



Protection des données avec System Manager

ONTAP 9

NetApp
April 24, 2024

Sommaire

Protection des données avec System Manager	1
Présentation de la protection des données avec System Manager	1
Création de règles personnalisées de protection des données	1
Configurez les copies Snapshot	2
Calculer l'espace récupérable avant de supprimer les copies Snapshot	2
Activez ou désactivez l'accès client au répertoire de copie Snapshot	2
Préparez-vous à la mise en miroir et à l'archivage	3
Configurer les miroirs et les coffres-forts	4
Resynchroniser une relation de protection	5
Restaurez un volume à partir d'une copie Snapshot antérieure	5
Effectuez des restaurations à partir de copies Snapshot	6
Restaurez vers un nouveau volume	6
Inverser la resynchronisation d'une relation de protection	7
Service des données à partir d'une destination SnapMirror	7
Configurer la reprise après incident des machines virtuelles de stockage	8
Service des données à partir d'une destination de reprise après incident des SVM	8
Réactiver une VM de stockage source	9
Resynchroniser une machine virtuelle de stockage de destination	9
Sauvegardez les données dans le cloud avec SnapMirror	10
Sauvegardez les données à l'aide de Cloud Backup	12

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 Politiques**, cliquez sur ➔.
3. Dans le volet **protection Politiques**, 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.

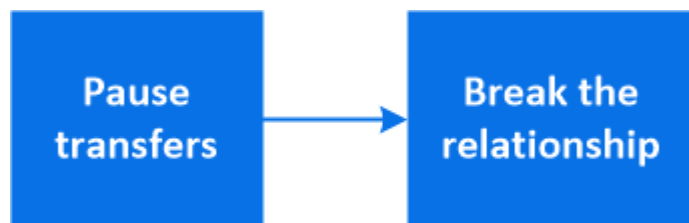
Lorsque vous effectuez une resynchronisation inverse, toutes les données du volume source qui sont plus récentes que les données de la copie Snapshot commune sont supprimées.

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	<ul style="list-style-type: none">• ID d'abonnement Azure• Région• Nom du groupe de ressources (existant ou nouveau)
AWS	<ul style="list-style-type: none">• ID de compte AWS• Touche d'accès• Clé secrète• Région
Projet Google Cloud (GCP)	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none"> • 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.

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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