Utiliser NetApp Backup and Recovery

NetApp Backup and Recovery

NetApp
February 11, 2026

Sommaire

Utiliser NetApp Backup and Recovery

Afficher l’état de la protection sur le tableau de bord de NetApp Backup and Recovery

La surveillance de l’état de vos charges de travail garantit que vous êtes conscient des problèmes de protection des charges de travail et que vous pouvez prendre des mesures pour les résoudre. Affichez l’état de vos sauvegardes et restaurations sur le tableau de bord de NetApp Backup and Recovery . Vous pouvez consulter le résumé du système, le résumé de la protection, le résumé du travail, le résumé de la restauration, etc.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération, administrateur de clone de sauvegarde et de récupération ou rôle de visualiseur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d’accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.

   Vous pouvez consulter les types d’informations suivants :

   - Nombre d’hôtes ou de machines virtuelles découverts
   - Nombre de clusters Kubernetes découverts
   - Nombre de cibles de sauvegarde sur le stockage d’objets
   - Nombre de vCenters
   - Nombre de clusters de stockage dans ONTAP

Voir le résumé de la protection

Consultez les informations suivantes dans le résumé de la protection :

- Le nombre total de bases de données, de machines virtuelles et de magasins de données protégés et non protégés.

  Une base de données protégée est une base de données à laquelle une politique de sauvegarde est attribuée. Une base de données non protégée est une base de données à laquelle aucune politique de sauvegarde n’est attribuée.

- Le nombre de sauvegardes qui ont réussi, qui ont reçu un avertissement ou qui ont échoué.
- La capacité totale découverte par le service de sauvegarde et la capacité protégée par rapport à la capacité non protégée. Passez la souris sur l’icône « **i** » pour voir les détails.

Voir le résumé du poste

Consultez le total des tâches terminées, en cours d'exécution ou ayant échoué dans le récapitulatif des tâches.

Étapes

1. Pour chaque distribution de tâches, modifiez un filtre pour afficher le résumé des tâches ayant échoué, en cours d'exécution et terminées en fonction du nombre de jours, par exemple, les 30 derniers jours, les 7 derniers jours, les dernières 24 heures ou la dernière année.
2. Affichez les détails des tâches ayant échoué, en cours d'exécution et terminées en sélectionnant **Afficher la surveillance des tâches**.

Afficher le résumé de la restauration

Consultez les informations suivantes sur le résumé de la restauration :

- Le nombre total de tâches de restauration effectuées
- La quantité totale de capacité qui a été restaurée
- Nombre de tâches de restauration effectuées sur le stockage local, secondaire et objet. Passez la souris sur le graphique pour voir les détails.

Créer et gérer des politiques pour régir les sauvegardes dans NetApp Backup and Recovery

Dans NetApp Backup and Recovery, créez vos propres stratégies qui régissent la fréquence de sauvegarde, l'heure à laquelle la sauvegarde est effectuée et le nombre de fichiers de sauvegarde conservés.

Certaines de ces options et sections de configuration ne sont pas disponibles pour toutes les charges de travail.

Si vous importez des ressources depuis SnapCenter, vous risquez de rencontrer des différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans NetApp Backup and Recovery. Voir"Différences de politique entre SnapCenter et NetApp Backup and Recovery" .

Vous pouvez atteindre les objectifs suivants liés aux politiques :

- Créer une politique de snapshot local
- Créer une politique de réplication vers le stockage secondaire
- Créer une politique pour les paramètres de stockage d'objets
- Configurer les paramètres de stratégie avancés
- Modifier les politiques (non disponible pour les charges de travail d'aperçu VMware)
- Supprimer les politiques

Voir les politiques

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Politiques**.

2. Consultez les détails de cette politique.
    - **Charge de travail** : des exemples incluent Microsoft SQL Server, Volumes, VMware, KVM, Hyper-V, Oracle Database ou Kubernetes.
    - **Type de sauvegarde** : les exemples incluent la sauvegarde complète et la sauvegarde du journal.
    - **Architecture** : les exemples incluent l'instantané local, la distribution en éventail, la mise en cascade, le disque à disque et le disque vers le magasin d'objets.
    - **Ressources protégées** : indique combien de ressources sur le total des ressources de cette charge de travail sont protégées.
    - **Protection contre les ransomwares** : indique si la politique inclut le verrouillage des instantanés sur l'instantané local, le verrouillage des instantanés sur le stockage secondaire ou le verrouillage DataLock sur le stockage d'objets.

Créer une politique

Vous pouvez créer des stratégies qui régissent vos snapshots locaux, vos réplications vers un stockage secondaire et vos sauvegardes vers un stockage d'objets. Une partie de votre stratégie 3-2-1 consiste à créer un instantané des instances, bases de données, applications ou machines virtuelles sur le système de stockage **principal**.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Avant de commencer

Si vous prévoyez de répliquer vers un stockage secondaire et que vous souhaitez utiliser le verrouillage des snapshots sur des snapshots locaux ou sur un stockage secondaire ONTAP distant, vous devez d'abord initialiser l'horloge de conformité ONTAP au niveau du cluster. Il s'agit d'une exigence pour activer le verrouillage des instantanés dans la politique.

Pour obtenir des instructions sur la façon de procéder, reportez-vous à "Initialiser l'horloge de conformité dans ONTAP" .

Pour plus d'informations sur le verrouillage des instantanés en général, reportez-vous à "Verrouillage des instantanés dans ONTAP" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Politiques**.
2. Depuis la page Politiques, sélectionnez **Créer une nouvelle politique**.
3. Dans la page Politiques, fournissez les informations suivantes.
    - Section **Détails** :
        - Type de charge de travail : sélectionnez la charge de travail qui utilisera la politique.
        - Entrez un nom de politique.

          Pour une liste de caractères à éviter, consultez l'info-bulle.

        - Sélectionnez un agent de console dans la liste **Agent**.
    - Section **Architecture de sauvegarde** : sélectionnez la flèche vers le bas et choisissez le flux de

données pour la sauvegarde, tel que 3-2-1 fan-out, 3-2-1 cascade ou disque à disque.

- **3-2-1 fanout** : du stockage principal (disque) au stockage secondaire (disque), puis au cloud (stockage objet). Crée plusieurs copies des données sur différents systèmes de stockage, tels que ONTAP vers ONTAP et ONTAP vers des configurations de stockage objet. Cela peut être un stockage objet d'un cloud hyperscaler ou un stockage objet privé. Ces configurations aident à atteindre une protection des données optimale et une reprise après sinistre.

  Cette option n'est pas disponible pour Amazon FSx for NetApp ONTAP.

  Pour les charges de travail VMware, cela configure l'instantané local sur les banques de données ou les machines virtuelles sur le disque principal et les réplique du stockage sur disque principal vers le stockage sur disque secondaire, ainsi que les répliques du stockage principal vers le stockage d'objets cloud.

- **Cascade 3-2-1** : (Non disponible pour les charges de travail Kubernetes) Stockage principal (disque) vers stockage secondaire (disque) et stockage principal (disque) vers stockage cloud (magasin d'objets). Il peut s'agir d'un magasin d'objets hyperscaler cloud ou d'un magasin d'objets privé - StorageGRID. Cela crée une chaîne de réplication de données sur plusieurs systèmes pour garantir la redondance et la fiabilité.

  Cette option n'est pas disponible pour Amazon FSx for NetApp ONTAP.

Pour les charges de travail VMware, cela configure l'instantané local sur les banques de données ou les machines virtuelles sur le stockage principal et une cascade du stockage sur disque principal vers le stockage sur disque secondaire, puis vers le stockage d'objets cloud.

- **Disque à disque** : (Non disponible pour les charges de travail Kubernetes) Stockage principal (disque) vers stockage secondaire (disque). La stratégie de protection des données ONTAP vers ONTAP réplique les données entre deux systèmes ONTAP pour garantir une haute disponibilité et une reprise après sinistre. Ceci est généralement réalisé à l'aide de SnapMirror, qui prend en charge la réplication synchrone et asynchrone. Cette méthode garantit que vos données sont continuellement mises à jour et disponibles sur plusieurs sites, offrant ainsi une protection robuste contre la perte de données.

  Pour les charges de travail VMware, cela configure l'instantané local sur les banques de données ou les VMware sur le système de stockage principal, puis réplique les données du système de stockage sur disque principal vers le système de stockage sur disque secondaire.

- **Disque vers magasin d'objets** : Stockage principal (disque) vers cloud (magasin d'objets). Cela réplique les données d'un système ONTAP vers un système de stockage d'objets, tel qu'AWS S3, Azure Blob Storage ou StorageGRID. Ceci est généralement réalisé à l'aide de SnapMirror Cloud, qui fournit des sauvegardes incrémentielles permanentes en transférant uniquement les blocs de données modifiés après le transfert de base initial. Il peut s'agir d'un magasin d'objets hyperscaler cloud ou d'un magasin d'objets privé - StorageGRID. Cette méthode est idéale pour la conservation et l'archivage des données à long terme, offrant une solution rentable et évolutive pour la protection des données.

  Pour les charges de travail VMWare, cela configure l'instantané local sur les banques de données ou les machines virtuelles sur le disque principal et la réplication du stockage sur disque principal vers le stockage d'objets cloud.

- **Fanout disque à disque** : (non disponible pour les charges de travail Kubernetes) Stockage principal (disque) vers stockage secondaire (disque) et stockage principal (disque) vers stockage

secondaire (disque).

> Vous pouvez configurer plusieurs paramètres secondaires pour l'option de répartition disque à disque.

Pour les charges de travail VMware, cela configure le stockage sur disque principal sur le stockage sur disque secondaire et réplique le stockage sur disque principal sur le stockage sur disque secondaire.

- **Instantanés locaux** : instantané local sur le volume sélectionné (Microsoft SQL Server). Les instantanés locaux sont un élément clé des stratégies de protection des données, capturant l'état de vos données à des moments précis. Cela crée des copies en lecture seule, à un instant T, des volumes de production sur lesquels vos charges de travail s'exécutent. L'instantané consomme un espace de stockage minimal et entraîne une surcharge de performances négligeable, car il enregistre uniquement les modifications apportées aux fichiers depuis le dernier instantané. Vous pouvez utiliser des instantanés locaux pour récupérer des données après une perte ou une corruption, ainsi que pour créer des sauvegardes à des fins de reprise après sinistre.

  Pour les charges de travail VMware, cela configure le snapshot local sur les banques de données ou les machines virtuelles sur le système de stockage principal.

Créer une politique de snapshot local

Fournir des informations pour l'instantané local.

- Sélectionnez l'option **Ajouter une planification** pour sélectionner la ou les planifications d'instantanés. Vous pouvez avoir un maximum de 5 horaires.
- **Fréquence des instantanés** : sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle. La fréquence annuelle n'est pas disponible pour les charges de travail Kubernetes.
- **Conservation des instantanés** : saisissez le nombre d'instantanés à conserver.
- **Activer la sauvegarde du journal** : (S'applique uniquement aux charges de travail Microsoft SQL Server et aux charges de travail Oracle Database.) Activez cette option pour sauvegarder les journaux et définir la fréquence et la conservation des sauvegardes des journaux. Pour ce faire, vous devez déjà avoir configuré une sauvegarde du journal. Voir"Configurer les répertoires de journaux" .
  - **Élaguer les journaux d'archive après la sauvegarde** : (charges de travail de base de données Oracle uniquement) Si les sauvegardes de journaux sont activées, vous pouvez éventuellement activer cette fonctionnalité pour limiter la durée pendant laquelle Backup and Recovery conserve les journaux d'archive Oracle. Vous pouvez choisir la période de conservation ainsi que l'endroit où Backup and Recovery doit supprimer les journaux d'archive.
- **Fournisseur** : (charges de travail Kubernetes uniquement) Sélectionnez le fournisseur de stockage qui héberge les ressources de l'application Kubernetes.

Créer une politique pour les paramètres secondaires (réplication vers le stockage secondaire)

Fournir des informations pour la réplication vers le stockage secondaire. Les informations de planification des paramètres d'instantané local s'affichent dans les paramètres secondaires. Ces paramètres ne sont pas disponibles pour les charges de travail Kubernetes.

- **Sauvegarde** : sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle.
- **Cible de sauvegarde** : sélectionnez le système cible sur le stockage secondaire pour la sauvegarde.
- **Rétention** : saisissez le nombre d'instantanés à conserver.

- **Activer le verrouillage des instantanés** : sélectionnez si vous souhaitez activer les instantanés inviolables.
- **Période de verrouillage de l'instantané** : saisissez le nombre de jours, de mois ou d'années pendant lesquels vous souhaitez verrouiller l'instantané.
- **Transfert vers le secondaire** :
  - L'option **Planification de transfert ONTAP - En ligne** est sélectionnée par défaut et indique que les snapshots sont immédiatement transférés vers le système de stockage secondaire. Vous n'avez pas besoin de planifier la sauvegarde.
  - Autres options : Si vous choisissez un virement différé, les virements ne sont pas immédiats et vous pouvez définir un calendrier.
- * Relation secondaire SnapMirror et SnapVault SMAS* : utilisez les relations secondaires SnapMirror et SnapVault SMAS pour les charges de travail SQL Server.

Créer une politique pour les paramètres de stockage d'objets

Fournir des informations pour la sauvegarde sur le stockage d'objets. Ces paramètres sont appelés « Paramètres de sauvegarde » pour les charges de travail Kubernetes.

Les champs qui s'affichent diffèrent selon le fournisseur et l'architecture sélectionnés.

Créer une politique pour le stockage d'objets AWS

Saisissez les informations dans ces champs :

- **Fournisseur** : sélectionnez **AWS**.
- **Compte AWS** : sélectionnez le compte AWS.
- **Cible de sauvegarde** : sélectionnez une cible de stockage d'objets S3 enregistrée. Assurez-vous que la cible est accessible dans votre environnement de sauvegarde.
- **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Ceci est utile si vous avez plusieurs espaces IP et que vous souhaitez contrôler lequel est utilisé pour les sauvegardes.
- **Paramètres de planification** : sélectionnez la planification qui a été définie pour les instantanés locaux. Vous pouvez supprimer une planification, mais vous ne pouvez pas en ajouter une, car les planifications sont définies en fonction des planifications d'instantanés locaux.
- **Copies de conservation** : saisissez le nombre d'instantanés à conserver.
- **Exécuter à** : choisissez la planification de transfert ONTAP pour sauvegarder les données sur le stockage d'objets.
- * Hiérarchisez vos sauvegardes du magasin d'objets au stockage d'archivage* : si vous choisissez de hiérarchiser les sauvegardes vers le stockage d'archivage (par exemple, AWS Glacier), sélectionnez l'option de hiérarchisation et le nombre de jours d'archivage.
- **Activer l'analyse d'intégrité** : (non disponible pour les charges de travail Kubernetes) Sélectionnez si vous souhaitez activer les analyses d'intégrité (verrouillage des instantanés) sur le stockage d'objets. Cela garantit que les sauvegardes sont valides et peuvent être restaurées avec succès. La fréquence d'analyse d'intégrité est définie sur 7 jours par défaut. Pour protéger vos sauvegardes contre toute modification ou suppression, sélectionnez l'option **Analyse d'intégrité**. L'analyse s'effectue uniquement sur le dernier instantané. Vous pouvez activer ou désactiver les analyses d'intégrité sur le dernier instantané.

Créer une politique pour le stockage d'objets Microsoft Azure

Saisissez les informations dans ces champs :

- **Fournisseur** : sélectionnez **Azure**.
- **Abonnement Azure** : sélectionnez l'abonnement Azure parmi ceux découverts.
- **Groupe de ressources Azure** : sélectionnez le groupe de ressources Azure parmi ceux découverts.
- **Cible de sauvegarde** : sélectionnez une cible de stockage d'objets enregistrée. Assurez-vous que la cible est accessible dans votre environnement de sauvegarde.
- **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Ceci est utile si vous avez plusieurs espaces IP et que vous souhaitez contrôler lequel est utilisé pour les sauvegardes.
- **Paramètres de planification** : sélectionnez la planification qui a été définie pour les instantanés locaux. Vous pouvez supprimer une planification, mais vous ne pouvez pas en ajouter une, car les planifications sont définies en fonction des planifications d'instantanés locaux.
- **Copies de conservation** : saisissez le nombre d'instantanés à conserver.
- **Exécuter à** : choisissez la planification de transfert ONTAP pour sauvegarder les données sur le stockage d'objets.
- * Hiérarchisez vos sauvegardes du magasin d'objets au stockage d'archivage* : si vous choisissez de hiérarchiser les sauvegardes vers le stockage d'archivage, sélectionnez l'option de hiérarchisation et le nombre de jours d'archivage.
- **Activer l'analyse d'intégrité** : (non disponible pour les charges de travail Kubernetes) Sélectionnez si vous souhaitez activer les analyses d'intégrité (verrouillage des instantanés) sur le stockage d'objets. Cela garantit que les sauvegardes sont valides et peuvent être restaurées avec succès. La fréquence d'analyse d'intégrité est définie sur 7 jours par défaut. Pour protéger vos sauvegardes contre toute modification ou suppression, sélectionnez l'option **Analyse d'intégrité**. L'analyse s'effectue uniquement sur le dernier instantané. Vous pouvez activer ou désactiver les analyses d'intégrité sur le dernier instantané.

Créer une politique pour le stockage d'objets StorageGRID

Saisissez les informations dans ces champs :

- **Fournisseur** : Sélectionnez * StorageGRID*.
- * Informations d'identification StorageGRID * : sélectionnez les informations d'identification StorageGRID parmi celles découvertes. Ces informations d'identification sont utilisées pour accéder au système de stockage d'objets StorageGRID et ont été saisies dans l'option Paramètres.
- **Cible de sauvegarde** : sélectionnez une cible de stockage d'objets S3 enregistrée. Assurez-vous que la cible est accessible dans votre environnement de sauvegarde.
- **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Ceci est utile si vous avez plusieurs espaces IP et que vous souhaitez contrôler lequel est utilisé pour les sauvegardes.
- **Paramètres de planification** : sélectionnez la planification qui a été définie pour les instantanés locaux. Vous pouvez supprimer une planification, mais vous ne pouvez pas en ajouter une, car les planifications sont définies en fonction des planifications d'instantanés locaux.
- **Copies de conservation** : saisissez le nombre d'instantanés à conserver pour chaque fréquence.
- **Planification de transfert pour le stockage d'objets** : (non disponible pour les charges de travail Kubernetes) Choisissez la planification de transfert ONTAP pour sauvegarder les données sur le stockage d'objets.
- **Activer l'analyse d'intégrité** : (non disponible pour les charges de travail Kubernetes) Sélectionnez si vous souhaitez activer les analyses d'intégrité (verrouillage des instantanés) sur le stockage d'objets. Cela

garantit que les sauvegardes sont valides et peuvent être restaurées avec succès. La fréquence d'analyse d'intégrité est définie sur 7 jours par défaut. Pour protéger vos sauvegardes contre toute modification ou suppression, sélectionnez l'option **Analyse d'intégrité**. L'analyse s'effectue uniquement sur le dernier instantané. Vous pouvez activer ou désactiver les analyses d'intégrité sur le dernier instantané.

- * Hiérarchisez vos sauvegardes du magasin d'objets vers le stockage d'archivage* : (non disponible pour les charges de travail Kubernetes) Si vous choisissez de hiérarchiser les sauvegardes vers le stockage d'archivage, sélectionnez l'option de hiérarchisation et le nombre de jours d'archivage.

Configurer les paramètres avancés dans la politique

En option, vous pouvez configurer des paramètres avancés dans la politique. Ces paramètres sont disponibles pour toutes les architectures de sauvegarde, y compris les snapshots locaux, la réplication vers le stockage secondaire et les sauvegardes vers le stockage d'objets. Ces paramètres ne sont pas disponibles pour les charges de travail Kubernetes. Les paramètres avancés disponibles varient en fonction de la charge de travail que vous avez sélectionnée en haut de la page. Par conséquent, les paramètres avancés décrits ici peuvent ne pas s'appliquer à toutes les charges de travail. Les paramètres avancés ne sont pas disponibles lors de la configuration d'une politique pour les charges de travail Kubernetes.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Politiques**.
2. Depuis la page Politiques, sélectionnez **Créer une nouvelle politique**.
3. Dans la section **Politique > Paramètres avancés**, sélectionnez le menu **Sélectionner une action avancée** pour choisir parmi une liste de paramètres avancés.
4. Activez les paramètres que vous souhaitez afficher ou modifier, puis sélectionnez **Accepter**.
5. Fournissez les informations suivantes :
    - **Sauvegarde par copie uniquement** : (s'applique uniquement aux charges de travail Microsoft SQL Server) Choisissez la sauvegarde par copie uniquement (un type de sauvegarde Microsoft SQL Server) si vous devez sauvegarder vos ressources à l'aide d'une autre application de sauvegarde.
    - **Paramètres du groupe de disponibilité** : (s'applique uniquement aux charges de travail Microsoft SQL Server) Sélectionnez les réplicas de sauvegarde préférés ou spécifiez un réplica particulier. Ce paramètre est utile si vous disposez d'un groupe de disponibilité SQL Server et que vous souhaitez contrôler la réplique utilisée pour les sauvegardes.
    - **Taux de transfert maximal** : pour ne pas définir de limite d'utilisation de la bande passante, sélectionnez **Illimité**. Si vous souhaitez limiter le taux de transfert, sélectionnez **Limité** et sélectionnez la bande passante réseau entre 1 et 1 000 Mbps allouée au téléchargement des sauvegardes vers le stockage d'objets. Par défaut, ONTAP peut utiliser une quantité illimitée de bande passante pour transférer les données de sauvegarde des volumes du système vers le stockage d'objets. Si vous remarquez que le trafic de sauvegarde affecte les charges de travail normales des utilisateurs, envisagez de réduire la quantité de bande passante réseau utilisée pendant le transfert.
    - * Nouvelles tentatives de sauvegarde* : (non applicable aux charges de travail VMware) Pour réessayer la tâche en cas d'échec ou d'interruption, sélectionnez **Activer les nouvelles tentatives de tâche en cas d'échec**. Saisissez le nombre maximal de tentatives de capture instantanée et de sauvegarde ainsi que l'intervalle de temps de nouvelle tentative. Le recomptage doit être inférieur à 10. Ce paramètre est utile si vous souhaitez garantir que la tâche de sauvegarde est relancée en cas d'échec ou d'interruption.

Si la fréquence des instantanés est définie sur 1 heure, le délai maximal ainsi que le nombre de nouvelles tentatives ne doivent pas dépasser 45 minutes.

- **Activer les instantanés cohérents avec la machine virtuelle** : Indiquez si vous souhaitez activer les instantanés cohérents avec la machine virtuelle. Cela garantit que les instantanés nouvellement créés sont cohérents avec l'état de la machine virtuelle au moment de la création de l'instantané. Ceci est utile pour garantir que les sauvegardes peuvent être restaurées avec succès et que les données sont dans un état cohérent. Ceci ne s'applique pas aux instantanés existants.
- **Analyse des ransomwares** : sélectionnez si vous souhaitez activer l'analyse des ransomwares sur chaque bucket. Cela nécessite le verrouillage DataLock sur le stockage d'objets. Entrez la fréquence de l'analyse en jours. Cette option s'applique au stockage d'objets AWS et Microsoft Azure. Notez que cette option peut entraîner des frais supplémentaires, selon le fournisseur de cloud.
- **Vérification de sauvegarde** : (Non applicable aux charges de travail VMware) Sélectionnez si vous souhaitez activer la vérification de sauvegarde et si vous la souhaitez immédiatement ou ultérieurement. Cette fonctionnalité garantit que les sauvegardes sont valides et peuvent être restaurées avec succès. Nous vous recommandons d'activer cette option pour garantir l'intégrité de vos sauvegardes. Par défaut, la vérification de la sauvegarde s'exécute à partir du stockage secondaire si le stockage secondaire est configuré. Si le stockage secondaire n'est pas configuré, la vérification de la sauvegarde s'exécute à partir du stockage principal.

  De plus, configurez les options suivantes :

  - Vérification **quotidienne**, **hebdomadaire**, **mensuelle** ou **annuelle** : si vous avez choisi **plus tard** comme vérification de sauvegarde, sélectionnez la fréquence de vérification de sauvegarde. Cela garantit que les sauvegardes sont régulièrement vérifiées pour leur intégrité et peuvent être restaurées avec succès.
  - **Étiquettes de sauvegarde** : saisissez une étiquette pour la sauvegarde. Cette étiquette est utilisée pour identifier la sauvegarde dans le système et peut être utile pour le suivi et la gestion des sauvegardes.
  - **Vérification de cohérence de la base de données** : (non applicable aux charges de travail VMware) Sélectionnez si vous souhaitez activer les vérifications de cohérence de la base de données. Cette option garantit que les bases de données sont dans un état cohérent avant la sauvegarde, ce qui est essentiel pour garantir l'intégrité des données.
  - **Vérifier les sauvegardes de journaux** : (Non applicable aux charges de travail VMware) Sélectionnez si vous souhaitez vérifier les sauvegardes de journaux. Sélectionnez le serveur de vérification. Si vous avez choisi disque à disque ou 3-2-1, sélectionnez également l'emplacement de stockage de vérification. Cette option garantit que les sauvegardes de journaux sont valides et peuvent être restaurées avec succès, ce qui est important pour maintenir l'intégrité de vos bases de données.
- **Réseau** : Sélectionnez l'interface réseau à utiliser pour les opérations de sauvegarde. Ceci est utile si vous disposez de plusieurs interfaces réseau et que vous souhaitez contrôler laquelle est utilisée pour les sauvegardes.
  - **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Ceci est utile si vous avez plusieurs espaces IP et que vous souhaitez contrôler lequel est utilisé pour les sauvegardes.
  - **Configuration de point de terminaison privé** : si vous utilisez un point de terminaison privé pour votre stockage d'objets, sélectionnez la configuration de point de terminaison privé à utiliser pour les opérations de sauvegarde. Ceci est utile si vous souhaitez garantir que les sauvegardes sont transférées en toute sécurité via une connexion réseau privée.
- **Notification** : sélectionnez si vous souhaitez activer les notifications par e-mail pour les opérations de sauvegarde. Ceci est utile si vous souhaitez être averti lorsqu'une opération de sauvegarde démarre, se termine ou échoue.
- **Disques indépendants** : (s'applique uniquement aux charges de travail VMware) Cochez cette case

pour inclure dans la sauvegarde tous les magasins de données avec des disques indépendants contenant des données temporaires. Un disque indépendant est un disque VM qui n'est pas inclus dans les snapshots VMware.

- * Format de volume et d'instantané SnapMirror * : si vous le souhaitez, entrez votre propre nom d'instantané dans une stratégie qui régit les sauvegardes pour les charges de travail Microsoft SQL Server. Saisissez le format et le texte personnalisé. Si vous choisissez d'effectuer une sauvegarde sur un stockage secondaire, vous pouvez également ajouter un préfixe et un suffixe de volume SnapMirror .

Modifier une politique

Vous pouvez modifier l'architecture de sauvegarde, la fréquence de sauvegarde, la politique de rétention et d'autres paramètres d'une politique.

Vous pouvez ajouter un autre niveau de protection lorsque vous modifiez une politique, mais vous ne pouvez pas supprimer un niveau de protection. Par exemple, si la politique protège uniquement les snapshots locaux, vous pouvez ajouter la réplication au stockage secondaire ou les sauvegardes au stockage d'objets. Si vous disposez de snapshots et de réplications locaux, vous pouvez ajouter un stockage d'objets. Cependant, si vous disposez de snapshots locaux, de réplication et de stockage d'objets, vous ne pouvez pas supprimer l'un de ces niveaux.

Si vous modifiez une politique qui sauvegarde sur un stockage d'objets, vous pouvez activer l'archivage.

Si vous avez importé des ressources depuis SnapCenter, vous risquez de rencontrer certaines différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans NetApp Backup and Recovery. Voir"Différences de politique entre SnapCenter et NetApp Backup and Recovery" .

Rôle de NetApp Console requis

Super administrateur de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans la NetApp Console, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'option **Politiques**.
3. Sélectionnez la politique que vous souhaitez modifier.
4. Sélectionnez les **Actions*** ••• **icône et sélectionnez *Modifier**.

Supprimer une politique

Vous pouvez supprimer une politique si vous n'en avez plus besoin.

Vous ne pouvez pas supprimer une politique associée à une charge de travail.

Étapes

1. Dans la console, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'option **Politiques**.
3. Sélectionnez la politique que vous souhaitez supprimer.
4. Sélectionnez les **Actions*** ••• **icône et sélectionnez *Supprimer**.
5. Confirmez l'action et sélectionnez **Supprimer**.

Protégez les charges de travail du volume ONTAP

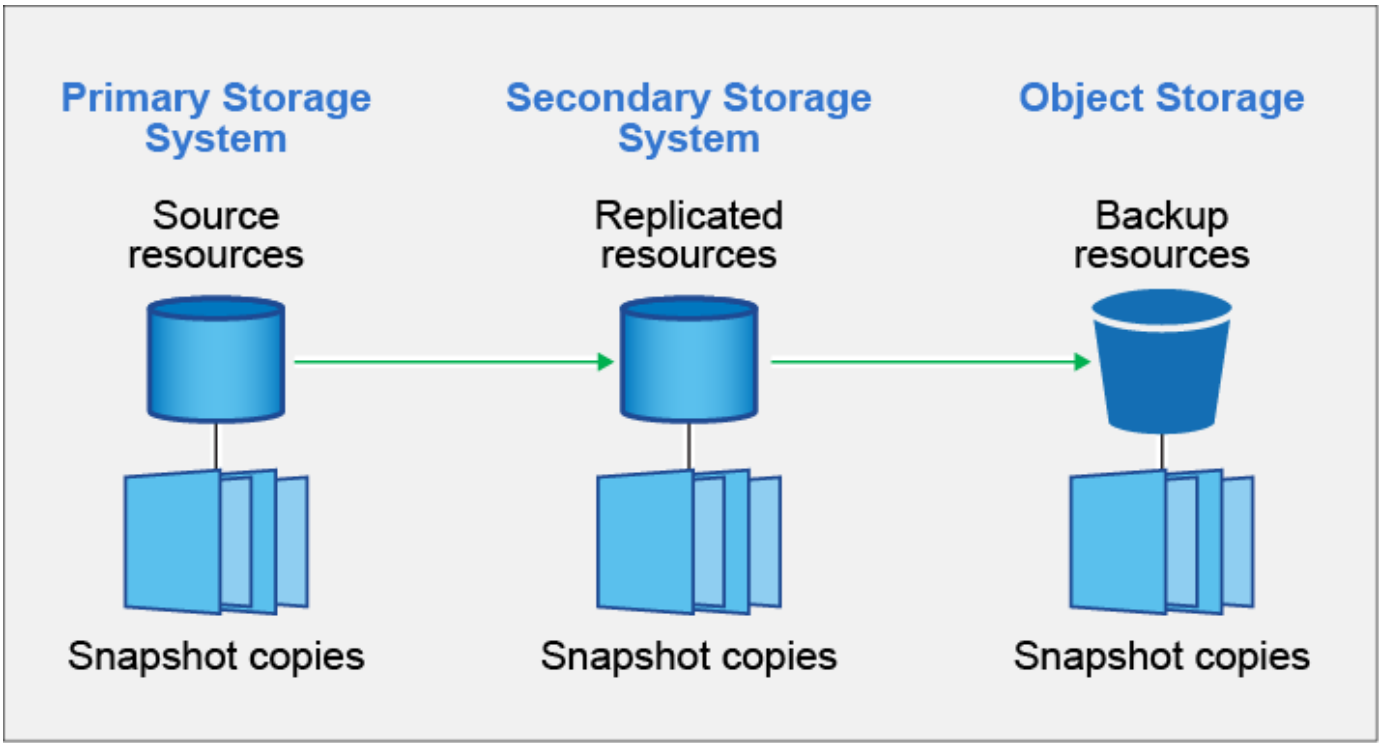
Protégez vos données de volume ONTAP à l'aide de NetApp Backup and Recovery

NetApp Backup and Recovery fournit des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données de volume ONTAP . Vous pouvez mettre en œuvre une stratégie 3-2-1 dans laquelle vous disposez de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Après l'activation, la sauvegarde et la récupération créent des sauvegardes incrémentielles permanentes au niveau des blocs qui sont stockées sur un autre cluster ONTAP et dans le stockage d'objets dans le cloud. En plus de votre volume source, vous disposerez de :

- Instantané du volume sur le système source
- Volume répliqué sur un autre système de stockage
- Sauvegarde du volume dans le stockage d'objets



NetApp Backup and Recovery exploite la technologie de réplication de données SnapMirror de NetApp pour garantir que toutes les sauvegardes sont entièrement synchronisées en créant des instantanés et en les transférant vers les emplacements de sauvegarde.

Les avantages de l'approche 3-2-1 incluent :

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.

- L’utilisation de différents types de supports vous aide à récupérer si l’un d’eux tombe en panne.
- Vous pouvez restaurer rapidement à partir de la copie sur site et utiliser les copies hors site si la copie sur site est compromise.

Si nécessaire, vous pouvez restaurer un *volume* entier, un *dossier* ou un ou plusieurs *fichiers*, à partir de n’importe quelle copie de sauvegarde vers le même système ou vers un système différent.

Caractéristiques

Fonctionnalités de réplication :

- Répliquez les données entre les systèmes de stockage ONTAP pour prendre en charge la sauvegarde et la reprise après sinistre.
- Assurez la fiabilité de votre environnement DR avec une haute disponibilité.
- Cryptage en vol ONTAP natif configuré via une clé pré-partagée (PSK) entre les deux systèmes.
- Les données copiées sont immuables jusqu’à ce que vous les rendiez accessibles en écriture et prêtes à être utilisées.
- La réplication est auto-réparatrice en cas d’échec de transfert.
- Par rapport à "NetApp Replication" , la réplication dans NetApp Backup and Recovery inclut les fonctionnalités suivantes :
  - Répliquez plusieurs volumes FlexVol à la fois sur un système secondaire.
  - Restaurez un volume répliqué sur le système source ou sur un autre système à l’aide de l’interface utilisateur.

Voir"Limitations de réplication pour les volumes ONTAP" pour obtenir la liste des fonctionnalités de réplication qui ne sont pas disponibles avec les volumes NetApp Backup and Recovery for ONTAP .

Fonctionnalités de sauvegarde sur objet :

- Sauvegardez des copies indépendantes de vos volumes de données sur un stockage d’objets à faible coût.
- Appliquez une politique de sauvegarde unique à tous les volumes d’un cluster ou attribuez différentes politiques de sauvegarde aux volumes ayant des objectifs de point de récupération uniques.
- Créez une politique de sauvegarde à appliquer à tous les futurs volumes créés dans le cluster.
- Créez des fichiers de sauvegarde immuables afin qu’ils soient verrouillés et protégés pendant la période de conservation.
- Analysez les fichiers de sauvegarde à la recherche d’une éventuelle attaque de ransomware et supprimez/remplacez automatiquement les sauvegardes infectées.
- Classez les fichiers de sauvegarde plus anciens dans un stockage d’archives pour réduire les coûts.
- Supprimez la relation de sauvegarde afin de pouvoir archiver les volumes sources inutiles tout en conservant les sauvegardes de volume.
- Sauvegardez d’un cloud à l’autre et des systèmes sur site vers un cloud public ou privé.
- Les données de sauvegarde sont sécurisées avec un cryptage AES-256 bits au repos et des connexions TLS 1.2 HTTPS en vol.
- Utilisez vos propres clés gérées par le client pour le chiffrement des données au lieu d’utiliser les clés de chiffrement par défaut de votre fournisseur de cloud.

- Prise en charge jusqu'à 4 000 sauvegardes d'un seul volume.

Restaurer les fonctionnalités :

- Restaurez des données à partir d'un point précis dans le temps à partir d'instantanés locaux, de volumes répliqués ou de volumes sauvegardés dans un stockage objet.
- Restaurer un volume, un dossier ou des fichiers individuels, sur le système source ou sur un autre système.
- Restaurer les données sur un système utilisant un abonnement/compte différent ou situé dans une région différente.
- Effectuez une *restauration rapide* d'un volume depuis un stockage cloud vers un système Cloud Volumes ONTAP ou vers un système sur site ; parfait pour les situations de reprise après sinistre où vous devez fournir l'accès à un volume dès que possible.
- Restaurez les données au niveau du bloc, en plaçant les données directement à l'emplacement que vous spécifiez, tout en préservant les ACL d'origine.
- Parcourez et recherchez des catalogues de fichiers pour une sélection facile de dossiers et de fichiers individuels pour la restauration d'un seul fichier.

Systèmes pris en charge pour les opérations de sauvegarde et de restauration

NetApp Backup and Recovery prend en charge les systèmes ONTAP et les fournisseurs de cloud public et privé.

Régions prises en charge

NetApp Backup and Recovery est pris en charge avec Cloud Volumes ONTAP dans de nombreuses régions Amazon Web Services, Microsoft Azure et Google Cloud.

"En savoir plus en utilisant la carte des régions mondiales"

Destinations de sauvegarde prises en charge

NetApp Backup and Recovery vous permet de sauvegarder des volumes ONTAP à partir des systèmes sources suivants vers les systèmes secondaires et le stockage objet suivants, chez les fournisseurs de cloud public et privé. Les snapshots résident sur le système source.

Système source	Système secondaire (réplication)	Magasin d'objets de destination (sauvegarde)
Cloud Volumes ONTAP dans AWS	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Amazon S3
Cloud Volumes ONTAP dans Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Azure Blob
Cloud Volumes ONTAP dans Google	Cloud Volumes ONTAP dans le système ONTAP sur site de Google	Stockage Google Cloud
Système ONTAP sur site	Cloud Volumes ONTAP Système ONTAP sur site	Amazon S3, Azure Blob, Google Cloud Storage, NetApp StorageGRID , ONTAP S3

Destinations de restauration prises en charge

Vous pouvez restaurer les données ONTAP à partir d'un fichier de sauvegarde situé sur un système secondaire (volume répliqué) ou dans un stockage objet (fichier de sauvegarde) vers les systèmes suivants. Les instantanés résident sur le système source et ne peuvent être restaurés que sur ce même système.

Emplacement du fichier de sauvegarde		Système de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Cloud Volumes ONTAP dans le système ONTAP sur site AWS
Azure Blob	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure
Stockage Google Cloud	Cloud Volumes ONTAP dans le système ONTAP sur site de Google	Cloud Volumes ONTAP dans le système ONTAP sur site de Google
NetApp StorageGRID	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site
ONTAP S3	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Volumes pris en charge

NetApp Backup and Recovery prend en charge les types de volumes suivants :

- Volumes de lecture-écriture FlexVol
- Volumes FlexGroup (nécessite ONTAP 9.12.1 ou version ultérieure)
- Volumes SnapLock Enterprise (nécessite ONTAP 9.11.1 ou version ultérieure)
- SnapLock Compliance pour les volumes sur site (nécessite ONTAP 9.14 ou version ultérieure)
- Volumes de destination de protection des données SnapMirror (DP)

NetApp Backup and Recovery ne prend pas en charge les sauvegardes des volumes FlexCache .

Voir les sections sur"Limitations de sauvegarde et de restauration pour les volumes ONTAP" pour des exigences et des limitations supplémentaires.

Coût

Il existe deux types de coûts associés à l'utilisation de NetApp Backup and Recovery avec les systèmes ONTAP : les frais de ressources et les frais de service. Ces deux frais concernent la partie sauvegarde sur objet du service.

La création d'instantanés ou de volumes répliqués est gratuite, hormis l'espace disque nécessaire à leur stockage.

Frais de ressources

Des frais de ressources sont payés au fournisseur de cloud pour la capacité de stockage d'objets et pour

l'écriture et la lecture de fichiers de sauvegarde dans le cloud.

- Pour la sauvegarde sur un stockage d'objets, vous payez votre fournisseur de cloud pour les coûts de stockage d'objets.

  Étant donné que NetApp Backup and Recovery préserve l'efficacité du stockage du volume source, vous payez au fournisseur de cloud les coûts de stockage d'objets pour les données *après* l'efficacité ONTAP (pour la plus petite quantité de données après l'application de la déduplication et de la compression).

- Pour restaurer des données à l'aide de la recherche et de la restauration, certaines ressources sont provisionnées par votre fournisseur de cloud et un coût par Tio est associé à la quantité de données analysées par vos demandes de recherche. (Ces ressources ne sont pas nécessaires pour parcourir et restaurer.)
  - Dans AWS, "Amazone Athéna" et "Colle AWS" les ressources sont déployées dans un nouveau bucket S3.
  - Dans Azure, un "Espace de travail Azure Synapse" et "Stockage Azure Data Lake" sont provisionnés dans votre compte de stockage pour stocker et analyser vos données.
  - Dans Google, un nouveau bucket est déployé et le "Services Google Cloud BigQuery" sont provisionnés au niveau du compte/projet.
- Si vous prévoyez de restaurer des données de volume à partir d'un fichier de sauvegarde qui a été déplacé vers un stockage d'objets d'archivage, des frais de récupération par Gio et des frais par demande supplémentaires sont facturés par le fournisseur de cloud.
- Si vous prévoyez d'analyser un fichier de sauvegarde à la recherche de ransomwares pendant le processus de restauration des données du volume (si vous avez activé DataLock et Ransomware Resilience pour vos sauvegardes cloud), vous devrez également supporter des frais de sortie supplémentaires auprès de votre fournisseur cloud.

Frais de service

Les frais de service sont payés à NetApp et couvrent à la fois le coût de *création* de sauvegardes sur le stockage d'objets et de *restauration* de volumes ou de fichiers à partir de ces sauvegardes. Vous payez uniquement pour les données que vous protégez dans le stockage d'objets, calculées par la capacité logique source utilisée (avant l'efficacité ONTAP) des volumes ONTAP qui sont sauvegardés dans le stockage d'objets. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

Il existe trois façons de payer le service de sauvegarde. La première option est de vous abonner auprès de votre fournisseur cloud, ce qui vous permet de payer par mois. La deuxième option est d'obtenir un contrat annuel. La troisième option consiste à acheter des licences directement auprès de NetApp.

Licences

NetApp Backup and Recovery est disponible avec les modèles de consommation suivants :

- **BYOL** : une licence achetée auprès de NetApp qui peut être utilisée avec n'importe quel fournisseur de cloud.
- **PAYGO** : Un abonnement horaire sur la place de marché de votre fournisseur cloud.
- **Annuel** : Un contrat annuel de la place de marché de votre fournisseur de cloud.

Une licence de sauvegarde est requise uniquement pour la sauvegarde et la restauration à partir du stockage d'objets. La création d'instantanés et de volumes répliqués ne nécessite pas de licence.

Apportez votre propre permis

BYOL est basé sur la durée (1, 2 ou 3 ans) *et* sur la capacité par incréments de 1 Tio. Vous payez NetApp pour utiliser le service pendant une période donnée, par exemple 1 an, et pour une capacité maximale, par exemple 10 Tio.

Vous recevrez un numéro de série que vous saisirez dans la NetApp Console pour activer le service. Lorsque l'une ou l'autre des limites est atteinte, vous devrez renouveler la licence. La licence Backup BYOL s'applique à tous les systèmes sources associés à votre organisation ou compte NetApp Console .

"Apprenez à gérer vos licences BYOL".

Abonnement à la carte

NetApp Backup and Recovery propose des licences basées sur la consommation dans un modèle de paiement à l'utilisation. Après avoir souscrit un abonnement via la place de marché de votre fournisseur cloud, vous payez par Gio pour les données sauvegardées — il n'y a pas de paiement initial. Vous êtes facturé par votre fournisseur cloud via votre facture mensuelle.

"Découvrez comment configurer un abonnement à la carte".

Notez qu'un essai gratuit de 30 jours est disponible lorsque vous souscrivez initialement à un abonnement PAYGO.

Contrat annuel

Lorsque vous utilisez AWS, deux contrats annuels sont disponibles pour des durées de 1, 2 ou 3 ans :

- Un plan « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un plan « CVO Professional » qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery. Cela inclut des sauvegardes illimitées pour les Cloud Volumes ONTAP facturés sur cette licence (la capacité de sauvegarde n'est pas comptabilisée dans la licence).

Lorsque vous utilisez Azure, deux contrats annuels sont disponibles pour des durées de 1, 2 ou 3 ans :

- Un plan « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un plan « CVO Professional » qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery. Cela inclut des sauvegardes illimitées pour les Cloud Volumes ONTAP facturés sur cette licence (la capacité de sauvegarde n'est pas comptabilisée dans la licence).

Lorsque vous utilisez GCP, vous pouvez demander une offre privée auprès de NetApp, puis sélectionner le plan lorsque vous vous abonnez à partir de Google Cloud Marketplace lors de l'activation de NetApp Backup and Recovery .

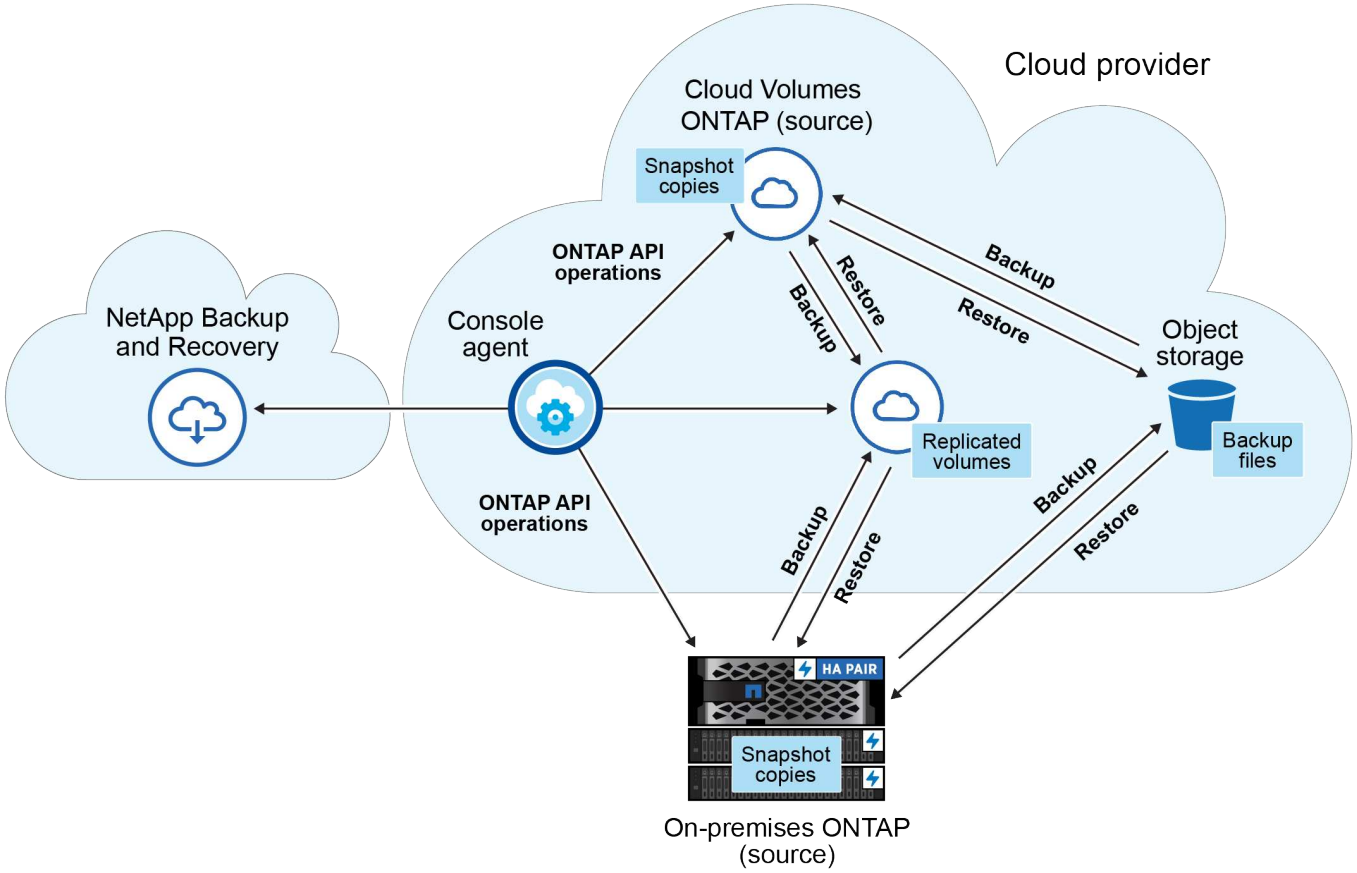
"Apprenez à mettre en place des contrats annuels".

Comment fonctionne la NetApp Backup and Recovery

Lorsque vous activez NetApp Backup and Recovery sur un système Cloud Volumes ONTAP ou ONTAP sur site, le service effectue une sauvegarde complète de vos données. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés. Cela permet de maintenir le trafic réseau à un minimum. La sauvegarde sur le stockage d'objets est construite sur la base de "Technologie NetApp SnapMirror Cloud" .

Toute action effectuée directement depuis l'environnement de votre fournisseur de cloud pour gérer ou modifier les fichiers de sauvegarde cloud peut corrompre les fichiers et entraîner une configuration non prise en charge.

L'image suivante montre la relation entre chaque composant :



Ce diagramme montre les volumes en cours de réplication sur un système Cloud Volumes ONTAP , mais les volumes peuvent également être répliqués sur un système ONTAP sur site.

Où résident les sauvegardes

Les sauvegardes résident à différents emplacements en fonction du type de sauvegarde :

- Les *instantanés* résident sur le volume source du système source.
- Les *volumes répliqués* résident sur le système de stockage secondaire : un système Cloud Volumes ONTAP ou ONTAP sur site.
- Les *copies de sauvegarde* sont stockées dans un magasin d'objets que la console crée dans votre compte cloud. Il existe un magasin d'objets par cluster/système, et la console nomme le magasin d'objets comme suit : « netapp-backup-clusteruuid ». Assurez-vous de ne pas supprimer ce magasin d'objets.
  - Dans AWS, la console permet "Fonctionnalité d'accès public au bloc Amazon S3" sur le compartiment S3.
  - Dans Azure, la console utilise un groupe de ressources nouveau ou existant avec un compte de stockage pour le conteneur Blob. La console "bloque l'accès public à vos données blob" par défaut.
  - Dans GCP, la console utilise un projet nouveau ou existant avec un compte de stockage pour le bucket Google Cloud Storage.

- Dans StorageGRID, la console utilise un compte locataire existant pour le compartiment S3.
- Dans ONTAP S3, la console utilise un compte utilisateur existant pour le bucket S3.

Si vous souhaitez modifier le magasin d'objets de destination d'un cluster à l'avenir, vous devrez"désinscrire NetApp Backup and Recovery pour le système" , puis activez NetApp Backup and Recovery à l'aide des informations du nouveau fournisseur de cloud.

Planification de sauvegarde et paramètres de conservation personnalisables

Lorsque vous activez NetApp Backup and Recovery pour un système, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide des stratégies que vous sélectionnez. Vous pouvez sélectionner des politiques distinctes pour les instantanés, les volumes répliqués et les fichiers de sauvegarde. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes ayant des objectifs de point de récupération (RPO) différents, vous pouvez créer des stratégies supplémentaires pour ce cluster et attribuer ces stratégies aux autres volumes une fois NetApp Backup and Recovery activé.

Vous pouvez choisir une combinaison de sauvegardes horaires, quotidiennes, hebdomadaires, mensuelles et annuelles de tous les volumes. Pour la sauvegarde d'un objet, vous pouvez également sélectionner l'une des politiques définies par le système qui fournissent des sauvegardes et une conservation pendant 3 mois, 1 an et 7 ans. Les stratégies de protection de sauvegarde que vous avez créées sur le cluster à l'aide ONTAP System Manager ou de l'interface de ligne de commande ONTAP apparaîtront également sous forme de sélections. Cela inclut les politiques créées à l'aide d'étiquettes SnapMirror personnalisées.

> La politique de capture instantanée appliquée au volume doit avoir l'une des étiquettes que vous utilisez dans votre politique de réplication et votre politique de sauvegarde vers l'objet. Si aucune étiquette correspondante n'est trouvée, aucun fichier de sauvegarde ne sera créé. Par exemple, si vous souhaitez créer des volumes répliqués et des fichiers de sauvegarde « hebdomadaires », vous devez utiliser une stratégie de snapshot qui crée des snapshots « hebdomadaires ».

Une fois que vous atteignez le nombre maximal de sauvegardes pour une catégorie ou un intervalle, les sauvegardes les plus anciennes sont supprimées afin que vous disposiez toujours des sauvegardes les plus récentes (et ainsi les sauvegardes obsolètes ne continuent pas à occuper de l'espace).

> La période de conservation des sauvegardes des volumes de protection des données est la même que celle définie dans la relation source SnapMirror . Vous pouvez modifier cela si vous le souhaitez en utilisant l'API.

Paramètres de protection des fichiers de sauvegarde

Si votre cluster utilise ONTAP 9.11.1 ou une version ultérieure, vous pouvez protéger vos sauvegardes dans le stockage d'objets contre les attaques de suppression et de ransomware. Chaque politique de sauvegarde fournit une section pour *DataLock et Ransomware Resilience* qui peut être appliquée à vos fichiers de sauvegarde pendant une période spécifique - la *période de conservation*.

- *DataLock* protège vos fichiers de sauvegarde contre toute modification ou suppression.
- *La protection contre les ransomwares* analyse vos fichiers de sauvegarde pour rechercher des preuves d'une attaque de ransomware lorsqu'un fichier de sauvegarde est créé et lorsque les données d'un fichier de sauvegarde sont en cours de restauration.

Les analyses de protection contre les ransomwares planifiées sont activées par défaut. Le paramètre par défaut pour la fréquence d'analyse est de 7 jours. L'analyse s'effectue uniquement sur le dernier instantané. Les analyses programmées peuvent être désactivées pour réduire vos coûts. Vous pouvez activer ou

désactiver les analyses planifiées de logiciels de ransomware sur le dernier instantané en utilisant l'option de la page Paramètres avancés. Si vous l'activez, les analyses sont effectuées chaque semaine par défaut. Vous pouvez modifier ce calendrier en jours ou en semaines ou le désactiver, ce qui permet de réduire les coûts.

La période de conservation des sauvegardes est la même que la période de conservation de la planification des sauvegardes, plus une mémoire tampon maximale de 31 jours. Par exemple, des sauvegardes hebdomadaires avec 5 copies conservées verrouillent chaque fichier de sauvegarde pendant 5 semaines. Les sauvegardes *mensuelles* avec *6* copies conservées verrouillent chaque fichier de sauvegarde pendant 6 mois.

L'assistance est actuellement disponible lorsque votre destination de sauvegarde est Amazon S3, Azure Blob ou NetApp StorageGRID. D'autres destinations de fournisseurs de stockage seront ajoutées dans les prochaines versions.

Pour plus de détails, reportez-vous à ces informations :

- "Comment fonctionnent DataLock et la protection contre les ransomwares".
- "Comment mettre à jour les options de protection contre les ransomwares dans la page Paramètres avancés".

DataLock ne peut pas être activé si vous hiérarchisez les sauvegardes vers un stockage d'archivage.

Stockage d'archives pour les fichiers de sauvegarde plus anciens

Lorsque vous utilisez certains stockages cloud, vous pouvez déplacer des fichiers de sauvegarde plus anciens vers une classe de stockage/un niveau d'accès moins coûteux après un certain nombre de jours. Vous pouvez également choisir d'envoyer immédiatement vos fichiers de sauvegarde vers un stockage d'archives sans les écrire sur un stockage cloud standard. Notez que le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.

- Dans AWS, les sauvegardes démarrent dans la classe de stockage *Standard* et passent à la classe de stockage *Standard-Infrequent Access* après 30 jours.

  Si votre cluster utilise ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive* dans l'interface utilisateur NetApp Backup and Recovery après un certain nombre de jours pour une optimisation supplémentaire des coûts. "En savoir plus sur le stockage d'archives AWS" .

- Dans Azure, les sauvegardes sont associées au niveau d'accès *Cool*.

  Si votre cluster utilise ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers le stockage *Azure Archive* dans l'interface utilisateur NetApp Backup and Recovery après un certain nombre de jours pour une optimisation supplémentaire des coûts. "En savoir plus sur le stockage d'archives Azure" .

- Dans GCP, les sauvegardes sont associées à la classe de stockage *Standard*.

  Si votre cluster utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers le stockage *Archive* dans l'interface utilisateur NetApp Backup and Recovery après un certain nombre de jours pour une optimisation supplémentaire des coûts. "En savoir plus sur le stockage d'archives Google" .

- Dans StorageGRID, les sauvegardes sont associées à la classe de stockage *Standard*.

Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure et que votre système StorageGRID utilise 11.4 ou une version ultérieure, vous pouvez archiver les anciens fichiers de sauvegarde sur un stockage d'archivage cloud public après un certain nombre de jours. La prise en charge actuelle concerne les niveaux de stockage AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. "En savoir plus sur l'archivage des fichiers de sauvegarde depuis StorageGRID" .

Voir le lien : prev-ontap-policy-object-options.html] pour plus de détails sur l'archivage des anciens fichiers de sauvegarde.

Considérations relatives à la politique de hiérarchisation de FabricPool

Il y a certaines choses que vous devez savoir lorsque le volume que vous sauvegardez réside sur un agrégat FabricPool et qu'il dispose d'une politique de hiérarchisation attribuée autre que `none` :

- La première sauvegarde d'un volume à plusieurs niveaux FabricPool nécessite la lecture de toutes les données locales et à plusieurs niveaux (à partir du magasin d'objets). Une opération de sauvegarde ne « réchauffe » pas les données froides hiérarchisées dans le stockage d'objets.

  Cette opération pourrait entraîner une augmentation ponctuelle du coût de lecture des données auprès de votre fournisseur de cloud.

  - Les sauvegardes ultérieures sont incrémentielles et n'ont pas cet effet.
  - Si la politique de hiérarchisation est attribuée au volume lors de sa création initiale, vous ne verrez pas ce problème.
- Tenez compte de l'impact des sauvegardes avant d'attribuer la `all` politique de hiérarchisation des volumes. Étant donné que les données sont hiérarchisées immédiatement, NetApp Backup and Recovery lira les données à partir du niveau cloud plutôt qu'à partir du niveau local. Étant donné que les opérations de sauvegarde simultanées partagent la liaison réseau avec le magasin d'objets cloud, une dégradation des performances peut se produire si les ressources réseau sont saturées. Dans ce cas, vous souhaiterez peut-être configurer de manière proactive plusieurs interfaces réseau (LIF) pour réduire ce type de saturation du réseau.

Planifiez votre parcours de protection avec NetApp Backup and Recovery

NetApp Backup and Recovery vous permet de créer jusqu'à trois copies de vos volumes sources pour protéger vos données. Il existe de nombreuses options que vous pouvez sélectionner lors de l'activation de la sauvegarde et de la récupération sur vos volumes. Vous devez donc revoir vos choix afin d'être prêt.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Nous passerons en revue les options suivantes :

- Quelles fonctionnalités de protection utiliserez-vous : instantanés, volumes répliqués et/ou sauvegarde dans le cloud ?
- Quelle architecture de sauvegarde utiliserez-vous : une sauvegarde en cascade ou en éventail de vos volumes ?
- Allez-vous utiliser les politiques de sauvegarde par défaut ou devez-vous créer des politiques personnalisées ?

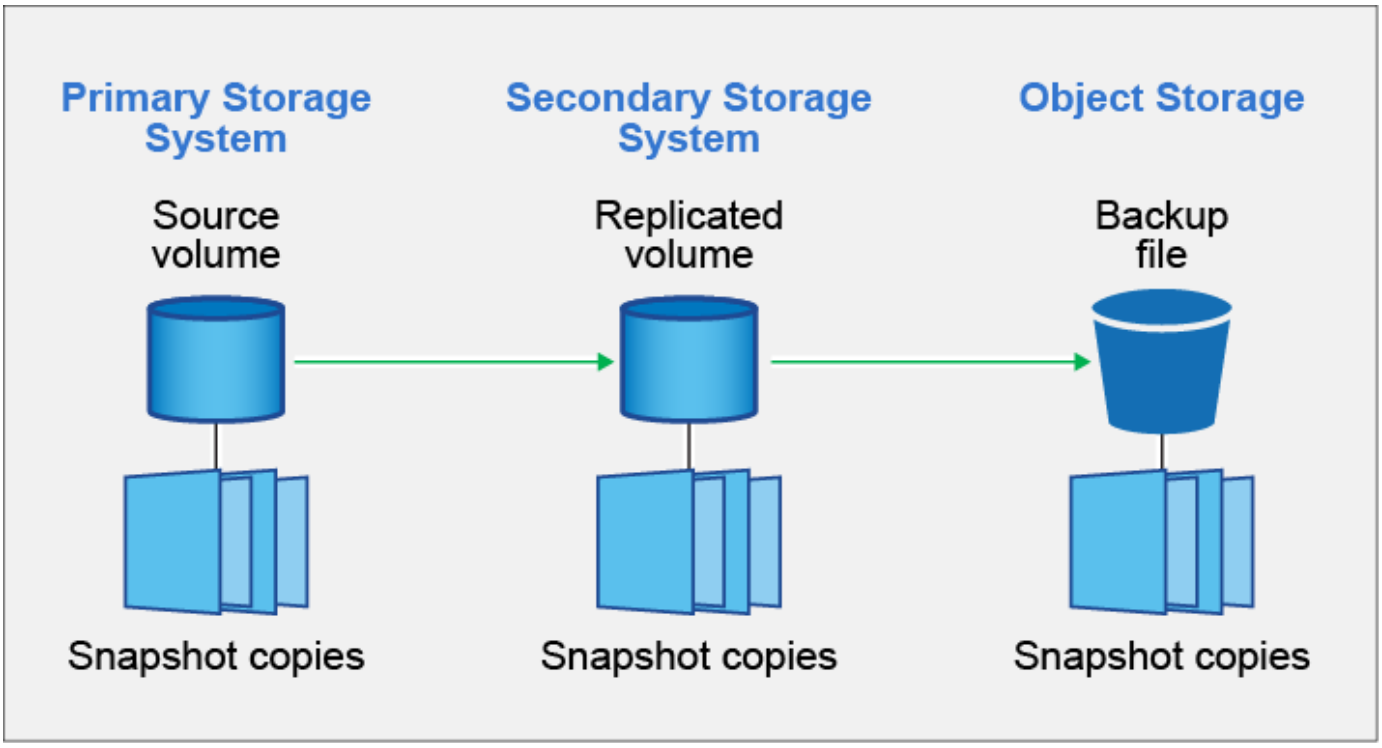
- Voulez-vous que le service crée les buckets cloud pour vous ou souhaitez-vous créer vos conteneurs de stockage d'objets avant de commencer ?
- Quel mode de déploiement de l'agent de console utilisez-vous (mode standard, restreint ou privé) ?

Quelles fonctionnalités de protection utiliserez-vous

Avant de sélectionner les fonctionnalités que vous utiliserez, voici une explication rapide de ce que fait chaque fonctionnalité et du type de protection qu'elle offre.

Type de sauvegarde	Description
Instantané	Crée une image en lecture seule et à un instant donné d'un volume au sein du volume source, sous forme d'instantané. Vous pouvez utiliser l'instantané pour récupérer des fichiers individuels ou pour restaurer l'intégralité du contenu d'un volume.
Réplication	Crée une copie secondaire de vos données sur un autre système de stockage ONTAP et met à jour en permanence les données secondaires. Vos données sont maintenues à jour et restent disponibles à chaque fois que vous en avez besoin.
Sauvegarde dans le cloud	Crée des sauvegardes de vos données dans le cloud à des fins de protection et d'archivage à long terme. Si nécessaire, vous pouvez restaurer un volume, un dossier ou des fichiers individuels à partir de la sauvegarde sur le même système ou sur un système différent.

Les instantanés sont la base de toutes les méthodes de sauvegarde et sont nécessaires pour utiliser le service de sauvegarde et de récupération. Un instantané est une image en lecture seule, à un instant T, d'un volume. L'image consomme un espace de stockage minimal et n'entraîne qu'une surcharge de performance négligeable, car elle n'enregistre que les modifications apportées aux fichiers depuis la dernière capture d'écran. L'instantané créé sur votre volume est utilisé pour maintenir la synchronisation entre le volume répliqué et le fichier de sauvegarde avec les modifications apportées au volume source, comme illustré sur la figure.



Vous pouvez choisir de créer à la fois des volumes répliqués sur un autre système de stockage ONTAP et des fichiers de sauvegarde dans le cloud. Ou vous pouvez choisir simplement de créer des volumes répliqués ou des fichiers de sauvegarde : c'est votre choix.

Pour résumer, voici les flux de protection valides que vous pouvez créer pour les volumes de votre système ONTAP :

- Volume source → Instantané → Volume répliqué → Fichier de sauvegarde
- Volume source → Instantané → Fichier de sauvegarde
- Volume source → Instantané → Volume répliqué

> La création initiale d'un volume répliqué ou d'un fichier de sauvegarde inclut une copie complète des données sources : c'est ce qu'on appelle un *transfert de base*. Les transferts ultérieurs ne contiennent que des copies différentielles des données sources (l'instantané).

Comparaison des différentes méthodes de sauvegarde

Le tableau suivant présente une comparaison généralisée des trois méthodes de sauvegarde. Bien que l'espace de stockage d'objets soit généralement moins cher que votre stockage sur disque local, si vous pensez que vous devrez restaurer fréquemment des données à partir du cloud, les frais de sortie des fournisseurs de cloud peuvent réduire une partie de vos économies. Vous devrez identifier la fréquence à laquelle vous devez restaurer les données à partir des fichiers de sauvegarde dans le cloud.

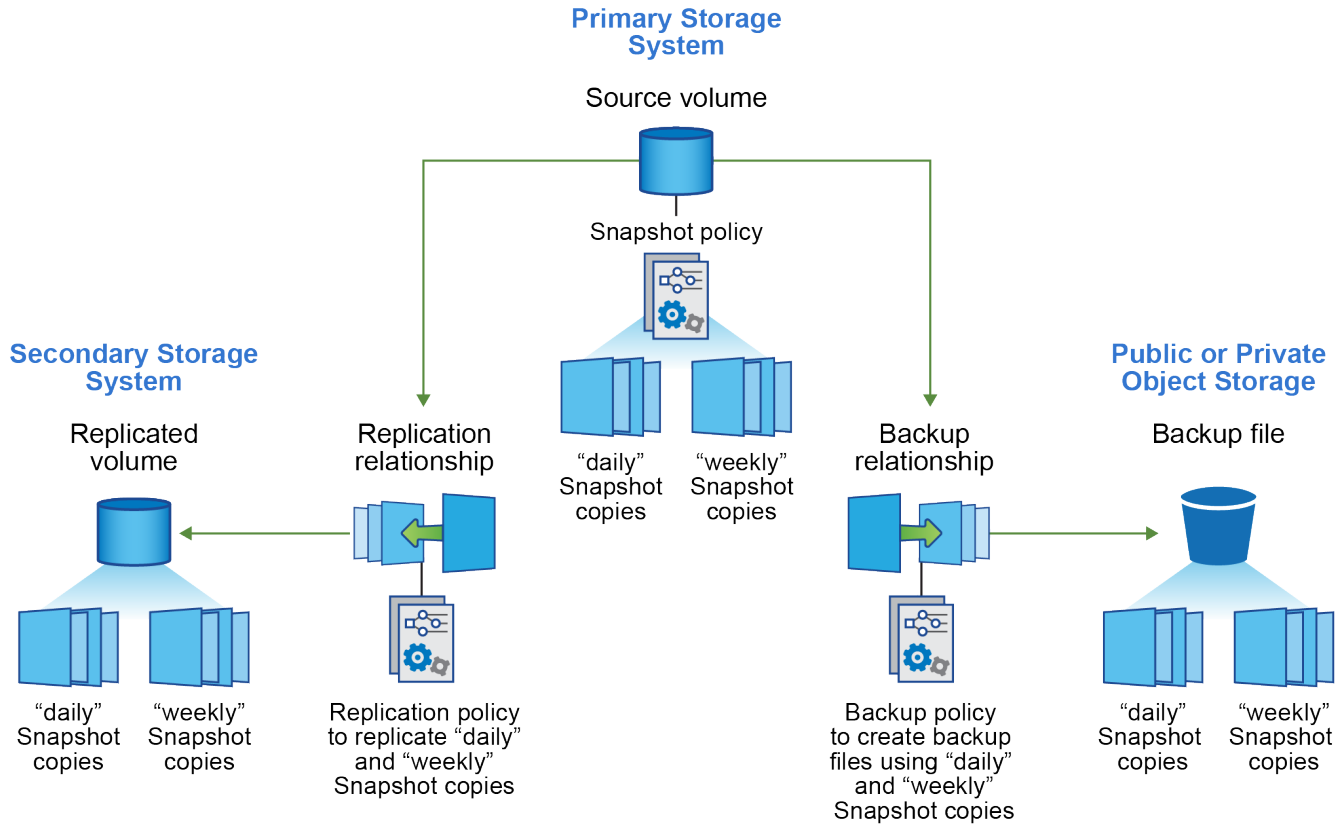
En plus de ces critères, le stockage cloud offre des options de sécurité supplémentaires si vous utilisez la fonctionnalité DataLock et Ransomware Resilience, ainsi que des économies de coûts supplémentaires en sélectionnant des classes de stockage d'archivage pour les fichiers de sauvegarde plus anciens. "En savoir plus sur la protection DataLock et Ransomware et les paramètres de stockage d'archives" .

Type de sauvegarde	Vitesse de sauvegarde	Coût de sauvegarde	Restaurer la vitesse	Coût de restauration
Instantané	Élevée	Faible (espace disque)	Élevée	Faible
Réplication	Moyen	Moyen (espace disque)	Moyen	Moyen (réseau)
Sauvegarde dans le cloud	Faible	Bas (espace objet)	Faible	Élevé (frais du fournisseur)

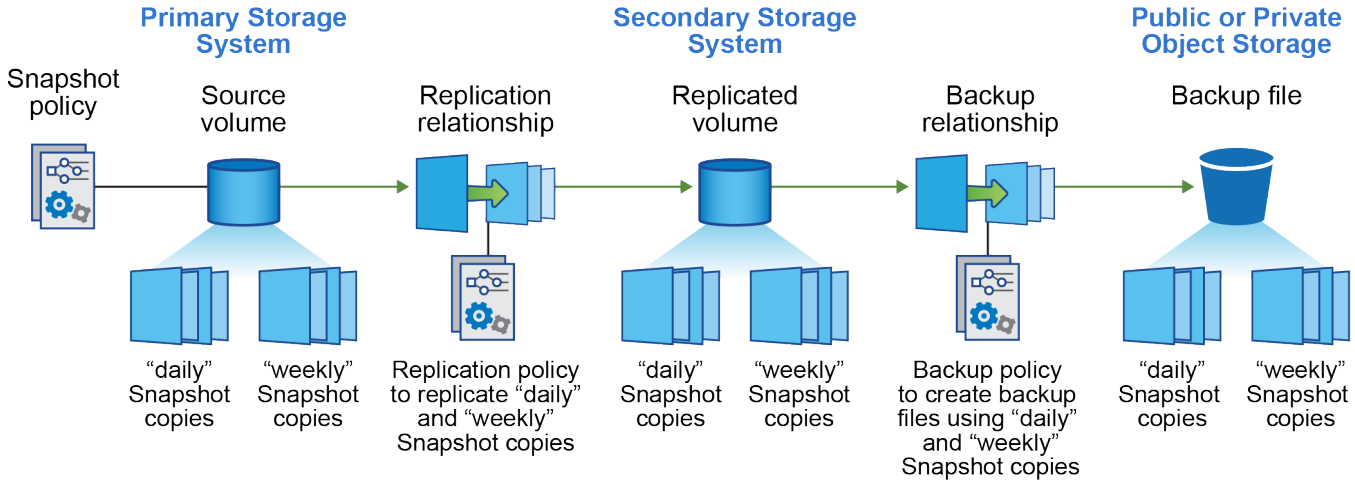
Quelle architecture de sauvegarde utiliserez-vous

Lors de la création de volumes répliqués et de fichiers de sauvegarde, vous pouvez choisir une architecture en éventail ou en cascade pour sauvegarder vos volumes.

