



En savoir plus sur la réplication de volume SnapMirror

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap/data-protection/snapmirror-disaster-recovery-concept.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

En savoir plus sur la réplication de volume SnapMirror	1
En savoir plus sur la reprise après incident asynchrone ONTAP SnapMirror	1
Relations de protection des données	1
Portée des relations de protection des données	2
Comment les relations de protection des données SnapMirror sont initialisées	2
Mise à jour des relations de protection des données SnapMirror	2
Politique MirrorLatest	3
Découvrez la reprise d'activité synchrone de ONTAP SnapMirror	4
Opérations synchrones SnapMirror autorisées	4
Fonctionnalités prises en charge	4
Fonctions non prises en charge	7
Modes de fonctionnement	7
État des relations	8
Règles de protection des données ONTAP par défaut	8
Liste des stratégies de protection par défaut et descriptions	8
En savoir plus sur les charges de travail prises en charge par les règles ONTAP StrictSync et Sync	10
En savoir plus sur l'archivage par coffre-fort grâce à la technologie ONTAP SnapMirror	10
Comment les relations de protection des données du coffre-fort sont initialisées	11
Mise à jour des relations de protection des données Vault	11
Découvrez la réplication unifiée ONTAP SnapMirror	12
Mode d'initialisation des relations de protection unifiée des données	12
Mise à jour des relations de protection unifiée des données	13
Politique unifiée sur 7ans	13
Protégez-vous contre les risques de corruption	14
À quel moment utiliser la réplication unifiée des données	14
En cas d'augmentation automatique du volume cible de protection des données ONTAP	14
Découvrez la protection des données ONTAP « Fan-Out » et les déploiements en cascade	15
Fonctionnement des déploiements « Fan-Out »	15
Fonctionnement des déploiements en cascade	17
En savoir plus sur les licences ONTAP SnapMirror	18
Licence synchrone SnapMirror	19
Licence cloud SnapMirror	19
Licence optimisée pour Data protection	20
Les systèmes DPO de ONTAP offrent des améliorations	20
En savoir plus sur la correspondance des motifs de nom de chemin dans les commandes ONTAP SnapMirror	21
En savoir plus sur les requêtes étendues pour les opérations liées à ONTAP SnapMirror	22
Compatibilité des versions ONTAP pour les relations SnapMirror	23
Relations de réplication unifiée	23
Relations synchrones SnapMirror	25
Relations de reprise d'activité SVM SnapMirror	25
Relations de reprise sur incident SnapMirror	31
Découvrez les limites de ONTAP SnapMirror	31

En savoir plus sur la réplication de volume SnapMirror

En savoir plus sur la reprise après incident asynchrone ONTAP SnapMirror

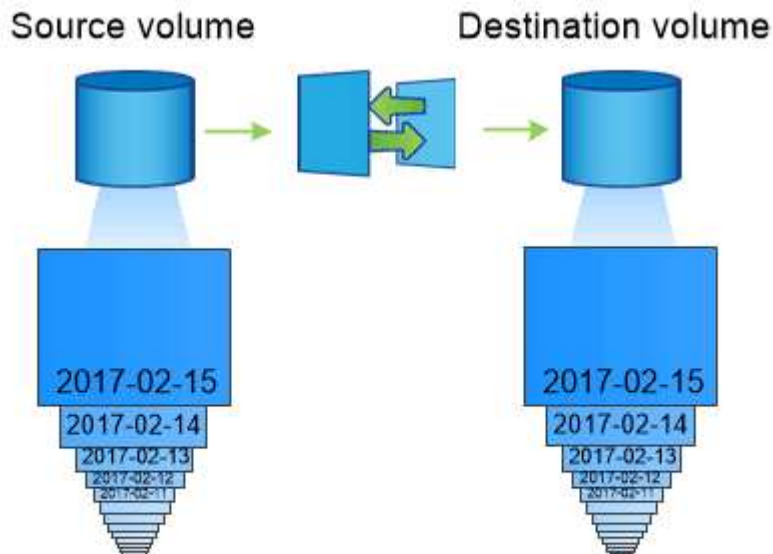
SnapMirror est une technologie de reprise après incident conçue pour le basculement du stockage primaire vers le stockage secondaire sur un site distant. Comme son nom l'indique, SnapMirror crée une réplique ou *mirror* de vos données de travail dans un stockage secondaire à partir duquel vous pouvez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

Si le site primaire assure toujours le service des données, il vous suffit de transférer les données requises vers celui-ci et ne transmet plus le tout aux clients depuis le miroir. 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.

Relations de protection des données

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 de protection des données ». Les clusters dans lesquels résident les volumes et les SVM qui fournissent des données depuis ces volumes doivent être de "touré". Grâce à une relation de pairs, les clusters et les SVM peuvent échanger les données de manière sécurisée.

Cette figure illustre les relations de protection des données SnapMirror :



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

Portée des relations de protection des données

Vous pouvez créer une relation de protection des données directement entre des volumes ou entre les SVM qui possèdent des volumes. Dans une relation de protection des données de SVM, tout ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB jusqu'au RBAC, est répliqué, ainsi que les données des volumes que la SVM possède.

Vous pouvez également utiliser SnapMirror pour des applications spéciales de protection des données :

- Une *partage de charge mirror* du volume root du SVM permet de garantir que les données restent accessibles en cas de panne ou de basculement du nœud.
- Une relation de protection des données entre *SnapLock volumes* vous permet de répliquer des fichiers WORM sur un stockage secondaire.

"Archivage et conformité grâce à la technologie SnapLock"

- À partir de ONTAP 9.13.1, vous pouvez utiliser SnapMirror asynchrone pour protéger [groupes de cohérence](#). Depuis la version ONTAP 9.14.1, vous pouvez utiliser la réplication asynchrone SnapMirror pour répliquer des snapshots granulaires par volume vers le cluster de destination à l'aide de la relation de groupe de cohérence. Pour plus d'informations, voir [Configurer la protection asynchrone SnapMirror](#).

Comment les relations de protection des données SnapMirror sont initialisées

La première fois que vous appelez SnapMirror, il effectue un *transfert de base* du volume source vers le volume de destination. La *SnapMirror policy* pour la relation définit le contenu de la base et toutes les mises à jour.

Transfert de base avec la règle SnapMirror par défaut `MirrorAllSnapshots` implique 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 ».

Mise à jour des relations de protection des données SnapMirror

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.

À chaque mise à jour de la `MirrorAllSnapshots` règle, SnapMirror crée un snapshot du volume source et transfère cet instantané ainsi que tous les snapshots effectués depuis la dernière mise à jour. Dans les valeurs de sortie suivantes de `snapmirror policy show` la commande pour la `MirrorAllSnapshots` règle, noter ce qui suit :

- `Create Snapshot Est` « true », ce qui signifie que `MirrorAllSnapshots` crée un snapshot lorsque SnapMirror met à jour la relation.
- `MirrorAllSnapshots` Possède des règles « `sm_created` » et « `all_source_snapshots` », indiquant que le snapshot créé par SnapMirror et tous les snapshots effectués depuis la dernière mise à jour sont transférés lorsque SnapMirror met à jour la relation.

```
cluster_dst:> snapmirror policy show -policy MirrorAllSnapshots -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: SnapMirror asynchronous policy for mirroring
all snapshots
and the latest active file system.
Total Number of Rules: 2
Total Keep: 2
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
sm_created                  1  false      0 -
all_source_snapshots       1  false      0 -
```

Politique MirrorLatest

La règle préconfigurée `MirrorLatest` fonctionne exactement de la même manière que `MirrorAllSnapshots`, sauf que seul le snapshot créé par `SnapMirror` est transféré à l'initialisation et à la mise à jour.

```
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
sm_created                  1  false      0 -
```

Informations associées

- ["afficher la politique de SnapMirror"](#)

Découvrez la reprise d'activité synchrone de ONTAP SnapMirror

À partir de ONTAP 9.5, la technologie SnapMirror synchrone (SM-S) est prise en charge sur toutes les plateformes FAS et AFF disposant d'au moins 16 Go de mémoire et sur toutes les plateformes ONTAP Select. La technologie synchrone SnapMirror est une fonction sous licence par nœud qui permet la réplication synchrone des données au niveau des volumes.

