Réplication de volume SnapMirror

ONTAP 9

NetApp
April 24, 2024

Sommaire

Réplication de volume SnapMirror

Principes de base de la reprise sur incident asynchrone 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.

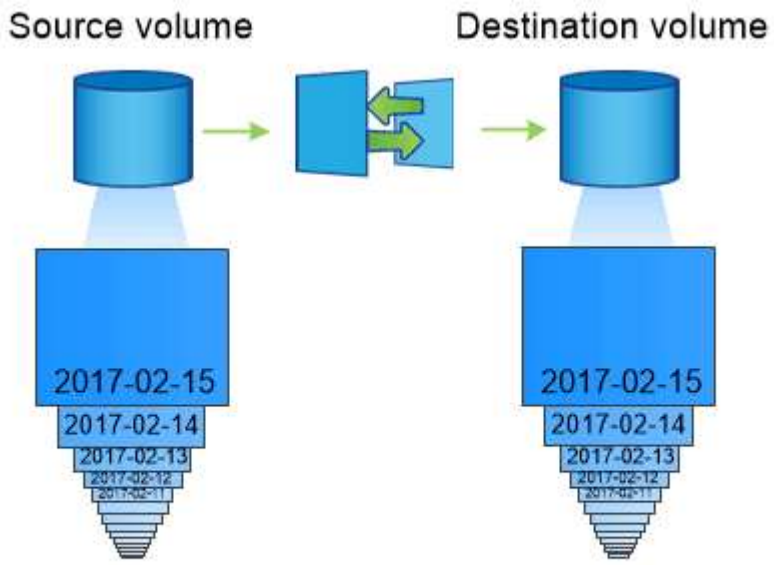
Si le site primaire assure toujours le service des données, il vous suffit de transférer les données requises vers celui-ci et ne transmet plus le tout aux clients depuis le miroir. Comme l'indique le cas de basculement, les contrôleurs du système secondaire doivent être équivalents ou presque équivalents 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 *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.

"Cluster et SVM peering"

La figure ci-dessous 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"

- Depuis la version ONTAP 9.13.1, vous pouvez utiliser la réplication asynchrone SnapMirror pour la protection groupes de cohérence. Depuis la version ONTAP 9.14.1, vous pouvez utiliser la réplication asynchrone SnapMirror pour répliquer des copies Snapshot 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 SnapMirror asynchrone.

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 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 ».

Mise à jour des relations de protection des données SnapMirror

Les mises à jour sont asynchrones, en fonction du planning que vous configurez. La conservation met en miroir la règle Snapshot sur la source.

À chaque mise à jour sous `MirrorAllSnapshots` SnapMirror crée une copie Snapshot du volume source, et transfère cette copie Snapshot ainsi que toutes les copies Snapshot qui ont été effectuées depuis la dernière mise à jour. Dans la sortie suivante du `snapmirror policy show` commande pour le `MirrorAllSnapshots` notez la règle suivante :

- `Create Snapshot` est « vrai », ce qui indique cela `MirrorAllSnapshots` Crée une copie Snapshot lorsque SnapMirror met à jour la relation.
- `MirrorAllSnapshots` Possède des règles « m_created » et « All_source_snapshots », ce qui indique que la copie Snapshot créée par SnapMirror et toutes les copies Snapshot effectuées depuis la dernière mise à jour sont transférées 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: Asynchronous SnapMirror 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

Le préconfiguré `MirrorLatest` la politique fonctionne exactement de la même manière que `MirrorAllSnapshots`, Sauf que seule la copie Snapshot créée par SnapMirror est transférée à l'initialisation et à la mise à jour.

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

Principes de base de la reprise après incident synchrone de SnapMirror

Depuis la version 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 SnapMirror synchrone est une fonctionnalité sous licence par nœud qui permet la réplication synchrone des données au niveau du volume.

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 SnapMirror synchrones 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 synchrone autorisées par paire HA en fonction du type de plateforme et de la version ONTAP.

