Documentation sur la NetApp Backup and Recovery

NetApp Backup and Recovery

NetApp
October 20, 2025

Sommaire

Documentation sur la NetApp Backup and Recovery

Notes de version

Nouveautés de NetApp Backup and Recovery

Découvrez les nouveautés de NetApp Backup and Recovery.

06 octobre 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

La BlueXP backup and recovery sont désormais NetApp Backup and Recovery

La BlueXP backup and recovery ont été renommées NetApp Backup and Recovery.

BlueXP est désormais NetApp Console

La NetApp Console, construite sur la base BlueXP améliorée et restructurée, fournit une gestion centralisée du stockage NetApp et des NetApp Data Services dans les environnements sur site et dans le cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée, hautement sécurisée et conforme.

Pour plus de détails sur ce qui a changé, consultez le"Notes de version de la NetApp Console ."

Prise en charge de la charge de travail Hyper-V en tant qu'aperçu privé

Cette version de NetApp Backup and Recovery introduit la prise en charge de la découverte et de la gestion des charges de travail Hyper-V :

- Sauvegarder et restaurer des machines virtuelles sur des instances autonomes ainsi que sur des instances de cluster de basculement (FCI)
- Protéger les machines virtuelles stockées sur des partages SMB3
- Protection en masse au niveau de la machine virtuelle
- Sauvegardes cohérentes avec les machines virtuelles et les pannes
- Restaurer les machines virtuelles à partir du stockage principal, secondaire et objet
- Rechercher et restaurer les sauvegardes de machines virtuelles

Pour plus de détails sur la protection des charges de travail Hyper-V, reportez-vous à "Présentation de la protection des charges de travail Hyper-V" .

Prise en charge de la charge de travail KVM en tant qu'aperçu privé

Cette version de NetApp Backup and Recovery introduit la prise en charge de la découverte et de la gestion des charges de travail KVM :

- Sauvegarder et restaurer les images de machines virtuelles qcow2 stockées sur des partages NFS
- Sauvegarder les pools de stockage
- Protection en masse des machines virtuelles et des pools de stockage à l'aide de groupes de protection
- Sauvegardes de machines virtuelles cohérentes et cohérentes en cas de panne

- Rechercher et restaurer des sauvegardes de machines virtuelles à partir du stockage principal, secondaire et objet
- Processus guidé pour sauvegarder et restaurer les machines virtuelles et les données de machines virtuelles basées sur KVM

Pour plus de détails sur la protection des charges de travail KVM, reportez-vous à "Présentation de la protection des charges de travail KVM" .

Améliorations de l'aperçu de Kubernetes

La version préliminaire des charges de travail Kubernetes introduit les fonctionnalités améliorées suivantes :

- Prise en charge de l'architecture de sauvegarde en éventail 3-2-1
- Prise en charge d' ONTAP S3 comme cible de sauvegarde
- Nouveau tableau de bord Kubernetes pour une gestion plus facile
- La configuration améliorée du contrôle d'accès basé sur les rôles (RBAC) inclut la prise en charge des rôles suivants :
  - Super administrateur de sauvegarde et de récupération
  - Sauvegarde et récupération de l'administrateur de sauvegarde
  - Administrateur de restauration de sauvegarde et de récupération
  - Visionneuse de sauvegarde et de récupération
- Prise en charge de la distribution SUSE Rancher Kubernetes
- Prise en charge de plusieurs compartiments : vous pouvez désormais protéger les volumes d'un système avec plusieurs compartiments par système sur différents fournisseurs de cloud.

Pour plus de détails sur la protection des charges de travail Kubernetes, reportez-vous à "Présentation de la protection des charges de travail Kubernetes" .

Améliorations de l'aperçu de VMware

La version préliminaire des charges de travail VMware introduit les fonctionnalités améliorées suivantes :

- Prise en charge de la restauration à partir du stockage d'objets
- Le tableau de bord de la NetApp Console affiche désormais les informations sur l'état de la charge de travail VMware
- Prise en charge du mode démo : explorez les fonctionnalités des charges de travail VMware sans ajouter d'environnement VMware vCenter Server
- Prise en charge du contrôle d'accès basé sur les rôles (RBAC)
- Alerte par e-mail et prise en charge des notifications pour les événements professionnels
- Prise en charge de la sauvegarde et de la restauration sur un stockage basé sur NVMe
- Modifier les groupes de protection
- Modifier les politiques de protection

Pour plus de détails sur la protection des charges de travail VMware, reportez-vous à "Présentation de la protection des charges de travail VMware" .

Prise en charge de la charge de travail de la base de données Oracle en tant qu'aperçu privé

Cette version de NetApp Backup and Recovery introduit la prise en charge de la découverte et de la gestion des charges de travail de base de données Oracle :

- Découvrez les bases de données Oracle autonomes
- Créer des politiques de protection pour les données uniquement ou pour les sauvegardes de données et de journaux
- Protégez les bases de données Oracle avec un schéma de sauvegarde 3-2-1
- Configurer la conservation des sauvegardes
- Monter et démonter les sauvegardes ARCHIVELOG
- Bases de données virtualisées
- Rechercher et restaurer les sauvegardes de bases de données
- Prise en charge du tableau de bord Oracle

Pour plus de détails sur la protection des charges de travail de la base de données Oracle, reportez-vous à "Présentation de Protect Oracle Workloads" .

25 août 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Prise en charge de la protection des charges de travail VMware dans l'aperçu

Cette version ajoute une prise en charge préliminaire pour la protection des charges de travail VMware. Sauvegardez les machines virtuelles VMware et les banques de données des systèmes ONTAP sur site vers Amazon Web Services et StorageGRID.

> La documentation sur la protection des charges de travail VMware est fournie sous forme d'aperçu technologique. 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.

"En savoir plus sur la protection des charges de travail VMware avec NetApp Backup and Recovery".

L'indexation haute performance pour AWS, Azure et GCP est généralement disponible

En février 2025, nous avons annoncé l'aperçu de l'indexation haute performance (Indexed Catalog v2) pour AWS, Azure et GCP. Cette fonctionnalité est désormais généralement disponible (GA). En juin 2025, nous l'avons fourni à tous les *nouveaux* clients par défaut. Avec cette version, le support est disponible pour *tous* les clients. L'indexation hautes performances améliore les performances des opérations de sauvegarde et de restauration pour les charges de travail protégées par le stockage d'objets.

Activé par défaut :

- Si vous êtes un nouveau client, l'indexation haute performance est activée par défaut.
- Si vous êtes un client existant, vous pouvez activer la réindexation en accédant à la section Restaurer de l'interface utilisateur.

12 août 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

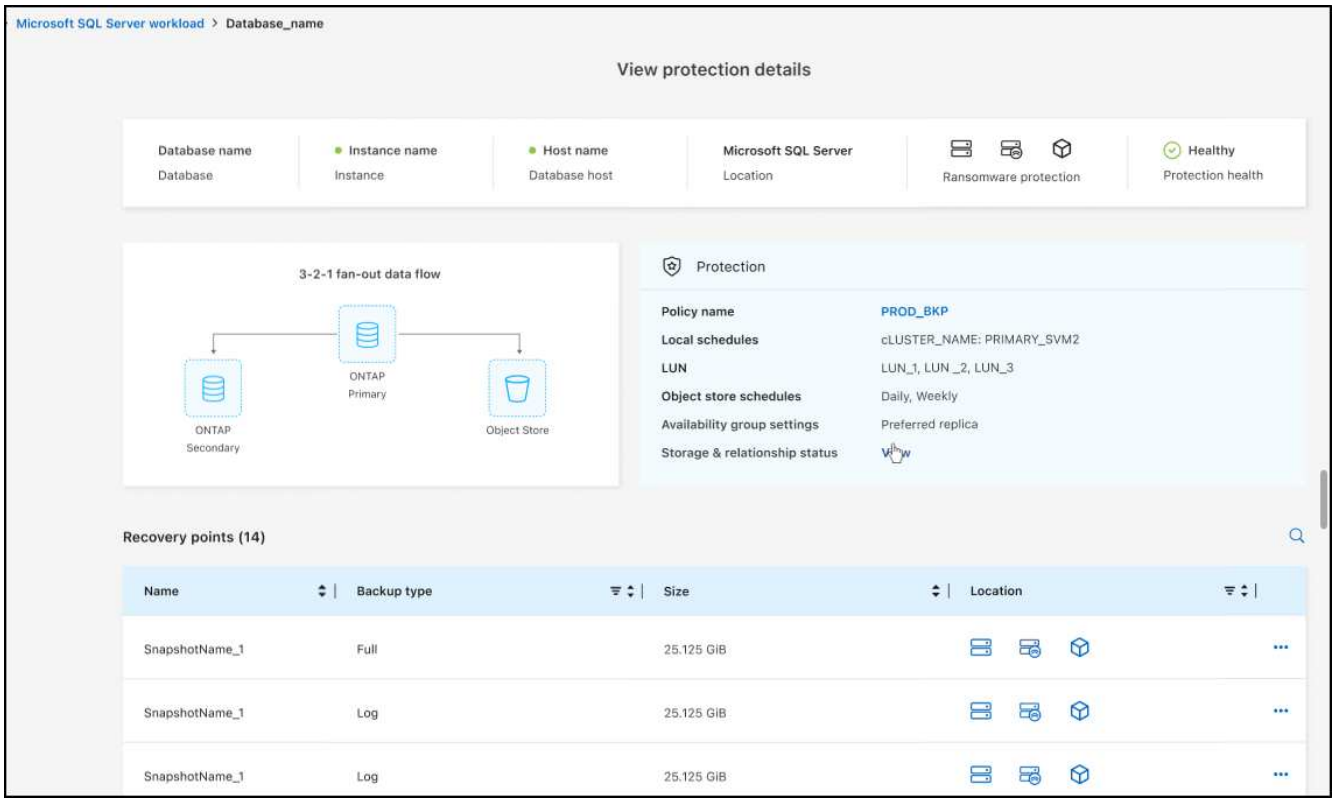
Charge de travail Microsoft SQL Server prise en charge en disponibilité générale (GA)

La prise en charge des charges de travail Microsoft SQL Server est désormais généralement disponible (GA) dans NetApp Backup and Recovery. Les organisations utilisant un environnement MSSQL sur ONTAP, Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP peuvent désormais profiter de ce nouveau service de sauvegarde et de récupération pour protéger leurs données.

Cette version inclut les améliorations suivantes apportées à la prise en charge de la charge de travail Microsoft SQL Server par rapport à la version d'aperçu précédente :

- * Synchronisation active SnapMirror * : cette version prend désormais en charge la synchronisation active SnapMirror (également appelée SnapMirror Business Continuity [SM-BC]), qui permet aux services d'entreprise de continuer à fonctionner même en cas de panne complète du site, en prenant en charge le basculement transparent des applications à l'aide d'une copie secondaire. NetApp Backup and Recovery prend désormais en charge la protection des bases de données Microsoft SQL Server dans une configuration SnapMirror Active Sync et Metrocluster. Les informations apparaissent dans la section **Statut de stockage et de relation** de la page Détails de la protection. Les informations sur la relation sont affichées dans la section **Paramètres secondaires** mise à jour de la page Politique.

  Se référer à "Utilisez des politiques pour protéger vos charges de travail" .

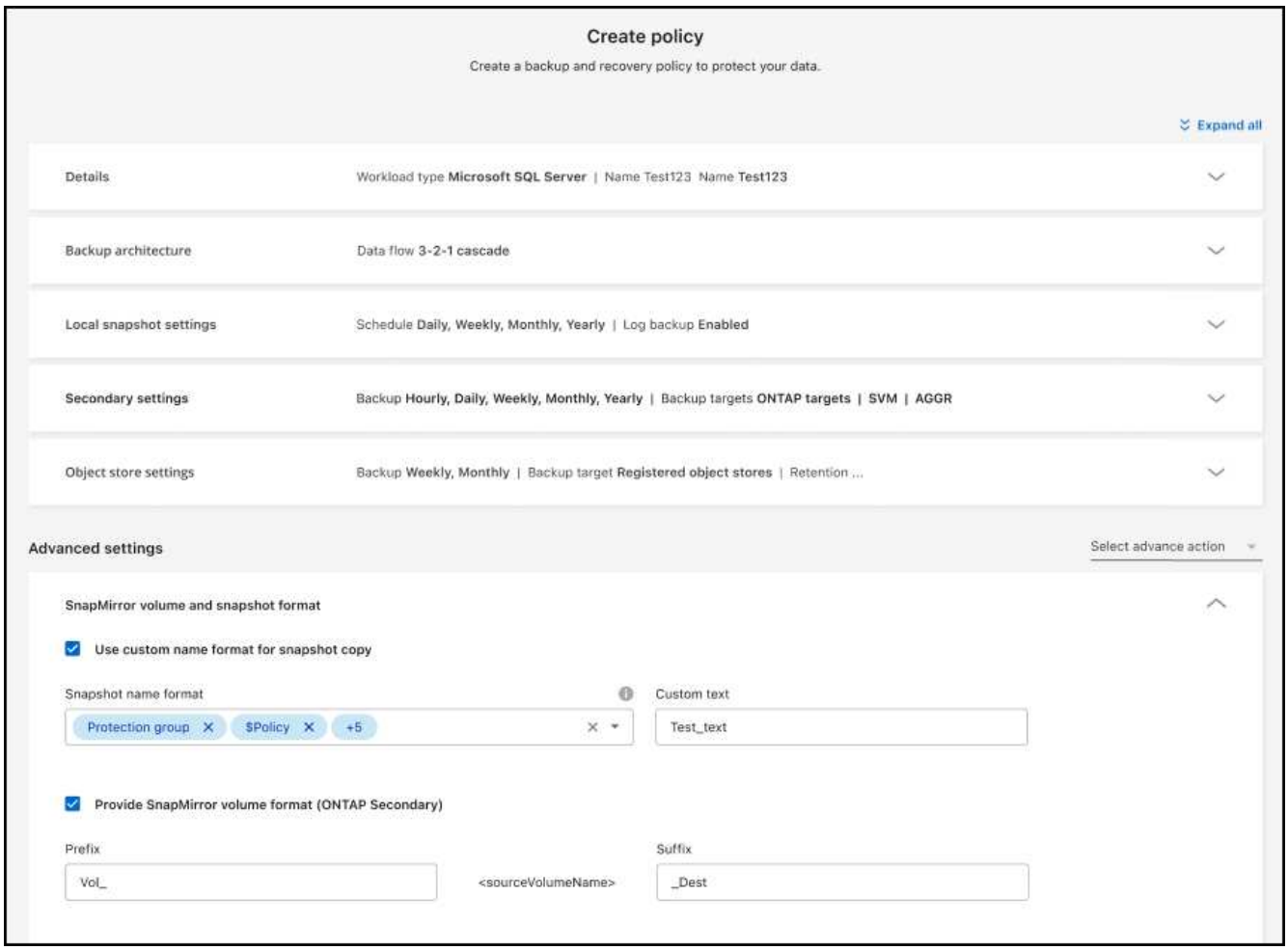


- **Prise en charge de plusieurs buckets** : vous pouvez désormais protéger les volumes au sein d'un environnement de travail avec jusqu'à 6 buckets par environnement de travail sur différents fournisseurs de cloud.
- **Mises à jour de licence et d'essai gratuites** pour les charges de travail SQL Server : vous pouvez désormais utiliser le modèle de licence NetApp Backup and Recovery existant pour protéger les charges

de travail SQL Server. Il n'existe aucune exigence de licence distincte pour les charges de travail SQL Server.

Pour plus de détails, reportez-vous à "Configurer les licences pour NetApp Backup and Recovery" .

- **Nom d'instantané personnalisé** : vous pouvez désormais utiliser votre propre nom d'instantané dans une stratégie qui régit les sauvegardes des charges de travail Microsoft SQL Server. Saisissez ces informations dans la section **Paramètres avancés** de la page Politique.



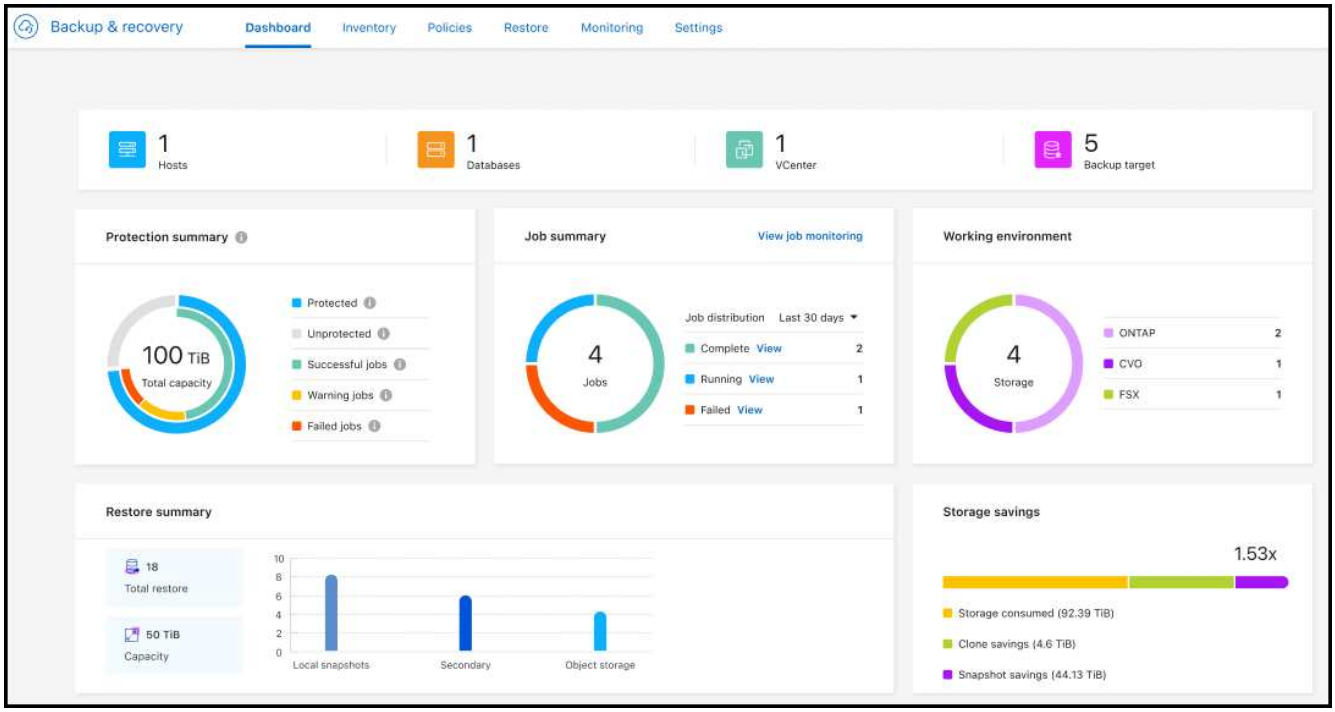
Se référer à "Utilisez des politiques pour protéger vos charges de travail" .

- **Préfixe et suffixe du volume secondaire** : Vous pouvez saisir un préfixe et un suffixe personnalisés dans la section **Paramètres avancés** de la page Politique.
- **Identité et accès** : Vous pouvez désormais contrôler l'accès des utilisateurs aux fonctionnalités.

  Se référer à "Connectez-vous à NetApp Backup and Recovery" et "Accès aux fonctionnalités de NetApp Backup and Recovery" .

- **Restauration à partir du stockage d'objets vers un autre hôte** : vous pouvez désormais restaurer à partir du stockage d'objets vers un autre hôte même si le stockage principal est en panne.
- **Données de sauvegarde du journal** : la page des détails de protection de la base de données affiche désormais les sauvegardes du journal. Vous pouvez voir la colonne Type de sauvegarde qui indique si la sauvegarde est une sauvegarde complète ou une sauvegarde de journal.
- **Tableau de bord amélioré** : le tableau de bord affiche désormais les économies de stockage et de

clonage.



Améliorations de la charge de travail du volume ONTAP

- *Restauration multi-dossiers pour les volumes ONTAP * : Jusqu'à présent, vous pouviez restaurer un dossier ou plusieurs fichiers à la fois à partir de la fonction Parcourir et restaurer. NetApp Backup and Recovery offre désormais la possibilité de sélectionner plusieurs dossiers à la fois à l'aide de la fonction Parcourir et restaurer.
- **Afficher et gérer les sauvegardes des volumes supprimés** : le tableau de bord de NetApp Backup and Recovery offre désormais une option permettant d'afficher et de gérer les volumes supprimés d' ONTAP. Avec cela, vous pouvez afficher et supprimer les sauvegardes des volumes qui n'existent plus dans ONTAP.
- **Forcer la suppression des 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 de l'environnement de travail).

> 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.

Se référer à "Protégez les charges de travail ONTAP" .

28 juillet 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Prise en charge des charges de travail Kubernetes en tant qu'aperçu

Cette version de NetApp Backup and Recovery introduit la prise en charge de la découverte et de la gestion des charges de travail Kubernetes :

- Découvrez Red Hat OpenShift et les clusters Kubernetes open source, soutenus par NetApp ONTAP, sans partager les fichiers kubeconfig.
- Découvrez, gérez et protégez les applications sur plusieurs clusters Kubernetes à l'aide d'un plan de contrôle unifié.
- Déchargez les opérations de déplacement de données pour la sauvegarde et la récupération des applications Kubernetes vers NetApp ONTAP.
- Orchestrez les sauvegardes d'applications locales et basées sur le stockage d'objets.
- Sauvegardez et restaurez des applications entières et des ressources individuelles sur n'importe quel cluster Kubernetes.
- Travaillez avec des conteneurs et des machines virtuelles exécutés sur Kubernetes.
- Créez des sauvegardes cohérentes avec les applications à l'aide de hooks d'exécution et de modèles.

Pour plus de détails sur la protection des charges de travail Kubernetes, reportez-vous à "Présentation de la protection des charges de travail Kubernetes" .

14 juillet 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Tableau de bord de volume ONTAP amélioré

En avril 2025, nous avons lancé un aperçu d'un tableau de bord de volume ONTAP amélioré, beaucoup plus rapide et plus efficace.

Ce tableau de bord a été conçu pour aider les clients d'entreprise avec un nombre élevé de charges de travail. Même pour les clients disposant de 20 000 volumes, le nouveau tableau de bord se charge en moins de 10 secondes.

Après un aperçu réussi et de très bons retours de la part des clients, nous en faisons désormais l'expérience par défaut pour tous nos clients. Préparez-vous pour un tableau de bord incroyablement rapide.

Pour plus de détails, voir"Afficher l'état de la protection dans le tableau de bord" .

Prise en charge de la charge de travail Microsoft SQL Server en tant qu'aperçu technologique public

Cette version de NetApp Backup and Recovery fournit une interface utilisateur mise à jour qui vous permet de gérer les charges de travail Microsoft SQL Server à l'aide d'une stratégie de protection 3-2-1, familière dans NetApp Backup and Recovery. Avec cette nouvelle version, vous pouvez sauvegarder ces charges de travail sur le stockage principal, les répliquer sur le stockage secondaire et les sauvegarder sur le stockage d'objets cloud.

Vous pouvez vous inscrire à l'aperçu en remplissant ce formulaire "Aperçu du formulaire d'inscription" .

Cette documentation sur la protection des charges de travail Microsoft SQL Server est fournie en avant-première technologique. NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de cette offre avant sa disponibilité générale.

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes :

- **Fonctionnalité de sauvegarde 3-2-1** : cette version intègre les fonctionnalités de SnapCenter , vous permettant de gérer et de protéger vos ressources SnapCenter avec une stratégie de protection des données 3-2-1 à partir de l'interface utilisateur de NetApp Backup and Recovery .
- **Importer depuis SnapCenter** : vous pouvez importer des données et des politiques de sauvegarde SnapCenter dans NetApp Backup and Recovery.
- **Une interface utilisateur repensée** offre une expérience plus intuitive pour la gestion de vos tâches de sauvegarde et de récupération.
- **Cibles de sauvegarde** : vous pouvez ajouter des buckets dans les environnements Amazon Web Services (AWS), Microsoft Azure Blob Storage, StorageGRID et ONTAP S3 à utiliser comme cibles de sauvegarde pour vos charges de travail Microsoft SQL Server.
- **Prise en charge de la charge de travail** : cette version vous permet de sauvegarder, restaurer, vérifier et cloner des bases de données et des groupes de disponibilité Microsoft SQL Server. (La prise en charge d'autres charges de travail sera ajoutée dans les prochaines versions.)
- **Options de restauration flexibles** : Cette version vous permet de restaurer les bases de données vers leurs emplacements d'origine et alternatifs en cas de corruption ou de perte accidentelle de données.
- **Copies de production instantanées** : générez des copies de production peu encombrantes pour le développement, les tests ou les analyses en quelques minutes au lieu de plusieurs heures ou jours.
- Cette version inclut la possibilité de créer des rapports détaillés.

Pour plus de détails sur la protection des charges de travail Microsoft SQL Server, consultez"Présentation de la protection des charges de travail Microsoft SQL Server" .

09 juin 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Mises à jour du support du catalogue indexé

En février 2025, nous avons introduit la fonctionnalité d'indexation mise à jour (Catalogue indexé v2) que vous utilisez pendant la méthode de recherche et de restauration des données. La version précédente a considérablement amélioré les performances d'indexation des données dans les environnements sur site. Avec cette version, le catalogue d'indexation est désormais disponible avec les environnements Amazon Web Services, Microsoft Azure et Google Cloud Platform (GCP).

Si vous êtes un nouveau client, le catalogue indexé v2 est activé par défaut pour tous les nouveaux environnements. Si vous êtes un client existant, vous pouvez réindexer votre environnement pour tirer parti du catalogue indexé v2.

Comment activer l'indexation ?

Avant de pouvoir utiliser la méthode de recherche et de restauration des données, vous devez activer « Indexation » sur chaque environnement de travail source à partir duquel vous prévoyez de restaurer des volumes ou des fichiers. Sélectionnez l'option **Activer l'indexation** lorsque vous effectuez une recherche et une restauration.

Le catalogue indexé peut ensuite suivre chaque volume et fichier de sauvegarde, rendant vos recherches rapides et efficaces.

Pour plus d'informations, reportez-vous à "Activer l'indexation pour la recherche et la restauration" .

Points de terminaison de liaison privée Azure et points de terminaison de service

En règle générale, NetApp Backup and Recovery établit un point de terminaison privé avec le fournisseur de cloud pour gérer les tâches de protection. Cette version introduit un paramètre facultatif qui vous permet d'activer ou de désactiver la création automatique d'un point de terminaison privé par NetApp Backup and Recovery . Cela peut vous être utile si vous souhaitez davantage de contrôle sur le processus de création de points de terminaison privés.

Vous pouvez activer ou désactiver cette option lorsque vous activez la protection ou démarrez le processus de restauration.

Si vous désactivez ce paramètre, vous devez créer manuellement le point de terminaison privé pour que NetApp Backup and Recovery fonctionne correctement. Sans connectivité appropriée, vous risquez de ne pas être en mesure d'effectuer correctement les tâches de sauvegarde et de récupération.

Prise en charge de SnapMirror vers Cloud Resync sur ONTAP S3

La version précédente a introduit la prise en charge de SnapMirror vers Cloud Resync (SM-C Resync). Cette fonctionnalité rationalise la protection des données lors de la migration de volumes dans les environnements NetApp . Cette version ajoute la prise en charge de SM-C Resync sur ONTAP S3 ainsi que d'autres fournisseurs compatibles S3 tels que Wasabi et MinIO.

Apportez votre propre bucket pour StorageGRID

Lorsque vous créez des fichiers de sauvegarde dans le stockage d'objets pour un environnement de travail, par défaut, NetApp Backup and Recovery crée le conteneur (bucket ou compte de stockage) pour les fichiers de sauvegarde dans le compte de stockage d'objets que vous avez configuré. Auparavant, vous pouviez remplacer cela et spécifier votre propre conteneur pour Amazon S3, Azure Blob Storage et Google Cloud Storage. Avec cette version, vous pouvez désormais apporter votre propre conteneur de stockage d'objets StorageGRID .

Voir "Créez votre propre conteneur de stockage d'objets" .

13 mai 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Resynchronisation de SnapMirror vers Cloud pour les migrations de volumes

La fonctionnalité SnapMirror to Cloud Resync 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 vers un autre ou vers une solution cloud telle que Cloud Volumes ONTAP ou Cloud Volumes Service, SnapMirror to Cloud Resync garantit que les sauvegardes cloud existantes restent intactes et opérationnelles.

Cette fonctionnalité élimine le besoin d'une opération de redéfinition de base longue et gourmande en ressources, permettant ainsi aux opérations de sauvegarde 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 .

En maintenant la continuité des sauvegardes dans tous les environnements, SnapMirror to Cloud Resync améliore l'efficacité opérationnelle et réduit la complexité de la gestion des données hybrides et multicloud.

Pour plus de détails sur la façon d'effectuer l'opération de resynchronisation, voir "Migrer des volumes à l'aide de SnapMirror vers Cloud Resync" .

Prise en charge du magasin d'objets MinIO tiers (aperçu)

NetApp Backup and Recovery étend désormais sa prise en charge aux magasins d'objets tiers, en mettant l'accent principalement sur MinIO. Cette nouvelle fonctionnalité d'aperçu vous permet d'exploiter n'importe quel magasin d'objets compatible S3 pour vos besoins de sauvegarde et de récupération.

Avec cette version préliminaire, nous espérons garantir une intégration robuste avec les magasins d'objets tiers avant que la fonctionnalité complète ne soit déployée. Nous vous encourageons à explorer cette nouvelle fonctionnalité et à fournir des commentaires pour aider à améliorer le service.

Cette fonctionnalité ne doit pas être utilisée en production.

Limites du mode aperçu

Bien que cette fonctionnalité soit en version préliminaire, il existe certaines limitations :

- L'option BYOB (Apportez votre propre seau) n'est pas prise en charge.
- L'activation de DataLock dans la politique n'est pas prise en charge.
- L'activation du mode d'archivage dans la politique n'est pas prise en charge.
- Seuls les environnements ONTAP sur site sont pris en charge.
- MetroCluster n'est pas pris en charge.
- Les options permettant d'activer le chiffrement au niveau du bucket ne sont pas prises en charge.

Commencer

Pour commencer à utiliser cette fonctionnalité d'aperçu, vous devez activer un indicateur sur l'agent de la console. Vous pouvez ensuite saisir les détails de connexion de votre magasin d'objets tiers MinIO dans le flux de travail de protection en choisissant le magasin d'objets **Compatible avec les tiers** dans la section de sauvegarde.

16 avril 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Améliorations de l'interface utilisateur

Cette version améliore votre expérience en simplifiant l'interface :

- La suppression de la colonne Agrégation des tables Volumes, ainsi que des colonnes Stratégie de snapshot, Stratégie de sauvegarde et Stratégie de réplication de la table Volume dans le tableau de bord V2, donne lieu à une présentation plus rationalisée.
- L'exclusion des environnements de travail non activés de la liste déroulante rend l'interface moins encombrée, la navigation plus efficace et le chargement plus rapide.
- Même si le tri sur la colonne Balises est désactivé, vous pouvez toujours afficher les balises, garantissant ainsi que les informations importantes restent facilement accessibles.
- La suppression des étiquettes sur les icônes de protection contribue à un aspect plus propre et réduit le temps de chargement.
- Pendant le processus d'activation de l'environnement de travail, une boîte de dialogue affiche une icône de chargement pour fournir des commentaires jusqu'à ce que le processus de découverte soit terminé, améliorant ainsi la transparence et la confiance dans les opérations du système.

Tableau de bord de volume amélioré (aperçu)

Le tableau de bord des volumes se charge désormais en moins de 10 secondes, offrant une interface beaucoup plus rapide et plus efficace. Cette version préliminaire est disponible pour certains clients, leur offrant un aperçu préliminaire de ces améliorations.

Prise en charge du magasin d'objets Wasabi tiers (aperçu)

NetApp Backup and Recovery étend désormais son support aux magasins d'objets tiers, en mettant l'accent principalement sur Wasabi. Cette nouvelle fonctionnalité d'aperçu vous permet d'exploiter n'importe quel magasin d'objets compatible S3 pour vos besoins de sauvegarde et de récupération.

Démarrer avec Wasabi

Pour commencer à utiliser un stockage tiers comme magasin d'objets, vous devez activer un indicateur dans l'agent de la console. Ensuite, vous pouvez saisir les détails de connexion de votre magasin d'objets tiers et l'intégrer dans vos flux de travail de sauvegarde et de récupération.

Étapes

1. Connectez-vous en SSH à votre connecteur.
2. Accédez au conteneur du serveur CBS NetApp Backup and Recovery :

```
docker exec -it cloudmanager_cbs sh
```

3. Ouvrez le `default.json` fichier à l'intérieur du `config` dossier via VIM ou tout autre éditeur :

```
vi default.json
```

4. Modifier `allow-s3-compatible` : faux à `allow-s3-compatible` : vrai.
5. Enregistrez les modifications.
6. Sortie du conteneur.
7. Redémarrez le conteneur du serveur NetApp Backup and Recovery CBS.

Résultat

Une fois le conteneur réactivé, ouvrez l'interface utilisateur de NetApp Backup and Recovery . Lorsque vous lancez une sauvegarde ou modifiez une stratégie de sauvegarde, vous verrez le nouveau fournisseur « Compatible S3 » répertorié avec d'autres fournisseurs de sauvegarde d'AWS, Microsoft Azure, Google Cloud, StorageGRID et ONTAP S3.

Limitations du mode aperçu

Bien que cette fonctionnalité soit en version préliminaire, tenez compte des limitations suivantes :

- L'option BYOB (Apportez votre propre seau) n'est pas prise en charge.
- L'activation de DataLock dans une politique n'est pas prise en charge.
- L'activation du mode d'archivage dans une politique n'est pas prise en charge.
- Seuls les environnements ONTAP sur site sont pris en charge.

- MetroCluster n’est pas pris en charge.
- Les options permettant d’activer le chiffrement au niveau du bucket ne sont pas prises en charge.

Au cours de cet aperçu, nous vous encourageons à explorer cette nouvelle fonctionnalité et à fournir des commentaires sur l’intégration avec les magasins d’objets tiers avant le déploiement complet des fonctionnalités.

17 mars 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Navigation dans les instantanés SMB

Cette mise à jour de NetApp Backup and Recovery a résolu un problème qui empêchait les clients de parcourir les snapshots locaux dans un environnement SMB.

Mise à jour de l’environnement AWS GovCloud

Cette mise à jour de NetApp Backup and Recovery a corrigé un problème qui empêchait l’interface utilisateur de se connecter à un environnement AWS GovCloud en raison d’erreurs de certificat TLS. Le problème a été résolu en utilisant le nom d’hôte de l’agent de console au lieu de l’adresse IP.

Limites de conservation de la politique de sauvegarde

Auparavant, l’interface utilisateur de NetApp Backup and Recovery limitait les sauvegardes à 999 copies, tandis que l’interface de ligne de commande en autorisait davantage. Désormais, vous pouvez attacher jusqu’à 4 000 volumes à une politique de sauvegarde et inclure 1 018 volumes non attachés à une politique de sauvegarde. Cette mise à jour inclut des validations supplémentaires qui empêchent de dépasser ces limites.

Resynchronisation de SnapMirror Cloud

Cette mise à jour garantit que la resynchronisation de SnapMirror Cloud ne peut pas être démarrée à partir de NetApp Backup and Recovery pour les versions ONTAP non prises en charge après la suppression d’une relation SnapMirror .

21 février 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Indexation haute performance

NetApp Backup and Recovery introduit une fonctionnalité d’indexation mise à jour qui rend l’indexation des données sur le système source plus efficace. La nouvelle fonctionnalité d’indexation inclut des mises à jour de l’interface utilisateur, des performances améliorées de la méthode de recherche et de restauration des données, des mises à niveau des capacités de recherche globale et une meilleure évolutivité.

Voici une ventilation des améliorations :

- **Consolidation des dossiers** : la version mise à jour regroupe les dossiers à l’aide de noms incluant des identifiants spécifiques, ce qui rend le processus d’indexation plus fluide.
- **Compactage des fichiers Parquet** : La version mise à jour réduit le nombre de fichiers utilisés pour l’indexation de chaque volume, simplifiant le processus et supprimant le besoin d’une base de données supplémentaire.

- **Extensibilité avec plus de sessions** : La nouvelle version ajoute plus de sessions pour gérer les tâches d'indexation, accélérant ainsi le processus.
- **Prise en charge de plusieurs conteneurs d'index** : la nouvelle version utilise plusieurs conteneurs pour mieux gérer et distribuer les tâches d'indexation.
- **Flux de travail d'indexation fractionné** : la nouvelle version divise le processus d'indexation en deux parties, améliorant ainsi l'efficacité.
- **Concurrence améliorée** : La nouvelle version permet de supprimer ou de déplacer des répertoires en même temps, accélérant ainsi le processus d'indexation.

À qui profite cette fonctionnalité ?

La nouvelle fonctionnalité d'indexation est disponible pour tous les nouveaux clients.

Comment activer l'indexation ?

Avant de pouvoir utiliser la méthode de recherche et de restauration des données, 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, rendant vos recherches rapides et efficaces.

Activez l'indexation sur l'environnement de travail source en sélectionnant l'option « Activer l'indexation » lorsque vous effectuez une recherche et une restauration.

Pour plus d'informations, consultez la documentation "comment restaurer les données ONTAP à l'aide de la recherche et de la restauration" .

Échelle prise en charge

La nouvelle fonctionnalité d'indexation 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.

Améliorations des performances de recherche globale

Cette version inclut également des améliorations des performances de recherche globale. Vous verrez désormais des indicateurs de progression et des résultats de recherche plus détaillés, notamment le nombre de fichiers et le temps nécessaire à la recherche. Des conteneurs dédiés à la recherche et à l'indexation garantissent que les recherches globales sont effectuées en moins de cinq minutes.

Notez ces considérations liées à la recherche globale :

- Le nouvel index n'est pas exécuté sur les instantanés étiquetés comme horaires.
- La nouvelle fonctionnalité d'indexation fonctionne uniquement sur les instantanés sur FlexVols, et non sur les instantanés sur FlexGroups.

13 février 2025

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Version préliminaire de NetApp Backup and Recovery

Cette version préliminaire de NetApp Backup and Recovery fournit une interface utilisateur mise à jour qui vous permet de gérer les charges de travail Microsoft SQL Server à l'aide d'une stratégie de protection 3-2-1, familière dans NetApp Backup and Recovery. Avec cette nouvelle version, vous pouvez sauvegarder ces charges de travail sur le stockage principal, les répliquer sur le stockage secondaire et les sauvegarder sur le stockage d'objets cloud.

> Cette documentation est fournie à titre d'aperçu technologique. 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.

Cette version de NetApp Backup and Recovery Preview 2025 inclut les mises à jour suivantes.

- Une interface utilisateur repensée qui offre une expérience plus intuitive pour la gestion de vos tâches de sauvegarde et de récupération.
- La version Preview vous permet de sauvegarder et de restaurer les bases de données Microsoft SQL Server. (La prise en charge d'autres charges de travail sera ajoutée dans les prochaines versions.)
- Cette version intègre les fonctionnalités de SnapCenter , vous permettant de gérer et de protéger vos ressources SnapCenter avec une stratégie de protection des données 3-2-1 à partir de l'interface utilisateur de NetApp Backup and Recovery .
- Cette version vous permet d'importer des charges de travail SnapCenter dans NetApp Backup and Recovery.