Cette fonctionnalité répond aux exigences réglementaires et nationales en matière de réplication synchrone dans les secteurs financiers, de la santé et autres secteurs réglementés où aucune perte de données n'est requise.

Opérations synchrones SnapMirror autorisées

La limite du nombre d'opérations de réplication synchrone SnapMirror par paire HA dépend du modèle de contrôleur.

Le tableau ci-dessous répertorie le nombre d'opérations SnapMirror synchrones autorisées par paire haute disponibilité selon le type de plateforme et la version de ONTAP.

Plateforme	ONTAP 9.14.1 à ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	Versions antérieures à ONTAP 9.9.1
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

Fonctionnalités prises en charge

Le tableau suivant indique les fonctionnalités prises en charge par SnapMirror synchrone et les versions ONTAP dans lesquelles la prise en charge est disponible.

Fonction	Version d'abord prise en charge	Informations supplémentaires
Antivirus sur le volume primaire de la relation synchrone SnapMirror	ONTAP 9.6	

Réplication Snapshot créée par les applications	ONTAP 9.7	Si un instantané est étiqueté avec l'étiquette appropriée au moment de la <code>snapshot create</code> opération, en utilisant la CLI ou l'API ONTAP , SnapMirror réplique de manière synchrone les snapshots, créés par l'utilisateur ou ceux créés avec des scripts externes, après avoir mis au repos les applications. Les instantanés planifiés créés à l'aide d'une stratégie d'instantané ne sont pas répliqués. Pour plus d'informations sur la réplication des instantanés créés par l'application, consultez le "Base de connaissances NetApp : Comment répliquer des snapshots créés par une application avec SnapMirror synchrone" .
Suppression automatique des clones	ONTAP 9.6	
Les agrégats FabricPool avec règles de Tiering aucune, Snapshot ou Auto sont pris en charge avec la source et la destination synchrones SnapMirror.	ONTAP 9.5	Le volume de destination d'un agrégat FabricPool ne peut pas être défini sur l'ensemble des règles de Tiering.
FC	ONTAP 9.5	Sur tous les réseaux pour lesquels la latence ne dépasse pas 10 ms.
NVMe-FC	ONTAP 9.7	
Clones de fichiers	ONTAP 9.7	
FPolicy sur le volume principal de la relation synchrone SnapMirror	ONTAP 9.6	
Quotas matériels et conditionnels sur le volume primaire de la relation synchrone SnapMirror	ONTAP 9.6	Les règles de quota ne sont pas répliquées vers la destination. Par conséquent, la base de données de quota n'est pas répliquée vers la destination.
Relations synchrones intra-cluster	ONTAP 9.14.1	Les volumes source et de destination sont placés sur différentes paires haute disponibilité. En cas de panne de l'intégralité du cluster, l'accès aux volumes ne sera pas possible tant que le cluster n'aura pas été restauré. Les relations synchrones SnapMirror intra-cluster contribueront à la limite globale de simultanément Relations par paire haute disponibilité .
ISCSI	ONTAP 9.5	
Clones de LUN et clones d'espace de noms NVMe	ONTAP 9.7	
Clones de LUN soutenus par des snapshots créés par les applications	ONTAP 9.7	
Accès à des protocoles mixtes (NFS v3 et SMB)	ONTAP 9.6	
Restauration NDMP/NDMP	ONTAP 9.13.1	Le cluster source et le cluster destination doivent exécuter ONTAP 9.13.1 ou une version ultérieure pour pouvoir utiliser NDMP avec SnapMirror synchrone. Pour plus d'informations, voir Transfert de données à l'aide d'une copie ndmp .

CONTINUITÉ de l'ACTIVITÉ (SnapMirror Synchronous Operations) sans interruption sur les plateformes AFF/ASA, uniquement.	ONTAP 9.12.1	La prise en charge de la continuité de l'activité vous permet d'effectuer de nombreuses tâches de maintenance courantes sans planifier de temps d'indisponibilité. Les opérations prises en charge incluent le basculement et le retour, ainsi que le déplacement de volumes, à condition qu'un seul nœud survive au sein de chacun des deux clusters.
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	
Suppression de la limitation de fréquence d'opération de métadonnées élevée	ONTAP 9.6	
Sécurité des données sensibles en transit avec le chiffrement TLS 1.2	ONTAP 9.6	
Restauration de fichiers uniques et partiels	ONTAP 9.13.1	
SMB 2.0 ou version ultérieure	ONTAP 9.6	
Cascade miroir-miroir synchrone SnapMirror	ONTAP 9.6	La relation provenant du volume de destination de la relation synchrone SnapMirror doit être une relation asynchrone SnapMirror.
Reprise d'activité de SVM	ONTAP 9.6	* Une source synchrone de SnapMirror peut également être une source de reprise d'activité de SVM, par exemple une configuration « Fan-Out » avec SnapMirror synchrone comme une seule étape et SVM de reprise d'activité comme l'autre. * Une source synchrone SnapMirror ne peut pas être une destination de reprise d'activité SVM, car SnapMirror synchrone ne prend pas en charge le cascading d'une source de protection des données. Vous devez relâcher la relation synchrone avant d'effectuer une resynchronisation de reprise d'activité SVM dans le cluster destination. * Une destination synchrone SnapMirror ne peut pas être une source de reprise d'activité SVM, car la reprise d'activité SVM ne prend pas en charge la réplication des volumes DP. Une resynchronisation de la source synchrone entraînerait la reprise d'activité du SVM excluant le volume DP dans le cluster de destination.
Restauration sur bande vers le volume source	ONTAP 9.13.1	

Parité temporelle entre les volumes source et de destination pour le NAS	ONTAP 9.6	Si vous avez effectué une mise à niveau de ONTAP 9.5 vers ONTAP 9.6, l'horodatage est uniquement répliqué pour les fichiers nouveaux et modifiés du volume source. L'horodatage des fichiers existants dans le volume source n'est pas synchronisé.
--	-----------	---

Fonctions non prises en charge

Les fonctionnalités suivantes ne sont pas prises en charge avec les relations SnapMirror synchrones :

- Protection autonome contre les ransomwares
- Groupes de cohérence
- Systèmes DP_optimisés (DPO)
- Volumes FlexGroup
- Volumes FlexCache
- Limitation globale
- Dans une configuration « Fan-Out », une seule relation peut être une relation synchrone SnapMirror ; toutes les autres relations du volume source doivent être des relations SnapMirror asynchrones.
- Déplacement de LUN
- Configurations MetroCluster
- Accès mixte SAN/NVMe
Les LUN et les namespaces NVMe ne sont pas pris en charge sur le même volume ou SVM.
- SnapCenter
- Volumes SnapLock
- Des snapshots inviolables
- Sauvegarde sur bande ou restauration à l'aide de dump et SMTape sur le volume de destination
- Débit au sol (QoS min) pour les volumes source
- SnapRestore du volume
- VVol

Modes de fonctionnement

SnapMirror synchrone dispose de deux modes de fonctionnement basés sur le type de la règle SnapMirror utilisée :