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

Fonctionnalités prises en charge

Le tableau suivant présente 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 SnapMirror synchrone	ONTAP 9.6	

Réplication de copie Snapshot créée par les applications	ONTAP 9.7	Si une copie Snapshot est étiquetée avec l'étiquette appropriée au moment du `snapshot create` Par ailleurs, lors de l'utilisation de l'interface de ligne de commandes ou de l'API ONTAP, SnapMirror synchrone réplique les copies Snapshot, créées par l'utilisateur ou créées avec des scripts externes, après la suspension des applications. Les copies Snapshot planifiées créées à l'aide d'une règle Snapshot ne sont pas répliquées. Pour plus d'informations sur la réplication de copies Snapshot créées par les applications, consultez l'article de la base de connaissances : "Réplication des copies Snapshot créées par les applications 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 SnapMirror synchrone.	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 SnapMirror synchrone	ONTAP 9.6	
Quotas matériels et conditionnels sur le volume principal de la relation SnapMirror synchrone	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 contribuent à la limite globale de simultanées Relations par paire haute disponibilité.
ISCSI	ONTAP 9.5	
Clones de LUN et clones d'espace de noms NVMe	ONTAP 9.7	
Clones LUN sauvegardés par des copies Snapshot créées 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.
Opérations SnapMirror synchrones sans interruption (NDO) 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 v4.3	ONTAP 9.5	
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	
SnapMirror Synchronous mirror-mirror cascade	ONTAP 9.6	La relation à partir du volume de destination de la relation SnapMirror synchrone doit être une relation SnapMirror asynchrone.

Reprise d'activité de SVM	ONTAP 9.6	* Une source SnapMirror synchrone peut également être une source de reprise d'activité SVM, par exemple une configuration « Fan-Out » avec SnapMirror synchrone comme une étape et la reprise d'activité SVM comme l'autre. * Une source SnapMirror synchrone ne peut pas être une destination de reprise d'activité SVM, car SnapMirror synchrone ne prend pas en charge la mise en cascade 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 SnapMirror synchrone ne peut pas être une source de reprise d'activité de SVM, car la reprise d'activité de 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 :

- Groupes de cohérence
- Systèmes DP_optimisés (DPO)
- Volumes FlexGroup
- Volumes FlexCache
- Limitation globale
- Dans une configuration « Fan-Out », seule une relation peut être une relation SnapMirror synchrone ; 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

- Copies Snapshot 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 règle SnapMirror utilisée :

- **Mode de synchronisation**
  En mode synchrone, les opérations d'E/S de l'application sont envoyées en parallèle au primaire et au secondaire
  systèmes de stockage netapp fas. 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. Lorsque l'erreur est résolue, la technologie SnapMirror synchrone se resynchronise automatiquement sur le système de stockage secondaire et reprend la réplication du stockage primaire sur 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.
- **Mode StrictSync**
  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 système primaire sont reprendre uniquement après le retour de la relation SnapMirror dans `InSync` état. 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 SnapMirror synchrone est toujours dans le `InSync` état pendant le fonctionnement normal. Si le transfert SnapMirror échoue, quelle qu'en soit la raison, la destination n'est pas en synchronisation avec la source et peut être transférée vers le système `OutofSync` état.

Pour les relations SnapMirror synchrones, le système vérifie automatiquement l'état de la relation `InSync` ou `OutofSync`) à intervalle fixe. Si le statut 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 pas déclencher une resynchronisation automatique.

Si le statut de la relation devient `OutofSync` Dans le cas d'une relation SnapMirror synchrone en mode StrictSync, toutes les opérations d'E/S vers le volume primaire sont arrêtées. Le `OutofSync` État de la relation SnapMirror synchrone en mode synchrone n'engendre pas d'interruption des opérations d'E/S primaires et du volume primaire.

Informations associées

"Rapport technique NetApp 4733 : configuration synchrone et bonnes pratiques pour SnapMirror"

À propos des workloads pris en charge par les règles de synchronisation et de synchronisation StrictSync

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. Depuis la version ONTAP 9.6, SnapMirror synchrone peut être utilisé pour les services de fichiers d'entreprise, tels que l'EDA, les répertoires locaux et les workloads de développement logiciel.

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 limites sont supprimées, et SnapMirror synchrone peut être utilisé pour les workloads de services de fichiers d'entreprise incluant des environnements multiutilisateurs, tels que les répertoires locaux et les workloads de développement logiciel.