Une architecture **en éventail** transfère l'instantané indépendamment vers le système de stockage de destination et l'objet de sauvegarde dans le cloud.



Une architecture en cascade transfère d'abord l'instantané vers le système de stockage de destination, puis ce système transfère la copie vers l'objet de sauvegarde dans le cloud.



Comparaison des différents choix d'architecture

Ce tableau fournit une comparaison des architectures en éventail et en cascade.

Fan-out	Cascade
Faible impact sur les performances du système source car il envoie des instantanés à 2 systèmes distincts	L'impact sur les performances du système de stockage source est moindre car l'instantané n'est envoyé qu'une seule fois.

Fan-out	Cascade
Plus facile à configurer car toutes les politiques, la mise en réseau et les configurations ONTAP sont effectuées sur le système source	Nécessite également que certaines configurations réseau et ONTAP soient effectuées à partir du système secondaire.

Utiliserez-vous les politiques par défaut pour les instantanés, les réplications et les sauvegardes ?

Vous pouvez utiliser les politiques par défaut fournies par NetApp pour créer vos sauvegardes, ou vous pouvez créer des politiques personnalisées. Lorsque vous utilisez l'assistant d'activation pour activer le service de sauvegarde et de récupération pour vos volumes, vous pouvez sélectionner parmi les stratégies par défaut et toutes les autres stratégies déjà existantes dans le système (Cloud Volumes ONTAP ou système ONTAP sur site). Si vous souhaitez utiliser une politique différente de celles existantes, vous pouvez créer la politique avant de démarrer ou pendant l'utilisation de l'assistant d'activation.

- La politique de capture d'instantanés par défaut crée des instantanés horaires, quotidiens et hebdomadaires, en conservant 6 instantanés horaires, 2 quotidiens et 2 hebdomadaires.
- La politique de réplication par défaut réplique les instantanés quotidiens et hebdomadaires, en conservant 7 instantanés quotidiens et 52 instantanés hebdomadaires.
- La politique de sauvegarde par défaut réplique les instantanés quotidiens et hebdomadaires, en conservant 7 instantanés quotidiens et 52 instantanés hebdomadaires.

Si vous créez des stratégies personnalisées pour la réplication ou la sauvegarde, les étiquettes de stratégie (par exemple, « quotidienne » ou « hebdomadaire ») doivent correspondre aux étiquettes qui existent dans vos stratégies de snapshot, sinon les volumes répliqués et les fichiers de sauvegarde ne seront pas créés.

Vous pouvez créer des stratégies de snapshot, de réplication et de sauvegarde vers des stockages d'objets dans l'interface utilisateur de NetApp Backup and Recovery . Voir la section pour"ajout d'une nouvelle politique de sauvegarde" pour plus de détails.

En plus d'utiliser NetApp Backup and Recovery pour créer des politiques personnalisées, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP (CLI) :

- "Créer une stratégie de capture instantanée à l'aide de System Manager ou de l'interface de ligne de commande ONTAP"
- "Créer une politique de réplication à l'aide de System Manager ou de l'interface de ligne de commande ONTAP"

Remarque : lorsque vous utilisez le Gestionnaire système, sélectionnez **Asynchrone** comme type de politique pour les politiques de réplication, et sélectionnez **Asynchrone** et **Sauvegarder dans le cloud** pour les politiques de sauvegarde vers les objets.

Voici quelques exemples de commandes CLI ONTAP qui pourraient être utiles si vous créez des politiques personnalisées. Notez que vous devez utiliser le vserver *admin* (VM de stockage) comme `<vserver_name>` dans ces commandes.

Description de la politique	Commande
Politique d'instantané simple	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`

Description de la politique	Commande
Sauvegarde simple dans le cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Sauvegarde dans le cloud avec DataLock et protection contre les ransomwares	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
Sauvegarde dans le cloud avec classe de stockage d'archivage	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Réplication simple vers un autre système de stockage	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Seules les politiques de coffre-fort peuvent être utilisées pour la sauvegarde vers les relations cloud.

Où résident mes politiques?

Les politiques de sauvegarde résident à différents emplacements en fonction de l'architecture de sauvegarde que vous prévoyez d'utiliser : en éventail ou en cascade. Les politiques de réplication et les politiques de sauvegarde ne sont pas conçues de la même manière, car les réplications associent deux systèmes de stockage ONTAP et la sauvegarde vers un objet utilise un fournisseur de stockage comme destination.

- Les politiques de capture instantanée résident toujours sur le système de stockage principal.
- Les politiques de réplication résident toujours sur le système de stockage secondaire.
- Les politiques de sauvegarde sur objet sont créées sur le système où réside le volume source : il s'agit du cluster principal pour les configurations en éventail et du cluster secondaire pour les configurations en cascade.

Ces différences sont présentées dans le tableau.

Architecture	Politique d'instantané	Politique de réplication	Politique de sauvegarde
Déploiement en éventail	Primaire	Secondaire	Primaire
Cascade	Primaire	Secondaire	Secondaire

Ainsi, si vous envisagez de créer des politiques personnalisées lors de l'utilisation de l'architecture en cascade, vous devrez créer les politiques de réplication et de sauvegarde sur les objets sur le système

secondaire où les volumes répliqués seront créés. Si vous envisagez de créer des politiques personnalisées lors de l'utilisation de l'architecture en éventail, vous devrez créer les politiques de réplication sur le système secondaire où les volumes répliqués seront créés et sauvegarder les politiques d'objet sur le système principal.

Si vous utilisez les politiques par défaut qui existent sur tous les systèmes ONTAP , alors vous êtes prêt.

Voulez-vous créer votre propre conteneur de stockage d'objets

Lorsque vous créez des fichiers de sauvegarde dans le stockage d'objets pour un système, par défaut, le service de sauvegarde et de récupération crée le conteneur (bucket ou compte de stockage) pour les fichiers de sauvegarde dans le compte de stockage d'objets que vous avez configuré. Le bucket AWS ou GCP est nommé « netapp-backup-<uuid> » par défaut. Le compte de stockage Azure Blob est nommé « netappbackup<uuid> ».

Vous pouvez créer le conteneur vous-même dans le compte du fournisseur d'objets si vous souhaitez utiliser un certain préfixe ou attribuer des propriétés spéciales. Si vous souhaitez créer votre propre conteneur, vous devez le créer avant de démarrer l'assistant d'activation. NetApp Backup and Recovery peut utiliser n'importe quel bucket et partager des buckets. L'assistant d'activation de sauvegarde détectera automatiquement vos conteneurs provisionnés pour le compte et les informations d'identification sélectionnés afin que vous puissiez sélectionner celui que vous souhaitez utiliser.

Vous pouvez créer le bucket à partir de la console ou de votre fournisseur de cloud.

- "Créer des buckets Amazon S3 à partir de la console"
- "Créer des comptes de stockage Azure Blob à partir de la console"
- "Créer des buckets Google Cloud Storage à partir de la console"

Si vous prévoyez d'utiliser un préfixe de bucket différent de « netapp-backup-xxxxxx », vous devrez modifier les autorisations S3 pour le rôle IAM de l'agent de console.

Paramètres de bucket avancés

Si vous prévoyez de déplacer des fichiers de sauvegarde plus anciens vers un stockage d'archives, ou si vous prévoyez d'activer la protection DataLock et Ransomware pour verrouiller vos fichiers de sauvegarde et les analyser à la recherche d'éventuels ransomwares, vous devrez créer le conteneur avec certains paramètres de configuration :

- Le stockage d'archives sur vos propres buckets est actuellement pris en charge dans le stockage AWS S3 lorsque vous utilisez le logiciel ONTAP 9.10.1 ou une version ultérieure sur vos clusters. Par défaut, les sauvegardes démarrent dans la classe de stockage S3 *Standard*. Assurez-vous de créer le bucket avec les règles de cycle de vie appropriées :
  - Déplacez les objets de l'ensemble de la portée du bucket vers S3 *Standard-IA* après 30 jours.
  - Déplacez les objets avec la balise « smc_push_to_archive: true » vers *Glacier Flexible Retrieval* (anciennement S3 Glacier)
- La protection DataLock et Ransomware est prise en charge dans le stockage AWS lors de l'utilisation du logiciel ONTAP 9.11.1 ou supérieur sur vos clusters, et dans le stockage Azure lors de l'utilisation du logiciel ONTAP 9.12.1 ou supérieur.
  - Pour AWS, vous devez activer le verrouillage d'objet sur le bucket à l'aide d'une période de conservation de 30 jours.
  - Pour Azure, vous devez créer la classe de stockage avec prise en charge de l'immuabilité au niveau de la version.

Quel mode de déploiement de l'agent de console utilisez-vous ?

Si vous utilisez déjà la console pour gérer votre stockage, un agent de console a déjà été installé. Si vous prévoyez d'utiliser le même agent de console avec NetApp Backup and Recovery, vous êtes prêt. Si vous devez utiliser un autre agent de console, vous devrez l'installer avant de démarrer votre implémentation de sauvegarde et de récupération.

La NetApp Console propose plusieurs modes de déploiement qui vous permettent d'utiliser la console d'une manière qui répond à vos exigences commerciales et de sécurité. Le *mode standard* exploite la couche SaaS de la console pour fournir toutes les fonctionnalités, tandis que le *mode restreint* et le *mode privé* sont disponibles pour les organisations qui ont des restrictions de connectivité.

"En savoir plus sur les modes de déploiement de la NetApp Console".

Prise en charge des sites avec une connectivité Internet complète

Lorsque NetApp Backup and Recovery est utilisé sur un site doté d'une connectivité Internet complète (également appelé *mode standard* ou *mode SaaS*), vous pouvez créer des volumes répliqués sur n'importe quel système ONTAP ou Cloud Volumes ONTAP local géré par la console, et vous pouvez créer des fichiers de sauvegarde sur le stockage d'objets dans l'un des fournisseurs de cloud pris en charge. "Consultez la liste complète des destinations de sauvegarde prises en charge" .

Pour obtenir la liste des emplacements d'agent de console valides, reportez-vous à l'une des procédures de sauvegarde suivantes pour le fournisseur de cloud où vous prévoyez de créer des fichiers de sauvegarde. Il existe certaines restrictions selon lesquelles l'agent de console doit être installé manuellement sur une machine Linux ou déployé chez un fournisseur de cloud spécifique.

- "Sauvegarder les données Cloud Volumes ONTAP sur Amazon S3"
- "Sauvegarder les données Cloud Volumes ONTAP sur Azure Blob"
- "Sauvegarder les données Cloud Volumes ONTAP sur Google Cloud"
- "Sauvegarder les données ONTAP sur site sur Amazon S3"
- "Sauvegarder les données ONTAP locales sur Azure Blob"
- "Sauvegarder les données ONTAP sur site sur Google Cloud"
- "Sauvegarder les données ONTAP sur site sur StorageGRID"
- "Sauvegarder ONTAP sur site vers ONTAP S3"

Prise en charge des sites avec une connectivité Internet limitée

NetApp Backup and Recovery peut être utilisé sur un site avec une connectivité Internet limitée (également appelé *mode restreint*) pour sauvegarder les données de volume. Dans ce cas, vous devrez déployer l'agent de console dans la région cloud de destination.

- Vous pouvez sauvegarder des données à partir de systèmes ONTAP sur site ou de systèmes Cloud Volumes ONTAP installés dans les régions commerciales AWS sur Amazon S3. "Sauvegarder les données Cloud Volumes ONTAP sur Amazon S3" .
- Vous pouvez sauvegarder des données à partir de systèmes ONTAP locaux ou de systèmes Cloud Volumes ONTAP installés dans des régions commerciales Azure vers Azure Blob. "Sauvegarder les données Cloud Volumes ONTAP sur Azure Blob" .

Prise en charge des sites sans connexion Internet

NetApp Backup and Recovery peut être utilisé sur un site sans connexion Internet (également appelé *mode privé* ou *sites sombres*) pour sauvegarder les données de volume. Dans ce cas, vous devrez déployer l'agent de console sur un hôte Linux sur le même site.

> Le mode privé BlueXP (interface BlueXP héritée) est généralement utilisé avec des environnements locaux qui n'ont pas de connexion Internet et avec des régions cloud sécurisées, notamment AWS Secret Cloud, AWS Top Secret Cloud et Azure IL6. NetApp continue de prendre en charge ces environnements avec l'interface BlueXP héritée. Pour la documentation du mode privé dans l'ancienne interface BlueXP , reportez-vous à la "Documentation PDF pour le mode privé BlueXP" .

- Vous pouvez sauvegarder des données à partir de systèmes ONTAP locaux sur site vers des systèmes NetApp StorageGRID locaux. "Sauvegarder les données ONTAP sur site sur StorageGRID" .
- Vous pouvez sauvegarder des données à partir de systèmes ONTAP locaux sur site vers des systèmes ONTAP locaux sur site ou des systèmes Cloud Volumes ONTAP configurés pour le stockage d'objets S3. "Sauvegarder les données ONTAP sur site sur ONTAP S3".

Gérez les politiques de sauvegarde pour les volumes ONTAP avec NetApp Backup and Recovery

Avec NetApp Backup and Recovery, utilisez les stratégies de sauvegarde par défaut fournies par NetApp pour créer vos sauvegardes ou créez des stratégies personnalisées. Les politiques régissent la fréquence de sauvegarde, l'heure à laquelle la sauvegarde est effectuée et le nombre de fichiers de sauvegarde conservés.

> Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Lorsque vous utilisez l'assistant d'activation pour activer le service de sauvegarde et de récupération pour vos volumes, vous pouvez sélectionner parmi les stratégies par défaut et toutes les autres stratégies déjà existantes dans le système (Cloud Volumes ONTAP ou système ONTAP sur site). Si vous souhaitez utiliser une politique différente de celles existantes, vous pouvez créer la politique avant ou pendant que vous utilisez l'assistant d'activation.

Pour en savoir plus sur les politiques de sauvegarde par défaut fournies, reportez-vous à"Planifiez votre voyage de protection" .

NetApp Backup and Recovery fournit trois types de sauvegardes de données ONTAP : les snapshots, les réplications et les sauvegardes sur le stockage d'objets. Leurs politiques résident à différents emplacements en fonction de l'architecture que vous utilisez et du type de sauvegarde :

Architecture	Emplacement de stockage de la politique d'instantané	Emplacement de stockage de la politique de réplication	Sauvegarde vers l'emplacement de stockage de la stratégie d'objet
Déploiement en éventail	Primaire	Secondaire	Primaire
Cascade	Primaire	Secondaire	Secondaire

Créez des politiques de sauvegarde à l'aide des outils suivants en fonction de votre environnement, de vos

préférences et du type de protection :

- UI de la NetApp Console
- Interface utilisateur du gestionnaire de système
- Interface de ligne de commande ONTAP

Lorsque vous utilisez le Gestionnaire système, sélectionnez **Asynchrone** comme type de politique pour les politiques de réplication et sélectionnez **Asynchrone** et **Sauvegarder dans le cloud** pour les politiques de sauvegarde vers les objets.

Afficher les politiques d'un système

1. Dans l'interface utilisateur de la console, sélectionnez **Volumes** > **Paramètres de sauvegarde**.
2. Depuis la page Paramètres de sauvegarde, sélectionnez le système, sélectionnez **Actions*** ••• **icône et sélectionnez *Gestion des politiques**.

   La page de gestion des politiques apparaît. Les stratégies de capture instantanée sont affichées par défaut.

3. Pour afficher les autres politiques existantes dans le système, sélectionnez **Politiques de réplication** ou **Politiques de sauvegarde**. Si les politiques existantes peuvent être utilisées pour vos plans de sauvegarde, vous êtes prêt. Si vous avez besoin d'une politique avec des caractéristiques différentes, vous pouvez créer de nouvelles politiques à partir de cette page.

Créer des politiques

Vous pouvez créer des politiques qui régissent vos instantanés, vos réplications et vos sauvegardes sur le stockage objet :

- Créer une politique de snapshot avant de lancer le snapshot
- Créer une politique de réplication avant de lancer la réplication
- Créez une politique de sauvegarde sur stockage d'objets avant de lancer la sauvegarde

Créer une politique de snapshot avant de lancer le snapshot

Une partie de votre stratégie 3-2-1 consiste à créer un instantané du volume sur le système de stockage **principal**.

Une partie du processus de création de politique implique l'identification des étiquettes d'instantané et de SnapMirror qui indiquent la planification et la conservation. Vous pouvez utiliser des étiquettes prédéfinies ou créer les vôtres.

Étapes

1. Dans l'interface utilisateur de la console, sélectionnez **Volumes** > **Paramètres de sauvegarde**.
2. Depuis la page Paramètres de sauvegarde, sélectionnez le système, sélectionnez **Actions*** ••• **icône et sélectionnez *Gestion des politiques**.

   La page de gestion des politiques apparaît.

3. Dans la page Politiques, sélectionnez **Créer une politique** > **Créer une politique d'instantané**.
4. Spécifiez le nom de la politique.

5. Sélectionnez le ou les programmes d'instantanés. Vous pouvez avoir un maximum de 5 étiquettes. Ou créez un planning.
6. Si vous choisissez de créer un planning :
   a. Sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle.
   b. Spécifiez les étiquettes d'instantané indiquant la planification et la conservation.
   c. Saisissez quand et à quelle fréquence l'instantané sera pris.
   d. Conservation : saisissez le nombre d'instantanés à conserver.
7. Sélectionnez **Créer**.

Exemple de politique d'instantané utilisant une architecture en cascade

Cet exemple crée une politique de snapshot avec deux clusters :

1. Groupe 1 :
   a. Sélectionnez le cluster 1 sur la page de politique.
   b. Ignorez les sections de stratégie de réplication et de sauvegarde vers un objet.
   c. Créez la politique de capture instantanée.
2. Groupe 2 :
   a. Sélectionnez le cluster 2 sur la page Politique.
   b. Ignorez la section de la politique d'instantané.
   c. Configurez les stratégies de réplication et de sauvegarde des objets.

Créer une politique de réplication avant de lancer la réplication

Votre stratégie 3-2-1 peut inclure la réplication d'un volume sur un système de stockage différent. La politique de réplication réside sur le système de stockage **secondaire**.

Étapes

1. Dans la page Politiques, sélectionnez **Créer une politique** > **Créer une politique de réplication**.
2. Dans la section Détails de la politique, spécifiez le nom de la politique.
3. Spécifiez les étiquettes SnapMirror (maximum 5) indiquant la rétention pour chaque étiquette.
4. Spécifiez le calendrier de transfert.
5. Sélectionnez **Créer**.

Créez une politique de sauvegarde sur stockage d'objets avant de lancer la sauvegarde

Votre stratégie 3-2-1 peut inclure la sauvegarde d'un volume sur un stockage d'objets.

Cette politique de stockage réside dans différents emplacements du système de stockage en fonction de l'architecture de sauvegarde :

- Fan-out : système de stockage principal
- Cascade : système de stockage secondaire

Étapes

1. Dans la page Gestion des politiques, sélectionnez **Créer une politique** > **Créer une politique de**

sauvegarde.

2. Dans la section Détails de la politique, spécifiez le nom de la politique.
3. Spécifiez les étiquettes SnapMirror (maximum 5) indiquant la rétention pour chaque étiquette.
4. Spécifiez les paramètres, y compris la planification du transfert et le moment d'archivage des sauvegardes.
5. (Facultatif) Pour déplacer les anciens fichiers de sauvegarde vers une classe de stockage ou un niveau d'accès moins coûteux après un certain nombre de jours, sélectionnez l'option **Archiver** et indiquez le nombre de jours qui doivent s'écouler avant que les données ne soient archivées. Entrez **0** comme « Archiver après jours » pour envoyer votre fichier de sauvegarde directement vers le stockage d'archivage.

   "En savoir plus sur les paramètres de stockage d'archives".

6. (Facultatif) Pour protéger vos sauvegardes contre toute modification ou suppression, sélectionnez l'option **Protection DataLock et Ransomware**.

   Si votre cluster utilise ONTAP 9.11.1 ou une version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre la suppression en configurant *DataLock* et *Ransomware protection*.

   "En savoir plus sur les paramètres DataLock disponibles".

7. Sélectionnez **Créer**.

Modifier une politique

Vous pouvez modifier une stratégie de snapshot, de réplication ou de sauvegarde personnalisée.

La modification de la politique de sauvegarde affecte tous les volumes qui utilisent cette politique.

Étapes

1. Dans la page de gestion des politiques, sélectionnez la politique, sélectionnez les **Actions*** icône et sélectionnez ***Modifier la politique**.

   Le processus est le même pour les politiques de réplication et de sauvegarde.

2. Dans la page Modifier la politique, effectuez les modifications.
3. Sélectionnez **Enregistrer**.

Supprimer une politique

Vous pouvez supprimer des stratégies qui ne sont associées à aucun volume.

Si une politique est associée à un volume et que vous souhaitez supprimer la politique, vous devez d'abord supprimer la politique du volume.

Étapes

1. Dans la page de gestion des politiques, sélectionnez la politique, sélectionnez les **Actions*** icône et sélectionnez ***Supprimer la politique d'instantané**.
2. Sélectionnez **Supprimer**.

Trouver plus d'informations

Pour obtenir des instructions sur la création de stratégies à l'aide de System Manager ou de l'interface de ligne de commande ONTAP , consultez les éléments suivants :

"Créer une politique de capture instantanée à l'aide du Gestionnaire de système" "Créer une politique de snapshot à l'aide de l'interface de ligne de commande ONTAP" "Créer une politique de réplication à l'aide du Gestionnaire de système" "Créer une politique de réplication à l'aide de l'interface de ligne de commande ONTAP" "Créer une sauvegarde vers une stratégie de stockage d'objets à l'aide du Gestionnaire de système" "Créer une sauvegarde vers une stratégie de stockage d'objets à l'aide de l'interface de ligne de commande ONTAP"

Options de stratégie de sauvegarde sur objet dans NetApp Backup and Recovery

NetApp Backup and Recovery vous permet de créer des politiques de sauvegarde avec une variété de paramètres pour vos systèmes ONTAP et Cloud Volumes ONTAP sur site.

Ces paramètres de stratégie s'appliquent uniquement au stockage de sauvegarde sur objet. Aucun de ces paramètres n'affecte vos stratégies de capture instantanée ou de réplication.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Options de planification de sauvegarde

NetApp Backup and Recovery vous permet de créer plusieurs politiques de sauvegarde avec des planifications uniques pour chaque système (cluster). Vous pouvez attribuer différentes politiques de sauvegarde à des volumes ayant des objectifs de point de récupération (RPO) différents.

Chaque politique de sauvegarde fournit une section pour *Étiquettes et rétention* que vous pouvez appliquer à vos fichiers de sauvegarde. Notez que la stratégie de snapshot appliquée au volume doit être l'une des stratégies reconnues par NetApp Backup and Recovery, sinon les fichiers de sauvegarde ne seront pas créés.

Le planning comporte deux parties : l'étiquette et la valeur de rétention :

- L'**étiquette** définit la fréquence à laquelle un fichier de sauvegarde est créé (ou mis à jour) à partir du volume. Vous pouvez choisir parmi les types d'étiquettes suivants :
  - Vous pouvez choisir un délai, ou une combinaison de délais, **horaires**, **quotidiens**, **hebdomadaires**, **mensuels** et **annuels**.
  - Vous pouvez sélectionner l'une des politiques définies par le système qui fournissent une sauvegarde et une conservation pendant 3 mois, 1 an ou 7 ans.
  - Si vous avez créé des stratégies de protection de sauvegarde personnalisées sur le cluster à l'aide ONTAP System Manager ou de l'interface de ligne de commande ONTAP , vous pouvez sélectionner l'une de ces stratégies.
- La valeur **rétention** définit le nombre de fichiers de sauvegarde conservés pour chaque étiquette (période). Une fois que le nombre maximal de sauvegardes a été atteint dans une catégorie ou un intervalle, les sauvegardes les plus anciennes sont supprimées afin que vous disposiez toujours des sauvegardes les plus récentes. Cela vous permet également d'économiser des coûts de stockage, car les sauvegardes obsolètes ne continuent pas à occuper de l'espace dans le cloud.

Par exemple, supposons que vous créiez une politique de sauvegarde qui crée 7 sauvegardes

hebdomadaires et 12 sauvegardes **mensuelles** :

- chaque semaine et chaque mois, un fichier de sauvegarde est créé pour le volume
- à la 8e semaine, la première sauvegarde hebdomadaire est supprimée et la nouvelle sauvegarde hebdomadaire de la 8e semaine est ajoutée (en conservant un maximum de 7 sauvegardes hebdomadaires)
- au 13e mois, la première sauvegarde mensuelle est supprimée et la nouvelle sauvegarde mensuelle du 13e mois est ajoutée (en conservant un maximum de 12 sauvegardes mensuelles)

Les sauvegardes annuelles sont automatiquement supprimées du système source après avoir été transférées vers le stockage d'objets. Ce comportement par défaut peut être modifié dans la page Paramètres avancés du système.

Options de protection DataLock et Ransomware

NetApp Backup and Recovery prend en charge la protection DataLock et Ransomware pour vos sauvegardes de volumes. Ces fonctionnalités vous permettent de verrouiller vos fichiers de sauvegarde et de les analyser pour détecter d'éventuels ransomwares sur les fichiers de sauvegarde. Il s'agit d'un paramètre facultatif que vous pouvez définir dans vos politiques de sauvegarde lorsque vous souhaitez une protection supplémentaire pour vos sauvegardes de volume pour un cluster.

Ces deux fonctionnalités protègent vos fichiers de sauvegarde afin que vous disposiez toujours d'un fichier de sauvegarde valide pour récupérer des données en cas de tentative d'attaque par ransomware sur vos sauvegardes. Il est également utile de répondre à certaines exigences réglementaires selon lesquelles les sauvegardes doivent être verrouillées et conservées pendant une certaine période. Lorsque l'option DataLock et Ransomware Resilience est activée, le verrouillage et le contrôle de version des objets seront activés pour le bucket cloud provisionné dans le cadre de l'activation de NetApp Backup and Recovery .

Cette fonctionnalité ne fournit pas de protection pour vos volumes sources ; uniquement pour les sauvegardes de ces volumes sources. Utilisez certains des "protections anti-ransomware fournies par ONTAP" pour protéger vos volumes sources.

- Si vous prévoyez d'utiliser la protection DataLock et Ransomware, vous pouvez l'activer lors de la création de votre première politique de sauvegarde et de l'activation de NetApp Backup and Recovery pour ce cluster. Vous pouvez ultérieurement activer ou désactiver l'analyse des ransomwares à l'aide des paramètres avancés de NetApp Backup and Recovery .
- Lorsque la console analyse un fichier de sauvegarde à la recherche de ransomware lors de la restauration des données du volume, vous encourez des frais de sortie supplémentaires auprès de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Qu'est-ce que DataLock

Grâce à cette fonctionnalité, vous pouvez verrouiller les instantanés cloud répliqués via SnapMirror sur le cloud et également activer la fonctionnalité permettant de détecter une attaque de ransomware et de récupérer une copie cohérente de l'instantané sur le stockage d'objets. Cette fonctionnalité est prise en charge sur AWS, Azure, Google Cloud Platform et StorageGRID.

DataLock protège vos fichiers de sauvegarde contre toute modification ou suppression pendant une certaine période de temps - également appelée *stockage immuable*. Cette fonctionnalité utilise la technologie du fournisseur de stockage d'objets pour le « verrouillage d'objets ».

Les fournisseurs de cloud utilisent une date de conservation jusqu'à (RUD), qui est calculée en fonction de la

période de conservation des instantanés. La période de conservation des instantanés est calculée en fonction de l'étiquette et du nombre de conservations définis dans la politique de sauvegarde.

La période minimale de conservation des instantanés est de 30 jours. Voyons quelques exemples de la façon dont cela fonctionne :

- Si vous choisissez l'étiquette **Quotidien** avec un nombre de rétention de 20, la période de rétention des instantanés est de 20 jours, la valeur par défaut étant le minimum de 30 jours.
- Si vous choisissez l'étiquette **Hebdomadaire** avec un nombre de rétention de 4, la période de rétention des instantanés est de 28 jours, la valeur par défaut étant le minimum de 30 jours.
- Si vous choisissez l'étiquette **Mensuel** avec le nombre de rétention 3, la période de rétention des instantanés est de 90 jours.
- Si vous choisissez l'étiquette **Annuel** avec le nombre de rétention 1, la période de rétention des instantanés est de 365 jours.

Qu'est-ce que la date de conservation jusqu'à (RUD) et comment est-elle calculée ?

La date de conservation jusqu'à (RUD) est déterminée en fonction de la période de conservation des instantanés. La date de conservation jusqu'à est calculée en additionnant la période de conservation des instantanés et une mémoire tampon.

- Le tampon correspond au tampon pour le temps de transfert (3 jours) + le tampon pour l'optimisation des coûts (28 jours), ce qui donne un total de 31 jours.
- La date de conservation minimale est de 30 jours + 31 jours de tampon = 61 jours.

Voici quelques exemples :

- Si vous créez une planification de sauvegarde mensuelle avec 12 rétentions, vos sauvegardes sont verrouillées pendant 12 mois (plus 31 jours) avant d'être supprimées (remplacées par le fichier de sauvegarde suivant).
- Si vous créez une politique de sauvegarde qui crée 30 sauvegardes quotidiennes, 7 sauvegardes hebdomadaires et 12 sauvegardes mensuelles, il existe trois périodes de conservation verrouillées :
  - Les sauvegardes « 30 journées quotidiennes » sont conservées pendant 61 jours (30 jours plus 31 jours de mémoire tampon),
  - Les sauvegardes « 7 semaines » sont conservées pendant 11 semaines (7 semaines plus 31 jours), et
  - Les sauvegardes « 12 mensuelles » sont conservées pendant 12 mois (plus 31 jours).
- Si vous créez une planification de sauvegarde horaire avec 24 rétentions, vous pourriez penser que les sauvegardes sont verrouillées pendant 24 heures. Cependant, comme cela est inférieur au minimum de 30 jours, chaque sauvegarde sera verrouillée et conservée pendant 61 jours (30 jours plus 31 jours de mémoire tampon).

> Les anciennes sauvegardes sont supprimées après l'expiration de la période de conservation de DataLock, et non après la période de conservation de la politique de sauvegarde.

Le paramètre de conservation DataLock remplace le paramètre de conservation de la politique de votre politique de sauvegarde. Cela pourrait affecter vos coûts de stockage, car vos fichiers de sauvegarde seront enregistrés dans le magasin d'objets pendant une période plus longue.

Activer DataLock et la protection contre les ransomwares

Vous pouvez activer la protection DataLock et Ransomware lorsque vous créez une politique. Vous ne pouvez pas activer, modifier ou désactiver cette option une fois la politique créée.

1. Lorsque vous créez une politique, développez la section **DataLock et résilience aux ransomwares**.
2. Choisissez l'une des options suivantes :
   - **Aucun** : la protection DataLock et la résilience aux ransomwares sont désactivées.
   - **Déverrouillé** : la protection DataLock et la résilience aux ransomwares sont activées. Les utilisateurs disposant d'autorisations spécifiques peuvent écraser ou supprimer les fichiers de sauvegarde protégés pendant la période de conservation.
   - **Verrouillé** : la protection DataLock et la résilience aux ransomwares sont activées. Aucun utilisateur ne peut écraser ou supprimer les fichiers de sauvegarde protégés pendant la période de conservation. Cela satisfait pleinement à la conformité réglementaire.

Se référer à"Comment mettre à jour les options de protection contre les ransomwares dans la page Paramètres avancés" .

Qu'est-ce que la protection contre les ransomwares

La protection contre les ransomwares analyse vos fichiers de sauvegarde pour rechercher des preuves d'une attaque de ransomware. La détection des attaques de ransomware est effectuée à l'aide d'une comparaison de somme de contrôle. Si un ransomware potentiel est identifié dans un nouveau fichier de sauvegarde par rapport au fichier de sauvegarde précédent, ce nouveau fichier de sauvegarde est remplacé par le fichier de sauvegarde le plus récent qui ne présente aucun signe d'attaque de ransomware. (Le fichier identifié comme ayant subi une attaque de ransomware est supprimé 1 jour après avoir été remplacé.)

Les analyses se produisent dans ces situations :

- Les analyses sur les objets de sauvegarde cloud sont lancées peu de temps après leur transfert vers le stockage d'objets cloud. L'analyse n'est pas effectuée sur le fichier de sauvegarde lors de sa première écriture sur le stockage cloud, mais lors de l'écriture du fichier de sauvegarde suivant.
- Les analyses de ransomware peuvent être lancées lorsque la sauvegarde est sélectionnée pour le processus de restauration.
- Les analyses peuvent être effectuées à la demande à tout moment.

Comment fonctionne le processus de récupération ?

Lorsqu'une attaque de ransomware est détectée, le service utilise l'API REST Integrity Checker de l'agent Active Data Console pour démarrer le processus de récupération. La version la plus ancienne des objets de données est la source de vérité et est transformée en version actuelle dans le cadre du processus de récupération.

Voyons comment cela fonctionne :

- En cas d'attaque de ransomware, le service tente d'écraser ou de supprimer l'objet dans le bucket.
- Étant donné que le stockage cloud est compatible avec le contrôle de version, il crée automatiquement une nouvelle version de l'objet de sauvegarde. Si un objet est supprimé avec le contrôle de version activé, il est marqué comme supprimé mais peut toujours être récupéré. Si un objet est écrasé, les versions précédentes sont stockées et marquées.
- Lorsqu'une analyse de ransomware est lancée, les sommes de contrôle sont validées pour les deux versions d'objet et comparées. Si les sommes de contrôle sont incohérentes, un ransomware potentiel a

été détecté.

- Le processus de récupération implique de revenir à la dernière bonne copie connue.

Systèmes pris en charge et fournisseurs de stockage d'objets

Vous pouvez activer la protection DataLock et Ransomware sur les volumes ONTAP des systèmes suivants lorsque vous utilisez le stockage d'objets dans les fournisseurs de cloud public et privé suivants.

Système source	Destination du fichier de sauvegarde
Cloud Volumes ONTAP dans AWS	Amazon S3
Cloud Volumes ONTAP dans Azure	Azure Blob
Cloud Volumes ONTAP dans Google Cloud	Google Cloud
Système ONTAP sur site	Amazon S3, Azure Blob, Google Cloud , NetApp StorageGRID

Exigences

- Pour AWS :
  - Vos clusters doivent exécuter ONTAP 9.11.1 ou supérieur
  - L'agent de console peut être déployé dans le cloud ou dans vos locaux
  - Les autorisations S3 suivantes doivent faire partie du rôle IAM qui fournit des autorisations à l'agent de console. Ils résident dans la section « backupS3Policy » pour la ressource « arn:aws:s3:::netapp-backup-* » :

Autorisations AWS S3

- s3 : Obtenir le balisage de la version de l'objet
- s3 : GetBucketObjectLockConfiguration
- s3 : ObtenirObjectVersionAcl
- s3 : Mettre en place un balisage d'objet
- s3:Supprimer l'objet
- s3 : Supprimer le balisage d'objet
- s3 : Obtenir la rétention d'objet
- s3 : Supprimer le balisage de version d'objet
- s3:PutObject
- s3:Obtenir l'objet
- s3 : PutBucketObjectLockConfiguration
- s3 : Obtenir la configuration du cycle de vie
- s3 : Obtenir le balisage du bucket
- s3 : Supprimer la version de l'objet
- s3 : ListBucketVersions
- s3:ListBucket
- s3 : Mettre en place le balisage du bucket
- s3 : Obtenir le balisage des objets
- s3 : PutBucketVersioning
- s3 : Mettre en place la version de l'objet
- s3 : Obtenir la gestion des versions du bucket
- s3 : Obtenir l'Acl du bucket
- s3 : Contournement de la gouvernance et de la rétention
- s3 : PutObjectRetention
- s3 : Obtenir l'emplacement du bucket
- s3 : Obtenir la version de l'objet

"Affichez le format JSON complet de la politique où vous pouvez copier et coller les autorisations requises".

- Pour Azure :
  - Vos clusters doivent exécuter ONTAP 9.12.1 ou supérieur
  - L'agent de console peut être déployé dans le cloud ou dans vos locaux
- Pour Google Cloud :
  - Vos clusters doivent exécuter ONTAP 9.17.1 ou une version ultérieure
  - L'agent de console peut être déployé dans le cloud ou dans vos locaux
- Pour StorageGRID:

- Vos clusters doivent exécuter ONTAP 9.11.1 ou supérieur
- Vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou supérieure
- L'agent Console doit être déployé dans vos locaux (il peut être installé sur un site avec ou sans accès Internet)
- Les autorisations S3 suivantes doivent faire partie du rôle IAM qui fournit des autorisations à l'agent de console :

Autorisations StorageGRID S3

- s3 : Obtenir le balisage de la version de l'objet
- s3 : GetBucketObjectLockConfiguration
- s3 : ObtenirObjectVersionAcl
- s3 : Mettre en place un balisage d'objet
- s3:Supprimer l'objet
- s3 : Supprimer le balisage d'objet
- s3 : Obtenir la rétention d'objet
- s3 : Supprimer le balisage de version d'objet
- s3:PutObject
- s3:Obtenir l'objet
- s3 : PutBucketObjectLockConfiguration
- s3 : Obtenir la configuration du cycle de vie
- s3 : Obtenir le balisage du bucket
- s3 : Supprimer la version de l'objet
- s3 : ListBucketVersions
- s3:ListBucket
- s3 : Mettre en place le balisage du bucket
- s3 : Obtenir le balisage des objets
- s3 : PutBucketVersioning
- s3 : Mettre en place la version de l'objet
- s3 : Obtenir la gestion des versions du bucket
- s3 : Obtenir l'Acl du bucket
- s3 : PutObjectRetention
- s3 : Obtenir l'emplacement du bucket
- s3 : Obtenir la version de l'objet

Restrictions

- La fonctionnalité de protection DataLock et Ransomware n'est pas disponible si vous avez configuré le stockage d'archives dans la politique de sauvegarde.
- L'option DataLock que vous sélectionnez lors de l'activation de NetApp Backup and Recovery doit être

utilisée pour toutes les stratégies de sauvegarde de ce cluster.

- Vous ne pouvez pas utiliser plusieurs modes DataLock sur un seul cluster.
- Si vous activez DataLock, toutes les sauvegardes de volumes seront verrouillées. Vous ne pouvez pas mélanger des sauvegardes de volumes verrouillés et non verrouillés pour un même cluster.
- La protection DataLock et Ransomware est applicable aux nouvelles sauvegardes de volume à l'aide d'une politique de sauvegarde avec la protection DataLock et Ransomware activée. Vous pouvez ultérieurement activer ou désactiver ces fonctionnalités à l'aide de l'option Paramètres avancés.
- Les volumes FlexGroup peuvent utiliser la protection DataLock et Ransomware uniquement lors de l'utilisation ONTAP 9.13.1 ou supérieur.

Conseils pour réduire les coûts de DataLock

Vous pouvez activer ou désactiver la fonction Ransomware Scan tout en gardant la fonction DataLock active. Pour éviter des frais supplémentaires, vous pouvez désactiver les analyses de ransomware programmées. Cela vous permet de personnaliser vos paramètres de sécurité et d'éviter d'engager des frais auprès du fournisseur de cloud.

Même si les analyses de ransomware programmées sont désactivées, vous pouvez toujours effectuer des analyses à la demande en cas de besoin.

Vous pouvez choisir différents niveaux de protection :

- **DataLock *sans* analyses de ransomware** : fournit une protection pour les données de sauvegarde dans le stockage de destination qui peut être en mode Gouvernance ou Conformité.
  - **Mode de gouvernance** : offre aux administrateurs la possibilité d'écraser ou de supprimer les données protégées.
  - **Mode de conformité** : Offre une indélébilité complète jusqu'à l'expiration de la période de conservation. Cela permet de répondre aux exigences de sécurité des données les plus strictes des environnements hautement réglementés. Les données ne peuvent pas être écrasées ou modifiées au cours de leur cycle de vie, offrant ainsi le niveau de protection le plus élevé pour vos copies de sauvegarde.

    Microsoft Azure utilise plutôt un mode de verrouillage et de déverrouillage.

- **DataLock *avec* analyses de ransomware** : Fournit une couche de sécurité supplémentaire pour vos données. Cette fonctionnalité permet de détecter toute tentative de modification des copies de sauvegarde. Si une tentative est faite, une nouvelle version des données est créée discrètement. La fréquence d'analyse peut être modifiée sur 1, 2, 3, 4, 5, 6 ou 7 jours. Si les analyses sont programmées tous les 7 jours, les coûts diminuent considérablement.

Pour plus de conseils pour atténuer les coûts de DataLock, consultezhttps://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475[]

De plus, vous pouvez obtenir des estimations du coût associé à DataLock en visitant le "Calculateur du coût total de possession (TCO) de NetApp Backup and Recovery" .

Options de stockage d'archives

Lorsque vous utilisez le stockage cloud AWS, Azure ou Google, vous pouvez déplacer les anciens fichiers de sauvegarde vers une classe de stockage d'archivage ou un niveau d'accès moins coûteux après un certain nombre de jours. Vous pouvez également choisir d'envoyer immédiatement vos fichiers de sauvegarde vers un

stockage d'archives sans les écrire sur un stockage cloud standard. Entrez simplement **0** comme « Archiver après jours » pour envoyer votre fichier de sauvegarde directement vers le stockage d'archivage. Cela peut être particulièrement utile pour les utilisateurs qui ont rarement besoin d'accéder aux données des sauvegardes cloud ou pour les utilisateurs qui remplacent une solution de sauvegarde sur bande.

Les données des niveaux d'archivage ne sont pas immédiatement accessibles en cas de besoin et nécessiteront un coût de récupération plus élevé. Vous devrez donc prendre en compte la fréquence à laquelle vous devrez peut-être restaurer les données à partir de fichiers de sauvegarde avant de décider d'archiver vos fichiers de sauvegarde.

- Même si vous sélectionnez « 0 » pour envoyer tous les blocs de données vers le stockage cloud d'archivage, les blocs de métadonnées sont toujours écrits dans le stockage cloud standard.
- Le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.
- Vous ne pouvez pas modifier la politique d'archivage après avoir sélectionné **0** jour (archiver immédiatement).

Chaque politique de sauvegarde fournit une section pour la *Politique d'archivage* que vous pouvez appliquer à vos fichiers de sauvegarde.

- Dans AWS, les sauvegardes démarrent dans la classe de stockage *Standard* et passent à la classe de stockage *Standard-Infrequent Access* après 30 jours.

  Si votre cluster utilise ONTAP 9.10.1 ou une version ultérieure, vous pouvez hiérarchiser les sauvegardes plus anciennes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive*. "En savoir plus sur le stockage d'archives AWS" .

  - Si vous ne sélectionnez aucun niveau d'archivage dans votre première politique de sauvegarde lors de l'activation de NetApp Backup and Recovery, *S3 Glacier* sera votre seule option d'archivage pour les politiques futures.
  - Si vous sélectionnez *S3 Glacier* dans votre première politique de sauvegarde, vous pouvez alors passer au niveau *S3 Glacier Deep Archive* pour les futures politiques de sauvegarde de ce cluster.
  - Si vous sélectionnez *S3 Glacier Deep Archive* dans votre première politique de sauvegarde, ce niveau sera le seul niveau d'archivage disponible pour les futures politiques de sauvegarde pour ce cluster.
- Dans Azure, les sauvegardes sont associées au niveau d'accès *Cool*.

  Si votre cluster utilise ONTAP 9.10.1 ou une version ultérieure, vous pouvez hiérarchiser les sauvegardes plus anciennes vers le stockage *Azure Archive*. "En savoir plus sur le stockage d'archives Azure" .
- Dans GCP, les sauvegardes sont associées à la classe de stockage *Standard*.

  Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers le stockage *Archive* dans l'interface utilisateur NetApp Backup and Recovery après un certain nombre de jours pour une optimisation supplémentaire des coûts. "En savoir plus sur le stockage d'archives Google" .
- Dans StorageGRID, les sauvegardes sont associées à la classe de stockage *Standard*.

  Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure et que votre système StorageGRID utilise 11.4 ou une version ultérieure, vous pouvez archiver les anciens fichiers de sauvegarde dans un stockage d'archivage cloud public.

- Pour AWS, vous pouvez hiérarchiser les sauvegardes vers le stockage AWS *S3 Glacier* ou *S3 Glacier Deep Archive*. "En savoir plus sur le stockage d'archives AWS".
- Pour Azure, vous pouvez hiérarchiser les anciennes sauvegardes vers le stockage *Azure Archive*. "En savoir plus sur le stockage d'archives Azure".

Gérer les options de stockage de sauvegarde vers objet dans les paramètres avancés de NetApp Backup and Recovery

Vous pouvez modifier les paramètres de stockage de sauvegarde sur objet au niveau du cluster que vous définissez lors de l'activation de NetApp Backup and Recovery pour chaque système ONTAP à l'aide de la page Paramètres avancés. Vous pouvez également modifier certains paramètres appliqués comme paramètres de sauvegarde « par défaut ». Cela inclut la modification du taux de transfert des sauvegardes vers le stockage objet, l'exportation des instantanés historiques en tant que fichiers de sauvegarde et l'activation ou la désactivation des analyses de ransomware pour un système.

Ces paramètres sont disponibles uniquement pour le stockage de sauvegarde sur objet. Aucun de ces paramètres n'affecte vos paramètres de snapshot ou de réplication.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Vous pouvez modifier les options suivantes dans la page Paramètres avancés :

- Modifier les clés de stockage qui autorisent votre système ONTAP à accéder au stockage d'objets
- Modification de l'espace IP ONTAP connecté au stockage d'objets
- Modification de la bande passante réseau allouée au chargement des sauvegardes vers le stockage d'objets à l'aide de l'option Taux de transfert maximal
- Modification de la façon dont les instantanés historiques sont exportés ou non en tant que fichiers de sauvegarde et inclus dans vos fichiers de sauvegarde de référence initiaux pour les volumes futurs
- Modifier si les instantanés « annuels » sont supprimés du système source
- Activation ou désactivation des analyses de ransomware pour un système, y compris les analyses planifiées

Afficher les paramètres de sauvegarde au niveau du cluster

Vous pouvez consulter les paramètres système au niveau du cluster et les paramètres du fournisseur pour chaque système.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
3. Depuis la page *Paramètres de sauvegarde*, sélectionnez ••• pour le système et sélectionnez **Configurer les paramètres avancés > Paramètres système** pour afficher les paramètres système et **Configurer les paramètres avancés > Paramètres du fournisseur** pour afficher les paramètres du fournisseur.

La page qui s'affiche présente les paramètres actuels de ce système. Lorsque vous consultez les paramètres du fournisseur, les paramètres affichés concernent le compartiment que vous sélectionnez en haut de la page.

Notez que certaines options ne sont pas disponibles en fonction de la version d' ONTAP sur le cluster source et du fournisseur de cloud de destination où se trouvent les sauvegardes.

Modifier la bande passante réseau disponible pour télécharger des sauvegardes vers le stockage d'objets

Lorsque vous activez NetApp Backup and Recovery pour un système, par défaut, ONTAP peut utiliser une quantité illimitée de bande passante pour transférer les données de sauvegarde des volumes du système vers le stockage d'objets. Si vous remarquez que le trafic de sauvegarde affecte les charges de travail normales des utilisateurs, vous pouvez limiter la quantité de bande passante réseau utilisée pendant le transfert à l'aide de l'option Taux de transfert maximal dans la page Paramètres avancés.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur ••• pour le système, sélectionnez **Configurer les paramètres avancés > Paramètres système**.
3. Dans la page Paramètres avancés, développez la section **Taux de transfert maximal**.
4. Choisissez une valeur comprise entre 1 et 1 000 Mbps comme débit de transfert maximal.
5. Sélectionnez le bouton radio **Limité** et entrez la bande passante maximale pouvant être utilisée, ou sélectionnez **Illimité** pour indiquer qu'il n'y a pas de limite.
6. Sélectionnez **Appliquer**.

Ce paramètre n'affecte pas la bande passante allouée à d'autres relations de réplication pouvant être configurées pour les volumes du système.

Modifiez si les instantanés historiques sont exportés en tant que fichiers de sauvegarde

S'il existe des instantanés locaux pour les volumes qui correspondent à l'étiquette de planification de sauvegarde que vous utilisez dans ce système (par exemple, quotidien, hebdomadaire, etc.), vous pouvez exporter ces instantanés historiques vers le stockage d'objets en tant que fichiers de sauvegarde. Cela vous permet d'initialiser vos sauvegardes dans le cloud en déplaçant les anciens instantanés dans la copie de sauvegarde de base.

Notez que cette option s'applique uniquement aux nouveaux fichiers de sauvegarde pour les nouveaux volumes de lecture/écriture et qu'elle n'est pas prise en charge avec les volumes de protection des données (DP).

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur ••• pour le système, sélectionnez **Configurer les paramètres avancés > Paramètres système**.
3. Dans la page Paramètres avancés, développez la section **Exporter les copies d'instantanés existantes**.
4. Indiquez si vous souhaitez exporter les instantanés existants.
5. Sélectionnez **Appliquer**.

Modifier si les instantanés « annuels » sont supprimés du système source

Lorsque vous sélectionnez l'étiquette de sauvegarde « annuelle » pour une stratégie de sauvegarde de l'un de vos volumes, l'instantané créé est très volumineux. Par défaut, ces instantanés annuels sont supprimés automatiquement du système source après avoir été transférés vers le stockage d'objets. Vous pouvez modifier ce comportement par défaut à partir de la section Suppression des instantanés annuels.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur ••• pour le système, sélectionnez **Configurer les paramètres avancés > Paramètres système**.
3. Dans la page Paramètres avancés, développez la section **Suppression des instantanés annuels**.
4. Sélectionnez **Désactivé** pour conserver les instantanés annuels sur le système source.
5. Sélectionnez **Appliquer**.

Activer ou désactiver les analyses de ransomware

Les analyses de protection contre les ransomwares sont activées par défaut. Le paramètre par défaut pour la fréquence d'analyse est de 7 jours. L'analyse s'effectue uniquement sur le dernier instantané.

Pour plus de détails sur les options DataLock et Ransomware Resilience, reportez-vous à"Options de résilience DataLock et Ransomware" .

Vous pouvez modifier ce calendrier en jours ou en semaines ou le désactiver, ce qui permet de réduire les coûts.

L'activation des analyses de ransomware entraînera des frais supplémentaires en fonction du fournisseur de cloud.

Si les analyses de ransomware planifiées sont désactivées, vous pouvez toujours effectuer des analyses à la demande et l'analyse pendant une opération de restauration se produira toujours.

Se référer à"Gérer les politiques" pour plus de détails sur la gestion des politiques qui mettent en œuvre la détection des ransomwares.

Activer ou désactiver les analyses de ransomware pour un système

Vous pouvez activer ou désactiver les analyses de ransomware pour un cluster.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur ••• pour le système, sélectionnez **Configurer les paramètres avancés > Paramètres système**.
3. Sur la page qui s'affiche, développez la section **Analyse des logiciels de ransomware**.
4. Activer ou désactiver **l'analyse Ransomware**.
5. Sélectionnez **Analyse de ransomware programmée**.
6. Vous pouvez également modifier l'analyse par défaut hebdomadaire en jours ou en semaines.
7. Définissez la fréquence en jours ou en semaines à laquelle l'analyse doit être exécutée.
8. Sélectionnez **Appliquer**.

Activer ou désactiver les analyses de ransomware pour un fournisseur

Vous pouvez activer ou désactiver les analyses de ransomware au niveau du fournisseur via la page des paramètres du fournisseur. Les paramètres affichés sur cette page concernent le compartiment que vous sélectionnez en haut de la page.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur ••• pour le système et sélectionnez **Configurer les paramètres avancés > Paramètres du fournisseur**.
3. En haut de la page qui s'affiche, sélectionnez le compartiment dont vous souhaitez modifier les paramètres.
4. Développez la section **Analyse des logiciels de ransomware**.
5. Activer ou désactiver **l'analyse Ransomware**.
6. Sélectionnez **Analyse de ransomware programmée**.
7. Vous pouvez également modifier l'analyse par défaut hebdomadaire en jours ou en semaines.
8. Définissez la fréquence en jours ou en semaines à laquelle l'analyse doit être exécutée.
9. Sélectionnez **Appliquer**.

Sauvegardez les données Cloud Volumes ONTAP sur Amazon S3 avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP sur Amazon S3.

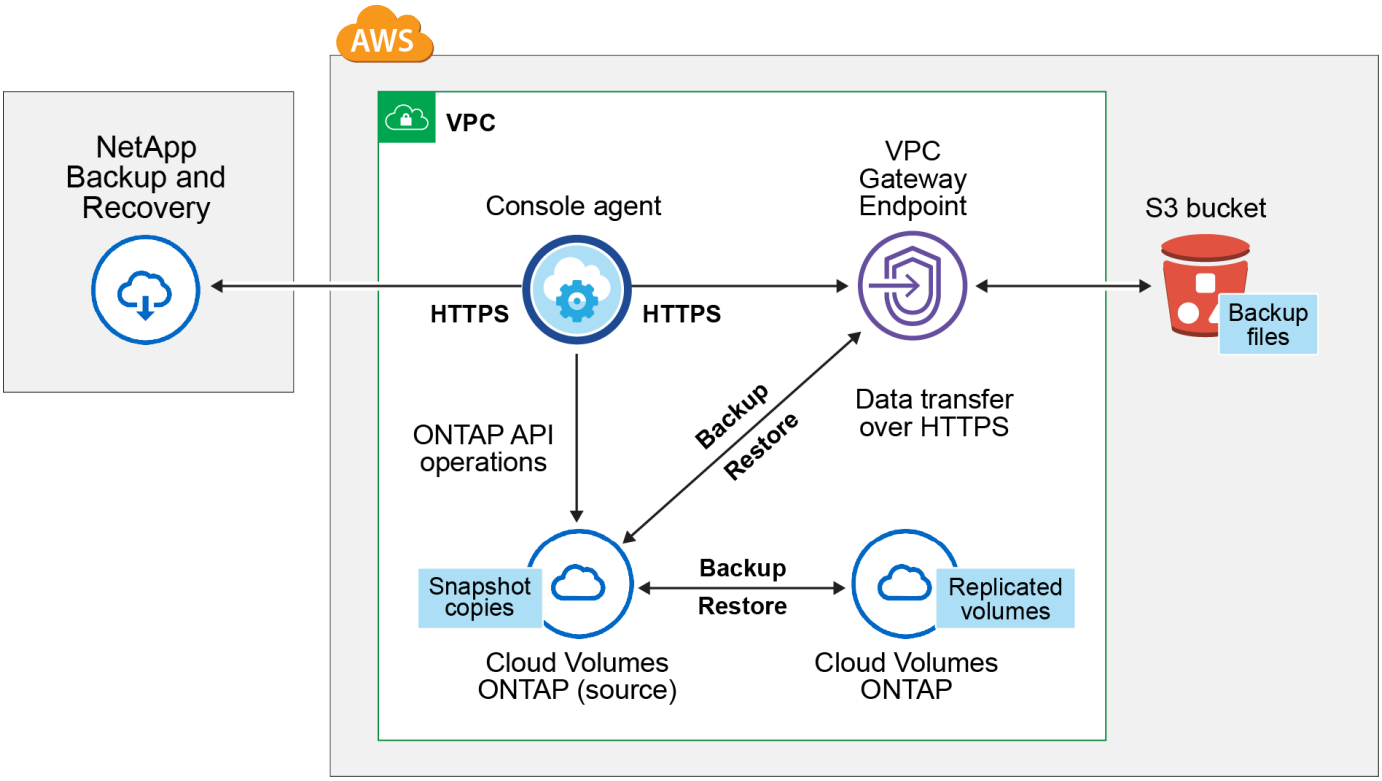
Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Vérifiez la prise en charge de votre configuration

Lisez les exigences suivantes pour vous assurer que vous disposez d'une configuration prise en charge avant de commencer à sauvegarder des volumes sur S3.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux.

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.



Le point de terminaison de la passerelle VPC doit déjà exister dans votre VPC. "En savoir plus sur les points de terminaison de passerelle" .

Versions ONTAP prises en charge

Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.

Informations requises pour l'utilisation de clés gérées par le client pour le chiffrement des données

Vous pouvez choisir vos propres clés gérées par le client pour le chiffrement des données dans l'assistant d'activation au lieu d'utiliser les clés de chiffrement Amazon S3 par défaut. Dans ce cas, vous devrez déjà avoir configuré les clés de gestion du cryptage. "Découvrez comment utiliser vos propres clés" .

Vérifier les exigences de licence

Pour les licences NetApp Backup and Recovery PAYGO, un abonnement Console est disponible sur AWS Marketplace qui permet les déploiements de Cloud Volumes ONTAP et NetApp Backup and Recovery. Vous devez "abonnez-vous à cet abonnement NetApp Console" avant d'activer NetApp Backup and Recovery. La facturation de NetApp Backup and Recovery s'effectue via cet abonnement.

Pour un contrat annuel qui vous permet de sauvegarder à la fois les données Cloud Volumes ONTAP et les données ONTAP sur site, vous devez vous abonner à partir du "Page AWS Marketplace" et puis "associer l'abonnement à vos informations d'identification AWS" .

Pour un contrat annuel qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery, vous devez configurer le contrat annuel lorsque vous créez un système Cloud Volumes ONTAP . Cette option ne vous permet pas de sauvegarder les données sur site.

Pour les licences BYOL de NetApp Backup and Recovery , vous avez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" . Vous devez utiliser une licence BYOL lorsque l'agent de console et le système Cloud Volumes ONTAP sont déployés sur un site sombre.

Et vous devez disposer d'un compte AWS pour l'espace de stockage où seront situées vos sauvegardes.

Préparez votre agent de console

L'agent de console doit être installé dans une région AWS avec un accès Internet complet ou limité (mode « standard » ou « restreint »). "Consultez les modes de déploiement de la NetApp Console pour plus de détails." .

- "En savoir plus sur les agents de console"
- "Déployer un agent de console dans AWS en mode standard (accès Internet complet)"
- "Installer l'agent de console en mode restreint (accès sortant limité)"

Vérifier ou ajouter des autorisations à l'agent de la console

Le rôle IAM qui fournit des autorisations à la console doit inclure les autorisations S3 de la dernière version. "Politique de la console" . Si la politique ne contient pas toutes ces autorisations, consultez le "Documentation AWS : Modification des politiques IAM" .

Voici les autorisations spécifiques de la politique :