- **Mode de synchronisation** en mode de synchronisation, les opérations d'E/S d'application sont envoyées en parallèle aux systèmes de stockage primaire et secondaire. Si l'écriture dans le stockage secondaire n'est pas terminée, pour une raison quelconque, l'application peut continuer à écrire sur le stockage primaire. Une fois l'erreur corrigée, la technologie synchrone SnapMirror se resynchronise automatiquement avec le stockage secondaire et reprend la réplication du stockage primaire vers le stockage secondaire en mode synchrone. En mode synchrone, RPO=0 et RTO sont très faibles jusqu'à ce qu'une défaillance de réplication secondaire se produise. Ainsi, les objectifs RPO et RTO deviennent indéterminés, mais équivalent au temps de résolution du problème à l'origine de la défaillance de la réplication secondaire et de la resynchronisation à réaliser.
- **StrictSync mode** SnapMirror synchrone peut fonctionner en mode StrictSync. Si l'écriture sur le stockage

secondaire n'est pas terminée, pour une raison quelconque, les E/S de l'application échouent, ce qui permet de s'assurer que les stockages primaire et secondaire sont identiques. Les E/S de l'application vers le primaire ne reprennent que lorsque la relation SnapMirror revient au InSync statut. En cas de panne du stockage primaire, les E/S des applications peuvent reprendre sur le système de stockage secondaire, après le basculement, sans perte de données. En mode StrictSync, le RPO est toujours nul et le RTO très faible.

État des relations

L'état d'une relation synchrone SnapMirror est toujours en InSync cours de fonctionnement normal. Si le transfert SnapMirror échoue pour une raison quelconque, la destination n'est pas synchronisée avec la source et peut passer à l' OutofSync`état.

Pour les relations synchrones SnapMirror, le système vérifie automatiquement l'état de InSync la relation ou OutofSync) à un intervalle fixe. Si l'état de la relation est OutofSync, ONTAP déclenche automatiquement le processus de resynchronisation automatique pour ramener la relation à l' InSync`état. La resynchronisation automatique n'est déclenchée que si le transfert échoue en raison de certaines opérations, telles que le basculement non planifié du stockage à la source ou à la destination, ou en cas de panne réseau. Les opérations initiées par l'utilisateur telles que `snapmirror quiesce et snapmirror break ne déclenchent pas de resynchronisation automatique.

Si la relation devient OutofSync pour une relation synchrone SnapMirror en mode StrictSync, toutes les opérations d'E/S vers le volume primaire sont arrêtées. L' OutofSync`état de la relation synchrone SnapMirror en mode synchrone ne perturbe pas les opérations principales et les opérations d'E/S sont autorisées sur le volume principal.

Informations associées

- ["Rapport technique NetApp 4733 : configuration synchrone et bonnes pratiques SnapMirror"](#)
- ["pause snapmirror"](#)
- ["SnapMirror arrête"](#)

Règles de protection des données ONTAP par défaut

ONTAP inclut plusieurs règles de protection par défaut que vous pouvez utiliser pour vos relations de protection des données. La stratégie que vous utilisez dépend du type de relation de protection.

Si les règles par défaut ne répondent pas aux besoins de vos relations de protection des données, vous pouvez ["créer une règle personnalisée"](#).

Liste des stratégies de protection par défaut et descriptions

Les règles de protection par défaut et les types de règles qui leur sont associés sont décrits ci-dessous.

Nom	Description	Type de règle
Asynchrone	Règle de copie et réplication asynchrone SnapMirror unifiée pour la mise en miroir du système de fichiers actif le plus récent et des copies Snapshot quotidiennes et hebdomadaires avec une planification de transfert horaire.	Asynchrone
Automatique - mode dégradé	La règle pour SnapMirror synchrone avec objectif de durée de restauration nul garantit que les E/S client ne seront pas interrompues en cas d'échec de réplication.	Synchrone
AutoFailOverDuplex	Règle pour SnapMirror synchrone avec garantie RTO nul et réplication synchrone bidirectionnelle.	Synchrone
CloudBackupDefault	Règle de coffre-fort avec règle quotidienne.	Asynchrone
Continu	Règle de mise en miroir des compartiments S3.	Continu
DailyBackup	Règle de coffre-fort avec une règle quotidienne et un planning de transfert quotidien.	Asynchrone
DPDefault	Règle asynchrone SnapMirror pour la mise en miroir de tous les snapshots et du dernier système de fichiers actif.	Asynchrone
MirrorAllsnapshots	Règle asynchrone SnapMirror pour la mise en miroir de tous les snapshots et du dernier système de fichiers actif.	Asynchrone
MirrorAllSnapshotsDisCardNetwork	Politique asynchrone de SnapMirror pour la mise en miroir de tous les snapshots et du dernier système de fichiers actif, à l'exclusion des configurations réseau.	Asynchrone
MirrorAndVault	Règle de copie et réplication asynchrone SnapMirror unifiée pour la mise en miroir du système de fichiers actif le plus récent et des snapshots quotidiens et hebdomadaires.	Asynchrone
MirrorAndVaultDiscartNetwork	Règle de copie asynchrone et unifiée SnapMirror pour la mise en miroir du dernier système de fichiers actif et des copies Snapshot quotidiennes et hebdomadaires à l'exclusion des configurations réseau.	Asynchrone
MirrorLatest	Règle asynchrone SnapMirror pour la mise en miroir du dernier système de fichiers actif.	Asynchrone
SnapCenterSync	Règle pour SnapMirror synchrone pour SnapCenter avec configuration Snapshot créée par l'application.	Synchrone
StrictSync	Règle de SnapMirror synchrone où l'accès client sera interrompu en cas d'échec de réplication.	Synchrone
Synchrone	Règle pour SnapMirror synchrone où l'accès client ne sera pas interrompu en cas d'échec de réplication.	Synchrone
Unifié 7ans	Règle de conservation unifiée SnapMirror de 7 ans	Asynchrone

Nom	Description	Type de règle
XDPDefault	Règle de coffre-fort avec règles quotidiennes et hebdomadaires.	Asynchrone

En savoir plus sur les charges de travail prises en charge par les règles ONTAP StrictSync et Sync

Les règles StrictSync et Sync prennent en charge toutes les applications basées sur les LUN avec les protocoles FC, iSCSI et FC-NVMe, ainsi que les protocoles NFSv3 et NFSv4 pour les applications d'entreprise telles que les bases de données, VMware, les quotas, SMB, etc. À partir de la version ONTAP 9.6, SnapMirror synchrone peut être utilisé pour les services de fichiers d'entreprise tels que l'automatisation de la conception électronique (EDA), les répertoires locaux et les workloads de conception logicielle.

Dans ONTAP 9.5, pour une règle de synchronisation, vous devez tenir compte de quelques aspects importants lors de la sélection des workloads NFSv3 ou NFSv4. Le nombre d'opérations de lecture ou d'écriture de données par workload n'est pas pris en compte, car la règle de synchronisation peut gérer des workloads d'E/S haute capacité de lecture ou d'écriture. Dans ONTAP 9.5, les charges de travail dont la création de fichiers, la création de répertoires, les modifications d'autorisations liées aux fichiers ou les modifications d'autorisations de répertoire sont excessives peuvent ne pas convenir (on parle alors de charges de travail hautement métadonnées). Un workload de métadonnées élevé est un exemple de workload DevOps dans lequel vous créez plusieurs fichiers de test, exécutez une automatisation et supprimez les fichiers. Il est également possible, par exemple, de créer une charge de travail parallèle qui génère plusieurs fichiers temporaires lors de la compilation. L'impact d'un taux élevé d'activité de métadonnées d'écriture est qu'il peut entraîner une rupture temporaire entre les miroirs, ce qui bloque les E/S de lecture et d'écriture du client.