Informations associées

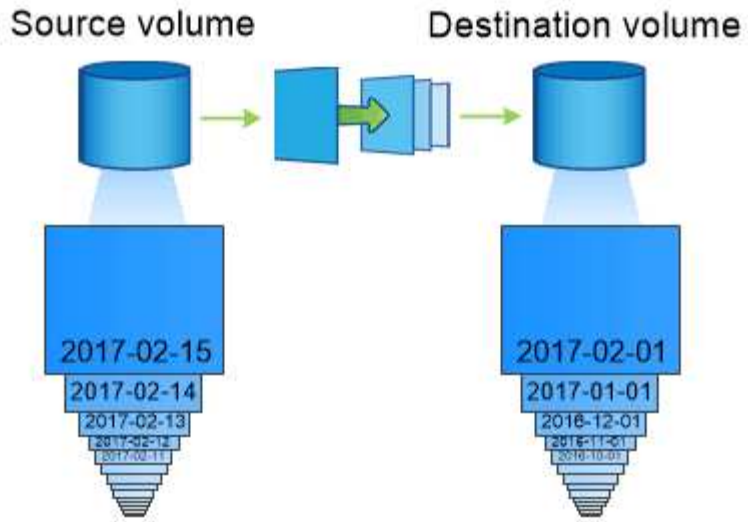
"Configuration synchrone de SnapMirror et bonnes pratiques"

Archivage à distance grâce à la technologie 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 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 d'une copie à distance 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.

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.

Transfert de base sous la stratégie de coffre-fort par défaut `XDPDefault` Crée une copie Snapshot du volume source, puis transfère cette copie et les blocs de données qu'il renvoie vers le volume de destination. Contrairement aux relations SnapMirror, une sauvegarde forte n'inclut pas d'anciennes copies Snapshot 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 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.

À chaque mise à jour sous `XDPDefault` Cette règle transfère les copies Snapshot qui ont été effectuées depuis la dernière mise à jour, à condition que leurs étiquettes correspondent aux étiquettes définies dans les règles de règle. Dans la sortie suivante du `snapmirror policy show` commande pour le `XDPDefault` notez la règle suivante :