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",
```

```
            "glue:CreateTable",
            "glue:CreateDatabase",
            "glue:GetPartitions",
            "glue:BatchCreatePartition",
            "glue:BatchDeletePartition"
        ],
        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ]
    }
```

Lors de la création de sauvegardes dans les régions AWS Chine, vous devez modifier le nom de ressource AWS « arn » sous toutes les sections *Resource* dans les politiques IAM de « aws » à « aws-cn » ; par exemple `arn:aws-cn:s3:::netapp-backup-*` .

Autorisations AWS Cloud Volumes ONTAP requises

Lorsque votre système Cloud Volumes ONTAP exécute le logiciel ONTAP 9.12.1 ou une version ultérieure, le rôle IAM qui fournit à ce système des autorisations doit inclure un nouvel ensemble d'autorisations S3 spécifiquement pour NetApp Backup and Recovery à partir de la dernière version. "Politique Cloud Volumes ONTAP" .

Si vous avez créé le système Cloud Volumes ONTAP à l'aide de la version 3.9.23 ou supérieure de la console, ces autorisations doivent déjà faire partie du rôle IAM. Sinon, vous devrez ajouter les autorisations manquantes.

Régions AWS prises en charge

NetApp Backup and Recovery est pris en charge dans toutes les régions AWS, y compris les régions AWS GovCloud.

Configuration requise pour créer des sauvegardes dans un autre compte AWS

Par défaut, les sauvegardes sont créées à l'aide du même compte que celui utilisé pour votre système Cloud Volumes ONTAP . Si vous souhaitez utiliser un autre compte AWS pour vos sauvegardes, vous devez :

- Vérifiez que les autorisations « s3:PutBucketPolicy » et « s3:PutBucketOwnershipControls » font partie du rôle IAM qui fournit des autorisations à l'agent de la console.
- Ajoutez les informations d'identification du compte AWS de destination dans la console. "Découvrez comment procéder" .
- Ajoutez les autorisations suivantes dans les informations d'identification de l'utilisateur dans le deuxième compte :

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

Créez vos propres seaux

Par défaut, le service crée des buckets pour vous. Si vous souhaitez utiliser vos propres buckets, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces buckets dans l'assistant.

"En savoir plus sur la création de vos propres buckets".

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.
- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (il s'agit du paramètre par défaut).

Activer la NetApp Backup and Recovery sur Cloud Volumes ONTAP

L'activation de la NetApp Backup and Recovery est simple. Les étapes diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau.

Activer la NetApp Backup and Recovery sur un nouveau système

NetApp Backup and Recovery est activé par défaut dans l'assistant système. Assurez-vous de garder l'option activée.

Voir "Lancement de Cloud Volumes ONTAP dans AWS" pour connaître les exigences et les détails de création de votre système Cloud Volumes ONTAP .

Étapes

1. Depuis la page **Systèmes** de la console, sélectionnez **Ajouter un système**, choisissez le fournisseur de cloud et sélectionnez **Ajouter un nouveau**. Sélectionnez **Créer des Cloud Volumes ONTAP**.
2. Sélectionnez **Amazon Web Services** comme fournisseur de cloud, puis choisissez un nœud unique ou un système HA.
3. Remplissez la page Détails et informations d'identification.
4. Sur la page Services, laissez le service activé et sélectionnez **Continuer**.
5. Complétez les pages de l'assistant pour déployer le système.

Résultat

NetApp Backup and Recovery est activé sur le système. Après avoir créé des volumes sur ces systèmes Cloud Volumes ONTAP , lancez NetApp Backup and Recovery et"activer la sauvegarde sur chaque volume que vous souhaitez protéger" .

Activer la NetApp Backup and Recovery sur un système existant

Activez NetApp Backup and Recovery sur un système existant à tout moment directement depuis la console.

Étapes

1. Depuis la page **Systèmes** de la console, sélectionnez le cluster et sélectionnez **Activer** à côté de Sauvegarde et récupération dans le panneau de droite.

   Si la destination Amazon S3 pour vos sauvegardes existe en tant que cluster sur la page **Systèmes**, vous pouvez faire glisser le cluster sur le système Amazon S3 pour lancer l'assistant de configuration.

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez égalementAfficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes**

de sauvegarde à côté de Sauvegarde et récupération dans le panneau de droite.

Si la destination AWS de vos sauvegardes existe en tant que système sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets AWS.

- Sélectionnez **Volumes** dans la barre Sauvegarde et restauration. Dans l'onglet Volumes, sélectionnez **Actions** ••• Choisissez l'option icône et sélectionnez **Activer la protection 3-2-1** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde sur le stockage d'objets activée).

La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.
   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur stockage d'objets

- Architecture
- Politique d'instantané local
- Cible et politique de réplication

> Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : Sauvegarde les volumes sur un stockage objet. Lors de la sélection de compartiments existants ou de la configuration de nouveaux compartiments, vous pouvez sauvegarder des volumes dans un maximum de six compartiments par cluster.
2. **Architecture** : Si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les informations circulent du système de stockage principal vers le secondaire, et du secondaire vers le stockage d'objets.
   - **Fan out** : les informations circulent du système de stockage principal vers le secondaire *et* du système principal vers le stockage d'objets.

     Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

   > Pour créer une politique personnalisée avant d'activer l'instantané, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

   a. Entrez le nom de la politique.
   b. Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   c. Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : Sélectionnez le système de destination et la machine virtuelle de stockage. Vous pouvez également sélectionner le ou les agrégats de destination ainsi que le préfixe ou le suffixe qui sera ajouté au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une.

     > Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

i. Entrez le nom de la politique.

ii. Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.

iii. Sélectionnez **Créer**.

5. **Sauvegarde** : Définissez les options suivantes :

   - **Fournisseur** : Sélectionnez **Amazon Web Services**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région où les sauvegardes seront stockées.

     Saisissez le compte AWS utilisé pour stocker les sauvegardes. Il peut s'agir d'un compte différent de celui sur lequel réside le système Cloud Volumes ONTAP .

     Si vous souhaitez utiliser un autre compte AWS pour vos sauvegardes, vous devez ajouter les informations d'identification du compte AWS de destination dans la console et ajouter les autorisations « s3:PutBucketPolicy » et « s3:PutBucketOwnershipControls » au rôle IAM qui fournit des autorisations à la console.

     Sélectionnez la région où les sauvegardes seront stockées. Il peut s'agir d'une région différente de celle dans laquelle réside le système Cloud Volumes ONTAP .

     Créez un nouveau bucket ou sélectionnez-en un existant.

   - **Chiffrement** : Si vous avez créé un nouveau compartiment, saisissez les informations de clé de chiffrement fournies par le fournisseur. Choisissez si vous utiliserez les clés de chiffrement AWS par défaut ou si vous choisirez vos propres clés gérées par le client depuis votre compte AWS pour gérer le chiffrement de vos données. ("Découvrez comment utiliser vos propres clés de chiffrement").

     Si vous choisissez d'utiliser vos propres clés gérées par le client, saisissez le coffre-fort de clés et les informations sur la clé.

     Si vous avez choisi un bucket existant, les informations de chiffrement sont déjà disponibles, vous n'avez donc pas besoin de les saisir maintenant.

   - **Réseau** : Configurez les options réseau pour ce fournisseur.
   - **Politique de sauvegarde** : sélectionnez une politique de stockage de sauvegarde sur objet existante ou créez-en une.

     Pour créer une politique personnalisée avant d'activer la sauvegarde, reportez-vous à"Créer une politique" .

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

     i. Entrez le nom de la politique.

     ii. Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.

     iii. Pour les politiques de sauvegarde sur objet, définissez les paramètres DataLock et Ransomware Resilience. Pour plus de détails sur DataLock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .

     iv. Sélectionnez **Créer**.

- **Exporter l'instantané existant** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés sur le stockage objet en tant que fichiers de sauvegarde afin de garantir la protection la plus complète possible de vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **corriger automatiquement les étiquettes incorrectes sur les instantanés locaux, la réplication et la sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques d'instantané, de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage principal. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume de stockage principal.

Un compartiment S3 est créé dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés.

Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Sauvegardez les données Cloud Volumes ONTAP sur le stockage Azure Blob avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP vers le

stockage Azure Blob.

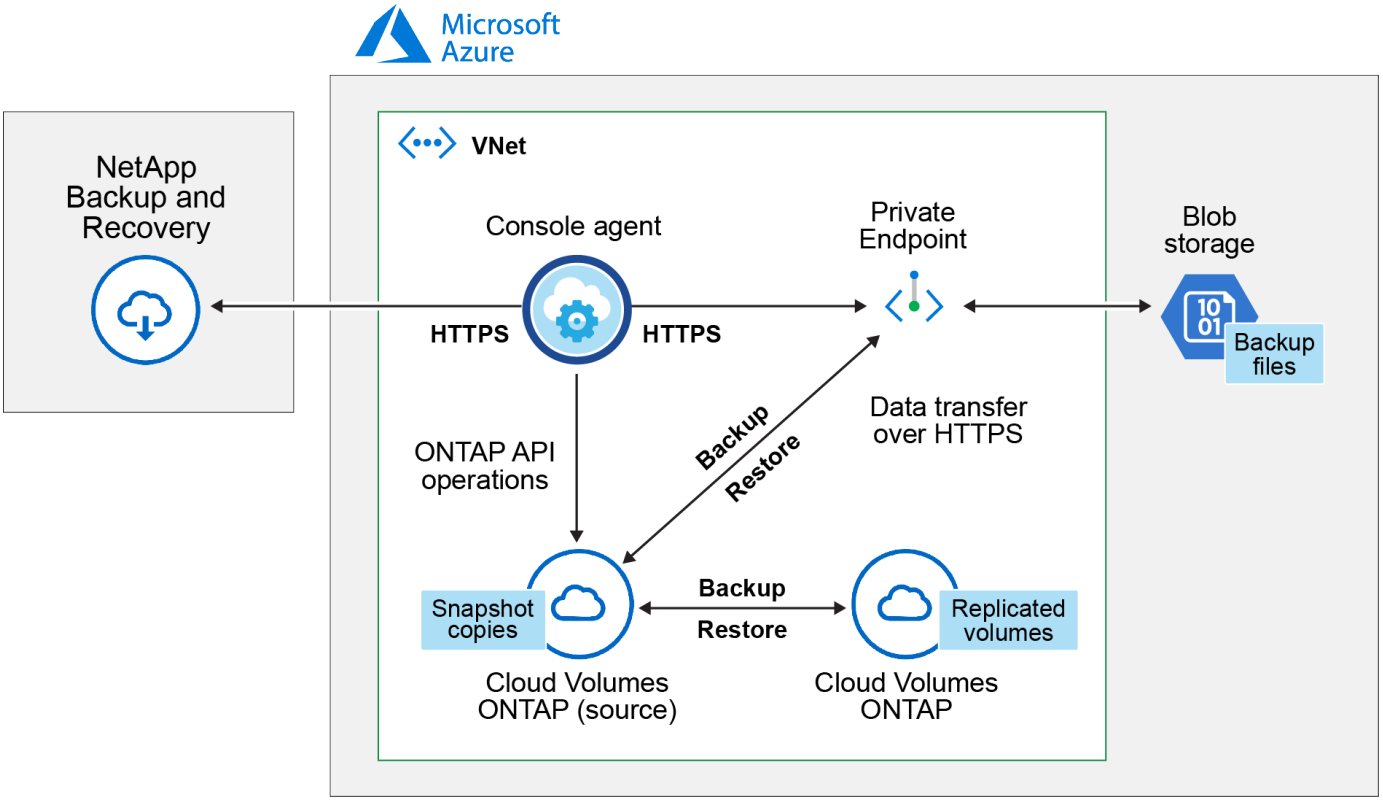
Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Vérifiez la prise en charge de votre configuration

Lisez les exigences suivantes pour vous assurer que vous disposez d'une configuration prise en charge avant de commencer à sauvegarder des volumes sur le stockage Blob Azure.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux.

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.



Versions ONTAP prises en charge

Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.

Régions Azure prises en charge

NetApp Backup and Recovery est pris en charge dans toutes les régions Azure, y compris les régions Azure Government.

Par défaut, NetApp Backup and Recovery provisionne le conteneur Blob avec une redondance locale (LRS) pour l'optimisation des coûts. Vous pouvez modifier ce paramètre sur Redondance de zone (ZRS) après l'activation de NetApp Backup and Recovery si vous souhaitez vous assurer que vos données sont répliquées entre différentes zones. Consultez les instructions de Microsoft pour "modifier la façon dont votre compte de stockage est répliqué" .

Configuration requise pour la création de sauvegardes dans un autre abonnement Azure

Par défaut, les sauvegardes sont créées à l'aide du même abonnement que celui utilisé pour votre système Cloud Volumes ONTAP .

Vérifier les exigences de licence

Pour les licences NetApp Backup and Recovery PAYGO, un abonnement via Azure Marketplace est requis avant d'activer NetApp Backup and Recovery. La facturation de NetApp Backup and Recovery s'effectue via cet abonnement. "Vous pouvez vous abonner à partir de la page Détails et informations d'identification de l'assistant système" .

Pour les licences BYOL de NetApp Backup and Recovery , vous avez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" . Vous devez utiliser une licence BYOL lorsque l'agent de console et le système Cloud Volumes ONTAP sont déployés sur un site sombre (« mode privé »).

Et vous devez disposer d'un abonnement Microsoft Azure pour l'espace de stockage où seront situées vos sauvegardes.

Préparez votre agent de console

L'agent de console peut être installé dans une région Azure avec un accès Internet complet ou limité (mode « standard » ou « restreint »). "Consultez les modes de déploiement de la NetApp Console pour plus de détails." .

- "En savoir plus sur les agents de console"
- "Déployer un agent de console dans Azure en mode standard (accès Internet complet)"
- "Installer l'agent de console en mode restreint (accès sortant limité)"

Vérifier ou ajouter des autorisations à l'agent de la console

Pour utiliser la fonctionnalité de recherche et de restauration de NetApp Backup and Recovery , vous devez disposer d'autorisations spécifiques dans le rôle de l'agent de console afin qu'il puisse accéder au compte Azure Synapse Workspace et Data Lake Storage. Consultez les autorisations ci-dessous et suivez les étapes si vous devez modifier la politique.

Avant de commencer

- Vous devez enregistrer le fournisseur de ressources Azure Synapse Analytics (appelé « Microsoft.Synapse ») avec votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement" . Vous devez être le **Propriétaire** ou le **Contributeur** de l'abonnement pour enregistrer le fournisseur de ressources.
- Le port 1433 doit être ouvert pour la communication entre l'agent de console et les services Azure Synapse SQL.

Étapes

1. Identifiez le rôle attribué à la machine virtuelle de l'agent de console :
   a. Dans le portail Azure, ouvrez le service de machines virtuelles.
   b. Sélectionnez la machine virtuelle de l'agent de console.
   c. Sous Paramètres, sélectionnez **Identité**.
   d. Sélectionnez **Attributions de rôles Azure**.

e. Prenez note du rôle personnalisé attribué à la machine virtuelle de l'agent de console.

2. Mettre à jour le rôle personnalisé :
   a. Dans le portail Azure, ouvrez votre abonnement Azure.
   b. Sélectionnez **Contrôle d'accès (IAM) > Rôles**.
   c. Sélectionnez les points de suspension (**…**) pour le rôle personnalisé, puis sélectionnez **Modifier**.
   d. Sélectionnez **JSON** et ajoutez les autorisations suivantes :

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Afficher le format JSON complet de la politique"

e. Sélectionnez **Réviser + mettre à jour**, puis sélectionnez **Mettre à jour**.

Informations requises pour l'utilisation de clés gérées par le client pour le chiffrement des données

Vous pouvez utiliser vos propres clés gérées par le client pour le chiffrement des données dans l'assistant d'activation au lieu d'utiliser les clés de chiffrement par défaut gérées par Microsoft. Dans ce cas, vous aurez besoin de l'abonnement Azure, du nom du coffre de clés et de la clé. "Découvrez comment utiliser vos propres clés" .

NetApp Backup and Recovery prend en charge les *stratégies d'accès Azure*, le modèle d'autorisation *contrôle d'accès basé sur les rôles Azure* (Azure RBAC) et le *modèle de sécurité matérielle géré* (HSM) (reportez-vous à "Qu'est-ce qu'Azure Key Vault Managed HSM ?").

Créez votre compte de stockage Azure Blob

Par défaut, le service crée des comptes de stockage pour vous. Si vous souhaitez utiliser vos propres comptes de stockage, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces comptes de stockage dans l'assistant.

"En savoir plus sur la création de vos propres comptes de stockage".

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.
- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (il s'agit du paramètre par défaut).

Activer la NetApp Backup and Recovery sur Cloud Volumes ONTAP

L'activation de la NetApp Backup and Recovery est simple. Les étapes diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau.

Activer la NetApp Backup and Recovery sur un nouveau système

NetApp Backup and Recovery est activé par défaut dans l'assistant système. Assurez-vous de garder l'option activée.

Voir "Lancement de Cloud Volumes ONTAP dans Azure" pour connaître les exigences et les détails de création de votre système Cloud Volumes ONTAP .

> Si vous souhaitez choisir le nom du groupe de ressources, **désactivez** NetApp Backup and Recovery lors du déploiement de Cloud Volumes ONTAP.

Étapes

1. Depuis la page **Systèmes** de la console, sélectionnez **Ajouter un système**, choisissez le fournisseur de cloud et sélectionnez **Ajouter un nouveau**. Sélectionnez **Créer des Cloud Volumes ONTAP**.
2. Sélectionnez **Microsoft Azure** comme fournisseur de cloud, puis choisissez un nœud unique ou un système HA.
3. Dans la page Définir les informations d'identification Azure, saisissez le nom des informations d'identification, l'ID client, la clé secrète client et l'ID du répertoire, puis sélectionnez **Continuer**.
4. Remplissez la page Détails et informations d'identification et assurez-vous qu'un abonnement Azure Marketplace est en place, puis sélectionnez **Continuer**.
5. Sur la page Services, laissez le service activé et sélectionnez **Continuer**.
6. Complétez les pages de l'assistant pour déployer le système.

Résultat

NetApp Backup and Recovery est activé sur le système. Après avoir créé des volumes sur ces systèmes Cloud Volumes ONTAP , lancez NetApp Backup and Recovery et"activer la sauvegarde sur chaque volume que vous souhaitez protéger" .

Activer la NetApp Backup and Recovery sur un système existant

Activez NetApp Backup and Recovery à tout moment directement depuis le système.

Étapes

1. Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer** à côté de Sauvegarde et récupération dans le panneau de droite.

   Si la destination Azure Blob pour vos sauvegardes existe en tant que système sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster sur le système Azure Blob pour lancer l'assistant de configuration.

2. Complétez les pages de l'assistant pour déployer NetApp Backup and Recovery.
3. Lorsque vous souhaitez lancer des sauvegardes, continuez avecActiver les sauvegardes sur vos volumes ONTAP .

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez égalementAfficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le

code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté de Sauvegarde et récupération dans le panneau de droite.

     Si la destination Azure de vos sauvegardes existe en tant que système sur la page **Systèmes**, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets Azure Blob.

   - Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez les **Actions*** ••• **icône et sélectionnez *Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.

   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol . (Les volumes FlexGroup ne peuvent être sélectionnés qu'un par un.) Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.

- Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : snapshots locaux, réplication et sauvegarde sur stockage d'objets
- Architecture
- Politique d'instantané local
- Cible et politique de réplication

> Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes sur le stockage d'objets.
2. **Architecture** : Si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les informations circulent du système de stockage principal vers le secondaire, et du secondaire vers le stockage d'objets.
   - **Fan out** : les informations circulent du système de stockage principal vers le secondaire *et* du système principal vers le stockage d'objets.

     Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une.

   > Pour créer une politique personnalisée avant d'activer l'instantané, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :

- **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.
- **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une.

  Pour créer une politique personnalisée avant d'activer la réplication, reportez-vous à"Créer une politique" .

  Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

  - Entrez le nom de la politique.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Microsoft Azure**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur.

     Entrez la région où les sauvegardes seront stockées. Il peut s'agir d'une région différente de celle dans laquelle réside le système Cloud Volumes ONTAP .

     Créez un nouveau compte de stockage ou sélectionnez-en un existant.

     Saisissez l'abonnement Azure utilisé pour stocker les sauvegardes. Il peut s'agir d'un abonnement différent de celui sur lequel réside le système Cloud Volumes ONTAP .

     Créez votre propre groupe de ressources qui gère le conteneur Blob ou sélectionnez le type de groupe de ressources et le groupe.

     Si vous souhaitez protéger vos fichiers de sauvegarde contre toute modification ou suppression, assurez-vous que le compte de stockage a été créé avec le stockage immuable activé à l'aide d'une période de conservation de 30 jours.

   - **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Azure, saisissez les informations de clé de chiffrement fournies par le fournisseur. Choisissez si vous utiliserez les clés de chiffrement Azure par défaut ou si vous choisirez vos propres clés gérées par le client à partir de votre compte Azure pour gérer le chiffrement de vos données.

     Si vous choisissez d'utiliser vos propres clés gérées par le client, saisissez le coffre-fort de clés et les informations sur la clé. "Apprenez à utiliser vos propres clés" .

     Si vous avez choisi un compte de stockage Microsoft existant, les informations de chiffrement sont déjà disponibles, vous n'avez donc pas besoin de les saisir maintenant.

   - **Réseau** : Choisissez l'espace IP et indiquez si vous utiliserez un point de terminaison privé. Le point de terminaison privé est désactivé par défaut.
     i. L'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
     ii. Vous pouvez également choisir si vous utiliserez un point de terminaison privé Azure que vous avez précédemment configuré. "En savoir plus sur l'utilisation d'un point de terminaison privé Azure" .

- **Politique de sauvegarde** : sélectionnez une politique de stockage de sauvegarde sur objet existante.

  Pour créer une politique personnalisée avant d'activer la sauvegarde, reportez-vous à"Créer une politique" .

  Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

  - Entrez le nom de la politique.
  - Pour les politiques de sauvegarde sur objet, définissez les paramètres DataLock et Ransomware Resilience. Pour plus de détails sur DataLock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

- **Exporter les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage principal. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume principal.

Un conteneur de stockage Blob est créé dans le groupe de ressources que vous avez entré et les fichiers de sauvegarde y sont stockés.

Par défaut, NetApp Backup and Recovery provisionne le conteneur Blob avec une redondance locale (LRS) pour l'optimisation des coûts. Vous pouvez modifier ce paramètre en Redondance de zone (ZRS) si vous souhaitez vous assurer que vos données sont répliquées entre différentes zones. Consultez les instructions de Microsoft pour "modifier la façon dont votre compte de stockage est répliqué" .

Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Quelle est la prochaine étape ?

- Tu peux"gérez vos fichiers de sauvegarde et vos politiques de sauvegarde" . Cela inclut le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification de sauvegarde, et bien plus encore.
- Tu peux"gérer les paramètres de sauvegarde au niveau du cluster" . Cela inclut la modification des clés de stockage ONTAP utilise pour accéder au stockage cloud, la modification de la bande passante réseau disponible pour télécharger des sauvegardes vers le stockage d'objets, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.
- Vous pouvez également"restaurer des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" vers un système Cloud Volumes ONTAP dans AWS ou vers un système ONTAP sur site.

Sauvegardez les données Cloud Volumes ONTAP sur Google Cloud Storage avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP vers Google Cloud Storage.

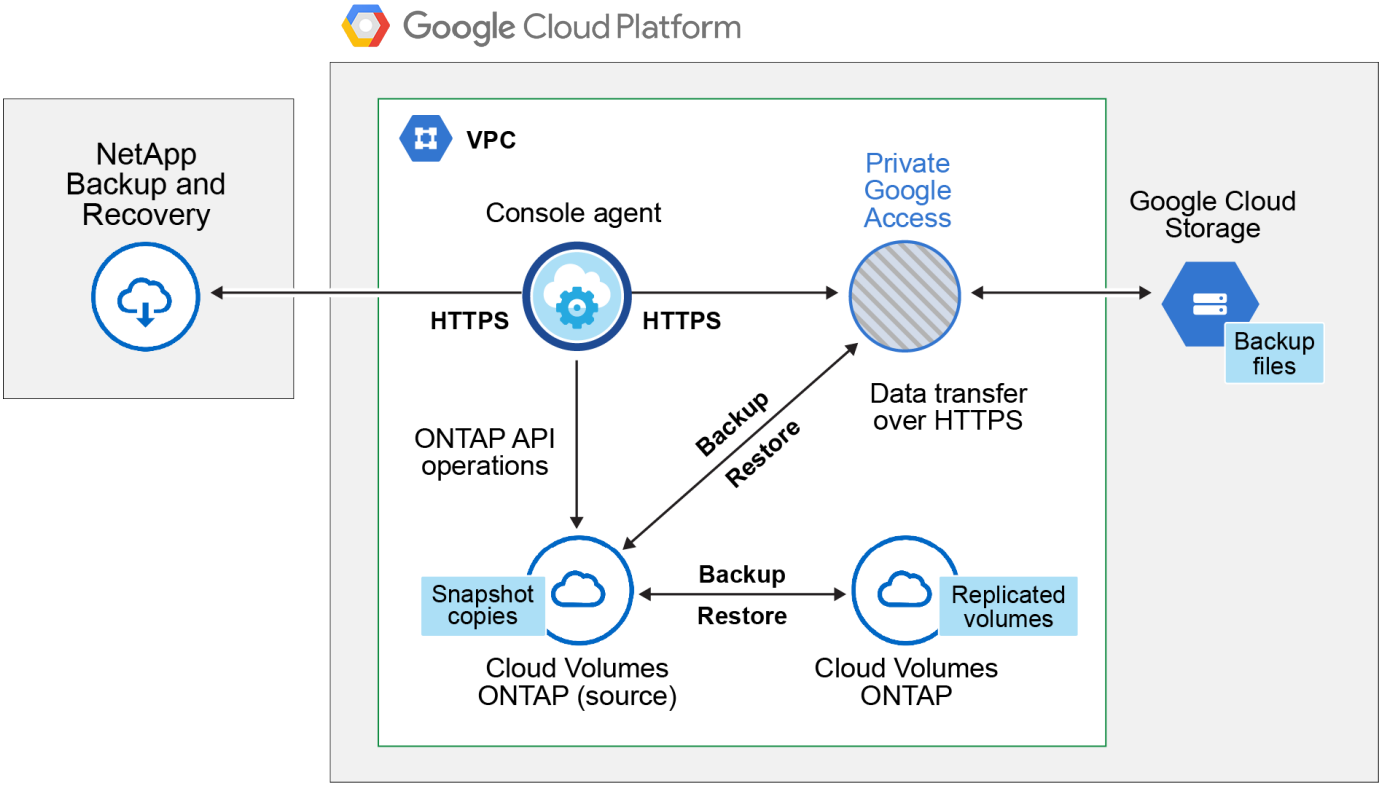
Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Vérifiez la prise en charge de votre configuration

Lisez les exigences suivantes pour vous assurer que vous disposez d'une configuration prise en charge avant de commencer à sauvegarder des volumes sur Google Cloud Storage.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux.

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.



Versions ONTAP prises en charge

Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.

Régions GCP prises en charge

NetApp Backup and Recovery est pris en charge dans toutes les régions GCP.

Compte de service GCP

Vous devez disposer d'un compte de service dans votre projet Google Cloud doté du rôle personnalisé. "Apprenez à créer un compte de service" .

Le rôle d'administrateur de stockage n'est plus requis pour le compte de service qui permet à NetApp Backup and Recovery d'accéder aux buckets Google Cloud Storage.

Vérifier les exigences de licence

Pour les licences NetApp Backup and Recovery PAYGO, un abonnement Console est disponible sur Google Marketplace qui permet les déploiements de Cloud Volumes ONTAP et NetApp Backup and Recovery. Vous devez "abonnez-vous à cet abonnement Console" avant d'activer NetApp Backup and Recovery. La facturation de NetApp Backup and Recovery s'effectue via cet abonnement. "Vous pouvez vous abonner à partir de la page Détails et informations d'identification de l'assistant système" .

Pour les licences BYOL de NetApp Backup and Recovery , vous avez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .

Et vous devez disposer d'un abonnement Google pour l'espace de stockage où seront situées vos sauvegardes.

Préparez votre agent de console

L'agent de console doit être installé dans une région Google avec accès Internet.

- "En savoir plus sur les agents de console"
- "Déployer un agent de console dans Google Cloud"

Vérifier ou ajouter des autorisations à l'agent de la console

Pour utiliser la fonctionnalité « Recherche et restauration » de NetApp Backup and Recovery , vous devez disposer d'autorisations spécifiques dans le rôle de l'agent de console afin qu'il puisse accéder au service Google Cloud BigQuery. Consultez les autorisations ci-dessous et suivez les étapes si vous devez modifier la politique.

Étapes

1. Dans le "Console Google Cloud" , allez à la page **Rôles**.
2. À l'aide de la liste déroulante en haut de la page, sélectionnez le projet ou l'organisation qui contient le rôle que vous souhaitez modifier.
3. Sélectionnez un rôle personnalisé.
4. Sélectionnez **Modifier le rôle** pour mettre à jour les autorisations du rôle.
5. Sélectionnez **Ajouter des autorisations** pour ajouter les nouvelles autorisations suivantes au rôle.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Sélectionnez **Mettre à jour** pour enregistrer le rôle modifié.

Informations requises pour l'utilisation des clés de chiffrement gérées par le client (CMEK)

Vous pouvez utiliser vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés de chiffrement par défaut gérées par Google. Les clés inter-régions et inter-projets sont prises en charge, vous pouvez donc choisir un projet pour un bucket différent du projet de la clé CMEK. Si vous prévoyez d'utiliser vos propres clés gérées par le client :

- Vous aurez besoin du trousseau de clés et du nom de la clé pour pouvoir ajouter ces informations dans l'assistant d'activation. "En savoir plus sur les clés de chiffrement gérées par le client" .
- Vous devrez vérifier que ces autorisations requises sont incluses dans le rôle de l'agent de console :

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Vous devrez vérifier que l'API Google « Cloud Key Management Service (KMS) » est activée dans votre projet. Voir le "Documentation Google Cloud : Activation des API" pour plus de détails.

Considérations CMEK :

- Les clés HSM (protégées par le matériel) et les clés générées par logiciel sont prises en charge.
- Les clés Cloud KMS nouvellement créées ou importées sont prises en charge.
- Seules les clés régionales sont prises en charge ; les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif « Cryptage/décryptage symétrique » est pris en charge.
- L'agent de service associé au compte de stockage se voit attribuer le rôle IAM « CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter) » par NetApp Backup and Recovery.

Créez vos propres seaux

Par défaut, le service crée des buckets pour vous. Si vous souhaitez utiliser vos propres buckets, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces buckets dans l'assistant.

"En savoir plus sur la création de vos propres buckets".

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.
- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (il s'agit du paramètre par défaut).

Activer la NetApp Backup and Recovery sur Cloud Volumes ONTAP

Les étapes d'activation de la NetApp Backup and Recovery diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau.

Activer la NetApp Backup and Recovery sur un nouveau système

NetApp Backup and Recovery peut être activé lorsque vous terminez l'assistant système pour créer un nouveau système Cloud Volumes ONTAP .

Vous devez avoir un compte de service déjà configuré. Si vous ne sélectionnez pas de compte de service lorsque vous créez le système Cloud Volumes ONTAP , vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP à partir de la console GCP.

Voir "Lancement de Cloud Volumes ONTAP dans GCP" pour connaître les exigences et les détails de création de votre système Cloud Volumes ONTAP .

Étapes

1. Depuis la page **Systèmes** de la console, sélectionnez **Ajouter un système**, choisissez le fournisseur de cloud et sélectionnez **Ajouter un nouveau**. Sélectionnez **Créer des Cloud Volumes ONTAP**.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud Platform**.
3. **Choisir le type** : Sélectionnez * Cloud Volumes ONTAP* (nœud unique ou haute disponibilité).
4. **Détails et informations d'identification** : Saisissez les informations suivantes :
    a. Cliquez sur **Modifier le projet** et sélectionnez un nouveau projet si celui que vous souhaitez utiliser est différent du projet par défaut (où réside l'agent de la console).
    b. Spécifiez le nom du cluster.
    c. Activez le commutateur **Compte de service** et sélectionnez le compte de service doté du rôle d'administrateur de stockage prédéfini. Ceci est nécessaire pour activer les sauvegardes et la hiérarchisation.
    d. Spécifiez les informations d'identification.

    Assurez-vous qu'un abonnement GCP Marketplace est en place.
5. **Services** : Laissez NetApp Backup and Recovery activé et cliquez sur **Continuer**.
6. Complétez les pages de l'assistant pour déployer le système comme décrit dans "Lancement de Cloud Volumes ONTAP dans GCP" .

Résultat

NetApp Backup and Recovery est activé sur le système. Après avoir créé des volumes sur ces systèmes Cloud Volumes ONTAP , lancez NetApp Backup and Recovery et"activer la sauvegarde sur chaque volume que vous souhaitez protéger" .

Activer la NetApp Backup and Recovery sur un système existant

Vous pouvez activer NetApp Backup and Recovery à tout moment directement depuis le système.

Étapes

1. Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer** à côté de Sauvegarde et récupération dans le panneau de droite.

   Si la destination Google Cloud Storage pour vos sauvegardes existe en tant que système sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster sur le système Google Cloud Storage pour lancer l'assistant de configuration.

Préparez Google Cloud Storage comme cible de sauvegarde

La préparation de Google Cloud Storage comme cible de sauvegarde implique les étapes suivantes :

- Configurer les autorisations.
- (Facultatif) Créez vos propres buckets. (Le service créera des buckets pour vous si vous le souhaitez.)
- (Facultatif) Configurer des clés gérées par le client pour le chiffrement des données

Configurer les autorisations

Vous devez fournir des clés d'accès au stockage pour un compte de service disposant d'autorisations spécifiques à l'aide d'un rôle personnalisé. Un compte de service permet à NetApp Backup and Recovery d'authentifier et d'accéder aux buckets Cloud Storage utilisés pour stocker les sauvegardes. Les clés sont nécessaires pour que Google Cloud Storage sache qui fait la demande.

Étapes

1. Dans le "Console Google Cloud" , allez à la page **Rôles**.
2. "Créer un nouveau rôle"avec les autorisations suivantes :

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Dans la console Google Cloud, "aller à la page Comptes de service" .
4. Sélectionnez votre projet Cloud.
5. Sélectionnez **Créer un compte de service** et fournissez les informations requises :
   a. **Détails du compte de service** : saisissez un nom et une description.
   b. **Accorder à ce compte de service l'accès au projet** : sélectionnez le rôle personnalisé que vous

venez de créer.

c. Sélectionnez **Terminé**.

6. Aller à "Paramètres de stockage GCP" et créez des clés d'accès pour le compte de service :

   a. Sélectionnez un projet et sélectionnez **Interopérabilité**. Si vous ne l'avez pas déjà fait, sélectionnez **Activer l'accès à l'interopérabilité**.

   b. Sous **Clés d'accès pour les comptes de service**, sélectionnez **Créer une clé pour un compte de service**, sélectionnez le compte de service que vous venez de créer et cliquez sur **Créer une clé**.

      Vous devrez saisir les clés dans NetApp Backup and Recovery ultérieurement lorsque vous configurerez le service de sauvegarde.

Créez vos propres seaux

Par défaut, le service crée des buckets pour vous. Ou, si vous souhaitez utiliser vos propres buckets, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces buckets dans l'assistant.

"En savoir plus sur la création de vos propres buckets".

Configurer des clés de chiffrement gérées par le client (CMEK) pour le chiffrement des données

Vous pouvez utiliser vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés de chiffrement par défaut gérées par Google. Les clés inter-régions et inter-projets sont prises en charge, vous pouvez donc choisir un projet pour un bucket différent du projet de la clé CMEK.

Si vous prévoyez d'utiliser vos propres clés gérées par le client :

- Vous aurez besoin du trousseau de clés et du nom de la clé pour pouvoir ajouter ces informations dans l'assistant d'activation. "En savoir plus sur les clés de chiffrement gérées par le client" .
- Vous devrez vérifier que ces autorisations requises sont incluses dans le rôle de l'agent de console :

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Vous devrez vérifier que l'API Google « Cloud Key Management Service (KMS) » est activée dans votre projet. Voir le "Documentation Google Cloud : Activation des API" pour plus de détails.

Considérations CMEK :

- Les clés HSM (protégées par le matériel) et les clés générées par logiciel sont prises en charge.
- Les clés Cloud KMS nouvellement créées ou importées sont prises en charge.
- Seules les clés régionales sont prises en charge, les clés globales ne sont pas prises en charge.

- Actuellement, seul l'objectif « Cryptage/décryptage symétrique » est pris en charge.
- L'agent de service associé au compte de stockage se voit attribuer le rôle IAM « CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter) » par NetApp Backup and Recovery.

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez égalementAfficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté de Sauvegarde et récupération dans le panneau de droite.

     Si la destination GCP pour vos sauvegardes existe en tant que système sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets GCP.

   - Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez les **Actions*** ••• **icône et sélectionnez *Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Notez que si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.
   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur stockage d'objets
- Architecture
- Politique d'instantané local
- Cible et politique de réplication

Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes sur le stockage d'objets.
2. **Architecture** : Si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les informations circulent du système de stockage principal vers le secondaire, et du secondaire vers le stockage d'objets.
   - **Fan out** : les informations circulent du système de stockage principal vers le secondaire *et* du système principal vers le stockage d'objets.

Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .

3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une.

   Pour créer une politique personnalisée avant d'activer la sauvegarde, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Pour les politiques de sauvegarde sur objet, configurez Datalock et Ransomware Resilience. Pour plus de détails sur Datalock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .
   - Sélectionnez **Créer**.

4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une.

     Pour créer une politique personnalisée avant d'activer la réplication, reportez-vous à"Créer une politique" .

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.

5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Google Cloud**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région où les sauvegardes seront stockées.

     Créez un nouveau bucket ou sélectionnez-en un existant.

   - **Clé de chiffrement** : si vous avez créé un nouveau bucket Google, saisissez les informations de clé de chiffrement fournies par le fournisseur. Choisissez si vous utiliserez les clés de chiffrement par défaut de Google Cloud ou si vous choisirez vos propres clés gérées par le client à partir de votre compte Google pour gérer le chiffrement de vos données.

     Si vous choisissez d'utiliser vos propres clés gérées par le client, saisissez le coffre-fort de clés et les informations sur la clé.

     Si vous avez choisi un bucket Google Cloud existant, les informations de chiffrement sont déjà disponibles, vous n'avez donc pas besoin de les saisir maintenant.

   - **Politique de sauvegarde** : sélectionnez une politique de stockage de sauvegarde sur objet existante

ou créez-en une.

> Pour créer une politique personnalisée avant d'activer la sauvegarde, reportez-vous à"Créer une politique" .

Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

- Entrez le nom de la politique.
- Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
- Sélectionnez **Créer**.

◦ **Exporter les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage principal. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume du système de stockage principal.

Un bucket Google Cloud Storage est créé dans le compte de service indiqué par la clé d'accès Google et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés.

Les sauvegardes sont associées à la classe de stockage *Standard* par défaut. Vous pouvez utiliser les classes de stockage *Nearline*, *Coldline* ou *Archive* à moindre coût. Cependant, vous configurez la classe de stockage via Google, et non via l'interface utilisateur de NetApp Backup and Recovery . Voir le sujet Google "Modification de la classe de stockage par défaut d'un bucket" pour plus de détails.

Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Quelle est la prochaine étape ?

- Tu peux"gérez vos fichiers de sauvegarde et vos politiques de sauvegarde" . Cela inclut le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification de sauvegarde, et bien plus encore.
- Tu peux"gérer les paramètres de sauvegarde au niveau du cluster" . Cela inclut la modification des clés de stockage ONTAP utilise pour accéder au stockage cloud, la modification de la bande passante réseau disponible pour télécharger des sauvegardes vers le stockage d'objets, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.
- Vous pouvez également"restaurer des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" vers un système Cloud Volumes ONTAP dans AWS ou vers un système ONTAP sur site.

Sauvegardez les données ONTAP sur site sur Amazon S3 avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes ONTAP sur site vers un système de stockage secondaire et vers le stockage cloud Amazon S3.

Les « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

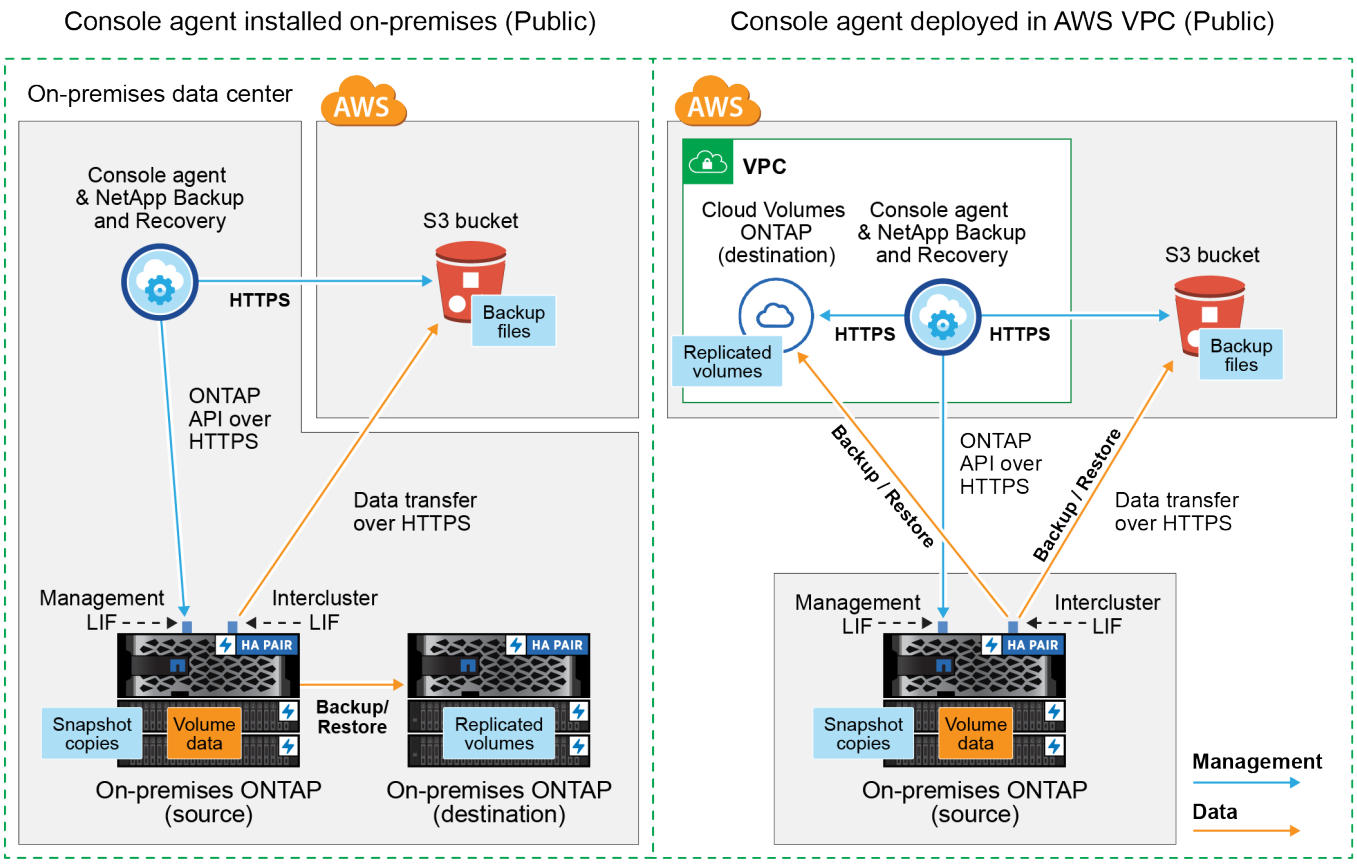
Identifier la méthode de connexion

Choisissez laquelle des deux méthodes de connexion vous utiliserez lors de la configuration des sauvegardes des systèmes ONTAP locaux vers AWS S3.

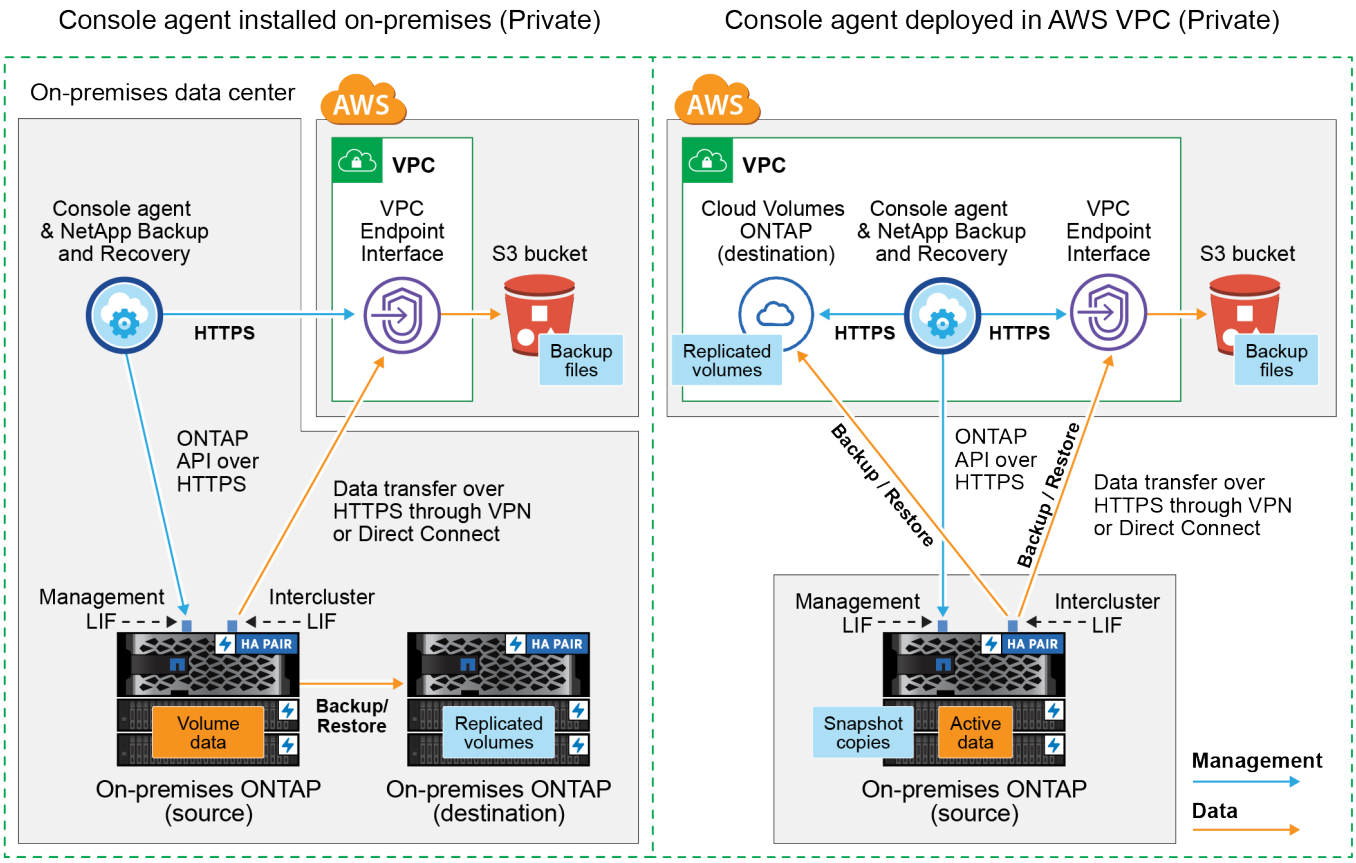
- **Connexion publique** - Connectez directement le système ONTAP à AWS S3 à l'aide d'un point de terminaison S3 public.
- **Connexion privée** - Utilisez un VPN ou AWS Direct Connect et acheminez le trafic via une interface de point de terminaison VPC qui utilise une adresse IP privée.

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.

Le diagramme suivant montre la méthode de **connexion publique** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un agent de console que vous avez installé sur vos locaux ou un agent de console que vous avez déployé dans AWS VPC.



Le diagramme suivant montre la méthode de **connexion privée** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un agent de console que vous avez installé sur vos locaux ou un agent de console que vous avez déployé dans AWS VPC.



Préparez votre agent de console

L'agent de console est le logiciel principal pour la fonctionnalité de la NetApp Console . Un agent de console est requis pour sauvegarder et restaurer vos données ONTAP .

Créer ou changer d'agents de console

Si vous disposez déjà d'un agent de console déployé dans votre AWS VPC ou sur vos locaux, vous êtes prêt.

Sinon, vous devrez créer un agent de console dans l'un de ces emplacements pour sauvegarder les données ONTAP sur le stockage AWS S3. Vous ne pouvez pas utiliser un agent de console déployé chez un autre fournisseur de cloud.

- "En savoir plus sur les agents de console"
- "Installer un agent de console dans AWS"
- "Installer un agent Console dans vos locaux"
- "Installer un agent de console dans une région AWS GovCloud"

  NetApp Backup and Recovery est pris en charge dans les régions GovCloud lorsque l'agent de console est déployé dans le cloud, et non lorsqu'il est installé dans vos locaux. De plus, vous devez déployer l'agent de console à partir d'AWS Marketplace. Vous ne pouvez pas déployer l'agent de console dans une région gouvernementale à partir du site Web SaaS de la NetApp Console .

Préparer les exigences réseau de l'agent de console

Assurez-vous que les exigences réseau suivantes sont respectées :

- Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :
  - Une connexion HTTPS sur le port 443 vers NetApp Backup and Recovery et vers votre stockage d'objets S3("voir la liste des points de terminaison")
  - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
  - Des règles de groupe de sécurité entrantes et sortantes supplémentaires sont requises pour les déploiements AWS et AWS GovCloud. Voir "Règles pour l'agent de console dans AWS" pour plus de détails.
- Si vous disposez d'une connexion Direct Connect ou VPN de votre cluster ONTAP au VPC et que vous souhaitez que la communication entre l'agent de console et S3 reste dans votre réseau interne AWS (une connexion **privée**), vous devrez activer une interface de point de terminaison VPC sur S3. Configurez votre système pour une connexion privée à l'aide d'une interface de point de terminaison VPC .

Vérifier les exigences de licence

Vous devrez vérifier les exigences de licence pour AWS et la NetApp Console:

- Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez soit vous abonner à une offre NetApp Console Marketplace à paiement à l'utilisation (PAYGO) d'AWS, soit acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour les licences NetApp Backup and Recovery PAYGO, vous aurez besoin d'un abonnement au "Offre NetApp Console de la place de marché AWS" . La facturation de NetApp Backup and Recovery s'effectue via cet abonnement.
  - Pour les licences BYOL de NetApp Backup and Recovery , vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence.
- Vous devez disposer d'un abonnement AWS pour l'espace de stockage d'objets où vos sauvegardes seront situées.

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes locaux vers Amazon S3 dans toutes les régions, y compris les régions AWS GovCloud. Vous spécifiez la région où les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

Préparez votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans la NetApp Console
- Vérifier la configuration système requise ONTAP
- Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets
- Vérifier les exigences réseau ONTAP pour la réplication des volumes

Découvrez vos systèmes ONTAP dans la NetApp Console

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site doivent être disponibles sur la page **Systèmes** de la NetApp Console .

Vous devrez connaître l'adresse IP de gestion du cluster et le mot de passe du compte utilisateur administrateur pour ajouter le cluster. "Apprenez à découvrir un cluster" .

Vérifier la configuration système requise ONTAP

Assurez-vous que votre système ONTAP répond aux exigences suivantes :

- Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.
- Une licence SnapMirror (incluse dans le cadre du pack Premium ou du pack de protection des données).

  Remarque : le « Hybrid Cloud Bundle » n'est pas requis lors de l'utilisation de NetApp Backup and Recovery.

  Apprenez à "gérez vos licences de cluster" .
- L'heure et le fuseau horaire sont correctement réglés. Apprenez à "configurer l'heure de votre cluster" .
- Si vous répliquez des données, vérifiez que les systèmes source et de destination exécutent des versions ONTAP compatibles.

  "Afficher les versions ONTAP compatibles pour les relations SnapMirror".

Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage d'objets.

- Pour une architecture de sauvegarde en éventail, configurez les paramètres suivants sur le système *principal*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondaire*.

Les exigences de mise en réseau du cluster ONTAP suivantes sont nécessaires :

- Le cluster nécessite une connexion HTTPS entrante de l'agent de console au LIF de gestion du cluster.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Ces LIF interclusters doivent pouvoir accéder au magasin d'objets.

  Le cluster initie une connexion HTTPS sortante via le port 443 depuis les LIF interclusters vers le stockage Amazon S3 pour les opérations de sauvegarde et de restauration. ONTAP lit et écrit des données vers et depuis le stockage d'objets : le stockage d'objets ne s'initialise jamais, il répond simplement.

- Les LIF intercluster doivent être associés à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

  Lorsque vous configurez NetApp Backup and Recovery, vous êtes invité à indiquer l'espace IP à utiliser. Vous devez choisir l'espace IP auquel ces LIF sont associés. Il peut s'agir de l'espace IP « par défaut » ou d'un espace IP personnalisé que vous avez créé.

  Si vous utilisez un espace IP différent de « Par défaut », vous devrez peut-être créer une route statique pour accéder au stockage d'objets.

Tous les LIF interclusters au sein de l'espace IP doivent avoir accès au magasin d'objets. Si vous ne pouvez pas configurer cela pour l'espace IP actuel, vous devrez créer un espace IP dédié où tous les LIF interclusters ont accès au magasin d'objets.

- Les serveurs DNS doivent avoir été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port 443 et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).
- Si vous utilisez un point de terminaison d'interface VPC privé dans AWS pour la connexion S3, pour que HTTPS/443 soit utilisé, vous devrez charger le certificat de point de terminaison S3 dans le cluster ONTAP . Configurez votre système pour une connexion privée à l'aide d'une interface de point de terminaison VPC.
- Assurez-vous que votre cluster ONTAP dispose des autorisations nécessaires pour accéder au compartiment S3.

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Amazon S3 comme cible de sauvegarde

La préparation d'Amazon S3 comme cible de sauvegarde implique les étapes suivantes :

- Configurer les autorisations S3.
- (Facultatif) Créez vos propres buckets S3. (Le service créera des buckets pour vous si vous le souhaitez.)
- (Facultatif) Configurez des clés AWS gérées par le client pour le chiffrement des données.
- (Facultatif) Configurez votre système pour une connexion privée à l'aide d'une interface de point de terminaison VPC.

Configurer les autorisations S3

Vous devrez configurer deux ensembles d'autorisations :

- Autorisations permettant à l'agent de console de créer et de gérer le compartiment S3.
- Autorisations pour le cluster ONTAP sur site afin qu'il puisse lire et écrire des données dans le bucket S3.

Étapes

1. Assurez-vous que l'agent de la console dispose des autorisations requises. Pour plus de détails, voir "Autorisations de stratégie de la NetApp Console" .

   Lors de la création de sauvegardes dans les régions AWS Chine, vous devez modifier le nom de ressource AWS « arn » sous toutes les sections *Resource* dans les politiques IAM de « aws » à « aws-cn » ; par exemple `arn:aws-cn:s3:::netapp-backup-*` .

2. Lorsque vous activez le service, l'assistant de sauvegarde vous invite à saisir une clé d'accès et une clé secrète. Ces informations d'identification sont transmises au cluster ONTAP afin ONTAP puisse sauvegarder et restaurer les données dans le bucket S3. Pour cela, vous devrez créer un utilisateur IAM avec les autorisations suivantes.

   Reportez-vous à la "Documentation AWS : Création d'un rôle pour déléguer des autorisations à un utilisateur IAM" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Créez vos propres seaux

Par défaut, le service crée des buckets pour vous. Ou, si vous souhaitez utiliser vos propres buckets, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces buckets dans l'assistant.

"En savoir plus sur la création de vos propres buckets".

Si vous créez vos propres buckets, vous devez utiliser un nom de bucket « netapp-backup ». Si vous devez utiliser un nom personnalisé, modifiez le `ontapcloud-instance-policy-netapp-backup` Ajoutez une IAMRole aux CVO existants et le bloc JSON suivant aux autorisations S3. `Statement` tableau. Vous devez inclure `"Resource": "arn:aws:s3:::*"` et attribuez toutes les autorisations nécessaires qui doivent être associées au bucket.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

Configurer des clés AWS gérées par le client pour le chiffrement des données

Si vous souhaitez utiliser les clés de chiffrement Amazon S3 par défaut pour chiffrer les données transmises entre votre cluster sur site et le compartiment S3, vous êtes prêt car l'installation par défaut utilise ce type de chiffrement.

Si, au lieu de cela, vous souhaitez utiliser vos propres clés gérées par le client pour le chiffrement des données plutôt que d'utiliser les clés par défaut, vous devrez alors avoir les clés gérées par le chiffrement déjà configurées avant de démarrer l'assistant de NetApp Backup and Recovery .

"Découvrez comment utiliser vos propres clés de chiffrement Amazon avec Cloud Volumes ONTAP".

"Découvrez comment utiliser vos propres clés de chiffrement Amazon avec NetApp Backup and Recovery".

Configurez votre système pour une connexion privée à l'aide d'une interface de point de terminaison VPC

Si vous souhaitez utiliser une connexion Internet publique standard, toutes les autorisations sont définies par l'agent de la console et vous n'avez rien d'autre à faire.

Si vous souhaitez disposer d'une connexion Internet plus sécurisée entre votre centre de données sur site et le VPC, vous pouvez sélectionner une connexion AWS PrivateLink dans l'assistant d'activation de sauvegarde. Cela est nécessaire si vous prévoyez d'utiliser un VPN ou AWS Direct Connect pour connecter votre système sur site via une interface de point de terminaison VPC qui utilise une adresse IP privée.

Étapes

1. Créez une configuration de point de terminaison d'interface à l'aide de la console Amazon VPC ou de la ligne de commande. "Consultez les détails sur l'utilisation d'AWS PrivateLink pour Amazon S3" .
2. Modifiez la configuration du groupe de sécurité associé à l'agent de console. Vous devez modifier la politique en « Personnalisé » (à partir de « Accès complet ») et vous devezajouter les autorisations S3 à partir de la politique de sauvegarde comme indiqué précédemment.

   Si vous utilisez le port 80 (HTTP) pour communiquer avec le point de terminaison privé, vous êtes prêt. Vous pouvez désormais activer NetApp Backup and Recovery sur le cluster.

   Si vous utilisez le port 443 (HTTPS) pour la communication avec le point de terminaison privé, vous devez copier le certificat du point de terminaison VPC S3 et l'ajouter à votre cluster ONTAP , comme indiqué dans les 4 étapes suivantes.

3. Obtenez le nom DNS du point de terminaison à partir de la console AWS.
4. Obtenez le certificat à partir du point de terminaison VPC S3. Vous faites cela en "connexion à la machine virtuelle qui héberge l'agent de la console" et exécutez la commande suivante. Lors de la saisie du nom DNS du point de terminaison, ajoutez « bucket » au début, en remplaçant le « * » :

   ```
   openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
   ```

5. À partir de la sortie de cette commande, copiez les données du certificat S3 (toutes les données comprises entre les balises BEGIN / END CERTIFICATE incluses) :

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Connectez-vous à l'interface de ligne de commande du cluster ONTAP et appliquez le certificat que vous avez copié à l'aide de la commande suivante (remplacez le nom de votre propre machine virtuelle de stockage) :

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez égalementAfficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté de Sauvegarde et récupération dans le panneau de droite.

     Si la destination Amazon S3 pour vos sauvegardes existe en tant que système sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets Amazon S3.

   - Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez les **Actions*** ••• **icône et sélectionnez *Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la

réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.
   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : snapshots locaux, réplication et sauvegarde sur stockage d'objets
- Architecture
- Politique d'instantané local
- Cible et politique de réplication

Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes sur le stockage d'objets.
2. **Architecture** : Si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les informations circulent du stockage primaire vers le stockage secondaire vers le stockage d'objets et du stockage secondaire vers le stockage d'objets.
   - **Fan out** : les informations circulent du primaire vers le secondaire *et* du primaire vers le stockage d'objets.

     Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez une politique.

   Pour créer une politique personnalisée avant d'activer l'instantané, reportez-vous à"Créer une politique" .
4. Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Pour les politiques de sauvegarde sur objet, définissez les paramètres DataLock et Ransomware Resilience. Pour plus de détails sur DataLock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .
   - Sélectionnez **Créer**.
5. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez une politique.

     Pour créer une politique personnalisée avant d'activer la réplication, reportez-vous à"Créer une politique" .

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
6. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :

- **Fournisseur** : Sélectionnez **Amazon Web Services**.
- **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région AWS où les sauvegardes seront stockées.

  La clé d'accès et la clé secrète sont destinées à l'utilisateur IAM que vous avez créé pour donner au cluster ONTAP l'accès au bucket S3.

- **Bucket** : Choisissez un bucket S3 existant ou créez-en un nouveau. Se référer à "Ajouter des buckets S3" .
- **Clé de chiffrement** : si vous avez créé un nouveau compartiment S3, saisissez les informations de clé de chiffrement fournies par le fournisseur. Choisissez si vous utiliserez les clés de chiffrement Amazon S3 par défaut ou si vous choisirez vos propres clés gérées par le client à partir de votre compte AWS pour gérer le chiffrement de vos données.

  Si vous avez choisi un bucket existant, les informations de chiffrement sont déjà disponibles, vous n'avez donc pas besoin de les saisir maintenant.

- **Réseau** : Choisissez l'espace IP et indiquez si vous utiliserez un point de terminaison privé. Le point de terminaison privé est désactivé par défaut.
  i. L'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
  ii. Vous pouvez également choisir si vous utiliserez un AWS PrivateLink que vous avez précédemment configuré. "Voir les détails sur l'utilisation d'AWS PrivateLink pour Amazon S3" .
- **Politique de sauvegarde** : sélectionnez une politique de sauvegarde existante ou créez une politique.

  Pour créer une politique personnalisée avant d'activer la sauvegarde, reportez-vous à"Créer une politique" .

  Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

  - Entrez le nom de la politique.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.
- **Exporter les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

7. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés

avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde.

3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage principal. Les transferts suivants contiennent des copies différentielles des données primaires contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume de stockage principal.

Le compartiment S3 est créé dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Sauvegardez les données ONTAP sur site sur le stockage Azure Blob avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes ONTAP locaux vers un système de stockage secondaire et vers le stockage Azure Blob.

Les « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

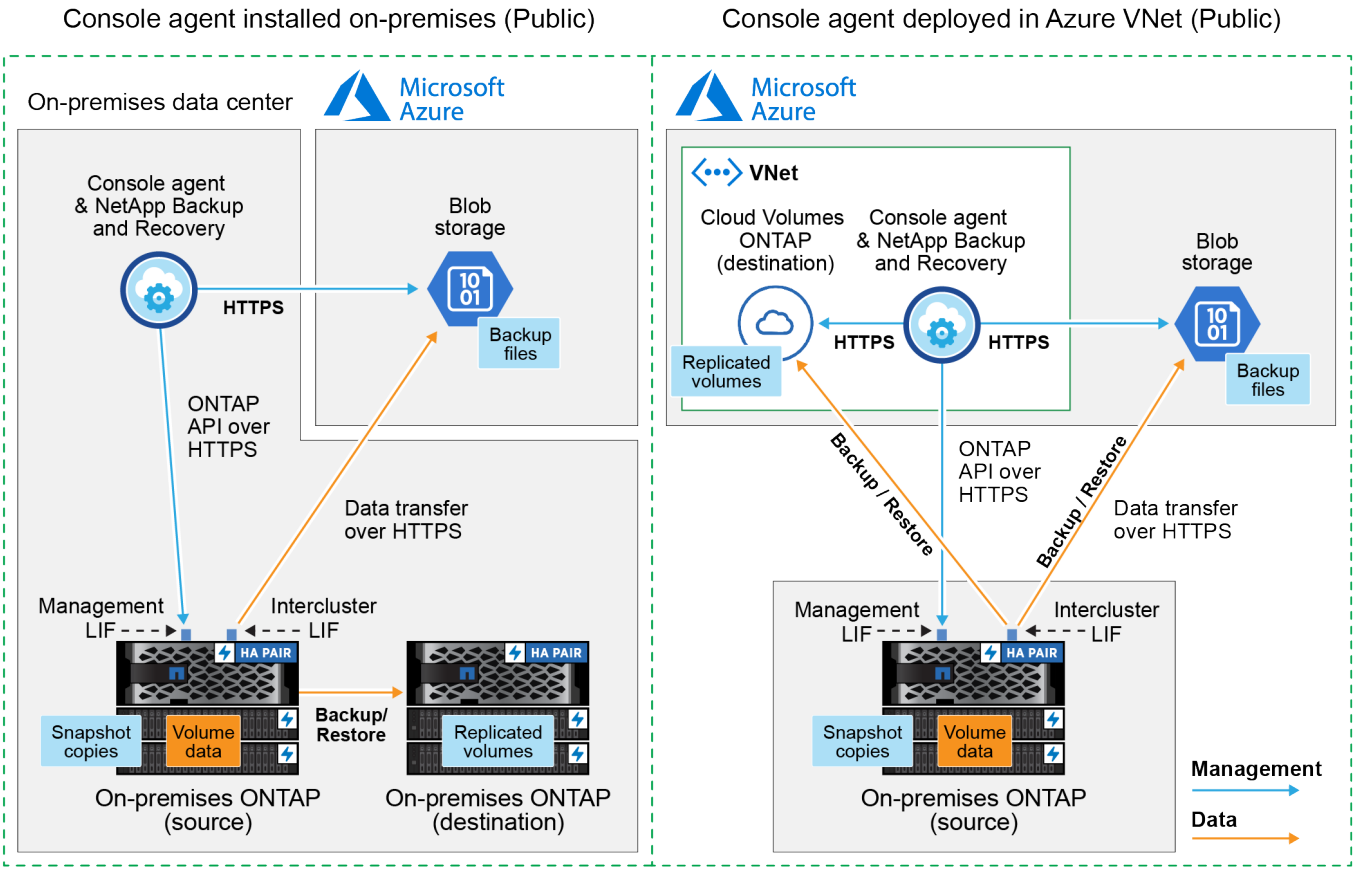
Identifier la méthode de connexion

Choisissez laquelle des deux méthodes de connexion vous utiliserez lors de la configuration des sauvegardes des systèmes ONTAP locaux vers Azure Blob.

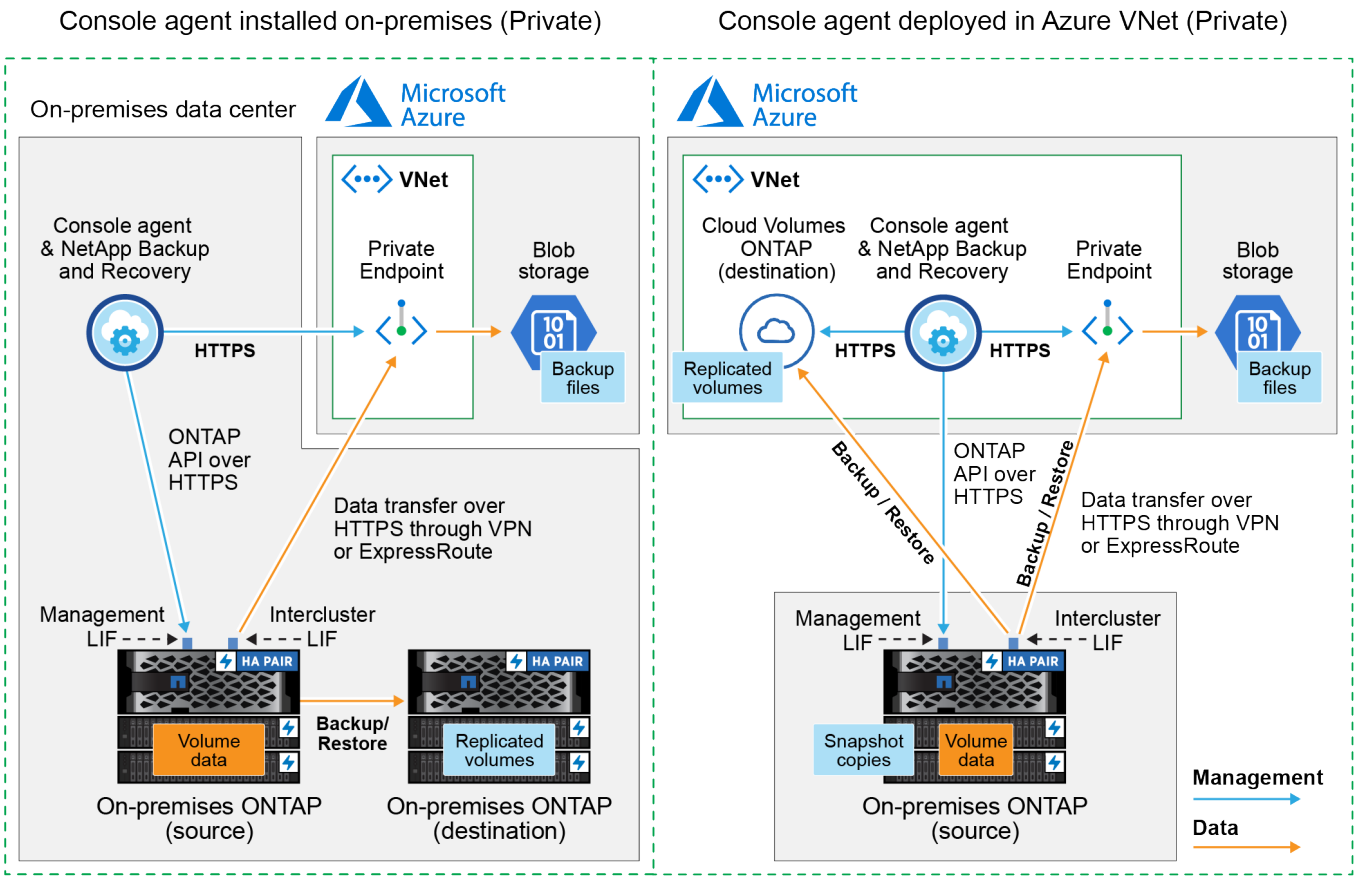
- **Connexion publique** - Connectez directement le système ONTAP au stockage Azure Blob à l'aide d'un point de terminaison Azure public.
- **Connexion privée** - Utilisez un VPN ou ExpressRoute et acheminez le trafic via un point de terminaison privé VNet qui utilise une adresse IP privée.

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.

Le diagramme suivant montre la méthode de **connexion publique** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un agent de console que vous avez installé sur votre site ou un agent de console que vous avez déployé dans le réseau virtuel Azure.



Le diagramme suivant montre la méthode de **connexion privée** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un agent de console que vous avez installé sur votre site ou un agent de console que vous avez déployé dans le réseau virtuel Azure.



Préparez votre agent de console

L'agent de console est le logiciel principal pour la fonctionnalité de la NetApp Console . Un agent de console est requis pour sauvegarder et restaurer vos données ONTAP .

Créer ou changer d'agents de console

Si vous disposez déjà d'un agent de console déployé sur votre réseau virtuel Azure ou sur vos locaux, vous êtes prêt.

Sinon, vous devrez créer un agent de console dans l'un de ces emplacements pour sauvegarder les données ONTAP sur le stockage Azure Blob. Vous ne pouvez pas utiliser un agent de console déployé chez un autre fournisseur de cloud.

- "En savoir plus sur les agents de console"
- "Installer un agent de console dans Azure"
- "Installer un agent Console dans vos locaux"
- "Installer un agent de console dans une région Azure Government"

  NetApp Backup and Recovery est pris en charge dans les régions Azure Government lorsque l'agent de console est déployé dans le cloud, et non lorsqu'il est installé dans vos locaux. De plus, vous devez déployer l'agent de console à partir de la Place de marché Azure. Vous ne pouvez pas déployer l'agent de console dans une région gouvernementale à partir du site Web SaaS de la console.

Préparer la mise en réseau pour l'agent de la console

Assurez-vous que l'agent de console dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :
   - Une connexion HTTPS via le port 443 vers NetApp Backup and Recovery et vers votre stockage d'objets Blob("voir la liste des points de terminaison")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
   - Pour que la fonctionnalité de recherche et de restauration de NetApp Backup and Recovery fonctionne, le port 1433 doit être ouvert pour la communication entre l'agent de la console et les services Azure Synapse SQL.
   - Des règles de groupe de sécurité entrantes supplémentaires sont requises pour les déploiements Azure et Azure Government. Voir "Règles pour l'agent de console dans Azure" pour plus de détails.
2. Activez un point de terminaison privé VNet sur le stockage Azure. Cela est nécessaire si vous disposez d'une connexion ExpressRoute ou VPN de votre cluster ONTAP au VNet et que vous souhaitez que la communication entre l'agent de console et le stockage Blob reste dans votre réseau privé virtuel (une connexion **privée**).

Vérifier ou ajouter des autorisations à l'agent de la console

Pour utiliser la fonctionnalité de recherche et de restauration de NetApp Backup and Recovery , vous devez disposer d'autorisations spécifiques dans le rôle de l'agent de console afin qu'il puisse accéder au compte Azure Synapse Workspace et Data Lake Storage. Consultez les autorisations ci-dessous et suivez les étapes si vous devez modifier la politique.

Avant de commencer

Vous devez enregistrer le fournisseur de ressources Azure Synapse Analytics (appelé « Microsoft.Synapse ») avec votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement" . Vous devez être le **Propriétaire** ou le **Contributeur** de l'abonnement pour enregistrer le fournisseur de ressources.

Étapes

1. Identifiez le rôle attribué à la machine virtuelle de l'agent de console :
   a. Dans le portail Azure, ouvrez le service Machines virtuelles.
   b. Sélectionnez la machine virtuelle de l'agent de console.
   c. Sous **Paramètres**, sélectionnez **Identité**.
   d. Sélectionnez **Attributions de rôles Azure**.
   e. Prenez note du rôle personnalisé attribué à la machine virtuelle de l'agent de console.
2. Mettre à jour le rôle personnalisé :
   a. Dans le portail Azure, ouvrez votre abonnement Azure.
   b. Sélectionnez **Contrôle d'accès (IAM) > Rôles**.
   c. Sélectionnez les points de suspension (**…**) pour le rôle personnalisé, puis sélectionnez **Modifier**.
   d. Sélectionnez **JSON** et ajoutez les autorisations suivantes :

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Afficher le format JSON complet de la politique"

e. Sélectionnez **Réviser + mettre à jour**, puis sélectionnez **Mettre à jour**.

Vérifier les exigences de licence

Vous devrez vérifier les exigences de licence pour Azure et la console :

- Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez soit vous abonner à une offre de paiement à l'utilisation (PAYGO) de la place de marché de la console d'Azure, soit acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour les licences NetApp Backup and Recovery PAYGO, vous aurez besoin d'un abonnement au "Offre NetApp Console de la Place de marché Azure" . La facturation de NetApp Backup and Recovery s'effectue via cet abonnement.
  - Pour les licences BYOL de NetApp Backup and Recovery , vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .
- Vous devez disposer d'un abonnement Azure pour l'espace de stockage d'objets où vos sauvegardes seront situées.

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes locaux vers Azure Blob dans toutes les régions, y compris les régions Azure Government. Vous spécifiez la région où les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

Préparez votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans la NetApp Console
- Vérifier la configuration système requise ONTAP
- Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets
- Vérifier les exigences réseau ONTAP pour la réplication des volumes

Découvrez vos systèmes ONTAP dans la NetApp Console

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site doivent être disponibles sur la page **Systèmes** de la NetApp Console .

Vous devrez connaître l'adresse IP de gestion du cluster et le mot de passe du compte utilisateur administrateur pour ajouter le cluster. "Apprenez à découvrir un cluster" .

Vérifier la configuration système requise ONTAP

Assurez-vous que votre système ONTAP répond aux exigences suivantes :

- Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.
- Une licence SnapMirror (incluse dans le cadre du pack Premium ou du pack de protection des données).

  Remarque : le « Hybrid Cloud Bundle » n'est pas requis lors de l'utilisation de NetApp Backup and Recovery.

Apprenez à "gérez vos licences de cluster" .

- L'heure et le fuseau horaire sont correctement réglés. Apprenez à "configurer l'heure de votre cluster" .
- Si vous répliquez des données, vérifiez que les systèmes source et de destination exécutent des versions ONTAP compatibles.

  "Afficher les versions ONTAP compatibles pour les relations SnapMirror".

Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage d'objets.

- Pour une architecture de sauvegarde en éventail, configurez les paramètres suivants sur le système *principal*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondaire*.

Les exigences de mise en réseau du cluster ONTAP suivantes sont nécessaires :

- Le cluster ONTAP initie une connexion HTTPS via le port 443 du LIF intercluster au stockage Azure Blob pour les opérations de sauvegarde et de restauration.

  ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.

- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster. L'agent de console peut résider dans un réseau virtuel Azure.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

  Lorsque vous configurez NetApp Backup and Recovery, vous êtes invité à indiquer l'espace IP à utiliser. Vous devez choisir l'espace IP auquel chaque LIF est associé. Il peut s'agir de l'espace IP « par défaut » ou d'un espace IP personnalisé que vous avez créé.

- Les LIF des nœuds et des interclusters peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions du service NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port 443 et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Azure Blob comme cible de sauvegarde

1. Vous pouvez utiliser vos propres clés gérées de manière personnalisée pour le chiffrement des données dans l'assistant d'activation au lieu d'utiliser les clés de chiffrement par défaut gérées par Microsoft. Dans ce cas, vous aurez besoin de l'abonnement Azure, du nom du coffre de clés et de la clé. "Apprenez à utiliser vos propres clés" .

   Notez que la sauvegarde et la récupération prennent en charge les *stratégies d'accès Azure* comme modèle d'autorisation. Le modèle d'autorisation *Azure role-based access control* (Azure RBAC) n'est actuellement pas pris en charge.

2. Si vous souhaitez disposer d'une connexion plus sécurisée sur l'Internet public depuis votre centre de données local vers le réseau virtuel, il existe une option permettant de configurer un point de terminaison privé Azure dans l'assistant d'activation. Dans ce cas, vous devrez connaître le VNet et le sous-réseau pour cette connexion. "Consultez les détails sur l'utilisation d'un point de terminaison privé" .

Créez votre compte de stockage Azure Blob

Par défaut, le service crée des comptes de stockage pour vous. Si vous souhaitez utiliser vos propres comptes de stockage, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces comptes de stockage dans l'assistant.

"En savoir plus sur la création de vos propres comptes de stockage".

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez également Afficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté du service de sauvegarde et de récupération dans le panneau de droite.

     Si la destination Azure de vos sauvegardes existe sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets Azure Blob.

   - Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez les **Actions*** **icône et sélectionnez *Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Notez que si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.

   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur stockage d'objets
- Architecture
- Politique d'instantané local
- Cible et politique de réplication

> Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes sur le stockage d'objets.
2. **Architecture** : Si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les informations circulent du primaire vers le secondaire, et du secondaire vers le stockage d'objets.
   - **Fan out** : les informations circulent du primaire vers le secondaire *et* du primaire vers le stockage d'objets.

     Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

   > Pour créer une politique personnalisée avant d'activer l'instantané, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au

nom du volume répliqué.

- **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une nouvelle.

  Pour créer une politique personnalisée avant d'activer la réplication, reportez-vous à"Créer une politique" .

  Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

  - Entrez le nom de la politique.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Microsoft Azure**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région où les sauvegardes seront stockées.

     Créez un nouveau compte de stockage ou sélectionnez-en un existant.

     Créez votre propre groupe de ressources qui gère le conteneur Blob ou sélectionnez le type de groupe de ressources et le groupe.

     Si vous souhaitez protéger vos fichiers de sauvegarde contre toute modification ou suppression, assurez-vous que le compte de stockage a été créé avec le stockage immuable activé à l'aide d'une période de conservation de 30 jours.

     Si vous souhaitez hiérarchiser les fichiers de sauvegarde plus anciens vers Azure Archive Storage pour une optimisation supplémentaire des coûts, assurez-vous que le compte de stockage dispose de la règle de cycle de vie appropriée.

   - **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Azure, saisissez les informations de clé de chiffrement fournies par le fournisseur. Choisissez si vous utiliserez les clés de chiffrement Azure par défaut ou si vous choisirez vos propres clés gérées par le client à partir de votre compte Azure pour gérer le chiffrement de vos données.

     Si vous choisissez d'utiliser vos propres clés gérées par le client, saisissez le coffre-fort de clés et les informations sur la clé.

     Si vous avez choisi un compte de stockage Microsoft existant, les informations de chiffrement sont déjà disponibles, vous n'avez donc pas besoin de les saisir maintenant.

   - **Réseau** : Choisissez l'espace IP et indiquez si vous utiliserez un point de terminaison privé. Le point de terminaison privé est désactivé par défaut.
     i. L'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
     ii. Vous pouvez également choisir si vous utiliserez un point de terminaison privé Azure que vous avez précédemment configuré. "En savoir plus sur l'utilisation d'un point de terminaison privé Azure" .
   - **Politique de sauvegarde** : sélectionnez une politique de sauvegarde sur stockage d'objets existante ou créez-en une nouvelle.

Pour créer une politique personnalisée avant d'activer la sauvegarde, reportez-vous à"Créer une politique" .

Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

- Entrez le nom de la politique.
- Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
- Pour les politiques de sauvegarde sur objet, définissez les paramètres DataLock et Ransomware Resilience. Pour plus de détails sur DataLock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .
- Sélectionnez **Créer**.

◦ **Exporter les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage principal. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume principal.

Un compte de stockage Blob est créé dans le groupe de ressources que vous avez entré et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Sauvegardez les données ONTAP sur site sur Google Cloud Storage avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers Google Cloud Storage.

Les « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

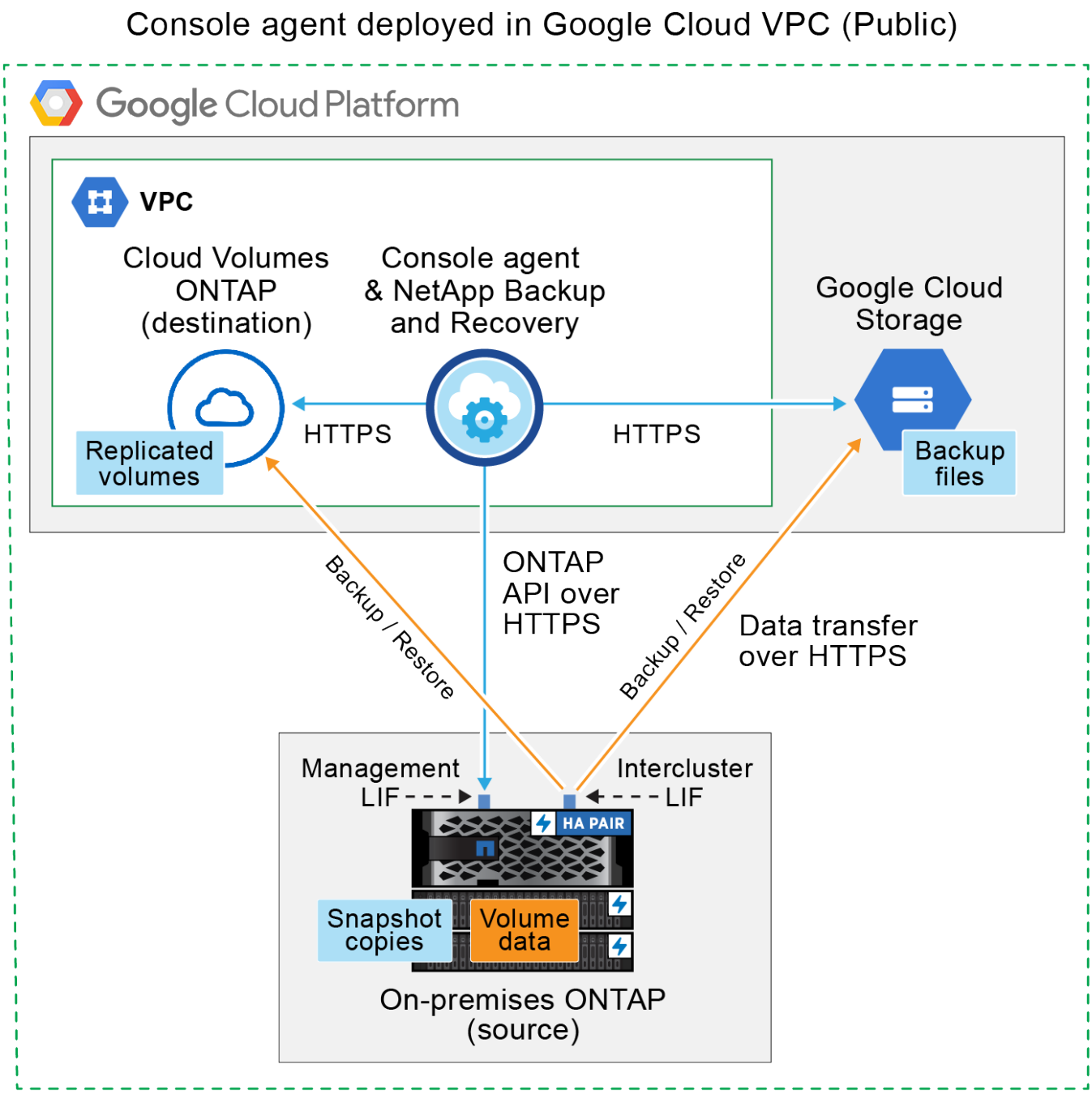
Identifier la méthode de connexion

Choisissez laquelle des deux méthodes de connexion vous utiliserez lors de la configuration des sauvegardes des systèmes ONTAP locaux vers Google Cloud Storage.

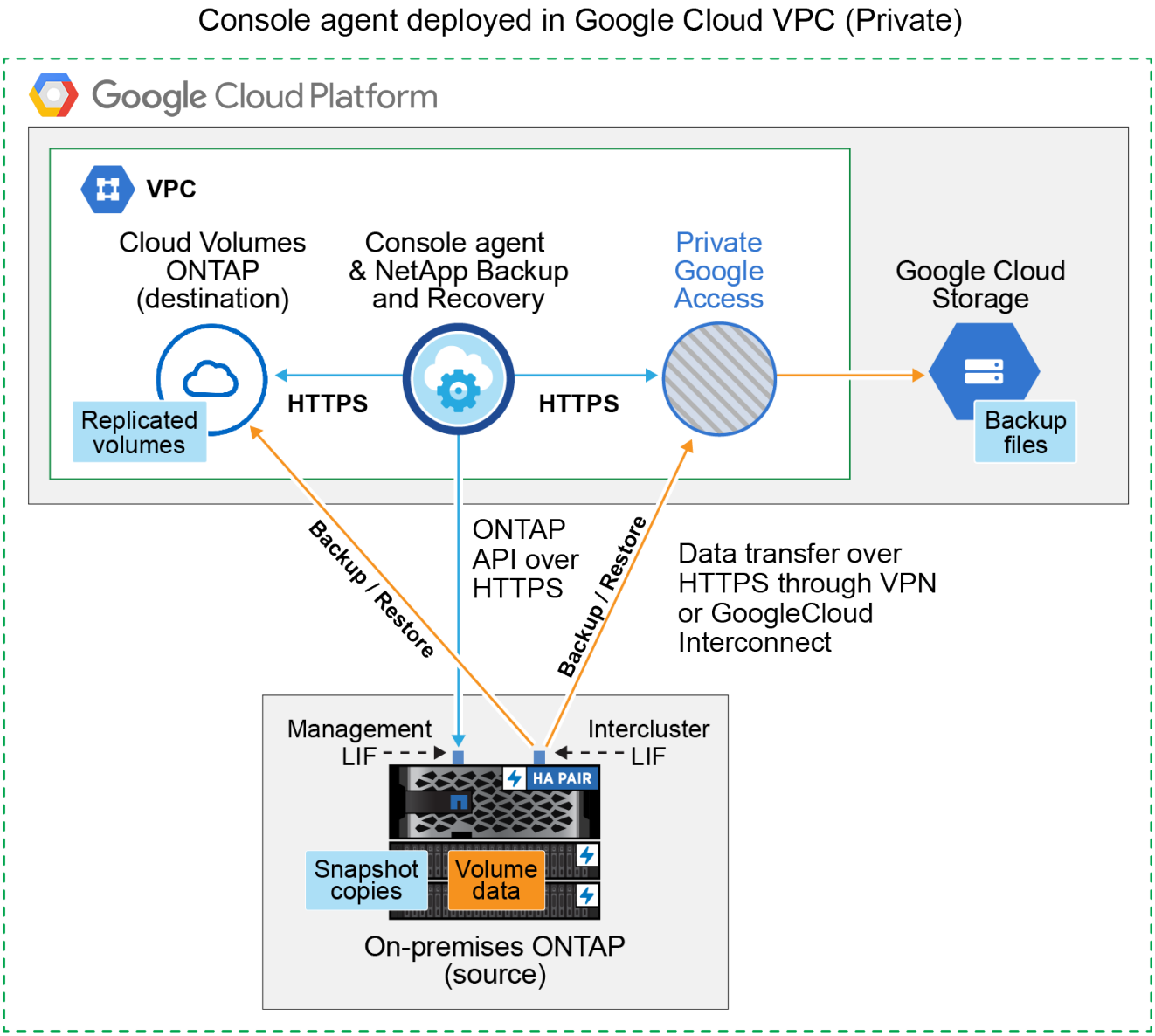
- **Connexion publique** - Connectez directement le système ONTAP à Google Cloud Storage à l'aide d'un point de terminaison Google public.
- **Connexion privée** - Utilisez un VPN ou Google Cloud Interconnect et acheminez le trafic via une interface d'accès privé Google qui utilise une adresse IP privée.

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.

Le diagramme suivant montre la méthode de **connexion publique** et les connexions que vous devez préparer entre les composants. L'agent de console doit être déployé dans le VPC Google Cloud Platform.



Le diagramme suivant montre la méthode de **connexion privée** et les connexions que vous devez préparer entre les composants. L'agent de console doit être déployé dans le VPC Google Cloud Platform.



Préparez votre agent de console

L'agent Console est le logiciel principal pour les fonctionnalités de la console. Un agent de console est requis pour sauvegarder et restaurer vos données ONTAP .

Créer ou changer d'agents de console

Si vous avez déjà un agent de console déployé dans votre VPC Google Cloud Platform, vous êtes prêt.

Sinon, vous devrez créer un agent de console à cet emplacement pour sauvegarder les données ONTAP sur Google Cloud Storage. Vous ne pouvez pas utiliser un agent de console déployé chez un autre fournisseur de cloud ou sur site.

- "En savoir plus sur les agents de console"
- "Installer un agent de console dans GCP"

Préparer la mise en réseau pour l'agent de la console

Assurez-vous que l'agent de console dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :
   - Une connexion HTTPS via le port 443 vers NetApp Backup and Recovery et vers votre stockage Google Cloud("voir la liste des points de terminaison")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
2. Activez l'accès privé à Google (ou Private Service Connect) sur le sous-réseau où vous prévoyez de déployer l'agent de console. "Accès privé à Google" ou "Connexion au service privé" sont nécessaires si vous disposez d'une connexion directe entre votre cluster ONTAP et le VPC et que vous souhaitez que la communication entre l'agent de la console et Google Cloud Storage reste dans votre réseau privé virtuel (une connexion **privée**).

   Suivez les instructions de Google pour configurer ces options d'accès privé. Assurez-vous que vos serveurs DNS ont été configurés pour pointer `www.googleapis.com` et `storage.googleapis.com` aux adresses IP internes (privées) correctes.

Vérifier ou ajouter des autorisations à l'agent de la console

Pour utiliser la fonctionnalité « Recherche et restauration » de NetApp Backup and Recovery , vous devez disposer d'autorisations spécifiques dans le rôle de l'agent de console afin qu'il puisse accéder au service Google Cloud BigQuery. Consultez les autorisations ci-dessous et suivez les étapes si vous devez modifier la politique.

Étapes

1. Dans le "Console Google Cloud" , allez à la page **Rôles**.
2. À l'aide de la liste déroulante en haut de la page, sélectionnez le projet ou l'organisation qui contient le rôle que vous souhaitez modifier.
3. Sélectionnez un rôle personnalisé.
4. Sélectionnez **Modifier le rôle** pour mettre à jour les autorisations du rôle.
5. Sélectionnez **Ajouter des autorisations** pour ajouter les nouvelles autorisations suivantes au rôle.

   ```
   bigquery.jobs.get
   bigquery.jobs.list
   bigquery.jobs.listAll
   bigquery.datasets.create
   bigquery.datasets.get
   bigquery.jobs.create
   bigquery.tables.get
   bigquery.tables.getData
   bigquery.tables.list
   bigquery.tables.create
   ```

6. Sélectionnez **Mettre à jour** pour enregistrer le rôle modifié.

Vérifier les exigences de licence

- Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez soit vous abonner à une offre de paiement à l'utilisation (PAYGO) de la Console Marketplace de Google, soit acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour les licences NetApp Backup and Recovery PAYGO, vous aurez besoin d'un abonnement au "Offre NetApp Console de Google Marketplace" . La facturation de NetApp Backup and Recovery s'effectue via cet abonnement.
  - Pour les licences BYOL de NetApp Backup and Recovery , vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .
- Vous devez disposer d'un abonnement Google pour l'espace de stockage d'objets où seront situées vos sauvegardes.

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes locaux vers Google Cloud Storage dans toutes les régions. Vous spécifiez la région où les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

Préparez votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans la NetApp Console
- Vérifier la configuration système requise ONTAP
- Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets
- Vérifier les exigences réseau ONTAP pour la réplication des volumes

Découvrez vos systèmes ONTAP dans la NetApp Console

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site doivent être disponibles sur la page **Systèmes** de la NetApp Console .

Vous devrez connaître l'adresse IP de gestion du cluster et le mot de passe du compte utilisateur administrateur pour ajouter le cluster. "Apprenez à découvrir un cluster" .

Vérifier la configuration système requise ONTAP

Assurez-vous que votre système ONTAP répond aux exigences suivantes :

- Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.
- Une licence SnapMirror (incluse dans le cadre du pack Premium ou du pack de protection des données).

  Remarque : le « Hybrid Cloud Bundle » n'est pas requis lors de l'utilisation de NetApp Backup and Recovery.

  Apprenez à "gérez vos licences de cluster" .

- L'heure et le fuseau horaire sont correctement réglés. Apprenez à "configurer l'heure de votre cluster" .
- Si vous répliquez des données, vérifiez que les systèmes source et de destination exécutent des versions ONTAP compatibles.

  "Afficher les versions ONTAP compatibles pour les relations SnapMirror".

Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage d'objets.

- Pour une architecture de sauvegarde en éventail, configurez les paramètres suivants sur le système *principal*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondaire*.

Les exigences de mise en réseau du cluster ONTAP suivantes sont nécessaires :

- Le cluster ONTAP initie une connexion HTTPS via le port 443 du LIF intercluster vers Google Cloud Storage pour les opérations de sauvegarde et de restauration.

  ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.

- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster. L'agent de la console peut résider dans un VPC Google Cloud Platform.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

  Lorsque vous configurez NetApp Backup and Recovery, vous êtes invité à indiquer l'espace IP à utiliser. Vous devez choisir l'espace IP auquel chaque LIF est associé. Il peut s'agir de l'espace IP « par défaut » ou d'un espace IP personnalisé que vous avez créé.

- Les LIF intercluster des nœuds peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .

  Si vous utilisez Private Google Access ou Private Service Connect, assurez-vous que vos serveurs DNS ont été configurés pour pointer `storage.googleapis.com` à l'adresse IP interne (privée) correcte.

- Notez que si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port 443 et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Google Cloud Storage comme cible de sauvegarde

La préparation de Google Cloud Storage comme cible de sauvegarde implique les étapes suivantes :

- Configurer les autorisations.
- (Facultatif) Créez vos propres buckets. (Le service créera des buckets pour vous si vous le souhaitez.)
- (Facultatif) Configurer des clés gérées par le client pour le chiffrement des données

Configurer les autorisations

Vous devez fournir des clés d'accès au stockage pour un compte de service disposant d'autorisations spécifiques à l'aide d'un rôle personnalisé. Un compte de service permet à NetApp Backup and Recovery d'authentifier et d'accéder aux buckets Cloud Storage utilisés pour stocker les sauvegardes. Les clés sont nécessaires pour que Google Cloud Storage sache qui fait la demande.

Étapes

1. Dans le "Console Google Cloud" , allez à la page **Rôles**.
2. "Créer un nouveau rôle"avec les autorisations suivantes :

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Dans la console Google Cloud, "aller à la page Comptes de service" .
4. Sélectionnez votre projet Cloud.
5. Sélectionnez **Créer un compte de service** et fournissez les informations requises :
   a. **Détails du compte de service** : saisissez un nom et une description.
   b. **Accorder à ce compte de service l'accès au projet** : sélectionnez le rôle personnalisé que vous venez de créer.
   c. Sélectionnez **Terminé**.
6. Aller à "Paramètres de stockage GCP" et créez des clés d'accès pour le compte de service :
   a. Sélectionnez un projet et sélectionnez **Interopérabilité**. Si vous ne l'avez pas déjà fait, sélectionnez **Activer l'accès à l'interopérabilité**.
   b. Sous **Clés d'accès pour les comptes de service**, sélectionnez **Créer une clé pour un compte de service**, sélectionnez le compte de service que vous venez de créer et cliquez sur **Créer une clé**.

      Vous devrez saisir les clés dans NetApp Backup and Recovery ultérieurement lorsque vous configurerez le service de sauvegarde.

Créez vos propres seaux

Par défaut, le service crée des buckets pour vous. Ou, si vous souhaitez utiliser vos propres buckets, vous pouvez les créer avant de démarrer l'assistant d'activation de sauvegarde, puis sélectionner ces buckets dans l'assistant.

"En savoir plus sur la création de vos propres buckets".

Configurer des clés de chiffrement gérées par le client (CMEK) pour le chiffrement des données

Vous pouvez utiliser vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés de chiffrement par défaut gérées par Google. Les clés inter-régions et inter-projets sont prises en charge, vous pouvez donc choisir un projet pour un bucket différent du projet de la clé CMEK.

Si vous prévoyez d'utiliser vos propres clés gérées par le client :

- Vous aurez besoin du trousseau de clés et du nom de la clé pour pouvoir ajouter ces informations dans l'assistant d'activation. "En savoir plus sur les clés de chiffrement gérées par le client" .
- Vous devrez vérifier que ces autorisations requises sont incluses dans le rôle de l'agent de console :

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Vous devrez vérifier que l'API Google « Cloud Key Management Service (KMS) » est activée dans votre projet. Voir le "Documentation Google Cloud : Activation des API" pour plus de détails.

Considérations CMEK :

- Les clés HSM (protégées par le matériel) et les clés générées par logiciel sont prises en charge.
- Les clés Cloud KMS nouvellement créées ou importées sont prises en charge.
- Seules les clés régionales sont prises en charge, les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif « Cryptage/décryptage symétrique » est pris en charge.
- L'agent de service associé au compte de stockage se voit attribuer le rôle IAM « CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter) » par NetApp Backup and Recovery.

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez également Afficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté de Sauvegarde et récupération dans le panneau de droite.

     Si la destination Google Cloud Storage pour vos sauvegardes existe comme sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets Google Cloud.

   - Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez les **Actions*** ••• **icône et sélectionnez *Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer à Préparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.
   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : snapshots locaux, réplication et sauvegarde sur stockage d'objets
- Architecture
- Politique d'instantané local
- Cible et politique de réplication

Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes sur le stockage d'objets.
2. **Architecture** : Si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :

- **En cascade** : les informations circulent du primaire vers le secondaire et du secondaire vers le stockage d'objets.
- **Fan out** : les informations circulent du primaire vers le secondaire *et* du primaire vers le stockage d'objets.

  Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .

3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

   Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une nouvelle.

     Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Google Cloud**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région où les sauvegardes seront stockées.

     Créez un nouveau bucket ou sélectionnez-en un que vous avez déjà créé.

     Si vous souhaitez hiérarchiser les fichiers de sauvegarde plus anciens vers le stockage Google Cloud Archive pour une optimisation supplémentaire des coûts, assurez-vous que le bucket dispose de la règle de cycle de vie appropriée.

     Saisissez la clé d'accès et la clé secrète de Google Cloud.
   - **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Google Cloud, saisissez les informations de clé de chiffrement fournies par le fournisseur. Choisissez si vous utiliserez les clés de chiffrement par défaut de Google Cloud ou si vous choisirez vos propres clés gérées par le client à partir de votre compte Google Cloud pour gérer le chiffrement de vos données.

Si vous avez choisi un compte de stockage Google Cloud existant, les informations de chiffrement sont déjà disponibles, vous n'avez donc pas besoin de les saisir maintenant.

Si vous choisissez d'utiliser vos propres clés gérées par le client, saisissez le trousseau et le nom de la clé. "En savoir plus sur les clés de chiffrement gérées par le client" .

- **Réseau** : Choisissez l'espace IP.

  L'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.

- **Politique de sauvegarde** : sélectionnez une politique de sauvegarde sur stockage d'objets existante ou créez-en une nouvelle.

  Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

  Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

  - Entrez le nom de la politique.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

- **Exporter les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage principal. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume source.

Un bucket Google Cloud Storage est créé automatiquement dans le compte de service indiqué par la clé d'accès Google et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Sauvegardez les données ONTAP sur site vers ONTAP S3 avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos principaux systèmes ONTAP sur site. Vous pouvez envoyer des sauvegardes vers un système de stockage ONTAP secondaire (un volume répliqué) ou vers un bucket sur un système ONTAP configuré comme serveur S3 (un fichier de sauvegarde), ou les deux.

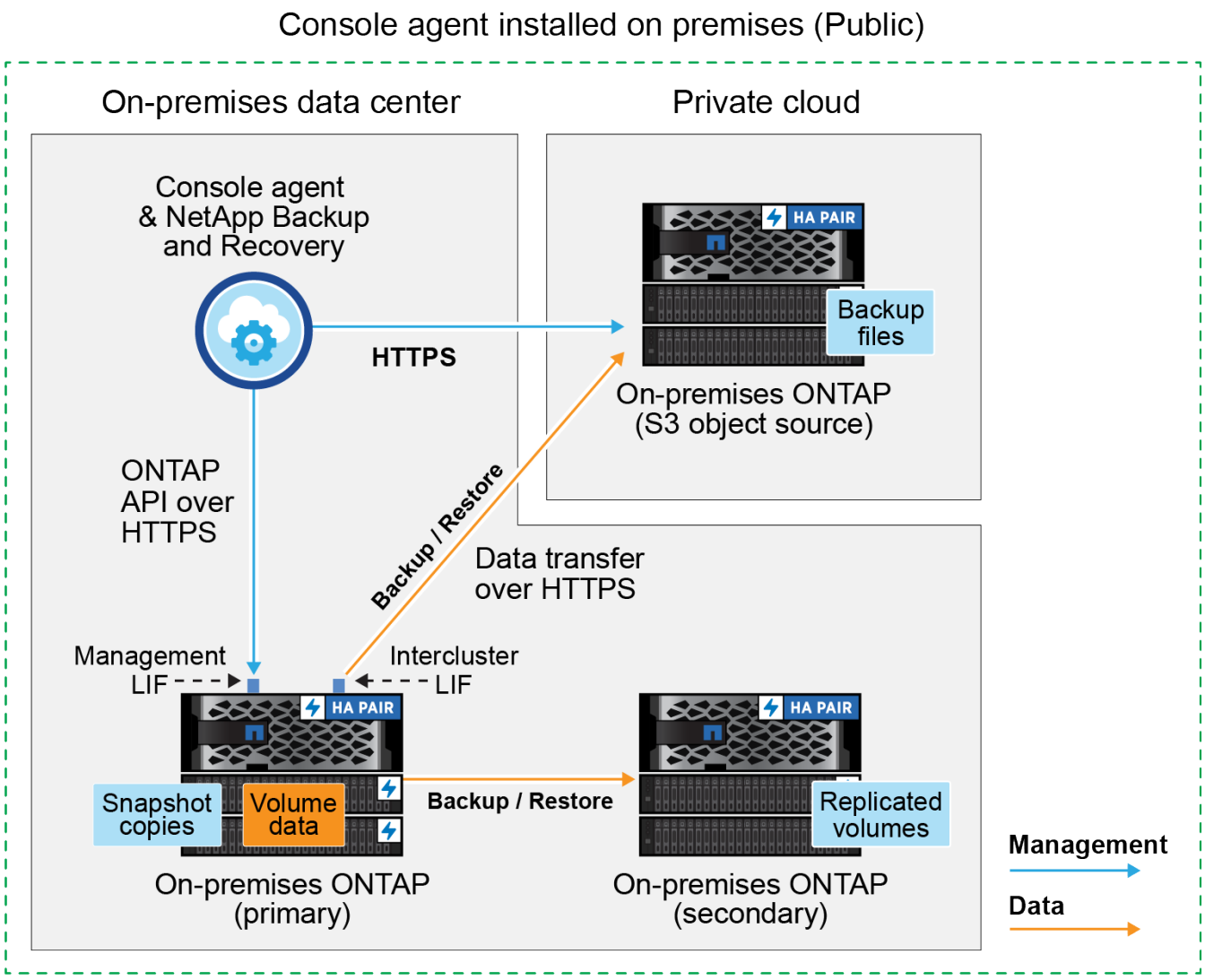
Le système ONTAP principal sur site peut être un système FAS, AFF ou ONTAP Select . Le système ONTAP secondaire peut être un système ONTAP local ou Cloud Volumes ONTAP . Le stockage d'objets peut se trouver sur un système ONTAP local ou sur un système Cloud Volumes ONTAP sur lequel vous avez activé un serveur de stockage d'objets Simple Storage Service (S3).

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Identifier la méthode de connexion

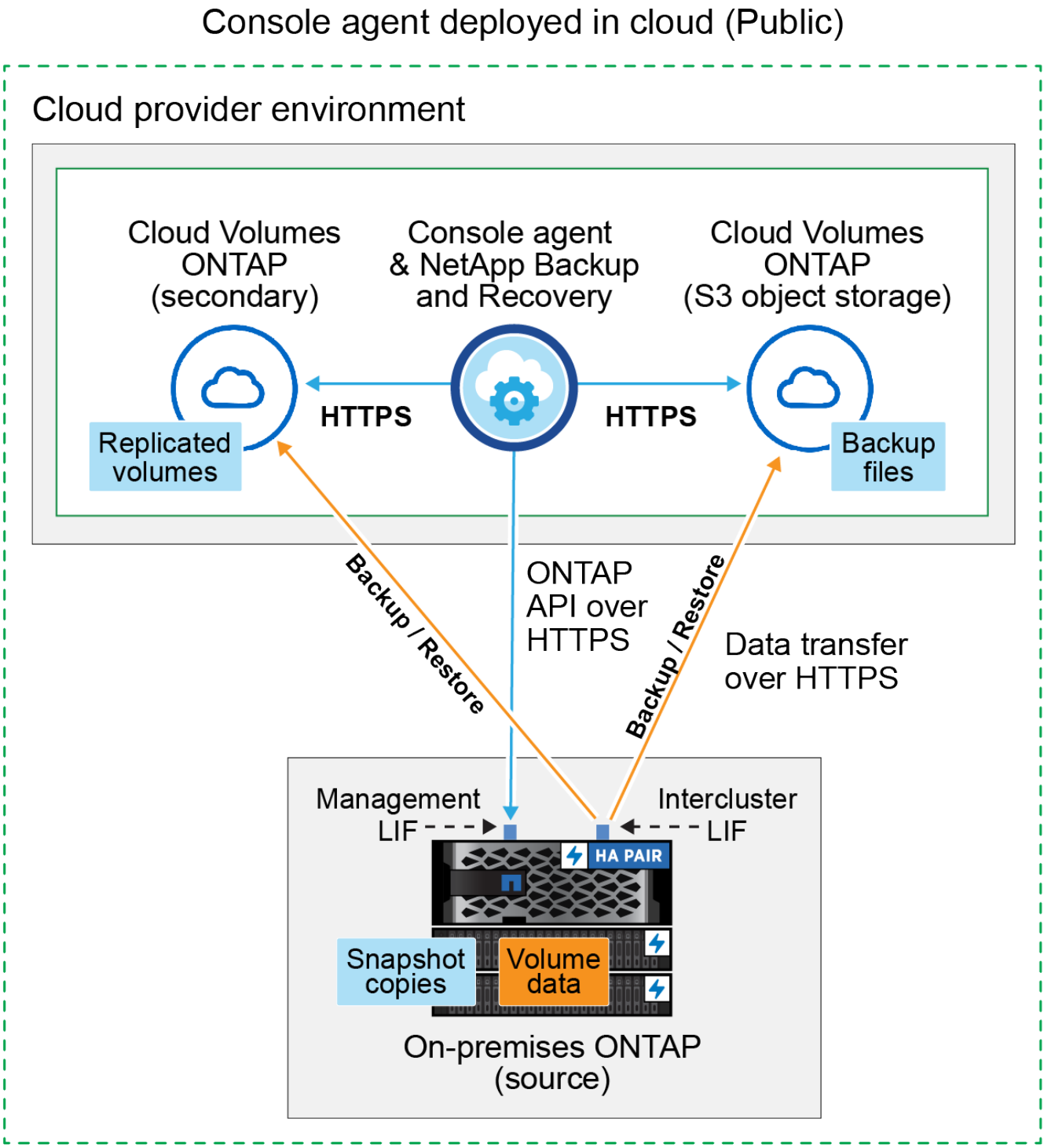
Il existe de nombreuses configurations dans lesquelles vous pouvez créer des sauvegardes dans un bucket S3 sur un système ONTAP . Deux scénarios sont présentés ci-dessous.

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP principal sur site vers un système ONTAP sur site configuré pour S3 et les connexions que vous devez préparer entre eux. Il montre également une connexion à un système ONTAP secondaire dans le même emplacement sur site pour répliquer les volumes.



Lorsque l'agent de console et le système ONTAP principal sur site sont installés dans un emplacement sur site sans accès Internet (déploiement en mode « privé »), le système ONTAP S3 doit être situé dans le même centre de données sur site.

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP principal sur site vers un système Cloud Volumes ONTAP configuré pour S3 et les connexions que vous devez préparer entre eux. Il montre également une connexion à un système Cloud Volumes ONTAP secondaire dans le même environnement de fournisseur de cloud pour répliquer les volumes.



Dans ce scénario, l'agent de console doit être déployé dans le même environnement de fournisseur de cloud dans lequel les systèmes Cloud Volumes ONTAP sont déployés.

Préparez votre agent de console

L'agent Console est le logiciel principal pour les fonctionnalités de la console. Un agent de console est requis pour sauvegarder et restaurer vos données ONTAP .

Créer ou changer d'agents de console

Lorsque vous sauvegardez des données sur ONTAP S3, un agent de console doit être disponible sur vos locaux ou dans le cloud. Vous devrez soit installer un nouvel agent de console, soit vous assurer que l'agent de console actuellement sélectionné réside dans l'un de ces emplacements. L'agent de console sur site peut être installé sur un site avec ou sans accès Internet.

- "En savoir plus sur les agents de console"
- "Installez l'agent de console dans votre environnement cloud"
- "Installation de l'agent de console sur un hôte Linux avec accès Internet"
- "Installation de l'agent Console sur un hôte Linux sans accès Internet"
- "Basculer entre les agents de la console"

Préparer les exigences réseau de l'agent de console

Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :

- Une connexion HTTPS sur le port 443 vers le serveur ONTAP S3
- Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP source
- Une connexion Internet sortante via le port 443 vers NetApp Backup and Recovery (non requise lorsque l'agent de console est installé sur un site « sombre »)

Considérations sur le mode privé (site sombre)

La fonctionnalité de NetApp Backup and Recovery est intégrée à l'agent de la console. Lorsqu'il est installé en mode privé, vous devrez mettre à jour périodiquement le logiciel de l'agent de la console pour accéder aux nouvelles fonctionnalités. Vérifiez le"Nouveautés de NetApp Backup and Recovery" pour voir les nouvelles fonctionnalités de chaque version de NetApp Backup and Recovery . Lorsque vous souhaitez utiliser les nouvelles fonctionnalités, suivez les étapes pour "mettre à niveau le logiciel de l'agent de la console" .

Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS standard, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le cloud. Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le compartiment ONTAP S3 où vos sauvegardes sont stockées.

Vérifier les exigences de licence

Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. La licence concerne la sauvegarde et la restauration sur stockage objet ; aucune licence n'est nécessaire pour créer des instantanés ou des volumes répliqués. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

Vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .

La licence PAYGO n'est pas prise en charge lors de la sauvegarde de fichiers sur ONTAP S3.

Préparez vos clusters ONTAP

Préparez votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans la NetApp Console
- Vérifier la configuration système requise ONTAP
- Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets
- Vérifier les exigences réseau ONTAP pour la réplication des volumes

Découvrez vos systèmes ONTAP dans la NetApp Console

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site doivent être disponibles sur la page **Systèmes** de la NetApp Console .

Vous devrez connaître l'adresse IP de gestion du cluster et le mot de passe du compte utilisateur administrateur pour ajouter le cluster. "Apprenez à découvrir un cluster" .

Vérifier la configuration système requise ONTAP

Assurez-vous que votre système ONTAP répond aux exigences suivantes :

- Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.
- Une licence SnapMirror (incluse dans le cadre du pack Premium ou du pack de protection des données).

  Remarque : le « Hybrid Cloud Bundle » n'est pas requis lors de l'utilisation de NetApp Backup and Recovery.

  Apprenez à "gérez vos licences de cluster" .
- L'heure et le fuseau horaire sont correctement réglés. Apprenez à "configurer l'heure de votre cluster" .
- Si vous répliquez des données, vérifiez que les systèmes source et de destination exécutent des versions ONTAP compatibles.

  "Afficher les versions ONTAP compatibles pour les relations SnapMirror".

Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets

Vous devez vous assurer que les exigences suivantes sont respectées sur le système qui se connecte au stockage d'objets.

- Lorsque vous utilisez une architecture de sauvegarde en éventail, les paramètres doivent être configurés sur le système de stockage *principal*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres doivent être configurés sur le système de stockage *secondaire*.

  "En savoir plus sur les types d'architecture de sauvegarde".

Les exigences de mise en réseau du cluster ONTAP suivantes sont nécessaires :

- Le cluster ONTAP initie une connexion HTTPS via un port spécifié par l'utilisateur depuis le LIF intercluster vers le serveur ONTAP S3 pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.

- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

  Lorsque vous configurez NetApp Backup and Recovery, vous êtes invité à indiquer l'espace IP à utiliser. Vous devez choisir l'espace IP auquel chaque LIF est associé. Il peut s'agir de l'espace IP « par défaut » ou d'un espace IP personnalisé que vous avez créé.

- Les LIF intercluster des nœuds peuvent accéder au magasin d'objets (non requis lorsque l'agent de console est installé sur un site « sombre »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions du service NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez ONTAP S3 comme cible de sauvegarde

Vous devez activer un serveur de stockage d'objets Simple Storage Service (S3) dans le cluster ONTAP que vous prévoyez d'utiliser pour les sauvegardes de stockage d'objets. Voir le "Documentation ONTAP S3" pour plus de détails.

Remarque : vous pouvez ajouter ce cluster à la page **Systèmes** de la console, mais il n'est pas identifié comme étant un serveur de stockage d'objets S3 et vous ne pouvez pas glisser-déposer un système source sur ce système S3 pour lancer l'activation de la sauvegarde.

Ce système ONTAP doit répondre aux exigences suivantes.

Versions ONTAP prises en charge

ONTAP 9.8 et versions ultérieures sont requis pour les systèmes ONTAP sur site. ONTAP 9.9.1 et versions ultérieures sont requis pour les systèmes Cloud Volumes ONTAP .

Informations d'identification S3

Vous devez avoir créé un utilisateur S3 pour contrôler l'accès à votre stockage ONTAP S3. "Consultez la documentation ONTAP S3 pour plus de détails" .

Lorsque vous configurez la sauvegarde sur ONTAP S3, l'assistant de sauvegarde vous demande une clé d'accès S3 et une clé secrète pour un compte utilisateur. Le compte utilisateur permet à NetApp Backup and Recovery d'authentifier et d'accéder aux buckets ONTAP S3 utilisés pour stocker les sauvegardes. Les clés sont nécessaires pour ONTAP S3 sache qui fait la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket",
"s3:GetBucketLocation"
```

