La réplication

ONTAP 9

NetApp
January 08, 2026

Sommaire

La réplication

Snapshots

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. Toutes ces utilisations reposent sur la technologie Snapshot de ONTAP.

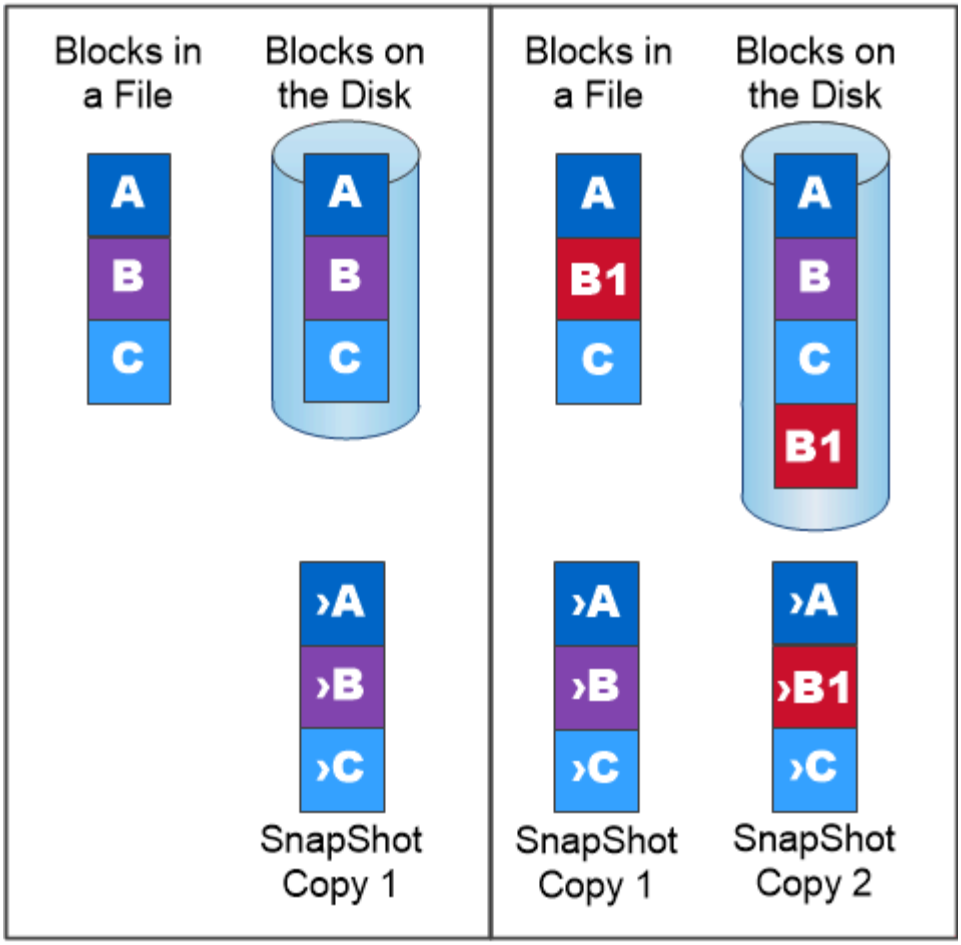
Un *snapshot* (anciennement *Snapshot copy*) est une image instantanée en lecture seule d'un volume. Après la création d'un snapshot, le système de fichiers actif et le snapshot pointent vers les mêmes blocs de disque ; par conséquent, le snapshot n'utilise pas d'espace disque supplémentaire. Au fil 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 le dernier snapshot.

Les snapshots doivent leur efficacité à la principale technologie de virtualisation du stockage de ONTAP, son modèle *WAFL (Write Anywhere File Layout).* à l'instar d'une base de données, WAFL utilise les métadonnées pour pointer vers les blocs de données réels sur le 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 snapshots sont efficaces car, au lieu de copier des blocs de données, ONTAP référence les métadonnées lors de la création d'un 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 un snapshot pour restaurer des fichiers individuels ou des LUN, ou pour restaurer l'intégralité du contenu d'un volume. ONTAP compare les informations de pointeur de la copie Snapshot aux données sur disque afin de reconstruire l'objet manquant ou endommagé, sans interruption ni coût de performance important.