22 novembre 2024

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Modes de protection SnapLock Compliance et SnapLock Enterprise

NetApp Backup and Recovery peut désormais sauvegarder les volumes locaux FlexVol et FlexGroup configurés à l'aide des modes de protection SnapLock Compliance ou SnapLock Enterprise . Vos clusters doivent exécuter ONTAP 9.14 ou une version ultérieure pour cette prise en charge. La sauvegarde des volumes FlexVol à l'aide du mode SnapLock Enterprise est prise en charge depuis la version 9.11.1 ONTAP . Les versions antérieures ONTAP ne fournissent aucune prise en charge pour la sauvegarde des volumes de protection SnapLock .

Consultez la liste complète des volumes pris en charge dans le "En savoir plus sur NetApp Backup and Recovery" .

Indexation du processus de recherche et de restauration sur la page Volumes

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. La page Volumes affiche désormais l'état de l'indexation :

- Indexé : Les volumes ont été indexés.
- En cours
- Non indexé
- Indexation interrompue

- Erreur
- Non activé

27 septembre 2024

Cette version de NetApp Backup and Recovery inclut les mises à jour suivantes.

Prise en charge de Podman sur RHEL 8 ou 9 avec navigation et restauration

NetApp Backup and Recovery prend désormais en charge les restaurations de fichiers et de dossiers sur les versions 8 et 9 de Red Hat Enterprise Linux (RHEL) à l'aide du moteur Podman. Ceci s'applique à la méthode de NetApp Backup and Recovery .

L'agent de console version 3.9.40 prend en charge certaines versions de Red Hat Enterprise Linux versions 8 et 9 pour toute installation manuelle du logiciel de l'agent de console sur un hôte RHEL 8 ou 9, quel que soit l'emplacement en plus des systèmes d'exploitation mentionnés dans le "exigences de l'hôte" . Ces nouvelles versions de RHEL nécessitent le moteur Podman au lieu du moteur Docker. Auparavant, NetApp Backup and Recovery présentait deux limitations lors de l'utilisation du moteur Podman. Ces limitations ont été supprimées.

"En savoir plus sur la restauration des données ONTAP à partir de fichiers de sauvegarde".

L'indexation plus rapide du catalogue améliore la recherche et la restauration

Cette version inclut un index de catalogue amélioré qui termine l'indexation de base beaucoup plus rapidement. Une indexation plus rapide vous permet d'utiliser la fonction Rechercher et restaurer plus rapidement.

"En savoir plus sur la restauration des données ONTAP à partir de fichiers de sauvegarde".

Limitations connues avec NetApp Backup and Recovery pour les volumes ONTAP

Les plates-formes, appareils ou fonctionnalités qui ne fonctionnent pas ou ne fonctionnent pas bien avec cette version sont répertoriés ici. Lisez attentivement ces limitations.

- NetApp Backup and Recovery peut sauvegarder Cloud Volumes ONTAP dans un magasin d'objets dans les régions AWS Chine (y compris Pékin et Ningxia) ; cependant, vous devrez peut-être d'abord modifier manuellement les stratégies d'identité et d'accès.

  Pour plus de détails sur la création d'un agent de console dans AWS, reportez-vous à "Installation d'un agent de console dans AWS" .

  Pour plus de détails, reportez-vous à l'article de blog "Blog sur les fonctionnalités de NetApp Backup and Recovery - mai 2023" .

- NetApp Backup and Recovery ne prend pas en charge les régions Microsoft Azure Chine.

  Pour plus de détails sur la création d'un agent de console dans Azure, reportez-vous à "Installation d'un agent de console dans Azure" .

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

Limitations de réplication pour les volumes ONTAP

- Vous ne pouvez sélectionner qu'un seul volume FlexGroup à la fois pour la réplication. Vous devrez activer les sauvegardes séparément pour chaque volume FlexGroup .

  Il n'y a aucune limitation pour les volumes FlexVol : vous pouvez sélectionner tous les volumes FlexVol de votre système et attribuer les mêmes politiques de sauvegarde.

- La fonctionnalité suivante est prise en charge dans "NetApp Replication" , mais pas lors de l'utilisation de la fonction de réplication de NetApp Backup and Recovery:
  - Il n'existe aucune prise en charge pour une configuration en cascade où la réplication se produit du volume A vers le volume B et du volume B vers le volume C. La prise en charge inclut la réplication du volume A vers le volume B.
  - Il n'existe aucune prise en charge de la réplication des données vers et depuis les systèmes FSx pour ONTAP .
  - Il n'existe aucune prise en charge pour la création d'une réplication unique d'un volume.
- Lors de la création de réplications à partir de systèmes ONTAP locaux, si la version ONTAP sur le système Cloud Volumes ONTAP cible est 9.8, 9.9 ou 9.11, seules les stratégies de coffre-fort miroir sont autorisées.

Limitations de sauvegarde sur objet pour les volumes ONTAP

- Lors de la sauvegarde des données, NetApp Backup and Recovery ne conservera pas le chiffrement de volume NetApp (NVE). Cela signifie que les données chiffrées sur le volume NVE seront déchiffrées pendant le transfert des données vers la destination et le chiffrement ne sera pas conservé.

  Pour une explication sur ces types de cryptage, reportez-vous àhttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Présentation de la configuration du chiffrement de volume NetApp"^] .

- Si les snapshots de rétention à long terme sont activés sur un volume de destination SnapMirror à l'aide de la planification de la stratégie SnapMirror , les snapshots sont créés directement sur le volume de destination. Dans ce cas, vous ne devez pas sauvegarder ces volumes à l'aide de NetApp Backup and Recovery, car ces snapshots ne seront pas déplacés vers le stockage d'objets.
- Lors de la sauvegarde des données, NetApp Backup and Recovery ne conservera pas le chiffrement de volume NetApp (NVE). Cela signifie que les données chiffrées sur le volume NVE seront déchiffrées pendant le transfert des données vers la destination et le chiffrement ne sera pas conservé.

  Pour une explication sur ces types de cryptage, reportez-vous àhttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Présentation de la configuration du chiffrement de volume NetApp"^] .

- Si les snapshots de rétention à long terme sont activés sur un volume de destination SnapMirror à l'aide de la planification de la stratégie SnapMirror , les snapshots sont créés directement sur le volume de destination. Dans ce cas, vous ne devez pas sauvegarder ces volumes à l'aide de NetApp Backup and Recovery, car ces snapshots ne seront pas déplacés vers le stockage d'objets.
- Lorsque vous créez ou modifiez une politique de sauvegarde alors qu'aucun volume n'est attribué à la politique, le nombre de sauvegardes conservées peut être au maximum de 1 018. Après avoir attribué des volumes à la politique, vous pouvez modifier la politique pour créer jusqu'à 4 000 sauvegardes.
- Lors de la sauvegarde des volumes de protection des données (DP) :

    - Relations avec les étiquettes SnapMirror `app_consistent` et `all_source_snapshot` ne sera pas sauvegardé dans le cloud.
    - Si vous créez des copies locales de snapshots sur le volume de destination SnapMirror (quelles que soient les étiquettes SnapMirror utilisées), ces snapshots ne seront pas déplacés vers le cloud en tant que sauvegardes. À ce stade, vous devrez créer une politique de snapshot avec les étiquettes souhaitées sur le volume DP source afin que NetApp Backup and Recovery les sauvegarde.
- Les sauvegardes de volume FlexGroup ne peuvent pas être déplacées vers un stockage d'archivage.
- Les sauvegardes de volume FlexGroup peuvent utiliser la protection DataLock et Ransomware si le cluster exécute ONTAP 9.13.1 ou une version ultérieure.
- La sauvegarde du volume SVM-DR est prise en charge avec les restrictions suivantes :
    - Les sauvegardes sont prises en charge uniquement à partir du serveur secondaire ONTAP .
    - La politique de snapshot appliquée au volume doit être l'une des politiques reconnues par NetApp Backup and Recovery, notamment quotidienne, hebdomadaire, mensuelle, etc. La politique par défaut « sm_created » (utilisée pour **Mettre en miroir tous les snapshots**) n'est pas reconnue et le volume DP ne sera pas affiché dans la liste des volumes pouvant être sauvegardés.
    - SVM-DR et la sauvegarde et la récupération de volume fonctionnent de manière totalement indépendante lorsque la sauvegarde est effectuée à partir de la source ou de la destination. La seule restriction est que SVM-DR ne réplique pas la relation cloud SnapMirror . Dans le scénario DR, lorsque le SVM est mis en ligne dans l'emplacement secondaire, vous devez mettre à jour manuellement la relation cloud SnapMirror .
- Prise en charge de MetroCluster :
    - Lorsque vous utilisez ONTAP 9.12.1 GA ou une version ultérieure, la sauvegarde est prise en charge lors de la connexion au système principal. L'ensemble de la configuration de sauvegarde est transféré vers le système secondaire afin que les sauvegardes vers le cloud se poursuivent automatiquement après le basculement. Vous n'avez pas besoin de configurer une sauvegarde sur le système secondaire (en fait, vous n'êtes pas autorisé à le faire).
    - Lorsque vous utilisez ONTAP 9.12.0 et versions antérieures, la sauvegarde est prise en charge uniquement à partir du système secondaire ONTAP .
    - Les sauvegardes des volumes FlexGroup ne sont pas prises en charge pour le moment.
- La sauvegarde de volume ad hoc à l'aide du bouton **Sauvegarder maintenant** n'est pas prise en charge sur les volumes de protection des données.
- Les configurations SM-BC ne sont pas prises en charge.
- ONTAP ne prend pas en charge la répartition des relations SnapMirror d'un seul volume vers plusieurs magasins d'objets ; par conséquent, cette configuration n'est pas prise en charge par NetApp Backup and Recovery.
- Le mode WORM/Compliance sur un magasin d'objets est actuellement pris en charge sur Amazon S3, Azure et StorageGRID . Il s'agit de la fonctionnalité DataLock et elle doit être gérée à l'aide des paramètres NetApp Backup and Recovery , et non à l'aide de l'interface du fournisseur de cloud.

Restaurer les limitations pour les volumes ONTAP

Ces limitations s'appliquent à la fois aux méthodes de recherche et de restauration et de navigation et de restauration de fichiers et de dossiers, sauf indication contraire spécifique.

- Parcourir et restaurer peut restaurer jusqu'à 100 fichiers individuels à la fois.
- Search & Restore peut restaurer 1 fichier à la fois.

- Lorsque vous utilisez ONTAP 9.13.0 ou une version ultérieure, Parcourir et restaurer et Rechercher et restaurer peuvent restaurer un dossier avec tous les fichiers et sous-dossiers qu'il contient.

  Lorsque vous utilisez une version d' ONTAP supérieure à 9.11.1 mais antérieure à 9.13.0, l'opération de restauration ne peut restaurer que le dossier sélectionné et les fichiers de ce dossier - aucun sous-dossier ni fichier dans les sous-dossiers n'est restauré.

  Lors de l'utilisation d'une version d' ONTAP antérieure à 9.11.1, la restauration de dossiers n'est pas prise en charge.

- La restauration de répertoire/dossier est prise en charge pour les données qui résident dans le stockage d'archives uniquement lorsque le cluster exécute ONTAP 9.13.1 et versions ultérieures.
- La restauration de répertoire/dossier est prise en charge pour les données protégées à l'aide de DataLock uniquement lorsque le cluster exécute ONTAP 9.13.1 et versions ultérieures.
- La restauration de répertoire/dossier n'est actuellement pas prise en charge à partir de réplications et/ou de snapshots locaux.
- La restauration des volumes FlexGroup vers les volumes FlexVol ou des volumes FlexVol vers les volumes FlexGroup n'est pas prise en charge.
- Le fichier en cours de restauration doit utiliser la même langue que celle du volume de destination. Vous recevrez un message d'erreur si les langues ne sont pas les mêmes.
- La priorité de restauration *Élevée* n'est pas prise en charge lors de la restauration de données à partir du stockage d'archivage Azure vers les systèmes StorageGRID .
- Si vous sauvegardez un volume DP, puis décidez de rompre la relation SnapMirror avec ce volume, vous ne pouvez pas restaurer les fichiers sur ce volume, sauf si vous supprimez également la relation SnapMirror ou si vous inversez la direction de SnapMirror .
- Limitations de la restauration rapide :
  - L'emplacement de destination doit être un système Cloud Volumes ONTAP utilisant ONTAP 9.13.0 ou supérieur.
  - Cette option n'est pas prise en charge avec les sauvegardes situées dans un stockage archivé.
  - Les volumes FlexGroup sont pris en charge uniquement si le système source à partir duquel la sauvegarde cloud a été créée exécutait ONTAP 9.12.1 ou une version ultérieure.
  - Les volumes SnapLock sont pris en charge uniquement si le système source à partir duquel la sauvegarde cloud a été créée exécutait ONTAP 9.11.0 ou une version ultérieure.

Limitations connues avec NetApp Backup and Recovery pour les charges de travail Microsoft SQL Server

Les plates-formes, appareils ou fonctionnalités qui ne fonctionnent pas ou ne fonctionnent pas bien avec cette version sont répertoriés ici. Lisez attentivement ces limitations.

Prise en charge du cycle de vie des clones

- Le clonage à partir du stockage d'objets n'est pas pris en charge.
- Les opérations de clonage en masse ne sont pas prises en charge pour les clones à la demande.
- Le choix des groupes I n'est pas pris en charge.

- Le choix des options QOS (débit maximal) n'est pas pris en charge.

Mode de déploiement standard uniquement

Cette version de NetApp Backup and Recovery fonctionne uniquement en mode de déploiement standard, et non en mode restreint ou privé.

Restriction du nom du cluster Windows

Le nom du cluster Windows ne peut pas contenir de caractère de soulignement (_).

Problèmes de migration de SnapCenter

La migration des ressources de SnapCenter vers NetApp Backup and Recovery présente les limitations suivantes.

Pour plus de détails sur la façon dont les politiques SnapCenter migrent vers les politiques de NetApp Backup and Recovery , consultez"Stratégies dans SnapCenter comparées à celles de NetApp Backup and Recovery" .

Limitations du groupe de ressources

Si toutes les ressources d'un groupe de ressources sont protégées et que l'une de ces ressources est également protégée en dehors du groupe de ressources, la migration depuis SnapCenter est bloquée.

Solution de contournement : protégez la ressource soit dans un groupe de ressources, soit seule, mais pas dans les deux.

Les ressources avec plusieurs politiques utilisant le même niveau de planification ne sont pas prises en charge

Vous ne pouvez pas attribuer plusieurs stratégies utilisant le même niveau de planification (par exemple, horaire, quotidien, hebdomadaire, etc.) à une ressource. NetApp Backup and Recovery n'importera pas ces ressources depuis SnapCenter.

Solution de contournement : attachez une seule stratégie utilisant le même niveau de planification à une ressource.

Les politiques horaires doivent commencer au début de l'heure

Si vous disposez d'une stratégie SnapCenter qui se répète toutes les heures mais n'utilise pas d'intervalles au début de l'heure, NetApp Backup and Recovery n'importera pas la ressource. Par exemple, les politiques avec des horaires de 1 h 30, 2 h 30, 3 h 30, etc. ne sont pas prises en charge, tandis que les politiques avec des horaires de 1 h 00, 2 h 00, 3 h 00, etc. sont prises en charge.

Solution de contournement : utilisez une stratégie qui se répète par intervalles d'une heure en commençant au début de l'heure.

Les politiques quotidiennes et mensuelles attachées à une ressource ne sont pas prises en charge

Si une politique SnapCenter se répète à la fois à des intervalles de jour et de mois, NetApp Backup and Recovery n'importera pas la politique.

Par exemple, vous ne pouvez pas attacher une politique quotidienne (avec une durée inférieure ou égale à 7 jours ou supérieure à 7 jours) à une ressource et attacher également une politique mensuelle à la même

ressource.

Solution de contournement : utilisez une stratégie qui utilise un intervalle quotidien ou mensuel, mais pas les deux.

Politiques de sauvegarde à la demande non migrées

NetApp Backup and Recovery n'importe pas les politiques de sauvegarde à la demande depuis SnapCenter.

Les politiques de sauvegarde des journaux uniquement n'ont pas été migrées

NetApp Backup and Recovery n'importe pas les stratégies de sauvegarde de journaux uniquement à partir de SnapCenter. Si une politique SnapCenter inclut des sauvegardes de journaux uniquement, NetApp Backup and Recovery n'importera pas la ressource.

Solution de contournement : utilisez une stratégie dans SnapCenter qui utilise plus que de simples sauvegardes de journaux uniquement.

Cartographie de l'hôte

SnapCenter ne dispose pas de clusters de stockage de cartes ou de SVM pour les ressources vers les hôtes, mais NetApp Backup and Recovery en dispose. Le cluster ONTAP ou SVM sur site ne sera pas mappé à un hôte dans les versions d'aperçu de NetApp Backup and Recovery . De plus, la NetApp Console ne prend pas en charge les SVM.

Solution de contournement : avant d'importer des ressources depuis SnapCenter, créez un système dans NetApp Backup and Recovery pour tous les systèmes de stockage ONTAP locaux enregistrés dans SnapCenter local. Ensuite, importez les ressources de ce cluster depuis SnapCenter dans NetApp Backup and Recovery.

Horaires non à intervalles de 15 minutes

Si vous disposez d'une planification de stratégie SnapCenter qui démarre à une certaine heure et se répète à des intervalles autres que ceux de 15 minutes, NetApp Backup and Recovery n'importera pas la planification.

Solution de contournement : utilisez SnapCenter pour ajuster la stratégie afin qu'elle se répète à des intervalles de 15 minutes.

Prise en charge limitée des logiciels de gestion de la virtualisation

Lorsque vous protégez les charges de travail KVM, NetApp Backup and Recovery ne prend pas en charge la découverte des charges de travail KVM lorsque le logiciel de gestion de virtualisation tel qu'Apache CloudStack ou Red Hat OpenShift Virtualization est utilisé.

Limitations connues avec NetApp Backup and Recovery pour les charges de travail VMware

Les plates-formes, appareils ou fonctionnalités qui ne fonctionnent pas ou ne fonctionnent pas bien avec cette version sont répertoriés ici. Lisez attentivement ces limitations.

Les actions suivantes ne sont pas prises en charge dans la version préliminaire des charges de travail VMware dans NetApp Backup and Recovery:

- Monter
- Démonter
- Restaurer vers un autre emplacement
- Restaurer VMDK
- Attacher VMDK
- Détacher VMDK
- Prise en charge de vVol
- Prise en charge NVMe
- Intégration de courrier électronique
- Modifier la politique
- Modifier le groupe de protection
- Prise en charge du contrôle d'accès basé sur les rôles (RBAC)

Limitations connues de NetApp Backup and Recovery pour les charges de travail Hyper-V

Les plates-formes, appareils ou fonctionnalités qui ne fonctionnent pas ou ne fonctionnent pas bien avec cette version sont répertoriés ici. Lisez attentivement ces limitations.

Actions non prises en charge

Les actions suivantes ne sont pas prises en charge dans la version d'aperçu privée des charges de travail Hyper-V dans NetApp Backup and Recovery:

- Créer des groupes de ressources
- Répartition des disques (sur plusieurs partages CIFS)
- Protéger les machines virtuelles via SAN
- Modifier les groupes de protection
- Protégez les hôtes Hyper-V mis en cluster à l'aide de System Center Virtual Machine Manager (SCVMM)

Comptes de NetApp Console hérités non pris en charge

Les comptes de NetApp Console hérités ne prennent pas en charge les fonctionnalités requises pour protéger les charges de travail Hyper-V. Vérifiez si vous utilisez un compte hérité dans l'interface utilisateur Web de la console. Si vous disposez d'un compte de console hérité, créez un nouveau compte avant de protéger les charges de travail Hyper-V.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Administration > Identité et accès**.
2. Sous **Organisation**, vérifiez si un **ID de compte** est affiché à côté de l'ID de l'organisation.

   Si un **ID de compte** s'affiche, vous utilisez un compte hérité.

3. Si vous utilisez un compte hérité, procédez comme suit :
    a. Déconnectez-vous de la console, puis accédez à la "Page de connexion à la console" .
    b. Sélectionnez **S'inscrire** pour créer un nouveau compte.

Limitations connues de NetApp Backup and Recovery pour les charges de travail KVM

Les plates-formes, appareils ou fonctionnalités qui ne fonctionnent pas ou ne fonctionnent pas bien avec cette version sont répertoriés ici. Lisez attentivement ces limitations.

Les actions et configurations suivantes ne sont pas prises en charge dans la version d'aperçu privée des charges de travail KVM dans NetApp Backup and Recovery:

Actions non prises en charge

Les actions suivantes ne sont pas prises en charge dans la version d'aperçu privée :

- Cloner, monter ou démonter des machines virtuelles
- Restaurer les machines virtuelles vers un autre emplacement
- Protéger les machines virtuelles stockées sur SAN
- Protéger les applications
- Modifier les groupes de protection
- Créer des groupes de protection à l'aide de machines virtuelles provenant de plusieurs hôtes KVM
- Créer des sauvegardes définies par l'utilisateur (seules les sauvegardes lancées à partir de la NetApp Console sont prises en charge)

Configurations non prises en charge

Les configurations suivantes ne sont pas prises en charge :

- Contrôle d'accès basé sur les rôles (RBAC)
- Disques directement connectés à l'hôte KVM
- Disques répartis sur plusieurs points de montage ou partages NFS
- Format de disque RAW
- Types de pools de stockage autres que NetFS (seul NetFS est pris en charge)

Comptes de NetApp Console hérités non pris en charge

Les comptes de NetApp Console hérités ne prennent pas en charge les fonctionnalités requises pour protéger les charges de travail KVM. Vérifiez si vous utilisez un compte hérité dans l'interface utilisateur Web de la console. Si vous disposez d'un compte de console hérité, créez un nouveau compte avant de protéger les charges de travail KVM.

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Administration > Identité et accès**.

2. Sous **Organisation**, vérifiez si un **ID de compte** est affiché à côté de l'ID de l'organisation.

   Si un **ID de compte** s'affiche, vous utilisez un compte hérité.

3. Si vous utilisez un compte hérité, procédez comme suit :
   a. Déconnectez-vous de la console, puis accédez à la "Page de connexion à la console" .
   b. Sélectionnez **S'inscrire** pour créer un nouveau compte.

Limitations connues avec NetApp Backup and Recovery pour les charges de travail Oracle

Les plates-formes, appareils ou fonctionnalités qui ne fonctionnent pas ou ne fonctionnent pas bien avec cette version sont répertoriés ici. Lisez attentivement ces limitations.

Les actions suivantes ne sont pas prises en charge dans la version d'aperçu privée des charges de travail Oracle Database dans NetApp Backup and Recovery:

- Sauvegarde hors ligne
- Cloner
- Configuration ASM
- Protection des bases de données stockées sur SAN

Oracle Database est pris en charge uniquement en tant que déploiement autonome à l'aide de NFS dans la version d'aperçu privée des charges de travail Oracle.

Commencer

En savoir plus sur NetApp Backup and Recovery

NetApp Backup and Recovery est un service de données qui fournit une protection des données efficace, sécurisée et rentable pour toutes vos charges de travail ONTAP , y compris les volumes, les bases de données, les machines virtuelles et les charges de travail Kubernetes.

La prise en charge de la sauvegarde et de la récupération est déjà intégrée à tous les systèmes ONTAP , il n'est donc pas nécessaire de recourir à du matériel supplémentaire, à des licences logicielles ou à des passerelles multimédias. Cela rend les opérations de sauvegarde simples et rentables. La console NetApp simplifie la mise en œuvre de toute stratégie de sauvegarde, y compris la gamme complète de variantes de sauvegarde 3-2-1, sans avoir besoin de plusieurs gestionnaires de ressources ou de personnel spécialisé.

> La documentation sur la protection des charges de travail VMware, KVM, Hyper-V et Kubernetes est fournie sous forme d'aperçu technologique. 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.

Ce que vous pouvez faire avec NetApp Backup and Recovery

Utilisez NetApp Backup and Recovery pour atteindre les objectifs suivants :

- * Charges de travail de volume ONTAP * :
  - Créez des instantanés locaux, répliquez-les vers un stockage secondaire et sauvegardez les volumes ONTAP à partir des systèmes ONTAP locaux ou Cloud Volumes ONTAP vers le stockage d'objets dans votre compte cloud public ou privé.
  - Créez des sauvegardes incrémentielles permanentes au niveau des blocs qui sont stockées sur un autre cluster ONTAP et dans un stockage d'objets dans le cloud.
  - Utilisez NetApp Backup and Recovery avec SnapCenter.
  - Se référer à"Protéger les volumes ONTAP" .
- **Charges de travail Microsoft SQL Server**:
  - Sauvegardez les instances et bases de données Microsoft SQL Server à partir ONTAP sur site, de Cloud Volumes ONTAP ou Amazon FSx for NetApp ONTAP.
  - Restaurer les bases de données Microsoft SQL Server.
  - Cloner des bases de données Microsoft SQL Server.
  - Utilisez NetApp Backup and Recovery sans SnapCenter.
  - Se référer à"Protégez les charges de travail Microsoft SQL Server" .
- **Charges de travail VMware (Aperçu avec nouvelle interface utilisateur sans SnapCenter Plug-in for VMware vSphere)**:
  - Protégez vos machines virtuelles et banques de données VMware avec NetApp Backup and Recovery.
  - Sauvegardez les charges de travail VMware sur Amazon Web Services S3 ou StorageGRID (pour l'aperçu).
  - Restaurez les données VMware du cloud vers le vCenter local.

- Utilisez NetApp Backup and Recovery sans SnapCenter Plug-in for VMware vSphere.
- Se référer à"Protégez les charges de travail VMware" .

- **Charges de travail VMware (avec SnapCenter Plug-in for VMware vSphere)** :
  - Sauvegardez les machines virtuelles et les banques de données sur Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform et StorageGRID et restaurez les machines virtuelles sur l'hôte SnapCenter Plug-in for VMware vSphere sur site.
  - Restaurez les données de la machine virtuelle depuis le cloud vers le vCenter local avec NetApp Backup and Recovery. Vous pouvez restaurer la machine virtuelle exactement au même emplacement à partir duquel la sauvegarde a été effectuée ou vers un autre emplacement.
  - Utilisez NetApp Backup and Recovery avec le SnapCenter Plug-in for VMware vSphere.
  - Se référer à"Protégez les charges de travail VMware" .
- **Charges de travail KVM (Aperçu)**:
  - Sauvegarder et restaurer des machines virtuelles
  - Sauvegarder les pools de stockage KVM
  - Utiliser des groupes de protection pour gérer les tâches de sauvegarde
  - Se référer à"Protégez les charges de travail KVM" .
- **Charges de travail Hyper-V (Aperçu)**:
  - Sauvegarder et restaurer des machines virtuelles
  - Utiliser des groupes de protection pour gérer les tâches de sauvegarde
  - Se référer à"Protégez les charges de travail Hyper-V" .
- **Charges de travail Oracle (Aperçu)**:
  - Sauvegarder et restaurer les bases de données et les journaux
  - Utiliser des groupes de protection pour gérer les tâches de sauvegarde
  - Créer des politiques pour gérer les sauvegardes de bases de données et de journaux
  - Protéger une base de données avec une architecture de sauvegarde 3-2-1
  - Configurer la conservation des sauvegardes
  - Monter et démonter les sauvegardes ARCHIVELOG
  - Se référer à"Protégez les charges de travail Oracle" .
- **Charges de travail Kubernetes (Aperçu)**:
  - Gérez et protégez vos applications et ressources Kubernetes en un seul endroit.
  - Utilisez des politiques de protection pour structurer vos sauvegardes incrémentielles.
  - Restaurez les applications et les ressources sur les mêmes clusters et espaces de noms ou sur des clusters et espaces de noms différents.
  - Utilisez NetApp Backup and Recovery sans SnapCenter.
  - Se référer à"Protégez les charges de travail Kubernetes" .

Avantages de l'utilisation de NetApp Backup and Recovery

NetApp Backup and Recovery offre les avantages suivants :

- **Efficace** : NetApp Backup and Recovery effectue une réplication incrémentielle permanente au niveau des blocs, ce qui réduit considérablement la quantité de données répliquées et stockées. Cela permet de minimiser le trafic réseau et les coûts de stockage.
- **Sécurisé** : NetApp Backup and Recovery crypte les données en transit et au repos, et utilise des protocoles de communication sécurisés pour protéger vos données.
- **Rentable** : NetApp Backup and Recovery utilise les niveaux de stockage les moins chers disponibles dans votre compte cloud, ce qui contribue à réduire les coûts.
- **Automatisé** : NetApp Backup and Recovery génère automatiquement des sauvegardes selon une planification prédéfinie, ce qui contribue à garantir la protection de vos données.
- **Flexible** : NetApp Backup and Recovery vous permet de restaurer des données sur le même système ou sur un système différent, ce qui offre une flexibilité dans la récupération des données.

Coût

NetApp ne vous facture pas l'utilisation de la version d'essai. Cependant, vous êtes responsable des coûts associés aux ressources cloud que vous utilisez, tels que les coûts de stockage et de transfert de données.

Il existe deux types de coûts associés à l'utilisation de la fonctionnalité de sauvegarde sur objet de NetApp Backup and Recovery avec les systèmes ONTAP :

- Frais de ressources
- Frais de service

La création de copies instantanées ou de volumes répliqués est gratuite, à l'exception de l'espace disque requis pour stocker les copies instantanées et les volumes répliqués.

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. endif::gcp[]
  - 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 sauvegardés sur le stockage d'objets. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

Pour Microsoft SQL Server, des frais s'appliquent lorsque vous lancez la réplication de snapshots vers une cible ONTAP secondaire ou un stockage d'objets.

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. Lire leLicences section pour plus de détails.

Licences

NetApp Backup and Recovery est disponible en version d'essai gratuite. Vous pouvez utiliser le service sans clé de licence pendant une durée limitée.

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

- **Apportez votre propre licence (BYOL)** : une licence achetée auprès de NetApp qui peut être utilisée avec n'importe quel fournisseur de cloud.
- **Payez à l'utilisation (PAYGO)** : un abonnement horaire sur la place de marché de votre fournisseur de 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 de copies instantanées 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 configurer des licences".

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.

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 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). endif::aws[]

Lorsque vous utilisez Azure, deux contrats annuels sont disponibles pour 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). endif::azure[]

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 . endif::gcp[]

Sources de données, systèmes et cibles de sauvegarde pris en charge

Sources de données de charge de travail prises en charge

NetApp Backup and Recovery protège les charges de travail suivantes :

- Volumes ONTAP
- Instances et bases de données Microsoft SQL Server pour NFS physique, VMware Virtual Machine File System (VMFS) et VMware Virtual Machine Disk (VMDK)
- Machines virtuelles et banques de données VMware
- Charges de travail KVM (Aperçu)
- Charges de travail Hyper-V (Aperçu)
- Charges de travail Kubernetes (Aperçu)

Systèmes pris en charge

- SAN ONTAP sur site (protocole iSCSI) et NAS (utilisant les protocoles NFS et CIFS) avec ONTAP version 9.8 et supérieure
- Cloud Volumes ONTAP 9.8 ou supérieur pour AWS (utilisant SAN et NAS)
- Cloud Volumes ONTAP 9.8 ou supérieur pour Microsoft Azure (utilisant SAN et NAS)
- Amazon FSx for NetApp ONTAP

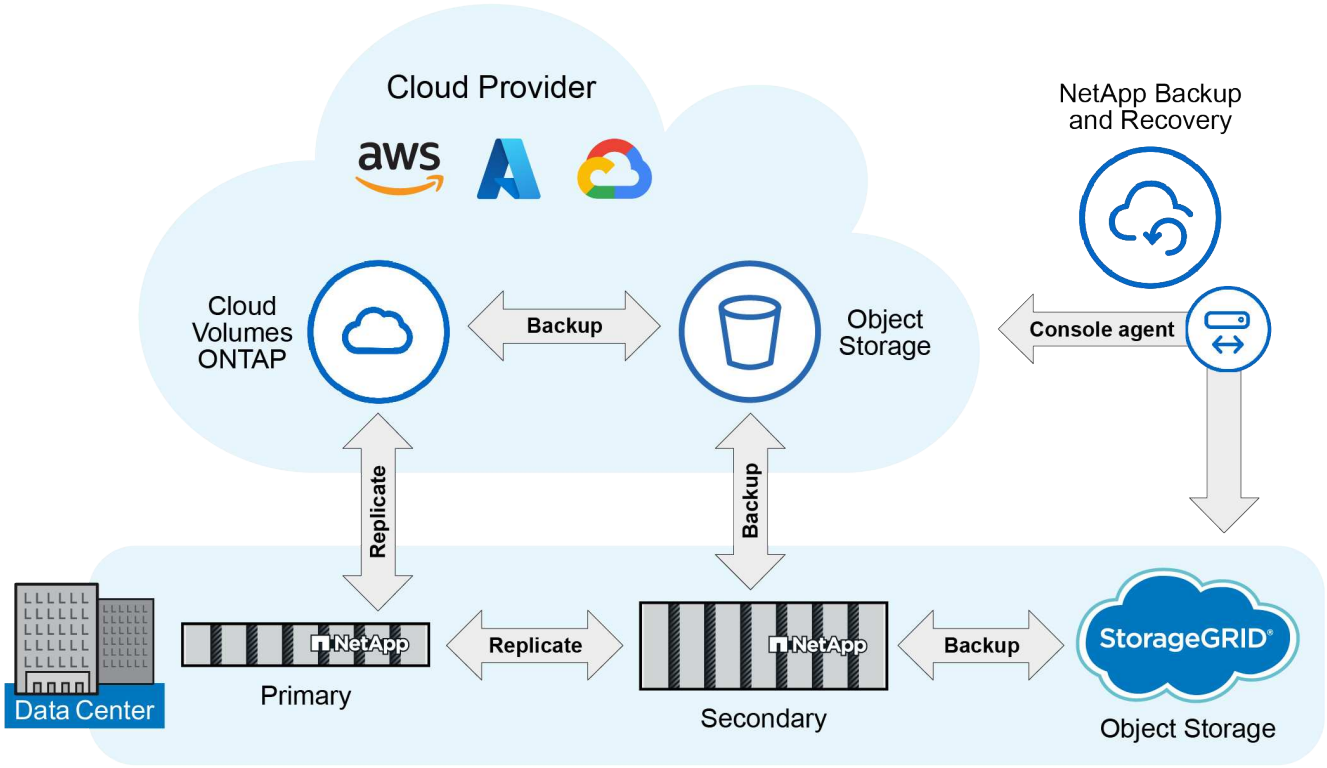
Cibles de sauvegarde prises en charge

- Amazon Web Services (AWS) S3
- Microsoft Azure Blob (non disponible pour les charges de travail VMware en version préliminaire)
- StorageGRID
- ONTAP S3 (non disponible pour les charges de travail VMware en version préliminaire)

Comment fonctionne la NetApp Backup and Recovery

Lorsque vous activez NetApp Backup and Recovery, le service effectue une sauvegarde complète de vos données. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles. Cela permet de maintenir le trafic réseau à un minimum.

L'image suivante montre la relation entre les composants.



Le stockage primaire vers le stockage d'objets est également pris en charge, et pas seulement du stockage secondaire vers le stockage d'objets.

Où résident les sauvegardes dans les emplacements de stockage d'objets

Les copies de sauvegarde sont stockées dans un magasin d'objets que la NetApp Console crée dans votre compte cloud. Il existe un magasin d'objets par cluster ou 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 NetApp Console permet la "Fonctionnalité d'accès public au bloc Amazon S3" sur le bucket S3. endif::aws[]
- Dans Azure, la NetApp 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.

endif::azure[]

- Dans StorageGRID, la console utilise un compte de stockage existant pour le bucket de magasin d'objets.
- Dans ONTAP S3, la console utilise un compte utilisateur existant pour le bucket S3.

Les copies de sauvegarde sont associées à votre organisation NetApp Console

Les copies de sauvegarde sont associées à l'organisation de la NetApp Console dans laquelle réside l'agent de la console. "En savoir plus sur l'identité et l'accès à la NetApp Console" .

Si vous disposez de plusieurs agents de console dans la même organisation de NetApp Console , chaque agent de console affiche la même liste de sauvegardes.

Termes qui pourraient vous aider avec NetApp Backup and Recovery

Il pourrait être utile de comprendre certains termes liés à la protection.

- **Protection** : La protection dans NetApp Backup and Recovery signifie garantir que les snapshots et les sauvegardes immuables se produisent régulièrement dans un domaine de sécurité différent à l'aide de politiques de protection.
- **Charge de travail** : une charge de travail dans NetApp Backup and Recovery peut inclure des volumes ONTAP , des instances et des bases de données Microsoft SQL Server ; des machines virtuelles et des banques de données VMware ; ou des clusters et des applications Kubernetes.

Conditions préalables à la NetApp Backup and Recovery

Commencez à utiliser NetApp Backup and Recovery en vérifiant l'état de préparation de votre environnement opérationnel, de l'agent NetApp Console et du compte NetApp Console . Pour utiliser NetApp Backup and Recovery, vous aurez besoin de ces prérequis.

Prérequis pour ONTAP 9.8 et versions ultérieures

Une licence ONTAP One doit être activée sur l'instance ONTAP locale.

Conditions préalables pour les sauvegardes sur le stockage d'objets

Pour utiliser le stockage d'objets comme cibles de sauvegarde, vous avez besoin d'un compte avec AWS S3, Microsoft Azure Blob, StorageGRID ou ONTAP et des autorisations d'accès appropriées configurées.

- "Protégez vos données de volume ONTAP"

Exigences pour la protection des charges de travail Microsoft SQL Server

Pour utiliser NetApp Backup and Recovery pour les charges de travail Microsoft SQL Server, vous avez besoin des prérequis suivants en matière de système hôte, d'espace et de dimensionnement.

Article	Exigences
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .
Versions de Microsoft SQL Server	Les versions 2012 et ultérieures sont prises en charge pour VMware Virtual Machine File System (VMFS) et VMware Virtual Machine Disk (VMDK) NFS.
Version du serveur SnapCenter	La version 5.0 ou supérieure de SnapCenter Server est requise si vous souhaitez importer vos données existantes de SnapCenter dans 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. Voir"Conditions préalables à l'importation de ressources depuis SnapCenter" .
RAM minimale pour le plug-in sur l'hôte SQL Server	1 Go
Espace minimum d'installation et de journalisation pour le plug-in sur l'hôte SQL Server	5 Go Allouez suffisamment d'espace disque et surveillez la consommation de stockage par le dossier des journaux. L'espace journal requis varie en fonction du nombre de sauvegardes effectuées et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace, les journaux ne seront pas créés pour les opérations.
Logiciels requis	• Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs) • PowerShell 7.4.2 Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .

Exigences pour la protection des charges de travail VMware

Vous avez besoin d'exigences spécifiques pour découvrir et protéger vos charges de travail VMware.

Support logiciel

- Les banques de données NFS et VMFS sont prises en charge. Les vVols ne sont pas pris en charge.
- Versions NFS prises en charge : NFS 3 et NFS 4.1
- Versions de VMware ESXi Server prises en charge : 7.0U1 et versions ultérieures
- Versions VMware vCenter vSphere prises en charge : 7.0U1 et supérieures
- Adresses IP : IPv4 et IPv6
- VMware TLS : 1.2, 1.3

Exigences de connexion et de port pour la protection des charges de travail VMware

Type de port	Port préconfiguré
Port du serveur VMware ESXi	443 (HTTPS), bidirectionnel. La fonction de restauration de fichiers invités utilise ce port.
Port du serveur VMware vSphere vCenter	Si vous protégez des machines virtuelles vVol, vous devez utiliser le port 443.
Cluster de stockage ou port de VM de stockage	443 (HTTPS), bidirectionnel. 80 (HTTP), bidirectionnel. Ce port est utilisé pour la communication entre l'appliance virtuelle et la machine virtuelle de stockage ou le cluster contenant la machine virtuelle de stockage.