Depuis la version ONTAP 9.6, ces limitations sont supprimées et SnapMirror synchrone peut être utilisé pour les workloads de services de fichiers d'entreprise qui incluent des environnements multi-utilisateurs, tels que les répertoires locaux et les workloads de développement logiciel.

Informations associées

["Configuration synchrone de SnapMirror et bonnes pratiques"](#)

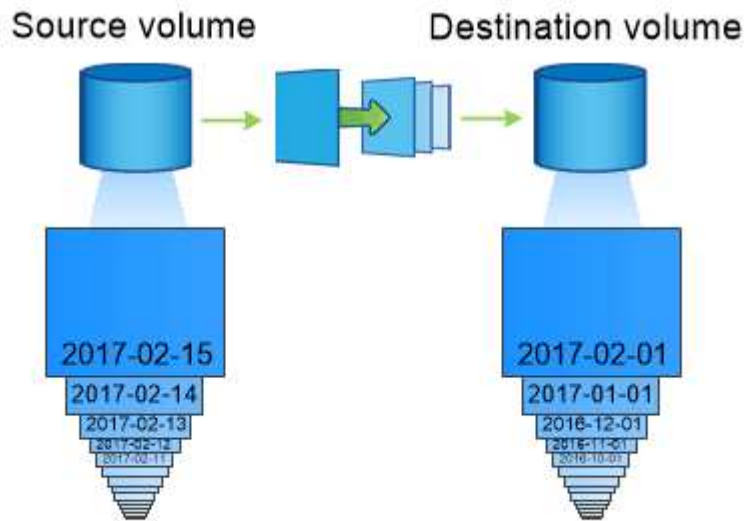
En savoir plus sur l'archivage par coffre-fort grâce à la technologie ONTAP SnapMirror

Les règles d'archivage sécurisé SnapMirror remplacent la technologie SnapVault dans ONTAP 9.3 et versions ultérieures. Vous utilisez une règle de copie SnapMirror pour la réplication snapshot disque à disque à des fins de conformité aux normes et autres questions de gouvernance. Contrairement à une relation SnapMirror, dans laquelle la destination ne contient généralement que les snapshots actuellement dans le volume source, une destination de coffre-fort 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.

La figure ci-dessous illustre les relations de protection des données du coffre-fort SnapMirror.



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.

Comment les relations de protection des données du coffre-fort sont initialisées

La règle SnapMirror pour la relation définit le contenu de la base et toutes les mises à jour.

Un transfert de base dans le cadre de la règle de coffre-fort par défaut `XDPDefault` crée un snapshot du volume source, puis transfère cette copie et les blocs de données qu'elle référence au volume de destination. Contrairement aux relations SnapMirror, la sauvegarde par copie ne comprend pas d'anciens snapshots dans la configuration de base.

Mise à jour des relations de protection des données Vault

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.

À chaque mise à jour de la `XDPDefault` règle, SnapMirror transfère les instantanés créés depuis la dernière mise à jour, à condition qu'ils aient des étiquettes correspondant aux étiquettes définies dans les règles de règle. Dans les valeurs de sortie suivantes de `snapmirror policy show` la commande pour la `XDPDefault` règle, noter ce qui suit :

- `Create Snapshot` Est « false », ce qui indique que `XDPDefault` ne crée pas de snapshot lorsque SnapMirror met à jour la relation.
- `XDPDefault` Possède des règles « quotidiennes » et « hebdomadaires », indiquant que tous les snapshots avec des libellés correspondants sur la source sont transférés lorsque SnapMirror met à jour la relation.

```
cluster_dst:> snapmirror policy show -policy XDPDefault -instance

Vserver: vs0
SnapMirror Policy Name: XDPDefault
SnapMirror Policy Type: vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: false
Comment: Default policy for XDP relationships with
daily and weekly
rules.
Total Number of Rules: 2
Total Keep: 59
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
daily                          7  false      0  -
weekly                        52  false      0  -
```

Informations associées

- ["afficher la politique de SnapMirror"](#)

Découvrez la réplication unifiée ONTAP SnapMirror

SnapMirror *réplication unifiée* permet de configurer la reprise après incident et l'archivage sur le même volume de destination. Lorsque la réplication unifiée est appropriée, elle offre des avantages en réduisant la quantité de stockage secondaire nécessaire, en limitant le nombre de transferts de base et en diminuant le trafic réseau.

Mode d'initialisation des relations de protection unifiée des données

Comme pour SnapMirror, la protection unifiée des données effectue un transfert de base dès le premier appel que vous l'appellez. La règle SnapMirror pour la relation définit le contenu de la base et toutes les mises à jour.

Un transfert de base dans le cadre de la règle de protection des données unifiée par défaut `MirrorAndVault` effectue un snapshot du volume source, puis transfère cette copie et les blocs de données qu'elle référence au volume de destination. Tout comme l'archivage en coffre-fort, la protection unifiée des données n'inclut pas les anciens snapshots dans la configuration de base.

Mise à jour des relations de protection unifiée des données

À chaque mise à jour de la MirrorAndVault règle, SnapMirror crée un snapshot du volume source et transfère ce snapshot ainsi que tous les snapshots créés depuis la dernière mise à jour, à condition qu'ils aient des étiquettes correspondant aux étiquettes définies dans les règles de la règle de snapshot. Dans les valeurs de sortie suivantes de `snapmirror policy show` la commande pour la MirrorAndVault règle, noter ce qui suit :

- Create Snapshot Est « true », ce qui signifie que MirrorAndVault crée un snapshot lorsque SnapMirror met à jour la relation.
- MirrorAndVault Possède des règles « `sm\_created` », « quotidiennes » et « hebdomadaires », ce qui indique que le snapshot créé par SnapMirror et les snapshots avec des libellés correspondants sur la source sont transférés lorsque SnapMirror met à jour la relation.

```
cluster_dst:> snapmirror policy show -policy MirrorAndVault -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAndVault
SnapMirror Policy Type: mirror-vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: A unified SnapMirror synchronous and
SnapVault policy for
mirroring the latest file system and daily
and weekly snapshots.
Total Number of Rules: 3
Total Keep: 59
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                  1  false    0  -
daily                       7  false    0  -
weekly                     52  false    0  -
```

Politique unifiée sur 7ans

La règle préconfigurée Unified7year fonctionne exactement de la même manière que MirrorAndVault, sauf qu'une quatrième règle transfère les snapshots mensuels et les conserve pendant sept ans.

Schedule Prefix	Rules: SnapMirror Label	Keep	Preserve	Warn
-----	-----	----	-----	----
-	sm_created	1	false	0 -
-	daily	7	false	0 -
-	weekly	52	false	0 -
-	monthly	84	false	0 -
-				

Protégez-vous contre les risques de corruption

La réplication unifiée limite le contenu du transfert de base vers le snapshot créé par SnapMirror au moment de l'initialisation. À chaque mise à jour, SnapMirror crée un autre snapshot de la source et le transfère ainsi que tout nouvel instantané dont les étiquettes correspondent aux étiquettes définies dans les règles de la règle de snapshot.

Vous pouvez vous protéger contre le risque de corruption d'un instantané mis à jour en créant une copie du dernier instantané transféré sur la destination. Cette « copie locale » est conservée indépendamment des règles de conservation sur la source, de sorte que même si l'instantané initialement transféré par SnapMirror n'est plus disponible sur la source, une copie de celui-ci sera disponible sur la destination.

À quel moment utiliser la réplication unifiée des données

Vous devez évaluer les avantages de la maintenance d'un miroir complet par rapport aux avantages offerts par la réplication unifiée : réduction de la quantité de stockage secondaire, limitation du nombre de transferts de base et diminution du trafic réseau.