Une *règle de snapshot* définit la façon dont le système crée des snapshots de volumes. La règle indique quand créer les snapshots, combien de copies conserver, comment les nommer et comment les étiqueter pour la réplication. Par exemple, un système peut créer un snapshot chaque jour à 12:10, conserver les deux copies les plus récentes, les nommer « quotidien » (ajouté à un horodatage) et les étiqueter « quotidien » 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.

Depuis la version 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 un snapshot du volume source.
- Transférez le snapshot et tous les blocs de données qu'il référence au volume de destination.
- Transférer les snapshots restants et moins récents sur le volume source vers le volume de destination en vue d'une utilisation en cas de corruption du miroir « actif ».

Une fois le transfert de base terminé, SnapMirror transfère uniquement les nouveaux snapshots vers le miroir. Les mises à jour sont asynchrones, en fonction du planning que vous configurez. La rétention met en miroir la règle de 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 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 cloud SnapMirror vers le stockage objet

SnapMirror Cloud 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. Le cloud SnapMirror offre une réplication du stockage ONTAP vers objet dans le cadre d'une stratégie de sauvegarde incrémentielle permanente.

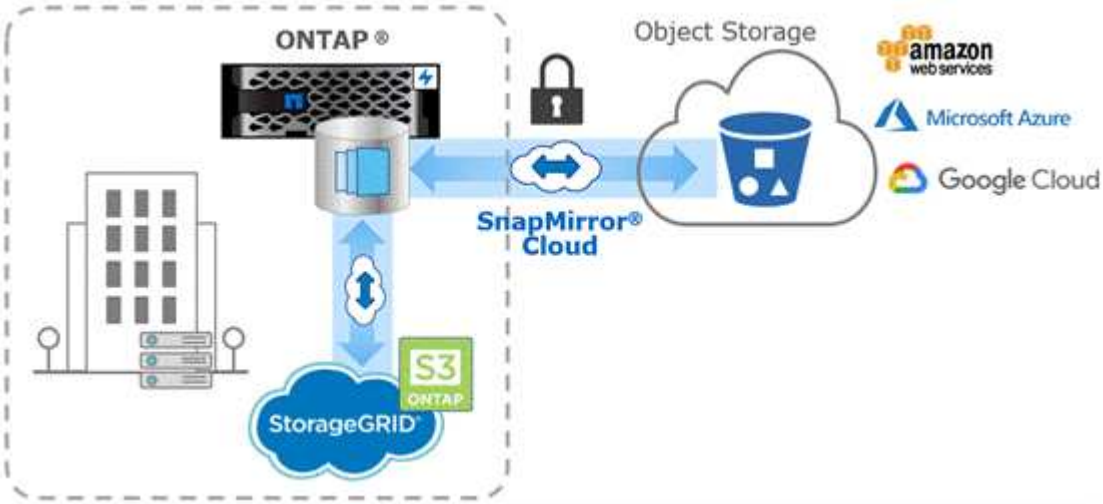
La réplication cloud SnapMirror est une fonctionnalité ONTAP sous licence. Le cloud SnapMirror a été introduit dans ONTAP 9.8 comme extension de la gamme de technologies de réplication SnapMirror. Tandis que SnapMirror est fréquemment utilisé pour les sauvegardes ONTAP à ONTAP, le cloud SnapMirror utilise le même moteur de réplication pour transférer les snapshots d'ONTAP vers des sauvegardes de stockage objet conformes à S3.

Conçu pour les cas d'usage de sauvegarde, le cloud SnapMirror prend en charge à la fois les workflows d'archivage et la conservation à long terme. Comme pour SnapMirror, la sauvegarde cloud SnapMirror initiale effectue un transfert de base d'un volume. Dans le cas des sauvegardes suivantes, le cloud SnapMirror génère un snapshot du volume source et transfère le Snapshot avec uniquement les blocs de données modifiés vers une cible de stockage objet.

Les relations cloud SnapMirror 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.