Exigences de contrôle d'accès basé sur les rôles (RBAC) pour la protection des charges de travail VMware

Le compte administrateur vCenter doit disposer des privilèges vCenter requis.

Pour obtenir la liste des privilèges vCenter nécessaires, consultez "SnapCenter Plug-in for VMware vSphere privilèges vCenter requis" .

Exigences pour la protection des charges de travail KVM

Vous avez besoin d'exigences spécifiques pour découvrir et protéger les machines virtuelles KVM.

- Une distribution Linux moderne exécutant la version du noyau 5.14.0-503.22.1.el9_5.x86_64 (long terme) ou ultérieure
- Assurez-vous que le trafic entrant vers le port 22 est autorisé depuis l'agent de console vers l'hôte KVM
- Agent invité QEMU version 9.0.0 ou ultérieure
- libvirt version 10.5.0 ou ultérieure

Exigences pour la protection des charges de travail Oracle

Assurez-vous que votre environnement répond à des exigences spécifiques pour découvrir et protéger les ressources Oracle.

- Base de données Oracle :
  - Oracle 19C et 21C sont pris en charge dans un déploiement autonome.
  - La base de données Oracle doit être déployée dans un stockage NetApp ONTAP principal ou secondaire.
- Prise en charge du stockage d'objets :
  - Stockage d'objets Azure
  - Amazon AWS
  - NetApp StorageGRID
  - ONTAP S3

Exigences pour la protection des applications Kubernetes

Vous avez besoin d'exigences spécifiques pour découvrir les ressources Kubernetes et protéger vos applications Kubernetes.

Pour connaître les exigences de la NetApp Console , reportez-vous àDans la NetApp Console .

- Un système ONTAP principal (ONTAP 9.16.1 ou version ultérieure)
- Un cluster Kubernetes - Les distributions et versions Kubernetes prises en charge incluent :
  - Anthos On-Prem (VMware) et Anthos sur bare metal 1.16
  - Kubernetes 1.27 - 1.33
  - OpenShift 4.10 - 4.18
  - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
  - Suse Rancher
- NetApp Trident 24.10 ou version ultérieure
- NetApp Trident Protect 25.07 ou version ultérieure (installé lors de la découverte de la charge de travail Kubernetes)
- NetApp Trident Protect Connector 25.07 ou version ultérieure (installé lors de la découverte de la charge de travail Kubernetes)
  - Assurez-vous que le port TCP 443 n'est pas filtré dans le sens sortant entre le cluster Kubernetes, le connecteur Trident Protect et le proxy Trident Protect.

Exigences pour la protection des charges de travail Hyper-V

Assurez-vous que votre instance Hyper-V répond à des exigences spécifiques pour découvrir et protéger les machines virtuelles.

- Configuration logicielle requise pour l'hôte Windows Server Hyper-V :
  - Éditions Microsoft Hyper-V 2019, 2022 et 2025
  - Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs)
  - PowerShell 7.4.2 ou version ultérieure
  - Assurez-vous que le rôle Host Guardian Service est installé (reportez-vous à la "Documentation de Microsoft Windows Server" pour les instructions)
  - Assurez-vous que le trafic HTTPS bidirectionnel est autorisé pour les ports suivants dans les paramètres du pare-feu Windows :
    - 8144 (plugin NetApp pour Hyper-V)
    - 8145 (plugin NetApp pour Windows)
- Configuration matérielle requise pour l'hôte Hyper-V :
  - Les hôtes autonomes et en cluster FCI sont pris en charge
  - 1 Go de RAM minimum pour le plug-in NetApp Hyper-V sur l'hôte Hyper-V
  - 5 Go minimum d'espace d'installation et de journal pour le plug-in sur l'hôte Hyper-V

Assurez-vous d'allouer suffisamment d'espace disque sur l'hôte Hyper-V pour le dossier des journaux et surveillez régulièrement son utilisation. L'espace requis dépend de la fréquence des sauvegardes et des opérations de protection des données. S'il n'y a pas assez d'espace, les journaux ne seront pas générés.

- Configuration requise NetApp ONTAP :
  - Un système ONTAP principal (ONTAP 9.14.1 ou version ultérieure)
  - Pour les déploiements Hyper-V utilisant des partages CIFS pour stocker les données de la machine virtuelle, assurez-vous que la propriété de partage de disponibilité continue est activée sur le système ONTAP . Reportez-vous à la "Documentation ONTAP" pour les instructions.

Dans la NetApp Console

Assurez-vous que la NetApp Console répond aux exigences suivantes.

- Un utilisateur de la console doit disposer du rôle et des privilèges requis pour effectuer des opérations sur les charges de travail Microsoft SQL Server et Kubernetes. Pour découvrir les ressources, vous devez disposer du rôle NetApp Backup and Recovery de Super administrateur. Voir"Accès aux fonctionnalités de NetApp Backup and Recovery basé sur les rôles" pour plus de détails sur les rôles et les autorisations requis pour effectuer des opérations dans NetApp Backup and Recovery.
- Une organisation de console avec au moins un agent de console actif qui se connecte aux clusters ONTAP locaux ou à Cloud Volumes ONTAP.
- Au moins un système de console avec un cluster NetApp sur site ONTAP ou Cloud Volumes ONTAP .
- Un agent de console

  Se référer à "Apprenez à configurer un agent de console" et "exigences standard de la NetApp Console" .

  - La version d'aperçu nécessite le système d'exploitation Ubuntu 22.04 LTS pour l'agent de console.

Configurer la NetApp Console

L'étape suivante consiste à configurer la console et la NetApp Backup and Recovery.

Revoir "exigences standard de la NetApp Console" .

Créer un agent de console

Vous devez contacter votre équipe produit NetApp pour essayer la sauvegarde et la récupération. Ensuite, lorsque vous utilisez l'agent de console, il inclura les fonctionnalités appropriées pour le service.

Pour créer un agent de console dans la NetApp Console avant d'utiliser le service, reportez-vous à la documentation de la console qui décrit "comment créer un agent de console" .

Où installer l'agent de console

Pour terminer une opération de restauration, l'agent de console peut être installé aux emplacements suivants :

- Pour Amazon S3, l'agent de console peut être déployé sur vos locaux.
- Pour Azure Blob, l'agent de console peut être déployé sur vos locaux.
- 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

Les références aux « systèmes ONTAP sur site » incluent les systèmes FAS et AFF .

Configurer les licences pour NetApp Backup and Recovery

Vous pouvez obtenir une licence NetApp Backup and Recovery en achetant un abonnement payant à l'utilisation (PAYGO) ou un abonnement annuel à * NetApp Intelligent Services* auprès de votre fournisseur de cloud, ou en achetant une licence BYOL (Bring Your Own License) auprès de NetApp. Une licence valide est requise pour activer NetApp Backup and Recovery sur un système, pour créer des sauvegardes de vos données de production et pour restaurer les données de sauvegarde sur un système de production.

Quelques notes avant de poursuivre votre lecture :

- Si vous êtes déjà abonné à l'abonnement à la carte (PAYGO) sur la place de marché de votre fournisseur de cloud pour un système Cloud Volumes ONTAP , vous êtes également automatiquement abonné à NetApp Backup and Recovery . Vous n'aurez pas besoin de vous abonner à nouveau.
- La licence BYOL (Bring Your Own License) de NetApp Backup and Recovery est une licence flottante que vous pouvez utiliser sur tous les systèmes associés à votre organisation ou compte NetApp Console . Ainsi, si vous disposez d'une capacité de sauvegarde suffisante à partir d'une licence BYOL existante, vous n'aurez pas besoin d'acheter une autre licence BYOL.
- Si vous utilisez une licence BYOL, il est recommandé de souscrire également à un abonnement PAYGO. Si vous sauvegardez plus de données que ce qui est autorisé par votre licence BYOL, ou si la durée de votre licence expire, la sauvegarde continue via votre abonnement à la carte - il n'y a aucune interruption de service.
- Lors de la sauvegarde des données ONTAP sur site sur StorageGRID, vous avez besoin d'une licence BYOL, mais il n'y a aucun coût pour l'espace de stockage du fournisseur cloud.

"En savoir plus sur les coûts liés à l'utilisation de NetApp Backup and Recovery."

Essai gratuit de 30 jours

Un essai gratuit de 30 jours de NetApp Backup and Recovery est disponible si vous souscrivez à un abonnement à la carte sur la place de marché de votre fournisseur de cloud pour * NetApp Intelligent Services*. L'essai gratuit commence au moment où vous vous abonnez à la liste du marché. Notez que si vous payez l'abonnement Marketplace lors du déploiement d'un système Cloud Volumes ONTAP , puis démarrez votre essai gratuit de NetApp Backup and Recovery 10 jours plus tard, il vous restera 20 jours pour utiliser l'essai gratuit.

Une fois l'essai gratuit terminé, vous passerez automatiquement à l'abonnement PAYGO sans interruption. Si vous décidez de ne pas continuer à utiliser NetApp Backup and Recovery,"désinscrire NetApp Backup and Recovery du système" avant la fin de l'essai et vous ne serez pas facturé.

Mettre fin à l'essai gratuit

Si vous souhaitez continuer à utiliser NetApp Backup and Recovery après la fin de la période d'essai gratuite, vous devez configurer un abonnement payant. Vous pouvez le faire à partir de l'interface de la NetApp Console en accédant à la section de facturation et en sélectionnant un plan d'abonnement adapté à vos

besoins. Si vous ne souhaitez pas continuer à utiliser NetApp Backup and Recovery, vous pouvez mettre fin à l'essai gratuit.

Lorsque vous mettez fin à l'essai gratuit sans souscrire à un forfait payant, vos données sont automatiquement supprimées 60 jours après la fin de l'essai gratuit. Vous pouvez éventuellement demander au système de supprimer immédiatement vos données.

Étapes

1. Depuis la page d'accueil de NetApp Backup and Recovery , sélectionnez **Afficher l'essai gratuit**.
2. Sélectionnez **Terminer l'essai gratuit**.
3. Sélectionnez **Supprimer les données immédiatement après la fin de mon essai gratuit** pour supprimer vos données immédiatement.
4. Tapez **fin de l'essai** dans la case.
5. Sélectionnez **Fin** pour confirmer.

Utiliser un abonnement NetApp Backup and Recovery PAYGO

Pour le paiement à l'utilisation, vous paierez à votre fournisseur de cloud les coûts de stockage d'objets et les coûts de licence de sauvegarde NetApp sur une base horaire dans un seul abonnement. Vous devez vous abonner à * NetApp Intelligent Services* sur la Marketplace même si vous disposez d'un essai gratuit ou si vous apportez votre propre licence (BYOL) :

- L'abonnement garantit qu'il n'y aura aucune interruption de service après la fin de votre essai gratuit. Une fois la période d'essai terminée, vous serez facturé toutes les heures en fonction de la quantité de données que vous sauvegardez.
- Si vous sauvegardez plus de données que ce qui est autorisé par votre licence BYOL, les opérations de sauvegarde et de restauration des données se poursuivent via votre abonnement à la carte. Par exemple, si vous disposez d'une licence BYOL de 10 Tio, toute capacité au-delà de 10 Tio est facturée via l'abonnement PAYGO.

Vous ne serez pas facturé sur votre abonnement prépayé pendant votre essai gratuit ou si vous n'avez pas dépassé votre licence BYOL.

Il existe quelques plans PAYGO pour NetApp Backup and Recovery:

- Un package « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un package « CVO Professional » qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery. Cela inclut des sauvegardes illimitées pour le système Cloud Volumes ONTAP à l'aide de la licence (la capacité de sauvegarde n'est pas comptabilisée dans la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

  Notez que cette option nécessite également un abonnement PAYGO de sauvegarde et de récupération, mais aucun frais ne sera facturé pour les systèmes Cloud Volumes ONTAP éligibles.

"En savoir plus sur ces packages de licences basés sur la capacité".

Utilisez ces liens pour vous abonner à NetApp Backup and Recovery depuis la place de marché de votre fournisseur de cloud :

- AWS : "Accédez à l'offre Marketplace pour les NetApp Intelligent Services pour connaître les détails des tarifs." . endif::aws[]

- Azuré: "Accédez à l'offre Marketplace pour les NetApp Intelligent Services pour connaître les détails des tarifs." . endif::azure[]
- Google Cloud : "Accédez à l'offre Marketplace pour les NetApp Intelligent Services pour connaître les détails des tarifs." . endif::gcp[]

Utiliser un contrat annuel

Payez NetApp Backup and Recovery annuellement en achetant un contrat annuel. Ils sont disponibles pour des durées de 1, 2 ou 3 ans.

Si vous disposez d'un contrat annuel auprès d'une place de marché, toute consommation de NetApp Backup and Recovery est facturée sur ce contrat. Vous ne pouvez pas combiner un contrat de marché annuel avec un BYOL.

Lorsque vous utilisez AWS, deux contrats annuels sont disponibles auprès du "Page AWS Marketplace" pour les systèmes Cloud Volumes ONTAP et ONTAP sur site :

- Un plan « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.

  Si vous souhaitez utiliser cette option, configurez votre abonnement depuis la page Marketplace puis "associer l'abonnement à vos informations d'identification AWS" . Notez que vous devrez également payer vos systèmes Cloud Volumes ONTAP à l'aide de cet abonnement contractuel annuel, car vous ne pouvez attribuer qu'un seul abonnement actif à vos informations d'identification AWS dans la console.

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

  Voir le "Sujet sur les licences Cloud Volumes ONTAP" pour en savoir plus sur cette option de licence.

  Si vous souhaitez utiliser cette option, vous pouvez configurer le contrat annuel lorsque vous créez un système Cloud Volumes ONTAP et que la console vous invite à vous abonner à AWS Marketplace. endif::aws[]

Lorsque vous utilisez Azure, deux contrats annuels sont disponibles auprès du "Page de la place de marché Azure" pour les systèmes Cloud Volumes ONTAP et ONTAP sur site :

- Un plan « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.

  Si vous souhaitez utiliser cette option, configurez votre abonnement depuis la page Marketplace puis "associer l'abonnement à vos informations d'identification Azure" . Notez que vous devrez également payer vos systèmes Cloud Volumes ONTAP à l'aide de cet abonnement contractuel annuel, car vous ne pouvez attribuer qu'un seul abonnement actif à vos informations d'identification Azure dans la console.

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

  Voir le "Sujet sur les licences Cloud Volumes ONTAP" pour en savoir plus sur cette option de licence.

Si vous souhaitez utiliser cette option, vous pouvez configurer le contrat annuel lorsque vous créez un système Cloud Volumes ONTAP et que la console vous invite à vous abonner à la Place de marché Azure. endif::azure[]

Lorsque vous utilisez GCP, contactez votre représentant commercial NetApp pour acheter un contrat annuel. Le contrat est disponible sous forme d'offre privée sur Google Cloud Marketplace.

Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à partir de Google Cloud Marketplace lors de l'activation de NetApp Backup and Recovery . endif::gcp[]

Utiliser une licence BYOL NetApp Backup and Recovery

Les licences Bring Your Own de NetApp offrent des durées de 1, 2 ou 3 ans. Vous ne payez que pour les données que vous protégez, calculées par la capacité logique utilisée (avant toute efficacité) des volumes ONTAP sources qui sont sauvegardés. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

La licence BYOL NetApp Backup and Recovery est une licence flottante où la capacité totale est partagée entre tous les systèmes associés à votre organisation ou compte NetApp Console . Pour les systèmes ONTAP , vous pouvez obtenir une estimation approximative de la capacité dont vous aurez besoin en exécutant la commande CLI `volume show -fields logical-used-by-afs` pour les volumes que vous prévoyez de sauvegarder.

Si vous ne disposez pas d'une licence BYOL NetApp Backup and Recovery , cliquez sur l'icône de chat en bas à droite de la console pour en acheter une.

En option, si vous disposez d'une licence basée sur un nœud non attribué pour Cloud Volumes ONTAP que vous n'utiliserez pas, vous pouvez la convertir en une licence NetApp Backup and Recovery avec la même équivalence en dollars et la même date d'expiration. "Cliquez ici pour plus de détails" .

Vous utilisez la NetApp Console pour gérer les licences BYOL. Vous pouvez ajouter de nouvelles licences, mettre à jour les licences existantes et afficher l'état des licences à partir de la console.

"En savoir plus sur l'ajout de licences".

Configurer des certificats de sécurité pour StorageGRID et ONTAP dans NetApp Backup and Recovery

Créez un certificat de sécurité pour activer la communication entre NetApp Backup and Recovery et StorageGRID ou ONTAP.

Créer un certificat de sécurité pour StorageGRID

Si la communication entre les conteneurs NetApp Backup and Recovery et StorageGRID doit vérifier le certificat StorageGRID , procédez comme suit.

Le certificat généré doit avoir un CN et un nom alternatif du sujet comme nom fourni dans NetApp Backup and Recovery lorsque vous avez activé la sauvegarde.

Étapes

1. Suivez les étapes de la documentation StorageGRID pour créer le certificat StorageGRID .

"Informations StorageGRID sur la configuration des certificats"

2. Mettez à jour StorageGRID avec le certificat si vous ne l'avez pas déjà fait.
3. Connectez-vous à l'agent de la console en tant qu'utilisateur root. Courir:

```
sudo su
```

4. Obtenez le volume Docker NetApp Backup and Recovery (Cloud Backup Service). Courir:

```
docker volume ls | grep cbs
```

Exemple de sortie :

```
local service-manager-2_cloudmanager_cbs_volume"
```

Le nom du volume diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple utilise le mode Standard. Se référer à "Modes de déploiement de la NetApp Console" .

5. Recherchez le point de montage du volume NetApp Backup and Recovery . Courir:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Exemple de sortie :

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data"
```

Le point de montage diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple montre un déploiement cloud standard. Se référer à "Modes de déploiement de la NetApp Console" .

6. Accédez au répertoire MountPoint. Courir:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

7. Si le certificat de StorageGRID est signé par l'autorité de certification racine et une autorité de certification intermédiaire, ajoutez le `pem` fichiers des deux dans un seul fichier nommé `sgws.crt` à l'emplacement actuel. N'ajoutez pas le certificat feuille à ce fichier.

Étapes pour le conteneur cloudmanager_cbs

Vous devrez activer la vérification du certificat du serveur StorageGRID dans NetApp Backup and Recovery (Cloud Backup Service).

1. Modifiez les répertoires vers le volume Docker obtenu lors des étapes précédentes.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Changez de répertoire vers le répertoire de configuration.

```
cd cbs_config
```

3. Créez et enregistrez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Sortez du conteneur. Courir:

```
exit
```

5. Redémarrage `cloudmanager_cbs` . Courir:

```
docker restart cloudmanager_cbs
```

Étapes pour le conteneur cloudmanager_cbs_catalog

Ensuite, vous devrez activer la vérification du certificat du serveur StorageGRID pour le service de catalogage.

1. Changer les répertoires du volume Docker :

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Configurer le catalogue. Courir:

```
cd cbs_catalog_config
```

3. Créez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration du catalogue

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Redémarrer le catalogue. Courir:

```
docker restart cloudmanager_cbs_catalog
```

Mettre à jour le certificat de l'agent de console avec le certificat StorageGRID en fonction du système d'exploitation de l'agent

Ubuntu

1. Copiez le certificat SGWS sur `/usr/local/share/ca-certificates` . Voici un exemple :

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

où `sgws.crt` est le certificat CA racine.

2. Mettez à jour les certificats d'hôte avec le certificat StorageGRID . Courir

```
sudo update-ca-certificates
```

Red Hat Enterprise Linux

1. Copiez le certificat SGWS sur `/etc/pki/ca-trust/source/anchors/` .

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

où `sgws.crt` est le certificat CA racine.

2. Mettez à jour les certificats d'hôte avec le certificat StorageGRID .

```
update-ca-trust extract
```

3. Mettre à jour le `ca-bundle.crt`

```
cd /etc/pki/tls/certs/
openssl x509 -in ca-bundle.crt -text -noout
```

4. Pour vérifier si les certificats sont présents, exécutez la commande suivante :

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
openssl pkcs7 -print_certs | grep subject | head
```

Créer un certificat de sécurité pour ONTAP

Si la communication entre les conteneurs NetApp Backup and Recovery et ONTAP doit valider le certificat ONTAP , procédez comme suit.

NetApp Backup and Recovery utilise l'IP de gestion de cluster pour se connecter à ONTAP. Saisissez l'adresse IP du cluster dans les noms alternatifs du sujet du certificat. Spécifiez cette étape lorsque vous générez la CSR à l'aide de l'interface utilisateur du gestionnaire système.

Utilisez la documentation du gestionnaire de système pour créer un nouveau certificat CA pour ONTAP.

- "Gérer les certificats avec System Manager"

- "Comment gérer les certificats SSL ONTAP avec System Manager"

Étapes

1. Connectez-vous à l'agent de la console en tant que root. Courir:

```
sudo su
```

2. Obtenez le volume Docker de NetApp Backup and Recovery . Courir:

```
docker volume ls | grep cbs
```

Exemple de sortie :

```
local service-manager-2_cloudmanager_cbs_volume
```

Le nom du volume diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple montre un déploiement cloud standard. Se référer à "Modes de déploiement de la NetApp Console" .

3. Obtenez le support pour le volume. Courir:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Exemple de sortie :

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

Le point de montage diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple montre un déploiement cloud standard. Se référer à "Modes de déploiement de la NetApp Console" .

4. Accédez au répertoire du point de montage. Courir:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

5. Effectuez l'une des étapes suivantes :
   - Si le certificat ONTAP est signé par l'autorité de certification racine et une autorité de certification intermédiaire, ajoutez le `pem` fichiers des deux dans un seul fichier nommé `ontap.crt` à l'emplacement actuel.

- Si le certificat ONTAP est signé par une seule autorité de certification, renommez-le `pem` déposer comme `ontap.crt` et copiez-le à l'emplacement actuel. N'ajoutez pas le certificat feuille à ce fichier.

Étapes pour le conteneur cloudmanager_cbs

Ensuite, activez la vérification du certificat du serveur ONTAP dans NetApp Backup and Recovery (Cloud Backup Service).

1. Modifiez les répertoires vers le volume Docker obtenu lors des étapes précédentes.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Accédez au répertoire de configuration. Courir:

```
cd cbs_config
```

3. Créez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Sortez du conteneur. Courir:

```
exit
```

5. Redémarrez NetApp Backup and Recovery. Courir:

```
docker restart cloudmanager_cbs
```

Étapes pour le conteneur cloudmanager_cbs_catalog

Activez la vérification du certificat du serveur ONTAP pour le service de catalogage.

1. Changez les répertoires vers le volume Docker. Courir:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Courir:

```
cd cbs_catalog_config
```

3. Créez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Redémarrez NetApp Backup and Recovery. Courir:

```
docker restart cloudmanager_cbs_catalog
```

Créer un certificat pour ONTAP et StorageGRID

Si vous devez activer le certificat pour ONTAP et StorageGRID, le fichier de configuration ressemble à ceci :

Fichier de configuration pour ONTAP et StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Configurez les destinations de sauvegarde avant d'utiliser NetApp Backup and Recovery

Avant d'utiliser NetApp Backup and Recovery, effectuez quelques étapes pour configurer les destinations de sauvegarde.

Avant de commencer, révisez"prérequis" pour garantir que votre environnement est prêt.

Préparer la destination de sauvegarde

Préparez une ou plusieurs des destinations de sauvegarde suivantes :

- StorageGRID NetApp .

  Se référer à "Découvrez StorageGRID" .

  Se référer à "Documentation de StorageGRID" pour plus de détails sur StorageGRID.

- Services Web Amazon. Se référer à "Documentation Amazon S3" .

  Procédez comme suit pour préparer AWS comme destination de sauvegarde :

  - Configurez un compte dans AWS.
  - Configurez les autorisations S3 dans AWS, répertoriées dans la section suivante.
  - Pour plus de détails sur la gestion de votre stockage AWS dans la console, reportez-vous à "Gérez vos buckets Amazon S3" .
- Microsoft Azure.
  - Se référer à "Documentation Azure NetApp Files" .
  - Configurez un compte dans Azure.

- Configure "Autorisations Azure" dans Azure.
- Pour plus de détails sur la gestion de votre stockage Azure dans la console, reportez-vous à "Gérez vos comptes de stockage Azure" .

Après avoir configuré les options dans la destination de sauvegarde elle-même, vous la configurerez ultérieurement comme destination de sauvegarde dans NetApp Backup and Recovery. Pour plus de détails sur la configuration de la destination de sauvegarde dans NetApp Backup and Recovery, reportez-vous à"Découvrir les cibles de sauvegarde" .

Configurer les autorisations S3

Vous devrez configurer deux ensembles d'autorisations AWS S3 :

