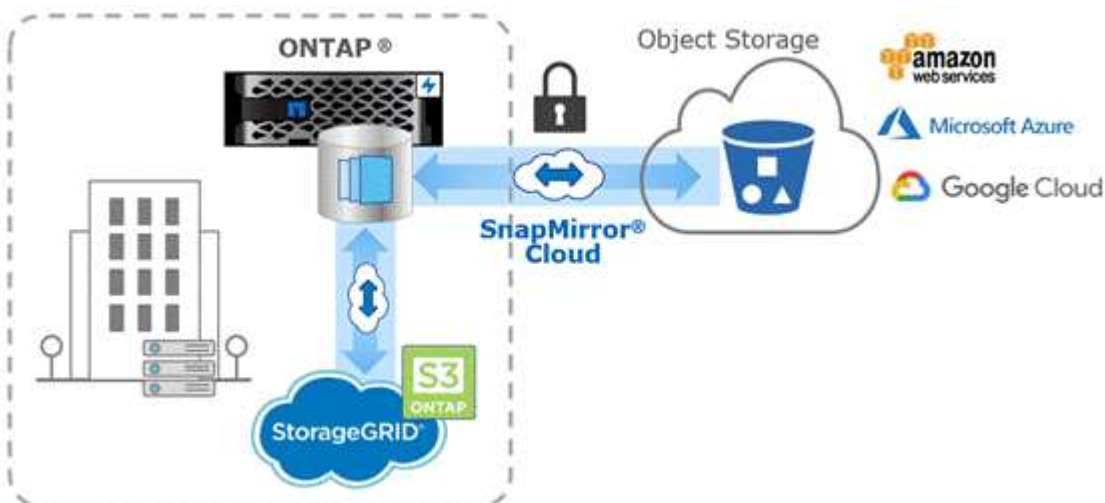
SnapMirror Cloud a été introduit dans ONTAP 9.8 en tant qu'extension de la gamme de technologies de réplication SnapMirror. Même si SnapMirror est fréquemment utilisé pour les sauvegardes ONTAP à ONTAP, SnapMirror Cloud utilise le même moteur de réplication pour transférer les copies Snapshot pour ONTAP vers des sauvegardes de stockage objet conformes S3.

Conçu pour les sauvegardes, SnapMirror Cloud prend en charge à la fois les workflows de conservation et d'archivage à long terme. Tout comme SnapMirror, la sauvegarde SnapMirror Cloud initiale effectue un transfert de base d'un volume. Pour les sauvegardes ultérieures, SnapMirror Cloud génère une copie Snapshot du volume source et transfère la copie Snapshot avec uniquement les blocs de données modifiés vers une cible de stockage objet.

Les relations SnapMirror Cloud peuvent être configurées entre les systèmes ONTAP et certaines cibles de stockage objet sur site et dans le cloud public, notamment Amazon S3, Google Cloud Storage et Microsoft Azure Blob Storage. Des cibles supplémentaires de stockage objet sur site incluent StorageGRID et ONTAP S3.

La réplication SnapMirror Cloud est une fonctionnalité ONTAP sous licence. Elle requiert une application approuvée pour orchestrer les workflows de protection des données. Plusieurs options d'orchestration sont disponibles pour la gestion des sauvegardes SnapMirror Cloud :

- Plusieurs partenaires de sauvegarde tiers qui prennent en charge la réplication SnapMirror Cloud. Les fournisseurs participants sont disponibles sur le ["Blog NetApp"](#).
- Sauvegarde et restauration BlueXP pour une solution NetApp native pour les environnements ONTAP
- API pour développer des logiciels personnalisés pour les workflows de protection des données ou exploiter les outils d'automatisation



Archivage SnapVault

La licence SnapMirror permet la prise en charge des relations SnapVault pour la sauvegarde et des relations SnapMirror pour la reprise sur incident. À partir de ONTAP

9.3, les licences SnapVault sont obsolètes et les licences SnapMirror peuvent être utilisées pour configurer les relations Vault, mirror et mirror-and-vault. La réplication SnapMirror est utilisée pour la réplication ONTAP vers ONTAP des copies Snapshot, et prend en charge à la fois des opérations de sauvegarde et de reprise d'activité.

SnapVault est une technologie d'archivage conçue pour la réplication de copie Snapshot disque à disque à des fins de conformité aux normes et autres pour la gouvernance. Contrairement à une relation SnapMirror, dans laquelle la destination contient généralement uniquement les copies Snapshot actuellement dans le volume source, la destination SnapVault conserve en général les copies Snapshot instantanées créées sur une période bien plus longue.

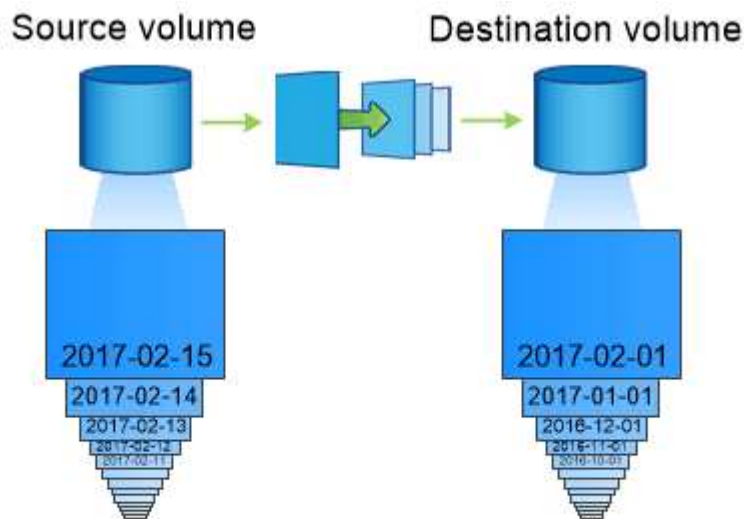
Vous pouvez conserver tous les mois des copies Snapshot de vos données sur une période de 20 ans, par exemple, pour vous conformer aux réglementations gouvernementales relatives à la comptabilité de votre entreprise. Etant donné qu'il n'est pas nécessaire de transmettre des données à partir du stockage Vault, vous pouvez utiliser des disques plus lents et moins coûteux sur le système de destination.

Tout comme SnapMirror, SnapVault effectue un transfert de base dès la première fois que vous l'appellez. Il effectue une copie Snapshot du volume source, puis transfère la copie et les blocs de données qu'il renvoie vers le volume de destination. Contrairement à SnapMirror, SnapVault n'inclut pas d'anciennes copies Snapshot dans la configuration de base.

Les mises à jour sont asynchrones, en fonction du planning que vous configurez. Les règles que vous définissez dans la règle pour la relation identifient les nouvelles copies Snapshot à inclure dans les mises à jour et le nombre de copies à conserver. Les libellés définis dans la politique (« mensuel », par exemple) doivent correspondre à un ou plusieurs libellés définis dans la politique Snapshot de la source. Dans le cas contraire, la réplication échoue.



SnapMirror et SnapVault partagent la même infrastructure de commandes. Vous spécifiez la méthode à utiliser lors de la création d'une stratégie. Les deux méthodes exigent des clusters de peering et des SVM.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Sauvegarde dans le cloud et prise en charge des sauvegardes classiques

Outre les relations de protection des données SnapMirror et SnapVault, qui étaient disque à disque uniquement pour ONTAP 9.7 et les versions antérieures, plusieurs solutions de sauvegarde offrent une alternative moins onéreuse pour la conservation à long terme des données.

De nombreuses applications tierces de protection des données proposent des sauvegardes classiques pour les données gérées par ONTAP. Veeam, Veritas et CommVault entre autres proposent une sauvegarde intégrée pour les systèmes ONTAP.

