Protection des données et reprise d'activité

ONTAP 9

NetApp
April 24, 2024

Sommaire

Protection des données et reprise d’activité

Protection des données avec System Manager

Présentation de la protection des données avec System Manager

Les sections de cette section expliquent comment configurer et gérer la protection des données avec System Manager dans ONTAP 9.7 et versions ultérieures.

Si vous utilisez System Manager avec ONTAP 9.7 ou une version antérieure, reportez-vous à la section "Documentation ONTAP System Manager Classic"

Protégez vos données en créant et en gérant des copies Snapshot, des miroirs, des coffres-forts et des relations entre miroir et archivage sécurisé.

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 un miroir de vos données de travail dans un système de stockage secondaire, à partir duquel vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.

Un *vault* est conçu pour la réplication de copies Snapshot disque à disque à des fins de conformité aux normes et de 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.

À partir de ONTAP 9.10.1, vous pouvez créer des relations de protection des données entre les compartiments S3 à l’aide de SnapMirror S3. Les compartiments de destination peuvent être sur les systèmes ONTAP locaux ou distants, ou sur les systèmes non ONTAP tels qu’StorageGRID et AWS. Pour plus d’informations, voir "Présentation de SnapMirror S3".

Création de règles personnalisées de protection des données

Vous pouvez créer des règles de protection des données personnalisées avec System Manager lorsque les règles de protection par défaut existantes ne sont pas adaptées à vos besoins. Depuis ONTAP 9.11.1, vous pouvez utiliser System Manager pour créer des stratégies de mise en miroir et de copie à distance personnalisées, pour afficher et sélectionner des règles existantes. Cette fonctionnalité est également disponible dans ONTAP 9.8P12 et versions ultérieures de ONTAP 9.8.

Créez des règles de protection personnalisées sur le cluster source et destination.

Étapes

1. Cliquez sur **protection > Paramètres de stratégie locale**.
2. Sous **protection Policies**, cliquez sur →.
3. Dans le volet **protection Policies**, cliquez sur + Add .
4. Entrez le nouveau nom de la stratégie et sélectionnez sa portée.
5. Choisissez un type de stratégie. Pour ajouter une stratégie de coffre-fort ou de miroir uniquement, choisissez **Asynchronous**, puis cliquez sur **utiliser un type de stratégie hérité**.

6. Renseignez les champs obligatoires.
7. Cliquez sur **Enregistrer**.
8. Répétez ces étapes sur l'autre cluster.

Configurez les copies Snapshot

Vous pouvez créer des règles de copie Snapshot afin de spécifier le nombre maximal de copies Snapshot automatiquement créées et la fréquence de leur création. La règle indique quand créer des copies Snapshot, le nombre de copies à conserver et comment les nommer.

Cette procédure crée une règle de copie Snapshot sur le cluster local uniquement.

Étapes

1. Cliquez sur **protection > Présentation > Paramètres de stratégie locale**.
2. Sous **stratégies Snapshot**, cliquez sur →, puis cliquez sur + Add .
3. Saisissez le nom de la stratégie, sélectionnez la portée de la stratégie et, sous **Schedules**, cliquez sur + Add pour saisir les détails de l'horaire.

Calculer l'espace récupérable avant de supprimer les copies Snapshot

Depuis la version ONTAP 9.10.1, vous pouvez utiliser System Manager pour sélectionner les copies Snapshot à supprimer et calculer l'espace récupérable avant de les supprimer.

Étapes

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez le volume depuis lequel vous souhaitez supprimer les copies Snapshot.
3. Cliquez sur **copies snapshot**.
4. Sélectionnez une ou plusieurs copies Snapshot.
5. Cliquez sur **calculer l'espace de récupération**.

Activez ou désactivez l'accès client au répertoire de copie Snapshot

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour activer ou désactiver les systèmes clients afin d'accéder à un répertoire de copies Snapshot sur un volume. L'activation de l'accès permet au répertoire de copies Snapshot de être visible par les clients et permet aux clients Windows de mapper un lecteur au répertoire des copies Snapshot pour afficher et accéder à son contenu.

Vous pouvez activer ou désactiver l'accès au répertoire de copie Snapshot d'un volume en modifiant les paramètres du volume ou en modifiant les paramètres de partage du volume.

Activez ou désactivez l'accès client au répertoire de copie Snapshot en modifiant un volume

Par défaut, le répertoire de copies Snapshot d'un volume est accessible aux clients.

Étapes

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez le volume contenant le répertoire des copies Snapshot que vous souhaitez afficher ou masquer.
3. Cliquez sur ⋮ Et sélectionnez **Modifier**.
4. Dans la section Paramètres* **copies snapshot (local), sélectionnez ou désélectionnez *Afficher le répertoire copies Snapshot sur les clients**.
5. Cliquez sur **Enregistrer**.

Activez ou désactivez l'accès client au répertoire de copie Snapshot en modifiant un partage

Par défaut, le répertoire de copies Snapshot d'un volume est accessible aux clients.

Étapes

1. Cliquez sur **stockage > partages**.
2. Sélectionnez le volume contenant le répertoire des copies Snapshot que vous souhaitez afficher ou masquer.
3. Cliquez sur ⋮ Et sélectionnez **Modifier**.
4. Dans la section **Share Properties**, sélectionnez ou désélectionnez **Allow clients to Access Snapshot copies Directory**.
5. Cliquez sur **Enregistrer**.

Préparez-vous à la mise en miroir et à l'archivage

Il est possible de protéger les données en les répliquant sur un cluster distant à des fins de sauvegarde des données et de reprise après incident.

Plusieurs stratégies de protection par défaut sont disponibles. Vous devez avoir créé vos stratégies de protection si vous souhaitez utiliser des stratégies personnalisées.

Étapes

1. Dans le cluster local, cliquez sur **protection > Présentation**.
2. Développez **Paramètres intercluster**. Cliquez sur **Ajouter des interfaces réseau** et ajoutez des interfaces réseau intercluster pour le cluster.

   Répétez cette étape sur le cluster distant.

3. Dans le cluster distant, cliquez sur **protection > Présentation**. Cliquez sur ⋮ Dans la section pairs de cluster, cliquez sur **générer la phrase de passe**.
4. Copiez la phrase secrète générée et collez-la dans le cluster local.
5. Dans le cluster local, sous pairs de cluster, cliquez sur **clusters homologues** et créez des clusters locaux

et distants.

6. Si vous le souhaitez, cliquez sur Storage VM pairs ⋮ Puis **Peer Storage VM** pour Peer les machines virtuelles de stockage.
7. Cliquez sur **Protect volumes** pour protéger vos volumes. Pour protéger vos LUN, cliquez sur **stockage > LUN**, sélectionnez une LUN à protéger, puis cliquez sur Protect.

   Sélectionnez la règle de protection en fonction du type de protection des données dont vous avez besoin.

8. Pour vérifier que les volumes et les LUN sont bien protégés du cluster local, cliquez sur **Storage > volumes** ou **Storage > LUNs** et développez la vue volume/LUN.

D'autres façons de le faire dans ONTAP

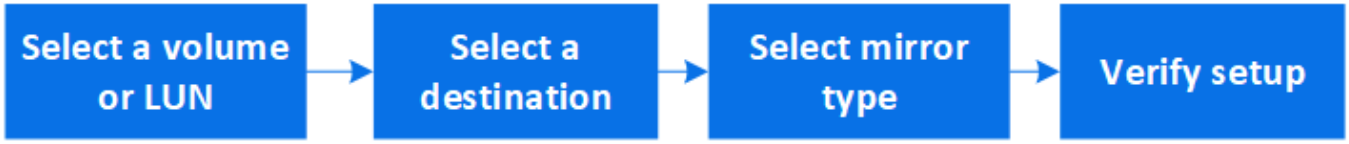
Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la préparation de la reprise sur incident de volume"
Interface de ligne de commande ONTAP	"Créer une relation entre clusters"

Configurer les miroirs et les coffres-forts

Créer une mise en miroir et un coffre-fort d'un volume afin de protéger les données en cas d'incident et d'avoir plusieurs versions archivées de données sur lesquelles vous pouvez restaurer. Depuis ONTAP 9.11.1, System Manager permet de sélectionner des règles de copie en miroir et de copie à distance prédéfinies et personnalisées, d'afficher et de sélectionner des règles existantes, et de remplacer les planifications de transfert définies dans une règle de protection lorsque les volumes et les machines virtuelles de stockage sont protégés. Cette fonctionnalité est également disponible dans ONTAP 9.8P12 et versions ultérieures de ONTAP 9.8.

> Si vous utilisez ONTAP 9.8P12 ou une version ultérieure de correctif ONTAP 9.8 et si vous avez configuré SnapMirror à l'aide de System Manager, vous devez utiliser ONTAP 9.9.1P13 ou version ultérieure et ONTAP 9.10.1P10 ou version ultérieure pour une mise à niveau vers ONTAP 9.9.1 ou ONTAP 9.10.1.

Cette procédure crée une règle de protection des données sur un cluster distant. Le cluster source et le cluster destination utilisent les interfaces réseau intercluster pour l'échange de données. La procédure suppose "les interfaces réseau intercluster sont créées et les clusters contenant les volumes sont associés" (apparié). Vous pouvez également Peer VM de stockage pour assurer la protection des données. Toutefois, si les machines virtuelles de stockage ne sont pas associées, mais que les autorisations sont activées, les machines virtuelles de stockage sont automatiquement créées lorsque la relation de protection est créée.



Étapes

1. Sélectionnez le volume ou le LUN à protéger : cliquez sur **Storage > volumes** ou **Storage > LUN**, puis cliquez sur le nom de volume ou de LUN souhaité.

2. Cliquez sur Protect.
3. Sélectionnez le cluster de destination et la VM de stockage.
4. La règle asynchrone est sélectionnée par défaut. Pour sélectionner une stratégie synchrone, cliquez sur **plus d'options**.
5. Cliquez sur **protéger**.
6. Cliquez sur l'onglet **SnapMirror (local ou Remote)** du volume ou du LUN sélectionné pour vérifier que la protection est correctement configurée.

Informations associées

- "Créez et supprimez des volumes de test de basculement SnapMirror".

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la sauvegarde de volume avec SnapVault"
Interface de ligne de commande ONTAP	"Créer une relation de réplication"

Resynchroniser une relation de protection

Lorsque votre volume source d'origine est de nouveau disponible après une catastrophe, vous pouvez resynchroniser les données depuis le volume de destination et rétablir la relation de protection.

Cette procédure remplace les données du volume source d'origine par une relation asynchrone. Vous pouvez ainsi reprendre le service des données du volume source d'origine et reprendre la relation de protection d'origine.

Étapes

1. Cliquez sur **protection > relations**, puis cliquez sur la relation rompue que vous souhaitez resynchroniser.
2. Cliquez sur ⋮ Puis sélectionnez **Resync**.
3. Sous **relations**, surveiller la progression de la resynchronisation en vérifiant l'état de la relation. L'état est modifié en « mis en miroir » une fois la resynchronisation terminée.

Restaurez un volume à partir d'une copie Snapshot antérieure

Lorsque les données d'un volume sont perdues ou corrompues, vous pouvez restaurer les données à partir d'une copie Snapshot antérieure.

Cette procédure remplace les données actuelles sur le volume source par des données issues d'une version antérieure de la copie Snapshot. Vous devez effectuer cette tâche sur le cluster de destination.

Étapes

1. Cliquez sur **protection > relations**, puis sur le nom du volume source.
2. Cliquez sur ⋮ Puis sélectionnez **Restaurer**.
3. Sous **Source**, le volume source est sélectionné par défaut. Cliquez sur **Other Volume** si vous souhaitez choisir un volume autre que la source.

4. Sous **destination**, choisissez la copie Snapshot à restaurer.
5. Si votre source et votre destination sont situées sur différents clusters, sur le cluster distant, cliquez sur **protection > relations** pour contrôler la progression de la restauration.

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la restauration de volume à l'aide de SnapVault"
Interface de ligne de commande ONTAP	"Restaurer le contenu d'un volume à partir d'une destination SnapMirror"

Effectuez des restaurations à partir de copies Snapshot

Vous pouvez restaurer un volume à un point antérieur, grâce à la restauration à partir d'une copie Snapshot.

Cette procédure restaure un volume à partir d'une copie Snapshot.

Étapes

1. Cliquez sur **Storage** et sélectionnez un volume.
2. Sous **copies snapshot**, cliquez sur ⋮ En regard de la copie Snapshot à restaurer, puis sélectionnez **Restaurer**.

Restaurez vers un nouveau volume

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour restaurer les données sauvegardées sur le volume de destination vers un volume autre que la source d'origine.

Lorsque vous restaurez un volume différent, vous pouvez sélectionner un volume existant ou créer un nouveau volume.

Étapes

1. Sélectionnez la relation de protection souhaitée : cliquez sur **protection > relations**.
2. Cliquez sur ⋮ Et cliquez sur **Restaurer**.
3. Dans la section **Source**, sélectionnez **Other Volume** et sélectionnez cluster et Storage VM.
4. Sélectionnez **Volume existant** ou **Créer un nouveau volume**.
5. Si vous créez un nouveau volume, entrez le nom du volume.
6. Dans la section **destination**, sélectionnez la copie Snapshot à restaurer.
7. Cliquez sur **Enregistrer**.
8. Sous **Relationship**, surveillez la progression de la restauration en visualisant **Transfer Status** pour la relation.

Inverser la resynchronisation d'une relation de protection

Depuis ONTAP 9.8, System Manager permet d'effectuer une opération de

resynchronisation inverse en vue de supprimer une relation de protection existante et d'inverser les fonctions des volumes source et de destination. Ensuite, vous utilisez le volume de destination pour transmettre des données pendant que vous réparez ou remplacez la source, mettez à jour la source, et rétablissez la configuration d'origine des systèmes.

> System Manager ne prend pas en charge la resynchronisation inverse avec des relations intracluster. Vous pouvez utiliser l'interface de ligne de commandes de ONTAP pour effectuer des opérations de resynchronisation inverse avec des relations intracluster.

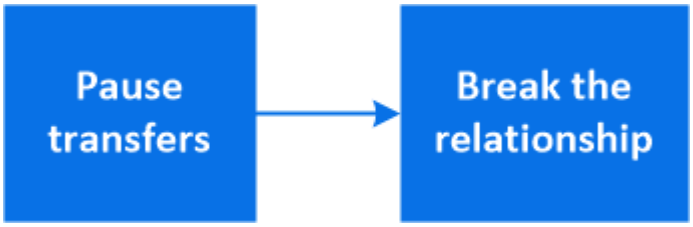
Lorsque vous effectuez une resynchronisation inverse, toutes les données du volume source qui sont plus récentes que les données de la copie Snapshot commune sont supprimées.

Étapes

1. Sélectionnez la relation de protection souhaitée : cliquez sur **protection > relations**.
2. Cliquez sur ⋮ Et cliquez sur **Reverse Resync**.
3. Sous **Relationship**, surveillez la progression de la resynchronisation inverse en visualisant **Transfer Status** pour la relation.

Service des données à partir d'une destination SnapMirror

Pour transmettre des données à partir d'une destination de miroir lorsqu'une source devient indisponible, arrêter les transferts programmés vers la destination, puis interrompre la relation SnapMirror pour rendre la destination inscriptible.



Étapes

1. Sélectionnez la relation de protection souhaitée : cliquez sur **protection > relations**, puis cliquez sur le nom de volume souhaité.
2. Cliquez sur ⋮.
3. Arrêter les transferts programmés : cliquez sur **Pause**.
4. Rendre la destination inscriptible : cliquez sur **Pause**.
5. Accédez à la page principale **relations** pour vérifier que l'état de la relation s'affiche comme « rompu ».

Étapes suivantes :

Lorsque le volume source désactivé est de nouveau disponible, vous devez resynchroniser la relation afin de copier les données actuelles sur le volume source d'origine. Ce processus remplace les données sur le volume source d'origine.

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la reprise après incident de volume"
Interface de ligne de commande ONTAP	"Activer le volume de destination"

Configurer la reprise après incident des machines virtuelles de stockage

Grâce à System Manager, vous pouvez créer une relation de reprise après incident de VM de stockage afin de répliquer une configuration de VM de stockage à une autre. En cas d'incident sur le site primaire, vous pouvez activer rapidement la VM de stockage de destination.

Effectuez cette procédure à partir de la destination. Si vous devez créer une nouvelle stratégie de protection, par exemple, lorsque votre machine virtuelle de stockage source a configuré SMB, vous devez utiliser System Manager pour créer la stratégie et sélectionner l'option **Identity Preserve** dans la fenêtre **Add protection Policy**.
Pour plus de détails, voir "Création de règles personnalisées de protection des données".

Étapes

1. Sur le cluster de destination, cliquez sur **protection > relations**.
2. Sous **relations**, cliquez sur protéger et choisissez **machines virtuelles de stockage (DR)**.
3. Sélectionnez une stratégie de protection. Si vous avez créé une règle de protection personnalisée, sélectionnez-la, puis choisissez le cluster source et la VM de stockage que vous souhaitez répliquer. Vous pouvez également créer une nouvelle machine virtuelle de stockage cible en entrant un nouveau nom de machine virtuelle de stockage.
4. Cliquez sur **Enregistrer**.

Service des données à partir d'une destination de reprise après incident des SVM

Depuis ONTAP 9.8, il est possible d'utiliser System Manager pour activer une machine virtuelle de stockage de destination après un incident. L'activation de la VM de stockage de destination rend les volumes de destination du SVM inscriptibles et vous permet de transmettre des données aux clients.

Étapes

1. Si le cluster source est accessible, vérifiez que le SVM est arrêté : accédez à **stockage > VM de stockage** et vérifiez la colonne **State** de la SVM.
2. Si l'état du SVM source est « running », stop-le : Select ⋮ Et choisissez **Stop**.
3. Sur le cluster de destination, recherchez la relation de protection souhaitée : accédez à **protection > relations**.
4. Cliquez sur ⋮ Et choisissez **Activer la VM de stockage de destination**.

Réactiver une VM de stockage source

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour réactiver une machine virtuelle de stockage source après un incident. La réactivation de la machine virtuelle de

stockage source arrête la machine virtuelle de stockage de destination et permet de réactiver la réplication de la source vers la destination.

Description de la tâche

Lorsque vous réactivez la machine virtuelle de stockage source, System Manager effectue les opérations suivantes en arrière-plan :

- Crée une relation SVM DR inverse de la destination initiale à la source d'origine à l'aide de la resynchronisation SnapMirror
- Arrête le SVM de destination
- Met à jour la relation SnapMirror
- Interrompt la relation SnapMirror
- Redémarre le SVM d'origine
- Renvoie une resynchronisation SnapMirror de la source d'origine vers la destination d'origine
- Nettoie les relations SnapMirror

Étapes

1. Sélectionnez la relation de protection souhaitée : cliquez sur **protection > relations**.
2. Cliquez sur ⋮ Et cliquez sur **réactiver la VM de stockage source**.
3. Sous **Relationship**, surveillez la progression de la réactivation de la source en visualisant **Transfer Status** pour la relation de protection.

Resynchroniser une machine virtuelle de stockage de destination

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour resynchroniser les données et les détails de configuration depuis la machine virtuelle de stockage source vers la machine virtuelle de stockage de destination dans une relation de protection défaillante et rétablir la relation.

ONTAP 9.11.1 offre la possibilité de contourner la reconstruction complète d'un entrepôt de données lorsque vous effectuez une répétition de reprise après incident, pour que vous puissiez revenir plus rapidement à la production.

Vous effectuez l'opération de resynchronisation uniquement à partir de la destination de la relation d'origine. La resynchronisation supprime toutes les données de la machine virtuelle de stockage de destination qui sont plus récentes que celles contenues dans la machine virtuelle de stockage source.

Étapes

1. Sélectionnez la relation de protection souhaitée : cliquez sur **protection > relations**.
2. Vous pouvez également sélectionner **effectuer une resynchronisation rapide** pour contourner la reconstruction complète d'un entrepôt de données lors d'une répétition de reprise après sinistre.
3. Cliquez sur ⋮ Et cliquez sur **Resync**.
4. Sous **Relationship**, surveillez la progression de la resynchronisation en affichant **Transfer Status** pour la relation.

Sauvegardez les données dans le cloud avec SnapMirror

Depuis ONTAP 9.9.1, vous pouvez sauvegarder vos données dans le cloud et les restaurer à partir du stockage cloud vers un autre volume à l'aide de System Manager. Vous pouvez utiliser StorageGRID ou ONTAP S3 en tant que magasin d'objets cloud.

Avant d'utiliser SnapMirror Cloud, nous vous recommandons de demander une clé de licence d'API SnapMirror Cloud sur le site de support NetApp : "Demandez la clé de licence de l'API SnapMirror Cloud". En suivant les instructions, vous devez fournir une description simple de votre opportunité commerciale et demander la clé API en envoyant un e-mail à l'adresse e-mail fournie. Vous devriez recevoir une réponse par e-mail dans les 24 heures avec des instructions supplémentaires sur l'acquisition de la clé API.

Ajouter un magasin d'objets cloud

Avant de configurer les sauvegardes cloud SnapMirror, vous devez ajouter un magasin d'objets cloud StorageGRID ou ONTAP S3.

Étapes

1. Cliquez sur **protection > Présentation > magasins d'objets cloud**.
2. Cliquez sur + Add .

Sauvegardez à l'aide de la règle par défaut

Vous pouvez rapidement configurer une sauvegarde SnapMirror Cloud pour un volume existant à l'aide de la règle de protection du cloud par défaut : DailyBackup.

Étapes

1. Cliquez sur **protection > Présentation** et sélectionnez **Sauvegarder les volumes dans le cloud**.
2. Si vous effectuez votre première sauvegarde dans le cloud, saisissez votre clé de licence SnapMirror Cloud API dans le champ de licence comme indiqué.
3. Cliquez sur **authentifier et continuer**.
4. Sélectionnez un volume source.
5. Sélectionnez un magasin d'objets cloud.
6. Cliquez sur **Enregistrer**.

Création d'une politique de sauvegarde cloud personnalisée

Si vous ne souhaitez pas utiliser la règle de cloud DailyBackup par défaut pour vos sauvegardes dans le cloud SnapMirror, vous pouvez créer votre propre règle.

Étapes

1. Cliquez sur **protection > Présentation > Paramètres de stratégie locale** et sélectionnez **stratégies de protection**.
2. Cliquez sur **Ajouter** et entrez les détails de la nouvelle stratégie.
3. Dans la section **Policy Type**, sélectionnez **Sauvegarder dans le cloud** pour indiquer que vous créez une stratégie de cloud.
4. Cliquez sur **Enregistrer**.

Créez une sauvegarde à partir de la page volumes

Vous pouvez utiliser la page System Manager **volumes** pour sélectionner et créer des sauvegardes de cloud pour plusieurs volumes à la fois ou lorsque vous souhaitez utiliser une règle de protection personnalisée.

Étapes

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez les volumes que vous souhaitez sauvegarder dans le nuage, puis cliquez sur **Protect**.
3. Dans la fenêtre **Protect Volume**, cliquez sur **plus d'options**.
4. Sélectionnez une stratégie.

   Vous pouvez sélectionner la stratégie par défaut, DailyBackup ou une stratégie cloud personnalisée que vous avez créée.

5. Sélectionnez un magasin d'objets cloud.
6. Cliquez sur **Enregistrer**.

Restaurez vos données à partir du cloud

System Manager permet de restaurer les données sauvegardées depuis le stockage cloud vers un autre volume du cluster source.

Étapes

1. Cliquez sur **Storage > volumes**.
2. Sélectionnez l'onglet **Sauvegarder dans le Cloud**.
3. Cliquez sur ⋮ En regard du volume source que vous souhaitez restaurer, sélectionnez **Restaurer**.
4. Sous **Source**, sélectionnez une VM de stockage, puis entrez le nom du volume sur lequel vous souhaitez restaurer les données.
5. Sous **destination**, sélectionnez la copie Snapshot à restaurer.
6. Cliquez sur **Enregistrer**.

Supprimez une relation cloud SnapMirror

Vous pouvez utiliser System Manager pour supprimer une relation cloud.

Étapes

1. Cliquez sur **Storage > volumes** et sélectionnez le volume à supprimer.
2. Cliquez sur ⋮ En regard du volume source et sélectionnez **Supprimer**.
3. Sélectionnez **Supprimer le noeud final du magasin d'objets Cloud (facultatif)** si vous souhaitez supprimer le noeud final du magasin d'objets Cloud.
4. Cliquez sur **Supprimer**.

Supprime un magasin d'objets cloud

Vous pouvez utiliser System Manager pour supprimer un magasin d'objets cloud s'il ne fait pas partie d'une relation de sauvegarde dans le cloud. Lorsqu'un magasin d'objets cloud fait partie d'une relation de sauvegarde dans le cloud, il ne peut pas être supprimé.

Étapes

1. Cliquez sur **protection > Présentation > magasins d'objets cloud**.
2. Sélectionnez le magasin d'objets à supprimer, puis cliquez sur ⋮ Et sélectionnez **Supprimer**.

Sauvegardez les données à l'aide de Cloud Backup

Depuis ONTAP 9.9.1, vous pouvez utiliser System Manager pour sauvegarder les données dans le cloud à l'aide de Cloud Backup.

> Cloud Backup prend en charge les volumes FlexVol de lecture-écriture et de protection des données (DP). Les volumes FlexGroup et SnapLock ne sont pas pris en charge.

Avant de commencer

Pour créer un compte dans BlueXP, vous devez effectuer les procédures suivantes. Pour le compte de service, vous devez créer le rôle « Administrateur de compte ». (Les autres rôles de compte de service ne disposent pas des privilèges requis pour établir une connexion à partir de System Manager.)

1. "Créez un compte dans BlueXP".
2. "Créez un connecteur dans BlueXP" avec l'un des nombreux fournisseurs de cloud suivants :
   - Microsoft Azure
   - Services Web Amazon (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > Depuis ONTAP 9.10.1, vous pouvez sélectionner StorageGRID comme fournisseur de sauvegarde cloud, mais uniquement si BlueXP est déployé sur site. Le connecteur BlueXP doit être installé sur site et disponible via l'application BlueXP Software-as-a-service (SaaS).

3. "Abonnez-vous à Cloud Backup Service dans BlueXP" (nécessite la licence appropriée).
4. "Générez une clé d'accès et une clé secrète à l'aide de BlueXP".

Enregistrez le cluster avec BlueXP

Vous pouvez enregistrer le cluster avec BlueXP en utilisant BlueXP ou System Manager.

Étapes

1. Dans System Manager, accédez à **Présentation de la protection**.
2. Sous **Cloud Backup Service**, fournissez les détails suivants :
   - ID client
   - Clé secrète du client
3. Sélectionnez **Enregistrer et continuer**.

Activation de Cloud Backup

Une fois le cluster enregistré auprès de BlueXP, vous devez activer Cloud Backup et lancer la première sauvegarde dans le cloud.

Étapes

1. Dans System Manager, cliquez sur **protection > Présentation**, puis faites défiler jusqu'à la section **Cloud Backup Service**.
2. Saisissez **ID client** et **secret client**.

> Depuis ONTAP 9.10.1, vous pouvez en savoir plus sur le coût d'utilisation du cloud en cliquant sur **en savoir plus sur le coût d'utilisation du cloud**.

3. Cliquez sur **connexion et activez Cloud Backup Service**.
4. Sur la page **Activer Cloud Backup Service**, indiquez les détails suivants, en fonction du fournisseur que vous avez sélectionné.

Pour ce fournisseur de cloud…	Entrez les données suivantes…
Azure	• ID d'abonnement Azure • Région • Nom du groupe de ressources (existant ou nouveau)
AWS	• ID de compte AWS • Touche d'accès • Clé secrète • Région
Projet Google Cloud (GCP)	• Nom du projet Google Cloud • Clé Google Cloud Access • Clé secrète Google Cloud • Région
StorageGRID (ONTAP 9.10.1 et versions ultérieures, pour le déploiement sur site de BlueXP uniquement)	• Serveur • Clé d'accès SG • Clé secrète SG

5. Sélectionnez une **stratégie de protection** :
   - **Politique existante** : choisir une politique existante.
   - **Nouvelle stratégie** : spécifiez un nom et définissez un calendrier de transfert.

> Depuis ONTAP 9.10.1, vous pouvez indiquer si vous souhaitez activer l'archivage avec Azure ou AWS.

> Si vous activez l'archivage pour un volume avec Azure ou AWS, vous ne pouvez pas désactiver l'archivage.

Si vous activez l'archivage pour Azure ou AWS, spécifiez les éléments suivants :

    - Nombre de jours après lequel le volume est archivé.
    - Nombre de sauvegardes à conserver dans l'archive. Spécifiez "0" (zéro) pour archiver jusqu'à la dernière sauvegarde.
    - Pour AWS, sélectionnez la classe de stockage d'archivage.
6. Sélectionnez les volumes à sauvegarder.
7. Sélectionnez **Enregistrer**.

Modifiez la règle de protection utilisée pour Cloud Backup

Vous pouvez modifier la règle de protection utilisée avec Cloud Backup.

Étapes

1. Dans System Manager, cliquez sur **protection > Présentation**, puis faites défiler jusqu'à la section **Cloud Backup Service**.
2. Cliquez sur ⋮, Puis **Modifier**.
3. Sélectionnez une **stratégie de protection** :
    - **Politique existante** : choisir une politique existante.
    - **Nouvelle stratégie** : spécifiez un nom et définissez un calendrier de transfert.

      Depuis ONTAP 9.10.1, vous pouvez indiquer si vous souhaitez activer l'archivage avec Azure ou AWS.

      Si vous activez l'archivage pour un volume avec Azure ou AWS, vous ne pouvez pas désactiver l'archivage.

      Si vous activez l'archivage pour Azure ou AWS, spécifiez les éléments suivants :

      - Nombre de jours après lequel le volume est archivé.
      - Nombre de sauvegardes à conserver dans l'archive. Spécifiez "0" (zéro) pour archiver jusqu'à la dernière sauvegarde.
      - Pour AWS, sélectionnez la classe de stockage d'archivage.
4. Sélectionnez **Enregistrer**.

Protection de nouveaux volumes ou LUN sur le cloud

Lorsque vous créez un nouveau volume ou une LUN, vous pouvez établir une relation de protection SnapMirror qui permet de sauvegarder les données dans le cloud pour le volume ou la LUN.

Avant de commencer

- Vous devez disposer d'une licence SnapMirror.
- Les LIFs intercluster doivent être configurées.
- NTP doit être configuré.
- Le cluster doit exécuter ONTAP 9.9.1.

Description de la tâche

Vous ne pouvez pas protéger de nouveaux volumes ou de nouvelles LUN dans le cloud pour les configurations

de cluster suivantes :

- Le cluster ne peut pas se trouver dans un environnement MetroCluster.
- SVM-DR n'est pas pris en charge.
- Impossible de sauvegarder FlexGroups à l'aide de Cloud Backup.

Étapes

1. Lors du provisionnement d'un volume ou d'une LUN, sur la page **protection** dans System Manager, cochez la case **Activer SnapMirror (local ou distant)**.
2. Sélectionnez le type de stratégie Cloud Backup.
3. Si la sauvegarde dans le cloud n'est pas activée, sélectionnez **Activer Cloud Backup Service**.

Protection des volumes ou des LUN existants sur le cloud

Vous pouvez établir une relation de protection SnapMirror pour les volumes et les LUN existants.

Étapes

1. Sélectionnez un volume ou une LUN existant, puis cliquez sur **Protect**.
2. Sur la page **Protect volumes**, spécifiez **Backup utilisant Cloud Backup Service** pour la stratégie de protection.
3. Cliquez sur **protéger**.
4. Sur la page **protection**, cochez la case **Activer SnapMirror (local ou distant)**.
5. Sélectionnez **Activer Cloud Backup Service**.

Restaurez les données à partir des fichiers de sauvegarde

Vous pouvez effectuer des opérations de gestion de sauvegarde, telles que la restauration de données, la mise à jour de relations et la suppression de relations, uniquement lorsque vous utilisez l'interface BlueXP. Reportez-vous à la section "Restauration des données à partir des fichiers de sauvegarde" pour en savoir plus.

Cluster et SVM peering avec l'interface de ligne de commande

Présentation du cluster et de SVM peering avec l'interface de ligne de commande

Il est possible de créer des relations entre les clusters source et de destination et entre les machines virtuelles de stockage source et de destination. Vous devez créer des relations de pairs entre ces entités avant de répliquer des copies Snapshot à l'aide de SnapMirror.

ONTAP 9.3 apporte des améliorations qui simplifient la configuration des relations entre les clusters et les SVM. Les procédures de peering de clusters et de SVM sont disponibles pour toutes les versions de ONTAP 9. Utilisez la procédure appropriée pour votre version de ONTAP.

Vous effectuez les procédures à l'aide de l'interface de ligne de commandes, et non de System Manager ou d'un outil de script automatisé.

Préparation du cluster et de la SVM peering

Bases du peering

Vous devez créer des relations *peer* entre les clusters source et de destination, et entre les SVM source et destination avant de pouvoir répliquer les copies Snapshot à l'aide de SnapMirror. Une relation de type peer-to-peer définit les connexions réseau qui permettent aux clusters et aux SVM d'échanger les données de manière sécurisée.

Les clusters et les SVM dans des relations entre pairs communiquent sur le réseau intercluster à l'aide de *interfaces logiques (LIF) intercluster.* une LIF intercluster est une LIF qui prend en charge le service d'interface réseau « intercluster-core » et qui est généralement créée en utilisant la politique de service d'interface réseau « default-intercluster ». On doit créer des LIF intercluster sur chaque nœud des clusters en cours de peering.

Les LIFs intercluster utilisent des routes qui appartiennent au SVM système auquel elles sont assignées. ONTAP crée automatiquement un SVM système pour les communications au niveau du cluster au sein d'un IPspace.

Les topologies en mode « Fan-Out » et en cascade sont toutes deux prises en charge. Dans une topologie en cascade, il suffit de créer des réseaux intercluster entre les clusters principal et secondaire, et entre les clusters secondaire et tertiaire. Il n'est pas nécessaire de créer un réseau intercluster entre le cluster principal et le cluster tertiaire.

> Il est possible (mais pas conseillé) à un administrateur de supprimer le service intercluster de la politique de service default-intercluster. Dans ce cas, les LIFs créées à l'aide de « Default-intercluster » ne seront en fait pas des LIFs intercluster. Pour vérifier que la politique de service par défaut-intercluster contient le service intercluster-core, utiliser la commande suivante :
>
> ```
> network interface service-policy show -policy default-intercluster
> ```

Conditions préalables au peering de clusters

Avant de configurer le peering de cluster, vous devez vérifier que la connectivité, le port, l'adresse IP, le sous-réseau, le pare-feu, et les exigences de nommage des clusters sont respectées.

> À partir de ONTAP 9.6, le chiffrement des pairs de cluster assure par défaut la prise en charge du chiffrement TLS 1.2 AES-256 GCM pour la réplication des données. Les chiffrements de sécurité par défaut (« PSK-AES256-GCM-SHA384 ») sont requis pour que le peering de cluster fonctionne même si le chiffrement est désactivé.
>
> À partir de ONTAP 9.11.1, les chiffrements de sécurité DHE-PSK sont disponibles par défaut.

Les besoins en connectivité

Chaque LIF intercluster du cluster local doit pouvoir communiquer avec chaque LIF intercluster sur le cluster distant.

Bien qu'il ne soit pas nécessaire, il est généralement plus simple de configurer les adresses IP utilisées pour les LIF intercluster dans le même sous-réseau. Les adresses IP peuvent résider dans le même sous-réseau que les LIF de données ou dans un autre sous-réseau. Le sous-réseau utilisé dans chaque cluster doit respecter les exigences suivantes :

- Le sous-réseau doit appartenir au broadcast domain qui contient les ports utilisés pour la communication intercluster.
- Le sous-réseau doit disposer de suffisamment d'adresses IP disponibles pour allouer à une LIF intercluster par nœud.

  Par exemple, dans un cluster à quatre nœuds, le sous-réseau utilisé pour la communication intercluster doit disposer de quatre adresses IP disponibles.

Chaque nœud doit disposer d'un LIF intercluster avec une adresse IP sur le réseau intercluster.

Les LIF intercluster peuvent disposer d'une adresse IPv4 ou IPv6.

> ONTAP vous permet de migrer vos réseaux de peering depuis IPv4 vers IPv6 en autorisant éventuellement la présence des deux protocoles simultanément sur les LIF intercluster. Dans les versions précédentes, toutes les relations intercluster pour un cluster entier étaient au format IPv4 ou IPv6. Cela signifiait que le changement de protocole était potentiellement source de perturbation.

Configuration requise pour les ports

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Les ports doivent répondre aux exigences suivantes :

- Tous les ports utilisés pour communiquer avec un cluster distant donné doivent se trouver dans le même IPspace.

  Vous pouvez utiliser plusieurs IPspaces pour gérer plusieurs clusters dans un même cluster. Une connectivité à maillage complet par paire est requise uniquement au sein d'un IPspace.

- Le broadcast domain utilisé pour la communication intercluster doit inclure au moins deux ports par nœud afin que la communication intercluster puisse basculer d'un port vers un autre.

  Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces (ifgrps).

- Tous les ports doivent être câblés.
- Tous les ports doivent être en état de santé.
- Les paramètres MTU des ports doivent être cohérents.

Exigences relatives au pare-feu

> Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

Les pare-feu et la politique de pare-feu intercluster doivent autoriser les protocoles suivants :

- Trafic ICMP bidirectionnel
- Le trafic TCP initié bidirectionnel vers les adresses IP de toutes les LIFs intercluster sur les ports 11104 et 11105
- HTTPS bidirectionnel entre les LIFs intercluster

Bien que HTTPS n'est pas requis lors de la configuration du peering de clusters à l'aide de l'interface de ligne de commande, HTTPS est requis plus tard si vous utilisez System Manager pour configurer la protection des données.

La valeur par défaut `intercluster` La politique de pare-feu permet l'accès via le protocole HTTPS et à partir de toutes les adresses IP (0.0.0.0/0). Vous pouvez modifier ou remplacer la stratégie si nécessaire.

Regroupement des clusters

Les clusters doivent répondre aux exigences suivantes :

- Un cluster ne peut pas se trouver dans une relation entre pairs et plus de 255 clusters.

Utiliser des ports partagés ou dédiés

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Lors de la décision de partager des ports, vous devez tenir compte de la bande passante du réseau, de l'intervalle de réplication et de la disponibilité des ports.

Vous pouvez partager les ports sur un cluster en utilisant des ports dédiés sur l'autre.

La bande passante du réseau

Si vous disposez d'un réseau haut débit (par exemple 10 GbE), vous disposez peut-être d'une bande passante LAN locale suffisante pour effectuer la réplication à l'aide des mêmes ports 10 GbE utilisés pour l'accès aux données.

Vous devriez même comparer votre bande passante WAN disponible à celle de votre réseau local. Si la bande passante WAN disponible est bien inférieure à 10 GbE, vous devrez peut-être utiliser des ports dédiés.

À l'exception de cette règle, on peut trouver lorsque tous les nœuds du cluster répliquent des données, auquel cas l'utilisation de la bande passante est généralement répartie entre ces nœuds.

Si vous n'utilisez pas de ports dédiés, la taille de l'unité de transmission maximale (MTU) du réseau de réplication doit généralement être identique à la taille de MTU du réseau de données.

Intervalle de réplication

Si la réplication se déroule en dehors des heures de pointe, vous devriez pouvoir utiliser des ports de données pour la réplication, même sans connexion LAN 10 GbE.

Si la réplication a lieu pendant les heures de bureau, vous devez tenir compte de la quantité de données à répliquer et de la quantité de bande passante nécessaire pour créer des conflits avec les protocoles de données. Si l'utilisation du réseau par les protocoles de données (SMB, NFS, iSCSI) est supérieure à 50 %, il est recommandé d'utiliser des ports dédiés pour la communication intercluster afin de permettre des performances non dégradées en cas de basculement du nœud.

Disponibilité du port

Si vous déterminez que le trafic de réplication interfère sur le trafic de données, vous pouvez migrer des LIFs intercluster vers n'importe quel autre port partagé intercluster sur le même nœud.

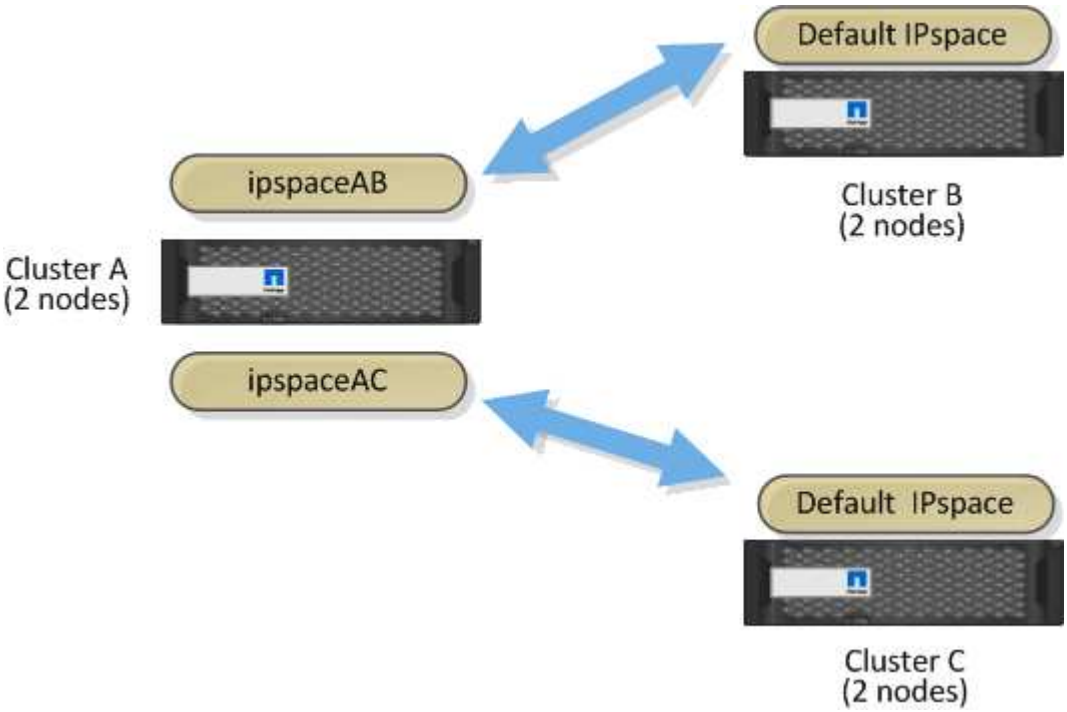
Vous pouvez également dédier des ports VLAN à la réplication. La bande passante du port est partagée entre tous les VLAN et le port de base.

Utilisez les IPspaces personnalisés pour isoler le trafic de réplication

Vous pouvez utiliser des IPspaces personnalisés pour séparer les interactions d'un cluster avec ses pairs. Appelée *connectivité intercluster désignée*, cette configuration permet aux fournisseurs de services d'isoler le trafic de réplication dans des environnements mutualisés.

Supposons, par exemple, que vous souhaitez que le trafic de réplication entre le Cluster A et le Cluster B soit séparé du trafic de réplication entre le Cluster A et le Cluster C. Pour ce faire, vous pouvez créer deux IPspaces sur le Cluster A.

Un IPspace contient les LIF intercluster que vous utilisez pour communiquer avec le Cluster B. L'autre contient les LIFs intercluster que vous utilisez pour communiquer avec le Cluster C, comme indiqué sur l'illustration suivante.



Pour une configuration IPspace personnalisée, consultez le *Network Management Guide*.

Configurer les LIFs intercluster

Configurer les LIFs intercluster sur des ports data partagés

Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Étapes

1. Lister les ports dans le cluster :

```
network port show
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Créer des LIF intercluster sur un SVM admin (IPspace par défaut) ou un SVM système (IPspace personnalisé) :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
Dans ONTAP 9.5 et versions antérieures:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Vérifier que les LIFs intercluster ont été créés :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vérifier que les LIFs intercluster sont redondants :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` sur le `e0c` le port basculera vers le `e0d` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Configurer les LIFs intercluster sur les ports dédiés

Vous pouvez configurer les LIFs intercluster sur des ports dédiés. Cela augmente généralement la bande passante disponible pour le trafic de réplication.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Déterminer les ports disponibles pour dédier aux communications intercluster :

   `network interface show -fields home-port,curr-port`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant indique ces ports `e0e` et `e0f` Ne se sont pas affectés de LIFs :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Créer un failover group pour les ports dédiés :

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

L'exemple suivant attribue des ports `e0e` et `e0f` vers le groupe de basculement `intercluster01` Sur le SVM système `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vérifier que le groupe de basculement a été créé :

   `network interface failover-groups show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Créer les LIF intercluster sur le SVM système et les assigner au failover group.

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home- port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover -group` *`failover_group`*

Option	Description
Dans ONTAP 9.5 et versions antérieures:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover-group` *`failover_group`*

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02` dans le groupe de basculement `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Vérifier que les LIFs intercluster ont été créés :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vérifier que les LIFs intercluster sont redondants :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` Sur le SVM`e0e` le port basculera vers le `e0f` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurez les LIF intercluster dans des IPspaces personnalisés

Vous pouvez configurer les LIF intercluster dans des IPspaces personnalisés. Il est ainsi possible d'isoler le trafic de réplication dans des environnements mutualisés.

Lorsque vous créez un IPspace personnalisé, le système crée une machine virtuelle de stockage système (SVM) afin de servir de conteneur pour les objets système dans cet IPspace. Vous pouvez utiliser le nouveau SVM en tant que conteneur pour toutes les LIF intercluster dans le nouvel IPspace. Le nouveau SVM porte le même nom que l'IPspace personnalisé.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau dans `cluster01`:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Créez des IPspaces personnalisés sur le cluster :

   `network ipspace create -ipspace` *`ipspace`*

   L'exemple suivant crée l'IPspace personnalisé `ipspace-IC1`:

   ```
   cluster01::> network ipspace create -ipspace ipspace-IC1
   ```

3. Déterminer les ports disponibles pour dédier aux communications intercluster :

   `network interface show -fields home-port,curr-port`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant indique ces ports `e0e` et `e0f` Ne se sont pas affectés de LIFs :

   ```
   cluster01::> network interface show -fields home-port,curr-port
   vserver lif                  home-port curr-port
   ------- -------------------- --------- ---------
   Cluster cluster01_clus1   e0a       e0a
   Cluster cluster01_clus2   e0b       e0b
   Cluster cluster02_clus1   e0a       e0a
   Cluster cluster02_clus2   e0b       e0b
   cluster01
           cluster_mgmt         e0c       e0c
   cluster01
           cluster01-01_mgmt1   e0c       e0c
   cluster01
           cluster01-02_mgmt1   e0c       e0c
   ```

4. Supprimer les ports disponibles du broadcast domain par défaut :

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Un port ne peut pas se trouver dans plusieurs domaines de diffusion à la fois. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant supprime les ports `e0e` et `e0f` depuis le broadcast domain par défaut :

   ```
   cluster01::> network port broadcast-domain remove-ports -broadcast
   -domain Default -ports
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

5. Vérifiez que les ports ont été supprimés du broadcast domain par défaut :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant indique ces ports `e0e` et `e0f` ont été supprimés du broadcast domain par défaut :

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Créer un domaine de diffusion dans l'IPspace personnalisé :

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   L'exemple suivant crée le domaine de diffusion `ipspace-IC1-bd` Dans l'IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Vérifiez que le domaine de diffusion a été créé :

   `network port broadcast-domain show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                         Update
Name    Domain Name    MTU  Port List                     Status Details
------- ----------- ------  ------------------------------ --------------
Cluster Cluster       9000
                            cluster01-01:e0a              complete
                            cluster01-01:e0b              complete
                            cluster01-02:e0a              complete
                            cluster01-02:e0b              complete
Default Default       1500
                            cluster01-01:e0c              complete
                            cluster01-01:e0d              complete
                            cluster01-01:e0f              complete
                            cluster01-01:e0g              complete
                            cluster01-02:e0c              complete
                            cluster01-02:e0d              complete
                            cluster01-02:e0f              complete
                            cluster01-02:e0g              complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e              complete
                            cluster01-01:e0f              complete
                            cluster01-02:e0e              complete
                            cluster01-02:e0f              complete
```

8. Créer les LIFs intercluster sur le SVM système et les assigner au broadcast domain :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
Dans ONTAP 9.5 et versions antérieures:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Le LIF est créé dans le broadcast domain auquel le home port est attribué. Le broadcast domain a un failover group par défaut avec le même nom que le broadcast domain. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02` dans le domaine de broadcast `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Vérifier que les LIFs intercluster ont été créés :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Vérifier que les LIFs intercluster sont redondants :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` Sur le SVM `e0e` le port passe au port « e0f'port :

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurer les relations de pairs

Créer une relation entre clusters

Vous pouvez utiliser le `cluster peer create` commande permettant de créer une relation homologue entre un cluster local et un cluster distant. Une fois la relation homologue créée, vous pouvez exécuter `cluster peer create` sur le cluster distant afin de l'authentifier auprès du cluster local.

Avant de commencer

- Vous devez avoir créé des LIF intercluster sur chaque nœud des clusters qui sont en cours de peering.
- Les clusters doivent exécuter ONTAP 9.3 ou version ultérieure. (Si les clusters exécutent ONTAP 9.2 ou une version antérieure, reportez-vous aux procédures de la "ce document archivé".)

Étapes

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

1. Dans le cluster local, cliquez sur **Cluster > Paramètres**.
2. Dans la section **intercluster Settings**, cliquez sur **Add Network interfaces** et ajoutez les interfaces réseau intercluster du cluster.

   Répétez cette étape sur le cluster distant.

3. Dans le cluster distant, cliquez sur **Cluster > Paramètres**.
4. Cliquez sur ⋮ Dans la section **homologues du cluster** et sélectionnez **générer une phrase de passe**.
5. Sélectionnez la version du cluster ONTAP distant.
6. Copiez la phrase de passe générée.
7. Dans le cluster local, sous **clusters homologues**, cliquez sur ⋮ Et sélectionnez **Peer Cluster**.
8. Dans la fenêtre **Peer Cluster**, collez la phrase de passe et cliquez sur **Initiate cluster peering**.

CLI

1. Sur le cluster destination, créez une relation entre pairs et le cluster source :

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS>|1...7days|1...168hours -peer-addrs
   <peer_LIF_IPs > -initial-allowed-vserver-peers <svm_name>|* -ipspace
   <ipspace>
   ```

   Si vous spécifiez les deux `-generate-passphrase` et `-peer-addrs`, Uniquement le cluster dont les LIFs intercluster sont spécifiés dans `-peer-addrs` peut utiliser le mot de passe généré.

   Vous pouvez ignorer `-ipspace` Option si vous n'utilisez pas un IPspace personnalisé. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   Si vous créez la relation de peering dans ONTAP 9.6 ou version ultérieure et que vous ne souhaitez pas que les communications de peering de clusters soient cryptées, vous devez utiliser le `-encryption-protocol-proposed none` option pour désactiver le cryptage.

   L'exemple suivant crée une relation de cluster peer-to-peer avec un cluster distant non spécifié, et autorise pré-les relations de pairs avec les SVM `vs1` et `vs2` sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

L'exemple suivant crée une relation de cluster peer-to-peer avec le cluster distant aux adresses IP LIF intercluster 192.140.112.103 et 192.140.112.104, et autorise pré-une relation de peer-to-peer avec n'importe quel SVM sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

L'exemple suivant crée une relation de cluster peer-to-peer avec un cluster distant non spécifié, et autorise pré-les relations de pairs avec les SVM`vs1` et `vs2` sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. Sur le cluster source, authentifier le cluster source sur le cluster destination :

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant authentifie le cluster local sur le cluster distant aux adresses IP 192.140.112.101 et 192.140.112.102 de LIF intercluster :

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Entrez la phrase de passe de la relation homologue lorsque vous y êtes invité.

3. Vérifiez que la relation entre clusters a été créée :

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                              Peer Cluster Name: cluster02
                   Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                            Remote Cluster Name: cluster2
                            Active IP Addresses: 192.140.112.101,
192.140.112.102
                          Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                                Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Vérifier la connectivité et l'état des nœuds de la relation peer-to-peer :

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Préparez-vous à la mise en miroir et à l'archivage"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la préparation de la reprise sur incident de volume"

Créer une relation SVM peer-to-peer

Vous pouvez utiliser le `vserver peer create` Commande pour créer une relation entre les SVM sur des clusters locaux et distants.

Avant de commencer

- Les clusters source et destination doivent être associés.
- Les clusters doivent exécuter ONTAP 9.3. (Si les clusters exécutent ONTAP 9.2 ou une version antérieure, reportez-vous aux procédures de la "ce document archivé".)
- Vous devez avoir des relations de pairs « pré-autorisées » pour les SVM sur le cluster distant.

  Pour plus d'informations, voir "Création d'une relation entre clusters".

Description de la tâche

Dans ONTAP 9.2 et versions antérieures, vous pouvez autoriser une relation de pairs pour un seul SVM à la fois. Cela signifie que vous devez exécuter `vserver peer accept` Chaque fois que vous autorisez une relation de SVM peer en attente.

Depuis ONTAP 9.3, vous pouvez « pré-autoriser » des relations entre pairs pour plusieurs SVM en répertoriant les SVM dans le `-initial-allowed-vserver` option lors de la création d'une relation de type cluster. Pour plus d'informations, voir "Création d'une relation entre clusters".

Étapes

1. Sur le cluster destination de protection des données, afficher les SVM qui sont pré-autorisés pour le peering :

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. Sur le cluster source de protection des données, créez une relation entre pairs et un SVM pré-autorisé sur le cluster cible de protection des données :

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant crée une relation de pairs entre le SVM local `pvs1` Et le SVM distant pré-autorisé `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Vérifier la relation entre SVM et :

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Ajouter une relation SVM peer-to-peer intercluster

Si vous créez un SVM après avoir configuré une relation de cluster peer-to-peer, vous devez ajouter manuellement une relation de peer-to-peer pour la SVM. Vous pouvez utiliser le `vserver peer create` Commande pour créer une relation entre SVM. Une fois la relation homologue créée, vous pouvez exécuter `vserver peer accept` sur le cluster distant, afin d'autoriser la relation peer-to-peer.

Avant de commencer

Les clusters source et destination doivent être associés.

Description de la tâche

Vous pouvez créer des relations peer-to-peer entre les SVM et dans le même cluster pour la sauvegarde des données locales. Pour plus d'informations, reportez-vous à la section `vserver peer create` page de manuel.

Les administrateurs utilisent parfois le `vserver peer reject` Commande permettant de refuser une relation SVM peer-to-peer proposée. Si la relation entre les SVM se trouve dans le `rejected` état, vous devez supprimer la relation pour en créer une nouvelle. Pour plus d'informations, reportez-vous à la section `vserver peer delete` page de manuel.

Étapes

1. Sur le cluster source de protection des données, créez une relation entre pairs et un SVM sur le cluster cible de protection des données :

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   L'exemple suivant crée une relation de pairs entre le SVM local`pvs1` Et le SVM distant`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Si les SVM locaux et distants ont les mêmes noms, vous devez utiliser un *local name* pour créer la relation SVM peer :

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. Sur le cluster source de protection des données, vérifiez que la relation de pairs a été initiée :

   `vserver peer show-all`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre que la relation de pairs entre SVM`pvs1` Et SVM`vs1` a été lancé :

```
cluster01::> vserver peer show-all
            Peer        Peer                        Peering
Vserver     Vserver     State      Peer Cluster   Applications
--------    --------    ---------  -------------  ------------
pvs1        vs1         initiated   Cluster02       snapmirror
```

3. Sur le cluster destination de protection des données, afficher la relation SVM peer-to-peer en attente :

   `vserver peer show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant répertorie les relations homologues en attente pour `cluster02`:

```
cluster02::> vserver peer show

                   Peer               Peer
Vserver            Vserver            State
-----------        -----------        ------------
vs1                pvs1               pending
```

4. Sur le cluster cible de protection des données, autoriser la relation peer-to-peer en attente :

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant autorise la relation de pairs entre la SVM locale `vs1` Et le SVM distant `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Vérifier la relation entre SVM et :

```
vserver peer show
```

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Activer le chiffrement de peering de cluster sur une relation de pairs existante

Depuis ONTAP 9.6, le chiffrement de peering de cluster est activé par défaut sur toutes les relations de peering de cluster que nous avons récemment créées. Le chiffrement de peering de cluster utilise une clé pré-partagée (PSK) et la couche de sécurité du transport (TLS) pour sécuriser les communications de peering entre clusters. Cela ajoute une couche de sécurité supplémentaire entre les clusters avec points.

Description de la tâche

Si vous mettez à niveau des clusters de peering vers ONTAP 9.6 ou version ultérieure et que la relation de peering a été créée dans ONTAP 9.5 ou version antérieure, le chiffrement de peering de cluster doit être activé manuellement après la mise à niveau. Les deux clusters de la relation de peering doivent exécuter ONTAP 9.6 ou version ultérieure afin de permettre le cryptage du cluster peering.

Étapes

1. Sur le cluster de destination, activez le chiffrement pour les communications avec le cluster source :

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Entrez une phrase de passe lorsque vous y êtes invité.
3. Sur le cluster source de protection des données, activez le chiffrement pour la communication avec le cluster cible de protection des données :

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Indiquez la même phrase secrète entrée sur le cluster de destination.

Retirer le cryptage de peering de cluster d’une relation de pairs existante

Par défaut, le cryptage de peering de cluster est activé sur toutes les relations entre pairs créées dans ONTAP 9.6 ou version ultérieure. Si vous ne souhaitez pas utiliser le cryptage pour les communications de peering intercluster, vous pouvez le désactiver.

Étapes

1. Sur le cluster de destination, modifier les communications avec le cluster source afin d'arrêter l'utilisation du cryptage de peering de cluster :
   - Pour supprimer le cryptage mais maintenir l'authentification, entrez :

     ```
     cluster peer modify _source_cluster_ -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Pour supprimer le cryptage et l'authentification, entrez :

     ```
     cluster peer modify _source_cluster_ -auth-status no-authentication
     ```

2. Entrez une phrase de passe lorsque vous y êtes invité.
3. Sur le cluster source, désactiver le cryptage pour la communication avec le cluster destination :
   - Pour supprimer le cryptage mais maintenir l'authentification, entrez :

     ```
     cluster peer modify _destination_cluster_ -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Pour supprimer le cryptage et l'authentification, entrez :

     ```
     cluster peer modify _destination_cluster_ -auth-status no-
     authentication
     ```

4. Indiquez la même phrase secrète entrée sur le cluster de destination.

Gérez les copies Snapshot locales

Gérer les copies Snapshot locales

Une *copie snapshot* est une image ponctuelle en lecture seule d'un volume. L'image consomme un espace de stockage minimal et entraîne une surcharge minime des performances, car elle enregistre uniquement les modifications apportées aux fichiers depuis la dernière copie Snapshot.

Vous pouvez utiliser une copie Snapshot pour restaurer l'intégralité du contenu d'un volume, ou restaurer des fichiers ou des LUN individuels. Les copies Snapshot sont stockées dans le répertoire `.snapshot` sur le volume.

Dans ONTAP 9.3 et versions antérieures, un volume peut contenir jusqu'à 255 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume FlexVol peut contenir jusqu'à 1023 copies Snapshot.

Depuis ONTAP 9.8, les volumes FlexGroup peuvent contenir 1023 copies Snapshot. Pour plus d'informations, voir "Protection des volumes FlexGroup à l'aide de copies Snapshot".

Configuration de règles Snapshot personnalisées

Présentation de la configuration de règles Snapshot personnalisées

Une règle *Snapshot* définit la façon dont le système crée des copies Snapshot. La règle indique quand créer des copies Snapshot, le nombre de copies à conserver et comment les nommer. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et nommer les copies « otidienne.`timestamp`.»

La règle par défaut d'un volume crée automatiquement des copies Snapshot selon le calendrier suivant, avec les plus anciennes copies Snapshot supprimées pour laisser de l'espace disponible pour les copies les plus récentes :

- Six copies Snapshot toutes les heures ont été effectuées au maximum cinq minutes au-delà de l'heure.
- Deux copies Snapshot quotidiennes maximum sont effectuées du lundi au samedi 10 minutes après minuit.
- Deux copies Snapshot hebdomadaires maximum sont réalisées tous les dimanches à 15 minutes après minuit.

Sauf si vous spécifiez une règle Snapshot lorsque vous créez un volume, le volume hérite des règles de Snapshot associées à sa machine virtuelle de stockage (SVM).

A quel moment configurer une règle Snapshot personnalisée

Si la politique Snapshot par défaut n'est pas adaptée à un volume, vous pouvez configurer une règle personnalisée modifiant la fréquence, la conservation et le nom des copies Snapshot. Le planning sera dicté principalement par le taux de changement du système de fichiers actif.

Vous pouvez sauvegarder toutes les heures un système de fichiers très utilisé, comme une base de données, et sauvegarder les fichiers rarement utilisés une fois par jour. Même pour une base de données, vous exécutez généralement une sauvegarde complète une ou deux fois par jour, tout en sauvegardant les journaux de transactions toutes les heures.

Les autres facteurs sont l'importance des fichiers pour votre entreprise, votre contrat de niveau de service (SLA), votre objectif de point de récupération (RPO) et votre objectif de délai de restauration (RTO). De manière générale, vous devez conserver autant de copies Snapshot que nécessaire.

Créer un planning de travail instantané

Une règle Snapshot requiert une planification d'au moins une tâche de copie Snapshot. Vous pouvez utiliser le `job schedule cron create` commande permettant de créer un programme de travail.

Description de la tâche

Par défaut, ONTAP forme les noms des copies Snapshot en ajoutant un horodatage au nom du calendrier des

travaux.

Si vous spécifiez des valeurs pour le jour du mois et le jour de la semaine, elles sont considérées indépendamment. Par exemple, une planification cron avec la spécification de jour `Friday` et le jour du mois `13` S'étend tous les vendredis et le 13ème jour de chaque mois, pas seulement tous les vendredis du 13ème.

Étape

1. Création d'un programme de travail :

   `job schedule cron create -name` *`job_name`* `-month month -dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

   Depuis ONTAP 9.10.1, vous pouvez inclure le vServer dans votre calendrier des tâches :

   `job schedule cron create -name` *`job_name`* `-vserver` *`Vserver_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   L'exemple suivant crée un programme de travail nommé `myweekly` Le samedi à 3:00 :

   ```
   cluster1::> job schedule cron create -name myweekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

   L'exemple suivant crée un programme nommé `myweeklymulti` ce délai est spécifié pour plusieurs jours, heures et minutes :

   ```
   job schedule cron create -name myweeklymulti -dayofweek
   "Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
   ```

Créer une règle Snapshot

Une règle Snapshot spécifie quand créer des copies Snapshot, le nombre de copies à conserver et comment les nommer. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et les nommer « `diotidienne.`*`timestamp`*.» Une règle Snapshot peut contenir jusqu'à cinq planifications de tâches.

Description de la tâche

Par défaut, ONTAP forme les noms des copies Snapshot en ajoutant un horodatage au nom de la planification des travaux :

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Si vous préférez, vous pouvez remplacer un préfixe par le nom du programme de travail.

Le `snapmirror-label` L'option concerne la réplication SnapMirror. Pour plus d'informations, voir "Définition d'une règle pour une règle".

Étape

1. Création d'une règle Snapshot :

   `volume snapshot policy create -vserver` *`SVM`* `-policy` *`policy_name`* `-enabled true|false -schedule1` *`schedule1_name`* `-count1` *`copies_to_retain`* `-prefix1` *`snapshot_prefix`* `-snapmirror-label1` *`snapshot_label`* `… -schedule5` *`schedule5_name`* `-count5` *`copies_to_retain`*`-prefix5` *`snapshot_prefix`* `-snapmirror-label5` *`snapshot_label`*

   L'exemple suivant illustre la création de la règle Snapshot nommée `snap_policy_daily` cela fonctionne sur un `daily` planification. La règle possède un maximum de cinq copies Snapshot, chacune portant le nom `daily.`*`timestamp`* Et étiquette SnapMirror `daily`:

   ```
   cluster1::> volume snapshot policy create -vserver vs0 -policy
   snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1 daily
   ```

Gestion manuelle des copies Snapshot

Créez et supprimez des copies Snapshot manuellement

Vous pouvez créer des copies Snapshot manuellement si vous ne pouvez pas attendre la création d'une copie Snapshot planifiée et supprimer les copies Snapshot lorsqu'elles ne sont plus nécessaires.

Créez une copie Snapshot manuellement

Vous pouvez créer manuellement une copie Snapshot à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

Étapes

1. Accédez à **stockage > volumes** et sélectionnez l'onglet **copies Snapshot**.
2. Cliquez sur + Add .
3. Dans la fenêtre **Ajouter une copie Snapshot**, acceptez le nom de la copie Snapshot par défaut ou modifiez-le si vous le souhaitez.
4. **Facultatif** : ajoutez une étiquette SnapMirror.
5. Cliquez sur **Ajouter**.

CLI

1. Créer une copie Snapshot :

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Supprimez manuellement une copie Snapshot

Vous pouvez supprimer manuellement une copie Snapshot à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

Étapes

1. Accédez à **stockage > volumes** et sélectionnez l'onglet **copies Snapshot**.
2. Recherchez la copie Snapshot à supprimer, cliquez sur ⋮, Et sélectionnez **Supprimer**.
3. Dans la fenêtre **Supprimer la copie Snapshot**, sélectionnez **Supprimer la copie Snapshot**.
4. Cliquez sur **Supprimer**.

CLI

1. Supprimer une copie Snapshot :

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Gérez la réserve de copies Snapshot

Gérer la présentation de la réserve de copies Snapshot

Le paramètre *Snapshot copy Reserve* permet de réserver un pourcentage d'espace disque pour les copies Snapshot, cinq pour cent par défaut. Lorsque les copies Snapshot utilisent de l'espace dans le système de fichiers actif lorsque la réserve de copies

Snapshot est épuisée, il peut donc être nécessaire d'augmenter la réserve de copies Snapshot si nécessaire. Vous pouvez également supprimer automatiquement les copies Snapshot lorsque la réserve est saturée.

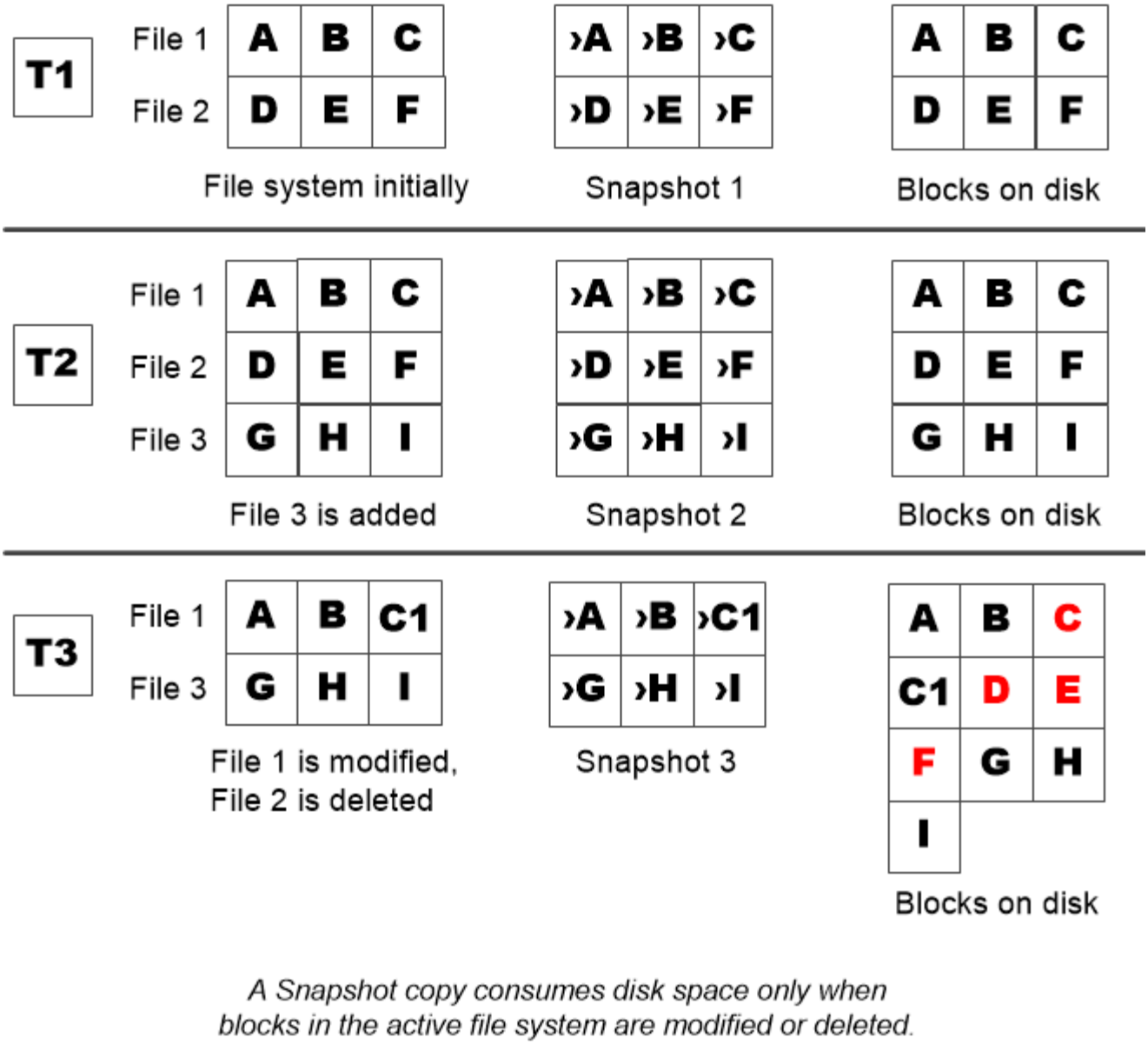
Quand augmenter la réserve de copies Snapshot

Lors du choix d'augmenter la réserve Snapshot, il est important de rappeler qu'une copie Snapshot n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot. Elle consomme de l'espace disque uniquement lorsque des blocs du système de fichiers actif sont modifiés ou supprimés.

Cela signifie que le taux de changement du système de fichiers est le principal facteur déterminant la quantité d'espace disque utilisée par les copies Snapshot. Quel que soit le nombre de copies Snapshot que vous créez, elles ne consomment pas d'espace disque si le système de fichiers actif n'a pas changé.

Un volume FlexVol contenant les journaux de transactions de base de données, par exemple, peut disposer d'une réserve de copies Snapshot pouvant atteindre 20 % pour prendre en compte son taux de modification supérieur. Vous souhaitez non seulement créer davantage de copies Snapshot pour capturer les mises à jour plus fréquentes de la base de données, mais également disposer d'une plus grande réserve de copies Snapshot pour gérer l'espace disque supplémentaire consommé par les copies Snapshot.

Une copie Snapshot se compose de pointeurs vers des blocs au lieu de copies de blocs. Vous pouvez considérer un pointeur comme une « réclamation » sur un bloc : la ONTAP « maintient » le bloc jusqu'à ce que la copie Snapshot soit supprimée.



La manière dont la suppression des fichiers protégés peut entraîner une diminution de l'espace fichier par rapport aux attentes

Une copie Snapshot pointe vers un bloc, même après la suppression du fichier utilisé par ce bloc. Cela explique pourquoi une réserve de copies Snapshot épuisée peut entraîner un résultat contre-intuitif, dans lequel la suppression d'un système de fichiers entier réduit l'espace disponible par rapport au système de fichiers occupé.

Prenons l'exemple suivant. Avant de supprimer des fichiers, le `df` la sortie de la commande est la suivante :

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Après avoir supprimé l'intégralité du système de fichiers et créé une copie Snapshot du volume, la `df` la

commande génère la sortie suivante :

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Comme le montre le résultat, l'intégralité des 3 Go utilisés auparavant par le système de fichiers actif est désormais utilisée par les copies Snapshot, en plus des 0.5 Go utilisés avant la suppression.

L'espace disque utilisé par les copies Snapshot dépasse maintenant la réserve de copies Snapshot, le débordement de 2.5 Go de « `spillss' » dans l'espace réservé aux fichiers actifs, vous laissant avec 0.5 Go d'espace libre pour les fichiers où vous aviez raisonnablement prévu des 3 Go.

Surveillez la consommation des copies Snapshot

Vous pouvez surveiller l'utilisation des copies Snapshot disque à l'aide du `df` commande. La commande affiche la quantité d'espace libre dans le système de fichiers actif et la réserve de copie Snapshot.

Étape

1. Afficher la consommation des copies Snapshot : `df`

   L'exemple suivant montre la consommation de disque de copie Snapshot :

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Vérifiez la réserve de copies Snapshot disponible sur un volume

Vous pouvez vérifier la quantité de réserve Snapshot disponible sur un volume en utilisant le `snapshot-reserve-available` paramètre avec le `volume show` commande.

Étape

1. Vérifier la réserve Snapshot disponible sur un volume :

   `vol show -vserver` *`SVM`* `-volume` *`volume`* `-fields snapshot-reserve-available`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre la réserve de copie Snapshot disponible pour `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ -------------------------
vs0     vol1   4.84GB
```

Modifiez la réserve de copies Snapshot

Vous pouvez vouloir configurer une plus grande réserve de copies Snapshot pour empêcher les copies Snapshot d'utiliser l'espace réservé pour le système de fichiers actif. La réserve Snapshot est réduite lorsque l'espace nécessaire aux copies Snapshot est réduit.

Étape

1. Modifiez la réserve Snapshot :

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-percent-snapshot-space` *`snap_reserve`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant définit la réserve de copie Snapshot pour `vol1` à 10 % :

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

Supprimer automatiquement les copies Snapshot

Vous pouvez utiliser le `volume snapshot autodelete modify` Commande permettant de déclencher la suppression automatique des copies Snapshot lorsque la réserve Snapshot est dépassée. Par défaut, les copies Snapshot les plus anciennes sont supprimées en premier.

Description de la tâche

Les clones de LUN et de fichiers sont supprimés lorsqu'il n'y a plus de copie Snapshot à supprimer.

Étape

1. Suppression automatique des copies Snapshot :

   `volume snapshot autodelete modify -vserver` *`SVM`* `-volume` *`volume`* `-enabled true|false -trigger volume|snap_reserve`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant illustre la suppression automatique des copies Snapshot de `vol1` Lorsque la réserve de copie Snapshot est épuisée :

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Restaurez les fichiers à partir de copies Snapshot

Restaurez un fichier à partir d'une copie Snapshot sur un client NFS ou SMB

Un utilisateur d'un client NFS ou SMB peut restaurer un fichier directement à partir d'une copie Snapshot sans l'intervention d'un administrateur de système de stockage.

Chaque répertoire du système de fichiers contient un sous-répertoire nommé `.snapshot` Accessible aux utilisateurs NFS et SMB. Le `.snapshot` Le sous-répertoire contient des sous-répertoires correspondant aux copies Snapshot du volume :

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Chaque sous-répertoire contient les fichiers référencés par la copie Snapshot. Si les utilisateurs suppriment ou remplacent accidentellement un fichier, ils peuvent restaurer ce dernier dans le répertoire de lecture-écriture parent en copiant le fichier du sous-répertoire Snapshot vers le répertoire de lecture-écriture :

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Activez et désactivez l'accès des clients NFS et SMB au répertoire de copie Snapshot

Pour déterminer si le répertoire de copie Snapshot est visible pour les clients NFS et SMB afin de restaurer un fichier ou une LUN à partir d'une copie Snapshot, vous pouvez activer et désactiver l'accès au répertoire de copie Snapshot à l'aide du `-snapdir -access` de la `volume modify` commande.

Étapes

1. Vérifier l'état d'accès au répertoire Snapshot :

   `volume show -vserver SVM_name -volume vol_name -fields snapdir-access`

   Exemple :

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

2. Activer ou désactiver l'accès au répertoire de copies Snapshot :

   `volume modify -vserver SVM_name -volume vol_name -snapdir-access true|false`

   L'exemple suivant active l'accès au répertoire de copie Snapshot sur vol1 :

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

Restaurez un seul fichier à partir d'une copie Snapshot

Vous pouvez utiliser le `volume snapshot restore-file` Commande permettant de restaurer un fichier ou une LUN à partir d'une copie Snapshot. Vous pouvez restaurer le fichier à un autre emplacement dans le volume en lecture-écriture parent si vous ne souhaitez pas remplacer un fichier existant.

Description de la tâche

Si vous restaurez une LUN existante, un clone de LUN est créé et sauvegardé sous le format d'une copie Snapshot. Pendant l'opération de restauration, vous pouvez lire et écrire sur la LUN.

Par défaut, les fichiers contenant des flux sont restaurés.

Étapes

1. Lister les copies Snapshot dans un volume :

   `volume snapshot show -vserver SVM -volume volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurer un fichier à partir d'une copie Snapshot :

   `volume snapshot restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-restore-path` *`destination_path`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant restaure le fichier `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Restaurez une partie d'un fichier à partir d'une copie Snapshot

Vous pouvez utiliser le `volume snapshot partial-restore-file` Commande permettant de restaurer une plage de données à partir d'une copie Snapshot vers une LUN ou vers un fichier de conteneur NFS ou SMB, en supposant que vous connaissez le décalage d'octet de départ des données et le nombre d'octets. Vous pouvez utiliser cette commande pour restaurer l'une des bases de données d'un hôte qui stocke plusieurs bases de données dans la même LUN.

Depuis ONTAP 9.12.1, la restauration partielle est disponible pour les volumes d'une relation SM-BC.

Étapes

1. Lister les copies Snapshot dans un volume :

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurer une partie d'un fichier à partir d'une copie Snapshot :

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   Le décalage d'octet de départ et le nombre d'octets doivent être des multiples de 4,096.

   L'exemple suivant restaure les 4,096 premiers octets du fichier `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Restaurer le contenu d'un volume à partir d'une copie Snapshot

Vous pouvez utiliser le `volume snapshot restore` Commande permettant de restaurer le contenu d'un volume à partir d'une copie Snapshot.

Description de la tâche

Si le volume possède des relations SnapMirror, répliquez manuellement toutes les copies miroir du volume immédiatement après la restauration à partir d'une copie Snapshot. Cette opération risque d'entraîner des copies miroir inutilisables qui doivent d'être supprimées et recréées.