Outre l'utilisation d'ONTAP System Manager pour gérer les configurations cloud de SnapMirror, plusieurs options d'orchestration sont disponibles pour la gestion des sauvegardes cloud de SnapMirror :

- Plusieurs partenaires de sauvegarde tiers qui prennent en charge la réplication cloud SnapMirror. Les fournisseurs participants sont disponibles sur le "Blog NetApp".
- Sauvegarde et restauration NetApp pour une solution native NetApp 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, prenant en charge à la fois la sauvegarde et la reprise après incident.

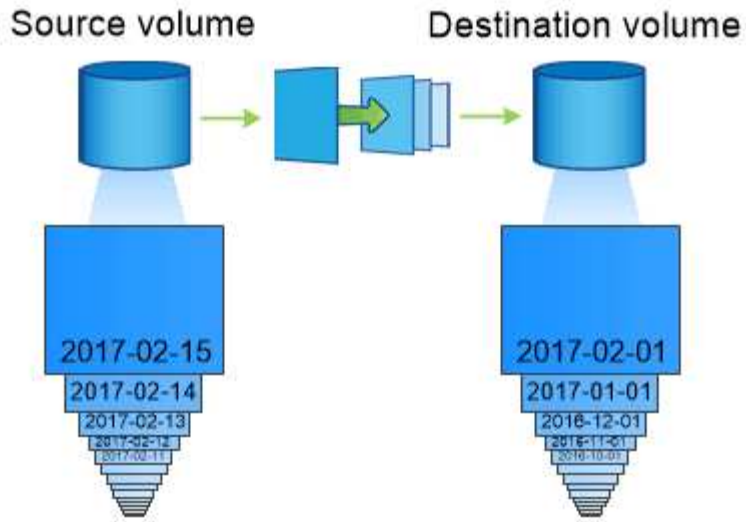
SnapVault est une technologie d'archivage conçue pour la réplication d'instantanés disque à disque à des fins de conformité aux normes et autres objectifs de gouvernance. Contrairement à une relation SnapMirror, dans laquelle la destination contient généralement uniquement les snapshots actuellement dans le volume source, une destination SnapVault conserve généralement les snapshots à un point dans le temps créés sur une période bien plus longue.

Vous pouvez conserver des snapshots mensuels de vos données sur une période de 20 ans, par exemple, pour respecter les réglementations comptables 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'appelez. Il crée un snapshot du volume source, puis transfère la copie et les blocs de données qu'il référence au volume de destination. Contrairement à SnapMirror, SnapVault n'inclut pas d'anciens snapshots 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 de relation identifient les nouveaux snapshots à inclure dans les mises à jour et le nombre de copies à conserver. Les étiquettes définies dans la règle (« mensuel, » par exemple) doivent correspondre à une ou plusieurs étiquettes définies dans la règle de snapshot sur 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.

À partir de ONTAP 9.8, le cloud SnapMirror offre une réplication asynchrone des copies Snapshot entre des instances ONTAP et des terminaux de stockage objet. La réplication cloud SnapMirror nécessite une application sous licence pour l'orchestration et la gestion des workflows de protection des données. Les relations cloud SnapMirror sont prises en charge par les systèmes ONTAP pour sélectionner des cibles de stockage objet sur site et dans le cloud public, y compris AWS S3, Google Cloud Storage Platform ou Microsoft Azure Blob Storage, pour une efficacité améliorée 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 vous êtes intéressé par la protection des données natives du cloud, la console NetApp peut être utilisée pour configurer les relations SnapMirror ou SnapVault entre les volumes locaux et les instances Cloud Volumes ONTAP dans le cloud public.

La console fournit également des sauvegardes d'instances Cloud Volumes ONTAP à l'aide d'un modèle SaaS (Software as a Service). Les utilisateurs peuvent sauvegarder leurs instances Cloud Volumes ONTAP sur un stockage d'objets cloud public compatible S3 et S3 à l'aide de NetApp Backup and Recovery.

