Protégez les charges de travail du volume ONTAP

NetApp Backup and Recovery

NetApp
November 26, 2025

Sommaire

Protégez les charges de travail du volume ONTAP

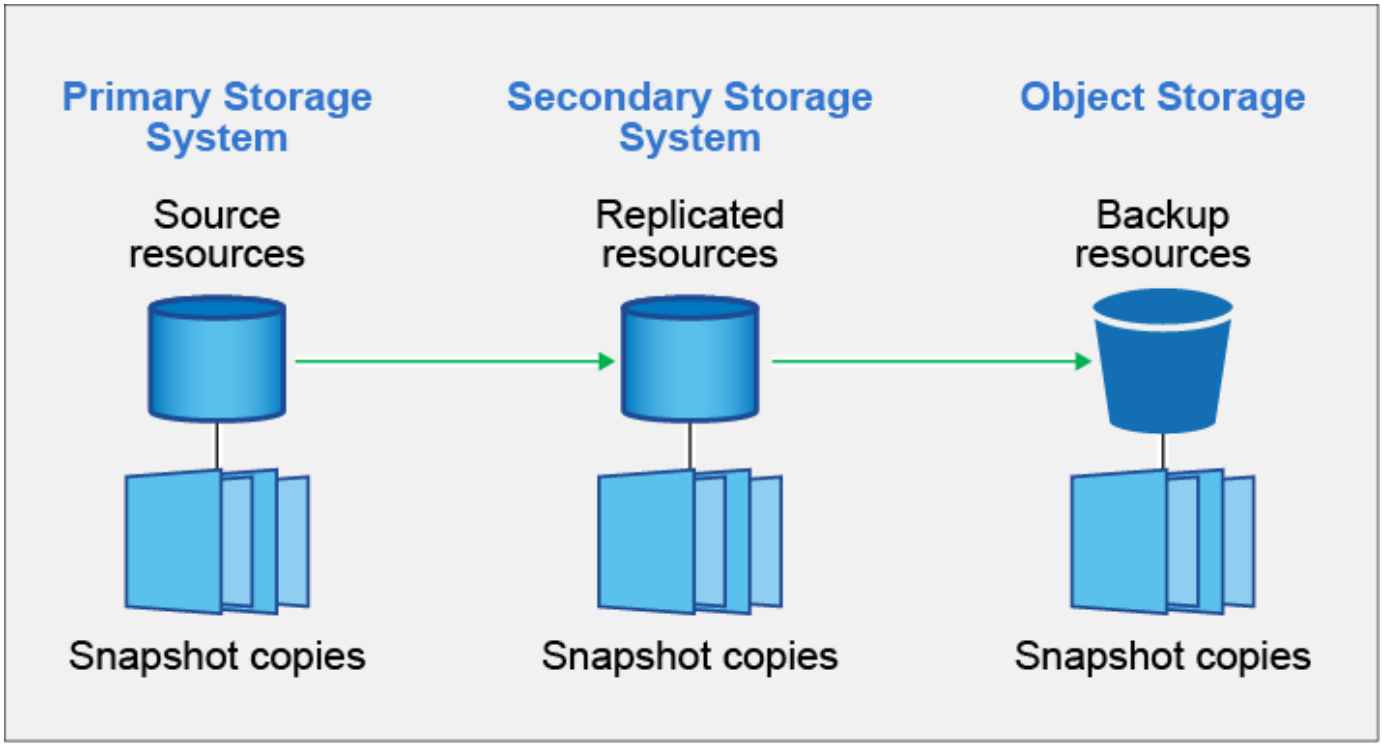
Protégez vos données de volume ONTAP à l'aide de NetApp Backup and Recovery

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

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

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

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



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

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

- Plusieurs copies de données protègent contre les menaces de cybersécurité internes et externes.
- L'utilisation de différents types de supports vous aide à récupérer si l'un d'eux tombe en panne.
- Vous pouvez restaurer rapidement à partir de la copie sur site et utiliser les copies hors site si la copie sur site est compromise.

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

Caractéristiques

Fonctionnalités de réplication :

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

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

Fonctionnalités de sauvegarde sur objet :

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

- Utilisez vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés de chiffrement par défaut de votre fournisseur de cloud.
- Prise en charge jusqu'à 4 000 sauvegardes d'un seul volume.

Restaurer les fonctionnalités :

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

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

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

Régions prises en charge

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

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

Destinations de sauvegarde prises en charge

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

Système source	Système secondaire (réplication)	Magasin d'objets de destination (sauvegarde) 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 source	Système secondaire (réplication)	Magasin d'objets de destination (sauvegarde) ifdef::aws[]
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 situé sur un système secondaire (volume répliqué) ou dans un stockage objet (fichier de sauvegarde) vers les systèmes suivants. Les instantanés résident sur le système source et ne peuvent être restaurés que sur ce même système.

Emplacement du fichier de sauvegarde		Système de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	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 d'instantanés ou de volumes répliqués est gratuite, hormis l'espace disque nécessaire à leur stockage.

Frais de ressources

Des frais de ressources sont payés au fournisseur de cloud pour la capacité de stockage d'objets et pour l'écriture et la lecture de fichiers de sauvegarde dans le cloud.

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

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

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

Frais de service

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

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

Licences

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

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

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

Apportez votre propre permis

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

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

"Apprenez à gérer vos licences BYOL".

Abonnement à la carte

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

"Découvrez comment configurer un abonnement à la carte".

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

Contrat annuel

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

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

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

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

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

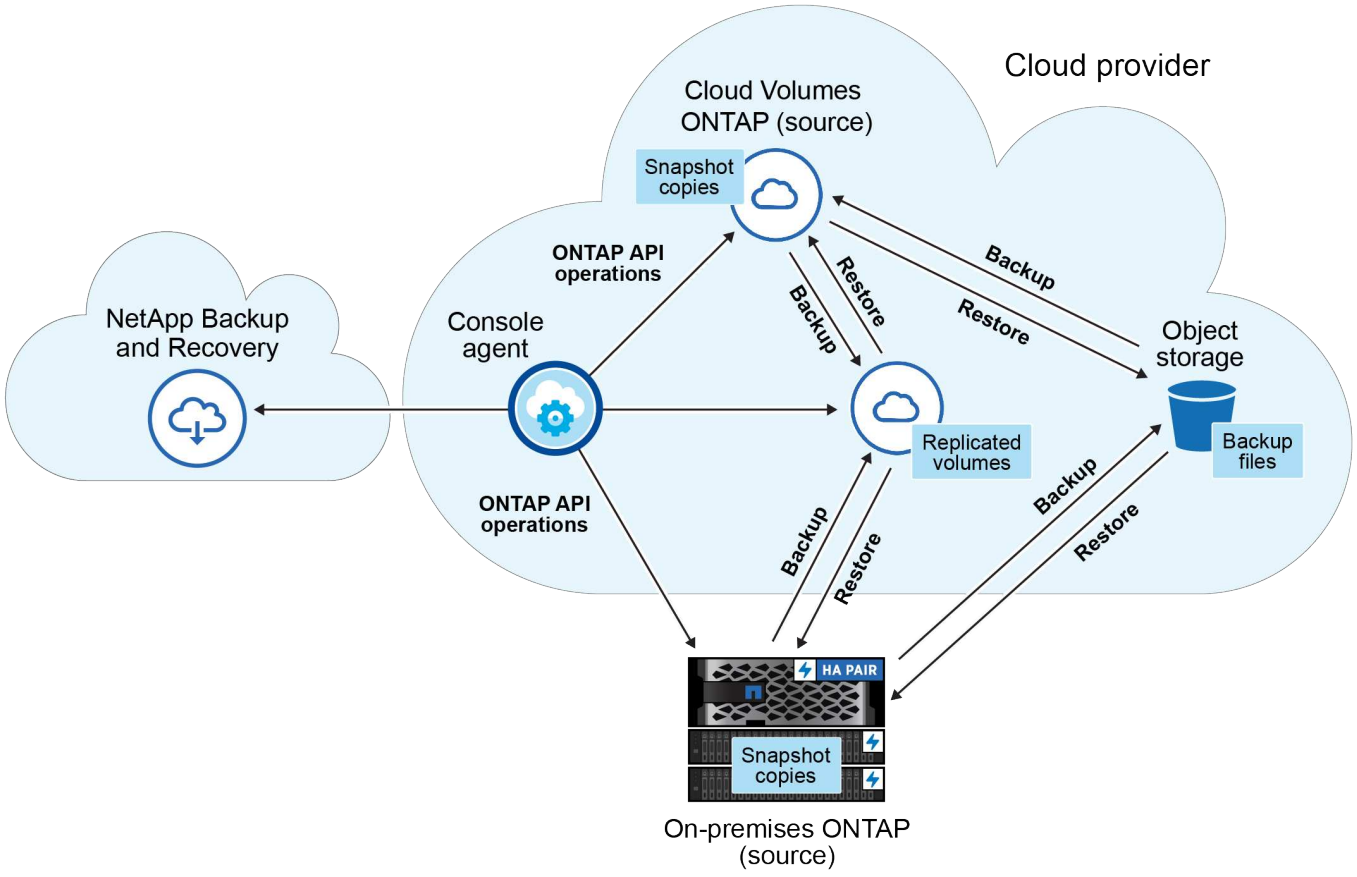
"Apprenez à mettre en place des contrats annuels".

Comment fonctionne la NetApp Backup and Recovery

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

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

L'image suivante montre la relation entre chaque composant :



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

Où résident les sauvegardes

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

- Les *instantanés* résident sur le volume source du système source.
- Les *volumes répliqués* résident sur le système de stockage secondaire : un système Cloud Volumes ONTAP ou ONTAP sur site.
- Les *copies de sauvegarde* sont stockées dans un magasin d'objets que la console crée dans votre compte cloud. Il existe un magasin d'objets par cluster/système, et la console nomme le magasin d'objets comme suit : « netapp-backup-clusteruuid ». Assurez-vous de ne pas supprimer ce magasin d'objets.

+ ** Dans AWS, la console permet 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 instantanés, les volumes répliqués et les fichiers de sauvegarde. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes ayant des objectifs de point de récupération (RPO) différents, vous pouvez créer des stratégies supplémentaires pour ce cluster et attribuer ces stratégies aux autres volumes une fois NetApp Backup and Recovery activé.

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

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

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

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

Paramètres de protection des fichiers de sauvegarde

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

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

Les analyses de protection contre les ransomwares planifiées sont activées par défaut. Le paramètre par défaut pour la fréquence d'analyse est de 7 jours. L'analyse s'effectue uniquement sur le dernier instantané. Les analyses programmées peuvent être désactivées pour réduire vos coûts. Vous pouvez activer ou désactiver les analyses planifiées de logiciels de ransomware sur le dernier instantané en utilisant l'option de la page Paramètres avancés. Si vous l'activez, les analyses sont effectuées chaque semaine par défaut. Vous pouvez modifier ce calendrier en jours ou en semaines ou le désactiver, ce qui permet de réduire les coûts.

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

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

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

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

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

Stockage d'archives pour les fichiers de sauvegarde plus anciens

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

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

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

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

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

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

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

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

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

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

Considérations relatives à la politique de hiérarchisation de FabricPool

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

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

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

  - Les sauvegardes ultérieures sont incrémentielles et n'ont pas cet effet.
  - Si la politique de hiérarchisation est attribuée au volume lors de sa création initiale, vous ne verrez pas ce problème.

- Tenez compte de l'impact des sauvegardes avant d'attribuer la `all` politique de hiérarchisation des volumes. Étant donné que les données sont hiérarchisées immédiatement, NetApp Backup and Recovery lira les données à partir du niveau cloud plutôt qu'à partir du niveau local. Étant donné que les opérations de sauvegarde simultanées partagent la liaison réseau avec le magasin d'objets cloud, une dégradation des performances peut se produire si les ressources réseau sont saturées. Dans ce cas, vous souhaiterez peut-être configurer de manière proactive plusieurs interfaces réseau (LIF) pour réduire ce type de saturation du réseau.

Planifiez votre parcours de protection avec NetApp Backup and Recovery

NetApp Backup and Recovery vous permet de créer jusqu'à trois copies de vos volumes sources pour protéger vos données. Il existe de nombreuses options que vous pouvez

sélectionner lors de l'activation de la sauvegarde et de la récupération sur vos volumes. Vous devez donc revoir vos choix afin d'être prêt.

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

Nous passerons en revue les options suivantes :

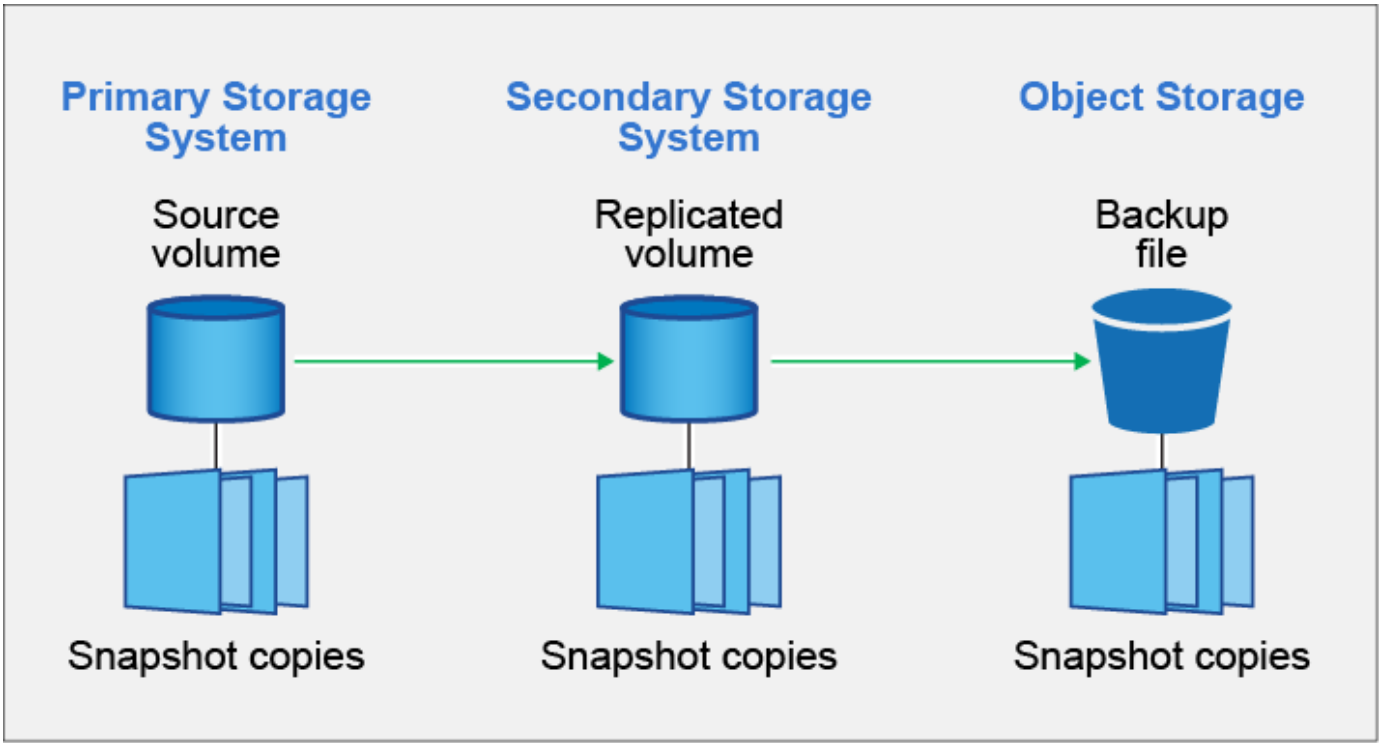
- Quelles fonctionnalités de protection utiliserez-vous : instantanés, volumes répliqués et/ou sauvegarde dans le cloud ?
- Quelle architecture de sauvegarde utiliserez-vous : une sauvegarde en cascade ou en éventail de vos volumes ?
- Allez-vous utiliser les politiques de sauvegarde par défaut ou devez-vous créer des politiques personnalisées ?
- Voulez-vous que le service crée les buckets cloud pour vous ou souhaitez-vous créer vos conteneurs de stockage d'objets avant de commencer ?
- Quel mode de déploiement de l'agent de console utilisez-vous (mode standard, restreint ou privé) ?

Quelles fonctionnalités de protection utiliserez-vous

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

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

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



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

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

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

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

Comparaison des différentes méthodes de sauvegarde

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

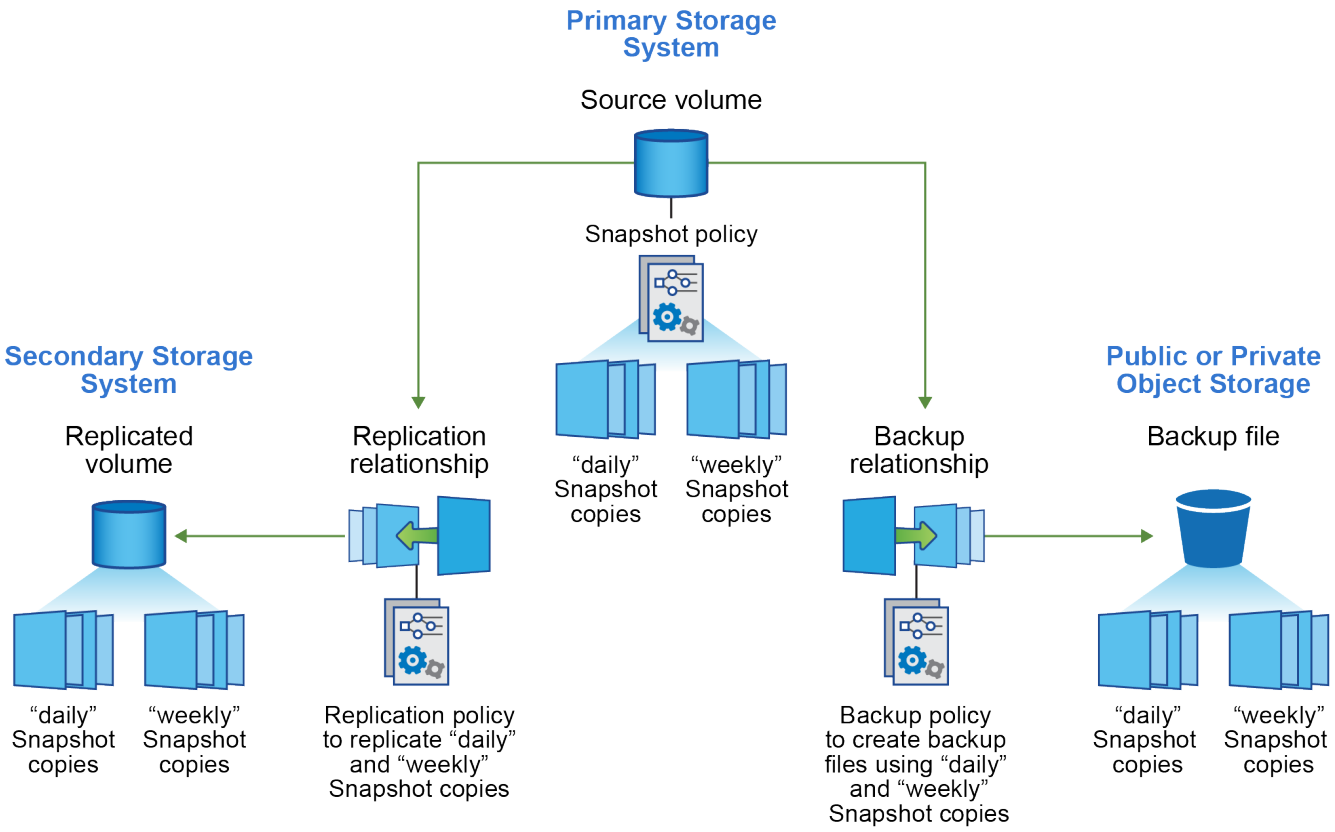
En plus de ces critères, le stockage cloud offre des options de sécurité supplémentaires si vous utilisez la fonctionnalité DataLock et Ransomware Resilience, ainsi que des économies de coûts supplémentaires en sélectionnant des classes de stockage d'archivage pour les fichiers de sauvegarde plus anciens.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

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

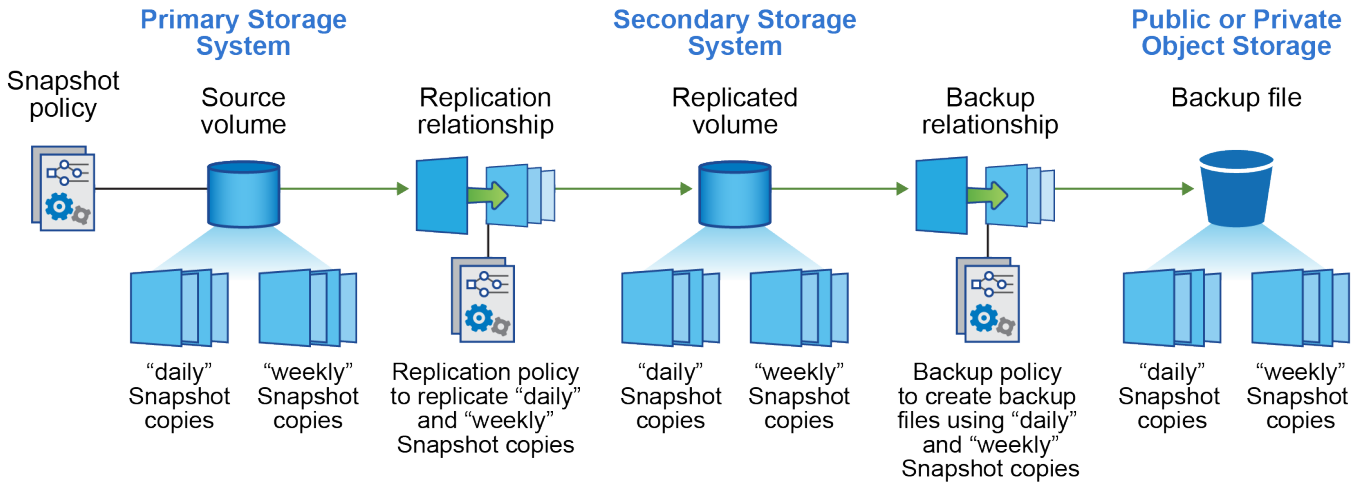
Quelle architecture de sauvegarde utiliserez-vous

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

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



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



Comparaison des différents choix d’architecture

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

Fan-out	Cascade
Faible impact sur les performances du système source car il envoie des instantanés à 2 systèmes distincts	L’impact sur les performances du système de stockage source est moindre car l’instantané n’est envoyé qu’une seule fois.
Plus facile à configurer car toutes les politiques, la mise en réseau et les configurations ONTAP sont effectuées sur le système source	Nécessite également que certaines configurations réseau et ONTAP soient effectuées à partir du système secondaire.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Créez des politiques de sauvegarde à l'aide des outils suivants en fonction de votre environnement, de vos préférences et du type de protection :

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

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

Afficher les politiques d'un système

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

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

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

Créer des politiques

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

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

Créer une politique de snapshot avant de lancer le snapshot

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

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

Étapes

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

   La page de gestion des politiques apparaît.
3. Dans la page Politiques, sélectionnez **Créer une politique** > **Créer une politique d'instantané**.
4. Spécifiez le nom de la politique.
5. Sélectionnez le ou les programmes d'instantanés. Vous pouvez avoir un maximum de 5 étiquettes. Ou créez un planning.
6. Si vous choisissez de créer un planning :
   a. Sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle.
   b. Spécifiez les étiquettes d'instantané indiquant la planification et la conservation.
   c. Saisissez quand et à quelle fréquence l'instantané sera pris.
   d. Conservation : saisissez le nombre d'instantanés à conserver.
7. Sélectionnez **Créer**.

Exemple de politique d'instantané utilisant une architecture en cascade

Cet exemple crée une politique de snapshot avec deux clusters :

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

c. Configurez les stratégies de réplication et de sauvegarde des objets.

Créer une politique de réplication avant de lancer la réplication

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

Étapes

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

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

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

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

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

Étapes

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

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

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

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

   "En savoir plus sur les paramètres DataLock disponibles".