- `Create Snapshot` est « faux », ce qui indique cela `XDPDefault` Ne crée pas de copie Snapshot lorsque SnapMirror met à jour la relation.
- `XDPDefault` Dispose de règles « diotidienne » et « hebdomadaire », ce qui indique que toutes les copies Snapshot avec des étiquettes correspondantes sur la source sont transférées 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 -
-
```

Notions de base sur la réplication unifiée 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'appelez. La règle SnapMirror pour la relation définit le contenu de la base et toutes les mises à jour.

Transfert de base avec la règle de protection des données unifiée par défaut `MirrorAndVault` Crée une copie Snapshot du volume source, puis transfère cette copie et les blocs de données qu'il renvoie vers le volume de destination. Tout comme l'archivage sécurisé, la protection unifiée des données n'inclut pas d'anciennes copies Snapshot de la ligne de base.

Mise à jour des relations de protection unifiée des données

À chaque mise à jour sous `MirrorAndVault` Règle : SnapMirror crée une copie Snapshot du volume source

et transfère la copie Snapshot ainsi que toutes les copies Snapshot créées depuis la dernière mise à jour, à condition que leurs étiquettes correspondent aux règles de règles Snapshot. Dans la sortie suivante du `snapmirror policy show` commande pour le `MirrorAndVault` notez la règle suivante :

- `Create Snapshot` est « vrai », ce qui indique cela `MirrorAndVault` Crée une copie Snapshot lorsque SnapMirror met à jour la relation.
- `MirrorAndVault` A règles « `sm_created', « diotidienne » et « hebdomadaire », ce qui indique que la copie Snapshot créée par SnapMirror et les copies Snapshot portant des étiquettes correspondantes sur la source sont transférées 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 Synchronous SnapMirror 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

Le préconfiguré `Unified7year` la politique fonctionne exactement de la même manière que `MirrorAndVault`, Sauf qu'une quatrième règle transfère les copies Snapshot mensuelles et les conserve pendant sept ans.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               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 la copie Snapshot créée par SnapMirror à l'initialisation. À chaque mise à jour, SnapMirror crée une autre copie Snapshot de la source et transfère cette copie Snapshot ainsi que toutes les nouvelles copies Snapshot dont les étiquettes correspondent aux règles définies dans les règles de règle Snapshot.

Vous pouvez vous protéger contre la possibilité de corruption d'une copie Snapshot mise à jour en créant une copie de la dernière copie Snapshot transférée sur le volume de destination. Cette « copie locale » est conservée indépendamment des règles de conservation à la source, de sorte que même si la copie Snapshot transférée à l'origine par SnapMirror n'est plus disponible sur la source, une copie de celle-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. Un miroir traditionnel peut mieux convenir à un volume qui contient des copies Snapshot horaires de journaux de transactions de base de données, par exemple.

XDP remplace DP par défaut SnapMirror

Depuis ONTAP 9.3, le mode SnapMirror Extended Data protection (XDP) remplace le mode SnapMirror Data protection (DP) par défaut.

Avant de mettre à niveau votre système vers ONTAP 9.12.1, vous devez convertir les relations de type DP en relation XDP avant de pouvoir procéder à une mise à niveau vers ONTAP 9.12.1 et versions ultérieures. Pour plus d'informations, voir "Convertir une relation de type DP existante en XDP".

Jusqu'à ONTAP 9.3, SnapMirror invoqué en mode DP et SnapMirror invoqué en mode XDP utilisait différents moteurs de réplication, avec différentes approches de la dépendance vis-à-vis de la version :

- SnapMirror appelé en mode DP utilisait un moteur de réplication *version-dépendante* dans lequel la