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie et les politiques de sauvegarde
- Revoyez vos sélections

Vous pouvez égalementAfficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

    - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté de Sauvegarde et récupération dans le panneau de droite.

- Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez l'option **Actions (…)** et sélectionnez **Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, les réplications et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous n'avez pas d'agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers un objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Notez que si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.
   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique la configuration des options suivantes :

- Options de protection : si vous souhaitez implémenter une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur le stockage d'objets
- Architecture : si vous souhaitez utiliser une architecture de sauvegarde en éventail ou en cascade
- Politique d'instantané local
- Cible et politique de réplication

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - **Instantanés locaux** : Crée des instantanés locaux.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes dans un bucket sur un système ONTAP configuré pour S3.
2. **Architecture** : Si vous avez choisi à la fois la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les données de sauvegarde circulent du système principal vers le système secondaire, puis du système secondaire vers le stockage d'objets.
   - **Fan out** : les données de sauvegarde circulent du système principal vers le système secondaire *et* du système principal vers le stockage d'objets.

     Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

   Si vous souhaitez créer une politique personnalisée avant d'activer le Snapshot, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP. `snapmirror policy create` commande. Se référer à .

   Pour créer une politique personnalisée à l'aide de Sauvegarde et récupération, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : Si vous avez sélectionné **Réplication**, définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat de destination (ou les agrégats pour les volumes FlexGroup) et un préfixe ou un suffixe qui sera ajouté au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une nouvelle.

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : Sélectionnez * ONTAP S3*.
   - **Paramètres du fournisseur** : saisissez les détails du nom de domaine complet (FQDN) du serveur

S3, le port, ainsi que la clé d'accès et la clé secrète des utilisateurs.

La clé d'accès et la clé secrète sont destinées à l'utilisateur que vous avez créé pour donner au cluster ONTAP l'accès au bucket S3.

- **Mise en réseau** : choisissez l'espace IP dans le cluster ONTAP source où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant (non requis lorsque l'agent de console est installé sur un site « sombre »).

  La sélection de l'espace IP correct garantit que NetApp Backup and Recovery peut établir une connexion d' ONTAP à votre stockage d'objets ONTAP S3.

- **Politique de sauvegarde** : sélectionnez une politique de sauvegarde existante ou créez-en une nouvelle.

  Vous pouvez créer une politique avec System Manager ou l'interface de ligne de commande ONTAP . Pour créer une politique personnalisée à l'aide de l'interface de ligne de commande ONTAP `snapmirror policy create` commande, se référer à .

  Pour créer une politique personnalisée à l'aide de Sauvegarde et récupération, reportez-vous à"Créer une politique" .

  Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

  - Entrez le nom de la politique.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Pour les politiques de sauvegarde sur objet, définissez les paramètres DataLock et Ransomware Resilience. Pour plus de détails sur DataLock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .
  - Sélectionnez **Créer**.

- **Exporter les instantanés existants vers le stockage objet en tant que fichiers de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde. Si les politiques ne correspondent pas, les sauvegardes ne seront pas créées.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données sources. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume de stockage principal.

Un compartiment S3 est créé dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés.

Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Sauvegardez les données ONTAP sur site sur StorageGRID avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers le stockage d'objets dans vos systèmes NetApp StorageGRID .

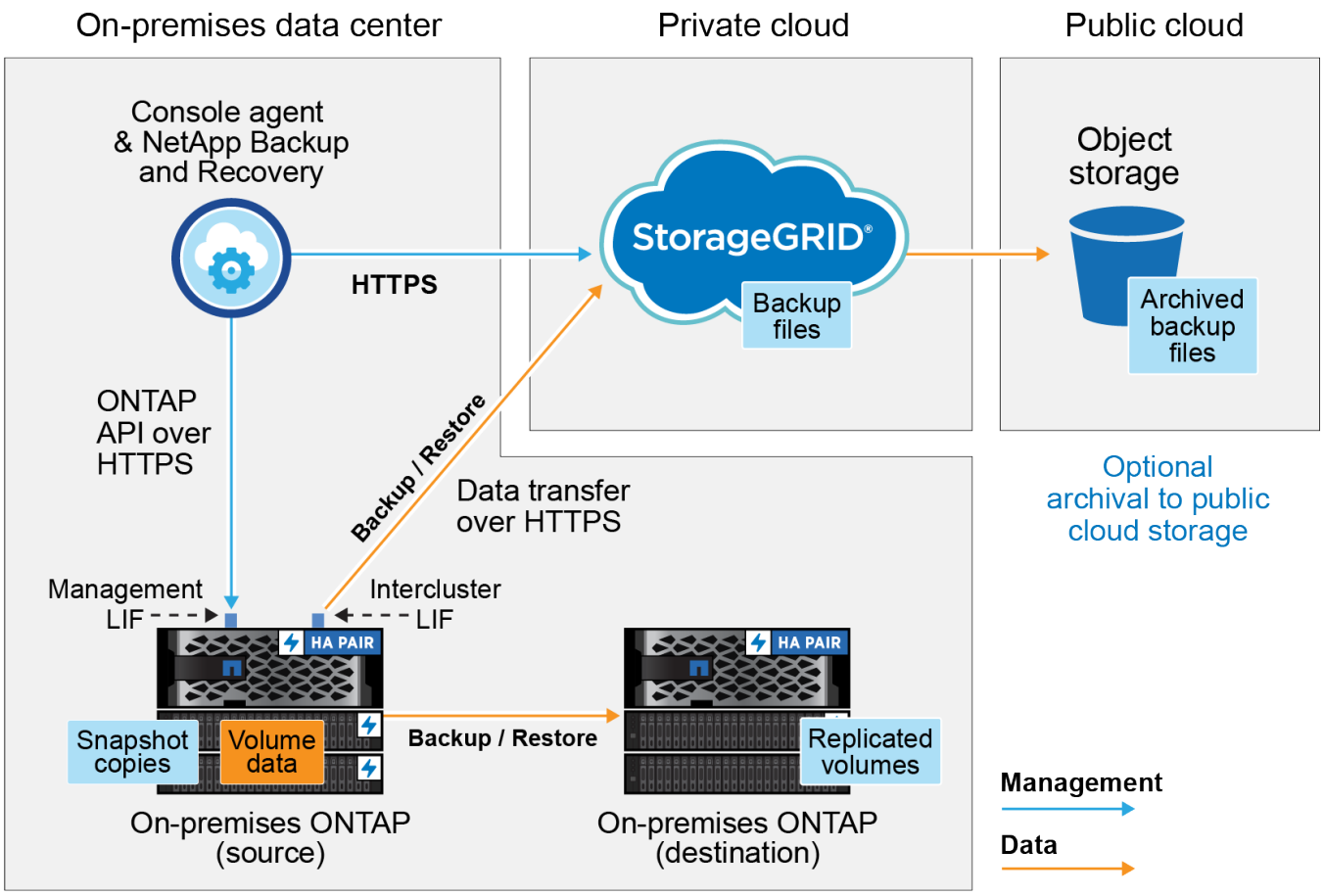
Les « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Identifier la méthode de connexion

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP sur site sur StorageGRID et les connexions que vous devez préparer entre eux.

En option, vous pouvez vous connecter à un système ONTAP secondaire dans le même emplacement sur site pour répliquer les volumes.



Lorsque l'agent de console et le système ONTAP sur site sont installés dans un emplacement sur site sans accès Internet (un « site sombre »), le système StorageGRID doit être situé dans le même centre de données sur site. L'archivage des anciens fichiers de sauvegarde dans le cloud public n'est pas pris en charge dans les configurations de site sombre.

Préparez votre agent de console

L'agent Console est le logiciel principal pour les fonctionnalités de la console. Un agent de console est requis pour sauvegarder et restaurer vos données ONTAP .

Créer ou changer d'agents de console

Lorsque vous sauvegardez des données sur StorageGRID, un agent de console doit être disponible dans vos locaux. Vous devrez soit installer un nouvel agent de console, soit vous assurer que l'agent de console actuellement sélectionné réside sur site. L'agent Console peut être installé sur un site avec ou sans accès Internet.

- "En savoir plus sur les agents de console"
- "Installation de l'agent de console sur un hôte Linux avec accès Internet"
- "Installation de l'agent Console sur un hôte Linux sans accès Internet"
- "Basculer entre les agents de la console"

Préparer les exigences réseau de l'agent de console

Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :

- Une connexion HTTPS via le port 443 vers le nœud de passerelle StorageGRID
- Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
- Une connexion Internet sortante via le port 443 vers NetApp Backup and Recovery (non requise lorsque l'agent de console est installé sur un site « sombre »)

Considérations sur le mode privé (site sombre)

- La fonctionnalité de NetApp Backup and Recovery est intégrée à l'agent de la console. Lorsqu'il est installé en mode privé, vous devrez mettre à jour périodiquement le logiciel de l'agent de la console pour accéder aux nouvelles fonctionnalités. Vérifiez le"Nouveautés de NetApp Backup and Recovery" pour voir les nouvelles fonctionnalités de chaque version de NetApp Backup and Recovery . Lorsque vous souhaitez utiliser les nouvelles fonctionnalités, suivez les étapes pour "mettre à niveau le logiciel de l'agent de la console" .

  La nouvelle version de NetApp Backup and Recovery , qui inclut la possibilité de planifier et de créer des instantanés et des volumes répliqués, en plus de créer des sauvegardes sur le stockage d'objets, nécessite que vous utilisiez la version 3.9.31 ou supérieure de l'agent Console. Il est donc recommandé d'obtenir cette dernière version pour gérer toutes vos sauvegardes.

- Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le cloud. Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le bucket StorageGRID où vos sauvegardes sont stockées.

Vérifier les exigences de licence

Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

Vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .

La licence PAYGO n'est pas prise en charge lors de la sauvegarde de fichiers sur StorageGRID.

Préparez vos clusters ONTAP

Préparez votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans la NetApp Console
- Vérifier la configuration système requise ONTAP
- Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets
- Vérifier les exigences réseau ONTAP pour la réplication des volumes

Découvrez vos systèmes ONTAP dans la NetApp Console

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site doivent être disponibles sur la page **Systèmes** de la NetApp Console .

Vous devrez connaître l'adresse IP de gestion du cluster et le mot de passe du compte utilisateur administrateur pour ajouter le cluster. "Apprenez à découvrir un cluster" .

Vérifier la configuration système requise ONTAP

Assurez-vous que votre système ONTAP répond aux exigences suivantes :

- Minimum ONTAP 9.8 ; ONTAP 9.8P13 et versions ultérieures sont recommandés.
- Une licence SnapMirror (incluse dans le cadre du pack Premium ou du pack de protection des données).

  Remarque : le « Hybrid Cloud Bundle » n'est pas requis lors de l'utilisation de NetApp Backup and Recovery.

  Apprenez à "gérez vos licences de cluster" .
- L'heure et le fuseau horaire sont correctement réglés. Apprenez à "configurer l'heure de votre cluster" .
- Si vous répliquez des données, vérifiez que les systèmes source et de destination exécutent des versions ONTAP compatibles.

  "Afficher les versions ONTAP compatibles pour les relations SnapMirror".

Vérifier les exigences réseau ONTAP pour la sauvegarde des données sur le stockage d'objets

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage d'objets.

- Lorsque vous utilisez une architecture de sauvegarde en éventail, les paramètres suivants doivent être configurés sur le système de stockage *principal*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres suivants doivent être configurés sur le système de stockage *secondaire*.

Les exigences de mise en réseau du cluster ONTAP suivantes sont nécessaires :

- Le cluster ONTAP initie une connexion HTTPS via un port spécifié par l'utilisateur depuis le LIF intercluster vers le nœud de passerelle StorageGRID pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

  ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.
- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster. L'agent de la console doit résider dans vos locaux.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

  Lorsque vous configurez NetApp Backup and Recovery, vous êtes invité à indiquer l'espace IP à utiliser. Vous devez choisir l'espace IP auquel chaque LIF est associé. Il peut s'agir de l'espace IP « par défaut » ou d'un espace IP personnalisé que vous avez créé.

- Les LIF intercluster des nœuds peuvent accéder au magasin d'objets (non requis lorsque l'agent de console est installé sur un site « sombre »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions du service NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de NetApp Backup and Recovery, assurez-vous que les systèmes source et de destination répondent aux exigences réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster est sur site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel chez le fournisseur de cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en matière de sous-réseau, de port, de pare-feu et de cluster.

  Étant donné que vous pouvez répliquer vers Cloud Volumes ONTAP ou vers des systèmes locaux, examinez les exigences de peering pour les systèmes ONTAP locaux. "Consultez les conditions préalables pour le peering de cluster dans la documentation ONTAP" .

Exigences réseau de Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles entrantes et sortantes requises : en particulier, les règles pour ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez StorageGRID comme cible de sauvegarde

StorageGRID doit répondre aux exigences suivantes. Voir le "Documentation de StorageGRID" pour plus d'informations.

Pour plus de détails sur les exigences de résilience DataLock et Ransomware pour StorageGRID, reportez-vous à"Options de politique de sauvegarde sur objet" .

Versions de StorageGRID prises en charge

StorageGRID 10.3 et versions ultérieures sont pris en charge.

Pour utiliser DataLock & Ransomware Resilience pour vos sauvegardes, vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou supérieure.

Pour hiérarchiser les sauvegardes plus anciennes vers le stockage d'archivage cloud, vos systèmes StorageGRID doivent exécuter la version 11.3 ou supérieure. De plus, vos systèmes StorageGRID doivent être découverts sur la page **Systèmes** de la console.

Pour le stockage d'archives des utilisateurs, un accès IP au nœud d'administration est nécessaire.

L'accès IP de la passerelle est toujours nécessaire.

Informations d'identification S3

Vous devez avoir créé un compte locataire S3 pour contrôler l'accès à votre stockage StorageGRID . "Consultez la documentation StorageGRID pour plus de détails" .

Lorsque vous configurez la sauvegarde sur StorageGRID, l'assistant de sauvegarde vous demande une clé d'accès S3 et une clé secrète pour un compte de locataire. Le compte locataire permet à NetApp Backup and Recovery d'authentifier et d'accéder aux buckets StorageGRID utilisés pour stocker les sauvegardes. Les clés sont nécessaires pour que StorageGRID sache qui fait la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Versionnage d'objet

Vous ne devez pas activer manuellement le contrôle de version des objets StorageGRID sur le bucket du magasin d'objets.

Préparez-vous à archiver les anciens fichiers de sauvegarde sur un stockage cloud public

La hiérarchisation des fichiers de sauvegarde plus anciens vers un stockage d'archives permet d'économiser de l'argent en utilisant une classe de stockage moins coûteuse pour les sauvegardes dont vous n'avez peut-être pas besoin. StorageGRID est une solution sur site (cloud privé) qui ne fournit pas de stockage d'archives, mais vous pouvez déplacer des fichiers de sauvegarde plus anciens vers un stockage d'archives dans le cloud public. Lorsqu'elles sont utilisées de cette manière, les données hiérarchisées vers le stockage cloud ou restaurées à partir du stockage cloud transitent entre StorageGRID et le stockage cloud - la console n'est pas impliquée dans ce transfert de données.

La prise en charge actuelle vous permet d'archiver les sauvegardes sur le stockage AWS *S3 Glacier*/*S3 Glacier Deep Archive* ou *Azure Archive*.

- Exigences ONTAP *
- Votre cluster doit utiliser ONTAP 9.12.1 ou une version ultérieure.
- Exigences de StorageGRID *
- Votre StorageGRID doit utiliser la version 11.4 ou supérieure.
- Votre StorageGRID doit être "découvert et disponible dans la console" .

Exigences Amazon S3

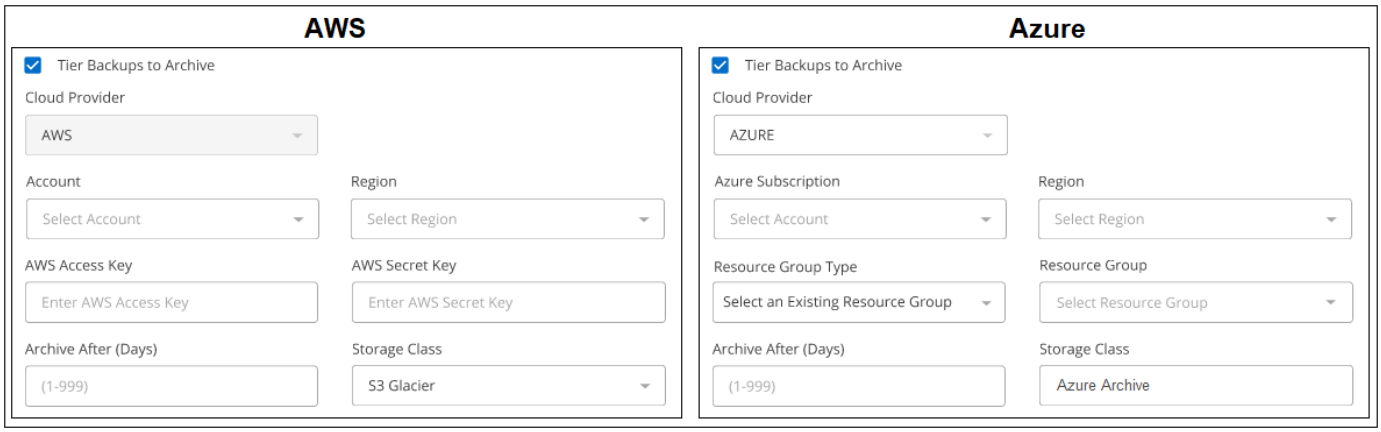
- Vous devrez créer un compte Amazon S3 pour l'espace de stockage où seront situées vos sauvegardes archivées.

- Vous pouvez choisir de hiérarchiser les sauvegardes vers le stockage AWS S3 Glacier ou S3 Glacier Deep Archive. "En savoir plus sur les niveaux d'archivage AWS" .
- StorageGRID doit avoir un accès de contrôle total au bucket(`s3:*`); cependant, si cela n'est pas possible, la politique de bucket doit accorder les autorisations S3 suivantes à StorageGRID:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Exigences Azure Blob

- Vous devrez souscrire à un abonnement Azure pour l'espace de stockage où seront situées vos sauvegardes archivées.
- L'assistant d'activation vous permet d'utiliser un groupe de ressources existant pour gérer le conteneur Blob qui stockera les sauvegardes, ou vous pouvez créer un nouveau groupe de ressources.

Lors de la définition des paramètres d'archivage pour la politique de sauvegarde de votre cluster, vous entrez les informations d'identification de votre fournisseur de cloud et sélectionnez la classe de stockage que vous souhaitez utiliser. NetApp Backup and Recovery crée le bucket cloud lorsque vous activez la sauvegarde pour le cluster. Les informations requises pour le stockage d'archives AWS et Azure sont présentées ci-dessous.



Les paramètres de politique d'archivage que vous sélectionnez généreront une politique de gestion du cycle de vie des informations (ILM) dans StorageGRID et ajouteront les paramètres en tant que « règles ».

- S'il existe une politique ILM active, de nouvelles règles seront ajoutées à la politique ILM pour déplacer les données vers le niveau d'archivage.
- S'il existe une politique ILM existante à l'état « proposé », la création et l'activation d'une nouvelle politique ILM ne seront pas possibles. "En savoir plus sur les politiques et règles ILM de StorageGRID" .

Activer les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre système sur site.

Un assistant vous guide à travers les principales étapes suivantes :

- Sélectionnez les volumes que vous souhaitez sauvegarder
- Définir la stratégie de sauvegarde
- Revoyez vos sélections

Vous pouvez égalementAfficher les commandes de l'API à l'étape de révision, vous pouvez donc copier le code pour automatiser l'activation de la sauvegarde pour les futurs systèmes.

Démarrer l'assistant

Étapes

1. Accédez à l'assistant d'activation de sauvegarde et de récupération en utilisant l'une des méthodes suivantes :

   - Depuis la page **Systèmes** de la console, sélectionnez le système et sélectionnez **Activer > Volumes de sauvegarde** à côté de Sauvegarde et récupération dans le panneau de droite.

     Si la destination de vos sauvegardes existe en tant que système sur la page **Systèmes** de la console, vous pouvez faire glisser le cluster ONTAP sur le stockage d'objets.

   - Sélectionnez **Volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez l'option **Actions (…)** et sélectionnez **Activer la sauvegarde** pour un seul volume (qui n'a pas déjà la réplication ou la sauvegarde vers le stockage d'objets activée).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page Définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un agent de console, vous êtes prêt. Sélectionnez simplement **Suivant**.
   - Si vous ne disposez pas encore d'un agent de console, l'option **Ajouter un agent de console** apparaît. Se référer àPréparez votre agent de console .

Sélectionnez les volumes que vous souhaitez sauvegarder

Choisissez les volumes que vous souhaitez protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup ; cependant, vous ne pouvez pas sélectionner une combinaison de ces volumes lors de l'activation de la sauvegarde pour un système. Découvrez comment"activer la sauvegarde pour des volumes supplémentaires dans le système" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes que vous sélectionnez doivent avoir le même paramètre SnapLock . SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner les volumes, sélectionnez le ou les volumes que vous souhaitez protéger.
   - Vous pouvez également filtrer les lignes pour afficher uniquement les volumes avec certains types de volumes, styles et plus encore pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique de définir les options suivantes :

- Que vous souhaitiez une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur stockage d'objets
- Architecture
- Politique d'instantané local
- Cible et politique de réplication

> Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde des informations de stockage d'objets (fournisseur, cryptage, mise en réseau, politique de sauvegarde et options d'exportation).

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - * Instantanés locaux * : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes sur le stockage d'objets.
2. **Architecture** : Si vous avez choisi à la fois la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les informations circulent du primaire au secondaire, puis du secondaire au stockage d'objets.
   - **Fan out** : les informations circulent du primaire vers le secondaire *et* du primaire vers le stockage d'objets.

     Pour plus de détails sur ces architectures, reportez-vous à"Planifiez votre voyage de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

- Entrez le nom de la politique.
- Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
- Sélectionnez **Créer**.

4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une.

     Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : Sélectionnez * StorageGRID*.
   - **Paramètres du fournisseur** : saisissez les détails du nom de domaine complet (FQDN), le port, la clé d'accès et la clé secrète du nœud de passerelle du fournisseur.

     La clé d'accès et la clé secrète sont destinées à l'utilisateur IAM que vous avez créé pour donner au cluster ONTAP l'accès au bucket.

   - **Mise en réseau** : Choisissez l'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant (non requis lorsque l'agent de console est installé sur un site « sombre »).

     La sélection de l'espace IP correct garantit que NetApp Backup and Recovery peut établir une connexion d' ONTAP à votre stockage d'objets StorageGRID .

   - **Politique de sauvegarde** : sélectionnez une politique de sauvegarde sur stockage d'objets existante ou créez-en une.

     Pour créer une politique personnalisée, reportez-vous à"Créer une politique" .

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :

     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Pour les politiques de sauvegarde sur objet, définissez les paramètres DataLock et Ransomware Resilience. Pour plus de détails sur DataLock et la résilience aux ransomwares, reportez-vous à"Paramètres de la politique de sauvegarde sur objet" .

Si votre cluster utilise ONTAP 9.11.1 ou une version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre la suppression et les attaques de ransomware en configurant *DataLock et Ransomware Resilience*. *DataLock* protège vos fichiers de sauvegarde contre toute modification ou suppression, et *Ransomware Resilience* analyse vos fichiers de sauvegarde pour rechercher des preuves d'une attaque de ransomware dans vos fichiers de sauvegarde.

- Sélectionnez **Créer**.

Si votre cluster utilise ONTAP 9.12.1 ou une version ultérieure et que votre système StorageGRID utilise la version 11.4 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers des niveaux d'archives de cloud public après un certain nombre de jours. La prise en charge actuelle concerne les niveaux de stockage AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. Découvrez comment configurer vos systèmes pour cette fonctionnalité .

- **Sauvegarde hiérarchisée vers le cloud public** : sélectionnez le fournisseur de cloud vers lequel vous souhaitez hiérarchiser les sauvegardes et saisissez les détails du fournisseur.

  Sélectionnez ou créez un nouveau cluster StorageGRID . Pour plus de détails sur la création d'un cluster StorageGRID afin que la console puisse le découvrir, reportez-vous à "Documentation de StorageGRID" .

- **Exporter les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

C'est l'occasion de revoir vos sélections et de faire des ajustements, si nécessaire.

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

NetApp Backup and Recovery commence à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données sources. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les instantanés.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume de stockage principal.

Un compartiment S3 est créé dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés.

Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l'"Page de surveillance des tâches" .

Afficher les commandes de l'API

Vous souhaiterez peut-être afficher et éventuellement copier les commandes API utilisées dans l'assistant d'activation de la sauvegarde et de la récupération. Vous souhaiterez peut-être faire cela pour automatiser l'activation de la sauvegarde dans les futurs systèmes.

Étapes

1. Dans l'assistant d'activation de la sauvegarde et de la récupération, sélectionnez **Afficher la demande d'API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Migrer des volumes à l'aide de SnapMirror vers Cloud Resync dans NetApp Backup and Recovery

La fonctionnalité SnapMirror to Cloud Resync de NetApp Backup and Recovery rationalise la protection et la continuité des données lors des migrations de volumes dans les environnements NetApp . Lorsqu'un volume est migré à l'aide de SnapMirror Logical Replication (LRSE) d'un déploiement NetApp sur site à un autre, ou vers une solution basée sur le cloud telle que Cloud Volumes ONTAP, SnapMirror to Cloud Resync garantit que les sauvegardes cloud existantes restent intactes et opérationnelles.

Cette fonctionnalité élimine le besoin d'un processus de réétablissement de la configuration de référence et permet aux sauvegardes de se poursuivre après la migration. Cette fonctionnalité est utile dans les scénarios de migration de charge de travail, prenant en charge à la fois FlexVols et FlexGroups, et est disponible à partir de la version 9.16.1 ONTAP .

Cette fonctionnalité est disponible à partir de la version 4.0.3 de NetApp Backup and Recovery publiée en mai 2025.

La resynchronisation SnapMirror vers le cloud assure la continuité des sauvegardes entre les environnements, facilitant ainsi la gestion des données dans les configurations hybrides et multicloud.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Avant de commencer

Assurez-vous que ces conditions préalables ont été remplies :

- Le cluster ONTAP de destination doit exécuter ONTAP version 9.16.1 ou ultérieure.
- L'ancien cluster ONTAP source doit être protégé à l'aide de NetApp Backup and Recovery.
- La fonctionnalité SnapMirror to Cloud Resync est disponible à partir de la version 4.0.3 de NetApp Backup and Recovery publiée en mai 2025.
- Assurez-vous que la dernière sauvegarde dans le stockage d'objets soit l'instantané commun à l'ancienne source, à la nouvelle source et au stockage d'objets. N'utilisez pas un instantané commun plus ancien que le dernier instantané sauvegardé sur le magasin d'objets.
- Les stratégies de snapshot et SnapMirror utilisées sur l'ancien cluster ONTAP doivent toutes deux être

créées sur le nouveau cluster ONTAP avant de démarrer l'opération de resynchronisation. Si vous utilisez une stratégie quelconque lors du processus de resynchronisation, vous devez également créer cette stratégie. L'opération de resynchronisation ne crée pas de stratégies.

- Assurez-vous que la stratégie SnapMirror appliquée à la relation SnapMirror du volume de migration inclut la même étiquette que celle utilisée par la relation cloud. Pour éviter les problèmes, utilisez la politique qui régit un miroir exact du volume et de tous les instantanés.

> La resynchronisation de SnapMirror vers Cloud après les migrations à l'aide des méthodes SVM-Migrate, SVM-DR ou Head Swap n'est actuellement pas prise en charge.

Comment fonctionne NetApp Backup and Recovery SnapMirror to Cloud Resync

Si vous effectuez une actualisation technique ou migrez des volumes d'un cluster ONTAP vers un autre, il est important que vos sauvegardes continuent de fonctionner sans interruption. NetApp Backup and Recovery SnapMirror to Cloud Resync vous aide à y parvenir en garantissant que vos sauvegardes cloud restent cohérentes même après une migration de volume.

Voici un exemple :

Imaginez que vous disposez d'un volume sur site appelé Vol1a. Ce volume contient trois instantanés : S1, S2 et S3. Ces instantanés sont des points de restauration. Le volume 1 est sauvegardé dans le cloud à l'aide de SnapMirror to Cloud (SM-C), mais seuls les volumes S1 et S2 sont stockés dans l'objet.

Maintenant, vous souhaitez migrer Vol1 vers un autre cluster ONTAP . Pour ce faire, vous créez une relation de réplication logique SnapMirror (LRSE) avec un nouveau volume cloud appelé Vol1b. Cela transfère les trois instantanés (S1, S2 et S3) du Vol1a au Vol1b.

Une fois la migration terminée, vous disposez de la configuration suivante :

- La relation SM-C d'origine (Vol1a → Magasin d'objets) est supprimée.
- La relation LRSE (Vol1a → Vol1b) est également supprimée.
- Vol1b est désormais votre volume actif.

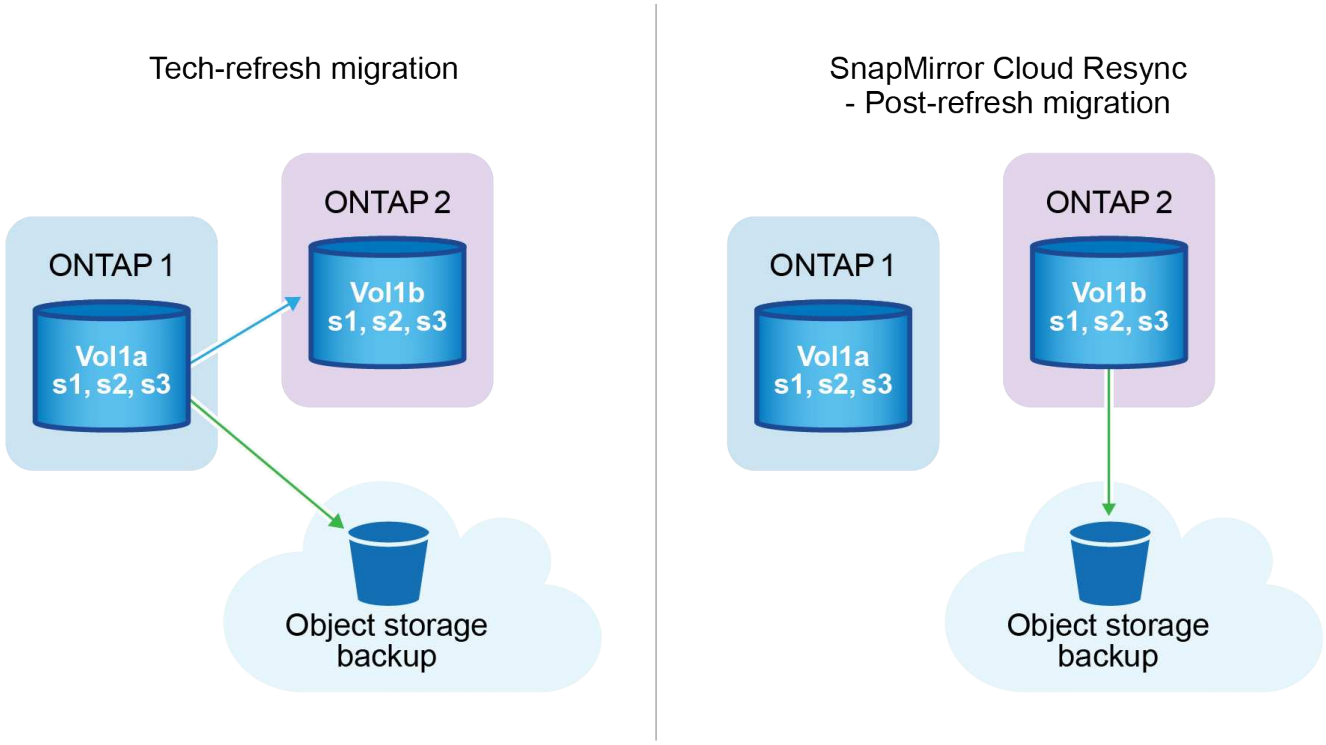
À ce stade, vous souhaitez continuer à sauvegarder Vol1b sur le même point de terminaison cloud. Mais au lieu de démarrer une sauvegarde complète à partir de zéro (ce qui prendrait du temps et des ressources), vous utilisez SnapMirror to Cloud Resync.

Voici comment fonctionne la resynchronisation :

- Le système vérifie un instantané commun entre Vol1a et le magasin d'objets. Dans ce cas, les deux ont S2.
- En raison de cet instantané partagé, le système doit transférer uniquement les modifications incrémentielles entre S2 et S3.

Cela signifie uniquement les nouvelles données ajoutées après l'envoi de S2 au magasin d'objets, et non le volume entier.

Ce processus évite les sauvegardes en double, économise de la bande passante et maintient les sauvegardes actives après la migration.



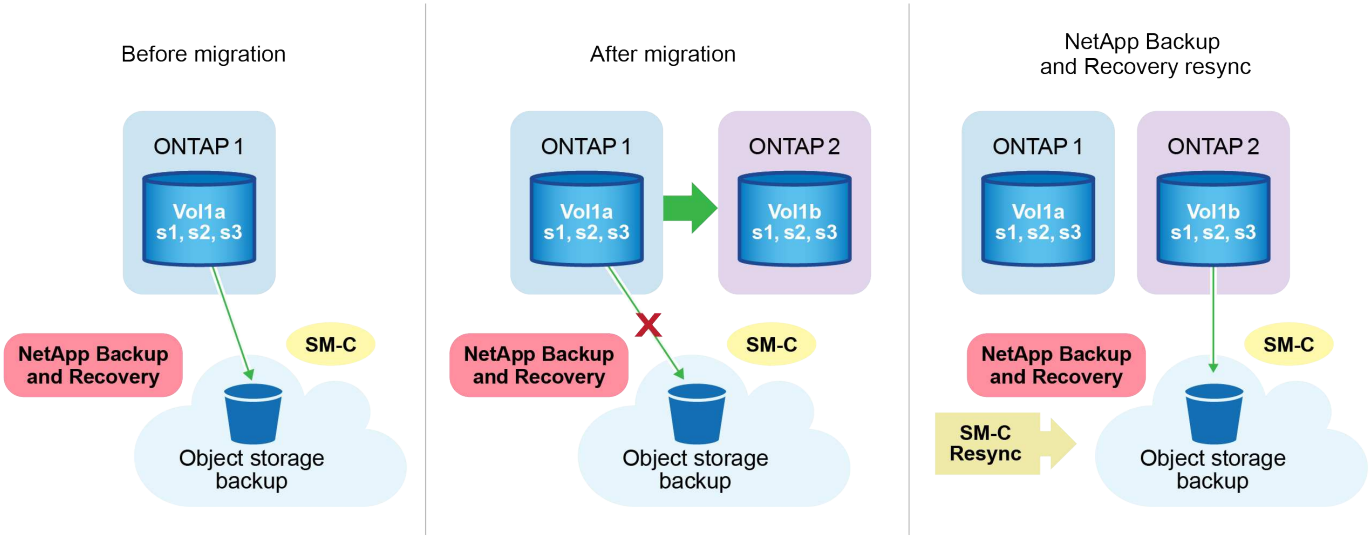
Notes de procédure

- Les migrations et les actualisations technologiques ne sont pas effectuées à l'aide de NetApp Backup and Recovery. Elles doivent être effectuées par une équipe de services professionnels ou un administrateur de stockage qualifié.
- Une équipe de migration NetApp crée la relation SnapMirror entre les clusters ONTAP source et de destination pour faciliter le déplacement des volumes.
- Assurez-vous que la migration lors d'une actualisation technologique est basée sur une migration basée sur SnapMirror.

Comment migrer des volumes à l'aide de SnapMirror vers Cloud Resync

La migration de volumes à l'aide de SnapMirror vers Cloud Resync implique les étapes principales suivantes, chacune décrite plus en détail ci-dessous :

- **Suivez une liste de contrôle de pré-migration** : Avant de commencer la migration, une équipe NetApp Tech Refresh s'assure que les conditions préalables suivantes sont remplies pour éviter la perte de données et garantir un processus de migration fluide.
- **Suivez une liste de contrôle post-migration** : après la migration, une équipe NetApp Tech Refresh s'assure que les étapes suivantes sont effectuées pour établir la protection et préparer la resynchronisation.
- **Effectuer une resynchronisation SnapMirror vers le cloud** : après la migration, une équipe NetApp Tech Refresh effectue une opération de resynchronisation SnapMirror vers le cloud pour reprendre les sauvegardes cloud à partir des volumes nouvellement migrés.



Suivez une liste de contrôle de pré-migration

Avant la migration, l'équipe NetApp Tech Refresh vérifie ces prérequis afin d'éviter toute perte de données et de garantir un processus sans accroc.

1. Assurez-vous que tous les volumes à migrer sont protégés à l'aide de NetApp Backup and Recovery.
2. Enregistrer les UUID des instances de volume. Notez les UUID d'instance de tous les volumes avant de démarrer la migration. Ces identifiants sont essentiels pour les opérations de mappage et de resynchronisation ultérieures.
3. Prenez un instantané final de chaque volume pour conserver l'état le plus récent, avant de supprimer toutes les relations SnapMirror .
4. Documenter les politiques SnapMirror . Enregistrez la politique SnapMirror actuellement attachée à la relation de chaque volume. Cela sera nécessaire plus tard lors du processus de resynchronisation de SnapMirror vers Cloud.
5. Supprimez les relations SnapMirror Cloud avec le magasin d'objets.
6. Créez une relation SnapMirror standard avec le nouveau cluster ONTAP pour migrer le volume vers le nouveau cluster ONTAP cible.

Suivez une liste de contrôle post-migration

Après la migration, une équipe NetApp Tech Refresh s'assure que les étapes suivantes sont effectuées pour établir la protection et préparer la resynchronisation.

1. Enregistrez les nouveaux UUID d'instance de volume de tous les volumes migrés dans le cluster ONTAP de destination.
2. Confirmez que toutes les stratégies SnapMirror requises qui étaient disponibles dans l'ancien cluster ONTAP sont correctement configurées dans le nouveau cluster ONTAP .
3. Ajoutez le nouveau cluster ONTAP en tant que système dans la page **Systèmes** de la console.

> L'UUID de l'instance de volume doit être utilisé, et non l'ID de volume. L'UUID de l'instance de volume est un identifiant unique qui reste cohérent d'une migration à l'autre, tandis que l'ID de volume peut changer après la migration.

Effectuer une resynchronisation SnapMirror vers le Cloud

Après la migration, une équipe NetApp Tech Refresh effectue une opération SnapMirror vers Cloud Resync pour reprendre les sauvegardes cloud à partir des volumes nouvellement migrés.