7. Sélectionnez **Créer**.

Modifier une politique

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

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

Étapes

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

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

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

Supprimer une politique

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

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

Étapes

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

Trouver plus d'informations

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

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

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

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

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

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

Options de planification de sauvegarde

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

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

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

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

Par exemple, supposons que vous créiez une politique de sauvegarde qui crée 7 sauvegardes **hebdomadaires** et 12 sauvegardes **mensuelles** :

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

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

Options de protection DataLock et Ransomware

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

Ces deux fonctionnalités protègent vos fichiers de sauvegarde afin que vous disposiez toujours d'un fichier de sauvegarde valide pour récupérer des données en cas de tentative d'attaque par ransomware sur vos sauvegardes. Il est également utile de répondre à certaines exigences réglementaires selon lesquelles les

sauvegardes doivent être verrouillées et conservées pendant une certaine période. Lorsque l'option DataLock et Ransomware Resilience est activée, le verrouillage et le contrôle de version des objets seront activés pour le bucket cloud provisionné dans le cadre de l'activation de NetApp Backup and Recovery .

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

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

Qu'est-ce que DataLock

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 objet, l'exportation des instantanés historiques en tant que fichiers de sauvegarde et l'activation ou la désactivation des analyses de ransomware pour un système.

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

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

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

- 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[]
- Modification de la façon dont les instantanés historiques sont exportés ou non en tant que fichiers de sauvegarde et inclus dans vos fichiers de sauvegarde de référence initiaux pour les volumes futurs
- Modifier si les instantanés « annuels » sont supprimés du système source
- Activation ou désactivation des analyses de ransomware pour un système, y compris les analyses planifiées

Afficher les paramètres de sauvegarde au niveau du cluster

Vous pouvez 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.

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

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

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

Étapes

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

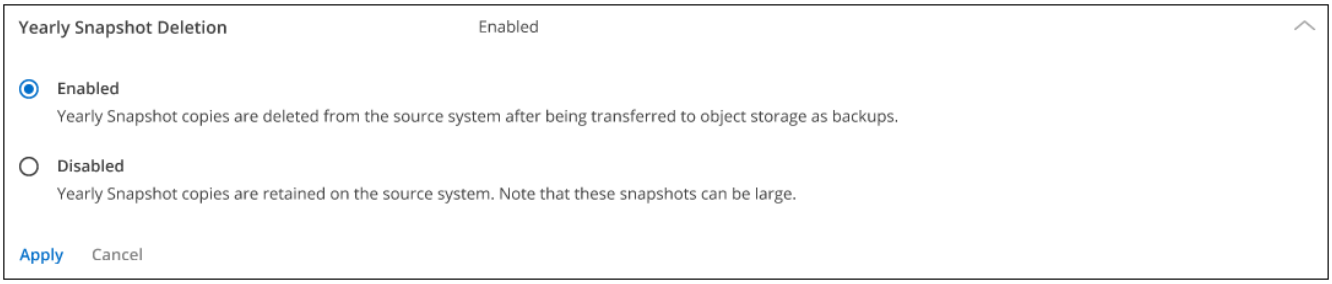
3. Dans la page Paramètres avancés, développez la section **Exporter les instantanés existants**.
4. Indiquez si vous souhaitez exporter les instantanés existants.
5. Sélectionnez **Appliquer**.

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

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

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, cliquez sur••• pour le système 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 le dernier instantané. Vous pouvez activer ou désactiver les analyses de ransomware sur le dernier instantané en utilisant l'option disponible 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 planifiées des logiciels de ransomware ne s'exécutent que sur le dernier instantané.

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.

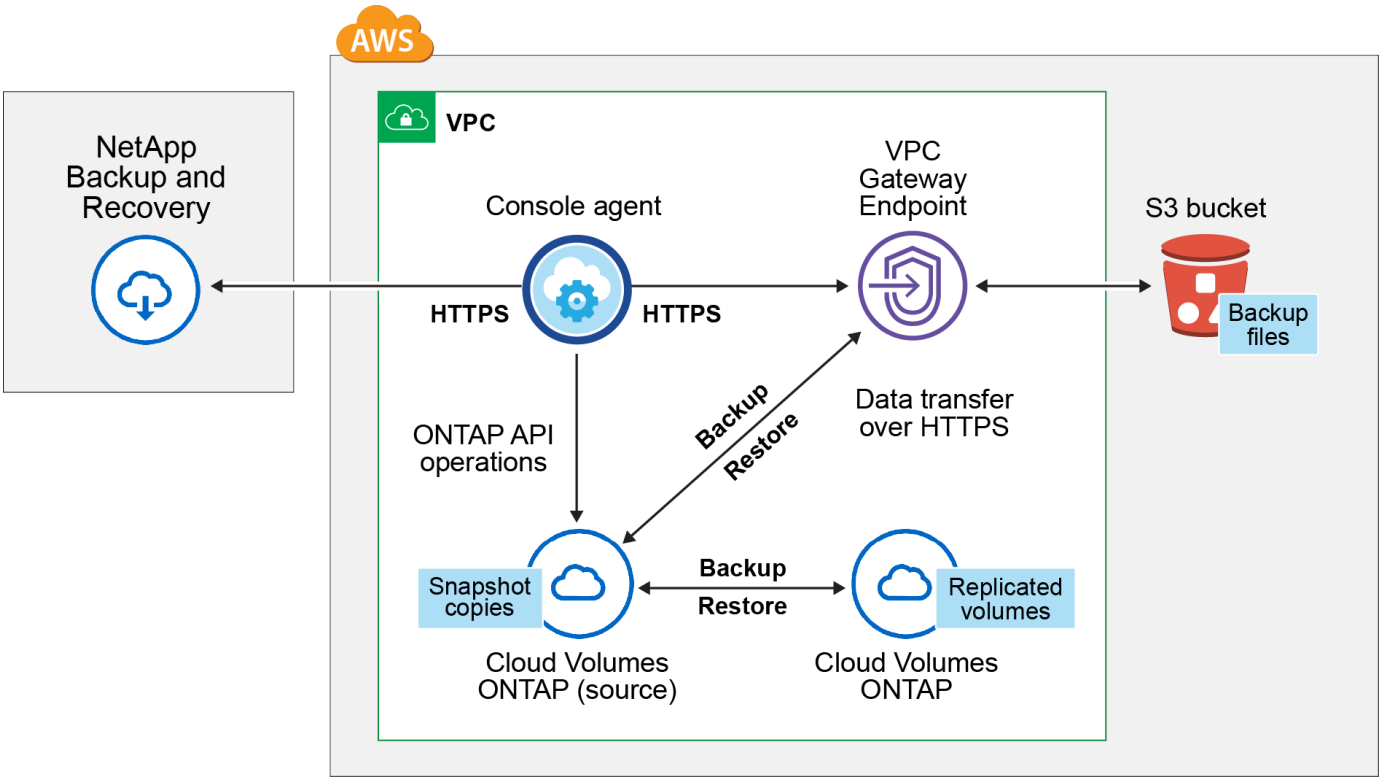
Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

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 les instantanés existants vers le stockage objet en tant que copies de sauvegarde** : Si des instantanés locaux de volumes de ce système correspondent à l'étiquette de planification de

sauvegarde que vous venez de sélectionner pour ce système (par exemple, quotidien, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage d'objets en tant que fichiers de sauvegarde afin de garantir la protection la plus complète pour vos volumes.

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

Résultat

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

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

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

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

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

Afficher les commandes de l'API

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

Étapes

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

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

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

stockage Azure Blob.

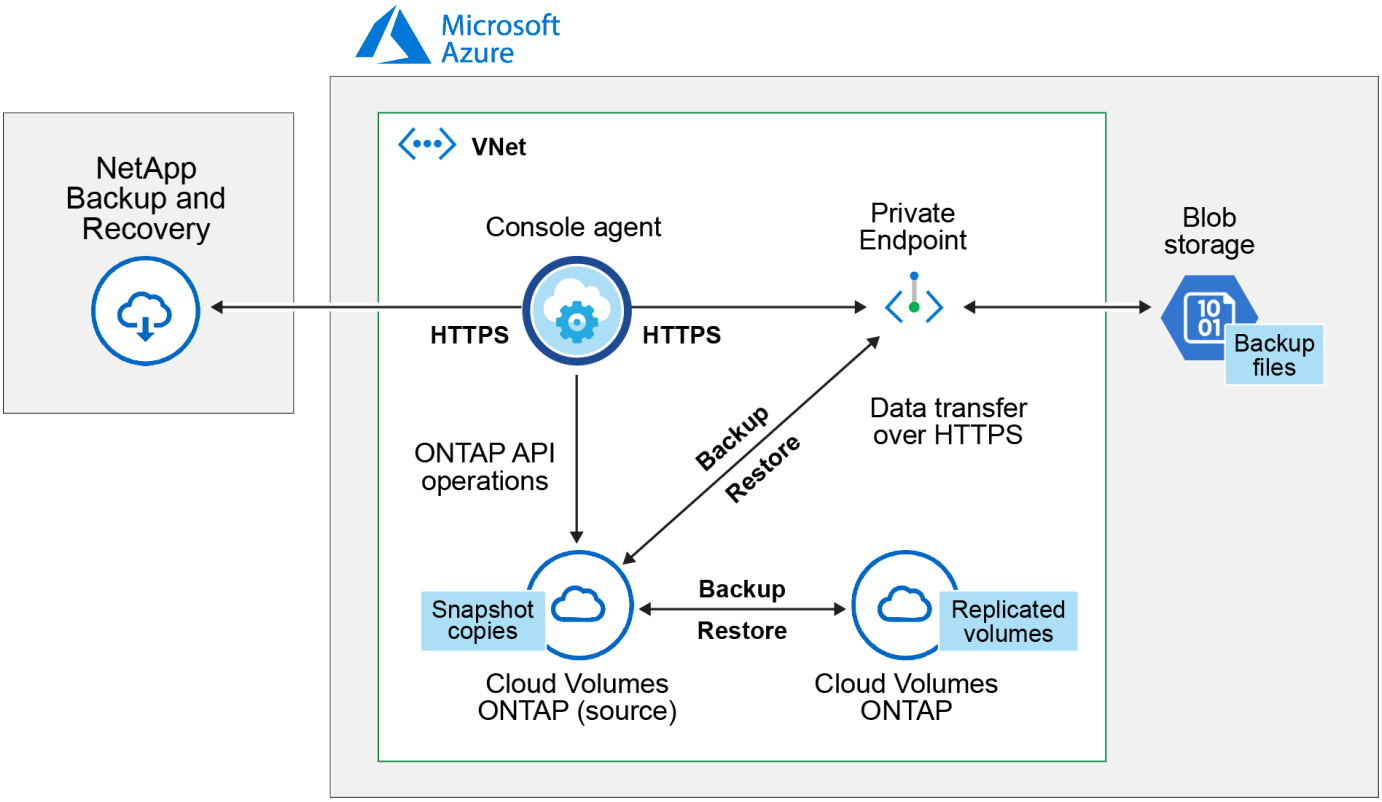
Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Vérifiez la prise en charge de votre configuration

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

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

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



Versions ONTAP prises en charge

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

Régions Azure prises en charge

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

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

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

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

Vérifier les exigences de licence

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

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

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

Préparez votre agent de console

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

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

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

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

Avant de commencer

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

Étapes

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

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

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

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

"Afficher le format JSON complet de la politique"

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

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

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

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

Créez votre compte de stockage Azure Blob

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

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

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Activer la NetApp Backup and Recovery sur Cloud Volumes ONTAP

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

Activer la NetApp Backup and Recovery sur un nouveau système

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

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

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

Étapes

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

Résultat

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

Activer la NetApp Backup and Recovery sur un système existant

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

Étapes

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

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

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

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

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

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

Démarrer l'assistant

Étapes

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

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

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

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

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

2. Continuez avec les options suivantes :

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

Sélectionnez les volumes que vous souhaitez sauvegarder

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

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

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

Étapes

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

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

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

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

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

Résultat

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

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

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

Par défaut, NetApp Backup and Recovery provisionne le conteneur Blob avec une redondance locale (LRS) pour l'optimisation des coûts. Vous pouvez modifier ce paramètre en Redondance de zone (ZRS) si vous

souhaitez vous assurer que vos données sont répliquées entre différentes zones. Consultez les instructions de Microsoft pour "modifier la façon dont votre compte de stockage est répliqué" .

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

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

Afficher les commandes de l'API

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

Étapes

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

Quelle est la prochaine étape ?

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

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

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

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

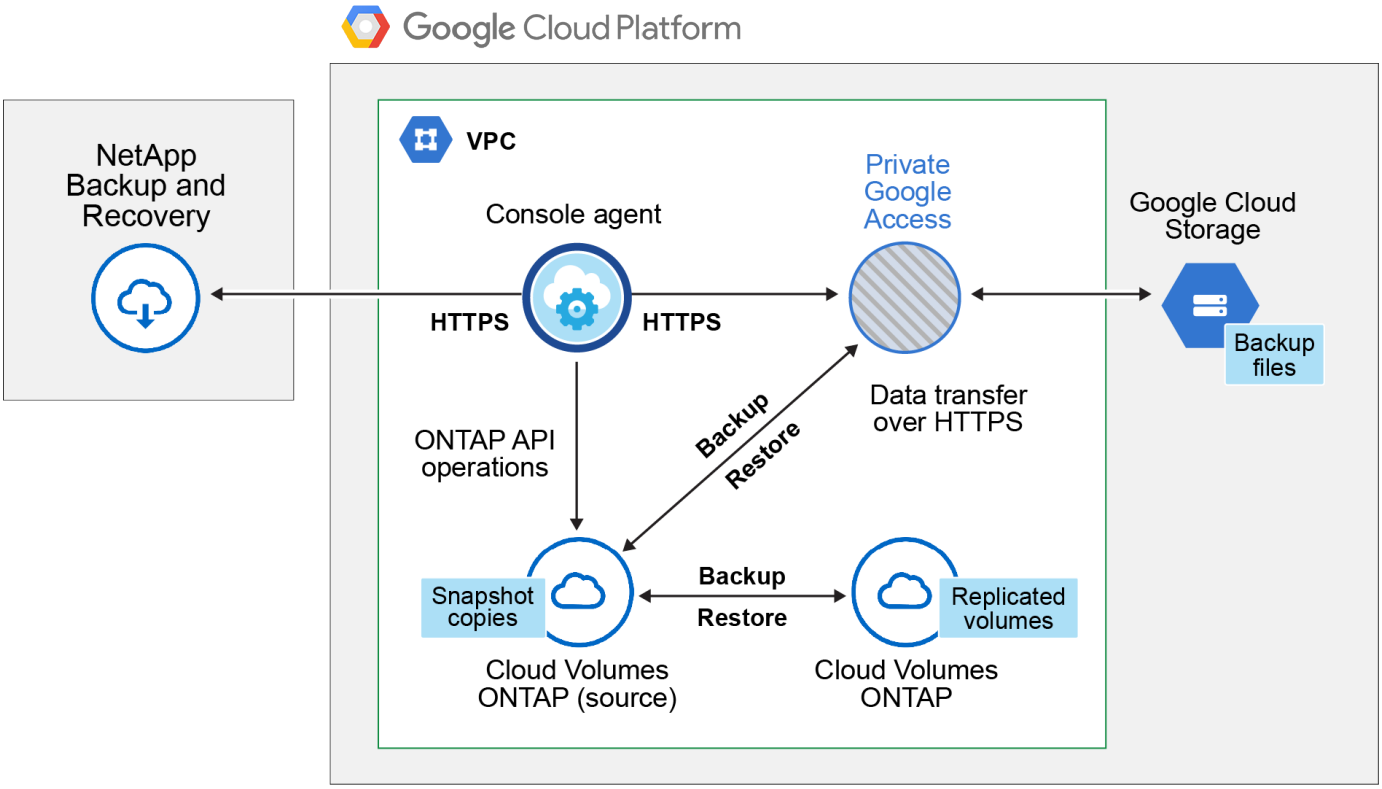
Vérifiez la prise en charge de votre configuration

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

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

En option, vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes

répliqués à l'aide de la connexion publique ou privée.



Versions ONTAP prises en charge

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

Régions GCP prises en charge

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

Compte de service GCP

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

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

Vérifier les exigences de licence

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

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

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

Préparez votre agent de console

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

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

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

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

Étapes

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

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

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

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

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

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

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

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

Considérations CMEK :

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

Créez vos propres seaux

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

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

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Activer la NetApp Backup and Recovery sur Cloud Volumes ONTAP

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

Activer la NetApp Backup and Recovery sur un nouveau système

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

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

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

Étapes

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

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

Résultat

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

Activer la NetApp Backup and Recovery sur un système existant

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

Étapes

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

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

Préparez Google Cloud Storage comme cible de sauvegarde

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

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

Configurer les autorisations

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

Étapes

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

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

3. Dans la console Google Cloud, "aller à la page Comptes de service" .
4. Sélectionnez votre projet Cloud.
5. Sélectionnez **Créer un compte de service** et fournissez les informations requises :

a. **Détails du compte de service** : saisissez un nom et une description.

b. **Accorder à ce compte de service l'accès au projet** : sélectionnez le rôle personnalisé que vous venez de créer.

c. Sélectionnez **Terminé**.

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

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

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

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

Créez vos propres seaux

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

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

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

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

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

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

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

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

Considérations CMEK :

- Les clés HSM (protégées par le matériel) et les clés générées par logiciel sont prises en charge.

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

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

Vous pouvez 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 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 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

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

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

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

secondaire vers le stockage d'objets.

- **Fan out** : les informations circulent du système de stockage principal vers le secondaire *et* du système principal vers le stockage d'objets.

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

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

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

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

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

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

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

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

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

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

     Créez un nouveau bucket ou sélectionnez-en un existant.

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

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

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

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

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

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

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

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

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

Résultat

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

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

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

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

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

sauvegardes.

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

Afficher les commandes de l'API

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

Étapes

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

Quelle est la prochaine étape ?

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

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

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

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

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

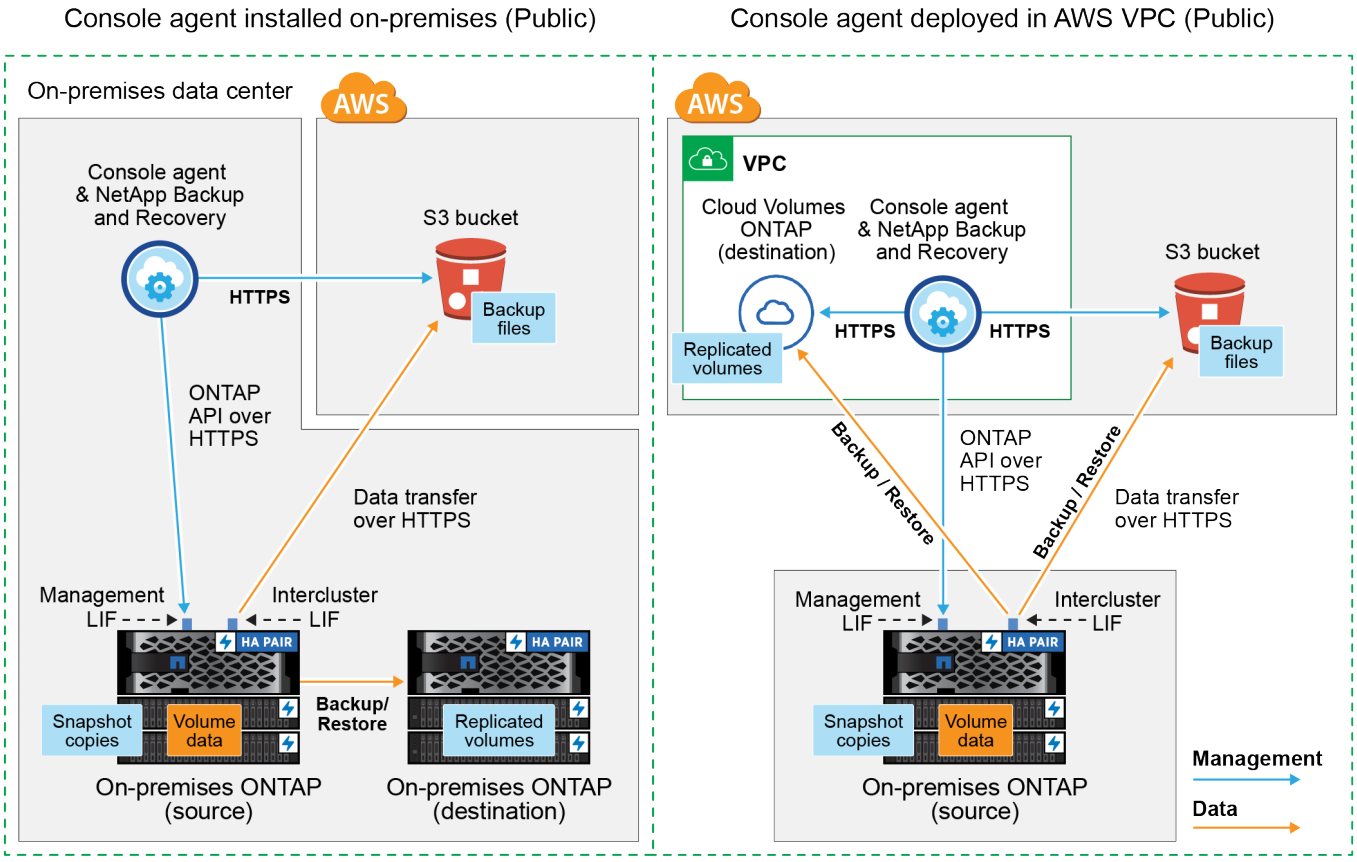
Identifier la méthode de connexion

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

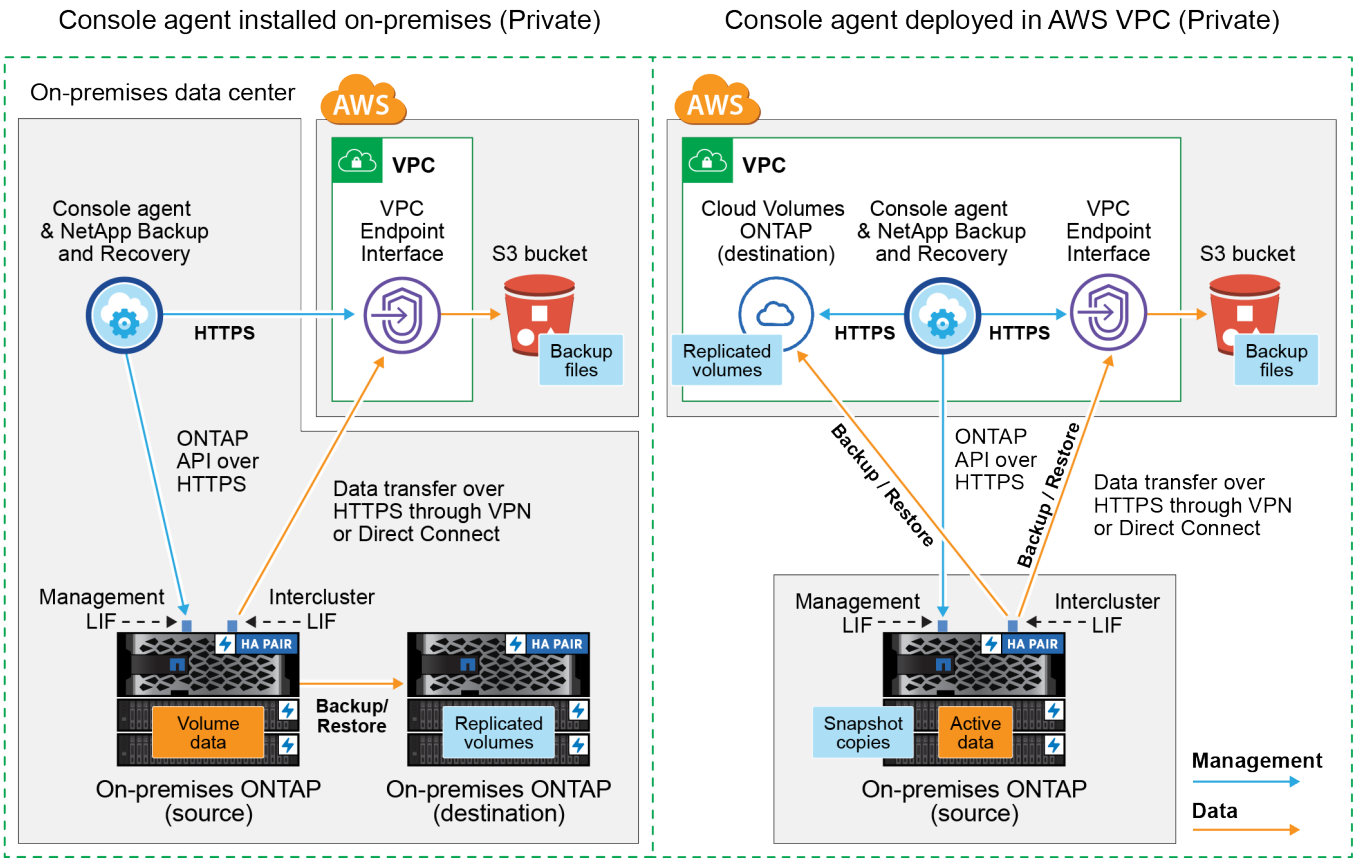
- **Connexion publique** - Connectez directement le système ONTAP à AWS S3 à l'aide d'un point de terminaison S3 public.
- **Connexion privée** - Utilisez un VPN ou AWS Direct Connect et acheminez le trafic via une interface de point de terminaison VPC qui utilise une adresse IP privée.