Depuis ONTAP 9.8, SnapMirror Cloud permet la réplication asynchrone des copies Snapshot à partir d'instances ONTAP vers les terminaux de stockage objet. La réplication SnapMirror Cloud requiert une application sous licence pour l'orchestration et la gestion des workflows de protection des données. Les relations SnapMirror avec le cloud sont prises en charge par les systèmes ONTAP afin de sélectionner des cibles de stockage objet sur site et dans le cloud public, notamment AWS S3, Google Cloud Storage Platform ou Microsoft Azure Blob Storage, qui améliorent l'efficacité avec les logiciels de sauvegarde des fournisseurs. Contactez votre conseiller NetApp pour obtenir une liste des fournisseurs d'applications certifiées et de stockage objet pris en charge.

Si la protection des données native du cloud vous intéresse, BlueXP peut être utilisé pour configurer les relations SnapMirror ou SnapVault entre les volumes sur site et les instances Cloud Volumes ONTAP dans le cloud public.

BlueXP fournit également des sauvegardes d'instances Cloud Volumes ONTAP à l'aide d'un modèle SaaS. Les utilisateurs peuvent sauvegarder leurs instances Cloud Volumes ONTAP dans le stockage objet de cloud public compatible S3 et S3 à l'aide de Cloud Backup disponible sur NetApp Cloud Central.

["Ressources de documentation Cloud Volumes ONTAP et BlueXP"](#)

["NetApp Cloud Central"](#)

Disponibilité sans interruption avec MetroCluster

Les configurations MetroCluster protègent les données grâce à la mise en œuvre de deux clusters en miroir séparés physiquement. Chaque cluster réplique de manière synchrone les données et la configuration SVM de l'autre. En cas d'incident sur un site, un administrateur peut activer la SVM en miroir et commencer à transférer les données depuis le site survivant.

- Les *configurations MetroCluster* reliées à la structure prennent en charge les clusters à l'échelle de la zone métropolitaine.
- *Stretch MetroCluster* configurations prennent en charge les clusters à l'échelle du campus.

Les grappes doivent être pételées dans les deux cas.

MetroCluster utilise la fonctionnalité ONTAP appelée *SyncMirror* pour mettre en miroir de manière synchrone les données d'agrégats pour chaque cluster dans des copies, ou *plex*, dans le stockage de l'autre cluster. En cas de basculement, le plex distant sur le cluster survivant est mis en ligne et le SVM secondaire commence à transmettre les données.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

utilisation de SyncMirror dans des implémentations non MetroCluster

Vous pouvez, par ailleurs, utiliser SyncMirror dans une implémentation non MetroCluster pour vous protéger contre la perte de données si le nombre de disques défaillants est supérieur à la protection du type RAID ou en cas de perte de connectivité avec les disques du groupe RAID. La fonctionnalité est disponible uniquement pour les paires haute disponibilité.

Les données agrégées sont mises en miroir dans des plexes stockés sur différents tiroirs disques. Si l'un des tiroirs n'est plus disponible, le plex non affecté continue à transmettre des données pendant que vous corrigez la défaillance.

N'oubliez pas qu'un agrégat en miroir avec SyncMirror nécessite deux fois plus de stockage qu'un agrégat non mis en miroir. Chaque plex requiert autant de disques que le plex IT miroirs. Vous auriez besoin de 2,880 Go d'espace disque, par exemple pour mettre en miroir un agrégat de 1,440 Go, 1,440 Go par plex.

Avec SyncMirror, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir pour une disponibilité et des performances de stockage optimales. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces bonnes pratiques peut avoir un impact négatif sur les performances de resynchronisation SyncMirror, qui a un impact indirect sur les workflows opérationnels, tels que la mise à niveau sans interruption pour les déploiements cloud non partagés et la reprise pour les déploiements MetroCluster.



SyncMirror est également disponible pour les implémentations de virtualisation FlexArray.

Efficacité du stockage

Présentation de l'efficacité du stockage ONTAP

L'efficacité du stockage mesure la manière dont un système de stockage utilise l'espace disponible en optimisant les ressources de stockage, en minimisant le gaspillage d'espace et en réduisant l'encombrement physique des données écrites. Un stockage plus efficace vous permet de stocker un maximum de données dans un minimum d'espace et à moindre coût. Par exemple, l'utilisation de technologies d'efficacité du stockage qui détectent et éliminent les blocs de données dupliqués et les blocs de données remplis de zéros réduit la quantité globale de stockage physique nécessaire et le coût global.

ONTAP propose une large gamme de technologies d'efficacité du stockage qui réduisent la quantité de matériel physique ou de stockage cloud consommée par vos données et qui améliorent considérablement les performances du système. Ces technologies incluent une lecture plus rapide des données, des copies plus rapides des jeux de données et un provisionnement plus rapide des machines virtuelles.

Les technologies ONTAP d'efficacité du stockage incluent :

- **Provisionnement fin**

Provisionnement fin Vous permet d'allouer du stockage dans un volume ou une LUN en fonction des besoins au lieu de le réserver à l'avance. Cela réduit la quantité de stockage physique nécessaire en vous permettant de surallouer vos volumes ou LUN en fonction de leur utilisation potentielle, sans réserver un

espace qui n'est pas utilisé actuellement.

- **Déduplication**

Déduplication réduit la quantité de stockage physique nécessaire pour un volume de trois manières distinctes.

- **Déduplication de blocs zéro**

La déduplication de blocs « zéro » détecte et élimine les blocs de données remplis de zéros, et met uniquement à jour les métadonnées. 100 % de l'espace généralement utilisé par les blocs « zéro » est ensuite économisé. La déduplication de blocs « zéro » est activée par défaut sur tous les volumes dédupliqués.

- **Déduplication à la volée**

La déduplication à la volée détecte les blocs de données dupliqués et les remplace par des références à un bloc partagé unique avant l'écriture des données sur le disque. La déduplication à la volée accélère le provisionnement des machines virtuelles de 20 à 30 %. Selon votre version d'ONTAP et votre plateforme, la déduplication à la volée est disponible au niveau du volume ou de l'agrégat. Il est activé par défaut sur les systèmes AFF et ASA. Vous devez activer manuellement la déduplication à la volée sur les systèmes FAS.

- **Déduplication en arrière-plan**

La déduplication en arrière-plan détecte également les blocs de données dupliqués et les remplace par des références à un bloc partagé unique. Elle améliore également l'efficacité du stockage après l'écriture des données sur le disque. Vous pouvez configurer la déduplication en arrière-plan pour qu'elle s'exécute lorsque certains critères sont remplis sur votre système de stockage. Par exemple, vous pouvez activer la déduplication en arrière-plan lorsque votre volume atteint 10 % d'utilisation. Vous pouvez également déclencher manuellement la déduplication en arrière-plan ou la configurer pour qu'elle s'exécute selon un planning spécifique. Il est activé par défaut sur les systèmes AFF et ASA. Vous devez activer manuellement la déduplication en arrière-plan sur les systèmes FAS.

La déduplication est prise en charge au sein des volumes et entre les volumes d'un agrégat. Les lectures de données dédupliquées n'entraînent en général aucun frais de performances.

- **Compression**

Compression réduit la quantité de stockage physique nécessaire pour un volume en combinant les blocs de données dans des groupes de compression, chacun étant stocké sous forme de bloc unique. Lorsqu'une demande de lecture ou de remplacement est reçue, seul un petit groupe de blocs est lu, et non le fichier entier. Ce processus optimise les performances de lecture et d'écriture et permet une plus grande évolutivité de la taille des fichiers compressés.

Elle peut être exécutée à la volée ou en post-traitement. La compression à la volée permet des gains d'espace immédiats en compressant les données dans la mémoire avant d'être écrites sur le disque. La compression post-traitement écrit d'abord les blocs sur le disque comme non compressés, puis compresse les données à un moment prédéfini. Vous devez activer manuellement la compression.