- 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"
        }
    ]
}
```

Connectez-vous à NetApp Backup and Recovery

Vous utilisez la NetApp Console pour vous connecter à NetApp Backup and Recovery.

NetApp Backup and Recovery utilise la gestion des identités et des accès pour contrôler ce que chaque utilisateur peut faire.

Pour plus de détails sur les actions que chaque rôle peut effectuer, voir"Rôles utilisateur de NetApp Backup and Recovery" .

Pour vous connecter à la NetApp Console, vous pouvez utiliser vos informations d'identification du site de support NetApp ou vous inscrire pour une connexion à la NetApp Console à l'aide de votre adresse e-mail et d'un mot de passe. "En savoir plus sur la connexion" .

Rôle de NetApp 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" .

Pour ajouter un agent de console, vous devez disposer du rôle de super administrateur de sauvegarde et de récupération.

Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console" .

   La page de connexion à la NetApp Console s'affiche.

2. Connectez-vous à la console.
3. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.
   - S'il s'agit de votre première connexion à Backup and Recovery et que vous n'avez pas encore ajouté de système à la page **Systèmes**, Backup and Recovery affiche la page d'accueil « Bienvenue sur la nouvelle NetApp Backup and Recovery» et propose une option pour ajouter un système. Pour plus de détails sur l'ajout d'un système à la page **Systèmes**, reportez-vous à "Prise en main du mode standard de la NetApp Console" .
   - S'il s'agit de votre première connexion à Backup and Recovery et que vous avez déjà ajouté un système à la page **Systèmes**, mais que vous n'avez découvert aucune ressource, la page d'accueil « Bienvenue dans la nouvelle version de NetApp Backup and Recovery» apparaît et affiche une option permettant de **Découvrir des ressources**.
4. Si vous ne l'avez pas déjà fait, sélectionnez l'option **Découvrir et gérer**.
   - Pour les charges de travail Microsoft SQL Server, reportez-vous à"Découvrez les charges de travail Microsoft SQL Server" .
   - Pour les charges de travail VMware, reportez-vous à"Découvrez les charges de travail VMware" .
   - Pour les charges de travail KVM, reportez-vous à"Découvrez les charges de travail KVM" .
   - Pour les charges de travail Oracle, reportez-vous à"Découvrez les charges de travail Oracle" .
   - Pour les charges de travail Hyper-V, reportez-vous à"Découvrez les charges de travail Hyper-V" .
   - Pour les charges de travail Kubernetes, reportez-vous à"Découvrez les charges de travail Kubernetes" .

Découvrez les cibles de sauvegarde hors site dans NetApp Backup and Recovery

Suivez quelques étapes pour découvrir ou ajouter manuellement des cibles de sauvegarde hors site dans NetApp Backup and Recovery.

Découvrir une cible de sauvegarde

Configurez vos cibles de sauvegarde (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage ou StorageGRID) avant d'utiliser NetApp Backup and Recovery.

Vous pouvez découvrir ces cibles automatiquement ou les ajouter manuellement.

Fournissez les informations d'identification pour accéder au compte de stockage. NetApp Backup and Recovery utilise ces informations d'identification pour découvrir les charges de travail que vous souhaitez sauvegarder.

Avant de commencer

Vous devez découvrir au moins une charge de travail avant de pouvoir ajouter une cible de sauvegarde hors site.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'onglet **Cibles de sauvegarde hors site**.
3. Sélectionnez **Découvrir la cible de sauvegarde**.
4. Sélectionnez l'un des types de cibles de sauvegarde : **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* ou * ONTAP S3*.
5. Dans la section **Choisir l'emplacement des informations d'identification**, choisissez l'emplacement où résident les informations d'identification, puis choisissez comment associer les informations d'identification.
6. Sélectionnez **Suivant**.
7. Saisissez les informations d'identification. Elles varient selon le type de cible de sauvegarde sélectionné et l'emplacement des informations d'identification choisi.
   - Pour AWS :
     - **Nom d'identification** : saisissez le nom d'identification AWS.
     - **Clé d'accès** : Saisissez le secret AWS.
     - **Clé secrète** : saisissez la clé secrète AWS.
   - Pour Azure :
     - **Nom des informations d'identification** : saisissez le nom des informations d'identification du stockage d'objets blob Azure.
     - **Secret client** : saisissez le secret client du stockage d'objets blob Azure.
     - **ID d'application (client)** : sélectionnez l'ID d'application Azure Blob Storage.
     - **ID de locataire du répertoire** : saisissez l'ID de locataire du stockage d'objets blob Azure.
   - Pour StorageGRID:
     - **Nom d'identification** : saisissez le nom d'identification StorageGRID .

- **Nom de domaine complet du nœud de passerelle** : saisissez un nom de domaine complet pour StorageGRID.
- **Port**: saisissez le numéro de port pour StorageGRID.
- **Clé d'accès** : saisissez la clé d'accès StorageGRID S3.
- **Clé secrète** : saisissez la clé secrète StorageGRID S3.

◦ Pour ONTAP S3 :

- **Nom d'identification** : saisissez le nom d'identification ONTAP S3.
- **Nom de domaine complet du nœud de passerelle** : saisissez un nom de domaine complet pour ONTAP S3.
- **Port** : saisissez le numéro de port pour ONTAP S3.
- **Clé d'accès** : Saisissez la clé d'accès ONTAP S3.
- **Clé secrète** : Saisissez la clé secrète ONTAP S3.

8. Sélectionnez **Découvrir**.

Ajouter un bucket pour une cible de sauvegarde

Plutôt que de laisser NetApp Backup and Recovery découvrir automatiquement les buckets, vous pouvez ajouter manuellement un bucket à une cible de sauvegarde hors site.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez **Cibles de sauvegarde hors site**.
3. Sélectionnez la cible et à droite, sélectionnez les **Actions*** icône et sélectionnez ***Ajouter un bucket**.
4. Saisissez les informations du bucket. Les informations diffèrent selon le type de cible de sauvegarde que vous avez sélectionné.

◦ Pour AWS :

- **Nom du bucket** : saisissez le nom du bucket S3. Le préfixe « netapp-backup » est un préfixe obligatoire et est automatiquement ajouté au nom que vous fournissez.
- **Compte AWS** : saisissez le nom du compte AWS.
- **Région du bucket** : saisissez la région AWS du bucket.
- **Activer le verrouillage d'objet S3** : sélectionnez cette option pour activer le verrouillage d'objet S3 pour le bucket. S3 Object Lock empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une couche supplémentaire de protection des données. Vous ne pouvez activer cette option que lorsque vous créez un bucket et vous ne pouvez pas la désactiver ultérieurement.
  - **Mode de gouvernance** : sélectionnez cette option pour activer le mode de gouvernance pour le bucket S3 Object Lock. Le mode de gouvernance vous permet de protéger les objets contre la suppression ou l'écrasement par la plupart des utilisateurs, mais permet à certains utilisateurs de modifier les paramètres de conservation.
  - **Mode de conformité** : sélectionnez cette option pour activer le mode de conformité pour le compartiment S3 Object Lock. Le mode de conformité empêche tout utilisateur, y compris l'utilisateur root, de modifier les paramètres de conservation ou de supprimer des objets jusqu'à l'expiration de la période de conservation.
- **Versioning** : sélectionnez cette option pour activer le contrôle de version pour le bucket S3. Le

contrôle de version vous permet de conserver plusieurs versions d'objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de récupération.

- **Tags** : sélectionnez les balises pour le bucket S3. Les balises sont des paires clé-valeur qui peuvent être utilisées pour organiser et gérer vos ressources S3.
- **Cryptage** : sélectionnez le type de cryptage pour le compartiment S3. Les options sont soit des clés gérées par AWS S3, soit des clés AWS Key Management Service. Si vous sélectionnez des clés AWS Key Management Service, vous devez fournir l'ID de clé.

◦ Pour Azure :

- **Abonnement** : sélectionnez le nom du conteneur de stockage d'objets blob Azure.
- **Groupe de ressources** : sélectionnez le nom du groupe de ressources Azure.
- **Détails de l'instance**:
  - **Nom du compte de stockage** : saisissez le nom du conteneur de stockage d'objets blob Azure.
  - **Région Azure** : saisissez la région Azure du conteneur.
  - **Type de performance** : sélectionnez le type de performance Standard ou Premium pour le conteneur de stockage d'objets blob Azure indiquant le niveau de performance requis.
  - **Chiffrement** : sélectionnez le type de chiffrement pour le conteneur de stockage d'objets blob Azure. Les options sont soit des clés gérées par Microsoft, soit des clés gérées par le client. Si vous sélectionnez des clés gérées par le client, vous devez fournir le nom du coffre de clés et le nom de la clé.

◦ Pour StorageGRID:

- **Nom de la cible de sauvegarde** : sélectionnez le nom du bucket StorageGRID .
- **Nom du bucket** : saisissez le nom du bucket StorageGRID .
- **Région** : saisissez la région StorageGRID pour le bucket.
- **Activer le contrôle de version** : sélectionnez cette option pour activer le contrôle de version pour le bucket StorageGRID . Le contrôle de version vous permet de conserver plusieurs versions d'objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de récupération.
- **Verrouillage d'objet** : sélectionnez cette option pour activer le verrouillage d'objet pour le bucket StorageGRID . Le verrouillage des objets empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une couche supplémentaire de protection des données. Vous ne pouvez activer cette option que lorsque vous créez un bucket et vous ne pouvez pas la désactiver ultérieurement.
- **Capacité** : saisissez la capacité du bucket StorageGRID . Il s'agit de la quantité maximale de données pouvant être stockée dans le bucket.

◦ Pour ONTAP S3 :

- **Nom de la cible de sauvegarde** : sélectionnez le nom du bucket ONTAP S3.
- **Nom de la cible du bucket** : saisissez le nom du bucket ONTAP S3.
- **Capacité** : saisissez la capacité du bucket ONTAP S3. Il s'agit de la quantité maximale de données pouvant être stockée dans le bucket.
- **Activer le contrôle de version** : sélectionnez cette option pour activer le contrôle de version pour le bucket ONTAP S3. Le contrôle de version vous permet de conserver plusieurs versions d'objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de récupération.
- **Verrouillage d'objet** : sélectionnez cette option pour activer le verrouillage d'objet pour le compartiment ONTAP S3. Le verrouillage des objets empêche la suppression ou l'écrasement des

objets pendant une période de conservation spécifiée, offrant ainsi une couche supplémentaire de protection des données. Vous ne pouvez activer cette option que lorsque vous créez un bucket et vous ne pouvez pas la désactiver ultérieurement.

5. Sélectionnez **Ajouter**.

Modifier les informations d'identification pour une cible de sauvegarde

Saisissez les informations d'identification nécessaires pour accéder à la cible de sauvegarde.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez **Cibles de sauvegarde hors site**.
3. Sélectionnez la cible et à droite, sélectionnez les **Actions*** **icône et sélectionnez *Modifier les informations d'identification**.
4. Saisissez les nouvelles informations d'identification pour la cible de sauvegarde. Les informations diffèrent selon le type de cible de sauvegarde que vous avez sélectionné.
5. Sélectionnez **Terminé**.

Basculer vers différentes charges de travail de NetApp Backup and Recovery

Vous pouvez basculer entre les différentes charges de travail de NetApp Backup and Recovery .

Passer à une charge de travail différente

Vous pouvez basculer vers une charge de travail différente dans l'interface utilisateur de NetApp Backup and Recovery .

Étapes

1. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Dans le coin supérieur droit de la page, sélectionnez la liste déroulante **Changer de charge de travail**.
3. Sélectionnez la charge de travail vers laquelle vous souhaitez basculer.

   La page s'actualise et affiche la charge de travail sélectionnée.

Configurer les paramètres de NetApp Backup and Recovery

Après avoir configuré la NetApp Console, configurez les paramètres de sauvegarde et de récupération. Ajoutez des informations d'identification pour les ressources de l'hôte, importez des ressources SnapCenter , configurez les répertoires de journaux et définissez les paramètres VMware vCenter. Effectuez ces étapes avant de sauvegarder ou de récupérer des données.

- Ajouter des informations d'identification pour les ressources de l'hôtepour les hôtes Windows et SQL Server que vous avez importés depuis SnapCenter et ajoutez des informations d'identification. (charges de travail Microsoft SQL Server uniquement)

- Maintenir les paramètres VMware vCenter.
- Importer et gérer les ressources de l'hôte SnapCenter. (charges de travail Microsoft SQL Server uniquement)
- Configurer les répertoires de journaux dans les instantanés pour les hôtes Windows.

Rôle de NetApp Console requis Super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration 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" .

Ajouter des informations d'identification pour les ressources de l'hôte

Ajoutez des informations d'identification pour les ressources hôtes à importer depuis SnapCenter. NetApp Backup and Recovery utilise ces informations d'identification pour découvrir les charges de travail et appliquer des stratégies de sauvegarde.

Si vous ne disposez pas d'informations d'identification, créez-les avec des autorisations pour accéder aux charges de travail de l'hôte et les gérer.

Vous devez configurer les types d'informations d'identification suivants :

- Informations d'identification Microsoft SQL Server
- Informations d'identification de l'hôte Windows SnapCenter

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour **Informations d'identification**.
3. Sélectionnez **Ajouter de nouvelles informations d'identification**.
4. Saisissez les informations pour les informations d'identification. Différents champs apparaissent en fonction du mode d'authentification que vous sélectionnez. Sélectionnez l'option Informations **i** pour plus d'informations sur les champs.
   - **Nom des informations d'identification** : saisissez un nom pour les informations d'identification.
   - **Mode d'authentification** : sélectionnez **Windows** ou **Microsoft SQL**.

     Vous devez saisir les informations d'identification pour Windows et Microsoft SQL Server. Vous devrez donc ajouter deux ensembles d'informations d'identification.

5. Si vous avez sélectionné **Windows** :
   - **Agent de console** : saisissez l'adresse IP de l'agent de console.
   - **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.
   - **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.
6. Si vous avez sélectionné **Microsoft SQL** :
   - **Hôte** : sélectionnez une adresse d'hôte SQL Server découverte.
   - **Instance SQL Server** : sélectionnez une instance SQL Server découverte.
7. Sélectionnez **Ajouter**.

Modifier les informations d'identification pour les ressources de l'hôte

Vous pouvez ultérieurement modifier le mot de passe des ressources hôtes que vous avez importées depuis SnapCenter.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **Informations d'identification**.
3. Sélectionnez l'icône Actions ••• > **Modifier les informations d'identification**.
   - **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.
4. Sélectionnez **Enregistrer**.

Maintenir les paramètres VMware vCenter

Fournissez les informations d'identification VMware vCenter pour découvrir les charges de travail à sauvegarder. Si vous ne disposez pas d'informations d'identification, créez-les avec des autorisations pour accéder et gérer les charges de travail VMware vCenter Server.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **VMware vCenter**.
3. Sélectionnez **Ajouter vCenter**.
4. Saisissez les informations du serveur VMware vCenter.
   - **VCenter FQDN ou adresse IP** : saisissez un nom de domaine complet ou l'adresse IP du serveur VMware vCenter.
   - **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur VMware vCenter.
   - **Port** : saisissez le numéro de port du serveur VMware vCenter.
   - **Protocole** : Sélectionnez **HTTP** ou **HTTPS**.
5. Sélectionnez **Ajouter**.

Importer et gérer les ressources de l'hôte SnapCenter

Si vous avez déjà utilisé SnapCenter pour sauvegarder vos ressources, vous pouvez importer et gérer ces ressources dans NetApp Backup and Recovery. Cette option vous permet d'importer les informations du serveur SnapCenter pour enregistrer plusieurs serveurs Snapcenter et découvrir les charges de travail de la base de données.

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 dans la page 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 en charge la gestion de la protection. Pour ce faire, vous devez choisir explicitement de gérer ces ressources dans NetApp Backup and Recovery.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **Importer depuis SnapCenter**.
3. Sélectionnez **Importer depuis SnapCenter** pour importer les ressources SnapCenter .
4. 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.
5. 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. Entrez 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.
6. 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.

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 importées, NetApp Backup and Recovery peut sauvegarder et récupérer les ressources que vous importez depuis SnapCenter. Vous n'avez plus besoin de gérer ces ressources dans SnapCenter Server.

Étapes

1. Après avoir importé les ressources SnapCenter , sur la page Inventaire qui s'affiche, sélectionnez les ressources SnapCenter que vous avez importées et que vous souhaitez que NetApp Backup and Recovery gère désormais.
2. Sélectionnez l'icône Actions ••• > **Gérer** pour gérer les ressources.
3. Sélectionnez **Gérer dans la NetApp Console**.

   La page Inventaire affiche **Géré** sous le nom d'hôte pour indiquer que les ressources d'hôte sélectionnées sont désormais gérées par NetApp Backup and Recovery.

Modifier les ressources SnapCenter importées

Vous pouvez ensuite réimporter les ressources SnapCenter ou modifier les ressources SnapCenter importées pour mettre à jour les détails d'enregistrement.

Vous ne pouvez modifier que les détails du port et du mot de passe pour le serveur SnapCenter .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour **Importer depuis SnapCenter**.

   La page Importer depuis SnapCenter affiche toutes les importations précédentes.

3. Sélectionnez l'icône Actions ••• > **Modifier** pour mettre à jour les ressources.
4. Mettez à jour le mot de passe et les détails du port SnapCenter , si nécessaire.
5. Sélectionnez **Importer**.

Configurer les répertoires de journaux dans les instantanés pour les hôtes Windows

Avant de créer des stratégies pour les hôtes Windows, vous devez configurer les répertoires de journaux dans les instantanés pour les hôtes Windows. Les répertoires de journaux sont utilisés pour stocker les journaux générés pendant le processus de sauvegarde.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Depuis la page Inventaire, sélectionnez une charge de travail, puis sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.
3. Dans la page Détails de l'inventaire affichant Microsoft SQL Server, sélectionnez l'onglet Hôtes.
4. Depuis la page Détails de l'inventaire, sélectionnez un hôte et sélectionnez l'icône Actions ••• > **Configurer le répertoire des journaux**.
5. Parcourez ou entrez le chemin d'accès au répertoire du journal.
6. Sélectionnez **Enregistrer**.

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 NetApp Backup and Recovery , sélectionnez **Tableau de bord**.
    - 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** : les exemples incluent Microsoft SQL Server, Volumes, VMware, KVM, Hyper-V 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 une copie instantanée des instances, des bases de données, des applications ou des 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** : Stockage principal (disque) vers stockage secondaire (disque) vers cloud (magasin d'objets). Crée plusieurs copies de données sur différents systèmes de stockage, tels que des configurations ONTAP vers ONTAP et ONTAP vers un magasin d'objets. Il peut s'agir d'un magasin d'objets hyperscaler cloud ou d'un magasin d'objets privé - StorageGRID. Ces configurations contribuent à obtenir une protection optimale des données 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 l'instantané cohérent avec la VM** : (s'applique uniquement aux charges de travail VMware) Sélectionnez si vous souhaitez activer les instantanés cohérents avec la VM. Cela garantit que les snapshots nouvellement créés sont cohérents avec l'état de la machine virtuelle au moment du snapshot. Cela 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

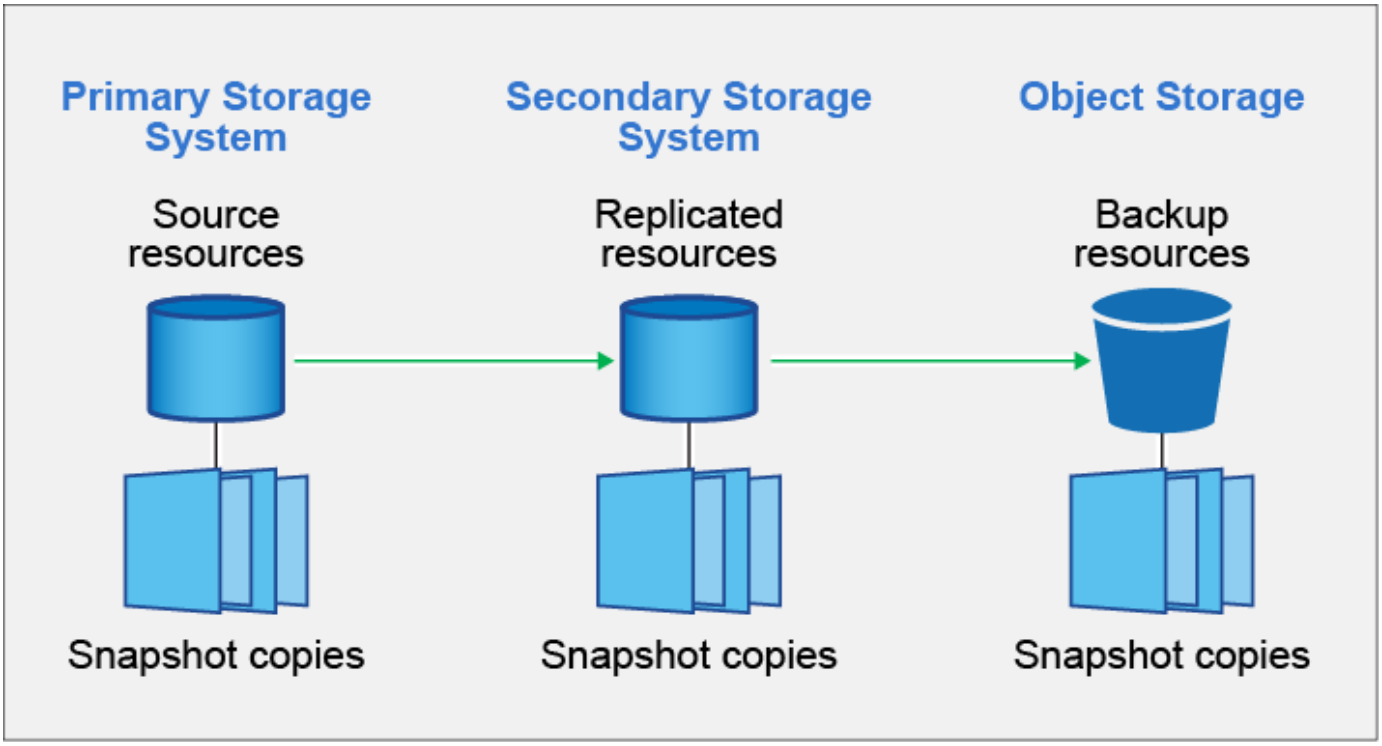
NetApp Backup and Recovery fournit des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données de volume ONTAP . Vous pouvez mettre en œuvre une stratégie 3-2-1 dans laquelle vous disposez

de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud.

REMARQUE 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 :

- Copie instantanée 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 copies Snapshot et en les transférant vers les emplacements de sauvegarde.

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

- Plusieurs copies de données offrent une protection multicouche contre les menaces de cybersécurité internes (initiées) 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 facilite les restaurations rapides, avec les copies hors site prêtes au cas où la copie sur site serait 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 les données à partir d’un moment précis à partir de copies Snapshot locales, de volumes répliqués ou de volumes sauvegardés dans le stockage d’objets.

- 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 les volumes ONTAP des systèmes sources suivants vers les systèmes secondaires suivants et le stockage d'objets dans les fournisseurs de cloud public et privé. Les copies instantanées résident sur le système source.

Système source	Système secondaire (réplication)	Magasin d'objets de destination (sauvegarde) ifdef::aws[]
Cloud Volumes ONTAP dans AWS	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Amazon S3 endif::aws[] ifdef::azure[]
Cloud Volumes ONTAP dans Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Objet blob Azure endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP dans Google	Cloud Volumes ONTAP dans le système ONTAP sur site de Google	Stockage Google Cloud endif::gcp[]
Système ONTAP sur site	Cloud Volumes ONTAP Système ONTAP sur site	ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Azure Blob endif::azure[] ifdef::gcp[] Google Cloud Storage endif::gcp[] NetApp StorageGRID ONTAP S3

Destinations de restauration prises en charge

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 copies instantanées résident sur le système source et ne peuvent être restaurées que sur ce même système.

Emplacement du fichier de sauvegarde		Système de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Cloud Volumes ONTAP dans AWS Système ONTAP sur site endif::aws[] ifdef::azure[]
Azure Blob	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP local Azure endif::azure[] ifdef::gcp[]
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 endif::gcp[]
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 de copies Snapshot ou de volumes répliqués est gratuite, à l'exception de l'espace disque requis pour stocker les copies Snapshot et les volumes répliqués.

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 de copies instantanées 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 .

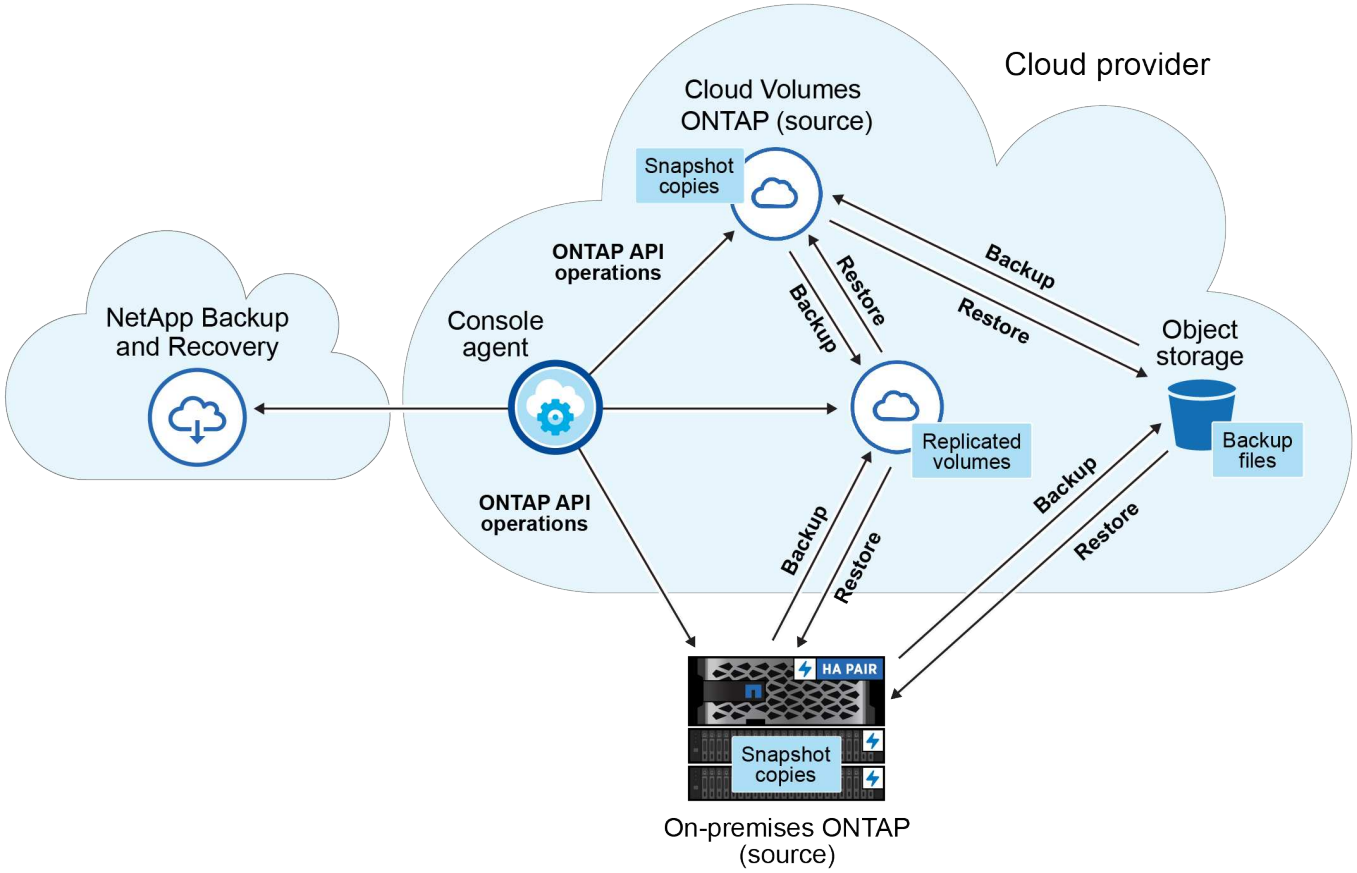
"Apprenez à mettre en place des contrats annuels".

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 *copies instantanées* résident sur le volume source dans le 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 la "Fonctionnalité d'accès public au bloc Amazon S3" sur le bucket 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 de locataire existant pour le bucket 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 copies instantanées, 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 copies de snapshot « 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 la dernière copie

Snapshot. Les analyses programmées peuvent être désactivées pour réduire vos coûts. Vous pouvez activer ou désactiver les analyses de ransomware planifiées sur la dernière copie Snapshot en utilisant l'option sur 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.

REMARQUE 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 : copies instantanées, 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 ?

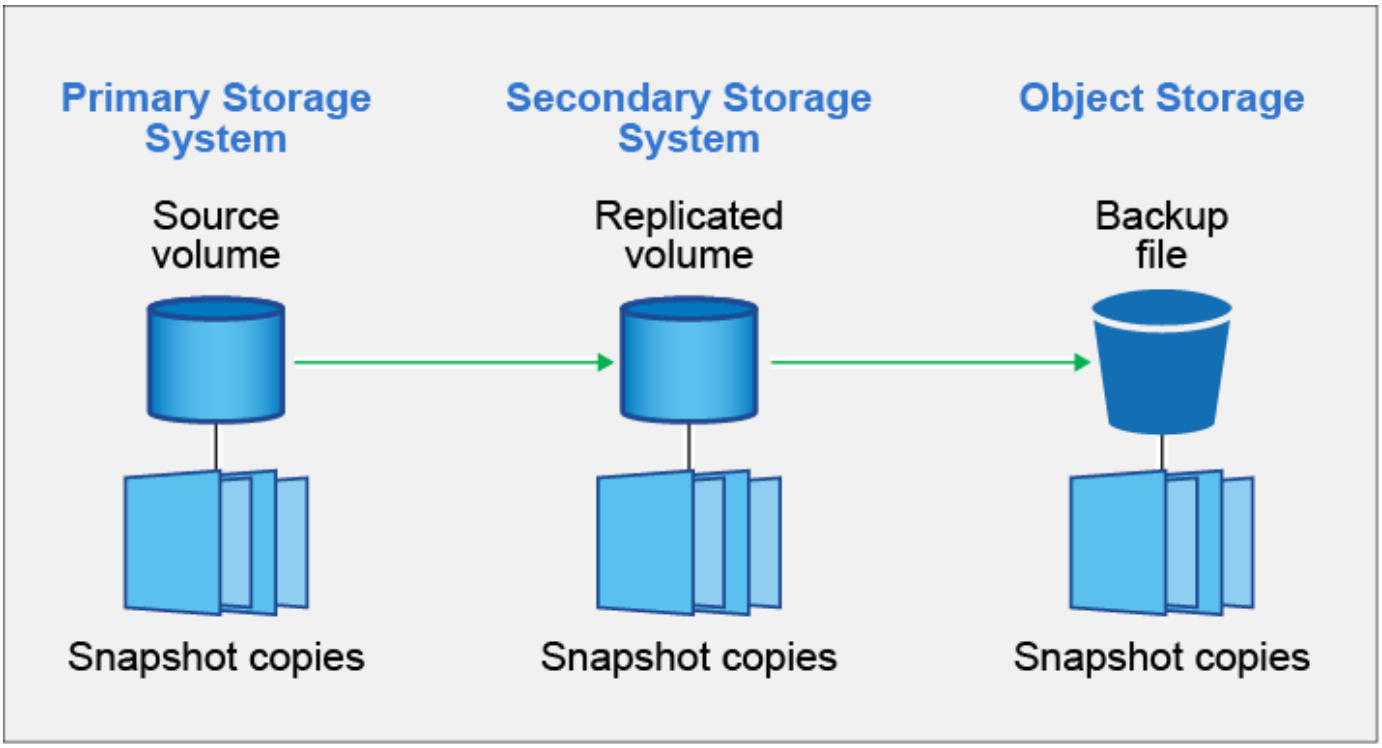
- Voulez-vous que le service crée les buckets cloud pour vous ou souhaitez-vous créer vos conteneurs de stockage d'objets avant de commencer ?
- Quel mode de déploiement de l'agent de console utilisez-vous (mode standard, restreint ou privé) ?

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, à un instant T, d'un volume dans le volume source sous forme de copie instantanée. Vous pouvez utiliser la copie instantanée 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. Une copie instantanée est une image en lecture seule, à un instant T, d'un volume. L'image consomme un espace de stockage minimal et entraîne une surcharge de performances négligeable, car elle enregistre uniquement les modifications apportées aux fichiers depuis la dernière copie instantanée. La copie instantanée créée sur votre volume est utilisée pour maintenir le volume répliqué et le fichier de sauvegarde synchronisés avec les modifications apportées au volume source, comme illustré dans 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 → Copie instantanée → Volume répliqué → Fichier de sauvegarde
- Volume source → Copie instantanée → Fichier de sauvegarde
- Volume source → Copie instantanée → 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.

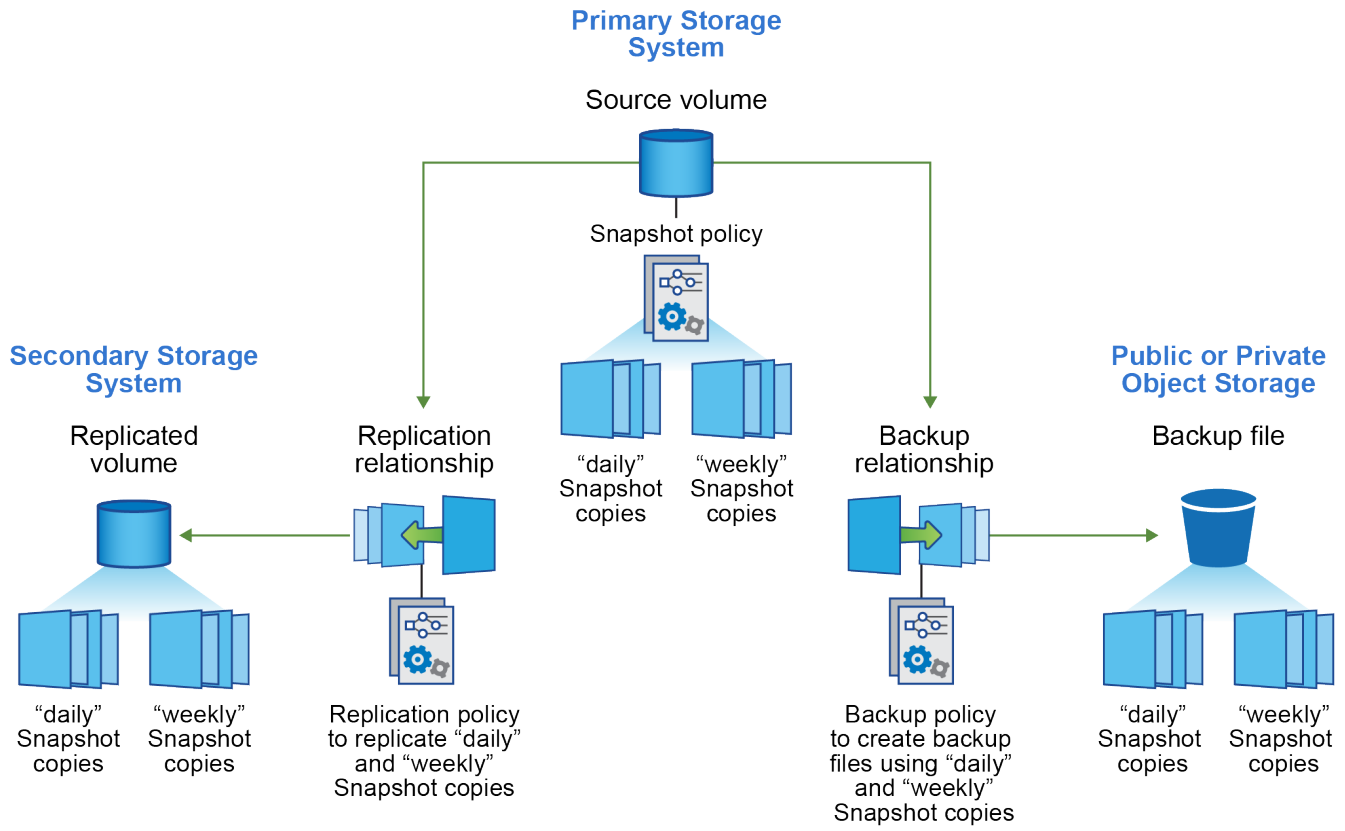
En plus de ces critères, le stockage cloud offre des options de sécurité supplémentaires si vous utilisez la fonctionnalité DataLock et Ransomware Resilience, ainsi que des économies de coûts supplémentaires en sélectionnant des classes de stockage d'archivage pour les fichiers de sauvegarde plus anciens.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

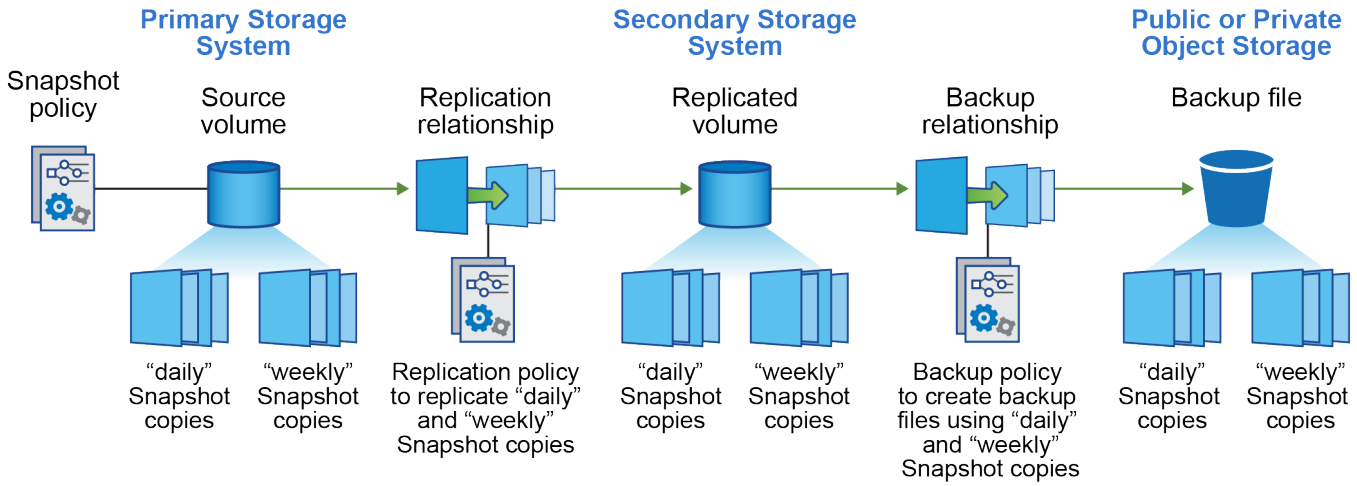
Quelle architecture de sauvegarde utiliserez-vous

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 **fan-out** transfère la copie instantanée indépendamment vers le système de stockage de destination et l'objet de sauvegarde dans le cloud.



Une architecture **en cascade** transfère d'abord la copie instantanée 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 copies instantanées à 2 systèmes distincts	Moins d'effet sur les performances du système de stockage source car il envoie la copie instantanée une seule fois
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 stratégie de capture instantanée par défaut crée des copies de capture instantanée horaires, quotidiennes et hebdomadaires, en conservant 6 copies de capture instantanée horaires, 2 copies de capture instantanée quotidiennes et 2 copies de capture instantanée hebdomadaires.
- La politique de réplication par défaut réplique des copies instantanées quotidiennes et hebdomadaires, en conservant 7 copies instantanées quotidiennes et 52 copies instantanées hebdomadaires.
- La politique de sauvegarde par défaut réplique des copies instantanées quotidiennes et hebdomadaires, en conservant 7 copies instantanées quotidiennes et 52 copies instantanées 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`
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" . ifdef::aws[]

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.

REMARQUE 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 copies instantanées, vos réplications et vos sauvegardes sur le stockage d'objets :

- 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 une copie instantanée 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.

REMARQUE 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 .

"Consultez le blog sur la protection DataLock et Ransomware pour plus de détails.".

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

Avec cette fonctionnalité, vous pouvez verrouiller les snapshots cloud répliqués via SnapMirror sur le cloud et également activer la fonctionnalité pour détecter une attaque de ransomware et récupérer une copie cohérente du snapshot sur le magasin d'objets. Cette fonctionnalité est prise en charge sur AWS, Azure 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 ifdef::aws[]
Cloud Volumes ONTAP dans AWS	Amazon S3 endif::aws[] ifdef::azure[]
Cloud Volumes ONTAP dans Azure	Objet blob Azure endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP dans Google Cloud	Google Cloud endif::gcp[]
Système ONTAP sur site	ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Azure Blob endif::azure[] ifdef::gcp[] Google Cloud endif::gcp[] 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 sauvegardes plus anciennes 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 d'objets, l'exportation ou non des copies Snapshot historiques sous forme de 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.

REMARQUE 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 :

- Modification de la bande passante réseau allouée au téléchargement des sauvegardes vers le stockage d'objets à l'aide de l'option Taux de transfert maximal ifdef::aws[]
- Modifier si les copies Snapshot historiques sont exportées en tant que fichiers de sauvegarde et incluses dans vos fichiers de sauvegarde de base 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 afficher les paramètres de sauvegarde au niveau du cluster 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*, cliquez sur••• pour le système et sélectionnez **Paramètres avancés**.

   La page *Paramètres avancés* affiche les paramètres actuels de ce système.

4. Développez l'option et effectuez la modification.

Toutes les opérations de sauvegarde après la modification utiliseront les nouvelles valeurs.

Notez que certaines options ne sont pas disponibles en fonction de la version d' ONTAP sur le cluster source et en fonction de la destination du fournisseur de cloud où résident 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 et sélectionnez **Paramètres avancés**.
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.

Modifier si les copies d'instantanés historiques sont exportées en tant que fichiers de sauvegarde

S'il existe des copies d'instantanés locaux pour les volumes qui correspondent à l'étiquette de planification de sauvegarde que vous utilisez dans ce système (par exemple, quotidienne, hebdomadaire, etc.), vous pouvez exporter ces instantanés historiques vers le stockage d'objets sous forme de fichiers de sauvegarde. Cela vous permet d'initialiser vos sauvegardes dans le cloud en déplaçant les anciennes copies instantanées vers 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 et sélectionnez **Paramètres avancés**.
3. Dans la page Paramètres avancés, développez la section **Exporter les copies d'instantanés existantes**.
4. Sélectionnez si vous souhaitez que les copies instantanées existantes soient exportées.
5. Sélectionnez **Appliquer**.

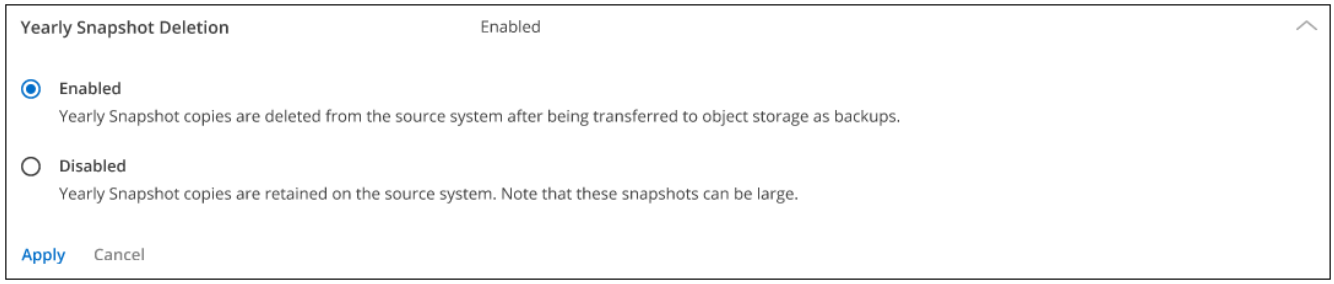
Modifier si les instantanés « annuels » sont supprimés du système source

Lorsque vous sélectionnez l'étiquette de sauvegarde « annuelle » pour une politique de sauvegarde pour l'un

de vos volumes, la copie instantanée créée est très volumineuse. 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 et sélectionnez **Paramètres avancés**.
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 la dernière copie instantanée. Vous pouvez activer ou désactiver les analyses de ransomware sur la dernière copie instantanée en utilisant l'option sur la page Paramètres avancés. Si vous l'activez, les analyses sont effectuées tous les 7 jours par défaut.

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.

Les analyses de ransomware planifiées s'exécutent uniquement sur la dernière copie instantanée.

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.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur••• pour le système et sélectionnez **Paramètres avancés**.
3. Dans la page Paramètres avancés, développez la section **Analyse des ransomwares**.

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**.

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.

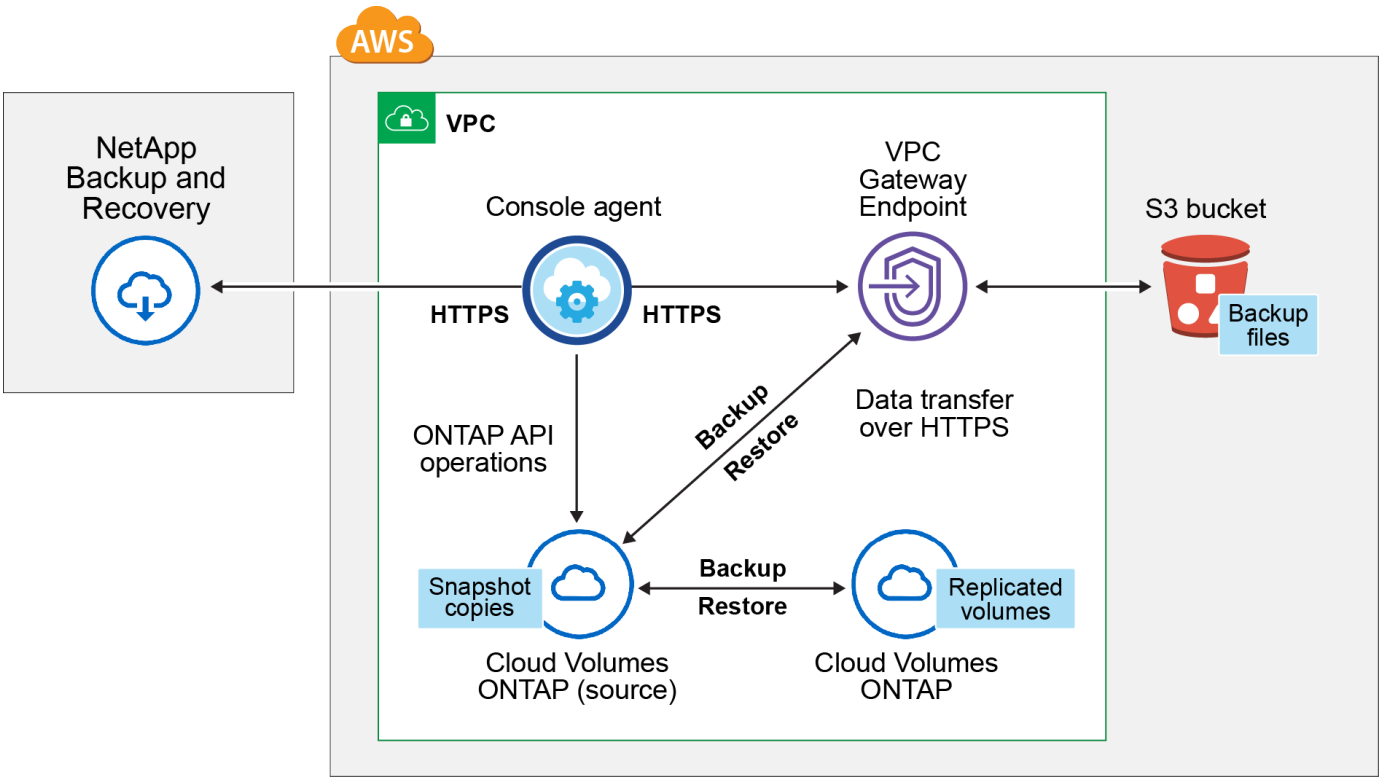
REMARQUE Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

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 de sauvegarde et de récupération. Dans l'onglet Volumes, sélectionnez les **Actions*** ••• **option d'icône et sélectionnez *Activer la sauvegarde** 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 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 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.

     > 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 **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.

   - **Clé de chiffrement** : si vous avez créé un nouveau bucket, 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 à partir de 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.

   - **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.
     - 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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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.

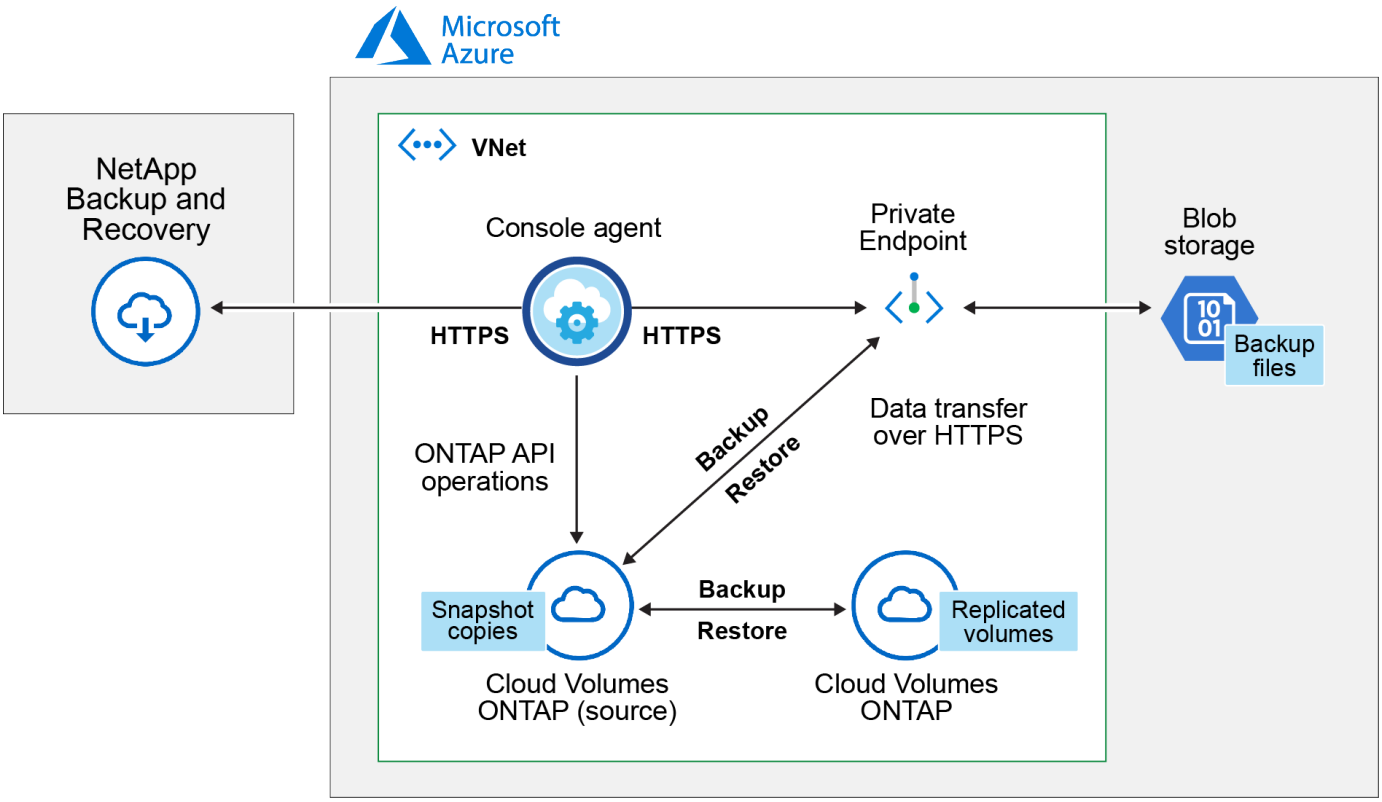
REMARQUE Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

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.

     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. "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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données de stockage principales contenues dans les copies Snapshot.

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.

> **REMARQUE** 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" .

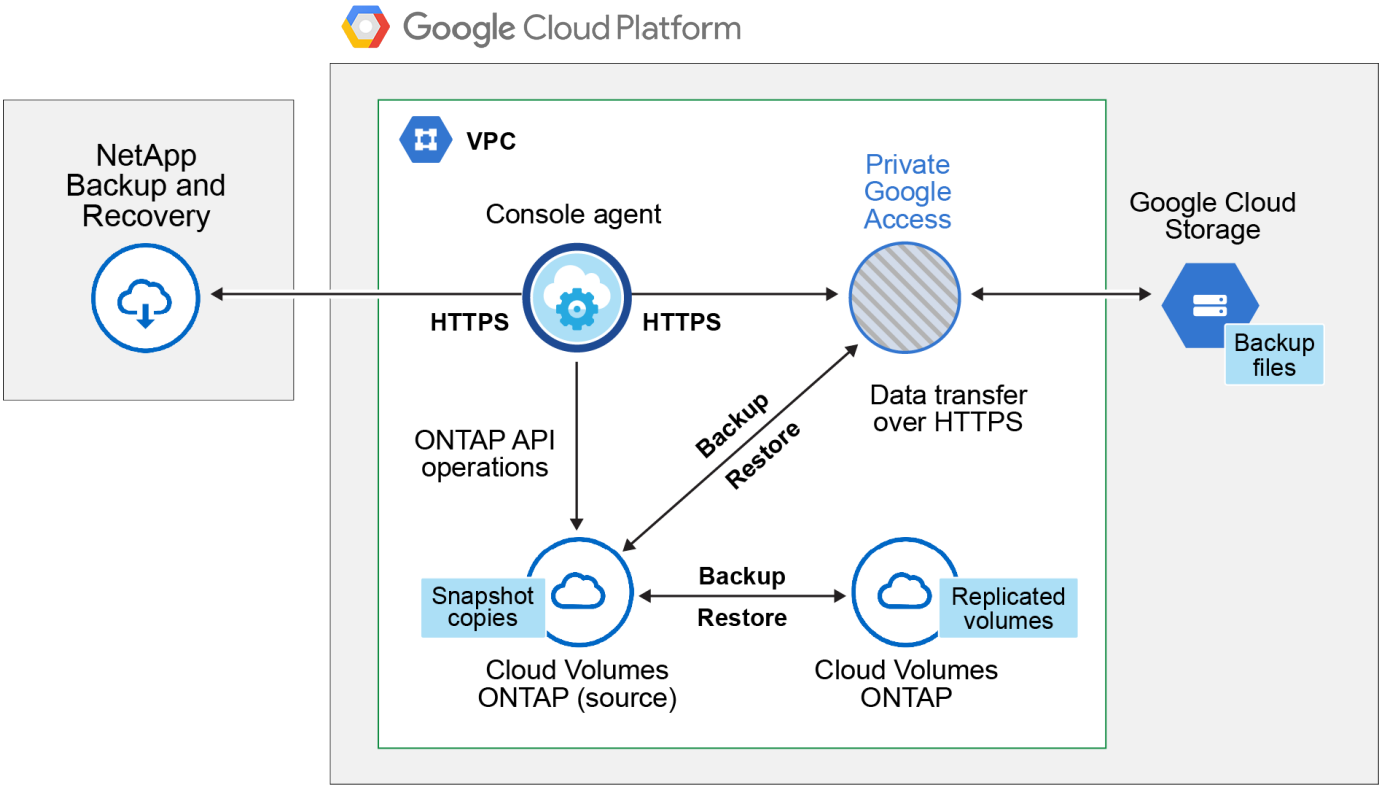
Vérifiez la prise en charge de votre configuration

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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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 .

REMARQUE 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

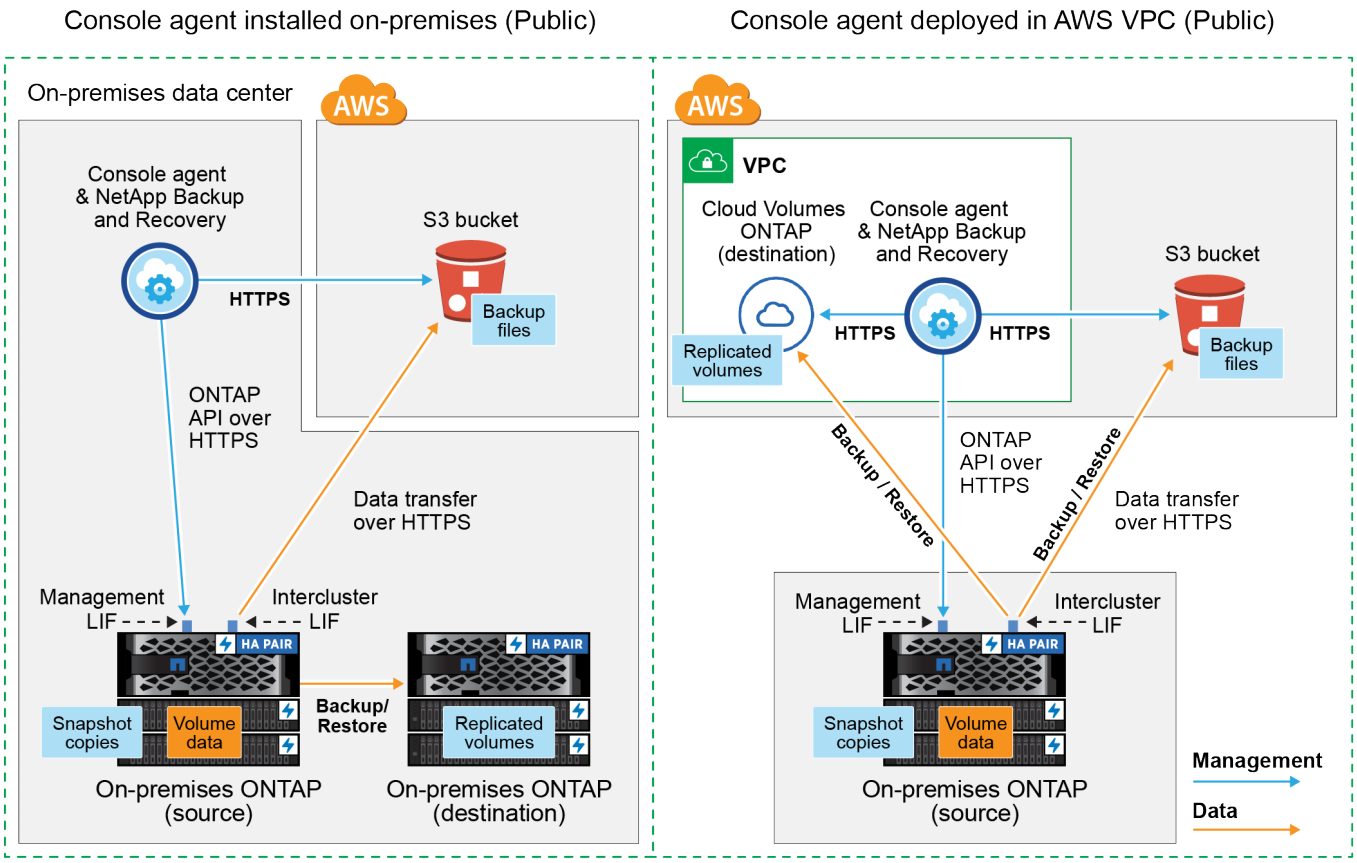
Choisissez laquelle des deux méthodes de connexion vous utiliserez lors de la configuration des sauvegardes des systèmes ONTAP locaux vers AWS S3.

- **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.

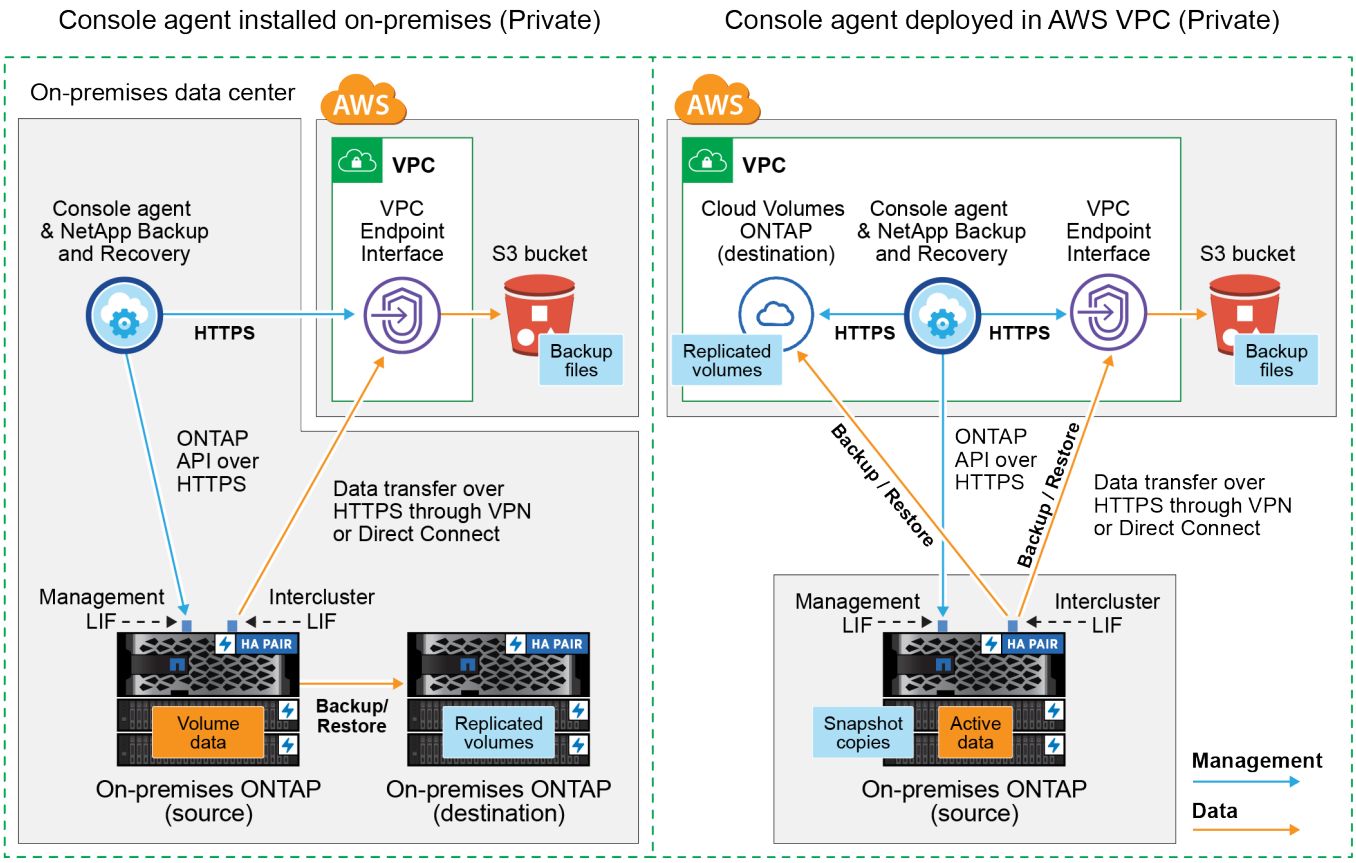
En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués à l'aide de la connexion publique ou privée.

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 bucket 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` IAMRole pour les CVO existants et ajoutez la liste suivante aux autorisations S3. Vous devez inclure `"Resource": "arn:aws:s3:::*"` et attribuez toutes les autorisations nécessaires qui doivent être associées au bucket.

"Action": ["S3:ListBucket" "S3:GetBucketLocation"] "Ressource": "arn:aws:s3:::*", "Effet": "Autoriser" }, { "Action": ["S3:GetObject", "S3:PutObject", "S3:DeleteObject", "S3:ListAllMyBuckets", "S3:PutObjectTagging", "S3:GetObjectTagging", "S3:RestoreObject", "S3:GetBucketObjectLockConfiguration", "S3:GetObjectRetention", "S3:PutBucketObjectLockConfiguration", "S3:PutObjectRetention"] "Ressource": "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 « * » :