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

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



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



Préparez votre agent de console

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

Créer ou changer d'agents de console

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

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

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

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

Préparer les exigences réseau de l'agent de console

Assurez-vous que les exigences réseau suivantes sont respectées :

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

Vérifier les exigences de licence

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

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

Régions prises en charge

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

Préparez vos clusters ONTAP

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

La préparation de vos clusters ONTAP implique les étapes suivantes :

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

Découvrez vos systèmes ONTAP dans la NetApp Console

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

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

Vérifier la configuration système requise ONTAP

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

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

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

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

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

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

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

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

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

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

  Le cluster initie une connexion HTTPS sortante via le port 443 depuis les LIF interclusters vers le stockage Amazon S3 pour les opérations de sauvegarde et de restauration. ONTAP lit et écrit des données vers et depuis le stockage d'objets : le stockage d'objets ne s'initialise jamais, il répond simplement.
- Les LIF intercluster doivent être associés à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

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

  Si vous utilisez un espace IP différent de « Par défaut », vous devrez peut-être créer une route statique

pour accéder au stockage d'objets.

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

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

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Préparez Amazon S3 comme cible de sauvegarde

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

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

Configurer les autorisations S3

Vous devrez configurer deux ensembles d'autorisations :

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

Étapes

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

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

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

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

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

Créez vos propres seaux

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

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

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

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

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

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

chiffrement.

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

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

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

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

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

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

Étapes

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

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

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

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

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

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

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

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

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

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

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

Démarrer l'assistant

Étapes

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

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

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

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

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

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

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

Sélectionnez les volumes que vous souhaitez sauvegarder

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

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

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

Étapes

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

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

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

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

3. Sélectionnez **Activer la sauvegarde**.

Résultat

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

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

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

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

Afficher les commandes de l'API

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

Étapes

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

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

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

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

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

Identifier la méthode de connexion

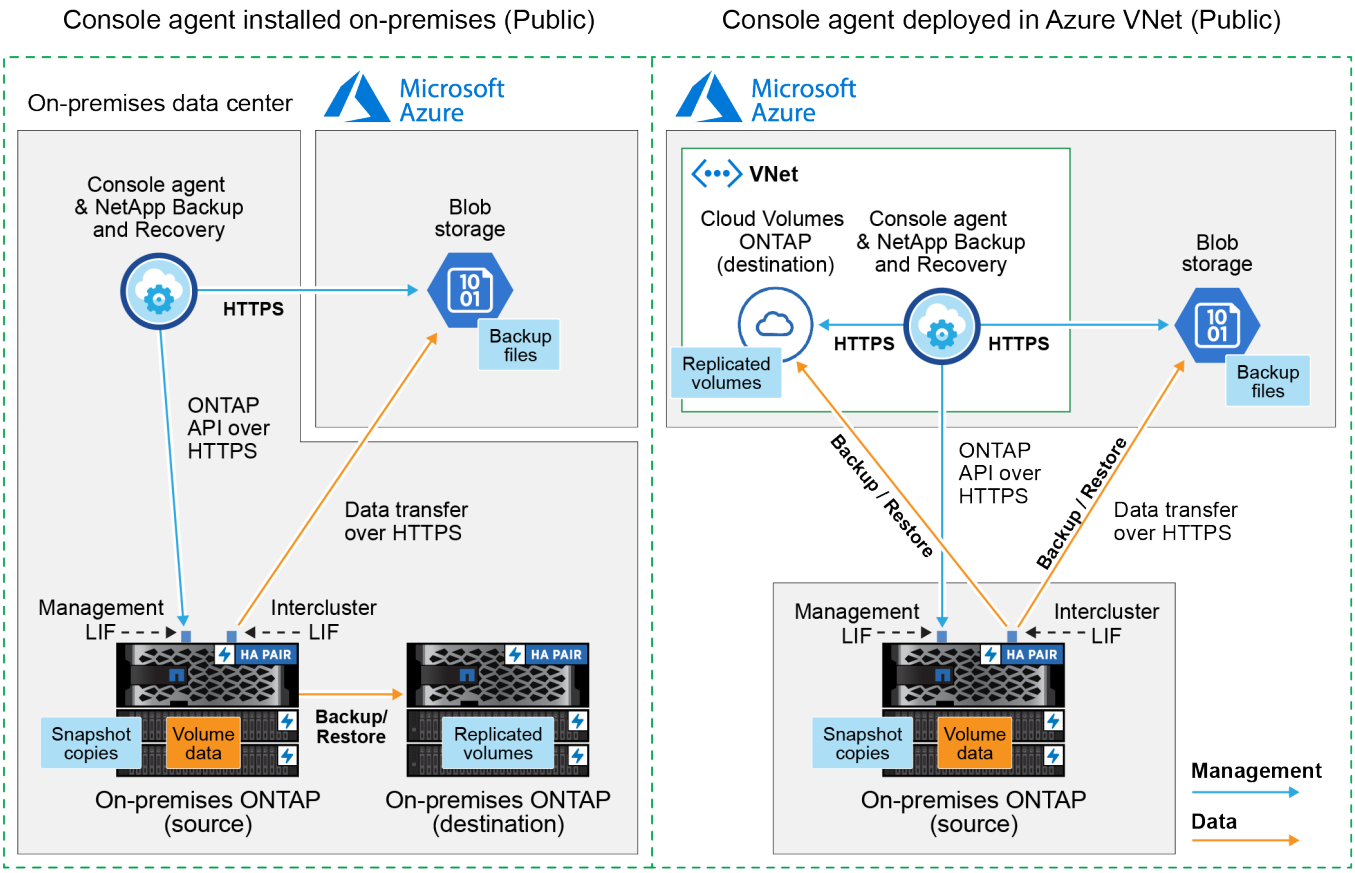
Choisissez laquelle des deux méthodes de connexion vous utiliserez lors de la configuration des sauvegardes des systèmes ONTAP locaux vers Azure Blob.

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

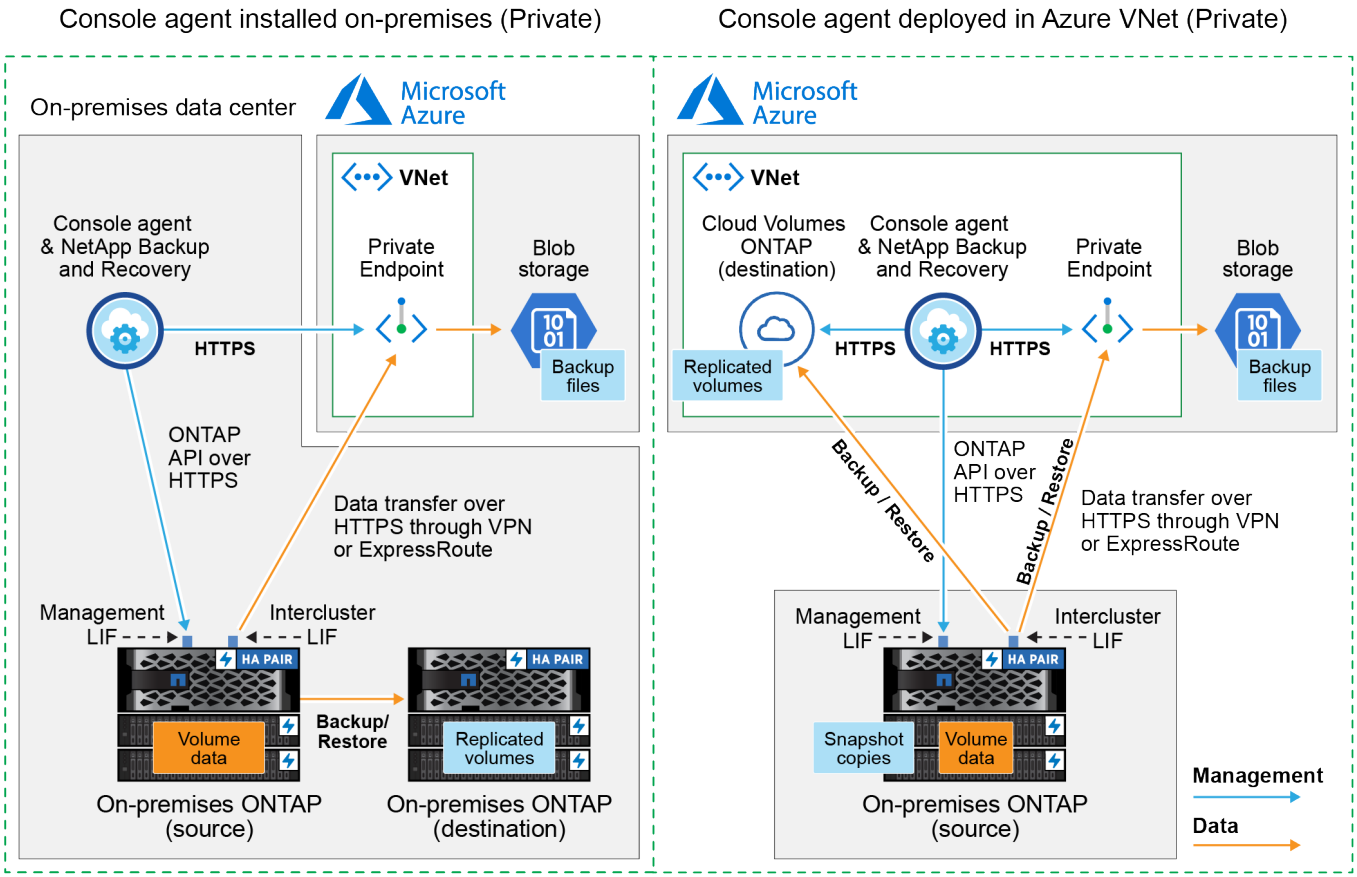
privé VNet qui utilise une adresse IP privée.

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

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



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



Préparez votre agent de console

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

Créer ou changer d'agents de console

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

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

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

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

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

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

Étapes

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

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

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

Avant de commencer

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

Étapes

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

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

"Afficher le format JSON complet de la politique"

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

Vérifier les exigences de licence

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

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

Régions prises en charge

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

Préparez vos clusters ONTAP

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

La préparation de vos clusters ONTAP implique les étapes suivantes :

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

Découvrez vos systèmes ONTAP dans la NetApp Console

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

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

Vérifier la configuration système requise ONTAP

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

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

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

Recovery.

Apprenez à "gérez vos licences de cluster" .

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

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

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

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

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

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

- Le cluster ONTAP initie une connexion HTTPS via le port 443 du LIF intercluster au stockage Azure Blob pour les opérations de sauvegarde et de restauration.

  ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.

- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster. L'agent de console peut résider dans un réseau virtuel Azure.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

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

- Les LIF des nœuds et des interclusters peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions du service NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port 443 et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Préparez Azure Blob comme cible de sauvegarde

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

   Notez que la sauvegarde et la récupération prennent en charge les *stratégies d'accès Azure* comme modèle d'autorisation. Le modèle d'autorisation *Azure role-based access control* (Azure RBAC) n'est actuellement pas pris en charge.

2. Si vous souhaitez disposer d'une connexion plus sécurisée sur l'Internet public depuis votre centre de données local vers le réseau virtuel, il existe une option permettant de configurer un point de terminaison privé Azure dans l'assistant d'activation. Dans ce cas, vous devrez connaître le VNet et le sous-réseau pour cette connexion. "Consultez les détails sur l'utilisation d'un point de terminaison privé" .

Créez votre compte de stockage Azure Blob

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

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

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

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

Démarrer l'assistant

Étapes

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

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

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

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

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

2. Continuez avec les options suivantes :

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

Sélectionnez les volumes que vous souhaitez sauvegarder

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

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

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

Étapes

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

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

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

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

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

sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.

- **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une nouvelle.

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

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

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

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

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

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

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

     Si vous souhaitez hiérarchiser les fichiers de sauvegarde plus anciens vers Azure Archive Storage pour une optimisation supplémentaire des coûts, assurez-vous que le compte de stockage dispose de la règle de cycle de vie appropriée.

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

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

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

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

- **Politique de sauvegarde** : sélectionnez une politique de sauvegarde sur stockage d'objets existante ou créez-en une nouvelle.

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

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

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

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

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

Résultat

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

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

Un compte de stockage Blob est créé dans le groupe de ressources que vous avez entré et les fichiers de sauvegarde y sont stockés. Le tableau de bord de sauvegarde des volumes s'affiche pour vous permettre de surveiller l'état des sauvegardes.

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

Afficher les commandes de l'API

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

Étapes

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

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

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers Google Cloud Storage.

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

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

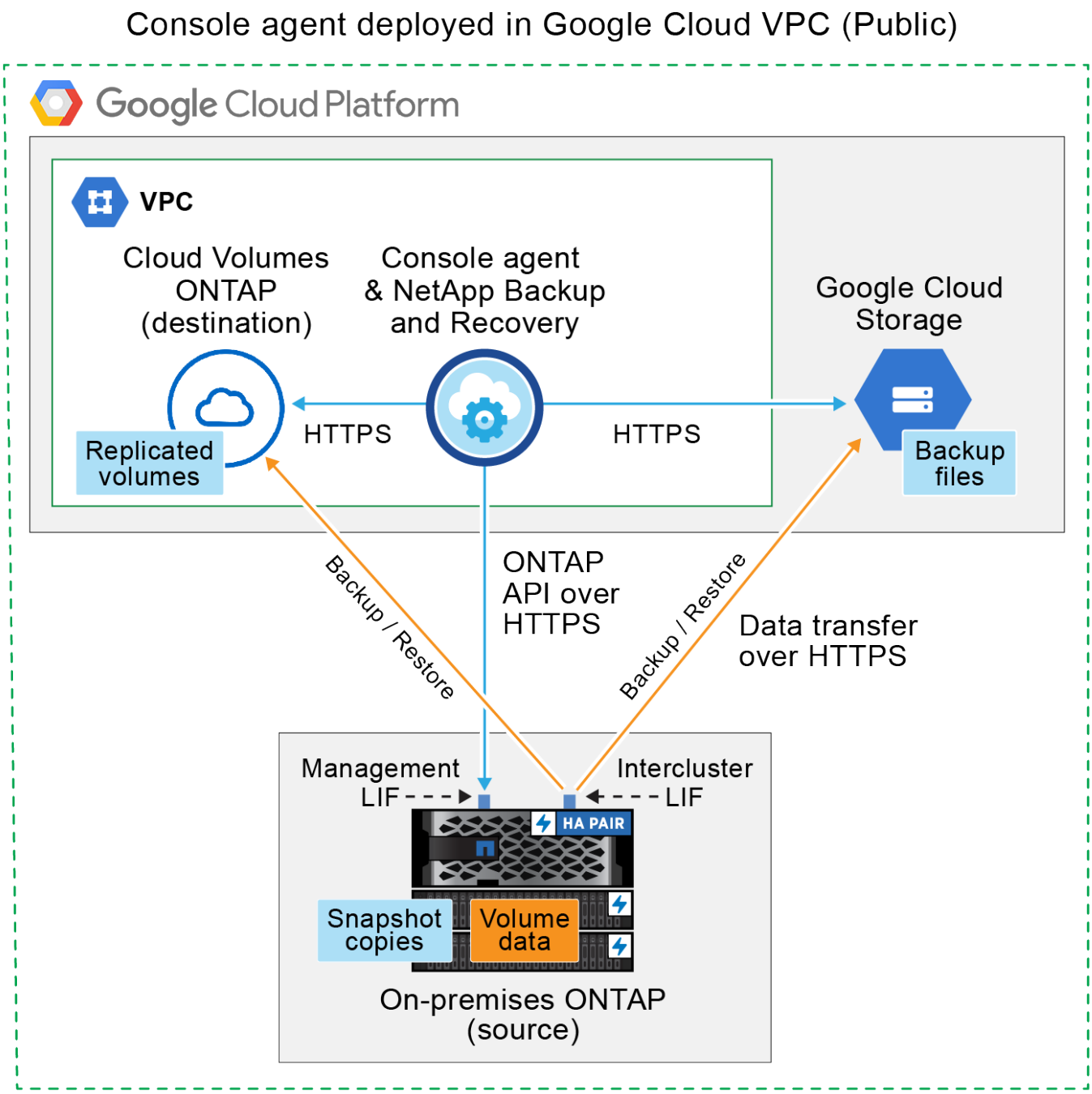
Identifier la méthode de connexion

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

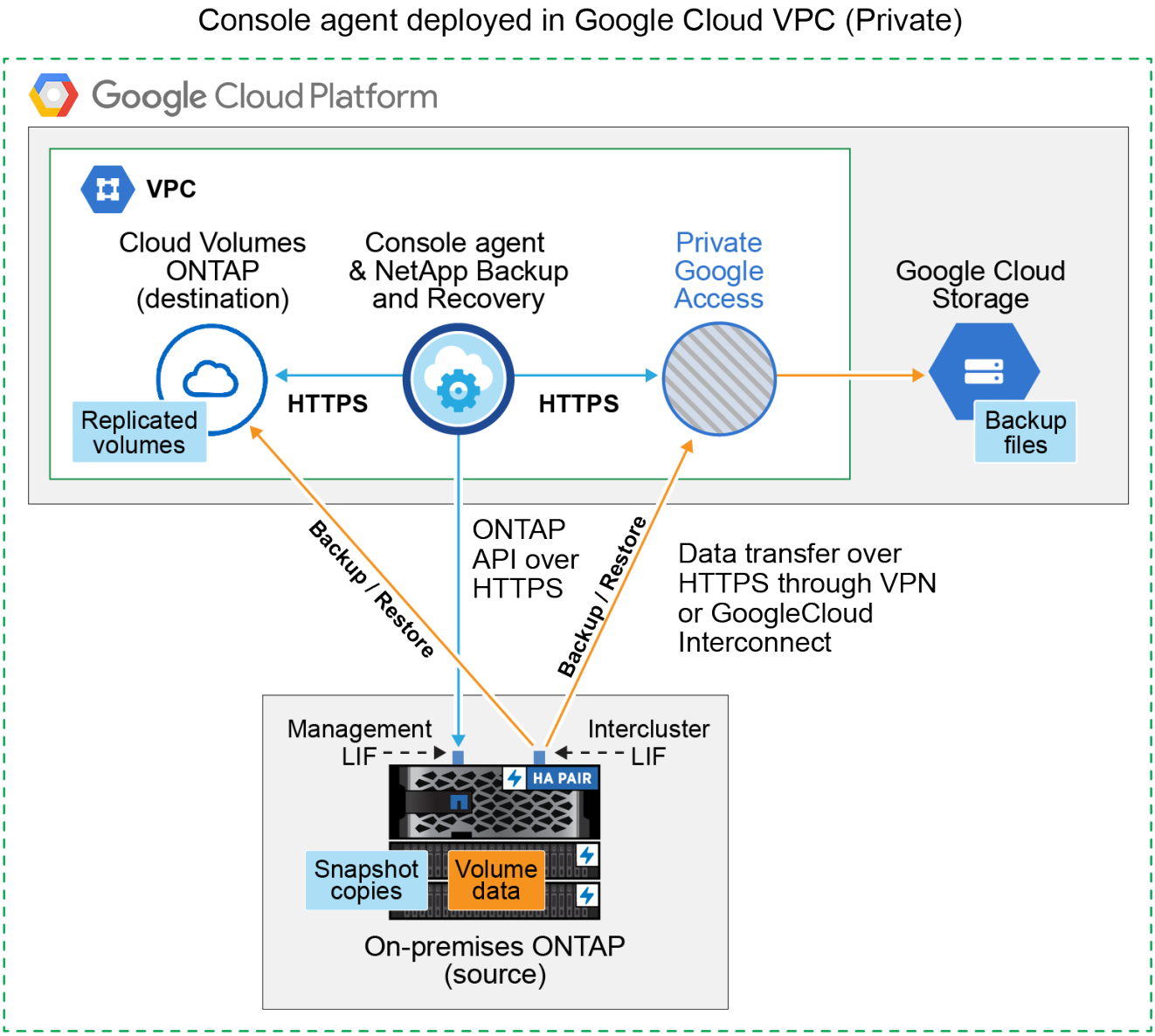
- **Connexion publique** - Connectez directement le système ONTAP à Google Cloud Storage à l'aide d'un point de terminaison Google public.
- **Connexion privée** - Utilisez un VPN ou Google Cloud Interconnect et acheminez le trafic via une interface d'accès privé Google qui utilise une adresse IP privée.

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

Le diagramme suivant montre la méthode de **connexion publique** et les connexions que vous devez préparer entre les composants. L'agent de console doit être déployé dans le VPC Google Cloud Platform.



Le diagramme suivant montre la méthode de **connexion privée** et les connexions que vous devez préparer entre les composants. L'agent de console doit être déployé dans le VPC Google Cloud Platform.



Préparez votre agent de console

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

Créer ou changer d'agents de console

Si vous avez déjà un agent de console déployé dans votre VPC Google Cloud Platform, vous êtes prêt.

Sinon, vous devrez créer un agent de console à cet emplacement pour sauvegarder les données ONTAP sur Google Cloud Storage. Vous ne pouvez pas utiliser un agent de console déployé chez un autre fournisseur de cloud ou sur site.

- "En savoir plus sur les agents de console"
- "Installer un agent de console dans GCP"

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

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

Étapes

1. Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :
   - Une connexion HTTPS via le port 443 vers NetApp Backup and Recovery et vers votre stockage Google Cloud("voir la liste des points de terminaison")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
2. Activez l'accès privé à Google (ou Private Service Connect) sur le sous-réseau où vous prévoyez de déployer l'agent de console. "Accès privé à Google" ou "Connexion au service privé" sont nécessaires si vous disposez d'une connexion directe entre votre cluster ONTAP et le VPC et que vous souhaitez que la communication entre l'agent de la console et Google Cloud Storage reste dans votre réseau privé virtuel (une connexion **privée**).

   Suivez les instructions de Google pour configurer ces options d'accès privé. Assurez-vous que vos serveurs DNS ont été configurés pour pointer `www.googleapis.com` et `storage.googleapis.com` aux adresses IP internes (privées) correctes.

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

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

Étapes

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

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

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

Vérifier les exigences de licence

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

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes locaux vers Google Cloud Storage dans toutes les régions. Vous spécifiez la région où les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

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

La préparation de vos clusters ONTAP implique les étapes suivantes :

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

Découvrez vos systèmes ONTAP dans la NetApp Console

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

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

Vérifier la configuration système requise ONTAP

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

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

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

  Apprenez à "gérez vos licences de cluster" .

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

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

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

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

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

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

- Le cluster ONTAP initie une connexion HTTPS via le port 443 du LIF intercluster vers Google Cloud Storage pour les opérations de sauvegarde et de restauration.

  ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.

- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster. L'agent de la console peut résider dans un VPC Google Cloud Platform.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

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

- Les LIF intercluster des nœuds peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .

  Si vous utilisez Private Google Access ou Private Service Connect, assurez-vous que vos serveurs DNS ont été configurés pour pointer `storage.googleapis.com` à l'adresse IP interne (privée) correcte.

- Notez que si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port 443 et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Préparez Google Cloud Storage comme cible de sauvegarde

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

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

Configurer les autorisations

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

Étapes

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

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

3. Dans la console Google Cloud, "aller à la page Comptes de service" .
4. Sélectionnez votre projet Cloud.
5. Sélectionnez **Créer un compte de service** et fournissez les informations requises :
   a. **Détails du compte de service** : saisissez un nom et une description.
   b. **Accorder à ce compte de service l'accès au projet** : sélectionnez le rôle personnalisé que vous venez de créer.
   c. Sélectionnez **Terminé**.
6. Aller à "Paramètres de stockage GCP" et créez des clés d'accès pour le compte de service :
   a. Sélectionnez un projet et sélectionnez **Interopérabilité**. Si vous ne l'avez pas déjà fait, sélectionnez **Activer l'accès à l'interopérabilité**.
   b. Sous **Clés d'accès pour les comptes de service**, sélectionnez **Créer une clé pour un compte de service**, sélectionnez le compte de service que vous venez de créer et cliquez sur **Créer une clé**.

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

Créez vos propres seaux

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

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

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

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

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

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

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

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

Considérations CMEK :

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

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

Vous pouvez 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 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 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 primaire vers le secondaire et du secondaire vers le stockage d'objets.
   - **Fan out** : les informations circulent du primaire vers le secondaire *et* du primaire vers le stockage d'objets.

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

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

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat ou les agrégats de destination et le préfixe ou le suffixe qui seront ajoutés au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une nouvelle.

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

     Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Google Cloud**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région où les sauvegardes seront stockées.

     Créez un nouveau bucket ou sélectionnez-en un que vous avez déjà créé.

     Si vous souhaitez hiérarchiser les fichiers de sauvegarde plus anciens vers le stockage Google Cloud Archive pour une optimisation supplémentaire des coûts, assurez-vous que le bucket dispose de la règle de cycle de vie appropriée.

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

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

Si vous choisissez d'utiliser vos propres clés gérées par le client, saisissez le trousseau et le nom de la clé. "En savoir plus sur les clés de chiffrement gérées par le client" .

- **Réseau** : Choisissez l'espace IP.

  L'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.

- **Politique de sauvegarde** : sélectionnez une politique de sauvegarde sur stockage d'objets existante ou créez-en une nouvelle.

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

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

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

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

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

Résultat

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

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

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

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

Afficher les commandes de l'API

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

Étapes

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

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

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos principaux systèmes ONTAP sur site. Vous pouvez envoyer des sauvegardes vers un système de stockage ONTAP secondaire (un volume répliqué) ou vers un bucket sur un système ONTAP configuré comme serveur S3 (un fichier de sauvegarde), ou les deux.

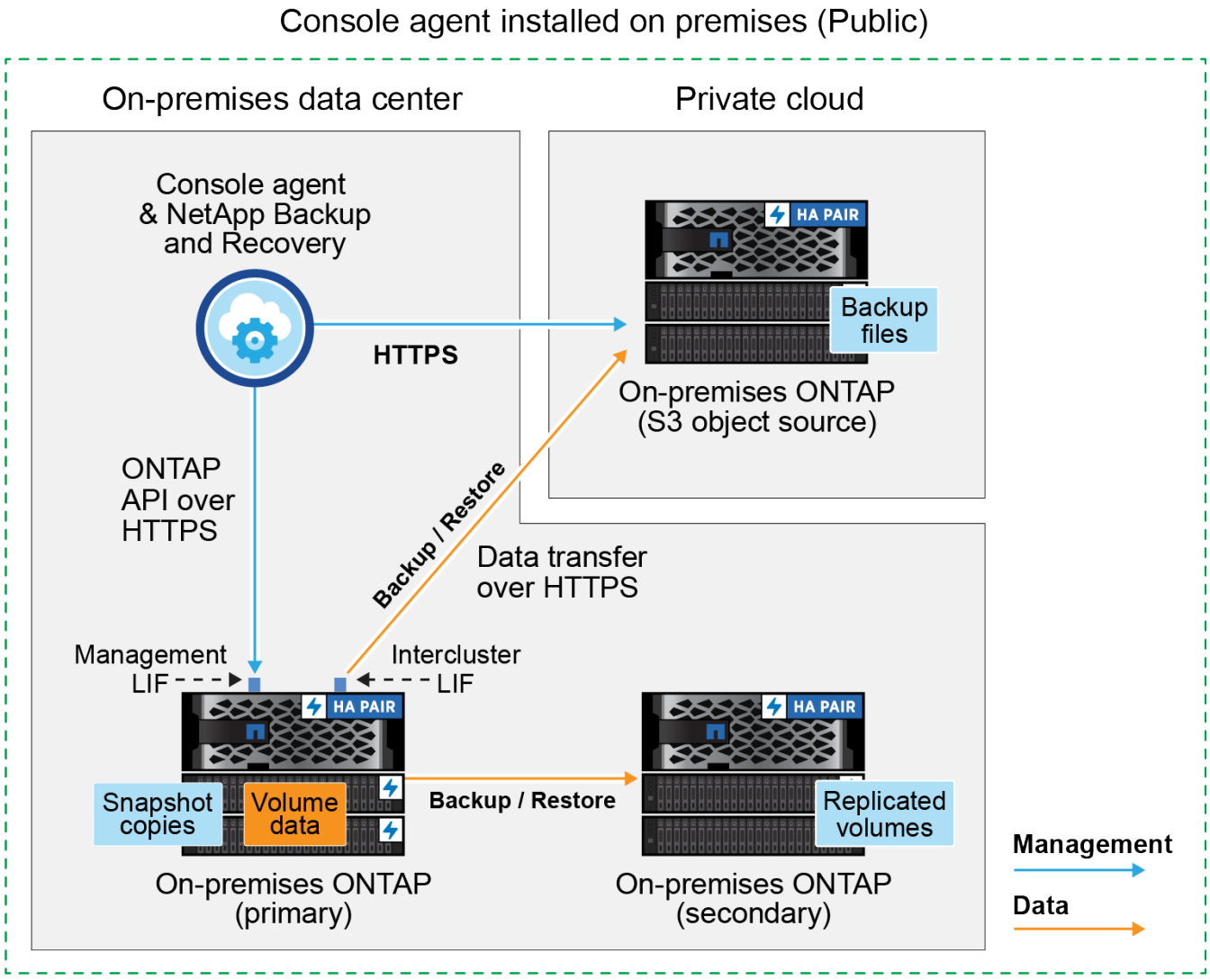
Le système ONTAP principal sur site peut être un système FAS, AFF ou ONTAP Select . Le système ONTAP secondaire peut être un système ONTAP local ou Cloud Volumes ONTAP . Le stockage d'objets peut se trouver sur un système ONTAP local ou sur un système Cloud Volumes ONTAP sur lequel vous avez activé un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

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

Identifier la méthode de connexion

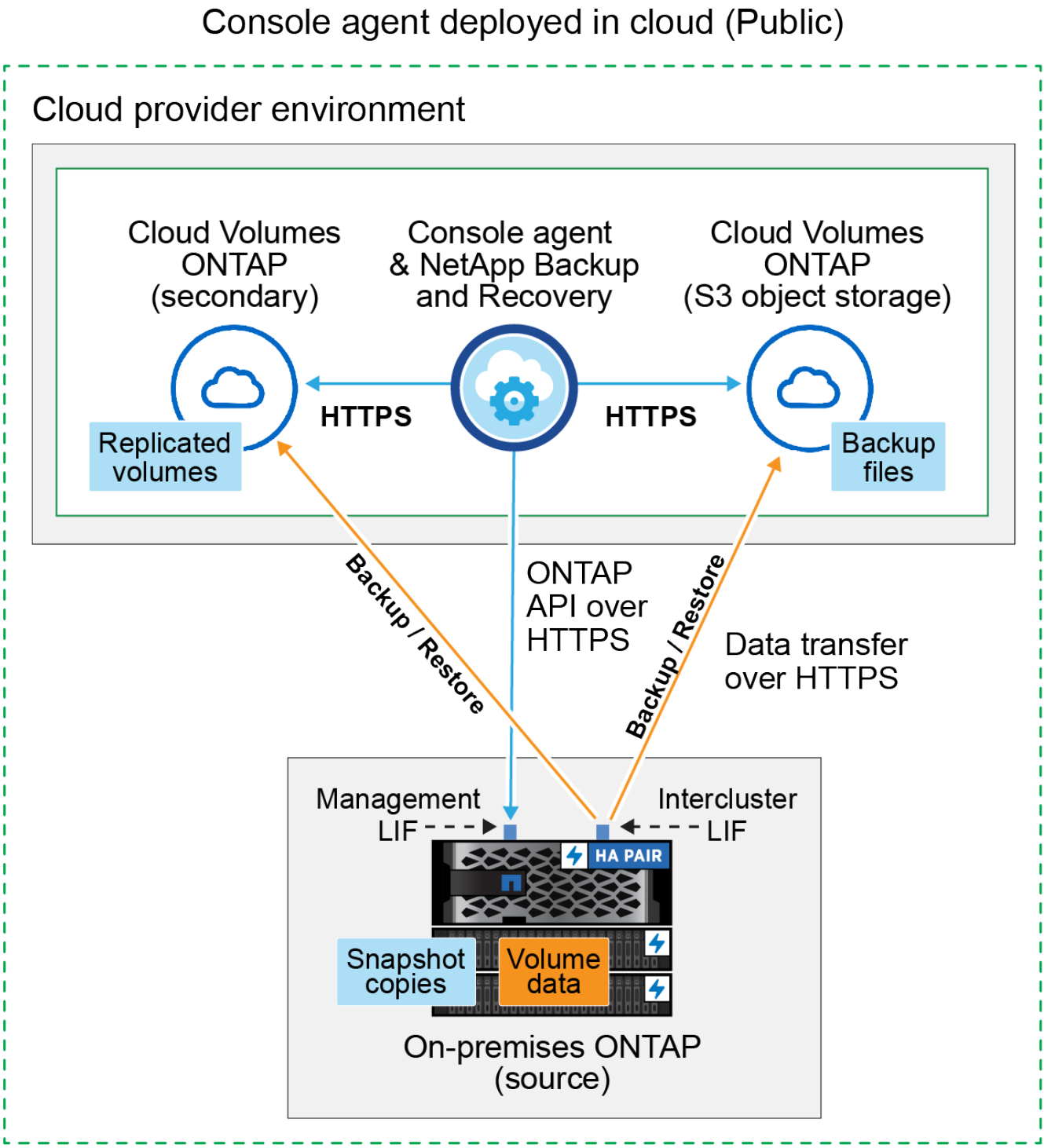
Il existe de nombreuses configurations dans lesquelles vous pouvez créer des sauvegardes dans un bucket S3 sur un système ONTAP . Deux scénarios sont présentés ci-dessous.

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP principal sur site vers un système ONTAP sur site configuré pour S3 et les connexions que vous devez préparer entre eux. Il montre également une connexion à un système ONTAP secondaire dans le même emplacement sur site pour répliquer les volumes.



Lorsque l'agent de console et le système ONTAP principal sur site sont installés dans un emplacement sur site sans accès Internet (déploiement en mode « privé »), le système ONTAP S3 doit être situé dans le même centre de données sur site.

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP principal sur site vers un système Cloud Volumes ONTAP configuré pour S3 et les connexions que vous devez préparer entre eux. Il montre également une connexion à un système Cloud Volumes ONTAP secondaire dans le même environnement de fournisseur de cloud pour répliquer les volumes.



Dans ce scénario, l'agent de console doit être déployé dans le même environnement de fournisseur de cloud dans lequel les systèmes Cloud Volumes ONTAP sont déployés.

Préparez votre agent de console

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

Créer ou changer d'agents de console

Lorsque vous sauvegardez des données sur ONTAP S3, un agent de console doit être disponible sur vos locaux ou dans le cloud. Vous devrez soit installer un nouvel agent de console, soit vous assurer que l'agent de console actuellement sélectionné réside dans l'un de ces emplacements. L'agent de console sur site peut être installé sur un site avec ou sans accès Internet.

- "En savoir plus sur les agents de console"
- "Installez l'agent de console dans votre environnement cloud"
- "Installation de l'agent de console sur un hôte Linux avec accès Internet"
- "Installation de l'agent Console sur un hôte Linux sans accès Internet"
- "Basculer entre les agents de la console"

Préparer les exigences réseau de l'agent de console

Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :

- Une connexion HTTPS sur le port 443 vers le serveur ONTAP S3
- Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP source
- Une connexion Internet sortante via le port 443 vers NetApp Backup and Recovery (non requise lorsque l'agent de console est installé sur un site « sombre »)

Considérations sur le mode privé (site sombre)

La fonctionnalité de NetApp Backup and Recovery est intégrée à l'agent de la console. Lorsqu'il est installé en mode privé, vous devrez mettre à jour périodiquement le logiciel de l'agent de la console pour accéder aux nouvelles fonctionnalités. Vérifiez le"Nouveautés de NetApp Backup and Recovery" pour voir les nouvelles fonctionnalités de chaque version de NetApp Backup and Recovery . Lorsque vous souhaitez utiliser les nouvelles fonctionnalités, suivez les étapes pour "mettre à niveau le logiciel de l'agent de la console" .

Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS standard, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le cloud. Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le compartiment ONTAP S3 où vos sauvegardes sont stockées.

Vérifier les exigences de licence

Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. La licence concerne la sauvegarde et la restauration sur stockage objet ; aucune licence n'est nécessaire pour créer des instantanés ou des volumes répliqués. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

Vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .

La licence PAYGO n'est pas prise en charge lors de la sauvegarde de fichiers sur ONTAP S3.

Préparez vos clusters ONTAP

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

secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

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

Découvrez vos systèmes ONTAP dans la NetApp Console

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

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

Vérifier la configuration système requise ONTAP

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

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

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

  Apprenez à "gérez vos licences de cluster" .

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

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

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

Vous devez vous assurer que les exigences suivantes sont respectées sur le système qui se connecte au stockage d'objets.

- Lorsque vous utilisez une architecture de sauvegarde en éventail, les paramètres doivent être configurés sur le système de stockage *principal*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres doivent être configurés sur le système de stockage *secondaire*.

  "En savoir plus sur les types d'architecture de sauvegarde".

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

- Le cluster ONTAP initie une connexion HTTPS via un port spécifié par l'utilisateur depuis le LIF intercluster vers le serveur ONTAP S3 pour les opérations de sauvegarde et de restauration. Le port est configurable

lors de la configuration de la sauvegarde.

ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.

- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

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

- Les LIF intercluster des nœuds peuvent accéder au magasin d'objets (non requis lorsque l'agent de console est installé sur un site « sombre »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions du service NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Préparez ONTAP S3 comme cible de sauvegarde

Vous devez activer un serveur de stockage d'objets Simple Storage Service (S3) dans le cluster ONTAP que vous prévoyez d'utiliser pour les sauvegardes de stockage d'objets. Voir le "Documentation ONTAP S3" pour

plus de détails.

Remarque : vous pouvez ajouter ce cluster à la page **Systèmes** de la console, mais il n'est pas identifié comme étant un serveur de stockage d'objets S3 et vous ne pouvez pas glisser-déposer un système source sur ce système S3 pour lancer l'activation de la sauvegarde.

Ce système ONTAP doit répondre aux exigences suivantes.

Versions ONTAP prises en charge

ONTAP 9.8 et versions ultérieures sont requis pour les systèmes ONTAP sur site. ONTAP 9.9.1 et versions ultérieures sont requis pour les systèmes Cloud Volumes ONTAP .

Informations d'identification S3

Vous devez avoir créé un utilisateur S3 pour contrôler l'accès à votre stockage ONTAP S3. "Consultez la documentation ONTAP S3 pour plus de détails" .