- **Compaction**

La compaction réduit la quantité de stockage physique requise pour un volume en prenant des segments de données stockés dans des blocs de 4 Ko mais dont la taille est inférieure à 4 Ko et en les combinant dans un seul bloc. La compaction a lieu lorsque les données sont encore dans la mémoire. Ainsi, l'espace inutile n'est jamais consommé sur les disques. Il est activé par défaut sur les systèmes AFF et ASA. Vous

devez activer manuellement la compaction sur les systèmes FAS.

- **Volumes FlexClone, fichiers et LUN**

Technologie FlexClone Exploite les métadonnées Snapshot pour créer des copies instantanées inscriptibles d'un volume, d'un fichier ou d'une LUN. Les copies partagent les blocs de données avec leurs parents. Elles ne consomment pas d'espace de stockage, à l'exception des éléments requis pour les métadonnées jusqu'à ce que les modifications soient écrites sur une copie ou sur son parent. Lorsqu'une modification est écrite, seul le delta est stocké.

Là où la création de copies de datasets classiques peut prendre quelques minutes, voire plusieurs heures, la technologie FlexClone vous permet de copier même les jeux de données les plus volumineux de manière quasi instantanée.

- **Efficacité de stockage sensible à la température**

ONTAP fournit "**efficacité du stockage sensible à la température**" les avantages sont multiples : il s'agit d'évaluer la fréquence d'accès aux données de votre volume et de mapper cette fréquence au niveau de compression appliqué à ces données. Pour les données inactives peu utilisées, les blocs de données plus volumineux sont compressés et pour les données actives, qui sont fréquemment utilisées et remplacées plus souvent, les blocs de données plus petits sont compressés, ce qui améliore l'efficacité du processus.

L'efficacité du stockage sensible à la température, introduite dans ONTAP 9.8, est automatiquement activée sur les volumes AFF nouvellement créés à provisionnement fin.

Et si vous le souhaitez, vous pouvez tirer parti de ces technologies dans vos opérations quotidiennes en toute simplicité. Supposons par exemple que vous devez fournir à 5,000 utilisateurs du stockage pour les répertoires locaux, et que vous estimez que l'espace maximal requis par un utilisateur est de 1 Go. Vous pouvez réserver un agrégat de 5 To à l'avance pour répondre au besoin total de stockage potentiel. Cependant, vous savez également que les besoins en capacité des répertoires locaux varient considérablement dans votre organisation. Au lieu de réserver 5 To d'espace total à votre entreprise, vous pouvez créer un agrégat de 2 To. Vous pouvez ensuite utiliser le provisionnement fin pour attribuer nominalelement 1 Go de stockage à chaque utilisateur, mais allouer le stockage uniquement en fonction des besoins. Vous pouvez activement surveiller l'agrégat dans le temps et augmenter sa taille physique réelle si nécessaire.

Dans un autre exemple, supposons que vous utilisiez une infrastructure de postes de travail virtuels (VDI) avec une grande quantité de données dupliquées au sein de vos postes de travail virtuels. La déduplication réduit l'utilisation du stockage en éliminant automatiquement les blocs d'informations dupliqués dans l'infrastructure VDI, puis en les remplaçant par un pointeur vers le bloc d'origine. D'autres technologies d'efficacité du stockage ONTAP, telles que la compression, peuvent également s'exécuter en arrière-plan sans intervention de votre part.

La technologie de partitionnement de disque ONTAP offre également une meilleure efficacité du stockage. La technologie RAID DP protège contre les doubles défaillances de disques sans sacrifier les performances ni augmenter la surcharge liée à la mise en miroir des disques. Le partitionnement SSD avancé avec ONTAP 9 augmente la capacité exploitable de près de 20 %.

NetApp fournit les mêmes fonctionnalités d'efficacité du stockage que celles disponibles avec ONTAP sur site dans le cloud. La migration des données depuis un environnement ONTAP sur site vers le cloud préserve l'efficacité du stockage. Supposons que vous disposiez d'une base de données SQL contenant des données stratégiques que vous souhaitez déplacer d'un système sur site vers le cloud. Vous pouvez utiliser la réplication des données dans BlueXP pour migrer vos données et, dans le cadre du processus de migration, vous pouvez activer votre dernière règle sur site pour les copies Snapshot dans le cloud.

Provisionnement fin

ONTAP propose un large éventail de technologies d'efficacité du stockage, en plus des copies Snapshot. Les technologies clés sont le provisionnement fin, la déduplication, la compression, ainsi que les volumes FlexClone, les fichiers Et des LUN. À l'instar des copies Snapshot, elles reposent sur le WAFL (Write Anywhere File Layout) d'ONTAP.

Un *volume* provisionné_ ou une LUN est un volume pour lequel le stockage n'est pas réservé à l'avance. Au contraire, le stockage est alloué de manière dynamique, selon les besoins. L'espace libre est relâché dans le système de stockage lorsque les données du volume ou de la LUN sont supprimées.

Imaginez que votre entreprise doit fournir à 5,000 utilisateurs du stockage pour les répertoires locaux. Vous estimez que les principaux répertoires locaux consommeront 1 Go d'espace.

Dans ce cas, vous pouvez acheter 5 To de stockage physique. Pour chaque volume qui stocke un home Directory, vous pouvez réserver suffisamment d'espace pour répondre aux besoins des plus grands consommateurs.

En pratique, cependant, vous savez aussi que les besoins en capacité des répertoires d'accueil varient considérablement d'un bout à l'autre de votre communauté. Pour chaque grand utilisateur du stockage, dix ne consomment que peu ou pas d'espace.

Le provisionnement fin vous permet de répondre aux besoins des grands consommateurs de stockage sans acheter de stockage que vous n'utiliserez probablement pas. L'espace de stockage n'étant pas alloué tant qu'il n'est pas consommé, vous pouvez « surallouer » un agrégat de 2 To en attribuant théoriquement une taille de 1 Go à chacun des 5,000 volumes que l'agrégat contient.

Tant que vous avez raison de ratios de lumière 10:1 pour les utilisateurs intensifs et tant que vous jouez un rôle actif dans la surveillance de l'espace libre de l'agrégat, vous pouvez compter sur le fait que les écritures de volume ne échouent pas en raison du manque d'espace.

Déduplication

Deduplication réduit le volume de stockage physique requis pour un volume (ou pour tous les volumes d'un agrégat AFF) en abandonnant les blocs dupliqués et en les remplaçant par des références à un seul bloc partagé. Les lectures de données dédupliquées n'entraînent en général aucun frais de performances. Les écritures entraînent un frais négligeable sauf sur les nœuds surchargés.

Au fur et à mesure que les données sont écrites pendant l'utilisation normale, WAFL crée un catalogue de signatures de blocs . après le démarrage de la déduplication, ONTAP compare les signatures dans le catalogue pour identifier les blocs dupliqués. Si une correspondance existe, une comparaison octet par octet est effectuée pour vérifier que les blocs candidats n'ont pas changé depuis la création du catalogue. Uniquement si tous les octets correspondent au bloc dupliqué supprimé et si son espace disque est récupéré.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

Compression

Compression réduit la quantité de stockage physique requise pour un volume en combinant des blocs de données dans *groupes de compression* dont chacun est stocké comme un seul bloc. Les lectures de données compressées sont plus rapides que dans les méthodes de compression traditionnelles, car ONTAP décompresse uniquement les groupes de compression contenant les données requises, et non un fichier ou une LUN entier.

Vous pouvez effectuer la compression à la volée ou post-traitement, séparément ou conjointement :

- *Inline compression* compresse les données en mémoire avant de les écrire sur le disque, ce qui réduit de manière significative la quantité d'opérations d'écriture E/S sur un volume, mais diminue potentiellement les performances d'écriture. Le cas échéant, les opérations exigeant des performances élevées sont reportées jusqu'à la prochaine opération de compression post-traitement.
- *Post-compression* compresse les données après leur écriture sur le disque, selon la même planification que la déduplication.