1. Lister les copies Snapshot dans un volume :

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurer le contenu d'un volume à partir d'une copie Snapshot :

   `volume snapshot restore -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

   L'exemple suivant restaure le contenu de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1 -snapshot
daily.2013-01-25_0010
```

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.

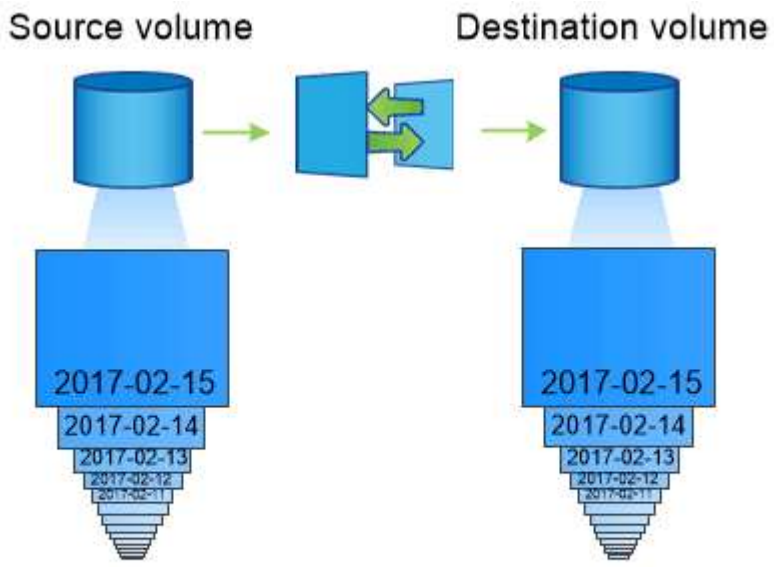
Si le site primaire assure toujours le service des données, il vous suffit de transférer les données requises vers celui-ci et ne transmet plus le tout aux clients depuis le miroir. Comme l'indique le cas de basculement, les contrôleurs du système secondaire doivent être équivalents ou presque équivalents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

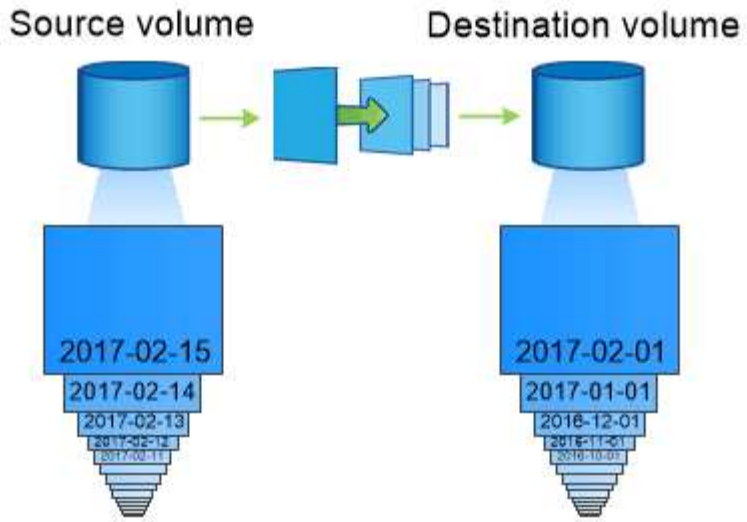
"Configuration synchrone de SnapMirror et bonnes pratiques"

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 ».

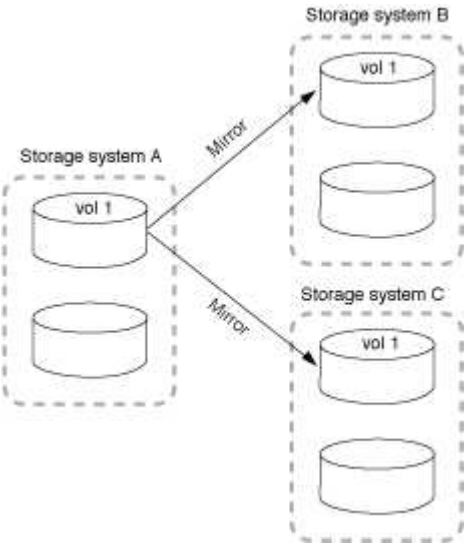
> Vous pouvez utiliser un déploiement *Fan-In* pour créer des relations de protection des données entre plusieurs systèmes primaires et un seul système secondaire. Chaque relation doit utiliser un volume différent sur le système secondaire.

> 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.

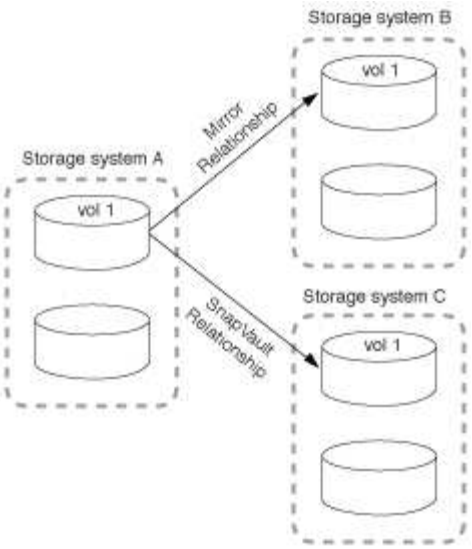
Fonctionnement des déploiements « Fan-Out »

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

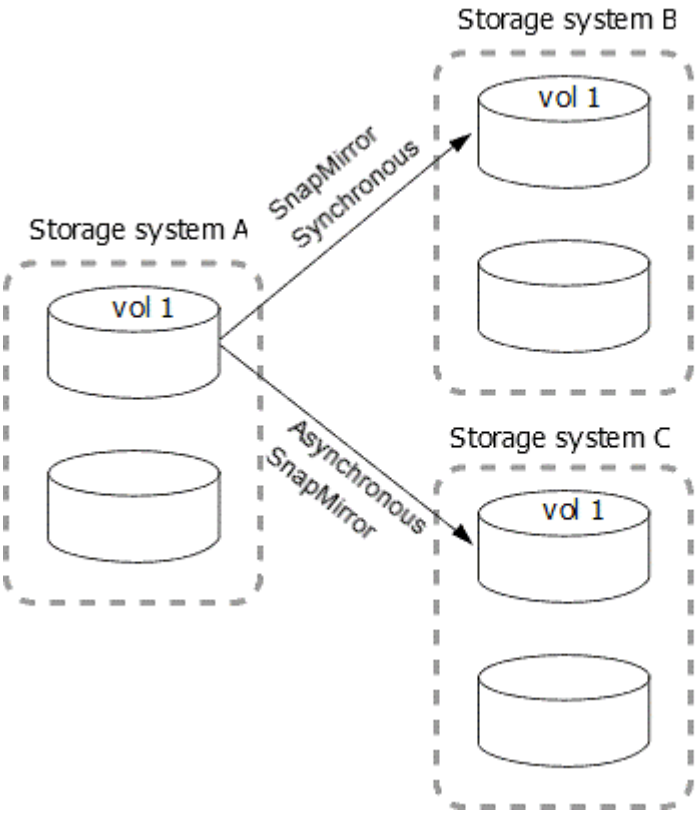
Un déploiement à plusieurs miroirs multiples sur « Fan-Out » comprend un volume source possédant une relation de mise en miroir sur plusieurs volumes secondaires.



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.

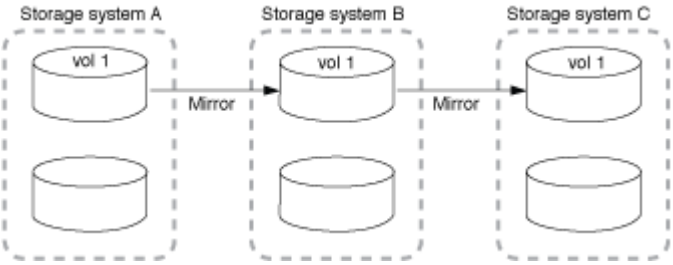


Fonctionnement des déploiements en cascade

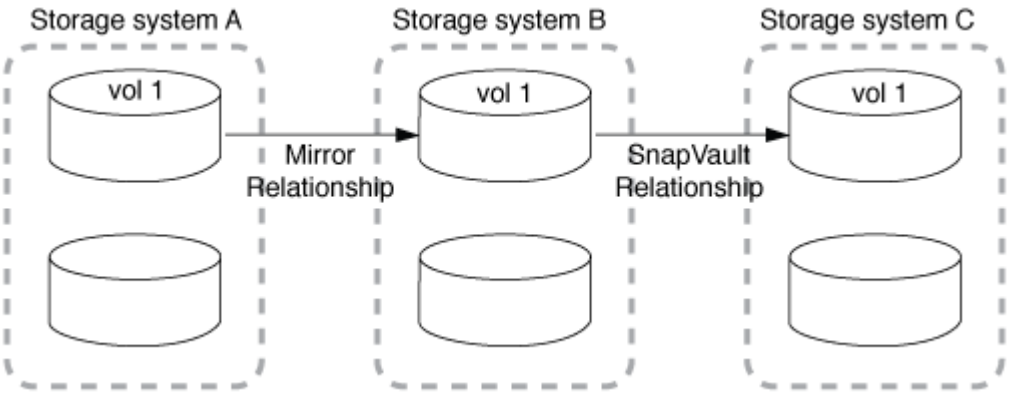
SnapMirror prend en charge les déploiements *mirror-mirror*, *mirror-vault*, *vault-mirror* et *vault-vault* cascade.

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.

Gérer la réplication de volume SnapMirror

Workflow de réplication SnapMirror

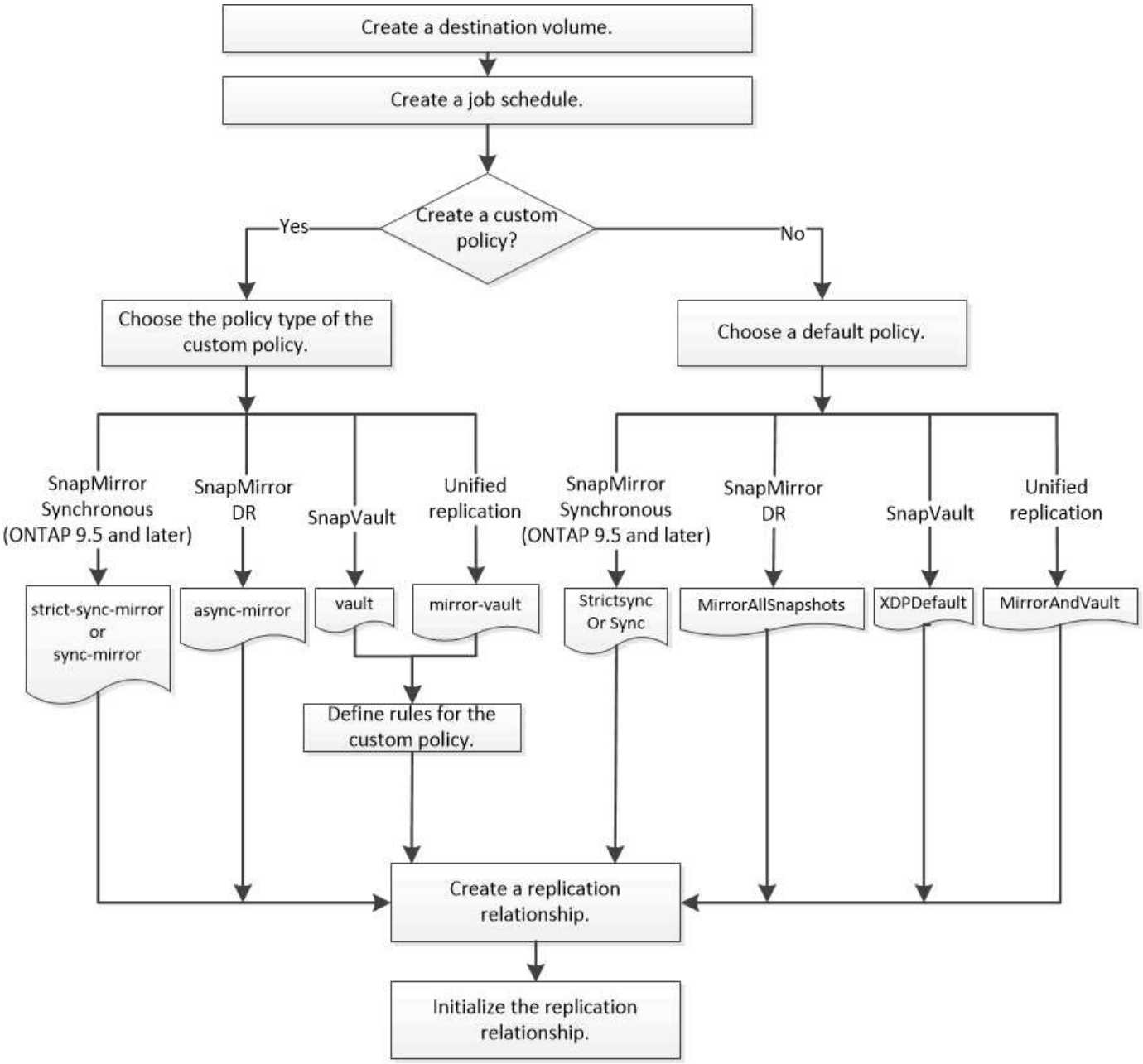
SnapMirror propose trois types de relation de protection des données : la reprise après incident SnapMirror, l'archivage (anciennement SnapVault) et la réplication unifiée. Vous pouvez suivre le même workflow de base pour configurer chaque type de relation.

Depuis la disponibilité générale d'ONTAP 9.9.1, la continuité de l'activité SnapMirror offre des objectifs de durée de restauration zéro (RTO nul) ou un basculement transparent des applications (TAF) pour permettre le basculement automatique des applications stratégiques dans les environnements SAN. SM-BC est pris en charge dans la configuration de deux clusters AFF ou de deux clusters ASA.

"Documentation NetApp : continuité de l'activité SnapMirror"

Pour chaque type de relation SnapMirror de protection des données, le workflow est identique : créer un volume de destination, créer un job schedule, spécifier une règle, créer et initialiser la relation.

Vous pouvez utiliser ONTAP 9.3 à partir de `snapmirror protect` commande permettant de configurer une relation de protection des données en une seule étape. Même si vous utilisez `snapmirror protect`, vous devez comprendre chaque étape du workflow.



Configurer une relation de réplication en une seule étape

Vous pouvez utiliser ONTAP 9.3 à partir de `snapmirror protect` commande permettant de configurer une relation de protection des données en une seule étape. Vous spécifiez une liste de volumes à répliquer, un SVM sur le cluster de destination, une planification de tâches et une policy SnapMirror. `snapmirror protect` se charge du reste.

Ce dont vous avez besoin

- Les clusters source et de destination et les SVM doivent être associés.

  "Cluster et SVM peering"

- La langue du volume de destination doit être identique à celle du volume source.

Description de la tâche

Le `snapmirror protect` La commande choisit un agrégat associé au SVM spécifié. Si aucun agrégat n'est associé à la SVM, il choisit tous les agrégats du cluster. Le choix de l'agrégat dépend de la quantité d'espace libre et du nombre de volumes sur l'agrégat.

Le `snapmirror protect` puis effectue les opérations suivantes :

- Crée un volume de destination avec un type et une quantité appropriés d'espace réservé pour chaque volume de la liste des volumes à répliquer.
- Configure une relation de réplication appropriée à la règle que vous spécifiez.
- Initialise la relation.

Le nom du volume de destination est du formulaire *`source_volume_name_dst`*. En cas de conflit avec le nom existant, la commande ajoute un nombre au nom du volume. Vous pouvez indiquer un préfixe et/ou un suffixe dans les options de la commande. Ce suffixe remplace le système fourni `dst` suffixe.

Dans ONTAP 9.3 et version antérieure, un volume de destination peut contenir jusqu'à 251 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies Snapshot

> L'initialisation peut prendre beaucoup de temps. `snapmirror protect` n'attend pas la fin de l'initialisation avant la fin du travail. Pour cette raison, vous devez utiliser le `snapmirror show` plutôt que le `job show` commande pour déterminer une fois l'initialisation terminée.

À partir de ONTAP 9.5, il est possible de créer des relations SnapMirror synchrone à l'aide de `snapmirror protect` commande.

Étape

1. Créer et initialiser une relation de réplication en une étape :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   > On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Le `-auto-initialize` l'option est définie par défaut sur « vrai ».

   L'exemple suivant crée et initialise une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorAllSnapshots` règle :

   ```
   cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
   -destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
   replication_daily
   ```

> Vous pouvez utiliser une police personnalisée si vous préférez. Pour plus d'informations, voir "Création d'une règle de réplication personnalisée".

L'exemple suivant crée et initialise une relation SnapVault à l'aide de la valeur par défaut `XDPDefault` règle :

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

L'exemple suivant crée et initialise une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` règle :

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

L'exemple suivant crée et initialise une relation SnapMirror synchrone à l'aide de la valeur par défaut `Sync` règle :

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

> Pour les règles de réplication SnapVault et unifiée, il est utile de définir une planification de la création d'une copie de la dernière copie Snapshot transférée sur la destination. Pour plus d'informations, voir "Définition d'un programme de création d'une copie locale sur la destination".

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Configurer une relation de réplication une étape à la fois

Créer un volume de destination

Vous pouvez utiliser le `volume create` commande située sur le volume de destination pour créer un volume de destination Le volume de destination doit avoir une taille égale ou supérieure à celle du volume source.

Étape

1. Créer un volume de destination :

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant crée un volume de destination de 2 Go nommé `volA_dst`:

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

Créer une planification de tâche de réplication

Vous pouvez utiliser le `job schedule cron create` commande pour créer une planification de tâche de réplication. La planification des tâches détermine lorsque SnapMirror met automatiquement à jour la relation de protection des données à laquelle la planification est attribuée.

Description de la tâche

Vous affectez un planning de travail lorsque vous créez une relation de protection des données. Si vous n'attribuez pas de programme de travail, vous devez mettre à jour la relation manuellement.

Étape

1. Création d'un programme de travail :

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

   Depuis ONTAP 9.10.1, vous pouvez inclure le vServer dans votre calendrier des tâches :

   `job schedule cron create -name` *`job_name`* `-vserver` *`Vserver_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   > La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation SnapMirror volume est de 5 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation SnapMirror volume est de 30 minutes.

   L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Personnaliser une règle de réplication

Création d'une règle de réplication personnalisée

Vous pouvez créer une stratégie de réplication personnalisée si la stratégie par défaut d'une relation n'est pas appropriée. Vous pouvez compresser les données d'un transfert

réseau, par exemple, ou modifier le nombre de tentatives de transfert de copies Snapshot par SnapMirror.

Vous pouvez utiliser une règle par défaut ou personnalisée lorsque vous créez une relation de réplication. Dans le cas d'une archivage personnalisé (anciennement SnapVault) ou d'une règle de réplication unifiée, vous devez définir une ou plusieurs *règles* qui déterminent les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour.vous pouvez également définir un calendrier pour la création de copies Snapshot locales sur le volume de destination.

Le *policy type* de la règle de réplication détermine le type de relation qu'elle prend en charge. Le tableau ci-dessous présente les types de stratégies disponibles.

Type de règle	Type de relation
mise en miroir asynchrone	Reprise sur incident SnapMirror
coffre-fort	SnapVault
coffre-fort	Réplication unifiée
miroir-synchro-strict	SnapMirror synchrone en mode StructSync (pris en charge à partir de ONTAP 9.5)
miroir synchrone	SnapMirror synchrone en mode synchrone (pris en charge à partir de ONTAP 9.5)

Lorsque vous créez une stratégie de réplication personnalisée, il est conseillé de modéliser la stratégie après une stratégie par défaut.

Étape

1. Création d'une règle de réplication personnalisée :

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror -comment comment
   -tries transfer_tries -transfer-priority low|normal -is-network-compression
   -enabled true|false
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   Depuis la version ONTAP 9.5, vous pouvez définir le planning de création d'un planning de copie Snapshot commun pour les relations SnapMirror synchrone à l'aide de la `-common-snapshot-schedule` paramètre. Par défaut, la planification commune de copies Snapshot pour les relations SnapMirror synchrone est d'une heure. Définissez une valeur de 30 minutes à deux heures pour la planification de copie Snapshot pour les relations SnapMirror synchrone.

   L'exemple suivant crée une règle de réplication personnalisée pour SnapMirror DR qui permet la compression réseau pour les transferts de données :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```

L'exemple suivant illustre la création d'une règle de réplication personnalisée pour SnapVault :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

L'exemple suivant crée une règle de réplication personnalisée pour la réplication unifiée :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

L'exemple suivant illustre la création d'une règle de réplication personnalisée pour la relation SnapMirror synchrone en mode StrictSync :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Une fois que vous avez terminé

Pour les types de règles « vault » et « miroir-coffre-fort », vous devez définir des règles qui déterminent les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour.

Utilisez le `snapmirror policy show` Commande pour vérifier que la règle SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Définir une règle pour une règle

Pour les règles personnalisées avec le type de règle « vault » ou « miroir-coffre-fort », vous devez définir au moins une règle qui détermine les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour. Vous pouvez également définir des règles pour les stratégies par défaut avec le type de stratégie « coffre-fort » ou « miroir-coffre-fort ».

Description de la tâche

Chaque règle avec le type de règle « vault » ou « miroir-coffre-fort » doit disposer d'une règle qui spécifie les copies Snapshot à répliquer. La règle « bimensuelle », par exemple, indique que seules les copies Snapshot affectées au label SnapMirror « bimensuel » doivent être répliquées. Vous spécifiez l'étiquette SnapMirror lors de la configuration de la règle Snapshot sur la source.

Chaque type de stratégie est associé à une ou plusieurs règles définies par le système. Ces règles sont automatiquement attribuées à une règle lorsque vous spécifiez son type de stratégie. Le tableau ci-dessous

présente les règles définies par le système.

Règle définie par le système	Utilisé dans les types de stratégie	Résultat
sm_créé	Async-mirror, mirror-vault, Sync, StrictSync	Une copie Snapshot créée par SnapMirror est transférée lors de l'initialisation et de la mise à jour.
all_source_snapshots	mise en miroir asynchrone	Les nouvelles copies Snapshot de la source sont transférées lors de l'initialisation et de la mise à jour.
tous les jours	coffre-fort,miroir-coffre-fort	Les nouvelles copies Snapshot de la source portant le label SnapMirror « `diotidienne » sont transférées lors de l'initialisation et de la mise à jour.
hebdomadaire	coffre-fort,miroir-coffre-fort	Les nouvelles copies Snapshot de la source portant l'étiquette SnapMirror « hebdomadaire » sont transférées lors de l'initialisation et de la mise à jour.
tous les mois	coffre-fort	Les nouvelles copies Snapshot de la source avec le libellé SnapMirror « `mensuel' » sont transférées lors de l'initialisation et de la mise à jour.
cohérent_app	Sync., StrictSync	Les copies snapshot portant le label SnapMirror « APP_cohérent » sur la source sont répliquées de manière synchrone sur la destination. Pris en charge à partir de ONTAP 9.7.

À l'exception du type de politique « async-mirror », vous pouvez spécifier des règles supplémentaires selon vos besoins, pour les stratégies par défaut ou personnalisées. Par exemple :

- Pour la valeur par défaut `MirrorAndVault` Politique, vous pouvez créer une règle appelée « deux mois » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux mois ».
- Dans le cas d'une règle personnalisée avec le type de règle « miroir-coffre-fort », vous pouvez créer une règle appelée « deux semaines » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux semaines ».

Étape

1. Définir une règle pour une règle :

   ```
   snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
   -label snapmirror-label -keep retention_count
   ```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-monthly` par défaut `MirrorAndVault` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-weekly` au personnalisé `my_snapvault` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `app_consistent` au personnalisé `Sync` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Vous pouvez ensuite répliquer les copies Snapshot à partir du cluster source correspondant à l'étiquette SnapMirror :

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Définissez un programme de création d'une copie locale sur la destination

Pour les relations SnapVault et de réplication unifiée, 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 la 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.

Description de la tâche

Vous spécifiez le planning de création d'une copie locale dans `-schedule` de la `snapmirror policy add-rule` commande.

Étape

1. Définissez un planning de création d'une copie locale sur la destination :

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. Pour obtenir un exemple de création d'un programme de travail, reportez-vous à la section "Création d'une planification de tâche de réplication".

L'exemple suivant ajoute un calendrier de création d'une copie locale par défaut `MirrorAndVault` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

L'exemple suivant ajoute un calendrier de création d'une copie locale à la personnalisée `my_unified` règle :

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Créer une relation de réplication

La relation entre le volume source dans le stockage primaire et le volume de destination dans le stockage secondaire est appelée « relation de protection des données »._ vous pouvez utiliser le `snapmirror create` Créez des relations de protection des données avec SnapMirror de reprise après incident, SnapVault ou réplication unifiée.

Ce dont vous avez besoin

- Les clusters source et de destination et les SVM doivent être associés.

  "Cluster et SVM peering"

- La langue du volume de destination doit être identique à celle du volume source.

Description de la tâche

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. 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	MirrorAllsnapshots (reprise après incident SnapMirror)
XDP	XDP	XDPDefault (SnapVault)

Voir également les exemples de la procédure ci-dessous.

Les seules exceptions à la conversion sont les suivantes :

- Les relations de protection des données des SVM continuent à être par défaut en mode DP.

  Spécifiez explicitement XDP pour obtenir le mode XDP par défaut `MirrorAllSnapshots` politique.

- Les relations de protection des données de partage de charge continuent à être par défaut en mode DP.
- Les relations de protection des données SnapLock continuent à être par défaut en mode DP.
- 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.

Dans ONTAP 9.3 et version antérieure, un volume de destination peut contenir jusqu'à 251 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies Snapshot

La prise en charge des relations SnapMirror synchrone est prise en charge à partir de la version ONTAP 9.5

Étape

1. Depuis le cluster destination, créer une relation de réplication :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

> Le `schedule` Le paramètre n'est pas applicable lors de la création de relations SnapMirror synchrone.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorLatest` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorLatest
```

L'exemple suivant illustre la création d'une relation SnapVault à l'aide de la valeur par défaut `XDPDefault` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
XDPDefault
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` règle :

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination-path
svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAndVault
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la commande personnalisée `my_unified` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

L'exemple suivant illustre la création d'une relation SnapMirror synchrone à l'aide de la valeur par défaut `Sync` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

L'exemple suivant illustre la création d'une relation SnapMirror synchrone à l'aide de la valeur par défaut `StrictSync` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

L'exemple suivant illustre la création d'une relation SnapMirror DR. Lorsque le type DP est automatiquement converti en XDP et sans policy spécifiée, la règle passe par défaut sur le `MirrorAllSnapshots` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

L'exemple suivant illustre la création d'une relation SnapMirror DR. Sans type ni règle définie, la règle de gestion par défaut est définie sur le `MirrorAllSnapshots` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

L'exemple suivant illustre la création d'une relation SnapMirror DR. Sans règle spécifiée, la règle est définie par défaut sur le `XDPDefault` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

L'exemple suivant illustre la création d'une relation SnapMirror synchrone avec la règle prédéfinie `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

> La règle prédéfinie `SnapCenterSync` est de type `Sync`. Cette règle réplique toute copie Snapshot créée avec le `snapmirror-label` de « cohérent_app ».

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Informations associées

- "Créez et supprimez des volumes de test de basculement SnapMirror".

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Configurer les miroirs et les coffres-forts"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la sauvegarde de volume avec SnapVault"

Initialiser une relation de réplication

Pour tous les types de relations, l'initialisation effectue un *transfert de base* : il effectue une copie Snapshot du volume source, puis transfère cette copie et tous les blocs de données qu'elle référence au volume de destination. Dans le cas contraire, le contenu du transfert dépend de la police.

Ce dont vous avez besoin

Les clusters source et de destination et les SVM doivent être associés.

"Cluster et SVM peering"

Description de la tâche

L'initialisation peut prendre beaucoup de temps. Vous pouvez exécuter le transfert de base en dehors des heures creuses.

La prise en charge des relations SnapMirror synchrone est prise en charge à partir de la version ONTAP 9.5

Étape

1. Initialiser une relation de réplication :

   ```
   snapmirror initialize -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

   L'exemple suivant initialise la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Exemple : configurer une cascade de coffre-fort

Un exemple montre en termes concrets comment vous pouvez configurer des relations de réplication une étape à la fois. Vous pouvez utiliser le déploiement Vault-vault en cascade configuré dans cet exemple pour conserver plus de 251 copies Snapshot

étiquetées « my-hebdomadaire ».

Ce dont vous avez besoin

- Les clusters source et de destination et les SVM doivent être associés.
- Vous devez exécuter ONTAP 9.2 ou version ultérieure. Les cascades de coffre-fort ne sont pas prises en charge dans les versions précédentes de ONTAP.

Description de la tâche

L'exemple suppose ce qui suit :

- Vous avez configuré des copies Snapshot sur le cluster source avec les libellés SnapMirror « my-Daily », « my-hebdomadaire » et « my-monmensuel ».
- Des volumes de destination nommés « Vola » ont été configurés sur les clusters de destination secondaire et tertiaire.
- Vous avez configuré des planifications de tâches de réplication nommées « my_snapvault » sur les clusters de destination secondaire et tertiaire.

L'exemple montre comment créer des relations de réplication basées sur deux règles personnalisées :

- La politique « napvault_Secondary » conserve 3 7 copies Snapshot par jour, 5 52 hebdomadaires et 3 180 mois dans le cluster de destination secondaire.
- La « politique napvault_tertiaire » conserve 250 copies Snapshot hebdomadaires sur le cluster de destination tertiaire.

Étapes

1. Sur le cluster de destination secondaire, créez la stratégie « napvault_Secondary » :

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment “Policy on secondary for vault to vault cascade” -vserver
   svm_secondary
   ```

2. Sur le cluster de destination secondaire, définissez la règle "my-Daily" pour la politique :

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. Sur le cluster de destination secondaire, définissez la règle "my-hebdomadaire" pour la politique :

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-weekly -keep 52 -vserver svm_secondary
   ```

4. Sur le cluster de destination secondaire, définissez la règle "mois-mois" pour la politique :

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-monthly -keep 180 -vserver svm_secondary
   ```

5. Sur le cluster de destination secondaire, vérifiez la policy :

   ```
   cluster_secondary::> snapmirror policy show snapvault_secondary -instance
   ```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      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: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. Sur le cluster de destination secondaire, créez la relation avec le cluster source :

   ```
   cluster_secondary::> snapmirror create -source-path svm_primary:volA
   -destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
   snapvault_secondary
   ```

7. Sur le cluster destination secondaire, initialiser la relation avec le cluster source :

   ```
   cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
   -destination-path svm_secondary:volA
   ```

8. Sur le cluster de destination tertiaire, créez la stratégie "napvault_tertiaire" :

   ```
   cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
   vault -comment “Policy on tertiary for vault to vault cascade” -vserver
   svm_tertiary
   ```

9. Sur le cluster de destination tertiaire, définissez la règle "semaine-moyenne" pour la politique :

   ```
   cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
   -snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
   ```

10. Sur le cluster de destination tertiaire, vérifiez la règle :

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                     Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      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: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. Sur le cluster de destination tertiaire, créez la relation avec le cluster secondaire :

    ```
    cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
    -destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
    snapvault_tertiary
    ```

12. Sur le cluster destination tertiaire, initialisez la relation avec le cluster secondaire :

    ```
    cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
    -destination-path svm_tertiary:volA
    ```

Convertir une relation de type DP existante en XDP

Si vous procédez à une mise à niveau vers ONTAP 9.12.1 ou version ultérieure, vous devez convertir les relations de type DP en relation XDP avant la mise à niveau. ONTAP 9.12.1 et versions ultérieures ne prennent pas en charge les relations de type DP. Vous pouvez facilement convertir une relation de type DP existante en XDP pour tirer parti de SnapMirror flexible à la version.

Description de la tâche

- SnapMirror ne convertit pas automatiquement les relations de type DP existantes en relation XDP. Pour convertir la relation, vous devez rompre et supprimer la relation existante, créer une nouvelle relation XDP et resynchroniser la relation. Pour plus d'informations, reportez-vous à la section "XDP remplace DP par défaut SnapMirror".

- Lors de la planification de votre conversion, notez que la préparation en arrière-plan et la phase d'entreposage des données d'une relation SnapMirror XDP peuvent prendre un certain temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.

> Après avoir converti un type de relation SnapMirror de DP en XDP, les paramètres d'espace, tels que la taille automatique et la garantie d'espace ne sont plus répliqués vers la destination.

Étapes

1. Depuis le cluster de destination, s'assurer que la relation SnapMirror est de type DP, que l'état du miroir est SnapMirror, que l'état de la relation est inactif et que la relation fonctionne correctement :

```
snapmirror show -destination-path <SVM:volume>
```

L'exemple suivant montre la sortie du `snapmirror show` commande :

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

> Vous pouvez le trouver utile de conserver une copie du `snapmirror show` sortie de la commande pour garder le suivi existant des paramètres de relation.

2. Depuis les volumes source et de destination, assurez-vous que les deux volumes disposent d'une copie Snapshot commune :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre le `volume snapshot show` sortie pour les volumes source et de destination :

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Pour vous assurer que les mises à jour planifiées ne s'exécutent pas pendant la conversion, mettez au repos la relation de type DP existante :

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au "page de manuel".

> On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant arrête la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Casser la relation de type DP existante :

```
snapmirror break -destination-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au "page de manuel".

> On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant rompt la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Si la suppression automatique des copies Snapshot est activée sur le volume de destination, désactivez-la :

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

L'exemple suivant désactive la suppression automatique de la copie Snapshot sur le volume de destination `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Supprimez la relation DP-type existante :

```
snapmirror delete -destination-path <SVM:volume>
```

Pour connaître la syntaxe complète de la commande, reportez-vous au "page de manuel".

> On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant supprime la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Relâcher la relation de reprise d'activité SVM d'origine sur la source :

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

L'exemple suivant permet de libérer la relation de SVM Disaster Recovery :

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. Vous pouvez utiliser la sortie que vous avez conservée de l' `snapmirror show` Commande pour créer la nouvelle relation de type XDP :

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

La nouvelle relation doit utiliser le même volume source et destination. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

> On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

L'exemple suivant illustre la création d'une relation de reprise d'activité SnapMirror entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup` utilisation de la valeur par défaut `MirrorAllSnapshots` règle :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resynchronisation des volumes source et de destination :

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Pour améliorer le temps de resynchronisation, vous pouvez utiliser le `-quick-resync` mais vous devez savoir que vous pouvez perdre des économies en matière d'efficacité du stockage. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man : "Commande SnapMirror resync".

> On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant resynchronque la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Si vous avez désactivé la suppression automatique de copies Snapshot, réactivez-la :

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Une fois que vous avez terminé

1. Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée.
2. Une fois que le volume de destination SnapMirror XDP commence à mettre à jour les copies Snapshot, comme défini par la règle SnapMirror, utilisez les valeurs de sortie de `snapmirror list-destinations` Commande depuis le cluster source pour afficher la nouvelle relation SnapMirror XDP

Convertir le type de relation SnapMirror

SnapMirror synchrone est pris en charge à partir de la version ONTAP 9.5 Vous pouvez convertir une relation SnapMirror asynchrone en relation SnapMirror synchrone ou vice-versa, sans avoir à effectuer de transfert de base.

Description de la tâche

Vous ne pouvez pas convertir une relation SnapMirror asynchrone en relation SnapMirror synchrone ou vice-versa en modifiant la règle SnapMirror

Étapes

- **Conversion d'une relation SnapMirror asynchrone en relation SnapMirror synchrone**

  a. Depuis le cluster destination, supprimez la relation SnapMirror asynchrone :

  ```
  snapmirror delete -destination-path SVM:volume
  ```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

b. Depuis le cluster source, libérer la relation SnapMirror sans supprimer les copies Snapshot courantes :

   `snapmirror release -relationship-info-only true -destination-path` *`dest_SVM:dest_volume`*

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. Depuis le cluster destination, créez une relation SnapMirror synchrone :

   `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path` *`dest_SVM:dest_volume`* `-policy sync-mirror`

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. Resynchroniser la relation SnapMirror synchrone :

   `snapmirror resync -destination-path` *`dest_SVM:dest_volume`*

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- **Conversion d'une relation SnapMirror synchrone en relation SnapMirror asynchrone**

a. Depuis le cluster de destination, suspendre la relation SnapMirror synchrone existante :

   `snapmirror quiesce -destination-path dest_SVM:dest_volume`

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. Depuis le cluster destination, supprimez la relation SnapMirror asynchrone :

   `snapmirror delete -destination-path` *`SVM:volume`*

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. Depuis le cluster source, libérer la relation SnapMirror sans supprimer les copies Snapshot courantes :

   `snapmirror release -relationship-info-only true -destination-path` *`dest_SVM:dest_volume`*

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. Depuis le cluster destination, créez une relation SnapMirror asynchrone :

   `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path` *`dest_SVM:dest_volume`* `-policy MirrorAllSnapshots`

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Resynchroniser la relation SnapMirror synchrone :

   `snapmirror resync -destination-path` *`dest_SVM:dest_volume`*

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Convertir le mode d'une relation SnapMirror synchrone

La prise en charge des relations SnapMirror synchrone est prise en charge à partir de la version ONTAP 9.5 Vous pouvez convertir le mode d'une relation SnapMirror synchrone de StrictSync en mode synchrone ou inversement.

Description de la tâche

Vous ne pouvez pas modifier la règle d'une relation SnapMirror synchrone pour convertir son mode.

Étapes

1. Depuis le cluster de destination, suspendre la relation SnapMirror synchrone existante :

   `snapmirror quiesce -destination-path dest_SVM:dest_volume`

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. Depuis le cluster de destination, supprimez la relation SnapMirror synchrone existante :

   `snapmirror delete -destination-path dest_SVM:dest_volume`

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. Depuis le cluster source, libérer la relation SnapMirror sans supprimer les copies Snapshot courantes :

   `snapmirror release -relationship-info-only true -destination-path dest_SVM:dest_volume`

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. Depuis le cluster de destination, créez une relation SnapMirror synchrone en spécifiant le mode vers lequel vous souhaitez convertir la relation SnapMirror synchrone :

   ```
   snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_volume
   -policy Sync|StrictSync
   ```

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. Depuis le cluster de destination, resynchroniser la relation SnapMirror :

   ```
   snapmirror resync -destination-path dest_SVM:dest_volume
   ```

   ```
   cluster2::> snapmirror resync -destination-path vs1_dr:vol1
   ```

Créez et supprimez des volumes de test de basculement SnapMirror

Depuis la version ONTAP 9.14.1, vous pouvez utiliser System Manager pour créer un clone de volume afin de tester le basculement SnapMirror et la reprise d'activité sans interrompre la relation SnapMirror active. Une fois le test terminé, vous pouvez nettoyer les données associées et supprimer le volume test.

Créez un volume de test de basculement SnapMirror

Description de la tâche

- Vous pouvez effectuer des tests de basculement sur des relations SnapMirror synchrones et asynchrones.
- Un clone de volume est créé pour effectuer le test de reprise d'activité.
- Le volume clone est créé sur la même machine virtuelle de stockage que la destination SnapMirror.
- Vous pouvez utiliser les relations FlexVol et FlexGroup SnapMirror.
- Si un clone test existe déjà pour la relation sélectionnée, vous ne pouvez pas créer un autre clone pour cette relation.
- Les relations de coffre-fort SnapLock ne sont pas prises en charge.

Avant de commencer

- Vous devez être un administrateur de cluster.
- La licence SnapMirror doit être installée sur le cluster source et le cluster destination.

Étapes

1. Sur le cluster de destination, sélectionnez **protection > relations**.
2. Sélectionnez ⋮ En regard de la source de la relation et choisissez **Test Failover**.

3. Dans la fenêtre **Test Failover**, sélectionnez **Test Failover**.
4. Sélectionnez **stockage > volumes** et vérifiez que le volume de basculement test est répertorié.
5. Sélectionnez **stockage > partager**.
6. Cliquez sur + Add Et choisissez **partager**.
7. Dans la fenêtre **Ajouter un partage**, saisissez un nom pour le partage dans le champ **Nom du partage**.
8. Dans le champ **Folder**, sélectionnez **Browse**, sélectionnez le volume clone test et **Save**.
9. Au bas de la fenêtre **Ajouter un partage**, choisissez **Enregistrer**.
10. Ouvrez le partage sur le client et vérifiez que le volume test dispose de capacités de lecture et d'écriture.

Nettoyez les données de basculement et supprimez le volume test

Une fois le test de basculement terminé, vous pouvez nettoyer toutes les données associées au volume test et les supprimer.

Étapes

1. Sur le cluster de destination, sélectionnez **protection > relations**.
2. Sélectionnez ⋮ En regard de la source de la relation et choisissez **nettoyer le basculement de test**.
3. Dans la fenêtre **nettoyage du basculement de test**, sélectionnez **nettoyage**.
4. Sélectionnez **stockage > volumes** et vérifiez que le volume test a été supprimé.

Activation des données à partir d'un volume de destination de reprise après incident SnapMirror

Rendre le volume de destination inscriptible

Vous devez rendre le volume de destination inscriptible avant de pouvoir transmettre les données du volume à des clients. Vous pouvez utiliser le `snapmirror quiesce` commande pour arrêter les transferts programmés vers la destination, le `snapmirror abort` pour arrêter les transferts en cours, et le `snapmirror break` commande permettant de rendre la destination inscriptible.

Description de la tâche

Cette tâche doit être effectuée depuis le SVM de destination ou le cluster de destination.

Étapes

1. Arrêter les transferts programmés vers la destination :

   ```
   snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant arrête les transferts programmés entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

2. Arrêter les transferts en cours vers la destination :

   `snapmirror abort -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Cette étape n'est pas requise pour les relations SnapMirror synchrone (prise en charge à partir de ONTAP 9.5).

   L'exemple suivant arrête les transferts en cours entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

3. Interrompre la relation SnapMirror DR :

   `snapmirror break -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant rompt la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Service des données à partir d'une destination SnapMirror"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la reprise après incident de volume"

Configurer le volume de destination pour l'accès aux données

Une fois le volume de destination inscriptible, vous devez configurer le volume pour l'accès aux données. Les clients NAS, le sous-système NVMe et les hôtes SAN peuvent accéder aux données à partir du volume de destination jusqu'à ce que le volume source

soit réactivé.

Environnement NAS :

1. Monter le volume NAS sur l'espace de noms en utilisant la même Junction path que le volume source a été monté sur dans le SVM source.
2. Appliquez les ACL appropriées aux partages SMB du volume de destination.
3. Attribuez les export-policies NFS au volume de destination.
4. Appliquer les règles de quota au volume de destination
5. Redirection des clients vers le volume de destination.
6. Remontez les partages NFS et SMB sur les clients.

Environnement SAN :

1. Mappez les LUN du volume sur le groupe initiateur approprié.
2. Pour iSCSI, créez des sessions iSCSI des initiateurs hôtes SAN vers les LIF SAN.
3. Sur le client SAN, effectuez une nouvelle analyse de stockage pour détecter les LUN connectés.

Pour plus d'informations sur l'environnement NVMe, reportez-vous à la section "Administration SAN".

Réactiver le volume source d'origine

Vous pouvez rétablir la relation initiale de protection des données entre les volumes source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination.

Description de la tâche

- La procédure ci-dessous suppose que la ligne de base du volume source d'origine est intacte. Si la base n'est pas intacte, vous devez créer et initialiser la relation entre le volume dont vous accédez aux données et le volume source d'origine avant d'effectuer la procédure.
- La préparation en arrière-plan et la phase d'entreposage des données d'une relation SnapMirror XDP peuvent prendre un certain temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.

Étapes

1. Inverser la relation de protection des données d'origine :

   ```
   snapmirror resync -source-path SVM:volume -destination-path SVM:volume
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine. Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe. Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant inverse la relation entre le volume source d'origine, `volA` marche `svm1`et le volume que vous servant de données, `volA_dst` marche `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

2. Lorsque vous êtes prêt à rétablir l'accès aux données à la source d'origine, l'accès au volume de destination d'origine est interrompu. L'une des façons de faire est d'arrêter le SVM de destination d'origine :

   `vserver stop -vserver SVM`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM destination d'origine ou du cluster destination d'origine. Cette commande arrête l'accès de l'utilisateur à l'ensemble du SVM de destination d'origine. Vous pouvez arrêter l'accès au volume de destination d'origine à l'aide d'autres méthodes.

   L'exemple suivant arrête le SVM destination original :

```
cluster_dst::> vserver stop svm_backup
```

3. Mettre à jour la relation inversée :

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

   L'exemple suivant met à jour la relation entre le volume que vous servant des données, `volA_dst` marche `svm_backup`, et le volume source d'origine, `volA` marche `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

4. Depuis le SVM source d'origine ou le cluster source d'origine, arrêter les transferts programmés pour la relation inversée :

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

   L'exemple suivant illustre la fin des transferts programmés entre le volume de destination d'origine. `volA_dst` marche `svm_backup`, et le volume source d'origine, `volA` marche `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

5. Lorsque la mise à jour finale est terminée et que la relation indique « suspendu » pour l'état de la relation, exécutez la commande suivante à partir du SVM source d'origine ou du cluster source d'origine pour interrompre la relation inversée :

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source.

   L'exemple suivant rompt la relation entre le volume de destination d'origine, `volA_dst` marche `svm_backup`, et le volume source d'origine, `volA` marche `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. Depuis le SVM source d'origine ou le cluster source d'origine, supprimer la relation de protection des données inversée :

   `snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

   L'exemple suivant supprime la relation inversée entre le volume source d'origine, `volA` marche `svm1`et le volume que vous servant de données, `volA_dst` marche `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Libérer la relation inverse de la SVM destination d'origine ou du cluster destination d'origine.

   `snapmirror release -source-path SVM:volume -destination-path SVM:volume`

   > Vous devez exécuter cette commande à partir du SVM destination d'origine ou du cluster destination d'origine.

   L'exemple suivant libère la relation inversée entre le volume de destination d'origine, `volA_dst` marche `svm_backup`, et le volume source d'origine, `volA` marche `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Rétablir la relation de protection des données d'origine à partir de la destination d'origine :

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant rétablit la relation entre le volume source d'origine, `volA` marche `svm1`, et le volume de destination d'origine, `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Si besoin démarrer le SVM de destination d'origine :

   `vserver start -vserver` *`SVM`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant démarre le SVM de destination d'origine :

```
cluster_dst::> vserver start svm_backup
```

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Restaurer les fichiers à partir d'un volume de destination SnapMirror

Restaurez un seul fichier, LUN ou namespace NVMe à partir d'une destination SnapMirror

Vous pouvez restaurer un seul fichier, une LUN, un ensemble de fichiers ou de LUN à partir d'une copie Snapshot ou un namespace NVMe à partir d'un volume de destination SnapMirror. À partir de ONTAP 9.7, vous pouvez également restaurer les espaces de noms NVMe à partir d'une destination SnapMirror synchrone. Vous pouvez restaurer des fichiers vers le volume source d'origine ou vers un volume différent.

Ce dont vous avez besoin

Pour restaurer un fichier ou une LUN à partir d'une destination SnapMirror synchrone (prise en charge à partir de ONTAP 9.5), vous devez d'abord supprimer et libérer la relation.

Description de la tâche

Le volume vers lequel vous restaurez des fichiers ou des LUN (le volume de destination) doit être un volume en lecture-écriture :

- SnapMirror effectue une *restauration incrémentielle* si les volumes source et de destination ont une copie Snapshot commune (comme c'est généralement le cas lors de la restauration vers le volume source d'origine).
- Sinon, SnapMirror exécute une *restauration de base*, dans laquelle la copie Snapshot spécifiée et tous les blocs de données qui lui sont transférés vers le volume de destination.

Étapes

1. Lister les copies Snapshot dans le volume de destination :

   `volume snapshot show -vserver SVM -volume volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les copies Snapshot sur le `vserverB:secondary1` destination :

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaurer un seul fichier ou une LUN, ou un ensemble de fichiers ou de LUN à partir d'une copie Snapshot dans un volume de destination SnapMirror :

   `snapmirror restore -source-path SVM:volume|cluster://SVM/volume, … -destination-path SVM:volume|cluster://SVM/volume, … -source-snapshot snapshot -file-list source_file_path,@destination_file_path`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

La commande suivante restaure les fichiers `file1` et `file2` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`, au même emplacement dans le système de fichiers actif du volume source d'origine `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

La commande suivante restaure les fichiers `file1` et `file2` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`, à un autre emplacement dans le système de fichiers actif du volume source d'origine `primary1`.

Le chemin du fichier de destination commence par le symbole @ suivi du chemin du fichier à partir de la racine du volume source d'origine. Dans cet exemple, `file1` est restauré sur `/dir1/file1.new` et le fichier 2 est restauré dans `/dir2.new/file2` marche `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

La commande suivante restaure les fichiers `file1` et `file3` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`, à différents emplacements dans le système de fichiers actif du volume source d'origine `primary1`, et restaure `file2` de `snap1` au même emplacement dans le système de fichiers actif de `primary1`.

Dans cet exemple, le fichier `file1` est restauré sur `/dir1/file1.new` et `file3` est restauré sur `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Restaurer le contenu d'un volume à partir d'une destination SnapMirror

Vous pouvez restaurer le contenu d'un volume entier à partir d'une copie Snapshot dans un volume de destination SnapMirror. Vous pouvez restaurer le contenu du volume vers le volume source d'origine ou vers un volume différent.

Description de la tâche

Le volume de destination de l'opération de restauration doit être l'un des suivants :

- Un volume de lecture/écriture, dans lequel cas SnapMirror exécute une *restauration incrémentielle*, à condition que les volumes source et de destination aient une copie Snapshot commune (comme c'est généralement le cas lors de la restauration vers le volume source d'origine).

  > La commande échoue si une copie Snapshot commune n'est pas disponible. Vous ne pouvez pas restaurer le contenu d'un volume sur un volume en lecture-écriture vide.

- Un volume de protection des données vide, dans lequel cas SnapMirror exécute une *restauration de base*, dans lequel la copie Snapshot spécifiée et tous les blocs de données qui lui font référence sont transférés vers le volume source.

La restauration du contenu d'un volume constitue une opération perturbateur. Lors de l'exécution d'une opération de restauration, le trafic SMB ne doit pas être exécuté sur le volume primaire SnapVault.

Si la compression est activée sur le volume de destination pour l'opération de restauration et que la compression n'est pas activée sur le volume source, désactivez la compression sur le volume de destination. Vous devez réactiver la compression une fois l'opération de restauration terminée.

Toute règle de quotas définie pour le volume de destination est désactivée avant la restauration effectuée. Vous pouvez utiliser le `volume quota modify` commande permettant de réactiver les règles de quota une fois l'opération de restauration terminée.

Étapes

1. Lister les copies Snapshot dans le volume de destination :

   ```
   volume snapshot show -vserver <SVM> -volume <volume>
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les copies Snapshot sur le `vserverB:secondary1` destination :

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaurer le contenu d'un volume à partir d'une copie Snapshot dans un volume de destination SnapMirror :

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
   <snapshot>
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez exécuter cette commande à partir du SVM source d'origine ou du cluster source d'origine.

   La commande suivante restaure le contenu du volume source d'origine `primary1` A partir de la copie Snapshot `daily.2013-01-25_0010` dans le volume de destination d'origine `secondary1`:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Remontez le volume restauré et redémarrez toutes les applications qui utilisent le volume.

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Restaurez un volume à partir d'une copie Snapshot antérieure"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la restauration de volume à l'aide de SnapVault"

Mettre à jour une relation de réplication manuellement

Vous devrez peut-être mettre à jour une relation de réplication manuellement si une mise à jour échoue, car le volume source a été déplacé.

Description de la tâche

SnapMirror interrompt tous les transferts depuis un volume source déplacé jusqu'à ce que vous mette à jour la relation de réplication manuellement.

La prise en charge des relations SnapMirror synchrone est prise en charge à partir de la version ONTAP 9.5 Bien que les volumes source et de destination soient synchronisés à tout moment dans ces relations, la vue du cluster secondaire est synchronisée avec la vue principale uniquement toutes les heures. Si vous souhaitez afficher les données ponctuelles sur la destination, vous devez effectuer une mise à jour manuelle en exécutant le `snapmirror update` commande.

Étape

1. Mettre à jour une relation de réplication manuellement :

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

> On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant met à jour la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Resynchroniser une relation de réplication

Vous devez resynchroniser une relation de réplication après avoir créé un volume de destination inscriptible, après une mise à jour échoue, car une copie Snapshot commune n'existe pas sur les volumes source et de destination, ou si vous souhaitez modifier la règle de réplication pour la relation.

Description de la tâche

- Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.
- La resynchronisation des volumes qui font partie d'une configuration « fan-out » ou en cascade peut prendre plus de temps. Il n'est pas rare de voir la relation SnapMirror indiquant l'état « préparation » pour une période prolongée.

Étape

1. Resynchronisation des volumes source et de destination :

   `snapmirror resync -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -type DP|XDP -policy` *`policy`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

   L'exemple suivant resynchronque la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Supprime une relation de réplication de volume

Vous pouvez utiliser le `snapmirror delete` et `snapmirror release` commandes permettant de supprimer une relation de réplication de volume. Vous pouvez ensuite supprimer manuellement les volumes de destination inutiles.

Description de la tâche

Le `snapmirror release` Commande permet de supprimer toutes les copies Snapshot créées par SnapMirror de la source. Vous pouvez utiliser le `-relationship-info-only` Option pour conserver les copies Snapshot.

Étapes

1. Arrêter la relation de réplication :

   `snapmirror quiesce -destination-path` *`SVM:volume|cluster://SVM/volume`*

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

2. (Facultatif) si vous souhaitez que le volume de destination soit un volume de lecture/écriture, romprez la relation de réplication. Vous pouvez ignorer cette étape si vous prévoyez de supprimer le volume de destination ou si vous n'avez pas besoin d'un volume en lecture/écriture :

   `snapmirror break -source-path SVM:volume|cluster://SVM/volume, … -destination -path SVM:volume|cluster://SVM/volume, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

3. Supprimez la relation de réplication :

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   On doit exécuter cette commande depuis le cluster de destination ou le SVM de destination.

   L'exemple suivant supprime la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

4. Libérer les informations de relation de réplication depuis le SVM source :

   `snapmirror release -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination-path` *`SVM:volume|cluster://SVM/volume, …`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   Vous devez exécuter cette commande à partir du cluster source ou du SVM source.

   L'exemple suivant publie des informations pour la relation de réplication spécifiée à partir du SVM source

svm1:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Gérer l'efficacité du stockage

SnapMirror préserve l'efficacité du stockage sur les volumes source et de destination, à une exception près lorsque la compression des données post-traitement est activée sur le volume de destination. Dans ce cas, l'efficacité du stockage n'est plus sur la destination. Pour corriger ce problème, vous devez désactiver la compression post-traitement sur la destination, mettre à jour la relation manuellement et réactiver l'efficacité du stockage.

Ce dont vous avez besoin

- Les clusters source et de destination et les SVM doivent être associés.

  "Cluster et SVM peering"

- Vous devez désactiver la compression post-traitement sur la destination.

Description de la tâche

Vous pouvez utiliser le `volume efficiency show` commande pour déterminer si l'efficacité est activée sur un volume. Pour plus d'informations, consultez les pages de manuel.

Vous pouvez vérifier si SnapMirror préserve l'efficacité du stockage en consultant les journaux d'audit SnapMirror et en localiser la description du transfert. Si la description du transfert s'affiche `transfer_desc=Logical Transfer`, SnapMirror n'assure pas l'efficacité du stockage. Si la description du transfert s'affiche `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror assure l'efficacité du stockage. Par exemple :

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Transfert logique avec stockage

Depuis ONTAP 9.3, il n'est plus nécessaire de mettre à jour manuellement l'efficacité du stockage. Si SnapMirror détecte que la compression post-traitement a été désactivée, l'efficacité du stockage est réactivée automatiquement lors de la prochaine mise à jour planifiée. La source et la destination doivent exécuter ONTAP 9.3.

Depuis ONTAP 9.3, les systèmes AFF gèrent les paramètres d'efficacité du stockage différemment des systèmes FAS après la création d'un volume de destination inscriptible :

- Après avoir créé un volume de destination inscriptible à l'aide du `snapmirror break` commande, la politique de mise en cache du volume est automatiquement définie sur « auto » (par défaut).

> Ce comportement est applicable aux volumes FlexVol, uniquement et ne s'applique pas aux volumes FlexGroup.

- Lors de la resynchronisation, la règle de mise en cache est automatiquement définie sur « aucune » et la déduplication et la compression à la volée sont automatiquement désactivées, quels que soient vos paramètres d'origine. Vous devez modifier les paramètres manuellement si nécessaire.

> Les mises à jour manuelles optimisant l'efficacité du stockage peuvent s'avérer chronophages. Vous pouvez exécuter l'opération en dehors des heures de pointe.

Étape

1. Mettre à jour une relation de réplication et réactiver l'efficacité du stockage :

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -enable-storage-efficiency true`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > On doit exécuter cette commande depuis le SVM de destination ou le cluster destination. Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant met à jour la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA_dst` marche `svm_backup`, et réactive l'efficacité du stockage :

   ```
   cluster_dst::> snapmirror update -source-path svm1:volA -destination
   -path svm_backup:volA_dst -enable-storage-efficiency true
   ```

Utilisez l'accélération globale de SnapMirror

La limitation du réseau globale est disponible pour tous les transferts SnapMirror et SnapVault au niveau de chaque nœud.

Description de la tâche

La limitation globale de SnapMirror restreint la bande passante utilisée par les transferts SnapMirror et SnapVault entrants et/ou sortants. La restriction est appliquée à l'échelle du cluster sur tous les nœuds du cluster.

Par exemple, si l'accélérateur sortant est réglé sur 100 Mbit/s, la bande passante sortante est définie sur 100 Mbit/s. Si l'accélération globale est désactivée, celle-ci est désactivée sur tous les nœuds.

Bien que les taux de transfert de données soient souvent exprimés en bits par seconde (bit/s), les valeurs de l'accélérateur doivent être saisies en kilo-octets par seconde (Kbit/s).

> Dans ONTAP 9.9.1 et versions antérieures, le papillon n'a aucun effet sur `volume move` transferts ou transferts entre miroirs de partage de charge. À partir de ONTAP 9.10.0, vous pouvez spécifier une option pour accélérer les opérations de déplacement de volume. Pour plus de détails, voir "Comment accélérer le déplacement du volume dans ONTAP 9.10 et versions ultérieures."

La régulation globale fonctionne à l'aide de la fonction de régulation de la relation pour les transferts SnapMirror et SnapVault. Le papillon par relation est appliqué jusqu'à ce que la bande passante combinée des transferts par relation dépasse la valeur de l'accélérateur global, après quoi l'accélérateur global est appliqué. Une valeur d'accélérateur `0` implique que la régulation globale est désactivée.

> La régulation globale de SnapMirror n'a aucun effet sur les relations SnapMirror synchrone lorsqu'elles sont In-Sync. Cependant, le papillon affecte les relations SnapMirror synchrone lorsqu'ils effectuent une phase de transfert asynchrone comme une opération d'initialisation ou après un événement hors synchronisation. Il n'est donc pas recommandé d'activer la régulation globale avec les relations SnapMirror synchrone.

Étapes

1. Activation de l'accélération globale :

   `options -option-name replication.throttle.enable on|off`

   L'exemple suivant montre comment activer la régulation globale de SnapMirror `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Spécifiez la bande passante totale maximale utilisée par les transferts entrants sur le cluster de destination :

   `options -option-name replication.throttle.incoming.max_kbs` *KBps*

   La bande passante minimale recommandée de l'accélérateur est de 4 kbit/s et la largeur maximale est de 2 Tbit/s. La valeur par défaut de cette option est `unlimited`, ce qui signifie qu'il n'y a pas de limite sur la bande passante totale utilisée.

   L'exemple suivant montre comment définir la bande passante totale maximale utilisée par les transferts entrants sur 100 Mbit/s :

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 Mbit/s = 12500 Kbit/s

3. Spécifiez la bande passante totale maximale utilisée par les transferts sortants sur le cluster source :

   `options -option-name replication.throttle.outgoing.max_kbs` *KBps*

   La bande passante minimale recommandée de l'accélérateur est de 4 kbit/s et la largeur maximale est de

2 Tbit/s. La valeur par défaut de cette option est `unlimited`, ce qui signifie qu'il n'y a pas de limite sur la bande passante totale utilisée. Les valeurs des paramètres sont en Kbit/s.

L'exemple suivant montre comment définir la bande passante totale maximale utilisée par les transferts sortants sur 100 Mbit/s :

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Gérer la réplication de SVM SnapMirror

À propos de la réplication SnapMirror SVM

Vous pouvez utiliser SnapMirror pour créer une relation de protection des données entre les SVM. Dans ce type de relation de protection des données, tout ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB jusqu'au RBAC, est répliquée, ainsi que les données des volumes que le SVM possède.

Types de relations pris en charge

Seuls les SVM servant les données peuvent être répliqués. Les types de relations de protection des données suivants sont pris en charge :

- *Reprise sur incident SnapMirror*, dans laquelle la destination contient généralement uniquement les copies Snapshot actuellement sur la source.

  À partir de ONTAP 9.9.1, ce comportement change lorsque vous utilisez la stratégie de coffre-fort miroir. Depuis la version ONTAP 9.9.1, vous pouvez créer différentes règles Snapshot sur la source et la destination, et les copies Snapshot de la destination ne sont pas écrasées par les copies Snapshot de la source :

  - Elles ne sont pas remplacées de la source vers la destination pendant les opérations, les mises à jour et les synchronisations standard
  - Ils ne sont pas supprimés pendant les opérations de pause.
  - Elles ne sont pas supprimées lors des opérations de bascule et resynchronisation.
    Lorsque vous configurez une relation de SVM Disaster à l'aide de la règle mirror-vault à l'aide de ONTAP 9.9.1 et versions ultérieures, la règle se comporte comme suit :
  - Les règles de copie Snapshot définies par l'utilisateur au niveau de la source ne sont pas copiées vers la destination.
  - Les règles de copie Snapshot définies par le système ne sont pas copiées vers la destination.
  - L'association de volumes aux règles Snapshot définies par l'utilisateur et par le système ne sont pas copiées vers la destination.

    SVM.
- Depuis ONTAP 9.2, la réplication unifiée *SnapMirror*, dans laquelle la destination est configurée pour la reprise après incident et la conservation à long terme.

Vous trouverez des détails sur ces types de relations ici : "Présentation de la réplication de volume

SnapMirror".

Le *policy type* de la règle de réplication détermine le type de relation qu'elle prend en charge. Le tableau suivant présente les types de politiques disponibles.

Type de règle	Type de relation
mise en miroir asynchrone	Reprise sur incident SnapMirror
coffre-fort	Réplication unifiée

XDP remplace DP en tant que valeur par défaut de réplication SVM dans ONTAP 9.4

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 SVM continuent à être par défaut en mode DP dans ONTAP 9.3 et versions antérieures.

Les relations existantes ne sont pas affectées par la nouvelle valeur par défaut. Si une relation est déjà de type DP, elle continuera d'être de type DP. Le tableau suivant 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	MirrorAllsnapshots (reprise après incident SnapMirror)
XDP	XDP	MirrorAndVault (réplication unifiée)

Vous trouverez ici des informations sur les modifications apportées par défaut : "XDP remplace DP par défaut SnapMirror".

> L'indépendance de version n'est pas prise en charge pour la réplication des SVM. En configuration de reprise d'activité d'un SVM, le SVM de destination doit se trouver sur un cluster exécutant la même version ONTAP que le cluster SVM source pour prendre en charge les opérations de basculement et de retour arrière.

"Compatibilité des versions ONTAP pour les relations SnapMirror"

Réplication des configurations SVM

Le contenu d'une relation de réplication SVM est déterminé par l'interaction des champs suivants :

- Le `-identity-preserve true` de la `snapmirror create` La commande réplique l'ensemble de la configuration du SVM.

  Le `-identity-preserve false` Option réplique uniquement les volumes et les configurations d'authentification et d'autorisation du SVM, ainsi que les paramètres de protocole et de service de nom

répertoriés dans "Configurations répliquées dans des relations SVM DR".

- Le `-discard-configs network` de la `snapmirror policy create` La commande n'exclut pas les LIFs et les paramètres réseau associés de la réplication SVM, pour les cas où les SVM source et de destination se trouvent dans différents sous-réseaux.
- Le `-vserver-dr-protection unprotected` de la `volume modify` La commande exclut le volume spécifié de la réplication SVM.

Sinon, la réplication SVM est quasiment identique à la réplication de volume. Vous pouvez utiliser quasiment le même workflow pour la réplication SVM que celui utilisé pour la réplication de volume.

Détails du support

Le tableau suivant présente les détails de prise en charge de la réplication de SVM SnapMirror.

Ressource ou fonctionnalité	Détails du support
Types de déploiement	• D'une source unique vers une destination unique • Depuis la version ONTAP 9.4, « Fan-Out ». Vous ne pouvez effectuer un « fan-out » que vers deux destinations. Par défaut, une seule relation -Identity-preserve true est autorisée par SVM source.
Types de relations	• Reprise sur incident SnapMirror • La réplication unifiée SnapMirror est à partir de ONTAP 9.2
Étendue de la réplication	Intercluster uniquement. Vous ne pouvez pas répliquer de SVM au sein du même cluster.
Protection autonome contre les ransomwares	• Pris en charge à partir de ONTAP 9.12.1. Pour plus d'informations, voir "Protection autonome contre les ransomwares"
Prise en charge asynchrone des groupes de cohérence	Depuis la version ONTAP 9.14.1, un maximum de 32 relations de reprise d'activité SVM sont prises en charge lorsque des groupes de cohérence existent. Voir "Protéger un groupe de cohérence" et "Limites des groupes de cohérence" pour en savoir plus.
FabricPool	Depuis ONTAP 9.6, la réplication des SVM SnapMirror est prise en charge par FabricPool.

MetroCluster	Depuis la version ONTAP 9.11.1, les deux côtés d'une relation de reprise d'activité de SVM dans une configuration MetroCluster peuvent servir de source pour des configurations supplémentaires de reprise d'activité de SVM. Depuis ONTAP 9.5, la réplication de SnapMirror SVM est prise en charge dans les configurations MetroCluster. • Dans les versions antérieures à ONTAP 9.10.X, une configuration MetroCluster ne peut pas être la destination d'une relation de SVM DR. • Dans ONTAP 9.10.1 et versions ultérieures, une configuration MetroCluster peut faire l'objet d'une relation de reprise d'activité de SVM à des fins de migration uniquement et elle doit répondre à toutes les exigences nécessaires décrites dans "Tr-4966 : migration d'une SVM vers une solution MetroCluster". • Seul un SVM actif au sein d'une configuration MetroCluster peut être à l'origine d'une relation de reprise d'activité de SVM. Une source peut être un SVM source synchrone avant le basculement ou un SVM de destination synchrone après le basculement. • Lorsqu'une configuration MetroCluster est dans un état stable, le SVM MetroCluster destination ne peut pas être à l'origine d'une relation de reprise d'activité SVM, car les volumes ne sont pas en ligne. • Lorsque le SVM source est la source d'une relation de SVM DR, les informations de la relation de SVM DR source sont répliquées vers le partenaire MetroCluster. • Lors des processus de basculement et de rétablissement, la réplication vers la destination de reprise d'activité du SVM peut échouer. Cependant, une fois le processus de basculement ou de rétablissement terminé, les mises à jour planifiées de reprise d'activité du SVM suivant réussiront.
Groupe de cohérence	Pris en charge à partir de ONTAP 9.14.1. Pour plus d'informations, voir Protéger un groupe de cohérence.
ONTAP S3	Non pris en charge avec la reprise d'activité SVM.

SnapMirror synchrone	Non pris en charge avec la reprise d'activité SVM.
Indépendance des versions	Non pris en charge.
Chiffrement de volume	• Les volumes chiffrés de la source sont chiffrés sur la destination. • Les serveurs KMIP ou Key Manager intégrés doivent être configurés sur le système de destination. • De nouvelles clés de chiffrement sont générées au niveau de la destination. • Si la destination ne contient pas de noeud qui prend en charge le cryptage de volume, la réplication réussit, mais les volumes de destination ne sont pas chiffrés.

Configurations répliquées dans des relations SVM DR

Le tableau suivant montre l'interaction du `snapmirror create -identity-preserve` et le `snapmirror policy create -discard-configs network` option :

Réplication de la configuration		**`-identity-preserve true`**		**`-identity-preserve false`**
		Police sans `-discard-configs network` réglage	**Police avec `-discard-configs network` réglage**	
Le réseau	LIF NAS	Oui.	Non	Non
Configuration Kerberos de la LIF	Oui.	Non	Non	LIF SAN
Non	Non	Non	Politiques de pare-feu	Oui.
Oui.	Non	Stratégies de service	Oui.	Oui.
Non	Itinéraires	Oui.	Non	Non
Broadcast-Domain	Non	Non	Non	Sous-réseau
Non	Non	Non	IPspace	Non
Non	Non	PME	Serveur SMB	Oui.

Oui.	Non	Groupes locaux et utilisateur local	Oui.	Oui.
Oui.	Privilège	Oui.	Oui.	Oui.
Copie en double	Oui.	Oui.	Oui.	BranchCache
Oui.	Oui.	Oui.	Options du serveur	Oui.
Oui.	Oui.	Sécurité des serveurs	Oui.	Oui.
Non	Répertoire personnel, partager	Oui.	Oui.	Oui.
Symlink	Oui.	Oui.	Oui.	Politique de FPolicy, politique de FSecurity et NTFS de FSecurity
Oui.	Oui.	Oui.	Mapping de noms et de groupes	Oui.
Oui.	Oui.	Informations d'audit	Oui.	Oui.
Oui.	NFS	Export-policies	Oui.	Oui.
Non	Règles des export-policy	Oui.	Oui.	Non
Serveur NFS	Oui.	Oui.	Non	RBAC
Certificats de sécurité	Oui.	Oui.	Non	Configuration de l'utilisateur de connexion, de la clé publique, du rôle et du rôle
Oui.	Oui.	Oui.	SSL	Oui.
Oui.	Non	Nommer les services	Hôtes DNS et DNS	Oui.
Oui.	Non	Utilisateur UNIX et groupe UNIX	Oui.	Oui.

Oui.	Domaine Kerberos et blocs de clés Kerberos	Oui.	Oui.	Non
Client LDAP et LDAP	Oui.	Oui.	Non	Groupe réseau
Oui.	Oui.	Non	NIS	Oui.
Oui.	Non	Accès Web et Web	Oui.	Oui.
Non	Volumétrie	Objet	Oui.	Oui.
Oui.	Les copies Snapshot, la règle Snapshot et la règle de suppression automatique	Oui.	Oui.	Oui.
Règle d’efficacité	Oui.	Oui.	Oui.	Règle des quotas et règle de politique des quotas
Oui.	Oui.	Oui.	File d’attente de récupération	Oui.
Oui.	Oui.	Volume racine	Espace de noms	Oui.
Oui.	Oui.	Données utilisateur	Non	Non
Non	Qtrees	Non	Non	Non
Quotas	Non	Non	Non	QoS au niveau des fichiers
Non	Non	Non	Attributs : état du volume racine, garantie d’espace, taille, taille automatique et nombre total de fichiers	Non
Non	Non	QoS du stockage	Groupe de règles de QoS	Oui.
Oui.	Oui.	Fibre Channel (FC)	Non	Non

Non	ISCSI	Non	Non	Non
LUN	Objet	Oui.	Oui.	Oui.
igroups	Non	Non	Non	ensembles de ports
Non	Non	Non	Numéros de série	Non
Non	Non	SNMP	v3 utilisateurs	Oui.

Limites du stockage de reprise d'activité SVM

Le tableau ci-dessous présente le nombre maximal recommandé de volumes et de relations de reprise d'activité SVM pris en charge par objet de stockage. Notez que les limites dépendent souvent de la plateforme. Reportez-vous à la "Hardware Universe" pour connaître les limites de votre configuration spécifique.

Objet de stockage	Limite
SVM	300 volumes flexibles
Paire HA	1,000 volumes flexibles
Cluster	128 relations SVM DR

Répliquer les configurations de SVM

Flux de production de réplication de SVM SnapMirror

La réplication SVM SnapMirror implique la création du SVM de destination, la création d'une planification des tâches de réplication et la création et l'initialisation d'une relation SnapMirror.

Vous devez déterminer le workflow de réplication le mieux adapté à vos besoins :

- "Réplication de l'ensemble d'une configuration de SVM"
- "Exclure les LIF et les paramètres réseau associés de la réplication du SVM"
- "Exude network, name service et autres paramètres de la configuration des SVM"

Critères de placement des volumes sur des SVM de destination

Lors de la réplication de volumes du SVM source vers le SVM de destination, il est important de connaître les critères de sélection des agrégats.

Les agrégats sont sélectionnés selon les critères suivants :

- Les volumes sont toujours placés sur des agrégats non racines.
- Les agrégats non racines sont sélectionnés en fonction de l'espace disponible et du nombre de volumes

déjà hébergés sur l'agrégat.

Les agrégats disposant d'un espace libre supérieur et avec moins de volumes sont prioritaires. L'agrégat avec la priorité la plus élevée est sélectionné.

- Les volumes source des agrégats FabricPool sont situés sur des agrégats FabricPool de destination avec la même règle de Tiering.
- Si un volume du SVM source se trouve sur un agrégat Flash Pool, celui-ci est placé sur un agrégat Flash Pool sur le SVM de destination, si un tel agrégat existe et dispose de suffisamment d'espace libre.
- Si le `-space-guarantee` l'option du volume répliqué est définie sur `volume`, seuls les agrégats avec un espace libre supérieur à la taille du volume sont pris en compte.
- La taille du volume augmente automatiquement sur le SVM de destination pendant la réplication, en fonction de la taille du volume source.

  Si vous souhaitez pré-réserver la taille sur le SVM de destination, vous devez redimensionner le volume. La taille du volume n'est pas réduite automatiquement sur le SVM de destination, en fonction du SVM source.

Si vous souhaitez déplacer un volume d'un agrégat à un autre, vous pouvez utiliser le `volume move` Commande sur le SVM de destination.

Réplication de l'ensemble d'une configuration de SVM

Vous pouvez utiliser le `-identity-preserve true` de la `snapmirror create` Commande permettant de répliquer l'ensemble d'une configuration de SVM.

Avant de commencer

Les clusters source et de destination et les SVM doivent être associés.
Pour plus d'informations, voir "Créer une relation entre clusters" et "Créer une relation SVM intercluster".

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Description de la tâche

Ce flux de travail suppose que vous utilisez déjà une règle par défaut ou une règle de réplication personnalisée.

Depuis ONTAP 9.9.1, lorsque vous utilisez la règle de copie en miroir, vous pouvez créer différentes règles Snapshot sur le SVM source et de destination, et les copies Snapshot de la destination ne sont pas écrasées par les copies Snapshot de la source. Pour plus d'informations, voir "Présentation de la réplication des SVM SnapMirror".

Étapes

1. Création d'un SVM de destination :

   ```
   vserver create -vserver SVM_name -subtype dp-destination
   ```

   Le nom de SVM doit être unique sur les clusters source et destination.

   L'exemple suivant crée un SVM de destination nommé `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Depuis le cluster destination, créez une relation de type SVM peer-to-peer à l'aide de `vserver peer create` commande.

   Pour plus d'informations, voir "Créer une relation SVM intercluster".

3. Créer une planification de travaux de réplication :

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

   > La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation de SVM SnapMirror est de 15 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation de SVM SnapMirror est de 30 minutes.

   L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   saturday -hour 3 -minute 0
   ```

4. Depuis le SVM destination ou le cluster destination, créer une relation de réplication :

   `snapmirror create -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`: -type DP|XDP -schedule` *`schedule`* `-policy` *`policy`* `-identity-preserve true`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options.

   L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorAllSnapshots` règle :

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
   -identity-preserve true
   ```

   L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` règle :

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

En supposant que vous avez créé une police personnalisée avec le type de police `async-mirror`, L'exemple suivant illustre la création d'une relation SnapMirror DR :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve true
```

En supposant que vous avez créé une police personnalisée avec le type de police `mirror-vault`, l'exemple suivant crée une relation de réplication unifiée :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve true
```

5. Arrêter le SVM de destination :

   `vserver stop`

   `SVM name`

   L'exemple suivant arrête un SVM de destination nommé dvs1 :

```
cluster_dst::> vserver stop -vserver dvs1
```

6. Depuis le SVM destination ou le cluster destination, initialiser la relation de réplication SVM : +

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

   L'exemple suivant initialise la relation entre le SVM source, `svm1`, Et le SVM de destination, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Exclure les LIF et les paramètres réseau associés de la réplication du SVM

Si les SVM source et destination se trouvent dans des sous-réseaux différents, vous pouvez utiliser le `-discard-configs network` de la `snapmirror policy create` Commande permettant d'exclure les LIFs et les paramètres réseau associés de la

réplication du SVM.

Ce dont vous avez besoin

Les clusters source et de destination et les SVM doivent être associés.

Pour plus d'informations, voir "Créer une relation entre clusters" et "Créer une relation SVM intercluster".

Description de la tâche

Le `-identity-preserve` de la `snapmirror create` la commande doit être définie sur `true` Lorsque vous créez la relation de réplication SVM.

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Étapes

1. Création d'un SVM de destination :

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

   Le nom de SVM doit être unique sur les clusters source et destination.

   L'exemple suivant crée un SVM de destination nommé `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Depuis le cluster destination, créez une relation de type SVM peer-to-peer à l'aide de `vserver peer create` commande.

   Pour plus d'informations, voir "Créer une relation SVM intercluster".

3. Création d'un programme de travail :

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

   > La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation de SVM SnapMirror est de 15 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation de SVM SnapMirror est de 30 minutes.

   L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Création d'une règle de réplication personnalisée :

   `snapmirror policy create -vserver` *`SVM`* `-policy` *`policy`* `-type async-`

```
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer
-priority low|normal -is-network-compression-enabled true|false -discard
-configs network
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création d'une règle de réplication personnalisée pour la reprise sur incident de SnapMirror, à l'exception des LIFs :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

L'exemple suivant crée une règle de réplication personnalisée pour la réplication unifiée, qui exclut les LIFs :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

5. Depuis le SVM destination ou le cluster destination, lancer la commande suivante pour créer une relation de réplication :

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false
```

> Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir les exemples ci-dessous.

L'exemple suivant crée une relation SnapMirror DR qui exclut les LIF :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
-identity-preserve true
```

L'exemple suivant crée une relation de réplication unifiée SnapMirror qui exclut les LIF :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs
-identity-preserve true
```

6. Arrêter le SVM de destination :

```
vserver stop

SVM name
```

L'exemple suivant arrête un SVM de destination nommé dvs1 :

```
cluster_dst::> vserver stop -vserver dvs1
```

7. Depuis le SVM destination ou le cluster destination, initialiser une relation de réplication :

   `snapmirror initialize -source-path SVM: -destination-path SVM:`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant initialise la relation entre la source, `svm1` et la destination, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Une fois que vous avez terminé

Vous devez configurer le réseau et les protocoles sur le SVM de destination pour l'accès aux données en cas d'incident.

Exclure le réseau, le nom service et d'autres paramètres de la réplication SVM

Vous pouvez utiliser le `-identity-preserve false` de la `snapmirror create` Commande permettant de répliquer uniquement les volumes et les configurations de sécurité d'un SVM. Certains paramètres de protocole et de service de nom sont également conservés.

Description de la tâche

Pour obtenir la liste des paramètres de protocole et de service de noms conservés, reportez-vous à la section "Configurations répliquées dans les relations de reprise après incident des SVM".

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Avant de commencer

Les clusters source et de destination et les SVM doivent être associés.

Pour plus d'informations, voir "Créer une relation entre clusters" et "Créer une relation SVM intercluster".

Étapes

1. Création d'un SVM de destination :

   `vserver create -vserver SVM -subtype dp-destination`

   Le nom de SVM doit être unique sur les clusters source et destination.

   L'exemple suivant crée un SVM de destination nommé `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Depuis le cluster destination, créez une relation de type SVM peer-to-peer à l'aide de `vserver peer create` commande.

   Pour plus d'informations, voir "Créer une relation SVM intercluster".

3. Créer une planification de travaux de réplication :

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

   > La planification (RPO) minimale prise en charge pour les volumes FlexVol dans une relation de SVM SnapMirror est de 15 minutes. La planification (RPO) minimale prise en charge pour les volumes FlexGroup dans une relation de SVM SnapMirror est de 30 minutes.

   L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Créez une relation de réplication qui exclut le réseau, le service de noms et d'autres paramètres de configuration :

   `snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir les exemples ci-dessous. On doit exécuter cette commande depuis le SVM de destination ou le cluster destination.

   L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorAllSnapshots` politique. La relation exclut le réseau, le nom service et d'autres paramètres de configuration de la réplication SVM :

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
   -identity-preserve false
   ```

   L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` politique. La relation exclut le réseau, le service de nom et d'autres paramètres de configuration :

   ```
   cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
   -type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
   false
   ```

En supposant que vous avez créé une police personnalisée avec le type de police `async-mirror`, L'exemple suivant illustre la création d'une relation SnapMirror DR. La relation exclut le réseau, le nom service et d'autres paramètres de configuration de la réplication SVM :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

En supposant que vous avez créé une police personnalisée avec le type de police `mirror-vault`, l'exemple suivant crée une relation de réplication unifiée. La relation exclut le réseau, le nom service et d'autres paramètres de configuration de la réplication SVM :

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

5. Arrêter le SVM de destination :

   `vserver stop`

   `SVM name`

   L'exemple suivant arrête un SVM de destination nommé dvs1 :

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. Si vous utilisez SMB, vous devez également configurer un serveur SMB.

   Voir "SMB uniquement : création d'un serveur SMB".

7. Depuis le SVM destination ou le cluster destination, initialiser la relation SVM de réplication :

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

Une fois que vous avez terminé

Vous devez configurer le réseau et les protocoles sur le SVM de destination pour l'accès aux données en cas d'incident.

Spécifiez les agrégats à utiliser pour les relations SVM DR

Une fois un SVM de reprise d'activité créé, vous pouvez utiliser le `aggr-list` option avec `vserver modify` Commande pour limiter les agrégats utilisés pour héberger les volumes de destination du SVM DR

Étape

1. Création d'un SVM de destination :

```
vserver create -vserver SVM -subtype dp-destination
```

2. Modifiez la liste d'agrégats du SVM de reprise d'activité pour limiter les agrégats utilisés pour héberger le volume du SVM de reprise d'activité :

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

SMB uniquement : créez un serveur SMB

Si le SVM source dispose d'une configuration SMB et que vous avez décidé de le définir `identity-preserve` à `false`, Vous devez créer un serveur SMB pour le SVM de destination. Le serveur SMB est requis pour certaines configurations SMB, par exemple les partages lors de l'initialisation de la relation SnapMirror.

Étapes

1. Démarrer le SVM de destination à l'aide de l' `vserver start` commande.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Vérifier que le SVM de destination est bien dans le `running` état et sous-type `dp-destination` à l'aide du `vserver show` commande.

```
destination_cluster::> vserver show
                                   Admin      Operational Root
Vserver  Type    Subtype           State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

3. Créer une LIF en utilisant le `network interface create` commande.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

4. Créez une route à l'aide de `network route create` commande.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Gestion du réseau"

5. Configurez DNS à l'aide de `vserver services dns create` commande.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Ajoutez le contrôleur de domaine préféré à l'aide du `vserver cifs domain preferred-dc add` commande.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Créez le serveur SMB à l'aide de `vserver cifs create` commande.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Arrêter le SVM de destination à l'aide de `vserver stop` commande.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Exclure des volumes de la réplication SVM

Par défaut tous les volumes de données RW du SVM source sont répliqués. Si vous ne souhaitez pas protéger tous les volumes du SVM source, vous pouvez utiliser le `-vserver-dr-protection unprotected` de la `volume modify` Commande pour exclure des volumes de la réplication SVM.

Étapes

1. Exclure un volume de la réplication SVM :

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant exclut le volume `volA_src` De la réplication SVM :

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

Si vous souhaitez inclure par la suite un volume dans la réplication SVM que vous avez initialement exclue, exécutez la commande suivante :

`volume modify -vserver *SVM* -volume *volume* -vserver-dr-protection protected`

L'exemple suivant inclut le volume `volA_src` Dans la SVM de réplication :

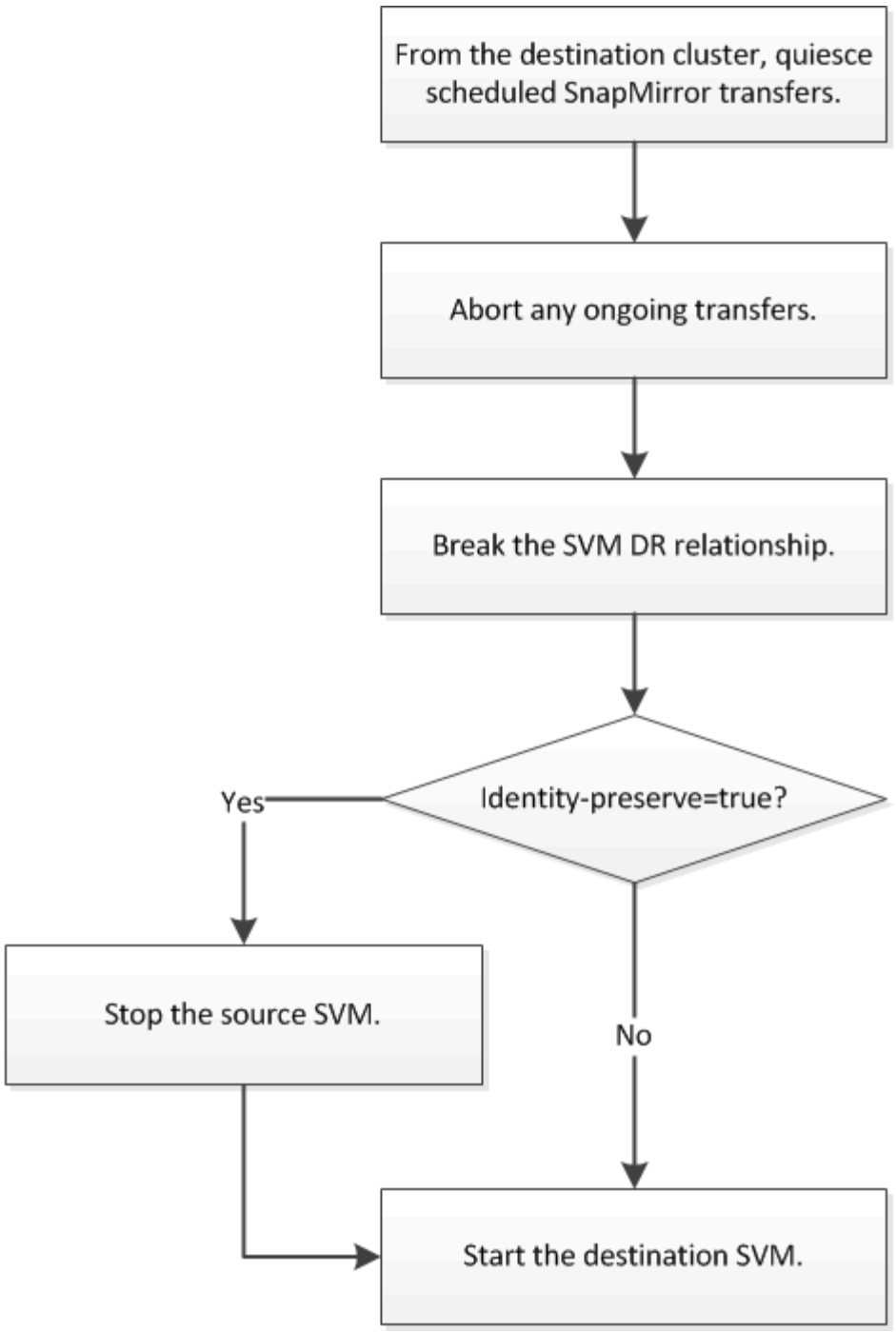
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Créer et initialiser la relation de réplication SVM comme décrit à la "Réplication de l'ensemble d'une configuration de SVM".

Service des données à partir d'une destination de reprise après incident des SVM

Flux de travail de reprise d'activité des SVM

Pour restaurer des données après un incident et transmettre leur données depuis le SVM de destination, vous devez activer le SVM de destination. L'activation de la SVM de destination implique l'arrêt de transferts SnapMirror planifiés, l'abandon de transferts SnapMirror en cours, le démantèlement de la relation de réplication, l'arrêt de la SVM source et le démarrage de la SVM de destination.



Rendre les volumes de destination du SVM inscriptibles

Vous devez rendre les volumes SVM de destination inscriptibles avant de pouvoir transmettre des données aux clients. La procédure est en grande partie identique à la procédure de réplication de volume, à exception près. Si vous avez défini `-identity -preserve true` Lorsque vous avez créé la relation de réplication SVM, vous devez arrêter le SVM source avant d'activer le SVM destination.

Description de la tâche

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

En cas de reprise d'activité, vous ne pouvez pas effectuer de mise à jour SnapMirror depuis le SVM source vers le SVM de destination de reprise après incident car votre SVM source et ses données sont inaccessibles. Les mises à jour depuis la dernière resynchronisation peuvent être en mauvais état ou corrompues.

Étapes

1. Depuis le SVM de destination ou le cluster de destination, arrêter les transferts programmés vers la destination :

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant arrête les transferts planifiés entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path
   svm_backup:
   ```

2. Depuis le SVM destination ou le cluster destination, arrêter les transferts en cours vers la destination :

   `snapmirror abort -source-path SVM: -destination-path SVM:`

   Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant arrête les transferts en cours entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path svm1: -destination-path
   svm_backup:
   ```

3. Depuis le SVM destination ou le cluster destination, faire un break de la relation de réplication :

   `snapmirror break -source-path SVM: -destination-path SVM:`

   Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant rompt la relation entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

4. Si vous avez défini `-identity-preserve true` Lorsque vous avez créé la relation de réplication de SVM, arrêter le SVM source :

   `vserver stop -vserver` *SVM*

   L'exemple suivant arrête le SVM source `svm1`:

   ```
   cluster_src::> vserver stop svm1
   ```

5. Démarrer le SVM de destination :

   `vserver start -vserver` *SVM*

   L'exemple suivant démarre le SVM de destination `svm_backup`:

   ```
   cluster_dst::> vserver start svm_backup
   ```

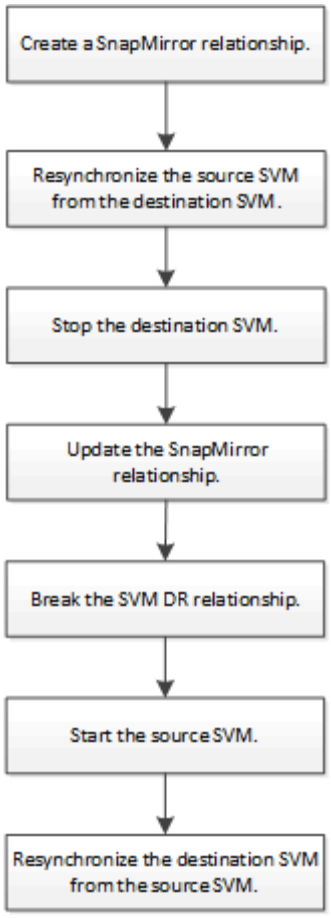
Une fois que vous avez terminé

Configuration des volumes de destination des SVM pour l'accès aux données, comme décrit à la section "Configuration du volume de destination pour l'accès aux données".

Réactiver la SVM source

Flux de travail de réactivation des SVM source

Si la SVM source existe après un incident, vous pouvez la réactiver et la protéger en recréant la relation de reprise d'activité de la SVM.



Réactiver la SVM source d'origine

Cette relation permet de rétablir la relation initiale de protection des données entre les SVM source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination. La procédure est en grande partie identique à la procédure de réplication de volume, à exception près. On doit arrêter le SVM de destination avant de réactiver la SVM source.

Avant de commencer

Si vous avez augmenté la taille du volume de destination tout en y servant des données, avant de réactiver le volume source, vous devez augmenter manuellement la taille automatique maximale sur le volume source d'origine afin de garantir une croissance suffisante.

"Lorsqu'un volume de destination augmente automatiquement"

Description de la tâche

Depuis ONTAP 9.11.1, vous pouvez réduire le temps de resynchronisation lors d'une reprise d'activité à l'aide de la `-quick-resync true` de la `snapmirror resync` Commande tout en effectuant une resynchronisation inverse d'une relation SVM DR. Une resynchronisation rapide permet de réduire le temps nécessaire au retour à la production en contournant les opérations de reconstruction et de restauration des entrepôts de données.

> La resynchronisation rapide ne permet pas de préserver l'efficacité du stockage des volumes de destination. L'activation des synchronisations rapides peut augmenter l'espace volume utilisé par les volumes de destination.

Cette procédure suppose que la ligne de base du volume source d'origine est intacte. Si la base n'est pas intacte, vous devez créer et initialiser la relation entre le volume dont vous accédez aux données et le volume source d'origine avant d'effectuer la procédure.

Pour connaître la syntaxe complète des commandes, reportez-vous à la page man.

Étapes

1. Depuis le SVM source d'origine ou le cluster source d'origine, créez une relation SVM DR inverse en utilisant les mêmes paramètres de configuration, de politique et de préservation de l'identité que la relation SVM DR d'origine :

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant crée une relation entre le SVM à partir duquel vous transmet des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

2. Depuis le SVM source d'origine ou le cluster source d'origine, exécutez la commande suivante pour inverser la relation de protection des données :

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

   > Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant inverse la relation entre la SVM source d'origine, `svm1`, Et le SVM depuis lequel vous servant des données, `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

   Exemple avec l'option -rapide-resynchronisation :

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1: -quick-resync true
   ```

3. Lorsque vous êtes prêt à rétablir l'accès aux données au SVM source d'origine, arrêter le SVM de destination d'origine pour déconnecter les clients actuellement connectés au SVM de destination d'origine.

   `vserver stop -vserver SVM`

   L'exemple suivant arrête le SVM destination d'origine qui transmet actuellement des données :

   ```
   cluster_dst::> vserver stop svm_backup
   ```

4. Vérifier que le SVM destination d'origine est bien à l'état stopped en utilisant le `vserver show` commande.

   ```
   cluster_dst::> vserver show
                                    Admin      Operational Root
   Vserver        Type    Subtype    State      State       Volume
   Aggregate
   --------       ------- ---------- ---------- ----------- ----------
   ----------
   svm_backup     data    default    stopped    stopped     rv
   aggr1
   ```

5. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour effectuer la mise à jour finale de la relation inversée afin de transférer toutes les modifications du SVM de destination d'origine vers le SVM source d'origine :

   `snapmirror update -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant met à jour la relation entre le SVM de destination d'origine à partir duquel vous accédez aux données,`svm_backup`, Et le SVM source d'origine, `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup: -destination
   -path svm1:
   ```

6. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour arrêter les transferts programmés pour la relation inverse :

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant arrête les transferts programmés entre le SVM où vous transmet des données, `svm_backup`, Et le SVM d'origine, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

7. Lorsque la mise à jour finale est terminée et que la relation indique « suspendu » pour l'état de la relation, exécutez la commande suivante à partir du SVM source d'origine ou du cluster source d'origine pour interrompre la relation inversée :

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant rupture de la relation entre le SVM de destination d'origine duquel vous servant des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

8. Si le SVM source d'origine était auparavant arrêté, depuis le cluster source d'origine, démarrer le SVM source d'origine :

   `vserver start -vserver SVM`

   L'exemple suivant démarre le SVM source d'origine :

```
cluster_src::> vserver start svm1
```

9. Depuis le SVM destination d'origine ou le cluster destination d'origine, rétablir la relation de protection des données d'origine :

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant reétablit la relation entre le SVM source d'origine, `svm1`, Et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

10. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour supprimer la relation de protection des données inversée :

    `snapmirror delete -source-path SVM: -destination-path SVM:`

> Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant supprime la relation inversée entre le SVM de destination d'origine, `svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

11. Depuis le SVM de destination d'origine ou le cluster de destination d'origine, relâcher la relation de protection des données inversée :

    `snapmirror release -source-path SVM: -destination-path SVM:`

    > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

    L'exemple suivant libère la relation inversée entre le SVM de destination d'origine, svm_backup et le SVM source d'origine, `svm1`

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1:
    ```

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Réactiver le SVM source d'origine (volumes FlexGroup uniquement)

Cette relation permet de rétablir la relation initiale de protection des données entre les SVM source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination. Pour réactiver la SVM source d'origine lorsque vous utilisez des volumes FlexGroup, vous devez effectuer quelques étapes supplémentaires, notamment la suppression de la relation SVM DR d'origine et la libération de la relation d'origine avant d'inverser la relation. Vous devez également libérer la relation inversée et recréer la relation d'origine avant d'arrêter les transferts programmés.

Étapes

1. Depuis le SVM destination d'origine ou le cluster destination d'origine, supprimer la relation SVM DR d'origine :

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

L'exemple suivant supprime la relation d'origine entre le SVM source d'origine, svm1 et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

2. Depuis le SVM source d'origine ou le cluster source d'origine, libérer la relation d'origine tout en conservant les copies Snapshot intactes :

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant libère la relation initiale entre la SVM source d'origine, svm1 et la SVM de destination d'origine, `svm_backup`.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. Depuis le SVM source d'origine ou le cluster source d'origine, créez une relation SVM DR inverse en utilisant les mêmes paramètres de configuration, de politique et de préservation de l'identité que la relation SVM DR d'origine :

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant crée une relation entre le SVM à partir duquel vous transmet des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. Depuis le SVM source d'origine ou le cluster source d'origine, exécutez la commande suivante pour inverser la relation de protection des données :

   `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

> Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

L'exemple suivant inverse la relation entre la SVM source d'origine, `svm1`, Et le SVM depuis lequel vous servant des données, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. Lorsque vous êtes prêt à rétablir l'accès aux données au SVM source d'origine, arrêter le SVM de destination d'origine pour déconnecter les clients actuellement connectés au SVM de destination d'origine.