Lorsque vous configurez la sauvegarde sur ONTAP S3, l'assistant de sauvegarde vous demande une clé d'accès S3 et une clé secrète pour un compte utilisateur. Le compte utilisateur permet à NetApp Backup and Recovery d'authentifier et d'accéder aux buckets ONTAP S3 utilisés pour stocker les sauvegardes. Les clés sont nécessaires pour ONTAP S3 sache qui fait la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket",
"s3:GetBucketLocation"
```

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

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

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

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

Sélectionnez les volumes que vous souhaitez sauvegarder

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

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

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

Étapes

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

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

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique la configuration des options suivantes :

- Options de protection : si vous souhaitez implémenter une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur le stockage d'objets
- Architecture : si vous souhaitez utiliser une architecture de sauvegarde en éventail ou en cascade

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

Étapes

1. Dans la page Définir la stratégie de sauvegarde, choisissez une ou toutes les options suivantes. Les trois sont sélectionnés par défaut :
   - **Instantanés locaux** : Crée des instantanés locaux.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP .
   - **Sauvegarde** : sauvegarde les volumes dans un bucket sur un système ONTAP configuré pour S3.
2. **Architecture** : Si vous avez choisi à la fois la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **En cascade** : les données de sauvegarde circulent du système principal vers le système secondaire, puis du système secondaire vers le stockage d'objets.
   - **Fan out** : les données de sauvegarde circulent du système principal vers le système secondaire *et* du système principal vers le stockage d'objets.

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

   Si vous souhaitez créer une politique personnalisée avant d'activer le Snapshot, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP. `snapmirror policy create` commande. Se référer à .

   Pour créer une politique personnalisée à l'aide de Sauvegarde et récupération, reportez-vous à"Créer une politique" .

   Pour créer une politique, sélectionnez **Créer une nouvelle politique** et procédez comme suit :
   - Entrez le nom de la politique.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : Si vous avez sélectionné **Réplication**, définissez les options suivantes :
   - **Cible de réplication** : sélectionnez le système de destination et le SVM. Vous pouvez également sélectionner l'agrégat de destination (ou les agrégats pour les volumes FlexGroup) et un préfixe ou un suffixe qui sera ajouté au nom du volume répliqué.
   - **Politique de réplication** : Choisissez une politique de réplication existante ou créez-en une nouvelle.

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

- **Fournisseur** : Sélectionnez * ONTAP S3*.
- **Paramètres du fournisseur** : saisissez les détails du nom de domaine complet (FQDN) du serveur S3, le port, ainsi que la clé d'accès et la clé secrète des utilisateurs.

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

- **Mise en réseau** : choisissez l'espace IP dans le cluster ONTAP source où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant (non requis lorsque l'agent de console est installé sur un site « sombre »).

  La sélection de l'espace IP correct garantit que NetApp Backup and Recovery peut établir une connexion d' ONTAP à votre stockage d'objets ONTAP S3.

- **Politique de sauvegarde** : sélectionnez une politique de sauvegarde existante ou créez-en une nouvelle.

  Vous pouvez créer une politique avec System Manager ou l'interface de ligne de commande ONTAP . Pour créer une politique personnalisée à l'aide de l'interface de ligne de commande ONTAP `snapmirror policy create` commande, se référer à .

  Pour créer une politique personnalisée à l'aide de Sauvegarde et récupération, reportez-vous à"Créer une politique" .

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

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

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

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

1. Dans la page Révision, vérifiez vos sélections.
2. Cochez éventuellement la case pour **Synchroniser automatiquement les étiquettes de politique de snapshot avec les étiquettes de politique de réplication et de sauvegarde**. Cela crée des instantanés avec une étiquette qui correspond aux étiquettes des politiques de réplication et de sauvegarde. Si les politiques ne correspondent pas, les sauvegardes ne seront pas créées.

3. Sélectionnez **Activer la sauvegarde**.

Résultat

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

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

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

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

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

Afficher les commandes de l'API

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

Étapes

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

Sauvegardez les données ONTAP sur site sur StorageGRID avec NetApp Backup and Recovery

Effectuez quelques étapes dans NetApp Backup and Recovery pour commencer à sauvegarder les données de volume de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers le stockage d'objets dans vos systèmes NetApp StorageGRID .

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

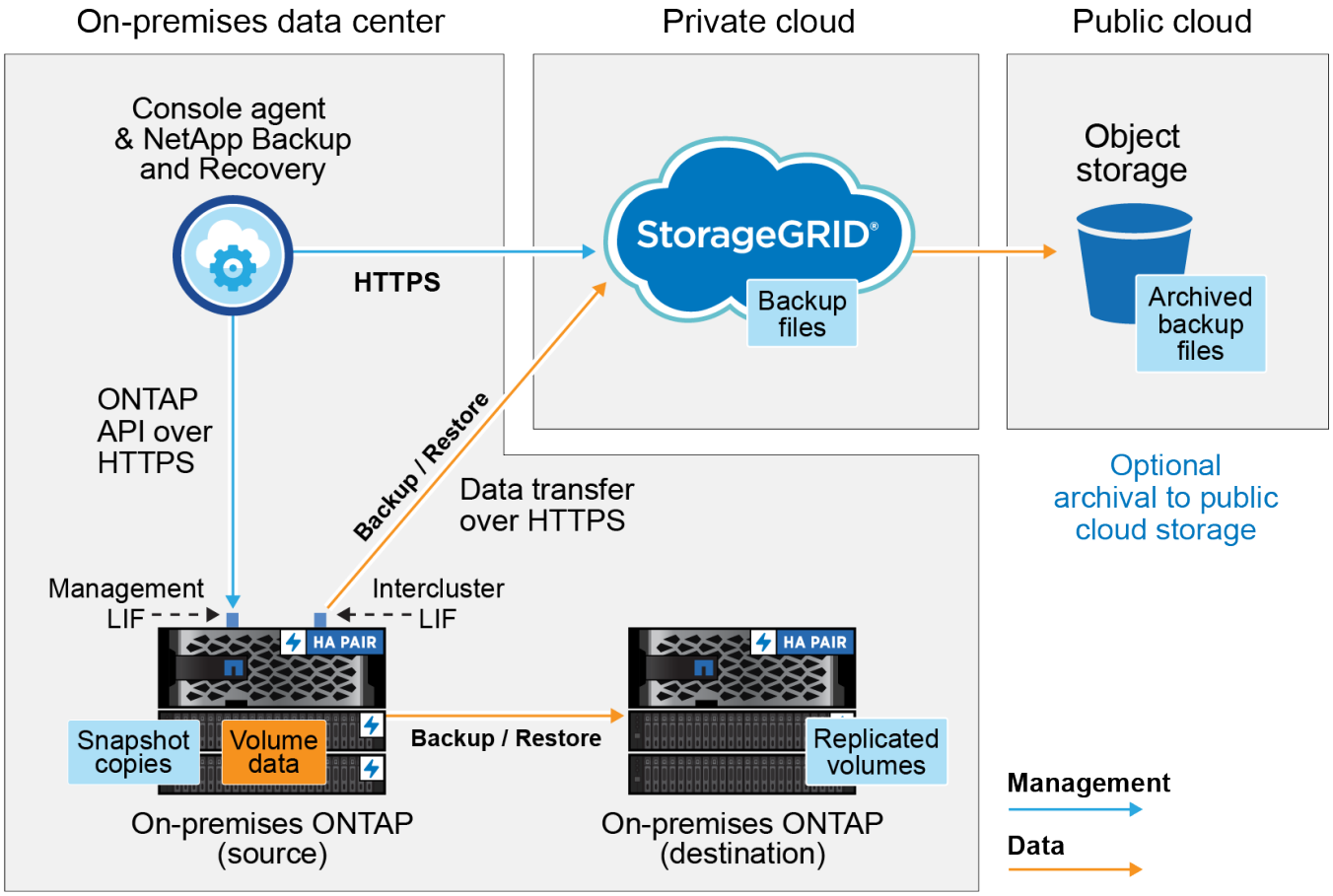
Pour basculer vers et depuis les charges de travail NetApp Backup and Recovery , reportez-vous à"Basculer vers différentes charges de travail de NetApp Backup and Recovery" .

Identifier la méthode de connexion

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP sur site sur StorageGRID et les connexions que vous devez préparer entre eux.

En option, vous pouvez vous connecter à un système ONTAP secondaire dans le même emplacement sur site

pour répliquer les volumes.



Lorsque l'agent de console et le système ONTAP sur site sont installés dans un emplacement sur site sans accès Internet (un « site sombre »), le système StorageGRID doit être situé dans le même centre de données sur site. L'archivage des anciens fichiers de sauvegarde dans le cloud public n'est pas pris en charge dans les configurations de site sombre.

Préparez votre agent de console

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

Créer ou changer d'agents de console

Lorsque vous sauvegardez des données sur StorageGRID, un agent de console doit être disponible dans vos locaux. Vous devrez soit installer un nouvel agent de console, soit vous assurer que l'agent de console actuellement sélectionné réside sur site. L'agent Console peut être installé sur un site avec ou sans accès Internet.

- "En savoir plus sur les agents de console"
- "Installation de l'agent de console sur un hôte Linux avec accès Internet"
- "Installation de l'agent Console sur un hôte Linux sans accès Internet"
- "Basculer entre les agents de la console"

Préparer les exigences réseau de l'agent de console

Assurez-vous que le réseau sur lequel l'agent de console est installé permet les connexions suivantes :

- Une connexion HTTPS via le port 443 vers le nœud de passerelle StorageGRID
- Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
- Une connexion Internet sortante via le port 443 vers NetApp Backup and Recovery (non requise lorsque l'agent de console est installé sur un site « sombre »)

Considérations sur le mode privé (site sombre)

- La fonctionnalité de NetApp Backup and Recovery est intégrée à l'agent de la console. Lorsqu'il est installé en mode privé, vous devrez mettre à jour périodiquement le logiciel de l'agent de la console pour accéder aux nouvelles fonctionnalités. Vérifiez le"Nouveautés de NetApp Backup and Recovery" pour voir les nouvelles fonctionnalités de chaque version de NetApp Backup and Recovery . Lorsque vous souhaitez utiliser les nouvelles fonctionnalités, suivez les étapes pour "mettre à niveau le logiciel de l'agent de la console" .

  La nouvelle version de NetApp Backup and Recovery , qui inclut la possibilité de planifier et de créer des instantanés et des volumes répliqués, en plus de créer des sauvegardes sur le stockage d'objets, nécessite que vous utilisiez la version 3.9.31 ou supérieure de l'agent Console. Il est donc recommandé d'obtenir cette dernière version pour gérer toutes vos sauvegardes.

- Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le cloud. Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le bucket StorageGRID où vos sauvegardes sont stockées.

Vérifier les exigences de licence

Avant de pouvoir activer NetApp Backup and Recovery pour votre cluster, vous devez acheter et activer une licence BYOL NetApp Backup and Recovery auprès de NetApp. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

Vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Apprenez à gérer vos licences BYOL" .

La licence PAYGO n'est pas prise en charge lors de la sauvegarde de fichiers sur StorageGRID.

Préparez vos clusters ONTAP

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

La préparation de vos clusters ONTAP implique les étapes suivantes :

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

Découvrez vos systèmes ONTAP dans la NetApp Console

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

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

Vérifier la configuration système requise ONTAP

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

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

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

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

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

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

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

- Lorsque vous utilisez une architecture de sauvegarde en éventail, les paramètres suivants doivent être configurés sur le système de stockage *principal*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres suivants doivent être configurés sur le système de stockage *secondaire*.

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

- Le cluster ONTAP initie une connexion HTTPS via un port spécifié par l'utilisateur depuis le LIF intercluster vers le nœud de passerelle StorageGRID pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

  ONTAP lit et écrit des données vers et depuis le stockage d'objets. Le stockage d'objets ne s'initialise jamais, il répond simplement.
- ONTAP nécessite une connexion entrante de l'agent de console au LIF de gestion du cluster. L'agent de la console doit résider dans vos locaux.
- Un LIF intercluster est requis sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Le LIF doit être associé à l'*IPspace* ONTAP doit utiliser pour se connecter au stockage d'objets. "En savoir plus sur IPspaces" .

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

- Les LIF intercluster des nœuds peuvent accéder au magasin d'objets (non requis lorsque l'agent de console est installé sur un site « sombre »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où se trouvent les volumes. Découvrez comment "configurer les services DNS pour le SVM" .
- Si vous utilisez un espace IP différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage d'objets.
- Mettez à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions du service NetApp Backup and Recovery d' ONTAP au stockage d'objets via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms de la machine virtuelle de stockage vers le serveur DNS via le port 53 (TCP/UDP).

Vérifier les exigences réseau ONTAP pour la réplication des volumes

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

Exigences de mise en réseau ONTAP sur site

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

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

Exigences réseau de Cloud Volumes ONTAP

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

Préparez StorageGRID comme cible de sauvegarde

StorageGRID doit répondre aux exigences suivantes. Voir le "Documentation de StorageGRID" pour plus d'informations.

Pour plus de détails sur les exigences de résilience DataLock et Ransomware pour StorageGRID, reportez-vous à"Options de politique de sauvegarde sur objet" .

Versions de StorageGRID prises en charge

StorageGRID 10.3 et versions ultérieures sont pris en charge.

Pour utiliser DataLock & Ransomware Resilience pour vos sauvegardes, vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou supérieure.

Pour hiérarchiser les sauvegardes plus anciennes vers le stockage d'archivage cloud, vos systèmes StorageGRID doivent exécuter la version 11.3 ou supérieure. De plus, vos systèmes StorageGRID doivent être découverts sur la page **Systèmes** de la console.

Pour le stockage d'archives des utilisateurs, un accès IP au nœud d'administration est nécessaire.

L'accès IP de la passerelle est toujours nécessaire.

Informations d'identification S3

Vous devez avoir créé un compte locataire S3 pour contrôler l'accès à votre stockage StorageGRID . "Consultez la documentation StorageGRID pour plus de détails" .

Lorsque vous configurez la sauvegarde sur StorageGRID, l'assistant de sauvegarde vous demande une clé d'accès S3 et une clé secrète pour un compte de locataire. Le compte locataire permet à NetApp Backup and Recovery d'authentifier et d'accéder aux buckets StorageGRID utilisés pour stocker les sauvegardes. Les clés sont nécessaires pour que StorageGRID sache qui fait la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Versionnage d'objet

Vous ne devez pas activer manuellement le contrôle de version des objets StorageGRID sur le bucket du magasin d'objets.

Préparez-vous à archiver les anciens fichiers de sauvegarde sur un stockage cloud public

La hiérarchisation des fichiers de sauvegarde plus anciens vers un stockage d'archives permet d'économiser de l'argent en utilisant une classe de stockage moins coûteuse pour les sauvegardes dont vous n'avez peut-être pas besoin. StorageGRID est une solution sur site (cloud privé) qui ne fournit pas de stockage d'archives, mais vous pouvez déplacer des fichiers de sauvegarde plus anciens vers un stockage d'archives dans le cloud public. Lorsqu'elles sont utilisées de cette manière, les données hiérarchisées vers le stockage cloud ou restaurées à partir du stockage cloud transitent entre StorageGRID et le stockage cloud - la console n'est pas impliquée dans ce transfert de données.

La prise en charge actuelle vous permet d'archiver les sauvegardes sur le stockage AWS *S3 Glacier*/*S3 Glacier Deep Archive* ou *Azure Archive*.

- Exigences ONTAP *
- Votre cluster doit utiliser ONTAP 9.12.1 ou une version ultérieure.
- Exigences de StorageGRID *
- Votre StorageGRID doit utiliser la version 11.4 ou supérieure.
- Votre StorageGRID doit être "découvert et disponible dans la console" .

Exigences Amazon S3

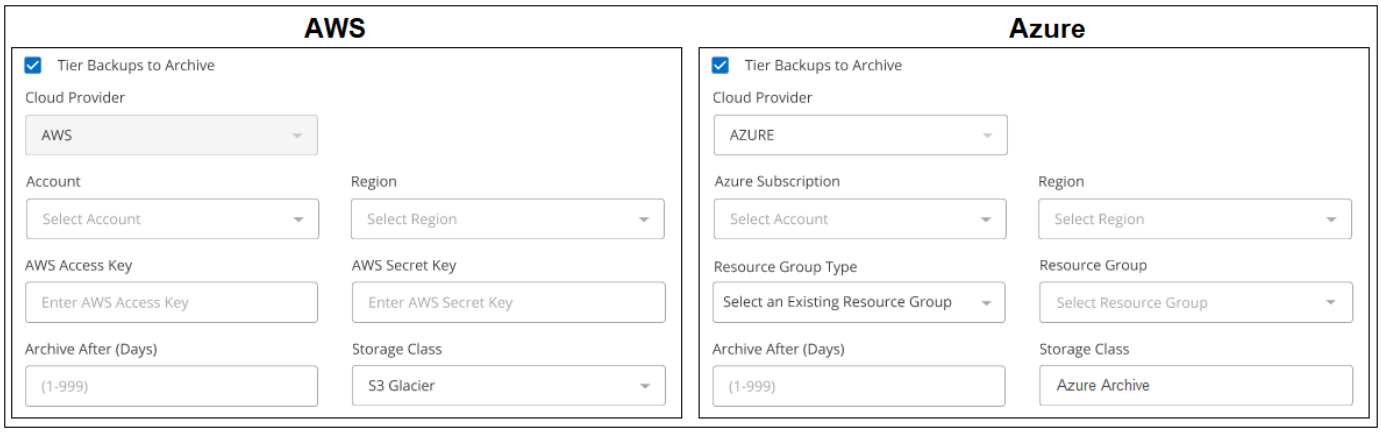
- Vous devrez créer un compte Amazon S3 pour l'espace de stockage où seront situées vos sauvegardes archivées.

- Vous pouvez choisir de hiérarchiser les sauvegardes vers le stockage AWS S3 Glacier ou S3 Glacier Deep Archive. "En savoir plus sur les niveaux d'archivage AWS" .
- StorageGRID doit avoir un accès de contrôle total au bucket(`s3:*`); cependant, si cela n'est pas possible, la politique de bucket doit accorder les autorisations S3 suivantes à StorageGRID:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Exigences Azure Blob

- Vous devrez souscrire à un abonnement Azure pour l'espace de stockage où seront situées vos sauvegardes archivées.
- L'assistant d'activation vous permet d'utiliser un groupe de ressources existant pour gérer le conteneur Blob qui stockera les sauvegardes, ou vous pouvez créer un nouveau groupe de ressources.

Lors de la définition des paramètres d'archivage pour la politique de sauvegarde de votre cluster, vous entrez les informations d'identification de votre fournisseur de cloud et sélectionnez la classe de stockage que vous souhaitez utiliser. NetApp Backup and Recovery crée le bucket cloud lorsque vous activez la sauvegarde pour le cluster. Les informations requises pour le stockage d'archives AWS et Azure sont présentées ci-dessous.



Les paramètres de politique d'archivage que vous sélectionnez généreront une politique de gestion du cycle de vie des informations (ILM) dans StorageGRID et ajouteront les paramètres en tant que « règles ».

- S'il existe une politique ILM active, de nouvelles règles seront ajoutées à la politique ILM pour déplacer les données vers le niveau d'archivage.
- S'il existe une politique ILM existante à l'état « proposé », la création et l'activation d'une nouvelle politique ILM ne seront pas possibles. "En savoir plus sur les politiques et règles ILM de StorageGRID" .

Activer les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les principales étapes suivantes :

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

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

Démarrer l'assistant

Étapes

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

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

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

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

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

2. Continuez avec les options suivantes :

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

Sélectionnez les volumes que vous souhaitez sauvegarder

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

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

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

Étapes

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

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

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

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

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

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

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

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

     - Entrez le nom de la politique.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder vers l'objet** : Si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : Sélectionnez * StorageGRID*.
   - **Paramètres du fournisseur** : saisissez les détails du nom de domaine complet (FQDN), le port, la clé d'accès et la clé secrète du nœud de passerelle du fournisseur.

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

   - **Mise en réseau** : Choisissez l'espace IP dans le cluster ONTAP où résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant (non requis lorsque l'agent de console est installé sur un site « sombre »).

     La sélection de l'espace IP correct garantit que NetApp Backup and Recovery peut établir une connexion d' ONTAP à votre stockage d'objets StorageGRID .

   - **Politique de sauvegarde** : sélectionnez une politique de sauvegarde sur stockage d'objets existante ou créez-en une.

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

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

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

Si votre cluster utilise ONTAP 9.11.1 ou une version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre la suppression et les attaques de ransomware en configurant *DataLock et Ransomware Resilience*. *DataLock* protège vos fichiers de sauvegarde contre toute modification ou suppression, et *Ransomware Resilience* analyse vos fichiers de sauvegarde pour rechercher des preuves d'une attaque de ransomware dans vos fichiers de sauvegarde.

- Sélectionnez **Créer**.

Si votre cluster utilise ONTAP 9.12.1 ou une version ultérieure et que votre système StorageGRID utilise la version 11.4 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers des niveaux d'archives de cloud public après un certain nombre de jours. La prise en charge actuelle concerne les niveaux de stockage AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. Découvrez comment configurer vos systèmes pour cette fonctionnalité .

- **Sauvegarde hiérarchisée vers le cloud public** : sélectionnez le fournisseur de cloud vers lequel vous souhaitez hiérarchiser les sauvegardes et saisissez les détails du fournisseur.

  Sélectionnez ou créez un nouveau cluster StorageGRID . Pour plus de détails sur la création d'un cluster StorageGRID afin que la console puisse le découvrir, reportez-vous à "Documentation de StorageGRID" .

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

6. Sélectionnez **Suivant**.

Revoyez vos sélections

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

Étapes

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

Résultat

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

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

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

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

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

Afficher les commandes de l'API

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

Étapes

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

Migrer des volumes à l'aide de SnapMirror vers Cloud Resync dans NetApp Backup and Recovery

La fonctionnalité SnapMirror to Cloud Resync de NetApp Backup and Recovery rationalise la protection et la continuité des données lors des migrations de volumes dans les environnements NetApp . Lorsqu'un volume est migré à l'aide de SnapMirror Logical Replication (LRSE) d'un déploiement NetApp sur site à un autre, ou vers une solution basée sur le cloud telle que Cloud Volumes ONTAP, SnapMirror to Cloud Resync garantit que les sauvegardes cloud existantes restent intactes et opérationnelles.

Cette fonctionnalité élimine le besoin d'un processus de réétablissement de la configuration de référence et permet aux sauvegardes de se poursuivre après la migration. Cette fonctionnalité est utile dans les scénarios de migration de charge de travail, prenant en charge à la fois FlexVols et FlexGroups, et est disponible à partir de la version 9.16.1 ONTAP .

Cette fonctionnalité est disponible à partir de la version 4.0.3 de NetApp Backup and Recovery publiée en mai 2025.

La resynchronisation SnapMirror vers le cloud assure la continuité des sauvegardes entre les environnements, facilitant ainsi la gestion des données dans les configurations hybrides et multicloud.

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

Avant de commencer

Assurez-vous que ces conditions préalables ont été remplies :

- Le cluster ONTAP de destination doit exécuter ONTAP version 9.16.1 ou ultérieure.
- L'ancien cluster ONTAP source doit être protégé à l'aide de NetApp Backup and Recovery.
- La fonctionnalité SnapMirror to Cloud Resync est disponible à partir de la version 4.0.3 de NetApp Backup and Recovery publiée en mai 2025.
- Assurez-vous que la dernière sauvegarde dans le stockage d'objets soit l'instantané commun à l'ancienne source, à la nouvelle source et au stockage d'objets. N'utilisez pas un instantané commun plus ancien que le dernier instantané sauvegardé sur le magasin d'objets.

- Les stratégies de snapshot et SnapMirror utilisées sur l'ancien cluster ONTAP doivent toutes deux être créées sur le nouveau cluster ONTAP avant de démarrer l'opération de resynchronisation. Si vous utilisez une stratégie quelconque lors du processus de resynchronisation, vous devez également créer cette stratégie. L'opération de resynchronisation ne crée pas de stratégies.
- Assurez-vous que la stratégie SnapMirror appliquée à la relation SnapMirror du volume de migration inclut la même étiquette que celle utilisée par la relation cloud. Pour éviter les problèmes, utilisez la politique qui régit un miroir exact du volume et de tous les instantanés.

La resynchronisation de SnapMirror vers Cloud après les migrations à l'aide des méthodes SVM-Migrate, SVM-DR ou Head Swap n'est actuellement pas prise en charge.

Comment fonctionne NetApp Backup and Recovery SnapMirror to Cloud Resync

Si vous effectuez une actualisation technique ou migrez des volumes d'un cluster ONTAP vers un autre, il est important que vos sauvegardes continuent de fonctionner sans interruption. NetApp Backup and Recovery SnapMirror to Cloud Resync vous aide à y parvenir en garantissant que vos sauvegardes cloud restent cohérentes même après une migration de volume.