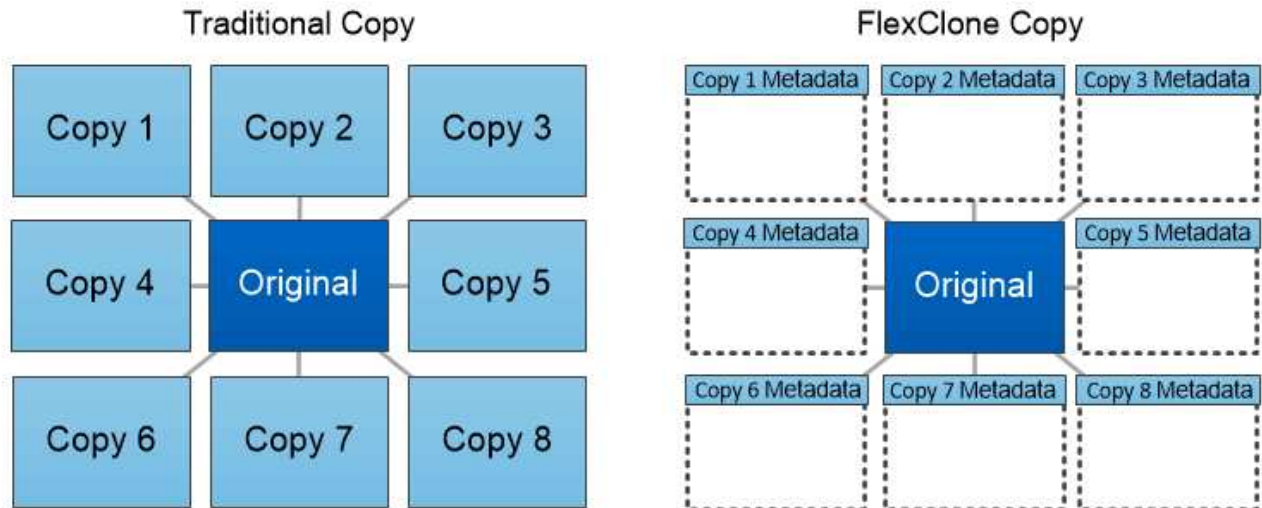
compaction des données à la volée les petits fichiers ou E/S rembourrés avec des zéros sont stockés dans un bloc de 4 Ko, qu'ils aient ou non besoin de 4 Ko de stockage physique. *La compaction des données à la volée* associe des blocs de données qui consomment normalement plusieurs blocs de 4 Ko dans un seul bloc de 4 Ko sur disque. La compaction a lieu tandis que les données sont encore dans la mémoire, il est donc recommandé d'accélérer les contrôleurs.

Volumes FlexClone, fichiers et LUN

FlexClone fait référence aux métadonnées Snapshot pour créer des copies inscriptibles instantanées d'un volume. Les copies partagent les blocs de données avec leurs parents. Aucun stockage n'est nécessaire, sauf pour les métadonnées, jusqu'à ce que les modifications soient écrites sur la copie. Les fichiers FlexClone et les LUN FlexClone utilisent une technologie identique, à la différence qu'une copie Snapshot de sauvegarde n'est pas requise.

Là où les copies classiques peuvent prendre des minutes, voire des heures, pour créer des copies, FlexClone vous permet de copier même les jeux de données les plus volumineux quasi instantanément. Cela est idéal si vous avez besoin de plusieurs copies de jeux de données identiques (par exemple, pour le déploiement de postes de travail virtuels) ou de copies temporaires d'un jeu de données (test d'une application par rapport à un jeu de données de production).

Vous pouvez cloner un volume FlexClone existant, cloner un volume contenant des clones de LUN ou cloner des données de miroir et d'archivage sécurisé. Vous pouvez *split* volume FlexClone de son parent, dans le cas où la copie lui serait allouée son propre stockage.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

Mesures de la capacité dans System Manager

La capacité du système peut être mesurée soit en tant qu'espace physique, soit en tant qu'espace logique. Depuis ONTAP 9.7, System Manager mesure la capacité physique et logique.

Les différences entre les deux mesures sont expliquées dans les descriptions suivantes :

- **Capacité physique** : l'espace physique fait référence aux blocs physiques de stockage utilisés dans le volume ou le niveau local. La valeur de la capacité physique utilisée est généralement inférieure à la valeur de la capacité logique utilisée grâce à la réduction des données provenant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- **Capacité logique** : l'espace logique fait référence à l'espace utilisable (les blocs logiques) dans un volume ou un niveau local. L'espace logique désigne la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats obtenus grâce à la déduplication ou à la compression. La valeur de l'espace logique utilisé est issue de la quantité d'espace physique utilisé, plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure est souvent supérieure à la capacité physique utilisée, car elle inclut des copies Snapshot, des clones et d'autres composants, et ne reflète pas la compression des données et autres réductions de l'espace physique. La capacité logique totale peut donc être supérieure à l'espace provisionné.



Dans System Manager, les représentations de capacité ne prennent pas en compte les capacités du niveau de stockage racine (agrégat).

Mesures de la capacité utilisée

Les mesures de la capacité utilisée s'affichent différemment en fonction de la version de System Manager que vous utilisez, comme expliqué dans le tableau ci-dessous :

Version de System Manager	Terme utilisé pour la capacité	Type de capacité visé
9.9.1 et versions ultérieures	Utilisation logique	Espace logique utilisé si les paramètres d'efficacité du stockage ont été activés)
9.7 et 9.8	Utilisé	Espace logique utilisé (si les paramètres d'efficacité du stockage ont été activés)
9.5 et 9.6 (Vue classique)	Utilisé	Espace physique utilisé

Termes de mesure de la capacité

Les termes suivants sont utilisés pour décrire la capacité :

- **Capacité allouée** : quantité d'espace allouée aux volumes d'une machine virtuelle de stockage.
- **Disponible** : quantité d'espace physique disponible pour stocker des données ou provisionner des volumes dans une machine virtuelle de stockage ou sur un niveau local.
- **Capacité sur les volumes** : somme du stockage utilisé et du stockage disponible de tous les volumes sur une machine virtuelle de stockage.
- **Données client** : quantité d'espace utilisée par les données client (physique ou logique).
 - Depuis ONTAP 9.13.1, la capacité utilisée par les données client est appelée **logique utilisée** et la capacité utilisée par les copies Snapshot est affichée séparément.
 - Dans ONTAP 9.12.1 et versions antérieures, la capacité utilisée par les données client ajoutées à la capacité utilisée par les copies Snapshot est appelée **logique utilisée**.
- **Validé** : le montant de la capacité engagée pour un niveau local.
- **Réduction des données** :
 - À partir de ONTAP 9.13.1, les taux de réduction des données sont affichés comme suit :
 - La valeur de réduction des données affichée sur le panneau **capacité** correspond au rapport entre l'espace logique utilisé et l'espace physique utilisé, sans tenir compte des réductions significatives obtenues lors de l'utilisation de fonctionnalités d'efficacité du stockage, telles que les copies Snapshot.
 - Lorsque vous affichez le panneau de détails, vous voyez à la fois le ratio affiché sur le panneau de vue d'ensemble et le ratio global de tout l'espace utilisé logique par rapport à l'espace physique utilisé. Appelé **avec les copies Snapshot**, cette valeur inclut les avantages découlant de l'utilisation des copies Snapshot et d'autres fonctionnalités d'efficacité du stockage.

- Dans la ONTAP 9.12.1 et les versions antérieures, les taux de réduction des données sont affichés comme suit :
 - La valeur de réduction des données affichée sur le panneau **capacité** correspond au rapport global de tout l'espace logique utilisé par rapport à l'espace physique utilisé, et elle inclut les avantages découlant de l'utilisation des copies Snapshot et d'autres fonctionnalités d'efficacité du stockage.
 - Lorsque vous affichez le panneau de détails, vous voyez à la fois le ratio **global** qui était affiché sur le panneau de vue d'ensemble et le rapport de l'espace logique utilisé uniquement par les données client par rapport à l'espace physique utilisé uniquement par les données client, appelé **sans copies Snapshot et clones**.