version de ONTAP était requise pour le stockage primaire et secondaire :

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror appelé en mode XDP utilisait un moteur de réplication *version-flexible* qui prenait en charge différentes versions ONTAP sur le stockage primaire et secondaire :

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Grâce aux améliorations des performances, les avantages significatifs de SnapMirror flexible à la version compensent légèrement l'avantage en termes de débit de réplication obtenu avec le mode dépendant de la version. C'est pour cette raison, depuis ONTAP 9.3, le mode XDP est devenu le nouveau paramètre par défaut et toutes les invocations du mode DP sur la ligne de commande ou dans les scripts nouveaux ou existants sont automatiquement converties en mode XDP.

Les relations existantes ne sont pas affectées. Si une relation est déjà de type DP, elle continuera d'être de type DP. Depuis ONTAP 9.5, MirrorAndVault est la nouvelle règle par défaut lorsqu'aucun mode de protection des données n'est spécifié ou lorsque le mode XDP est spécifié comme type de relation. Le tableau ci-dessous montre le comportement auquel vous pouvez vous attendre.

Si vous spécifiez…	Le type est…	La stratégie par défaut (si vous ne spécifiez pas de règle) est…
DP	XDP	MirrorAllsnapshots (reprise après incident SnapMirror)
Rien	XDP	MirrorAndVault (réplication unifiée)
XDP	XDP	MirrorAndVault (réplication unifiée)

Comme le tableau le montre, les règles par défaut attribuées à XDP dans différentes circonstances garantissent que la conversion conserve l'équivalence fonctionnelle des anciens types. Vous pouvez bien sûr utiliser différentes règles si nécessaire, y compris des règles pour la réplication unifiée :

Si vous spécifiez…	Et la politique est…	Résultat :
DP	MirrorAllsnapshots	Reprise sur incident SnapMirror
XDPDefault	SnapVault	MirrorAndVault
Réplication unifiée	XDP	MirrorAllsnapshots
Reprise sur incident SnapMirror	XDPDefault	SnapVault

Les seules exceptions à la conversion sont les suivantes :

- Les relations de protection des données de SVM continuent à être par défaut en mode DP dans ONTAP 9.3 et versions antérieures.

  Depuis ONTAP 9.4, les relations de protection des données du SVM sont définies par défaut en mode XDP

- Les relations de protection des données de partage de la charge du volume racine continuent à être par défaut en mode DP.
- Les relations de protection des données SnapLock continuent à être par défaut en mode DP dans ONTAP 9.4 et versions antérieures.

  Depuis ONTAP 9.5, les relations de protection des données SnapLock se servent par défaut du mode XDP.

- Les invocations explicites de DP continuent à être activées par défaut avec le mode DP si vous définissez l'option d'ensemble du cluster suivante :

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Cette option est ignorée si vous n'appelez pas explicitement DP.

Lorsqu'un volume de destination augmente automatiquement

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 :

- FAS6220, DP volume DP max-autosize par défaut = 70 To
- FAS8200, volume DP par défaut max. Par auto = 100 To

Pour plus d'informations, voir "NetApp Hardware Universe".

Déploiements de la protection des données en cascade et « Fan-Out »

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 n'importe quelle combinaison de reprise

après incident SnapMirror, d'SnapVault ou de réplication unifiée. Cependant, les relations SnapMirror synchrone (prises en charge à partir de ONTAP 9.5) prennent en charge uniquement les déploiements « Fan-Out » avec une ou plusieurs relations SnapMirror asynchrones, et ne prennent pas en charge les déploiements en cascade. Une seule relation dans la configuration « Fan-Out » peut être une relation SnapMirror synchrone, toutes les autres relations du volume source doivent être des relations SnapMirror asynchrones. Continuité de l'activité SnapMirror (Pris en charge depuis ONTAP 9.8) prend également en charge les configurations « Fan-Out ».