"Documentation Cloud Volumes ONTAP"

"Documentation de la console NetApp"

"Console NetApp"

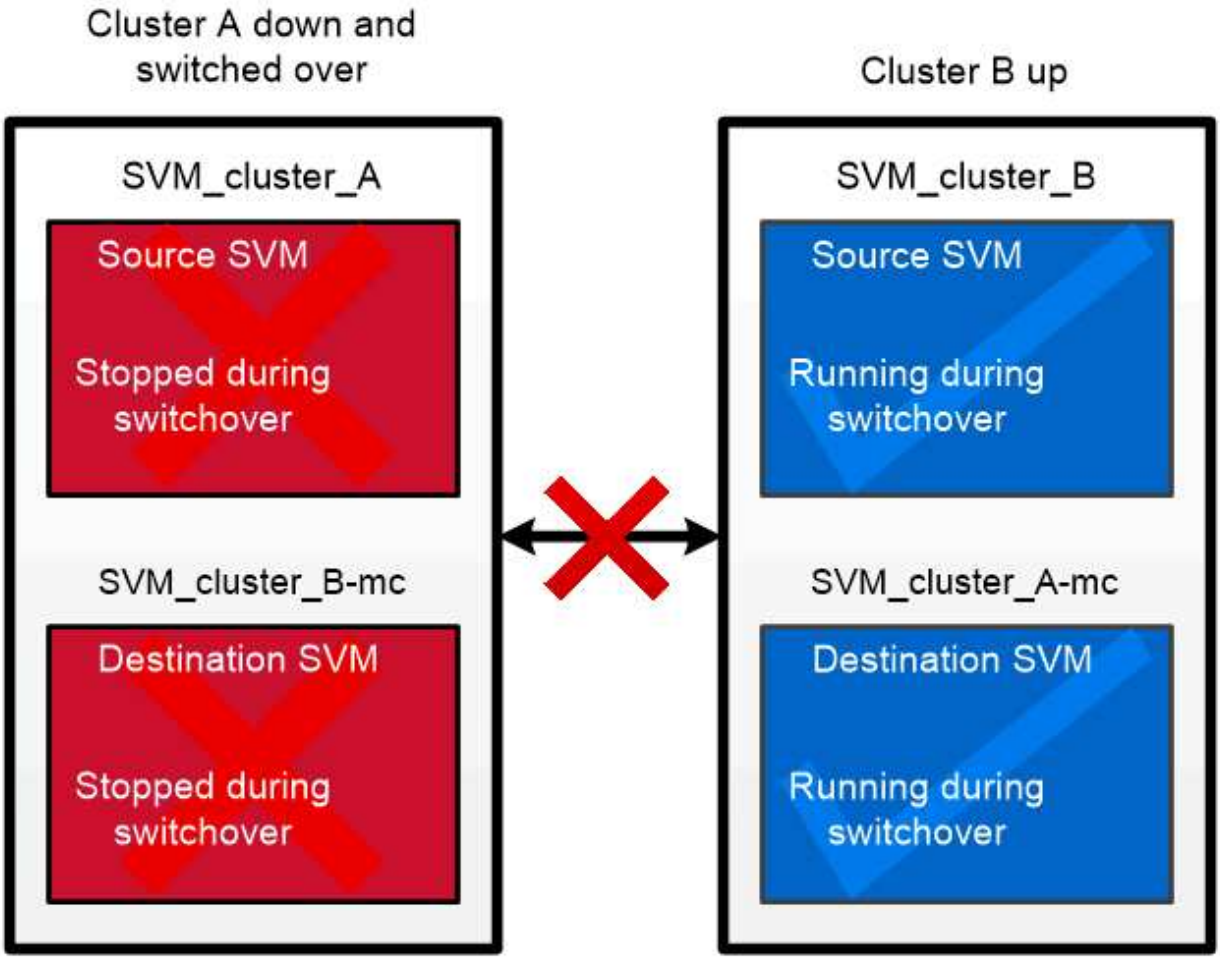
Disponibilité sans interruption avec MetroCluster

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 *Fabric-Attached MetroCluster* et *MetroCluster IP* prennent en charge les clusters à l'échelle 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 de copie sur écriture de ONTAP. 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.

Informations sur le copyright

Informations sur les marques commerciales