   `vserver stop -vserver` *`SVM`*

   L'exemple suivant arrête le SVM destination d'origine qui transmet actuellement des données :

```
cluster_dst::> vserver stop svm_backup
```

6. Vérifier que le SVM destination d'origine est bien à l'état stopped en utilisant le `vserver show` commande.

```
cluster_dst::> vserver show
                                  Admin      Operational Root
Vserver        Type    Subtype    State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default    stopped    stopped     rv
aggr1
```

7. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour effectuer la mise à jour finale de la relation inversée afin de transférer toutes les modifications du SVM de destination d'origine vers le SVM source d'origine :

   `snapmirror update -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant met à jour la relation entre le SVM de destination d'origine à partir duquel vous accédez aux données,`svm_backup`, Et le SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. Depuis le SVM source d'origine ou le cluster source d'origine, lancer la commande suivante pour arrêter les transferts programmés pour la relation inverse :

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant arrête les transferts programmés entre le SVM où vous transmet des données, `svm_backup`, Et le SVM d'origine, `svm1`:

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
   -path svm1:
   ```

9. Lorsque la mise à jour finale est terminée et que la relation indique « suspendu » pour l'état de la relation, exécutez la commande suivante à partir du SVM source d'origine ou du cluster source d'origine pour interrompre la relation inversée :

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant rupture de la relation entre le SVM de destination d'origine duquel vous servant des données, `svm_backup`, Et le SVM source d'origine, `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

10. Si le SVM source d'origine était auparavant arrêté, depuis le cluster source d'origine, démarrer le SVM source d'origine :

    `vserver start -vserver SVM`

    L'exemple suivant démarre le SVM source d'origine :

    ```
    cluster_src::> vserver start svm1
    ```

11. Depuis le SVM source d'origine ou le cluster source d'origine, supprimer la relation SVM DR inversée :

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

    L'exemple suivant supprime la relation inversée entre le SVM de destination d'origine, svm_backup et le

SVM source d'origine, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Depuis le SVM de destination d'origine ou le cluster de destination d'origine, relâcher la relation inversée tout en préservant l'intégrité des copies Snapshot :

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

    L'exemple suivant libère la relation inversée entre la SVM de destination d'origine, svm_backup et la SVM source d'origine, svm1 :

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1: -relationship-info-only true
    ```

13. Depuis le SVM destination d'origine ou le cluster destination d'origine, recréer la relation d'origine. Utilisez le même paramètre de configuration, de politique et de préservation de l'identité que la relation SVM DR d'origine :

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

    L'exemple suivant crée une relation entre le SVM source d'origine, `svm1`, Et le SVM de destination d'origine, `svm_backup`:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. Depuis le SVM destination d'origine ou le cluster destination d'origine, rétablir la relation de protection des données d'origine :

    `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

    > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

    L'exemple suivant reétablit la relation entre le SVM source d'origine, `svm1`, Et le SVM de destination d'origine, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Conversion des relations de réplication de volume en relation de réplication SVM

Vous pouvez convertir des relations de réplication entre les volumes en une relation de réplication entre les SVM (Storage Virtual machines) qui sont propriétaires des volumes, à condition que chaque volume de la source (à l'exception du volume root) soit répliqué, et chaque volume de la source (y compris le volume root) porte le même nom que le volume de destination.

Description de la tâche

Utilisez le `volume rename` Commande lorsque la relation SnapMirror est inactive pour renommer des volumes de destination, si nécessaire.

Étapes

1. Depuis le SVM de destination ou le cluster de destination, exécutez la commande suivante pour resynchroniser les volumes source et destination :

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`* `-type DP|XDP -policy` *`policy`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

   L'exemple suivant resynchronque la relation entre le volume source `volA` marche `svm1` et le volume de destination `volA` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. Créer une relation de réplication SVM entre les SVM source et destination, comme décrit à la "Réplication des configurations de SVM".

   Vous devez utiliser le `-identity-preserve true` de la `snapmirror create` commande lorsque vous créez votre relation de réplication.

3. Arrêter le SVM de destination :

   `vserver stop -vserver` *`SVM`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant arrête le SVM de destination `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

4. Depuis le SVM de destination ou le cluster de destination, exécutez la commande suivante pour resynchroniser les SVM source et destination :

   `snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP -policy policy`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.
   >
   > Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

   L'exemple suivant resynchronque la relation entre le SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Supprime une relation de réplication SVM

Vous pouvez utiliser le `snapmirror delete` et `snapmirror release` Commandes permettant de supprimer une relation de réplication SVM. Vous pouvez ensuite supprimer manuellement les volumes de destination inutiles.

Description de la tâche

Le `snapmirror release` Commande permet de supprimer toutes les copies Snapshot créées par SnapMirror de la source. Vous pouvez utiliser le `-relationship-info-only` Option pour conserver les copies Snapshot.

Pour connaître la syntaxe complète des commandes, reportez-vous à la page man.

Étapes

1. Lancer la commande suivante depuis le SVM de destination ou le cluster de destination pour faire un break de la relation de réplication :

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant rompt la relation entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

2. Lancer la commande suivante depuis le SVM de destination ou le cluster de destination pour supprimer la relation de réplication :

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant supprime la relation entre la SVM source `svm1` Et le SVM de destination `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

3. Lancer la commande suivante depuis le cluster source ou le SVM source pour libérer les informations relatives aux relations de réplication du SVM source :

   `snapmirror release -source-path SVM: -destination-path SVM:`

   > Vous devez entrer deux-points (:) après le nom de SVM dans la `-source-path` et `-destination-path` options. Voir l'exemple ci-dessous.

   L'exemple suivant publie des informations pour la relation de réplication spécifiée à partir du SVM source `svm1`:

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

Gérer la réplication de volume root SnapMirror

Gérer la présentation de la réplication du volume racine SnapMirror

Chaque SVM d'un environnement NAS possède un espace de noms unique. Le SVM *root volume,* contenant le système d'exploitation et les informations associées, est le point d'entrée de la hiérarchie de l'espace de noms. Pour garantir que les données restent accessibles aux clients en cas de panne ou de basculement d'un nœud, vous devez créer une copie miroir de partage de la charge du volume racine du SVM.

L'objectif principal des miroirs de partage de charge pour les volumes root des SVM n'est plus de permettre le partage de charge ; ils ont plutôt pour objectif la reprise sur incident.

- Si le volume racine est temporairement indisponible, le miroir de partage de charge permet un accès en

lecture seule aux données du volume racine.

- Si le volume racine n'est définitivement pas disponible, vous pouvez promouvoir l'un des volumes de partage de charge pour fournir un accès en écriture aux données du volume racine.

Créer et initialiser des relations de miroir de partage de charge

Il est recommandé de créer un miroir de partage de charge (LSM) pour chaque volume root du SVM qui transmet les données NAS au sein du cluster. Pour les clusters composés d'au moins deux paires HA, il est conseillé de tenir compte des miroirs de partage de charge des volumes root du SVM afin de s'assurer que le namespace reste accessible aux clients dans le cas contraire
Les deux nœuds d'une paire haute disponibilité sont défaillants. Les miroirs de partage de charge ne sont pas adaptés aux clusters constitués d'une seule paire haute disponibilité.

Description de la tâche

Si vous créez un LSM sur le même nœud et que le nœud n'est pas disponible, vous disposez d'un point d'échec unique et vous ne disposez pas d'une seconde copie pour vous assurer que les données restent accessibles aux clients. Cependant, si vous créez le LSM sur un nœud autre que celui contenant le volume root ou sur une autre paire HA, vos données sont toujours accessibles en cas de panne.

Par exemple, dans un cluster à quatre nœuds avec un volume racine sur trois nœuds :

- Pour le volume racine sur HA 1 nœud 1, créez le LSM sur HA 2 nœud 1 ou HA 2 nœud 2.
- Pour le volume racine sur HA 1 nœud 2, créez le LSM sur HA 2 nœud 1 ou HA 2 nœud 2.
- Pour le volume racine sur HA 2 nœud 1, créez le LSM sur HA 1 nœud 1 ou HA 1 nœud 2.

Étapes

1. Créer un volume de destination pour le LSM :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

   ```
   volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
   -type DP -size <size>
   ```

   La taille du volume de destination doit être identique ou supérieure à celle du volume racine.

   Il est recommandé de nommer le volume racine et le volume de destination avec des suffixes, par exemple `_root` et `_m1`.

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant illustre la création d'un volume miroir de partage de charge pour le volume racine `svm1_root` dans `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Créez un planning de travaux de réplication".
3. Créer une relation de miroir de partage de charge entre le volume root du SVM et le volume de destination pour le LSM :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type LS -schedule <schedule>
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant crée une relation de miroir de partage de charge entre le volume racine `svm1_root` et le volume du miroir de partage de charge `svm1_m1`:

   ```
   cluster_src::> snapmirror create -source-path svm1:svm1_root
   -destination-path svm1:svm1_m1 -type LS -schedule hourly
   ```

   L'attribut type du miroir de partage de charge passe de `DP` à `LS`.

4. Initialiser le miroir de partage de charge :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

   ```
   snapmirror initialize-ls-set -source-path <SVM:volume>
   ```

   L'initialisation peut prendre beaucoup de temps. Vous pouvez exécuter le transfert de base en dehors des heures creuses.

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant initialise le miroir de partage de charge pour le volume racine `svm1_root`:

   ```
   cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
   ```

Mettre à jour une relation de miroir de partage de charge

Les relations LSM (Load-sharing mirror) sont mises à jour automatiquement pour les volumes root du SVM après le montage ou le montage d'un volume du SVM et pendant

`volume create` opérations qui incluent l'option `junction-path'. Vous pouvez mettre à jour manuellement une relation LSM si vous souhaitez la mettre à jour avant la prochaine mise à jour planifiée.

Les relations miroir de partage de charge sont mises à jour automatiquement dans les cas suivants :

- Il est temps d'effectuer une mise à jour planifiée
- Une opération de montage ou de démontage est effectuée sur un volume dans le volume root du SVM
- A `volume create` la commande a été émise qui inclut le `juntion-path` option

Étape

1. Mettre à jour manuellement une relation de miroir de partage de charge :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   L'exemple suivant met à jour la relation entre miroir de partage de charge pour le volume racine `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

Promotion d'un miroir de partage de charge

Si un volume racine est définitivement indisponible, vous pouvez promouvoir le volume LSM (Load-sharing mirror) pour fournir un accès en écriture aux données du volume racine.

Ce dont vous avez besoin

Vous devez utiliser des commandes de niveau de privilège avancé pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Promouvoir un volume LSM :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

   ```
   snapmirror promote -destination-path <SVM:volume>
   ```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant promeut le volume `svm1_m2` En tant que nouveau volume root SVM :

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Entrez `y`. ONTAP fait du volume LSM un volume en lecture/écriture et supprime le volume racine d'origine s'il est accessible.

> Le volume racine promu peut ne pas avoir toutes les données contenues dans le volume racine d'origine si la dernière mise à jour n'a pas eu lieu récemment.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

4. Renommez le volume promu en respectant la convention de nommage utilisée pour le volume racine :

   Vous devez remplacer les variables entre parenthèses angulaires par les valeurs requises avant d'exécuter cette commande.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   L'exemple suivant renomme le volume promu `svm1_m2` avec le nom `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Protégez le volume racine renommé, comme décrit aux étapes 3 à 4 de la section "Création et initialisation de relations de miroir de partage de charge".

Détails techniques de SnapMirror

Utiliser la correspondance de motif de nom de chemin d'accès

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.

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

```
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    -
```

Utilisez des requêtes étendues pour agir sur de nombreuses relations 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} *
   ```

Garantir une copie Snapshot commune dans un déploiement de copie en miroir

Vous pouvez utiliser le `snapmirror snapshot-owner create` Commande permettant de conserver une copie Snapshot étiquetée sur le système secondaire dans un déploiement mis en miroir-vault. Cela garantit qu'il existe une copie Snapshot commune pour la mise à jour de la relation de coffre-fort.

Description de la tâche

Si vous utilisez une combinaison de mirror-vault Fan-Out ou de cascade, sachez que les mises à jour échoueront si une copie Snapshot commune n'existe pas sur les volumes source et de destination.

Ce problème ne se pose jamais pour la relation de miroir dans un déploiement de type « fan-out » (fan-out) à base de miroir ou en cascade, car SnapMirror crée toujours une copie Snapshot du volume source avant d'effectuer la mise à jour.

Il peut en revanche s'agir d'un problème pour la relation de copie à distance, puisque SnapMirror ne crée pas de copie Snapshot du volume source lors de la mise à jour d'une relation de copie à distance. Vous devez utiliser le `snapmirror snapshot-owner create` Pour s'assurer qu'il existe au moins une copie Snapshot commune à la fois sur la source et la destination de la relation de coffre-fort.

Étapes

1. Sur le volume source, attribuez un propriétaire à la copie Snapshot nommée que vous souhaitez conserver :

   `snapmirror snapshot-owner create -vserver SVM -volume volume -snapshot snapshot -owner owner`

   L'exemple suivant affecte `ApplicationA` en tant que propriétaire du `snap1` Copie Snapshot :

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

2. Mettez à jour la relation de miroir, comme décrit dans "Mise à jour manuelle d'une relation de réplication".

   Vous pouvez également attendre la mise à jour planifiée de la relation miroir.

3. Transférer la copie Snapshot étiquetée vers la destination du coffre-fort :

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -source-snapshot snapshot`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant transfère le `snap1` La copie Snapshot

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   La copie Snapshot nommée sera conservée lors de la mise à jour de la relation de coffre-fort.

4. Sur le volume source, supprimez le propriétaire de la copie Snapshot nommée :

   `snapmirror snapshot-owner delete -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-owner` *`owner`*

   Les exemples suivants sont supprimés `ApplicationA` en tant que propriétaire du `snap1` Copie Snapshot :

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

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.
- 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.

L'interopérabilité est bidirectionnelle.

Interopérabilité pour ONTAP version 9.3 et ultérieure

Version ONTAP…	Interopérabilité avec ces versions précédentes de ONTAP…																	
	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4	9.3
9.14.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non	Non	Non	Non
9.14.0*	**Oui**	**Oui**	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	Non	Non	Non	Non
9.13.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non	Non	Non
9.13.0*	**Oui**	Non	**Oui**	**Oui**	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	Non	Non	Non	Non
9.12.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non	Non
9.12.0*	**Oui**	Non	**Oui**	Non	**Oui**	**Oui**	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	**Oui**	Non	Non	Non	Non
9.11.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non
9.11.0*	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	**Oui**	**Oui**	Non	**Oui**	Non	**Oui**	**Oui**	**Oui**	Non	Non	Non
9.10.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.10.0*	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	**Oui**	**Oui**	Non	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.9.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.9.0*	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.8	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	**Oui**

9.7	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	**Oui**
9.6	Non	Non	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	**Oui**
9.5	Non	Non	Non	Non	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**
9.4	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**
9.3	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**

Relations SnapMirror synchrones

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

Version ONTAP …	Interopérabilité avec ces versions précédentes de ONTAP…									
	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
9.14.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non
9.13.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.12.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.11.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non	Non
9.10.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non	Non
9.9.1	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non	Non
9.8	**Oui**	**Oui**	**Oui**	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Non
9.7	Non	**Oui**	**Oui**	Non	Non	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**
9.6	Non	Non	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**	**Oui**
9.5	Non	Non	Non	Non	Non	Non	Non	**Oui**	**Oui**	**Oui**

Relations de reprise d'activité SVM SnapMirror

- 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 récente que deux versions majeures sur site ou deux versions majeures de cloud plus récentes, 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).

Source	Destination																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1
9.3	Reprise sur incident/migration	Migration	Migration	Migration	Migration													
9.4		Reprise sur incident/migration	Migration	Migration	Migration	Migration												
9.5			Reprise sur incident/migration	Migration	Migration	Migration	Migration											
9.6				Reprise sur incident/migration	Migration	Migration	Migration	Migration										
9.7					Reprise sur incident/migration	Migration	Migration	Migration	Migration									

9.8						Reprise sur incident/ migration	Migration	Migration	Migration	Migration								
9.9.0*							Reprise sur incident/ migration	Migration	Migration	Migration	Migration							
9.9.1								Reprise sur incident/ migration	Migration	Migration	Migration	Migration						
9.10.0*									Reprise sur incident/ migration	Migration	Migration	Migration	Migration					
9.10.1										Reprise sur incident/ migration	Migration	Migration	Migration	Migration				
9.11.0*											Reprise sur incident/ migration	Migration	Migration	Migration	Migration			

9.11.1												Reprise sur incident/migration	Migration	Migration	Migration	Migration		
9.12.0*													Reprise sur incident/migration	Migration	Migration	Migration	Migration	
9.12.1														Reprise sur incident/migration	Migration	Migration	Migration	Migration
9.13.0*															Reprise sur incident/migration	Migration	Migration	Migration
9.13.1																Reprise sur incident/migration	Migration	Migration
9.14.0*																	Reprise sur incident/migration	Migration

9.14.1																		Reprise sur incident/migration

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	9.2	9.1	9
9.11.1	Oui.	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
9.10.1	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
9.9.1	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non	Non	Non
9.8	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non	Non
9.7	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non	Non
9.6	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non	Non
9.5	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non	Non
9.4	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non	Non
9.3	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non	Non
9.2	Non	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non	Non
9.1	Non	Non	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.	Non
9	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui.	Oui.	Oui.

> L'interopérabilité n'est pas bidirectionnelle.

SnapMirror limitations

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.

Archivage et conformité grâce à la technologie SnapLock

Qu'est-ce que SnapLock

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM pour conserver les fichiers sous une forme non modifiée à des fins réglementaires et de gouvernance.

SnapLock empêche la suppression, la modification ou la modification des données pour répondre aux réglementations SEC 17a-4, HIPAA, FINRA, CFTC et le RGPD. SnapLock vous permet de créer des volumes spéciaux dans lesquels les fichiers peuvent être stockés et archivés dans un état non effaçable et non inscriptible pour une période de conservation définie ou indéfiniment. SnapLock permet cette conservation au niveau fichier via des protocoles de fichiers ouverts standard tels que CIFS et NFS. Les protocoles de fichier ouvert pris en charge pour SnapLock sont les suivants : NFS (versions 2, 3 et 4) et CIFS (SMB 1.0, 2.0 et 3.0).

Avec SnapLock, vous archivage des fichiers et des copies Snapshot sur le stockage WORM et définissez des périodes de conservation pour les données protégées WORM. Le stockage WORM SnapLock utilise la technologie NetApp Snapshot et peut exploiter la réplication SnapMirror ainsi que les sauvegardes SnapVault comme technologie de base pour offrir une protection des données de restauration de sauvegarde.
En savoir plus sur le stockage WORM : "Conformité du stockage WORM avec NetApp SnapLock - TR-4526".

Vous pouvez utiliser une application pour valider les fichiers en mode WORM sur NFS ou CIFS, ou utiliser la fonctionnalité d'autovalidation de SnapLock pour allouer automatiquement les fichiers en mode WORM. Vous pouvez utiliser un fichier *WORM appliable* pour conserver les données écrites de manière incrémentielle, comme les informations de journal. Pour plus d'informations, voir "Utilisez le mode d'ajout de volumes pour créer des fichiers d'ajout WORM".

SnapLock prend en charge les méthodes de protection des données qui doivent répondre à la plupart des exigences de conformité :

- Vous pouvez utiliser SnapLock pour SnapVault pour protéger les copies Snapshot WORM sur le stockage secondaire. Voir "Archivage des copies Snapshot en mode WORM".
- Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins de reprise après incident. Voir "Fichiers WORM en miroir".

SnapLock est une fonctionnalité sous licence de NetApp ONTAP. Une seule licence vous donne le droit

d'utiliser SnapLock en mode strict conformité, afin de répondre aux exigences externes telles que la règle SEC 17a-4 et un mode perte de l'entreprise, afin de respecter les réglementations internes régissant la protection des ressources numériques. Les licences SnapLock font partie du "ONTAP One" suite logicielle.

SnapLock est pris en charge sur tous les systèmes AFF, FAS et ONTAP Select. SnapLock n'est pas une solution exclusivement logicielle ; il s'agit d'une solution matérielle et logicielle intégrée. Cette distinction est importante pour les réglementations WORM strictes, telles que la norme SEC 17a-4, qui requièrent une solution matérielle et logicielle intégrée. Pour plus d'informations, reportez-vous à la section "SEC interprétation : stockage électronique des dossiers des courtiers-concessionnaires".

Les avantages de SnapLock

Une fois SnapLock configuré, vous pouvez effectuer les tâches suivantes :

- "Archivage des fichiers en mode WORM"
- "Archivage des copies Snapshot sur le stockage WORM pour le stockage secondaire"
- "Mise en miroir des fichiers WORM pour la reprise après incident"
- "Conservation des fichiers WORM en cas de litiges avec la conservation légale"
- "Supprimez des fichiers WORM à l'aide de la fonction de suppression privilégiée"
- "Définissez la période de rétention des fichiers"
- "Déplacer un volume SnapLock"
- "Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware"
- "Vérifiez l'utilisation de SnapLock avec le journal d'audit"
- "Utilisez les API SnapLock"

SnapLock Compliance et Enterprise modes

Les modes SnapLock Compliance et Enterprise diffèrent principalement du niveau auquel chaque mode protège les fichiers WORM :

Mode SnapLock	Niveau de protection	Suppression du fichier WORM pendant la conservation
Mode de conformité	Au niveau fichier	Ne peut pas être supprimé
Mode entreprise	Au niveau du disque	Peut être supprimé par l'administrateur de conformité à l'aide d'une procédure auditée de "suppression privilégiée"

Une fois la période de rétention écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin. Une fois qu'un fichier a été engagé en mode WORM, qu'il soit en mode conformité ou entreprise, il ne peut pas être modifié, même après l'expiration de la période de conservation.

Vous ne pouvez pas déplacer un fichier WORM pendant ou après la période de conservation. Vous pouvez copier un fichier WORM, mais la copie ne conserve pas ses caractéristiques WORM.

Le tableau suivant présente les différences de capacités prises en charge par les modes SnapLock Compliance et Enterprise :

Fonctionnalité	Conformité SnapLock	SnapLock Enterprise
Activer et supprimer des fichiers à l'aide de la suppression privilégiée	Non	Oui.
Réinitialiser les disques	Non	Oui.
Destruction des agrégats et des volumes SnapLock pendant la période de conservation	Non	Oui, à l'exception du volume du journal d'audit de SnapLock
Renommer les agrégats ou les volumes	Non	Oui.
Utiliser des disques non NetApp	Non	Oui (avec "Virtualisation FlexArray")
Utilisation du volume SnapLock pour la journalisation des audits	Oui.	Oui, à partir de ONTAP 9.5

Fonctionnalités prises en charge et non prises en charge avec SnapLock

Le tableau suivant présente les fonctionnalités prises en charge avec le mode SnapLock Compliance, le mode SnapLock Enterprise ou les deux :

Fonction	Prise en charge par SnapLock Compliance	Pris en charge par SnapLock Enterprise
Groupes de cohérence	Non	Non
Volumes chiffrés	Oui, à partir de ONTAP 9.2. En savoir plus sur Cryptage et SnapLock.	Oui, à partir de ONTAP 9.2. En savoir plus sur Cryptage et SnapLock.
FabricPool sur les agrégats SnapLock	Non	Oui, à partir de ONTAP 9.8. En savoir plus sur FabricPool sur les agrégats SnapLock Enterprise.
Les agrégats Flash Pool	Oui, à partir de ONTAP 9.1.	Oui, à partir de ONTAP 9.1.
FlexClone	Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock.	Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock.
Volumes FlexGroup	Oui, à partir de ONTAP 9.11.1. En savoir plus sur [flexgroup].	Oui, à partir de ONTAP 9.11.1. En savoir plus sur [flexgroup].

LUN	Non En savoir plus sur Prise en charge LUN Avec SnapLock.	Non En savoir plus sur Prise en charge LUN Avec SnapLock.
Configurations MetroCluster	Oui, à partir de ONTAP 9.3. En savoir plus sur Prise en charge de MetroCluster.	Oui, à partir de ONTAP 9.3. En savoir plus sur Prise en charge de MetroCluster.
Vérification multiadministrateur	Oui, à partir de ONTAP 9.13.1. En savoir plus sur Prise en charge MAV.	Oui, à partir de ONTAP 9.13.1. En savoir plus sur Prise en charge MAV.
SAN	Non	Non
SnapRestore pour un seul fichier	Non	Oui.
Continuité de l'activité SnapMirror	Non	Non
SnapRestore	Non	Oui.
SMTape	Non	Non
SnapMirror synchrone	Non	Non
SSD	Oui, à partir de ONTAP 9.1.	Oui, à partir de ONTAP 9.1.
Fonctionnalités d'efficacité du stockage	Oui, depuis ONTAP 9.9.1. En savoir plus sur prise en charge de l'efficacité du stockage.	Oui, depuis ONTAP 9.9.1. En savoir plus sur prise en charge de l'efficacité du stockage.

FabricPool sur les agrégats SnapLock Enterprise

FabricPool est pris en charge sur les agrégats SnapLock Enterprise à partir de ONTAP 9.8. Toutefois, votre équipe de compte doit ouvrir une demande de modification des produits afin de documenter que les données FabricPool hiérarchisées vers un cloud public ou privé ne sont plus protégées par SnapLock, car les administrateurs cloud peuvent les supprimer.

> Les données FabricPool placées dans un cloud public ou privé n'sont plus protégées par SnapLock, car les administrateurs cloud peuvent les supprimer.

Volumes FlexGroup

SnapLock prend en charge les volumes FlexGroup depuis ONTAP 9.11.1, mais les fonctionnalités suivantes ne sont pas prises en charge :

- Obligation légale
- Conservation basée sur les événements
- SnapLock pour SnapVault (prise en charge à partir de ONTAP 9.12.1)

Vous devez également connaître les comportements suivants :

- L'horloge de conformité de volume (VCC) d'un volume FlexGroup est déterminée par le VCC du composant racine. Tous les composants non racines auront leur VCC étroitement synchronisé avec le VCC racine.
- Les propriétés de configuration de SnapLock sont définies uniquement sur la FlexGroup dans son ensemble. Les composants individuels ne peuvent pas avoir des propriétés de configuration différentes, telles que le temps de rétention par défaut et la période de validation automatique.

Prise en charge LUN

Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

Prise en charge de MetroCluster

La prise en charge de SnapLock dans les configurations MetroCluster diffère entre le mode SnapLock Compliance et le mode SnapLock Enterprise.

Conformité SnapLock

- Depuis ONTAP 9.3, la conformité SnapLock est prise en charge sur les agrégats MetroCluster sans miroir.
- Depuis ONTAP 9.3, la conformité SnapLock est prise en charge sur les agrégats en miroir, mais uniquement si l'agrégat est utilisé pour héberger les volumes du journal d'audit SnapLock.
- Les configurations SnapLock spécifiques à SVM peuvent être répliquées sur les sites principal et secondaire à l'aide de MetroCluster.

SnapLock Enterprise

- Les agrégats SnapLock Enterprise sont pris en charge depuis la version ONTAP 9.
- Depuis ONTAP 9.3, les agrégats SnapLock Enterprise avec suppression privilégiée sont pris en charge.
- Les configurations SnapLock spécifiques à SVM peuvent être répliquées vers les deux sites à l'aide de MetroCluster.

Configurations MetroCluster et horloges de conformité

Les configurations MetroCluster utilisent deux mécanismes d'horloge de conformité, l'horloge de conformité du volume (VCC) et l'horloge de conformité du système (SCC). Les VCC et SCC sont disponibles dans toutes les configurations SnapLock. Lorsque vous créez un nouveau volume sur un noeud, son VCC est initialisé avec la valeur actuelle du SCC sur ce noeud. Une fois le volume créé, la durée de rétention du volume et du fichier est toujours suivie avec le VCC.

Lorsqu'un volume est répliqué vers un autre site, son VCC est également répliqué. Lors d'un basculement de volume, du site A vers le site B, par exemple, le VCC continue d'être mis à jour sur le site B pendant que le SCC sur le site A s'arrête lorsque le site A passe hors ligne.

Lorsque le site A est remis en ligne et que le rétablissement du volume est effectué, l'horloge du site A SCC redémarre alors que le VCC du volume continue d'être mis à jour. Étant donné que le VCC est mis à jour en permanence, indépendamment des opérations de basculement et de rétablissement, les délais de conservation des fichiers ne dépendent pas des horloges SCC et ne sont pas extensibles.

Prise en charge de la vérification multiadministrateur

Depuis la version ONTAP 9.13.1, un administrateur de cluster peut explicitement activer la vérification multiadministrateur sur un cluster afin de demander l'approbation du quorum avant l'exécution de certaines opérations SnapLock. Lorsque MAV est activé, les propriétés du volume SnapLock telles que temps-conservation-défaut, temps-conservation-minimum, temps-conservation-maximum, mode-ajout-volume, période-allocation-auto et suppression-privilégiée requièrent l'approbation du quorum. En savoir plus sur "VAM".

Efficacité du stockage

Depuis la version ONTAP 9.9.1, SnapLock prend en charge les fonctionnalités d'efficacité du stockage, telles que la compaction des données, la déduplication entre les volumes et la compression adaptative pour les volumes et les agrégats SnapLock. Pour plus d'informations sur l'efficacité du stockage, voir "Présentation de la gestion du stockage logique avec l'interface de ligne de commande".

Le cryptage

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

Avertissement : NetApp ne peut pas garantir que les fichiers WORM protégés par SnapLock sur des disques ou volumes à autochiffrement seront récupérables en cas de perte de la clé d'authentification ou si le nombre de tentatives d'authentification échouées dépasse la limite spécifiée et entraîne le verrouillage permanent du disque. Vous êtes responsable de vous assurer contre les échecs d'authentification.

> Depuis ONTAP 9.2, les volumes chiffrés sont pris en charge sur les agrégats SnapLock.

Transition depuis la version 7-mode

Vous pouvez migrer des volumes SnapLock de 7-mode vers ONTAP à l'aide de la fonctionnalité de transition basée sur la copie de l'outil de transition 7-mode. Le mode SnapLock du volume de destination, conformité ou entreprise doit correspondre au mode SnapLock du volume source. Vous ne pouvez pas utiliser la transition sans copie pour migrer des volumes SnapLock.

Configurez SnapLock

Configurez SnapLock

Avant d'utiliser SnapLock, vous devez configurer SnapLock en exécutant diverses tâches telles que "Installez la licence SnapLock" Pour chaque nœud qui héberge un agrégat avec un volume SnapLock, initialisez le "Horloge de conformité", Créer un agrégat SnapLock pour les clusters exécutant des versions ONTAP antérieures à ONTAP 9.10.1, "Créez et montez un volume SnapLock", et plus encore.

Initialiser l'horloge de conformité

SnapLock utilise le *volume Compliance Clock* pour éviter toute altération susceptible de modifier la période de conservation des fichiers WORM. Vous devez d'abord initialiser le *système CompléanceClock* sur chaque nœud hébergeant un agrégat SnapLock.

Depuis ONTAP 9.14.1, vous pouvez initialiser ou réinitialiser l'horloge de conformité du système en l'absence

de volumes SnapLock ou de volumes sur lesquels le verrouillage des copies Snapshot est activé. La possibilité de réinitialiser permet aux administrateurs système de réinitialiser l'horloge de conformité du système dans les cas où elle a été mal initialisée ou de corriger la dérive de l'horloge sur le système. Dans ONTAP 9.13.1 et les versions antérieures, une fois que vous avez initialisé l'horloge de conformité sur un nœud, vous ne pouvez pas l'initialiser à nouveau.

Avant de commencer

Pour réinitialiser l'horloge de conformité :

- Tous les nœuds du cluster doivent être en état de santé.
- Tous les volumes doivent être en ligne.
- Aucun volume ne peut être présent dans la file d'attente de récupération.
- Aucun volume SnapLock ne peut être présent.
- Aucun volume sur lequel le verrouillage des copies Snapshot est activé ne peut être présent.

Exigences générales pour l'initialisation de l'horloge de conformité :

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- "La licence SnapLock doit être installée sur le nœud".

Description de la tâche

L'heure de l'horloge de conformité du système est héritée par le *volume Compliance Clock*, qui contrôle la période de conservation des fichiers WORM sur le volume. L'horloge de conformité du volume est initialisée automatiquement lorsque vous créez un nouveau volume SnapLock.

> Le réglage initial de l'horloge de conformité du système est basé sur l'horloge du système matériel actuel. C'est pourquoi vous devez vérifier que l'heure et le fuseau horaire du système sont corrects avant d'initialiser l'horloge de conformité du système sur chaque nœud. Une fois que vous avez initialisé l'horloge de conformité du système sur un nœud, vous ne pouvez plus l'initialiser lorsque des volumes SnapLock ou des volumes dont le verrouillage est activé sont présents.

Étapes

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour initialiser l'horloge de conformité ou, à partir de ONTAP 9.12.1, vous pouvez utiliser System Manager pour initialiser l'horloge de conformité.

System Manager

1. Accédez à **Cluster > Présentation**.
2. Dans la section **noeuds**, cliquez sur **Initialize SnapLock Compliance Clock**.
3. Pour afficher la colonne **horloge de conformité** et vérifier que l'horloge de conformité est initialisée, dans la section **Cluster > Présentation > nœuds**, cliquez sur **Afficher/Masquer** et sélectionnez **horloge de conformité SnapLock**.

CLI

1. Initialiser l'horloge de conformité du système :

   `snaplock compliance-clock initialize -node` *`node_name`*

   La commande suivante initialise l'horloge de conformité du système `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. Lorsque vous y êtes invité, vérifiez que l'horloge du système est correcte et que vous souhaitez initialiser l'horloge de conformité :

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Répétez cette procédure pour chaque nœud qui héberge un agrégat SnapLock.

Activez la resynchronisation Compliance Clock pour un système configuré en NTP

Vous pouvez activer la fonction de synchronisation de l'heure de l'horloge de conformité SnapLock lorsqu'un serveur NTP est configuré.

Ce dont vous avez besoin

- Cette fonction est disponible uniquement au niveau de privilège avancé.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- "La licence SnapLock doit être installée sur le nœud".
- Cette fonction est disponible uniquement sur les plates-formes Cloud Volumes ONTAP, ONTAP Select et VSIM.

Description de la tâche

Lorsque le démon d'horloge sécurisée SnapLock détecte une inclinaison au-delà du seuil, ONTAP utilise l'heure système pour réinitialiser les horloges de conformité du système et du volume. Une période de 24 heures est définie comme seuil d'inclinaison. Cela signifie que l'horloge de conformité du système est synchronisée sur l'horloge du système uniquement si l'inclinaison a plus d'un jour.

Le démon d'horloge sécurisée SnapLock détecte une inclinaison et modifie l'horloge de conformité en l'heure système. Toute tentative de modification de l'heure du système pour forcer la synchronisation de l'horloge de conformité avec l'heure du système échoue, car l'horloge de conformité se synchronise avec l'heure du système uniquement si l'heure du système est synchronisée avec l'heure NTP.

Étapes

1. Activez la fonction de synchronisation de l'heure de l'horloge de conformité SnapLock lorsqu'un serveur NTP est configuré :

   `snaplock compliance-clock ntp`

   La commande suivante active la fonction de synchronisation de l'horloge de conformité du système :

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. Lorsque vous y êtes invité, vérifiez que les serveurs NTP configurés sont approuvés et que le canal de communication est sécurisé pour activer la fonction :
3. Vérifiez que la fonction est activée :

   `snaplock compliance-clock ntp show`

   La commande suivante vérifie que la fonction de synchronisation de l'horloge de conformité du système est activée :

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Créer un agrégat SnapLock

Vous utilisez le volume `-snaplock-type` Pour spécifier un type de volume Compliance ou Enterprise SnapLock. Pour les versions antérieures à ONTAP 9.10.1, vous devez créer un agrégat SnapLock distinct. Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le SnapLock "la licence doit être installée" sur le nœud. Cette licence est incluse dans "ONTAP One".
- "L'horloge de conformité sur le nœud doit être initialisée".
- Si vous avez partitionné les disques comme « root », « data1 » et « data2 », vous devez vous assurer que les disques de secours sont disponibles.

Mise à niveau

Lors de la mise à niveau vers ONTAP 9.10.1, les agrégats SnapLock et non SnapLock existants sont mis à niveau pour prendre en charge la présence de volumes SnapLock et non SnapLock. Cependant, les attributs des volumes SnapLock existants ne sont pas automatiquement mis à jour. Par exemple, les champs de compaction des données, de déduplication entre les volumes et de déduplication entre les volumes en arrière-plan restent inchangés. Les nouveaux volumes SnapLock créés sur des agrégats existants ont les mêmes valeurs par défaut que les volumes qui ne sont pas SnapLock. Les valeurs par défaut des nouveaux volumes et des agrégats dépendent de la plateforme.

Ne tenez pas compte des considérations

Pour restaurer une version ONTAP antérieure à la version 9.10.1, vous devez déplacer les volumes SnapLock Compliance, SnapLock Enterprise et SnapLock vers leurs propres agrégats SnapLock.

Description de la tâche

- Vous ne pouvez pas créer d'agrégats de conformité pour les LUN FlexArray, mais les agrégats de conformité SnapLock sont pris en charge avec les LUN FlexArray.
- L'option SyncMirror ne permet pas de créer des agrégats de conformité.
- Vous pouvez créer des agrégats de conformité en miroir dans une configuration MetroCluster uniquement si l'agrégat est utilisé pour héberger des volumes du journal d'audit SnapLock.

> Dans une configuration MetroCluster, SnapLock Enterprise est pris en charge sur des agrégats en miroir ou non mis en miroir. La conformité SnapLock est prise en charge uniquement sur les agrégats sans miroir.

Étapes

1. Créer un agrégat SnapLock :

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

La page man de la commande contient une liste complète d'options.

La commande suivante crée une SnapLock `Compliance` agrégat nommé `aggr1` avec trois disques sur `node1`:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

Création et montage de volumes SnapLock

Vous devez créer un volume SnapLock pour les fichiers ou les copies Snapshot que vous souhaitez valider en état WORM. Depuis ONTAP 9.10.1, tout volume que vous créez, quel que soit le type d'agrégat, est créé par défaut en tant que volume non SnapLock. Vous devez utiliser le `-snaplock-type` Option permettant de créer explicitement un volume SnapLock en spécifiant Compliance ou Enterprise comme type SnapLock. Par

défaut, le type de SnapLock est défini sur `non-snaplock`.

Avant de commencer

- L'agrégat SnapLock doit être en ligne.
- Vous devriez "Vérifiez qu'une licence SnapLock est installée". Si aucune licence SnapLock n'est installée sur le nœud, vous devez "installer" il. Cette licence est incluse avec "ONTAP One". Avant ONTAP One, la licence SnapLock était incluse dans le bundle sécurité et conformité. Le bundle sécurité et conformité n'est plus proposé, mais reste valide. Bien qu'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire "Passez à ONTAP One".
- "L'horloge de conformité sur le nœud doit être initialisée".

Description de la tâche

Avec les autorisations SnapLock appropriées, vous pouvez détruire ou renommer un volume d'entreprise à tout moment. Vous ne pouvez pas détruire un volume Compliance tant que la période de conservation n'est pas écoulée. Vous ne pouvez jamais renommer un volume Compliance.

Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock. Le volume clone sera du même type SnapLock que le volume parent.

> Les LUN ne sont pas prises en charge dans les volumes SnapLock. Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour créer un volume SnapLock.

Étapes

1. Accédez à **Storage > volumes** et cliquez sur **Add**.
2. Dans la fenêtre **Ajouter un volume**, cliquez sur **plus d'options**.
3. Entrez les informations du nouveau volume, notamment le nom et la taille du volume.
4. Sélectionnez **Activer SnapLock** et choisissez le type SnapLock, conformité ou entreprise.
5. Dans la section **Auto-commit Files**, sélectionnez **Modified** et entrez la durée pendant laquelle un fichier doit rester inchangé avant qu'il ne soit automatiquement engagé. La valeur minimale est de 5 minutes et la valeur maximale est de 10 ans.
6. Dans la section **Data Retention**, sélectionnez la période de rétention minimale et maximale.
7. Sélectionnez la période de rétention par défaut.
8. Cliquez sur **Enregistrer**.
9. Sélectionnez le nouveau volume dans la page **volumes** pour vérifier les paramètres SnapLock.

CLI

1. Créer un volume SnapLock :

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise>
   ```

   Pour obtenir la liste complète des options, consultez la page man de la commande. Les options suivantes ne sont pas disponibles pour les volumes SnapLock : `-nvfail`, `-atime-update`, `-is -autobalance-eligible`, `-space-mgmt-try-first`, et `vmalign`.

   La commande suivante crée une SnapLock `Compliance` volume nommé `vol1` marche `aggr1` marche `vs1`:

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
   -snaplock-type compliance
   ```

Montez un volume SnapLock

Vous pouvez monter un volume SnapLock sur une Junction path dans le SVM namespace pour accéder au client NAS.

Ce dont vous avez besoin

Le volume SnapLock doit être en ligne.

Description de la tâche

- Vous pouvez monter un volume SnapLock uniquement sous la racine de la SVM.

- Vous ne pouvez pas monter un volume normal sous un volume SnapLock.

Étapes

1. Monter un volume SnapLock :

   `volume mount -vserver SVM_name -volume volume_name -junction-path path`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante monte un volume SnapLock nommé `vol1` au chemin de jonction `/sales` dans le `vs1` espace de noms :

   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Définissez la durée de rétention

Vous pouvez définir explicitement la durée de conservation d'un fichier ou utiliser la période de rétention par défaut pour le volume afin de définir la durée de conservation. Sauf si vous définissez explicitement la durée de conservation, SnapLock utilise la période de conservation par défaut pour calculer la durée de conservation. Vous pouvez également définir la conservation des fichiers après un événement.

À propos de la période de conservation et de la durée de conservation

Le paramètre *rétention_période* pour un fichier WORM spécifie la durée pendant laquelle le fichier doit être conservé après son activation à l'état WORM. Le *temps de rétention* pour un fichier WORM est le temps après lequel le fichier n'a plus besoin d'être conservé. Une période de conservation de 20 ans pour un dossier engagé à l'état WORM le 10 novembre 2020 6 h 00, par exemple, entraînerait un temps de rétention de 10 novembre 2040 6 h 00

> Depuis ONTAP 9.10.1, vous pouvez définir une durée de conservation allant jusqu'au 26 octobre 3058 et une période de conservation pouvant aller jusqu'à 100 ans. Lorsque vous prolongez les dates de conservation, les anciennes règles sont automatiquement converties. Dans ONTAP 9.9.1 et versions antérieures, sauf si vous avez défini la période de conservation par défaut sur infinie, la durée maximale de conservation prise en charge est de janvier 19 2071 (GMT).

Considérations importantes relatives à la réplication

Lorsque vous définissez une relation SnapMirror avec un volume source SnapLock à une date de conservation postérieure au 19 janvier 2071 (GMT), le cluster de destination doit exécuter ONTAP 9.10.1 ou version ultérieure, sinon le transfert SnapMirror échoue.

Considérations importantes concernant la restauration

ONTAP vous empêche de restaurer un cluster depuis ONTAP 9.10.1 vers une version antérieure de ONTAP

lorsqu'il y a des fichiers avec une période de conservation postérieure à « janvier 19, 2071 8:44:07 ».

Comprendre les périodes de conservation

Un volume SnapLock Compliance ou Enterprise a quatre périodes de conservation :

- Durée de conservation minimale (`min`), avec une valeur par défaut de 0
- Durée de conservation maximale (`max`), avec une valeur par défaut de 30 ans
- Période de rétention par défaut, avec une valeur par défaut égale à `min` Pour le mode conformité et le mode entreprise à partir de ONTAP 9.10.1. Dans les versions ONTAP antérieures à ONTAP 9.10.1, la période de conservation par défaut dépend du mode :
  - Pour le mode conformité, la valeur par défaut est égale à `max`.
  - Pour le mode entreprise, la valeur par défaut est égale à `min`.
- Période de conservation non spécifiée.

  Depuis ONTAP 9.8, vous pouvez définir la période de conservation des fichiers d'un volume sur `unspecified`, pour activer le fichier à conserver jusqu'à ce que vous ayez défini une durée de conservation absolue. Vous pouvez définir un fichier avec un temps de conservation absolu sur une rétention non spécifiée et revenir à une conservation absolue tant que la nouvelle durée de conservation absolue est postérieure à la durée absolue que vous avez définie précédemment.

  Depuis ONTAP 9.12.1, les fichiers WORM dont la période de conservation est définie sur `unspecified` Est garanti que la période de conservation est définie sur la période minimale de conservation configurée pour le volume SnapLock. Lorsque vous modifiez la période de rétention des fichiers de `unspecified` pour une durée de conservation absolue, la nouvelle durée de rétention spécifiée doit être supérieure à la durée de conservation minimale déjà définie sur le fichier.

Ainsi, si vous ne définissez pas explicitement la durée de rétention avant de valider un fichier en mode conformité à l'état WORM et que vous ne modifiez pas les valeurs par défaut, le fichier sera conservé pendant 30 ans. De même, si vous ne définissez pas explicitement la durée de rétention avant de valider un fichier Enterprise-mode à l'état WORM et que vous ne modifiez pas les valeurs par défaut, le fichier sera conservé pendant 0 ans, ou, de manière efficace, pas du tout.

Définir la période de conservation par défaut

Vous pouvez utiliser le `volume snaplock modify` Commande pour définir la période de conservation par défaut pour les fichiers d'un volume SnapLock.

Ce dont vous avez besoin

Le volume SnapLock doit être en ligne.

Description de la tâche

Le tableau suivant indique les valeurs possibles pour l'option de période de conservation par défaut :

> La période de conservation par défaut doit être supérieure ou égale à (>=) la période de rétention minimale et inférieure ou égale à (<=) la période de rétention maximale.

Valeur	Unité	Remarques
0 - 65535	secondes	

Valeur	Unité	Remarques
0 - 24	heures	
0 - 365	jours	
0 - 12	mois	
0 - 100	années	À partir d'ONTAP 9.10.1. Pour les versions antérieures de ONTAP, la valeur est comprise entre 0 et 70.
capacité	-	Utilisez la période de rétention maximale.
minimum	-	Utilisez la période de rétention minimale.
illimitée	-	Conservez toujours les fichiers.
non spécifié	-	Conservez les fichiers jusqu'à ce qu'une période de conservation absolue soit définie.

Les valeurs et les plages des périodes de rétention maximale et minimale sont identiques, sauf pour `max` et `min`, qui ne sont pas applicables. Pour plus d'informations sur cette tâche, voir "Définissez l'aperçu de la durée de conservation".

Vous pouvez utiliser le `volume snaplock show` commande pour afficher les paramètres de la période de rétention du volume. Pour plus d'informations, consultez la page man de la commande

> Une fois qu'un fichier a été engagé à l'état WORM, vous pouvez prolonger mais pas raccourcir la période de rétention.

Étapes

1. Définissez la période de conservation par défaut pour les fichiers d'un volume SnapLock :

   ```
   volume snaplock modify -vserver SVM_name -volume volume_name -default
   -retention-period default_retention_period -minimum-retention-period
   min_retention_period -maximum-retention-period max_retention_period
   ```

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   > Les exemples suivants supposent que les périodes de rétention minimale et maximale n'ont pas été modifiées auparavant.

   La commande suivante définit la période de conservation par défaut pour un volume Compliance ou Enterprise sur 20 jours :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

La commande suivante définit la période de conservation par défaut pour un volume Compliance sur 70 ans :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

La commande suivante définit la période de conservation par défaut pour un volume entreprise sur 10 ans :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Les commandes suivantes définissent la période de conservation par défaut pour un volume entreprise sur 10 jours :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

La commande suivante définit la période de conservation par défaut d'un volume Compliance sur infinie :

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Définissez explicitement la durée de rétention d'un fichier

Vous pouvez définir explicitement la durée de conservation d'un fichier en modifiant son heure de dernier accès. Vous pouvez utiliser n'importe quelle commande ou programme approprié via NFS ou CIFS pour modifier l'heure du dernier accès.

Description de la tâche

Une fois qu'un fichier a été enregistré sur WORM, vous pouvez prolonger mais pas réduire la durée de conservation. La durée de rétention est stockée dans le `atime` champ du fichier.

> Vous ne pouvez pas définir explicitement la durée de conservation d'un fichier sur `infinite`. Cette valeur n'est disponible que lorsque vous utilisez la période de rétention par défaut pour calculer la durée de rétention.

Étapes

1. Utilisez une commande ou un programme approprié pour modifier l'heure du dernier accès pour le fichier dont vous souhaitez définir la durée de rétention.

   Dans un shell UNIX, utilisez la commande suivante pour définir un temps de rétention de 21 novembre 2020 6 h 00 sur un fichier nommé `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

   > Vous pouvez utiliser n'importe quelle commande ou programme approprié pour modifier l'heure du dernier accès dans Windows.

Définissez la période de rétention des fichiers après un événement

À partir de ONTAP 9.3, vous pouvez définir la durée de conservation d'un fichier après un événement en utilisant la fonction SnapLock *Event Based Retention (EBR)*.

Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.

  "Créez un compte d'administrateur SnapLock"

- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Description de la tâche

La stratégie *Event Retention* définit la période de rétention du fichier après l'événement. La règle peut être appliquée à un seul fichier ou à tous les fichiers d'un répertoire.

- Si un fichier n'est pas un fichier WORM, il est mis à l'état WORM pour la période de conservation définie dans la stratégie.
- Si un fichier est un fichier WORM ou un fichier inscriptible WORM, sa période de conservation sera prolongée par la période de conservation définie dans la stratégie.

Vous pouvez utiliser un volume Compliance-mode ou Enterprise-mode.

> Les politiques EBR ne peuvent pas être appliquées aux fichiers en attente légale.

Pour une utilisation avancée, voir "Stockage WORM conforme avec NetApp SnapLock".

utilisation d'EBR pour prolonger la période de conservation des fichiers WORM déjà existants

EBR est pratique lorsque vous souhaitez prolonger la période de conservation des fichiers WORM existants. Par exemple, votre entreprise a peut-être pour politique de conserver les enregistrements W-4 des employés sous forme non modifiée pendant trois ans après que l'employé change de retenue d'impôt. Une autre politique de l'entreprise pourrait exiger que les enregistrements W-4 soient conservés pendant cinq ans après la cessation d'emploi de l'employé.

Dans ce cas, vous pouvez créer une police EBR avec une période de rétention de cinq ans. Une fois l'employé résilié (l'« événement »), vous appliqueriez la politique de l'EBR au registre W-4 de l'employé, ce qui entraînerait la prolongation de sa période de conservation. Ce processus est généralement plus simple que de prolonger manuellement la période de conservation, en particulier lorsqu'un grand nombre de fichiers sont impliqués.

Étapes

1. Créer une règle EBR :

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   La commande suivante crée la règle EBR `employee_exit` marche `vs1` avec une période de rétention de dix ans :

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. Appliquer une politique EBR :

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   La commande suivante applique la règle EBR `employee_exit` marche `vs1` à tous les fichiers du répertoire `d1`:

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Créer un journal d'audit

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, vous devez d'abord créer un agrégat SnapLock, puis créer un journal d'audit protégé par SnapLock avant d'effectuer une suppression privilégiée ou un déplacement de volume SnapLock. Le journal d'audit enregistre la création et la suppression de comptes administrateur SnapLock, les modifications du volume du journal, si la suppression privilégiée est activée, les opérations de suppression privilégiée et les opérations de déplacement de volume SnapLock.

Depuis ONTAP 9.10.1, vous ne créez plus d'agrégat SnapLock. Vous devez utiliser l'option -snaplock-type

pour "Créez un volume SnapLock de manière explicite" En spécifiant soit conformité, soit entreprise comme type SnapLock.

Avant de commencer

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, vous devez être administrateur du cluster pour créer un agrégat SnapLock.

Description de la tâche

Vous ne pouvez pas supprimer un journal d'audit tant que la période de conservation du fichier journal n'est pas écoulée. Vous ne pouvez pas modifier un journal d'audit même après la période de conservation écoulée. Ceci est vrai pour les modes SnapLock Compliance et Enterprise.

> Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas utiliser un volume SnapLock Enterprise pour la journalisation des audits. Vous devez utiliser un volume SnapLock Compliance. Dans ONTAP 9.5 et versions ultérieures, vous pouvez utiliser un volume SnapLock Enterprise ou un volume SnapLock Compliance pour la journalisation des audits. Dans tous les cas, le volume du journal d'audit doit être monté sur le Junction path `/snaplock_audit_log`. Aucun autre volume ne peut utiliser cette Junction path

Les journaux d'audit SnapLock sont disponibles dans le `/snaplock_log` répertoire sous la racine du volume du journal de vérification, dans les sous-répertoires nommés `privdel_log` (opérations de suppression privilégiée) et `system_log` (autres). Les noms des fichiers journaux d'audit contiennent l'horodatage de la première opération consignée, ce qui facilite la recherche des enregistrements en fonction de l'heure approximative d'exécution des opérations.

- Vous pouvez utiliser le `snaplock log file show` commande pour afficher les fichiers journaux sur le volume du journal d'audit.
- Vous pouvez utiliser le `snaplock log file archive` commande pour archiver le fichier journal actuel et en créer un nouveau, ce qui est utile dans les cas où vous devez enregistrer les informations du journal d'audit dans un fichier distinct.

Pour plus d'informations, consultez les pages de manuels des commandes.

> Un volume de protection des données ne peut pas être utilisé comme volume de journal d'audit SnapLock.

Étapes

1. Créer un agrégat SnapLock.

   Créer un agrégat SnapLock

2. Sur le SVM que vous voulez configurer pour la journalisation d'audit, créez un volume SnapLock.

   Créer un volume SnapLock

3. Configuration du SVM pour la journalisation d'audit :

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   -size size -retention-period default_retention_period
   ```

> La période de conservation minimale par défaut des fichiers journaux d'audit est de six mois. Si la période de conservation d'un fichier affecté est supérieure à la période de conservation du journal d'audit, la période de conservation du journal hérite de la période de conservation du fichier. Ainsi, si la période de conservation d'un fichier supprimé avec suppression privilégiée est de 10 mois et que la période de conservation du journal d'audit est de 8 mois, la période de conservation du journal est étendue à 10 mois. Pour plus d'informations sur la durée de conservation et la période de rétention par défaut, reportez-vous à la section "Définissez la durée de rétention".

La commande suivante configure `SVM1` Pour la journalisation des audits à l'aide du volume SnapLock `logVol`. Le journal d'audit a une taille maximale de 20 Go et est conservé pendant huit mois.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. Sur le SVM que vous avez configuré pour la journalisation d'audit, montez le volume SnapLock sur la Junction path `/snaplock_audit_log`.

   Montez un volume SnapLock

Vérifiez les paramètres SnapLock

Vous pouvez utiliser le `volume file fingerprint start` et `volume file fingerprint dump` Commandes permettant d'afficher des informations clés sur les fichiers et volumes, y compris le type de fichier (standard, WORM ou WORM appliable), la date d'expiration du volume, etc.

Étapes

1. Générer une empreinte de fichier :

   `volume file fingerprint start -vserver` *`SVM_name`* `-file` *`file_path`*

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   La commande génère un ID de session que vous pouvez utiliser comme entrée dans `volume file fingerprint dump` commande.

   > Vous pouvez utiliser le `volume file fingerprint show` Commande avec l'ID de session pour contrôler la progression de l'opération d'empreinte digitale. Assurez-vous que l'opération est terminée avant d'essayer d'afficher l'empreinte digitale.

2. Afficher l'empreinte du fichier :

   `volume file fingerprint dump -session-id` *`session_ID`*

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
```

```
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Gérer les fichiers WORM

Gérer les fichiers WORM

Vous pouvez gérer les fichiers WORM de l'une des manières suivantes :

- "Archivage des fichiers en mode WORM"
- "Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé"
- "Mise en miroir des fichiers WORM pour la reprise après incident"
- "Conservation des fichiers WORM en cas de litige"
- "Supprimez les fichiers WORM"

Archivage des fichiers en mode WORM

Vous pouvez archiver les fichiers en mode WORM (write once, read many) manuellement ou automatiquement. Vous pouvez également créer des fichiers modifiables WORM.

Archivage manuel des fichiers en mode WORM

Vous devez valider manuellement un fichier en mode WORM en le rendant en lecture seule. Vous pouvez utiliser n'importe quelle commande ou programme approprié sur NFS ou CIFS pour changer l'attribut lecture-écriture d'un fichier en lecture seule. Vous pouvez choisir de valider manuellement les fichiers si vous voulez vous assurer qu'une application a terminé l'écriture dans un fichier de sorte que le fichier n'est pas validé prématurément ou qu'il existe des problèmes de mise à l'échelle pour le scanner à validation automatique en raison d'un nombre élevé de volumes.

Ce dont vous avez besoin

- Le fichier à valider doit résider sur un volume SnapLock.
- Le fichier doit être accessible en écriture.

Description de la tâche

L'heure de la durée de la période de conformité du volume est écrite sur le `ctime` champ du fichier lors de l'exécution de la commande ou du programme. L'heure de la fin de l'horloge détermine quand la durée de conservation du fichier a été atteinte.

Étapes

1. Utilisez une commande ou un programme approprié pour modifier l'attribut lecture-écriture d'un fichier en lecture seule.

   Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture

seule :

```
chmod -w document.txt
```

Dans un shell Windows, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

```
attrib +r document.txt
```

Archivage automatique des fichiers sur WORM

La fonctionnalité d'autovalidation de SnapLock vous permet d'allouer automatiquement les fichiers en mode WORM. La fonction autocommit valide un fichier à l'état WORM sur un volume SnapLock si le fichier n'a pas été modifié pendant la période autocommit
durée. La fonction de validation automatique est désactivée par défaut.

Ce dont vous avez besoin

- Les fichiers que vous souhaitez effectuer une validation automatique doivent résider sur un volume SnapLock.
- Le volume SnapLock doit être en ligne.
- Le volume SnapLock doit être un volume en lecture/écriture.

> La fonction SnapLock autocommit analyse tous les fichiers du volume et valide un fichier s'il répond à l'exigence d'autocommit. Il peut y avoir un intervalle de temps entre le moment où le fichier est prêt pour la validation automatique et celui où il est réellement engagé par le scanner SnapLock autocommit. Cependant, le fichier est toujours protégé contre les modifications et la suppression par le système de fichiers dès qu'il est éligible à l'auto-validation.

Description de la tâche

Le paramètre *autocommit Period* spécifie le temps pendant lequel les fichiers doivent rester inchangés avant leur validation automatique. La modification d'un fichier avant que la période de validation automatique ne soit écoulée entraîne le redémarrage de la période de validation automatique du fichier.

Le tableau suivant présente les valeurs possibles pour la période de validation automatique :

Valeur	Unité	Remarques
Aucune	-	La valeur par défaut.
5 - 5256000	quelques minutes	-
1 - 87600	heures	-
1 - 3650	jours	-
1 - 120	mois	-

Valeur	Unité	Remarques
1 - 10	années	-

La valeur minimale est de 5 minutes et la valeur maximale est de 10 ans.

Étapes

1. Validation automatique des fichiers sur un volume SnapLock vers WORM :

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-autocommit -period` *`autocommit_period`*

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante valide automatiquement les fichiers sur le volume `vol1` Du SVM vs1, tant que les fichiers restent inchangés pendant 5 heures :

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

Créez un fichier d'ajout WORM

Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Vous pouvez utiliser n'importe quelle commande ou programme approprié pour créer un fichier compatible WORM, ou vous pouvez utiliser la fonction SnapLock *volume append mode* pour créer des fichiers compatibles WORM par défaut.

Utilisez une commande ou un programme pour créer un fichier inscriptible WORM

Vous pouvez utiliser n'importe quelle commande ou programme appropriée sur NFS ou CIFS pour créer un fichier compatible WORM. Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Les données sont ajoutées au fichier par blocs de 256 Ko. Au fur et à mesure que chaque bloc est écrit, le bloc précédent devient protégé par WORM. Vous ne pouvez pas supprimer le fichier tant que la période de conservation n'est pas écoulée.

Ce dont vous avez besoin

Le fichier fiable WORM doit résider sur un volume SnapLock.

Description de la tâche

Les données n'ont pas besoin d'être écrites de manière séquentielle dans le bloc actif de 256 Ko. Lorsque les données sont écrites sur l'octet n×256 Ko+1 du fichier, le segment 256 Ko précédent devient protégé par WORM.

Étapes

1. Utilisez une commande ou un programme approprié pour créer un fichier de longueur nulle avec le temps de rétention souhaité.

   Dans un shell UNIX, utilisez la commande suivante pour définir un temps de rétention de 21 novembre 2020 6 h 00 sur un fichier de longueur zéro nommé `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Utilisez une commande ou un programme approprié pour modifier l'attribut lecture-écriture du fichier en lecture seule.

   Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

   ```
   chmod 444 document.txt
   ```

3. Utilisez une commande ou un programme approprié pour remettre l'attribut de lecture-écriture du fichier en inscriptible.

   > Cette étape n'est pas considérée comme un risque de conformité, car aucune donnée n'est présente dans le fichier.

   Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` inscriptible :

   ```
   chmod 777 document.txt
   ```

4. Utilisez une commande ou un programme approprié pour commencer à écrire des données dans le fichier.

   Dans un shell UNIX, utiliser la commande suivante pour écrire des données sur `document.txt`:

   ```
   echo test data >> document.txt
   ```

   > Rétablissez les autorisations de fichier en lecture seule lorsque vous n'avez plus besoin d'ajouter des données au fichier.

Utilisez le mode d'ajout de volumes pour créer des fichiers d'ajout WORM

Depuis ONTAP 9.3, vous pouvez utiliser la fonctionnalité SnapLock *volume append mode* (VAM) pour créer par défaut des fichiers WORM utilisables. Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Les données sont ajoutées au fichier par blocs de 256 Ko. Au fur et à mesure que chaque bloc est écrit, le bloc précédent devient protégé par WORM. Vous ne pouvez pas supprimer le fichier tant que la période de conservation n'est pas écoulée.

Ce dont vous avez besoin

- Le fichier fiable WORM doit résider sur un volume SnapLock.
- Le volume SnapLock doit être démonté et vide des copies Snapshot et des fichiers créés par l'utilisateur.

Description de la tâche

Les données n'ont pas besoin d'être écrites de manière séquentielle dans le bloc actif de 256 Ko. Lorsque les données sont écrites sur l'octet n×256 Ko+1 du fichier, le segment 256 Ko précédent devient protégé par

WORM.

Si vous spécifiez une période de validation automatique pour le volume, les fichiers modifiables WORM qui ne sont pas modifiés pour une période supérieure à la période de validation automatique sont validés en mode WORM.

> Le mode VAM n'est pas pris en charge sur les volumes des journaux d'audit SnapLock.

Étapes

1. Activer VAM :

   `volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append -mode-enabled true|false`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante active le mode VAM sur le volume `vol1` De SVM`vs1`:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. Utilisez une commande ou un programme approprié pour créer des fichiers avec des autorisations d'écriture.

   Les fichiers sont par défaut modifiables.

Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé

Vous pouvez utiliser SnapLock pour SnapVault pour protéger les copies Snapshot WORM sur le stockage secondaire. Vous exécutez toutes les tâches SnapLock de base sur la destination du coffre-fort. Le volume de destination est automatiquement monté en lecture seule. Il est donc inutile de valider de manière explicite les copies Snapshot sur WORM. Ainsi, la création de copies Snapshot planifiées sur le volume de destination à l'aide des règles SnapMirror n'est pas prise en charge.

Avant de commencer

- Le cluster source doit exécuter ONTAP 8.2.2 ou version ultérieure.
- Les agrégats source et de destination doivent être de 64 bits.
- Le volume source ne peut pas être un volume SnapLock.
- Les volumes source et destination doivent être créés dans des clusters associés avec des SVM peering.

  Pour plus d'informations, voir "Peering de clusters".

- Si la croissance automatique du volume est désactivée, l'espace disponible sur le volume de destination doit être au moins cinq pour cent supérieur à l'espace utilisé sur le volume source.

Description de la tâche

Le volume source peut utiliser le stockage NetApp ou autre. Pour le stockage non NetApp, vous devez utiliser

la virtualisation FlexArray.

> Vous ne pouvez pas renommer une copie Snapshot engagée en état WORM.

Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock.

> Les LUN ne sont pas prises en charge dans les volumes SnapLock. Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

Depuis la version ONTAP 9.14.1, vous pouvez spécifier des périodes de conservation pour des étiquettes SnapMirror spécifiques dans la règle SnapMirror de la relation SnapMirror, de sorte que les copies Snapshot répliquées du volume source vers le volume de destination soient conservées pendant la période de conservation spécifiée dans la règle. Si aucune période de conservation n'est spécifiée, la période de rétention par défaut du volume de destination est utilisée.

À partir de ONTAP 9.13.1, vous pouvez restaurer instantanément une copie Snapshot verrouillée sur le volume SnapLock de destination d'une relation de copie SnapLock en créant une copie FlexClone avec `snaplock-type` Défini sur non snaplock et spécifiant la copie Snapshot comme « snapshot-parent » lors de l'exécution de l'opération de création du clone de volume. En savoir plus sur "Création d'un volume FlexClone avec un type SnapLock".

Pour les configurations MetroCluster, il est important de connaître les éléments suivants :

- Vous pouvez créer une relation SnapVault uniquement entre des SVM source synchrone, et non entre un SVM source synchrone et une SVM de destination synchrone.
- Vous pouvez créer une relation SnapVault depuis un volume d'un SVM source synchrone vers une SVM transmettant les données.
- Vous pouvez créer une relation SnapVault depuis un volume d'une SVM diffusant les données vers un volume DP au sein d'un SVM source synchrone.

L'illustration suivante montre la procédure d'initialisation d'une relation de coffre-fort SnapLock :

Étapes

1. Identifier le cluster de destination
2. Sur le cluster de destination, "Installez la licence SnapLock", "Initialiser l'horloge de conformité", Et, si vous utilisez une version de ONTAP antérieure à 9.10.1, "Créer un agrégat SnapLock".
3. Sur le cluster de destination, créez un volume de destination SnapLock de type `DP` taille identique ou supérieure à celle du volume source :

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
   -snaplock-type compliance|enterprise -type DP -size size
   ```

> Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1. Utilisez l'option volume -snaplock-type pour spécifier un type de volume Compliance ou Enterprise SnapLock. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock, conformité ou entreprise, est hérité de l'agrégat. Les volumes de destination flexibles de la version ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

La commande suivante crée un SnapLock de 2 Go `Compliance` volume nommé `dstvolB` dans `SVM2` sur l'agrégat `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Sur le cluster de destination, définissez la période de conservation par défaut, comme décrit dans Définir la période de conservation par défaut.

> Une période de conservation par défaut est affectée à un volume SnapLock cible du coffre-fort. La valeur pour cette période est initialement définie sur un minimum de 0 ans pour les volumes SnapLock Enterprise et un maximum de 30 ans pour les volumes SnapLock Compliance. À chaque copie NetApp Snapshot, toutes les copies NetApp Snapshot sont conservées pendant cette période de conservation par défaut. La période de conservation peut être prolongée ultérieurement, si nécessaire. Pour plus d'informations, voir Aperçu de la durée de conservation.

5. Créer une nouvelle relation de réplication Entre la source non SnapLock et la nouvelle destination SnapLock que vous avez créée à l'étape 3.

   Dans cet exemple, une nouvelle relation SnapMirror est créée avec un volume SnapLock de destination `dstvolB` à l'aide d'une règle de `XDPDefault` Pour archiver les copies Snapshot étiquetées tous les jours et toutes les semaines selon une planification horaire :

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

> Création d'une règle de réplication personnalisée ou un planification personnalisée si les valeurs par défaut disponibles ne sont pas appropriées.

6. Sur le SVM destination, initialiser la relation SnapVault créée à l'étape 5 :

   `snapmirror initialize -destination-path` *`destination_path`*

   La commande suivante initialise la relation entre le volume source `srcvolA` marche `SVM1` et le volume de destination `dstvolB` marche `SVM2`:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

7. Une fois la relation initialisée et inactive, utilisez le `snapshot show` Commande de la destination pour vérifier que la durée d'expiration du SnapLock est appliquée aux copies Snapshot répliquées.

   Cet exemple répertorie les copies Snapshot sur le volume `dstvolB` Étiquette SnapMirror et date d'expiration du SnapLock :

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
   snapmirror-label, snaplock-expiry-time
   ```

Informations associées

"Cluster et SVM peering"

"Sauvegarde de volume avec SnapVault"

Mise en miroir des fichiers WORM pour la reprise après incident

Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins autres que la reprise après incident. Le volume source et le volume de destination doivent être configurés pour SnapLock et les deux volumes doivent disposer du même mode SnapLock, Compliance ou Enterprise. Toutes les propriétés SnapLock clés du volume et les fichiers sont répliqués.

Prérequis

Les volumes source et destination doivent être créés dans des clusters associés avec des SVM peering. Pour plus d'informations, voir "Cluster et SVM peering".

Description de la tâche

- Depuis ONTAP 9.5, vous pouvez répliquer les fichiers WORM avec la relation SnapMirror de type XDP (protection étendue des données) plutôt qu'avec la relation de type DP (protection des données). Le mode XDP ne dépend pas de la version d'ONTAP. Il peut donc différencier les fichiers stockés dans le même bloc, ce qui facilite la resynchronisation des volumes du mode Compliance répliqué. Pour plus d'informations sur la conversion d'une relation de type DP existante en relation de type XDP, reportez-vous à "La protection des données".
- Une opération de resynchronisation dans une relation SnapMirror de type DP échoue pour un volume en mode conformité si SnapLock détermine qu'elle entraînera une perte de données. Si une opération de resynchronisation échoue, vous pouvez utiliser le `volume clone create` commande pour créer un clone du volume de destination. Vous pouvez ensuite resynchroniser le volume source avec le clone.
- Une relation SnapMirror de type XDP entre des volumes compatibles SnapLock prend en charge une resynchronisation après une interruption, même si les données de la destination ont divergé de la source après l'arrêt.

  Lors d'une resynchronisation, lorsque des divergences de données sont détectées entre la source et la destination au-delà du snapshot commun, un nouvel instantané est coupé sur la destination pour capturer cette divergence. Le nouvel instantané et le snapshot commun sont tous deux verrouillés avec un temps de rétention comme suit :

  - Heure d'expiration du volume de la destination
  - Si le délai d'expiration du volume est passé ou n'a pas été défini, le snapshot est verrouillé pendant une période de 30 jours

    - Si la destination dispose de mises en attente légales, la période d'expiration du volume réel est masquée et apparaît comme « indéfinie », mais l'instantané est verrouillé pendant la durée de la période d'expiration du volume réel.

Si le volume de destination a une période d'expiration postérieure à la source, la période d'expiration de destination est conservée et ne sera pas écrasée par la période d'expiration du volume source après la resynchronisation.

Si la destination dispose de mentions légales qui diffèrent de la source, une resynchronisation n'est pas autorisée. La source et la destination doivent disposer de mentions légales identiques ou toutes les mentions légales de la destination doivent être libérées avant toute tentative de resynchronisation.

Une copie Snapshot verrouillée sur le volume de destination créé pour capturer les données divergentes peut être copiée vers la source à l'aide de la CLI en exécutant le `snapmirror update -s snapshot` commande. Une fois copié, le snapshot reste également verrouillé à la source.

- Les relations de protection des données des SVM ne sont pas prises en charge.
- Les relations de protection des données de partage de charge ne sont pas prises en charge.

L'illustration suivante montre la procédure d'initialisation d'une relation SnapMirror :

System Manager

Depuis ONTAP 9.12.1, System Manager vous permet de configurer la réplication SnapMirror des fichiers WORM.

Étapes

1. Accédez à **Storage > volumes**.
2. Cliquez sur **Afficher/Masquer** et sélectionnez **Type SnapLock** pour afficher la colonne dans la fenêtre **volumes**.
3. Recherchez un volume SnapLock.
4. Cliquez sur ⋮ Et sélectionnez **protéger**.
5. Choisir le cluster de destination et la VM de stockage de destination
6. Cliquez sur **plus d'options**.
7. Sélectionnez **Afficher les règles héritées** et **DPDefault (TDA/TDE/s)**.
8. Dans la section **Détails de configuration de destination**, sélectionnez **remplacer le programme de transfert** et sélectionnez **horaire**.
9. Cliquez sur **Enregistrer**.
10. À gauche du nom du volume source, cliquez sur la flèche pour développer les détails du volume, puis, à droite de la page, consultez les informations relatives à la protection SnapMirror distante.
11. Sur le cluster distant, accédez à **protection relations**.
12. Localisez la relation et cliquez sur le nom du volume de destination pour afficher les détails de la relation.
13. Vérifiez que le type de SnapLock du volume de destination et d'autres informations SnapLock.

CLI

1. Identifier le cluster de destination
2. Sur le cluster de destination, "Installez la licence SnapLock", "Initialiser l'horloge de conformité", Et, si vous utilisez une version de ONTAP antérieure à 9.10.1, "Créer un agrégat SnapLock".
3. Sur le cluster de destination, créez un volume de destination SnapLock de type `DP` taille identique ou supérieure à celle du volume source :

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1. Utilisez l'option volume -snaplock-type pour spécifier un type de volume Compliance ou Enterprise SnapLock. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock—Compliance ou Enterprise—est hérité de l'agrégat. Les volumes de destination flexibles de la version ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

   La commande suivante crée un SnapLock de 2 Go `Compliance` volume nommé `dstvolB` dans `SVM2` sur l'agrégat `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Sur le SVM de destination, créer une règle SnapMirror :

   snapmirror policy create -vserver *SVM_name* -policy *policy_name*

   La commande suivante crée la politique au niveau du SVM `SVM1-mirror`:

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```

5. Sur le SVM de destination, créer une planification SnapMirror :

   job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*

   La commande suivante crée une planification SnapMirror nommée `weekendcron`:

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek
   "Saturday, Sunday" -hour 3 -minute 0
   ```

6. Sur le SVM de destination, créer une relation SnapMirror :

   snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*

   La commande suivante crée une relation SnapMirror entre le volume source `srcvolA` marche `SVM1` et le volume de destination `dstvolB` marche `SVM2`, et affecte la stratégie `SVM1-mirror` et le planning `weekendcron`:

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
   weekendcron
   ```

   > Le type XDP est disponible dans ONTAP 9.5 et versions ultérieures. Vous devez utiliser le type DP dans ONTAP 9.4 et versions antérieures.

7. Sur le SVM de destination, initialiser la relation SnapMirror :

   snapmirror initialize -destination-path *destination_path*

   Le processus d'initialisation effectue un transfert *baseline* vers le volume de destination. SnapMirror effectue une copie Snapshot du volume source, puis transfère la copie ainsi que tous les blocs de données qu'il renvoie au volume de destination. Il transfère également toutes les autres copies Snapshot du volume source vers le volume de destination.

La commande suivante initialise la relation entre le volume source `srcvolA` marche `SVM1` et le volume de destination `dstvolB` marche `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Informations associées

"Cluster et SVM peering"

"Préparation de la reprise après incident de volume"

"Protection des données"

Conservation des fichiers WORM en cas de litiges avec la conservation légale

À partir de ONTAP 9.3, vous pouvez conserver des fichiers WORM en mode conformité pendant la durée d'un litige en utilisant la fonction *Legal Hold*.

Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.

  "Créez un compte d'administrateur SnapLock"

- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Description de la tâche

Un fichier placé dans une mise en attente légale se comporte comme un fichier WORM ayant une période de conservation indéfinie. Il est de votre responsabilité de préciser à quel moment la période de conservation légale prend fin.

Le nombre de fichiers que vous pouvez placer sous conservation légale dépend de l'espace disponible sur le volume.

Étapes

1. Démarrer une mise en garde légale :

   `snaplock legal-hold begin -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   La commande suivante démarre une mise en attente légale pour tous les fichiers dans `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Mettre fin à l'attente légale :

   `snaplock legal-hold end -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

La commande suivante met fin à la mise en attente légale de tous les fichiers dans `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Vue d'ensemble de la suppression des fichiers WORM

Vous pouvez supprimer des fichiers WORM en mode entreprise pendant la période de conservation à l'aide de la fonction de suppression privilégiée.
Avant de pouvoir utiliser cette fonction, vous devez créer un compte administrateur SnapLock, puis activer la fonction à l'aide du compte.

Créez un compte d'administrateur SnapLock

Vous devez disposer des privilèges d'administrateur SnapLock pour effectuer une suppression privilégiée. Ces privilèges sont définis dans le rôle vsadmin-snaplock. Si ce rôle n'est pas encore attribué, vous pouvez demander à l'administrateur du cluster de créer un compte d'administrateur SVM avec le rôle d'administrateur SnapLock.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Étapes

1. Créer un compte administrateur SVM avec le rôle d'administrateur SnapLock :

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   La commande suivante active le compte d'administrateur du SVM `SnapLockAdmin` avec le prédéfini `vsadmin-snaplock` rôle d'accès `SVM1` utilisation d'un mot de passe :

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

Activer la fonction de suppression privilégiée

Vous devez activer explicitement la fonction de suppression privilégiée sur le volume entreprise contenant les fichiers WORM que vous souhaitez supprimer.

Description de la tâche

La valeur du `-privileged-delete` détermine si la suppression privilégiée est activée. Les valeurs possibles sont `enabled`, `disabled`, et `permanently-disabled`.

> `permanently-disabled` est l'état du terminal. Vous ne pouvez pas activer la suppression privilégiée sur le volume après avoir défini l'état sur `permanently-disabled`.

Étapes

1. Activer la suppression privilégiée pour un volume SnapLock Enterprise :

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   La commande suivante active la fonction de suppression privilégiée pour le volume entreprise `dataVol` marche `SVM1`:

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

Supprimez les fichiers WORM en mode entreprise

Vous pouvez utiliser la fonction de suppression privilégiée pour supprimer des fichiers WORM en mode entreprise pendant la période de conservation.

Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.
- Vous devez avoir créé un journal d'audit SnapLock et activé la fonctionnalité de suppression privilégiée sur le volume entreprise.

Description de la tâche

Vous ne pouvez pas utiliser une opération de suppression privilégiée pour supprimer un fichier WORM expiré. Vous pouvez utiliser le `volume file retention show` Commande pour afficher la durée de conservation du fichier WORM que vous souhaitez supprimer. Pour plus d'informations, consultez la page man de la commande

Étape

1. Supprimez un fichier WORM sur un volume d'entreprise :

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   La commande suivante supprime le fichier `/vol/dataVol/f1` Sur le SVM`SVM1`:

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```

Déplacer un volume SnapLock

Depuis ONTAP 9.8, vous pouvez déplacer un volume SnapLock vers un agrégat de destination du même type (entreprise vers entreprise ou conformité vers conformité).

Vous devez avoir le rôle de sécurité SnapLock pour déplacer un volume SnapLock.

Créez un compte administrateur de sécurité SnapLock

Pour effectuer un déplacement de volume SnapLock, vous devez disposer des privilèges administrateur de sécurité SnapLock. Ce privilège vous est accordé avec le rôle *SnapLock*, introduit dans ONTAP 9.8. Si ce rôle n'est pas encore attribué, vous pouvez demander à votre administrateur de cluster de créer un utilisateur de sécurité SnapLock avec ce rôle de sécurité SnapLock.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Description de la tâche

Le rôle SnapLock est associé au SVM admin, contrairement au rôle vsadmin-snaplock, qui est associé au SVM de données.

Étape

1. Créer un compte administrateur SVM avec le rôle d'administrateur SnapLock :

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   La commande suivante active le compte d'administrateur du SVM `SnapLockAdmin` avec le prédéfini `snaplock` Rôle permettant d'accéder à la SVM d'admin `cluster1` utilisation d'un mot de passe :

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

Déplacer un volume SnapLock

Vous pouvez utiliser le `volume move` Commande de déplacement d'un volume SnapLock vers un agrégat de destination.

Ce dont vous avez besoin

- Vous devez avoir créé un journal d'audit protégé SnapLock avant d'effectuer le déplacement de volume SnapLock.

  "Créer un journal d'audit".

- Si vous utilisez une version de ONTAP antérieure à ONTAP 9.10.1, l'agrégat de destination doit être du même type SnapLock que le volume SnapLock que vous souhaitez déplacer : conformité à la conformité ou entreprise à la norme. Depuis ONTAP 9.10.1, cette restriction est supprimée et un agrégat peut inclure des volumes Compliance et Enterprise SnapLock, ainsi que des volumes non SnapLock.
- Vous devez être un utilisateur ayant le rôle de sécurité SnapLock.

Étapes

1. Via une connexion sécurisée, connectez-vous à la LIF de gestion du cluster ONTAP :

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Déplacer un volume SnapLock :

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
-aggregate destination_aggregate_name
```

3. Vérifier l'état de l'opération de déplacement de volume :

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
volume,phase,vserver
```

Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware

Depuis ONTAP 9.12.1, vous pouvez verrouiller une copie Snapshot sur un volume non SnapLock pour vous protéger des attaques par ransomware. Le verrouillage des copies Snapshot permet de ne pas les supprimer accidentellement ou accidentellement.

La fonction horloge de conformité de SnapLock vous permet de verrouiller les copies Snapshot pendant une période spécifiée, de sorte qu'elles ne puissent pas être supprimées tant que l'heure d'expiration n'est pas atteinte. Le verrouillage des copies Snapshot est inviolable, ce qui les protège contre les menaces de ransomware. Vous pouvez utiliser des copies Snapshot verrouillées pour récupérer des données si un volume est compromis par une attaque par ransomware.

À partir de la version ONTAP 9.14.1, le verrouillage des copies Snapshot prend en charge les copies Snapshot à conservation à long terme sur les destinations des coffres-forts SnapLock et sur les volumes de destination SnapMirror non SnapLock. Le verrouillage des copies Snapshot est activé en définissant la période de conservation à l'aide des règles de règles SnapMirror associées à un libellé de police existant. La règle remplace la période de rétention par défaut définie sur le volume. Si aucune période de conservation n'est associée au label SnapMirror, la période de conservation par défaut du volume est utilisée.

Exigences et considérations relatives à la non-conformité des copies Snapshot

- Si vous utilisez l'interface de ligne de commandes ONTAP, tous les nœuds du cluster doivent exécuter ONTAP 9.12.1 ou une version ultérieure. Si vous utilisez System Manager, tous les nœuds doivent exécuter ONTAP 9.13.1 ou une version ultérieure.
- "La licence SnapLock doit être installée sur le cluster". Cette licence est incluse dans "ONTAP One".
- "L'horloge de conformité du cluster doit être initialisée".
- Lorsque le verrouillage Snapshot est activé sur un volume, vous pouvez mettre à niveau les clusters vers une version d'ONTAP ultérieure à ONTAP 9.12.1 ; Cependant, vous ne pouvez pas revenir à une version antérieure de ONTAP tant que toutes les copies Snapshot verrouillées n'ont pas atteint leur date d'expiration. Elles sont supprimées et le verrouillage des copies Snapshot est désactivé.
- Lorsqu'un snapshot est verrouillé, la durée d'expiration du volume est définie sur la date d'expiration de la copie Snapshot. Si plusieurs copies Snapshot sont verrouillées, la date d'expiration du volume reflète la date d'expiration la plus élevée parmi toutes les copies Snapshot.
- La période de conservation des copies Snapshot verrouillées est prioritaire sur le nombre de copies Snapshot conservées. En d'autres termes, la limite de conservation des copies Snapshot n'est pas respectée si la période de conservation des copies Snapshot verrouillées n'a pas expiré.
- Dans une relation SnapMirror, vous pouvez définir une période de conservation sur une règle de stratégie de copie en miroir et la période de conservation est appliquée aux copies Snapshot répliquées vers la

destination si le volume de destination est activé pour le verrouillage des copies Snapshot. La période de conservation est prioritaire sur le nombre de copies. Par exemple, les copies Snapshot qui n'ont pas dépassé leur expiration seront conservées même si le nombre de copies à conserver est dépassé.

- Vous pouvez renommer une copie Snapshot sur un volume non SnapLock. Les opérations de renommage de snapshot sur le volume principal d'une relation SnapMirror sont reflétées sur le volume secondaire uniquement si la règle est MirrorAllsnapshots. Pour les autres types de règles, la copie Snapshot renommée n'est pas propagée lors des mises à jour.
- Si vous utilisez l'interface de ligne de commandes de ONTAP, vous pouvez restaurer une copie Snapshot verrouillée avec `volume snapshot restore` Commande uniquement si la copie Snapshot verrouillée est la plus récente. Si des copies Snapshot non expirées sont présentes dans la suite de la restauration, l'opération de restauration de copie Snapshot échoue.

Fonctionnalités prises en charge par les copies Snapshot inviolables

- Volumes FlexGroup

  Le verrouillage des copies Snapshot est pris en charge sur les volumes FlexGroup. Le verrouillage des snapshots n'a lieu que sur la copie Snapshot du composant racine. La suppression du volume FlexGroup n'est autorisée que si la durée d'expiration du composant racine est passée.

- Conversion FlexVol en FlexGroup

  Vous pouvez convertir un volume FlexVol avec des copies Snapshot verrouillées en un volume FlexGroup. Les copies Snapshot restent verrouillées après la conversion.

- Clone de volume et de fichiers

  Vous pouvez créer des clones de volumes et de fichiers à partir d'une copie Snapshot verrouillée.

Fonctions non prises en charge

Les fonctionnalités suivantes ne sont actuellement pas prises en charge par les copies Snapshot inviolables :

- Cloud Volumes ONTAP
- Groupes de cohérence
- FabricPool
- Volumes FlexCache
- Bande SMtape
- Continuité de l'activité SnapMirror (SM-BC)
- Règle SnapMirror utilisant le `-schedule` paramètre
- SnapMirror synchrone
- Mobilité des données des SVM (utilisé pour la migration ou le déplacement d'un SVM d'un cluster source vers un cluster destination)

Activez le verrouillage des copies Snapshot lors de la création d'un volume

Depuis ONTAP 9.12.1, vous pouvez activer le verrouillage des copies Snapshot lorsque vous créez un nouveau volume ou que vous modifiez un volume existant à l'aide du `-snapshot-locking-enabled` avec le `volume create` et `volume modify` Dans l'interface de ligne de commande. Depuis la version ONTAP 9.13.1, System Manager permet le verrouillage des copies Snapshot.

System Manager

1. Naviguez jusqu'à **stockage > volumes** et sélectionnez **Ajouter**.
2. Dans la fenêtre **Ajouter un volume**, choisissez **plus d'options**.
3. Entrez le nom du volume, sa taille, la règle d'export et le nom du partage.
4. Sélectionnez **Activer le verrouillage des instantanés**. Cette sélection ne s'affiche pas si la licence SnapLock n'est pas installée.
5. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
6. Enregistrez les modifications.
7. Dans la fenêtre **volumes**, sélectionnez le volume que vous avez mis à jour et choisissez **vue d'ensemble**.
8. Vérifiez que **SnapLock snapshot Copy Locking** affiche **enabled**.

CLI

1. Pour créer un nouveau volume et activer le verrouillage des copies Snapshot, entrez la commande suivante :

   ```
   volume create -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

   La commande suivante permet de verrouiller les copies Snapshot sur un nouveau volume nommé vol1 :

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Activez le verrouillage des copies Snapshot sur un volume existant

Depuis la version ONTAP 9.12.1, vous pouvez activer le verrouillage des copies Snapshot sur un volume existant à l'aide de l'interface de ligne de commande ONTAP. Depuis ONTAP 9.13.1, vous pouvez utiliser System Manager pour activer le verrouillage des copies Snapshot sur un volume existant.

System Manager

1. Accédez à **Storage > volumes**.
2. Sélectionnez ⋮ Et choisissez **Modifier > Volume**.
3. Dans la fenêtre **Modifier le volume**, localisez la section Paramètres des copies Snapshot (local) et sélectionnez **Activer le verrouillage des instantanés**.

   Cette sélection ne s'affiche pas si la licence SnapLock n'est pas installée.

4. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
5. Enregistrez les modifications.
6. Dans la fenêtre **volumes**, sélectionnez le volume que vous avez mis à jour et choisissez **vue d'ensemble**.
7. Vérifiez que **SnapLock snapshot Copy Locking** affiche **enabled**.

CLI

1. Pour modifier un volume existant afin d'activer le verrouillage des copies Snapshot, entrez la commande suivante :

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

Créez une règle de copie Snapshot verrouillée et appliquez la conservation

Depuis ONTAP 9.12.1, vous pouvez créer des règles de copie Snapshot pour appliquer une période de conservation de copies Snapshot et appliquer la règle à un volume afin de verrouiller les copies Snapshot pour la période spécifiée. Vous pouvez également verrouiller une copie Snapshot en définissant manuellement une période de conservation. Depuis ONTAP 9.13.1, System Manager permet de créer des règles de verrouillage des copies Snapshot et de les appliquer à un volume.

Créer une règle de verrouillage des copies Snapshot

System Manager

1. Accédez à **Storage > Storage VM** et sélectionnez une VM de stockage.
2. Sélectionnez **Paramètres**.
3. Localisez **stratégies d'instantanés** et sélectionnez →.
4. Dans la fenêtre **Ajouter une stratégie d'instantanés**, entrez le nom de la stratégie.
5. Sélectionnez + Add .
6. Fournissez les détails de la planification de la copie Snapshot, notamment le nom de la planification, le nombre maximal de copies Snapshot à conserver et la période de conservation SnapLock.
7. Dans la colonne **SnapLock Retention Period**, entrez le nombre d'heures, de jours, de mois ou d'années pour conserver les copies instantanées. Par exemple, une règle de copie Snapshot avec une période de conservation de 5 jours verrouille une copie Snapshot pendant 5 jours à compter de sa création. Elle ne peut pas être supprimée pendant cette période. Les périodes de conservation suivantes sont prises en charge :
   - Années: 0 - 100
   - Mois: 0 - 1200
   - Jours: 0 - 36500
   - Heures: 0 - 24
8. Enregistrez les modifications.