1. Ajoutez le nouveau cluster ONTAP en tant que système dans la page **Systèmes** de la console.
2. Consultez la page Volumes de NetApp Backup and Recovery pour vous assurer que les détails de l'ancien système source sont disponibles.
3. Sur la page Volumes de NetApp Backup and Recovery , sélectionnez **Paramètres de sauvegarde**.
   - Dans la page Paramètres de sauvegarde, sélectionnez **Afficher tout**.
   - Dans le menu Actions… à droite de la *nouvelle* source, sélectionnez **Resynchroniser la sauvegarde**.
4. Dans la page système Resync, procédez comme suit :
   a. **Nouveau système source** : saisissez le nouveau cluster ONTAP vers lequel les volumes ont été migrés.
   b. **Magasin d'objets cible existant** : sélectionnez le magasin d'objets cible qui contient les sauvegardes de l'ancien système source.
5. Sélectionnez **Télécharger le modèle CSV** pour télécharger la feuille Excel des détails de resynchronisation. Utilisez cette feuille pour saisir les détails des volumes à migrer. Dans le fichier CSV, saisissez les détails suivants :
   - L'UUID de l'ancienne instance de volume du cluster source
   - Le nouvel UUID de l'instance de volume du cluster de destination
   - La politique SnapMirror à appliquer à la nouvelle relation.
6. Sélectionnez **Télécharger** sous **Télécharger les détails du mappage de volume** pour télécharger la feuille CSV complétée dans l'interface utilisateur de NetApp Backup and Recovery .

   L'UUID de l'instance de volume doit être utilisé, et non l'ID de volume. L'UUID de l'instance de volume est un identifiant unique qui reste cohérent d'une migration à l'autre, tandis que l'ID de volume peut changer après la migration.

7. Saisissez les informations de configuration du fournisseur et du réseau requises pour l'opération de resynchronisation.
8. Sélectionnez **Soumettre** pour démarrer le processus de validation.

   NetApp Backup and Recovery valide que chaque volume sélectionné pour la resynchronisation est le dernier snapshot et possède au moins un snapshot commun. Cela garantit que les volumes sont prêts pour l'opération de resynchronisation SnapMirror vers Cloud.

9. Examinez les résultats de la validation, y compris les nouveaux noms de volumes sources et l'état de resynchronisation de chaque volume.
10. Vérifiez l'éligibilité du volume. Le système vérifie si les volumes sont éligibles à la resynchronisation. Si un volume n'est pas éligible, cela signifie qu'il ne s'agit pas du dernier instantané ou qu'aucun instantané commun n'a été trouvé.

    Pour garantir que les volumes restent éligibles pour l'opération de resynchronisation SnapMirror vers Cloud, prenez un instantané final de chaque volume avant de supprimer toute relation SnapMirror pendant la phase de pré-migration. Cela préserve l'état le plus récent des données.

11. Sélectionnez **Resynchroniser** pour démarrer l'opération de resynchronisation. Le système utilise le snapshot le plus récent et le plus courant pour transférer uniquement les modifications incrémentielles, garantissant ainsi la continuité de la sauvegarde.
12. Surveillez le processus de resynchronisation dans la page Moniteur de tâches.

Restaurer les données de configuration de NetApp Backup and Recovery sur un site sombre

Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, appelé *mode privé*, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où vos sauvegardes sont stockées. Si vous rencontrez un problème avec le système hôte de l'agent de console, vous pouvez déployer un nouvel agent de console et restaurer les données critiques de NetApp Backup and Recovery .

Cette procédure s'applique uniquement aux données de volume ONTAP .

Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS avec l'agent de console déployé chez votre fournisseur de cloud ou sur votre propre hôte connecté à Internet, le système sauvegarde et protège toutes les données de configuration importantes dans le cloud. Si vous rencontrez un problème avec l'agent de console, créez un nouvel agent de console et ajoutez vos systèmes. Les détails de la sauvegarde sont automatiquement restaurés.

Il existe deux types de données sauvegardées :

- Base de données de NetApp Backup and Recovery : contient une liste de tous les volumes, fichiers de sauvegarde, politiques de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés - contiennent des index détaillés utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lorsque vous recherchez des données de volume que vous souhaitez restaurer.

Ces données sont sauvegardées une fois par jour à minuit et un maximum de 7 copies de chaque fichier sont conservées. Si l'agent de console gère plusieurs systèmes ONTAP sur site, les fichiers de NetApp Backup and Recovery sont stockés dans le compartiment du système qui a été activé en premier.

Aucune donnée de volume n'est jamais incluse dans la base de données NetApp Backup and Recovery ou dans les fichiers de catalogue indexés.

Restaurer les données de NetApp Backup and Recovery vers un nouvel agent de console

Si votre agent de console sur site cesse de fonctionner, vous devrez installer un nouvel agent de console, puis restaurer les données de NetApp Backup and Recovery sur le nouvel agent de console.

Vous devrez effectuer les tâches suivantes pour remettre votre système NetApp Backup and Recovery en état de fonctionnement :

- Installer un nouvel agent de console
- Restaurer la base de données de NetApp Backup and Recovery
- Restaurer les fichiers du catalogue indexé

- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site sur l'interface utilisateur de la NetApp Console

Après avoir vérifié que votre système fonctionne, créez de nouveaux fichiers de sauvegarde.

Ce dont vous aurez besoin

Vous devrez accéder aux sauvegardes de base de données et d'index les plus récentes à partir du compartiment StorageGRID ou ONTAP S3 où vos fichiers de sauvegarde sont stockés :

- Fichier de base de données MySQL de NetApp Backup and Recovery

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/mysql_backup/` , et il s'appelle `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Fichier zip de sauvegarde du catalogue indexé

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/catalog_backup/` , et il s'appelle `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installer un nouvel agent de console sur un nouvel hôte Linux local

Lors de l'installation d'un nouvel agent de console, téléchargez la même version du logiciel que l'agent d'origine. Les modifications apportées à la base de données NetApp Backup and Recovery peuvent empêcher les nouvelles versions du logiciel de fonctionner avec les anciennes sauvegardes de base de données. Tu peux "mettre à niveau le logiciel de l'agent de la console vers la version la plus récente après la restauration de la base de données de sauvegarde" .

1. "Installer l'agent de console sur un nouvel hôte Linux local"
2. Connectez-vous à la console à l'aide des informations d'identification de l'utilisateur administrateur que vous venez de créer.

Restaurer la base de données de NetApp Backup and Recovery

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte de l'agent de console. Nous utiliserons le nom de fichier d'exemple « CBS_DB_Backup_23_05_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur Docker MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

   ```
   docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
   ```

   ```
   podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
   ```

3. Accédez au shell du conteneur MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

   ```
   docker exec -it ds_mysql_1 sh
   ```

```
podman exec -it ds_mysql_1 sh
```

4. Dans le shell du conteneur, déployez « env ».
5. Vous aurez besoin du mot de passe de la base de données MySQL, copiez donc la valeur de la clé « MYSQL_ROOT_PASSWORD ».
6. Restaurez la base de données MySQL de NetApp Backup and Recovery à l'aide de la commande suivante :

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Vérifiez que la base de données MySQL de NetApp Backup and Recovery a été restaurée correctement à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

8. Entrez le mot de passe.

```
mysql> show tables;
mysql> select * from volume;
```

9. Vérifiez que les volumes affichés correspondent bien à ceux de votre environnement d'origine.

Restaurer les fichiers du catalogue indexé

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons le nom de fichier d'exemple « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte de l'agent de console dans le dossier « /opt/application/netapp/cbs ».
2. Décompressez le fichier « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip » à l'aide de la commande suivante :

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Exécutez la commande **ls** pour vous assurer que le dossier « catalogdb1 » a été créé avec les sous-dossiers « changes » et « snapshots » en dessous.

Découvrez vos clusters ONTAP et vos systèmes StorageGRID

1. "Découvrez tous les systèmes ONTAP sur site"qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.
2. "Découvrez vos systèmes StorageGRID".

Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos systèmes ONTAP tels qu'ils ont été configurés lors de la configuration de l'agent de console d'origine à l'aide de l' "API de la NetApp Console" .

Les informations suivantes s'appliquent aux installations en mode privé à partir de NetApp Console 3.9.xx. Pour les versions plus anciennes, utilisez la procédure suivante : "Sauvegarde Cloud DarkSite : sauvegarde et restauration de MySQL et du catalogue indexé" .

Vous devrez effectuer ces étapes pour chaque système qui sauvegarde des données sur StorageGRID.

1. Extrayez le jeton d'autorisation à l'aide de l'API oauth/token suivante.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   Alors que l'adresse IP, le nom d'utilisateur et les mots de passe sont des valeurs personnalisées, le nom du compte ne l'est pas. Le nom du compte est toujours « account-DARKSITE1 ». De plus, le nom d'utilisateur doit utiliser un nom au format e-mail.

   Cette API renverra une réponse comme celle-ci. Vous pouvez récupérer le jeton d'autorisation comme indiqué ci-dessous.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extrayez l'ID système et l'ID X-Agent à l'aide de l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Cette API renverra une réponse comme celle-ci. La valeur sous « resourceIdentifier » désigne l'*ID de l'environnement de travail* et la valeur sous « agentId » désigne *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Mettez à jour la base de données NetApp Backup and Recovery avec les détails du système StorageGRID associé aux systèmes. Assurez-vous de saisir le nom de domaine complet du StorageGRID, ainsi que la clé d'accès et la clé de stockage comme indiqué ci-dessous :

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Vérifier les paramètres de NetApp Backup and Recovery

1. Sélectionnez chaque système ONTAP et cliquez sur **Afficher les sauvegardes** à côté du service de sauvegarde et de récupération dans le panneau de droite.

   Vous devriez voir toutes les sauvegardes créées pour vos volumes.

2. Depuis le tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

   Assurez-vous que les systèmes sur lesquels le catalogage indexé était précédemment activé restent activés.

3. À partir de la page Rechercher et restaurer, exécutez quelques recherches de catalogue pour confirmer que la restauration du catalogue indexé a été effectuée avec succès.

Gérez les sauvegardes de vos systèmes ONTAP avec NetApp Backup and Recovery

Avec NetApp Backup and Recovery, gérez les sauvegardes de vos systèmes Cloud Volumes ONTAP et ONTAP sur site en modifiant la planification de sauvegarde, en activant/désactivant les sauvegardes de volume, en suspendant les sauvegardes, en supprimant les sauvegardes, en forçant la suppression des sauvegardes, etc. Cela inclut tous les types de sauvegardes, y compris les instantanés, les volumes répliqués et les fichiers de sauvegarde stockés dans des objets. Vous pouvez également désinscrire

Ne gérez pas et ne modifiez pas les fichiers de sauvegarde directement sur vos systèmes de stockage ou depuis l'environnement de votre fournisseur de cloud. Cela peut corrompre les fichiers et entraîner une configuration non prise en charge.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Afficher l'état de sauvegarde des volumes de vos systèmes

Vous pouvez afficher une liste de tous les volumes en cours de sauvegarde dans le tableau de bord de sauvegarde des volumes. Cela inclut tous les types de sauvegardes, y compris les instantanés, les volumes répliqués et les fichiers de sauvegarde stockés dans des objets. Vous pouvez également afficher les volumes des systèmes qui ne sont pas actuellement sauvegardés.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez le menu **Volumes** pour afficher la liste des volumes sauvegardés pour vos systèmes Cloud Volumes ONTAP et ONTAP sur site.
3. Si vous recherchez des volumes spécifiques dans certains systèmes, vous pouvez affiner la liste par système et par volume. Vous pouvez également utiliser le filtre de recherche ou trier les colonnes en fonction du style de volume (FlexVol ou FlexGroup), du type de volume, etc.

   Pour afficher des colonnes supplémentaires (agrégats, style de sécurité (Windows ou UNIX), politique de snapshot, politique de réplication et politique de sauvegarde), sélectionnez le signe plus.

4. Vérifiez l'état des options de protection dans la colonne « Protection existante ». Les 3 icônes représentent « Instantanés locaux », « Volumes répliqués » et « Sauvegardes dans le stockage d'objets ».

   Chaque icône s'illumine lorsque le type de sauvegarde correspondant est activé, et elle est grise lorsque le type de sauvegarde est inactif. Vous pouvez survoler chaque icône avec votre curseur pour afficher la politique de sauvegarde utilisée, ainsi que d'autres informations pertinentes pour chaque type de sauvegarde.

Activer la sauvegarde sur des volumes supplémentaires dans un système

Si vous avez activé la sauvegarde uniquement sur certains volumes d'un système lorsque vous avez activé NetApp Backup and Recovery pour la première fois, vous pouvez activer les sauvegardes sur des volumes supplémentaires ultérieurement.

Étapes

1. Dans l'onglet **Volumes**, identifiez le volume sur lequel vous souhaitez activer les sauvegardes, puis sélectionnez le menu Actions. ••• à la fin de la ligne, et sélectionnez **Activer la protection 3-2-1**.
2. Sur la page *Définir la stratégie de sauvegarde*, sélectionnez l'architecture de sauvegarde, puis définissez les politiques et autres détails pour les instantanés locaux, les volumes répliqués et les fichiers de sauvegarde. Consultez les détails des options de sauvegarde des volumes initiaux que vous avez activés dans ce système. Sélectionnez ensuite **Suivant**.
3. Vérifiez les paramètres de sauvegarde de ce volume, puis sélectionnez **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde attribués aux volumes existants

Vous pouvez modifier les politiques de sauvegarde attribuées à vos volumes existants auxquels des politiques sont attribuées. Vous pouvez modifier les stratégies appliquées à vos instantanés locaux, à vos volumes répliqués et à vos fichiers de sauvegarde. Toute nouvelle stratégie de snapshot, de réplication ou de sauvegarde que vous souhaitez appliquer aux volumes doit déjà exister.

Modifier les paramètres de sauvegarde sur un seul volume

Étapes

1. Dans le menu **Volumes**, repérez le volume dont vous souhaitez modifier les paramètres de stratégie, puis sélectionnez le menu Actions. ••• à la fin de la ligne, et sélectionnez **Modifier la stratégie de sauvegarde**.
2. Sur la page *Modifier la stratégie de sauvegarde*, apportez des modifications aux politiques de sauvegarde existantes pour les instantanés locaux, les volumes répliqués et les fichiers de sauvegarde, puis sélectionnez **Suivant**.

   Si vous avez activé *DataLock et Ransomware Resilience* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, vous ne verrez que les autres stratégies qui ont été configurées avec DataLock. Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne verrez que d'autres stratégies de sauvegarde cloud pour lesquelles DataLock n'est pas configuré.

3. Vérifiez les paramètres de sauvegarde de ce volume, puis sélectionnez **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde sur plusieurs volumes

Si vous souhaitez utiliser les mêmes paramètres de sauvegarde sur plusieurs volumes, vous pouvez activer ou modifier les paramètres de sauvegarde sur plusieurs volumes en même temps. Vous pouvez sélectionner des volumes qui n'ont pas de paramètres de sauvegarde, uniquement des paramètres de snapshot, uniquement des paramètres de sauvegarde dans le cloud, etc., et effectuer des modifications en masse sur tous ces volumes avec divers paramètres de sauvegarde.

Lorsque vous travaillez avec plusieurs volumes, tous les volumes doivent avoir ces caractéristiques communes :

- même système
- même style (volume FlexVol ou FlexGroup)
- même type (volume en lecture-écriture ou de protection des données)

Lorsque plus de cinq volumes sont activés pour la sauvegarde, NetApp Backup and Recovery n'initialise que cinq volumes à la fois. Une fois ces étapes terminées, le processus se poursuit par groupes de 5 jusqu'à ce que tous les volumes soient initialisés.

Étapes

1. À partir de l'onglet **Volumes**, filtrez par le système sur lequel résident les volumes.
2. Sélectionnez tous les volumes sur lesquels vous souhaitez gérer les paramètres de sauvegarde.
3. Selon le type d'action de sauvegarde que vous souhaitez configurer, cliquez sur le bouton dans le menu Actions en masse :

Action de sauvegarde…	Sélectionnez ce bouton…
Gérer les paramètres de sauvegarde des instantanés	**Gérer les instantanés locaux**

Action de sauvegarde…	Sélectionnez ce bouton…
Gérer les paramètres de sauvegarde de réplication	**Gérer la réplication**
Gérer les paramètres de sauvegarde dans le cloud	**Gérer la sauvegarde**
Gérez plusieurs types de paramètres de sauvegarde. Cette option vous permet également de modifier l'architecture de sauvegarde.	**Gérer la sauvegarde et la récupération**

4. Sur la page de sauvegarde qui apparaît, modifiez les politiques de sauvegarde existantes pour les instantanés locaux, les volumes répliqués ou les fichiers de sauvegarde, puis sélectionnez **Enregistrer**.

   Si vous avez activé *DataLock et Ransomware Resilience* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, vous ne verrez que les autres stratégies qui ont été configurées avec DataLock. Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne verrez que d'autres stratégies de sauvegarde cloud pour lesquelles DataLock n'est pas configuré.

Créez une sauvegarde manuelle du volume à tout moment

Vous pouvez créer une sauvegarde à la demande à tout moment pour capturer l'état actuel du volume. Cela peut être utile si des modifications très importantes ont été apportées à un volume et que vous ne souhaitez pas attendre la prochaine sauvegarde planifiée pour protéger ces données. Vous pouvez également utiliser cette fonctionnalité pour créer une sauvegarde pour un volume qui n'est pas actuellement en cours de sauvegarde et dont vous souhaitez capturer l'état actuel.

Vous pouvez créer un instantané ad hoc ou une sauvegarde sur le stockage d'objets d'un volume. Vous ne pouvez pas créer un volume répliqué ad hoc.

Le nom de la sauvegarde inclut l'horodatage afin que vous puissiez identifier votre sauvegarde à la demande parmi d'autres sauvegardes planifiées.

Si vous avez activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery pour ce cluster, la sauvegarde à la demande sera également configurée avec DataLock et la période de conservation sera de 30 jours. Les analyses de ransomware ne sont pas prises en charge pour les sauvegardes ad hoc. "En savoir plus sur DataLock et la protection contre les ransomwares" .

Lorsque vous créez une sauvegarde ad hoc, un instantané est créé sur le volume source. Étant donné que cet instantané ne fait pas partie d'une planification d'instantanés normale, il ne sera pas désactivé. Vous souhaiterez peut-être supprimer manuellement cet instantané du volume source une fois la sauvegarde terminée. Cela permettra de libérer les blocs liés à cet instantané. Le nom de l'instantané commencera par `cbs-snapshot-adhoc-` . "Découvrez comment supprimer un instantané à l'aide de l'interface de ligne de commande ONTAP" .

> La sauvegarde de volume à la demande n'est pas prise en charge sur les volumes de protection des données.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume et sélectionnez **Sauvegarde** > **Créer une sauvegarde ad hoc**.

La colonne État de la sauvegarde pour ce volume affiche « En cours » jusqu'à ce que la sauvegarde soit créée.

Afficher la liste des sauvegardes pour chaque volume

Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche les détails sur le volume source, l'emplacement de destination et les détails de sauvegarde tels que la dernière sauvegarde effectuée, la politique de sauvegarde actuelle, la taille du fichier de sauvegarde, etc.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Afficher les détails du volume**.

   Les détails du volume et la liste des instantanés sont affichés.

2. Sélectionnez **Snapshot**, **Réplication** ou **Sauvegarde** pour voir la liste de tous les fichiers de sauvegarde pour chaque type de sauvegarde.

Exécuter une analyse de ransomware sur une sauvegarde de volume dans le stockage d'objets

NetApp Backup and Recovery analyse vos fichiers de sauvegarde pour rechercher des preuves d'une attaque de ransomware lorsqu'une sauvegarde vers un fichier objet est créée et lorsque les données d'un fichier de sauvegarde sont en cours de restauration. Vous pouvez également exécuter une analyse à la demande à tout moment pour vérifier la facilité d'utilisation d'un fichier de sauvegarde spécifique dans le stockage d'objets. Cela peut être utile si vous avez rencontré un problème de ransomware sur un volume particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

Cette fonctionnalité est disponible uniquement si la sauvegarde du volume a été créée à partir d'un système avec ONTAP 9.11.1 ou une version ultérieure, et si vous avez activé *DataLock et Ransomware Resilience* dans la stratégie de sauvegarde vers objet.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Afficher les détails du volume**.

   Les détails du volume sont affichés.

2. Sélectionnez **Sauvegarde** pour voir la liste des fichiers de sauvegarde dans le stockage d'objets.
3. Sélectionner••• pour le fichier de sauvegarde du volume que vous souhaitez analyser pour détecter les ransomwares et cliquez sur **Rechercher les ransomwares**.

   La colonne Résilience aux ransomwares indique que l'analyse est en cours.

Gérer la relation de réplication avec le volume source

Après avoir configuré la réplication des données entre deux systèmes, vous pouvez gérer la relation de réplication des données.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez l'option **Réplication**. Vous pouvez voir toutes les options disponibles.
2. Sélectionnez l'action de réplication que vous souhaitez effectuer.

   Le tableau suivant décrit les actions disponibles :

Action	Description
Afficher la réplication	Affiche les détails sur la relation de volume : informations de transfert, informations sur le dernier transfert, détails sur le volume et informations sur la politique de protection attribuée à la relation.
Mettre à jour la réplication	Démarre un transfert incrémentiel pour mettre à jour le volume de destination à synchroniser avec le volume source.
Suspendre la réplication	Interrompez le transfert incrémentiel des instantanés pour mettre à jour le volume de destination. Vous pouvez reprendre plus tard si vous souhaitez redémarrer les mises à jour incrémentielles.
Interrompre la réplication	Rompt la relation entre les volumes source et de destination et active le volume de destination pour l'accès aux données - le rend en lecture-écriture. Cette option est généralement utilisée lorsque le volume source ne peut pas fournir de données en raison d'événements tels qu'une corruption de données, une suppression accidentelle ou un état hors ligne.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["Découvrez comment configurer un volume de destination pour l'accès aux données et réactiver un volume source dans la documentation ONTAP"^]
Abandonner la réplication	Désactive les sauvegardes de ce volume sur le système de destination et désactive également la possibilité de restaurer un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne supprime pas la relation de protection des données entre les volumes source et de destination.
Resynchronisation inversée	Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est écrasé par le contenu du volume de destination. Cela est utile lorsque vous souhaitez réactiver un volume source qui est devenu hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et le moment où le volume source a été désactivé ne sont pas conservées.
Supprimer la relation	Supprime la relation de protection des données entre les volumes source et de destination, ce qui signifie que la réplication des données ne se produit plus entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données, ce qui signifie qu'il n'est pas accessible en lecture-écriture. Cette action supprime également la relation d'homologue de cluster et la relation d'homologue de machine virtuelle de stockage (SVM), s'il n'existe aucune autre relation de protection des données entre les systèmes.

Résultat

Après avoir sélectionné une action, la console met à jour la relation.

Modifier une politique de sauvegarde dans le cloud existante

Vous pouvez modifier les attributs d'une politique de sauvegarde actuellement appliquée aux volumes d'un système. La modification de la politique de sauvegarde affecte tous les volumes existants qui utilisent la politique.

- Si vous avez activé *DataLock et Ransomware Resilience* dans la stratégie initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, toutes les stratégies que vous modifiez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne pouvez pas activer DataLock maintenant.
- Lors de la création de sauvegardes sur AWS, si vous avez choisi *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première politique de sauvegarde lors de l'activation de NetApp Backup and Recovery, ce niveau sera le seul niveau d'archivage disponible lors de la modification des politiques de sauvegarde. Et si vous n'avez sélectionné aucun niveau d'archivage dans votre première politique de sauvegarde, *S3 Glacier* sera votre seule option d'archivage lors de la modification d'une politique.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez modifier les paramètres de stratégie, puis sélectionnez **Gérer les stratégies**.
3. Depuis la page *Gérer les politiques*, sélectionnez **Modifier** pour la politique de sauvegarde que vous souhaitez modifier dans ce système.
4. Depuis la page *Modifier la politique*, sélectionnez la flèche vers le bas pour développer la section *Étiquettes et rétention* afin de modifier la planification et/ou la rétention de sauvegarde, puis sélectionnez **Enregistrer**.

   Si votre cluster exécute ONTAP 9.10.1 ou une version ultérieure, vous avez également la possibilité d'activer ou de désactiver la hiérarchisation des sauvegardes vers le stockage d'archivage après un certain nombre de jours.

   "En savoir plus sur l'utilisation du stockage d'archives AWS". "En savoir plus sur l'utilisation du stockage d'archives Azure". "En savoir plus sur l'utilisation du stockage d'archives Google". (Nécessite ONTAP 9.12.1.)

   Notez que les fichiers de sauvegarde qui ont été classés dans le stockage d'archives restent dans ce niveau si vous arrêtez de classer les sauvegardes dans l'archive ; ils ne sont pas automatiquement déplacés vers le niveau standard. Seules les nouvelles sauvegardes de volumes seront stockées dans le niveau standard.

Ajouter une nouvelle politique de sauvegarde dans le cloud

Lorsque vous activez NetApp Backup and Recovery pour un système, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la stratégie de sauvegarde par défaut que vous avez définie. Si vous souhaitez attribuer différentes politiques de sauvegarde à certains volumes ayant des objectifs de point de récupération (RPO) différents, vous pouvez créer des politiques supplémentaires pour ce cluster et attribuer ces politiques à d'autres volumes.

Si vous souhaitez appliquer une nouvelle politique de sauvegarde à certains volumes d'un système, vous devez d'abord ajouter la politique de sauvegarde au système. Alors tu peuxappliquer la politique aux volumes de ce système .

- Si vous avez activé *DataLock et Ransomware Resilience* dans la stratégie initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, toutes les stratégies supplémentaires que vous créez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne pouvez pas créer de nouvelles politiques qui utilisent DataLock.
- Lors de la création de sauvegardes sur AWS, si vous avez choisi *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de NetApp Backup and Recovery, ce niveau sera le seul niveau d'archivage disponible pour les futures stratégies de sauvegarde pour ce cluster. Et si vous n'avez sélectionné aucun niveau d'archivage dans votre première politique de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage pour les politiques futures.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez ajouter la nouvelle politique, puis sélectionnez **Gérer les politiques**.
3. Depuis la page *Gérer les politiques*, sélectionnez **Ajouter une nouvelle politique**.
4. Depuis la page *Ajouter une nouvelle politique*, sélectionnez la flèche vers le bas pour développer la section *Étiquettes et rétention* afin de définir la planification et la rétention des sauvegardes, puis sélectionnez **Enregistrer**.

   Si votre cluster exécute ONTAP 9.10.1 ou une version ultérieure, vous avez également la possibilité d'activer ou de désactiver la hiérarchisation des sauvegardes vers le stockage d'archivage après un certain nombre de jours.

   "En savoir plus sur l'utilisation du stockage d'archives AWS". "En savoir plus sur l'utilisation du stockage d'archives Azure". "En savoir plus sur l'utilisation du stockage d'archives Google". (Nécessite ONTAP 9.12.1.)

Supprimer les sauvegardes

NetApp Backup and Recovery vous permet de supprimer un seul fichier de sauvegarde, de supprimer toutes les sauvegardes d'un volume ou de supprimer toutes les sauvegardes de tous les volumes d'un système. Vous souhaiterez peut-être supprimer toutes les sauvegardes si vous n'en avez plus besoin ou si vous avez supprimé le volume source et souhaitez supprimer toutes les sauvegardes.

Vous ne pouvez pas supprimer les fichiers de sauvegarde que vous avez verrouillés à l'aide de la protection DataLock et Ransomware. L'option « Supprimer » ne sera pas disponible depuis l'interface utilisateur si vous avez sélectionné un ou plusieurs fichiers de sauvegarde verrouillés.

Si vous prévoyez de supprimer un système ou un cluster contenant des sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. NetApp Backup and Recovery ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système, et il n'existe actuellement aucune prise en charge dans l'interface utilisateur pour supprimer les sauvegardes une fois le système supprimé. Les frais de stockage d'objets pour toutes les sauvegardes restantes continueront à vous être facturés.

Supprimer tous les fichiers de sauvegarde d'un système

La suppression de toutes les sauvegardes sur le stockage d'objets d'un système ne désactive pas les futures

sauvegardes des volumes de ce système. Si vous souhaitez arrêter de créer des sauvegardes de tous les volumes d'un système, vous pouvez désactiver les sauvegardescomme décrit ici .

Notez que cette action n'affecte pas les instantanés ni les volumes répliqués ; ces types de fichiers de sauvegarde ne sont pas supprimés.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Sélectionner••• pour le système où vous souhaitez supprimer toutes les sauvegardes et sélectionnez **Supprimer toutes les sauvegardes**.
3. Dans la boîte de dialogue de confirmation, entrez le nom du système.
4. Sélectionnez **Paramètres avancés**.
5. **Forcer la suppression des sauvegardes** : Indiquez si vous souhaitez ou non forcer la suppression de toutes les sauvegardes.

   Dans certains cas extrêmes, vous souhaiterez peut-être que NetApp Backup and Recovery n'ait plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau du volume et du système).

   Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. NetApp Backup and Recovery n'aura plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

6. Sélectionnez **Supprimer**.

Supprimer tous les fichiers de sauvegarde d'un volume

La suppression de toutes les sauvegardes d'un volume désactive également les sauvegardes futures pour ce volume.

Étapes

1. Dans l'onglet **Volumes**, cliquez sur••• pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

   La liste de tous les fichiers de sauvegarde s'affiche.

2. Sélectionnez **Actions** > **Supprimer toutes les sauvegardes**.
3. Entrez le nom du volume.
4. Sélectionnez **Paramètres avancés**.
5. **Forcer la suppression des sauvegardes** : Indiquez si vous souhaitez ou non forcer la suppression de toutes les sauvegardes.

   Dans certains cas extrêmes, vous souhaiterez peut-être que NetApp Backup and Recovery n'ait plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau

du volume et du système).

> Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. NetApp Backup and Recovery n'aura plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

6. Sélectionnez **Supprimer**.

Supprimer un seul fichier de sauvegarde pour un volume

Vous pouvez supprimer un seul fichier de sauvegarde si vous n'en avez plus besoin. Cela inclut la suppression d'une seule sauvegarde d'un instantané de volume ou d'une sauvegarde dans un stockage d'objets.

Vous ne pouvez pas supprimer les volumes répliqués (volumes de protection des données).

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Afficher les détails du volume**.

   Les détails du volume sont affichés et vous pouvez sélectionner **Snapshot**, **Réplication** ou **Sauvegarde** pour voir la liste de tous les fichiers de sauvegarde du volume. Par défaut, les instantanés disponibles sont affichés.

2. Sélectionnez **Instantané** ou **Sauvegarde** pour voir le type de fichiers de sauvegarde que vous souhaitez supprimer.
3. Sélectionner••• pour le fichier de sauvegarde du volume que vous souhaitez supprimer et sélectionnez **Supprimer**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer**.

Supprimer les relations de sauvegarde de volume

La suppression de la relation de sauvegarde d'un volume vous fournit un mécanisme d'archivage si vous souhaitez arrêter la création de nouveaux fichiers de sauvegarde et supprimer le volume source, mais conserver tous les fichiers de sauvegarde existants. Cela vous donne la possibilité de restaurer le volume à partir du fichier de sauvegarde à l'avenir, si nécessaire, tout en libérant de l'espace sur votre système de stockage source.

Vous n'avez pas nécessairement besoin de supprimer le volume source. Vous pouvez supprimer la relation de sauvegarde d'un volume et conserver le volume source. Dans ce cas, vous pouvez « activer » la sauvegarde sur le volume ultérieurement. Dans ce cas, la copie de sauvegarde de base d'origine continue d'être utilisée : une nouvelle copie de sauvegarde de base n'est pas créée ni exportée vers le cloud. Notez que si vous réactivez une relation de sauvegarde, la politique de sauvegarde par défaut est attribuée au volume.

Cette fonctionnalité est disponible uniquement si votre système exécute ONTAP 9.12.1 ou une version ultérieure.

Vous ne pouvez pas supprimer le volume source de l'interface utilisateur de NetApp Backup and Recovery . Cependant, vous pouvez ouvrir la page Détails du volume sur la page **Systèmes** de la console et "supprimer le volume à partir de là" .

> Vous ne pouvez pas supprimer les fichiers de sauvegarde de volume individuels une fois la relation supprimée. Vous pouvez cependant supprimer toutes les sauvegardes du volume.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Sauvegarde** > **Supprimer la relation**.

Désactiver NetApp Backup and Recovery pour un système

La désactivation de NetApp Backup and Recovery pour un système désactive les sauvegardes de chaque volume du système et désactive également la possibilité de restaurer un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne désenregistre pas le service de sauvegarde de ce système. Cela vous permet essentiellement de suspendre toutes les activités de sauvegarde et de restauration pendant un certain temps.

Notez que votre fournisseur de cloud continuera à vous facturer les coûts de stockage d'objets pour la capacité utilisée par vos sauvegardes, sauf si voussupprimer les sauvegardes .

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez désactiver les sauvegardes et sélectionnez **Désactiver la sauvegarde**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Désactiver**.

> Un bouton **Activer la sauvegarde** apparaît pour ce système lorsque la sauvegarde est désactivée. Vous pouvez sélectionner ce bouton lorsque vous souhaitez réactiver la fonctionnalité de sauvegarde pour ce système.

Annuler l'enregistrement de NetApp Backup and Recovery pour un système

Vous pouvez annuler l'enregistrement de NetApp Backup and Recovery pour un système si vous ne souhaitez plus utiliser la fonctionnalité de sauvegarde et que vous souhaitez cesser d'être facturé pour les sauvegardes dans ce système. En général, cette fonctionnalité est utilisée lorsque vous prévoyez de supprimer un système et que vous souhaitez annuler le service de sauvegarde.

Vous pouvez également utiliser cette fonctionnalité si vous souhaitez modifier le magasin d'objets de destination dans lequel vos sauvegardes de cluster sont stockées. Après avoir désenregistré NetApp Backup and Recovery pour le système, vous pouvez activer NetApp Backup and Recovery pour ce cluster à l'aide des informations du nouveau fournisseur de cloud.

Avant de pouvoir désinscrire NetApp Backup and Recovery, vous devez effectuer les étapes suivantes, dans cet ordre :

- Désactiver NetApp Backup and Recovery pour le système
- Supprimer toutes les sauvegardes de ce système

L'option de désinscription n'est pas disponible tant que ces deux actions ne sont pas terminées.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez désinscrire le service de sauvegarde et sélectionnez **Désinscrire**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Désinscrire**.

Restaurer à partir des sauvegardes ONTAP

Restaurer les données ONTAP à partir de fichiers de sauvegarde avec NetApp Backup and Recovery

Les sauvegardes de vos données de volume ONTAP sont stockées sous forme d'instantanés, sur des volumes répliqués ou dans un stockage objet. Vous pouvez restaurer des données à partir de n'importe lequel de ces emplacements à un moment précis. Avec NetApp Backup and Recovery, vous pouvez restaurer un volume entier, un dossier ou des fichiers individuels selon vos besoins.

Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

- Vous pouvez restaurer un **volume** (en tant que nouveau volume) sur le système d'origine, sur un autre système utilisant le même compte cloud ou sur un système ONTAP sur site.
- Vous pouvez restaurer un **dossier** sur un volume du système d'origine, sur un volume d'un autre système utilisant le même compte cloud ou sur un volume d'un système ONTAP local.
- Vous pouvez restaurer des **fichiers** sur un volume du système d'origine, sur un volume d'un autre système utilisant le même compte cloud ou sur un volume d'un système ONTAP local.

Vous avez besoin d'une licence NetApp Backup and Recovery valide pour restaurer des données sur un système de production.

Pour résumer, voici les flux valides que vous pouvez utiliser pour restaurer des données de volume sur un système ONTAP :

- Fichier de sauvegarde → volume restauré
- Volume répliqué → volume restauré
- Instantané → volume restauré

Si l'opération de restauration ne se termine pas, attendez que le moniteur de tâches affiche « Échec » avant de réessayer l'opération de restauration.

Pour connaître les limitations liées à la restauration des données ONTAP , consultez"Limitations de sauvegarde et de restauration pour les volumes ONTAP" .

Le tableau de bord de restauration

Vous utilisez le tableau de bord de restauration pour effectuer des opérations de restauration de volumes, de dossiers et de fichiers. Pour accéder au tableau de bord de restauration, sélectionnez **Sauvegarde et récupération** dans le menu Console, puis sélectionnez l'onglet **Restaurer**. Vous pouvez également sélectionner > **Afficher le tableau de bord de restauration** à partir du service de sauvegarde et de récupération du panneau Services.

NetApp Backup and Recovery doit déjà être activé pour au moins un système et les fichiers de sauvegarde initiaux doivent exister.

Le tableau de bord de restauration propose deux manières différentes de restaurer des données à partir de fichiers de sauvegarde : **Parcourir et restaurer** et **Rechercher et restaurer**.

Comparaison de Parcourir et restaurer et de Rechercher et restaurer

En termes généraux, *Parcourir et restaurer* est généralement préférable lorsque vous devez restaurer un volume, un dossier ou un fichier spécifique de la semaine ou du mois dernier - et que vous connaissez le nom et l'emplacement du fichier, ainsi que la date à laquelle il était en bon état pour la dernière fois. *Rechercher et restaurer* est généralement plus efficace lorsque vous devez restaurer un volume, un dossier ou un fichier, mais que vous ne vous souvenez pas du nom exact, du volume dans lequel il réside ou de la date à laquelle il était en bon état pour la dernière fois.

Ce tableau fournit une comparaison des fonctionnalités des deux méthodes.

Parcourir et restaurer	Rechercher et restaurer
Parcourez une structure de type dossier pour trouver le volume, le dossier ou le fichier dans un seul fichier de sauvegarde.	Recherchez un volume, un dossier ou un fichier dans **tous les fichiers de sauvegarde** par nom de volume partiel ou complet, nom de dossier/fichier partiel ou complet, plage de taille et filtres de recherche supplémentaires.
Ne gère pas la récupération de fichier si le fichier a été supprimé ou renommé et que l'utilisateur ne connaît pas le nom du fichier d'origine	Gère les répertoires nouvellement créés/supprimés/renommés et les fichiers nouvellement créés/supprimés/renommés
La restauration rapide est prise en charge.	La restauration rapide n'est pas prise en charge.

Ce tableau fournit une liste d'opérations de restauration valides en fonction de l'emplacement où résident vos fichiers de sauvegarde.

Type de sauvegarde	Parcourir et restaurer			Rechercher et restaurer		
	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier
Instantané	Oui	Non	Non	Oui	Oui	Oui
Volume répliqué	Oui	Non	Non	Oui	Oui	Oui
Fichier de sauvegarde	Oui	Oui	Oui	Oui	Oui	Oui

Avant d'utiliser l'une ou l'autre méthode de restauration, configurez votre environnement pour qu'il réponde aux exigences en ressources. Consultez les sections suivantes pour plus de détails.

Consultez les exigences et les étapes de restauration pour le type d'opération de restauration que vous souhaitez utiliser :

- "Restaurer les volumes à l'aide de Parcourir et restaurer"
- "Restaurer des dossiers et des fichiers à l'aide de Parcourir et restaurer"
- "Restaurer des volumes, des dossiers et des fichiers à l'aide de la recherche et de la restauration"

Restaurez les données à partir des sauvegardes ONTAP à l'aide de la fonction Rechercher et restaurer.

Vous pouvez utiliser la fonction Rechercher et restaurer pour récupérer des volumes, des dossiers ou des fichiers à partir de fichiers de sauvegarde ONTAP . La fonction

Recherche et restauration vous permet d'effectuer des recherches dans toutes les sauvegardes (y compris les instantanés locaux, les volumes répliqués et le stockage d'objets) sans avoir besoin des noms exacts du système, du volume ou des fichiers.

La restauration à partir d'instantanés locaux ou de volumes répliqués est généralement plus rapide et moins coûteuse que la restauration à partir d'un stockage objet.

Lors de la restauration d'un volume complet, NetApp Backup and Recovery crée un nouveau volume à partir des données de sauvegarde. Vous pouvez effectuer une restauration sur le système d'origine, sur un autre système du même compte cloud ou sur un système ONTAP sur site. Les dossiers et les fichiers peuvent être restaurés à leur emplacement d'origine, sur un autre volume du même système, sur un autre système du même compte cloud ou sur un système sur site.

Les fonctionnalités de restauration dépendent de votre version ONTAP :

- **Dossiers :** Avec ONTAP 9.13.0 ou une version supérieure, vous pouvez restaurer des dossiers avec tous les fichiers et sous-dossiers ; avec les versions antérieures, vous ne pouvez restaurer que les fichiers contenus dans le dossier.
- **Stockage d'archives :** La restauration à partir du stockage d'archives (disponible avec ONTAP 9.10.1 ou supérieur) est plus lente et peut entraîner des coûts supplémentaires.
- **Exigences relatives aux clusters de destination :**
  - Restauration du volume : ONTAP 9.10.1 ou version ultérieure
  - Restauration de fichiers : ONTAP 9.11.1 ou version ultérieure
  - Google Archive et StorageGRID: ONTAP 9.12.1 ou version ultérieure
  - Restauration de dossiers : ONTAP 9.13.1 ou version ultérieure

"En savoir plus sur la restauration à partir du stockage d'archives AWS". "En savoir plus sur la restauration à partir du stockage d'archives Azure". "En savoir plus sur la restauration à partir du stockage d'archives Google".

- Si le fichier de sauvegarde dans le stockage d'objets a été configuré avec la protection DataLock et Ransomware, la restauration au niveau du dossier n'est prise en charge que si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Si le fichier de sauvegarde dans le stockage d'objets réside dans le stockage d'archives, la restauration au niveau du dossier est prise en charge uniquement si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer l'intégralité du volume à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.
- La priorité de restauration « Élevée » n'est pas prise en charge lors de la restauration des données du stockage d'archivage Azure vers les systèmes StorageGRID .
- La restauration de dossiers n'est actuellement pas prise en charge à partir de volumes dans le stockage d'objets ONTAP S3.

Avant de commencer, vous devez avoir une idée du nom ou de l'emplacement du volume ou du fichier que vous souhaitez restaurer.

Systèmes pris en charge par la recherche et la restauration et fournisseurs de stockage d'objets

Vous pouvez restaurer les données ONTAP à partir d'un fichier de sauvegarde résidant dans un système secondaire (un volume répliqué) ou dans un stockage d'objets (un fichier de sauvegarde) sur les systèmes suivants. Les instantanés résident sur le système source et ne peuvent être restaurés que sur ce même système.

Remarque : vous pouvez restaurer des volumes et des fichiers à partir de n'importe quel type de fichier de sauvegarde, mais vous ne pouvez restaurer un dossier qu'à partir de fichiers de sauvegarde dans le stockage d'objets pour le moment.

Emplacement du fichier de sauvegarde		Système de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Cloud Volumes ONTAP dans le système ONTAP sur site AWS
Azure Blob	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure
Stockage Google Cloud	Cloud Volumes ONTAP dans le système ONTAP sur site de Google	Cloud Volumes ONTAP dans le système ONTAP sur site de Google
NetApp StorageGRID	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site
ONTAP S3	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site

Pour la recherche et la restauration, l'agent de console peut être installé aux emplacements suivants :

- Pour Amazon S3, l'agent de console peut être déployé dans AWS ou dans vos locaux
- Pour Azure Blob, l'agent de console peut être déployé dans Azure ou dans vos locaux
- Pour Google Cloud Storage, l'agent de la console doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, l'agent de console doit être déployé dans vos locaux ; avec ou sans accès Internet
- Pour ONTAP S3, l'agent de console peut être déployé dans vos locaux (avec ou sans accès Internet) ou dans un environnement de fournisseur de cloud

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Prérequis de recherche et de restauration

Assurez-vous que votre environnement répond à ces exigences avant d'activer la fonction Rechercher et restaurer :

- Exigences du cluster :
  - La version ONTAP doit être 9.8 ou supérieure.
  - La machine virtuelle de stockage (SVM) sur laquelle réside le volume doit avoir un LIF de données configuré.
  - NFS doit être activé sur le volume (les volumes NFS et SMB/CIFS sont pris en charge).
  - Le serveur SnapDiff RPC doit être activé sur le SVM. La console le fait automatiquement lorsque vous activez l'indexation sur le système. (SnapDiff est la technologie qui identifie rapidement les différences

entre les fichiers et les répertoires dans les instantanés.)

- NetApp recommande de monter un volume distinct sur l'agent Console pour améliorer la résilience de la fonction Recherche et restauration. Pour les instructions, reportez-vous àmonter le volume pour réindexer le catalogue .

Prérequis pour la recherche et la restauration héritées (avec Indexed Catalog v1)

Voici les exigences relatives à la recherche et à la restauration lors de l'utilisation de l'indexation héritée :

- Exigences AWS :
  - Des autorisations spécifiques Amazon Athena, AWS Glue et AWS S3 doivent être ajoutées au rôle d'utilisateur qui fournit des autorisations à la console. "Assurez-vous que toutes les autorisations sont correctement configurées" .

    Notez que si vous utilisiez déjà NetApp Backup and Recovery avec un agent de console que vous avez configuré dans le passé, vous devrez désormais ajouter les autorisations Athena et Glue au rôle d'utilisateur de la console. Ils sont nécessaires pour la recherche et la restauration.

- Exigences Azure :
  - Vous devez enregistrer le fournisseur de ressources Azure Synapse Analytics (appelé « Microsoft.Synapse ») avec votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement" . Vous devez être le **Propriétaire** ou le **Contributeur** de l'abonnement pour enregistrer le fournisseur de ressources.
  - Des autorisations spécifiques au compte Azure Synapse Workspace et Data Lake Storage doivent être ajoutées au rôle d'utilisateur qui fournit des autorisations à la console. "Assurez-vous que toutes les autorisations sont correctement configurées" .

    Notez que si vous utilisiez déjà NetApp Backup and Recovery avec un agent de console que vous avez configuré dans le passé, vous devrez désormais ajouter les autorisations du compte Azure Synapse Workspace et Data Lake Storage au rôle d'utilisateur de la console. Ils sont nécessaires pour la recherche et la restauration.

  - L'agent de console doit être configuré **sans** serveur proxy pour la communication HTTP vers Internet. Si vous avez configuré un serveur proxy HTTP pour votre agent de console, vous ne pouvez pas utiliser la fonctionnalité de recherche et de restauration.
- Exigences de Google Cloud :
  - Des autorisations Google BigQuery spécifiques doivent être ajoutées au rôle d'utilisateur qui fournit des autorisations à la NetApp Console . "Assurez-vous que toutes les autorisations sont correctement configurées" .

    Si vous utilisiez déjà NetApp Backup and Recovery avec un agent de console que vous avez configuré dans le passé, vous devrez maintenant ajouter les autorisations BigQuery au rôle d'utilisateur de la console. Ils sont nécessaires pour la recherche et la restauration.

- Exigences StorageGRID et ONTAP S3 :

  Selon votre configuration, la recherche et la restauration sont implémentées de deux manières :

  - S'il n'y a pas d'informations d'identification de fournisseur cloud dans votre compte, les informations du catalogue indexé sont stockées sur l'agent de la console.

    Pour plus d'informations sur le catalogue indexé v2, consultez la section ci-dessous expliquant comment activer le catalogue indexé.

  - Si vous utilisez un agent de console sur un site privé (sombre), les informations du catalogue indexé sont stockées sur l'agent de console (nécessite la version 3.9.25 ou supérieure de l'agent de console).
  - Si vous avez "Informations d'identification AWS" ou "Informations d'identification Azure" dans le compte, le catalogue indexé est alors stocké chez le fournisseur de cloud, tout comme avec un agent de console déployé dans le cloud. (Si vous disposez des deux informations d'identification,

AWS est sélectionné par défaut.)

Même si vous utilisez un agent de console sur site, les exigences du fournisseur de cloud doivent être respectées pour les autorisations de l'agent de console et les ressources du fournisseur de cloud. Consultez les exigences AWS et Azure ci-dessus lors de l'utilisation de cette implémentation.

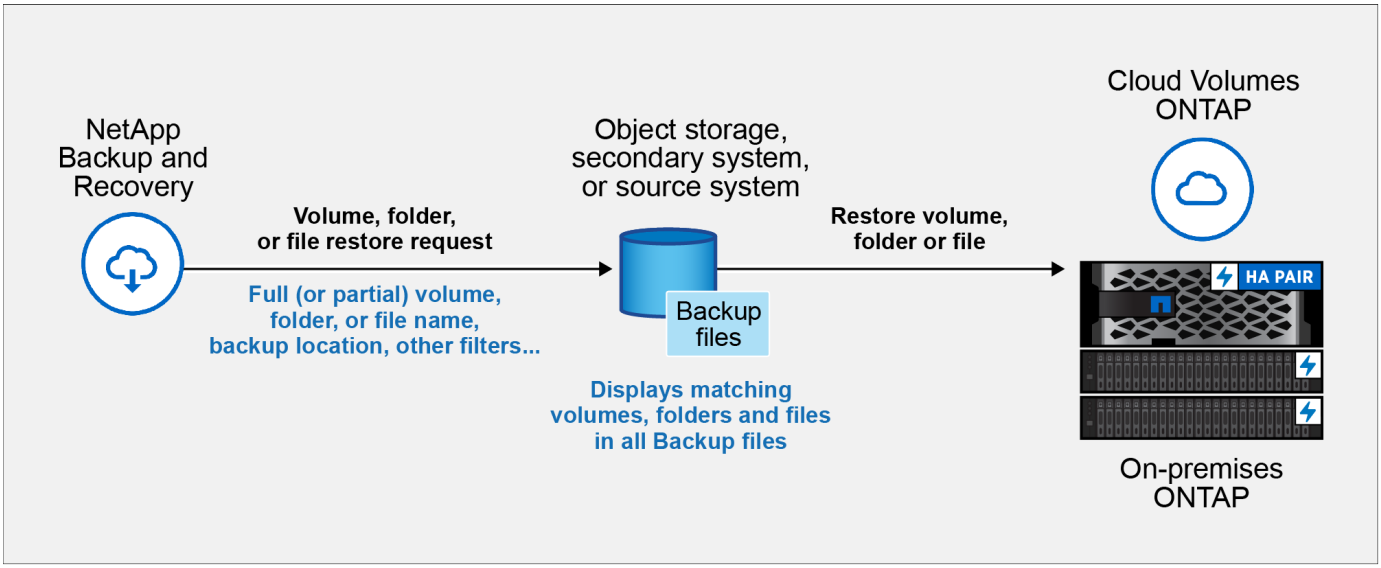
Processus de recherche et de restauration

Le processus se déroule comme suit :

1. Avant de pouvoir utiliser la recherche et la restauration, vous devez activer « Indexation » sur chaque système source à partir duquel vous souhaitez restaurer les données du volume. Cela permet au catalogue indexé de suivre les fichiers de sauvegarde pour chaque volume.
2. Lorsque vous souhaitez restaurer un volume ou des fichiers à partir d'une sauvegarde de volume, sous *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
3. Saisissez les critères de recherche d'un volume, d'un dossier ou d'un fichier par nom de volume partiel ou complet, nom de fichier partiel ou complet, emplacement de sauvegarde, plage de taille, plage de dates de création, autres filtres de recherche, puis sélectionnez **Rechercher**.

   La page Résultats de la recherche affiche tous les emplacements contenant un fichier ou un volume correspondant à vos critères de recherche.

4. Sélectionnez **Afficher toutes les sauvegardes** pour l'emplacement que vous souhaitez utiliser pour restaurer le volume ou le fichier, puis sélectionnez **Restaurer** sur le fichier de sauvegarde réel que vous souhaitez utiliser.
5. Sélectionnez l'emplacement où vous souhaitez que le volume, le dossier ou les fichiers soient restaurés et sélectionnez **Restaurer**.
6. Le volume, le dossier ou le(s) fichier(s) sont restaurés.



Il vous suffit de connaître une partie du nom, et NetApp Backup and Recovery effectue une recherche dans tous les fichiers de sauvegarde correspondants.

Activer le catalogue indexé pour chaque système

Avant de pouvoir utiliser la recherche et la restauration, vous devez activer « Indexation » sur chaque système source à partir duquel vous prévoyez de restaurer des volumes ou des fichiers. Cela permet au catalogue indexé de suivre chaque volume et chaque fichier de sauvegarde, ce qui rend vos recherches très rapides et efficaces.

Le catalogue indexé est une base de données qui stocke les métadonnées sur tous les volumes et fichiers de sauvegarde de votre système. Il est utilisé par la fonctionnalité Rechercher et restaurer pour trouver rapidement les fichiers de sauvegarde contenant les données que vous souhaitez restaurer.

Fonctionnalités du catalogue indexé

NetApp Backup and Recovery ne provisionne pas de compartiment séparé lorsque vous utilisez le catalogue indexé. Au lieu de cela, pour les sauvegardes stockées dans AWS, Azure, Google Cloud Platform, StorageGRID ou ONTAP S3, le service fournit de l'espace sur l'agent de la console ou sur l'environnement du fournisseur de cloud.

Le catalogue indexé prend en charge les éléments suivants :

- Efficacité de la recherche globale en moins de 3 minutes
- Jusqu'à 5 milliards de fichiers
- Jusqu'à 5 000 volumes par cluster
- Jusqu'à 100 000 instantanés par volume
- Le délai maximal pour l'indexation de base est inférieur à 7 jours. Le temps réel varie en fonction de votre environnement.

Étapes pour activer l'indexation pour un système :

Si l'indexation a déjà été activée pour votre système, passez à la section suivante pour restaurer vos données.

Vous devrez d'abord monter un volume séparé pour stocker les fichiers de catalogue. Cela évite la perte de données si la taille des fichiers contenant les instantanés devient trop importante. Cela n'est pas nécessaire sur tous les clusters ; vous pouvez monter n'importe quel volume provenant de n'importe quel cluster de votre environnement. Si vous ne le faites pas, l'indexation risque de ne pas fonctionner correctement.

Pour le volume monté, utilisez les indications de dimensionnement suivantes :

- Utilisez un volume NFS NetApp
- Stockage AFF recommandé avec un débit disque de 300 Mo/s. La baisse du débit aura un impact sur la recherche et les autres opérations.
- Activez les instantanés NetApp pour sécuriser les métadonnées du catalogue en plus des fichiers zip de sauvegarde du catalogue.
- 50 Go par milliard de fichiers
- 20 Go pour les données du catalogue, avec un espace supplémentaire pour la création de fichiers zip et les fichiers temporaires.

Étape pour monter le volume afin de réindexer le catalogue

1. Montez le volume sur `/opt/application/netapp/cbs` en saisissant la commande suivante, où :
    - `volume name` est le volume du cluster où seront stockés les fichiers de catalogue
    - `/opt/application/netapp/cbs` est le chemin où il est monté

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

Exemple:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Étapes pour activer l'index

1. Effectuez l'une des opérations suivantes :
   - Si aucun système n'a été indexé, sur le tableau de bord de restauration sous *Rechercher et restaurer*, sélectionnez **Activer l'indexation pour les systèmes**.
   - Si au moins un système a déjà été indexé, sur le tableau de bord de restauration sous *Rechercher et restaurer*, sélectionnez **Paramètres d'indexation**.
2. Sélectionnez **Activer l'indexation** pour le système.

Résultat

Une fois tous les services provisionnés et le catalogue indexé activé, le système s'affiche comme « Actif ».

Selon la taille des volumes du système et le nombre de fichiers de sauvegarde dans les 3 emplacements de sauvegarde, le processus d'indexation initial peut prendre jusqu'à une heure. Après cela, il est mis à jour de manière transparente toutes les heures avec des modifications progressives pour rester à jour.

Restaurer des volumes, des dossiers et des fichiers à l'aide de la recherche et de la restauration

Après avoirActivation de l'indexation pour votre système , vous pouvez restaurer des volumes, des dossiers et des fichiers à l'aide de la recherche et de la restauration. Cela vous permet d'utiliser une large gamme de filtres pour trouver le fichier ou le volume exact que vous souhaitez restaurer à partir de tous les fichiers de sauvegarde.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
4. Dans la section *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
5. Depuis la page Rechercher et restaurer :
   a. Dans la *barre de recherche*, saisissez un nom de volume, un nom de dossier ou un nom de fichier complet ou partiel.
   b. Sélectionnez le type de ressource : **Volumes**, **Fichiers**, **Dossiers** ou **Tous**.
   c. Dans la zone *Filtrer par*, sélectionnez les critères de filtre. Par exemple, vous pouvez sélectionner le système sur lequel résident les données et le type de fichier, par exemple un fichier .JPEG. Vous pouvez également sélectionner le type d'emplacement de sauvegarde si vous souhaitez effectuer la recherche uniquement parmi les instantanés ou les fichiers de sauvegarde disponibles dans le stockage d'objets.
6. Sélectionnez **Rechercher** et la zone Résultats de la recherche affiche toutes les ressources qui ont un fichier, un dossier ou un volume correspondant à votre recherche.

7. Recherchez la ressource contenant les données que vous souhaitez restaurer et sélectionnez **Afficher toutes les sauvegardes** pour afficher tous les fichiers de sauvegarde contenant le volume, le dossier ou le fichier correspondant.
8. Localisez le fichier de sauvegarde que vous souhaitez utiliser pour restaurer les données et sélectionnez **Restaurer**.

   Notez que les résultats identifient les instantanés de volumes locaux et les volumes répliqués distants qui contiennent le fichier recherché. Vous pouvez choisir de restaurer à partir du fichier de sauvegarde cloud, à partir de l'instantané ou à partir du volume répliqué.

9. Sélectionnez l'emplacement de destination où vous souhaitez que le volume, le dossier ou les fichiers soient restaurés et sélectionnez **Restaurer**.
   - Pour les volumes, vous pouvez sélectionner le système de destination d'origine ou un autre système. Lors de la restauration d'un volume FlexGroup , vous devrez choisir plusieurs agrégats.
   - Pour les dossiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, notamment le système, le volume et le dossier.
   - Pour les fichiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, notamment le système, le volume et le dossier. Lors de la sélection de l'emplacement d'origine, vous pouvez choisir d'écraser le(s) fichier(s) source ou de créer de nouveaux fichiers.

     Si vous sélectionnez un système ONTAP sur site et que vous n'avez pas encore configuré la connexion du cluster au stockage d'objets, vous êtes invité à fournir des informations supplémentaires :

     - Lors de la restauration à partir d'Amazon S3, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, entrez la clé d'accès et la clé secrète de l'utilisateur que vous avez créé pour donner au cluster ONTAP l'accès au compartiment S3 et choisissez éventuellement un point de terminaison VPC privé pour un transfert de données sécurisé. "Voir les détails sur ces exigences" .
     - Lors de la restauration à partir d'Azure Blob, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination et choisissez éventuellement un point de terminaison privé pour le transfert de données sécurisé en sélectionnant le réseau virtuel et le sous-réseau. "Voir les détails sur ces exigences" .
     - Lors de la restauration à partir de Google Cloud Storage, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, ainsi que la clé d'accès et la clé secrète pour accéder au stockage d'objets. "Voir les détails sur ces exigences" .
     - Lors de la restauration à partir de StorageGRID, entrez le nom de domaine complet du serveur StorageGRID et le port ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où réside le volume de destination. "Voir les détails sur ces exigences" .
     - Lors de la restauration à partir d' ONTAP S3, saisissez le nom de domaine complet du serveur ONTAP S3 et le port ONTAP doit utiliser pour la communication HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où résidera le volume de destination. "Voir les détails sur ces exigences" .

Résultats

Le volume, le dossier ou les fichiers sont restaurés et vous revenez au tableau de bord de restauration afin que vous puissiez examiner la progression de l'opération de restauration. Vous pouvez également sélectionner l'onglet **Surveillance des tâches** pour voir la progression de la restauration. Voir"Page de surveillance des

tâches" .

Restaurer les données ONTAP à l'aide de Parcourir et restaurer

Avec NetApp Backup and Recovery, restaurez les données ONTAP à l'aide de Browse & Restore. Avant la restauration, notez le nom du volume source, le système source et le SVM, ainsi que la date du fichier de sauvegarde. Vous pouvez restaurer les données ONTAP à partir d'un instantané, d'un volume répliqué ou de sauvegardes stockées dans un stockage objet.

Les fonctionnalités de restauration dépendent de votre version ONTAP :

- **Dossiers :** Avec ONTAP 9.13.0 ou une version supérieure, vous pouvez restaurer des dossiers avec tous les fichiers et sous-dossiers ; avec les versions antérieures, vous ne pouvez restaurer que les fichiers contenus dans le dossier.
- **Stockage d'archives :** La restauration à partir du stockage d'archives (disponible avec ONTAP 9.10.1 ou supérieur) est plus lente et peut entraîner des coûts supplémentaires.
- **Exigences relatives aux clusters de destination :**
  - Restauration du volume : ONTAP 9.10.1 ou version ultérieure
  - Restauration de fichiers : ONTAP 9.11.1 ou version ultérieure
  - Google Archive et StorageGRID: ONTAP 9.12.1 ou version ultérieure
  - Restauration de dossiers : ONTAP 9.13.1 ou version ultérieure

"En savoir plus sur la restauration à partir du stockage d'archives AWS". "En savoir plus sur la restauration à partir du stockage d'archives Azure". "En savoir plus sur la restauration à partir du stockage d'archives Google".

La priorité élevée n'est pas prise en charge lors de la restauration des données du stockage d'archivage Azure vers les systèmes StorageGRID .

Parcourir et restaurer les systèmes pris en charge et les fournisseurs de stockage d'objets

Vous pouvez restaurer les données ONTAP à partir d'un fichier de sauvegarde résidant dans un système secondaire (un volume répliqué) ou dans un stockage d'objets (un fichier de sauvegarde) sur les systèmes suivants. Les instantanés résident sur le système source et ne peuvent être restaurés que sur ce même système.

Remarque : vous pouvez restaurer un volume à partir de n'importe quel type de fichier de sauvegarde, mais vous ne pouvez restaurer un dossier ou des fichiers individuels qu'à partir d'un fichier de sauvegarde dans le stockage d'objets pour le moment.

Depuis le magasin d'objets (sauvegarde)	Depuis le primaire (instantané)	Depuis le système secondaire (réplication)	Vers le système de destination
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Azure Blob
Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Stockage Google Cloud	Cloud Volumes ONTAP dans le système ONTAP sur site de Google

Depuis le magasin d'objets (sauvegarde)	Depuis le primaire (instantané)	Depuis le système secondaire (réplication)	Vers le système de destination
Cloud Volumes ONTAP dans le système ONTAP sur site de Google	NetApp StorageGRID	Système ONTAP sur site	Système ONTAP sur site Cloud Volumes ONTAP
Vers le système ONTAP sur site	ONTAP S3	Système ONTAP sur site	Système ONTAP sur site Cloud Volumes ONTAP

Pour la navigation et la restauration, l'agent de console peut être installé aux emplacements suivants :

- Pour Amazon S3, l'agent de console peut être déployé dans AWS ou dans vos locaux
- Pour Azure Blob, l'agent de console peut être déployé dans Azure ou dans vos locaux
- Pour Google Cloud Storage, l'agent de la console doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, l'agent de console doit être déployé dans vos locaux ; avec ou sans accès Internet
- Pour ONTAP S3, l'agent de console peut être déployé dans vos locaux (avec ou sans accès Internet) ou dans un environnement de fournisseur de cloud

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

Si la version ONTAP de votre système est inférieure à 9.13.1, vous ne pouvez pas restaurer de dossiers ou de fichiers si le fichier de sauvegarde a été configuré avec DataLock & Ransomware. Dans ce cas, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder aux fichiers dont vous avez besoin.

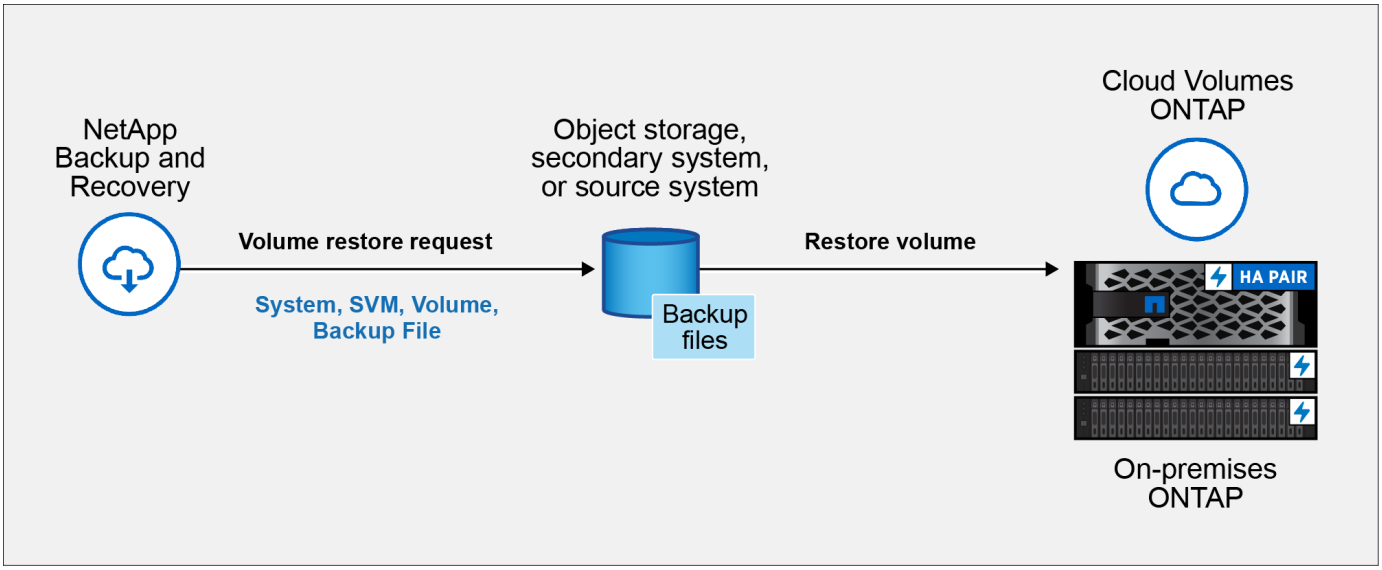
Restaurer les volumes à l'aide de Parcourir et restaurer

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, NetApp Backup and Recovery crée un *nouveau* volume à l'aide des données de la sauvegarde. Lorsque vous utilisez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données sur un volume du système d'origine, sur un autre système situé dans le même compte cloud que le système source ou sur un système ONTAP local.

Lors de la restauration d'une sauvegarde cloud sur un système Cloud Volumes ONTAP utilisant ONTAP 9.13.0 ou une version ultérieure ou sur un système ONTAP local exécutant ONTAP 9.14.1, vous aurez la possibilité d'effectuer une opération de *restauration rapide*. La restauration rapide est idéale pour les situations de reprise après sinistre où vous devez fournir l'accès à un volume dès que possible. Une restauration rapide restaure les métadonnées du fichier de sauvegarde sur un volume au lieu de restaurer l'intégralité du fichier de sauvegarde. La restauration rapide n'est pas recommandée pour les applications sensibles aux performances ou à la latence, et elle n'est pas prise en charge avec les sauvegardes dans le stockage archivé.

La restauration rapide est prise en charge pour les volumes FlexGroup uniquement si le système source à partir duquel la sauvegarde cloud a été créée exécutait ONTAP 9.12.1 ou une version ultérieure. Et il est pris en charge pour les volumes SnapLock uniquement si le système source exécutait ONTAP 9.11.0 ou une version ultérieure.

Lors de la restauration à partir d'un volume répliqué, vous pouvez restaurer le volume sur le système d'origine ou sur un système Cloud Volumes ONTAP ou ONTAP sur site.



Pour restaurer un volume, vous avez besoin du nom du système source, de la machine virtuelle de stockage, du nom du volume et de la date du fichier de sauvegarde.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Parcourir et restaurer*, sélectionnez **Restaurer le volume**.
4. Dans la page *Sélectionner la source*, accédez au fichier de sauvegarde du volume que vous souhaitez restaurer. Sélectionnez le **système**, le **volume** et le fichier de **sauvegarde** contenant l'horodatage à partir duquel vous souhaitez effectuer la restauration.

   La colonne **Emplacement** indique si le fichier de sauvegarde (instantané) est **Local** (un instantané sur le système source), **Secondaire** (un volume répliqué sur un système ONTAP secondaire) ou **Stockage d'objets** (un fichier de sauvegarde dans le stockage d'objets). Choisissez le fichier que vous souhaitez restaurer.

5. Sélectionnez **Suivant**.

   Notez que si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que Ransomware Resilience est actif pour cette sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la politique de sauvegarde), vous êtes invité à exécuter une analyse de ransomware supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'analyser le fichier de sauvegarde à la recherche de ransomwares. (Vous devrez payer des frais de sortie supplémentaires auprès de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.)

6. Dans la page *Sélectionner la destination*, sélectionnez le **système** sur lequel vous souhaitez restaurer le volume.
7. Lors de la restauration d'un fichier de sauvegarde à partir du stockage d'objets, si vous sélectionnez un système ONTAP local et que vous n'avez pas déjà configuré la connexion du cluster au stockage d'objets, vous êtes invité à fournir des informations supplémentaires :
   - Lors de la restauration à partir d'Amazon S3, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, entrez la clé d'accès et la clé secrète de l'utilisateur que vous avez créé pour donner au cluster ONTAP l'accès au compartiment S3 et choisissez éventuellement un point de terminaison VPC privé pour un transfert de données sécurisé.

- Lors de la restauration à partir d'Azure Blob, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, sélectionnez l'abonnement Azure pour accéder au stockage d'objets et choisissez éventuellement un point de terminaison privé pour le transfert de données sécurisé en sélectionnant le réseau virtuel et le sous-réseau.
- Lors de la restauration à partir de Google Cloud Storage, sélectionnez le projet Google Cloud et la clé d'accès et la clé secrète pour accéder au stockage d'objets, la région où les sauvegardes sont stockées et l'espace IP dans le cluster ONTAP où résidera le volume de destination.
- Lors de la restauration à partir de StorageGRID, saisissez le nom de domaine complet du serveur StorageGRID et le port ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où résidera le volume de destination.
- Lors de la restauration à partir d' ONTAP S3, saisissez le nom de domaine complet du serveur ONTAP S3 et le port ONTAP doit utiliser pour la communication HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où résidera le volume de destination.

8. Saisissez le nom que vous souhaitez utiliser pour le volume restauré, puis sélectionnez la machine virtuelle de stockage et l'agrégat où résidera le volume. Lors de la restauration d'un volume FlexGroup , vous devrez sélectionner plusieurs agrégats. Par défaut, **<source_volume_name>_restore** est utilisé comme nom de volume.

   Lors de la restauration d'une sauvegarde à partir du stockage d'objets vers un système Cloud Volumes ONTAP utilisant ONTAP 9.13.0 ou une version ultérieure ou vers un système ONTAP local exécutant ONTAP 9.14.1, vous aurez la possibilité d'effectuer une opération de *restauration rapide*.

   Et si vous restaurez le volume à partir d'un fichier de sauvegarde qui réside dans un niveau de stockage d'archivage (disponible à partir d' ONTAP 9.10.1), vous pouvez sélectionner la priorité de restauration.

   "En savoir plus sur la restauration à partir du stockage d'archives AWS". "En savoir plus sur la restauration à partir du stockage d'archives Azure" . "En savoir plus sur la restauration à partir du stockage d'archives Google" . Les fichiers de sauvegarde dans le niveau de stockage Google Archive sont restaurés presque immédiatement et ne nécessitent aucune priorité de restauration.