- **Logique utilisée :**

- Depuis ONTAP 9.13.1, la capacité utilisée par les données client est appelée **logique utilisée** et la capacité utilisée par les copies Snapshot est affichée séparément.
- Dans ONTAP 9.12.1 et versions antérieures, la capacité utilisée par les données client ajoutées à la capacité utilisée par les copies Snapshot est appelée **logique utilisée**.

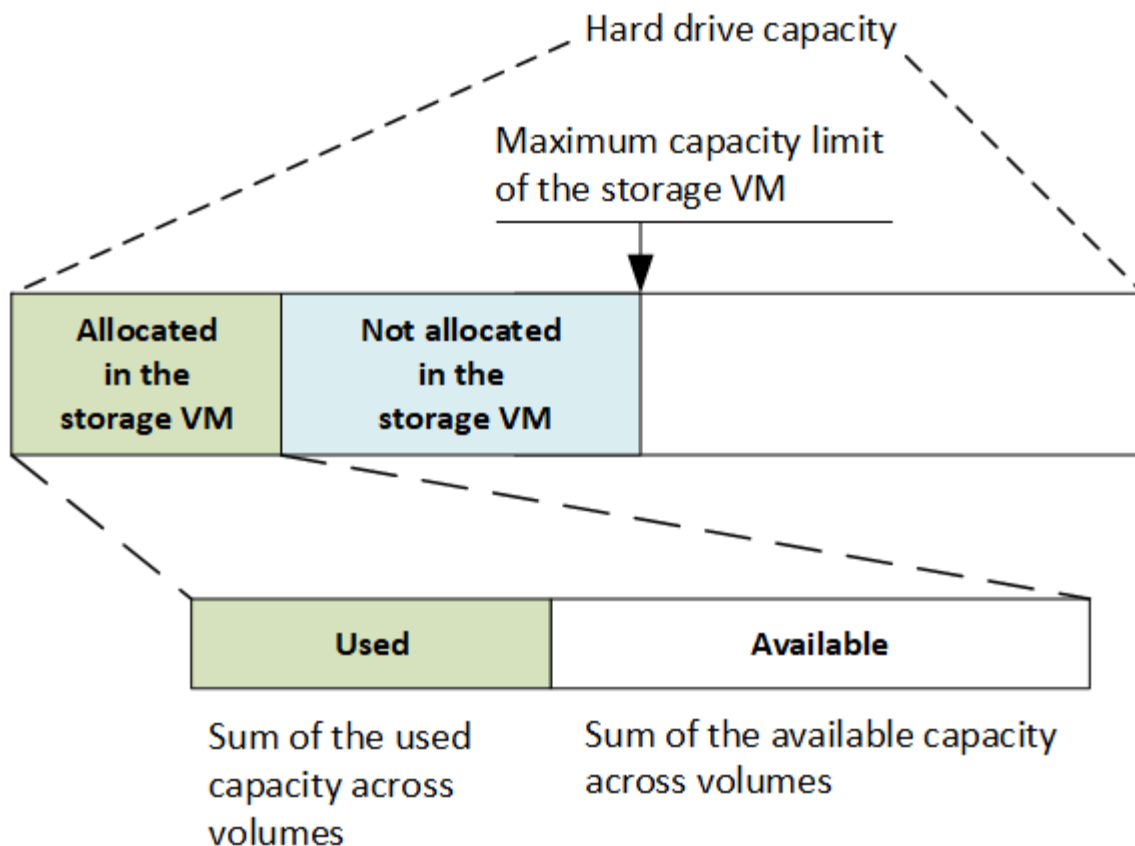
- **Logical Used %** : pourcentage de la capacité logique utilisée actuelle par rapport à la taille provisionnée, à l'exclusion des réserves snapshot. Cette valeur peut être supérieure à 100 %, grâce aux économies en termes d'efficacité réalisées dans le volume.
- **Capacité maximale** : quantité maximale d'espace allouée aux volumes sur une machine virtuelle de stockage.
- **Physical Used**: La capacité utilisée dans les blocs physiques d'un volume ou d'un niveau local.
- **Physical Used %** : pourcentage de capacité utilisée dans les blocs physiques d'un volume par rapport à la taille provisionnée.
- **Capacité provisionnée** : un système de fichiers (volume) qui a été alloué à partir d'un système Cloud Volumes ONTAP et est prêt à stocker les données des utilisateurs ou des applications.
- **Réservé** : espace réservé pour les volumes déjà provisionnés dans un niveau local.
- **Utilisé**: La quantité d'espace qui contient des données.
- **Utilisé et réservé** : somme de l'espace physique utilisé et réservé.

Capacité d'une VM de stockage

La capacité maximale d'une machine virtuelle de stockage est déterminée par l'espace total alloué aux volumes plus l'espace restant non alloué.

- L'espace alloué aux volumes correspond à la somme de la capacité utilisée et de la capacité disponible des volumes FlexVol, des volumes FlexGroup et des volumes FlexCache.
- La capacité des volumes est incluse dans les sommes, même lorsqu'elles sont restreintes, hors ligne ou dans la file d'attente de restauration après suppression.
- Si les volumes sont configurés avec l'extension automatique, la valeur de taille automatique maximale du volume est utilisée dans les sommes. Sans croissance automatique, la capacité réelle du volume est utilisée dans les sommes.

Le tableau suivant explique comment la mesure de la capacité sur l'ensemble des volumes est liée à la limite de capacité maximale.



À partir de ONTAP 9.13.1, les administrateurs du cluster peuvent "[Limiter la capacité maximale pour une VM de stockage](#)". Toutefois, il est impossible de définir des limites de stockage pour une VM de stockage qui contient des volumes destinés à la protection des données, dans une relation SnapMirror ou dans une configuration MetroCluster. De même, les quotas ne peuvent pas être configurés pour dépasser la capacité maximale d'une machine virtuelle de stockage.

Une fois la limite de capacité maximale définie, elle ne peut pas être modifiée pour obtenir une taille inférieure à la capacité actuellement allouée.

Lorsqu'une machine virtuelle de stockage atteint sa capacité maximale, certaines opérations ne peuvent pas être effectuées. System Manager fournit des suggestions pour les étapes suivantes de "[Aperçus](#)".

Unités de mesure de la capacité

System Manager calcule la capacité de stockage en fonction des unités binaires de 1024 (2^{10}) octets.

- À partir de la version ONTAP 9.10.1, les unités de capacité de stockage sont affichées dans System Manager sous la forme KiB, MiB, GiB, TiB et PiB.
- Dans ONTAP 9.10.0 et les versions antérieures, ces unités sont affichées dans System Manager sous la forme de Ko, Mo, Go, To et po.



Les unités utilisées dans System Manager pour le débit continuent à être les Ko/s, Mo/s, Go/s, To/s et po/s pour toutes les versions des systèmes ONTAP.

Unité de capacité affichée dans System Manager pour ONTAP 9.10.0 et versions antérieures	Unité de capacité affichée dans System Manager pour ONTAP 9.10.1 et versions ultérieures	Calcul	Valeur en octets
KO	Kio	1024	1024 octets
MO	Mio	1024 * 1024	1,048,576 octets
GO	Gio	1024 * 1024 * 1024	1,073,741,824 octets
TO	Tio	1024 * 1024 * 1024 * 1024	1,099,511,627,776 octets
PO	Pio	1024 * 1024 * 1024 * 1024 * 1024	1,125,899,906,842,624 octets

Informations associées

["Contrôle de la capacité dans System Manager"](#)

["Création de rapports sur l'espace logique et application des volumes"](#)

Présentation de l'efficacité du stockage sensible à la température

Pour améliorer l'efficacité du stockage selon la température, ONTAP évalue la fréquence d'accès aux données de votre volume et mappe cette fréquence sur le degré de compression appliqué à ces données. Pour les données inactives peu utilisées, les blocs de données plus volumineux sont compressés et pour les données actives, qui sont fréquemment utilisées et remplacées plus souvent, les blocs de données plus petits sont compressés, ce qui améliore l'efficacité du processus.