CLI

1. Pour créer une règle de copie Snapshot, entrez la commande suivante :

   ```
   volume snapshot policy create -policy policy_name -enabled true -schedule1
   schedule1_name -count1 maximum_Snapshot_copies -retention-period1
   _retention_period
   ```

   La commande suivante crée une règle de verrouillage des copies Snapshot :

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   Une copie Snapshot n'est pas remplacée si la conservation est active ; autrement dit, le nombre de conservation n'est pas respecté si des copies Snapshot verrouillées n'ont pas encore expiré.

Application d'une politique de verrouillage à un volume

System Manager

1. Accédez à **Storage > volumes**.
2. Sélectionnez ⋮ Et choisissez **Modifier > Volume**.
3. Dans la fenêtre **Edit Volume**, sélectionnez **Schedule Snapshot copies**.
4. Sélectionnez la règle de verrouillage des copies Snapshot dans la liste.
5. Si le verrouillage des copies Snapshot n'est pas déjà activé, sélectionnez **Activer le verrouillage des instantanés**.
6. Enregistrez les modifications.

CLI

1. Pour appliquer une règle de verrouillage des copies Snapshot à un volume existant, entrez la commande suivante :

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

Appliquez une période de conservation à la création manuelle de copies Snapshot

Vous pouvez appliquer une période de conservation des copies Snapshot lorsque vous créez manuellement une copie Snapshot. Le verrouillage des copies Snapshot doit être activé sur le volume, sinon le paramètre de période de conservation est ignoré.

System Manager

1. Accédez à **stockage > volumes** et sélectionnez un volume.
2. Dans la page de détails du volume, sélectionnez l'onglet **copies Snapshot**.
3. Sélectionnez + Add .
4. Indiquez le nom de la copie Snapshot et la date d'expiration du SnapLock. Vous pouvez sélectionner le calendrier pour choisir la date et l'heure d'expiration de la conservation.
5. Enregistrez les modifications.
6. Sur la page **volumes > copies instantanées**, sélectionnez **Afficher/Masquer** et choisissez **SnapLock expiration Time** pour afficher la colonne **SnapLock expiration Time** et vérifier que la durée de conservation est définie.

CLI

1. Pour créer une copie Snapshot manuellement et appliquer une période de conservation de verrouillage, entrez la commande suivante :

   `volume snapshot create -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-snaplock-expiry-time` *`expiration_date_time`*

   La commande suivante crée une nouvelle copie Snapshot et définit la période de conservation :

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Appliquez une période de conservation à une copie Snapshot existante

System Manager

1. Accédez à **stockage > volumes** et sélectionnez un volume.
2. Dans la page de détails du volume, sélectionnez l'onglet **copies Snapshot**.
3. Sélectionnez la copie Snapshot, puis ⋮, Et choisissez **Modifier le temps d'expiration SnapLock**. Vous pouvez sélectionner le calendrier pour choisir la date et l'heure d'expiration de la conservation.
4. Enregistrez les modifications.
5. Sur la page **volumes > copies instantanées**, sélectionnez **Afficher/Masquer** et choisissez **SnapLock expiration Time** pour afficher la colonne **SnapLock expiration Time** et vérifier que la durée de conservation est définie.

CLI

1. Pour appliquer manuellement une période de conservation à une copie Snapshot existante, entrez la commande suivante :

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   L'exemple suivant applique une période de conservation à une copie Snapshot existante :

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Modifiez une stratégie existante pour appliquer la conservation à long terme

Depuis la version ONTAP 9.14.1, vous pouvez modifier une règle SnapMirror existante en ajoutant une règle afin de définir la conservation à long terme des copies Snapshot. La règle permet de remplacer la période de conservation par défaut du volume sur les destinations du coffre-fort SnapLock et sur les volumes de destination non SnapLock SnapMirror.

1. Ajouter une règle à une règle SnapMirror existante :

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of Snapshot copies> -retention
   -period [<integer> days|months|years]
   ```

   L'exemple suivant crée une règle qui applique une période de rétention de 6 mois à la stratégie existante appelée « lockvault » :

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

Les API SnapLock

Vous pouvez utiliser les API Zephyr pour intégrer la fonctionnalité SnapLock dans les scripts ou l'automatisation des flux de travail. Les API utilisent la messagerie XML via

HTTP, HTTPS et Windows DCE/RPC. Pour plus d'informations, voir "Documentation sur l'automatisation ONTAP".

abandon-empreinte-fichier

Annuler une opération d'empreinte digitale de fichier.

fichier-empreinte-dump

Affiche les informations relatives aux empreintes digitales du fichier.

fichier-empreinte-get-iter

Affiche l'état des opérations d'empreinte des fichiers.

démarrage de fichier-empreinte-fichier

Générez une empreinte de fichier.

snaplock-archive-vserver-log

Archivez le fichier journal d'audit actif.

snaplock-create-vserver-log

Créer une configuration de journal d'audit pour un SVM.

snaplock-delete-vserver-log

Supprime une configuration du journal d'audit pour une SVM.

snaplock-file-privileged-delete

Exécutez une opération de suppression privilégiée.

snaplock-get-file-retention

Obtenir la période de conservation d'un fichier.

snaplock-get-node-conformité-clock

Obtenir la date et l'heure de la fin de l'horloge du nœud.

snaplock-get-vserver-active-log-files-iter

Affiche l'état des fichiers journaux actifs.

snaplock-get-vserver-log-iter

Afficher la configuration du journal d'audit.

snaplock-modify-vserver-log

Modifier la configuration du journal d'audit d'un SVM

snaplock-set-file-conservation

Définissez la durée de conservation d'un fichier.

snaplock-set-node-compliance-clock

Définissez la date et l'heure de la fin de l'horloge du nœud.

snaplock-volume-set-privileged-delete

Définissez l'option Privileged-delete sur un volume SnapLock Enterprise.

volumes-get-snaplock-attrs

Obtenir les attributs d'un volume SnapLock.

volume-set-snaplock-attrs

Définissez les attributs d'un volume SnapLock.

Groupes de cohérence

Présentation des groupes de cohérence

Un groupe de cohérence est un ensemble de volumes gérés comme une seule unité. Dans ONTAP, les groupes de cohérence simplifient la gestion et garantissent la protection d'une charge de travail applicative couvrant plusieurs volumes.

Pour simplifier la gestion du stockage, vous pouvez utiliser des groupes de cohérence. Imaginez que vous disposez d'une base de données importante couvrant 20 LUN. Vous pouvez gérer les LUN de manière individuelle ou les traiter comme un jeu de données unique, les organiser au sein d'un même groupe de cohérence.

Les groupes de cohérence facilitent la gestion des charges de travail des applications en fournissant des règles de protection locales et distantes facilement configurées, ainsi que des copies Snapshot cohérentes au niveau des applications ou après panne d'un ensemble de volumes à un point dans le temps. Les copies Snapshot d'un groupe de cohérence permettent de restaurer l'ensemble d'une charge de travail applicative.

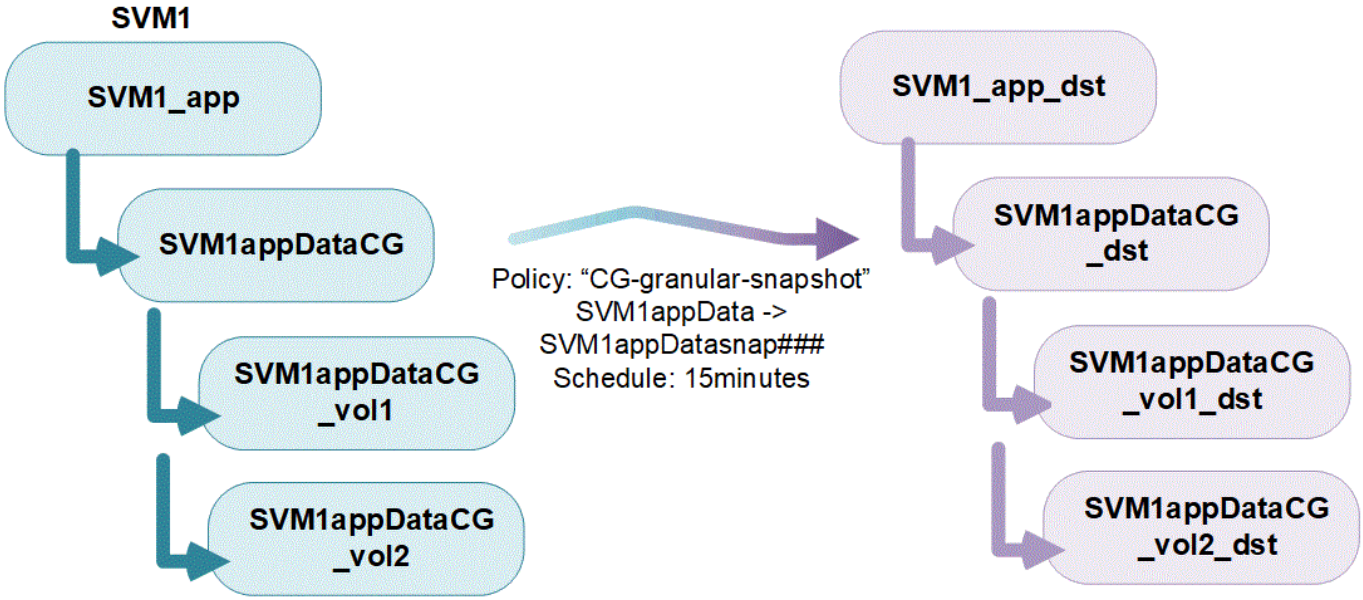
En savoir plus sur les groupes de cohérence

Les groupes de cohérence prennent en charge n'importe quel volume FlexVol, quel que soit le protocole (NAS, SAN ou NVMe). Ils peuvent être gérés via l'API REST de ONTAP ou dans System Manager, dans l'élément de menu **stockage > groupes de cohérence**. Depuis la version ONTAP 9.14.1, la gestion des groupes de cohérence peut s'effectuer via l'interface de ligne de commandes ONTAP.

Les groupes de cohérence peuvent exister sous la forme d'entités individuelles, sous la forme d'un ensemble de volumes, ou dans une relation hiérarchique constituée d'autres groupes de cohérence. Les volumes individuels peuvent disposer de leur propre règle Snapshot granulaire par volume. En outre, des règles Snapshot peuvent être définies au niveau du groupe de cohérence. Le groupe de cohérence ne peut avoir

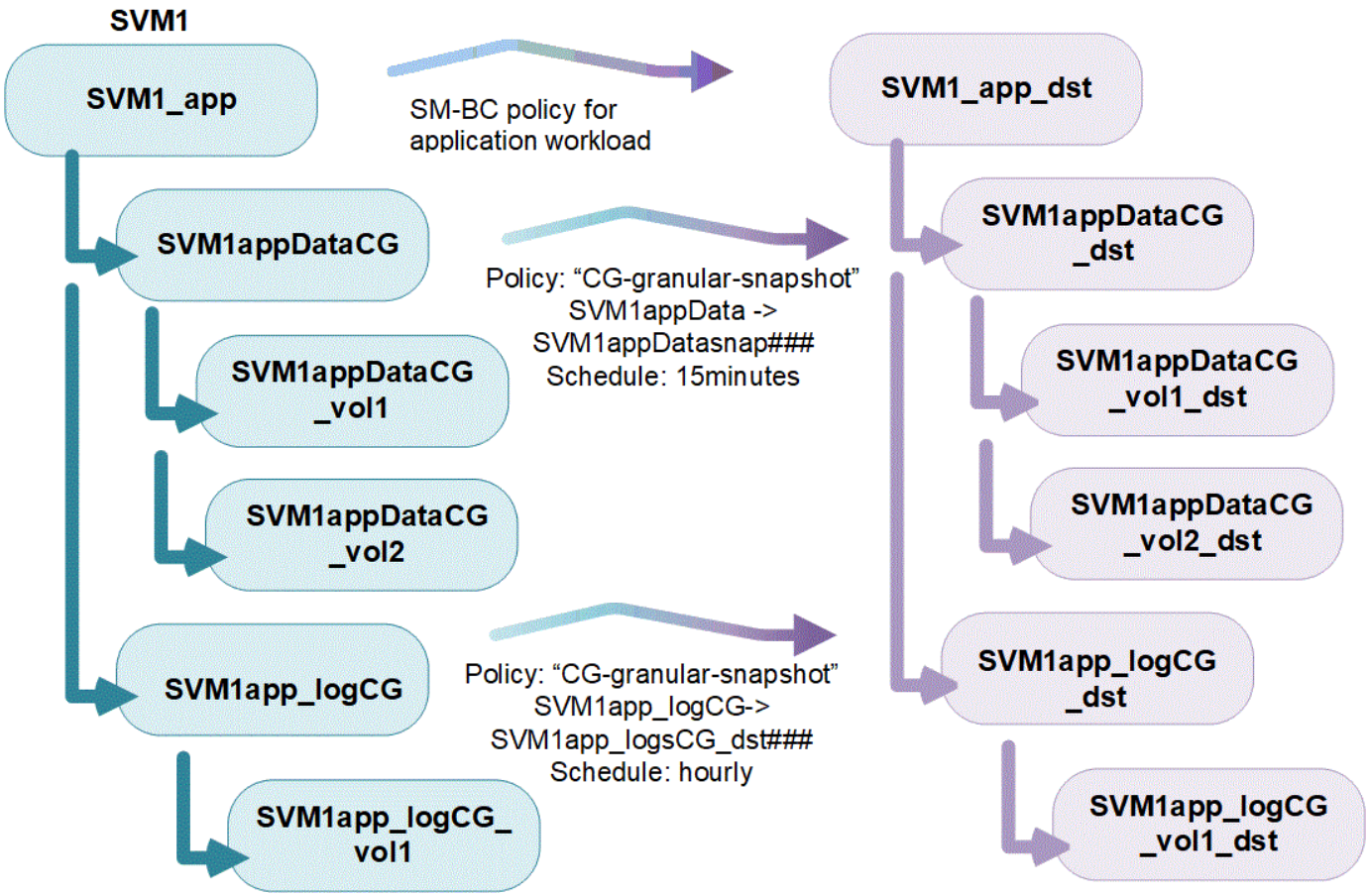
qu'une seule relation SnapMirror Business Continuity (SM-BC) et une politique SM-BC partagée, qui peut être utilisée pour restaurer l'ensemble du groupe de cohérence.

Le graphique suivant illustre l'utilisation possible d'un groupe de cohérence individuel. Données d'une application hébergée sur `SVM1` s'étend sur deux volumes : `vol1` et `vol2`. Une règle Snapshot définie sur le groupe de cohérence capture des copies Snapshot des données toutes les 15 minutes.



Des charges de travail applicatives plus importantes peuvent nécessiter plusieurs groupes de cohérence. Dans ce cas, vous pouvez créer des groupes de cohérence hiérarchiques, où un seul groupe de cohérence devient les composants enfants d'un groupe de cohérence parent. Le groupe de cohérence parent peut inclure au maximum cinq groupes de cohérence enfant. Comme dans les groupes de cohérence individuels, une stratégie de protection SM-BC distante peut être appliquée à la configuration complète des groupes de cohérence (parents et enfants) pour restaurer la charge de travail de l'application.

Dans l'exemple suivant, une application est hébergée sur `SVM1`. L'administrateur a créé un groupe de cohérence parent, `SVM1_app`, qui inclut deux groupes de cohérence enfant : `SVM1appDataCG` pour les données et `SVM1app_logCG` pour les journaux. Chaque groupe de cohérence enfant dispose de sa propre règle Snapshot. Copies Snapshot des volumes dans `SVM1appDataCG` sont prises toutes les 15 minutes. Snapshots de `SVM1app_logCG` sont prises toutes les heures. Groupe de cohérence parent `SVM1_app` Dispose d'une politique SM-BC qui réplique les données pour assurer un service continu en cas d'incident.



Depuis la version ONTAP 9.12.1, les groupes de cohérence sont pris en charge clonage et en modifiant les membres de la cohérence par ajout ou suppression de volumes Dans System Manager et dans l’API REST de ONTAP. Depuis la version ONTAP 9.12.1, l’API REST ONTAP prend également en charge :

- Création de groupes de cohérence avec de nouveaux volumes NFS ou SMB ou espaces de noms NVMe.
- Ajout de volumes NFS ou SMB ou d’espaces de noms NVMe nouveaux ou existants à des groupes de cohérence existants.

Pour plus d’informations sur l’API REST de ONTAP, reportez-vous à "Documentation de référence de l’API REST ONTAP".

Surveillez les groupes de cohérence

À partir de la version ONTAP 9.13.1, les groupes de cohérence assurent le contrôle de la capacité et des performances en temps réel et historiques, offrant ainsi un aperçu des performances des applications et des groupes de cohérence individuels.

Les données de surveillance sont actualisées toutes les cinq minutes et sont conservées jusqu’à un an. Vous pouvez suivre les mesures pour :

- Performances : IOPS, latence et débit
- Capacité : taille, logique utilisée, disponible

Vous pouvez afficher les données de surveillance dans l’onglet **Présentation** du menu Groupe de cohérence dans System Manager ou en les demandant dans l’API REST. Depuis la version ONTAP 9.14.1, vous pouvez afficher les metrics des groupes de cohérence via l’interface de ligne de commandes du système

`consistency-group metrics show` commande.

> Dans ONTAP 9.13.1, vous pouvez uniquement récupérer les metrics historiques à l'aide de l'API REST. Depuis la version ONTAP 9.14.1, les indicateurs d'historique sont également disponibles dans System Manager.

Protégez les groupes de cohérence

La protection est assurée par des groupes de cohérence :

- Règles relatives aux snapshots
- Continuité de l'activité SnapMirror (SM-BC)
- [mcc] (À partir de ONTAP 9.11.1)
- Réplication asynchrone SnapMirror (À partir de ONTAP 9.13.1)
- "Reprise d'activité de SVM" (À partir de ONTAP 9.14.1)

La création d'un groupe de cohérence n'active pas automatiquement la protection. Il est possible de définir des règles de protection locale et à distance lors de la création ou après la création d'un groupe de cohérence.

Pour configurer la protection sur un groupe de cohérence, reportez-vous à la section "Protéger un groupe de cohérence".

Pour utiliser la protection à distance, vous devez répondre aux exigences de Déploiements de continuité de l'activité SnapMirror.

> Les relations SM-BC ne peuvent pas être établies sur les volumes montés pour l'accès NAS.

Groupes de cohérence dans les configurations MetroCluster

Depuis ONTAP 9.11.1, vous pouvez provisionner les groupes de cohérence avec de nouveaux volumes sur un cluster dans une configuration MetroCluster. Ces volumes sont provisionnés sur des agrégats en miroir.

Une fois ces agrégats provisionnés, vous pouvez déplacer les volumes associés aux groupes de cohérence entre les agrégats en miroir et non mis en miroir. Les volumes associés à des groupes de cohérence peuvent donc être situés sur des agrégats en miroir, des agrégats sans mise en miroir, ou les deux. Vous pouvez modifier les agrégats en miroir contenant des volumes associés à des groupes de cohérence pour ne plus mettre en miroir. De même, vous pouvez modifier les agrégats non mis en miroir contenant les volumes associés à des groupes de cohérence pour activer la mise en miroir.

Les volumes et les copies Snapshot associés aux groupes de cohérence placés sur des agrégats en miroir sont répliqués sur le site distant (site B). Le contenu des volumes sur le site B garantit l'ordre d'écriture du groupe de cohérence, ce qui vous permet d'effectuer une restauration depuis le site B en cas d'incident. Vous pouvez accéder aux copies Snapshot de groupe de cohérence à l'aide du groupe de cohérence avec l'API REST et System Manager sur les clusters exécutant ONTAP 9.11.1 ou version ultérieure. Depuis la version ONTAP 9.14.1, vous pouvez également accéder aux copies Snapshot via l'interface de ligne de commandes ONTAP.

Si certains ou l'ensemble des volumes associés à un groupe de cohérence se trouvent sur des agrégats non mis en miroir qui ne sont pas actuellement accessibles, LES opérations D'OBTENTION ou DE SUPPRESSION du groupe de cohérence se comportent comme si les volumes locaux ou les agrégats d'hébergement sont hors ligne.

Configurations de groupes de cohérence pour la réplication

Si le site B exécute ONTAP 9.10.1 ou une version antérieure, seuls les volumes associés aux groupes de cohérence situés sur les agrégats en miroir sont répliqués sur le site B. Les configurations de groupes de cohérence sont uniquement répliquées vers le site B, si les deux sites exécutent ONTAP 9.11.1 ou une version ultérieure. Une fois le site B mis à niveau vers ONTAP 9.11.1, les données destinées aux groupes de cohérence du site A où tous leurs volumes associés sont répliqués sur le site B.

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

Mise à niveau

Les groupes de cohérence créés avec SM-BC dans ONTAP 9.8 et 9.9.1 seront automatiquement mis à niveau et gérables sous **stockage > groupes de cohérence** dans System Manager ou l'API REST ONTAP lors de la mise à niveau vers ONTAP 9.10.1 ou version ultérieure. Pour plus d'informations sur la mise à niveau à partir de ONTAP 9.8 ou 9.9.1, reportez-vous à la section "Considérations relatives à la mise à niveau et à la restauration de SM-BC".

Les copies Snapshot de groupe de cohérence créées dans l'API REST peuvent être gérées via l'interface de groupe de cohérence de System Manager et via les terminaux d'API REST de groupe de cohérence. Depuis la version ONTAP 9.14.1, les snapshots des groupes de cohérence peuvent également être gérés à l'aide de l'interface de ligne de commandes ONTAP.

> Copies Snapshot créées à l'aide des commandes ONTAPI `cg-start` et `cg-commit` Sont reconnues comme des copies Snapshot de groupe de cohérence et ne peuvent donc pas être gérées via l'interface de groupe de cohérence de System Manager ou les terminaux de groupe de cohérence de l'API REST ONTAP. Depuis la version ONTAP 9.14.1, ces copies Snapshot peuvent être mises en miroir sur le volume de destination si vous utilisez une règle SnapMirror asynchrone. Pour plus d'informations, voir Configurer la protection SnapMirror asynchrone.

Fonctionnalités prises en charge par version

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Groupes de cohérence hiérarchiques	✓	✓	✓	✓	✓
Protection locale grâce aux copies Snapshot	✓	✓	✓	✓	✓
Continuité de l'activité SnapMirror	✓	✓	✓	✓	✓
Prise en charge de MetroCluster	✓	✓	✓	✓	
Validations en deux phases (API REST uniquement)	✓	✓	✓	✓	
Balises d'application et de composant	✓	✓	✓		
Cloner des groupes de cohérence	✓	✓	✓		

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Ajouter et supprimer des volumes	✓	✓	✓		
Créez un CGS avec de nouveaux volumes NAS	✓	✓	API REST uniquement		
Créez un CGS avec les nouveaux espaces de noms NVMe	✓	✓	API REST uniquement		
Déplacez des volumes entre des groupes de cohérence enfants	✓	✓			
Modifier la géométrie du groupe de cohérence	✓	✓			
Contrôle	✓	✓			
SnapMirror asynchrone (groupes de cohérence uniques uniquement)	✓	✓			
Reprise d'activité de SVM (groupes de cohérence uniques uniquement)	✓				
Prise en charge de la CLI	✓				

En savoir plus sur les groupes de cohérence

Plus d'informations

- "Documentation sur l'automatisation ONTAP"
- Continuité de l'activité SnapMirror
- Principes de base de la reprise sur incident asynchrone SnapMirror

- "Documentation MetroCluster"

Limites des groupes de cohérence

Lors de la planification et de la gestion de vos groupes de cohérence, prenez en compte les limites d'objets au sein du cluster et du groupe de cohérence parent ou enfant.

Limites imposées

Le tableau suivant indique les limites des groupes de cohérence. Des limites distinctes s'appliquent aux groupes de cohérence à l'aide de SnapMirror Business Continuity (SM-BC). Pour plus d'informations, voir "Restrictions et limitations de SM-BC pour les limites".

Limite	Portée	Minimum	Maximum
Nombre de groupes de cohérence	Cluster	0	Identique au nombre maximum de volumes dans le cluster
Nombre de groupes de cohérence parent	Cluster	0	Identique au nombre maximum de volumes dans le cluster
Nombre de groupes de cohérence individuels et parents	Cluster	0	Identique au nombre maximum de volumes dans le cluster
Nombre de volumes dans un groupe de cohérence	Groupe de cohérence unique	1 volume	80 volumes
Nombre de volumes dans l'enfant d'un groupe de cohérence parent	Groupe de cohérence parent	1 volume	80 volumes
Nombre de volumes dans un groupe de cohérence enfant	Groupe de cohérence enfant	1 volume	80 volumes
Nombre de groupes de cohérence enfants dans un groupe de cohérence parent	Groupe de cohérence parent	1 groupe de cohérence	5 groupes de cohérence
Nombre de relations de reprise d'activité du SVM où existe un groupe de cohérence (disponible depuis la ONTAP 9.14.1)	Cluster	0	32

Limites non appliquées

La planification minimale des copies Snapshot prise en charge pour les groupes de cohérence est de 30 minutes. Elle est basée sur "Test des FlexGroups", Qui partagent la même infrastructure Snapshot que les groupes de cohérence.

Configurez un seul groupe de cohérence

Les groupes de cohérence peuvent être créés avec des volumes existants ou de nouveaux LUN ou volumes (selon la version de ONTAP). Un volume ou une LUN ne peut être associé qu'à un seul groupe de cohérence à la fois.

Description de la tâche

- Dans les ONTAP 9.10.1 à 9.11.1, la modification des volumes membres d'un groupe de cohérence après sa création n'est pas prise en charge.

  Depuis la version ONTAP 9.12.1, vous pouvez modifier les volumes membres d'un groupe de cohérence. Pour plus d'informations sur ce processus, reportez-vous à la section Modifier un groupe de cohérence.

Créez un groupe de cohérence avec les nouvelles LUN ou les nouveaux volumes

Dans ONTAP 9.10.1 à 9.12.1, vous pouvez créer un groupe de cohérence à l'aide de nouvelles LUN. Depuis ONTAP 9.13.1, System Manager prend également en charge la création d'un groupe de cohérence avec de nouveaux namespaces NVMe ou de nouveaux volumes NAS. (Ceci est également pris en charge par l'API REST ONTAP à partir de ONTAP 9.12.1.)

System Manager

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Add**, puis sélectionnez le protocole de votre objet de stockage.

   Dans ONTAP 9.10.1 à 9.12.1, la seule option pour un nouvel objet de stockage est **en utilisant de nouvelles LUN**. Depuis ONTAP 9.13.1, System Manager prend en charge la création de groupes de cohérence avec de nouveaux namespaces NVMe et de nouveaux volumes NAS.

3. Nommer le groupe de cohérence. Indiquez le nombre de volumes ou de LUN et la capacité par volume ou LUN.
   a. **Type d'application** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type d'application. Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans Balises d'application et de composant. Si vous prévoyez de créer un groupe de cohérence avec une stratégie de protection à distance, vous devez utiliser **Other**.
   b. Pour **nouveaux LUN** : sélectionnez le système d'exploitation hôte et le format de LUN. Entrez les informations sur l'initiateur hôte.
   c. Pour **nouveaux volumes NAS** : choisissez l'option d'exportation appropriée (NFS ou SMB/CIFS) en fonction de la configuration NAS de votre SVM.
   d. Pour **nouveaux espaces de noms NVMe** : sélectionnez le système d'exploitation hôte et le sous-système NVMe.
4. Pour configurer des stratégies de protection, ajoutez un groupe de cohérence enfant ou des autorisations d'accès, sélectionnez **plus d'options**.
5. Sélectionnez **Enregistrer**.
6. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail terminé. Si vous définissez une stratégie de protection, vous savez qu'elle a été appliquée lorsque vous voyez un bouclier vert sous regarder sous la stratégie appropriée, distant ou local.

CLI

À partir de la version ONTAP 9.14.1, vous pouvez créer un groupe de cohérence avec les nouveaux volumes via l'interface de ligne de commandes ONTAP. Les paramètres spécifiques dépendent si les volumes sont SAN, NVMe ou NFS.

Créez un groupe de cohérence avec les volumes NFS

1. Créer le groupe de cohérence :

```
consistency-group create -vserver SVM_name -consistency-group consistency-
group-name -volume volume-prefix -volume-count number -size size -export
-policy policy_name
```

Créez un groupe de cohérence avec des volumes SAN

1. Créer le groupe de cohérence :

```
consistency-group create -vserver SVM_name -consistency-group consistency-
group-name -lun lun_name -size size -lun-count number -igroup igroup_name
```

Créez un groupe de cohérence avec les namespaces NVMe

1. Créer le groupe de cohérence :

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group_name -namespace namespace_name -volume-count number
   -namespace-count number -size size -subsystem subsystem_name
   ```

Après avoir terminé

1. Vérifiez que votre groupe de cohérence a été créé à l'aide de `consistency-group show` commande.

Créez un groupe de cohérence avec les volumes existants

Vous pouvez utiliser des volumes existants pour créer un groupe de cohérence.

System Manager

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Ajouter** puis **en utilisant des volumes existants**.
3. Nommez le groupe de cohérence et sélectionnez la VM de stockage.
   a. **Type d'application** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type d'application. Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans Balises d'application et de composant. Si le groupe de cohérence a une relation SM-BC, vous devez utiliser **autre**.
4. Sélectionnez les volumes existants à inclure. Seuls les volumes qui ne font pas déjà partie d'un groupe de cohérence seront disponibles à la sélection.

   > Si vous créez un groupe de cohérence avec des volumes existants, le groupe de cohérence prend en charge les volumes FlexVol. Il est possible d'ajouter des volumes avec des relations SnapMirror asynchrones ou synchrones aux groupes de cohérence, mais ils ne en tiennent pas compte pour les groupes de cohérence. Les groupes de cohérence ne prennent pas en charge les compartiments S3 ni les machines virtuelles de stockage avec des relations SVMDR.

5. Sélectionnez **Enregistrer**.
6. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail ONTAP terminé. Si vous avez choisi une règle de protection, vérifiez qu'elle a été correctement définie en sélectionnant votre groupe de cohérence dans le menu. Si vous définissez une stratégie de protection, vous savez qu'elle a été appliquée lorsque vous voyez un bouclier vert sous regarder sous la stratégie appropriée, distant ou local.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer un groupe de cohérence avec les volumes existants à l'aide de l'interface de ligne de commandes ONTAP.

Étapes

1. Émettez le `consistency-group create` commande. Le `-volumes` le paramètre accepte une liste de noms de volumes séparés par des virgules.

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
   ```

2. Affichez votre groupe de cohérence à l'aide du `consistency-group show` commande.

Étapes suivantes

- Protéger un groupe de cohérence
- Modifier un groupe de cohérence
- Cloner un groupe de cohérence

Configurez un groupe de cohérence hiérarchique

Les groupes de cohérence hiérarchiques vous permettent de gérer des charges de travail

volumineuses couvrant plusieurs volumes. En effet, vous créez un groupe de cohérence parent qui sert de parapluie pour les groupes de cohérence enfant.

Les groupes de cohérence hiérarchiques ont un parent qui peut inclure jusqu'à cinq groupes de cohérence individuels. Les groupes de cohérence hiérarchiques peuvent prendre en charge différentes règles Snapshot locales sur plusieurs groupes de cohérence ou volumes individuels. Si vous utilisez une règle de protection à distance, elle s'applique à l'ensemble du groupe de cohérence hiérarchique (parent et enfant).

À partir de ONTAP 9.13.1, vous pouvez modifier la géométrie de vos groupes de cohérence et déplacez des volumes entre des groupes de cohérence enfants.

Pour connaître les limites d'objets relatives aux groupes de cohérence, reportez-vous à la section Limites d'objets pour les groupes de cohérence.

Créez un groupe de cohérence hiérarchique avec de nouveaux LUN ou volumes

Lorsque vous créez un groupe de cohérence hiérarchique, vous pouvez le remplir avec de nouvelles LUN. Depuis la version ONTAP 9.13.1, vous pouvez également utiliser de nouveaux espaces de noms NVMe et volumes NAS.

System Manager

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Add**, puis sélectionnez le protocole de votre objet de stockage.

   Dans ONTAP 9.10.1 à 9.12.1, la seule option pour un nouvel objet de stockage est **en utilisant de nouvelles LUN**. Depuis ONTAP 9.13.1, System Manager prend en charge la création de groupes de cohérence avec de nouveaux namespaces NVMe et de nouveaux volumes NAS.

3. Nommer le groupe de cohérence. Indiquez le nombre de volumes ou de LUN et la capacité par volume ou LUN.
   a. **Type d'application** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type d'application. Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans Balises d'application et de composant. Si vous prévoyez d'utiliser une stratégie de protection à distance, vous devez choisir **autre**.
4. Sélectionnez le système d'exploitation hôte et le format LUN. Entrez les informations sur l'initiateur hôte.
   a. Pour **nouveaux LUN** : sélectionnez le système d'exploitation hôte et le format de LUN. Entrez les informations sur l'initiateur hôte.
   b. Pour **nouveaux volumes NAS** : choisissez l'option d'exportation appropriée (NFS ou SMB/CIFS) en fonction de la configuration NAS de votre SVM.
   c. Pour **nouveaux espaces de noms NVMe** : sélectionnez le système d'exploitation hôte et le sous-système NVMe.
5. Pour ajouter un groupe de cohérence enfant, sélectionnez **plus d'options** puis **+Ajouter un groupe de cohérence enfant**.
6. Sélectionnez le niveau de performance, le nombre de LUN ou de volumes et la capacité par LUN ou volume. Indiquez les configurations d'exportation ou les informations du système d'exploitation appropriées en fonction du protocole que vous utilisez.
7. Vous pouvez également sélectionner une stratégie de snapshot locale et définir les autorisations d'accès.
8. Répétez l'opération pour jusqu'à cinq groupes de cohérence enfant.
9. Sélectionnez **Enregistrer**.
10. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail ONTAP terminé. Si vous définissez une stratégie de protection, examinez la stratégie appropriée, à distance ou locale, qui doit afficher un bouclier vert avec une coche.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer un nouveau groupe de cohérence hiérarchique à l'aide de l'interface de ligne de commandes.

Étape

1. Créez le nouveau groupe de cohérence à l'aide de `consistency-group create` commande.

   Le `volume-count` le paramètre définit le nombre de volumes de chaque groupe de cohérence enfant. Vous pouvez créer un groupe de cohérence parent avec un maximum de cinq groupes de

cohérence enfant.

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -cg-count number_of_child_consistency_groups
-volume volume_prefix -volume-count number -size size -export-policy
policy_name -storage-service extreme
```

Créez un groupe de cohérence hiérarchique avec les volumes existants

Vous pouvez organiser des volumes existants en un groupe de cohérence hiérarchique.

System Manager

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez **+Ajouter** puis **en utilisant des volumes existants**.
3. Sélectionnez la VM de stockage.
4. Sélectionnez les volumes existants à inclure. Seuls les volumes qui ne font pas déjà partie d'un groupe de cohérence seront disponibles à la sélection.
5. Pour ajouter un groupe de cohérence enfant, sélectionnez **+Ajouter un groupe de cohérence enfant**. Créez les groupes de cohérence nécessaires, qui seront nommés automatiquement.
   a. **Type de composant** : si vous utilisez ONTAP 9.12.1 ou version ultérieure, sélectionnez un type de composant "données", "logs" ou "autre". Si aucune valeur n'est sélectionnée, le groupe de cohérence se voit attribuer le type de **autre** par défaut. En savoir plus sur la cohérence du balisage dans Balises d'application et de composant. Si vous prévoyez d'utiliser une stratégie de protection à distance, vous devez utiliser **autre**.
6. Attribuez des volumes existants à chaque groupe de cohérence.
7. Si vous le souhaitez, sélectionnez une règle Snapshot locale.
8. Répétez l'opération pour jusqu'à cinq groupes de cohérence enfant.
9. Sélectionnez **Enregistrer**.
10. Vérifiez que votre groupe de cohérence a été créé en retournant au menu principal du groupe de cohérence sur lequel il apparaîtra une fois le travail ONTAP terminé. Si vous avez choisi une stratégie de protection, vérifiez qu'elle a été correctement définie en sélectionnant votre groupe de cohérence dans le menu ; sous le type de stratégie approprié, vous verrez un bouclier vert avec une coche à l'intérieur de celle-ci.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer un groupe de cohérence hiérarchique à l'aide de l'interface de ligne de commandes.

Étapes

1. Provisionner un nouveau groupe de cohérence parent et attribuer des volumes à un nouveau groupe de cohérence enfant :

   ```
   consistency-group create -vserver svm_name -consistency-group
   child_consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volumes volume_names
   ```

2. Entrez `y` pour confirmer la création d'un groupe de cohérence parent et enfant.

Étapes suivantes

- Modifier la géométrie d'un groupe de cohérence
- Modifier un groupe de cohérence
- Protéger un groupe de cohérence

Protégez les groupes de cohérence

Les groupes de cohérence offrent une protection locale et à distance simple à gérer pour les applications SAN, NAS et NVMe couvrant plusieurs volumes.

La création d'un groupe de cohérence n'active pas automatiquement la protection. Les règles de protection peuvent être définies au moment de la création ou après la création du groupe de cohérence. Vous pouvez protéger les groupes de cohérence à l'aide des éléments suivants :

- Copies Snapshot locales
- Continuité de l'activité SnapMirror (SM-BC)
- MetroCluster (début 9.11.1)
- SnapMirror asynchrone (début 9.13.1)
- Reprise d'activité asynchrone d'un SVM (début 9.14.1)

Si vous utilisez des groupes de cohérence imbriqués, vous pouvez définir différentes règles de protection pour les groupes de cohérence parent et enfant.

À partir de la version ONTAP 9.11.1, les groupes de cohérence proposent Création de copies Snapshot de groupe de cohérence en deux phases. L'opération Snapshot en deux phases exécute un pré-contrôle, en s'assurant que la copie Snapshot est correctement capturée.

La restauration peut être effectuée pour un groupe de cohérence entier, un seul groupe de cohérence dans une configuration hiérarchique ou pour des volumes individuels dans un groupe de cohérence. La restauration peut être effectuée en sélectionnant le groupe de cohérence à partir duquel vous souhaitez effectuer une restauration, en sélectionnant le type de copie Snapshot, puis en identifiant la copie Snapshot pour laquelle repose la restauration. Pour plus d'informations sur ce processus, voir "Restaurez un volume à partir d'une copie Snapshot antérieure".

Configurer une règle Snapshot locale

La définition d'une règle de protection locale des snapshots permet de créer une stratégie couvrant tous les volumes d'un groupe de cohérence.

Description de la tâche

La planification minimale des copies Snapshot prise en charge pour les groupes de cohérence est de 30 minutes. Elle est basée sur "Test des FlexGroups", Qui partagent la même infrastructure Snapshot que les groupes de cohérence.

System Manager

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence que vous avez créé dans le menu Groupe de cohérence.
3. Dans le coin supérieur droit de la page de vue d'ensemble du groupe de cohérence, sélectionnez **Modifier**.
4. Cochez la case en regard de **planifier les copies Snapshot (locales)**.
5. Sélectionnez une règle Snapshot. Pour configurer une nouvelle règle personnalisée, reportez-vous à la section "Création d'une règle de protection des données personnalisée".
6. Sélectionnez **Enregistrer**.
7. Revenez au menu de présentation du groupe de cohérence. Dans la colonne de gauche sous **copies snapshot (local)**, l'état est protégé à côté de .

CLI

Depuis la version ONTAP 9.14.1, vous pouvez modifier la règle de protection d'un groupe de cohérence à l'aide de l'interface de ligne de commandes.

Étape

1. Exécutez la commande suivante pour définir ou modifier la règle de protection :

   Si vous modifiez la règle de protection d'une cohérence enfant, vous devez identifier le groupe de cohérence parent à l'aide de `-parent-consistency-group` *`parent_consistency_group_name`* paramètre.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Créer une copie Snapshot à la demande

Si vous devez créer une copie Snapshot de votre groupe de cohérence en dehors d'une règle normalement planifiée, vous pouvez en créer une à la demande.

System Manager

Étapes

1. Accédez à **Storage** > **groupes de cohérence**.
2. Sélectionnez le groupe de cohérence pour lequel vous souhaitez créer une copie Snapshot à la demande.
3. Passez à l'onglet **copies instantanées**, puis sélectionnez **+Ajouter**.
4. Indiquez un **Nom** et un **libellé SnapMirror**. Dans le menu déroulant **cohérence**, sélectionnez **cohérence application** ou **cohérence collision**.
5. Sélectionnez **Enregistrer**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer une copie Snapshot à la demande d'un groupe de cohérence à l'aide de l'interface de ligne de commandes.

Étape

1. Créer la copie Snapshot :

   Par défaut, le type de Snapshot est cohérent après panne. Vous pouvez modifier le type de snapshot avec l'option `-type` paramètre.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Créez des copies Snapshot de groupe de cohérence en deux phases

Depuis la version ONTAP 9.11.1, les groupes de cohérence prennent en charge les validations en deux phases pour la création des copies Snapshot de groupe de cohérence, qui exécutent un précontrôle avant la validation de la copie Snapshot. Cette fonctionnalité n'est disponible qu'avec l'API REST de ONTAP.

La création de copies Snapshot de groupe de cohérence biphasées est uniquement disponible pour la création de copies Snapshot, et non pour le provisionnement des groupes de cohérence ou la restauration des groupes de cohérence.

Un Snapshot de groupe de cohérence biphasé divise le processus de création des snapshots en deux phases :

1. Dans la première phase, l'API exécute des contrôles préalables et déclenche la création de snapshots. La première phase inclut un paramètre de délai d'expiration, indiquant la durée pendant laquelle la copie Snapshot doit être validée.
2. Si la demande de la phase un s'exécute correctement, vous pouvez appeler la deuxième phase dans l'intervalle désigné à partir de la première phase, en archivant la copie Snapshot sur le terminal approprié.

Avant de commencer

- Pour utiliser la création Snapshot de groupe de cohérence en deux phases, tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou version ultérieure.
- Une seule invocation active d'une opération Snapshot de groupe de cohérence est prise en charge sur une instance de groupe de cohérence à la fois, qu'il s'agisse d'une ou deux phases. Toute tentative d'appel d'une opération de snapshot alors qu'une autre opération est en cours entraîne un échec.

- Lorsque vous appelez la création de Snapshot, vous pouvez définir une valeur de délai d'attente facultative comprise entre 5 et 120 secondes. Si aucune valeur de temporisation n'est fournie, l'opération expire par défaut à 7 secondes. Dans l'API, définissez la valeur du délai d'attente avec le `action_timeout` paramètre. Dans l'interface de ligne de commandes, utilisez `-timeout` drapeau.

Étapes

Vous pouvez réaliser une copie Snapshot en deux phases avec l'API REST ou, depuis ONTAP 9.14.1, avec l'interface de ligne de commandes ONTAP. Cette opération n'est pas prise en charge dans System Manager.

> Si vous appelez la création de Snapshot avec l'API, vous devez valider la copie Snapshot avec l'API. Si vous appelez la création de Snapshot avec l'interface de ligne de commandes, vous devez valider la copie Snapshot avec l'interface de ligne de commandes. Les méthodes de mélange ne sont pas prises en charge.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez créer une copie Snapshot en deux phases à l'aide de l'interface de ligne de commandes.

Étapes

1. Lancer l'instantané :

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Vérifier que l'instantané a été pris :

   ```
   consistency-group snapshot show
   ```

3. Valider le snapshot :

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Appelez la création du Snapshot. Envoyez une demande POST au terminal du groupe de cohérence à l'aide de `action=start` paramètre.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. Si la demande de POST réussit, le résultat inclut un UUID d'instantané. En utilisant cet UUID, envoyez une demande de CORRECTIF pour valider la copie Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Définissez la protection à distance pour un groupe de cohérence

Les groupes de cohérence offrent une protection à distance via SM-BC et, depuis ONTAP 9.13.1, SnapMirror asynchrone.

Configurez la protection avec SM-BC

Vous pouvez utiliser SM-BC pour vous assurer que les copies Snapshot des groupes de cohérence créés dans votre groupe de cohérence sont copiées vers la destination. Pour en savoir plus sur SM-BC ou sur la configuration de SM-BC à l'aide de l'interface de ligne de commande, reportez-vous à la section Configuration de la protection pour la continuité de l'activité.

Avant de commencer

- Les relations SM-BC ne peuvent pas être établies sur les volumes montés pour l'accès NAS.
- Les étiquettes de règles doivent correspondre dans le cluster source et dans le cluster destination.
- SM-BC ne réplique pas les copies Snapshot par défaut, sauf si une règle avec étiquette SnapMirror est ajoutée au prédéfini `AutomatedFailOver` La règle et les copies Snapshot sont créées avec cette étiquette.

  Pour en savoir plus sur ce processus, voir "Protégez avec SM-BC".

- Déploiements en cascade Ne sont pas pris en charge par SM-BC.
- À partir de ONTAP 9.13.1, vous pouvez réaliser des opérations sans interruption ajouter des volumes à un groupe de cohérence Avec une relation SM-BC active. Toute autre modification apportée à un groupe de cohérence entraîne une interruption de la relation SM-BC, la modification du groupe de cohérence, puis la restauration et la resynchronisation de la relation.

> Pour configurer SM-BC avec l'interface de ligne de commande, reportez-vous à la section Protégez avec SM-BC.

Étapes pour System Manager

1. Assurez-vous d'avoir rencontré le "Conditions préalables à l'utilisation de SM-BC".
2. Sélectionnez **stockage > groupes de cohérence**.
3. Sélectionnez le groupe de cohérence que vous avez créé dans le menu Groupe de cohérence.
4. En haut à droite de la page de présentation, sélectionnez **plus** puis **protéger**.

5. System Manager remplit automatiquement les informations côté source. Sélectionnez le cluster et la VM de stockage appropriés pour la destination. Sélectionnez une stratégie de protection. Vérifier que **Initialize relation** est coché.
6. Sélectionnez **Enregistrer**.
7. Le groupe de cohérence doit être initialisé et synchronisé. Vérifiez que la synchronisation s'est bien terminée en retournant au menu **groupe de cohérence**. L'état **SnapMirror (Remote)** s'affiche `Protected` à côté de .

Configurer la protection SnapMirror asynchrone

Depuis la version ONTAP 9.13.1, vous pouvez configurer la protection SnapMirror asynchrone pour un groupe de cohérence unique. 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.

Description de la tâche

Pour répliquer des copies Snapshot granulaires par volume, vous devez exécuter ONTAP 9.14.1 ou une version ultérieure. Pour les règles MirrorAndVault et Vault, l'étiquette SnapMirror de la règle Snapshot granulaire des volumes doit correspondre à la règle de règle SnapMirror du groupe de cohérence. Les snapshots granulaires par volume respectent la règle SnapMirror du groupe de cohérence, qui est calculée indépendamment des snapshots du groupe de cohérence. Par exemple, si une règle permet de conserver deux copies Snapshot sur la destination, vous pouvez avoir deux copies Snapshot granulaires au niveau du volume et deux copies Snapshot de groupe de cohérence.

Lors de la resynchronisation de la relation SnapMirror avec des copies Snapshot granulaires par volume, vous pouvez conserver les copies Snapshot granulaires par volume avec le `-preserve` drapeau. Les copies Snapshot granulaires par volume, plus récentes que les copies Snapshot du groupe de cohérence, sont conservées. Si aucune copie Snapshot de groupe de cohérence n'est créée, aucune copie Snapshot granulaire par volume ne peut être transférée lors de l'opération de resynchronisation.

Avant de commencer

- La protection asynchrone SnapMirror n'est disponible que pour les groupes de cohérence uniques. Elle n'est pas prise en charge pour les groupes de cohérence hiérarchiques. Pour convertir un groupe de cohérence hiérarchique en un seul groupe de cohérence, reportez-vous à la section modifier l'architecture d'un groupe de cohérence.
- Les étiquettes de règles doivent correspondre dans le cluster source et dans le cluster destination.
- Vous pouvez interrompre l'activité ajouter des volumes à un groupe de cohérence Avec une relation SnapMirror asynchrone active. Toute autre modification apportée à un groupe de cohérence exige que vous rompez la relation SnapMirror, modifiez le groupe de cohérence, puis rétablissez et resynchronisez la relation.
- Si vous avez configuré une relation de protection SnapMirror asynchrone pour plusieurs volumes individuels, vous pouvez convertir ces volumes en groupe de cohérence tout en conservant les copies Snapshot existantes. Pour convertir les volumes avec succès :
  - Il doit y avoir une copie Snapshot commune des volumes.
  - Vous devez interrompre la relation SnapMirror existante, ajoutez les volumes à un seul groupe de cohérence, puis resynchronisez la relation à l'aide du flux de travail suivant.

Étapes

1. Depuis le cluster de destination, sélectionnez **stockage > groupes de cohérence**.

2. Sélectionnez le groupe de cohérence que vous avez créé dans le menu Groupe de cohérence.
3. En haut à droite de la page de présentation, sélectionnez **plus** puis **protéger**.
4. System Manager remplit automatiquement les informations côté source. Sélectionnez le cluster et la VM de stockage appropriés pour la destination. Sélectionnez une stratégie de protection. Vérifier que **Initialize relation** est coché.

   Lorsque vous sélectionnez une stratégie asynchrone, vous avez la possibilité de **remplacer le programme de transfert**.

   > La planification minimale prise en charge (objectif de point de récupération, ou RPO) pour les groupes de cohérence avec SnapMirror asynchrone est de 30 minutes.

5. Sélectionnez **Enregistrer**.
6. Le groupe de cohérence doit être initialisé et synchronisé. Vérifiez que la synchronisation s'est bien terminée en retournant au menu **groupe de cohérence**. L'état **SnapMirror (Remote)** s'affiche `Protected` à côté de .

Configuration de la reprise d'activité SVM

À partir de ONTAP 9.14.1, Reprise d'activité de SVM prend en charge les groupes de cohérence et permet de mettre en miroir les informations relatives aux groupes de cohérence entre le cluster source et le cluster destination.

Si vous activez la reprise d'activité SVM sur un SVM qui contient déjà un groupe de cohérence, suivez les workflows de configuration du SVM pour System Manager ou le INTERFACE DE LIGNE DE COMMANDES DE ONTAP.

Si vous ajoutez un groupe de cohérence à un SVM figurant dans une relation de reprise d'activité de SVM active et saine, vous devez mettre à jour la relation de SVM DR depuis le cluster destination. Pour plus d'informations, voir Mettre à jour une relation de réplication manuellement. Vous devez mettre à jour la relation chaque fois que vous développez le groupe de cohérence.

Limites

- La reprise d'activité des SVM ne prend pas en charge les groupes de cohérence hiérarchiques.
- La reprise après incident des SVM ne prend pas en charge les groupes de cohérence protégés par SnapMirror asynchrone. Vous devez rompre la relation SnapMirror avant de configurer la reprise d'activité d'un SVM.
- Les deux clusters doivent exécuter ONTAP 9.14.1 ou une version ultérieure.
- Les relations « Fan-Out » ne sont pas prises en charge pour les configurations de reprise d'activité des SVM contenant des groupes de cohérence.
- Pour les autres limites, voir limites des groupes de cohérence.

Visualiser les relations

System Manager visualise les mappages de LUN dans le menu **protection > relations**. Lorsque vous sélectionnez une relation source, System Manager affiche une visualisation des relations source. En sélectionnant un volume, vous pouvez approfondir ces relations pour afficher la liste des LUN et des relations de groupe d'initiateurs. Ces informations peuvent être téléchargées sous forme de classeur Excel à partir de la vue de volume individuelle ; l'opération de téléchargement s'exécute en arrière-plan.

Informations associées

- "Cloner un groupe de cohérence"
- "Configurez les copies Snapshot"
- "Création de règles personnalisées de protection des données"
- "Effectuez des restaurations à partir de copies Snapshot"
- "Restaurez un volume à partir d'une copie Snapshot antérieure"
- "Présentation de SM-BC"
- "Documentation sur l'automatisation ONTAP"
- Principes de base de la reprise sur incident asynchrone SnapMirror

Modifiez les volumes membres d'un groupe de cohérence

À partir de la version ONTAP 9.12.1, vous pouvez modifier un groupe de cohérence en supprimant des volumes ou en ajoutant des volumes (en développant le groupe de cohérence). Depuis la version ONTAP 9.13.1, vous pouvez déplacer des volumes entre des groupes de cohérence enfants s'ils partagent un parent commun.

Ajouter des volumes à un groupe de cohérence

À partir de ONTAP 9.12.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption.

Description de la tâche

- Vous ne pouvez pas ajouter des volumes associés à un autre groupe de cohérence.
- Les groupes de cohérence prennent en charge les protocoles NAS, SAN et NVMe.
- Si les ajustements se situent dans l'ensemble, vous pouvez ajouter jusqu'à 16 volumes à la fois à un groupe de cohérence limites des groupes de cohérence.
- Depuis la version ONTAP 9.13.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption avec une règle de protection SnapMirror Business Continuity (SM-BC) active ou asynchrone.
- Lorsque vous ajoutez des volumes à un groupe de cohérence protégé par SM-BC, l'état de la relation SM-BC passe à « expansion » jusqu'à ce que la mise en miroir et la protection soient configurées pour le nouveau volume. Si un incident se produit sur le cluster principal avant la fin de ce processus, le groupe de cohérence revient à sa composition d'origine dans le cadre de l'opération de basculement.
- Dans ONTAP 9.12.1 et les versions antérieures, vous *ne pouvez pas* ajouter de volumes à un groupe de cohérence dans une relation SM-BC. Vous devez d'abord interrompre la relation SM-BC, modifier le groupe de cohérence, puis restaurer la protection avec SM-BC.
- Depuis ONTAP 9.12.1, l'API REST de ONTAP prend en charge l'ajout de volumes *New* ou existants à un groupe de cohérence. Pour plus d'informations sur l'API REST de ONTAP, reportez-vous à "Documentation de référence de l'API REST ONTAP".

  Depuis ONTAP 9.13.1, cette fonctionnalité est prise en charge dans System Manager.

- Lors de l'extension d'un groupe de cohérence, les copies Snapshot du groupe de cohérence capturé avant la modification sont considérées comme partielles. Toute opération de restauration basée sur cette copie Snapshot reflète le groupe de cohérence à l'instant T du snapshot.
- Si vous utilisez les ONTAP 9.10.1 à 9.11.1, vous ne pouvez pas modifier un groupe de cohérence. Pour modifier la configuration d'un groupe de cohérence dans les ONTAP 9.10.1 ou 9.11.1, vous devez supprimer ce groupe, puis créer un nouveau groupe de cohérence avec les volumes à inclure.

- Depuis la version ONTAP 9.14.1, vous pouvez répliquer des copies Snapshot granulaires par volume sur le cluster de destination lorsque vous utilisez la réplication asynchrone SnapMirror. Lors de l'extension d'un groupe de cohérence à l'aide de SnapMirror asynchrone, les snapshots granulaires par volume ne sont répliqués qu'après l'extension du groupe de cohérence lorsque la règle SnapMirror est MirrorAll ou MirrorAndVault. Seuls les snapshots granulaires par volume plus récents que le snapshot du groupe de cohérence de référence sont répliqués.
- Si vous ajoutez des volumes à un groupe de cohérence dans une relation de reprise d'activité de SVM (prise en charge depuis ONTAP 9.14.1), vous devez mettre à jour la relation de reprise d'activité de SVM depuis le cluster de destination après avoir étendu le groupe de cohérence. Pour plus d'informations, reportez-vous à la section Mettre à jour une relation de réplication manuellement.

Exemple 1. Étapes

System Manager

Depuis ONTAP 9.12.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à modifier.
3. Si vous modifiez un seul groupe de cohérence, en haut du menu **volumes**, sélectionnez **plus**, puis **plus** pour ajouter un volume.

   Si vous modifiez un groupe de cohérence enfant, identifiez le groupe de cohérence parent à modifier. Sélectionnez le bouton **>** pour afficher les groupes de cohérence enfant, puis sélectionnez ⋮ en regard du nom du groupe de cohérence enfant à modifier. Dans ce menu, sélectionnez **développer**.

4. Sélectionnez jusqu'à 16 volumes à ajouter au groupe de cohérence.
5. Sélectionnez **Enregistrer**. Une fois l'opération terminée, affichez les nouveaux volumes ajoutés dans le menu **volumes** du groupe de cohérence.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez ajouter des volumes à un groupe de cohérence à l'aide de l'interface de ligne de commandes ONTAP.

Ajouter des volumes existants

1. Exécutez la commande suivante. Le `-volumes` le paramètre accepte une liste de volumes séparés par une virgule.

   > Inclure uniquement le `-parent-consistency-group` paramètre si le groupe de cohérence appartient à une relation hiérarchique.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Ajouter de nouveaux volumes

La procédure d'ajout de nouveaux volumes dépend du protocole que vous utilisez.

> Inclure uniquement le `-parent-consistency-group` paramètre si le groupe de cohérence appartient à une relation hiérarchique.

- Pour ajouter de nouveaux volumes sans les exporter :

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  volume_name -size size
  ```

- Pour ajouter de nouveaux volumes NFS :

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency-group-name -volume volume-prefix -volume-count number -size
  size -export-policy policy_name
  ```

- Pour ajouter de nouveaux volumes SAN :

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency-group-name -lun lun_name -size size -lun-count number -igroup
  igroup_name
  ```

- Pour ajouter de nouveaux espaces de noms NVMe :

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency_group_name -namespace namespace_name -volume-count number
  -namespace-count number -size size -subsystem subsystem_name
  ```

Supprimez des volumes d'un groupe de cohérence

Les volumes supprimés d'un groupe de cohérence ne sont pas supprimés. Ils restent actifs dans le cluster.

Description de la tâche

- Vous ne pouvez pas supprimer des volumes d'un groupe de cohérence dans une relation de reprise d'activité SM-BC ou SVM. Vous devez d'abord interrompre la relation SM-BC pour modifier le groupe de cohérence, puis rétablir la relation.
- Si un groupe de cohérence ne contient aucun volume après l'opération de suppression, le groupe de cohérence est supprimé.
- Lorsqu'un volume est supprimé d'un groupe de cohérence, les snapshots existants du groupe de cohérence restent considérés comme non valides. Les snapshots existants ne peuvent pas être utilisés pour restaurer le contenu d'un groupe de cohérence. Les snapshots granulaires volume restent valides.
- Si vous supprimez un volume du cluster, il est automatiquement supprimé du groupe de cohérence.
- Pour modifier la configuration d'un groupe de cohérence dans ONTAP 9.10.1 ou 9.11.1, vous devez supprimer ce groupe de cohérence, puis en créer un nouveau avec les volumes membres souhaités.
- La suppression d'un volume du cluster entraîne sa suppression automatique.

System Manager

Depuis ONTAP 9.12.1, vous pouvez effectuer cette opération avec System Manager.

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence enfant ou unique à modifier.
3. Dans le menu **volumes**, sélectionnez les cases à cocher en regard des volumes individuels que vous souhaitez supprimer du groupe de cohérence.
4. Sélectionnez **Supprimer des volumes du groupe de cohérence**.
5. Vérifiez que vous avez bien compris que la suppression des volumes entraîne la non-validité de toutes les copies Snapshot du groupe de cohérence et sélectionnez **Remove**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez supprimer des volumes d'un groupe de cohérence à l'aide de l'interface de ligne de commandes.

Étape

1. Supprimer les volumes. Le `-volumes` le paramètre accepte une liste de volumes séparés par une virgule.

   Inclure uniquement le `-parent-consistency-group` paramètre si le groupe de cohérence appartient à une relation hiérarchique.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Déplacez des volumes entre les groupes de cohérence

Depuis la version ONTAP 9.13.1, vous pouvez déplacer des volumes entre des groupes de cohérence enfants qui partagent un parent.

Description de la tâche

- Vous pouvez uniquement déplacer des volumes entre des groupes de cohérence imbriqués sous le même groupe de cohérence parent.
- Les snapshots de groupe de cohérence existants sont devenus non valides et ne sont plus accessibles en tant que snapshots de groupe de cohérence. Les snapshots de volumes individuels restent valides.
- Les copies Snapshot du groupe de cohérence parent restent valides.
- Si vous déplacez tous les volumes hors d'un groupe de cohérence enfant, ce groupe de cohérence est supprimé.
- Les modifications apportées à un groupe de cohérence doivent être respectées limites des groupes de cohérence.

System Manager

Depuis ONTAP 9.12.1, vous pouvez effectuer cette opération avec System Manager.

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent contenant les volumes à déplacer. Recherchez le groupe de cohérence enfant, puis développez le menu **volumes**. Sélectionnez les volumes à déplacer.
3. Sélectionnez **déplacer**.
4. Indiquez si vous souhaitez déplacer les volumes vers un nouveau groupe de cohérence ou un groupe existant.
   a. Pour déplacer le groupe de cohérence vers un groupe existant, sélectionnez **groupe de cohérence enfant existant**, puis choisissez le nom du groupe de cohérence dans le menu déroulant.
   b. Pour passer à un nouveau groupe de cohérence, sélectionnez **Nouveau groupe de cohérence enfant**. Indiquez le nom du nouveau groupe de cohérence enfant et sélectionnez un type de composant.
5. Sélectionnez **déplacer**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez déplacer des volumes entre des groupes de cohérence à l'aide de l'interface de ligne de commandes ONTAP.

Déplacez les volumes vers un nouveau groupe de cohérence enfant

1. La commande suivante crée un nouveau groupe de cohérence enfant dans lequel sont situés les volumes désignés.

   Lorsque vous créez le nouveau groupe de cohérence, vous pouvez désigner de nouvelles règles de Snapshot, de QoS et de hiérarchisation.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Déplacez les volumes vers un groupe de cohérence enfant existant

1. Réaffectez les volumes. Le `-volumes` le paramètre accepte une liste de noms de volumes séparés par des virgules.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Informations associées

- Limites des groupes de cohérence

- Cloner un groupe de cohérence

Modifier la géométrie du groupe de cohérence

Depuis la version ONTAP 9.13.1, vous pouvez modifier la géométrie d'un groupe de cohérence. La modification de la géométrie d'un groupe de cohérence vous permet de modifier la configuration des groupes de cohérence enfant ou parent sans interrompre les opérations d'E/S en cours.

La modification de la géométrie d'un groupe de cohérence a un impact sur les copies Snapshot existantes.

> Vous ne pouvez pas modifier la géométrie d'un groupe de cohérence configuré avec une règle de protection à distance. Vous devez d'abord rompre la relation de protection, modifier la géométrie, puis restaurer la protection à distance.

Ajouter un nouveau groupe de cohérence enfant

Depuis la version ONTAP 9.13.1, vous pouvez ajouter un nouveau groupe de cohérence enfant à un groupe de cohérence parent existant.

Avant de commencer

- Un groupe de cohérence parent peut contenir cinq groupes de cohérence enfant au maximum. Voir limites des groupes de cohérence pour les autres limites.
- Vous ne pouvez pas ajouter un groupe de cohérence enfant à un seul groupe de cohérence. Vous devez d'abord [promouvoir] groupe de cohérence, vous pouvez ensuite ajouter un groupe de cohérence enfant.
- Les copies Snapshot existantes du groupe de cohérence capturé avant l'opération d'extension sont considérées comme partielles. Toute opération de restauration basée sur cette copie Snapshot reflète le groupe de cohérence au moment de la copie Snapshot.

Exemple 2. Étapes

System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent auquel vous souhaitez ajouter un groupe de cohérence enfant.
3. En regard du nom du groupe de cohérence parent, sélectionnez **plus** puis **Ajouter un nouveau groupe de cohérence enfant**.
4. Indiquez le nom du groupe de cohérence.
5. Indiquez si vous souhaitez ajouter des volumes nouveaux ou existants.
   a. Si vous ajoutez des volumes existants, sélectionnez **volumes existants** puis choisissez les volumes dans le menu déroulant.
   b. Si vous ajoutez de nouveaux volumes, sélectionnez **nouveaux volumes** puis indiquez le nombre de volumes et leur taille.
6. Sélectionnez **Ajouter**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez ajouter un groupe de cohérence enfant via l'interface de ligne de commandes ONTAP.

Ajoutez un groupe de cohérence enfant avec les nouveaux volumes

1. Créez le nouveau groupe de cohérence. Indiquez des valeurs pour le nom du groupe de cohérence, le préfixe de volume, le nombre de volumes, la taille du volume, le service de stockage, et nom de la règle d'export :

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Ajoutez un groupe de cohérence enfant avec les volumes existants

1. Créez le nouveau groupe de cohérence. Le `volumes` le paramètre accepte une liste de noms de volumes séparés par des virgules.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Détacher un groupe de cohérence enfant

Depuis la version ONTAP 9.13.1, vous pouvez supprimer un groupe de cohérence enfant de son groupe de cohérence parent et le convertir en groupe de cohérence individuel.

Avant de commencer

- Le détachement d'un groupe de cohérence enfant entraîne l'invalidation et l'inaccessibilité des snapshots du groupe de cohérence parent. Les snapshots granulaires de volume restent valides.

- Les copies Snapshot existantes d'un groupe de cohérence individuel restent valides.
- Cette opération échoue si un groupe de cohérence unique existant porte le même nom que le groupe de cohérence enfant que vous souhaitez détacher. Si ce scénario se produit, vous devez renommer le groupe de cohérence lorsque vous le détachez.

Exemple 3. Étapes

System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent contenant l'enfant à détacher.
3. En regard du groupe de cohérence enfant à détacher, sélectionnez **plus** puis **détacher du parent**.
4. Si vous le souhaitez, renommez le groupe de cohérence et sélectionnez un type d'application.
5. Sélectionnez **détacher**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez détacher un groupe de cohérence enfant à l'aide de l'interface de ligne de commandes ONTAP.

1. Détachez le groupe de cohérence. Si vous le souhaitez, renommez le groupe de cohérence détaché avec le `-new-name` paramètre.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Déplacez un groupe de cohérence unique existant sous un groupe de cohérence parent

À partir de la version ONTAP 9.13.1, vous pouvez convertir un groupe de cohérence existant en groupe de cohérence enfant. Au cours de l'opération de déplacement, vous pouvez déplacer le groupe de cohérence sous un groupe de cohérence parent existant ou créer un nouveau groupe de cohérence parent.

Avant de commencer

- Le groupe de cohérence parent doit avoir au moins quatre enfants. Un groupe de cohérence parent peut contenir cinq groupes de cohérence enfant au maximum. Voir limites des groupes de cohérence pour les autres limites.
- Les copies snapshot existantes du groupe de cohérence *parent* capturées avant cette opération seront considérées comme partielles. Toute opération de restauration basée sur l'une de ces copies Snapshot reflète le groupe de cohérence au moment précis de la copie Snapshot.
- Les snapshots de groupes de cohérence existants d'un seul groupe de cohérence restent valides.

Exemple 4. Étapes

System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à convertir.
3. Sélectionnez **plus** puis **déplacer sous un autre groupe de cohérence**.
4. Si vous le souhaitez, indiquez un nouveau nom pour le groupe de cohérence et sélectionnez un type de composant. Par défaut, le type de composant sera autre.
5. Indiquez si vous souhaitez migrer vers un groupe de cohérence parent existant ou créer un nouveau groupe de cohérence parent :
   a. Pour migrer vers un groupe de cohérence parent existant, sélectionnez **groupe de cohérence existant**, puis choisissez le groupe de cohérence dans le menu déroulant.
   b. Pour créer un nouveau groupe de cohérence parent, sélectionnez **Nouveau groupe de cohérence**, puis indiquez le nom du nouveau groupe de cohérence.
6. Sélectionnez **déplacer**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez déplacer un groupe de cohérence unique sous un groupe de cohérence parent à l'aide de l'interface de ligne de commandes ONTAP.

Déplacez un groupe de cohérence sous un nouveau groupe de cohérence parent

1. Créez le groupe de cohérence parent. Le `-consistency-groups` ce paramètre va migrer tous les groupes de cohérence existants vers le nouveau parent.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

Déplacez un groupe de cohérence sous un groupe de cohérence existant

1. Déplacer le groupe de cohérence :

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

Promouvoir un groupe de cohérence enfant

Depuis la version ONTAP 9.13.1, vous pouvez promouvoir un groupe de cohérence unique en tant que groupe de cohérence parent. Lorsque vous promouvez le groupe de cohérence unique en parent, vous créez également un nouveau groupe de cohérence enfant qui hérite de tous les volumes du groupe de cohérence unique d'origine.

Avant de commencer

- Pour convertir un groupe de cohérence enfant en groupe de cohérence parent, vous devez d'abord le faire [detach] le groupe de cohérence enfant doit ensuite suivre la procédure suivante.
- Une fois le groupe de cohérence mis en avant, les copies Snapshot existantes du groupe de cohérence restent valides.

Exemple 5. Étapes

System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à promouvoir.
3. Sélectionnez **plus** puis **promouvoir en groupe de cohérence parent**.
4. Entrez un **Nom** et sélectionnez un **Type de composant** pour le groupe de cohérence enfant.
5. Sélectionnez **promouvoir**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez déplacer un groupe de cohérence unique sous un groupe de cohérence parent à l'aide de l'interface de ligne de commandes ONTAP.

1. Promouvoir le groupe de cohérence. Cette commande entraîne la création d'un groupe de cohérence parent et d'un groupe enfant.

   ```
   consistency-group promote -vserver SVM_name -consistency-group
   existing_consistency_group -new-name new_child_consistency_group
   ```

Rétrograder un parent en un seul groupe de cohérence

Depuis la version ONTAP 9.13.1, vous pouvez rétrograder un groupe de cohérence parent en un seul groupe de cohérence. La rétrogradation du parent aplatit la hiérarchie du groupe de cohérence, supprimant tous les groupes de cohérence enfants associés. Tous les volumes du groupe de cohérence restent dans le nouveau groupe de cohérence unique.

Avant de commencer

- Les copies Snapshot existantes du groupe de cohérence parent restent valides après la rétrogradation vers une cohérence unique. Les copies Snapshot existantes de l'un des groupes de cohérence enfant associés de ce parent deviennent non valides, mais les snapshots de volumes individuels continuent d'être accessibles sous forme de copies Snapshot granulaires de volumes.

Exemple 6. Étapes

System Manager

Depuis ONTAP 9.13.1, vous pouvez effectuer cette opération avec System Manager.

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent à rétrograder.
3. Sélectionnez **plus** puis **Rétrograder à un seul groupe de cohérence**.
4. Un avertissement vous informe que tous les groupes de cohérence enfants associés seront supprimés et que leurs volumes seront déplacés dans le nouveau groupe de cohérence unique. Sélectionnez **Rétrograder** pour confirmer que vous comprenez l'impact.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez rétrograder un groupe de cohérence à l'aide de l'interface de ligne de commandes ONTAP.

1. Rétrograder le groupe de cohérence. Utilisez l'option `-new-name` paramètre permettant de renommer le groupe de cohérence.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Modifier les balises d'application et de composant

Depuis la version ONTAP 9.12.1, les groupes de cohérence prennent en charge le balisage des composants et des applications. Les balises d'application et de composant sont un outil de gestion qui vous permet de filtrer et d'identifier différentes charges de travail dans vos groupes de cohérence.

Description de la tâche

Les groupes de cohérence proposent deux types de balises :

- **Balises d'application** : elles s'appliquent aux groupes de cohérence individuel et parent. Les balises d'application fournissent un étiquetage pour les charges de travail telles que MongoDB, Oracle ou SQL Server. La balise d'application par défaut pour les groupes de cohérence est autre.
- **Balises de composant**: Les enfants des groupes de cohérence hiérarchiques ont des balises de composant au lieu de balises d'application. Les options pour les balises de composant sont « données », « journaux » ou « autre ». La valeur par défaut est autre.

Lors de la création de groupes de cohérence ou après la création de groupes de cohérence, vous pouvez appliquer les balises.

> Si le groupe de cohérence possède une relation SM-BC, vous devez utiliser **Other** comme balise d'application ou de composant.

Étapes

Depuis ONTAP 9.12.1, vous pouvez modifier les balises d'application et de composant à l'aide de System Manager. Depuis ONTAP 9.14.1, vous pouvez modifier les balises d'application et de composant à l'aide de

l'interface de ligne de commande ONTAP.

System Manager

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence dont vous souhaitez modifier la balise. Sélectionner ⋮ En regard du nom du groupe de cohérence, puis de **Edit**.
3. Dans le menu déroulant, choisissez la balise d'application ou de composant appropriée.
4. Sélectionnez **Enregistrer**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez modifier la balise d'application ou de composant d'un groupe de cohérence existant à l'aide de l'interface de ligne de commandes ONTAP.

Modifier la balise d'application

1. Les balises d'application acceptent un nombre limité de chaînes prédéfinies. Pour voir la liste des chaînes acceptées, exécutez la commande suivante :
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Choisissez la chaîne appropriée dans le résultat, puis modifiez le groupe de cohérence :
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Modifier la balise du composant

1. Modifier le type de composant. Le type de composant peut être données, journaux ou autre. Si vous utilisez SM-BC, il doit être « autre ».
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Cloner un groupe de cohérence

Depuis la version ONTAP 9.12.1, vous pouvez cloner un groupe de cohérence pour créer une copie du groupe de cohérence et de son contenu. Le clonage d'un groupe de cohérence crée une copie de la configuration de groupe de cohérence, de ses métadonnées telles que le type d'application, et de tous les volumes et leur contenu tels que les fichiers, les répertoires, les LUN ou les espaces de noms NVMe.

Description de la tâche

Lors du clonage d'un groupe de cohérence, vous pouvez le cloner avec sa configuration actuelle, mais avec un contenu de volume tel qu'ils sont ou basé sur un Snapshot de groupe de cohérence existant.

Le clonage d'un groupe de cohérence est pris en charge uniquement pour l'ensemble du groupe de cohérence. Vous ne pouvez pas cloner un groupe de cohérence enfant individuel dans une relation hiérarchique : seule la configuration complète des groupes de cohérence peut être clonée.

Lorsque vous clonez un groupe de cohérence, les composants suivants ne sont pas clonés :

- IGroups

- Mappages de LUN
- Sous-systèmes NVMe
- Mappages de sous-systèmes d’espace de noms NVMe

Avant de commencer

- Lorsque vous clonez un groupe de cohérence, ONTAP ne crée pas de partages SMB pour les volumes clonés si aucun nom de partage n’est spécifié. * Les groupes de cohérence clonés ne sont pas montés si aucun chemin de jonction n’est spécifié.
- Si vous tentez de cloner un groupe de cohérence à partir d’une copie Snapshot qui ne reflète pas les volumes constituants actuels du groupe de cohérence, l’opération échoue.
- Une fois que vous avez cloné un groupe de cohérence, vous devez effectuer l’opération de mappage appropriée.

  Reportez-vous à la section Mappez les igroups sur plusieurs LUN ou Mappez un namespace NVMe à un sous-système pour en savoir plus.

- Le clonage d’un groupe de cohérence n’est pas pris en charge pour un groupe de cohérence dans une relation SnapMirror de continuité de l’activité ou avec les volumes DP associés.

System Manager

Étapes

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à cloner dans le menu **Groupe de cohérence**.
3. En haut à droite de la page de présentation du groupe de cohérence, sélectionnez **Clone**.
4. Indiquez un nom pour le nouveau groupe de cohérence cloné ou acceptez le nom par défaut.
   a. Choisissez si vous souhaitez activer **"Provisionnement fin"**.
   b. Choisissez **Split Clone** si vous souhaitez dissocier le groupe de cohérence de sa source et allouer de l'espace disque supplémentaire au groupe de cohérence cloné.
5. Pour cloner le groupe de cohérence dans son état actuel, choisissez **Ajouter une nouvelle copie Snapshot**.

   Pour cloner le groupe de cohérence à partir d'un snapshot, choisissez **utiliser une copie Snapshot existante**. La sélection de cette option ouvre un nouveau sous-menu. Sélectionnez la copie Snapshot que vous souhaitez utiliser comme base de l'opération de clonage.
6. Sélectionnez **Clone**.
7. Retournez au menu **Groupe de cohérence** pour confirmer que votre groupe de cohérence a été cloné.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez cloner un groupe de cohérence à l'aide de l'interface de ligne de commandes.

Cloner un groupe de cohérence

1. Le `consistency-group clone create` la commande clone le groupe de cohérence à l'état instantané actuel. Pour baser l'opération de clonage sur un snapshot, incluez le `-source-snapshot` paramètre.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

Étapes suivantes

- Mappez les igroups sur plusieurs LUN
- Mappez un namespace NVMe à un sous-système

Supprimez un groupe de cohérence

Si vous décidez de ne plus avoir besoin d'un groupe de cohérence, vous pouvez le supprimer.

Description de la tâche

- La suppression d'un groupe de cohérence supprime l'instance du groupe de cohérence et n'a _pas d'impact sur les volumes ou les LUN constitutifs. La suppression d'un groupe de cohérence n'entraîne pas la suppression des snapshots présents sur chaque volume, mais ils ne sont plus accessibles en tant que

snapshots de groupe de cohérence. Toutefois, les snapshots peuvent continuer à être gérés comme des snapshots granulaires de volume ordinaires.

- ONTAP supprime automatiquement un groupe de cohérence si tous les volumes du groupe de cohérence sont supprimés.
- La suppression d'un groupe de cohérence parent entraîne la suppression de tous les groupes de cohérence enfant associés.
- Si vous utilisez une version de ONTAP comprise entre 9.10.1 et 9.12.0, les volumes ne peuvent être supprimés d'un groupe de cohérence que si le volume lui-même est supprimé, auquel cas le volume est automatiquement supprimé du groupe de cohérence. Depuis la version ONTAP 9.12.1, vous pouvez supprimer des volumes d'un groupe de cohérence sans le supprimer. Pour plus d'informations sur ce processus, reportez-vous à la section Modifier un groupe de cohérence.

Exemple 7. Étapes

System Manager

1. Sélectionnez **stockage > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence à supprimer.
3. En regard du nom du groupe de cohérence, sélectionnez ⋮ Puis **Supprimer**.

CLI

Depuis la version ONTAP 9.14.1, vous pouvez supprimer un groupe de cohérence à l'aide de l'interface de ligne de commandes.

Supprimez un groupe de cohérence

1. Supprimez le groupe de cohérence :

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

Continuité de l'activité SnapMirror

Présentation de la continuité de l'activité SnapMirror

SnapMirror Business Continuity (SM-BC), également appelé synchronisation active SnapMirror, assure la continuité des services de l'entreprise même en cas de défaillance complète du site. Les applications peuvent ainsi basculer en toute transparence à l'aide d'une copie secondaire. Aucune intervention manuelle ni script supplémentaire n'est nécessaire pour déclencher un basculement avec SM-BC.

SM-BC est disponible à partir de ONTAP 9.8. SM-BC est pris en charge sur les clusters AFF ou les clusters de baies SAN 100 % Flash (ASA), dans lesquels les clusters principal et secondaire peuvent être AFF ou ASA. SM-BC protège les applications avec des LUN iSCSI ou FCP.

Avantages

SM-BC offre les avantages suivants :

- Disponibilité sans interruption pour les applications stratégiques

- Possibilité d'héberger les applications stratégiques en alternance depuis les sites principal et secondaire
- Gestion des applications simplifiée grâce à des groupes de cohérence pour assurer la cohérence des écritures dépendantes
- Possibilité de tester le basculement pour chaque application
- Création instantanée de clones miroir sans impact sur la disponibilité des applications
- À partir de ONTAP 9.11.1, SM-BC prend en charge SnapRestore pour un seul fichier.
- À partir de ONTAP 9.14.1, SM-BC prend en charge la mise en cluster de basculement Windows et "Réservations persistantes SCSI 3", amélioration de la haute disponibilité.

Cas d'utilisation

Déploiement des applications pour un objectif de délai de restauration (RTO) nul

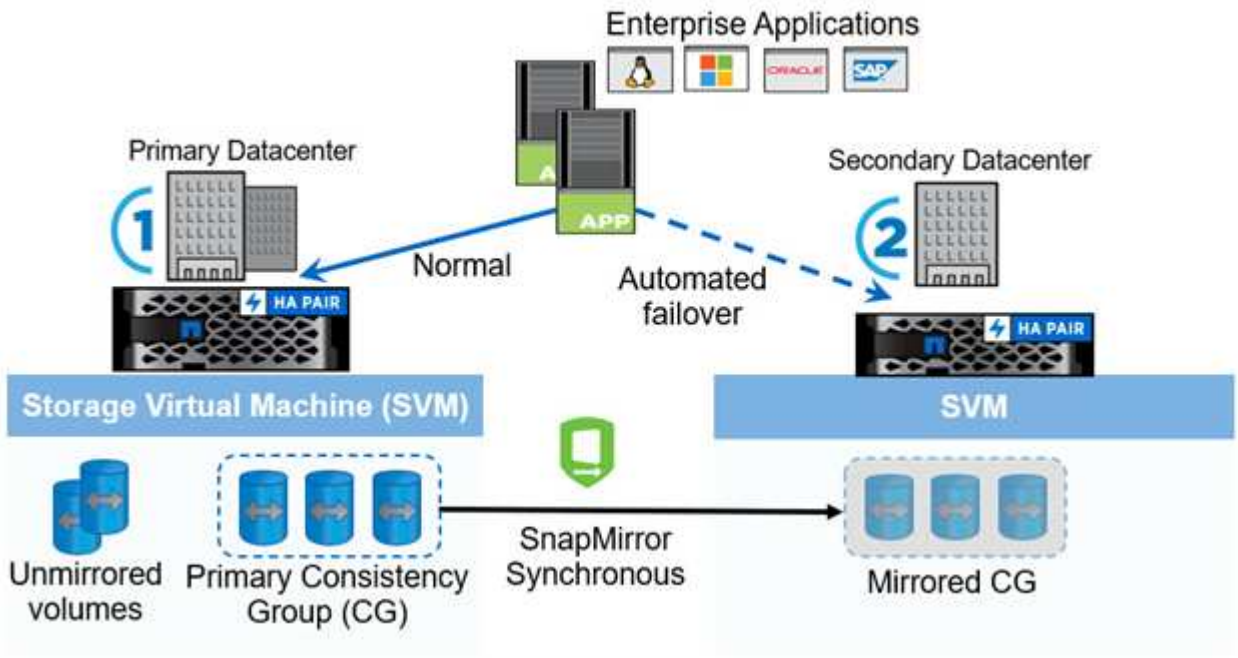
Dans un déploiement SM-BC, vous aurez un cluster principal et un cluster secondaire. Une LUN dans le cluster principal `1LP`) aura un miroir (`L1s`) Sur le serveur secondaire ; les deux LUN partagent le même ID de série et sont signalées comme des LUN de lecture-écriture à l'hôte. En revanche, les opérations de lecture et d'écriture sont uniquement gérées sur le LUN principal, `1LP`. Toutes les écritures sont effectuées sur le miroir `L1S` sont servis par proxy.

Scénario d'incident

Avec SM-BC, vous pouvez répliquer de manière synchrone plusieurs volumes pour une application entre des sites répartis géographiquement. En cas d'interruption du stockage primaire, vous pouvez basculer automatiquement vers la copie secondaire, assurant ainsi la continuité de l'activité pour les applications de niveau 1.

Architecture

La figure suivante illustre le fonctionnement général de la fonctionnalité de continuité de l'activité SnapMirror.



Dans la section un du diagramme, une application est déployée sur un SVM dans le data Center principal. Les volumes ajoutés au groupe de cohérence principal sont protégés par SM-BC et mis en miroir sur le groupe de

cohérence secondaire d'un data Center secondaire. En cas d'interruption, les volumes du groupe de cohérence principal basculeront vers le groupe de cohérence mis en miroir. Les volumes qui ne se trouvent pas dans un groupe de cohérence mis en miroir ne sont pas servis en cas de basculement.

Plus d'informations

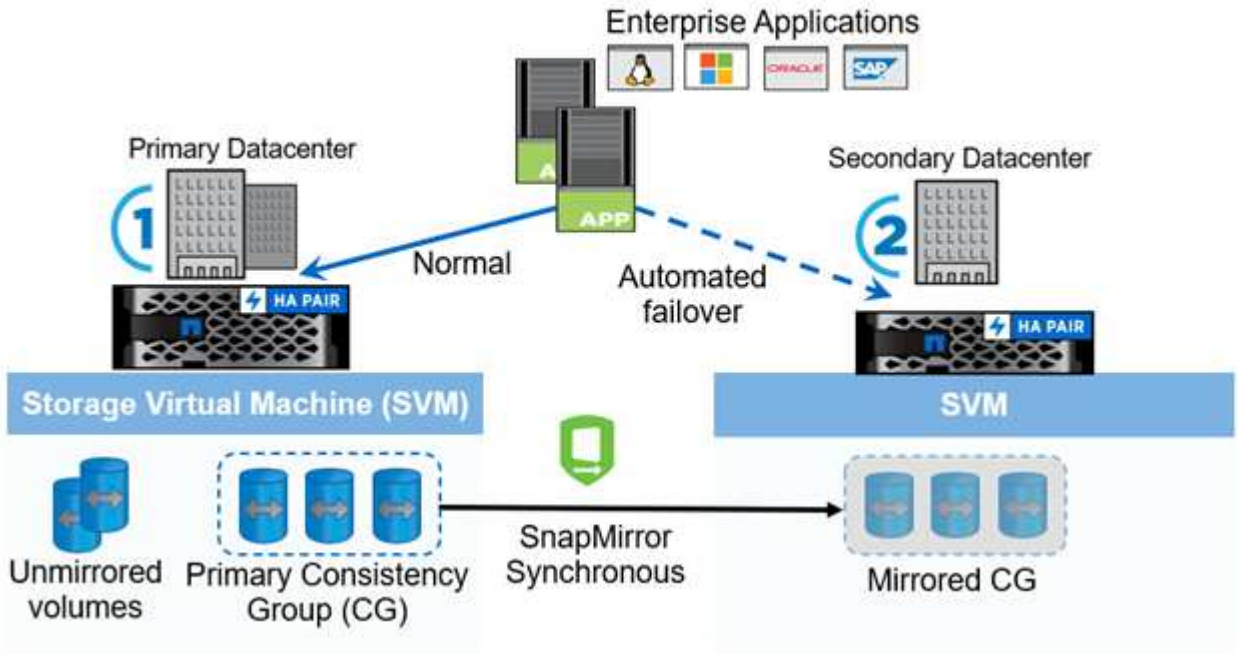
- "Tr-4878 : continuité de l'activité avec SnapMirror"

Concepts clés

SnapMirror Business Continuity (SM-BC) exploite des fonctionnalités telles que les groupes de cohérence et le médiateur ONTAP pour assurer la réplication et le service de vos données même en cas d'incident. Lors de la planification de votre déploiement SM-BC, il est important de comprendre les concepts essentiels de SM-BC et de son architecture.

Architecture

La figure suivante présente un aperçu général d'un déploiement SM-BC.



Le schéma représente une application d'entreprise hébergée sur une machine virtuelle de stockage (SVM) au niveau du data Center principal. La SVM contient cinq volumes, dont trois font partie d'un groupe de cohérence. Les trois volumes du groupe de cohérence sont mis en miroir sur un data Center secondaire. Dans des circonstances normales, toutes les opérations d'écriture sont effectuées sur le data Center principal. Dans les faits, ce data Center sert de source pour les opérations d'E/S, tandis que le data Center secondaire sert de destination.

En cas d'incident au niveau du data Center principal, le médiateur ONTAP charge le data Center secondaire à agir comme le data Center principal, afin de prendre en charge toutes les opérations d'E/S. Seuls les volumes mis en miroir dans le groupe de cohérence sont gérés. Toutes les opérations relatives aux deux autres volumes du SVM seront affectées par le sinistre.

Concepts essentiels

Comprendre les termes suivants vous aidera à déployer SM-BC.

Groupe de cohérence

Un groupe de cohérence est un ensemble de volumes ou de LUN qui offrent une garantie de cohérence de l'ordre d'écriture pour la charge de travail d'application qui doit être protégée pour assurer la continuité de l'activité. Un groupe de cohérence veille à ce que tous les volumes de ce jeu de données soient suspendus, puis pris en charge au même moment, fournissant ainsi un point de restauration cohérent avec les données sur tous les volumes de ce jeu de données.

Dans SM-BC, vous allez créer un groupe de cohérence principal et secondaire pour la réplication et la protection des données. Le groupe de cohérence secondaire assure le service de vos données en cas d'interruption.

Pour en savoir plus sur les groupes de cohérence, reportez-vous à la section "Présentation des groupes de cohérence".

Composant

Volume individuel ou LUN faisant partie d'un groupe de cohérence, qui est protégé par la relation SM-BC.