Le facteur clé pour déterminer la pertinence de la réplication unifiée est le taux de changement du système de fichiers actif. Par exemple, un miroir traditionnel convient mieux à un volume contenant des snapshots horaires de journaux de transactions de base de données.

Informations associées

- ["afficher la politique de SnapMirror"](#)

En cas d'augmentation automatique du volume cible de protection des données ONTAP

Lors d'un transfert de miroir de protection des données, la taille du volume de destination augmente automatiquement si le volume source a augmenté, à condition que l'espace disponible soit présent dans l'agrégat qui contient le volume.

Ce comportement se produit quel que soit le paramètre de croissance automatique sur la destination. Vous ne pouvez ni limiter la croissance du volume ni empêcher ONTAP de l'augmenter.

Par défaut, les volumes de protection des données sont définis sur le `grow_shrink` le mode `autosize`, qui permet au volume d'augmenter ou de diminuer en réponse à la quantité d'espace utilisé. La taille automatique max. Des volumes de protection des données est égale à la taille maximale des FlexVol et dépend de la plateforme. Par exemple :

- FAS8200, volume DP par défaut max. Par auto = 100 To

Pour plus d'informations, voir ["NetApp Hardware Universe"](#).

Découvrez la protection des données ONTAP « Fan-Out » et les déploiements en cascade

Vous pouvez utiliser un déploiement *Fan-Out* pour étendre la protection des données à plusieurs systèmes secondaires. Vous pouvez utiliser un déploiement *cascade* pour étendre la protection des données aux systèmes tertiaires.

Les déploiements « Fan-Out » et « Cascade » prennent en charge toutes les combinaisons de SnapMirror DR, de SnapVault ou de réplication unifiée. Depuis la version ONTAP 9.5, les relations synchrones SnapMirror prennent en charge les déploiements « Fan-Out » avec une ou plusieurs relations SnapMirror asynchrones. Une seule relation de la configuration « Fan-Out » peut être une relation synchrone SnapMirror ; toutes les autres relations du volume source doivent être des relations SnapMirror asynchrones. Les relations synchrones SnapMirror prennent également en charge les déploiements en cascade (à partir de ONTAP 9.6). Toutefois, la relation depuis le volume de destination de la relation synchrone SnapMirror doit être une relation asynchrone SnapMirror. [Synchronisation active SnapMirror](#) (Pris en charge à partir de ONTAP 9.13.1) prend également en charge les configurations « Fan-Out ».



Vous pouvez utiliser un déploiement *Fan-In* pour créer des relations de protection des données entre plusieurs systèmes primaires et un seul système secondaire. Chaque relation doit utiliser un volume différent sur le système secondaire.

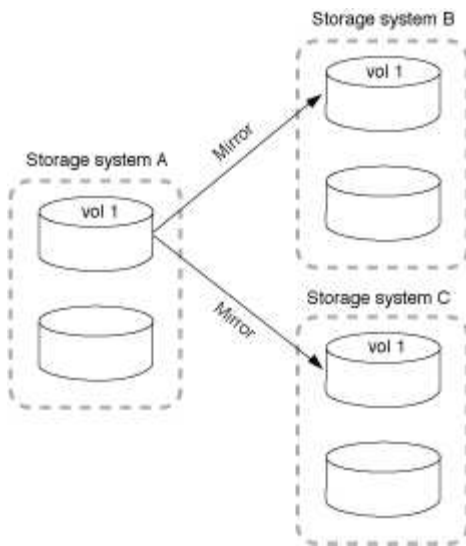


Sachez que les volumes faisant partie d'une configuration en cascade ou en « Fan-Out » peuvent prendre plus de temps resynchroniser. Il n'est pas rare d'avoir accès aux rapports de relation SnapMirror l'état « préparation » pour une période prolongée.

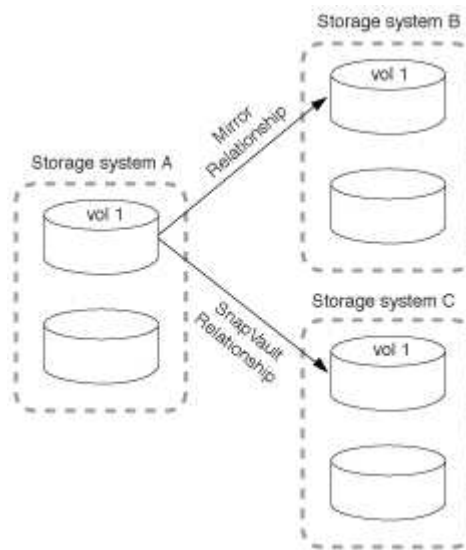
Fonctionnement des déploiements « Fan-Out »

SnapMirror prend en charge les déploiements *plusieurs-miroirs* et *mirror-vault* Fan-Out.

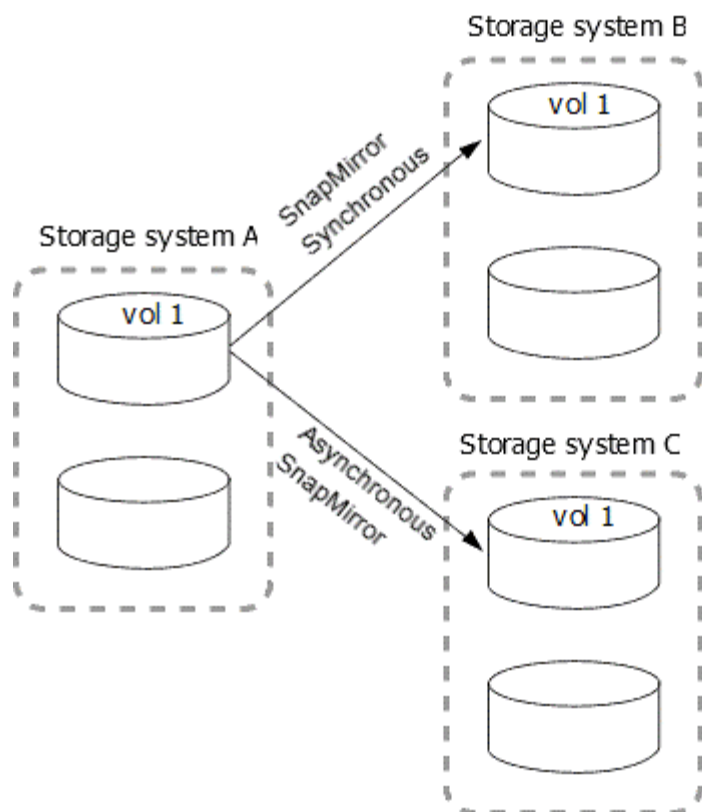
Un déploiement à plusieurs miroirs multiples sur « Fan-Out » comprend un volume source possédant une relation de mise en miroir sur plusieurs volumes secondaires.



Le déploiement de « fan-out » en miroir-coffre-fort consiste en un volume source avec une relation de miroir vers un volume secondaire et une relation SnapVault vers un autre volume secondaire.



À partir de ONTAP 9.5, vous pouvez avoir des déploiements « Fan-Out » avec des relations SnapMirror synchrones. Cependant, une seule relation de la configuration « Fan-Out » peut être une relation SnapMirror synchrone, toutes les autres relations du volume source doivent être des relations SnapMirror asynchrones.



Fonctionnement des déploiements en cascade

SnapMirror prend en charge les déploiements *mirror-mirror*, *mirror-vault*, *vault-mirror* et *vault-vault* cascade.