9. Sélectionnez **Suivant** pour choisir si vous souhaitez effectuer un processus de restauration normale ou rapide :
   - **Restauration normale** : utilisez la restauration normale sur les volumes qui nécessitent des performances élevées. Les volumes ne seront pas disponibles tant que le processus de restauration ne sera pas terminé.
   - **Restauration rapide** : les volumes et données restaurés seront disponibles immédiatement. N'utilisez pas cette option sur des volumes nécessitant des performances élevées, car pendant le processus de restauration rapide, l'accès aux données peut être plus lent que d'habitude.
10. Sélectionnez **Restaurer** et vous revenez au tableau de bord de restauration afin de pouvoir examiner la progression de l'opération de restauration.

Résultat

NetApp Backup and Recovery crée un nouveau volume basé sur la sauvegarde que vous avez sélectionnée.

Notez que la restauration d'un volume à partir d'un fichier de sauvegarde résidant dans un stockage d'archives peut prendre plusieurs minutes ou heures selon le niveau d'archivage et la priorité de restauration. Vous pouvez sélectionner l'onglet **Surveillance des tâches** pour voir la progression de la restauration.

Restaurer des dossiers et des fichiers à l'aide de Parcourir et restaurer

Si vous devez restaurer uniquement quelques fichiers à partir d'une sauvegarde de volume ONTAP , vous pouvez choisir de restaurer un dossier ou des fichiers individuels au lieu de restaurer l'intégralité du volume. Vous pouvez restaurer des dossiers et des fichiers sur un volume existant dans le système d'origine ou sur un autre système utilisant le même compte cloud. Vous pouvez également restaurer des dossiers et des fichiers sur un volume sur un système ONTAP local.

> Vous ne pouvez restaurer un dossier ou des fichiers individuels qu'à partir d'un fichier de sauvegarde dans le stockage d'objets à ce stade. La restauration de fichiers et de dossiers n'est actuellement pas prise en charge à partir d'un instantané local ou d'un fichier de sauvegarde situé sur un système secondaire (un volume répliqué).

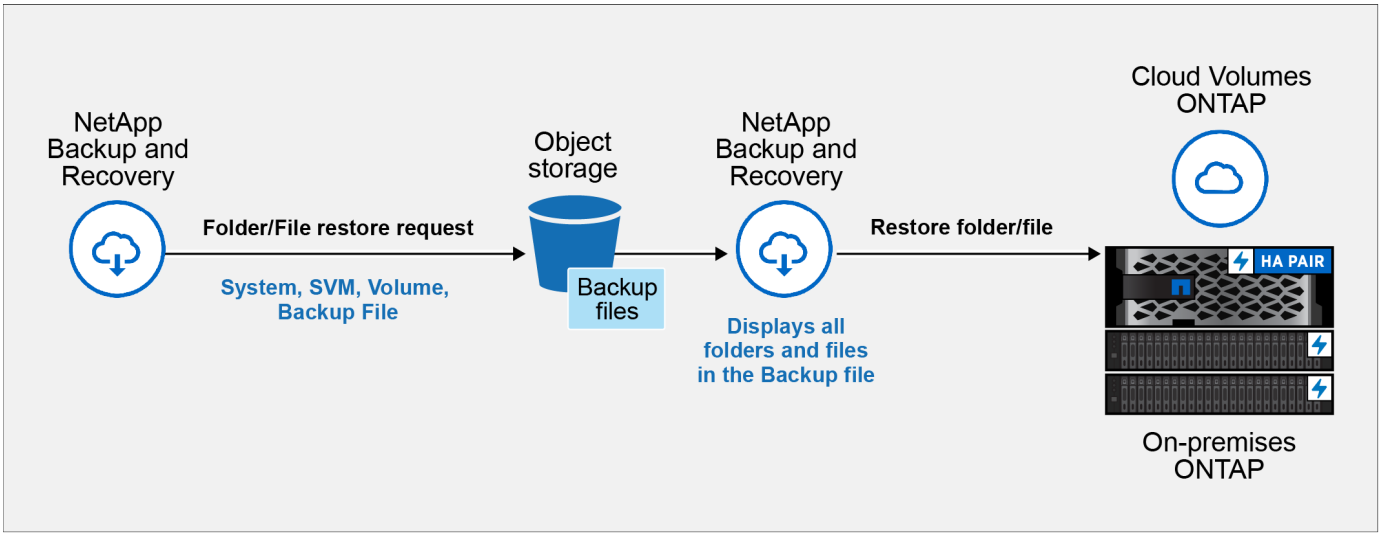
Si vous sélectionnez plusieurs fichiers, ils seront restaurés sur le même volume de destination. Pour restaurer des fichiers sur différents volumes, exécutez le processus plusieurs fois.

Lorsque vous utilisez ONTAP 9.13.0 ou une version ultérieure, vous pouvez restaurer un dossier avec tous les fichiers et sous-dossiers qu'il contient. Lorsque vous utilisez une version d' ONTAP antérieure à 9.13.0, seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans les sous-dossiers, n'est restauré.

> - Si le fichier de sauvegarde a été configuré avec la protection DataLock et Ransomware, la restauration au niveau du dossier n'est prise en charge que si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder au dossier et aux fichiers dont vous avez besoin.
> - Si le fichier de sauvegarde réside dans un stockage d'archives, la restauration au niveau du dossier n'est prise en charge que si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer l'intégralité du volume à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.
> - Avec ONTAP 9.15.1, vous pouvez restaurer les dossiers FlexGroup à l'aide de l'option « Parcourir et restaurer ». Cette fonctionnalité est en mode Aperçu technologique.
>
> Vous pouvez le tester en utilisant un indicateur spécial décrit dans le "Blog sur la version de juillet 2024 de NetApp Backup and Recovery" .

Restaurer des dossiers et des fichiers

Suivez ces étapes pour restaurer des dossiers ou des fichiers sur un volume à partir d'une sauvegarde de volume ONTAP . Vous devez connaître le nom du volume et la date du fichier de sauvegarde que vous souhaitez utiliser pour restaurer le dossier ou le(s) fichier(s). Cette fonctionnalité utilise la navigation en direct pour que vous puissiez afficher la liste des répertoires et des fichiers dans chaque fichier de sauvegarde.



Avant de commencer

- La version ONTAP doit être 9.6 ou supérieure pour effectuer des opérations de restauration de *fichier*.
- La version ONTAP doit être 9.11.1 ou supérieure pour effectuer des opérations de restauration de *dossier*. La version 9.13.1 ONTAP est requise si les données sont stockées dans un stockage d'archives ou si le fichier de sauvegarde utilise la protection DataLock et Ransomware.
- La version ONTAP doit être 9.15.1 p2 ou supérieure pour restaurer les répertoires FlexGroup à l'aide de l'option Parcourir et restaurer.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Parcourir et restaurer*, sélectionnez **Restaurer les fichiers ou le dossier**.
4. Dans la page *Sélectionner la source*, accédez au fichier de sauvegarde du volume qui contient le dossier ou les fichiers que vous souhaitez restaurer. Sélectionnez le **système**, le **volume** et la **sauvegarde** contenant la date et l'heure à partir desquelles vous souhaitez restaurer les fichiers.
5. Sélectionnez **Suivant** et la liste des dossiers et fichiers de la sauvegarde du volume s'affiche.

   Si vous restaurez des dossiers ou des fichiers à partir d'un fichier de sauvegarde qui réside dans un niveau de stockage d'archivage, vous pouvez sélectionner la priorité de restauration.

   "En savoir plus sur la restauration à partir du stockage d'archives AWS". "En savoir plus sur la restauration à partir du stockage d'archives Azure" . "En savoir plus sur la restauration à partir du stockage d'archives Google" . Les fichiers de sauvegarde dans le niveau de stockage Google Archive sont restaurés presque immédiatement et ne nécessitent aucune priorité de restauration.

   Et si Ransomware Resilience est actif pour le fichier de sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la politique de sauvegarde), vous êtes alors invité à exécuter une analyse de ransomware supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'analyser le fichier de sauvegarde à la recherche de ransomwares. (Vous devrez payer des frais de sortie supplémentaires auprès de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.)

6. Dans la page *Sélectionner les éléments*, sélectionnez le dossier ou le(s) fichier(s) que vous souhaitez restaurer et sélectionnez **Continuer**. Pour vous aider à trouver l'article :

- Vous pouvez sélectionner le nom du dossier ou du fichier si vous le voyez.
- Vous pouvez sélectionner l'icône de recherche et saisir le nom du dossier ou du fichier pour accéder directement à l'élément.
- Vous pouvez parcourir les niveaux vers le bas dans les dossiers en utilisant la flèche vers le bas à la fin de la ligne pour rechercher des fichiers spécifiques.

  Au fur et à mesure que vous sélectionnez des fichiers, ils sont ajoutés sur le côté gauche de la page afin que vous puissiez voir les fichiers que vous avez déjà choisis. Vous pouvez supprimer un fichier de cette liste si nécessaire en sélectionnant le **x** à côté du nom du fichier.

7. Dans la page *Sélectionner la destination*, sélectionnez le **système** sur lequel vous souhaitez restaurer les éléments.

   Si vous sélectionnez un cluster sur site et que vous n'avez pas encore configuré la connexion du cluster au stockage d'objets, vous êtes invité à fournir des informations supplémentaires :

   - Lors de la restauration à partir d'Amazon S3, saisissez l'espace IP dans le cluster ONTAP où réside le volume de destination, ainsi que la clé d'accès AWS et la clé secrète nécessaires pour accéder au stockage d'objets. Vous pouvez également sélectionner une configuration de lien privé pour la connexion au cluster.
   - Lors de la restauration à partir d'Azure Blob, entrez l'espace IP dans le cluster ONTAP où réside le volume de destination. Vous pouvez également sélectionner une configuration de point de terminaison privé pour la connexion au cluster.
   - Lors de la restauration à partir de Google Cloud Storage, saisissez l'espace IP dans le cluster ONTAP où résident les volumes de destination, ainsi que la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets.
   - Lors de la restauration à partir de StorageGRID, entrez le nom de domaine complet du serveur StorageGRID et le port ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où réside le volume de destination.
8. Sélectionnez ensuite le **Volume** et le **Dossier** dans lesquels vous souhaitez restaurer le dossier ou les fichiers.

   Vous disposez de plusieurs options pour l'emplacement lors de la restauration des dossiers et des fichiers.

   - Lorsque vous avez choisi **Sélectionner le dossier cible**, comme indiqué ci-dessus :
     - Vous pouvez sélectionner n'importe quel dossier.
     - Vous pouvez survoler un dossier et cliquer à la fin de la ligne pour accéder aux sous-dossiers, puis sélectionner un dossier.
   - Si vous avez sélectionné le même système de destination et le même volume que celui où se trouvait le dossier/fichier source, vous pouvez sélectionner **Conserver le chemin du dossier source** pour restaurer le dossier ou les fichiers dans le même dossier où ils existaient dans la structure source. Tous les mêmes dossiers et sous-dossiers doivent déjà exister ; les dossiers ne sont pas créés. Lors de la restauration des fichiers à leur emplacement d'origine, vous pouvez choisir d'écraser le(s) fichier(s) source ou de créer de nouveaux fichiers.
9. Sélectionnez **Restaurer** pour revenir au tableau de bord de restauration et consulter la progression de l'opération de restauration.

Protégez les charges de travail Microsoft SQL Server

Présentation de la protection des charges de travail Microsoft SQL à l'aide de NetApp Backup and Recovery

Sauvegardez les données de votre application Microsoft SQL Server à partir de systèmes ONTAP locaux vers AWS, Azure ou StorageGRID à l'aide de NetApp Backup and Recovery. Le système crée et stocke automatiquement des sauvegardes dans votre compte cloud, conformément à vos politiques. Utilisez une stratégie 3-2-1 : conservez trois copies de vos données sur deux systèmes de stockage et une copie dans le cloud.

Les avantages de l'approche 3-2-1 incluent :

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.
- L'utilisation de différents types de supports vous aide à récupérer si l'un d'eux tombe en panne.
- Vous pouvez restaurer rapidement à partir de la copie sur site et utiliser les copies hors site si la copie sur site est compromise.

NetApp Backup and Recovery utilise NetApp SnapMirror pour synchroniser les sauvegardes en créant des instantanés et en les transférant vers les emplacements de sauvegarde.

Vous pouvez faire ce qui suit pour protéger vos données :

- "Configurer des éléments supplémentaires en cas d'importation depuis SnapCenter"
- "Découvrez les charges de travail Microsoft SQL Server et importez éventuellement des ressources SnapCenter"
- "Sauvegardez les charges de travail avec des snapshots locaux sur le stockage principal ONTAP local"
- "Répliquer les charges de travail vers le stockage secondaire ONTAP"
- "Sauvegarder les charges de travail vers un emplacement de stockage d'objets"
- "Sauvegardez les charges de travail maintenant"
- "Restaurer les charges de travail"
- "Cloner les charges de travail"
- "Gérer l'inventaire des charges de travail"
- "Gérer les instantanés"

Pour sauvegarder les charges de travail, vous créez des stratégies qui gèrent les opérations de sauvegarde et de restauration. Voir"Créer des politiques" pour plus d'informations.

Destinations de sauvegarde prises en charge

NetApp Backup and Recovery vous permet de sauvegarder des instances et des bases de données Microsoft SQL Server à partir des systèmes sources suivants vers les systèmes secondaires et le stockage objet suivants, chez les fournisseurs de cloud public et privé. Les instantanés résident sur le système source.

Système source	Système secondaire (réplication)	Magasin d'objets de destination (sauvegarde)
Cloud Volumes ONTAP dans AWS	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Amazon S3 ONTAP S3
Cloud Volumes ONTAP dans Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Azure Blob ONTAP S3
Système ONTAP sur site	Cloud Volumes ONTAP Système ONTAP sur site	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / A

Destinations de restauration prises en charge

Vous pouvez restaurer des instances et des bases de données Microsoft SQL Server à partir d'une sauvegarde qui réside dans le stockage principal ou un système secondaire (un volume répliqué) ou dans le stockage d'objets (un fichier de sauvegarde) sur les systèmes suivants. Les instantanés résident sur le système source et ne peuvent être restaurés que sur ce même système.

À partir de l'emplacement du fichier de sauvegarde		Vers le système de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Volumes cloud dans le système ONTAP sur site AWS ONTAP S3
Azure Blob	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans Azure, système ONTAP local , ONTAP S3
StorageGRID	Cloud Volumes ONTAP Système ONTAP sur site	Système ONTAP sur site ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / A

Les références aux « systèmes ONTAP sur site » incluent les systèmes FAS et AFF .

Conditions préalables à l'importation depuis le service Plug-in vers NetApp Backup and Recovery

Si vous souhaitez importer des ressources du service de plug-in SnapCenter pour Microsoft SQL Server dans NetApp Backup and Recovery, vous devrez configurer quelques éléments supplémentaires.

Créez d'abord des systèmes dans la NetApp Console

Si vous souhaitez importer des ressources depuis SnapCenter, vous devez d'abord ajouter tout le stockage de cluster SnapCenter local à la page **Systèmes** de la console avant de procéder à l'importation depuis SnapCenter. Cela garantit que les ressources de l'hôte peuvent être découvertes et importées correctement.

Assurez-vous que les exigences de l'hôte sont respectées pour installer le plug-in SnapCenter

Pour importer des ressources à partir du plug-in SnapCenter pour Microsoft SQL Server, assurez-vous que les exigences de l'hôte pour installer le plug-in SnapCenter pour Microsoft SQL Server sont respectées.

Vérifiez spécifiquement les exigences de SnapCenter dans"Conditions préalables à la NetApp Backup and Recovery" .

Désactiver les restrictions à distance du contrôle de compte d'utilisateur

Avant d'importer des ressources depuis SnapCenter, désactivez les restrictions à distance du contrôle de compte d'utilisateur (UAC) sur l'hôte Windows SnapCenter . Désactivez l'UAC si vous utilisez un compte d'administration local pour vous connecter à distance à l'hôte SnapCenter Server ou à l'hôte SQL.

Considérations de sécurité

Tenez compte des points suivants avant de désactiver les restrictions à distance UAC :

- Risques de sécurité : la désactivation du filtrage des jetons peut exposer votre système à des vulnérabilités de sécurité, en particulier si les comptes administratifs locaux sont compromis par des acteurs malveillants.
- À utiliser avec précaution :
  - Modifiez ce paramètre uniquement s'il est essentiel pour vos tâches administratives.
  - Assurez-vous que des mots de passe forts et d'autres mesures de sécurité sont en place pour protéger les comptes administratifs.

Solutions alternatives

- Si un accès administratif à distance est requis, envisagez d'utiliser des comptes de domaine avec des privilèges appropriés.
- Utilisez des outils de gestion à distance sécurisés qui adhèrent aux meilleures pratiques de sécurité pour minimiser les risques.

Étapes pour désactiver les restrictions à distance du contrôle de compte d'utilisateur

1. Modifier le `LocalAccountTokenFilterPolicy` clé de registre sur l'hôte Windows SnapCenter .

   Faites-le en utilisant l'un des éléments suivants, avec les instructions ci-après :

   - Méthode 1 : Éditeur du Registre
   - Méthode 2 : script PowerShell

Méthode 1 : désactiver le contrôle de compte d'utilisateur à l'aide de l'éditeur de registre

C'est l'une des méthodes que vous pouvez utiliser pour désactiver le contrôle de compte d'utilisateur.

Étapes

1. Ouvrez l'Éditeur du Registre sur l'hôte Windows SnapCenter en procédant comme suit :
   a. Presse `Windows+R` pour ouvrir la boîte de dialogue Exécuter.
   b. Taper `regedit` et appuyez sur `Enter` .
2. Accédez à la clé de politique :

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

3. Créer ou modifier le `DWORD` valeur:

a. Situer: `LocalAccountTokenFilterPolicy`

b. S'il n'existe pas, créez-en un nouveau `DWORD` (32 bits) Valeur nommée `LocalAccountTokenFilterPolicy` .

4. Les valeurs suivantes sont prises en charge. Pour ce scénario, définissez la valeur sur `1` :
   - `0`(Par défaut) : les restrictions à distance UAC sont activées. Les comptes locaux ont des jetons filtrés lors de l'accès à distance.
   - `1`:Les restrictions à distance UAC sont désactivées. Les comptes locaux contournent le filtrage des jetons et disposent de privilèges administratifs complets lors de l'accès à distance.
5. Cliquez sur **OK**.
6. Fermez l'éditeur du registre.
7. Redémarrez l'hôte Windows SnapCenter .

Exemple de modification du registre

Cet exemple définit LocalAccountTokenFilterPolicy sur « 1 », désactivant ainsi les restrictions à distance UAC.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Méthode 2 : désactiver le contrôle de compte d'utilisateur à l'aide d'un script PowerShell

Il s'agit d'une autre méthode que vous pouvez utiliser pour désactiver le contrôle de compte d'utilisateur.

> L'exécution de commandes PowerShell avec des privilèges élevés peut affecter les paramètres système. Assurez-vous de comprendre les commandes et leurs implications avant de les exécuter.

Étapes

1. Ouvrez une fenêtre PowerShell avec des privilèges administratifs sur l'hôte Windows SnapCenter :
   a. Cliquez sur le menu **Démarrer**.
   b. Recherchez **PowerShell 7** ou **Windows Powershell**.
   c. Faites un clic droit sur cette option et sélectionnez **Exécuter en tant qu'administrateur**.
2. Assurez-vous que PowerShell est installé sur votre système. Après l'installation, il devrait apparaître dans le menu **Démarrer**.

   > PowerShell est inclus par défaut dans Windows 7 et les versions ultérieures.

3. Pour désactiver les restrictions à distance UAC, définissez LocalAccountTokenFilterPolicy sur « 1 » en exécutant la commande suivante :

```
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
```

4. Vérifiez que la valeur actuelle est définie sur « 1 » dans `LocalAccountTokenFilterPolicy` en exécutant :

```
Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"
```

   - Si la valeur est 1, les restrictions à distance UAC sont désactivées.
   - Si la valeur est 0, les restrictions à distance UAC sont activées.

5. Pour appliquer les modifications, redémarrez votre ordinateur.

Exemples de commandes PowerShell 7 pour désactiver les restrictions à distance UAC :

Cet exemple avec la valeur définie sur « 1 » indique que les restrictions à distance UAC sont désactivées.

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Découvrez les charges de travail Microsoft SQL Server et importez-les éventuellement depuis SnapCenter dans NetApp Backup and Recovery

NetApp Backup and Recovery doit d'abord découvrir les charges de travail Microsoft SQL Server pour que vous puissiez utiliser le service. Vous pouvez éventuellement importer des données de sauvegarde et des politiques à partir de SnapCenter si SnapCenter est déjà installé.

Rôle de NetApp Console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp

Console pour tous les services" .

Découvrez les charges de travail Microsoft SQL Server et importez éventuellement des ressources SnapCenter

Lors de la découverte, NetApp Backup and Recovery analyse les instances et les bases de données Microsoft SQL Server dans les systèmes de votre organisation.

NetApp Backup and Recovery évalue les applications Microsoft SQL Server. Ce service évalue le niveau de protection existant, y compris les politiques de protection des sauvegardes, les instantanés et les options de sauvegarde et de restauration en vigueur.

La découverte se déroule de la manière suivante :

- Si vous disposez déjà de SnapCenter, importez les ressources SnapCenter dans NetApp Backup and Recovery à l'aide de l'interface utilisateur de NetApp Backup and Recovery .

> Si vous disposez déjà de SnapCenter, vérifiez d'abord que vous avez rempli les conditions préalables avant d'importer depuis SnapCenter. Par exemple, vous devez d'abord ajouter des systèmes de stockage en cluster SnapCenter sur site à la NetApp Console avant de procéder à l'importation depuis SnapCenter. Voir"Conditions préalables à l'importation de ressources depuis SnapCenter" .

- Si vous ne disposez pas déjà de SnapCenter, vous pouvez toujours découvrir des charges de travail en ajoutant un vCenter manuellement et en effectuant la découverte.

Si SnapCenter est déjà installé, importez les ressources SnapCenter dans NetApp Backup and Recovery

Si vous avez déjà installé SnapCenter , importez les ressources SnapCenter dans NetApp Backup and Recovery en suivant ces étapes. La NetApp Console découvre les ressources, les hôtes, les informations d'identification et les planifications à partir de SnapCenter; vous n'avez pas besoin de recréer toutes ces informations.

Vous pouvez le faire des manières suivantes :

- Lors de la découverte, sélectionnez une option pour importer des ressources depuis SnapCenter.
- Après la découverte, à partir de la page Inventaire, sélectionnez une option pour importer les ressources SnapCenter .
- Après la découverte, dans le menu Paramètres, sélectionnez une option pour importer les ressources SnapCenter . Pour plus de détails, voir"Configurer la NetApp Backup and Recovery" .

Il s'agit d'un processus en deux parties :

- Importer l'application SnapCenter Server et les ressources de l'hôte
- Gérer les ressources hôtes SnapCenter sélectionnées

Importer l'application SnapCenter Server et les ressources de l'hôte

Cette première étape importe les ressources de l'hôte depuis SnapCenter et affiche ces ressources sur la page d'inventaire de NetApp Backup and Recovery . À ce stade, les ressources ne sont pas encore gérées par NetApp Backup and Recovery.

Une fois les ressources de l'hôte SnapCenter importées, NetApp Backup and Recovery ne prend pas automatiquement en charge la gestion de la protection. Pour ce faire, vous devez choisir explicitement de gérer les ressources importées dans NetApp Backup and Recovery. Cela garantit que vous êtes prêt à ce que ces ressources soient sauvegardées par NetApp Backup and Recovery.

Étapes

1. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez **Inventaire**.
3. Sélectionnez **Découvrir les ressources**.
4. À partir de la page des ressources de charge de travail NetApp Backup and Recovery Discover, sélectionnez **Importer depuis SnapCenter**.
5. Saisissez * les informations d'identification de l'application SnapCenter * :
   a. * Adresse FQDN ou IP de SnapCenter * : saisissez le FQDN ou l'adresse IP de l'application SnapCenter elle-même.
   b. **Port** : saisissez le numéro de port du serveur SnapCenter .
   c. **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur SnapCenter .
   d. **Agent de console** : sélectionnez l'agent de console pour SnapCenter.
6. Saisissez * les informations d'identification de l'hôte du serveur SnapCenter * :
   a. **Informations d'identification existantes** : si vous sélectionnez cette option, vous pouvez utiliser les informations d'identification existantes que vous avez déjà ajoutées. Choisissez le nom des informations d'identification.
   b. **Ajouter de nouvelles informations d'identification** : si vous ne disposez pas d'informations d'identification d'hôte SnapCenter existantes, vous pouvez en ajouter de nouvelles. Saisissez le nom des informations d'identification, le mode d'authentification, le nom d'utilisateur et le mot de passe.
7. Sélectionnez **Importer** pour valider vos entrées et enregistrer le serveur SnapCenter .

Si le serveur SnapCenter est déjà enregistré, vous pouvez mettre à jour les détails d'enregistrement existants.

Résultat

La page Inventaire affiche les ressources SnapCenter importées qui incluent les hôtes, les instances et les bases de données MS SQL.

Pour voir les détails des ressources SnapCenter importées, sélectionnez l'option **Afficher les détails** dans le menu Actions.

Gérer les ressources de l'hôte SnapCenter

Après avoir importé les ressources SnapCenter , gérez ces ressources hôtes dans NetApp Backup and Recovery. Une fois que vous avez choisi de gérer ces ressources, NetApp Backup and Recovery est en mesure de sauvegarder et de récupérer les ressources que vous avez importées depuis SnapCenter. Vous ne gérez plus ces ressources dans SnapCenter Server.

Étapes

1. Après avoir importé les ressources SnapCenter , dans le menu Sauvegarde et récupération, sélectionnez **Inventaire**.
2. À partir de la page Inventaire, sélectionnez l'hôte SnapCenter importé que vous souhaitez confier à NetApp Backup and Recovery pour la gestion à partir de maintenant.
3. Sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.
4. Depuis la page Inventaire > Charge de travail, sélectionnez l'icône Actions ••• > **Gérer** pour afficher la page Gérer l'hôte.
5. Sélectionnez **Gérer**.
6. Dans la page Gérer l'hôte, choisissez d'utiliser un vCenter existant ou d'ajouter un nouveau vCenter.
7. Sélectionnez **Gérer**.

   La page Inventaire affiche les ressources SnapCenter nouvellement gérées.

Vous pouvez éventuellement créer un rapport des ressources gérées en sélectionnant l'option **Générer des rapports** dans le menu Actions.

Importer les ressources SnapCenter après la découverte à partir de la page Inventaire

Si vous avez déjà découvert des ressources, vous pouvez importer des ressources SnapCenter à partir de la page Inventaire.

Étapes

1. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez **Inventaire**.
3. Depuis la page Inventaire, sélectionnez *Importer les ressources SnapCenter *.
4. Suivez les étapes de la section *Importer les ressources SnapCenter * ci-dessus pour importer les ressources SnapCenter .

Si vous n'avez pas installé SnapCenter , ajoutez un vCenter et découvrez les ressources

Si SnapCenter n'est pas déjà installé, vous pouvez ajouter des informations vCenter et demander à NetApp de détecter les charges de travail de sauvegarde et de récupération. Dans chaque agent de console, sélectionnez les systèmes sur lesquels vous souhaitez découvrir les charges de travail.

Ceci est facultatif si vous disposez d'un environnement VMware.

Étapes

1. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.

   Si vous vous connectez à Backup and Recovery pour la première fois et que vous avez un système dans la console mais aucune ressource découverte, la page *Bienvenue sur le nouveau NetApp Backup and Recovery* apparaît avec une option pour **Découvrir les ressources**.

2. Sélectionnez **Découvrir les ressources**.
3. Saisissez les informations suivantes :
   a. **Type de charge de travail** : Pour cette version, seul Microsoft SQL Server est disponible.
   b. **Paramètres vCenter** : sélectionnez un vCenter existant ou ajoutez-en un nouveau. Pour ajouter un nouveau vCenter, saisissez le nom de domaine complet ou l'adresse IP du vCenter, le nom

d'utilisateur, le mot de passe, le port et le protocole.

> Si vous saisissez des informations vCenter, saisissez les informations relatives aux paramètres vCenter et à l'enregistrement de l'hôte. Si vous avez ajouté ou saisi des informations sur vCenter ici, vous devez également ajouter des informations sur le plug-in dans les paramètres avancés.

c. **Enregistrement de l'hôte** : sélectionnez **Ajouter des informations d'identification** et saisissez des informations sur les hôtes contenant les charges de travail que vous souhaitez découvrir.

> Si vous ajoutez un serveur autonome et non un serveur vCenter, entrez uniquement les informations sur l'hôte.

4. Sélectionnez **Découvrir**.

> Ce processus peut prendre quelques minutes.

5. Continuer avec les paramètres avancés.

Définissez les options des paramètres avancés lors de la découverte et installez le plugin

Avec les paramètres avancés, vous pouvez installer manuellement l'agent du plug-in sur tous les serveurs enregistrés. Cela vous permet d'importer toutes les charges de travail SnapCenter dans NetApp Backup and Recovery afin de pouvoir y gérer les sauvegardes et les restaurations. NetApp Backup and Recovery montre les étapes nécessaires à l'installation du plug-in.

Étapes

1. Depuis la page Découvrir les ressources, passez aux Paramètres avancés en cliquant sur la flèche vers le bas à droite.
2. Dans la page Découvrir les ressources de charge de travail, saisissez les informations suivantes.
   - **Entrez le numéro de port du plug-in** : saisissez le numéro de port utilisé par le plug-in.
   - **Chemin d'installation** : Saisissez le chemin où le plugin sera installé.
3. Si vous souhaitez installer l'agent SnapCenter manuellement, cochez les cases des options suivantes :
   - **Utiliser l'installation manuelle** : Cochez cette case pour installer le plugin manuellement.
   - **Ajouter tous les hôtes du cluster** : cochez cette case pour ajouter tous les hôtes du cluster à NetApp Backup and Recovery pendant la découverte.
   - **Ignorer les vérifications de préinstallation facultatives** : cochez cette case pour ignorer les vérifications de préinstallation facultatives. Vous souhaiterez peut-être le faire par exemple si vous savez que les considérations de mémoire ou d'espace seront modifiées dans un avenir proche et que vous souhaitez installer le plugin maintenant.
4. Sélectionnez **Découvrir**.

Accéder au tableau de bord de NetApp Backup and Recovery

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.

4. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

   "Découvrez ce que le tableau de bord vous montre".

Sauvegardez les charges de travail Microsoft SQL Server avec NetApp Backup and Recovery

Sauvegardez les données d'application Microsoft SQL Server à partir de systèmes ONTAP locaux vers Amazon Web Services, Microsoft Azure ou StorageGRID. Le système crée automatiquement des sauvegardes et les stocke dans un magasin d'objets de votre compte cloud pour la protection des données.

- Pour sauvegarder des charges de travail selon une planification, créez des stratégies qui gèrent les opérations de sauvegarde et de restauration. Voir"Créer des politiques" pour les instructions.
- Configurez le répertoire de journaux pour les hôtes découverts avant de démarrer une sauvegarde.
- Sauvegardez vos charges de travail maintenant (créez une sauvegarde à la demande maintenant).

Afficher l'état de protection de la charge de travail

Avant de démarrer une sauvegarde, affichez l'état de protection de vos charges de travail.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération, administrateur de clone de sauvegarde et de récupération ou rôle de visualiseur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Consultez les détails des onglets Hôtes, Groupes de protection, Groupes de disponibilité, Instances et Bases de données.

Configurer le répertoire de journaux pour les hôtes découverts

Définissez le chemin du journal d'activité pour les hôtes découverts afin de suivre l'état de l'opération avant de sauvegarder les charges de travail.

Rôle de NetApp Console requis Rôle de visualiseur de stockage, de super administrateur de sauvegarde et de récupération, d'administrateur de sauvegarde et de récupération ou d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.

3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez un hôte.
5. Sélectionnez l'icône Actions ••• > **Configurer le répertoire des journaux**.
6. Saisissez le chemin de l'hôte ou parcourez une liste d'hôtes ou de nœuds pour trouver où vous souhaitez stocker le journal de l'hôte.
7. Sélectionnez ceux sur lesquels vous souhaitez stocker les journaux.

   Les champs qui s'affichent diffèrent selon le modèle de déploiement sélectionné, par exemple, instance de cluster de basculement ou autonome.

8. Sélectionnez **Enregistrer**.

Créer un groupe de protection

Créez un groupe de protection pour gérer les opérations de sauvegarde et de restauration de plusieurs charges de travail. Un groupe de protection est un regroupement logique de charges de travail.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les instances ou les bases de données que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.

   Si vous souhaitez créer une politique, sélectionnez **Créer une nouvelle politique** et suivez les instructions pour créer une politique. Voir"Créer des politiques" pour plus d'informations.

10. Sélectionnez **Suivant**.
11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

Sauvegardez vos charges de travail maintenant avec une sauvegarde à la demande

Exécutez une sauvegarde à la demande avant d'apporter des modifications à votre système pour garantir la protection de vos données.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les

rôles d’accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu, sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l’icône Actions ••• > **Voir les détails**.
4. Sélectionnez l’onglet **Groupe de protection**, **Instances** ou **Bases de données**.
5. Sélectionnez l’instance ou la base de données que vous souhaitez sauvegarder.
6. Sélectionnez l’icône Actions ••• > **Reculez maintenant**.
7. Sélectionnez la politique que vous souhaitez appliquer à la sauvegarde.
8. Sélectionnez le niveau de planification.
9. Sélectionnez **Sauvegarder maintenant**.

Suspendre la planification de sauvegarde

Suspendez la planification pour arrêter temporairement les sauvegardes pendant la maintenance ou le dépannage.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d’administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d’accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l’icône Actions ••• > **Voir les détails**.
4. Sélectionnez l’onglet **Groupe de protection**, **Instances** ou **Bases de données**.
5. Sélectionnez le groupe de protection, l’instance ou la base de données que vous souhaitez suspendre.
6. Sélectionnez l’icône Actions ••• > **Suspendre**.

Supprimer un groupe de protection

La suppression d’un groupe de protection le supprime ainsi que toutes les planifications de sauvegarde associées. Vous souhaiterez peut-être supprimer un groupe de protection s’il n’est plus nécessaire.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d’administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d’accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l’icône Actions ••• > **Voir les détails**.
4. Sélectionnez l’onglet **Groupes de protection**.
5. Sélectionnez l’icône Actions ••• > **Supprimer le groupe de protection**.

Supprimer la protection d'une charge de travail

Vous pouvez supprimer la protection d'une charge de travail si vous ne souhaitez plus la sauvegarder ou si vous souhaitez arrêter de la gérer dans NetApp Backup and Recovery.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupe de protection**, **Instances** ou **Bases de données**.
5. Sélectionnez le groupe de protection, l'instance ou la base de données.
6. Sélectionnez l'icône Actions ••• > **Supprimer la protection**.
7. Dans la boîte de dialogue Supprimer la protection, sélectionnez si vous souhaitez conserver les sauvegardes et les métadonnées ou les supprimer.
8. Sélectionnez **Supprimer** pour confirmer l'action.

Restaurez les charges de travail Microsoft SQL Server avec NetApp Backup and Recovery

Restaurez les charges de travail Microsoft SQL Server à l'aide de NetApp Backup and Recovery. Utilisez des instantanés, des sauvegardes répliquées sur un stockage secondaire ou des sauvegardes dans un stockage objet. Restaurez les charges de travail sur le système d'origine, un système différent avec le même compte cloud ou un système ONTAP sur site.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des charges de travail à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal
- Restaurer à partir d'une ressource répliquée
- Restaurer à partir d'une sauvegarde de magasin d'objets

Restaurer ces points

Vous pouvez restaurer les données vers le dernier instantané ou vers ces points :

- Restaurer à partir d'instantanés
- Restaurez à un moment précis si vous connaissez le nom du fichier, l'emplacement et la dernière date valide
- Restaurer la dernière sauvegarde

Considérations relatives à la restauration à partir du stockage d'objets

Si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que Ransomware Resilience est actif pour cette sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la stratégie de

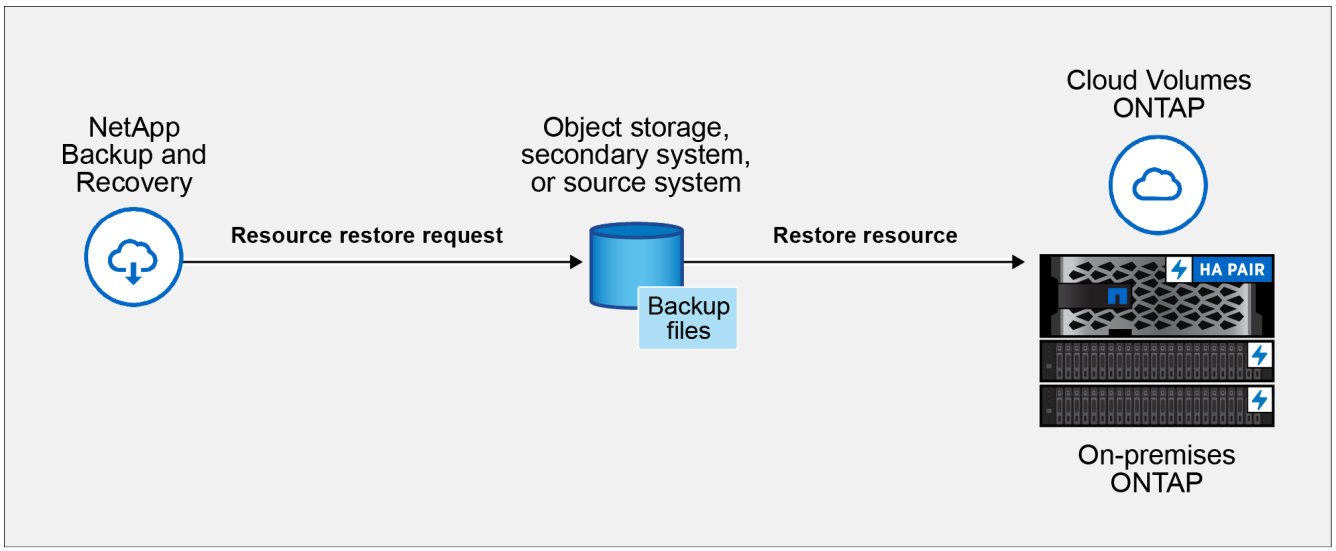
sauvegarde), vous êtes invité à exécuter une vérification d'intégrité supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'effectuer l'analyse.

Vous payez des frais supplémentaires à votre fournisseur de cloud pour accéder au fichier de sauvegarde.

Comment fonctionne la restauration des charges de travail

Lorsque vous restaurez des charges de travail, les événements suivants se produisent :

- Lorsque vous restaurez une charge de travail à partir d'un fichier de sauvegarde, NetApp Backup and Recovery crée une *nouvelle* ressource à l'aide des données de la sauvegarde.
- Lorsque vous effectuez une restauration à partir d'une charge de travail répliquée, vous pouvez restaurer la charge de travail sur le système d'origine ou sur un système ONTAP local.



- Lorsque vous restaurez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données sur le système d'origine ou sur un système ONTAP local.

Méthodes de restauration

Restaurez les charges de travail à l'aide de l'une de ces méthodes :

- **Depuis la page Restaurer** : utilisez cette option pour restaurer une ressource lorsque vous ne connaissez pas son nom, son emplacement ou sa dernière date de validité. Recherchez l'instantané à l'aide de filtres.
- **Depuis la page Inventaire** : utilisez cette option pour restaurer une ressource spécifique lorsque vous connaissez son nom, son emplacement et sa dernière date de disponibilité. Parcourez la liste pour trouver la ressource.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Restaurer les données de charge de travail à partir de l'option Restaurer

Restaurez les charges de travail de la base de données à l'aide de l'option Restaurer.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Restaurer**.
2. Sélectionnez la base de données que vous souhaitez restaurer. Utilisez les filtres pour rechercher.
3. Sélectionnez l'option de restauration :
    - Restaurer à partir d'instantanés
    - Restaurez à un moment précis si vous connaissez le nom du fichier, l'emplacement et la dernière date valide
    - Restaurer la dernière sauvegarde

Restaurer les charges de travail à partir de snapshots

1. En continuant à partir de la page Options de restauration, sélectionnez **Restaurer à partir d'instantanés**.

   Une liste d'instantanés apparaît.

2. Sélectionnez l'instantané que vous souhaitez restaurer.
3. Sélectionnez **Suivant**.

   Vous verrez ensuite les options de destination.

4. Dans la page Détails de la destination, saisissez les informations suivantes :
    - **Paramètres de destination** : choisissez si vous souhaitez restaurer les données à leur emplacement d'origine ou à un autre emplacement. Pour un autre emplacement, sélectionnez le nom de l'hôte et l'instance, entrez le nom de la base de données et entrez le chemin de destination où vous souhaitez restaurer l'instantané.
    - **Options de pré-restauration**:
        - **Écraser la base de données avec le même nom lors de la restauration** : Lors de la restauration, le nom de la base de données d'origine est conservé.
        - **Conserver les paramètres de réplication de la base de données SQL** : conserve les paramètres de réplication de la base de données SQL après l'opération de restauration.
        - **Créer une sauvegarde du journal des transactions avant la restauration** : Crée une sauvegarde du journal des transactions avant l'opération de restauration.*** Quitter la restauration si la sauvegarde du journal des transactions avant la restauration échoue** : arrête l'opération de restauration si la sauvegarde du journal des transactions échoue.
        - **Prescript** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration, tous les arguments utilisés par le script et le temps d'attente pour que le script se termine.
    - **Options post-restauration**:
        - **Opérationnel**, mais indisponible pour restaurer des journaux de transactions supplémentaires. Cela remet la base de données en ligne après l'application des sauvegardes du journal des transactions.
        - **Non opérationnel**, mais disponible pour restaurer des journaux de transactions supplémentaires. Maintient la base de données dans un état non opérationnel après l'opération de restauration lors de la restauration des sauvegardes du journal des transactions. Cette option est utile pour restaurer des journaux de transactions supplémentaires.
        - **Mode lecture seule** et disponible pour restaurer des journaux de transactions supplémentaires. Restaure la base de données en mode lecture seule et applique les sauvegardes du journal des transactions.

        - **Postscript** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.
5. Sélectionnez **Restaurer**.

Restaurer à un moment précis

NetApp Backup and Recovery utilise les journaux et les instantanés les plus récents pour créer une restauration ponctuelle de vos données.

1. En continuant à partir de la page Options de restauration, sélectionnez **Restaurer à un moment précis**.
2. Sélectionnez **Suivant**.
3. Dans la page Restaurer à un moment précis, saisissez les informations suivantes :
    - **Date et heure de restauration des données** : saisissez la date et l'heure exactes des données que vous souhaitez restaurer. Cette date et cette heure proviennent de l'hôte de la base de données Microsoft SQL Server.
4. Sélectionnez **Rechercher**.
5. Sélectionnez l'instantané que vous souhaitez restaurer.
6. Sélectionnez **Suivant**.
7. Dans la page Détails de la destination, saisissez les informations suivantes :
    - **Paramètres de destination** : Choisissez si vous souhaitez restaurer les données à leur emplacement d'origine ou à un autre emplacement. Pour un autre emplacement, sélectionnez le nom de l'hôte et l'instance, entrez le nom de la base de données et entrez le chemin de destination.
    - **Options de pré-restauration**:
        - **Conserver le nom de la base de données d'origine** : lors de la restauration, le nom de la base de données d'origine est conservé.
        - **Conserver les paramètres de réplication de la base de données SQL** : conserve les paramètres de réplication de la base de données SQL après l'opération de restauration.
        - **Prescript** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration, tous les arguments utilisés par le script et le temps d'attente pour que le script se termine.
    - **Options post-restauration**:
        - **Opérationnel**, mais indisponible pour restaurer des journaux de transactions supplémentaires. Cela remet la base de données en ligne après l'application des sauvegardes du journal des transactions.
        - **Non opérationnel**, mais disponible pour restaurer des journaux de transactions supplémentaires. Maintient la base de données dans un état non opérationnel après l'opération de restauration lors de la restauration des sauvegardes du journal des transactions. Cette option est utile pour restaurer des journaux de transactions supplémentaires.
        - **Mode lecture seule** et disponible pour restaurer des journaux de transactions supplémentaires. Restaure la base de données en mode lecture seule et applique les sauvegardes du journal des transactions.
        - **Postscript** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.
8. Sélectionnez **Restaurer**.

Restaurer la dernière sauvegarde

Cette option utilise les dernières sauvegardes complètes et journaux pour restaurer vos données au dernier état correct. Le système analyse les journaux depuis le dernier instantané jusqu'à présent. Le processus suit les modifications et les activités pour restaurer la version la plus récente et la plus précise de vos données.

1. En continuant à partir de la page Options de restauration, sélectionnez **Restaurer vers la dernière sauvegarde**.

   NetApp Backup and Recovery vous montre les snapshots disponibles pour l'opération de restauration.

2. Dans la page Restaurer vers l'état le plus récent, sélectionnez l'emplacement de l'instantané du stockage local, secondaire ou d'objets.
3. Sélectionnez **Suivant**.
4. Dans la page Détails de la destination, saisissez les informations suivantes :
   - **Paramètres de destination** : Choisissez si vous souhaitez restaurer les données à leur emplacement d'origine ou à un autre emplacement. Pour un autre emplacement, sélectionnez le nom de l'hôte et l'instance, entrez le nom de la base de données et entrez le chemin de destination.
   - **Options de pré-restauration**:
     - **Écraser la base de données avec le même nom lors de la restauration** : Lors de la restauration, le nom de la base de données d'origine est conservé.
     - **Conserver les paramètres de réplication de la base de données SQL** : conserve les paramètres de réplication de la base de données SQL après l'opération de restauration.
     - **Créer une sauvegarde du journal des transactions avant la restauration** : Crée une sauvegarde du journal des transactions avant l'opération de restauration.
     - **Quitter la restauration si la sauvegarde du journal des transactions avant la restauration échoue** : arrête l'opération de restauration si la sauvegarde du journal des transactions échoue.
     - **Prescript** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration, tous les arguments utilisés par le script et le temps d'attente pour que le script se termine.
   - **Options post-restauration**:
     - **Opérationnel**, mais indisponible pour restaurer des journaux de transactions supplémentaires. Cela remet la base de données en ligne après l'application des sauvegardes du journal des transactions.
     - **Non opérationnel**, mais disponible pour restaurer des journaux de transactions supplémentaires. Maintient la base de données dans un état non opérationnel après l'opération de restauration lors de la restauration des sauvegardes du journal des transactions. Cette option est utile pour restaurer des journaux de transactions supplémentaires.
     - **Mode lecture seule** et disponible pour restaurer des journaux de transactions supplémentaires. Restaure la base de données en mode lecture seule et applique les sauvegardes du journal des transactions.
     - **Postscript** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.
5. Sélectionnez **Restaurer**.

Restaurer les données de charge de travail à partir de l'option Inventaire

Restaurer les charges de travail de la base de données à partir de la page Inventaire. En utilisant l'option

Inventaire, vous pouvez restaurer uniquement les bases de données, pas les instances.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Choisissez l'hôte sur lequel se trouve la ressource que vous souhaitez restaurer.
3. Sélectionnez les **Actions*** **icône et sélectionnez *Afficher les détails**.
4. Sur la page Microsoft SQL Server, sélectionnez l'onglet **Bases de données**.
5. Dans le menu Bases de données, sélectionnez une base de données avec le statut « Protégé ».
6. Sélectionnez les **Actions*** **icône et sélectionnez *Restaurer**.

   Les trois mêmes options s'affichent lorsque vous restaurez à partir de la page Restaurer :

   - Restaurer à partir d'instantanés
   - Restaurer à un moment précis dans le temps
   - Restaurer la dernière sauvegarde
7. Continuez avec les mêmes étapes pour l'option de restauration à partir de la page Restaurer

Cloner les charges de travail Microsoft SQL Server à l'aide de NetApp Backup and Recovery

Clonez les données d'application Microsoft SQL Server sur une machine virtuelle à des fins de développement, de test ou de protection avec NetApp Backup and Recovery. Créez des clones à partir d'instantanés instantanés ou existants de vos charges de travail SQL Server.

Choisissez entre les types de clones suivants :

- * Instantané instantané et clone * : vous pouvez créer un clone de vos charges de travail Microsoft SQL Server à partir d'un instantané instantané, qui est une copie ponctuelle des données sources créées à partir d'une sauvegarde. Le clone est stocké dans un magasin d'objets dans votre compte cloud public ou privé. Vous pouvez utiliser le clone pour restaurer vos charges de travail en cas de perte ou de corruption de données.
- **Cloner à partir d'un snapshot existant** : vous pouvez choisir un snapshot existant dans une liste de snapshots disponibles pour la charge de travail. Cette option est utile si vous souhaitez créer un clone à partir d'un moment précis. Cloner vers un stockage principal ou secondaire.

Vous pouvez atteindre les objectifs de protection suivants :

- Créer un clone
- Rafraîchir un clone
- Diviser un clone
- Supprimer un clone

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Créer un clone

Vous pouvez créer un clone de vos charges de travail Microsoft SQL Server. Un clone est une copie des données sources créée à partir d'une sauvegarde. Le clone est stocké dans un magasin d'objets dans votre compte cloud public ou privé. Vous pouvez utiliser le clone pour restaurer vos charges de travail en cas de perte ou de corruption de données.

Vous pouvez créer un clone à partir d'un instantané existant ou d'un instantané instantané. Un instantané est une copie ponctuelle des données sources créée à partir d'une sauvegarde. Vous pouvez utiliser le clone pour restaurer vos charges de travail en cas de perte ou de corruption de données.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Cloner**.
2. Sélectionnez **Créer un nouveau clone**.
3. Sélectionnez le type de clone :
   - **Clonage et actualisation de la base de données à partir d'un instantané existant** : Choisissez un instantané et configurez les options de clonage.
   - **Instantané et clonage instantanés** : Prenez maintenant un instantané des données sources et créez un clone à partir de cet instantané. Cette option est utile si vous souhaitez créer un clone à partir des données les plus récentes de la charge de travail source.
4. Complétez la section **Source de la base de données** :
   - **Clone unique ou clone en masse** : sélectionnez si vous souhaitez créer un clone unique ou plusieurs clones. Si vous sélectionnez **Clonage en masse**, vous pouvez créer plusieurs clones à la fois en utilisant un groupe de protection que vous avez déjà créé. Cette option est utile si vous souhaitez créer plusieurs clones pour différentes charges de travail.
   - **Hôte, instance et nom de la base de données source** : sélectionnez l'hôte, l'instance et le nom de la base de données source pour le clone. La base de données source est la base de données à partir de laquelle le clone sera créé.
5. Complétez la section **Cible de la base de données** :
   - **Hôte, instance et nom de la base de données cible** : sélectionnez l'hôte, l'instance et le nom de la base de données cible pour le clone. La base de données cible est l'emplacement où le clone sera créé.

     Vous pouvez également sélectionner **Suffixe** dans la liste déroulante du nom cible et ajouter un suffixe au nom de la base de données clonée. Si vous n'ajoutez pas de suffixe, le nom de la base de données clonée est le même que le nom de la base de données source.

   - **QoS (débit maximal)** : sélectionnez le débit maximal de qualité de service (QoS) en Mbit/s pour le clone. La QoS définit les caractéristiques de performances du clone, telles que le débit maximal et les IOPS.
6. Complétez la section **Monture** :
   - **Point de montage à attribution automatique** : attribuez automatiquement un point de montage pour le clone dans le magasin d'objets.
   - **Définir le chemin du point de montage** : saisissez un point de montage pour le clone. Le point de montage est l'emplacement où le clone sera monté dans le magasin d'objets. Sélectionnez la lettre du lecteur, entrez le chemin du fichier de données et entrez le chemin du fichier journal.
7. Sélectionnez **Suivant**.
8. Sélectionnez le point de restauration :

- **Instantanés existants** : sélectionnez un instantané existant dans la liste des instantanés disponibles pour la charge de travail. Cette option est utile si vous souhaitez créer un clone à partir d'un moment précis.
- * Instantané instantané et clonage * : sélectionnez le dernier instantané dans la liste des instantanés disponibles pour la charge de travail. Cette option est utile si vous souhaitez créer un clone à partir des données les plus récentes de la charge de travail source.

9. Si vous choisissez de créer un **instantané instantané et de cloner**, choisissez l'emplacement de stockage du clone :
   - **Stockage local** : sélectionnez cette option pour créer le clone dans le stockage local du système ONTAP . Le stockage local est le stockage directement connecté au système ONTAP .
   - **Stockage secondaire** : sélectionnez cette option pour créer le clone dans le stockage secondaire du système ONTAP . Le stockage secondaire est le stockage utilisé pour les charges de travail de sauvegarde et de récupération.
10. Sélectionnez l'emplacement de destination des données et des journaux.
11. Sélectionnez **Suivant**.
12. Complétez la section **Options avancées**.
13. Si vous avez choisi **Instantané et clonage instantanés**, complétez les options suivantes :
    - **Programme d'actualisation et expiration du clonage** : Si vous avez choisi **Clonage instantané**, saisissez la date à laquelle commencer l'actualisation du clone. Le calendrier de clonage définit quand le clone sera créé.
      - **Supprimer le clone si la planification expire** : si vous souhaitez supprimer le clone à la date d'expiration du clone.
      - **Actualiser le clone toutes les** : sélectionnez la fréquence à laquelle le clone doit être actualisé. Vous pouvez choisir d'actualiser le clone toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les trimestres. Cette option est utile si vous souhaitez maintenir le clone à jour avec la charge de travail source.
    - **Prescripts et postscripts** : Ajoutez éventuellement des scripts à exécuter avant et après la création du clone. Ces scripts peuvent effectuer des tâches supplémentaires, telles que la configuration du clone ou l'envoi de notifications.
    - **Notification** : Vous pouvez également spécifier des adresses e-mail pour recevoir des notifications sur l'état de création du clone ainsi que le rapport de tâche. Vous pouvez également spécifier une URL de webhook pour recevoir des notifications sur l'état de création du clone. Vous pouvez spécifier si vous souhaitez des notifications de réussite et d'échec ou seulement l'une ou l'autre.
    - **Tags** : Sélectionnez des étiquettes pour vous aider à rechercher des groupes de ressources ultérieurement et sélectionnez **Appliquer**. Par exemple, si vous ajoutez « RH » comme balise à plusieurs groupes de ressources, vous pourrez ultérieurement trouver tous les groupes de ressources associés à la balise « RH ».
14. Sélectionnez **Créer**.
15. Une fois le clone créé, vous pouvez le visualiser dans la page **Inventaire**.

Rafraîchir un clone

Vous pouvez actualiser un clone de vos charges de travail Microsoft SQL Server. L'actualisation d'un clone met à jour le clone avec les dernières données de la charge de travail source. Ceci est utile si vous souhaitez maintenir le clone à jour avec la charge de travail source.

Vous avez la possibilité de modifier le nom de la base de données, d'utiliser le dernier instantané ou

d’actualiser à partir d’un instantané de production existant.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Cloner**.
2. Sélectionnez le clone que vous souhaitez actualiser.
3. Sélectionnez l’icône Actions ••• > **Actualiser le clone**.
4. Complétez la section **Paramètres avancés** :
   - **Étendue de la récupération** : choisissez de récupérer toutes les sauvegardes de journaux ou les sauvegardes de journaux jusqu’à un moment précis. Cette option est utile si vous souhaitez récupérer le clone à un moment précis.
   - **Programme d’actualisation et expiration du clonage** : Si vous avez choisi **Clonage instantané**, saisissez la date à laquelle commencer l’actualisation du clone. Le calendrier de clonage définit quand le clone sera créé.
     - **Supprimer le clone si la planification expire** : si vous souhaitez supprimer le clone à la date d’expiration du clone.
     - **Actualiser le clone toutes les** : sélectionnez la fréquence à laquelle le clone doit être actualisé. Vous pouvez choisir d’actualiser le clone toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les trimestres. Cette option est utile si vous souhaitez maintenir le clone à jour avec la charge de travail source.
   - **Paramètres iGroup** : sélectionnez l’iGroup pour le clone. L’iGroup est un regroupement logique d’initiateurs utilisés pour accéder au clone. Vous pouvez sélectionner un iGroup existant ou en créer un nouveau. Sélectionnez l’iGroup à partir du système de stockage ONTAP principal ou secondaire.
   - **Prescripts et postscripts** : Ajoutez éventuellement des scripts à exécuter avant et après la création du clone. Ces scripts peuvent effectuer des tâches supplémentaires, telles que la configuration du clone ou l’envoi de notifications.
   - **Notification** : Vous pouvez également spécifier des adresses e-mail pour recevoir des notifications sur l’état de création du clone ainsi que le rapport de tâche. Vous pouvez également spécifier une URL de webhook pour recevoir des notifications sur l’état de création du clone. Vous pouvez spécifier si vous souhaitez des notifications de réussite et d’échec ou seulement l’une ou l’autre.
   - **Tags**: Saisissez une ou plusieurs étiquettes qui vous aideront à rechercher ultérieurement le groupe de ressources. Par exemple, si vous ajoutez « RH » comme balise à plusieurs groupes de ressources, vous pouvez ultérieurement trouver tous les groupes de ressources associés à la balise RH.
5. Dans la boîte de dialogue de confirmation d’actualisation, pour continuer, sélectionnez **Actualiser**.

Ignorer une actualisation du clone

Ignorez une actualisation du clone pour conserver le clone inchangé.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Cloner**.
2. Sélectionnez le clone pour lequel vous souhaitez ignorer l’actualisation.
3. Sélectionnez l’icône Actions ••• > **Ignorer l’actualisation**.
4. Dans la boîte de dialogue de confirmation d’actualisation, procédez comme suit :
   a. Pour ignorer uniquement le prochain programme d’actualisation, sélectionnez **Ignorer uniquement le prochain programme d’actualisation**.
   b. Pour continuer, sélectionnez **Ignorer**.

Diviser un clone

Vous pouvez diviser un clone de vos charges de travail Microsoft SQL Server. La division d'un clone crée une nouvelle sauvegarde à partir du clone. La nouvelle sauvegarde peut être utilisée pour restaurer les charges de travail.

Vous pouvez choisir de diviser un clone en clones indépendants ou à long terme. Un assistant affiche la liste des agrégats qui font partie du SVM, leurs tailles et l'emplacement où réside le volume cloné. NetApp Backup and Recovery indique également s'il y a suffisamment d'espace pour diviser le clone. Une fois le clone divisé, le clone devient une base de données indépendante pour la protection.

Le travail de clonage ne doit pas être supprimé et peut être réutilisé pour d'autres clones.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Cloner**.
2. Sélectionnez un clone.
3. Sélectionnez l'icône Actions ••• > **Clone divisé**.
4. Vérifiez les détails du clone divisé et sélectionnez **Diviser**.
5. Une fois le clone divisé créé, vous pouvez le visualiser dans la page **Inventaire**.

Supprimer un clone

Vous pouvez supprimer un clone de vos charges de travail Microsoft SQL Server. La suppression d'un clone supprime le clone du magasin d'objets et libère de l'espace de stockage.

Si une politique protège le clone, le clone et son travail sont supprimés.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Cloner**.
2. Sélectionnez un clone.
3. Sélectionnez l'icône Actions ••• > **Supprimer le clone**.
4. Dans la boîte de dialogue de confirmation de suppression du clone, vérifiez les détails de la suppression.
    a. Pour supprimer les ressources clonées de SnapCenter même si les clones ou leur stockage ne sont pas accessibles, sélectionnez **Forcer la suppression**.
    b. Sélectionnez **Supprimer**.
5. Lorsque le clone est supprimé, il est supprimé de la page **Inventaire**.

Gérez l'inventaire Microsoft SQL Server avec NetApp Backup and Recovery

NetApp Backup and Recovery vous aide à gérer vos hôtes, bases de données et instances Microsoft SQL Server. Vous pouvez afficher, modifier ou supprimer les paramètres de protection de votre inventaire.

Vous pouvez accomplir les tâches suivantes liées à la gestion de votre inventaire :

- Gérer les informations de l'hôte
    - Suspendre les horaires
    - Modifier ou supprimer des hôtes

- Gérer les informations des instances
  - Associer les informations d'identification à une ressource
  - Sauvegardez maintenant en démarrant une sauvegarde à la demande
  - Modifier les paramètres de protection
- Gérer les informations de la base de données
  - Protéger les bases de données
  - Restaurer les bases de données
  - Modifier les paramètres de protection
  - Sauvegardez maintenant en démarrant une sauvegarde à la demande
- Configurez le répertoire des journaux (depuis **Inventaire** > **Hôtes**). Si vous souhaitez sauvegarder les journaux de vos hôtes de base de données dans l'instantané, configurez d'abord les journaux dans NetApp Backup and Recovery. Pour plus de détails, reportez-vous à"Configurer les paramètres de NetApp Backup and Recovery" .

Gérer les informations de l'hôte

Vous pouvez gérer les informations de l'hôte pour garantir que les bons hôtes sont protégés. Vous pouvez afficher, modifier et supprimer les informations de l'hôte.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération ou rôle d'administrateur de clone de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

- Configurer le répertoire des journaux. Pour plus de détails, reportez-vous à"Configurer les paramètres de NetApp Backup and Recovery" .
- Suspendre les horaires
- Modifier un hôte
- Supprimer un hôte

Gérer les hôtes

Vous pouvez gérer les hôtes découverts dans votre système. Vous pouvez les gérer séparément ou en groupe.

Vous pouvez gérer les hôtes avec un statut « Non géré » dans la colonne Hôtes. NetApp Backup and Recovery gère déjà les hôtes avec un statut « Géré ».

Une fois que vous avez géré les hôtes dans NetApp Backup and Recovery, SnapCenter ne gère plus les ressources sur ces hôtes.

Rôle de NetApp Console requis Visualiseur de stockage ou super administrateur de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu, sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.

3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Hôtes**.
5. Sélectionnez un ou plusieurs hôtes. Si vous sélectionnez plusieurs hôtes, une option Actions groupées apparaît dans laquelle vous pouvez sélectionner **Gérer (jusqu'à 5 hôtes)**.
6. Sélectionnez l'icône Actions ••• > **Gérer**.
7. Examiner les dépendances de l'hôte :
   - Si le vCenter ne s'affiche pas, sélectionnez l'icône en forme de crayon pour ajouter ou modifier les détails du vCenter.
   - Si vous ajoutez un vCenter, vous devez également enregistrer le vCenter en sélectionnant **Enregistrer vCenter**.
8. Sélectionnez **Valider les paramètres** pour tester vos paramètres.
9. Sélectionnez **Gérer** pour gérer l'hôte.

Suspendre les horaires

Suspendez les planifications pour arrêter les opérations de sauvegarde et de restauration pendant la maintenance de l'hôte.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'hôte sur lequel vous souhaitez suspendre les planifications.
3. Sélectionnez les **Actions*** ••• **icône et sélectionnez *Suspendre les programmes**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Suspendre**.

Modifier un hôte

Vous pouvez modifier les informations du serveur vCenter, les informations d'identification d'enregistrement de l'hôte et les options de paramètres avancés.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'hôte que vous souhaitez modifier.
3. Sélectionnez les **Actions*** ••• **icône et sélectionnez *Modifier l'hôte**.
4. Modifier les informations de l'hôte.
5. Sélectionnez **Terminé**.

Supprimer un hôte

Vous pouvez supprimer les informations de l'hôte pour arrêter les frais de service.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'hôte que vous souhaitez supprimer.
3. Sélectionnez les **Actions*** ••• **icône et sélectionnez *Supprimer l'hôte**.
4. Vérifiez les informations de confirmation et sélectionnez **Supprimer**.

Gérer les informations des instances

Vous pouvez gérer les informations des instances pour attribuer les informations d'identification appropriées pour la protection des ressources et sauvegarder les ressources des manières suivantes :

- Protéger les instances
- Titres d'associé
- Dissocier les informations d'identification
- Protection contre les modifications
- Sauvegardez maintenant

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Protéger les instances de base de données

Vous pouvez attribuer une politique à une instance de base de données à l'aide de politiques qui régissent les planifications et la conservation de la protection des ressources.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions*** icône et sélectionnez *Protéger**.
6. Sélectionnez une politique ou créez-en une nouvelle.

   Pour plus de détails sur la création d'une politique, reportez-vous à"Créer une politique" .

7. Fournissez des informations sur les scripts que vous souhaitez exécuter avant et après la sauvegarde.
   - **Pré-script** : saisissez le nom de fichier et l'emplacement de votre script pour l'exécuter automatiquement avant que l'action de protection ne soit déclenchée. Cela est utile pour effectuer des tâches ou des configurations supplémentaires qui doivent être exécutées avant le flux de travail de protection.
   - **Post-script** : Saisissez le nom de fichier et l'emplacement de votre script pour l'exécuter automatiquement une fois l'action de protection terminée. Cela est utile pour effectuer des tâches ou des configurations supplémentaires qui doivent être exécutées après le flux de travail de protection.
8. Fournissez des informations sur la manière dont vous souhaitez que l'instantané soit vérifié :
   - Emplacement de stockage : sélectionnez l'emplacement où l'instantané de vérification sera stocké.
   - Ressource de vérification : sélectionnez si la ressource que vous souhaitez vérifier se trouve sur le snapshot local et sur le stockage secondaire ONTAP .
   - Calendrier de vérification : sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle.

Associer les informations d'identification à une ressource

Vous pouvez associer des informations d'identification à une ressource afin que la protection puisse se

produire.

Pour plus de détails, voir"Configurer les paramètres de NetApp Backup and Recovery , y compris les informations d'identification" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions*** icône et sélectionnez *Associer les informations d'identification**.
6. Utilisez les informations d'identification existantes ou créez-en de nouvelles.

Modifier les paramètres de protection

Vous pouvez modifier la politique, créer une nouvelle politique, définir une planification et définir les paramètres de conservation.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions*** icône et sélectionnez *Modifier la protection**.

   Pour plus de détails sur la création d'une politique, reportez-vous à"Créer une politique" .

Sauvegardez maintenant

Sauvegardez vos données maintenant pour les protéger immédiatement.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions*** icône et sélectionnez *Sauvegarder maintenant**.
6. Choisissez le type de sauvegarde et définissez la planification.

   Pour plus de détails sur la création d'une sauvegarde ad hoc, reportez-vous à"Créer une politique" .

Gérer les informations de la base de données

Vous pouvez gérer les informations de la base de données des manières suivantes :

- Protéger les bases de données

- Restaurer les bases de données
- Afficher les détails de la protection
- Modifier les paramètres de protection
- Sauvegardez maintenant

Protéger les bases de données

Vous pouvez modifier la politique, créer une nouvelle politique, définir une planification et définir les paramètres de conservation.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données.
5. Sélectionnez les **Actions*** **icône et sélectionnez *Protéger**.

   Pour plus de détails sur la création d'une politique, reportez-vous à"Créer une politique" .

Restaurer les bases de données

Restaurez une base de données pour protéger vos données.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

1. Sélectionnez l'onglet **Bases de données**.
2. Sélectionnez la base de données.
3. Sélectionnez les **Actions*** **icône et sélectionnez *Restaurer**.

   Pour plus d'informations sur la restauration des charges de travail, reportez-vous à"Restaurer les charges de travail" .

Modifier les paramètres de protection

Vous pouvez modifier la politique, créer une nouvelle politique, définir une planification et définir les paramètres de conservation.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.

2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données.
5. Sélectionnez les **Actions*** icône et sélectionnez *Modifier la protection**.

   Pour plus de détails sur la création d'une politique, reportez-vous à"Créer une politique" .

Sauvegardez maintenant

Vous pouvez désormais sauvegarder vos instances et bases de données Microsoft SQL Server pour protéger vos données immédiatement.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances** ou **Bases de données**.
4. Sélectionnez l'instance ou la base de données.
5. Sélectionnez les **Actions*** icône et sélectionnez *Sauvegarder maintenant**.

Gérez les instantanés Microsoft SQL Server avec NetApp Backup and Recovery

Vous pouvez gérer les instantanés Microsoft SQL Server en les supprimant de NetApp Backup and Recovery.

Supprimer un instantané

Vous ne pouvez supprimer que les instantanés locaux.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données pour laquelle vous souhaitez supprimer un instantané.
5. Dans le menu Actions, sélectionnez **Afficher les détails de la protection**.
6. Sélectionnez l'instantané local que vous souhaitez supprimer.

Vérifiez que l'icône d'instantané local dans la colonne **Emplacement** de cette ligne apparaît en bleu.

7. Sélectionnez les **Actions*** icône et sélectionnez *Supprimer l'instantané local*.
8. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer**.

Créer des rapports pour les charges de travail Microsoft SQL Server dans NetApp Backup and Recovery

Dans NetApp Backup and Recovery, créez des rapports pour les charges de travail Microsoft SQL Server afin de consulter l'état et les détails des sauvegardes, notamment le nombre de sauvegardes réussies et échouées, les types de sauvegarde, les systèmes de stockage et les horodatages.

Créer un rapport

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération, administrateur de clone de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

1. Dans le menu NetApp Backup and Recovery , sélectionnez l'option **Rapports**.
2. Sélectionnez **Créer un rapport**.
3. Saisissez les détails de la portée du rapport :
   - **Nom du rapport** : saisissez un nom unique pour le rapport.
   - **Type de rapport** : Choisissez si vous souhaitez un rapport par compte ou par charge de travail (Microsoft SQL Server).
   - **Sélectionner l'hôte** : si vous avez sélectionné par charge de travail, sélectionnez l'hôte pour lequel vous souhaitez générer le rapport.
   - **Sélectionner le contenu** : Choisissez si vous souhaitez que le rapport inclue un résumé de toutes les sauvegardes ou les détails de chaque sauvegarde. (Si vous avez choisi « Par compte »)
4. Entrez la plage de rapport : choisissez si vous souhaitez que le rapport inclue les données du dernier jour, des 7 derniers jours, des 30 derniers jours, du dernier trimestre ou de l'année dernière.
5. Saisissez les détails de livraison du rapport : si vous souhaitez que le rapport soit envoyé par e-mail, cochez **Envoyer le rapport par e-mail**. Saisissez l'adresse e-mail à laquelle vous souhaitez que le rapport soit envoyé.

   Configurez les notifications par e-mail dans la page Paramètres. Pour plus de détails sur la configuration des notifications par e-mail, voir"Configurer les paramètres" .

Protéger les charges de travail VMware (sans le plug-in SnapCenter pour VMware)

Présentation de la protection des charges de travail VMware avec NetApp Backup and Recovery

Protégez vos machines virtuelles et banques de données VMware avec NetApp Backup and Recovery. NetApp Backup and Recovery fournit des opérations de sauvegarde et de

restauration rapides, peu encombrantes, cohérentes en cas de panne et cohérentes avec les machines virtuelles. Vous pouvez sauvegarder les charges de travail VMware sur Amazon Web Services S3 ou StorageGRID et restaurer les charges de travail VMware sur un hôte VMware local.

Cette version de NetApp Backup and Recovery prend uniquement en charge VMware vCenter et ne détecte pas les vVols ou les machines virtuelles sur les vVols.

Utilisez NetApp Backup and Recovery pour mettre en œuvre une stratégie 3-2-1, où vous disposez de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud. Les avantages de l'approche 3-2-1 incluent :

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.
- L'utilisation de différents types de supports vous aide à récupérer si l'un d'eux tombe en panne.
- Vous pouvez restaurer rapidement à partir de la copie sur site et utiliser les copies hors site si la copie sur site est compromise.