```
[ec2-user@ip-10-160-4-68 ~]$ 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 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 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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données primaires contenues dans les copies Snapshot.

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 .

REMARQUE 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" .

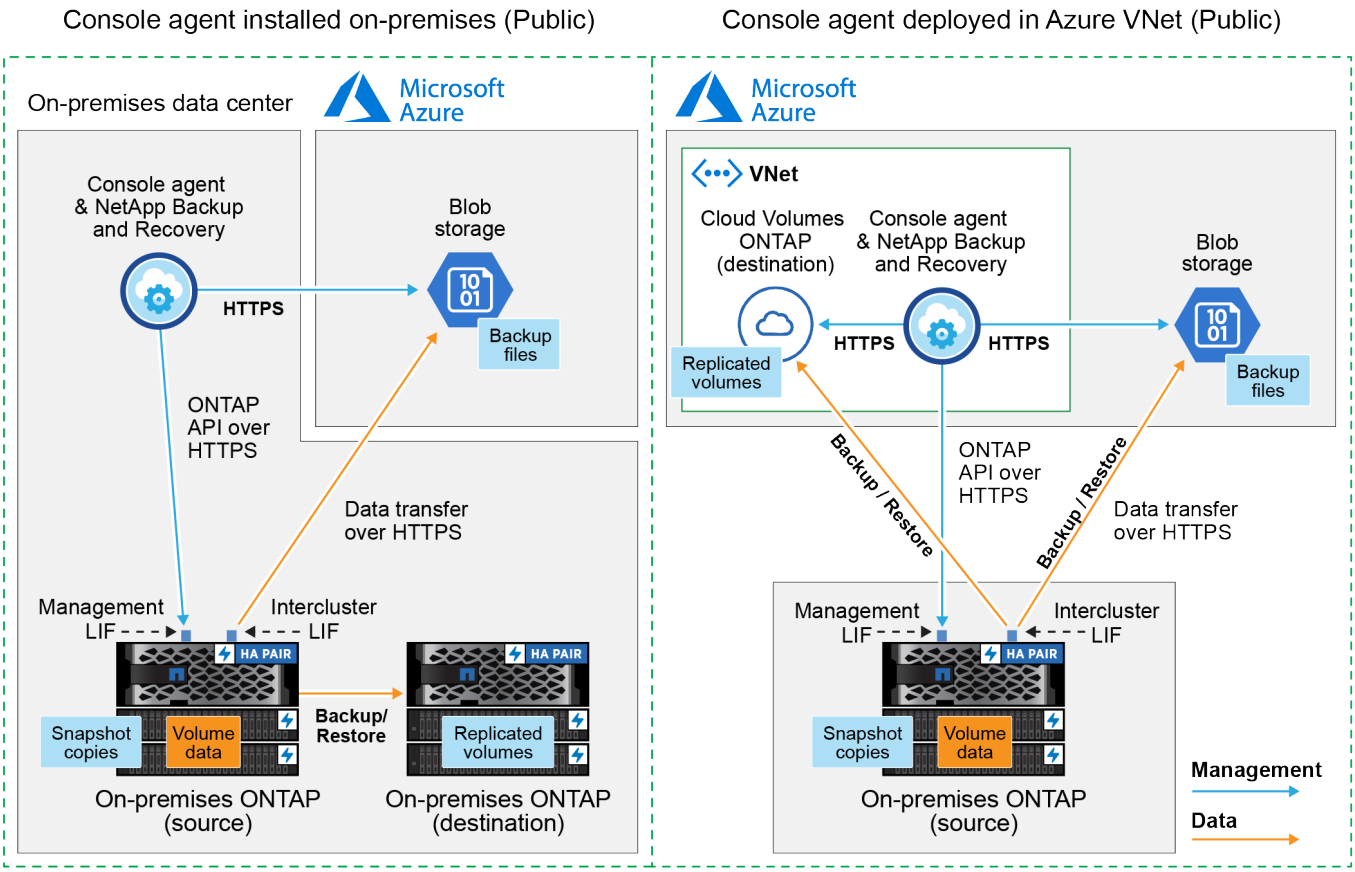
Identifier la méthode de connexion

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

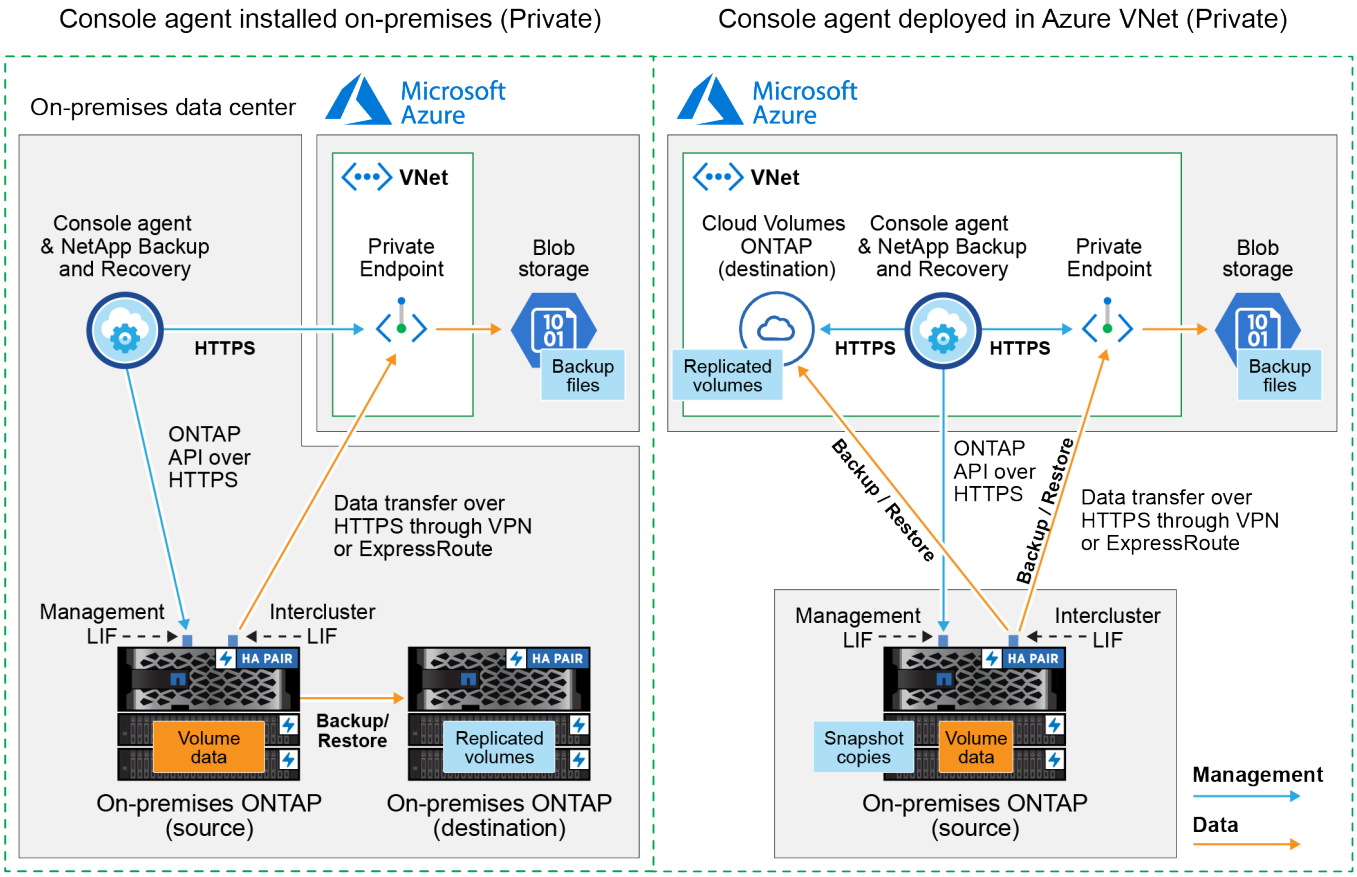
- **Connexion publique** - Connectez directement le système ONTAP au stockage Azure Blob à l'aide d'un point de terminaison Azure public.
- **Connexion privée** - Utilisez un VPN ou ExpressRoute et acheminez le trafic via un point de terminaison privé VNet qui utilise une adresse IP privée.

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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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 .

REMARQUE 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" .

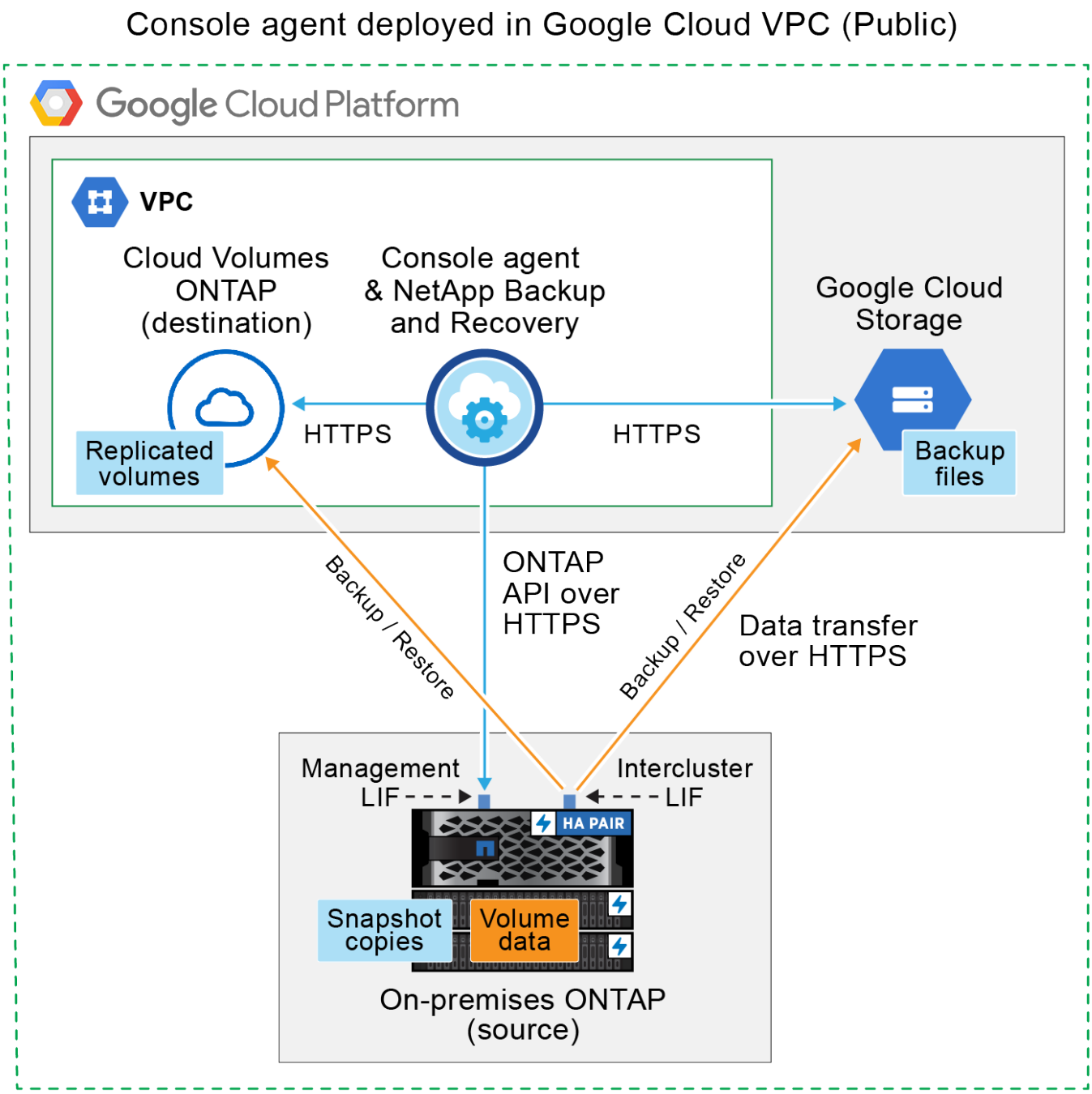
Identifier la méthode de connexion

Choisissez laquelle des deux méthodes de connexion vous utiliserez lors de la configuration des sauvegardes des systèmes ONTAP locaux vers Google Cloud Storage.

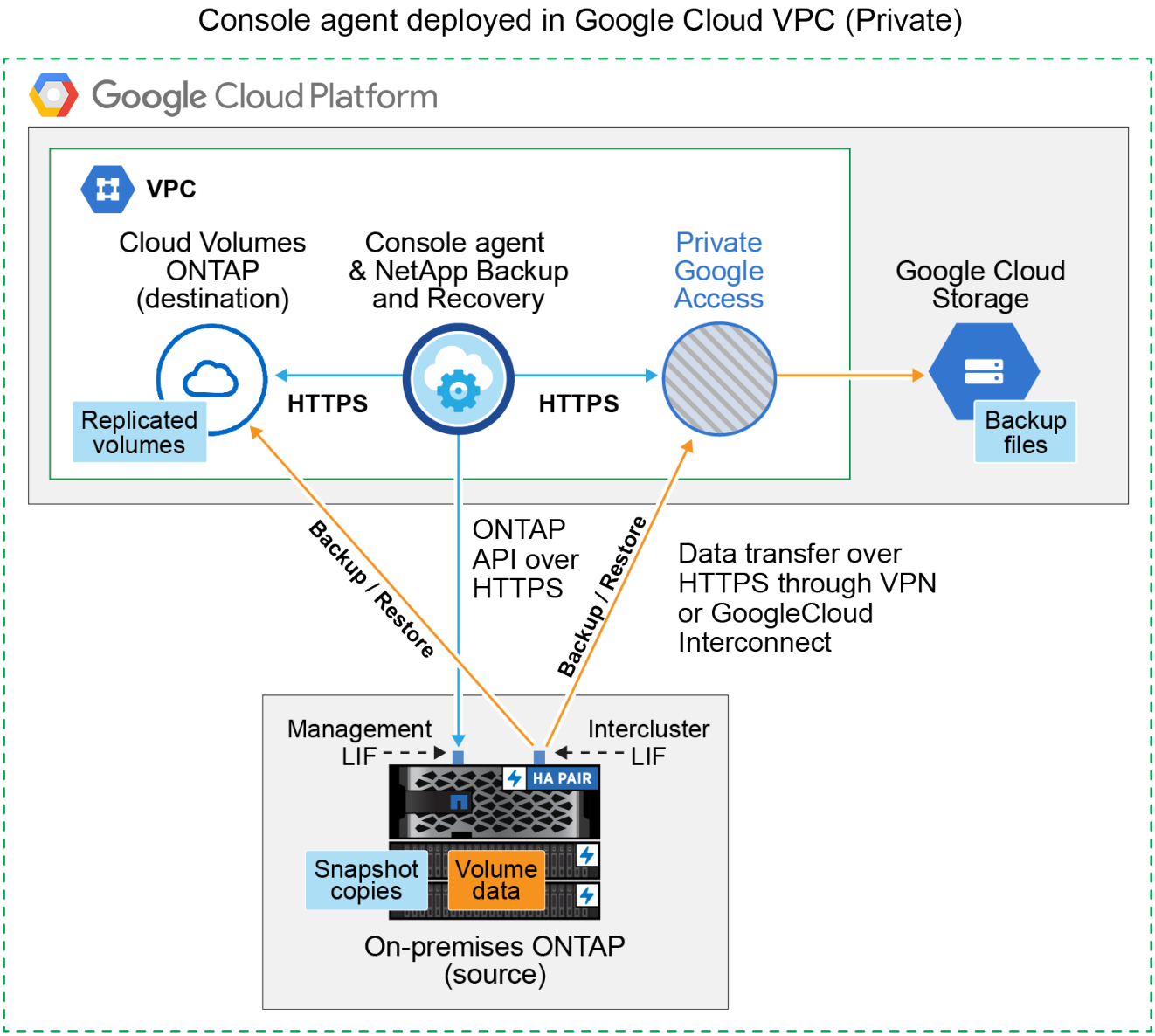
- **Connexion publique** - Connectez directement le système ONTAP à Google Cloud Storage à l'aide d'un point de terminaison Google public.
- **Connexion privée** - Utilisez un VPN ou Google Cloud Interconnect et acheminez le trafic via une interface d'accès privé Google qui utilise une adresse IP privée.

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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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.

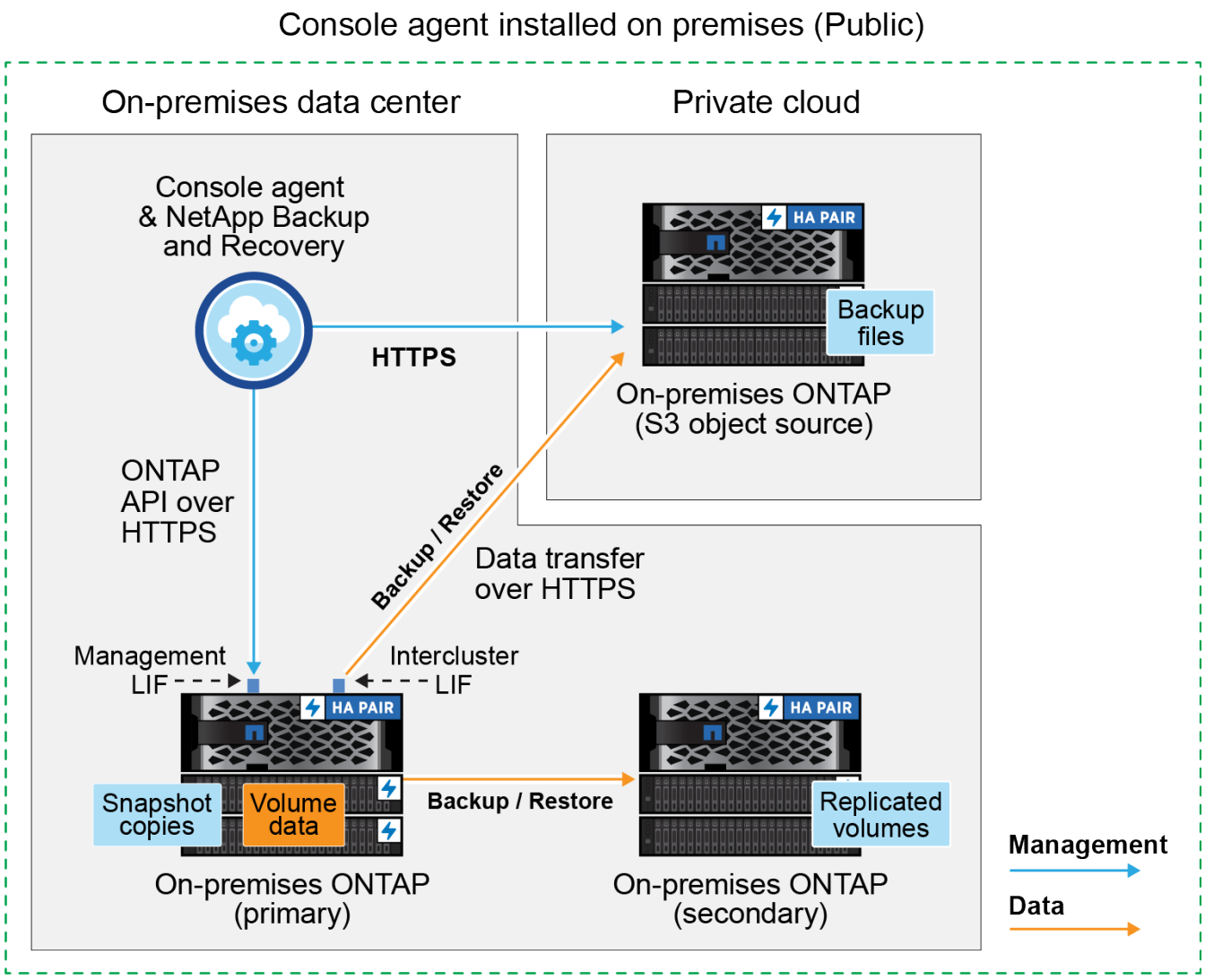
Le système ONTAP principal sur site peut être un système FAS, AFF ou ONTAP Select . Le système ONTAP secondaire peut être un système ONTAP local ou Cloud Volumes ONTAP . Le stockage d'objets peut se trouver sur un système ONTAP local ou sur un système Cloud Volumes ONTAP sur lequel vous avez activé un serveur de stockage d'objets Simple Storage Service (S3).

> **REMARQUE** 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

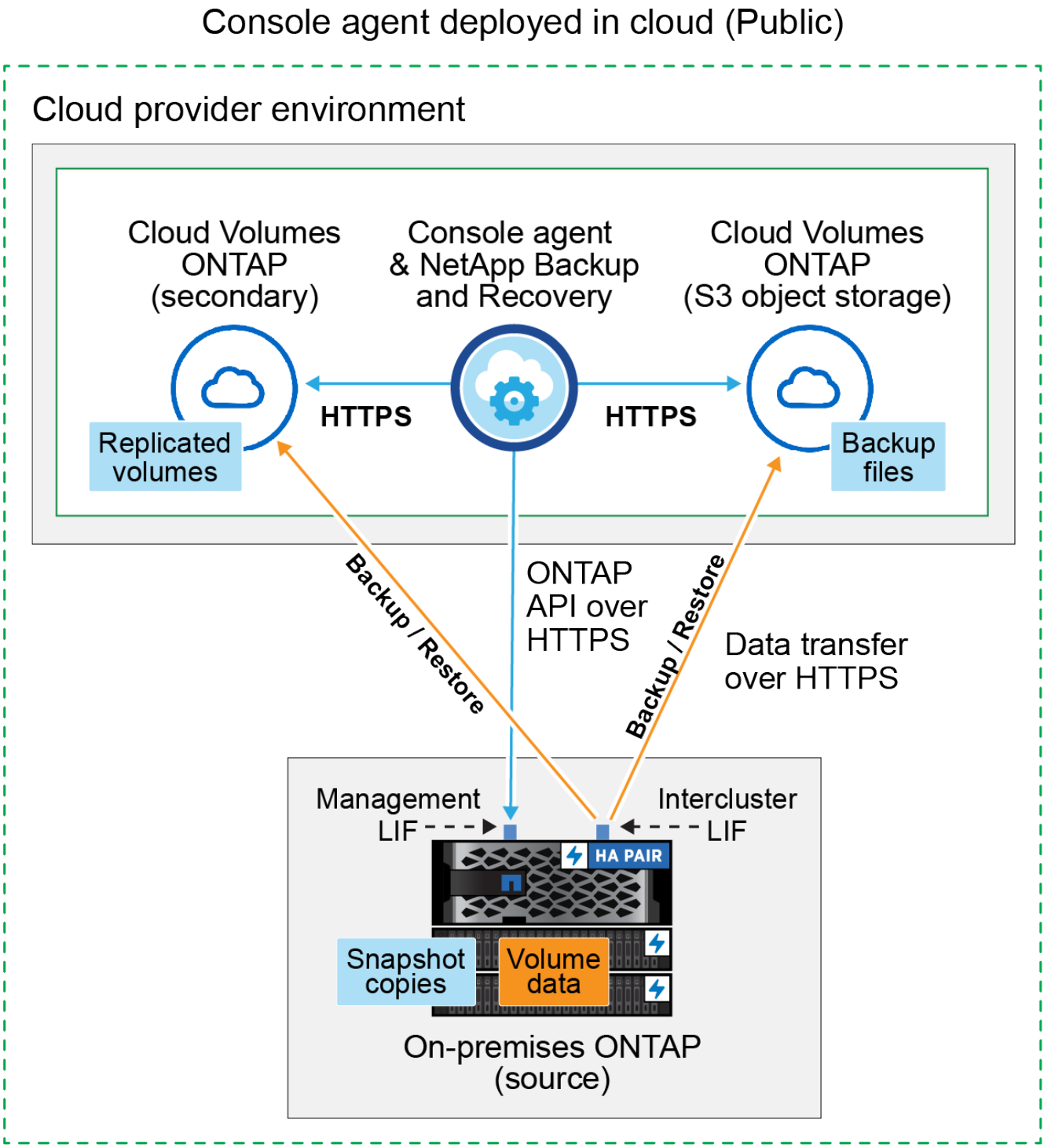
Il existe de nombreuses configurations dans lesquelles vous pouvez créer des sauvegardes dans un bucket S3 sur un système ONTAP . Deux scénarios sont présentés ci-dessous.