Le déploiement en cascade de mise en miroir consiste en une chaîne de relations dans laquelle un volume source est mis en miroir sur un volume secondaire, et le volume secondaire est mis en miroir sur un volume tertiaire. Si le volume secondaire n'est plus disponible, vous pouvez synchroniser la relation entre les volumes primaire et tertiaire sans effectuer de nouveau transfert de base.

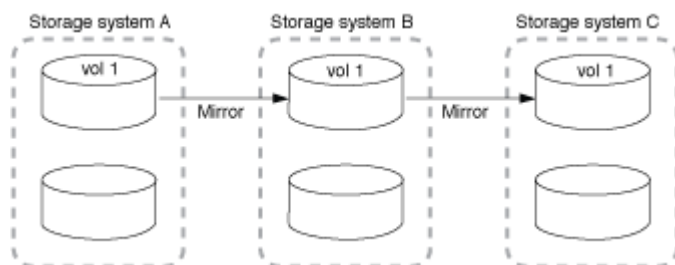
Dans une relation de volumes en cascade, les instantanés de conservation à long terme ne sont pris en charge que sur le volume de destination SnapMirror final de la cascade dans toutes les versions d'ONTAP 9. L'activation des instantanés de conservation à long terme sur n'importe quel volume intermédiaire de la cascade entraîne la perte de sauvegardes et d'instantanés. Si vous utilisez une configuration non prise en charge dans laquelle les instantanés de conservation à long terme sont activés sur un volume intermédiaire d'une cascade, contactez le support technique et indiquez la documentation correspondante. ["Base de connaissances NetApp : la mise en cascade d'un volume avec des snapshots de rétention à long terme \(LTR\) activés n'est pas prise en charge."](#) pour obtenir de l'aide.

Les versions ONTAP suivantes ne vous permettent pas d'activer les instantanés de conservation à long terme sur un volume quelconque dans une cascade, à l'exception du volume de destination final SnapMirror .

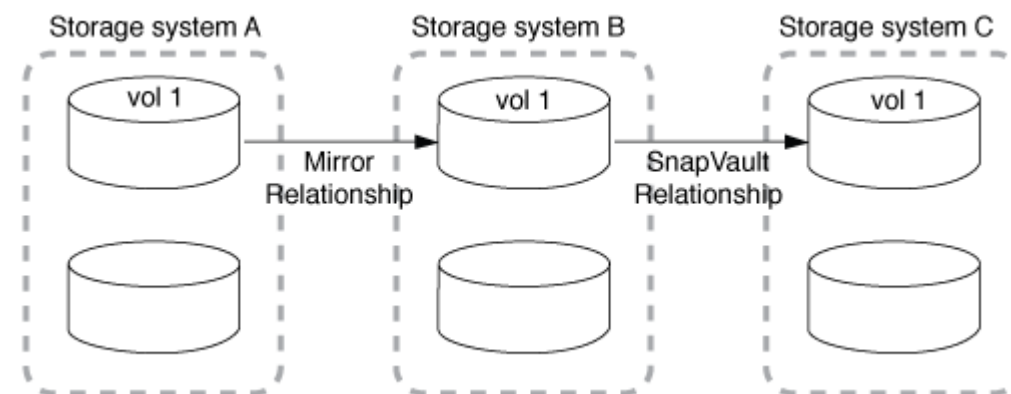
- 9.15.1 et versions ultérieures
- 9.14.1P2 et P4 à P14
- 9.13.1P9 à P17
- 9.12.1 P12 à P19
- 9.11.1P15 à P20
- 9.10.1P18 à P20

En savoir plus sur ["instantanés de rétention à long terme"](#) .

Depuis ONTAP 9.6, les relations SnapMirror synchrones sont prises en charge dans un déploiement en cascade miroir-miroir. Seuls les volumes principaux et secondaires peuvent se trouver dans une relation synchrone SnapMirror. La relation entre les volumes secondaires et les volumes tertiaires doit être asynchrone.



Le déploiement de la mise en miroir à distance en cascade consiste en une chaîne de relations dans laquelle le volume source est mis en miroir sur un volume secondaire, et le volume secondaire est copié sur un volume tertiaire.



Les déploiements en cascade Vault-miroir et Vault-Vault sont également pris en charge :

- Le déploiement de la mise en miroir en cascade de l'espace de stockage comprend une chaîne de relations dans laquelle le volume source est copié sur un volume secondaire et le volume secondaire est mis en miroir sur un volume tertiaire.
- Un déploiement en cascade vault-vault consiste en une chaîne de relations dans laquelle un volume source est voûté vers un volume secondaire, et le volume secondaire est voûté vers un volume tertiaire.

Informations associées

- [Reprenez la protection dans une configuration « Fan-Out » avec la synchronisation active SnapMirror](#)

En savoir plus sur les licences ONTAP SnapMirror

Depuis ONTAP 9.3, la licence a été simplifiée pour la réplication entre les instances ONTAP. Dans les versions de ONTAP 9, la licence SnapMirror prend en charge les relations d'archivage sécurisé et en miroir. Vous pouvez utiliser une licence SnapMirror pour prendre en charge la réplication ONTAP, aussi bien pour la sauvegarde que pour la reprise après incident.

Avant la version ONTAP 9.3, une licence SnapVault distincte était nécessaire pour configurer les relations *vault* entre les instances ONTAP, où l'instance DP pouvait conserver un nombre plus élevé de snapshots pour prendre en charge les cas d'utilisation de sauvegarde avec des durées de conservation plus longues, et une licence SnapMirror était nécessaire pour configurer les relations *mirror* entre les instances ONTAP, où chaque instance ONTAP conservera le même nombre de snapshots (c'est-à-dire qu'une image de cluster_ pouvait utiliser des basculements de reprise d'incident). Les licences SnapMirror et SnapVault sont toujours utilisées et prises en charge pour les versions ONTAP 8.x et 9.x.

Les licences SnapVault continuent de fonctionner et sont prises en charge aussi bien pour les versions ONTAP 8.x que 9.x, mais la licence SnapMirror peut être utilisée à la place d'une licence SnapVault et peut être utilisée pour les configurations en miroir et en coffre-fort.

Pour la réplication asynchrone ONTAP, à partir de ONTAP 9.3, un moteur de réplication unifié unique est utilisé pour configurer les règles de mode de protection étendue des données (XDP), où la licence SnapMirror peut être configurée pour une règle de miroir, une règle de copie à distance ou une règle de copie miroir-coffre. Une licence SnapMirror est requise sur les clusters source et de destination. Une licence SnapVault n'est pas requise si une licence SnapMirror est déjà installée. La licence perpétuelle asynchrone SnapMirror est incluse dans la suite logicielle ONTAP One installée sur les nouveaux systèmes AFF et FAS.

Les limites de configuration de la protection des données sont déterminées à l'aide de plusieurs facteurs, notamment la version de ONTAP, la plateforme matérielle et les licences installées. Pour plus d'informations, voir "[Hardware Universe](#)".

Licence synchrone SnapMirror

Depuis ONTAP 9.5, les relations SnapMirror synchrones sont prises en charge. Pour créer une relation synchrone SnapMirror, vous avez besoin des licences suivantes :

- La licence synchrone SnapMirror est requise à la fois sur le cluster source et sur le cluster destination.

La licence synchrone SnapMirror fait partie du "[Suite de licences ONTAP One](#)".

Si votre système a été acheté avant juin 2019 avec un bundle Premium ou Flash, vous pouvez télécharger une clé principale NetApp pour obtenir la licence synchrone SnapMirror requise sur le site de support NetApp : "[Clés de licence maîtresse](#)".

- La licence SnapMirror est requise sur le cluster source et le cluster cible.