Pour basculer vers et depuis les versions de l'interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Vous pouvez utiliser NetApp Backup and Recovery pour effectuer les tâches suivantes liées aux charges de travail VMware :

- "Découvrez les charges de travail VMware"
- "Créer et gérer des groupes de protection pour les charges de travail VMware"
- "Sauvegarder les charges de travail VMware"
- "Restaurer les charges de travail VMware"

Découvrez les charges de travail VMware avec NetApp Backup and Recovery

Le service NetApp Backup and Recovery doit d'abord détecter les banques de données VMware et les machines virtuelles exécutées sur les systèmes ONTAP pour que vous puissiez utiliser le service. Vous pouvez éventuellement importer des données et des politiques de sauvegarde à partir du SnapCenter Plug-in for VMware vSphere si vous l'avez déjà installé.

Rôle de console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Découvrez les charges de travail VMware et importez éventuellement des ressources SnapCenter

Lors de la phase de découverte, NetApp Backup and Recovery analyse les charges de travail VMware au sein de votre organisation, évalue et importe les politiques de protection, les instantanés et les options de sauvegarde et de restauration existants.

Vous pouvez importer des banques de données et des machines virtuelles VMware NFS et VMFS à partir de leur SnapCenter Plug-in for VMware vSphere dans l'inventaire NetApp Backup and Recovery .

Cette version de NetApp Backup and Recovery prend uniquement en charge VMware vCenter et ne détecte pas les vVols ou les machines virtuelles sur les vVols.

Pendant le processus d'importation, NetApp Backup and Recovery effectue les tâches suivantes :

- Active l'accès SSH sécurisé au serveur vCenter.
- Active le mode de maintenance sur tous les groupes de ressources du serveur vCenter.
- Prépare les métadonnées du vCenter et les marque comme non gérées dans la NetApp Console.
- Configure l'accès à la base de données.
- Découvre VMware vCenter, les banques de données et les machines virtuelles.
- Importe les politiques de protection, les instantanés et les options de sauvegarde et de restauration existants à partir du SnapCenter Plug-in for VMware vSphere.
- Affiche les ressources découvertes dans la page Inventaire de NetApp Backup and Recovery .

La découverte se déroule de la manière suivante :

- Si vous disposez déjà du SnapCenter Plug-in for VMware vSphere, importez les ressources SnapCenter dans NetApp Backup and Recovery à l'aide de l'interface utilisateur de NetApp Backup and Recovery .

  Si vous disposez déjà du plug-in SnapCenter , assurez-vous d'avoir rempli les conditions préalables avant d'importer depuis SnapCenter. Par exemple, vous devez d'abord créer des systèmes dans la NetApp Console pour tous les stockages de cluster SnapCenter sur site avant de procéder à l'importation depuis SnapCenter. Voir"Conditions préalables à l'importation de ressources depuis SnapCenter" .

- Si vous ne disposez pas déjà du plug-in SnapCenter , vous pouvez toujours découvrir les charges de travail au sein de vos systèmes en ajoutant un vCenter manuellement et en effectuant la découverte.

Si le plug-in SnapCenter n'est pas déjà installé, ajoutez un vCenter et découvrez les ressources

Si vous n'avez pas encore installé SnapCenter Plug-in pour VMware, ajoutez les informations vCenter et demandez à NetApp Backup and Recovery de découvrir les charges de travail. Dans chaque agent de console, sélectionnez les systèmes sur lesquels vous souhaitez découvrir les charges de travail.

Étapes

1. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.

   Si vous vous connectez à Backup and Recovery pour la première fois et que vous avez un système dans la console mais aucune ressource découverte, la page *Bienvenue sur le nouveau NetApp Backup and Recovery* apparaît avec une option pour **Découvrir les ressources**.

2. Sélectionnez **Découvrir les ressources**.
3. Saisissez les informations suivantes :
   a. **Type de charge de travail** : sélectionnez **VMware**.
   b. **Paramètres vCenter** : Ajouter un nouveau vCenter. Pour ajouter un nouveau vCenter, saisissez le nom de domaine complet ou l'adresse IP du vCenter, le nom d'utilisateur, le mot de passe, le port et le protocole.

Si vous saisissez des informations vCenter, saisissez les informations relatives aux paramètres vCenter et à l'enregistrement de l'hôte. Si vous avez ajouté ou saisi des informations sur vCenter ici, vous devez également ajouter des informations sur le plug-in dans les paramètres avancés.

c. **Enregistrement de l'hôte** : Non requis pour VMware.

4. Sélectionnez **Découvrir**.

Ce processus peut prendre quelques minutes.

5. Continuer avec les paramètres avancés.

Si le plug-in SnapCenter est déjà installé, importez les ressources SnapCenter Plug-in pour VMware dans NetApp Backup and Recovery

Si vous avez déjà installé SnapCenter Plug-in pour VMware, importez les ressources SnapCenter Plug-in dans NetApp Backup and Recovery en suivant ces étapes. La console détecte les hôtes ESXi, les banques de données et les machines virtuelles dans les vCenters, et planifie à partir du plug-in ; vous n'avez pas besoin de recréer toutes ces informations.

Vous pouvez le faire des manières suivantes :

- Lors de la découverte, sélectionnez une option pour importer des ressources à partir du plug-in SnapCenter .
- Après la découverte, à partir de la page Inventaire, sélectionnez une option pour importer les ressources du plug-in SnapCenter .
- Après la découverte, dans le menu Paramètres, sélectionnez une option pour importer les ressources du plug-in SnapCenter . Pour plus de détails, voir"Configurer la NetApp Backup and Recovery" . Ceci n'est pas pris en charge pour VMware.

Il s'agit d'un processus en deux parties décrit dans cette section :

1. Importez les métadonnées vCenter depuis le plug-in SnapCenter . Les ressources vCenter importées ne sont pas encore gérées par NetApp Backup and Recovery.
2. Lancez la gestion des vCenters, des machines virtuelles et des banques de données sélectionnés dans NetApp Backup and Recovery. Une fois la gestion lancée, NetApp Backup and Recovery étiquette le vCenter comme « Géré » sur la page Inventaire et est en mesure de sauvegarder et de récupérer les ressources que vous avez importées. Une fois que vous avez lancé la gestion dans NetApp Backup and Recovery, vous ne gérez plus ces ressources dans SnapCenter Plug-in.

Importer les métadonnées vCenter à partir du plug-in SnapCenter

Cette première étape importe les métadonnées vCenter depuis le plug-in SnapCenter . À ce stade, les ressources ne sont pas encore gérées par NetApp Backup and Recovery.

Une fois que vous avez importé les métadonnées vCenter à partir du plug-in SnapCenter , NetApp Backup and Recovery ne prend pas automatiquement en charge la gestion de la protection. Pour ce faire, vous devez choisir explicitement de gérer les ressources importées dans NetApp Backup and Recovery. Cela garantit que vous êtes prêt à ce que ces ressources soient sauvegardées par NetApp Backup and Recovery.

Étapes

1. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez **Inventaire**.
3. À partir de la page des ressources de charge de travail NetApp Backup and Recovery Discover, sélectionnez **Importer depuis SnapCenter**.
4. Dans le champ Importer depuis, sélectionnez * SnapCenter Plug-in pour VMware*.
5. Saisissez les **informations d'identification VMware vCenter** :
   a. **vCenter IP/nom d'hôte** : saisissez le nom de domaine complet ou l'adresse IP du vCenter que vous souhaitez importer dans NetApp Backup and Recovery.
   b. **Numéro de port vCenter** : saisissez le numéro de port du vCenter.
   c. **Nom d'utilisateur vCenter** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du vCenter.
   d. **Connecteur** : sélectionnez l'agent de console pour vCenter.
6. Saisissez les informations d'identification de l'hôte du plug-in SnapCenter * :
   a. **Informations d'identification existantes** : si vous sélectionnez cette option, vous pouvez utiliser les informations d'identification existantes que vous avez déjà ajoutées. Choisissez le nom des informations d'identification.
   b. **Ajouter de nouvelles informations d'identification** : si vous ne disposez pas d'informations d'identification d'hôte SnapCenter Plug-in existantes, vous pouvez en ajouter de nouvelles. Saisissez le nom des informations d'identification, le mode d'authentification, le nom d'utilisateur et le mot de passe.
7. Sélectionnez **Importer** pour valider vos entrées et enregistrer le plug-in SnapCenter .

> Si le plug-in SnapCenter est déjà enregistré, vous pouvez mettre à jour les détails d'enregistrement existants.

Résultat

La page Inventaire affiche le vCenter comme non géré dans NetApp Backup and Recovery jusqu'à ce que vous choisissiez explicitement de le gérer.

Gérer les ressources importées depuis le plug-in SnapCenter

Après avoir importé les métadonnées vCenter à partir du plug-in SnapCenter pour VMware, gérez les ressources dans NetApp Backup and Recovery. Une fois que vous avez choisi de gérer ces ressources, NetApp Backup and Recovery est en mesure de sauvegarder et de récupérer les ressources que vous avez importées. Une fois que vous avez lancé la gestion dans NetApp Backup and Recovery, vous ne gérez plus ces ressources dans SnapCenter Plug-in.

Une fois que vous avez choisi de gérer les ressources, les ressources, les machines virtuelles et les stratégies sont importées à partir du plug-in SnapCenter pour VMware. Les groupes de ressources, les stratégies et les instantanés sont migrés à partir du plug-in et sont gérés dans NetApp Backup and Recovery.

Étapes

1. Après avoir importé les ressources VMware à partir du plug-in SnapCenter , dans le menu Sauvegarde et récupération, sélectionnez **Inventaire**.
2. Depuis la page Inventaire, sélectionnez le vCenter importé que vous souhaitez que NetApp Backup and Recovery gère désormais.

3. Sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.
4. Depuis la page Inventaire > Charge de travail, sélectionnez l'icône Actions ••• > **Gérer** pour afficher la page Gérer vCenter.
5. Cochez la case « Voulez-vous continuer la migration ? » et sélectionnez **Migrer**.

Résultat

La page Inventaire affiche les ressources vCenter nouvellement gérées.

Accéder au tableau de bord de NetApp Backup and Recovery

1. Pour afficher le tableau de bord, dans le menu Sauvegarde et restauration, sélectionnez **Tableau de bord**.
2. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

   "Découvrez ce que le tableau de bord vous montre".

Créez et gérez des groupes de protection pour les charges de travail VMware avec NetApp Backup and Recovery

Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de charges de travail. Un groupe de protection est un regroupement logique de ressources telles que des machines virtuelles et des banques de données que vous souhaitez protéger ensemble.

Vous pouvez effectuer les tâches suivantes liées aux groupes de protection :

- Créer un groupe de protection.
- Afficher les détails de la protection.
- Sauvegardez un groupe de protection maintenant. Voir"Sauvegardez les charges de travail VMware maintenant" .
- Suspendre et reprendre la planification de sauvegarde d'un groupe de protection.
- Supprimer un groupe de protection.

Créer un groupe de protection

Regroupez les charges de travail que vous souhaitez protéger dans un groupe de protection pour les sauvegarder et les restaurer ensemble.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.

5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les machines virtuelles ou les bases de données que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.

   Si vous souhaitez créer une politique, sélectionnez **Créer une nouvelle politique** et suivez les instructions pour créer une politique. Voir"Créer des politiques" pour plus d'informations.

10. Sélectionnez **Suivant**.
11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

Suspendre la planification de sauvegarde d'un groupe de protection

Suspendez un groupe de protection pour suspendre ses sauvegardes planifiées.

L'état de protection passe à « En maintenance » lorsque vous suspendez un groupe de protection. Vous pouvez reprendre le programme de sauvegarde à tout moment.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez l'icône Actions ••• > **Suspendre le groupe de protection**.
6. Vérifiez le message de confirmation et sélectionnez **Suspendre**.

Reprendre la planification de sauvegarde d'un groupe de protection

La reprise d'un groupe de protection suspendu redémarre les sauvegardes planifiées pour le groupe de protection.

L'état de protection passe de « En maintenance » lorsque vous suspendez un groupe de protection à « Protégé » lorsque vous le reprenez. Vous pouvez reprendre le programme de sauvegarde à tout moment.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez l'icône Actions ••• > **Reprendre le groupe de protection**.
6. Vérifiez le message de confirmation et sélectionnez **Reprendre**.

Résultat

Le système valide les plannings et change le statut de protection en « Protégé » si les plannings sont valides.

Si les planifications ne sont pas valides, le système affiche un message d'erreur et ne reprend pas le groupe de protection.

Supprimer un groupe de protection

Lorsque vous supprimez un groupe de protection, vous le supprimez ainsi que toutes les planifications de sauvegarde du groupe. Supprimez un groupe de protection si vous n'en avez plus besoin.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez le groupe de protection que vous souhaitez supprimer.
6. Sélectionnez l'icône Actions ••• > **Supprimer**.
7. Consultez le message de confirmation concernant la suppression des sauvegardes associées et confirmez la suppression.

Sauvegardez les charges de travail VMware avec NetApp Backup and Recovery

Sauvegardez les machines virtuelles VMware et les banques de données des systèmes ONTAP locaux vers Amazon Web Services, Azure NetApp Files ou StorageGRID pour garantir la protection de vos données. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets sur votre compte cloud public ou privé.

- Pour sauvegarder des charges de travail selon une planification, créez des stratégies qui régissent les opérations de sauvegarde et de restauration. Voir"Créer des politiques" pour les instructions.
- Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de ressources. Voir"Créez et gérez des groupes de protection pour les charges de travail VMware avec NetApp Backup and Recovery" pour plus d'informations.
- Sauvegardez vos charges de travail maintenant (créez une sauvegarde à la demande maintenant).

Sauvegardez vos charges de travail maintenant avec une sauvegarde à la demande

Créez immédiatement une sauvegarde à la demande. Vous souhaiterez peut-être exécuter une sauvegarde à la demande si vous êtes sur le point d'apporter des modifications à votre système et que vous souhaitez vous assurer que vous disposez d'une sauvegarde avant de commencer.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu Sauvegarde et récupération, sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**, **Magasins de données** ou **Machines virtuelles**.

5. Sélectionnez le groupe de protection, les banques de données ou les machines virtuelles que vous souhaitez sauvegarder.
6. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.

> La politique appliquée à la sauvegarde est la même politique que celle attribuée au groupe de protection, à la banque de données ou à la machine virtuelle.

7. Sélectionnez le niveau de planification.
8. Sélectionnez **Sauvegarder maintenant**.

Restaurer les charges de travail VMware

Restaurer les charges de travail VMware avec NetApp Backup and Recovery

Restaurez les charges de travail VMware à partir d'instantanés, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage objet à l'aide de NetApp Backup and Recovery.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des charges de travail à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal (instantané local)
- Restaurer à partir d'une ressource répliquée sur un stockage secondaire
- Restaurer à partir d'une sauvegarde de stockage d'objets

Restaurer ces points

Vous pouvez restaurer les données à ces points :

- **Restauration à l'emplacement d'origine** : La machine virtuelle est restaurée à son emplacement d'origine, sur le même déploiement vCenter, le même hôte ESXi et la même banque de données. La machine virtuelle et toutes ses données ont été écrasées.
- **Restaurer vers un autre emplacement** : Vous pouvez choisir un autre vCenter, hôte ESXi ou datastore comme cible de restauration pour la VM. Ceci est utile pour gérer différentes copies d'une même machine virtuelle situées à différents endroits et dans différents états.

Considérations relatives à la restauration à partir du stockage d'objets

Si la résilience aux ransomwares est activée pour un fichier de sauvegarde dans le stockage d'objets, vous êtes invité à exécuter une vérification supplémentaire avant la restauration. Nous vous recommandons d'effectuer l'analyse.

> Vous devrez peut-être payer des frais supplémentaires à votre fournisseur de cloud pour accéder au fichier de sauvegarde.

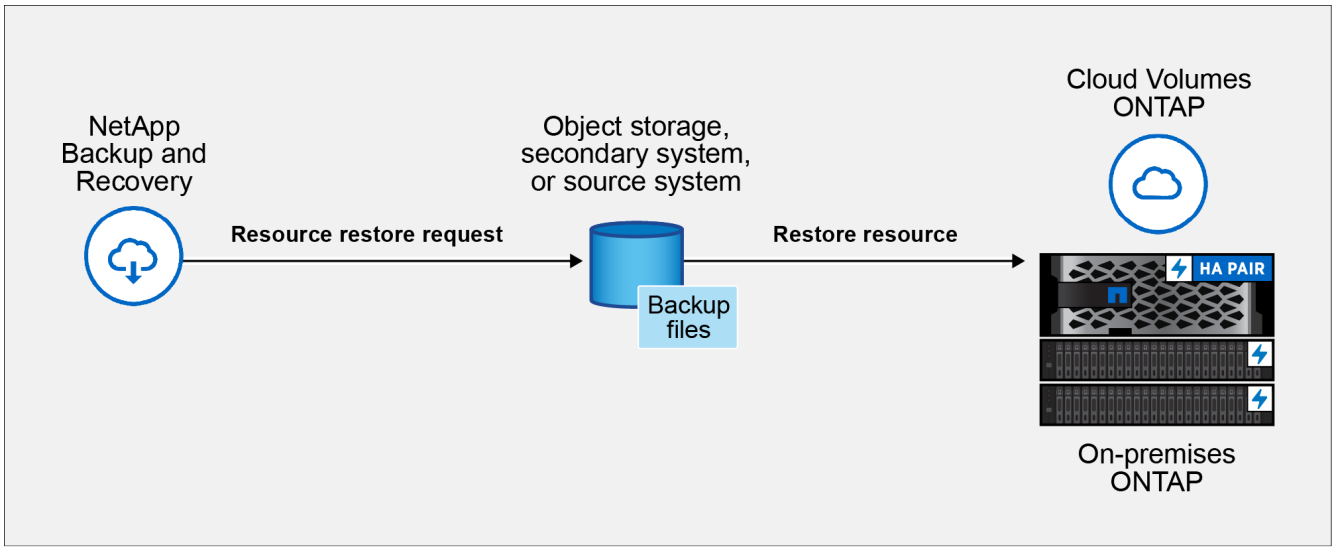
Comment fonctionne la restauration des charges de travail

Lorsque vous restaurez des charges de travail, les événements suivants se produisent :

- Lorsque vous restaurez une charge de travail à partir d'un instantané local ou d'une sauvegarde distante, NetApp Backup and Recovery écrase la machine virtuelle d'origine si vous effectuez la restauration à l'emplacement d'origine, et crée une *nouvelle* ressource si vous effectuez la restauration à un

emplacement alternatif.

- Lorsque vous restaurez une charge de travail répliquée, vous pouvez la restaurer sur le système ONTAP local d'origine ou sur un autre système ONTAP local.



- Lorsque vous restaurez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données sur le système d'origine ou sur un système ONTAP local.

À partir de la page Restaurer (Rechercher et restaurer), vous pouvez restaurer une ressource en recherchant l'instantané avec des filtres, même si vous ne vous souvenez pas de son nom exact, de son emplacement ou de sa dernière date connue.

Restaurer les données de charge de travail à partir de l'option Restaurer (Rechercher et restaurer)

Restaurez les charges de travail VMware à l'aide de l'option Restaurer. Vous pouvez rechercher l'instantané par son nom ou en utilisant des filtres.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Restaurer**.
2. Dans la liste déroulante située à droite du champ de recherche par nom, sélectionnez **VMware**.
3. Saisissez le nom de la ressource que vous souhaitez restaurer ou filtrez le vCenter, le centre de données ou la banque de données où se trouve la ressource que vous souhaitez restaurer.

   Une liste de machines virtuelles correspondant à vos critères de recherche s'affiche.

4. Trouvez dans la liste la machine virtuelle que vous souhaitez restaurer, puis sélectionnez le bouton du menu des options correspondant à cette machine virtuelle.
5. Dans le menu qui s'affiche, sélectionnez **Restaurer la machine virtuelle**.

   Une liste des instantanés (points de restauration) créés sur cette machine virtuelle s'affiche. Par défaut, les dernières captures d'écran sont affichées pour la période que vous sélectionnez dans le menu déroulant **Période**.

Pour chaque instantané, les icônes illuminées dans la colonne **Emplacement** indiquent les emplacements de stockage où l'instantané est disponible (stockage principal, secondaire ou objet).

6. Activez l'option correspondant à la capture d'écran que vous souhaitez restaurer.
7. Sélectionnez **Suivant**.

   Les options de localisation de l'instantané apparaissent.

8. Sélectionnez la destination de restauration de l'instantané :
   - **Local** : Restaure l'instantané à partir de l'emplacement local.
   - **Secondaire** : Restaure l'instantané à partir d'un emplacement de stockage distant.
   - **Stockage d'objets** : Restaure l'instantané à partir du stockage d'objets.

     Si vous choisissez un stockage secondaire, sélectionnez l'emplacement de destination dans la liste déroulante.

9. Sélectionnez **Suivant** pour continuer.
10. Choisissez la destination et les paramètres de restauration :

Sélection de la destination

Restaurer à l'emplacement d'origine

Lors de la restauration à l'emplacement d'origine, vous ne pouvez pas modifier le vCenter de destination, l'hôte ESXi, le datastore ou le nom de la VM. La machine virtuelle d'origine est écrasée lors de l'opération de restauration.

1. Sélectionnez le volet **Emplacement d'origine**.
2. Choisissez parmi les options suivantes :
   - Section **Options de pré-restauration** :
     - **Script** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé avant le début de l'opération de restauration. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
   - Section **Options après restauration** :
     - **Redémarrer la machine virtuelle** : Activez cette option pour redémarrer la machine virtuelle une fois l'opération de restauration terminée et après l'application du script post-restauration.
     - **Post-scriptum** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé une fois la restauration terminée. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
3. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

Lors de la restauration vers un autre emplacement, vous pouvez modifier le vCenter de destination, l'hôte ESXi, le datastore et le nom de la VM pour créer une nouvelle copie de la VM dans un emplacement différent ou avec un nom différent.

1. Sélectionnez le volet **Emplacement alternatif**.
2. Saisissez les informations suivantes :
   - Section **Paramètres de destination** :
     - **Nom de domaine complet (FQDN) ou adresse IP du serveur vCenter** : Sélectionnez le serveur vCenter sur lequel vous souhaitez restaurer l'instantané.
     - **Hôte ESXi** : Sélectionnez l'hôte sur lequel vous souhaitez restaurer l'instantané.
     - **Réseau** : Sélectionnez le réseau sur lequel vous souhaitez restaurer l'instantané.
     - **Banque de données** : Dans la liste déroulante, sélectionnez le nom de la banque de données dans laquelle vous souhaitez restaurer l'instantané.
     - **Nom de la machine virtuelle** : Saisissez le nom de la machine virtuelle sur laquelle vous souhaitez restaurer l'instantané. Si le nom correspond à une machine virtuelle qui existe déjà dans la banque de données, Backup and Recovery rend le nom unique en y ajoutant un horodatage actuel.
   - Section **Options de pré-restauration** :
     - **Script** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé avant le début de l'opération de restauration. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
   - Section **Options après restauration** :
     - **Redémarrer la machine virtuelle** : Activez cette option pour redémarrer la machine virtuelle une fois l'opération de restauration terminée et après l'application du script post-restauration.

- **Post-scriptum** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé une fois la restauration terminée. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.

3. Sélectionnez **Restaurer**.

Restaurer des disques virtuels spécifiques à partir de sauvegardes

Vous pouvez restaurer des disques virtuels existants (VMDK), ou des disques virtuels supprimés ou détachés, à partir d'une sauvegarde primaire ou secondaire de machines virtuelles traditionnelles. Cela vous permet de restaurer uniquement des données ou des applications spécifiques de la machine virtuelle, vous évitant ainsi de restaurer l'intégralité de la machine virtuelle et tous ses disques virtuels associés dans les cas où seules certaines données sont affectées. Une fois le disque virtuel restauré, il est rattaché à sa machine virtuelle d'origine et prêt à l'emploi.

Vous pouvez restaurer un ou plusieurs disques de machine virtuelle (VMDK) sur une VM sur le même datastore ou sur des datastores différents.

Pour améliorer les performances des opérations de restauration dans les environnements NFS, activez l'API vStorage de l'application VMware pour l'intégration de baies (VAAI).

Avant de commencer

- Une sauvegarde doit exister.
- La VM ne doit pas être en transit.

  La machine virtuelle que vous souhaitez restaurer ne doit pas être dans un état vMotion ou Storage vMotion.

À propos de cette tâche

- Si le VMDK est supprimé ou détaché de la VM, l'opération de restauration attache le VMDK à la VM.
- Une opération de restauration peut échouer si le niveau de stockage du FabricPool où se trouve la machine virtuelle n'est pas disponible.
- Les opérations de connexion et de restauration connectent les VMDK à l'aide du contrôleur SCSi par défaut. Cependant, lorsque les VMDK attachés à une machine virtuelle avec un disque NVMe sont sauvegardés, les opérations d'attachement et de restauration utilisent le contrôleur NVMe s'il est disponible.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Restaurer**.
2. Dans la liste déroulante située à droite du champ de recherche par nom, sélectionnez **VMware**.
3. Saisissez le nom de la ressource que vous souhaitez restaurer ou filtrez le vCenter, le centre de données ou la banque de données où se trouve la ressource que vous souhaitez restaurer.

   Une liste de machines virtuelles correspondant à vos critères de recherche s'affiche.

4. Trouvez dans la liste la machine virtuelle que vous souhaitez restaurer, puis sélectionnez le bouton du menu des options correspondant à cette machine virtuelle.

5. Dans le menu qui s’affiche, sélectionnez **Restaurer les disques virtuels**.

   Une liste des instantanés (points de restauration) créés sur cette machine virtuelle s’affiche. Par défaut, les dernières captures d’écran sont affichées pour la période que vous sélectionnez dans le menu déroulant **Période**.

   Pour chaque instantané, les icônes illuminées dans la colonne **Emplacement** indiquent les emplacements de stockage où l’instantané est disponible (stockage principal, secondaire ou objet).

6. Activez l’option correspondant à la capture d’écran que vous souhaitez restaurer.
7. Sélectionnez **Suivant**.

   Les options de localisation de l’instantané apparaissent.

8. Sélectionnez la destination de restauration de l’instantané :
   - **Local** : Restaure l’instantané à partir de l’emplacement local.
   - **Secondaire** : Restaure l’instantané à partir d’un emplacement de stockage distant.
   - **Stockage d’objets** : Restaure l’instantané à partir du stockage d’objets.

     Si vous choisissez un stockage secondaire, sélectionnez l’emplacement de destination dans la liste déroulante.

9. Sélectionnez **Suivant** pour continuer.
10. Choisissez la destination et les paramètres de restauration :

Sélection de la destination

Restaurer à l'emplacement d'origine

Lors de la restauration à l'emplacement d'origine, vous ne pouvez pas modifier le vCenter de destination, l'hôte ESXi, le datastore ou le nom du disque virtuel. Le disque virtuel d'origine est écrasé.

1. Sélectionnez le volet **Emplacement d'origine**.
2. Dans la section **Paramètres de destination**, cochez la case correspondant aux disques virtuels que vous souhaitez restaurer.
3. Choisissez parmi les options suivantes :
   - Section **Options de pré-restauration** :
     - **Script** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé avant le début de l'opération de restauration. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
   - Section **Options après restauration** :
     - **Post-scriptum** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé une fois la restauration terminée. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
4. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

Lors de la restauration vers un emplacement alternatif, vous pouvez modifier le magasin de données de destination. Le disque virtuel est rattaché à la machine virtuelle d'origine après l'opération de restauration, quel que soit le datastore choisi.

1. Sélectionnez le volet **Emplacement alternatif**.
2. Dans la section **Paramètres de destination**, cochez la case correspondant aux disques virtuels que vous souhaitez restaurer.
3. Pour tous les disques virtuels que vous avez sélectionnés :
   a. Choisissez **Sélectionner un datastore** pour choisir une autre cible de restauration pour le disque virtuel.
   b. Sélectionnez **Sélectionner** pour confirmer votre choix et fermer la fenêtre de sélection.
4. Choisissez parmi les options suivantes :
   - Section **Options de pré-restauration** :
     - **Script** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé avant le début de l'opération de restauration. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
   - Section **Options après restauration** :
     - **Post-scriptum** : Activez cette option pour automatiser des tâches supplémentaires en exécutant un script personnalisé une fois la restauration terminée. Saisissez le chemin d'accès complet au script à exécuter ainsi que les arguments qu'il accepte.
5. Sélectionnez **Restaurer**.

Restaurer les fichiers et dossiers invités

Vous pouvez restaurer des fichiers ou des dossiers à partir d'un disque de machine virtuelle (VMDK) sur un système d'exploitation invité Windows.

Flux de travail de restauration des invités

Les opérations de restauration du système d'exploitation invité incluent les étapes suivantes :

1. Attacher

   Attachez un disque virtuel à une machine virtuelle invitée et démarrez une session de restauration de fichiers invitée.

2. Attendez

   Veuillez patienter jusqu'à la fin de l'opération de rattachement avant de pouvoir parcourir et restaurer les données. Une fois l'opération de connexion terminée, une session de restauration de fichiers invité est automatiquement créée.

3. Sélectionner des fichiers ou des dossiers

   Parcourez les fichiers VMDK et sélectionnez un ou plusieurs fichiers ou dossiers à restaurer.

4. Restaurer

   Restaurer les fichiers ou dossiers sélectionnés à un emplacement spécifié.

Conditions préalables à la restauration des fichiers et dossiers invités

Veuillez vérifier toutes les exigences avant de restaurer des fichiers ou des dossiers à partir d'une VMDK sur un système d'exploitation invité Windows.

- Les outils VMware doivent être installés et en cours d'exécution.

  NetApp Backup and Recovery utilise les informations des outils VMware pour établir une connexion avec le système d'exploitation invité VMware.

- Le système d'exploitation invité Windows doit exécuter Windows Server 2008 R2 ou une version ultérieure.

  Pour obtenir les dernières informations sur les versions prises en charge, reportez-vous à "Outil de matrice d'interopérabilité NetApp (IMT)" .

- Les informations d'identification de la machine virtuelle cible utilisent le compte d'administrateur de domaine ou local intégré avec le nom d'utilisateur « Administrateur ». Avant de lancer l'opération de restauration, configurez les informations d'identification de la machine virtuelle sur laquelle vous souhaitez attacher le disque virtuel. Des informations d'identification sont requises pour les opérations de connexion et de restauration. Les utilisateurs du groupe de travail peuvent utiliser le compte d'administrateur local intégré.

  Si vous devez utiliser un compte qui n'est pas le compte administrateur intégré, mais qui dispose de privilèges administratifs au sein de la machine virtuelle, vous devez désactiver l'UAC sur la machine virtuelle invitée.

- Vous devez connaître l'instantané de sauvegarde et le VMDK à partir desquels effectuer la restauration.

  NetApp Backup and Recovery ne prend pas en charge la recherche de fichiers ou de dossiers à restaurer. Avant de commencer, vous devez savoir où se trouvent les fichiers ou dossiers dans l'instantané et le VMDK correspondant.

- Le disque virtuel à connecter doit figurer dans une sauvegarde NetApp Backup and Recovery .

  Le disque virtuel contenant le fichier ou le dossier que vous souhaitez restaurer doit se trouver dans une sauvegarde de machine virtuelle effectuée à l'aide de NetApp Backup and Recovery.

- Pour les fichiers dont les noms ne sont pas en alphabet anglais, vous devez les restaurer dans un répertoire et non sous forme de fichier unique.

  Vous pouvez restaurer des fichiers avec des noms non alphabétiques, tels que des kanji japonais, en restaurant le répertoire dans lequel se trouvent les fichiers.

Limitations de la restauration des fichiers invités

Avant de restaurer un fichier ou un dossier à partir d'un système d'exploitation invité, vous devez prendre connaissance des limitations de cette fonctionnalité.

- Vous ne pouvez pas restaurer les types de disques dynamiques dans un système d'exploitation invité.
- Si vous restaurez un fichier ou un dossier chiffré, l'attribut de chiffrement n'est pas conservé.
- Vous ne pouvez pas restaurer des fichiers ou des dossiers dans un dossier crypté.
- Les fichiers et dossiers cachés sont affichés dans la page de navigation des fichiers, et vous ne pouvez pas les filtrer.
- Vous ne pouvez pas restaurer à partir d'un système d'exploitation invité Linux.

  Vous ne pouvez pas restaurer des fichiers et des dossiers à partir d'une machine virtuelle exécutant un système d'exploitation invité Linux. Cependant, vous pouvez attacher un VMDK, puis restaurer manuellement les fichiers et les dossiers. Pour obtenir les dernières informations sur les systèmes d'exploitation invités pris en charge, reportez-vous à la "Outil de matrice d'interopérabilité NetApp (IMT)" .

- Vous ne pouvez pas restaurer d'un système de fichiers NTFS vers un système de fichiers FAT.

  Lorsque vous essayez de restaurer du format NTFS au format FAT, le descripteur de sécurité NTFS n'est pas copié car le système de fichiers FAT ne prend pas en charge les attributs de sécurité Windows.

- Vous ne pouvez pas restaurer les fichiers invités à partir d'un VMDK cloné ou d'un VMDK non initialisé.
- Vous ne pouvez pas restaurer la structure du répertoire d'un fichier.

  Lorsque vous restaurez un fichier à partir d'un répertoire imbriqué, le système ne restaure que le fichier, et non sa structure de répertoires. Pour restaurer l'intégralité de l'arborescence de répertoires, copiez le répertoire racine.

- Vous ne pouvez pas restaurer les fichiers invités d'une machine virtuelle vVol vers un autre hôte.
- Vous ne pouvez pas restaurer les fichiers invités cryptés.

Restaurer les fichiers et dossiers invités à partir des VMDK

Vous pouvez restaurer un ou plusieurs fichiers ou dossiers à partir d'un VMDK sur un

système d'exploitation invité Windows.

Avant de commencer

Vous devez créer des informations d'identification pour la machine virtuelle invitée dans NetApp Backup and Recovery avant de pouvoir restaurer des fichiers et des dossiers à partir de celle-ci. NetApp Backup and Recovery utilise ces informations d'identification pour s'authentifier auprès de la machine virtuelle invitée lors de la connexion du disque virtuel.

À propos de cette tâche

Les performances de restauration des fichiers ou dossiers invités dépendent de deux facteurs : la taille des fichiers ou dossiers restaurés ; et le nombre de fichiers ou dossiers restaurés. La restauration d'un grand nombre de fichiers de petite taille peut prendre plus de temps que prévu par rapport à la restauration d'un petit nombre de fichiers de grande taille, si l'ensemble de données à restaurer est de la même taille.

Une seule opération d'attachement ou de restauration peut être exécutée en même temps sur une machine virtuelle. Vous ne pouvez pas exécuter d'opérations d'attachement ou de restauration parallèles sur la même machine virtuelle.

Grâce à la fonction de restauration invité, vous pouvez afficher et restaurer les fichiers système et cachés, ainsi que visualiser les fichiers chiffrés. Ne pas écraser un fichier système existant ni restaurer des fichiers chiffrés dans un dossier chiffré. Lors de l'opération de restauration, les attributs cachés, système et chiffrés des fichiers invités ne sont pas conservés dans le fichier restauré. La consultation ou la navigation dans les partitions réservées peut provoquer une erreur.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez le menu **Machines virtuelles**.
3. Choisissez dans la liste la machine virtuelle contenant les fichiers que vous souhaitez restaurer.
4. Sélectionnez l'icône Actions ••• pour cette machine virtuelle.
5. Sélectionnez **Restaurer les fichiers et dossiers**.
6. Sélectionnez un instantané à partir duquel effectuer la restauration, puis sélectionnez **Suivant**.
7. Choisissez l'emplacement du snapshot à restaurer. Si vous choisissez un emplacement secondaire, sélectionnez l'instantané secondaire dans la liste.
8. Sélectionnez **Suivant**.
9. Choisissez le disque virtuel dans la liste à attacher à la machine virtuelle, puis sélectionnez **Suivant**.
10. Sur la page *Sélectionner les informations d'identification de la machine virtuelle*, si vous n'avez pas encore enregistré d'informations d'identification pour la machine virtuelle invitée, sélectionnez **Ajouter des informations d'identification** et procédez comme suit :
    a. **Nom des informations d'identification** : saisissez un nom pour les informations d'identification.
    b. **Mode d'authentification** : Sélectionnez **Windows**.
    c. **Agents** : Sélectionnez dans la liste un agent de console qui gérera la communication entre NetApp Backup and Recovery et cet hôte.
    d. **Domaine et nom d'utilisateur** : saisissez le nom de domaine complet NetBIOS ou du domaine et le nom d'utilisateur pour les informations d'identification.
    e. **Mot de passe** : Veuillez saisir un mot de passe pour l'identifiant.

f. Sélectionnez **Ajouter**.

11. Choisissez des informations d'identification de machine virtuelle à utiliser pour vous authentifier auprès de la machine virtuelle invitée.

    NetApp Backup and Recovery attache le disque virtuel à la machine virtuelle et affiche tous les fichiers et dossiers, y compris les fichiers cachés. Il attribue une lettre de lecteur à chaque partition, y compris les partitions réservées au système.

    Les fichiers et dossiers que vous avez sélectionnés sont listés dans le volet droit de l'écran.

12. Sélectionnez **Suivant**.
13. Saisissez le chemin de partage UNC vers l'invité où les fichiers sélectionnés seront restaurés.

    - Exemple d'adresse IPv4 : `\\10.60.136.65\c$`
    - Exemple d'adresse IPv6 : `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

    S'il existe déjà des fichiers portant le même nom, vous pouvez choisir de les écraser ou de les ignorer.

14. Sélectionnez **Restaurer**.

    Vous pouvez consulter la progression de la restauration sur la page de suivi des tâches.

Résolution des problèmes de restauration des fichiers invités

Lorsque vous tentez de restaurer un fichier invité, vous pouvez rencontrer l'un des scénarios suivants.

La session de restauration du fichier invité est vide

Ce problème survient si vous créez une session de restauration de fichiers invité et que le système d'exploitation invité redémarre pendant la session. Les fichiers VMDK du système d'exploitation invité peuvent rester hors ligne, la liste des sessions de restauration de fichiers invités est donc vide.

Pour corriger le problème, remettez manuellement les VMDK en ligne dans le système d'exploitation invité. Lorsque les VMDK sont en ligne, la session de restauration des fichiers invités affiche le contenu correct.

L'opération de restauration du fichier invité et de connexion au disque échoue

Ce problème se produit lorsque vous démarrez une opération de restauration de fichier invité, mais que l'opération de connexion de disque échoue même si les outils VMware sont en cours d'exécution et que les informations d'identification du système d'exploitation invité sont correctes. Si cela se produit, l'erreur suivante est renvoyée :

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

Pour corriger le problème, redémarrez le service Windows VMware Tools sur le système d'exploitation invité, puis réessayez l'opération de restauration du fichier invité.

Les sauvegardes ne sont pas détachées après l'arrêt de la session de restauration des fichiers invités

Ce problème se produit lorsque vous effectuez une opération de restauration de fichier invité à partir d'une sauvegarde cohérente avec la machine virtuelle. Pendant que la session de restauration de fichiers invités est active, une autre sauvegarde cohérente avec la machine virtuelle est effectuée pour la même machine virtuelle. Lorsque la session de restauration de fichiers invités est déconnectée, manuellement ou automatiquement après 24 heures, les sauvegardes de la session ne sont pas détachées.

Pour corriger le problème, détachez manuellement les VMDK qui ont été attachés à la session de restauration de fichiers invités active.

Protéger les charges de travail KVM (Aperçu)

Présentation de la protection des charges de travail KVM

Protégez vos machines virtuelles KVM gérées et vos pools de stockage avec NetApp Backup and Recovery. NetApp Backup and Recovery offre des opérations de sauvegarde et de restauration rapides, économes en espace, cohérentes en cas de panne et compatibles avec les machines virtuelles. Vos hôtes KVM et vos machines virtuelles doivent être gérés par une plateforme de gestion telle qu'Apache CloudStack avant que vous puissiez les protéger à l'aide de la sauvegarde et de la restauration.

Vous pouvez sauvegarder les charges de travail KVM sur Amazon Web Services S3, Azure NetApp Files ou StorageGRID et restaurer les charges de travail KVM sur un hôte KVM local.

Utilisez NetApp Backup and Recovery pour mettre en œuvre une stratégie de protection 3-2-1, où vous disposez de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud. Les avantages de l'approche 3-2-1 incluent :

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.
- L'utilisation de différents types de supports vous aide à récupérer si l'un d'eux tombe en panne.
- Vous pouvez restaurer rapidement à partir de la copie sur site et utiliser les copies hors site si la copie sur site est compromise.

Pour basculer vers et depuis les versions de l'interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Vous pouvez utiliser NetApp Backup and Recovery pour effectuer les tâches suivantes liées aux charges de travail KVM :

- "Découvrez les charges de travail KVM"
- "Créer et gérer des groupes de protection pour les charges de travail KVM"
- "Sauvegarder les charges de travail KVM"
- "Restaurer les charges de travail KVM"

Découvrez les charges de travail KVM dans NetApp Backup and Recovery

NetApp Backup and Recovery doit détecter les hôtes KVM et les machines virtuelles avant de les protéger. Vos hôtes KVM et vos machines virtuelles doivent être gérés par

une plateforme de gestion telle qu'Apache CloudStack avant de pouvoir être ajoutés à la sauvegarde et à la restauration.

Rôle de console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Ajoutez une plateforme de gestion, un hôte KVM et découvrez les ressources.

Ajoutez les informations relatives à la plateforme de gestion et à l'hôte KVM, et laissez NetApp Backup and Recovery découvrir les charges de travail.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Sous **Charges de travail**, sélectionnez la vignette **KVM**.

   Si vous vous connectez à Backup and Recovery pour la première fois et que vous avez un système dans la console mais aucune ressource découverte, la page *Bienvenue sur le nouveau NetApp Backup and Recovery* apparaît avec une option pour **Découvrir les ressources**.

3. Sélectionnez **Découvrir les ressources**.
4. Saisissez les informations suivantes :
   a. **Type de charge de travail** : sélectionnez **KVM**.
   b. Si vous n'avez pas encore intégré votre plateforme de gestion à Backup and Recovery, sélectionnez **Ajouter une plateforme de gestion**.
      i. Saisissez les informations suivantes :
         - **Adresse IP ou nom de domaine complet de la plateforme de gestion** : Saisissez l'adresse IP ou le nom de domaine complet de la plateforme de gestion.
         - **Clé API** : Saisissez la clé API à utiliser pour authentifier les requêtes API.
         - **Clé secrète** : Saisissez la clé secrète à utiliser pour authentifier les requêtes API.
         - **Port** : Saisissez le port à utiliser pour la communication entre la sauvegarde et la restauration et la plateforme de gestion.
         - **Agents** : Sélectionnez un agent de console à utiliser pour faciliter la communication entre la sauvegarde et la restauration et la plateforme de gestion.
      ii. Une fois terminé, sélectionnez **Ajouter**.
   c. **Paramètres KVM** : Ajoutez un nouvel hôte KVM en saisissant les informations suivantes :
      - **Nom de domaine complet KVM ou adresse IP** : Saisissez le nom de domaine complet ou l'adresse IP de l'hôte.
      - **Identifiants** : Veuillez saisir le nom d'utilisateur et le mot de passe de l'hôte KVM.
      - **Agent de console** : Choisissez l'agent de console à utiliser pour la communication entre Backup and Recovery et l'hôte KVM.
      - **Numéro de port** : Saisissez le port à utiliser pour la communication entre Backup and Recovery et l'hôte KVM.
      - **Plateforme de gestion** : Si l'hôte KVM est géré et que vous avez ajouté la plateforme de gestion à Backup and Recovery, sélectionnez la plateforme de gestion dans la liste.

5. Sélectionnez **Découvrir**.

Ce processus peut prendre quelques minutes.

Résultat

La charge de travail KVM s'affiche dans la liste des charges de travail sur la page Inventaire.

Accéder au tableau de bord de NetApp Backup and Recovery

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.
4. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

Créez et gérez des groupes de protection pour les charges de travail KVM avec NetApp Backup and Recovery

Créez des groupes de protection pour gérer les opérations de sauvegarde d'un ensemble de ressources KVM. Un groupe de protection est un regroupement logique de ressources telles que des machines virtuelles et des pools de stockage que vous souhaitez protéger ensemble. Vous devez créer un groupe de protection pour sauvegarder les machines virtuelles KVM ou les pools de stockage.

Vous pouvez effectuer les tâches suivantes liées aux groupes de protection :

- Créer un groupe de protection.
- Afficher les détails de la protection.
- Sauvegardez un groupe de protection maintenant. Voir"Sauvegardez les charges de travail KVM maintenant" .
- Supprimer un groupe de protection.

Créer un groupe de protection

Regroupez les machines virtuelles et les pools de stockage que vous souhaitez protéger dans un groupe de protection.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.

4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les machines virtuelles ou les pools de stockage que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.

   Pour plus d'informations sur la création d'une politique de sauvegarde, reportez-vous à"Créer et gérer des politiques" .
10. Sélectionnez **Suivant**.
11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

Supprimer un groupe de protection

La suppression d'un groupe de protection le supprime ainsi que toutes les planifications de sauvegarde associées. Vous souhaiterez peut-être supprimer un groupe de protection s'il n'est plus nécessaire.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez le groupe de protection que vous souhaitez supprimer.
6. Sélectionnez l'icône Actions ••• > **Supprimer**.
7. Consultez le message de confirmation concernant la suppression des sauvegardes associées et confirmez la suppression.

Sauvegardez les charges de travail KVM avec NetApp Backup and Recovery

Sauvegardez les groupes de protection KVM des systèmes ONTAP locaux vers Amazon Web Services, Azure NetApp Files ou StorageGRID pour garantir la protection de vos données. Lorsque vous sauvegardez un groupe de protection, la NetApp Console sauvegarde les machines virtuelles et les pools de stockage contenus dans le groupe de protection. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets sur votre compte cloud public ou privé.

Pour sauvegarder des groupes de protection selon une planification, créez des stratégies qui régissent les opérations de sauvegarde et de restauration. Voir"Créer des politiques" pour les instructions.

- Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de ressources. Voir"Créez et gérez des groupes de protection pour les charges de travail KVM avec NetApp Backup and Recovery" pour plus d'informations.

Sauvegardez maintenant les groupes de protection avec une sauvegarde à la demande

Vous pouvez exécuter une sauvegarde à la demande immédiatement. Cela est utile si vous êtes sur le point d'apporter des modifications à votre système et que vous souhaitez vous assurer que vous disposez d'une sauvegarde avant de commencer.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Dans la mosaïque KVM, sélectionnez **Découvrir et gérer**.
3. Sélectionnez **Inventaire**.
4. Sélectionnez une charge de travail pour afficher les détails de protection.
5. Sélectionnez l'icône Actions ••• > **Voir les détails**.
6. Sélectionnez l'onglet **Groupes de protection**, **Magasins de données** ou **Machines virtuelles**.
7. Sélectionnez le groupe de protection que vous souhaitez sauvegarder.
8. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.

   La politique appliquée à la sauvegarde est la même politique que celle attribuée au groupe de protection.

9. Sélectionnez le niveau de planification.
10. Sélectionnez **Sauvegarder**.

Restaurer les machines virtuelles KVM avec NetApp Backup and Recovery

Restaurez des machines virtuelles KVM à partir d'instantanés, d'une sauvegarde de groupe de protection répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage objet à l'aide de NetApp Backup and Recovery.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des machines virtuelles à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal (instantané local)
- Restaurer à partir d'une ressource répliquée sur un stockage secondaire
- Restaurer à partir d'une sauvegarde de stockage d'objets

Restaurer ces points

Vous pouvez restaurer les données à ces points :

- Restaurer à l'emplacement d'origine

Considérations relatives à la restauration à partir du stockage d'objets

Si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que la protection contre les ransomwares est active pour cette sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la stratégie de sauvegarde), vous êtes invité à exécuter une vérification d'intégrité supplémentaire sur le fichier

de sauvegarde avant de restaurer les données. Nous vous recommandons d'effectuer l'analyse.

Des frais de sortie supplémentaires seront facturés par votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Comment fonctionne la restauration des machines virtuelles

Lorsque vous restaurez des machines virtuelles, les événements suivants se produisent :

- Lorsque vous restaurez une charge de travail à partir d'un fichier de sauvegarde local, NetApp Backup and Recovery crée une *nouvelle* ressource à l'aide des données de la sauvegarde.
- Lorsque vous effectuez une restauration à partir d'une machine virtuelle répliquée, vous pouvez la restaurer sur le système d'origine ou sur un système ONTAP local.
- Lorsque vous restaurez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données sur le système d'origine ou sur un système ONTAP local.

À partir de la page Restaurer (également appelée Rechercher et restaurer), vous pouvez restaurer une machine virtuelle, même si vous ne vous souvenez pas du nom exact, de l'emplacement où elle réside ou de la date à laquelle elle était en bon état pour la dernière fois. Vous pouvez rechercher l'instantané à l'aide de filtres.

Restaurer les machines virtuelles à partir de l'option Restaurer (Rechercher et restaurer)

Restaurez les machines virtuelles KVM à l'aide de l'option Restaurer. Vous pouvez rechercher l'instantané par son nom ou en utilisant des filtres.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Dans le menu NetApp Backup and Recovery , sélectionnez **Restaurer**.
3. Dans la liste déroulante à droite du champ de recherche de nom, sélectionnez **KVM**.
4. Saisissez le nom de la machine virtuelle que vous souhaitez restaurer ou filtrez l'hôte de la machine virtuelle ou le pool de stockage où se trouve la ressource que vous souhaitez restaurer.

   Une liste d'instantanés correspondant à vos critères de recherche apparaît.

5. Sélectionnez le bouton **Restaurer** pour l'instantané que vous souhaitez restaurer.

   Une liste de points de restauration possibles apparaît.

6. Sélectionnez le point de restauration que vous souhaitez utiliser.
7. Sélectionnez un emplacement source d'instantané.
8. Sélectionnez **Suivant** pour continuer.
9. Choisissez la destination et les paramètres de restauration :

Sélection de la destination

Restaurer à l'emplacement d'origine

1. **Activer la restauration rapide** : sélectionnez cette option pour effectuer une opération de restauration rapide. Les volumes et données restaurés seront disponibles immédiatement. N'utilisez pas cette option sur des volumes nécessitant des performances élevées, car pendant le processus de restauration rapide, l'accès aux données peut être plus lent que d'habitude.
2. **Options de pré-restauration** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration et tous les arguments que le script prend.
3. **Options post-restauration**:
   - **Redémarrer la machine virtuelle** : sélectionnez cette option pour redémarrer la machine virtuelle une fois l'opération de restauration terminée et une fois le script de post-restauration appliqué.
   - **Postscript** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.
4. Section **Notification** :
   - **Activer les notifications par e-mail** : sélectionnez cette option pour recevoir des notifications par e-mail concernant l'opération de restauration et indiquez le type de notifications que vous souhaitez recevoir.
5. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

Non disponible en préversion pour les charges de travail KVM.

Protégez les charges de travail Hyper-V

Présentation de la protection des charges de travail Hyper-V

Protégez vos machines virtuelles Hyper-V avec NetApp Backup and Recovery. NetApp Backup and Recovery offre des opérations de sauvegarde et de restauration rapides, économes en espace, cohérentes en cas de panne et cohérentes avec les machines virtuelles, pour les instances autonomes et les clusters FCI. Vous pouvez également protéger les machines virtuelles Hyper-V provisionnées par System Center Virtual Machine Manager (SCVMM) et hébergées sur un partage CIFS.

Vous pouvez sauvegarder les charges de travail Hyper-V sur Amazon Web Services S3 ou StorageGRID et restaurer les charges de travail Hyper-V sur un hôte Hyper-V local.

Utilisez NetApp Backup and Recovery pour mettre en œuvre une stratégie de protection 3-2-1, où vous disposez de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud. Les avantages de l'approche 3-2-1 incluent :

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.
- Plusieurs types de supports garantissent la viabilité du basculement en cas de défaillance physique ou logique d'un type de support.
- La copie sur site vous aide à restaurer rapidement les données et vous pouvez utiliser les copies hors site si la copie sur site est compromise.

Lorsque vous ajoutez des hôtes Hyper-V et découvrez des ressources, NetApp Backup and Recovery installe

le plug-in NetApp Hyper-V et le plug-in NetApp SnapCenter Windows FileSystem sur l'hôte Hyper-V pour faciliter la gestion et la protection des machines virtuelles.

> Pour basculer vers et depuis les versions de l'interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Vous pouvez utiliser NetApp Backup and Recovery pour effectuer les tâches suivantes liées aux charges de travail Hyper-V :

- "Découvrez les charges de travail Hyper-V"
- "Créer et gérer des groupes de protection pour les charges de travail Hyper-V"
- "Sauvegarder les charges de travail Hyper-V"
- "Restaurer les charges de travail Hyper-V"

Découvrez les charges de travail Hyper-V dans NetApp Backup and Recovery

NetApp Backup and Recovery doit détecter les machines virtuelles Hyper-V avant de pouvoir les protéger.

Rôle de console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Ajoutez un hôte Hyper-V et découvrez des ressources

Ajoutez les informations de l'hôte Hyper-V et laissez NetApp Backup and Recovery découvrir les machines virtuelles. Dans chaque agent de console, sélectionnez les systèmes sur lesquels vous souhaitez découvrir les ressources.

> Lorsque vous ajoutez des hôtes Hyper-V et découvrez des ressources, NetApp Backup and Recovery installe le plug-in NetApp Hyper-V et le plug-in NetApp SnapCenter Windows FileSystem sur l'hôte Hyper-V pour faciliter la gestion et la protection des machines virtuelles.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.

   Si c'est la première fois que vous vous connectez à NetApp Backup and Recovery, que vous avez déjà un système dans la console, mais que vous n'avez découvert aucune ressource, la page d'accueil « Bienvenue dans la nouvelle NetApp Backup and Recovery» apparaît et affiche une option pour **Découvrir les ressources**.

2. Sélectionnez **Découvrir les ressources**.
3. Saisissez les informations suivantes :
   a. **Type de charge de travail** : sélectionnez **Hyper-V**.
   b. Si vous n'avez pas encore enregistré les informations d'identification pour cet hôte Hyper-V, sélectionnez **Ajouter des informations d'identification**.
      i. Sélectionnez l'agent de console à utiliser avec cet hôte.
      ii. Saisissez un nom pour ces informations d'identification.

iii. Entrez le nom d'utilisateur et le mot de passe du compte.

iv. Sélectionnez **Terminé**.

c. **Enregistrement de l'hôte** : Ajoutez un nouvel hôte Hyper-V en saisissant le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte, ses informations d'identification, l'agent de console et le numéro de port. Si le nom de domaine complet (FQDN) n'est pas résoluble par l'agent de la console, utilisez plutôt l'adresse IP. Pour les clusters FCI, saisissez l'adresse IP de gestion du cluster FCI.

4. Sélectionnez **Découvrir**.

Ce processus peut prendre quelques minutes.

Résultat

Une fois que NetApp Backup and Recovery a découvert les ressources, la page Inventaire affiche la charge de travail Hyper-V dans la liste des charges de travail.

Accéder au tableau de bord de NetApp Backup and Recovery

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.
4. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

Créez et gérez des groupes de protection pour les charges de travail Hyper-V avec NetApp Backup and Recovery

Créez des groupes de protection pour gérer les opérations de sauvegarde d'un ensemble de machines virtuelles. Un groupe de protection est un regroupement logique de ressources telles que des machines virtuelles que vous souhaitez protéger ensemble.

Vous pouvez effectuer les tâches suivantes liées aux groupes de protection :

- Créer un groupe de protection.
- Afficher les détails de la protection.
- Sauvegardez un groupe de protection maintenant. Voir"Sauvegardez les charges de travail Hyper-V maintenant" .
- Supprimer un groupe de protection.

Créer un groupe de protection

Regroupez les charges de travail que vous souhaitez protéger dans un groupe de protection. Créez un groupe de protection pour sauvegarder et restaurer les charges de travail ensemble.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez le menu **Groupes de protection**.
5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les machines virtuelles que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.
10. Sélectionnez **Suivant**.
11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

Modifier un groupe de protection

Modifiez un groupe de protection pour en changer le nom ou les paramètres. Vous pourriez souhaiter modifier un groupe de protection si les ressources qui le composent ont changé.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez le groupe de protection que vous souhaitez modifier.
6. Sélectionnez l'icône Actions ••• > **Modifier**.
7. Modifiez les paramètres du groupe de protection, tels que son nom ou les machines virtuelles qui le composent.
8. Sélectionnez **Suivant**.
9. Modifiez la politique de protection si nécessaire. Une fois terminé, sélectionnez **Suivant**.
10. Vérifiez la configuration et sélectionnez **Soumettre**.

Supprimer un groupe de protection

La suppression d'un groupe de protection le supprime ainsi que toutes les planifications de sauvegarde associées. Vous souhaiterez peut-être supprimer un groupe de protection s'il n'est plus nécessaire.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.

5. Sélectionnez le groupe de protection que vous souhaitez supprimer.
6. Sélectionnez l'icône Actions ••• > **Supprimer**.
7. Consultez le message de confirmation concernant la suppression des sauvegardes associées et confirmez la suppression.

Sauvegardez les charges de travail Hyper-V avec NetApp Backup and Recovery

Sauvegardez les machines virtuelles Hyper-V des systèmes ONTAP locaux vers Amazon Web Services, Azure NetApp Files ou StorageGRID pour garantir la protection de vos données. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets sur votre compte cloud public ou privé.

- Pour sauvegarder des charges de travail selon une planification, créez des stratégies qui régissent les opérations de sauvegarde et de restauration. Voir"Créer des politiques" pour les instructions.
- Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de ressources. Voir"Créez et gérez des groupes de protection pour les charges de travail Hyper-V avec NetApp Backup and Recovery" pour plus d'informations.
- Sauvegardez vos charges de travail maintenant (créez une sauvegarde à la demande maintenant).

Sauvegardez vos charges de travail maintenant avec une sauvegarde à la demande

Utilisez la sauvegarde à la demande afin que vos données soient protégées avant d'effectuer des modifications sur le système.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu, sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**, **Magasins de données** ou **Machines virtuelles**.
5. Sélectionnez le groupe de protection ou les machines virtuelles que vous souhaitez sauvegarder.
6. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.

> ⓘ La sauvegarde utilise la même politique que celle que vous avez attribuée au groupe de protection ou à la machine virtuelle.

7. Sélectionnez le niveau de planification.
8. Sélectionnez **Sauvegarder**.

Restaurer les charges de travail Hyper-V avec NetApp Backup and Recovery

Restaurez les charges de travail Hyper-V à partir d'instantanés, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage objet à l'aide de NetApp Backup and Recovery.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des charges de travail à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal (instantané local)
- Restaurer à partir d'une ressource répliquée sur un stockage secondaire
- Restaurer à partir d'une sauvegarde de stockage d'objets

Restaurer ces points

Vous pouvez restaurer les données à ces points :

- Restaurer à l'emplacement d'origine
- Restaurer à un autre emplacement

Considérations relatives à la restauration à partir du stockage d'objets

Si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que la protection contre les ransomwares est active pour cette sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la stratégie de sauvegarde), vous êtes invité à exécuter une vérification d'intégrité supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'effectuer l'analyse.

Des frais de sortie supplémentaires seront facturés par votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Comment fonctionne la restauration des charges de travail

Lorsque vous restaurez des charges de travail, les événements suivants se produisent :

- Lorsque vous restaurez une charge de travail à partir d'un fichier de sauvegarde local, NetApp Backup and Recovery crée une *nouvelle* ressource à l'aide des données de la sauvegarde.
- Lorsque vous effectuez une restauration à partir d'une charge de travail répliquée, vous pouvez restaurer la charge de travail sur le système d'origine ou sur un système ONTAP local.

À partir de la page Restaurer (également appelée Rechercher et restaurer), vous pouvez restaurer une ressource, même si vous ne vous souvenez pas du nom exact, de l'emplacement où elle réside ou de la date à laquelle elle était en bon état pour la dernière fois. Vous pouvez rechercher l'instantané à l'aide de filtres.

Restaurer les données de charge de travail à partir de l'option Restaurer (Rechercher et restaurer)

Restaurez les charges de travail Hyper-V à l'aide de l'option Restaurer. Vous pouvez rechercher l'instantané par son nom ou en utilisant des filtres.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Restaurer**.
2. Dans la liste déroulante à droite du champ de recherche de nom, sélectionnez **Hyper-V**.
3. Saisissez le nom de la ressource que vous souhaitez restaurer ou filtrez le nom de la machine virtuelle, l'hôte de la machine virtuelle ou le pool de stockage où se trouve la ressource que vous souhaitez restaurer.

Une liste d'instantanés correspondant à vos critères de recherche apparaît.

4. Sélectionnez le bouton **Restaurer** pour l'instantané que vous souhaitez restaurer.

   Une liste de points de restauration possibles apparaît.

5. Sélectionnez le point de restauration que vous souhaitez utiliser.
6. Sélectionnez un emplacement source d'instantané.
7. Sélectionnez **Suivant** pour continuer.
8. Choisissez la destination et les paramètres de restauration :

Sélection de la destination

Restaurer à l'emplacement d'origine

Lorsque vous restaurez l'emplacement d'origine, vous pouvez consulter les paramètres de destination en développant la section **Paramètres de destination**, mais vous ne pouvez pas les modifier.

1. Dans la section **Options post-restauration**, considérez l'option suivante :
   - **Démarrer la machine virtuelle** : Activez cette option pour démarrer la nouvelle machine virtuelle après sa restauration.
2. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

1. Dans la section **Paramètres de destination**, saisissez les informations suivantes :
   - **Nom de domaine complet ou adresse IP Hyper-V** : Saisissez le nom de domaine complet ou l'adresse IP de l'hôte Hyper-V de destination.
   - **Réseau** : Sélectionnez le réseau de destination sur lequel vous souhaitez restaurer l'instantané.
   - **Nom de la machine virtuelle** : Saisissez le nom de la machine virtuelle que vous souhaitez restaurer.
   - **Emplacement de destination** : Saisissez le dossier de destination ou le partage CIFS qui doit contenir les données restaurées.
2. Dans la section **Options de pré-restauration**, considérez les options suivantes :
   - **Restauration rapide** : Activez cette option pour rendre la machine virtuelle restaurée immédiatement disponible. Seuls les fichiers nécessaires au fonctionnement de la machine virtuelle sont restaurés à partir du stockage d'objets, et non la totalité du volume.
3. Dans la section **Options après restauration**, considérez les options suivantes :
   - **Démarrer la machine virtuelle** : Activez cette option pour démarrer la nouvelle machine virtuelle après sa restauration.
4. Sélectionnez **Restaurer**.

Protéger les charges de travail Oracle Database (Aperçu)

Présentation de la protection des charges de travail de la base de données Oracle

Protégez les bases de données et journaux Oracle à l'aide de NetApp Backup and

Recovery. Obtenez des sauvegardes et des restaurations rapides, économes en espace, cohérentes en cas de panne et cohérentes au niveau de la base de données. Sauvegardez les charges de travail Oracle Database vers AWS S3, NetApp StorageGRID, Azure Blob Storage ou ONTAP S3. Restaurez les sauvegardes sur un hôte Oracle sur site.

Utilisez NetApp Backup and Recovery pour mettre en œuvre une stratégie de protection 3-2-1, où vous disposez de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud. Les avantages de l'approche 3-2-1 incluent :

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.
- L'utilisation de différents types de supports vous aide à récupérer si l'un d'eux tombe en panne.
- Vous pouvez restaurer rapidement à partir de la copie sur site et utiliser les copies hors site si la copie sur site est compromise.

Pour basculer vers et depuis les versions de l'interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Vous pouvez utiliser NetApp Backup and Recovery pour effectuer les tâches suivantes liées aux charges de travail d'Oracle Database :

- "Découvrez les charges de travail Oracle Database"
- "Créer et gérer des groupes de protection pour les charges de travail Oracle Database"
- "Sauvegardez les charges de travail Oracle Database"
- "Restaurer les charges de travail Oracle Database"

Découvrez les charges de travail Oracle Database dans NetApp Backup and Recovery

NetApp Backup and Recovery doit d'abord découvrir vos bases de données Oracle afin que vous puissiez les protéger.

Rôle de console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Ajoutez un hôte Oracle et découvrez des ressources

Ajoutez les informations sur l'hôte Oracle et laissez NetApp Backup and Recovery découvrir les charges de travail. Dans chaque agent de console, sélectionnez les systèmes sur lesquels vous souhaitez découvrir les charges de travail.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Sous **Charges de travail**, sélectionnez la vignette **Oracle**.

   Si vous vous connectez à Backup and Recovery pour la première fois et que vous avez un système dans la console mais aucune ressource découverte, la page *Bienvenue sur le nouveau NetApp Backup and Recovery* apparaît avec une option pour **Découvrir les ressources**.

3. Sélectionnez **Découvrir les ressources**.
4. Saisissez les informations suivantes :
   a. **Type de charge de travail** : sélectionnez **Oracle**.
   b. Si vous n'avez pas encore enregistré les informations d'identification pour cet hôte Oracle, sélectionnez **Ajouter des informations d'identification**.
      i. Sélectionnez l'agent de console à utiliser avec cet hôte.
      ii. Saisissez un nom pour ces informations d'identification.
      iii. Entrez le nom d'utilisateur et le mot de passe du compte.
      iv. Sélectionnez **Terminé**.
   c. **Enregistrement de l'hôte** : ajoutez un nouvel hôte Oracle. Saisissez le nom de domaine complet ou l'adresse IP de l'hôte, les informations d'identification, l'agent de console et le numéro de port.
5. Sélectionnez **Découvrir**.

Ce processus peut prendre quelques minutes.

Résultat

La charge de travail Oracle s'affiche dans la liste des charges de travail sur la page Inventaire.

Accéder au tableau de bord de NetApp Backup and Recovery

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.
4. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

Créez et gérez des groupes de protection pour les charges de travail Oracle Database avec NetApp Backup and Recovery

Créez des groupes de protection pour gérer les opérations de sauvegarde d'un ensemble de ressources de base de données Oracle. Un groupe de protection est un regroupement logique de ressources telles que des bases de données que vous souhaitez protéger ensemble. Vous devez créer un groupe de protection pour sauvegarder les bases de données Oracle.

Vous pouvez effectuer les tâches suivantes liées aux groupes de protection :

- Créer un groupe de protection.
- Afficher les détails de la protection.
- Sauvegardez un groupe de protection maintenant. Voir "Sauvegardez dès maintenant les charges de travail Oracle Database".
- Supprimer un groupe de protection.

Créer un groupe de protection

Regroupez les machines virtuelles et les pools de stockage que vous souhaitez protéger dans un groupe de protection.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les machines virtuelles ou les pools de stockage que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.

   Si vous souhaitez créer une politique, sélectionnez **Créer une nouvelle politique** et suivez les instructions pour créer une politique. Voir"Créer des politiques" pour plus d'informations.

10. Sélectionnez **Suivant**.
11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

Supprimer un groupe de protection

La suppression d'un groupe de protection le supprime ainsi que toutes les planifications de sauvegarde associées. Vous souhaiterez peut-être supprimer un groupe de protection s'il n'est plus nécessaire.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez le groupe de protection que vous souhaitez supprimer.
6. Sélectionnez l'icône Actions ••• > **Supprimer la protection**.
7. Consultez le message de confirmation concernant la suppression des sauvegardes associées et confirmez la suppression.

Sauvegardez les charges de travail Oracle Database à l'aide de NetApp Backup and Recovery

Utilisez NetApp Backup and Recovery pour sauvegarder les groupes de protection ou les bases de données Oracle Database à partir de systèmes ONTAP locaux vers un stockage cloud, notamment Amazon S3, NetApp StorageGRID, Microsoft Azure Blob Storage ou ONTAP S3. NetApp Backup and Recovery sauvegarde les bases de données et les données de journal dans chaque groupe de protection.

Pour sauvegarder des groupes de protection ou des bases de données uniques selon une planification, créez des stratégies qui gèrent les opérations de sauvegarde et de restauration. Voir"Créer des politiques" pour les instructions.

- Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de ressources. Voir "Créez et gérez des groupes de protection pour les charges de travail Oracle Database avec NetApp Backup and Recovery" pour plus d'informations.
- Sauvegardez un groupe de protection maintenant (créez une sauvegarde à la demande maintenant).
- Sauvegardez une base de données maintenant.

Sauvegardez maintenant les groupes de protection avec une sauvegarde à la demande

Exécutez une sauvegarde à la demande avant d'apporter des modifications au système pour garantir la protection de vos données.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Sous **Charges de travail**, sélectionnez la vignette **Oracle**.
3. Sélectionnez **Inventaire**.
4. Sélectionnez une charge de travail pour afficher les détails de protection.
5. Sélectionnez l'icône Actions ••• > **Voir les détails**.
6. Sélectionnez l'onglet **Groupes de protection**, **Magasins de données** ou **Machines virtuelles**.
7. Sélectionnez le groupe de protection que vous souhaitez sauvegarder.
8. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.

   NetApp Backup and Recovery utilise la même politique pour la sauvegarde et le groupe de protection.

9. Sélectionnez le niveau de planification.
10. Sélectionnez **Sauvegarder**.

Sauvegardez une base de données maintenant avec une sauvegarde à la demande

Vous pouvez exécuter une sauvegarde à la demande d'une seule base de données.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Sous **Charges de travail**, sélectionnez la vignette **Oracle**.
3. Sélectionnez **Inventaire**.
4. Sélectionnez une charge de travail pour afficher les détails de protection.
5. Sélectionnez l'icône Actions ••• > **Voir les détails**.
6. Sélectionnez l'onglet **Bases de données**.
7. Sélectionnez la base de données que vous souhaitez sauvegarder.
8. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.
9. Sélectionnez le niveau de planification.
10. Sélectionnez **Sauvegarder**.

Restaurer les bases de données Oracle avec NetApp Backup and Recovery

Restaurez les bases de données Oracle à partir d'instantanés, d'une sauvegarde répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage objet à l'aide de NetApp Backup and Recovery.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des bases de données à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal (instantané local)
- Restaurer à partir d'une ressource répliquée sur un stockage secondaire
- Restaurer à partir d'une sauvegarde de stockage d'objets

Restaurer ces points

Vous pouvez restaurer les données à l'emplacement d'origine ; la restauration vers un autre emplacement n'est pas disponible dans cette version d'aperçu privée.

- Restaurer à l'emplacement d'origine

Comment fonctionne la restauration des bases de données Oracle

Lorsque vous restaurez des bases de données Oracle, les événements suivants se produisent :

- Lorsque vous restaurez une base de données à partir d'un snapshot local, NetApp Backup and Recovery crée une *nouvelle* ressource à l'aide des données de la sauvegarde.
- Lorsque vous effectuez une restauration à partir d'un stockage répliqué, vous pouvez le restaurer à l'emplacement d'origine.
- Lorsque vous restaurez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données vers le stockage source ou vers un système ONTAP local et récupérer la base de données à partir de là.

À partir de la page Restaurer (également appelée Rechercher et restaurer), vous pouvez restaurer une base

de données, même si vous ne vous souvenez pas du nom exact, de l'emplacement où elle réside ou de la date à laquelle elle était en bon état pour la dernière fois. Vous pouvez rechercher la base de données à l'aide de filtres.

Restaurer une base de données Oracle

Selon vos besoins, restaurez une base de données Oracle à un moment précis, à un numéro de modification système (SCN) spécifique ou au dernier état correct. Vous pouvez également simplement restaurer la base de données à partir d'instantanés et ignorer le processus de récupération automatique. Vous souhaiterez peut-être ignorer le processus de récupération automatique si vous souhaitez effectuer la récupération manuellement. Vous pouvez rechercher la base de données en utilisant son nom ou avec des filtres spécifiques.