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 est destinée à la sauvegarde et à la restauration sur le stockage d'objets - aucune licence n'est nécessaire pour créer des copies Snapshot 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"
```

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 copies d'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 des copies Snapshot existantes vers le stockage d'objets en tant que fichiers de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de ce système qui 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 ultérieurs contiennent des copies différentielles des données de stockage principales contenues dans les copies instantanées.

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 .

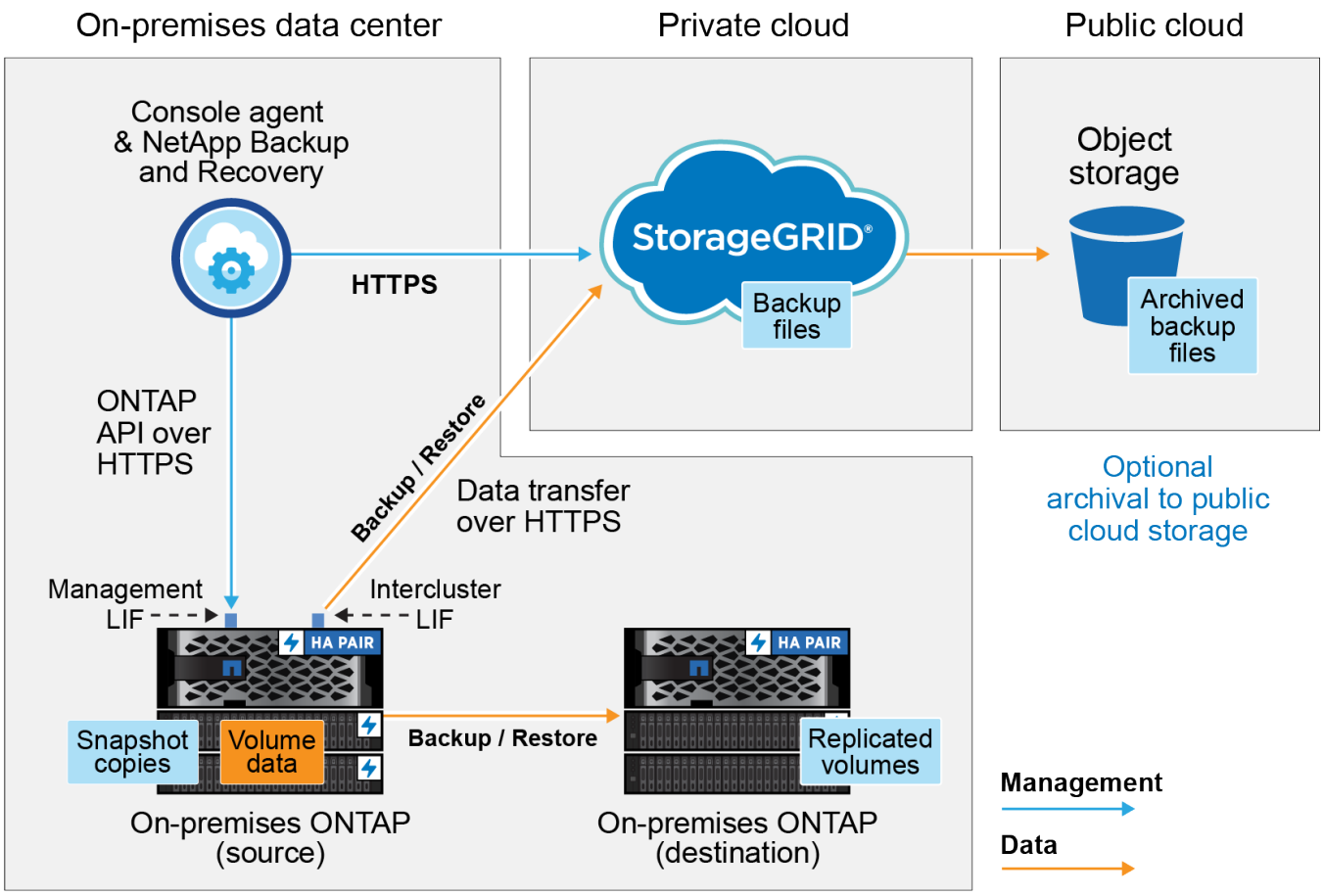
Les « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select .

REMARQUE 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 copies Snapshot 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 de 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

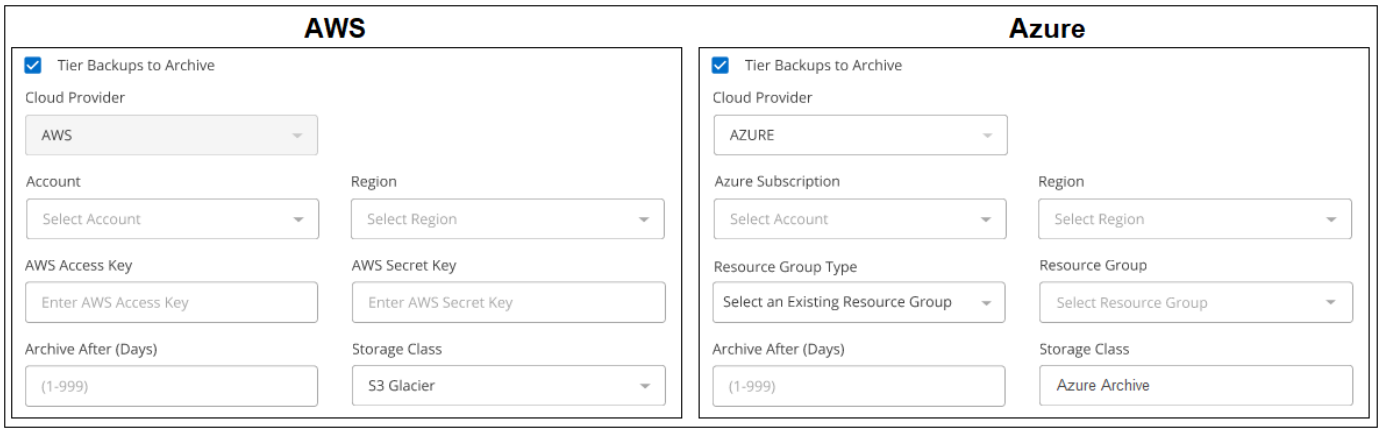
- Vous devrez créer un compte Amazon S3 pour l'espace de stockage où seront situées vos sauvegardes archivées.

- 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 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 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 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 : 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 des copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de ce système qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour ce système (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.
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 ultérieurs contiennent des copies différentielles des données de stockage principales contenues dans les copies Snapshot.

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 vers un autre ou vers une solution cloud telle que Cloud Volumes ONTAP ou Cloud Volumes Service, SnapMirror to Cloud Resync garantit que les sauvegardes cloud existantes restent intactes et opérationnelles.

Cette fonctionnalité élimine le besoin d'une opération de redéfinition de base longue et gourmande en ressources, permettant ainsi aux opérations de sauvegarde 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.

En maintenant la continuité des sauvegardes dans tous les environnements, SnapMirror to Cloud Resync améliore l'efficacité opérationnelle et réduit la complexité de la gestion des données hybrides et multicloud.

REMARQUE 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.
- La dernière sauvegarde dans le stockage d'objets doit être l'instantané commun à l'ancienne source, à la nouvelle source et au magasin d'objets. L'instantané commun ne peut pas être plus ancien que le dernier instantané sauvegardé dans le magasin d'objets.

- Les stratégies de snapshot et de SnapMirror , qui étaient utilisées sur l'ancien ONTAP, doivent être créées sur le nouveau cluster ONTAP avant de démarrer l'opération de resynchronisation. Si une politique doit être utilisée dans le processus de resynchronisation, cette politique doit également être créée. L'opération de resynchronisation ne crée pas les politiques.
- 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 comme des points de restauration. Vol1 est déjà sauvegardé sur un point de terminaison de magasin d'objets cloud à l'aide de SnapMirror to Cloud (SM-C). Cependant, seuls S1 et S2 ont été sauvegardés dans le magasin d'objets jusqu'à présent.

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.

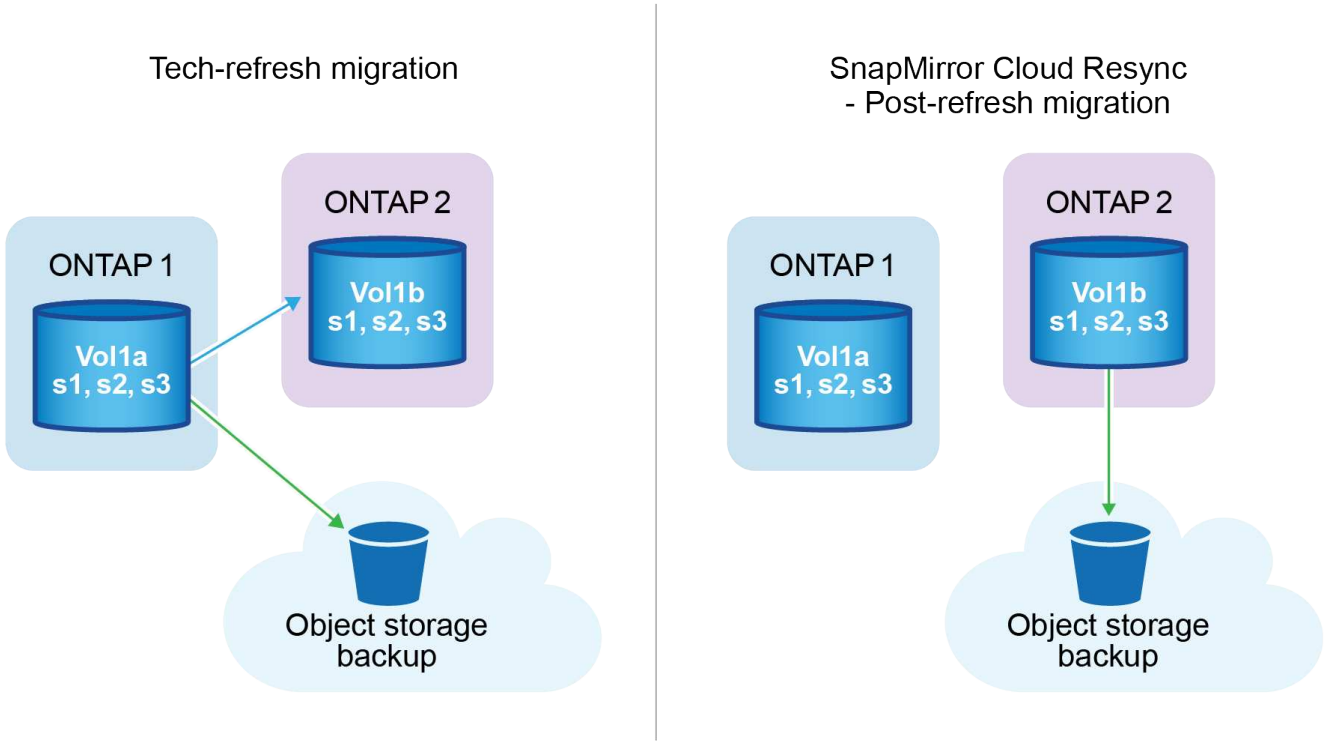
À ce stade, vous souhaitez continuer à sauvegarder Vol1b sur le même point de terminaison cloud. Mais au lieu de démarrer une sauvegarde complète à partir de zéro (ce qui prendrait du temps et des ressources), vous utilisez SnapMirror to Cloud Resync.

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 de renvoyer des données déjà sauvegardées, économise de la bande passante et garantit que votre chaîne de sauvegarde se poursuit sans problème après la migration.



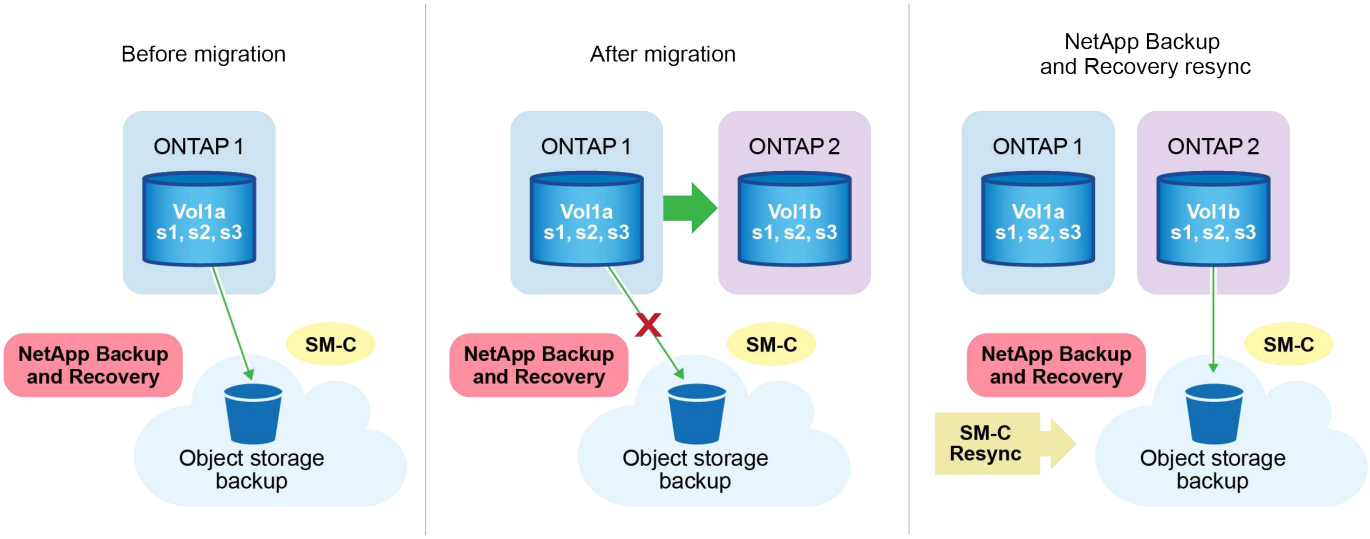
Notes de procédure

- 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 est chargée de créer la relation SnapMirror entre les clusters ONTAP source et de destination pour faciliter la migration 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 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.

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
```

Entrez le mot de passe.

```
mysql> show tables;
mysql> select * from volume;
```