L'efficacité du stockage sensible à la température, introduite dans ONTAP 9.8, est automatiquement activée sur les volumes AFF nouvellement créés à provisionnement fin. Vous pouvez activer l'efficacité du stockage sensible à la température sur les volumes AFF existants et sur les volumes non-AFF DP à provisionnement fin.

Introduction des modes « par défaut » et « efficace »

À partir de ONTAP 9.10.1, deux modes d'efficacité du stockage au niveau des volumes sont introduits uniquement pour les systèmes AFF, *default* et *Efficient*. Les deux modes permettent de choisir entre la compression de fichiers (par défaut), qui est le mode par défaut lors de la création de nouveaux volumes AFF, ou l'efficacité du stockage sensible à la température (efficace), ce qui permet d'obtenir une efficacité du stockage sensible à la température. Avec ONTAP 9.10.1, ["l'efficacité du stockage sensible à la température doit être définie de manière explicite"](#) pour activer la compression auto-adaptative. Cependant, d'autres fonctionnalités d'efficacité du stockage telles que la compaction des données, la déduplication automatique, la déduplication à la volée, la déduplication à la volée entre volumes et la déduplication en arrière-plan entre volumes sont activées par défaut sur les plateformes AFF pour les modes par défaut et efficaces.

Les deux modes d'efficacité du stockage (par défaut et efficace) sont pris en charge sur les agrégats compatibles avec FabricPool et avec tous les types de règles de Tiering.

Efficacité du stockage sensible à la température activée sur les plateformes C-Series

L'efficacité du stockage sensible à la température est activée par défaut sur les plates-formes AFF série C et lors de la migration de volumes d'une plate-forme non TSSE vers une plate-forme C-Series compatible TSSE à l'aide de Volume Move ou de SnapMirror avec les versions suivantes installées sur la destination :

- ONTAP 9.12.1P4 et versions ultérieures
- ONTAP 9.13.1 et versions ultérieures

Pour plus d'informations, voir ["Efficacité du stockage avec déplacement de volumes et opérations SnapMirror"](#).

Pour les volumes existants, l'efficacité du stockage sensible à la température n'est pas activée automatiquement, mais elle le peut ["modifier le mode d'efficacité du stockage"](#) manuellement pour passer en mode efficace.



Une fois que vous avez défini le mode d'efficacité du stockage sur efficace, vous ne pouvez plus le redéfinir.

Amélioration de l'efficacité du stockage grâce à la compression séquentielle des blocs physiques contigus

Depuis la version ONTAP 9.13.1, l'efficacité du stockage sensible à la température ajoute la compaction séquentielle des blocs physiques contigus afin d'améliorer encore l'efficacité du stockage. Sur les volumes dont l'efficacité du stockage sensible à la température est activée automatiquement, la compression séquentielle est activée lorsque vous mettez à niveau des systèmes vers ONTAP 9.13.1. Une fois l'emballage séquentiel activé, vous devez le faire ["reconditionnement manuel des données existantes"](#).

Mise à niveau

Lors de la mise à niveau vers ONTAP 9.10.1 et versions ultérieures, un mode d'efficacité du stockage est attribué aux volumes existants, basé sur le type de compression actuellement activé sur les volumes. Au cours d'une mise à niveau, le mode par défaut est attribué aux volumes dont la compression est activée et le mode efficace est activé pour les volumes dont l'efficacité de stockage est sensible à la température. Si la compression n'est pas activée, le mode d'efficacité du stockage reste vide.

Sécurité

Authentification et autorisation du client

ONTAP utilise des méthodes standard pour sécuriser l'accès client et administrateur au stockage et se protéger contre les virus. Des technologies avancées sont disponibles pour le chiffrement des données au repos et WORM.

ONTAP authentifie un ordinateur client et un utilisateur en vérifiant son identité avec une source de confiance. ONTAP autorise un utilisateur à accéder à un fichier ou à un répertoire en comparant les informations d'identification de l'utilisateur aux autorisations configurées sur le fichier ou le répertoire.

Authentification

Vous pouvez créer des comptes utilisateur locaux ou distants :

- Un compte local est un compte dans lequel les informations de compte résident sur le système de stockage.
- Un compte distant est un compte dans lequel les informations de compte sont stockées sur un contrôleur

de domaine Active Directory, un serveur LDAP ou un serveur NIS.

ONTAP utilise des services de noms locaux ou externes pour rechercher les informations de nom d'hôte, d'utilisateur, de groupe, de groupe réseau et de mappage de noms. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux
- DNS
- Domaines NIS externes
- Domaines LDAP externes

Un *name service switch table* spécifie les sources à rechercher des informations sur le réseau et l'ordre dans lequel les rechercher (fournissant la fonctionnalité équivalente du fichier `/etc/nsswitch.conf` sur les systèmes UNIX). Lorsqu'un client NAS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations requises.

prise en charge de Kerberos Kerberos est un protocole d'authentification réseau qui fournit "l'authentification" en cryptant les mots de passe utilisateur dans les implémentations client-serveur. ONTAP prend en charge l'authentification Kerberos 5 avec contrôle d'intégrité (krb5i) et l'authentification Kerberos 5 avec vérification de la confidentialité (krb5p).

Autorisation

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM. L'accès est déterminé par les autorisations effectives après évaluation des niveaux de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

La sécurité des exportations et des partages s'applique à l'accès client à une exportation NFS ou à un partage SMB donné. Les utilisateurs disposant de privilèges d'administration peuvent gérer la sécurité au niveau de l'exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

La sécurité Access Guard du niveau de stockage s'applique aux accès des clients SMB et NFS pour les volumes SVM. Seules les autorisations d'accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d'accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l'utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l'objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d'un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

Authentification avec SAML

ONTAP prend en charge le langage SAML (Security assertion Markup Language) pour l'authentification des utilisateurs distants. Plusieurs fournisseurs d'identité (PDI) populaires sont pris en charge. Pour plus d'informations sur les PDI pris en charge et pour savoir comment activer l'authentification SAML, reportez-vous

à la section ["Configurez l'authentification SAML"](#).

OAuth 2.0 avec clients API REST ONTAP

La prise en charge de l'infrastructure d'autorisation ouverte (OAuth 2.0) est disponible à partir de ONTAP 9.14. Vous ne pouvez utiliser OAuth 2.0 que pour prendre des décisions d'autorisation et de contrôle d'accès lorsque le client utilise l'API REST pour accéder à ONTAP. Toutefois, vous pouvez configurer et activer cette fonctionnalité avec n'importe quelle interface d'administration ONTAP, y compris l'interface de ligne de commandes, System Manager et l'API REST.

Les fonctionnalités standard d'OAuth 2.0 sont prises en charge avec plusieurs serveurs d'autorisation courants. Vous pouvez améliorer davantage la sécurité ONTAP en utilisant des jetons d'accès limités par l'expéditeur basés sur le protocole commun. De plus, de nombreuses options d'autorisation sont disponibles, notamment des étendues autonomes, ainsi que l'intégration avec les rôles REST ONTAP et les définitions d'utilisateur local. Voir ["Présentation de la mise en œuvre de ONTAP OAuth 2.0"](#) pour en savoir plus.