Médiateur de ONTAP

Les médiateurs ONTAP surveillent les deux clusters ONTAP et orchestrent le basculement en cas de défaillance de votre système de stockage principal. Avec le médiateur ONTAP, votre application se reconnecte automatiquement aux ressources du système de stockage secondaire.

Grâce aux informations de santé du médiateur ONTAP, les clusters peuvent faire la différence entre une panne du LIF intercluster et une défaillance du site. Lorsque le site est en panne, le médiateur ONTAP transmet à la demande les informations de santé au cluster homologue, ce qui facilite le basculement du cluster homologue.

En savoir plus sur le "Médiateur de ONTAP".

Basculement planifié

Opération manuelle pour modifier les rôles des copies dans une relation SM-BC. Les sites principaux deviennent les sites secondaires, et le site secondaire devient le site principal.

Basculement automatique non planifié (AUFO)

Opération automatique pour effectuer un basculement vers la copie miroir. L'opération nécessite l'aide du médiateur pour détecter que la copie principale n'est pas disponible.

Non synchronisé (OOS)

Lorsque les E/S de l'application ne sont pas répliquées sur le système de stockage secondaire, elles sont signalées comme **hors synchronisation**. L'état « non synchronisé » signifie que les volumes secondaires ne sont pas synchronisés avec le volume primaire (source) et que la réplication SnapMirror n'est pas en cours.

Si l'état du miroir est `Snapmirrored`, indique un échec ou un échec de transfert dû à une opération non prise en charge.

RPO nul

L'objectif RPO correspond à l'objectif de point de récupération, qui correspond à la quantité de perte de données jugée acceptable au cours d'une période donnée. La valeur RPO de zéro signifie qu'aucune perte de données n'est acceptable.

Le RTO nul

L’objectif RTO désigne l’objectif de délai de restauration, qui correspond au temps jugé acceptable pour qu’une application revienne à un fonctionnement normal suite à une panne, une défaillance ou tout autre événement de perte de données. La valeur zéro RTO indique qu’aucune interruption n’est acceptable.

Planification

Prérequis

Lors de la planification du déploiement de la continuité de l’activité SnapMirror, assurez-vous de répondre aux différentes exigences en matière de configuration du système, du matériel et des logiciels.

Sous-jacent

- Seuls les clusters haute disponibilité à deux nœuds sont pris en charge
- Les deux clusters doivent être soit AFF (y compris AFF C-Series), soit ASA (pas de combinaison)

Logiciel

- ONTAP 9.8 ou version ultérieure
- ONTAP Mediator 1.2 ou version ultérieure
- Un serveur Linux ou une machine virtuelle pour le médiateur ONTAP exécutant l’un des éléments suivants :

Version du médiateur ONTAP	Versions Linux prises en charge
1.7	• Red Hat Enterprise Linux : 8.5, 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2 et 9.3 • Rocky Linux 8 et 9
1.6	• Red Hat Enterprise Linux : 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2 • Rocky Linux 8 et 9
1.5	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.4	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.3	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

Licences

- La licence synchrone SnapMirror (SM-S) doit être appliquée aux deux clusters
- La licence SnapMirror doit être appliquée aux deux clusters

> Si vous avez acheté vos systèmes de stockage ONTAP avant juin 2019, consultez la page "Clés de licence principales pour ONTAP NetApp" Pour obtenir la licence SM-S requise.

La licence SnapMirror synchrone et SnapMirror est incluse dans "ONTAP One".

Environnement de mise en réseau

- Le temps de réponse aller-retour de latence entre clusters doit être inférieur à 10 millisecondes.
- Les réservations persistantes SCSI-3 sont **non** prises en charge par SM-BC .

Protocoles pris en charge

- Seuls les protocoles SAN sont pris en charge (pas NFS/SMB).
- Seuls les protocoles Fibre Channel et iSCSI sont pris en charge.
- L'IPspace par défaut est requis par SM-BC pour les relations cluster peer-to-peer. L'IPspace personnalisé n'est pas pris en charge.

Style de sécurité NTFS

Le style de sécurité NTFS est **non** pris en charge sur les volumes SM-BC.

Médiateur de ONTAP

- Le Mediator ONTAP peut être provisionné en externe et connecté à ONTAP pour un basculement transparent des applications.
- Pour fonctionner entièrement et permettre un basculement non planifié automatique, le médiateur ONTAP externe doit être provisionné et configuré avec des clusters ONTAP.
- Le médiateur ONTAP doit être installé dans un troisième domaine de défaillance, distinct des deux clusters ONTAP.
- Lors de l'installation du médiateur ONTAP, vous devez remplacer le certificat auto-signé par un certificat valide signé par une autorité de certification grand public fiable.
- Pour plus d'informations sur le médiateur ONTAP, reportez-vous à la section "Préparez-vous à installer le service ONTAP Mediator".

Volumes de destination en lecture/écriture

- Les relations SM-BC ne sont pas prises en charge sur les volumes de destination en lecture/écriture. Avant de pouvoir utiliser un volume en lecture-écriture, vous devez le convertir en volume DP en créant une relation SnapMirror au niveau du volume, puis en supprimant la relation. Pour plus de détails, voir "Conversion de relations existantes en relations SM-BC"

Des LUN de grande taille et de grands volumes

La prise en charge de LUN et de volumes importants (supérieurs à 100 To) dépend de la version de ONTAP que vous utilisez et de votre plateforme.

ONTAP 9.12.1P2 et versions ultérieures

- Pour ONTAP 9.12.1 P2 et versions ultérieures, SMBC prend en charge les grandes LUN et les volumes de plus de 100 To sur ASA et AFF (y compris C-Series).

> Pour les versions ONTAP 9.12.1P2 et ultérieures, vous devez vous assurer que les clusters principal et secondaire sont des baies SAN 100 % Flash ou des baies 100 % Flash, et que ONTAP 9.12.1 P2 ou version ultérieure est installé sur les deux. Si le cluster secondaire exécute une version antérieure à ONTAP 9.12.1P2 ou si le type de baie n'est pas le même que le cluster principal, la relation synchrone peut être désynchronisée si le volume primaire dépasse 100 To.

ONTAP 9.8 - 9.12.1P1

- Pour les versions ONTAP comprises entre ONTAP 9.8 et 9.12.1 P1 (inclus), les LUN de grande taille et les volumes de grande taille supérieurs à 100 To sont pris en charge uniquement sur les baies SAN 100 % Flash.

> Pour les versions ONTAP comprises entre ONTAP 9.8 et 9.12.1 P2, vous devez vous assurer que les clusters principal et secondaire sont des baies SAN 100 % Flash, et que ONTAP 9.8 ou version ultérieure est installé sur les deux. Si le cluster secondaire exécute une version antérieure à ONTAP 9.8 ou s'il ne s'agit pas d'une baie SAN 100 % Flash, la relation synchrone peut être désynchronisée si le volume principal dépasse les 100 To.

Plus d'informations

- "Hardware Universe"
- "Présentation du médiateur ONTAP"

Fonctionnalités et configurations prises en charge

SnapMirror Business Continuity est compatible avec de nombreux systèmes d'exploitation et d'autres fonctionnalités de ONTAP. En savoir plus sur les détails et les configurations recommandées.

Configurations compatibles

SM-BC est pris en charge par de nombreux systèmes d'exploitation, notamment :

- AIX (à partir de ONTAP 9.11.1)
- HP-UX (à partir de ONTAP 9.10.1)
- Solaris 11.4 (à partir de ONTAP 9.10.1)

AIX

Depuis ONTAP 9.11.1, AIX est pris en charge par SM-BC. Dans le cas d'une configuration AIX, le cluster principal est le cluster « actif ».

Dans une configuration AIX, les basculements sont disruptifs. Chaque basculement nécessite une nouvelle analyse de l'hôte pour que les opérations d'E/S reprennent.

Pour configurer un hôte AIX avec SM-BC, reportez-vous à l'article de la base de connaissances "Comment configurer un hôte AIX pour SnapMirror Business Continuity (SM-BC)".

HP-UX

Depuis ONTAP 9.10.1, SM-BC pour HP-UX est pris en charge.

Limitations de HP-UX

Un événement de basculement automatique non planifié (AUFO) sur le cluster maître isolé peut être causé par une défaillance de double événement lorsque la connexion entre le cluster principal et le cluster secondaire est perdue et que la connexion entre le cluster principal et le médiateur est également perdue. Ce phénomène est considéré comme un événement rare, contrairement à d'autres événements AUFO.

- Dans ce scénario, la reprise des E/S sur l'hôte HP-UX peut prendre plus de 120 secondes. Selon les applications en cours d'exécution, il se peut que cela n'entraîne aucune interruption d'E/S ni aucun message d'erreur.
- Pour résoudre ce problème, vous devez redémarrer les applications sur l'hôte HP-UX dont la tolérance d'interruption est inférieure à 120 secondes.

Recommandation de configuration de l'hôte Solaris

À partir de ONTAP 9.10.1, SM-BC prend en charge Solaris 11.4.

Pour vous assurer que les applications client Solaris ne sont pas perturbatrices lorsqu'un basculement de site non planifié se produit dans un environnement SM-BC, modifiez les paramètres par défaut du système d'exploitation Solaris. Pour configurer Solaris avec les paramètres recommandés, reportez-vous à l'article de la base de connaissances "Prise en charge de Solaris Host Paramètres recommandés dans la configuration de SnapMirror Business Continuity (SM-BC)".

Mise en cluster de basculement Windows

À partir de ONTAP 9.14.1, le clustering avec basculement Windows est pris en charge par SM-BC. Pour plus d'informations, voir "Tr-4878 : continuité de l'activité avec SnapMirror".

Intégrations ONTAP

SM-BC prend en charge d'autres fonctionnalités de ONTAP, notamment :

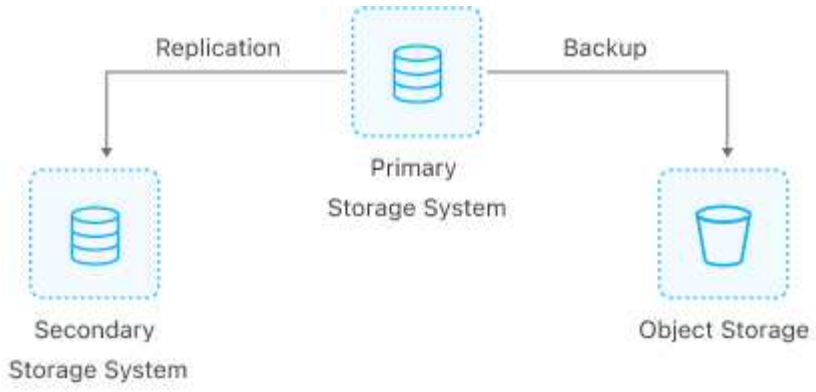
- Configurations « Fan-Out »
- Copie NDMP (à partir de ONTAP 9.13.1)
- Restauration partielle de fichiers (à partir de ONTAP 9.12.1)

FabricPool

SM-BC prend en charge les volumes source et de destination sur les agrégats FabricPool avec les règles de Tiering aucune, Snapshot ou Auto. SM-S SM-BC ne prend pas en charge les agrégats FabricPool à l'aide d'une règle de Tiering.

Configurations « Fan-Out »

Dans un configurations « fan-out », Votre volume source peut être mis en miroir vers un terminal de destination SM-BC et vers une ou plusieurs relations SnapMirror asynchrones.



Supports SM-BC configurations « fan-out » avec le `MirrorAllSnapshots` Et, à partir de ONTAP 9.11.1, le `MirrorAndVault` politique. Les configurations « fan-out » ne sont pas prises en charge dans les modèles SM-BC avec `XDPDefault` politique.

Si vous rencontrez un basculement sur la destination SM-BC dans une configuration de « Fan-Out », vous devez le faire manuellement reprendre la protection dans la configuration du « fan-out ».

Restauration NDMP

Depuis ONTAP 9.13.1, vous pouvez utiliser NDMP pour copier et restaurer des données avec SM-BC. L'utilisation de NDMP vous permet de déplacer des données vers la source SM-BC pour effectuer une restauration sans interrompre la protection. Cette fonctionnalité est particulièrement utile dans les configurations « Fan-Out ».

Pour en savoir plus sur ce processus, voir Transfert de données à l'aide d'une copie ndmp.

Restauration partielle des fichiers

Depuis ONTAP 9.12.1, la restauration partielle de LUN est prise en charge pour les volumes SM-BC. Pour plus d'informations sur ce processus, reportez-vous à la section "Restaurez une partie d'un fichier à partir d'une copie Snapshot".

Limites des objets pour la continuité de l'activité SnapMirror

Lorsque vous vous préparez à utiliser et à gérer SnapMirror Business Continuity, tenez compte des limitations suivantes.

Groupes de cohérence dans un cluster

Les limites de groupes de cohérence d'un cluster avec SM-BC sont calculées en fonction des relations et dépendent de la version de ONTAP utilisée. Les limites sont indépendantes de la plateforme.

Version ONTAP	Nombre maximal de relations
ONTAP 9.8-9.9.1	5
ONTAP 9.10.1	20
ONTAP 9.11.1 et versions ultérieures	50

Volumes par groupe de cohérence

Le nombre maximal de volumes par groupe de cohérence avec SM-BC est indépendant de la plateforme.

Version ONTAP	Nombre maximal de volumes pris en charge dans une relation de groupe de cohérence
ONTAP 9.8-9.9.1	12
ONTAP 9.10.1 et versions ultérieures	16

Volumes

Les limites de volume dans SM-BC sont calculées en fonction du nombre de points finaux, et non du nombre de relations. Un groupe de cohérence de 12 volumes contribue à hauteur de 12 terminaux sur le cluster principal et le cluster secondaire. Les relations SM-BC et SnapMirror synchrone contribuent au nombre total de terminaux.

Le nombre maximum de terminaux par plateforme est inclus dans le tableau suivant.

S. Non	Plateforme	Terminaux par HA pour SM-BC			Synchronisation globale et terminaux SM-BC par haute disponibilité		
		ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 et versions ultérieures	ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 et versions ultérieures
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

Limites D’objets SAN

Les limites des objets SAN sont incluses dans le tableau suivant. Les limites s’appliquent quelle que soit la plate-forme.

Objet dans une relation SM-BC	Nombre
LUN par volume	256
Mappages de LUN par nœud	• 4096 (ONTAP 9.10 et versions ultérieures) • 2048 (ONTAP 9.9.1 et versions antérieures)
Mappages de LUN par cluster	• 8192 (ONTAP 9.10 et versions ultérieures) • 4096 (ONTAP 9.9.1 et versions antérieures)
LIFs par SVM (avec au moins un volume dans une relation SM-BC)	256
LIF inter-cluster par nœud	4
LIF inter-cluster par cluster	8

Informations associées

- "Hardware Universe"
- "Limites des groupes de cohérence"

Installation et configuration

Configurez le médiateur ONTAP et les clusters pour la continuité de l'activité SnapMirror

SnapMirror Business Continuity (SM-BC) utilise des clusters à peering pour assurer la disponibilité de vos données en cas de basculement. Le médiateur ONTAP est une ressource clé qui assure la continuité de l'activité et surveille l'état de santé de chaque cluster. Pour configurer SM-BC, vous devez d'abord installer le médiateur ONTAP et vous assurer que les clusters principal et secondaire sont correctement configurés.

Une fois que vous avez installé le médiateur ONTAP et configuré vos clusters, vous devez le faire [initialize-the-ontap-mediator] Le médiateur ONTAP à utiliser avec SM-BC. Vous devez alors Créez, initialisez et mappez le groupe de cohérence pour SM-BC

Médiateur de ONTAP

Le médiateur ONTAP établit un quorum pour les clusters ONTAP dans une relation SM-BC. Il coordonne le basculement automatisé lors de la détection d'une défaillance, en déterminant quel cluster agit comme le cluster principal et en veillant à ce que les données soient servies à la destination correcte et en partant de celle-ci.

Conditions requises pour le médiateur ONTAP

- Le médiateur ONTAP comprend son propre ensemble de prérequis. Vous devez remplir ces conditions préalables avant d'installer le médiateur.

  Pour plus d'informations, voir "Préparez-vous à installer le service ONTAP Mediator".

- Par défaut, le médiateur ONTAP fournit un service via le port TCP 31784. Assurez-vous que le port 31784 est ouvert et disponible entre les clusters ONTAP et le médiateur.

Installer le médiateur ONTAP et confirmer la configuration du cluster

Suivez chacune des étapes suivantes. Pour chaque étape, vous devez confirmer que la configuration spécifique a été effectuée. Utilisez le lien fourni après chaque étape pour obtenir plus d'informations si nécessaire.

Étapes

1. Installez le service Mediator ONTAP avant de vous assurer que vos clusters source et destination sont correctement configurés.

   Préparez l'installation ou la mise à niveau du service Mediator ONTAP

2. Vérifier qu'une relation de peering de cluster existe entre les clusters

   > L'IPspace par défaut est requis par SM-BC pour les relations cluster peer-to-peer. Un IPspace personnalisé n'est pas pris en charge.

   Configurer les relations de pairs

3. Vérifier que les machines virtuelles de stockage sont créées sur chaque cluster

   Création d'un SVM

4. Vérifiez qu'il existe une relation homologue entre les machines virtuelles de stockage de chaque cluster.

   Création d'une relation de SVM peering

5. Vérifiez que les volumes existent pour vos LUN.

   Création d'un volume

6. Confirmer qu'au moins une LIF SAN est créée sur chaque nœud du cluster

   "Considérations relatives aux LIF dans un environnement SAN de cluster"

   "Création d'une LIF"

7. Vérifiez que les LUN nécessaires sont créées et mappées sur un groupe initiateur, qui est utilisé pour mapper les LUN sur l'initiateur sur l'hôte d'application.

   Créer des LUN et mapper des igroups

8. Relancez l'analyse de l'hôte de l'application pour détecter toute nouvelle LUN.

Initialisez le médiateur ONTAP pour SM-BC

Une fois que vous avez installé le médiateur ONTAP et confirmé la configuration du cluster, vous devez initialiser le médiateur ONTAP pour la surveillance du cluster. Vous pouvez initialiser le médiateur ONTAP à l'aide du Gestionnaire système ou de l'interface de ligne de commande ONTAP.

System Manager

Avec System Manager, vous pouvez configurer le serveur ONTAP Mediator pour un basculement automatisé. Vous pouvez également remplacer le SSL et l'autorité de certification auto-signés par le certificat SSL et l'autorité de certification validés par un tiers si vous ne l'avez pas déjà fait.

Étapes

1. Accédez à **protection > vue d'ensemble > Médiateur > configurer**.
2. Sélectionnez **Ajouter** et entrez les informations suivantes sur le serveur ONTAP Mediator :
   - Adresse IPv4
   - Nom d'utilisateur
   - Mot de passe
   - Certificat

CLI

Vous pouvez initialiser le médiateur ONTAP à partir du cluster principal ou secondaire à l'aide de l'interface de ligne de commande ONTAP. Lorsque vous émettez le `mediator add` Sur un cluster, le médiateur ONTAP est automatiquement ajouté sur l'autre cluster.

Étapes

1. Initialiser le médiateur sur l'un des clusters :

   ```
   snapmirror mediator add -mediator-address IP_Address -peer-cluster
   cluster_name -username user_name
   ```

   Exemple

   ```
   cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
   -peer-cluster cluster2 -username mediatoradmin
   Notice: Enter the mediator password.

   Enter the password: ******
   Enter the password again: ******
   ```

2. Vérifiez l'état de la configuration du médiateur :

   ```
   snapmirror mediator show
   ```

   ```
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   192.168.10.1     cluster-2        connected         true
   ```

   `Quorum Status` Indique si les relations de groupe de cohérence SnapMirror sont synchronisées avec le médiateur ; le statut est `true` indique une synchronisation réussie.

Protégez-vous avec la continuité de l'activité SnapMirror

Configurer la protection à l'aide de SnapMirror Business Continuity implique de sélectionner des LUN sur le cluster source ONTAP et de les ajouter à un groupe de cohérence.

Avant de commencer

- Vous devez avoir un "Licence SnapMirror synchrone".
- Vous devez être un administrateur de cluster ou de machines virtuelles de stockage.
- Tous les volumes constitutifs d'un groupe de cohérence doivent se trouver dans une seule VM de stockage (SVM).
  - Les LUN peuvent résider sur des volumes différents.
- Le cluster source et le cluster destination ne peuvent pas être identiques.
- Vous ne pouvez pas établir de relations de groupe de cohérence SM-BC entre les clusters ASA et les clusters non ASA.
- L'IPspace par défaut est requis par SM-BC pour les relations cluster peer-to-peer. L'IPspace personnalisé n'est pas pris en charge.
- Le nom du groupe de cohérence doit être unique.
- Les volumes du cluster secondaire (destination) doivent être de type DP.
- Les SVM primaire et secondaire doivent être en relation de peering.

Étapes

Vous pouvez configurer un groupe de cohérence via l'interface de ligne de commandes ONTAP ou System Manager.

Depuis ONTAP 9.10.1, ONTAP propose un menu et un terminal de groupe de cohérence dans System Manager, ainsi que des utilitaires de gestion supplémentaires. Si vous utilisez ONTAP 9.10.1 ou une version ultérieure, reportez-vous à la section "Configurer un groupe de cohérence" ensuite "configurer la protection" Pour créer une relation SM-BC.

System Manager

1. Sur le cluster principal, accédez à **protection > Présentation > protéger pour la continuité de l'activité > protéger les LUN**.
2. Sélectionnez les LUN que vous souhaitez protéger et ajoutez-les à un groupe de protection.
3. Sélectionner le cluster de destination et le SVM.
4. **Initialize relation** est sélectionné par défaut. Cliquez sur **Save** pour commencer la protection.
5. Accédez à **Tableau de bord > performances** pour vérifier l'activité IOPS des LUN.
6. Sur le cluster de destination, utilisez System Manager pour vérifier que la protection de la relation de continuité de l'activité est en mode synchrone : **protection > relations**.

CLI

1. Créez une relation de groupe de cohérence à partir du cluster destination.
   `destinatio:> snapmirror create -source-path *source-path* -destination-path *destination-path* -cg-item -mappings *volume-paths* -policy *policy-name*

   Vous pouvez mapper jusqu'à 12 volumes constitutifs à l'aide du `cg-item-mappings` sur le `snapmirror create` commande.

   La création de deux groupes de cohérence dans l'exemple suivant : `cg_src_ on the source with `vol1` et `vol2` et un groupe de cohérence de destination en miroir, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. Depuis le cluster de destination, initialisez le groupe de cohérence.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

3. Confirmer que l'opération d'initialisation a réussi. Le statut doit être de `InSync`.

   ```
   snapmirror show
   ```

4. Sur chaque cluster, créez un groupe initiateur afin de mapper les LUN sur l'initiateur de l'hôte d'application.
   `lun igroup create -igroup *name* -protocol *fcp|iscsi* -ostype *os* -initiator *initiator_name*`
5. Sur chaque cluster, mappez les LUN sur le groupe initiateur :

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Vérifiez que le mappage de LUN a réussi avec le `lun map` commande. Vous pouvez ensuite détecter les nouveaux LUN sur l'hôte d'application.

Gestion de SM-BC et protection des données

Créer une copie Snapshot commune

Outre les opérations de copie Snapshot planifiées régulièrement, vous pouvez créer manuellement une commune "La copie Snapshot" Entre les volumes du groupe de cohérence SnapMirror principal et les volumes du groupe de cohérence SnapMirror secondaire.

Description de la tâche

- Dans ONTAP 9.8, l'intervalle de création d'instantanés planifié est d'une heure.

  Depuis ONTAP 9.9.1, cet intervalle est de 12 heures.

Avant de commencer

- La relation de groupe SnapMirror doit être en mode synchrone.

Étapes

1. Créer une copie Snapshot commune :

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. Surveiller la progression de la mise à jour :

   ```
   destination::>snapmirror show -fields -newest-snapshot
   ```

Effectuer un basculement planifié

Lors d'un basculement planifié, vous changez les rôles des clusters principal et secondaire, de sorte que le cluster secondaire prenne le relais du cluster principal. Lors d'un basculement, ce qui est généralement le cluster secondaire traite les demandes d'entrée et de sortie localement sans interrompre les opérations client.

Vous pouvez effectuer un basculement planifié pour tester l'état de santé de votre configuration de reprise sur incident ou pour effectuer des opérations de maintenance sur le cluster principal.

Description de la tâche

Un basculement planifié est initié par l'administrateur du cluster secondaire. L'opération nécessite le basculement des rôles principal et secondaire afin que le cluster secondaire prenne le relais du cluster principal. Le nouveau cluster principal peut alors commencer à traiter les demandes d'entrée et de sortie localement, sans interrompre les opérations client.

Avant de commencer

- La relation SM-BC doit être synchronisée.
- Vous ne pouvez pas lancer de basculement planifié lorsqu'une opération sans interruption est en cours. La continuité de l'activité inclut les déplacements de volumes, les transferts d'agrégats et les basculements de stockage.
- Le médiateur ONTAP doit être configuré, connecté et en quorum.

Étapes

Vous pouvez effectuer un basculement planifié via l'interface de ligne de commande ONTAP ou System Manager.

System Manager

1. Dans System Manager, sélectionnez **protection > vue d'ensemble > relations**.
2. Identifiez la relation SM-BC à basculer. En regard de son nom, sélectionnez le … À côté du nom de la relation, puis sélectionnez **basculement**.
3. Pour surveiller l'état du basculement, utilisez `snapmirror failover show` Dans l'interface de ligne de commandes ONTAP.

CLI

1. Depuis le cluster de destination, lancer l'opération de basculement :

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Surveiller la progression du basculement :

   ```
   destination::>snapmirror failover show
   ```

3. À la fin de l'opération de basculement, vous pouvez surveiller l'état de la relation de protection SnapMirror synchrone depuis la destination :

   ```
   destination::>snapmirror show
   ```

Restaurez vos données après des opérations automatiques de basculement non planifié

Une opération automatique de basculement non planifié (AUFO) se produit lorsque le cluster principal est en panne ou isolé. Le médiateur ONTAP détecte les basculements et exécute un basculement automatique non planifié vers le cluster secondaire. Le cluster secondaire est converti en cluster principal et commence à servir les clients. Cette opération est effectuée uniquement avec l'aide du médiateur ONTAP.

> Après le basculement automatique non planifié, il est important d'analyser à nouveau les chemins d'E/S des LUN hôtes afin d'éviter toute perte de chemins d'E/S.

Rétablir la relation de protection après un basculement non planifié

Vous pouvez rétablir la relation de protection à l'aide de System Manager ou de l'interface de ligne de commandes ONTAP.

System Manager

Étapes

1. Accédez à **protection > relations** et attendez que l'état de la relation affiche "insync".
2. Pour reprendre les opérations sur le cluster source d'origine, cliquez sur ⋮ Et sélectionnez **basculement**.

CLI

Vous pouvez surveiller l'état du basculement automatique non planifié à l'aide du `snapmirror failover show` commande.

Par exemple :

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Reportez-vous à la "Référence EMS" pour en savoir plus sur les messages d'événement et sur les actions correctives à mener.

Reprise de la protection dans une configuration « Fan-Out » après le basculement

Si vous rencontrez un basculement sur le cluster secondaire dans la relation SM-BC, la destination SnapMirror asynchrone devient défectueuse. Vous devez restaurer manuellement la protection en supprimant et en recréant la relation avec le terminal SnapMirror asynchrone.

Étapes

1. Vérifiez que le basculement s'est terminé correctement :
   `snapmirror failover show`
2. Sur le terminal SnapMirror asynchrone, supprimez le terminal « Fan-Out » :
   `snapmirror delete -destination-path` *`destination_path`*
3. Sur le troisième site, créer des relations SnapMirror asynchrones entre le nouveau volume primaire SM-BC et le volume de destination asynchrone Fan-Out :
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. Resynchroniser la relation :
   `snapmirror resync -destination-path` *`destination_path`*
5. Vérifiez l'état et l'état de la relation :

```
snapmirror show
```

Surveiller les opérations de continuité de l'activité SnapMirror

Vous pouvez contrôler les opérations SnapMirror Business Continuity (SM-BC) suivantes pour assurer l'état de votre configuration SM-BC :

- Médiateur de ONTAP
- Opérations de basculement planifiées
- Opérations de basculement non planifiées automatiques
- Disponibilité de SM-BC

Médiateur de ONTAP

En fonctionnement normal, l'état du médiateur ONTAP doit être connecté. S'il est dans un autre état, cela peut indiquer une condition d'erreur. Vous pouvez consulter le "Messages du système de gestion des événements (EMS)" pour déterminer l'erreur et les actions correctives appropriées.

Opérations de basculement planifiées

Vous pouvez surveiller l'état et la progression d'une opération de basculement planifié à l'aide de l' `snapmirror failover show` commande. Par exemple :

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Une fois le basculement terminé, vous pouvez surveiller l'état de protection SnapMirror synchrone depuis le nouveau cluster de destination. Par exemple :

```
ClusterA::> snapmirror show
```

Reportez-vous à la "Référence EMS" pour en savoir plus sur les messages d'événement et les actions correctives à mener.

Opérations de basculement non planifiées automatiques

Lors d'un basculement automatique non planifié, vous pouvez surveiller l'état de l'opération à l'aide du `snapmirror failover show` commande.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Reportez-vous à la "Référence EMS" pour en savoir plus sur les messages d'événement et sur les actions correctives à mener.

Disponibilité de SM-BC

Vous pouvez vérifier la disponibilité de la relation SM-BC à l'aide d'une série de commandes, soit sur le cluster principal, soit sur le cluster secondaire, soit les deux.

Les commandes que vous utilisez incluent `snapmirror mediator show` commande sur le cluster principal et le cluster secondaire pour vérifier le statut de connexion et de quorum, le `snapmirror show` et la `volume show` commande. Par exemple :

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored InSync  -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored InSync    -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                     Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                      No-consensus
```

Permet d’ajouter ou de supprimer des volumes à un groupe de cohérence

À mesure que les exigences des charges de travail applicatives évoluent, vous devrez peut-être ajouter ou supprimer des volumes d’un groupe de cohérence pour assurer la continuité de l’activité. Le processus d’ajout et de suppression de volumes dans une relation SM-BC active dépend de la version de ONTAP que vous utilisez.

Dans la plupart des cas, il s’agit d’un processus perturbateur qui vous oblige à interrompre la relation SnapMirror, à modifier le groupe de cohérence, puis à reprendre la protection. Depuis ONTAP 9.13.1, l’ajout de volumes à un groupe de cohérence avec une relation SM-BC active n’entraîne aucune interruption.

Description de la tâche

- Dans ONTAP 9.8 à 9.9.1, vous pouvez ajouter ou supprimer des volumes à un groupe de cohérence à l'aide de l'interface de ligne de commandes ONTAP.
- Depuis ONTAP 9.10.1, il est recommandé de le gérer "groupes de cohérence" Via System Manager ou avec l'API REST ONTAP.

  Si vous souhaitez modifier la composition du groupe de cohérence en ajoutant ou en supprimant un volume, vous devez d'abord supprimer la relation d'origine, puis créer à nouveau le groupe de cohérence avec la nouvelle composition.

- À partir de ONTAP 9.13.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption avec une relation SM-BC active à partir de la source ou de la destination.

  La suppression de volumes est une opération disruptive. Vous devez interrompre la relation SnapMirror avant de procéder à la suppression de volumes.

ONTAP 9.8-9.13.0

Avant de commencer

- Vous ne pouvez pas commencer à modifier le groupe de cohérence tant qu'il se trouve dans le groupe `InSync` état.
- Le volume de destination doit être de type DP.
- Le nouveau volume que vous ajoutez pour développer le groupe de cohérence doit disposer d'une paire de copies Snapshot communes entre les volumes source et de destination.

Étapes

Les exemples présentés dans deux mappages de volume : `vol_src1` ←→ `vol_dst1` et `vol_src2` ←→ `vol_dst2`, dans une relation de groupe de cohérence entre les points d'extrémité `vs1_src:/cg/cg_src` et `vs1_dst:/cg/cg_dst`.

1. Sur le cluster source et le cluster destination, vérifiez qu'il existe un Snapshot commun entre le cluster source et le cluster destination avec la commande `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. Si aucune copie Snapshot n'existe déjà, créez et initialisez une relation FlexVol SnapMirror :

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Supprimez la relation de groupe de cohérence :

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
   ```

4. Libérer la relation SnapMirror source et conserver les copies Snapshot courantes :

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Annulez le mappage des LUN et supprimez la relation de groupe de cohérence existante :

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > Les LUN de destination ne sont pas mappées, tandis que les LUN présentes sur la copie primaire continuent de servir les E/S de l'hôte

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **Si vous utilisez ONTAP 9.10.1 à 9.13.0,** supprimez et recréez et le groupe de cohérence sur la source avec la composition correcte. Suivez les étapes de la section Supprimez un groupe de cohérence puis Configurez un seul groupe de cohérence. Dans ONTAP 9.10.1 et les versions ultérieures, vous devez effectuer les opérations de suppression et de création dans System Manager ou avec l'API REST ONTAP ; il n'existe pas de procédure d'interface de ligne de commandes.

   Si vous utilisez ONTAP 9.8, 9.0 ou 9.9.1, passez à l'étape suivante.

7. Créez le nouveau groupe de cohérence sur la destination avec la nouvelle composition :

   ```
   destination::>snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
   vol_src2:@vol_dst2, vol_src3:@vol_dst3
   ```

8. Resynchroniser la relation de groupe de cohérence RTO zéro pour garantir qu'elle est synchronisée :

   ```
   destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

9. Remappage des LUN que vous n'avez pas mappées à l'étape 5 :

   ```
   destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
   ```

10. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

ONTAP 9.13.1 et versions ultérieures

À partir de ONTAP 9.13.1, vous pouvez ajouter des volumes à un groupe de cohérence sans interruption avec une relation SM-BC active. SM-BC prend en charge l'ajout de volumes à partir de la source ou de la destination.

Pour plus d'informations sur l'ajout de volumes provenant du groupe de cohérence source, reportez-vous à la section Modifier un groupe de cohérence.

Ajout d'un volume depuis le cluster de destination

1. Sur le cluster de destination, sélectionnez **protection** > **relations**.
2. Recherchez la relation SM-BC à laquelle vous souhaitez ajouter des volumes. Sélectionnez ⋮ Puis **développer**.
3. Sélectionnez les relations de volume dont les volumes doivent être ajoutés au groupe de cohérence
4. Sélectionnez **développer**.

Convertir les relations existantes en relations SM-BC

Si vous avez une relation SnapMirror synchrone existante entre un cluster source et un cluster destination, vous pouvez la convertir en relation SM-BC. Vous pouvez ainsi associer les volumes en miroir à un groupe de cohérence, garantissant ainsi un RPO nul sur une charge de travail à plusieurs volumes. En outre, vous pouvez conserver les snapshots SnapMirror existants si vous devez revenir à un point dans le temps avant d'établir la relation SM-BC.

Avant de commencer

- Une relation SnapMirror synchrone avec RPO nul doit exister entre le cluster principal et le cluster

secondaire.

- Avant de pouvoir créer la relation SnapMirror avec un objectif RTO nul, toutes les LUN du volume de destination doivent être démappées.
- SM-BC prend uniquement en charge les protocoles SAN (et non NFS/CIFS). Assurez-vous qu'aucun composant du groupe de cohérence n'est monté pour l'accès au NAS.

Description de la tâche

- Vous devez être administrateur du cluster et SVM sur les clusters principal et secondaire.
- Vous ne pouvez pas convertir le RPO nul en synchronisation RTO zéro en modifiant la règle SnapMirror.
- Vous devez vous assurer que le mappage des LUN est annulé avant d'émettre le `snapmirror create` commande.

  Si les LUN existantes du volume secondaire sont mappées et l' `AutomatedFailover` la règle est configurée, le `snapmirror create` déclenche une erreur.

Étapes

1. Depuis le cluster secondaire, effectuer une mise à jour SnapMirror sur la relation existante :

   ```
   destination::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Vérifier que la mise à jour SnapMirror a été correctement effectuée :

   ```
   destination::>snapmirror show
   ```

3. Arrêter chaque relation synchrone RPO zéro :

   ```
   destination::>snapmirror quiesce -destination-path vs1_dst:vol1

   destination::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Supprimez chacune des relations synchrones RPO zéro :

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol1

   destination::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Relâcher la relation SnapMirror source mais conserver les copies Snapshot courantes :

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Création d'une relation SnapMirror synchrone RTO nul groupe :

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination
   -path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Resynchroniser le groupe de cohérence :

```
destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

Mettez à niveau et restaurez ONTAP avec SM-BC

SnapMirror Business Continuity (SM-BC) est pris en charge à partir de la version 9.8 de ONTAP. La mise à niveau et la restauration de votre cluster ONTAP ont des implications sur vos relations SM-BC selon la version de ONTAP vers laquelle vous effectuez la mise à niveau ou la restauration.

Mettez à niveau ONTAP avec SM-BC

Pour utiliser SM-BC, tous les nœuds des clusters source et cible doivent exécuter ONTAP 9.8 ou une version ultérieure.

Lorsque vous mettez à niveau ONTAP avec des relations SM-BC actives, vous devez utiliser Mise à niveau automatisée sans interruption (ANDU). L'utilisation d'ANDU garantit que vos relations SM-BC sont synchronisées et saines pendant le processus de mise à niveau.

Il n'y a pas d'étape de configuration pour préparer les déploiements SM-BC pour les mises à niveau ONTAP. Cependant, il est recommandé de vérifier, avant et après la mise à niveau :

- Les relations SM-BC sont synchronisées.
- Il n'y a pas d'erreur liée à SnapMirror dans le journal des événements.
- Le Mediator est en ligne et sain à partir des deux clusters.
- Tous les hôtes peuvent voir tous les chemins correctement pour protéger les LUN.

> Lorsque vous mettez à niveau des clusters de ONTAP 9.8 ou 9.9.1 vers ONTAP 9.10.1 et versions ultérieures, ONTAP crée de nouvelles données groupes de cohérence Sur les clusters source et cible pour les relations SM-BC qui peuvent être configurées à l'aide de System Manager.

> Le `snapmirror quiesce` et `snampirror resume` Les commandes ne sont pas prises en charge par SM-BC.

Restaurez ONTAP 9.9.1 à partir de ONTAP 9.10.1

Pour rétablir des relations de 9.10.1 à 9.9.1, les relations SM-BC doivent être supprimées, suivies de l'instance de groupe de cohérence 9.10.1. Impossible de supprimer les groupes de cohérence avec une relation SM-BC active. Tout volume FlexVol mis à niveau vers la version 9.10.1 précédemment associé à une autre application de conteneur intelligent ou d'entreprise en 9.9.1 ou version antérieure ne sera plus associé à la restauration. La suppression des groupes de cohérence ne supprime pas les volumes constitutifs ou les snapshots granulaires volume. Reportez-vous à la section "Supprimez un groupe de cohérence" Pour plus d'informations sur cette tâche dans ONTAP 9.10.1 et versions ultérieures.

Restaurez ONTAP 9.7 à partir de ONTAP 9.8

> SM-BC n'est pas pris en charge avec les clusters mixtes ONTAP 9.7 et ONTAP 9.8.

Lorsque vous restaurez ONTAP 9.8 vers ONTAP 9.7, vous devez tenir compte des éléments suivants :

- Si le cluster héberge une destination SM-BC, le retour à ONTAP 9.7 n'est pas autorisé tant que la relation n'est pas rompue et supprimée.
- Si le cluster héberge une source SM-BC, le retour à ONTAP 9.7 n'est pas autorisé tant que la relation n'est pas validée.
- Toutes les politiques SnapMirror personnalisées SM-BC créées par l'utilisateur doivent être supprimées avant de revenir à ONTAP 9.7.

Pour répondre à ces exigences, reportez-vous à la section "Supprimer une configuration SM-BC".

Étapes

1. Effectuer une vérification de restauration à partir de l'un des clusters de la relation SM-BC :

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   ```

   Exemple :

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
      abort
       Command to see if the Relationship Status of a SnapMirror
   relationship
   ```

```
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.8"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

Pour plus d'informations sur le rétablissement des clusters, reportez-vous à la section "Restaurez la ONTAP".

Supprimer une configuration SM-BC

Si vous n'avez plus besoin de la protection SnapMirror Syncronous RTO nul, vous pouvez supprimer votre relation SM-BC.

Description de la tâche

- Avant de supprimer la relation SM-BC, toutes les LUN du cluster destination doivent être mappées.
- Une fois que les LUN sont démappées et que l'hôte est réanalysé, la cible SCSI informe les hôtes que l'inventaire des LUN a changé. Les LUN existantes sur les volumes secondaires RTO de zéro sont modifiées pour refléter une nouvelle identité après la suppression de la relation RTO de zéro. Les hôtes découvrent les LUN du volume secondaire en tant que nouveaux LUN sans relation avec les LUN du volume source.
- Les volumes secondaires restent des volumes DP une fois la relation supprimée. Vous pouvez lancer le `snapmirror break` pour les convertir en lecture/écriture.
- La suppression de la relation n'est pas autorisée à l'état d'échec lorsque la relation n'est pas inversée.

Étapes

1. Depuis le cluster secondaire, supprimez la relation du groupe de cohérence SM-BC entre le noeud final source et le noeud final de destination :

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. Depuis le cluster principal, relationer la relation de groupe de cohérence et les copies Snapshot créées pour la relation :

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Effectuez une nouvelle analyse de l'hôte pour mettre à jour l'inventaire des LUN.
4. Depuis la version ONTAP 9.10.1, la suppression de la relation SnapMirror ne supprime pas le groupe de cohérence. Pour supprimer le groupe de cohérence, vous devez utiliser System Manager ou l'API REST de ONTAP. Voir Supprimez un groupe de cohérence pour en savoir plus.

Supprimer le médiateur ONTAP

Si vous souhaitez supprimer une configuration de médiateur ONTAP existante de vos clusters ONTAP, vous pouvez le faire à l'aide du `snapmirror mediator remove` commande.

Étapes

1. Supprimer un médiateur ONTAP :

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
   cluster_xyz
   ```

Résoudre les problèmes

L'opération de suppression de SnapMirror a échoué lors du basculement

Problème :

Lorsque ONTAP 9.9.1 est installé sur un cluster, exécutant le `snapmirror delete` La commande échoue lorsqu'une relation de groupe de cohérence SM-BC est à l'état basculement.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solution

Lorsque les nœuds d'une relation SM-BC sont en état de basculement, exécutez l'opération de suppression et de libération de SnapMirror avec l'option « force » définie sur vrai.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Échec de la création d'une relation SnapMirror et initialisation du groupe de cohérence

Problème :

La création de la relation SnapMirror et l'initialisation du groupe de cohérence échouent.

Solution :

Vérifiez que vous n'avez pas dépassé la limite des groupes de cohérence par cluster. Les limites de groupes de cohérence dans SM-BC sont indépendantes de la plate-forme et diffèrent selon la version de ONTAP. Voir "Restrictions et limitations supplémentaires" Pour connaître les limites basées sur la version ONTAP.

Erreur :

Si le groupe de cohérence reste en cours d'initialisation, vérifiez l'état des initialisations de groupes de cohérence avec l'API REST de ONTAP, System Manager ou la commande `sn show -expand`.

Solution :

Si les groupes de cohérence ne s'initialisent pas, supprimez la relation SM-BC, supprimez le groupe de cohérence, recréez la relation et initialisez-la. Ce flux de travail diffère selon la version de ONTAP que vous utilisez.

Si vous utilisez ONTAP 9.8-9.9.1	Si vous utilisez ONTAP 9.10.1 ou version ultérieure
1. "Déposer la configuration SM-BC" 2. "Créer une relation de groupe de cohérence" 3. "Initialiser la relation de groupe de cohérence"	1. Sous **protection > relations**, recherchez la relation SM-BC sur le groupe de cohérence. Sélectionnez ⋮, Puis **Supprimer** pour supprimer la relation SM-BC. 2. "Supprimez le groupe de cohérence" 3. "Configurer le groupe de cohérence"

Échec du basculement planifié

Problème :

Après avoir exécuté le `snapmirror failover start` commande, sortie de `snapmirror failover show` commande affiche un message indique qu'une opération sans interruption est en cours.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                          08:35:04
08:35:04
```

Cause :

Un basculement planifié ne peut pas commencer lorsqu'une opération sans interruption est en cours, notamment le déplacement de volumes, le déplacement d'agrégats et le basculement du stockage.

Solution :

Attendez la fin de l'opération sans interruption et réessayez l'opération de basculement.

Le médiateur ONTAP est inaccessible ou l'état du quorum du médiateur est faux

Problème :

Après avoir exécuté le `snapmirror failover start` commande, sortie de `snapmirror failover show` Commande affiche un message indiquant que le médiateur n'est pas configuré.

Voir "Initialisez le médiateur ONTAP".

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Cause :

Le médiateur n'est pas configuré ou il existe des problèmes de connectivité réseau.

Solution :

Si le médiateur ONTAP n'est pas configuré, vous devez configurer le médiateur ONTAP avant de pouvoir établir une relation SM-BC. Résolvez tous les problèmes de connectivité réseau. Vérifiez que Mediator est connecté et que l'état du quorum est défini sur le site source et le site de destination à l'aide de la commande snapmirror médiateur show. Pour plus d'informations, voir Configurez le médiateur ONTAP.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Basculement non planifié automatique non déclenché sur le site B

Problème :

Une défaillance sur le site A ne déclenche pas de basculement non planifié sur le site B.

Cause possible n° 1 :

Le médiateur ONTAP n'est pas configuré. Pour déterminer si c'est la cause, lancez le `snapmirror mediator show` Commande sur le cluster site B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Cet exemple indique que le médiateur ONTAP n'est pas configuré sur le site B.

Solution :

Assurez-vous que ONTAP Mediator est configuré sur les deux clusters, que l'état est connecté et que le quorum est défini sur vrai.

Cause possible n°2 :

Le groupe de cohérence SnapMirror est désynchronisé. Pour déterminer s'il en est ainsi, consultez le journal des événements pour savoir si le groupe de cohérence était en cours de synchronisation au moment où le site A défaillant.

```
cluster::*> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solution :

Procédez comme suit pour effectuer un basculement forcé sur le site B.

1. Annulez le mappage de toutes les LUN appartenant au groupe de cohérence à partir du site B.
2. Supprimez la relation de groupe de cohérence SnapMirror à l'aide du `force` option.

3. Entrez le `snapmirror break` Commande sur les volumes constitutifs du groupe de cohérence pour convertir les volumes DP en R/W, afin d'activer les E/S à partir du site B.
4. Démarrez les nœuds du site A pour créer une relation RTO zéro du site B au site A.
5. Libérez le groupe de cohérence avec `relationship-info-only` Sur le site A pour conserver la copie Snapshot commune et annuler le mappage des LUN appartenant au groupe de cohérence.
6. Convertissez les volumes du site A de la lecture/écriture en DP en configurant une relation de niveau volume en utilisant la règle de synchronisation ou la stratégie asynchrone.
7. Émettez le `snapmirror resync` pour synchroniser les relations.
8. Supprimez les relations SnapMirror avec la règle de synchronisation sur le site A.
9. Libérer les relations SnapMirror avec la règle de synchronisation à l'aide de `relationship-info-only true` Sur le site B.
10. Créer une relation de groupe de cohérence entre le site B et le site A.
11. Effectuez une resynchronisation de groupe de cohérence à partir du site A, puis vérifiez que le groupe de cohérence est en cours de synchronisation.
12. Relancez les chemins d'E/S de la LUN hôte pour restaurer tous les chemins d'accès aux LUN.

Lien entre le site B et le médiateur vers le bas et le site A vers le bas

Pour vérifier la connexion du médiateur ONTAP, utilisez le `snapmirror mediator show` commande. Si l'état de la connexion est injoignable et que le site B ne parvient pas à atteindre le site A, vous aurez une sortie similaire à celle ci-dessous. Suivez les étapes de la solution pour restaurer la connexion

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solution

Forcer un basculement pour activer les E/S depuis le site B, puis établir une relation RTO nul entre le site B et le site A. Procédez comme suit pour effectuer un basculement forcé sur le site B.

1. Annulez le mappage de toutes les LUN appartenant au groupe de cohérence à partir du site B.
2. Supprimez la relation de groupe de cohérence SnapMirror à l'aide de l'option force.
3. Entrez la commande SnapMirror break (`snapmirror break -destination_path svm:_volume_`) Sur les volumes constitutifs du groupe de cohérence pour convertir les volumes de DP en RW, afin d'activer les E/S à partir du site B.

   Vous devez lancer la commande SnapMirror break pour chaque relation du groupe de cohérence. Par exemple, si le groupe de cohérence contient trois volumes, vous exécutez la commande pour chaque volume.

4. Démarrez les nœuds du site A pour créer une relation RTO zéro du site B au site A.
5. Libérer le groupe de cohérence avec les informations uniquement sur le site A pour conserver la copie Snapshot commune et annuler le mappage des LUN appartenant au groupe de cohérence.
6. Convertissez les volumes du site A de RW en DP en configurant une relation au niveau du volume à l'aide de la règle de synchronisation ou de la stratégie asynchrone.
7. Émettez le `snapmirror resync` pour synchroniser les relations.
8. Supprimez les relations SnapMirror avec la règle de synchronisation sur le site A.
9. Établissez les relations SnapMirror avec la règle de synchronisation à l'aide de Relationship-info-only true sur le site B.
10. Créer une relation de groupe de cohérence entre le site B et le site A.
11. Depuis le cluster source, resynchronisez le groupe de cohérence. Vérifiez que l'état du groupe de cohérence est synchronisé.
12. Relancez la recherche des chemins d'E/S de la LUN hôte pour restaurer tous les chemins vers les LUN.

Lien entre le site A et le médiateur vers le bas et le site B vers le bas

Si vous utilisez SM-BC, vous risquez de perdre la connectivité entre le médiateur ONTAP ou vos clusters de peering. Vous pouvez diagnostiquer le problème en vérifiant la connexion, la disponibilité et l'état de consensus des différentes parties de la relation SM-BC, puis en revoyant fermement la connexion.

Que vérifier	Commande CLI	Indicateur
Médiateur du site A	`snapmirror mediator show`	L'état de la connexion sera `unreachable`
Connectivité du site B.	`cluster peer show`	Disponibilité `unavailable`
État du consensus du volume SM-BC	`volume show` *`volume_name`* `-fields smbc-consensus`	Le `sm-bc consensus` le champ va être lu `Awaiting-consensus`

Pour plus d'informations sur le diagnostic et la résolution de ce problème, reportez-vous à l'article de la base de connaissances "Lien entre le site A et le médiateur vers le bas et le site B vers le bas lors de l'utilisation de SM-BC".

La suppression de SnapMirror SM-BC échoue lorsque la clôture est définie sur le volume de destination

Problème :

L'opération de suppression de SnapMirror échoue lorsque l'un des volumes de destination a une barrière de redirection définie.

Solution

Effectuer les opérations suivantes pour réessayer la redirection et supprimer la clôture du volume de destination.

- Resynchronisation de SnapMirror
- Mise à jour SnapMirror

Opération de déplacement de volume bloquée lorsque le volume principal est en baisse

Problème :

Une opération de déplacement de volume est bloquée indéfiniment dans un état de mise en service différé lorsque le site primaire n'est pas dans une relation SM-BC. Lorsque le site principal est en panne, le site secondaire effectue un basculement automatique non planifié (AUFO). Lorsqu'une opération de déplacement de volume est en cours lorsque l'AUFO est déclenché, le déplacement de volume devient bloqué.

Solution :

Interrompez l'instance de déplacement de volume bloquée et redémarrez l'opération de déplacement de volume.

Échec de la version de SnapMirror lorsqu'il est impossible de supprimer la copie Snapshot

Problème :

L'opération de version de SnapMirror échoue lorsque la copie Snapshot ne peut pas être supprimée.

Solution :

La copie Snapshot contient une balise transitoire. Utilisez le `snapshot delete` commande avec `-ignore -owners` Option pour supprimer la copie Snapshot transitoire.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Réessayez `snapmirror release` commande.

Le déplacement de volume la copie Snapshot de référence s'affiche comme la plus récente

Problème :

Après avoir effectué une opération de déplacement de volume sur un volume de groupe de cohérence, la copie Snapshot de référence du déplacement de volume peut s'afficher comme la plus récente dans la relation SnapMirror.

Vous pouvez afficher la dernière copie Snapshot avec la commande suivante :

```
snapmirror show -fields newest-snapshot status -expand
```

Solution :

Effectuez manuellement une opération `snapmirror resync` ou attendez la resynchronisation automatique suivante une fois l'opération de déplacement du volume terminée.

Service médiateur pour MetroCluster et SnapMirror Business Continuity

Présentation du médiateur ONTAP

Le Mediator ONTAP offre plusieurs fonctions pour les fonctionnalités ONTAP :

- Magasin persistant et cloisonné pour les métadonnées haute disponibilité.
- Sert de proxy ping pour la vivacité du contrôleur.
- Fournit une fonctionnalité de requête d'intégrité de nœud synchrone pour aider à déterminer le quorum.

Le médiateur ONTAP fournit deux services systemctl supplémentaires :

- **`ontap_mediator.service`**

  Gère le serveur API REST pour la gestion des relations ONAP.

- **`mediator-scst.service`**

  Contrôle le démarrage et l'arrêt du module iSCSI (SCST).

Outils fournis à l'administrateur système

Outils fournis à l'administrateur système :

- **`/usr/local/bin/mediator_change_password`**

  Définit un nouveau mot de passe d'API lorsque le nom d'utilisateur et le mot de passe d'API actuels sont fournis.

- **`/usr/local/bin/mediator_change_user`**

  Définit un nouveau nom d'utilisateur d'API lorsque le nom d'utilisateur et le mot de passe d'API actuels sont fournis.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Génère un fichier tgz local contenant toutes les informations de support utiles qui sont nécessaires à la communication avec le support client NetApp. Cela inclut la configuration de l'application, les journaux et certaines informations système. Les bundles sont générés sur le disque local et peuvent être transférés manuellement, si nécessaire. Emplacement de stockage : /opt/netapp/data/support_bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Supprime le progiciel ONTAP Mediator et le module du noyau SCST. Cela inclut la configuration, les journaux et les données de boîte aux lettres.

- **`/usr/local/bin/mediator_unlock_user`**

  Libère un verrouillage sur le compte utilisateur de l'API si la limite de tentatives d'authentification a été atteinte. Cette fonction est utilisée pour empêcher la dérivation de mot de passe par force brute. Il invite l'utilisateur à entrer le nom d'utilisateur et le mot de passe corrects.

- **`/usr/local/bin/mediator_add_user`**

  (Support uniquement) utilisé pour ajouter l'utilisateur de l'API lors de l'installation.

Notes spéciales

ONTAP Mediator s'appuie sur SCST pour fournir iSCSI (voir http://scst.sourceforge.net/index.html). Ce paquet est un module de noyau qui est compilé lors de l'installation spécifiquement pour le noyau. Toute mise à jour du noyau peut nécessiter la réinstallation de SCST. Vous pouvez également désinstaller puis réinstaller le médiateur ONTAP, puis reconfigurer la relation ONTAP.

> Toute mise à jour du noyau du système d'exploitation du serveur doit être coordonnée avec une fenêtre de maintenance dans ONTAP.

Nouveautés du médiateur ONTAP

De nouvelles améliorations du médiateur ONTAP sont fournies avec chaque version. Voici les nouveautés.

Améliorations

Version du médiateur ONTAP	Améliorations
1.7	• Prise en charge de RHEL 8.5, 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2 et 9.3 • Prise en charge de Rocky Linux 8 et 9
1.6	• Mises à jour Python 3.9. • Prise en charge de RHEL 8.4-8.8, 9.0-9.2, Rocky Linux 8 et 9. • Support interrompu pour RHEL 7.x/CentOS toutes les versions.
1.5	• Optimise la vitesse pour les systèmes SMBC à plus grande échelle. • Signature de code cryptographique ajoutée au programme d'installation. • Inclut des avertissements de dérécupération pour RHEL 7.x / CentOS 7.x.
1.4	• Prise en charge de RHEL 8.4 et 8.5. • Inclut SCST version 3.6.0. • Ajout de la prise en charge de Secure Boot (SB) du micrologiciel basé sur UFEI.
1.3	• Prise en charge de RHEL/CentOS 8.2 et 8.3. • Inclut SCST version 3.5.0.
1.2	• Prise en charge des boîtes aux lettres HTTPS. • A utiliser avec ONTAP 9.8+ MCC-IP AUSO et SM-BC ZRTO. • Inclut SCST version 3.4.0.

1.1	• Prise en charge de RHEL/CentOS 7.6, 7.7, 8.0 et 8.1. • Élimine les dépendances Perl. • Inclut SCST version 3.4.0.
1.0	• Prise en charge des boîtes aux lettres iSCSI. • A utiliser avec ONTAP 9.7+ MCC-IP AUSO. • Prise en charge de RHEL/CentOS 7.6.

Matrice de prise en charge du se

Système d'exploitation pour le médiateur ONTAP	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
7.6	Obsolète	Obsolète	Oui.	Oui.	Oui.	Oui.	Oui.	Oui (RHEL uniquement)
7.7	Obsolète	Obsolète	Oui.	Oui.	Oui.	Oui.	Non	Non
7.8	Obsolète	Obsolète	Oui.	Oui.	Oui.	Oui.	Non	Non
7.9	Obsolète	Obsolète	Oui.	Oui.	Oui.	Implicite	Non	Non
RHEL 8.0	Obsolète	Obsolète	Oui.	Oui.	Oui.	Oui.	Oui.	Non
RHEL 8.1	Obsolète	Obsolète	Oui.	Oui.	Oui.	Oui.	Non	Non
RHEL 8.2	Obsolète	Obsolète	Oui.	Oui.	Oui.	Non	Non	Non
RHEL 8.3	Obsolète	Obsolète	Oui.	Oui.	Oui.	Non	Non	Non
RHEL 8.4	Obsolète	Oui.	Oui.	Oui.	Non	Non	Non	Non
RHEL 8.5	Oui.	Oui.	Oui.	Oui.	Non	Non	Non	Non
RHEL 8.6	Oui.	Oui.	Non	Non	Non	Non	Non	Non
RHEL 8.7	Oui.	Oui.	Non	Non	Non	Non	Non	Non
RHEL 8.8	Oui.	Oui.	Non	Non	Non	Non	Non	Non
RHEL 9.0	Oui.	Oui.	Non	Non	Non	Non	Non	Non

RHEL 9.1	Oui.	Oui.	Non	Non	Non	Non	Non	Non
RHEL 9.2	Oui.	Oui.	Non	Non	Non	Non	Non	Non
RHEL 9.3	Oui.	Non	Non	Non	Non	Non	Non	Non
CentOS 8 et flux	Non	Non	Non	Non	Non	S/O	S/O	S/O
Rocky Linux 8	Oui.	Oui.	S/O	S/O	S/O	S/O	S/O	S/O
Rocky Linux 9	Oui.	Oui.	S/O	S/O	S/O	S/O	S/O	S/O

- Sauf mention contraire, le système d'exploitation fait référence aux versions RedHat et CentOS.
- « Non » signifie que le système d'exploitation et le médiateur ONTAP ne sont pas compatibles.
- CentOS 8 a été retiré pour toutes les versions en raison de sa ramification. CentOS Stream a été considéré comme un OS cible de production non approprié. Aucun support n'est planifié.
- ONTAP Mediator 1.5 était la dernière version prise en charge pour les systèmes d'exploitation de succursale RHEL 7.x.
- ONTAP Mediator 1.6 ajoute la prise en charge de Rocky Linux 8 et 9.

Résolution des problèmes

Date de modification	Modifier l'ID	Description
10 janvier 2023	6567145	Les modifications suivantes ont été apportées : • Ajout de la prise en charge de systèmes d'exploitation supplémentaires pour ONTAP Mediator : RHEL 9.6, 8.7, 9.0 et 9.1. • Ajout de la nouvelle version 3.7.0 de SCST pour débloquer les problèmes liés aux nouveaux systèmes d'exploitation pris en charge. • Ajout de la prise en charge de Rocky Linux : Rocky 8 et 9.
24 janvier 2023	6621319	Bibliothèque SCST pré-installée autorisée pour les installations de Mediator ONTAP.
27 févr. 2023	6623764	Mises en œuvre des modifications pour toujours charger le module de noyau scst_Disk lorsque le service médiateur-scst redémarre. Ces modifications garantissent que le service sera toujours prêt à créer de nouvelles cibles iSCSI à l'aide de la logique standard.

28 févr. 2023	6625194	Ajout d'une nouvelle option au programme d'installation du médiateur ONTAP : `--skip-yum-dependencies`
24 mars 2023	6652840	Mise à jour du programme d'installation du Mediator ONTAP afin qu'il puisse réinstaller ou réparer l'installation du SCST.
27 mars 2023	6655179	Correction d'un problème d'analyse qui s'est produit lorsque la collection de packs de support avec un mot de passe complexe a été déclenchée.
28 mars 2023	6656739	Modification de la logique de comparaison SCST de sorte que soit installé la bonne version lorsque ONTAP Mediator est mis à niveau.

Installer ou mettre à niveau

Préparez l'installation ou la mise à niveau du service Mediator ONTAP

Pour installer le service ONTAP Mediator, vous devez vous assurer que toutes les conditions préalables sont remplies, récupérer le package d'installation et exécuter le programme d'installation sur l'hôte. Cette procédure est utilisée pour une installation ou une mise à niveau d'une installation existante.

Description de la tâche

- À partir de ONTAP 9.7, vous pouvez utiliser n'importe quelle version du Mediator ONTAP pour contrôler une configuration IP MetroCluster.
- À partir de ONTAP 9.8, vous pouvez utiliser n'importe quelle version du médiateur ONTAP pour surveiller une relation SM-BC.

Avant de commencer

Vous devez remplir les conditions suivantes.

Version du médiateur ONTAP	Versions Linux prises en charge
1.7	• Red Hat Enterprise Linux : 8.5, 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2 et 9.3 • Rocky Linux 8 et 9
1.6	• Red Hat Enterprise Linux : 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2 • Rocky Linux 8 et 9
1.5	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.4	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9

1.3	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux : 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

La version du noyau doit correspondre à la version du système d'exploitation.

- installation physique 64 bits ou machine virtuelle
- 8 GO DE RAM
- 1 Go d'espace disque (utilisé pour l'installation des applications, les journaux du serveur et la base de données)
- Utilisateur : accès racine

Tous les packages de bibliothèque, à l'exception du noyau, peuvent être mis à jour en toute sécurité, mais ils peuvent nécessiter un redémarrage pour prendre effet dans l'application ONTAP Mediator. Une fenêtre de service est recommandée lorsqu'un redémarrage est nécessaire.

Si vous installez le `yum-utils` vous pouvez utiliser le `needs-restarting` commande.

Le noyau du noyau peut être mis à jour s'il est mis à jour vers une version qui est toujours prise en charge par la matrice de version du médiateur ONTAP. Un redémarrage est obligatoire, une fenêtre de maintenance est donc nécessaire.

Le module du noyau SCST doit être désinstallé avant le redémarrage, puis réinstallé après le redémarrage.

La mise à niveau vers un noyau au-delà de la version du système d'exploitation prise en charge pour la version spécifique du logiciel ONTAP Mediator n'est pas prise en charge. (Cela indique probablement que le module SCST testé ne se compile pas).

Enregistrez une clé de sécurité lorsque le démarrage sécurisé UEFI est activé

Si le démarrage sécurisé UEFI est activé, pour installer le médiateur ONTAP, vous devez enregistrer une clé de sécurité avant de pouvoir démarrer le service du médiateur ONTAP. Pour déterminer si le système est activé pour UEFI et si l'amorçage sécurisé est activé, effectuez les opérations suivantes :

Étapes

1. Si mokutil n'est pas installé, exécutez la commande suivante :

   ```
   yum install mokutil
   ```

2. Pour déterminer si le démarrage sécurisé UEFI est activé sur votre système, exécutez la commande suivante :

   ```
   mokutil --sb-state
   ```

   Les résultats indiquent si le démarrage sécurisé UEFI est activé sur ce système.

   ONTAP Mediator 1.2.0 et les versions précédentes ne prennent pas en charge ce mode.

Désactivez le démarrage sécurisé UEFI

Vous pouvez également choisir de désactiver le démarrage sécurisé UEFI avant d'installer le médiateur ONTAP.

Étapes

1. Dans les paramètres du BIOS de la machine physique, désactivez l'option « démarrage sécurisé UEFI ».
2. Dans les paramètres VMware de la machine virtuelle, désactivez l'option « démarrage sécurisé » pour vSphere 6.x ou l'option « démarrage sécurisé » pour vSphere 7.x.

Mettez à niveau le système d'exploitation hôte, puis le médiateur ONTAP

Pour mettre à niveau le système d'exploitation hôte pour ONTAP Mediator vers une version ultérieure, vous devez d'abord désinstaller ONTAP Mediator.

Avant de commencer

Les meilleures pratiques d'installation de Red Hat Enterprise Linux ou Rocky Linux et des référentiels associés sur votre système sont répertoriées ci-dessous. Les systèmes installés ou configurés différemment peuvent nécessiter des étapes supplémentaires.

- Vous devez installer Red Hat Enterprise Linux ou Rocky Linux conformément aux meilleures pratiques de Red Hat. En raison de la fin de vie des versions CentOS 8.x, les versions compatibles de CentOS 8.x ne sont pas recommandées.
- Lors de l'installation du service ONTAP Mediator sur Red Hat Enterprise Linux ou Rocky Linux, le système doit avoir accès au référentiel approprié pour que le programme d'installation puisse accéder à toutes les dépendances logicielles requises et les installer.
- Pour que le programme d'installation de yum trouve des logiciels dépendants dans les référentiels Red Hat Enterprise Linux, vous devez avoir enregistré le système pendant l'installation de Red Hat Enterprise Linux ou ultérieurement en utilisant un abonnement Red Hat valide.

  Pour plus d'informations sur le Gestionnaire d'abonnement Red Hat, reportez-vous à la documentation Red Hat.

- Les ports suivants doivent être inutilisés et disponibles pour le médiateur :
  - 31784
  - 3260
- Si vous utilisez un pare-feu tiers : reportez-vous à la "Exigences relatives au pare-feu pour le médiateur ONTAP"
- Si l'hôte Linux se trouve dans un emplacement sans accès à Internet, vous devez vous assurer que les packages requis sont disponibles dans un référentiel local.

  Si vous utilisez le protocole LACP (Link Aggregation Control Protocol) dans un environnement Linux, vous devez configurer correctement le noyau et vous assurer que le `sysctl net.ipv4.conf.all.arp_ignore` est réglé sur « 2 ».

Ce dont vous avez besoin

Les packages suivants sont requis par le service ONTAP Mediator :

Toutes les versions de RHEL/CentOS	Packages supplémentaires pour RHEL 8.x / Rocky Linux 8	Packages supplémentaires pour RHEL 9.x / Rocky Linux 9

• openssl • openssl-devel • kernel-devel-$ (nom_uname -r) • gcc • marque • libselinux-utils • correctif • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeMaker • efibootmgr • mokutil	• python3-pip • elfutils-libelf-devel • politiqueutils-python-utils • red hat-lsb-core • python39 • python39-devel	• python3-pip • elfutils-libelf-devel • politiqueutils-python-utils • python3 • python3-devel

Le package d'installation Mediator est un fichier tar compressé auto-extractible qui comprend :

- Un fichier RPM contenant toutes les dépendances qui ne peuvent pas être obtenues du référentiel de la version prise en charge.
- Un script d'installation.

Une certification SSL valide est recommandée.

Description de la tâche

Lorsque vous mettez à niveau le système d'exploitation hôte pour ONTAP Mediator vers une version majeure ultérieure (par exemple, de 7.x à 8.x) à l'aide de l'outil de mise à niveau leapp, Vous devez désinstaller ONTAP Mediator car l'outil tente de détecter les nouvelles versions de tous les RPM installés dans les référentiels enregistrés avec le système.

Comme un fichier .rpm a été installé dans le cadre du programme d'installation de ONTAP Mediator, il est inclus dans cette recherche. Cependant, comme ce fichier .rpm a été décompressé dans le cadre du programme d'installation et n'a pas été téléchargé à partir d'un référentiel enregistré, une mise à niveau est introuvable. Dans ce cas, l'outil de mise à niveau leapp désinstalle le package.

Afin de conserver les fichiers journaux, qui seront utilisés pour trier les dossiers de support, vous devez sauvegarder les fichiers avant de procéder à une mise à niveau du système d'exploitation et les restaurer après une réinstallation du progiciel ONTAP Mediator. Étant donné que le médiateur ONTAP est en cours de réinstallation, tous les clusters ONTAP qui y sont connectés devront être reconnectés après la nouvelle installation.

> Les étapes suivantes doivent être effectuées dans l'ordre. Immédiatement après la réinstallation du médiateur ONTAP, vous devez arrêter le service ontap_médiateur, remplacer les fichiers journaux et redémarrer le service. Cela permet de s'assurer que les journaux ne seront pas perdus.

Étapes

1. Sauvegardez les fichiers journaux.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Effectuez une mise à niveau avec l'outil de mise à niveau leapp.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Réinstallez le médiateur ONTAP.

> Effectuez le reste des étapes immédiatement après la réinstallation du médiateur ONTAP pour éviter la perte des fichiers journaux.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Arrêtez le service ontap_médiateur.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Remplacez les fichiers journaux.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Démarrez le service ontap_médiateur.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Reconnectez tous les clusters ONTAP au médiateur ONTAP mis à niveau

Procédure pour MetroCluster sur IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

Procédure de continuité de l'activité SnapMirror

Pour SnapMirror Business Continuity, si vous avez installé votre certificat TLS en dehors du répertoire /opt/netapp, vous n'aurez pas besoin de le réinstaller. Si vous utilisiez le certificat auto-signé généré par défaut ou si vous placez votre certificat personnalisé dans le répertoire /opt/netapp, vous devez le sauvegarder et le restaurer.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
future reference.
```

```
The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237
-peer-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true
```

```
peer1::>
```

Autoriser l’accès aux référentiels

Vous devez activer l’accès aux référentiels pour que le médiateur ONTAP puisse accéder aux packages requis pendant le processus d’installation

Étapes

1. Déterminez les référentiels à accéder, comme indiqué dans le tableau suivant :

Si votre système d’exploitation est…	Vous devez donner l’accès à ces référentiels…
RHEL 7.x	• rhel-7-server-optional-rms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
CentOS 7.x	• C7.6.1810 - référentiel de base
Rocky Linux 8	• appstream • bases
Rocky Linux 9	• appstream • bases

2. Utilisez l’une des procédures suivantes pour activer l’accès aux référentiels répertoriés ci-dessus afin que ONTAP Mediator puisse accéder aux packages requis pendant le processus d’installation.

Procédure pour le système d'exploitation RHEL 7.x.

Utilisez cette procédure si votre système d'exploitation est **RHEL 7.x** pour activer l'accès aux référentiels :

Étapes

1. Abonnez-vous au référentiel requis :

   ```
   subscription-manager repos --enable rhel-7-server-optional-rpms
   ```

   L'exemple suivant montre l'exécution de cette commande :

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-7-
   server-optional-rpms
   Repository 'rhel-7-server-optional-rpms' is enabled for this system.
   ```

2. Exécutez le `yum repolist` commande.

   L'exemple suivant montre l'exécution de cette commande. Le référentiel "rhel-7-Server-optional-rpms" devrait apparaître dans la liste.

   ```
   [root@localhost ~]# yum repolist
   Loaded plugins: product-id, search-disabled-repos, subscription-
   manager
   rhel-7-server-optional-rpms | 3.2 kB  00:00:00
   rhel-7-server-rpms | 3.5 kB  00:00:00
   (1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
   |  26 kB  00:00:00
   (2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
   | 2.5 MB  00:00:00
   (3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
   | 8.3 MB  00:00:01
   repo id                                       repo name
   status
   rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
   Linux 7 Server - Optional (RPMs)   19,447
   rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
   Linux 7 Server (RPMs)              26,758
   repolist: 46,205
   [root@localhost ~]#
   ```

Procédure pour le système d'exploitation RHEL 8.x.

Utilisez cette procédure si votre système d'exploitation est **RHEL 8.x** pour activer l'accès aux référentiels :

Étapes

1. Abonnez-vous au référentiel requis :

   `subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms`

   L'exemple suivant montre l'exécution de cette commande :

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-baseos-rpms
   Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-appstream-rpms
   Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Exécutez le `yum repolist` commande.

   Les nouveaux référentiels auxquels vous êtes abonné doivent apparaître dans la liste.

Procédure pour le système d'exploitation RHEL 9.x.

Utilisez cette procédure si votre système d'exploitation est **RHEL 9.x** pour activer l'accès aux référentiels :

Étapes

1. Abonnez-vous au référentiel requis :

   `subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms`

   L'exemple suivant montre l'exécution de cette commande :

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-baseos-rpms
   Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-appstream-rpms
   Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Exécutez le `yum repolist` commande.

   Les nouveaux référentiels auxquels vous êtes abonné doivent apparaître dans la liste.

Procédure pour le système d'exploitation CentOS 7.x.

Utilisez cette procédure si votre système d'exploitation est **CentOS 7.x** pour activer l'accès aux référentiels :

> Les exemples suivants montrent un référentiel pour CentOS 7.6 et peuvent ne pas fonctionner pour d'autres versions de CentOS. Utilisez le référentiel de base pour votre version de CentOS.

Étapes

1. Ajoutez le référentiel C7.6.1810 - base. Le référentiel de coffre-fort C7.6.1810 - base contient le paquet "kernel-devel" nécessaire pour le Mediator ONTAP.
2. Ajoutez les lignes suivantes à /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Exécutez le `yum repolist` commande.

   L'exemple suivant montre l'exécution de cette commande. Le référentiel CentOS-7.6.1810 - base doit apparaître dans la liste.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                  | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz           | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db         | 6.0 MB  00:00:04
repo id                      repo name                 status
C7.6.1810-base/x86_64        CentOS-7.6.1810 - Base    10,019
base/7/x86_64                CentOS-7 - Base           10,097
extras/7/x86_64              CentOS-7 - Extras         307
updates/7/x86_64             CentOS-7 - Updates        1,010
repolist: 21,433
[root@localhost ~]#
```

Procédure pour les systèmes d'exploitation Rocky Linux 8 ou 9

Utilisez cette procédure si votre système d'exploitation est **Rocky Linux 8** ou **Rocky Linux 9** pour permettre l'accès aux référentiels :

Étapes

1. Abonnez-vous aux référentiels requis :

   ```
   dnf config-manager --set-enabled baseos

   dnf config-manager --set-enabled appstream
   ```

2. Exécutez un `clean` fonctionnement :

   ```
   dnf clean all
   ```

3. Vérifiez la liste des référentiels :

   ```
   dnf repolist
   ```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

Téléchargez le package d'installation du Mediator

Téléchargez le package d'installation Mediator dans le cadre du processus d'installation.

Étapes

1. Téléchargez le progiciel d'installation du médiateur à partir de la page ONTAP Mediator.

   "Page de téléchargement du médiateur ONTAP"

2. Vérifiez que le package d'installation du Mediator se trouve dans le répertoire de travail actuel :

   `ls`

   ```
   [root@mediator-host ~]#ls
   ontap-mediator-1.7.0.tgz
   ```

   > Pour ONTAP Mediator versions 1.4 et antérieures, le programme d'installation est nommé `ontap-mediator`.

   Si vous êtes à un endroit sans accès à Internet, vous devez vous assurer que le programme d'installation a accès aux packages requis.

3. Si nécessaire, déplacez le package d'installation du Mediator du répertoire de téléchargement vers le répertoire d'installation de l'hôte Linux Mediator.
4. Décompressez le programme d'installation :

   `tar xvfz ontap-mediator-1.7.0.tgz`

   ```
   [root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
   ontap-mediator-1.7.0/
   ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
   ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/ontap-mediator-1.7.0
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
   ```

Vérifiez la signature du code du médiateur ONTAP

Vous devez vérifier la signature de code du médiateur ONTAP avant d'installer le progiciel d'installation du médiateur.

Avant de commencer

Avant de vérifier la signature du code du médiateur, votre système doit répondre aux exigences suivantes.

- openssl versions 1.0.2 à 3.0 pour la vérification de base
- openssl version 1.1.0 ou ultérieure pour les opérations TSA (Time Stamping Authority)
- Accès public Internet pour vérification OCSP

Le pack de téléchargement contient les fichiers suivants :

Fichier	Description
`ONTAP-Mediator-development.pub`	Clé publique utilisée pour vérifier la signature
`csc-prod-chain-ONTAP-Mediator.pem`	La chaîne de confiance de l'autorité de certification publique
`csc-prod-ONTAP-Mediator.pem`	Certificat utilisé pour générer la clé
`ontap-mediator-1.7.0`	Exécutable d'installation du produit pour la version 1.7.0
`ontap-mediator-1.7.0.sig`	Le SHA-256 a été écrasé, puis signé par RSA à l'aide de la clé csc-prod, signature de l'installateur
`ontap-mediator-1.7.0.sig.tsr`	La demande de révocation que OCSCP doit utiliser pour la signature de l'installateur
`tsa-prod-ONTAP-Mediator.pem`	Le certificat public pour le TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	La chaîne CA du certificat public pour le TSR

Étapes

1. Effectuez la vérification de révocation sur `csc-prod-ONTAP-Mediator.pem` Via le protocole OCSP (Online Certificate Status Protocol).
   a. Recherchez l'URL OCSP utilisée pour enregistrer le certificat car les certificats de développeur ne fournissent pas nécessairement d'uri.

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. Générez une demande OCSP pour le certificat.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. Connectez-vous au OCSP Manager pour envoyer la demande OCSP :

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. Vérifiez la chaîne de confiance du CSC et sa date d'expiration par rapport à l'hôte local :

   `openssl verify`

   > Le `openssl` La version du CHEMIN d'ACCÈS doit être valide `cert.pem` (pas auto-signé).

   ```
   openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
   Signature-Check certificate has expired or is invalid. Download a newer
   version of the ONTAP Mediator.
   openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
   Stamp certificate has expired or is invalid. Download a newer version of
   the ONTAP Mediator.
   ```

3. Vérifiez le `ontap-mediator-1.6.0.sig.tsr` et `ontap-mediator-1.7.0.tsr` fichiers utilisant les certificats associés :

   `openssl ts -verify`

   > `.tsr` les fichiers contiennent la réponse de l'horodatage associée au programme d'installation et à la signature du code. Le traitement confirme que l'horodatage a une signature valide de TSA et que votre fichier d'entrée n'a pas changé.
   > La vérification est effectuée localement sur votre machine. De façon indépendante, il n'est pas nécessaire d'accéder aux serveurs TSA.

   ```
   openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
   1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
   prod-ONTAP-Mediator.pem
   openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
   1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
   ONTAP-Mediator.pem
   ```

4. Vérifiez les signatures par rapport à la clé :

   `openssl -dgst -verify`

   ```
   openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
   ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
   ```

Exemple de vérification de la signature de code du médiateur ONTAP (sortie de console)

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#
```

Installez le package d'installation du Mediator ONTAP

Pour installer le service ONTAP Mediator, vous devez obtenir le package d'installation et exécuter le programme d'installation sur l'hôte.

Étapes

1. Exécutez le programme d'installation et répondez aux invites si nécessaire :

   `./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y`

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
   ```

   Le processus d'installation permet de créer les comptes requis et d'installer les packages requis. Si une version antérieure de Mediator est installée sur l'hôte, vous serez invité à confirmer la mise à niveau.

2. À partir de ONTAP Mediator 1.4, le mécanisme de démarrage sécurisé est activé sur les systèmes UEFI. Lorsque le démarrage sécurisé est activé, vous devez suivre les étapes supplémentaires pour enregistrer la clé de sécurité après l'installation :

   - Suivez les instructions du fichier README pour signer le module de noyau SCST. :

     `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

   - Repérez les touches requises :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

Une fois l’installation terminée, les fichiers README et l’emplacement des clés sont également fournis dans la sortie du système.

Exemple d'installation du Mediator 1.6 de ONTAP (sortie console)

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
ONTAP Mediator: Self Extracting Installer


+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode


+ Checking for default Linux firewall
success
success
success


################################################################
Preparing for installation of ONTAP Mediator packages.


+ Installing required packages.


Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

```
Package python3-pip-9.0.3-19.el8.noarch is already installed.
Package policycoreutils-python-utils-2.9-14.el8.noarch is already
installed.
Dependencies resolved.
=========================================================================
=========================================================================
========================================
 Package                                        Architecture
Version                                                   Repository
Size
=========================================================================
=========================================================================
========================================
Installing:
 bzip2                                          x86_64
1.0.6-26.el8                                              rhel-8-for-
x86_64-baseos-rpms                       60 k
 elfutils-libelf-devel                          x86_64
0.186-1.el8                                               rhel-8-for-
x86_64-baseos-rpms                       60 k
 kernel-devel                                   x86_64
4.18.0-348.el8                                            rhel-8-for-
x86_64-baseos-rpms                       20 M
 make                                           x86_64
1:4.2.1-11.el8                                            rhel-8-for-
x86_64-baseos-rpms                      498 k
 openssl-devel                                  x86_64
1:1.1.1k-7.el8_6                                          rhel-8-for-
x86_64-baseos-rpms                      2.3 M
 patch                                          x86_64
2.7.6-11.el8                                              rhel-8-for-
x86_64-baseos-rpms                      138 k
 perl-ExtUtils-MakeMaker                        noarch
1:7.34-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                   301 k
 python36-devel                                 x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                    rhel-8-for-
x86_64-appstream-rpms                    17 k
 redhat-lsb-core                                x86_64
4.1-47.el8                                                rhel-8-for-
x86_64-appstream-rpms                    45 k
Upgrading:
 cpp                                            x86_64
8.5.0-10.1.el8_6                                          rhel-8-for-
x86_64-appstream-rpms                    10 M
 elfutils-libelf                                x86_64
```

```
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      229 k
 elfutils-libs                                  x86_64
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      295 k
 gcc                                            x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-appstream-rpms                    23 M
 libgcc                                         x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                       80 k
 libgomp                                        x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      207 k
 libsemanage                                    x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      168 k
 mokutil                                        x86_64
1:0.3.0-11.el8_6.1                                          rhel-8-for-
x86_64-baseos-rpms                       46 k
 openssl                                        x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      709 k
 openssl-libs                                   x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      1.5 M
 platform-python-pip                            noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-baseos-rpms                      1.6 M
 policycoreutils                                x86_64
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      374 k
 policycoreutils-python-utils                   noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      253 k
 python3-libsemanage                            x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      128 k
 python3-pip                                    noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-appstream-rpms                    20 k
 python3-policycoreutils                        noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      2.2 M
 python36                                       x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                      rhel-8-for-
```

```
x86_64-appstream-rpms                    19 k
Installing dependencies:
 annobin                                         x86_64
10.29-3.el8                                               rhel-8-for-
x86_64-appstream-rpms                   117 k
 at                                              x86_64
3.1.20-11.el8                                             rhel-8-for-
x86_64-baseos-rpms                       81 k
 bc                                              x86_64
1.07.1-5.el8                                              rhel-8-for-
x86_64-baseos-rpms                      129 k
 cups-client                                     x86_64
1:2.2.6-38.el8                                            rhel-8-for-
x86_64-appstream-rpms                   169 k
 dwz                                             x86_64
0.12-10.el8                                               rhel-8-for-
x86_64-appstream-rpms                   109 k
 ed                                              x86_64
1.14.2-4.el8                                              rhel-8-for-
x86_64-baseos-rpms                       82 k
 efi-srpm-macros                                 noarch
3-3.el8                                                   rhel-8-for-
x86_64-appstream-rpms                    22 k
 esmtp                                           x86_64
1.2-15.el8                                                EPEL-8
57 k
 ghc-srpm-macros                                 noarch
1.4.2-7.el8                                               rhel-8-for-
x86_64-appstream-rpms                   9.4 k
 go-srpm-macros                                  noarch
2-17.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    13 k
 keyutils-libs-devel                             x86_64
1.5.10-6.el8                                              rhel-8-for-
x86_64-baseos-rpms                       48 k
 krb5-devel                                      x86_64
1.18.2-14.el8                                             rhel-8-for-
x86_64-baseos-rpms                      560 k
 libcom_err-devel                                x86_64
1.45.6-2.el8                                              rhel-8-for-
x86_64-baseos-rpms                       38 k
 libesmtp                                        x86_64
1.0.6-18.el8                                              EPEL-8
70 k
 libkadm5                                        x86_64
1.18.2-14.el8                                             rhel-8-for-
```

```
x86_64-baseos-rpms                      187 k
 liblockfile                                    x86_64
1.14-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                    32 k
 libselinux-devel                               x86_64
2.9-5.el8                                               rhel-8-for-
x86_64-baseos-rpms                      200 k
 libsepol-devel                                 x86_64
2.9-3.el8                                               rhel-8-for-
x86_64-baseos-rpms                       87 k
 libverto-devel                                 x86_64
0.3.0-5.el8                                             rhel-8-for-
x86_64-baseos-rpms                       18 k
 m4                                             x86_64
1.4.18-7.el8                                            rhel-8-for-
x86_64-baseos-rpms                      223 k
 mailx                                          x86_64
12.5-29.el8                                             rhel-8-for-
x86_64-baseos-rpms                      257 k
 ncurses-compat-libs                            x86_64
6.1-9.20180224.el8                                      rhel-8-for-
x86_64-baseos-rpms                      328 k
 ocaml-srpm-macros                              noarch
5-4.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   9.5 k
 openblas-srpm-macros                           noarch
2-2.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   8.0 k
 pcre2-devel                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      605 k
 pcre2-utf16                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      229 k
 pcre2-utf32                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      220 k
 perl-CPAN-Meta-YAML                            noarch
0.018-397.el8                                           rhel-8-for-
x86_64-appstream-rpms                    34 k
 perl-ExtUtils-Command                          noarch
1:7.34-1.el8                                            rhel-8-for-
x86_64-appstream-rpms                    19 k
 perl-ExtUtils-Install                          noarch
2.14-4.el8                                              rhel-8-for-
x86_64-appstream-rpms                    46 k
```

```
 perl-ExtUtils-Manifest                          noarch
1.70-395.el8                                             rhel-8-for-
x86_64-appstream-rpms                    37 k
 perl-ExtUtils-ParseXS                           noarch
1:3.35-2.el8                                             rhel-8-for-
x86_64-appstream-rpms                    83 k
 perl-JSON-PP                                    noarch
1:2.97.001-3.el8                                         rhel-8-for-
x86_64-appstream-rpms                    68 k
 perl-Math-BigInt                                noarch
1:1.9998.11-7.el8                                        rhel-8-for-
x86_64-baseos-rpms                      196 k
 perl-Math-Complex                               noarch
1.59-421.el8                                             rhel-8-for-
x86_64-baseos-rpms                      109 k
 perl-Test-Harness                               noarch
1:3.42-1.el8                                             rhel-8-for-
x86_64-appstream-rpms                   279 k
 perl-devel                                      x86_64
4:5.26.3-419.el8_4.1                                     rhel-8-for-
x86_64-appstream-rpms                   599 k
 perl-srpm-macros                                noarch
1-25.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    11 k
 perl-version                                    x86_64
6:0.99.24-1.el8                                          rhel-8-for-
x86_64-appstream-rpms                    67 k
 platform-python-devel                           x86_64
3.6.8-41.el8                                             rhel-8-for-
x86_64-appstream-rpms                   249 k
 python-rpm-macros                               noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python-srpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python3-pyparsing                               noarch
2.1.10-7.el8                                             rhel-8-for-
x86_64-baseos-rpms                      142 k
 python3-rpm-generators                          noarch
5-7.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    25 k
 python3-rpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    14 k
 qt5-srpm-macros                                 noarch
```

```
5.15.2-1.el8                                                rhel-8-for-
x86_64-appstream-rpms                   11 k
 redhat-lsb-submod-security                     x86_64
4.1-47.el8                                                  rhel-8-for-
x86_64-appstream-rpms                   22 k
 redhat-rpm-config                              noarch
125-1.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   87 k
 rust-srpm-macros                               noarch
5-2.el8                                                     rhel-8-for-
x86_64-appstream-rpms                  9.3 k
 spax                                           x86_64
1.5.3-13.el8                                                rhel-8-for-
x86_64-baseos-rpms                    217 k
 systemtap-sdt-devel                            x86_64
4.6-4.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   86 k
 time                                           x86_64
1.9-3.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      54 k
 unzip                                          x86_64
6.0-46.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    196 k
 util-linux-user                                x86_64
2.32.1-28.el8                                               rhel-8-for-
x86_64-baseos-rpms                    100 k
 zip                                            x86_64
3.0-23.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    270 k
 zlib-devel                                     x86_64
1.2.11-17.el8                                               rhel-8-for-
x86_64-baseos-rpms                      58 k
Installing weak dependencies:
 perl-CPAN-Meta                                 noarch
2.150010-396.el8                                            rhel-8-for-
x86_64-appstream-rpms                   191 k
 perl-CPAN-Meta-Requirements                    noarch
2.140-396.el8                                               rhel-8-for-
x86_64-appstream-rpms                   37 k
 perl-Encode-Locale                             noarch
1.05-10.module+el8.3.0+6498+9eecfe51                        rhel-8-for-
x86_64-appstream-rpms                   22 k
 perl-Time-HiRes                                x86_64
4:1.9758-2.el8                                              rhel-8-for-
x86_64-appstream-rpms                   61 k
```

```
Transaction Summary
================================================================================
================================================================================
==========================================
Install  69 Packages
Upgrade  17 Packages

Total download size: 72 M
Is this ok [y/N]: y
Downloading Packages:
(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm
735 kB/s |  46 kB     00:00
(2/86): libesmtp-1.0.6-18.el8.x86_64.rpm
1.0 MB/s |  70 kB     00:00
(3/86): esmtp-1.2-15.el8.x86_64.rpm
747 kB/s |  57 kB     00:00
(4/86): rust-srpm-macros-5-2.el8.noarch.rpm
308 kB/s | 9.3 kB     00:00
(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm
781 kB/s |  37 kB     00:00
(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm
2.7 MB/s | 191 kB     00:00
(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm
214 kB/s | 9.5 kB     00:00
(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm
1.2 MB/s |  68 kB     00:00
(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm
5.8 MB/s | 301 kB     00:00
(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm
317 kB/s | 9.4 kB     00:00
(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm
4.5 MB/s | 279 kB     00:00
(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm
520 kB/s |  19 kB     00:00

...

15 MB/s | 1.5 MB     00:00
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------
Total
35 MB/s |  72 MB     00:02
Running transaction check
Transaction check succeeded.
Running transaction test
```

```
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
  Upgrading        : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Upgrading        : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Upgrading        : elfutils-libelf-0.186-1.el8.x86_64
3/103
  Installing       : perl-version-6:0.99.24-1.el8.x86_64
4/103
  Installing       : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
  Upgrading        : libsemanage-2.9-8.el8.x86_64
6/103
  Installing       : zlib-devel-1.2.11-17.el8.x86_64
7/103
  Installing       : python-srpm-macros-3-41.el8.noarch
8/103
  Installing       : python-rpm-macros-3-41.el8.noarch
9/103
  Installing       : python3-rpm-macros-3-41.el8.noarch
10/103
  Installing       : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
  Installing       : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
  Installing       : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
  Upgrading        : python3-libsemanage-2.9-8.el8.x86_64
14/103
  Upgrading        : policycoreutils-2.9-19.el8.x86_64
15/103
  Running scriptlet: policycoreutils-2.9-19.el8.x86_64
15/103
  Upgrading        : python3-policycoreutils-2.9-19.el8.noarch
16/103
  Installing       : dwz-0.12-10.el8.x86_64
17/103
```

```
  Installing       : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
  Installing       : libesmtp-1.0.6-18.el8.x86_64
19/103
  Installing       : mailx-12.5-29.el8.x86_64
20/103
  Installing       : libkadm5-1.18.2-14.el8.x86_64
21/103
  Upgrading        : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Upgrading        : platform-python-pip-9.0.3-22.el8.noarch
23/103
  Upgrading        : python3-pip-9.0.3-22.el8.noarch
24/103
  Upgrading        : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Upgrading        : cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Upgrading        : gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Installing       : annobin-10.29-3.el8.x86_64
28/103
  Installing       : unzip-6.0-46.el8.x86_64
29/103
  Installing       : zip-3.0-23.el8.x86_64
30/103
  Installing       : perl-Math-Complex-1.59-421.el8.noarch
31/103
  Installing       : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
  Installing       : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
  Installing       : make-1:4.2.1-11.el8.x86_64
34/103
  Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103
```

```
  Installing       : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
  Installing       : util-linux-user-2.32.1-28.el8.x86_64
36/103
  Installing       : libsepol-devel-2.9-3.el8.x86_64
37/103
  Installing       : pcre2-utf32-10.32-2.el8.x86_64
38/103
  Installing       : pcre2-utf16-10.32-2.el8.x86_64
39/103
  Installing       : pcre2-devel-10.32-2.el8.x86_64
40/103
  Installing       : libselinux-devel-2.9-5.el8.x86_64
41/103
  Installing       : patch-2.7.6-11.el8.x86_64
42/103
  Installing       : python3-pyparsing-2.1.10-7.el8.noarch
43/103
  Installing       : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
  Installing       : spax-1.5.3-13.el8.x86_64
45/103
  Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
  Installing       : m4-1.4.18-7.el8.x86_64
46/103
  Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
  Installing       : libverto-devel-0.3.0-5.el8.x86_64
47/103
  Installing       : bc-1.07.1-5.el8.x86_64
48/103
  Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
  Installing       : at-3.1.20-11.el8.x86_64
49/103
  Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
  Installing       : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
  Installing       : krb5-devel-1.18.2-14.el8.x86_64
51/103
  Installing       : time-1.9-3.el8.x86_64
52/103
  Running scriptlet: time-1.9-3.el8.x86_64
52/103
```

```
  Upgrading        : policycoreutils-python-utils-2.9-19.el8.noarch
80/103
  Installing       : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
  Upgrading        : elfutils-libs-0.186-1.el8.x86_64
82/103
  Upgrading        : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
  Upgrading        : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
  Installing       : kernel-devel-4.18.0-348.el8.x86_64
85/103
  Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

  ...

85/103
  Installing       : bzip2-1.0.6-26.el8.x86_64
86/103
  Cleanup          : policycoreutils-python-utils-2.9-14.el8.noarch
87/103
  Cleanup          : python3-policycoreutils-2.9-14.el8.noarch
88/103
  Cleanup          : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Cleanup          : elfutils-libs-0.185-1.el8.x86_64
90/103
  Cleanup          : openssl-1:1.1.1k-4.el8.x86_64
91/103
  Cleanup          : python3-libsemanage-2.9-6.el8.x86_64
92/103
  Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
  Cleanup          : gcc-8.4.1-1.el8.x86_64
93/103
  Running scriptlet: policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : mokutil-1:0.3.0-11.el8.x86_64
95/103
```

```
  Cleanup          : python3-pip-9.0.3-19.el8.noarch
96/103
  Cleanup          : platform-python-pip-9.0.3-19.el8.noarch
97/103
  Cleanup          : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Cleanup          : libsemanage-2.9-6.el8.x86_64
99/103
  Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : libgomp-8.4.1-1.el8.x86_64
102/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : elfutils-libelf-0.185-1.el8.x86_64
103/103
  Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
  Verifying        : esmtp-1.2-15.el8.x86_64
1/103
  Verifying        : libesmtp-1.0.6-18.el8.x86_64

  ...

Upgraded:
  cpp-8.5.0-10.1.el8_6.x86_64                              elfutils-
libelf-0.186-1.el8.x86_64     elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
  libgcc-8.5.0-10.1.el8_6.x86_64                           libgomp-
8.5.0-10.1.el8_6.x86_64        libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
  openssl-1:1.1.1k-7.el8_6.x86_64                          openssl-
libs-1:1.1.1k-7.el8_6.x86_64   platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
  policycoreutils-python-utils-2.9-19.el8.noarch           python3-
libsemanage-2.9-8.el8.x86_64   python3-pip-9.0.3-22.el8.noarch
```

```
python3-policycoreutils-2.9-19.el8.noarch
  python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
  annobin-10.29-3.el8.x86_64                                          at-
3.1.20-11.el8.x86_64                              bc-1.07.1-5.el8.x86_64
  bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64                   dwz-0.12-
10.el8.x86_64
  ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch                      elfutils-libelf-
devel-0.186-1.el8.x86_64
  esmtp-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch                  go-srpm-macros-2-
17.el8.noarch
  kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64             krb5-devel-1.18.2-
14.el8.x86_64
  libcom_err-devel-1.45.6-2.el8.x86_64
libesmtp-1.0.6-18.el8.x86_64                        libkadm5-1.18.2-
14.el8.x86_64
  liblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64                   libsepol-devel-2.9-
3.el8.x86_64
  libverto-devel-0.3.0-5.el8.x86_64                                   m4-
1.4.18-7.el8.x86_64                               mailx-12.5-
29.el8.x86_64
  make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64       ocaml-srpm-macros-
5-4.el8.noarch
  openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64               patch-2.7.6-
11.el8.x86_64
  pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64                      pcre2-utf32-10.32-
2.el8.x86_64
  perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch    perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
  perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch           perl-ExtUtils-
Install-2.14-4.el8.noarch
  perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch          perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
  perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch           perl-Math-Complex-
```

```
1.59-421.el8.noarch
  perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64               perl-devel-
4:5.26.3-419.el8_4.1.x86_64
  perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64                 platform-python-
devel-3.6.8-41.el8.x86_64
  python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch                  python3-pyparsing-
2.1.10-7.el8.noarch
  python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch                  python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
  qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64                   redhat-lsb-submod-
security-4.1-47.el8.x86_64
  redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch                     spax-1.5.3-
13.el8.x86_64
  systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64                               unzip-6.0-
46.el8.x86_64
  util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64                               zlib-devel-1.2.11-
17.el8.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /tmp/ontap_mediator.JixKGP/ontap-
mediator-1.6.0/ontap-mediator-1.6.0/install_20221021155929.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20221021155929.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that reboot will be
```

```
needed.
     SCST will not start automatically when Secure Boot is enabled and
not configured properly.
+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@scs000099753 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.5 (Ootpa)
[root@scs000099753 ~]#
```

Vérifiez l'installation

Une fois le médiateur ONTAP installé, vous devez vérifier que les services du médiateur ONTAP sont en cours d'exécution.

Étapes

1. Afficher l'état des services du médiateur ONTAP :
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Vérifiez les ports utilisés par le service ONTAP Mediator :

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Configuration post-installation

Une fois le service ONTAP Mediator installé et en cours d'exécution, des tâches de configuration supplémentaires doivent être effectuées dans le système de stockage ONTAP pour utiliser les fonctions du Mediator :

- Pour utiliser le service médiateur ONTAP dans une configuration IP MetroCluster, reportez-vous à la section "Configuration du service médiateur ONTAP à partir d'une configuration IP MetroCluster".
- Pour utiliser SnapMirror Business Continuity, voir "Installez le service médiateur ONTAP et confirmez la configuration du cluster ONTAP".

Configurer les stratégies de sécurité du médiateur ONTAP

Le serveur ONTAP Mediator prend en charge plusieurs paramètres de sécurité configurables. Les valeurs par défaut pour tous les paramètres sont fournies dans un fichier basse_space_Threshold_mib: 10read-only :

`/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Toutes les valeurs placées dans le `ontap_mediator.user_config.yaml` Remplace les valeurs par défaut et sera conservé dans toutes les mises à niveau du Mediator ONTAP.

Après modification `ontap_mediator.user_config.yaml`, Redémarrez le service ONTAP Mediator :

```
systemctl restart ontap_mediator
```

Modifier les attributs du médiateur ONTAP

Les attributs suivants peuvent être configurés :

> Autres valeurs par défaut dans `ontap_mediator.config.yaml` ne doit pas être modifié.

- **Paramètres utilisés pour installer des certificats SSL tiers en remplacement des certificats auto-signés par défaut**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095'                  # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap'            # passphrase for the signed
client cert
```

- **Paramètres qui fournissent des protections contre les attaques de devinettes de mots de passe par force brute**

  Pour activer la fonction, définissez une valeur pour `window_seconds` et le `retry_limit`

  Exemples :

  - Fournissez une fenêtre de 5 minutes pour les hypothèses, puis réinitialisez le compte à zéro échec :

    `authentication_lock_window_seconds: 300`

  - Verrouiller le compte si cinq défaillances se produisent dans la période de la fenêtre :

    `authentication_retry_limit: 5`

  - Réduisez l'impact des attaques par tâtonnements de mots de passe par force brute en définissant un

délai qui se produit avant le rejet de chaque tentative, ce qui ralentit les attaques.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to
allow before locking API access, null = unlimited
```

- **Champs qui contrôlent les règles de complexité du mot de passe du compte utilisateur de l'API ONTAP Mediator**

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

- **Paramètre qui contrôle l'espace libre requis sur le `/opt/netapp/lib/ontap_mediator` disque.**

  Si l'espace est inférieur au seuil défini, le service émet un avertissement.

```
low_space_threshold_mib: 10
```

- **Paramètre qui contrôle RESERVE_LOG_SPACE.**

  L'installation par défaut du serveur ONTAP Mediator crée un espace disque distinct pour les journaux. Le programme d'installation crée un nouveau fichier de taille fixe avec un total de 700 Mo d'espace disque à utiliser explicitement pour la journalisation Mediator.

  Pour désactiver cette fonction et utiliser l'espace disque par défaut, effectuez les opérations suivantes :

  a. Dans le fichier suivant, remplacez la valeur de RESERVE_LOG_SPACE de "`1'" à "`0'" :

     ```
     /opt/netapp/lib/ontap_mediator/tools/mediator_env
     ```

  b. Redémarrez le Mediator :

i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

ii. `systemctl restart ontap_mediator`

Pour réactiver la fonction, changez la valeur de « 0 » à « 1 » et redémarrez le Mediator.

> Le basculement entre les espaces disque ne purge pas les journaux existants. Tous les journaux précédents sont sauvegardés puis déplacés vers l'espace disque actuel après avoir basculé et redémarré le Mediator.

Gérez le service ONTAP médiateur

Une fois le service ONTAP Mediator installé, vous pouvez modifier le nom d'utilisateur ou le mot de passe. Vous pouvez également désinstaller le service ONTAP Mediator.

Modifier le nom d'utilisateur

À propos de ces tâches

Cette tâche est exécutée sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.

Si vous ne pouvez pas atteindre cette commande, il vous faudra peut-être exécuter la commande en utilisant le chemin d'accès complet, comme illustré dans l'exemple suivant :

```
/usr/local/bin/mediator_username
```

Procédure

Modifiez le nom d'utilisateur en choisissant l'une des options suivantes :

- Exécutez la commande mediator_change_user et répondez aux invites comme indiqué dans l'exemple suivant :

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                   Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Exécutez la commande suivante :

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
 [root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

Changer le mot de passe

Description de la tâche

Cette tâche est effectuée sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.

Si vous ne pouvez pas atteindre cette commande, il vous faudra peut-être exécuter la commande en utilisant le chemin d'accès complet, comme illustré dans l'exemple suivant :

```
/usr/local/bin/mediator_change_password
```

Procédure

Modifiez le mot de passe en choisissant l'une des options suivantes :

- Exécutez le `mediator_change_password` commande et répond aux invites, comme illustré dans l'exemple suivant :

  ```
  [root@mediator-host ~]# mediator_change_password
  Change the Mediator API password by entering the following values:
     Mediator API User Name: mediatoradmin
                Old Password:
                New Password:
           Confirm Password:
  The password has been updated successfully.
  [root@mediator-host ~]#
  ```

- Exécutez la commande suivante :

  ```
  MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
  MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
  ```

  L'exemple montre que le mot de passe passe passe de "mediator1" à "mediator2".

  ```
   [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
  MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
  mediator_change_password
   The password has been updated successfully.
   [root@mediator-host ~]#
  ```

Arrêtez le service ONTAP Mediator

Pour arrêter le service du médiateur ONTAP, effectuez les opérations suivantes :

Étapes

1. Arrêtez le médiateur ONTAP.

   ```
   systemctl stop ontap_mediator
   ```

2. Arrêter SCST.

   ```
   systemctl stop mediator-scst
   ```

3. Désactivez le Mediator ONTAP et le SCST.

   ```
   systemctl diable ontap_mediator mediator-scst
   ```

Réactiver le service ONTAP Mediator

Pour réactiver le service ONTAP Mediator, effectuez les opérations suivantes :

Étapes

1. Activez le Mediator ONTAP et le SCST.

   ```
   systemctl enable ontap_mediator mediator-scst
   ```

2. Démarrez SCST.

   ```
   systemctl start mediator-scst
   ```

3. Démarrez ONTAP Mediator.

   ```
   systemctl start ontap_mediator
   ```

Vérifiez que le médiateur ONTAP fonctionne correctement

Une fois le médiateur ONTAP installé, vous devez vérifier que les services du médiateur ONTAP sont en cours d'exécution.

Étapes

1. Afficher l'état des services du médiateur ONTAP :

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Vérifiez les ports utilisés par le service ONTAP Mediator :

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Désinstallez manuellement SCST pour effectuer la maintenance de l'hôte

Pour désinstaller SCST, vous avez besoin du paquet tar SCST utilisé pour la version installée de ONTAP Mediator.

Étapes

1. Téléchargez l'ensemble SCST approprié (comme indiqué dans le tableau suivant) et décompressez-le.

Pour cette version …	Utiliser ce paquet tar…
Médiateur ONTAP 1.7	scst-3.7.0.tar.bz2
Médiateur ONTAP 1.6	scst-3.7.0.tar.bz2
Médiateur ONTAP 1.5	scst-3.6.0.tar.bz2
Médiateur ONTAP 1.4	scst-3.6.0.tar.bz2
Médiateur ONTAP 1.3	scst-3.5.0.tar.bz2
Médiateur ONTAP 1.1	scst-3.4.0.tar.bz2
Médiateur ONTAP 1.0	scst-3.3.0.tar.bz2

2. Exécutez les commandes suivantes dans le répertoire « scst » :
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Installez manuellement SCST pour effectuer la maintenance de l'hôte

Pour installer manuellement le SCST, vous devez disposer du paquet tar SCST utilisé pour la version installée du Mediator ONTAP (voir le tableau ci-dessus).

1. Exécutez les commandes suivantes dans le répertoire « scst » :
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`
   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`
2. (Facultatif) si le démarrage sécurisé est activé, effectuez les opérations suivantes avant de redémarrer :
   a. Déterminez chaque nom de fichier pour les modules "scst_vdisk", "scst" et "iscsi_scst".

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. Déterminez la version du noyau.

      ```
      [root@localhost ~]# uname -r
      ```

   c. Signez chaque fichier avec le noyau.

      ```
      [root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-file \sha256 \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.priv \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der \
      _module-filename_
      ```

   d. Installez la clé correcte avec le micrologiciel UEFI.

      Les instructions d'installation de la clé UEFI se trouvent à l'adresse suivante :

      `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

      La clé UEFI générée se trouve à l'emplacement suivant :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. Redémarrer.

```
reboot
```

Désinstallez le service ONTAP Mediator

Avant de commencer

Si nécessaire, vous pouvez supprimer le service ONTAP Mediator. Le médiateur doit être déconnecté de ONTAP avant de supprimer le service médiateur.

Description de la tâche

Cette tâche est effectuée sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.

Si vous ne pouvez pas atteindre cette commande, il vous faudra peut-être exécuter la commande en utilisant le chemin d'accès complet, comme illustré dans l'exemple suivant :

```
/usr/local/bin/uninstall_ontap_mediator
```

Étape

1. Désinstallez le service ONTAP Mediator :

```
uninstall_ontap_mediator
```

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Régénérez un certificat auto-signé temporaire

Description de la tâche

- Vous effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.
- Vous pouvez effectuer cette tâche uniquement si les certificats auto-signés générés sont devenus obsolètes en raison de modifications apportées au nom d'hôte ou à l'adresse IP de l'hôte après l'installation du médiateur ONTAP.
- Une fois que le certificat auto-signé temporaire a été remplacé par un certificat tiers approuvé, vous devez *ne* pas_ utiliser cette tâche pour régénérer un certificat. L'absence d'un certificat auto-signé entraînera l'échec de cette procédure.

Étape

Pour régénérer un nouveau certificat auto-signé temporaire pour l'hôte actuel, effectuez l'étape suivante :

1. Redémarrez le médiateur ONTAP :

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.......................................................++++
e is 65537 (0x010001)
Generating a RSA private key
...............................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

Maintenir l’hôte du système d’exploitation pour le médiateur ONTAP

Pour des performances optimales, vous devez maintenir régulièrement le système d’exploitation hôte pour ONTAP Mediator.

Redémarrez l’hôte

Redémarrez l’hôte lorsque les clusters fonctionnent correctement. Bien que le médiateur ONTAP soit hors ligne, les clusters risquent de ne pas pouvoir réagir correctement aux pannes. Une fenêtre de service est recommandée si un redémarrage est nécessaire.

Le médiateur ONTAP reprend automatiquement au cours du redémarrage et entre de nouveau les relations qui avaient été précédemment configurées avec les clusters ONTAP.

Mises à jour du package hôte

N'importe quelle bibliothèque ou paquets yum (à l'exception du noyau) peut être mis à jour en toute sécurité, mais peut nécessiter un redémarrage pour prendre effet. Une fenêtre de service est recommandée si un redémarrage est nécessaire.

Si vous installez le `yum-utils` utiliser le `needs-restarting` commande permettant de détecter si des modifications de pack nécessitent un redémarrage.

Vous devez redémarrer si l'une des dépendances du médiateur ONTAP est mise à jour car elles ne prendront pas effet immédiatement sur les processus en cours d'exécution.

Mises à niveau mineures du noyau du système d'exploitation hôte

SCST doit être compilé pour le noyau utilisé. Pour mettre à jour le système d'exploitation, une fenêtre de maintenance est requise.

Étapes

Procédez comme suit pour mettre à niveau le noyau du système d'exploitation hôte.

1. Arrêtez le médiateur ONTAP
2. Désinstallez le progiciel SCST. (SCST ne fournit pas de mécanisme de mise à niveau.)
3. Mettez à niveau le système d'exploitation, puis redémarrez.
4. Réinstallez le progiciel SCST.
5. Réactiver les services du médiateur ONTAP.

L'hôte modifie le nom d'hôte ou l'adresse IP

Description de la tâche

- Vous effectuez cette tâche sur l'hôte Linux sur lequel le service ONTAP Mediator est installé.
- Vous pouvez effectuer cette tâche uniquement si les certificats auto-signés générés sont devenus obsolètes en raison de modifications apportées au nom d'hôte ou à l'adresse IP de l'hôte après l'installation du médiateur ONTAP.
- Une fois que le certificat auto-signé temporaire a été remplacé par un certificat tiers approuvé, vous devez *ne* pas_ utiliser cette tâche pour régénérer un certificat. L'absence d'un certificat auto-signé entraînera l'échec de cette procédure.

Étape

Pour régénérer un nouveau certificat auto-signé temporaire pour l'hôte actuel, effectuez l'étape suivante :

1. Redémarrez le médiateur ONTAP :

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.......................................................++++
e is 65537 (0x010001)
Generating a RSA private key
...............................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Gérez des sites MetroCluster avec System Manager

Présentation de la gestion de site MetroCluster avec System Manager

Depuis ONTAP 9.8, System Manager peut être utilisé comme interface simplifiée pour gérer une configuration d'une configuration MetroCluster.

Une configuration MetroCluster permet aux deux clusters de mettre en miroir les données les uns aux autres. Ainsi, si un cluster tombe en panne, les données ne sont pas perdues.

En général, une entreprise configure les clusters dans deux emplacements géographiques distincts. Un administrateur situé sur chaque emplacement configure un cluster et le configure. Ensuite, l'un des administrateurs peut configurer le peering entre les clusters afin que ceux-ci puissent partager les données.

L'entreprise peut également installer un médiateur ONTAP dans un troisième emplacement. Le service ONTAP Mediator surveille l'état de chaque cluster. Lorsque l'un des clusters détecte qu'il ne peut pas communiquer avec le cluster partenaire, il demande au moniteur de déterminer si l'erreur est un problème avec le système

de cluster ou avec la connexion réseau.

Si le problème vient de la connexion réseau, l'administrateur système effectue des méthodes de dépannage pour corriger l'erreur et se reconnecter. Si le cluster partenaire est défaillant, l'autre cluster démarre un processus de basculement pour contrôler les E/S de données pour les deux clusters.

Vous pouvez également effectuer un basculement pour arrêter l'un des systèmes du cluster dans le cadre d'une maintenance planifiée. Le cluster partenaire gère toutes les opérations d'E/S des données pour les deux clusters jusqu'à ce que vous ayez mis en place le cluster sur lequel vous avez effectué les opérations de maintenance et de rétablissement.

Vous pouvez gérer les opérations suivantes :

- "Configurer un site IP MetroCluster"
- "Configuration du peering de MetroCluster IP"
- "Configurez un site MetroCluster IP"
- "Réalisez le basculement et le rétablissement IP MetroCluster"
- "Résolution des problèmes liés aux configurations IP MetroCluster"
- "Mettre à niveau ONTAP sur des clusters MetroCluster"

Configurer un site IP MetroCluster

Depuis ONTAP 9.8, vous pouvez utiliser System Manager pour configurer une configuration IP sur un site MetroCluster.

Un site MetroCluster se compose de deux clusters. En règle générale, les clusters se trouvent dans des emplacements géographiques différents.

Avant de commencer

- Votre système doit déjà être installé et câblé conformément au "Instructions d'installation et de configuration" fourni avec le système.
- Les interfaces réseau de clusters doivent être configurées sur chaque nœud de chaque cluster pour des communications intra-cluster.

Attribuez une adresse IP de gestion des nœuds

Système Windows

Vous devez connecter votre ordinateur Windows au même sous-réseau que les contrôleurs. L'adresse IP de gestion des nœuds sera automatiquement attribuée à votre système.

Étapes

1. À partir du système Windows, ouvrez le lecteur **réseau** pour découvrir les nœuds.
2. Double-cliquez sur le nœud pour lancer l'assistant de configuration du cluster.

Autres systèmes

Vous devez configurer l'adresse IP node-management pour l'un des nœuds du cluster. Vous pouvez utiliser cette adresse IP node-management pour lancer l'assistant de configuration des clusters.

Voir "Création du cluster sur le premier node" Pour plus d'informations sur l'attribution d'une adresse IP de

gestion des nœuds.

Initialiser et configurer le cluster

Vous initialisez le cluster en définissant un mot de passe administratif pour le cluster et en configurant les réseaux de gestion du cluster et de gestion des nœuds. Vous pouvez également configurer des services tels qu'un serveur DNS pour résoudre les noms d'hôtes et un serveur NTP pour synchroniser l'heure.

Étapes

1. Dans un navigateur Web, saisissez l’adresse IP de gestion des nœuds que vous avez configurée : "https://node-management-IP"

   System Manager détecte automatiquement les nœuds restants dans le cluster.

2. Dans la fenêtre **Initialize Storage System**, effectuez les opérations suivantes :
   a. Saisissez les données de configuration du réseau de gestion du cluster.
   b. Entrez les adresses IP de gestion des nœuds pour tous les nœuds.
   c. Indiquez les détails des serveurs de noms de domaine (DNS).
   d. Dans la section **autre**, cochez la case **utiliser le service de temps (NTP)** pour ajouter les serveurs de temps.

Lorsque vous cliquez sur **Submit**, attendez que le cluster soit créé et configuré. Ensuite, un processus de validation a lieu.

Et la suite ?

Une fois les deux clusters configurés, initialisés et configurés, effectuez la procédure suivante :

- "Configuration du peering de MetroCluster IP"

Configurez ONTAP sur une nouvelle vidéo de cluster

Configuration du peering de MetroCluster IP

Depuis ONTAP 9.8, vous pouvez gérer la configuration IP d'une opération MetroCluster avec System Manager. Une fois que deux clusters sont configurés, vous configurez le peering entre eux.

Avant de commencer

Vous devez avoir terminé la procédure suivante pour configurer deux clusters :

- "Configurer un site IP MetroCluster"

Différentes étapes sont réalisées par différents administrateurs système sur les sites géographiques de chaque cluster. Pour expliquer ce processus, les clusters sont appelés « grappe de sites A » et « grappe de sites B ».

Exécution du processus de peering à partir du site A

Ce processus est exécuté par un administrateur système sur le site A.

Étapes

1. Connectez-vous au site A cluster.
2. Dans System Manager, sélectionnez **Dashboard** dans la colonne de navigation de gauche pour afficher la vue d'ensemble du cluster.

   Le tableau de bord affiche les détails de ce cluster (site A). Dans la section **MetroCluster**, site Un cluster est affiché sur la gauche.

3. Cliquez sur **attacher le cluster partenaire**.
4. Entrez les détails des interfaces réseau permettant aux nœuds du cluster site A de communiquer avec les

nœuds du cluster site B.

5. Cliquez sur **Enregistrer et continuer**.
6. Dans la fenêtre **Attach Partner Cluster**, sélectionnez **Je n'ai pas de phrase de passe**, ce qui vous permet de générer une phrase de passe.
7. Copiez le mot de passe généré et partagez-le avec l'administrateur système du site B.
8. Sélectionnez **Fermer**.

Exécution du processus de peering depuis le site B

Ce processus est effectué par un administrateur système sur le site B.

Étapes

1. Connectez-vous au cluster site B.
2. Dans System Manager, sélectionnez **Dashboard** pour afficher la vue d'ensemble du cluster.

   Le tableau de bord affiche les détails de ce cluster (site B). Dans la section MetroCluster, le cluster du site B est indiqué sur la gauche.

3. Cliquez sur **Attach Partner Cluster** pour démarrer le processus de peering.
4. Entrez les détails des interfaces réseau permettant aux nœuds du cluster site B de communiquer avec les nœuds du cluster site A.
5. Cliquez sur **Enregistrer et continuer**.
6. Dans la fenêtre **Attach Partner Cluster**, sélectionnez **J'ai une phrase de passe**, qui vous permet de saisir la phrase de passe que vous avez reçue de l'administrateur système sur le site A.
7. Sélectionnez **Peer** pour terminer le processus de peering.

Et la suite ?

Une fois le processus de peering terminé avec succès, vous configurez les clusters. Voir "Configurez un site MetroCluster IP".

Configurez un site MetroCluster IP

Depuis ONTAP 9.8, vous pouvez gérer la configuration IP d'une opération MetroCluster avec System Manager. Après avoir configuré deux clusters et peering, vous configurez chaque cluster.

Avant de commencer

Vous devez avoir effectué les procédures suivantes :

- "Configurer un site IP MetroCluster"
- "Configuration du peering de MetroCluster IP"

Configurer la connexion entre les clusters

Étapes

1. Connectez-vous à System Manager sur l'un des sites et sélectionnez **Dashboard**.

   Dans la section **MetroCluster**, le graphique montre les deux clusters que vous avez configurés et associés

pour les sites MetroCluster. Le cluster depuis lequel vous travaillez (cluster local) s'affiche sur la gauche.

2. Cliquez sur **configurer MetroCluster**. Dans cette fenêtre, vous pouvez effectuer les tâches suivantes :
   a. Les nœuds de chaque cluster de la configuration MetroCluster sont affichés. Utilisez les listes déroulantes pour sélectionner les nœuds du cluster local qui seront des partenaires de reprise après sinistre avec lesquels les nœuds du cluster distant seront présents.
   b. Cochez la case si vous souhaitez configurer un service de médiateur ONTAP. Voir Configurez le service Mediator ONTAP.
   c. Si les deux clusters disposent d'une licence pour activer le chiffrement, la section **Encryption** s'affiche.

      Pour activer le chiffrement, entrez une phrase de passe.

   d. Cochez la case si vous souhaitez configurer MetroCluster avec un réseau partagé de couche 3.

      > Les nœuds partenaires haute disponibilité et les commutateurs réseau qui se connectent aux nœuds doivent avoir une configuration correspondante.

3. Cliquez sur **Enregistrer** pour configurer les sites MetroCluster.

   Dans la section **MetroCluster** du **Tableau de bord**, le graphique montre une coche sur la liaison entre les deux grappes, indiquant une connexion saine.

Configurez le service Mediator ONTAP

Le service médiateur ONTAP est généralement installé dans un emplacement géographique distinct de l'un ou l'autre des clusters. Les clusters communiquent régulièrement avec le service pour indiquer qu'ils sont opérationnels. Si l'un des clusters de la configuration MetroCluster détecte que la communication avec son cluster partenaire est en panne, il consulte le médiateur ONTAP pour déterminer si le cluster partenaire est en panne.

Avant de commencer

Les deux clusters des sites MetroCluster doivent être up et associés.

Étapes

1. Dans System Manager sous ONTAP 9.8, sélectionnez **Cluster > Paramètres**.
2. Dans la section **Mediator**, cliquez sur ⚙.
3. Dans la fenêtre **Configure Mediator**, cliquez sur **Add+**.
4. Entrez les détails de configuration du médiateur ONTAP.

   Vous pouvez entrer les détails suivants lors de la configuration d'un médiateur ONTAP avec le Gestionnaire système.

   - Adresse IP du Mediator.
   - Nom d'utilisateur.
   - Le mot de passe.

Gérer le Mediator avec System Manager

À l'aide de System Manager, vous pouvez effectuer des tâches de gestion du Mediator.

À propos de ces tâches

À partir de ONTAP 9.8, vous pouvez utiliser System Manager comme interface simplifiée pour gérer une configuration IP à quatre nœuds d'une configuration MetroCluster, qui peut inclure un médiateur ONTAP installé à un troisième emplacement.

Depuis ONTAP 9.14.1, vous pouvez utiliser System Manager pour effectuer ces opérations dans une configuration IP à huit nœuds d'un site MetroCluster. Bien que vous ne puissiez pas configurer ou développer un système à huit nœuds avec System Manager, si vous avez déjà configuré un système IP MetroCluster à huit nœuds, vous pouvez effectuer ces opérations.

Effectuez les tâches suivantes pour gérer le Mediator.

Pour effectuer cette tâche…	Prenez ces mesures…
Configurez le service Mediator	Suivez les étapes de la section "Configurez le service Mediator ONTAP".
Activer ou désactiver la commutation automatique assistée par Mediator (MAUSO)	1. Dans System Manager, cliquez sur **Dashboard**. 2. Faites défiler jusqu'à la section MetroCluster. 3. Cliquez sur ⋮ En regard du nom du site MetroCluster. 4. Sélectionnez **Activer** ou **Désactiver**. 5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Activer** ou **Désactiver**. ⓘ Vous pouvez activer ou désactiver le Mediator lorsqu'il est accessible et que les deux sites sont en mode « Normal ». Le médiateur est toujours accessible lorsque MAUSO est activé ou désactivé si le système MetroCluster est en bon état.
Retirez le Mediator de la configuration MetroCluster	1. Dans System Manager, cliquez sur **Dashboard**. 2. Faites défiler jusqu'à la section MetroCluster. 3. Cliquez sur ⋮ En regard du nom du site MetroCluster. 4. Sélectionnez **Supprimer le médiateur**. 5. Entrez le nom d'utilisateur et le mot de passe de l'administrateur, puis cliquez sur **Supprimer**.
Vérifiez l'état de santé du Mediator	Suivez les étapes de la section "Résolution des problèmes liés aux configurations IP MetroCluster".
Effectuer un basculement et un rétablissement	Suivez les étapes de la section "Réalisez le basculement et le rétablissement IP MetroCluster".

Réalisez le basculement et le rétablissement IP MetroCluster

Vous pouvez basculer le contrôle d'un site IP MetroCluster à un autre pour effectuer des opérations de maintenance ou de restauration suite à un problème.

Les procédures de basculement et de rétablissement ne sont prises en charge que pour les configurations IP MetroCluster.

Présentation du basculement et du rétablissement

Un basculement peut se produire dans deux cas :

- **Un basculement planifié**

  Le basculement est initié par un administrateur système qui utilise System Manager. Le basculement planifié permet à l'administrateur système d'un cluster local de contrôler par commutation afin que les services de données du cluster distant soient gérés par le cluster local. Ensuite, un administrateur système sur le site distant du cluster peut réaliser des opérations de maintenance sur le cluster distant.

- **Un basculement non planifié**

  Dans certains cas, lorsqu'un cluster MetroCluster tombe en panne ou que les connexions entre les clusters sont en panne, ONTAP lance automatiquement une procédure de basculement, de sorte que le cluster toujours en cours d'exécution gère les responsabilités de gestion des données du cluster en panne.

  Lorsque ONTAP ne peut pas déterminer l'état de l'un des clusters, l'administrateur système du site qui travaille lance la procédure de basculement pour prendre le contrôle des responsabilités de gestion des données de l'autre site.

Pour tout type de procédure de basculement, la fonctionnalité de service de données est renvoyée au cluster au moyen d'un processus *rétablissement*.

Plusieurs processus de basculement et de rétablissement sont exécutés pour ONTAP 9.7 et 9.8 :

- Utilisez System Manager dans ONTAP 9.7 pour le basculement et le rétablissement
- Utilisez System Manager dans ONTAP 9.8 pour le basculement et le rétablissement

Utilisez System Manager dans ONTAP 9.7 pour le basculement et le rétablissement

Étapes

1. Connectez-vous à System Manager dans ONTAP 9.7.
2. Cliquez sur * (revenir à la version classique)*.
3. Cliquez sur **Configuration > MetroCluster**.

   System Manager vérifie si un basculement négocié est possible.

4. Effectuez l'une des opérations suivantes lorsque le processus de validation est terminé :
   a. Si la validation échoue, mais que le site B est en cours, une erreur s'est produite. Par exemple, il peut y avoir un problème avec un sous-système, ou la mise en miroir NVRAM peut ne pas être synchronisée.
      i. Corrigez le problème à l'origine de l'erreur, cliquez sur **Fermer**, puis recommencez à l'étape 2.
      ii. Arrêtez les nœuds du site B, cliquez sur **Fermer**, puis effectuez les étapes de la section "Effectuer un basculement non planifié".
   b. Si la validation échoue et que le site B est en panne, il est fort probable qu'il y ait un problème de connexion. Vérifiez que le site B est en panne, puis effectuez les étapes de la section "Effectuer un

basculement non planifié".

5. Cliquez sur **basculer du site B vers le site A** pour lancer le processus de basculement.
6. Cliquez sur **basculer vers la nouvelle expérience**.

Utilisez System Manager dans ONTAP 9.8 pour le basculement et le rétablissement

Exécution d'un basculement planifié (ONTAP 9.8)

Étapes

1. Connectez-vous au Gestionnaire système dans ONTAP 9.8.
2. Sélectionnez **Tableau de bord**. Dans la section **MetroCluster**, les deux clusters sont affichés avec une connexion.
3. Dans le cluster local (affiché à gauche), cliquez sur ⋮, Puis sélectionnez **basculer les services de données distants vers le site local**.

   Une fois la demande de basculement validée, le contrôle est transféré du site distant vers le site local, qui effectue les demandes de service de données pour les deux clusters.

   Le cluster distant redémarre, mais les composants de stockage ne sont pas actifs et le cluster ne répond pas aux demandes de données. Elle est maintenant disponible pour la maintenance planifiée.

> Le cluster distant ne doit pas être utilisé pour la maintenance des données tant que vous n'avez pas effectué de rétablissement.

Exécution d'un basculement non planifié (ONTAP 9.8)

Un basculement non planifié peut être initié automatiquement par ONTAP. Si ONTAP ne peut pas déterminer s'il est nécessaire de procéder au rétablissement, l'administrateur système du site MetroCluster en cours d'exécution lance le basculement. Pour ce faire, procédez comme suit :

Étapes

1. Connectez-vous au Gestionnaire système dans ONTAP 9.8.
2. Sélectionnez **Tableau de bord**.

   Dans la section **MetroCluster**, la connexion entre les deux clusters est indiquée par un « X », ce qui signifie qu'une connexion ne peut pas être détectée. Les connexions ou le cluster sont arrêtés.

3. Dans le cluster local (affiché à gauche), cliquez sur ⋮, Puis sélectionnez **basculer les services de données distants vers le site local**.

   Si le basculement échoue par erreur, cliquez sur le lien « Afficher les détails » dans le message d'erreur et confirmez le basculement non planifié.

   Une fois la demande de basculement validée, le contrôle est transféré du site distant vers le site local, qui effectue les demandes de service de données pour les deux clusters.

   Le cluster doit être réparé avant de pouvoir être remis en ligne.

> Une fois le cluster distant mis en ligne à nouveau, il ne doit pas être utilisé pour le service des données tant que vous n'avez pas effectué de rétablissement.

Exécution d'un rétablissement (ONTAP 9.8)

Avant de commencer

Si le cluster distant était indisponible pour la maintenance planifiée ou en raison d'un incident, il devrait être à présent opérationnel et en attente du rétablissement.

Étapes

1. Sur le cluster local, connectez-vous à System Manager dans ONTAP 9.8.
2. Sélectionnez **Tableau de bord**.

   Dans la section **MetroCluster**, les deux clusters sont affichés.

3. Dans le cluster local (affiché à gauche), cliquez sur ⋮, Et sélectionnez **reprendre le contrôle**.

   Les données sont *guéri* en premier, pour garantir que les données sont synchronisées et mises en miroir entre les deux clusters.

4. Une fois la correction des données terminée, cliquez sur ⋮, Et sélectionnez **lancer le rétablissement**.

   Lorsque le rétablissement est terminé, les deux clusters sont actifs et le service des requêtes de données. De plus, les données sont en miroir et synchronisées entre les clusters.

Modifiez l'adresse, le masque de réseau et la passerelle dans une adresse IP MetroCluster

Depuis ONTAP 9.10.1, vous pouvez modifier les propriétés suivantes d'une interface IP MetroCluster : adresse IP et masque, et passerelle. Vous pouvez utiliser n'importe quelle combinaison de paramètres pour la mise à jour.

Vous devrez peut-être mettre à jour ces propriétés, par exemple si une adresse IP dupliquée est détectée ou si une passerelle doit changer dans le cas d'un réseau de couche 3 en raison de modifications de configuration du routeur. Vous ne pouvez modifier qu'une interface à la fois. Cette interface entraînera une perturbation du trafic jusqu'à ce que les autres interfaces soient mises à jour et que les connexions soient reétablies.

> Vous devez effectuer les modifications sur chaque port. De même, les commutateurs réseau doivent également mettre à jour leur configuration. Par exemple, si la passerelle est mise à jour, elle est idéalement modifiée sur les deux nœuds d'une paire haute disponibilité, car ils sont identiques. De plus, le switch connecté à ces nœuds doit également mettre à jour sa passerelle.

Étape

Mettez à jour l'adresse IP, le masque de réseau et la passerelle pour chaque nœud et interface.

Résolution des problèmes liés aux configurations IP MetroCluster

Depuis ONTAP 9.8, System Manager surveille l'intégrité des configurations IP MetroCluster et vous aide à identifier et à corriger les problèmes potentiels.

Présentation de la vérification de l'état du système MetroCluster

System Manager vérifie régulièrement l'état de santé de votre configuration IP MetroCluster. Lorsque vous affichez la section MetroCluster du tableau de bord, le message généralement « les systèmes MetroCluster

sont sains ».

Cependant, lorsqu'un problème se produit, le message indique le nombre d'événements. Vous pouvez cliquer sur ce message et afficher les résultats de la vérification de l'état des composants suivants :

- Nœud
- Interface réseau
- Niveau (stockage)
- Cluster
- Connexion
- Volumétrie
- Réplication de la configuration

La colonne **Status** identifie les composants qui présentent des problèmes et la colonne **Details** indique comment corriger le problème.

Dépannage de MetroCluster

Étapes

1. Dans System Manager, sélectionnez **Dashboard**.
2. Dans la section **MetroCluster**, notez le message.
   a. Si le message indique que la configuration de votre MetroCluster est correcte et que les connexions entre les clusters et le médiateur ONTAP sont en bon état (avec des cases à cocher), alors vous n'avez aucun problème à corriger.
   b. Si le message indique le nombre d'événements, ou si les connexions ont diminué (indiqué par un « X »), passez à l'étape suivante.
3. Cliquez sur le message indiquant le nombre d'événements.

   Le rapport d'intégrité MetroCluster s'affiche.
4. Dépanner les problèmes qui apparaissent dans le rapport en utilisant les suggestions dans la colonne **Détails**.
5. Lorsque tous les problèmes ont été corrigés, cliquez sur **vérifier l'état de santé du MetroCluster**.

   > La vérification de l'état de santé MetroCluster utilise une quantité importante de ressources. Il est donc recommandé d'effectuer toutes vos tâches de dépannage avant d'exécuter la vérification.

   La vérification de l'état de santé de MetroCluster s'exécute en arrière-plan. Vous pouvez travailler sur d'autres tâches pendant que vous attendez la fin.

Protection des données par sauvegarde sur bandes

Présentation de la sauvegarde sur bande des volumes FlexVol

ONTAP supporte la sauvegarde sur bande et la restauration via le protocole NDMP (Network Data Management Protocol). NDMP vous permet de sauvegarder directement

les données des systèmes de stockage sur bande, ce qui optimise l'utilisation de la bande passante réseau. ONTAP prend en charge les moteurs dump et SMTape pour la sauvegarde sur bande.

Vous pouvez effectuer une sauvegarde ou une restauration dump ou SMTape à l'aide des applications de sauvegarde conformes à NDMP. Seule la version 4 de NDMP est prise en charge.

Sauvegarde sur bande à l'aide de dump

Dump est une sauvegarde à base de copies Snapshot dans laquelle les données de votre système de fichiers sont sauvegardées sur bande. Le moteur de vidage ONTAP sauvegarde les fichiers, les répertoires et les informations de la liste de contrôle d'accès (ACL) applicable sur bande. Vous pouvez sauvegarder un volume entier, un qtree entier ou un sous-arbre qui n'est pas un volume entier ou un qtree entier. Le dump prend en charge les sauvegardes de base, différentielles et incrémentielles.

Sauvegarde sur bande utilisant SMTape

SMTape est une solution de reprise après incident basée sur les copies Snapshot de ONTAP qui sauvegarde des blocs de données sur bande. Vous pouvez utiliser SMTape afin d'effectuer des sauvegardes de volume sur bandes. Toutefois, vous ne pouvez pas effectuer de sauvegarde au niveau qtree ou sous-arbre. SMTape prend en charge les sauvegardes de base, différentielles et incrémentielles.

À partir de ONTAP 9.13.1, la sauvegarde sur bande à l'aide de SMTape est prise en charge par Continuité de l'activité SnapMirror.

Sauvegarde sur bande et restauration du flux de travail

Vous pouvez effectuer des opérations de sauvegarde sur bande et de restauration à l'aide d'une application de sauvegarde NDMP.

Description de la tâche

Le flux de production de sauvegarde et restauration sur bande présente les tâches impliquées dans les opérations de sauvegarde et de restauration sur bande. Pour plus d'informations sur l'exécution d'une opération de sauvegarde et de restauration, reportez-vous à la documentation de l'application de sauvegarde.

Étapes

1. Définissez une configuration de librairie de bandes en choisissant une topologie de bande prise en charge par NDMP.
2. Activez les services NDMP sur votre système de stockage.

   Vous pouvez activer les services NDMP au niveau des nœuds ou au niveau des machines virtuelles de stockage (SVM). Cela dépend du mode NDMP dans lequel vous choisissez d'effectuer l'opération de sauvegarde sur bande et de restauration.

3. Utilisez les options NDMP pour gérer NDMP sur votre système de stockage.

   Vous pouvez utiliser les options NDMP au niveau des nœuds ou au niveau de la SVM. Cela dépend du mode NDMP dans lequel vous choisissez d'effectuer l'opération de sauvegarde sur bande et de restauration.

   Vous pouvez modifier les options NDMP au niveau du nœud en utilisant la `system services ndmp modify` Commande et au niveau du SVM à l'aide de `vserver services ndmp modify` commande. Pour plus d'informations sur ces commandes, consultez les pages de manuels.

4. Effectuez une opération de sauvegarde sur bande ou de restauration à l'aide d'une application de sauvegarde NDMP.

   ONTAP prend en charge les moteurs dump et SMTape pour la sauvegarde sur bande et la restauration.

   Pour plus d'informations sur l'utilisation de l'application de sauvegarde (également appelée *Data Management applications* ou *DMA*) pour effectuer des opérations de sauvegarde ou de restauration, consultez la documentation de votre application de sauvegarde.

Informations associées

Topologies de sauvegarde sur bande NDMP courantes

Présentation du moteur de dump pour les volumes FlexVol

Cas d'utilisation pour choisir un moteur de sauvegarde sur bandes

ONTAP prend en charge deux moteurs de sauvegarde : SMTape et dump. Il est important de connaître les cas d'utilisation des moteurs de sauvegarde SMTape et dump afin de vous aider à choisir le moteur de sauvegarde permettant d'effectuer des opérations de sauvegarde sur bande et de restauration.

Le vidage peut être utilisé dans les cas suivants :

- La récupération d'accès direct des fichiers et des répertoires
- Sauvegarde d'un sous-ensemble de sous-répertoires ou de fichiers dans un chemin spécifique
- Exclusion de fichiers et de répertoires spécifiques pendant les sauvegardes
- Conserver les sauvegardes sur de longues durées

SMTape peut être utilisé dans les cas suivants :

- Solution de reprise après incident
- Préservation des économies de déduplication et des paramètres de déduplication sur les données sauvegardées au cours d'une opération de restauration
- Sauvegarde de volumes volumineux

Gérer les lecteurs de bandes

Présentation de la gestion des lecteurs de bandes

Vous pouvez vérifier les connexions de la librairie de bandes et afficher les informations relatives au lecteur de bandes avant d'effectuer une sauvegarde sur bande ou une restauration. Vous pouvez utiliser un lecteur de bande non qualifié en l'émulant sur un lecteur de bande qualifié. Vous pouvez également attribuer et supprimer des alias de bande en plus d'afficher des alias existants.

Lorsque vous sauvegardez des données sur bande, celles-ci sont stockées dans des fichiers sur bande. Les repères de fichier séparent les fichiers de bande et les fichiers n'ont pas de nom. Vous spécifiez un fichier de bande en fonction de sa position sur la bande. Vous écrivez un fichier de bande à l'aide d'un lecteur de bande. Lorsque vous lisez le fichier de bande, vous devez spécifier un périphérique ayant le même type de

compression que celui utilisé pour écrire ce fichier de bande.

Commandes pour la gestion des lecteurs de bande, des changeurs de supports et des opérations de lecteurs de bande

Il existe des commandes permettant d'afficher des informations sur les lecteurs de bande et les changeurs de support d'un cluster, de mettre un lecteur de bande en ligne et de le mettre hors ligne, de modifier la position de la cartouche du lecteur de bande, de définir et d'effacer le nom d'alias du lecteur de bande, et de réinitialiser un lecteur de bande. Vous pouvez également afficher et réinitialiser les statistiques du lecteur de bande.

Les fonctions que vous recherchez…	Utilisez cette commande…
Mettre un lecteur de bande en ligne	`storage tape online`
Effacez un nom d'alias pour le lecteur de bande ou le changeur de supports	`storage tape alias clear`
Permet d'activer ou de désactiver une opération de trace de bande pour un lecteur de bande	`storage tape trace`
Modifiez la position de la cartouche du lecteur de bande	`storage tape position`
Réinitialisez un lecteur de bande	`storage tape reset` Cette commande est disponible uniquement au niveau de privilège avancé.
Définissez un nom d'alias pour le lecteur de bande ou le changeur de supports	`storage tape alias set`
Mettez un lecteur de bande hors ligne	`storage tape offline`
Permet d'afficher des informations sur tous les lecteurs de bande et les changeurs de supports	`storage tape show`
Afficher des informations sur les lecteurs de bande connectés au cluster	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Affiche des informations sur les changeurs de supports reliés au cluster	`storage tape show-media-changer`
Afficher les informations d'erreur relatives aux lecteurs de bande connectés au cluster	`storage tape show-errors`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affichez tous les lecteurs de bande ONTAP qualifiés et pris en charge reliés à chaque nœud du cluster	`storage tape show-supported-status`
Afficher les alias de tous les lecteurs de bande et changeurs de support reliés à chaque nœud du cluster	`storage tape alias show`
Réinitialisez la lecture des statistiques d'un lecteur de bande	`storage stats tape zero tape_name` Vous devez utiliser cette commande au niveau du nodeshell.
Afficher les lecteurs de bande pris en charge par ONTAP	`storage show tape supported [-v]` Vous devez utiliser cette commande au niveau du nodeshell. Vous pouvez utiliser le `-v` option permettant d'afficher plus de détails sur chaque lecteur de bande.
Affichez les statistiques des lecteurs de bande pour comprendre les performances des bandes et vérifier le modèle d'utilisation	`storage stats tape tape_name` Vous devez utiliser cette commande au niveau du nodeshell.

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Utilisez un lecteur de bande non qualifié

Vous pouvez utiliser un lecteur de bande non qualifié sur un système de stockage s'il peut émuler un lecteur de bande qualifié. Il est ensuite traité comme un lecteur de bande qualifié. Pour utiliser un lecteur de bande non qualifié, vous devez d'abord déterminer s'il émule un des lecteurs de bande qualifiés.

Description de la tâche

Un lecteur de bande non qualifié est connecté au système de stockage, mais il n'est pas pris en charge ou reconnu par ONTAP.

Étapes

1. Affichez les lecteurs de bande non qualifiés connectés à un système de stockage à l'aide du `storage tape show-supported-status` commande.

   La commande suivante affiche les lecteurs de bande connectés au système de stockage ainsi que l'état de support et de qualification de chaque lecteur de bande. Les lecteurs de bande non qualifiés sont également répertoriés. `tape_drive_vendor_name` Est un lecteur de bande non qualifié connecté au système de stockage, mais non pris en charge par ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Émuler le lecteur de bande qualifié.

   "Téléchargements NetApp : fichiers de configuration des lecteurs de bande"

Informations associées

Lecteurs de bande qualifiés

Attribuer des alias de bande

Pour faciliter l'identification du périphérique, vous pouvez attribuer des alias de bande à un lecteur de bande ou à un changeur de support. Les alias fournissent une correspondance entre les noms logiques des périphériques de sauvegarde et un nom attribué de façon permanente au lecteur de bande ou au changeur de support.

Étapes

1. Attribuez un alias à un lecteur de bande ou à un changeur de support à l'aide de la `storage tape alias set` commande.

   Pour plus d'informations sur cette commande, consultez les pages de manuels.

   Vous pouvez afficher les informations relatives au numéro de série (SN) sur les lecteurs de bande en utilisant le `system node hardware tape drive show` commande et à propos des bibliothèques de bandes à l'aide du `system node hardware tape library show` commandes.

   La commande suivante définit un nom d'alias sur un lecteur de bande dont le numéro de série SN[123456]L4 est rattaché au nœud, cluster1-01 :

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

La commande suivante définit un nom d'alias sur un changeur de supports avec le numéro de série SN[65432] attaché au nœud, cluster1-01 :

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

Informations associées

Quel est le crénelage de la bande

Suppression des alias de bande

Supprimer les alias de bande

Vous pouvez supprimer des alias en utilisant le `storage tape alias clear` commande lorsque les alias persistants ne sont plus nécessaires pour un lecteur de bande ou un chargeur de support.

Étapes

1. Retirez un alias d'un lecteur de bande ou d'un changeur de support à l'aide de la `storage tape alias clear` commande.

   Pour plus d'informations sur cette commande, consultez les pages de manuels.

   La commande suivante supprime les alias de tous les lecteurs de bande en spécifiant l'étendue de l'opération d'effacement d'alias à `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Une fois que vous avez terminé

Si vous effectuez une sauvegarde sur bande ou une opération de restauration à l'aide de NDMP, après avoir supprimé un alias d'un lecteur de bande ou d'un changeur de support, vous devez attribuer un nouveau nom d'alias au lecteur de bande ou au changeur de support pour continuer à accéder au périphérique de bande.

Informations associées

Quel est le crénelage de la bande

Attribution d'alias de bande

Activation ou désactivation des réservations sur bandes

Vous pouvez contrôler la manière dont ONTAP gère les réservations de périphériques de bandes à l'aide de `tape.reservations` option. Par défaut, la réservation sur bande est désactivée.

Description de la tâche

L'activation de l'option de réservation de bandes peut entraîner des problèmes si les lecteurs de bandes, les changeurs de supports, les ponts ou les bibliothèques ne fonctionnent pas correctement. Si les commandes

sur bande signalent que le périphérique est réservé lorsqu'aucun autre système de stockage n'utilise le périphérique, cette option doit être désactivée.

Étapes

1. Pour utiliser le mécanisme de réserve/libération SCSI ou la réserve permanente SCSI pour désactiver les réservations sur bande, entrez la commande suivante :

   ```
   options -option-name tape.reservations -option-value {scsi | persistent | off}
   ```

   `scsi` Sélectionne le mécanisme de réserve/libération SCSI.

   `persistent` Sélectionne les réservations persistantes SCSI.

   `off` désactive les réservations sur bande.

Informations associées

Quelles sont les réservations sur bandes

Commandes permettant de vérifier les connexions de la bibliothèque de bandes

Vous pouvez afficher des informations sur le chemin de connexion entre un système de stockage et une configuration de bibliothèque de bandes attachée au système de stockage. Vous pouvez utiliser ces informations pour vérifier le chemin de connexion à la configuration de la bibliothèque de bandes ou pour résoudre les problèmes liés aux chemins de connexion.

Vous pouvez afficher les détails de la bibliothèque de bandes suivants pour vérifier les connexions de la bibliothèque de bandes après avoir ajouté ou créé une nouvelle bibliothèque de bandes, ou après avoir restauré un chemin d'accès à un seul chemin ou à un chemin d'accès multichemin vers une bibliothèque de bandes. Vous pouvez également utiliser ces informations pendant le dépannage des erreurs liées au chemin ou en cas d'échec de l'accès à une bibliothèque de bandes.

- Nœud auquel la bibliothèque de bandes est attachée
- ID de périphérique
- Chemin NDMP
- Nom de la bibliothèque de bandes
- ID de port cible et de port initiateur
- Un accès à chemin unique ou multivoie à une bibliothèque de bandes pour chaque port cible ou initiateur FC
- Détails sur l'intégrité des données liées aux chemins, tels que « erreurs de chemin » et « Path Qual »
- Groupes de LUN et nombre de LUN

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur une bibliothèque de bandes dans un cluster	`system node hardware tape library show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher les informations sur le chemin d'accès d'une bibliothèque de bandes	`storage tape library path show`
Affiche les informations sur le chemin d'accès d'une bibliothèque de bandes pour chaque port d'initiateur	`storage tape library path show-by-initiator`
Affichez les informations de connectivité entre une librairie de bandes de stockage et un cluster	`storage tape library config show`

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

À propos des lecteurs de bande

Présentation des lecteurs de bande qualifiés

Vous devez utiliser un lecteur de bande qualifié qui a été testé et trouvé pour fonctionner correctement sur un système de stockage. Vous pouvez suivre le repliement des bandes et également activer les réservations de bandes pour vous assurer qu'un seul système de stockage accède à un lecteur de bande à tout moment.

Un lecteur de bande qualifié est un lecteur de bande qui a été testé et qui fonctionne correctement sur les systèmes de stockage. Vous pouvez qualifier les lecteurs de bande pour les versions ONTAP existantes à l'aide du fichier de configuration de bande.

Format du fichier de configuration de la bande

Le format du fichier de configuration de bande comprend des champs tels que l'ID du fournisseur, l'ID du produit et les détails des types de compression pour un lecteur de bande. Ce fichier se compose également de champs facultatifs pour l'activation de la fonction d'autochargement d'un lecteur de bande et la modification des valeurs de délai de commande d'un lecteur de bande.

Le tableau suivant affiche le format du fichier de configuration de la bande :

Élément	Taille	Description
`vendor_id` (chaîne)	jusqu'à 8 octets	L'ID du fournisseur tel que signalé par le `SCSI Inquiry` commande.
`product_id`(chaîne)	jusqu'à 16 octets	L'ID du produit tel qu'indiqué par le `SCSI Inquiry` commande.

Élément	Taille	Description
`id_match_size`(nombre)		Nombre d'octets de l'ID produit à utiliser pour la correspondance pour détecter le lecteur de bande à identifier, en commençant par le premier caractère de l'ID produit dans les données de la requête.
`vendor_pretty` (chaîne)	jusqu'à 16 octets	Si ce paramètre est présent, il est spécifié par la chaîne affichée par la commande, `storage tape show -device-names`; Sinon, INQ_VENDOR_ID est affiché.
`product_pretty`(chaîne)	jusqu'à 16 octets	Si ce paramètre est présent, il est spécifié par la chaîne affichée par la commande, `storage tape show -device-names`; Sinon, INQ_PRODUCT_ID s'affiche.

> Le `vendor_pretty` et `product_pretty` les champs sont facultatifs, mais si l'un de ces champs a une valeur, l'autre doit également avoir une valeur.

Le tableau suivant explique la description, le code de densité et l'algorithme de compression des différents types de compression, tels que `l`, `m`, `h`, et `a`:

Élément	Taille	Description
`{l	m	h
a}_description=(string)`	jusqu'à 24 octets	La chaîne à imprimer pour la commande nodeshell, `sysconfig -t`, qui décrit les caractéristiques du paramètre de densité particulier.
`{l	m	h
a}_density=(hex codes)`		Le code de densité à définir dans le descripteur de bloc de page en mode SCSI correspondant au code de densité souhaité pour l, m, h ou a.
`{l	m	h

Élément	Taille	Description
a}_algorithm=(hex codes)`		L'algorithme de compression à définir dans la page du mode de compression SCSI correspondant au code de densité et à la caractéristique de densité souhaitée.

Le tableau suivant décrit les champs facultatifs disponibles dans le fichier de configuration de bande :

Champ	Description
`autoload=(Boolean yes/no)`	Ce champ est défini sur `yes` si le lecteur de bande dispose d'une fonction de chargement automatique, c'est-à-dire après l'insertion de la cartouche de bande, le lecteur de bande devient prêt sans avoir à exécuter un `SCSI load` (unité de démarrage/arrêt). La valeur par défaut de ce champ est `no`.
`cmd_timeout_0x`	Valeur de temporisation individuelle. Vous devez utiliser ce champ uniquement si vous souhaitez spécifier une valeur de temporisation différente de celle utilisée par défaut par le pilote de bande. L'exemple de fichier répertorie les valeurs de délai d'expiration de la commande SCSI par défaut utilisées par le lecteur de bande. La valeur de temporisation peut être exprimée en minutes (m), secondes (s) ou millisecondes (ms). Vous ne devez pas modifier ce champ.

Vous pouvez télécharger et afficher le fichier de configuration de bandes sur le site de support NetApp.

Exemple de format de fichier de configuration de bande

Le format de fichier de configuration de bande pour le lecteur de bande HP LTO5 ULTRIUM est le suivant :

`vendor_id`= « HP »

`product_id`= « Ultrium 5-SCSI »

`id_match_size`=9

`vendor_pretty`= « Hewlett-Packard »

`product_pretty`= « LTO-5 »

`l_description`=« LTO-3 (ro)/4 4 Go »

`l_density`=0x00

`l_algorithm`=0x00

`m_description`=« LTO-3(ro)/4 8/1600 go cmp »

`m_density`=0x00

`m_algorithm`=0x01

`h_description`=« LTO-5 1600 GO »

`h_density`=0x58

`h_algorithm`=0x00

`a_description`=« LTO-5 700 Go cmp »

`a_density`=0x58

`a_algorithm`=0x01

`autoload`= « oui »

Informations associées

"Outils NetApp : fichiers de configuration des lecteurs de bandes"

Comment le système de stockage qualifie de façon dynamique un nouveau lecteur de bande

Le système de stockage qualifie dynamiquement un lecteur de bande en faisant correspondre son ID fournisseur et son ID produit avec les informations contenues dans le tableau de qualification de bande.

Lorsque vous connectez un lecteur de bande au système de stockage, il recherche un ID de fournisseur et un ID de produit correspondant entre les informations obtenues lors de la détection de bande et les informations de la table de qualification de bande interne. Si le système de stockage détecte une correspondance, il marque le lecteur de bande comme étant qualifié et peut accéder au lecteur de bande. Si le système de stockage ne trouve pas de correspondance, le lecteur de bande reste dans l'état non qualifié et n'est pas accessible.

Présentation des lecteurs de bande

Présentation des lecteurs de bande

Un lecteur de bande est une représentation d'un lecteur de bande. Il s'agit d'une combinaison spécifique de type de rembobinage et de capacité de compression d'un lecteur de bande.

Un périphérique de bande est créé pour chaque combinaison de type de rembobinage et de capacité de compression. Par conséquent, un lecteur de bande ou une bibliothèque de bandes peut avoir plusieurs périphériques de bande qui lui sont associés. Vous devez spécifier un périphérique de bande pour déplacer, écrire ou lire des bandes.

Lorsque vous installez un lecteur de bande ou une bibliothèque de bandes sur un système de stockage,

ONTAP crée des unités de bande associées au lecteur de bande ou à la bibliothèque de bandes.

ONTAP détecte les lecteurs de bandes et les bibliothèques de bandes et leur attribue des numéros logiques et des lecteurs de bandes. ONTAP détecte les lecteurs et librairies de bandes Fibre Channel, SAS et SCSI parallèle lorsqu'ils sont connectés aux ports d'interface. ONTAP détecte ces disques lorsque leurs interfaces sont activées.

Format du nom du périphérique de bande

Chaque unité de bande possède un nom associé qui apparaît dans un format défini. Le format inclut des informations sur le type de périphérique, le type de rembobinage, l'alias et le type de compression.

Le format d'un nom de périphérique de bande est le suivant :

`rewind_type st alias_number compression_type`

`rewind_type` est le type de rembobinage.

La liste suivante décrit les différentes valeurs de type de rembobinage :

- **r**

  ONTAP rembobinait la bande après avoir fini d'écrire le fichier de bande.

- **nr**

  ONTAP ne rembobinait pas la bande après avoir terminé l'écriture du fichier de bande. Vous devez utiliser ce type de rembobinage pour écrire plusieurs fichiers de bande sur la même bande.

- **ur**

  Il s'agit du type de rembobinage de déchargement/rechargement. Lorsque vous utilisez ce type de rembobinage, la bibliothèque de bandes décharge la bande lorsqu'elle atteint la fin d'un fichier de bande, puis charge la bande suivante, s'il en existe une.

  Vous devez utiliser ce type de rembobinage uniquement dans les cas suivants :

  - Le lecteur de bande associé à ce périphérique se trouve dans une bibliothèque de bandes ou dans un changeur de support en mode bibliothèque.
  - Le lecteur de bande associé à ce périphérique est connecté à un système de stockage.
  - Le nombre de bandes suffisant pour l'opération que vous effectuez est disponible dans la séquence de bandes de bibliothèque définie pour ce lecteur de bande.

> Si vous enregistrez une bande à l'aide d'un périphérique sans rembobinage, vous devez rembobiner la bande avant de la lire.

`st` est la désignation standard pour un lecteur de bande.

`alias_number` Est l'alias attribué par ONTAP au lecteur de bande. Lorsque ONTAP détecte un nouveau lecteur de bande, ONTAP attribue un alias au lecteur de bande.

`compression_type` est un code spécifique au lecteur pour la densité des données sur la bande et le type de

compression.

La liste suivante décrit les différentes valeurs de `compression_type`:

- **a**

  Compression la plus élevée

- **h**

  Compression élevée

- **m**

  Compression moyenne

- **l**

  Compression faible

Exemples

`nrst0a` spécifie un périphérique sans rembobinage sur le lecteur de bande 0 en utilisant la compression la plus élevée.

Exemple de liste des lecteurs de bande

L'exemple suivant illustre les périphériques de bande associés à HP Ultrium 2-SCSI :

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,        format is: HP (200GB)
nrst0l -  no rewind device,     format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,        format is: HP (200GB)
nrst0m -  no rewind device,     format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,        format is: HP (200GB)
nrst0h -  no rewind device,     format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,        format is: HP (400GB w/comp)
nrst0a -  no rewind device,     format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

La liste suivante décrit les abréviations présentées dans l'exemple précédent :

- Go—gigaoctets ; il s'agit de la capacité de la bande.
- avec compression ; indique la capacité de bande avec compression.

Nombre de périphériques de bande simultanés pris en charge

ONTAP prend en charge un maximum de 64 connexions simultanées de lecteurs de

bande, 16 changeurs de taille moyenne et 16 dispositifs de pont ou de routeur pour chaque système de stockage (par nœud) dans n'importe quelle combinaison de connexions Fibre Channel, SCSI ou SAS.

Les lecteurs de bandes ou les changeurs de taille moyenne peuvent être des périphériques dans des bibliothèques de bandes physiques ou virtuelles ou des périphériques autonomes.

> Bien qu'un système de stockage puisse détecter 64 connexions de lecteur de bande, le nombre maximal de sessions de sauvegarde et de restauration pouvant être exécutées simultanément dépend des limites d'évolutivité du moteur de sauvegarde.

Informations associées

Limite d'évolutivité pour les sessions de sauvegarde et de restauration

Crénelage de l'adhésif

Présentation de l'alias de bande

Le crénelage simplifie le processus d'identification du dispositif. Le crénelage lie un nom de chemin physique (PPN) ou un numéro de série (SN) d'une bande ou d'un changeur de support à un nom d'alias persistant mais modifiable.

Le tableau suivant décrit comment le repliement de bande vous permet de vous assurer qu'un lecteur de bande (ou une bibliothèque de bandes ou un changeur de support) est toujours associé à un nom d'alias unique :

Scénario	Réaffectation de l'alias
Lorsque le système redémarre	Le lecteur de bande est automatiquement réaffecté à son alias précédent.
Lorsqu'un périphérique de bande se déplace vers un autre port	L'alias peut être réglé pour pointer vers la nouvelle adresse.
Lorsque plusieurs systèmes utilisent un lecteur de bande particulier	L'utilisateur peut définir l'alias de manière à ce qu'il soit identique pour tous les systèmes.

> Lorsque vous effectuez une mise à niveau de Data ONTAP 8.1.x vers Data ONTAP 8.2.x, la fonction d'alias de bande de Data ONTAP 8.2.x modifie les noms d'alias de bande existants. Dans ce cas, vous devrez peut-être mettre à jour les noms d'alias de bande dans l'application de sauvegarde.

L'attribution d'alias de bande fournit une correspondance entre les noms logiques des périphériques de sauvegarde (par exemple st0 ou mc1) et un nom attribué de façon permanente à un port, un lecteur de bande ou un chargeur de support.

> st0 et st00 sont des noms logiques différents.

> Les noms logiques et les numéros de série sont utilisés uniquement pour accéder à un périphérique. Une fois le périphérique accédé, il renvoie tous les messages d'erreur en utilisant le nom du chemin physique.

Il existe deux types de noms disponibles pour le changement de dénomination : le nom du chemin physique et le numéro de série.

Quels sont les noms de chemin physique

Les noms de chemin physique (PPN) sont les séquences d'adresses numériques que ONTAP attribue aux lecteurs de bande et aux bibliothèques de bandes en fonction de l'adaptateur ou du commutateur SCSI-2/3 (emplacement spécifique) qu'ils sont connectés au système de stockage. Les noms PPN sont également appelés noms électriques.

Les PPN des périphériques connectés directement utilisent le format suivant : `host_adapter.device_id_lun`

> La valeur LUN s'affiche uniquement pour les unités de bande et de changeur de support dont les valeurs LUN ne sont pas nulles, c'est-à-dire si la valeur LUN est zéro `lun` Une partie du PPN n'est pas affichée.

Par exemple, le PPN 8.6 indique que le numéro de l'adaptateur hôte est 8, que l'ID du périphérique est 6 et que le numéro de l'unité logique (LUN) est 0.

Les lecteurs de bande SAS sont également des périphériques à connexion directe. Par exemple, le PPN 5c.4 indique que dans un système de stockage, l'adaptateur HBA SAS est connecté à l'emplacement 5, la bande SAS est connectée au port C de l'adaptateur HBA SAS et l'ID du périphérique est 4.

Les PPN des périphériques connectés par commutateur Fibre Channel utilisent le format suivant : `switch:port_id.device_id_lun`

Par exemple, le PPN MY_SWITCH:5.3L2 indique que le lecteur de bande connecté au port 5 d'un commutateur appelé MY_SWITCH est défini avec l'ID de périphérique 3 et possède la LUN 2.

La LUN (numéro d'unité logique) est déterminée par le lecteur. Les bibliothèques et lecteurs de bande SCSI, Fibre Channel et les disques possèdent des PPN.

Les PPN des lecteurs de bande et des bibliothèques ne changent pas, sauf si le nom du commutateur change, que le lecteur de bande ou la bibliothèque se déplace ou que le lecteur de bande ou la bibliothèque est reconfiguré. Les PPN restent inchangés après le redémarrage. Par exemple, si un lecteur de bande nommé MY_SWITCH:5.3L2 est retiré et qu'un nouveau lecteur de bande avec le même ID de périphérique et le même LUN est connecté au port 5 du commutateur MY_SWITCH, le nouveau lecteur de bande sera accessible à l'aide DE MY_SWITCH:5.3L2.

Quels sont les numéros de série

Un numéro de série (SN) est un identifiant unique pour un lecteur de bande ou un chargeur de support. ONTAP génère des alias basés sur SN à la place du WWN.

Comme le SN est un identifiant unique pour un lecteur de bande ou un chargeur de support, l'alias reste le même quel que soit le chemin de connexion multiple vers le lecteur de bande ou le changeur de support. Les

systèmes de stockage peuvent ainsi suivre le même lecteur de bande ou le même changeur de support dans une configuration de librairie de bandes.

Le numéro de série d'un lecteur de bande ou d'un changeur de support ne change pas même si vous renommez le commutateur Fibre Channel auquel le lecteur de bande ou le changeur de support est connecté. Toutefois, dans une bibliothèque de bandes, si vous remplacez un lecteur de bandes existant par un nouveau, ONTAP génère de nouveaux alias car le numéro de série du lecteur de bande change. De même, si vous déplacez un lecteur de bande existant dans un nouveau slot dans une librairie de bandes ou si vous remappage le LUN du lecteur de bande, ONTAP génère un nouvel alias pour ce lecteur de bande.

> Vous devez mettre à jour les applications de sauvegarde avec les alias nouvellement générés.

Le numéro de série d'un périphérique à bande utilise le format suivant : `SN[xxxxxxxxxx]L[X]`

`x` Est un caractère alphanumérique et un caractère L`X` Est le LUN du périphérique de bande. Si le LUN est 0, le L`X` une partie de la chaîne n'est pas affichée.

Chaque numéro de série comprend jusqu'à 32 caractères ; le format du numéro de série n'est pas sensible à la casse.

Considérations relatives à la configuration de l'accès aux bandes multivoie

Vous pouvez configurer deux chemins à partir du système de stockage pour accéder aux lecteurs de bande dans une bibliothèque de bandes. En cas de défaillance d'un chemin, le système de stockage peut utiliser les autres chemins pour accéder aux lecteurs de bande sans avoir à réparer immédiatement le chemin défaillant. Ainsi, les opérations sur bandes peuvent être redémarrées.

Vous devez tenir compte des éléments suivants lors de la configuration de l'accès aux bandes multivoies à partir de votre système de stockage :

- Dans les bibliothèques de bandes prenant en charge le mappage des LUN, pour l'accès multivoie à un groupe de LUN, le mappage des LUN doit être symétrique sur chaque chemin.

  Les lecteurs de bande et les changeurs de supports sont affectés à des groupes de LUN (ensemble de LUN partageant le même chemin d'accès d'initiateur) dans une bibliothèque de bandes. Tous les lecteurs de bande d'un groupe de LUN doivent être disponibles pour les opérations de sauvegarde et de restauration sur tous les chemins multiples.

- Il est possible de configurer deux chemins au maximum à partir du système de stockage pour accéder aux lecteurs de bande d'une bibliothèque de bandes.
- L'accès aux bandes multivoie prend en charge l'équilibrage de la charge. L'équilibrage de la charge est désactivé par défaut.