Vérifiez si les volumes affichés sont les mêmes que ceux qui existaient dans 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":"pa
ssword"}
> '
```

   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*.

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 copies instantanées, les volumes répliqués et les fichiers de sauvegarde dans le stockage d'objets. Vous pouvez également désinscrire NetApp Backup and Recovery.

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.

REMARQUE 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 copies instantanées, les volumes répliqués et les fichiers de sauvegarde dans le stockage d'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 « Copies de snapshots locaux », « Volumes répliqués » et « Sauvegardes dans le stockage d'objets ».

   Chaque icône est bleue lorsque ce type de sauvegarde est activé et elle est grise lorsque le type de sauvegarde est inactif. Vous pouvez passer votre curseur sur chaque icône pour voir la politique de sauvegarde utilisée et 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. Depuis l'onglet **Volumes**, identifiez le volume sur lequel vous souhaitez activer les sauvegardes, sélectionnez le menu Actions ••• à la fin de la ligne, puis sélectionnez **Activer la sauvegarde**.
2. Dans la page *Définir la stratégie de sauvegarde*, sélectionnez l'architecture de sauvegarde, puis définissez les politiques et autres détails pour les copies de snapshots 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 politiques de vos copies instantanées locales, de vos volumes répliqués et de 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 l'onglet **Volumes**, identifiez le volume pour lequel vous souhaitez modifier la stratégie, sélectionnez le menu Actions ••• à la fin de la ligne et sélectionnez **Modifier la stratégie de sauvegarde**.
2. Dans la page *Modifier la stratégie de sauvegarde*, apportez des modifications aux stratégies de sauvegarde existantes pour les copies de snapshots 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 initialise uniquement cinq volumes à la fois. Une fois ces opérations terminées, il crée le lot suivant de cinq sous-tâches pour démarrer l'ensemble suivant et continue 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**
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. Dans la page de sauvegarde qui s'affiche, modifiez les stratégies de sauvegarde existantes pour les copies d'instantanés locaux, les volumes répliqués ou les fichiers de sauvegarde et 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 une copie instantanée ad hoc ou une sauvegarde sur un objet 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 copies instantanées 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	Suspendez le transfert incrémentiel des copies Snapshot 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.

Action	Description
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 tous les fichiers de sauvegarde qui ont été hiérarchisés vers le stockage d'archivage sont laissés dans ce niveau si vous arrêtez de hiérarchiser les sauvegardes vers l'archive - ils ne sont pas automatiquement déplacés vers le niveau standard. Seules les nouvelles sauvegardes de volume résideront 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 copies instantanées ou 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 de l'environnement de travail).

   > 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 de l'environnement de travail).

   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'une copie instantanée de volume ou d'une sauvegarde dans le 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 copies instantanées disponibles sont affichées.

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 les données ONTAP à partir de fichiers de sauvegarde avec NetApp Backup and Recovery

Les sauvegardes de vos données de volume ONTAP sont disponibles à partir des emplacements où vous avez créé des sauvegardes : copies instantanées, volumes répliqués et sauvegardes stockées dans le stockage d'objets. Vous pouvez restaurer des données à partir d'un moment précis à partir de n'importe lequel de ces emplacements de sauvegarde. Avec NetApp Backup and Recovery, restaurez un volume ONTAP entier à partir d'un fichier de sauvegarde ou, si vous avez seulement besoin de restaurer quelques fichiers, restaurez un dossier ou des fichiers individuels.

REMARQUE 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.

Une licence NetApp Backup and Recovery valide est requise pour restaurer les données des fichiers de sauvegarde 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
- Copie instantanée → 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. Vous accédez au tableau de bord de restauration en cliquant sur **Sauvegarde et récupération** dans le menu de la console, puis en cliquant sur l'onglet **Restaurer**. Vous pouvez également cliquer sur > **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
Aucune ressource supplémentaire du fournisseur de cloud n'est requise	Lorsque vous restaurez à partir du cloud, des ressources de bucket et de fournisseur de cloud public supplémentaires sont requises par compte.

Parcourir et restaurer	Rechercher et restaurer
Aucun coût supplémentaire n'est requis pour le fournisseur de cloud	Lorsque vous restaurez à partir du cloud, des coûts supplémentaires sont nécessaires lors de l'analyse de vos sauvegardes et volumes pour obtenir des résultats de recherche.
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
Copie instantanée	Oui	Non	Non	Oui	Oui	Oui
Volume répliqué	Oui	Non	Non	Oui	Oui	Oui
Fichier de sauvegarde	Oui	Oui	Oui	Oui	Oui	Oui

Avant de pouvoir utiliser l'une ou l'autre méthode de restauration, assurez-vous d'avoir configuré votre environnement pour les besoins uniques en ressources. Ces exigences sont décrites dans les sections ci-dessous.

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

Restaurer les données ONTAP à l'aide de Parcourir et restaurer

Avant de commencer à restaurer un volume, un dossier ou un fichier, vous devez connaître le nom du volume à partir duquel vous souhaitez effectuer la restauration, le nom du système et du SVM où réside le volume, ainsi que la date approximative du fichier de sauvegarde à partir duquel vous souhaitez effectuer la restauration. Vous pouvez restaurer les données ONTAP à partir d'une copie Snapshot, d'un volume répliqué ou de sauvegardes stockées dans le stockage d'objets.

Remarque : si le fichier de sauvegarde contenant les données que vous souhaitez restaurer réside dans un stockage cloud d'archivage (à partir d' ONTAP 9.10.1), l'opération de restauration prendra plus de temps et entraînera un coût. De plus, le cluster de destination doit également exécuter ONTAP 9.10.1 ou une version ultérieure pour la restauration de volumes, 9.11.1 pour la restauration de fichiers, 9.12.1 pour Google Archive et StorageGRID et 9.13.1 pour la restauration de dossiers.

"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 copies instantanées résident sur le système source et ne peuvent être restaurées 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 ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Cloud Volumes ONTAP dans AWS Système ONTAP sur site endif::aws[] ifdef::azure[]	Azure Blob
Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP local Azure endif::azure[] ifdef::gcp[]	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 endif::gcp[]	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.

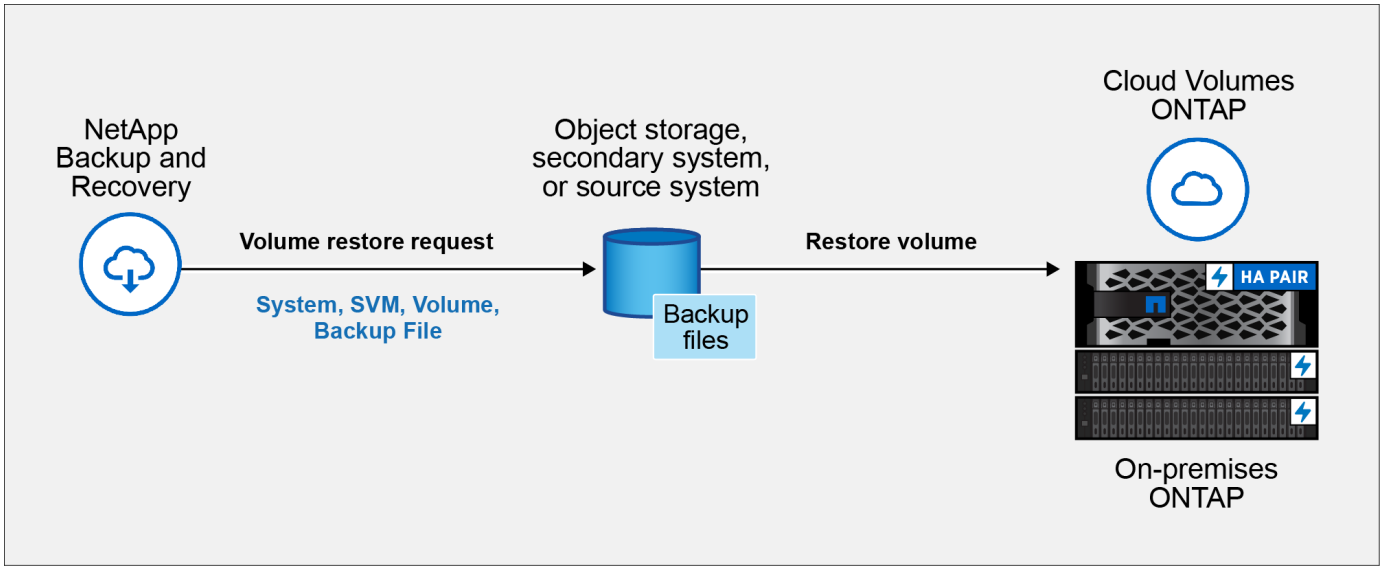
Restaurer les volumes à l'aide de Parcourir et restaurer

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.



Comme vous pouvez le voir, vous devrez connaître le nom du système source, la machine virtuelle de stockage, le nom du volume et la date du fichier de sauvegarde pour effectuer une restauration de volume.

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 (Snapshot) est **Local** (une copie Snapshot

sur le système source), **Secondaire** (un volume répliqué sur un système ONTAP secondaire) ou **Object Storage** (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.

       a. 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.

1. 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.
2. 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'une copie instantanée locale ou d'un fichier de sauvegarde résidant dans un système secondaire (un volume répliqué).

Si vous sélectionnez plusieurs fichiers, tous les fichiers sont restaurés sur le même volume de destination que vous choisissez. Donc, si vous souhaitez restaurer des fichiers sur différents volumes, vous devrez exécuter le processus de restauration 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" .

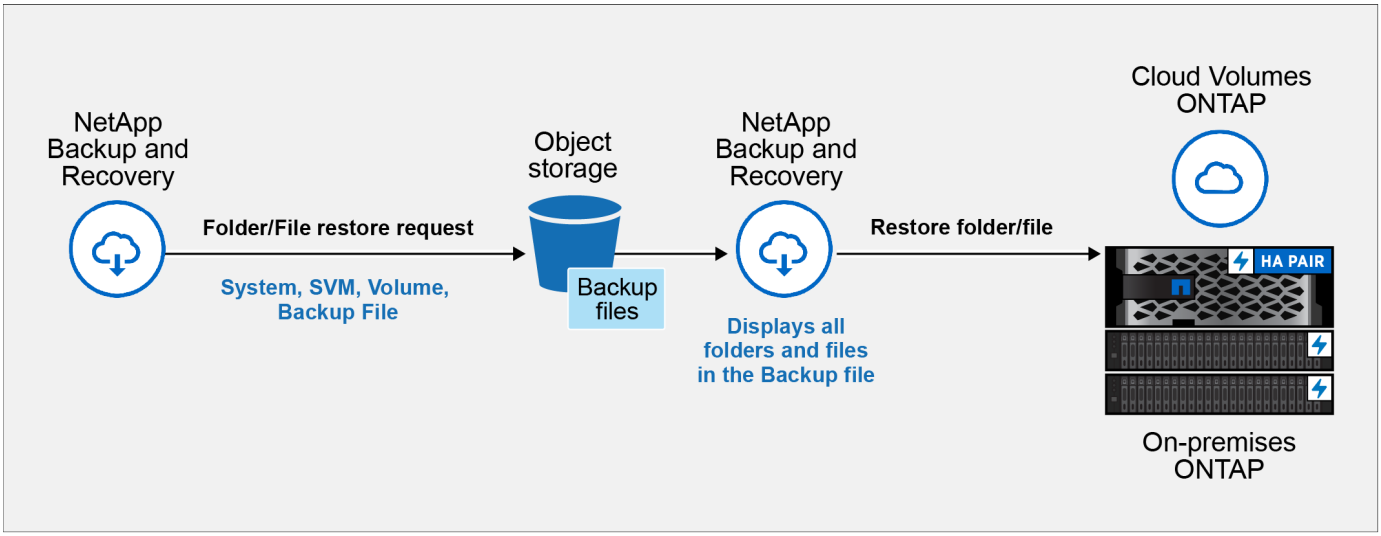
Prérequis

- 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.

Processus de restauration de dossiers et de fichiers

Le processus se déroule comme suit :

1. Lorsque vous souhaitez restaurer un dossier, ou un ou plusieurs fichiers, à partir d'une sauvegarde de volume, cliquez sur l'onglet **Restaurer**, puis sur **Restaurer les fichiers ou le dossier** sous *Parcourir et restaurer*.
2. Sélectionnez le système source, le volume et le fichier de sauvegarde dans lesquels résident le dossier ou les fichiers.
3. NetApp Backup and Recovery affiche les dossiers et fichiers qui existent dans le fichier de sauvegarde sélectionné.
4. Sélectionnez le dossier ou le(s) fichier(s) que vous souhaitez restaurer à partir de cette sauvegarde.
5. Sélectionnez l'emplacement de destination où vous souhaitez que le dossier ou les fichiers soient restaurés (le système, le volume et le dossier), puis cliquez sur **Restaurer**.
6. Le(s) fichier(s) sont restaurés.



Comme vous pouvez le voir, vous devez connaître le nom du système, le nom du volume, la date du fichier de sauvegarde et le nom du dossier/fichier pour effectuer une restauration de dossier ou de fichier.

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.

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.

       a. 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.

       a. Sélectionnez **Restaurer** et vous serez renvoyé au tableau de bord de restauration afin que vous puissiez examiner la progression de l'opération de restauration. Vous pouvez également cliquer sur l'onglet **Surveillance des tâches** pour voir la progression de la restauration.

Restaurer les données ONTAP à l'aide de la recherche et de la restauration

Vous pouvez restaurer un volume, un dossier ou des fichiers à partir d'un fichier de sauvegarde ONTAP à l'aide de la fonction Rechercher et restaurer. La recherche et la restauration vous permettent de rechercher un volume, un dossier ou un fichier spécifique à partir de toutes les sauvegardes, puis d'effectuer une restauration. Vous n'avez pas besoin de connaître le nom exact du système, le nom du volume ou le nom du fichier : la recherche examine tous les fichiers de sauvegarde de volume.

L'opération de recherche examine toutes les copies de snapshots locaux qui existent pour vos volumes ONTAP , tous les volumes répliqués sur les systèmes de stockage secondaires et tous les fichiers de sauvegarde qui existent dans le stockage d'objets. Étant donné que la restauration des données à partir d'une copie instantanée locale ou d'un volume répliqué peut être plus rapide et moins coûteuse que la restauration à partir d'un fichier de sauvegarde dans un stockage d'objets, vous souhaiterez peut-être restaurer les données à partir de ces autres emplacements.

Lorsque vous restaurez un *volume complet* à partir d'un fichier de sauvegarde, NetApp Backup and Recovery crée un *nouveau* volume à l'aide des données de la sauvegarde. Vous pouvez restaurer les données sous forme de volume dans le système d'origine, sur un autre système situé dans le même compte cloud que le système source ou sur un système ONTAP sur site.

Vous pouvez restaurer des *dossiers ou des fichiers* vers l'emplacement du volume d'origine, vers un volume différent dans le même système, vers un système différent utilisant le même compte cloud ou vers un volume sur un système ONTAP local.

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 du volume que vous souhaitez restaurer réside dans un stockage d'archives (disponible à partir d' ONTAP 9.10.1), l'opération de restauration prendra plus de temps et entraînera des coûts supplémentaires. Notez que le cluster de destination doit également exécuter ONTAP 9.10.1 ou supérieur pour la restauration de volume, 9.11.1 pour la restauration de fichiers, 9.12.1 pour Google Archive et StorageGRID et 9.13.1 pour la restauration de dossiers.

"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 copies instantanées résident sur le système source et ne peuvent être restaurées 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)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS	Cloud Volumes ONTAP dans AWS Système ONTAP sur site endif::aws[] ifdef::azure[]
Azure Blob	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP local Azure endif::azure[] ifdef::gcp[]
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 endif::gcp[]
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

- 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 de fichiers et de répertoires entre les copies Snapshot.)
- 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.

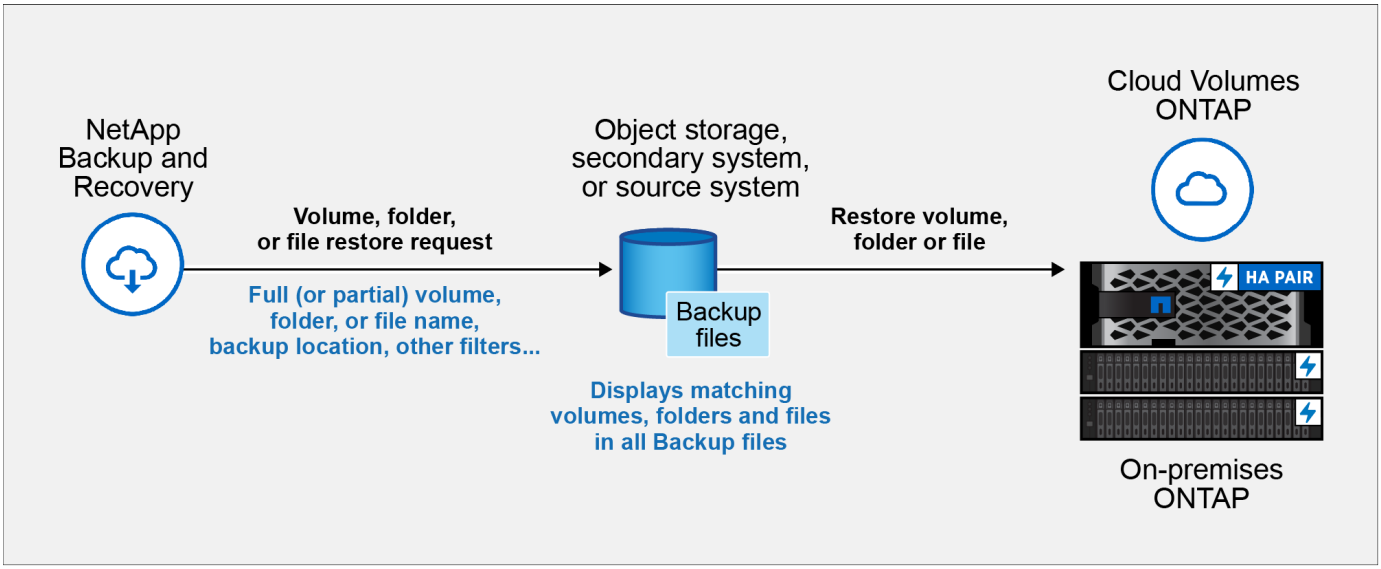
Processus de recherche et de restauration

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.



Comme vous pouvez le voir, vous n'avez besoin de connaître qu'un nom partiel et NetApp Backup and Recovery recherche tous les fichiers de sauvegarde correspondant à votre recherche.

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 v2

Le Catalogue Indexé v2, publié en février 2025 et mis à jour en juin 2025, comprend des fonctionnalités qui le rendent plus efficace et plus facile à utiliser. Cette version présente une amélioration significative des performances et est activée par défaut pour tous les nouveaux clients.

Passez en revue les considérations suivantes concernant la v2 :

- Le catalogue indexé v2 est disponible en mode aperçu.
- Si vous êtes un client existant et que vous souhaitez utiliser le Catalogue v2, vous devez réindexer complètement votre environnement.
- Le catalogue v2 indexe uniquement les instantanés qui ont une étiquette d'instantané.
- NetApp Backup and Recovery n'indexe pas les snapshots avec des étiquettes SnapMirror « horaires ». Si vous souhaitez indexer les instantanés avec l'étiquette SnapMirror « horaire », vous devez l'activer manuellement pendant que la v2 est en mode aperçu.
- NetApp Backup and Recovery indexera les volumes et les snapshots associés aux systèmes protégés par NetApp Backup and Recovery uniquement avec le catalogue v2. Les autres systèmes découverts sur la plateforme Console ne seront pas indexés.
- L'indexation des données avec Catalog v2 s'effectue dans des environnements locaux et dans des environnements Amazon Web Services, Microsoft Azure et Google Cloud Platform (GCP).

Le catalogue indexé v2 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.

Activation du catalogue indexé pour un système

Le service ne fournit pas de bucket séparé lorsque vous utilisez le catalogue indexé v2. 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.

Si vous avez activé le catalogue indexé avant la version v2, les événements suivants se produisent avec les systèmes :

- Pour les sauvegardes stockées dans AWS, il provisionne un nouveau compartiment S3 et le "Service de requête interactif Amazon Athena" et "Service d'intégration de données sans serveur AWS Glue" .
- Pour les sauvegardes stockées dans Azure, il provisionne un espace de travail Azure Synapse et un système de fichiers Data Lake comme conteneur qui stockera les données de l'espace de travail.
- Pour les sauvegardes stockées dans Google Cloud, il provisionne un nouveau bucket et le "Services Google Cloud BigQuery" sont provisionnés au niveau du compte/projet.
- Pour les sauvegardes stockées dans StorageGRID ou ONTAP S3, il provisionne de l'espace sur l'agent de la console ou sur l'environnement du fournisseur de cloud.

Si l'indexation a déjà été activée pour votre système, passez à la section suivante pour restaurer vos données.

Étapes pour activer l'indexation pour un système :

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 rechercher des résultats uniquement dans les copies instantanées disponibles ou les fichiers de sauvegarde 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 copies instantanées du volume local et les volumes répliqués distants qui contiennent le fichier dans votre recherche. Vous pouvez choisir de restaurer à partir du fichier de sauvegarde cloud, de la copie instantanée ou 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" .

Protégez les charges de travail Microsoft SQL Server

Présentation de la protection des charges de travail Microsoft SQL avec NetApp Backup and Recovery

Protégez les données de vos applications Microsoft SQL Server depuis les systèmes ONTAP locaux vers Amazon Web Services, Microsoft Azure ou StorageGRID à l'aide de NetApp Backup and Recovery. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé en fonction des politiques que vous créez. Vous pouvez 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 offrent une protection multicouche contre les menaces de cybersécurité internes (initiées) 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 facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait compromise.

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

Vous pouvez atteindre les objectifs de protection suivants :

- "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 généralement des politiques qui régissent 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 suivants et le stockage d'objets dans les fournisseurs de cloud public et privé. Les copies instantanées 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	NA ifdef::gcp[] endif::gcp[] ifdef::gcp[] endif::gcp[]

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 copies instantanées résident sur le système source et ne peuvent être restaurées 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 sur site ONTAP S3 ifdef::gcp[] endif::gcp[]
StorageGRID	Cloud Volumes ONTAP Système ONTAP sur site	Système ONTAP sur site ONTAP S3

À partir de l'emplacement du fichier de sauvegarde		Vers le système de destination
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\Sys
tem]

"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. Le service évalue le niveau de protection existant, y compris les politiques de protection de sauvegarde actuelles, les copies instantanées et les options de sauvegarde et de récupération.

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 dans la page 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 c'est la première fois que vous vous connectez à 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 version de 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** : 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. Pour afficher le tableau de bord de NetApp Backup and Recovery , dans le menu Sauvegarde et récupération, 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".

Sauvegardez les charges de travail Microsoft SQL Server avec NetApp Backup and Recovery

Sauvegardez les données des applications Microsoft SQL Server à partir des systèmes ONTAP locaux vers Amazon Web Services, Microsoft Azure et 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.
- Configurez le répertoire de journaux pour les hôtes découverts avant de lancer 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 lancer 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

Avant de sauvegarder vos charges de travail, définissez le chemin d'accès aux journaux d'activité des hôtes découverts. Cela vous aide à suivre l'état des opérations.

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. Fournissez le chemin de l'hôte ou parcourez une liste d'hôtes ou de nœuds hôtes sur l'hôte pour localiser l'endroit où vous souhaitez que le journal de l'hôte soit stocké.
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

Vous pouvez créer un groupe 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 charges de travail que vous souhaitez protéger ensemble.

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

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, 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

La suspension de la planification empêche temporairement l'exécution de la sauvegarde à l'heure planifiée. Vous souhaiterez peut-être le faire si vous effectuez une maintenance sur le système ou si vous rencontrez des problèmes avec la sauvegarde.

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

Vous pouvez créer un groupe 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 charges de travail que vous souhaitez protéger ensemble.

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 partir de copies instantanées, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage d'objets à l'aide de NetApp Backup and Recovery. Vous pouvez restaurer une charge de travail sur le système d'origine, sur un autre système utilisant le même compte cloud ou sur 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
- Restaurer à un moment précis dans le temps. Cela est utile si vous connaissez le nom et l'emplacement du fichier, ainsi que la date à laquelle il a été conservé en bon état pour la dernière fois.
- Restaurer la dernière sauvegarde

Considérations relatives à la restauration à partir du stockage d'objets

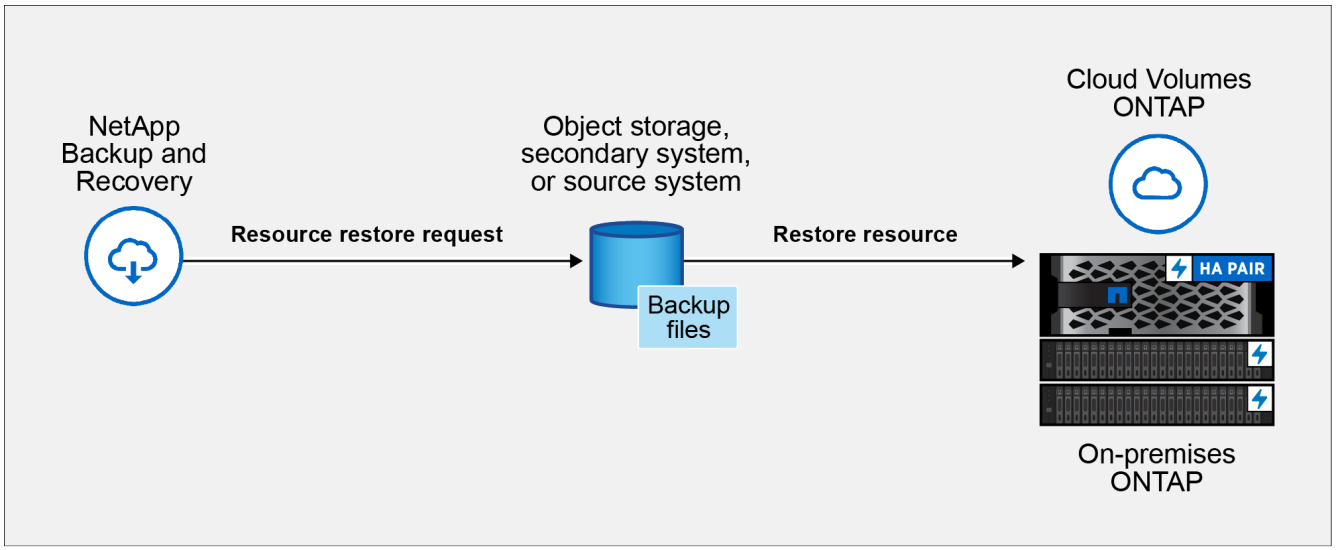
Si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que Ransomware Resilience est actif pour cette sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la stratégie de sauvegarde), vous êtes invité à exécuter une vérification d'intégrité supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'effectuer l'analyse.

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, 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

Vous pouvez restaurer les charges de travail à l'aide de l'une des méthodes suivantes. En règle générale, choisissez l'une des méthodes suivantes en fonction de vos besoins de restauration :

- **Depuis la page Restaurer** : utilisez cette option lorsque vous devez restaurer une ressource, mais que vous ne vous souvenez pas du nom exact, de l'emplacement où elle se trouve 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.
- **À partir de la page Inventaire** : utilisez cette option lorsque vous devez restaurer une ressource spécifique de la semaine ou du mois dernier, et que vous connaissez le nom et l'emplacement de la ressource, ainsi que la date à laquelle elle était en bon état pour la dernière fois. Vous parcourez une liste de ressources pour trouver celle que vous souhaitez restaurer.

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
    - Restaurer à un moment précis dans le temps. Cela est utile si vous connaissez le nom et l'emplacement du fichier, ainsi que la date à laquelle il a été conservé en bon état pour la dernière fois.
    - 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 l'onglet Bases de données, sélectionnez la base de données qui affiche un statut « Protégé » indiquant qu'il existe une sauvegarde que vous pouvez restaurer.

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 avec NetApp Backup and Recovery

Clonez les données des applications Microsoft SQL Server sur la même machine virtuelle ou sur une machine virtuelle différente à des fins de développement, de test ou de protection à l'aide de NetApp Backup and Recovery. Vous pouvez créer des clones à partir d'instantanés instantanés ou d'instantanés existants de vos charges de travail Microsoft SQL Server.

Choisissez entre les types de clones suivants :

- * Instantané et clonage instantanés * : vous pouvez créer un clone de vos charges de travail Microsoft SQL Server à partir d'un instantané. Un instantané est une copie ponctuelle 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.
- **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 l'instantané pour le clone et configurez les options du clone. Ceci est utile si vous souhaitez choisir l'instantané pour le clone et configurer les options.
   - **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 ne spécifiez pas de suffixe, le nom de la base de données clonée sera 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** :
   - **Attribuer automatiquement un point de montage** : sélectionnez cette option pour attribuer automatiquement un point de montage au clone. Le point de montage est l'emplacement où le clone sera monté 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.
    - **Préscripts et post-scripts** : Vous pouvez également spécifier des scripts de pré- et post-clonage à exécuter avant et après la création du clone. Ces scripts peuvent être utilisés pour 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 une ou plusieurs étiquettes qui vous aideront à rechercher ultérieurement le groupe de ressources et sélectionnez **Appliquer**. 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.
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 le groupe i à partir du système de stockage ONTAP principal ou secondaire.
    - **Préscripts et post-scripts** : Vous pouvez également spécifier des scripts de pré- et post-clonage à exécuter avant et après la création du clone. Ces scripts peuvent être utilisés pour 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

Vous souhaiterez peut-être ignorer une actualisation du clone si vous ne souhaitez pas mettre à jour le clone avec les dernières données de la charge de travail source. Ignorer une actualisation du clone vous permet de conserver le clone tel quel sans le mettre à jour.

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 le clone est protégé par une politique, le clone est supprimé, y compris le travail.

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 permet de gérer les informations de l'hôte de charge de travail, de la base de données et des instances de votre Microsoft SQL Server. Vous pouvez afficher, modifier et 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.

L'icône d'instantané local dans la colonne **Emplacement** de cette ligne doit apparaître 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 d'afficher l'état de vos sauvegardes, y compris le nombre de

sauvegardes, le nombre de sauvegardes réussies et le nombre de sauvegardes ayant échoué. Vous pouvez également afficher les détails de chaque sauvegarde, y compris le type de sauvegarde, le système de stockage utilisé pour la sauvegarde et l'heure de la sauvegarde.

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" .

Protégez les charges de travail VMware (Aperçu sans 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 offrent une protection multicouche contre les menaces de cybersécurité internes (initiées) 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 facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait compromise.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de 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 découverte, NetApp Backup and Recovery analyse les charges de travail VMware au sein de votre organisation et évalue et importe les politiques de protection existantes, les copies instantanées et les options de sauvegarde et de restauration.

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 existantes, les copies instantanées et les options de sauvegarde et de restauration 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 c'est la première fois que vous vous connectez à 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 version de 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 **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.

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. Vous pouvez créer un groupe de protection pour un ensemble de charges de travail que vous souhaitez sauvegarder et 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

La suspension d'un groupe de protection interrompt les sauvegardes planifiées pour le groupe de protection. Vous souhaiterez peut-être suspendre un groupe de protection si vous souhaitez arrêter temporairement les sauvegardes pour les charges de travail de ce groupe.

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

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 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 avec NetApp Backup and Recovery

Restaurez les charges de travail VMware à partir de copies instantanées, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage d'objets 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

Considérations relatives à la restauration à partir du stockage d'objets

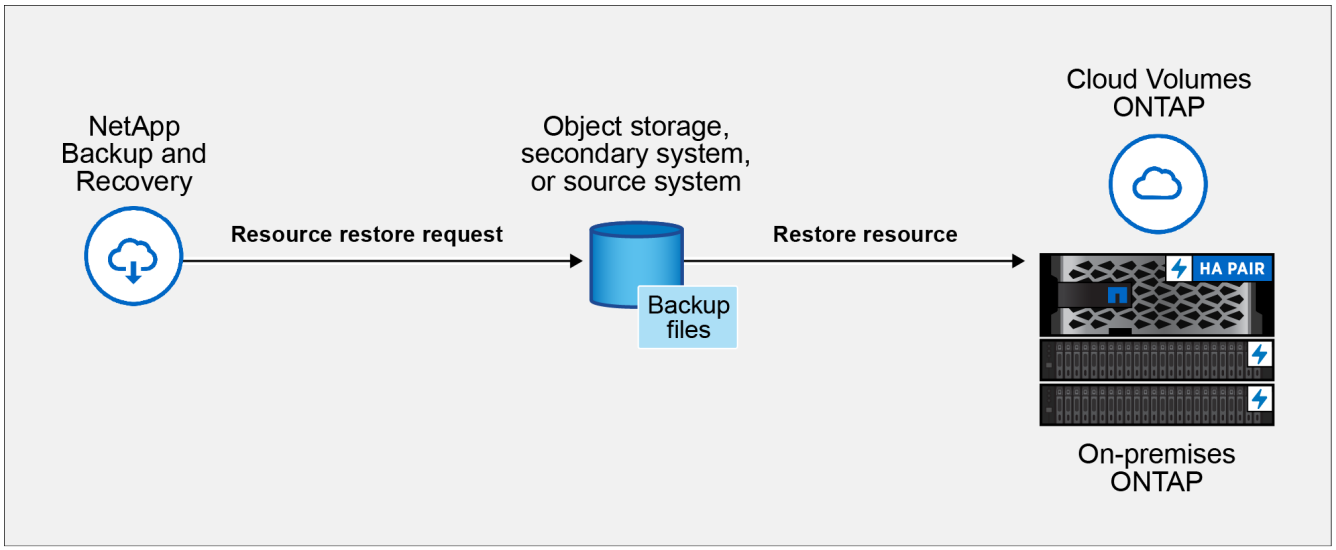
Si la résilience aux ransomwares est activée pour un fichier de sauvegarde dans le stockage d'objets, vous êtes invité à exécuter une vérification supplémentaire avant la restauration. Nous vous recommandons d'effectuer l'analyse.

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 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.



- 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 à droite du champ de recherche de nom, sélectionnez **Machines virtuelles**.
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 d'instantanés correspondant à vos critères de recherche apparaît.

4. Sélectionnez l'instantané que vous souhaitez restaurer.

   Une liste d'options d'emplacement de restauration s'affiche.

5. Sélectionnez l'emplacement de restauration où vous souhaitez restaurer l'instantané :
   - Local : restaure l'instantané à l'emplacement d'origine.
   - Stockage secondaire : restaure l'instantané vers un emplacement de stockage secondaire.

     Si vous choisissez un stockage secondaire, saisissez les emplacements source et de destination des données et des journaux.

   - Stockage d'objets : restaure l'instantané vers un emplacement de stockage d'objets.

Si vous choisissez le stockage d'objets, vérifiez si vous souhaitez analyser à nouveau l'instantané avant la restauration.

6. Sélectionnez **Terminé** ou **Suivant** pour continuer vers la page des paramètres de destination de restauration.

   Ensuite, choisissez les paramètres de destination et les options de pré- et post-restauration.

Sélection de la destination

1. Choisissez les paramètres de destination et les options de pré-restauration et de post-restauration.

Restaurer à l'emplacement d'origine

Dans la page Détails de la destination de restauration, saisissez les informations suivantes :

1. **Activer la restauration rapide** : sélectionnez cette option pour effectuer une opération de restauration rapide. Vous pouvez utiliser les volumes et les données restaurés 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 choisissez les types de notification souhaités.
5. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

Non disponible pour l'aperçu VMware.

Protégez les charges de travail VMware (avec le plug-in SnapCenter pour VMware)

Présentation de la protection des charges de travail des machines virtuelles dans NetApp Backup and Recovery

Protégez les charges de travail de vos machines virtuelles 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 pour les machines virtuelles, les banques de données et les VMDK.

Vous pouvez sauvegarder des banques de données sur Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform et StorageGRID et restaurer des machines virtuelles sur l'hôte SnapCenter Plug-in for VMware vSphere sur site.

REMARQUE 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" .

Pour obtenir des instructions sur la protection des charges de travail des machines virtuelles, consultez les rubriques suivantes :

- "Créer une politique pour les charges de travail VMware"
- "Sauvegarder les banques de données VMware sur Amazon Web Services"
- "Sauvegarder les banques de données VMware sur Microsoft Azure"
- "Sauvegarder les banques de données VMware sur Google Cloud Platform"
- "Sauvegarder les banques de données VMware sur StorageGRID"
- "Restaurer les charges de travail VMware"
- "Gérer la protection des charges de travail VMware"

Conditions préalables pour les charges de travail des machines virtuelles dans NetApp Backup and Recovery

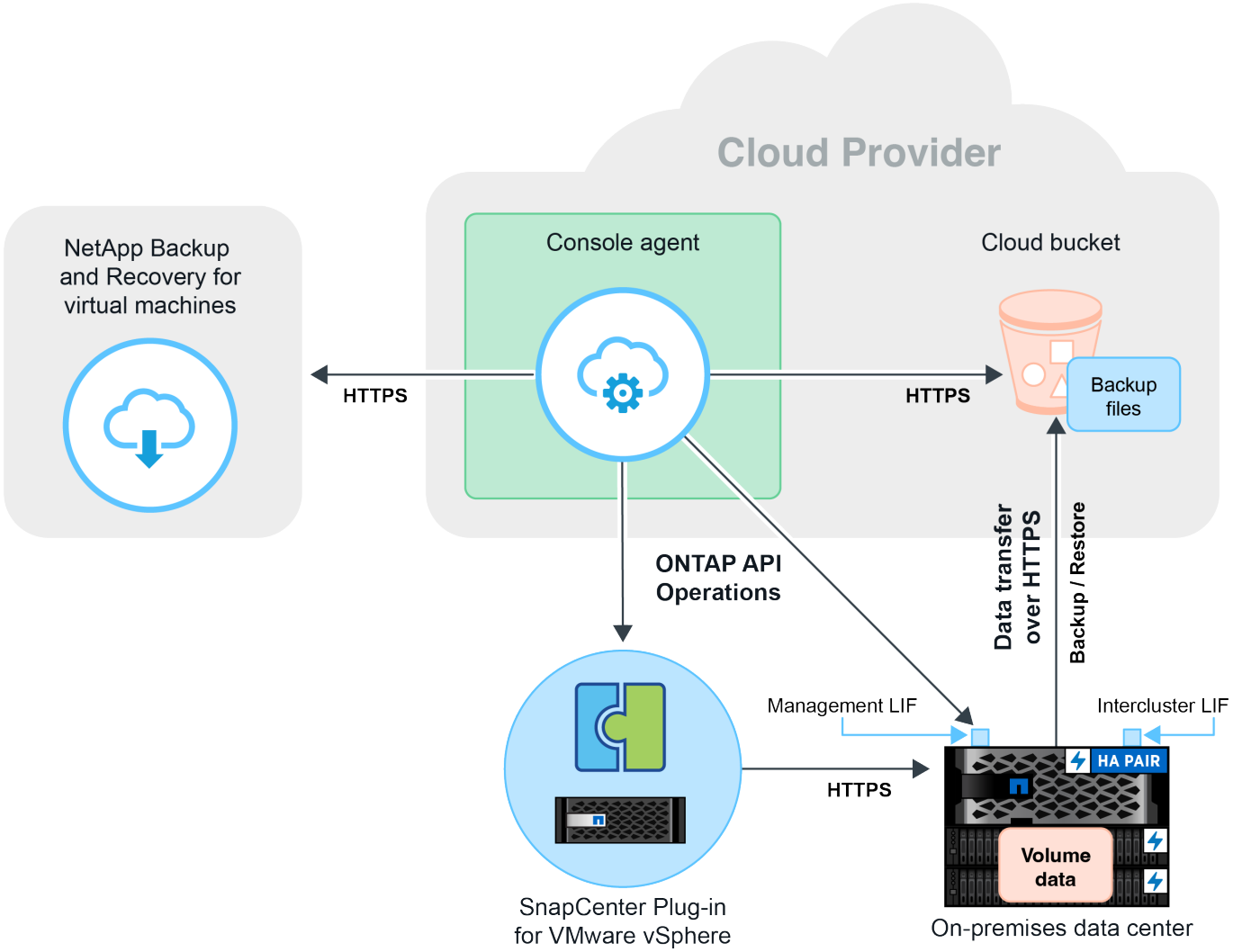
Avant de commencer à protéger les charges de travail de vos machines virtuelles avec NetApp Backup and Recovery, assurez-vous de remplir les conditions préalables suivantes :

- SnapCenter Plug-in for VMware vSphere 4.6P1 ou version ultérieure
  - Vous devez utiliser SnapCenter Plug-in for VMware vSphere 4.7P1 ou version ultérieure pour sauvegarder les banques de données à partir du stockage secondaire sur site.
- ONTAP 9.8 ou version ultérieure
- NetApp Console
- Les banques de données NFS et VMFS sont prises en charge. Les vVols ne sont pas pris en charge.
- Pour la prise en charge de VMFS, le SnapCenter Plug-in for VMware vSphere doit être exécuté sur la version 4.9 ou une version ultérieure. Assurez-vous d'effectuer une sauvegarde de la banque de données VMFS si l'hôte SnapCenter Plug-in for VMware vSphere a été mis à niveau d'une version antérieure vers la version 4.9.
- Au moins une sauvegarde doit avoir été effectuée dans SnapCenter Plug-in for VMware vSphere 4.6P1.
- Au moins une politique quotidienne, hebdomadaire ou mensuelle dans SnapCenter Plug-in for VMware vSphere sans étiquette ou avec la même étiquette que celle de la politique des machines virtuelles dans la console.
- Pour une stratégie prédéfinie, le niveau de planification doit être le même pour la banque de données dans SnapCenter Plug-in for VMware vSphere et dans le cloud.
- Assurez-vous qu'il n'y a pas de volumes FlexGroup dans la banque de données, car la sauvegarde et la restauration des volumes FlexGroup ne sont pas prises en charge.
- Désactivez « **_recent** » sur les groupes de ressources requis. Si vous avez activé « **_recent** » pour le

groupe de ressources, les sauvegardes de ces groupes de ressources ne peuvent pas être utilisées pour la protection des données dans le cloud et ne peuvent donc pas être utilisées pour l'opération de restauration.

- Assurez-vous que la banque de données de destination où la machine virtuelle sera restaurée dispose de suffisamment d'espace pour accueillir une copie de tous les fichiers de la machine virtuelle tels que VMDK, VMX, VMSD, etc.
- Assurez-vous que la banque de données de destination ne contient pas de fichiers de machine virtuelle obsolètes au format restore_xxx_xxxxxx_filename provenant des échecs d'opération de restauration précédents. Vous devez supprimer les fichiers obsolètes avant de déclencher une opération de restauration.
- Pour déployer un connecteur avec un proxy configuré, assurez-vous que tous les appels de connecteur sortants sont acheminés via le serveur proxy.
- Si un volume sauvegardant une banque de données est déjà protégé depuis l'onglet Volumes (NetApp Backup and Recovery → Volumes), la même banque de données ne peut pas être protégée à nouveau depuis l'onglet Machines virtuelles (NetApp Backup and Recovery → Machines virtuelles).

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



Enregistrez le SnapCenter Plug-in for VMware vSphere à utiliser avec NetApp Backup and Recovery

Vous devez enregistrer le SnapCenter Plug-in for VMware vSphere dans NetApp Backup and Recovery pour que les banques de données et les machines virtuelles soient affichées. Seul un utilisateur disposant d'un accès administratif peut enregistrer le SnapCenter Plug-in for VMware vSphere .

REMARQUE 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" .

Étapes

1. Dans l'interface utilisateur de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez * SnapCenter Plug-in for VMware vSphere*.
3. Sélectionnez **Enregistrer le SnapCenter Plug-in for VMware vSphere**.
4. Précisez les détails suivants :
   a. Dans le champ SnapCenter Plug-in for VMware vSphere , spécifiez le nom de domaine complet ou l'adresse IP de l'hôte SnapCenter Plug-in for VMware vSphere .
   b. Dans le champ Port, spécifiez le numéro de port sur lequel l'hôte SnapCenter Plug-in for VMware vSphere s'exécute.

      Vous devez vous assurer que la communication est ouverte entre l'hôte SnapCenter Plug-in for VMware vSphere sur site qui s'exécute sur le port 8144 par défaut et l'instance de l'agent de console qui peut s'exécuter dans n'importe quel fournisseur de cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform) ou sur site.

   c. Dans le champ Nom d'utilisateur et Mot de passe, spécifiez les informations d'identification de l'utilisateur vCenter avec le rôle d'administrateur.
5. Sélectionnez **S'inscrire**.

Après avoir fini

Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles** pour afficher toutes les banques de données et machines virtuelles protégées à l'aide du SnapCenter Plug-in for VMware vSphere .

Créer une politique de sauvegarde des banques de données dans NetApp Backup and Recovery

Vous pouvez créer une politique ou utiliser l'une des politiques prédéfinies suivantes disponibles dans NetApp Backup and Recovery.

REMARQUE 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

- Vous devez créer des politiques si vous ne souhaitez pas modifier les politiques prédéfinies.
- Pour déplacer des sauvegardes du magasin d'objets vers le stockage d'archivage, vous devez exécuter ONTAP 9.10.1 ou une version ultérieure et Amazon Web Services ou Microsoft Azure doit être le fournisseur de cloud.
- Vous devez configurer le niveau d'accès aux archives pour chaque fournisseur de cloud.

À propos de cette tâche

Les politiques prédéfinies suivantes sont disponibles dans la NetApp Console:

Nom de la politique	Étiquette	Valeur de rétention
1 an de rétention quotidienne à long terme (LTR)	Tous les jours	366
5 ans de LTR quotidien	Tous les jours	1830
LTR hebdomadaire sur 7 ans	Hebdomadaire	370
LTR mensuel sur 10 ans	Mensuel	120

Étapes

1. Dans la page Machines virtuelles, dans la liste déroulante Paramètres, sélectionnez **Politiques**.
2. Sélectionnez **Créer une politique**.
3. Dans la section Détails de la politique, spécifiez le nom de la politique.
4. Dans la section Rétention, sélectionnez l'un des types de rétention et spécifiez le nombre de sauvegardes à conserver.
5. Sélectionnez Principal ou Secondaire comme source de stockage de sauvegarde.
6. (Facultatif) Si vous souhaitez déplacer les sauvegardes du magasin d'objets vers le stockage d'archivage après un certain nombre de jours pour optimiser les coûts, cochez la case **Horaires de sauvegarde vers l'archivage** et saisissez le nombre de jours après lesquels la sauvegarde doit être archivée.
7. Sélectionnez **Créer**.

Vous ne pouvez pas modifier ou supprimer une politique associée à une banque de données.

Sauvegarder les banques de données sur Amazon Web Services dans NetApp Backup and Recovery

Vous pouvez sauvegarder et archiver un ou plusieurs magasins de données avec NetApp Backup and Recovery sur Amazon Web Services pour améliorer l'efficacité du stockage et la transition vers le cloud.

Si le magasin de données est associé à une politique d'archivage, vous avez la possibilité de sélectionner le niveau d'archivage. Les niveaux d'archivage pris en charge sont Glacier et Glacier Deep.

REMARQUE 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 d'avoir respecté toutes les"exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur de la console, sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant à la banque de données que vous souhaitez sauvegarder et cliquez sur **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajoutez le système.

   Configurez le LIF de gestion de cluster que vous souhaitez que la console découvre. Après avoir ajouté le système pour l'un des magasins de données, il peut être réutilisé pour tous les autres magasins de données résidant sur le même cluster ONTAP .

   a. Sélectionnez **Ajouter un système** correspondant au SVM.
   b. Dans l'assistant d'ajout de système :
      i. Spécifiez l'adresse IP du LIF de gestion du cluster.
      ii. Spécifiez les informations d'identification de l'utilisateur du cluster ONTAP .
   c. Sélectionnez **Ajouter un système**.
5. Sélectionnez **Amazon Web Services** pour le configurer comme fournisseur de cloud.
   a. Spécifiez le compte AWS.
   b. Dans le champ Clé d'accès AWS, spécifiez la clé de chiffrement des données.
   c. Dans le champ Clé secrète AWS, spécifiez le mot de passe pour le chiffrement des données.
   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   e. Spécifiez les adresses IP du LIF de gestion de cluster qui ont été ajoutées en tant que systèmes.
   f. Sélectionnez le niveau d'archivage.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité ponctuelle et vous ne pouvez pas la configurer ultérieurement.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Sauvegardez vos banques de données sur Microsoft Azure avec NetApp Backup and Recovery

Vous pouvez sauvegarder une ou plusieurs banques de données sur Microsoft Azure en intégrant le SnapCenter Plug-in for VMware vSphere à NetApp Backup and Recovery. Cela aidera les administrateurs de machines virtuelles à sauvegarder et archiver facilement et rapidement les données pour une efficacité de stockage et une accélération

de la transition vers le cloud.

Si le magasin de données est associé à une politique d'archivage, vous aurez la possibilité de sélectionner le niveau d'archivage. Le niveau d'archivage pris en charge est Azure Archive Blob Storage.

REMARQUE 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 d'avoir respecté toutes les"exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant à la banque de données que vous souhaitez sauvegarder et sélectionnez **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajoutez le système.

   Configurez le LIF de gestion de cluster que vous souhaitez que la console découvre. Après avoir ajouté le système pour l'un des magasins de données, il peut être réutilisé pour tous les autres magasins de données résidant sur le même cluster ONTAP .

   a. Sélectionnez **Ajouter un système** correspondant au SVM.
   b. Dans l'assistant d'ajout de système :
      i. Spécifiez l'adresse IP du LIF de gestion du cluster.
      ii. Spécifiez les informations d'identification de l'utilisateur du cluster ONTAP .
   c. Sélectionnez **Ajouter un système**.
5. Sélectionnez **Microsoft Azure** pour le configurer comme fournisseur de cloud.
   a. Spécifiez l'ID d'abonnement Azure.
   b. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   c. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant.
   d. Spécifiez les adresses IP du LIF de gestion de cluster qui ont été ajoutées en tant que systèmes.
   e. Sélectionnez le niveau d'archivage.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité ponctuelle et vous ne serez pas autorisé à le configurer ultérieurement.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Sauvegardez vos banques de données sur Google Cloud Platform avec NetApp Backup and Recovery

Vous pouvez sauvegarder une ou plusieurs banques de données sur Google Cloud Platform en intégrant le SnapCenter Plug-in for VMware vSphere à NetApp Backup and

Recovery. Cela aidera les administrateurs de machines virtuelles à sauvegarder et archiver facilement et rapidement les données pour une efficacité de stockage et une accélération de la transition vers le cloud.

REMARQUE 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 d'avoir respecté toutes les"exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant à la banque de données que vous souhaitez sauvegarder et sélectionnez **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajoutez le système.

   Configurez le LIF de gestion de cluster que vous souhaitez que la console découvre. Après avoir ajouté le système pour l'un des magasins de données, il peut être réutilisé pour tous les autres magasins de données résidant sur le même cluster ONTAP .

   a. Sélectionnez **Ajouter un système** correspondant au SVM.
   b. Dans l'assistant d'ajout de système :
      i. Spécifiez l'adresse IP du LIF de gestion du cluster.
      ii. Spécifiez les informations d'identification de l'utilisateur du cluster ONTAP .
   c. Sélectionnez **Ajouter un système**.
5. Sélectionnez **Google Cloud Platform** pour le configurer comme fournisseur de cloud.
   a. Sélectionnez le projet Google Cloud dans lequel vous souhaitez que le bucket Google Cloud Storage soit créé pour les sauvegardes.
   b. Dans le champ Clé d'accès Google Cloud, spécifiez la clé.
   c. Dans le champ Clé secrète Google Cloud, spécifiez le mot de passe.
   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   e. Spécifiez l'espace IP.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Sauvegardez les banques de données sur StorageGRID avec NetApp Backup and Recovery

Vous pouvez sauvegarder une ou plusieurs banques de données sur StorageGRID en intégrant le SnapCenter Plug-in for VMware vSphere avec NetApp Backup and Recovery. Cela aidera les administrateurs de machines virtuelles à sauvegarder et archiver facilement et rapidement les données pour une efficacité de stockage et une accélération

de la transition vers le cloud.

REMARQUE 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 d'avoir respecté toutes les"exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant à la banque de données que vous souhaitez sauvegarder et cliquez sur **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajoutez le système.

   Configurez le LIF de gestion de cluster que vous souhaitez que la console découvre. Après avoir ajouté le système pour l'un des magasins de données, il peut être réutilisé pour tous les autres magasins de données résidant sur le même cluster ONTAP .

   a. Sélectionnez **Ajouter un système** correspondant au SVM.
   b. Dans l'assistant d'ajout de système :
      i. Spécifiez l'adresse IP du LIF de gestion du cluster.
      ii. Spécifiez les informations d'identification de l'utilisateur du cluster ONTAP .
   c. Sélectionnez **Ajouter un système**.
5. Sélectionnez * StorageGRID*.
   a. Spécifiez l'adresse IP du serveur de stockage.
   b. Sélectionnez la clé d'accès et la clé secrète.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Gérer la protection des banques de données et des machines virtuelles dans NetApp Backup and Recovery

Vous pouvez afficher les politiques, les banques de données et les machines virtuelles avant de sauvegarder et de restaurer les données avec NetApp Backup and Recovery. En fonction de la modification apportée à la base de données, aux stratégies ou aux groupes de ressources, vous pouvez afficher les mises à jour à partir de l'interface utilisateur de la NetApp Console .

REMARQUE 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" .

Voir les politiques

Vous pouvez afficher toutes les politiques prédéfinies par défaut. Pour chacune de ces politiques, lorsque vous affichez les détails, toutes les politiques et machines virtuelles associées sont répertoriées.

1. Dans l'interface utilisateur de la console, sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez **Politiques**.
3. Sélectionnez **Afficher les détails** correspondant à la politique dont vous souhaitez afficher les détails.

Les politiques et machines virtuelles associées sont répertoriées.

Afficher les magasins de données et les machines virtuelles

Les banques de données et les machines virtuelles protégées à l'aide du SnapCenter Plug-in for VMware vSphere sont affichées.

Étapes

1. Dans l'interface utilisateur de la console, sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles** > **Paramètres** > * SnapCenter Plug-in for VMware vSphere*.
2. Sélectionnez le SnapCenter Plug-in for VMware vSphere pour lequel vous souhaitez afficher les banques de données et les machines virtuelles.

Déprotéger les banques de données

Vous pouvez déprotéger une banque de données qui était déjà protégée auparavant. Vous pouvez déprotéger une banque de données lorsque vous souhaitez supprimer les sauvegardes dans le cloud ou que vous ne souhaitez plus la sauvegarder dans le cloud. Le magasin de données peut être à nouveau protégé une fois la déprotection réussie.

Étapes

1. Dans l'interface utilisateur de la console, sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionnez l'icône Actions ••• correspondant à la banque de données que vous souhaitez déprotéger et sélectionnez **Déprotéger**.

Modifier le SnapCenter Plug-in for VMware vSphere

Vous pouvez modifier les détails de l'hôte SnapCenter Plug-in for VMware vSphere dans la console.

Étapes

1. Dans l'interface utilisateur de la console, sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles** > **Paramètres** > * SnapCenter Plug-in for VMware vSphere*.
2. Sélectionnez l'icône Actions ••• et sélectionnez **Modifier**.
3. Modifiez les détails selon vos besoins.
4. Sélectionnez **Enregistrer**.

Actualiser les ressources et les sauvegardes

Si vous souhaitez afficher les derniers magasins de données et sauvegardes qui ont été ajoutés à l'application, vous devez actualiser les ressources et les sauvegardes. Cela lancera la découverte des ressources et des

sauvegardes et les derniers détails seront affichés.

1. Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez * SnapCenter Plug-in for VMware vSphere*.
3. Sélectionnez l'icône Actions ••• correspondant au SnapCenter Plug-in for VMware vSphere et sélectionnez **Actualiser les ressources et les sauvegardes**.

Actualiser la politique ou le groupe de ressources

En cas de modification de la politique ou du groupe de ressources, vous devez actualiser la relation de protection.

1. Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionnez l'icône Actions ••• correspondant au magasin de données et sélectionnez **Actualiser la protection**.

Désinscrire le SnapCenter Plug-in for VMware vSphere

Toutes les banques de données et machines virtuelles associées à l'hôte SnapCenter Plug-in for VMware vSphere ne seront pas protégées.

1. Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez * SnapCenter Plug-in for VMware vSphere*.
3. Sélectionnez l'icône Actions ••• correspondant au SnapCenter Plug-in for VMware vSphere et sélectionnez **Désinscrire**.

Surveiller les emplois

Des tâches sont créées pour toutes les opérations de NetApp Backup and Recovery . Vous pouvez surveiller tous les travaux et toutes les sous-tâches qui sont effectuées dans le cadre de chaque tâche.

1. Sélectionnez **Sauvegarde et récupération** > **Surveillance des tâches**.

   Lorsque vous lancez une opération, une fenêtre apparaît indiquant que la tâche est lancée. Vous pouvez sélectionner le lien pour surveiller le travail.

2. Sélectionnez la tâche principale pour afficher les sous-tâches et l'état de chacune de ces sous-tâches.

Restaurer les données des machines virtuelles avec NetApp Backup and Recovery

Vous pouvez restaurer les données des machines virtuelles depuis le cloud vers le serveur vCenter local avec NetApp Backup and Recovery. Vous pouvez restaurer la machine virtuelle exactement au même emplacement à partir duquel la sauvegarde a été effectuée ou vers un autre emplacement. Si la machine virtuelle a été sauvegardée à l'aide d'une stratégie d'archivage, vous pouvez définir la priorité de restauration d'archivage.

Vous ne pouvez pas restaurer des machines virtuelles qui s'étendent sur plusieurs banques de données.

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 d'avoir respecté toutes les"exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.
- Si vous effectuez une restauration vers un autre emplacement :
  - Assurez-vous que les vCenters source et de destination sont en mode lié.
  - Assurez-vous que les détails du cluster source et de destination sont ajoutés dans la page **Systèmes** de la NetApp Console et dans les vCenters en mode lié dans les deux hôtes SnapCenter Plug-in for VMware vSphere .
  - Assurez-vous que le système est ajouté pour l'autre emplacement dans la page **Systèmes** de la console.

Étapes

1. Dans l'interface utilisateur de la console, sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles** > * SnapCenter Plug-in for VMware vSphere* et sélectionnez l'hôte SnapCenter Plug-in for VMware vSphere .

Si vous déplacez une machine virtuelle à l'aide de VMware vSphere vMotion et la restaurez à partir de la console, Backup and Recovery la restaure à l'emplacement de sauvegarde d'origine.

1. Vous pouvez restaurer la machine virtuelle à l'emplacement d'origine ou à un autre emplacement à partir du magasin de données ou des machines virtuelles :

Si vous souhaitez restaurer la machine virtuelle…	Fais ceci…
vers l’emplacement d’origine à partir du magasin de données	1. Sélectionnez l’icône Actions ••• correspondant à la banque de données que vous souhaitez restaurer et cliquez sur **Afficher les détails**. 2. Sélectionnez **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer. 3. Sélectionnez la machine virtuelle que vous souhaitez restaurer à partir de la sauvegarde et sélectionnez **Suivant**. 4. Assurez-vous que **Original** est sélectionné et sélectionnez **Continuer**. 5. Si la machine virtuelle est protégée à l’aide d’une politique dans laquelle les paramètres d’archivage sont configurés, sélectionnez **Priorité de restauration d’archivage** et sélectionnez **Suivant**. Les priorités de restauration d’archives prises en charge sont élevées, standard et faibles pour Amazon Web Services, et élevées et standard pour Microsoft Azure. 6. Vérifiez les détails et sélectionnez **Restaurer**.

Si vous souhaitez restaurer la machine virtuelle…	Fais ceci…
vers un autre emplacement à partir du magasin de données	1. Sélectionnez l'icône Actions ••• correspondant à la banque de données que vous souhaitez restaurer et sélectionnez **Afficher les détails**. 2. Sélectionnez **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer. 3. Sélectionnez la machine virtuelle que vous souhaitez restaurer à partir de la sauvegarde et sélectionnez **Suivant**. 4. Sélectionnez **Alternatif**. 5. Sélectionnez le serveur vCenter, l'hôte ESXi, la banque de données et le réseau alternatifs. 6. Donnez un nom à la machine virtuelle après la restauration et sélectionnez **Continuer**. 7. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Les priorités de restauration d'archives prises en charge sont élevées, standard et faibles pour Amazon Web Services, et élevées et standard pour Microsoft Azure. 8. Vérifiez les détails et sélectionnez **Restaurer**.
vers l'emplacement d'origine à partir des machines virtuelles	1. Sélectionnez l'icône Actions ••• correspondant à la machine virtuelle que vous souhaitez restaurer et sélectionnez **Restaurer**. 2. Sélectionnez la sauvegarde via laquelle vous souhaitez restaurer la machine virtuelle. 3. Assurez-vous que **Original** est sélectionné et sélectionnez **Continuer**. 4. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Les priorités de restauration d'archives prises en charge sont élevées, standard et faibles pour Amazon Web Services, et élevées et standard pour Microsoft Azure. 5. Vérifiez les détails et sélectionnez **Restaurer**.

Si vous souhaitez restaurer la machine virtuelle…	Fais ceci…
vers un autre emplacement à partir de machines virtuelles	1. Sélectionnez l'icône Actions ••• correspondant à la machine virtuelle que vous souhaitez restaurer et sélectionnez **Restaurer**. 2. Sélectionnez la sauvegarde via laquelle vous souhaitez restaurer la machine virtuelle. 3. Sélectionnez **Alternatif**. 4. Sélectionnez le serveur vCenter, l'hôte ESXi, la banque de données et le réseau alternatifs. 5. Donnez un nom à la machine virtuelle après la restauration et sélectionnez **Continuer**. 6. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Les priorités de restauration d'archives prises en charge sont élevées, standard et faibles pour Amazon Web Services, et élevées et standard pour Microsoft Azure. 7. Vérifiez les détails et sélectionnez **Restaurer**.

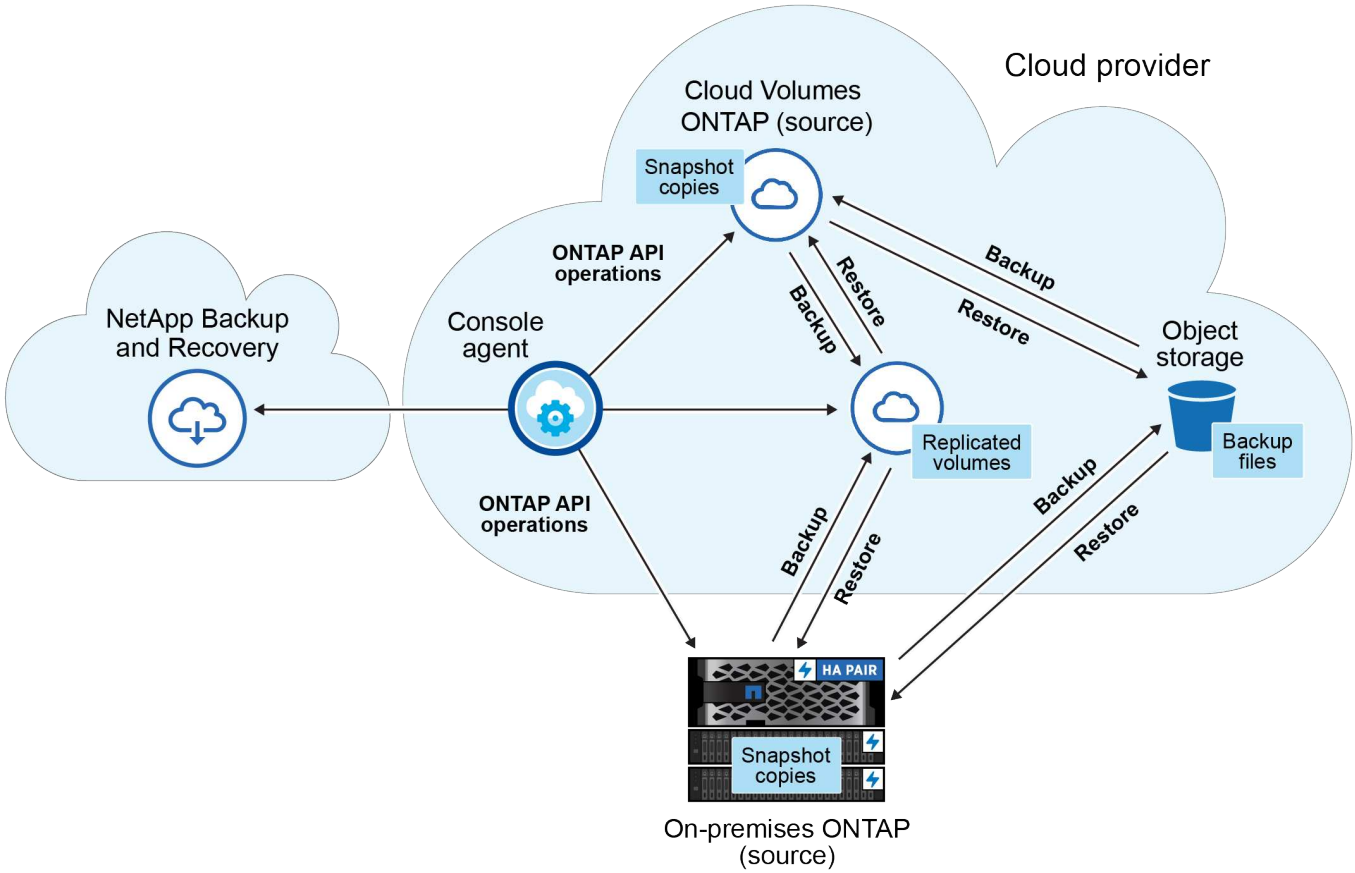
Si l'opération de restauration ne se termine pas, attendez que le moniteur de tâches affiche « Échec » avant de réessayer l'opération de restauration.

Protéger les charges de travail KVM (Aperçu)

Présentation de la protection des charges de travail KVM

Protégez vos machines virtuelles KVM et vos pools de stockage 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 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 offrent une protection multicouche contre les menaces de cybersécurité internes (initiées) 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 facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait 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 découvrir les hôtes KVM et les machines virtuelles avant de 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 KVM et découvrez des ressources

Ajoutez les informations de l'hôte KVM 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. Dans la mosaïque KVM, sélectionnez **Découvrir et gérer**.

   Si c'est la première fois que vous vous connectez à 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 version de NetApp Backup and Recovery» apparaît et affiche 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 enregistré les informations d'identification pour cet hôte KVM, 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. Choisissez d'utiliser des informations d'identification root ou non root.
      iv. Entrez le nom d'utilisateur et le mot de passe du compte.
      v. Sélectionnez **Terminé**.
   c. **Enregistrement de l'hôte** : ajoutez un nouvel hôte KVM. 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 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. Pour afficher le tableau de bord de NetApp Backup and Recovery , dans le menu supérieur, 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.

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 de copies instantanées, d'une sauvegarde de groupe de protection répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage d'objets 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 l'emplacement d'origine ; la restauration vers un autre emplacement n'est pas disponible dans cette version d'aperçu.

- 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 **Terminé** ou **Suivant** pour continuer vers la page des paramètres de destination de restauration.

   Ensuite, vous pouvez choisir les paramètres de destination et les options de pré-restauration et de post-restauration.

Sélection de la destination

1. Choisissez les paramètres de destination et les options de pré-restauration et de post-restauration.

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 pour l'aperçu KVM.

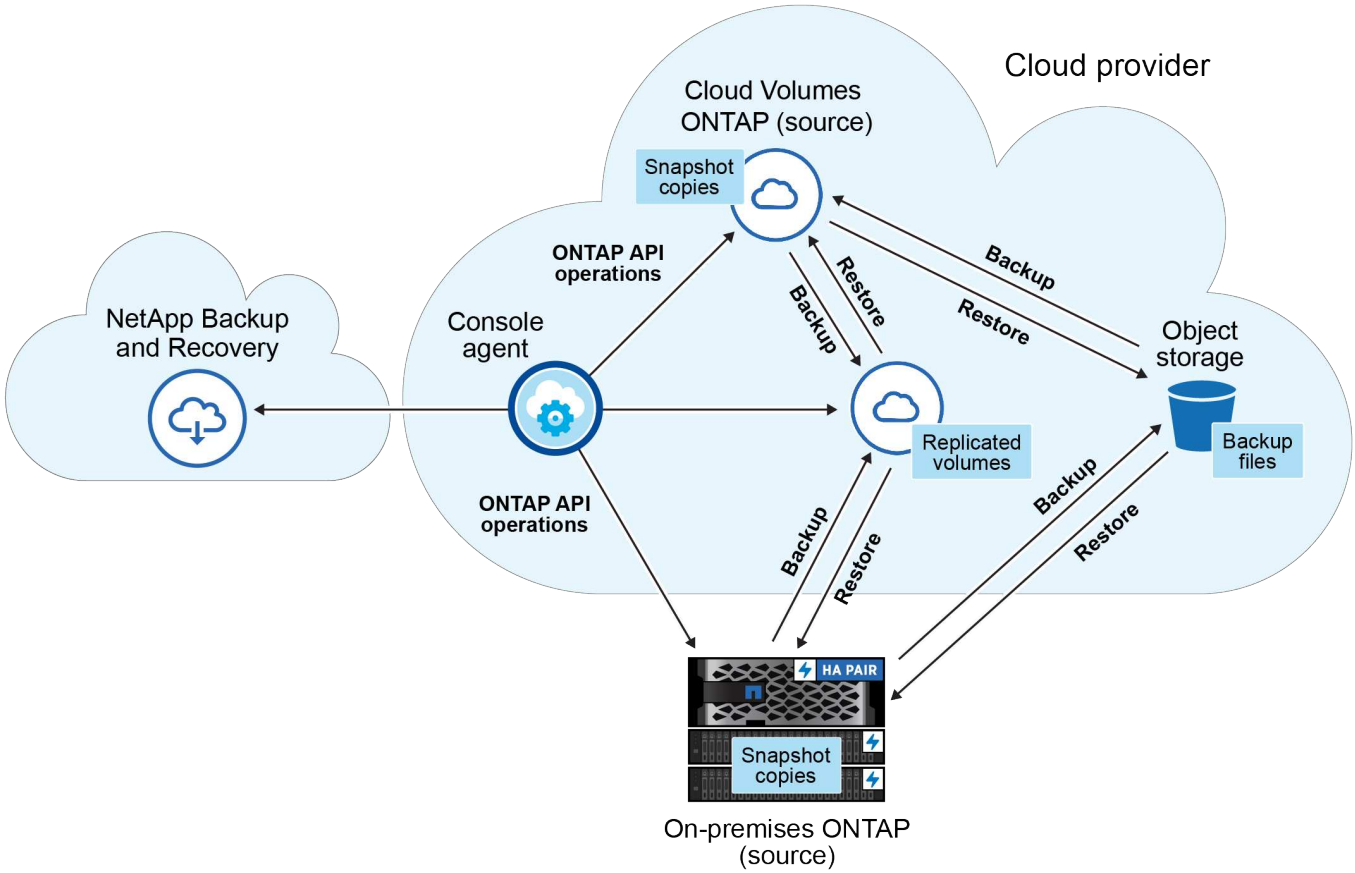
1. Sélectionnez **Restaurer**.

Protéger les charges de travail Hyper-V (Aperçu)

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 fournit des opérations de sauvegarde et de restauration rapides, peu encombrantes, cohérentes en cas de panne et cohérentes avec les machines virtuelles pour les instances de cluster autonomes et FCI.

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 offrent une protection multicouche contre les menaces de cybersécurité internes (initiées) 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 facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait 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. 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.
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. Pour afficher le tableau de bord de NetApp Backup and Recovery , dans le menu de la NetApp Console , 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.

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. Vous pouvez créer un groupe de protection pour un ensemble de charges de travail que vous souhaitez sauvegarder et 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 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.

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

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, 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 politique appliquée à la sauvegarde est la même politique que celle 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 de copies instantanées, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage d'objets 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 l'emplacement d'origine ; la restauration vers un autre emplacement n'est pas disponible dans cette version d'aperçu privée.

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 **Terminé** ou **Suivant** pour continuer vers la page des paramètres de destination de restauration.

   Ensuite, vous pouvez choisir les paramètres de destination et les options de pré-restauration et de post-restauration.

Sélection de la destination

1. Choisissez les paramètres de destination et les options de pré-restauration et de post-restauration.

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

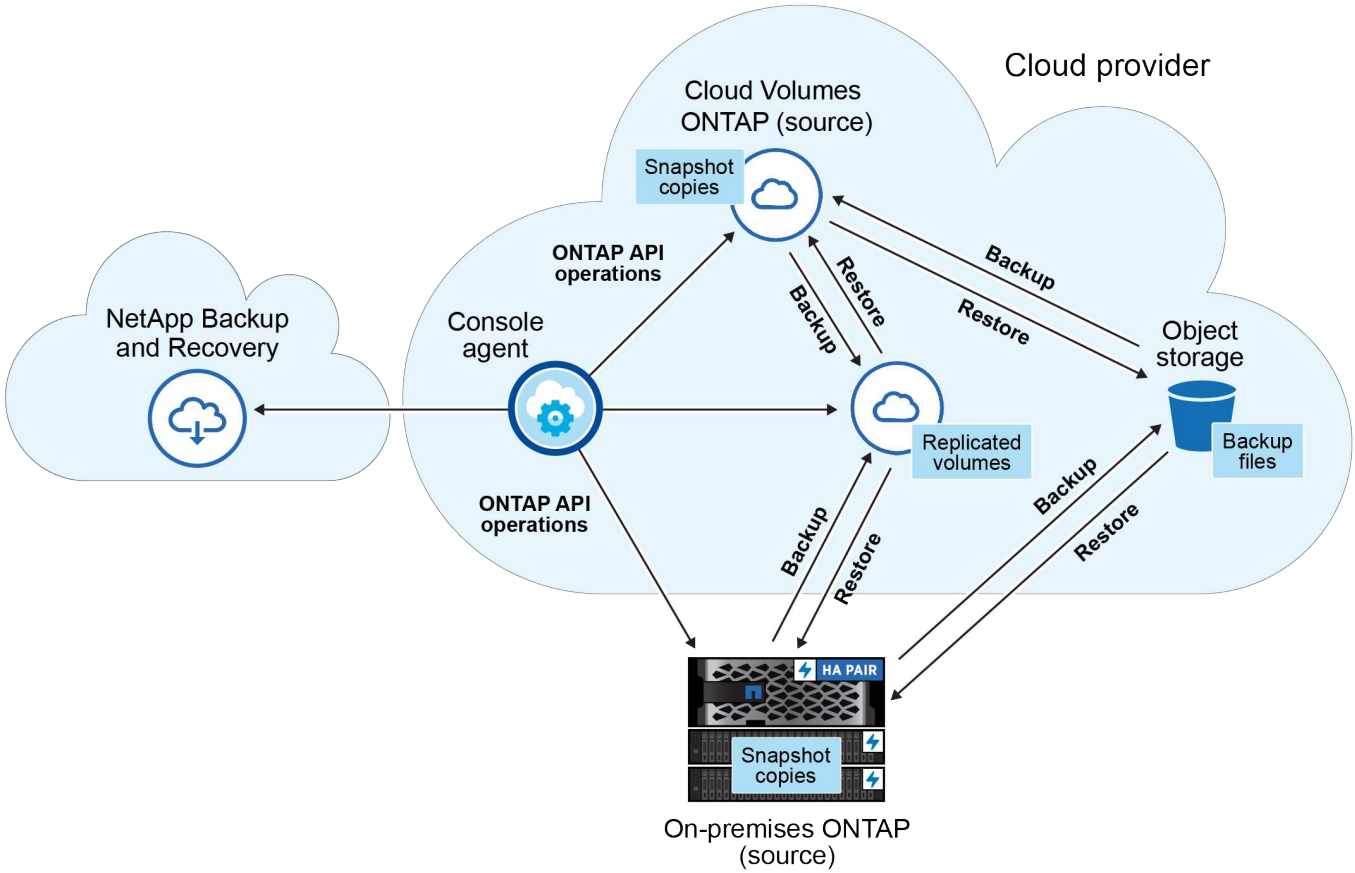
Non disponible pour l'aperçu privé Hyper-V.

1. Sélectionnez **Restaurer**.

Protéger les charges de travail Oracle (Aperçu)

Présentation de la protection des charges de travail de la base de données Oracle

Protégez vos bases de données et journaux Oracle 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 la base de données. Vous pouvez sauvegarder les charges de travail Oracle sur Amazon Web Services S3, NetApp StorageGRID, Microsoft Azure Blob Storage ou ONTAP S3 et les restaurer sur un hôte Oracle 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 offrent une protection multicouche contre les menaces de cybersécurité internes (initiées) 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 facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait 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 Oracle :

- "Découvrez les charges de travail Oracle"
- "Créer et gérer des groupes de protection pour les charges de travail Oracle"
- "Sauvegarder les charges de travail Oracle"
- "Restaurer les charges de travail Oracle"

Découvrez les charges de travail Oracle 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. Dans la mosaïque Oracle, sélectionnez **Découvrir et gérer**.

   Si c'est la première fois que vous vous connectez à 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 version de NetApp Backup and Recovery» apparaît et affiche 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. Pour afficher le tableau de bord de NetApp Backup and Recovery , dans le menu supérieur, 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.

Créez et gérez des groupes de protection pour les charges de travail Oracle 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 les charges de travail Oracle 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.

   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 avec NetApp Backup and Recovery

Sauvegardez les groupes de protection ou les bases de données Oracle Database à partir de systèmes ONTAP locaux vers Amazon Web Services S3, NetApp StorageGRID, Microsoft Azure Blob Storage ou ONTAP S3 pour garantir la protection de vos données. Lorsque vous sauvegardez un groupe de protection, la NetApp Console sauvegarde les bases de données et les données de journal contenues dans le groupe de protection.

> Pour sauvegarder des groupes de protection ou des bases de données uniques 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 Oracle 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

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 Oracle, 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**.

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. Dans la mosaïque Oracle, 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 **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 des bases de données Oracle à partir de copies instantanées, d'une sauvegarde répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage d'objets 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 vers la page des paramètres de destination de restauration.

   Ensuite, vous pouvez choisir les paramètres de destination et les options de pré-restauration et de post-restauration.

Sélection de la destination

1. Choisissez les paramètres de destination et les options de pré-restauration et de post-restauration.

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.

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 pour conserver les journaux d'archive, vous pouvez monter les points de récupération de la base de données pour afficher l'historique de toutes les modifications apportées à 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.

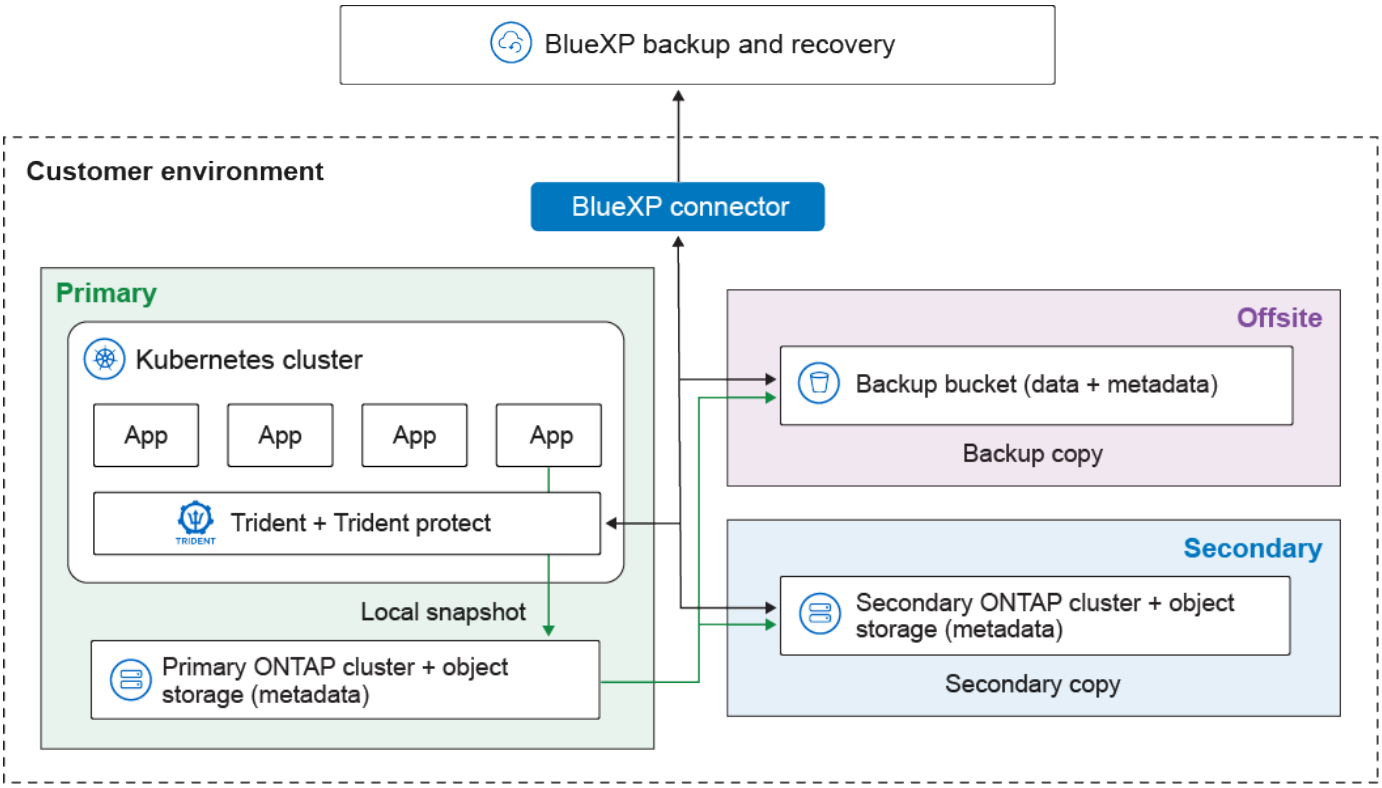
7. Choisissez un point de récupération dans la liste et sélectionnez l'icône Actions ••• > **Démonter**.
8. Confirmez l'action en sélectionnant **Démonter**.

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.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Si vous découvrez des charges de travail Kubernetes pour la première fois, dans NetApp Backup and Recovery, sélectionnez **Découvrir et gérer** sous le type de charge de travail 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 de protection Trident
   - Créer un secret Kubernetes
   - Ajouter un dépôt Helm
   - Installer 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 supérieur, 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".

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" .

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.

Protéger une application Kubernetes existante

Activez une politique de protection sur une application Kubernetes que vous avez déjà ajoutée.

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 protéger et sélectionnez le menu Actions associé.
5. Sélectionnez **Protéger**.
6. Dans la zone **Politique**, choisissez une politique de protection existante pour protéger l'application ou créez une nouvelle politique. Se référer à"Créer une politique" pour plus d'informations sur la création de politiques de protection.
7. 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. Vous pouvez configurer le type de hook d'exécution, le modèle qu'il utilise, les arguments et les sélecteurs d'étiquettes.
8. Sélectionnez **Terminé**.

Résultat

La 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. Dès que vous activez la protection d'une application, la console crée une sauvegarde complète de l'application. Les sauvegardes incrémentielles ultérieures sont créées selon la planification définie dans la politique de protection associée à l'application.

Sauvegarder une application Kubernetes maintenant

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.

Restaurer les applications Kubernetes

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.

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 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 restaurer et sélectionnez le menu Actions associé.
5. Sélectionnez **Afficher et restaurer**.

   La liste des points de restauration apparaît.

6. Ouvrez le menu Actions pour le point de restauration que vous souhaitez utiliser et sélectionnez **Restaurer**.

Paramètres généraux

1. Choisissez la source à partir de laquelle restaurer (local ou magasin d'objets).
2. Choisissez le cluster de destination dans la liste **Cluster**.
3. Choisissez l'espace de noms de destination de restauration.

   Vous pouvez restaurer l'espace de noms d'origine ou restaurer un nouvel espace de noms.

4. 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. Choisissez de restaurer soit la classe de stockage par défaut, soit une classe de stockage différente.
2. Si vous choisissez de restaurer vers une classe de stockage différente, sélectionnez une classe de stockage de destination correspondant à chaque classe de stockage source.
3. Sélectionnez **Restaurer**.

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

Si vous n'avez plus besoin de protéger les ressources hébergées par un cluster Kubernetes, vous pouvez le supprimer de NetApp Backup and Recovery. La suppression d'un cluster ne supprime pas le cluster ni ses ressources ; elle supprime uniquement le cluster de l'inventaire de la NetApp Console . Avant de pouvoir supprimer un cluster, vous devez désactiver la protection et supprimer les applications associées de NetApp Backup and Recovery.

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.

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

Vous pouvez supprimer une application dont vous n'avez plus besoin. Lorsque vous supprimez une application, NetApp Backup and Recovery cesse de protéger l'application et supprime toutes les sauvegardes et snapshots associés.

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**.

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 débloque les systèmes de fichiers pour des applications comme KubeVirt pendant la protection des données. Vous pouvez désactiver ce comportement globalement ou pour des applications spécifiques à l'aide de 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.

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 l'état des snapshots locaux, des réplications et des tâches de sauvegarde vers le stockage d'objets que vous avez initiées, ainsi que les tâches de restauration que vous avez initiées. Vous pouvez voir les tâches terminées, en cours ou ayant échoué afin de pouvoir diagnostiquer et résoudre les problèmes. À l'aide du centre de notifications de la NetApp Console , vous pouvez activer l'envoi de notifications par e-mail afin d'être informé de l'activité importante du système, même lorsque vous n'êtes pas connecté au système. À l'aide de la chronologie de la console, vous pouvez voir les détails de toutes les actions initiées via l'interface utilisateur ou l'API.

NetApp Backup and Recovery conserve les informations des tâches pendant 15 jours, après quoi elles sont purgées et ne sont plus visibles dans le moniteur des tâches.

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, vous devrez redémarrer 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 Surveillance des tâches à l'aide de plusieurs filtres, tels que la stratégie, l'étiquette d'instantané, le type d'opération (protection, restauration, rétention 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 de visualiser 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 l'avoir affiné. 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)

La surveillance des flux de rétention (ou *cycle de vie de sauvegarde*) vous aide à garantir l'exhaustivité de l'audit, la responsabilité et la sécurité des sauvegardes. Pour vous aider à suivre le cycle de vie de la sauvegarde, vous souhaiterez peut-être identifier l'expiration de toutes les copies de sauvegarde.

Une tâche de cycle de vie de sauvegarde suit toutes les copies Snapshot qui sont supprimées ou dans la file d'attente pour être supprimées. À partir d' ONTAP 9.13, vous pouvez consulter tous les types de tâches appelés « Rétention » sur la page Surveillance des tâches.

Le type de tâche « Rétention » capture toutes les tâches de suppression de snapshots 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.

En plus d'afficher les alertes dans le centre de notifications, vous pouvez configurer la console pour envoyer certains types de notifications par e-mail sous forme d'alertes afin d'être informé de l'activité importante du système même lorsque vous n'êtes pas connecté au système. "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	Niveau d'alerte	E-mail envoyé
Activation	L'activation de la sauvegarde et de la récupération a échoué pour le système	Erreur	Oui
Activation	Échec de la modification de la sauvegarde et de la récupération pour le système	Erreur	Oui
Instantané local	Échec de la tâche de création d'instantanés ad hoc de NetApp Backup and Recovery	Erreur	Oui
Réplication	Échec de la tâche de réplication ad hoc de NetApp Backup and Recovery	Erreur	Oui
Réplication	Échec de la tâche de pause de réplication de NetApp Backup and Recovery	Erreur	Non

Type d'opération	Événement	Niveau d'alerte	E-mail envoyé
Réplication	Échec de la tâche d'interruption de la réplication de NetApp Backup and Recovery	Erreur	Non
Réplication	Échec de la tâche de resynchronisation de la réplication NetApp Backup and Recovery	Erreur	Non
Réplication	Échec de la tâche d'arrêt de la réplication de NetApp Backup and Recovery	Erreur	Non
Réplication	Échec de la tâche de resynchronisation inverse de la réplication NetApp Backup and Recovery	Erreur	Oui
Réplication	Échec de la tâche de suppression de réplication de NetApp Backup and Recovery	Erreur	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 ». Tous les autres utilisateurs et destinataires sont configurés, par défaut, pour ne recevoir aucun e-mail de notification. Les e-mails peuvent être envoyés à tous les utilisateurs de la console qui font partie de votre compte NetApp Cloud, ou à tout autre destinataire qui doit être informé 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`

Automatisez avec les API REST de NetApp Backup and Recovery

Les fonctionnalités de NetApp Backup and Recovery disponibles via l'interface utilisateur Web sont également disponibles via l'API REST de sauvegarde et de récupération.

Il existe dix catégories de points de terminaison définis dans NetApp Backup and Recovery:

- `backup`- gère les opérations de sauvegarde des ressources cloud et sur site et récupère les détails des données de sauvegarde
- `catalog`- gère la recherche de catalogue indexée de fichiers en fonction d'une requête (Recherche et restauration)
- `cloud`- récupère des informations sur diverses ressources de fournisseurs de cloud à partir de la NetApp Console
- `job`- gère les entrées de détails des tâches dans la base de données de la NetApp Console
- `license`- récupère la validité de la licence des systèmes à partir de la NetApp Console
- `ransomware scan`- lance une analyse de ransomware sur un fichier de sauvegarde spécifique
- `restore`- vous permet d'effectuer des opérations de restauration au niveau du volume, du fichier et du dossier
- `sfr`- récupère les fichiers à partir d'un fichier de sauvegarde pour les opérations de restauration au niveau d'un seul fichier (Parcourir et restaurer)
- `storagegrid`- récupère les détails d'un serveur StorageGRID et vous permet de découvrir un serveur StorageGRID
- `system`- gère les politiques de sauvegarde et configure le magasin d'objets de destination associé à un système

Référence API

La documentation de chaque API de NetApp Backup and Recovery est disponible à partir de "Automatisation de la NetApp Console pour la NetApp Backup and Recovery" .

Commencer

Pour commencer à utiliser les API de NetApp Backup and Recovery , vous devez obtenir un jeton utilisateur, votre ID de compte de NetApp Console et l'ID de l'agent de console.

Lors des appels d'API, vous ajouterez le jeton utilisateur dans l'en-tête d'autorisation et l'ID de l'agent de la console dans l'en-tête x-agent-id. Vous devez utiliser l'ID de compte de la NetApp Console dans les API.

> Si vous utilisez un compte de service, vous devez utiliser le jeton d'accès au service au lieu d'un jeton utilisateur. La valeur de « client_id » (« Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC ») est une valeur fixe et ne peut pas être modifiée. Dans ce cas, suivez les instructions ici : "Créer un jeton d'accès au service" .

Étapes

1. Obtenez un jeton utilisateur à partir du site Web NetApp NetApp Console .

   Assurez-vous de générer le jeton d'actualisation à partir du lien suivant : https://services.cloud.netapp.com/refresh-token/. Le jeton d'actualisation est une chaîne alphanumérique que vous utiliserez pour générer un jeton utilisateur.

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

   Le jeton utilisateur du site Web de la NetApp Console a une date d'expiration. La réponse de l'API inclut un champ « expires_in » qui indique quand le jeton expire. Pour actualiser le jeton, vous devrez appeler à nouveau cette API.

2. Obtenez votre ID de compte NetApp Console .

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR
```