Authentification de l'administrateur et RBAC

Les administrateurs utilisent des comptes de connexion locaux ou distants pour s'authentifier auprès du cluster et du SVM. Le contrôle d'accès basé sur des rôles (RBAC) détermine les commandes à laquelle un administrateur a accès.

Authentification

Vous pouvez créer des comptes d'administrateur du cluster et des SVM locaux ou distants :

- Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage.
- Un compte distant est un compte dans lequel les informations de compte sont stockées sur un contrôleur de domaine Active Directory, un serveur LDAP ou un serveur NIS.

À l'exception du DNS, ONTAP utilise les mêmes services de noms pour authentifier les comptes d'administrateur qu'il utilise pour authentifier les clients.

RBAC

Le *role* attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Analyse antivirus

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur le système de stockage afin de protéger vos données contre les virus ou tout autre code malveillant. L'analyse antivirus ONTAP, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Les systèmes de stockage délèguent des opérations d'analyse à des serveurs externes hébergeant le logiciel antivirus de fournisseurs tiers. Le *ONTAP antivirus Connector*, fourni par NetApp et installé sur le serveur externe, gère les communications entre le système de stockage et le logiciel antivirus.

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. L'opération de fichier est suspendue jusqu'à ce que le serveur externe indique l'état de numérisation du fichier. Si le fichier a déjà été numérisé, ONTAP autorise l'opération de fichier. Dans le cas contraire, il demande un scan à partir du serveur.

L'analyse lors de l'accès n'est pas prise en charge par NFS.

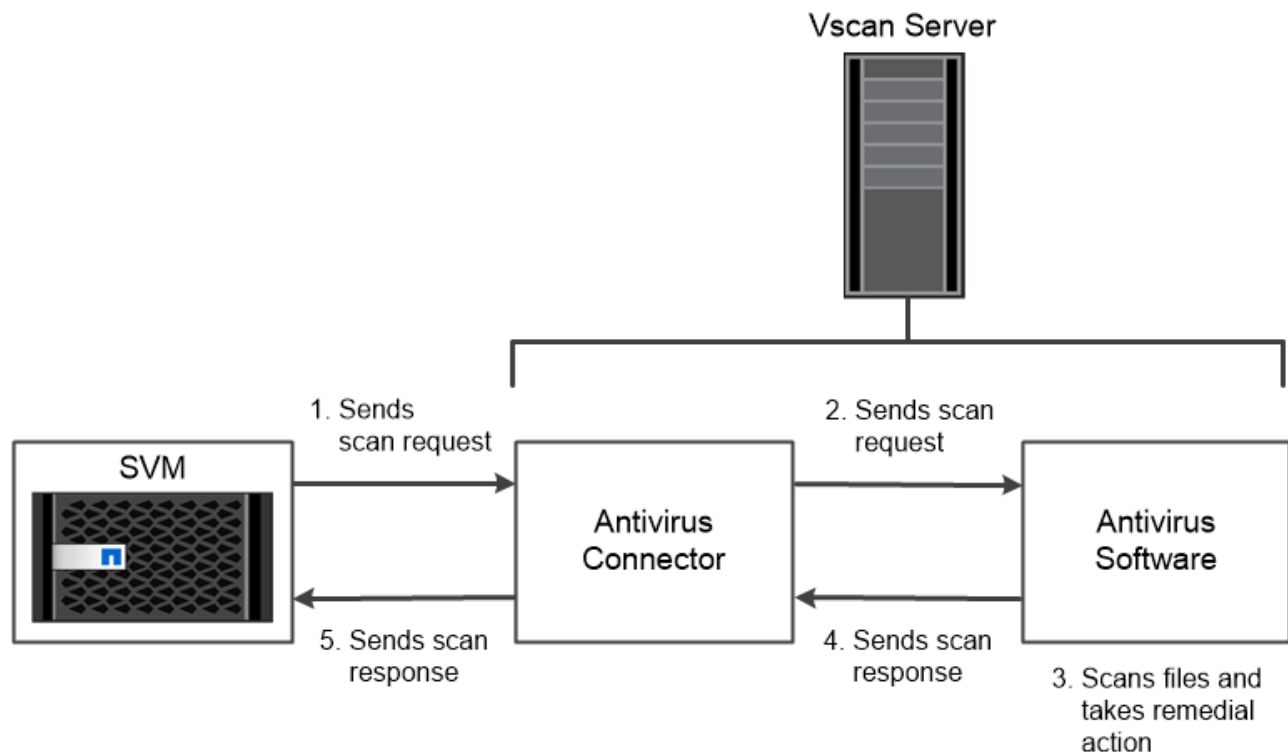
- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Il se peut que vous souhaitiez exécuter des analyses uniquement pendant les heures creuses, par exemple. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés, de sorte que la latence d'accès aux fichiers pour ces fichiers (en supposant qu'ils n'ont pas été modifiés) est généralement réduite lorsqu'ils sont ensuite accédés par SMB.

Vous pouvez utiliser l'analyse à la demande pour n'importe quel chemin du namespace du SVM, même pour les volumes exportés uniquement via NFS.

Vous activez généralement les deux modes de scan sur un SVM. Dans les deux modes, le logiciel antivirus prend des mesures correctives sur les fichiers infectés en fonction de vos paramètres dans le logiciel.

analyse antivirus dans la reprise après sinistre et configurations MetroCluster

Pour la reprise sur incident et les configurations MetroCluster, il faut configurer des serveurs Vscan séparés pour les clusters locaux et partenaires.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Le cryptage

ONTAP propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

ONTAP est conforme à la norme FIPS (Federal Information Processing Standards) 140-2 pour toutes les connexions SSL. Vous pouvez utiliser les solutions de cryptage suivantes :

- Solutions matérielles :

- NetApp Storage Encryption (NSE)

NSE est une solution matérielle qui utilise des lecteurs auto-cryptés (SED).

- Disques SED NVMe

ONTAP fournit le chiffrement de disque intégral pour les disques SED NVMe qui ne sont pas certifiés FIPS 140-2.

- Solutions logicielles :

- Chiffrement d'agrégat NetApp (NAE)

NAE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

- NVE (NetApp Volume Encryption)

NVE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.

Utilisez les solutions de chiffrement logiciel (NAE ou NVE) et matériel (NSE ou NVMe SED) afin d'obtenir le double chiffrement au repos. L'efficacité du stockage n'est pas affectée par le chiffrement NAE ou NVE.

NetApp Storage Encryption

NetApp Storage Encryption (NSE) prend en charge les disques SED qui cryptent les données au fur et à mesure de leur écriture. Les données ne peuvent pas être lues sans une clé de chiffrement stockée sur le disque. La clé de chiffrement, à son tour, n'est accessible qu'à un nœud authentifié.

Lors d'une demande d'E/S, un nœud s'authentifie auprès d'un SED à l'aide d'une clé d'authentification extraite d'un serveur de gestion de clés externe ou d'un gestionnaire de clés intégré :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés d'authentification aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données.

NSE prend en charge les disques durs et SSD à autocryptage. Vous pouvez utiliser NetApp Volume Encryption avec NSE pour doubler le chiffrement des données sur les disques NSE.



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

Disques à autochiffrement NVMe

Les disques SED NVMe ne disposent pas de la certification FIPS 140-2-2. Cependant, ces disques utilisent le chiffrement de disque transparent AES 256 bits pour protéger les données au repos.

Les opérations de chiffrement des données, telles que la génération d'une clé d'authentification, sont effectuées en interne. La clé d'authentification est générée la première fois que le système de stockage accède au disque. Les disques protègent ensuite les données au repos en demandant une authentification du système de stockage à chaque fois que des opérations de données sont demandées.

Chiffrement d'agrégat NetApp

NetApp Aggregate Encryption (NAE) est une technologie logicielle de chiffrement de toutes les données dans un agrégat. NAE a pour avantage de regrouper les volumes dans la déduplication au niveau des agrégats, là où les volumes NVE sont exclus.