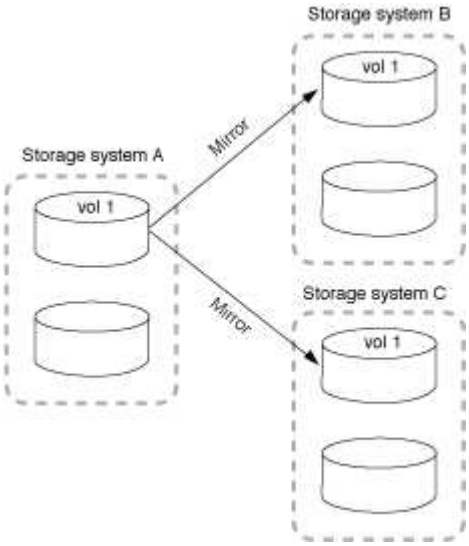
> Vous pouvez utiliser un déploiement *Fan-In* pour créer des relations de protection des données entre plusieurs systèmes primaires et un seul système secondaire. Chaque relation doit utiliser un volume différent sur le système secondaire.

> 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.

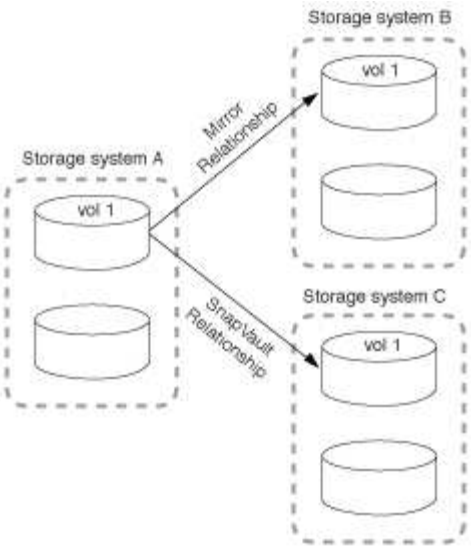
Fonctionnement des déploiements « Fan-Out »

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

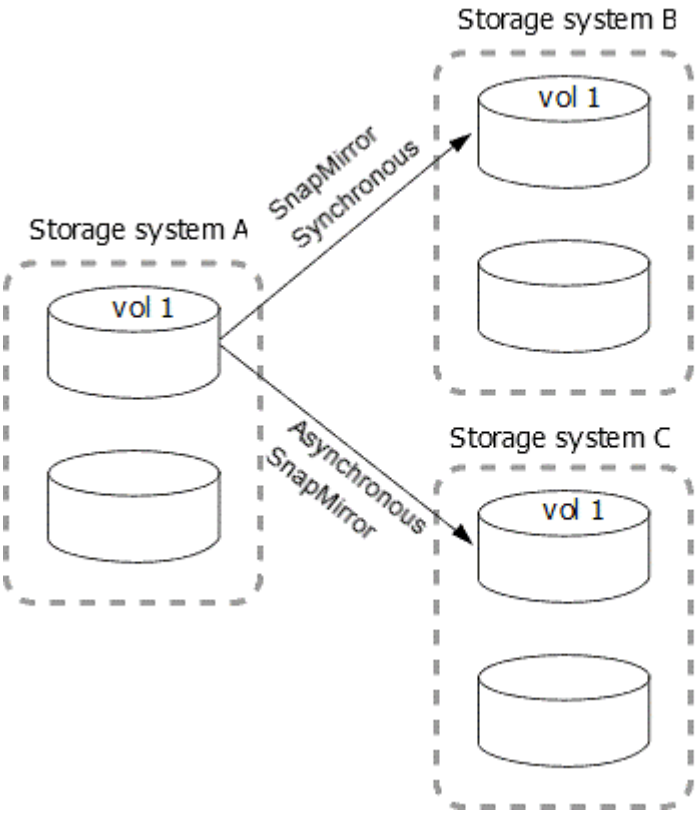
Un déploiement à plusieurs miroirs multiples sur « Fan-Out » comprend un volume source possédant une relation de mise en miroir sur plusieurs volumes secondaires.



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.



Depuis ONTAP 9.5, vous pouvez avoir déployé « Fan-Out » avec des relations SnapMirror synchrone. Cependant, seule une 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.

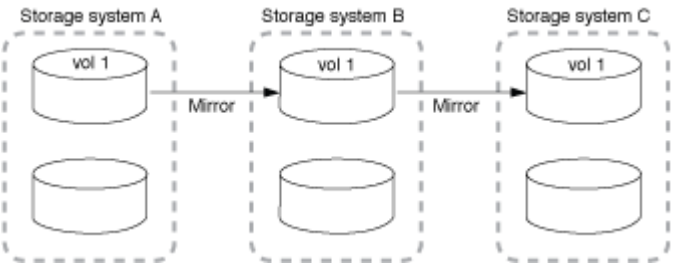


Fonctionnement des déploiements en cascade

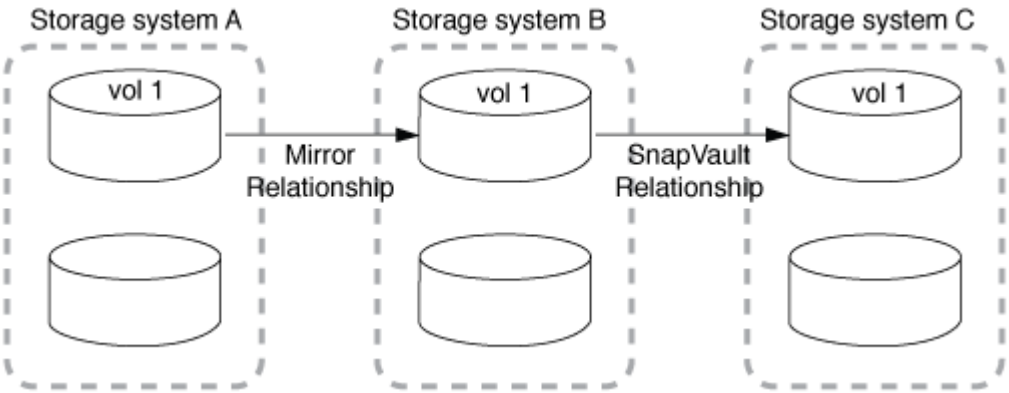
SnapMirror prend en charge les déploiements *mirror-mirror*, *mirror-vault*, *vault-mirror* et *vault-vault* cascade.

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.

Depuis ONTAP 9.6, les relations SnapMirror synchrone sont prises en charge dans un déploiement en cascade en miroir. Seuls les volumes primaires et secondaires peuvent être dans une relation SnapMirror synchrone. 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 vault-mirror et, depuis ONTAP 9.2, vault-vault-vault en cascade 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.
- (Depuis ONTAP 9.2), Le déploiement de coffre-fort en cascade consiste en une chaîne de relations dans laquelle un volume source est copié sur un volume secondaire, et le volume secondaire est copié sur un volume tertiaire.

Plus de lecture

- Reprendre la protection dans une configuration de « Fan-Out » avec SM-BC

Licences SnapMirror

Présentation des licences 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. L'instance DP pouvait conserver un nombre plus élevé de copies Snapshot pour prendre en charge les cas d'utilisation de sauvegarde avec des durées de conservation plus longues. une licence SnapMirror était nécessaire pour configurer les relations *mirror* entre les instances ONTAP, où chaque instance ONTAP devait conserver le même nombre de copies Snapshot (c'est-à-dire, une image *mirror*) pour prendre en charge les cas d'utilisation de reprise sur incident afin de permettre le basculement du cluster. 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 SnapMirror synchrone

La prise en charge des relations SnapMirror synchrone est prise en charge à partir de la version ONTAP 9.5 Vous avez besoin des licences suivantes pour créer une relation SnapMirror synchrone :

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

  La licence SnapMirror synchrone fait partie du "Suite de licences ONTAP One".

  Si votre système a été acheté avant le 2019 juin avec un bundle Premium ou Flash, vous pouvez télécharger une clé maître NetApp pour obtenir la licence SnapMirror synchrone 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 SnapMirror Cloud permet la réplication asynchrone des copies Snapshot à partir des instances ONTAP vers les 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 des 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 SnapMirror Cloud, la licence asynchrone SnapMirror est également requise.

Vous avez besoin des licences suivantes pour créer une relation de cloud SnapMirror :

- Licence SnapMirror et licence SnapMirror Cloud pour la réplication directe sur le terminal du magasin d'objets.