Licence cloud SnapMirror

Depuis ONTAP 9.8, la licence cloud SnapMirror assure la réplication asynchrone des copies Snapshot entre des instances ONTAP et des terminaux de stockage objet. Les cibles de réplication peuvent être configurées à la fois via des magasins d'objets sur site et des services de stockage objet dans le cloud public compatibles S3 et S3. Les relations cloud SnapMirror sont prises en charge par les systèmes ONTAP vers les cibles de stockage objet préqualifiées.

SnapMirror Cloud n'est pas disponible en tant que licence autonome. Une seule licence est requise par cluster ONTAP. Outre une licence cloud SnapMirror, la licence asynchrone SnapMirror est également requise.

Pour créer une relation cloud avec SnapMirror, vous avez besoin des licences suivantes :

- Licence SnapMirror et licence cloud SnapMirror pour la réplication directe sur le terminal du magasin d'objets.
- Lors de la configuration d'un workflow de réplication à règles multiples (par exemple, disque à disque à

cloud), une licence SnapMirror est requise sur toutes les instances ONTAP, tandis que la licence cloud SnapMirror est uniquement requise pour le cluster source qui réplique directement sur le terminal de stockage objet.

À partir d' ONTAP 9.9.1, vous pouvez ["Utilisez System Manager pour la réplication cloud SnapMirror"](#) .

La liste des applications tierces cloud SnapMirror autorisées est publiée sur le site Web de NetApp.

Licence optimisée pour Data protection

Les licences DPO (Data protection Optimized) ne sont plus vendues et DPO n'est pas pris en charge sur les plates-formes actuelles. Cependant, si vous disposez d'une licence DPO installée sur une plate-forme prise en charge, NetApp continue à fournir le support jusqu'à la fin de la disponibilité de cette plate-forme.

DPO n'est pas inclus avec le pack de licences ONTAP One et vous ne pouvez pas mettre à niveau vers le pack de licences ONTAP One si la licence DPO est installée sur un système.

Pour plus d'informations sur les plates-formes prises en charge, voir ["Hardware Universe"](#).

Les systèmes DPO de ONTAP offrent des améliorations

Depuis ONTAP 9.6, le nombre maximal de volumes FlexVol pris en charge augmente lorsque la licence DP_Optimized (DPO) est installée. Depuis ONTAP 9.4, les systèmes dotés d'une licence DPO prennent en charge la fonctionnalité SnapMirror Backoff, la déduplication en arrière-plan entre les volumes, l'utilisation de blocs Snapshot comme donneurs et la compaction.

Depuis ONTAP 9.6, le nombre maximal de volumes FlexVol pris en charge sur les systèmes de protection des données ou secondaires a augmenté pour vous permettre de monter jusqu'à 2,500 volumes FlexVol par nœud ou jusqu'à 5,000 en mode de basculement. L'augmentation des volumes FlexVol est activée avec ["Licence DP_Optimized \(DPO\)"](#). Un ["Licence SnapMirror"](#) est toujours requis sur les nœuds source et de destination.

À partir de ONTAP 9.4, les fonctions suivantes sont améliorées pour les systèmes DPO :

- Retour arrière SnapMirror : dans les systèmes DPO, le trafic de réplication se voit attribuer la même priorité que les charges de travail client.

La désactivation de la sauvegarde SnapMirror est désactivée par défaut sur les systèmes DPO.

- La déduplication en arrière-plan des volumes et la déduplication en arrière-plan entre les volumes : la déduplication en arrière-plan des volumes et la déduplication en arrière-plan entre les volumes sont activées dans les systèmes DPO.

Vous pouvez exécuter le `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` commande de déduplication des données existantes. Il est recommandé d'exécuter la commande pendant les heures creuses afin de réduire l'impact sur les performances.

Pour en savoir plus, `storage aggregate efficiency cross-volume-dedupe start` consultez le ["Référence de commande ONTAP"](#).

- Gains d'espace grâce à l'utilisation de blocs Snapshot comme donneurs : les blocs de données qui ne sont pas disponibles dans le système de fichiers actif mais qui sont bloqués dans des snapshots sont utilisés

comme donneurs pour la déduplication des volumes.

Les nouvelles données peuvent être dédupliquées avec les données piégées dans les snapshots et partagées également avec efficacité les blocs de snapshot. L'espace accru réservé aux donneurs permet de réaliser davantage d'économies, en particulier lorsque le volume contient un grand nombre de snapshots.

- **Compaction** : la compaction des données est activée par défaut sur les volumes DPO.

En savoir plus sur la correspondance des motifs de nom de chemin dans les commandes ONTAP SnapMirror

Vous pouvez utiliser la correspondance de motif pour spécifier les chemins source et de destination dans `snapmirror` commandes.

```
`snapmirror` les commandes utilisent des noms de chemin complets au format
suivant : `vserver:volume`. Vous pouvez abréger le nom du chemin en
n'entrant pas le nom de la SVM. Si vous le faites, le `snapmirror`
Commande suppose le contexte SVM local de l'utilisateur.
```

En supposant que la SVM est appelée « `vserver1` » et que le volume est appelé « `vol1` », le chemin d'accès complet est `vserver1:vol1`.

Vous pouvez utiliser l'astérisque (*) dans les chemins comme caractère générique pour sélectionner des noms de chemin complets et correspondants. Le tableau suivant fournit des exemples d'utilisation du caractère générique pour sélectionner une plage de volumes.

<code>*</code>	Correspond à tous les chemins.
<code>vs*</code>	Correspondance de tous les SVM et volumes avec des noms de SVM commençant par <code>vs</code> .
<code>:*src</code>	Correspond à tous les SVM avec des noms de volume contenant le <code>src</code> texte.
<code>:vol</code>	Correspond à tous les SVM avec des noms de volume commençant par <code>vol</code> .

```
vs1::> snapmirror show -destination-path *:*dest*
```

Progress	Source	Destination	Mirror	Relationship	Total
Last	Path	Type Path	State	Status	Progress
Healthy	Updated				
-----	-----	-----	-----	-----	-----
-----	-----				
vs1:sm_src2		DP vs2:sm_dest1			
			Snapmirrored	Idle	-
true	-				

Pour en savoir plus, `snapmirror show` consultez le ["Référence de commande ONTAP"](#).

En savoir plus sur les requêtes étendues pour les opérations liées à ONTAP SnapMirror

Vous pouvez utiliser *requêtes étendues* pour effectuer des opérations SnapMirror simultanément sur de nombreuses relations SnapMirror. Par exemple, vous pouvez avoir plusieurs relations SnapMirror non initialisées que vous souhaitez initialiser à l'aide d'une commande.

Description de la tâche

Vous pouvez appliquer des requêtes étendues aux opérations SnapMirror suivantes :

- Initialisation des relations non initialisées
- Reprise des relations suspendues
- Resynchronisation des relations interrompues
- Mise à jour des relations inactives
- Abandon des transferts de données de relation

Étape

1. Effectuer une opération SnapMirror sur de nombreuses relations :

```
snapmirror command {-state state } *
```

La commande suivante initialise les relations SnapMirror qui se trouvent dans un Uninitialized état :

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

Pour en savoir plus, `snapmirror initialize` consultez le ["Référence de commande ONTAP"](#).

Compatibilité des versions ONTAP pour les relations SnapMirror

Les volumes source et destination doivent exécuter des versions ONTAP compatibles avant de créer une relation de protection des données SnapMirror. Avant de mettre à niveau ONTAP, vérifiez que votre version actuelle de ONTAP est compatible avec votre version cible de ONTAP pour les relations SnapMirror.

Relations de réplication unifiée

Pour les relations SnapMirror de type « XDP », utilisant des versions sur site ou Cloud Volumes ONTAP.