Voici un exemple :

Imaginez que vous disposez d'un volume sur site appelé Vol1a. Ce volume contient trois instantanés : S1, S2 et S3. Ces instantanés sont des points de restauration. Le volume 1 est sauvegardé dans le cloud à l'aide de SnapMirror to Cloud (SM-C), mais seuls les volumes S1 et S2 sont stockés dans l'objet.

Maintenant, vous souhaitez migrer Vol1 vers un autre cluster ONTAP . Pour ce faire, vous créez une relation de réplication logique SnapMirror (LRSE) avec un nouveau volume cloud appelé Vol1b. Cela transfère les trois instantanés (S1, S2 et S3) du Vol1a au Vol1b.

Une fois la migration terminée, vous disposez de la configuration suivante :

- La relation SM-C d'origine (Vol1a → Magasin d'objets) est supprimée.
- La relation LRSE (Vol1a → Vol1b) est également supprimée.
- Vol1b est désormais votre volume actif.

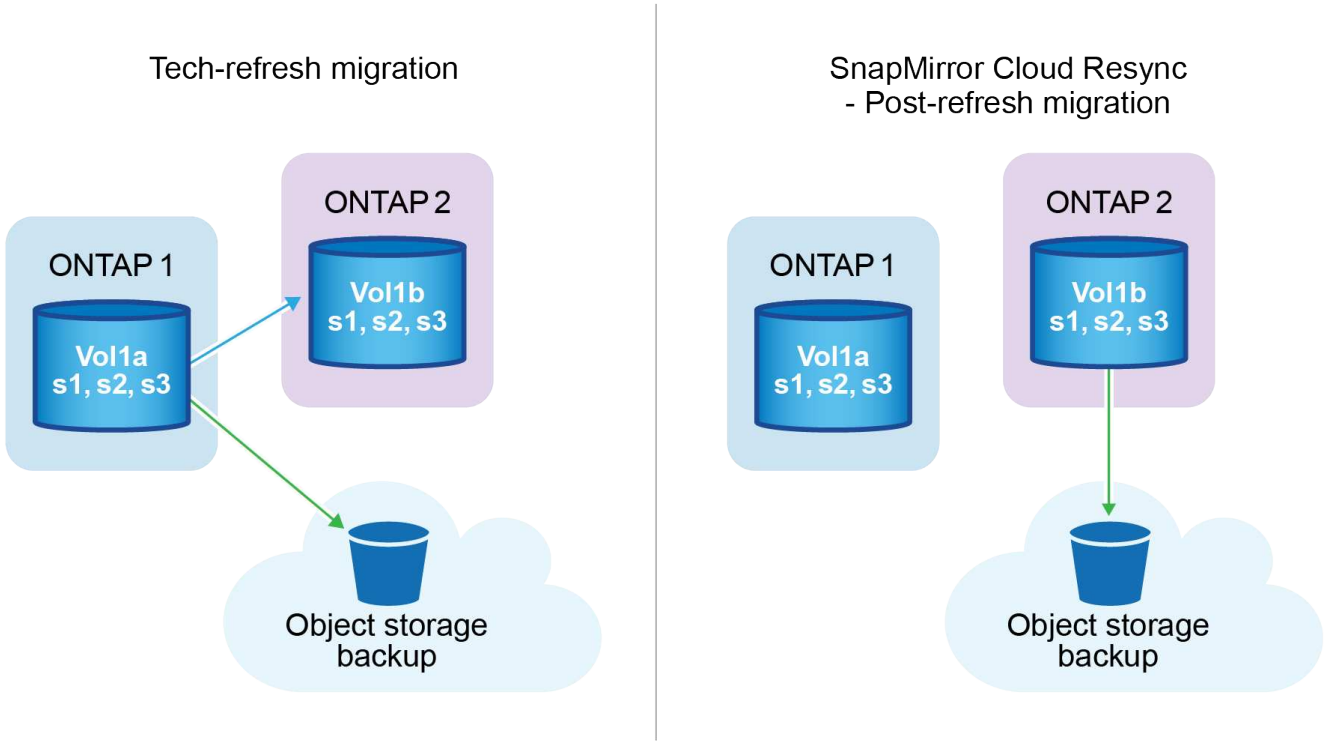
À ce stade, vous souhaitez continuer à sauvegarder Vol1b sur le même point de terminaison cloud. Mais au lieu de démarrer une sauvegarde complète à partir de zéro (ce qui prendrait du temps et des ressources), vous utilisez SnapMirror to Cloud Resync.

Voici comment fonctionne la resynchronisation :

- Le système vérifie un instantané commun entre Vol1a et le magasin d'objets. Dans ce cas, les deux ont S2.
- En raison de cet instantané partagé, le système doit transférer uniquement les modifications incrémentielles entre S2 et S3.

Cela signifie uniquement les nouvelles données ajoutées après l'envoi de S2 au magasin d'objets, et non le volume entier.

Ce processus évite les sauvegardes en double, économise de la bande passante et maintient les sauvegardes actives après la migration.



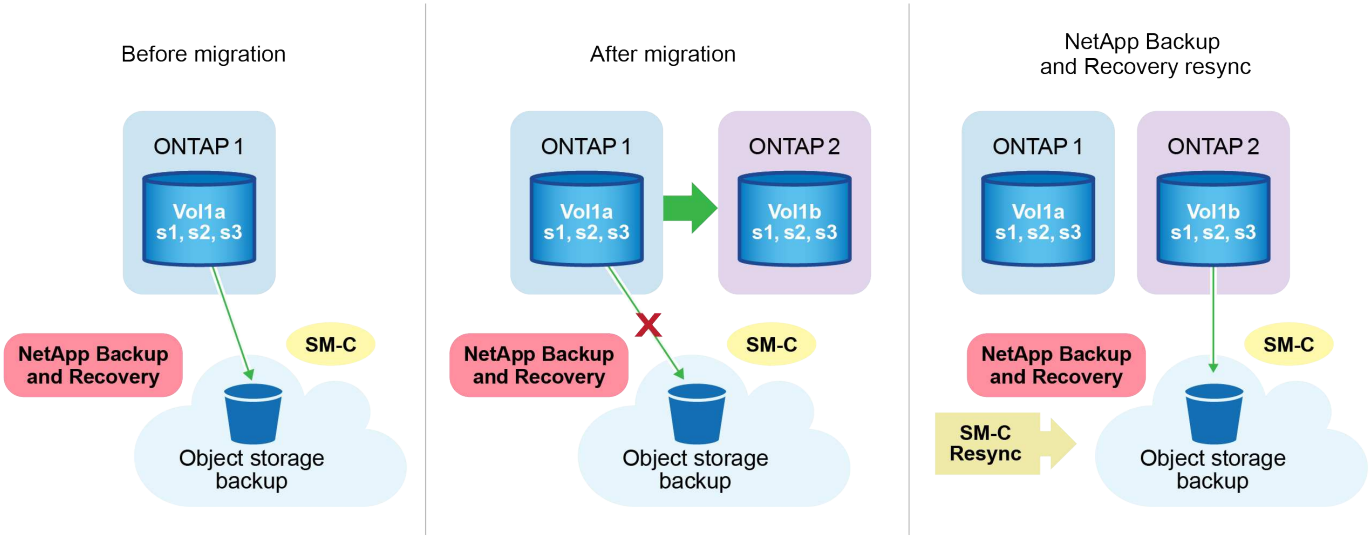
Notes de procédure

- Les migrations et les actualisations technologiques ne sont pas effectuées à l'aide de NetApp Backup and Recovery. Elles doivent être effectuées par une équipe de services professionnels ou un administrateur de stockage qualifié.
- Une équipe de migration NetApp crée la relation SnapMirror entre les clusters ONTAP source et de destination pour faciliter le déplacement des volumes.
- Assurez-vous que la migration lors d'une actualisation technologique est basée sur une migration basée sur SnapMirror.

Comment migrer des volumes à l'aide de SnapMirror vers Cloud Resync

La migration de volumes à l'aide de SnapMirror vers Cloud Resync implique les étapes principales suivantes, chacune décrite plus en détail ci-dessous :

- **Suivez une liste de contrôle de pré-migration** : Avant de commencer la migration, une équipe NetApp Tech Refresh s'assure que les conditions préalables suivantes sont remplies pour éviter la perte de données et garantir un processus de migration fluide.
- **Suivez une liste de contrôle post-migration** : après la migration, une équipe NetApp Tech Refresh s'assure que les étapes suivantes sont effectuées pour établir la protection et préparer la resynchronisation.
- **Effectuer une resynchronisation SnapMirror vers le cloud** : après la migration, une équipe NetApp Tech Refresh effectue une opération de resynchronisation SnapMirror vers le cloud pour reprendre les sauvegardes cloud à partir des volumes nouvellement migrés.



Suivez une liste de contrôle de pré-migration

Avant la migration, l'équipe NetApp Tech Refresh vérifie ces prérequis afin d'éviter toute perte de données et de garantir un processus sans accroc.

1. Assurez-vous que tous les volumes à migrer sont protégés à l'aide de NetApp Backup and Recovery.
2. Enregistrer les UUID des instances de volume. Notez les UUID d'instance de tous les volumes avant de démarrer la migration. Ces identifiants sont essentiels pour les opérations de mappage et de resynchronisation ultérieures.
3. Prenez un instantané final de chaque volume pour conserver l'état le plus récent, avant de supprimer toutes les relations SnapMirror .
4. Documenter les politiques SnapMirror . Enregistrez la politique SnapMirror actuellement attachée à la relation de chaque volume. Cela sera nécessaire plus tard lors du processus de resynchronisation de SnapMirror vers Cloud.
5. Supprimez les relations SnapMirror Cloud avec le magasin d'objets.
6. Créez une relation SnapMirror standard avec le nouveau cluster ONTAP pour migrer le volume vers le nouveau cluster ONTAP cible.

Suivez une liste de contrôle post-migration

Après la migration, une équipe NetApp Tech Refresh s'assure que les étapes suivantes sont effectuées pour établir la protection et préparer la resynchronisation.

1. Enregistrez les nouveaux UUID d'instance de volume de tous les volumes migrés dans le cluster ONTAP de destination.
2. Confirmez que toutes les stratégies SnapMirror requises qui étaient disponibles dans l'ancien cluster ONTAP sont correctement configurées dans le nouveau cluster ONTAP .
3. Ajoutez le nouveau cluster ONTAP en tant que système dans la page **Systèmes** de la console.

L'UUID de l'instance de volume doit être utilisé, et non l'ID de volume. L'UUID de l'instance de volume est un identifiant unique qui reste cohérent d'une migration à l'autre, tandis que l'ID de volume peut changer après la migration.

Effectuer une resynchronisation SnapMirror vers le Cloud

Après la migration, une équipe NetApp Tech Refresh effectue une opération SnapMirror vers Cloud Resync pour reprendre les sauvegardes cloud à partir des volumes nouvellement migrés.

1. Ajoutez le nouveau cluster ONTAP en tant que système dans la page **Systèmes** de la console.
2. Consultez la page Volumes de NetApp Backup and Recovery pour vous assurer que les détails de l'ancien système source sont disponibles.
3. Sur la page Volumes de NetApp Backup and Recovery , sélectionnez **Paramètres de sauvegarde**.
   - Dans la page Paramètres de sauvegarde, sélectionnez **Afficher tout**.
   - Dans le menu Actions… à droite de la *nouvelle* source, sélectionnez **Resynchroniser la sauvegarde**.
4. Dans la page système Resync, procédez comme suit :
   a. **Nouveau système source** : saisissez le nouveau cluster ONTAP vers lequel les volumes ont été migrés.
   b. **Magasin d'objets cible existant** : sélectionnez le magasin d'objets cible qui contient les sauvegardes de l'ancien système source.
5. Sélectionnez **Télécharger le modèle CSV** pour télécharger la feuille Excel des détails de resynchronisation. Utilisez cette feuille pour saisir les détails des volumes à migrer. Dans le fichier CSV, saisissez les détails suivants :
   - L'UUID de l'ancienne instance de volume du cluster source
   - Le nouvel UUID de l'instance de volume du cluster de destination
   - La politique SnapMirror à appliquer à la nouvelle relation.
6. Sélectionnez **Télécharger** sous **Télécharger les détails du mappage de volume** pour télécharger la feuille CSV complétée dans l'interface utilisateur de NetApp Backup and Recovery .

   L'UUID de l'instance de volume doit être utilisé, et non l'ID de volume. L'UUID de l'instance de volume est un identifiant unique qui reste cohérent d'une migration à l'autre, tandis que l'ID de volume peut changer après la migration.

7. Saisissez les informations de configuration du fournisseur et du réseau requises pour l'opération de resynchronisation.
8. Sélectionnez **Soumettre** pour démarrer le processus de validation.

   NetApp Backup and Recovery valide que chaque volume sélectionné pour la resynchronisation est le dernier snapshot et possède au moins un snapshot commun. Cela garantit que les volumes sont prêts pour l'opération de resynchronisation SnapMirror vers Cloud.

9. Examinez les résultats de la validation, y compris les nouveaux noms de volumes sources et l'état de resynchronisation de chaque volume.
10. Vérifiez l'éligibilité du volume. Le système vérifie si les volumes sont éligibles à la resynchronisation. Si un volume n'est pas éligible, cela signifie qu'il ne s'agit pas du dernier instantané ou qu'aucun instantané commun n'a été trouvé.

    Pour garantir que les volumes restent éligibles pour l'opération de resynchronisation SnapMirror vers Cloud, prenez un instantané final de chaque volume avant de supprimer toute relation SnapMirror pendant la phase de pré-migration. Cela préserve l'état le plus récent des données.

11. Sélectionnez **Resynchroniser** pour démarrer l'opération de resynchronisation. Le système utilise le snapshot le plus récent et le plus courant pour transférer uniquement les modifications incrémentielles, garantissant ainsi la continuité de la sauvegarde.
12. Surveillez le processus de resynchronisation dans la page Moniteur de tâches.

Restaurer les données de configuration de NetApp Backup and Recovery sur un site sombre

Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, appelé *mode privé*, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où vos sauvegardes sont stockées. Si vous rencontrez un problème avec le système hôte de l'agent de console, vous pouvez déployer un nouvel agent de console et restaurer les données critiques de NetApp Backup and Recovery .

Cette procédure s'applique uniquement aux données de volume ONTAP .

Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS avec l'agent de console déployé chez votre fournisseur de cloud ou sur votre propre hôte connecté à Internet, le système sauvegarde et protège toutes les données de configuration importantes dans le cloud. Si vous rencontrez un problème avec l'agent de console, créez un nouvel agent de console et ajoutez vos systèmes. Les détails de la sauvegarde sont automatiquement restaurés.

Il existe deux types de données sauvegardées :

- Base de données de NetApp Backup and Recovery : contient une liste de tous les volumes, fichiers de sauvegarde, politiques de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés - contiennent des index détaillés utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lorsque vous recherchez des données de volume que vous souhaitez restaurer.

Ces données sont sauvegardées une fois par jour à minuit et un maximum de 7 copies de chaque fichier sont conservées. Si l'agent de console gère plusieurs systèmes ONTAP sur site, les fichiers de NetApp Backup and Recovery sont stockés dans le compartiment du système qui a été activé en premier.

Aucune donnée de volume n'est jamais incluse dans la base de données NetApp Backup and Recovery ou dans les fichiers de catalogue indexés.

Restaurer les données de NetApp Backup and Recovery vers un nouvel agent de console

Si votre agent de console sur site cesse de fonctionner, vous devrez installer un nouvel agent de console, puis restaurer les données de NetApp Backup and Recovery sur le nouvel agent de console.

Vous devrez effectuer les tâches suivantes pour remettre votre système NetApp Backup and Recovery en état de fonctionnement :

- Installer un nouvel agent de console
- Restaurer la base de données de NetApp Backup and Recovery

- Restaurer les fichiers du catalogue indexé
- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site sur l'interface utilisateur de la NetApp Console

Après avoir vérifié que votre système fonctionne, créez de nouveaux fichiers de sauvegarde.

Ce dont vous aurez besoin

Vous devrez accéder aux sauvegardes de base de données et d'index les plus récentes à partir du compartiment StorageGRID ou ONTAP S3 où vos fichiers de sauvegarde sont stockés :

- Fichier de base de données MySQL de NetApp Backup and Recovery

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/mysql_backup/` , et il s'appelle `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Fichier zip de sauvegarde du catalogue indexé

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/catalog_backup/` , et il s'appelle `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installer un nouvel agent de console sur un nouvel hôte Linux local

Lors de l'installation d'un nouvel agent de console, téléchargez la même version du logiciel que l'agent d'origine. Les modifications apportées à la base de données NetApp Backup and Recovery peuvent empêcher les nouvelles versions du logiciel de fonctionner avec les anciennes sauvegardes de base de données. Tu peux "mettre à niveau le logiciel de l'agent de la console vers la version la plus récente après la restauration de la base de données de sauvegarde" .

1. "Installer l'agent de console sur un nouvel hôte Linux local"
2. Connectez-vous à la console à l'aide des informations d'identification de l'utilisateur administrateur que vous venez de créer.

Restaurer la base de données de NetApp Backup and Recovery

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte de l'agent de console. Nous utiliserons le nom de fichier d'exemple « CBS_DB_Backup_23_05_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur Docker MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

   ```
   docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
   ```

   ```
   podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
   ```

3. Accédez au shell du conteneur MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Dans le shell du conteneur, déployez « env ».
5. Vous aurez besoin du mot de passe de la base de données MySQL, copiez donc la valeur de la clé « MYSQL_ROOT_PASSWORD ».
6. Restaurez la base de données MySQL de NetApp Backup and Recovery à l'aide de la commande suivante :

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Vérifiez que la base de données MySQL de NetApp Backup and Recovery a été restaurée correctement à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

8. Entrez le mot de passe.

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

9. Vérifiez que les volumes affichés correspondent bien à ceux de votre environnement d'origine.

Restaurer les fichiers du catalogue indexé

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons le nom de fichier d'exemple « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte de l'agent de console dans le dossier « /opt/application/netapp/cbs ».
2. Décompressez le fichier « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip » à l'aide de la commande suivante :

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Exécutez la commande **ls** pour vous assurer que le dossier « catalogdb1 » a été créé avec les sous-dossiers « changes » et « snapshots » en dessous.

Découvrez vos clusters ONTAP et vos systèmes StorageGRID

1. "Découvrez tous les systèmes ONTAP sur site"qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.

2. "Découvrez vos systèmes StorageGRID".

Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos systèmes ONTAP tels qu'ils ont été configurés lors de la configuration de l'agent de console d'origine à l'aide de l' "API de la NetApp Console" .

Les informations suivantes s'appliquent aux installations en mode privé à partir de NetApp Console 3.9.xx. Pour les versions plus anciennes, utilisez la procédure suivante : "Sauvegarde Cloud DarkSite : sauvegarde et restauration de MySQL et du catalogue indexé" .

Vous devrez effectuer ces étapes pour chaque système qui sauvegarde des données sur StorageGRID.

1. Extrayez le jeton d'autorisation à l'aide de l'API oauth/token suivante.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

Alors que l'adresse IP, le nom d'utilisateur et les mots de passe sont des valeurs personnalisées, le nom du compte ne l'est pas. Le nom du compte est toujours « account-DARKSITE1 ». De plus, le nom d'utilisateur doit utiliser un nom au format e-mail.

Cette API renverra une réponse comme celle-ci. Vous pouvez récupérer le jeton d'autorisation comme indiqué ci-dessous.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extrayez l'ID système et l'ID X-Agent à l'aide de l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Cette API renverra une réponse comme celle-ci. La valeur sous « resourceIdentifier » désigne l'*ID de l'environnement de travail* et la valeur sous « agentId » désigne *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Mettez à jour la base de données NetApp Backup and Recovery avec les détails du système StorageGRID associé aux systèmes. Assurez-vous de saisir le nom de domaine complet du StorageGRID, ainsi que la clé d'accès et la clé de stockage comme indiqué ci-dessous :

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Vérifier les paramètres de NetApp Backup and Recovery

1. Sélectionnez chaque système ONTAP et cliquez sur **Afficher les sauvegardes** à côté du service de sauvegarde et de récupération dans le panneau de droite.

   Vous devriez voir toutes les sauvegardes créées pour vos volumes.

2. Depuis le tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

   Assurez-vous que les systèmes sur lesquels le catalogage indexé était précédemment activé restent activés.

3. À partir de la page Rechercher et restaurer, exécutez quelques recherches de catalogue pour confirmer que la restauration du catalogue indexé a été effectuée avec succès.

Gérez les sauvegardes de vos systèmes ONTAP avec NetApp Backup and Recovery

Avec NetApp Backup and Recovery, gérez les sauvegardes de vos systèmes Cloud Volumes ONTAP et ONTAP sur site en modifiant la planification de sauvegarde, en activant/désactivant les sauvegardes de volume, en suspendant les sauvegardes, en supprimant les sauvegardes, en forçant la suppression des sauvegardes, etc. Cela inclut tous les types de sauvegardes, y compris les instantanés, les volumes répliqués et les

fichiers de sauvegarde stockés dans des objets. Vous pouvez également désinscrire 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.

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

Afficher l'état de sauvegarde des volumes de vos systèmes

Vous pouvez afficher une liste de tous les volumes en cours de sauvegarde dans le tableau de bord de sauvegarde des volumes. Cela inclut tous les types de sauvegardes, y compris les instantanés, les volumes répliqués et les fichiers de sauvegarde stockés dans des objets. Vous pouvez également afficher les volumes des systèmes qui ne sont pas actuellement sauvegardés.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez le menu **Volumes** pour afficher la liste des volumes sauvegardés pour vos systèmes Cloud Volumes ONTAP et ONTAP sur site.
3. Si vous recherchez des volumes spécifiques dans certains systèmes, vous pouvez affiner la liste par système et par volume. Vous pouvez également utiliser le filtre de recherche ou trier les colonnes en fonction du style de volume (FlexVol ou FlexGroup), du type de volume, etc.

   Pour afficher des colonnes supplémentaires (agrégats, style de sécurité (Windows ou UNIX), politique de snapshot, politique de réplication et politique de sauvegarde), sélectionnez le signe plus.

4. Vérifiez l'état des options de protection dans la colonne « Protection existante ». Les 3 icônes représentent « Instantanés locaux », « Volumes répliqués » et « Sauvegardes dans le stockage d'objets ».

   Chaque icône 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. Sur la page *Définir la stratégie de sauvegarde*, sélectionnez l'architecture de sauvegarde, puis définissez les politiques et autres détails pour les instantanés locaux, les volumes répliqués et les fichiers de sauvegarde. Consultez les détails des options de sauvegarde des volumes initiaux que vous avez activés dans ce système. Sélectionnez ensuite **Suivant**.
3. Vérifiez les paramètres de sauvegarde de ce volume, puis sélectionnez **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde attribués aux volumes existants

Vous pouvez modifier les politiques de sauvegarde attribuées à vos volumes existants auxquels des politiques sont attribuées. Vous pouvez modifier les stratégies appliquées à vos instantanés locaux, à vos volumes répliqués et à vos fichiers de sauvegarde. Toute nouvelle stratégie de snapshot, de réplication ou de sauvegarde que vous souhaitez appliquer aux volumes doit déjà exister.

Modifier les paramètres de sauvegarde sur un seul volume

Étapes

1. Dans 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. Sur la page *Modifier la stratégie de sauvegarde*, apportez des modifications aux politiques de sauvegarde existantes pour les instantanés locaux, les volumes répliqués et les fichiers de sauvegarde, puis sélectionnez **Suivant**.

   Si vous avez activé *DataLock et Ransomware Resilience* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, vous ne verrez que les autres stratégies qui ont été configurées avec DataLock. Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne verrez que d'autres stratégies de sauvegarde cloud pour lesquelles DataLock n'est pas configuré.

3. Vérifiez les paramètres de sauvegarde de ce volume, puis sélectionnez **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde sur plusieurs volumes

Si vous souhaitez utiliser les mêmes paramètres de sauvegarde sur plusieurs volumes, vous pouvez activer ou modifier les paramètres de sauvegarde sur plusieurs volumes en même temps. Vous pouvez sélectionner des volumes qui n'ont pas de paramètres de sauvegarde, uniquement des paramètres de snapshot, uniquement des paramètres de sauvegarde dans le cloud, etc., et effectuer des modifications en masse sur tous ces volumes avec divers paramètres de sauvegarde.

Lorsque vous travaillez avec plusieurs volumes, tous les volumes doivent avoir ces caractéristiques communes :

- même système
- même style (volume FlexVol ou FlexGroup)
- même type (volume en lecture-écriture ou de protection des données)

Lorsque plus de cinq volumes sont activés pour la sauvegarde, NetApp Backup and Recovery 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**

Action de sauvegarde…	Sélectionnez ce bouton…
Gérer les paramètres de sauvegarde de réplication	**Gérer la réplication**
Gérer les paramètres de sauvegarde dans le cloud	**Gérer la sauvegarde**
Gérez plusieurs types de paramètres de sauvegarde. Cette option vous permet également de modifier l'architecture de sauvegarde.	**Gérer la sauvegarde et la récupération**

4. Sur la page de sauvegarde qui apparaît, modifiez les politiques de sauvegarde existantes pour les instantanés locaux, les volumes répliqués ou les fichiers de sauvegarde, puis sélectionnez **Enregistrer**.

   Si vous avez activé *DataLock et Ransomware Resilience* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, vous ne verrez que les autres stratégies qui ont été configurées avec DataLock. Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne verrez que d'autres stratégies de sauvegarde cloud pour lesquelles DataLock n'est pas configuré.

Créez une sauvegarde manuelle du volume à tout moment

Vous pouvez créer une sauvegarde à la demande à tout moment pour capturer l'état actuel du volume. Cela peut être utile si des modifications très importantes ont été apportées à un volume et que vous ne souhaitez pas attendre la prochaine sauvegarde planifiée pour protéger ces données. Vous pouvez également utiliser cette fonctionnalité pour créer une sauvegarde pour un volume qui n'est pas actuellement en cours de sauvegarde et dont vous souhaitez capturer l'état actuel.

Vous pouvez créer un instantané ad hoc ou une sauvegarde d'un volume. Vous ne pouvez pas créer un volume répliqué ad hoc.

Le nom de la sauvegarde inclut l'horodatage afin que vous puissiez identifier votre sauvegarde à la demande parmi d'autres sauvegardes planifiées.

Si vous avez activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery pour ce cluster, la sauvegarde à la demande sera également configurée avec DataLock et la période de conservation sera de 30 jours. Les analyses de ransomware ne sont pas prises en charge pour les sauvegardes ad hoc. "En savoir plus sur DataLock et la protection contre les ransomwares" .

Lorsque vous créez une sauvegarde ad hoc, un instantané est créé sur le volume source. Étant donné que cet instantané ne fait pas partie d'une planification d'instantanés normale, il ne sera pas désactivé. Vous souhaiterez peut-être supprimer manuellement cet instantané du volume source une fois la sauvegarde terminée. Cela permettra de libérer les blocs liés à cet instantané. Le nom de l'instantané commencera par `cbs-snapshot-adhoc-` . "Découvrez comment supprimer un instantané à l'aide de l'interface de ligne de commande ONTAP" .

> La sauvegarde de volume à la demande n'est pas prise en charge sur les volumes de protection des données.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume et sélectionnez **Sauvegarde** > **Créer une sauvegarde ad hoc**.

La colonne État de la sauvegarde pour ce volume affiche « En cours » jusqu'à ce que la sauvegarde soit créée.

Afficher la liste des sauvegardes pour chaque volume

Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche les détails sur le volume source, l'emplacement de destination et les détails de sauvegarde tels que la dernière sauvegarde effectuée, la politique de sauvegarde actuelle, la taille du fichier de sauvegarde, etc.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Afficher les détails du volume**.