- Lors de la configuration d'un workflow de réplication multi-règles (par exemple, disque à disque à cloud), une licence SnapMirror est requise sur toutes les instances ONTAP, tandis que la licence SnapMirror Cloud n'est requise que pour le cluster source qui est répliqué directement vers le terminal de stockage objet.

À partir de ONTAP 9.9.1, vous pouvez "Utilisez System Manager pour la réplication SnapMirror Cloud".

Une liste des applications tierces SnapMirror Cloud 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".

Installez les licences SnapMirror Cloud

Les relations SnapMirror Cloud peuvent être orchestrées à l'aide d'applications de sauvegarde tierces préqualifiées. Depuis la version ONTAP 9.9.1, vous pouvez également utiliser System Manager pour orchestrer la réplication SnapMirror Cloud. Les licences de capacité SnapMirror et SnapMirror Cloud sont requises pour orchestrer la sauvegarde ONTAP sur site avec les sauvegardes de stockage objet à l'aide de System Manager. Vous devez également demander et installer la licence SnapMirror Cloud API.

Description de la tâche

Les licences SnapMirror Cloud et S3 SnapMirror sont des licences de cluster, et non des licences de nœud. Elles sont donc *non* fournies avec le bundle de licences ONTAP One. Ces licences sont incluses dans le pack de compatibilité ONTAP One distinct. Pour activer SnapMirror Cloud, vous devez demander ce pack.

En outre, l'orchestration par System Manager des sauvegardes SnapMirror Cloud sur le stockage objet nécessite une clé d'API SnapMirror Cloud. Cette licence d'API est une licence à instance unique au niveau du cluster, ce qui signifie qu'il n'est pas nécessaire de l'installer sur chaque nœud du cluster.

Étapes

Vous devez demander et télécharger le bundle de compatibilité ONTAP One et la licence de l'API cloud SnapMirror, puis les installer à l'aide de System Manager.

1. Recherchez et enregistrez l'UUID de cluster pour le cluster que vous souhaitez obtenir une licence.

   L'UUID de cluster est requis lorsque vous envoyez votre demande de commande du bundle ONTAP One Compatibility pour votre cluster.

2. Contactez votre équipe commerciale NetApp et demandez le pack compatibilité ONTAP One.
3. Demandez la licence d'API SnapMirror Cloud en suivant les instructions fournies sur le site du support NetApp.

   "Demandez la clé de licence de l'API SnapMirror Cloud"

4. Une fois que vous avez reçu et téléchargé les fichiers de licence, utilisez System Manager pour télécharger le fichier NLF ONTAP Cloud Compatibility et le fichier NLF SnapMirror Cloud API sur le cluster :
   a. Cliquez sur **Cluster > Paramètres**.
   b. Dans la fenêtre **Paramètres**, cliquez sur **licences**.
   c. Dans la fenêtre **licences**, cliquez sur + Add .
   d. Dans la boîte de dialogue **Ajouter une licence**, cliquez sur **Parcourir** pour sélectionner le fichier NLF que vous avez téléchargé, puis cliquez sur **Ajouter** pour télécharger le fichier sur le cluster.

Informations associées

"Sauvegardez les données dans le cloud avec SnapMirror"

"Recherche de licences logicielles NetApp"

Améliorations des fonctionnalités des systèmes DPO

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 des 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)". A "Licence SnapMirror" reste 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.

- Économies accrues grâce à l'utilisation des blocs Snapshot en tant que donneurs : les blocs de données non disponibles dans le système de fichiers actif, mais bloqués dans des copies Snapshot, sont utilisés comme donneurs pour la déduplication du volume.

  Les nouvelles données peuvent être dédupliquées avec les données piégées dans les copies Snapshot, ce qui est également le partage efficace des blocs Snapshot. L'augmentation de l'espace de donneurs permet de réaliser plus d'économies, notamment lorsque le volume possède un grand nombre de copies Snapshot.

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