   Cette API renverra une réponse comme celle-ci. Vous pouvez récupérer l'ID de compte en analysant la sortie de **[0].[accountPublicId]**.

```
{
  "accountPublicId": "account-i6vJXvZW",
  "accountName": "rashidn",
  "isSaas": true,
  "isGov": false,
  "isPrivatePreviewEnabled": false,
  "is3rdPartyServicesEnabled": false,
  "accountSerial": "96064469711530003565",
  "userRole": "Role-1"
}
```

3. Obtenez le x-agent-id qui contient l'ID de l'agent de la console.

```
GET 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5……
```

Vous pouvez récupérer l'ID de l'agent à partir de la réponse en analysant la sortie de **occm.[0].[agent].[agentId]**.

Exemple utilisant les API

L'exemple suivant montre un appel d'API pour activer NetApp Backup and Recovery sur un système avec une nouvelle stratégie qui a des étiquettes quotidiennes, horaires et hebdomadaires définies, l'archivage après les jours étant défini sur 180 jours, dans la région East-US-2 dans le cloud Azure. Notez que cela active uniquement la sauvegarde sur le système, mais aucun volume n'est sauvegardé.

Demande d'API

Vous verrez que nous utilisons l'ID de compte de la NetApp Console `account-DpTFcxN3` , ID de l'agent de la console `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients` , et le jeton utilisateur `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4V alobjUmju2x0xUH48g` dans cette commande.

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }
```

La réponse est un identifiant de tâche que vous pouvez ensuite surveiller :

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

Surveiller la réponse :

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Réponse:

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Surveiller jusqu'à ce que le « statut » soit « TERMINÉ » :

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Référence

Stratégies dans SnapCenter comparées à celles de NetApp Backup and Recovery

Il existe certaines différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans NetApp Backup and Recovery qui peuvent avoir un impact sur ce que vous voyez après l'importation de ressources et de stratégies depuis SnapCenter.

Niveaux de planification

SnapCenter utilise les niveaux de planification suivants :

- **Horaire** : Plusieurs heures et minutes avec n'importe quelle heure (0-23) et n'importe quelle minute (0-60).
- **Quotidien** : Option permettant de répéter tous les nombres de jours définis, par exemple, tous les 3 jours.
- **Hebdomadaire** : du dimanche au lundi, avec la possibilité d'effectuer un instantané le jour 1 de la semaine ou sur plusieurs jours de la semaine.
- **Mensuel** : de janvier à décembre, avec la possibilité de jouer un ou plusieurs jours spécifiques chaque mois, par exemple le 7.

NetApp Backup and Recovery utilise les niveaux de planification suivants, qui sont légèrement différents :

- **Toutes les heures** : effectue des instantanés uniquement à des intervalles de 15 minutes, par exemple, des intervalles d'une heure ou de 15 minutes inférieurs à 60.
- **Quotidien** : Heures de la journée (0-23) avec heure de début par exemple à 10h00 avec une option pour effectuer toutes les heures.
- **Hebdomadaire** : Jour de la semaine (du dimanche au lundi) avec possibilité de jouer sur 1 jour ou plusieurs jours. C'est la même chose que SnapCenter.
- **Mensuel** : Dates du mois (0-30) avec une heure de début à plusieurs dates du mois.
- **Annuel** : Mensuel. Cela correspond au mensuel de SnapCenter.

Plusieurs politiques dans SnapCenter avec le même niveau de planification

Vous pouvez attribuer plusieurs politiques avec le même niveau de planification à une ressource dans SnapCenter. Cependant, NetApp Backup and Recovery ne prend pas en charge plusieurs stratégies sur une ressource qui utilise le même niveau de planification.

Exemple : Si vous utilisez trois stratégies (pour les données, le journal et le journal des snapshots) dans SnapCenter, après la migration depuis SnapCenter, NetApp Backup and Recovery utilise une seule stratégie au lieu des trois.

Horaires quotidiens SnapCenter importés

NetApp Backup and Recovery ajuste les planifications SnapCenter comme suit :

- Si la planification SnapCenter est définie sur une durée inférieure ou égale à 7 jours, NetApp Backup and Recovery définit la planification sur une durée hebdomadaire. Certains instantanés sont ignorés au cours de la semaine.

Exemple : Si vous disposez d'une stratégie quotidienne SnapCenter avec un intervalle répétitif tous les 3 jours à partir du lundi, NetApp Backup and Recovery définit la planification sur une base hebdomadaire le lundi, le jeudi et le dimanche. Certains jours seront sautés car ce n'est pas exactement tous les 3 jours.

- Si la planification SnapCenter est définie sur une durée supérieure à 7 jours, NetApp Backup and Recovery définit la planification sur mensuelle. Certains instantanés seront ignorés au cours du mois.

  Exemple : Si vous disposez d'une stratégie quotidienne SnapCenter avec un intervalle répétitif tous les 10 jours à partir du 2 du mois, NetApp Backup and Recovery, après la migration, définit la planification sur une base mensuelle les 2, 12 et 22 du mois. NetApp Backup and Recovery saute quelques jours au cours du mois prochain.

Horaires horaires SnapCenter importés

Les politiques horaires SnapCenter avec des intervalles répétitifs supérieurs à une heure sont converties en politique quotidienne dans NetApp Backup and Recovery.

Toute politique horaire avec des intervalles répétitifs qui ne sont pas un facteur de 24 (par exemple 5, 7, etc.) ignorera certains instantanés dans une journée.

Exemple : Si vous disposez d'une stratégie horaire SnapCenter avec un intervalle répétitif toutes les 5 heures à partir de 1 h 00 du matin, NetApp Backup and Recovery (après la migration) définira la planification sur quotidienne avec des intervalles de 5 heures à 1 h 00, 6 h 00, 11 h 00, 16 h 00 et 21 h 00. Certaines heures seront ignorées, après 21h00, il devrait être 2h00 du matin pour se répéter toutes les 5 heures, mais ce sera toujours 1h00 du matin.

Conservation des journaux à partir des politiques SnapCenter

Si vous disposez d'une ressource dans SnapCenter avec plusieurs stratégies, NetApp Backup and Recovery utilise l'ordre de priorité suivant pour attribuer la valeur de conservation des journaux :

- Pour les stratégies « Sauvegarde complète avec sauvegarde du journal » et « Journal uniquement » dans SnapCenter, NetApp Backup and Recovery utilise la valeur de rétention de la stratégie Journal uniquement.
- Pour les stratégies « Sauvegarde complète avec journal uniquement » et « Complète et journal » dans SnapCenter, NetApp Backup and Recovery utilise la valeur de rétention du journal uniquement.
- Pour « Sauvegarde complète et journal » plus « Sauvegarde complète » dans SnapCenter, NetApp Backup and Recovery utilise la valeur de rétention « Sauvegarde complète et journal ».
- Si vous ne disposez que d'une sauvegarde complète dans SnapCenter, NetApp Backup and Recovery n'active pas la sauvegarde du journal.

Conservation des sauvegardes des journaux

SnapCenter prend en charge plusieurs valeurs de rétention pour les stratégies sur une ressource. NetApp Backup and Recovery ne prend en charge qu'une seule valeur de rétention par ressource.

Nombre de rétentions à partir des politiques SnapCenter

Si vous disposez d'une ressource avec une protection secondaire activée dans SnapCenter avec plusieurs volumes sources, plusieurs volumes de destination et plusieurs relations SnapMirror , NetApp Backup and Recovery utilise uniquement le nombre de rétention de la première stratégie.

Exemple : Si vous disposez d'une stratégie SnapCenter avec un nombre de rétention de 5 et d'une autre stratégie avec un nombre de rétention de 10, NetApp Backup and Recovery utilise le nombre de rétention de 5.

Étiquettes SnapMirror à partir des politiques SnapCenter

SnapCenter conserve les étiquettes SnapMirror pour chaque politique après la migration, même si le niveau change.

Exemple : Une politique horaire de SnapCenter peut changer en quotidienne dans NetApp Backup and Recovery. Cependant, les étiquettes SnapMirror restent les mêmes après la migration.

Rôles de gestion des identités et des accès (IAM) de NetApp Backup and Recovery

NetApp Backup and Recovery utilise la gestion des identités et des accès (IAM) pour gérer l'accès de chaque utilisateur à des fonctionnalités et actions spécifiques.

Pour en savoir plus sur les rôles IAM spécifiques à NetApp Backup and Recovery, reportez-vous à "Rôles de NetApp Backup and Recovery dans la NetApp Console" .

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
```

Entrez le mot de passe.

```
mysql> show tables;
mysql> select * from volume;
```

Vérifiez si les volumes affichés sont les mêmes que ceux qui existaient dans 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":"pa
ssword"}
> '
```

   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*.

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.

Niveaux de stockage d'archives AWS pris en charge avec NetApp Backup and Recovery

NetApp Backup and Recovery prend en charge deux classes de stockage d'archivage S3 et la plupart des régions.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Classes de stockage d'archivage S3 prises en charge pour NetApp Backup and Recovery

Lorsque les fichiers de sauvegarde sont initialement créés, ils sont stockés dans le stockage S3 *Standard*. Ce niveau est optimisé pour stocker des données rarement consultées, mais qui vous permet également d'y accéder immédiatement. Après 30 jours, les sauvegardes passent à la classe de stockage S3 *Standard-Infrequent Access* pour réduire les coûts.

Si vos clusters sources exécutent ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive* après un certain nombre de jours (généralement plus de 30 jours) pour une optimisation supplémentaire des coûts. Vous pouvez définir cette valeur sur « 0 » ou sur 1 à 999 jours. Si vous le définissez sur « 0 » jours, vous ne pourrez pas le modifier ultérieurement sur 1 à 999 jours.

Les données de ces niveaux ne sont pas accessibles immédiatement en cas de besoin et nécessiteront un coût de récupération plus élevé. Vous devez donc tenir compte de la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Consultez la section sur cette page concernant la restauration des données à partir du stockage d'archives.

- 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.

Notez que lorsque vous configurez NetApp Backup and Recovery avec ce type de règle de cycle de vie, vous ne devez configurer aucune règle de cycle de vie lors de la configuration du bucket dans votre compte AWS.

"En savoir plus sur les classes de stockage S3".

Restaurer les données à partir du stockage d'archives

Bien que le stockage des fichiers de sauvegarde plus anciens dans un stockage d'archives soit beaucoup moins coûteux que le stockage Standard ou Standard-IA, l'accès aux données d'un fichier de sauvegarde dans un stockage d'archives pour les opérations de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données d'Amazon S3 Glacier et d'Amazon S3 Glacier Deep Archive ?

Vous pouvez choisir entre 3 priorités de restauration lors de la récupération de données depuis Amazon S3 Glacier et 2 priorités de restauration lors de la récupération de données depuis Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive coûte moins cher que S3 Glacier :

Niveau d'archivage	Restaurer la priorité et le coût		
	Haut	Standard	Faible

Niveau d'archivage	Restaurer la priorité et le coût		
Glacier S3	Récupération la plus rapide, coût le plus élevé	Récupération plus lente, coût moindre	Récupération la plus lente, coût le plus bas
Archives S3 Glacier Deep		Récupération plus rapide, coût plus élevé	Récupération plus lente, coût le plus bas

Chaque méthode a des frais de récupération par Go et des frais par demande différents. Pour connaître les tarifs détaillés de S3 Glacier par région AWS, visitez le "Page de tarification Amazon S3" .

Combien de temps faudra-t-il pour restaurer mes objets archivés dans Amazon S3 Glacier ?

Le temps de restauration total est composé de deux parties :

- **Temps de récupération** : Le temps nécessaire pour récupérer le fichier de sauvegarde de l'archive et le placer dans le stockage standard. C'est ce qu'on appelle parfois le temps de « réhydratation ». Le temps de récupération est différent selon la priorité de restauration que vous choisissez.

Niveau d'archivage	Restaurer la priorité et le temps de récupération		
	Haut	**Standard**	**Faible**
Glacier S3	3 à 5 minutes	3 à 5 heures	5 à 12 heures
Archives S3 Glacier Deep		12 heures	48 heures

- **Temps de restauration** : Le temps nécessaire pour restaurer les données à partir du fichier de sauvegarde dans le stockage standard. Cette fois, ce n'est pas différent de l'opération de restauration typique directement à partir du stockage standard, lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Amazon S3 Glacier et S3 Glacier Deep Archive, reportez-vous à "la FAQ d'Amazon sur ces classes de stockage" .

Niveaux d'accès aux archives Azure pris en charge avec NetApp Backup and Recovery

NetApp Backup and Recovery prend en charge un niveau d'accès aux archives Azure et la plupart des régions.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Niveaux d'accès Azure Blob pris en charge pour NetApp Backup and Recovery

Lorsque les fichiers de sauvegarde sont initialement créés, ils sont stockés dans le niveau d'accès *Cool*. Ce niveau est optimisé pour stocker des données rarement consultées, mais auxquelles il est possible d'accéder immédiatement en cas de besoin.

Si vos clusters sources exécutent ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes du stockage *Cool* vers *Azure Archive* après un certain nombre de jours (généralement plus de 30 jours) pour une optimisation supplémentaire des coûts. Les données de ce niveau ne sont pas accessibles immédiatement en cas de besoin et nécessiteront un coût de récupération plus élevé. Vous devez

donc tenir compte de la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Consultez la section sur cette page concernant la restauration des données à partir du stockage d'archives.

Notez que lorsque vous configurez NetApp Backup and Recovery avec ce type de règle de cycle de vie, vous ne devez configurer aucune règle de cycle de vie lors de la configuration du conteneur dans votre compte Azure.

"En savoir plus sur les niveaux d'accès Azure Blob".

Restaurer les données à partir du stockage d'archives

Bien que le stockage d'anciens fichiers de sauvegarde dans un stockage d'archives soit beaucoup moins coûteux que le stockage Cool, l'accès aux données d'un fichier de sauvegarde dans Azure Archive pour les opérations de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données à partir d'Azure Archive ?

Vous pouvez choisir deux priorités de restauration lors de la récupération de données à partir d'Azure Archive :

- **Élevé** : Récupération la plus rapide, coût plus élevé
- **Standard** : Récupération plus lente, coût inférieur

Chaque méthode a des frais de récupération par Go et des frais par demande différents. Pour connaître les tarifs détaillés d'Azure Archive par région Azure, visitez le "Page de tarification Azure" .

> La priorité élevée n'est pas prise en charge lors de la restauration des données d'Azure vers les systèmes StorageGRID .

Combien de temps faudra-t-il pour restaurer mes données archivées dans Azure Archive ?

Le temps de restauration se compose de deux parties :

- **Heure de récupération** : le temps nécessaire pour récupérer le fichier de sauvegarde archivé à partir d'Azure Archive et le placer dans le stockage Cool. C'est ce qu'on appelle parfois le temps de « réhydratation ». Le temps de récupération est différent selon la priorité de restauration que vous choisissez :
  - **Élevé** : < 1 heure
  - **Standard** : < 15 heures
- **Temps de restauration** : Le temps nécessaire pour restaurer les données à partir du fichier de sauvegarde dans le stockage Cool. Cette fois, ce n'est pas différent de l'opération de restauration typique directement à partir du stockage Cool - lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Azure Archive, reportez-vous à "cette FAQ Azure" .

Niveaux de stockage d'archives Google pris en charge avec NetApp Backup and Recovery

NetApp Backup and Recovery prend en charge une classe de stockage d'archivage Google et la plupart des régions.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Classes de stockage d'archivage Google prises en charge pour NetApp Backup and Recovery

Lorsque les fichiers de sauvegarde sont initialement créés, ils sont stockés dans le stockage *Standard*. Ce niveau est optimisé pour stocker des données rarement consultées, mais qui vous permet également d'y accéder immédiatement.

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 (généralement plus de 30 jours) pour une optimisation supplémentaire des coûts. Les données de ce niveau nécessiteront un coût de récupération plus élevé. Vous devez donc tenir compte de la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Consultez la section sur cette page concernant la restauration des données à partir du stockage d'archives.

Notez que lorsque vous configurez NetApp Backup and Recovery avec ce type de règle de cycle de vie, vous ne devez configurer aucune règle de cycle de vie lors de la configuration du bucket dans votre compte Google.

"En savoir plus sur les classes de stockage Google".

Restaurer les données à partir du stockage d'archives

Bien que le stockage d'anciens fichiers de sauvegarde dans le stockage d'archives soit beaucoup moins coûteux que le stockage standard, l'accès aux données d'un fichier de sauvegarde dans le stockage d'archives pour les opérations de restauration prendra un peu plus de temps et coûtera plus cher.

Combien coûte la restauration des données de Google Archive ?

Pour connaître les tarifs détaillés de Google Cloud Storage par région, visitez le "Page de tarification de Google Cloud Storage" .

Combien de temps faudra-t-il pour restaurer mes objets archivés dans Google Archive ?

Le temps de restauration total est composé de deux parties :

- **Temps de récupération** : Le temps nécessaire pour récupérer le fichier de sauvegarde de l'archive et le placer dans le stockage standard. C'est ce qu'on appelle parfois le temps de « réhydratation ». Contrairement aux solutions de stockage « les plus froides » fournies par d'autres fournisseurs de cloud, vos données sont accessibles en quelques millisecondes.
- **Temps de restauration** : Le temps nécessaire pour restaurer les données à partir du fichier de sauvegarde dans le stockage standard. Cette fois, ce n'est pas différent de l'opération de restauration typique directement à partir du stockage standard, lorsque vous n'utilisez pas de niveau d'archivage.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

- "Avis concernant la NetApp Console"
- "Avis concernant la NetApp Backup and Recovery"
- "Avis concernant la restauration d'un fichier unique"