Dans l'exemple suivant, le système de stockage accède au groupe LUN 0 via deux chemins d'initiateur : 0b et 0d. Dans ces deux chemins, le groupe de LUN porte le même numéro de LUN, 0, et le nombre de LUN, 5. Le système de stockage accède à la LUN group 1 via un seul chemin d'initiateur, la 3d.

```
STSW-3070-2_cluster::> storage tape library config show

Node                     LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Pour plus d'informations, consultez les pages de manuel.

Comment ajouter des lecteurs de bande et des bibliothèques aux systèmes de stockage

Vous pouvez ajouter des lecteurs de bandes et des bibliothèques au système de stockage de façon dynamique (sans mettre le système de stockage hors ligne).

Lorsque vous ajoutez un nouveau chargeur de support, le système de stockage détecte sa présence et l'ajoute à la configuration. Si le chargeur de support est déjà référencé dans les informations d'alias, aucun nouveau nom logique n'est créé. Si la bibliothèque n'est pas référencée, le système de stockage crée un nouvel alias pour le changeur de support.

Dans une configuration de librairie de bandes, vous devez configurer un lecteur de bande ou un changeur de support sur la LUN 0 d'un port cible pour ONTAP afin de détecter tous les changeurs de support et lecteurs de bande sur ce port cible.

Quelles sont les réservations sur bandes

Plusieurs systèmes de stockage peuvent partager l'accès aux lecteurs de bande, aux changeurs de taille moyenne, aux ponts ou aux bibliothèques de bandes. Les réservations sur bande garantissent qu'un seul système de stockage accède à un périphérique à un moment donné en activant soit le mécanisme de réserve/libération SCSI, soit les réservations permanentes SCSI pour tous les lecteurs de bande, les changeurs de taille moyenne, les ponts et les bibliothèques de bandes.

> Tous les systèmes qui partagent des périphériques dans une bibliothèque, qu'ils soient impliqués ou non, doivent utiliser la même méthode de réservation.

Le mécanisme de réserve/libération SCSI pour la réservation des périphériques fonctionne bien dans des conditions normales. Cependant, durant les procédures de récupération des erreurs de l'interface, les réservations peuvent être perdues. Dans ce cas, les initiateurs autres que le propriétaire réservé peuvent accéder au périphérique.

Les réservations effectuées avec SCSI persistent Reservations ne sont pas affectées par les mécanismes de récupération d'erreurs, tels que la réinitialisation de boucle ou la réinitialisation de la cible ; cependant, tous les périphériques n'implémentent pas correctement les réservations permanentes SCSI.

Transférer des données à l'aide de ndmpcopy

Transférer des données à l'aide de la vue d'ensemble ndmpcopy

Le `ndmpcopy` La commande nodeshell transfère les données entre les systèmes de stockage qui prennent en charge NDMP v4. Vous pouvez effectuer des transferts de données complets et incrémentiels. Vous pouvez transférer des volumes complets ou partiels, des qtrees, des répertoires ou des fichiers individuels.

Description de la tâche

Avec ONTAP 8.x et les versions antérieures, les transferts incrémentiels sont limités à deux niveaux au maximum (une sauvegarde complète et jusqu'à deux sauvegardes incrémentielles).

Depuis la version ONTAP 9.0 et les versions ultérieures, les transferts incrémentiels se limitent à neuf niveaux maximum (une sauvegarde complète et jusqu'à neuf sauvegardes incrémentielles).

Vous pouvez exécuter `ndmpcopy` à la ligne de commande nodeshell des systèmes de stockage source et de destination, ou d'un système de stockage qui n'est ni la source ni la destination du transfert de données. Vous pouvez également exécuter `ndmpcopy` sur un système de stockage unique qui est à la fois la source et la destination du transfert de données.

Vous pouvez utiliser les adresses IPv4 ou IPv6 des systèmes de stockage source et de destination dans `ndmpcopy` commande. Le format du chemin d'accès est `/vserver_name/volume_name \[path\]`.

Étapes

1. Activer le service NDMP sur les systèmes de stockage source et cible :

Si vous effectuez le transfert des données à la source ou à la destination dans…	Utiliser la commande suivante…
Mode SVM-scoped NDMP	`vserver services ndmp on` Pour l'authentification NDMP au SVM admin, le compte utilisateur est `admin` et le rôle de l'utilisateur est `admin` ou `backup`. Au sein de la SVM de données, le compte utilisateur est `vsadmin` et le rôle de l'utilisateur est `vsadmin` ou `vsadmin-backup` rôle.
Mode node-scoped NDMP	`system services ndmp on`

2. Transfert de données au sein d'un système de stockage ou entre des systèmes de stockage utilisant le `ndmpcopy` commande au nodeshell :

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

> Les noms DNS ne sont pas pris en charge dans ndmpcopy. Vous devez fournir l'adresse IP de la source et de la destination. L'adresse de bouclage (127.0.0.1) n'est pas prise en charge pour l'adresse IP source ou l'adresse IP de destination.

- Le `ndmpcopy` commande détermine le mode d'adresse pour les connexions de contrôle comme suit :
  - Le mode d'adresse pour la connexion de contrôle correspond à l'adresse IP fournie.
  - Vous pouvez remplacer ces règles à l'aide du `-mcs` et `-mcd` options.
- Si la source ou la destination est le système ONTAP, selon le mode NDMP (node-scoped ou SVM-scoped), utiliser une adresse IP permettant d'accéder au volume cible.
- `source_path` et `destination_path` sont les noms de chemin absolus jusqu'au niveau granulaire du volume, qtree, répertoire ou fichier.
- `-mcs` spécifie le mode d'adressage préféré pour la connexion de contrôle au système de stockage source.

  `inet` Indique un mode d'adresse IPv4 et `inet6` Indique un mode d'adresse IPv6.

- `-mcd` spécifie le mode d'adressage préféré pour la connexion de contrôle au système de stockage de destination.

  `inet` Indique un mode d'adresse IPv4 et `inet6` Indique un mode d'adresse IPv6.

- `-md` spécifie le mode d'adressage préféré pour les transferts de données entre les systèmes de stockage source et de destination.

  `inet` Indique un mode d'adresse IPv4 et `inet6` Indique un mode d'adresse IPv6.

  Si vous n'utilisez pas le `-md` dans le `ndmpcopy` commande, le mode d'adressage de la connexion de données est déterminé comme suit :

  - Si l'une des adresses spécifiées pour les connexions de contrôle est une adresse IPv6, le mode d'adresse de la connexion de données est IPv6.
  - Si les deux adresses spécifiées pour les connexions de contrôle sont des adresses IPv4, le `ndmpcopy` La commande tente d'abord de passer en mode d'adresse IPv6 pour la connexion de données.

    Si cela échoue, la commande utilise un mode d'adresse IPv4.

    > Une adresse IPv6, si elle est spécifiée, doit être entre crochets.

    Cet exemple de commande migre les données d'un chemin source (`source_path`) vers un chemin de destination (`destination_path`).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
Cet exemple de commande définit explicitement les connexions de contrôle et la connexion de données pour utiliser le mode d'adresse IPv6 :

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Options de la commande ndmpcopy

Il est important de connaître les options disponibles pour le `ndmpcopy` nodeshell commande pour le transfert des données réussi.

Le tableau suivant répertorie les options disponibles. Pour plus d'informations, reportez-vous à la section `ndmpcopy` pages man disponibles via le nodeshell.

Option	Description
`-sa` `username`:[`password`]	Cette option définit le nom d'utilisateur et le mot de passe d'authentification source pour la connexion au système de stockage source. Cette option est obligatoire. Pour un utilisateur sans privilège admin, vous devez spécifier le mot de passe spécifique NDMP généré par le système de l'utilisateur. Le mot de passe généré par le système est obligatoire pour les utilisateurs admin et non-admin.
`-da` `username`:[`password`]	Cette option définit le nom d'utilisateur et le mot de passe d'authentification de destination pour la connexion au système de stockage de destination. Cette option est obligatoire.
`-st` {`md5`	`text`}
Cette option définit le type d'authentification source à utiliser lors de la connexion au système de stockage source. Il s'agit d'une option obligatoire. L'utilisateur doit donc fournir l'une ou l'autre `text` ou `md5` option.	`-dt` {`md5`

Option	Description
`text}`	Cette option définit le type d'authentification de destination à utiliser lors de la connexion au système de stockage de destination.
`-l`	Cette option définit le niveau de vidage utilisé pour le transfert vers la valeur spécifiée de niveau.les valeurs valides sont `0`, `1`, à `9`, où `0` indique un transfert complet et `1` à `9` spécifie un transfert incrémentiel. La valeur par défaut est `0`.
`-d`	Cette option permet de générer des messages de journal de débogage ndmpcopy. Les fichiers journaux de débogage ndmpcopy se trouvent dans le `/mroot/etc/log` volume racine. Les noms des fichiers journaux de débogage ndmpcopy se trouvent dans le `ndmpcopy.yyyymmdd` format.
`-f`	Cette option active le mode forcé. Ce mode permet d'écraser les fichiers système dans `/etc` Répertoire à la racine du volume 7-mode.
`-h`	Cette option imprime le message d'aide.
`-p`	Cette option vous invite à saisir le mot de passe pour l'autorisation source et de destination. Ce mot de passe remplace le mot de passe spécifié pour `-sa` et `-da` options. Vous ne pouvez utiliser cette option que lorsque la commande s'exécute dans une console interactive.
`-exclude`	Cette option exclut les fichiers ou répertoires spécifiés du chemin spécifié pour le transfert de données. Cette valeur peut être une liste séparée par des virgules de noms de répertoire ou de fichier tels que **`.pst`** `ou .txt`.

NDMP pour volumes FlexVol

À propos de NDMP pour volumes FlexVol

Le protocole Network Data Management Protocol (NDMP) est un protocole standardisé pour contrôler la sauvegarde, la restauration et d'autres types de transfert de données entre les périphériques de stockage primaire et secondaire, tels que les systèmes de stockage et les librairies de bandes.

En activant la prise en charge NDMP sur un système de stockage, vous permettez à ce système de stockage de communiquer avec les applications de sauvegarde NAS compatibles NDMP (également appelées *Data Management applications* ou *DMA*), les serveurs de données et les serveurs de bandes participant aux opérations de sauvegarde ou de restauration. Toutes les communications réseau sont effectuées sur le réseau TCPIP ou TCP/IPv6. NDMP offre également un contrôle bas niveau des lecteurs de bandes et des changeurs de taille moyenne.

Il est possible d'effectuer des opérations de sauvegarde sur bande et de restauration en mode node-scoped NDMP ou SVM (Storage Virtual machine) scoped NDMP.

Vous devez tenir compte des considérations à prendre en compte lors de l'utilisation du protocole NDMP, de la liste des variables d'environnement et des topologies de sauvegarde sur bande NDMP prises en charge. Vous pouvez également activer ou désactiver la fonctionnalité DAR améliorée. Les deux méthodes d'authentification prises en charge par ONTAP pour l'authentification de l'accès NDMP sur un système de stockage sont : texte clair et défi.

Informations associées

Variables d'environnement prises en charge par ONTAP

À propos des modes de fonctionnement NDMP

Vous pouvez effectuer des opérations de sauvegarde sur bande et de restauration au niveau du nœud ou du SVM (Storage Virtual machine). Pour réaliser correctement ces opérations au niveau du SVM, le service NDMP doit être activé sur la SVM.

Si vous effectuez une mise à niveau de Data ONTAP 8.2 vers Data ONTAP 8.3, le mode d'opération NDMP utilisé dans 8.2 sera conservé après la mise à niveau de 8.2 à 8.3.

Si vous installez un nouveau cluster avec Data ONTAP 8.2 ou version ultérieure, NDMP est en mode SVM-scoped NDMP par défaut. Pour effectuer des opérations de sauvegarde sur bande et de restauration en mode node-scoped NDMP, vous devez activer de façon explicite le mode node-scoped NDMP.

Informations associées

Commandes permettant de gérer le mode node-scoped NDMP

Gérer le mode NDMP node-scoped pour les volumes FlexVol

Gérer le mode SVM-scoped NDMP pour les volumes FlexVol

Le mode node-scoped NDMP est

En mode node-scoped NDMP, vous pouvez effectuer des opérations de backup sur bande et restore au niveau du noeud. Le mode d'opération NDMP utilisé dans Data ONTAP 8.2 reste conservé après la mise à niveau de 8.2 à 8.3.

En mode node-scoped NDMP, vous pouvez effectuer des opérations de backup sur bande et restore sur un noeud propriétaire du volume. Pour effectuer ces opérations, vous devez établir des connexions de contrôle NDMP sur une LIF hébergée sur le nœud qui détient le volume ou les lecteurs de bande.

Ce mode est obsolète et sera supprimé dans une prochaine version majeure.

Informations associées

Gérer le mode NDMP node-scoped pour les volumes FlexVol

Le mode SVM-scoped NDMP est

Vous pouvez réaliser des opérations de sauvegarde sur bande et de restauration au niveau des SVM (Storage Virtual machine) si le service NDMP est activé sur la SVM. Vous pouvez sauvegarder et restaurer tous les volumes hébergés sur différents nœuds du SVM d'un cluster si l'application de sauvegarde prend en charge l'extension CAB.

Une connexion de contrôle NDMP peut être établie sur différents types de LIF. En mode SVM-scoped NDMP, ces LIFs appartiennent au SVM de données ou au SVM admin. La connexion peut être établie sur une LIF uniquement si le service NDMP est activé sur le SVM qui possède cette LIF.

Une LIF de données appartient au SVM de données et au LIF intercluster, ainsi qu'au LIF node-management et au LIF cluster-management appartient au SVM admin.

En mode SVM-scoped NDMP, la disponibilité des volumes et des dispositifs sur bande pour les opérations de backup et restore dépend du type de LIF sur lequel la connexion NDMP control est établie et de l'état de l'extension CAB. Si votre application de sauvegarde prend en charge l'extension CAB et qu'un volume et le périphérique de bande partagent la même affinité, alors l'application de sauvegarde peut effectuer une opération de sauvegarde ou de restauration locale, au lieu d'une opération de sauvegarde ou de restauration à trois voies.

Informations associées

Gérer le mode SVM-scoped NDMP pour les volumes FlexVol

Considérations relatives à l'utilisation de NDMP

Lorsque vous démarrez le service NDMP sur votre système de stockage, vous devez prendre en compte un certain nombre de considérations.

- Chaque nœud prend en charge jusqu'à 16 sauvegardes, restaurations ou combinaisons de les deux à l'aide de lecteurs de bande connectés.
- Les services NDMP peuvent générer des données d'historique de fichiers à la demande des applications de sauvegarde NDMP.

  L'historique des fichiers est utilisé par les applications de sauvegarde pour permettre la restauration optimisée de sous-ensembles de données sélectionnés à partir d'une image de sauvegarde. La génération et le traitement de l'historique des fichiers peuvent s'avérer chronophages et nécessitent beaucoup de ressources CPU pour le système de stockage et l'application de sauvegarde.

  SMTape ne prend pas en charge l'historique des fichiers.

  Si la protection de vos données est configurée pour la reprise après incident, où l'image de sauvegarde complète sera récupérée, vous pouvez désactiver la génération de l'historique des fichiers pour réduire le temps de sauvegarde. Consultez la documentation de votre application de sauvegarde pour déterminer s'il est possible de désactiver la génération de l'historique du fichier NDMP.

- La politique de pare-feu pour NDMP est activée par défaut sur tous les types LIF.
- En mode node-scoped NDMP, la sauvegarde d'un volume FlexVol nécessite que vous utilisiez l'application de backup pour initier une sauvegarde sur un nœud propriétaire du volume.

Toutefois, vous ne pouvez pas sauvegarder un volume racine de nœud.

- Vous pouvez effectuer une sauvegarde NDMP à partir de n'importe quelle LIF, comme le permettent les politiques de pare-feu.

  Si vous utilisez une LIF de données, vous devez sélectionner une LIF qui n'est pas configurée pour le basculement. Si une LIF de données bascule lors d'une opération NDMP, l'opération NDMP échoue et doit être de nouveau exécutée.

- En mode node-scoped NDMP et Storage Virtual machine (SVM) scoped NDMP sans support d'extension CAB, la connexion de données NDMP utilise le même LIF que la connexion NDMP control.
- Au cours de la migration de LIF, les opérations régulières de sauvegarde et de restauration sont interrompues.

  Vous devez lancer les opérations de sauvegarde et de restauration après la migration LIF.

- Le chemin de sauvegarde NDMP est du format `/vserver_name/volume_name/path_name`.

  `path_name` Est facultatif et spécifie le chemin d'accès au répertoire, au fichier ou à la copie Snapshot.

- Lorsqu'une destination SnapMirror est sauvegardée sur bande à l'aide du moteur de dump, seules les données du volume sont sauvegardées.

  Toutefois, lorsqu'une destination SnapMirror est sauvegardée sur bande à l'aide de SMTape, les métadonnées sont également sauvegardées. Les relations SnapMirror et les métadonnées associées ne sont pas sauvegardées sur bande. Dès lors, pendant la restauration, seules les données de ce volume sont restaurées, mais les relations SnapMirror associées ne sont pas restaurées.

Informations associées

Rôle de l'extension Cluster Aware Backup

"Concepts relatifs à ONTAP"

"Administration du système"

Variable d'environnement

Présentation des variables d'environnement

Les variables d'environnement servent à communiquer des informations sur une opération de sauvegarde ou de restauration entre une application de sauvegarde NDMP et un système de stockage.

Par exemple, si un utilisateur indique qu'une application de sauvegarde doit effectuer une sauvegarde `/vserver1/vol1/dir1`, L'application de sauvegarde définit la variable d'environnement DU SYSTÈME DE FICHIERS sur `/vserver1/vol1/dir1`. De même, si un utilisateur spécifie qu'une sauvegarde doit être une sauvegarde de niveau 1, l'application de sauvegarde définit la variable d'environnement DE NIVEAU sur 1 (une).

> La définition et l'examen des variables d'environnement sont généralement transparents pour les administrateurs de sauvegarde, c'est-à-dire que l'application de sauvegarde les définit automatiquement.

Un administrateur de sauvegarde spécifie rarement des variables d'environnement. Il est toutefois préférable de modifier la valeur d'une variable d'environnement dans cette variable définie par l'application de sauvegarde pour caractériser ou contourner un problème de fonctionnement ou de performances. Par exemple, un administrateur peut désactiver temporairement la génération de l'historique des fichiers pour déterminer si le traitement par l'application de sauvegarde des informations de l'historique des fichiers contribue à des problèmes de performances ou à des problèmes fonctionnels.

De nombreuses applications de sauvegarde offrent un moyen de remplacer ou de modifier des variables d'environnement ou de spécifier des variables d'environnement supplémentaires. Pour plus d'informations, consultez la documentation de votre application de sauvegarde.

Variables d'environnement prises en charge par ONTAP

Les variables d'environnement servent à communiquer des informations sur une opération de sauvegarde ou de restauration entre une application de sauvegarde NDMP et un système de stockage. ONTAP prend en charge les variables d'environnement qui ont une valeur par défaut associée. Toutefois, vous pouvez modifier manuellement ces valeurs par défaut.

Si vous modifiez manuellement les valeurs définies par l'application de sauvegarde, il se peut que l'application se comporte de façon imprévisible. En effet, les opérations de sauvegarde ou de restauration ne peuvent pas faire ce que l'application de sauvegarde attend d'elles. Mais dans certains cas, une modification judicieuse pourrait aider à identifier ou à gérer des problèmes.

Les tableaux ci-dessous répertorient les variables d'environnement dont le comportement est commun à dump et SMTape, ainsi que les variables prises en charge uniquement pour dump et SMTape. Ces tableaux contiennent également des descriptions du fonctionnement des variables d'environnement prises en charge par ONTAP, le cas échéant :

> Dans la plupart des cas, les variables qui ont la valeur, `Y` accepter également `T` et `N` accepter également `F`.

Variables d'environnement prises en charge pour dump et SMTape

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
DÉBOGAGE	`Y` ou `N`	`N`	Spécifie que les informations de débogage sont imprimées.
SYSTÈME DE FICHIERS	`string`	`none`	Indique le chemin d'accès de la racine des données en cours de sauvegarde.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
NDMP_VERSION	`return_only`	`none`	Vous ne devez pas modifier la variable NDMP_VERSION. Créée par l'opération de sauvegarde, la variable NDMP_VERSION renvoie la version NDMP. ONTAP définit la variable NDMP_VERSION lors d'une sauvegarde à des fins d'utilisation interne et de la transmission à une application de sauvegarde à titre d'information. La version NDMP d'une session NDMP n'est pas définie avec cette variable.
SÉPARATEUR_CHEMIN	`return_value`	`none`	Spécifie le caractère séparateur de nom de chemin d'accès. Ce caractère dépend du système de fichiers à sauvegarder. Pour ONTAP, le caractère "/" est attribué à cette variable. Le serveur NDMP définit cette variable avant de démarrer une opération de sauvegarde sur bande.
TYPE	`dump` ou `smtape`	`dump`	Indique le type de sauvegarde pris en charge pour effectuer des opérations de sauvegarde et de restauration sur bande.
PROLIXE	`Y` ou `N`	`N`	Augmente les messages du journal lors de l'exécution d'une opération de sauvegarde sur bande ou de restauration.

Variables d’environnement prises en charge pour dump

Variable d’environnement	Valeurs valides	Valeur par défaut	Description
ACL_START	`return_only`	`none`	Créée par l’opération de sauvegarde, la variable ACL_START est une valeur de décalage utilisée par une opération de restauration à accès direct ou de sauvegarde NDMP redémarrable. La valeur de décalage est le décalage d’octet dans le fichier de vidage où les données ACL (Pass V) commencent et sont renvoyées à la fin d’une sauvegarde. Pour qu’une opération de restauration d’accès direct restaure correctement les données sauvegardées, la valeur ACL_START doit être transmise à l’opération de restauration lorsqu’elle démarre. Une opération de sauvegarde NDMP redémarrable utilise la valeur ACL_START pour communiquer à l’application de sauvegarde où la partie non redémarrable du flux de sauvegarde commence.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
DATE_DE_BASE	`0`, `-1`, ou `DUMP_DATE` valeur	`-1`	Spécifie la date de début des sauvegardes incrémentielles. Lorsqu'il est réglé sur `-1`, LE spécificateur incrémentiel BASE_DATE est désactivé. Lorsqu'il est réglé sur `0` sur une sauvegarde de niveau 0, les sauvegardes incrémentielles sont activées. Après la sauvegarde initiale, la valeur de la variable DUMP_DATE de la sauvegarde incrémentielle précédente est affectée à la variable BASE_DATE. Ces variables constituent une alternative aux sauvegardes incrémentielles BASÉES SUR LE NIVEAU/MISE À JOUR.
DIRECTE	`Y` ou `N`	`N`	Indique qu'une restauration doit être envoyée rapidement vers l'emplacement de la bande sur lequel se trouvent les données du fichier au lieu d'analyser la bande entière. Pour que la restauration puisse fonctionner, l'application de sauvegarde doit fournir des informations de positionnement. Si cette variable est définie sur `Y`, l'application de sauvegarde indique les noms de fichier ou de répertoire et les informations de positionnement.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
NOM_DMP	`string`	`none`	Indique le nom d'une sauvegarde de plusieurs sous-arborescences. Cette variable est obligatoire pour les sauvegardes de plusieurs sous-arborescences.
DUMP_DATE	`return_value`	`none`	Vous ne modifiez pas cette variable directement. Elle est créée par la sauvegarde si la variable BASE_DATE est définie sur une valeur autre que `-1`. La variable DUMP_DATE est dérivée par la préattente de la valeur de niveau 32 bits vers une valeur de temps de 32 bits calculée par le logiciel dump. Le niveau est incrémenté à partir de la valeur du dernier niveau passée dans la variable BASE_DATE. La valeur obtenue est utilisée comme valeur BASE_DATE sur une sauvegarde incrémentielle ultérieure.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
ENHANCED_DAR_ENABLED	`Y` ou `N`	`N`	Indique si la fonctionnalité DAR améliorée est activée. La fonctionnalité DAR améliorée prend en charge les fichiers de DAR et DAR avec les flux NT. Elle permet d'améliorer les performances. La DAR améliorée pendant la restauration n'est possible que si les conditions suivantes sont remplies : • ONTAP prend en charge les applications de DAR optimisées. • L'historique des fichiers est activé (HIST=y) pendant la sauvegarde. • Le `ndmpd.offset_map.enable` l'option est définie sur `on`. • LA variable ENHANCED_DAR_ENABLED est définie sur `Y` pendant la restauration.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
EXCLURE	`pattern_string`	`none`	Spécifie les fichiers ou les répertoires qui sont exclus lors de la sauvegarde des données. La liste d'exclusion est une liste séparée par des virgules de noms de fichier ou de répertoire. Si le nom d'un fichier ou d'un répertoire correspond à l'un des noms de la liste, il est exclu de la sauvegarde. Les règles suivantes s'appliquent lors de la spécification de noms dans la liste d'exclusion : • Le nom exact du fichier ou répertoire doit être utilisé. • L'astérisque (*), caractère générique, doit être le premier ou le dernier caractère de la chaîne. Chaque chaîne peut comporter jusqu'à deux astérisques. • Une virgule dans un fichier ou un nom de répertoire doit être précédée d'une barre oblique inverse. • La liste d'exclusion peut contenir jusqu'à 32 noms.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
EXTRAIRE	`Y`, `N`, ou `E`	`N`	Indique que les sous-arborescences d'un ensemble de données sauvegardées doivent être restaurées. L'application de sauvegarde spécifie les noms des sous-arborescences à extraire. Si un fichier spécifié correspond à un répertoire dont le contenu a été sauvegardé, le répertoire est extrait de façon récursive. Pour renommer un fichier, un répertoire ou un qtree pendant la restauration sans utiliser DAR, vous devez définir la variable d'environnement D'EXTRACTION sur `E`.
EXTRAIRE_ACL	`Y` ou `N`	`Y`	Spécifie que les listes de contrôle d'accès du fichier sauvegardé sont restaurées lors d'une opération de restauration. La valeur par défaut est de restaurer les listes de contrôle d'accès lors de la restauration des données, à l'exception de DDARS (DIRECT=y).

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
DE FORCE	`Y` ou `N`	`N`	Détermine si l'opération de restauration doit vérifier l'espace du volume et la disponibilité des inode sur le volume de destination. Réglage de cette variable sur `Y` provoque l'opération de restauration pour ignorer les vérifications de l'espace volume et de la disponibilité d'inode sur le chemin de destination. Si un espace volume suffisant ou des inodes ne sont pas disponibles sur le volume de destination, l'opération de restauration récupère autant de données que l'espace du volume de destination et la disponibilité d'inodes. L'opération de restauration s'arrête lorsque l'espace de volume ou les inodes ne sont pas disponibles.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
HIST	`Y` ou `N`	`N`	Indique que les informations de l'historique des fichiers sont envoyées à l'application de sauvegarde. La plupart des applications de sauvegarde commerciales définissent la variable HIST sur `Y`. Si vous voulez augmenter la vitesse d'une opération de sauvegarde ou si vous voulez résoudre un problème avec la collecte de l'historique de fichiers, vous pouvez définir cette variable sur `N`. Vous ne devez pas définir la variable HIST sur `Y` si l'application de sauvegarde ne prend pas en charge l'historique des fichiers.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
IGNORE_CTIME	`Y` ou `N`	`N`	Spécifie qu'un fichier n'est pas sauvegardé de façon incrémentielle si seule sa valeur de temps de restauration a changé depuis la sauvegarde incrémentielle précédente. Certaines applications, telles que les logiciels d'analyse antivirus, modifient la valeur de temps de lecture d'un fichier au sein de l'inode, même si le fichier ou ses attributs n'ont pas changé. Par conséquent, une sauvegarde incrémentielle peut sauvegarder des fichiers qui n'ont pas été modifiés. Le `IGNORE_CTIME` variable ne doit être spécifiée que si les sauvegardes incrémentielles prennent une quantité de temps ou d'espace inacceptable car la valeur de temps de ctime a été modifiée. Le `NDMP dump` jeux de commandes `IGNORE_CTIME` à `false` par défaut. Réglage sur `true` peut entraîner la perte de données suivante : 1. Si `IGNORE_CTIME` est défini sur vrai

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
IGNORE_QTREES	`Y` ou `N`	`N`	Spécifie que l'opération de restauration ne restaure pas les informations qtree à partir de qtrees sauvegardés.
NIVEAU	`0-31`	`0`	Spécifie le niveau de sauvegarde. Le niveau 0 copie l'ensemble du jeu de données. Les niveaux de sauvegarde incrémentielle, spécifiés par les valeurs supérieures à 0, copient tous les fichiers (nouveaux ou modifiés) depuis la dernière sauvegarde incrémentielle. Par exemple, un niveau 1 sauvegarde les fichiers nouveaux ou modifiés depuis la sauvegarde de niveau 0, un niveau 2 sauvegarde les fichiers nouveaux ou modifiés depuis la sauvegarde de niveau 1, etc.
LISTE	`Y` ou `N`	`N`	Répertorie les noms de fichiers sauvegardés et les numéros d'inode sans restaurer les données.
LISTE_QTREE	`Y` ou `N`	`N`	Le répertorie les qtrees sauvegardés sans réellement restaurer les données.

qui sont déplacés via des qtrees sur la source lors de la restauration incrémentielle.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
NOMS_DE_SOUS-ARBRE_MULTIPLES	`string`	`none`	Indique que la sauvegarde est une sauvegarde à plusieurs sous-arborescences. Plusieurs sous-arborescences sont spécifiées dans la chaîne, qui est une liste de noms de sous-arborescences séparées par une nouvelle ligne et comportant des valeurs NULL. Les sous-arbres sont spécifiés par des noms de chemin par rapport à leur répertoire racine commun, qui doivent être spécifiés comme dernier élément de la liste. Si vous utilisez cette variable, vous devez également utiliser la variable DMP_NAME.
NDMP_UNICODE_ FH	`Y` ou `N`	`N`	Indique qu'un nom Unicode est inclus en plus du nom NFS du fichier dans les informations de l'historique des fichiers. Cette option n'est pas utilisée par la plupart des applications de sauvegarde et ne doit pas être définie sauf si l'application de sauvegarde est conçue pour recevoir ces noms de fichiers supplémentaires. La variable HIST doit également être définie.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
NO_ACL	`Y` ou `N`	`N`	Spécifie que les listes de contrôle d'accès ne doivent pas être copiées lors de la sauvegarde des données.
NON_QUOTA_TREE	`Y` ou `N`	`N`	Spécifie que les fichiers et les répertoires des qtrees doivent être ignorés lors de la sauvegarde des données. Lorsqu'il est réglé sur `Y`, Les éléments dans les qtrees du jeu de données spécifié par la variable DE SYSTÈME DE FICHIERS ne sont pas sauvegardés. Cette variable n'a un effet que si la variable FILESYSTEM spécifie un volume entier. La variable NON_QUOTA_TREE fonctionne uniquement sur une sauvegarde de niveau 0 et ne fonctionne pas si LA variable MULTI_SUBTREE_NAMES est spécifiée. ⓘ Les fichiers ou les répertoires spécifiés à exclure pour la sauvegarde ne sont pas exclus si vous définissez NON_QUOTA_TREE sur `Y` simultanément.

Variable d’environnement	Valeurs valides	Valeur par défaut	Description
NON WRITE	`Y` ou `N`	`N`	Spécifie que l’opération de restauration ne doit pas écrire de données sur le disque. Cette variable est utilisée pour le débogage.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
RÉCURSIF	`Y` ou `N`	`Y`	Indique que les entrées de répertoire lors d'une restauration DAR sont développées. Les variables d'environnement DIRECTES et OPTIMISÉES_DAR_ENABLED doivent être activées (définies sur `Y`) également. Si la variable RÉCURSIVE est désactivée (définie sur `N`), seules les autorisations et listes de contrôle d'accès de tous les répertoires du chemin source d'origine sont restaurées à partir de la bande, et non du contenu des répertoires. Si la variable RÉCURSIVE est définie sur `N` Ou LA variable RECOVER_FULL_PATHS est définie sur `Y`, le chemin de récupération doit se terminer par le chemin d'origine.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
RECOVER_FULL_PATHS	`Y` ou `N`	`N`	Indique que le chemin de récupération complet aura ses autorisations et listes de contrôle d'accès restaurées après le DAR. DIRECT et ENHANCED_DAR_ENABLED doivent être activés (défini sur `Y`) également. Si LE paramètre RECOVER_FULL_PATHS est défini sur `Y`, le chemin de récupération doit se terminer par le chemin d'origine. Si des répertoires existent déjà sur le volume de destination, leurs autorisations et listes de contrôle d'accès ne seront pas restaurées à partir d'une bande.
MISE À JOUR	`Y` ou `N`	`Y`	Met à jour les informations de métadonnées pour permettre une sauvegarde incrémentielle BASÉE SUR LE NIVEAU.

Variables d'environnement prises en charge par SMTape

trouvent dans `foo/dir1/deepdir/myfile`:

- `/foo`
- `/foo/dir`
- `/foo/dir1/deepdir`
- `/foo/dir1/deepdir/myfile`

Les chemins de récupération suivants ne sont pas valides :

- `/foo`
- `/foo/dir`

  `/foo/dir1/myfile`

  `/foo/dir2`

-
- /foo/dir2/myfile

Variable d'environnement	Valeurs valides	Valeur par défaut	Description

DATE_DE_BASE	`DUMP_DATE`	`-1`	Spécifie la date de début des sauvegardes incrémentielles.
			
			`` `BASE_DATE` Est une représentation de chaîne des identificateurs d'instantané de référence. À l'aide du `BASE_DATE` String, SMTape localise la copie Snapshot de référence. ``
			
			`` `BASE_DATE` n'est pas requis pour les sauvegardes de base. Pour une sauvegarde incrémentielle, la valeur de `DUMP_DATE` variable de la sauvegarde de base ou incrémentielle précédente est attribuée à `BASE_DATE` variable. ``
			
			L'application de sauvegarde affecte `DUMP_DATE` Valeur d'une copie de base SMTape précédente ou sauvegarde incrémentielle.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
DUMP_DATE	`return_value`	`none`	À la fin d'une sauvegarde SMTape, DUMP_DATE contient un identifiant de chaîne qui identifie la copie Snapshot utilisée pour cette sauvegarde. Cette copie Snapshot peut être utilisée comme copie Snapshot de référence pour une sauvegarde incrémentielle ultérieure. La valeur résultante de DUMP_DATE est utilisée comme valeur BASE_DATE pour les sauvegardes incrémentielles suivantes.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifie la séquence des sauvegardes incrémentielles associées à la sauvegarde de base. L'ID du jeu de sauvegardes est un ID unique de 128 bits généré au cours d'une sauvegarde de base. L'application de sauvegarde attribue cet ID en tant qu'entrée au `SMTAPE_BACKUP_SET_ID` variable pendant une sauvegarde incrémentielle.

Variable d'environnement	Valeurs valides	Valeur par défaut	Description
SMTAPE_SNAPSHOT_NAME	Toute copie Snapshot valide disponible dans le volume	`Invalid`	Lorsque la variable SMTAPE_SNAPSHOT_NAME est définie sur une copie Snapshot, cette copie Snapshot et ses anciennes copies Snapshot sont sauvegardées sur bande. Pour la sauvegarde incrémentielle, cette variable spécifie la copie Snapshot incrémentielle. LA variable BASE_DATE fournit la copie Snapshot de base.
SMTAPE_DELETE_SNAPSHOT	`Y` ou `N`	`N`	Pour une copie Snapshot créée automatiquement par SMTape, lorsque la variable SMTAPE_DELETE_SNAPSHOT est définie sur `Y`, Puis, une fois l'opération de sauvegarde terminée, SMTape supprime cette copie Snapshot. Cependant, une copie Snapshot créée par l'application de sauvegarde ne sera pas supprimée.
SMTAPE_BREAK_MIRROR	`Y` ou `N`	`N`	Lorsque la variable SMTAPE_BREAK_MIRROR est définie sur `Y`, le volume de type `DP` est remplacé par un `RW` volume après une restauration réussie.

Topologies de sauvegarde sur bande NDMP courantes

NDMP prend en charge un certain nombre de topologies et de configurations entre les applications de sauvegarde et les systèmes de stockage ou d'autres serveurs NDMP fournissant des données (systèmes de fichiers) et des services de bande.

Du système de stockage sur bande locale

Dans la configuration la plus simple, une application de sauvegarde sauvegarde sauvegarde sauvegarde sauvegarde des données d'un système de stockage vers un sous-système de bande connecté au système de stockage. Il existe une connexion de contrôle NDMP sur la limite du réseau. La connexion de données NDMP qui existe dans le système de stockage entre les services de données et de bande est appelée configuration locale NDMP.

Système de stockage à bande connecté à un autre système de stockage

Une application de sauvegarde peut également sauvegarder les données d'un système de stockage vers une librairie de bandes (un changeur de moyenne taille avec un ou plusieurs lecteurs de bande) connectée à un autre système de stockage. Dans ce cas, la connexion de données NDMP entre les services de données et de bande est fournie par une connexion réseau TCP ou TCP/IPv6. Il s'agit d'une configuration NDMP à trois voies système de stockage vers stockage.

Bibliothèque de bandes reliée système/réseau de stockage

Les bibliothèques de bandes NDMP fournissent une variante de la configuration à trois voies. Dans ce cas, la bibliothèque de bandes se connecte directement au réseau TCP/IP et communique avec l'application de sauvegarde et le système de stockage par l'intermédiaire d'un serveur NDMP interne.

Système de stockage à serveur de données sur bande ou serveur de données à système de stockage sur bande

NDMP prend également en charge les configurations trivoies entre système de stockage à serveur de données et serveur de données à stockage, bien que ces variantes soient moins largement déployées. Le système de stockage à serveur permet de sauvegarder les données du système de stockage dans une bibliothèque de bandes reliée à l'hôte de l'application de sauvegarde ou à un autre système de serveur de données. La configuration du système de serveur à stockage permet de sauvegarder les données du serveur dans une bibliothèque de bandes reliée au système de stockage.

Méthodes d'authentification NDMP prises en charge

Vous pouvez spécifier une méthode d'authentification pour autoriser les requêtes de connexion NDMP. ONTAP prend en charge deux méthodes d'authentification de l'accès NDMP à un système de stockage : le texte brut et les défis.

En mode node-scoped NDMP, challenge et texte sont tous deux activés par défaut. Toutefois, vous ne pouvez pas désactiver le défi. Vous pouvez activer et désactiver le texte en texte brut. Dans la méthode d'authentification en texte clair, le mot de passe de connexion est transmis en texte clair.

En mode SVM (Storage Virtual machine)-scoped NDMP, la méthode d'authentification est par défaut un défi. Contrairement au mode node-scoped NDMP, dans ce mode, vous pouvez activer et désactiver à la fois les méthodes d'authentification en texte clair et les méthodes d'authentification en question.

Informations associées

Authentification de l'utilisateur en mode node-scoped NDMP

Authentification de l'utilisateur en mode SVM-scoped NDMP

Extensions NDMP prises en charge par ONTAP

NDMP v4 fournit un mécanisme de création d'extensions de protocole NDMP v4 sans modifier le protocole NDMP v4 principal. Vous devez connaître les extensions NDMP v4

prises en charge par ONTAP.

Les extensions NDMP v4 suivantes sont prises en charge par ONTAP :

- Sauvegarde « cluster Aware Backup » (CAB)

  Cette extension n'est supportée que en mode SVM-scoped NDMP.

- Extension d'adresse de connexion (CAE) pour la prise en charge d'IPv6
- Classe d'extension 0x2050

  Cette extension prend en charge les opérations de sauvegarde redémarrables et les extensions de gestion Snapshot.

  Le `NDMP_SNAP_RECOVER` Message, qui fait partie de Snapshot Management Extensions, sert à lancer une opération de restauration et à transférer les données récupérées depuis une copie Snapshot locale vers un emplacement local du système de fichiers. Dans ONTAP, ce message permet de restaurer des volumes et des fichiers standard uniquement.

  Le `NDMP_SNAP_DIR_LIST` Message vous permet de parcourir les copies Snapshot d'un volume. Si une opération sans interruption a lieu pendant une opération de navigation, l'application de sauvegarde doit recommencer l'opération de navigation.

Extension de sauvegarde NDMP redémarrable pour un dump pris en charge par ONTAP

Vous pouvez utiliser la fonctionnalité RBE (NDMP restartable Backup extension) pour redémarrer une sauvegarde à partir d'un point de contrôle connu dans le flux de données avant la panne.

Qu'est-ce que la fonctionnalité DAR améliorée

Vous pouvez utiliser la fonctionnalité de récupération d'accès direct (DAR) améliorée pour les DAR et DAR de fichiers et les flux NT. Par défaut, la fonctionnalité améliorée DAR est activée.

L'activation de la fonctionnalité DAR améliorée peut avoir un impact sur les performances de sauvegarde car une carte de décalage doit être créée et écrite sur bande. Vous pouvez activer ou désactiver Enhanced DAR dans les modes node-scoped et SVM (Storage Virtual machine)-scoped NDMP.

Limite d'évolutivité pour les sessions NDMP

Vous devez connaître le nombre maximal de sessions NDMP qui peuvent être établies simultanément sur les systèmes de stockage de différentes capacités de mémoire système. Ce nombre maximum dépend de la mémoire système d'un système de stockage.

Les limites mentionnées dans le tableau suivant sont destinées au serveur NDMP. Les limites mentionnées dans la section «limites de capacités pour les sessions de sauvegarde et de restauration de vidage» sont pour la session de sauvegarde et de restauration.

Limite d'évolutivité pour les sessions de sauvegarde et de restauration

Mémoire système d'un système de stockage	Nombre maximal de sessions NDMP
Moins de 16 Go	8
Supérieur ou égal à 16 Go mais inférieur à 24 Go	20
Supérieur ou égal à 24 Go	36

Vous pouvez obtenir la mémoire système de votre système de stockage à l'aide du `sysconfig -a` commande (disponible via le nodeshell). Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

À propos de NDMP pour volumes FlexGroup

Depuis ONTAP 9.7, NDMP est pris en charge sur les volumes FlexGroup.

Depuis ONTAP 9.7, la commande ndmpcopy est prise en charge pour le transfert de données entre les volumes FlexVol et FlexGroup.

Si vous restaurez ONTAP 9.7 vers une version antérieure, les informations de transfert incrémentiel des transferts précédents ne sont pas conservées. Par conséquent, vous devez effectuer une copie de base après le rétablissement.

Les fonctionnalités NDMP suivantes sont prises en charge sur les volumes FlexGroup depuis ONTAP 9.8 :

- Le message NDMP_SNAP_RECOVER de la classe d'extension 0x2050 peut être utilisé pour récupérer des fichiers individuels dans un volume FlexGroup.
- L'extension de sauvegarde NDMP redémarrable (RBE) est prise en charge pour les volumes FlexGroup.
- Les variables d'environnement EXCLUDE et MULTI_SUBTREE_NAMES sont prises en charge pour les volumes FlexGroup.

À propos de NDMP avec les volumes SnapLock

La création de plusieurs copies de données réglementées vous permet de bénéficier de scénarios de restauration redondants. En outre, grâce à ce processus, vous pouvez conserver les caractéristiques WORM (Write Once, Read Many) des fichiers source sur un volume SnapLock.

Les attributs WORM des fichiers du volume SnapLock sont conservés lors de la sauvegarde, de la restauration et de la copie des données. Toutefois, les attributs WORM ne sont appliqués que lors de la restauration vers un volume SnapLock. Si une sauvegarde d'un volume SnapLock est restaurée dans un volume autre qu'un volume SnapLock, les attributs WORM sont conservés, mais ils sont ignorés et ne sont pas appliqués par ONTAP.

Gérer le mode node-scoped NDMP pour les volumes FlexVol

Manage node-scoped NDMP mode for FlexVol volumes overview

Vous pouvez gérer NDMP au niveau nœud à l'aide des options et commandes NDMP. Vous pouvez modifier les options NDMP en utilisant le `options` commande. Vous devez utiliser les identifiants spécifiques à NDMP pour accéder à un système de stockage afin d'effectuer des opérations de sauvegarde sur bande et de restauration.

Pour plus d'informations sur le `options` commandes, consultez les pages de manuels.

Informations associées

Commandes permettant de gérer le mode node-scoped NDMP

Le mode node-scoped NDMP est

Commandes permettant de gérer le mode node-scoped NDMP

Vous pouvez utiliser le `system services ndmp` Commandes permettant de gérer NDMP au niveau des nœuds. Certaines de ces commandes sont obsolètes et seront supprimées dans une prochaine version majeure.

Vous ne pouvez utiliser les commandes NDMP suivantes qu'au niveau de privilège avancé :

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez le service NDMP	`system services ndmp on*`
Désactiver le service NDMP	`system services ndmp off*`
Affiche la configuration NDMP	`system services ndmp show*`
Modifier la configuration NDMP	`system services ndmp modify*`
Afficher la version NDMP par défaut	`system services ndmp version*`
Afficher la configuration du service NDMP	`system services ndmp service show`
Modifier la configuration du service NDMP	`system services ndmp service modify`
Affiche toutes les sessions NDMP	`system services ndmp status`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations détaillées sur toutes les sessions NDMP	`system services ndmp probe`
Mettre fin à la session NDMP spécifiée	`system services ndmp kill`
Mettre fin à toutes les sessions NDMP	`system services ndmp kill-all`
Modifier le mot de passe NDMP	`system services ndmp password*`
Activer le mode node-scoped NDMP	`system services ndmp node-scope-mode on*`
Désactiver le mode node-scoped NDMP	`system services ndmp node-scope-mode off*`
Afficher l'état du mode node-scoped NDMP	`system services ndmp node-scope-mode status*`
Arrêtez toutes les sessions NDMP avec force	`system services ndmp service terminate`
Démarrez le démon du service NDMP	`system services ndmp service start`
Arrêtez le démon du service NDMP	`system services ndmp service stop`
Démarrez la connexion pour la session NDMP spécifiée	`system services ndmp log start*`
Arrêter la journalisation de la session NDMP spécifiée	`system services ndmp log stop*`

- Ces commandes sont obsolètes et seront supprimées dans une prochaine version majeure.

Pour plus d'informations sur ces commandes, consultez les pages de manuels pour le `system services ndmp` commandes.

Authentification de l'utilisateur en mode node-scoped NDMP

En mode node-scoped NDMP, il faut utiliser des identifiants spécifiques NDMP pour accéder à un système de stockage afin de réaliser des opérations de backup sur bande et restore.

L'ID utilisateur par défaut est « root ». Avant d'utiliser NDMP sur un nœud, veillez à modifier le mot de passe NDMP par défaut associé à l'utilisateur NDMP. Vous pouvez également modifier l'ID utilisateur NDMP par défaut.

Informations associées

Commandes permettant de gérer le mode node-scoped NDMP

Gérer le mode SVM-scoped NDMP pour les volumes FlexVol

Gérer le mode SVM-scoped NDMP pour les volumes FlexVol présentation

Vous pouvez gérer NDMP par SVM en utilisant les options et commandes NDMP. Vous pouvez modifier les options NDMP en utilisant le `vserver services ndmp modify` commande. En mode SVM-scoped NDMP, l'authentification de l'utilisateur est intégrée au mécanisme de contrôle d'accès basé sur des rôles.

Vous pouvez ajouter NDMP dans la liste des protocoles autorisés ou interdits en utilisant le `vserver modify` commande. Par défaut, NDMP se trouve dans la liste des protocoles autorisés. Si NDMP est ajouté à la liste des protocoles interdits, les sessions NDMP ne peuvent pas être établies.

Vous pouvez contrôler le type LIF sur lequel une connexion de données NDMP est établie en utilisant le `-preferred-interface-role` option. Au cours d'un établissement de connexion de données NDMP, NDMP choisit une adresse IP appartenant au type LIF comme spécifié par cette option. Si les adresses IP n'appartiennent à aucun de ces types LIF, la connexion de données NDMP ne peut pas être établie. Pour plus d'informations sur le `-preferred-interface-role` reportez-vous aux pages de manuel.

Pour plus d'informations sur le `vserver services ndmp modify` commandes, consultez les pages de manuels.

Informations associées

Commandes de gestion du mode SVM-scoped NDMP

Rôle de l'extension Cluster Aware Backup

"Concepts relatifs à ONTAP"

Le mode SVM-scoped NDMP est

"Administration du système"

Commandes de gestion du mode SVM-scoped NDMP

Vous pouvez utiliser le `vserver services ndmp` Commandes permettant de gérer NDMP sur chaque machine virtuelle de stockage (SVM, précédemment appelé Vserver).

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez le service NDMP	`vserver services ndmp on` Le service NDMP doit toujours être activé sur tous les nœuds d'un cluster. Vous pouvez activer le service NDMP sur un nœud en utilisant le `system services ndmp on` commande. Par défaut, le service NDMP est toujours activé sur un nœud.

Les fonctions que vous recherchez…	Utilisez cette commande…
Désactiver le service NDMP	`vserver services ndmp off`
Affiche la configuration NDMP	`vserver services ndmp show`
Modifier la configuration NDMP	`vserver services ndmp modify`
Affiche la version NDMP par défaut	`vserver services ndmp version`
Affiche toutes les sessions NDMP	`vserver services ndmp status`
Affiche des informations détaillées sur toutes les sessions NDMP	`vserver services ndmp probe`
Mettre fin à une session NDMP spécifiée	`vserver services ndmp kill`
Mettre fin à toutes les sessions NDMP	`vserver services ndmp kill-all`
Générer le mot de passe NDMP	`vserver services ndmp generate-password`
Affiche l'état de l'extension NDMP	`vserver services ndmp extensions show` Cette commande est disponible au niveau de privilège avancé.
Modifier (activer ou désactiver) l'état de l'extension NDMP	`vserver services ndmp extensions modify` Cette commande est disponible au niveau de privilège avancé.
Démarrez la connexion pour la session NDMP spécifiée	`vserver services ndmp log start` Cette commande est disponible au niveau de privilège avancé.
Arrêter la journalisation de la session NDMP spécifiée	`vserver services ndmp log stop` Cette commande est disponible au niveau de privilège avancé.

Pour plus d'informations sur ces commandes, consultez les pages de manuels pour le `vserver services ndmp` commandes.

Rôle de l'extension Cluster Aware Backup

CAB (Cluster Aware Backup) est une extension de protocole NDMP v4. Cette extension permet au serveur NDMP d'établir une connexion de données sur un nœud qui possède un volume. Cela permet également à l'application de sauvegarde de déterminer si les volumes et les lecteurs de bande sont situés sur le même nœud d'un cluster.

Pour permettre au serveur NDMP d'identifier le nœud qui possède un volume et d'établir une connexion de données sur ce nœud, l'application de backup doit prendre en charge l'extension CAB. L'extension CAB requiert que l'application de backup informe le serveur NDMP au sujet du volume à sauvegarder ou à restaurer avant d'établir la connexion de données. Cela permet au serveur NDMP de déterminer le nœud qui héberge le volume et d'établir de manière appropriée la connexion de données.

Avec l'extension CAB prise en charge par l'application de sauvegarde, le serveur NDMP fournit des informations d'affinité sur les volumes et les lecteurs de bande. Avec ces informations d'affinité, l'application de sauvegarde peut effectuer une sauvegarde locale au lieu d'une sauvegarde à trois voies si un volume et un périphérique de bande se trouvent sur le même nœud d'un cluster.

Disponibilité de volumes et de bandes pour les sauvegardes et les restaurations sur différents types de LIF

Vous pouvez configurer une application de backup pour établir une connexion de contrôle NDMP sur l'un des types LIF d'un cluster. En mode NDMP (SVM)-scoped, il est possible de déterminer la disponibilité des volumes et des dispositifs à bandes pour les opérations de backup et restore, selon ces types de LIF et le statut de l'extension CAB.

Les tableaux suivants montrent la disponibilité des volumes et des dispositifs à bande pour les types LIF de connexion de contrôle NDMP et le statut de l'extension CAB :

Disponibilité des volumes et des dispositifs à bande lorsque l'extension CAB n'est pas prise en charge par l'application de sauvegarde

Type LIF de connexion de contrôle NDMP	Volumes disponibles pour la sauvegarde ou la restauration	Périphériques à bande disponibles pour la sauvegarde ou la restauration
LIF node-management	Tous volumes hébergés par un nœud	Dispositifs de bande connectés au nœud hébergeant la LIF de node-management
LIF de données	Seuls les volumes qui appartiennent au SVM hébergé par un nœud qui héberge la LIF de données	Aucune
LIF Cluster-management	Tous les volumes hébergés par un nœud qui héberge la LIF de cluster-management	Aucune

Type LIF de connexion de contrôle NDMP	Volumes disponibles pour la sauvegarde ou la restauration	Périphériques à bande disponibles pour la sauvegarde ou la restauration
FRV InterCluster	Tous les volumes hébergés par un nœud qui héberge le LIF intercluster	Périphériques de bande connectés au nœud hébergeant le LIF intercluster

Disponibilité des volumes et des dispositifs à bande lorsque l'extension CAB est prise en charge par l'application de sauvegarde

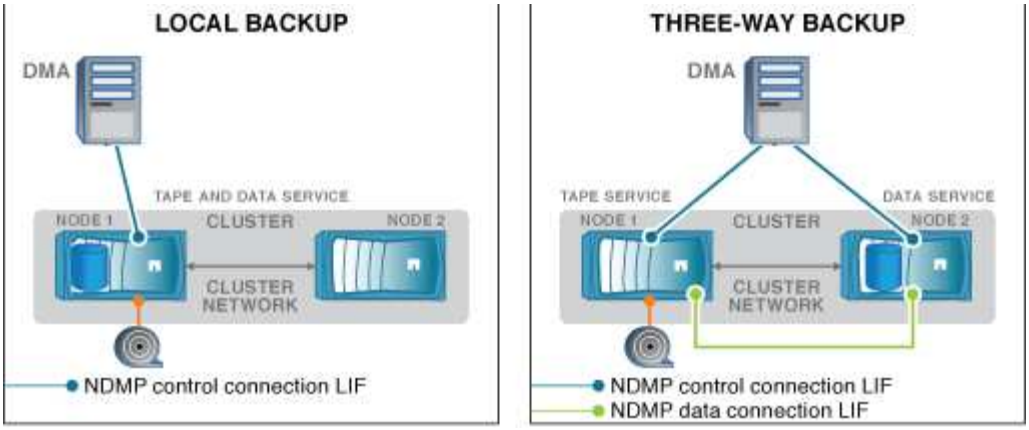
Type LIF de connexion de contrôle NDMP	Volumes disponibles pour la sauvegarde ou la restauration	Périphériques à bande disponibles pour la sauvegarde ou la restauration
LIF node-management	Tous volumes hébergés par un nœud	Dispositifs de bande connectés au nœud hébergeant la LIF de node-management
LIF de données	Tous les volumes qui appartiennent au SVM qui héberge la LIF de données	Aucune
LIF Cluster-management	Tous les volumes du cluster	Tous les périphériques de bande du cluster
FRV InterCluster	Tous les volumes du cluster	Tous les périphériques de bande du cluster

Quelles sont les informations d'affinité

Avec l'application de sauvegarde orientée CAB, le serveur NDMP fournit des informations d'emplacement uniques sur les volumes et les lecteurs de bande. Avec ces informations d'affinité, l'application de sauvegarde peut effectuer une sauvegarde locale au lieu d'une sauvegarde à trois voies si un volume et un périphérique de bande partagent la même affinité.

Si la connexion de contrôle NDMP est établie sur une LIF de node-management, LIF de cluster management, Ou d'une LIF intercluster, l'application de sauvegarde peut utiliser les informations d'affinité pour déterminer si un volume et une unité de bande sont situés sur le même nœud, puis effectuer une opération de sauvegarde ou de restauration locale ou à trois voies. Si la connexion de contrôle NDMP est établie sur une LIF de données, l'application de sauvegarde effectue toujours une sauvegarde à trois voies.

Sauvegarde NDMP locale et sauvegarde NDMP à trois voies



À l'aide des informations d'affinité concernant les volumes et les périphériques de bande, le DMA (application de sauvegarde) effectue une sauvegarde NDMP locale sur le volume et le périphérique de bande situés sur le nœud 1 du cluster. Si le volume passe du nœud 1 au nœud 2, les informations d'affinité concernant le volume et le périphérique de bande changent. Par conséquent, pour une sauvegarde ultérieure, le DMA effectue une opération de sauvegarde NDMP à trois voies. Cela assure la continuité de la stratégie de sauvegarde pour le volume, quel que soit le nœud vers lequel le volume est déplacé.

Informations associées

Rôle de l'extension Cluster Aware Backup

NDMP Server prend en charge les connexions de contrôle sécurisé en mode SVM-scoped

Une connexion de contrôle sécurisée peut être établie entre l'application de gestion des données (DMA) et le serveur NDMP en utilisant des sockets sécurisés (SSL/TLS) comme mécanisme de communication. Cette communication SSL est basée sur les certificats du serveur. Le serveur NDMP écoute sur le port 30000 (attribué par IANA au service « ndmps »).

Une fois la connexion établie à partir du client sur ce port, la liaison SSL standard s'ensuivit lorsque le serveur présente le certificat au client. Lorsque le client accepte le certificat, l'établissement de liaison SSL est terminé. Une fois ce processus terminé, toute la communication entre le client et le serveur est cryptée. Le workflow du protocole NDMP reste identique à celui précédent. La connexion NDMP sécurisée ne nécessite qu'une authentification par certificat côté serveur. Un DMA peut choisir d'établir une connexion soit en se connectant au service NDMP sécurisé soit au service NDMP standard.

Par défaut, le service NDMP sécurisé est désactivé pour les machines virtuelles de stockage (SVM). Vous pouvez activer ou désactiver le service NDMP sécurisé sur une SVM donnée en utilisant le `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` commande.

Types de connexions de données NDMP

En mode SVM (Storage Virtual machine)-scoped NDMP, les types de connexions de données NDMP pris en charge dépendent du type LIF de « NDMP control connection » et du statut de l'extension CAB. Ce type de connexion de données NDMP indique si vous pouvez effectuer une opération de sauvegarde ou de restauration NDMP locale ou à trois voies.

Vous pouvez effectuer une sauvegarde ou une restauration NDMP à trois voies sur un réseau TCP ou

TCP/IPv6. Les tableaux suivants présentent les types de connexions de données NDMP, basés sur le type LIF de connexion de contrôle NDMP et le statut de l'extension DE CAB.

Type de connexion de données NDMP lorsque l'extension CAB est prise en charge par l'application de backup

Type LIF de connexion de contrôle NDMP	Type de connexion de données NDMP
LIF node-management	LOCAL, TCP, TCP/IPV6
LIF de données	TCP, TCP/IPv6
LIF Cluster-management	LOCAL, TCP, TCP/IPV6
FRV InterCluster	LOCAL, TCP, TCP/IPV6

Type de connexion de données NDMP lorsque l'extension CAB n'est pas prise en charge par l'application de backup

Type LIF de connexion de contrôle NDMP	Type de connexion de données NDMP
LIF node-management	LOCAL, TCP, TCP/IPV6
LIF de données	TCP, TCP/IPv6
LIF Cluster-management	TCP, TCP/IPv6
FRV InterCluster	LOCAL, TCP, TCP/IPV6

Informations associées

Rôle de l'extension Cluster Aware Backup

"Gestion du réseau"

Authentification de l'utilisateur en mode SVM-scoped NDMP

En mode SVM (Storage Virtual machine)-scoped NDMP, l'authentification utilisateur NDMP est intégrée au contrôle d'accès basé sur des rôles. Dans le contexte SVM, l'utilisateur NDMP doit avoir le rôle « vsadmin » ou « vsadmin-backup ». Dans un contexte de cluster, l'utilisateur NDMP doit avoir le rôle « admin » ou « backup ».

Outre ces rôles prédéfinis, un compte utilisateur associé à un rôle personnalisé peut également être utilisé pour l'authentification NDMP à condition que le rôle personnalisé ait le dossier « vserver services ndmp » dans son répertoire de commandes et que le niveau d'accès du dossier n'est pas « nul ». Dans ce mode, vous devez générer un mot de passe NDMP pour un compte utilisateur donné, créé par le biais du contrôle d'accès basé sur des rôles. Les utilisateurs de cluster en rôle d'administrateur ou de sauvegarde peuvent accéder à une LIF de node-management, à une LIF de cluster-management ou à un LIF intercluster. Les utilisateurs ayant un rôle vsadmin-backup ou vsadmin peuvent accéder uniquement à la LIF de données pour ce SVM. Par conséquent, selon le rôle d'un utilisateur, la disponibilité des volumes et des périphériques de bande pour les opérations de sauvegarde et de restauration varie.

Ce mode prend également en charge l'authentification des utilisateurs pour les utilisateurs NIS et LDAP. Ainsi, les utilisateurs NIS et LDAP peuvent accéder à plusieurs SVM avec un ID utilisateur et un mot de passe communs. Cependant, l'authentification NDMP ne prend pas en charge les utilisateurs Active Directory.

Dans ce mode, un compte utilisateur doit être associé à l'application SSH et à la méthode d'authentification « Mot de passe utilisateur ».

Informations associées

Commandes de gestion du mode SVM-scoped NDMP

"Administration du système"

"Concepts relatifs à ONTAP"

Générez un mot de passe spécifique NDMP pour les utilisateurs NDMP

En mode Storage Virtual machine (SVM)-scoped NDMP, vous devez générer un mot de passe pour un ID utilisateur spécifique. Le mot de passe généré est basé sur le mot de passe de connexion réel pour l'utilisateur NDMP. Si le mot de passe de connexion change, vous devez générer à nouveau le mot de passe spécifique au NDMP.

Étapes

1. Utilisez le `vserver services ndmp generate-password` Commande permettant de générer un mot de passe spécifique au NDMP.

   Vous pouvez utiliser ce mot de passe pour toute opération NDMP actuelle ou future nécessitant la saisie d'un mot de passe.

   > Depuis le contexte SVM (anciennement appelé Vserver), vous pouvez générer des mots de passe NDMP pour les utilisateurs appartenant uniquement à ce SVM.

   L'exemple suivant montre comment générer un mot de passe spécifique au protocole NDMP pour un ID utilisateur utilisateur1 :

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. Si vous remplacez le mot de passe par votre compte normal du système de stockage, répétez cette procédure pour obtenir votre nouveau mot de passe spécifique au NDMP.

L'impact des opérations de sauvegarde sur bande et de restauration sur la reprise après incident en configuration MetroCluster

Vous pouvez effectuer des opérations de sauvegarde sur bande et de restauration simultanément pendant la reprise sur incident dans une configuration MetroCluster. Vous devez comprendre l'impact de ces opérations sur la reprise sur incident.

Si les opérations de sauvegarde et de restauration sur bande sont effectuées sur un volume d'SVM dans une relation de reprise après incident, vous pouvez continuer à effectuer les opérations de sauvegarde et de restauration sur bande incrémentielles après le basculement et le rétablissement.

À propos du moteur de dump pour les volumes FlexVol

À propos du moteur de dump pour les volumes FlexVol

Dump est une solution de sauvegarde et de restauration basée sur des copies Snapshot de ONTAP qui vous permet de sauvegarder des fichiers et des répertoires d'une copie Snapshot sur un périphérique de bande et de restaurer les données sauvegardées sur un système de stockage.

Vous pouvez sauvegarder les données de votre système de fichiers, telles que les répertoires, les fichiers et leurs paramètres de sécurité associés, sur un périphérique de bande à l'aide de la sauvegarde dump. Vous pouvez sauvegarder un volume entier, un qtree entier ou un sous-arbre qui n'est ni un volume entier, ni un qtree entier.

Vous pouvez effectuer une sauvegarde ou une restauration de dump à l'aide d'applications de sauvegarde conformes NDMP.

Lorsque vous effectuez une sauvegarde de dump, vous pouvez spécifier la copie Snapshot à utiliser pour une sauvegarde. Si vous ne spécifiez pas de copie Snapshot pour la sauvegarde, le moteur de dump crée une copie Snapshot pour la sauvegarde. Une fois l'opération de sauvegarde terminée, le moteur de dump supprime cette copie Snapshot.

Vous pouvez effectuer des sauvegardes de niveau 0, incrémentielles ou différentielles sur bande à l'aide du moteur de vidage.

> Après avoir revenir à une version antérieure à Data ONTAP 8.3, vous devez effectuer une opération de sauvegarde de base avant d'effectuer une opération de sauvegarde incrémentielle.

Informations associées

"Mise à niveau, rétablissement ou mise à niveau vers une version antérieure"

Fonctionnement d'une sauvegarde de vidage

Une sauvegarde de vidage écrit les données du système de fichiers de disque à bande en utilisant un processus prédéfini. Vous pouvez sauvegarder un volume, un qtree ou une sous-arborescence qui n'est ni un volume entier, ni un qtree entier.

Le tableau ci-dessous décrit le processus utilisé par ONTAP pour sauvegarder l'objet indiqué par le chemin de vidage :

Étape	Action
1	Pour les sauvegardes qtree complètes ou à volume complet, ONTAP traverse des répertoires pour identifier les fichiers à sauvegarder. Si vous sauvegardez un volume entier ou un qtree, ONTAP associe cette étape à la phase 2.

Étape	Action
2	Pour une sauvegarde de volume complet ou qtree complet, ONTAP identifie les répertoires des volumes ou des qtrees à sauvegarder.
3	ONTAP écrit les répertoires sur bande.
4	ONTAP écrit les fichiers sur bande.
5	ONTAP écrit les informations de l'ACL (le cas échéant) sur bande.

La sauvegarde de dump utilise une copie Snapshot de vos données à des fins de sauvegarde. Par conséquent, vous n'avez pas besoin de mettre le volume hors ligne avant de lancer la sauvegarde.

La sauvegarde de dump attribue la création de chaque copie Snapshot `snapshot_for_backup.n`, où `n` est un entier commençant à 0. Chaque fois que la sauvegarde de dump crée une copie Snapshot, elle incrémente le nombre entier de 1. L'entier est réinitialisé à 0 après le redémarrage du système de stockage. Une fois l'opération de sauvegarde terminée, le moteur de dump supprime cette copie Snapshot.

Lorsque ONTAP effectue plusieurs sauvegardes de dump simultanément, le moteur de dump crée plusieurs copies Snapshot. Par exemple, si ONTAP exécute simultanément deux sauvegardes de dump, vous trouverez les copies Snapshot suivantes dans les volumes à partir desquels les données sont sauvegardées : `snapshot_for_backup.0` et `snapshot_for_backup.1`.

> Lorsque vous effectuez une sauvegarde à partir d'une copie Snapshot, le moteur de dump ne crée pas de copie Snapshot supplémentaire.

Types de données que le moteur de vidage sauvegarde

Le moteur de dump vous permet de sauvegarder les données sur bande afin d'éviter les incidents ou les perturbations sur les contrôleurs. Outre la sauvegarde d'objets de données tels que des fichiers, des répertoires, des qtrees ou des volumes entiers, le moteur de dump peut sauvegarder de nombreux types d'informations sur chaque fichier. La connaissance des types de données que le moteur de dump peut sauvegarder et des restrictions à prendre en compte peut vous aider à planifier votre approche de la reprise sur incident.

En plus de sauvegarder des données dans des fichiers, le moteur de vidage peut sauvegarder les informations suivantes sur chaque fichier, selon le cas :

- GID UNIX, UID de propriétaire et autorisations de fichier
- Heure d'accès, de création et de modification UNIX
- Type de fichier
- Taille du fichier
- Nom DOS, attributs DOS et heure de création
- Listes de contrôle d'accès (ACL) avec 1,024 entrées de contrôle d'accès (ACE)
- Informations sur les qtrees

- Chemins de liaison

Les chemins de jonction sont sauvegardés en tant que liens symboliques.

- Clones de LUN et de LUN

  Vous pouvez sauvegarder un objet LUN entier ; cependant, vous ne pouvez pas sauvegarder un seul fichier dans cet objet. De la même manière, vous pouvez restaurer tout un objet LUN, mais pas un seul fichier au sein de ce dernier.

  > Le moteur de dump sauvegarde les clones de LUN en tant que LUN indépendantes.

- Fichiers alignés sur les machines virtuelles

  La sauvegarde des fichiers alignés sur les machines virtuelles n'est pas prise en charge dans les versions antérieures à Data ONTAP 8.1.2.

> Lorsqu'un clone de LUN avec snapshot est passé de Data ONTAP 7-mode à ONTAP, il devient LUN incohérent. Le moteur de vidage ne sauvegarde pas les LUN incohérentes.

Lorsque vous restaurez les données sur un volume, les E/S client sont restreintes sur les LUN en cours de restauration. La restriction de LUN est supprimée uniquement lorsque l'opération de restauration de vidage est terminée. De même, lors de l'opération de restauration de fichiers ou de LUN SnapMirror, les E/S clientes sont limitées sur les fichiers et les LUN en cours de restauration. Cette restriction est supprimée uniquement lorsque l'opération de restauration de fichier ou de LUN est terminée. Lorsqu'une sauvegarde de dump est effectuée sur un volume sur lequel une restauration de dump ou une opération de restauration de fichier unique SnapMirror ou de restauration de LUN est en cours, les fichiers ou les LUN dont les restrictions d'E/S sont présentes sur le client ne sont pas inclus dans la sauvegarde. Ces fichiers ou LUN sont inclus dans une opération de sauvegarde suivante si la restriction d'E/S du client est supprimée.

> Une LUN exécutée sur Data ONTAP 8.3 et qui est sauvegardée sur bande ne peut être restaurée qu'à partir des versions 8.3 et ultérieures, et non vers une version antérieure. Si la LUN est restaurée dans une version antérieure, la LUN est restaurée en tant que fichier.

Lorsque vous sauvegardez un volume secondaire SnapVault ou une destination SnapMirror volume sur bande, seules les données du volume sont sauvegardées. Les métadonnées associées ne sont pas sauvegardées. Par conséquent, lorsque vous tentez de restaurer le volume, seules les données de ce volume sont restaurées. Les informations relatives aux relations SnapMirror volume ne sont pas disponibles dans la sauvegarde et n'sont donc pas restaurées.

Si vous dump un fichier qui ne dispose que d'autorisations Windows NT et le restaurez sur un qtree ou un volume de style UNIX, le fichier obtient les autorisations UNIX par défaut pour ce qtree ou volume.

Si vous dump un fichier qui ne dispose que d'autorisations UNIX et que vous le restaurez sur un qtree ou un volume de style NTFS, le fichier obtient les autorisations Windows par défaut pour ce qtree ou ce volume.

Les autres « dumps » et les restaurations préservent les autorisations.

Vous pouvez sauvegarder des fichiers alignés sur les machines virtuelles et le `vm-align-sector` option. Pour plus d'informations sur les fichiers alignés sur les machines virtuelles, voir "Gestion du stockage logique".

Quelles sont les chaînes d'incrémentation

Une chaîne d'incrémentation est une série de sauvegardes incrémentielles du même chemin. Comme vous pouvez spécifier n'importe quel niveau de sauvegarde à tout moment, vous devez comprendre incrémenter les chaînes pour pouvoir effectuer efficacement les sauvegardes et les restaurations. Vous pouvez effectuer 31 niveaux d'opérations de sauvegarde incrémentielles.

Il existe deux types de chaînes d'incrémentation :

- Une chaîne d'incrémentation consécutive, qui est une séquence de sauvegardes incrémentielles commençant par le niveau 0 et qui est élevée par 1 à chaque sauvegarde suivante.
- Chaîne d'incrémentation non consécutive, où les sauvegardes incrémentielles ignorent des niveaux ou ont des niveaux hors séquence, tels que 0, 2, 3, 1, 4, ou plus fréquemment 0, 1, 1, 1 ou 0, 1, 2, 1, 2.

Les sauvegardes incrémentielles reposent sur la sauvegarde de niveau inférieur la plus récente. Par exemple, la séquence des niveaux de sauvegarde 0, 2, 3, 1, 4 fournit deux chaînes d'incrément : 0, 2, 3 et 0, 1, 4. Le tableau suivant explique les bases de sauvegardes incrémentielles :

Ordre de sauvegarde	Niveau d'incrémentation	Incrémenter la chaîne	Base	Fichiers sauvegardés
1	0	Les deux	Fichiers sur le système de stockage	Tous les fichiers du chemin de sauvegarde
2	2	0, 2, 3	Sauvegarde de niveau 0	Fichiers dans le chemin de sauvegarde créé depuis la sauvegarde de niveau 0
3	3	0, 2, 3	Sauvegarde de niveau 2	Fichiers dans le chemin de sauvegarde créé depuis la sauvegarde de niveau 2
4	1	0, 1, 4	Sauvegarde de niveau 0, car il s'agit du niveau le plus récent qui est inférieur à la sauvegarde de niveau 1	Fichiers dans le chemin de sauvegarde créé depuis la sauvegarde de niveau 0, y compris les fichiers qui se trouvent dans les sauvegardes de niveau 2 et de niveau 3

Ordre de sauvegarde	Niveau d'incrémentation	Incrémenter la chaîne	Base	Fichiers sauvegardés
5	4	0, 1, 4	La sauvegarde de niveau 1, car elle est un niveau inférieur et est plus récente que les sauvegardes de niveau 0, 2 ou 3	Fichiers créés depuis la sauvegarde de niveau 1

Quel est le facteur de blocage

Un bloc de bandes est de 1,024 octets de données. Lors d'une sauvegarde ou d'une restauration sur bande, vous pouvez spécifier le nombre de blocs de bandes transférés dans chaque opération de lecture/écriture. Ce nombre est appelé le *facteur de blocage*.

Vous pouvez utiliser un facteur de blocage de 4 à 256. Si vous envisagez de restaurer une sauvegarde sur un système autre que celui qui a effectué la sauvegarde, le système de restauration doit prendre en charge le facteur de blocage que vous avez utilisé pour la sauvegarde. Par exemple, si vous utilisez un facteur de blocage de 128, le système sur lequel vous restaurez cette sauvegarde doit prendre en charge un facteur de blocage de 128.

Lors d'une sauvegarde NDMP, LE MOVER_RECORD_SIZE détermine le facteur de blocage. ONTAP autorise une valeur maximale de 256 Ko pour MOVER_RECORD_SIZE.

Quand redémarrer une sauvegarde de vidage

Une sauvegarde de dump ne se termine parfois pas en raison d'erreurs internes ou externes, telles que les erreurs d'écriture sur les bandes, les pannes d'alimentation, les interruptions accidentelles des utilisateurs ou les incohérences internes du système de stockage. Si votre sauvegarde échoue pour l'une de ces raisons, vous pouvez la redémarrer.

Vous pouvez choisir d'interrompre et de redémarrer une sauvegarde pour éviter les pics de trafic sur le système de stockage ou d'éviter la concurrence pour d'autres ressources limitées sur le système de stockage, comme les lecteurs de bandes. Vous pouvez interrompre une sauvegarde longue et la redémarrer ultérieurement si une restauration (ou une sauvegarde) plus urgente nécessite le même lecteur de bande. Les sauvegardes redémarrables sont conservées entre les redémarrages. Vous ne pouvez redémarrer une sauvegarde abandonnée sur bande que si les conditions suivantes sont vraies :

- La sauvegarde abandonnée est en phase IV
- Toutes les copies Snapshot associées qui ont été verrouillées par la commande dump sont disponibles.
- L'historique du fichier doit être activé.

Lorsqu'une telle opération de vidage est abandonnée et reste à l'état redémarrable, les copies Snapshot associées sont verrouillées. Ces copies Snapshot sont libérées une fois ces contextes supprimés. Vous pouvez afficher la liste des contextes de sauvegarde à l'aide du `vserver services ndmp restartable backup show` commande.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Fonctionnement d’une restauration de vidage

Une restauration de vidage écrit les données du système de fichiers de la bande sur le disque à l’aide d’un processus prédéfini.

Le processus du tableau suivant montre le fonctionnement de la restauration de vidage :

Étape	Action
1	ONTAP catalogue les fichiers à extraire de la bande.
2	ONTAP crée des répertoires et des fichiers vides.

Étape	Action
3	ONTAP lit un fichier à partir de la bande, l'écrit sur le disque et définit les autorisations (y compris les listes de contrôle d'accès) sur celui-ci.
4	ONTAP répète les étapes 2 et 3 jusqu'à ce que tous les fichiers spécifiés soient copiés à partir de la bande.

Types de données que le moteur de vidage restaure

En cas d'incident ou de perturbation du contrôleur, le moteur de dump offre plusieurs méthodes permettant de restaurer l'ensemble des données sauvegardées, depuis des fichiers uniques jusqu'aux attributs de fichiers, vers des répertoires entiers. Connaître les types de données que le moteur de vidage peut restaurer et quand utiliser quelle méthode de récupération peut aider à réduire les temps d'arrêt.

Vous pouvez restaurer les données sur une LUN mappée en ligne. Cependant, les applications hôtes ne peuvent pas accéder à cette LUN tant que l'opération de restauration n'est pas terminée. Une fois l'opération de restauration terminée, le cache hôte des données de la LUN doit être vidé pour assurer la cohérence avec les données restaurées.

Le moteur de vidage peut récupérer les données suivantes :

- Contenu des fichiers et répertoires
- Autorisations relatives aux fichiers UNIX
- ACL

  Si vous restaurez un fichier possédant uniquement des autorisations de fichier UNIX sur un qtree ou un volume NTFS, le fichier ne dispose pas de listes de contrôle d'accès Windows NT. Le système de stockage utilise uniquement les autorisations de fichier UNIX sur ce fichier jusqu'à ce que vous y créiez une liste de contrôle d'accès Windows NT.

  > Si vous restaurez les listes de contrôle d'accès sauvegardées à partir des systèmes de stockage exécutant Data ONTAP 8.2 vers les systèmes de stockage exécutant Data ONTAP 8.1.x et les versions antérieures ayant une limite ACE inférieure à 1,024, une liste de contrôle d'accès par défaut est restaurée.

- Informations sur les qtrees

  Les informations relatives à qtree sont utilisées uniquement si un qtree est restauré à la racine d'un volume. Les informations qtree ne sont pas utilisées si un qtree est restauré dans un répertoire inférieur, par exemple `/vs1/vol1/subdir/lowerdir`, et il cesse d'être un qtree.

- Tous les autres attributs de fichier et de répertoire
- Flux Windows NT
- LUN
  - Une LUN doit être restaurée au niveau d'un volume ou d'une qtree pour qu'elle reste une LUN.

    S'il est restauré dans un répertoire, il est restauré en tant que fichier car il ne contient aucune

métadonnées valide.

  - Une LUN 7-mode est restaurée sous forme de LUN sur un volume ONTAP.
- Un volume 7-mode peut être restauré vers un volume ONTAP.
- Les fichiers alignés sur les machines virtuelles restaurés sur un volume de destination héritent des propriétés d'alignement des machines virtuelles du volume de destination.
- Le volume de destination pour une opération de restauration peut avoir des fichiers avec des verrous obligatoires ou consultatifs.

  Lors de l'exécution de l'opération de restauration sur un tel volume de destination, le moteur de vidage ignore ces verrous.

Considérations avant de restaurer les données

Vous pouvez restaurer les données sauvegardées dans leur chemin d'origine ou vers une destination différente. Si vous restaurez les données sauvegardées vers une autre destination, vous devez préparer la destination pour l'opération de restauration.

Avant de restaurer les données sur son chemin d'origine ou vers une autre destination, vous devez disposer des informations suivantes et satisfaire les exigences suivantes :

- Niveau de la restauration
- Le chemin vers lequel vous restaurez les données
- Facteur de blocage utilisé pendant la sauvegarde
- Si vous effectuez une restauration incrémentielle, toutes les bandes doivent être dans la chaîne de sauvegarde
- Lecteur de bande disponible et compatible avec la bande à restaurer

Avant de restaurer les données vers une autre destination, vous devez effectuer les opérations suivantes :

- Si vous restaurez un volume, vous devez créer un nouveau volume.
- Si vous restaurez un qtree ou un répertoire, vous devez renommer ou déplacer des fichiers susceptibles d'avoir les mêmes noms que les fichiers que vous restaurez.

> Dans ONTAP 9, les noms de qtree prennent en charge le format Unicode. Les versions antérieures de ONTAP ne prennent pas en charge ce format. Si un qtree avec des noms Unicode dans ONTAP 9 est copié dans une version antérieure de ONTAP à l'aide de l' `ndmpcopy` Commande ou par restauration à partir d'une image de sauvegarde sur bande, le qtree est restauré en tant que répertoire normal et non en tant que qtree au format Unicode.

> Si un fichier restauré porte le même nom qu'un fichier existant, le fichier existant est écrasé par le fichier restauré. Toutefois, les répertoires ne sont pas écrasés.

Pour renommer un fichier, un répertoire ou un qtree pendant la restauration sans utiliser DAR, vous devez définir la variable d'environnement D'EXTRACTION sur `E`.

Espace requis sur le système de stockage de destination

Vous avez besoin d'environ 100 Mo d'espace supplémentaire sur le système de stockage de destination par

rapport à la quantité de données à restaurer.

> L'opération de restauration vérifie l'espace volume et la disponibilité d'inode sur le volume de destination au démarrage de l'opération de restauration. Définition de la variable d'environnement DE FORCE sur `Y` provoque l'opération de restauration pour ignorer les vérifications de l'espace volume et de la disponibilité d'inode sur le chemin de destination. S'il n'y a pas assez d'espace volume ou d'inodes disponible sur le volume de destination, l'opération de restauration restaure autant de données que l'espace du volume de destination et la disponibilité d'inode. L'opération de restauration s'arrête lorsqu'il ne reste plus d'espace ou d'inodes.

Limite d'évolutivité pour les sessions de sauvegarde et de restauration

Vous devez connaître le nombre maximal de sessions de sauvegarde et de restauration de vidage que vous pouvez effectuer simultanément sur les systèmes de stockage de différentes capacités de mémoire système. Ce nombre maximum dépend de la mémoire système d'un système de stockage.

Les limites mentionnées dans le tableau suivant concernent le moteur de vidage ou de restauration. Les limites mentionnées dans les limites d'évolutivité des sessions NDMP sont destinées au serveur NDMP, qui sont supérieures aux limites du moteur.

Mémoire système d'un système de stockage	Nombre total de sessions de sauvegarde et de restauration de vidage
Moins de 16 Go	4
Supérieur ou égal à 16 Go mais inférieur à 24 Go	16
Supérieur ou égal à 24 Go	32

> Si vous utilisez `ndmpcopy` Commande pour copier les données dans les systèmes de stockage, deux sessions NDMP sont établies, l'une pour dump backup et l'autre pour dump restore.

Vous pouvez obtenir la mémoire système de votre système de stockage à l'aide du `sysconfig -a` commande (disponible via le nodeshell). Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

Informations associées

Limite d'évolutivité pour les sessions NDMP

Prise en charge de la sauvegarde sur bande et des restaurations entre Data ONTAP sous 7-mode et ONTAP

Vous pouvez restaurer les données sauvegardées à partir d'un système de stockage sous 7-mode ou exécutant ONTAP vers un système de stockage sous 7-mode ou exécutant ONTAP.

Les opérations suivantes de sauvegarde sur bande et de restauration sont prises en charge entre Data ONTAP en 7-mode et ONTAP :

- Sauvegarde d'un volume 7-mode sur un lecteur de bandes connecté à un système de stockage exécutant ONTAP
- Sauvegarde d'un volume ONTAP sur un lecteur de bandes connecté à un système 7-mode
- Restauration des données sauvegardées d'un volume 7-mode depuis un lecteur de bande connecté à un système de stockage exécutant ONTAP
- Restauration des données sauvegardées d'un volume ONTAP à partir d'un lecteur de bande connecté à un système 7-mode
- Restauration d'un volume 7-mode vers un volume ONTAP

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Restauration d'un volume ONTAP sur un volume 7-mode

Une LUN ONTAP est restaurée sous forme de fichier standard sur un volume 7-mode.

Supprimer des contextes réstartables

Si vous souhaitez démarrer une sauvegarde au lieu de redémarrer un contexte, vous pouvez supprimer le contexte.

Description de la tâche

Vous pouvez supprimer un contexte redémarrable à l'aide de l' `vserver services ndmp restartable-backup delete` Commande utilisant le nom du SVM et l'ID de contexte.

Étapes

1. Supprimer un contexte redémarrable :

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context -id` *`context_identifier`*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Fonctionnement de dump sur un volume secondaire SnapVault

Vous pouvez effectuer des opérations de sauvegarde sur bande sur des données mises en miroir sur le volume secondaire SnapVault. Vous pouvez sauvegarder uniquement les données mises en miroir sur le volume secondaire SnapVault sur bande, et non sur les métadonnées liées à la relation SnapVault.

Quand on rompent la relation de miroir de protection des données (`snapmirror break`) Ou lorsqu'une resynchronisation SnapMirror se produit, vous devez toujours effectuer une sauvegarde de base.

Fonctionnement de dump avec les opérations de basculement de stockage et d'ARL

Avant d'effectuer des opérations de sauvegarde et de restauration de type dump, il est important de comprendre le fonctionnement de ces opérations avec les opérations de basculement du stockage (Takeover et giveback) ou de transfert d'agrégats (ARL). Le `-override-vetoes` Détermine le comportement du moteur de vidage lors d'une opération de basculement du stockage ou d'ARL.

Lorsqu'une opération de sauvegarde ou de restauration est en cours d'exécution et `-override-vetoes` l'option est définie sur `false`, Un basculement de stockage ou une opération ARL initié par l'utilisateur est arrêté. Cependant, si `-override-vetoes` l'option est définie sur `true`, Le basculement du stockage ou l'opération ARL est ensuite poursuivi et l'opération de sauvegarde ou de restauration de vidage est abandonnée. Lorsqu'une opération de basculement ou d'ARL de stockage est automatiquement lancée par le système de stockage, une opération de sauvegarde ou de restauration des données de dump actif est toujours abandonnée. Vous ne pouvez pas redémarrer les opérations de sauvegarde et de restauration de vidage,

même après la fin des opérations de basculement du stockage ou d'ARL.

Opérations de vidage lorsque l'extension DE CABINE est prise en charge

Si l'application de sauvegarde prend en charge l'extension CAB, vous pouvez continuer à effectuer les opérations de sauvegarde et de restauration incrémentielles sans reconfigurer les règles de sauvegarde après un basculement de stockage ou un transfert d'agrégats.

Les opérations de vidage lorsque l'extension DE CABINE n'est pas prise en charge

Si l'application de sauvegarde ne prend pas en charge l'extension CAB, vous pouvez continuer d'effectuer les opérations de sauvegarde et de restauration du dump incrémentiel si vous migrez la LIF configurée dans la politique de sauvegarde vers le nœud qui héberge l'agrégat de destination. Sinon, après le basculement du stockage et l'ARL, vous devez effectuer une sauvegarde de base avant d'effectuer l'opération de sauvegarde incrémentielle.

> Pour les opérations de basculement du stockage, la LIF configurée dans la stratégie de sauvegarde doit être migrée vers le nœud partenaire.

Informations associées

"Concepts relatifs à ONTAP"

"Haute disponibilité"

Fonctionnement de dump lors du déplacement de volumes

Les opérations de sauvegarde et de restauration sur bande et de déplacement de volumes peuvent être exécutées en parallèle jusqu'à la phase de mise en service finale du système de stockage. Après cette phase, les nouvelles opérations de sauvegarde et de restauration sur bandes ne sont pas autorisées sur le volume en cours de déplacement. Cependant, les opérations en cours continuent de fonctionner jusqu'à la fin.

Le tableau suivant décrit le comportement des opérations de sauvegarde et de restauration sur bande après le déplacement du volume :

Si vous effectuez des opérations de sauvegarde sur bande et de restauration dans…	Alors…
Storage Virtual machine (SVM) a scoped NDMP (mode NDMP) lorsque l'extension CAB est prise en charge par l'application de backup	Vous pouvez continuer à effectuer des sauvegardes incrémentielles sur bande et restaurer des volumes en lecture/écriture et en lecture seule sans reconfigurer les règles de sauvegarde.

Si vous effectuez des opérations de sauvegarde sur bande et de restauration dans…	Alors…
Mode SVM-scoped NDMP lorsque l'extension CAB n'est pas prise en charge par l'application de backup	Vous pouvez continuer à effectuer des opérations de sauvegarde incrémentielle sur bande et de restauration sur des volumes en lecture/écriture et en lecture seule si vous migrez la LIF configurée dans la stratégie de sauvegarde vers le nœud qui héberge l'agrégat de destination. Sinon, après le déplacement du volume, vous devez effectuer une sauvegarde de base avant d'effectuer l'opération de sauvegarde incrémentielle.

Lorsqu'un déplacement de volumes se produit, si le volume appartenant à un autre SVM sur le nœud de destination porte le même nom que celui du volume déplacé, vous ne pouvez pas effectuer d'opérations de sauvegarde incrémentielle du volume déplacé.

Informations associées

"Concepts relatifs à ONTAP"

Fonctionnement de dump lorsqu'un volume FlexVol est plein

Avant d'effectuer une opération de sauvegarde incrémentielle de dump, vous devez vérifier que l'espace disponible est suffisant dans le volume FlexVol.

En cas d'échec de l'opération, vous devez augmenter l'espace libre du volume Flex vol, soit en augmentant sa taille, soit en supprimant les copies Snapshot. Effectuez ensuite à nouveau l'opération de sauvegarde incrémentielle.

Fonctionnement de dump lorsque le type d'accès de volume change

Lorsqu'un volume de destination SnapMirror ou un volume secondaire SnapVault passe de l'état lecture/écriture à lecture seule ou de la lecture seule à la lecture/écriture, vous devez effectuer une opération de sauvegarde ou de restauration de base sur bande.

La destination SnapMirror et les volumes secondaires SnapVault sont des volumes en lecture seule. Si vous effectuez des opérations de sauvegarde sur bande et de restauration sur de tels volumes, vous devez effectuer une opération de sauvegarde ou de restauration de base chaque fois que le volume passe de l'état lecture seule à lecture/écriture ou de la lecture/écriture à la lecture seule.

Informations associées

"Concepts relatifs à ONTAP"

Fonctionnement de dump avec la restauration de fichiers ou de LUN SnapMirror

Avant d'effectuer des sauvegardes de dump ou des opérations de restauration sur un volume sur lequel un fichier ou une LUN unique est restauré à l'aide de la technologie SnapMirror, vous devez comprendre le fonctionnement des opérations de dump avec une seule opération de restauration de fichiers ou de LUN.

Lors de l'opération de restauration d'un seul fichier ou de LUN SnapMirror, le nombre d'E/S client est limité sur le fichier ou la LUN en cours de restauration. Une fois l'opération de restauration de fichier ou de LUN terminée, la restriction d'E/S sur le fichier ou la LUN est supprimée. Si une sauvegarde de dump est effectuée sur un volume sur lequel un seul fichier ou LUN est restauré, alors le fichier ou la LUN qui a une restriction d'E/S client n'est pas inclus dans la sauvegarde dump. Lors d'une opération de sauvegarde ultérieure, ce fichier ou ce LUN est sauvegardé sur bande après suppression de la restriction d'E/S.

Vous ne pouvez pas effectuer simultanément une restauration de dump et une opération de restauration SnapMirror ou de LUN sur le même volume.

Le rôle des opérations de vidage et de restauration dans les configurations MetroCluster est affecté

Avant d'effectuer les opérations de sauvegarde et de restauration de dump dans une configuration MetroCluster, vous devez en déterminer l'impact des opérations de dump en cas d'opération de basculement ou de rétablissement.

Vidage de l'opération de sauvegarde ou de restauration suivi du basculement

Envisager deux clusters : cluster 1 et cluster 2. Lors d'une opération de sauvegarde ou de restauration sur le cluster 1, si un basculement est initié du cluster 1 au cluster 2, ce qui suit se produit :

- Si la valeur de `override-vetoes` l'option est `false`, le basculement est alors interrompu et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, l'opération de sauvegarde ou de restauration du vidage est alors abandonnée et le basculement se poursuit.

Vidage de l'opération de sauvegarde ou de restauration, suivi du rétablissement

Un basculement est effectué du cluster 1 vers le cluster 2 et une opération de sauvegarde ou de restauration de « dump » est lancée sur le cluster 2. L'opération de dump sauvegarde ou restaure un volume situé sur le cluster 2. À ce stade, si un rétablissement est initié du cluster 2 au cluster 1, ce qui suit se produit :

- Si la valeur de `override-vetoes` l'option est `false`, le rétablissement est alors annulé et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, l'opération de sauvegarde ou de restauration est alors abandonnée et le rétablissement se poursuit.

Vidage de l'opération de sauvegarde ou de restauration initié lors d'un basculement ou d'un rétablissement

Lors du basculement d'un cluster 1 vers un cluster 2, si une opération de sauvegarde ou de restauration de dump est initiée sur le cluster 1, l'opération de sauvegarde ou de restauration échoue et le basculement se poursuit.

Lors du rétablissement d'un cluster 2 vers le cluster 1, si une opération de sauvegarde ou de restauration de vidage est lancée depuis le cluster 2, l'opération de sauvegarde ou de restauration échoue et le rétablissement se poursuit.

À propos du moteur SMTape pour les volumes FlexVol

À propos du moteur SMTape pour les volumes FlexVol

SMTape est une solution de reprise après incident de ONTAP qui sauvegarde des blocs

de données sur bande. Vous pouvez utiliser SMTape afin d'effectuer des sauvegardes de volume sur bandes. Toutefois, vous ne pouvez pas effectuer de sauvegarde au niveau qtree ou sous-arbre. SMTape prend en charge les sauvegardes de base, différentielles et incrémentielles. SMTape ne nécessite pas de licence.

Vous pouvez effectuer une opération de sauvegarde et de restauration SMTape à l'aide d'une application de sauvegarde conforme au protocole NDMP. Vous pouvez choisir SMTape afin d'effectuer des opérations de sauvegarde et de restauration uniquement en mode NDMP étendue de la machine virtuelle de stockage (SVM).

> Le processus de réversion n'est pas pris en charge lorsqu'une session de sauvegarde ou de restauration SMTape est en cours. Vous devez attendre la fin de la session ou abandonner la session NDMP.

SMTape permet de sauvegarder 255 copies Snapshot. Pour les sauvegardes de base, incrémentielles ou différentielles suivantes, vous devez supprimer les anciennes copies Snapshot sauvegardées.

Avant d'effectuer la restauration de base, le volume sur lequel les données sont restaurées doit être de type `DP` et ce volume doit être à l'état restreint. Une fois la restauration effectuée, ce volume est automatiquement en ligne. Vous pouvez effectuer ensuite des restaurations incrémentielles ou différentielles sur ce volume dans l'ordre dans lequel les sauvegardes ont été effectuées.

Utilisation des copies Snapshot pendant la sauvegarde SMTape

Il est important de comprendre comment les copies Snapshot sont utilisées lors d'une sauvegarde de base SMTape et d'une sauvegarde incrémentielle. Vous devez également tenir compte des considérations d'ordre à prendre en compte lors de la sauvegarde sur SMTape.

Sauvegarde de base

Lors de l'exécution d'une sauvegarde de base, vous pouvez indiquer le nom de la copie Snapshot à sauvegarder sur bande. Si aucune copie Snapshot n'est spécifiée, selon le type d'accès du volume (lecture/écriture ou lecture seule), une copie Snapshot est créée automatiquement ou des copies Snapshot existantes sont utilisées. Lorsque vous spécifiez une copie Snapshot pour la sauvegarde, toutes les copies Snapshot antérieures à la copie Snapshot spécifiée sont également sauvegardées sur bande.

Si vous ne spécifiez pas de copie Snapshot pour la sauvegarde, les événements suivants se produisent :

- Pour un volume en lecture/écriture, une copie Snapshot est créée automatiquement.

  La nouvelle copie Snapshot et toutes les anciennes copies Snapshot sont sauvegardées sur bande.

- Pour un volume en lecture seule, toutes les copies Snapshot, y compris la dernière copie Snapshot, sont sauvegardées sur bande.

  Aucune sauvegarde n'est effectuée après le démarrage de la sauvegarde.

Sauvegarde incrémentielle

Pour les opérations de sauvegarde incrémentielle ou différentielle SMTape, les applications de sauvegarde conformes au protocole NDMP créent et gèrent les copies Snapshot.

Vous devez toujours spécifier une copie Snapshot lors de l'opération de sauvegarde incrémentielle. Pour que la sauvegarde incrémentielle soit couronnée de succès, la copie Snapshot sauvegardée lors de l'opération de sauvegarde précédente (copie de base ou incrémentielle) doit se trouver sur le volume à partir duquel la sauvegarde est effectuée. Pour vous assurer que vous utilisez cette copie Snapshot sauvegardée, vous devez tenir compte de la règle Snapshot attribuée à ce volume lors de la configuration de la règle de sauvegarde.

Considérations relatives aux sauvegardes SMTape sur les destinations SnapMirror

- Une relation de miroir de protection des données crée des copies Snapshot temporaires sur le volume de destination pour la réplication.

  Il est interdit d'utiliser ces copies Snapshot pour la sauvegarde SMTape.

- Lorsqu'une mise à jour SnapMirror se produit sur un volume de destination dans une relation de miroir de protection des données lors d'une opération de sauvegarde SMTape sur le même volume, la copie Snapshot sauvegardée par SMTape ne doit pas être supprimée du volume source.

  Lors de la sauvegarde, SMTape verrouille la copie Snapshot sur le volume de destination. Si la copie Snapshot correspondante est supprimée sur le volume source, l'opération de mise à jour SnapMirror suivante échoue.

- Vous ne devez pas utiliser ces copies Snapshot pendant la sauvegarde incrémentielle.

Fonctionnalités SMTape

Les fonctionnalités SMTape, telles que la sauvegarde des copies Snapshot, les sauvegardes incrémentielles et différentielles, la préservation des fonctions de déduplication et de compression des volumes restaurés et la « Tape seeding » des bandes, vous permettent d'optimiser vos opérations de sauvegarde et de restauration sur bande.

SMTape offre les fonctionnalités suivantes :

- Offre une solution de reprise après incident
- Permet des sauvegardes incrémentielles et différentielles
- Sauvegarde des copies Snapshot
- Permet la sauvegarde et la restauration des volumes dédupliqués et préserve la déduplication sur les volumes restaurés
- Sauvegarde les volumes compressés et préserve la compression sur les volumes restaurés
- Permet l'ensemencement des bandes

SMTape prend en charge le facteur de blocage en multiples de 4 Ko, dans une plage de 4 Ko à 256 Ko.

> Vous pouvez restaurer les données sur des volumes créés pour deux versions ONTAP consécutives majeures uniquement.

Fonctionnalités non prises en charge par SMTape

SMTape ne prend pas en charge les sauvegardes redémarrables et la vérification des fichiers sauvegardés.

Limites d'évolutivité pour les sessions de sauvegarde et de restauration SMTape

Lors de la réalisation des opérations de sauvegarde et de restauration SMTape via NDMP ou CLI (Tape seeding), vous devez connaître le nombre maximal de sessions de sauvegarde et de restauration SMTape qui peuvent être effectuées simultanément sur les systèmes de stockage dotés de différentes capacités de mémoire système. Ce nombre maximum dépend de la mémoire système d'un système de stockage.

> Les limites d'évolutivité des sessions de sauvegarde et de restauration SMTape sont différentes des limites des sessions NDMP et des sessions de vidage.

Mémoire système du système de stockage	Nombre total de sessions de sauvegarde et de restauration SMTape
Moins de 16 Go	6
Supérieur ou égal à 16 Go mais inférieur à 24 Go	16
Supérieur ou égal à 24 Go	32

Vous pouvez obtenir la mémoire système de votre système de stockage à l'aide du `sysconfig -a` commande (disponible via le nodeshell). Pour plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

Informations associées

Limite d'évolutivité pour les sessions NDMP

Limite d'évolutivité pour les sessions de sauvegarde et de restauration

En quoi consiste l'amorçage des bandes

La fonction SMTape permet d'initialiser un volume FlexVol de destination dans une relation de miroir de protection des données.

Le « Tape seeding » permet d'établir une relation de miroir de protection des données entre le système source et le système de destination via une connexion à faible bande passante.

La mise en miroir incrémentielle des copies Snapshot de la source vers la destination est possible via une connexion à faible bande passante. Cependant, une mise en miroir initiale de la copie Snapshot de base prend beaucoup de temps sur une connexion à faible bande passante. Il est ainsi possible d'effectuer une sauvegarde SMTape du volume source sur bande, puis d'utiliser la bande pour transférer la copie Snapshot de la base initiale vers la destination. Vous pouvez ensuite configurer des mises à jour SnapMirror incrémentielles sur le système de destination à l'aide de la connexion à faible bande passante.

Informations associées

"Concepts relatifs à ONTAP"

Fonctionnement de SMTape avec basculement du stockage et opérations d'ARL

Avant d'effectuer des opérations de sauvegarde ou de restauration SMTape, vous devez

comprendre le fonctionnement de ces opérations grâce au basculement du stockage (basculement et rétablissement) ou au transfert d'agrégats (ARL). Le `-override -vetoes` Détermine le comportement du moteur SMTape lors du basculement du stockage ou du transfert d'agrégats.

Lorsqu'une opération de sauvegarde ou de restauration SMTape est en cours d'exécution sur `-override -vetoes` l'option est définie sur `false`, Un basculement de stockage initié par l'utilisateur ou une opération ARL est arrêté et l'opération de sauvegarde ou de restauration est terminée. Si l'application de sauvegarde prend en charge l'extension CAB, vous pouvez continuer à effectuer les opérations de sauvegarde et de restauration incrémentielles SMTape sans reconfigurer les règles de sauvegarde. Cependant, si `-override-vetoes` l'option est définie sur `true`, Le basculement du stockage ou l'opération ARL est ensuite poursuivi et l'opération de sauvegarde ou de restauration SMTape est abandonnée.

Informations associées

"Gestion du réseau"

"Haute disponibilité"

Fonctionnement de SMTape avec le déplacement de volumes

Les opérations de sauvegarde SMTape et de déplacement de volumes peuvent fonctionner en parallèle jusqu'à la fin de la phase de mise en service finale du système de stockage. Après cette phase, les nouvelles opérations de sauvegarde SMTape ne peuvent pas s'exécuter sur le volume en cours de déplacement. Cependant, les opérations en cours continuent de fonctionner jusqu'à la fin.

Avant le démarrage de la phase de mise en service d'un volume, l'opération de déplacement de volume vérifie si les opérations de sauvegarde SMTape actives sur le même volume. En cas d'opérations de sauvegarde SMTape actives, l'opération de déplacement des volumes passe en mode « différé » de mise en service et permet le processus de sauvegarde SMTape. Une fois ces opérations de sauvegarde terminées, vous devez redémarrer manuellement l'opération de déplacement de volume.

Si l'application de sauvegarde prend en charge l'extension CAB, vous pouvez continuer à effectuer les sauvegardes incrémentielles sur bande et à les restaurer sur les volumes en lecture/écriture et en lecture seule sans reconfigurer les règles de sauvegarde.

Les opérations de restauration de base et de déplacement des volumes ne peuvent pas être exécutées simultanément. Toutefois, la restauration incrémentielle peut être exécutée en parallèle avec les opérations de déplacement de volumes, avec un comportement similaire à celui des opérations de sauvegarde SMTape lors des opérations de déplacement de volumes.

Informations associées

"Concepts relatifs à ONTAP"

Fonctionnement de SMTape avec les opérations de réhébergement de volumes

Les opérations SMTape ne peuvent pas commencer lorsqu'une opération de réhébergement de volume est en cours sur un volume. Lorsqu'un volume est impliqué dans une opération de réhébergement de volumes, les sessions SMTape ne doivent pas être lancées sur ce volume.

Lorsque des opérations de réhébergement de volumes sont en cours, la sauvegarde ou la restauration SMTape échoue. Lorsqu'une sauvegarde ou une restauration SMTape est en cours, les opérations de réhébergement de volume rencontrent un message d'erreur approprié. Cette condition s'applique aux opérations de sauvegarde ou de restauration basées sur NDMP et sur l'interface de ligne de commande.

Comment la politique de sauvegarde NDMP est-elle affectée pendant ADB

Lorsque l'équilibreur de données automatique (ADB) est activé, l'équilibreur analyse les statistiques d'utilisation des agrégats afin d'identifier l'agrégat qui a dépassé le pourcentage d'utilisation à seuil élevé configuré.

Après avoir identifié l'agrégat qui a dépassé le seuil, l'équilibreur identifie un volume pouvant être déplacé vers des agrégats résidant dans un autre nœud du cluster et tente de déplacer ce volume. Cette situation affecte la stratégie de sauvegarde configurée pour ce volume car si l'application de gestion des données (DMA) n'est pas compatible AVEC CAB, l'utilisateur doit reconfigurer la stratégie de sauvegarde et exécuter l'opération de sauvegarde de base.

> Si le DMA est conscient DE CAB et que la politique de sauvegarde a été configurée à l'aide d'une interface spécifique, alors l'ADB n'est pas affecté.

Comment les opérations de sauvegarde et de restauration SMTape sont affectées dans les configurations MetroCluster

Avant d'effectuer les opérations de sauvegarde et de restauration SMTape sur une configuration MetroCluster, vous devez d'abord comprendre comment les opérations SMTape sont affectées lors d'une opération de basculement ou de rétablissement.

Opération de sauvegarde ou de restauration SMTape, suivie du basculement

Envisager deux clusters : cluster 1 et cluster 2. Lors d'une opération de sauvegarde ou de restauration SMTape sur le cluster 1, si un basculement est initié du cluster 1 au cluster 2, ce qui suit se produit :

- Si la valeur de `-override-vetoes` l'option est `false`, le processus de basculement est alors interrompu et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, Puis l'opération de sauvegarde ou de restauration SMTape est abandonnée et le processus de basculement se poursuit.

Opération de sauvegarde ou de restauration SMTape, suivie du rétablissement

Un basculement est effectué du cluster 1 vers le cluster 2. Une opération de sauvegarde ou de restauration SMTape est lancée sur le cluster 2. L'opération SMTape permet de sauvegarder ou de restaurer un volume situé sur le cluster 2. À ce stade, si un rétablissement est initié du cluster 2 au cluster 1, ce qui suit se produit :

- Si la valeur de `-override-vetoes` l'option est `false`, le processus de rétablissement est alors interrompu et l'opération de sauvegarde ou de restauration se poursuit.
- Si la valeur de l'option est `true`, l'opération de sauvegarde ou de restauration est alors abandonnée et le processus de rétablissement se poursuit.

Opération de sauvegarde ou de restauration SMTape initiée lors du basculement ou du rétablissement

Lors d'un processus de basculement du cluster 1 vers le cluster 2, si une opération de sauvegarde ou de restauration SMTape est lancée sur le cluster 1, alors l'opération de sauvegarde ou de restauration échoue et

le basculement se poursuit.

Lors du processus de rétablissement du cluster 2 vers le cluster 1, si une opération de sauvegarde ou de restauration SMTape est lancée depuis le cluster 2, l'opération de sauvegarde ou de restauration échoue et le rétablissement se poursuit.

Surveillance des opérations de sauvegarde sur bande et de restauration des volumes FlexVol

Surveiller les opérations de sauvegarde sur bande et de restauration des volumes FlexVol

Vous pouvez afficher les fichiers journaux des événements pour surveiller les opérations de sauvegarde et de restauration sur bande. ONTAP consigne automatiquement des événements significatifs relatifs aux sauvegardes et aux restaurations, ainsi que l'heure à laquelle ils se produisent dans un fichier journal nommé `backup` dans les contrôleurs `/etc/log/` répertoire. Par défaut, la journalisation des événements est définie sur `on`.

Vous pouvez vouloir afficher les fichiers journaux des événements pour les raisons suivantes :

- Vérification de la réussite d'une sauvegarde nocturne
- Collecte de statistiques sur les opérations de sauvegarde
- Pour utiliser les informations contenues dans les fichiers journaux d'événements précédents afin de faciliter le diagnostic des problèmes liés aux opérations de sauvegarde et de restauration

Une fois par semaine, les fichiers journaux d'événements sont pivotés. Le `/etc/log/backup` le fichier est renommé `/etc/log/backup.0`, le `/etc/log/backup.0` le fichier est renommé `/etc/log/backup.1`, etc. Le système enregistre les fichiers journaux pendant six semaines maximum ; vous pouvez donc avoir jusqu'à sept fichiers de messages (`/etc/log/backup.[0-5]` et le courant `/etc/log/backup` fichier).

Accéder aux fichiers journaux des événements

Vous pouvez accéder aux fichiers journaux des événements pour les opérations de sauvegarde sur bande et de restauration dans `/etc/log/` répertoire à l'aide du `rdfile` commande au nodeshell. Vous pouvez afficher ces fichiers journaux d'événements pour surveiller les opérations de sauvegarde sur bande et de restauration.

Description de la tâche

Avec des configurations supplémentaires, telles qu'un rôle de contrôle d'accès avec accès à l' `spi` service web ou compte d'utilisateur configuré avec le `http` méthode d'accès, vous pouvez également utiliser un navigateur web pour accéder à ces fichiers journaux.

Étapes

1. Pour accéder au nodeshell, entrez la commande suivante :

   `node run -node` ***`node_name`***

   `node_name` est le nom du nœud.

2. Pour accéder aux fichiers journaux des événements pour les opérations de sauvegarde et de restauration sur bande, entrez la commande suivante :