Depuis ONTAP 9.9 :

- Les versions ONTAP 9.x.0 sont des versions cloud uniquement et prennent en charge les systèmes Cloud Volumes ONTAP. L'astérisque (*) après la version de la version indique une version en nuage uniquement.



ONTAP 9.16.0 fait exception à la règle du cloud uniquement car il prend en charge :["Systèmes ASA r2"](#) . Le signe plus (+) après le numéro de version indique une version compatible à la fois avec ASA r2 et le cloud. Les systèmes ASA r2 prennent en charge les relations SnapMirror uniquement avec d'autres systèmes ASA r2.

- Les versions ONTAP 9.x.1 sont des versions générales qui prennent en charge à la fois les systèmes sur site et les systèmes Cloud Volumes ONTAP.



Lorsque ["équilibrage avancé de la capacité"](#) est activé sur les volumes des clusters exécutant ONTAP 9.16.1 ou version ultérieure, les transferts SnapMirror ne sont pas pris en charge sur les clusters exécutant des versions ONTAP antérieures à ONTAP 9.16.1.



L'interopérabilité est bidirectionnelle.

Interopérabilité pour ONTAP version 9.4 et ultérieures

Ver sio n ON TA P ...	Interopérabilité avec ces versions précédentes de ONTAP...																					
	9.1 8.1	9.1 7.1	9.1 6.1	9.1 6.0 +	9.1 5.1	9.1 5.0 *	9.1 4.1	9.1 4.0 *	9.1 3.1	9.1 3.0 *	9.1 2.1	9.1 2.0 *	9.1 1.1	9.1 1.0 *	9.1 0.1	9.1 0.0 *	9.9 .1	9.9 .0*	9.8	9.7	9.6	9.5
9.1 8.1	Ou i	Ou i	Ou i	Ou i	Ou i	No n	Ou i	No n	Ou i	Ou i	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n
9.1 7.1	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n

9.6	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i
9.5	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	No n	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i	Ou i

Relations synchrones SnapMirror



SnapMirror synchrone n'est pas pris en charge par les instances de cloud ONTAP.

Versi on ONTA P...	Interopérabilité avec ces versions précédentes de ONTAP...													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.18.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non
9.17.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Non
9.16.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non
9.15.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non
9.14.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
9.13.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.12.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.11.1	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non
9.10.1	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
9.9.1	Non	Non	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
9.8	Non	Non	Non	Non	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Non
9.7	Non	Non	Non	Non	Non	Oui	Oui	Non	Non	Oui	Oui	Oui	Oui	Oui
9.6	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui	Oui
9.5	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui

Relations de reprise d'activité SVM SnapMirror



- Cette matrice s'applique à la fonctionnalité de migration de données SVM à partir d' ONTAP 9.10.1.
- Vous pouvez utiliser SVM DR pour migrer une SVM qui ne répond pas aux restrictions indiquées pour "[Migration SVM \(mobilité des données SVM\)](#)".
- Dans les deux cas, un maximum de 2 versions majeures **plus récentes** ONTAP peuvent séparer les clusters source et de destination, à condition que la destination soit de la même version ou plus récente que la version ONTAP source.

Pour les données de reprise d'activité SVM et la protection des SVM :

La reprise d'activité SVM n'est prise en charge qu'entre les clusters exécutant la même version d'ONTAP.

L'indépendance de la version n'est pas prise en charge pour la réplication du SVM.

Pour la reprise d'activité de SVM pour la migration de SVM :

- La réplication est prise en charge dans une direction unique depuis une version antérieure de ONTAP sur la source vers la même version ou une version ultérieure de ONTAP sur la destination.
- La version ONTAP du cluster cible ne doit pas être plus de deux versions majeures sur site plus récentes ou deux versions majeures de cloud plus récentes (à partir de ONTAP 9.9.0), comme illustré dans le tableau ci-dessous.
 - La réplication n'est pas prise en charge pour les cas d'usage de protection des données à long terme.

L'astérisque (*) après la version de la version indique une version en nuage uniquement.

Pour déterminer la prise en charge, recherchez la version source dans la colonne de gauche du tableau, puis recherchez la version de destination sur la ligne supérieure (DR/migration pour les versions similaires et migration uniquement pour les versions plus récentes).



Si vous utilisez ONTAP 9.10.1 ou une version ultérieure, vous pouvez utiliser "[Mobilité des données des SVM](#)" une fonctionnalité alternative à SVM DR pour migrer les SVM d'un cluster à un autre.

Source	Destination																					
	9.5	9.6	9.7	9.8	9.9 .0*	9.9 .1	9.1 0.0 *	9.1 0.1	9.1 1.0 *	9.1 1.1	9.1 2.0 *	9.1 2.1	9.1 3.0 *	9.1 3.1	9.1 4.0 *	9.1 4.1	9.1 5.0 *	9.1 5.1	9.1 6.0	9.1 6.1	9.1 7.1	9.1 8.1
9.5	Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on																			
9.6		Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on																		

9.7			Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on															
9.8				Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on		Mig rati on												
9.9 .0*					Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on											
9.9 .1						Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on										
9.1 0.0 *							Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on								

9.1 0.1							Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on									
9.1 1.0 *							Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on								
9.1 1.1								Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on								
9.1 2.0 *									Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on						
9.1 2.1										Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on						

9.1 3.0 *												Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on				
9.1 3.1												Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on					
9.1 4.0 *													Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on		
9.1 4.1														Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on		
9.1 5.0 *															Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	Mig rati on	

9.1 5.1																		Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	
9.1 6.0																		Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	Mig rati on	
9.1 6.1																			Re pris e sur inci de nt/ mig rati on	Mig rati on	Mig rati on	
9.1 7.1																				Re pris e sur inci de nt/ mig rati on	Mig rati on	
9.1 8.1																					Re pris e sur inci de nt/ mig rati on	

Relations de reprise sur incident SnapMirror

Pour les relations SnapMirror de type « DP » et de type de règle « asynchrone-mirror » :



Les miroirs de type DP ne peuvent pas être initialisés depuis ONTAP 9.11.1 et sont complètement obsolètes dans ONTAP 9.12.1. Pour plus d'informations, voir "[Dérecation des relations SnapMirror de protection des données](#)".



Dans le tableau suivant, la colonne de gauche indique la version ONTAP sur le volume source, et la ligne supérieure indique les versions ONTAP que vous pouvez avoir sur le volume de destination.

Source	Destination								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	Oui.	Non	Non	Non	Non	Non	Non	Non	Non
9.10.1	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non
9.9.1	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non
9.8	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non
9.7	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non
9.6	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non
9.5	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non
9.4	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non
9.3	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.



L'interopérabilité n'est pas bidirectionnelle.

Découvrez les limites de ONTAP SnapMirror

Avant de créer une relation de protection des données, il est recommandé de connaître les limites élémentaires de SnapMirror.

- Un volume de destination ne peut avoir qu'un seul volume source.



Un volume source peut avoir plusieurs volumes de destination. Le volume de destination peut être le volume source pour tout type de relation de réplication SnapMirror.

- Selon le modèle de baie, vous pouvez ventiler jusqu'à huit ou seize volumes de destination à partir d'un seul volume source. Voir la "[Hardware Universe](#)" pour en savoir plus sur votre configuration spécifique.
- Vous ne pouvez pas restaurer de fichiers vers la destination d'une relation SnapMirror DR.
- Les volumes SnapVault source ou de destination ne peuvent pas être de 32 bits.
- Le volume source d'une relation SnapVault ne doit pas être un volume FlexClone.



La relation fonctionnera, mais l'efficacité offerte par les volumes FlexClone ne sera pas préservée.

Informations sur le copyright

Copyright © 2026 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.