Rôle de console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Dans le menu NetApp Backup and Recovery , sélectionnez **Restaurer**.
3. Dans la liste déroulante à droite du champ de recherche de nom, sélectionnez **Oracle**.
4. Saisissez le nom de la base de données que vous souhaitez restaurer ou filtrez l'hôte de base de données sur lequel se trouve la base de données que vous souhaitez restaurer.

   Une liste d'instantanés correspondant à vos critères de recherche apparaît.

5. Sélectionnez le bouton **Restaurer** pour la base de données que vous souhaitez restaurer.
6. Choisissez une option de restauration :

Restaurer à un moment précis

a. Sélectionnez **Restaurer à un moment précis**.
b. Sélectionnez **Suivant**.
c. Choisissez une date dans la liste déroulante et sélectionnez **Rechercher**.

   Une liste des instantanés correspondants à la date spécifiée s'affiche.

Restaurer vers un numéro de modification système spécifique (SCN)

a. Sélectionnez **Restaurer vers un numéro de modification système spécifique (SCN)**.
b. Sélectionnez **Suivant**.
c. Saisissez le SCN à utiliser comme point de restauration et sélectionnez **Rechercher**.

   Une liste des instantanés correspondants pour le SCN spécifié s'affiche.

Restaurer la dernière sauvegarde (dernier état correct)

a. Sélectionnez **Restaurer vers la dernière sauvegarde**.
b. Sélectionnez **Suivant**.

   Les dernières sauvegardes complètes et journaux sont affichés.

Restaurer à partir d'instantanés sans récupération

a. Sélectionnez **Restaurer à partir d'instantanés sans récupération**.
b. Sélectionnez **Suivant**.

   Les instantanés correspondants sont affichés.

7. Sélectionnez un emplacement source d'instantané.
8. Sélectionnez **Suivant** pour continuer.
9. Choisissez la destination et les paramètres de restauration :

Sélection de la destination

Restaurer à l'emplacement d'origine

1. **Paramètres de destination**:
   - Choisissez de restaurer la base de données entière ou uniquement les espaces table de la base de données.
   - **Fichiers de contrôle** : Activez éventuellement cette option pour restaurer également les fichiers de contrôle de la base de données.
2. **Options de pré-restauration**:
   - Vous pouvez également activer cette option et saisir le chemin complet d'un script qui doit être exécuté avant l'opération de restauration ainsi que tous les arguments pris par le script.
   - Choisissez une valeur de délai d'expiration pour le script. Si le script ne parvient pas à s'exécuter dans ce délai, la restauration se poursuivra quand même.
3. **Options post-restauration**:
   - **Postscript** : Activez éventuellement cette option et saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.
   - **Ouvrez la base de données ou la base de données conteneur en mode LECTURE-ÉCRITURE après la récupération** : Une fois l'opération de restauration terminée, Backup and Recovery activera le mode LECTURE-ÉCRITURE pour la base de données.
4. Section **Notification** :
   - **Activer les notifications par e-mail** : sélectionnez cette option pour recevoir des notifications par e-mail concernant l'opération de restauration et indiquez le type de notifications que vous souhaitez recevoir.
5. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

Non disponible pour l'aperçu des charges de travail Oracle Database.

Monter et démonter des points de récupération de base de données Oracle avec NetApp Backup and Recovery

Vous souhaiterez peut-être monter un point de récupération de base de données Oracle si vous devez accéder à la base de données dans un état contrôlé pour effectuer des opérations de récupération.

Monter un point de restauration de base de données Oracle

Si vous configurez la politique de protection d'une base de données afin de conserver les journaux d'archive, vous pouvez monter des points de récupération pour afficher l'historique des modifications de la base de données.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez la tuile Oracle.
3. Dans le menu Sauvegarde et récupération, sélectionnez **Inventaire**.
4. Pour la charge de travail de la base de données Oracle dans la liste, sélectionnez **Afficher**.

5. Sélectionnez le menu **Bases de données**.
6. Choisissez une base de données dans la liste et sélectionnez l'icône Actions ••• > **Voir les détails de la protection**.

   Une liste de points de récupération pour cette base de données s'affiche.

7. Choisissez un point de récupération dans la liste et sélectionnez l'icône Actions ••• > **Monture**.
8. Dans la boîte de dialogue qui s'affiche, procédez comme suit :
   a. Choisissez l'hôte qui doit monter le point de récupération dans la liste.
   b. Sélectionnez l'emplacement que Backup and Recovery doit utiliser pour monter le point de récupération. Pour la version préliminaire, le montage à partir du magasin d'objets n'est pas pris en charge.

      Le chemin de montage que Backup and Recovery doit utiliser s'affiche.

9. Sélectionnez **Monter**.

   Le point de récupération est monté sur l'hôte Oracle.

Démonter un point de restauration de base de données Oracle

Démontez le point de récupération lorsque vous n'avez plus besoin d'afficher les modifications apportées à cette base de données.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez la tuile Oracle.
3. Dans le menu Sauvegarde et récupération, sélectionnez **Inventaire**.
4. Pour la charge de travail Oracle dans la liste, sélectionnez **Afficher**.
5. Sélectionnez le menu **Bases de données**.
6. Choisissez une base de données dans la liste et sélectionnez l'icône Actions ••• > **Voir les détails de la protection**.

   Une liste de points de récupération pour cette base de données s'affiche.

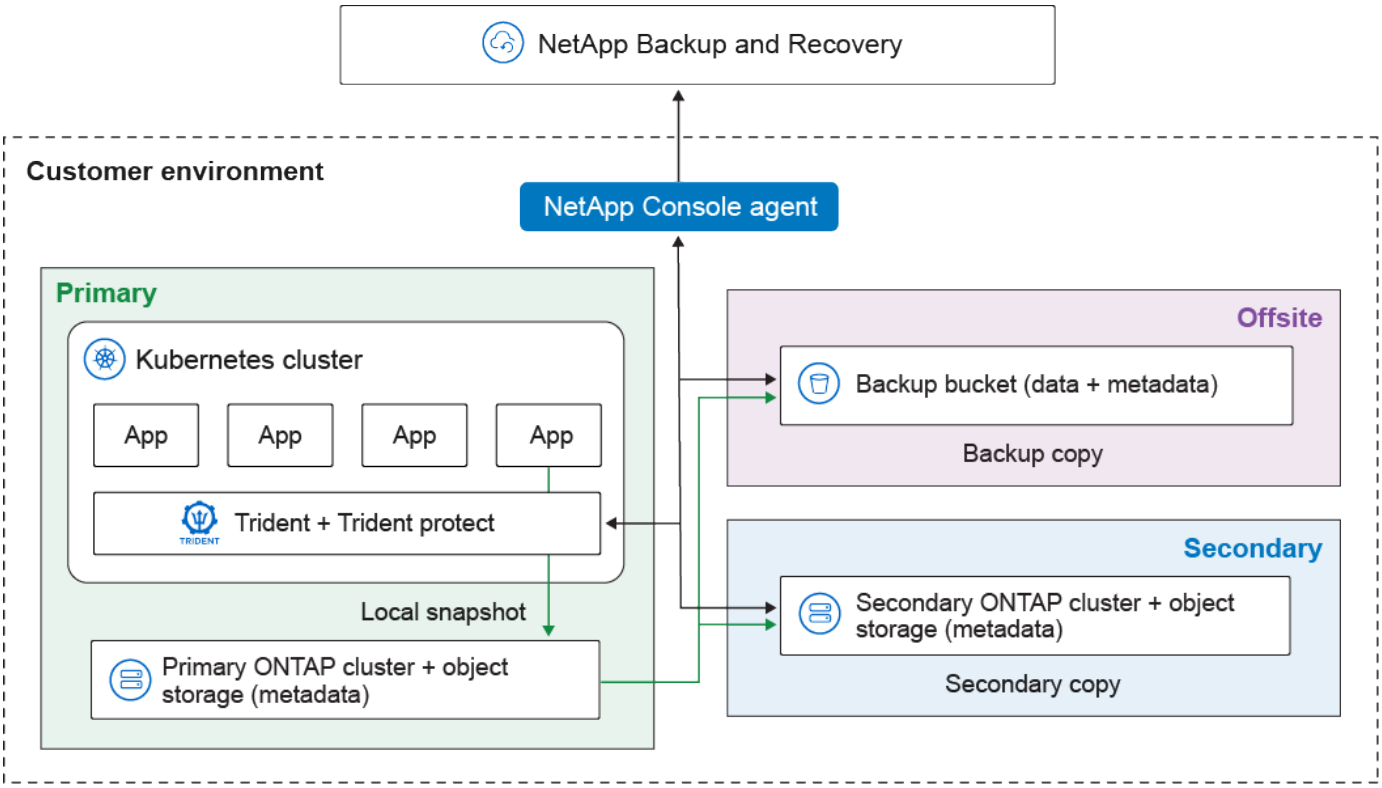
7. Choisissez un point de récupération dans la liste et sélectionnez l'icône Actions ••• > **Démonter**.
8. Confirmez l'action en sélectionnant **Démonter**.

Protéger les charges de travail Kubernetes (Aperçu)

Présentation de la gestion des charges de travail Kubernetes

La gestion des charges de travail Kubernetes dans NetApp Backup and Recovery vous permet de découvrir, de gérer et de protéger vos clusters et applications Kubernetes en un seul endroit. Vous pouvez gérer les ressources et les applications hébergées sur vos clusters Kubernetes. Vous pouvez également créer et associer des politiques de protection à vos charges de travail Kubernetes, le tout depuis une interface unique.

Le diagramme suivant montre les composants et l'architecture de base de la sauvegarde et de la restauration des charges de travail Kubernetes et comment différentes copies de vos données peuvent être stockées à différents emplacements :



NetApp Backup and Recovery offre les avantages suivants pour la gestion des charges de travail Kubernetes :

- Un plan de contrôle unique pour protéger les applications exécutées sur plusieurs clusters Kubernetes. Ces applications peuvent inclure des conteneurs ou des machines virtuelles exécutés sur vos clusters Kubernetes.
- Intégration native avec NetApp SnapMirror, permettant des capacités de déchargement du stockage pour tous les flux de travail de sauvegarde et de récupération.
- Sauvegardes incrémentielles permanentes pour les applications Kubernetes, se traduisant par des objectifs de point de récupération (RPO) et des objectifs de temps de récupération (RTO) inférieurs.

> Cette documentation est fournie à titre d'aperçu technologique. Pendant la phase d'aperçu, la fonctionnalité Kubernetes n'est pas recommandée pour les charges de travail de production. Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Vous pouvez effectuer les tâches suivantes liées à la gestion des charges de travail Kubernetes :

- "Découvrez les charges de travail Kubernetes".
- "Gérer les clusters Kubernetes".
- "Ajouter et protéger les applications Kubernetes".
- "Gérer les applications Kubernetes".
- "Restaurer les applications Kubernetes".

Découvrez les charges de travail Kubernetes dans NetApp Backup and Recovery

NetApp Backup and Recovery doit découvrir les charges de travail Kubernetes avant de les protéger.

Rôle de NetApp Console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Découvrez les charges de travail Kubernetes

Dans l'inventaire de sauvegarde et de récupération, découvrez les charges de travail Kubernetes dans votre environnement. L'ajout d'une charge de travail ajoute un cluster Kubernetes à NetApp Backup and Recovery. Vous pouvez ensuite ajouter des applications et protéger les ressources du cluster.

> Lorsque vous découvrez un cluster actuellement protégé avec Trident Protect, toutes les planifications de sauvegarde utilisées avec Trident Protect sont désactivées pendant le processus de découverte (les planifications de sauvegarde Trident Protect ne sont pas compatibles avec Backup and Recovery). Pour protéger les applications du cluster, "créer une nouvelle stratégie de protection" ou associez les applications à une stratégie existante. Vous pouvez ensuite supprimer les planifications de sauvegarde Trident Protect si nécessaire.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Si vous découvrez les charges de travail Kubernetes pour la première fois, dans NetApp Backup and Recovery, sous **Charges de travail**, sélectionnez la vignette **Kubernetes**.
   - Si vous avez déjà découvert des charges de travail Kubernetes, dans NetApp Backup and Recovery, sélectionnez **Inventaire** > **Charges de travail**, puis sélectionnez **Découvrir les ressources**.
2. Sélectionnez le type de charge de travail **Kubernetes**.
3. Saisissez un nom de cluster et choisissez un connecteur à utiliser avec le cluster.
4. Suivez les instructions de la ligne de commande qui s'affichent :
   - Créer un espace de noms Trident Protect
   - Créer un secret Kubernetes
   - Ajouter un dépôt Helm
   - Installez ou mettez à niveau Trident Protect et le connecteur Trident Protect

     Ces étapes garantissent que NetApp Backup and Recovery peut interagir avec le cluster.
5. Une fois les étapes terminées, sélectionnez **Découvrir**.

   Le cluster est ajouté à l'inventaire.
6. Sélectionnez **Afficher** dans la charge de travail Kubernetes associée pour voir la liste des applications, des clusters et des espaces de noms pour cette charge de travail.

Accéder au tableau de bord de NetApp Backup and Recovery

Suivez ces étapes pour afficher le tableau de bord de NetApp Backup and Recovery .

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.
4. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

   "Découvrez ce que le tableau de bord vous montre".

Ajouter et protéger les applications Kubernetes

Ajouter et protéger les applications Kubernetes

NetApp Backup and Recovery vous permet de découvrir facilement vos clusters Kubernetes, sans générer ni télécharger de fichiers kubeconfig. Vous pouvez connecter des clusters Kubernetes et installer le logiciel requis à l'aide de commandes simples copiées à partir de l'interface utilisateur de la NetApp Console .

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Ajouter et protéger une nouvelle application Kubernetes

La première étape de la protection des applications Kubernetes consiste à créer une application dans NetApp Backup and Recovery. Lorsque vous créez une application, vous informez la console de l'application en cours d'exécution sur le cluster Kubernetes.

Avant de commencer

Avant de pouvoir ajouter et protéger une application Kubernetes, vous devez"découvrir les charges de travail Kubernetes" .

Ajouter une application à l'aide de l'interface utilisateur web

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Sélectionnez **Créer une application**.
5. Entrez un nom pour l'application.
6. Vous pouvez également choisir l'un des champs suivants pour rechercher les ressources que vous souhaitez protéger :
   - Cluster associé
   - Espaces de noms associés
   - Types de ressources
   - Sélecteurs d'étiquettes
7. Vous pouvez également sélectionner « Ressources à portée de cluster » pour choisir les ressources à portée de cluster. Si vous les incluez, elles seront ajoutées à l'application lors de sa création.
8. Vous pouvez également sélectionner **Rechercher** pour trouver les ressources en fonction de vos critères de recherche.

   La console ne stocke pas les paramètres ou les résultats de recherche ; les paramètres sont utilisés pour rechercher dans le cluster Kubernetes sélectionné des ressources pouvant être incluses dans l'application.

9. La console affiche une liste de ressources correspondant à vos critères de recherche.
10. Si la liste contient les ressources que vous souhaitez protéger, sélectionnez **Suivant**.
11. Vous pouvez également, dans la zone **Politique**, choisir une politique de protection existante pour protéger l'application ou en créer une nouvelle. Si vous ne sélectionnez pas de politique, l'application est créée sans politique de protection. Tu peux"ajouter une politique de protection" plus tard.
12. Dans la zone **Préscripts et postscripts**, activez et configurez tous les hooks d'exécution de préscripts ou de postscripts que vous souhaitez exécuter avant ou après les opérations de sauvegarde. Pour activer les prescripts ou les postscripts, vous devez déjà en avoir créé au moins un"modèle de crochet d'exécution" .
13. Sélectionnez **Créer**.

Résultat

L'application est créée et apparaît dans la liste des applications dans l'onglet **Applications** de l'inventaire Kubernetes. La NetApp Console active la protection de l'application en fonction de vos paramètres et vous pouvez surveiller la progression dans la zone **Surveillance** de la sauvegarde et de la récupération.

Ajouter une application à l'aide d'un CR

Étapes

1. Créez le fichier CR de l'application de destination :
   a. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `my-app-name.yaml`).

b. Configurez les attributs suivants :

- **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée de l'application. Notez le nom que vous choisissez, car d'autres fichiers CR nécessaires aux opérations de protection font référence à cette valeur.
- **spec.includedNamespaces** : (*Obligatoire*) Utilisez un espace de noms et un sélecteur d'étiquette pour spécifier les espaces de noms et les ressources utilisés par l'application. L'espace de noms de l'application doit figurer dans cette liste. Le sélecteur d'étiquette est facultatif et peut être utilisé pour filtrer les ressources au sein de chaque espace de noms spécifié.
- **spec.includedClusterScopedResources**: (*Facultatif*) Utilisez cet attribut pour spécifier les ressources de portée cluster à inclure dans la définition de l'application. Cet attribut vous permet de sélectionner ces ressources en fonction de leur groupe, version, type et étiquettes.
  - **groupVersionKind**: (*Obligatoire*) Spécifie le groupe d'API, la version et le type de la ressource à portée de cluster.
  - **labelSelector** : (*Optionnel*) Filtre les ressources à portée du cluster en fonction de leurs étiquettes.

c. Configurez les annotations suivantes, si nécessaire :

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze** : (*Optionnel*) Cette annotation s'applique uniquement aux applications définies à partir de machines virtuelles, telles que dans les environnements KubeVirt, où le gel du système de fichiers intervient avant la création d'instantanés. Indiquez si cette application peut écrire sur le système de fichiers pendant la création d'un instantané. Si la valeur est true, l'application ignore le paramètre global et peut écrire sur le système de fichiers pendant la création d'un instantané. Si la valeur est false, l'application ignore le paramètre global et le système de fichiers est gelé pendant la création d'un instantané. Si cette annotation est spécifiée mais que l'application ne comporte aucune machine virtuelle dans sa définition, elle est ignorée. Si elle n'est pas spécifiée, l'application suit le "paramètre de gel global du système de fichiers".
- **protect.trident.netapp.io/protection-command** : (*Optionnel*) Utilisez cette annotation pour indiquer à Backup and Recovery de protéger ou d'arrêter de protéger l'application. Les valeurs possibles sont `protect` ou `unprotect`.
- **protect.trident.netapp.io/protection-policy-name** : (*Facultatif*) Utilisez cette annotation pour spécifier le nom de la protection des données NetApp Backup and Recovery que vous souhaitez utiliser pour protéger cette application. Cette protection des données doit déjà exister dans NetApp Backup and Recovery.

Si vous devez appliquer cette annotation après qu'une application a déjà été créée, vous pouvez utiliser la commande suivante :

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
Exemple YAML :

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (*Facultatif*) Ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

   - **resourceFilter.resourceSelectionCriteria** : (Obligatoire pour le filtrage) Utilisez `Include` ou `Exclude` pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :

     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (group, kind, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.

- **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
- **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Optionnel*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes tel que défini dans le "Documentation Kubernetes". Par exemple : `"trident.netapp.io/os=linux"`.

> ⓘ Lorsque `resourceFilter` et `labelSelector` sont utilisés, `resourceFilter` s'exécute en premier, puis `labelSelector` est appliqué aux ressources résultantes.

Par exemple :

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. Après avoir créé la CR d'application adaptée à votre environnement, appliquez la CR. Par exemple :

```
kubectl apply -f my-app-name.yaml
```

Sauvegardez dès maintenant vos applications Kubernetes à l'aide de l'interface web Backup and Recovery.

NetApp Backup and Recovery vous permet de sauvegarder manuellement des applications Kubernetes via l'interface web.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp

Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Sauvegardez une application Kubernetes dès maintenant à l'aide de l'interface web

Créez manuellement une sauvegarde d'une application Kubernetes pour établir une base de référence pour les futures sauvegardes et instantanés, ou pour garantir la protection des données les plus récentes.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez sauvegarder et sélectionnez le menu Actions associé.
5. Sélectionnez **Sauvegarder maintenant**.
6. Assurez-vous que le nom d'application correct est sélectionné.
7. Sélectionnez **Sauvegarder**.

Résultat

La console crée une sauvegarde de l'application et affiche la progression dans la zone **Surveillance** de Sauvegarde et récupération. La sauvegarde est créée en fonction de la politique de protection associée à l'application.

Sauvegardez dès maintenant vos applications Kubernetes à l'aide de ressources personnalisées dans NetApp Backup and Recovery

NetApp Backup and Recovery vous permet de sauvegarder manuellement des applications Kubernetes à l'aide de ressources personnalisées (CR).

Sauvegardez une application Kubernetes dès maintenant à l'aide de ressources personnalisées

Créez manuellement une sauvegarde d'une application Kubernetes pour établir une base de référence pour les futures sauvegardes et instantanés, ou pour garantir la protection des données les plus récentes.

> Les ressources à portée de cluster sont incluses dans une sauvegarde, un instantané ou un clone si elles sont explicitement référencées dans la définition de l'application ou si elles ont des références à l'un des espaces de noms de l'application.

Avant de commencer

Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de sauvegarde s3 de longue durée. Si le jeton expire pendant l'opération de sauvegarde, l'opération peut échouer.

- Consultez la "Documentation de l'API AWS" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Consultez la "Documentation AWS IAM" pour plus d'informations sur les identifiants relatifs aux ressources AWS.

Créer un instantané local à l'aide d'une ressource personnalisée

Pour créer un instantané de votre application Kubernetes et le stocker localement, utilisez la ressource personnalisée Snapshot avec des attributs spécifiques.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `local-snapshot-cr.yaml`.
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef** : Le nom Kubernetes de l'application à capturer.
   - **spec.appVaultRef** : (*Obligatoire*) Le nom de l'AppVault où le contenu de l'instantané (métadonnées) doit être stocké.
   - **spec.reclaimPolicy** : (Optionnel) Définit ce qui arrive à l'AppArchive d'un instantané lorsque le CR de l'instantané est supprimé. Cela signifie que même lorsqu'il est défini sur `Retain`, l'instantané sera supprimé. Options valides :
     - `Retain` (défaut)
     - `Delete`

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: Snapshot
     metadata:
       namespace: my-app-namespace
       name: local-snapshot-cr
     spec:
       applicationRef: my-application
       appVaultRef: appvault-name
       reclaimPolicy: Retain
     ```
3. Après avoir rempli le fichier `local-snapshot-cr.yaml` avec les valeurs correctes, appliquez le CR :

   ```
   kubectl apply -f local-snapshot-cr.yaml
   ```

Sauvegardez une application sur un stockage d'objets à l'aide d'une ressource personnalisée

Créez un CR de sauvegarde avec des attributs spécifiques pour sauvegarder votre application vers un magasin d'objets.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `object-store-backup-cr.yaml`.
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.

- **spec.applicationRef**: (*Obligatoire*) Le nom Kubernetes de l'application à sauvegarder.
- **spec.appVaultRef** : (*Obligatoire, incompatible avec spec.appVaultTargetsRef*) Si vous utilisez le même compartiment pour stocker l'instantané et la sauvegarde, il s'agit du nom du AppVault où le contenu de la sauvegarde doit être stocké.
- **spec.appVaultTargetsRef** : (*Obligatoire, incompatible avec spec.appVaultRef*) Si vous utilisez des compartiments différents pour stocker l'instantané et la sauvegarde, il s'agit du nom du AppVault où le contenu de la sauvegarde doit être stocké.
- **spec.dataMover** : (*Facultatif*) Une chaîne indiquant l'outil de sauvegarde à utiliser pour l'opération de sauvegarde. La valeur est sensible à la casse et doit être `CBS`.
- **spec.reclaimPolicy** : (*Facultatif*) Définit ce qui se passe pour le contenu de la sauvegarde (métadonnées/données du volume) lorsque la Backup CR est supprimée. Valeurs possibles :
  - `Delete`
  - `Retain` (défaut)
- **spec.cleanupSnapshot** : (Obligatoire) Garantit que l'instantané temporaire créé par le Backup CR n'est pas supprimé une fois l'opération de sauvegarde terminée. Valeur recommandée `false`.

  Exemple YAML lors de l'utilisation du même compartiment pour stocker l'instantané et la sauvegarde :

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

  Exemple YAML lors de l'utilisation de compartiments différents pour stocker l'instantané et la sauvegarde :

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. Après avoir rempli le `object-store-backup-cr.yaml` fichier avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f object-store-backup-cr.yaml
```

Créez une sauvegarde fanout 3-2-1 à l'aide d'une ressource personnalisée

La sauvegarde utilisant une architecture de distribution 3-2-1 copie une sauvegarde vers un stockage secondaire ainsi que vers un magasin d'objets. Pour créer une sauvegarde de distribution 3-2-1, créez un CR Backup avec des attributs spécifiques.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `3-2-1-fanout-backup-cr.yaml`.
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef**: (*Obligatoire*) Le nom Kubernetes de l'application à sauvegarder.
   - **spec.appVaultTargetsRef** : (*Obligatoire*) Le nom du AppVault où le contenu de la sauvegarde doit être stocké.
   - **spec.dataMover** : (*Facultatif*) Une chaîne indiquant l'outil de sauvegarde à utiliser pour l'opération de sauvegarde. La valeur est sensible à la casse et doit être `CBS`.
   - **spec.reclaimPolicy** : (*Facultatif*) Définit ce qui se passe pour le contenu de la sauvegarde (métadonnées/données du volume) lorsque la Backup CR est supprimée. Valeurs possibles :
     - `Delete`
     - `Retain` (défaut)
   - **spec.cleanupSnapshot** : (Obligatoire) Garantit que l'instantané temporaire créé par le Backup CR n'est pas supprimé une fois l'opération de sauvegarde terminée. Valeur recommandée `false`.
   - **spec.replicateSnapshot** : (*Obligatoire*) Indique à NetApp Backup and Recovery de répliquer l'instantané vers un stockage secondaire. Valeur requise `true`.
   - **spec.replicateSnapshotReclaimPolicy** : (*Optionnel*) Définit ce qui se passe pour l'instantané répliqué

lorsqu'il est supprimé. Valeurs possibles :

- `Delete`
- `Retain` (défaut)

Exemple YAML :

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. Après avoir rempli le fichier `3-2-1-fanout-backup-cr.yaml` avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

Annotations de sauvegarde prises en charge

Le tableau suivant décrit les annotations que vous pouvez utiliser lors de la création d'un CR de sauvegarde.

Annotation	Type	Description	valeur par défaut
protect.trident.netapp.io/full-backup	chaîne	Indique si une sauvegarde doit être non incrémentielle. Définissez sur `true` pour créer une sauvegarde non incrémentielle. Il est bonne pratique d'effectuer périodiquement une sauvegarde complète, puis des sauvegardes incrémentielles entre les sauvegardes complètes afin de minimiser le risque associé aux restaurations.	"false"
protect.trident.netapp.io/snapshot-completion-timeout	chaîne	Le temps maximal autorisé pour que l'opération globale de capture d'instantané soit terminée.	"60m"
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	chaîne	Le temps maximal autorisé pour que les instantanés de volume atteignent l'état prêt à l'emploi.	"30m"

Annotation	Type	Description	valeur par défaut
protect.trident.netapp.io/volume-snapshots-created-timeout	chaîne	Durée maximale autorisée pour la création d'instantanés de volume.	"5m"
protect.trident.netapp.io/pvc-bind-timeout-sec	chaîne	Temps maximal (en secondes) à attendre pour que les nouveaux PersistentVolumeClaims (PVCs) atteignent la `Bound` phase avant que l'opération échoue.	"1200" (20 minutes)

Restaurer les applications Kubernetes

Restaurez les applications Kubernetes à l'aide de l'interface utilisateur Web

NetApp Backup and Recovery vous permet de restaurer les applications que vous avez protégées avec une politique de protection. Pour restaurer une application, celle-ci doit disposer d'au moins un point de restauration. Un point de restauration est constitué soit de l'instantané local, soit de la sauvegarde dans le magasin d'objets (ou des deux). Vous pouvez restaurer une application à partir de l'archive locale, secondaire ou du magasin d'objets.

Avant de commencer

Si vous restaurez une application qui a été sauvegardée à l'aide de Trident Protect, assurez-vous que Trident Protect est installé sur les clusters source et de destination.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans le menu NetApp Backup and Recovery, sélectionnez **Restaurer**.
2. Choisissez une application Kubernetes dans la liste, et sélectionnez **Afficher et restaurer** pour cette application.

   La liste des points de restauration apparaît.

3. Sélectionnez le bouton **Restore** pour le point de restauration que vous souhaitez utiliser.

Paramètres généraux

1. Choisissez l'emplacement source à partir duquel effectuer la restauration.
2. Choisissez le cluster de destination dans la liste **Cluster**.

   La restauration d'un instantané local créé par Trident Protect vers un cluster différent n'est pas prise en charge pour le moment.

3. Choisissez de restaurer vers les espaces de noms d'origine ou vers de nouveaux espaces de noms.
4. Si vous avez choisi de restaurer dans de nouveaux espaces de noms, saisissez le ou les espaces de noms de destination à utiliser.

5. Sélectionnez **Suivant**.

Sélection des ressources

1. Choisissez si vous souhaitez restaurer toutes les ressources associées à l'application ou utiliser un filtre pour sélectionner des ressources spécifiques à restaurer :

Restaurer toutes les ressources

1. Sélectionnez **Restaurer toutes les ressources**.
2. Sélectionnez **Suivant**.

Restaurer des ressources spécifiques

1. Sélectionnez **Ressources sélectives**.
2. Choisissez le comportement du filtre de ressources. Si vous choisissez **Inclure**, les ressources que vous sélectionnez sont restaurées. Si vous choisissez **Exclure**, les ressources que vous sélectionnez ne sont pas restaurées.
3. Sélectionnez **Ajouter des règles** pour ajouter des règles qui définissent des filtres pour la sélection des ressources. Vous avez besoin d'au moins une règle pour filtrer les ressources.

   Chaque règle peut filtrer selon des critères tels que l'espace de noms de la ressource, les étiquettes, le groupe, la version et le type.
4. Sélectionnez **Enregistrer** pour enregistrer chaque règle.
5. Lorsque vous avez ajouté toutes les règles dont vous avez besoin, sélectionnez **Rechercher** pour voir les ressources disponibles dans l'archive de sauvegarde qui correspondent à vos critères de filtre.

   Les ressources affichées sont les ressources qui existent actuellement sur le cluster.
6. Lorsque vous êtes satisfait des résultats, sélectionnez **Suivant**.

Paramètres de destination

1. Développez la section **Paramètres de destination** et choisissez de restaurer soit vers la classe de stockage par défaut, une autre classe de stockage, ou, si vous restaurez vers un autre cluster, de mapper les classes de stockage au cluster de destination.
2. Si vous avez choisi de restaurer vers une classe de stockage différente, sélectionnez une classe de stockage de destination correspondant à chaque classe de stockage source.
3. Optionnellement, si vous restaurez une sauvegarde ou un instantané créé avec Trident Protect, consultez les détails du AppVault utilisé comme compartiment de stockage pour l'opération de restauration. S'il y a un changement dans votre environnement ou dans le statut du AppVault, sélectionnez **Sync App Vault** pour actualiser les détails.

   Si vous devez créer un AppVault sur un cluster Kubernetes pour faciliter la restauration d'une sauvegarde ou d'un instantané créé à l'aide de Trident Protect, reportez-vous à "Utilisez les objets Trident Protect AppVault pour gérer les compartiments".
4. Vous pouvez également développer la section **Scripts de restauration** et activer l'option **Postscript** pour

choisir un modèle de hook d'exécution qui s'exécutera une fois l'opération de restauration terminée. Si nécessaire, saisissez les arguments requis par le script et ajoutez des sélecteurs d'étiquettes pour filtrer les ressources en fonction des étiquettes de ressource.

5. Sélectionnez **Restaurer**.

Restaurez des applications Kubernetes à l'aide d'une ressource personnalisée

Vous pouvez utiliser des ressources personnalisées pour restaurer vos applications à partir d'un instantané ou d'une sauvegarde. La restauration à partir d'un instantané existant sera plus rapide lors de la restauration de l'application sur le même cluster.

- Lors de la restauration d'une application, tous les points d'exécution configurés pour l'application sont restaurés avec l'application. Si un point d'exécution post-restauration est présent, il s'exécute automatiquement dans le cadre de l'opération de restauration.
- La restauration à partir d'une sauvegarde vers un espace de noms différent ou vers l'espace de noms d'origine est prise en charge pour les volumes qtree. Cependant, la restauration à partir d'un instantané vers un espace de noms différent ou vers l'espace de noms d'origine n'est pas prise en charge pour les volumes qtree.
- Vous pouvez utiliser les paramètres avancés pour personnaliser les opérations de restauration. Pour en savoir plus, consultez "Utilisez les paramètres avancés de restauration des ressources personnalisées".

Restaurer une sauvegarde dans un espace de noms différent

Lorsque vous restaurez une sauvegarde dans un espace de noms différent à l'aide d'un BackupRestore CR, Backup and Recovery restaure l'application dans un nouvel espace de noms et crée un CR d'application pour l'application restaurée. Pour protéger l'application restaurée, créez des sauvegardes ou des instantanés à la demande, ou établissez une planification de protection.

- La restauration d'une sauvegarde dans un espace de noms différent contenant des ressources existantes ne modifiera pas les ressources portant le même nom que celles de la sauvegarde. Pour restaurer toutes les ressources de la sauvegarde, supprimez et recréez l'espace de noms cible ou restaurez la sauvegarde dans un nouvel espace de noms.
- Lors de l'utilisation d'une CR pour restaurer dans un nouvel espace de noms, vous devez créer manuellement l'espace de noms de destination avant d'appliquer la CR. NetApp Backup and Recovery crée automatiquement les espaces de noms uniquement lors de l'utilisation de la CLI.

Avant de commencer

Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de restauration s3 de longue durée. Si le jeton expire pendant l'opération de restauration, l'opération peut échouer.

- Consultez la "Documentation de l'API AWS" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Consultez la "Documentation AWS IAM" pour plus d'informations sur les identifiants relatifs aux ressources AWS.

Lorsque vous restaurez des sauvegardes en utilisant Kopia comme outil de déplacement de données, vous pouvez éventuellement spécifier des annotations dans le CR pour contrôler le comportement du stockage temporaire utilisé par Kopia. Consultez la "Documentation Kopia" pour plus d'informations sur les options que vous pouvez configurer.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `trident-protect-backup-restore-cr.yaml`.
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appArchivePath** : Le chemin à l'intérieur de AppVault où le contenu de la sauvegarde est stocké. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef** : (*Obligatoire*) Le nom du AppVault où les contenus de sauvegarde sont stockés.
   - **spec.namespaceMapping** : La correspondance de l'espace de noms source de l'opération de restauration avec l'espace de noms de destination. Remplacez `my-source-namespace` et `my-destination-namespace` par les informations de votre environnement.

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: my-cr-name
       namespace: my-destination-namespace
     spec:
       appArchivePath: my-backup-path
       appVaultRef: appvault-name
       namespaceMapping: [{"source": "my-source-namespace", "destination":
     "my-destination-namespace"}]
     ```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

   Trident Protect sélectionne automatiquement certaines ressources en fonction de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de type revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Obligatoire pour le filtrage) Utilisez `Include` ou `Exclude` pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez

plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (group, kind, version) correspondent selon une opération ET.

- **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
- **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
- **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
- **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Optionnel*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes tel que défini dans le "Documentation Kubernetes". Par exemple : `"trident.netapp.io/os=linux"`.

  Par exemple :

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le fichier `trident-protect-backup-restore-cr.yaml` avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Restaurer une sauvegarde dans l'espace de noms d'origine

Vous pouvez restaurer une sauvegarde dans l'espace de noms d'origine à tout moment.

Avant de commencer

Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de restauration s3 de longue durée. Si le jeton expire pendant l'opération de restauration, l'opération peut échouer.

- Consultez la "Documentation de l'API AWS" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Consultez la "Documentation AWS IAM" pour plus d'informations sur les identifiants relatifs aux ressources AWS.

> Lorsque vous restaurez des sauvegardes en utilisant Kopia comme outil de déplacement de données, vous pouvez éventuellement spécifier des annotations dans le CR pour contrôler le comportement du stockage temporaire utilisé par Kopia. Consultez la "Documentation Kopia" pour plus d'informations sur les options que vous pouvez configurer.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `trident-protect-backup-ipr-cr.yaml`.
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appArchivePath** : Le chemin à l'intérieur de AppVault où le contenu de la sauvegarde est stocké. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef** : (*Obligatoire*) Le nom du AppVault où les contenus de sauvegarde sont stockés.

     Par exemple :

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

> Trident Protect sélectionne automatiquement certaines ressources en fonction de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de type revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Obligatoire pour le filtrage) Utilisez `Include` ou `Exclude` pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :

- **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (group, kind, version) correspondent selon une opération ET.
  - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
  - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
  - **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
  - **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
  - **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
  - **resourceMatchers[].labelSelectors** : (*Optionnel*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes tel que défini dans le "Documentation Kubernetes". Par exemple : `"trident.netapp.io/os=linux"`.

    Par exemple :

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le fichier `trident-protect-backup-ipr-cr.yaml` avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Restaurer une sauvegarde sur un cluster différent

Vous pouvez restaurer une sauvegarde sur un cluster différent en cas de problème avec le cluster d'origine.

- Lorsque vous restaurez des sauvegardes en utilisant Kopia comme outil de déplacement de données, vous pouvez éventuellement spécifier des annotations dans le CR pour contrôler le comportement du stockage temporaire utilisé par Kopia. Consultez la "Documentation Kopia" pour plus d'informations sur les options que vous pouvez configurer.
- Lorsque vous utilisez un CR pour restaurer dans un nouvel espace de noms, vous devez créer manuellement l'espace de noms de destination avant d'appliquer le CR.

Avant de commencer

Assurez-vous que les conditions préalables suivantes sont remplies :

- Le cluster de destination a Trident Protect installé.
- Le cluster de destination a accès au chemin du compartiment du même AppVault que le cluster source, où la sauvegarde est stockée.
- Assurez-vous que la durée de validité du jeton de session AWS soit suffisante pour toute opération de restauration de longue durée. Si le jeton expire pendant l'opération de restauration, l'opération peut échouer.
  - Consultez la "Documentation de l'API AWS" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
  - Consultez la "Documentation AWS" pour plus d'informations sur les identifiants relatifs aux ressources AWS.

Étapes

1. Vérifiez la disponibilité de la AppVault CR sur le cluster de destination à l'aide du plugin CLI Trident Protect :

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

   Assurez-vous que l'espace de noms destiné à la restauration de l'application existe sur le cluster de destination.

2. Consultez le contenu de la sauvegarde disponible de AppVault depuis le cluster de destination :

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

   L'exécution de cette commande affiche les sauvegardes disponibles dans le AppVault, y compris leurs clusters d'origine, les noms des applications correspondantes, les horodatages et les chemins d'accès aux archives.

   Exemple de sortie :

```
+------------+----------+--------+----------------
+-------------------------+------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |        TIMESTAMP
|    PATH     |
+------------+----------+--------+----------------
+-------------------------+------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+------------+----------+--------+----------------
+-------------------------+------------+
```

3. Restaurez l'application sur le cluster de destination en utilisant le nom AppVault et le chemin d'accès à l'archive :
4. Créez le fichier de ressource personnalisée (CR) et nommez-le `trident-protect-backup-restore-cr.yaml`.
5. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appVaultRef** : (*Obligatoire*) Le nom du AppVault où les contenus de sauvegarde sont stockés.
   - **spec.appArchivePath** : Le chemin à l'intérieur de AppVault où le contenu de la sauvegarde est stocké. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

     Si le BackupRestore CR n'est pas disponible, vous pouvez utiliser la commande mentionnée à l'étape 2 pour afficher le contenu de la sauvegarde.

   - **spec.namespaceMapping** : La correspondance de l'espace de noms source de l'opération de restauration avec l'espace de noms de destination. Remplacez `my-source-namespace` et `my-destination-namespace` par les informations de votre environnement.

     Par exemple :

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. Après avoir rempli le fichier `trident-protect-backup-restore-cr.yaml` avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Restaurer un instantané dans un espace de noms différent

Vous pouvez restaurer des données à partir d'un instantané à l'aide d'un fichier de ressource personnalisé (CR) soit vers un autre espace de noms, soit vers l'espace de noms source d'origine. Lorsque vous restaurez un instantané vers un autre espace de noms à l'aide d'un SnapshotRestore CR, Backup and Recovery restaure l'application dans un nouvel espace de noms et crée un CR d'application pour l'application restaurée. Pour protéger l'application restaurée, créez des sauvegardes ou des instantanés à la demande, ou définissez une planification de protection.

- SnapshotRestore prend en charge l' `spec.storageClassMapping`attribut, mais uniquement lorsque les classes de stockage source et de destination utilisent le même système de stockage. Si vous tentez de restaurer vers une classe de stockage `StorageClass` qui utilise un système de stockage différent, l'opération de restauration échouera.
- Lorsque vous utilisez un CR pour restaurer dans un nouvel espace de noms, vous devez créer manuellement l'espace de noms de destination avant d'appliquer le CR.

Avant de commencer

Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de restauration s3 de longue durée. Si le jeton expire pendant l'opération de restauration, l'opération peut échouer.

- Consultez la "Documentation de l'API AWS" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Consultez la "Documentation AWS IAM" pour plus d'informations sur les identifiants relatifs aux ressources AWS.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `trident-protect-snapshot-restore-cr.yaml`.

2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appVaultRef** : (*Obligatoire*) Le nom du AppVault où le contenu de l'instantané est stocké.
   - **spec.appArchivePath** : Le chemin à l'intérieur de AppVault où les contenus de l'instantané sont stockés. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.namespaceMapping** : La correspondance de l'espace de noms source de l'opération de restauration avec l'espace de noms de destination. Remplacez `my-source-namespace` et `my-destination-namespace` par les informations de votre environnement.

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
       namespaceMapping: [{"source": "my-source-namespace", "destination":
     "my-destination-namespace"}]
     ```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

   > Trident Protect sélectionne automatiquement certaines ressources en fonction de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de type revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Obligatoire pour le filtrage) Utilisez `Include` ou `Exclude` pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (group, kind, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
       - **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
       - **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ Kubernetes metadata.name de la ressource à filtrer.

- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Optionnel*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes tel que défini dans le "Documentation Kubernetes". Par exemple : `"trident.netapp.io/os=linux"`.

  Par exemple :

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le fichier `trident-protect-snapshot-restore-cr.yaml` avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Restaurez un instantané dans l'espace de noms d'origine

Vous pouvez restaurer un instantané dans l'espace de noms d'origine à tout moment.

Avant de commencer

Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de restauration s3 de longue durée. Si le jeton expire pendant l'opération de restauration, l'opération peut échouer.

- Consultez la "Documentation de l'API AWS" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Consultez la "Documentation AWS IAM" pour plus d'informations sur les identifiants relatifs aux ressources AWS.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `trident-protect-snapshot-ipr-`

`cr.yaml`.

2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name**: (*Obligatoire*) Le nom de cette ressource personnalisée; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appVaultRef** : (*Obligatoire*) Le nom du AppVault où le contenu de l'instantané est stocké.
   - **spec.appArchivePath** : Le chemin à l'intérieur de AppVault où les contenus de l'instantané sont stockés. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

> Trident Protect sélectionne automatiquement certaines ressources en fonction de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de type revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Obligatoire pour le filtrage) Utilisez `Include` ou `Exclude` pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (group, kind, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
       - **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
       - **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
       - **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
       - **resourceMatchers[].labelSelectors** : (*Optionnel*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes tel que défini dans le "Documentation Kubernetes". Par exemple : `"trident.netapp.io/os=linux"`.

Par exemple :

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le fichier `trident-protect-snapshot-ipr-cr.yaml` avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Utilisez les paramètres avancés de restauration des ressources personnalisées

Vous pouvez personnaliser les opérations de restauration à l'aide de paramètres avancés tels que les annotations, les paramètres de namespace et les options de stockage pour répondre à vos besoins spécifiques.

Annotations et étiquettes d'espace de noms lors des opérations de restauration et de basculement

Lors des opérations de restauration et de basculement, les étiquettes et annotations de l'espace de noms de destination sont mises à jour pour correspondre aux étiquettes et annotations de l'espace de noms source. Les étiquettes ou annotations de l'espace de noms source qui n'existent pas dans l'espace de noms de destination sont ajoutées, et toutes les étiquettes ou annotations déjà présentes sont remplacées pour correspondre à la valeur de l'espace de noms source. Les étiquettes ou annotations qui existent uniquement dans l'espace de noms de destination restent inchangées.

Si vous utilisez Red Hat OpenShift, il est important de noter le rôle crucial des annotations d'espace de noms dans les environnements OpenShift. Les annotations d'espace de noms garantissent que les pods restaurés respectent les permissions et les configurations de sécurité appropriées définies par les contraintes de contexte de sécurité (OpenShift SCC) et peuvent accéder aux volumes sans problème de permissions. Pour plus d'informations, consultez la "Documentation des contraintes de contexte de sécurité OpenShift".

Vous pouvez empêcher l'écrasement de certaines annotations dans l'espace de noms de destination en définissant la variable d'environnement Kubernetes `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` avant d'effectuer l'opération de restauration ou de basculement. Par exemple :

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

Lors d'une opération de restauration ou de basculement, les annotations et étiquettes d'espace de noms spécifiées dans `restoreSkipNamespaceAnnotations` et `restoreSkipNamespaceLabels` sont exclues de l'opération de restauration ou de basculement. Assurez-vous que ces paramètres sont configurés lors de l'installation initiale de Helm. Pour en savoir plus, consultez "Configurer des paramètres supplémentaires du chart Helm Trident Protect".

Si vous avez installé l'application source avec Helm avec le `--create-namespace` flag, un traitement spécial est appliqué à la clé de label `name`. Lors du processus de restauration ou de basculement, Trident Protect copie ce label dans l'espace de noms de destination, mais met à jour la valeur avec celle de l'espace de noms de destination si la valeur provenant de la source correspond à l'espace de noms source. Si cette valeur ne correspond pas à l'espace de noms source, elle est copiée dans l'espace de noms de destination sans modification.

Exemple

L'exemple suivant présente un espace de noms source et un espace de noms de destination, chacun possédant des annotations et des étiquettes différentes. Vous pouvez voir l'état de l'espace de noms de destination avant et après l'opération, et comment les annotations et les étiquettes sont combinées ou écrasées dans l'espace de noms de destination.

Avant l'opération de restauration ou de basculement

Le tableau suivant illustre l'état des espaces de noms source et de destination de l'exemple avant l'opération de restauration ou de basculement :

Espace de noms	Annotations	Étiquettes
Espace de noms ns-1 (source)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• environment=production • conformité=hipaa • name=ns-1
Espace de noms ns-2 (destination)	• annotation.one/key: "true" • annotation.three/key: "false"	• rôle=base de données

Après l'opération de restauration

Le tableau suivant illustre l'état de l'espace de noms de destination après l'opération de restauration ou de basculement. Certaines clés ont été ajoutées, d'autres ont été écrasées, et l' `name`étiquette a été mise à jour pour correspondre à l'espace de noms de destination :

Espace de noms	Annotations	Étiquettes
Espace de noms ns-2 (destination)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotation.three/key: "false"	• name=ns-2 • conformité=hipaa • environment=production • rôle=base de données

Champs pris en charge

Cette section décrit les champs supplémentaires disponibles pour les opérations de restauration.

Correspondance des classes de stockage

L' `spec.storageClassMapping`attribut définit une correspondance entre une classe de stockage présente dans l'application source et une nouvelle classe de stockage sur le cluster cible. Vous pouvez l'utiliser lors de la migration d'applications entre des clusters avec des classes de stockage différentes ou lors du changement de système de stockage pour les opérations BackupRestore.

Exemple :

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Annotations prises en charge

Cette section répertorie les annotations prises en charge pour configurer différents comportements du système. Si une annotation n'est pas explicitement définie par l'utilisateur, le système utilisera la valeur par défaut.

Annotation	Type	Description	valeur par défaut
protect.trident.netapp.io/data-mover-timeout-sec	chaîne	Le temps maximal (en secondes) autorisé pour que l'opération de déplacement de données soit bloquée.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	chaîne	La limite de taille maximale (en mégaoctets) pour le cache de contenu Kopia.	"1000"

Annotation	Type	Description	valeur par défaut
protect.trident.netapp.io/pvc-bind-timeout-sec	chaîne	Temps maximal (en secondes) d'attente pour que tout nouveau PersistentVolumeClaims (PVC) atteigne la phase `Bound` avant que l'opération n'échoue. S'applique à tous les types de CR de restauration (BackupRestore, BackupInplaceRestore, SnapshotRestore, SnapshotInplaceRestore). Utilisez une valeur plus élevée si votre backend de stockage ou votre cluster nécessite souvent plus de temps.	"1200" (20 minutes)

Gérer les clusters Kubernetes

NetApp Backup and Recovery vous permet de découvrir et de gérer vos clusters Kubernetes afin de protéger les ressources hébergées par les clusters.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Pour découvrir les clusters Kubernetes, reportez-vous à"Découvrez les charges de travail Kubernetes" .

Modifier les informations du cluster Kubernetes

Vous pouvez modifier un cluster si vous devez changer son nom.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire** > **Clusters**.
2. Dans la liste des clusters, choisissez un cluster que vous souhaitez modifier et sélectionnez le menu Actions associé.
3. Sélectionnez **Modifier le cluster**.
4. Apportez les modifications nécessaires au nom du cluster. Ce nom doit correspondre à celui utilisé avec la commande Helm lors de la découverte.
5. Sélectionnez **Terminé**.

Supprimer un cluster Kubernetes

Pour arrêter la protection d'un cluster Kubernetes, désactivez la protection et supprimez les applications associées, puis supprimez le cluster de NetApp Backup and Recovery. NetApp Backup and Recovery ne supprime pas le cluster ni ses ressources ; il supprime uniquement le cluster de l'inventaire de la NetApp Console .

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire** > **Clusters**.
2. Dans la liste des clusters, choisissez un cluster que vous souhaitez modifier et sélectionnez le menu Actions associé.
3. Sélectionnez **Supprimer le cluster**.

4. Vérifiez les informations dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.

Gérer les applications Kubernetes

NetApp Backup and Recovery vous permet de déprotéger et de supprimer vos applications Kubernetes et les ressources associées.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Déprotéger une application Kubernetes

Vous pouvez déprotéger une application si vous ne souhaitez plus la protéger. Lorsque vous déprotégez une application, NetApp Backup and Recovery cesse de protéger l'application mais conserve toutes les sauvegardes et tous les snapshots associés.

> Vous ne pouvez pas déprotéger une application tant que des opérations de protection sont en cours. Attendez la fin de l'opération ou, à titre de solution de contournement, supprimer le point de restauration l'opération de protection en cours utilise. Vous pouvez alors déprotéger l'application.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez déprotéger et sélectionnez le menu Actions associé.
5. Sélectionnez **Déprotéger**.
6. Lisez l'avis et, lorsque vous êtes prêt, sélectionnez **Déprotéger**.

Supprimer une application Kubernetes

Supprimez une application dont vous n'avez plus besoin. NetApp Backup and Recovery arrête la protection et supprime toutes les sauvegardes et tous les instantanés des applications supprimées.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez supprimer et sélectionnez le menu Actions associé.
5. Sélectionnez **Supprimer**.
6. Activez **Supprimer les instantanés et les sauvegardes** pour supprimer tous les instantanés et sauvegardes de l'application.

Vous ne pourrez plus restaurer l'application à l'aide de ces instantanés et sauvegardes.

7. Confirmez l'action et sélectionnez **Supprimer**.

Supprimer un point de restauration pour une application Kubernetes

Vous devrez peut-être supprimer un point de restauration pour une application si vous devez la déprotéger et que des opérations de protection sont en cours.

Étapes

1. Dans le menu NetApp Backup and Recovery, sélectionnez **Restaurer**.
2. Choisissez une application Kubernetes dans la liste, et sélectionnez **Afficher et restaurer** pour cette application.

   La liste des points de restauration apparaît.

3. Choisissez le point de récupération que vous souhaitez supprimer et sélectionnez l'icône Actions ••• > **Supprimer le point de récupération** pour le supprimer.

Gérer les modèles de hook d'exécution de NetApp Backup and Recovery pour les charges de travail Kubernetes

Un hook d'exécution est une action personnalisée qui s'exécute avec une opération de protection des données dans une application Kubernetes gérée. Par exemple, créez des instantanés cohérents avec l'application en utilisant un hook d'exécution pour suspendre les transactions de base de données avant un instantané et les reprendre après. Lorsque vous créez un modèle de hook d'exécution, spécifiez le type de hook, le script à exécuter et les filtres pour les conteneurs cibles. Utilisez le modèle pour lier les hooks d'exécution à vos applications.

NetApp Backup and Recovery gèle et dégèle les systèmes de fichiers pour des applications comme KubeVirt lors de la protection des données. Vous pouvez désactiver ce comportement globalement ou pour des applications spécifiques en utilisant la documentation Trident Protect :

- Pour désactiver ce comportement pour toutes les applications, reportez-vous à "Protection des données avec les machines virtuelles KubeVirt" .
- Pour désactiver ce comportement pour une application spécifique, reportez-vous à "Définir une application" .

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Types de hooks d'exécution

NetApp Backup and Recovery prend en charge les types de hooks d'exécution suivants, en fonction du moment où ils peuvent être exécutés :

- Pré-instantané

- Post-instantané
- Pré-sauvegarde
- Post-sauvegarde
- Post-restauration

Ordre d'exécution

Lorsqu'une opération de protection des données est exécutée, les événements de hook d'exécution se produisent dans l'ordre suivant :

1. Tous les hooks d'exécution de pré-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer plusieurs hooks de pré-opération personnalisés, mais leur ordre d'exécution n'est ni garanti ni configurable.
2. Des blocages du système de fichiers se produisent, le cas échéant.
3. L'opération de protection des données est effectuée.
4. Les systèmes de fichiers gelés sont dégelés, le cas échéant.
5. NetApp Backup and Recovery exécute tous les hooks d'exécution de pré-opération personnalisés applicables sur les conteneurs appropriés. Vous pouvez créer plusieurs hooks post-opération personnalisés, mais leur ordre d'exécution n'est ni garanti ni configurable.

Si vous créez plusieurs hooks du même type, leur ordre d'exécution n'est pas garanti. Les crochets de différents types fonctionnent toujours dans l'ordre spécifié. Par exemple, voici l'ordre d'exécution d'une configuration qui possède tous les différents types de hooks :

1. Hooks pré-instantanés exécutés
2. Hooks post-instantanés exécutés
3. Hooks de pré-sauvegarde exécutés
4. Hooks post-sauvegarde exécutés

Testez les scripts d'exécution avant de les activer en production. Utilisez « kubectl exec » pour tester les scripts, puis vérifiez les instantanés et les sauvegardes en clonant l'application dans un espace de noms temporaire et en la restaurant.

Si un hook d'exécution pré-snapshot ajoute, modifie ou supprime des ressources Kubernetes, ces modifications sont incluses dans le snapshot ou la sauvegarde et dans toute opération de restauration ultérieure.

Remarques importantes sur les hooks d'exécution personnalisés

Tenez compte des éléments suivants lors de la planification des hooks d'exécution pour vos applications.

- Un hook d'exécution doit utiliser un script pour effectuer des actions. De nombreux hooks d'exécution peuvent référencer le même script.
- Les hooks d'exécution doivent être écrits au format de scripts shell exécutables.
- La taille du script est limitée à 96 Ko.
- Les paramètres de hook d'exécution et tous les critères de correspondance sont utilisés pour déterminer quels hooks sont applicables à une opération de snapshot, de sauvegarde ou de restauration.

Les hooks d'exécution peuvent réduire ou désactiver les fonctionnalités de l'application. Faites fonctionner vos crochets personnalisés le plus rapidement possible. Si vous démarrez une opération de sauvegarde ou de snapshot avec des hooks d'exécution associés, mais que vous l'annulez ensuite, les hooks sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou de snapshot a déjà commencé. Cela signifie que la logique utilisée dans un hook d'exécution post-sauvegarde ne peut pas supposer que la sauvegarde a été terminée.

Filtres de crochet d'exécution

Lorsque vous ajoutez ou modifiez un hook d'exécution pour une application, vous pouvez ajouter des filtres au hook d'exécution pour gérer les conteneurs auxquels le hook correspondra. Les filtres sont utiles pour les applications qui utilisent la même image de conteneur sur tous les conteneurs, mais peuvent utiliser chaque image à des fins différentes (comme Elasticsearch). Les filtres vous permettent de créer des scénarios dans lesquels les hooks d'exécution s'exécutent sur certains conteneurs identiques, mais pas nécessairement sur tous. Si vous créez plusieurs filtres pour un seul hook d'exécution, ils sont combinés avec un opérateur AND logique. Vous pouvez avoir jusqu'à 10 filtres actifs par hook d'exécution.

Chaque filtre que vous ajoutez à un hook d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un hook correspond à un conteneur, le hook exécutera son script associé sur ce conteneur. Les expressions régulières pour les filtres utilisent la syntaxe d'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre excluant les conteneurs de la liste des correspondances. Pour plus d'informations sur la syntaxe prise en charge par NetApp Backup and Recovery pour les expressions régulières dans les filtres de hook d'exécution, consultez "Prise en charge de la syntaxe des expressions régulières 2 (RE2)" .

Si vous ajoutez un filtre d'espace de noms à un hook d'exécution qui s'exécute après une opération de restauration ou de clonage et que la source et la destination de restauration ou de clonage se trouvent dans des espaces de noms différents, le filtre d'espace de noms est appliqué uniquement à l'espace de noms de destination.

Exemples de crochets d'exécution

Visitez le "Projet GitHub NetApp Verda" pour télécharger de véritables hooks d'exécution pour des applications populaires telles qu'Apache Cassandra et Elasticsearch. Vous pouvez également voir des exemples et obtenir des idées pour structurer vos propres hooks d'exécution personnalisés.

Créer un modèle de hook d'exécution

Vous pouvez créer un modèle de hook d'exécution personnalisé que vous pouvez utiliser pour effectuer des actions avant ou après une opération de protection des données sur une application.

Les modèles que vous créez ici ne sont utilisables que lors de la protection des charges de travail Kubernetes.

Étapes

1. Dans la console, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Paramètres**.
3. Développez la section **Modèle de hook d'exécution**.
4. Sélectionnez **Créer un modèle de hook d'exécution**.
5. Entrez un nom pour le hook d'exécution.

6. Vous pouvez également choisir un type de hook. Par exemple, un hook post-restauration est exécuté une fois l'opération de restauration terminée.
7. Dans la zone de texte **Script**, saisissez le script shell exécutable que vous souhaitez exécuter dans le cadre du modèle de hook d'exécution. Vous pouvez également sélectionner **Télécharger le script** pour télécharger un fichier de script à la place.
8. Sélectionnez **Créer**.

   Une fois le modèle créé, il apparaît dans la liste des modèles dans la section **Modèle de hook d'exécution**.

Surveiller les tâches dans NetApp Backup and Recovery

Avec NetApp Backup and Recovery, surveillez les snapshots locaux, les réplications et les tâches de sauvegarde que vous démarrez. Suivez les tâches de restauration que vous lancez. Affichez les tâches terminées, en cours ou ayant échoué pour aider à diagnostiquer les problèmes. Activez les notifications par e-mail dans le centre de notifications de la NetApp Console pour rester informé de l'activité du système lorsque vous n'êtes pas connecté. Utilisez la chronologie de la console pour voir les détails de toutes les actions démarrées à partir de l'interface utilisateur ou de l'API.

NetApp Backup and Recovery conserve les informations sur les tâches pendant 15 jours, puis les supprime et les supprime du Job Monitor.

Rôle de NetApp Console requis Visualiseur de stockage, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération, administrateur de clone de sauvegarde et de récupération ou rôle de visualiseur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Afficher l'état du travail sur le moniteur de travail

Vous pouvez afficher une liste de toutes les opérations de snapshot, de réplication, de sauvegarde sur stockage d'objets et de restauration ainsi que leur état actuel dans l'onglet **Surveillance des tâches**. Cela inclut les opérations de vos Cloud Volumes ONTAP, ONTAP sur site, applications et machines virtuelles. Chaque opération, ou tâche, possède un identifiant et un statut uniques.

Le statut peut être :

- Succès
- En cours
- En file d'attente
- Avertissement
- Échec

Les instantanés, les réplications, les sauvegardes sur le stockage d'objets et les opérations de restauration que vous avez lancées à partir de l'interface utilisateur et de l'API NetApp Backup and Recovery sont disponibles dans l'onglet Surveillance des tâches.

Si vous avez mis à niveau vos systèmes ONTAP vers la version 9.13.x et que vous ne voyez pas d'opérations de sauvegarde planifiées en cours dans le moniteur de tâches, redémarrez NetApp Backup and Recovery. "Apprenez à redémarrer NetApp Backup and Recovery".

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Surveillance**.
2. Pour afficher des colonnes supplémentaires (Système, SVM, Nom d'utilisateur, Charge de travail, Nom de la politique, Étiquette d'instantané), sélectionnez le signe plus.

Rechercher et filtrer la liste des emplois

Vous pouvez filtrer les opérations sur la page de surveillance des tâches à l'aide de plusieurs filtres, tels que la politique, l'étiquette de l'instantané, le type d'opération (protection, restauration, conservation ou autre) et le type de protection (instantané local, réplication ou sauvegarde dans le cloud).

Par défaut, la page Surveillance des tâches affiche les tâches de protection et de récupération des dernières 24 heures. Vous pouvez modifier la période à l'aide du filtre Période.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Surveillance**.
2. Pour trier les résultats différemment, sélectionnez chaque en-tête de colonne pour trier par statut, heure de début, nom de la ressource, etc.
3. Si vous recherchez des emplois spécifiques, sélectionnez la zone **Recherche avancée et filtrage** pour ouvrir le panneau de recherche.

   Utilisez ce panneau pour saisir une recherche de texte libre pour n'importe quelle ressource ; par exemple « volume 1 » ou « application 3 ». Vous pouvez également filtrer la liste des tâches en fonction des éléments des menus déroulants.

   La plupart des filtres sont explicites. Le filtre « Charge de travail » vous permet d'afficher les emplois dans les catégories suivantes :

   - Volumes ONTAP (Cloud Volumes ONTAP et volumes ONTAP sur site)
   - Microsoft SQL Server
   - Machines virtuelles
   - Kubernetes

   - Vous ne pouvez rechercher des données dans un « SVM » spécifique que si vous avez d'abord sélectionné un système.
   - Vous pouvez effectuer une recherche en utilisant le filtre « Type de protection » uniquement lorsque vous avez sélectionné le « Type » de « Protection ».

4. Pour mettre à jour la page immédiatement, sélectionnez l'icône bouton. Sinon, cette page s'actualise toutes les 15 minutes afin que vous puissiez toujours voir les résultats les plus récents en matière d'état des tâches.

Voir les détails du poste

Vous pouvez afficher les détails correspondant à un travail terminé spécifique. Vous pouvez exporter les

détails d'un travail particulier au format JSON.

Vous pouvez afficher des détails tels que le type de tâche (planifiée ou à la demande), le type de sauvegarde SnapMirror (initiale ou périodique), les heures de début et de fin, la durée, la quantité de données transférées du système vers le stockage d'objets, le taux de transfert moyen, le nom de la politique, le verrouillage de rétention activé, l'analyse des ransomwares effectuée, les détails de la source de protection et les détails de la cible de protection.

Les tâches de restauration affichent des détails tels que le fournisseur cible de sauvegarde (Amazon Web Services, Microsoft Azure, Google Cloud, sur site), le nom du bucket S3, le nom de la SVM, le nom du volume source, le volume de destination, l'étiquette de l'instantané, le nombre d'objets récupérés, les noms de fichiers, les tailles de fichiers, la date de dernière modification et le chemin d'accès complet au fichier.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Surveillance**.
2. Sélectionnez le nom du travail.
3. Sélectionnez le menu Actions ••• et sélectionnez **Afficher les détails**.
4. Développez chaque section pour voir les détails.

Télécharger les résultats de la surveillance des tâches sous forme de rapport

Vous pouvez télécharger le contenu de la page principale de surveillance des tâches sous forme de rapport après avoir filtré ou trié les résultats. NetApp Backup and Recovery génère et télécharge un fichier .CSV que vous pouvez consulter et envoyer à d'autres groupes selon vos besoins. Le fichier .CSV comprend jusqu'à 10 000 lignes de données.

À partir des informations sur les détails de la surveillance des tâches, vous pouvez télécharger un fichier JSON contenant les détails d'une tâche unique.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Surveillance**.
2. Pour télécharger un fichier CSV pour tous les travaux, sélectionnez le bouton Télécharger et recherchez le fichier dans votre répertoire de téléchargement.
3. Pour télécharger un fichier JSON pour une seule tâche, sélectionnez le menu Actions ••• pour le travail, sélectionnez **Télécharger le fichier JSON** et localisez le fichier dans votre répertoire de téléchargement.

Examiner les tâches de rétention (cycle de vie des sauvegardes)

Surveillez les flux de rétention (*cycle de vie des sauvegardes*) pour vérifier les sauvegardes, les protéger et prendre en charge les audits. Identifiez quand les copies de sauvegarde expirent pour suivre le cycle de vie.

Une tâche de cycle de vie de sauvegarde suit tous les instantanés supprimés ou en attente de suppression. À partir d' ONTAP 9.13, vous pouvez consulter tous les types de tâches appelés « Rétention » sur la page de surveillance des tâches.

Le type de tâche « Rétention » capture toutes les tâches de suppression d'instantanés lancées sur un volume protégé par NetApp Backup and Recovery.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Surveillance**.
2. Sélectionnez la zone **Recherche avancée et filtrage** pour ouvrir le panneau de recherche.

3. Sélectionnez « Rétention » comme type de travail.

Consultez les alertes de sauvegarde et de restauration dans le centre de notifications de la NetApp Console

Le centre de notifications de la NetApp Console suit la progression des tâches de sauvegarde et de restauration que vous avez lancées afin que vous puissiez vérifier si l'opération a réussi ou non.

Vous pouvez afficher les alertes dans le Centre de notifications et configurer la console pour envoyer des alertes par e-mail pour les activités système importantes, même lorsque vous n'êtes pas connecté. "En savoir plus sur le centre de notifications et comment envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration" .

Le Centre de notifications affiche de nombreux événements de capture instantanée, de réplication, de sauvegarde dans le cloud et de restauration, mais seuls certains événements déclenchent des alertes par e-mail :

Type d'opération	Événement	Alerte générée	E-mail envoyé
Activation	L'activation de la sauvegarde et de la récupération a échoué pour le système	Oui	Oui
Activation	Échec de la modification de la sauvegarde et de la récupération pour le système	Oui	Oui
Activation	Volume désormais associé à la politique d'instantané	Oui	Oui
Activation	Sauvegarde de volume ou état modifié	Oui	Oui
Activation	Activation de la sauvegarde et de la restauration réussie pour le système	Oui	Oui
Activation	La sauvegarde ad hoc du volume a échoué	Oui	Oui
Activation	Sauvegarde de volume ad hoc réussie	Oui	Non
Activation	La sauvegarde multivolume a échoué	Oui	Oui
Opérations Cron	Vérification des étiquettes d'instantané manquantes	Oui	Oui
Opérations Cron	Échec de l'envoi du jeton de sécurité à ONTAP pour ce système	Oui	Oui
Événements Pub/Sub	Échec de la connexion	Oui	Non
Événements Pub/Sub	Échec de la suppression d'un instantané planifié	Oui	Non
Événements Pub/Sub	La sauvegarde planifiée du volume a échoué	Oui	Non
Événements Pub/Sub	La restauration du volume a réussi.	Oui	Non
Événements Pub/Sub	La restauration du volume a échoué.	Oui	Non

Type d'opération	Événement	Alerte générée	E-mail envoyé
Ransomware	Attaque potentielle par ransomware identifiée sur une copie de sauvegarde	Oui	Oui
Ransomware	Une attaque potentielle de type ransomware a été identifiée sur une copie de sauvegarde de ce système.	Oui	Oui
Instantané local	Échec de la tâche de création d'instantanés ad hoc de NetApp Backup and Recovery	Oui	Oui
Réplication	Modification de la relation de réplication de l'échec de volume	Oui	Oui
Réplication	Échec de la tâche de réplication ad hoc de NetApp Backup and Recovery	Oui	Oui
Réplication	Échec de la tâche de pause de réplication de NetApp Backup and Recovery	Oui	Non
Réplication	Échec de la tâche d'interruption de la réplication de NetApp Backup and Recovery	Oui	Non
Réplication	Échec de la tâche de resynchronisation de la réplication NetApp Backup and Recovery	Oui	Non
Réplication	Échec de la tâche d'arrêt de la réplication de NetApp Backup and Recovery	Oui	Non
Réplication	Échec de la tâche de resynchronisation inverse de la réplication NetApp Backup and Recovery	Oui	Oui
Réplication	Échec de la tâche de suppression de réplication de NetApp Backup and Recovery	Oui	Oui
Opérations ciblées	Échec de la restauration vers une destination locale ou cloud	Oui	Oui
Opérations ciblées	Échec de la restauration à la demande	Oui	Oui
Opérations système	Échec de la création d'un instantané de volume ad hoc	Oui	Oui

À partir d' ONTAP 9.13.0, toutes les alertes apparaissent pour Cloud Volumes ONTAP et les systèmes ONTAP sur site. Pour les systèmes avec Cloud Volumes ONTAP 9.13.0 et ONTAP sur site, seule l'alerte relative à « Tâche de restauration terminée, mais avec des avertissements » s'affiche.

Par défaut, les administrateurs de compte et d'organisation de la NetApp Console reçoivent des e-mails pour toutes les alertes « Critiques » et « Recommandation ». Par défaut, le système ne configure pas les autres utilisateurs et destinataires pour recevoir des e-mails de notification. Configurez des alertes par e-mail pour tous les utilisateurs de la console de votre compte NetApp Cloud ou pour d'autres destinataires qui doivent être informés de l'activité de sauvegarde et de restauration.

Pour recevoir les alertes par e-mail de NetApp Backup and Recovery , vous devez sélectionner les types de gravité de notification « Critique », « Avertissement » et « Erreur » dans la page des paramètres de notifications.

"Découvrez comment envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration".

Étapes

1. Dans le menu de la console, sélectionnez l'option ( ).
2. Consultez les notifications.

Examiner l'activité opérationnelle dans la chronologie de la console

Vous pouvez afficher les détails des opérations de sauvegarde et de restauration pour une enquête plus approfondie dans la chronologie de la console. La chronologie de la console fournit des détails sur chaque événement, qu'il soit initié par l'utilisateur ou par le système, et affiche les actions initiées dans l'interface utilisateur ou via l'API.

"Découvrez les différences entre la chronologie et le centre de notifications".

Redémarrer NetApp Backup and Recovery

Il peut y avoir des situations dans lesquelles vous devrez redémarrer NetApp Backup and Recovery.

L'agent de console inclut la fonctionnalité de NetApp Backup and Recovery .

Étapes

1. Connectez-vous au système Linux sur lequel l'agent de console s'exécute.

Emplacement de l'agent de la console	Procédure
Déploiement dans le cloud	Suivez les instructions pour "connexion à la machine virtuelle Linux de l'agent de console" selon le fournisseur de cloud que vous utilisez.
Installation manuelle	Connectez-vous au système Linux.

2. Entrez la commande pour redémarrer le service.

Emplacement de l'agent de la console	Commande Docker	Commande Podman
Déploiement dans le cloud	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installation manuelle avec accès Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installation manuelle sans accès Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`