NAE permet de chiffrer les volumes au sein de l'agrégat à l'aide de clés d'agrégat.

Depuis la version ONTAP 9.7, les nouveaux agrégats et volumes créés sont chiffrés par défaut lorsque vous disposez de "[Licence NVE](#)" et une gestion intégrée ou externe des clés.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Une clé de chiffrement accessible uniquement au système de stockage garantit que les données du volume ne peuvent pas être lues si le périphérique sous-jacent est séparé du système.

Les données, y compris les copies Snapshot, et les métadonnées sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume. Un gestionnaire de clés intégré sécurise les clés du même système avec vos données.

Vous pouvez utiliser NVE sur n'importe quel type d'agrégat (HDD, SSD, hybride, LUN de baie), avec n'importe quel type RAID et dans n'importe quelle implémentation ONTAP prise en charge, y compris ONTAP Select. Vous pouvez également utiliser NVE avec NetApp Storage Encryption (NSE) pour doubler le chiffrement des données sur les disques NSE.

quand utiliser des serveurs KMIP bien qu'il soit moins onéreux et généralement plus pratique pour utiliser le gestionnaire de clés intégré, vous devez configurer des serveurs KMIP si l'un des cas suivants est vrai :

- Votre solution de gestion des clés de chiffrement doit être conforme à la norme FIPS 140-2 (Federal Information Processing Standards) ou OASIS KMIP.
- Vous avez besoin d'une solution à plusieurs clusters. Les serveurs KMIP prennent en charge plusieurs clusters avec une gestion centralisée des clés de chiffrement.

Les serveurs KMIP prennent en charge plusieurs clusters avec une gestion centralisée des clés de chiffrement.

- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

Les serveurs KMIP stockent les clés d'authentification séparément des données.

Informations associées

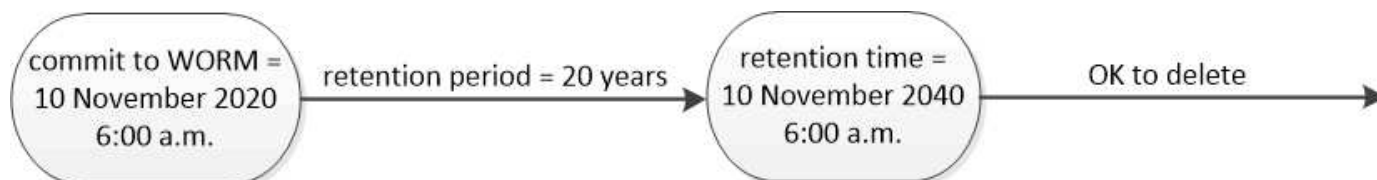
["FAQ : NetApp Volume Encryption et NetApp Aggregate Encryption"](#)

Stockage WORM

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM (Write Once, Read Many)_ pour conserver les fichiers stratégiques sous une forme non modifiée à des fins réglementaires et de gouvernance.

Une seule licence vous donne droit à l'utilisation de *SnapLock* en mode strict *Compliance*, afin de répondre aux obligations externes telles que la règle SEC 17a-4 et un mode plus lâche *Enterprise* afin de respecter les réglementations internes régissant la protection des ressources numériques. *SnapLock* utilise un *ComplianceClock* inviolable pour déterminer quand la période de conservation d'un fichier WORM est écoulée.

Vous pouvez utiliser *SnapLock for SnapVault* pour protéger les copies Snapshot sur un stockage secondaire. Vous pouvez utiliser *SnapMirror* pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins autres que la reprise après incident.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

Gestion des données intégrant la cohérence applicative

La gestion des données intégrant la cohérence applicative vous permet de décrire l'application que vous souhaitez déployer sur ONTAP en termes d'application, et non en termes de stockage. L'application peut être configurée et prête à diffuser les données

rapidement avec un minimum d'entrées grâce à System Manager et aux API REST.

La fonction de gestion des données intégrant la cohérence applicative offre un moyen de configurer, de gérer et de surveiller le stockage au niveau de chaque application. Cette fonctionnalité inclut les meilleures pratiques ONTAP qui permettent de provisionner des applications de manière optimale, avec un placement équilibré des objets de stockage en fonction des niveaux de service de performances souhaités et des ressources du système disponibles.

La fonction de gestion des données intégrant la cohérence applicative comprend un ensemble de modèles d'application, chaque modèle étant composé d'un ensemble de paramètres décrivant collectivement la configuration d'une application. Ces paramètres, qui sont souvent prédéfinis avec des valeurs par défaut, définissent les caractéristiques qu'un administrateur d'applications peut spécifier pour le provisionnement du stockage sur un système ONTAP, comme la taille des bases de données, les niveaux de service, les éléments d'accès par protocole tels que les LIF, ainsi que les critères de protection locale et les critères de protection à distance. En fonction des paramètres spécifiés, ONTAP configure des entités de stockage telles que les LUN et les volumes, avec des tailles et des niveaux de service appropriés pour l'application.

Vous pouvez effectuer les tâches suivantes pour vos applications :

- Créez des applications à l'aide des modèles d'application
- Gérez le stockage associé aux applications
- Modifiez ou supprimez les applications
- Afficher les applications
- Gérer les copies Snapshot des applications
- Création [groupes de cohérence](#) Pour fournir des fonctionnalités de protection des données, sélectionnez plusieurs LUN dans le même volume ou sur des volumes différents

FabricPool

De nombreux clients de NetApp disposent d'une quantité importante de données stockées rarement utilisées. On appelle les données *COLD*. Les clients disposent également de données fréquemment utilisées, que nous appelons les données *hot*. Dans l'idéal, vous souhaitez maintenir vos données actives dans votre système de stockage le plus rapide pour obtenir des performances optimales. Les données inactives peuvent être déplacées vers un stockage plus lent tant qu'elles sont immédiatement disponibles si nécessaire. Mais comment savoir quelles parties de vos données sont actives et lesquelles sont inactives ?

FabricPool est une fonctionnalité ONTAP qui déplace automatiquement les données entre un Tier local (agrégat) haute performance et un Tier cloud selon les modèles d'accès. Le Tiering libère du stockage local coûteux pour les données actives, tout en maintenant les données inactives disponibles immédiatement à partir d'un stockage objet à faible coût dans le cloud. FabricPool surveille en permanence l'accès aux données et les déplace entre les différents niveaux pour des performances optimales et des économies maximales.

L'utilisation de FabricPool pour déplacer les données inactives vers le cloud est l'un des moyens les plus simples d'obtenir des services efficaces dans le cloud et de créer une configuration de cloud hybride. FabricPool fonctionne au niveau du bloc de stockage et fonctionne donc aussi bien avec les données de fichiers que de LUN.

Toutefois, FabricPool n'est pas seulement pour le Tiering des données sur site vers le cloud. De nombreux

clients utilisent FabricPool dans Cloud Volumes ONTAP pour transférer les données inactives d'un stockage cloud plus onéreux vers un stockage objet moins coûteux au sein du fournisseur cloud. À partir de ONTAP 9.8, vous pouvez capturer l'analytique sur les volumes compatibles avec FabricPool avec ["Analytique du système de fichiers"](#) ou ["efficacité du stockage sensible à la température"](#).

Les applications qui utilisent les données n'ont pas connaissance du Tier de stockage. Aucune modification n'est donc nécessaire. Le Tiering est entièrement automatique. Aucune administration n'est donc nécessaire.

Vous pouvez stocker les données inactives dans le stockage objet à partir de l'un des principaux fournisseurs cloud. Vous pouvez également choisir NetApp StorageGRID pour conserver vos données inactives dans votre propre cloud privé et bénéficier d'une performance optimale et d'un contrôle total sur vos données.

Informations associées

["Document FabricPool System Manager"](#)

["Tiering BlueXP"](#)

["Liste de lecture FabricPool sur NetApp TechComm TV"](#)

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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