   Les détails du volume et la liste des instantanés sont affichés.

2. Sélectionnez **Snapshot**, **Réplication** ou **Sauvegarde** pour voir la liste de tous les fichiers de sauvegarde pour chaque type de sauvegarde.

Exécuter une analyse de ransomware sur une sauvegarde de volume dans le stockage d'objets

NetApp Backup and Recovery analyse vos fichiers de sauvegarde pour rechercher des preuves d'une attaque de ransomware lorsqu'une sauvegarde vers un fichier objet est créée et lorsque les données d'un fichier de sauvegarde sont en cours de restauration. Vous pouvez également exécuter une analyse à la demande à tout moment pour vérifier la facilité d'utilisation d'un fichier de sauvegarde spécifique dans le stockage d'objets. Cela peut être utile si vous avez rencontré un problème de ransomware sur un volume particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

Cette fonctionnalité est disponible uniquement si la sauvegarde du volume a été créée à partir d'un système avec ONTAP 9.11.1 ou une version ultérieure, et si vous avez activé *DataLock et Ransomware Resilience* dans la stratégie de sauvegarde vers objet.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Afficher les détails du volume**.

   Les détails du volume sont affichés.

2. Sélectionnez **Sauvegarde** pour voir la liste des fichiers de sauvegarde dans le stockage d'objets.
3. Sélectionner••• pour le fichier de sauvegarde du volume que vous souhaitez analyser pour détecter les ransomwares et cliquez sur **Rechercher les ransomwares**.

   La colonne Résilience aux ransomwares indique que l'analyse est en cours.

Gérer la relation de réplication avec le volume source

Après avoir configuré la réplication des données entre deux systèmes, vous pouvez gérer la relation de réplication des données.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez l'option **Réplication**. Vous pouvez voir toutes les options disponibles.
2. Sélectionnez l'action de réplication que vous souhaitez effectuer.

   Le tableau suivant décrit les actions disponibles :

Action	Description
Afficher la réplication	Affiche les détails sur la relation de volume : informations de transfert, informations sur le dernier transfert, détails sur le volume et informations sur la politique de protection attribuée à la relation.
Mettre à jour la réplication	Démarre un transfert incrémentiel pour mettre à jour le volume de destination à synchroniser avec le volume source.
Suspendre la réplication	Interrompez le transfert incrémentiel des instantanés pour mettre à jour le volume de destination. Vous pouvez reprendre plus tard si vous souhaitez redémarrer les mises à jour incrémentielles.
Interrompre la réplication	Rompt la relation entre les volumes source et de destination et active le volume de destination pour l'accès aux données - le rend en lecture-écriture. Cette option est généralement utilisée lorsque le volume source ne peut pas fournir de données en raison d'événements tels qu'une corruption de données, une suppression accidentelle ou un état hors ligne.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["Découvrez comment configurer un volume de destination pour l'accès aux données et réactiver un volume source dans la documentation ONTAP"^]
Abandonner la réplication	Désactive les sauvegardes de ce volume sur le système de destination et désactive également la possibilité de restaurer un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne supprime pas la relation de protection des données entre les volumes source et de destination.
Resynchronisation inversée	Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est écrasé par le contenu du volume de destination. Cela est utile lorsque vous souhaitez réactiver un volume source qui est devenu hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et le moment où le volume source a été désactivé ne sont pas conservées.
Supprimer la relation	Supprime la relation de protection des données entre les volumes source et de destination, ce qui signifie que la réplication des données ne se produit plus entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données, ce qui signifie qu'il n'est pas accessible en lecture-écriture. Cette action supprime également la relation d'homologue de cluster et la relation d'homologue de machine virtuelle de stockage (SVM), s'il n'existe aucune autre relation de protection des données entre les systèmes.

Résultat

Après avoir sélectionné une action, la console met à jour la relation.

Modifier une politique de sauvegarde dans le cloud existante

Vous pouvez modifier les attributs d'une politique de sauvegarde actuellement appliquée aux volumes d'un système. La modification de la politique de sauvegarde affecte tous les volumes existants qui utilisent la politique.

- Si vous avez activé *DataLock et Ransomware Resilience* dans la stratégie initiale lors de l'activation de NetApp Backup and Recovery pour ce cluster, toutes les stratégies que vous modifiez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et Ransomware Resilience* lors de l'activation de NetApp Backup and Recovery, vous ne pouvez pas activer DataLock maintenant.
- Lors de la création de sauvegardes sur AWS, si vous avez choisi *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première politique de sauvegarde lors de l'activation de NetApp Backup and Recovery, ce niveau sera le seul niveau d'archivage disponible lors de la modification des politiques de sauvegarde. Et si vous n'avez sélectionné aucun niveau d'archivage dans votre première politique de sauvegarde, *S3 Glacier* sera votre seule option d'archivage lors de la modification d'une politique.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez modifier les paramètres de stratégie, puis sélectionnez **Gérer les stratégies**.
3. Depuis la page *Gérer les politiques*, sélectionnez **Modifier** pour la politique de sauvegarde que vous souhaitez modifier dans ce système.
4. Depuis la page *Modifier la politique*, sélectionnez la flèche vers le bas pour développer la section *Étiquettes et rétention* afin de modifier la planification et/ou la rétention de sauvegarde, puis sélectionnez **Enregistrer**.

   Si votre cluster exécute ONTAP 9.10.1 ou une version ultérieure, vous avez également la possibilité d'activer ou de désactiver la hiérarchisation des sauvegardes vers le stockage d'archivage après un certain nombre de jours.

"En savoir plus sur l'utilisation du stockage d'archives AWS".

"En savoir plus sur l'utilisation du stockage d'archives Azure".

"En savoir plus sur l'utilisation du stockage d'archives Google". (Nécessite ONTAP 9.12.1.)

+ Notez que 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 instantanés ni les volumes répliqués ; ces types de fichiers de sauvegarde ne sont pas supprimés.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Sélectionner••• pour le système où vous souhaitez supprimer toutes les sauvegardes et sélectionnez **Supprimer toutes les sauvegardes**.
3. Dans la boîte de dialogue de confirmation, entrez le nom du système.
4. Sélectionnez **Paramètres avancés**.
5. **Forcer la suppression des sauvegardes** : Indiquez si vous souhaitez ou non forcer la suppression de toutes les sauvegardes.

   Dans certains cas extrêmes, vous souhaiterez peut-être que NetApp Backup and Recovery n'ait plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau du volume et du système).

   > Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. NetApp Backup and Recovery n'aura plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

6. Sélectionnez **Supprimer**.

Supprimer tous les fichiers de sauvegarde d'un volume

La suppression de toutes les sauvegardes d'un volume désactive également les sauvegardes futures pour ce volume.

Étapes

1. Dans l'onglet **Volumes**, cliquez sur••• pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

   La liste de tous les fichiers de sauvegarde s'affiche.

2. Sélectionnez **Actions** > **Supprimer toutes les sauvegardes**.
3. Entrez le nom du volume.
4. Sélectionnez **Paramètres avancés**.
5. **Forcer la suppression des sauvegardes** : Indiquez si vous souhaitez ou non forcer la suppression de toutes les sauvegardes.

   Dans certains cas extrêmes, vous souhaiterez peut-être que NetApp Backup and Recovery n'ait plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de

sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau du volume et du système).

> Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. NetApp Backup and Recovery n'aura plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

6. Sélectionnez **Supprimer**.

Supprimer un seul fichier de sauvegarde pour un volume

Vous pouvez supprimer un seul fichier de sauvegarde si vous n'en avez plus besoin. Cela inclut la suppression d'une seule sauvegarde d'un instantané de volume ou d'une sauvegarde dans un stockage d'objets.

Vous ne pouvez pas supprimer les volumes répliqués (volumes de protection des données).

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Afficher les détails du volume**.

   Les détails du volume sont affichés et vous pouvez sélectionner **Snapshot**, **Réplication** ou **Sauvegarde** pour voir la liste de tous les fichiers de sauvegarde du volume. Par défaut, les instantanés disponibles sont affichés.

2. Sélectionnez **Instantané** ou **Sauvegarde** pour voir le type de fichiers de sauvegarde que vous souhaitez supprimer.
3. Sélectionner••• pour le fichier de sauvegarde du volume que vous souhaitez supprimer et sélectionnez **Supprimer**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer**.

Supprimer les relations de sauvegarde de volume

La suppression de la relation de sauvegarde d'un volume vous fournit un mécanisme d'archivage si vous souhaitez arrêter la création de nouveaux fichiers de sauvegarde et supprimer le volume source, mais conserver tous les fichiers de sauvegarde existants. Cela vous donne la possibilité de restaurer le volume à partir du fichier de sauvegarde à l'avenir, si nécessaire, tout en libérant de l'espace sur votre système de stockage source.

Vous n'avez pas nécessairement besoin de supprimer le volume source. Vous pouvez supprimer la relation de sauvegarde d'un volume et conserver le volume source. Dans ce cas, vous pouvez « activer » la sauvegarde sur le volume ultérieurement. Dans ce cas, la copie de sauvegarde de base d'origine continue d'être utilisée : une nouvelle copie de sauvegarde de base n'est pas créée ni exportée vers le cloud. Notez que si vous réactivez une relation de sauvegarde, la politique de sauvegarde par défaut est attribuée au volume.

Cette fonctionnalité est disponible uniquement si votre système exécute ONTAP 9.12.1 ou une version ultérieure.

Vous ne pouvez pas supprimer le volume source de l'interface utilisateur de NetApp Backup and Recovery . Cependant, vous pouvez ouvrir la page Détails du volume sur la page **Systèmes** de la console et "supprimer le volume à partir de là" .

Vous ne pouvez pas supprimer les fichiers de sauvegarde de volume individuels une fois la relation supprimée. Vous pouvez cependant supprimer toutes les sauvegardes du volume.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez••• pour le volume source et sélectionnez **Sauvegarde** > **Supprimer la relation**.

Désactiver NetApp Backup and Recovery pour un système

La désactivation de NetApp Backup and Recovery pour un système désactive les sauvegardes de chaque volume du système et désactive également la possibilité de restaurer un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne désenregistre pas le service de sauvegarde de ce système. Cela vous permet essentiellement de suspendre toutes les activités de sauvegarde et de restauration pendant un certain temps.

Notez que votre fournisseur de cloud continuera à vous facturer les coûts de stockage d'objets pour la capacité utilisée par vos sauvegardes, sauf si voussupprimer les sauvegardes .

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez désactiver les sauvegardes et sélectionnez **Désactiver la sauvegarde**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Désactiver**.

Un bouton **Activer la sauvegarde** apparaît pour ce système lorsque la sauvegarde est désactivée. Vous pouvez sélectionner ce bouton lorsque vous souhaitez réactiver la fonctionnalité de sauvegarde pour ce système.

Annuler l'enregistrement de NetApp Backup and Recovery pour un système

Vous pouvez annuler l'enregistrement de NetApp Backup and Recovery pour un système si vous ne souhaitez plus utiliser la fonctionnalité de sauvegarde et que vous souhaitez cesser d'être facturé pour les sauvegardes dans ce système. En général, cette fonctionnalité est utilisée lorsque vous prévoyez de supprimer un système et que vous souhaitez annuler le service de sauvegarde.

Vous pouvez également utiliser cette fonctionnalité si vous souhaitez modifier le magasin d'objets de destination dans lequel vos sauvegardes de cluster sont stockées. Après avoir désenregistré NetApp Backup and Recovery pour le système, vous pouvez activer NetApp Backup and Recovery pour ce cluster à l'aide des informations du nouveau fournisseur de cloud.

Avant de pouvoir désinscrire NetApp Backup and Recovery, vous devez effectuer les étapes suivantes, dans cet ordre :

- Désactiver NetApp Backup and Recovery pour le système
- Supprimer toutes les sauvegardes de ce système

L'option de désinscription n'est pas disponible tant que ces deux actions ne sont pas terminées.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez **Paramètres de sauvegarde**.

2. Depuis la page *Paramètres de sauvegarde*, sélectionnez••• pour le système sur lequel vous souhaitez désinscrire le service de sauvegarde et sélectionnez **Désinscrire**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Désinscrire**.

Restaurer à partir des sauvegardes ONTAP

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

Les sauvegardes de vos données de volume ONTAP sont stockées sous forme d'instantanés, sur des volumes répliqués ou dans un stockage objet. Vous pouvez restaurer des données à partir de n'importe lequel de ces emplacements à un moment précis. Avec NetApp Backup and Recovery, vous pouvez restaurer un volume entier, un dossier ou des fichiers individuels selon vos besoins.

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

- Vous pouvez restaurer un **volume** (en tant que nouveau volume) sur le système d'origine, sur un autre système utilisant le même compte cloud ou sur un système ONTAP sur site.
- Vous pouvez restaurer un **dossier** sur un volume du système d'origine, sur un volume d'un autre système utilisant le même compte cloud ou sur un volume d'un système ONTAP local.
- Vous pouvez restaurer des **fichiers** sur un volume du système d'origine, sur un volume d'un autre système utilisant le même compte cloud ou sur un volume d'un système ONTAP local.

Vous avez besoin d'une licence NetApp Backup and Recovery valide pour restaurer des données sur un système de production.

Pour résumer, voici les flux valides que vous pouvez utiliser pour restaurer des données de volume sur un système ONTAP :

- Fichier de sauvegarde → volume restauré
- Volume répliqué → volume restauré
- Instantané → volume restauré

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

Pour connaître les limitations liées à la restauration des données ONTAP , consultez"Limitations de sauvegarde et de restauration pour les volumes ONTAP" .

Le tableau de bord de restauration

Vous utilisez le tableau de bord de restauration pour effectuer des opérations de restauration de volumes, de dossiers et de fichiers. Pour accéder au tableau de bord de restauration, sélectionnez **Sauvegarde et récupération** dans le menu Console, puis sélectionnez l'onglet **Restaurer**. Vous pouvez également sélectionner > **Afficher le tableau de bord de restauration** à partir du service de sauvegarde et de récupération du panneau Services.

NetApp Backup and Recovery doit déjà être activé pour au moins un système et les fichiers de sauvegarde initiaux doivent exister.

Le tableau de bord de restauration propose deux manières différentes de restaurer des données à partir de fichiers de sauvegarde : **Parcourir et restaurer** et **Rechercher et restaurer**.

Comparaison de Parcourir et restaurer et de Rechercher et restaurer

En termes généraux, *Parcourir et restaurer* est généralement préférable lorsque vous devez restaurer un volume, un dossier ou un fichier spécifique de la semaine ou du mois dernier - et que vous connaissez le nom et l'emplacement du fichier, ainsi que la date à laquelle il était en bon état pour la dernière fois. *Rechercher et restaurer* est généralement plus efficace lorsque vous devez restaurer un volume, un dossier ou un fichier, mais que vous ne vous souvenez pas du nom exact, du volume dans lequel il réside ou de la date à laquelle il était en bon état pour la dernière fois.

Ce tableau fournit une comparaison des fonctionnalités des deux méthodes.

Parcourir et restaurer	Rechercher et restaurer
Parcourez une structure de type dossier pour trouver le volume, le dossier ou le fichier dans un seul fichier de sauvegarde.	Recherchez un volume, un dossier ou un fichier dans **tous les fichiers de sauvegarde** par nom de volume partiel ou complet, nom de dossier/fichier partiel ou complet, plage de taille et filtres de recherche supplémentaires.
Ne gère pas la récupération de fichier si le fichier a été supprimé ou renommé et que l'utilisateur ne connaît pas le nom du fichier d'origine	Gère les répertoires nouvellement créés/supprimés/renommés et les fichiers nouvellement créés/supprimés/renommés
La restauration rapide est prise en charge.	La restauration rapide n'est pas prise en charge.

Ce tableau fournit une liste d'opérations de restauration valides en fonction de l'emplacement où résident vos fichiers de sauvegarde.

Type de sauvegarde	Parcourir et restaurer			Rechercher et restaurer		
	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier
Instantané	Oui	Non	Non	Oui	Oui	Oui
Volume répliqué	Oui	Non	Non	Oui	Oui	Oui
Fichier de sauvegarde	Oui	Oui	Oui	Oui	Oui	Oui

Avant d'utiliser l'une ou l'autre méthode de restauration, configurez votre environnement pour qu'il réponde aux exigences en ressources. Consultez les sections suivantes pour plus de détails.

Consultez les exigences et les étapes de restauration pour le type d'opération de restauration que vous souhaitez utiliser :

- "Restaurer les volumes à l'aide de Parcourir et restaurer"

- "Restaurer des dossiers et des fichiers à l'aide de Parcourir et restaurer"
- "Restaurer des volumes, des dossiers et des fichiers à l'aide de la recherche et de la restauration"

Restaurez les données à partir des sauvegardes ONTAP à l'aide de la fonction Rechercher et restaurer.

Vous pouvez utiliser la fonction Rechercher et restaurer pour récupérer des volumes, des dossiers ou des fichiers à partir de fichiers de sauvegarde ONTAP . La fonction Recherche et restauration vous permet d'effectuer des recherches dans toutes les sauvegardes (y compris les instantanés locaux, les volumes répliqués et le stockage d'objets) sans avoir besoin des noms exacts du système, du volume ou des fichiers.

La restauration à partir d'instantanés locaux ou de volumes répliqués est généralement plus rapide et moins coûteuse que la restauration à partir d'un stockage objet.

Lors de la restauration d'un volume complet, NetApp Backup and Recovery crée un nouveau volume à partir des données de sauvegarde. Vous pouvez effectuer une restauration sur le système d'origine, sur un autre système du même compte cloud ou sur un système ONTAP sur site. Les dossiers et les fichiers peuvent être restaurés à leur emplacement d'origine, sur un autre volume du même système, sur un autre système du même compte cloud ou sur un système sur site.

Les fonctionnalités de restauration dépendent de votre version ONTAP :

- **Dossiers :** Avec ONTAP 9.13.0 ou une version supérieure, vous pouvez restaurer des dossiers avec tous les fichiers et sous-dossiers ; avec les versions antérieures, vous ne pouvez restaurer que les fichiers contenus dans le dossier.
- **Stockage d'archives :** La restauration à partir du stockage d'archives (disponible avec ONTAP 9.10.1 ou supérieur) est plus lente et peut entraîner des coûts supplémentaires.
- **Exigences relatives aux clusters de destination :**
  - Restauration du volume : ONTAP 9.10.1 ou version ultérieure
  - Restauration de fichiers : ONTAP 9.11.1 ou version ultérieure
  - Google Archive et StorageGRID: ONTAP 9.12.1 ou version ultérieure
  - Restauration de dossiers : ONTAP 9.13.1 ou version ultérieure

"En savoir plus sur la restauration à partir du stockage d'archives AWS".

"En savoir plus sur la restauration à partir du stockage d'archives Azure".

"En savoir plus sur la restauration à partir du stockage d'archives Google".

- Si le fichier de sauvegarde dans le stockage d'objets a été configuré avec la protection DataLock et Ransomware, la restauration au niveau du dossier n'est prise en charge que si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Si le fichier de sauvegarde dans le stockage d'objets réside dans le stockage d'archives, la restauration au niveau du dossier est prise en charge uniquement si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer l'intégralité du volume à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.
- La priorité de restauration « Élevée » n'est pas prise en charge lors de la restauration des données du stockage d'archivage Azure vers les systèmes StorageGRID .
- La restauration de dossiers n'est actuellement pas prise en charge à partir de volumes dans le stockage d'objets ONTAP S3.

Avant de commencer, vous devez avoir une idée du nom ou de l'emplacement du volume ou du fichier que vous souhaitez restaurer.

Systèmes pris en charge par la recherche et la restauration et fournisseurs de stockage d'objets

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

Remarque : vous pouvez restaurer des volumes et des fichiers à partir de n'importe quel type de fichier de sauvegarde, mais vous ne pouvez restaurer un dossier qu'à partir de fichiers de sauvegarde dans le stockage d'objets pour le moment.

Emplacement du fichier de sauvegarde		**Système de destination**
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	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 de recherche et de restauration

Assurez-vous que votre environnement répond à ces exigences avant d'activer la fonction Rechercher et restaurer :

- Exigences du cluster :
  - La version ONTAP doit être 9.8 ou supérieure.
  - La machine virtuelle de stockage (SVM) sur laquelle réside le volume doit avoir un LIF de données configuré.
  - NFS doit être activé sur le volume (les volumes NFS et SMB/CIFS sont pris en charge).
  - Le serveur SnapDiff RPC doit être activé sur le SVM. La console le fait automatiquement lorsque vous activez l'indexation sur le système. (SnapDiff est la technologie qui identifie rapidement les différences entre les fichiers et les répertoires dans les instantanés.)
- NetApp recommande de monter un volume distinct sur l'agent Console pour améliorer la résilience de la fonction Recherche et restauration. Pour les instructions, reportez-vous àmonter le volume pour réindexer le catalogue .

Prérequis pour la recherche et la restauration héritées (avec Indexed Catalog v1)

Voici les exigences relatives à la recherche et à la restauration lors de l'utilisation de l'indexation héritée :

- Exigences AWS :
  - Des autorisations spécifiques Amazon Athena, AWS Glue et AWS S3 doivent être ajoutées au rôle d'utilisateur qui fournit des autorisations à la console. "Assurez-vous que toutes les autorisations sont correctement configurées" .

    Notez que si vous utilisiez déjà NetApp Backup and Recovery avec un agent de console que vous avez configuré dans le passé, vous devrez désormais ajouter les autorisations Athena et Glue au rôle d'utilisateur de la console. Ils sont nécessaires pour la recherche et la restauration.

- Exigences Azure :
  - Vous devez enregistrer le fournisseur de ressources Azure Synapse Analytics (appelé « Microsoft.Synapse ») avec votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement" . Vous devez être le **Propriétaire** ou le **Contributeur** de l'abonnement pour enregistrer le fournisseur de ressources.
  - Des autorisations spécifiques au compte Azure Synapse Workspace et Data Lake Storage doivent être ajoutées au rôle d'utilisateur qui fournit des autorisations à la console. "Assurez-vous que toutes les autorisations sont correctement configurées" .

    Notez que si vous utilisiez déjà NetApp Backup and Recovery avec un agent de console que vous avez configuré dans le passé, vous devrez désormais ajouter les autorisations du compte Azure Synapse Workspace et Data Lake Storage au rôle d'utilisateur de la console. Ils sont nécessaires pour la recherche et la restauration.