```
rdfile /etc/log/backup
```

Informations associées

"Administration du système"

"Concepts relatifs à ONTAP"

Format du message du journal des événements de vidage et de restauration

Présentation du format de message du journal des événements de vidage et de restauration

Pour chaque événement de vidage et de restauration, un message est écrit dans le fichier journal de sauvegarde.

Le format du message du journal des événements de vidage et de restauration est le suivant :

`type timestamp identifier event (event_info)`

La liste suivante décrit les champs au format des messages du journal des événements :

- Chaque message du journal commence par l'un des indicateurs de type décrits dans le tableau suivant :

Type	Description
journal	Journalisation de l'événement
dmp	Événement de vidage
rst	Événement de restauration

- `timestamp` affiche la date et l'heure de l'événement.
- Le `identifier` Le champ d'un événement de vidage inclut le chemin de vidage et l'ID unique du dump. Le `identifier` le champ d'un événement de restauration utilise uniquement le nom du chemin de destination de restauration comme identifiant unique. Les messages d'événement liés à la journalisation n'incluent pas de `identifier` légale.

En quoi sont les événements d'enregistrement

Le champ d'événement d'un message qui commence par un journal indique le début d'une consignation ou la fin d'une consignation.

Il contient l'un des événements présentés dans le tableau suivant :

Événement	Description
Démarrer_Logging	Indique le début de la consignation ou que la consignation a été remise sous tension après la désactivation.

Événement	Description
Stop_Logging	Indique que la consignation a été désactivée.

Quels sont les événements de vidage

Le champ événement d'un événement de vidage contient un type d'événement suivi d'informations spécifiques à un événement entre parenthèses.

Le tableau suivant décrit les événements, leurs descriptions et les informations d'événement associées qui peuvent être enregistrées pour une opération de vidage :

Événement	Description	Informations sur l'événement
Démarrer	Le dump NDMP est démarré	Niveau de vidage et type de vidage
Fin	Vidage terminé avec succès	Quantité de données traitées
Abandonner	L'opération est annulée	Quantité de données traitées
Options	Les options spécifiées sont répertoriées	Toutes les options et leurs valeurs associées, y compris les options NDMP
Tape_open	La bande est ouverte en lecture/écriture	Nom du nouveau périphérique de bande
Tape_close	La bande est fermée pour lecture/écriture	Nom du lecteur de bande
Changement de phase	Un vidage entre dans une nouvelle phase de traitement	Nom de la nouvelle phase
Erreur	Un vidage a rencontré un événement inattendu	Message d'erreur
Snapshot	Une copie Snapshot est créée ou située	Nom et heure de la copie Snapshot
Base_dump	Une entrée de vidage de base dans le métafichier interne a été localisée	Le niveau et le temps du vidage de la base (pour les vidages incrémentiels uniquement)

Que sont les événements de restauration

Le champ événement d'un événement de restauration contient un type d'événement suivi d'informations spécifiques à un événement entre parenthèses.

Le tableau suivant fournit des informations sur les événements, leurs descriptions et les informations sur l'événement associé qui peuvent être enregistrées pour une opération de restauration :

Événement	Description	Informations sur l'événement
Démarrer	La restauration NDMP est démarrée	Niveau de restauration et type de restauration
Fin	Restaurations effectuées avec succès	Nombre de fichiers et quantité de données traitées
Abandonner	L'opération est annulée	Nombre de fichiers et quantité de données traitées
Options	Les options spécifiées sont répertoriées	Toutes les options et leurs valeurs associées, y compris les options NDMP
Tape_open	La bande est ouverte en lecture/écriture	Nom du nouveau périphérique de bande
Tape_close	La bande est fermée pour lecture/écriture	Nom du lecteur de bande
Changement de phase	La restauration entre dans une nouvelle phase de traitement	Nom de la nouvelle phase
Erreur	La restauration rencontre un événement inattendu	Message d'erreur

Activation ou désactivation de la journalisation des événements

Vous pouvez activer ou désactiver la journalisation des événements.

Étapes

1. Pour activer ou désactiver la journalisation des événements, entrez la commande suivante au niveau du clustershell :

   options -*option_name* backup.log.enable -*option-value* {on | off}

   `on` active la journalisation des événements.

   `off` désactive la journalisation des événements.

   Le journal des événements est activé par défaut.

Messages d’erreur relatifs à la sauvegarde sur bande et à la restauration des volumes FlexVol

Messages d’erreur de sauvegarde et de restauration

Limitation des ressources : pas de thread disponible

- **Message**

  ```
  Resource limitation: no available thread
  ```

- **Cause**

  Le nombre maximal de threads d’E/S de bande locale actifs est actuellement utilisé. Vous pouvez avoir un maximum de 16 lecteurs de bande locaux actifs.

- * Action corrective*

  Attendez la fin de certaines tâches de bande avant de lancer une nouvelle tâche de sauvegarde ou de restauration.

Réservation de bandes préemptée

- **Message**

  ```
  Tape reservation preempted
  ```

- **Cause**

  Le lecteur de bande est utilisé par une autre opération ou la bande a été fermée prématurément.

- * Action corrective*

  Assurez-vous que le lecteur de bande n’est pas utilisé par une autre opération et que l’application DMA n’a pas interrompu le travail, puis réessayez.

Impossible d’initialiser le support

- **Message**

  ```
  Could not initialize media
  ```

- **Cause**

  Cette erreur peut s’afficher pour l’une des raisons suivantes :

  - Le lecteur de bande utilisé pour la sauvegarde est corrompu ou endommagé.
  - La bande ne contient pas la sauvegarde complète ou est corrompue.
  - Le nombre maximal de threads d’E/S de bande locale actifs est actuellement utilisé.

    Vous pouvez avoir un maximum de 16 lecteurs de bande locaux actifs.

- * Action corrective*

- Si le lecteur de bande est endommagé ou endommagé, relancez l'opération avec un lecteur de bande valide.
- Si la bande ne contient pas la sauvegarde complète ou est corrompue, vous ne pouvez pas effectuer l'opération de restauration.
- Si les ressources sur bande ne sont pas disponibles, attendez la fin de certaines tâches de sauvegarde ou de restauration, puis relancez l'opération.

Nombre maximal de sauvegardes ou de restaurations autorisées (limite maximale de session) en cours

- **Message**

  `Maximum number of allowed dumps or restores (maximum session limit) in progress`

- **Cause**

  Le nombre maximal de tâches de sauvegarde ou de restauration est déjà en cours d'exécution.

- * Action corrective*

  Réessayez l'opération une fois que certains travaux en cours d'exécution ont terminé.

Erreur de support lors de l'écriture sur bande

- **Message**

  `Media error on tape write`

- **Cause**

  La bande utilisée pour la sauvegarde est endommagée.

- * Action corrective*

  Remplacez la bande et relancez la procédure de sauvegarde.

Échec de l'écriture sur bande

- **Message**

  `Tape write failed`

- **Cause**

  La bande utilisée pour la sauvegarde est endommagée.

- * Action corrective*

  Remplacez la bande et relancez la procédure de sauvegarde.

Échec de l'écriture sur la bande - une nouvelle bande a rencontré une erreur de support

- **Message**

```
Tape write failed - new tape encountered media error
```

- **Cause**

  La bande utilisée pour la sauvegarde est endommagée.

- * Action corrective*

  Remplacez la bande et réessayez la sauvegarde.

Échec de l'écriture de la bande : la nouvelle bande est cassée ou protégée en écriture

- **Message**

```
Tape write failed - new tape is broken or write protected
```

- **Cause**

  La bande utilisée pour la sauvegarde est corrompue ou protégée en écriture.

- * Action corrective*

  Remplacez la bande et réessayez la sauvegarde.

Échec de l'écriture sur bande : la nouvelle bande est déjà à la fin du support

- **Message**

```
Tape write failed - new tape is already at the end of media
```

- **Cause**

  L'espace disponible sur la bande est insuffisant pour terminer la sauvegarde.

- * Action corrective*

  Remplacez la bande et réessayez la sauvegarde.

Erreur d'écriture de bande

- **Message**

```
Tape write error - The previous tape had less than the required minimum
capacity, size MB, for this tape operation, The operation should be restarted
from the beginning
```

- **Cause**

  La capacité de la bande est insuffisante pour contenir les données de sauvegarde.

- * Action corrective*

  Utilisez des bandes d'une capacité supérieure et relancez la tâche de sauvegarde.

Erreur de support lors de la lecture de la bande

- **Message**

  ```
  Media error on tape read
  ```

- **Cause**

  La bande à partir de laquelle les données sont restaurées est corrompue et peut ne pas contenir toutes les données de sauvegarde.

- * Action corrective*

  Si vous êtes sûr que la bande a la sauvegarde complète, réessayez l'opération de restauration. Si la bande ne contient pas la sauvegarde complète, vous ne pouvez pas effectuer l'opération de restauration.

Erreur de lecture de bande

- **Message**

  ```
  Tape read error
  ```

- **Cause**

  Le lecteur de bande est endommagé ou la bande ne contient pas la sauvegarde complète.

- * Action corrective*

  Si le lecteur de bande est endommagé, utilisez un autre lecteur de bande. Si la bande ne contient pas la sauvegarde complète, vous ne pouvez pas restaurer les données.

Déjà à la fin de la bande

- **Message**

  ```
  Already at the end of tape
  ```

- **Cause**

  La bande ne contient pas de données ou doit être rembobinée.

- * Action corrective*

  Si la bande ne contient pas de données, utilisez la bande contenant la sauvegarde et relancez la procédure de restauration. Sinon, rembobinez la bande et relancez la tâche de restauration.

La taille de l'enregistrement sur bande est trop petite. Essayez une taille plus grande.

- **Message**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Cause**

Le facteur de blocage spécifié pour l'opération de restauration est plus petit que le facteur de blocage utilisé pendant la sauvegarde.

- * Action corrective*

  Utilisez le même facteur de blocage que celui spécifié lors de la sauvegarde.

La taille de l'enregistrement sur bande doit être Block_size1 et non block_site2

- **Message**

  `Tape record size should be block_size1 and not block_size2`

- **Cause**

  Le facteur de blocage spécifié pour la restauration locale est incorrect.

- * Action corrective*

  Relancez la tâche de restauration avec `block_size1` comme facteur de blocage.

La taille d'enregistrement de la bande doit être comprise entre 4 Ko et 256 Ko

- **Message**

  `Tape record size must be in the range between 4KB and 256KB`

- **Cause**

  Le facteur de blocage spécifié pour l'opération de sauvegarde ou de restauration n'est pas dans la plage autorisée.

- * Action corrective*

  Spécifiez un facteur de blocage compris entre 4 Ko et 256 Ko.

Messages d'erreur NDMP

Erreur de communication réseau

- **Message**

  `Network communication error`

- **Cause**

  La communication avec une bande distante dans une connexion NDMP à trois voies a échoué.

- * Action corrective*

  Vérifiez la connexion réseau au dispositif de déplacement distant.

Message de Read Socket : error_string

- **Message**

  ```
  Message from Read Socket: error_string
  ```

- **Cause**

  La restauration de la communication à partir de la bande distante dans la connexion NDMP à 3 voies comporte des erreurs.

- * Action corrective*

  Vérifiez la connexion réseau au dispositif de déplacement distant.

Message de Write Dirnet : chaîne_d'erreur

- **Message**

  ```
  Message from Write Dirnet: error_string
  ```

- **Cause**

  Une erreur est survenue lors de la sauvegarde de la communication sur une bande distante au niveau d'une connexion NDMP à trois voies.

- * Action corrective*

  Vérifiez la connexion réseau au dispositif de déplacement distant.

Prise de lecture reçue EOF

- **Message**

  ```
  Read Socket received EOF
  ```

- **Cause**

  Tentative de communication avec une bande distante dans une connexion à trois voies NDMP a atteint la fin du repère de fichier. Vous tentez peut-être d'effectuer une restauration à trois voies à partir d'une image de sauvegarde d'une taille de bloc supérieure.

- * Action corrective*

  Spécifiez la taille de bloc correcte et relancez l'opération de restauration.

ndmpd numéro de version non valide : numéro_version ``

- **Message**

  ```
  ndmpd invalid version number: version_number
  ```

- **Cause**

La version NDMP spécifiée n’est pas prise en charge par le système de stockage.

- * Action corrective*

  Spécifiez NDMP version 4.

Session ndmpd session session_ID non active

- **Message**

  `ndmpd session session_ID not active`

- **Cause**

  Il se peut que la session NDMP n’existe pas.

- * Action corrective*

  Utilisez le `ndmpd status` Commande pour afficher les sessions NDMP actives.

Impossible d’obtenir la référence vol pour Volume nom_volume

- **Message**

  `Could not obtain vol ref for Volume vol_name`

- **Cause**

  La référence de volume n’a pas pu être obtenue car le volume peut être utilisé par d’autres opérations.

- * Action corrective*

  Réessayez ultérieurement.

Type de connexion de données ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] non pris en charge pour les connexions de contrôle ["IPv6"|"IPv4"]

- **Message**

  `Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported for ["IPv6"|"IPv4"] control connections`

- **Cause**

  En mode node-scoped NDMP, la connexion de données NDMP établie doit être du même type d’adresse réseau (IPv4 ou IPv6) que la connexion de contrôle NDMP.

- * Action corrective*

  Contactez le fournisseur de votre application de sauvegarde.

ÉCOUTE DES DONNÉES : erreur de préparation de la connexion des données DE LA CABINE

- **Message**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Cause**

  L'écoute des données NDMP échoue lorsque l'application de sauvegarde a négocié l'extension CAB avec le serveur NDMP et il existe une discordance dans le type d'adresse de connexion de données NDMP spécifié entre le message NDMP_CAB_DATA_CONN_READY et NDMP_DATA_LISTEN.

- * Action corrective*

  Contactez le fournisseur de votre application de sauvegarde.

CONNEXION DES DONNÉES : erreur de préparation de la connexion des données DE LA CABINE

- **Message**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Cause**

  La connexion des données NDMP échoue lorsque l'application de sauvegarde a négocié l'extension CAB avec le serveur NDMP et qu'il existe une discordance dans le type d'adresse de connexion de données NDMP spécifié entre le message NDMP_CAB_DATA_CONN_READY et le message NDMP_DATA_CONNECT.

- * Action corrective*

  Contactez le fournisseur de votre application de sauvegarde.

Erreur:échec de l'affichage : impossible d'obtenir le mot de passe de l'utilisateur '<nom d'utilisateur>'

- **Message**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Cause**

  Configuration de compte utilisateur incomplète pour NDMP

- * Action corrective*

  Assurez-vous que le compte utilisateur est associé à la méthode d'accès SSH et que la méthode d'authentification est un mot de passe utilisateur.

Vidage des messages d'erreur

Le volume de destination est en lecture seule

- **Message**

```
Destination volume is read-only
```

- **Cause**

  Le chemin vers lequel l'opération de restauration est tentée est en lecture seule.

- * Action corrective*

  Essayez de restaurer les données à un autre emplacement.

Le qtree de destination est en lecture seule

- **Message**

```
Destination qtree is read-only
```

- **Cause**

  Le qtree vers laquelle la restauration est tentée de lire uniquement.

- * Action corrective*

  Essayez de restaurer les données à un autre emplacement.

Vidages temporairement désactivés sur le volume, réessayez

- **Message**

```
Dumps temporarily disabled on volume, try again
```

- **Cause**

  La tentative de sauvegarde du dump NDMP est effectuée sur un volume de destination SnapMirror faisant partie d'un ou plusieurs `snapmirror break` ou un `snapmirror resync` fonctionnement.

- * Action corrective*

  Attendez le `snapmirror break` ou `snapmirror resync` opération pour terminer puis effectuer l'opération de vidage.

> Chaque fois que l'état d'un volume de destination SnapMirror passe de la lecture/écriture à la lecture seule ou de la lecture seule à la lecture/écriture, vous devez effectuer une sauvegarde de base.

Étiquettes NFS non reconnues

- **Message**

```
Error: Aborting: dump encountered NFS security labels in the file system
```

- **Cause**

  Les étiquettes de sécurité NFS sont prises en charge à partir de ONTAP 9.9.1 lorsque NFSv4.2 est activé.

Toutefois, les étiquettes de sécurité NFS ne sont actuellement pas reconnues par le moteur de vidage. S'il rencontre des étiquettes de sécurité NFS sur les fichiers, les répertoires ou tout fichier spécial dans un format quelconque de dump, le dump échoue.

- * Action corrective*

  Vérifiez qu'aucun fichier ni répertoire ne possède d'étiquettes de sécurité NFS.

Aucun fichier n'a été créé

- **Message**

  ```
  No files were created
  ```

- **Cause**

  Une tentative de DAR d'annuaire a été effectuée sans activer la fonctionnalité DAR améliorée.

- * Action corrective*

  Activez la fonctionnalité DAR améliorée et réessayez le DAR.

Échec de la restauration du fichier <nom du fichier>

- **Message**

  ```
  Restore of the file file name failed
  ```

- **Cause**

  Lorsqu'un fichier DAR (Direct Access Recovery) d'un fichier dont le nom de fichier est le même que celui d'un LUN sur le volume de destination est exécuté, le DAR échoue.

- * Action corrective*

  Essayez de nouveau DAR du fichier.

La troncature a échoué pour src inode <numéro inode>…

- **Message**

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  inode.
  ```

- **Cause**

  L'inode d'un fichier est supprimé lors de la restauration du fichier.

- * Action corrective*

  Attendez la fin de l'opération de restauration sur un volume avant d'utiliser ce volume.

Impossible de verrouiller un snapshot requis par le dump

- **Message**

  ```
  Unable to lock a snapshot needed by dump
  ```

- **Cause**

  La copie Snapshot spécifiée pour la sauvegarde n’est pas disponible.

- * Action corrective*

  Réessayez la sauvegarde avec une autre copie Snapshot.

  Utilisez le `snap list` Commande pour afficher la liste des copies Snapshot disponibles.

Impossible de localiser les fichiers bitmap

- **Message**

  ```
  Unable to locate bitmap files
  ```

- **Cause**

  Les fichiers bitmap requis pour l’opération de sauvegarde ont peut-être été supprimés. Dans ce cas, la sauvegarde ne peut pas être redémarrée.

- * Action corrective*

  Effectuez à nouveau la sauvegarde.

Le volume est temporairement dans un état transitoire

- **Message**

  ```
  Volume is temporarily in a transitional state
  ```

- **Cause**

  Le volume en cours de sauvegarde est temporairement démonté.

- * Action corrective*

  Attendez un certain temps avant d’effectuer à nouveau la sauvegarde.

Messages d’erreur SMTape

Blocs hors service

- **Message**

  ```
  Chunks out of order
  ```

- **Cause**

Les bandes de sauvegarde ne sont pas restaurées dans l'ordre correct.

- * Action corrective*

  Relancez l'opération de restauration et chargez les bandes dans l'ordre correct.

Le format de bloc n'est pas pris en charge

- **Message**

  ```
  Chunk format not supported
  ```

- **Cause**

  L'image de sauvegarde n'est pas SMTape.

- * Action corrective*

  Si l'image de sauvegarde n'est pas SMTape, essayez de procéder à nouveau à l'opération avec une bande dotée de la sauvegarde SMTape.

Impossible d'allouer de la mémoire

- **Message**

  ```
  Failed to allocate memory
  ```

- **Cause**

  La mémoire du système est insuffisante.

- * Action corrective*

  Réessayez ultérieurement lorsque le système n'est pas trop occupé.

Impossible d'obtenir le tampon de données

- **Message**

  ```
  Failed to get data buffer
  ```

- **Cause**

  Le système de stockage est à court de mémoire tampon.

- * Action corrective*

  Attendez la fin de certaines opérations du système de stockage, puis relancez la tâche.

Impossible de trouver le snapshot

- **Message**

  ```
  Failed to find snapshot
  ```

- **Cause**

  La copie Snapshot spécifiée pour la sauvegarde est indisponible.

- * Action corrective*

  Vérifiez si la copie Snapshot spécifiée est disponible. Si ce n’est pas le cas, réessayez avec la copie Snapshot appropriée.

Impossible de créer un snapshot

- **Message**

  ```
  Failed to create snapshot
  ```

- **Cause**

  Le volume contient déjà le nombre maximal de copies Snapshot.

- * Action corrective*

  Supprimez certaines copies Snapshot, puis réessayez l’opération de sauvegarde.

Impossible de verrouiller le snapshot

- **Message**

  ```
  Failed to lock snapshot
  ```

- **Cause**

  La copie Snapshot est utilisée ou a été supprimée.

- * Action corrective*

  Si la copie Snapshot est utilisée par une autre opération, attendez la fin de cette opération, puis réessayez la sauvegarde. Si la copie Snapshot a été supprimée, vous ne pouvez pas effectuer la sauvegarde.

Impossible de supprimer le snapshot

- **Message**

  ```
  Failed to delete snapshot
  ```

- **Cause**

  Impossible de supprimer la copie Snapshot automatique, car elle est en cours d’utilisation par d’autres opérations.

- * Action corrective*

  Utilisez le `snap` Commande permettant de déterminer l’état de la copie Snapshot. Si aucune copie Snapshot n’est requise, supprimez-la manuellement.

Impossible d’obtenir le dernier snapshot

- **Message**

  ```
  Failed to get latest snapshot
  ```

- **Cause**

  Il se peut que la dernière copie Snapshot n’existe pas, car le volume est en cours d’initialisation par SnapMirror.

- * Action corrective*

  Réessayez une fois l’initialisation terminée.

Impossible de charger une nouvelle bande

- **Message**

  ```
  Failed to load new tape
  ```

- **Cause**

  Erreur dans le lecteur de bande ou le support.

- * Action corrective*

  Remplacez la bande et réessayez l’opération.

Impossible d’initialiser la bande

- **Message**

  ```
  Failed to initialize tape
  ```

- **Cause**

  Ce message d’erreur peut s’afficher pour l’une des raisons suivantes :

  - L’image de sauvegarde n’est pas SMTape.
  - Le facteur de blocage de la bande spécifié est incorrect.
  - La bande est corrompue ou endommagée.
  - La mauvaise bande est chargée pour la restauration.

- * Action corrective*
  - Si l’image de sauvegarde n’est pas SMTape, essayez de procéder à nouveau à l’opération avec une bande dotée d’une sauvegarde SMTape.
  - Si le facteur de blocage est incorrect, spécifiez le facteur de blocage correct et relancez l’opération.
  - Si la bande est corrompue, vous ne pouvez pas effectuer l’opération de restauration.
  - Si la mauvaise bande est chargée, recommencez l’opération avec la bonne bande.

Impossible d’initialiser le flux de restauration

- **Message**

  ```
  Failed to initialize restore stream
  ```

- **Cause**

  Ce message d’erreur peut s’afficher pour l’une des raisons suivantes :

  - L’image de sauvegarde n’est pas SMTape.
  - Le facteur de blocage de la bande spécifié est incorrect.
  - La bande est corrompue ou endommagée.
  - La mauvaise bande est chargée pour la restauration.

- * Action corrective*
  - Si l’image de sauvegarde n’est pas SMTape, essayez de procéder à nouveau à l’opération avec une bande dotée de la sauvegarde SMTape.
  - Si le facteur de blocage est incorrect, spécifiez le facteur de blocage correct et relancez l’opération.
  - Si la bande est corrompue, vous ne pouvez pas effectuer l’opération de restauration.
  - Si la mauvaise bande est chargée, recommencez l’opération avec la bonne bande.

Impossible de lire l’image de sauvegarde

- **Message**

  ```
  Failed to read backup image
  ```

- **Cause**

  La bande est corrompue

- * Action corrective*

  Si la bande est corrompue, vous ne pouvez pas effectuer l’opération de restauration.

En-tête d’image manquant ou corrompu

- **Message**

  ```
  Image header missing or corrupted
  ```

- **Cause**

  La bande ne contient pas de sauvegarde SMTape valide.

- * Action corrective*

  Réessayez avec une bande contenant une sauvegarde valide.

Assertion interne

- **Message**

  `Internal assertion`

- **Cause**

  Il y a une erreur SMTape interne.

- * Action corrective*

  Signalez l'erreur et envoyez le `etc/log/backup` dossier au support technique.

Numéro magique d'image de sauvegarde non valide

- **Message**

  `Invalid backup image magic number`

- **Cause**

  L'image de sauvegarde n'est pas SMTape.

- * Action corrective*

  Si l'image de sauvegarde n'est pas SMTape, essayez de procéder à nouveau à l'opération avec une bande dotée de la sauvegarde SMTape.

Checksum d'image de sauvegarde non valide

- **Message**

  `Invalid backup image checksum`

- **Cause**

  La bande est corrompue

- * Action corrective*

  Si la bande est corrompue, vous ne pouvez pas effectuer l'opération de restauration.

Bande d'entrée non valide

- **Message**

  `Invalid input tape`

- **Cause**

  La signature de l'image de sauvegarde n'est pas valide dans l'en-tête de bande. Les données de la bande sont corrompues ou ne contiennent pas d'image de sauvegarde valide.

- * Action corrective*

  Relancez la procédure de restauration avec une image de sauvegarde valide.

Chemin de volume non valide

- **Message**

  `Invalid volume path`

- **Cause**

  Le volume spécifié pour l'opération de sauvegarde ou de restauration est introuvable.

- * Action corrective*

  Relancez le travail avec un chemin de volume et un nom de volume valides.

Non-concordance de l'ID du jeu de sauvegarde

- **Message**

  `Mismatch in backup set ID`

- **Cause**

  La bande chargée pendant un changement de bande ne fait pas partie du jeu de sauvegarde.

- * Action corrective*

  Chargez la bonne bande et relancez le travail.

Incompatibilité dans l'horodatage de sauvegarde

- **Message**

  `Mismatch in backup time stamp`

- **Cause**

  La bande chargée pendant un changement de bande ne fait pas partie du jeu de sauvegarde.

- * Action corrective*

  Utilisez le `smtape restore -h` commande pour vérifier les informations d'en-tête d'une bande.

Travail interrompu en raison de l'arrêt

- **Message**

  `Job aborted due to shutdown`

- **Cause**

Le système de stockage est en cours de redémarrage.

- * Action corrective*

  Relancez le travail après le redémarrage du système de stockage.

Travail interrompu en raison de la suppression automatique de l'instantané

- **Message**

  ```
  Job aborted due to Snapshot autodelete
  ```

- **Cause**

  L'espace disponible sur le volume est insuffisant et a déclenché la suppression automatique des copies Snapshot.

- * Action corrective*

  Libérez de l'espace dans le volume et relancez le travail.

La bande est actuellement utilisée par d'autres opérations

- **Message**

  ```
  Tape is currently in use by other operations
  ```

- **Cause**

  Le lecteur de bande est utilisé par un autre travail.

- * Action corrective*

  Réessayez la sauvegarde une fois la tâche active terminée.

Bandes hors service

- **Message**

  ```
  Tapes out of order
  ```

- **Cause**

  La première bande de la séquence de restauration pour l'opération de restauration n'a pas d'en-tête d'image.

- * Action corrective*

  Chargez la bande avec l'en-tête de l'image et relancez le travail.

Echec du transfert (abandon en raison de l'opération MetroCluster)

- **Message**

```
Transfer failed (Aborted due to MetroCluster operation)
```

- **Cause**

  L'opération SMTape est abandonnée en raison d'une opération de basculement ou de rétablissement.

- * Action corrective*

  Effectuez l'opération SMTape une fois le basculement ou le rétablissement terminé.

Échec du transfert (annulation initiée par l'ARL)

- **Message**

```
Transfer failed (ARL initiated abort)
```

- **Cause**

  Lorsqu'une opération SMTape est en cours lorsqu'un transfert d'agrégats est lancé, l'opération SMTape est abandonnée.

- * Action corrective*

  Effectuez l'opération SMTape une fois l'opération de transfert d'agrégats terminée.

Echec du transfert (annulation initiée par le CFO)

- **Message**

```
Transfer failed (CFO initiated abort)
```

- **Cause**

  L'opération SMTape est abandonnée en raison d'une opération de basculement du stockage (basculement et rétablissement) d'un agrégat CFO.

- * Action corrective*

  Effectuez l'opération SMTape après le basculement du stockage vers la fin de l'agrégat CFO.

Echec du transfert (annulation initiée SFO)

- **Message**

```
Transfer failed (SFO initiated abort)
```

- **Cause**

  L'opération SMTape est abandonnée en raison d'une opération de basculement du stockage (basculement et rétablissement).

- * Action corrective*

  Effectue l'opération SMTape après la fin de l'opération de basculement (basculement et rétablissement) du

stockage.

Agrégat sous-jacent en cours de migration

- **Message**

  ```
  Underlying aggregate under migration
  ```

- **Cause**

  Lorsqu'une opération SMTape est lancée sur un agrégat en cours de migration (basculement du stockage ou transfert d'agrégats), l'opération SMTape échoue.

- * Action corrective*

  Effectuez l'opération SMTape une fois la migration de l'agrégat terminée.

Le volume est en cours de migration

- **Message**

  ```
  Volume is currently under migration
  ```

- **Cause**

  La migration de volumes et la sauvegarde SMTape ne peuvent pas s'exécuter simultanément.

- * Action corrective*

  Relancez la procédure de sauvegarde une fois la migration du volume terminée.

Volume hors ligne

- **Message**

  ```
  Volume offline
  ```

- **Cause**

  Le volume sauvegardé est hors ligne.

- * Action corrective*

  Mettez le volume en ligne et réessayez la sauvegarde.

Volume non restreint

- **Message**

  ```
  Volume not restricted
  ```

- **Cause**

  Le volume de destination vers lequel les données sont restaurées n'est pas restreint.

- * Action corrective*

  Limitez le volume et relancez l'opération de restauration.

Configuration NDMP

Présentation de la configuration NDMP

Vous pouvez rapidement configurer un cluster ONTAP 9 de sorte qu'il utilise le protocole NDMP (Network Data Management Protocol) pour sauvegarder les données directement sur bande à l'aide d'une application de sauvegarde tierce.

Si l'application de backup supporte Cluster Aware Backup (CAB), vous pouvez configurer NDMP sous la forme *SVM-scoped* ou *node-scoped* :

- SVM-scoped au niveau du cluster (admin SVM) permet de sauvegarder tous les volumes hébergés sur différents nœuds du cluster. SVM-scoped NDMP est recommandé si possible.
- Node-scoped NDMP vous permet de sauvegarder tous les volumes hébergés sur ce nœud.

Si l'application de backup ne prend pas en charge CAB, il faut utiliser node-scoped NDMP.

SVM-scoped et node-scoped NDMP sont mutuellement exclusifs ; ils ne peuvent pas être configurés sur le même cluster.

> Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

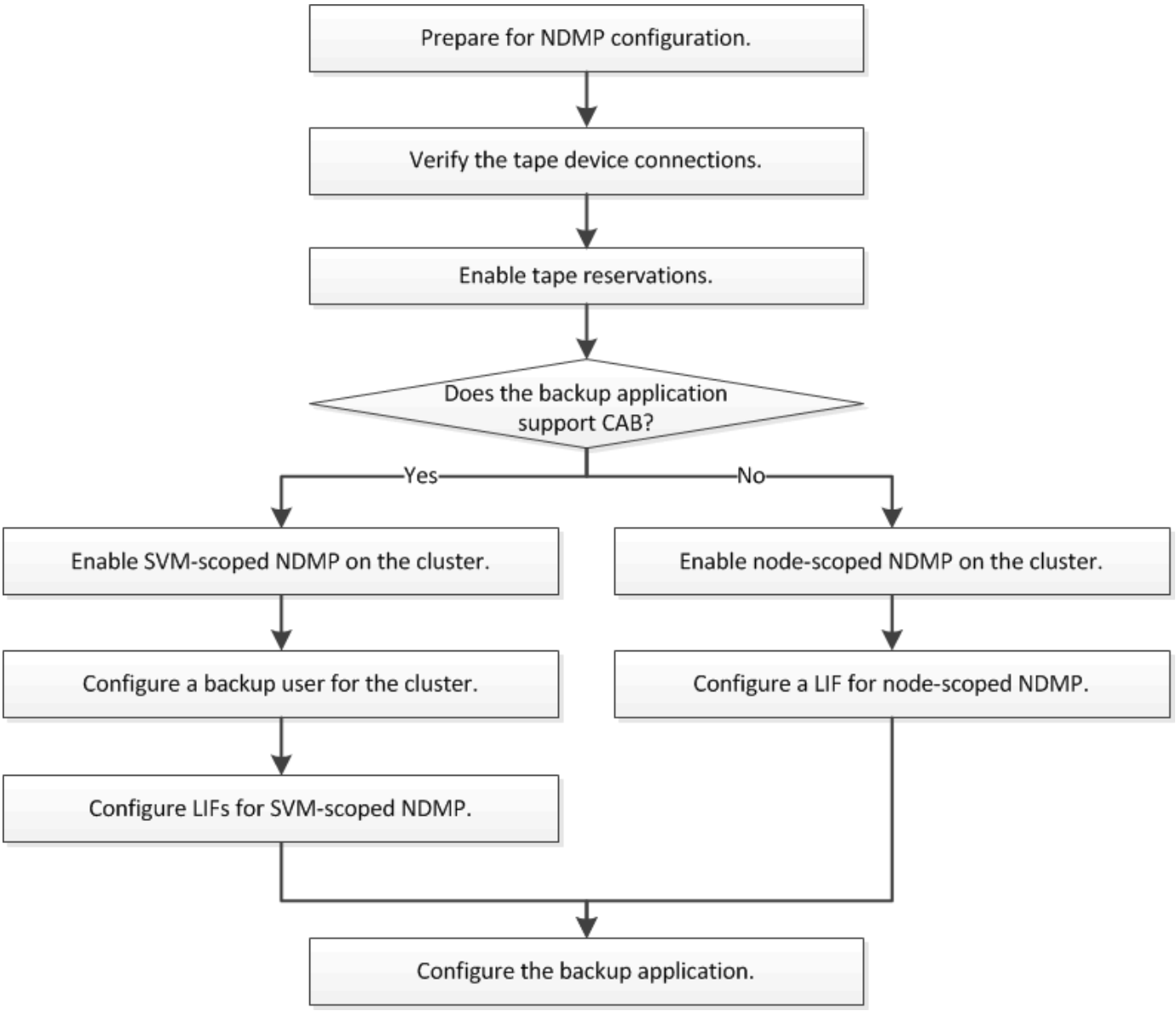
En savoir plus sur "Sauvegarde « cluster Aware Backup » (CAB)".

Avant de configurer NDMP, vérifiez les points suivants :

- Vous disposez d'une application de sauvegarde tierce (également appelée Data Management application ou DMA).
- Vous êtes un administrateur de cluster.
- Les périphériques de bande et un serveur multimédia en option sont installés.
- Les périphériques de bande sont connectés au cluster via un commutateur Fibre Channel (FC) et ne sont pas directement connectés.
- Au moins une unité de bande a un numéro d'unité logique (LUN) de 0.

Workflow de configuration NDMP

La configuration de la sauvegarde sur bande sur NDMP implique la préparation de la configuration NDMP, la vérification des connexions du périphérique de bande, l'activation des réservations sur bande, la configuration de NDMP au niveau SVM ou node, l'activation de NDMP sur le cluster, la configuration d'un utilisateur de sauvegarde, la configuration des LIFs et la configuration de l'application de sauvegarde.



Préparation à la configuration NDMP

Avant de configurer l'accès de sauvegarde sur bande via le protocole NDMP (Network Data Management Protocol), vous devez vérifier que la configuration planifiée est prise en charge. Vérifier que vos lecteurs de bande sont répertoriés comme disques qualifiés sur chaque nœud, vérifier que tous les nœuds disposent des LIF intercluster, Et déterminer si l'application de sauvegarde prend en charge l'extension CLUSTER Aware Backup (CAB).

Étapes

1. Consultez le tableau de compatibilité de votre fournisseur d'applications de sauvegarde pour la prise en charge du protocole ONTAP (NetApp ne qualifier pas les applications de sauvegarde tierces avec ONTAP ou NDMP).

   Vérifiez que les composants NetApp suivants sont compatibles :

   - Version de ONTAP 9 qui s'exécute sur le cluster.

- Le fournisseur et la version de l'application de sauvegarde, par exemple Veritas NetBackup 8.2 ou CommVault.
- Les lecteurs de bande décrivent en détail le fabricant, le modèle et l'interface des lecteurs de bande, par exemple IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- Plateformes des nœuds du cluster : par exemple, FAS8700 ou A400

> Vous trouverez des matrices de support de compatibilité ONTAP existantes pour les applications de sauvegarde dans le "Matrice d'interopérabilité NetApp".

2. Vérifiez que vos lecteurs de bande sont répertoriés comme lecteurs qualifiés dans le fichier de configuration de bande intégré de chaque nœud :

   a. Sur l'interface de ligne de commande, affichez le fichier de configuration de bande intégré à l'aide du `storage tape show-supported-status` commande.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                Is
Tape Drives                     Supported  Support Status
-------------------------------  ---------
-------------------------------
Certance Ultrium 2              true       Dynamically Qualified
Certance Ultrium 3              true       Dynamically Qualified
Digital DLT2000                 true       Qualified
```

   b. Comparez vos lecteurs de bande à la liste des lecteurs qualifiés dans la sortie.

> Les noms des périphériques de bande dans la sortie peuvent varier légèrement par rapport aux noms figurant sur l'étiquette du périphérique ou dans la matrice d'interopérabilité. Par exemple, le DLT2000 numérique peut également être appelé DL2k. Vous pouvez ignorer ces différences mineures de dénomination.

   c. Si un périphérique ne figure pas dans la liste comme indiqué dans le résultat, même si celui-ci est qualifié conformément à la matrice d'interopérabilité, téléchargez et installez un fichier de configuration mis à jour pour le périphérique, en suivant les instructions du site du support NetApp.

      "Téléchargements NetApp : fichiers de configuration des lecteurs de bande"

   Il se peut qu'un périphérique qualifié ne figure pas dans le fichier de configuration de bande intégré si le périphérique de bande a été qualifié après l'expédition du nœud.

3. Vérifier que chaque nœud du cluster dispose d'un LIF intercluster :

   a. Afficher les LIFs intercluster sur les nœuds en utilisant le `network interface show -role intercluster` commande.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

b. Si aucune LIF intercluster n'existe sur un nœud, créer une LIF intercluster en utilisant le `network interface create` commande.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

"Gestion du réseau"

4. Déterminez si l'application de sauvegarde prend en charge Cluster Aware Backup (CAB) à l'aide de la documentation fournie avec l'application de sauvegarde.

   Le support CAB est un facteur clé pour déterminer le type de sauvegarde que vous pouvez effectuer.

Vérifiez les connexions du lecteur de bande

Vous devez vous assurer que tous les lecteurs et changeurs de supports sont visibles dans ONTAP en tant que périphériques.

Étapes

1. Affichez des informations sur tous les lecteurs et changeurs de supports à l'aide du `storage tape show` commande.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                Device Type     Description
Status
----------------------  --------------  ------------------------------
--------
sw4:10.11                tape drive      HP LTO-3
normal
0b.125L1                 media changer   HP MSL G3 Series
normal
0d.4                     tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                   media changer   IBM 3573-TL
normal
...
```

2. Si aucun lecteur de bande n'est affiché, résolvez le problème.
3. Si un changeur de supports n'est pas affiché, affichez les informations relatives aux changeurs de supports à l'aide du `storage tape show-media-changer` commande, puis résolution du problème.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Activer les réservations sur bande

Vous devez vous assurer que les lecteurs de bande sont réservés à l'utilisation par les applications de sauvegarde pour les opérations de sauvegarde NDMP.

Description de la tâche

Les paramètres de réservation varient selon les applications de sauvegarde et ces paramètres doivent correspondre à l'application de sauvegarde et aux nœuds ou serveurs utilisant les mêmes lecteurs. Consultez la documentation fournisseur de l'application de sauvegarde pour connaître les paramètres de réservation corrects.

Étapes

1. Activer les réservations à l'aide de `options -option-name tape.reservations -option-value persistent` commande.

   La commande suivante active les réservations avec le `persistent` valeur :

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Vérifiez que les réservations sont activées sur tous les nœuds à l'aide de l' `options tape.reservations` commande, puis vérifiez la sortie.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                 persistent

   cluster1-2
       tape.reservations                 persistent
   2 entries were displayed.
   ```

Configurer SVM-scoped NDMP

Activer SVM-scoped NDMP sur le cluster

Si le DMA prend en charge l'extension Cluster Aware Backup (CAB), vous pouvez sauvegarder tous les volumes hébergés sur différents nœuds d'un cluster en activant SVM-scoped NDMP, en activant le service NDMP sur le cluster (admin SVM) et en configurant les LIF de données et de contrôle.

Ce dont vous avez besoin

L'extension CAB doit être prise en charge par le DMA.

Description de la tâche

La désactivation du mode node-scoped NDMP permet d'activer le mode SVM-scoped NDMP sur le cluster.

Étapes

1. Activer le mode NDMP SVM-scoped :

```
cluster1::> system services ndmp node-scope-mode off
```

   Le mode NDMP SVM-scoped est activé.

2. Activer le service NDMP sur le SVM d'admin:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

   Le type d'authentification est défini sur `challenge` par défaut, l'authentification en texte brut est désactivée.

   > Pour des communications sécurisées, vous devez maintenir l'authentification en texte brut désactivée.

3. Vérifier que le service NDMP est activé :

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Activez un utilisateur de sauvegarde pour l'authentification NDMP

Pour authentifier SVM-scoped NDMP depuis l'application de backup, un utilisateur administratif doit disposer des privilèges suffisants et d'un mot de passe NDMP.

Description de la tâche

Vous devez générer un mot de passe NDMP pour les utilisateurs admin de sauvegarde. Vous pouvez activer les utilisateurs admin de sauvegarde au niveau du cluster ou de la SVM et, si nécessaire, vous pouvez créer un nouvel utilisateur. Par défaut, les utilisateurs disposant des rôles suivants peuvent s'authentifier pour la sauvegarde NDMP :

- Au niveau du cluster : `admin` ou `backup`
- SVM individuels : `vsadmin` ou `vsadmin-backup`

Si vous utilisez un utilisateur NIS ou LDAP, l'utilisateur doit exister sur le serveur respectif. Vous ne pouvez pas utiliser un utilisateur Active Directory.

Étapes

1. Afficher les utilisateurs et autorisations admin actuels :

   ```
   security login show
   ```

2. Si nécessaire, créez un nouvel utilisateur de sauvegarde NDMP avec le `security login create` Commande et le rôle approprié pour les privilèges des SVM au niveau du cluster ou individuels.

   Vous pouvez spécifier un nom d'utilisateur de sauvegarde locale ou un nom d'utilisateur NIS ou LDAP pour l' `-user-or-group-name` paramètre.

   La commande suivante crée l'utilisateur de sauvegarde `backup_admin1` avec le `backup` rôle pour l'ensemble du cluster :

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   La commande suivante crée l'utilisateur de sauvegarde `vsbackup_admin1` avec le `vsadmin-backup` Rôle d'un SVM individuel :

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Entrez un mot de passe pour le nouvel utilisateur et confirmez.

3. Générer un mot de passe pour la SVM d'admin via le `vserver services ndmp generate password` commande.

   Le mot de passe généré doit être utilisé pour authentifier la connexion NDMP par l'application de sauvegarde.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   Password: qG5CqQHYxw7tE57g
   ```

Configurez les LIF

Vous devez identifier les LIF qui seront utilisées pour établir une connexion de données entre les données et les ressources sur bande, et pour contrôler la connexion entre la SVM d'administration et l'application de sauvegarde. Une fois les LIF définies, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour les LIF et spécifier le rôle d'interface privilégié.

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Étapes

1. Identifier les LIF intercluster, cluster-management et node-management en utilisant le `network interface show` commande avec `-role` paramètre.

   La commande suivante affiche les LIFs intercluster :

```
cluster1::> network interface show -role intercluster

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    IC1               up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2               up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   La commande suivante affiche la LIF cluster-management :

```
cluster1::> network interface show -role cluster-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    cluster_mgmt      up/up      192.0.2.60/24      cluster1-2
e0M     true
```

   La commande suivante affiche les LIFs de node-management :

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------ ------------
------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24      cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24      cluster1-2
e0M     true
```

2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIF intercluster, cluster-management (cluster-mgmt) et node-management (node-mgmt) :

   a. Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de `system services firewall policy show` commande.

      La commande suivante affiche la politique de pare-feu pour la LIF cluster-management :

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                        ** ndmp       0.0.0.0/0**
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour la LIF node-management :

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

   La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :

   a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur `broadcast-`

`domain-wide`, Et la policy pour les LIFs intercluster et node-management est définie sur `local-only` à l'aide du `network interface show -failover` commande.

La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ----------------- --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                     Failover Targets:
                                                     .......

**cluster1   cluster_mgmt       cluster1-1:e0m    broadcast-domain-wide
Default**
                                                     Failover Targets:
                                                     .......
           **IC1                 cluster1-1:e0a    local-only
Default**
                                                     Failover Targets:
           **IC2                 cluster1-1:e0b    local-only
Default**
                                                     Failover Targets:
                                                     .......
**cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
**cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
```

a. Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant le `network interface modify` commande avec `-failover-policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Spécifier les LIFs requises pour la connexion de données à l'aide de `vserver services ndmp modify` commande avec `preferred-interface-role` paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de `vserver services ndmp show` commande.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

Configurer node-scoped NDMP

Activez NDMP node-scoped sur le cluster

Vous pouvez sauvegarder des volumes hébergés sur un seul nœud en activant NDMP node-scoped, en activant le service NDMP et en configurant une LIF pour la connexion data et contrôle. Cela peut être effectué pour tous les nœuds du cluster.

> Le protocole NDMP avec étendue du nœud est obsolète dans ONTAP 9.

Description de la tâche

Si vous utilisez NDMP en mode node-scope, l'authentification doit être configurée sur la base de chaque nœud. Pour plus d'informations, voir "L'article de la base de connaissances "Comment configurer l'authentification NDMP en mode 'node-scope'"".

Étapes

1. Activer le mode NDMP node-scoped :

```
cluster1::> system services ndmp node-scope-mode on
```

   NDMP node-scope-mode est activé.

2. Activer le service NDMP sur tous les nœuds du cluster :

   L'utilisation du caractère générique "*" permet le service NDMP sur tous les nœuds en même temps.

   Vous devez spécifier un mot de passe pour l'authentification de la connexion NDMP par l'application de

backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Désactivez le `-clear-text` Option pour la communication sécurisée du mot de passe NDMP :

   Utilisation du caractère générique “*” disables the `-clear-text` option sur tous les nœuds simultanément.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Vérifiez que le service NDMP est activé et que `-clear-text` l’option est désactivée :

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configurer une LIF

Vous devez identifier une LIF qui sera utilisée pour établir une connexion de données et une connexion de contrôle entre le nœud et l’application de sauvegarde. Après avoir identifié le LIF, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour le LIF.

> Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d’informations, voir "Configuration des politiques de pare-feu pour les LIF".

Étapes

1. Identifier le LIF intercluster hébergé sur les nœuds en utilisant le `network interface show` commande avec `-role` paramètre.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a
true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b
true
```

2. S'assurer que la politique de pare-feu est activée pour NDMP sur les LIFs intercluster :

   a. Vérifiez que la politique de pare-feu est activée pour NDMP à l'aide de `system services firewall policy show` commande.

      La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

      La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la politique de basculement est correctement définie pour les LIFs intercluster :

a. Vérifier que la policy de basculement pour les LIFs intercluster est définie sur `local-only` à l'aide du `network interface show -failover` commande.

```
cluster1::> network interface show -failover
            Logical          Home               Failover     Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  ----------------- ------------ --------
cluster1    **IC1               cluster1-1:e0a    local-only
Default**
                                                    Failover Targets:
                                                    .......
            **IC2               cluster1-2:e0b    local-only
Default**
                                                    Failover Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only    Default
                                                    Failover Targets:
                                                    .......
```

b. Si la stratégie de basculement n'est pas définie de manière appropriée, modifiez la stratégie de basculement en utilisant le `network interface modify` commande avec `-failover-policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configurez l'application de sauvegarde

Une fois le cluster configuré pour l'accès NDMP, vous devez collecter les informations de la configuration du cluster, puis configurer le reste du processus de sauvegarde dans l'application de sauvegarde.

Étapes

1. Collectez les informations suivantes que vous avez configurées précédemment dans ONTAP :
   - Nom d'utilisateur et mot de passe requis par l'application de sauvegarde pour créer la connexion NDMP
   - Les adresses IP des LIFs intercluster que l'application de sauvegarde nécessite pour se connecter au cluster
2. Dans ONTAP, affichez les alias attribués par ONTAP à chaque périphérique en utilisant le `storage tape alias show` commande.

   Les alias sont souvent utiles pour configurer l'application de sauvegarde.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                        Alias     Mapping
--------------------------- --------- ------------------------------
stsw-3220-4a-4b-02          st2       SN[HU19497WVR]
...
```

3. Dans l'application de sauvegarde, configurez le reste du processus de sauvegarde à l'aide de la documentation de l'application de sauvegarde.

Une fois que vous avez terminé

En cas de mobilité des données, comme un déplacement de volume ou une migration LIF, vous devez être prêt à réinitialiser les opérations de sauvegarde interrompues.

Réplication entre le logiciel NetApp Element et ONTAP

Réplication entre le logiciel NetApp Element et ONTAP en vue d'ensemble

Pour assurer la continuité de l'activité sur les systèmes Element, utilisez SnapMirror pour répliquer les copies Snapshot d'un volume Element vers une destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver ce système une fois que le service est restauré.

Depuis ONTAP 9.4, vous pouvez répliquer les copies Snapshot d'une LUN créée sur un nœud ONTAP et les renvoyer dans un système Element. Vous pouvez avoir créé une LUN en cas de panne sur le site Element ou utiliser un LUN pour migrer les données d'un système ONTAP vers le logiciel Element.

Vous devez travailler avec Element pour la sauvegarde ONTAP si les conditions suivantes s'appliquent :

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.
- Vous souhaitez utiliser l'interface de ligne de commandes ONTAP et non System Manager, ni un outil de création de scripts automatisé.
- Vous utilisez le protocole iSCSI pour transmettre des données aux clients.

Si vous avez besoin d'informations supplémentaires sur la configuration ou les concepts, consultez les documents suivants :

- Configuration d'élément

  "Documentation du logiciel NetApp Element"

- Concepts et configuration de SnapMirror

  "Présentation de la protection des données"

À propos de la réplication entre Element et ONTAP

Depuis ONTAP 9.3, vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un volume Element vers une destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver le volume source Element une fois que le service est restauré.

Depuis ONTAP 9.4, vous pouvez répliquer les copies Snapshot d'une LUN créée sur un nœud ONTAP et les renvoyer dans un système Element. Vous pouvez avoir créé une LUN en cas de panne sur le site Element ou utiliser un LUN pour migrer les données d'un système ONTAP vers le logiciel Element.

Types de relation de protection des données

SnapMirror propose deux types de relation de protection des données. Pour chaque type, SnapMirror crée une copie Snapshot du volume source Element avant d'initialiser ou de mettre à jour la relation :

- Dans une relation *Disaster Recovery* protection de données, le volume de destination ne contient que la copie Snapshot créée par SnapMirror, à partir de laquelle vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.
- Dans une relation *conservation* protection des données à long terme, le volume de destination contient des copies Snapshot ponctuelles créées par le logiciel Element, ainsi que la copie Snapshot créée par SnapMirror. Par exemple, vous pouvez conserver les copies Snapshot mensuelles créées sur 20 ans.

Règles par défaut

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

Vous pouvez utiliser une règle par défaut ou personnalisée lors de la création d'une relation de protection des données. Le *type de stratégie* détermine les copies Snapshot à inclure et le nombre de copies à conserver.

Le tableau ci-dessous présente les policies par défaut. Utilisez le `MirrorLatest` Règle permettant de créer une relation classique de reprise sur incident. Utilisez le `MirrorAndVault` ou `Unified7year` Règle permettant de créer une relation de réplication unifiée dans laquelle la reprise sur incident et la conservation à long terme sont configurées sur le même volume de destination.

Politique	Type de stratégie	Comportement de mise à jour
MirrorLatest	mise en miroir asynchrone	Transférez la copie Snapshot créée par SnapMirror.
MirrorAndVault	coffre-fort	Transférer la copie Snapshot créée par SnapMirror et toutes les copies Snapshot moins récentes effectuées depuis la dernière mise à jour, à condition qu'elles aient des étiquettes SnapMirror « diotidienne » ou « hebdomadaires ».
Unifié 7ans	coffre-fort	Transférer la copie Snapshot créée par SnapMirror et toutes les copies Snapshot moins récentes effectuées depuis la dernière mise à jour, à condition qu'elles aient des étiquettes SnapMirror « diotidienne », « hebdomadaire » ou « mensuelle ».

Pour obtenir des informations complètes sur les règles de SnapMirror, notamment des instructions sur la règle à utiliser, reportez-vous à "La protection des données".

Présentation des étiquettes SnapMirror

Chaque règle avec le type de règle « iroir-vault » doit disposer d'une règle qui spécifie les copies Snapshot à répliquer. La règle « diotidienne », par exemple, indique que seules les copies Snapshot affectées à l'étiquette SnapMirror « q uotidienne » doivent être répliquées. Vous attribuez l'étiquette SnapMirror lors de la configuration des copies Snapshot Element.

La réplication s'effectue depuis un cluster source Element vers un cluster cible ONTAP

Vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un volume Element sur un système de destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver le volume source Element une fois que le service est restauré.

Un volume Element équivaut à peu près à un LUN ONTAP. SnapMirror crée un LUN avec le nom du volume Element lorsqu'une relation de protection des données entre le logiciel Element et ONTAP est initialisée. SnapMirror réplique les données vers un LUN existant si le LUN répond aux besoins de réplication d'Element vers ONTAP.

Les règles de réplication sont les suivantes :

- Un volume ONTAP peut contenir uniquement des données d'un volume Element.
- Vous ne pouvez pas répliquer les données depuis un volume ONTAP vers plusieurs volumes Element.

Effectuer une réplication depuis un cluster source ONTAP vers un cluster cible Element

Depuis ONTAP 9.4, vous pouvez répliquer les copies Snapshot d'un LUN créé sur un système ONTAP et les renvoyer dans un volume Element :

- Si une relation SnapMirror existe déjà entre une source Element et une destination ONTAP, une LUN créée pendant l'accès aux données de la destination est automatiquement répliquée lorsque la source est réactivée.
- Sinon, vous devez créer et initialiser une relation SnapMirror entre le cluster source ONTAP et le cluster destination Element.

Les règles de réplication sont les suivantes :

- La relation de réplication doit avoir une règle de type « async-mirror ».

  Les règles de type "iroir-vault" ne sont pas prises en charge.

- Seules les LUN iSCSI sont prises en charge.
- Vous ne pouvez pas répliquer plusieurs LUN depuis un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN depuis un volume ONTAP vers plusieurs volumes Element.

Prérequis

Vous devez avoir effectué les tâches suivantes avant de configurer une relation de protection des données entre Element et ONTAP :

- Le cluster Element doit exécuter NetApp Element version 10.1 ou ultérieure.

- Le cluster ONTAP doit exécuter ONTAP 9.3 ou version ultérieure.
- SnapMirror doit avoir été sous licence sur le cluster ONTAP.
- Vous devez disposer de volumes configurés sur les clusters Element et ONTAP suffisamment grands pour gérer les transferts de données anticipés.
- Si vous utilisez le type de règle « miroir-coffre-fort », une étiquette SnapMirror doit avoir été configurée pour que les copies Snapshot Element soient répliquées.

> Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element. Pour plus d'informations, reportez-vous à la section "Documentation du logiciel NetApp Element"

- Vous devez vous assurer que le port 5010 est disponible.
- Si vous pensez avoir besoin de déplacer un volume de destination, vous devez vous assurer que la connectivité full-mesh existe entre la source et la destination. Chaque nœud du cluster source Element doit pouvoir communiquer avec chaque nœud du cluster cible ONTAP.

Détails du support

Le tableau suivant présente les informations de support pour la sauvegarde Element vers ONTAP.

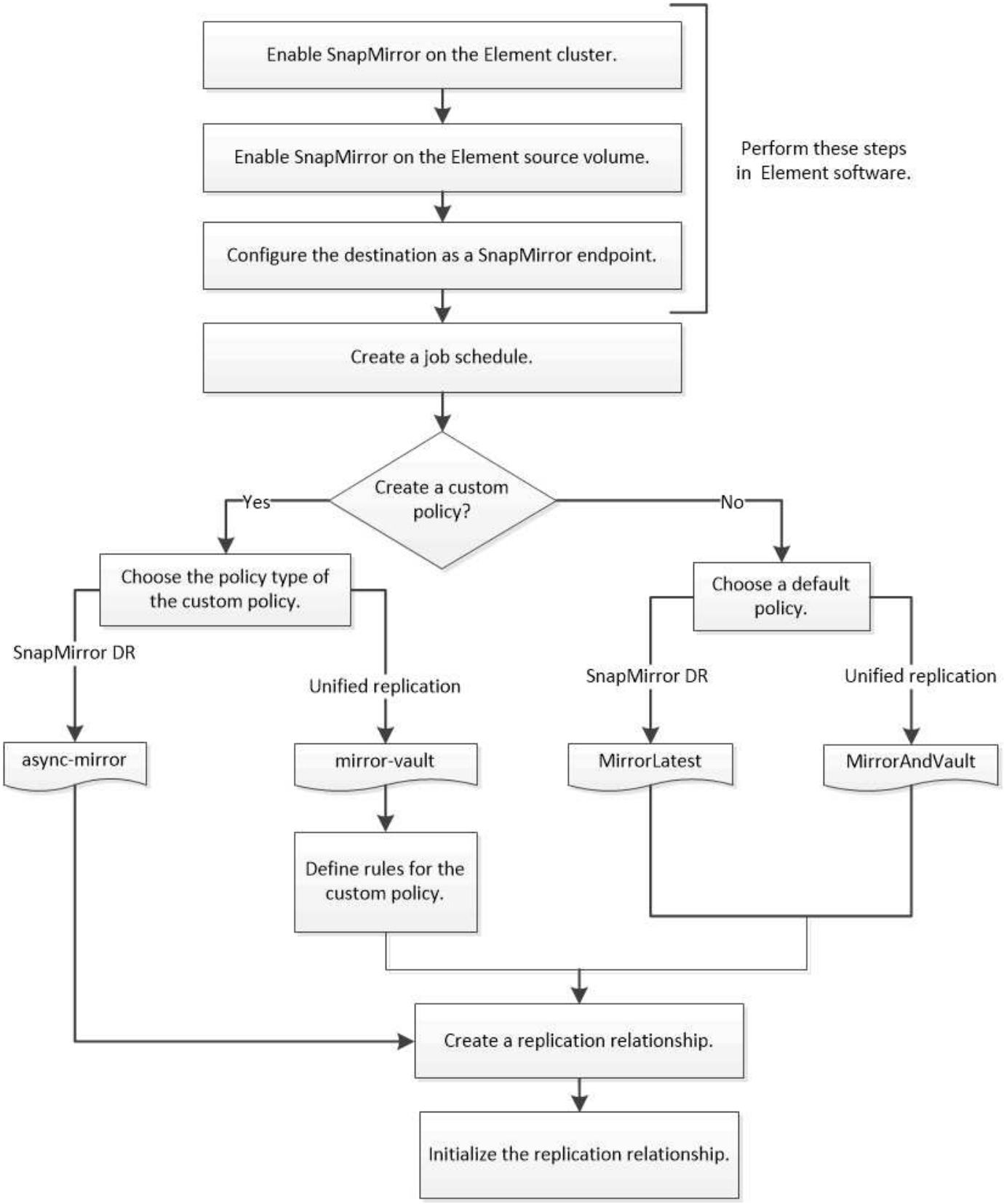
Ressource ou fonctionnalité	Détails du support
SnapMirror	• La fonctionnalité de restauration SnapMirror n'est pas prise en charge. • Le `MirrorAllSnapshots` et `XDPDefault` les règles ne sont pas prises en charge. • Le type de politique « coffre-fort » n'est pas pris en charge. • La règle définie par le système « tous_source_snapshots » n'est pas prise en charge. • Le type de règle « miroir-coffre-fort » n'est pris en charge que pour la réplication à partir du logiciel Element vers ONTAP. Utilisez le mot « asynchrone-miroir » pour la réplication du logiciel ONTAP vers le logiciel Element. • Le `-schedule` et `-prefix` options pour `snapmirror policy add-rule` ne sont pas pris en charge. • Le `-preserve` et `-quick-resync` options pour `snapmirror resync` ne sont pas pris en charge. • L'efficacité du stockage n'est pas préservée. • Les déploiements de protection des données « Fan-Out » et « cascade » ne sont pas pris en charge.
ONTAP	• ONTAP Select est pris en charge à partir de ONTAP 9.4 et Element 10.3. • Cloud Volumes ONTAP est pris en charge à partir de ONTAP 9.5 et Element 11.0.

Elément	• La taille maximale du volume est de 8 Tio. • La taille de bloc du volume doit être de 512 octets. Une taille de bloc de 4 Ko n'est pas prise en charge. • La taille du volume doit être un multiple de 1 MIB. • Les attributs de volume ne sont pas conservés. • Le nombre maximal de copies Snapshot à répliquer est de 30.
Le réseau	• Une connexion TCP unique est autorisée par transfert. • Le nœud élément doit être spécifié en tant qu'adresse IP. La recherche de nom d'hôte DNS n'est pas prise en charge. • Les IPspaces ne sont pas prises en charge.
SnapLock	Les volumes SnapLock ne sont pas pris en charge.
FlexGroup	Les volumes FlexGroup ne sont pas pris en charge.
REPRISE APRÈS INCIDENT DES SVM	Les volumes ONTAP d'une configuration SVM de reprise après incident ne sont pas pris en charge.
MetroCluster	Les volumes ONTAP avec une configuration MetroCluster ne sont pas pris en charge.

Workflow de réplication entre Element et ONTAP

Que vous répliquant des données d'Element vers ONTAP ou de ONTAP vers Element, vous devez configurer une planification de tâche, spécifier une règle et créer et initialiser la relation. Vous pouvez utiliser une stratégie par défaut ou personnalisée.

Le flux de travail suppose que vous avez terminé les tâches préalables répertoriées dans Prérequis. Pour obtenir des informations complètes sur les règles de SnapMirror, notamment des instructions sur la règle à utiliser, reportez-vous à "Protection des données".



Activez SnapMirror dans Element

Activez SnapMirror sur le cluster Element

Vous devez activer SnapMirror sur le cluster Element avant de créer une relation de

réplication. Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element.

Avant de commencer

- Le cluster Element doit exécuter NetApp Element version 10.1 ou ultérieure.
- SnapMirror ne peut être activé que pour les clusters Element utilisés avec les volumes NetApp ONTAP.

Description de la tâche

Le système Element est fourni avec SnapMirror désactivé par défaut. SnapMirror n'est pas automatiquement activé dans le cadre d'une nouvelle installation ou mise à niveau.

> Une fois activé, SnapMirror ne peut pas être désactivé. Vous pouvez uniquement désactiver la fonctionnalité SnapMirror et restaurer les paramètres par défaut en retournant le cluster à l'image d'usine.

Étapes

1. Cliquez sur **clusters** > **Paramètres**.
2. Recherchez les paramètres cluster pour SnapMirror.
3. Cliquez sur **Activer SnapMirror**.

Activez SnapMirror sur le volume source Element

Vous devez activer SnapMirror sur le volume source Element avant de créer une relation de réplication. Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element.

Avant de commencer

- Vous devez avoir activé SnapMirror sur le cluster Element.
- La taille de bloc du volume doit être de 512 octets.
- Le volume ne doit pas participer à la réplication à distance d'Element.
- Le type d'accès au volume ne doit pas être « cible de réplication ».

Description de la tâche

La procédure ci-dessous suppose que le volume existe déjà. Vous pouvez également activer SnapMirror lorsque vous créez ou clonez un volume.

Étapes

1. Sélectionnez **Management** > **volumes**.
2. Sélectionner ⚙ bouton du volume.
3. Dans le menu déroulant, sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier le volume**, sélectionnez **Activer SnapMirror**.
5. Sélectionnez **Enregistrer les modifications**.

Créer un terminal SnapMirror

Vous devez créer un terminal SnapMirror avant de pouvoir créer une relation de réplication. Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web

du logiciel Element.

Avant de commencer

Vous devez avoir activé SnapMirror sur le cluster Element.

Étapes

1. Cliquez sur **Data protection** > **SnapMirror Endpoints**.
2. Cliquez sur **Créer un point final**.
3. Dans la boîte de dialogue **Créer un nouveau point final**, entrez l'adresse IP de gestion du cluster ONTAP.
4. Entrez l'ID utilisateur et le mot de passe de l'administrateur du cluster ONTAP.
5. Cliquez sur **Créer un point final**.

Configurer une relation de réplication

Créer une planification de tâche de réplication

Que vous répliquant des données d'Element vers ONTAP ou de ONTAP vers Element, vous devez configurer une planification de tâche, spécifier une règle et créer et initialiser la relation. Vous pouvez utiliser une stratégie par défaut ou personnalisée.

Vous pouvez utiliser le `job schedule cron create` commande pour créer une planification de tâche de réplication. La planification des tâches détermine lorsque SnapMirror met automatiquement à jour la relation de protection des données à laquelle la planification est attribuée.

Description de la tâche

Vous affectez un planning de travail lorsque vous créez une relation de protection des données. Si vous n'attribuez pas de programme de travail, vous devez mettre à jour la relation manuellement.

Étape

1. Création d'un programme de travail :

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Pour `-month`, `-dayofweek`, et `-hour`, vous pouvez spécifier `all` pour exécuter le travail chaque mois, jour de la semaine et heure, respectivement.

   Depuis ONTAP 9.10.1, vous pouvez inclure le vServer dans votre calendrier des tâches :

   `job schedule cron create -name` *`job_name`* `-vserver` *`Vserver_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   L'exemple suivant crée un programme de travail nommé `my_weekly` Le samedi à 3:00 :

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

Personnaliser une règle de réplication

Création d'une règle de réplication personnalisée

Vous pouvez utiliser une règle par défaut ou personnalisée lorsque vous créez une relation de réplication. Pour une règle de réplication unifiée personnalisée, vous devez définir une ou plusieurs *règles* qui déterminent quelles copies Snapshot sont transférées lors de l'initialisation et de la mise à jour.

Vous pouvez créer une stratégie de réplication personnalisée si la stratégie par défaut d'une relation n'est pas appropriée. Vous pouvez compresser les données d'un transfert réseau, par exemple, ou modifier le nombre de tentatives de transfert de copies Snapshot par SnapMirror.

Description de la tâche

Le *policy type* de la règle de réplication détermine le type de relation qu'elle prend en charge. Le tableau ci-dessous présente les types de stratégies disponibles.

Type de règle	Type de relation
mise en miroir asynchrone	Reprise sur incident SnapMirror
coffre-fort	Réplication unifiée

Étape

1. Création d'une règle de réplication personnalisée :

   `snapmirror policy create -vserver` *`SVM`* `-policy policy -type async-mirror|mirror-vault -comment` *`comment`* `-tries` *`transfer_tries`* `-transfer-priority low|normal -is-network-compression-enabled true|false`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   Depuis la version ONTAP 9.5, vous pouvez définir le planning de création d'un planning de copie Snapshot commun pour les relations SnapMirror synchrone à l'aide de la `-common-snapshot-schedule` paramètre. Par défaut, la planification commune de copies Snapshot pour les relations SnapMirror synchrone est d'une heure. Définissez une valeur de 30 minutes à deux heures pour la planification de copie Snapshot pour les relations SnapMirror synchrone.

   L'exemple suivant crée une règle de réplication personnalisée pour SnapMirror DR qui permet la compression réseau pour les transferts de données :

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_compressed -type async-mirror -comment "DR with network compression
   enabled" -is-network-compression-enabled true
   ```

   L'exemple suivant crée une règle de réplication personnalisée pour la réplication unifiée :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Une fois que vous avez terminé

Pour les types de règles « miroir-coffre-fort », vous devez définir des règles qui déterminent les copies Snapshot qui sont transférées lors de l'initialisation et de la mise à jour.

Utilisez le `snapmirror policy show` Commande pour vérifier que la règle SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Définir une règle pour une règle

Pour les règles personnalisées avec le type de règle « miroir-coffre-fort », vous devez définir au moins une règle qui détermine les copies Snapshot transférées lors de l'initialisation et de la mise à jour. Vous pouvez également définir des règles pour les stratégies par défaut avec le type de stratégie "miroir-coffre-fort".

Description de la tâche

Chaque règle avec le type de règle « iroir-vault » doit disposer d'une règle qui spécifie les copies Snapshot à répliquer. La règle « bimensuelle », par exemple, indique que seules les copies Snapshot affectées au label SnapMirror « bimensuel » doivent être répliquées. Vous attribuez l'étiquette SnapMirror lors de la configuration des copies Snapshot Element.

Chaque type de stratégie est associé à une ou plusieurs règles définies par le système. Ces règles sont automatiquement attribuées à une règle lorsque vous spécifiez son type de stratégie. Le tableau ci-dessous présente les règles définies par le système.

Règle définie par le système	Utilisé dans les types de stratégie	Résultat
sm_créé	asynchrone-mirror, mirror-vault	Une copie Snapshot créée par SnapMirror est transférée lors de l'initialisation et de la mise à jour.
tous les jours	coffre-fort	Les nouvelles copies Snapshot de la source portant le label SnapMirror « `diotidienne » sont transférées lors de l'initialisation et de la mise à jour.
hebdomadaire	coffre-fort	Les nouvelles copies Snapshot de la source portant l'étiquette SnapMirror « hebdomadaire » sont transférées lors de l'initialisation et de la mise à jour.

tous les mois	coffre-fort	Les nouvelles copies Snapshot de la source avec le libellé SnapMirror « `mensuel' » sont transférées lors de l'initialisation et de la mise à jour.

Vous pouvez indiquer des règles supplémentaires selon vos besoins pour les règles par défaut ou personnalisées. Par exemple :

- Pour la valeur par défaut `MirrorAndVault` Politique, vous pouvez créer une règle appelée « deux mois » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux mois ».
- Dans le cas d'une règle personnalisée avec le type de règle « miroir-coffre-fort », vous pouvez créer une règle appelée « deux semaines » pour faire correspondre les copies Snapshot de la source avec l'étiquette SnapMirror « deux semaines ».

Étape

1. Définir une règle pour une règle :

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-monthly` par défaut `MirrorAndVault` règle :

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-weekly` au personnalisé `my_snapvault` règle :

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `app_consistent` au personnalisé `Sync` règle :

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   Vous pouvez ensuite répliquer les copies Snapshot à partir du cluster source correspondant à l'étiquette SnapMirror :

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Créer une relation de réplication

Création d'une relation entre une source d'élément et une destination ONTAP

La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation de protection des données ». Vous pouvez utiliser le `snapmirror create` Commande permettant de créer une relation de protection des données à partir d'une source Element vers une destination ONTAP, ou d'une source ONTAP vers une destination Element.

Vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un volume Element sur un système de destination ONTAP. En cas d'incident au niveau du système Element, vous pouvez délivrer les données aux clients via le système ONTAP, puis réactiver le volume source Element une fois que le service est restauré.

Avant de commencer

- Le nœud Element contenant le volume à répliquer doit avoir été accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror.
- Si vous utilisez le type de règle « miroir-coffre-fort », une étiquette SnapMirror doit avoir été configurée pour que les copies Snapshot Element soient répliquées.

> Vous pouvez effectuer cette tâche uniquement dans l'interface utilisateur Web du logiciel Element. Pour plus d'informations, reportez-vous à la section "Documentation sur les éléments".

Description de la tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

Un volume Element équivaut à peu près à un LUN ONTAP. SnapMirror crée un LUN avec le nom du volume Element lorsqu'une relation de protection des données entre le logiciel Element et ONTAP est initialisée. SnapMirror réplique les données vers une LUN existante si la LUN répond aux exigences en matière de réplication depuis le logiciel Element vers ONTAP.

Les règles de réplication sont les suivantes :

- Un volume ONTAP peut contenir uniquement des données d'un volume Element.
- Vous ne pouvez pas répliquer les données depuis un volume ONTAP vers plusieurs volumes Element.

Dans ONTAP 9.3 et version antérieure, un volume de destination peut contenir jusqu'à 251 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies Snapshot

Étape

1. Depuis le cluster destination, créer une relation de réplication depuis une source Element vers une destination ONTAP :

`snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume -type XDP -schedule schedule -policy policy`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorLatest` règle :

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la valeur par défaut `MirrorAndVault` règle :

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de `Unified7year` règle :

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

L'exemple suivant illustre la création d'une relation de réplication unifiée à l'aide de la commande personnalisée `my_unified` règle :

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Création d'une relation entre une source ONTAP et une destination Element

Depuis ONTAP 9.4, vous pouvez utiliser SnapMirror pour répliquer les copies Snapshot d'un LUN créé sur une source ONTAP et les renvoyer vers une destination Element. Il est possible d'utiliser le LUN pour migrer les données d'ONTAP vers le logiciel Element.

Avant de commencer

- Le nœud de destination de l'élément doit avoir été accessible à ONTAP.

- Le volume Element doit avoir été activé pour la réplication SnapMirror.

Description de la tâche

Vous devez spécifier le chemin de destination de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

Les règles de réplication sont les suivantes :

- La relation de réplication doit avoir une règle de type « async-mirror ».

  Vous pouvez utiliser une stratégie par défaut ou personnalisée.

- Seules les LUN iSCSI sont prises en charge.
- Vous ne pouvez pas répliquer plusieurs LUN depuis un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN depuis un volume ONTAP vers plusieurs volumes Element.

Étape

1. Créer une relation de réplication depuis une source ONTAP vers une destination Element :

   `snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -type XDP -schedule schedule -policy policy`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la valeur par défaut `MirrorLatest` règle :

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   L'exemple suivant illustre la création d'une relation SnapMirror DR à l'aide de la commande personnalisée `my_mirror` règle :

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy my_mirror
   ```

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Initialiser une relation de réplication

Pour tous les types de relations, l'initialisation effectue un *transfert de base* : il effectue une copie Snapshot du volume source, puis transfère cette copie et tous les blocs de données qu'elle référence au volume de destination.

Avant de commencer

- Le nœud Element contenant le volume à répliquer doit avoir été accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror.
- Si vous utilisez le type de règle « miroir-coffre-fort », une étiquette SnapMirror doit avoir été configurée pour que les copies Snapshot Element soient répliquées.

Description de la tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

L'initialisation peut prendre beaucoup de temps. Vous pouvez exécuter le transfert de base en dehors des heures creuses.

> Si l'initialisation d'une relation entre une source ONTAP et une destination d'élément échoue pour une raison quelconque, elle continuera à échouer même après avoir corrigé le problème (un nom de LUN non valide, par exemple). La solution est la suivante :
>
> 1. Supprimer la relation.
> 2. Supprimez le volume de destination Element.
> 3. Créer un nouveau volume de destination Element.
> 4. Créez et initialisez une nouvelle relation entre la source ONTAP et le volume cible Element.

Étape

1. Initialiser une relation de réplication :

   `snapmirror initialize -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant initialise la relation entre le volume source `0005` À l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Activation des données à partir d'un volume de destination de reprise après incident SnapMirror

Rendre le volume de destination inscriptible

Lorsque l'incident désactive le site principal pour une relation SnapMirror DR, vous pouvez transmettre les données à partir du volume de destination sans interruption minimale. Vous pouvez réactiver le volume source une fois que le service est restauré au niveau du site principal.

Vous devez rendre le volume de destination inscriptible avant de pouvoir transmettre les données du volume à

des clients. Vous pouvez utiliser le `snapmirror quiesce` commande pour arrêter les transferts programmés vers la destination, le `snapmirror abort` pour arrêter les transferts en cours, et le `snapmirror break` commande permettant de rendre la destination inscriptible.

Description de la tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

Étapes

1. Arrêter les transferts programmés vers la destination :

   `snapmirror quiesce -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant arrête les transferts programmés entre le volume source `0005` À l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Arrêter les transferts en cours vers la destination :

   `snapmirror abort -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant arrête les transferts en cours entre le volume source `0005` À l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. Interrompre la relation SnapMirror DR :

   `snapmirror break -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant rompt la relation entre le volume source `0005` À l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` marche `svm_backup` et le volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Configurer le volume de destination pour l'accès aux données

Une fois le volume de destination inscriptible, vous devez configurer le volume pour l'accès aux données. LES hôtes SAN peuvent accéder aux données à partir du volume de destination jusqu'à ce que le volume source soit réactivé.

1. Mappez la LUN Element sur le groupe initiateur approprié.
2. Créer des sessions iSCSI entre les initiateurs d'hôte SAN et les LIFs SAN.
3. Sur le client SAN, effectuez une nouvelle analyse de stockage pour détecter la LUN connectée.

Réactiver le volume source d'origine

Vous pouvez rétablir la relation initiale de protection des données entre les volumes source et destination lorsque vous n'avez plus besoin de transmettre des données depuis la destination.

Description de la tâche

La procédure ci-dessous suppose que la ligne de base du volume source d'origine est intacte. Si la base n'est pas intacte, vous devez créer et initialiser la relation entre le volume dont vous accédez aux données et le volume source d'origine avant d'effectuer la procédure.

Vous devez spécifier le chemin source de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

Depuis ONTAP 9.4, les copies Snapshot d'une LUN créée pendant l'accès aux données depuis la destination ONTAP sont automatiquement répliquées à la réactivation de la source Element.

Les règles de réplication sont les suivantes :

- Seules les LUN iSCSI sont prises en charge.
- Vous ne pouvez pas répliquer plusieurs LUN depuis un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN depuis un volume ONTAP vers plusieurs volumes Element.

Étapes

1. Supprimez la relation de protection des données d'origine :

   ```
   snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination
   -path hostip:/lun/name -policy policy
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant supprime la relation entre le volume source d'origine, `0005` À l'adresse IP 10.0.0.11, et le volume que vous servant des données, `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```

2. Inverser la relation de protection des données d'origine :

`snapmirror resync -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -policy policy`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

L'exemple suivant inverse la relation entre le volume source d'origine, `0005` À l'adresse IP 10.0.0.11, et le volume que vous servant des données, `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Mettre à jour la relation inversée :

   `snapmirror update -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant met à jour la relation entre le volume que vous servant des données, `volA_dst` marche `svm_backup`, et le volume source d'origine, `0005` À l'adresse IP 10.0.0.11 :

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. Arrêter les transferts programmés pour la relation inversée :

   `snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant arrête les transferts programmés entre le volume à partir de où vous accédez les données, `volA_dst` marche `svm_backup`, et le volume source d'origine, `0005` À l'adresse IP 10.0.0.11 :

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Arrêter les transferts en cours pour la relation inversée :

   `snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant arrête les transferts en cours entre le volume dont vous accédez à des données, `volA_dst` marche `svm_backup`, et le volume source d'origine, `0005` À l'adresse IP 10.0.0.11 :

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Rompez la relation inversée :

   `snapmirror break -source-path` *`SVM:volume`*`|`*`cluster://SVM/volume`* `-destination -path` *`hostip`*`:/lun/`*`name`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant rompt la relation entre le volume dont vous servant des données, `volA_dst` marche `svm_backup`, et le volume source d'origine, `0005` À l'adresse IP 10.0.0.11 :

   ```
   cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005
   ```

7. Supprimez la relation de protection des données inversée :

   `snapmirror delete -source-path` *`SVM:volume`*`|`*`cluster://SVM/volume`* `-destination -path` *`hostip`*`:/lun/`*`name`* `-policy` *`policy`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant supprime la relation inversée entre le volume source d'origine, `0005` À l'adresse IP 10.0.0.11, et le volume que vous servant des données, `volA_dst` marche `svm_backup`:

   ```
   cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
   ```

8. Rétablir la relation initiale de protection des données :

   `snapmirror resync -source-path` *`hostip`*`:/lun/`*`name`* `-destination-path` *`SVM:volume`*`|`*`cluster://SVM/volume`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant rétablit la relation entre le volume source d'origine, `0005` À l'adresse IP 10.0.0.11, et au volume de destination d'origine, `volA_dst` marche `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Une fois que vous avez terminé

Utilisez le `snapmirror show` Commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Mettre à jour une relation de réplication manuellement

Vous devrez peut-être mettre à jour une relation de réplication manuellement si une mise à jour échoue en raison d'une erreur réseau.

Description de la tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

Étapes

1. Mettre à jour une relation de réplication manuellement :

   ```
   snapmirror update -source-path hostip:/lun/name -destination-path SVM:volume
   |cluster://SVM/volume
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Échec de la commande si une copie Snapshot commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant met à jour la relation entre le volume source `0005` À l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` marche `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Resynchroniser une relation de réplication

Vous devez resynchroniser une relation de réplication après avoir créé un volume de destination inscriptible, après une mise à jour échoue, car une copie Snapshot commune n'existe pas sur les volumes source et de destination, ou si vous souhaitez modifier la règle de réplication pour la relation.

Description de la tâche

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Vous pouvez exécuter la resynchronisation en dehors des heures de pointe.

Vous devez spécifier le chemin source de l'élément dans le formulaire `hostip:/lun/name`, où « lun » est la chaîne réelle « lun » et `name` Est le nom du volume Element.

Étape

1. Resynchronisation des volumes source et de destination :

   ```
   snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume
   ```

`|cluster://SVM/volume -type XDP -policy policy`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant resynchronque la relation entre le volume source `0005` À l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` marche `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```