  - L'agent de console doit être configuré **sans** serveur proxy pour la communication HTTP vers Internet. Si vous avez configuré un serveur proxy HTTP pour votre agent de console, vous ne pouvez pas utiliser la fonctionnalité de recherche et de restauration.
- Exigences de Google Cloud :
  - Des autorisations Google BigQuery spécifiques doivent être ajoutées au rôle d'utilisateur qui fournit des autorisations à la NetApp Console . "Assurez-vous que toutes les autorisations sont correctement configurées" .

    Si vous utilisiez déjà NetApp Backup and Recovery avec un agent de console que vous avez configuré dans le passé, vous devrez maintenant ajouter les autorisations BigQuery au rôle d'utilisateur de la console. Ils sont nécessaires pour la recherche et la restauration.

- Exigences StorageGRID et ONTAP S3 :

  Selon votre configuration, la recherche et la restauration sont implémentées de deux manières :

  - S'il n'y a pas d'informations d'identification de fournisseur cloud dans votre compte, les informations du catalogue indexé sont stockées sur l'agent de la console.

    Pour plus d'informations sur le catalogue indexé v2, consultez la section ci-dessous expliquant comment activer le catalogue indexé.

  - Si vous utilisez un agent de console sur un site privé (sombre), les informations du catalogue indexé sont stockées sur l'agent de console (nécessite la version 3.9.25 ou supérieure de l'agent de console).
  - Si vous avez "Informations d'identification AWS" ou "Informations d'identification Azure" dans le compte, le catalogue indexé est alors stocké chez le fournisseur de cloud, tout comme avec un agent de console déployé dans le cloud. (Si vous disposez des deux informations d'identification,

AWS est sélectionné par défaut.)

Même si vous utilisez un agent de console sur site, les exigences du fournisseur de cloud doivent être respectées pour les autorisations de l'agent de console et les ressources du fournisseur de cloud. Consultez les exigences AWS et Azure ci-dessus lors de l'utilisation de cette implémentation.

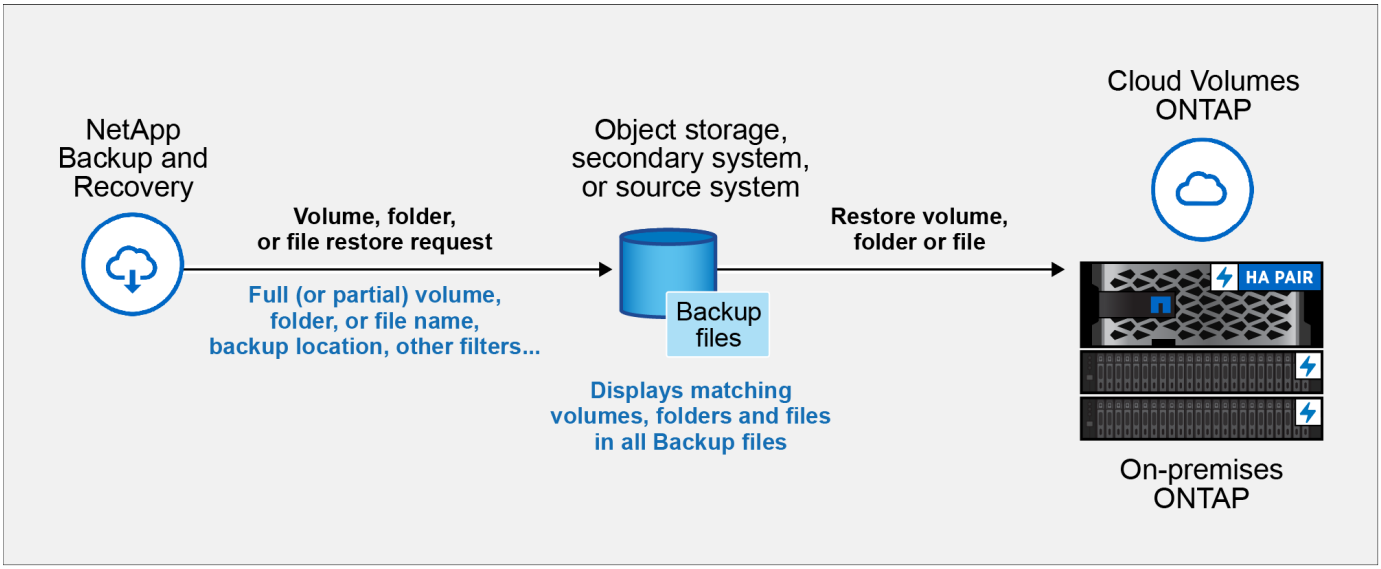
Processus de recherche et de restauration

Le processus se déroule comme suit :

1. Avant de pouvoir utiliser la recherche et la restauration, vous devez activer « Indexation » sur chaque système source à partir duquel vous souhaitez restaurer les données du volume. Cela permet au catalogue indexé de suivre les fichiers de sauvegarde pour chaque volume.
2. Lorsque vous souhaitez restaurer un volume ou des fichiers à partir d'une sauvegarde de volume, sous *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
3. Saisissez les critères de recherche d'un volume, d'un dossier ou d'un fichier par nom de volume partiel ou complet, nom de fichier partiel ou complet, emplacement de sauvegarde, plage de taille, plage de dates de création, autres filtres de recherche, puis sélectionnez **Rechercher**.

   La page Résultats de la recherche affiche tous les emplacements contenant un fichier ou un volume correspondant à vos critères de recherche.

4. Sélectionnez **Afficher toutes les sauvegardes** pour l'emplacement que vous souhaitez utiliser pour restaurer le volume ou le fichier, puis sélectionnez **Restaurer** sur le fichier de sauvegarde réel que vous souhaitez utiliser.
5. Sélectionnez l'emplacement où vous souhaitez que le volume, le dossier ou les fichiers soient restaurés et sélectionnez **Restaurer**.
6. Le volume, le dossier ou le(s) fichier(s) sont restaurés.



Il vous suffit de connaître une partie du nom, et NetApp Backup and Recovery effectue une recherche dans tous les fichiers de sauvegarde correspondants.

Activer le catalogue indexé pour chaque système

Avant de pouvoir utiliser la recherche et la restauration, vous devez activer « Indexation » sur chaque système source à partir duquel vous prévoyez de restaurer des volumes ou des fichiers. Cela permet au catalogue indexé de suivre chaque volume et chaque fichier de sauvegarde, ce qui rend vos recherches très rapides et efficaces.

Le catalogue indexé est une base de données qui stocke les métadonnées sur tous les volumes et fichiers de sauvegarde de votre système. Il est utilisé par la fonctionnalité Rechercher et restaurer pour trouver rapidement les fichiers de sauvegarde contenant les données que vous souhaitez restaurer.

Fonctionnalités du catalogue indexé

NetApp Backup and Recovery ne provisionne pas de compartiment séparé lorsque vous utilisez le catalogue indexé. Au lieu de cela, pour les sauvegardes stockées dans AWS, Azure, Google Cloud Platform, StorageGRID ou ONTAP S3, le service fournit de l'espace sur l'agent de la console ou sur l'environnement du fournisseur de cloud.

Le catalogue indexé prend en charge les éléments suivants :

- Efficacité de la recherche globale en moins de 3 minutes
- Jusqu'à 5 milliards de fichiers
- Jusqu'à 5 000 volumes par cluster
- Jusqu'à 100 000 instantanés par volume
- Le délai maximal pour l'indexation de base est inférieur à 7 jours. Le temps réel varie en fonction de votre environnement.

Étapes pour activer l'indexation pour un système :

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

Vous devrez d'abord monter un volume séparé pour stocker les fichiers de catalogue. Cela évite la perte de données si la taille des fichiers contenant les instantanés devient trop importante. Cela n'est pas nécessaire sur tous les clusters ; vous pouvez monter n'importe quel volume provenant de n'importe quel cluster de votre environnement. Si vous ne le faites pas, l'indexation risque de ne pas fonctionner correctement.

Pour le volume monté, utilisez les indications de dimensionnement suivantes :

- Utilisez un volume NFS NetApp
- Stockage AFF recommandé avec un débit disque de 300 Mo/s. La baisse du débit aura un impact sur la recherche et les autres opérations.
- Activez les instantanés NetApp pour sécuriser les métadonnées du catalogue en plus des fichiers zip de sauvegarde du catalogue.
- 50 Go par milliard de fichiers
- 20 Go pour les données du catalogue, avec un espace supplémentaire pour la création de fichiers zip et les fichiers temporaires.

Étape pour monter le volume afin de réindexer le catalogue

1. Montez le volume sur `/opt/application/netapp/cbs` en saisissant la commande suivante, où :
    - `volume name` est le volume du cluster où seront stockés les fichiers de catalogue
    - `/opt/application/netapp/cbs` est le chemin où il est monté

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

Exemple:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Étapes pour activer l'index

1. Effectuez l'une des opérations suivantes :
   - Si aucun système n'a été indexé, sur le tableau de bord de restauration sous *Rechercher et restaurer*, sélectionnez **Activer l'indexation pour les systèmes**.
   - Si au moins un système a déjà été indexé, sur le tableau de bord de restauration sous *Rechercher et restaurer*, sélectionnez **Paramètres d'indexation**.
2. Sélectionnez **Activer l'indexation** pour le système.

Résultat

Une fois tous les services provisionnés et le catalogue indexé activé, le système s'affiche comme « Actif ».

Selon la taille des volumes du système et le nombre de fichiers de sauvegarde dans les 3 emplacements de sauvegarde, le processus d'indexation initial peut prendre jusqu'à une heure. Après cela, il est mis à jour de manière transparente toutes les heures avec des modifications progressives pour rester à jour.

Restaurer des volumes, des dossiers et des fichiers à l'aide de la recherche et de la restauration

Après avoirActivation de l'indexation pour votre système , vous pouvez restaurer des volumes, des dossiers et des fichiers à l'aide de la recherche et de la restauration. Cela vous permet d'utiliser une large gamme de filtres pour trouver le fichier ou le volume exact que vous souhaitez restaurer à partir de tous les fichiers de sauvegarde.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
4. Dans la section *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
5. Depuis la page Rechercher et restaurer :
   a. Dans la *barre de recherche*, saisissez un nom de volume, un nom de dossier ou un nom de fichier complet ou partiel.
   b. Sélectionnez le type de ressource : **Volumes**, **Fichiers**, **Dossiers** ou **Tous**.
   c. Dans la zone *Filtrer par*, sélectionnez les critères de filtre. Par exemple, vous pouvez sélectionner le système sur lequel résident les données et le type de fichier, par exemple un fichier .JPEG. Vous pouvez également sélectionner le type d'emplacement de sauvegarde si vous souhaitez effectuer la recherche uniquement parmi les instantanés ou les fichiers de sauvegarde disponibles dans le stockage d'objets.
6. Sélectionnez **Rechercher** et la zone Résultats de la recherche affiche toutes les ressources qui ont un fichier, un dossier ou un volume correspondant à votre recherche.

7. Recherchez la ressource contenant les données que vous souhaitez restaurer et sélectionnez **Afficher toutes les sauvegardes** pour afficher tous les fichiers de sauvegarde contenant le volume, le dossier ou le fichier correspondant.
8. Localisez le fichier de sauvegarde que vous souhaitez utiliser pour restaurer les données et sélectionnez **Restaurer**.

   Notez que les résultats identifient les instantanés de volumes locaux et les volumes répliqués distants qui contiennent le fichier recherché. Vous pouvez choisir de restaurer à partir du fichier de sauvegarde cloud, à partir de l'instantané ou à partir du volume répliqué.

9. Sélectionnez l'emplacement de destination où vous souhaitez que le volume, le dossier ou les fichiers soient restaurés et sélectionnez **Restaurer**.
   - Pour les volumes, vous pouvez sélectionner le système de destination d'origine ou un autre système. Lors de la restauration d'un volume FlexGroup , vous devrez choisir plusieurs agrégats.
   - Pour les dossiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, notamment le système, le volume et le dossier.
   - Pour les fichiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, notamment le système, le volume et le dossier. Lors de la sélection de l'emplacement d'origine, vous pouvez choisir d'écraser le(s) fichier(s) source ou de créer de nouveaux fichiers.

     Si vous sélectionnez un système ONTAP sur site et que vous n'avez pas encore configuré la connexion du cluster au stockage d'objets, vous êtes invité à fournir des informations supplémentaires :

     - Lors de la restauration à partir d'Amazon S3, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, entrez la clé d'accès et la clé secrète de l'utilisateur que vous avez créé pour donner au cluster ONTAP l'accès au compartiment S3 et choisissez éventuellement un point de terminaison VPC privé pour un transfert de données sécurisé. "Voir les détails sur ces exigences" .
       - Lors de la restauration à partir d'Azure Blob, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination et choisissez éventuellement un point de terminaison privé pour le transfert de données sécurisé en sélectionnant le réseau virtuel et le sous-réseau. "Voir les détails sur ces exigences" .
       - Lors de la restauration à partir de Google Cloud Storage, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, ainsi que la clé d'accès et la clé secrète pour accéder au stockage d'objets. "Voir les détails sur ces exigences" .
       - Lors de la restauration à partir de StorageGRID, entrez le nom de domaine complet du serveur StorageGRID et le port ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où réside le volume de destination. "Voir les détails sur ces exigences" .
       - Lors de la restauration à partir d' ONTAP S3, saisissez le nom de domaine complet du serveur ONTAP S3 et le port ONTAP doit utiliser pour la communication HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où résidera le volume de destination. "Voir les détails sur ces exigences" .

Résultats

Le volume, le dossier ou les fichiers sont restaurés et vous revenez au tableau de bord de restauration afin que vous puissiez examiner la progression de l'opération de restauration. Vous pouvez également sélectionner l'onglet **Surveillance des tâches** pour voir la progression de la restauration. Voir"Page de surveillance des

tâches" .

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

Avec NetApp Backup and Recovery, restaurez les données ONTAP à l'aide de Browse & Restore. Avant la restauration, notez le nom du volume source, le système source et le SVM, ainsi que la date du fichier de sauvegarde. Vous pouvez restaurer les données ONTAP à partir d'un instantané, d'un volume répliqué ou de sauvegardes stockées dans un stockage objet.

Les fonctionnalités de restauration dépendent de votre version ONTAP :

- **Dossiers :** Avec ONTAP 9.13.0 ou une version supérieure, vous pouvez restaurer des dossiers avec tous les fichiers et sous-dossiers ; avec les versions antérieures, vous ne pouvez restaurer que les fichiers contenus dans le dossier.
- **Stockage d'archives :** La restauration à partir du stockage d'archives (disponible avec ONTAP 9.10.1 ou supérieur) est plus lente et peut entraîner des coûts supplémentaires.
- **Exigences relatives aux clusters de destination :**
  - Restauration du volume : ONTAP 9.10.1 ou version ultérieure
  - Restauration de fichiers : ONTAP 9.11.1 ou version ultérieure
  - Google Archive et StorageGRID: ONTAP 9.12.1 ou version ultérieure
  - Restauration de dossiers : ONTAP 9.13.1 ou version ultérieure

"En savoir plus sur la restauration à partir du stockage d'archives AWS".

"En savoir plus sur la restauration à partir du stockage d'archives Azure".

"En savoir plus sur la restauration à partir du stockage d'archives Google".

La priorité élevée n'est pas prise en charge lors de la restauration des données du stockage d'archivage Azure vers les systèmes StorageGRID .

Parcourir et restaurer les systèmes pris en charge et les fournisseurs de stockage d'objets

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

Remarque : vous pouvez restaurer un volume à partir de n'importe quel type de fichier de sauvegarde, mais vous ne pouvez restaurer un dossier ou des fichiers individuels qu'à partir d'un fichier de sauvegarde dans le stockage d'objets pour le moment.

Depuis le magasin d'objets (sauvegarde)	Depuis le primaire (instantané)	Depuis le système secondaire (réplication)	Vers le système de destination 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

Depuis le magasin d'objets (sauvegarde)	Depuis le primaire (instantané)	Depuis le système secondaire (réplication)	Vers le système de destination ifdef::aws[]
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.

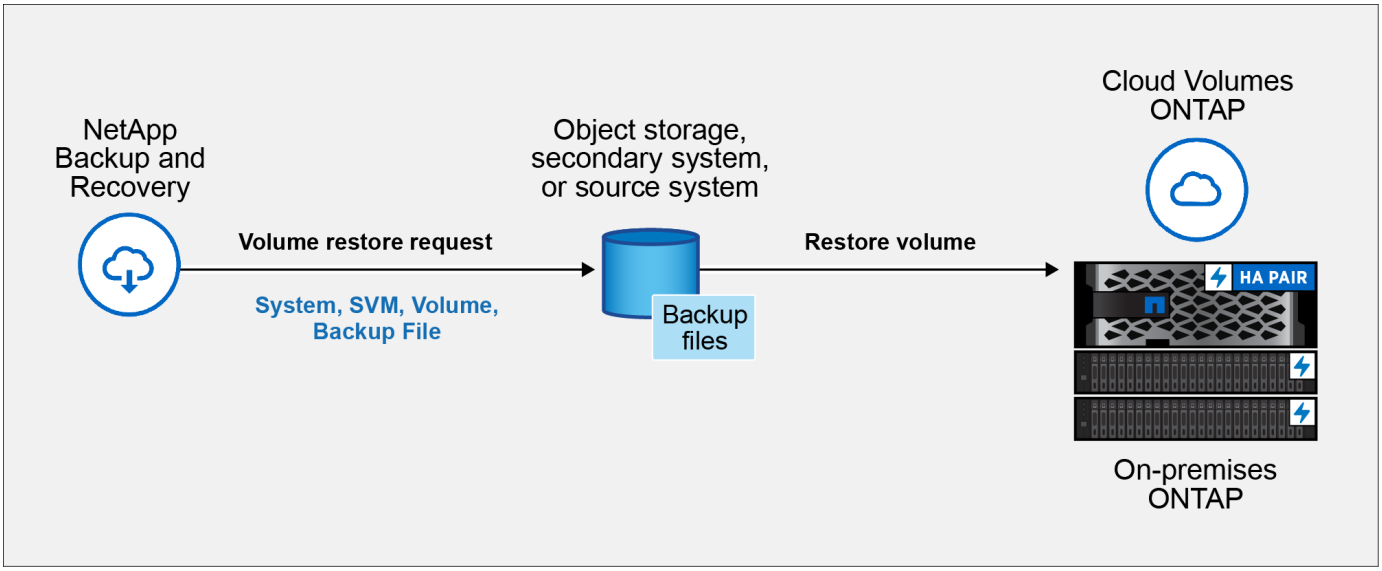
Restaurer les volumes à l'aide de Parcourir et restaurer

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.



Pour restaurer un volume, vous avez besoin du nom du système source, de la machine virtuelle de stockage, du nom du volume et de la date du fichier de sauvegarde.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Parcourir et restaurer*, sélectionnez **Restaurer le volume**.
4. Dans la page *Sélectionner la source*, accédez au fichier de sauvegarde du volume que vous souhaitez restaurer. Sélectionnez le **système**, le **volume** et le fichier de **sauvegarde** contenant l'horodatage à partir duquel vous souhaitez effectuer la restauration.

   La colonne **Emplacement** indique si le fichier de sauvegarde (instantané) est **Local** (un instantané sur le système source), **Secondaire** (un volume répliqué sur un système ONTAP secondaire) ou **Stockage d'objets** (un fichier de sauvegarde dans le stockage d'objets). Choisissez le fichier que vous souhaitez restaurer.

5. Sélectionnez **Suivant**.

   Notez que si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que Ransomware Resilience est actif pour cette sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la politique de sauvegarde), vous êtes invité à exécuter une analyse de ransomware supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'analyser le fichier de sauvegarde à la recherche de ransomwares. (Vous devrez payer des frais de sortie supplémentaires auprès de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.)

6. Dans la page *Sélectionner la destination*, sélectionnez le **système** sur lequel vous souhaitez restaurer le volume.
7. Lors de la restauration d'un fichier de sauvegarde à partir du stockage d'objets, si vous sélectionnez un système ONTAP local et que vous n'avez pas déjà configuré la connexion du cluster au stockage d'objets, vous êtes invité à fournir des informations supplémentaires :
   - Lors de la restauration à partir d'Amazon S3, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, entrez la clé d'accès et la clé secrète de l'utilisateur que vous avez

créé pour donner au cluster ONTAP l'accès au compartiment S3 et choisissez éventuellement un point de terminaison VPC privé pour un transfert de données sécurisé.

- Lors de la restauration à partir d'Azure Blob, sélectionnez l'espace IP dans le cluster ONTAP où résidera le volume de destination, sélectionnez l'abonnement Azure pour accéder au stockage d'objets et choisissez éventuellement un point de terminaison privé pour le transfert de données sécurisé en sélectionnant le réseau virtuel et le sous-réseau.
- Lors de la restauration à partir de Google Cloud Storage, sélectionnez le projet Google Cloud et la clé d'accès et la clé secrète pour accéder au stockage d'objets, la région où les sauvegardes sont stockées et l'espace IP dans le cluster ONTAP où résidera le volume de destination.
- Lors de la restauration à partir de StorageGRID, saisissez le nom de domaine complet du serveur StorageGRID et le port ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où résidera le volume de destination.
- Lors de la restauration à partir d' ONTAP S3, saisissez le nom de domaine complet du serveur ONTAP S3 et le port ONTAP doit utiliser pour la communication HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où résidera le volume de destination.

  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'un instantané local ou d'un fichier de sauvegarde situé sur un système secondaire (un volume répliqué).

Si vous sélectionnez plusieurs fichiers, ils seront restaurés sur le même volume de destination. Pour restaurer des fichiers sur différents volumes, exécutez le processus plusieurs fois.

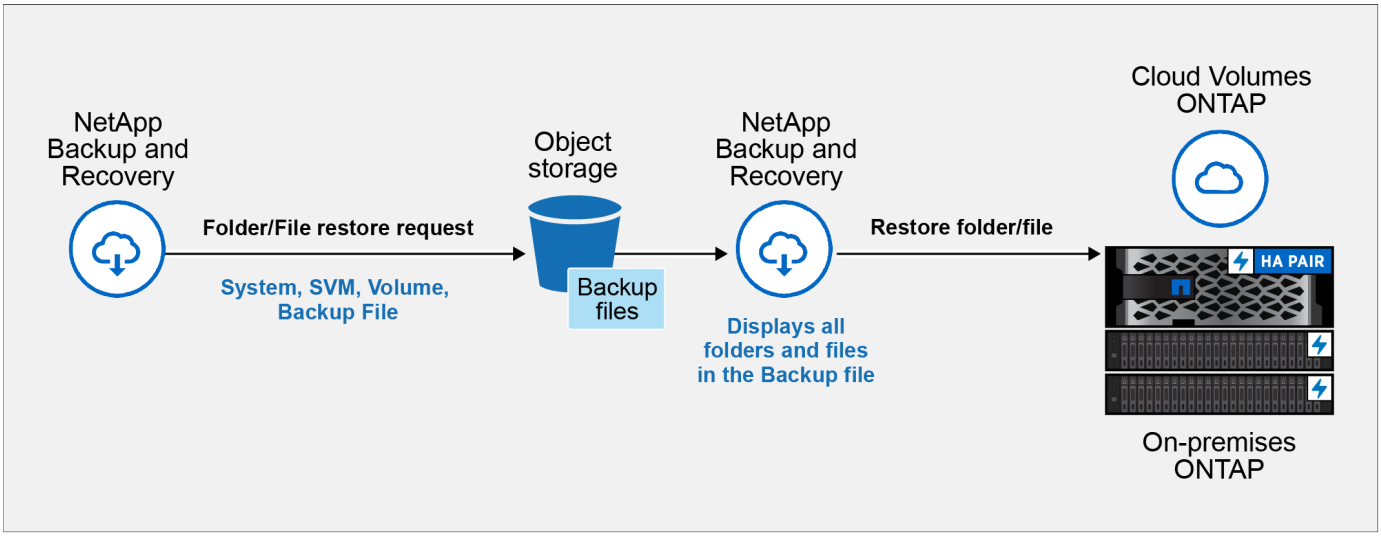
Lorsque vous utilisez ONTAP 9.13.0 ou une version ultérieure, vous pouvez restaurer un dossier avec tous les fichiers et sous-dossiers qu'il contient. Lorsque vous utilisez une version d' ONTAP antérieure à 9.13.0, seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans les sous-dossiers, n'est restauré.

- Si le fichier de sauvegarde a été configuré avec la protection DataLock et Ransomware, la restauration au niveau du dossier n'est prise en charge que si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Si le fichier de sauvegarde réside dans un stockage d'archives, la restauration au niveau du dossier n'est prise en charge que si la version ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure d' ONTAP, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer l'intégralité du volume à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Avec ONTAP 9.15.1, vous pouvez restaurer les dossiers FlexGroup à l'aide de l'option « Parcourir et restaurer ». Cette fonctionnalité est en mode Aperçu technologique.

  Vous pouvez le tester en utilisant un indicateur spécial décrit dans le "Blog sur la version de juillet 2024 de NetApp Backup and Recovery" .

Restaurer des dossiers et des fichiers

Suivez ces étapes pour restaurer des dossiers ou des fichiers sur un volume à partir d'une sauvegarde de volume ONTAP . Vous devez connaître le nom du volume et la date du fichier de sauvegarde que vous souhaitez utiliser pour restaurer le dossier ou le(s) fichier(s). Cette fonctionnalité utilise la navigation en direct pour que vous puissiez afficher la liste des répertoires et des fichiers dans chaque fichier de sauvegarde.



Avant de commencer

- La version ONTAP doit être 9.6 ou supérieure pour effectuer des opérations de restauration de *fichier*.
- La version ONTAP doit être 9.11.1 ou supérieure pour effectuer des opérations de restauration de *dossier*. La version 9.13.1 ONTAP est requise si les données sont stockées dans un stockage d'archives ou si le fichier de sauvegarde utilise la protection DataLock et Ransomware.
- La version ONTAP doit être 9.15.1 p2 ou supérieure pour restaurer les répertoires FlexGroup à l'aide de l'option Parcourir et restaurer.

Étapes

1. Dans le menu de la console, sélectionnez **Protection > Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Parcourir et restaurer*, sélectionnez **Restaurer les fichiers ou le dossier**.
4. Dans la page *Sélectionner la source*, accédez au fichier de sauvegarde du volume qui contient le dossier ou les fichiers que vous souhaitez restaurer. Sélectionnez le **système**, le **volume** et la **sauvegarde** contenant la date et l'heure à partir desquelles vous souhaitez restaurer les fichiers.
5. Sélectionnez **Suivant** et la liste des dossiers et fichiers de la sauvegarde du volume s'affiche.

   Si vous restaurez des dossiers ou des fichiers à partir d'un fichier de sauvegarde qui réside dans un niveau de stockage d'archivage, vous pouvez sélectionner la priorité de restauration.

   "En savoir plus sur la restauration à partir du stockage d'archives AWS". "En savoir plus sur la restauration à partir du stockage d'archives Azure" . "En savoir plus sur la restauration à partir du stockage d'archives Google" . Les fichiers de sauvegarde dans le niveau de stockage Google Archive sont restaurés presque immédiatement et ne nécessitent aucune priorité de restauration.

   Et si Ransomware Resilience est actif pour le fichier de sauvegarde (si vous avez activé DataLock et Ransomware Resilience dans la politique de sauvegarde), vous êtes alors invité à exécuter une analyse de ransomware supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'analyser le fichier de sauvegarde à la recherche de ransomwares. (Vous devrez payer des frais de sortie supplémentaires auprès de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.)

6. Dans la page *Sélectionner les éléments*, sélectionnez le dossier ou le(s) fichier(s) que vous souhaitez restaurer et sélectionnez **Continuer**. Pour vous aider à trouver l'article :

- Vous pouvez sélectionner le nom du dossier ou du fichier si vous le voyez.
- Vous pouvez sélectionner l'icône de recherche et saisir le nom du dossier ou du fichier pour accéder directement à l'élément.
- Vous pouvez parcourir les niveaux vers le bas dans les dossiers en utilisant la flèche vers le bas à la fin de la ligne pour rechercher des fichiers spécifiques.

  Au fur et à mesure que vous sélectionnez des fichiers, ils sont ajoutés sur le côté gauche de la page afin que vous puissiez voir les fichiers que vous avez déjà choisis. Vous pouvez supprimer un fichier de cette liste si nécessaire en sélectionnant le **x** à côté du nom du fichier.

7. Dans la page *Sélectionner la destination*, sélectionnez le **système** sur lequel vous souhaitez restaurer les éléments.

   Si vous sélectionnez un cluster sur site et que vous n'avez pas encore configuré la connexion du cluster au stockage d'objets, vous êtes invité à fournir des informations supplémentaires :

   - Lors de la restauration à partir d'Amazon S3, saisissez l'espace IP dans le cluster ONTAP où réside le volume de destination, ainsi que la clé d'accès AWS et la clé secrète nécessaires pour accéder au stockage d'objets. Vous pouvez également sélectionner une configuration de lien privé pour la connexion au cluster.
     - Lors de la restauration à partir d'Azure Blob, entrez l'espace IP dans le cluster ONTAP où réside le volume de destination. Vous pouvez également sélectionner une configuration de point de terminaison privé pour la connexion au cluster.
     - Lors de la restauration à partir de Google Cloud Storage, saisissez l'espace IP dans le cluster ONTAP où résident les volumes de destination, ainsi que la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets.
     - Lors de la restauration à partir de StorageGRID, entrez le nom de domaine complet du serveur StorageGRID et le port ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage d'objets, ainsi que l'espace IP dans le cluster ONTAP où réside le volume de destination.

       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** pour revenir au tableau de bord de restauration et consulter la progression de l'opération de restauration.